

Best Practices for Oracle FMW Identity and Access Management (11.1.2.3): Extending an Enterprise Deployment with Oracle Privileged Account

ORACLE WHITE PAPER | JULY 2016





Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. 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 for Oracle's products remains at the sole discretion of Oracle.



ORACLE®




Table of Contents

Disclaimer	1
Introduction	1
The Enterprise Deployment Topology with OPAM	1
Typical Memory, File Descriptors, and Processes Required for an Oracle Identity and Access Management Enterprise Deployment	3
Overview	2
Prerequisites	2
Creating a Highly Available Database	2
Encrypt the OPAM schema in the Database	2
Creating OPAM Users and Groups in LDAP	3
Creating a Configuration File	3
Create User and Groups using idmConfigTool.	3
Extending Domain for OPAM	4
Restarting Administration Server on OIMHOST1	7
Deploying Managed Server Configuration to Local Storage	7
Configure Managed Servers for Node Manager SSL	8
Configure OPAM	9
Disable SSL	9
Add Load Balancer Certificate to Trust Stores	10
Load the Certificate into the JDK and Node Manager Trust Stores	11
Adding OPAM Servers to Start and Stop Scripts	12
Starting and Validating OPAM	12

Starting OPAM on OIMHOST1	12
Validating OIMHOST1	12
Starting OPAM on OIMHOST2	13
Validating OIMHOST2	13
Configuring OPAM to Work with Web Tier	13
Configuring Access from Oracle Traffic Director	13
Create an OTD server Pool for OPAM	13
Create OTD Routes	14
Deploying a Configuration Using the Administration Console	14
Configuring Access from Oracle HTTP Server	14
Updating IGDADMIN.example.com	15
Updating prov.example.com	15
Restarting Oracle HTTP Servers and OPAM Managed Servers	15
Validating the Web Tier	15
Create OAM Policy for OPAM	15
Configuring OPAM Console to use the OPAM Cluster	16
Configuring OPAM to Manage a Target	16
Add Host as a Target to OPAM	17
Assign Privileged Accounts to OPAM to Manage	17
Grant a User Access to the Account	18
Validating OPAM	18
Integrating OPAM with Oracle Identity Manager	18
Configure IT Resource	19

The Oracle logo, consisting of the word "ORACLE" in white, uppercase letters on a red rectangular background.



Create an Identity Management Sandbox	20
Create a UI form for the new IT Resource	20
Create an Application for OPAM in OIM	20
Publish Sandbox	21
Integrate OPAM with OIM using opamSetup.sh	21
Creating the OPAM_TAGS UDF	22
Create an Identity Management Sandbox	22
Create a Custom Field	23
Publish Sandbox	23
Tagging Catalog Entries with OPAM Metadata	24



Introduction

The Oracle Enterprise Deployment Guide for Identity and Access Management 11.1.2.3 describes how to setup an Enterprise Deployment of Oracle Identity and Access Management. By following the processes in this guide, you can setup a mission critical deployment of:

- » Oracle Unified Directory
- » Oracle Access Manager
- » Oracle Identity Manager

This document describes how to take this deployment and extend it further with Oracle Privileged Account Manager.

Oracle Privileged Account Manager is a secure password management solution designed to generate, provision, and manage access to passwords for privileged accounts like Linux/Unix 'root' or Oracle database 'sys'. It enables auditing and establishes accountability for users who normally share privileged account credentials. OPAM, together with Oracle Identity Manager (OIM) and Oracle Identity Analytics (OIA), forms the complete Oracle Identity Governance platform that provides central governance for regular users and privileged users, complete auditing, reporting and certification of user's regular accounts and shared accounts, and lifecycle management from request, approval, to certification and usage tracking. OPAM greatly enhances security and significantly improves compliance. This document describes how to extend an already provisioned Identity and Access Management solution with Oracle Privileged Account Manager. It follows the best practices established in the Enterprise Deployment Guide to extend an already existing deployment.

This document is to be used only after the steps in the Enterprise Deployment Guide have been completed. It covers the steps for both traditional and Exalogic Implementations.

Note: You will not be able to patch OPAM using Patch Manager.

The Enterprise Deployment Topology with OPAM

After completing the steps in this document your Enterprise Deployment Topology will look like the following:

