Oracle® Retail High Availability Case Study – Retail Applications Installation

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

Contents ii

1 Installation Overview 5

2 Directory Structure 7

3 Installing WebLogic Server for FORMS 9

Install WebLogic Release 10.3.6 9

Install and Configure Forms 13

Install Oracle Forms 11.1.2.2 13

Configure Forms 19

Configure Forms on appserver2: 25

Understanding the Forms Post Installation Tasks 31

Finalize Forms Installation 32

3 Configuring Single Sing On 35

Configure Forms for Single Sign On 35

Register WebTier with Forms EM 36

Update forms config to accept SSO connections 37

Configure webtier to redirect forms request 37

Post Install steps for Forms SSO set up: 39

4 Preparing and Installing Retail Java Applications 43

Middleware Infrastructure and WebLogic Server 12c (12.1.3) Installation 43

Apply Security Patch for 12.1.3 Weblogic version 49

Install RCU Database Schemas 50

Create a New ADF Domain (with managed server and EM) 57

ALLOC Domain setup screens 69

SIM Domain setup screens 74

RESA Domain setup screens 78

RPM Domain setup screens 83

Procedure to start Nodemanger, AdminServer and Managed Server: 87

Start the Node Manager 87

Start the AdminServer (admin console) 87

Start the Managed Server hosted in Appserver1 88

Pack Domain and Copy to appserver2 88

Unpack Domain in appserver2 89

Install the Oracle Retail Java Applications 90

WebLogic.policy entry for both hosts 90

Configuration of OID Provider in WebLogic Domain 92

Configure Oracle Single Sign-On 96

Create the SSO provider in the REIMDomain 97

Creating mds-CustomPortalDS Datasource using EM 98

Deployment of jax-rs-2.0 library in WebLogic 104

4 Installing the REIM Application 111
Prerequisite Task for REIM 111
Steps to Configure WebLogic Work Manager 111
Clustered Installations – Preinstallation Steps 118
Expand the ReIM Application Distribution 118
Run the Oracle Retail Invoice Matching Installer 119
Post-Installation Steps 119
Clustered Installations – Post-Installation Steps 120
Test the ReIM Application 120
ReIM Batch Scripts 120
Online Help 121
Single Sign-On 121
Adding Logout URI 122
5 Installing the Allocation Application 123
Clustered Installations – Preinstallation Steps 123
Expand the Oracle Retail Allocation Application Distribution 123
Run the Oracle Retail Allocation Application Installer 123
Post-Installation Steps 124
Increase Max JMS messages 125
Steps to Configure WebLogic Work Manager 125
Clustered Installations – Post-Installation Steps 125
Test the Oracle Retail Allocation Application 126
Allocation Batch Scripts 126
Single Sign-On 127
Adding Logout URI 127
6 Installing the SIM 129
Expand the SIM Application Distribution 129
Set the Environment Variables for the SIM Installer 129
Run the SIM Application Installer 129
SIM Database Authentication Provider set up (to be done after the application deploy) 130
Review and/or Configure Oracle Single Sign-On 132
Create the SIM SSO provider in the SIMDomain 132
SIM Batch Scripts 137
Starting and Stopping the Wavelink Server 137
Test the SIM Application 137
7 Installing the RPM Application 139
Expand the RPM Application Distribution 139
Clustered Installations – Preinstallation Steps 139
Provide the Hibernate4.3.10 Jar File 139
Run the RPM Application Installer 140
Clustered Installations – Post-Installation Steps 141

Review and/or Configure Oracle Single Sign-On....141
Sign the RPM Client Configuration Jar File....143
Transaction Timeout....144
Test the RPM Application....144
RPM Batch Scripts....145
Adding a User to the RPM Application....146

8 Installing the ReSA Application....147

Clustered Installations – Preinstallation Steps....147
Expand the ReSA Application Distribution....147
Run the ReSA Application Installer....147
Test the ReSA Application....148
REST Web Service Disable/Re-enable....148
Disable REST Web Services war....148
Re-enable REST Web Services war....149
Single Sign-On....149

A Appendix: REIM Application Installer Screens....150

B Appendix: Oracle Retail Allocation Application Installer Screens....161

C Appendix: SIM Application Installer Screens....171

D Appendix: RPM Application Installer Screens....189

E Appendix: ReSA Installer Screens....201

F Appendix: ant.install.properties - ReIM....209

G Appendix: ant.install.properties - ALLOC....211

H Appendix: ant.install.properties - SIM....213

I Appendix: ant.install.properties - RPM....217

J Appendix: ant.install.properties - ReSA....221

K Appendix: Entries of mod_wl_ohs.conf File....223

1

Installation Overview

Oracle Retail applications can be deployed in a High Availability environment, utilizing WebLogic Server (WLS) active-active clustering and Oracle Real Application Cluster (RAC) databases to provide high availability and scalability. This configuration allows lower-cost commodity systems to be combined into a single scalable, fault-tolerant computing environment.

There are many options for configuring an Oracle Retail 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 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 apply in their entirety only to the exact hardware and software configuration described in this case study.

- Install Oracle WebLogic Server 10.3.6 environment for FORMS
  - Install WebLogic 10.3.6 Software – Clustered.
  - Install Oracle Forms 11.1.2.2 for RMS, RWMS, ARI forms use. Configure forms.
- Install Oracle Weblogic Server 12.1.3 for MOM applications
  - Install Java applications (such as, RPM, Alloc, ReIM, SIM).
  - Apply patch as per Weblogic 12.1.3
- Configure SSO for Forms.
- Configure SSO for Applications

> **Note:** This document uses the hostnames appserver1 and appserver2 for different hosts in the cluster. You should substitute the appropriate names of the hosts for your installation. In some cases, the screenshots show msp00acs and msp00acf, which are appserver1 and appserver2, respectively. The hostnames idmhost1 and idmhost2 are for different hosts in the cluster where you have OID/OAM and WebTier components installed. You should substitute the appropriate names of the hosts for your installation. In some cases, the screenshots show msp00acz.us.oracle.com and msp00ada.us.oracle.com, which are idmhost1 and idmhost2, respectively.

Before proceeding to **Next** sections kindly ensure that:

LDAP Server is accessible using Loadbalancer url.

E.g. ldap:// msp00acz-ada-vip.us.oracle.com:3060

Oracle WebTier has been configured and accessible using Loadbalancer url.

E.g. http:// msp00acz-ada-vip.us.oracle.com:7777

2

Directory Structure

- APPDomain (for Retail Applications) — WebLogic 12.1.3 (needed for Web Tier):
  APP_WEBLOGIC_HOME=/u00/webadmin/product/wls_retail
  APP_WEBLOGIC_DOMAIN_HOME=
  /u00/webadmin/config/domains/wls_retail/<App>DOMAIN
  Eg: /u00/webadmin/config/domains/wls_retail/REIMDOMAIN

- ClassicDomain (for Forms) — WebLogic 10.3.6, Forms 11gR2 (frmrpts_11.1.2.2):
  FORMS_WEBLOGIC_HOME=/u00/webadmin/product/wls_forms
  FORMS_WEBLOGIC_DOMAIN_HOME=
  /u00/webadmin/config/domains/wls_forms/ClassicDomain

- Java for APPDomain, ClassicDomain - JDK 1.7.0+:
  JAVA_HOME=/u00/webadmin/product/jdk_java

3

Installing WebLogic Server for FORMS

This chapter describes how to install WebLogic Server Release 10.3.6.

Install WebLogic Release 10.3.6

Complete these steps on all two application server systems - appserver1 and appserver2. The installations on appserver1 and appserver2 are clustered together. The appserver1 host Admin and managed_server1 and appserver2 host managed_server2.

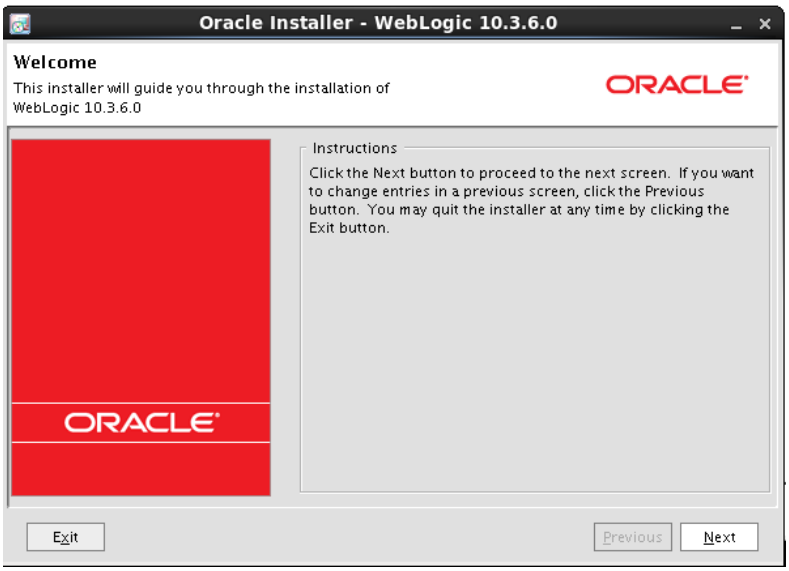
To install the WebLogic Server:

- Create a directory to install the WebLogic (this will be the WLS_HOME):
  $ mkdir -p /u00/webadmin/product/wls_forms

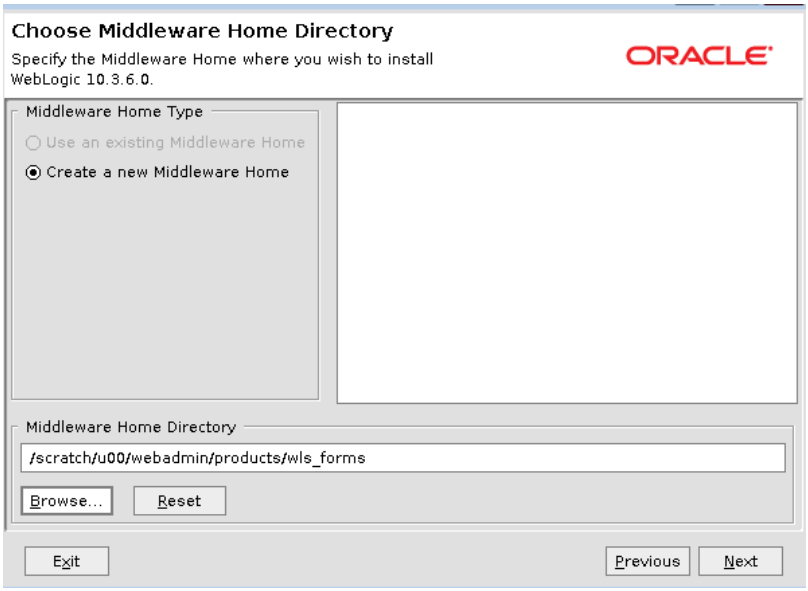
- Copy the java distribution locally, set JAVA_HOME and add it to the PATH.
  $ cp -r <Path_to_Java_Distro>/jdk1.7 /u00/webadmin/product/jdk_java
  $ export JAVA_HOME=/u00/webadmin/product/jdk_java
  $ export PATH=$JAVA_HOME/bin:$PATH

- Start the installer, make sure DISPLAY variable is set.
  $ java -jar <Path_to_WebLogic_Distro>/wls1036_generic.jar

- The Welcome screen of the WebLogic 10.3.6 Installer opens. Click **Next**.

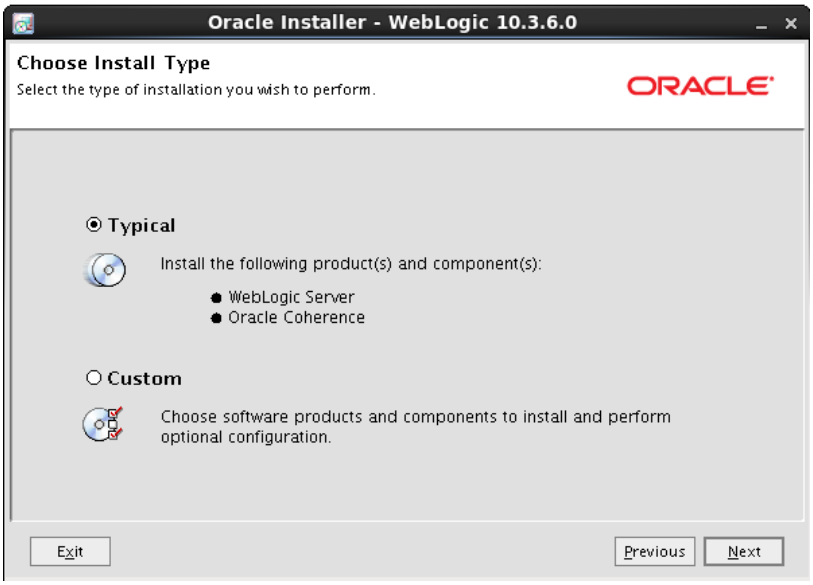


- The Specify Middleware Home Directory window opens. Click **Next**.

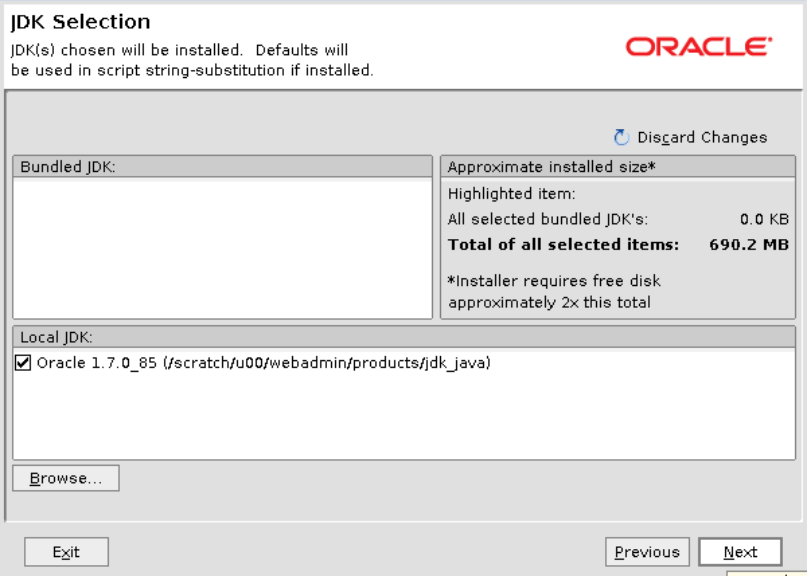


- The Email Registration window opens. Uncheck the receive security box, and then Click **Yes** to bypass. Click **Continue**, and then click **Next**.

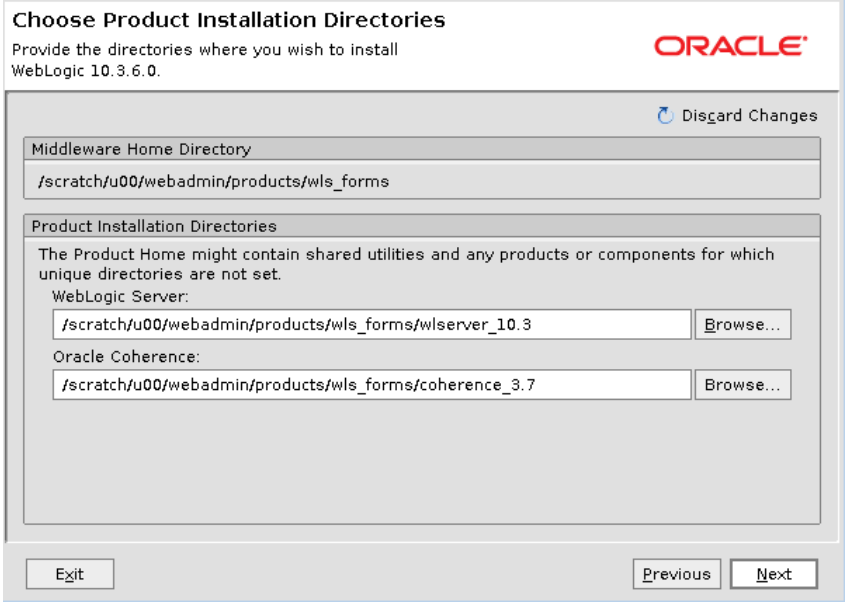
- The Choose Install Type window opens. Select **Typical**, and click **Next**.



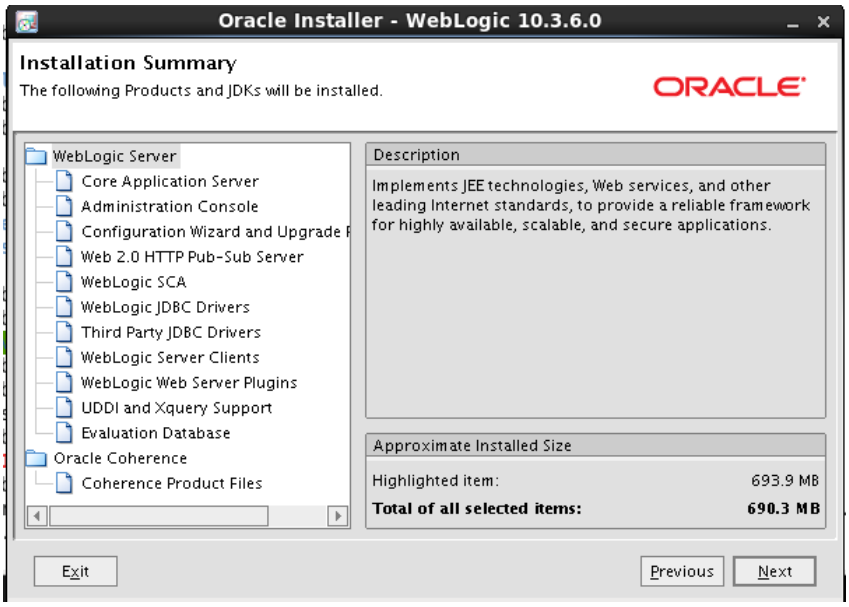
- The JDK Selection window displays. By default, it will select the JDK in your JAVA_HOME setting. Ensure the JAVA_HOME points to JDK 1.7.0+. Click **Next**



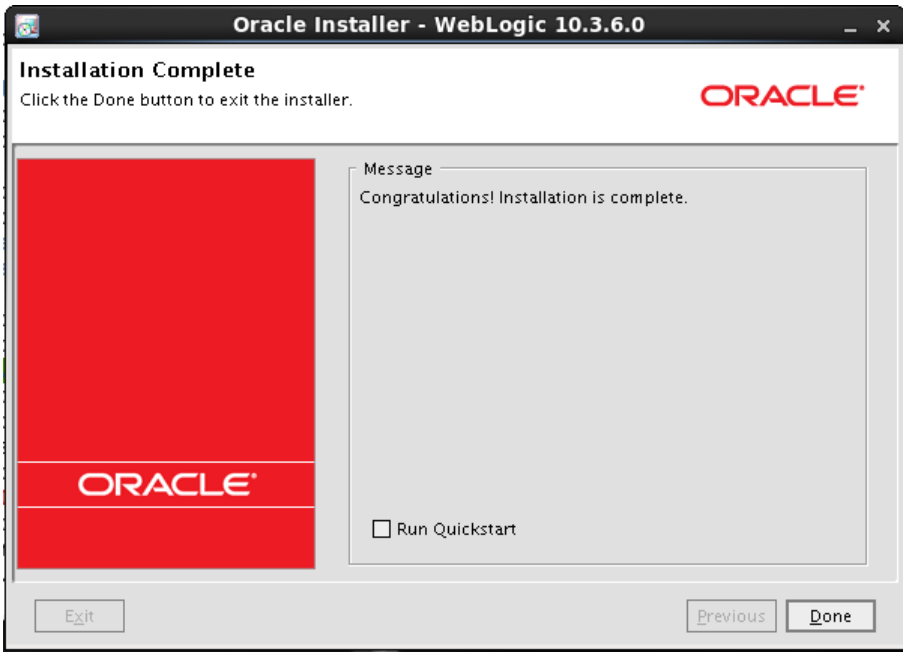
- The Choose Product Installation Directories window opens. Retain the default values, and click **Next**.



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



- The product install will begin. Once finished, the Installation Complete window opens. Uncheck Run Quickstart, and click **Done**.



- The installation is complete.
- Similarly, install weblogic in appserver2 using above steps.

Install and Configure Forms

This section describes how to install and configure forms.

Install Oracle Forms 11.1.2.2

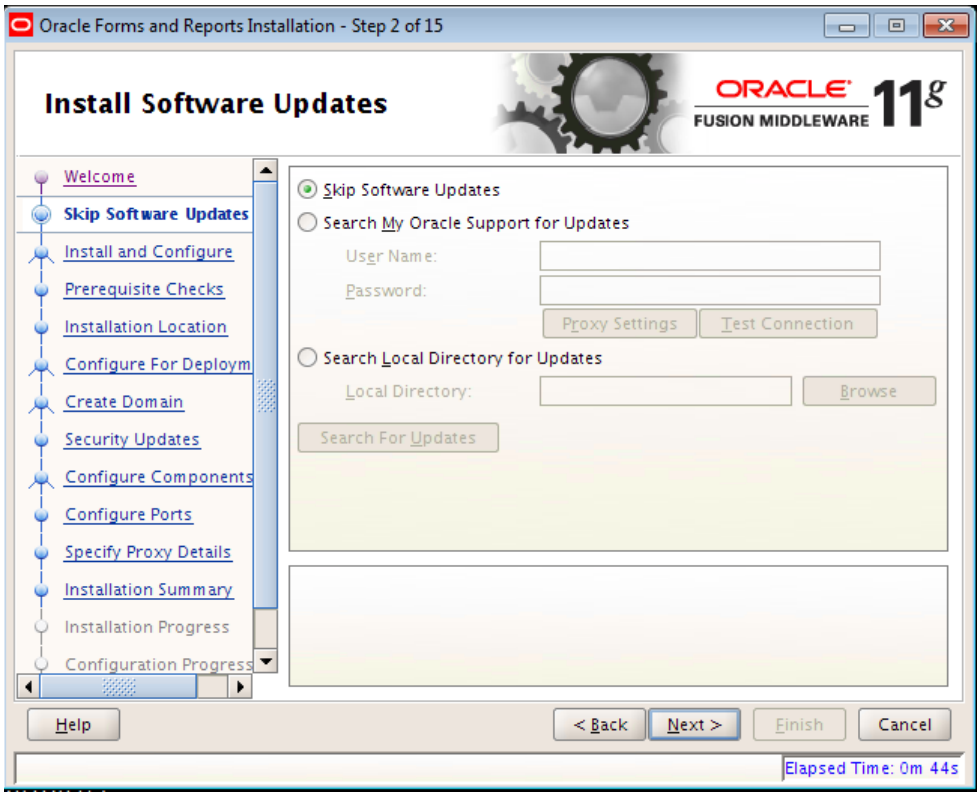
To install Oracle forms 11.1.2.2:

> **Note:** Root access is needed twice during this install, once on initial install and then again with the patch.

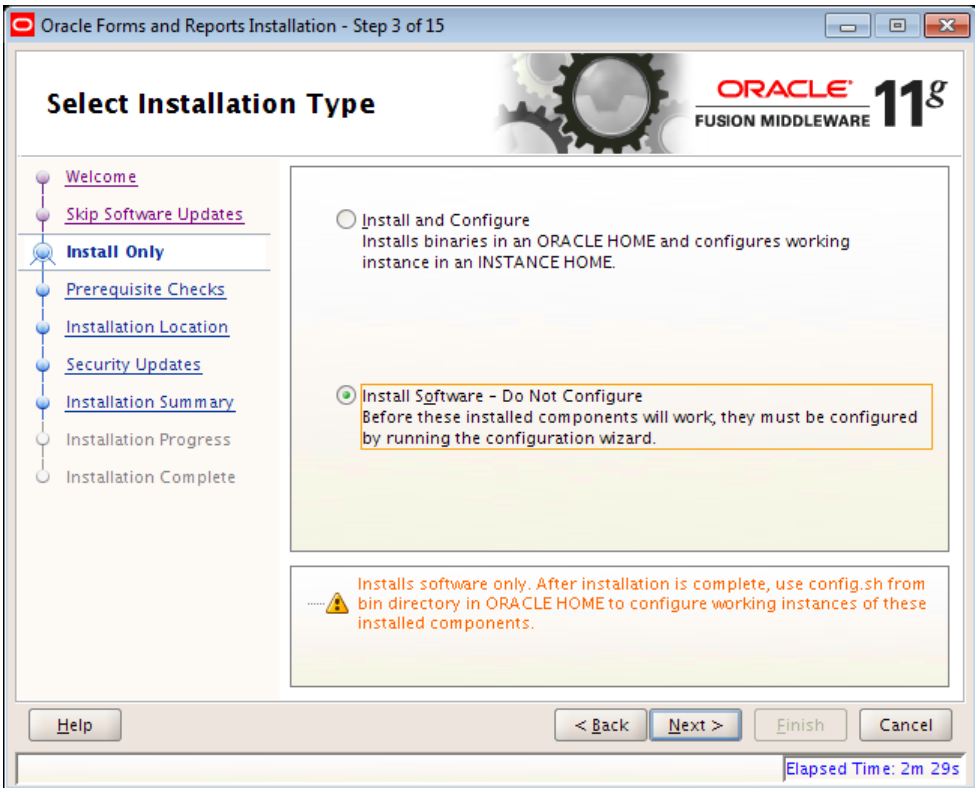
- Apply Patch 20836354 as the FR 11.1.2.2 PREREQ CHECK will not fail on ORACLE LINUX 7 X86-64BIT OS
  - Copy to the some media directory and unzip it.
  - Unzip –d PATCH_TOP p20836354_111220_Generic.zip
- Go to forms installer location and run the installer from the same user WebLogic is installed as. ./runInstaller PREREQ_CONFIG_LOCATION=/u00/webadmin/media/PATCH_TOP/prereq/ $ ./runInstaller

Oracle Forms and Reports Installation - Step 1 of 15
Welcome
ORACLE
FUSION MIDDLEWARE
11g
Welcome
Install Software Updates
Install and Configure
Prerequisite Checks
Installation Location
Configure For Deploym
Create Domain
Security Updates
Configure Components
Configure Ports
Specify Proxy Details
Installation Summary
Installation Progress
Configuration Progress
Welcome to Oracle Fusion Middleware 11g R2 Forms and Reports Installer version 11.1.2.2.0.
This installer can be used to install a new Forms and Reports Oracle Home or to update an existing Forms and Reports Oracle Home.
Context-sensitive help is available by clicking Help.
Click Next to begin the installation.
Copyright (c) 1982, 2013, Oracle and/or its affiliates. All rights reserved.
Help
< Back
Next >
Finish
Cancel
Elapsed Time: 0m 19s

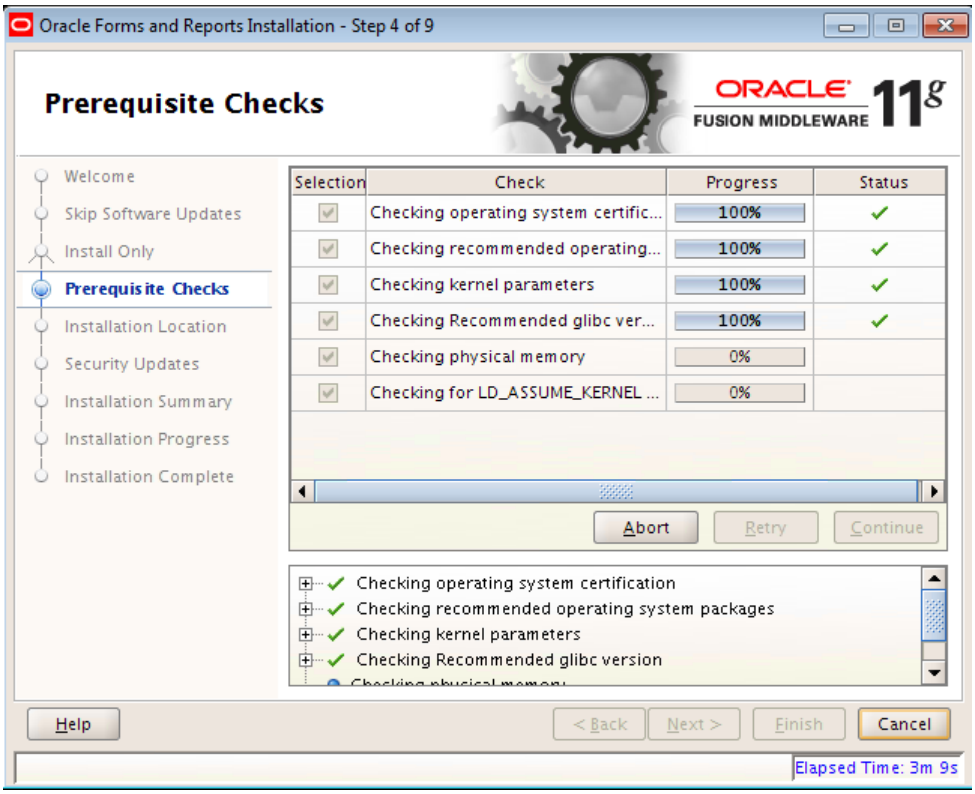
- Click **Next**.


Oracle Forms and Reports Installation - Step 2 of 15
Install Software Updates
ORACLE
FUSION MIDDLEWARE
11g
Welcome
Skip Software Updates
Install and Configure
Prerequisite Checks
Installation Location
Configure For Deploym
Create Domain
Security Updates
Configure Components
Configure Ports
Specify Proxy Details
Installation Summary
Installation Progress
Configuration Progress
Skip Software Updates
Search My Oracle Support for Updates
User Name:
Password:
Proxy Settings
Test Connection
Search Local Directory for Updates
Local Directory:
Browse
Search For Updates
Help
< Back
Next >
Finish
Cancel
Elapsed Time: 0m 44s

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



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

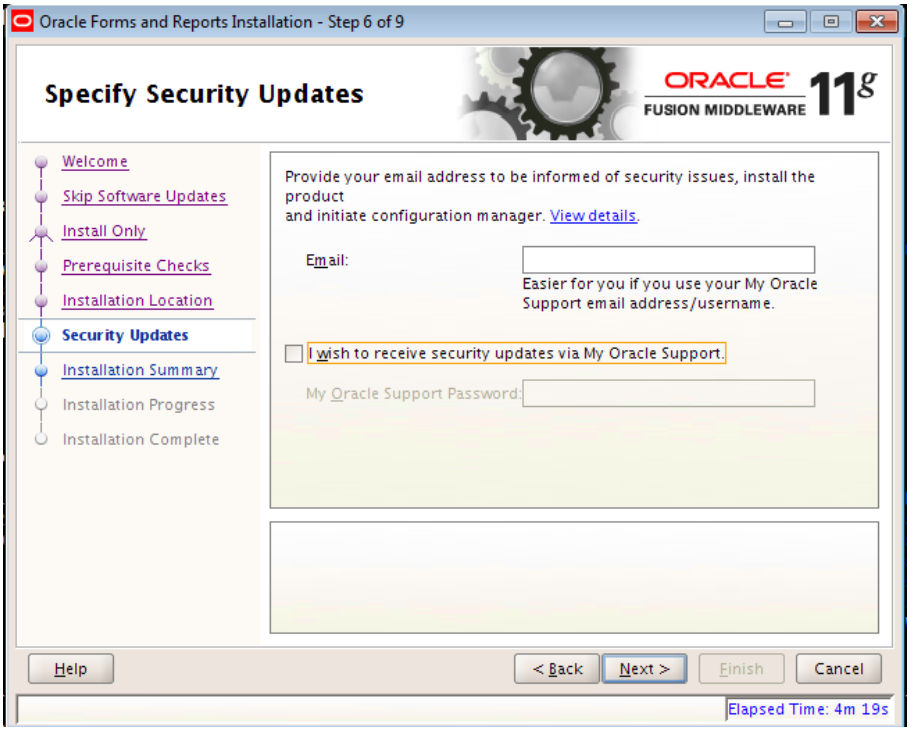


- The Specify Installation Location window opens. Select the same directory as the WebLogic install.

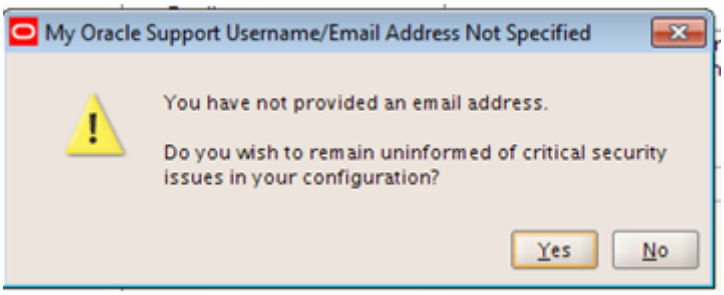
  Example: /u00/webadmin/product/wls_retail

  Click **Next**.

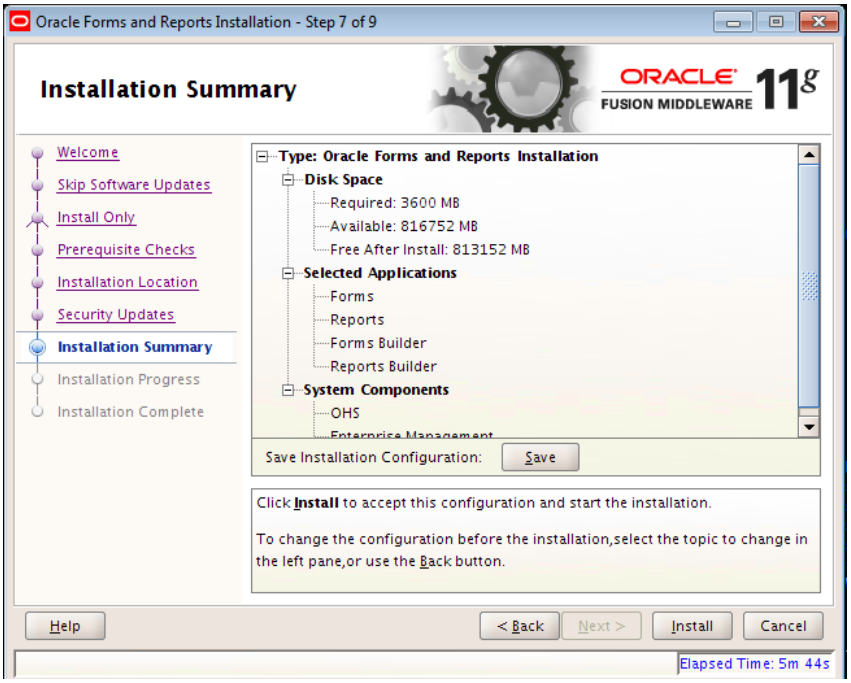
- The Specify Security Updates window opens.



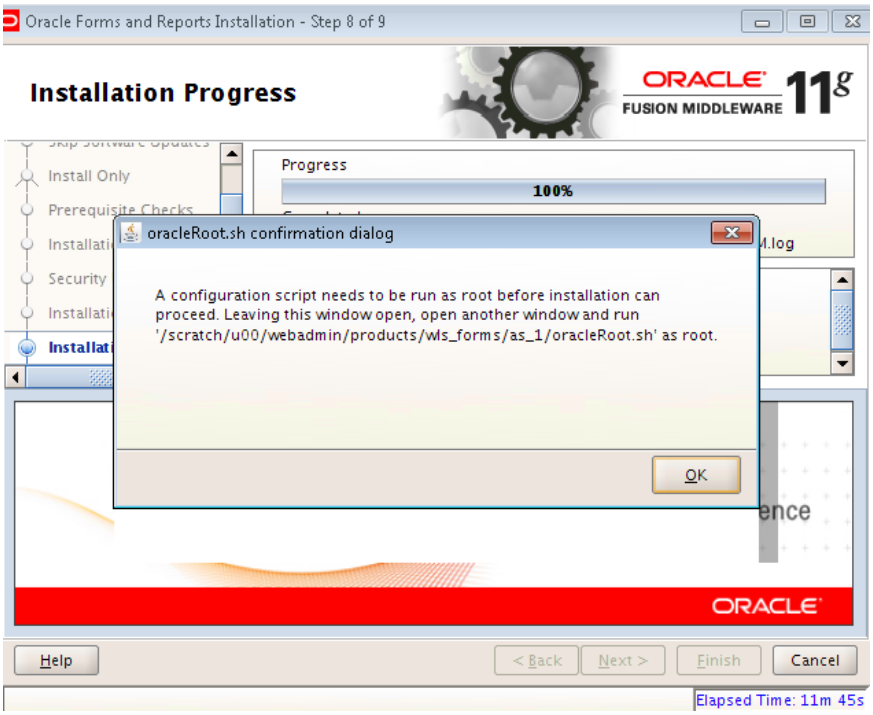
- Click **Yes** if you do not want to be informed of the critical security issues in your configuration.



- The Installation Summary window opens. Click **Install**. The Installation Progress window opens. The installation may take 5-15 minutes.



- After the installation is complete, the Installation Progress window opens. A confirmation window opens as above. Click **OK** to run a script as root.



- Run oracleRoot.sh before confirming dialog. Run the command as root user:
  Example: sudo /u00/webadmin/product/wls_forms/as_1/oracleRoot.sh
- Click **OK** when the script is complete.
- Click **Finish** once the installation is completed.
- Repeat this installation on appserver2.

Note: Forms do not Compile on Oracle Linux 7, after successful installation of Forms 11.1.2.2 on Oracle Linux 7 as the new version of motif library libXm.so.3 is not available on Oracle Linux 7. As a solution, a sym link with older version of motif library must be made as below:

`ln -s /usr/lib64/libXm.so.4.0.4 libXm.so.3`

Note: Forms do not Compile on Oracle Linux 7, after successful installation of Forms 11.1.2.2 on Oracle Linux 7 as the new version of motif library libXm.so.3 is not available on Oracle Linux 7. As a solution, a sym link with older version of motif library must be made as below:

`ln -s /usr/lib64/libXm.so.4.0.4 libXm.so.3`

Note: If Error in invoking target 'agent nmb nmo nmhs tclexec' in oracle 11g installation

When installing Oracle 11g you may get the following error:

Error in invoking target 'agent nmb nmo nmhs tclexec' of makefile '/u01/app/oracle/product/11.1.0/db_1/sysman/lib/ins_emagent.mk

Solution:

Within the file detailed in the error edit it and find the line that reads '$(MK_EMAGENT_NMECTL)' change this to '$(MK_EMAGENT_NMECTL) -lnnz11'

It will look like:

$(SYSMANBIN)emdctl:

$(MK_EMAGENT_NMECTL) -lnnz11

Edit this file while you still have the installer open, once you have changed it just click retry.

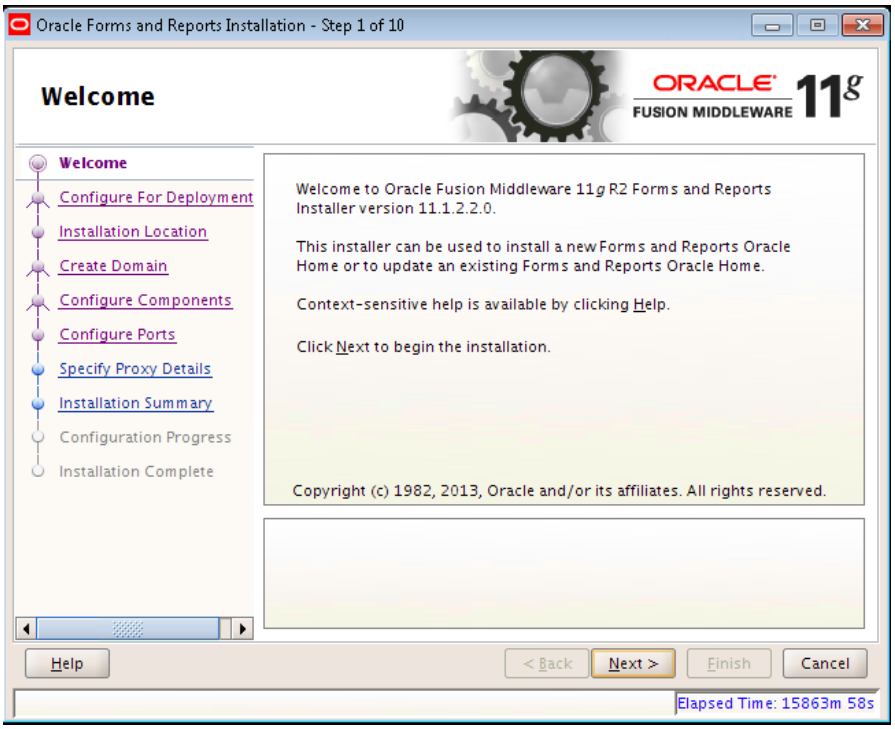
Configure Forms

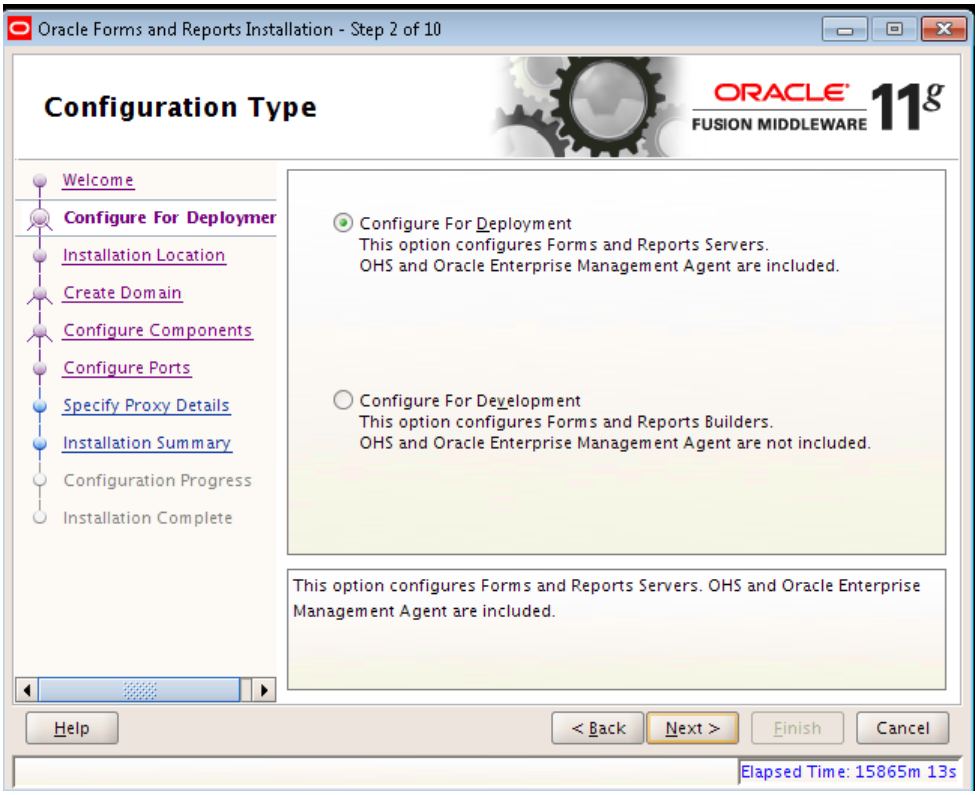
This section describes the steps to configure forms.

Configure Forms on appserver1

To configure forms on appserver1:

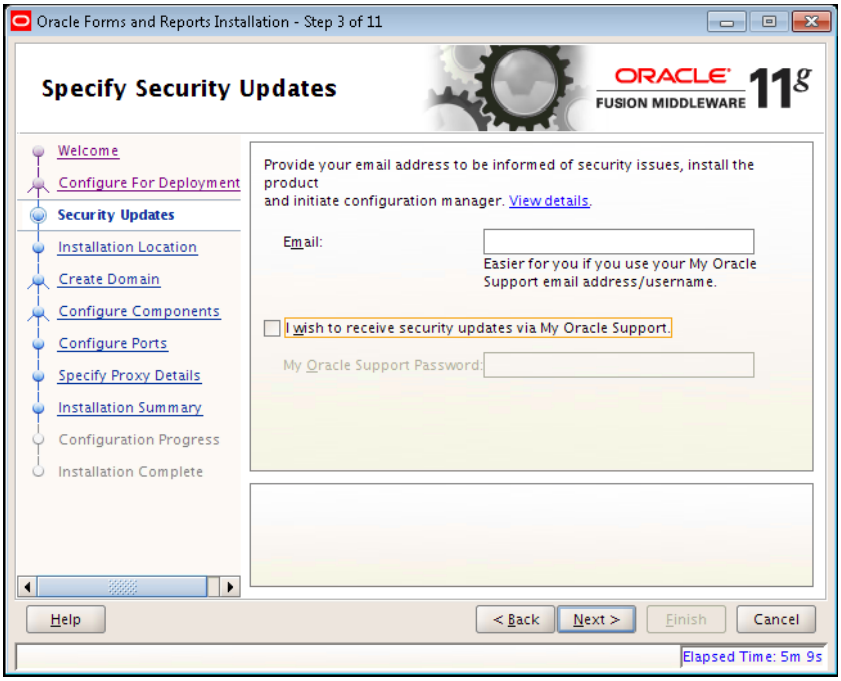
- Run the following command:
  (/u00/webadmin/product/wls_forms/as_1/bin/config.sh)
  $ ORACLE_HOME/bin/config.sh
- The Welcome window opens.



