Oracle® Retail High Availability Case Study - Fusion Middleware Cluster Installation for Retail Applications

Release 15.0
2151366.1

August 2016

ORACLE
RETAIL

ORACLE

Note: 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.

Contents

1 Installation Overview 1

Single Sign-On Process Overview 1

What Do I Need for Single Sign-On? 2

Can Oracle Access Manager Work with Other SSO Implementations? 2

What Single Sign-On is not? 2

How Oracle Single Sign-On Works 2

About SSO Login Processing with OAM Agents 2

Installation Overview 4

Infrastructure Installation and Configuration 5

OID User Data 5

User Management 5

ODSM 5

LDIF Scripts 5

User Data Synchronization 5

2 Understanding Installation Directories 7

3 Configuring the Load Balancer 8

4 Installing Oracle Web Tier 9

Configuring Web Tier on idmhost1 and idmhost2 14

Verification – Web Tier Installation and Virtual Host Alias 21

5 Installing OAM Webgate 23

Configuring OAM WebGate 26

6 Installing Oracle Internet Directory 29

Install WebLogic Server 10.3.6 on idmhost1 and idmhost2 29

Install Oracle Internet Directory on idmhost1 and idmhost2 34

Backing up Installations 39

7 Configuring the Oracle Internet Directory in a Cluster 41

Configuring IDM on idmhost1 41

Additional Information on RAC: 46

Create WebLogic boot.properties for OID WLS Domain on idmhost1 49

Update IDMDomain Listen Address on idmhost1 49

Configuring IDM on idmhost2 51

Node Manager Configuration for OID on idmhost1 and idmhost2 59

Verification – OID on idmhost2 is Registered with Enterprise Manager 59

Verification – Installation of ODSM 60

9 Seed OID with Retail Specific Entries 63

10 Installing Oracle Access Manager 1

Install WebLogic Server 10.3.6 on idmhost1 and idmhost2 1

Install Oracle Access Manager Software on idmhost1 and idmhost2 5

Creating Database Repository for Oracle Access Manager (OAM) 9

11 Configuring Oracle Access Manager in Cluster 17

Configuring OAM on idmhost1 17

Node Manager Configuration for OAM on idmhost1 and idmhost2 29

Start AdminServer for OAM_WEBLOGIC_HOME on idmhost1 29

Create WebLogic boot.properties for OAM WLS Domain on idmhost1 31

Removing IAMSuite Agent in OAM 31

Configure OID and OAM Identity Asserter Providers For OAM 33

Propagating OAMDomain to idmhost2 42

Start OAMDomain - Admin and Managed Servers 43

Creating Administrators Group in OID for OAM Identity Store 46

Create a WebLogic Admin User in OID 50

Add orcladmin and WebLogic Admin Users to the Administrators Group 52

Launching OAMConsole and Configuring Identity Store 53

Set Identity Store as the Default Store and the Default System Store 57

Configure OAM to use VIP URL and OHS Port 62

Set Protection Level for Resource URL's in OAM 65

14 Registering a New WebGate Agent 79

15 Installing and Configuring OBIEE 11.1.1.9 87

Create RCU Schemas for OBIEE 87

Install OBIEE Software on idmhost1 and idmhost2 93

Create WebLogic boot.properties for OBIEE WLS Domain on idmhost1 109

Configure OID Provider in Oracle BI EE WebLogic Domain 110

Create the OAM SSO provider in the Oracle BI EE Domain 119

Configure BI Publisher for Application Reports 124

Verification – Validate BI Publisher Reports Non-SSO configuration 139

16 Configuring the Oracle BI EE Environment for Operational Insights 143

Configure Oracle Retail Operational Insights Roles and Application Roles 143

Configure RPD for Operational Insights 144

Migrate RPD and Catalog for Operational Insights 150

Troubleshooting 157

Refresh User GUIDs 157

Post install Configuration for OBIEE Display 164

Prepare the Operational Insights Environment for Oracle BIEE Presentation Services Connection 173

Single Sign-On Configuration for Oracle BI EE 179

Configure Alias for Static Resources in Web Tier for OBIEE 180

Update Oracle Web Tier for OBIEE and OAM Redirects 181

Make the Static Resources Publicly Available 182

Enable Caching and Compression of the Oracle BI EE Static Resources 183

Verification – Verify the Static Resources using the Oracle Web 185

Configure for In-Context launches of RMS forms 187

Verification – Validate BI Publisher Reports SSO Configuration 188
Verification – Verify OBIEE analytics is Accessible via Web Tier using Application Specific Credentials.....190
Verification – Verify OAMConsole is Accessible via Web Tier using SSO Login 192

A Appendix: Creating Static Ports for OID 195

B Appendix: A Summary of Installing the Oracle Internet Directory (idmhost1) . 197

C Appendix: A Summary of Installing the Oracle Internet Directory (idmhost2) . 199

D Appendix: Setting Node Manager for IDM_WEBLOGIC_HOME..... 201

E Appendix: Setting Nodemanager for OAM_WEBLOGIC_HOME..... 203

F Appendix: Creating Staticports for OBIEE Configuration..... 205

G Appendix: Creating Staticports for OBIEE Configuration..... 207

H Appendix VII – LDIF Files..... 209

1

Installation Overview

There are many options to configure an Oracle High Availability environment, and these options can have a significant impact on how the environment is configured and built. The intent of this case study is not to provide exhaustive documentation on all possible ways to configure a suitable High Availability environment for Oracle Retail, but rather to document a specific configuration that was used for verification purposes. Because of this, the specific installation steps documented in this case study only apply in their entirety to the exact hardware and software configuration described in this case study.

This case study details the steps needed to create a Single Sign-On environment on a WebLogic Server using Oracle Access Manager the following steps are performed to install the infrastructure to Oracle Retail installation.

- Install Web Tier
- Install OAM WebGate
- Create Database Repository for Oracle Internet Directory (OID) and Oracle Access Manager (OAM)
- Install, Configure, and Seed OID
- Install and Configure OAM
- Connect to Web Tier to WebLogic application domain
- Install and configure OBIEE for BI Publisher and Analytics for Operational Insights for SSO
- Register Application Web Tier and Forms Web Tier with OAM
- Configure Web Tier for SSO
- Configure Forms for SSO
- Install and configure RIB application on active/passive server
- Install and configure RSB and other RTG applications in cluster

Single Sign-On Process Overview

Single Sign-On (SSO) is a term for the ability to sign onto multiple web applications via a single user ID/password. There are many implementations of SSO. Oracle provides an implementation with Oracle Access Manager.

Most, if not all, SSO technologies use a session cookie to hold encrypted data passed to each application. The SSO infrastructure has the responsibility to validate these cookies and, possibly, update this information. The user is directed to log on only if the cookie is not present or has become invalid. These session cookies are restricted to a single browser session and are never written to a file.

Another facet of SSO is how these technologies redirect a user's web browser to various servlets. The SSO implementation determines when and where these are redirected, and determine the final window shown to the user.

Most SSO implementations are performed in an application's infrastructure and not in the application logic itself. Applications that leverage infrastructure managed authentication (such as deployment specifying Basic or Form authentication) typically have little or no code changes when adapted to work in an SSO environment.

What Do I Need for Single Sign-On?

A Single Sign-On system involves the integration of several components, including Oracle Identity Management and Oracle Access Management. This includes the following components:

- An Oracle Internet Directory (OID) LDAP server, used to store user, role, security, and other information. OID uses an Oracle database as the back-end storage of this information.
- An Oracle Access Manager (OAM) 11g Release 2 server and administrative console for implementing and configuring policies for single sign-on.
- A Policy Enforcement Agent such as Oracle Access Manager 11g Agent (WebGate), used to authenticate the user and create the Single Sign-On cookies.
- Oracle Directory Services Manager (ODSM) application in OIM11g, used to administer users and group information. This information may also be loaded or modified via standard LDAP Data Interchange Format (LDIF) scripts.
- Additional administrative scripts for configuring the OAM system and registering HTTP servers.

Additional WebLogic-managed servers will be needed to deploy the business applications leveraging the Single Sign-On technology.

Can Oracle Access Manager Work with Other SSO Implementations?

Oracle Access Manager has the ability to inter-operate with many other SSO implementations, but with some restrictions.

What Single Sign-On is not?

Single Sign-On is not a user ID/password mapping technology.

However, some applications can store and retrieve user IDs and passwords for non-SSO applications within an OID LDAP server. An example of this is the Oracle Forms Web Application framework, which maps Single Sign-On user IDs to a database logins on a per-application basis.

How Oracle Single Sign-On Works

Oracle Access Manager involves several different components. These are:

- The Oracle Access Manager (OAM) server, which is responsible for the back-end authentication of the user.
- The Oracle Internet Directory LDAP server, which stores user IDs, passwords, and group (role) membership.
- The Oracle Access Manager Agent associated with the Web application, which verifies and controls browser redirection to the Oracle Access Manager server.
- The Web application (if the Web application implements dynamic protection).

About SSO Login Processing with OAM Agents

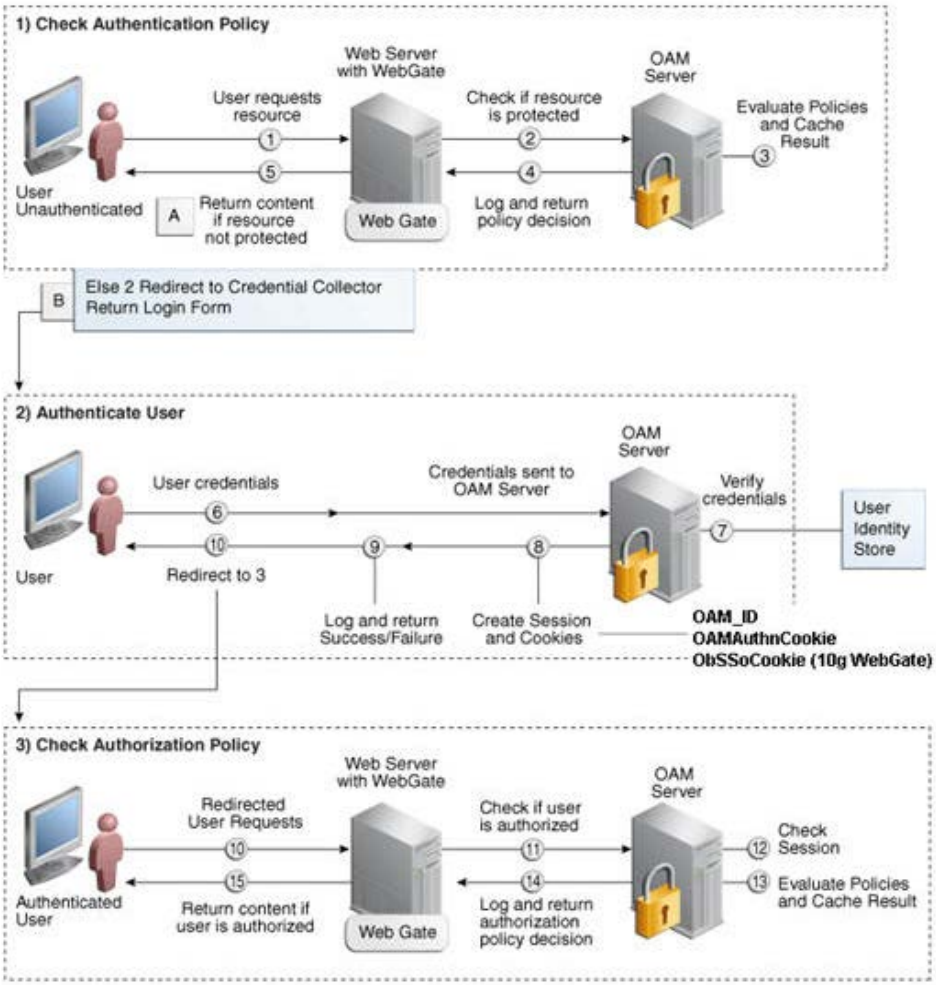
The following steps describe the SSO login processing with OAM agents:

- The user requests a resource.
- WebGate forwards the request to OAM for policy evaluation.
- OAM:

  - Checks for the existence of an SSO cookie.
  - Checks policies to determine if the resource is protected, and, if so, how?
- OAM Server logs and returns the decision.
- WebGate responds as follows:
  - Unprotected Resource: Resource is served to the user.
  - Protected Resource: Resource is redirected to the credential collector. The login form is served based on the authentication policy. Authentication processing begins.
- User sends credentials.
- OAM verifies credentials using the OID for the credential store.
- OAM starts the session and creates the following host-based cookies:
  - One per partner: OAMAuthnCookie set by 11g WebGates using authentication token received from the OAM Server after successful authentication.

    Note: A valid cookie is required for a session

  - One for OAM Server: OAM_ID.
- OAM logs Success of Failure.
- Credential collector redirects to WebGate and authorization processing begin.
- WebGate prompts OAM to look up policies, compare them to the user's identity, and determine the user's level of authorization.
- OAM logs policy decision and checks the session cookie.
- OAM Server evaluates authorization policies and caches the result.
- OAM Server logs and returns decisions.
- WebGate responds as follows:
  - If the authorization policy allows access, the desired content or applications are served to the user.
  - If the authorization policy denies access, the user is redirected to another URL determined by the administrator.



Installation Overview

Installing an Oracle Retail supported Single Sign-On using OAM11g requires installation of the following:

- Installation of web tier on all hosts in the clustered environment. Final configuration will occur
- Oracle Internet Directory (OID) LDAP server and the Oracle Directory Services Manager (ODSM). They are typically installed using the Installer of Oracle Identity Management (11.1.1.9). The ODSM application (included in the OID distribution) can be used for user and realm management within OID.
- Oracle Access Manager (11.1.2.3) has to be installed and configured.
- Additional mid tier instances (such as Oracle Forms 11g) for Oracle Retail applications based on Oracle Forms technologies (such as RMS). These instances must be registered with the OAM installed.
- Additional application servers to deploy other Oracle Retail applications and performing application specific initialization and deployment activities must be registered with OAM. For additional information on SSO 11g installation, see the Oracle Access Manager and Single Sign-On Whitepaper (My Oracle Support Doc ID 1492047.1).

Infrastructure Installation and Configuration

The Infrastructure installation for Oracle Access Manager (OAM) depends on the environment and requirements for its use. Deploying Oracle Access Manager (OAM) to be used in a test environment does not have the same availability requirements as for a production environment. Similarly, the Oracle Internet Directory (OID) LDAP server can be deployed in a variety of different configurations. See the Oracle Identity Management Installation Guide11g.

OID User Data

Oracle Internet Directory is an LDAP v3 compliant directory server. It provides standards-based user definitions out of the box.

Customers with existing corporate LDAP implementations may need to synchronize user information between their existing LDAP directory servers and OID. OID supports standard LDIF file formats and provides a JNDI compliant set of Java classes as well.

Moreover, OID provides additional synchronization and replication facilities to integrate with other corporate LDAP implementations.

Each user ID stored in OID has a specific record containing user specific information. For role-based access, groups of users can be defined and managed within OID. Applications can thus grant access based on group (role) membership saving administration time and providing a more secure implementation.

User Management

User Management consists of displaying, creating, updating or removing user information. There are many methods of managing an LDAP directory including LDIF scripts or Oracle Directory Services Manager (ODSM) available for OID11g.

ODSM

Oracle Directory Services Manager (ODSM) is a Web-based application included in the OID11g distribution and is designed for both administrators and users. It enables you to configure the structure of the directory, define objects in the directory, add and configure users, groups, and other entries. ODSM is the interface you use to manage entries, schema, security, adapters, extensions, and other directory features.

LDIF Scripts

Script based user management can be used to synchronize data between multiple LDAP servers. The standard format for these scripts is the LDAP Data Interchange Format (LDIF). OID supports LDIF script for importing and exporting user information. LDIF scripts may also be used for bulk user load operations.

User Data Synchronization

The user store for Oracle Access Manager resides within the Oracle Internet Directory (OID) LDAP server. Oracle Retail applications may require additional information attached to a user name for application-specific purposes and may be stored in an application-specific database. Currently, there are no Oracle Retail tools for synchronizing changes in OID stored information with application-specific user stores. Implementers should plan appropriate time and resources for this process. Oracle Retail strongly suggests that you configure any Oracle Retail application using an LDAP for its user store to point to the same OID server used with Oracle Access Manager.

2

Understanding Installation Directories

The following technical stack is installed from the locations described.

- Oracle Web Tier 11.1.1.9
  - WEBLOGIC_HOME=/u00/webadmin/products/wls_ohs
  - ORACLE_HOME= /u00/webadmin/products/wls_ohs/Oracle_WT1
- Oracle WebGate 11.1.2.3
  - WEBLOGIC_HOME=/u00/webadmin/products/wls_ohs
  - ORACLE_HOME=/u00/webadmin/products/wls_ohs/WebGate
- Oracle Internet Directory (OID) 11.1.1.9 (Part of Identity Management suite)
  - WEBLOGIC_HOME=/u00/webadmin/products/wls_idm
  - ORACLE_HOME=/u00/webadmin/products/wls_idm/Oracle_IDM1
- Oracle Identity Management (IDM) 11.1.1.9 (Part of Identity Management suite)
  - WEBLOGIC_HOME=/u00/webadmin/products/wls_idm
  - DOMAIN_HOME=/u00/webadmin/products/wls_idm/user_projects/domains/IDMDomain
- Oracle Access Manager (OAM) 11.1.2.3
  - OAM_WEBLOGIC_HOME=/u00/webadmin/products/wls_iam
  - OAM_DOMAIN_HOME= /u00/webadmin/config/domains/wls_iam/OAMDomain
- Oracle Business Intelligence Enterprise Edition 11.1.1.9
  - WEBLOGIC_HOME=/u00/webadmin/products/wls_obiee_oi
  - DOMAIN_HOME= /u00/webadmin/config/domains/wls_obiee_oi/bifoundation_domain_oi
- Java
  - JDK 1.7+ 64 bit (Using Java 7 update 85 for case stud)
  - JAVA_HOME=/u00/webadmin/products/jdk_java

3

Configuring the Load Balancer

Configure load balancer setup with below redirection policies for cluster setup.

Host Designation	Load Balancer URL	Load Balancer Port	Host	Application
idmhost	idmhost-vip.us.oracle.com	3060	idmhost1.us.oracle.com idmhost2.us.oracle.com	LDAP
idmhost	idmhost-vip.us.oracle.com	15003	idmhost1.us.oracle.com idmhost2.us.oracle.com	ODSM
idmhost	idmhost-vip.us.oracle.com	16001	idmhost1.us.oracle.com idmhost2.us.oracle.com	OAM CONSOLE
idmhost	idmhost-vip.us.oracle.com	7777	idmhost1.us.oracle.com idmhost2.us.oracle.com	Web Tier
idmhost	apphost-vip.us.oracle.com	7777	apphost1.us.oracle.com apphost2.us.oracle.com	Web Tier
idmhost	ribhost-vip.us.oracle.com	7777	ribhost1.us.oracle.com ribhost2.us.oracle.com	Web Tier
rtghost	rtghost-vip.us.oracle.com	7777	rtghost1.us.oracle.com rtghost2.us.oracle.com	

4

Installing Oracle Web Tier

This chapter describes the installation of Oracle Web Tier.

Perform the following steps to install Web Tier 11.1.1.9 on the hosts listed below:

- idmhost1.us.oracle.com
- idmhost2.us.oracle.com
- apphost1.us.oracle.com
- apphost2.us.oracle.com
- ribhost1.us.oracle.com (only ribhost1.us.oracle.com)
- rtghost1.us.oracle.com
- rtghost2.us.oracle.com
- Download software installation for Web Tier 11.1.1.9 and place it in an installation staging directory (referenced as <INSTALL_DIR>) on the Linux host and unpack the distribution. <INSTALL_DIR>/Webtier_11.1.1.9.
- Set the following variables by exporting them before running the installer:
  - JAVA_HOME
  - PATH
  - DISPLAY

Example:

```
$ export JAVA_HOME=/u00/webadmin/products/jdk_java
$ export PATH=$JAVA_HOME/bin:$PATH
$ export DISPLAY=<pc_ip_address:0.0>
```

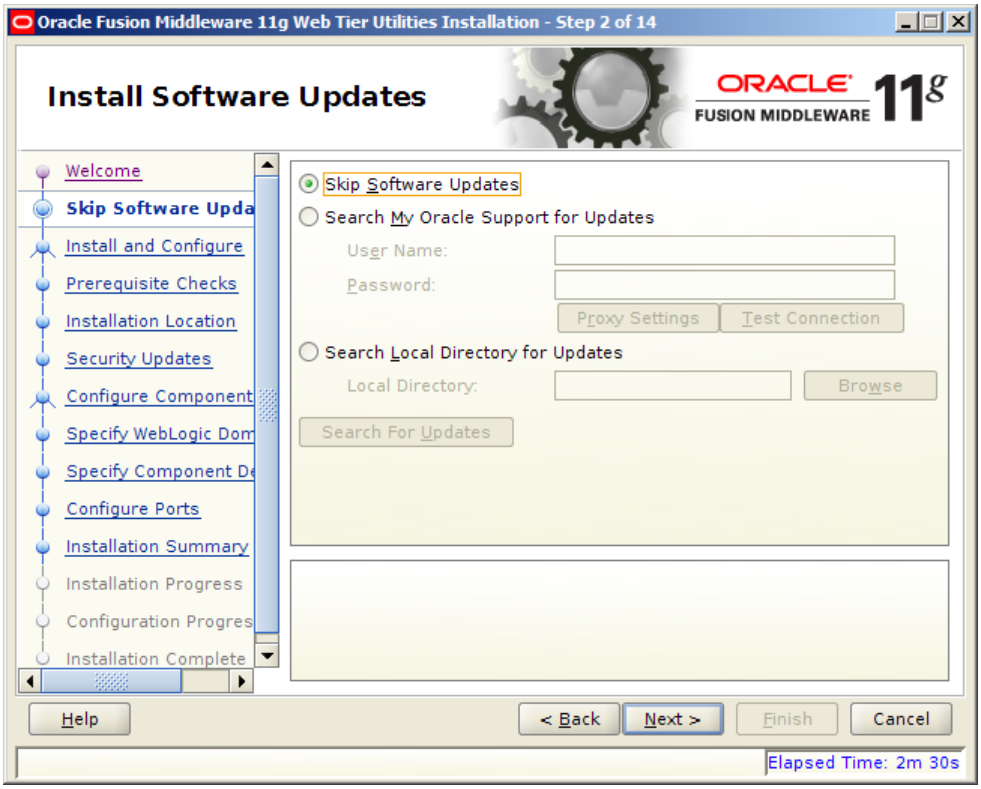
- Run the following commands to run the installer:

Example:

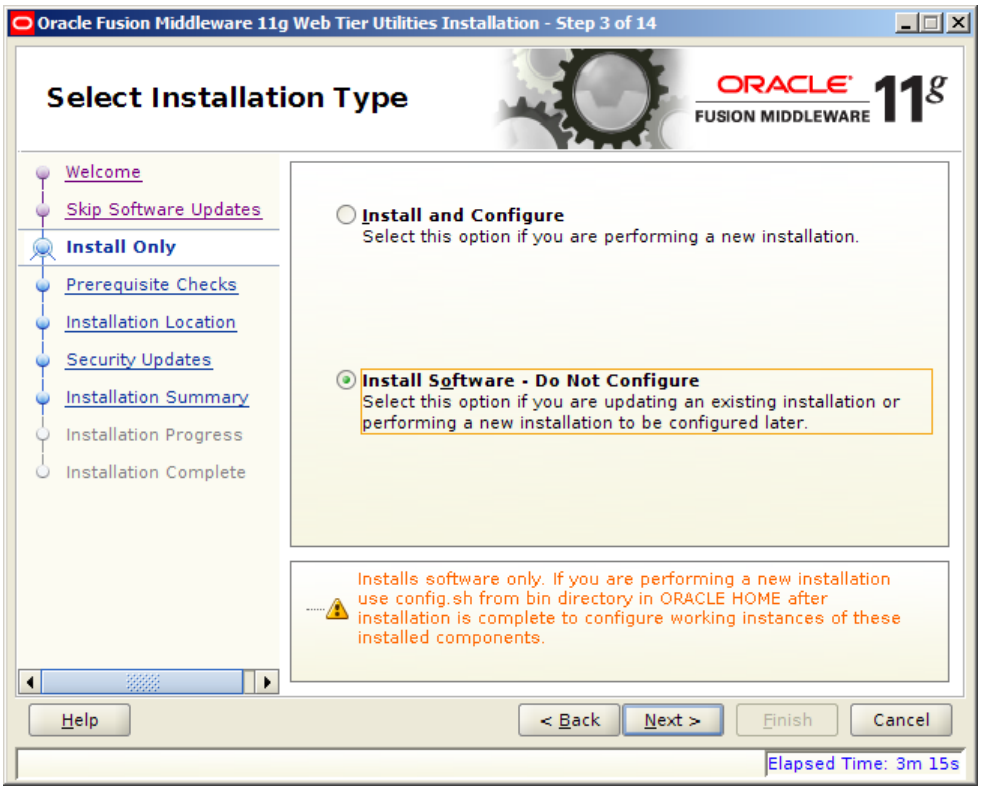
```
$ cd <INSTALL_DIR>/Webtier_11.1.1.9/Disk1
$ ./runInstaller
```

- The Web Tier Welcome window opens. Click **Next**.

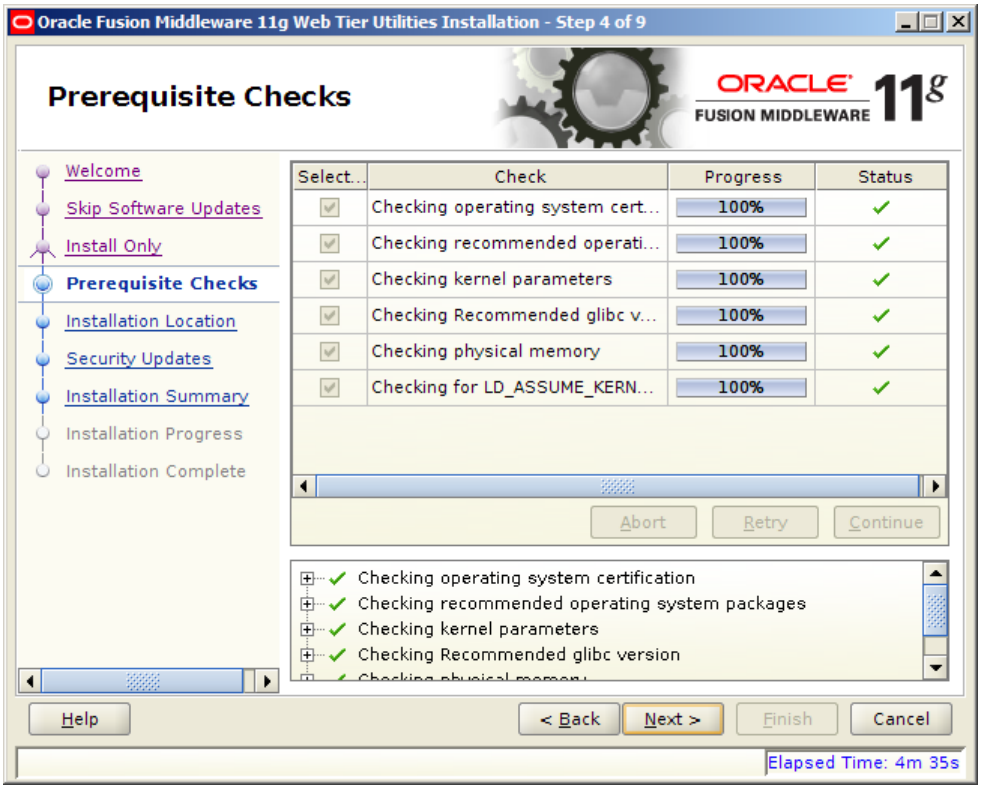
- The Install Software Updates window opens. Select **Skip Software Updates,** and click **Next.**



- The Select Installation Type window opens. Select **Install Software - Do Not Configure** and click **Next**.



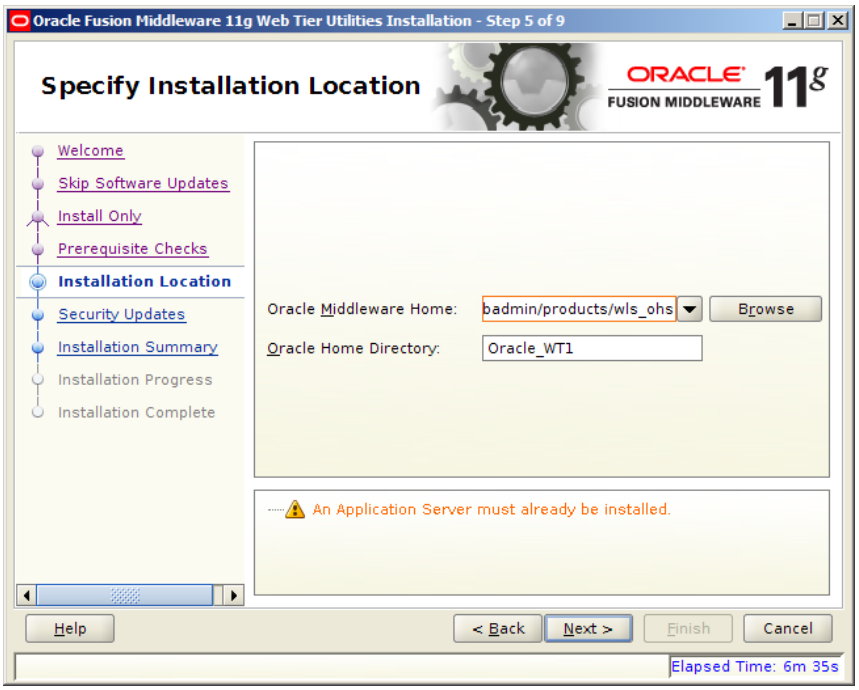
- The Prerequisite Checks window opens. Click **Next**.



- The Specify Installation Location window opens. Select the Oracle Middleware Home install directory, and click **Next**.

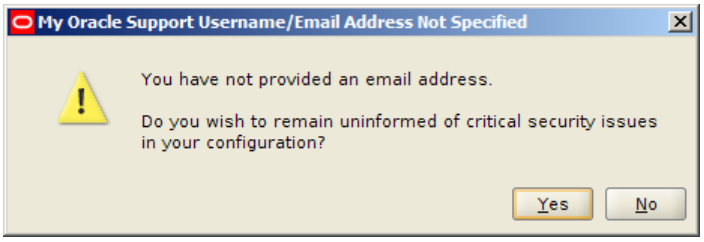
Example:

`/u00/webadmin/products/wls_ohs`

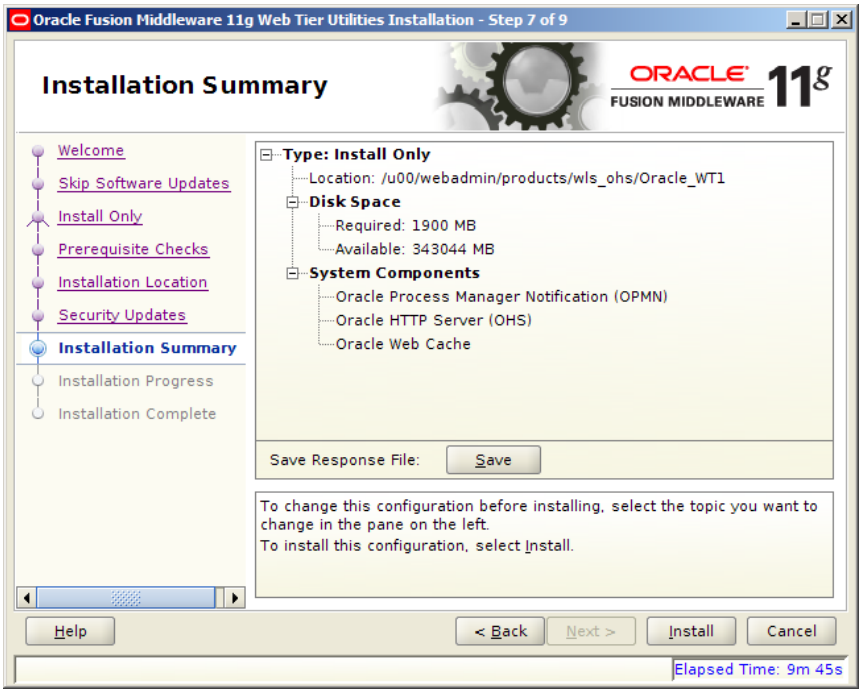


- The Specify Security Updates window opens. Uncheck the check box, and click **Next**.

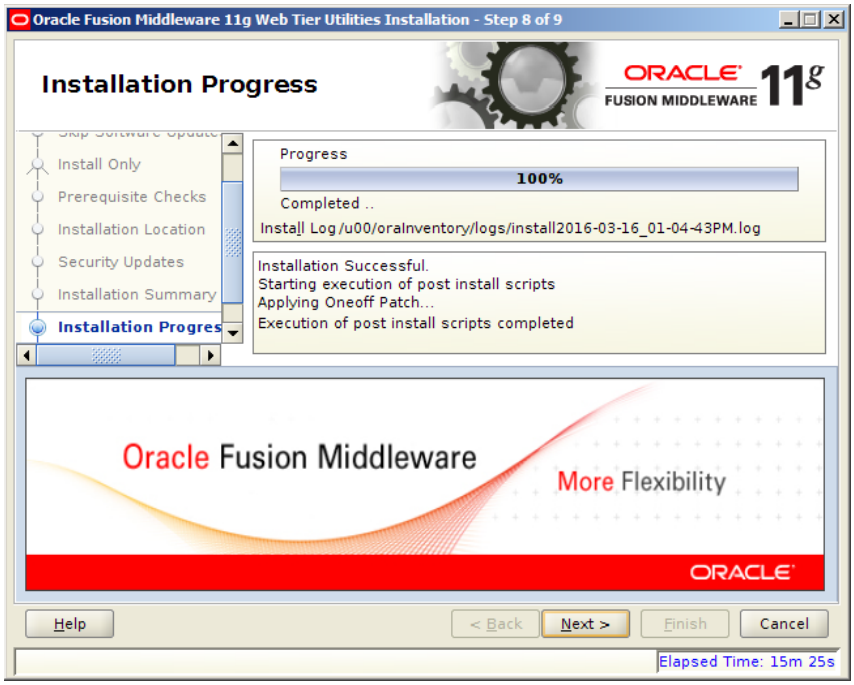
- A warning dialog opens, indicating that an email address was not provided. Click **Yes**.



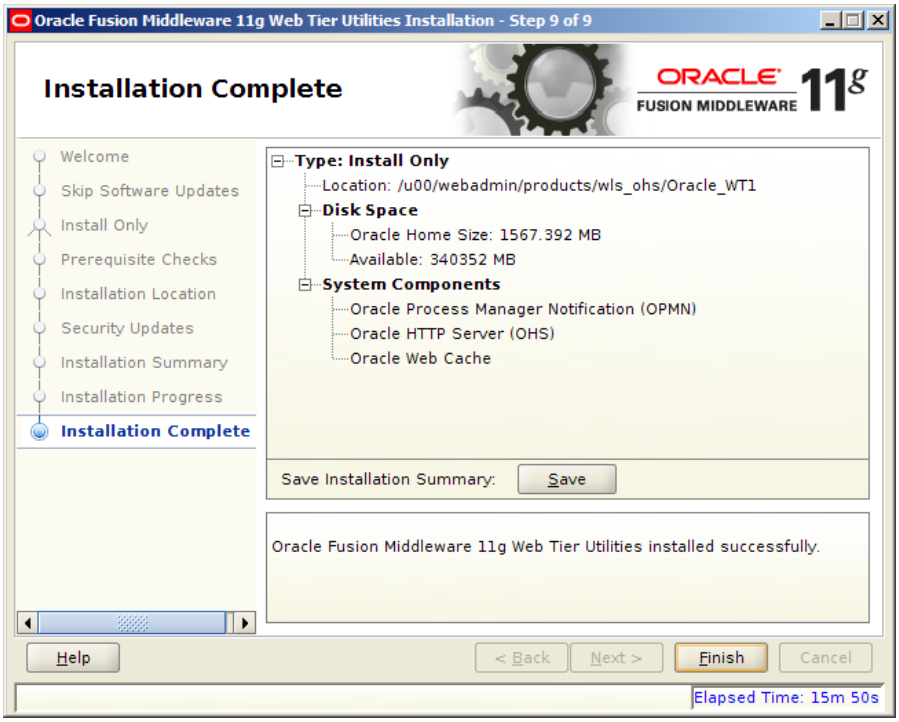
- The Installation Summary window opens. Click **Install**.



- The Installation Progress window opens. Click **Install**.



- The Installation Complete window opens. Click **Next** and then **Finish**.



- The installation is complete.

Configuring Web Tier on idmhost1 and idmhost2

This chapter describes the configuration of Web Tier11.1.1.9 on both the hosts.

Perform the following steps for the following hosts in the environment to configure Web Tier 11.1.1.9:

- idmhost1.us.oracle.com
- idmhost2.us.oracle.com
- apphost1.us.oracle.com
- apphost2.us.oracle.com
- ribhost1.us.oracle.com (Just ribhost1)
- rtghost1.us.oracle.com
- rtghost2.us.oracle.com
- Set the following variables by exporting them before running the installer:
  - JAVA_HOME
  - PATH
  - DISPLAY

  Example:

  ```
  $ export JAVA_HOME=/u00/webadmin/products/jdk_java
  $ export PATH=$JAVA_HOME/bin:$PATH
  $ export DISPLAY=<pc_ip_address:0.0>
  ```

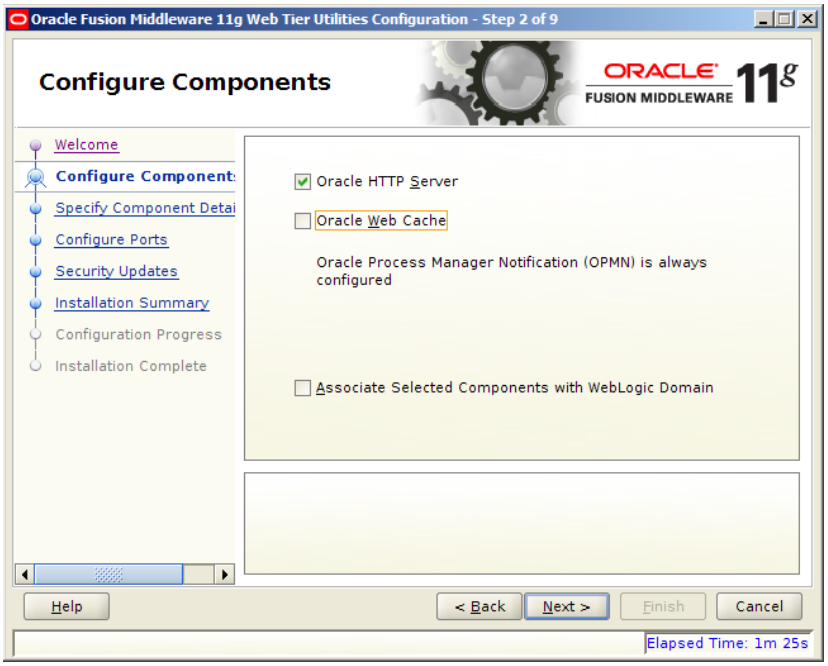
- Execute the following commands to start the Web Tier Utilities Configuration wizard:

  Example:

```
$ cd /u00/webadmin/products/wls_ohs/Oracle_WT1/bin
$ ./config.sh
```

- The Web Tier Welcome window opens. Click **Next**.

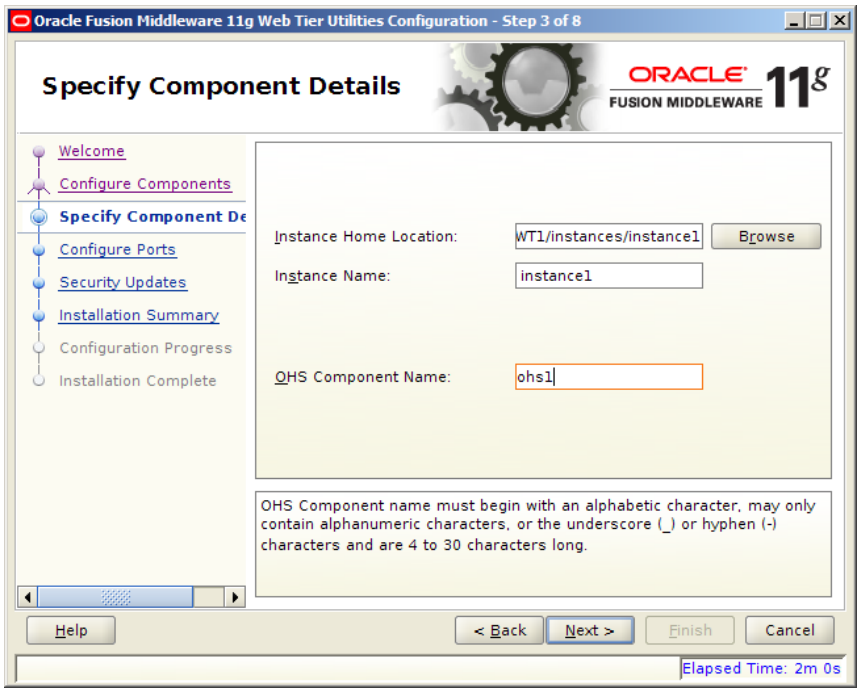
- The Configure Components window opens:
  - Select Oracle HTTP Server.
  - Do not select Ensure that Associate Selected Components with WebLogic Domain.
  - Do not select Oracle Web Cache.
  - Click **Next**.



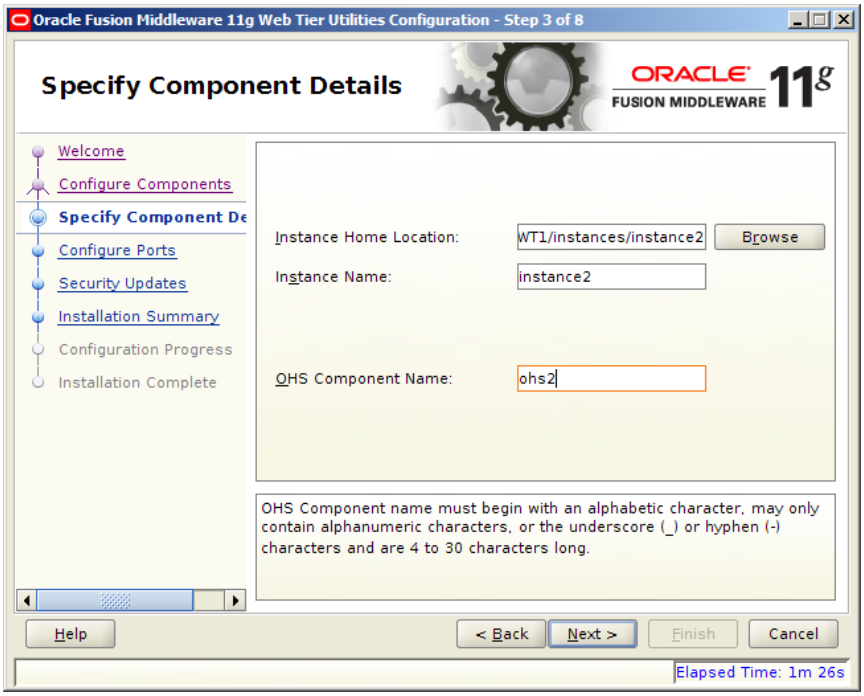
- The Specify Component Details window opens. Enter values in according to instructions below depending upon host1 or host2 and then click **Next**. When

running config.sh on host1 (idmhost1, apphost1, ribhost1, rtghost1) Specify the following values:

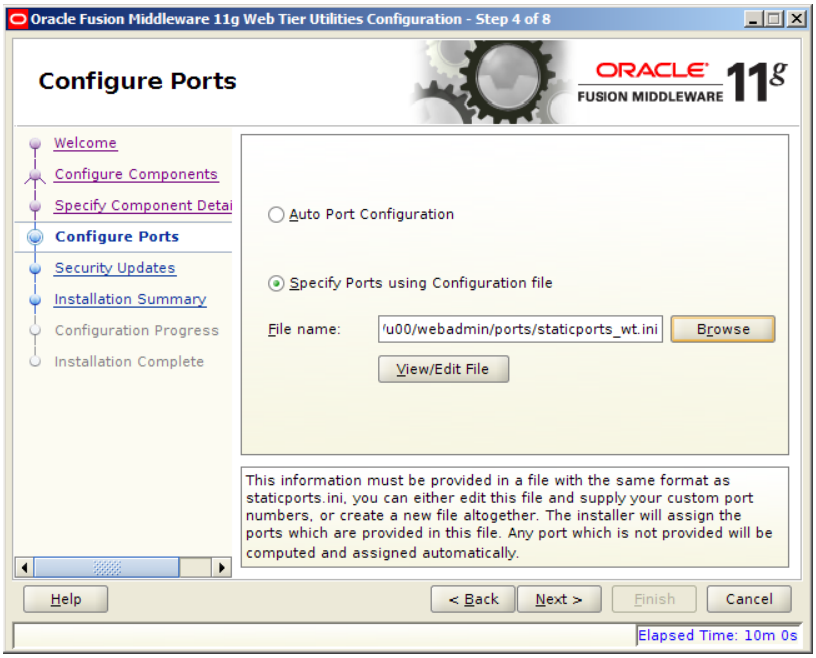
- Instance Home Location: /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1
- Instance Name: instance1
- OHS Component Name ohs1



- When running config.sh on host2 (idmhost2, apphost2, rtghost2) Specify the following values:
  - Instance Home Location: /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance2
  - Instance Name: instance2
  - OHS Component Name ohs2

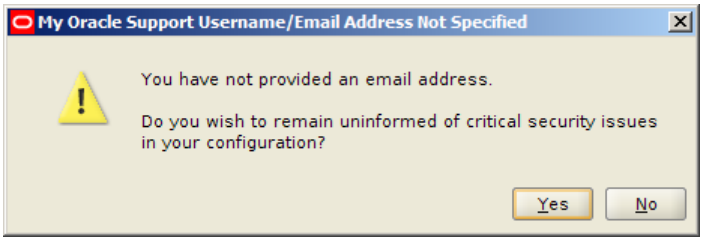


- The Configure Ports window opens.
  - Use the radio button to select Specify Ports using Configuration file
  - Navigate to and copy the sample staticports.ini from:
  - <INSTALL_DIR>/Webtier_11.1.1.9/Disk1/stage/Response directory, to: `/u00/webadmin/ports/`
  - Rename it as staticports_wt.ini and modify the values as per Appendix VI - Creating Staticports for Web Tier Configuration.
  - Click **Next**.

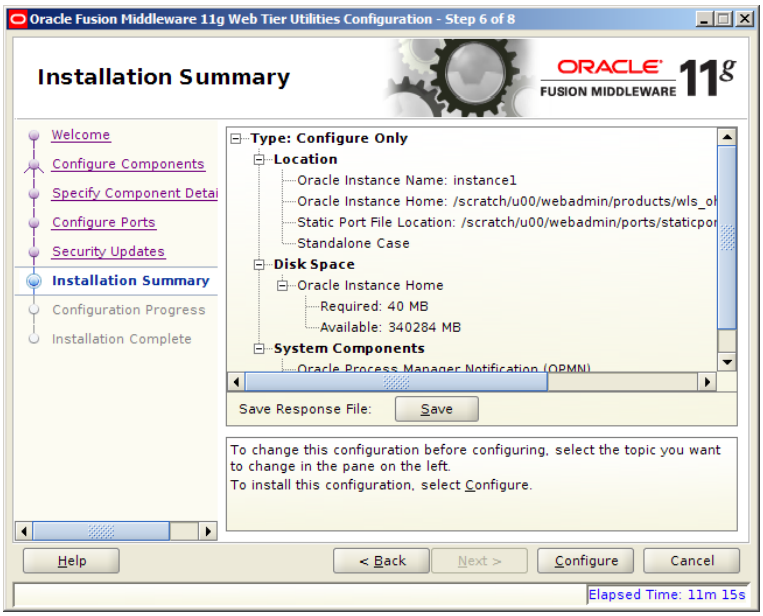


- The Specify Security Updates window opens. Uncheck the checkbox, and click **Next**.

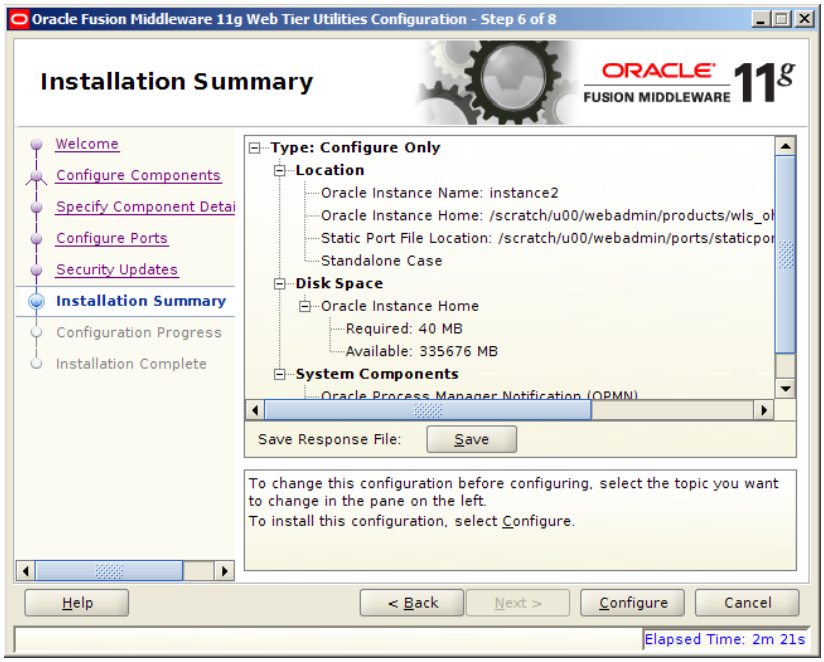
- A warning message opens. Click **Yes** to confirm.



- The Installation Summary window opens. Review the selections to ensure that they are correct. If they are not, click Back to modify selections on previous windows. Click Configure.
  - Screen shot host1 (idmhost1, apphost1, ribhost1, rtghost1)

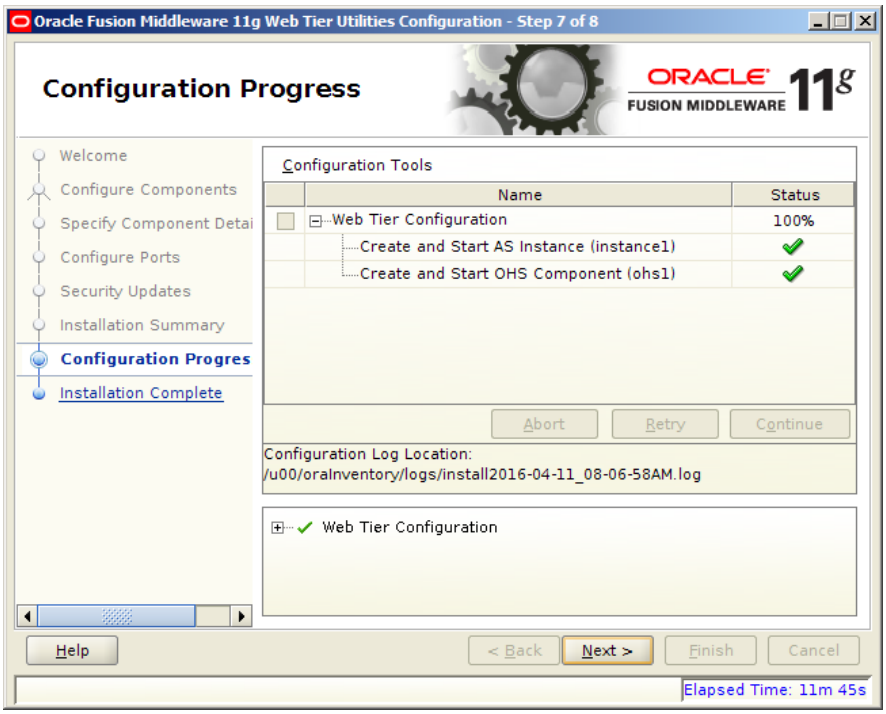


– Screen shot host2 (idmhost2, apphost2, rtghost2)

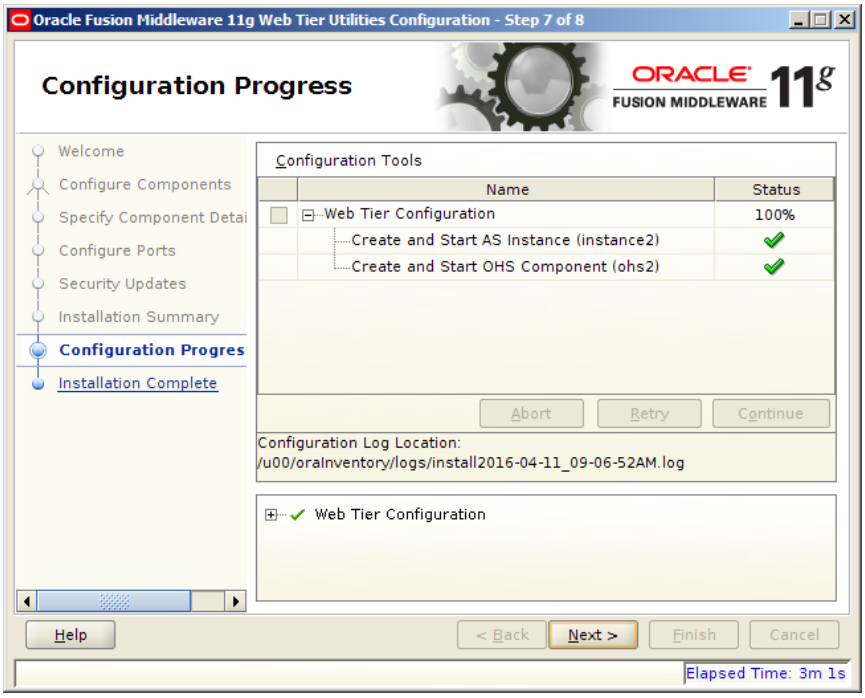


- The Configuration window opens. Click **Next**.

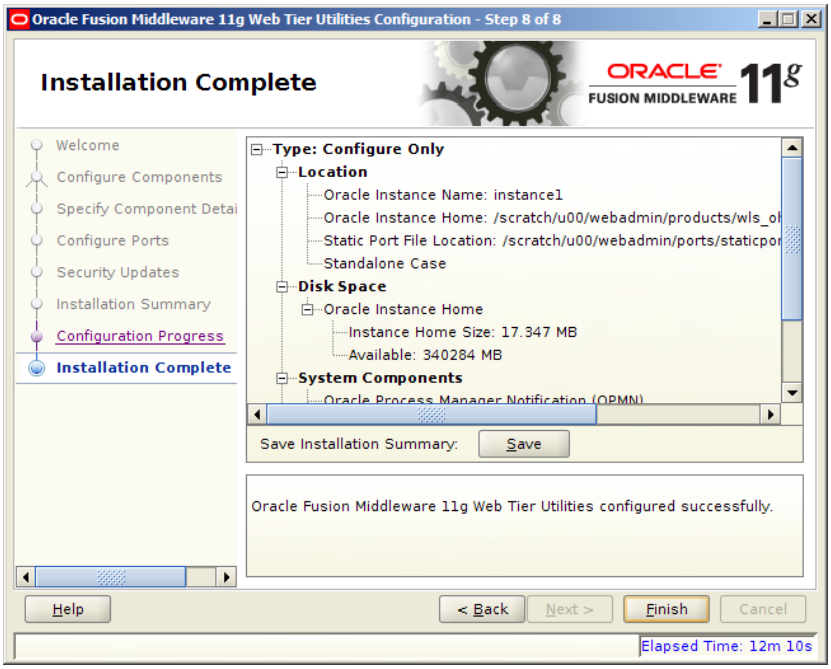
– Screen shot host1 (idmhost1, apphost1, ribhost1, rtghost1)



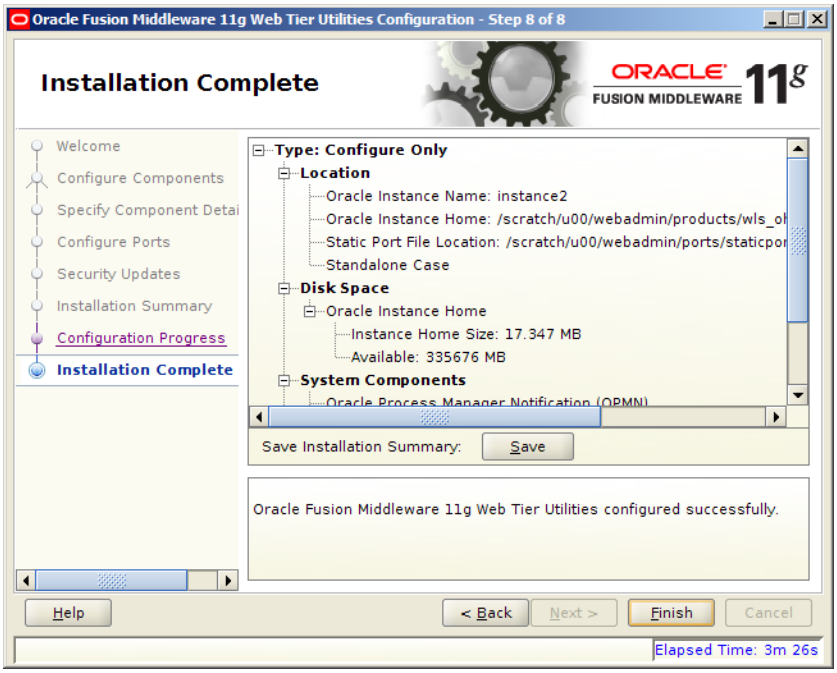
– Screen shot host2 (idmhost2, apphost2, rtghost2)



- The Installation Complete window opens . Click **Finish** to exit.
  - Screen shot host1 (idmhost1, apphost1, ribhost1, rtghost1)



  - Screen shot host2 (idmhost2, apphost2, rtghost2)



- The configuration is complete.

Verification – Web Tier Installation and Virtual Host Alias

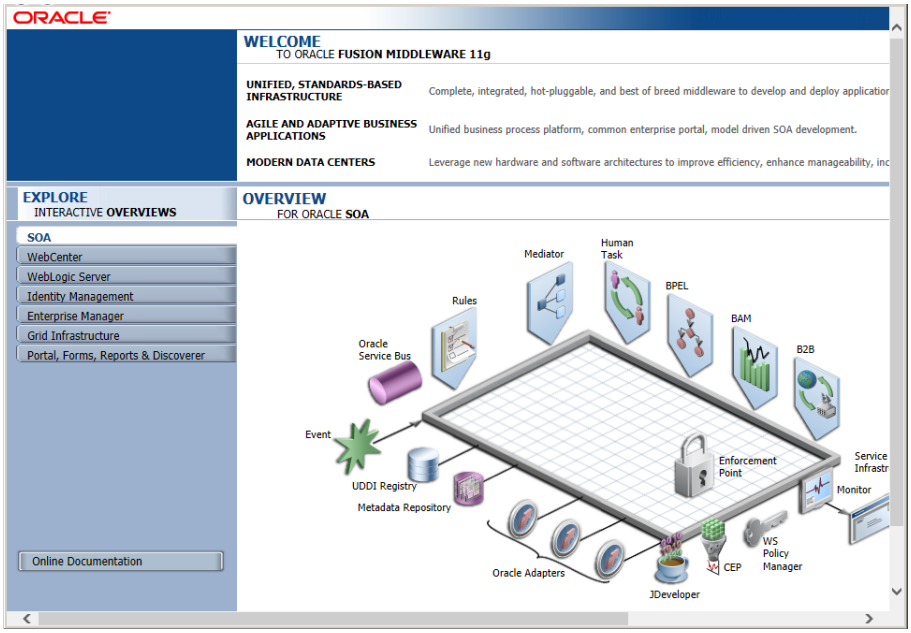
Now that that the Web Tier is installed – There is a good way to validate that virtual host alias has been setup and is allowing traffic in on port 7777 and that applications can be accessed using Web Tier.

> **Note:** Port 7777 was configured to be opened up for the virtual host alias in this case study.
>
> Web Tier is usually started automatically at the time it is installed

- For each virtual host alias Launch Web Tier using the virtual host alias as a part of the URL with port 7777

Examples:

```
http://apphost-vip.us.oracle.com:7777/   (apphost1.us.oracle.com,
apphost7.us.oracle.com)
http://idmhost-vip.us.oracle.com:7777/   (idmhost1.us.oracle.com,
idmhost2.us.oracle.com)
http://10.141.32.77:7777/                          (floating IP for
ribhost1.us.oracle.com, ribhost2.us.oracle.com)
http://rtghost-vip.us.oracle.com:7777/    (rtghost1.us.oracle.com,
rtghost2.us.oracle.com)
```



Note: Web Tier is usually started at the time it is installed automatically. If it fails – validate that the opmn processes are running.

Example:

```
$ export
ORACLE_INSTANCE=/u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1
$ cd /u00/webadmin/products/wls_ohs/Oracle_WT1/opmn/bin
$ ./opmnctl status
```

Output

Processes in Instance: instance1

ias-component	process-type	pid	status
ohs1	OHS	9318	Alive

5

Installing OAM Webgate

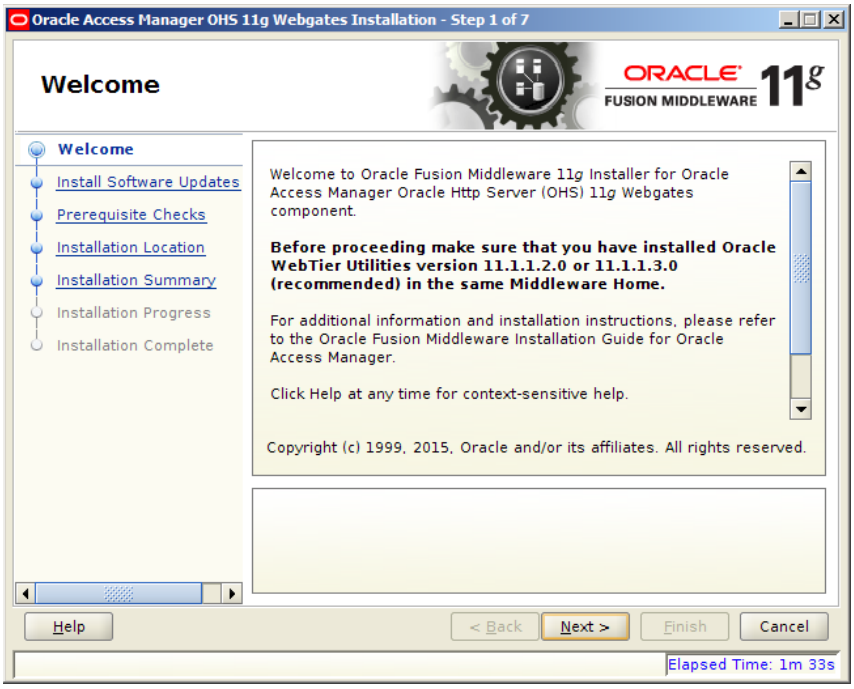
This chapter describes the installation of OAM WebGate.
Perform the following steps for the following hosts in the environment to install OAM WebGate 11.1.2.3:

- idmhost1.us.oracle.com
- idmhost2.us.oracle.com
- apphost1.us.oracle.com
- apphost2.us.oracle.com
- Download software installation for OAM WebGate 11.1.2.3 and place it in an installation staging directory (referenced as <INSTALL_DIR>) on the Linux host and unpack the distribution. <INSTALL_DIR>/oam_webgate_11.1.2.3.
- Set the following variables by exporting them before running the installer:
  - JAVA_HOME
  - PATH
  - DISPLAY

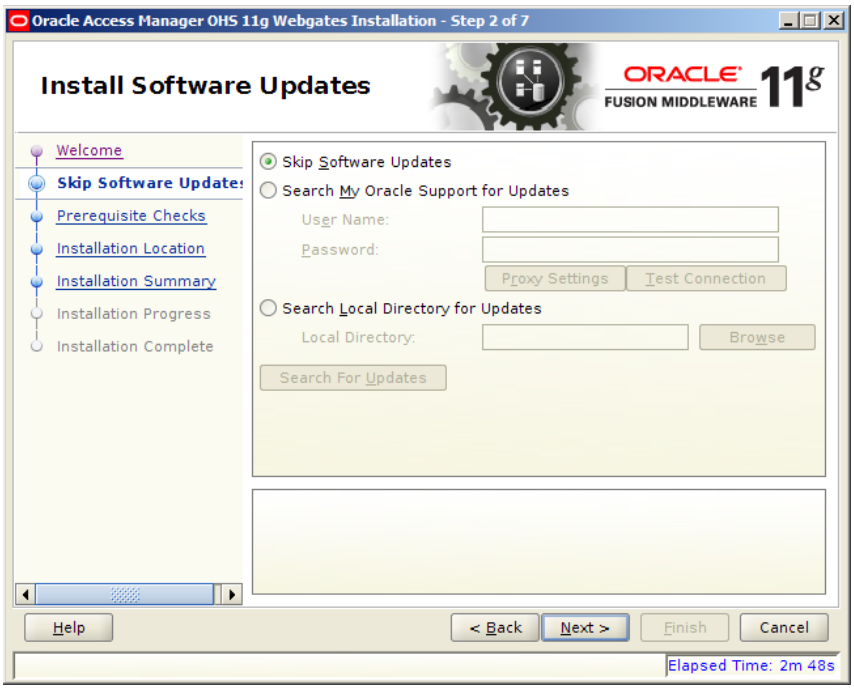
  Example:

  ```
  $ export JAVA_HOME=/u00/webadmin/products/jdk_java
  $ export PATH=$JAVA_HOME/bin:$PATH
  $ export DISPLAY=<pc_ip_address:0.0>
  ```
- Run the following commands to run the installer:

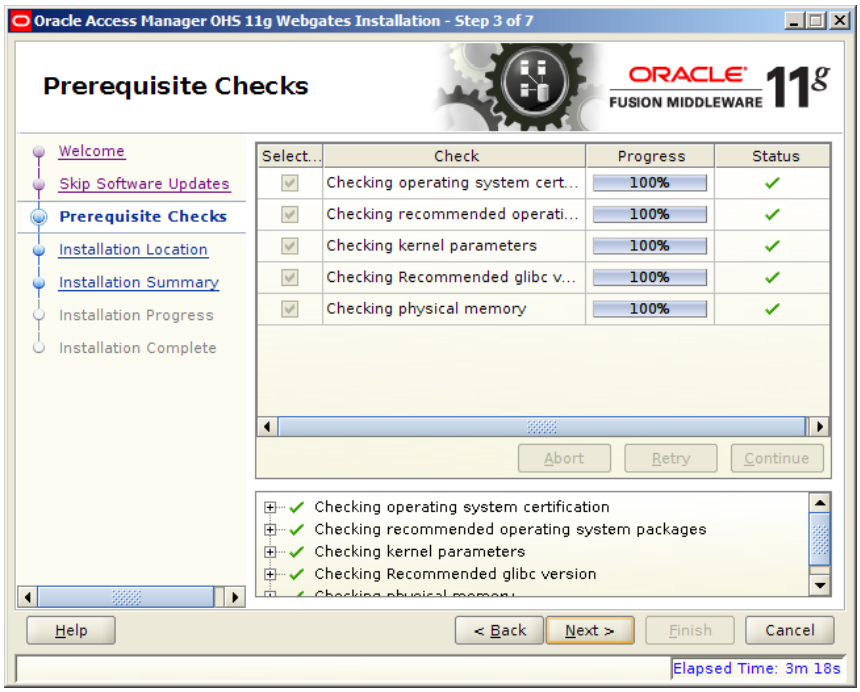
  ```
  $ cd <INSTALL_DIR>/oam_webgate_11.1.2.3/Disk1
  $ ./runInstaller
  ```
- The Welcome window opens. Click **Next**.



- The Install Software Updates window opens. Select Skip Software Updates and click **Next**.



- The Prerequisite Checks window opens. Click **Next**.

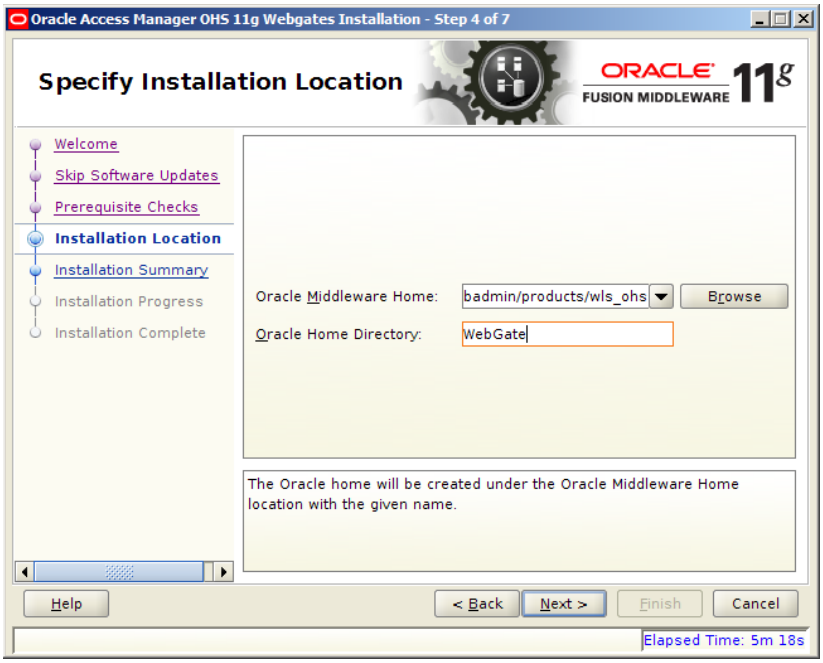


- On the Installation Location window, enter values for Oracle Middleware Home and the Oracle Home Directory, and click **Next**.

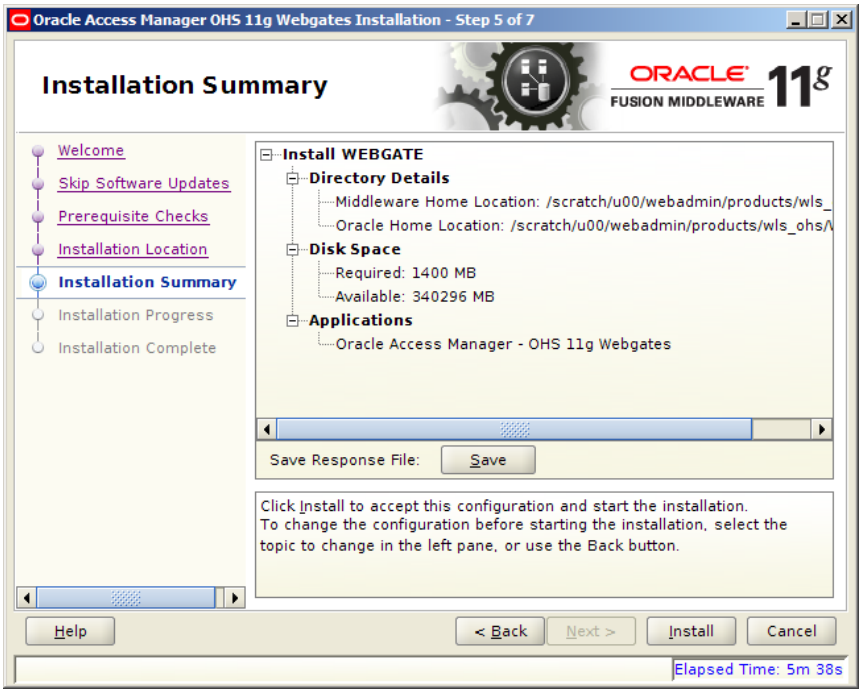
  Example:

  ```
  Oracle Middleware Home: /u00/webadmin/products/wls_ohs
  Oracle Home Directory: WebGate
  ```

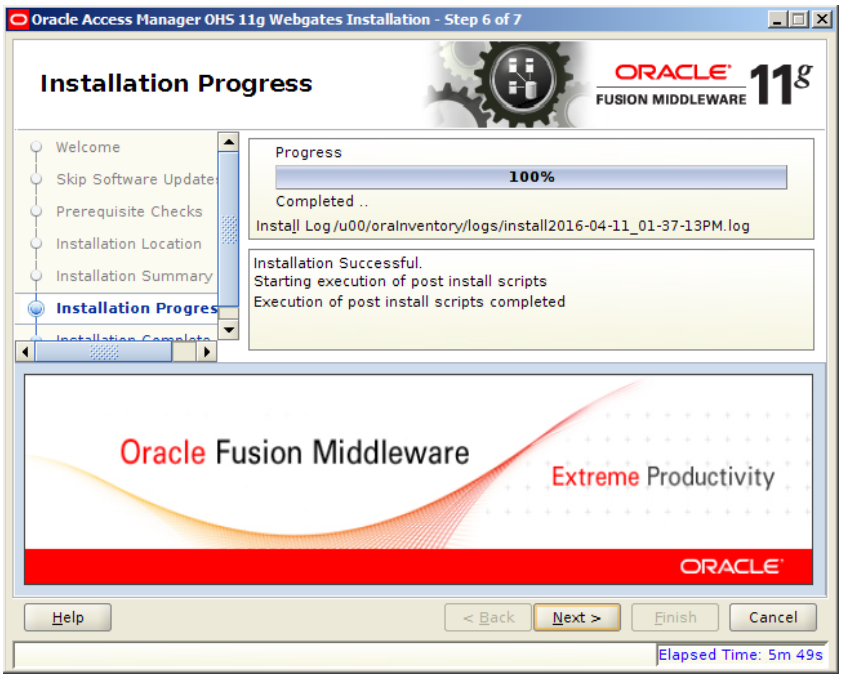
Note: Oracle WebLogic Server is not a prerequisite for installing Oracle HTTP Server WebGate.



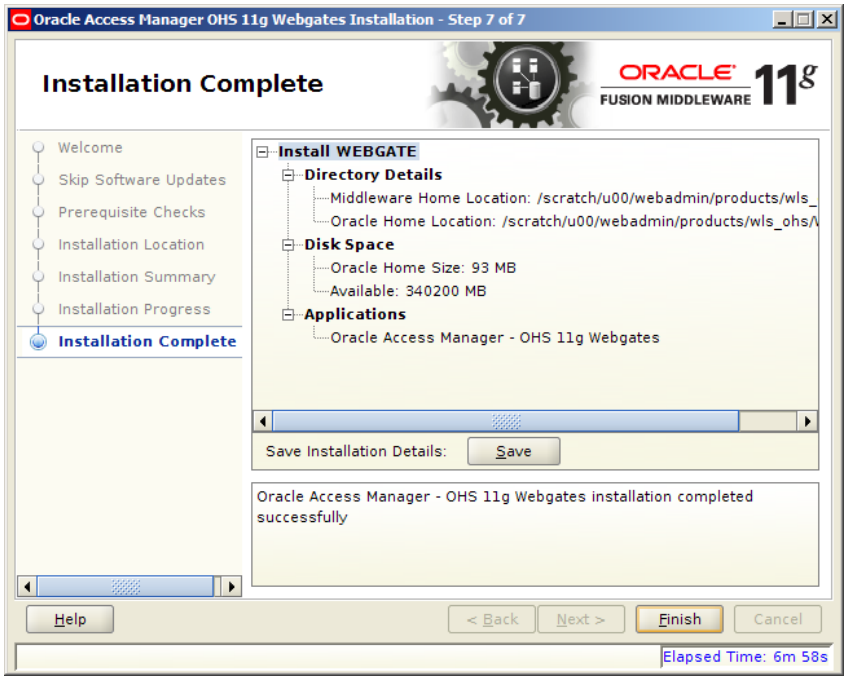
- The Installation Summary window opens. Verify the response information you have provided. Click **Install** to begin the installation.



- The Installation Progress window opens. Click **Next**.



- The Installation Complete window opens. Click **Save**, and save the summary as webgateInstall.txt. Click **Finish** to complete the WebGate installation.



- The installation is complete.

Configuring OAM WebGate

This chapter describes the steps to incorporate the OAM WebGate installation into Web Tier instances.

Perform the following steps for the 4 hosts listed below to deploy and configure the WebGate:

- idmhost1.us.oracle.com
- idmhost2.us.oracle.com
- apphost1.us.oracle.com
- apphost2.us.oracle.com
- For each host in the list above Change directories to the WebGate deployWebGate directory:
  <WEBGATE_ORACLE_HOME>/webgate/ohs/tools/deployWebGate

  Example:

  ```
  $ cd
  /u00/webadmin/products/wls_ohs/WebGate/webgate/ohs/tools/deployWebGate
  ```
- On host1 (idmhost1 and apphost1) Execute the deployWebgatesInstance.sh using the following syntax:

  Example:

  ```
  $ ./deployWebGateInstance.sh -w
  /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1/config/OHS/o
  hs1 -oh /u00/webadmin/products/wls_ohs/WebGate
  ```

  Output:

  Copying files from WebGate Oracle Home to WebGate Instancedir
- On host2 (idmhost2 and apphost2) Execute the deployWebgatesInstance.sh using the following syntax:

  Example:

  ```
  $ ./deployWebGateInstance.sh -w
  /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance2/config/OHS/o
  hs2 -oh /u00/webadmin/products/wls_ohs/WebGate
  ```

  Output:

  Copying files from WebGate Oracle Home to WebGate Instancedir
- For each host (idmhost1, idmhost2, apphost1, apphost2):
  - Set the LD_LIBRARY_PATH to contain the OHS lib:<Oracle_Home_for_Oracle_HTTP_Server>/lib
  - Change directories to the WebGate InstallTools directory:
    <WEBGATE_ORACLE_HOME>/webgate/ohs/tools/setup/InstallTools

    Example:

    ```
    $ export
    LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/u00/webadmin/products/wls_ohs/Oracle_
    WT1/lib
    $ cd
    /u00/webadmin/products/wls_ohs/WebGate/webgate/ohs/tools/setup/InstallT
    ools
    ```
- On host1 (idmhost1 and apphost1) Execute the following command to copy the WebGate template to the OHS WebGate instance location and update the httpd.conf file:

  Example:

  ```
  $ ./EditHttpConf -w
  /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1/config/OHS/o
  hs1 -oh /u00/webadmin/products/wls_ohs/WebGate
  ```

  Output:

  The web server configuration file was successfully updated.

- On host2 (idmhost2 and apphost2) Execute the following command to copy the WebGate template to the OHS WebGate instance location and update the httpd.conf file:

  Example:

  ```
  $ ./EditHttpConf -w
  /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance2/config/OHS/o
  hs2 -oh /u00/webadmin/products/wls_ohs/WebGate
  ```

  Output:

  The web server configuration file was successfully updated.

6

Installing Oracle Internet Directory

This chapter describes the steps to install the Oracle Internet Directory.

The following hosts will have IDM 11.1.1.9 installed on them: (Pay attention host specific instructions.)

- idmhost1.us.oracle.com
- idmhost2.us.oracle.com

Install WebLogic Server 10.3.6 on idmhost1 and idmhost2

Perform the following steps to install a WebLogic 10.3.6 server on idmhost1 and idmhost2:

- Download software installation for WebLogic and place it in an installation staging directory on the Linux host.

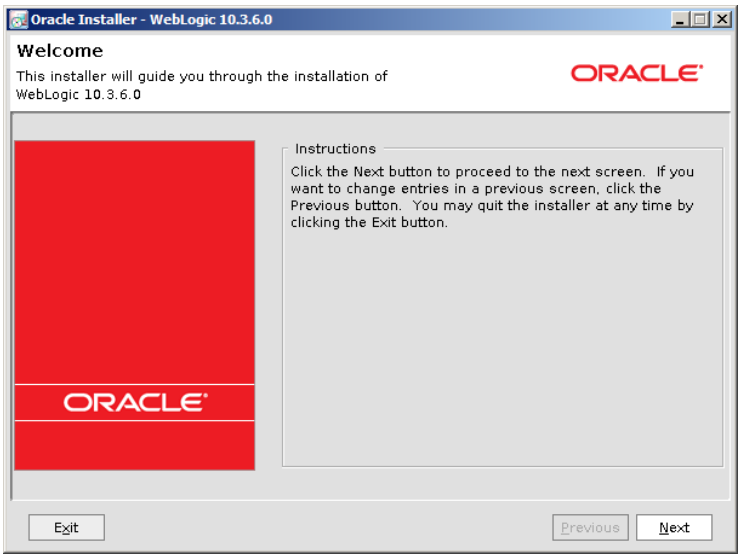
  `<INSTALL_DIR>/WLS_10.3.6.`
- Set the following variables by exporting them before running the installer:
  - JAVA_HOME
  - PATH
  - DISPLAY

  Example:

  ```
  $ export JAVA_HOME=/u00/webadmin/products/jdk_java
  $ export PATH=$JAVA_HOME/bin:$PATH
  $ export DISPLAY=<pc_ip_address:0.0>
  ```
- Run the following commands to run the installer:

  Example:

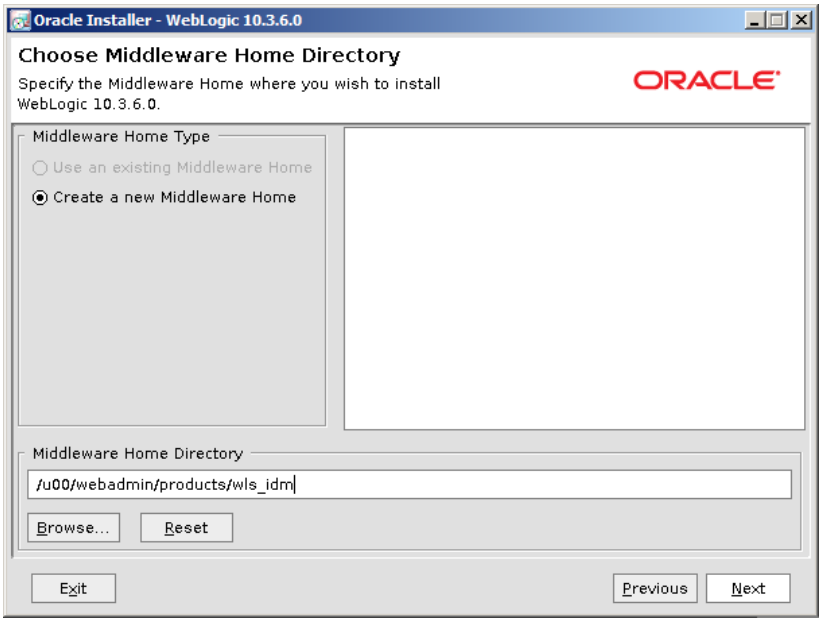
  ```
  $ cd <INSTALL_DIR>/WLS_10.3.6
  $ java -jar ./wls1036_generic.jar
  ```
- The Welcome window of the WebLogic 10.3.6 Installer opens. Click **Next**.



- The Choose Middleware Home Directory window opens. Enter the path to where the WEBLOGIC_HOME for IDM should be and click **Next**.

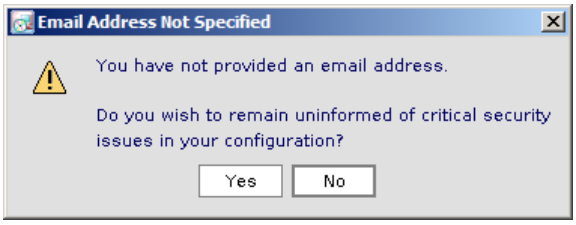
  Example:

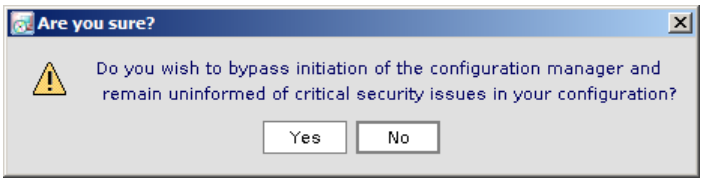
  `/u00/webadmin/products/wls_idm`



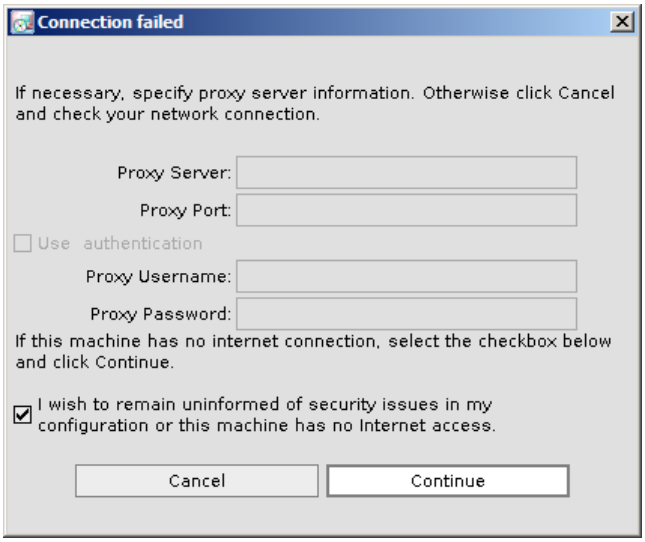
- The Email Registration window opens. Leave check box checked and click **Next**.

- Click **Yes** in the following two prompts.

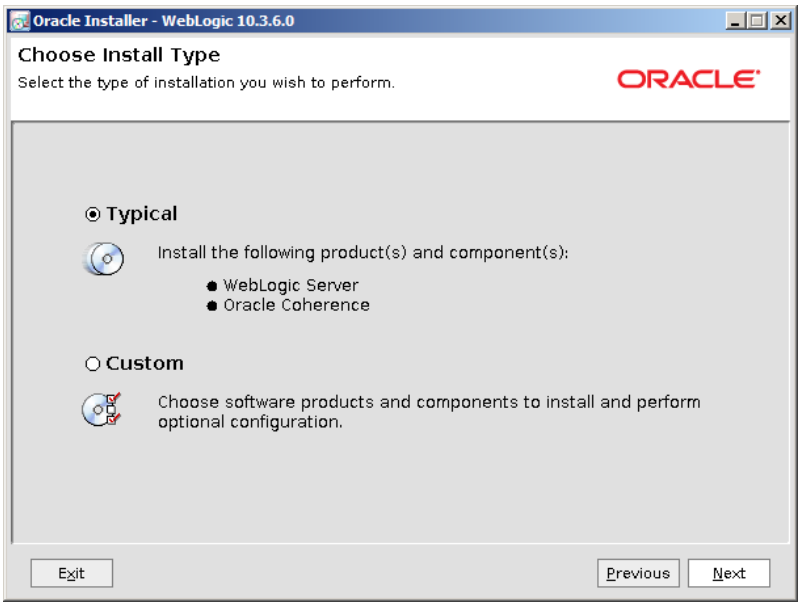




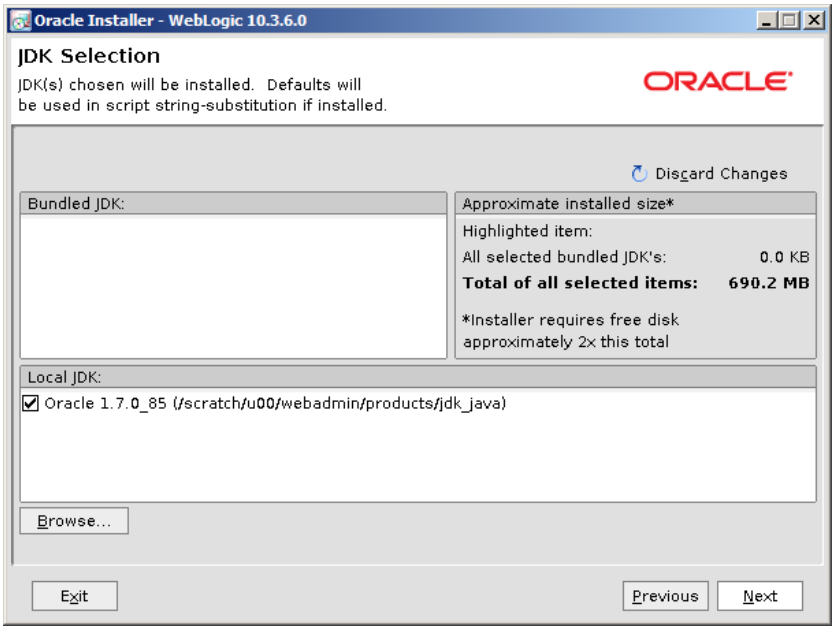
- The Connection Failed warning window opens. Click **Continue**.



- The Choose Install Type window opens. Select Typical, and click **Next**.

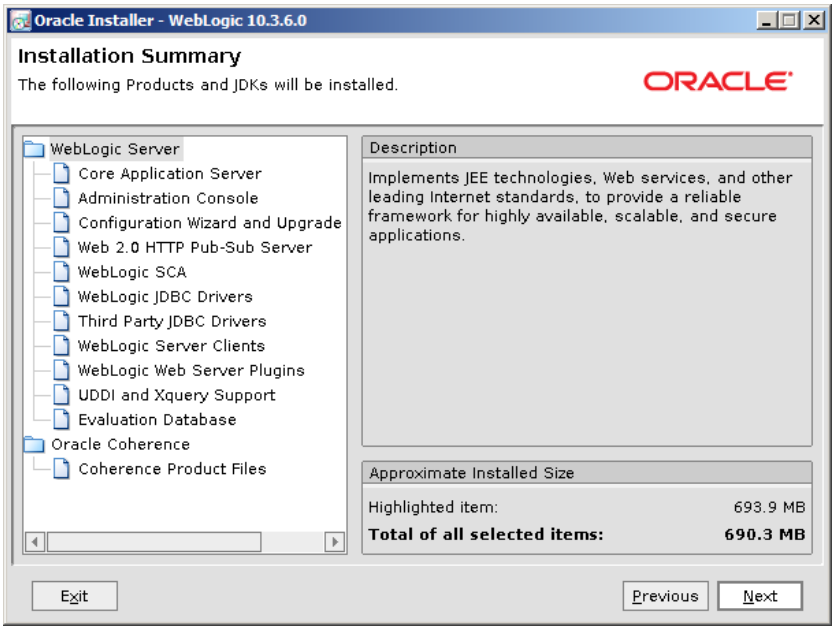


- The JDK Selection window opens. By default, it will select the JDK in your JAVA_HOME setting. Ensure the JAVA_HOME points to JDK 1.7.0+ and click **Next**.

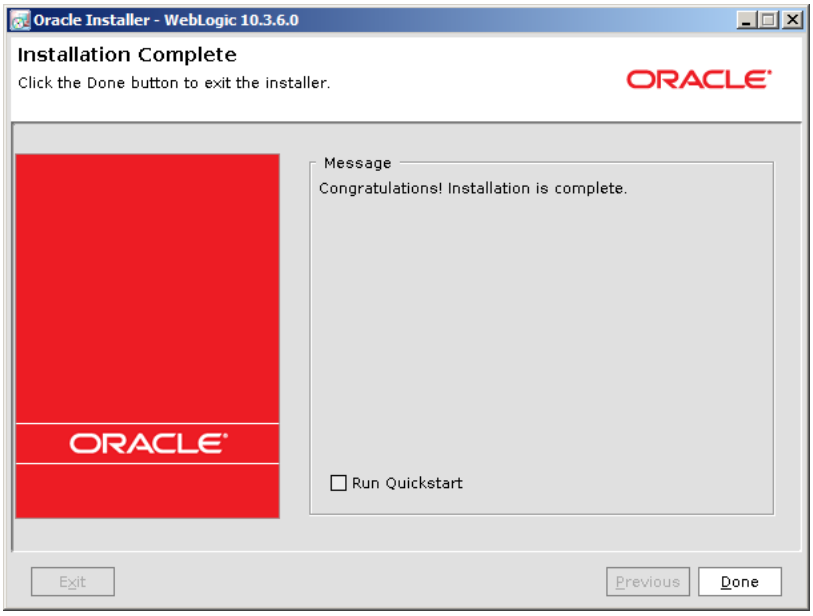


- The Choose Product Installation Directories window opens. Keep the defaults, and click **Next**.

- The Installation Summary window opens. Click **Next**. The product install begins.



- Once finished, the Installation Complete window opens. Un-check the Run Quickstart check box, and click **Done**.



- The installation is complete.

Install Oracle Internet Directory on idmhost1 and idmhost2

Perform the following steps to install a IDM 11.1.1.9 on idmhost1 and idmhost2:

- Download software installation for IDM 1.1.1.9 and place it in an installation staging directory (<INSTALL_DIR>/idm_11.1.1.9) on the Linux host and extract the contents of the zip files.
- Set the following variables by exporting them before running the installer:
  - JAVA_HOME
  - PATH
  - DISPLAY

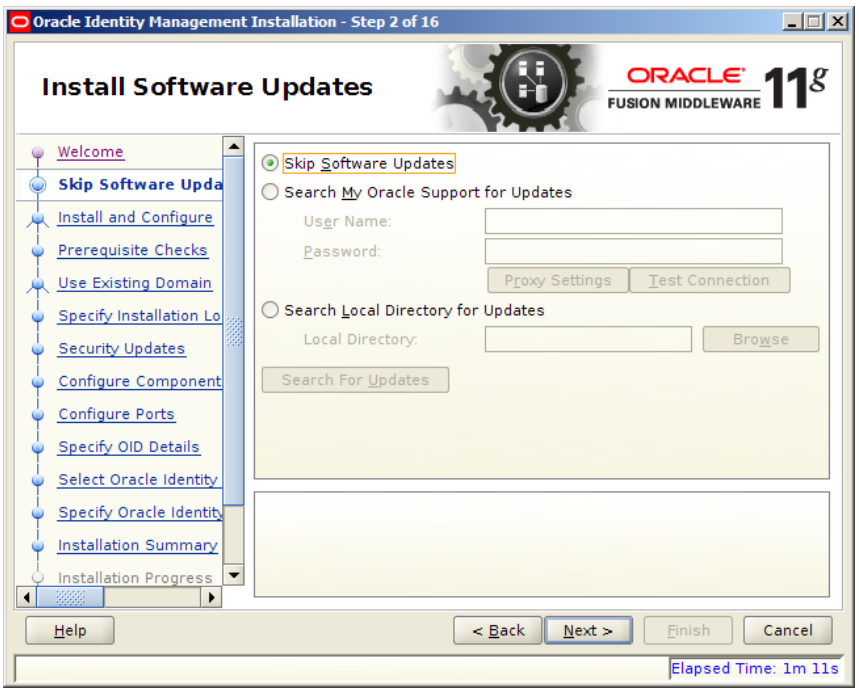
  Example:

  ```
  $ export JAVA_HOME=/u00/webadmin/products/jdk_java
  $ export PATH=$JAVA_HOME/bin:$PATH
  $ export DISPLAY=<pc_ip_address:0.0>
  ```
- Run the following commands to run the installer:

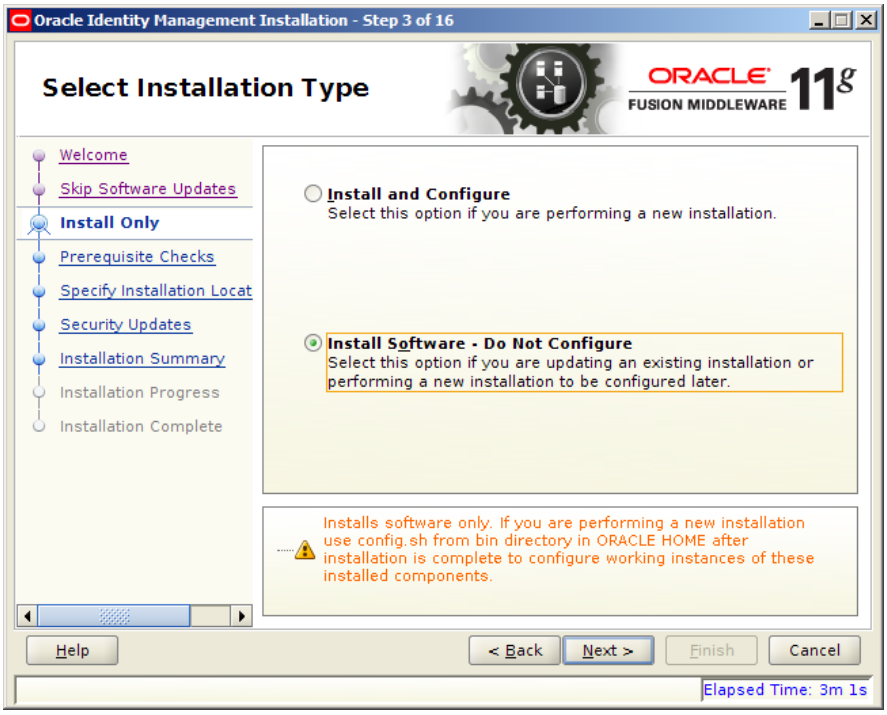
  Example:

  ```
  $ cd <INSTALL_DIR>/idm_11.1.1.9/Disk1
  $ ./runInstaller
  ```
- The Welcome window opens. Click **Next**.

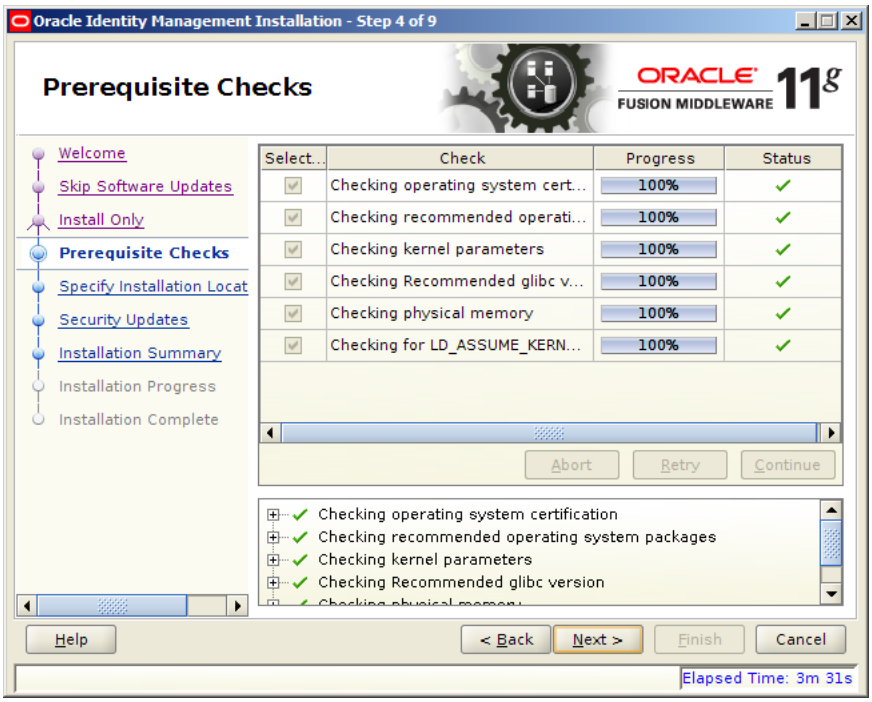
- The Install Software Updates window opens. Select **Skip Software Updates,** and click **Next**.



- The Select Installation Type window opens. Select **Install Software - Do Not Configure**, and click **Next**.



- The Prerequisite Checks window opens. Click **Next**.

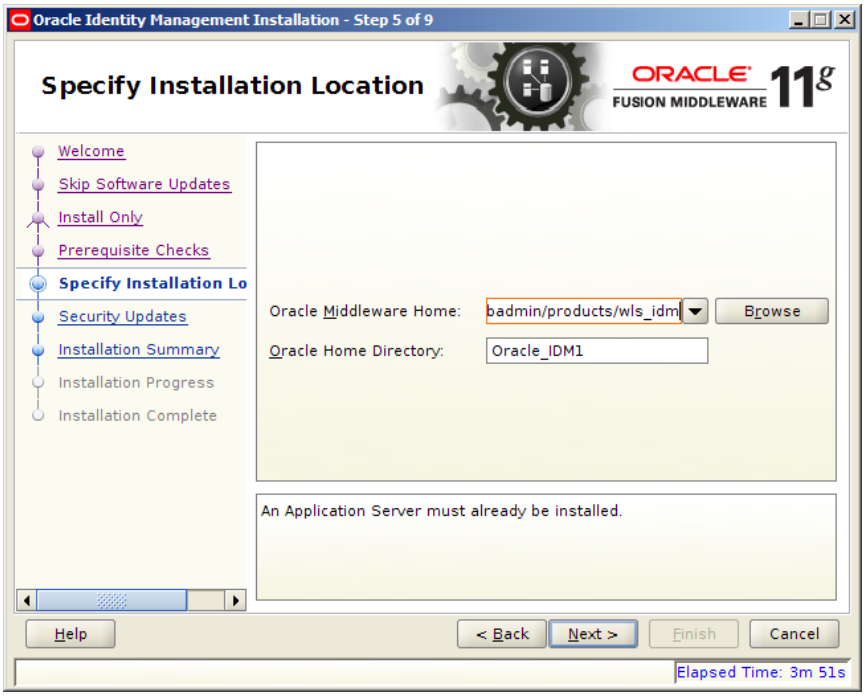


- The Specify Installation Location window opens. Provide the Oracle Middleware Home (WebLogic) for the OID install. Click **Next**.

  Example:

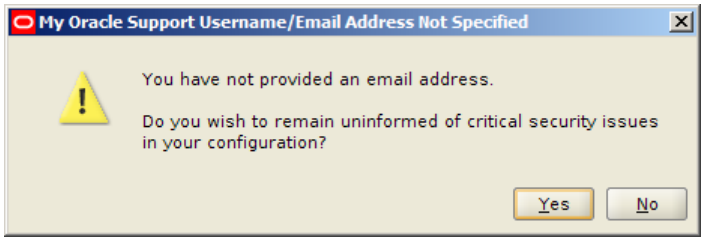
  `/u00/webadmin/products/wls_idm`

> **Note**: Oracle Home Directory can be Oracle_IDM1 on both IDM hosts.

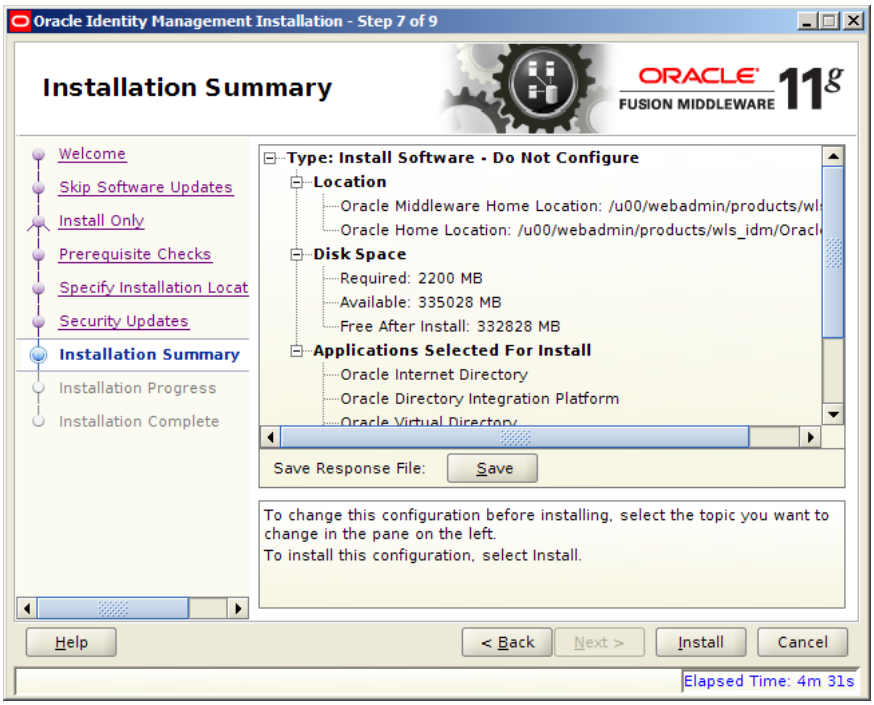


- The Specify Security Updates window opens. Uncheck the check box, and click **Next** .

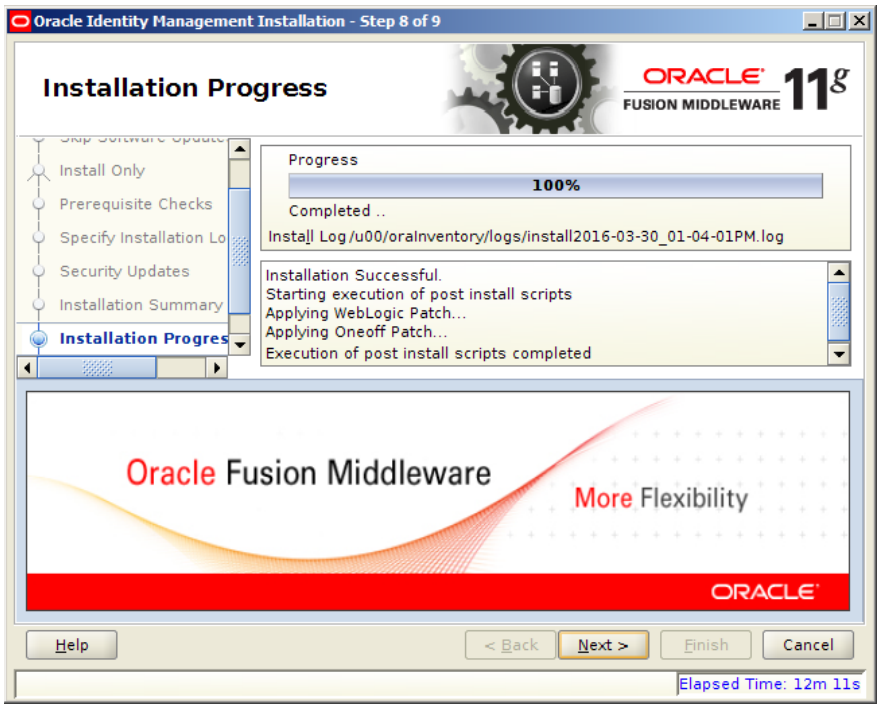
- The following warning displays if an email address is not provided. Click **Yes**.



- The Installation Summary window opens. Click **Install**.



- The Installation Progress window opens. Click **Finish**.

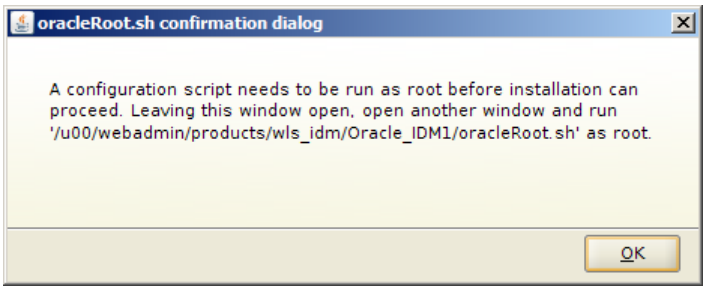


- A prompt to run a script as root.
  - Logon to the host in another window as root and run the following commands:

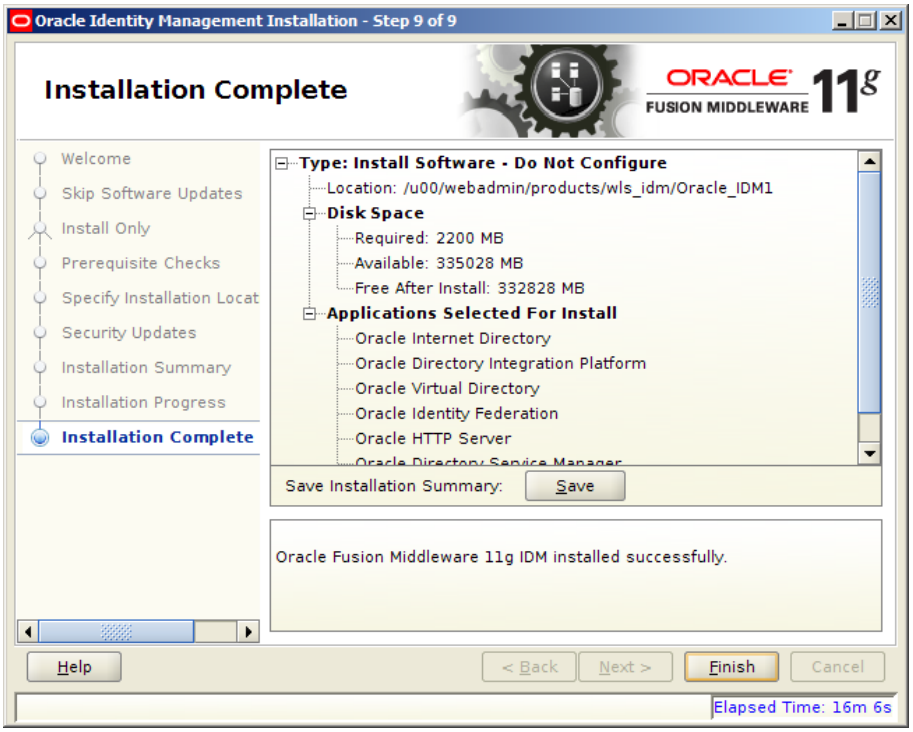
    Example:

    ```
    $ cd /u00/webadmin/products/wls_idm/Oracle_IDM1
    $ ./oracleRoot.sh
    ```

  - Click **OK**.