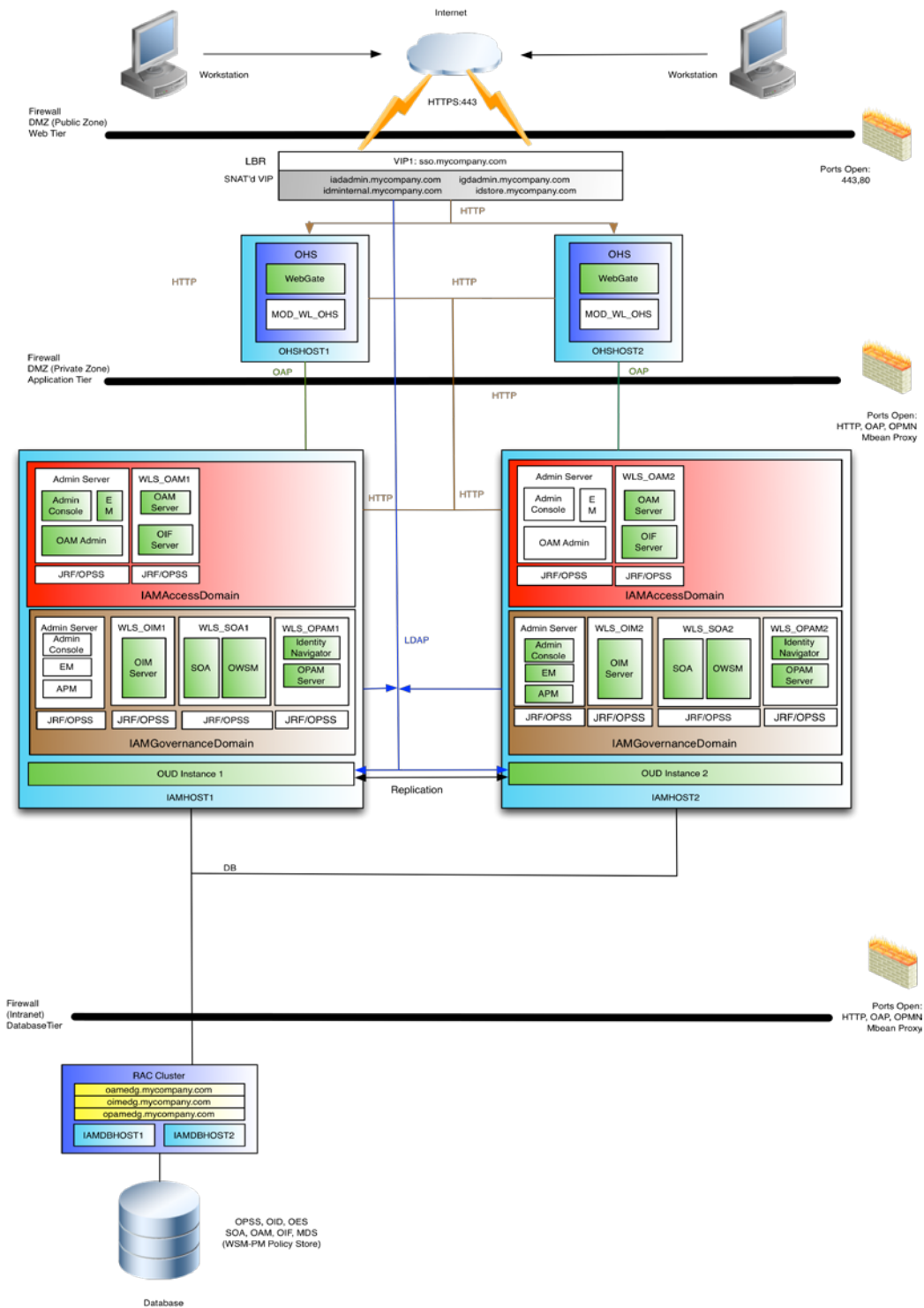


Figure 1. OPAM Deployment Topology

Typical Memory, File Descriptors, and Processes Required for an Oracle Identity and Access Management Enterprise Deployment

Table 1 summarizes the memory, file descriptors, and processes required for the Administration Server and each of the Managed Servers computers in a typical Oracle SOA Suite enterprise deployment. These values are provided as an example only, but they can be used to estimate the minimum amount of memory required for an initial enterprise deployment.

The example in Table 1 reflects the minimum requirements for configuring the Managed Servers and other services required on IAMHOST1, as depicted in the reference topologies in Section Deployment Topology

When you are procuring machines, use the information in the Approximate Top Memory column as a guide when determining how much physical memory each host computer should have available.

After you procure the host computer hardware and verify the operating system requirements, review the software configuration to be sure the operating system settings are configured to accommodate the number of open files listed in the File Descriptors column and the number processes listed in the Operating System Processes and Tasks column..

TABLE 1: TYPICAL MEMORY, FILE DESCRIPTORS, AND PROCESSES REQUIRED FOR EACH ENTERPRISE DEPLOYMENT HOST

Managed Server, Utility, or Service	Approximate Top Memory	Number of File Descriptors	Operating System Processes and Tasks
Access Administration Server	3 GB	1300	180
Governance Administration Server	3 GB	2100	100
WLS_SOA	2 GB	1400	210
WLS_OIM	2 GB	1400	190
WLS_BI	2 GB	900	100
WLS_OAM	1 GB	900	170
WLS_AMA	2 GB	1200	160
WLS_MSM	2 GB	900	120
Node Manager	268 MB	300	20



Overview

The process consists of the following steps:

- » Ensuring necessary Perquisites have been met.
- » Create OPAM Administrative User and Groups in LDAP
- » Extend the IAMGovernanceDomain with OPAM
- » Encrypt OPAM Schema
- » Configure OPAM
- » Disable OPAM SSL
- » Add Load Balancer Certificate to JDK Trust Store
- » Add OPAM to system Start and Stop Scripts
- » Integrate OPAM with the Web Tier
- » Configure Oracle Identity Navigator to use OPAM cluster
- » Configure OPAM to Manage a Target
- » Integrate OPAM with OIM

Prerequisites

Before you extend the domain to include Oracle Privileged account Manager (OPAM)), the following prerequisites must be in place.

Creating a Highly Available Database

Create a highly available database to hold the OPAM data, if you are not using the IAMDB. Pre- seed the database with OPAM data objects using the repository creation utility as described in [Oracle Fusion Middleware Repository Creation Utility](#) selecting the schema Oracle Privileged Account Manager.

This document refers to the OPAM schema name as “*igdedg_opam*” and the database service name same as the service created for the IAMGovernanceDomain, ‘*IGDEDG.EXAMPLE.COM*’.

Note it is highly recommended that Transparent Data Encryption is enabled on the database. This document assumes that it is.

Encrypt the OPAM schema in the Database

Oracle Privileged account manager requires that the information in the OPAM schema be encrypted. In order to do this you must have configured your database to use Transparent Database Encryption as described in the Oracle Advanced Security Administrators Guide:

<http://www.oracle.com/pls/topic/lookup?ctx=idm111220&id=ASOAG9522>

Once TDE is enabled the OPAM schema needs to be encrypted. This is achieved by running the sql script opamxencrypt.sql which is located in the directory *IAM_ORACLE_HOME/opam/sql*

For example

```
sqlplus EDGIGD_OPAM/password @opamxencrypt.sql
```

where:

EDGIGD_OPAM is the OPAM schema username

Note: You will have to run this command on a host which has sqlplus installed this will usually be the database host itself. In this scenario copy the file to the database machine before executing the command.

Creating OPAM Users and Groups in LDAP

Create OPAM Users and Groups as follows.

Creating a Configuration File

Create a configuration file with the following contents:

```
# Common
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 1389
IDSTORE_ADMIN_PORT: 4444
IDSTORE_BINDDN: cn=oudadmin
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_APMUSER: opamadmin
```

Where:


Note Values in *Italics* refer to document variables defined in the Oracle Enterprise Deployment Guide for Identity and Access Management 11.1.2.3