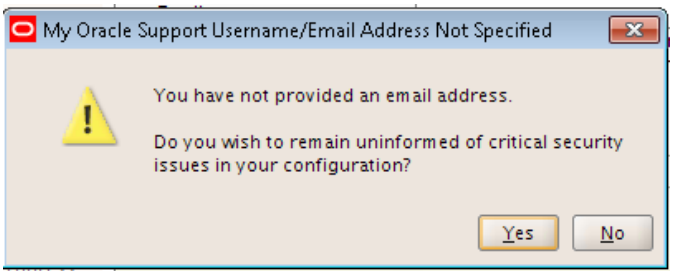


- The Specify Security Updates window opens. Enter the email id and support password, and click **Next**.

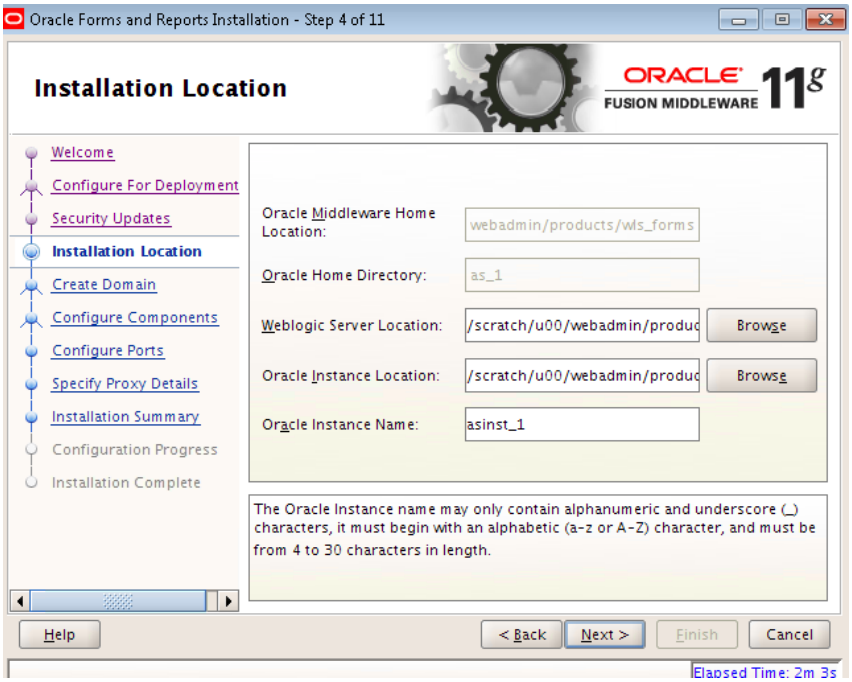
Note: The rest of this document assumes ClassicDomain is used for Domain Name.



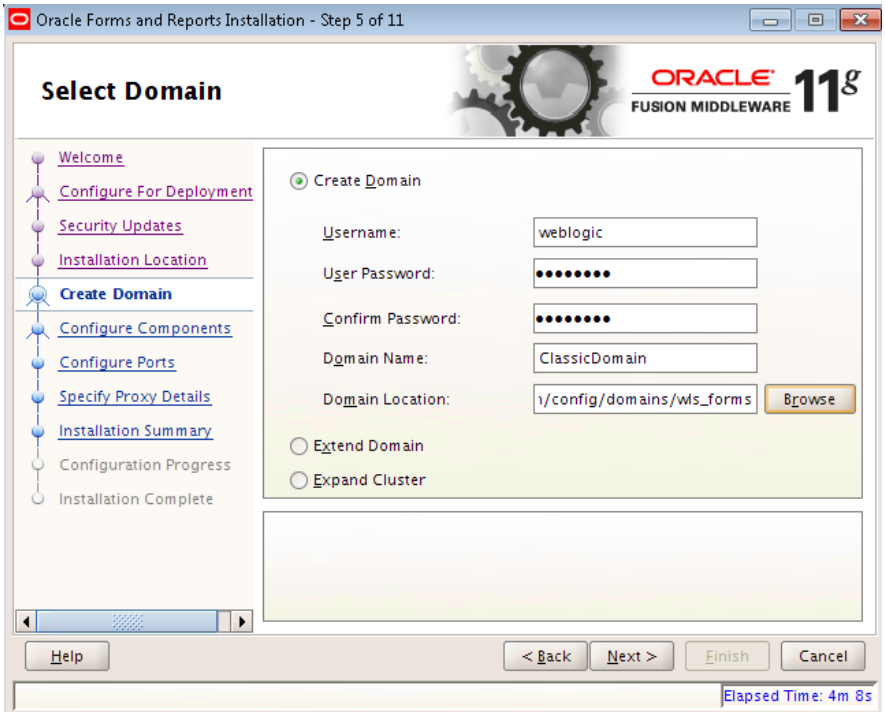
- Click **Yes** in the confirmation window.



- The **Installation Location** window opens. Verify the directories, and click **Next**.

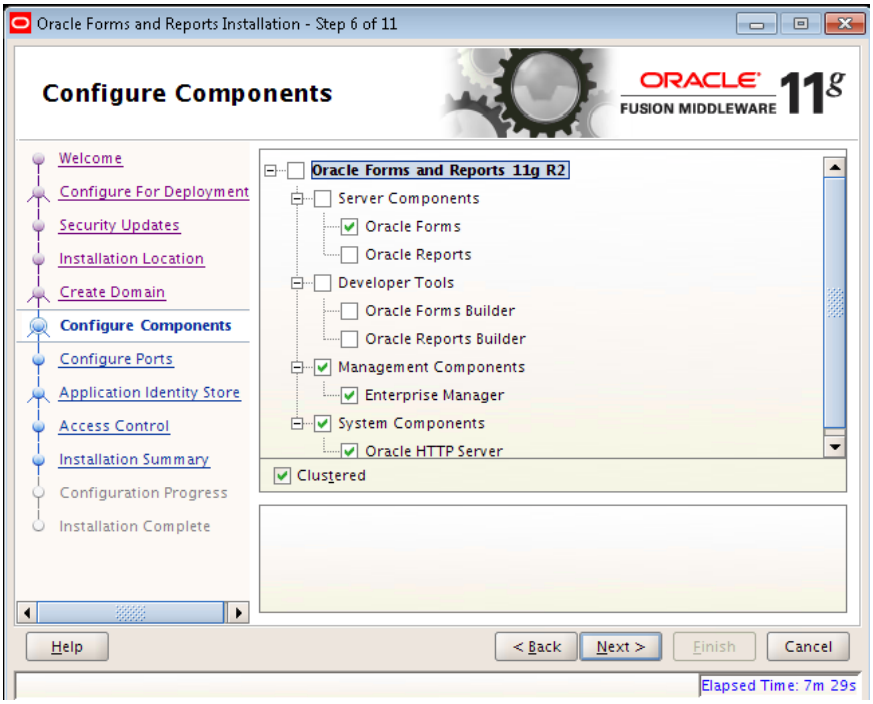


- The Prerequisite Checks window opens. Verify the prerequisites are installed, and click **Next**.
- The Create Domain window opens.

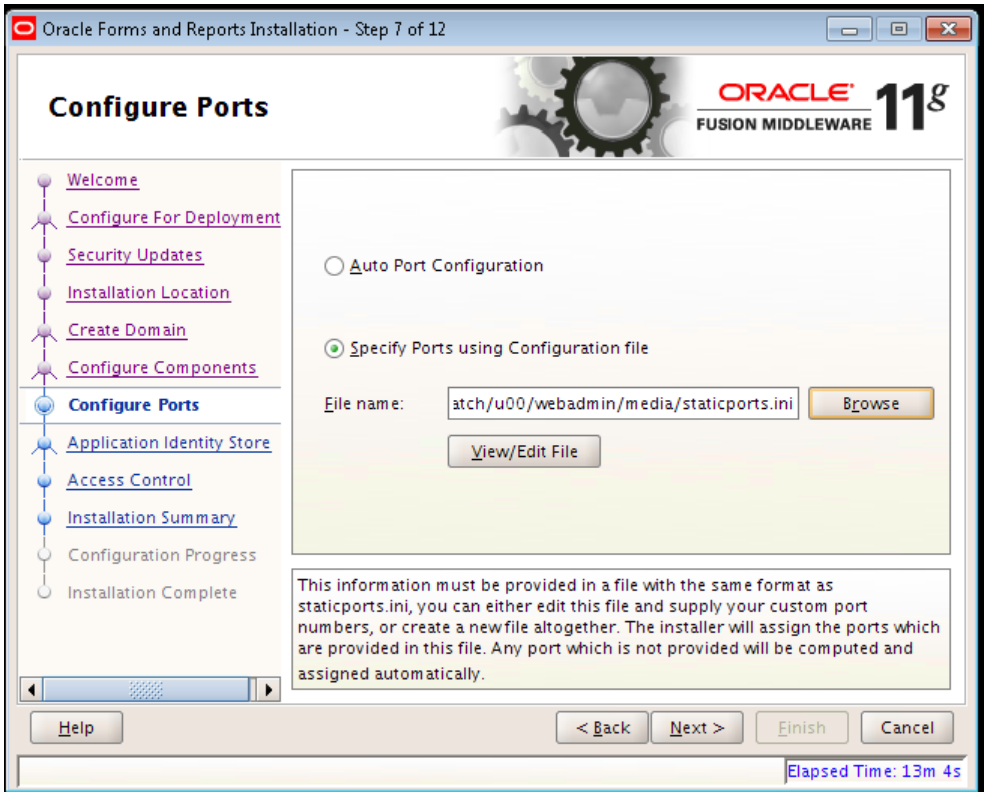


- Enter WebLogic user a password, and Click **Next**.
- The Configure Components window opens. Select the options as shown in the screenshot, and click **Next**.

> **Note:** The rest of this document assumes defaults are used for Oracle Instance Name, asinst_1 and asinst_2 for appserver1 and appserver2 respectively.

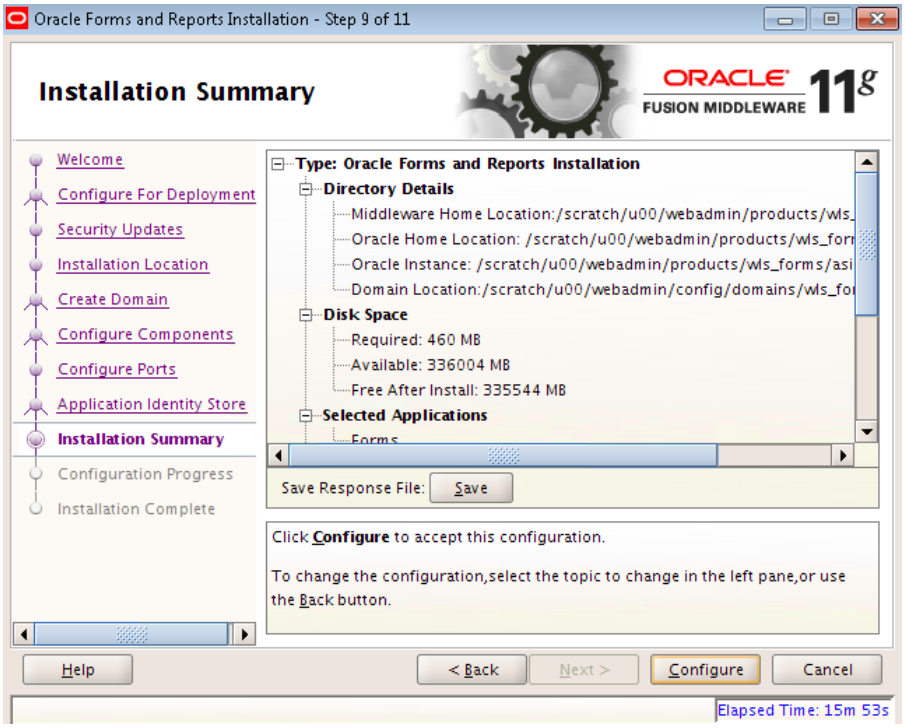


- The Configure Ports window opens. Click **Next**.

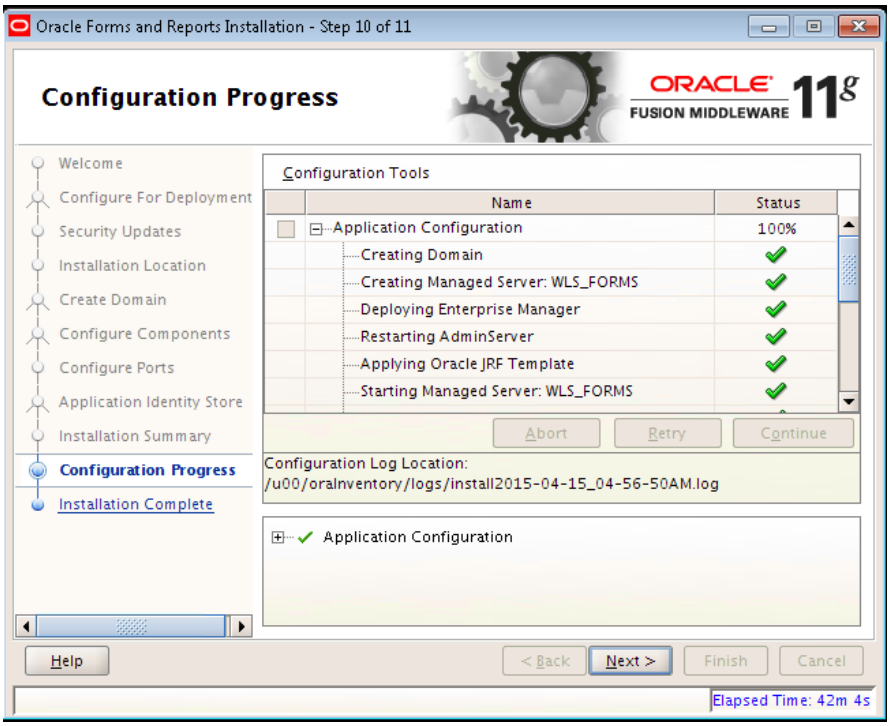


- The Specify Proxy Details window opens. Click **Next**.
- The Specify Application OID window opens. Clear the **Use Application Level Identity Store** checkbox, and click **Next**.

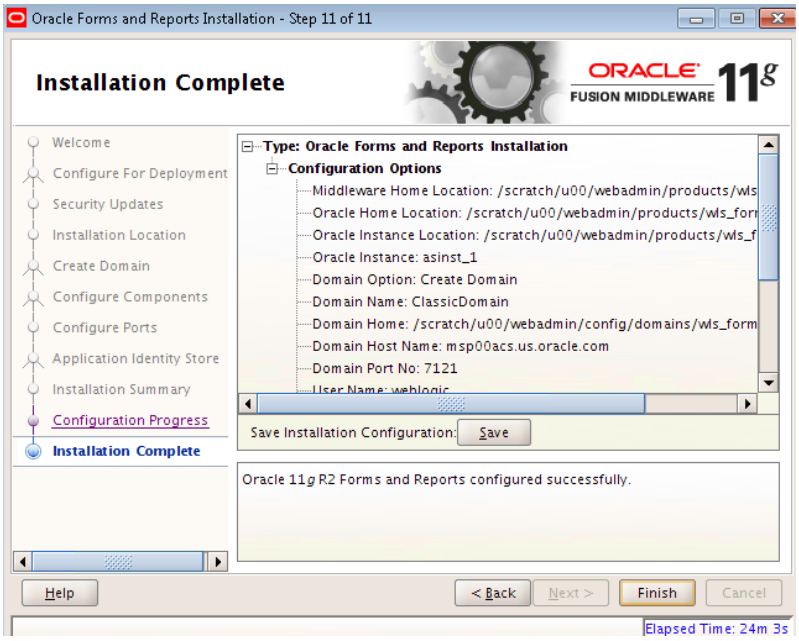
- The Installation Summary window opens. Click **Configure**.



- The Configuration Progress window opens.



- The cluster and managed servers are created. Click **Next**.
- The Installation Complete window opens.

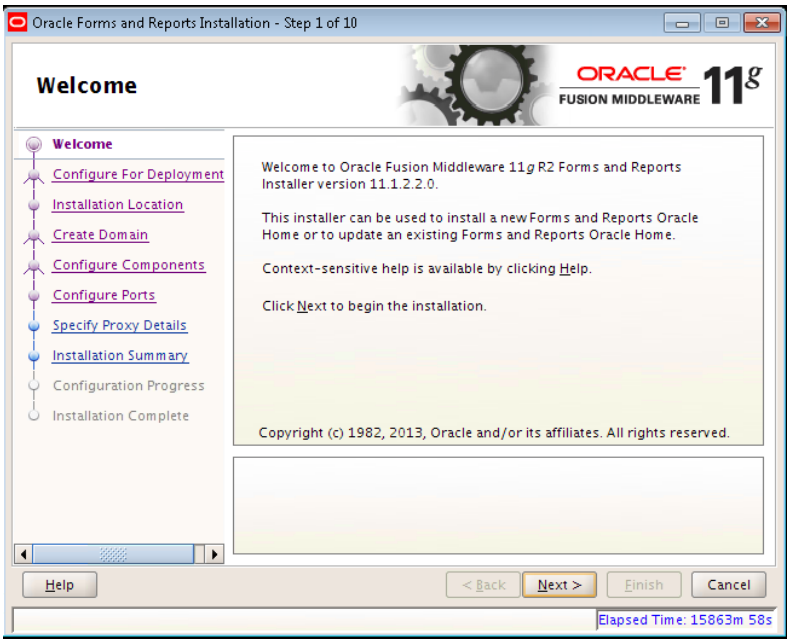


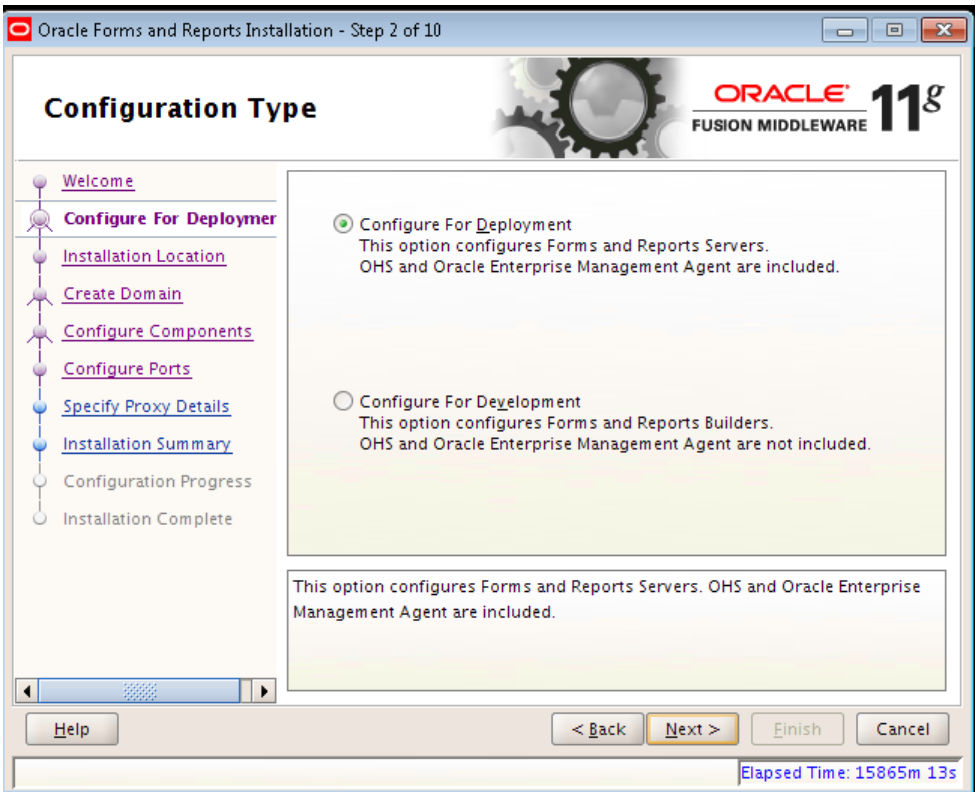
- Save the configuration log because this includes the url addresses.
- Verify the installation by logging into the WebLogic Admin Console.
  http:<hostname.us.oracle.com>:7001<port used>/console
  The classic domain and managed server exist once the installation is done.

Configure Forms on appserver2:

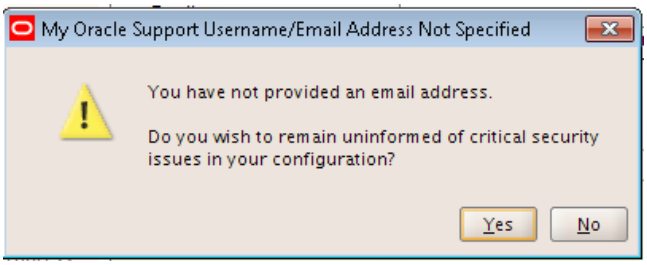
To configure forms on appserver2:

- Run the following command:
  $ORACLE_HOME/bin/config.sh
- The Welcome window opens. Click **Next**.





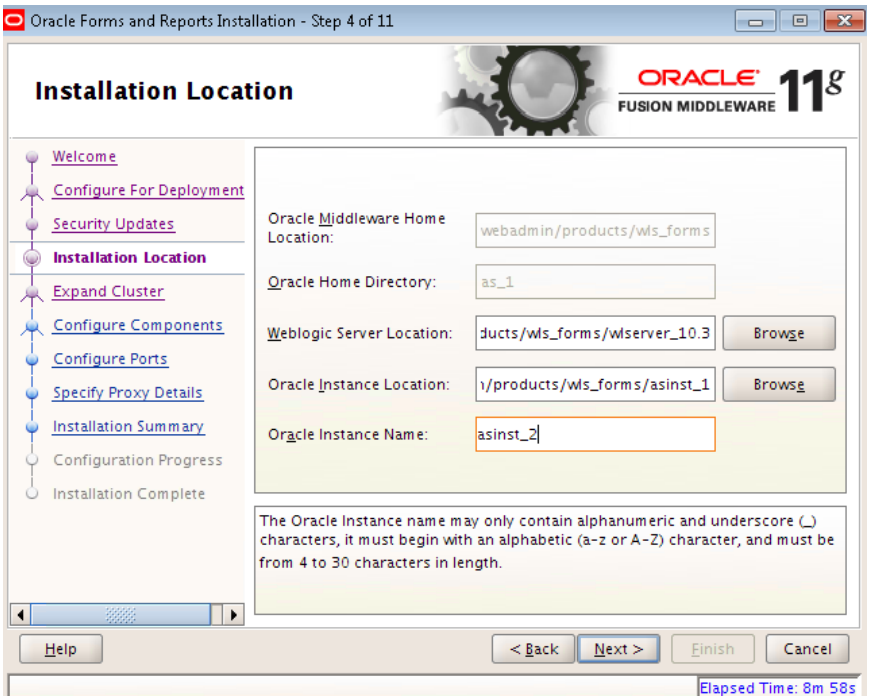
- The Specify Security Updates window opens. Uncheck **I wish to receive security updates via My Oracle Support**, and click **Next**.



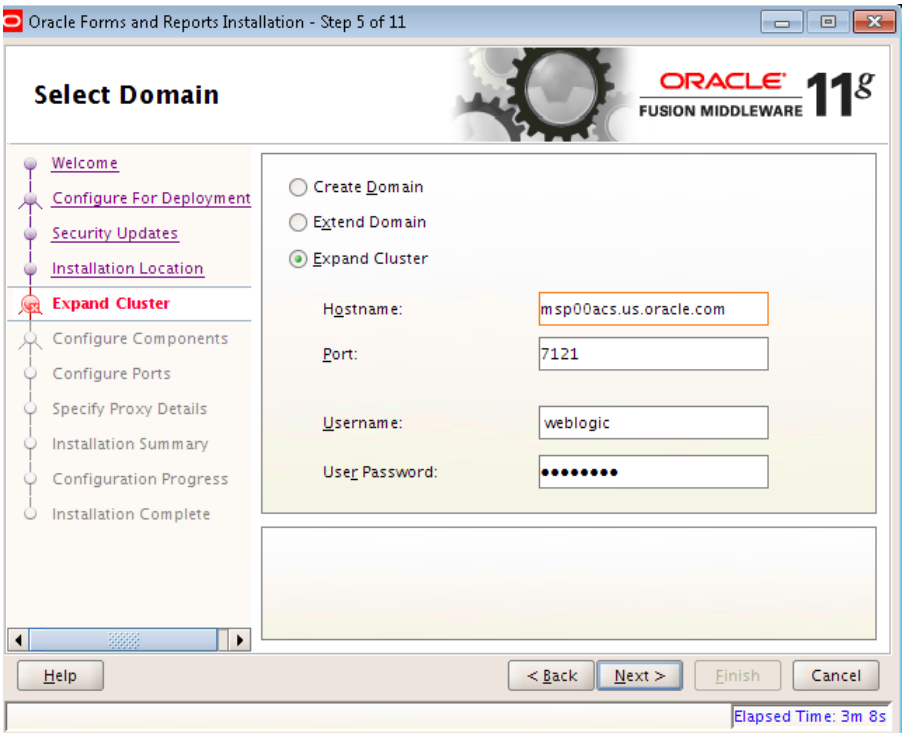
- The Specify Installation Location window opens.

> **Note:** This will create a new instance name as it needs to be different than the one on appserver1. The rest of this document assumes that asinst_2 is used for Oracle Instance Home.

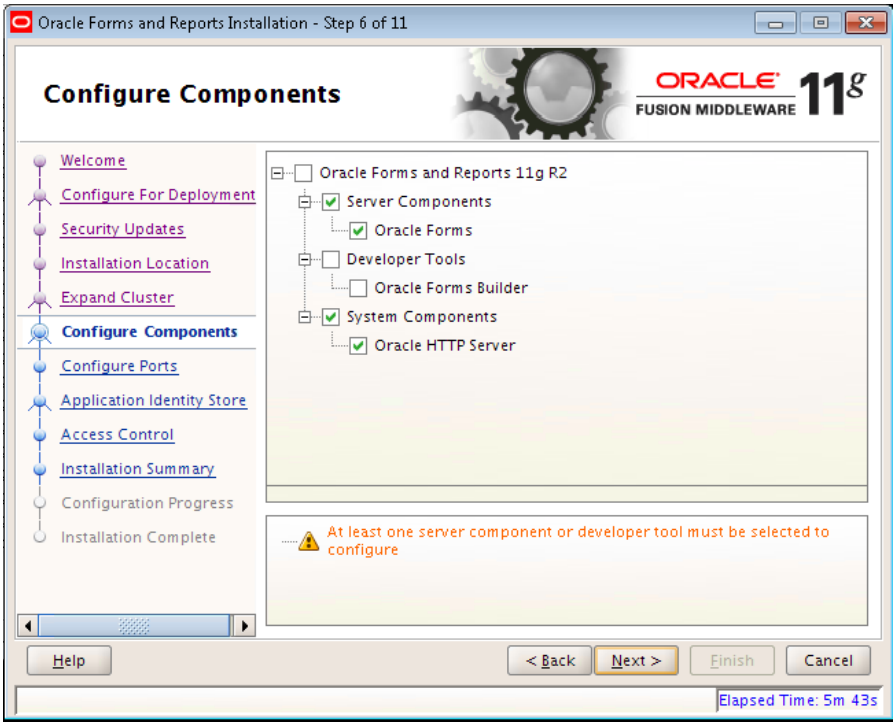
- Click **Next**.



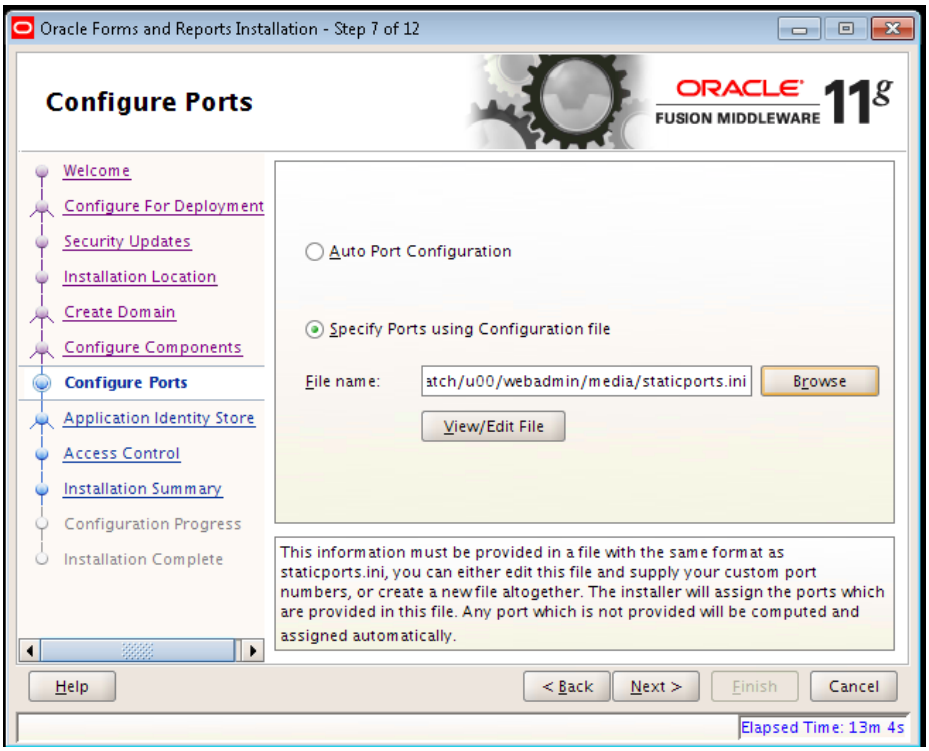
- The Prerequisite Checks window opens. Click **Next**.
- The Select Domain Window opens. Select **Expand Cluster**, enter the **Host name, Admin console port**, **Weblogic user**, and **password** of Appserver1, and click **Next**.



- . The Configure Components window opens. Select **Oracle HTTP Server**, and click **Next**.



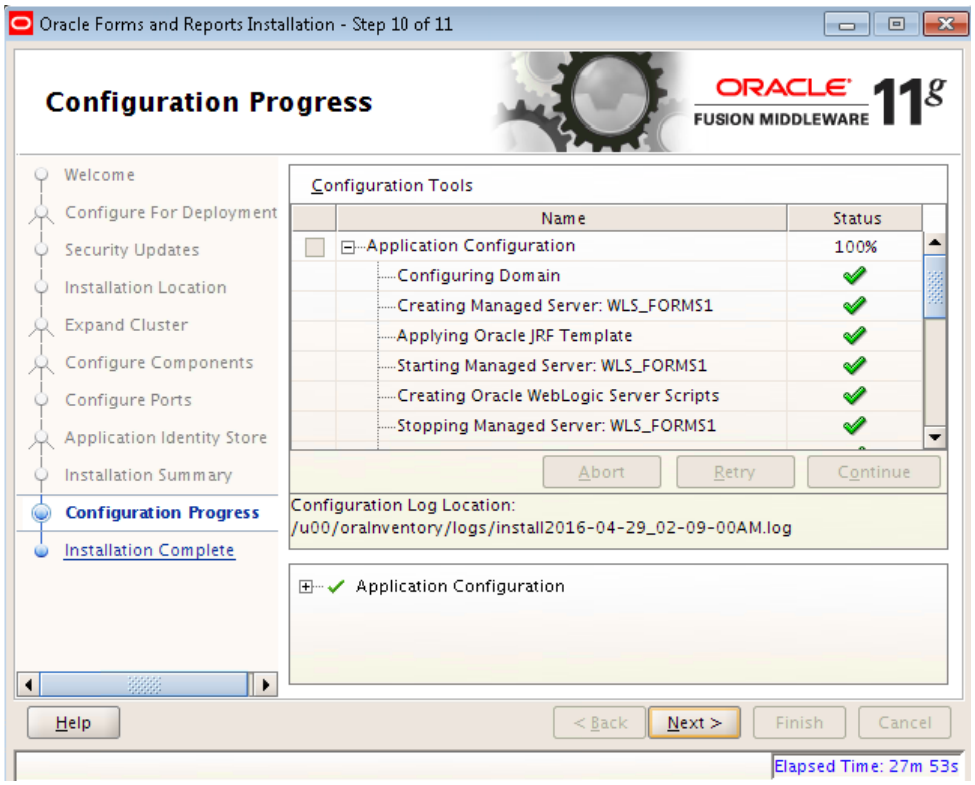
- The Configure Ports window opens. Click **Next**.



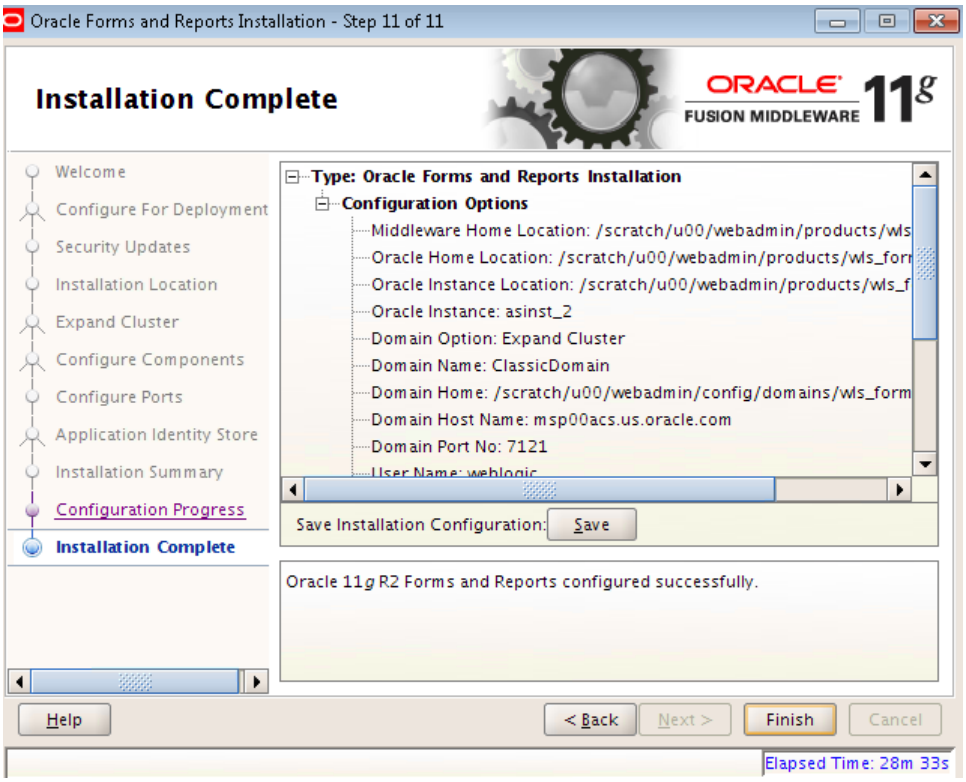
- The Specify Proxy Details window opens. Click **Next**.
- The Specify Application OID window opens. **Uncheck Use Application Level Identity Store**, and click **Next**.

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

- The installation will take some time. Once complete, the Configuration Progress window opens. Click **Next**.



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



- The installation is complete.
- Log into Admin Console to verify new servers have been added to cluster http://<Hostname>:<port>/console

Understanding the Forms Post Installation Tasks

- Change to:
  $ClassicDomain_path/AdminServer/security

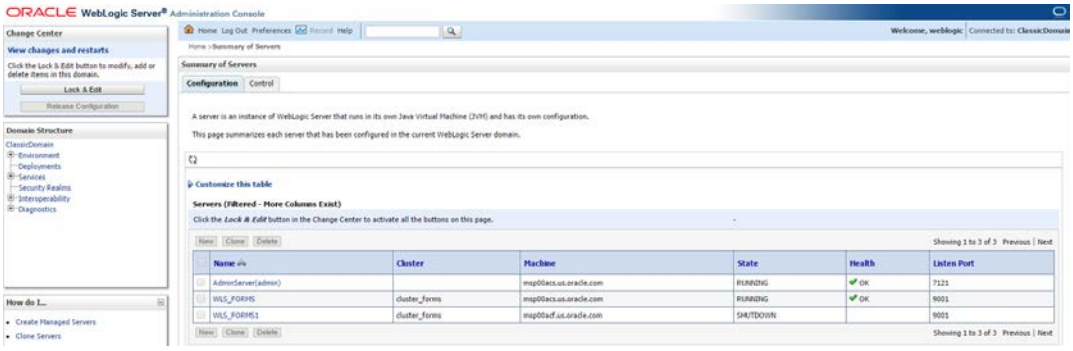
- Create a file boot.properties with the following two lines:
  username=Weblogic
  password=<password for Weblogic>
  The password will be encrypted after the first start.

- Create the boot.properties file in all the other security directories for managed servers, so they can be started from the command line.

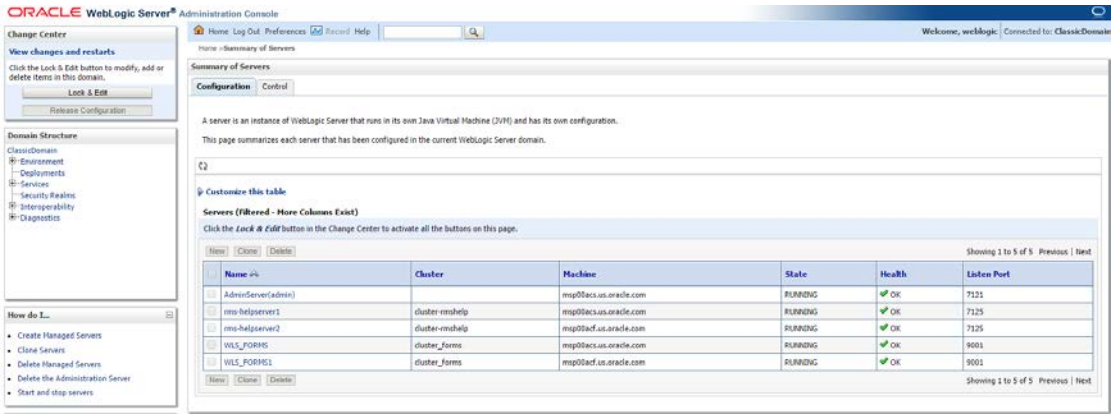
  appserver1:
  $ClassicDomain_path/servers/WLS_FORMS/security

  appserver2:
  $ClassicDomain_path/servers/WLS_FORMS1/security

- Start the managed server of the appserver2



- Configure rms_help server and start the servers after adding boot.properties.



Servers are in running state.

Finalize Forms Installation

To finalize forms installation, complete the following steps on both servers:

- Change directory to: $WLS_HOME/asinst_[12]/config/FRComponent/frcommon/guicommon/tk/admin/

  Note: *asinst_[12]* will be asinst_1 on appserver1, and asinst_2 on appserver2.

- Edit the Tk2Motif.rgb file.

- Uncomment and change the following line:
  !Tk2Motif*fontMapCs: iso8859-2=EE8ISO8859P2 To:

  Tk2Motif*fontMapCs: iso8859-2=AL32UTF8

- Copy the same file to /u00/webadmin/product/wls_forms/as_1/guicommon/tk/admin and $WLS_HOME/as_1/frcommon/templates/tk/config/ in both the host.

- Also check in $WLS_HOME/asinst_1/config/FRComponent/frcommon/guicommon/tk/admin/
- Update tnsnames.ora in $WLS_HOME/asinst_1/config (or $WLS_HOME/asinst_2/config) and $ORACLE_HOME/network/admin

```
retaildb =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCP)(HOST = scan.domain)(PORT = 1521))
```

```
    )
    (CONNECT_DATA =(SERVICE_NAME = retaildb))
    )
```

Scan.domain is the same from the RAC installation document.

Example:

We have tnsnames.ora file under /dba/network/extproc_1521/tnsnames.ora so we need to create a soft link.

```
[webadmin@msp52777 config]$ ln -s /dba/network/extproc_1521/tnsnames.ora ./
                        [webadmin@msp52777 config]$ pwd
/u00/webadmin/products/wls_forms/asinst_1/config
[webadmin@msp52777 config]$ ls -ltr
total 24
drwx------ 3 webadmin rgbudba 4096 Apr 15 05:15 OPMN
drwxr-x--- 2 webadmin rgbudba 4096 Apr 15 05:16 JPS
drwx------ 3 webadmin rgbudba 4096 Apr 15 05:16 OHS
drwx------ 4 webadmin rgbudba 4096 Apr 15 05:16 FRComponent
drwx------ 3 webadmin rgbudba 4096 Apr 15 05:16 FormsComponent
drwx------ 3 webadmin rgbudba 4096 Apr 15 05:16 EMAGENT
lrwxrwxrwx 1 webadmin rgbudba   38 Apr 15 23:01 tnsnames.ora ->
/dba/network/extproc_1521/tnsnames.ora

[webadmin@msp52777 admin]$ pwd
/u00/webadmin/products/wls_forms/as_1/network/admin
[webadmin@msp52777 admin]$ ls -ltr
total 8
-rw-r----- 1 webadmin rgbudba  187 May  7  2007 shrept.lst
drwxr-x--- 2 webadmin rgbudba 4096 Jan 23 04:40 samples
lrwxrwxrwx 1 webadmin rgbudba   38 Apr 15 22:56 tnsnames.ora ->
/dba/network/extproc_1521/tnsnames.ora

Same changes need to be done for appserver2.

Entry of tnsnames.ora file:

dolrc04 =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ENABLE = broken)
      (LOAD_BALANCE = yes)
      (ADDRESS = (PROTOCOL = TCP)(HOST = msp00avyp-r)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = dolrc04)
      (failover_mode=(type=select)(method=basic)
                    (retries=60)(delay=5))
    )
  )
```

- Copy Registry.dat from /u00/webadmin/config/domains/wls_forms/ClassicDomain/config/fmwconfig/servers/WLS_FORMS/applications/formsapp_11.1.2/config/forms/registry/oracle/forms/registry of APPHOST1 to APPHOST2.

  And bounce the complete domain.

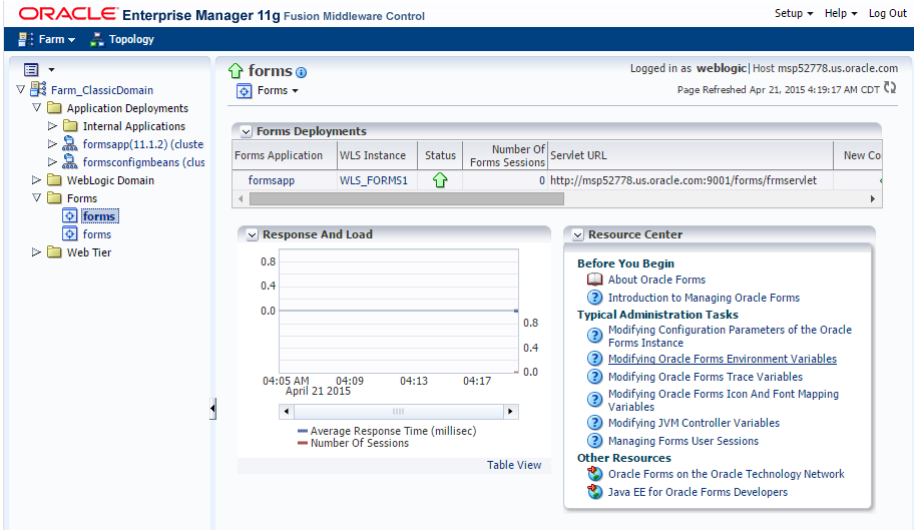
3

Configuring Single Sing On

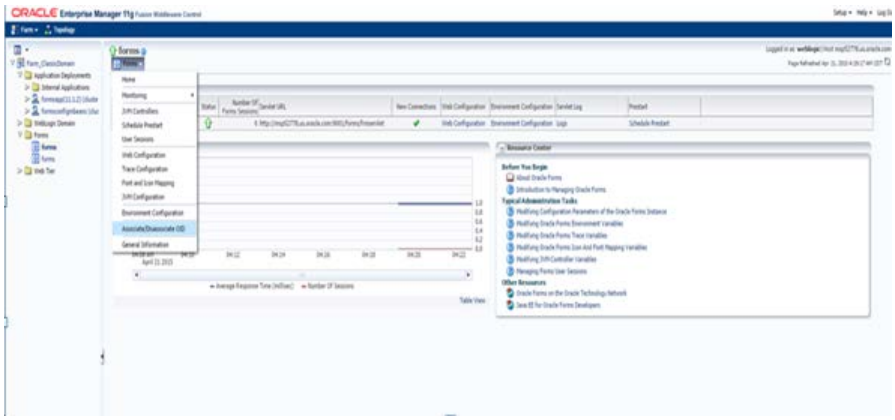
Configure Forms for Single Sign On

This section describes how to configure forms for single sign-on.