- The Installation Complete window opens. Click **Finish**.



- The installation is complete.

Backing up Installations

Perform the backup installations on both idmhost1 and idmhost2. The installations can be quickly restored if there is a failed configuration.

Example:

```
$ tar cvf IDM.tar /u00/webadmin/product/wls_idm
```

7

Configuring the Oracle Internet Directory in a Cluster

This chapter describes the configuration of the Oracle Internet Directory in a cluster.

Configuring IDM on idmhost1

Perform the following steps to configure IDM on idmhost1 only. (OID will be configured on idmhost2 using separate instructions.)

- Set the following variables by exporting them before running the domain configuration setup script :
  - JAVA_HOME
  - PATH
  - DISPLAY

  Example:

  ```
  $ export JAVA_HOME=/u00/webadmin/products/jdk_java
  $ export PATH=$JAVA_HOME/bin:$PATH
  $ export DISPLAY=<pc_ip_address:0.0>
  ```

- Navigate to the (WLS_IDM_HOME)/Oracle_IDM1/bin:

  Example:

  ```
  $ cd /u00/webadmin/products/wls_idm/Oracle_IDM1/bin
  ```

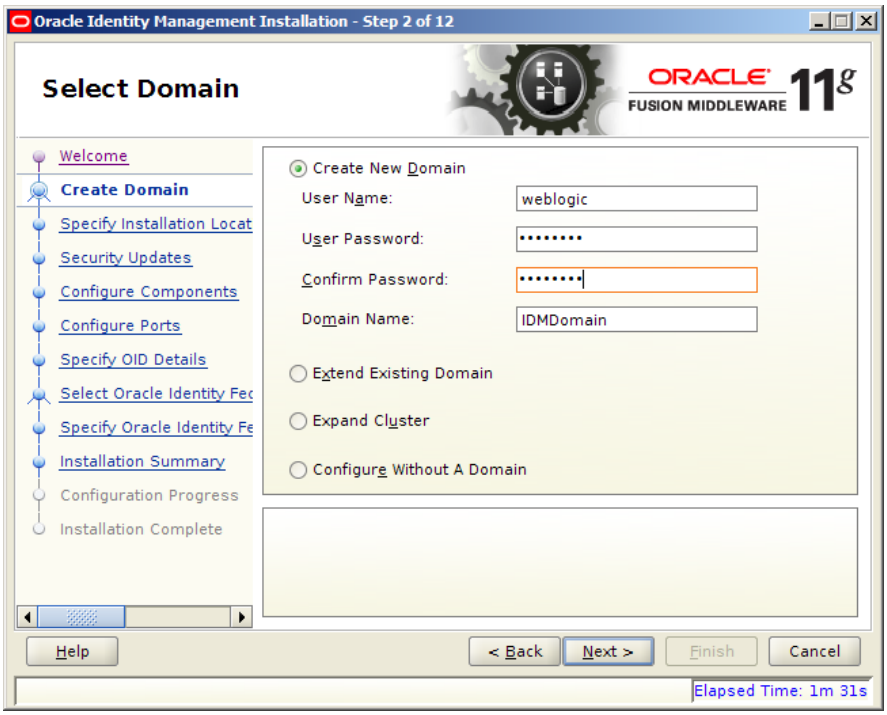
- Run the following command:

  Example:

  ```
  $ ./config.sh
  ```

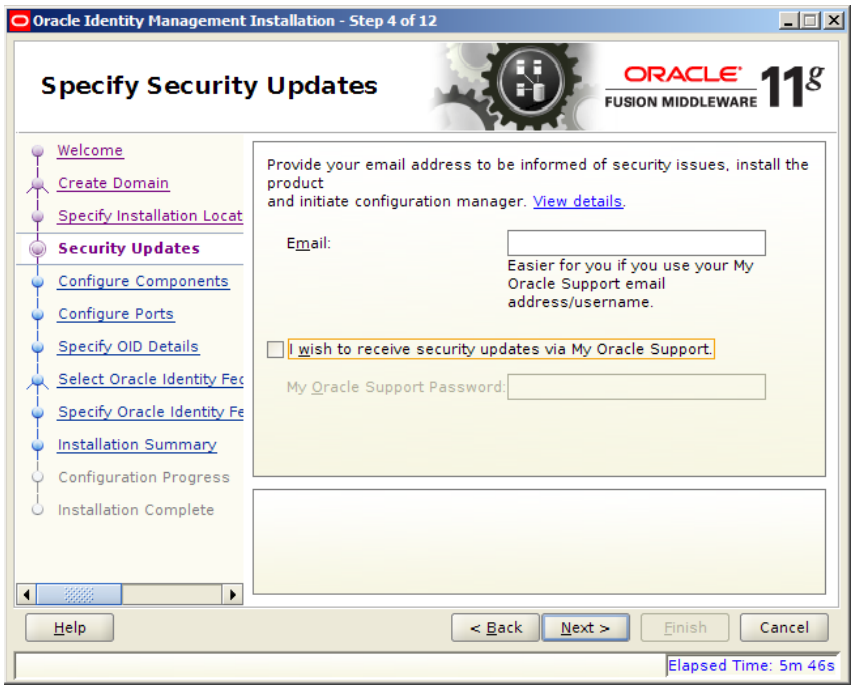
- The Welcome window opens. Click **Next**.

- The Select Domain window opens. Enter in the following and click **Next**.
  - Select **Create New Domain** and add the domain administration credentials.
  - User Name and Password for your WLS administrative user.
  - Domain name: IDMDomain

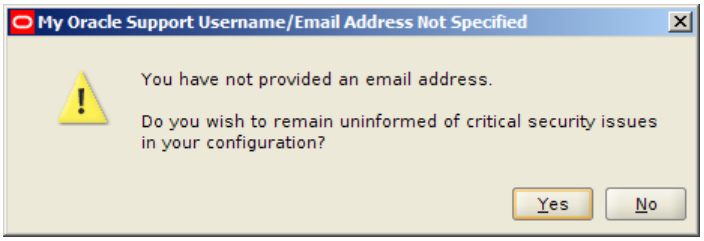


- The Specify Installation Location window opens. Update the following from the default values provided, and click **Next**.
  - Oracle Instance Location: /u00/webadmin/products/wls_idm/oidinst_1
  - Oracle Instance Name: oidinst_1.

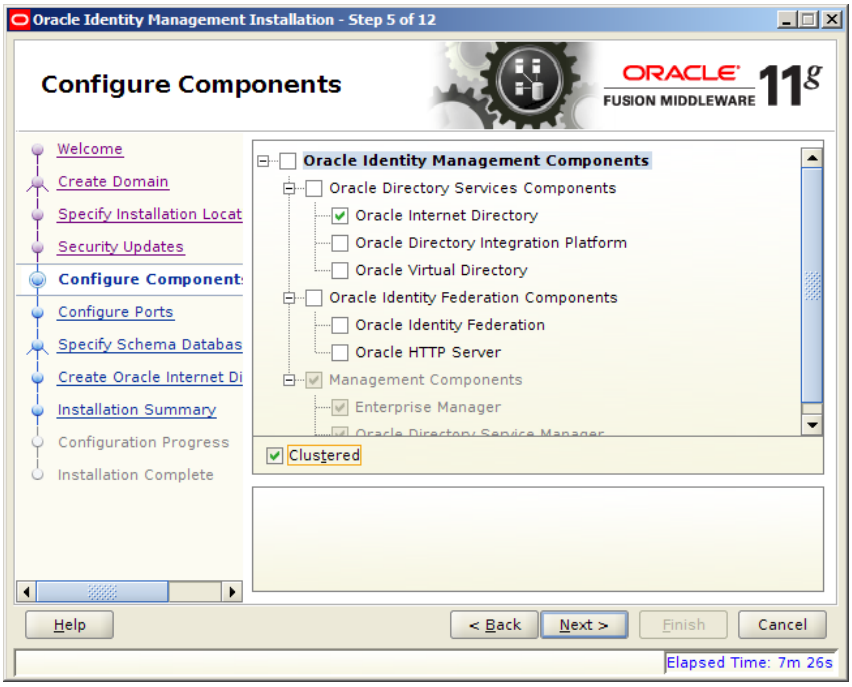
- The Specify Security Updates window opens. Uncheck the Checkbox and click **Next**.



- The following warning displays if an email address was not provided. Click Yes.



- The Configure Components window opens. Select the following items and click **Next**.
  - Oracle Interne Directory
  - Enterprise Manager
  - Oracle Directory Service Manager
  - Check the check box for Clustered

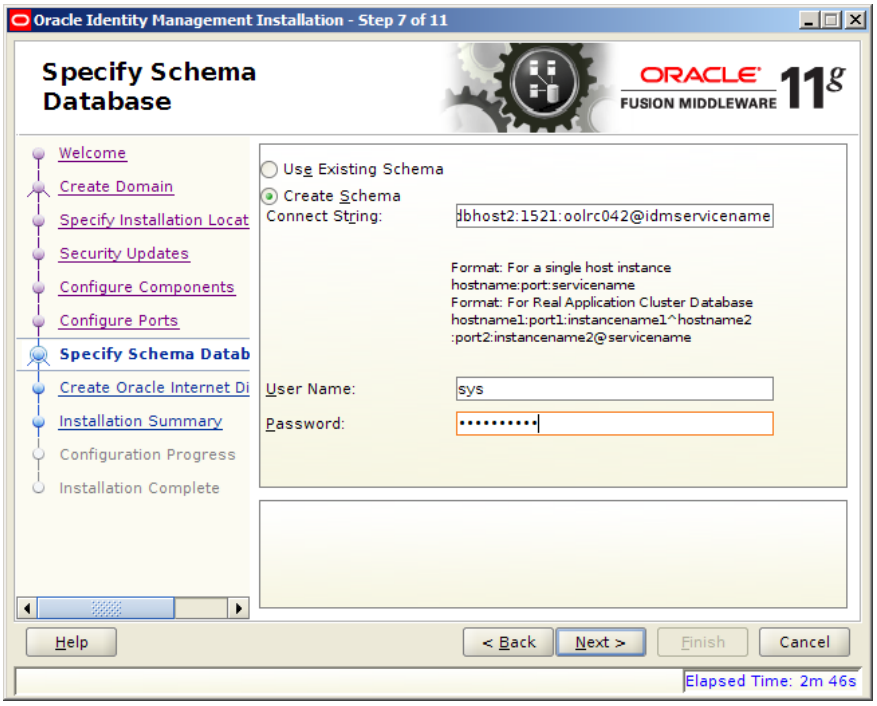


- The Configure Ports window opens.
  - Select the radio button – Specify Ports using Configuration file.
  - Navigate to and copy the sample staticports.ini from: <INSTALL_DIR>/idm_11.1.1.9/Disk1/stage/Response directory, to: /u00/webadmin/ports/
  - Rename it as staticports_idm.ini and modify the values as per Appendix I - Static ports for OID.
  - Click **Next**.

- The Specify Schema Database window opens.
  - Select the Create Schema Connect String
  - For RAC database use the connection string similar to below:

    Example:

    `dbhost1:1521:oolrc041^dbhost2:1521:oolrc042@idmservicename`
  - Click **Next**.



Additional Information on RAC:

The RAC (Real Application Cluster) consist of 2 DB host in a cluster and pointing to RAC instances.

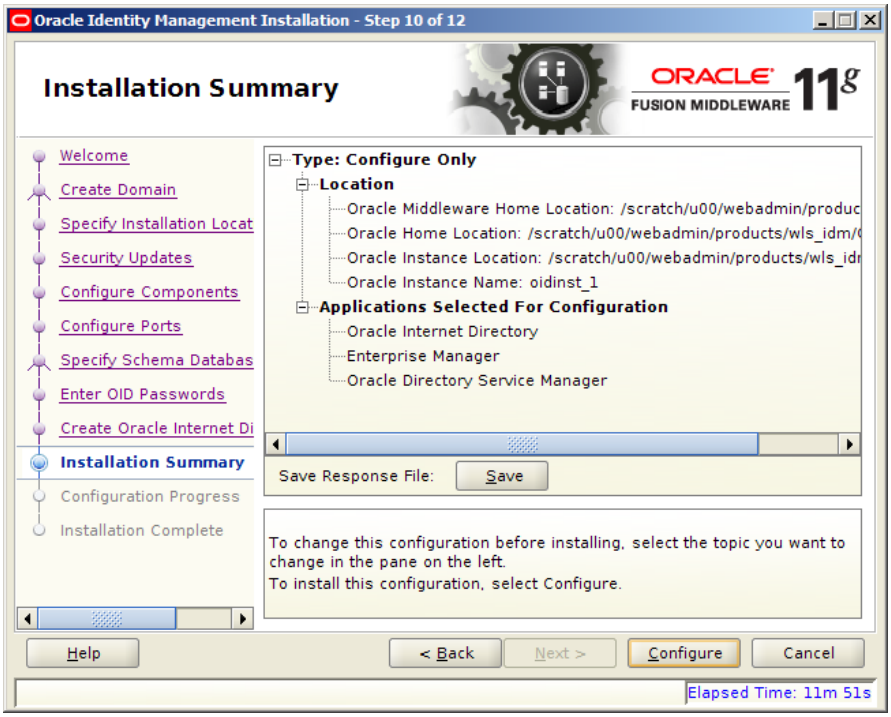
Oracle Clusterware provides a complete, integrated clusterware management solution on all Oracle Database platforms. This clusterware functionality provides all of the features required to manage your cluster database including node membership, group services, global resource management, and high availability functions. You can install Oracle Clusterware independently or as a prerequisite to the Oracle RAC installation process. Oracle Database features such as services use the underlying Oracle Clusterware mechanisms to provide their capabilities. Oracle Database also continues to support select third-party clusterware products on specified platforms.

Oracle Clusterware is designed for, and tightly integrated with, Oracle RAC. When you create an Oracle RAC database using any of the management tools, the database is registered with and managed by Oracle Clusterware, along with the other Oracle Database processes such as Virtual Internet Protocol (VIP) address, Global Services Daemon (GSD), the Oracle Notification Service (ONS), and the Oracle Net listeners. These resources are automatically started when Oracle Clusterware starts the node and automatically restarted if they fail. The Oracle Clusterware daemons run on each node.

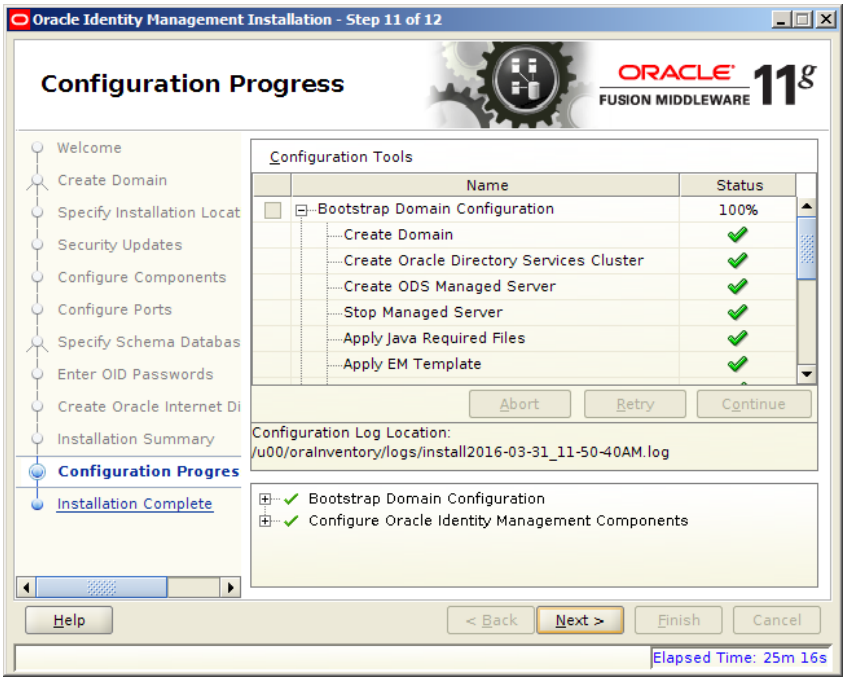
- The Enter OID Passwords window opens. Provide passwords to the ODS and ODSM schemas, and click **Next**.

- The Create Oracle Internet Directory window opens. Set the password for the OID superuser (cn=orcladmin), and click **Next**.

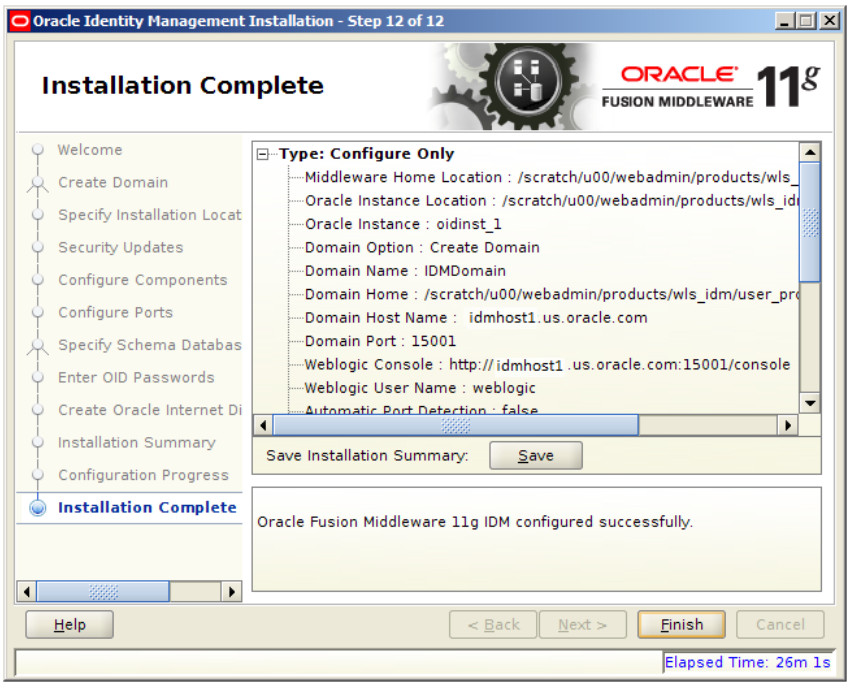
- The Installation Summary window opens. Click **Configure**.



- The Configuration Progress window opens. (This will take between 15 and 45 minutes to finish running.) Click **Next** when the button becomes enabled.



- The Installation Complete window opens.
  - Optionally save the Installation Summary for reference to Application URL's and installation specific information. The output from the installation summary should look like sample in Appendix II - Oracle Internet directory installation summary.
  - Click **Finish.**



- The installation is complete.

Create WebLogic boot.properties for OID WLS Domain on idmhost1

Create WebLogic boot.properties file with username and password so that the startup script does not prompt or require user input to start the admin server.

- Change directories to the admin servers security directory and create a boot.properites file.

```
$ cd
/scratch/u00/webadmin/config/domains/wls_iam/OAMDomain/servers/AdminServer
$ mkdir security
$ cd security
$ vi boot.properties

username=weblogic
password=<password>
```

- Start the WebLogic admin server if it is not running.

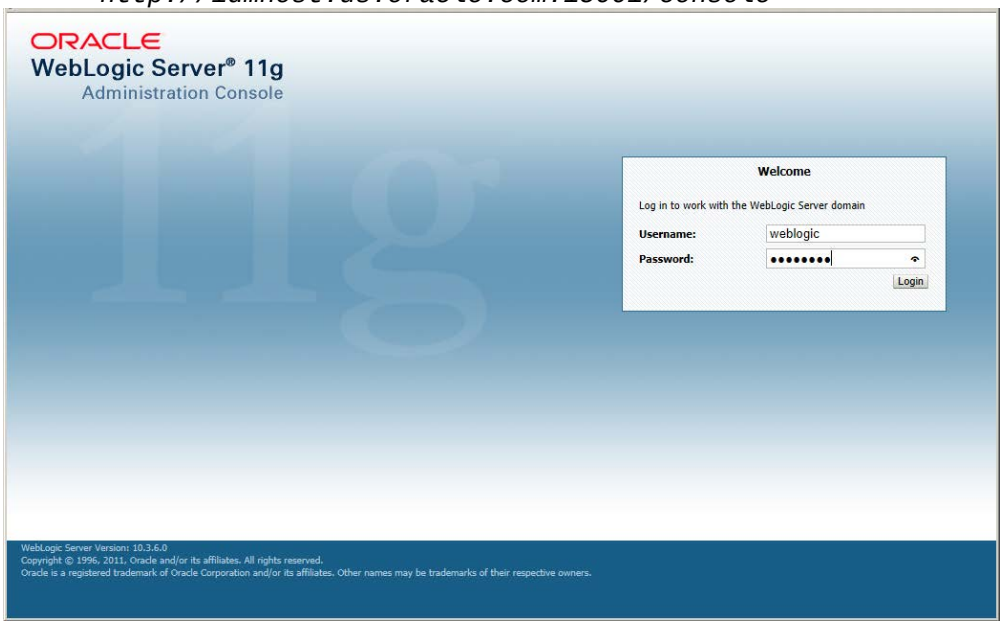
```
$ cd /scratch/u00/webadmin/config/domains/wls_iam/OAMDomain/bin
$ nohup ./startWebLogic.sh &
```

Update IDMDomain Listen Address on idmhost1

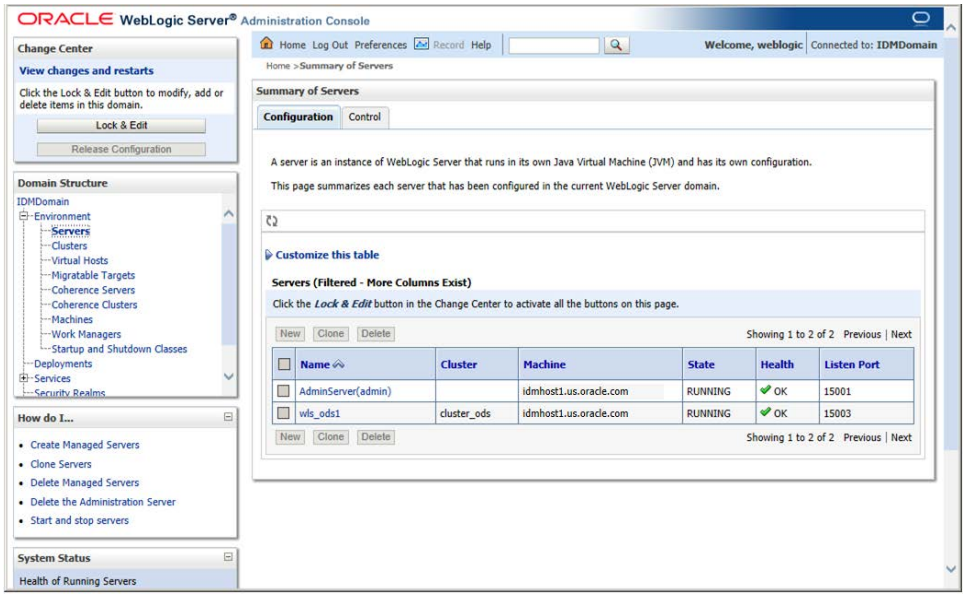
Perform the following steps to update IDMDomain listen address:

- Login to WebLogic Admin console by launching the following URL and using WebLogic admin user.

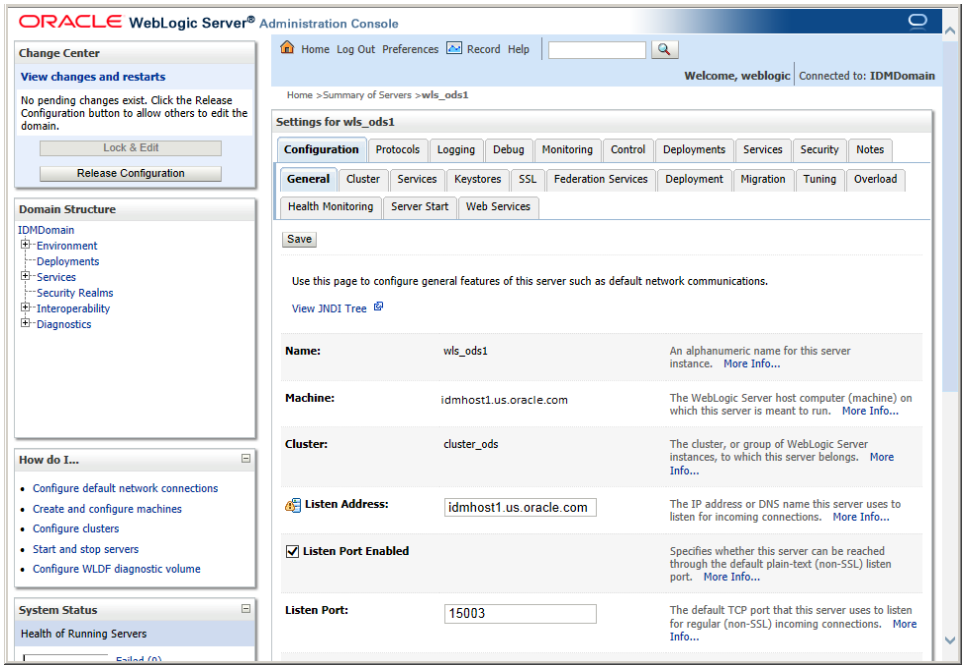
  http://idmhost.us.oracle.com:15001/console



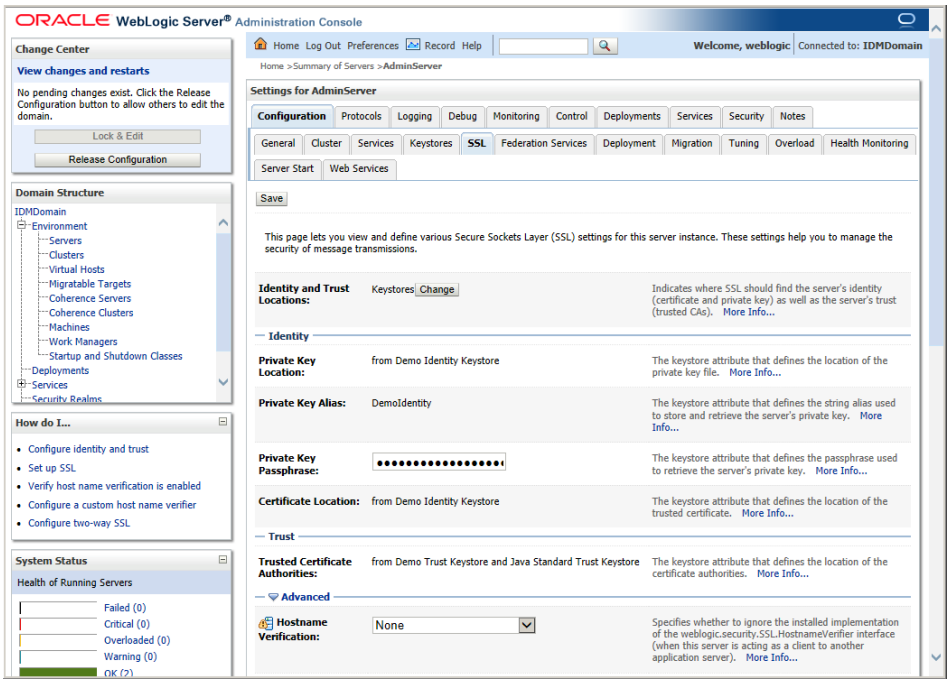
- Navigate to IDMDomain > Environment Servers.



- Click Lock & Edit and navigate to AdminServer > Configuration tab > General tab. Update the Listen Address to idmhost1.



- Navigate to SSL tab > Advanced section. Select None in the Hostname Verification field.



- Click Save and Activate Changes.
- Perform the same steps as for wls_ods1.
- Restart to complete the IDMDomain.

Configuring IDM on idmhost2

Perform the following steps to configure IDM on idmhost2 only.

- Set the following variables by exporting them before running the domain configuration setup script :
  - JAVA_HOME
  - PATH
  - DISPLAY

  Example:

  ```
  $ export JAVA_HOME=/u00/webadmin/products/jdk_java
  $ export PATH=$JAVA_HOME/bin:$PATH
  $ export DISPLAY=<pc_ip_address:0.0>
  ```

- Navigate to the (WLS_IDM_HOME)/Oracle_IDM1/bin:

  Example:

  ```
  $ cd /u00/webadmin/products/wls_idm/Oracle_IDM1/bin
  ```

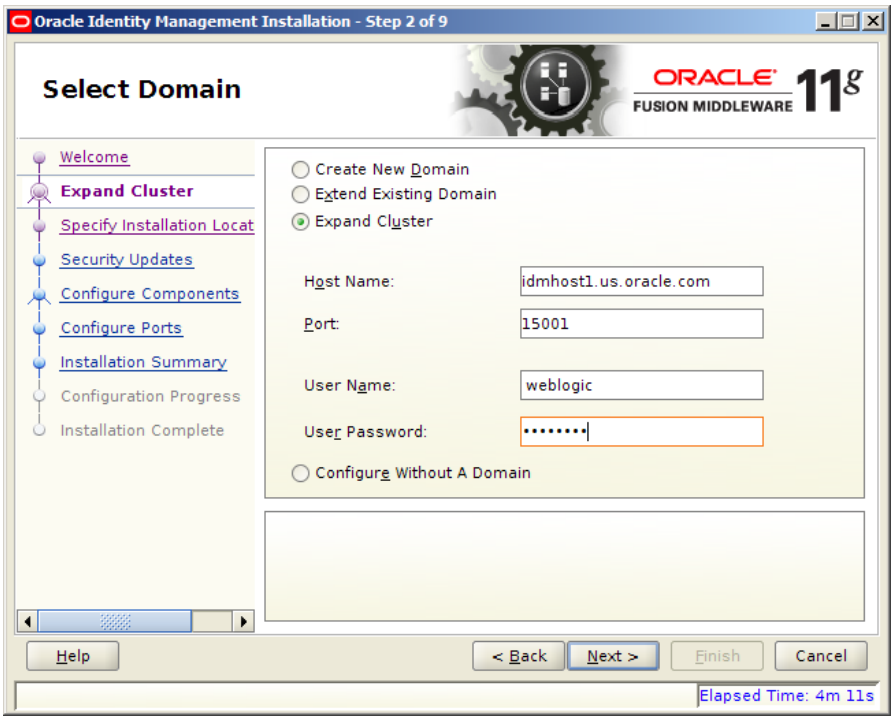
- Run the following command to start the WLS Configuration Wizard:

  Example:

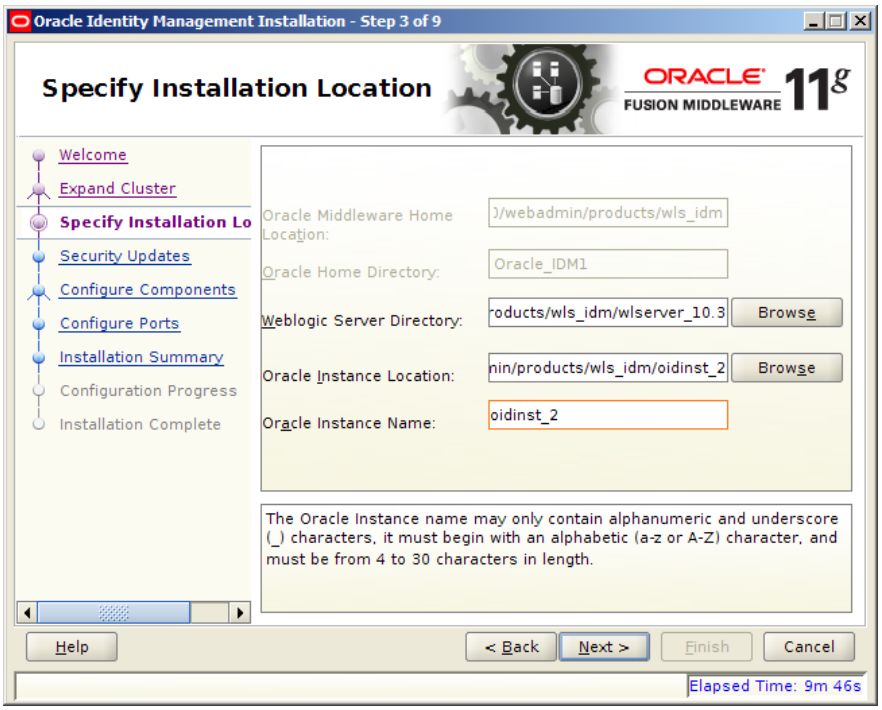
  ```
  $ ./config.sh
  ```

- The Welcome window opens. Click **Next**.

- The Select Domain window opens. Enter in the following and click **Next**.
  - Select Expand Cluster option
  - Enter in idmhost1 (idmhost1 is the master node in the cluster.)
  - User Name and Password for your WLS administrative user from idmhost1.

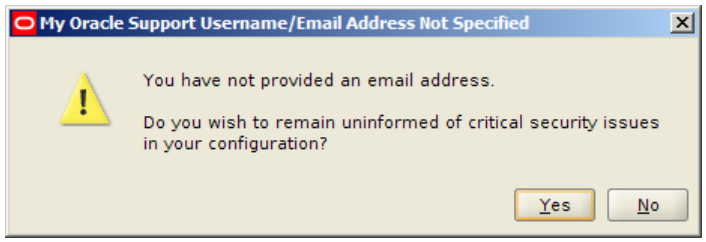


- The Specify Installation Location window opens. Update the following from the default values provided and click **Next**.
  - Oracle Instance Location: /u00/webadmin/products/wls_idm/oidinst_2
  - Oracle Instance Name: oidinst_2.

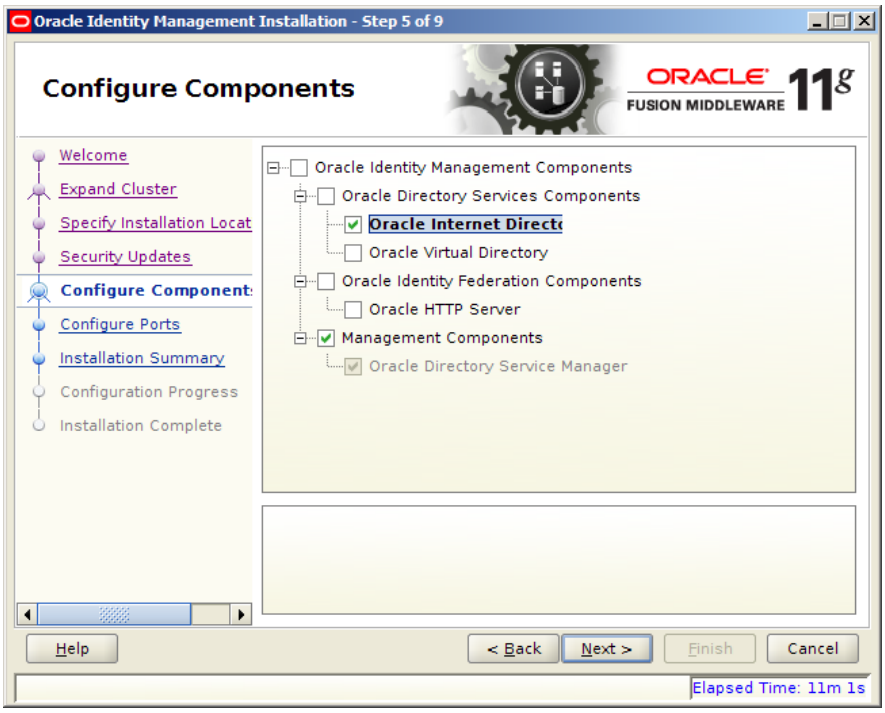


- The Specify Security Updates window opens. Uncheck the Checkbox and click **Next**.

- The following warning displays if an email address was not provided. Click Yes.



- The Configure Components window opens. Select the following items and click **Next**.
  - Oracle Interne Directory
  - Oracle Directory Service Manager



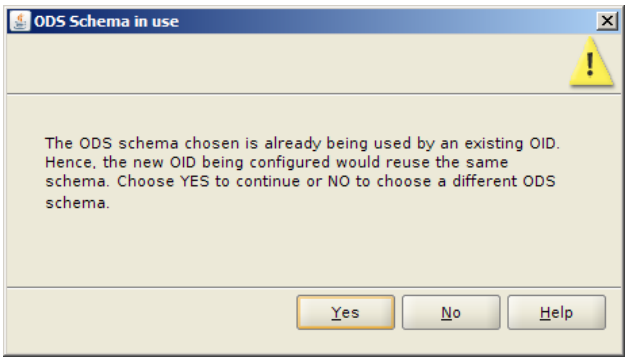
- The Configure Ports window opens.
  - Use the Radio button to select 'Specify Ports using Configuration file'
    - Copy the staticports_idm.ini
      From idmhost1: `/u00/webadmin/ports/`
      To idmhost2: `/u00/webadmin/ports/`

    - This will make sure the configuration files are exactly the same.
      Example: From command line on idmhost2
      ```
      $ mkdir ports
      $ scp webadmin@idmhost1:/u00/webadmin/ports/staticports_idm.ini
      /u00/webadmin/ports/staticports_idm.ini
      ```
- Click **Next**.

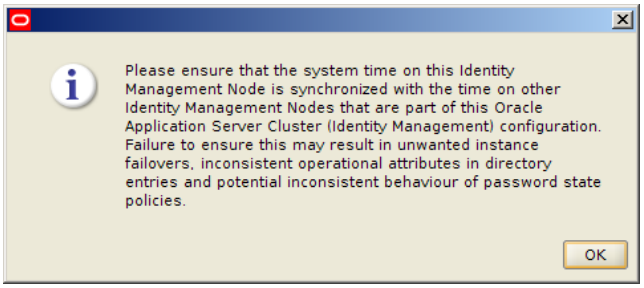
- The Specify Schema Database window opens.
  - Select the Use Existing Schema Connect String
  - For RAC database use the connection string similar to below:

    Example:
    `dbhost1:1521:oolrc041^dbhost2:1521:oolrc042@idmservicename`
  - Enter in the ODS schema password. (NOTE: This was created during steps for configuring idmhost1)
  - Click **Next**.

- A warning window opens. Click Yes.

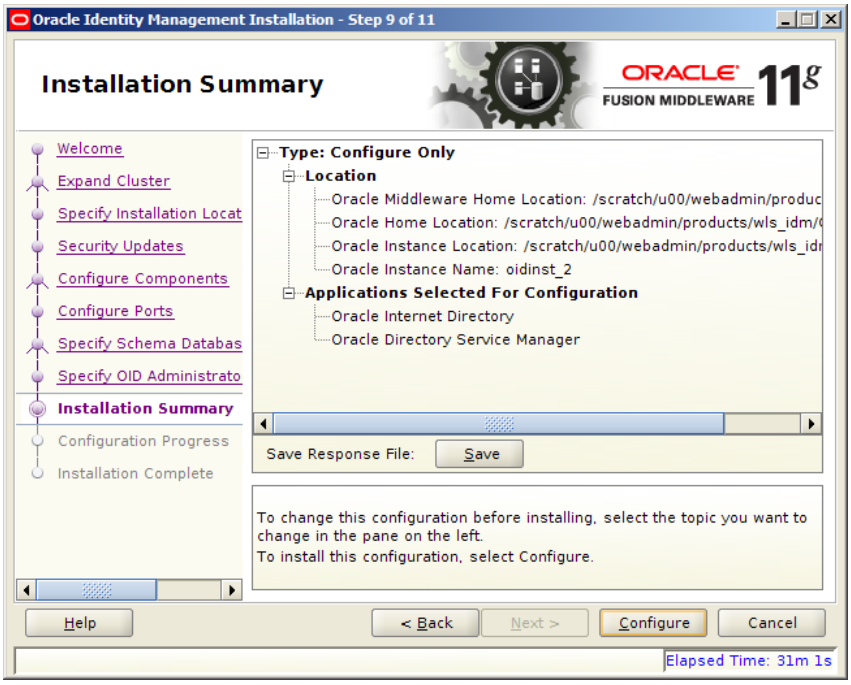


- A confirmation window opens. Click OK.

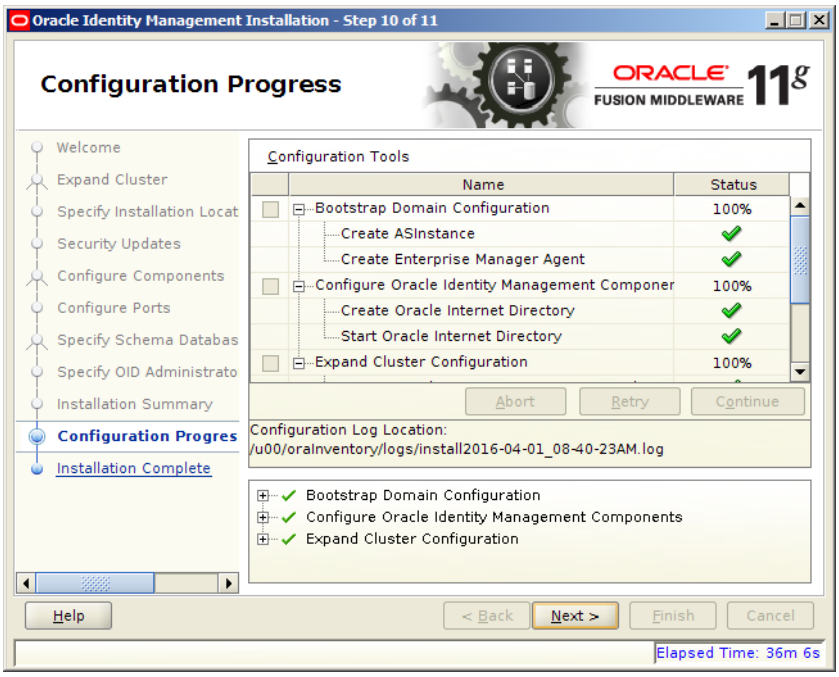


- The Specify OID Administrator Password window opens. Set the password for the OID superuser (cn=orcladmin) and click **Next**.

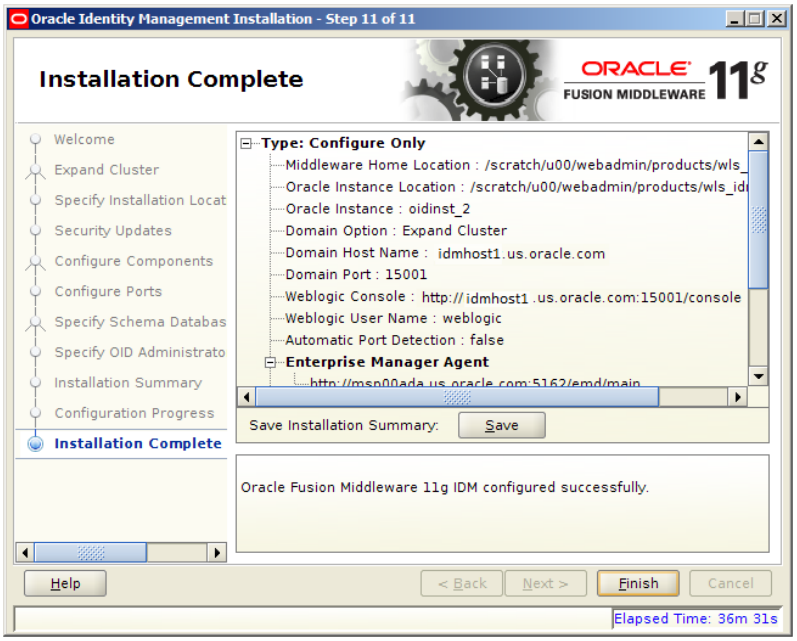
- The Installation Summary window opens. Click Configure.



- The Configuration Progress window opens. (This will take between 15 and 45 minutes to finish running.) Click **Next** when the button becomes enabled.



- The Installation Complete window opens.
  - Optionally save the Installation Summary for reference to Application URL's and installation specific information. The output from the installation summary should look like sample in Appendix III - Oracle Internet directory installation summary.
  - Click Finish



- The installation is complete.

Node Manager Configuration for OID on idmhost1 and idmhost2

Server instances in a WebLogic Server production environment are often distributed across multiple domains, machines, and geographic locations. Node Manager is a WebLogic Server utility that enables you to start, shut down, and restart Administration Server and Managed Server instances from a remote location.

A Node Manager process is not associated with a specific WebLogic domain but with a machine. You can use the same Node Manager process to control server instances in any WebLogic Server domain, as long as the server instances reside on the same machine as the Node Manager process. Node Manager must run on each computer that hosts WebLogic Server instances—whether Administration Server or Managed Server—that you want to control with Node Manager.

Perform the following steps configure the nodemanager on both idmhost1 and idmhost2:

- First start the nodemanager on idmhost2 using the startNodeManager.sh script (Located at: <IDM_WEBLOGIC_HOME>/wlserver_10.3/server/bin) so that it creates the nodemanager.properties file in the following location: `<IDM_WEBLOGIC_HOME>/wlserver_10.3/common/nodemanager`

  NOTE: This step is not needed for idmhost1 since it should already have been started automatically during the OID configuration process.

- On both idmhost1 and idmhost2 perform the following steps:
  - Stop the nodemanager if already running by checking the port.

    Example:

    ```
    $ netstat -nap | grep 5560
    (Not all processes could be identified, non-owned process info will not
    be shown, you would have to be root to see it all.)
    tcp 0 0 0.0.0.0:5560 0.0.0.0:* LISTEN 16120/java
    $ kill -9 16120
    ```

  - Navigate to <IDM_WEBLOGIC_HOME>/wlserver_10.3/common/nodemanager.
  - Make a backup of the nodemanager.properties

    Example:

    ```
    $ cp -rp nodemanager.properties nodemanager.properties_ORIG
    ```

  - Update the values as per Appendix III - Node manager setting for IDM_WEBLOGIC_HOME.
  - Restart the nodemanager using the startNodeManager.sh script located at: <IDM_WEBLOGIC_HOME>/wlserver_10.3/server/bin

    Example:

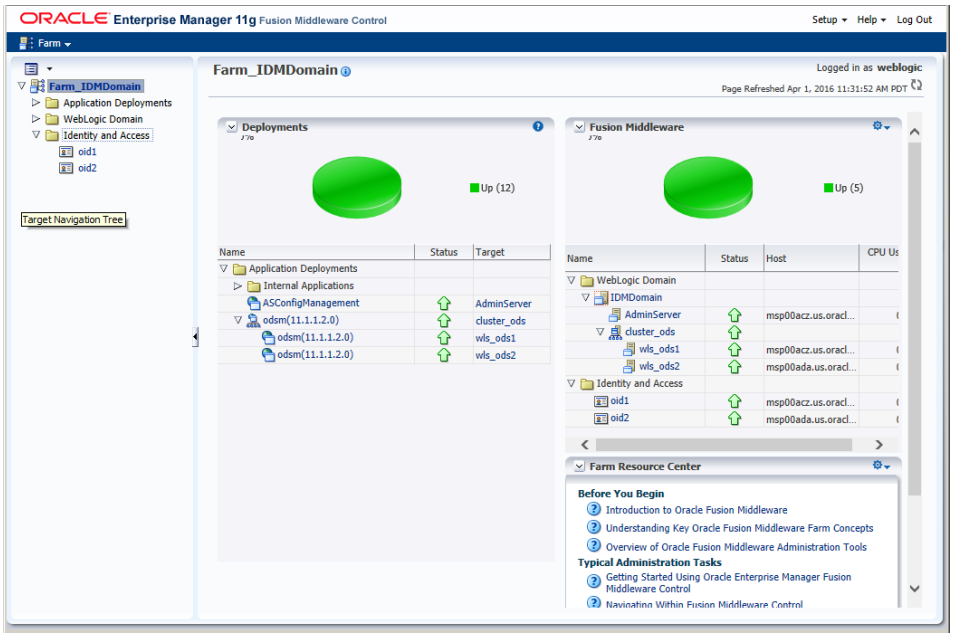
    ```
    $ nohup ./startNodeManager.sh &
    ```

Verification – OID on idmhost2 is Registered with Enterprise Manager

This section describes how to validate that OID on idmhost2 is registered with EM on idmhost1.

- Log onto the Enterprise Manager for OID on idmhost1: (http://idmhost1.us.oracle.com:15001/em)
- In the navigation Pane on the left hand side of window navigate – click on Identity and Access

- Validate that oid1 and oid2 are listed.



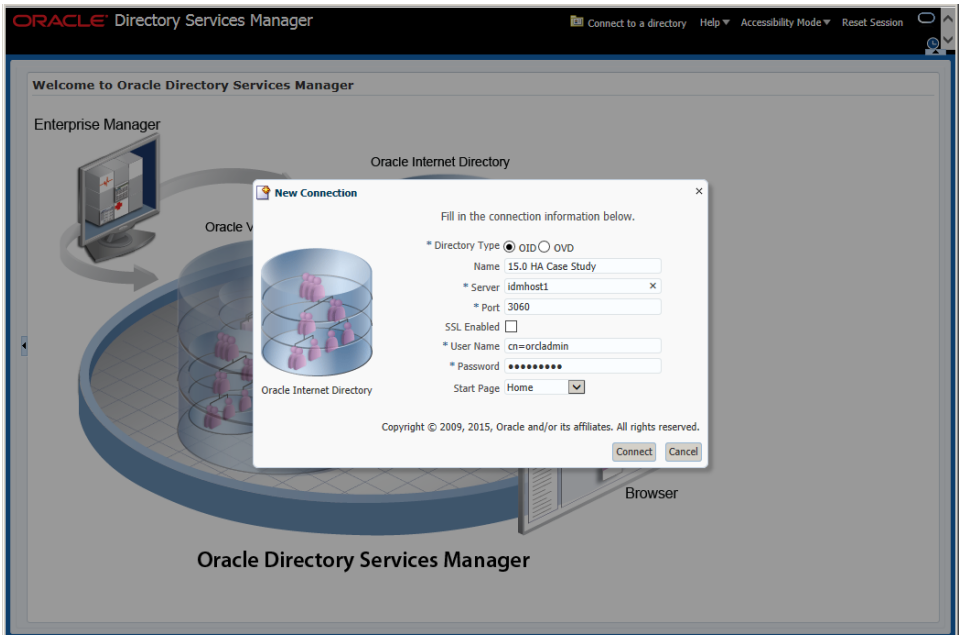
Verification – Installation of ODSM

This section describes how to validate that ODSM was installed correctly.

Run the validation steps for the following URLS:

http://idmhost1.us.oracle.com:15003/odsm/faces/odsm.jspx
http://idmhost2.us.oracle.com:15003/odsm/faces/odsm.jspx
http://idmhost-vip.us.oracle.com:15003/odsm/faces/odsm.jspx

- After Launching the ODSM application URL - Create connection and Log onto ODSM.



- If the connection and logon are successful the following window will be displayed.

9

Seed OID with Retail Specific Entries

This section describes the SEED OID with data for the applications using ldif scripts.

Most of the applications that are being installed contain ldif scripts as a part of their distribution. Several of the applications are packaged with the same set of ldif scripts and the OBIEE ldif scripts are not packaged with any of the applications. Before getting started with seeding OID – perform the following tasks to get the appropriate ldif scripts downloaded to a common staing directory on idmhost1.

- Create a staging directories for the ldif scripts on idmhost1 using the following as an example.

  ```
  $ mkdir -p /u00/webadmin/media/ldif_scripts/15.0/rpm_ldifs
  $ mkdir -p /u00/webadmin/media/ldif_scripts/15.0/obiee_ldifs
  $ mkdir -p /u00/webadmin/media/ldif_scripts/15.0/enterprise_ldifs
  $ mkdir -p /u00/webadmin/media/ldif_scripts/15.0/sim_ldifs
  ```

- From the RPM application distribution (rpm15application.zip/rpm/application/rpm/ldif/) copy the ldif scripts to the following location on idmhost1:

  `/u00/webadmin/media/ldif_scripts/15.0/rpm_ldifs`

- From the SIM application distribution (sim15-application.zip/sim/application/sim15/ldap/sim-ldap.zip/) copy the ldif scripts to the following location on idmhost1:

  `/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs`

  > **NOTE**: There are multiple sets of files with same name – they are similar subsets for designed for different types of SIM users. Pick one set or combine them as desired. Make sure to get at leas one of each.

- From the REIM application distribution (reim15application.zip/reim/application/reim/ldif/) copy the ldif scripts to the following location on idmhost1:

  `/u00/webadmin/media/ldif_scripts/15.0/enterprise_ldifs`

- For the creation of object classes prerequisite - use the sample ldif text in Appendix VII – LDIF Files – under the objectclasses_ldifs section to create ldif files with the names as they appear in the appendix. Once created place them in the following location on idmhost1:

  `/u00/webadmin/media/ldif_scripts/15.0/ obiee_ldifs`

  > **NOTE**: ldif files are are text files with an extension of .ldif

- For OBIEE use the sample ldif text in Appendix VII – LDIF Files – under the obiee_ldifs section to create ldif files with the names as they appear in the appendix. Once created place them in the following location on idmhost1:

  `/u00/webadmin/media/ldif_scripts/15.0/obiee_ldifs`

  > **NOTE**: ldif files are are text files with an extension of .ldif

- For the user ID retail.user that is used as a common user for a number off applications in this document - Use the sample ldif text in Appendix VII – LDIF Files – under the retail.user_ldifs section to create ldif files with the names as they appear in the appendix. Once created place them in the following location on idmhost1:

  `/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs`

  NOTE: ldif files are are text files with an extension of .ldif

- When finished validate that the ldif files exist in the directories as intended by checking them against the examples below. It is important that this is done correctly so that the file structure is in alignment with examples provided in the next set of steps to run the ldif scripts that seed OID.

  rpm_ldifs:

  ```
  $ ls /u00/webadmin/media/ldif_scripts/15.0/rpm_ldifs
  RPM_Group.ldif
  RPM_Users.ldif
  ```

  obiee_ldifs:

  ```
  $ ls /u00/webadmin/media/ldif_scripts/15.0/obiee_ldifs
  retailuser_objectclasses.ldif
  OBIEE_SSO_groups.ldif
  OBIEE_SSO_Users.ldif
  ```

  enterprise_ldifs:

  ```
  $ ls /u00/webadmin/media/ldif_scripts/15.0/enterprise_ldifs
  RGBU-oid-create-groups.ldif
  RGBU-oid-create-users.ldif
  RGBU-oid-delete-groups.ldif
  RGBU-oid-delete-users.ldif
  ```

  sim_ldifs:

  ```
  $ ls /u00/webadmin/media/ldif_scripts/15.0/sim_ldifs
  retail.user.ldif
  sim_add_company.ldif
  sim_add_containers.ldif
  sim_data_groups.ldif
  sim_data_roles.ldif
  sim_data_stores.ldif
  sim_data_user_groups.ldif
  sim_data_users.ldif
  sim_data_users_roles.ldif
  sim_objectclasses.ldif
  ```

On idmhost1 perform the following steps to seed OID using the ldif scripts:

- Set environment variables

  Example:

  ```
  export oid_host=idmhost1
  export oid_port=3060
  export oid_pwd=<password>
  export ORACLE_HOME=/u00/webadmin/products/wls_idm/Oracle_IDM1
  export PATH=$ORACLE_HOME/bin:$PATH
  ```

- Run the rpm_ldif scripts that will seed OID with the objects required for RPM by running the commands below.

  NOTE: Running RPM scripts first because they contain the creation of the retailUser object class which is a pre-requisite to running subsequent ldif scripts

```
$ ldapadd -o
/u00/webadmin/media/ldif_scripts/15.0/rpm_ldifs/RPM_Group_error -v -c -h
idmhost1.us.oracle.com -p 3060 -w oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/rpm_ldifs/RPM_Group.ldif
```

```
$ ldapadd -o /u00/webadmin/media/ldif_scripts/15.0/rpm_ldifs/RPM_Users_error -v -c -h
idmhost1.us.oracle.com -p 3060 -w oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/rpm_ldifs/RPM_Users.ldif
```

- Run the obiee_ldifs scripts that will seed OID with the objects required for Operational Insights (analytics) by running the commands below.

```
$ ldapadd -o
/u00/webadmin/media/ldif_scripts/15.0/obiee_ldifs/retailuser_objectclasses
_error -v -c -h idmhost1.us.oracle.com -p 3060 -w oracle10g -D
cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/obiee_ldifs/retailuser_objectclasses
.ldif
```

```
$ ldapadd -o
/u00/webadmin/media/ldif_scripts/15.0/obiee_ldifs/OBIEE_SSO_groups_error.l
dif -v -c -h msp00acz.us.oracle.com -p 3060 -w oracle10g -D cn=orcladmin -
f  /u00/webadmin/media/ldif_scripts/15.0/obiee_ldifs/OBIEE_SSO_groups.ldif
```

```
$ ldapadd -o
/u00/webadmin/media/ldif_scripts/15.0/obiee_ldifs/OBIEE_SSO_Users_error.ld
if -v -c -h msp00acz.us.oracle.com -p 3060 -w oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/obiee_ldifs/OBIEE_SSO_Users.ldif
```

- Run the enterprise_ldifs scripts that will seed OID with the objects required for application users and groups by running the commands below.

```
$ ldapadd -o /u00/webadmin/media/ldif_scripts/15.0/enterprise_ldifs/RGBU-
oid-create-groups_error -v -c -h msp00acz.us.oracle.com -p 3060 -w
oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/enterprise_ldifs/RGBU-oid-create-
groups.ldif
```

```
$ ldapadd -o /u00/webadmin/media/ldif_scripts/15.0/enterprise_ldifs/RGBU-
oid-create-users_error -v -c -h msp00acz.us.oracle.com -p 3060 -w
oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/enterprise_ldifs/RGBU-oid-create-
users.ldif
```

- Run the enterprise_ldifs scripts that will seed OID with the objects required for the SIM application by running the commands below.

```
$ ldapadd -o
/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_objectclasses_error -v
-c -h msp00acz.us.oracle.com -p 3060 -w oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_objectclasses.ldif
```

```
$ ldapadd -o
/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_add_company_error -v -
c -h msp00acz.us.oracle.com -p 3060 -w oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_add_company.ldif
```

```
$ ldapadd -o
/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_add_containers_error -
v -c -h msp00acz.us.oracle.com -p 3060 -w oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_add_containers.ldif
```

```
$ ldapadd -o
/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_data_groups_error -v -c -h
msp00acz.us.oracle.com -p 3060 -w oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_data_groups.ldif

$ ldapadd -o /u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_data_roles_error -v -c -
h msp00acz.us.oracle.com -p 3060 -w oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_data_roles.ldif

$ ldapadd -o /u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_data_stores_error -v -c
-h msp00acz.us.oracle.com -p 3060 -w oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_data_stores.ldif

$ ldapadd -o /u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_data_user_groups_error -
v -c -h msp00acz.us.oracle.com -p 3060 -w oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_data_user_groups.ldif

$ ldapadd -o /u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_data_users_error -v -c -
h msp00acz.us.oracle.com -p 3060 -w oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_data_users.ldif

$ ldapadd -o /u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/retail.user_error -v -c -h
msp00acz.us.oracle.com -p 3060 -w oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/retail.user.ldif

$ ldapadd -o /u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_data_user_roles_error -v
-c -h msp00acz.us.oracle.com -p 3060 -w oracle10g -D cn=orcladmin -f
/u00/webadmin/media/ldif_scripts/15.0/sim_ldifs/sim_data_user_roles.ldif
```

10

Installing Oracle Access Manager

This chapter describes the steps to install the Oracle Access Manager.

The following hosts will have OAM 11.1.2.3 installed on them:

- idmhost1.us.oracle.com
- idmhost2.us.oracle.com

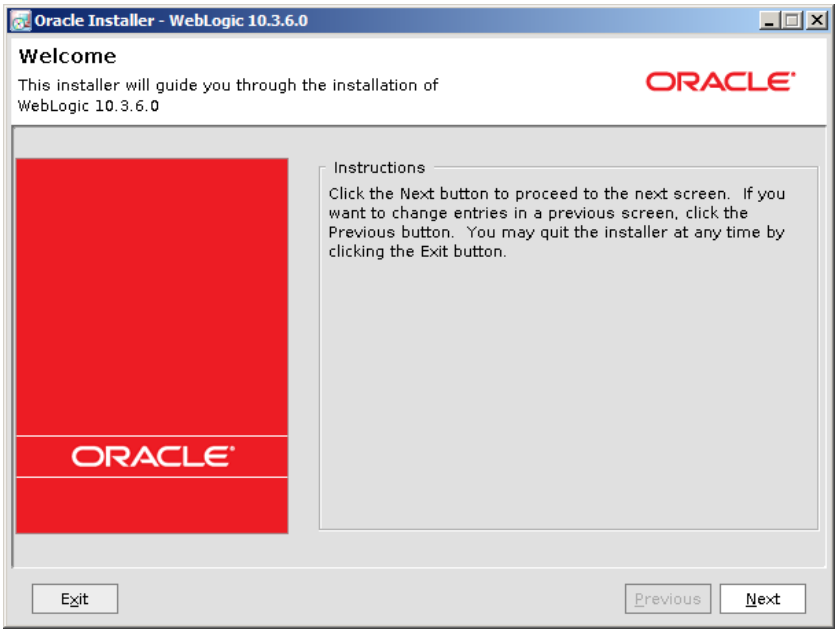
Install WebLogic Server 10.3.6 on idmhost1 and idmhost2

Perform the following steps to install a WebLogic 10.3.6 server on idmhost1 and idmhost2:

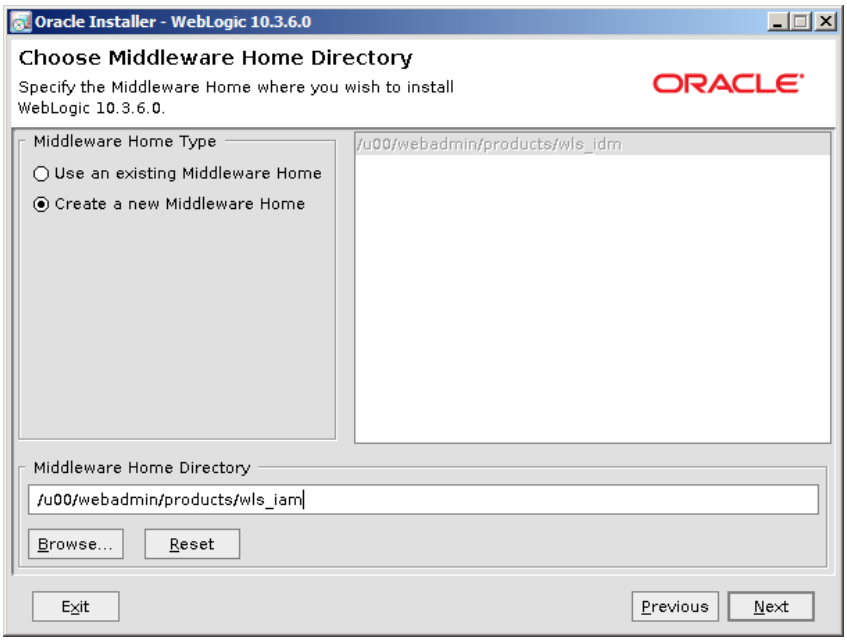
- Download software installation for WebLogic and place it in an installation staging directory (<INSTALL_DIR>/WLS_10.3.6) on the Linux host.
- Set the following variables by exporting them before running the installer:
  - JAVA_HOME
  - PATH
  - DISPLAY

  Example:
  ```
  $ export JAVA_HOME=/u00/webadmin/products/jdk_java
  $ export PATH=$JAVA_HOME/bin:$PATH
  $ export DISPLAY=<pc_ip_address:0.0>
  ```
- Run the following commands to run the installer:

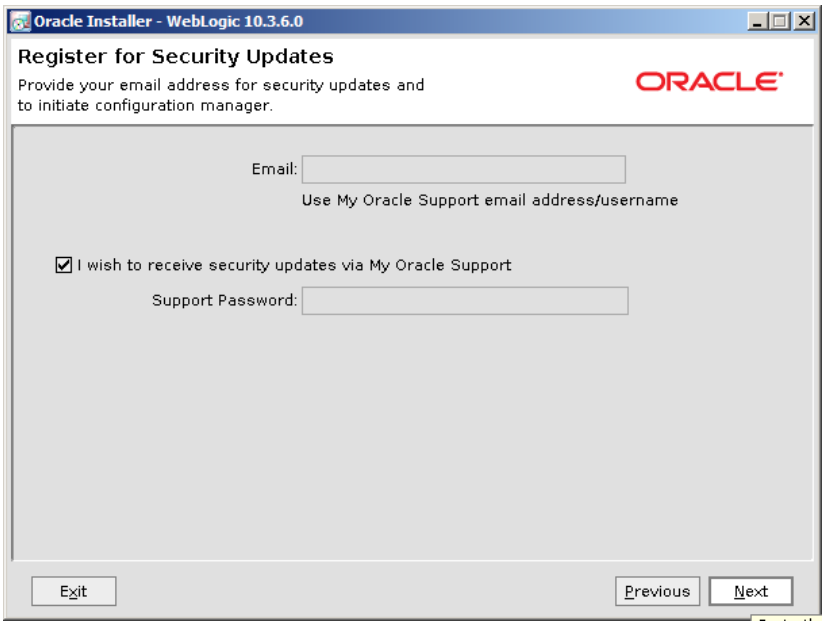
  Example:
  ```
  $ cd <INSTALL_DIR>/WLS_10.3.6
  $ java -jar ./wls1036_generic.jar
  ```
- The Welcome window of the WebLogic 10.3.6 Installer displays. Click **Next**.



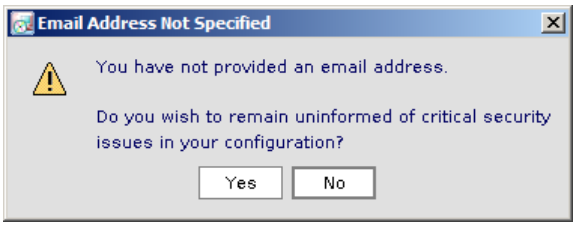
- The Choose Middleware Home Directory window opens. Enter the location for the OAM WEBLOGIC_HOME directory to be created in and click **Next**.

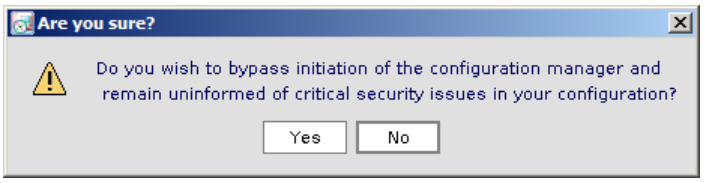


- The Email Registration window opens. Make sure the check box is selected, and click **Next**.

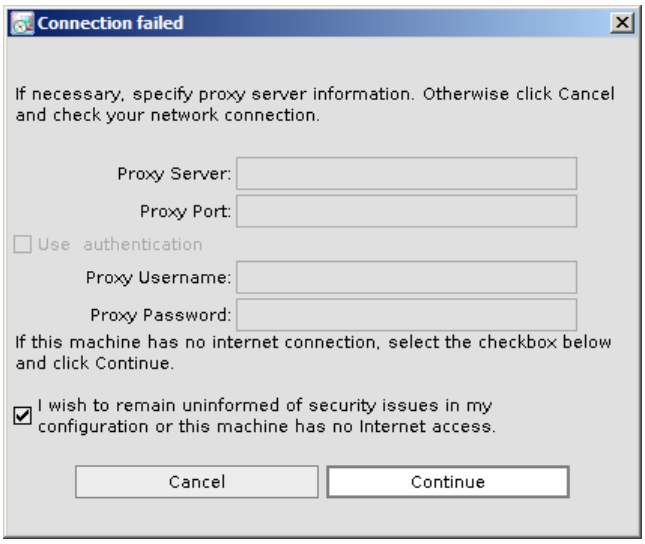


- Confirm the following 2 prompts by clicking **Yes**.

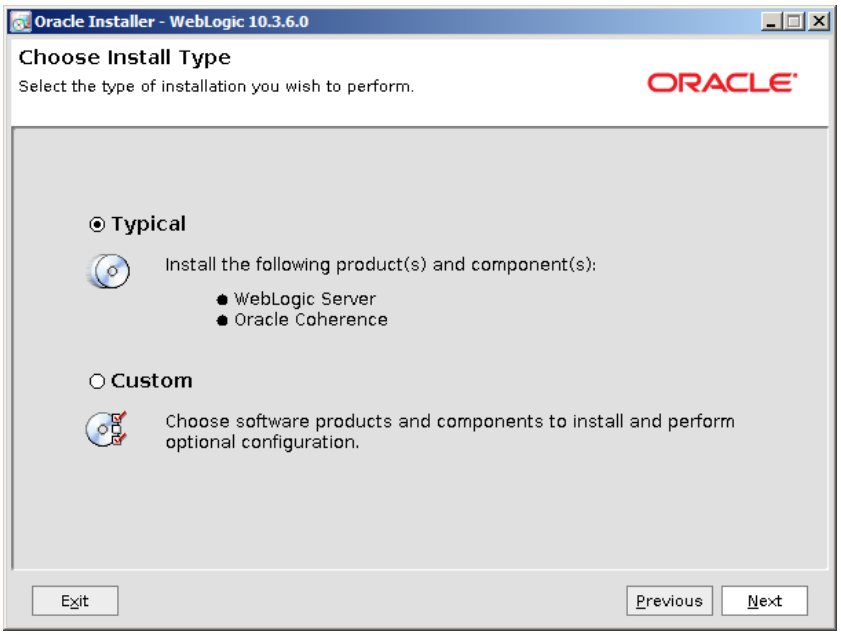




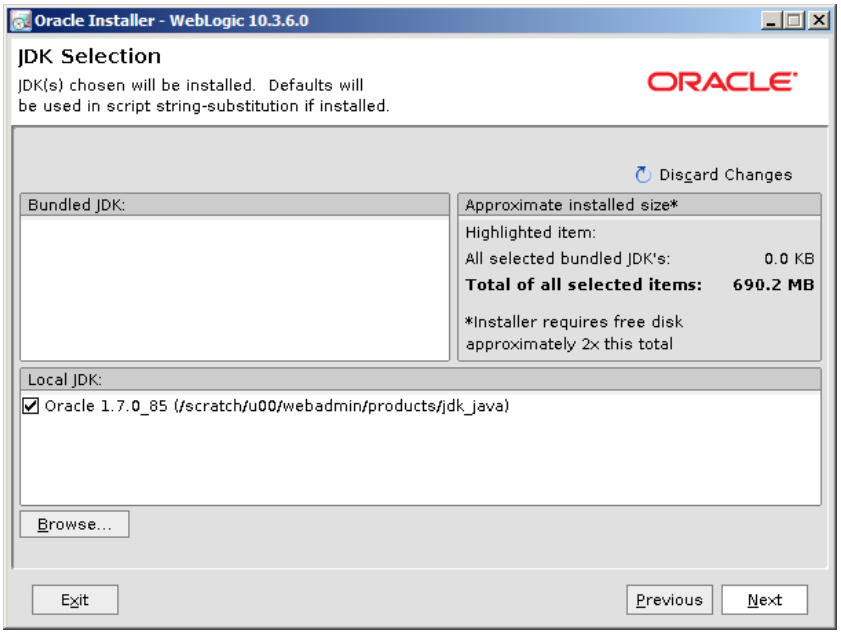
- The Connection Failed warning window opens. Click **Continue**.



- The Choose Install Type window opens. Select **Typical** and click **Next**.

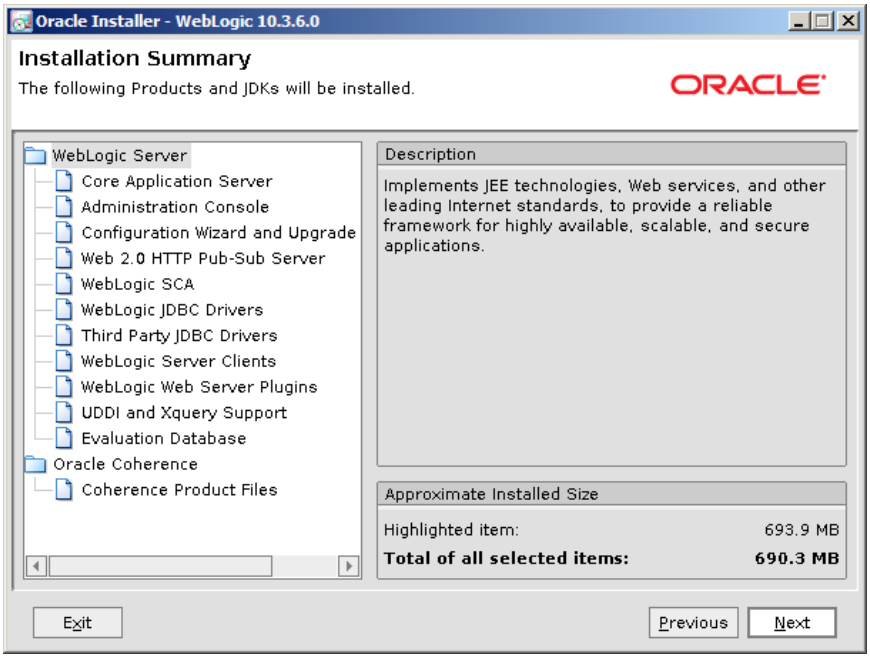


- The JDK Selection window opens. By default, it will select the JDK in your JAVA_HOME setting. Ensure the JAVA_HOME points to JDK 1.7.0+ and click **Next**.

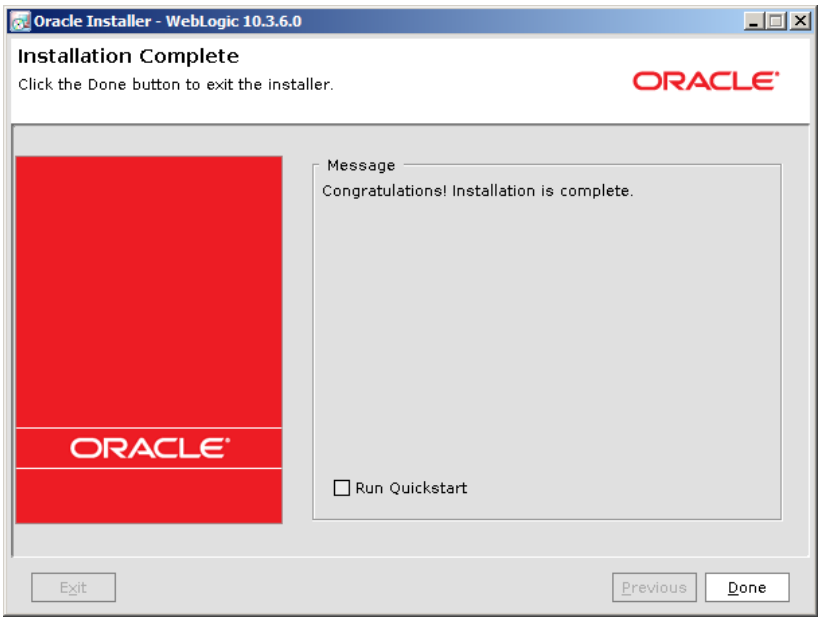


- The Choose Product Installation Directories window opens. Keep the defaults. Click **Next**.

- The Installation Summary window opens. Click **Next**. The product install begins.



- Once finished, the Installation Complete window opens. Un-check the Run Quickstart check box and click **Done**.



- The installation is complete.

Install Oracle Access Manager Software on idmhost1 and idmhost2

Perform the following steps to install Oracle Access Manager (OAM) 11.1.2.3 on idmhost1 and idmhost2:

- Download software installation for OAM 1.1.2.3 and place it in an installation staging directory on the Linux host and extract the contents of the zip files. <INSTALL_DIR>/OAM_11.1.2.3.

- Set the following variables by exporting them before running the installer:
  - JAVA_HOME
  - PATH
  - DISPLAY

  Example:

  ```
  $ export JAVA_HOME=/u00/webadmin/products/jdk_java
  $ export PATH=$JAVA_HOME/bin:$PATH
  $ export DISPLAY=<pc_ip_address:0.0>
  ```

- Run the following commands to run the installer:

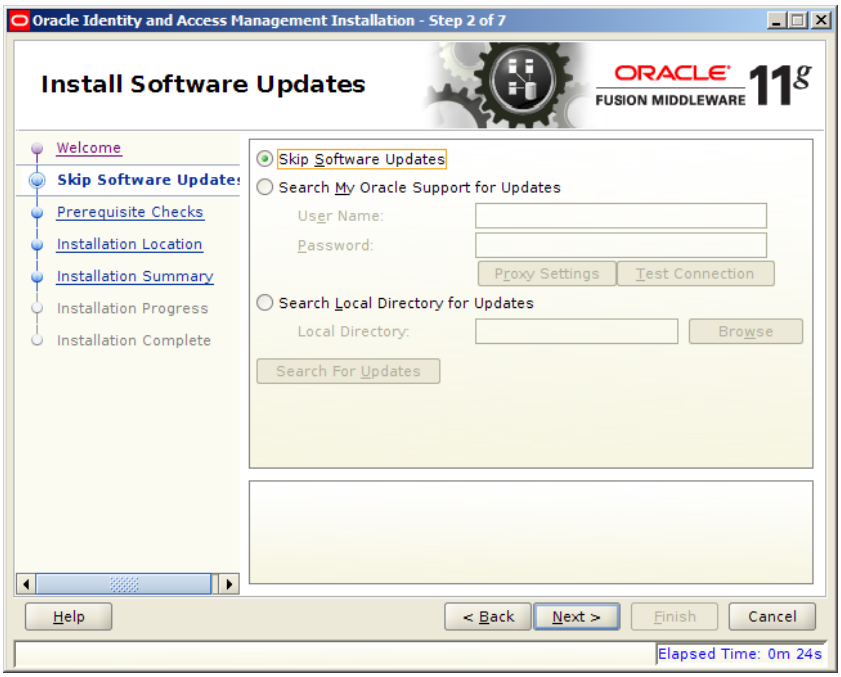
  ```
  $ cd <INSTALL_DIR>/OAM_11.1.2.3/Disk1
  $ ./runInstaller
  ```

- The installer prompts a request for the JAVA_HOME – enter in the JAVA_HOME and press enter.

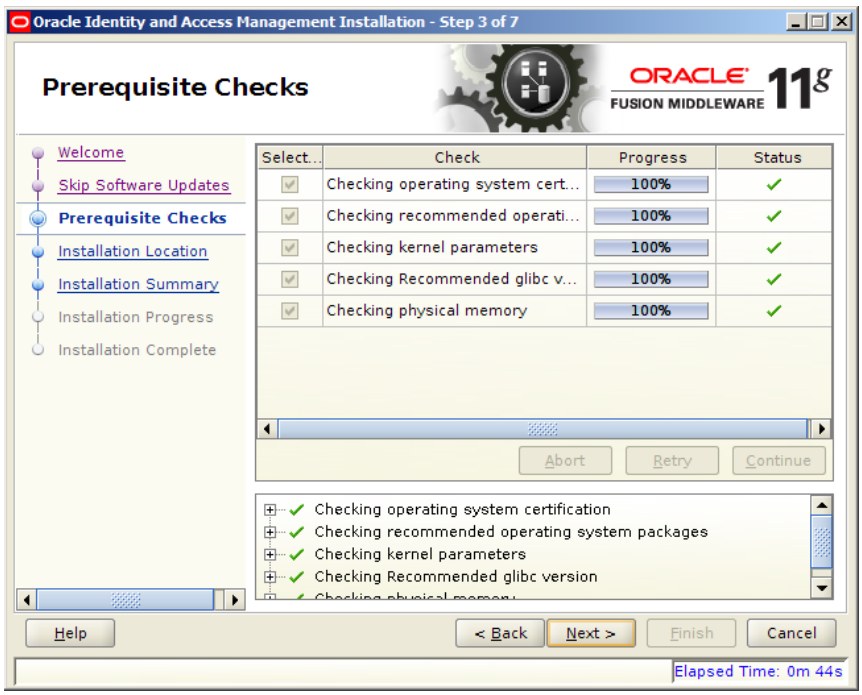
  ```
  $ Please specify JRE/JDK location ( Ex. /home/jre ),
  <location>/bin/java should exist :/u00/webadmin/products/jdk_java
  ```

- The Welcome window opens. Click **Next**.

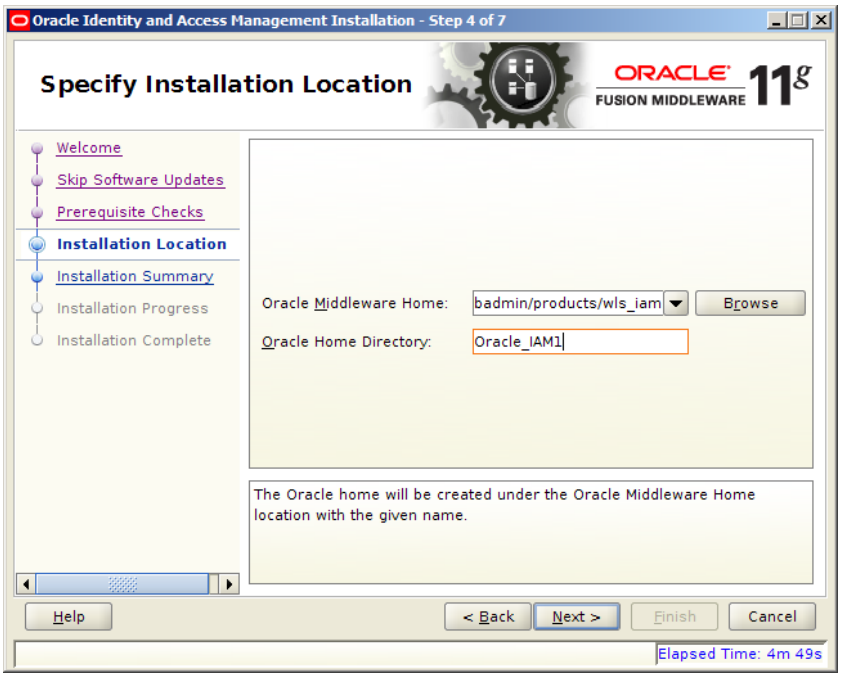
- The Install Software Updates window opens. Select the 'Skip Software Updates' option and, click **Next**.



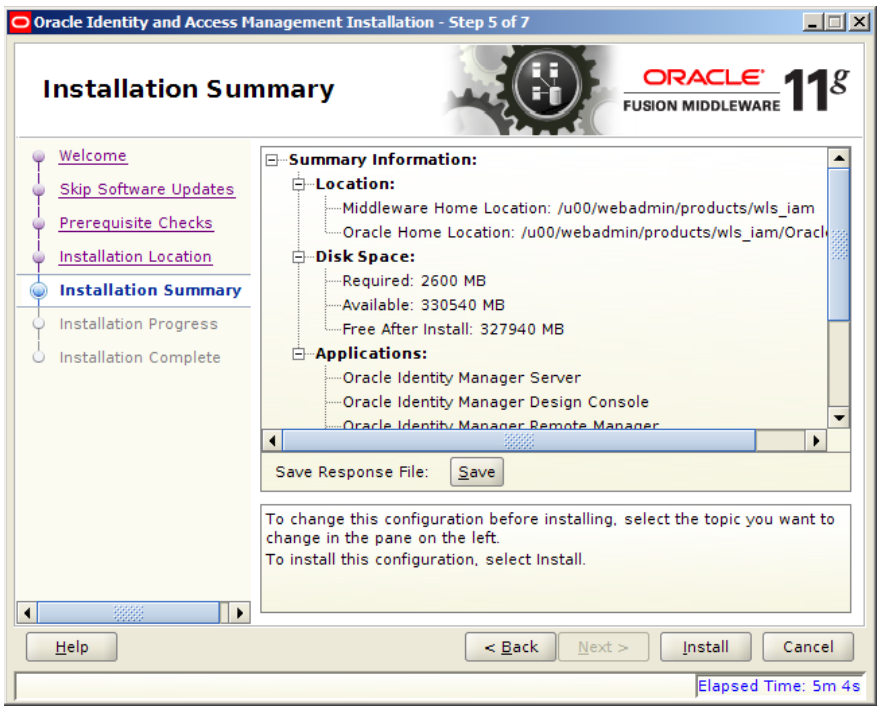
- The Prerequisite Checks window opens. Click **Next**.



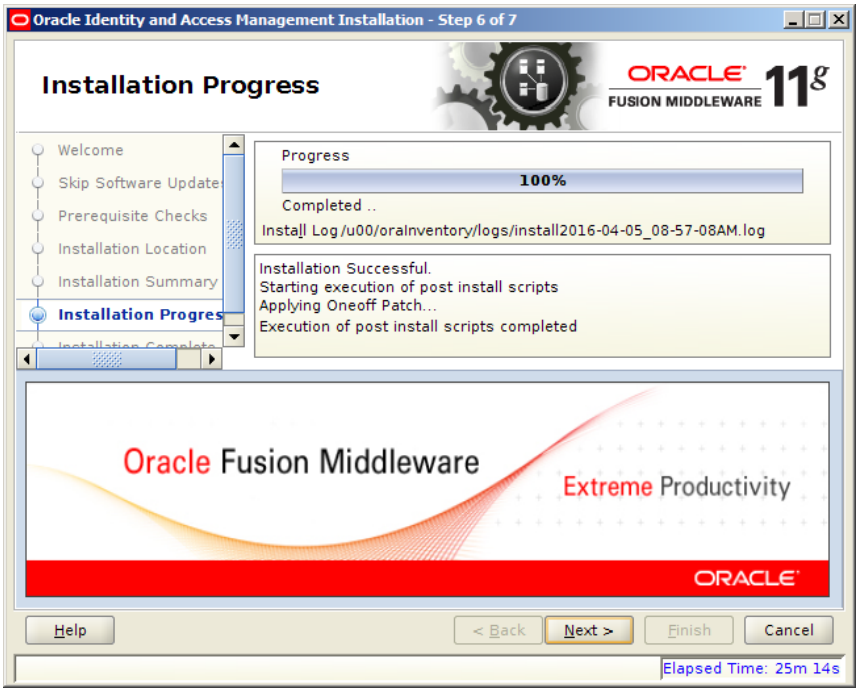
- The Specify Installation Location window opens. Enter the following:
- Oracle Middleware Home where the OAM will be installed: /u00/webadmin/products/wls_iam
  - Oracle Home Directory: Oracle_IAM1
  - Click **Next**.



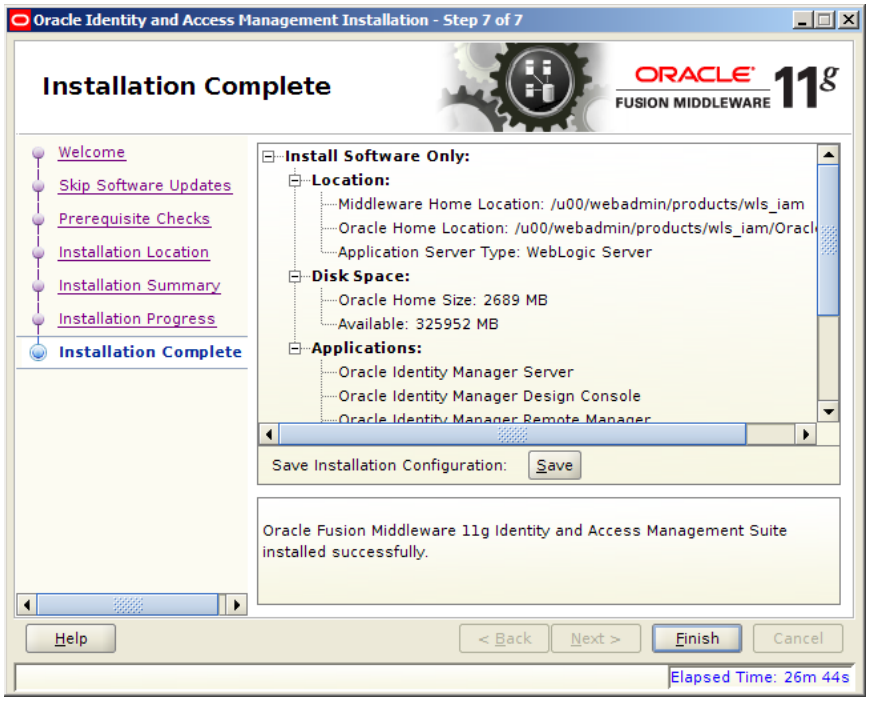
- The Installation Summary window opens. Click **Install**.



- The Installation Progress window opens. Click **Next** when installer finishes.



- The Installation Complete window opens. Click **Finish**.



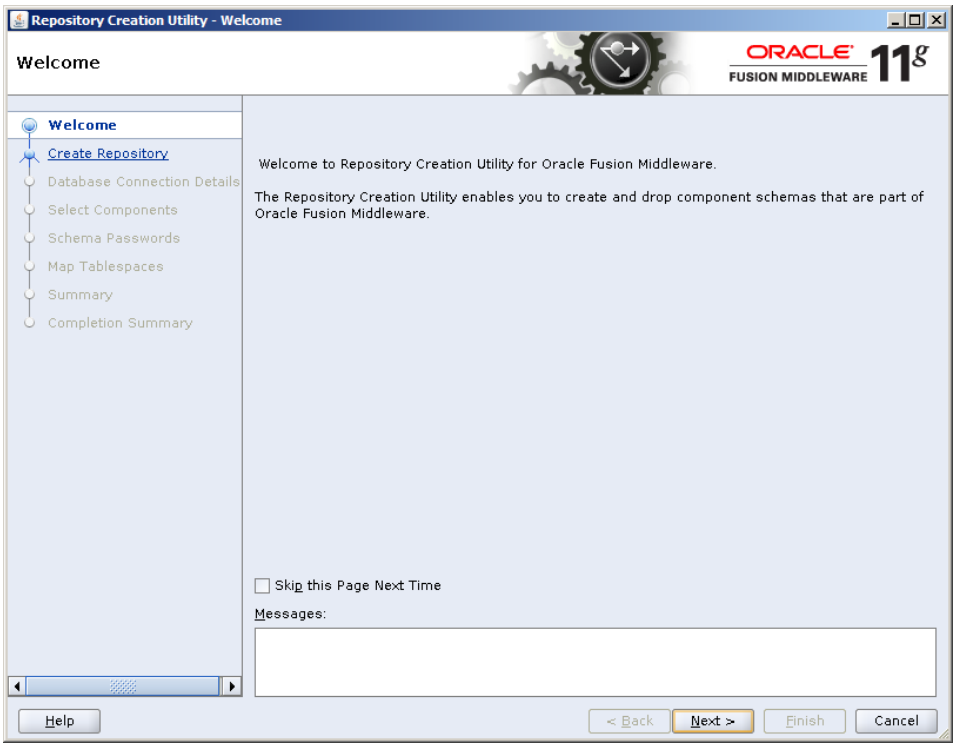
- The installation is complete.

Creating Database Repository for Oracle Access Manager (OAM)

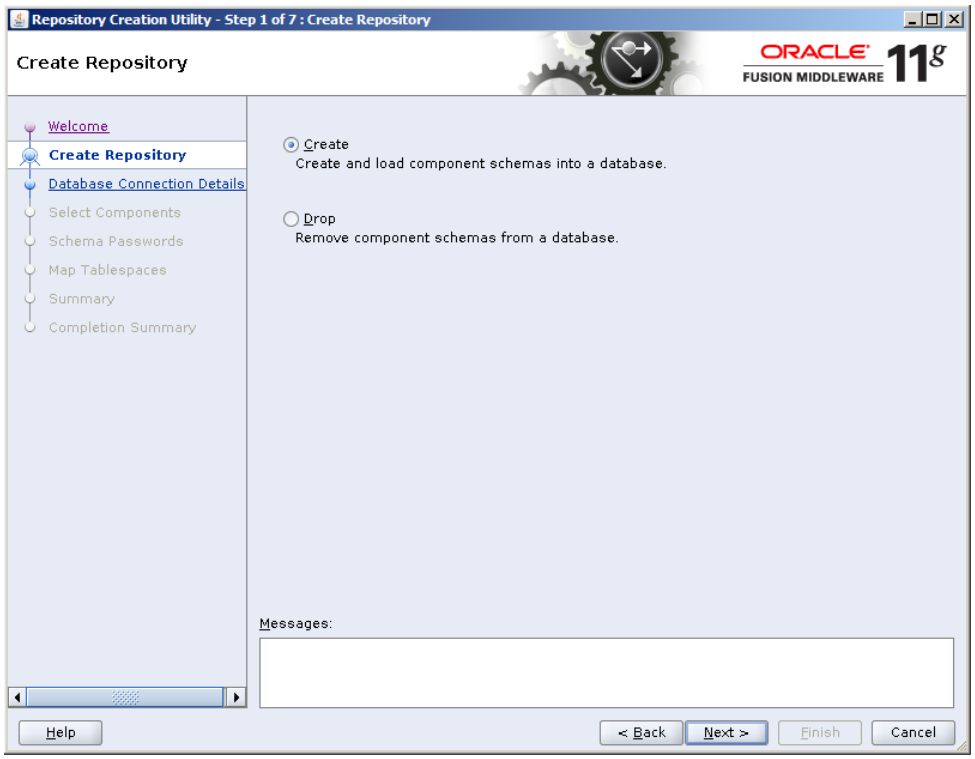
This chapter describes the steps to create a proper schema needed for the OAM installation. In order to run the Repository Creation Utility (RCU) - It is required to use the database credentials for the SYS user. Perform the following steps to create a database repository using Repository Creation Utility:

- Download software installation for Oracle Fusion Middleware Repository Creation Utility 11g (11.1.1.9.0) and place it in an installation staging directory on the Linux host and extract the contents of the zip files. <INSTALL_DIR>/RCU_11.1.1.9.
- Set the following variables by exporting them before running the installer:
  - JAVA_HOME
  - PATH
  - DISPLAY

    Example:
    ```
    $ export JAVA_HOME=/u00/webadmin/products/jdk_java
    $ export PATH=$JAVA_HOME/bin:$PATH
    $ export DISPLAY=<pc_ip_address:0.0>
    ```
- Run the following commands to run the installer:
  ```
  $ cd <INSTALL_DIR>/RCU_11.1.1.9/rcuHome/bin
  $ ./rcu
  ```
- The Welcome Window opens. Click **Next**.

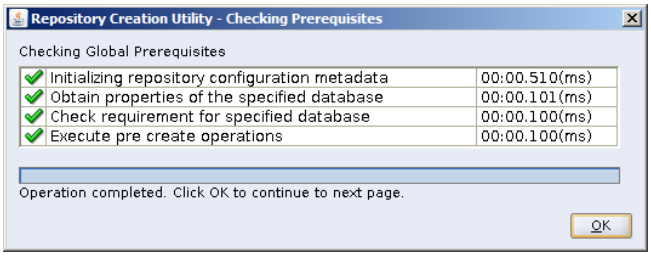


- The Create Repository window opens. Select **Create,** and click **Next**.



- The Database Connection Details window opens. Enter the database details, and click **Next**:
  - Host Name: dbhost-r
  - Port: 1521
  - Service Name: idmservicename
  - Username (must have DBA or SYSDBA privileges)
  - Password

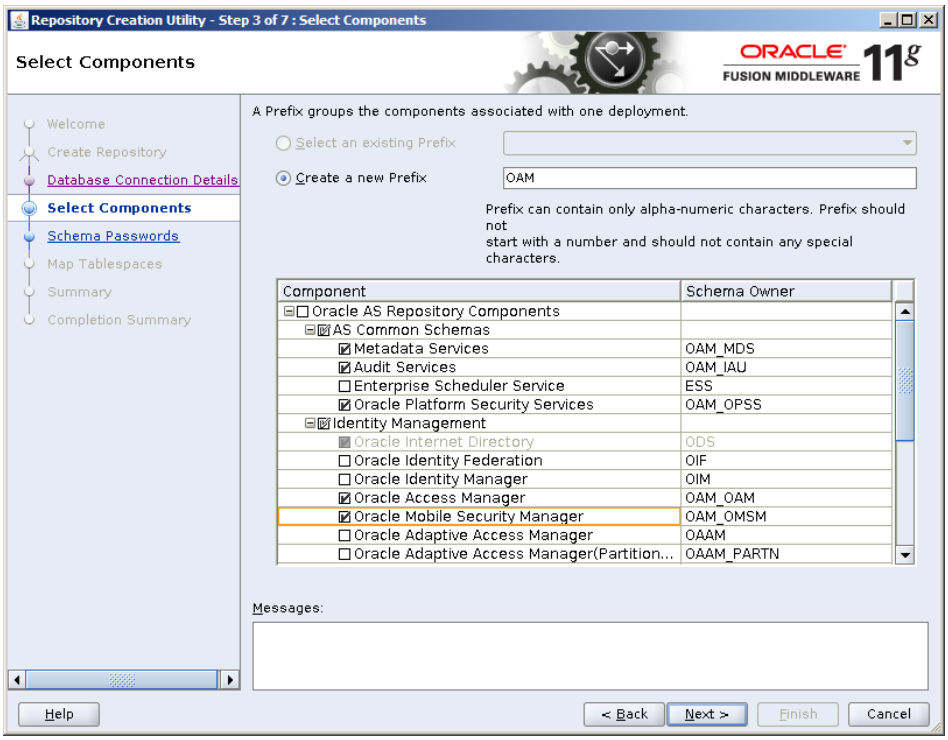
- RCU checks database prerequisites. Click **OK**.



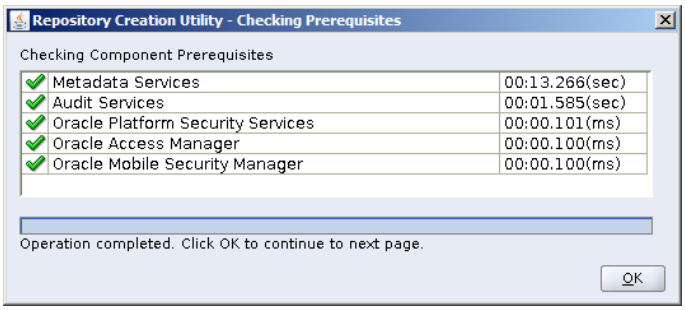
- The Select Components window opens. Select just the following items below, and click **Next**.
  - Select **OAM** for Create a new Prefix.
  - Select the following components:
    - **a.** Oracle Mobile Security Manager

      NOTE: Start selection process with Identity Management - Oracle Mobile Security Manager schema and the rest should auto select the other required components.

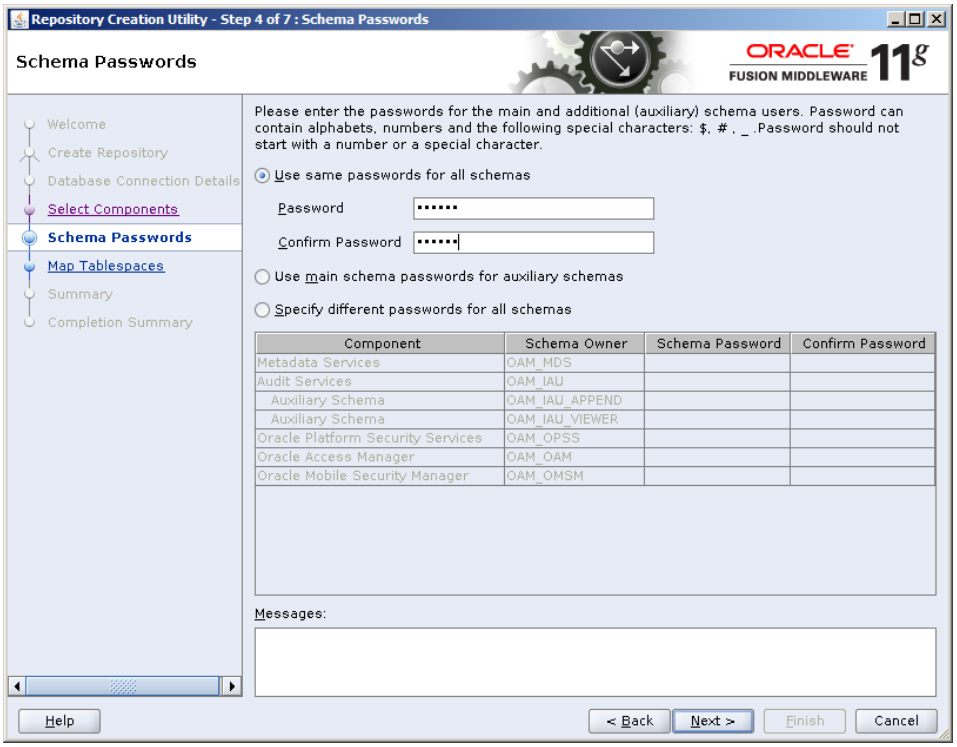
    - **b.** Metadata Services
    - **c.** Audit Services
    - **d.** Oracle Platform security Services
    - **e.** Oracle Access Manager



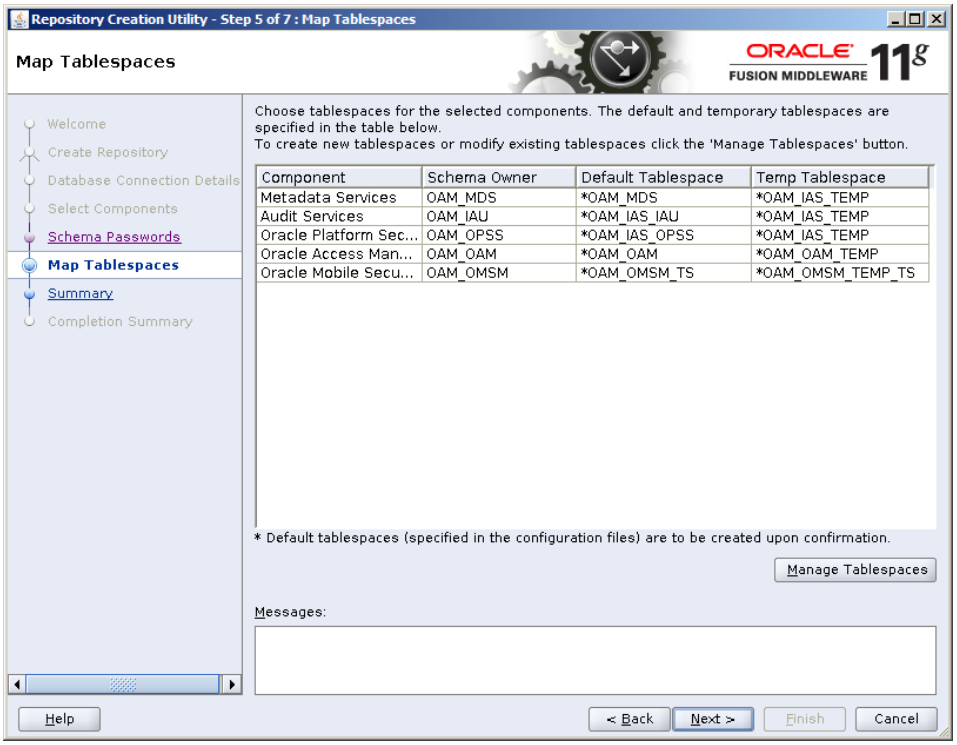
- RCU will check database prerequisites to make sure it can create the selected components. Click **OK**.



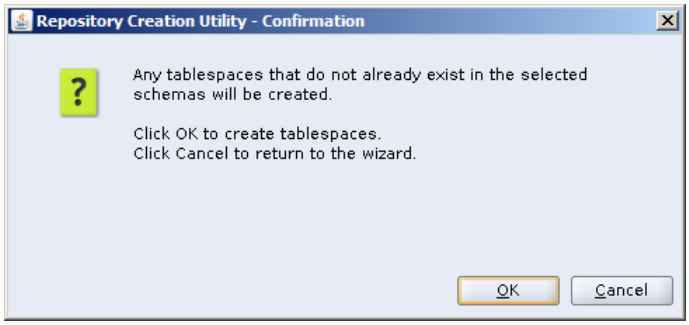
- The Schema Passwords window opens.
  - Select the Use same passwords for all schemas option.
  - Enter the password.
  - Click **Next**.



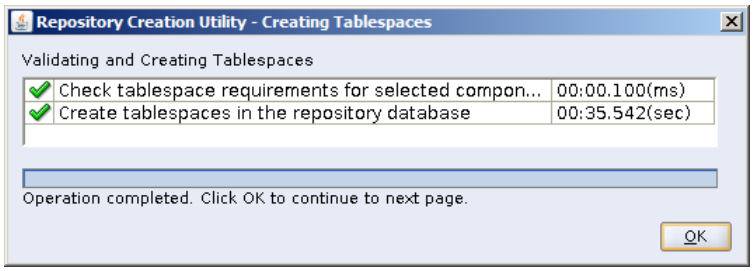
- Map Tablespaces window opens. Click **Next**.



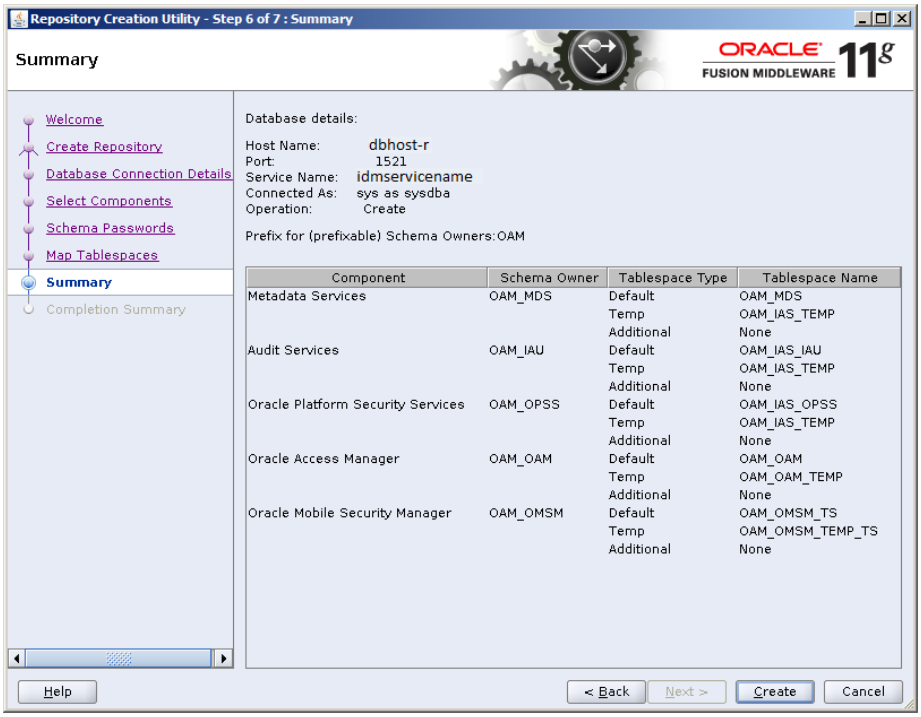
- The Repository Creation Utility - Confirmation window opens. Click **OK**.



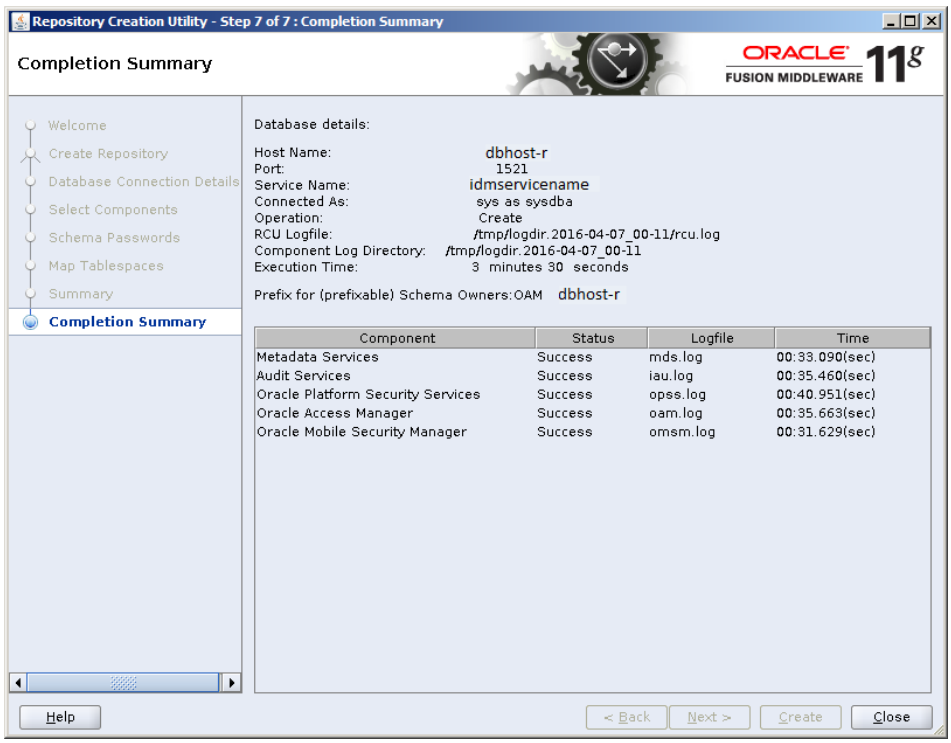
- The Repository Creation Utility – Creating Tablespaces window opens. Click **OK**.