- » *IDSTORE_HOST* and *IDSTORE_PORT* (*LDAP_PORT*) are, respectively, the host and port of your Identity Store directory. This should point to the load balancer entry point for the directory instances, for example *idstore.example.com* and 1389
- » *IDSTORE_ADMIN_PORT* (*LDAP_ADMIN_PORT*) is the administration port of your Oracle Unified Directory instance.
- » *IDSTORE_BINDDN* is an administrative user in the Identity Store Directory for example *cn=oudadmin*
- » *IDSTORE_SEARCHBASE* is the location in the directory where users and groups are stored. This is the same as the *REALM_DN* defined in for example: *cn=Users,dc=example,dc=com*
- » *IDSTORE_GROUPSEARCHBASE* is the location in the directory where groups are stored. This is composed of *cn=Groups* combined with the *REALM_DN* for example *cn=Groups,dc=example,dc=com*
- » *IDSTORE_USERSEARCHBASE* is the location in the directory where users are stored. This is composed of *cn=Users* combined with the *REALM_DN* defined for example: *cn=Users,dc=example,dc=com*
- » *IDSTORE_USERNAMEATTRIBUTE* is the name of the directory attribute containing the user's name, for example: *cn*. Note that this is different from the login name.
- » *IDSTORE_LOGINATTRIBUTE* is the LDAP attribute, which contains the users Login name, for example: *uid*.
- » *IDSTORE_OPAMUSER* is the name of the user you want to create as your Oracle Adaptive Privileged Account Administrator for example *opamadmin*

Create User and Groups using idmConfigTool.

You must seed the Identity Store with users and groups that are required by the Identity and Access Management components. To seed the Identity Store, perform the following tasks on OIMHOST1:

1. Set environment variables.



Set MW_HOME to IGD_MW_HOME.

Set ORACLE_HOME to IGD_ORACLE_HOME.

Set JAVA_HOME to JAVA_HOME.

2. Configure the Identity Store by using the command `idmConfigTool`, which is located at: `IGD_ORACLE_HOME/idmtools/bin`

The syntax of the command on Linux is:

```
idmConfigTool.sh -prepareIDStore mode=APM input_file=configfile
```

Where

`configfile` is the name of the configuration file you created at the beginning of this section.

When the command runs, you are prompted to enter the password of the account you are connecting to the Identity Store with.

After running each command, check the log file for any errors or warnings and correct them. The file with the name `automation.log` is created in the directory where you run the tool.

Extending Domain for OPAM

Start the configuration wizard by executing the following command on OIMHOST1:

```
IGD_MW_HOME/oracle_common/common/bin/config.sh
```

Note: The domain must be stopped before performing these steps

Then proceed as follows:

1. On the Welcome Screen, select Extend an Existing WebLogic Domain. Click Next.
2. On the Select a WebLogic Domain screen, using the navigator select the domain home of the Administration Server, for example: `IGD_ASERVER_HOME` (IAMGovernanceDomain)
Click Next.
3. On the Select Extension Source screen, select the following:
Oracle Privileged Account Manager
Click **Next**.
4. On the Configure JDBC Component Schema screen, do the following:
Select: OPAM Schema
Select Convert to GridLink.
Click **Next**.
5. The Gridlink RAC Component Schema screen appears. In this screen, enter values for the following fields, specifying the connect information for the Oracle RAC database that was seeded with RCU.
Driver: Select Oracle's driver (Thin) for GridLink Connections, Versions:10 and later.
Select Enable FAN.
Do one of the following:

● If SSL is not configured for ONS notifications to be encrypted, deselect SSL.

Or

- Select SSL and provide the appropriate wallet and wallet password.

Service Listener: Enter the SCAN address and port for the RAC database being used. You can identify this address by querying the parameter **remote_listener** in the database:

```
SQL>show parameter remote_listener;
NAME          TYPE        VALUE
-----
remote_listener string      DB-SCAN.EXAMPLE.COM:1521
```

ONS Host: Enter the SCAN address for the Oracle RAC database and the ONS remote port as reported by the database:

Note:

For Oracle Database 11g Release 1 (11.1), use the virtual IP and port of each database instance listener, for example: DBHOST1- VIP.example.com (port 1521) and DBHOST2-VIP.example.com (port 1521), where 1521 is *DB_LSNR_PORT*

```
srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016
```

Note:

For Oracle Database 11g Release 1 (11.1), use the hostname and port of each database's ONS service, for example:

DBHOST1.example.com (port 6200)

and

DBHOST2.example.com (port 6200)

Enter the following RAC component schema information:

Schema Name: OPAM Schema

Service Name: igdedg.us.oracle.com

Schema Owner: EDGIGD_OPAM

Password: Password for the above account.

Click **Next**.

6. On the Test Component Schema screen, the configuration wizard attempts to validate the data source. If the data source validation succeeds, click **Next**.

If it fails, click Previous, correct the issue, and try again.

7. On the Select Optional Configuration screen,
Select Managed Server Clusters and Machines.

Click **Next**.

8. When you first enter the Configure Managed Servers screen, you will see entries for components already configured such as Identity Manager. In addition you will create 2 new managed servers for OPAM

Notes:

- » When you first enter this screen the config wizard has created a default Managed Server for you (opam_server1)
- » Change the details of the default Managed Server to reflect the following details and add a new managed server. That is, change one entry and add one new entry.
- » Do not change the configuration of any Managed Servers which have already been configured as part of previous application deployments.
- » You MUST use the names listed in the table below.
- » Leave all other fields at the default settings

Default Name	Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
opam_server	wls_opam1	OIMHOST1	18101	18102	Yes
	wls_opam2	OIMHOST2	18101	18102	Yes

Click **Next**

9. On the Configure Clusters screen, create a cluster by clicking Add and provide the values shown for opam_cluster in the following table.

Name	Cluster Messaging mode	Multi Cast address	Multi Cast port	Cluster Address
Opam_cluster	unicast	n/a	n/a	n/a

Leave all other fields at the default settings.

Click **Next**.

10. On the Assign Servers to Clusters screen, associate the Managed Servers with the cluster. Click the cluster name in the right pane. Click the Managed Server under Servers, then click the arrow to assign it to the cluster

Assign servers to the clusters as follows:

CLUSTER	SERVICES
opam_server	wls_opam1
	wls_opam2

Note:

Do not change the configuration of any clusters which have already been configured as part of previous application deployments.

Click **Next**.

11. On the Configure Machines screen, click **Next**.
12. On the Assign Servers to Machines screen, assign servers to machines as follows:

OIMHOST1: wls_opam1

OIMHOST2: wls_opam2,

Click **Next** to continue.

13. On the Configuration Summary screen, click Extend to extend the domain.

Notes:

- » Deployment will have created Machines for you
- » If you receive a warning that says:
CFGFWK: Server listen ports in your domain configuration

conflict with ports in use by active processes on this host

Click **OK**.

This warning appears if Managed Servers have been defined as part of previous installs and can safely be ignored.