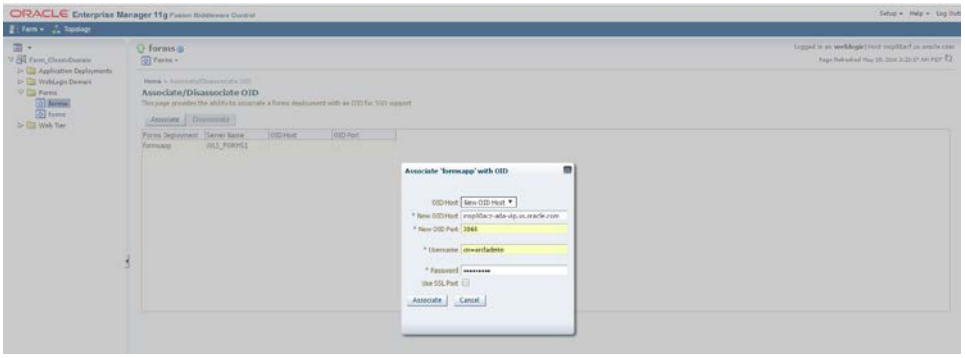
- Connect to the Enterprise Manager on the Forms admin server.
  Example: http://appserver1:7121/em/
  Log in with administrative credentials (for example, WebLogic/<password>).
  For each server, under the left-hand menu, select the first Forms:
  Farm_ClassicDomain
  Forms
  forms
  forms



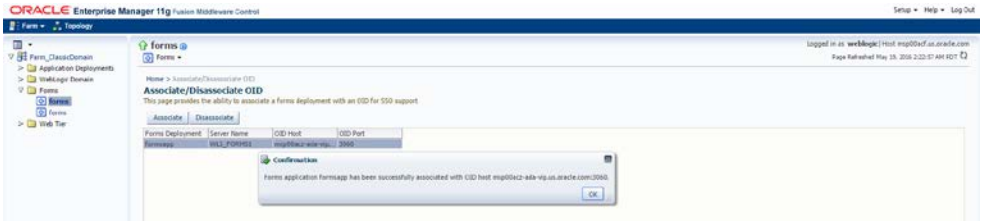
- Right click **forms,** and select **Associate/Disassociate OID**. Click **Associate**.



- Select formsapp, and click **Associate** and update OID details.



- Enter the **LDAP** credentials. Click **Associate**.
- The Associate Confirmation window opens.



- Repeat the previous steps for the second forms server.

Register WebTier with Forms EM

For Oracle Enterprise Manager Fusion Middleware Control to be able to manage and monitor the Oracle HTTP server, you must register the Oracle HTTP server with the domain. To do this, you must register Oracle HTTP Server with WebLogic Server using the following command:

idmhost1$ cd ORACLE_BASE/admin/instance_name/bin

idmhost1$ ./opmnctl registerinstance -adminHost ADMINVHN.mycompany.com \

-adminPort 7121 -adminUsername weblogic

Example: <IDMHOST1>

[webadmin@msp00acz bin]$ pwd

/u00/webadmin/product/fmw/wls_iam/Oracle_WT1/instances/instance1/bin

[webadmin@msp00acs bin]$ ./opmnctl registerinstance -adminHost msp00acs.us.oracle.com -adminPort 7121 -adminUsername weblogic

Command requires login to weblogic admin server (msp00acs.us.oracle.com):

Username: weblogic

Password:

Registering instance

Command succeeded.

You must also run the registration command from idmhost2:

Example: <IDMHOST2>

[webadmin@msp00ada bin]$ ./opmnctl registerinstance -adminHost msp52777.us.oracle.com -adminPort 7121 -adminUsername weblogic

Command requires login to weblogic admin server (msp00ada.us.oracle.com):

Username: weblogic

Password:

Registering instance

Command succeeded.

Update forms config to accept SSO connections

- Navigate to below located on example servers:

  Appserver1:

  $ClassicDomain_Home/config/fmwconfig/servers/WLS_FORMS/applications/formsapp_11.1.2/config

  Appserver2:

  $ClassicDomain_Home/config/fmwconfig/servers/WLS_FORMS1/applications/formsapp_11.1.2/config

- In the Named Configuration section add the following two lines to the context root you want protected:

  Example:

  [rms150hasso]

  ssoMode=webgate

  ssoDynamicResourceCreate=true

  envfile=./develop/rms150ha.env

  width=950

  [rmsfreleaseqa4sso]

  ssoMode=webgate

  ssoDynamicResourceCreate=true

  envfile=./develop/rmsfreleaseqa4.env

  width=950

Configure webtier to redirect forms request

- Edit the mod_wl_ohs.conf in WebTier at location to add the below entry. Add after </IfModule> tag.

  Location in idmhost1

  /u00/webadmin/product/fmw/wls_iam/Oracle_WT1/instances/instance1/config/OHS/ohs1

  Location in idmhost2

  /u00/webadmin/product/fmw/wls_iam/Oracle_WT1/instances/instance2/config/OHS/ohs2

  Entry:

  <Location /forms/frmservlet?* >

  WebLogicCluster msp00acs.us.oracle.com:9001,msp00acf.us.oracle.com:9001

  SetHandler weblogic-handler

  </Location>

Note: Refer to sample entries in the end

- Create forms redirect config file.
- Navigate to below locations in the host where webtier is deployed.

  Location in idmhost1

  /u00/webadmin/product/fmw/wls_iam/Oracle_WT1/instances/instance1/config/OHS/ohs1/moduleconf

  Location in idmhost2

  /u00/webadmin/product/fmw/wls_iam/Oracle_WT1/instances/instance2/config/OHS/ohs2/moduleconf

  Create file forms.conf with entry as below:

```
RewriteEngine on
RewriteRule ^/forms/html/(..*) /workaroundhtml/$1 [PT]
AliasMatch ^/workaroundhtml/(..*) "/u00/webadmin/products/wls_forms/asinst_1/config/FormsComponent/forms/html/$1"

RewriteRule ^/forms/registry/(..*) /workaroundregistry/$1 [PT]
AliasMatch ^/workaroundregistry/(..*) "/u00/webadmin/config/domains/wls_forms/ClassicDomain/config/fmwconfig/servers/WLS_FORMS/applications/formsapp_11.1.2/config/forms/registry/$1"

<Location /forms>
SetHandler weblogic-handler
 WebLogicCluster msp00acs.us.oracle.com:9001,msp00acf.us.oracle.com:9001
 DynamicServerList OFF
 WLCookieName JSESSIONID_FORMS
</Location>
```

- Restart webtier to make the changes permanent.

  [webadmin@msp00acz bin]$ pwd

  /u00/webadmin/product/fmw/wls_iam/Oracle_WT1/instances/instance1/bin

  [webadmin@msp00acz bin]$ ./opmnctl stopall

  opmnctl stopall: stopping opmn and all managed processes...

  [webadmin@msp00acz bin]$ ./opmnctl startall

  opmnctl startall: starting opmn and all managed processes...

  [webadmin@msp00ada bin]$ ./opmnctl status -l

  Processes in Instance: instance1

ias-component	process-type	pid	Status	uid	memused	uptime	ports
ohs1	OHS	31261	Alive	65278862	1301000	0:00:09	https:7780,https:7780,http:7777

Post Install steps for Forms SSO set up:

- Log into forms server on both boxes

  cd /scratch/u00/webadmin/config/domains/wls_forms/ClassicDomain/deploymentplans/formsapp/11.1.2
- Take a back up

  cp plan.xml plan.xmlbk1
- Update the plan.xml
  - Add the following lines to the file. The new lines are added under the <application-name> --> <variable-definition> element.

    <variable>

    <name>NewCookieName</name>

    <value>JSESSIONID_FORMS</value>

    </variable>
  - Then further down the file (towards the bottom of the file) , add the following lines within the formsweb.war <module-name>

  Do it as part of variable assignments prior to </module-descriptor.end tag for formsweb.war

  <variable-assignment>

  <name>NewCookieName</name>

  <xpath>/weblogic-web-app/session-descriptor/cookie-name</xpath>

  </variable-assignment>
  - Save the file
- Redeploy the Oracle Forms application (formsapp.ear) so that it picks up changes made in plan.xml.

Actual File changes below

```
<?xml version='1.0' encoding='UTF-8'?>
<!--
 Copyright (c) 2009, 2013, Oracle and/or its affiliates. All rights reserved.
   NAME
     formsapp-deployment-plan.xml
   DESCRIPTION
     Forms J2EE application deployment plan.
-->
<deployment-plan xmlns="http://xmlns.oracle.com/weblogic/deployment-plan"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xmlns.oracle.com/weblogic/deployment-plan
http://xmlns.oracle.com/weblogic/deployment-plan/1.0/deployment-plan.xsd">
  <variable-definition>
   <variable>
      <name>vd-/scratch/u00/webadmin/products/wls_forms/as_1/forms</name>
      <value>/scratch/u00/webadmin/products/wls_forms/as_1/forms</value>
```

```
   </variable>
   <variable>
      <name>vd-
/scratch/u00/webadmin/config/domains/wls_forms/ClassicDomain/config/fmwconfig/serv
ers/WLS_FORMS/applications/formsapp_11.1.2/config/forms</name>

<value>/scratch/u00/webadmin/config/domains/wls_forms/ClassicDomain/config/fmwconf
ig/servers/WLS_FORMS/applications/formsapp_11.1.2/config/forms</value>
   </variable>
<variable>
<name>NewCookieName</name>
<value>JSESSIONID_FORMS</value>
</variable>
  </variable-definition>
  <application-name>formsapp</application-name>
  <module-override>
    <module-name>formsapp.ear</module-name>
    <module-type>ear</module-type>
    <module-descriptor external="false">
      <root-element>weblogic-application</root-element>
      <uri>META-INF/weblogic-application.xml</uri>
    </module-descriptor>
    <module-descriptor external="false">
      <root-element>application</root-element>
      <uri>META-INF/application.xml</uri>
    </module-descriptor>
    <module-descriptor external="true">
      <root-element>wldf-resource</root-element>
      <uri>META-INF/weblogic-diagnostics.xml</uri>
    </module-descriptor>
  </module-override>
  <module-override>
    <module-name>formsweb.war</module-name>
    <module-type>war</module-type>
    <module-descriptor external="false">
      <root-element>weblogic-web-app</root-element>
      <uri>WEB-INF/weblogic.xml</uri>
<variable-assignment>
<name>NewCookieName</name>
<xpath>/weblogic-web-app/session-descriptor/cookie-name</xpath>
</variable-assignment>
      <variable-assignment>
        <name>vd-/scratch/u00/webadmin/products/wls_forms/as_1/forms</name>
        <xpath>/weblogic-web-app/virtual-directory-mapping/[url-
pattern="java/*"]/local-path</xpath>
      </variable-assignment>
      <variable-assignment>
        <name>vd-/scratch/u00/webadmin/products/wls_forms/as_1/forms</name>
        <xpath>/weblogic-web-app/virtual-directory-mapping/[url-
pattern="webutil/*"]/local-path</xpath>
      </variable-assignment>
      <variable-assignment>
        <name>vd-
/scratch/u00/webadmin/config/domains/wls_forms/ClassicDomain/config/fmwconfig/serv
ers/WLS_FORMS/applications/formsapp_11.1.2/config/forms</name>
        <xpath>/weblogic-web-app/virtual-directory-mapping/[url-
pattern="registry/*"]/local-path</xpath>
      </variable-assignment>
    </module-descriptor>
    <module-descriptor external="false">
      <root-element>web-app</root-element>
      <uri>WEB-INF/web.xml</uri>
    </module-descriptor>
```

```
  </module-override>
</deployment-plan>
```

Note: Please launch the forms SSO URL.

Example: msp00acs-acf-vip.us.oracle.com:7777/forms/frmservlet?config=rms150hasso

4

Preparing and Installing Retail Java Applications

Before proceeding, you must install Oracle WebLogic 12.1.3 using Fusion Middleware Infrastructure with ADF.

These are the other prerequisites before installing Oracle Retail Invoice Matching application:

- Install WebLogic domain with ADF and EM (Enterprise Manager). Managed server used to install Allocation must be set up with ADF libraries extended.
- Set up MDS schema Datasource in Enterprise Manager (EM).
- Configuration of OID Authenticator in WebLogic domain
- Load LDIF files in LDAP to create Users and Roles

It is assumed Oracle database has already been configured and loaded with the appropriate RMS and Oracle Retail Invoice Matching schemas for your installation.

MDS schema, OPSS schema and other required schemas for ADF must be created using RCU utility. Steps to create the schemas are explained in this document.

Installing a separate domain as part of ADF configuration is recommended.

The Oracle Retail Invoice Matching application is deployed to a managed server (example: reim-server) which is created inside the new domain (example: REIMDomain). This managed server must contain all the ADF libraries.

Middleware Infrastructure and WebLogic Server 12c (12.1.3) Installation

Create a directory to install the WebLogic (this will be the MW_HOME):

Example: mkdir -p /u00/webadmin/products/wls_retail

Set the MW_HOME, JAVA_HOME, and DOMAIN_HOME environment variables:

- ORACLE_HOME should point to your WebLogic installation.
- JAVA_HOME should point to the Java JDK 1.7+. This is typically the same JDK which is being used by the WebLogic domain where application is getting installed.
- DOMAIN_HOME should point to the full path of the domain into which application will be installed.

Example:

```
$ export MW_HOME=/u00/webadmin/products/wls_retail
$ export DOMAIN_HOME=/u00/webadmin/config/domains/wls_retail/APPNAMEDomain
$ export JAVA_HOME=/u00/webadmin/products/jdk_java
(This should point to the Java which is installed on your server)
$ export PATH=$JAVA_HOME/bin:$PATH
```

Going forward we will use the above references for further installations.

- Set the system environment variable MW_HOME to the new directory then cd to location where the jar is downloaded and run the installer using the following command:

  ```
  ./ java -jar ./fmw_12.1.3.0.0_infrastructure.jar
  ```

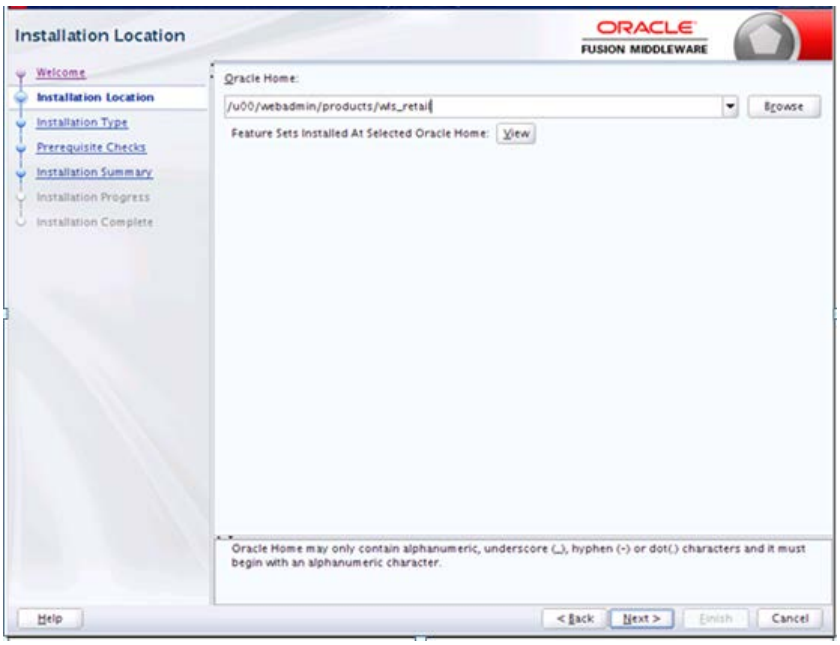
- Welcome screen appears. Click **Next**.

- Enter the following and click **Next**.

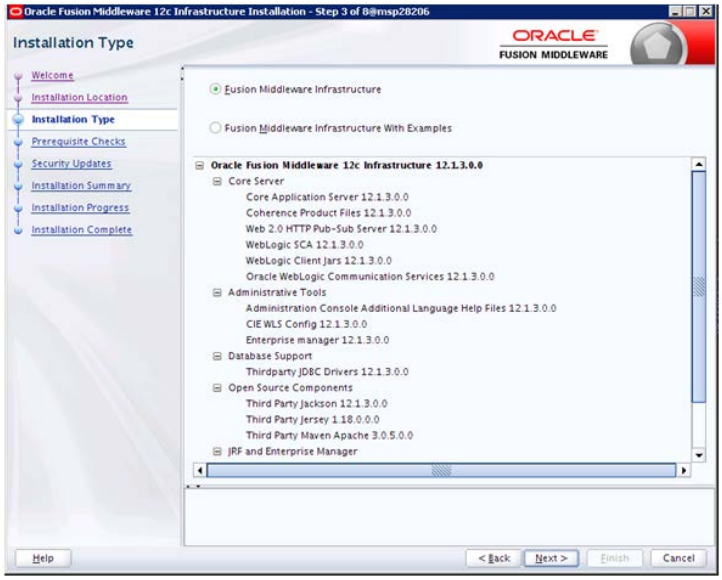
  Oracle home =<Path to the middleware home>

  Example:

  /u00/webadmin/products/wls_retail

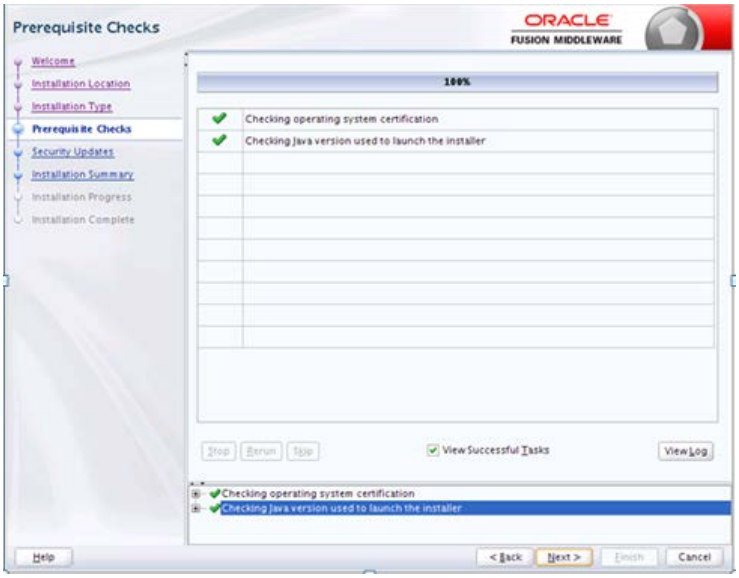


- Select the **Fusion Middleware Infrastructure** install type. Click **Next**.



- This screen will verify that the system meets the minimum necessary requirements. Click **Next**.

- Click **Next**.



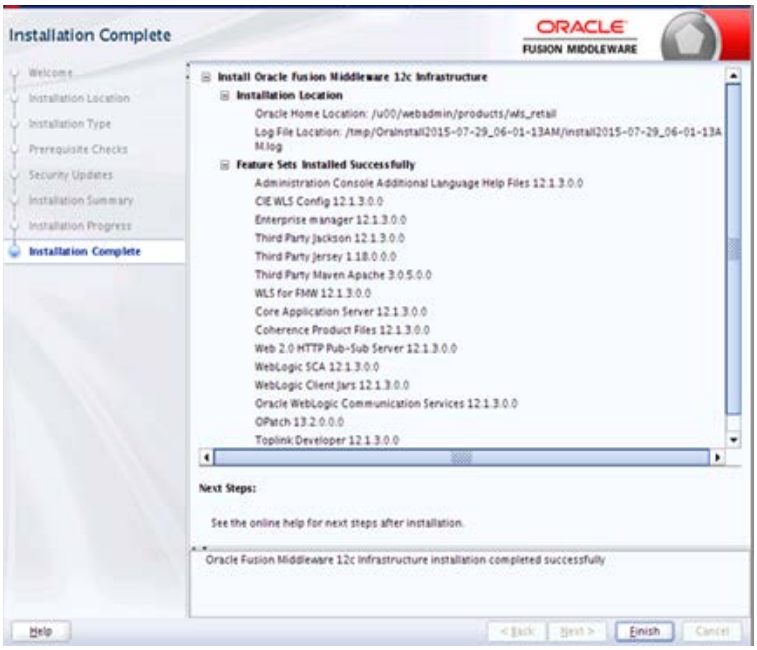
- If you already have an Oracle Support account, use this screen to indicate how you would like to receive security updates.
- If you do not have one or if you want to skip this step, clear the check box and verify your selection in the follow-up dialog box, and click **Next**.

Security Updates
ORACLE
FUSION MIDDLEWARE
Welcome
Installation Location
Installation Type
Prerequisite Checks
Security Updates
Installation Summary
Installation Progress
Installation Complete
Provide your email address to be informed of security issues, install the product and initiate configuration manager. View details.
Email:
Easier for you if you use your My Oracle Support email address/username.
I wish to receive security updates via My Oracle Support.
My Oracle Support Password:
Help
< Back
Next >
Finish
Cancel

Security Updates
ORACLE
FUSION MIDDLEWARE
Welcome
Installation Location
Installation Type
Prerequisite Checks
Security Updates
Installation Summary
Installation Progress
Installation Complete
Provide your email address to be informed of security issues, install the product and initiate configuration manager. View details.
Email:
Easier for you if you use your My Oracle Support email address/username.
My Oracle Support Username/Email Address Not Specified@m...
You have not provided an email address.
Do you wish to remain uninformed of critical security issues in your configuration?
Yes
No
Help
< Back
Next >
Finish
Cancel

- Click **Next**.

- Click **Finish**.



Apply Security Patch for 12.1.3 Weblogic version

Once the 12.1.3 weblogic is installed we need to apply security patch for 12.1.3 Weblogic Version. Please download the patch from below link.

https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=2140512651210 83&id=2075927.1&_afrWindowMode=0&_adf.ctrl-state=sdqghll78_4

- Please download the 12.1.3.0PSU 12.1.3.0.5 (Patch 21370953) + Patch 22248372 for CVE-2015-4852 and copy to the media directory and unzip.

- Before applying patch need to export some of the environment variables as below in both the host.

  export JAVA_HOME=/u00/webadmin/products/jdk_java
  export PATH=$JAVA_HOME/bin:$PATH
  export ORACLE_HOME=/u00/weblogic/products/wls_retail
  export PATH=$ORACLE_HOME/OPatch:$PATH

- Change directory to the patch directory and execute opatch apply.

  Eg: msp00acs.us.oracle.com:[] /u00/webadmin/media/PATCHES_13MAY2016/21370953> **opatch apply**

- It will check Is the local system ready for patching? [y|n]. Please update 'y' and proceed. The patch will be applied successfully.

- Please proceed with the same steps for second patch and complete in appserver2 as well.

Install RCU Database Schemas

The RCU database schemas are required for the installation of retail application and configuration of domain.

> **Note**: You need 'SYS' user privileges to install the RCU database schemas.

The following steps are provided for the creation of the database schemas:

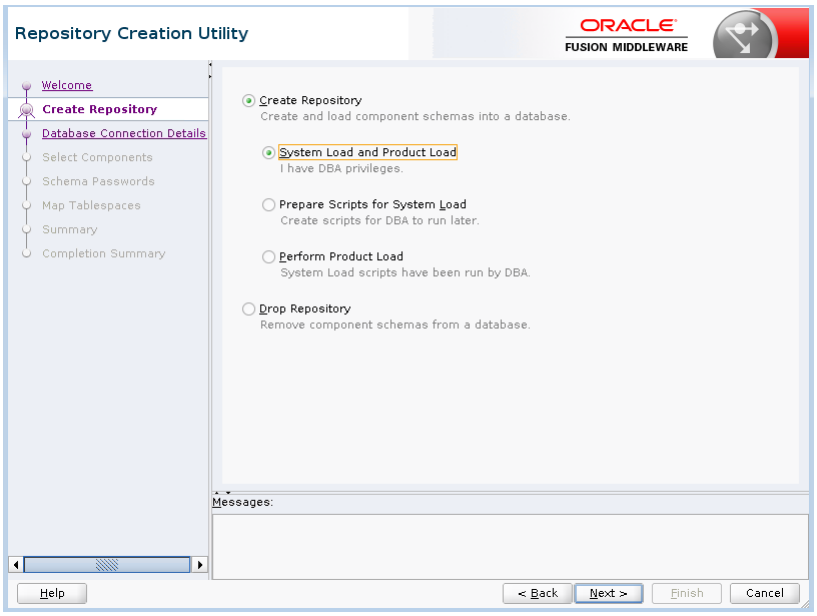
- Navigate to the directory into which RCU is installed.

  For example:

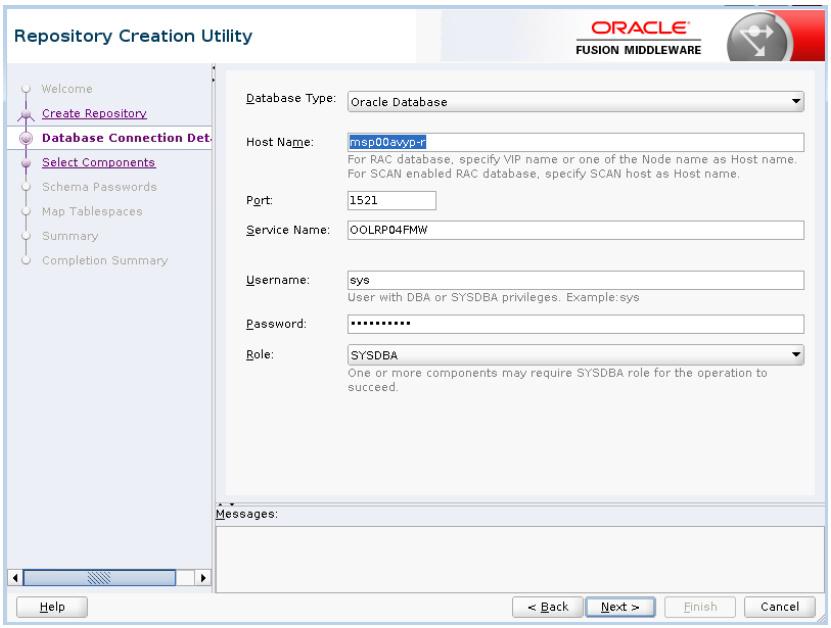
  <MW_HOME>/oracle_common/bin/

  Run "./rcu"
- Click **Next**.

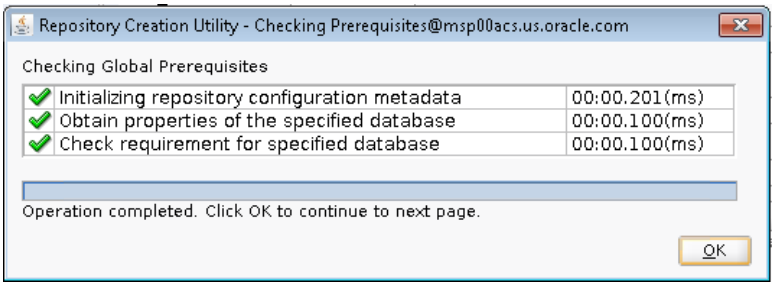
- Select Create Repository and System Load and Product Load. Click **Next**.



- Enter database connection details:
  - Database Type: Oracle Database
  - Host Name: scan address
  - Port: 1521
  - Service Name: dbservicename
  - Username: sys
  - Password: <syspassword>
  - Role: SYSDBA



- Click **Next**. The Installer checks prerequisites.
- When the prerequisite checks are complete, click **OK**. Click **Next**.



- Click the Create a new prefix option, the prefix name for your schemas should be unique to your application environment.

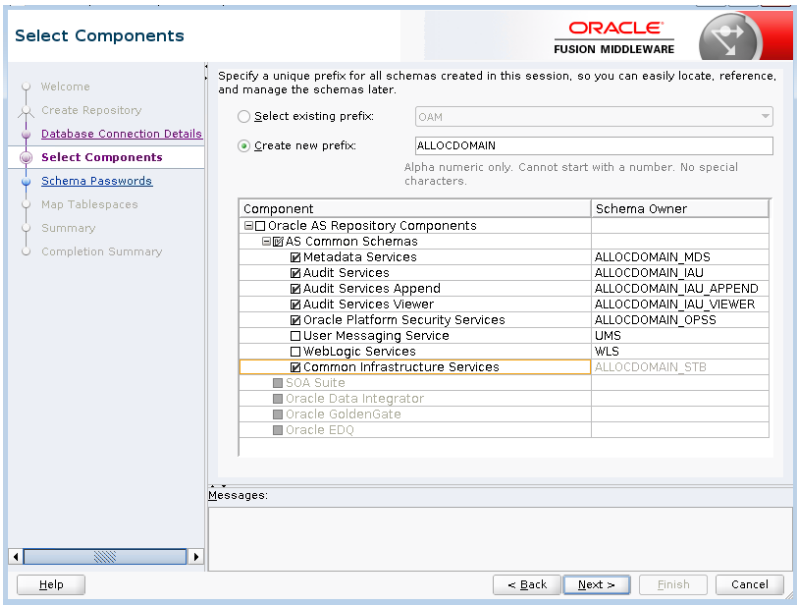
  Example: ReIM, ALLOC, ReSA, etc

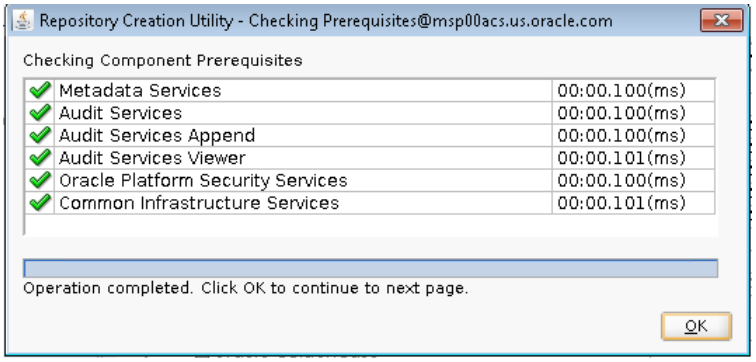
- Select the components to create:
  - Meta Data ServicesOracle Platform Security Services

    Note: Once OPSS schema is selected, the following dependent schemas will get selected automatically.

  - Audit Services
  - Audit Services Append
  - Audit Services Viewer

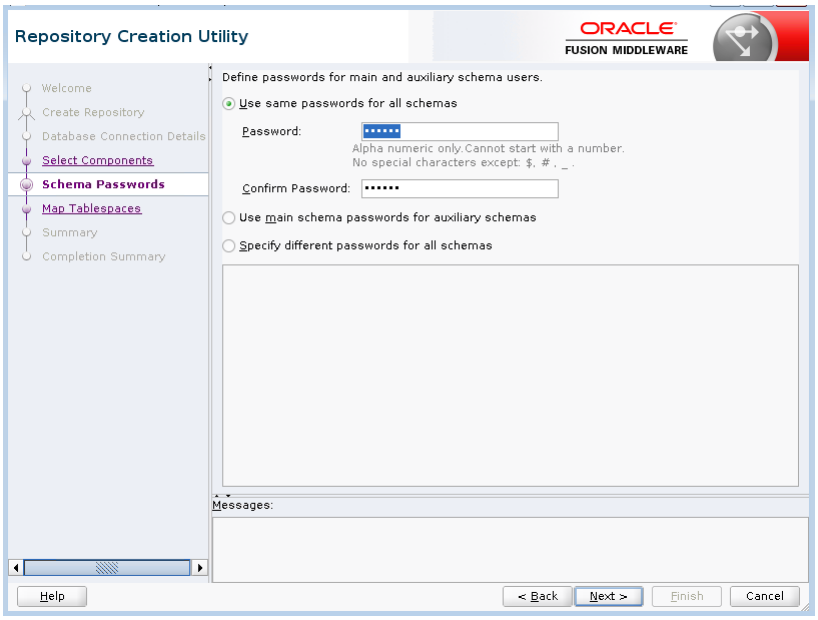
    Note: STB schema will be already selected as part of the Common Infrastructure component.



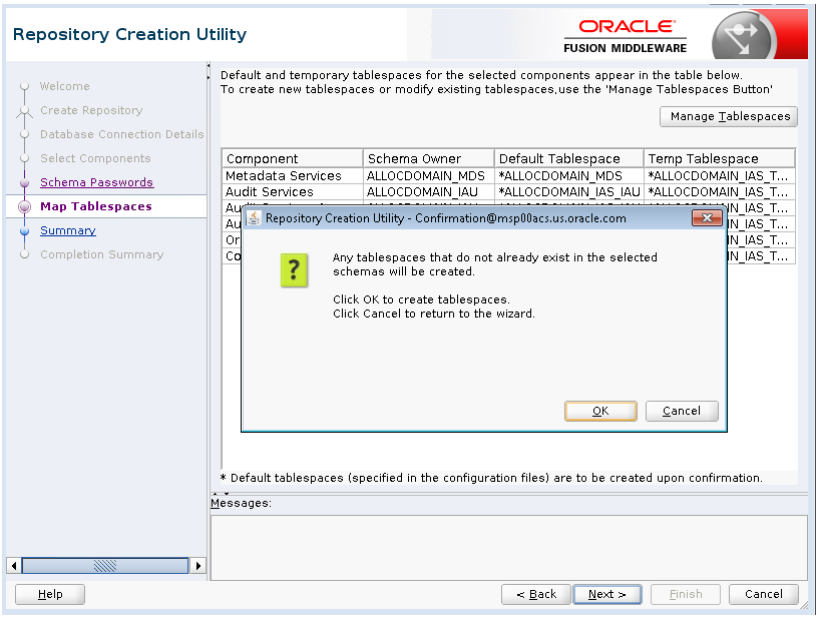


- Select Use same passwords for all schemas.
- Enter your password.

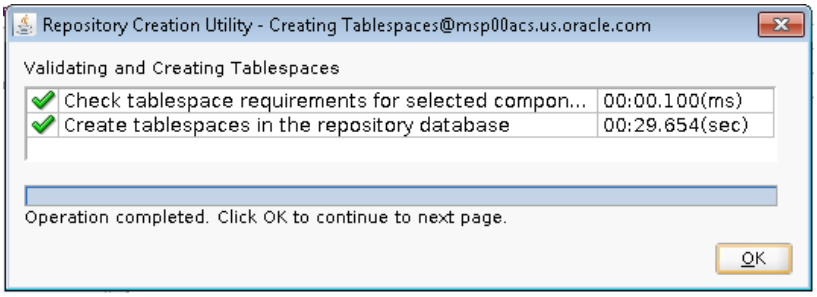
> **Note**: This password is needed at the time of ADF domain creation.



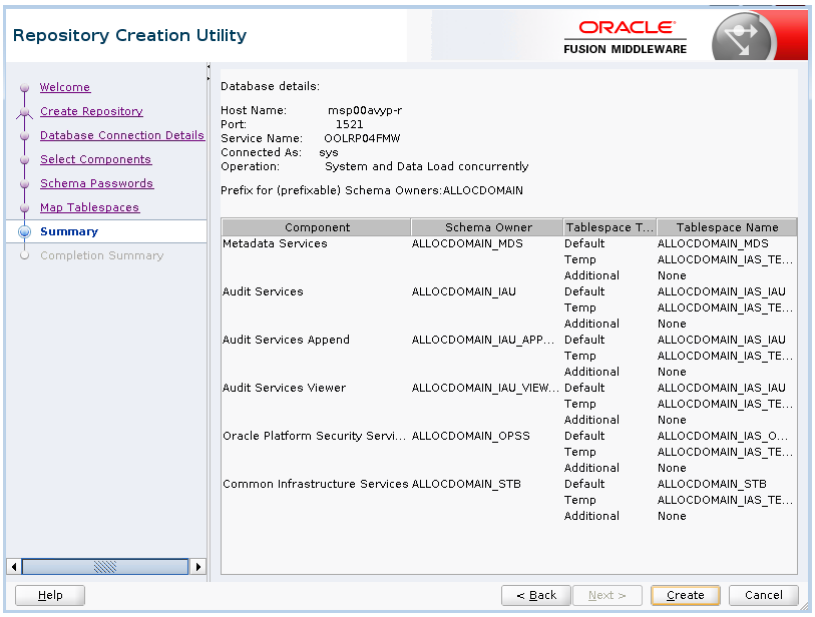
- Click **Next**. A Repository Creation notification will appear. Click **OK**.



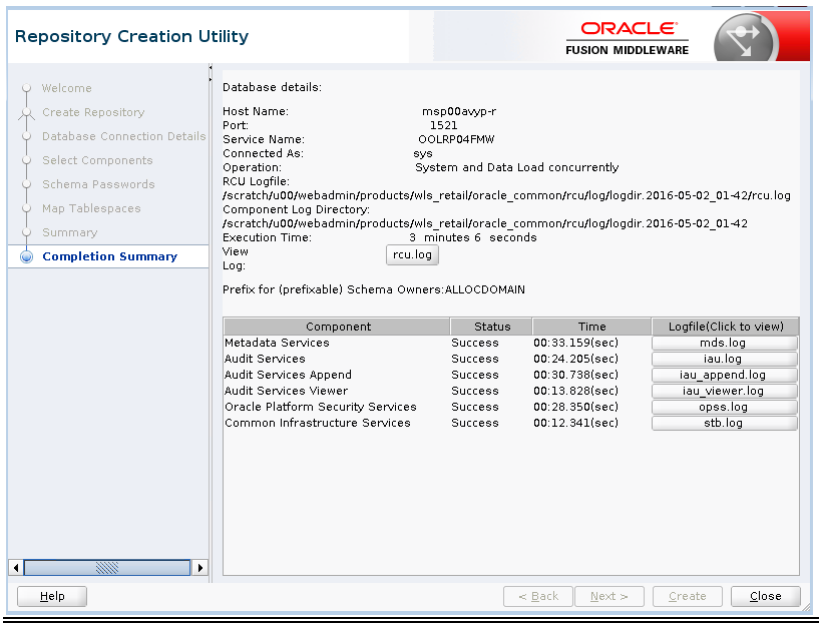
- Tablespaces are created, and the progress will be displayed in a pop-up notification. When the operation is completed, click **OK**.



- Click Create. The schema is created.

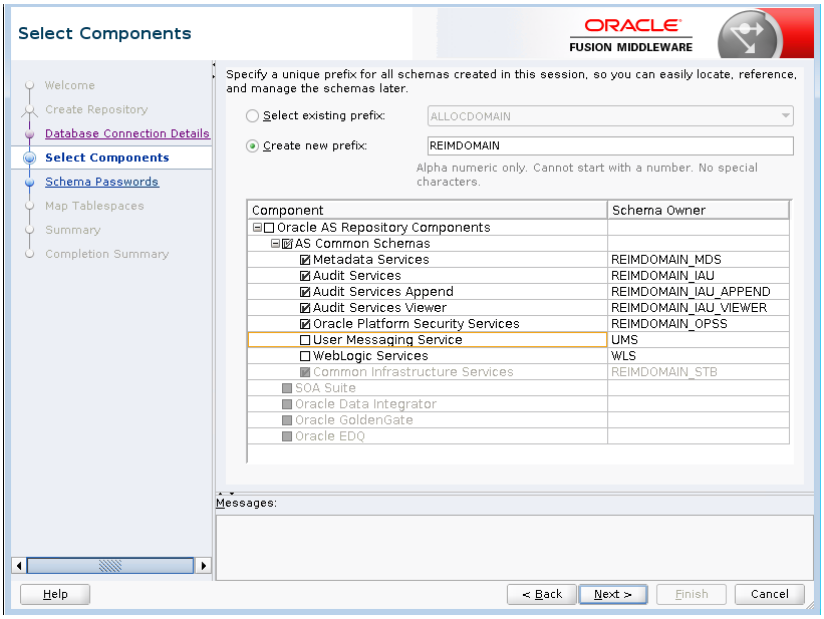


- Upon successful creation of database schemas, a screen will appear with all the schemas created .
- Click **Close**.

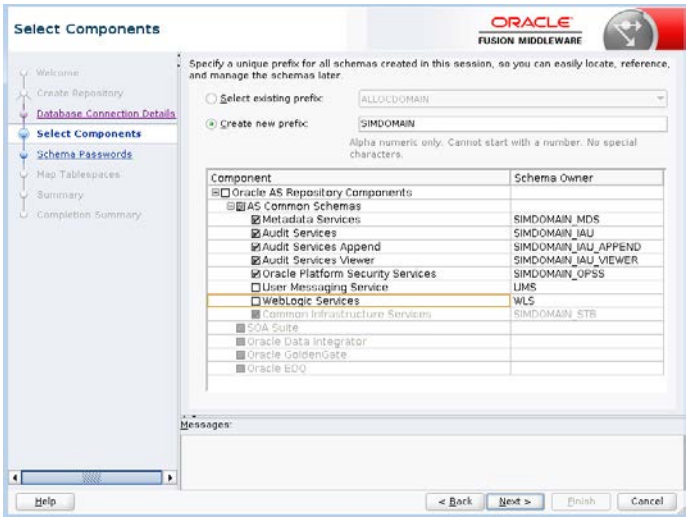


Note: The above RCU example for ALLOC and in the same manner need to create RCU for REIM, RESA,SIM and RPM.

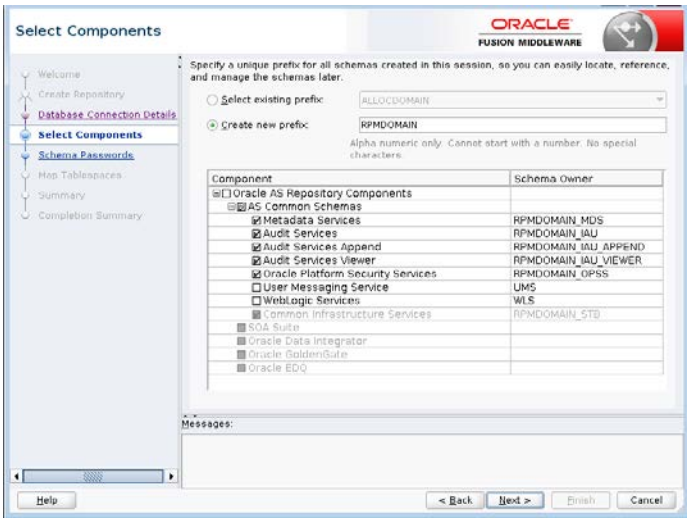
REIM RCU screen:



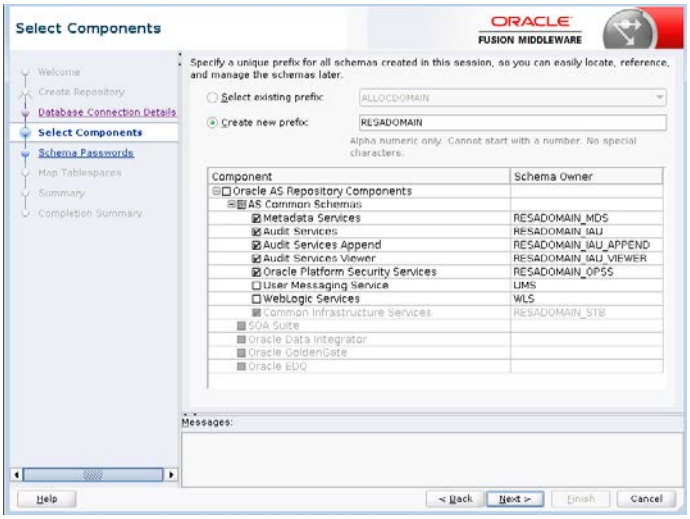
SIM RCU screen:



RPM RCU screen:



RESA RCU screen:



Create a New ADF Domain (with managed server and EM)

To create a new domain and managed server with ADF libraries and EM, follow the below steps:

- Set Environment Variables:

  export JAVA_HOME=<JDK_HOME>

  (Example:/u00/webadmin/products/jdk_java) [JDK_HOME is the location where jdk has been installed)

  export PATH=$JAVA_HOME/bin:$PATH

  export ORACLE_HOME=<MW_HOME>/oracle_common (Example:/u00/webadmin/products/wls_retail/oracle_common)

  cd $MW_HOME/oracle_common/common/bin

  (MW_HOME is the location where Weblogic has been installed.)