- The Summary window opens. Click **Create**.



- The Completion Summary window opens. Click **Close**.



- The installation is complete.

11

Configuring Oracle Access Manager in Cluster

This chapter describes the configuration of Oracle Access Manager in a cluster.

Configuring OAM on idmhost1

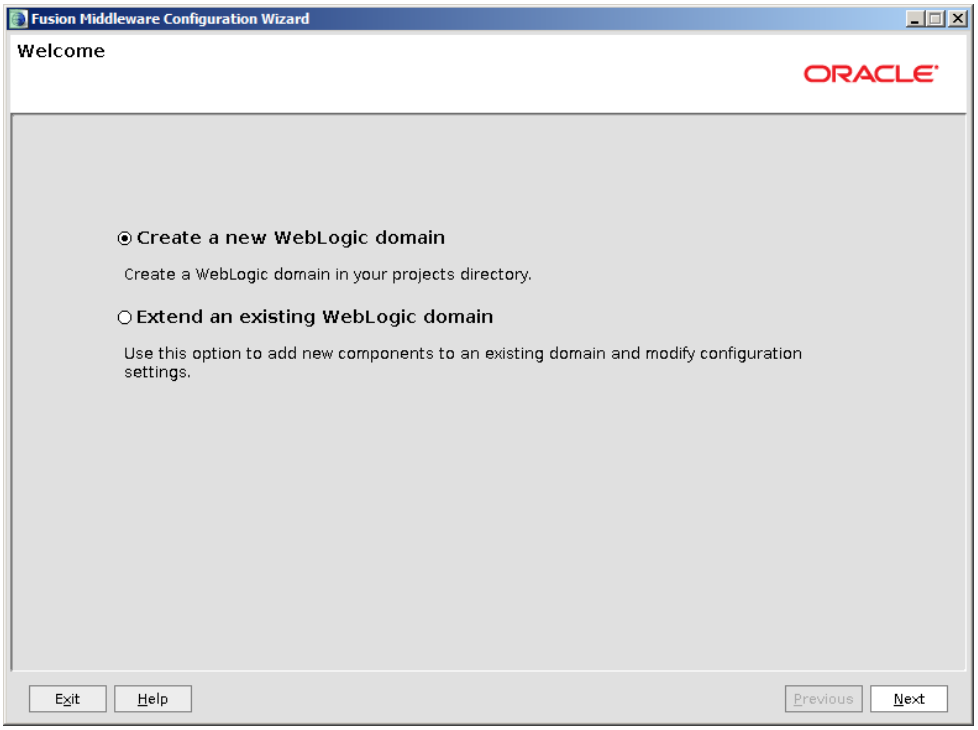
Perform the following steps to configure OAM on idmhost1 only. (OAM will be configured on idmhost2 using separate instructions.)

- Set the following variables by exporting them before running the domain configuration setup script :
  - JAVA_HOME
  - PATH
  - DISPLAY

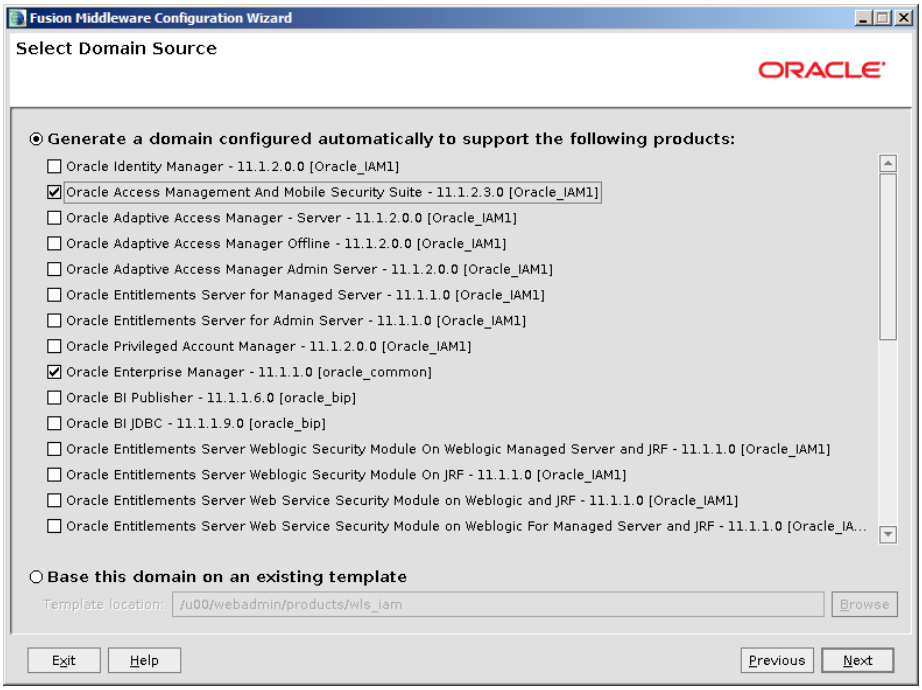
    Example:
    ```
    $ export JAVA_HOME=/u00/webadmin/products/jdk_java
    $ export PATH=$JAVA_HOME/bin:$PATH
    $ export DISPLAY=<pc_ip_address:0.0>
    ```
- Navigate to the Navigate to <OAM_WEBLOGIC_HOME>/oracle_common/common/bin and run config.sh:

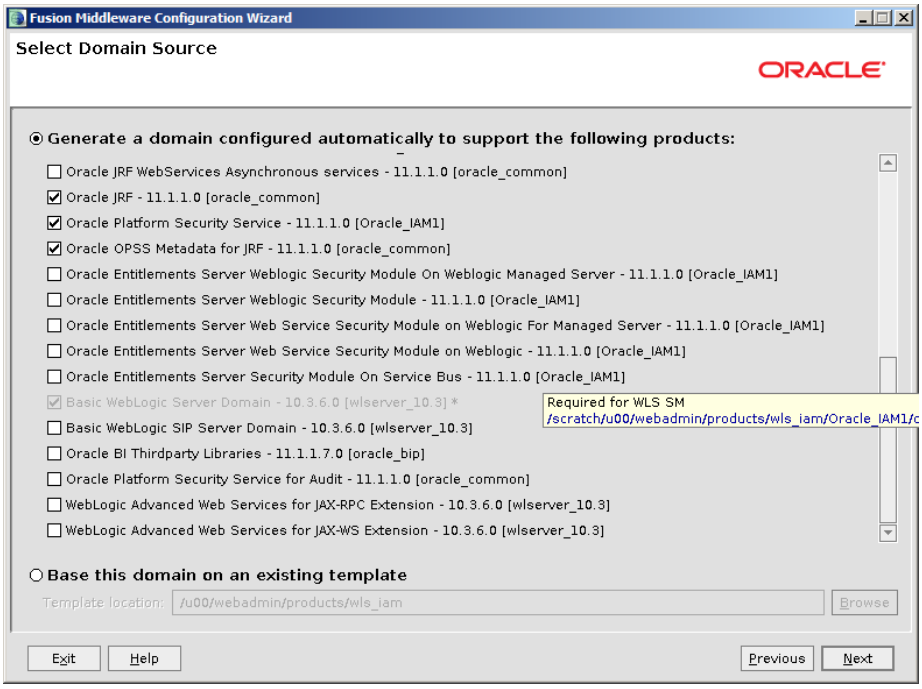
  ```
  $ cd /u00/webadmin/products/wls_iam/oracle_common/common/bin
  ```
- Run the following command:

  ```
  $ ./config.sh
  ```
- The Welcome window opens. Select 'Create a new WebLogic domain'. Click **Next**.

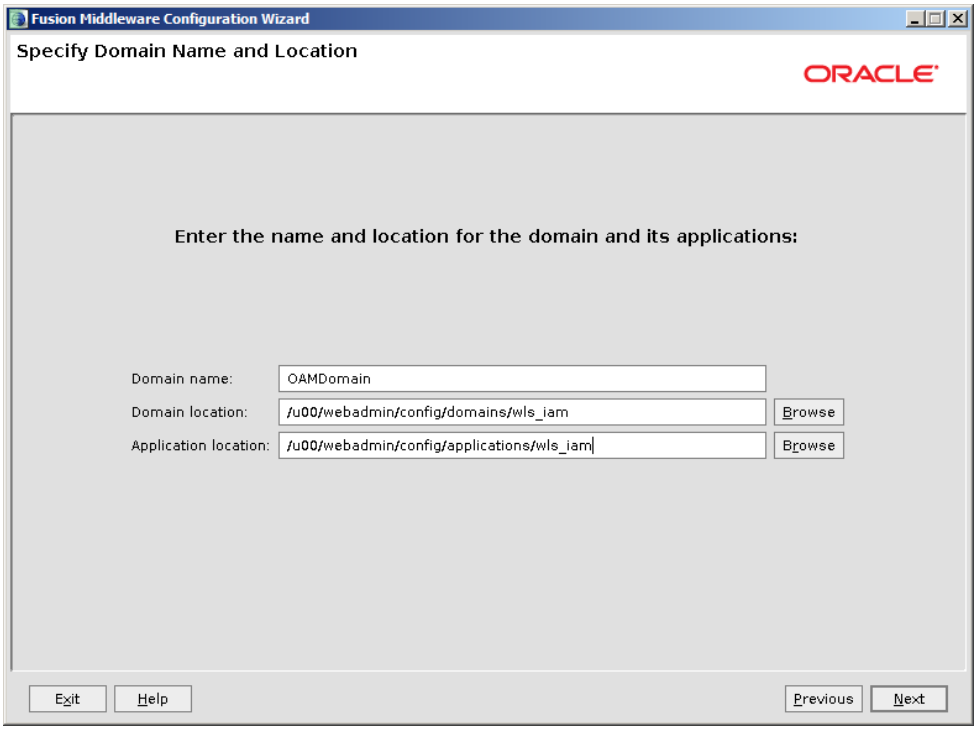


- The Select Domain Source window opens. Select the following products to be installed, and click **Next**. (NOTE: Selecting the Oracle Access Management And Mobile Security Suite - 11.1.2.3.0 [IAM_HOME]) option will auto select the rest.
  - Oracle Access Management And Mobile Security Suite - 11.1.2.3.0 [IAM_HOME]
  - Oracle Platform Security Service 11.1.1.0 [IAM_HOME]
  - Oracle JRF 11.1.1.0 [oracle_common]
  - Oracle OPSS Metadata for JRF - 11.1.1.0 [oracle_common]
  - Oracle Enterprise Manager - 11.1.1.0 [oracle_common]
  - Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]

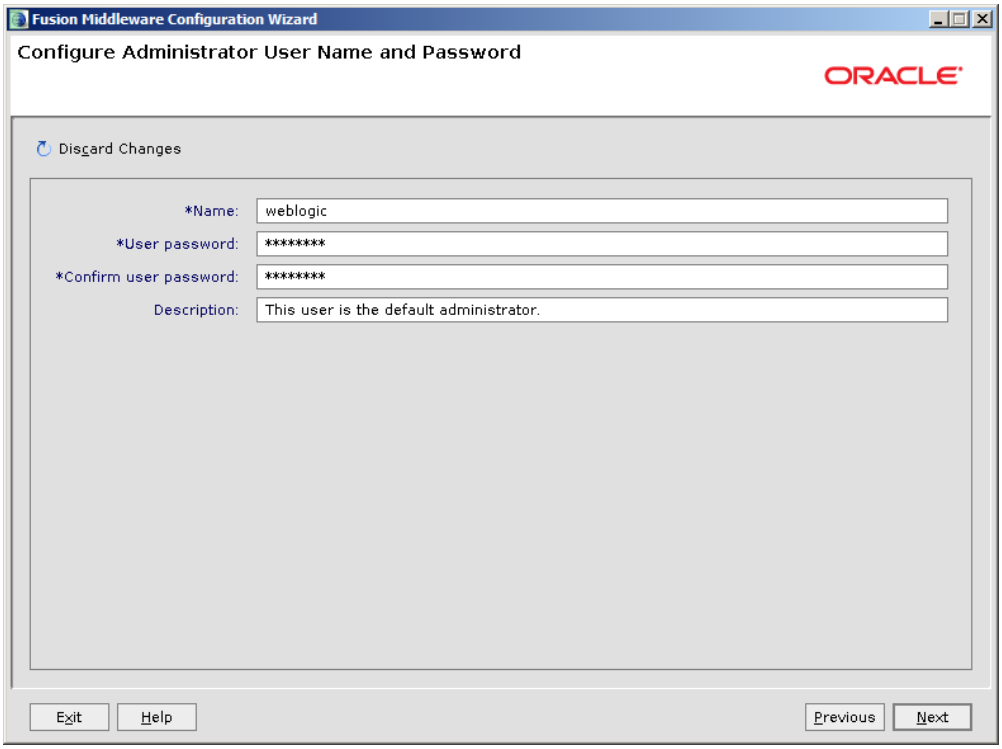




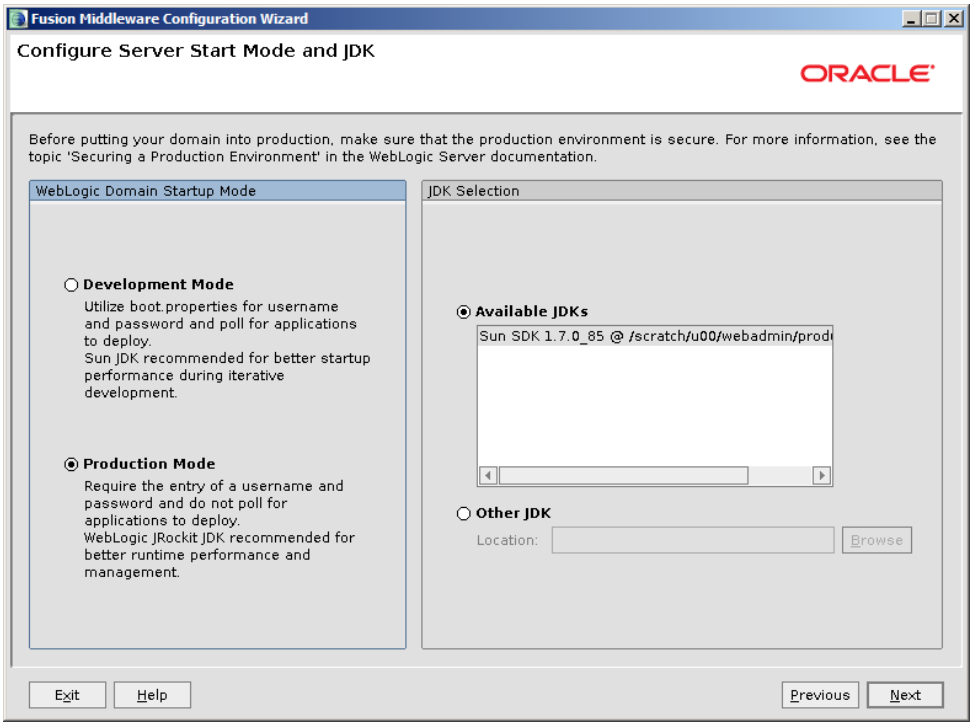
- The Specify the Domain Name and Location window opens. Enter in the following and click **Next**.
  - Domain name: OAMDomain
  - Domain location: /u00/webadmin/config/domains/wls_iam
  - Application location: /u00/webadmin/config/applications/wls_iam



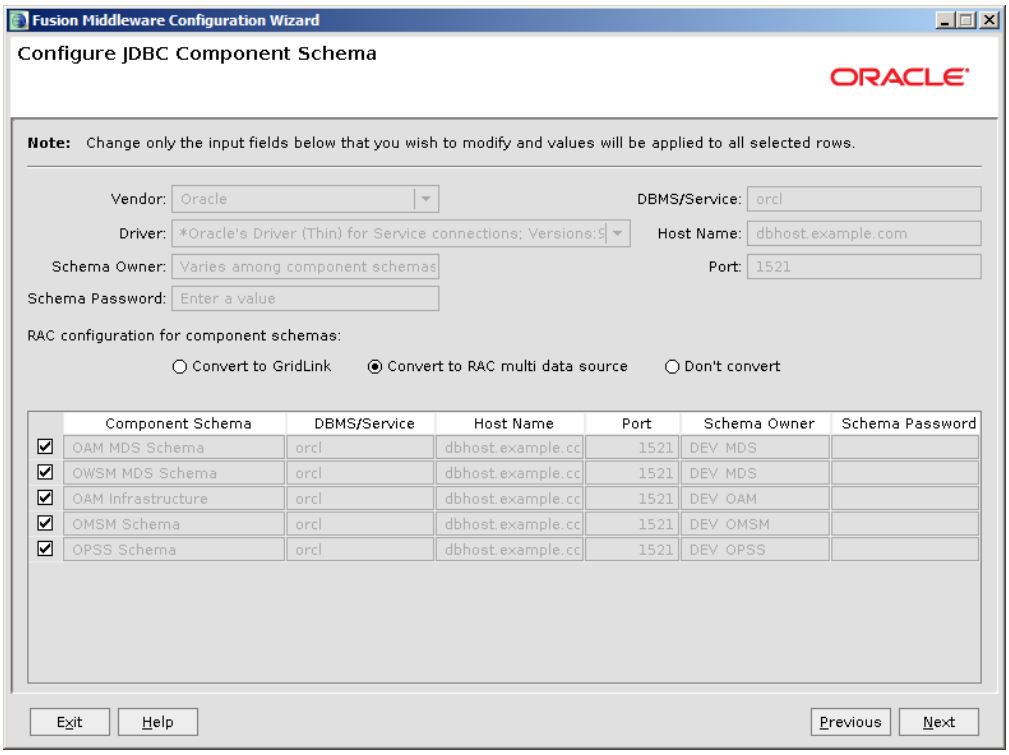
- The Configure Administrator User name and Password window opens. Provide the WebLogic administrator credentials. Click **Next**.



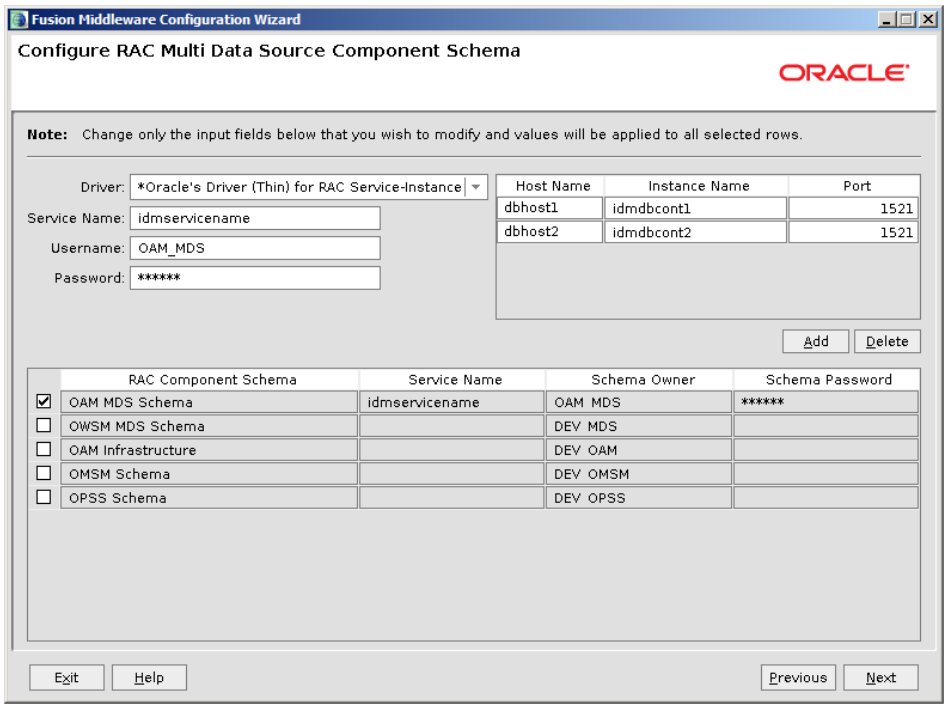
- The Configure Server Start Mode and JDK window opens. Select the **Production Mode** and the **Available JDKs** options. Click **Next**.



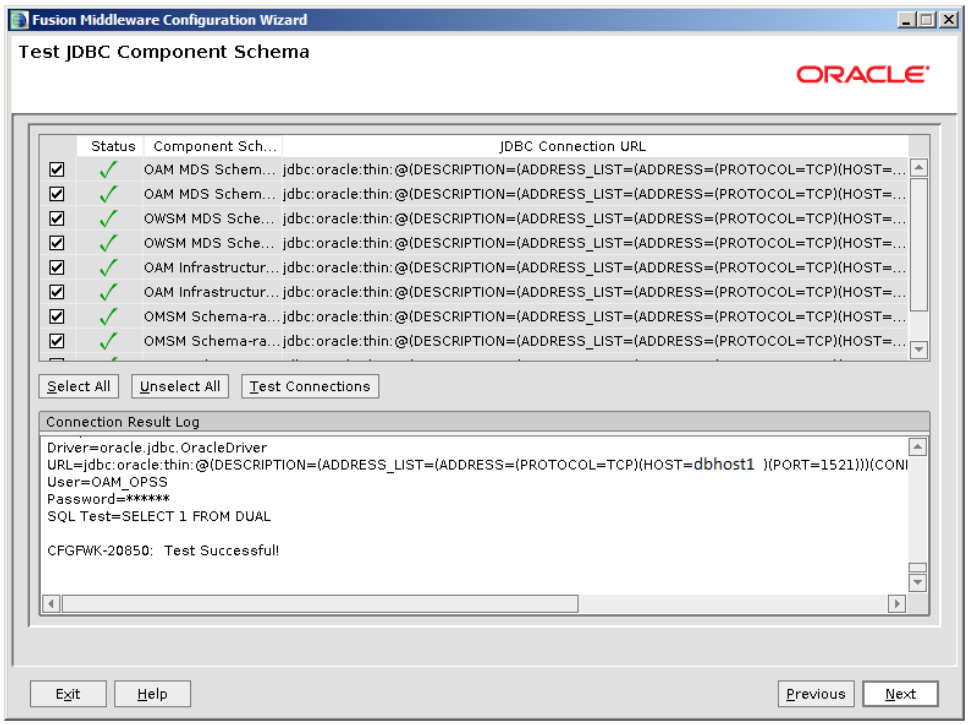
- The Configure JDBC Component Schema window opens.
  - Select all 5 rows in the details section of the screen by checking the check box.
  - Select the **Convert to RAC multi data source** option.
  - Click **Next**.



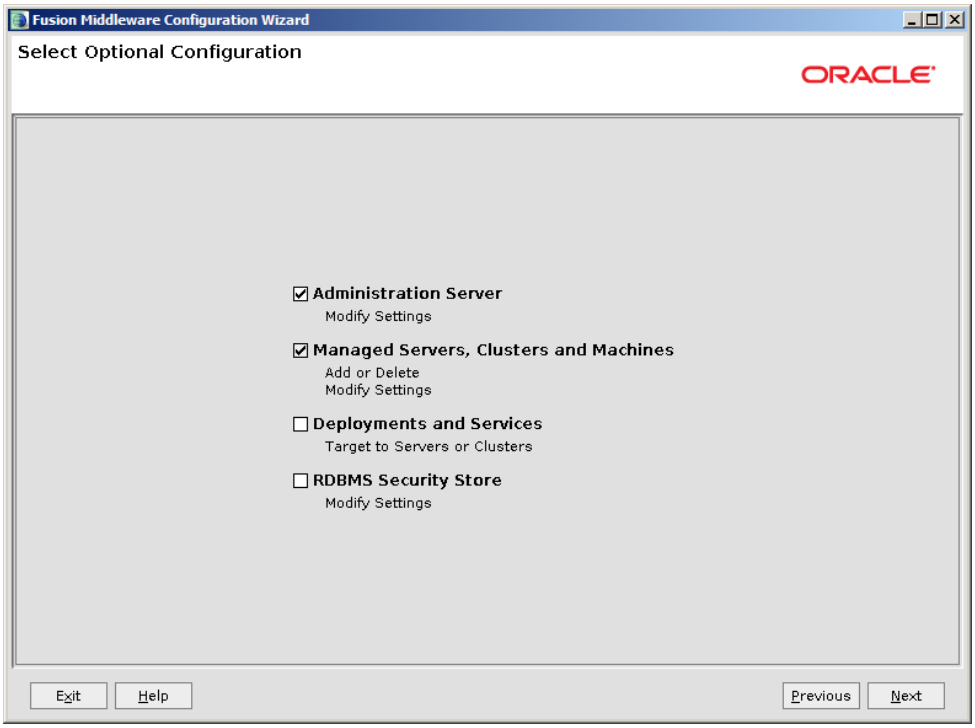
- For all 5 rows in the details section of the screen - make the following updates 1 row at a time by just checking one check box at a time while making updates. Click **Next** when finished updating all 5 rows.
  - Service Name: idmservicename
  - User Name: Update the prefix with the prefix that was used to during RCU creation – See screen shot for example. (OAM)
  - Password: provide the same password that was given during RCU creation.
  - Host Name section:
    - **a.** Click **Add** until there are 2 rows in the section.
    - **b.** Host Name: Each row gets a database host name from cluster. (example: dbhost1 and dbhost2)
    - **c.** Instance Name: Each row gets a corresponding instance name for its database host. (example: cont1 and cont2)
    - **d.** Port: 1521



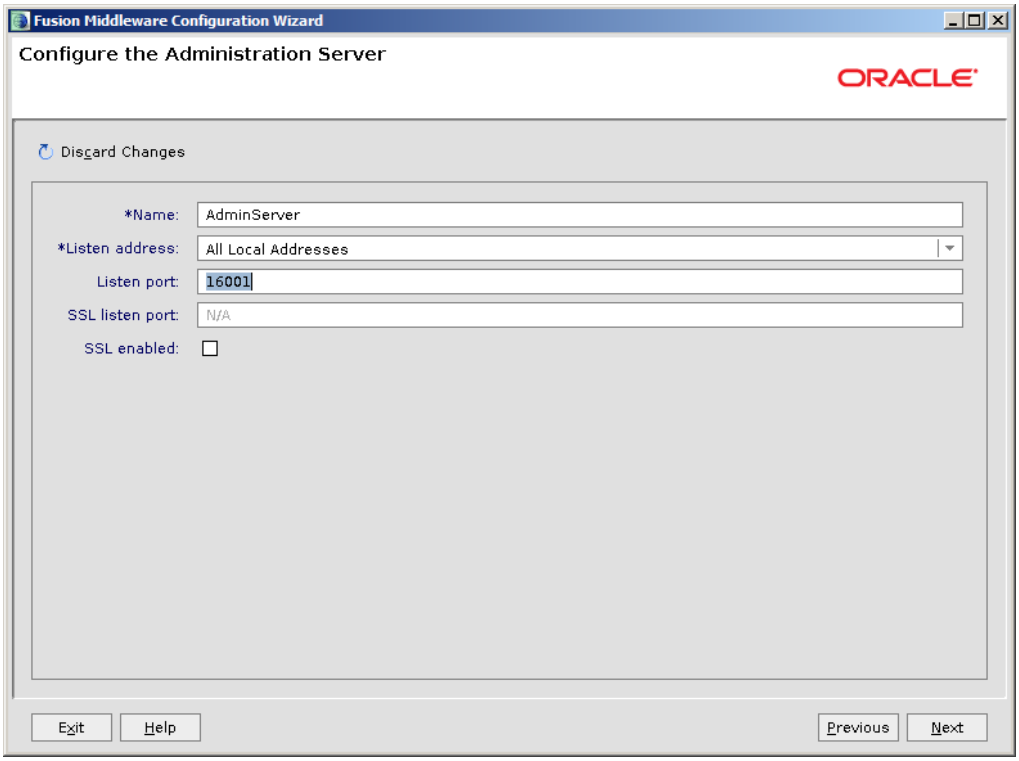
- The Test JDBC Component Schema window opens. Ensure the statuses are all green, and click **Next**. If not – The issue needs to be resolved before continuing.



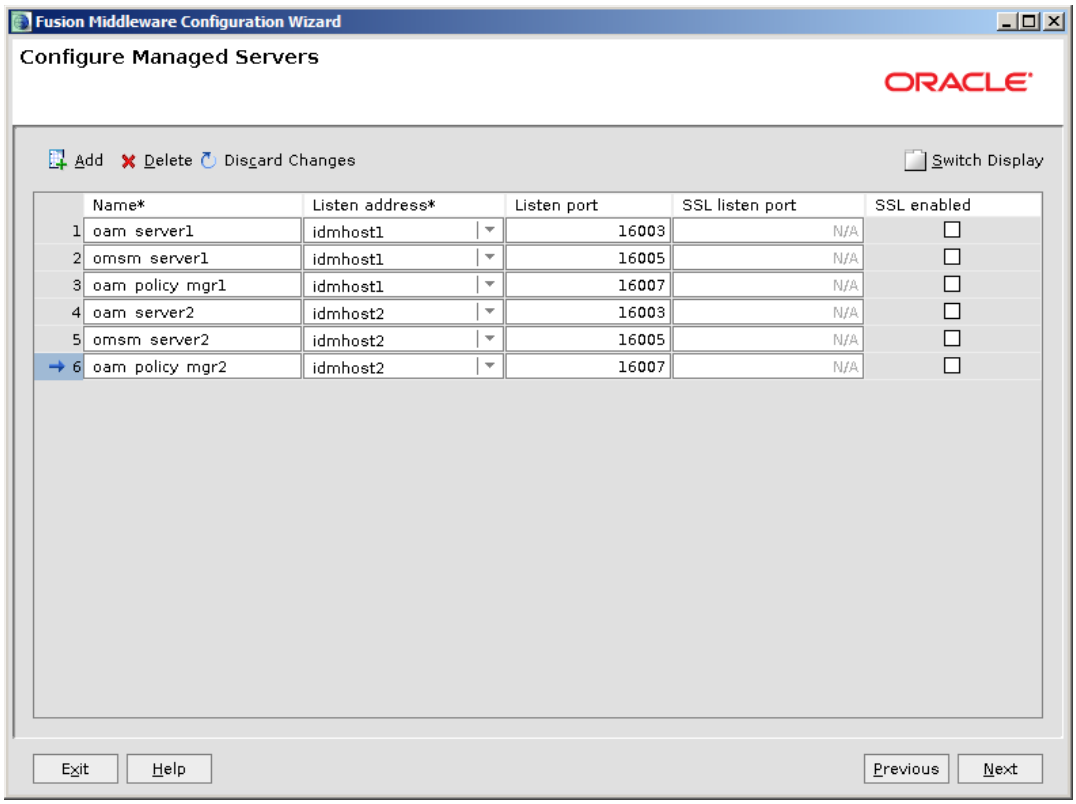
- The Select Optional Configuration window opens.
  - Select **Administration Server**, and **Managed Servers, Clusters and Machines.**
  - Click **Next**.



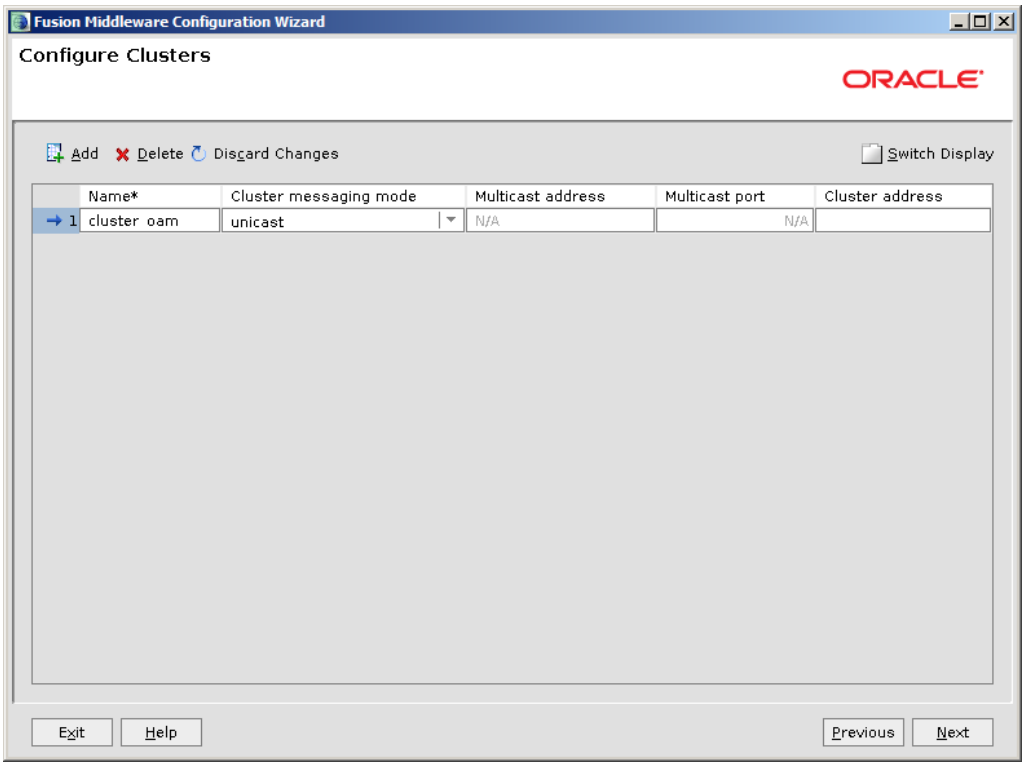
- The Configure the Administration Server window opens. Provide the port for AdminServer (example: 16001), and click **Next**.



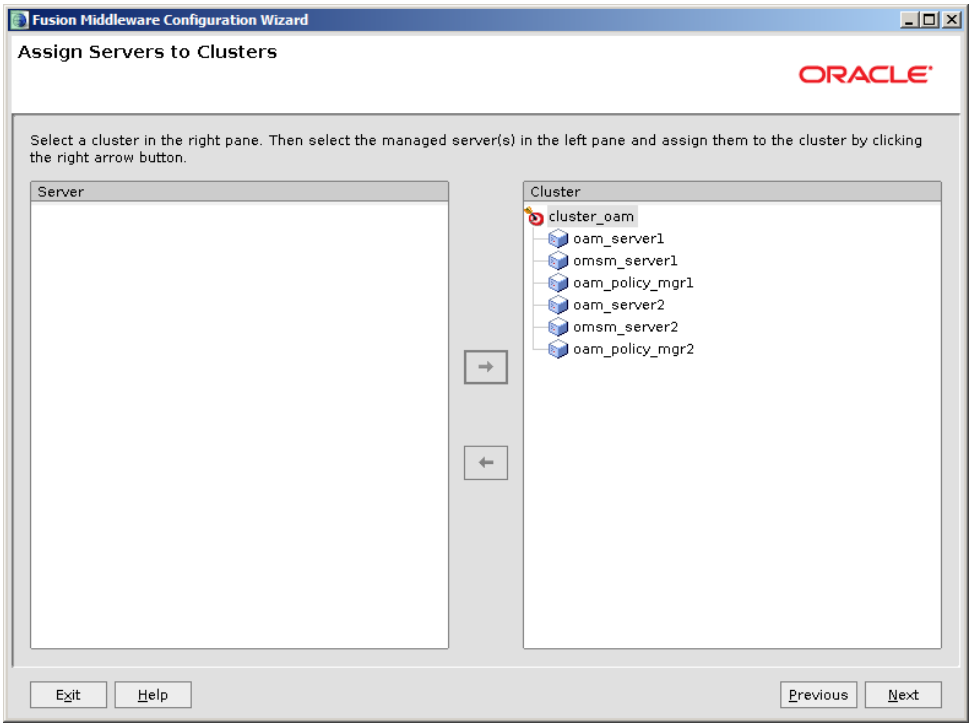
- The Configure Managed Servers window opens.
  - The window opens displaying pre-populated components selected for managed servers. Click **Add** to add an additional row for each managed server so that we can have matching managed servers configured on each host in the cluster.
  - Update the new rows that were added so that the names can logically be linked. See screen shot for example.
  - For each managed server update the listen address to point to the intended idmhost.
  - Update the ports as shown in screen shot below.
  - Click **Next**.



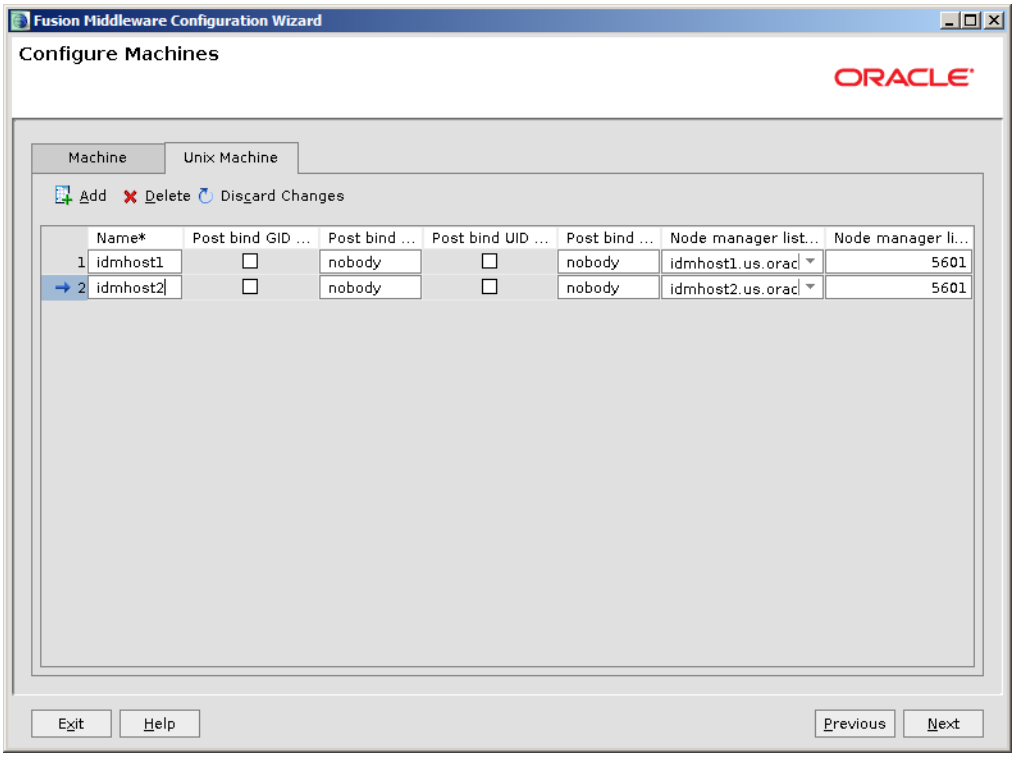
- The Configure Clusters window opens. Update the name to cluster_oam and click **Next**.



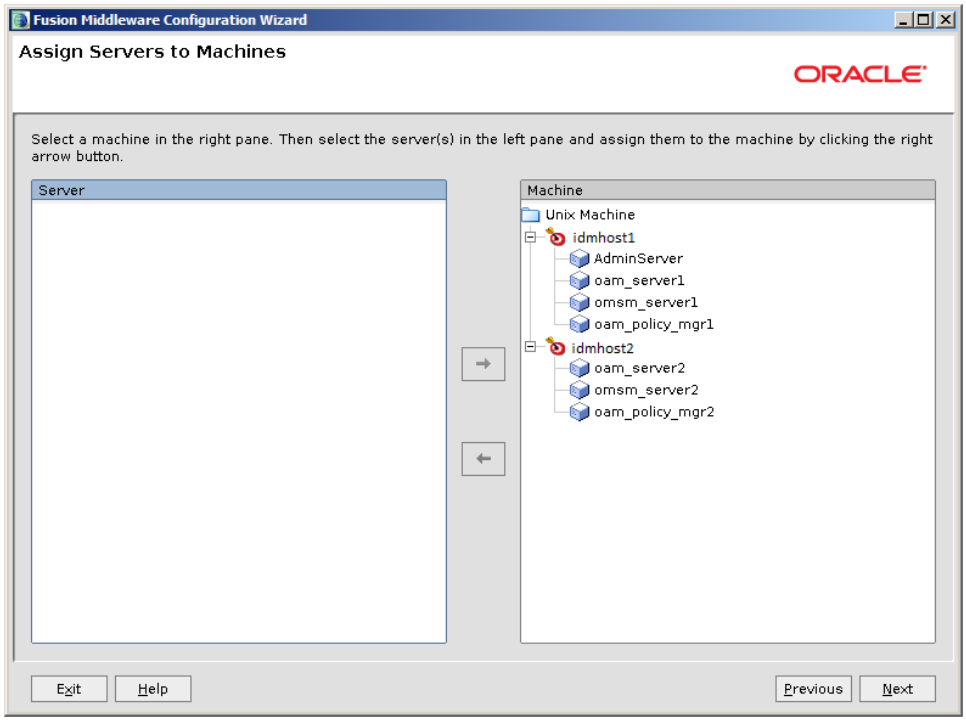
- The Assign Servers to Clusters window opens. Add all of the managed servers to the cluster_oam and click **Next**.



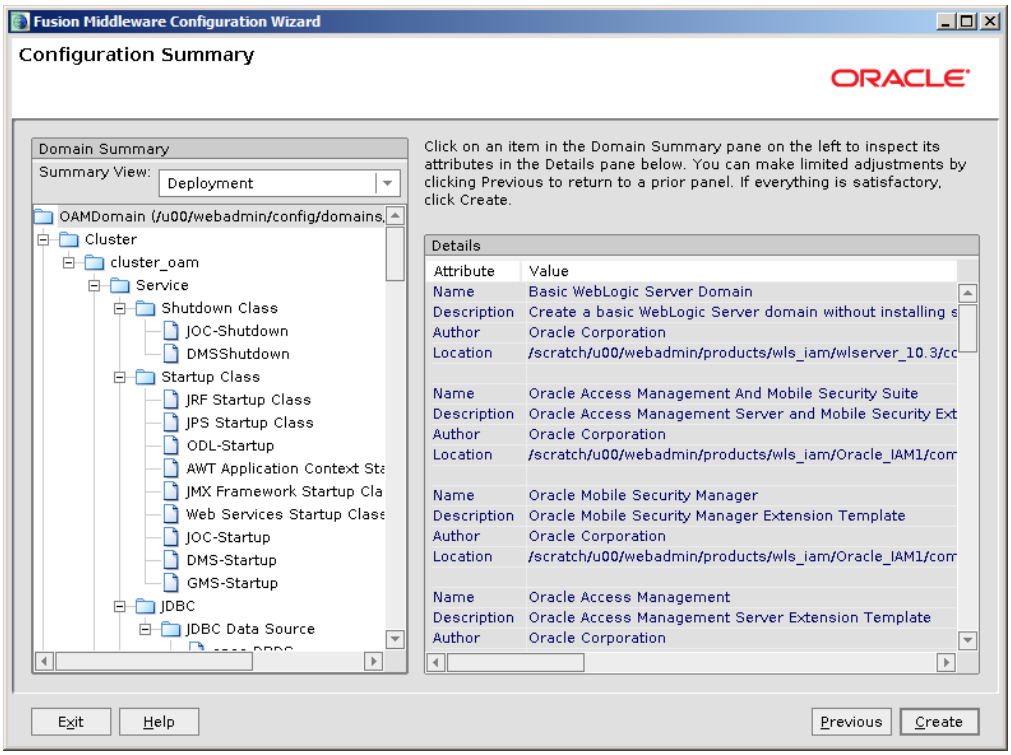
- The Configure Machines window opens.
  - Click the **Unix Machine** tab.
  - Add a 1 row for idmhost1 and idmhost2
  - Machine Name: idmhost1 and idmhost2
  - Node manager listen address: idmhost1.us.oracle.com and idmhost2.us.oracle.com (Fully qualified name of alias.)
  - Node manager listen port: 5601
  - Click **Next**.



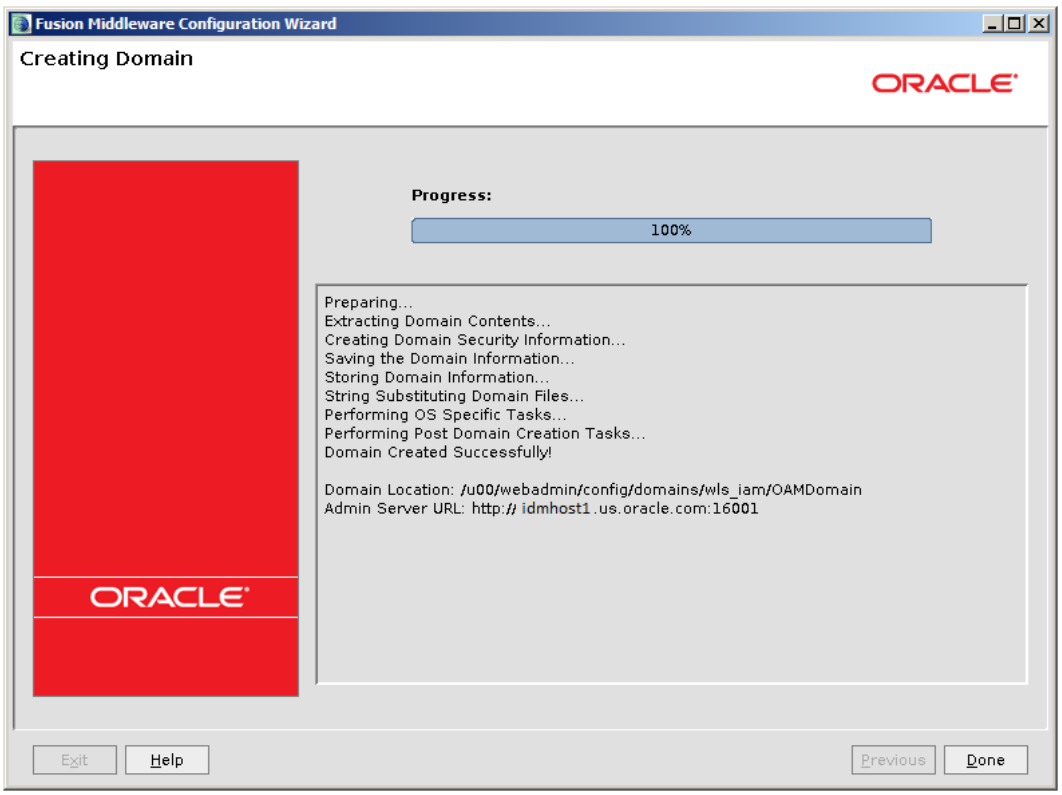
- The Assign Servers to Machines window opens.
  - Add servers to the machines using the screen shot below as an example
  - Click **Next**.



- The Configuration Summary window opens. Review the Configuration Summary and click **Create**.



- The Creating Domain window opens. Click **Done.**



- The installation is complete.

Node Manager Configuration for OAM on idmhost1 and idmhost2

Perform the following steps configure the nodemanager for OAM on both idmhost1 and idmhost2:

- Start the node managers using the startNodeManager.sh script so that it will create the nodemanager.properties file

  ```
  $ cd /u00/webadmin/products/wls_iam/wlserver_10.3/server/bin
  $ nohup ./startNodeManager.sh &
  ```

- Validate and update the nodemanager.properties (<OAM_MW_HOME>/wlserver_10.3/common/nodemanager)
  - First take a backup of the nodemanager.properties

    Example:

    ```
    $ cd /u00/webadmin/products/wls_iam/wlserver_10.3/common/nodemanager
    $ cp nodemanager.properties nodemanager.propertiesbk1
    ```

  - Update StartScriptEnabled=true
  - Update ListenPort=5601
    a. This should be the port that was specified for the node manager during config.sh setup.
    b. Take note of the ListenPort that is currently listed as it will be needed to restarting nodemanger after changes are made.
- Stop the node manager
  - Stop the nodemanager using the port that was listed in the nodemanager.properties file. (This is the original value of ListenPort)

    Example:

    ```
    $ netstat -nap | grep 5556
    Not all processes could be identified, non-owned process info will not
    be shown, you would have to be root to see it all.)
    tcp 0 0 0.0.0.0:5560 0.0.0.0:* LISTEN 16120/java
    $ kill -9 16120
    ```

- Start the node managers using the startNodeManager.sh script so that it will create the nodemanager.properties file

  Example:

  ```
  $ cd /u00/webadmin/products/wls_iam/wlserver_10.3/server/bin
  $ nohup ./startNodeManager.sh &
  ```

Start AdminServer for OAM_WEBLOGIC_HOME on idmhost1

Perform the following steps configure and start the WebLogic admin server on idmhost1.

When trying to start the admin server before completing the initial configuration of the security store – it will throw an error stating that it could not create security store. Perform the following steps to configure the security store:

- Navigate to <OAM_MW_HOME>/oracle_common/common/bin/

  ```
  $ cd /u00/webadmin/products/wls_iam/oracle_common/common/bin
  ```

- Execute the following command: wlst.sh <OAM_HOME>/common/tools/configureSecurityStore.py –d <domaindir> -c IAM –p <opss_schema_password> -m create

  Example:

```
$ wlst.sh
/u00/webadmin/products/wls_iam/Oracle_IAM1/common/tools/configureSecurityS
tore.py -d /u00/webadmin/config/domains/wls_iam/OAMDomain -c IAM -p retail
-m create
```

Output:

Info: Create operation has completed successfully.

- Use the Oracle Platform Security Services (OPSS) script exportEncryptionKey to extract the encryption key from the Oracle Entitlements Server 11g R2 PS3 (11.1.2.3) domain and export it into the ewallet.p12 file.
  - First create a directory to create a wallet in for the policy store.

    Example:

    ```
    $ mkdir /u00/webadmin/config/domains/wls_iam/OAMDomain/mydir
    ```

  - Run the following command to launch the WebLogic Scripting Tool (WLST):

    Example:

    ```
    $ wlst.sh
    ```

  - At the WLST prompt, run the following command:

    Example:

    ```
    $ wls:/offline>
    exportEncryptionKey(jpsConfigFile="/u00/webadmin/config/domains/wls_iam
    /OAMDomain/config/fmwconfig/jps-config.xml",
    keyFilePath="/u00/webadmin/config/domains/wls_iam/OAMDomain/mydir",
    keyFilePassword="retail123")
    ```

    Output:

    ```
    Apr 08, 2016 11:51:38 AM oracle.security.jps.util.JpsUtil disableAudit
    INFO: JpsUtil: isAuditDisabled set to true
    Apr 08, 2016 11:51:39 AM oracle.security.jps.util.JpsUtil disableAudit
    INFO: JpsUtil: isAuditDisabled set to false
    Export of Encryption key(s) is done. Remember the password chosen, it
    will be required while importing the key(s)
    ```

- Migrate the policies with join operation with wlst command as follows:

  Example:

  ```
  $ cd /u00/webadmin/products/wls_iam/oracle_common/common/bin
  $ wlst.sh
  /u00/webadmin/products/wls_iam/Oracle_IAM1/common/tools/configureSecurityS
  tore.py -d /u00/webadmin/config/domains/wls_iam/OAMDomain  -c IAM -p
  retail -m join -k /u00/webadmin/config/domains/wls_iam/OAMDomain/mydir -w
  retail123
  ```

  Output:

  Info: Join operation has completed successfully.

- Validate the security store with wlst command as follows:

  Example:

  ```
  $ cd /u00/webadmin/products/wls_iam/oracle_common/common/bin
  $ wlst.sh
  /u00/webadmin/products/wls_iam/Oracle_IAM1/common/tools/configureSecurityS
  tore.py -d /u00/webadmin/config/domains/wls_iam/OAMDomain -m validate
  ```

  Output:

  Info: Diagnostics data was saved to the credential store.

  Info: Validate operation has completed successfully.

- Start the WebLogic admin server

  Example:

  ```
  $ cd /u00/webadmin/config/domains/wls_iam/OAMDomain/bin
  ```

```
$ ./startWebLogic.sh
```

– Enter in WebLogic admin username and password when prompted.

Create WebLogic boot.properties for OAM WLS Domain on idmhost1

Create WebLogic boot.properties file with username and password so that startup script does not prompt or require user input to start the admin server.

- Change directories to the admin servers security directory and create a boot.properites file.

  Example:

  ```
  $ cd /u00/webadmin/config/domains/wls_iam/OAMDomain/servers/AdminServer
  $ mkdir security
  $ cd security
  $ vi boot.properties
  username=weblogic
  password=<password>
  ```

- Start the WebLogic admin server if it is not running.

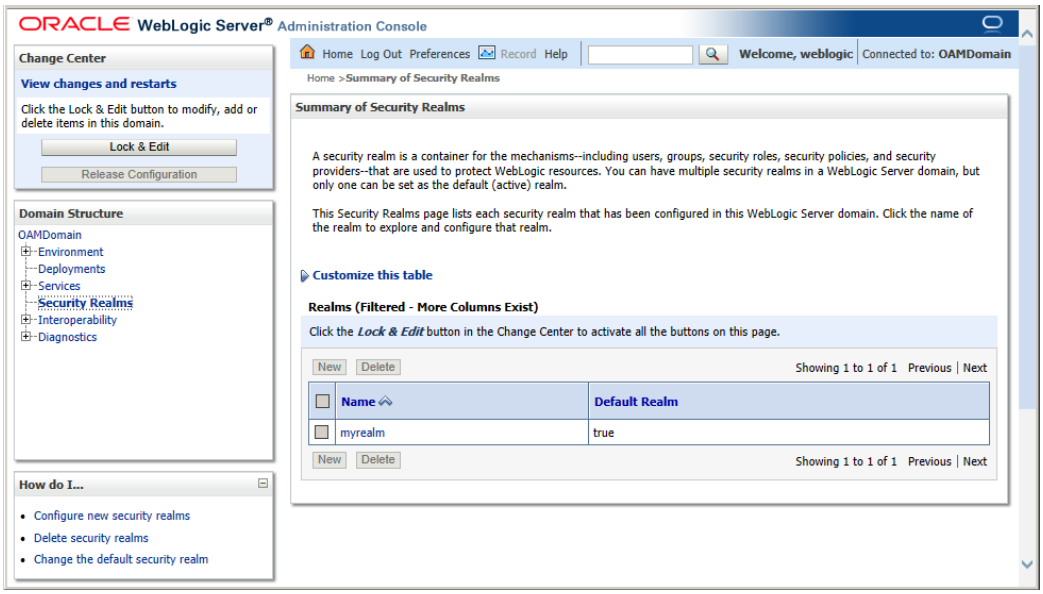
  Example:

  ```
  $ cd /u00/webadmin/config/domains/wls_iam/OAMDomain/bin
  $ nohup ./startWebLogic.sh &
  ```

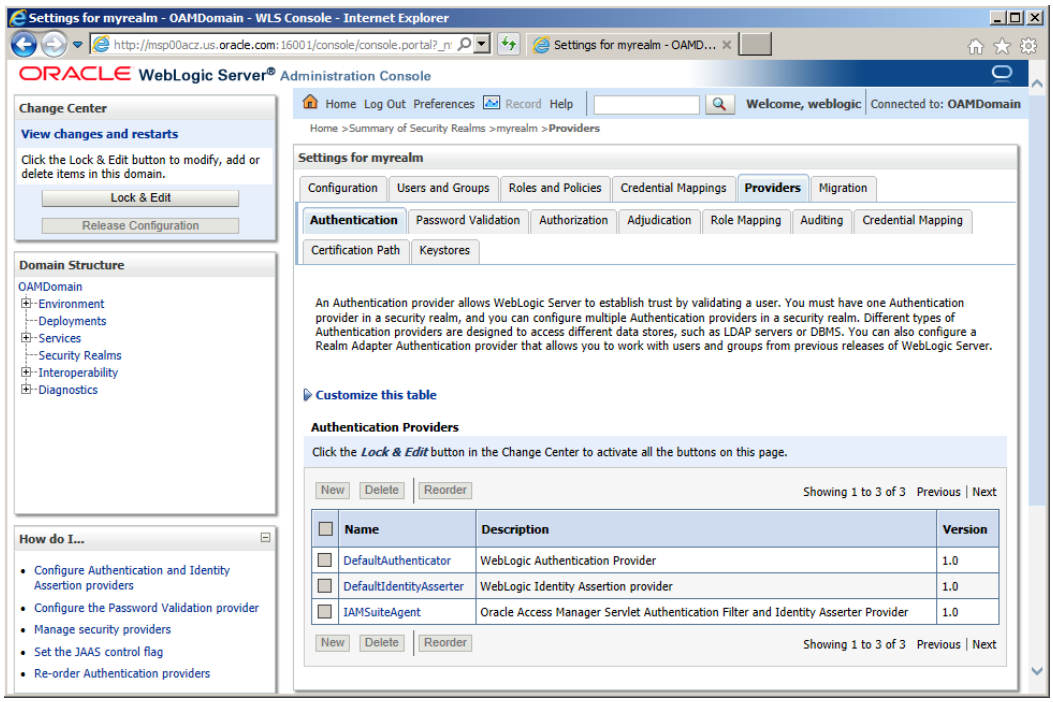
Removing IAMSuite Agent in OAM

To remove the IAMSuite Agent:

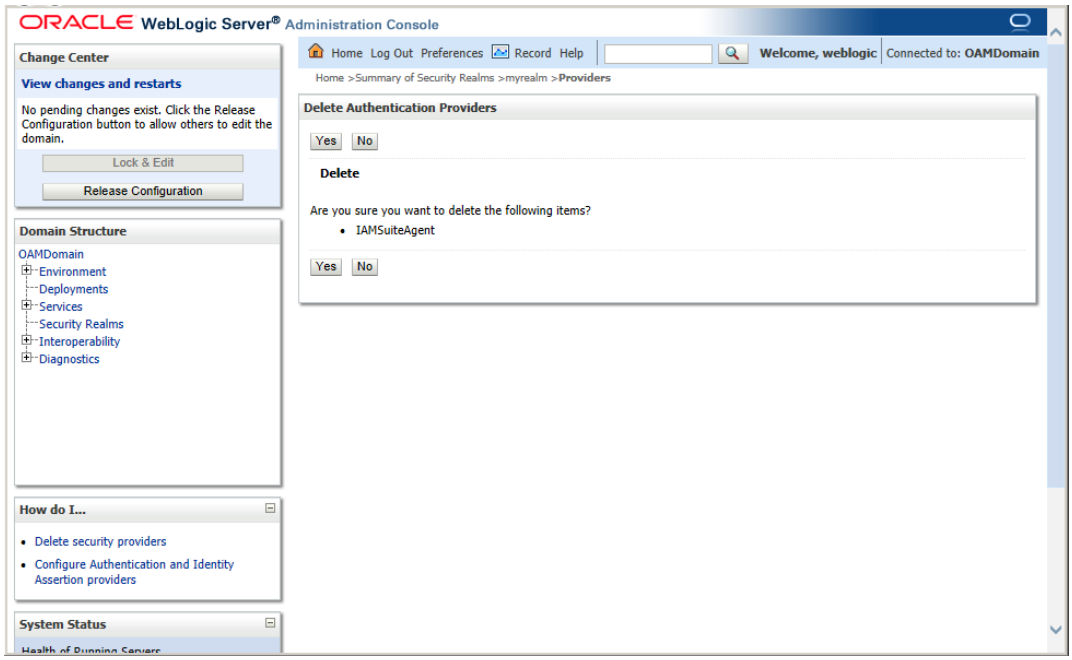
- Login to OAM Administration Server Console running in idmhost1 using Admin user WebLogic. Navigate to OAMDomain > Security Realms. Click myrealm.



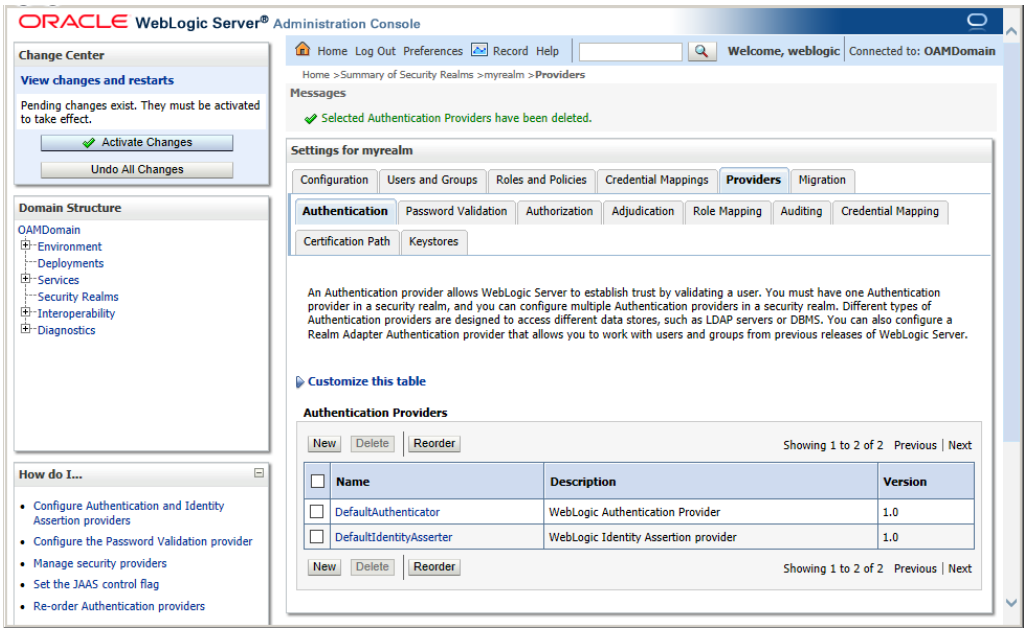
- Navigate to Providers tab > Authentication tab. Click **Lock & Edit**. Select IAMSuiteAgent and click **Delete**.



- Click **Yes** when prompted.



- Click Activate Changes.



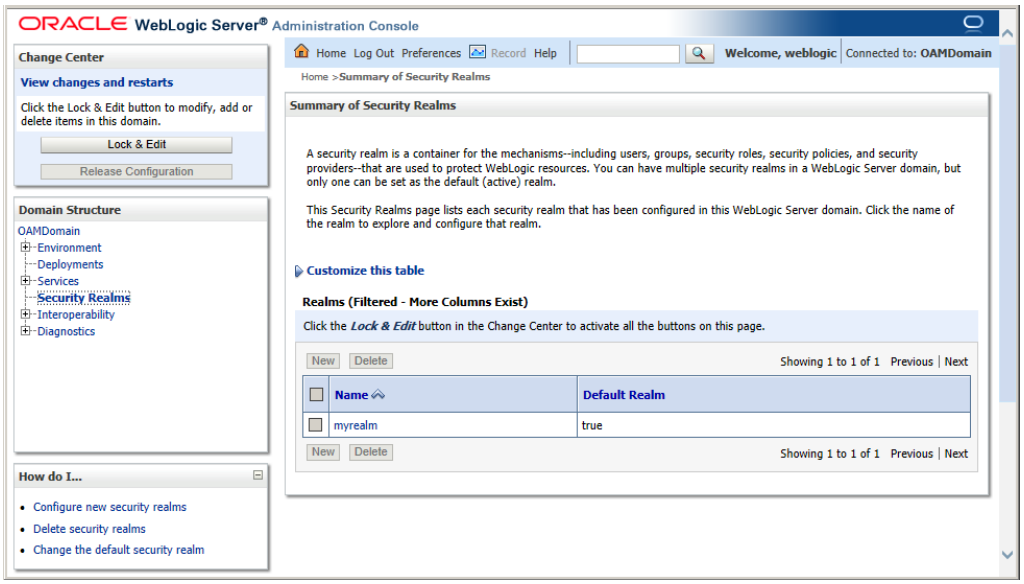
Configure OID and OAM Identity Asserter Providers For OAM

The OID Provider needs to be configured in Oracle Access Manager WebLogic domain.

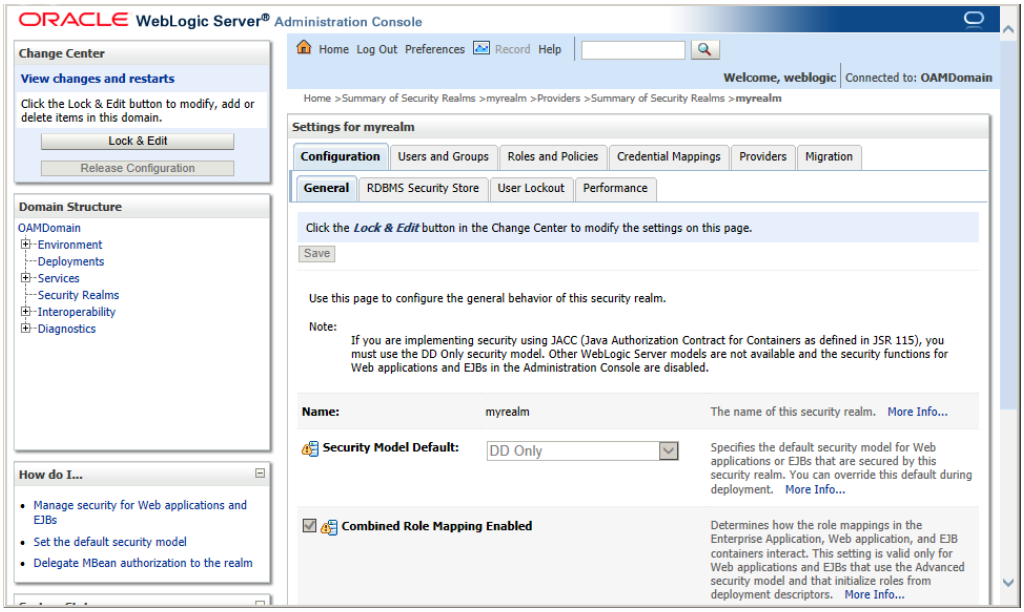
Note: In this section, the base DN "dn=us,dn=oracle,dn=com" is used as an example. Modify this value as per your organization's LDAP settings.

Perform the following procedure to create providers in the domain created in the previous steps.

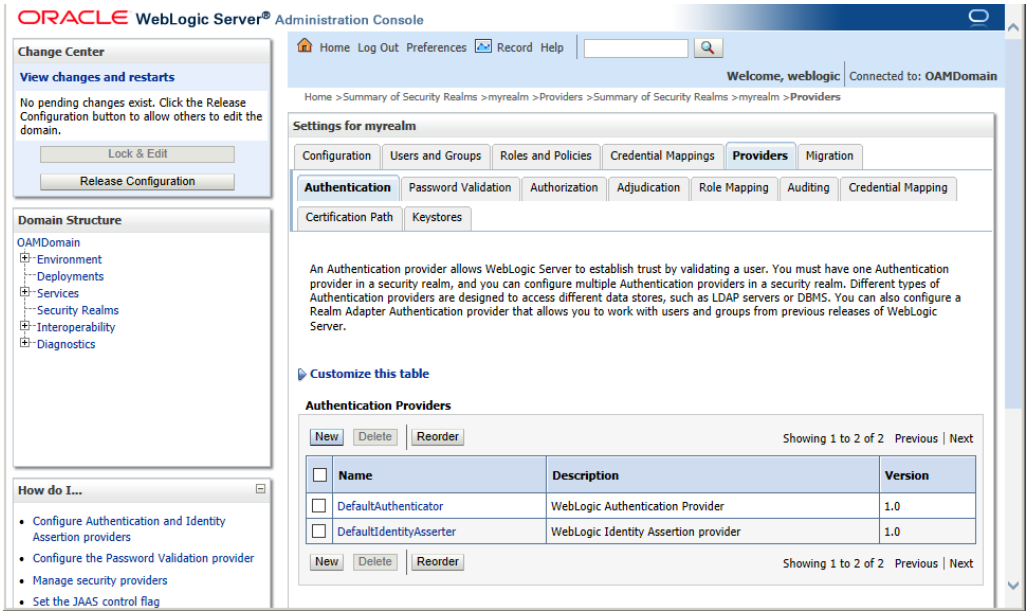
- Login to OAM Administration Server Console running in idmhost1 using Admin user WebLogic. Navigate to OAMDomain > Security Realms. Click **myrealm**.



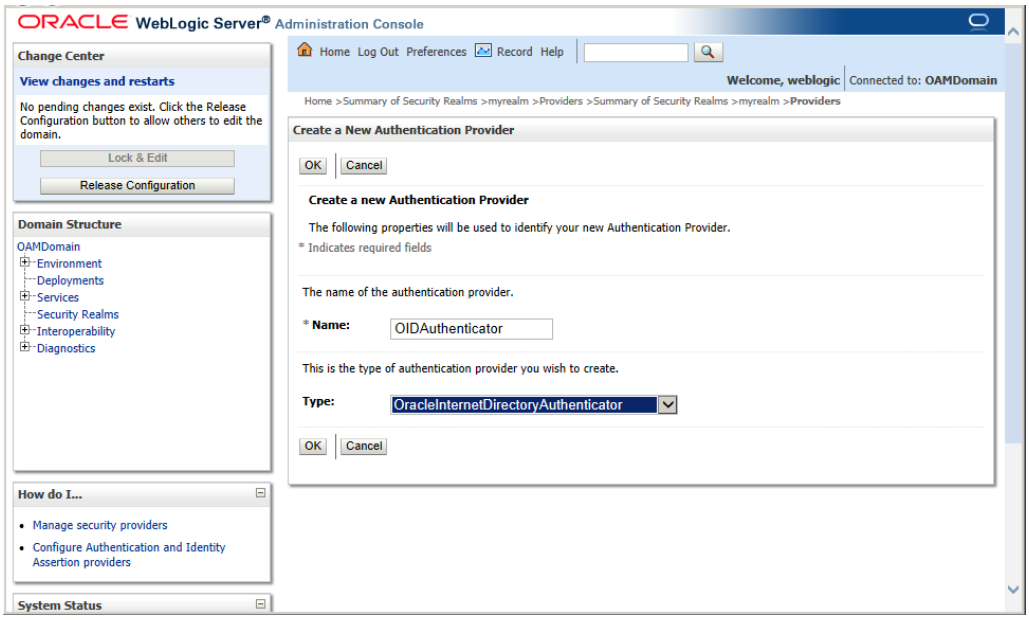
- The Settings for myrealm window opens. Click the **Providers** tab.



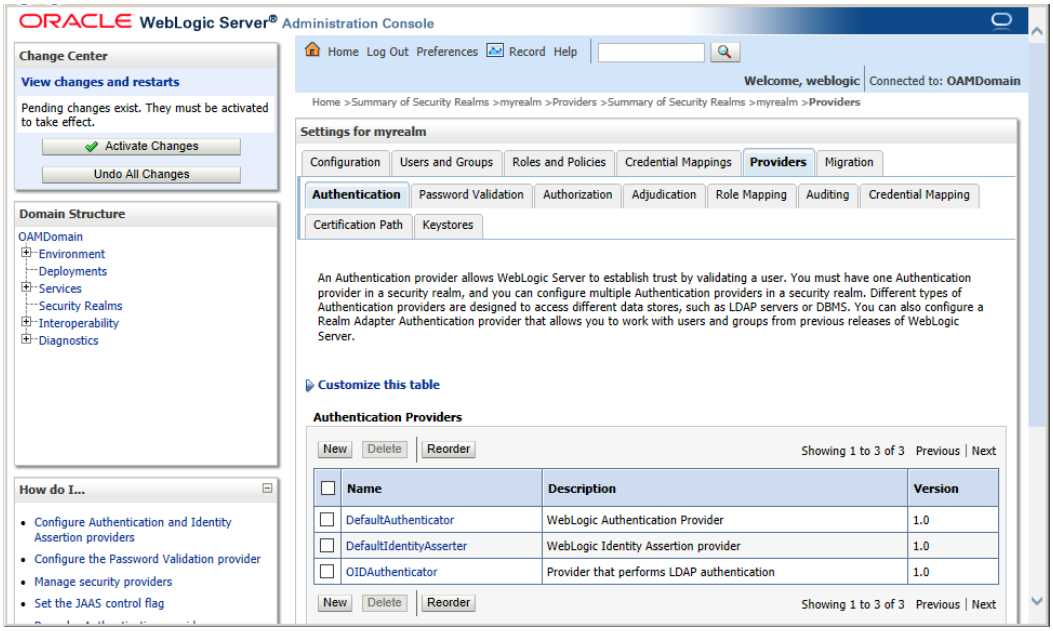
- Click **Lock & Edit** and then click **New**.



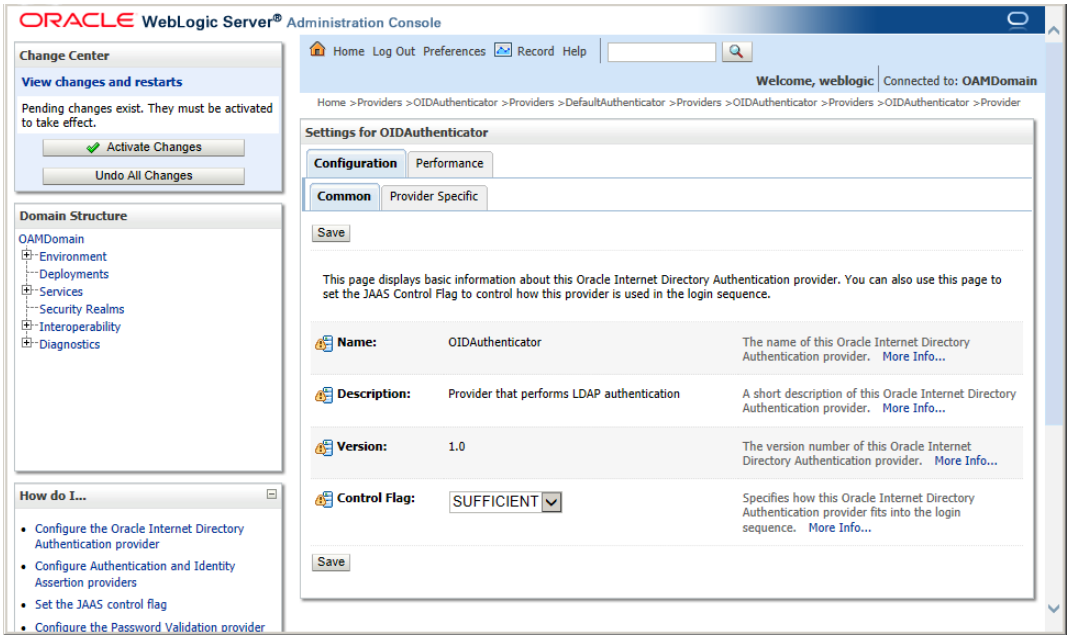
- The Create a New Authentication Provider window opens.
  - Enter OIDAuthenticator in the Name field
  - Select **OracleInternetDirectoryAuthenticator** as the type.
  - Click **OK**.



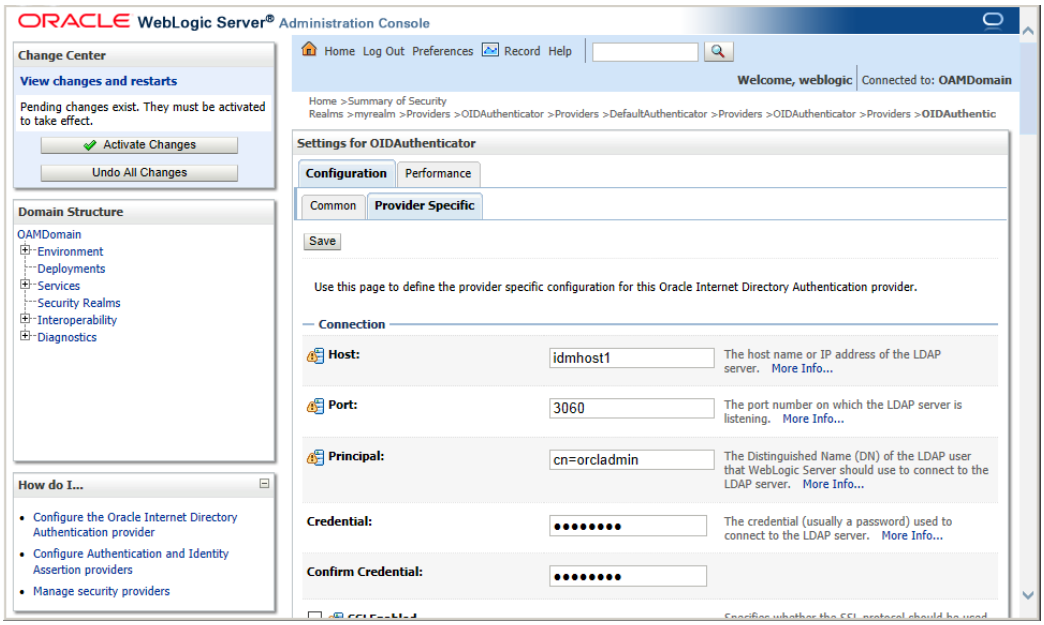
- All the providers are displayed. Click **OIDAuthenticator**.

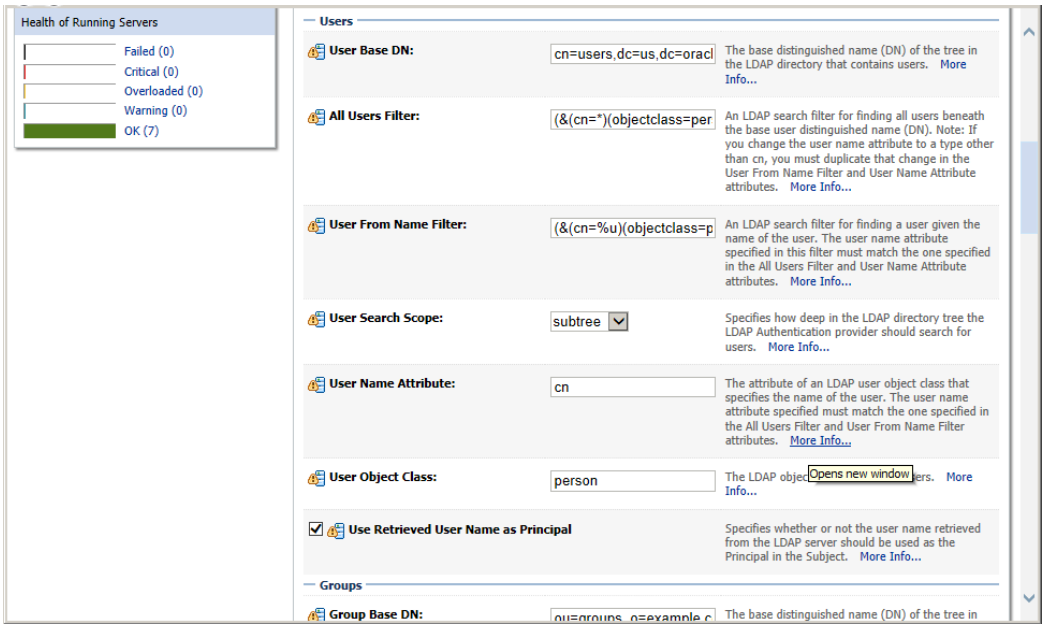


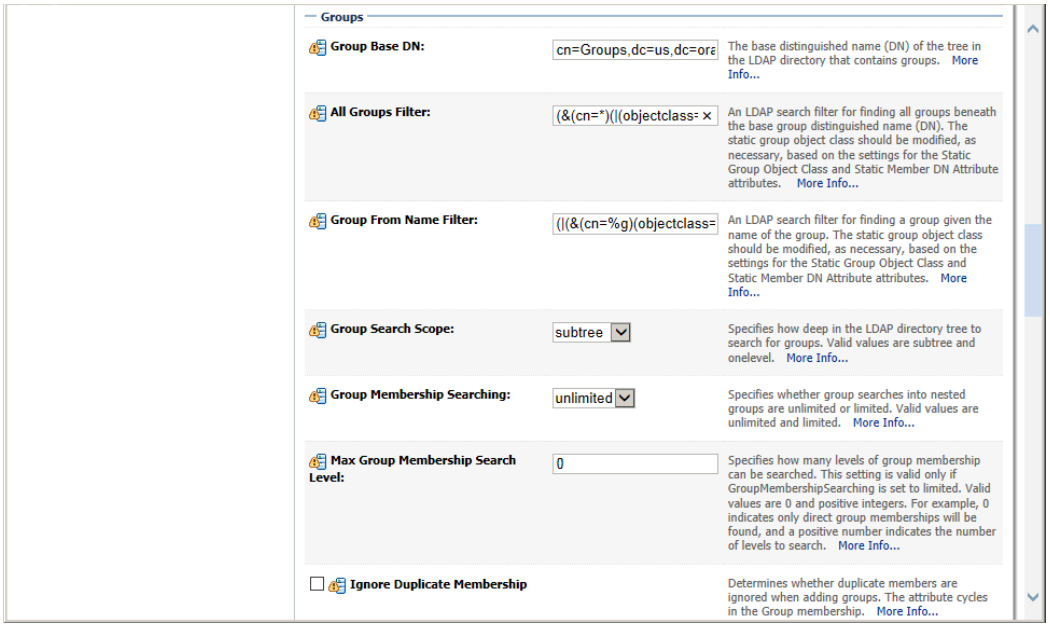
- Settings of OIDAuthenticator are displayed - Set the Control Flag field to SUFFICIENT and click **Save**. Then Click the **Providers** Specific tab.

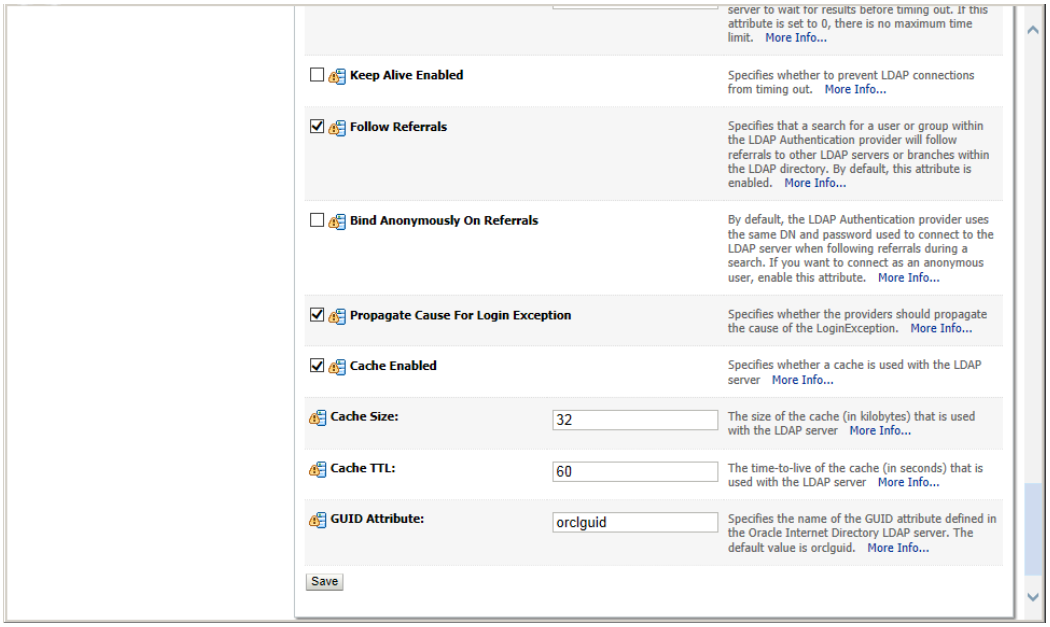


- Make the following changes and Click **Save**. Then click the **Providers** link at the top of screen. (Screen shots shown as it is scrolled down to make the changes.)
  - Host: idmhost1
  - Port: 3060
  - Principal: cn=orcladmin
  - Credential: <password>
  - Confirm Credential: <password>
  - User Base DN: cn=users,dc=us,dc=oracle,dc=com
  - Check 'Retrieve credentials as principal.'
  - Group Base DN: cn=Groups,dc=us,dc=oracle,dc=com
  - Check Propagate Cause For Login Exception

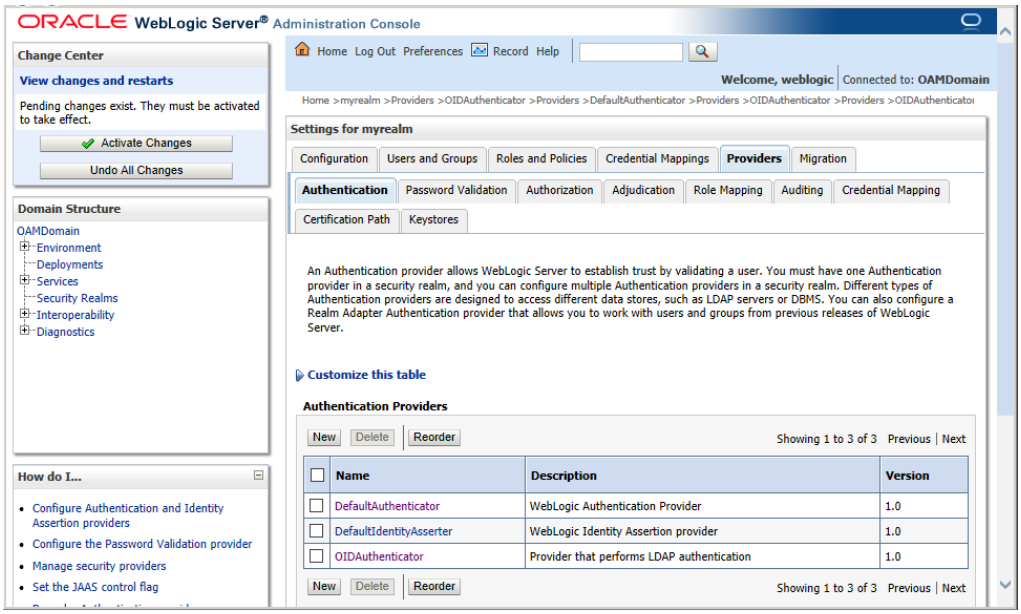



Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (7)
Users
User Base DN:
cn=users,dc=us,dc=oracl
The base distinguished name (DN) of the tree in the LDAP directory that contains users. More Info...
All Users Filter:
(&(cn=*)(objectclass=per
An LDAP search filter for finding all users beneath the base user distinguished name (DN). Note: If you change the user name attribute to a type other than cn, you must duplicate that change in the User From Name Filter and User Name Attribute attributes. More Info...
User From Name Filter:
(&(cn=%u)(objectclass=p
An LDAP search filter for finding a user given the name of the user. The user name attribute specified in this filter must match the one specified in the All Users Filter and User Name Attribute attributes. More Info...
User Search Scope:
subtree
Specifies how deep in the LDAP directory tree the LDAP Authentication provider should search for users. More Info...
User Name Attribute:
cn
The attribute of an LDAP user object class that specifies the name of the user. The user name attribute specified must match the one specified in the All Users Filter and User From Name Filter attributes. More Info...
User Object Class:
person
Opens new window
More Info...
Use Retrieved User Name as Principal
Specifies whether or not the user name retrieved from the LDAP server should be used as the Principal in the Subject. More Info...
Groups
Group Base DN:

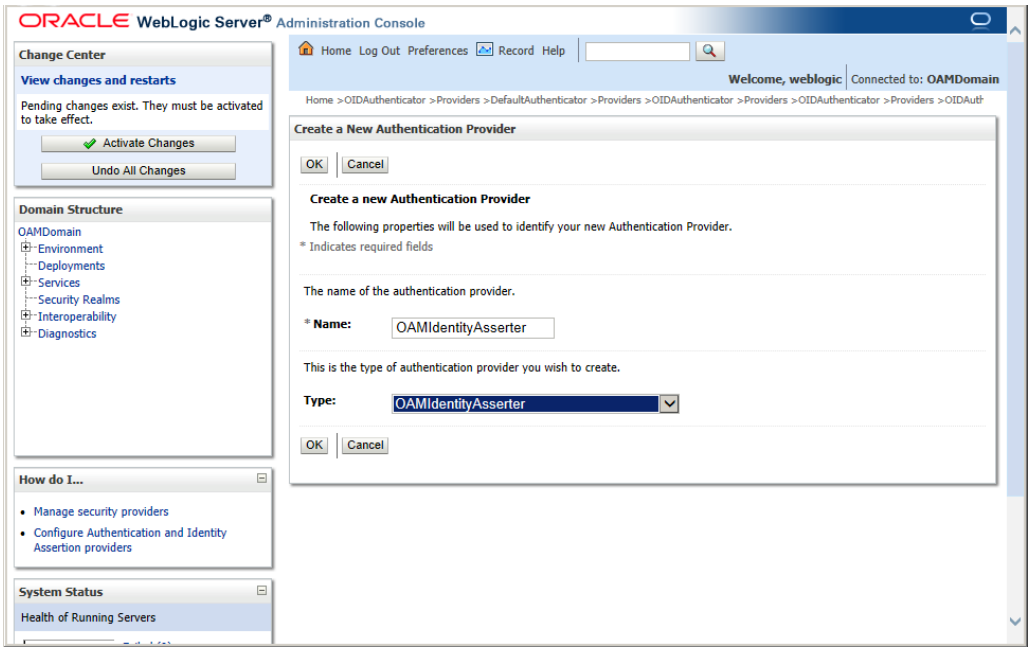

Groups
Group Base DN:
cn=Groups,dc=us,dc=ora
The base distinguished name (DN) of the tree in the LDAP directory that contains groups. More Info...
All Groups Filter:
(&(cn=*)(|(objectclass=
An LDAP search filter for finding all groups beneath the base group distinguished name (DN). The static group object class should be modified, as necessary, based on the settings for the Static Group Object Class and Static Member DN Attribute attributes. More Info...
Group From Name Filter:
(|(&(cn=%g)(objectclass=
An LDAP search filter for finding a group given the name of the group. The static group object class should be modified, as necessary, based on the settings for the Static Group Object Class and Static Member DN Attribute attributes. More Info...
Group Search Scope:
subtree
Specifies how deep in the LDAP directory tree to search for groups. Valid values are subtree and onelevel. More Info...
Group Membership Searching:
unlimited
Specifies whether group searches into nested groups are unlimited or limited. Valid values are unlimited and limited. More Info...
Max Group Membership Search Level:
0
Specifies how many levels of group membership can be searched. This setting is valid only if GroupMembershipSearching is set to limited. Valid values are 0 and positive integers. For example, 0 indicates only direct group memberships will be found, and a positive number indicates the number of levels to search. More Info...
Ignore Duplicate Membership
Determines whether duplicate members are ignored when adding groups. The attribute cycles in the Group membership. More Info...



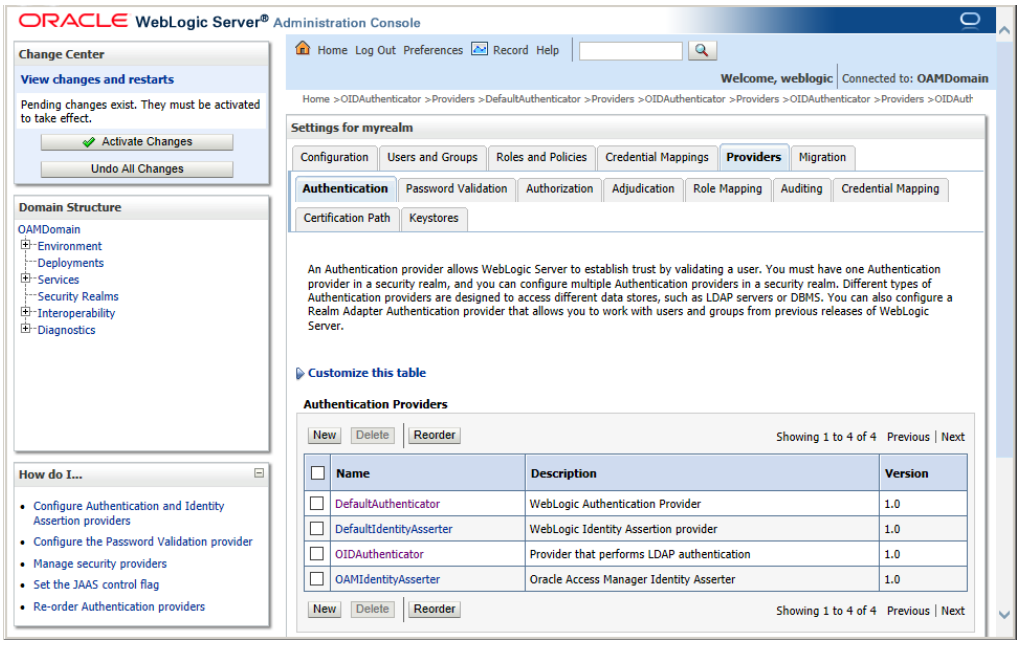
- From the Providers tab, click **New**



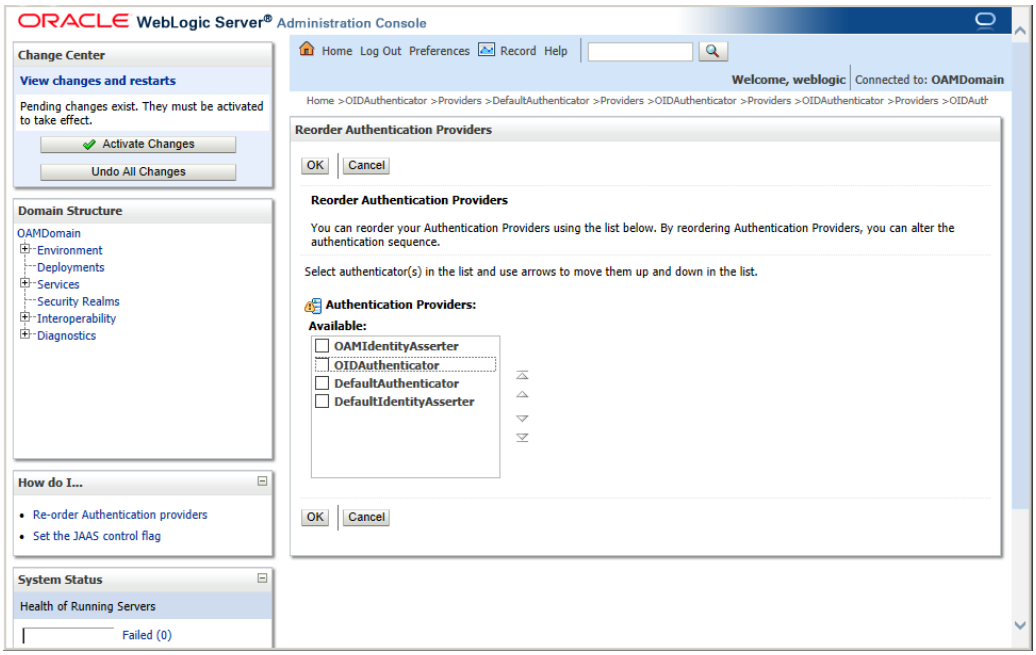
- The Create a New Authentication Provider window opens.
  - Enter OAMIdentityAsserter in the Name field
  - Select **OAMIdentityAsserter** as the type.
  - Click **OK**.



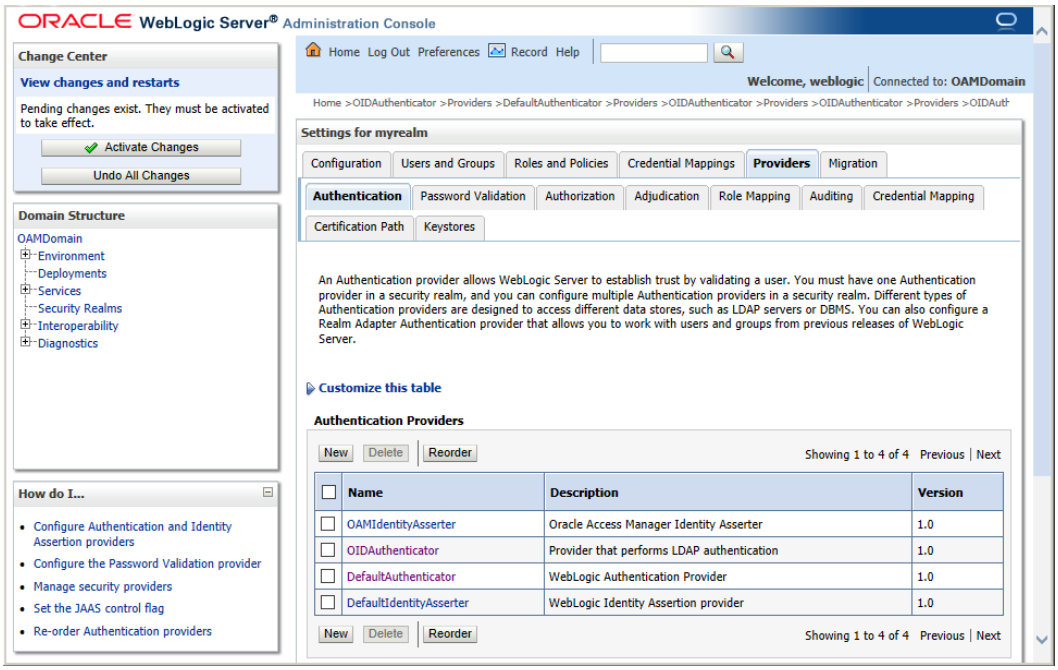
- Click the **Reorder** button.



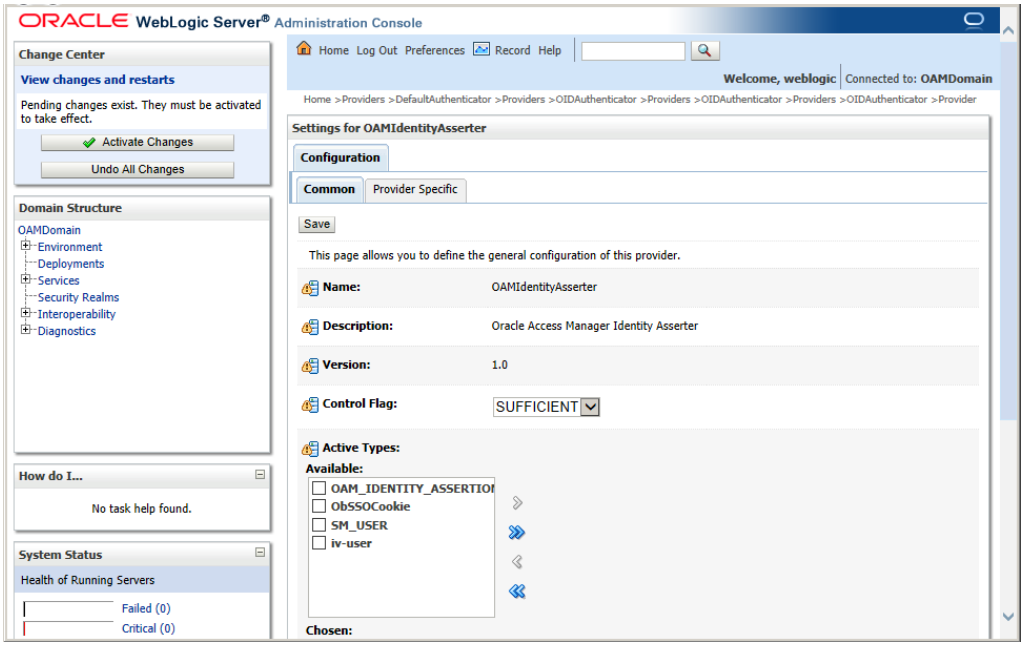
- Move OAMIdentityAsserter and OIDAuthenticator to the top of the list using the arrow buttons, and click **OK**.



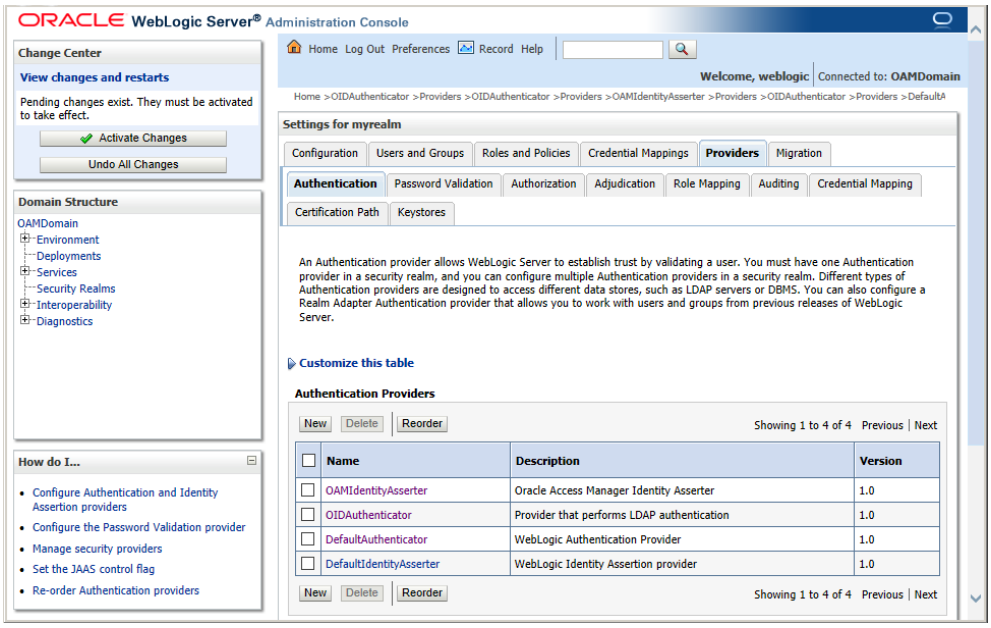
- Click the **OAMIdentiryAsserter** provider link.



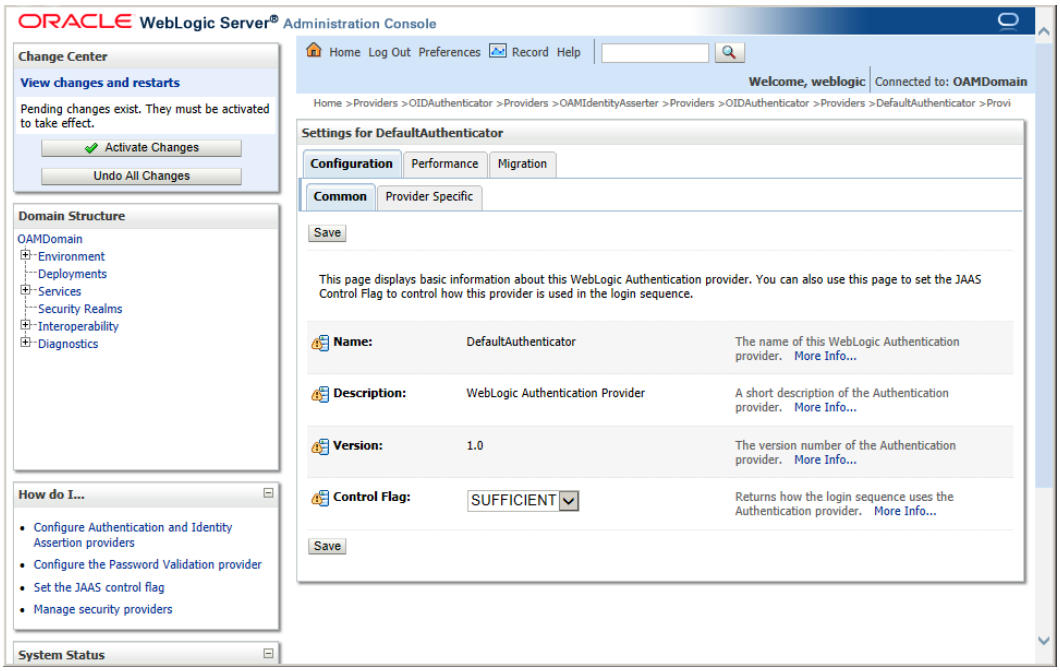
- Select the **SUFFICIENT** control flag , click **Save** and then click the **Provider** link located at the top of the screen.



- Click the **OIDAuthenticator** provider link.



- Select the **SUFFICIENT** control flag, click **Save** and **Activate Changes.**



- Shutdown OAM admin and managed servers and then restart them.

Propagating OAMDomain to idmhost2

Perform the following steps to propogate the OAMDomain from idmhost1 to idmhost2:

- Stop the AdminServer on idmhost1 if not down already.
- Pack the OAMDomain using pack.sh on idmhost1.
  - Export pack.sh to PATH variable.

    Example:
    ```
    $ export
    PATH=/u00/webadmin/products/wls_iam/oracle_common/common/bin:$PATH
    ```

  - Run pack.sh on idmhost1

    Example:
    ```
    $ pack.sh -domain=/u00/webadmin/config/domains/wls_iam/OAMDomain -
    template=/u00/webadmin/config/domains/wls_iam/OAMDomain.jar -
    template_name=OAMDomain -managed=true
    ```

    Output:
    ```
    << read domain from "/u00/webadmin/config/domains/wls_iam/OAMDomain"
    >>  succeed: read domain from
    "/u00/webadmin/config/domains/wls_iam/OAMDomain"
    << set config option Managed to "true"
    >>  succeed: set config option Managed to "true"
    << write template to
    "/u00/webadmin/config/domains/wls_iam/OAMDomain.jar"
    ..........................................................................
    ............................
    >>  succeed: write template to
    "/u00/webadmin/config/domains/wls_iam/OAMDomain.jar"
    << close template
    >>  succeed: close template
    ```

- Logged into idmhost2 - Copy the OAMDomain.jar from idmhost1 to directory that where the OAMDomain should be placed on idmhost2

Example:
```
$ mkdir -p /u00/webadmin/config/domains/wls_iam
$ cd /u00/webadmin/config/domains/wls_iam
$ scp -r
webadmin@idmhost1:/u00/webadmin/config/domains/wls_iam/OAMDomain.jar .
```

- Un-pack the OAMDomain on idmhost2 using unpack.sh
  - Export unpack.sh to PATH variable onidmhost2

    Example:
    ```
    $ export
    PATH=/u00/webadmin/products/wls_iam/oracle_common/common/bin:$PATH
    ```
  - Run unpack.sh on idmhost2

    Example:
    ```
    $ unpack.sh -domain=/u00/webadmin/config/domains/wls_iam/OAMDomain -
    template=/u00/webadmin/config/domains/wls_iam/OAMDomain.jar -
    overwrite_domain=true -
    app_dir=/u00/webadmin/config/applications/wls_iam/OAMDomain
    ```

    Output:
    ```
    << read template from
    "/u00/webadmin/config/domains/wls_iam/OAMDomain.jar"
    >>  succeed: read template from
    "/u00/webadmin/config/domains/wls_iam/OAMDomain.jar"
    << set config option OverwriteDomain to "true"
    >>  succeed: set config option OverwriteDomain to "true"
    << set config option AppDir to
    "/u00/webadmin/config/applications/wls_iam/OAMDomain"
    >>  succeed: set config option AppDir to
    "/u00/webadmin/config/applications/wls_iam/OAMDomain"
    << set config option DomainName to "OAMDomain"
    >>  succeed: set config option DomainName to "OAMDomain"
    << write Domain to "/u00/webadmin/config/domains/wls_iam/OAMDomain"
    ..................................................................
    ......................
    >>  succeed: write Domain to
    "/u00/webadmin/config/domains/wls_iam/OAMDomain"
    << close template
    >>  succeed: close template
    ```

Start OAMDomain - Admin and Managed Servers

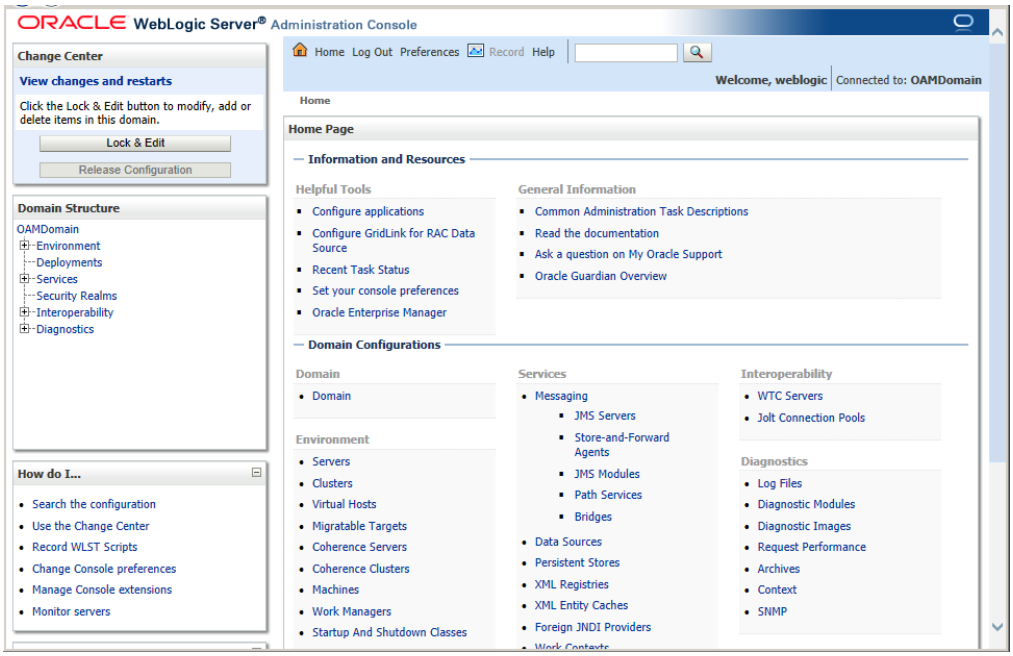
The following section describes the procedure to start OAMDomain and managed servers.