Restarting Administration Server on OIMHOST1

Restart WebLogic Administration Server on OIMHOST 1.

Deploying Managed Server Configuration to Local Storage

Once the configuration is complete, you must propagate the configuration to the managed server directory on OIMHOST1 and OIMHOST2.

You do this by packing and unpacking the domain, you pack the domain first on IAMGovernanceDomain on OIMHOST1 then unpack it on OIMHOST1 and OIMHOST2.

Follow these steps to propagate the domain to the managed server domain directory. 1. Invoke the pack utility from `ORACLE_COMMON_HOME/common/bin/` on OIMHOST1.

```
./pack.sh -domain=IGD_ASERVER_HOME -template=iam_domain.jar -  
template_name="IAM Domain" -managed=true
```

This creates a file called `iam_domain.jar`. Copy this file to OIMHOST2.

On OIMHOST1 and OIMHOST2, invoke the utility `unpack`, which is also located in the directory: `ORACLE_COMMON_HOME/common/bin/`

```
./unpack.sh -domain=IGD_MSERVER_HOME -template=iam_domain.jar -  
overwrite_domain=true -app_dir=IGD_MSERVER_HOME/applications
```

If you see a message similar to this, you may safely ignore it:

>> Server listen ports in your domain configuration conflict with ports in use by active processes on this host.

Configure Managed Servers for Node Manager SSL

In the standard Enterprise Deployment Node Manager has been configured to communicate with the managed servers using SSL. Now that there are two new managed servers for OPAM these also need to be SSL enabled. The automation tool will already have created the keystores so only the managed servers need to be updated. To do these perform the following steps:

1. login to the WebLogic console using the URL <http://igdadmin.us.oracle.com/console> using the weblogic_idm user.
2. Click Lock and Edit.
3. Navigate to Environment – Servers, the WebLogic server Summary page is displayed.
4. Click on one of the newly created OPAM servers for example wls_opam1.
5. Select Configuration then keystores
6. Click **change** next to the keystores field then select the **Custom Identity and Custom Trust** method for storing and managing private keys/digital certificate pairs and trusted CA stores. Then click **Save**.
7. In the Identity section, define attributes for the identity keystore:
 - **Custom Identity Keystore:** The fully qualified path to the identity keystore: `SHARED_CONFIG_DIR/keystores/appIdentityKeyStore.jks`
 - **Custom Identity Keystore Type:** Leave blank; it defaults to JKS.
 - **Custom Identity Keystore Passphrase/Confirmation:** The keystore password. This will be the `COMMON_IAM_PASSWORD` provided as part of the provisioning process.
8. In the Trust section, define properties for the trust keystore:
 - **Custom Trust Keystore:** The fully qualified path to the trust keystore: `SHARED_CONFIG_DIR/keystores/appTrustKeyStore-oimhost1.example.com.jks`
Note: the host name oimhost1 will be the value applicable to your environment.
 - **Custom Trust Keystore Type:** Leave blank; it defaults to JKS.
 - **Custom Trust Keystore Passphrase:** The keystore password. This will be the `COMMON_IAM_PASSWORD` provided as part of the provisioning process.
9. Click **Save**.
10. Select Configuration, then SSL.
11. In the **Private Key Alias** field, enter the alias you used for the host name the Managed Server listens on, for example:
 - For WLS_OPAM1, use `appIdentity-oimhost1.example.com`.
 - For WLS_OPAM2, use `appIdentity-oimhost2.example.com`.Substitute the host and domain you are using for your implementation.
12. In the **Private Key Passphrase** and the **Confirm Private Key Passphrase** fields, enter the `COMMON_IAM_PASSWORD` provided as part of the provisioning process.
13. Click **Save**.
14. Expand the **Advanced** section of the page.
15. Set host name verification to **BEA Hostname Verifier**.
16. Click **Save**.
17. Click **Activate Changes** in the Administration Console's Change Center to make the changes take effect.
Note: If you are using a test certificate and the host in the certificate does not match the site name then in set 15 set host name verification to none.

Configure OPAM

Before starting the OPAM managed servers, some initial OPAM configuration is required. This is simply a matter of running the script `opam-config.sh` which is located in the directory `IAM_ORACLE_HOME/opam/bin`

To run this command perform the following commands:

set `ORACLE_HOME` to `IAM_ORACLE_HOME`

set `ANT_HOME` to `IGD_MW_HOME/modules/org.apache.ant_1.7.1`

set `JAVA_HOME` to `JAVA_HOME`

set `ANT_OPTS` to `'-Xmx512M -XX:MaxPermSize=512m'`

```
cd IAM_ORACLE_HOME/opam/bin
./opam-config.sh
```

When prompted enter the following values:

Oracle WebLogic Administration User Name: `weblogic`

Oracle WebLogic Administration Password: `IAM_COMMON_PASSWORD`

Oracle WebLogic Administration Server URL: `t3://igdadminvhn.example.com:7101`

Oracle WebLogic Domain Name: `IAMGovernanceDomain`

Oracle Middleware Home: `IGD_MW_HOME`

Restart the WebLogic Administration Server.

Disable SSL

By default Oracle Privileged account manager communicates with the web server using SSL. In an enterprise deployment SSL is off loaded to the load balancer so the Oracle HTTP Server needs to communicate with the OPAM Managed Servers using non SSL (http). Traffic between the load balancer and the client will still be SSL enabled as that is taken care of by the load balancer.

Perform the following steps to disable OPAM SSL

1. Create a directory on the shared storage called `opam` for example:

```
mkdir SHARED_CONFIG_DIR/opam
```

2. Create a file called `plan.xml` in this directory with the following contents:


```

<?xml version='1.0' encoding='UTF-8'?>
<deployment-plan xmlns="http://xmlns.oracle.com/weblogic/deployment-plan"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.oracle.com/weblogic/deployment-plan
  http://xmlns.oracle.com/weblogic/deployment-plan/1.0/deployment-plan.xsd" global-
  variables="false">
  <application-name>opam</application-name>
  <variable-definition>
    <variable>
      <name>TransportGuarantee_type</name>
      <value>NONE</value>
    </variable>
  </variable-definition>

  <module-override>
    <module-name>opam.war</module-name>
    <module-type>war</module-type>
    <module-descriptor external="false">
      <root-element>web-app</root-element>
      <uri>WEB-INF/web.xml</uri>
      <variable-assignment>
        <name>TransportGuarantee_type</name>
        <xpath>/web-app/security-constraint/user-data-constraint/transport-guarantee</xpath>
      </variable-assignment>
    </module-descriptor>
  </module-override>

  <config-root>/u01/oracle/config/opam</config-root>
</deployment-plan>

```

Save the file.