- Run the following command:

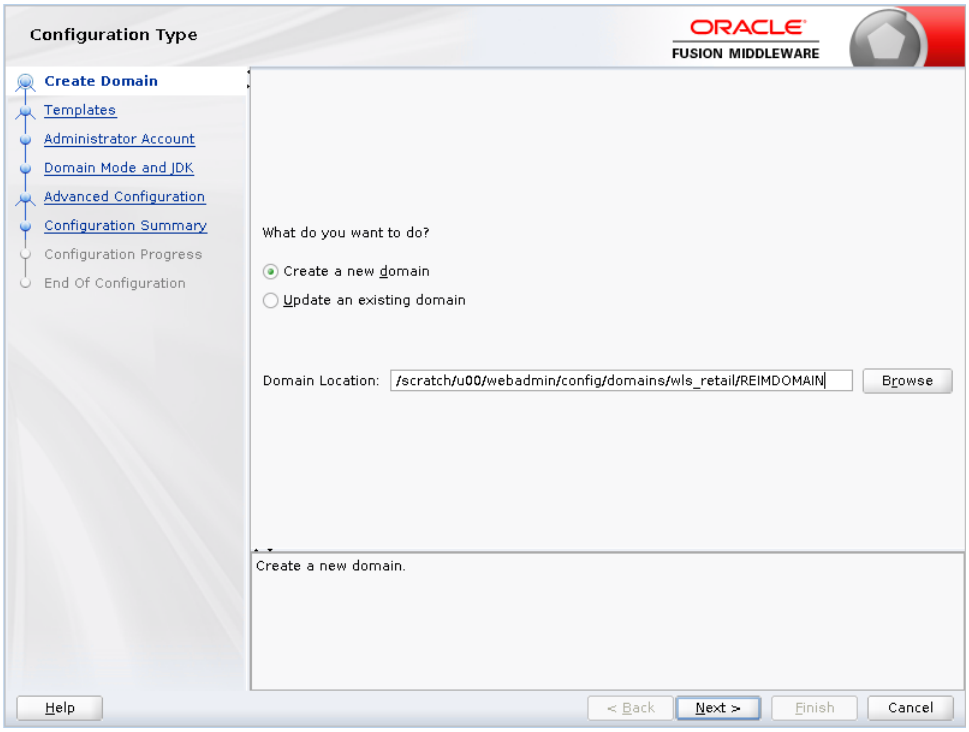
  ./config.sh

- Select **Create a new domain**.

  Domain location: Specify the path to the <DOMAIN_HOME>
  Example:/u00/webadmin/config/domains/wls_retail/REIMDomain

  NOTE: Below screen are example for REIMDomain. In the same manner the other ALLOC/RESA/SIM/RPM domain can be created.

- Click **Next**.



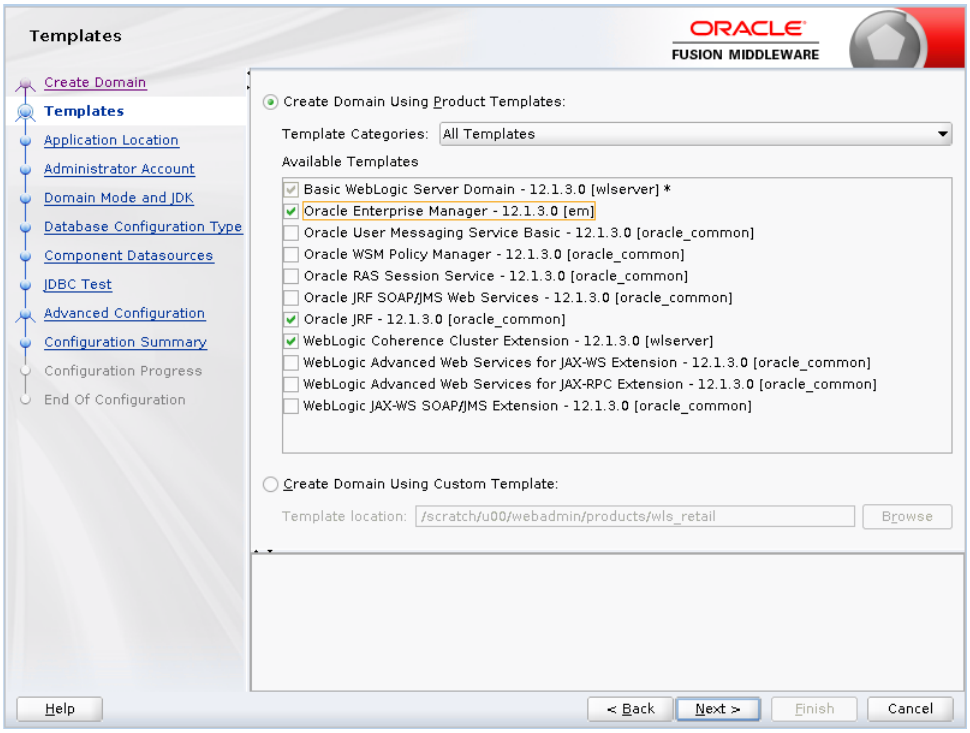
- Select **Create Domain Using Product Templates**.
- Check the Oracle Enterprise Manager component.

Note: When the Oracle Enterprise Manager component is selected, the following dependent components are selected automatically:

Oracle JRF

Weblogic Coherence Cluster Extension

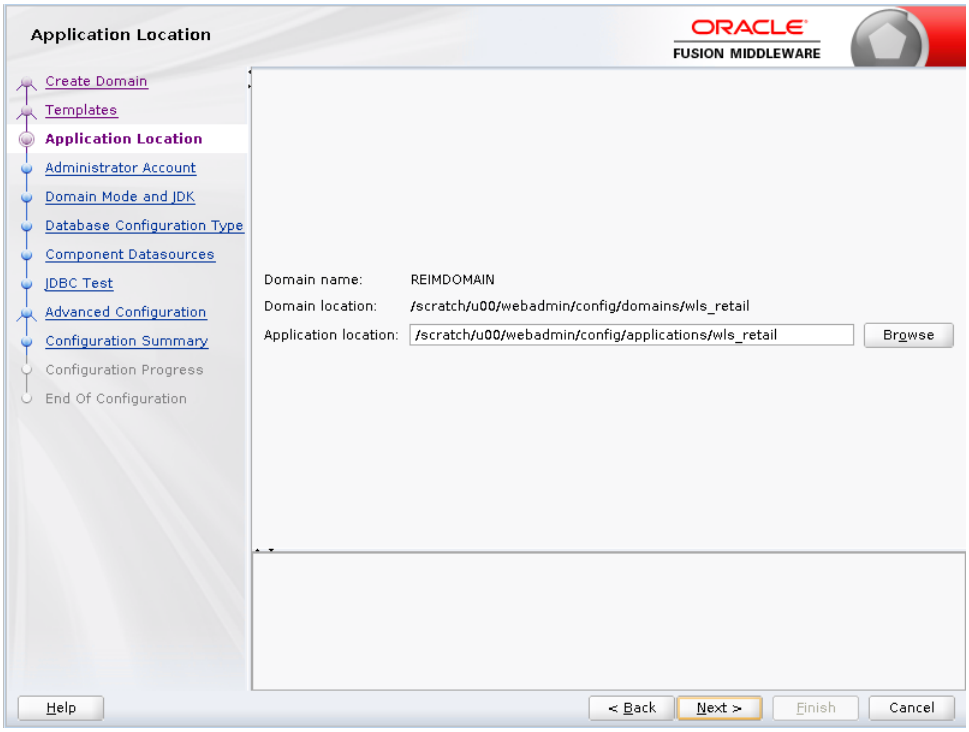
- Click **Next**.



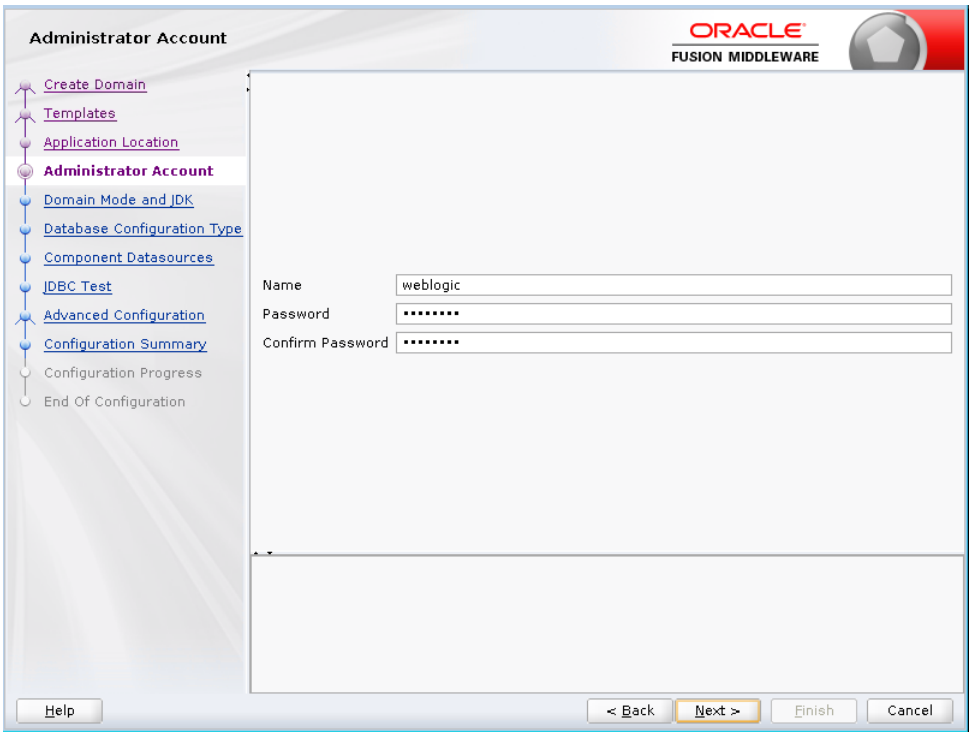
Application location: Application directory location. Example: /u00/webadmin/config/applications/wls_retail/REIMDomain

- Click **Next**.

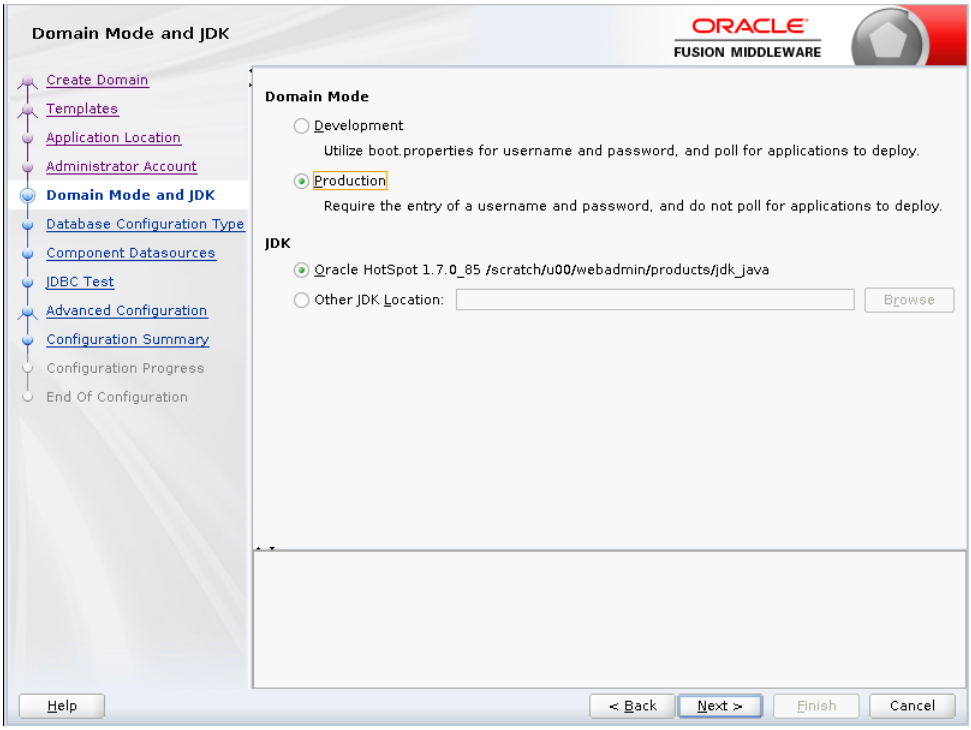
.



- Provide the WebLogic administrator credentials and click **Next**:
  - Username: <weblogic administrator user>
  - Password: <Password for weblogic administrator user>

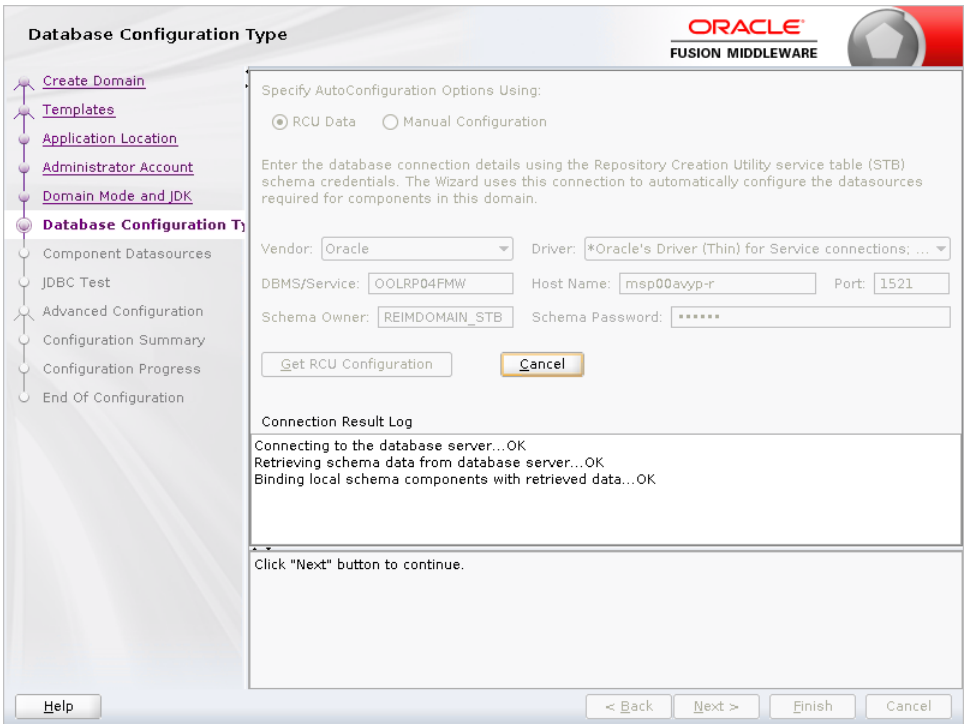


- Select Domain Mode as Production and the JDK to use (as applicable).

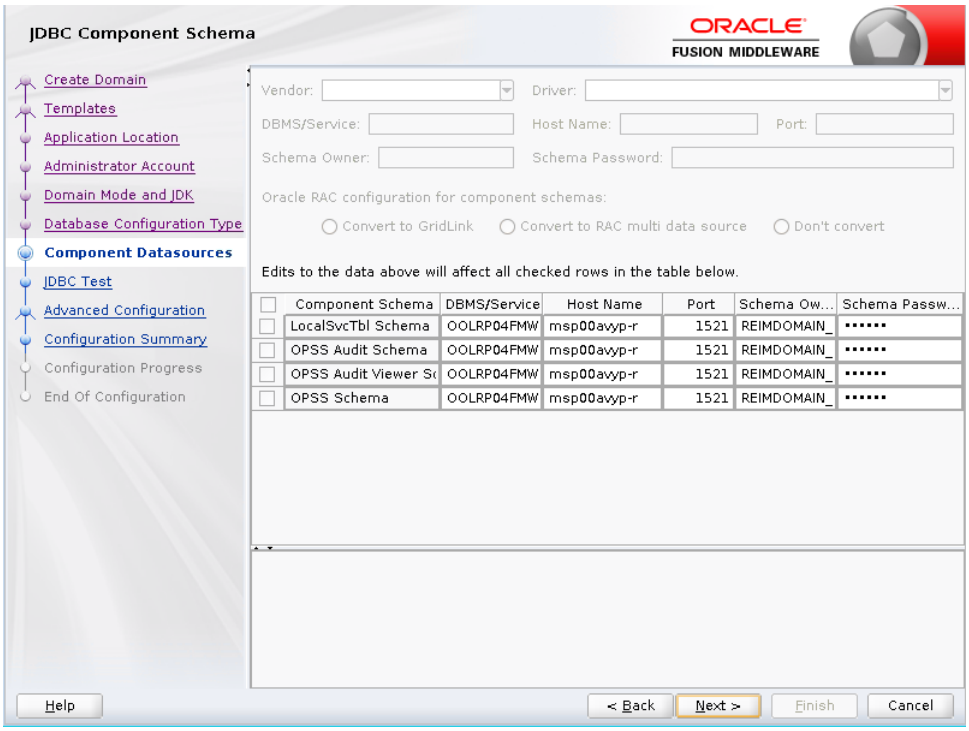


- Select **RCU Data**.
  - Vendor: Oracle
  - DBMS/Service: dbservicename
  - Host Name: scan address
  - Port: 1521
  - Schema Owner: REIMDOMAIN_STB (Example: ALLOCDOMAIN_STB, RESADOMAIN_STB, etc)
  - Password: <Password>. This password which was used for RCU schema creation.

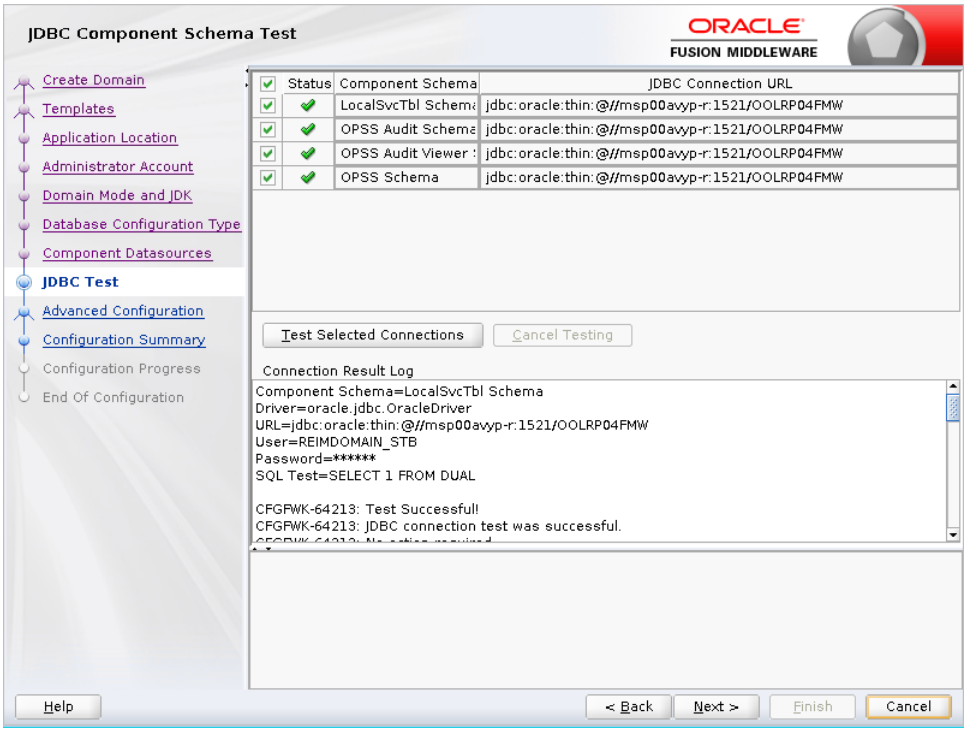
- Click the **Get RCU Configuration** button.



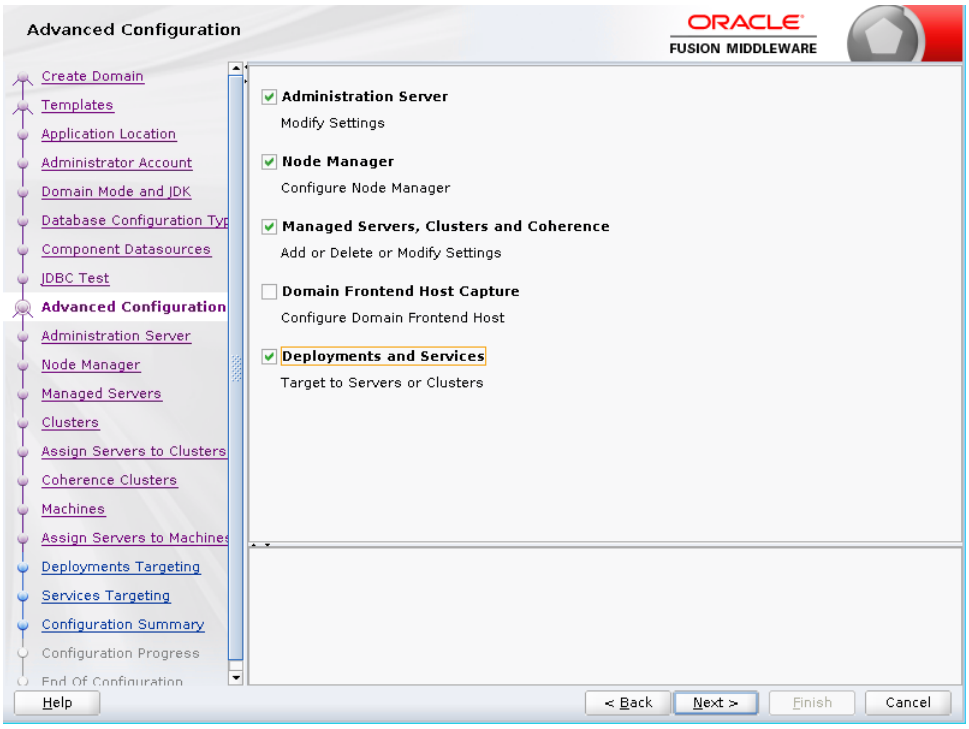
- Click **Next**.



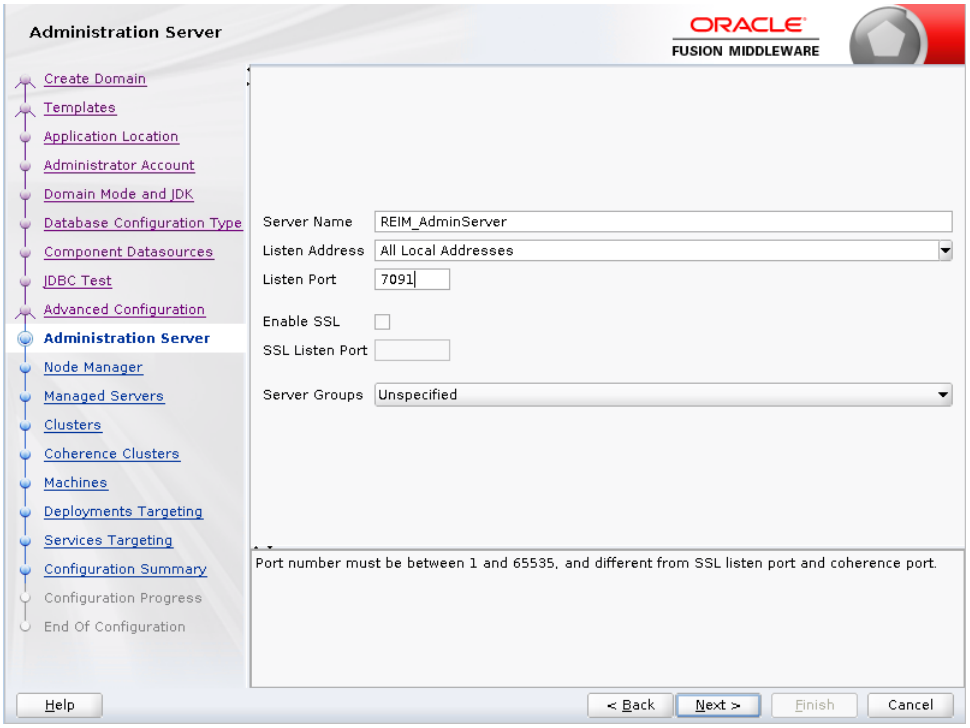
- Click **Next** and it will test to make sure it can connect to your datasources.



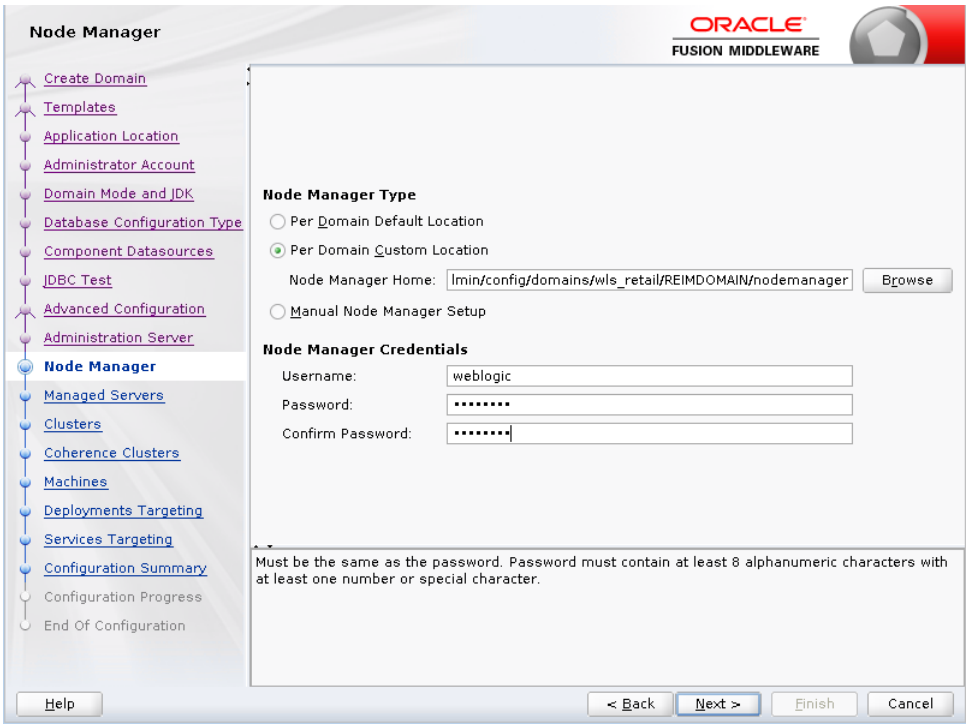
- Select advanced configuration for:
  - Administration Server
  - Managed Server, Clusters and coherence
  - Node manager



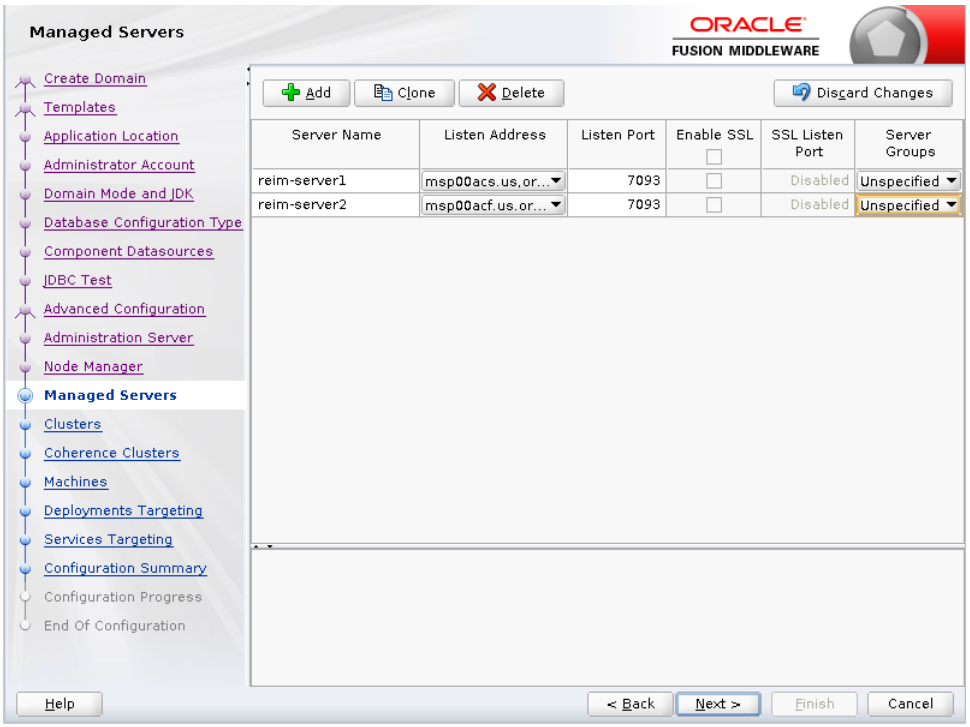
- Configure the Administration Server:
  - Server Name: <APP name>_AdminServer. Eg: REIM_AdminServer
  - Listen address: Appserver Hostname or IPAddress of the Appserver Host.
  - Listen port: <Port for Admin Server> Note: The port used here must be a free port.
  - Server Groups: Unspecified



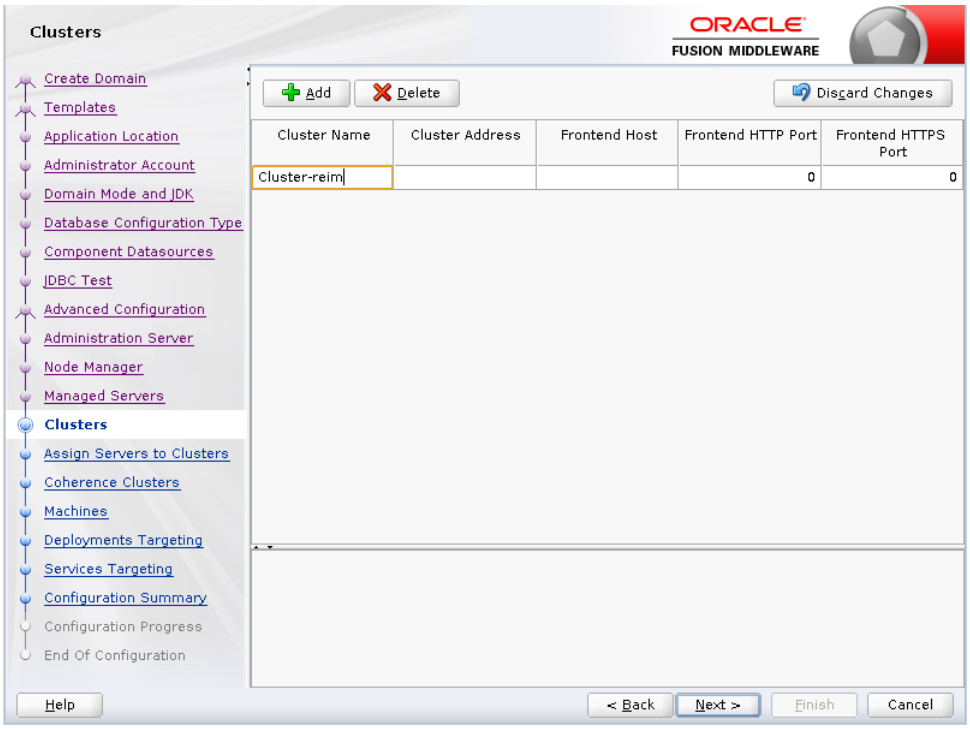
- Configure Node Manager:
  - Node manager type: Per domain default location
  - Username: <weblogic administrator user>
  - Password: <Password for weblogic administrator user>



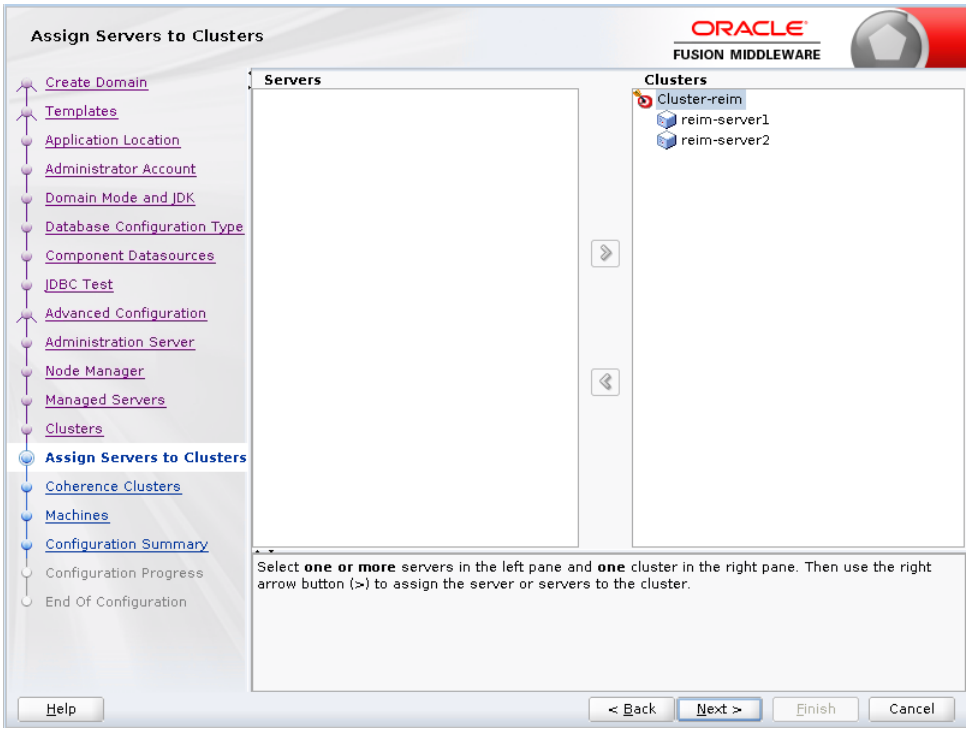
- Configure Managed Servers with the ADF template.
- Click the **Add** button.
  - Server Name: <appname-server> eg: reim-server1 and reim-server2 as this is cluster setup.
  - Listen address: Appserver1 Hostname for reim-server1 and Appserver2 Hostname for reim-server2
  - Listen port: <Port for Managed Server> Note: The port used here must be a free port.
  - Server Groups: <JRF-MAN-SVR>



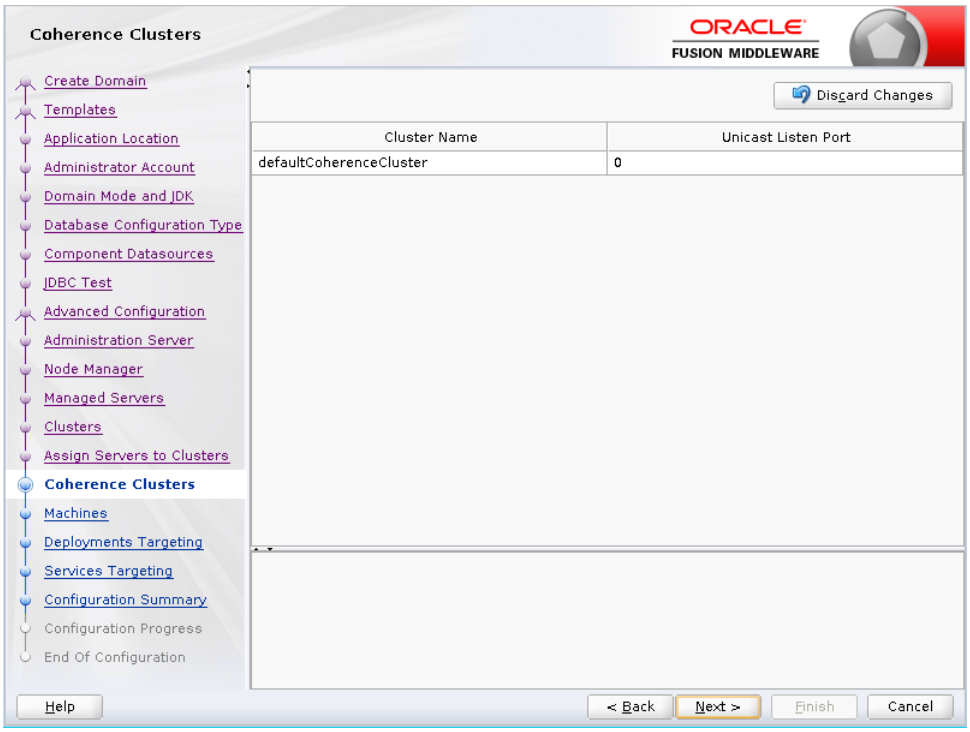
- Configure Clusters and click **Next**.



- Assign servers to the cluster.

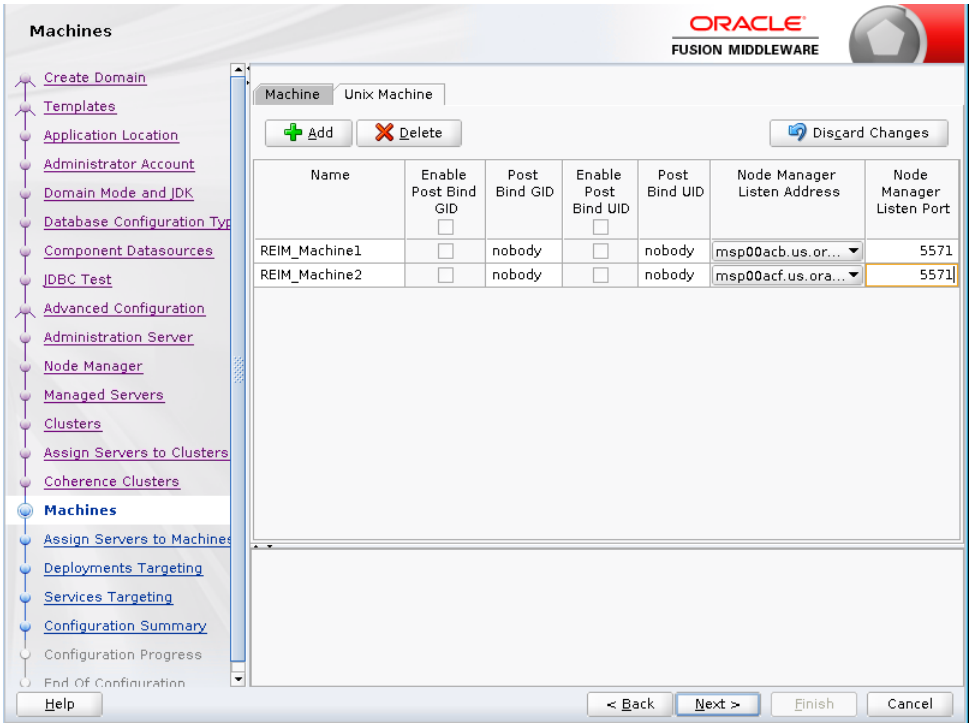


- Retain the default values, and click **Next**.

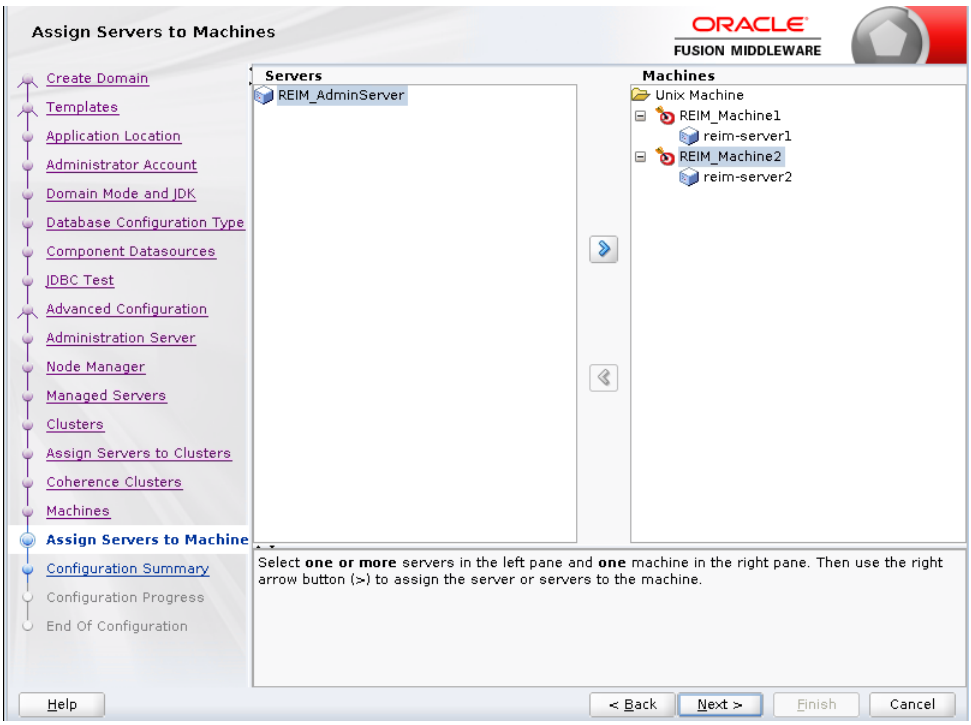


- Configure Machines:apphost1 and apphost2
- Click the **Add** button.
  - Name: APP_Machine1 and APP_Machine2
  - Listen address: apphostname1 for App_Machine1 and apphostname2 for APP_Machine2

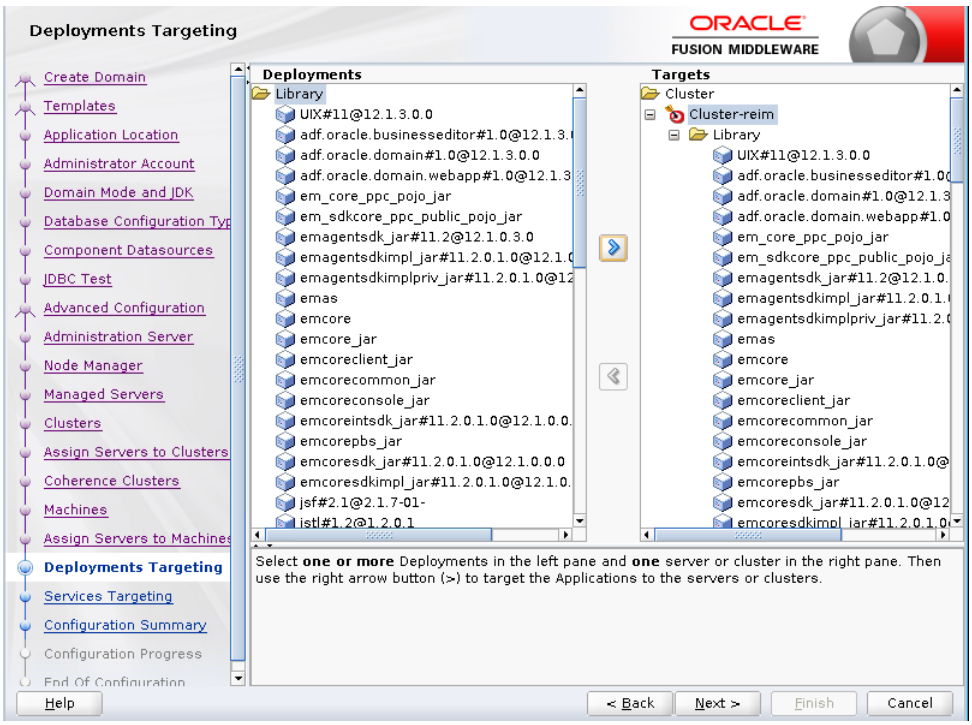
- Listen port: <Port for node manager> Note: The port used here must be a free port.