The domain copy that was just completed in the previous step copies the contents of the domain from idmhost1 to idmhost2, however the AdminServer will only run from idmhost1.

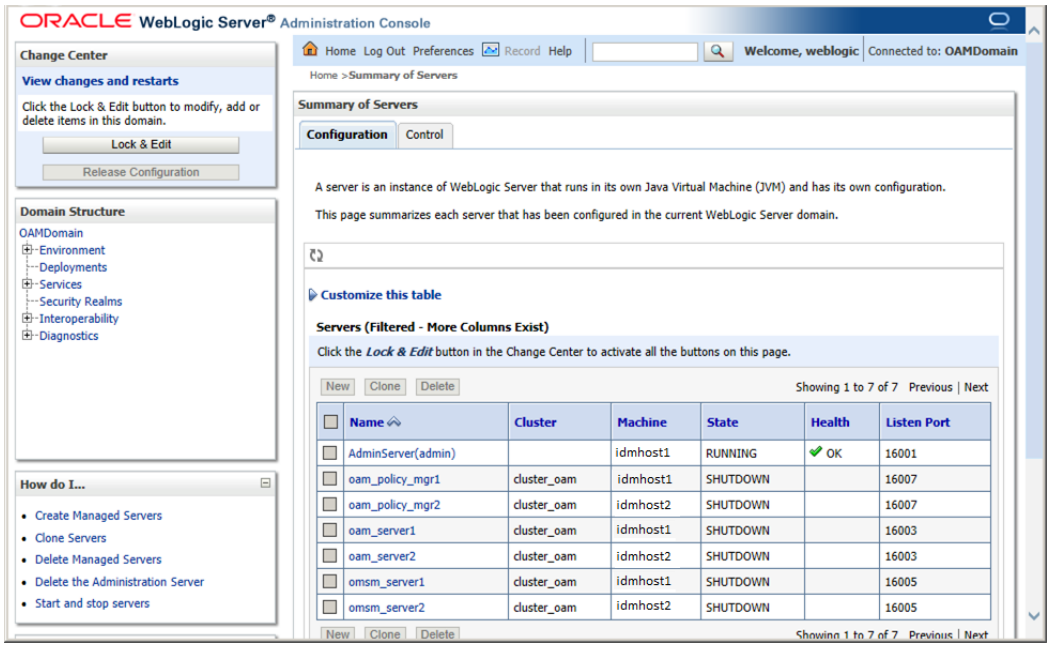
- Start the WebLogic admin server on idmhost1 id it is not already running.

  Example:
  ```
  $ cd /u00/webadmin/config/domains/wls_iam/OAMDomain/bin
  $ nohup ./startWebLogic.sh &
  ```
- Log into the Admin console.

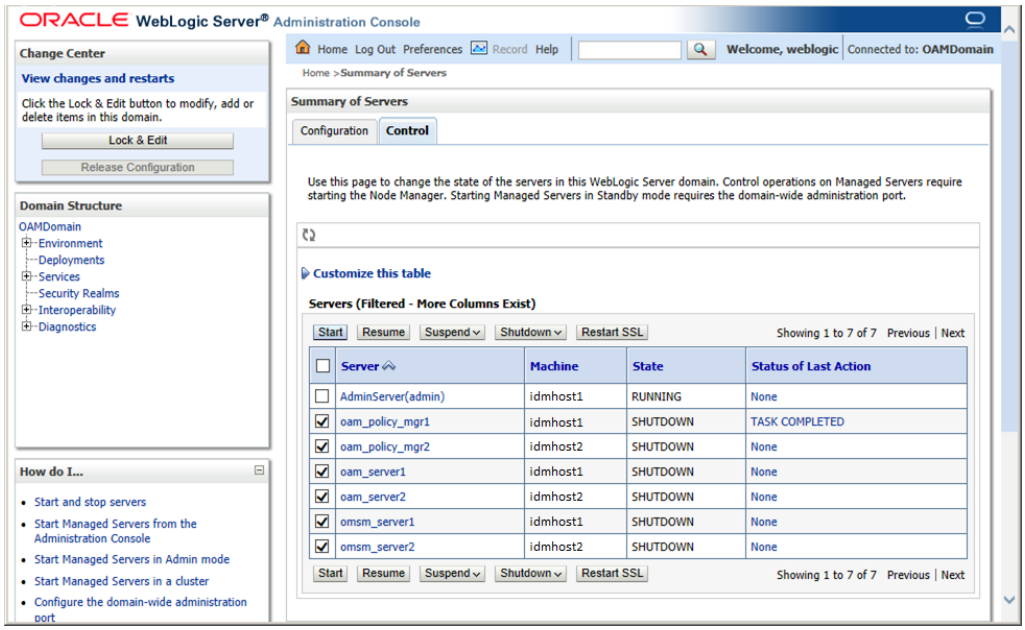
- The WebLogic Home window opens. Click the **Servers** link.



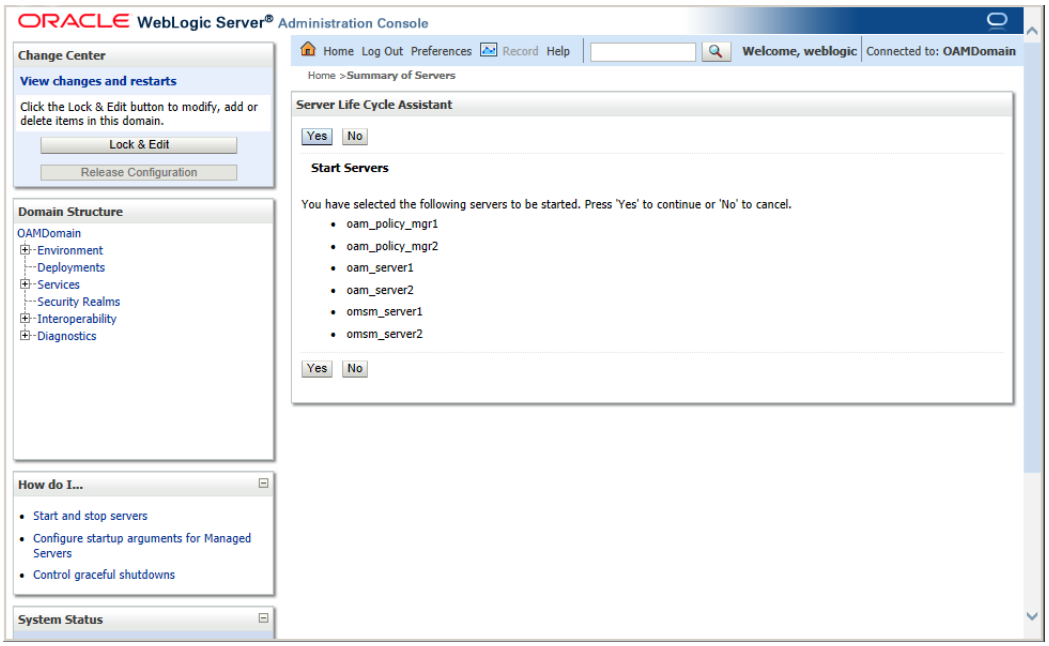
- The Summary of Servers window opens. Click the **Control** tab.



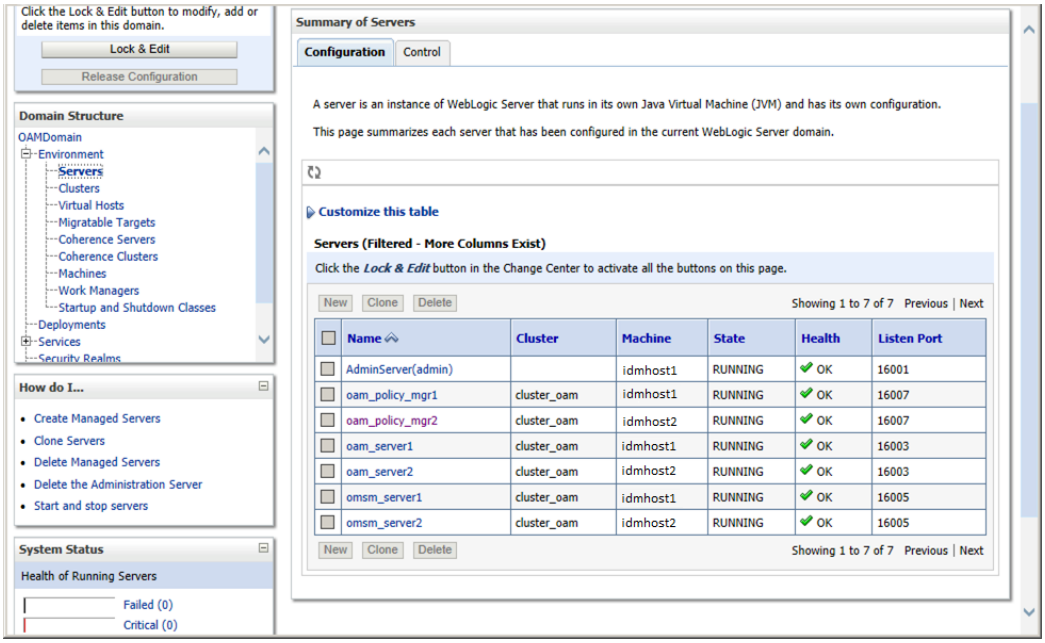
- The Summary of Servers Control window opens.
  - Select all the servers that are in the SHUTDOWN State.
  - Click **Start**.



- The Server Life Cycle Assistant window opens. Click **Yes** to start the managed servers.



- The Summary of Servers Control window opens again. Initially the status of all the servers will be STARTING. Upon refreshing the screen, the status will eventually be updated to RUNNING.
  - If the managed servers fail to start – Review your setup and fix the issues before continuing.

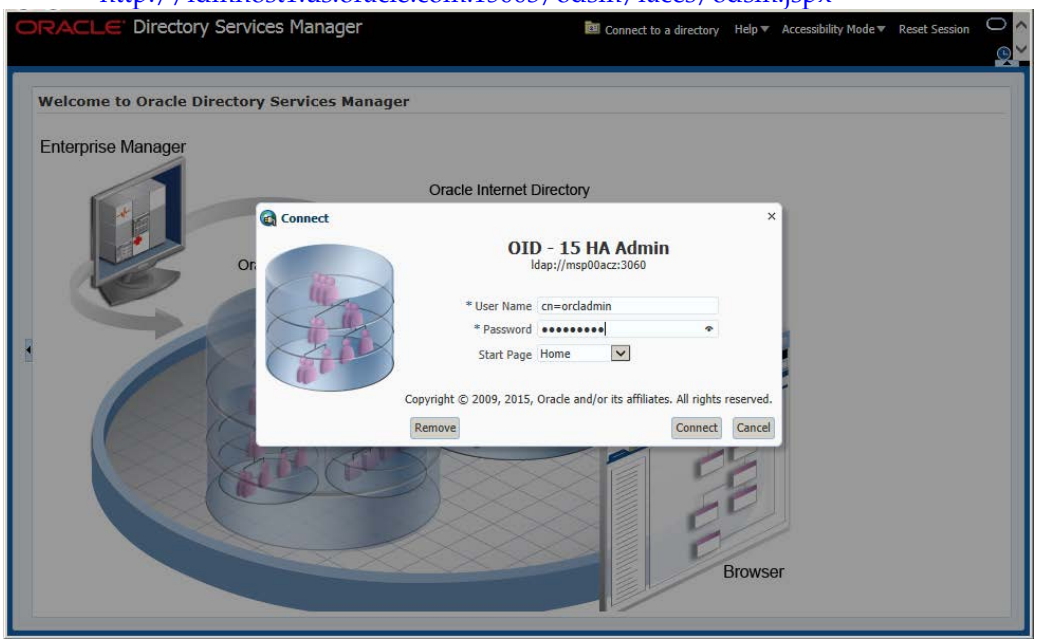


Creating Administrators Group in OID for OAM Identity Store

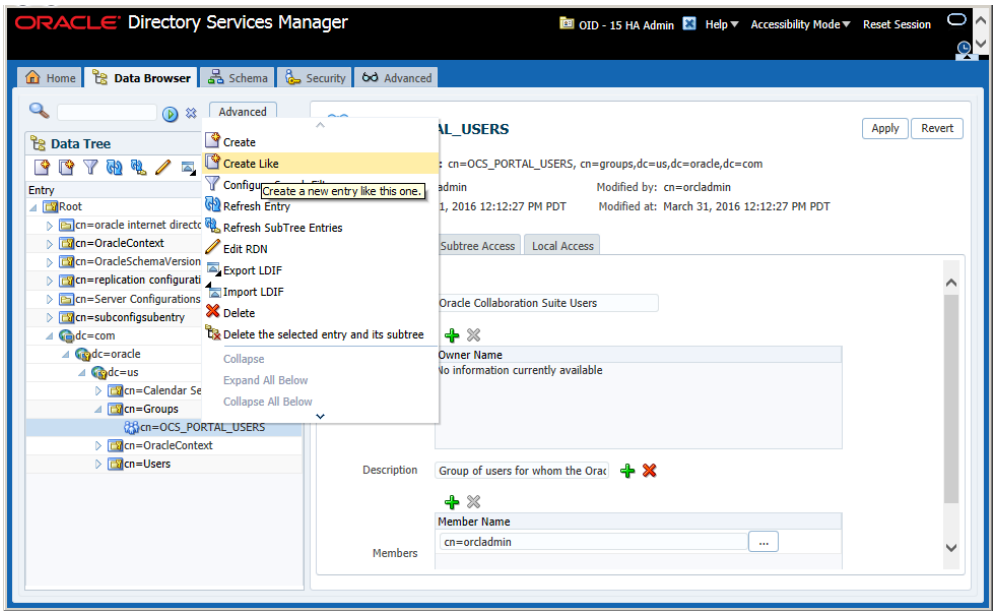
To create an administrators group:

- Connect to ODSM with the cn=orcladmin user and create Administrators group in OID.

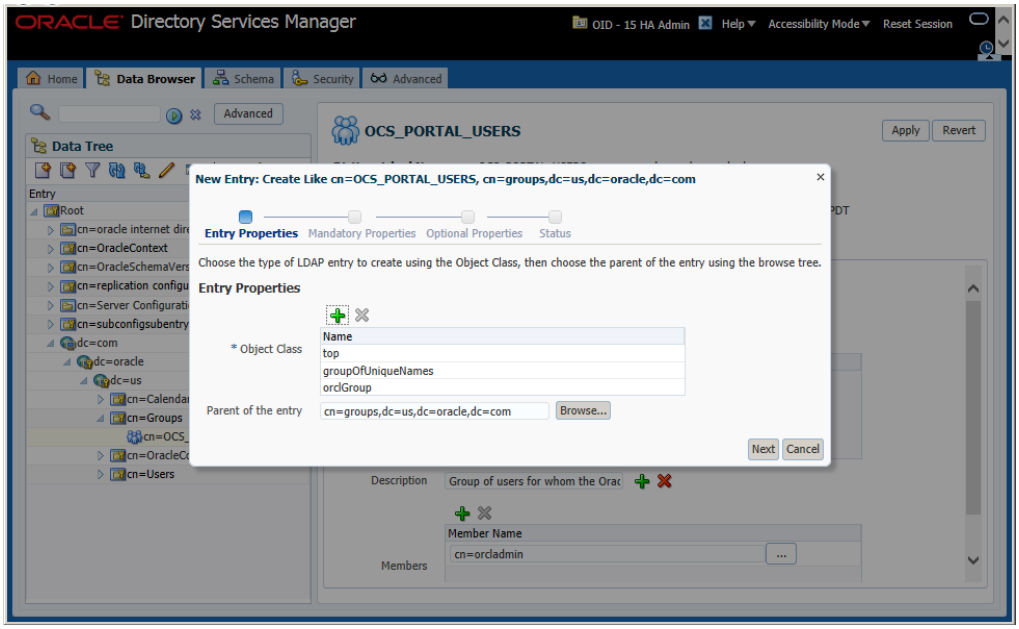
http://idmhost1.us.oracle.com:15003/odsm/faces/odsm.jspx



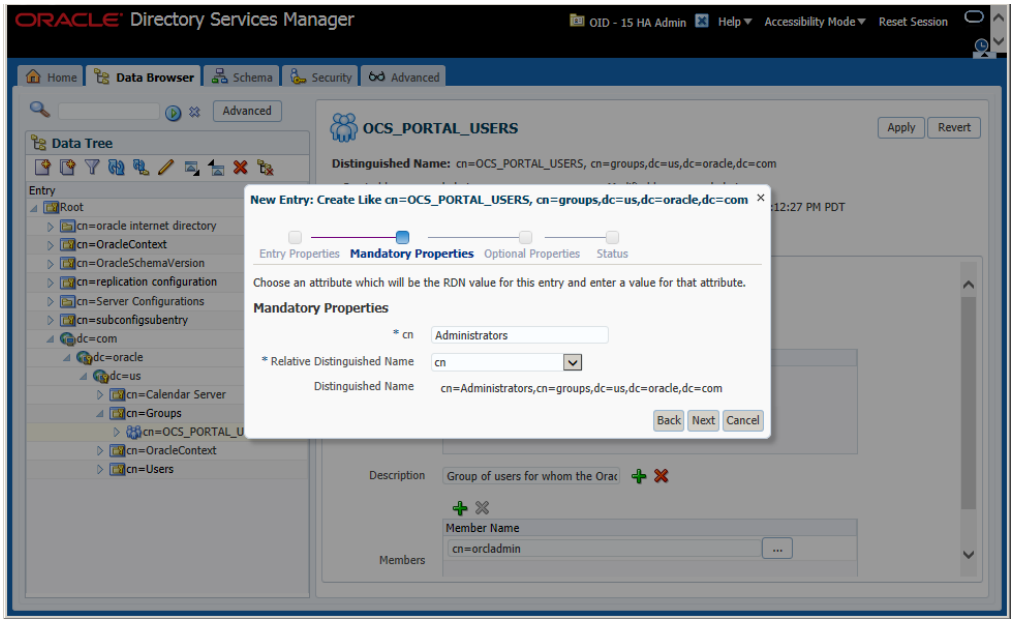
- The Home Page window opens.
  - Click the **Data Browser** tab.
  - Expand the Data Tree dc=com - dc=oracle - dc=us - cn=groups
  - Right-click **OCS_PORTAL_USERS**.
  - Select **Create Like**.



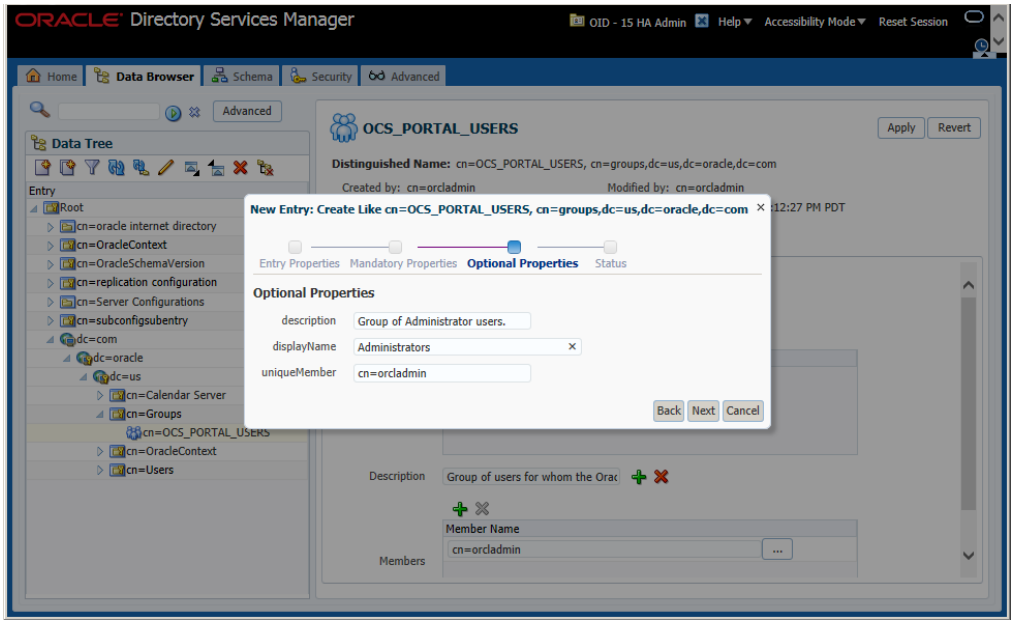
  - The Create Administrators Group: Entry Properties window opens. Click **Next**.



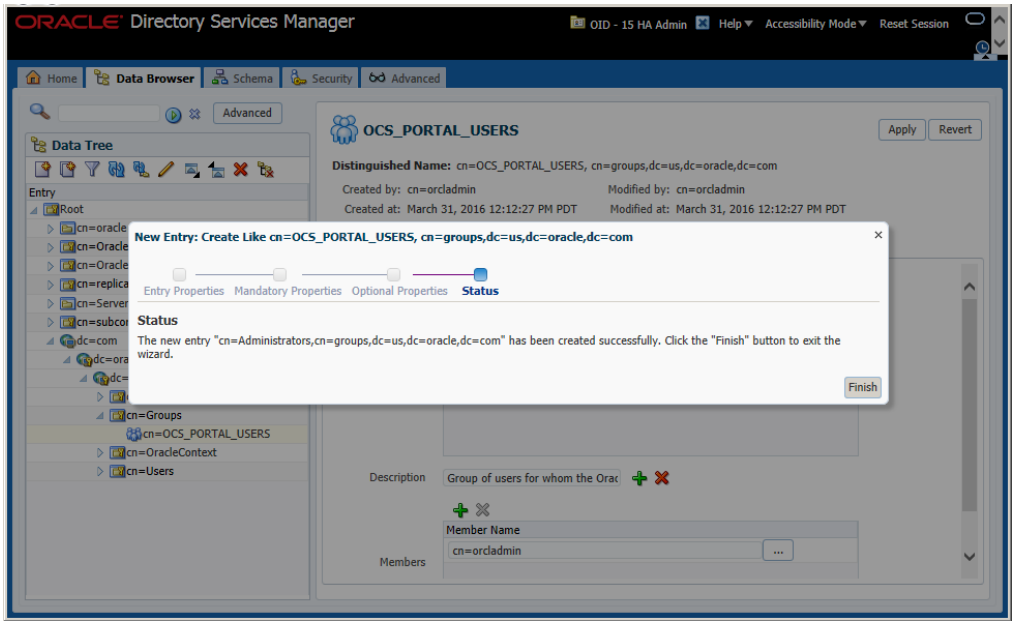
- The Create Administrators Group: Mandatory Properties window opens. Enter in the following:
  - *cn= Administrators
  - *Relative Distinguished Name= cn
  - Click **Next**



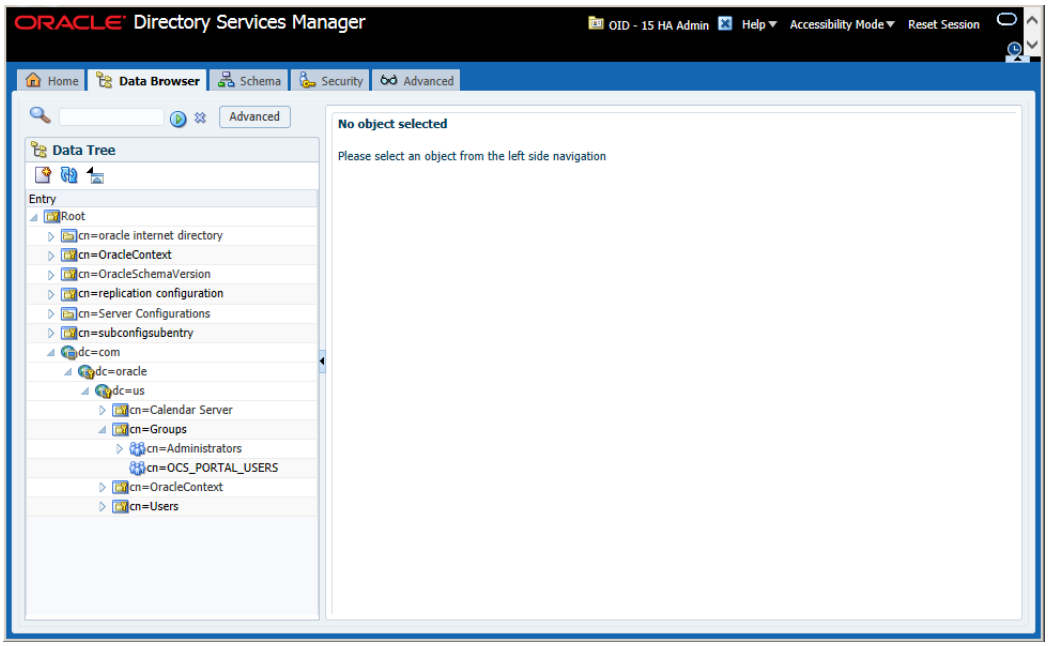
- The Create Administrators Group: Optional Properties window opens. Enter in the following:
  - Description= Group of Administrative users.
  - DisplayName= Administrators
  - uniqueMember= cn= orcladmin
  - Click **Next.**



- The Create Administrators Group: Status window opens. Click **Finish**.



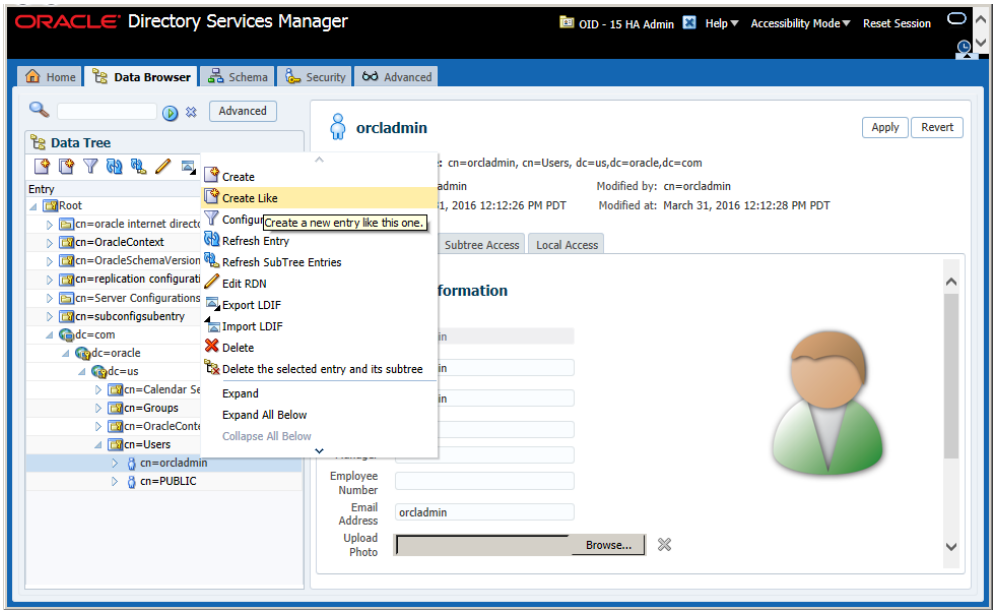
- The Main window opens and Administrators group is shown in the left hand navigation pane.



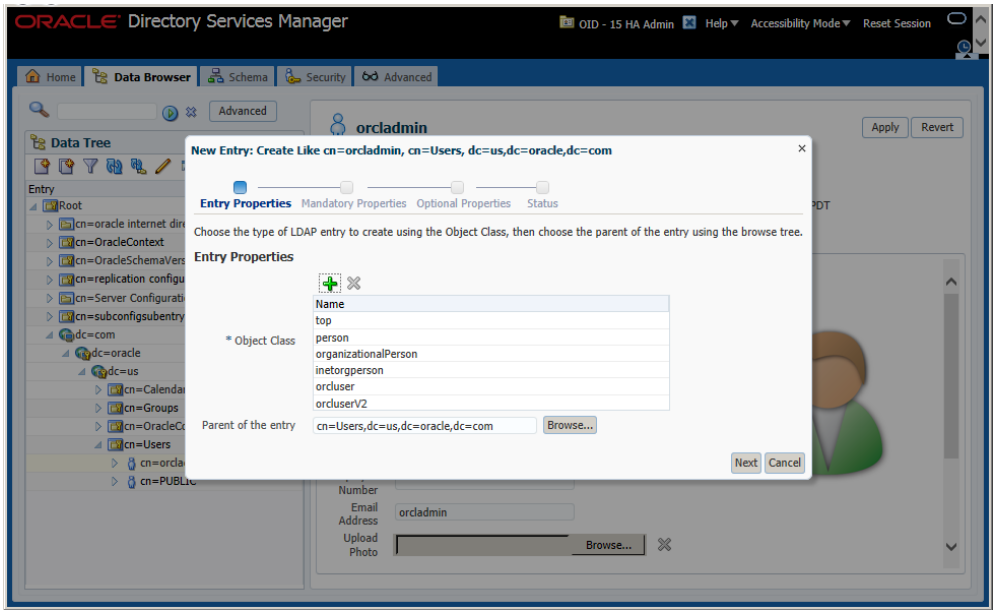
Create a WebLogic Admin User in OID

Create a WebLogic admin user in OID by doing the following:

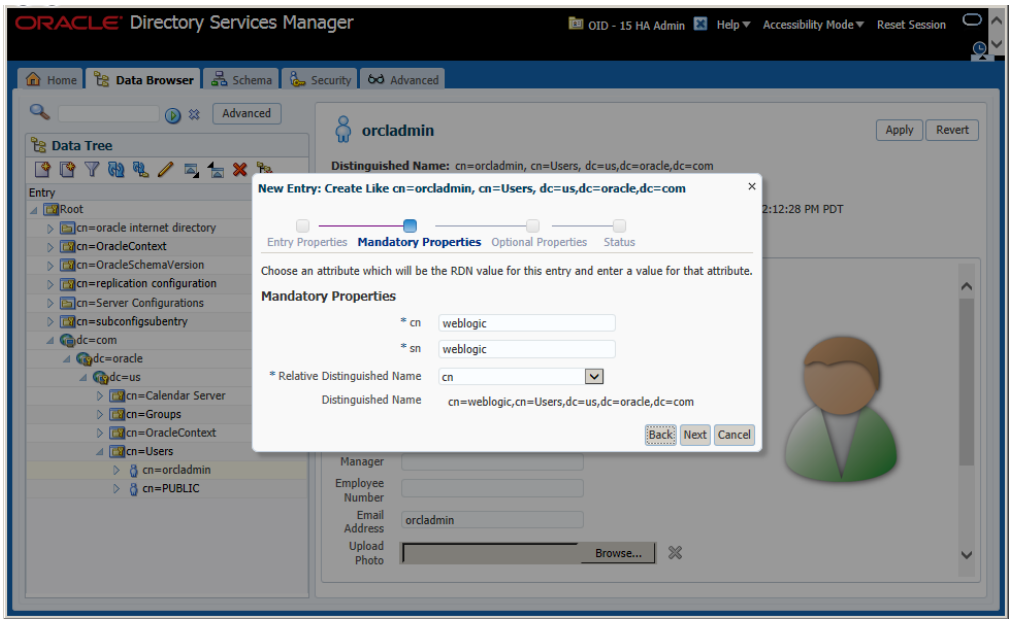
- In the left navigation pane, click **dc=com, dc=oracle, dc=us, and then cn=Users**.
- Right-click **cn=orcladmin** and select **Create Like cn=orcladmin** to create a WebLogic admin user.



- The Create WebLogic User: Entry Properties window opens. Click **Next**.

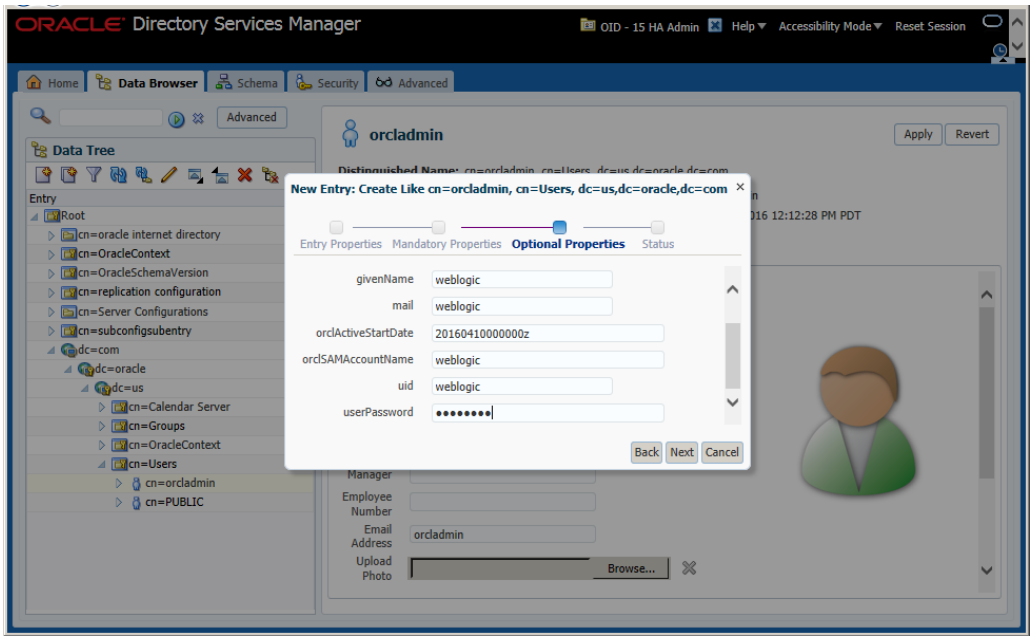


- The Create WebLogic User: Mandatory Properties window opens. Enter in the following values:
  - *cn= weblogic
  - *sn= weblogic
  - *Relative Distinguished Name= cn
  - Click **Next**

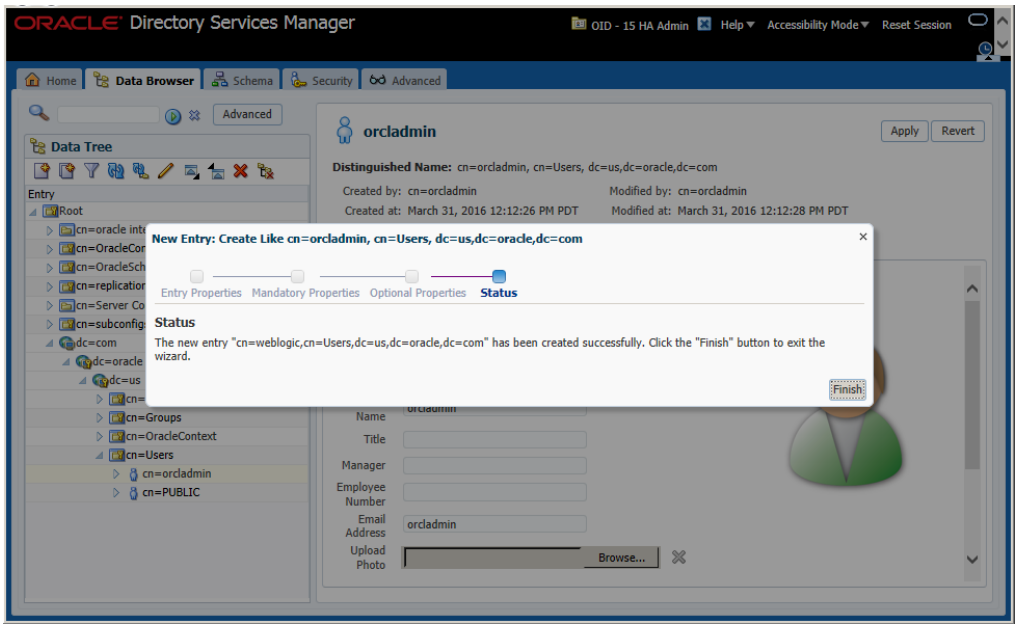


- The Create WebLogic User: Optional Properties window opens. Enter in the following values:
  - givenName= weblogic
  - mail= weblogic
  - orclAvtiveStartDate= Leave as default value
  - orclSAMAccountName= weblogic

- uid= weblogic
- userPassword= <weblogic_password>
- Click **Next**



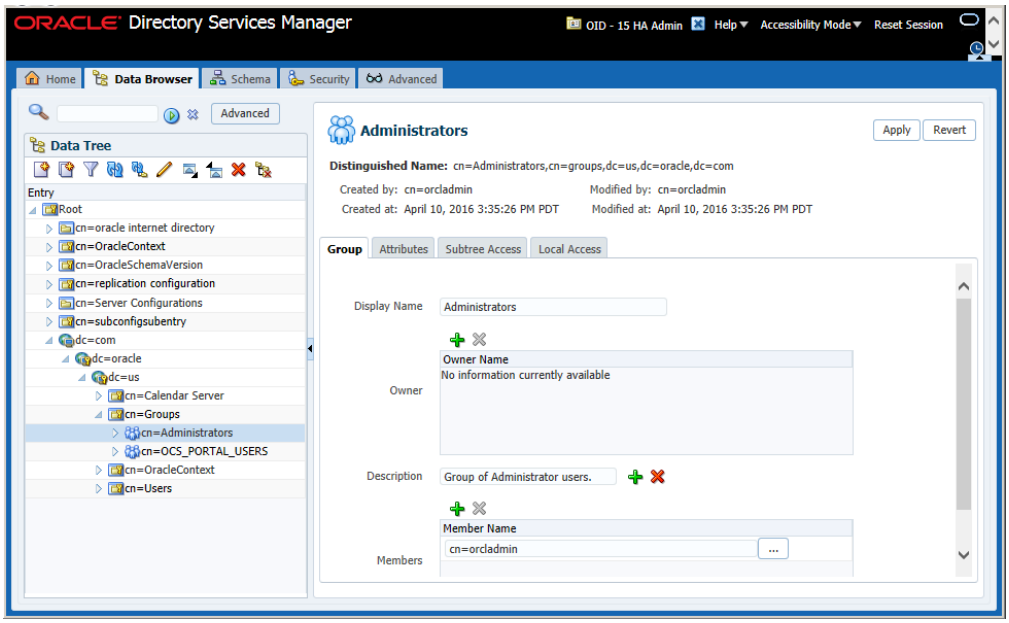
- The Create WebLogic User: Status window opens. Click **Finish**.



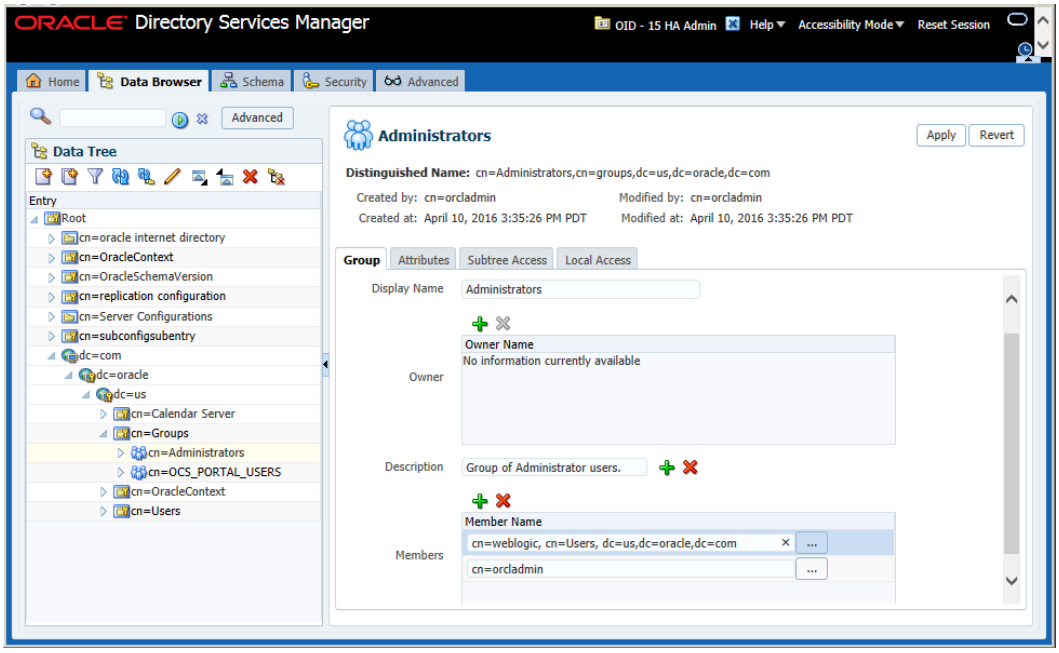
Add orcladmin and WebLogic Admin Users to the Administrators Group

Add orcladmin and WebLogic admin users to the administrators group by doing the following:

- In the **Data Browser** tab - expand the Data Tree dc=com - dc=oracle - dc=us - cn=groups and click on cn=Administrators. The Administrators properties window opens. Click the **Plus** icon to add a member.



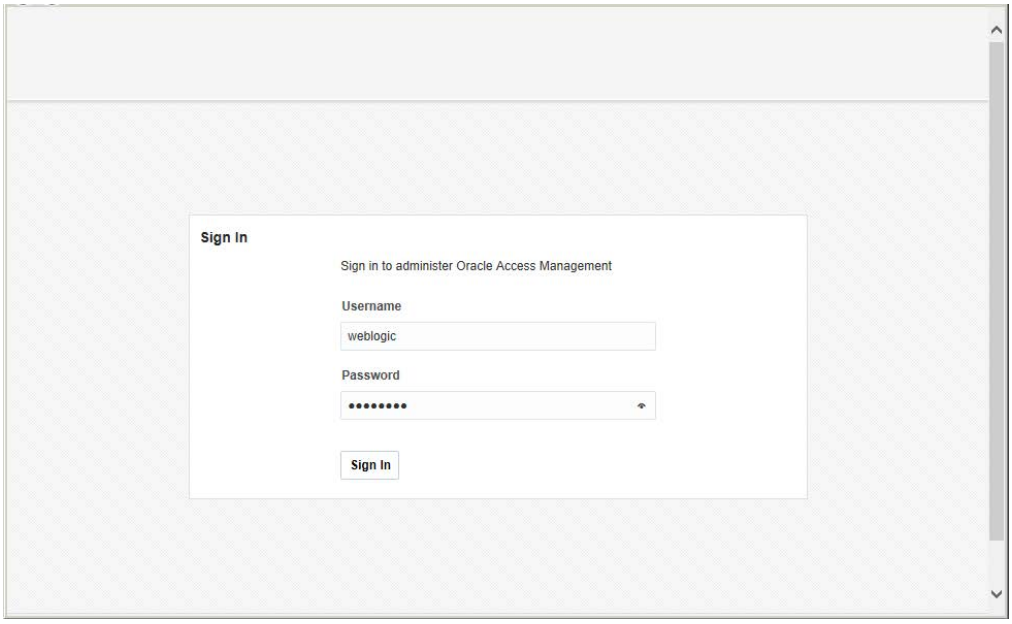
- Another row is added to the Members section of the screen. Enter the following:
  - cn=weblogic,cn=users,dc=us,dc=oracle,dc=com
  - Click the **Apply**.



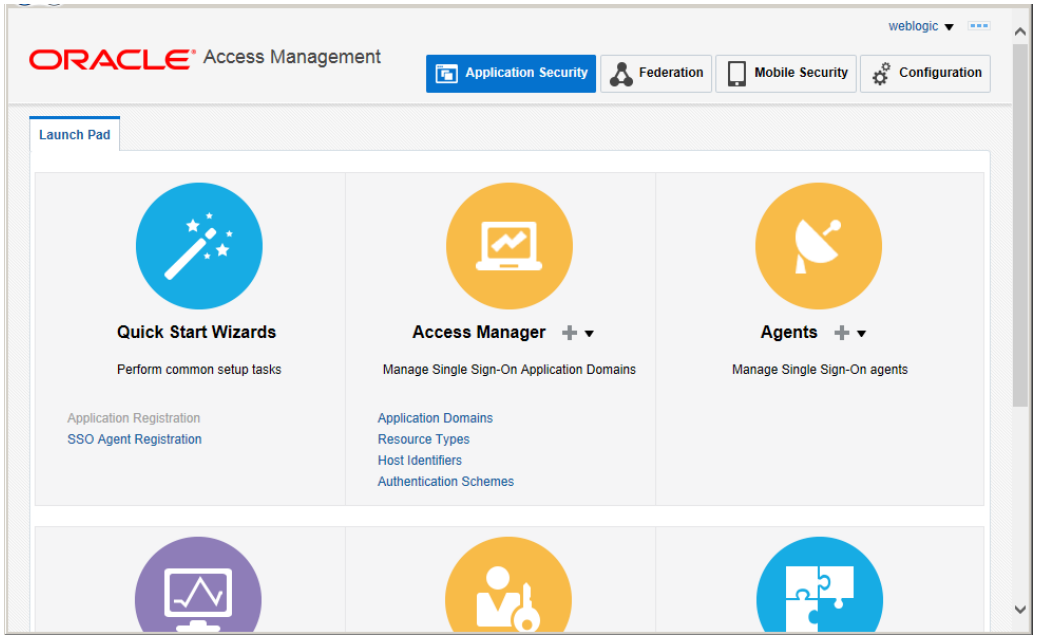
Launching OAMConsole and Configuring Identity Store

To launch the OAMConsole and configure the identity store perform the following steps:

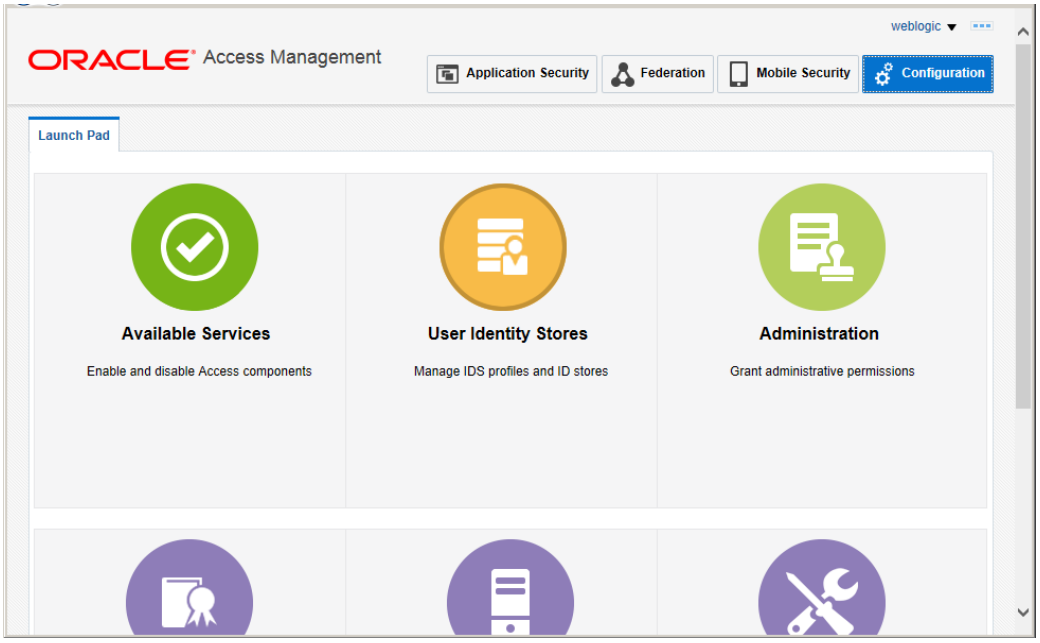
- Launch OAMConsole http://idmhost1.us.oracle.com:16001/oamconsole and login using WebLogic admin user.



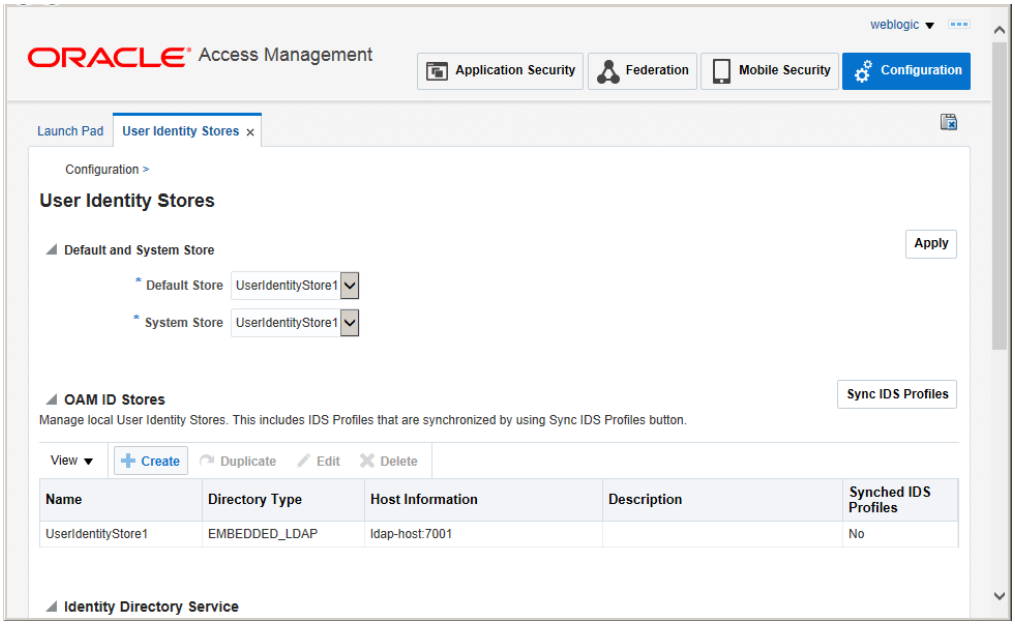
- The Access Management Launch window opens. Click **Configuration**.



- The Access Management Launch page is displayed with different options. Click **User Identity Stores**.

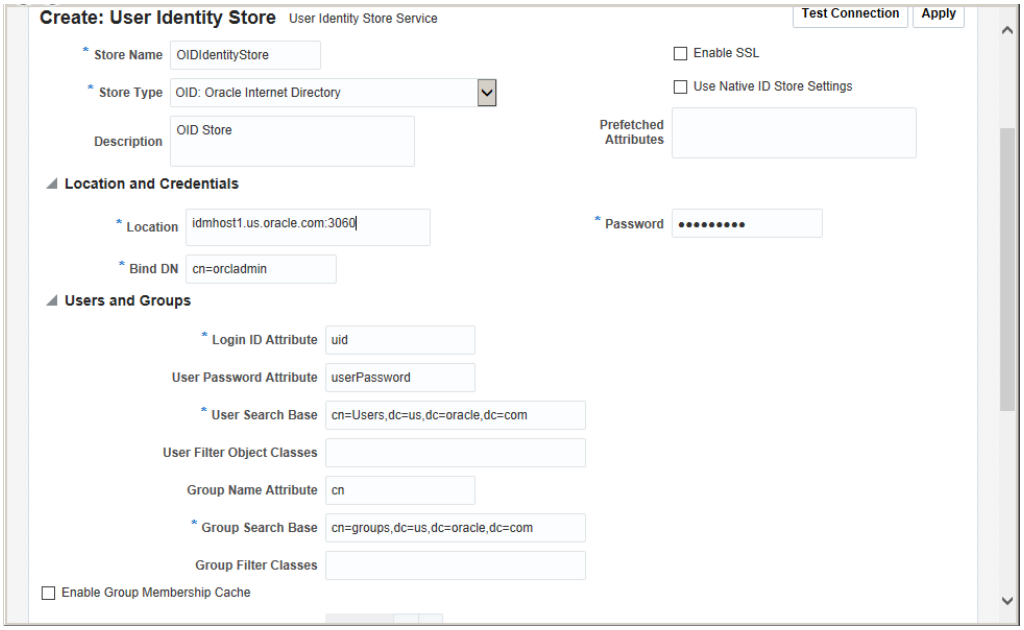


- The User Identity Stores tab opens. Click the **Create** button in the OAM ID Stores section.

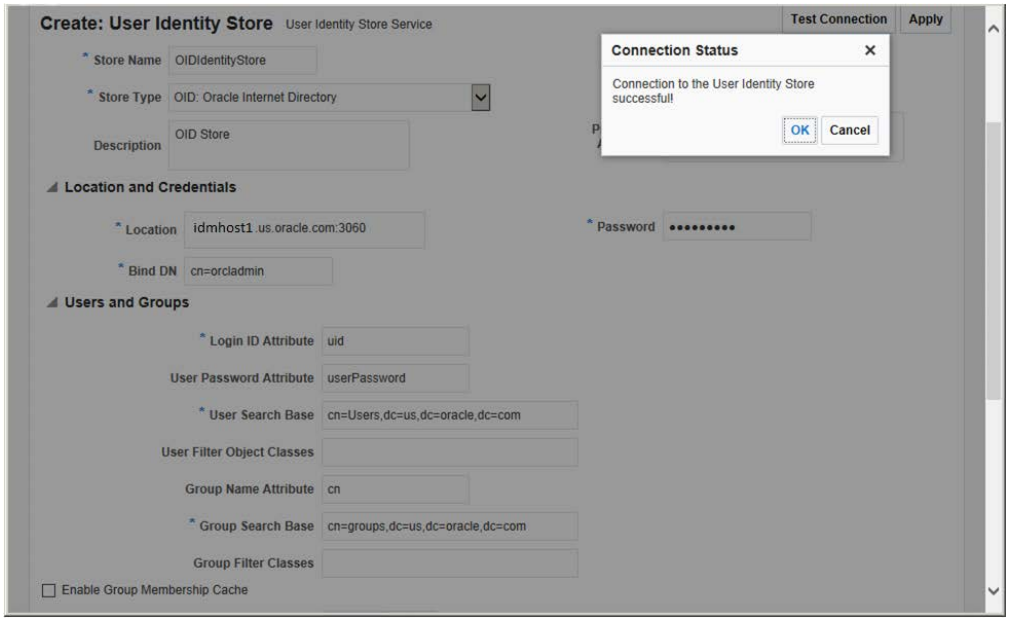


- The Create: User Identity Store window opens. Enter the following values:
  - Store Name= OIDIdentityStore
  - Store Type= OID: Oracle Internet Directory
  - Location= idmhost1.us.oracle.com:3060
  - Bind DN= cn=orcladmin
  - Password= <password>
  - Login ID Attribute= uid
  - User Password Attribute= userPassword
  - User Search Base= cn=Users,dc=us,dc=oracle,dc=com

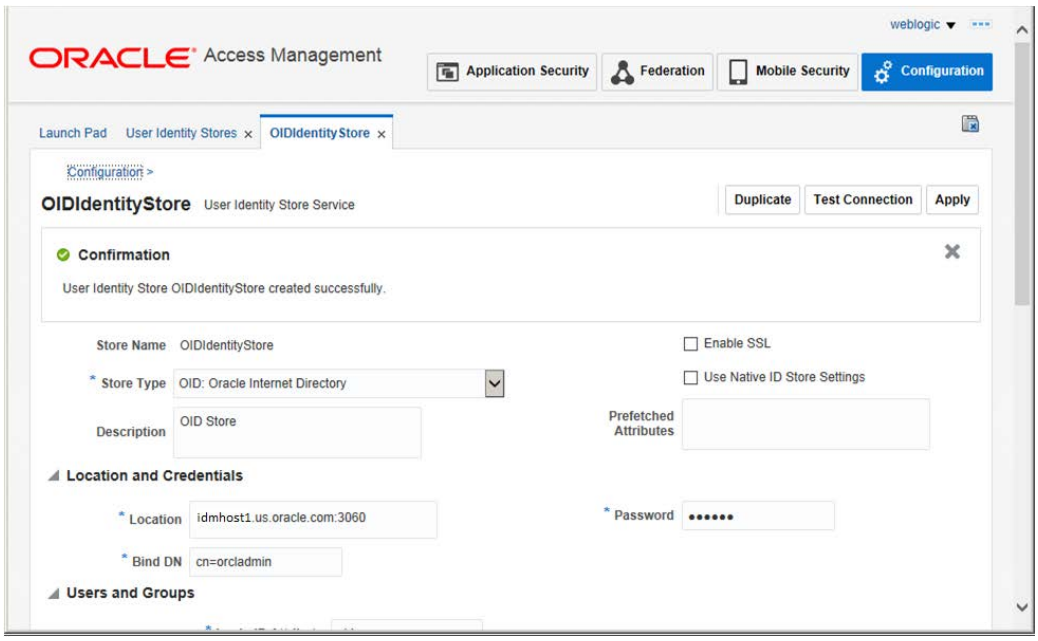
- Group Name Attribute= cn
- Group Search Base= cn=groups,dc=us,dc=oracle,dc=com
- Leave rest as default
- Click **Test Connection**



- The Connection Status window opens. Click **OK**.



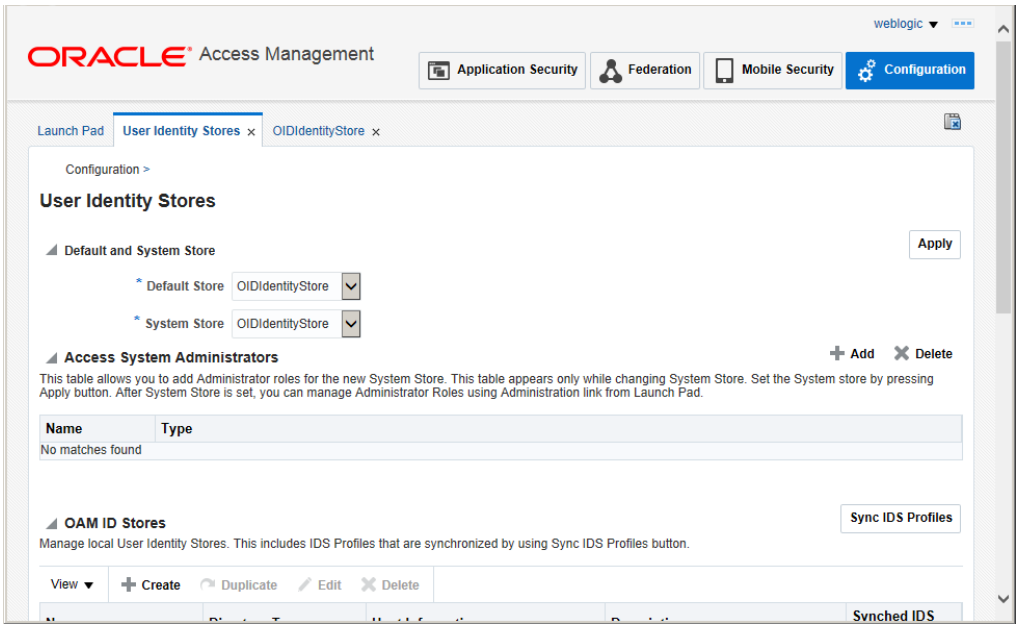
- The Create User Identity Store window opens again. Click **Apply** and the OIDIdentity Store tab opens.



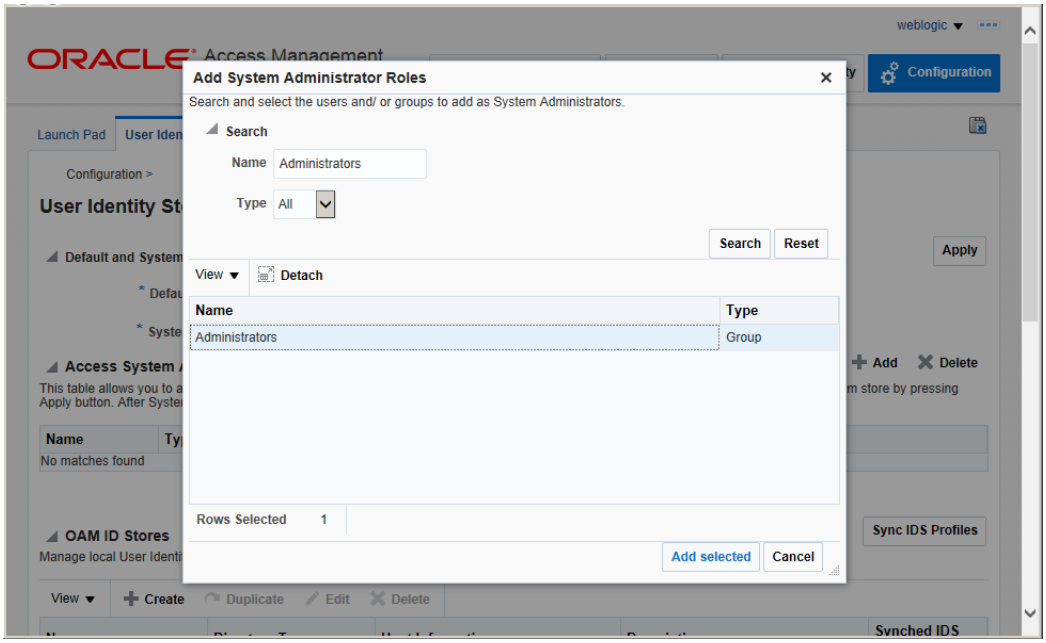
Set Identity Store as the Default Store and the Default System Store

To set the identity store as the default store and the default system store:

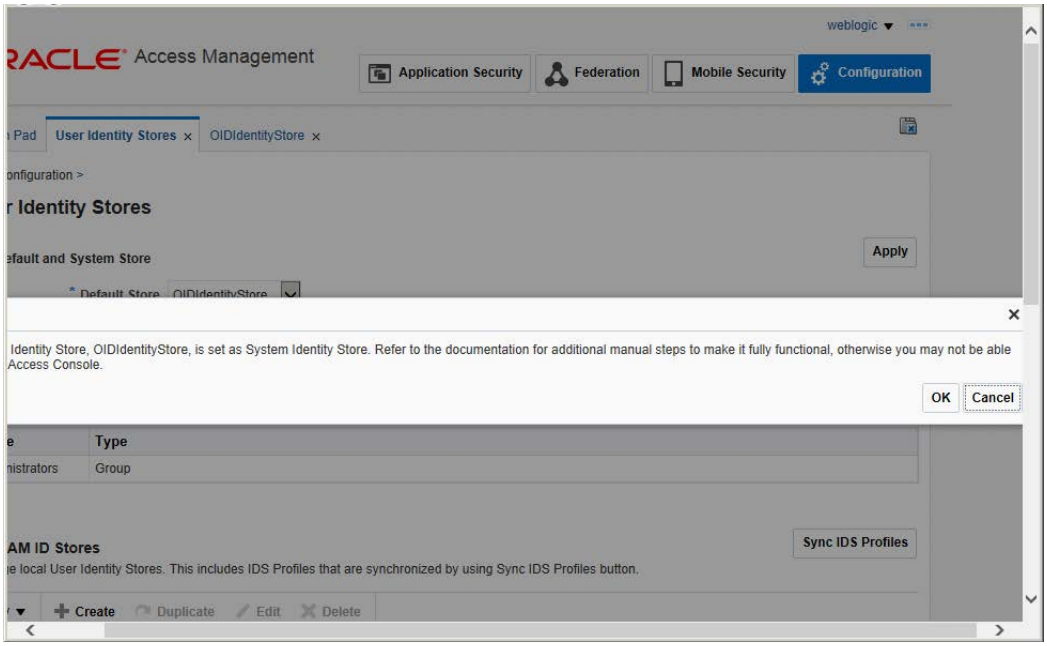
- In the OAM console – click the User Identity Stores tab.
- The User Identity Stores window opens. Make the following updates:
  - Default Store= OID Identity Store
  - System Store= OID Identity Store
  - Click the **Add** button in the Access System Administrators section of the screen.



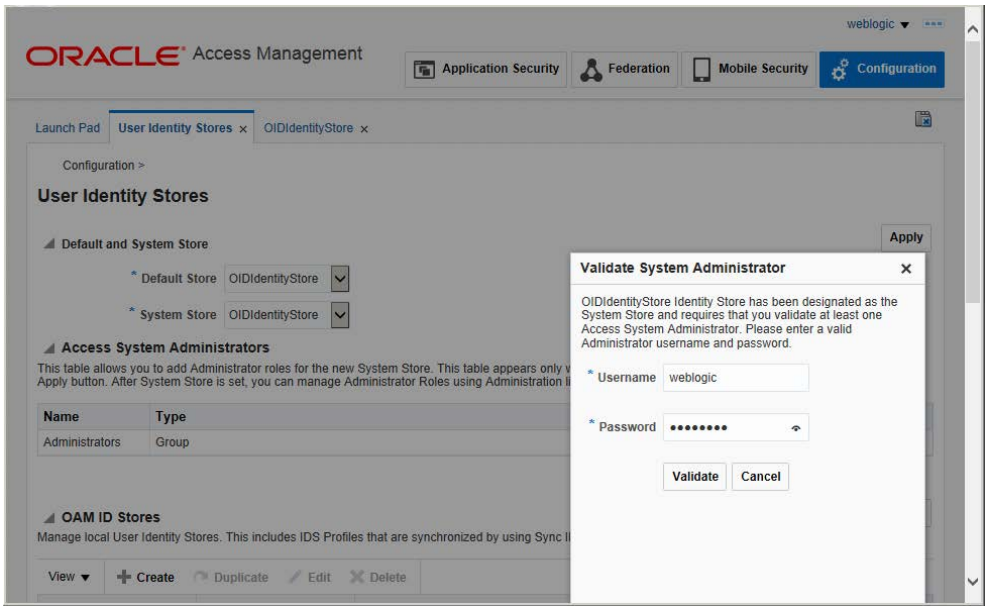
- The Add System Administrator Roles window opens.
  - Enter Administrators in the Name input field.
  - Click **Search.**
  - Click the **Administrators** row.
  - Click **Add Selected**.



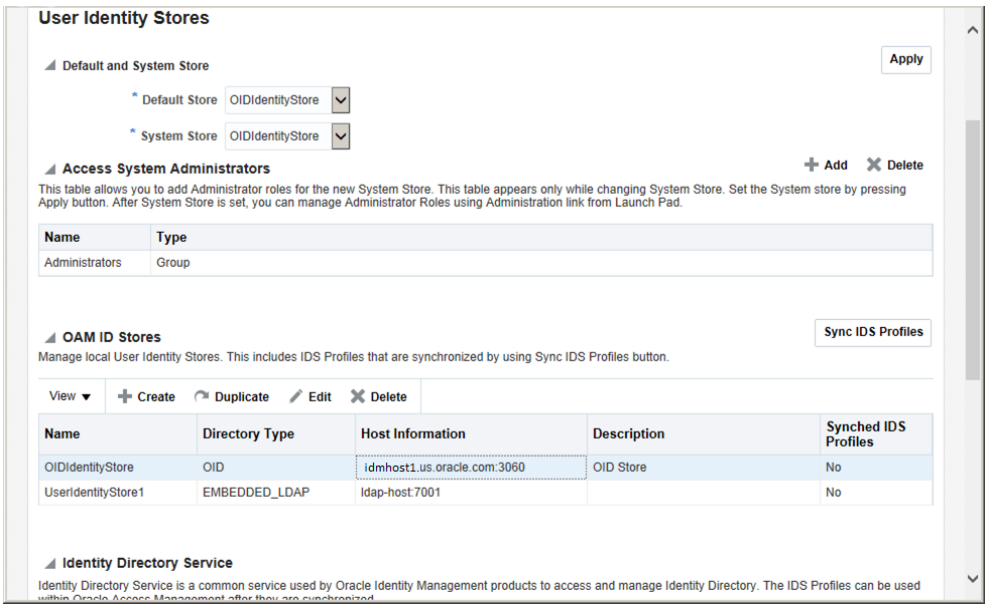
- A popup warning window opens. Click **OK**



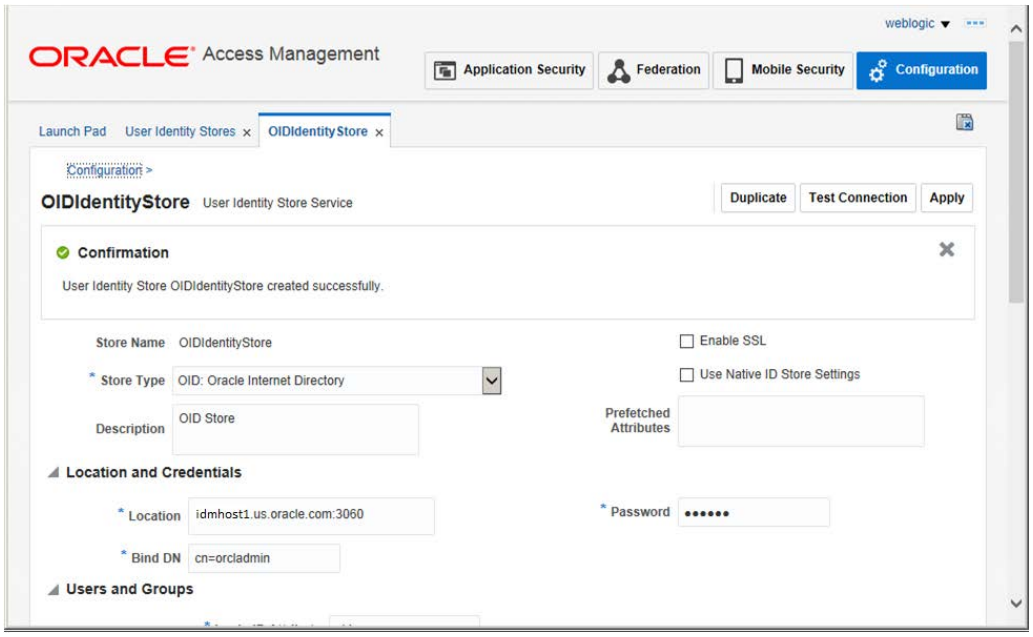
- The Validate System Administrator popup window opens. Enter in WebLogic credentials and Click **Validate**.



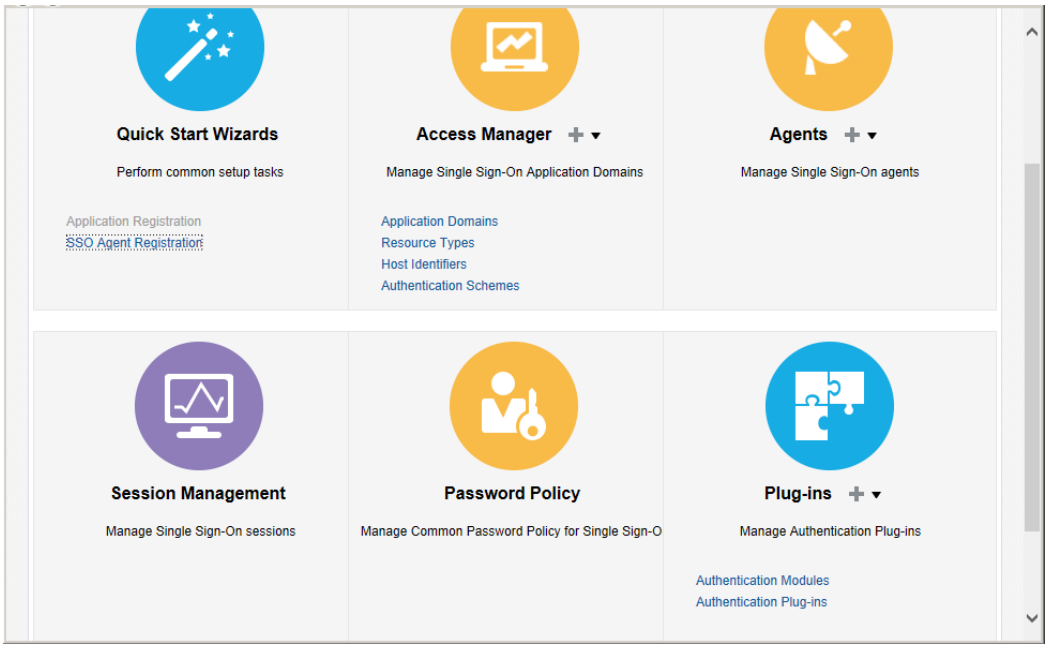
- The User Identity Stores window opens. Click the **Apply.**



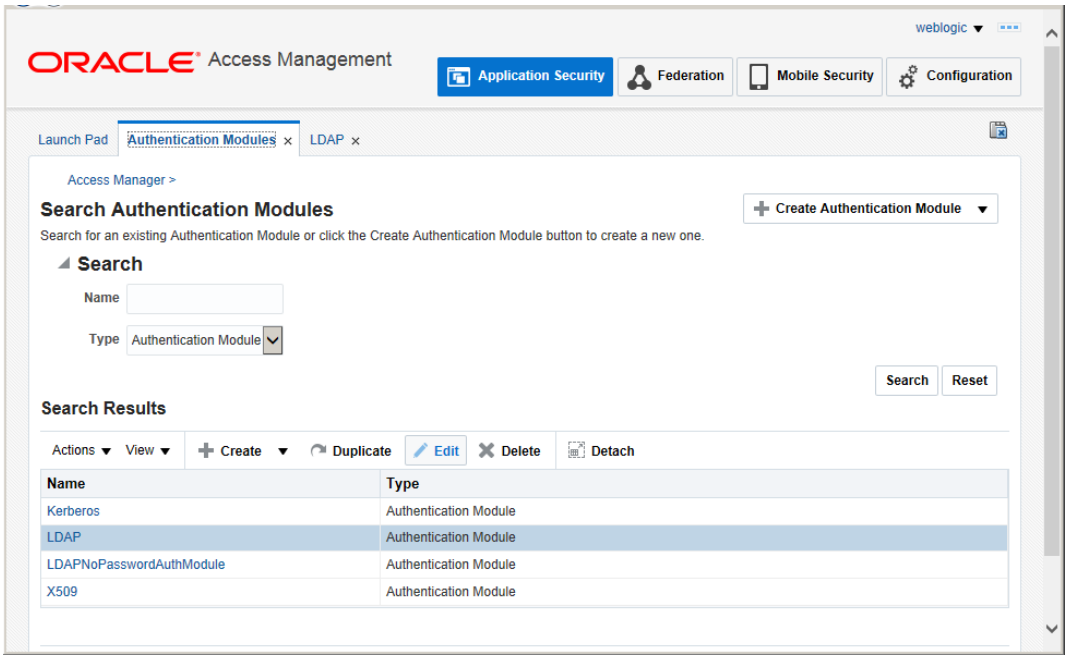
- Click on the OIDIdentity Store tab and validate that the green flag is displayed to indicate the process to set the OIDIdentitystore as the default store and System store was successful.



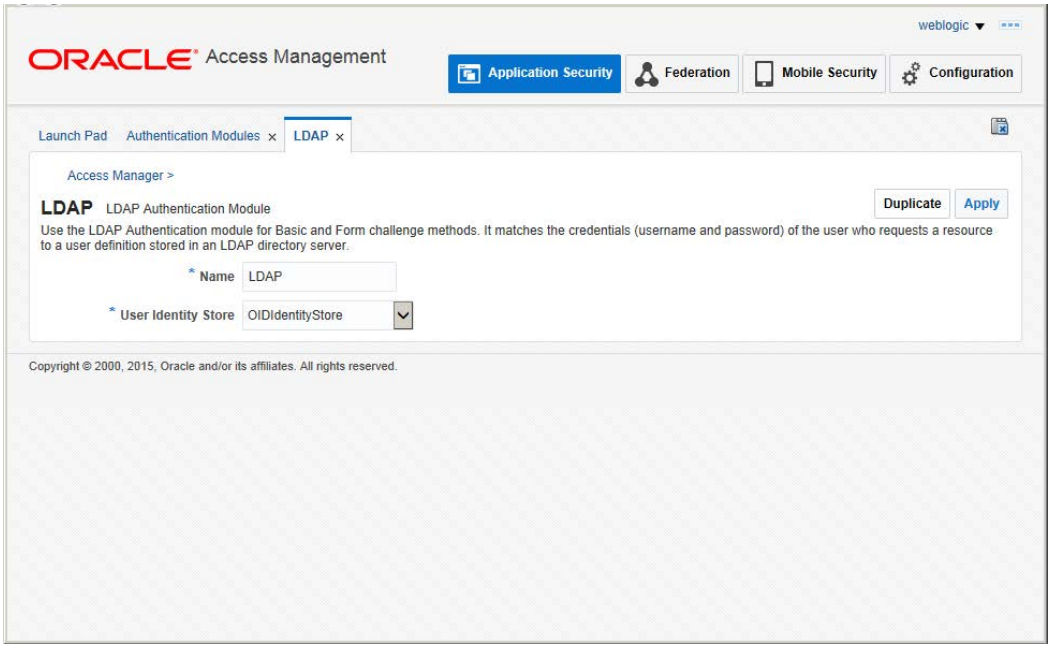
- Click the **Application Security** button located at the top of the page.
- The Launch Pad for the Application Security window opens. Click the **Authentication Modules** link located in the Plug-ins section of the screen.



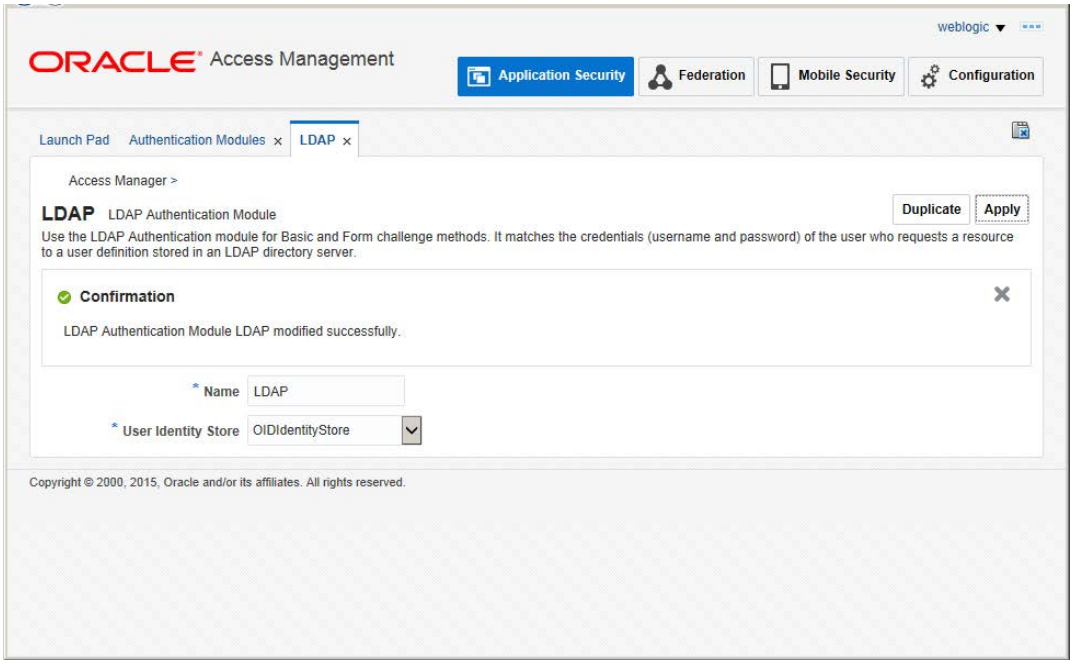
- The Authentication Modules window opens.
  - Select Authentication Module from drop down.
  - Click **Search**
  - Select the LDAP row
  - Click **Edit**



- The LDAP Authentication Module edit window opens.
  - Select OIDIdentityStore from drop down.
  - Click **Apply.**



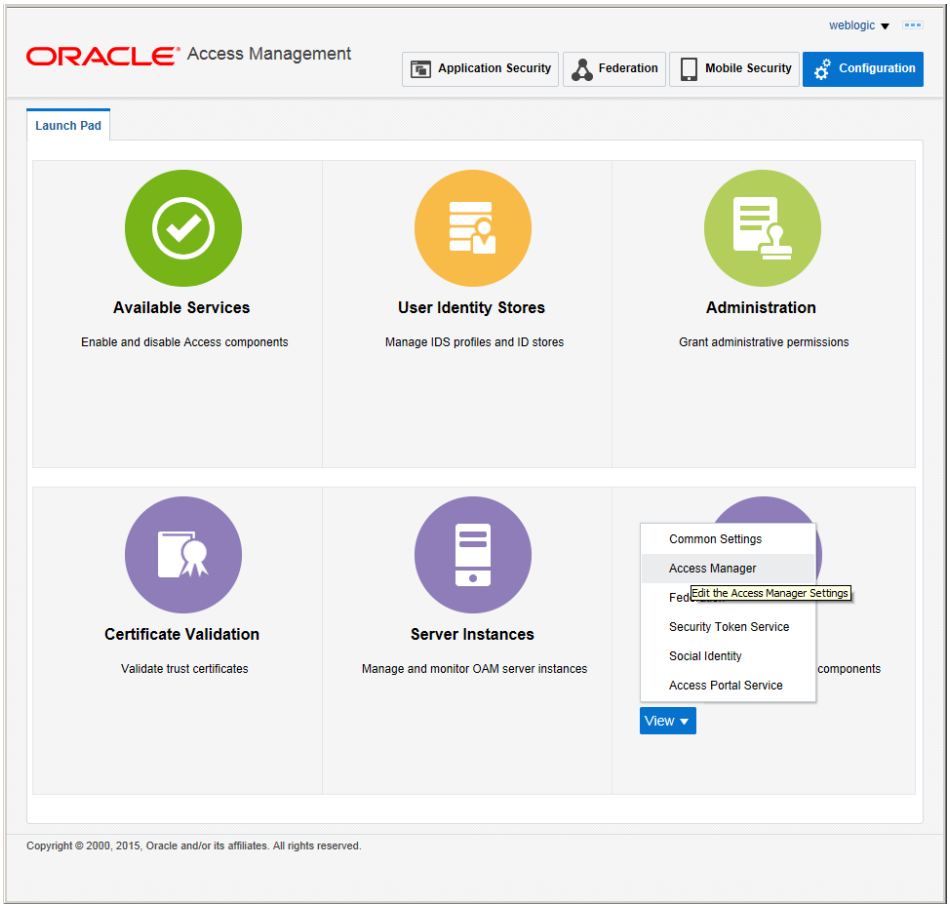
- Confirmation message opens.



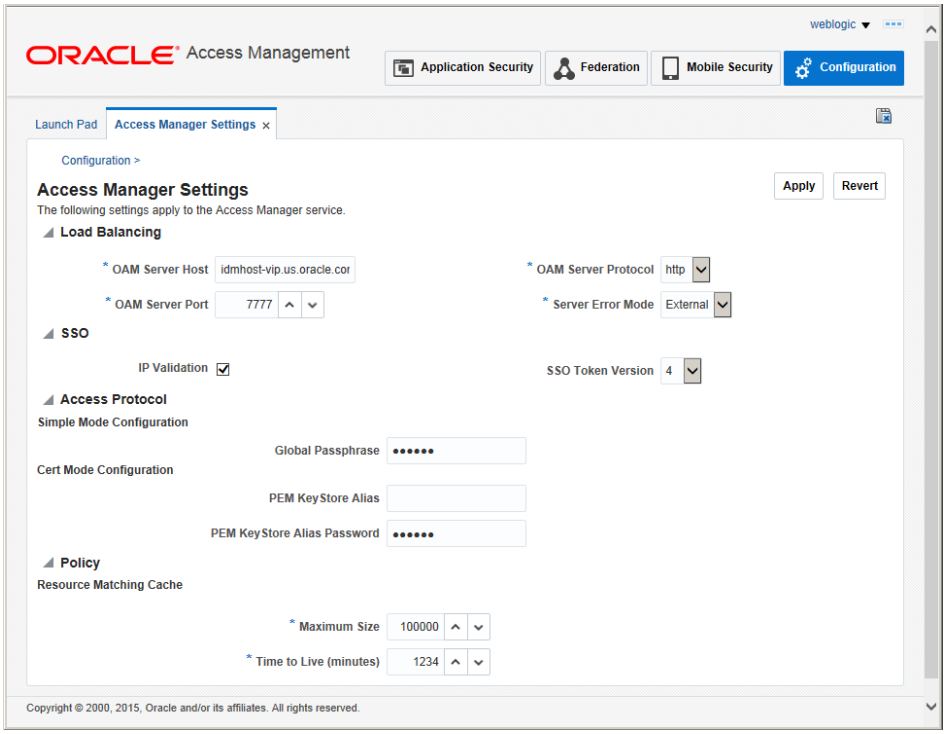
Configure OAM to use VIP URL and OHS Port

Perform the following steps to configure Oracel Access Manager to be able to use the VIP URL and OHS port.

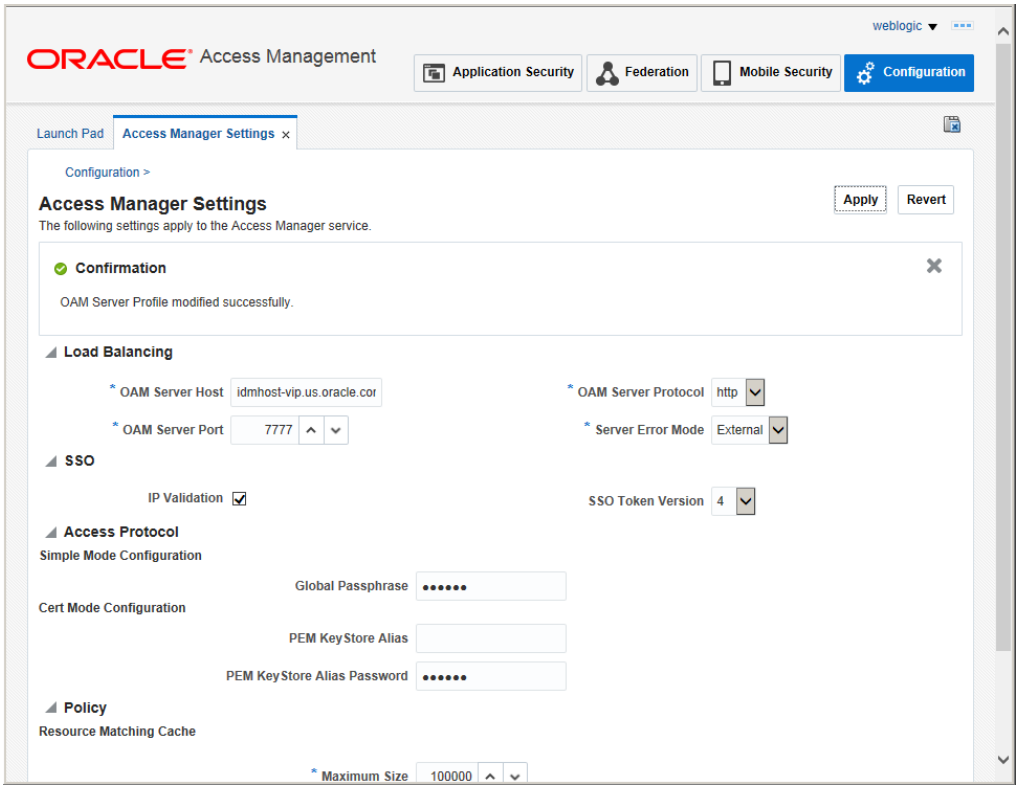
- Assuming still logged in from the previous steps – Close the Authentication Modules and LDAP tabs.
- The Configuration Launch Pad window opens. In the settings section – Click the View drop down and select the **Access Manager** option:



- The Access Manager Settings window opens. Make the following updates:
  - OAM Server Host: idmhost-vip.us.oracle.com
  - OAM Server Port: 7777
  - Leave the rest as is and click **Apply**.



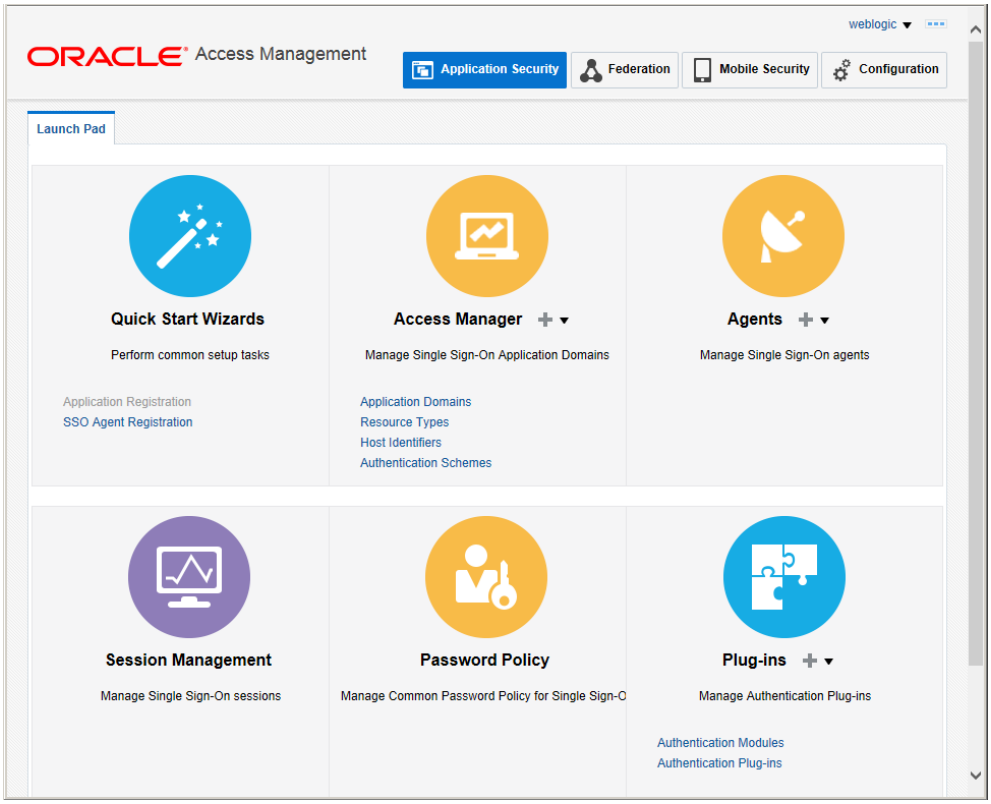
- A confirmation message should be displayed if successful.



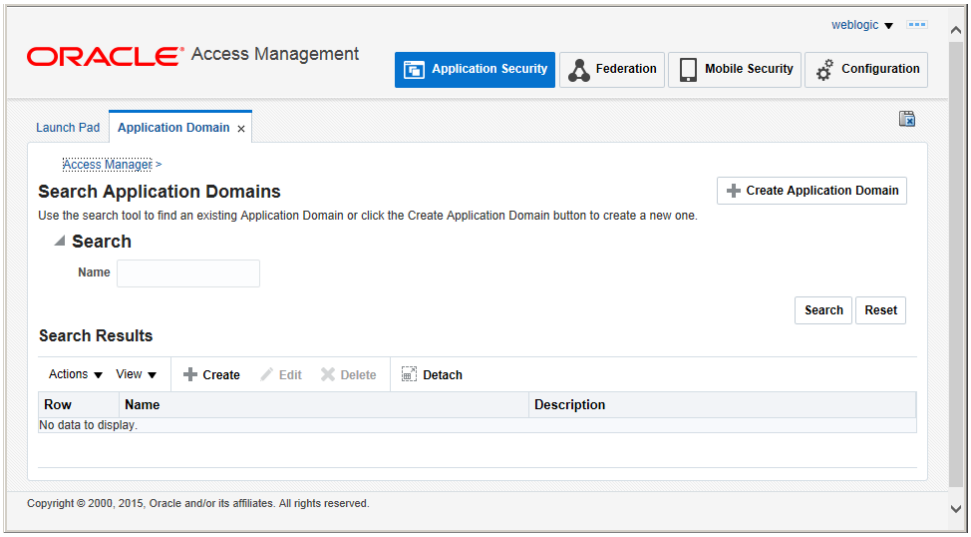
Set Protection Level for Resource URL's in OAM

Perform the following steps to configure Oracel Access Manager to be able to use the VIP URL and OHS port.

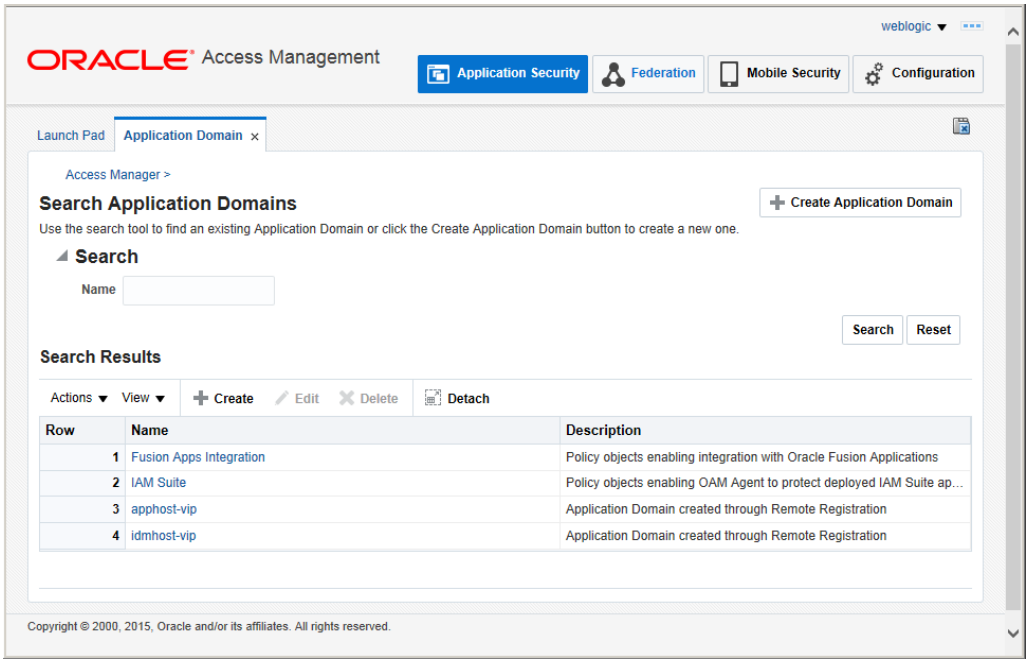
- Assuming still logged in from the previous steps, close the Access Manager tab and click the **Application Security** button at the top of the screen.
- The Application Security Launch Pad window opens. In the Access Manager section, click the **Application Domains** link:



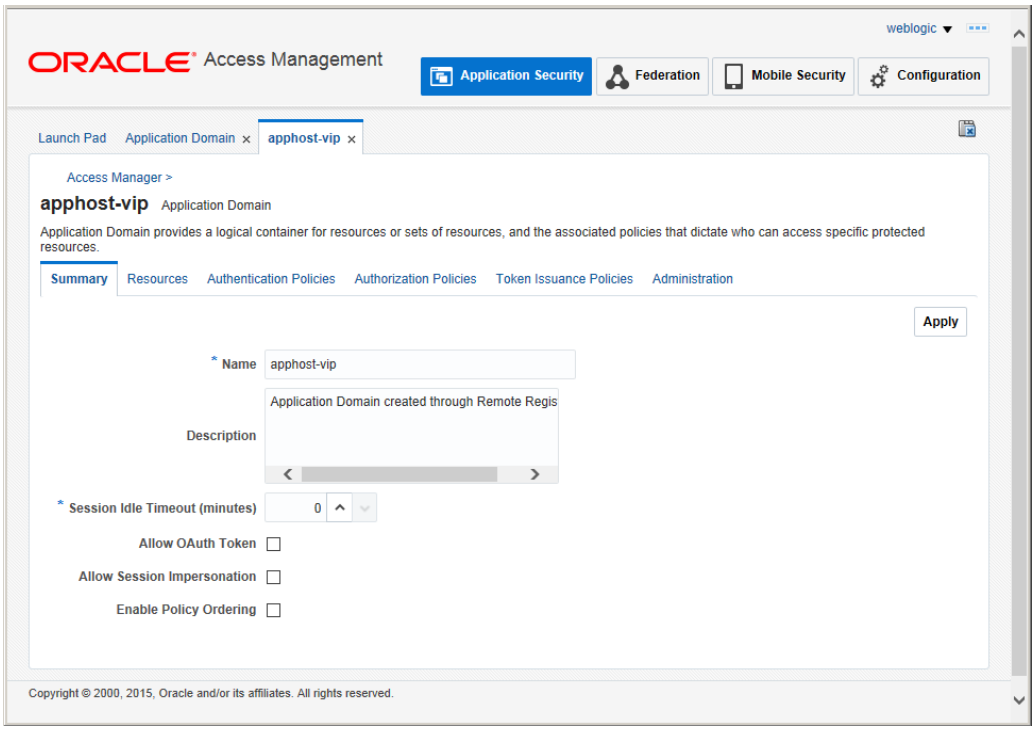
- The Search Application Domains tab opens. Click **Search**:



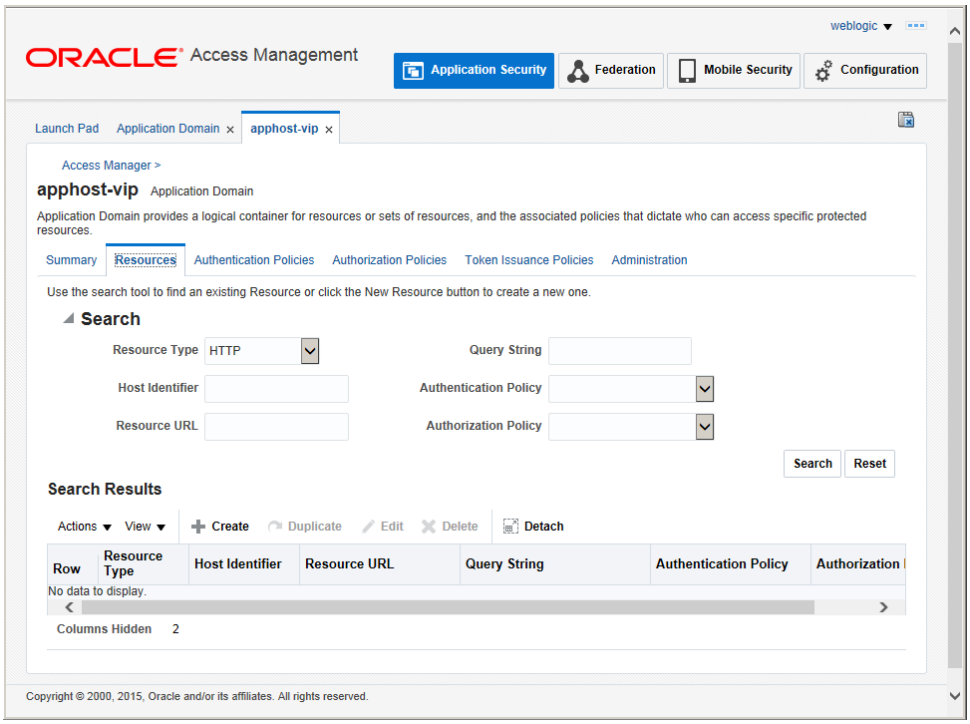
- In the Search Results section , click the **apphost-vip** link.



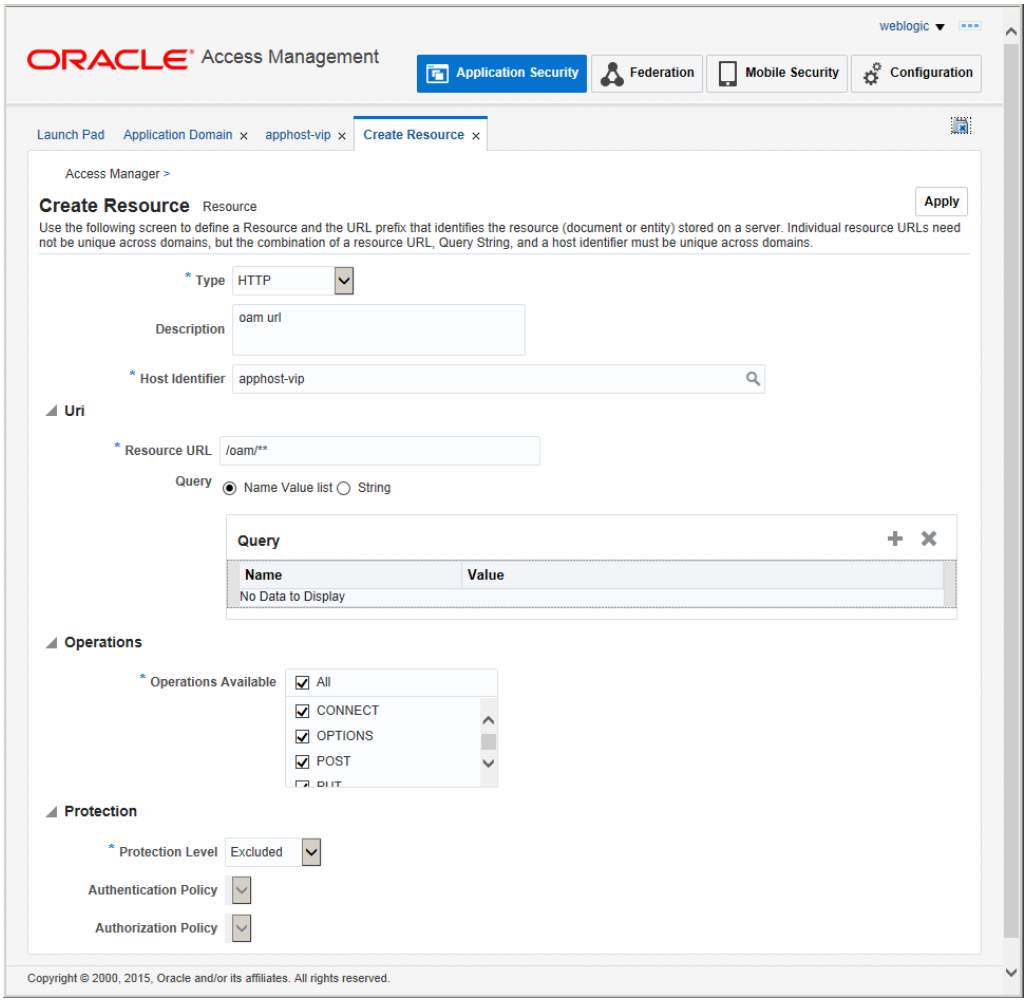
- The apphost-vip tab opens. Click the **Resources** sub-tab.



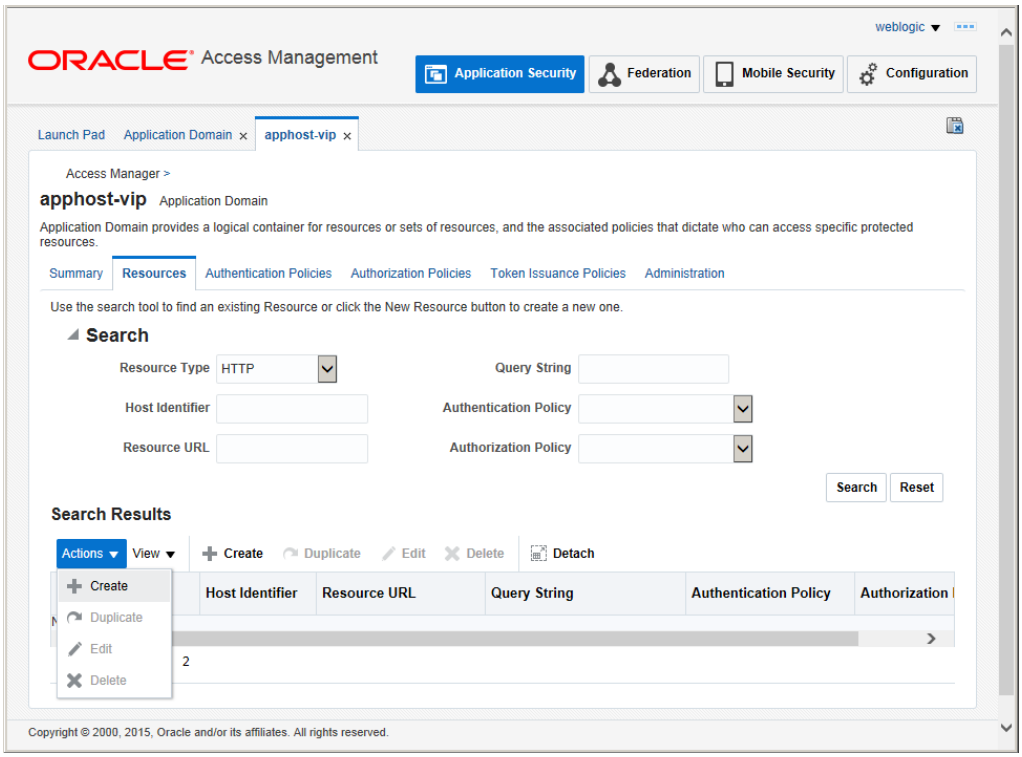
- In the Search Results section, select **Create** from the Actions dropdown menu.



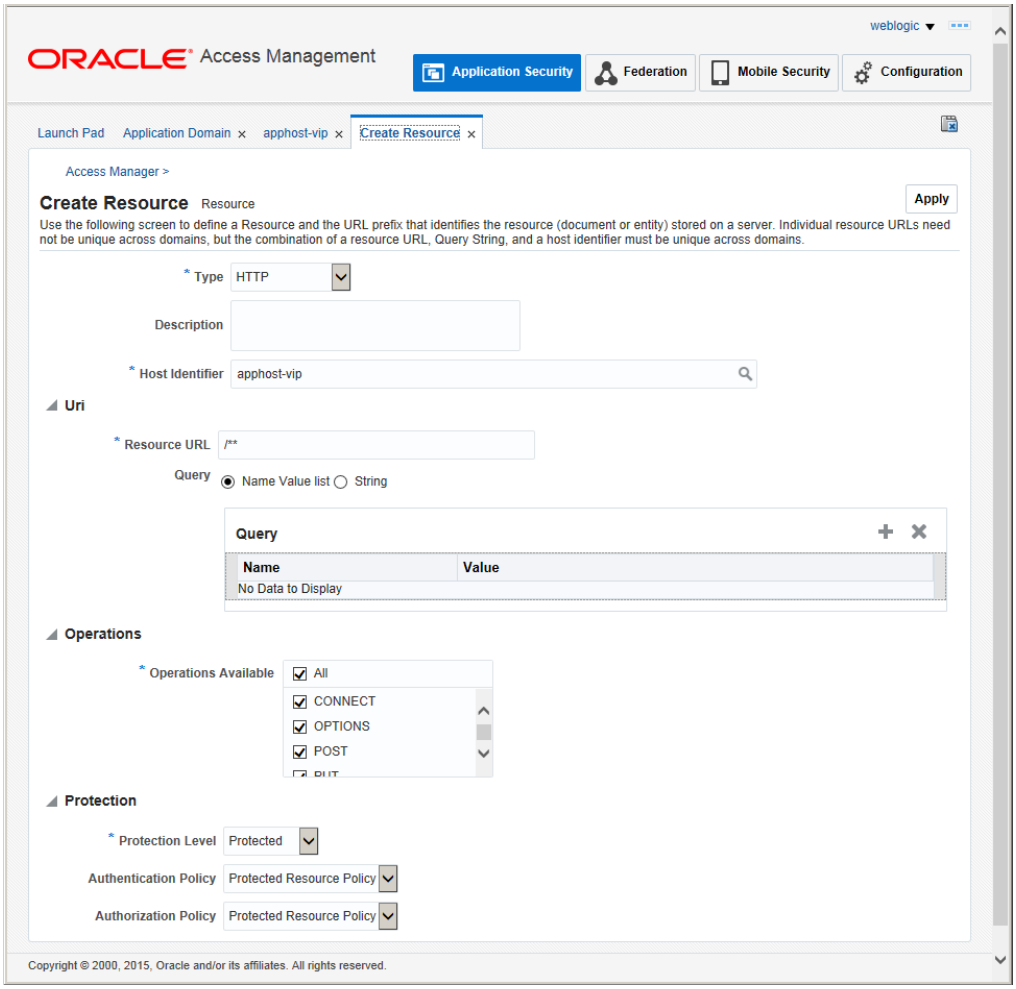
- The Create Resource tab opens. Make the following updates and close the Create Resource tab when finished.
  - Type: HTTP
  - Description: oam url
  - Host Identifier: apphost-vip
  - Resource URL: /oam/**
  - Protection Level: Excluded
  - Leave all other settings as defaulted.
  - Click **Apply**



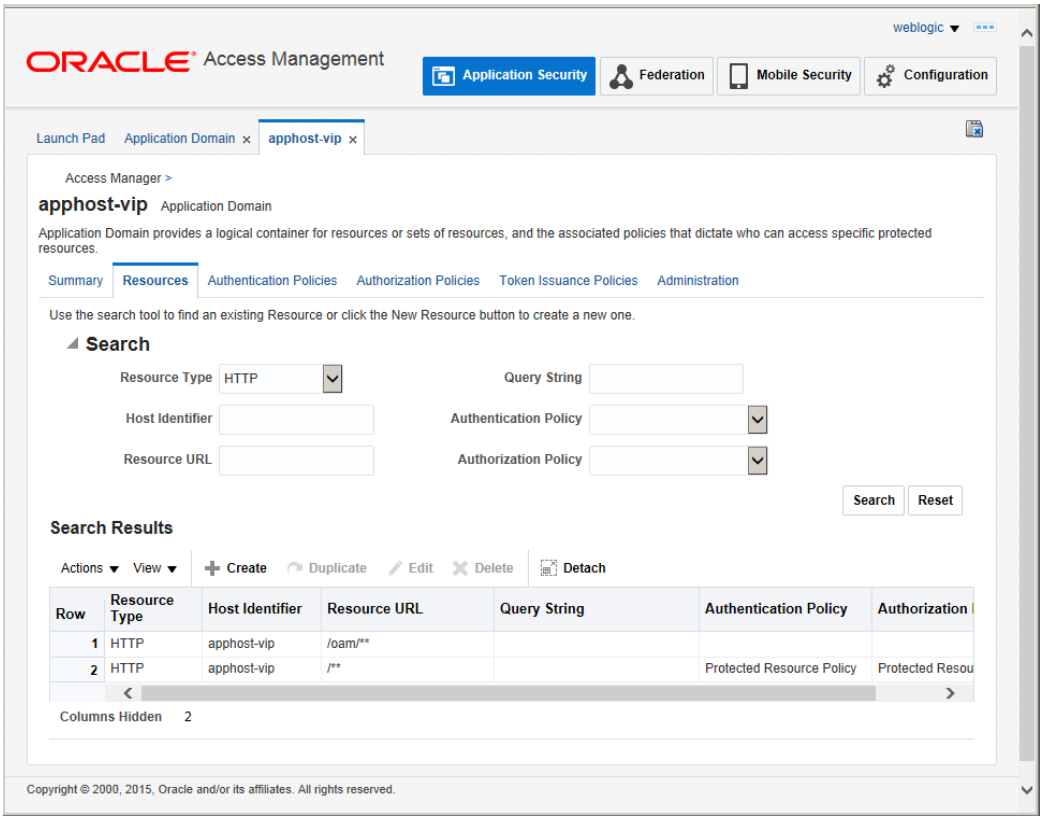
- In the Search Results section of the Resources tab, select **Create** from the Actions dropdown menu.