3. Login to the IAMGovernanceDomain Weblogic console using the url:
<http://igdadmin.us.oracle.com/console>
4. Click on **Deployments** in the Domain Structure Menu. A list of deployments is displayed.
5. Select OPAM (*version*) from the list of deployments – Do not click on it tick the check box next to it.
6. Click Lock & Edit
7. Click on **Update**
8. Click **Change Path** next to Deployment Plan Path.
9. Set the path to be the deployment file created above. For example
 SHARED_CONFIG_DIR/opam/plan.xml
10. Click **Next**
11. Select Redeploy this application using the following deployment files
12. Click **Next**
13. Click **Finish**
14. Click Activate Changes.
15. Restart the Administration Server and any running OPAM managed servers.

Add Load Balancer Certificate to Trust Stores

Oracle Privileged account Manager requires that the SSL certificate used by the load balancer be added to the trusted certificates in the JDK used by OPAM. To do these perform the following steps.

Obtain Certificate from the Load Balancer



The easiest way to obtain the certificate is to save it from an internet browser. The following instructions relate to using Firefox.

To retrieve the Oracle Privileged Account Manager server's CA certificate:

From your browser, connect to the Oracle Privileged Account Manager server web service:

<https://sso.example.com>

For example, from a Firefox browser

1. Click the lock icon in the browser's address bar.
2. When the information dialog displays, click **More information**.
3. On the Page Info dialog, click **View certificate**.
4. On the Certificate Viewer dialog, select the Details tab to view the Certificate Hierarchy.
5. Select the first (root) certificate in the Certificate Hierarchy list, and then click **Export**.
6. When the Save Certificate to File dialog displays, navigate to the directory where you want to save the file. For example, `/tmp/opam.pem`.
7. Select **X.509 Certificate (PEM)** from the Save as type menu, enter `sso.pem` as the file name, and click **Save**.
8. Alternatively if this is the first time you have accessed the website using the browser you can use the following steps:
9. When cert exception is shown click **add exception**
10. Click on get certificate
11. Click confirm security exception
12. Navigate to Firefox preferences - advanced - encryption - view certificates
13. Click servers
14. Find certificate just added for example MyCompany - sso.example.com
15. Click on the certificate
16. Click **Export**
17. Choose a name (`sso.pem`) and where to export the certificate.
18. Copy the certificate to `oimhost1`

Load the Certificate into the JDK and Node Manager Trust Stores

Run the following command to import the CA certificate file, `sso.pem`, into the following truststores:

`IGD_MW_HOME` Java Trust Store

Node Manager Trust Stores.

To do this on the server where you are running Oracle Identity Manager execute the following commands:

set `JAVA_HOME` to `IGD_MW_HOME/jdk6`

set `PATH` to include `JAVA_HOME/bin`

```
keytool -importcert -file Path_to_cert/sso.pem -trustcacerts -keystore
$JAVA_HOME/jre/lib/security/cacerts

keytool -importcert -file Path_to_cert/sso.pem -trustcacerts -keystore
SHARED_CONFIG_DIR/keystores/appTrustKeyStore-oimhost1vhn.example.com.jks

keytool -importcert -file Path_to_cert/sso.pem -trustcacerts -keystore
SHARED_CONFIG_DIR/keystores/appTrustKeyStore-oimhost2vhn.example.com.jks

keytool -importcert -file Path_to_cert/sso.pem -trustcacerts -keystore
SHARED_CONFIG_DIR/keystores/appTrustKeyStore-oimhost1.example.com.jks

keytool -importcert -file Path_to_cert/sso.pem -trustcacerts -keystore
SHARED_CONFIG_DIR/keystores/appTrustKeyStore-oimhost2.example.com.jks
```

Where JAVA_HOME is set to *IGD_MW_HOME/jdk6*

You will be prompted to enter a password for the keystore, the default password for the JDK changeit and the *COMMON_IAM_PASSWORD* for the node manager keystores. You will also be asked to confirm that the certificate is valid.

Note: oimhost1vhn and oimhost2vhn will be the names of the virtual hosts you assigned to your OIM server. oimhost1 and oimhost2 will be the names of the hosts your OPAM servers are running on.

Adding OPAM Servers to Start and Stop Scripts

Deployment creates a set of scripts to start and stop managed servers defined in the domain. Whenever you create a new managed server in the domain you must update the domain

configuration so that these start and stop scripts can also start the newly created managed server. You must now do this for each of the OPAM managed servers.

To update the domain configuration, edit the file *serverInstancesCustom.txt*, which is located in the directory: *SHARED_CONFIG_DIR/scripts*

For example:

```
OIMHOST1 OAAM wls_opam1 IGDADMINVHN 7101
OIMHOST2 OAAM wls_opam2 IGDADMINVHN 7101
```

Note: There is not type of OPAM but server type of OAAM can be used instead.

Save the file.

Starting and Validating OPAM

Starting OPAM on OIMHOST1


Start the OPAM Managed servers by logging into the IAMGovernanceDomain Administration server using the URL

<http://igdadmin.example.com/console>

Select Servers - Control.

Select the servers *wls_opam_admin1* and click **Start**.

Validating OIMHOST1



Validate the implementation by connecting to the OPAM Administration console at:

<http://OIMHOST1.example.com:18101/oinav/opam>

and to the OPAM server at:

<http://OIMHOST1.example.com:18101/opam>

Note you have to fire a browser up inside an exalogic machine to see these as you are accessing the internal network.

The implementation is valid if the OPAM Server login page is displayed and you can log in using the opamadmin account you created in [Creating OPAM Users and Groups in LDAP](#)

Starting OPAM on OIMHOST2

Start Oracle Privileged Account Manager on OIMHOST2 by following the start procedures in [Starting and Stopping Components for WebLogic Managed Servers wls_opam2](#)

Validating OIMHOST2

Validate the implementation by connecting to the OPAM Administration Console at <http://OIMHOST2.example.com:18101/oinav/opam>

The implementation is valid if OPAM Administration console login page is displayed and you can login using the opamadmin account you created in

Validate the implementation by connecting to the OPAM Server at: <http://OIMHOST2.example.com:18101/opam> The implementation is valid if the OPAM Server login page is displayed.