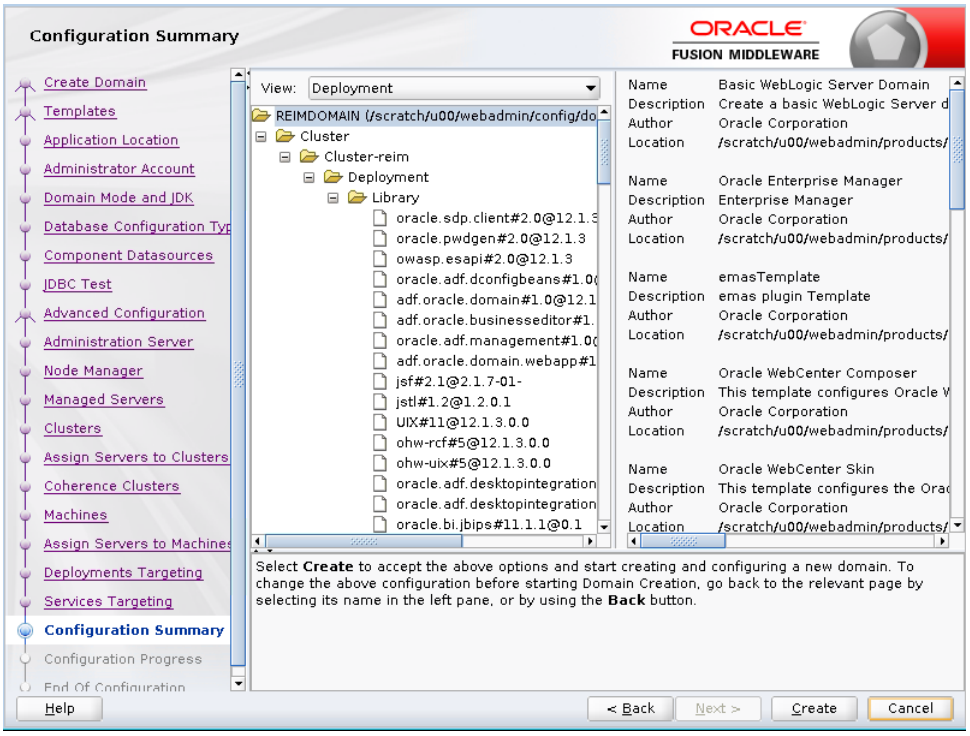
- Assign the configured Admin server and managed servers to the new machine. In the below screen can assign adminserver to machine1.



- Add libraries to the cluster-reim.



- And click **Next** in the Services Targeting screen.
- Click **Create**.



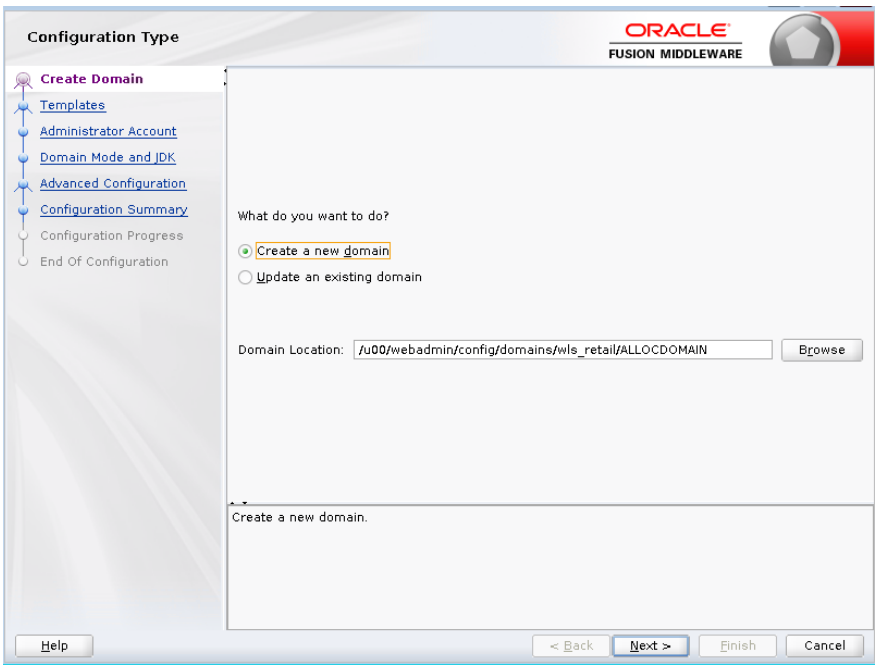
- Click **Next**.

- When the process completes, click **Finish**.

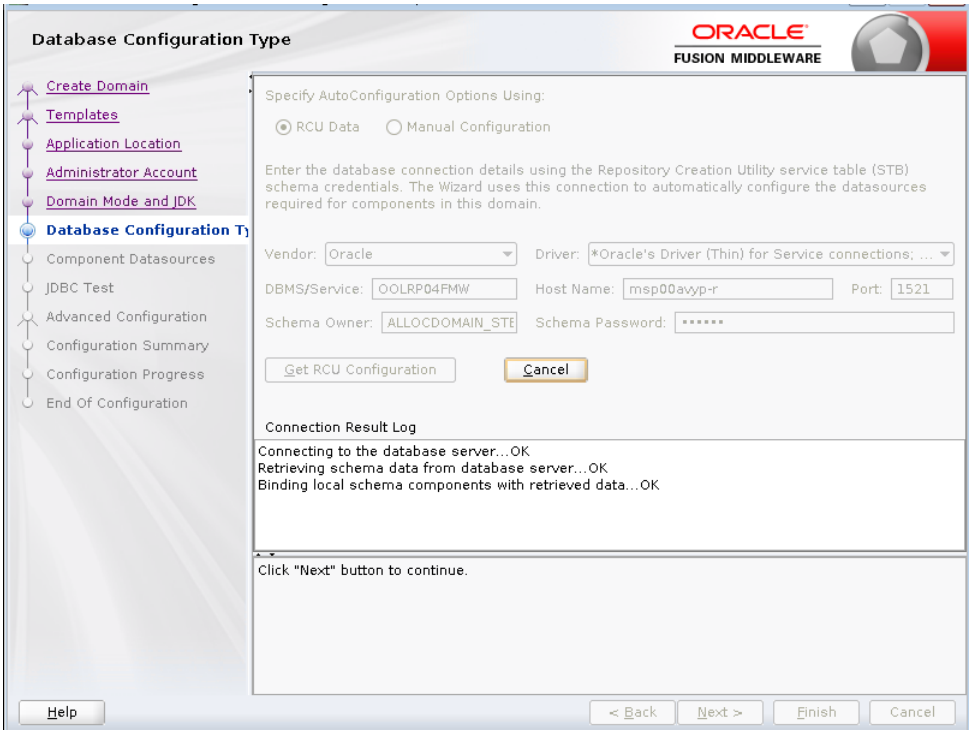
Note: Below listed screens are for ALLOC/SIM/RPM/RESA domain. Only the major screens are highlighted.

ALLOC Domain setup screens

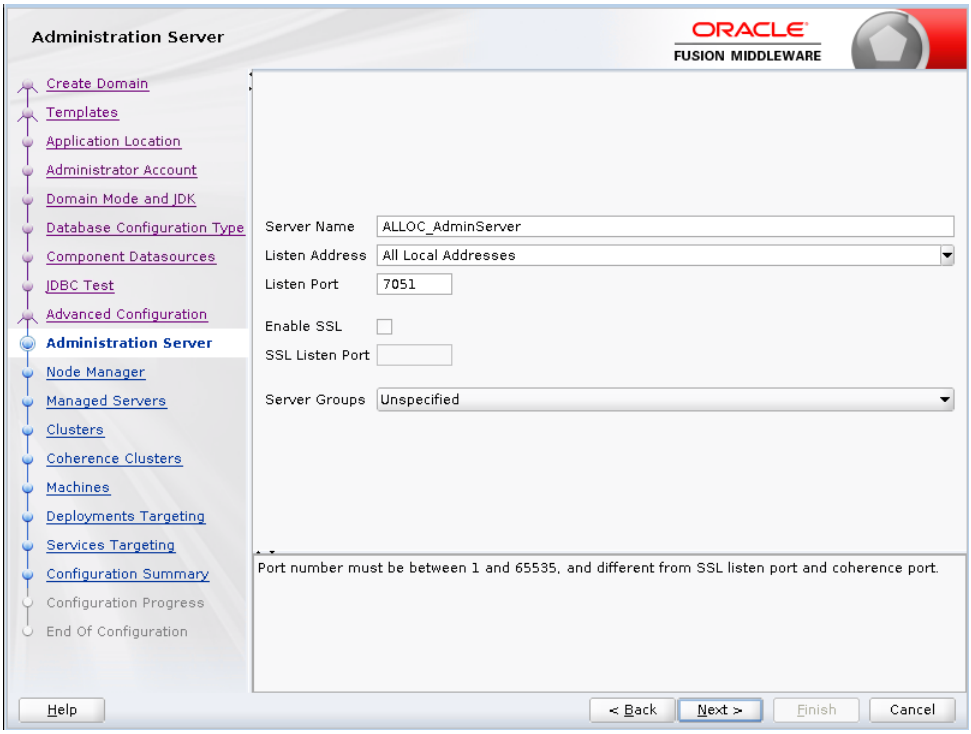
- Create new domain with the name **ALLOCDOMAIN.**



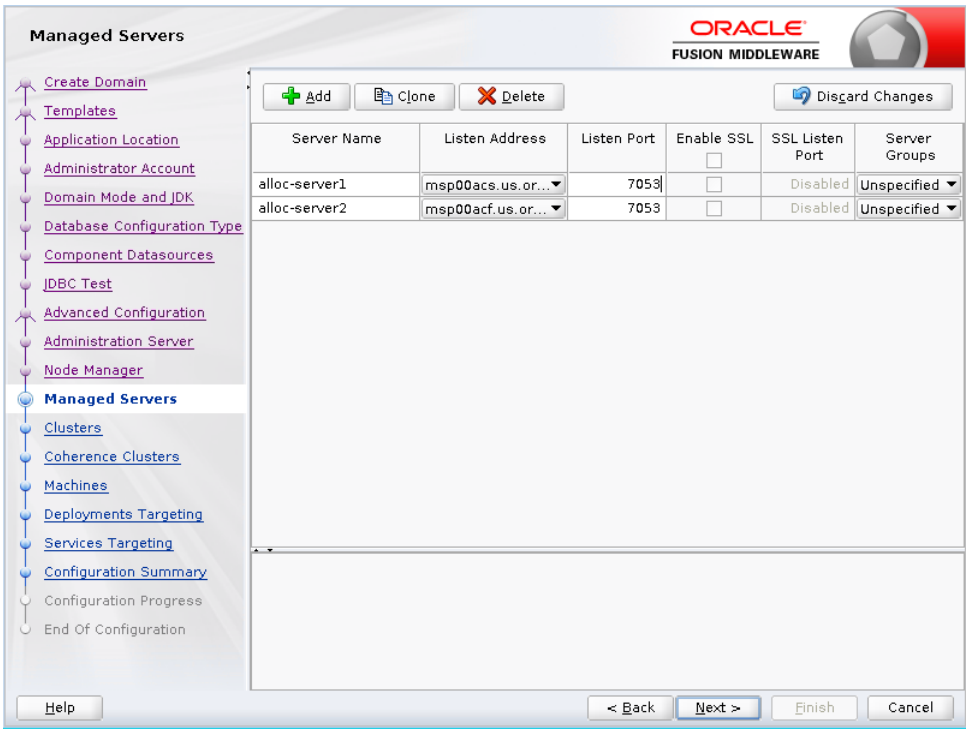
- Database Configuration Type screen for Alloc.



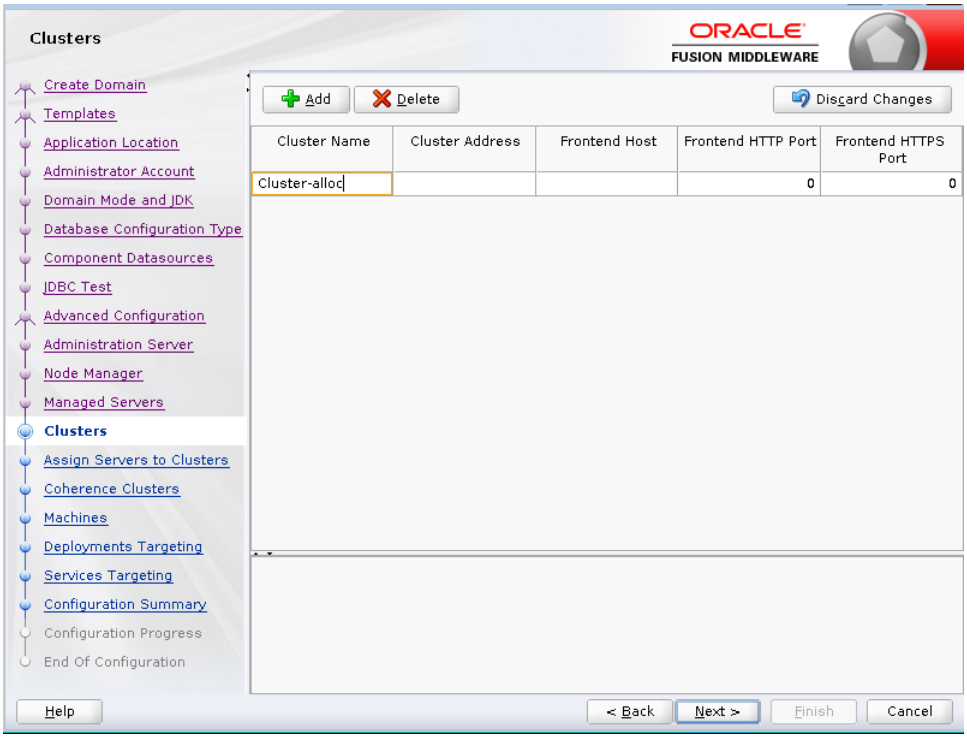
- Configure Admin server and name as **ALLOC_AdminServer**.



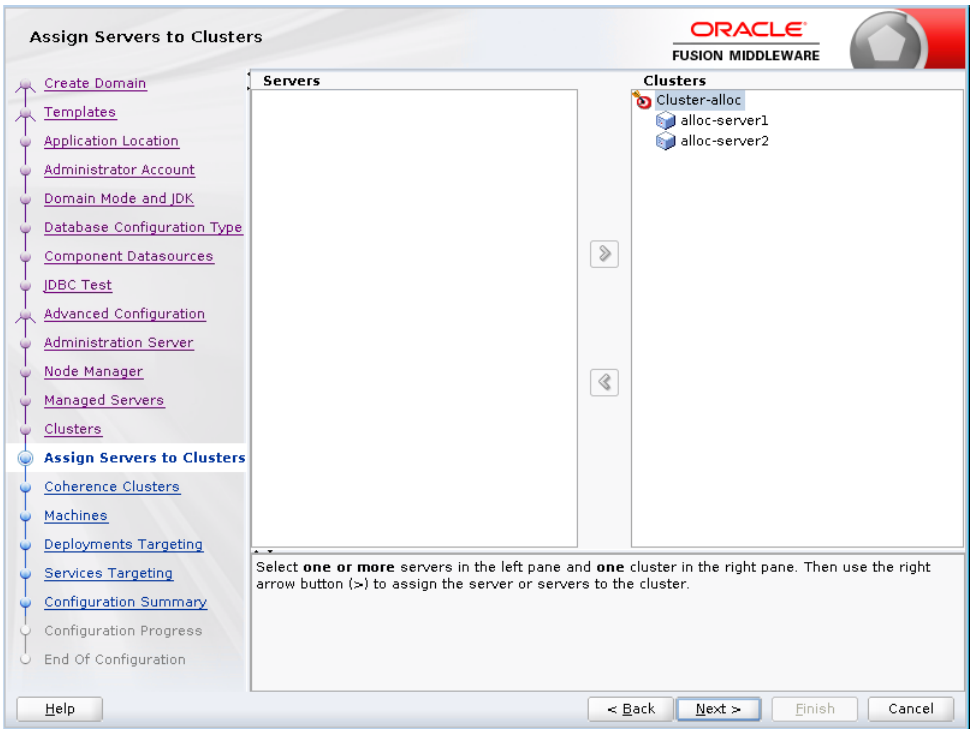
- Configure Managed servers and name as alloc-server1 and alloc-server2



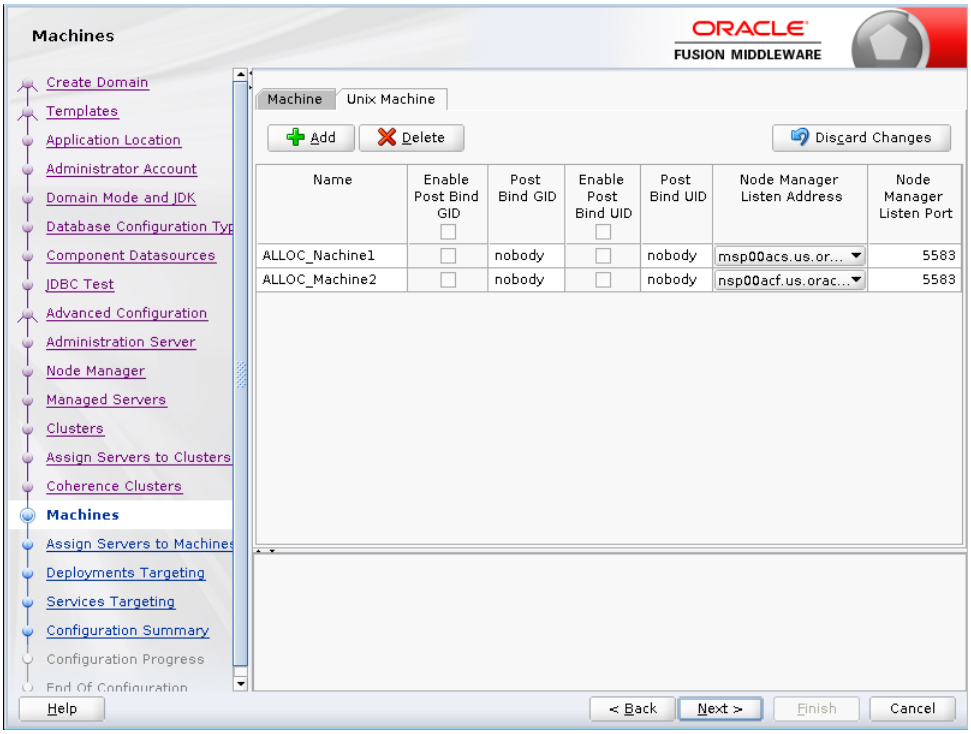
- Configure Cluster.



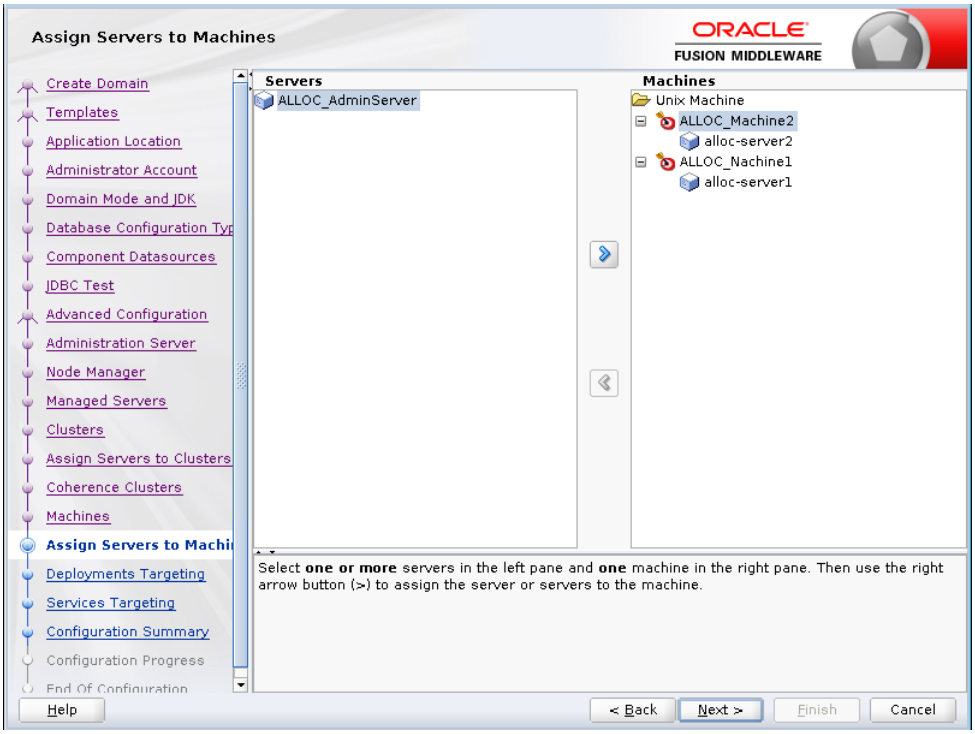
- Assign Servers to the cluster.



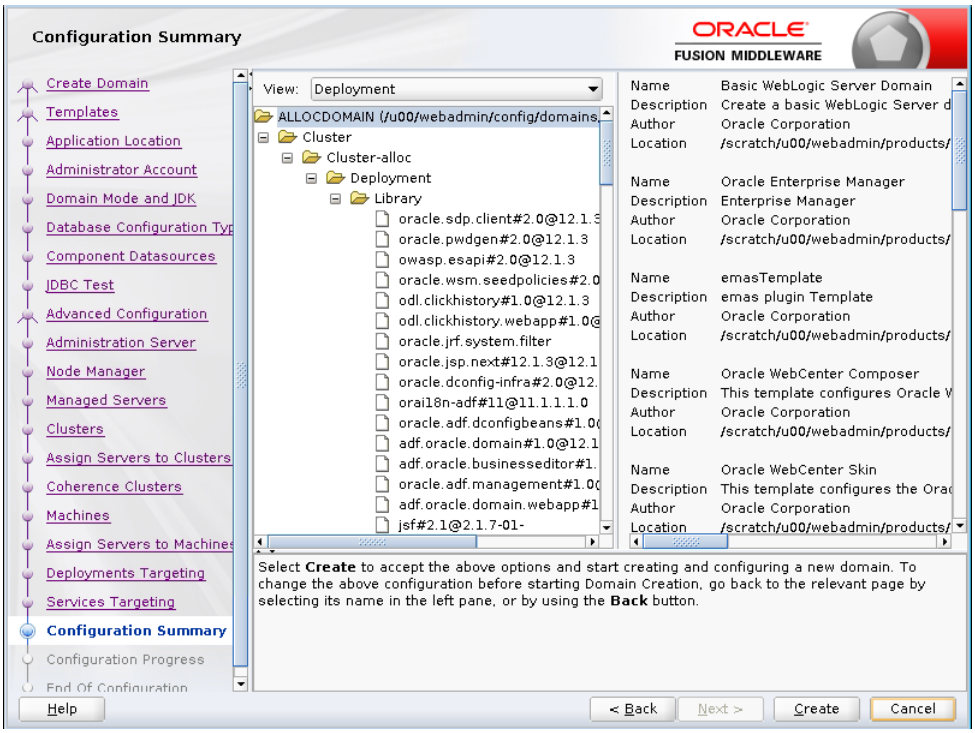
- Configure Machines as ALLOC_Machine1 and ALLOC_Machine2.



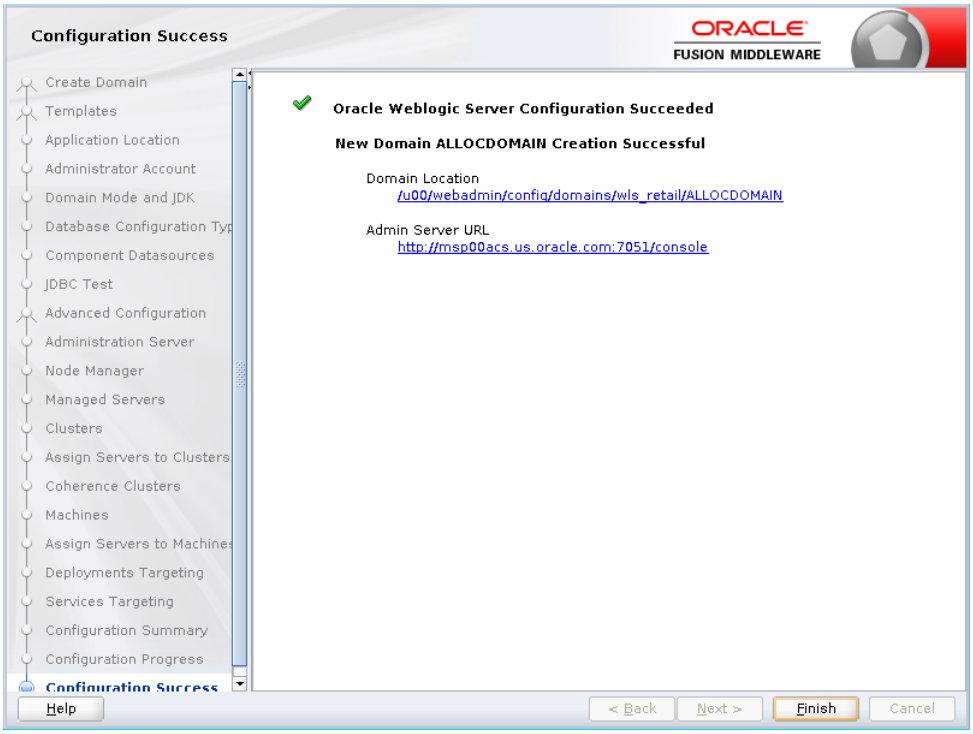
- Assign Managed servers to the Machine.



- Finally click create button to configure Domain.

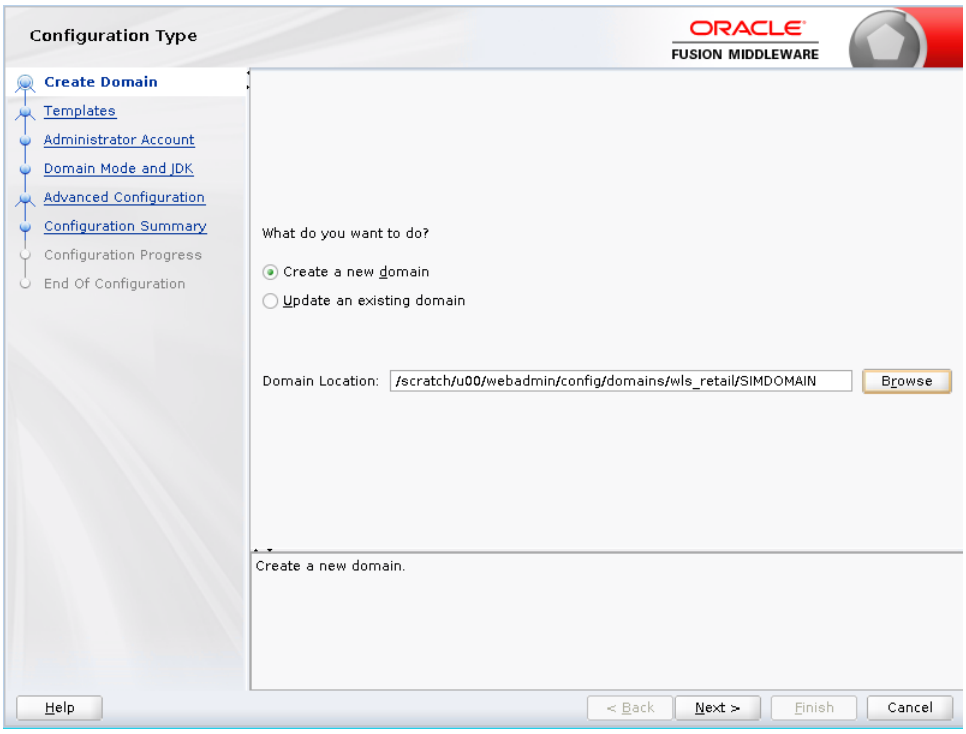


- When process completes, Click **Finish.**

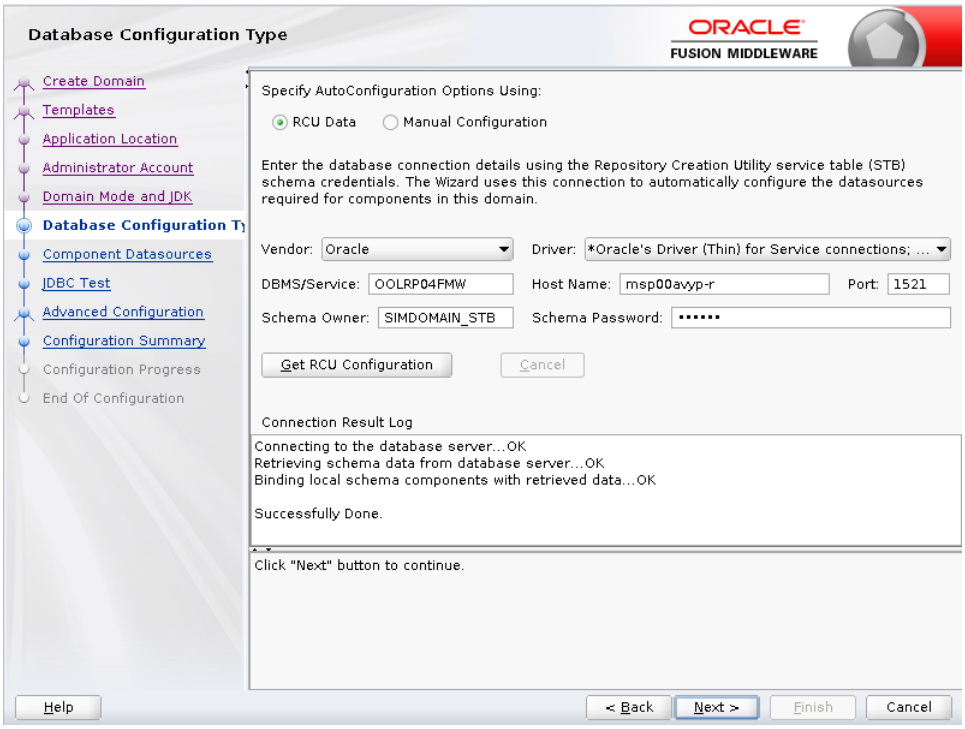


SIM Domain setup screens

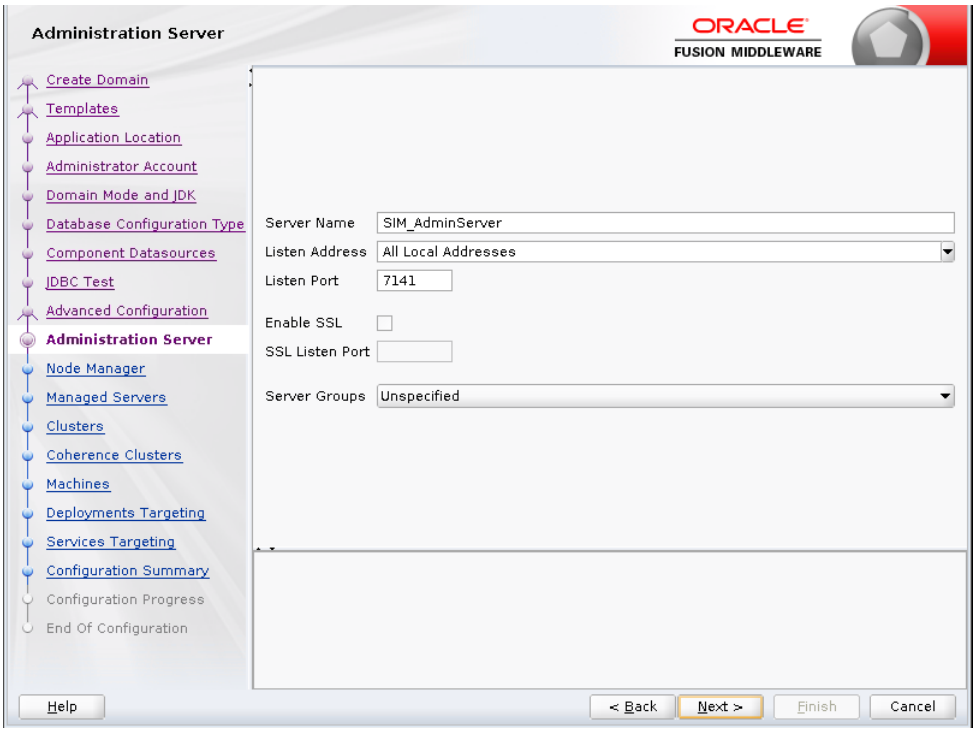
- Create new domain with the name SIMDOMAIN



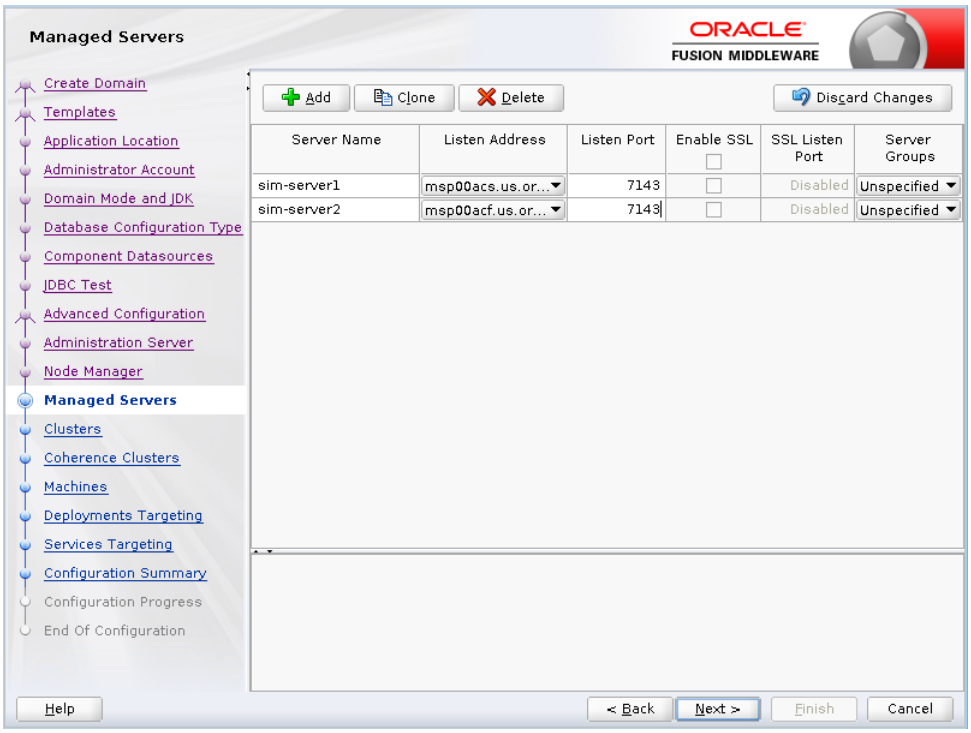
- Database Configuration Type screen for SIM



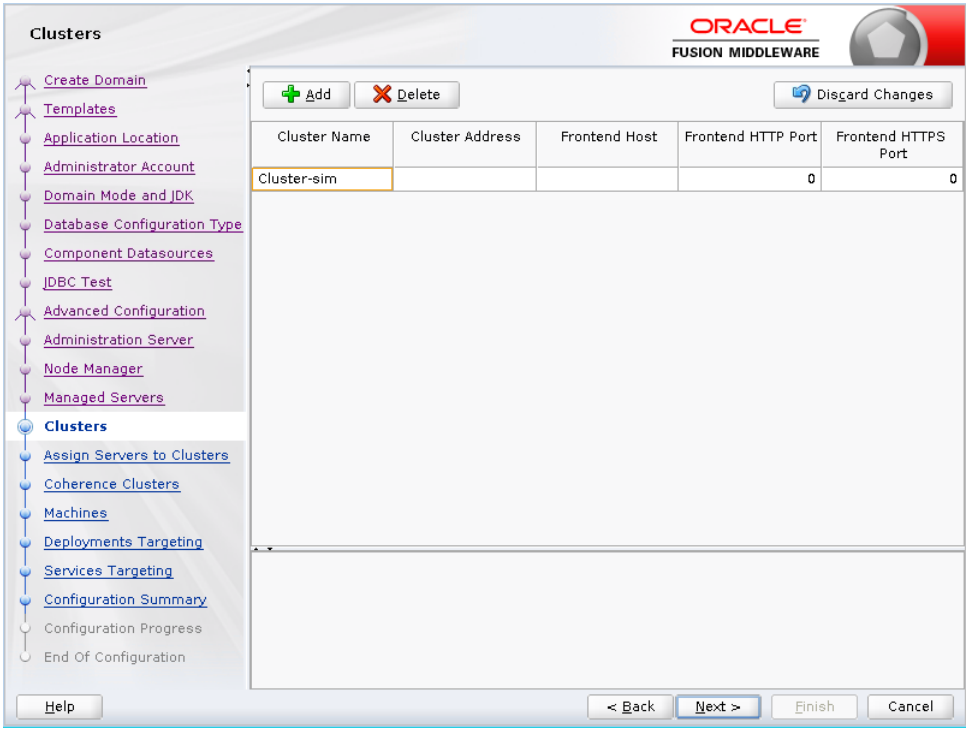
- Configure Admin server and name as **SIM_AdminServer**.



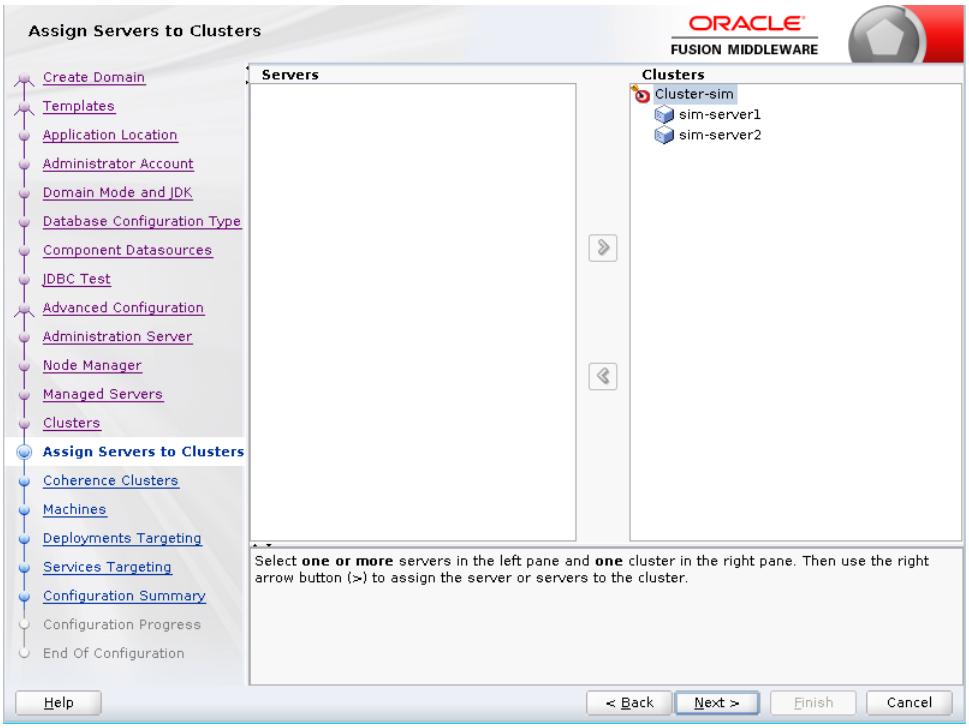
- Configure Managed servers and name as **sim-server1** and **sim-server2.**



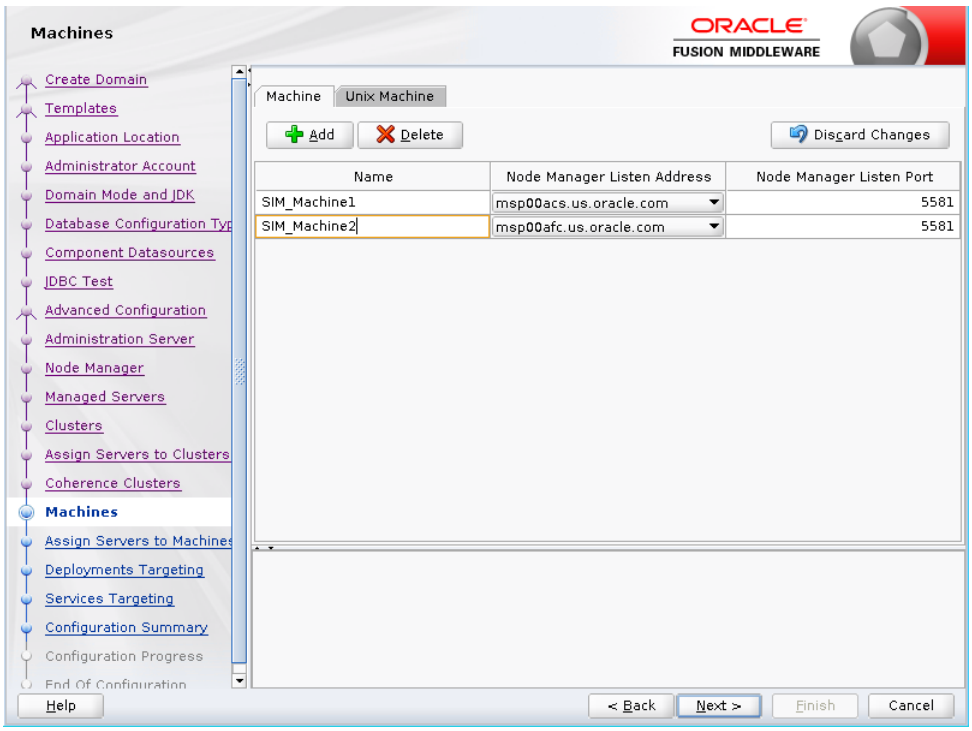
- Configure Cluster.



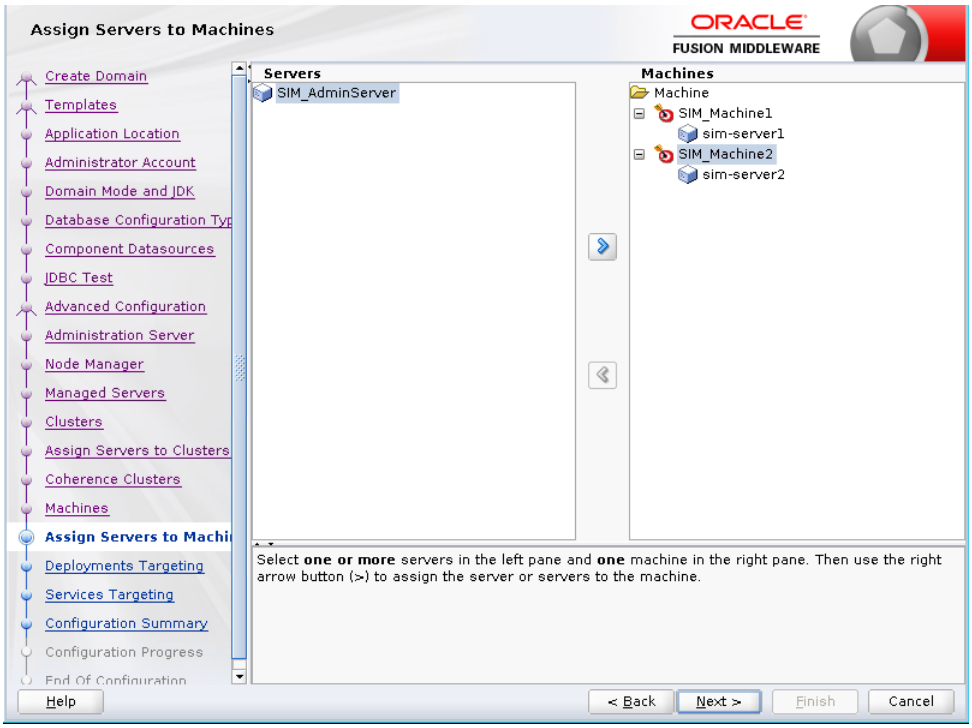
- Assign servers to the cluster.



- Configure Machines as **SIM_Machine1** and **SIM_Machine2**.