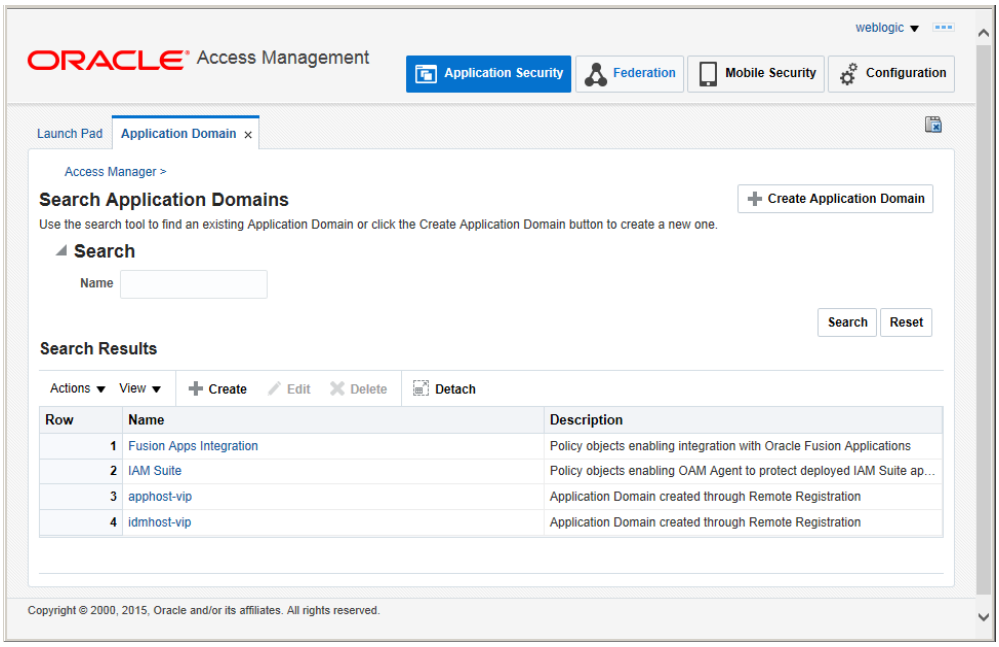
- The Create Resource window opens. Make the following updates and close the Create Resource tab when finished.
  - Type: HTTP
  - Host Identifier: apphost-vip
  - Resource URL: /**
  - Protection Level: Protected
  - Authentication Policy: Protected Resource Policy
  - Authorization Policy: Protected Resource Policy
  - Leave all other settings as defaulted.
  - Click **Apply.**



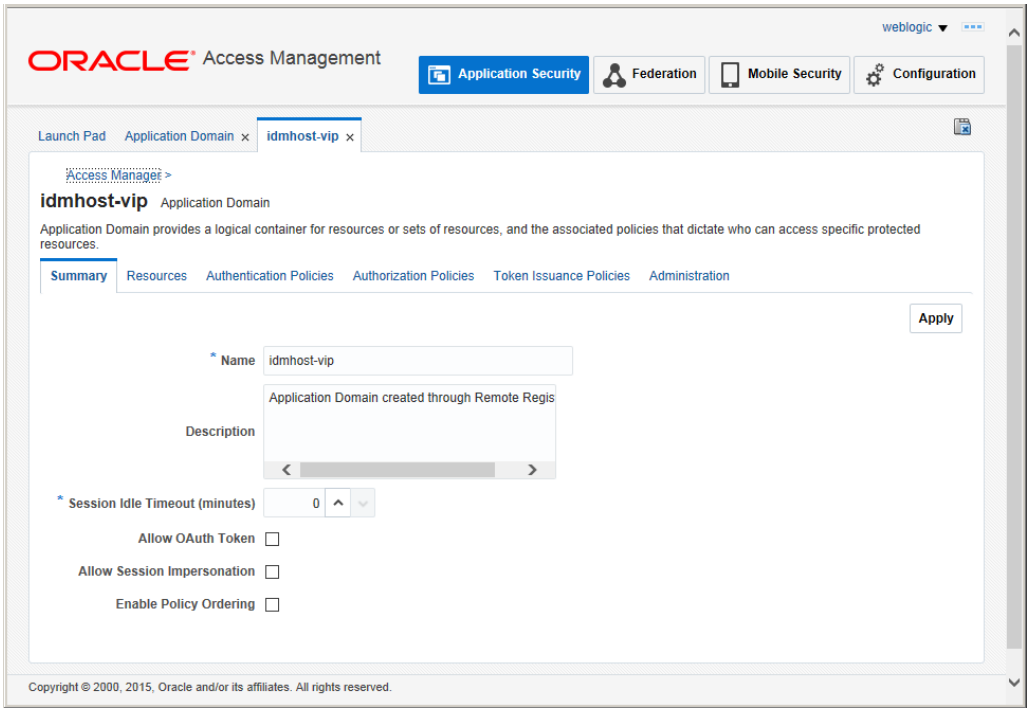
- In the Search section of the Resources tab, click **Search** to validate the changes were committed. Close the apphost-vip tab located at top of screen when finished.



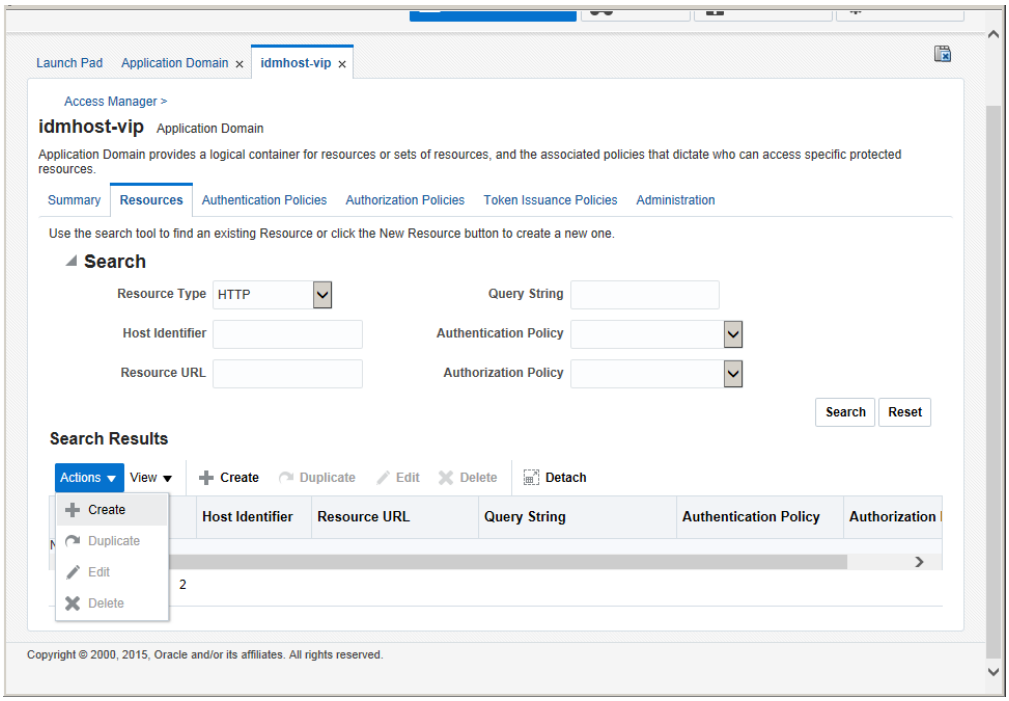
- In the Application Domain tab should be displayed. In the Search Results section, click the **idmhost-vip** link:



- The idmhost-vip tab opens. Click the **Resources** sub-tab.

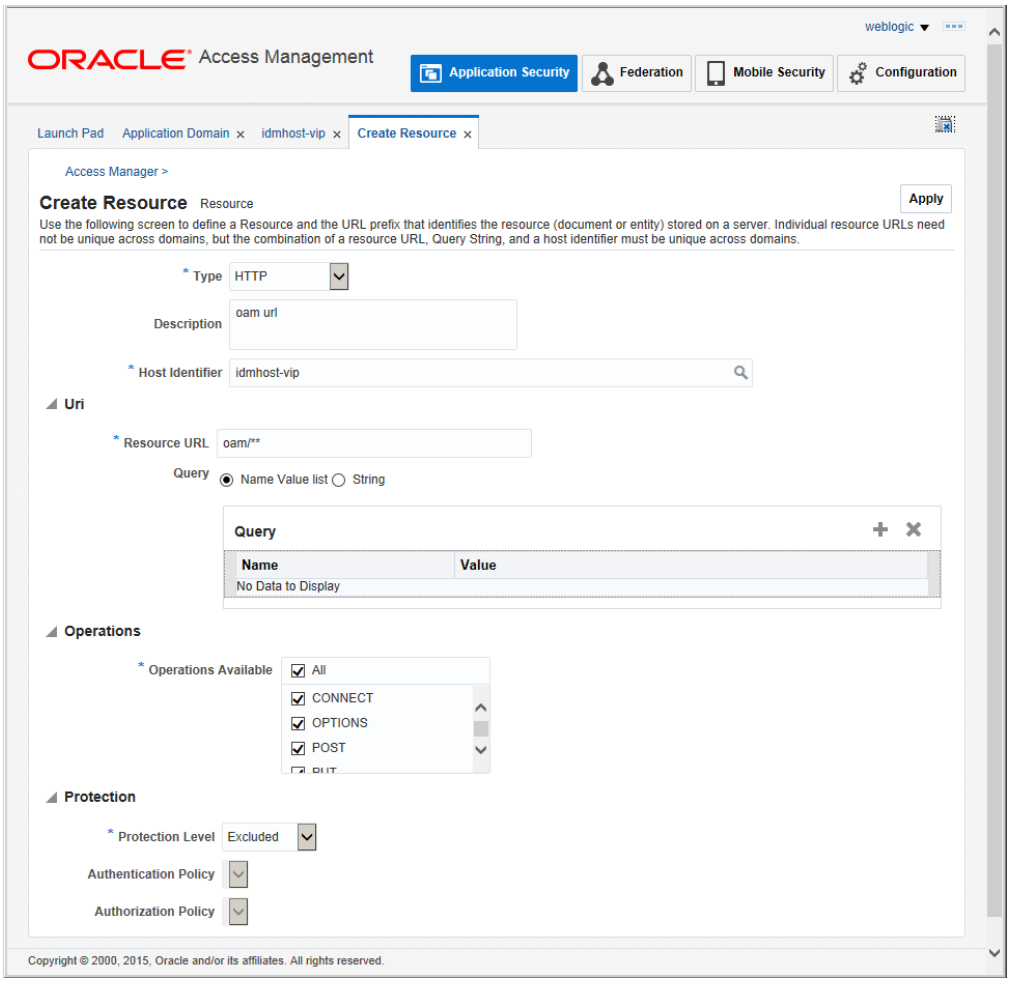


- In the Search Results section, select **Create** from the Actions dropdown menu.

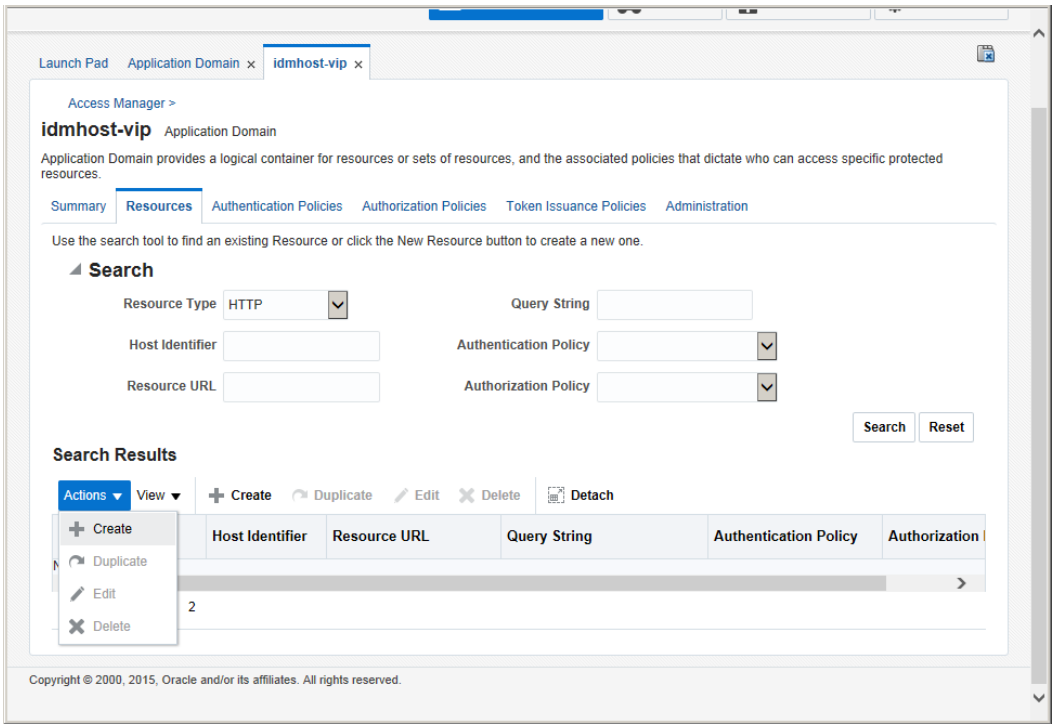


- The Create Resource tab opens. Make the following updates and close the Create Resource tab when finished.
  - Type: HTTP
  - Description: oam url
  - Host Identifier: idmhost-vip
  - Resource URL: /oam/**

- Protection Level: Excluded
- Leave all other settings as defaulted.
- Click **Apply.**

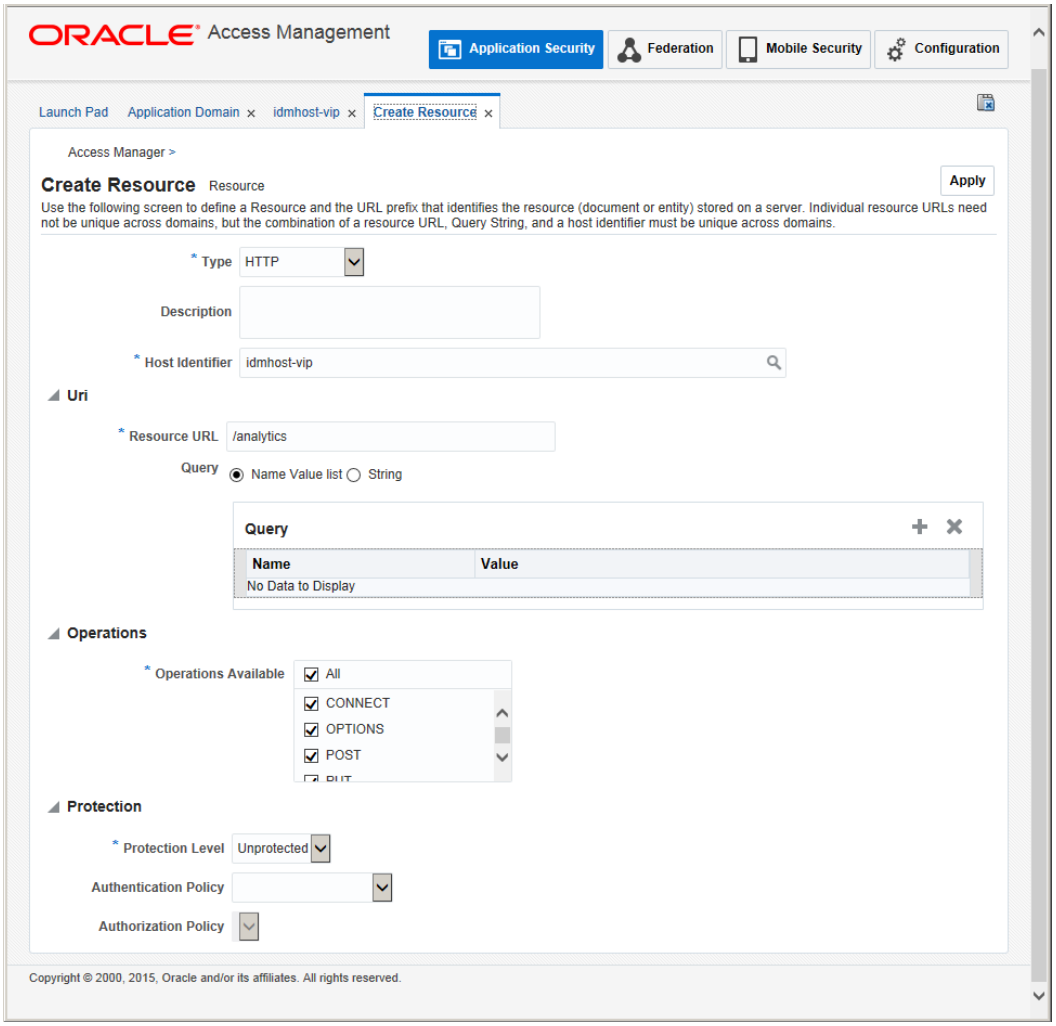


- In the Search Results section of the Resources tab, select **Create** from the Actions dropdown menu.

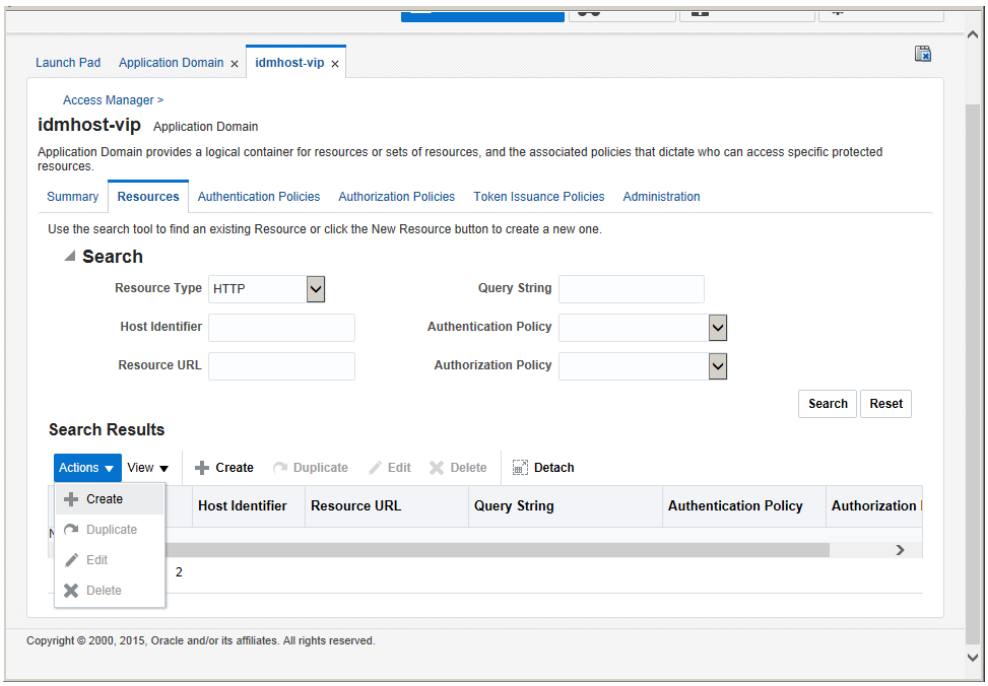


- The Create Resource tab opens. Make the following updates and close the Create Resource tab when finished.
  - Type: HTTP
  - Host Identifier: idmhost-vip
  - Resource URL: /analytics
  - Protection Level: Unprotected
  - Leave all other settings as defaulted.
  - Click **Apply.**

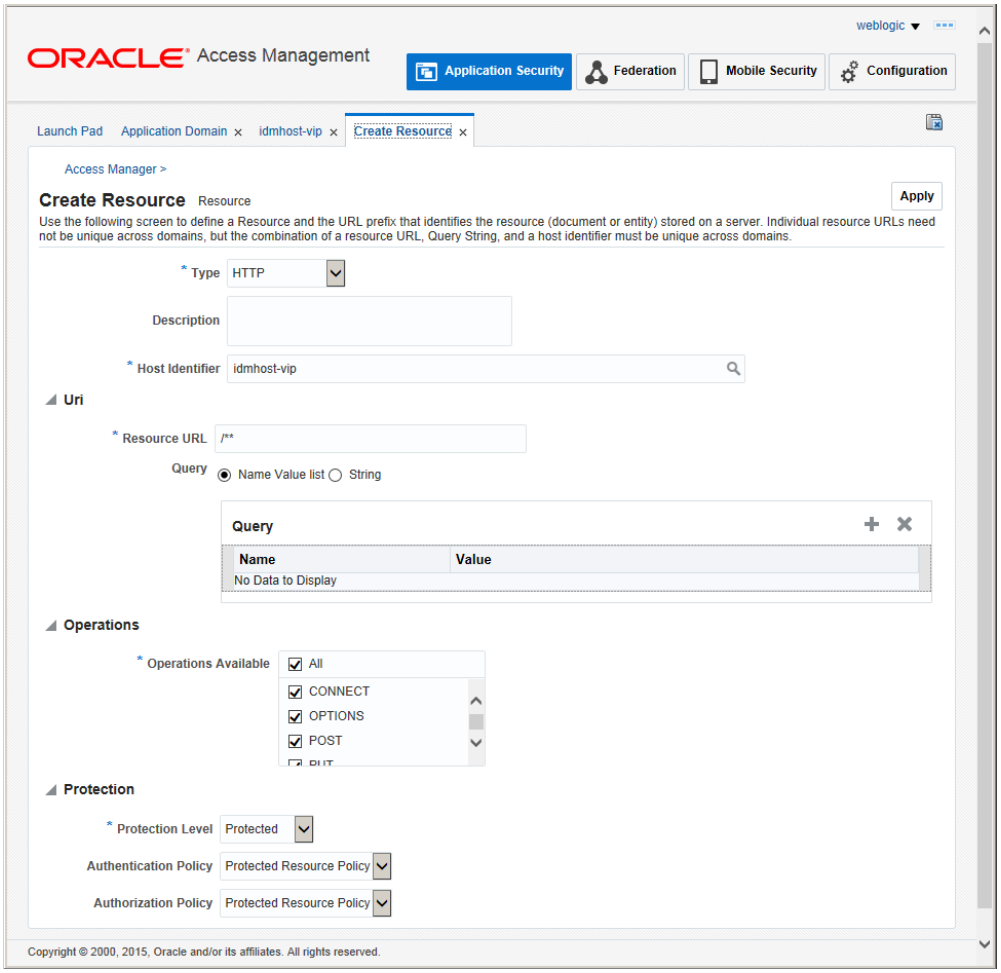
> **NOTE**: The /analytics resource URL is setting is for OBIEE analytics. The installation steps will occur later in this document. We are adding in the resource URL in advance so these screens do not need to be accessed again.



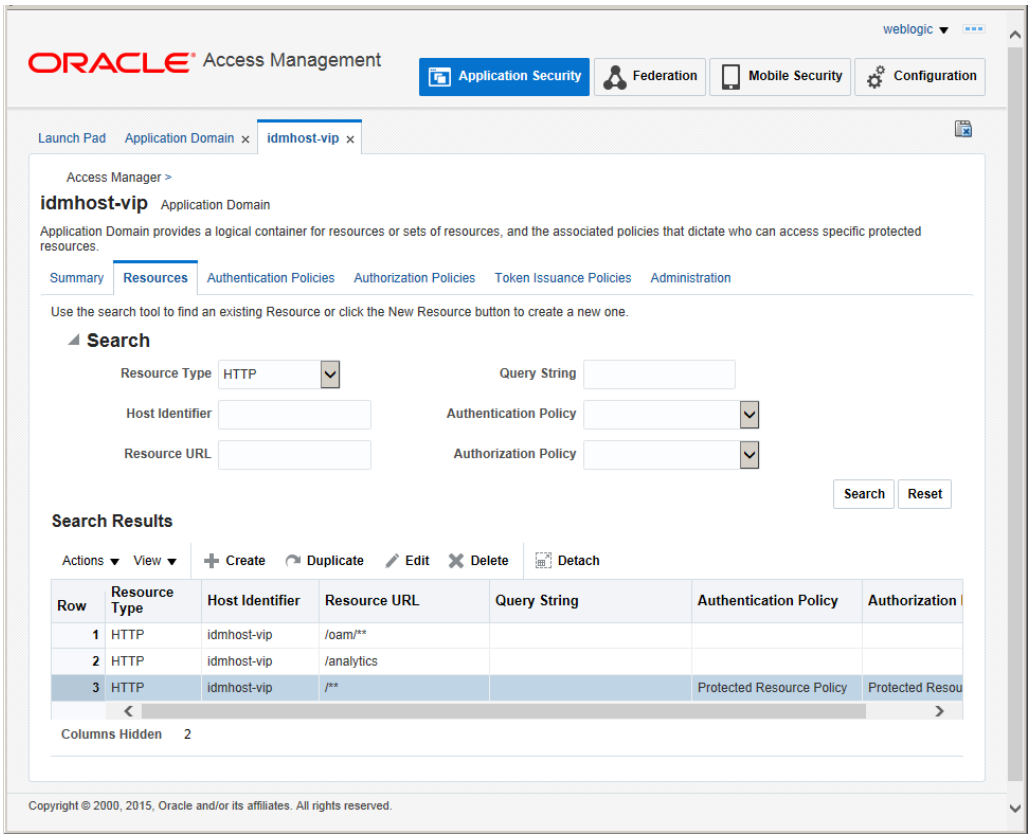
- In the Search Results section of the Resources tab, select **Create** from the Actions dropdown menu.



- The Create Resource tab opens. Make the following updates and close the Create Resource tab when finished.
  - Type: HTTP
  - Host Identifier: idmhost-vip
  - Resource URL: /**
  - Protection Level: Protected
  - Authentication Policy: Protected Resource Policy
  - Authorization Policy: Protected Resource Policy
  - Leave all other settings as defaulted.
  - Click **Apply.**



- In the Search section of the Resources tab, click **Search** to validate the changes were committed.



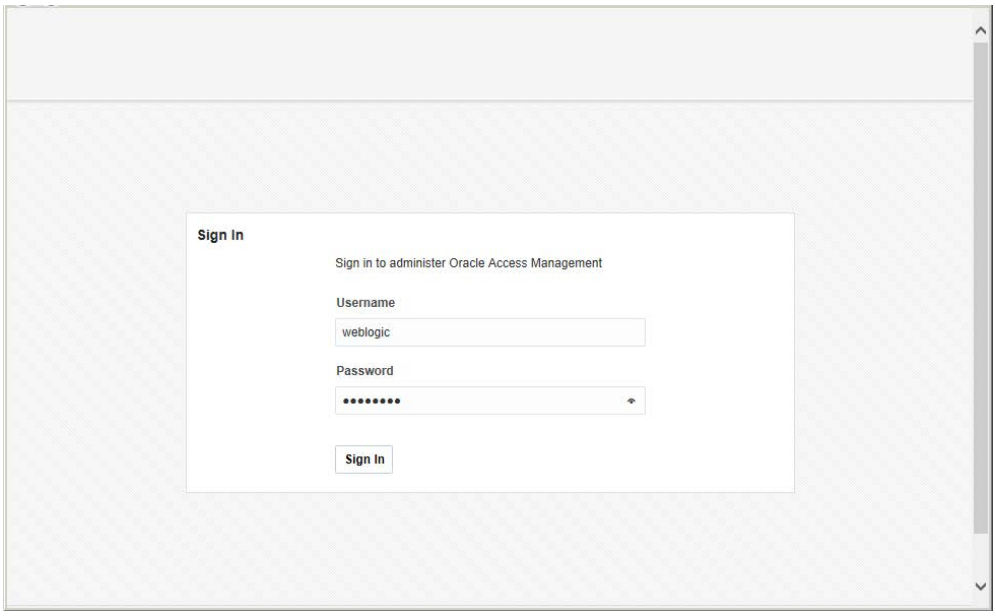
- Done with setting protection Level Resource URL's in OAM.

14

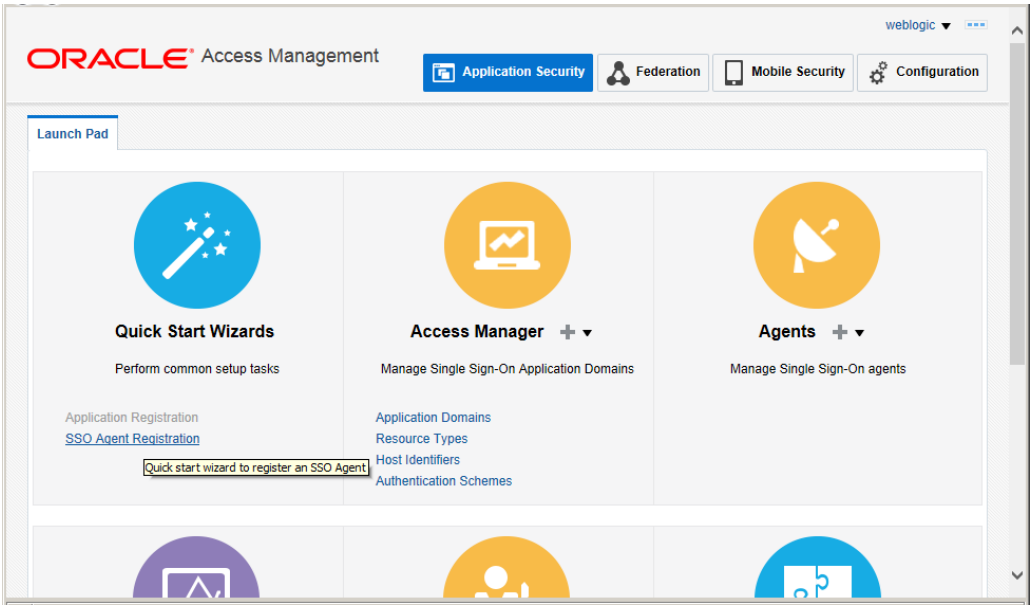
Registering a New WebGate Agent

Perform the following steps to register a new WebGate Agent as Single Sign on provider in OAM:

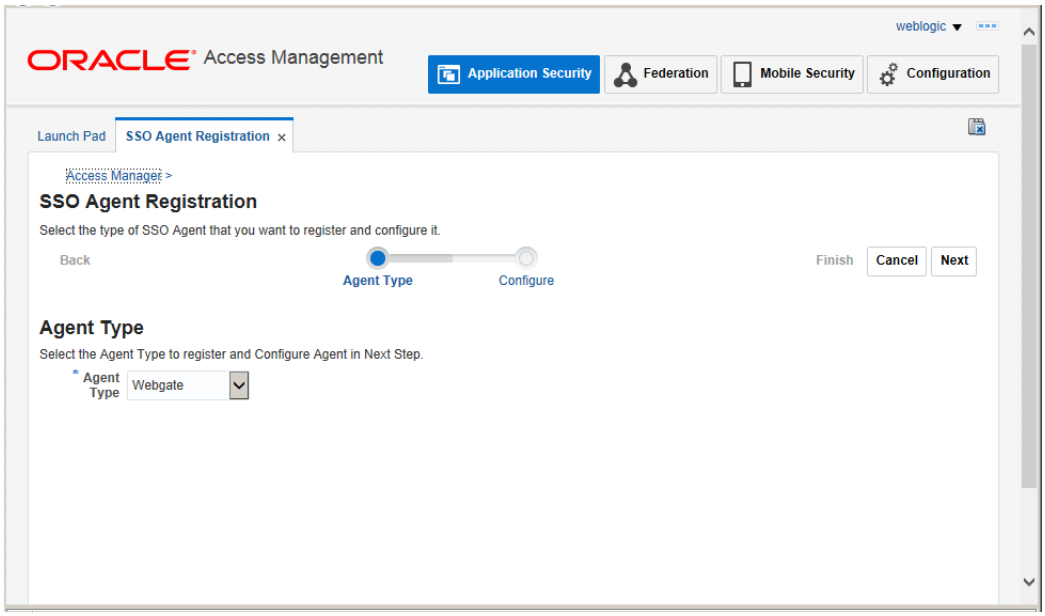
- Launch OAMConsole http://idmhost1.us.oracle.com:16001/oamconsole and login using WebLogic admin user.



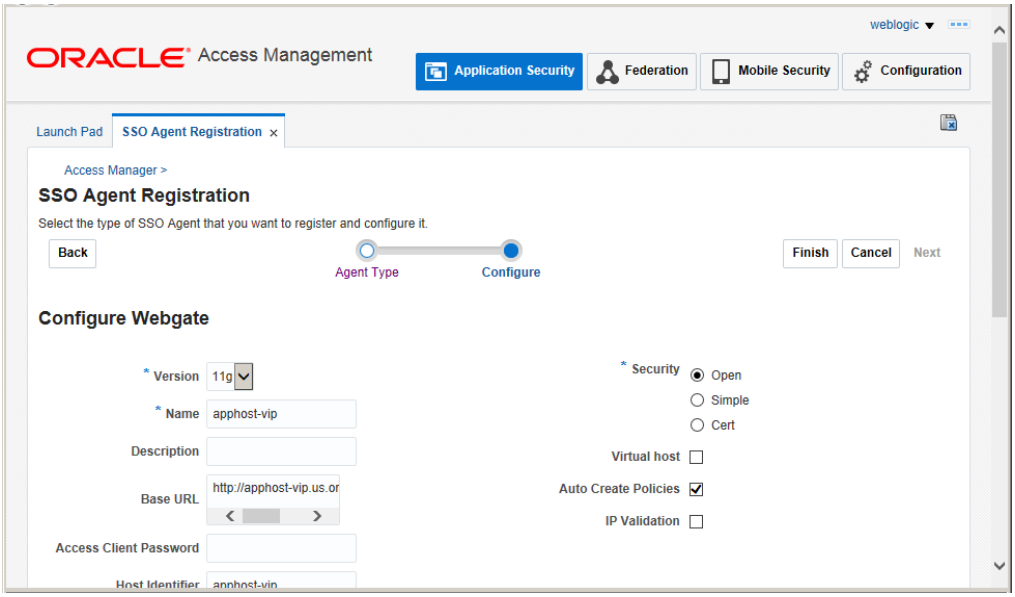
- The Access Management Launch window opens. Click **SSO Agent Registration** link.



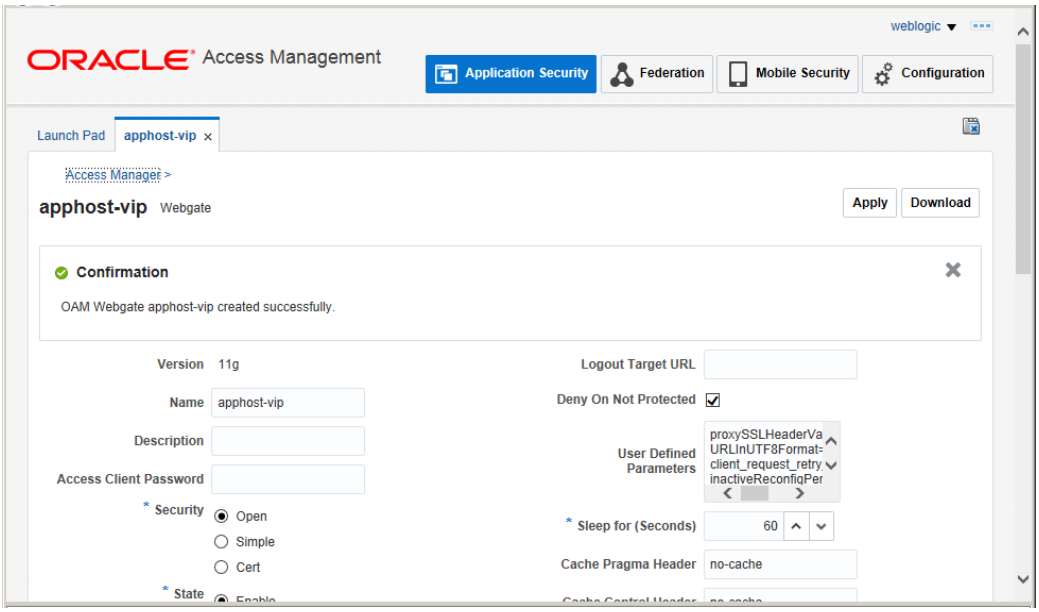
- The SSO Agent Registration: Agent Type window opens.
  - Select Webgate from the drop down.
  - Click **Next**.



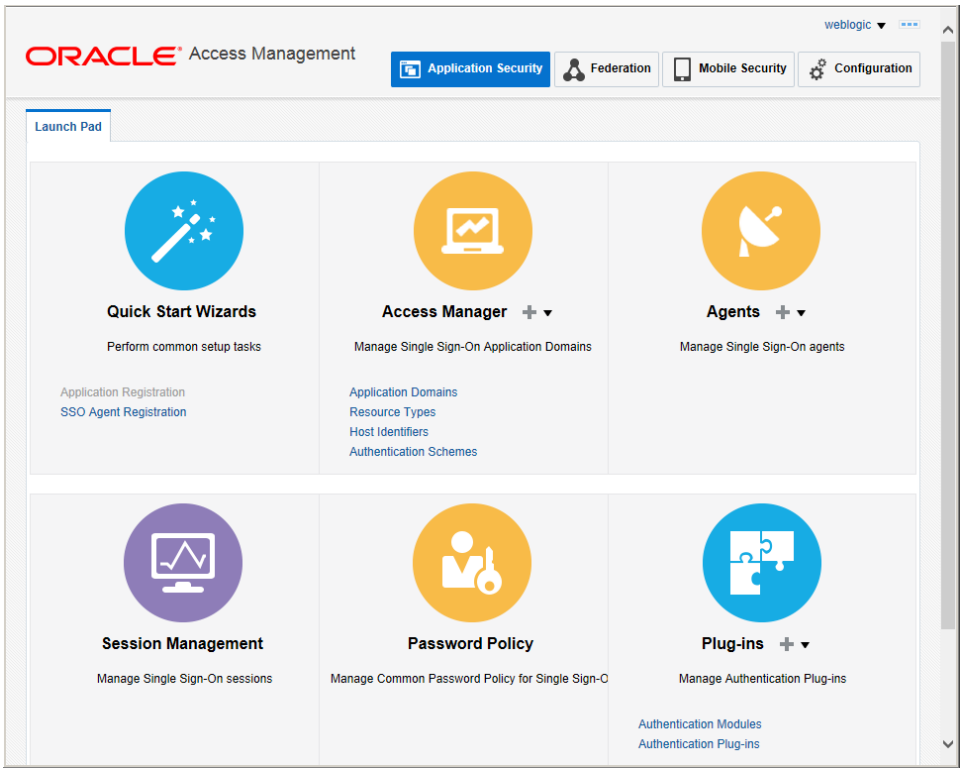
- The SSO Agent Registration: Configure window opens. Set the following values.
  - Version: 11g
  - Name: apphost-vip
  - Base URL: http://apphost-vip.us.oracle.com:7777
  - Leave the rest of the page as is.
  - Click **Finish**.



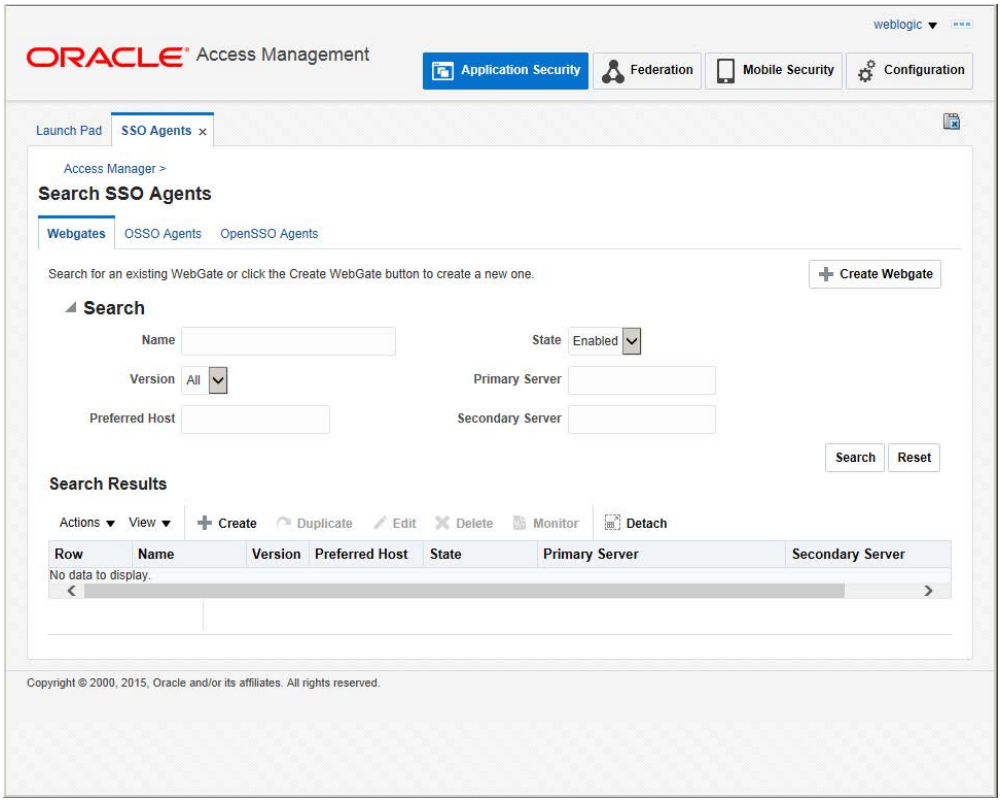
- The Access Management apphost-vip Confirmation window opens.



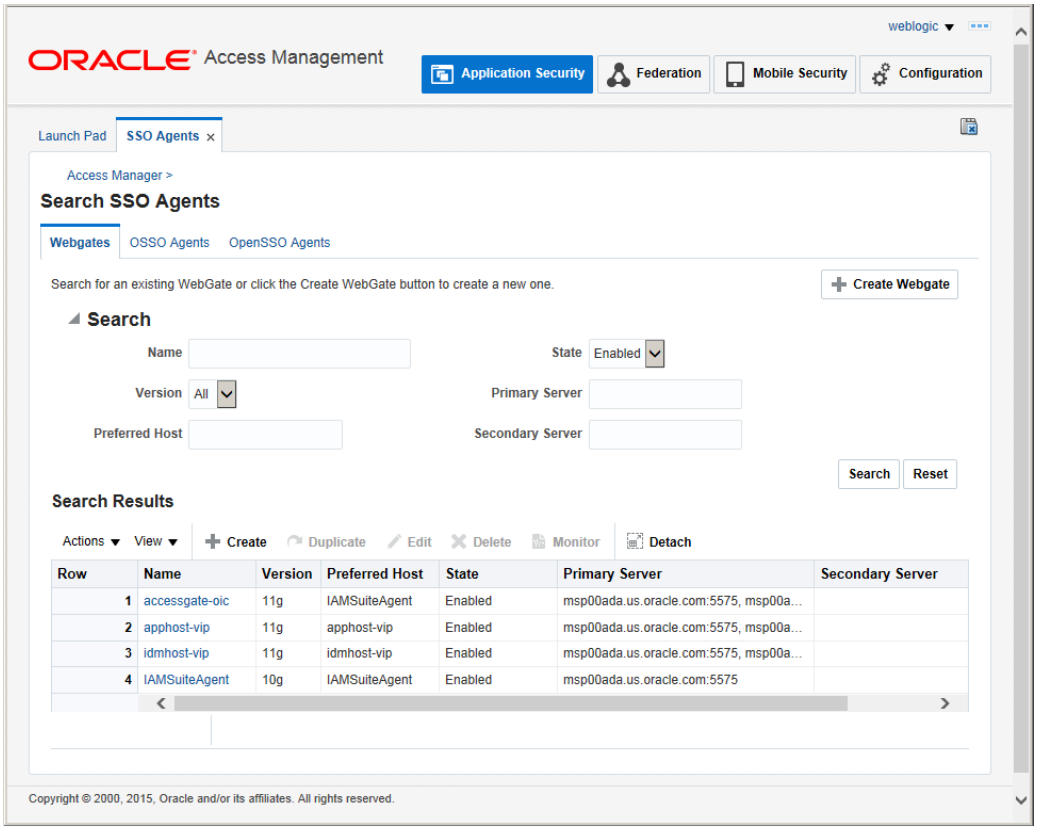
- Repeat the steps above to register the WebGate agent for the idmhosts. Replace apphost-vip with idmhost-vip.
- Close all the open tabs so the Application Security/Launch Pad window opens, and then click the **Agents** icon.



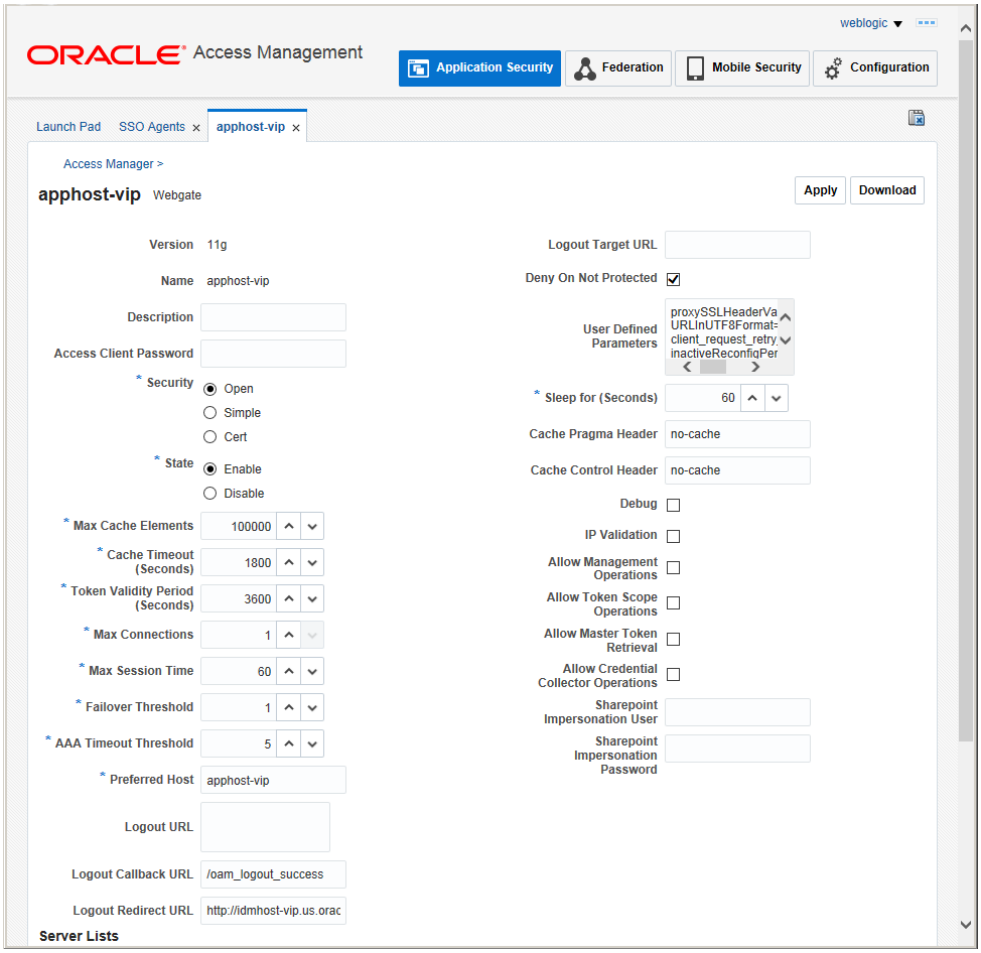
- The SSO Agents window opens. Click the **Search** button.



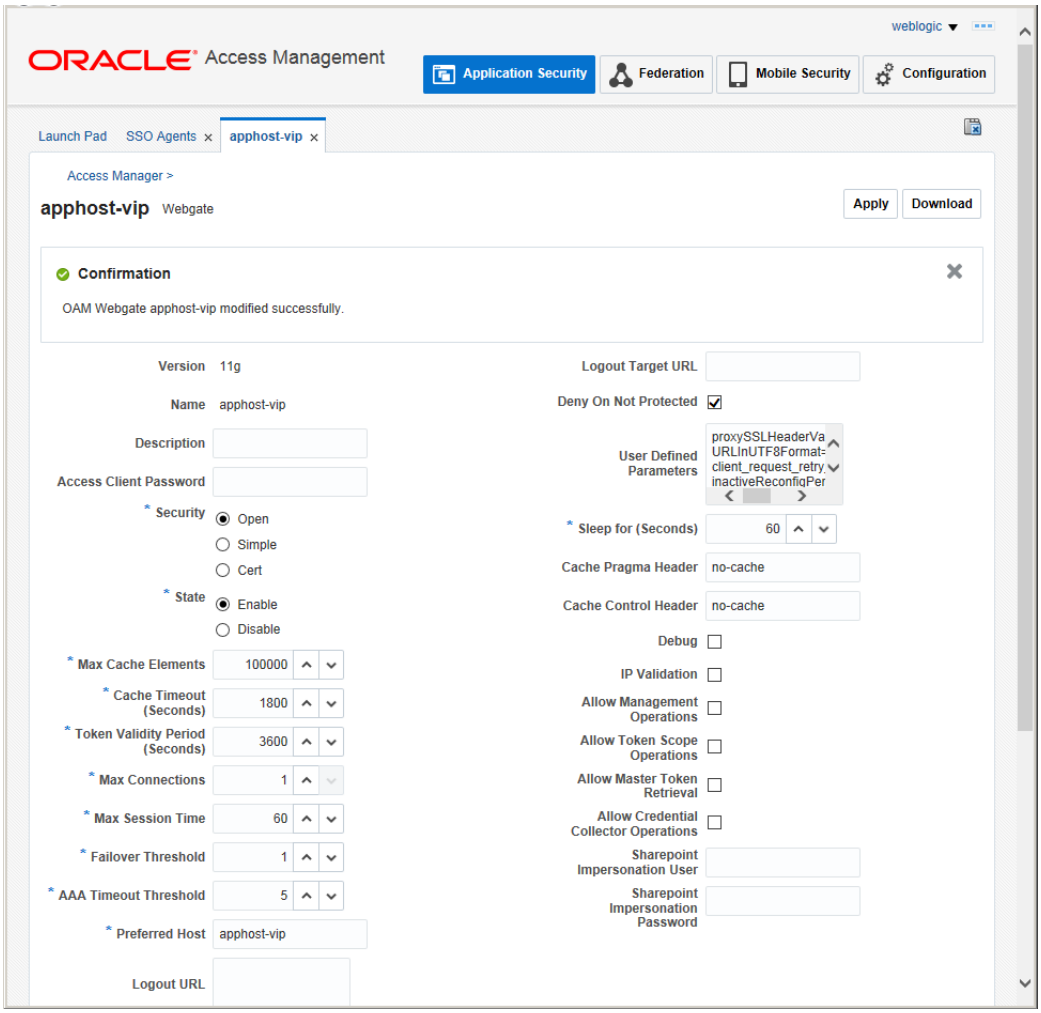
- Click the **apphost-vip** link.



- At the bottom of the screen make the following updates and click **Apply**.
  - Logout Callback URL: /oam_logout_success
  - Logout Redirect URL: http://idmhost-vip.us.oracle.com:7777/oam/server/logout



- A confirmation window opens. Go back to the SSO Agents tab above and **repeat the steps for the idmhost-vip**.



- Using the following instructions - Copy the files that were created above on idmhost1 to the <WEBTIER_ORACLE_HOME>/instances/instance1/config/OHS/<instance-name>/webgate/config directory for each hosts Web Tier instance. (Make sure to copy the files to the right hosts - idmhost-vip goes to idmhost1 and idmhost2 and apphost-vip goes to apphost1 and apphost2.)
  - Copy idmhost-vip file to idmhost1 and validate the copy:

    Example:
    ```
    $ cp -r /u00/webadmin/config/domains/wls_iam/OAMDomain/output/idmhost-vip/*
    /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1/config/OHS/ohs1/webgate/config
    $ cd
    /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1/config/OHS/ohs1/webgate/config
    $ ls
    ```

    Output:
    ```
    cwallet.sso  cwallet.sso.lck  ObAccessClient.xml  oblog_config_wg.xml
    simple  wallet
    ```

  - Copy idmhost-vip file to idmhost2 and validate the copy:

Example:
```
$ scp -r /u00/webadmin/config/domains/wls_iam/OAMDomain/output/idmhost-
vip/*
webadmin@idmhost2.us.oracle.com:/u00/webadmin/products/wls_ohs/Oracle_W
T1/instances/instance2/config/OHS/ohs2/webgate/config
$ cd
/u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance2/config/OH
S/ohs2/webgate/config
$ ls
```

Output:
```
cwallet.sso  cwallet.sso.lck  ObAccessClient.xml  oblog_config_wg.xml
simple  wallet
```

– Copy apphost-vip file to apphost1 and validate the copy:

Example:
```
$ scp -r /u00/webadmin/config/domains/wls_iam/OAMDomain/output/apphost-
vip/*
webadmin@apphost1.us.oracle.com:/u00/webadmin/products/wls_ohs/Oracle_W
T1/instances/instance1/config/OHS/ohs1/webgate/config
$ cd
/u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1/config/OH
S/ohs1/webgate/config
$ ls
```

Output:
```
cwallet.sso  cwallet.sso.lck  ObAccessClient.xml  oblog_config_wg.xml
simple  wallet
```

– Copy apphost-vip file to apphost2 and validate the copy:

Example:
```
$ scp -r /u00/webadmin/config/domains/wls_iam/OAMDomain/output/apphost-
vip/*
webadmin@apphost2.us.oracle.com:/u00/webadmin/products/wls_ohs/Oracle_W
T1/instances/instance2/config/OHS/ohs2/webgate/config
$ cd
/u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1/config/OH
S/ohs1/webgate/config
$ ls
```

Output:
```
cwallet.sso  cwallet.sso.lck  ObAccessClient.xml  oblog_config_wg.xml
simple  wallet
```

15

Installing and Configuring OBIEE 11.1.1.9

This chapter describes the installation and configuration of OBIEE 11.1.1.9 in a cluster with instances on a shared mount.

Create RCU Schemas for OBIEE

In order to to run the Repository Creation Utility (RCU) - It is required to use the database credentials for the sysadmin user. Perform the following steps to create a database repository using Repository Creation Utility:

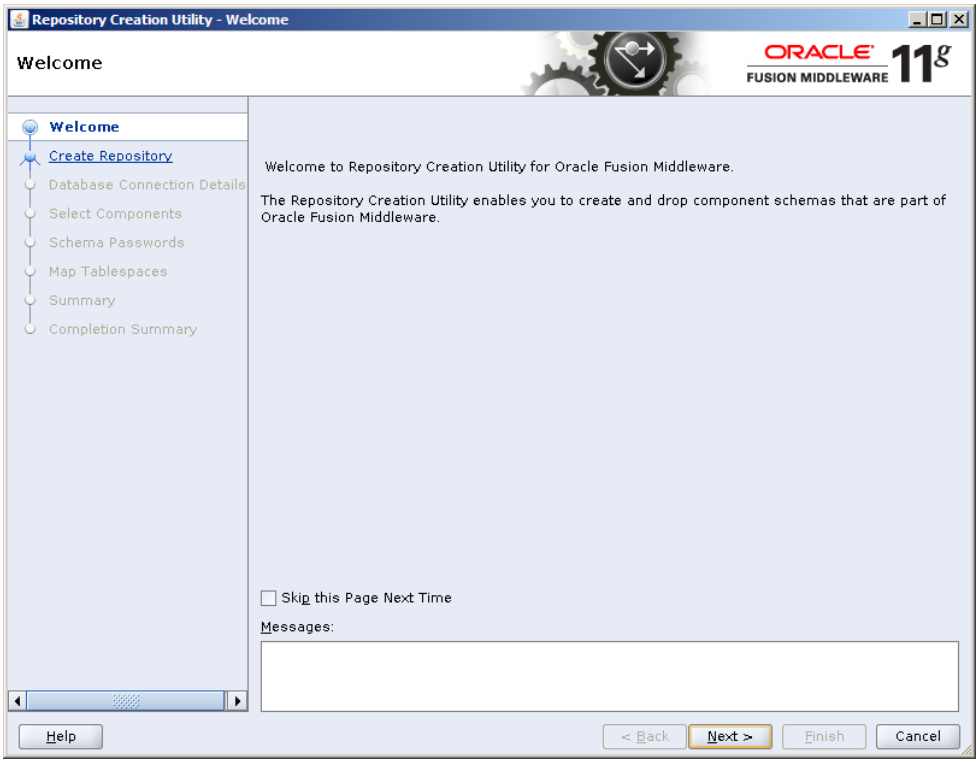
- Using the same software installation for Oracle Fusion Middleware Repository Creation Utility 11g (11.1.1.9.0) that was used for . <INSTALL_DIR>/RCU_11.1.1.9.
- Set the following variables by exporting them before running the installer:
  - JAVA_HOME
  - PATH
  - DISPLAY

  Example:

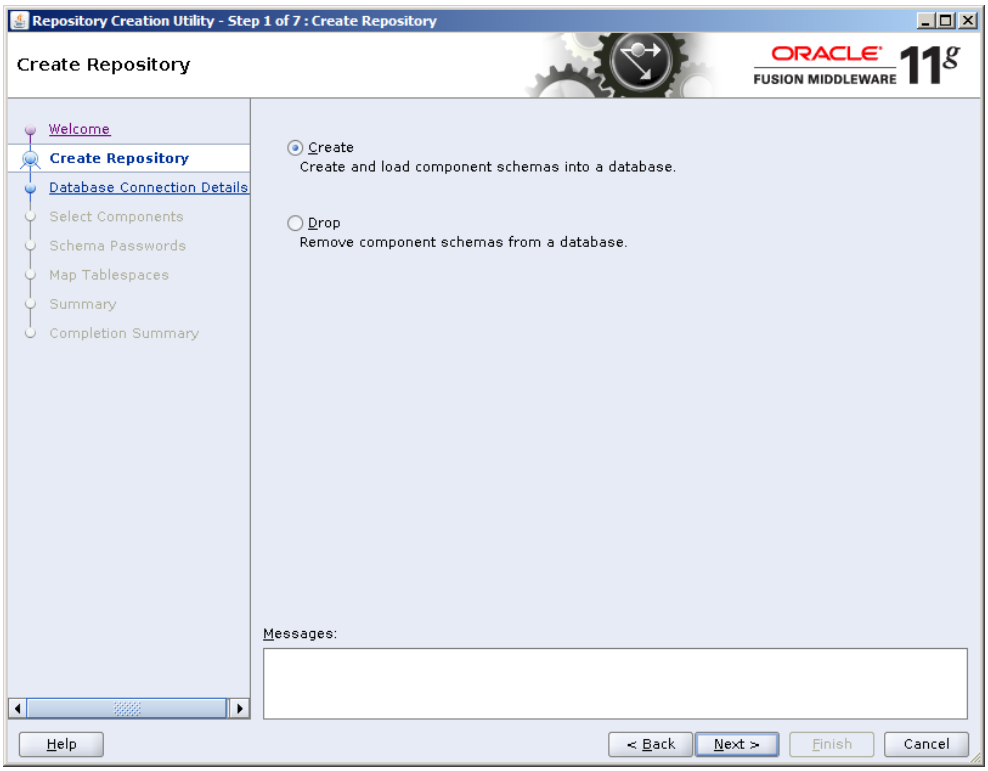
  ```
  $ export JAVA_HOME=/u00/webadmin/products/jdk_java
  $ export PATH=$JAVA_HOME/bin:$PATH
  $ export DISPLAY=<pc_ip_address:0.0>
  ```
- Run the following commands to run the installer:

  Example:

  ```
  $ cd <INSTALL_DIR>/RCU_11.1.1.9/rcuHome/bin
  $ ./rcu
  ```
- The Welcome Window opens. Click **Next**.



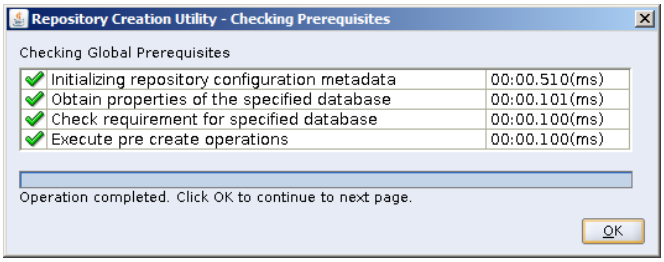
- The Create Repository window opens. Select **Create,** and click **Next**.



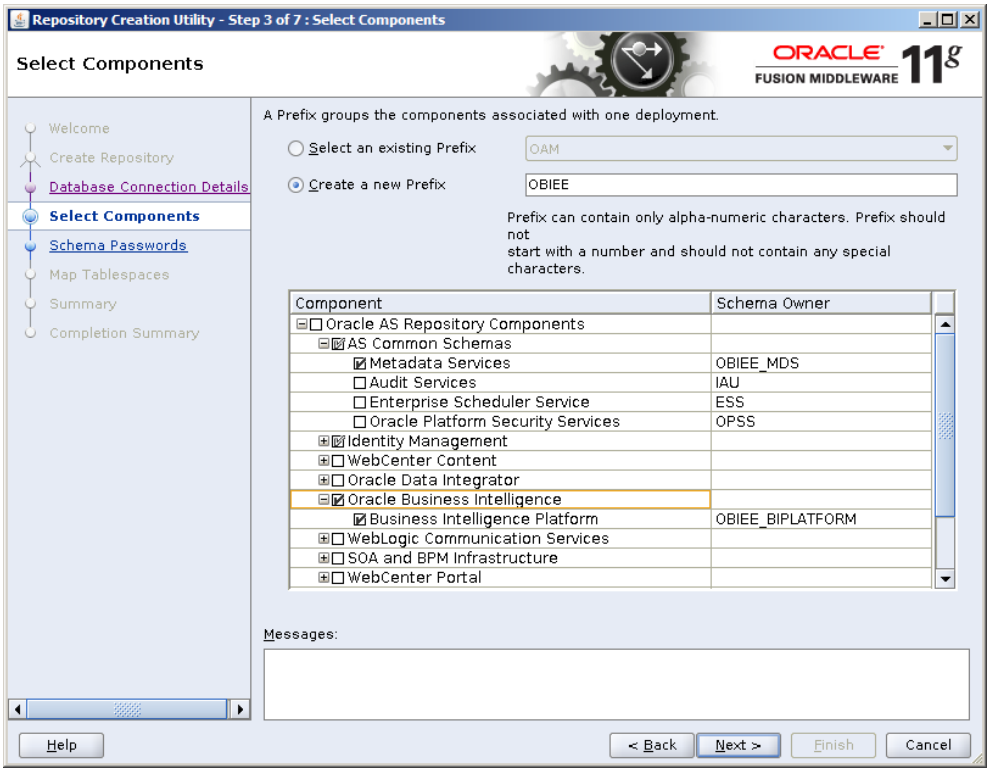
- The Database Connection Details window opens. Provide the database details and click **Next**.
  - Host Name: dbhost-r
  - Port: 1521

- Service Name: fmwservicename
- Username (must have DBA or SYSDBA privileges)
- Password

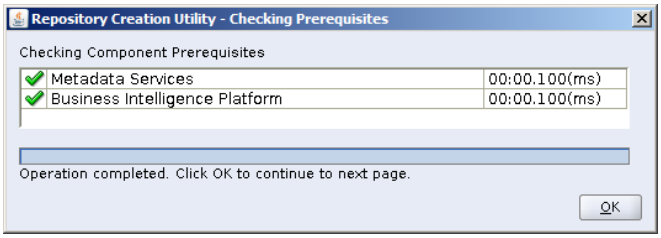
- RCU checks database prerequisites. Click **OK**.



- The Select Components window opens. Select just the following items below and click **Next**.
  - Select **Create a new Prefix: OBIEE.**
  - Click the plus sign (+) next to the Business Intelligence component group.
  - Click Business Intelligence Platform so that a check appears next to it. This action automatically selects the Metadata Services (MDS) schema (under the AS Common Schemas group), which is also required by Oracle Business Intelligence.
  - Do not select the Oracle AS Repository Components option, as this configures RCU to install many other schemas that are not required by Oracle Business Intelligence. Select the following components as shown in the screenshot.

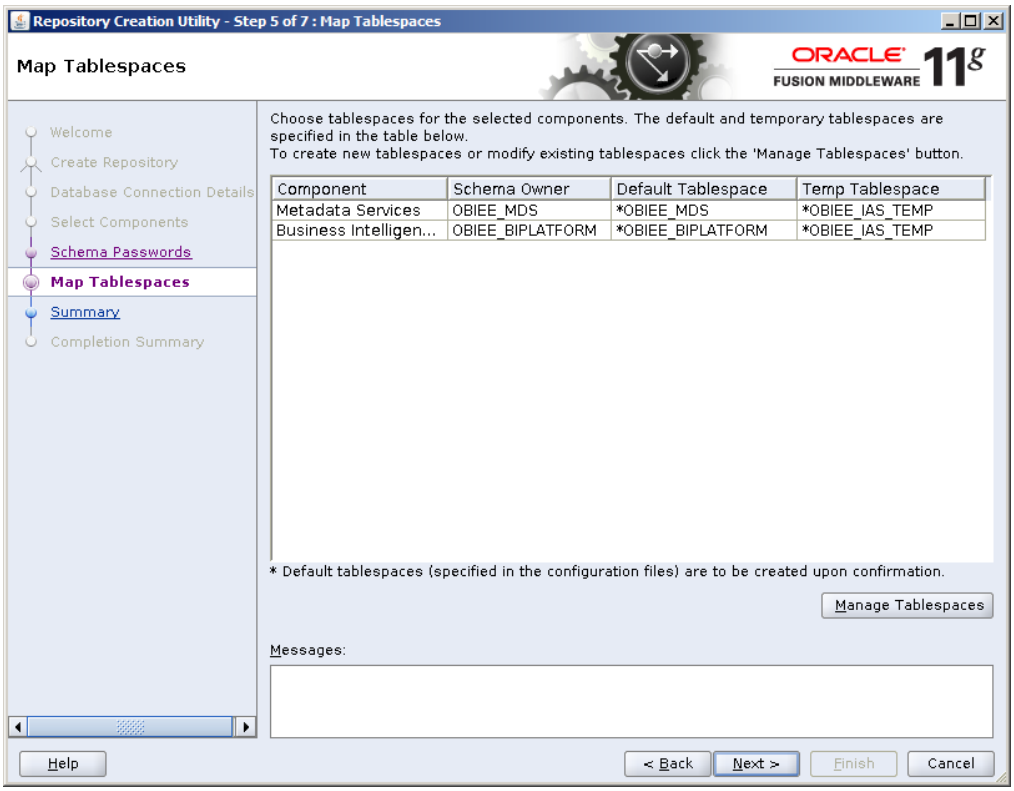


- RCU will check database prerequisites to make sure it can create the selected components. Click **OK**.

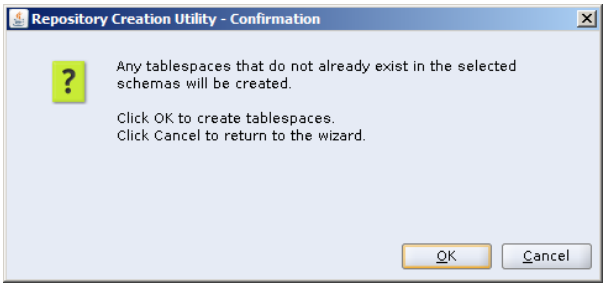


- The Schema Passwords window opens.
  - Select the Use same passwords for all schemas option.
  - Enter the password.
  - Click **Next**.

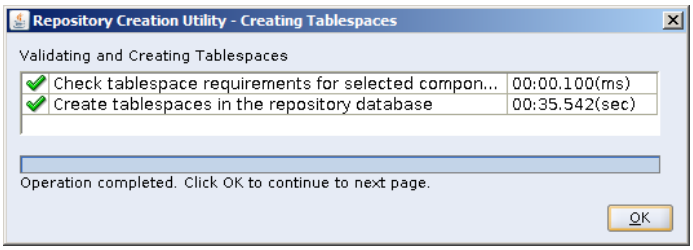
- The Map Tablespaces window opens. Click **Next**.



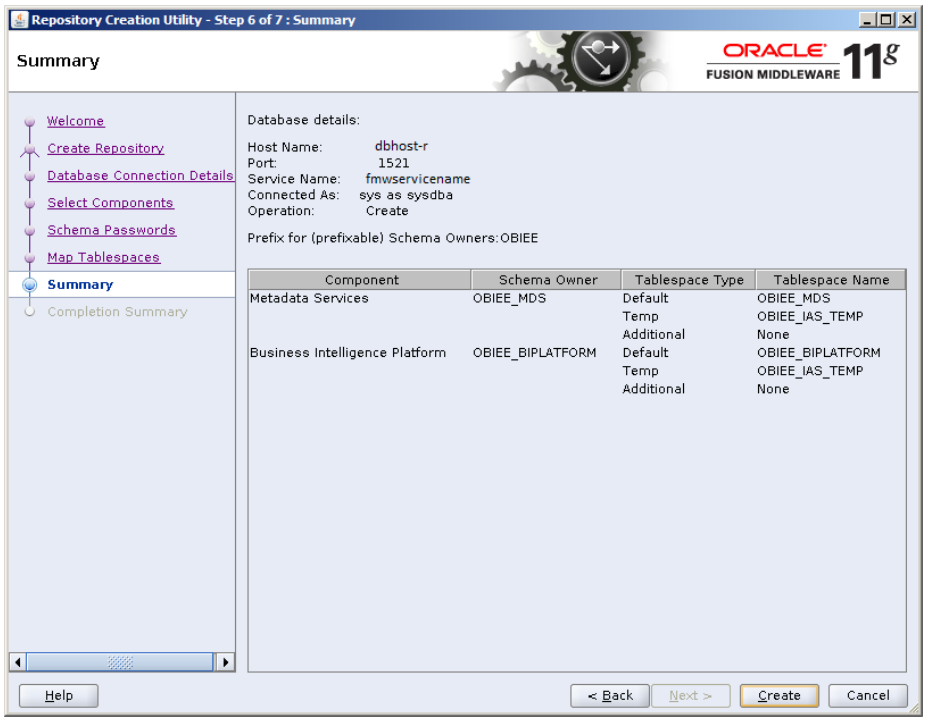
- The Repository Creation Utility - Confirmation window opens. Click **OK**.



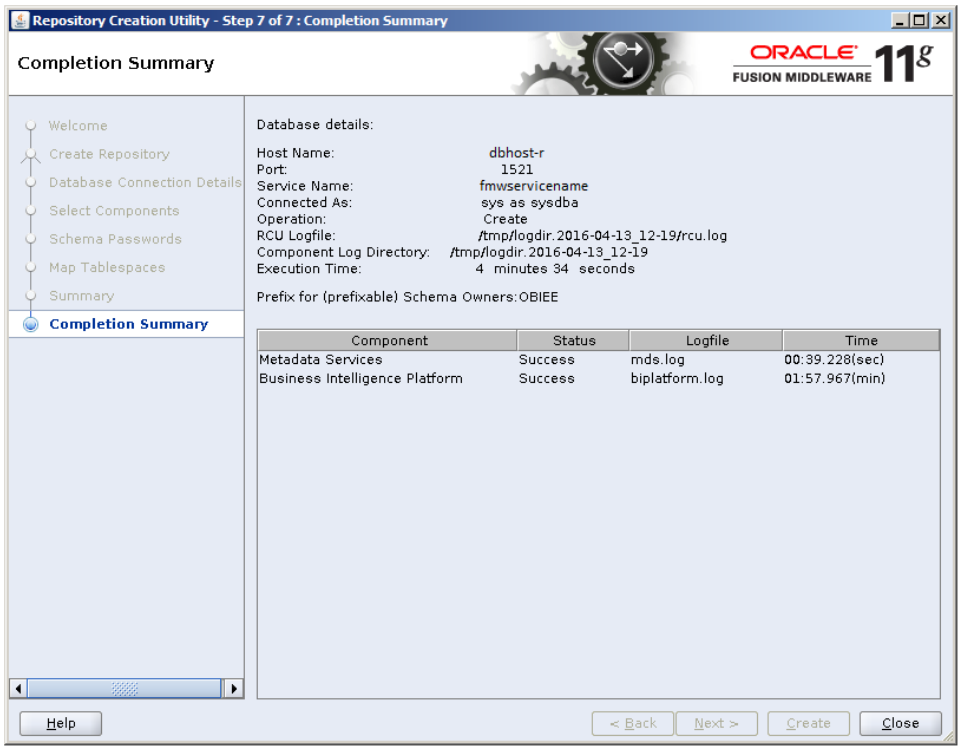
- The Repository Creation Utility – Creating Tablespaces window opens. Click **OK**.



- The Summary window opens. Click **Create**.



- The Completion Summary window opens. Click **Close**.



- The installation is complete.

Install OBIEE Software on idmhost1 and idmhost2

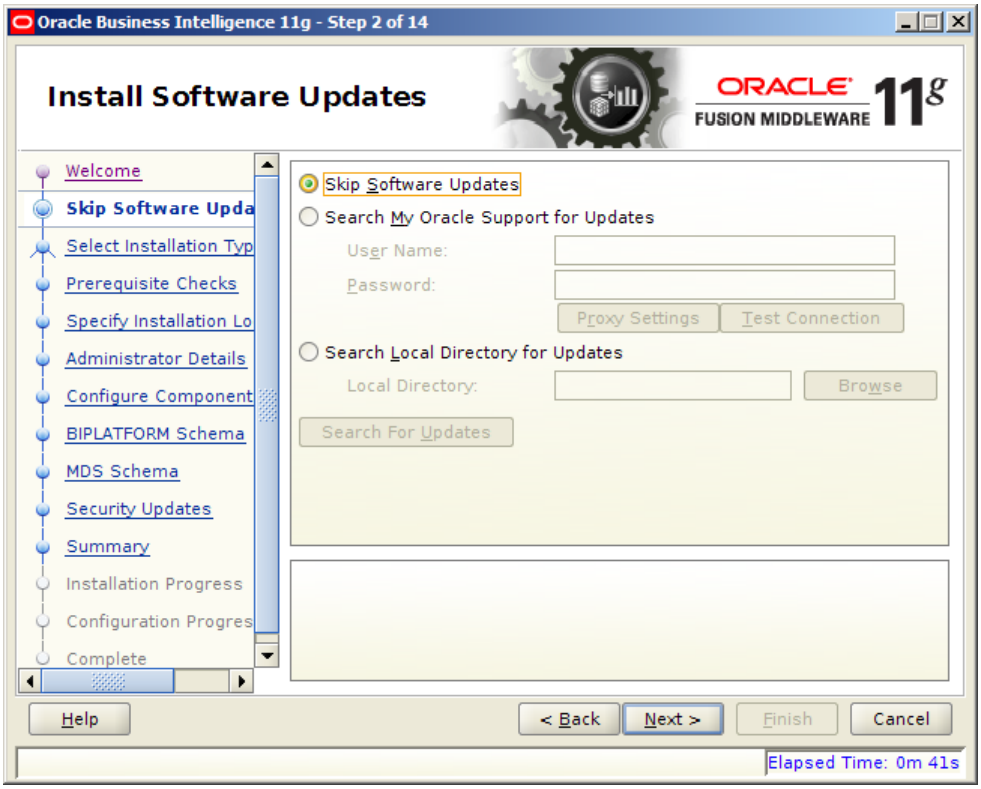
Perform the following steps to install Oracle Access Manager (OBIEE) 11.1.1.9 on idmhost1 and idmhost2:

- Download software installation for OAM 1.1.2.3 and place it in an installation staging directory on the Linux host and extract the contents of the zip files. <INSTALL_DIR>/obiee_11.1.1.9.
- Set the following variables by exporting them before running the installer:
  - JAVA_HOME
  - PATH
  - DISPLAY

    Example:
    ```
    $ export JAVA_HOME=/u00/webadmin/products/jdk_java
    $ export PATH=$JAVA_HOME/bin:$PATH
    $ export DISPLAY=<pc_ip_address:0.0>
    ```
- First on idmhost1 - Run the following commands to run the installer:

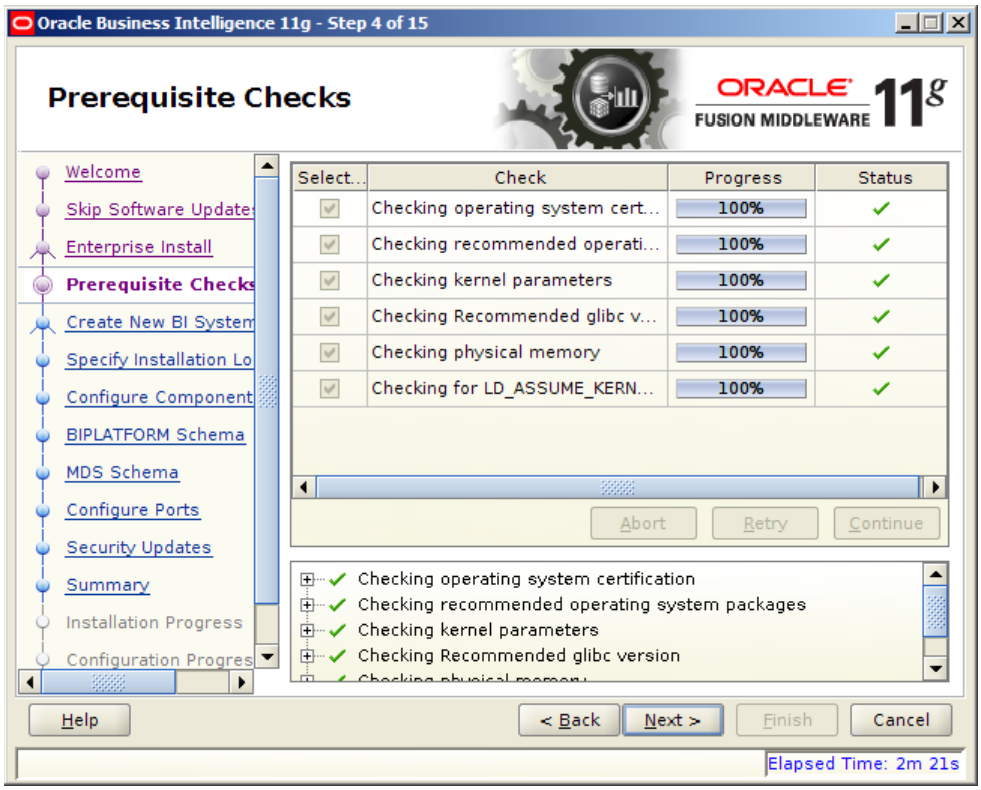
  Example:
  ```
  $ cd <INSTALL_DIR>/obiee_11.1.1.9/bishiphome/Disk1
  $ ./runInstaller
  ```
- The Welcome window opens. Click **Next**.

- The Install Software Updates window opens. Select the **Skip Software Updates** option, and click **Next**.



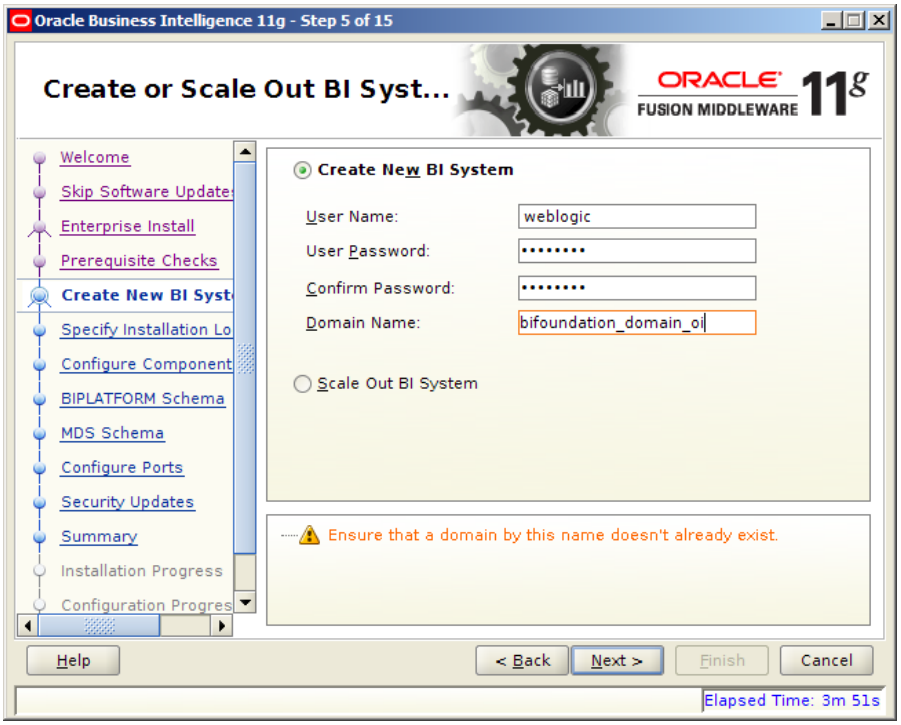
- The Select Installation Type window opens. Select **Enterprise Install**, and click **Next**.

- The Installation Progress window opens. Click **Next** when the prerequisite checks are finished.



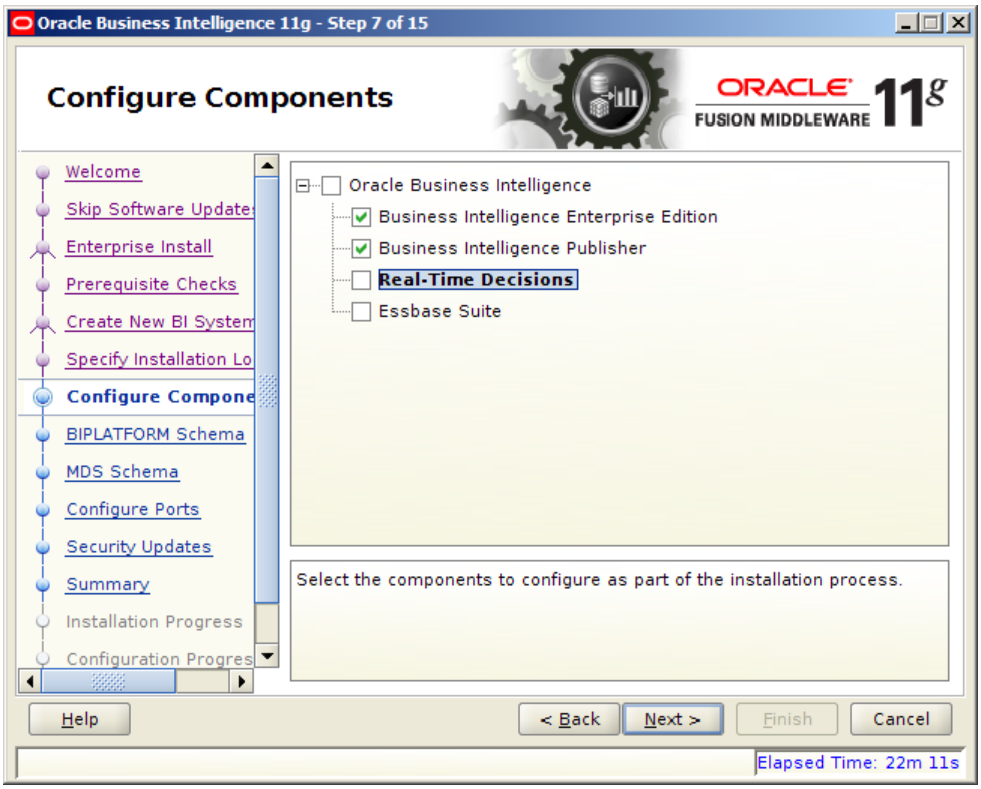
- The Create or Scale Out BI System window opens.
  - Provide the WebLogic admin users password.

  - Provide Domain Name.
  - Click **Next**.



- The Specify Installation Location window opens. Enter the following:
  - Oracle Middleware Home Location: /u00/webadmin/products/wls_obiee_oi
  - Oracle Home Directoy: Defaulted by value provided by Oracle Middleware Home Location
  - WebLogic Server Directoy: Defaulted by value provided by Oracle Middleware Home Location
  - Oracle Instance Location: /vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1
  - NOTE: The Oracle Instance Location has to be in a directory that is shared by both idmhost1 and idmhost2
  - Oracle Instance Name: instance1
  - Click **Next**.

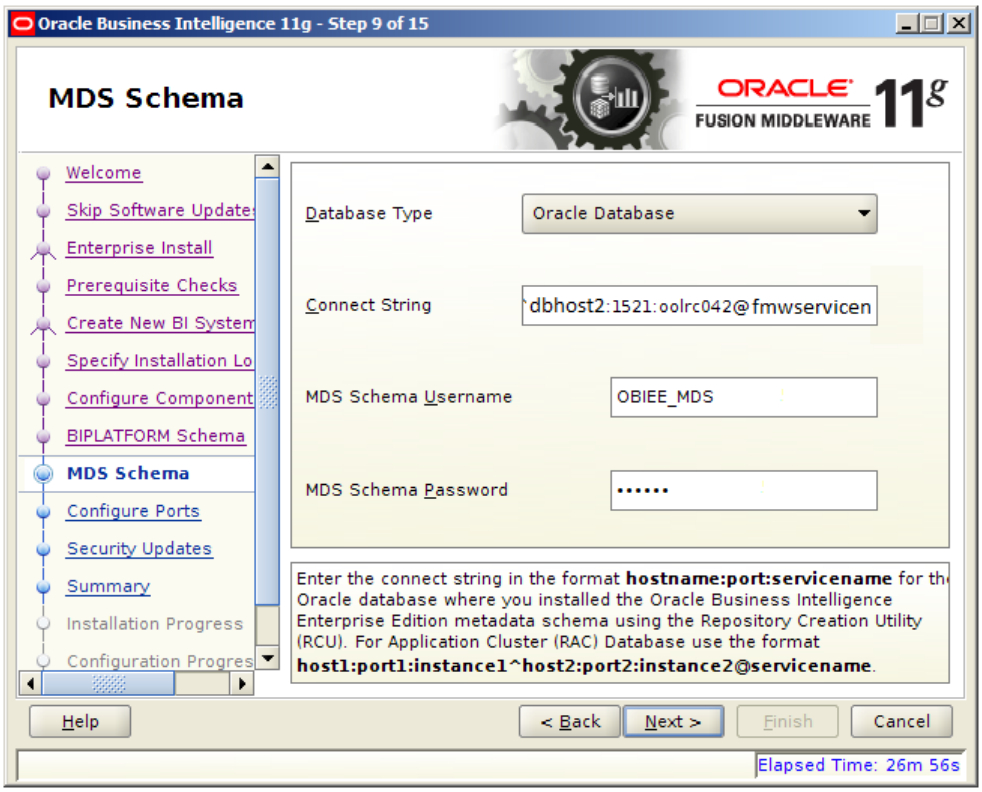
- The Configure Components window opens. Select the following as shown in the screenshot, and click **Next**.
  - Business Intelligence Enterprise Edition
  - Business Intelligence Publisher



- The BIPLATFORM Schema window opens.
  - Database Type: Oracle Database

- Connect String: dbhost1:1521:oolrc041^dbhost2:1521:oolrc042@fmwservicename
  a. This should be setup as a clustered RAC database connection string.
- BIPLATFORM Schema Username: OBIEE_BIPLATFORM
  a. This is one of the schemas that were setup using RCU.
- BIPLATFORM Schema Pasword: <password>
- Click **Next**.

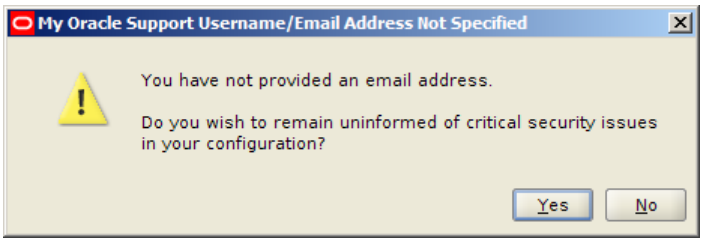
- The MDS Schema Complete window opens.
  - Database Type: Oracle Database
  - Connect String: dbhost1:1521:oolrc041^dbhost2:1521:oolrc042@fmwservicename
  - This should be setup as a clustered RAC database connection string.
  - MDS Schema Username: OBIEE_MDS
  - This is one of the schemas that were setup using RCU.
  - MDS Schema Pasword: <password>
  - Click **Next**.



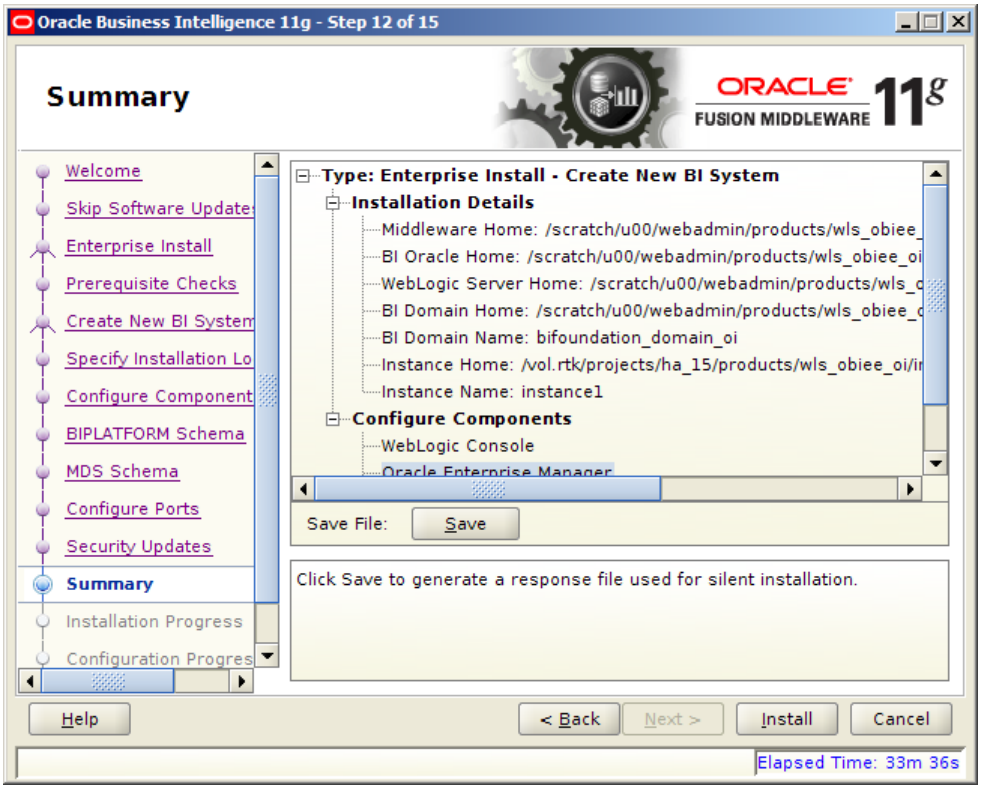
- The Configure Ports window opens.
  - Select the radio button – Specify Ports using Configuration file.
  - Navigate to and copy the sample staticports.ini from:
  - <INSTALL_DIR>/ obiee_11.1.1.9/bishiphome/Disk1/stage/Response directory,
  - to: (You may need to create this directory on the host if it does not yet exist.)
  - /u00/webadmin/ports/
  - Rename it as staticports_obiee.ini and modify the values as per Appendix VI - Creating Staticports for OBIEE Configuration
  - Click **Next**

- The Specify Security Updates window opens. Uncheck the checkbox and click **Next**.

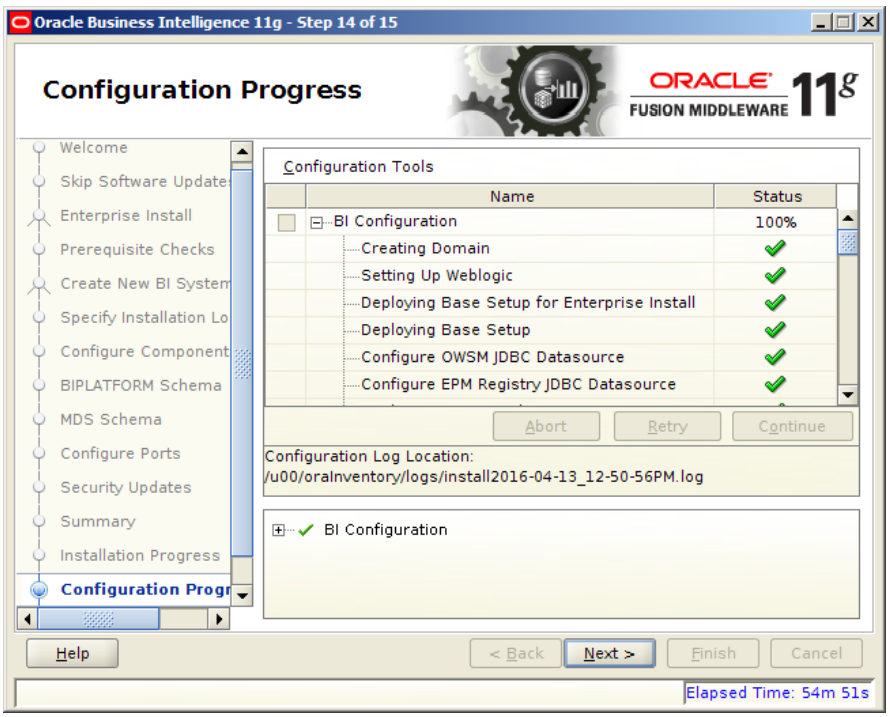
- A warning is displayed in a pop-up window. Click **Yes**.



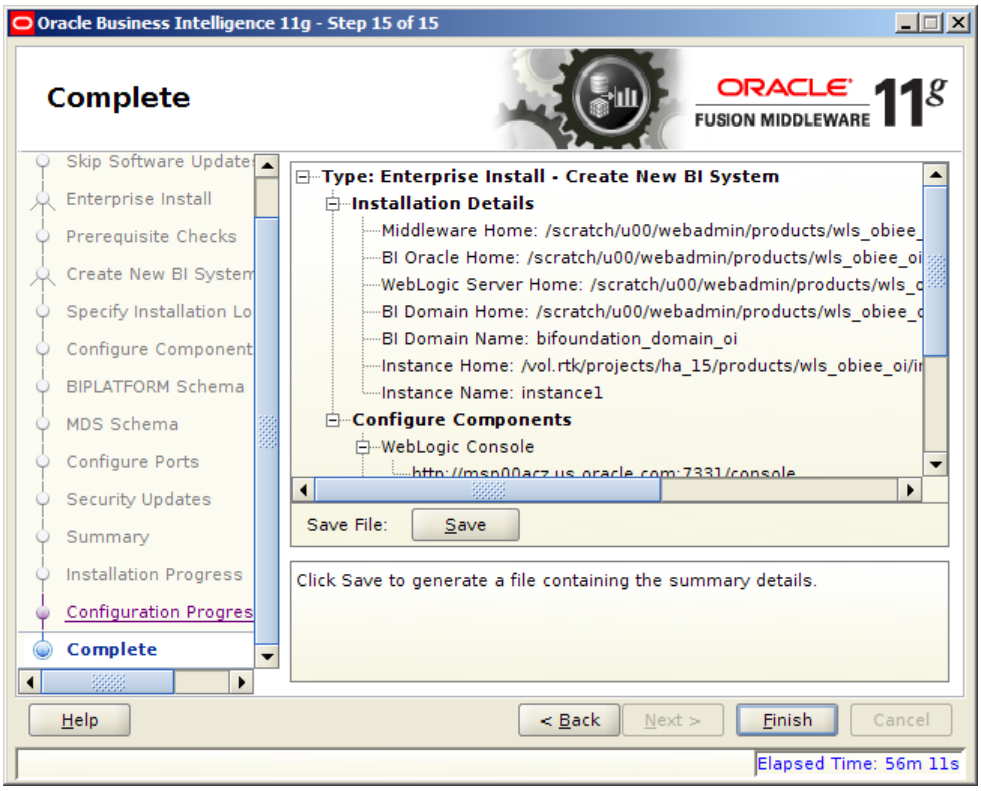
- The Summary window opens. Click **Install**.



- The Configuration Progress window opens. Click **Next**.



- The Complete window opens. Click **Finish**.



- The installation is complete for idmhost1.
- On idmhost2 - Run the following commands to run the installer and scale out the OBIEE configuration to idmhost2 :

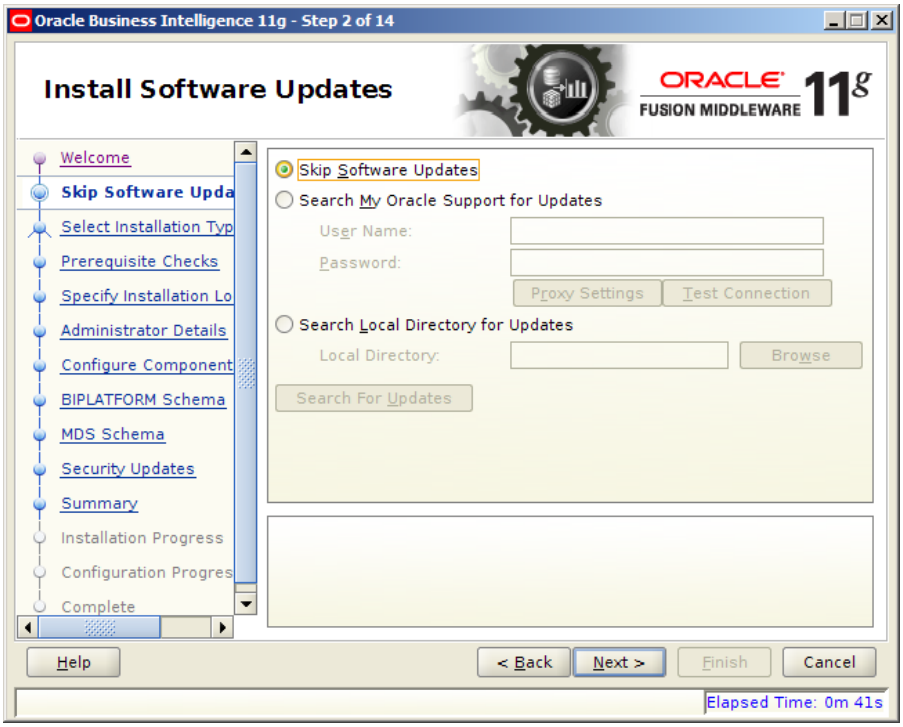
  Example:

  ```
  $ cd <INSTALL_DIR>/obiee_11.1.1.9/bishiphome/Disk1
  ```

```
$ ./runInstaller
```

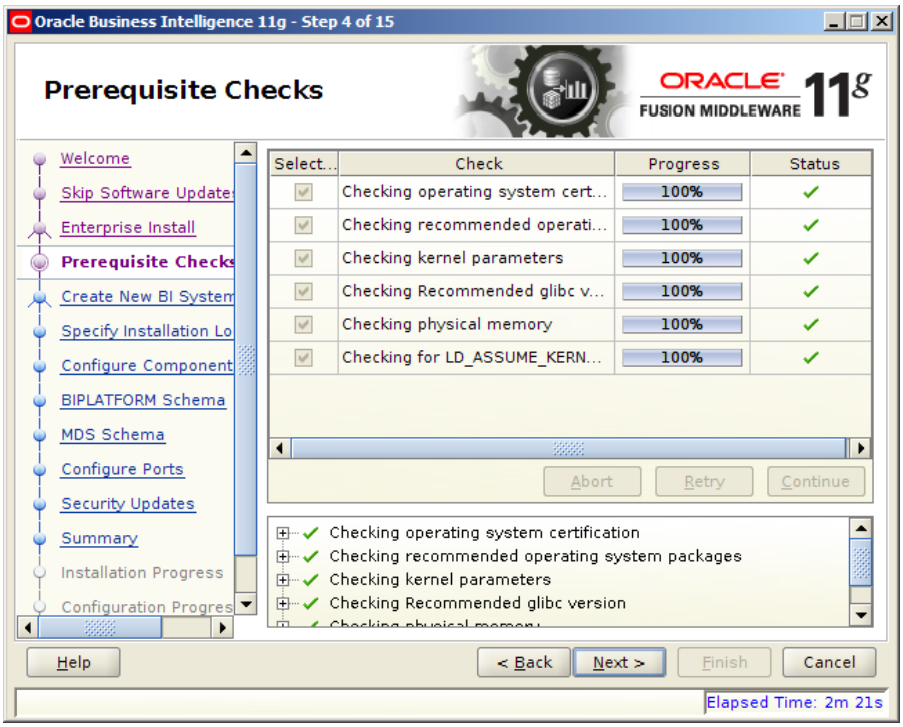
- The Welcome window opens. Click **Next**.

- The Install Software Updates window opens. Select the **Skip Software Updates** option and click **Next**.



- The Select Installation Type window opens. Select **Enterprise Install** and click **Next**.

- The Prerequisite Checks window opens. Click **Next** when the prerequisite checks are finished.



- The Create or Scale Out BI System window opens.
  - Select **Scale Out Bi System.**
  - Host Name: idmhost1
    - **a.** Needs to be the host that the BI System was created on.
  - Port: 7331

a. Needs to be the WebLogic admin server port that was setup on idmhost1.

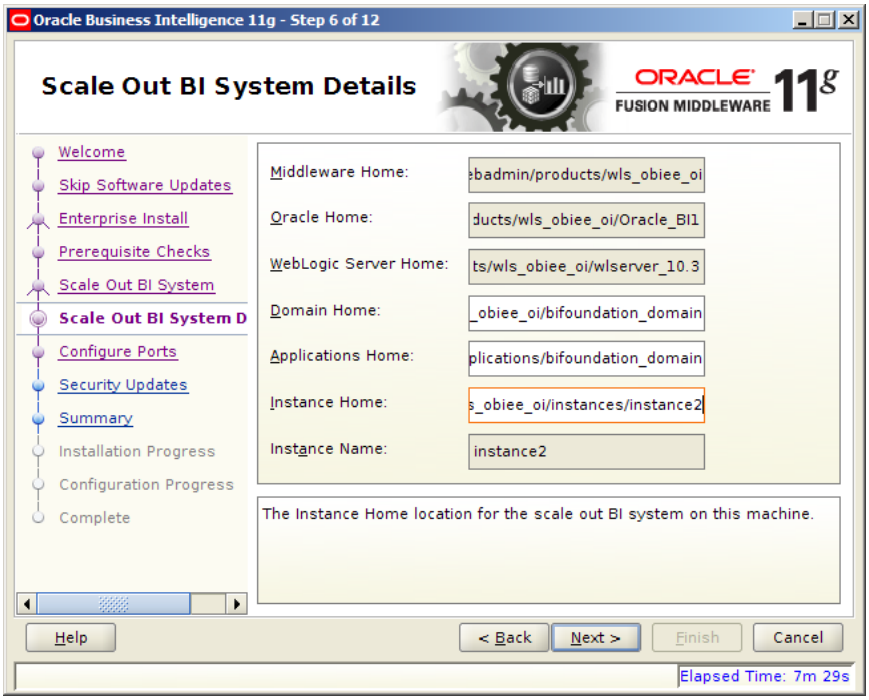
– User Name: weblogic

a. Needs to be the username that was setup on idmhost1 for the WebLogic administrator.

– User Password: <Password>

– Click **Next**.

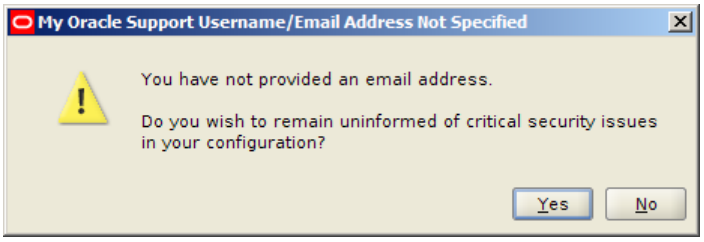
- The Scale Out BI System Details window opens. Enter in the following:
  – Oracle Middleware Home Location: (defaulted from idmhost1 creation)
  – Oracle Home: (defaulted from idmhost1 creation)
  – WebLogic Server Home: (defaulted from idmhost1 creation)
  – Domain Home: /u00/webadmin/config/domains/wls_obiee_oi/bifoundation_domain_oi
  – Applications Home: /u00/webadmin/config/applications/wls_obiee_oi/bifoundation_domain_oi
  – Oracle Instance Location: /vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance2
  – Oracle Instance Name: instance2
  – Click **Next**.



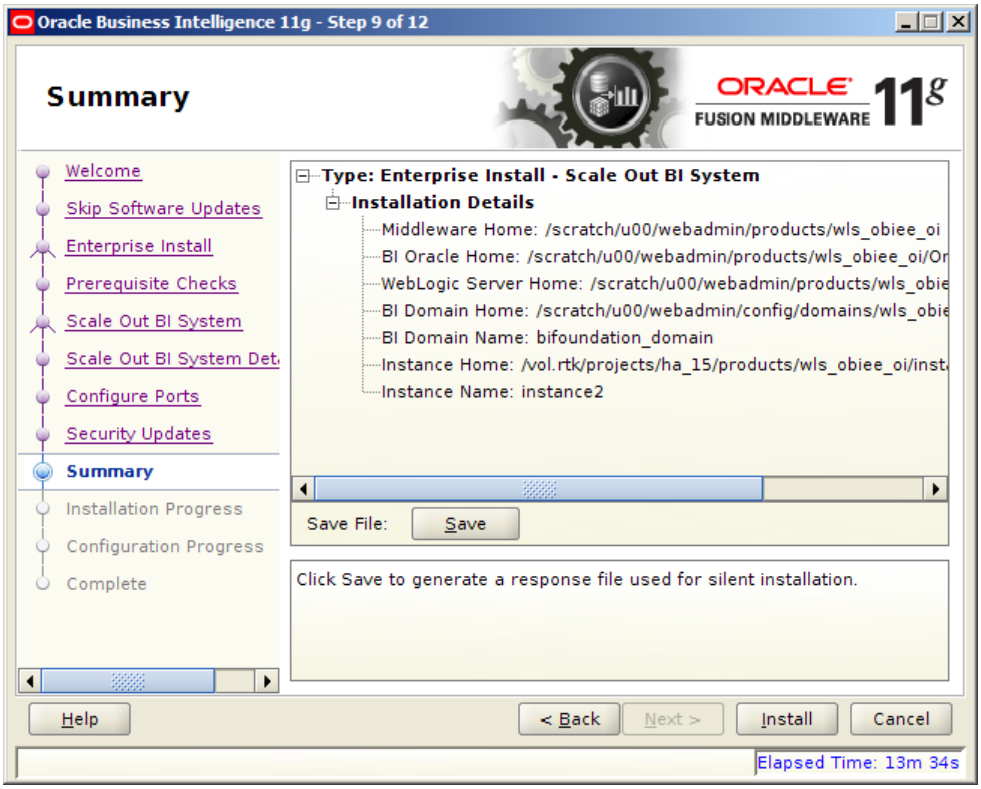
- The Configure Ports window opens. Click **Next**.
  - Use the radio button to select Specify Ports using Configuration file
    Copy the staticports_obiee.ini file /u00/webadmin/ports/
    from:
    idmhost1:/u00/webadmin/ports/
    to:
    idmhost2:/u00/webadmin/ports/
  - Click **Next**

- The Specify Security Updates window opens. Uncheck the checkbox and click **Next**.