Configuring OPAM to Work with Web Tier

This section describes how to configure Oracle Adaptive Access Manager to work with the Oracle Web Tier be it Oracle Traffic Director or Oracle HTTP Server.

Configuring Access from Oracle Traffic Director

You must create a server pool in Oracle traffic director and modify the routes created for each of the virtual hosts.

Create an OTD server Pool for OPAM

1. Log in to the Administration Console using the following URL:
<https://OTDADMINVHN:8989>
2. Click the **Configurations** button that is situated at the upper left corner of the page.
A list of the available configurations is displayed.
3. Select the configuration for which you want to create a server pool.
4. In the Common Tasks pane, click **New Server Pool**.
5. The New Origin-Server Pool wizard starts.

Enter the following information in the Server Pool Information screen:

Name: Name of the server pool. For example, opam-pool

Origin Server Type: The type of requests the pool handles. For example, HTTP.

Click **Next**.

6. Enter the following information in the Origin Server Information screen:

Origin Server Host: OIMMHOST1.example.com

Port: 18101

Click **Add Server**.

7. Enter the information for any other servers. For example:

Origin Server Host: OIMHOST2.example.com

Port: 18101

Click **Next**

Create OTD Routes

The following OTD Routes need to be created.

VIRTUAL HOST	ROUTE	ORIGIN SERVER POOL	CONDITIONS
lgdadmin.example.com	Opam-admin-route	Opam-pool	\$uri =~ '/oinav'
sso.example.com	Opam-route	Opam-pool	\$uri =~ '/opam'

For the route opam-route Enable SSO Passthrough as described in Enabling SSO PassThorough for [sso.example.com](#)

Deploying a Configuration Using the Administration Console

To deploy a configuration by using the administration console, do the following:

1. Log in to the administration console using the following URL:
`https://OTDADMINVHN:8989`
2. Click the Configurations button at the upper left corner of the page.
A list of the available configurations is displayed.
Select the IAM configuration.
Click **Deploy**.
A message is displayed confirming that the updated configuration was successfully deployed.
3. Click **Close**.

Configuring Access from Oracle HTTP Server

You must include OPAM in the Oracle HTTP configuration by updating the following files on WEBHOST1 and WEBHOST2

Updating IGDADMIN.example.com

Add the following to *OHS_ORACLE_INSTANCE*/config/OHS/component_name/moduleconf/ igdadmin_vh.conf:

```
## Entries Required by Oracle Privileged Manager
#####
# OPAM Console
<Location /oinav>
    SetHandler weblogic-handler
    WebLogicCluster OIMHOST1.example.com:18101,OIMHOST2.example.com:18101
</Location>
```

Updating prov.example.com

Add the following to *OHS_ORACLE_INSTANCE*/config/OHS/component_name/moduleconf/ prov_vh.conf:

```
#####
## Entries Required by Oracle Privileged Acct Manager
#####

<Location /opam>
    SetHandler weblogic-handler
    WebLogicCluster OIMHOST1.example.com:18101,OIMHOST2.example.com:18101
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>
```

Restarting Oracle HTTP Servers and OPAM Managed Servers

Restart the Oracle HTTP Server on WEBHOST1 and WEBHOST2.

Restart the managed servers wls_opam1, wls_opam2.

Validating the Web Tier

To validate that the web tier is has been setup correctly. Try accessing OPAM using the following URL's


<https://prov.example.com/opam> - You will be asked to enter the user name and password of an OPAM user. Use the opamadmin user you created in Creating OPAM users and Groups in LDAP.

<http://igdadmin.example.com/oinav/opam> - When the OAM login page appears login using the opamadmin user created above.

Create OAM Policy for OPAM

You need to create a policy in OAM to ensure that webgate does not intercept requests to the OPAM url. To do this perform the following:

1. Login to the OAM console using the url:
<http://iadadmin.example.com/oamconsole>
2. Click on Application Domains.
3. Click Search.
4. Click IAM Suite.
5. Click the **Resources** Tab



6. Click **New Resource** and provide the following information:

- Type: http
- Description: Opam
- Host Identifier: IAMSuiteAgent
- Protection Level: Excluded
- Authentication Policy: n/a
- Authorization Policy: n/a

7. Click Apply

Configuring OPAM Console to use the OPAM Cluster

1. Login to the OPAM console using the url:

<http://igdadmin.example.com/oinav/opam>

2. When the OAM login page appears login using the opamadmin user created above.

3. Click on Server Configuration

4. Enter the following information:

Host: prov.example.com

SSL Port: 389

Click **Test**.

If the test is successful then click **Apply**. If not then check the log files for the managed server wls_opamx, determine the issue and resolve it.

5. Click on Session Manager Configuration

In the Oracle Privileged Account Manager URL's click **Ad**

In the OPAM Server URL enter

<https://prov.example.com/opam>

Remove any other URLs such as the default url which points to one of the managed servers.

Click **Apply**

6. Restart the Managed Servers wls_opam1 and wls_opam2

Configuring OPAM to Manage a Target

For full details on configuring OPAM to manage systems refer to the OPAM Administrators Guide. The instructions below are included to ensure that OPAM is configured and working correctly.

The instructions involve configuring a UNIX host.

Create a Service Account on the Host Operating System

OPAM needs an account set up on the target system which is not used by normal users. This is the account that OPAM will use to perform operations on the target system for example, Searching and viewing details about accounts on the system and locating accounts during checkout. It will also be used to change account passwords on the target etc.



To create an account on the target system called `opam_service` issue the following command whilst logged in as root.

```
useradd -d /home/opam_service -m -g root -G bin,daemon,sys,adm,disk,wheel -o -u 0 opam_service
```

Set a password for the account using the command:

```
passwd opam_service
```

Add Host as a Target to OPAM

Now that the account has been created it must be added as a target to OPAM. To do this perform the following steps:

1. Login to the OPAM console using the url <http://igdadmin.us.oracle.com/oinav/opam> as the `opamadmin` account.
2. Click on **Targets**
3. Click **Add** and Enter the following information

Target Type: `unix`

Target Name: A name identifying the target for Example `idmhost1`

Description - A description of the target

Domain - The domain that the target server resides in for Example example.com

Password Policy - Leave at Default Password Policy

Host - The host name of the target server for example oimhost1.example.com

Port - Enter the SSH port to use for example `22`

Login User - Enter the service user name on the host for example `opam_service`

Login Password - Enter the password of the service account

4. Click **Test** to test the connection.

If the test succeeds click **Save**

Assign Privileged Accounts to OPAM to Manage

For the purpose of validation we will create a dummy account on the target system for OPAM to manage. This account will be called `opam_test`


On the Unix host create the account `opam_test` by issuing the following command as root

```
useradd opam_test
```

Assign a password to the account by using the command

```
passwd opam_test
```

1. Login to the OPAM console using the url <http://igdadmin.example.com/oinav/opam> as the `opamadmin` account.
 2. Click on **Accounts**
 3. Click **Add**
 4. Click the magnifying glass next to Target Name and the Search Window is displayed
 5. Click **Search** the search window is displayed
-

- 
6. Enter % in the Target Name and click **Search**. The search results window is displayed.
 7. Select the target oimhost1.example.com and Click **Set**
 8. In the Account Name field enter opam_test and an appropriate description
 9. Click **Test**
 10. If the test is successful then Click **OK** and then Click **Save**.