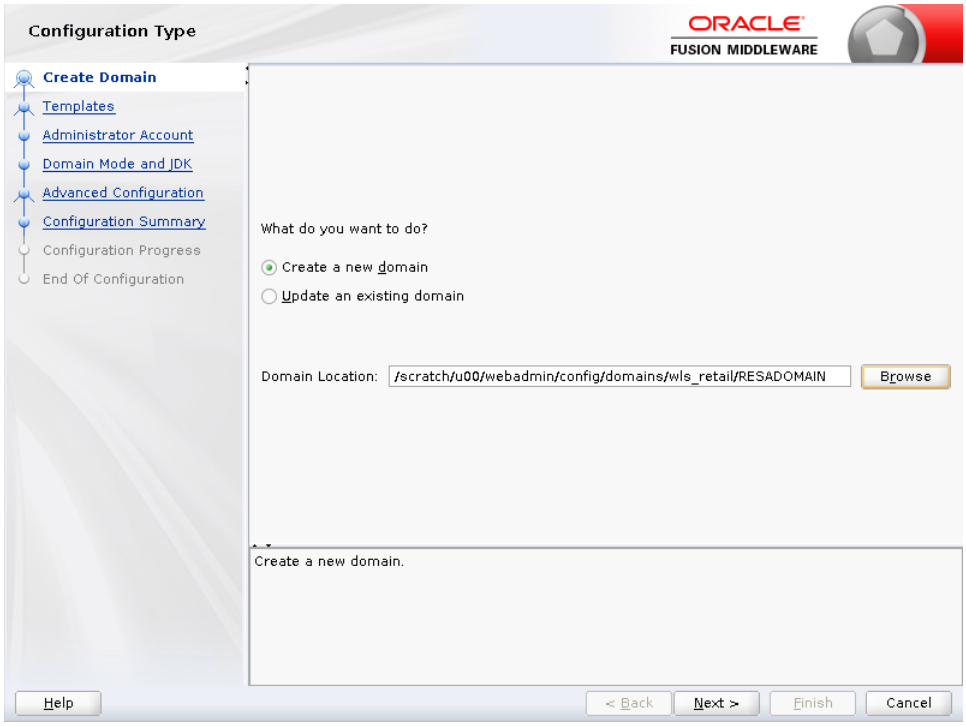
- Assign Managed servers to the machine.



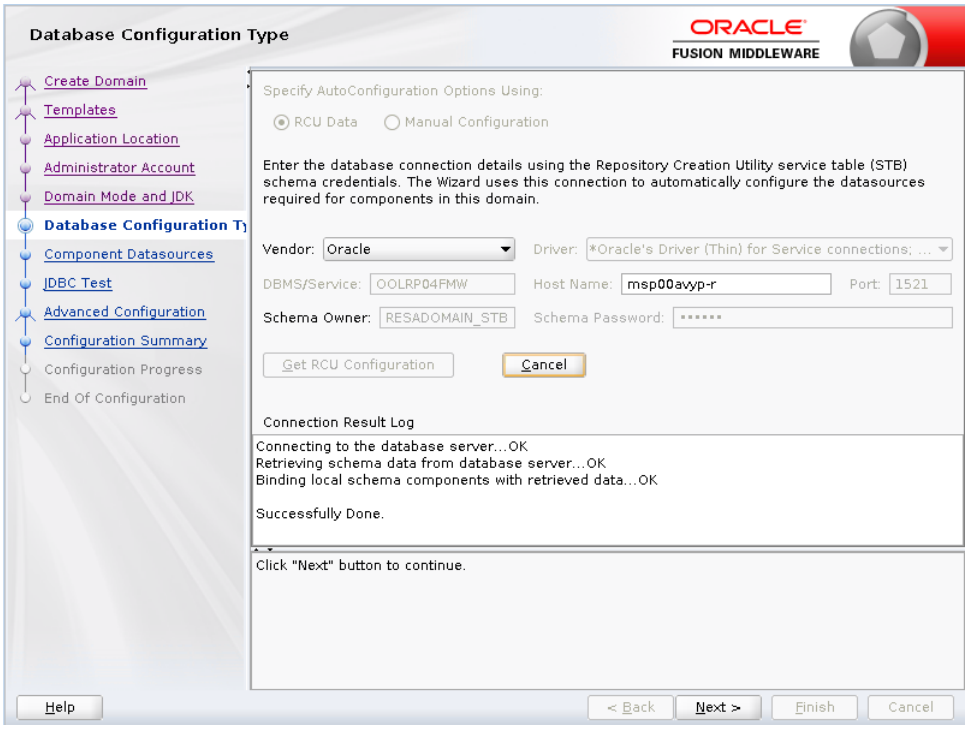
- Finally click **Create** to configure Domain.
- When the process completes, click **Finish**.

RESA Domain setup screens

- Create new domain with the name **RESADOMAIN.**

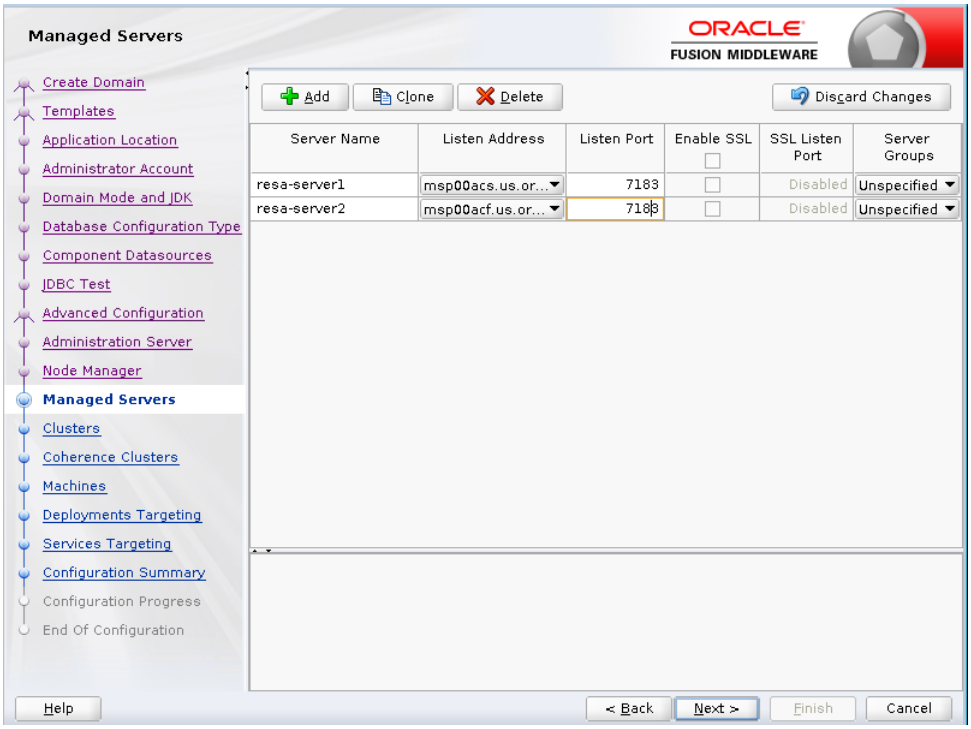


- Database Configuration Type screen for RESA

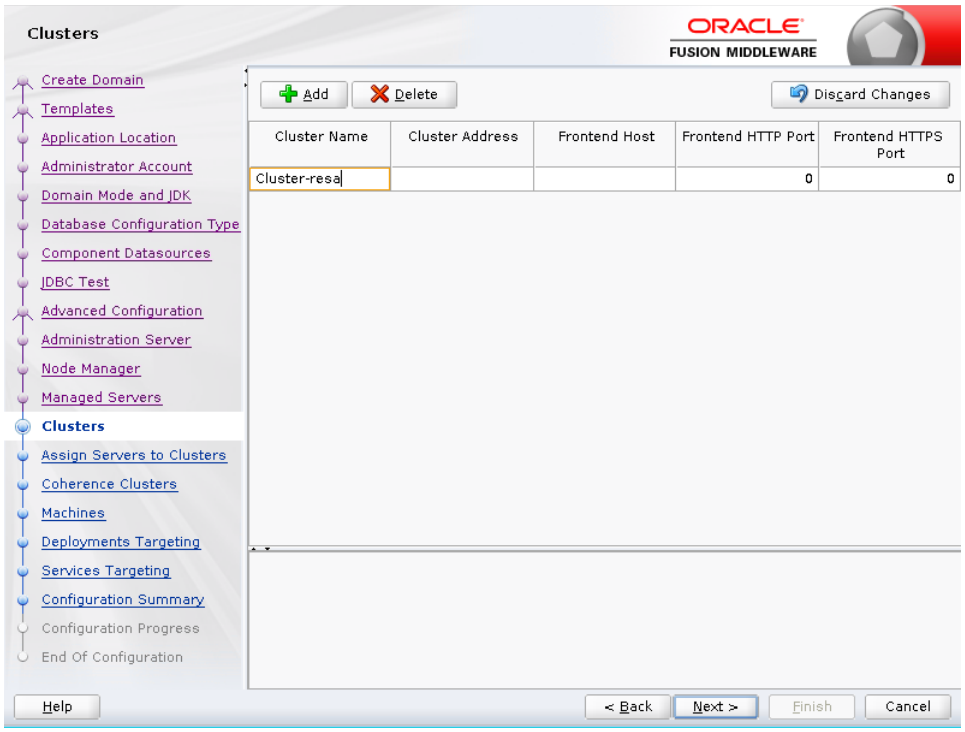


- Configure Admin server and name as **RESA_AdminServer** .

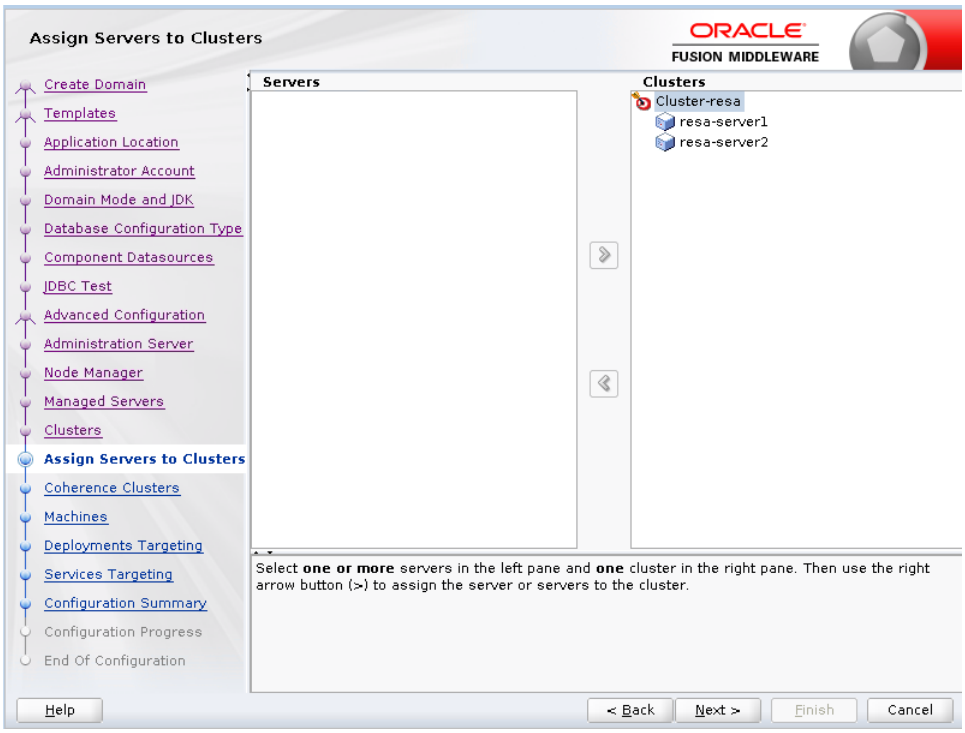
- Configure Managed servers and name as **resa-server1** and **resa-server2**.



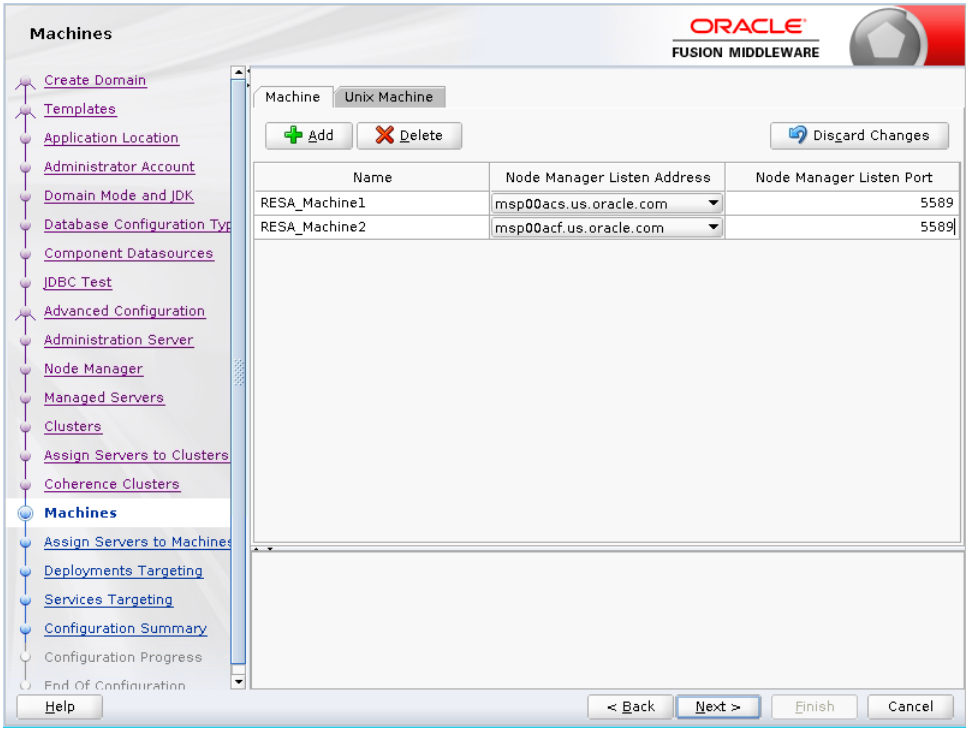
- Configure Cluster



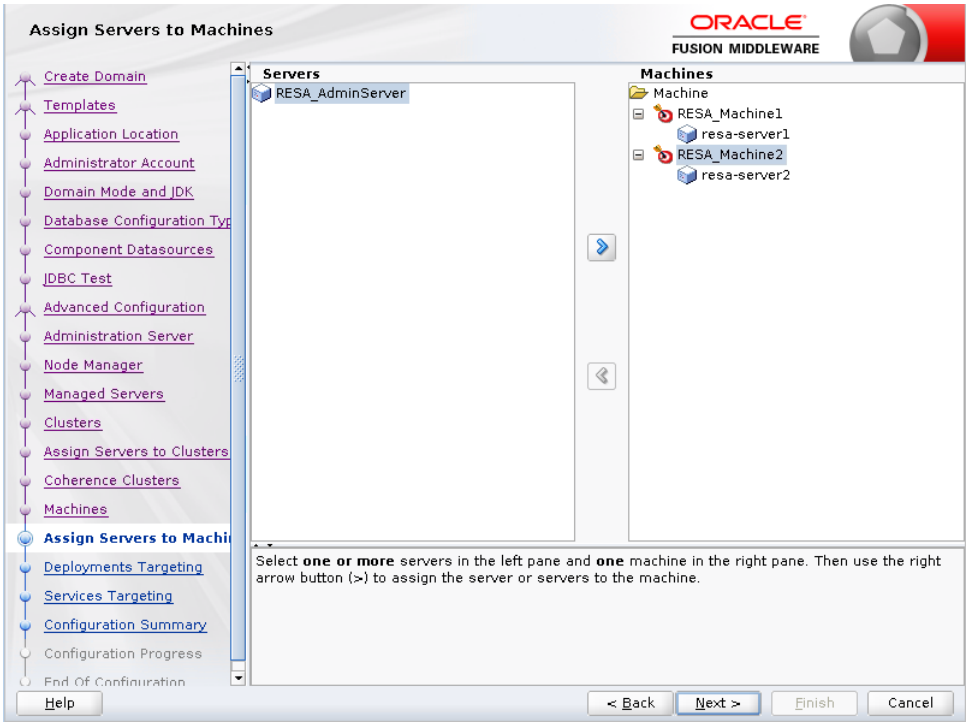
- Assign servers to the cluster.



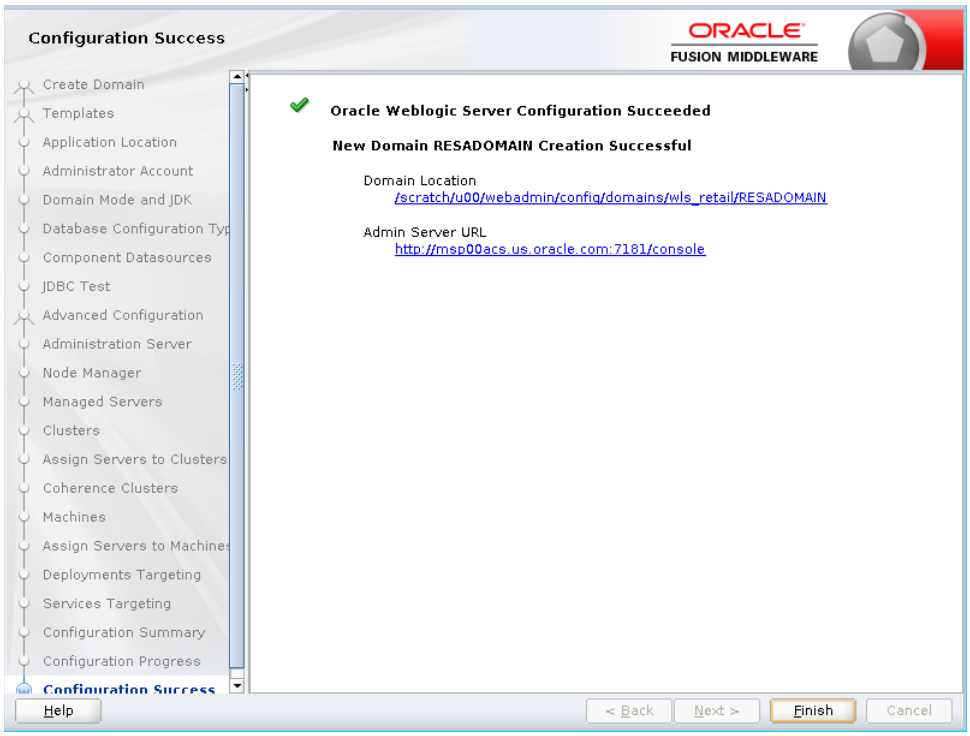
- Configure Machines as **RESA_Machine1** and **RESA_Machine2**.



- Assign Managed servers to the Machine.

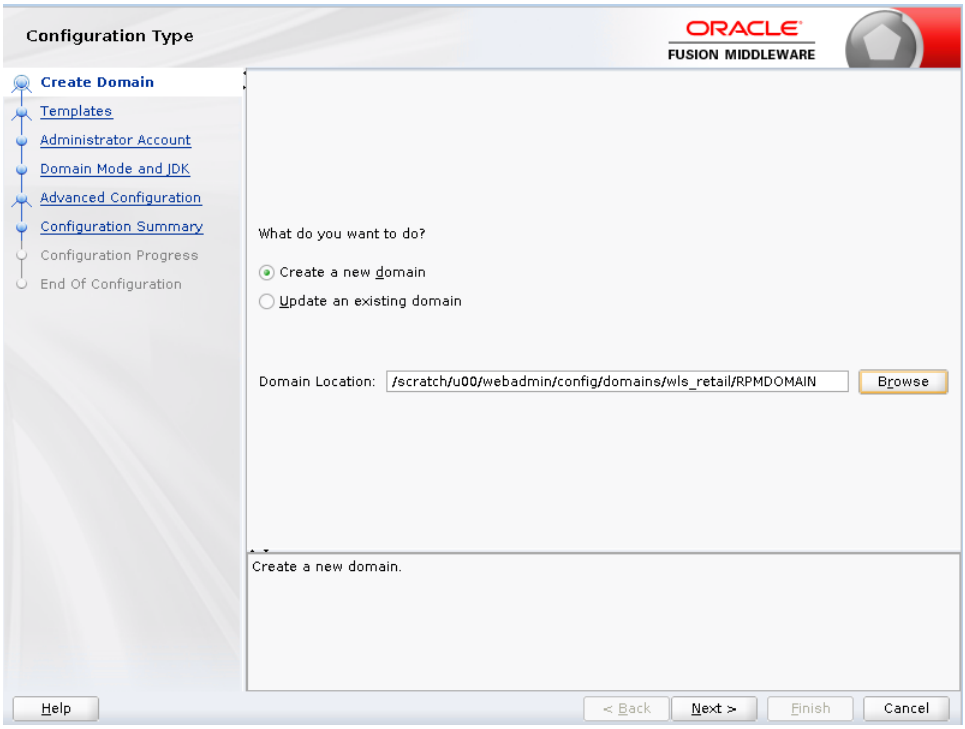


- Finally click **create** button to configure Domain.
- When the process completes, click **Finish**.

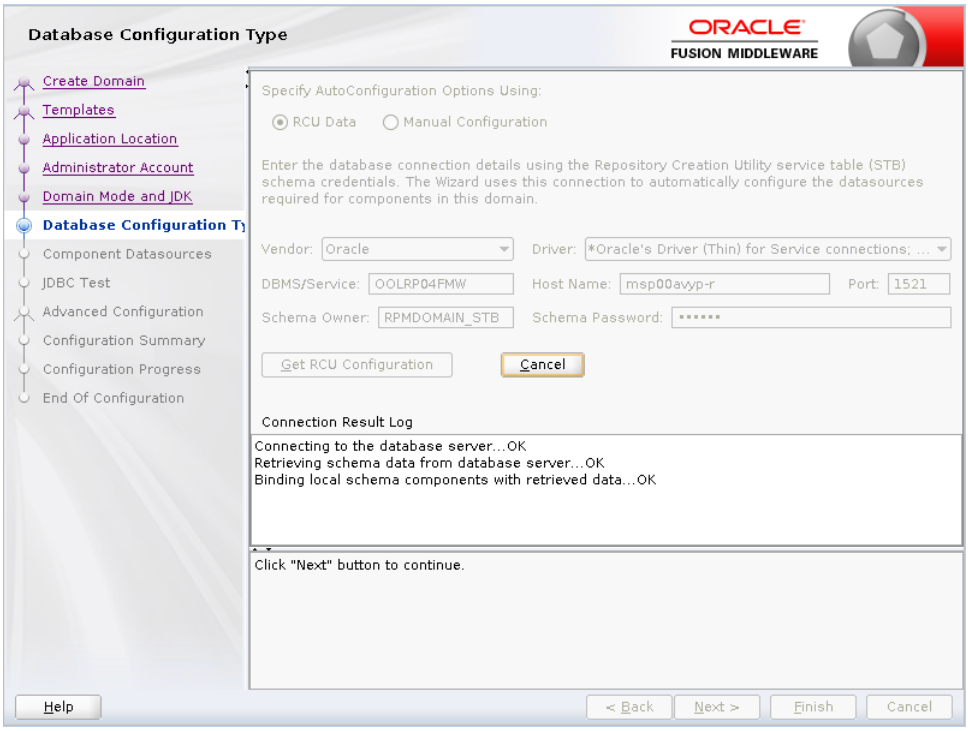


RPM Domain setup screens

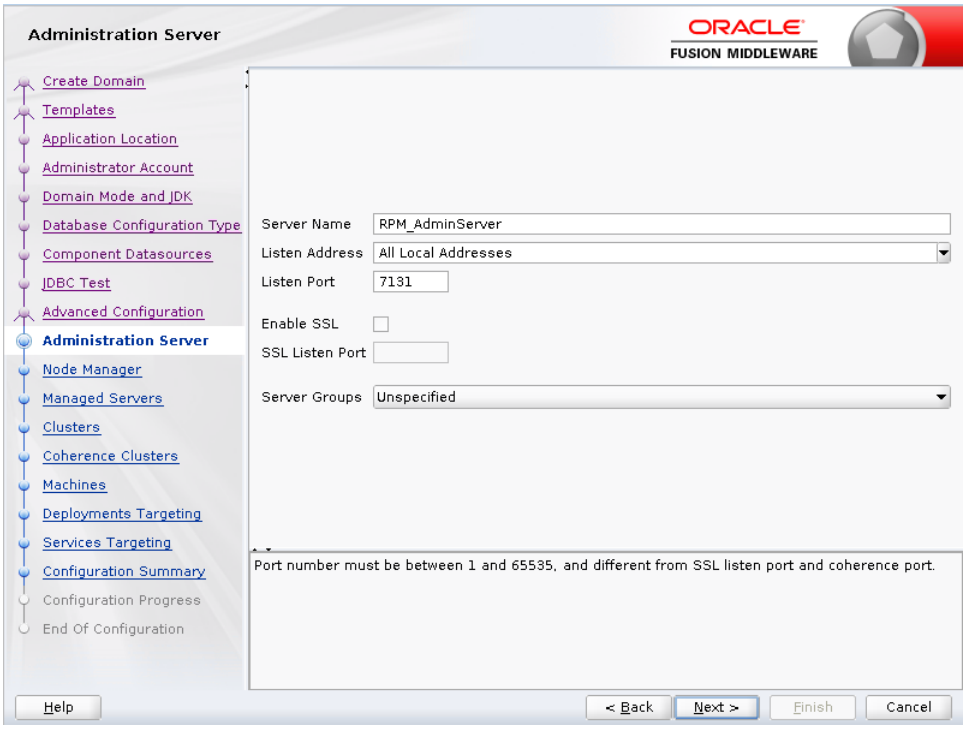
- Create new domain with the name **RPMDOMAIN.**



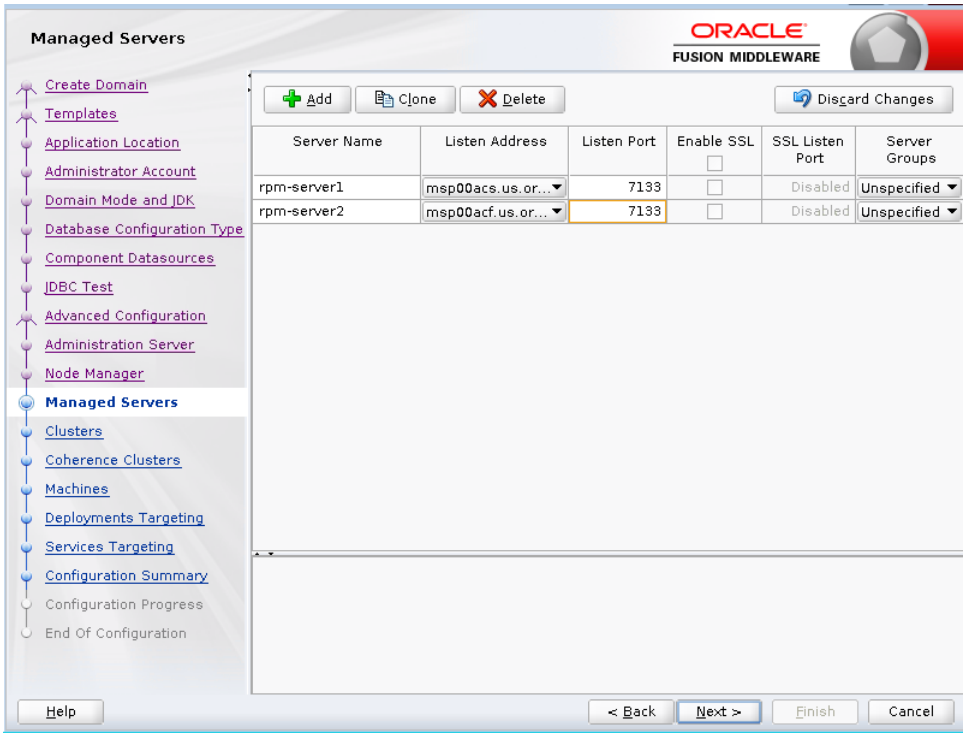
- Database Configuration Type screen for RPM



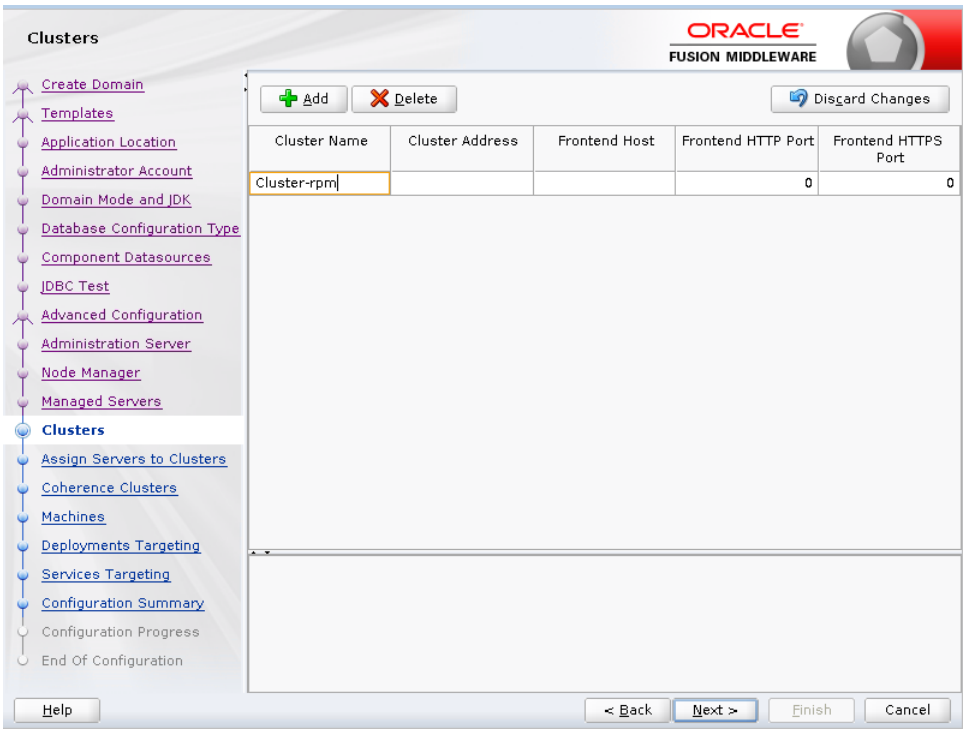
- Configure Admin server and name as **RPM_AdminServer**.



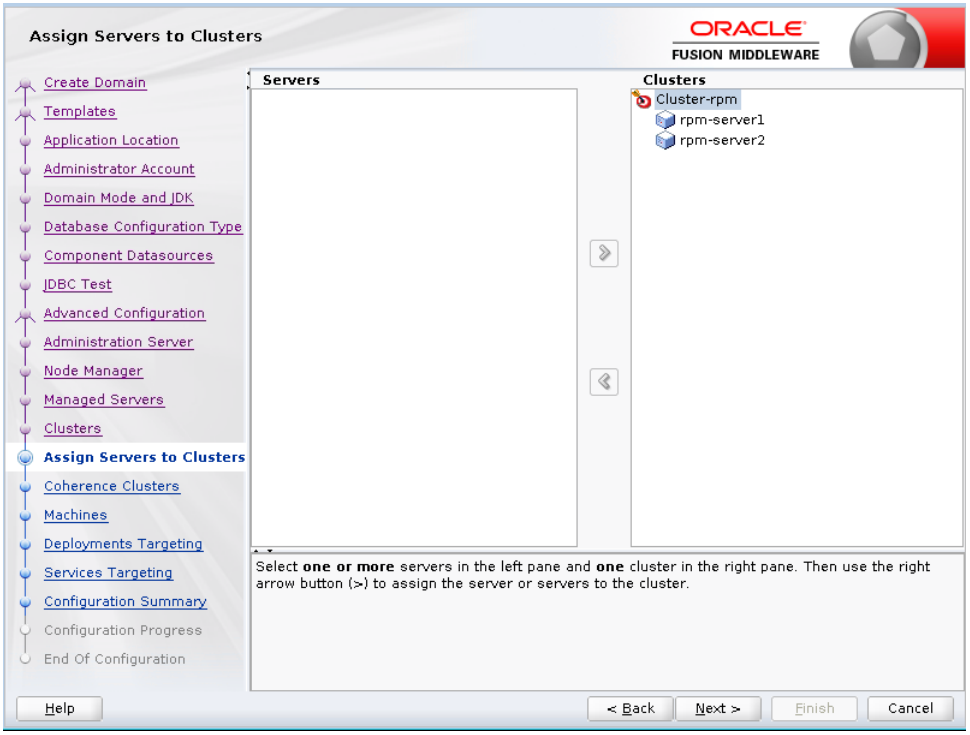
- Configure Managed servers and name as **rpm-server1** and **rpm-server2.**



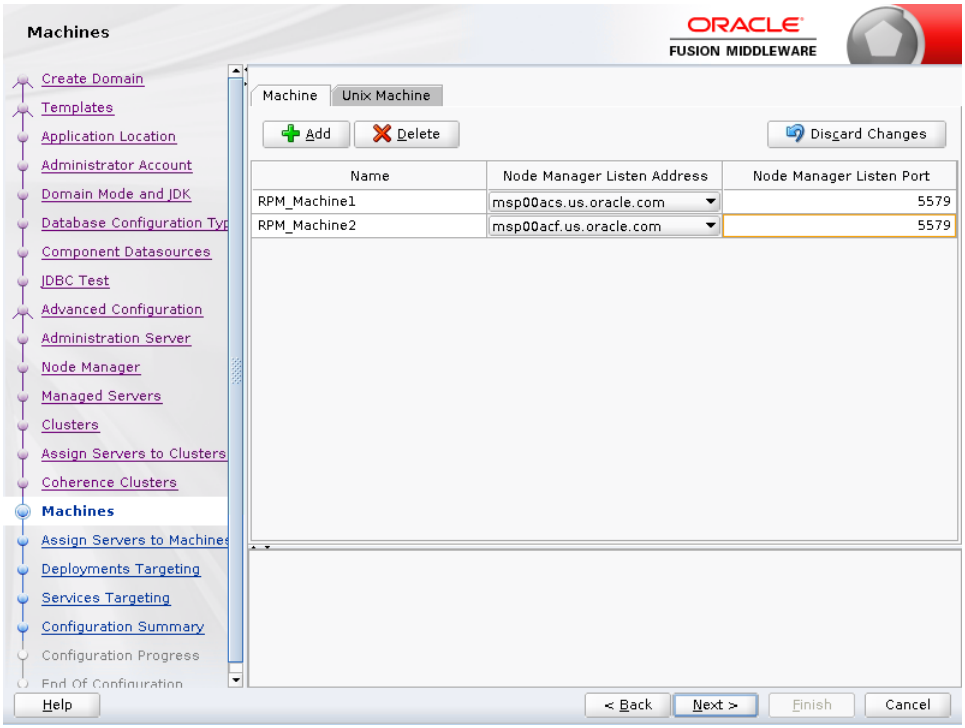
- Configure Cluster



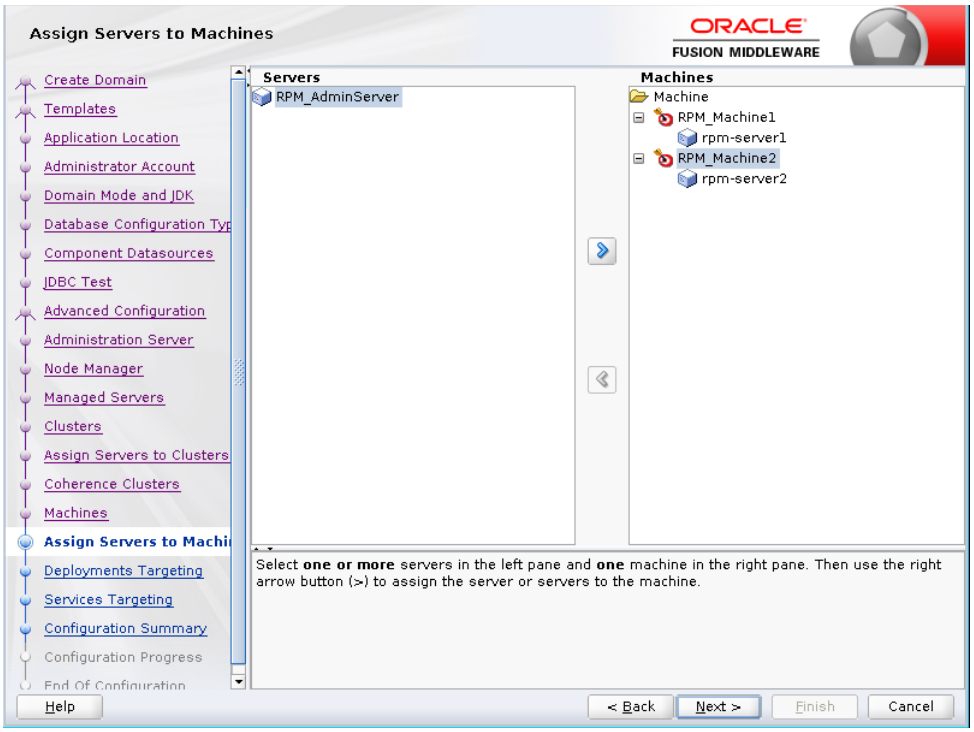
- Assign Servers to the cluster



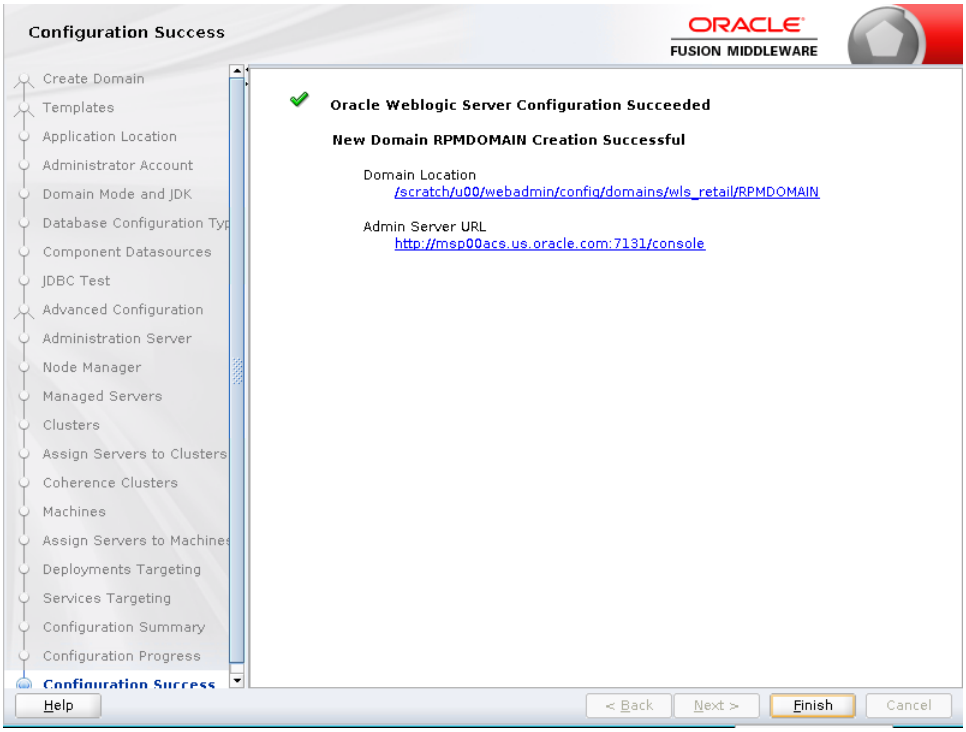
- Configure Machines as **RPM_Machine1** and **RPM_Machine2**.



- Assign Managed servers to the Machine.



- Finally click **create** to configure Domain.
- When the process completes, click **Finish**.



Procedure to start Nodemanger, AdminServer and Managed Server:

Start the Node Manager

1. Start the nodemanager from all <DOMAIN_HOME>/bin in the both the host using the following:

   ./startNodeManager.sh

Start the AdminServer (admin console)

- Start the WebLogic Domain (Admin Server) from <DOMAIN_HOME>/bin using the following:

  ./startWebLogic.sh

  Provide Weblogic username and password when prompted

  Example:

  /u00/webadmin/config/domains/wls_retail/REIMdomain/bin/startWebLogic.sh

  Configure boot.properties for starting the Weblogic domain without prompting to username and password using the following command:

- Create security folder at <DOMAIN_HOME>/servers/<AdminServer>/ and create boot.properties file under <DOMAIN_HOME>/servers/<AdminServer>/security

  The file 'boot.properties' should have the following:

  username=weblogic

  password=<password>

In the above, the password value is the password of WebLogic domain which is given at the time of domain creation.

- Save the boot.properties file and restart the WebLogic server.
- Access the Weblogic Admin console

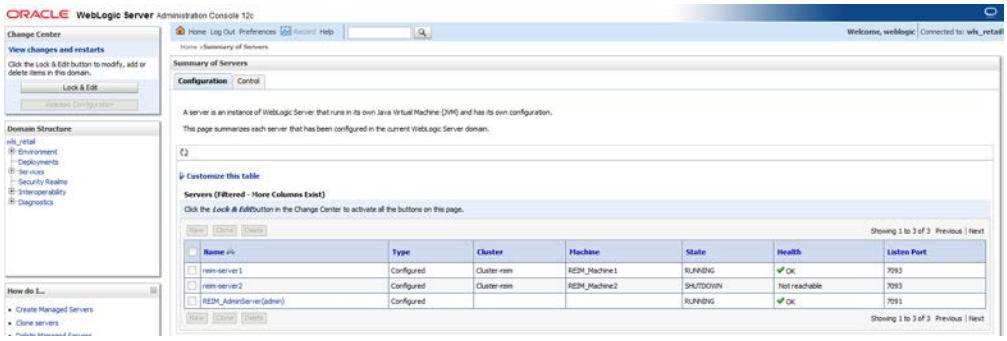
  Example: http://<HOST_NAME>:<ADMIN_PORT>/console

  In the below screen, provide username=weblogic and password=<weblogic password>

Start the Managed Server hosted in Appserver1

After NodeManager is started, the managed servers can be started via the admin console. http://<host>:<port>/console

Navigate to Environments -> Servers and click the Control tab. Select reim-server1 and click **Start**.



Managed Server should be up and running before configuring further steps.

Pack Domain and Copy to appserver2

This section describes how to pack the domain and copy to the appserver2. Follow the below steps for each of the Domain created earlier. Substitute <APP> below with the application for which the domain created. E.g. SIM, RPM, REIM

1. Shut down the AdminServer, Managed server.
2. Shutdown all WebLogic processes on both machines including NodeManager.
3. Pack the domain to copy to secondary appserver.

export PATH=$WLS_HOME/wlserver_10.3/common/bin:$PATH in both the servers.

cd $WLS_HOME

appserver1$: pack.sh -
domain=/u00/webadmin/config/domains/wls_retail/<APP>DOMAIN -
template=/u00/webadmin/config/domains/wls_retail/<APP>Domain.jar -
template_name=<APP>DOMAIN -managed=true

Eg: REIMDOMAIN

pack.sh -domain=/u00/webadmin/config/domains/wls_retail/REIMDomain -
template=/u00/webadmin/config/domains/wls_retail/REIMDOMAIN.jar -
template_name=REIMDOMAIN -managed=true

output:

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

Note: Follow same steps for ALLOCDOMAIN, RESADOMAIN, ALLOCDOMAIN and SIMDOMAIN to pack the domain and copy to appserver2.

Unpack Domain in appserver2

Copy the <App>Domain.jar under $WLS_HOME and unpack using below command and variables as below.

export PATH=$WLS_HOME/wlserver_10.3/common/bin:$PATH in both the servers.

cd $WLS_HOME

appserver2$:unpack.sh -
template=/u00/webadmin/config/domains/wls_retail/<APP>DOMAIN.jar -
domain=/u00/webadmin/config/domains/wls_retail/<APP>DOMAIN -
overwrite_domain=true -
app_dir=/u00/webadmin/config/applications/wls_retail/<APP>DOMAIN

Eg: REIMDOMAIN

unpack.sh -template=/u00/webadmin/config/domains/wls_retail/REIMDOMAIN.jar
-domain=/u00/webadmin/config/domains/wls_retail/REIMDOMAIN -
overwrite_domain=true -
app_dir=/u00/webadmin/config/applications/wls_retail/REIMDOMAIN

Output:

```
<< read template from
"/scratch/u00/webadmin/config/domains/wls_retail/REIMDOMAIN.jar"
>>  succeed: read template from
"/scratch/u00/webadmin/config/domains/wls_retail/REIMDOMAIN.jar"
<< set config option OverwriteDomain to "true"
>>  succeed: set config option OverwriteDomain to "true"
<< set config option AppDir to
"/scratch/u00/webadmin/config/applications/wls_retail/REIMDOMAIN"
```

```
>>  succeed: set config option AppDir to
"/scratch/u00/webadmin/config/applications/wls_retail/REIMDOMAIN"
<< set config option DomainName to "REIMDOMAIN"
>>  succeed: set config option DomainName to "REIMDOMAIN"
<< write Domain to "/scratch/u00/webadmin/config/domains/wls_retail/REIMDOMAIN"
.............................................................................
........
>>  succeed: write Domain to
"/scratch/u00/webadmin/config/domains/wls_retail/REIMDOMAIN"
<< close template
>>  succeed: close template
```

Note: Follow same steps for ALLOCDOMAIN, RESADOMAIN, ALLOCDOMAIN and SIMDOMAIN to Unpack the domain in appserver2.