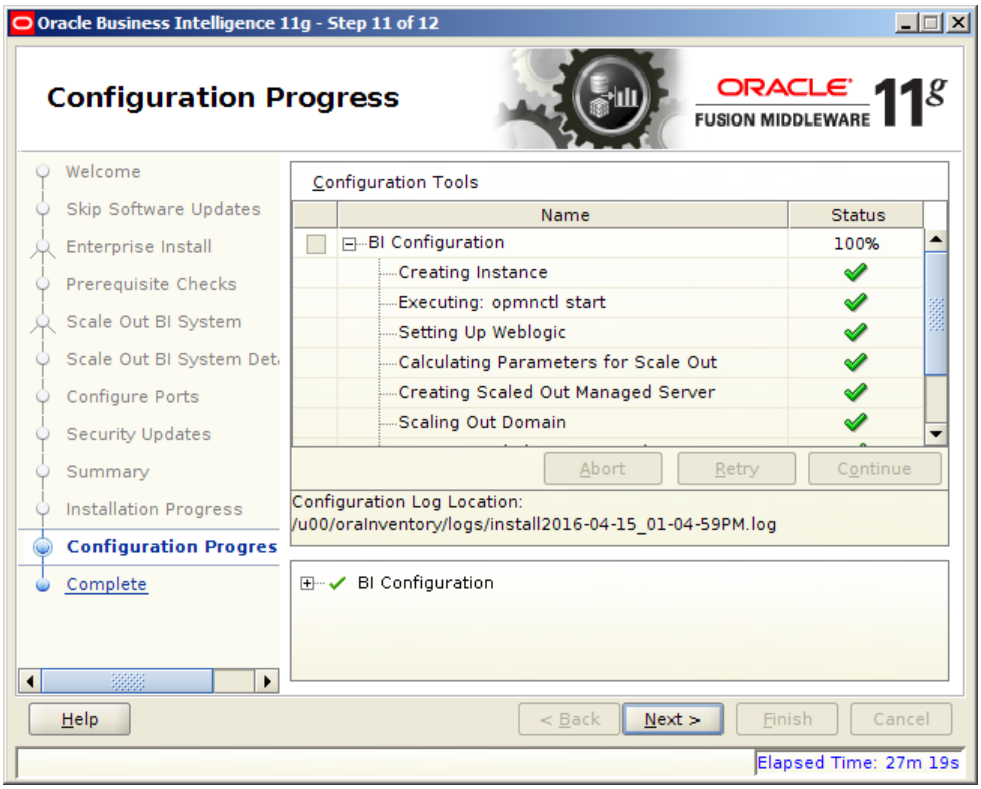
- A warning is displayed in a pop-up window. Click **Yes**.



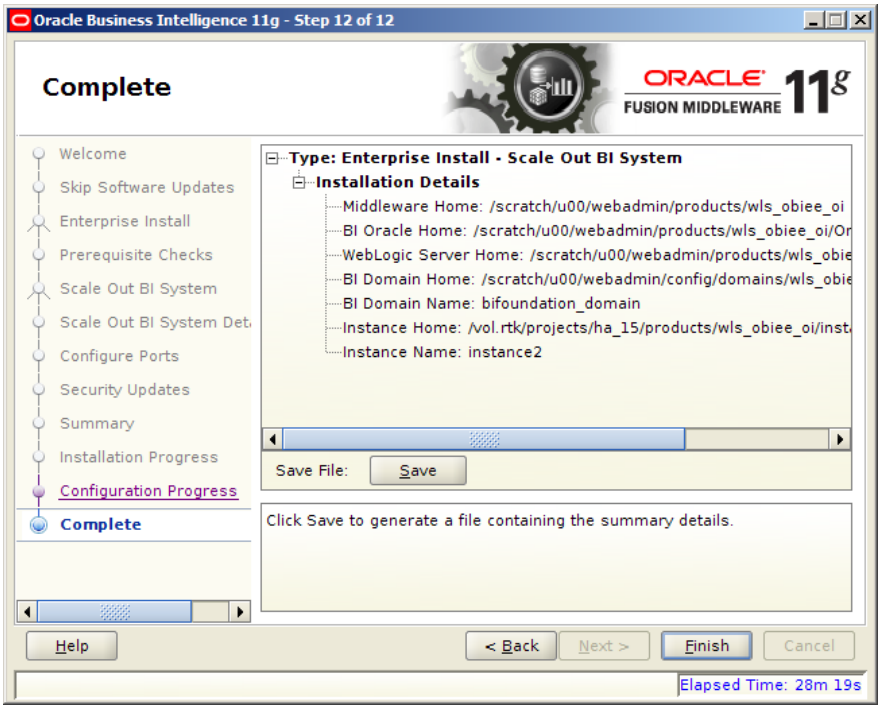
- The Summary window opens. Click **Install**.



- The Configuration Progress window opens. Click **Next**.



- The Complete window opens. Click **Finish**.



- The installation is complete for idmhost2.

Create WebLogic boot.properties for OBIEE WLS Domain on idmhost1

Start WebLogic admin server and create WebLogic boot.properties file with username and password so that the startup script does not prompt or require user input to start the admin server.

Create WebLogic boot.properties as follows:

- On idmhost1 - navigate to <DOMAIN_HOME>/bin and run the startWebLogic.sh script. Enter in the admin server name user and password when prompted

  Example:
  ```
  $ cd /u00/webadmin/config/domains/wls_obiee_oi/bifoundation_domain_oi/bin
  $ ./startWebLogic.sh
  username=weblogic
  password=<password>
  ```
- Shut down the admin server.
- Navigate to <DOMAIN_HOME>/servers/AdminServer/security. If the security directory does not yet exist – create it.
- Create a new file called boot.properties and add the WLS admin username and password credentials.

  Example:
  ```
  $ cd
  /u00/webadmin/config/domains/wls_obiee_oi/bifoundation_domain_oi/servers/A
  dminServer/security
  $ vi boot.properties

  username=weblogic
  password=<password>
  ```

- Start the WebLogic admin server.

  Example:
  ```
  $ cd /u00/webadmin/config/domains/wls_obiee_oi/bifoundation_domain_oi/bin
  $ nohup ./startWebLogic.sh &
  ```
- Log onto the WebLogic admin server and start the managed servers.

Configure OID Provider in Oracle BI EE WebLogic Domain

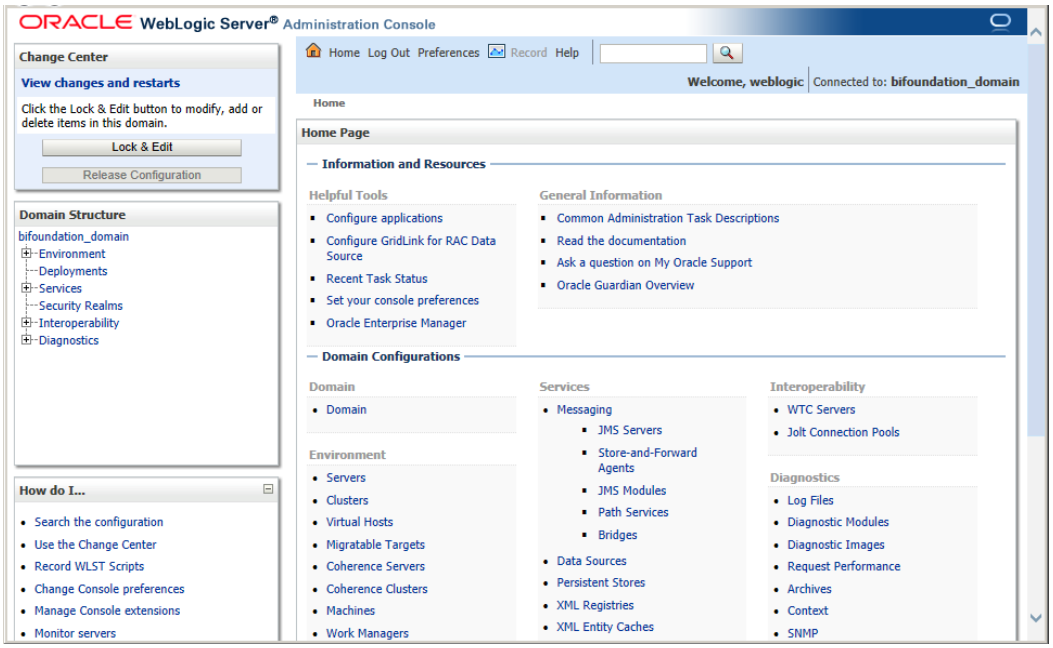
The OID Provider needs to be configured in Oracle BI EE WebLogic domain.

> **Note:** In this section, the base DN "dn=us,dn=oracle,dn=com" is used as an example. Modify this value as per your organization's LDAP settings.

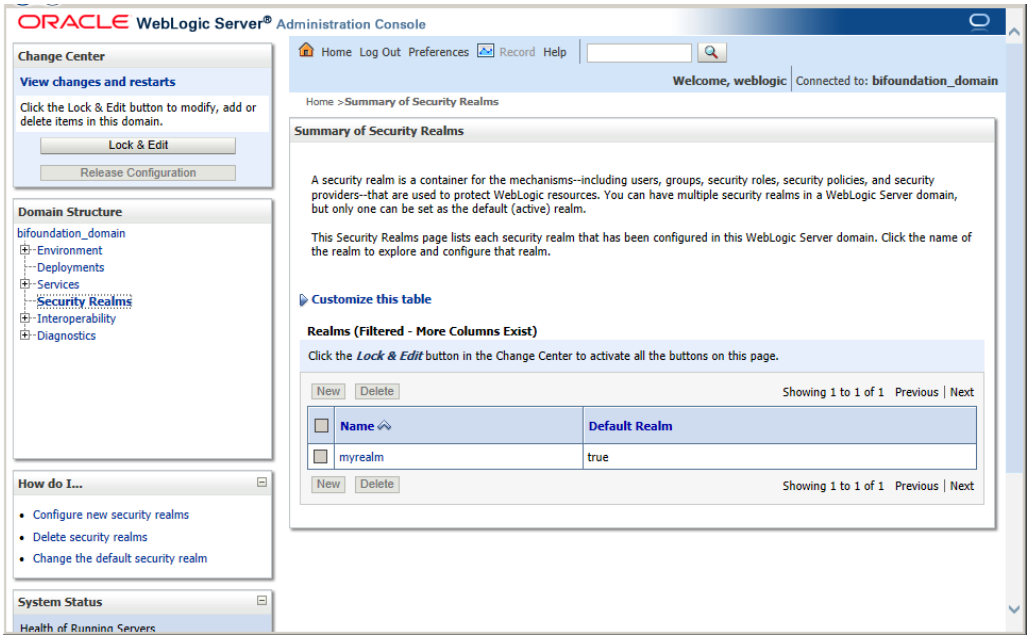
Perform the following procedure to create providers, in the domain created in the previous steps.

- Log in to the Administration Console.

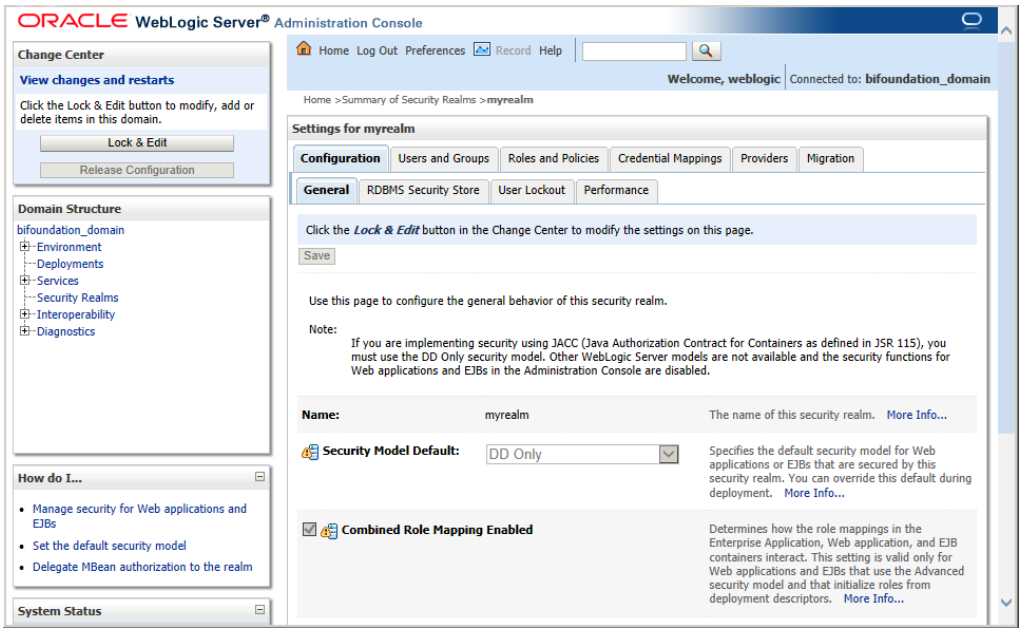
- In the Domain Structure frame, click **Security Realms**.



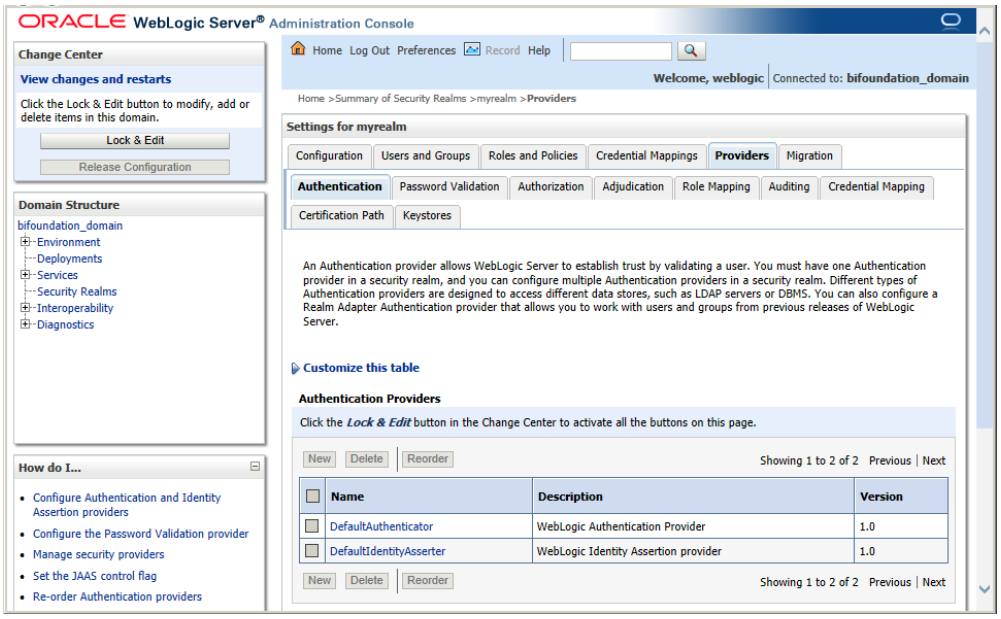
- In the Realms table, click **myrealm**.



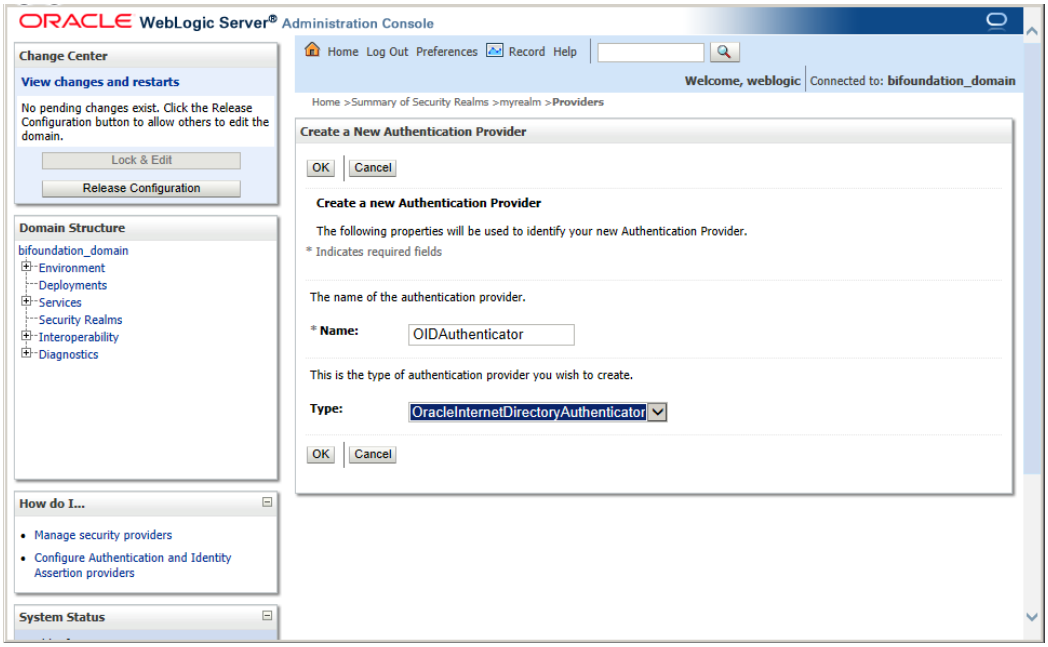
- The Settings for myrealm window opens. Click the **Providers** tab.



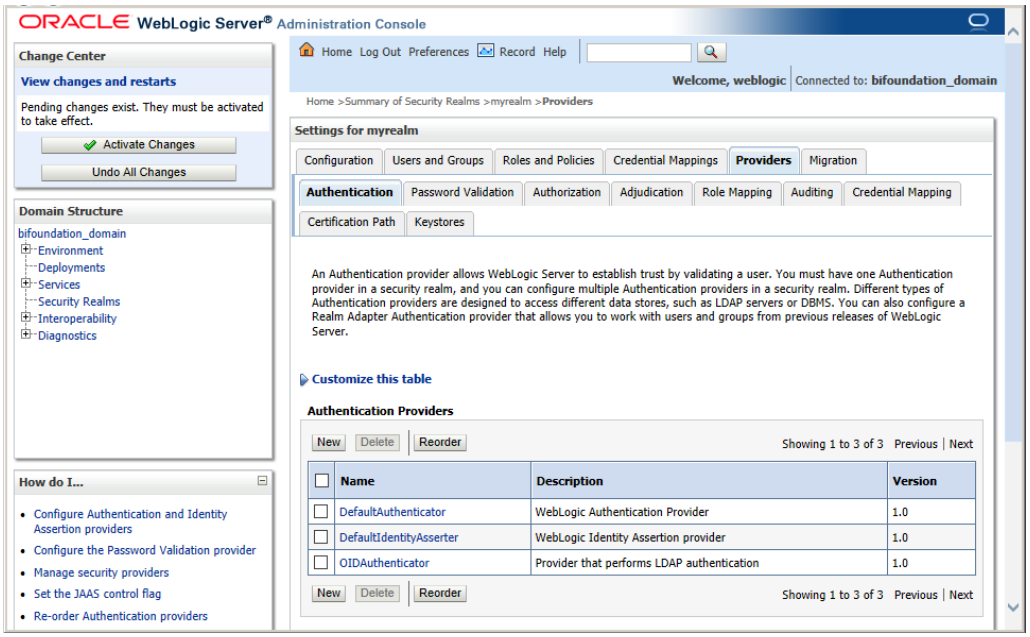
- Click **Lock & Edit** and then click **New**. The Create a New Authentication Provider window opens.



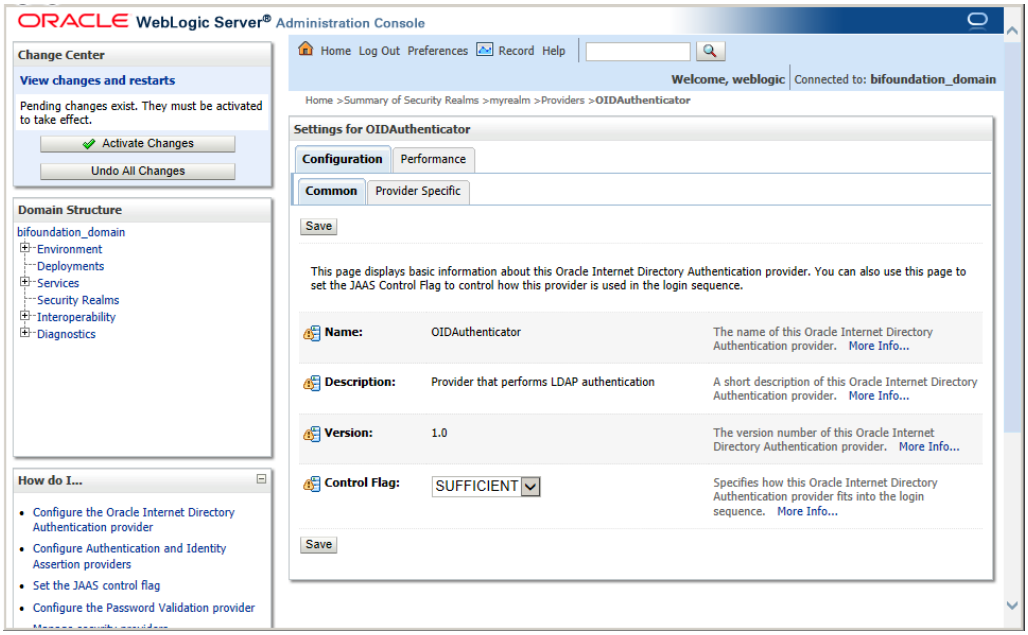
- Enter OIDAuthenticator in the Name field and select **OracleInternetDirectoryAuthenticator** as the type. Click **OK**.



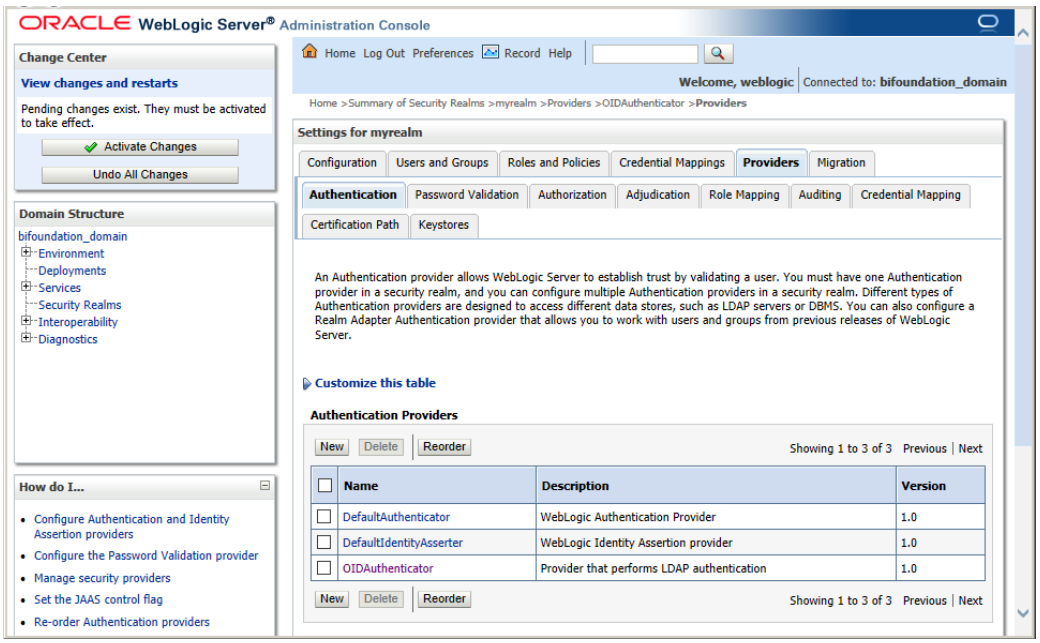
- All the providers are displayed. Click **OIDAuthenticator**.



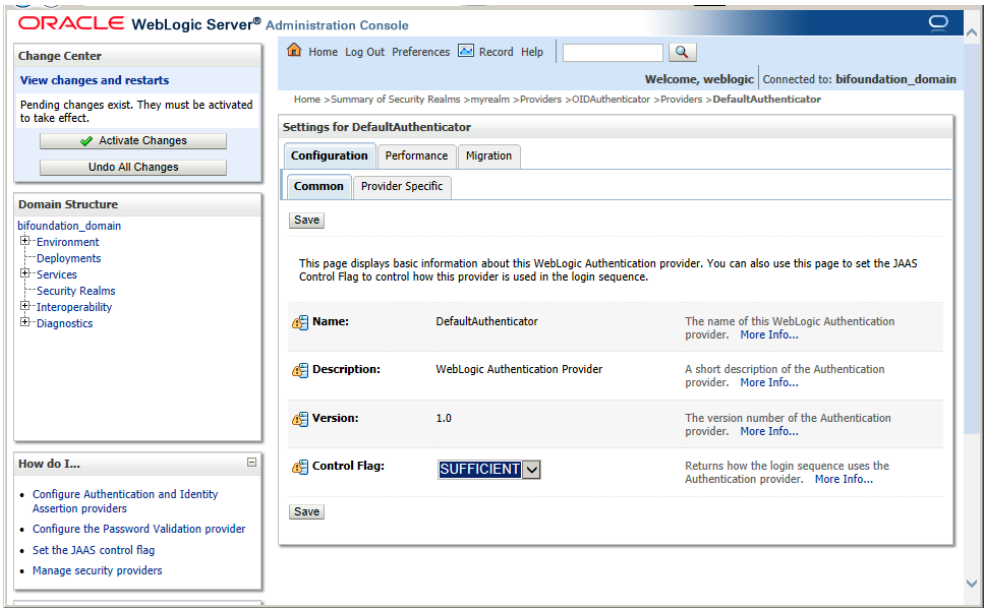
- Settings of OIDAuthenticator are displayed - Set the Control Flag field to SUFFICIENT and click **Save**. Then Click the **Providers** link at the top of the screen.



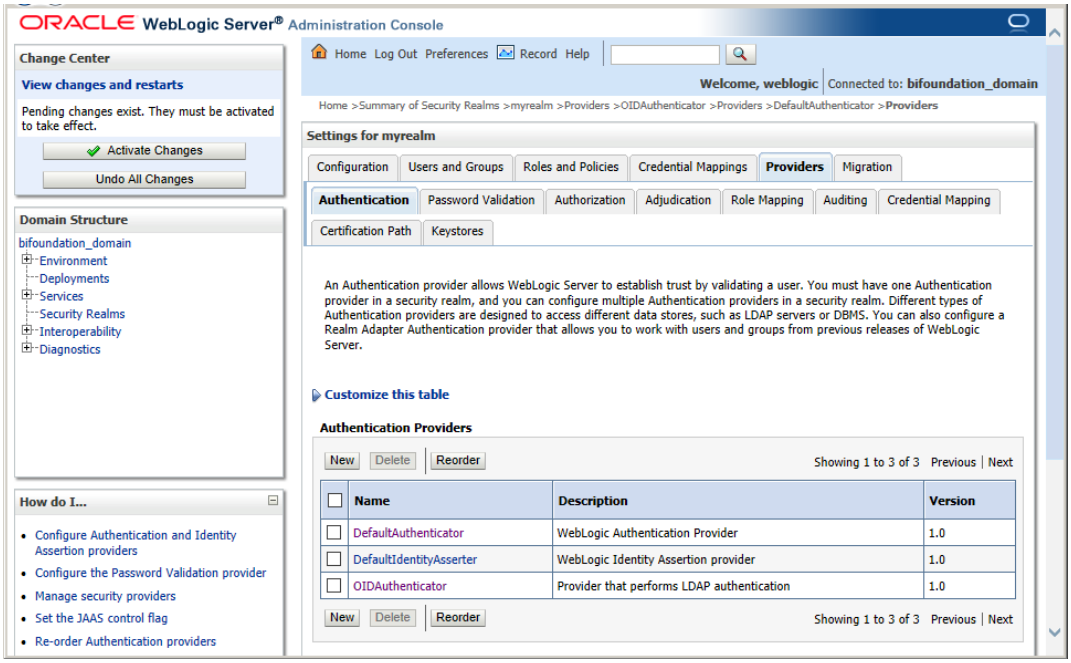
- From the Providers tab, click **DefaultAuthenticator**



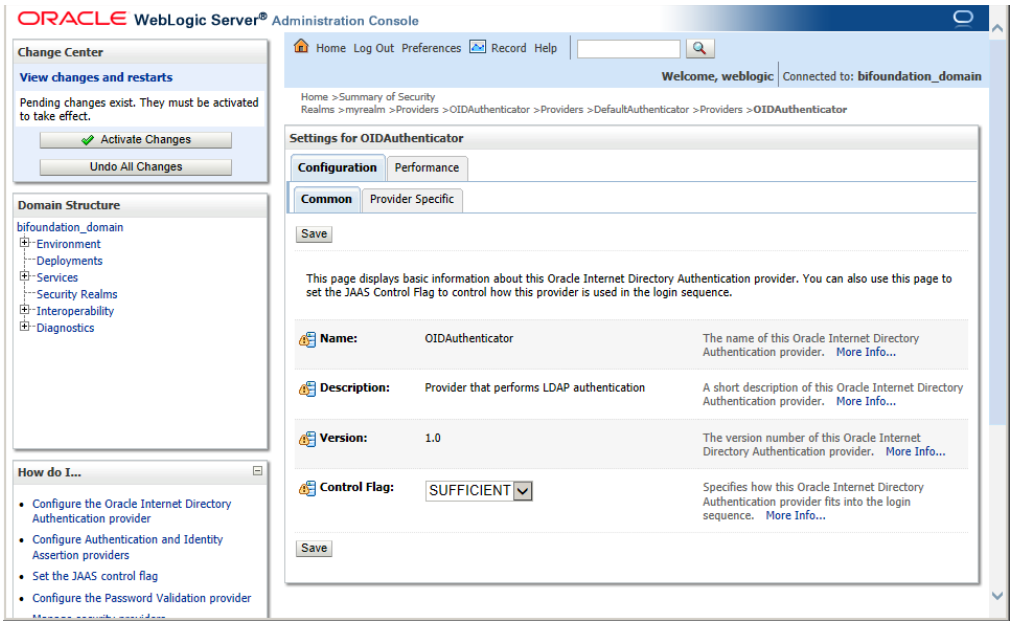
- From Configuration tab and Common sub-tab, update the Control Flag to **SUFFICIENT** and click **Save**. Then click the **Providers** link at the top of the screen.



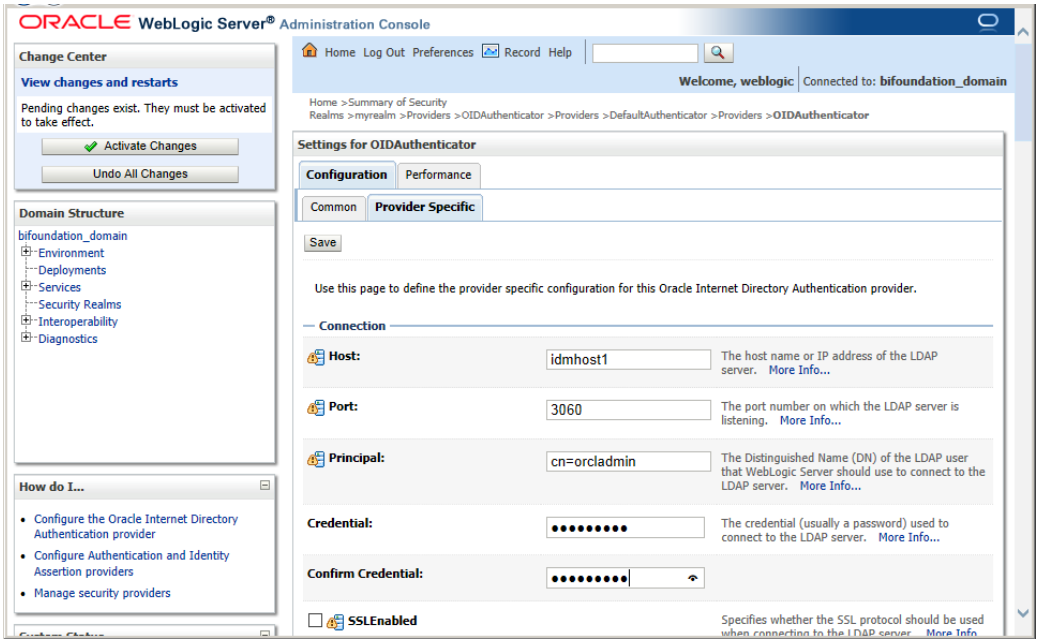
- Click the **OIDAuthenticator** link.

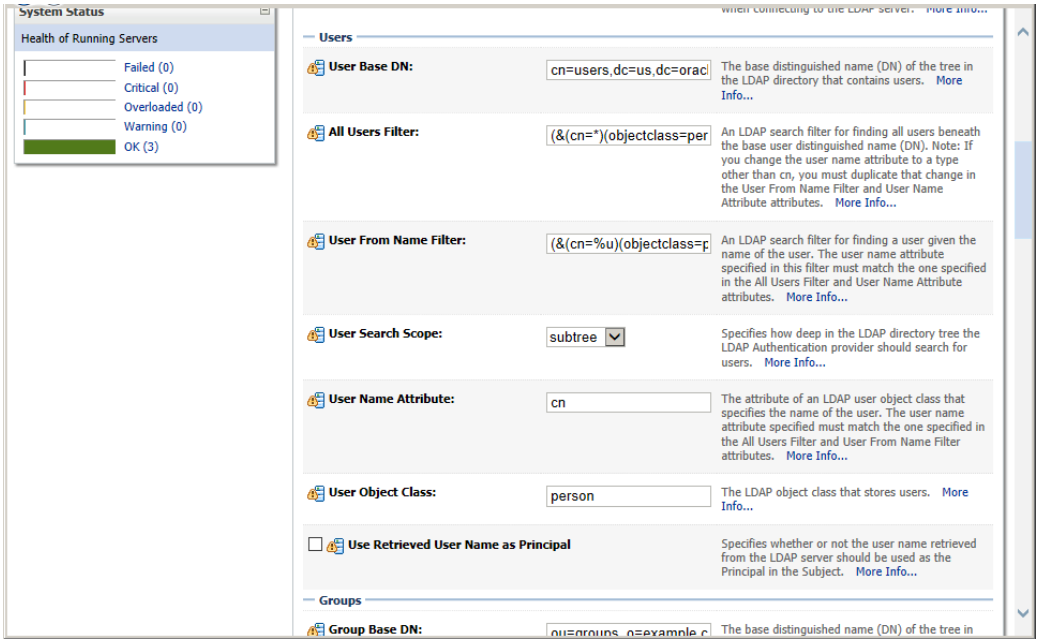


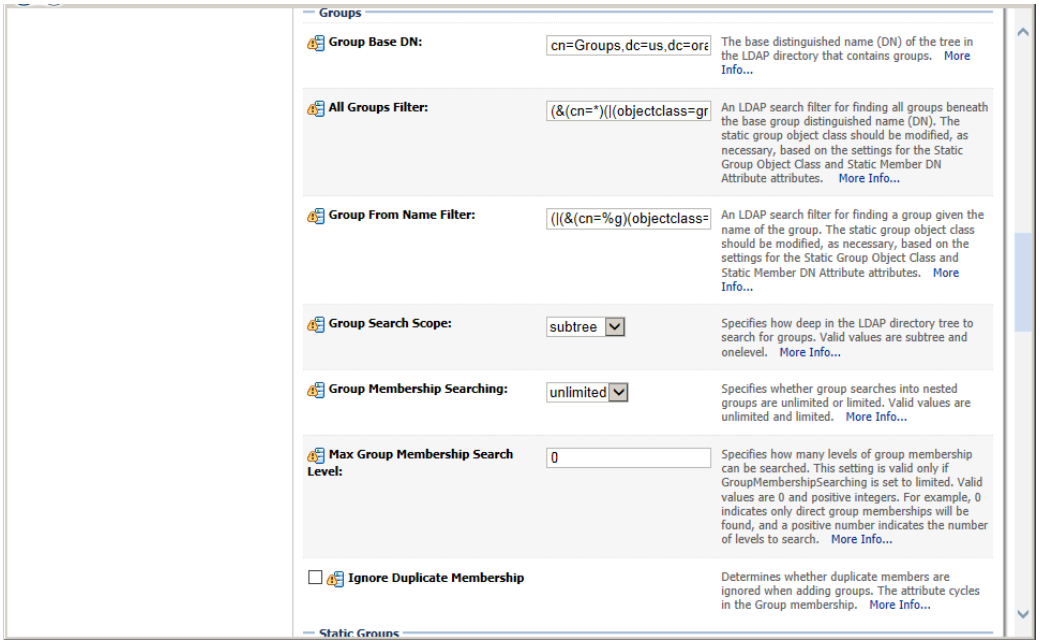
- Click the **Provider Specific** tab.

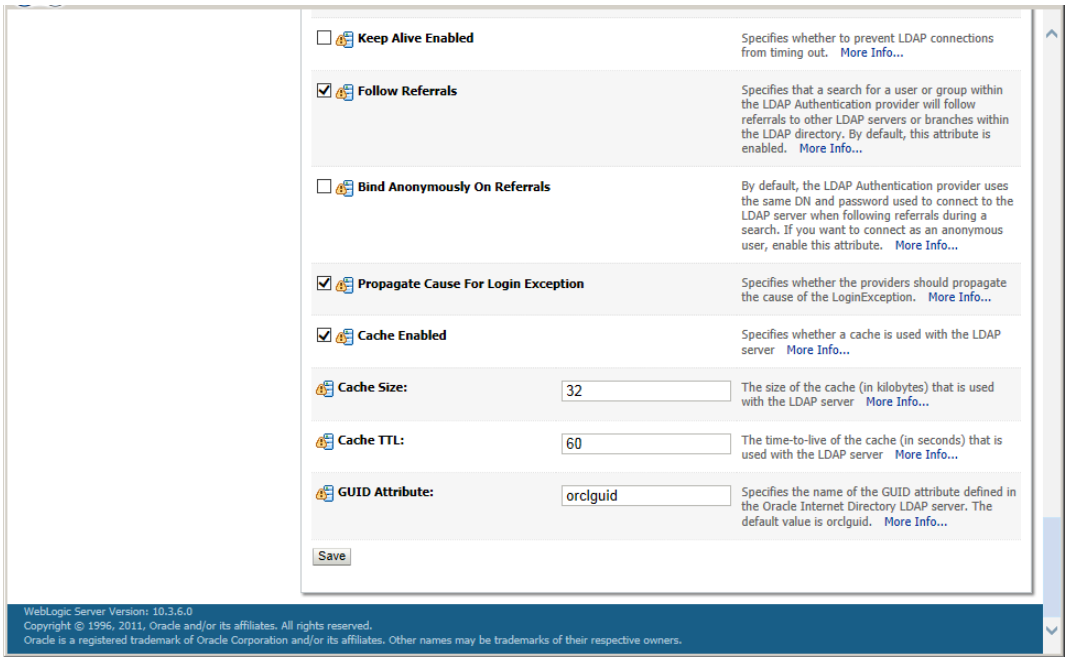


- Make the following changes and Click **Save**. Then click the **Providers** link at the top of screen. (Screen shots shown as it is scrolled down to make the changes.)
  - Host: idmhost1
  - Port: 3060
  - Principal: cn=orcladmin
  - Credential: <password>
  - Confirm Credential: <password>
  - User Base DN: cn=users,dc=us,dc=oracle,dc=com
  - Check 'Retrieve credentials as principal.'
  - Group Base DN: cn=Groups,dc=us,dc=oracle,dc=com
  - Check Propagate Cause For Login Exception

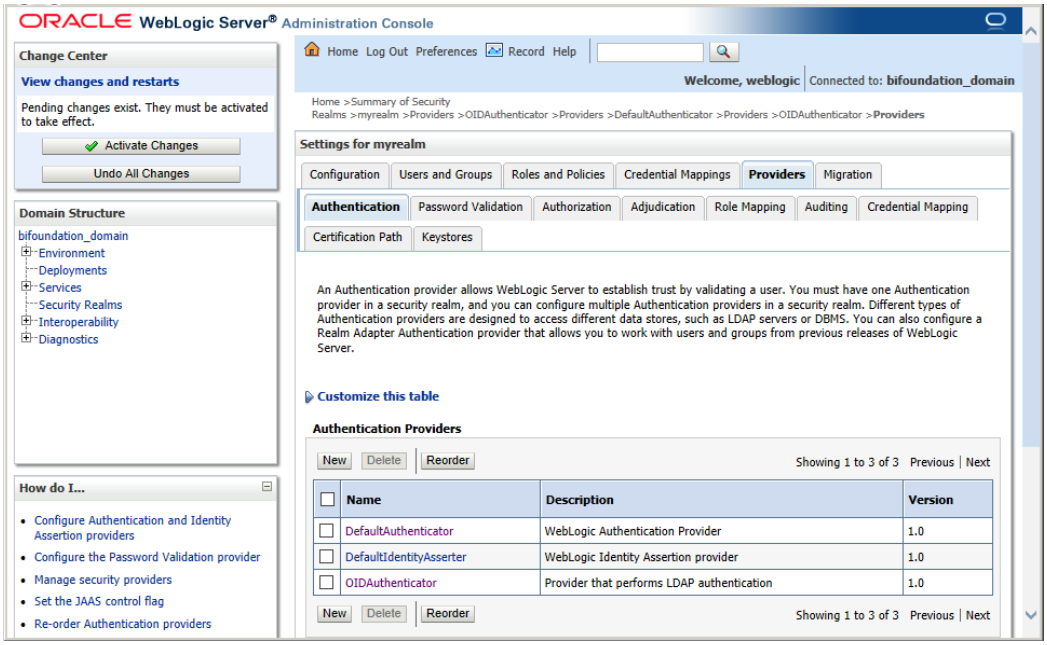



System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (3)
Users
User Base DN:
cn=users,dc=us,dc=orac
The base distinguished name (DN) of the tree in the LDAP directory that contains users. More Info...
All Users Filter:
(&(cn=*)(objectclass=per
An LDAP search filter for finding all users beneath the base user distinguished name (DN). Note: If you change the user name attribute to a type other than cn, you must duplicate that change in the User From Name Filter and User Name Attribute attributes. More Info...
User From Name Filter:
(&(cn=%u)(objectclass=p
An LDAP search filter for finding a user given the name of the user. The user name attribute specified in this filter must match the one specified in the All Users Filter and User Name Attribute attributes. More Info...
User Search Scope:
subtree
Specifies how deep in the LDAP directory tree the LDAP Authentication provider should search for users. More Info...
User Name Attribute:
cn
The attribute of an LDAP user object class that specifies the name of the user. The user name attribute specified must match the one specified in the All Users Filter and User From Name Filter attributes. More Info...
User Object Class:
person
The LDAP object class that stores users. More Info...
Use Retrieved User Name as Principal
Specifies whether or not the user name retrieved from the LDAP server should be used as the Principal in the Subject. More Info...
Groups
Group Base DN:

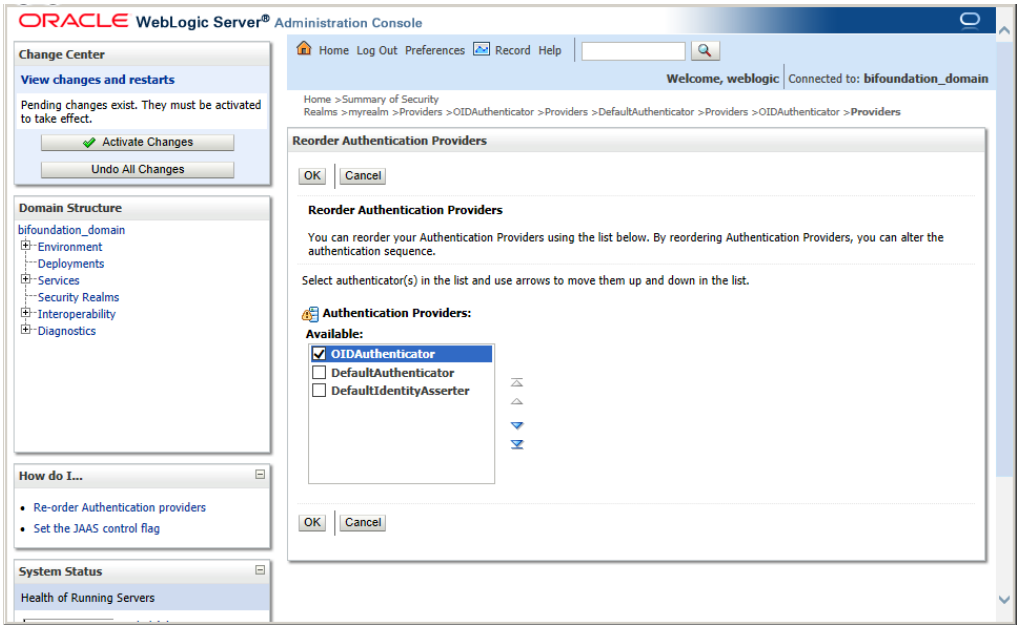

Groups
Group Base DN:
cn=Groups,dc=us,dc=ora
The base distinguished name (DN) of the tree in the LDAP directory that contains groups. More Info...
All Groups Filter:
(&(cn=*)(|(objectclass=gr
An LDAP search filter for finding all groups beneath the base group distinguished name (DN). The static group object class should be modified, as necessary, based on the settings for the Static Group Object Class and Static Member DN Attribute attributes. More Info...
Group From Name Filter:
(|(&(cn=%g)(objectclass=
An LDAP search filter for finding a group given the name of the group. The static group object class should be modified, as necessary, based on the settings for the Static Group Object Class and Static Member DN Attribute attributes. More Info...
Group Search Scope:
subtree
Specifies how deep in the LDAP directory tree to search for groups. Valid values are subtree and onelevel. More Info...
Group Membership Searching:
unlimited
Specifies whether group searches into nested groups are unlimited or limited. Valid values are unlimited and limited. More Info...
Max Group Membership Search Level:
0
Specifies how many levels of group membership can be searched. This setting is valid only if GroupMembershipSearching is set to limited. Valid values are 0 and positive integers. For example, 0 indicates only direct group memberships will be found, and a positive number indicates the number of levels to search. More Info...
Ignore Duplicate Membership
Determines whether duplicate members are ignored when adding groups. The attribute cycles in the Group membership. More Info...
Static Groups



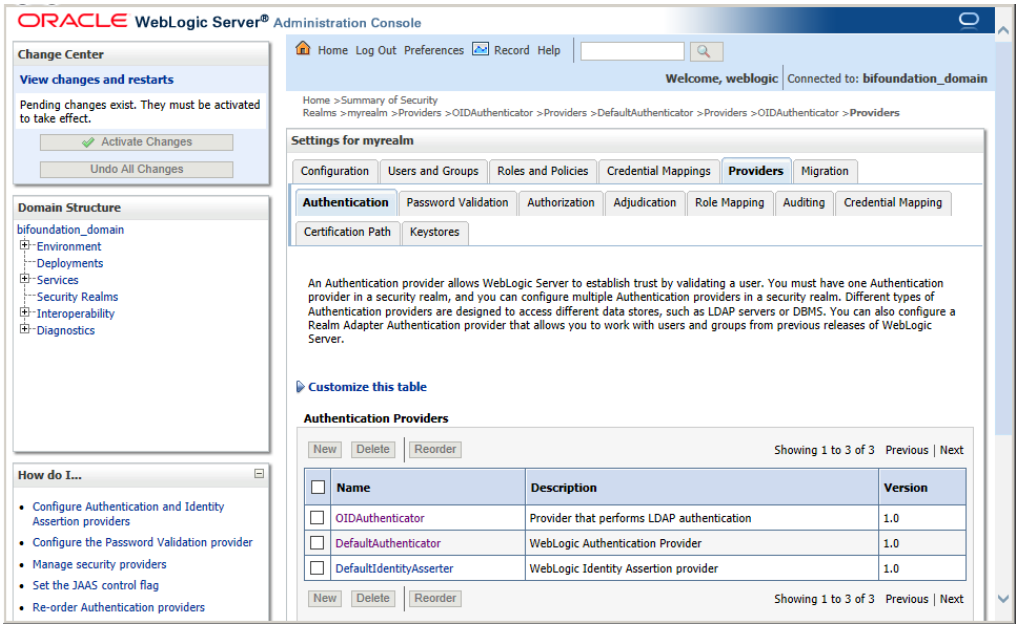
- Click **Reorder**.



- Move OIDAuthenticator to the top of the list and click **OK**.



- Click **Activate Changes**.

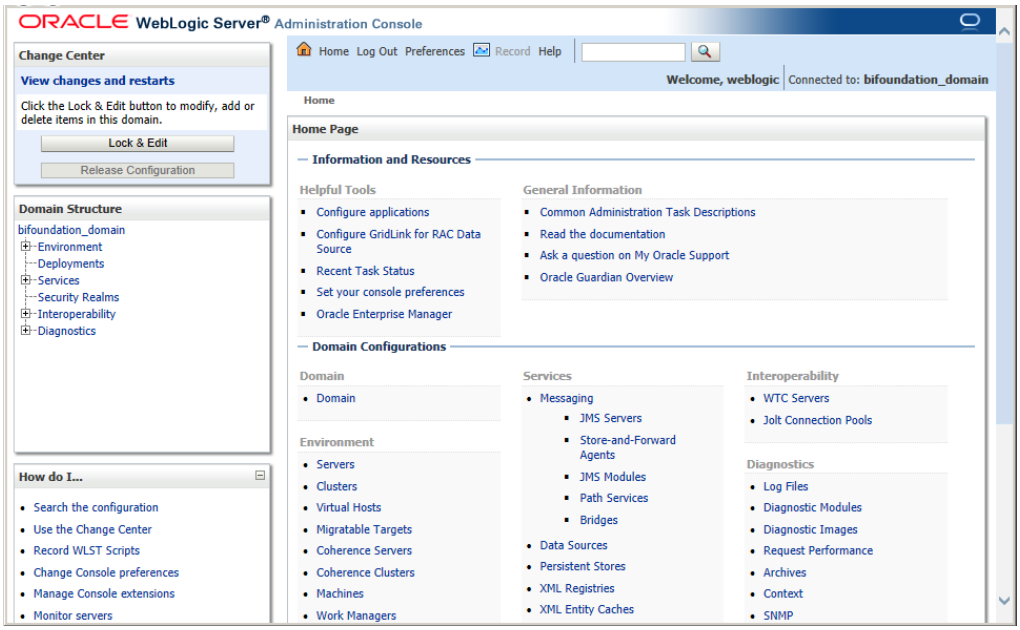


- Shutdown OBIEE admin and managed servers and then restart them.

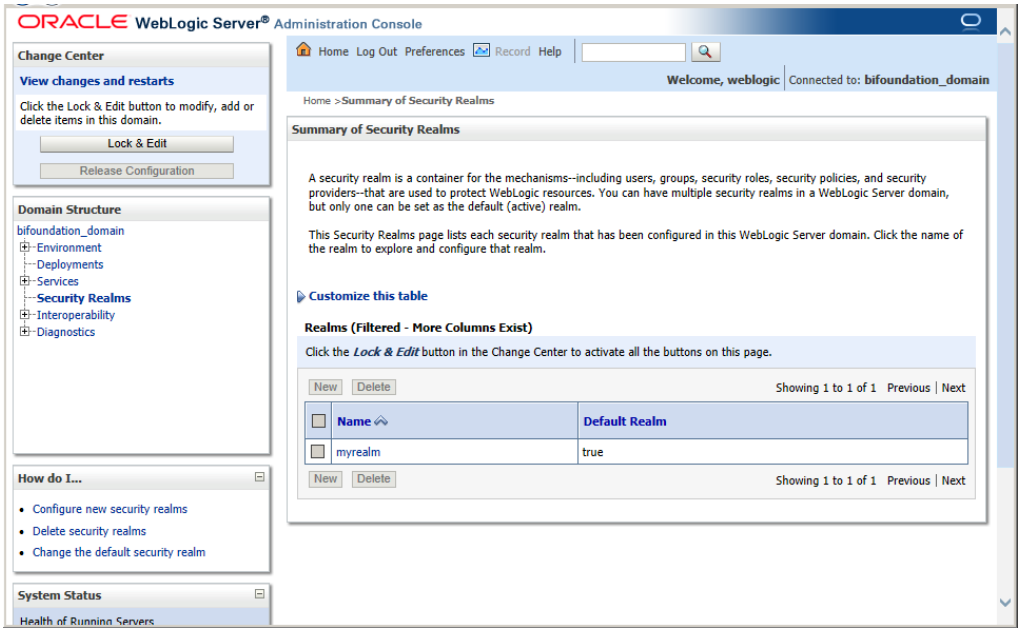
Create the OAM SSO provider in the Oracle BI EE Domain

1. Log into the WebLogic console.

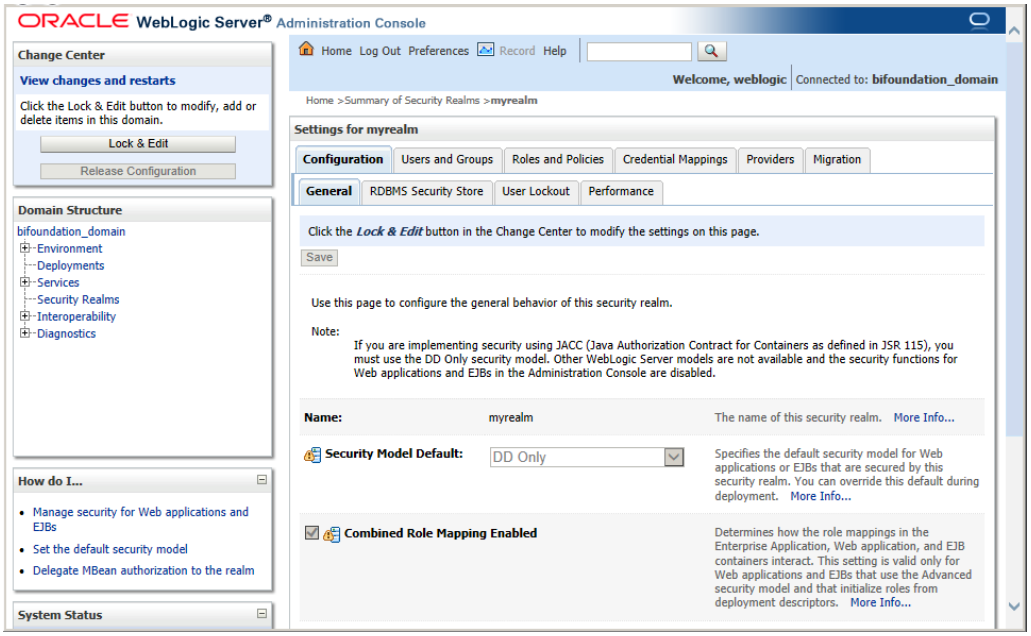
2. Click the **Security Realms** link located in the navigation pane on the left side of the screen.



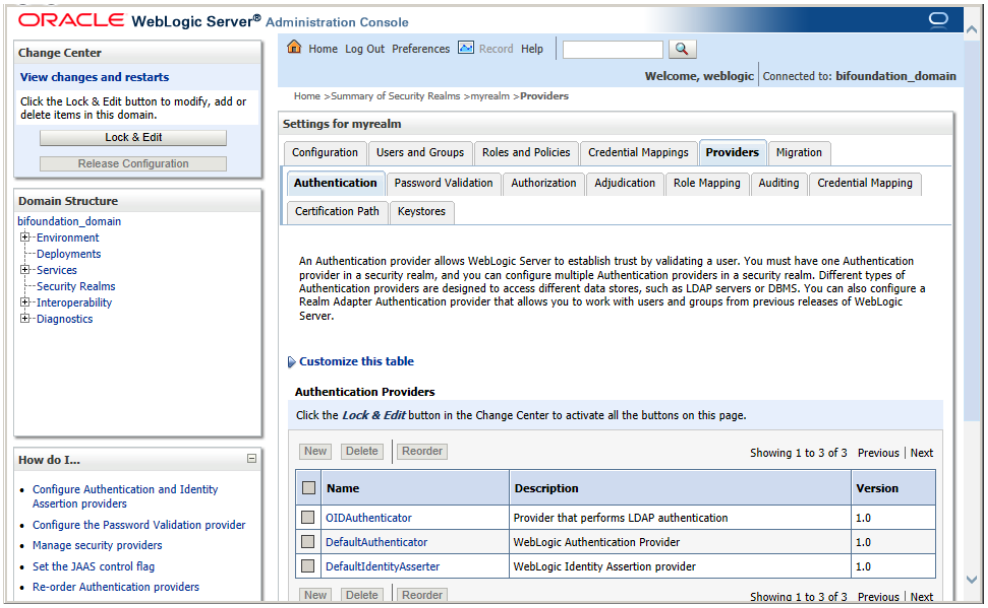
3. Click **myrealm** (default realm) link.



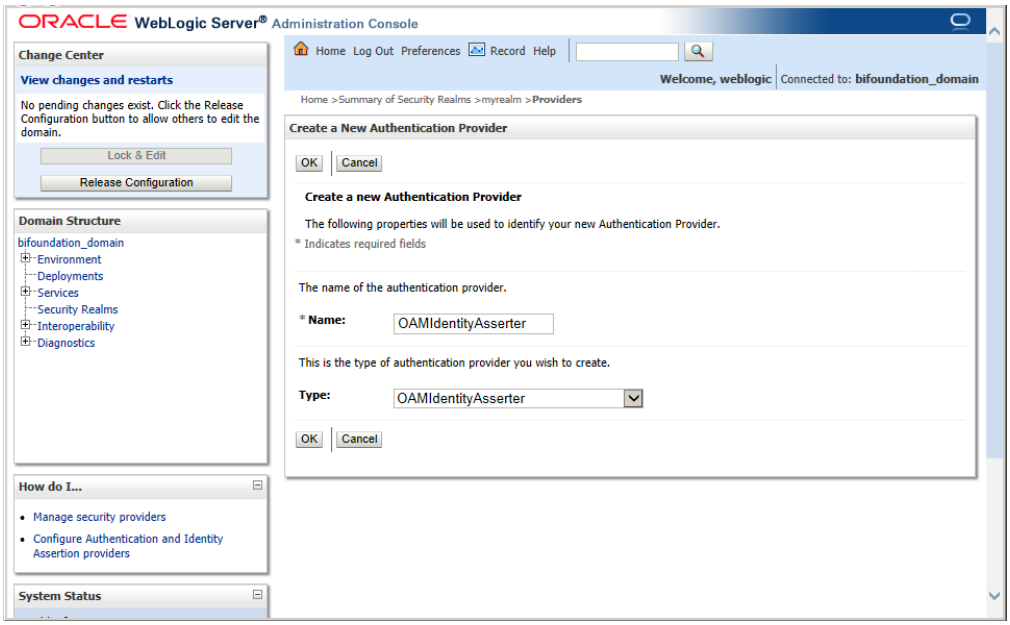
4. Click the **Providers** tab.



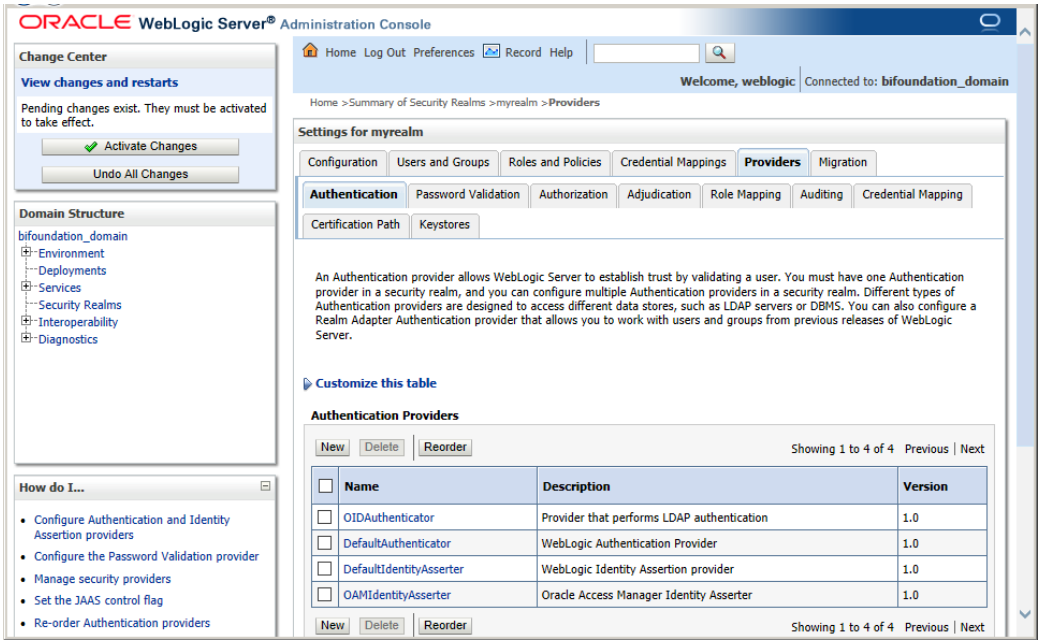
5. Click **Lock & Edit,** and then click **New**.



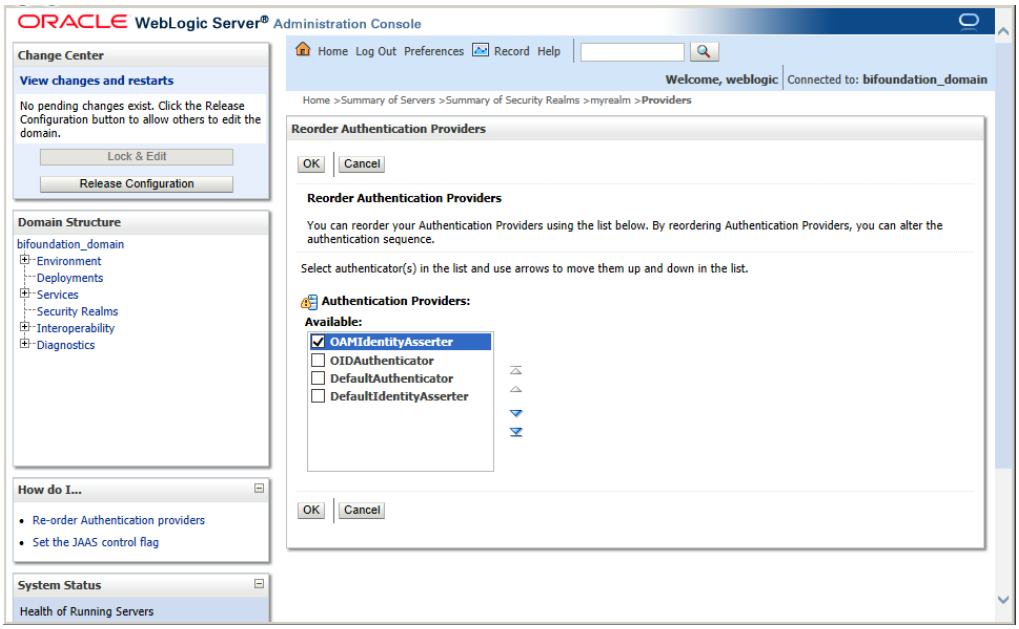
6. Make the following updates and click **OK**.
   a. Name: OAMIdentityAsserter
   b. Type: OAMIdentityAsserter



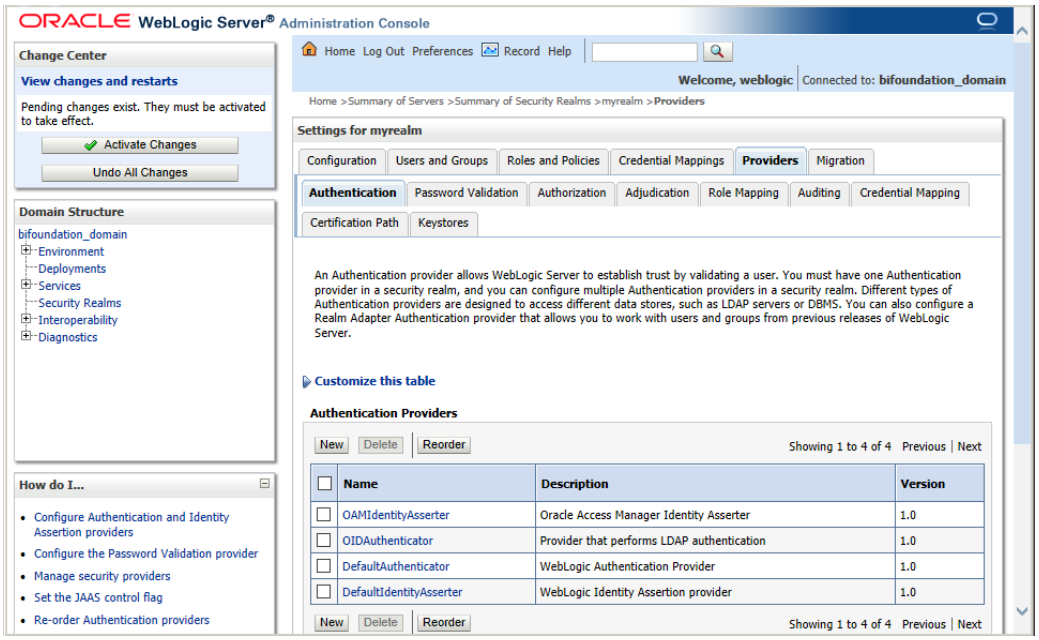
7. Click **Reorder**.



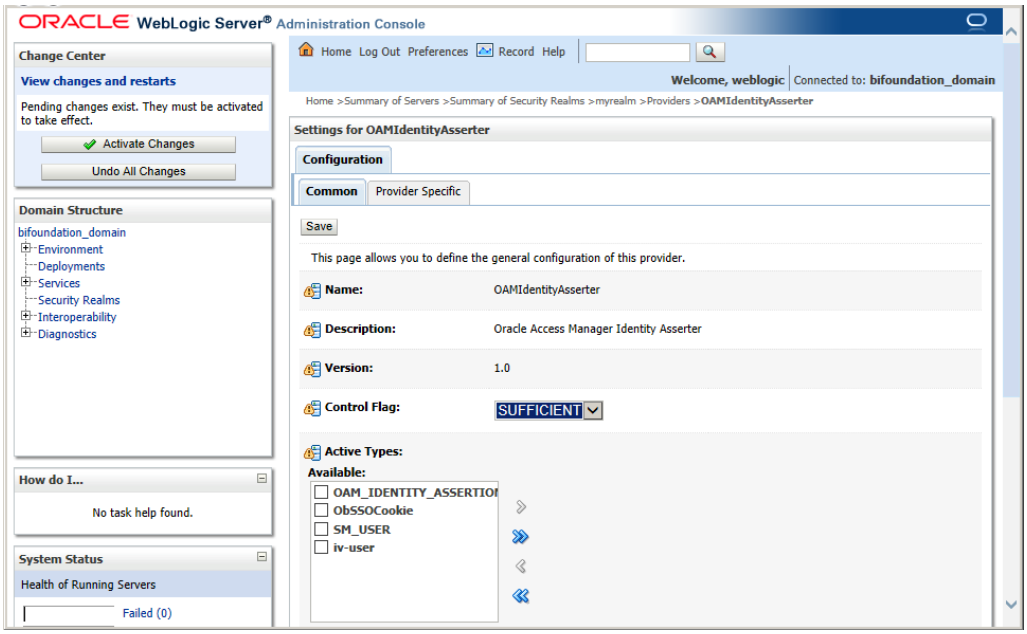
8. Move the OAMIdentityAsserter to the top of the list, or above the DefaultAuthenticator and click **Ok**.



9. Click the **OAMIdentityAsserter provider** link.



10. Set the Control Flag to SUFFICIENT and click **Save**.

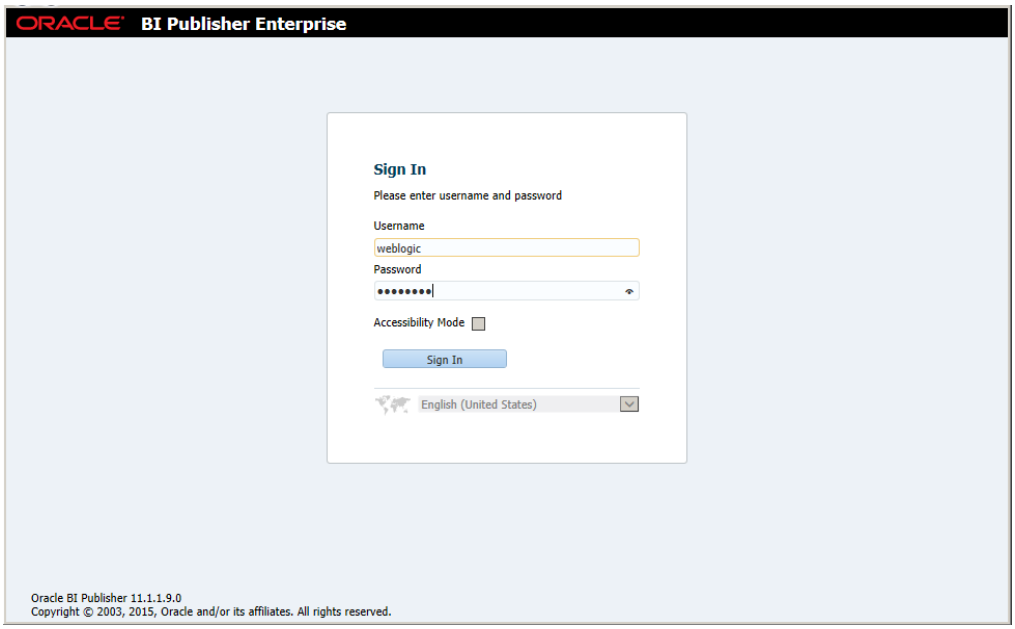


11. Click **Activate Changes**.
12. Shut down and restart the admin and managed servers.

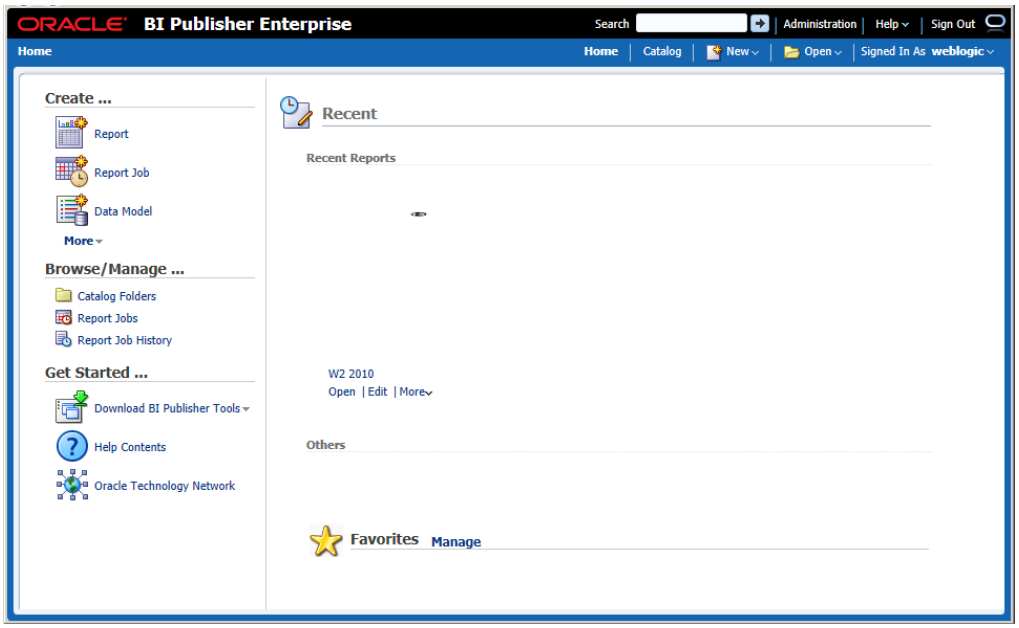
Configure BI Publisher for Application Reports

RMS, SIM, and REIM utilize BI Publisher reports - The following instructions are for setting up BI Publisher to properly interface with the applications and allow users to run the reports via BI Publisher application.

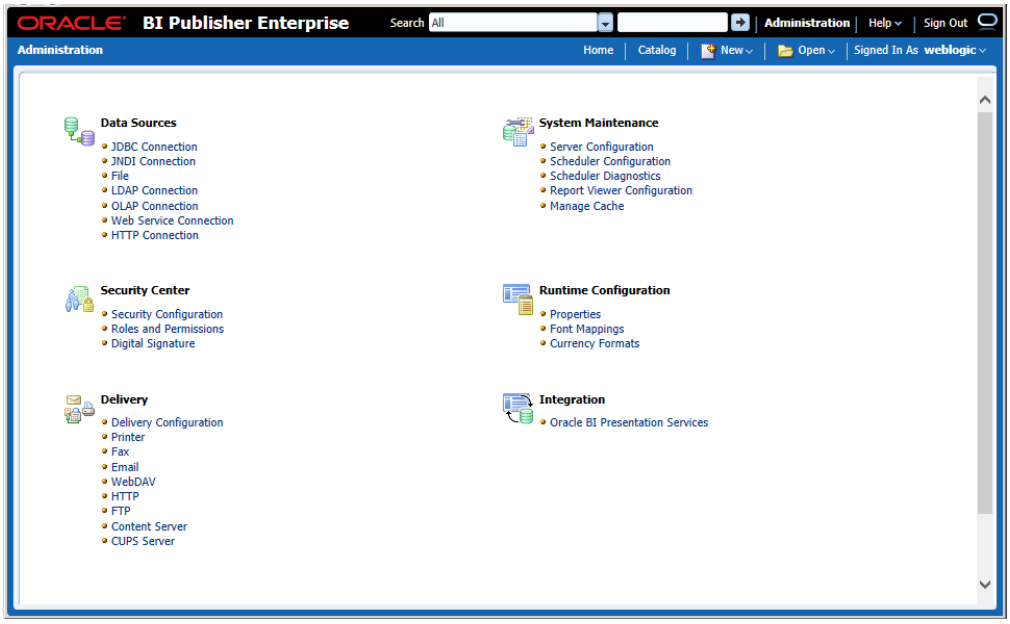
- Login to BI Publisher on idmhost1 with the credentials you entered in your Oracle BI EE configuration (weblogic / password). Example URL: http://idmhost1:7333xmlpserver



- The BI Publisher home window opens. Click the **Administration** link in the upper right corner.

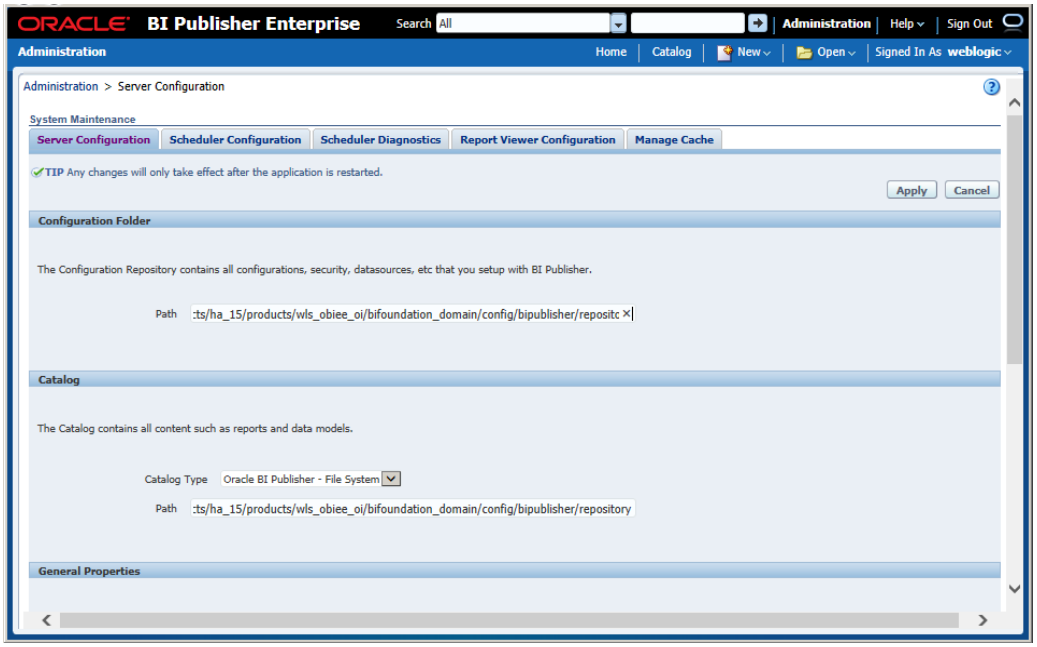


- From the Administration window, click **Server Configuration** from System Maintenance.



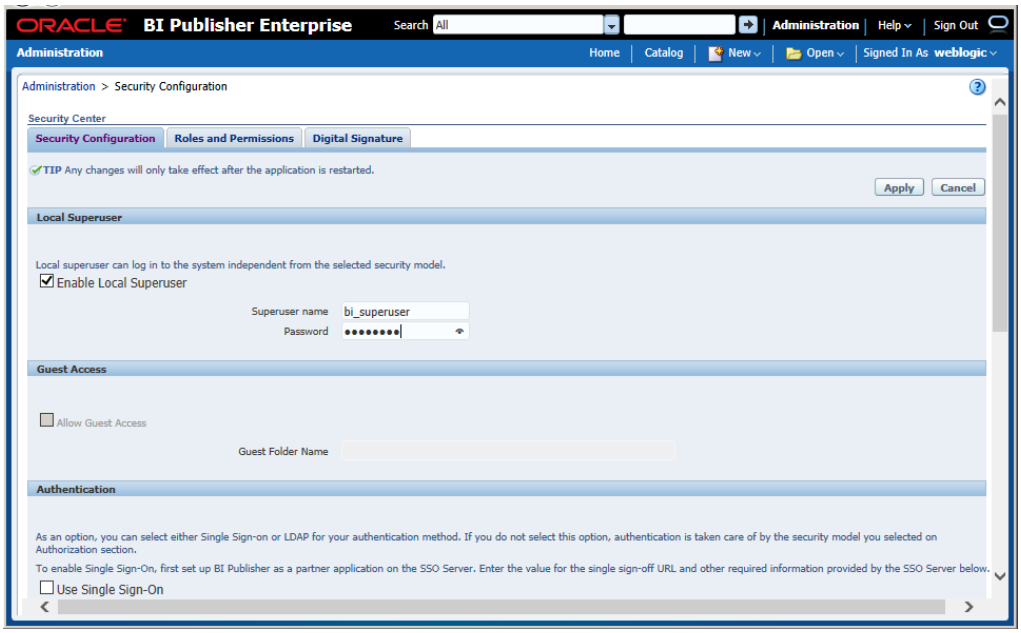
- In the Server Maintenance window, under the Server Configuration tab, make the following changes:
  - Configuration Folder - Path: /vol.rtk/projects/ha_15/products/wls_obiee_oi/bifoundation_domain_oi/config/bipublisher/

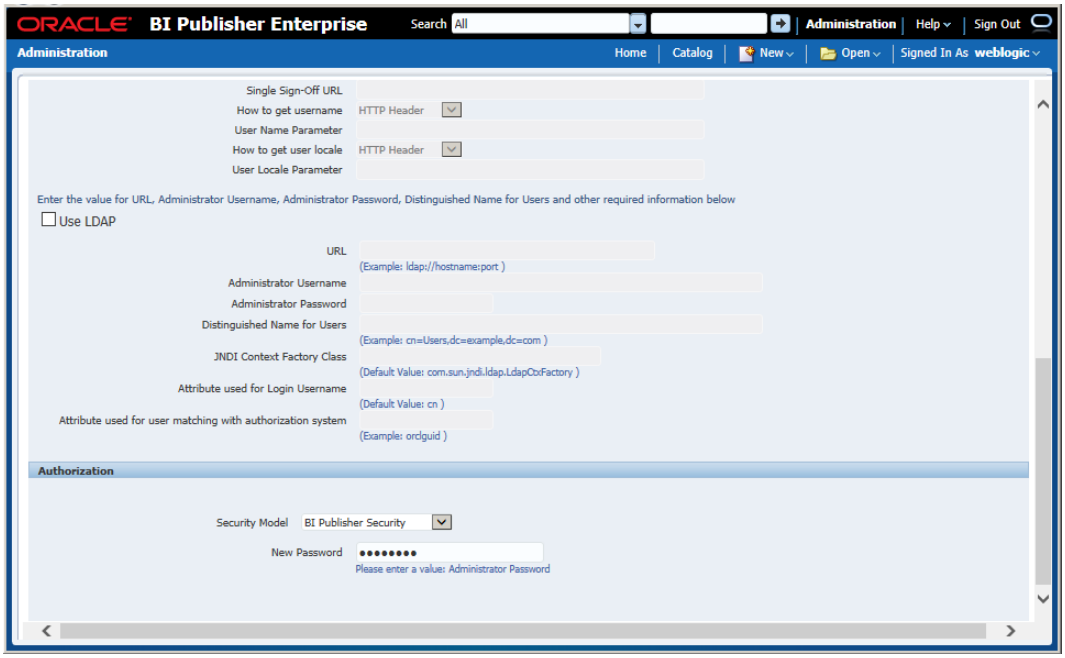
    NOTE: The Location has to be in a directory that is shared by both idmhost1 and idmhost2 and be suitable for storing BI Publisher reports files.
  - Catalog - Catalog Type: Oracle BI Publisher – File System
  - Catalog - Path: /vol.rtk/projects/ha_15/products/wls_obiee_oi/bifoundation_domain_oi/config/bipublisher/
  - Click **Apply** button and then click the Administration link in upper right hand corner.



- From the Administration window, under Security Center, click the **Security Configuration** link.

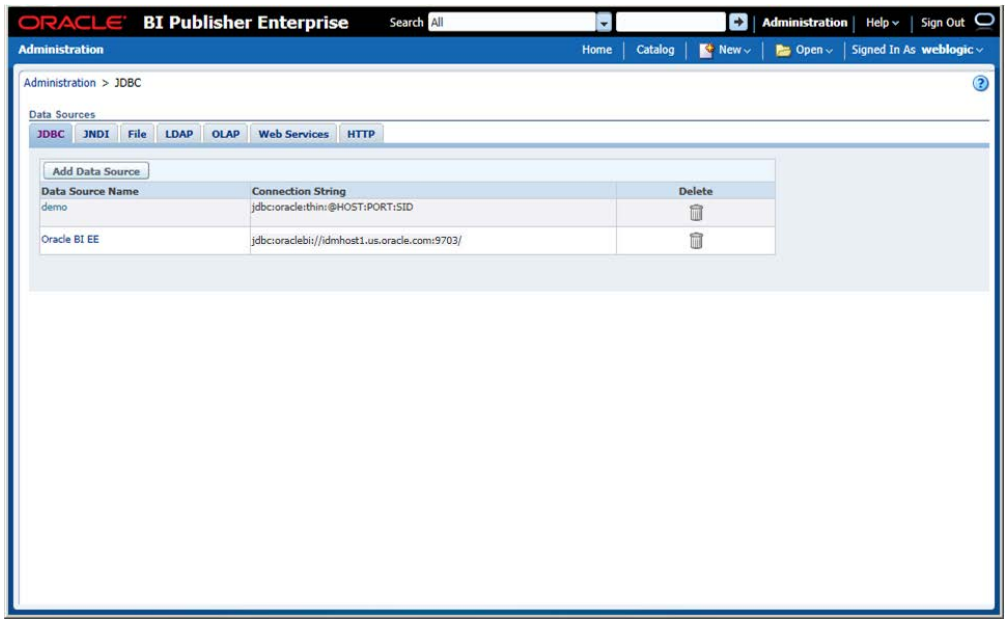
- In the Security Configuration window, make the following changes:
  - Select Enable Local Superuser
  - Superuser name: bi_superuser
  - Password: <password>
  - (Scroll to bottom of screen)
  - Security Model: BI Publisher Security
  - New Password: <password>
  - Click **Apply** and then click the Administration link in upper right hand corner.





- From the Administration window, under Data Sources, click the **JDBC Connection** link.

- Click **Add Data Source**.



- In the Add Data Source window, make the following updates:
  - Data Source Name: RMS

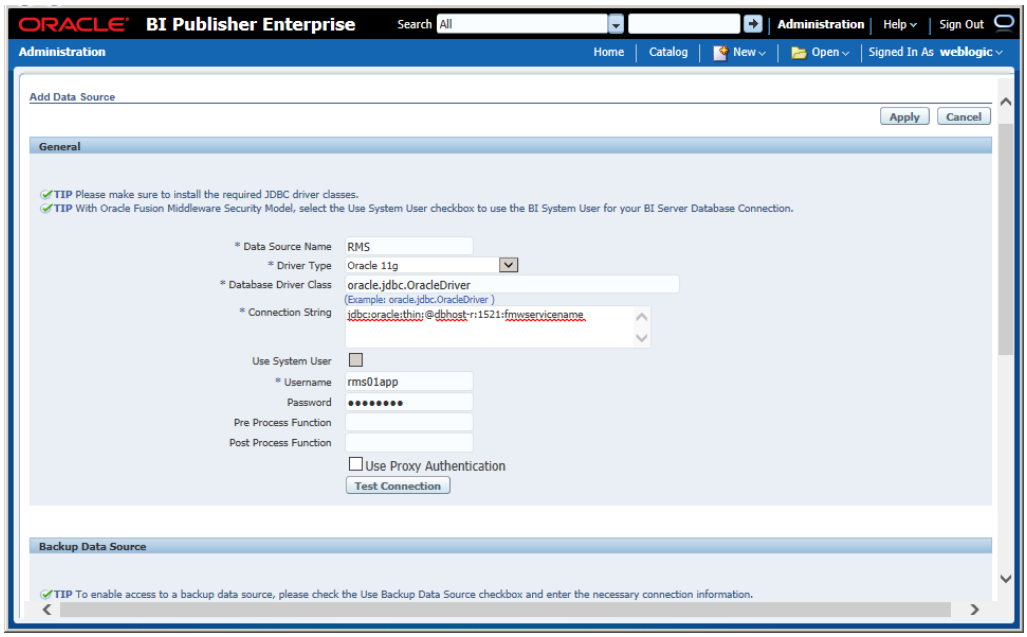
    NOTE: Has to be RMS due to reports dependencies

  - Driver Type: Oracle 11g
  - Database Driver Class: oracle.jdbc.OracleDriver
  - Connection String: jdbc:oracle:thin:@dbhost-r:1521/appservicename
  - Username: rms01app

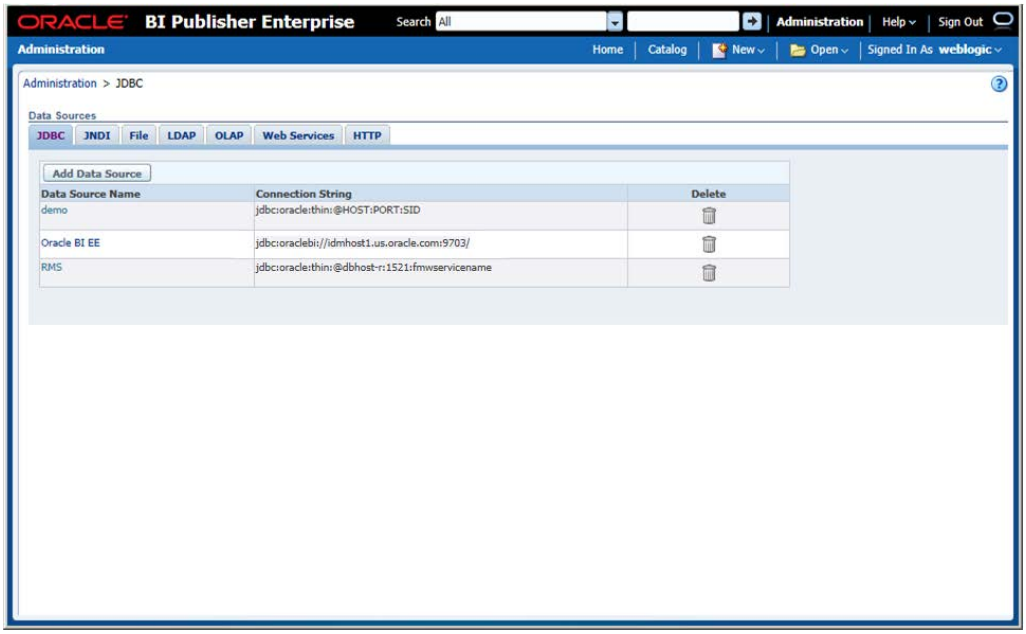
    NOTE: schema used for RMS application

  - Password: <password>
  - Scroll to the bottom of the screen.

- Select Allow Guest Access
- Click Apply.



- Click **Add Data Source**.



- In the Add Data Source window, make the following updates:
  - Data Source Name: BIP-SIM-DATASOURCE

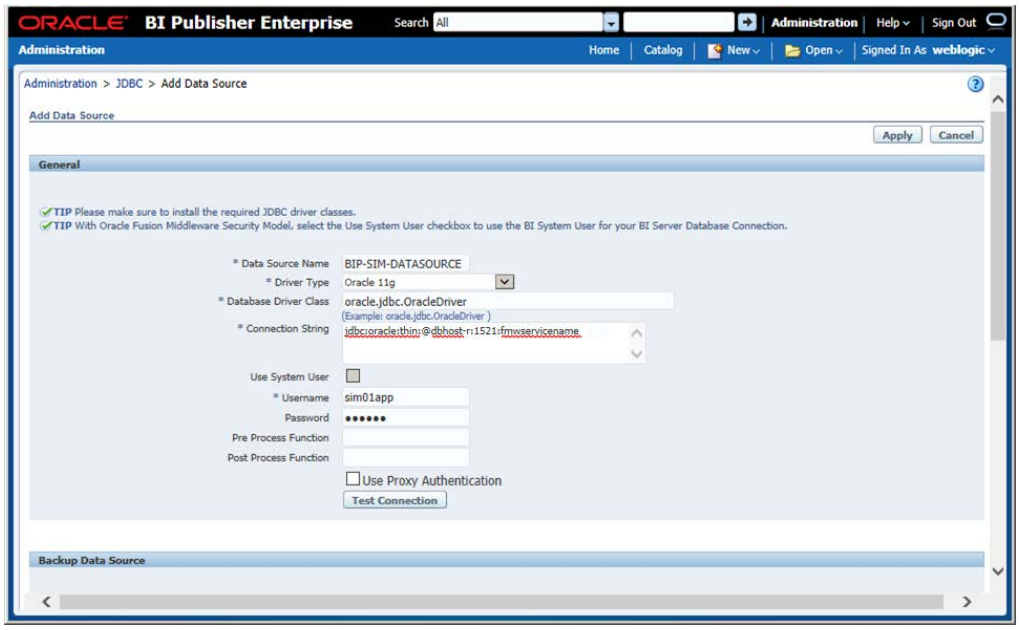
    NOTE: Has to be BIP-SIM-DATASOURCE due to reports dependencies

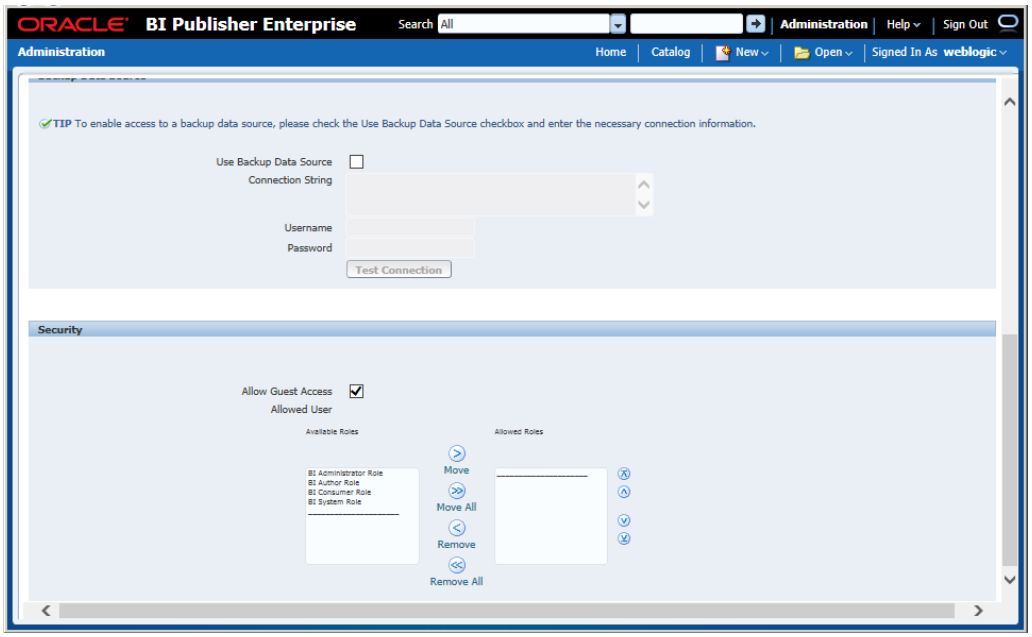
  - Driver Type: Oracle 11g
  - Database Driver Class: oracle.jdbc.OracleDriver
  - Connection String: jdbc:oracle:thin:@dbhost-r:1521/appservicename

– Username: sim01app

NOTE: schema used for SIM application

– Password: <password>
– Scroll to the bottom of the screen.
– Select Allow Guest Access
– Click **Apply**.





- Using the WebLogic admin console, shutdown BI Publisher admin and managed servers, so that reports can be migrated before final configuration.

Access the RMS, SIM, and REIM application installation distributions and migrate the reports using the following instructions:

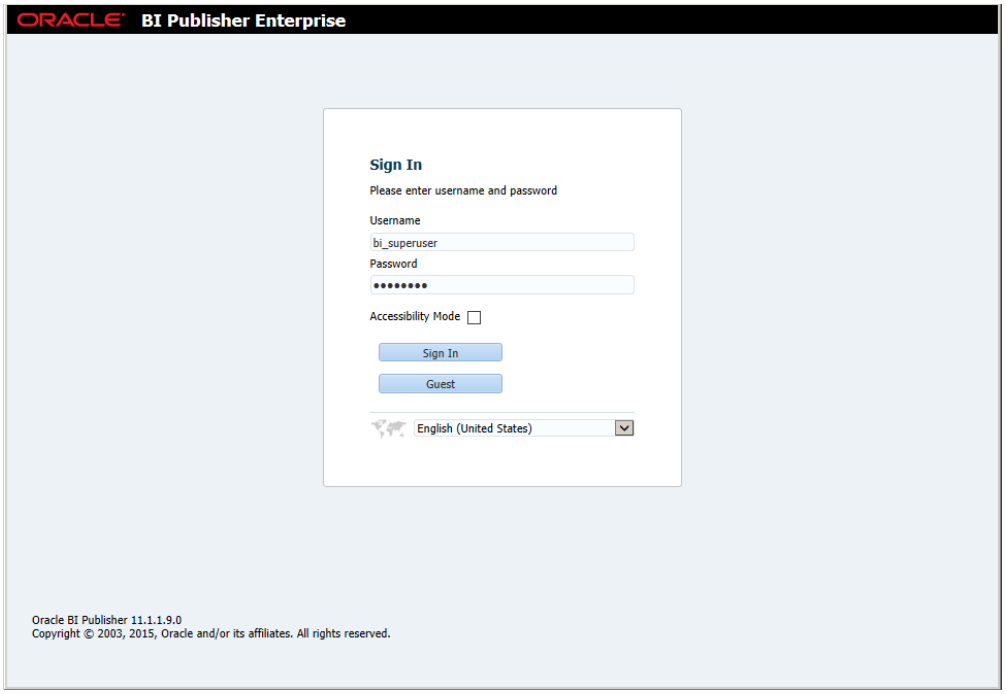
- Create the reports directories for the applications for Guest access under the Configuration Folder – Path (/vol.rtk/projects/ha_15/products/wls_obiee_oi/bifoundation_domain_oi/config/bipublisher/repository)

  Example:
  ```
  $ mkdir -p
  /vol.rtk/projects/ha_15/products/wls_obiee_oi/bifoundation_domain_oi/confi
  g/bipublisher/repository/Reports/Guest/RMS
  $ mkdir -p
  /vol.rtk/projects/ha_15/products/wls_obiee_oi/bifoundation_domain_oi/confi
  g/bipublisher/repository/Reports/Guest/REIM
  $ mkdir -p
  /vol.rtk/projects/ha_15/products/wls_obiee_oi/bifoundation_domain_oi/confi
  g/bipublisher/repository/Reports/Guest/SIM
  ```
- Gather reports from application installation distributions. Since installing obiee before applications they may or may not yet be not be loaded onto apphost1. Look for them in the following location whether on apphost1 or if application distribution is opened on desktop to retrieve reports.
  ```
  <rms_install_dir>/app/retail_home/reports/RMS
  <rms_install_dir>/sim/application/sim15/reports
  <rms_install_dir>/reim/application/reim/reports/11g/REIM
  ```
- Copy the reports into the Guest directory on host1 for each respective application
  ```
  /vol.rtk/projects/ha_15/products/wls_obiee_oi/bifoundation_domain_oi/confi
  g/bipublisher/repository/Reports/Guest/RMS

  /vol.rtk/projects/ha_15/products/wls_obiee_oi/bifoundation_domain_oi/confi
  g/bipublisher/repository/Reports/Guest/REIM

  /vol.rtk/projects/ha_15/products/wls_obiee_oi/bifoundation_domain_oi/confi
  g/bipublisher/repository/Reports/Guest/SIM
  ```
- For SIM the added step of unzipping the reports is required.

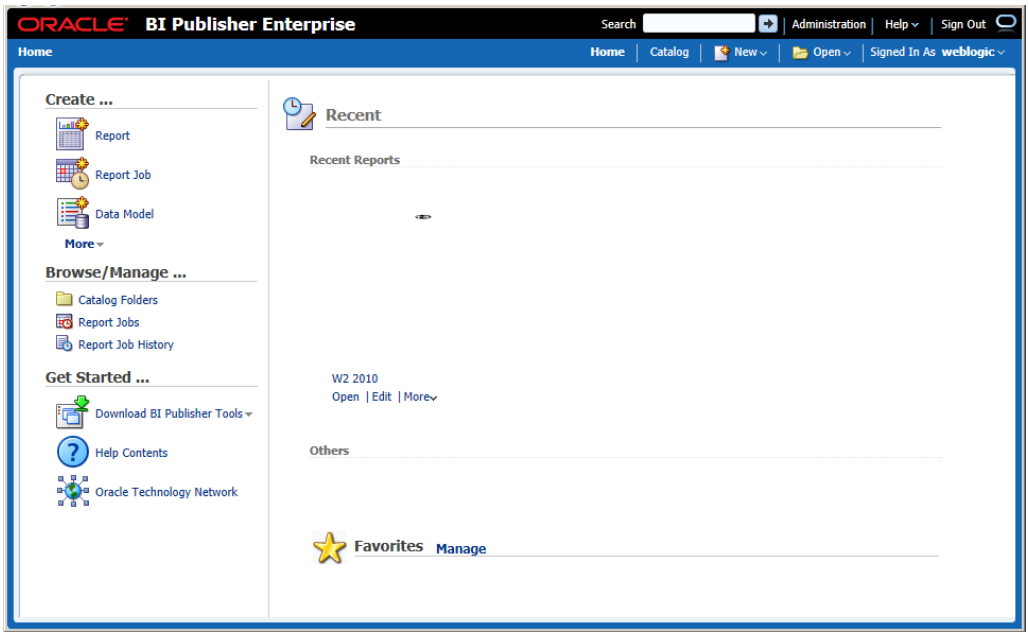
  Example:
  ```
  $ cd
  /u00/webadmin/config/domains/wls_obiee_oi/bifoundation_domain_oi/config/bi
  publisher/repository/Reports/Guest/SIM

  $ unzip *.zip
  ```

Restart BI Publisher admin and managed servers and then follow the instructions below to complete the configuration for BI Publisher reports.

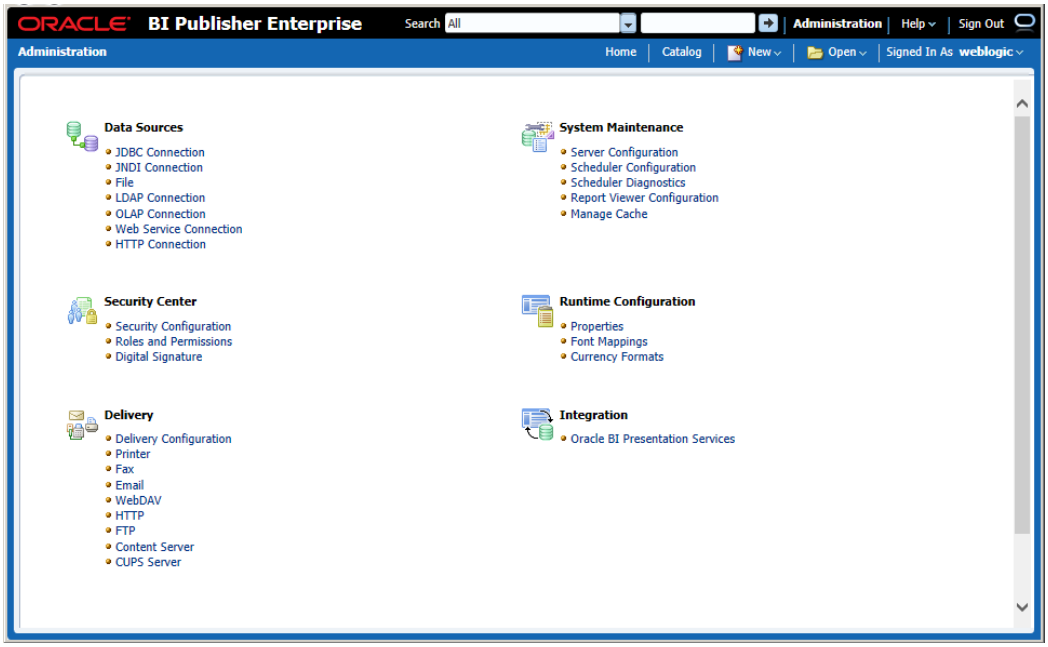
- Login to BI Publisher on idmhost1 with the credentials you created during the configuration for a Super user (bi_superuser/<password>). Example URL: http://idmhost1:7333/xmlpserver



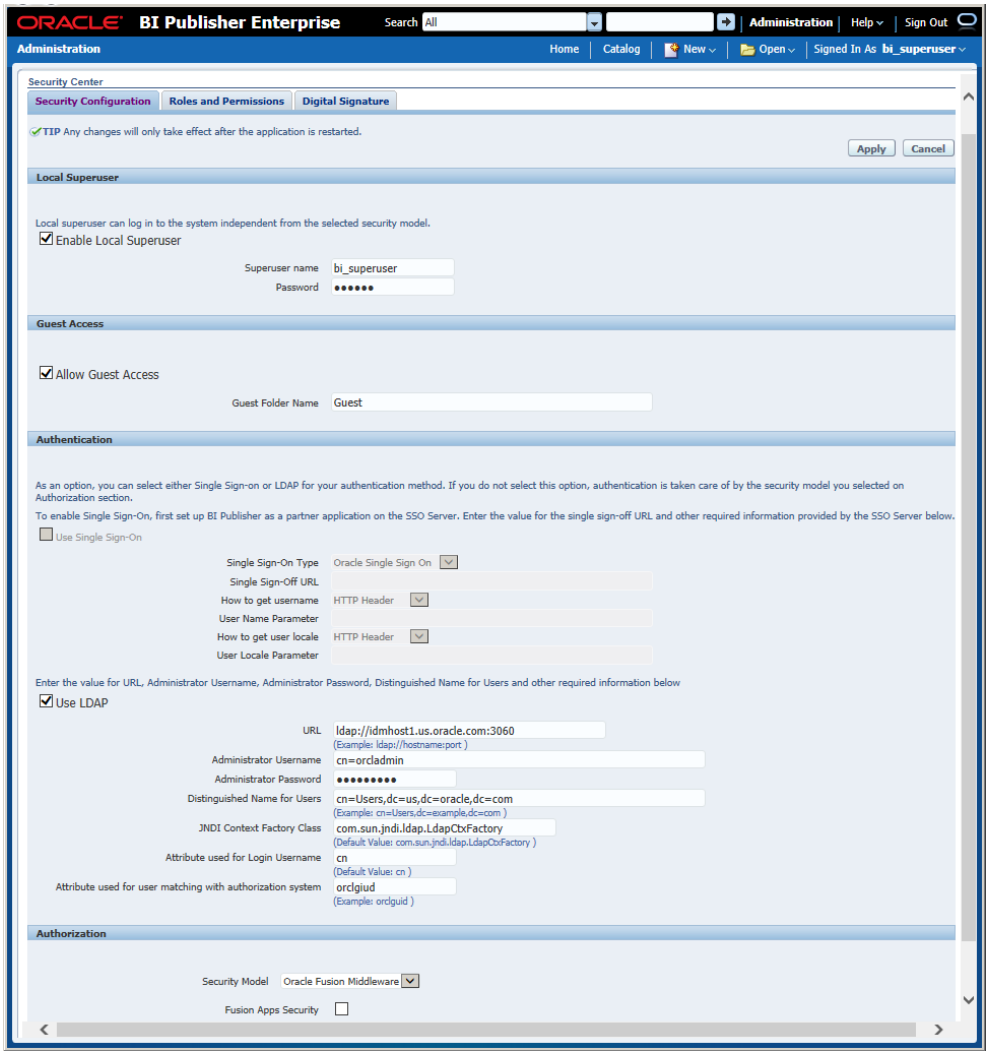
- The BI Publisher home window opens. Click the **Administration** link in the upper right corner.



- From the Administration Menu screen under Security Center, click the **Security Configuration** link.