Grant a User Access to the Account

- » Click on **Accounts**
- » Click **Search** the newly assigned account opam_test should appear
- » Click on this account the account window appears
- » Click on **Grants**
- » Click **Add** - The add users dialogue appears.
- » Enter the username opamadmin and click **search**
- » Click on the returned opamadmin account and click **add**
- » Click **Close** to close the search window.
- » Click **Apply**.

Validating OPAM

Now that you have an account that OPAM can manage you can check that OPAM is working correctly by checking out the account and then logging into the target machine. To do this perform the following steps:


- » Login to the OPAM console using the url <http://igdadmin.example.com/oinav/opam> as the opamadmin account.
- » Click **My Accounts**
- » Click on **search**
- » The account opam_test is returned.
- » Click on the account and then click **Password Check Out**
- » Enter a justification and click **check out**.
- » The account will then be checked out and the password made available - to see it click **Show password**.
- » Login in to the target machine for example oimhost1 using the account opam_test and the password obtained in step 7.
- » When you have finished, click on **My Checkouts**.
- » Click on the account opam_test and click **Check In**
- » When the confirmation window is displayed, click **Check In**

Integrating OPAM with Oracle Identity Manager

Now that you are satisfied that OPAM is working you can integrate it with Oracle Identity Manager.

To do this you must perform the following steps:

Install Generic LDAP Connector



Although Oracle Identity Manager is already linked to your OUD directory you need to configure the Generic LDAP connector to access the same directory. This is to allow OPAM to appear in the OIM catalog.

To install the Generic LDAP connector you need to perform the following steps:

Obtain the latest Oracle Internet Directory connector from

<http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html>

Do not worry if the version number is different to 11.1.2.2 and do not worry that it says Oracle Internet Directory this is a generic LDAP connector.

Unzip the file *oid-version.zip* to the directory *IGD_ORACLE_HOME/server/ConnectorDefaultDirectory*

» Login to the Oracle Identity Manager System administration console using the URL:

<http://igdadmin.us.oracle.com/sysadmin>

login using the user *xelsysadm*

- » Click **Manage Connector** under System Management. The Manage connector screen is shown.
- » Click **Install**
- » Select ODSEE/OUD/LDAPV3 Connector *version* from the Connector List and click **Load**.
- » Click Continue to Install the connector, this may take some time (if the screen goes blank be patient).
- » When the Connector is installed a summary page will be displayed showing success. Click **Exit**.

Configure IT Resource

When the connector was installed it created and IT resource called DSEE Server. This IT resource needs to be updated with the connection details of the OUD server. To do this perform the following steps:

» Login to the Oracle Identity Manager System administration console using the URL:

<http://igdadmin.us.oracle.com/sysadmin>

login using the user *xelsysadm*

- » Click on **IT Resource** under Provisioning Configuration - The search results window is displays
- » Enter DSEE Server in the IT Resource Name and click **Search**
- » DSEE Server is returned in the search results window click **Edit**
- » Enter the following information:

Configuration Lookup: Lookup.LDAP.OUD.Configuration

Connector Server Name: Leave blank

baseContexts: "dc=example,dc=com"

Principal:cn=oimLDAP,cn=systemids,dc=example,dc=com

Credentials: Password of the above account. This will be the *COMMON_IAM_PASSWORD*

Host: idstore.example.com

Port: Port that the Load Balancer is listening on *LDAP_LBR_PORT* for example 1389



ssl: false

- » Click **Update**
- » Close the window.

Create an Identity Management Sandbox

Before you can add entries to the Identity Manager Catalogue you need to place Oracle Identity Manager into Sandbox mode. To do this perform the following steps:

- » Login to the Oracle Identity Manager System administration console using the URL:

<http://igdadmin.example.com/sysadmin>

login using the user xelsysadm

- » Click on **Sandbox** in the top right corner of the screen
- » Click **Create Sandbox**
- » Enter the following information:
 - Sandbox Name: OPAM
 - Sandbox Description: OPAM
 - Select Activate Sandbox
 - Click **save and close**
- » Click **OK** when the confirmation message is displayed

Create a UI form for the new IT Resource

- » Login to the Oracle Identity Manager System administration console using the URL:

<http://igdadmin.example.com/sysadmin>

login using the user xelsysadm


- » Click on **Form Designer** under Provisioning Configuration, the search results window is displayed.
- » Click **Create** and enter the following information:
 - Resource Type: LDAP User
 - Form Name: OUDUser
 - Leave everything else at the default and click **Create**.

Create an Application for OPAM in OIM

- » Login to the Oracle Identity Manager System administration console using the URL:

<http://igdadmin.example.com/sysadmin>

login using the user xelsysadm



» Click **Application Instances** Under Provisioning Configuration, the search window is displayed.

» Click **Create**, the Create Application Instance window is displayed, Enter the following Information:

Name: OPAM

Display Name : Oracle Privileged Account Manager

Description: Oracle Privileged Account Manager

Resource Object: LDAP User

IT Resource Instance: DSEE Server

Form: OUDUser

Click **Save**

Publish Sandbox

To publish the new provisioning form and Application instance, perform the following steps:

» Login to the Oracle Identity Manager System administration console using the URL:

<http://igdadmin.example.com/sysadmin>

login using the user xelsysadm

» Click on **Sandbox** in the top right corner of the screen

» Click the Sandbox **OPAM**

» Click Publish Sandbox

» Click **Yes** when asked to confirm

Integrate OPAM with OIM using opamSetup.sh

Now that you have created an IT Resource and Application you can associate OPAM with OIM. To do this you run the script `opamSetup.sh` which is located in the directory `IGD_ORACLE_HOME/server/bin` directory on `iamhost1`.