Note: Once domain is up, please go to Services and then Datasource in weblogic console and check the OPSS and other Datasource should be targeted to Managed server and Admin Server both.

Install the Oracle Retail Java Applications

To install the Oracle Retail Java applications following each installation guide. Following sections will provide a brief outline of the steps.

1. When prompted by the installer to enter the managed server/cluster, enter the cluster name (for example, Cluster-sim).
2. Perform the post install steps for cluster and SSO.
3. Configuration files that are updated need to be completed on both appservers (for example, weblogic.policy updates).

.

WebLogic.policy entry for both hosts

Update the weblogic.policy files on both the appservers for each of the apps. Please refer to actual install document for syntax.

Example: weblogic.policy entry in apphost1

RPM:

Update policy file for RPM Application in both the host:

APPHOST1:

```
grant codeBase
"file:/u00/webadmin/config/domains/wls_retail/RPMDOMAIN/servers/rpm-
server1/tmp/_WL_user/rpm/-"
{
permission java.security.AllPermission;
permission oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore", "read,write,update,delete";
```

```
permission
oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore.*", "read,write,update,delete";
};

grant codeBase
"file:/u00/webadmin/config/domains/wls_retail/RPMDOMAIN/servers/rpm-
server1/cache/EJBCompilerCache/-"
{
permission java.security.AllPermission;
permission
oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore", "read,write,update,delete";
permission
oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore.*", "read,write,update,delete";
};


grant codeBase
"file:/u00/webadmin/config/domains/wls_retail/RPMDOMAIN/lib/-"
{
 permission java.security.AllPermission;
 permission
oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore", "read,write,update,delete";
 permission
oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore.*", "read,write,update,delete";
};
```

APPHOST2:

```
 grant codeBase
"file:/u00/webadmin/config/domains/wls_retail/RPMDOMAIN/servers/rpm-
server2/tmp/_WL_user/rpm/-"
{
permission java.security.AllPermission;
permission
oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore", "read,write,update,delete";
permission
oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore.*", "read,write,update,delete";
};

grant codeBase
"file:/u00/webadmin/config/domains/wls_retail/RPMDOMAIN/servers/rpm-
server2/cache/EJBCompilerCache/-"
{
permission java.security.AllPermission;
permission
oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore", "read,write,update,delete";
permission
oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore.*", "read,write,update,delete";
};


grant codeBase
"file:/u00/webadmin/config/domains/wls_retail/RPMDOMAIN/lib/-"
{
 permission java.security.AllPermission;
```

```
 permission
oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore", "read,write,update,delete";
 permission
oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore.*", "read,write,update,delete";
};
```

REIM:

Update the Policy file for REIM:

APPHOST1:

```
grant codeBase
"file:/u00/webadmin/config/domains/wls_retail/REIMDOMAIN/servers/reim-
server1/tmp/_WL_user/reim15/-" {
permission java.security.AllPermission;
permission oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore", "read,write,update,delete";
permission oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore.*", "read,write,update,delete";
};
```

APPHOST2:

```
grant codeBase
"file:/u00/webadmin/config/domains/wls_retail/REIMDOMAIN/servers/reim-
server2/tmp/_WL_user/reim15/-" {
permission java.security.AllPermission;
permission oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore", "read,write,update,delete";
permission oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore.*", "read,write,update,delete";
};
```

Configuration of OID Provider in WebLogic Domain

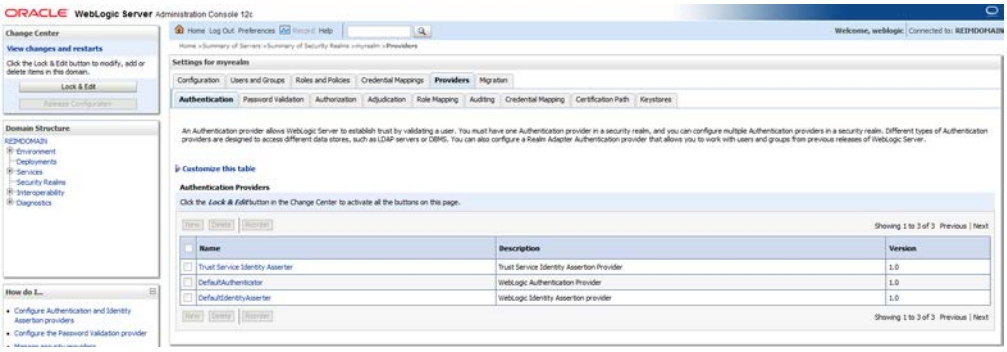
Note: In this section, the base DN "dn=us,dn=oracle,dn=com" is used as an example. Modify this value as per the organisation's ldap settings.

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

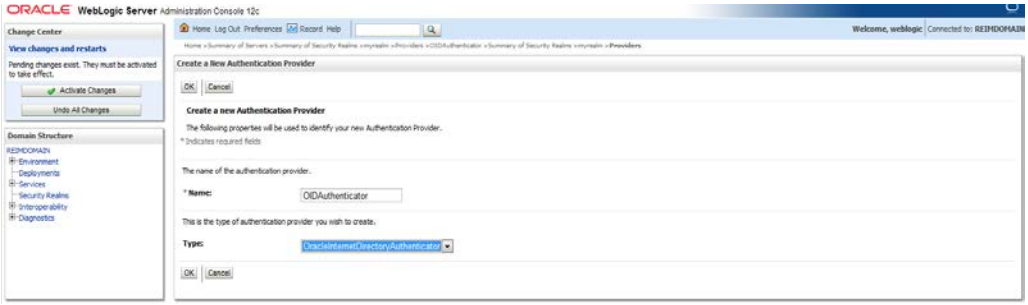
Log in to the Administration Console.

http://<host>:<port>/console/

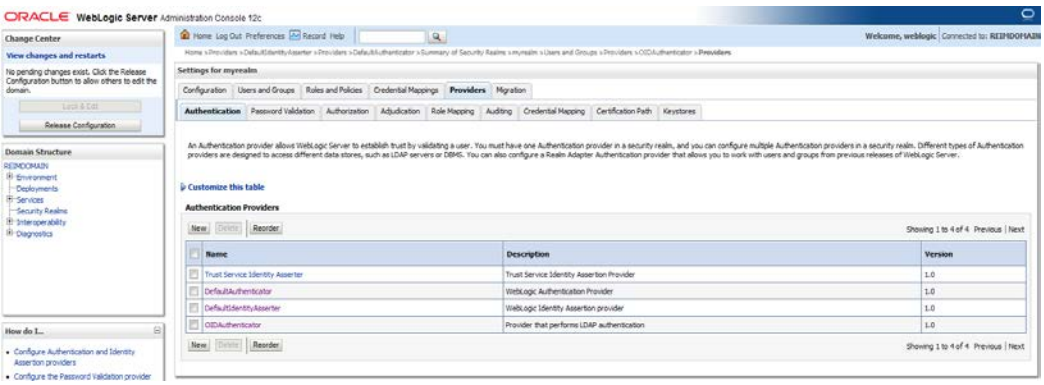
1. In the Domain Structure frame, click **Security Realms**.
2. In the Realms table, click **myrealm**. The Settings for myrealm window opens.
3. Click the **Providers** tab.



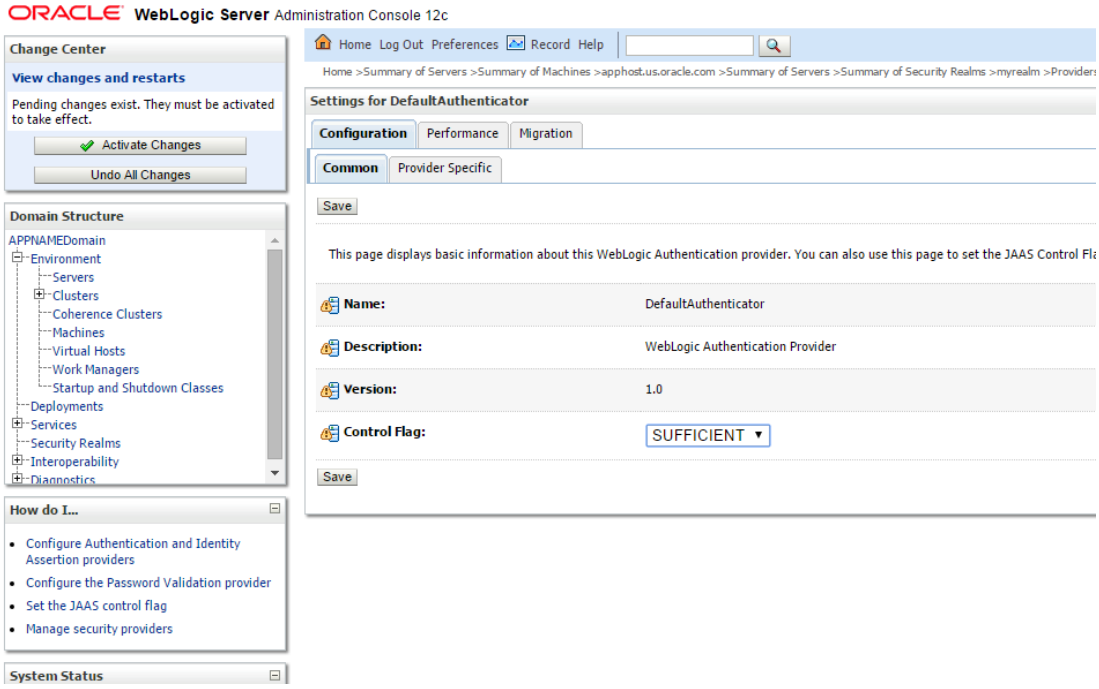
4. Click **Lock & Edit** and then click **New**. The Create a New Authentication Provider window opens.



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



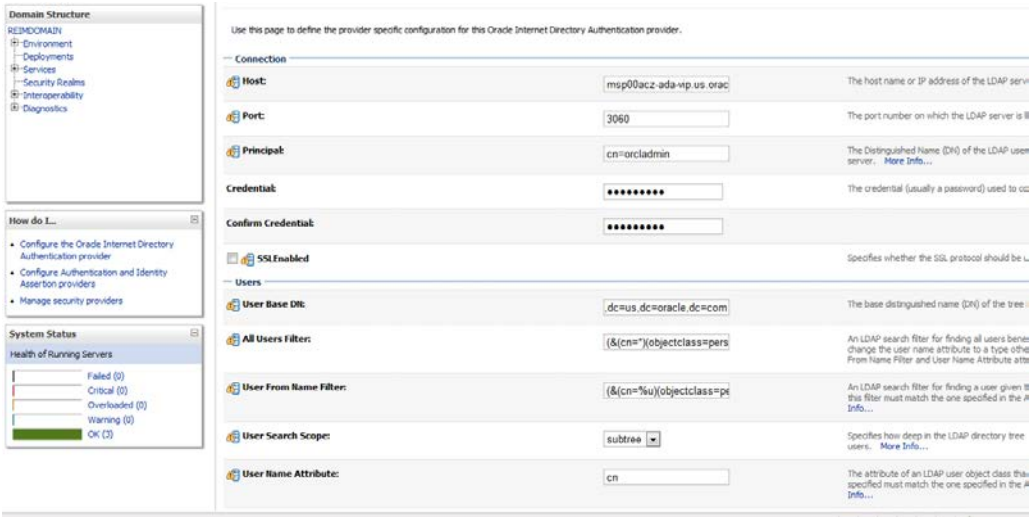
6. All the providers are displayed. Click **OIDAuthenticator**. Settings of OIDAuthenticator are displayed.
7. Set the Control Flag field to **SUFFICIENT**, and click **Save**.
8. From the Providers tab, click the **DefaultAuthenticator > Configuration tab > Common** tab. Update the Control Flag to SUFFICIENT.
9. Click **Save**.



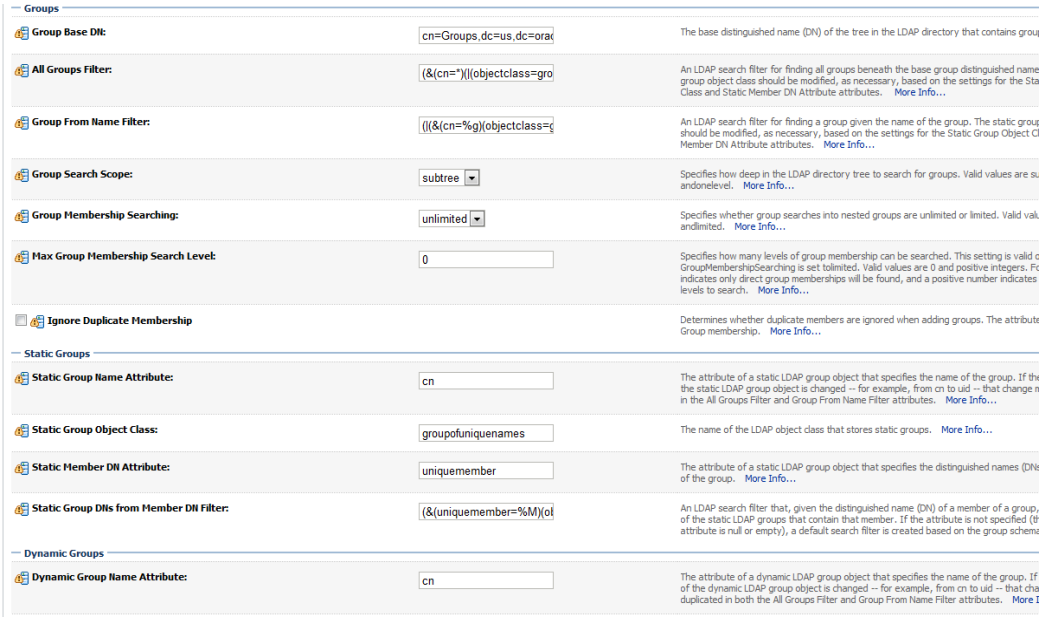
10. From the Providers tab, click the **OIDAuthenticator** (you just created), in the **configuration > Provider Specific** tab enter your LDAP connection details:

The values shown below are examples only. You should match the entries to your OID.

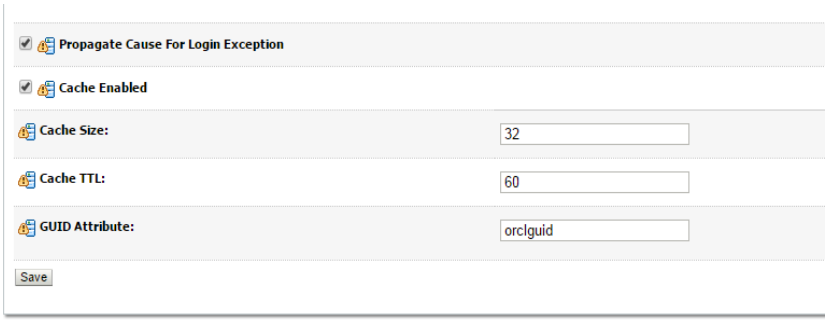
a. Host: *<oidhost>*
b. Port: *<oidport>*
c. Principal: cn=orcladmin
d. Credential: *<password>*
e. Confirm Credential: *<password>*
f. User Base DN: cn=users,dc=us,dc=oracle,dc=com
g. Check 'Use Retrieved User Name as Principal '.
h. Check 'SSL Enabled' if the OID is SSL enabled. Port mentioned above must be an SSL port if OID is enabled.



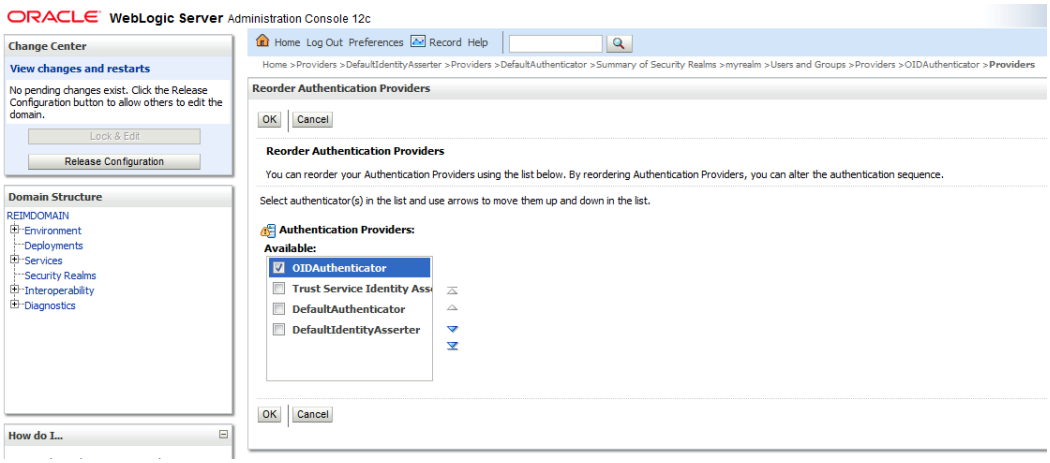
11. Modify the following:
    a. Group Base DN: cn=Groups,dc=us,dc=oracle,dc=com



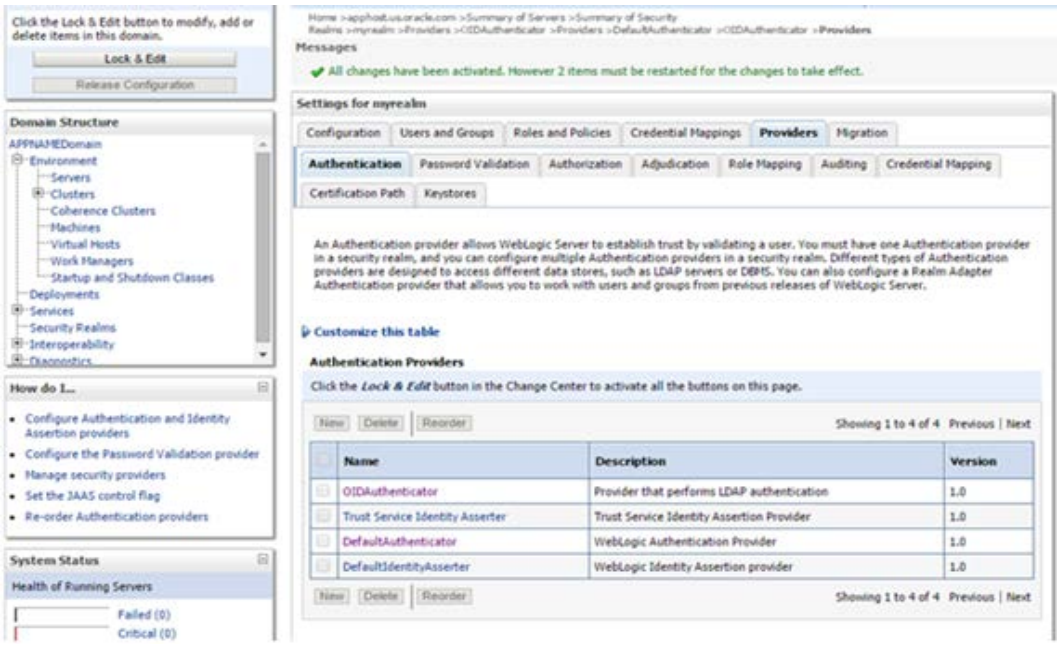
12. Check **Propagate Cause For Login Exception**.



13. Click **Save**.
14. Click the **Providers** tab.
15. Click **Reorder**.
16. Move OIDAuthenticator to the top of the providers list



17. Click **OK**.
18. Once your changes are saved, click **Activate Changes**.



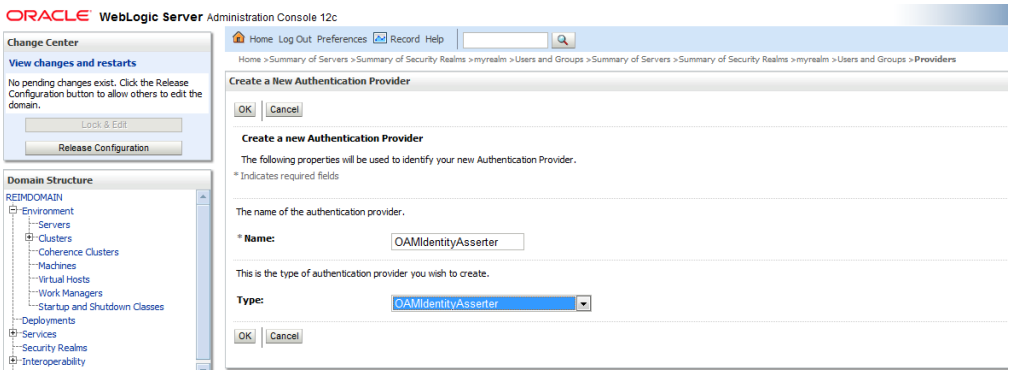
19. The control flag for Default Authenticator should be sufficient.
20. Restart Weblogic Adminserver and Managed server.
21. The above screens are examples for REIMDOMAIN. Please follow the same for other domains.

Configure Oracle Single Sign-On

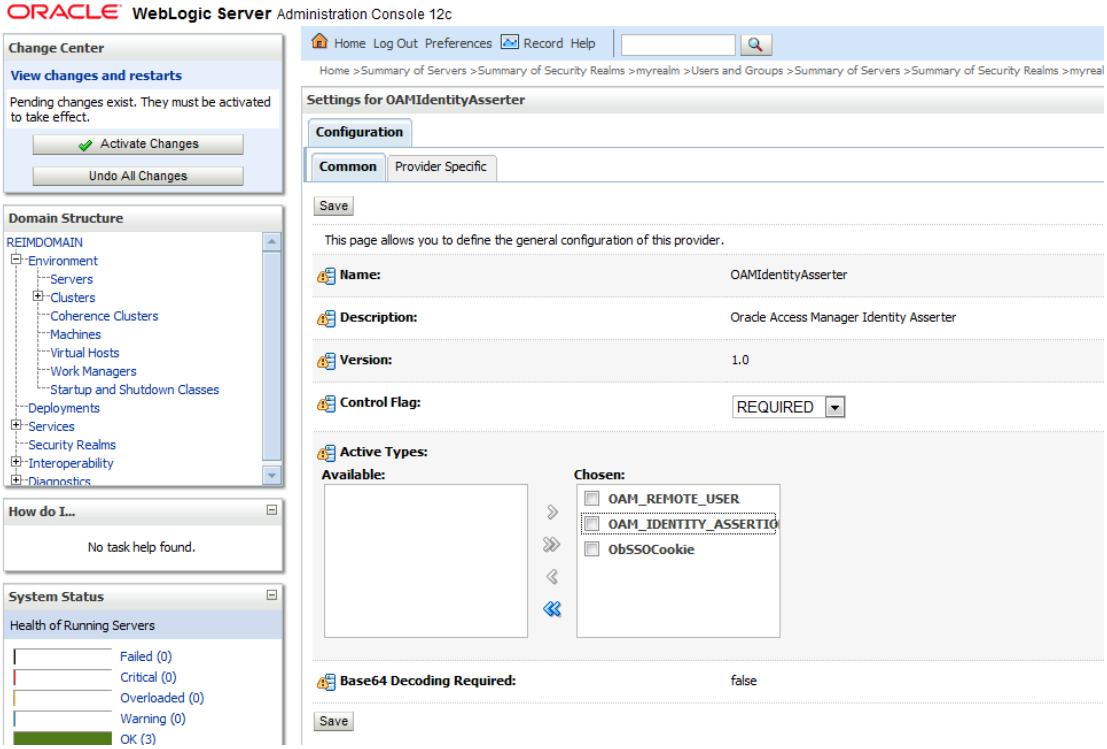
Note: This procedure is only needed if you plan on setting up the ReIM application using Single Sign On (SSO) authentication. This can be skipped if SSO is not going to be configured for this environment. The Oracle Access Manager must be configured and the Oracle http server (Webtier and webgate) must be registered into the Oracle Access Manager.

Create the SSO provider in the REIMDomain

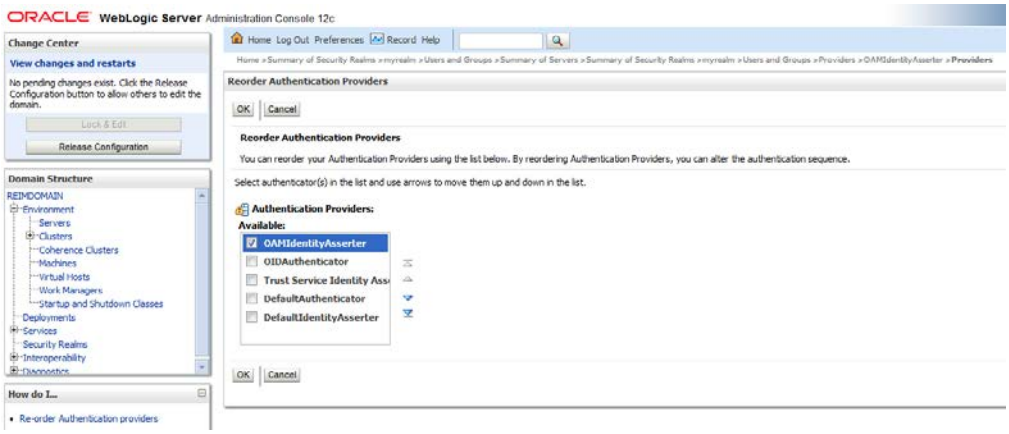
1. Log into the WebLogic console
2. Navigate to **security realms > myrealm (default realm) > providers**.
3. Start a Lock and Edit session.
4. Click **New provider**.
5. Set the provider name (Default: OAMIdentityAsserter).



6. Click **OK**.
7. Open the new provider configuration. Under Common, set the Control Flag to **REQUIRED**.



8. On the provider list, click **Reorder**.
9. Move the OAMIdentityAsserter to the top of the list, or above the DefaultAuthenticator.

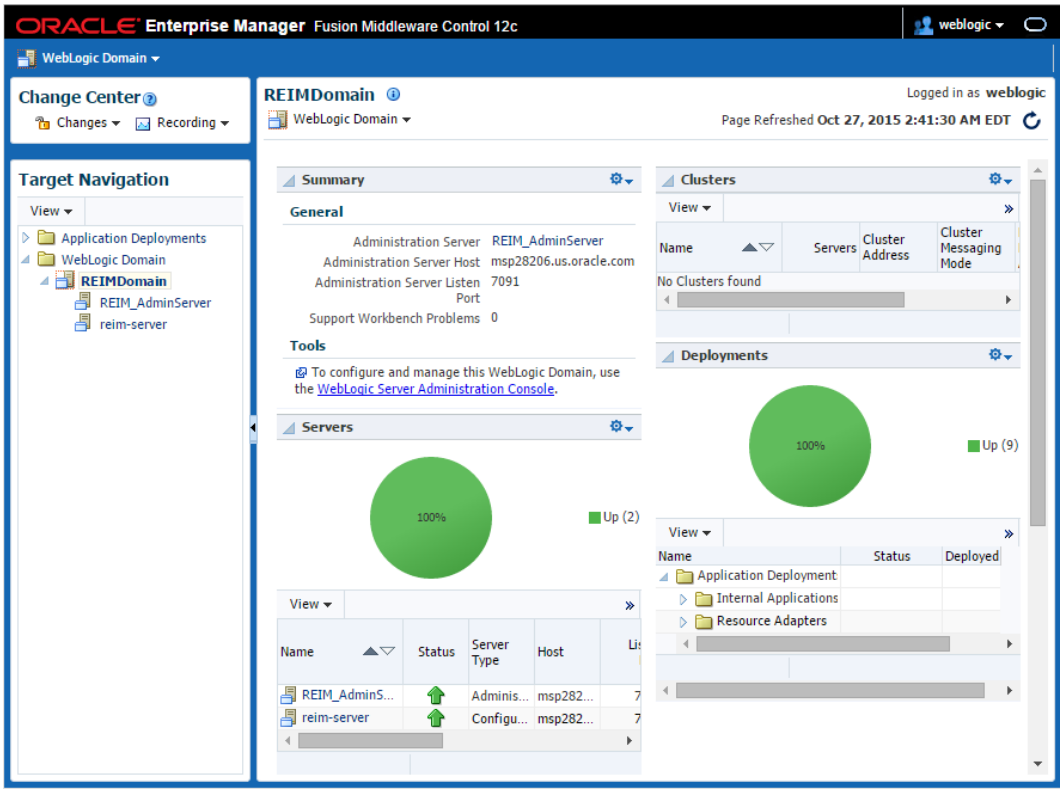


10. Click **OK**.
11. Click **Activate Changes**.
12. Shutdown the domain.
13. Start the admin and managed servers for the domain.
14. Configure SSO provider in ALLOCDOMAIN, RESADOMAIN, SIMDOMAIN, RPMDOMAIN also.

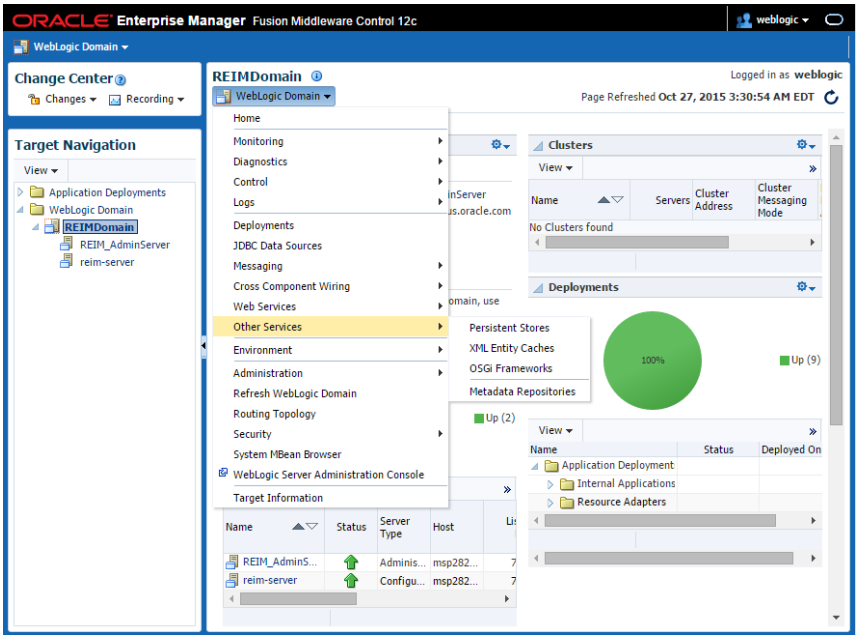
Creating mds-CustomPortalDS Datasource using EM

Follow the below steps to create mds-CustomPortal datasource.

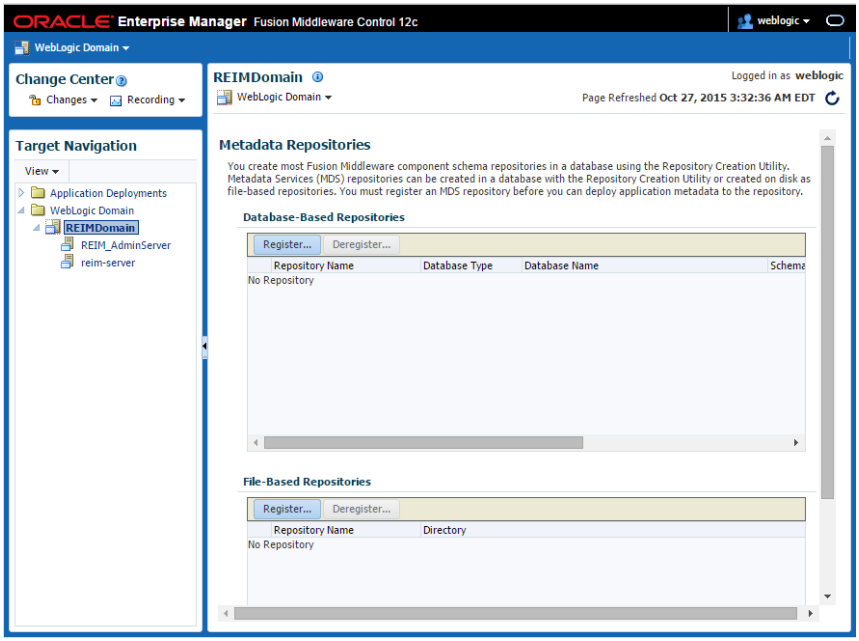
Login to EM console.



1. Navigate to **WebLogic Domain > Other Services > MetaData Repositories**.

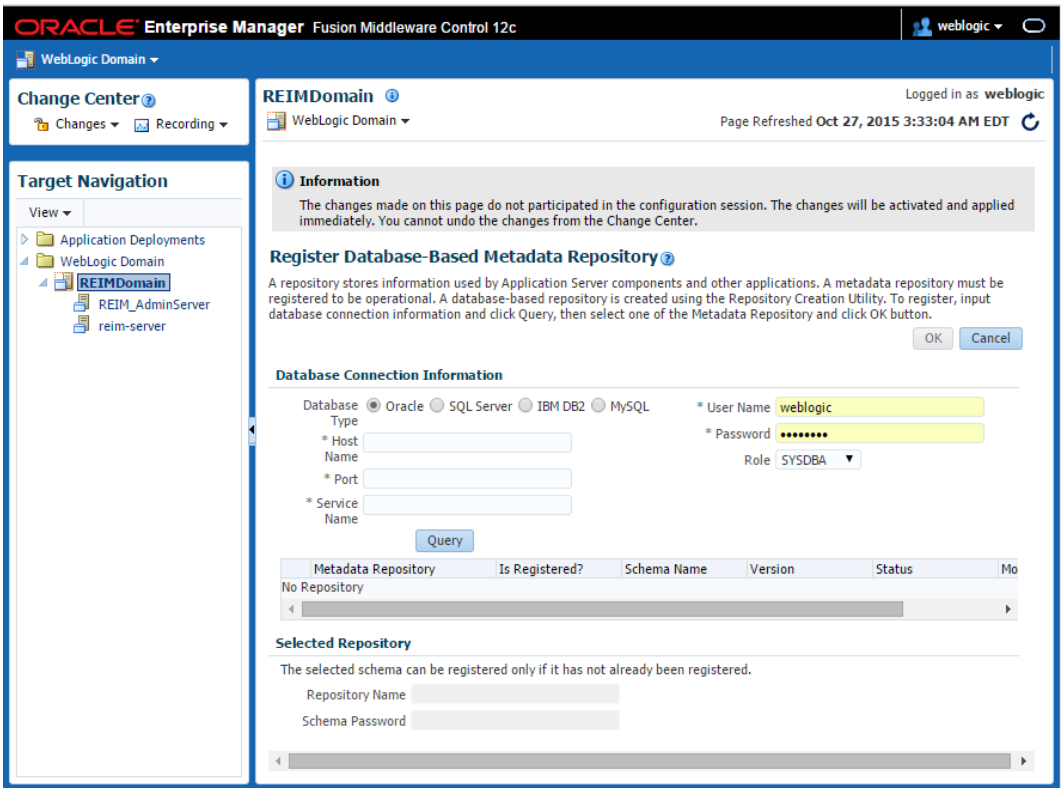


2. Under Database-Based Repositories, click the **Register** button.

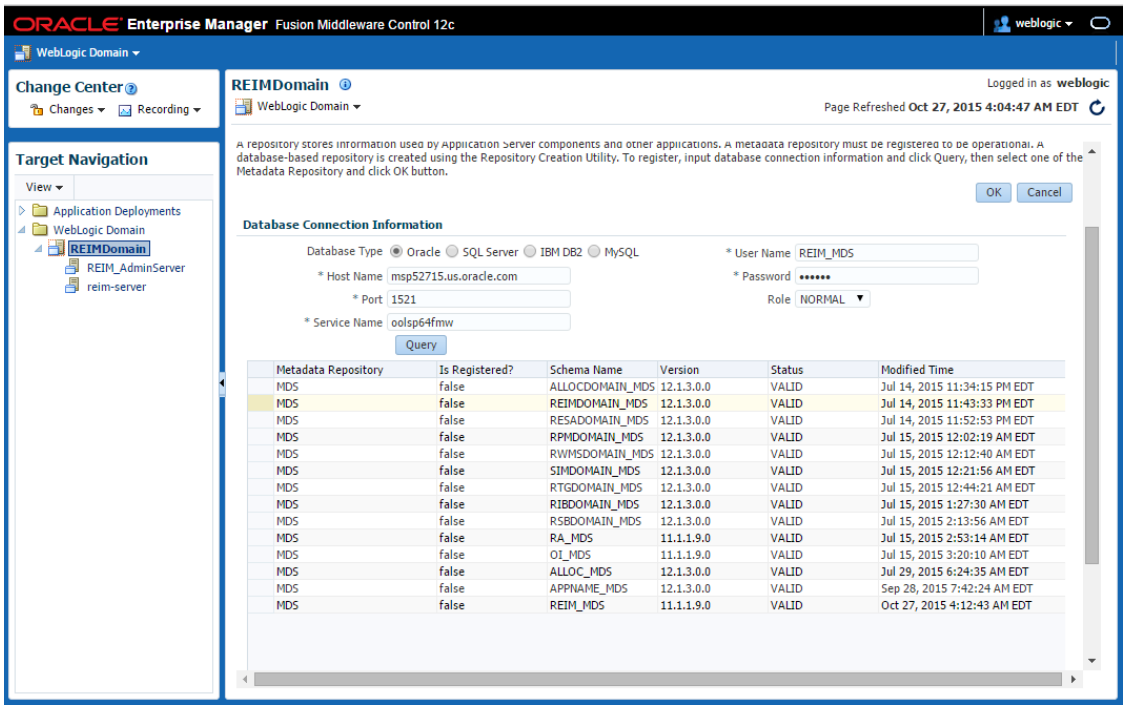


3. Remove weblogic user if it appears in the Username field. Provide the MDS Schema user created in RCU as part of RCU schemas creation.

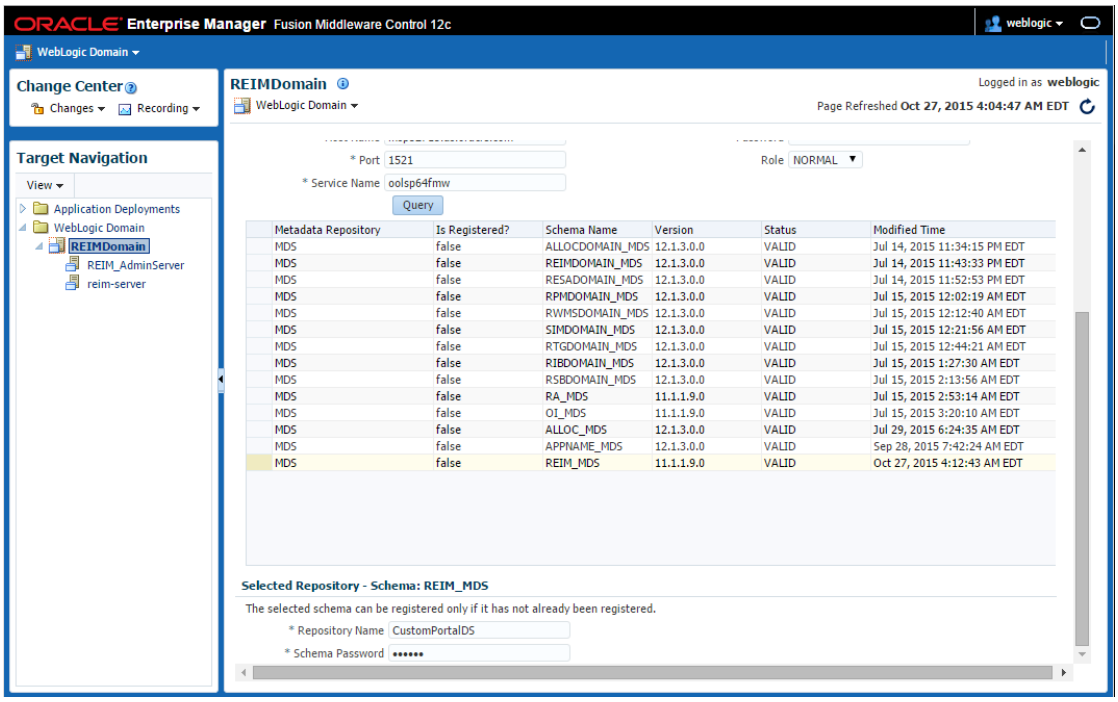
   Example: REIM_MDS



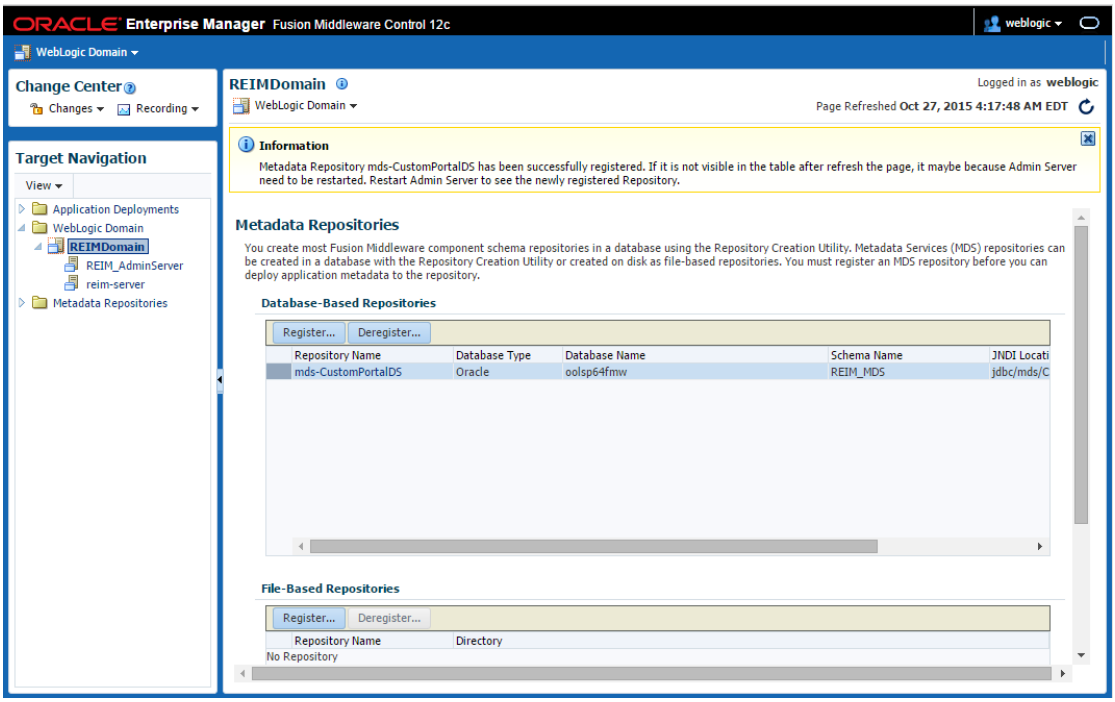
4. Input the details of Database Hostname, Port number and Service name. Click **Query** and a list of all the schemas will be displayed.