- In the Security Configuration window, do the following:
  - Select Allow Guest Access
    - **a.** Guest Floder Name: Guest
  - Select Use LDAP and update the section with the following values:
    - **a.** URL: ldap://idmhost1.us.oracle.com:30690
    - **b.** Adminstrator Username: cn=orcladmin
    - **c.** Distinguished Name for Users: cn=Users,dc=us,dc=oracle,dc=com
    - **d.** JINDI Conect Factory Class: com.sun.jindi,.LdapCtxFactory
    - **e.** Attribute used for Login Username: cn
    - **f.** Attribute used for user matching authorization system: orclguid
  - In the Authorization section at the bottom – select Oracle Fusion Middleware from drop down menu.
  - Click **Apply.**



- On the same screen:
  - Select **Use Single Sign-On** and update the section with the following values:

    NOTE: The values in the section for Use LDAP will be removed auomatically.

    a. Single sign-On Type: Oracel Access Manager

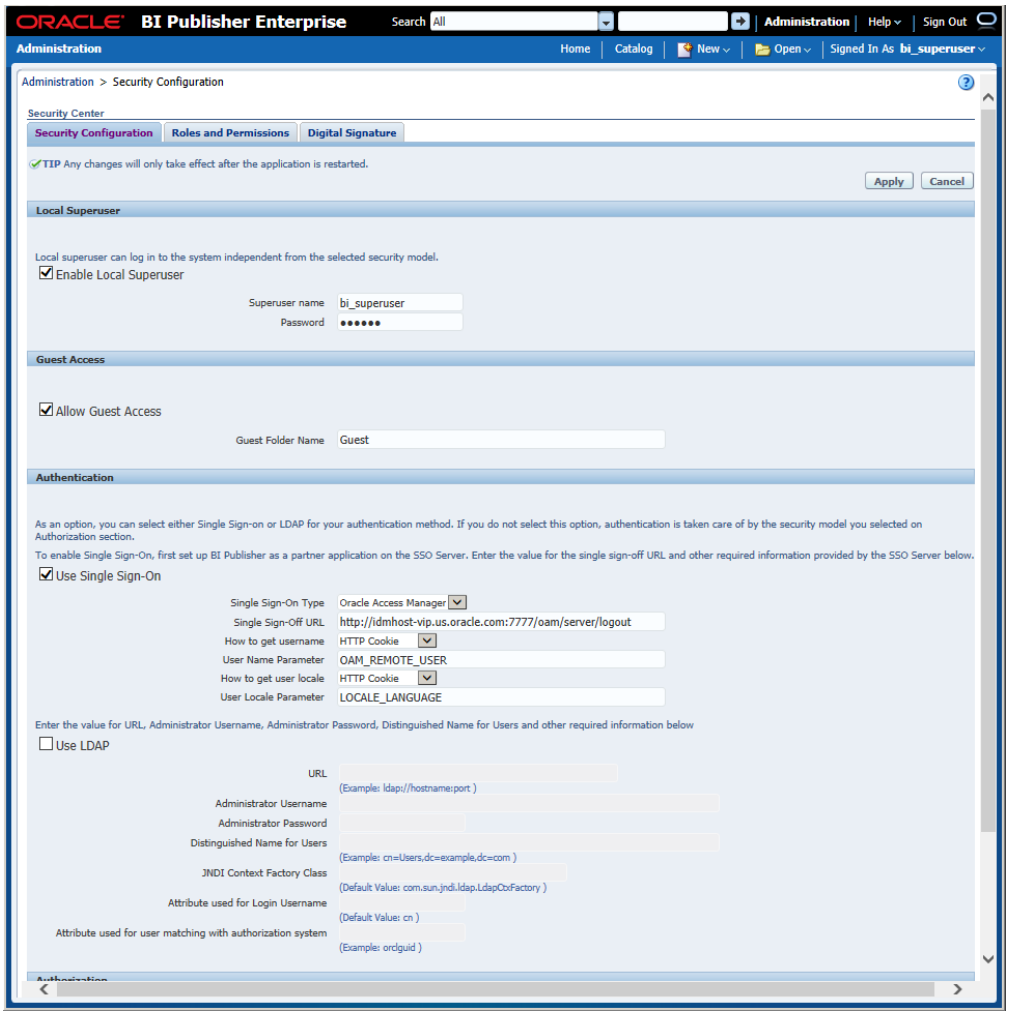
    b. Single Sign-Off URL: http://idmhost-vip.us.oracle.com:7777/oam/server/logout

    c. How to get username: HTTP Cookie

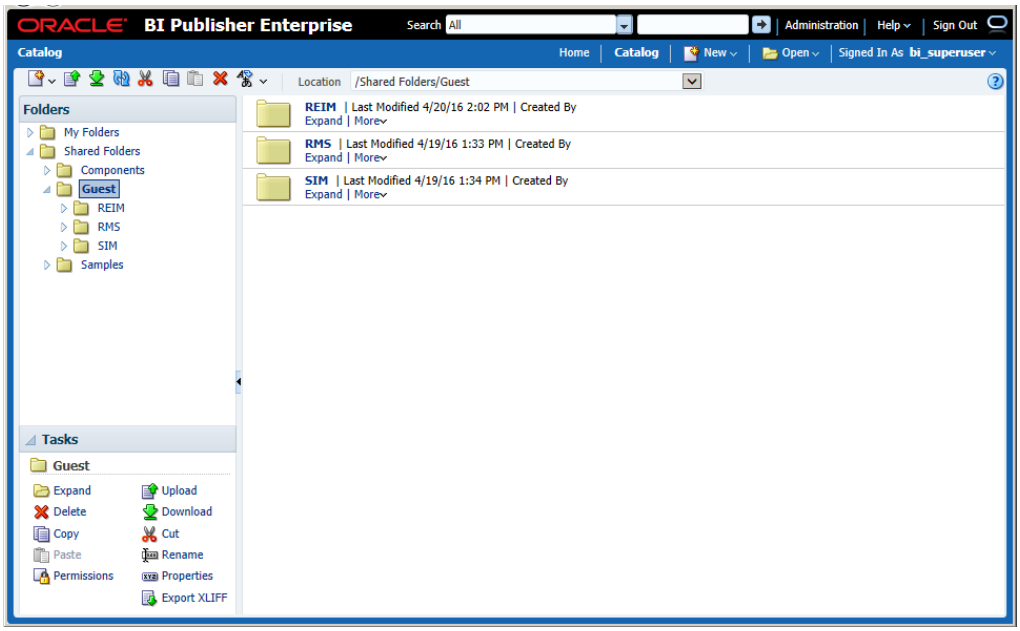
    d. User Name Parameter: OAM_REMOTE_USER

    e. How to get user locale: HTTP Cookie

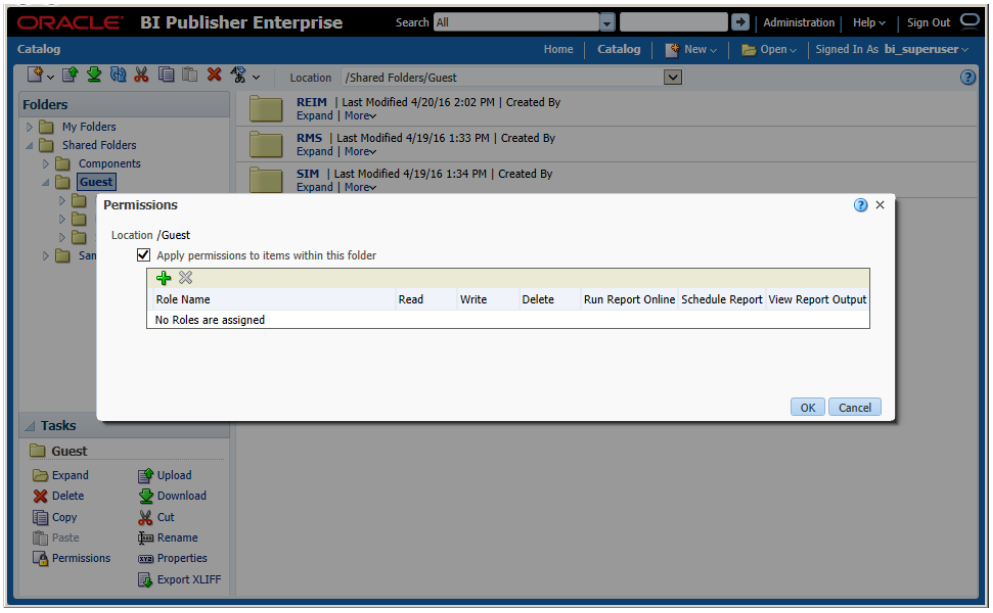
    f. User Locale Parameter: LOCALE_LANGUAGE
  - Click **Apply.**
  - Click the **Catalog** link from the top of the screen.



- Click the **Guest** folder on the left hand navigation pane. Then from the lower portion of the navigation pane, click **Permissions**.



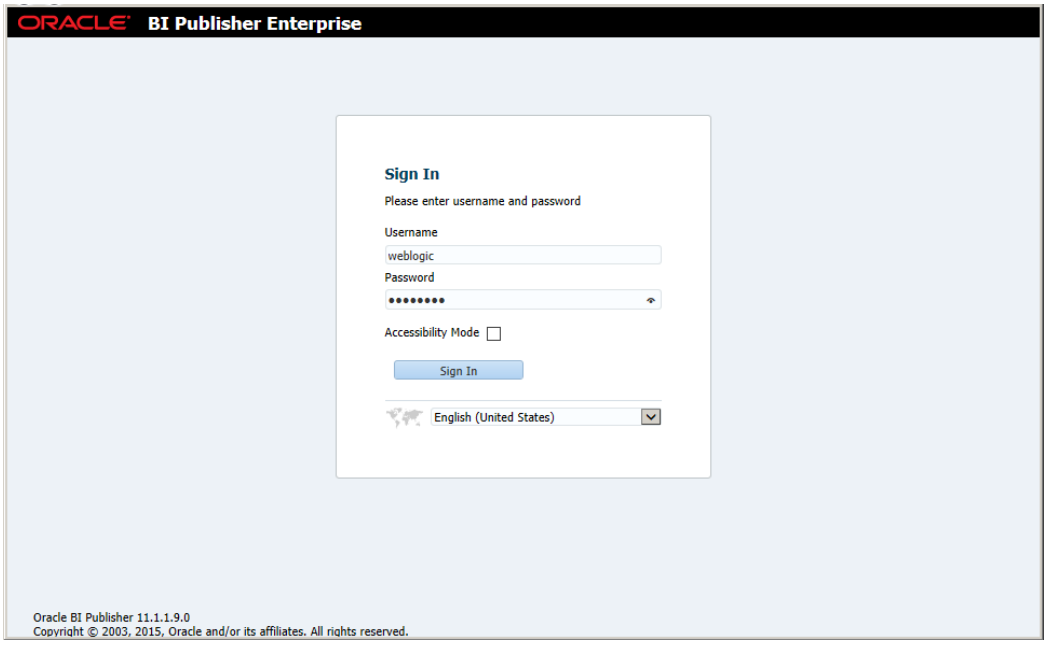
- Select **Apply permissions to items within this folder**, and click **OK**..



- Exit BI Publisher on idmhost1.

Logon to idmhost2 and configure it to use the same repositories as idmhost1.

- Login to BI Publisher on idmhost2 with the credentials you entered in your Oracle BI EE configuration (weblogic / password). Example URL: http://idmhost2:7333/xmlpserver



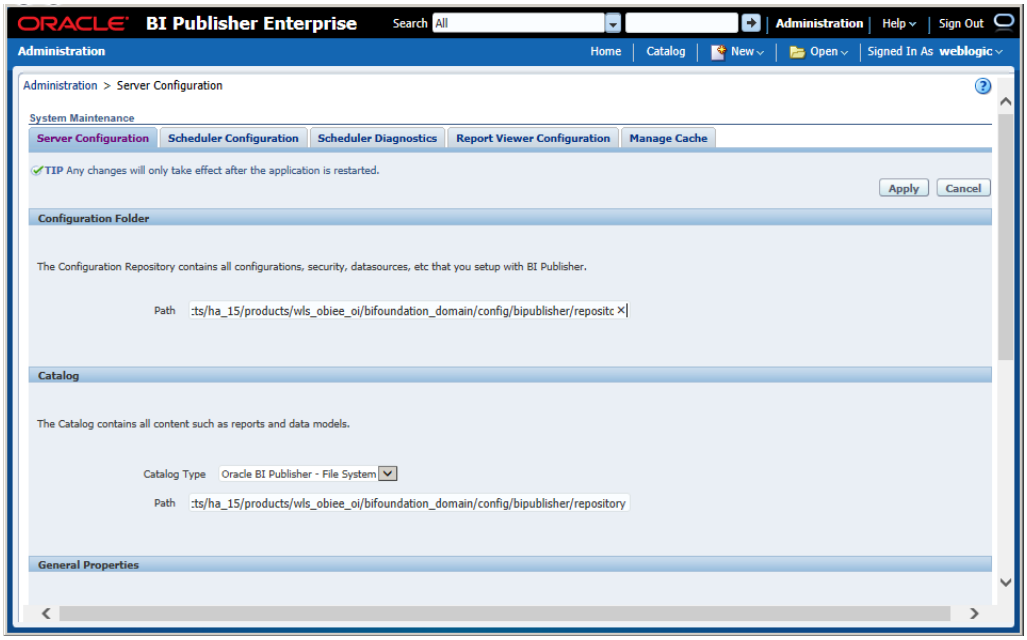
- From the Administration window, under System Maintenance, click the **Server Configuration** link.

- On the Server Maintenance screen – under the Server configuration tab make the following updates:
  - Configuration Folder - Path: /vol.rtk/projects/ha_15/products/wls_obiee_oi/bifoundation_domain_oi/config/bipublisher/

    NOTE: The Location has to be in a directory that is shared by both idmhost1 and idmhost2 and be suitable for storing BI Publisher reports files.

  - Catalog - Catalog Type: Oracle BI Publisher – File System

- Catalog - Path: /vol.rtk/projects/ha_15/products/wls_obiee_oi/bifoundation_domain_oi/config/bipublisher/
- Click **Apply** button and then click the Administration link in upper right hand corner.



- Stop and restart OBIEE WebLogic admin and managed servers.
- This completes the configuration of BI Publisher for reports.

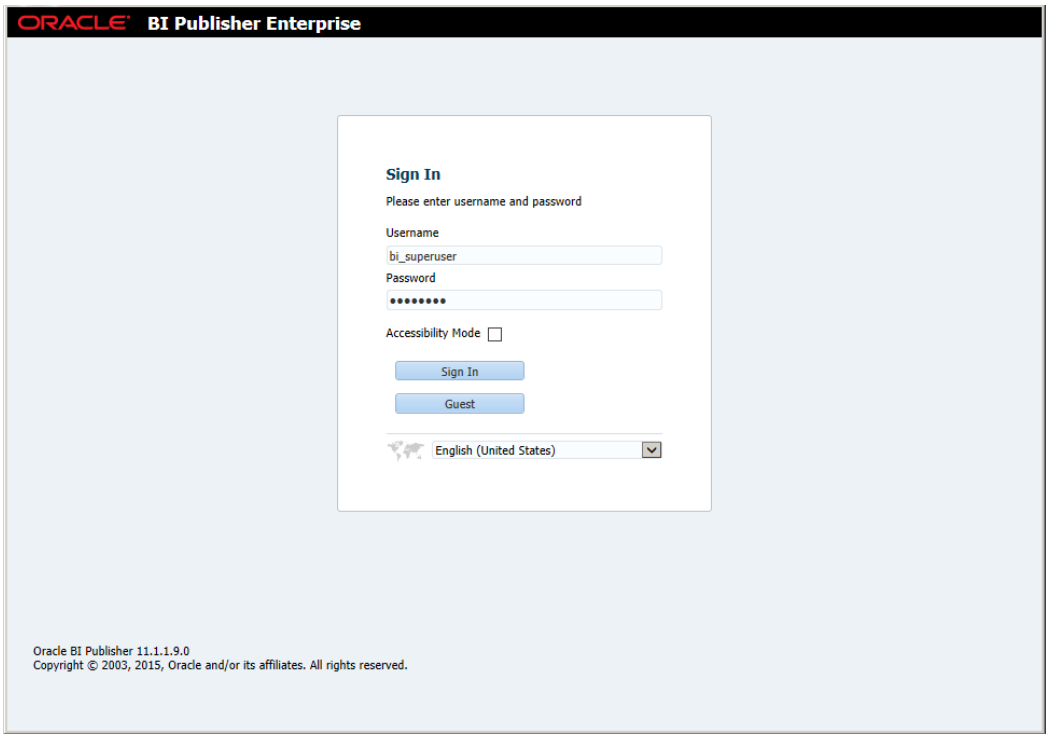
Verification – Validate BI Publisher Reports Non-SSO configuration

Perform the following steps to validate the migration and configuration of BI Publisher reports.

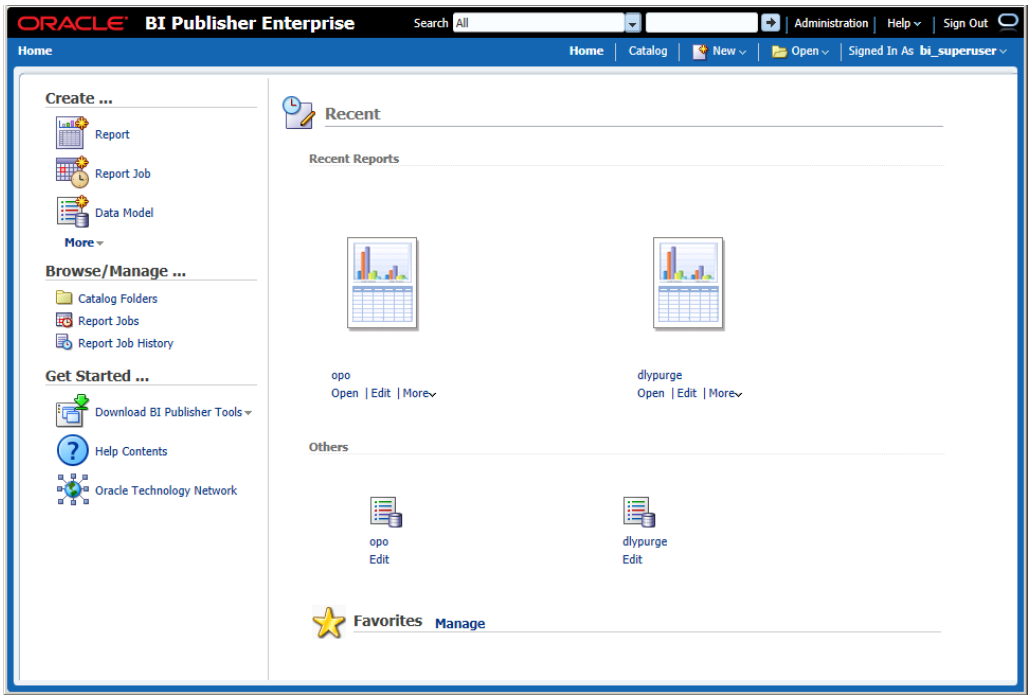
> **NOTE**: SSO and VIP configuration hasn't been completed yet for the reports. This test is to provide a check point in which reports can be validated to see if they are functioning prior to continuing on with the next steps of configuring analytics for Operational Insights and SSO configuration.

1. The following steps can be done on both idmhost1 and idmhost2. Screen shots below are from idmhost1.

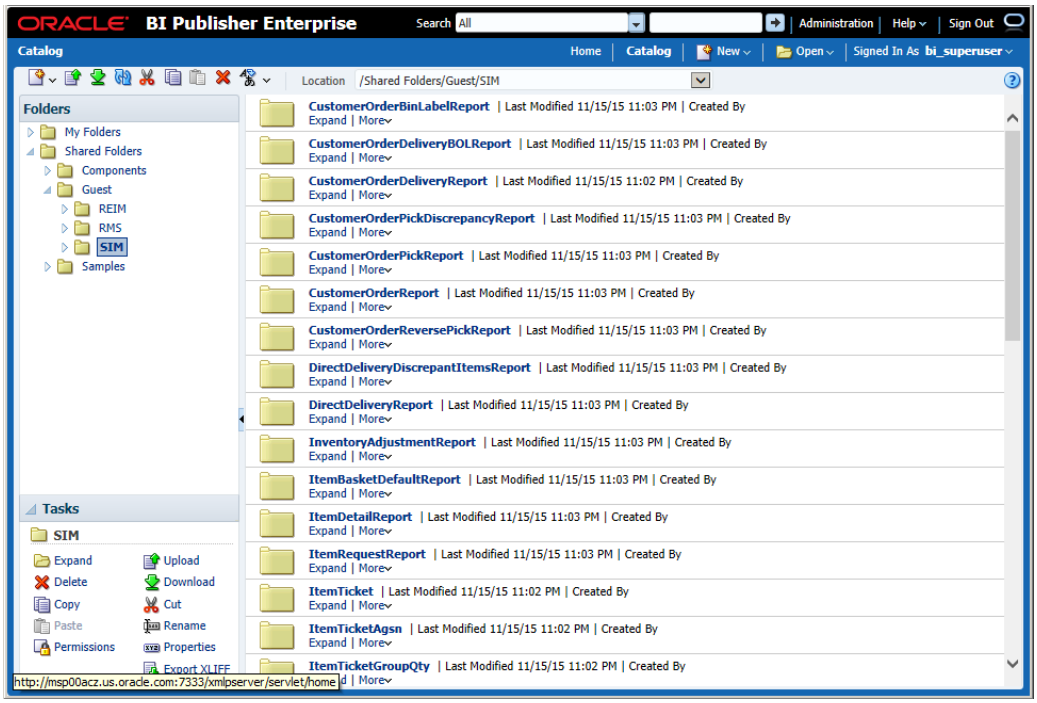
   Log into BI Publisher installed on idmhost with the BI Publisher Superuser. (http://msp00acz.us.oracle.com:7333/xmlpserver)



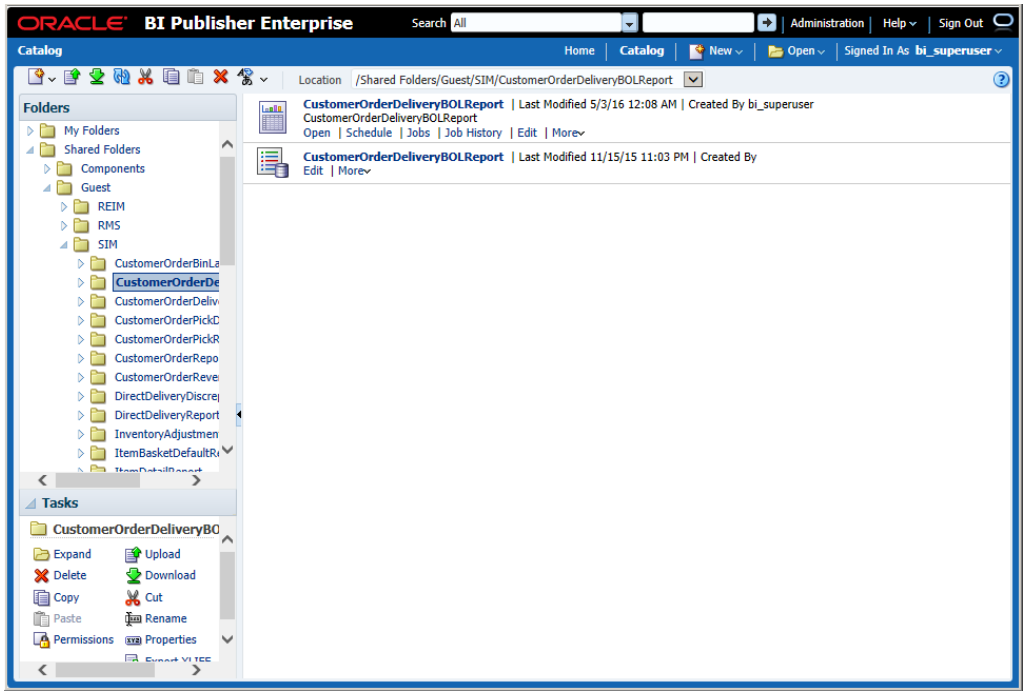
2. Click the **Catalog** link at the top of the screen.



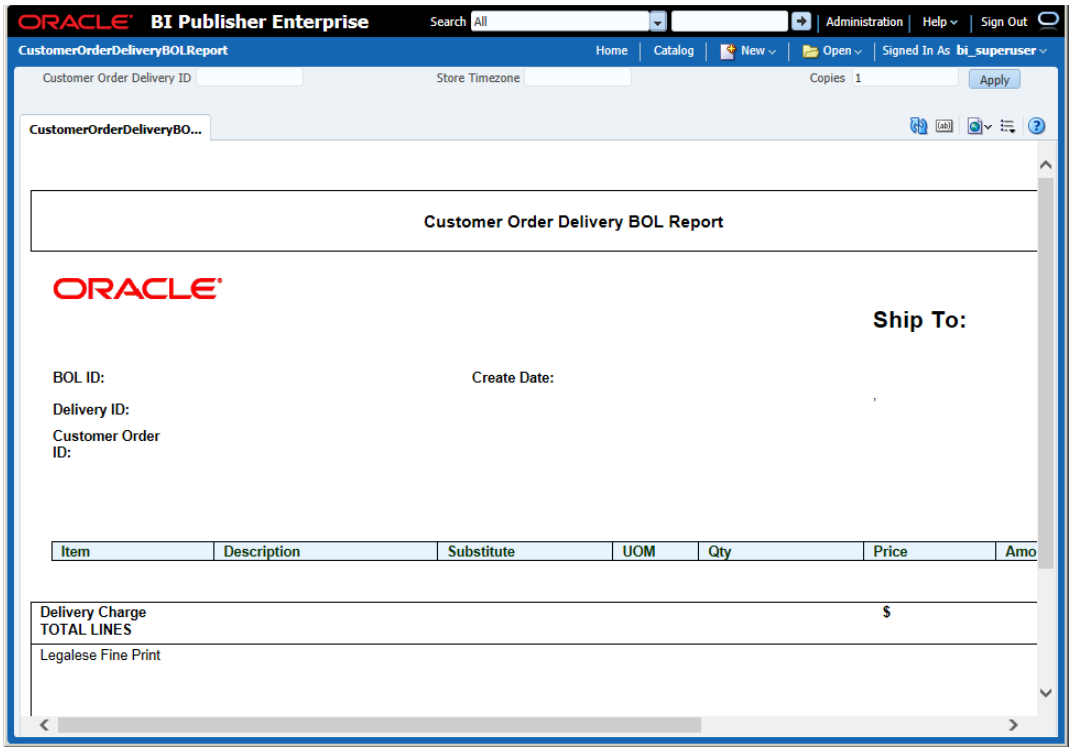
3. In the left hand navigation pane click **SIM** folder link.



4. Click the **CustomerOrderDeliveryBOLReport** link.



5. The Customer Order delivery BOL Report is displayed as shown below.


ORACLE BI Publisher Enterprise
Search All
Administration
Help
Sign Out
CustomerOrderDeliveryBOLReport
Home
Catalog
New
Open
Signed In As bi_superuser
Customer Order Delivery ID
Store Timezone
Copies 1
Apply
CustomerOrderDeliveryBO...
Customer Order Delivery BOL Report
ORACLE
Ship To:
BOL ID:
Create Date:
Delivery ID:
Customer Order ID:
Item
Description
Substitute
UOM
Qty
Price
Amo
Delivery Charge
TOTAL LINES
$
Legalese Fine Print

16

Configuring the Oracle BI EE Environment for Operational Insights

Configure Oracle Retail Operational Insights Roles and Application Roles

Perform the following procedure to configure pre-packaged security roles in Oracle Retail Operational Insights:

Shut down the OBIEE WLS server and opmn processes.

1. On idmhost1 and idmhost2 - Make a backup of system-jazn-data.xml from the following location: `<OBIEE_WEBLOGIC_DOMAIN_HOME>/config/fmwconfig/system-jazn-data.xml`

   Example:

   ```
   $ cd
   /u00/webadmin/config/domains/wls_obiee_oi/bifoundation_domain_oi/config/fm
   wconfig
   $ mv system-jazn-data.xml system-jazn-data.xml_original
   ```

2. From idmhost1 (For both idmhost1 and idmhost2) copy the pre-packaged Oracle Retail Operational Insights system-jazn-data.xml file from

   `<INSTALL DIR>/OperationalInsights/XML`

   Into

   `<OBIEE_WEBLOGIC_DOMAIN_HOME>/config/fmwconfig`

   Example:

   ```
   $ cd /u00/webadmin/media/install_dir/OperationalInsights/XML/
   $ cp system-jazn-data.xml
   /u00/webadmin/config/domains/wls_obiee_oi/bifoundation_domain_oi/config/fm
   wconfig

   $ scp system-jazn-data.xml
   webadmin@idmhost2:/u00/webadmin/config/domains/wls_obiee_oi/bifoundation_d
   omain_oi/config/fmwconfig
   ```

   > **NOTE**: For more information regarding Oracle Retail Operational Insights application roles and associated user groups of Oracle Retail MOM products, please refer to the below Oracle Retail Security Guides. The install guides for REIM – ReSA and Allocations have additional information in regards to merging roles and user groups as well.

3. Oracle Retail Merchandising Security Guide.
4. Part III Oracle Retail Sales Audit (ReSA).
5. Part IV Oracle Retail Invoice Matching (ReIM).
6. Part VI Oracle Retail Allocation.

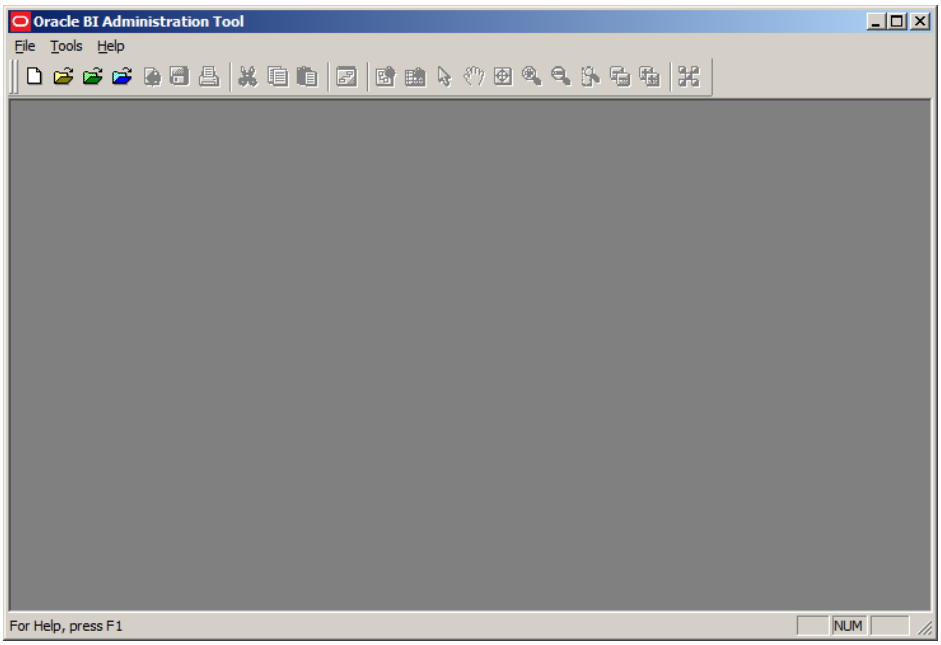
7. From idmhost1 - Navigate to NQSConfig.INI file and update FMW_UPDATE_ROLE_AND_USER_REF_GUIDS = YES. The NQSConfig.INI is located in the following shared mount directory :

   `/vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/config/OracleBIServerComponent/coreapplication_obis1`
8. Start WebLogic admin and managed servers.
9. Start all opmn processes.

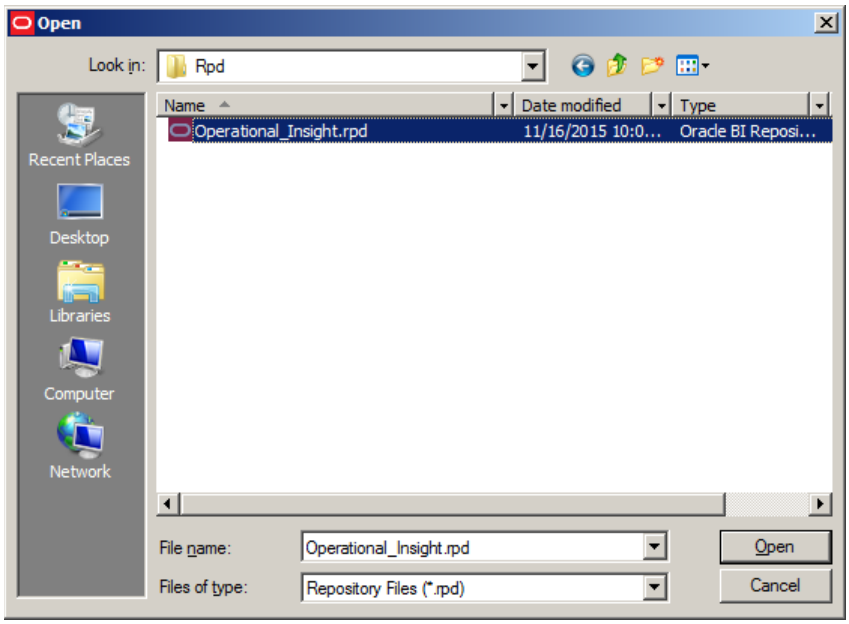
Configure RPD for Operational Insights

Refer to the "Configuring Repositories" chapter of the Oracle BI EE System Administrator's Guide for additional details.

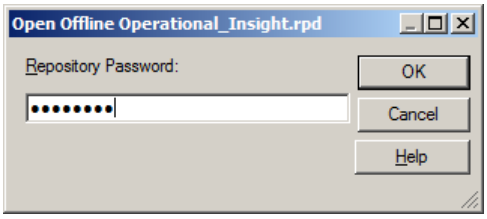
- This change requires the rpd OperationalInsights.rpd to be on a Microsoft Windows system which has Oracle Business Intelligence Enterprise Edition Plus Client installed. The file is located under <INSTALL DIR>/ OperationalInsights/Rpd
  - Copy the Rpd.zip to Windows system in a staging directory and unzip it so that the Operational_Insight.rpd file is accessible.
- Launch the Oracle BI Server Administration tool.



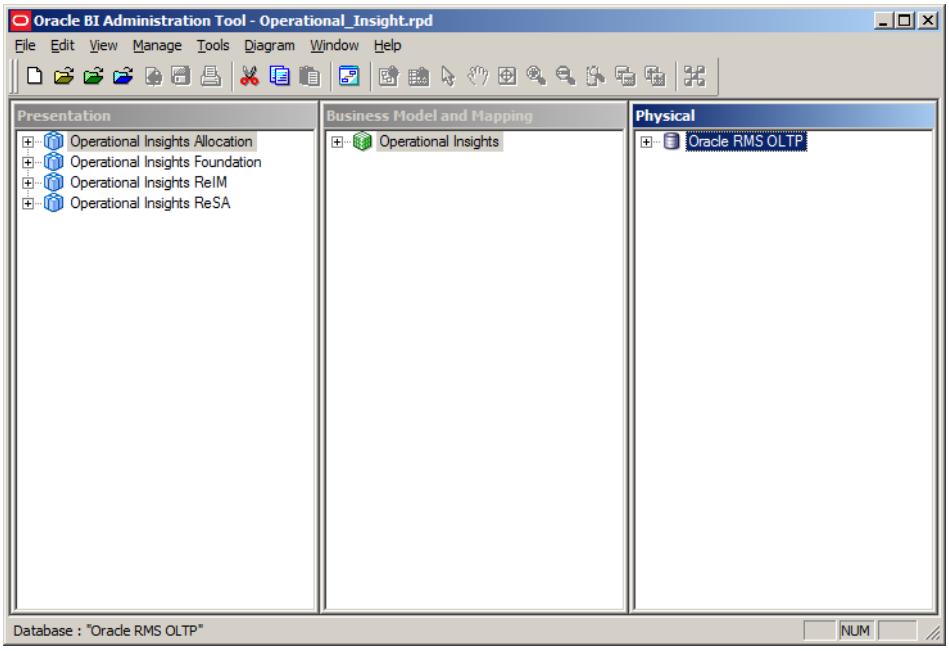
- Under **File** select **Open --> offline**. Navigate to Operational_Insight.rpd file and click **Open**.



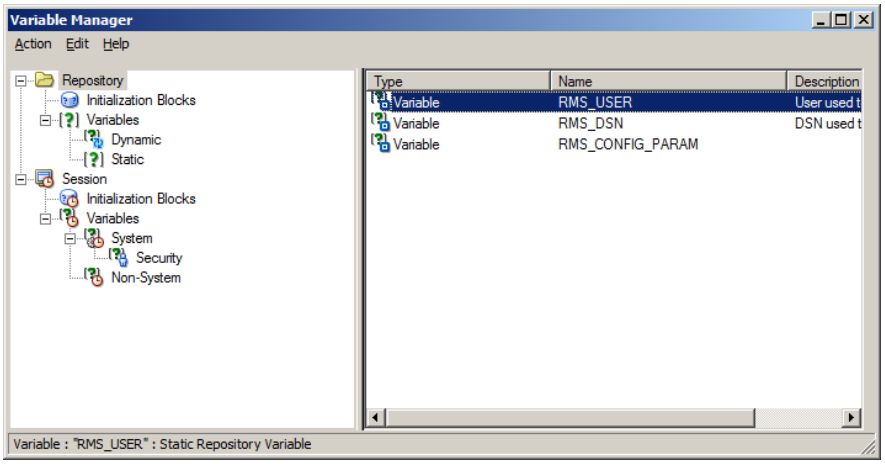
- When prompted for the password, enter **Admin123**.

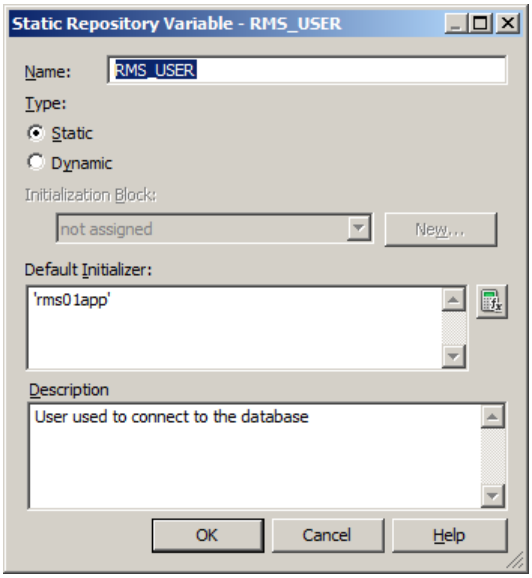


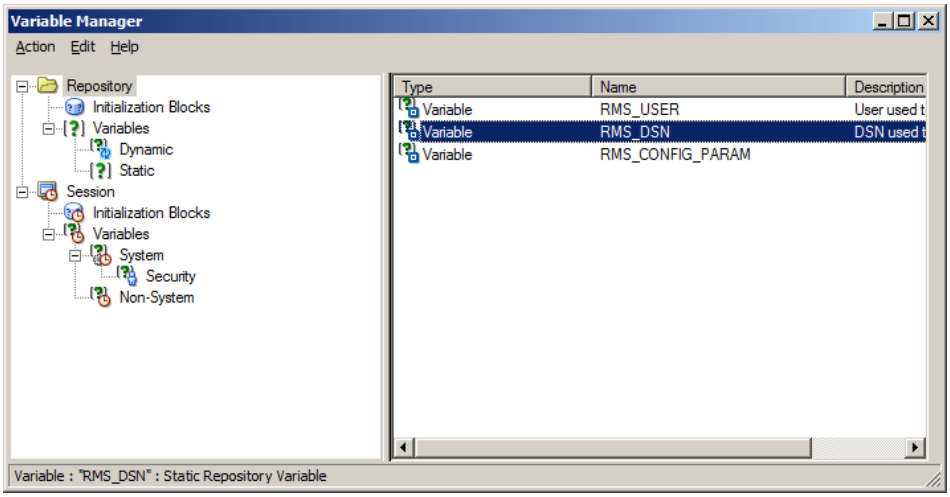
2. When the rpd opens, navigate to Manage > Variable.

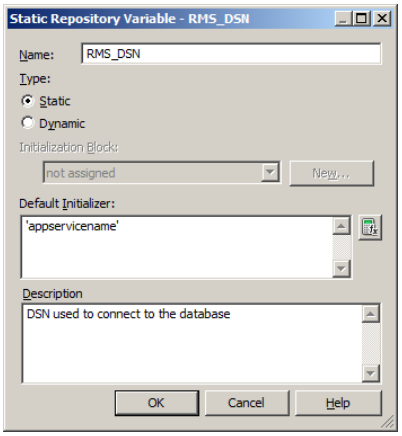


- Under Repository Static variables, Double-click on RMS_USER to edit with main RMS schema username (for example, RMS01) and RMS_DSN with Data Source Name of the RMS Database.

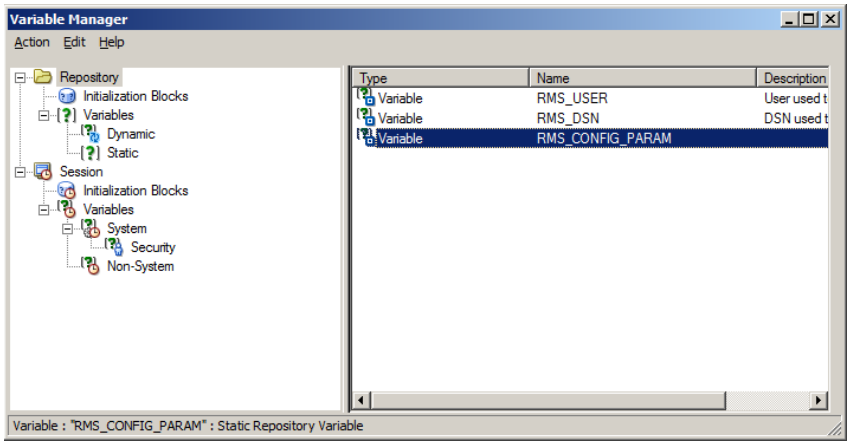

Variable Manager
Action Edit Help
Repository
Initialization Blocks
Variables
Dynamic
Static
Session
Initialization Blocks
Variables
System
Security
Non-System
Type
Name
Description
Variable
RMS_USER
User used t
Variable
RMS_DSN
DSN used t
Variable
RMS_CONFIG_PARAM
Variable : "RMS_USER" : Static Repository Variable

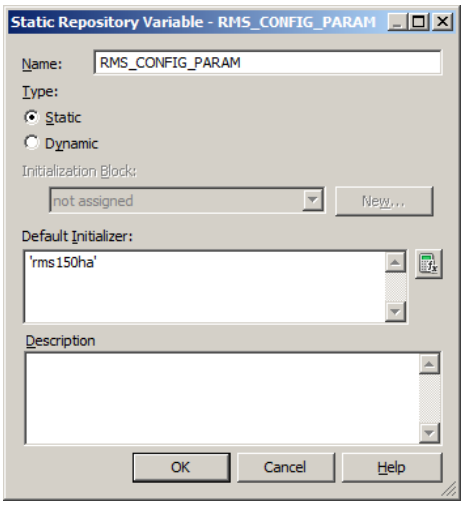

Static Repository Variable - RMS_USER
Name:
RMS_USER
Type:
Static
Dynamic
Initialization Block:
not assigned
New...
Default Initializer:
'rms01app'
Description
User used to connect to the database
OK
Cancel
Help


Variable Manager
Action Edit Help
Repository
Initialization Blocks
Variables
Dynamic
Static
Session
Initialization Blocks
Variables
System
Security
Non-System
Type
Name
Description
Variable
RMS_USER
User used t
Variable
RMS_DSN
DSN used t
Variable
RMS_CONFIG_PARAM
Variable : "RMS_DSN" : Static Repository Variable



- Configure Rpd variable for RMS forms In-context launch
- Change the value of Repository variable: **RMS_CONFIG_PARAM**



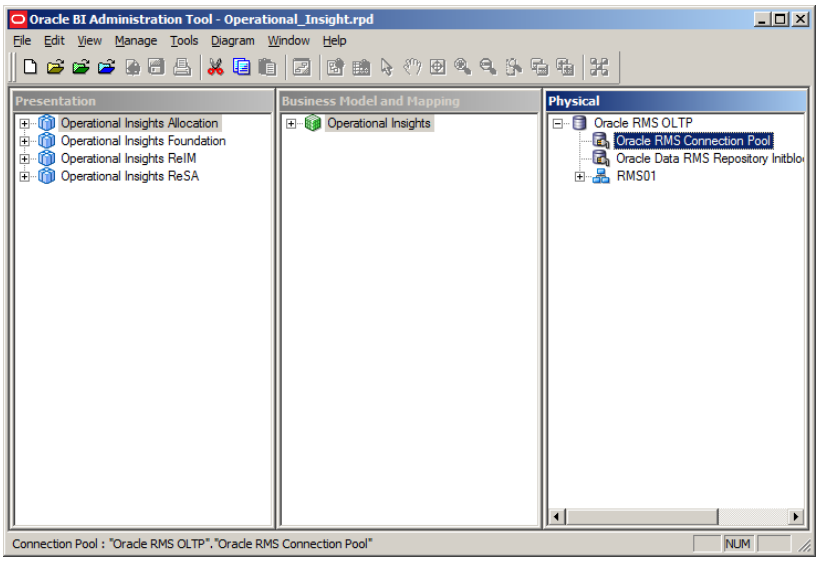


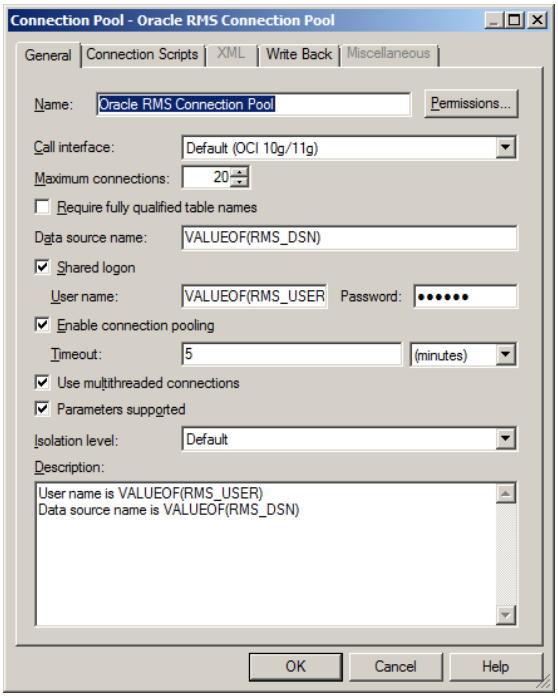
Note: If RMS URL is as below:

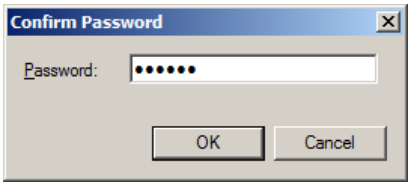
http://<RMS_HOST>:<PORT>/forms/frmservlet?config=<RMS15SSO>

Then the value of "RMS_CONFIG_PARAM" variable will be "RMS15SSO".

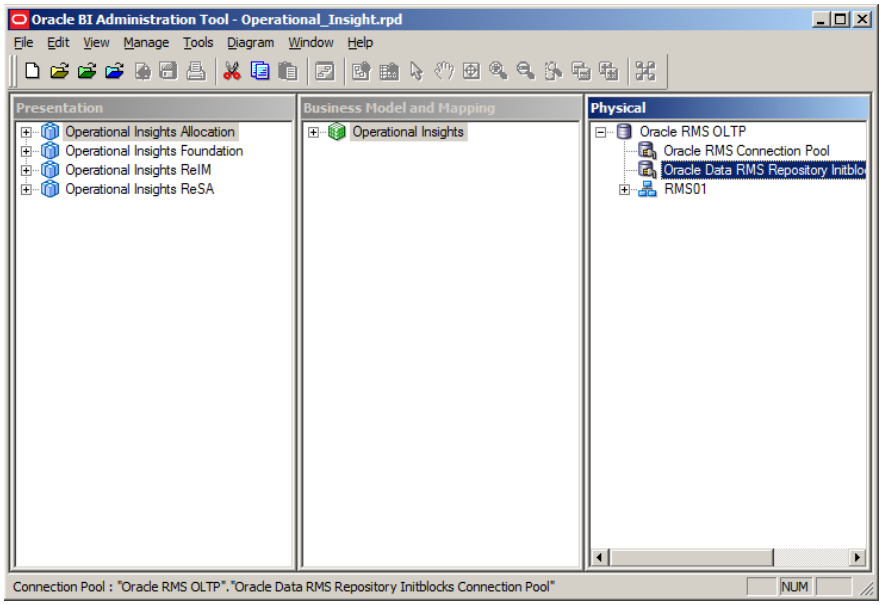
In the Physical Layer, open the Connection Pool (Oracle RMS Connection Pool) under "Oracle RMS OLTP" by right clicking on the icon and update the password for the RMS User. The following is a sample of the Oracle RMS Connection Pool screen.

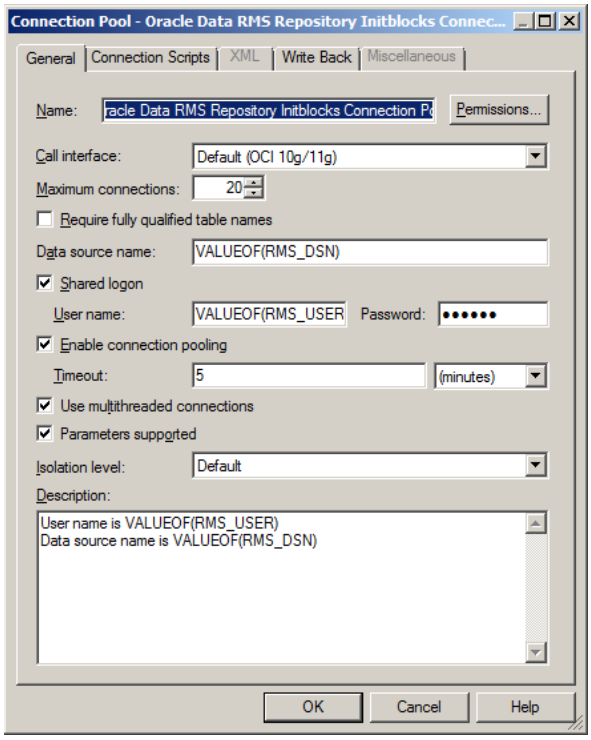


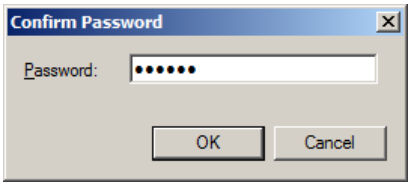




3. Follow the same steps for Oracle Data RMS Repository Initblocks Connection Pool.







4. Click Save to save the changes to the Operational_Insights.rpd file.

5. Test the database connection by right-clicking on any of the tables in the Physical Layer, and select Update Row Count. The number of rows will be shown when that table is highlighted if the database connection is successful.

> **Note:** When making any changes to the repository, does it in the offline mode and before saving the changes perform a global consistency check. The global consistency check should not show any errors. Out of the box Operational Insight repository will have some warnings when a Global Consistency Check is done. These warnings do not affect Operational Insight functionality in any way and these are been thoroughly verified.

Migrate RPD and Catalog for Operational Insights

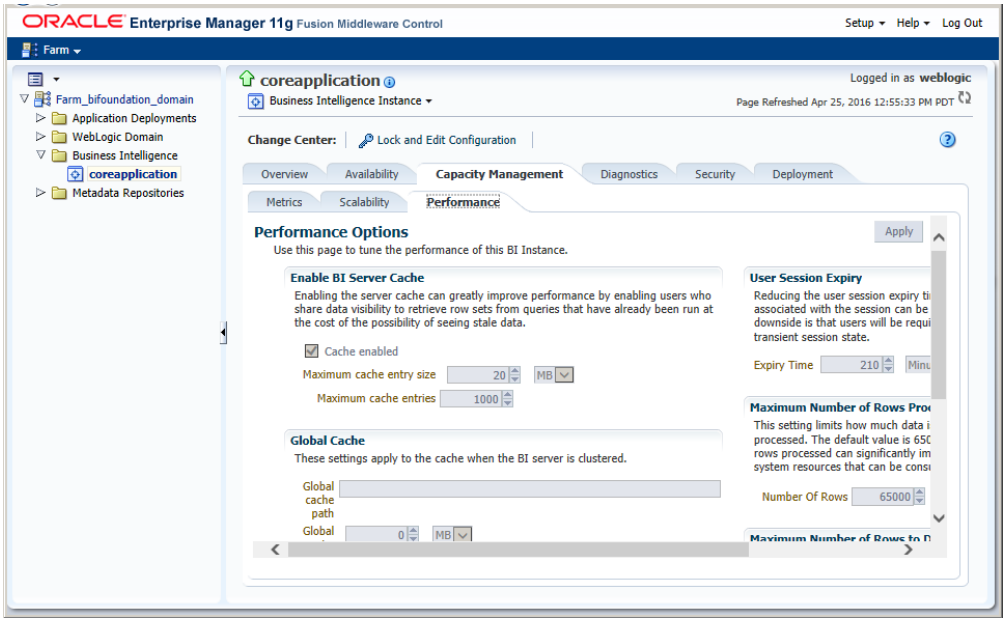
- First verify the existence of tnsnames.ora file on idmhost1 and idmhost2 under <BI_INSTALL_DIRECTORY>/Oracle_BI1/network/admin and the file has an entry of the database used by Operational Insights shown below. If it does not exist create it.

  Example:

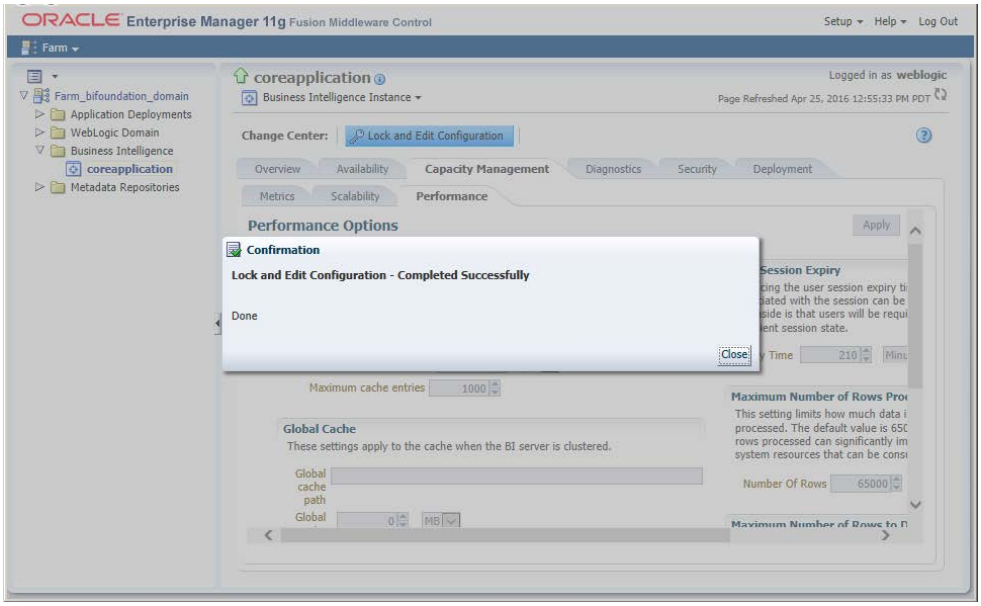
```
FMWSERVICENAME=
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = DBHOST1)(PORT = 1521))
      (ADDRESS = (PROTOCOL = TCP)(HOST = DBHOST2)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = FMWSERVICENAME)
    )
  )
```

- On idmhost1: Navigate to where the Operational_Insight catalog exists in the application installation distribution and copy it to the following directory.
- /vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/catalog
- Complete the following steps to migrate the RPD:
  - Log onto the OBIEE Enterprise Manager.

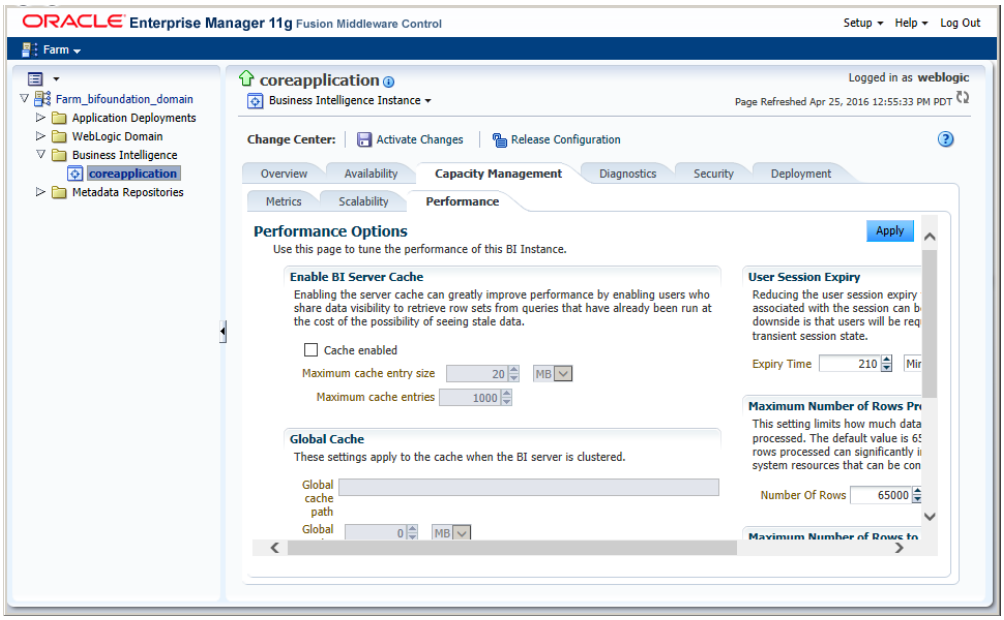
- From the left pane, click **Business Intelligence > coreapplication**, and select **Capacity Management > Performance** tab.



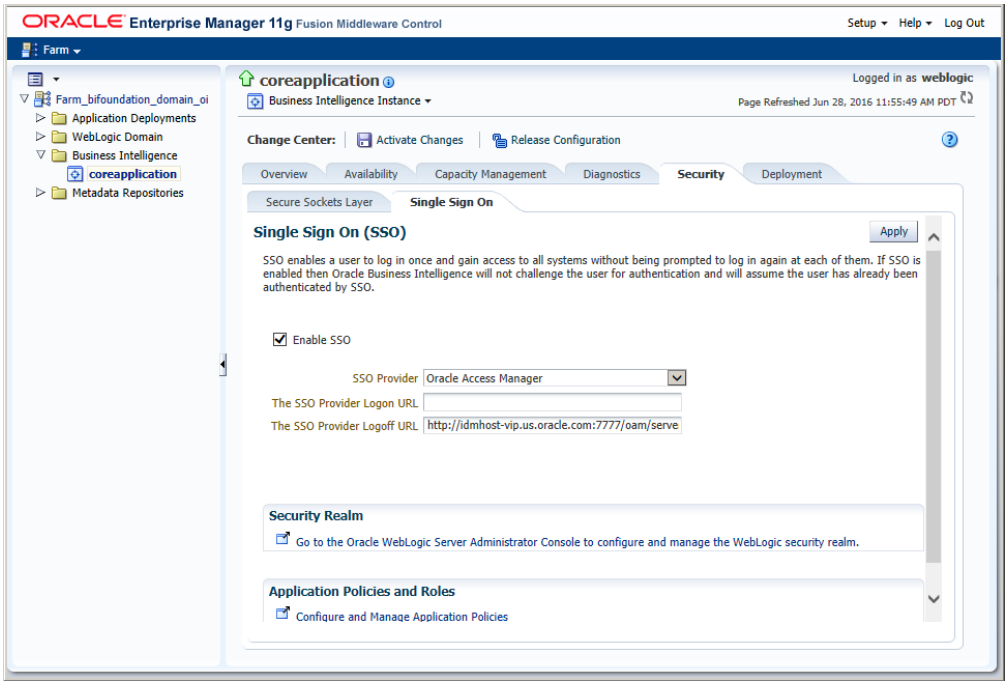
- Click **Lock and Edit Configuration** and then **Close** once the Confirmation window opens.



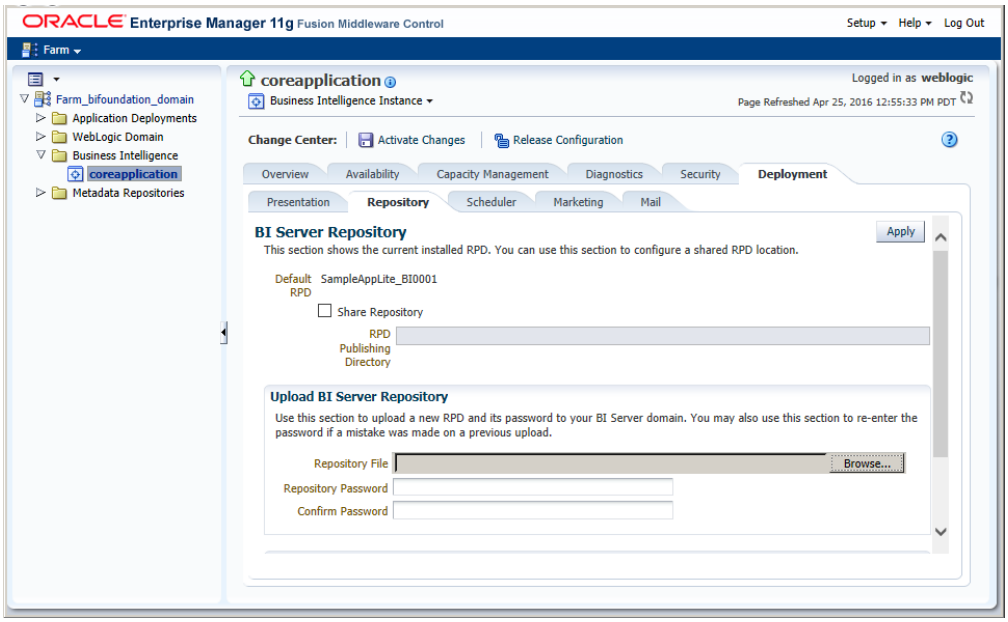
- Uncheck the **Cache enabled** check box and then click **Apply**.



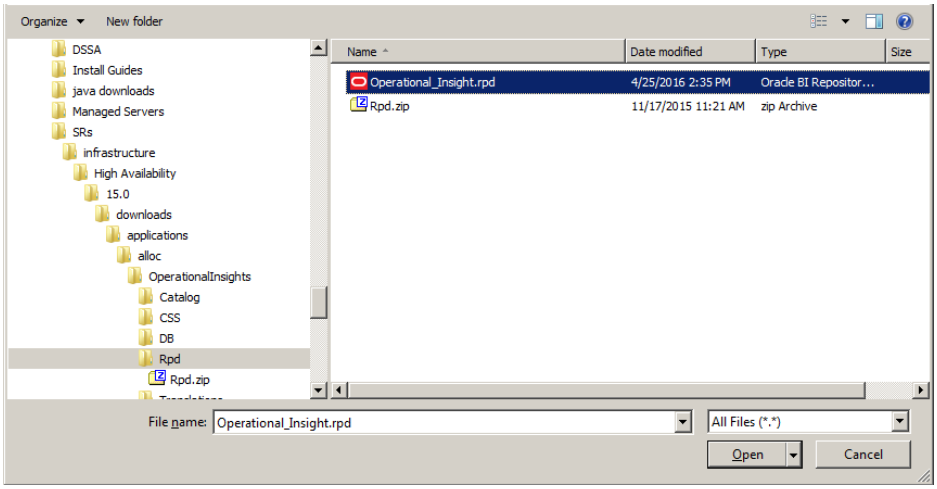
- Navigate to the Security tab and make the following changes:
  - Select Enable SSO.
  - SSO Provider: Oracle Access Manager
  - The SSO Provider Logon URL: <Leave Blank>
  - The SSO Provider Logoff URL: http://idmhost-vip.us.oracle.com:7777/oam/server/logout



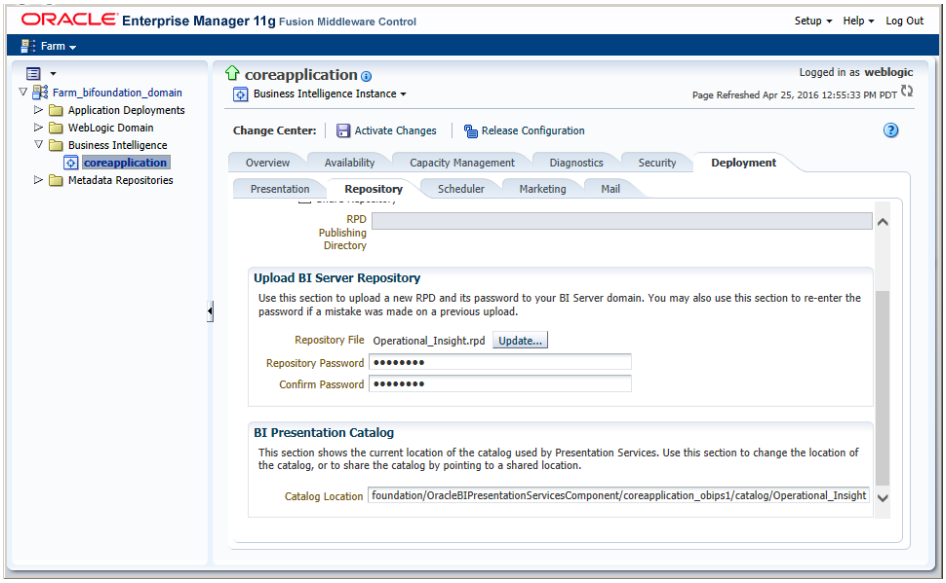
- Navigate to the **Deployment > Repository** tab, and then click **Browse**.



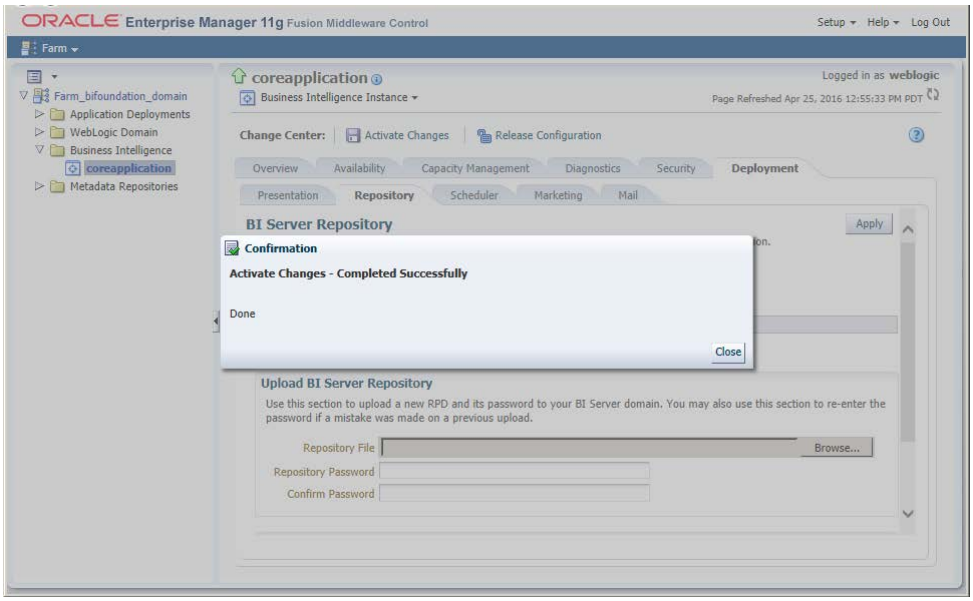
- Select the **Operational_Insight.rpd** file that was updated on the Windows system.



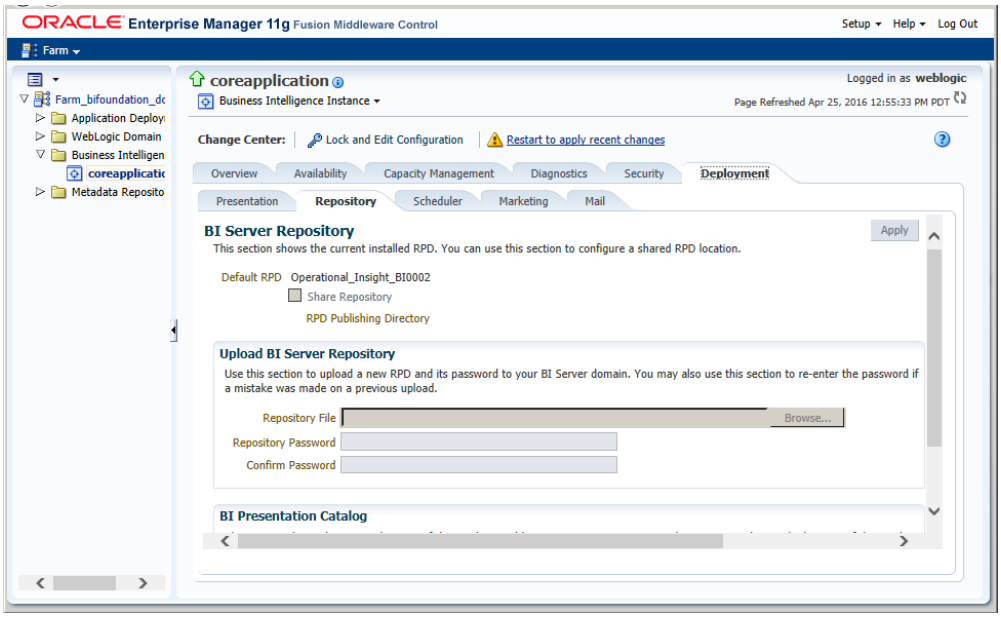
- Make the following updates and then click **Apply**.
  - Repository Password: Admin123
  - Confirm Password: Admin123
  - Catalog Location: `/vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/catalog/Operational_Insight`



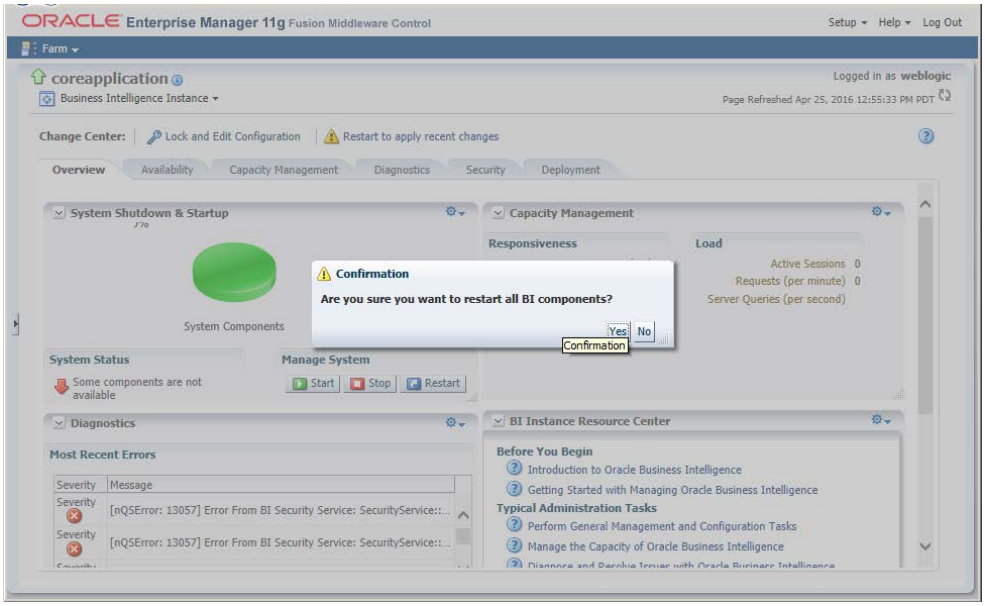
- Click **Activate Changes** and then click **Close** when the Confirmation window opens.



- Click the **Restart to apply recent changes** link.



- Click **Restart** and then click **Yes** when the Confirmation window opens.



Verification – Operational Insights Logon

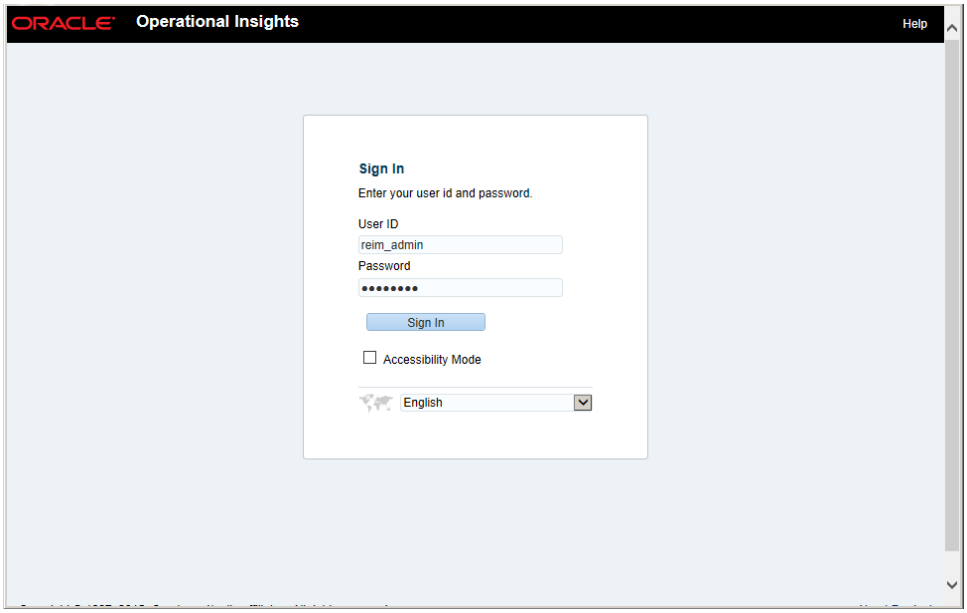
At this time enough the configuration should be completed for Operational Insights in order to test to make sure that the installation has been done correctly so far by logging into Operational Insights and viewing the Operational Insights dashboards.

1. Launch the OBIEE analytics URL using the managed server bi_server1 port (http://idmhost1.us.oracle.com:7333/analytics) and logon with one of the credentials that was created by importing LDIF scripts into OID.

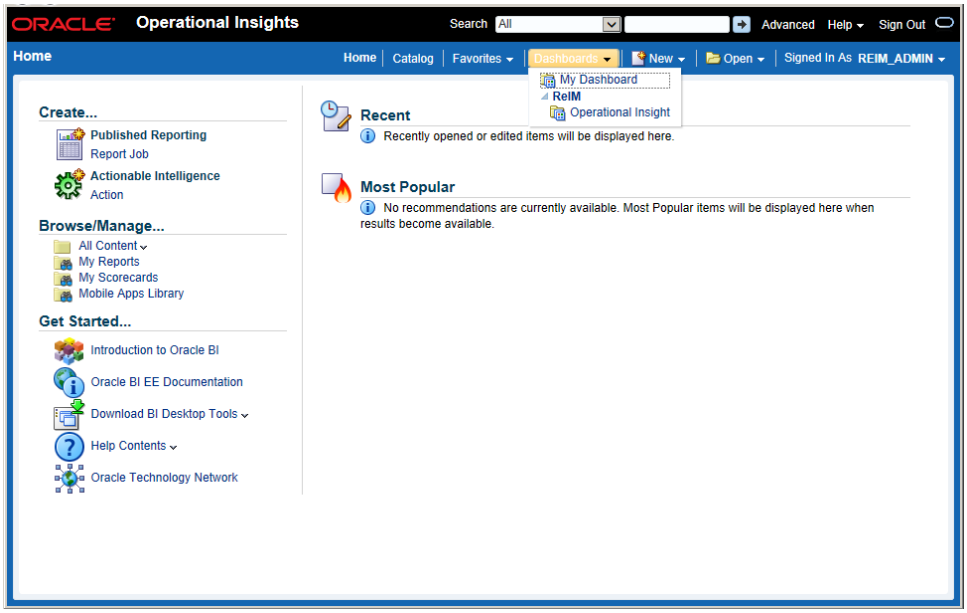
   Example:

   User Name: reim_admin

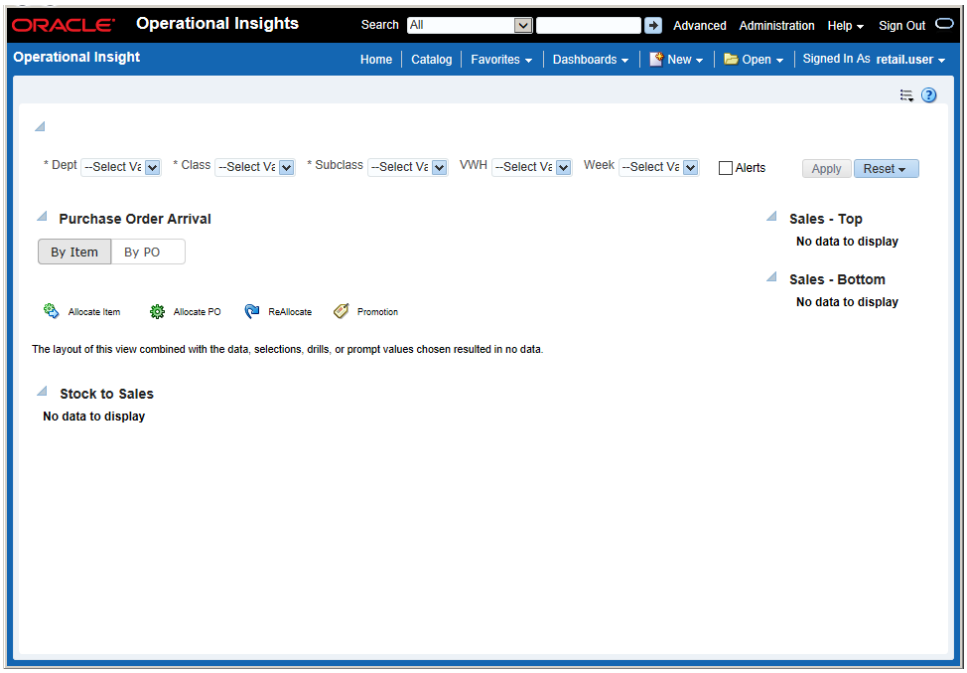
   Password: `<password>`



2. Click on the **Dashboards** menu item and select **Operational Insight** from the drop down list.



3. The following window will be displayed.



Troubleshooting

If you face any login issue after rpd and catalog migration, or if Oracle BI EE presentation services are going to init state, then you must refresh the GUID using the steps below.

Refresh User GUIDs

This task requires that you manually edit the configuration files to instruct the Oracle BI Server and Presentation Services to refresh the GUIDs on restart. Once completed, you edit these files to remove the modification. For information about where to locate Oracle Business Intelligence configuration files, see "Where Configuration Files are Located"

in the Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition.

To refresh user GUIDs, perform the following steps on idmhost1.

1. Update the FMW_UPDATE_ROLE_AND_USER_REF_GUIDS parameter in NQSConfig.INI located in the following directory:
2. /vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/config/OraclBIServerComponent/coreapplication_obis1
3. Locate the FMW_UPDATE_ROLE_AND_USER_REF_GUIDS parameter and set it to YES, as follows:
4. FMW_UPDATE_ROLE_AND_USER_REF_GUIDS = YES;
5. Save and close the file.
6. Update the Catalog element in instanceconfig.xml located in the following directory:
   `/vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/config/OraclBIPresentationServicesComponent/coreapplication_obips1`
7. Locate the Catalog element and update it as follows:

   Example:
   ```
   <Catalog>
   <UpgradeAndExit>false</UpgradeAndExit>
   <UpdateAccountGUIDs>UpdateAndExit</UpdateAccountGUIDs>
   </Catalog>
   ```
8. Save and close the file.
9. Restart the Oracle BI Server and Presentation Services using opmnctl:

   Example:
   ```
   $ export
   ORACLE_INSTANCE=/vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1
   ```
   $ cd /u00/webadmin/products/wls_obiee_oi/Oracle_BI1/opmn/bin

   $./opmnctl stopall

   $./opmnctl startall
10. After you confirm that the opmn processes have started – pause a few moments and wait for the ias-compnent coreapplication_obips1 stop running. Keep checking the status until the opmn process does go down:

    Example:

    $ ./opmnctl status
11. Processes in Instance: instance1

ias-component	Process-type	pid	Status
coreapplication_obiccs1	OracleBIClusterCo~	1498	Alive
coreapplication_obisch1	OracleBIScheduler~	1498	Alive
coreapplication_obijh1	OracleBIJavaHostC~	1491	Alive
coreapplication_obips1	OracleBIPresentat~	N/A	Down
coreapplication_obis1	OracleBIServerCom~	1490	Alive

Note: The service will come up and go down which is normal.

12. Set the FMW_UPDATE_ROLE_AND_USER_REF_GUIDS parameter in NQSConfig.INI back to NO.

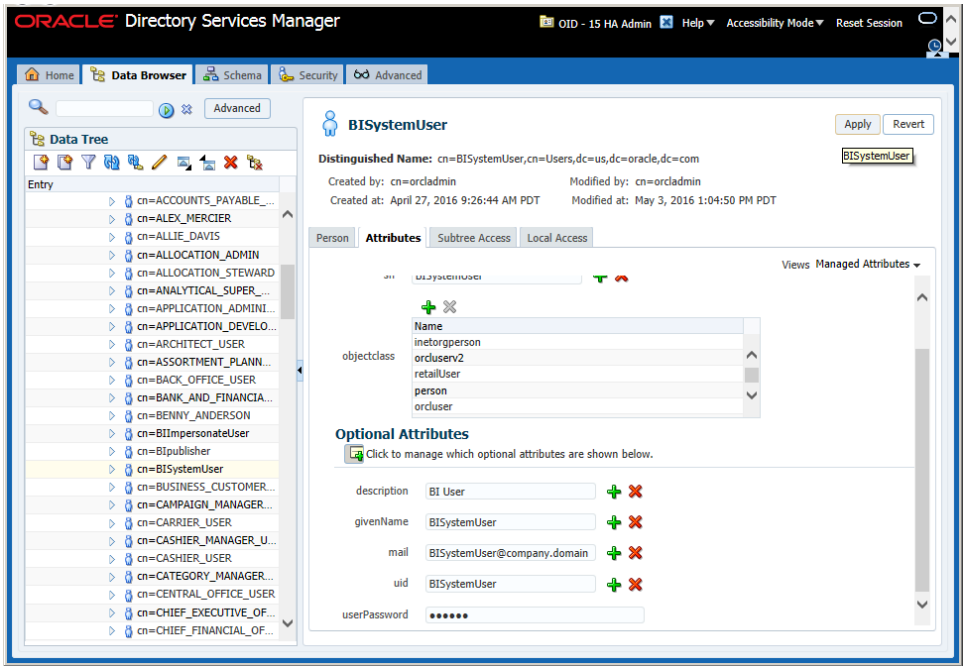
    Important: You must perform this step to ensure that your system is secure.

13. Update the Catalog element in instanceconfig.xml to remove the UpdateAccount GUIDs entry.
14. Restart the Oracle Business Intelligence system components again using opmnctl:

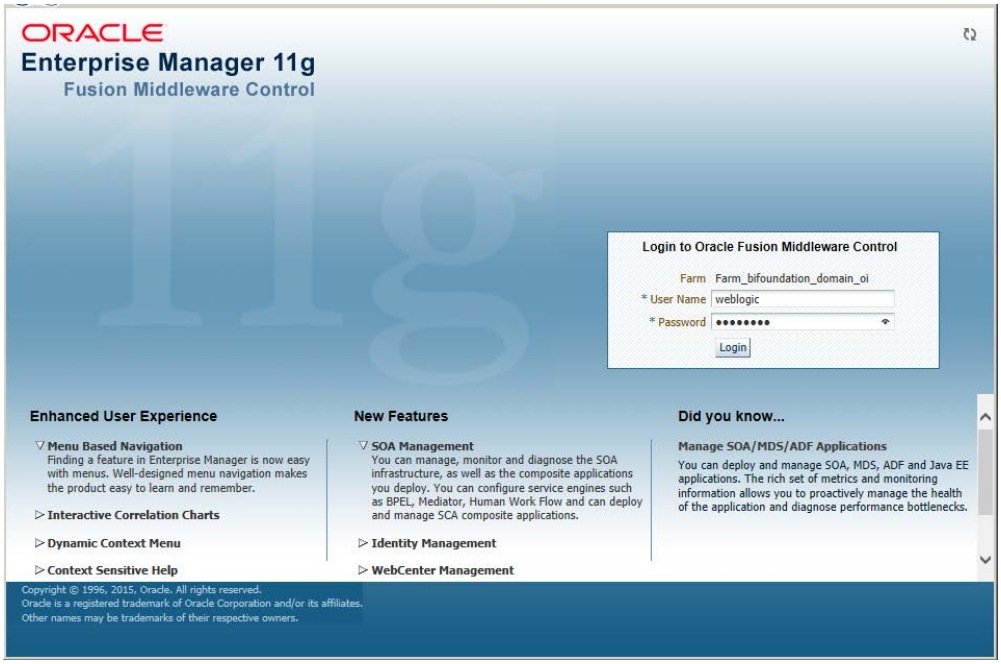
    Example:

    ```
    $ cd /u00/webadmin/products/wls_obiee_oi/Oracle_BI1/opmn/bin
    $./opmnctl stopall
    $./opmnctl startall
    ```

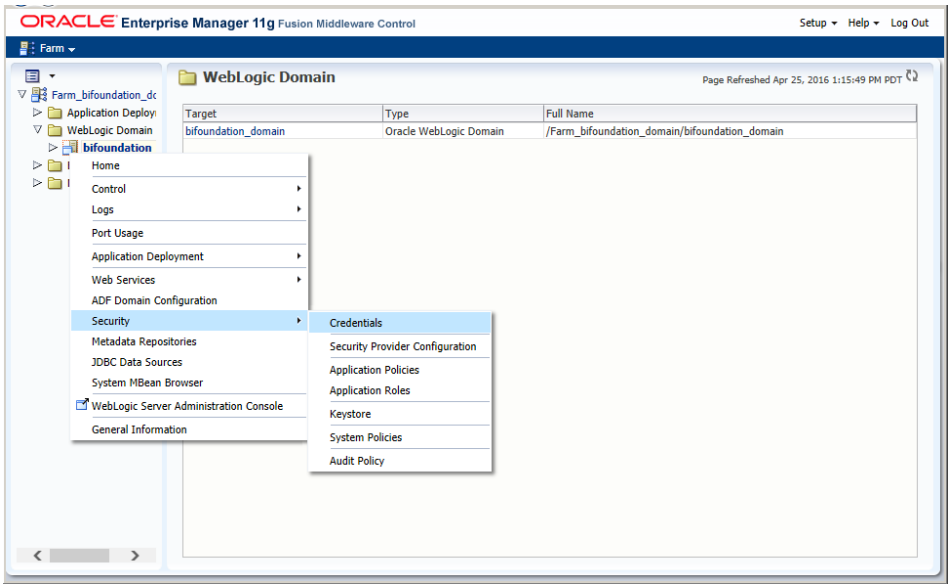
15. If BISytemUser fails to authenticate and the error is in presentation service - follow the procedure below procedure to synchronize the password for the BISystemUser across the WebLogic admin console, WebLogic Enterprise Manager and OID.
    a. Log onto ODSM
    b. Under the Data Browser tab – Navigate: Root --> dc=com --> dc=oracle --> dc=us --> cn=Users --> cn=BISystemUser. Then under the Attributes tab - Update the BISystemUser password to <password> and click Apply



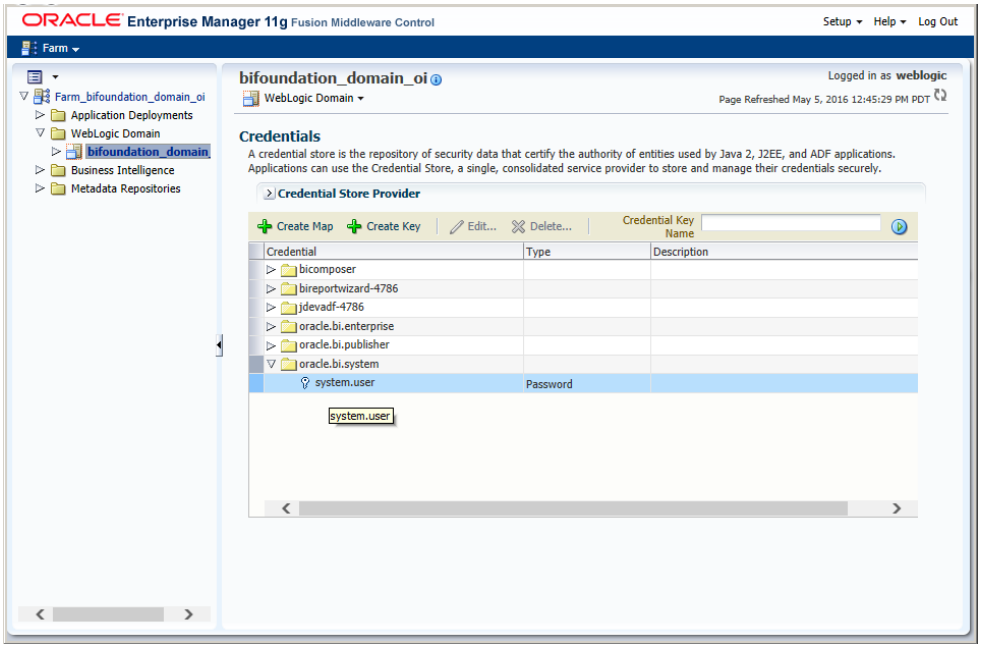
    c. Log onto Enterprise Manager



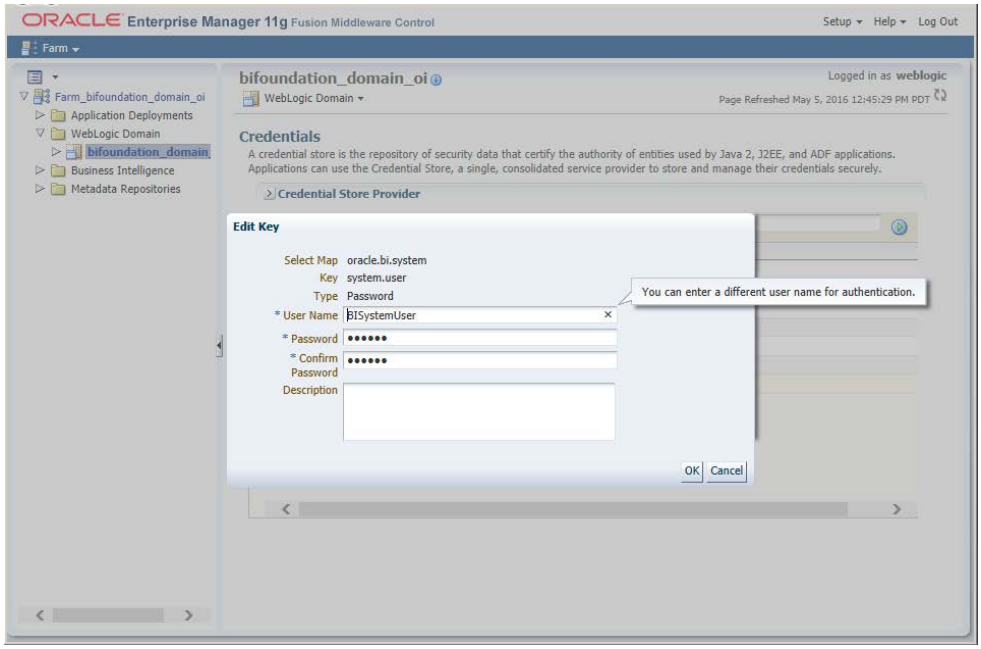
d. From the left pane, click **bifoundation > Security > Credentials**.



e. Under oracle.bi.syste, select **system.user** and click **Edit.**

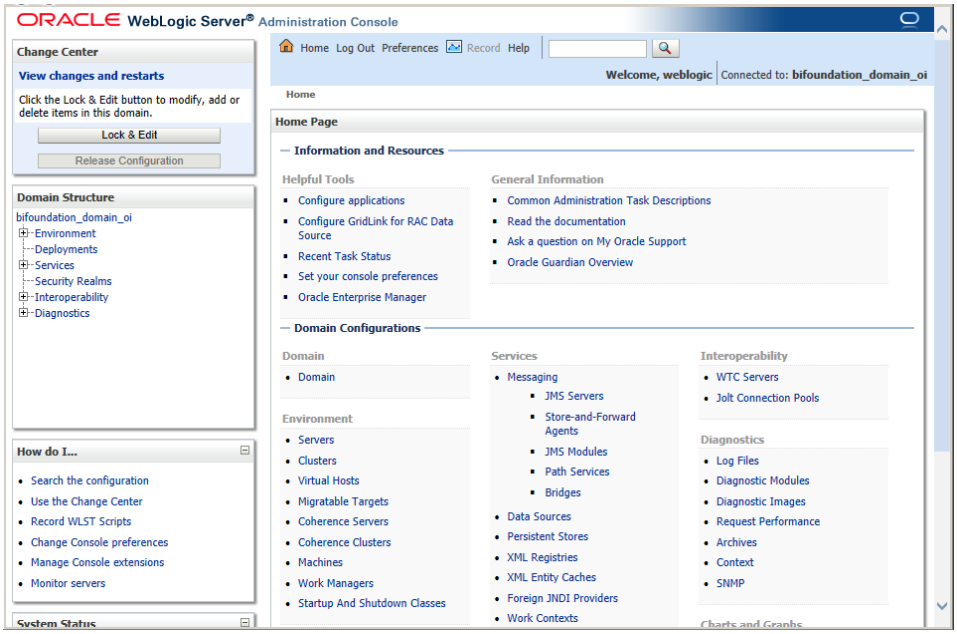


f. Set the password to the same that was set in ODSM and click **OK**.

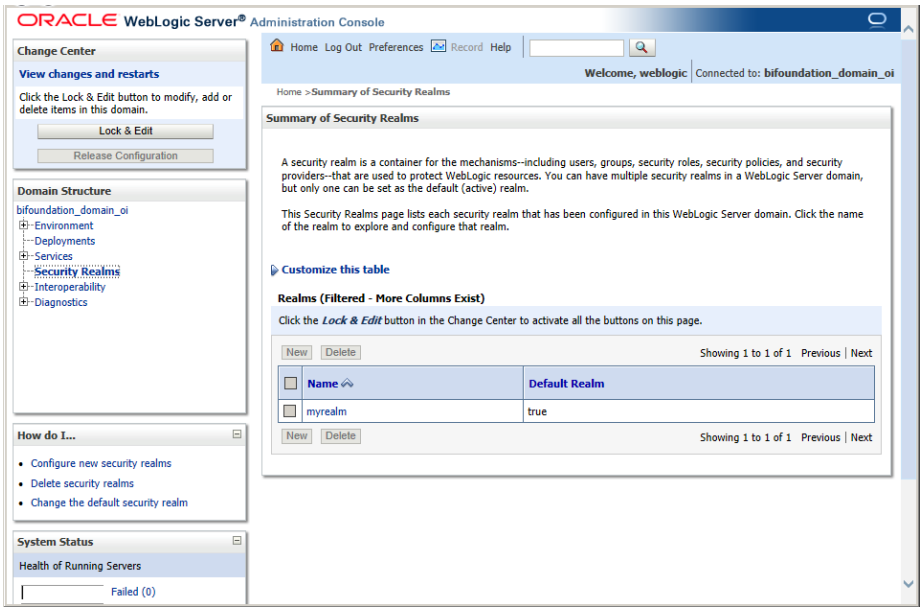


g. Log onto the WebLogic admin console.

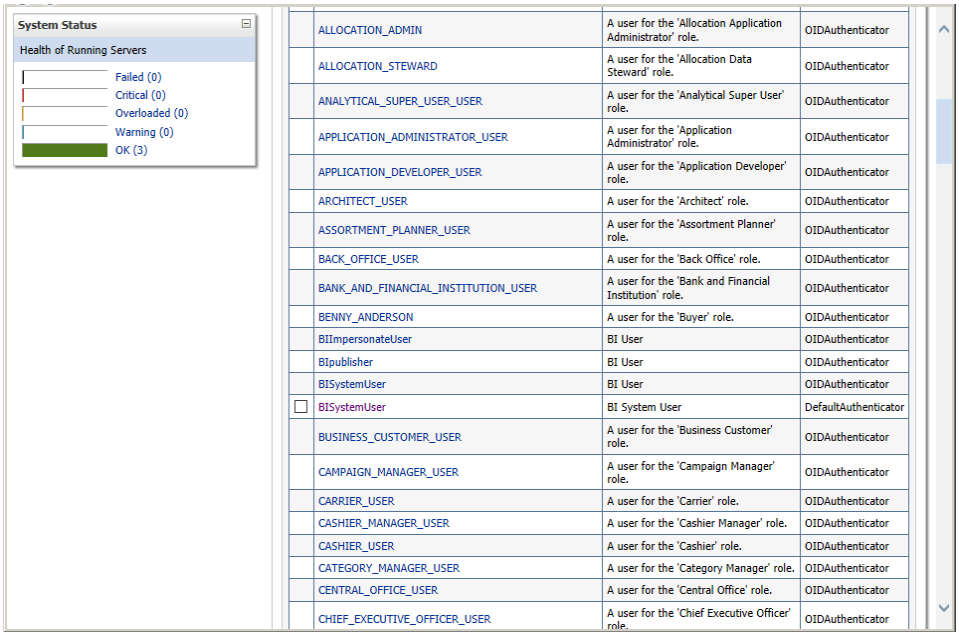
h. Click **Security Realms** from the navigation pane.



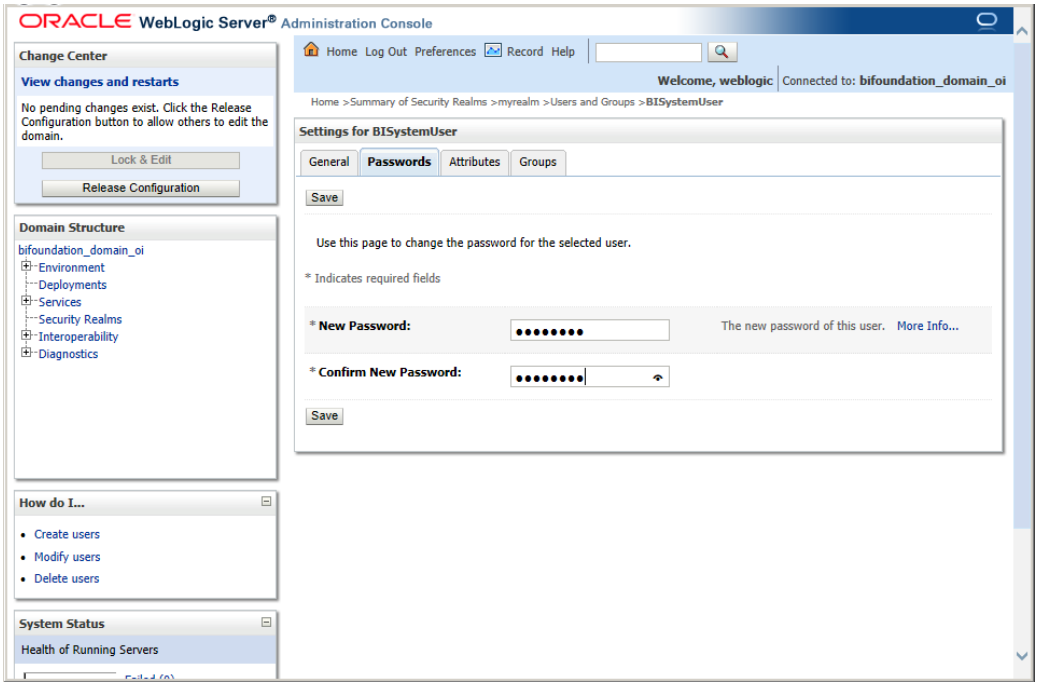
i. Click **myrealm**.



j. Under the Users and Groups, click the **BISytsemUser** tab.



k. Under the Passwords tab updated the password to be the same that was entered in ODSM and Enterprise Manager, and click **Save**.



l. Stop the WebLogic admin and managed servers and then restart them again.

m. Stop and restart all opmn processes.

Post install Configuration for OBIEE Display

The Oracle BI EE environment has to be configured for enabling Operational Insights. Please follow the steps to configure the Oracle BI EE environment for Operational Insights.

1. There are several modifications that are needed to the instanceconfig.xml and NQSConfig.INI files in OBIEE to enable functionality and enhance performance. The requirements are described in singular steps seperately in the REIM, ReSA, and Allocation install guides and are listed below.

   a. Enable the Oracle BI EE Content to be displayed in IFrame.

   b. Configure Charts /Charts/to use HTML5.

   c. Enable EVALUATE Function in Oracle BI EE.

   d. Disable Cache in Oracle BI EE.

   e. Deploy Operational Insights Skin and Styles.

   f. Enable the ADF Contextual Event Action in Oracle BI EE.

   First stop all opmn processes for OBIEE.

   Example:

```
$ export
ORACLE_INSTANCE=/vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/in
stance1
$ cd /u00/webadmin/products/wls_obiee_oi/Oracle_BI1/opmn/bin
$./opmnctl stopall
$./opmnctl startall
```

Updating instanceconfig.xml

Since it is more efficient to update the instanceconfig.xml and restart the opmn processes, make the following changes to the instanceconfig.xml file.

> **Note**: The changes listed below with corresponding requirement.

- Navigate to instanceconfig.xml file and take a back up.

  Example:
  ```
  $ cd
  /vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/config/O
  racleBIPresentationServicesComponent/coreapplication_obips1

  $ cp instanceconfig.xml instanceconfig.xml_backup
  ```

Updates to instanceconfig.xml file for Enable the Oracle BI EE Content to be displayed in IFrame:

- Add the following somewhere between the <Security></Security> tags.

  Example:
  ```
  <InIFrameRenderingMode>allow</InIFrameRenderingMode>
  ```

Updates to instanceconfig.xml file for Configure Charts /Charts/to use HTML5:

- In order to enable charts to use HTML5 instead of Flash - Add the code below between the </Table> and </views> tags.

  Example:
  ```
  <Charts>
  <DefaultWebImageType>html5</DefaultWebImageType>
  <MaxVisibleColumns>2000</MaxVisibleColumns>
  <MaxVisiblePages>1000</MaxVisiblePages>
  <MaxVisibleRows>2000</MaxVisibleRows>
  <MaxVisibleSections>25</MaxVisibleSections>
  </Charts>
  ```

Updates to instanceconfig.xml file for **Disable Cache in Oracle BI EE:**

- To disable cache in Oracle BIEE - add the code below in between the `<ServerInstance> </ServerInstance> tags.`

  > **NOTE**: There is also a requirement to update the Enable BI Server Cache in EM. That was already done during the steps for deploying the RPD and catalog.)

  Example:
  ```
  <Cache>
  <Query>
  <MaxEntries>100</MaxEntries>
  <MaxExpireMinutes>1</MaxExpireMinutes>
  <MinExpireMinutes>1</MinExpireMinutes>
  <MinUserExpireMinutes>1</MinUserExpireMinutes>
  </Query>
  </Cache>
  ```

Updates to instanceconfig.xml file for Deploy Operational Insights Skin and Styles

- To enable the Operational Insights skins and styles - Replace the following tags:

```
<UI>
  <DefaultSkin>Skyros</DefaultSkin>
  <DefaultStyle>Skyros</DefaultStyle>
</UI>
```

  With:

  Example:

```
<UI>
  <DefaultStyle>skyros_custom</DefaultStyle>
  <DefaultSkin>skyros_custom</DefaultSkin>
</UI>
<URL>
<CustomerResourcePhysicalPath>/vol.rtk/projects/ha_15/products/wls_obiee_o
i/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/c
oreapplication_obips1/analyticsRes
</CustomerResourcePhysicalPath>

  <CustomerResourceVirtualPath>/analyticsRes</CustomerResourceVirtualPath>
</URL>
```

- Updates to instanceconfig.xml file to Enable the ADF Contextual Event Action in Oracle BI EE:
- In file instanceconfig.xml add a new ActionLinks attribute between the <ServerInstance> </ServerInstance> tag of the instanceconfig.xml file as follows:

  Example:

```
<ActionLinks>
     <EnableADFContextualEvent>true</EnableADFContextualEvent>
</ActionLinks>
```

Updating NQSConfig.INI

- Navigate to NQSConfig.INI file and take a back up.

  Example:

```
$ cd
/vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/config/O
racleBIServerComponent/coreapplication_obis1
$ cp NQSConfig.INI NQSConfig.INI_backup
```

Updates to NQSConfig.INI file for **Enable EVALUATE Function in Oracle BI EE:**

- Change the parameter EVALUATE_SUPPORT_LEVEL to 2 as follows

  Example:

```
EVALUATE_SUPPORT_LEVEL = 2;
```

The changes required for instanceconfig.xml and NQSConfig.INI are complete - Restart opmn processes.

Example:

```
$ export
ORACLE_INSTANCE=/vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/in
stance1
$ cd /u00/webadmin/products/wls_obiee_oi/Oracle_BI1/opmn/bin
```

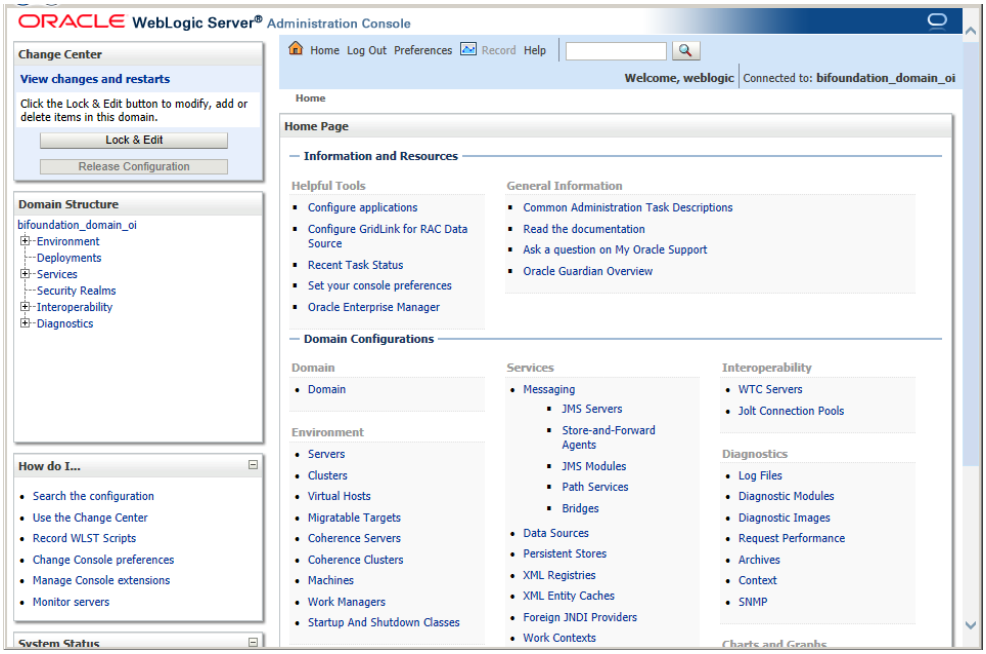
Deploy Operational Insights Skin and Styles

Create a web application called 'analyticsRes' in the OBIEE for Operational Insights environment by creating an application deployment in the WebLoic admin Console

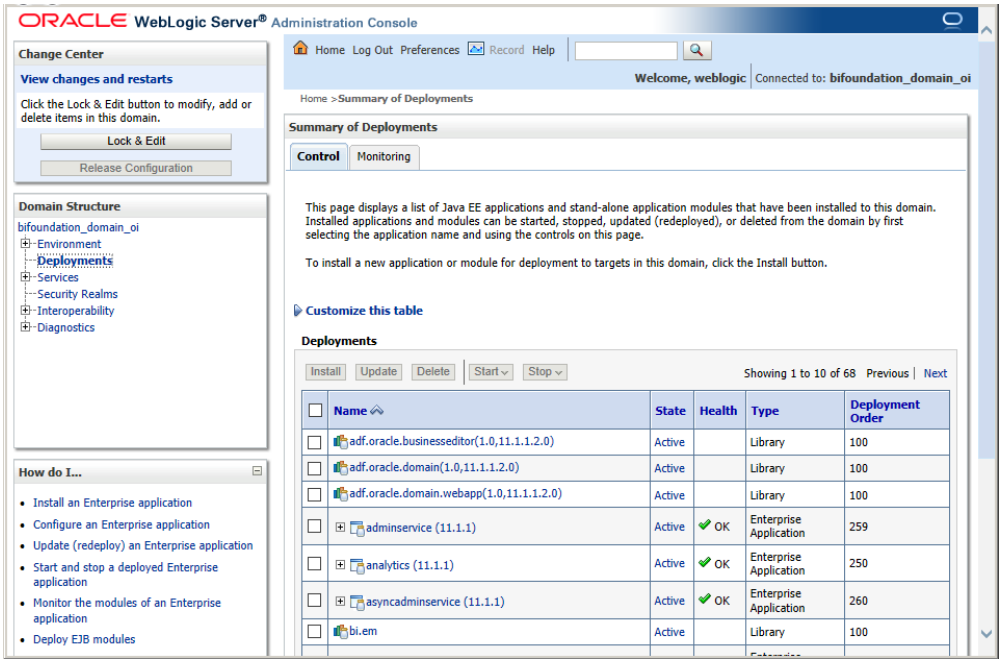
called analyticsRes that points to the <ORACLE_INSTANCE>/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/analyticsRes directory and targeting the OBIEE cluster.

- Logon to the OBIEE WebLogic admin console.

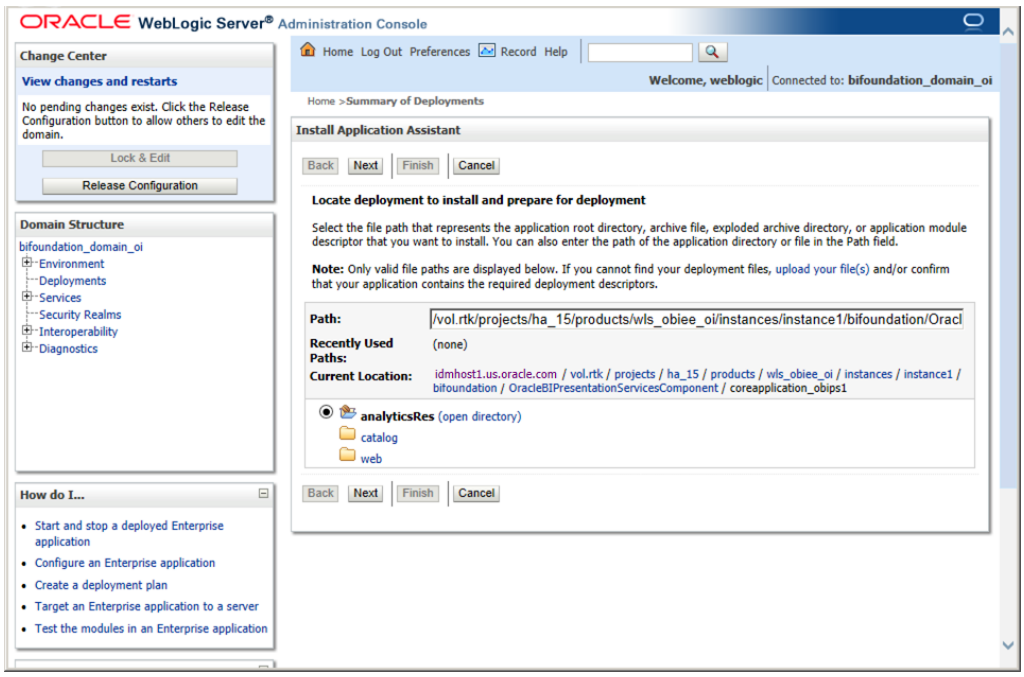
- Click **Deployments** from the left pane.