Before running the command set the following environment variables:

set APP_SERVER to `weblogic`

set OIM_ORACLE_HOME to `IGD_ORACLE_HOME`

set JAVA_HOME to `JAVA_HOME`


set MW_HOME to `IGD_MW_HOME`

set WL_HOME to `IGD_MW_HOME/wlserver_10.3`

set DOMAIN_HOME to `IGD_ASERVER_HOME`

The command is:

```
opamSetup.sh
```



When prompted Enter the following information

- » OIM URL : The t3 URL address of one of the OIM Managed Servers for example: t3://oimhost1vhn1.example.com:14000
- » OIM username : An Oracle Identity Manager log-in user name for example xelsysadm
- » OIM User Password : The Password of the account OIM username
- » OPAM IT resource name : The Oracle Privileged Account Manager IT resource name, this is the name of the resource that will be created for OPAM.
- » OPAM server name : The name of the OPAM server for example sso.example.com
- » OPAM server port : The Oracle Privileged Account Manager server port for example 443.
- » OPAM user : The Oracle Privileged Account Manager log-in user name for Example opamadmin
- » OPAM user password : The Oracle Privileged Account Manager log-in password.
- » ID Store IT resource name : is the name of the IT resource of the identity store, for example DSEE Server
- » Context : This should be weblogic.jndi.WLInitialContextFactory

When the command completes you should see Success Messages.

The opamSetup script performs the following tasks:

- » Creates the Oracle Privileged Account Manager IT resource with the opamServer, opamPort, opamUser, and opamPassword set-up script parameters.
- » Creates a UDF column named OPAM_TAGS in the Oracle Identity Manager catalog.
- » Creates an Oracle Privileged Account Manager synchronization scheduled job with the following characteristics:
 - » Name: Oracle Privileged Account Manager Catalog Synchronization Job. If a job with this name already exists, the job appends a -1 to the name, then a -2, and so on.
 - » Schedule type: Periodic, runs every 15 minutes.
 - » OPAMServerIdStoreItResource: The idStoreItResource parameter of the set-up script.
 - » OpamServerItResource: The opamItResource parameter of the set-up script.
- » Creates the OIM.OPAM.Integration system property (if it does not yet exist) and sets it to true.

If any of these tasks fail, the script automatically executes the next task.

Creating the OPAM_TAGS UDF

After setting up the Oracle Privileged Account Manager-Oracle Identity Manager integration environment, you must manually create an OPAM_TAGS and OPAM_CERT_TAGS user-defined fields (UDF) in the Oracle Identity Manager catalog. The OPAM_TAGS and OPAM_CERT_TAGS UDF enables Oracle Privileged Account Manager to search the Oracle Identity Manager catalog.


To manually create the OPAM_TAGS and OPAM_CERT_TAGS UDF, perform the following steps:

Create an Identity Management Sandbox

Before you can add entries to the Identity Manager Catalogue you need to place Oracle Identity Manager into Sandbox mode. To do this perform the following steps:

- » Login to the Oracle Identity Manager System administration console using the URL:

<http://igdadmin.example.com/sysadmin>



login using the user xelsysadm

- » Click on **Sandbox** in the top right corner of the screen
- » Click Create Sandbox
- » Enter the following information:

Sandbox Name: OPAM_TAG

Sandbox Description: OPAM TAG

- » Click save and close
- » Click **OK** when the confirmation message is displayed
- » On the toolbar Click **Activate Sandbox**.

Create a Custom Field

- » Login to the Oracle Identity Manager System administration console using the URL:

<http://igdadmin.example.com/sysadmin>

login using the user xelsysadm

- » In the left pane, under **System Entities**, click **Catalog** to open the manage Catalog page.
- » Click the Create a custom field icon.
- » When the Select Field Type dialog box displays, select the **Text** field type to create a text field. Click **OK**.
- » When the page to create a custom field displays, enter the following information:

Appearance section:

Display Label : OPAM tags

Display Width: 256

Name section:

Name: OPAM_TAGS

Description: OPAM metadata tags

Constraints section:


Searchable: Select

Leave everything else at the defaults

- » Click **Save and Close**, then verify that the user defined field appears in the custom fields table.
- » To create the OPAM_CERT_TAGS UDF, repeat the above "procedure with the following changes:
 - » Replace 'OPAM_TAGS' with "OPAM CERT TAGS" as the value of the **Display Label** field in the **Appearance section**
 - » Replace "OPAM_TAGS" with "OPAM_CERT_TAGS" as the value of the **Name** field in the **Name section**.

Publish Sandbox

Before you can add entries to the Identity Manager Catalogue you need to place Oracle Identity Manager into Sandbox mode. To do this perform the following steps:

- 
- » Login to the Oracle Identity Manager System administration console using the URL:

<http://igdadmin.example.com/sysadmin>

login using the user xelsysadm

- » Click on **Sandbox** in the top right corner of the screen
- » Click the Sandbox OPAM_TAG

- » Click Publish Sandbox
- » Click **Yes** when asked to confirm

Tagging Catalog Entries with OPAM Metadata

The Oracle Privileged Account Manager Catalog Synchronization Job created by the `opamSetup` script tags the catalog entries with the Oracle Privileged Account Manager metadata. This job automatically runs every 15 minutes.

If you need to run the job immediately, instead of waiting for the next cycle to begin, you can manually perform the following steps from the Oracle Identity Manager Admin Console:

- » Login to the Oracle Identity Manager System administration console using the URL:

<http://igdadmin.example.com/sysadmin>

login using the user xelsysadm





- » Click Scheduler under System Configuration.
- » When the Search Scheduled jobs screen displays, Enter LDAP Connector Group Lookup Reconciliation into the search field and click **Search**.
- » Click on the Job in the Search Results window
- » Click **Run Now**.
- » After the job finishes, click **Refresh**.
- » Verify that the job ran successfully, check the **Job History** view.
- » Repeat steps 1-7 for the Job **OPAM Catalog Synchronization**.



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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

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

Integrated Cloud Applications & Platform Services

Copyright © 2015, 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.

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. 0615

White Paper Extending Identity and Access Management Enterprise Deployment with Oracle Privileged Account Manager
July 2016
Author: Michael Rhys
Contributing Authors: Firdaus Fraz



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