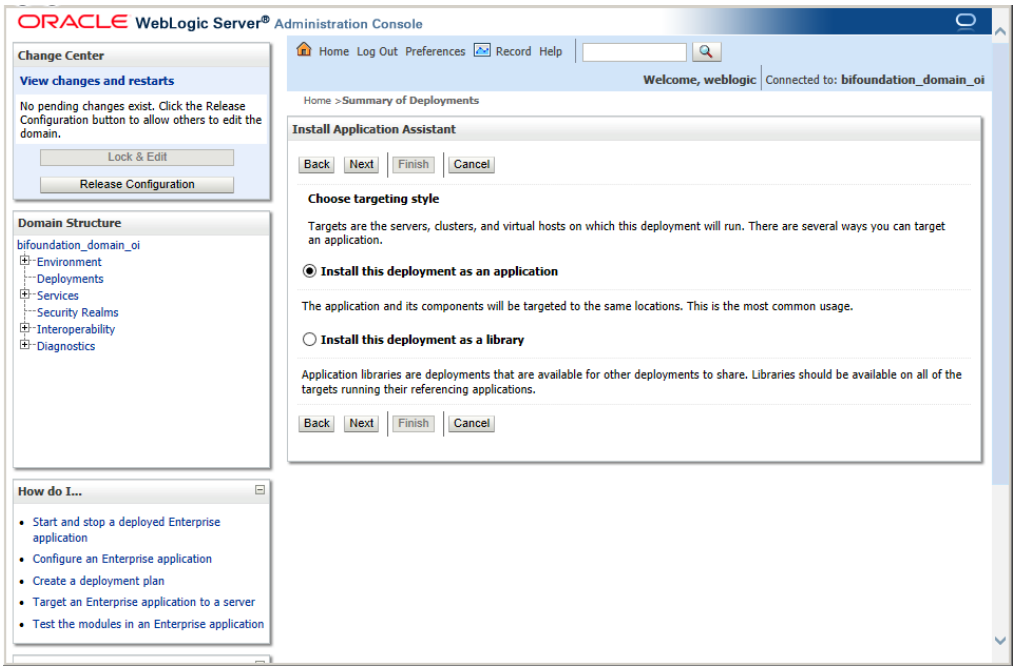
- Click the **Lock & Edit** button, and then click **Install**.



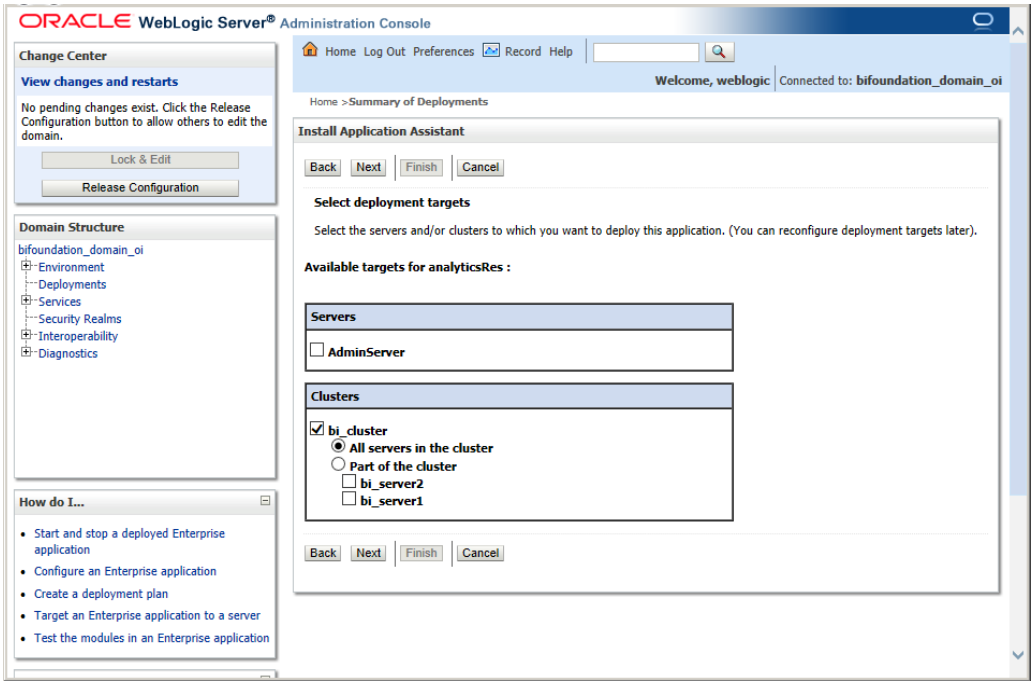
- Set the value for Path to the following, and click **Next**.
  - /vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/analyticsRes



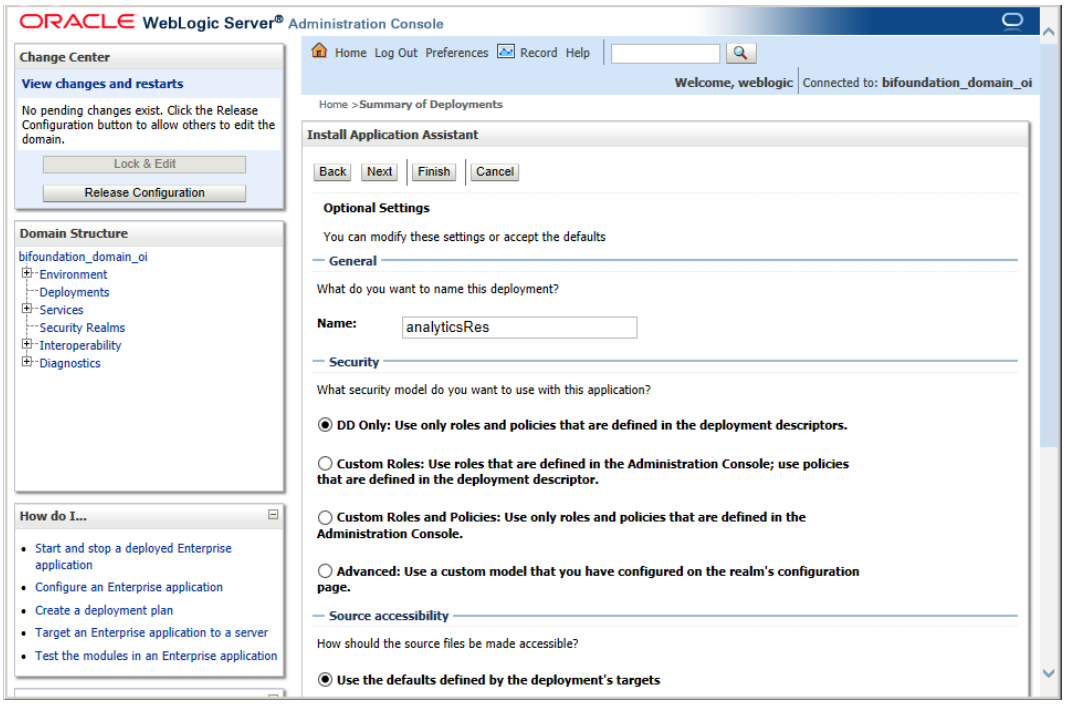
- Select **Install this deployment as a application,** and click **Next**.



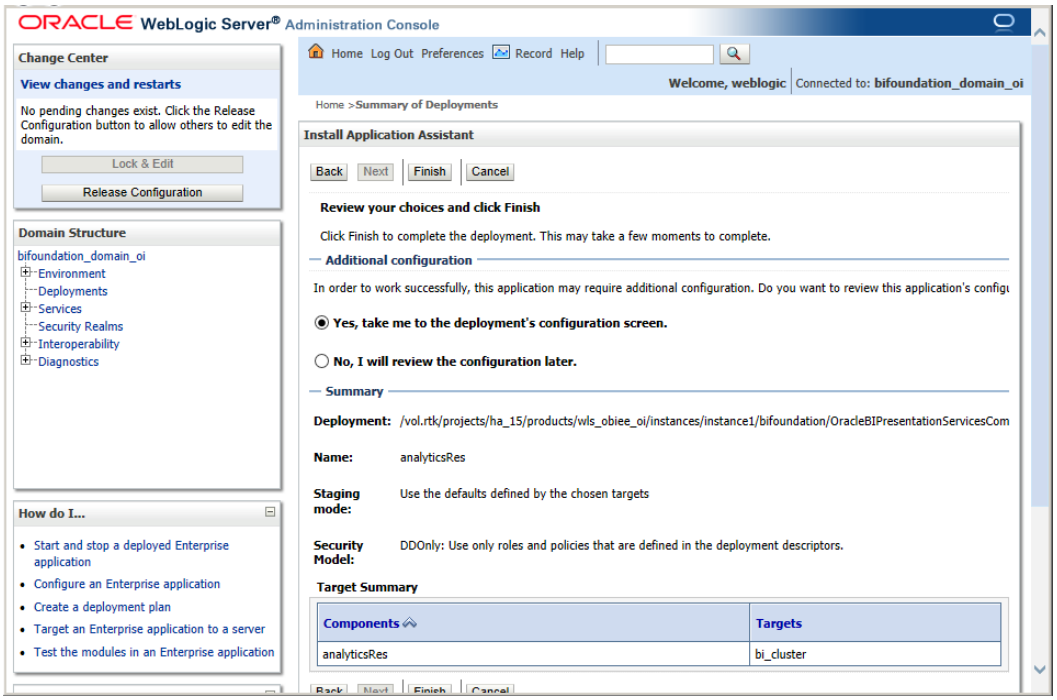
- In the Select deployment targets window , select **All servers in the cluster,** and click **Next**.



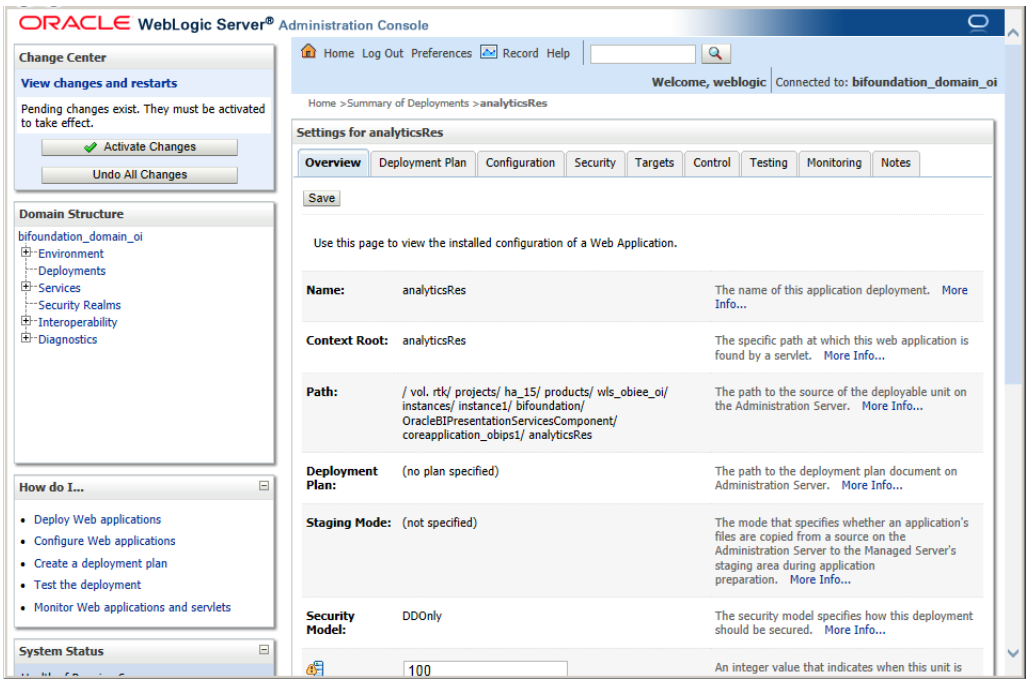
- Click **Next**.



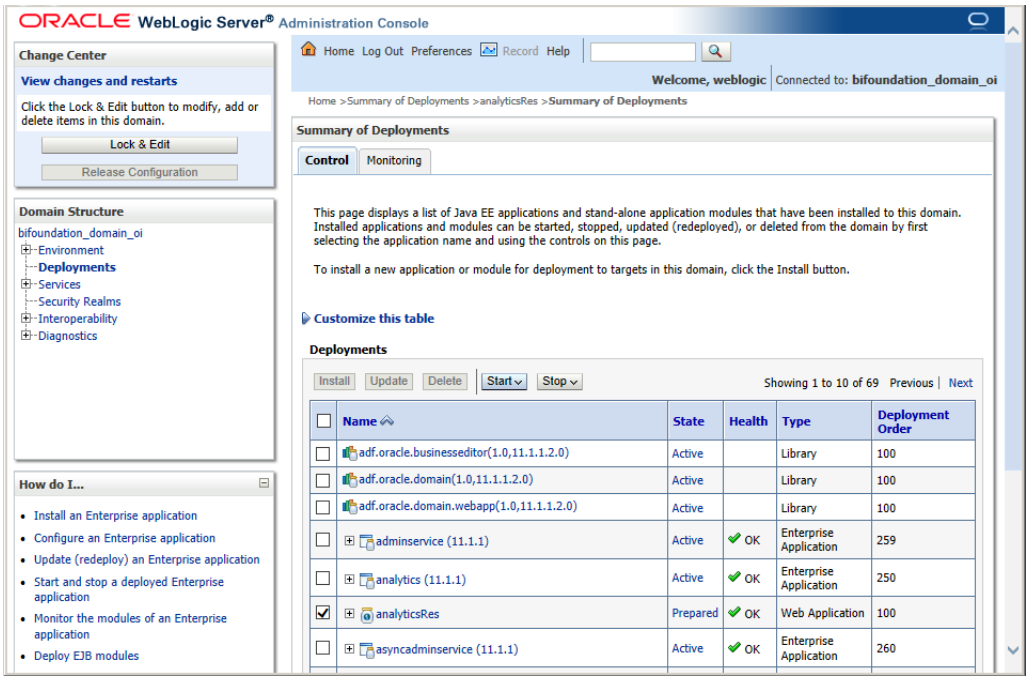
- Click **Finish**.



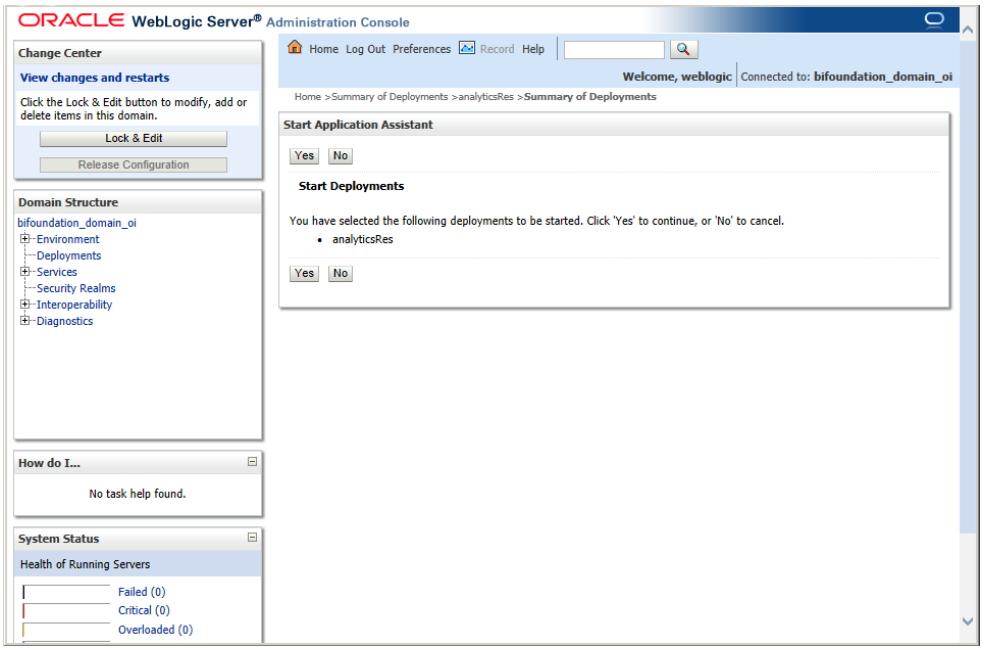
- Click the **Activate Changes** button, and then click the **Deployments** left pane.



- Select the **analyticRes** deployment, and then click **Start**



- Click **Start.**



- From the REIM application installation distribution <install_dir>/OperationalInsights/CSS/ copy the OI_Custom_Style.zip file to the following location on idmhost1.

  Example:
  `/vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/analyticsRes`

- Navigate the location the OI_Custom_Style.zip file was copied to and unzip it.

  Example:
  ```
  $ cd
  /vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/analyticsRes
  $ unzip OI_Custom_Style.zip
  ```

The unzipped directory will have an OI_Custom_Style folder. The OI_Custom_Style folder includes the following four directories:

- s_skyros_custom
- sk_skyros_custom
- customMessages
- oicustomjs
- Copy the above Four directories to the following location (Up one directory to analyticsRes):
  vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/analyticsRes

  Example:
  ```
  $ cd
  /vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/analyticsRes/OI_Custom_Style

  $ cp -R * ..
  ```

Create Symbolic Link to analyticsRes Directory

Create Symbolic Link to analyticsRes Directory for the custom resources to be available to the Oracle BI EE Presentations Services connection when using the StaticResourceMode as Auto.

- Change the directory to <OBIEE_DOMAIN_NAME>/servers/bi_server1/tmp/_WL_user/analytics_11.1.1/7dezjl/war on idmhost1

  Example:

  ```
  $ cd
  /u00/webadmin/config/domains/wls_obiee_oi/bifoundation_domain_oi/servers/bi_server1/tmp/_WL_user/analytics_11.1.1/7dezjl/war
  ```

- Change the directory to <OBIEE_DOMAIN_NAME>/servers/bi_server1/tmp/_WL_user/analytics_11.1.1/sc09uk/war on idmhost2

  Example:

  ```
  $ cd
  /u00/webadmin/config/domains/wls_obiee_oi/bifoundation_domain_oi/servers/bi_server2/tmp/_WL_user/analytics_11.1.1/sc09uk/war
  ```

- On both idmhost1 and idmhost2 - Create a symbolic link to the analyticRes directory in the <OBIEE_INSTANCE>/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/analyticsRes directory

  Example:

  ```
  $ ln -s
  /vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/analyticsRes
  ```

- Validate its creation

  Example:

  ```
  $ ls -ltr
  ```

  Output:

  ```
  total 28
  -rw-r-----  1 webadmin dba   69 Apr 15  2015 default.jsp
  drwxr----- 14 webadmin dba 4096 Apr 15  2015 res
  drwxr-----  5 webadmin dba 4096 Apr 15  2015 workspace
  drwxr-----  3 webadmin dba 4096 Apr 15  2015 WEB-INF
  drwxr----- 31 webadmin dba 4096 Apr 15  2015 olh
  drwxr-----  2 webadmin dba 4096 Apr 15  2015 META-INF
  lrwxrwxrwx  1 webadmin dba  152 May  5 11:33 analyticsRes ->
  /vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/analyticsRes
  ```

Prepare the Operational Insights Environment for Oracle BIEE Presentation Services Connection

The Operational Insights environment has to be prepared for the Oracle BI EE Presentation Services connection. The Oracle BI EE Presentation Services connection

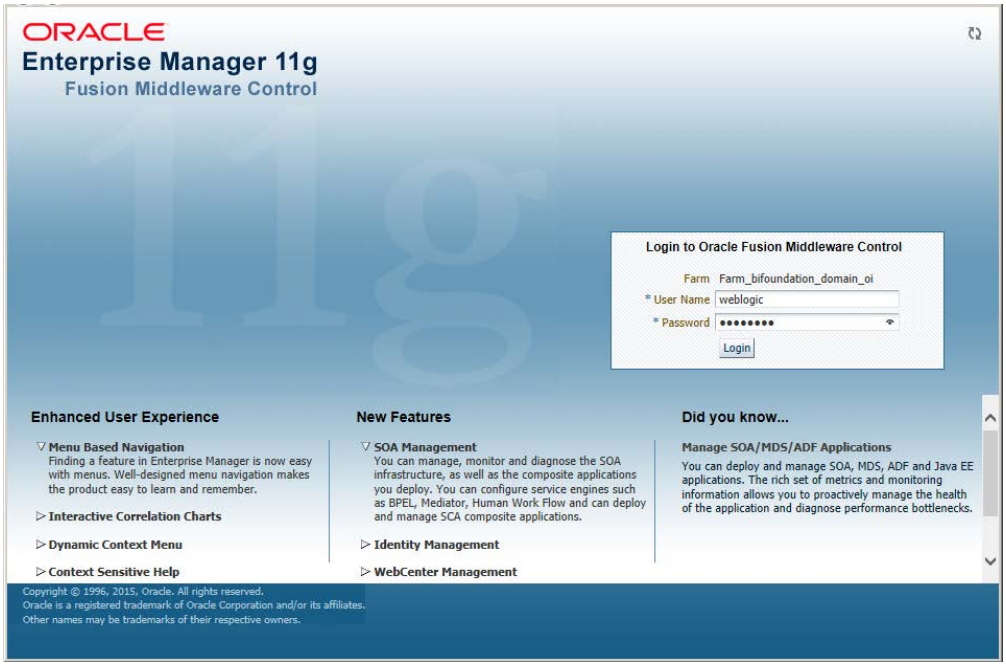
requires a BIImpersonateUser to be created on the Oracle BI EE with the permission to impersonate the logged in user. Perform the following steps to do so.

> **NOTE**: Refer to the section 'Credentials for Connecting to the Oracle BI Presentation Catalog' of the Fusion Middleware Developer's Guide for Oracle Business Intelligence Enterprise Edition for any clarifications needed.

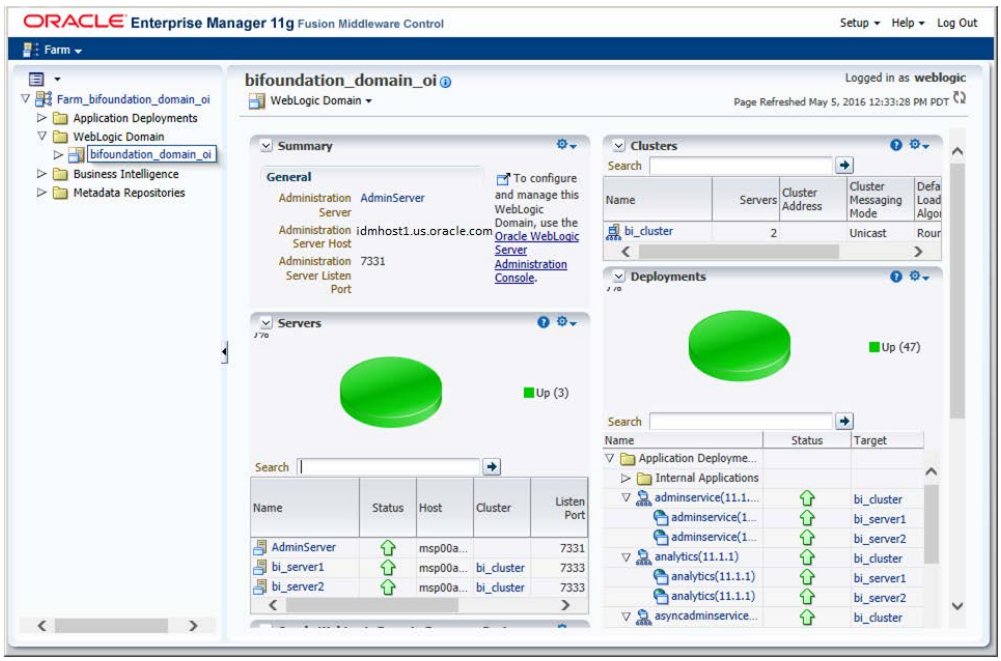
(http://docs.oracle.com/cd/E28280_01/bi.1111/e10545/embedding_adf.htm#BIEDV1028)

> **NOTE**: The instructions in the document listed above indicate to create the BIImpersonateUser in OID. That has already happened during earlier steps in this document at the time of running LDIF scripts, so there is no need to do that now.

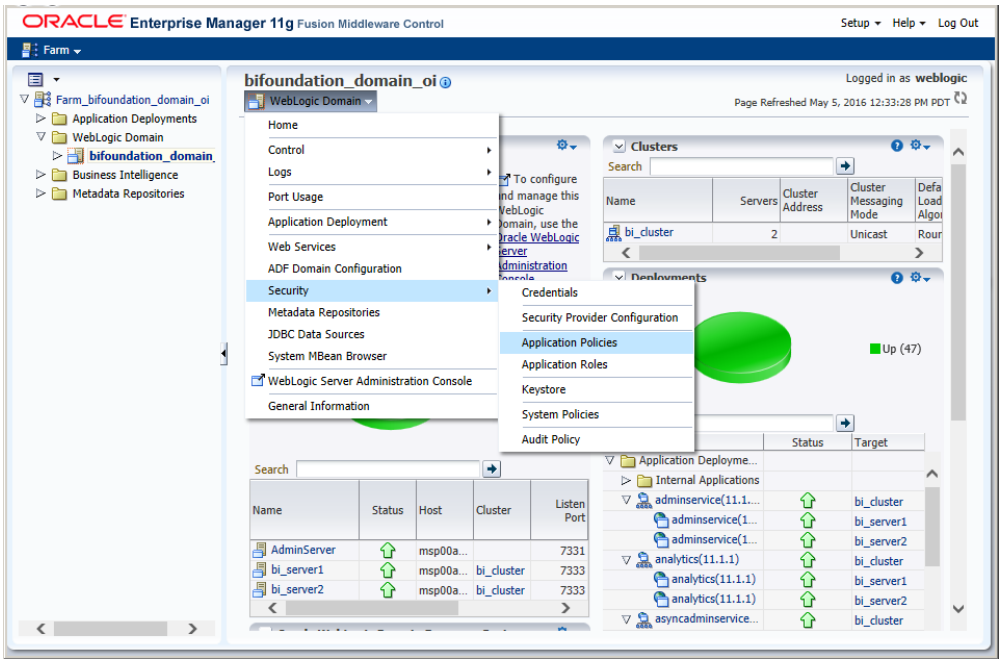
- Login to the Enterprise Manager for OBIEE.



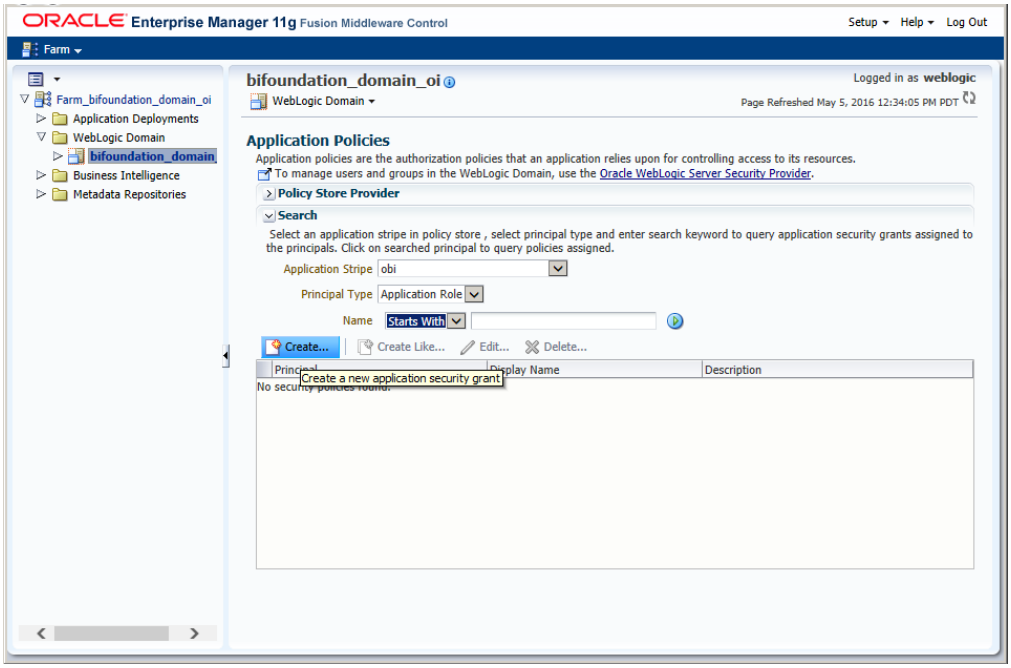
- From the left pane, click **WebLogic Domain > bifoundation_domain_oi**.



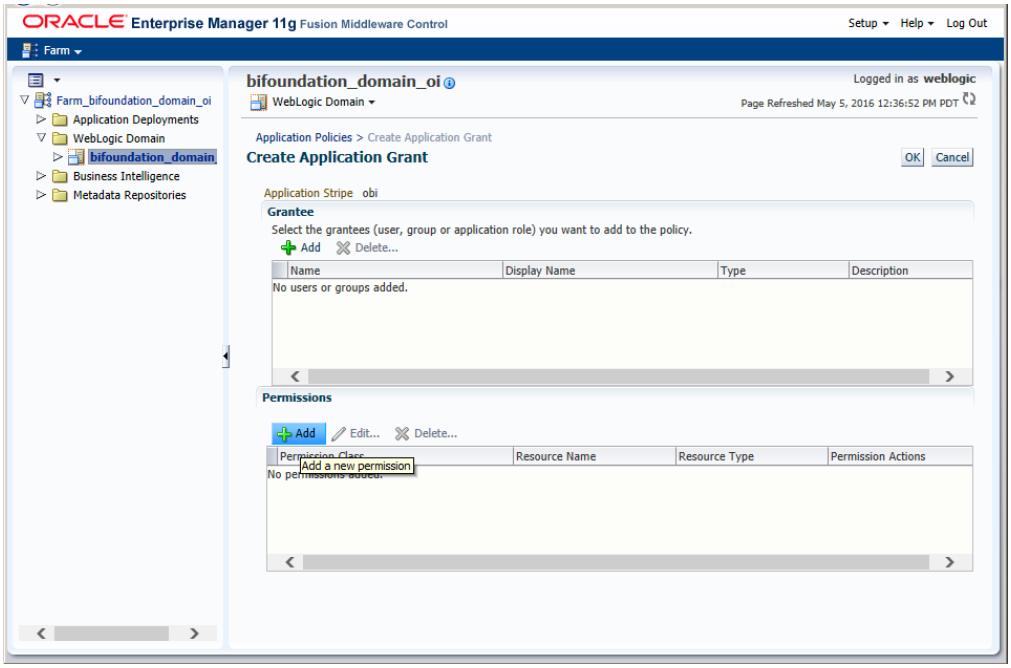
- Click the **Weblogic Domain** drop-down list, and select **Navigate Security > Application Policies**.



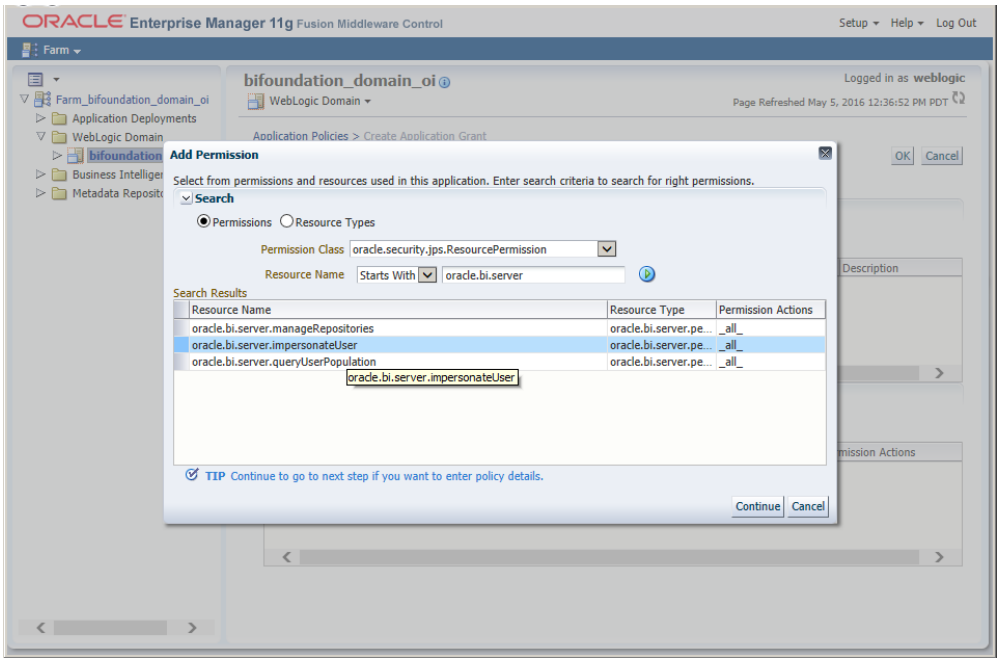
- From the Application Stripe drop down menu, select **obi**, and click **Create**.



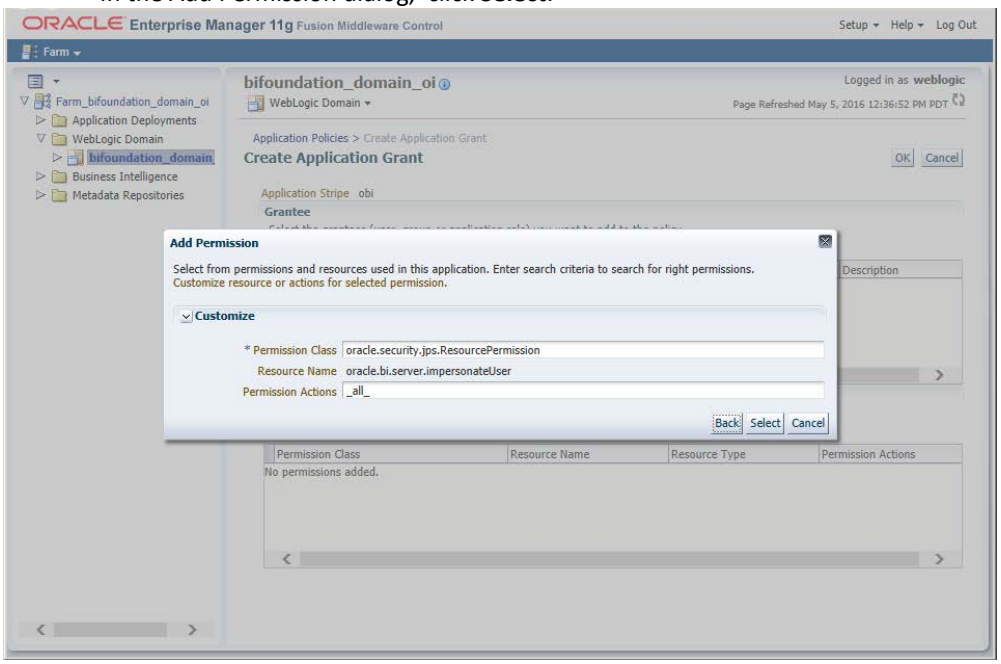
- The Add Permission window opens. In the Permission Class section click **Add**.



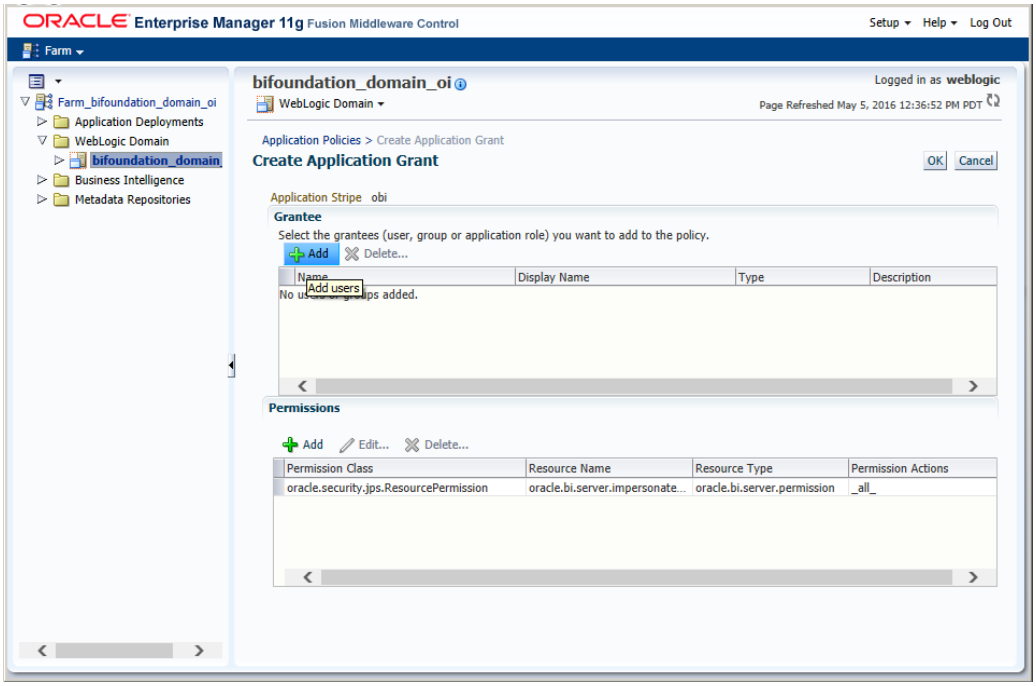
- The Add Permission dialog opens.
  - In the Permission Class field, select **oracle.security.jps.ResourcePermission**.
  - In the Resource Name field, select **oracle.bi.server.impersonateUser**.
  - Click **Continue**.



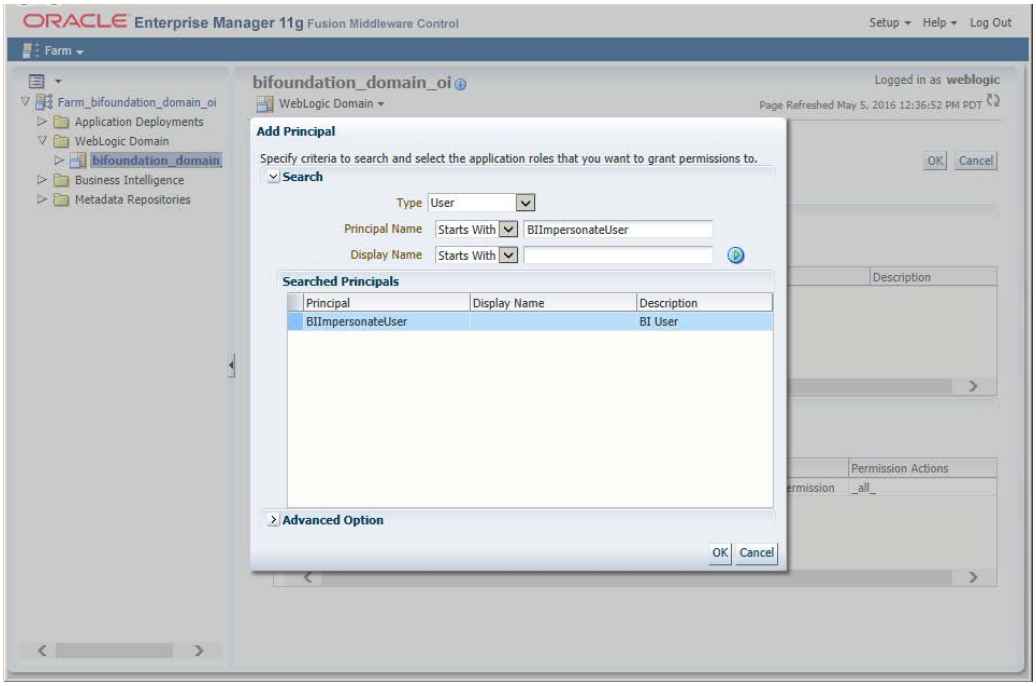
- In the Add Permission dialog, click **Select**.



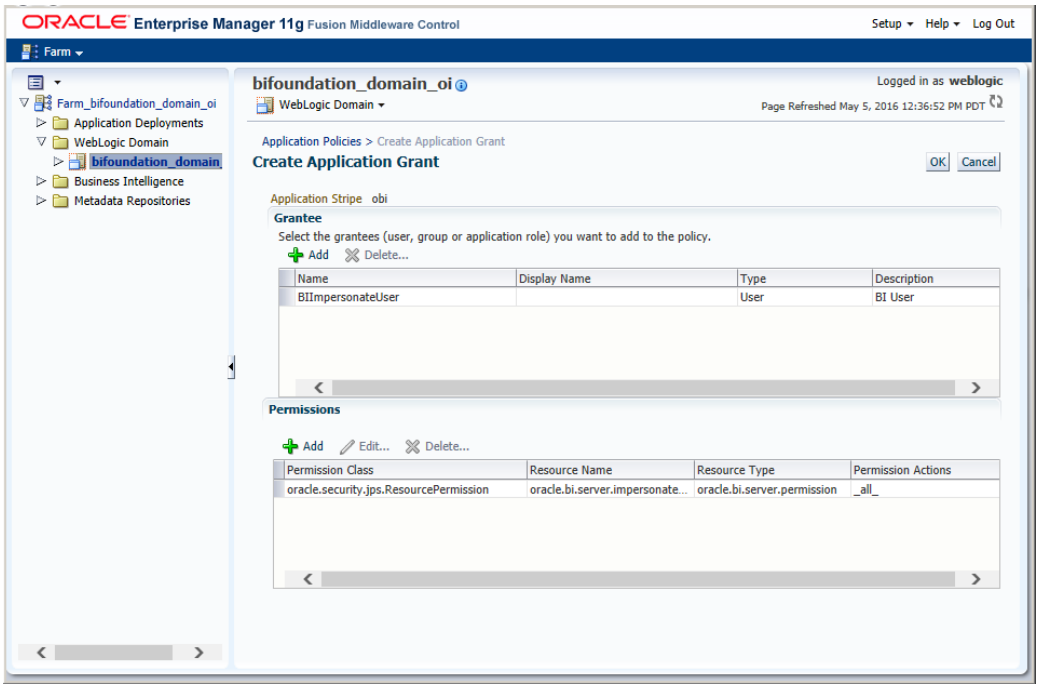
- In the Grantee section of the window, click the **Add** button.



- In the Add Principal screen select **BIImpersonateUser,** and click **OK**.



- Notice that the BIImpersonateUser as a Grantee and the oracle.security.jps.ResourcePermission are listed in the Permissions section.



- Bounce OBIEE WLS Server and opmn processes.

Single Sign-On Configuration for Oracle BI EE

When the Oracle BI EE is configured to use Single Sign-On using the Oracle Access Manager and the Oracle Web Tier then the following steps should be followed to enable the Operation Insights custom skins and styles.

First make the Oracle BIEE static resources available to the Oracle Web Tier. Since the Oracle Web Tier is installed on the same machine where the Oracle BI EE is installed - the steps below should be performed to make the Oracle BI EE static resources and the Operational Insights skins and styles available to the Oracle Web Tier.

> **NOTE**: In installations where Web Tier is installed on separate host – Look to REIM, Allocations, or ReSA installation guides for proper configuration.

- On both idmhost1 and idmhost2 navigate to the Oracle Web Tier installation which has been configured with the current Operational Insights environment for Single Sign-On.
  <WEB_TIER_ORACLE_HOME>/Oracle_WT1/instances/<INSTANCE_NAME>/config/OHS/ohs1/htdocs

  Examples:

  idmhost1:

  ```
  $ cd
  /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1/config/OHS/ohs1/htdocs
  ```

  idmhost2:

```
$ cd
/u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance2/config/OHS/ohs2/
htdocs
```

- Create symbolic links to the analyticsRes directory in the OBIEE instance deployment locations on idmhost1 and idmhost2.

  Examples:

  idmhost1:

  ```
  $ ln -s
  /vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/bifounda
  tion/OracleBIPresentationServicesComponent/coreapplication_obips1/analytic
  sRes

  $ ln -s
  /u00/webadmin/config/domains/wls_obiee_oi/bifoundation_domain_oi/servers/b
  i_server1/tmp/_WL_user/analytics_11.1.1/7dezjl/war/res
  ```

  idmhost2:

  ```
  $ ln -s
  /vol.rtk/projects/ha_15/products/wls_obiee_oi/instances/instance1/bifounda
  tion/OracleBIPresentationServicesComponent/coreapplication_obips1/analytic
  sRes

  $ ln -s
  /u00/webadmin/config/domains/wls_obiee_oi/bifoundation_domain_oi/servers/b
  i_server2/tmp/_WL_user/analytics_11.1.1/sc09uk/war/res
  ```

2. Verify that you can list these new directories.

   ```
   $ ls res
   $ ls analyticsRes
   ```

3. Restart the Oracle Web Tier.

Configure Alias for Static Resources in Web Tier for OBIEE

For the resources in the 'res' directory to be available from Oracle Web Tier we need to configure alias in the Oracle Web Tier. Perform follow the following steps to configure the alias.

- Stop Oracle Web Tier on both idmhost1 and idmhost2.
- On idmhost1: Navigate to the directory <WEBTIER_INSTANCE>/config/OHS/ohs1.

  Example:

  ```
  $ cd
  /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1/config/OHS/o
  hs1
  ```

- On idmhost2: Navigate to the directory <WEBTIER_INSTANCE>/config/OHS/ohs2.

  Example:

  ```
  $ cd
  /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance2/config/OHS/o
  hs2
  ```

- On idmhost1 and idmhost2 - Create a new file called alias.conf in the directory with the following contents:

  Example:

  ```
  Alias /res/v-UBtil9ur9Q4/
  "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/htdocs/res/
  "
  ```

```
Alias /res/v-ISAcoW1LJVY/
"${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/htdocs/res/
"
<Directory
"${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/htdocs/res"
>
AllowOverride None
Order allow,deny
Allow from all
</Directory>
```

- In the same directory on idmhost1 and idmhost2: Update the httpd.conf file and include the recently created file alias.conf at the end.

  Examples:

  idmhost1:

  ```
  Include
  "/u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1/config/OHS/
  ohs1/alias.conf"
  ```

  Idmhost2:

  ```
  Include
  "/u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance2/config/OHS/
  ohs2/alias.conf"
  ```

Update Oracle Web Tier for OBIEE and OAM Redirects

In order for SSO to work with OAM and have URL's that are comprised of load balanced virtual hosts and aliases – the Oracle Web Tier will need to be configured to to properly redirect incoming requests to the correct WebLogic servers. In addition to that - If the analyticRes directory has already been configured to be redirected, the analyticRes redirection entry will need to be removed.

- Navigate to the mod_wl_ohs.conf on idmhost1 and idmhost2 and edit the file.

  Examples:

  idmhost1:

  ```
  $ cd
  /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1/config/OHS/o
  hs1
  ```

  idmhost2:

  ```
  $ cd
  /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance2/config/OHS/o
  hs2
  ```

- Update mod_wl_ohs.conf to redirect the following context roots to corresponding WebLogic servers:
  - /oamconsole – This is for OAM administration.
  - /oam – This is for application SSO Logon.
  - /analytics – This is for Operational Insights.
  - /xmlpserver – This is for BI Publisher reports.
  - /If it is configured to redirect the /analyticsres to the WebLogic server – delete the entry.

– When finished it should look like below the example below.

Example:

```
<Location /oamconsole>
 WebLogicHost msp00acz.us.oracle.com
 WebLogicPort 16001
 SetHandler weblogic-handler
</Location>

<Location /oam>
 WebLogicCluster
msp00acz.us.oracle.com:16007,msp00ada.us.oracle.com:16007
 SetHandler weblogic-handler
 WLCookieName oamjsessionid
</Location>

<Location /oam/server/logout>
 WebLogicCluster
msp00acz.us.oracle.com:16007,msp00ada.us.oracle.com:16007
 SetHandler weblogic-handler
</Location>


<Location /analytics>
 WebLogicHost msp00acz.us.oracle.com:7331
 WebLogicCluster
msp00acz.us.oracle.com:7333,msp00ada.us.oracle.com:7333
 Idempotent OFF
 SetHandler weblogic-handler
 ErrorPage downtime.html
</Location>

<Location /xmlpserver>
 WebLogicHost msp00acz.us.oracle.com:7331
 WebLogicCluster
msp00acz.us.oracle.com:7333,msp00ada.us.oracle.com:7333
 Idempotent OFF
 SetHandler weblogic-handler
 ErrorPage downtime.html
</Location>

# <Location /weblogic>
#      SetHandler weblogic-handler
#      PathTrim /weblogic
#      ErrorPage  http:/WEBLOGIC_HOME:WEBLOGIC_PORT/
#  </Location>
```

NOTE: After this point you should be able to access the OAM and BI Publisher application SSO URL's after bouncing Oracle Web Tier. Verfication steps for this are placed in this document to occur after the configuration for analytics is complete.

Make the Static Resources Publicly Available

The static resources are images, css and javascripts. These resources can be made publicly available. Perform the steps below to make them publicly available.

- Navigate to the webgate.conf on idmhost1 and idmhost2, and edit the file.

  Examples:

  idmhost1:

```
$ cd
/u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1/config/OHS/o
hs1
```

idmhost2:

```
$ cd
/u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance2/config/OHS/o
hs2
```

- Inside the file webgate.conf, you will see the following lines: (These lines instruct the Oracle Web Tier to route any request to the Oracle Access Manager for authentication)

  Example:

  ```
  <LocationMatch "/*">
  AuthType Oblix
  require valid-user
  </LocationMatch>
  ```

- Add the following lines after the above lines. (This means for any request under the /analyticsRes or /res context roots, we do not want to route to Oracle Access Manager for authentication. The resources under these context roots can be served to users without any authentication.)

  Example:

  ```
  <LocationMatch "/analyticsRes/*">
  Satisfy any
  </LocationMatch>
  <LocationMatch "/res/*">
  Satisfy any
  </LocationMatch>
  ```

Enable Caching and Compression of the Oracle BI EE Static Resources

The Oracle BI EE static resources like css and javascripts can be compressed by the Oracle Web Tier to optimize the Oracle BI EE performance. We will use the mod_expire and mod_deflate modules of the Oracle Web Tier to enable the browser caching and compression of the Oracle BI EE static resources.

The mod_expire module controls the setting of the Expires HTTP header and the max-age directive of the Cache-Control HTTP header in server responses. These HTTP headers are an instruction to the browser about the document's validity and persistence. If cached, the document may be fetched from the cache rather than from the source until this time has passed. After that, the cache copy is considered expired and invalid, and a new copy must be obtained from the source. The mod_deflate module provides the DEFLATE output filter that allows output from the Oracle Web Tier to be compressed before being sent to the client over the network.

Perform the following steps to enable the browser caching of the Oracle BI EE static resources.

- Navigate to the httpd.conf on idmhost1 and idmhost2 and edit the file

  Examples:

  idmhost1:

  ```
  $ cd
  /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1/config/OHS/o
  hs1
  ```

idmhost2:

```
$ cd
/u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance2/config/OHS/o
hs2
```

- Verify that the following line has been uncommented.

  Example:

  ```
  LoadModule expires_module "${ORACLE_HOME}/ohs/modules/mod_expires.so"
  ```

- Go to the end of the file httpd.conf and add the following line:

  Example:

  ```
  include
  "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/expire.conf
  "
  ```

- In the same location create a new file called expire.conf and add the following:

  Example:

  ```
  <IfModule mod_expires.c>
  ExpiresActive On
  ExpiresByType image/jpg "access plus 60 days"
  ExpiresByType image/png "access plus 60 days"
  ExpiresByType image/gif "access plus 60 days"
  ExpiresByType image/jpeg "access plus 60 days"
  ExpiresByType text/css "access plus 1 days"
  ExpiresByType image/x-icon "access plus 1 month"
  ExpiresByType application/pdf "access plus 1 month"
  ExpiresByType audio/x-wav "access plus 1 month"
  ExpiresByType audio/mpeg "access plus 1 month"
  ExpiresByType video/mpeg "access plus 1 month"
  ExpiresByType video/mp4 "access plus 1 month"
  ExpiresByType video/quicktime "access plus 1 month"
  ExpiresByType video/x-ms-wmv "access plus 1 month"
  ExpiresByType application/x-shockwave-flash "access 1 month"
  ExpiresByType text/javascript "access plus 1 week"
  ExpiresByType application/x-javascript "access plus 1 week"
  ExpiresByType application/javascript "access plus 1 week"
  </IfModule>
  ```

Complete the following steps to enable compression of the Oracle BI EE static resources in the Oracle Web Tier.

- Navigate to the httpd.conf on idmhost1 and idmhost2 and edit the file.

  Examples:

  idmhost1:

  ```
  $ cd
  /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance1/config/OHS/o
  hs1
  ```

  idmhost2:

  ```
  $ cd
  /u00/webadmin/products/wls_ohs/Oracle_WT1/instances/instance2/config/OHS/o
  hs2
  ```

- Verify that the following line has been uncommented. If the line does not exist then add it.

Example:

```
LoadModule deflate_module "${ORACLE_HOME}/ohs/modules/mod_deflate.so"
```

- Go to the end of the file httpd.conf and add the following line:

  Example:

```
include
"${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/deflate.con
f"
```

- In the same location create a new file called deflate.conf and add the following:

  Example:

```
<IfModule mod_deflate.c>
AddOutputFilterByType DEFLATE text/plain
AddOutputFilterByType DEFLATE text/html
AddOutputFilterByType DEFLATE text/xml
AddOutputFilterByType DEFLATE text/css
AddOutputFilterByType DEFLATE text/javascript
AddOutputFilterByType DEFLATE image/svg+xml
AddOutputFilterByType DEFLATE image/x-icon
AddOutputFilterByType DEFLATE application/xml
AddOutputFilterByType DEFLATE application/xhtml+xml
AddOutputFilterByType DEFLATE application/rss+xml
AddOutputFilterByType DEFLATE application/javascript
AddOutputFilterByType DEFLATE application/x-javascript
DeflateCompressionLevel 9
# Browser specific settings
BrowserMatch ^Mozilla/4 gzip-only-text/html
BrowserMatch ^Mozilla/4\.0[678] no-gzip
BrowserMatch \bMSIE !no-gzip !gzip-only-text/html
BrowserMatch \bOpera !no-gzip
# Setup custom deflate log
DeflateFilterNote Input instream
DeflateFilterNote Output outstream
DeflateFilterNote Ratio ratio
LogFormat '"%r" %{outstream}n/%{instream}n (%{ratio}n%%)' deflate
# Example of log file
CustomLog logs/deflate_log DEFLATE
</IfModule>
```

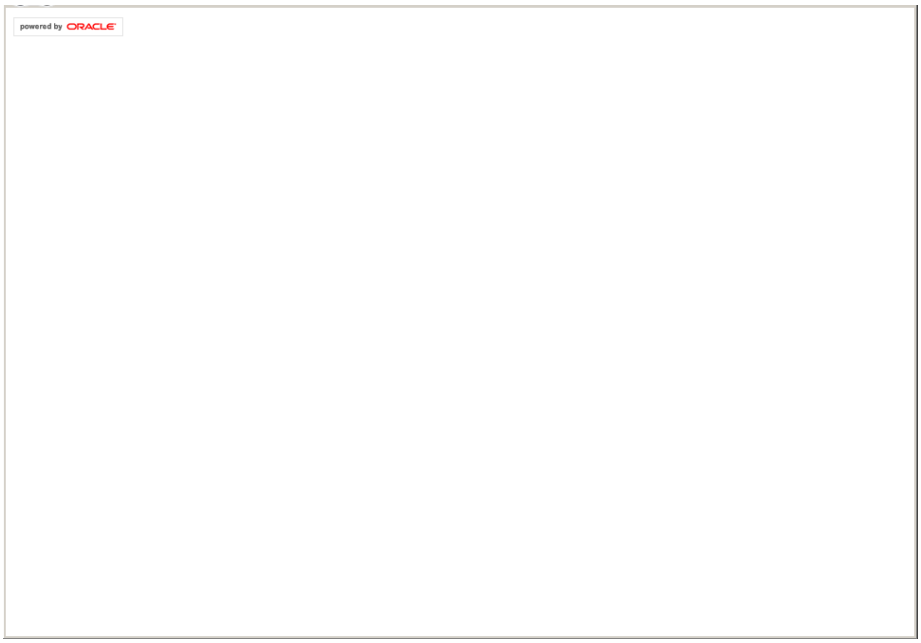
- Once the above steps are completed, restart the Oracle Web Tier.

Verification – Verify the Static Resources using the Oracle Web

Verify that you can access the following URLs using the Oracle Web Tier host and port. If the Oracle Web Tier port has not been changed during installation then the default port is 7777.

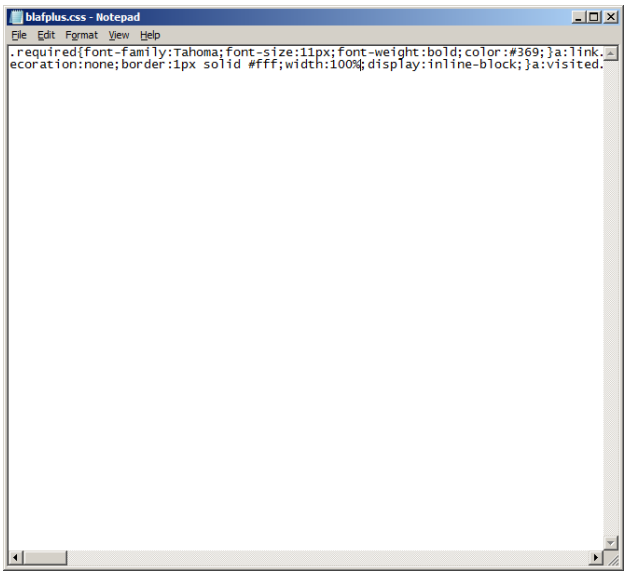
- Clear your browser cache.

http://idmhost-vip.us.oracle.com.us.oracle.com:7777/res/siebelbug.gif



http://idmhost-vip.us.oracle.com:7777/analyticsRes/s_skyros_custom/answers/database.png

http://idmhost-vip.us.oracle.com:7777/res/s_blafp/uicomponents/blafplus.css



- Go to the directory <WEB_TIER_HOME>/Oracle_WT1/instances/instance1/diagnostics/logs/OHS/ohs1. This directory will have a log file called deflate_log. View it and you will notice that the css file blafplus.css was served using compression.

  Example:

  ```
  "GET /res/s_blafp/uicomponents/blafplus.css HTTP/1.1" 493/1402 (35%)
  ```

Configure for In-Context launches of RMS forms

- To configure the In-Context launches of RMS forms - Add the below configuration in ActionFrameworkConfig.xml file located at <OBIEE_DOMAIN>/config/fmwconfig/biinstances/coreapplication.

  Example:

  ```
  /u00/webadmin/config/domains/wls_obiee_oi/bifoundation_domain_oi/config/fm
  wconfig/biinstances/coreapplication
  ```

- For idmhost1 - Place the following lines above the </aliases> line of code.

  Example:

  ```
  <aliases>
    <location-alias>
    <alias>rmshost</alias>
    <actual>http://msp00acs.us.oracle.com:7123</actual>
    </location-alias>
  ```

- For idmhost2 - Place the following lines above the </aliases> line of code.

  Example:

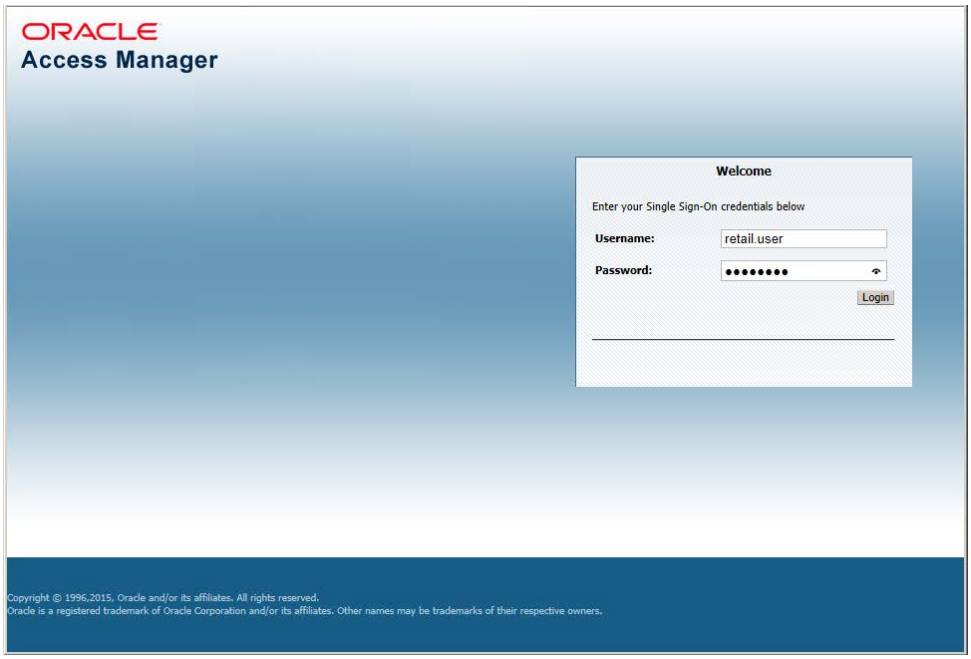
  ```
  <aliases>
    <location-alias>
    <alias>rmshost</alias>
    <actual>http://msp00acf.us.oracle.com:7123</actual>
    </location-alias>
  ```

> **NOTE**: RPD already configured in previous steps for In-Context launches of RMS forms.
>
> When finished – stop and restart the WebLogic admin and managed servers, as well as the opmn processes for OBIEE.

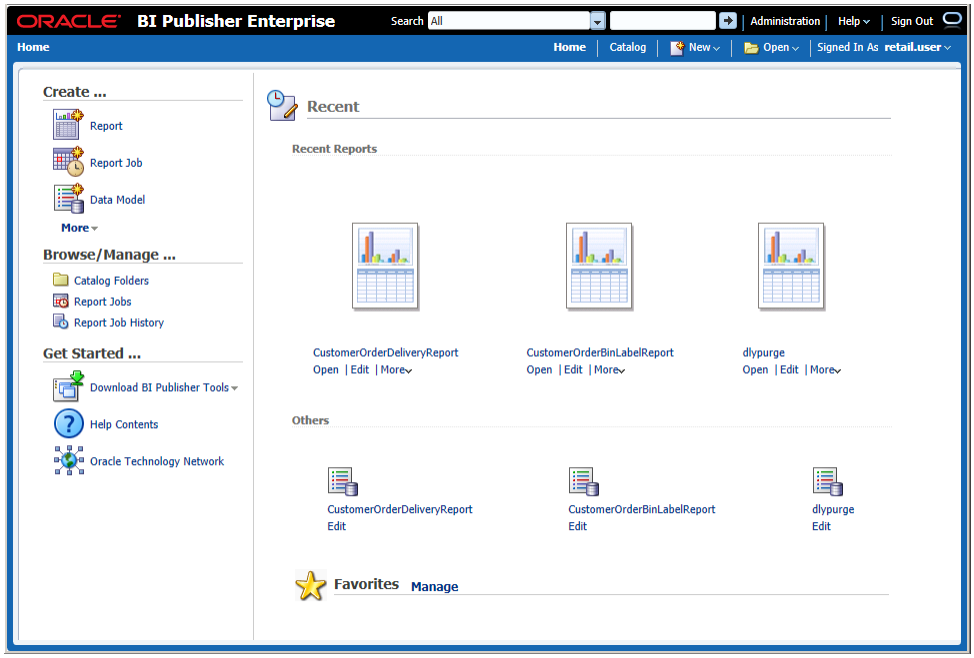
Verification – Validate BI Publisher Reports SSO Configuration

BI Publisher reports should be validated for utilizing non-SSO URL after the BI Publisher configuration is completed. In this section, you will learn to validate using SSO user credentials after being redirected from Oracle Web Tier .

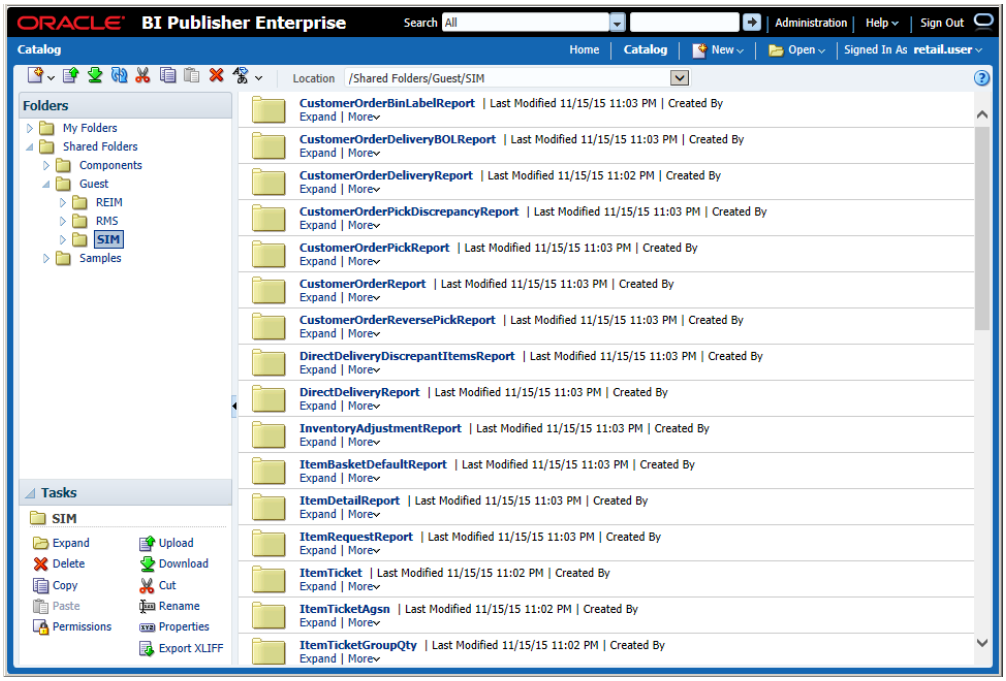
1. Log into BI Publisher using virtual host and alias. (http://idmhost-vip.us.oracle.com:7777/xmlpserver). The user id to login with is retail.user – which was created during the steps to add users to OID and was setup for OBIEE during those steps.



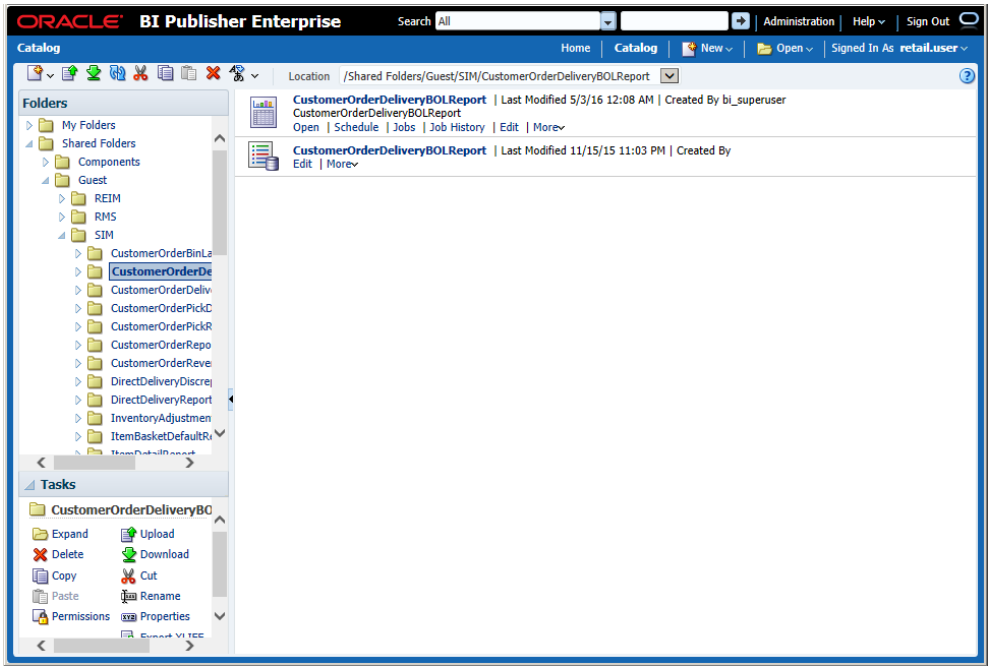
2. Click the Catalog link located at the top of the window.



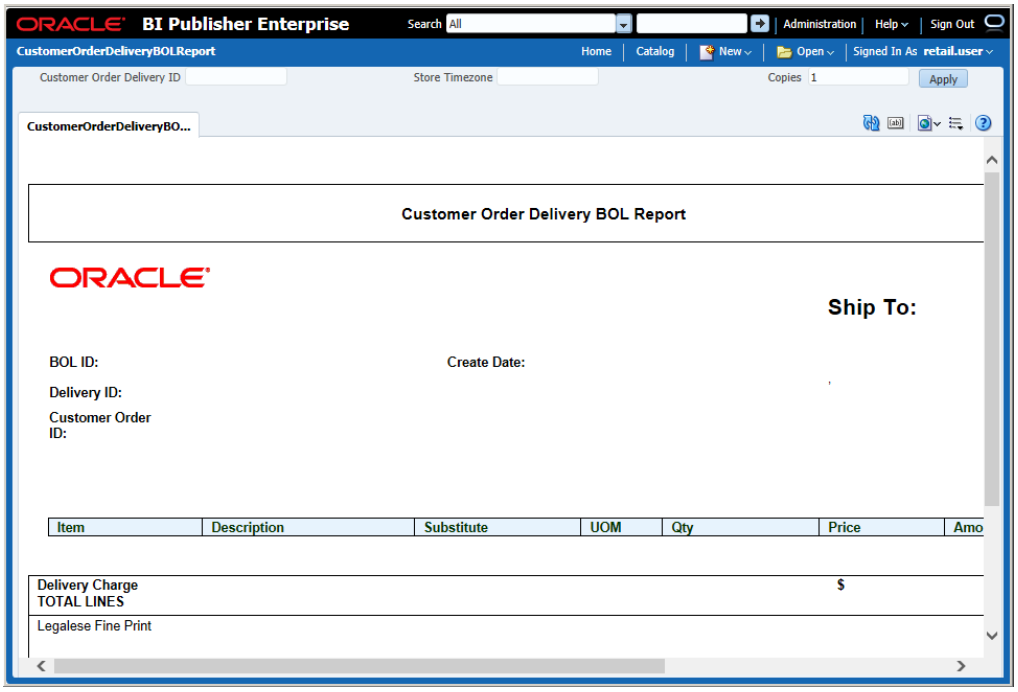
3. From the left pane, click **SIM**.



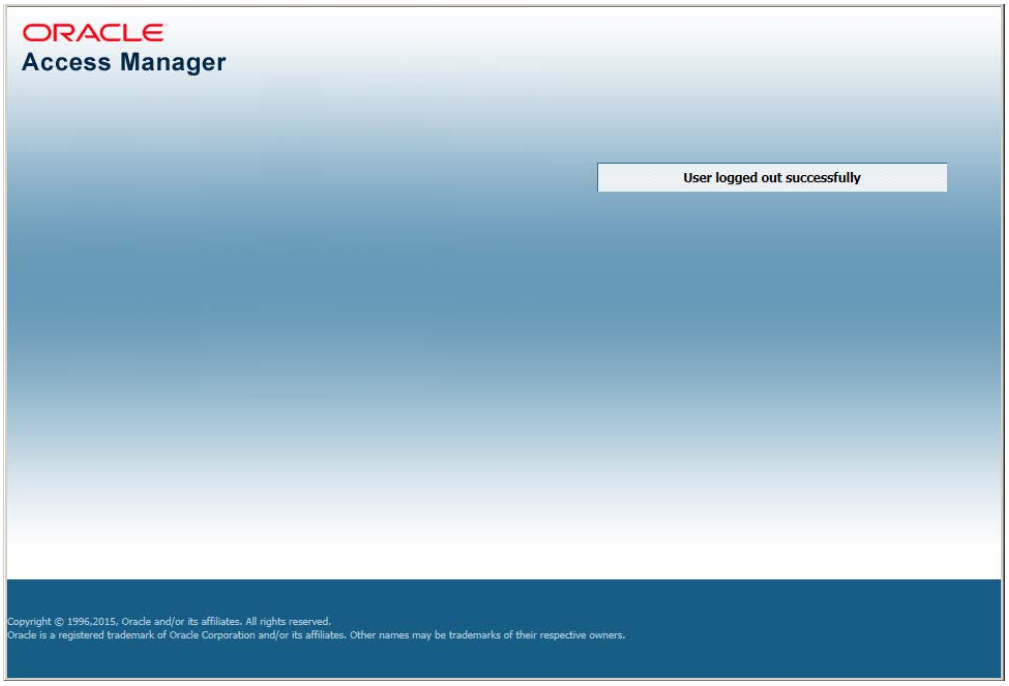
4. Click the **CustomerOrderDeliveryBOLReport** link.



5. The Customer Order delivery BOL Report is displayed as shown below. Click **Logout** in upper right-hand corner of screen.



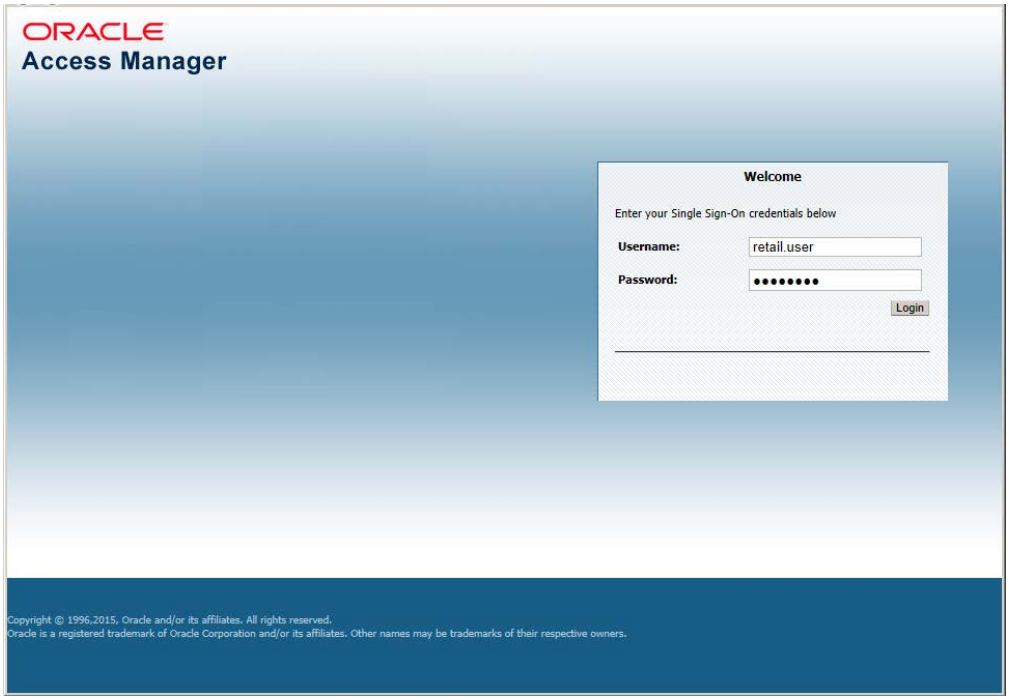
6. The OAM Logout window opens and user is logged out of application.



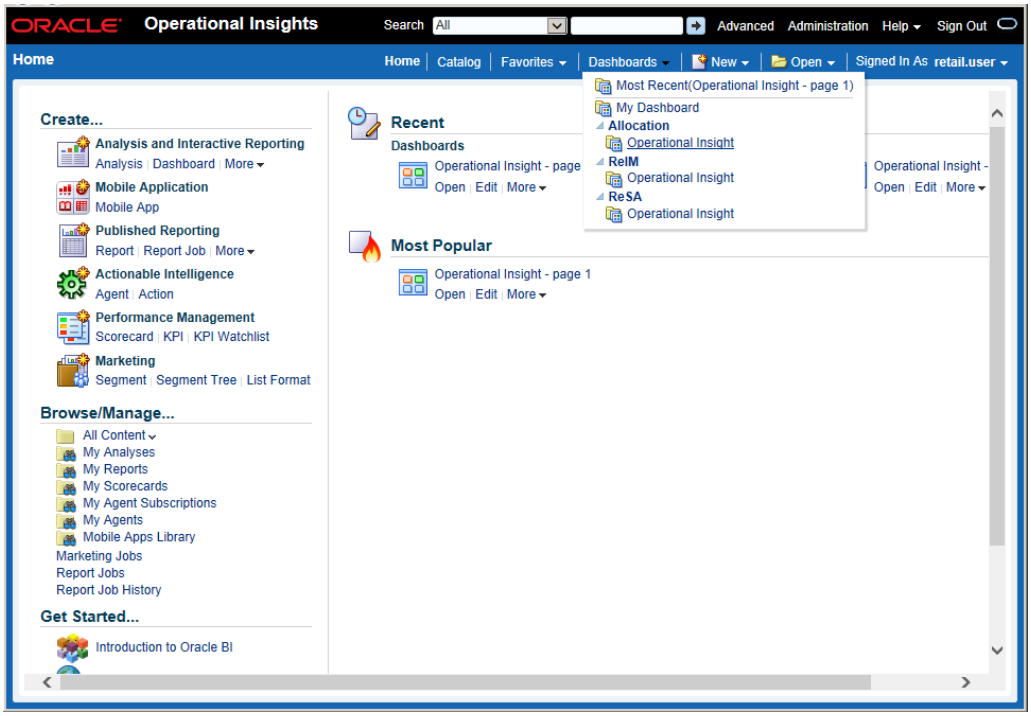
Verification – Verify OBIEE analytics is Accessible via Web Tier using Application Specific Credentials

Oracle BI EE Analytics should be able to login with RESA/REIM/ALLOC application user and able to view dashboard as well.

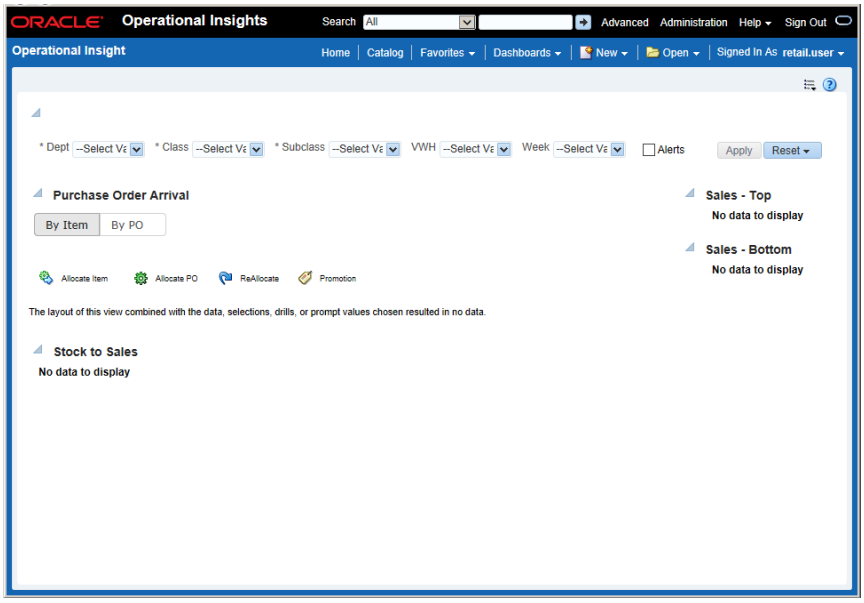
- Launch Operational Insights with clustered URL and OHS port and login to the application using an application user.
  (http://idmhost-vip.us.oracle.com:7777/analytics)



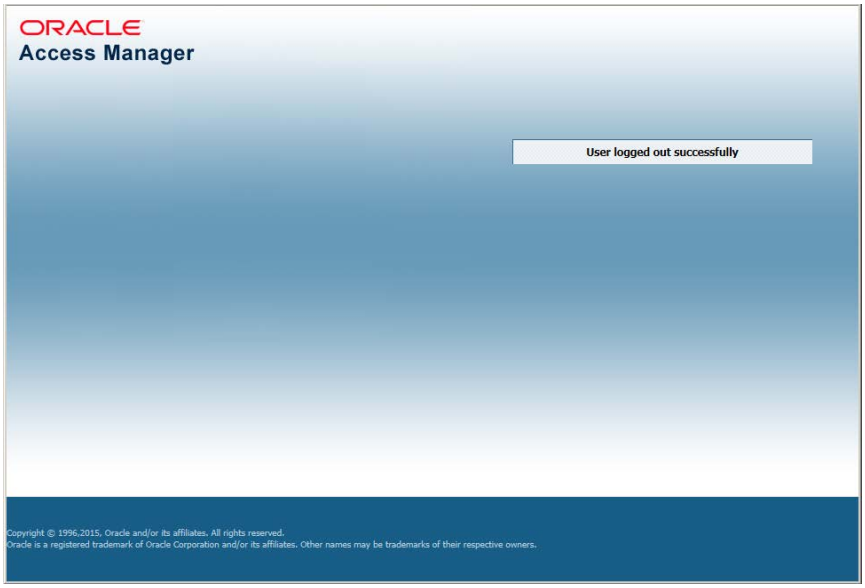
- On the home page of Analytics, click **Dashboards > Operational Insight**.



- Verify that there are no visible errors on the screen. Click Sign Out in the upper right hand corner of screen.



- The OAM Logout window opens and user is logged out of the application.

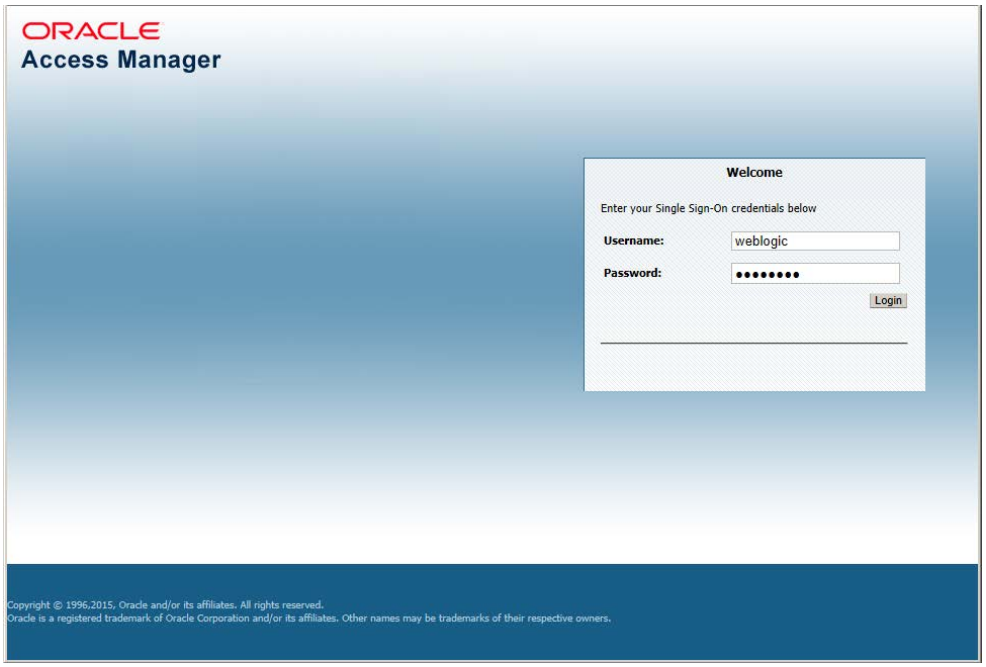


Verification – Verify OAMConsole is Accessible via Web Tier using SSO Login

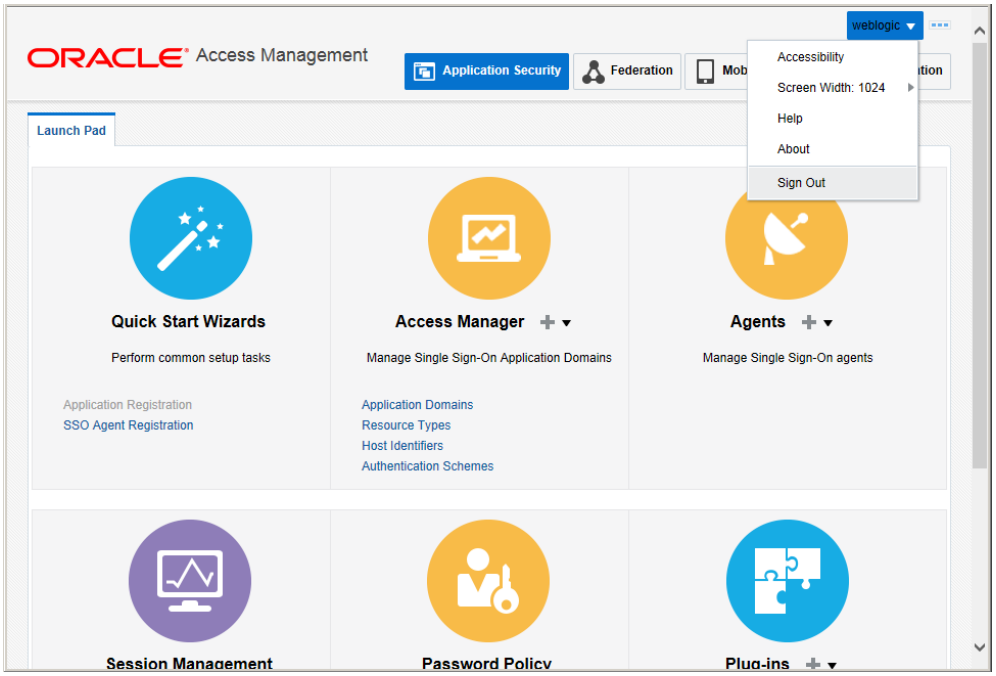
The purpose of this screen is to validate that OAM is accessible via virtual host and alias by accessing OAM console.

- Launch Oracle Access management with clustered URL and OHS port. Login to the application using the weblogic admin user that was created in OID. (weblogic)

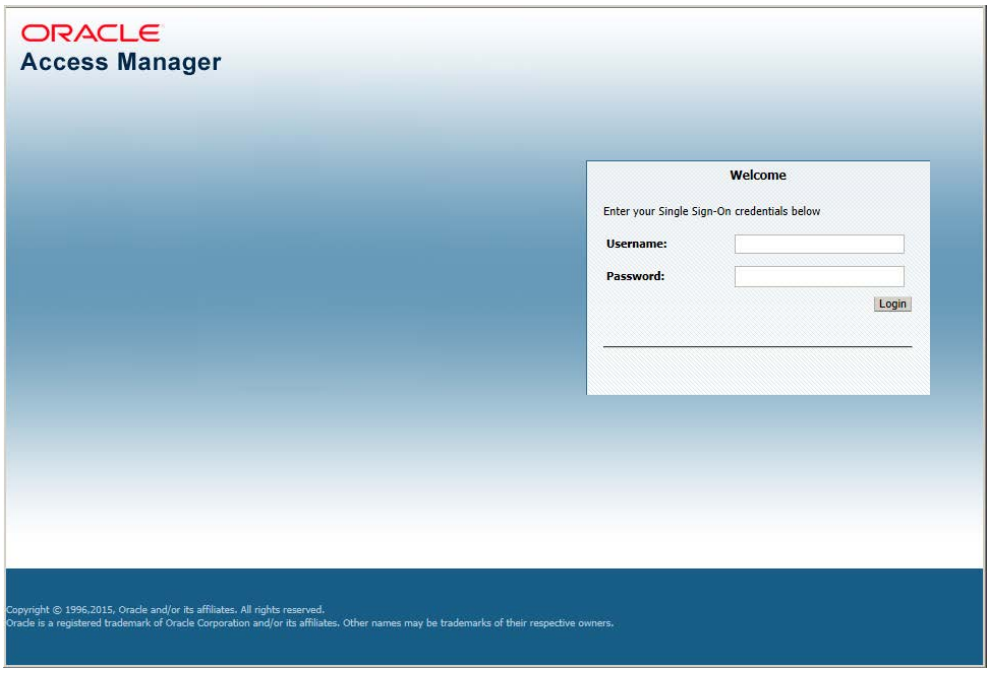
  (http://msp00acz-ada-vip.us.oracle.com:7777/oamconsole)



- The Access Management window opens. Select **Sign Out** from the dropdown menu in the upper right hand corner of window.



- The OAM Sign-on window opens.


ORACLE
Access Manager
Welcome
Enter your Single Sign-On credentials below
Username:
Password:
Login
Copyright © 1996,2015, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

A

Appendix: Creating Static Ports for OID

```
##################################################################################
#####
#This file is a template file for staticports.ini
#This file must be edited to provide the ports which required to be set
#Those ports which are not provided explicitly in this file will be assigned
automatically
#Note:  Please keep in mind to uncomment the rows of the port numbers of your
choice in order
#to use that port.
##################################################################################
#####


#########################Begin section for Domain ################################
#This port number is not required if you are using a extend existing domain
scenario
##################################################################################
####

[DOMAIN]

#This port indicates the Domain port number
Domain Port No = 15001
Node Manager Port No = 5560

#########################Begin section for ovd1 ##################################
#This port numbers will be considered only if OVD is selected for configuration
##################################################################################
#####

[OVD]

#The HTTP Admin port for OVD
#Oracle Virtual Directory Port No for HTTP Admin = 8899

#The SSL LDAP port for OVD
#Oracle Virtual Directory (SSL) Port No for LDAP = 6052

#The Non-SSL LDAP port for OVD
#Oracle Virtual Directory (Non-SSL) Port No for LDAP = 6051

#The HTTP Web Gateway port for OVD
#Oracle Virtual Directory Port No for HTTP Web Gateway = 2223


#########################Begin section for oid1 ##################################
#This port numbers will be considered only if OID is selected for configuration
##################################################################################
#####

[OID]

#The Non-SSL port for OID
Oracle Internet Directory Port No = 3060
```

```
#The SSL port for OID
Oracle Internet Directory (SSL) Port No = 3061


#######################Begin section for emAgent ################################
#This port numbers will be considered only if EM is selected for configuration
##########################################################################################

[EMAGENT]

#The port for EM Agent port
#Oracle EM Agent Port No = 5162

#######################Begin section for oif ################################
#This port numbers will be considered only if OIF is selected for configuration
##########################################################################################

[OIF]

#The port for OIF Server port
#OIF Server Port No = 7499

#######################Begin section for ods ################################
#This port numbers will be considered if ODSM or DIP or both are selected for configuration
##########################################################################################

[ODS]

#The port for ODSM Server port
ODS Server Port No = 15003

#######################Begin section for ohs1 ################################
#This port numbers will be considered only if OHS is selected for configuration
##########################################################################################

[OHS]

#The Proxy Port For OHS
#Oracle Http Server Proxy Port No = 7015

#The Listen Port For OHS
#Oracle Http Server Administrator Port No = 7016


#The SSL Port For OHS
#Oracle Http Server SSL Port No = 7017


#######################Begin section for opmn ################################
#This port numbers will be considered for OPMN configuration
##########################################################################################

[OPMN]

#The  Local port for OPMN
#OPMN Local Port No = 6800

#The Remote port for OPMN
#OPMN Remote Port No = 6801

#The Request port for OPMN
#OPMN Request Port No = 6802
```

B

Appendix: A Summary of Installing the Oracle Internet Directory (idmhost1)

```
Type: Configure Only
    Middleware Home Location : /u00/webadmin/products/wls_idm
    Oracle Instance Location : /u00/webadmin/products/wls_idm/oidinst_1
    Oracle Instance : oidinst_1
    Domain Option : Create Domain
    Domain Name : IDMDomain
    Domain Home : /u00/webadmin/products/wls_idm/user_projects/domains/IDMDomain
    Domain Host Name : idmhost1.us.oracle.com
    Domain Port : 15001
    Weblogic Console : http://idmhost1.us.oracle.com:15001/console
    Weblogic User Name : weblogic
    Automatic Port Detection : false
    Enterprise Manager :
        http://idmhost1.us.oracle.com:15001/em
    Enterprise Manager Agent
        http://idmhost1.us.oracle.com:5162/emd/main
    Oracle Internet Directory
        SSL Port : 3061
        Non SSL Port : 3060
        Database : dbhost1:1521^dbhost2:1521@idmservicename
    Oracle Directory Services Manager :
        http://idmhost1.us.oracle.com:15003/odsm/faces/odsm.jspx
```

C

Appendix: A Summary of Installing the Oracle Internet Directory (idmhost2)

```
Type: Configure Only
        Middleware Home Location : /u00/webadmin/products/wls_idm
        Oracle Instance Location : /u00/webadmin/products/wls_idm/oidinst_2
        Oracle Instance : oidinst_2
        Domain Option : Expand Cluster
        Domain Host Name : idmhost1.us.oracle.com
        Domain Port : 15001
        Weblogic Console : http://idmhost1.us.oracle.com:15001/console
        Weblogic User Name : weblogic
        Automatic Port Detection : false
        Enterprise Manager Agent
                http://idmhost2.us.oracle.com:5162/emd/main
        Oracle Internet Directory
                SSL Port : 3061
                Non SSL Port : 3060
                Database : dbhost1:1521^ dbhost2:1521@OOLRP04FMW
        Expand Cluster Managed Server Details
                wls_ods2 : 15003
```

D

Appendix: Setting Node Manager for IDM_WEBLOGIC_HOME

```
<IDM_WEBLOGIC_HOME>/wlserver_10.3/common/nodemanager/nodemanager.properties
#Changed NM Listen Port
#Thu Mar 31 12:04:37 PDT 2016
DomainsFile=/u00/webadmin/products/wls_idm/wlserver_10.3/common/nodemanager/nodema
nager.domains
LogLimit=0
DomainsDirRemoteSharingEnabled=false
PropertiesVersion=10.3
AuthenticationEnabled=true
NodeManagerHome=/u00/webadmin/products/wls_idm/wlserver_10.3/common/nodemanager
javaHome=/u00/webadmin/products/jdk_java
JavaHome=/u00/webadmin/products/jdk_java/jre
LogLevel=INFO
DomainsFileEnabled=true
StartScriptName=startWebLogic.sh
ListenAddress=
NativeVersionEnabled=true
ListenPort=5560
weblogic.security.SSL.enableJSSE=true
LogToStderr=true
SecureListener=false
LogCount=1
StopScriptEnabled=false
DomainRegistrationEnabled=false
QuitEnabled=false
LogAppend=true
StateCheckInterval=500
CrashRecoveryEnabled=false
StartScriptEnabled=true
LogFile=/u00/webadmin/products/wls_idm/wlserver_10.3/common/nodemanager/nodemanage
r.log
LogFormatter=weblogic.nodemanager.server.LogFormatter
ListenBacklog=50
```

E

Appendix: Setting Nodemanager for OAM_WEBLOGIC_HOME

```
<OAM_WEBLOGIC_HOME>/wlserver_10.3/common/nodemanager/nodemanager.properties
#Tue Mar 10 23:18:15 CDT 2015
DomainsFile=/u00/webadmin/product/fmw/wls_iam/wlserver_10.3/common/nodemanager/nod
emanager.domains
LogLimit=0
PropertiesVersion=10.3
DomainsDirRemoteSharingEnabled=false
javaHome=/u00/webadmin/product/jdk
AuthenticationEnabled=true
NodeManagerHome=/u00/webadmin/product/fmw/wls_iam/wlserver_10.3/common/nodemanager
JavaHome=/u00/webadmin/product/jdk/jre
LogLevel=INFO
DomainsFileEnabled=true
StartScriptName=startWebLogic.sh
ListenAddress=msp52777.us.oracle.com
NativeVersionEnabled=true
ListenPort=5561
LogToStderr=true
SecureListener=true
LogCount=1
DomainRegistrationEnabled=false
StopScriptEnabled=false
QuitEnabled=false
LogAppend=true
StateCheckInterval=500
CrashRecoveryEnabled=false
StartScriptEnabled=true
LogFile=/u00/webadmin/product/fmw/wls_iam/wlserver_10.3/common/nodemanager/nodeman
ager.log
LogFormatter=weblogic.nodemanager.server.LogFormatter
ListenBacklog=50
```

F

Appendix: Creating Staticports for OBIEE Configuration

staticport_wt.ini

```
##################################################################################
#####
#This file is a template file for staticports.ini
#This file must be edited to provide the ports which required to be set
#Those ports which are not provided explicitly in this file will be assigned
automatically
#The ports should be specified as a single port
#Keep in mind to uncomment the port no
##################################################################################
#####

#######################Begin section for OPMN Port
No################################
##################################################################################
####

[OPMN]

#This port indicates the OPMN Local Port
#OPMN Local Port = 6700

#This port indicates the OPMN Remote Port
#OPMN Remote Port = 6701

#######################Begin section for ohs
component################################
#This port nos will be considered only if OHS is selected for configuration
##################################################################################
#####

[OHS]

#The http_main port for ohs component
OHS Port = 7777

#This port indicates the OHS Proxy Port
#OHS Proxy Port = 8889

#This port indicates the OHS SSL Port
#OHS SSL Port = 4443

#######################Begin section for Web Cache
component################################
#This port nos will be considered only if Web Cache is selected for configuration
##################################################################################
#####

[WEBCACHE]
```

```
#The port indicates the Web Cache Listen Port
#Web Cache Listen Port = 7777

#The port indicates the Web Cache Admin Port
#Web Cache Admin Port = 7778

#The port indicates the Web Cache Statistics Port
#Web Cache Statistics Port = 7779

#The port indicates the Web Cache Invalidation Port
#Web Cache Invalidation Port = 7780

#The port indicates the Web Cache SSL Port
#Web Cache SSL Port = 7781
```

G

Appendix: Creating Staticports for OBIEE Configuration

```
# Note that if ports are not defined in this file they will be autoallocated
starting at port 9500
# It is recommended that ports 9500-9520 are left unassigned for this auto-
allocation

[WEBLOGIC]

#The Domain port no. This is the listen port of Weblogic Adminserver for the
domain.
Domain Port No = 7331

#The "content" port for the BIEE apps. This is the Weblogic Managed Server
port on which BIEE applications are deployed.
Oracle WLS BIEE Managed Server Port No = 7333

#The SSL port for the Weblogic Managed Server
#Oracle WLS BIEE Managed Server SSL Port No = 9804

#The Weblogic node manager port
Node Manager Port No = 5607

[OPMN]

#Process Manager Local port no
#Oracle Process Manager Local Port No = 6700

#Process Manager Remote port no
#Oracle Process Manager Remote Port No = 6701

#Process Manager Request port no
#Oracle Process Manager Request Port No = 6702

[BIFOUNDATION]

#The listen port for OracleBIServer component
#Oracle BI Server Port No = 9703

#The monitor port for OracleBIServer component
#Oracle BI Server Monitor Port No = 9701

#The listen port for OracleBIPresentationServices component
#Oracle BI Presentation Services Port No = 9710

#The listen port for OracleBIScheduler component
#Oracle BI Scheduler Port No = 9705

#The monitor port for OracleBIScheduler component
#Oracle BI Scheduler Monitor Port No = 9708

#The script RPC port for OracleBIScheduler component
#Oracle BI Scheduler Script RPC Port No = 9707

#The listen port for OracleBIClusterController component
#Oracle BI ClusterController Port No = 9706

#The monitor port for OracleBIClusterController component
#Oracle BI ClusterController Monitor Port No = 9700

#The listen port for OracleBIJavaHost component
```

```
#Oracle BI JavaHost Port No = 9810

[ESSBASE]

#The listen port for Essbase Agent
#Essbase Agent Port No = 1423

#The listen port for Essbase Studio
#Essbase Studio Port No = 5300
```

H

Appendix VII – LDIF Files

obiee_ldifs

retailuser_objectclasses.ldif

```
dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: ( 1.3.6.1.4.1.1.11380.97.11
NAME 'retailuser' DESC 'Oracle Retail Users for MOM' STRUCTURAL
sup ( top )
MUST ( sn $ cn ) MAY ( uid $ userPassword ) )
```

OBIEE_SSO_groups.ldif

```
dn: cn=BI Publisher Administrator,cn=groups,dc=us,dc=oracle,dc=com
objectclass: orclGroup
objectclass: groupOfUniqueNames
objectclass: top
cn: BI Publisher Administrator
description: BI Publisher Administrator
displayname: BI Publisher Administrator
uniquemember: cn=BIPublisher,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=bisystemuser,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=retail.user,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=xmlpadmin,cn=users,dc=us,dc=oracle,dc=com

dn: cn=BIAdministrators,cn=groups,dc=us,dc=oracle,dc=com
displayname: OBIEE Users
description: OBIEE Users
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
uniquemember: cn=bisystemuser,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=orcladmin
uniquemember: cn=retail.user,cn=users,dc=us,dc=oracle,dc=com
cn: BIAdministrators

dn: cn=BISystemUsers,cn=groups,dc=us,dc=oracle,dc=com
displayname: OBIEE Users
description: OBIEE Users
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
uniquemember: cn=bisystemuser,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=orcladmin
uniquemember: cn=retail.user,cn=users,dc=us,dc=oracle,dc=com
cn: BISystemUsers

dn: cn=BIConsumers,cn=groups,dc=us,dc=oracle,dc=com
displayname: OBIEE Users
description: OBIEE Users
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
uniquemember: cn=bisystemuser,cn=users,dc=us,dc=oracle,dc=com
```

```
uniquemember: cn=orcladmin
uniquemember: cn=retail.user,cn=users,dc=us,dc=oracle,dc=com
cn: BIConsumers

dn: cn=BIAuthors,cn=groups,dc=us,dc=oracle,dc=com
objectclass: orclGroup
objectclass: groupOfUniqueNames
objectclass: top
description: BI Authors
displayname: BI Authors
uniquemember: cn=BIPublisher,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=retail.user,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=useranalysts,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=userbuyers,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=userbuyersanalysts,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=userinventoryanalysts,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=userinventorymanagers,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=usermerchandiseexecutives,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=usermerchandisefinancialplanners,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=userplanningexecutives,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=userpricinganalysts,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=userpromotionalplanners,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=xmlpadmin,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=bisystemuser,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=orcladmin
cn: BIAuthors
```

OBIEE_SSO_Users.ldif

```
dn: cn=BIImpersonateUser,cn=Users,dc=us,dc=oracle,dc=com
objectclass: inetorgperson
objectclass: orcluserv2
objectclass: retailUser
objectclass: person
objectclass: orcluser
objectclass: organizationalperson
objectclass: top
cn: BIImpersonateUser
sn: user
description: BI User
givenname: BIImpersonateUser
mail: BIImpersonateUser@company.domain
uid: BIImpersonateUser
userpassword: <password>

dn: cn=BIpublisher,cn=Users,dc=us,dc=oracle,dc=com
objectclass: inetorgperson
objectclass: orcluserv2
objectclass: retailUser
objectclass: person
objectclass: orcluser
objectclass: organizationalperson
objectclass: top
cn: BIpublisher
sn: BIpublisher
description: BI User
givenname: BIpublisher
mail: BIpublisher@company.domain
uid: BIpublisher
userpassword: <password>

dn: cn=BISystemUser,cn=Users,dc=us,dc=oracle,dc=com
objectclass: inetorgperson
```

```
objectclass: orcluserv2
objectclass: retailUser
objectclass: person
objectclass: orcluser
objectclass: organizationalperson
objectclass: top
cn: BISystemUser
sn: BISystemUser
description: BI User
givenname: BISystemUser
mail: BISystemUser@company.domain
uid: BISystemUser
userpassword: <password>

dn: cn=UserAnalysts,cn=Users,dc=us,dc=oracle,dc=com
objectclass: inetorgperson
objectclass: orcluserv2
objectclass: retailUser
objectclass: person
objectclass: orcluser
objectclass: organizationalperson
objectclass: top
cn: UserAnalysts
sn: UserAnalysts
description: BI User
givenname: UserAnalysts
mail: UserAnalysts@company.domain
uid: UserAnalysts
userpassword: <password>

dn: cn=UserBuyerAnalysts,cn=Users,dc=us,dc=oracle,dc=com
objectclass: inetorgperson
objectclass: orcluserv2
objectclass: retailUser
objectclass: person
objectclass: orcluser
objectclass: organizationalperson
objectclass: top
cn: UserBuyerAnalysts
sn: UserBuyerAnalysts
description: BI User
givenname: UserBuyerAnalysts
mail: UserBuyerAnalysts@company.domain
uid: UserBuyerAnalysts
userpassword: <password>

dn: cn=UserInventoryAnalysts,cn=Users,dc=us,dc=oracle,dc=com
objectclass: inetorgperson
objectclass: orcluserv2
objectclass: retailUser
objectclass: person
objectclass: orcluser
objectclass: organizationalperson
objectclass: top
cn: UserInventoryAnalysts
sn: UserInventoryAnalysts
description: BI User
givenname: UserInventoryAnalysts
mail: UserInventoryAnalysts@company.domain
uid: UserInventoryAnalysts
userpassword: <password>

dn: cn=UserInventoryManagers,cn=Users,dc=us,dc=oracle,dc=com
```

```
objectclass: inetorgperson
objectclass: orcluserv2
objectclass: retailUser
objectclass: person
objectclass: orcluser
objectclass: organizationalperson
objectclass: top
cn: UserInventoryManagers
sn: UserInventoryManagers
description: BI User
givenname: UserInventoryManagers
mail: UserInventoryManagers@company.domain
uid: UserInventoryManagers
userpassword: <password>

dn: cn=UserMerchandiseExecutives,cn=Users,dc=us,dc=oracle,dc=com
objectclass: inetorgperson
objectclass: orcluserv2
objectclass: retailUser
objectclass: person
objectclass: orcluser
objectclass: organizationalperson
objectclass: top
cn: UserMerchandiseExecutives
sn: UserMerchandiseExecutives
description: BI User
givenname: UserMerchandiseExecutives
mail: UserMerchandiseExecutives@company.domain
uid: UserMerchandiseExecutives
userpassword: <password>

dn: cn=UserMerchandiseFinancialPlanners,cn=Users,dc=us,dc=oracle,dc=com
objectclass: inetorgperson
objectclass: orcluserv2
objectclass: retailUser
objectclass: person
objectclass: orcluser
objectclass: organizationalperson
objectclass: top
cn: UserMerchandiseFinancialPlanners
sn: UserMerchandiseFinancialPlanners
description: BI User
givenname: UserMerchandiseFinancialPlanners
mail: UserMerchandiseFinancialPlanners@company.domain
uid: UserMerchandiseFinancialPlanners
userpassword: <password>

dn: cn=UserPlanningExecutives,cn=Users,dc=us,dc=oracle,dc=com
objectclass: inetorgperson
objectclass: orcluserv2
objectclass: retailUser
objectclass: person
objectclass: orcluser
objectclass: organizationalperson
objectclass: top
cn: UserPlanningExecutives
sn: UserPlanningExecutives
description: BI User
givenname: UserPlanningExecutives
mail: UserPlanningExecutives@company.domain
uid: UserPlanningExecutives
userpassword: <password>
```

```
dn: cn=UserPricingAnalysts,cn=Users,dc=us,dc=oracle,dc=com
objectclass: inetorgperson
objectclass: orcluserv2
objectclass: retailUser
objectclass: person
objectclass: orcluser
objectclass: organizationalperson
objectclass: top
cn: UserPricingAnalysts
sn: UserPricingAnalysts
description: BI User
givenname: UserPricingAnalysts
mail: UserPricingAnalysts@company.domain
uid: UserPricingAnalysts
userpassword: <password>

dn: cn=UserPromotionalPlanners,cn=Users,dc=us,dc=oracle,dc=com
objectclass: inetorgperson
objectclass: orcluserv2
objectclass: retailUser
objectclass: person
objectclass: orcluser
objectclass: organizationalperson
objectclass: top
cn: UserPromotionalPlanners
sn: UserPromotionalPlanners
description: BI User
givenname: UserPromotionalPlanners
mail: UserPromotionalPlanners@company.domain
uid: UserPromotionalPlanners
userpassword: <password>

dn: cn=xmlpadmin,cn=Users,dc=us,dc=oracle,dc=com
objectclass: inetorgperson
objectclass: orcluserv2
objectclass: retailUser
objectclass: person
objectclass: orcluser
objectclass: organizationalperson
objectclass: top
cn: xmlpadmin
sn: xmlpadmin
description: BI User
givenname: xmlpadmin
mail: xmlpadmin@company.domain
uid: xmlpadmin
userpassword: <password>
```

retail.user_ldifs

retail.user.ldif

```
dn: cn=retail.user,cn=Users,dc=us,dc=oracle,dc=com
defaultstore: storeId=4241,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
givenname: retail.user
orclsamaccountname: retail.user
externalid: RETAIL.USER
orclactivestartdate: 20150702000000Z
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: orclUser
objectclass: orclUserV2
```

```
objectclass: simUser
objectclass: retailUser
sn: retail.user
superuser: true
userpassword: <password>
preferredcountry: US
preferredLanguage: en
uid: retail.user
mail: retail.user
cn: retail.user
empstatus: 0
userstores: storeId=7000,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
userstores: storeId=4241,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
userstores: storeId=5251,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
userstores: storeId=9000,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
userstores: storeId=8989,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
userstores: storeId=3211,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
userstores: storeId=2233,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
userstores: storeId=7778,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
userstores: storeId=1212,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
userstores: storeId=4444,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
userstores: storeId=6666,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
userstores: storeId=7777,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
userstores: storeId=5999,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
userstores: storeId=5998,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
userstores: storeId=2689,cn=SIMStores,cn=SIM,dc=us,dc=oracle,dc=com
description: Seed administrative user for subscriber.
```

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Copyright © 2016, Oracle. All rights reserved.
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.