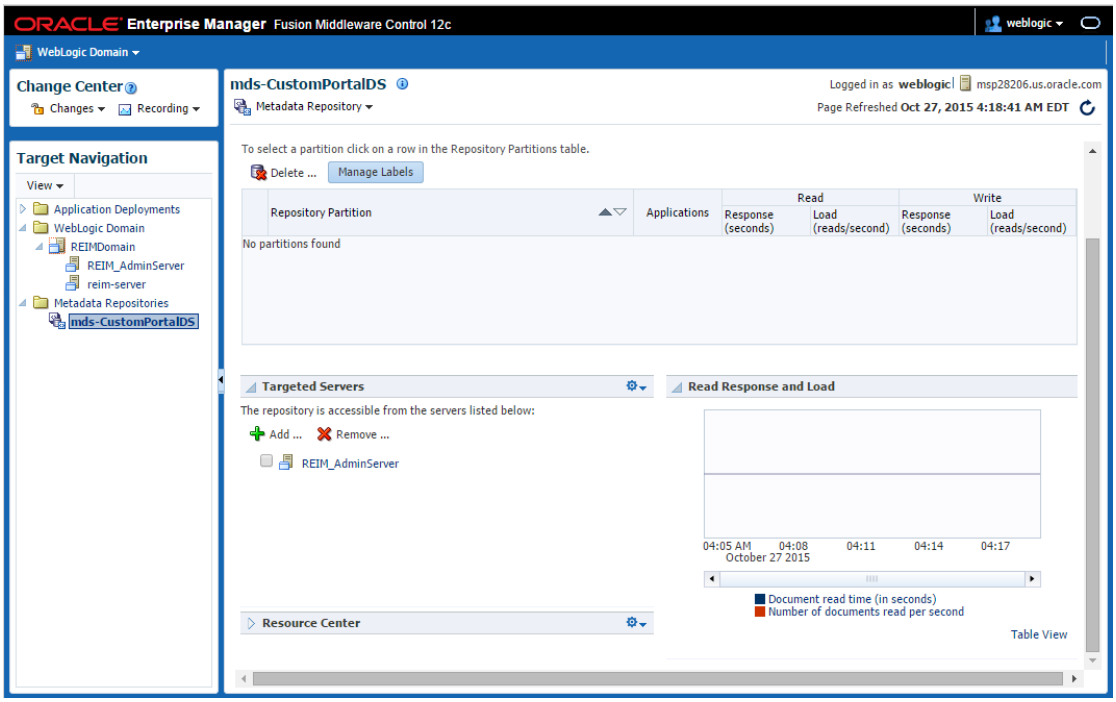
5. Select the <**ALLOC_MDS**> schema. Enter the repository name as **CustomPortalDS,** and enter the password. Click **OK**.

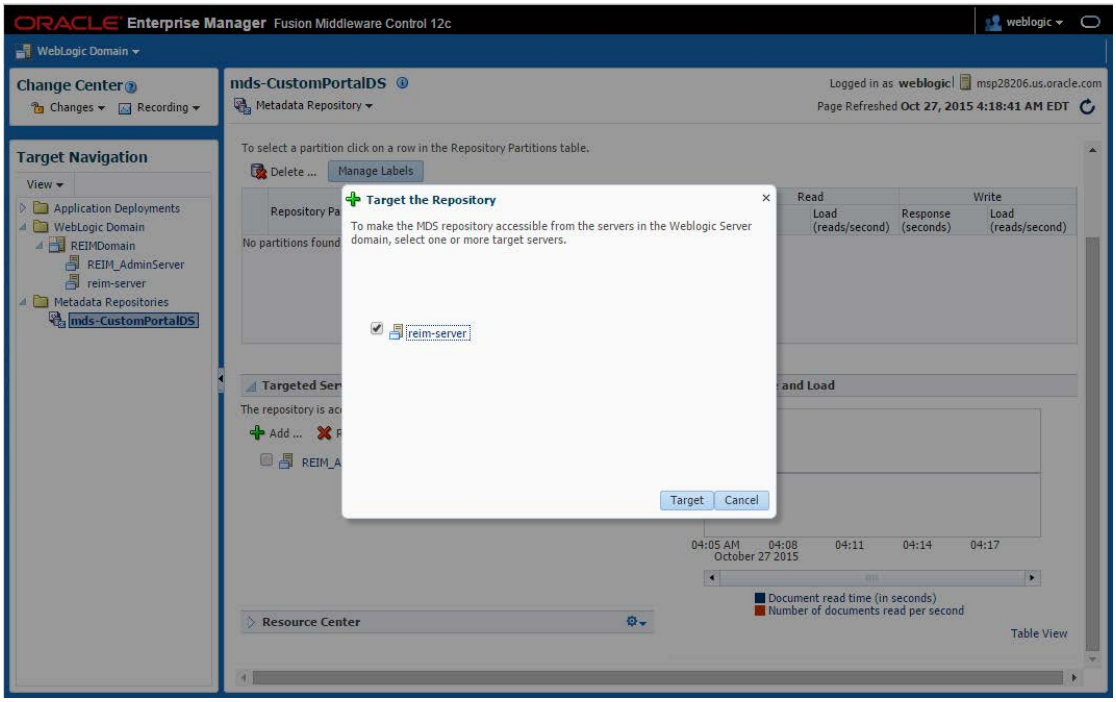


6. The MDS Repository will appear. Click **mds-CustomPortalDS**.

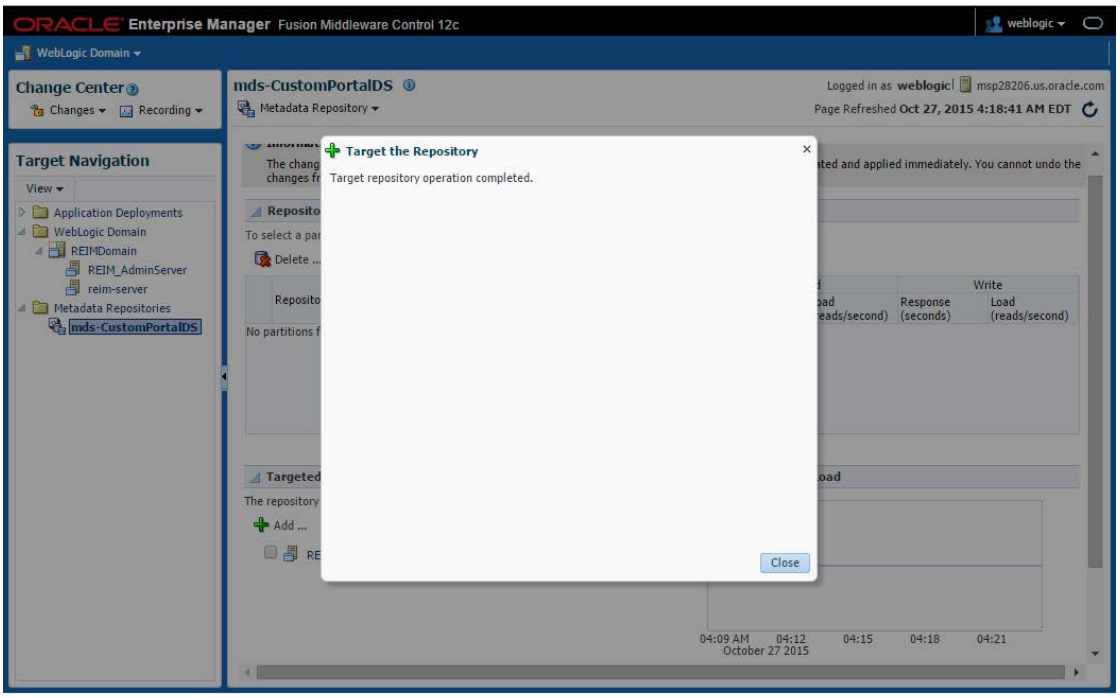


7. Under Targeted Servers, Click **add** and add the managed server **alloc-server**. Click **Target**.

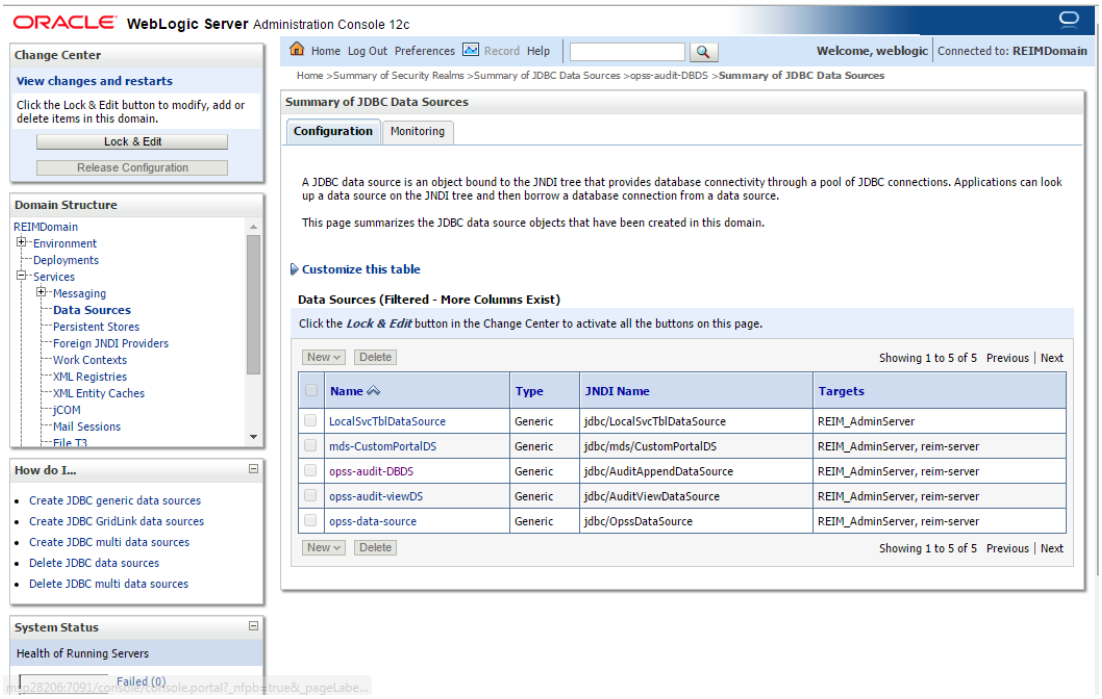




8. A message Target repository operation completed is displayed. Click **Close**.



9. Restart the Admin server and the Managed server. Login to the Admin console URL and verify mds-CustomPortalDS datasource exists.



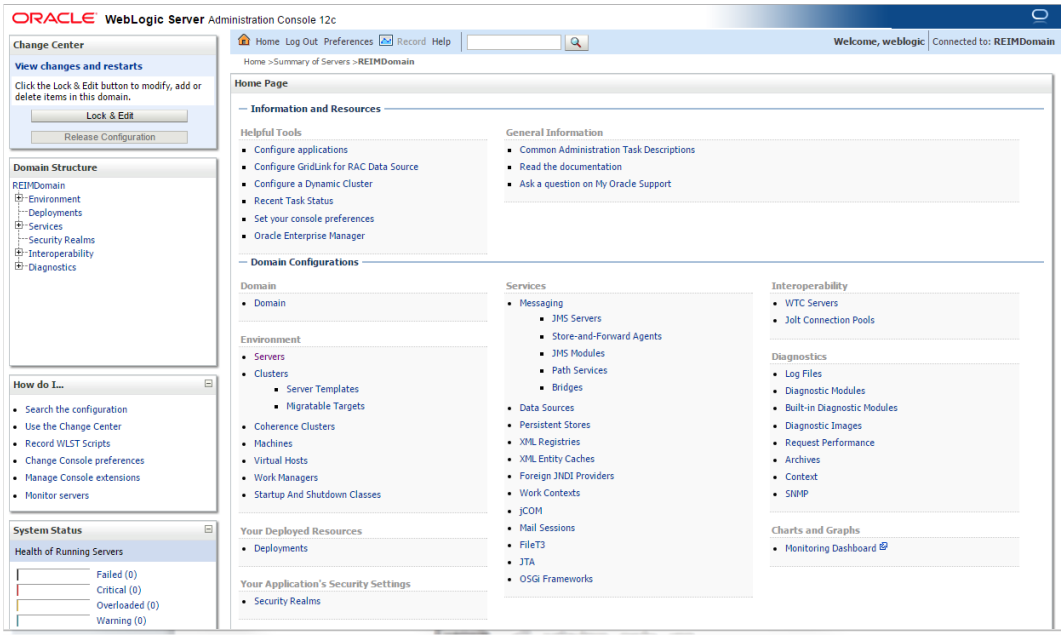
Note: Above is example for REIM and please Follow the above steps for all the domains and bounce whole domain.

Deployment of jax-rs-2.0 library in WebLogic

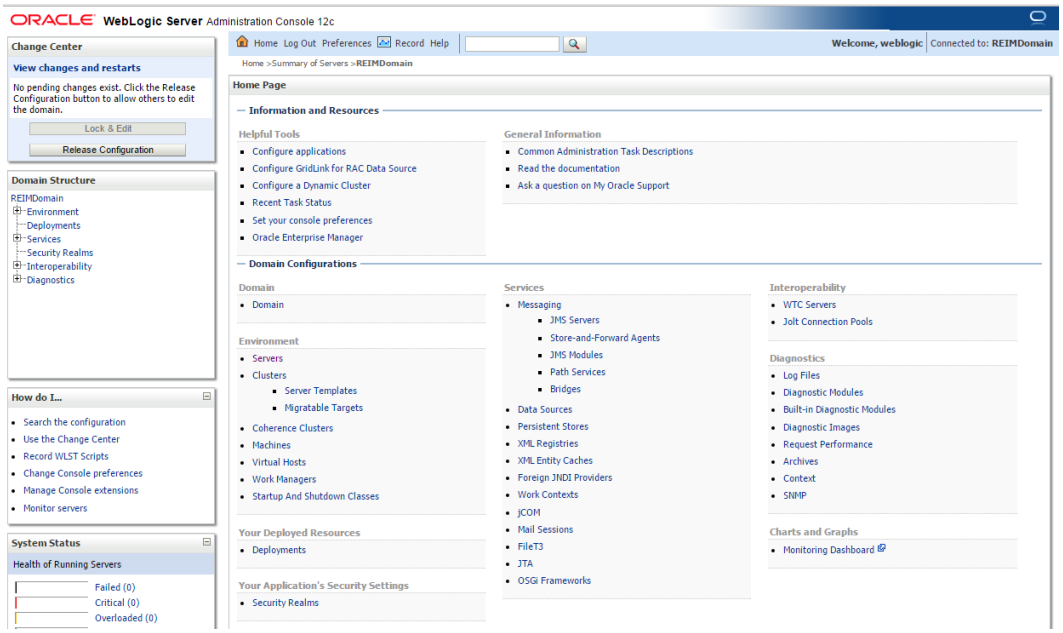
The library jax-rs-2.0.war needs to be deployed in WebLogic prior to ReIM Application install. This library is available at /u00/webadmin/products/wls_retail/wlserver/common/deployable-libraries/jax-rs-2.0.war.

Perform the following procedure to deploy the jax-rs-2.0 library:

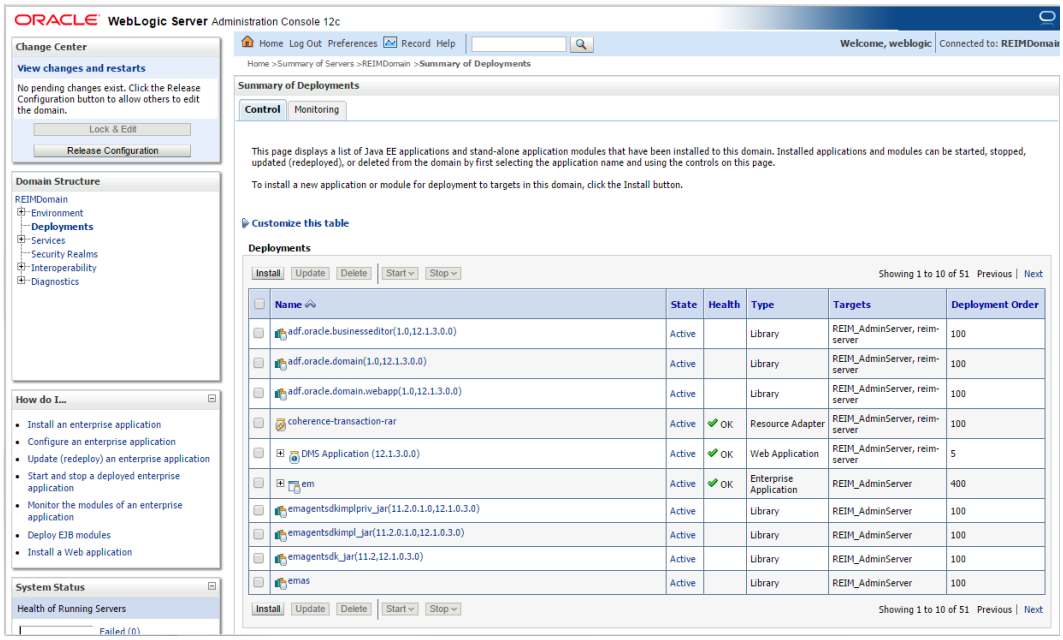
1. Login to the WebLogic Admin Console.



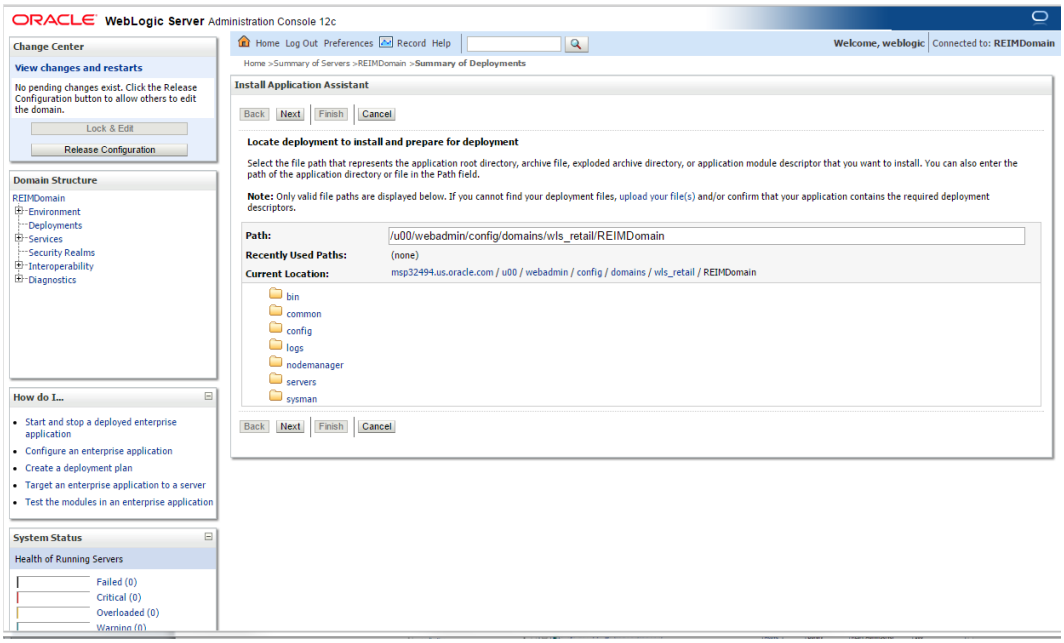
2. Click **Lock and Edit**.



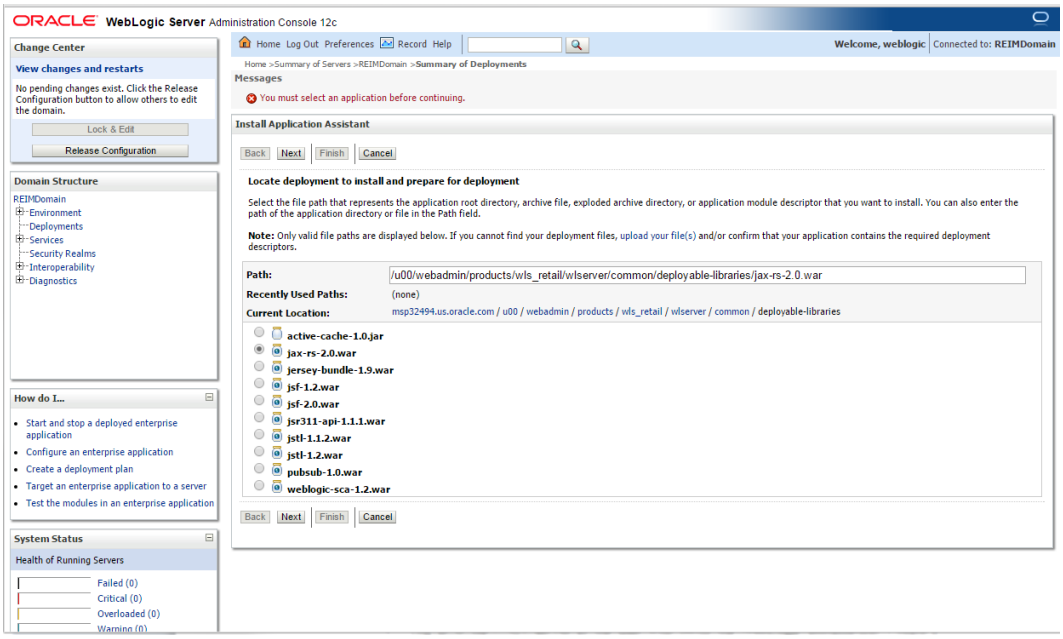
3. Click **Deployments**.



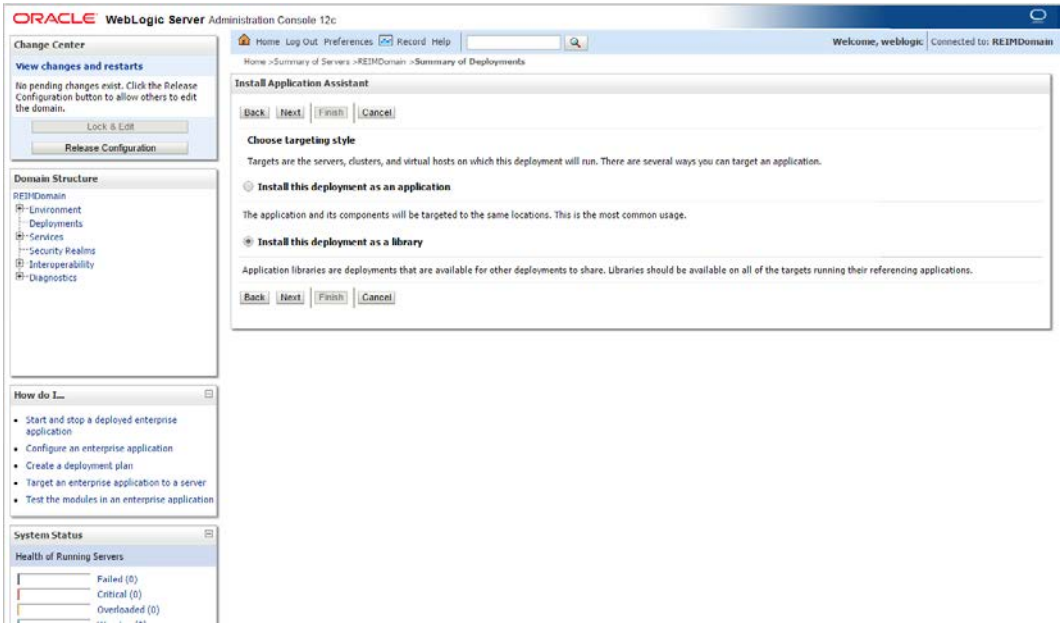
4. Click **Install**.



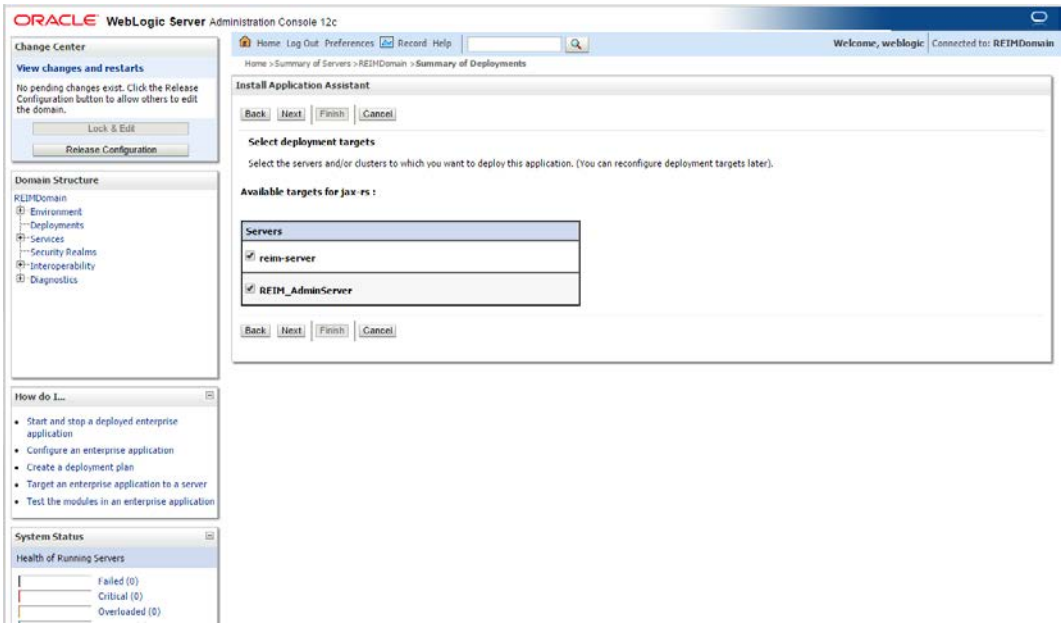
5. Select the library from the path /u00/webadmin/products/wls_retail/wlserver/common/deployable-libraries/jax-rs-2.0.war on the server. Click **Next**.



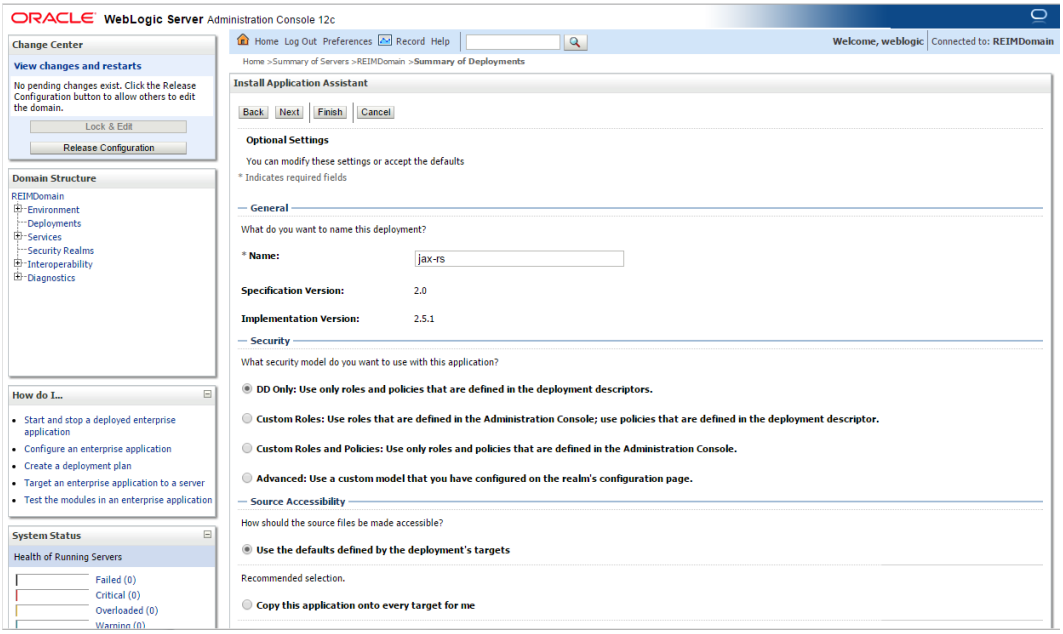
6. Select **Install the deployment as a library**. Click **Next**.



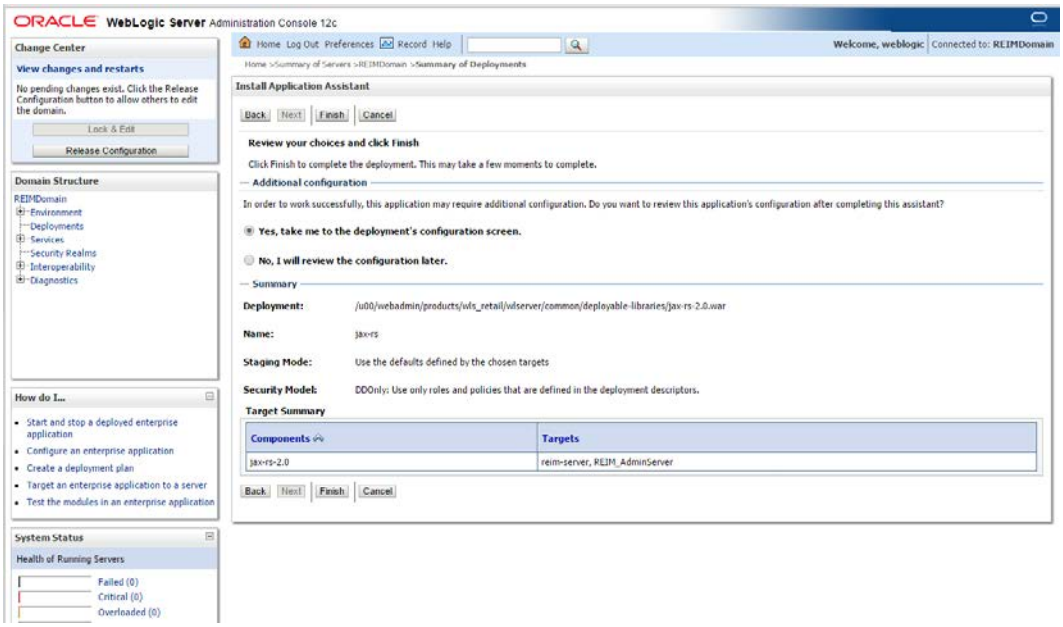
7. Target to both Admin server (eg:REIM_AdminServer) and Managed server(eg: reim-server). Click **Next**.



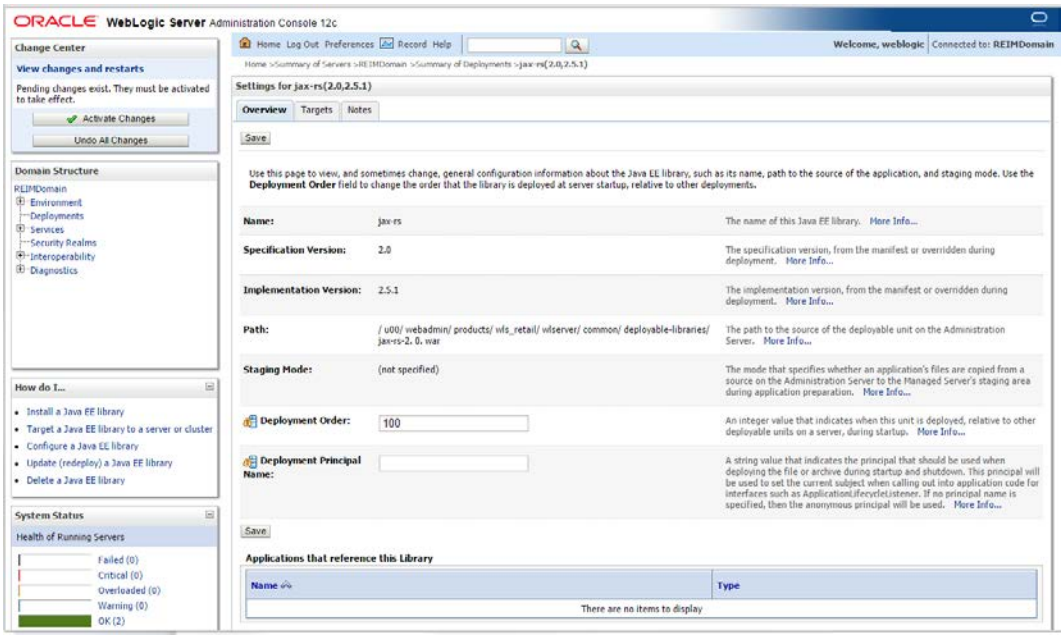
8. Retain the default value for Name as **jax-rs**, and click **Next**.



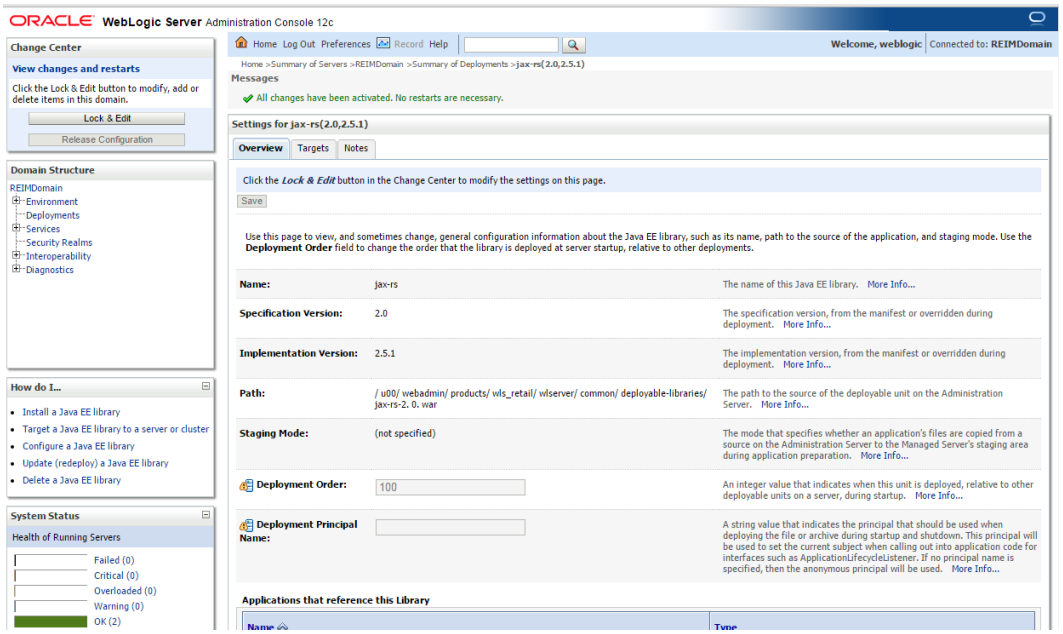
9. Select **Defaults** and click **Finish**.



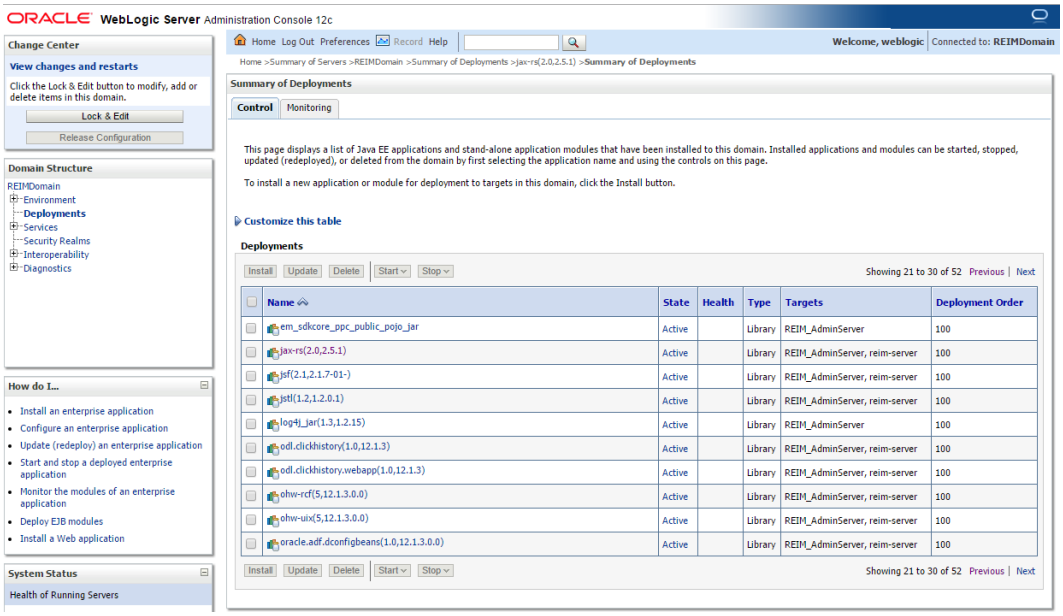
10. Click **Activate Changes**.



11. The following window opens.



12. Verify the jax-rs library is shown in the Deployments.



Note: Above is example for REIM and please Follow the above steps for all the domains and bounce whole domain.

4

Installing the REIM Application

This Chapter describes the Pre-installation task, on how to install the ReIM application and how to perform post installation for Cluster configuration. And also describes on WebTier settings for REIM.

Prerequisite Task for REIM

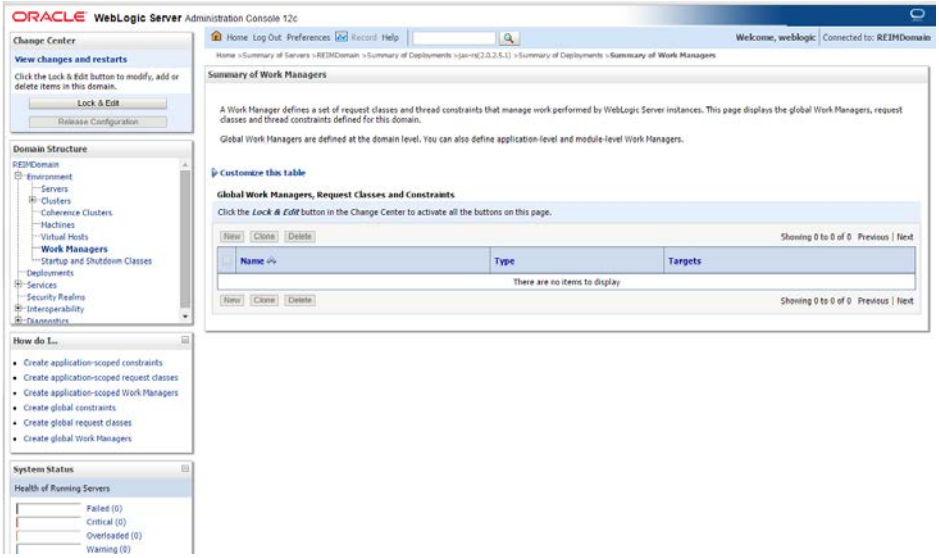
Steps to Configure WebLogic Work Manager

For the Invoice Matching Batch programs to use independent work managers for the thread processing, we need to create a work manager for each batch program. The names of the work managers need to be exactly the same as the ones mentioned in the table below. In case a named work manager is not created, the default work manager will be used by the server.

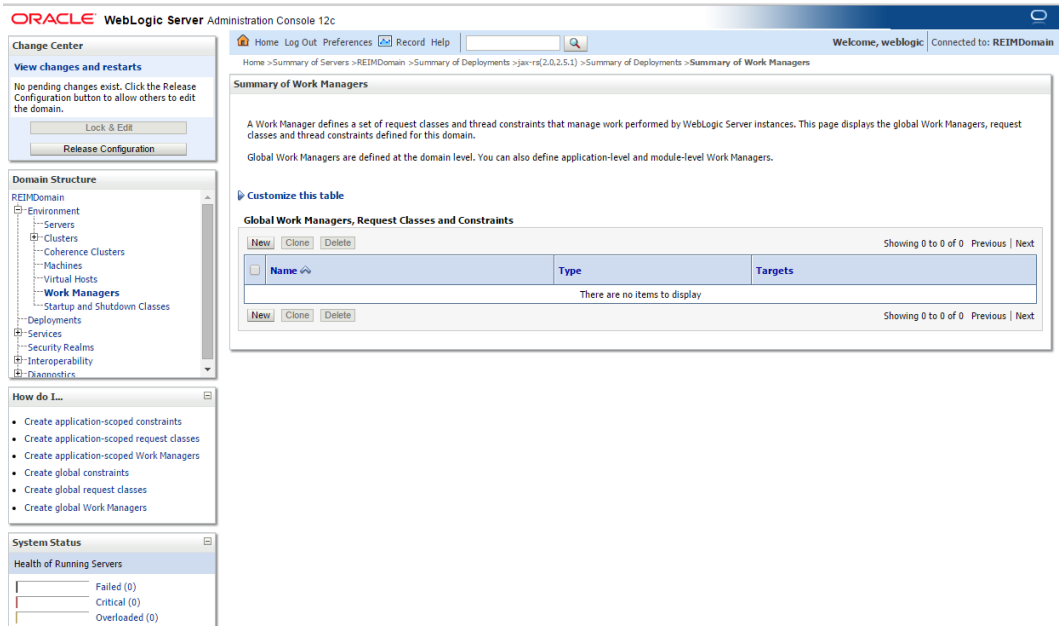
Batch Name	Work Manager
Automatch	AutoMatchWM
Edi Injector	EdiInjectorWM
Credit note automatch	CNAutoMatchWM
Complex deal upload	CDUploadWM
Fixed deal upload	FDUploadWM
Financial Posting	PostingWM

Steps to Create a Named Work Manager

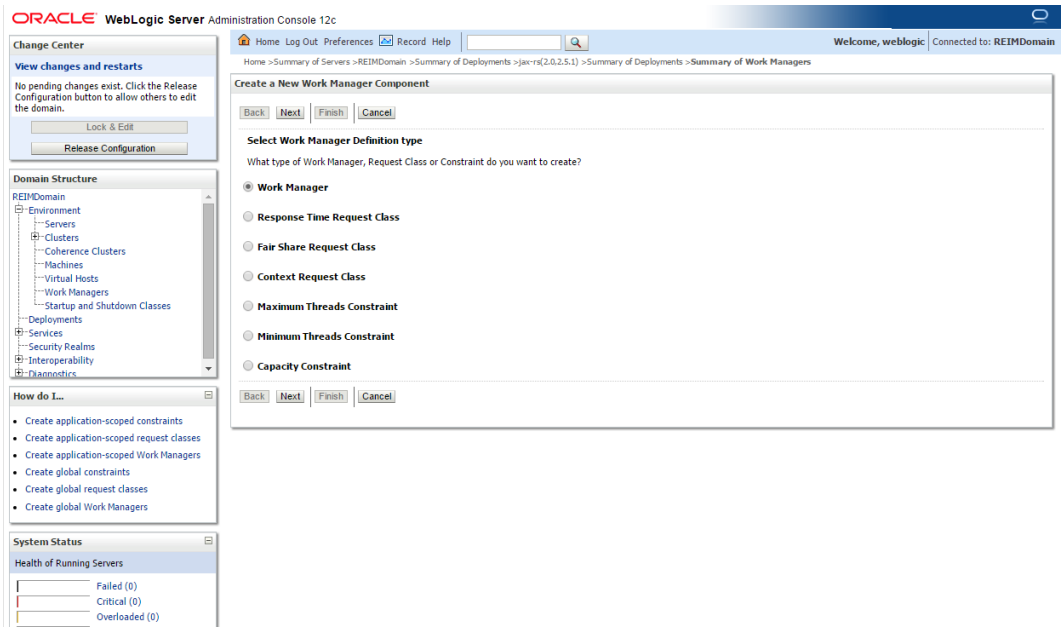
1. From WebLogic Console navigate to Work Manager pane (**Domain>Environment>Work Manager**).



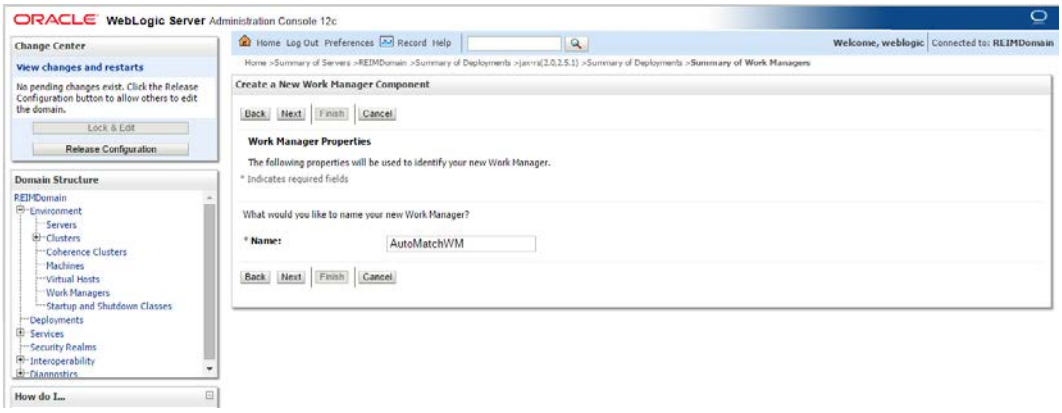
2. Click **Lock and Edit**.



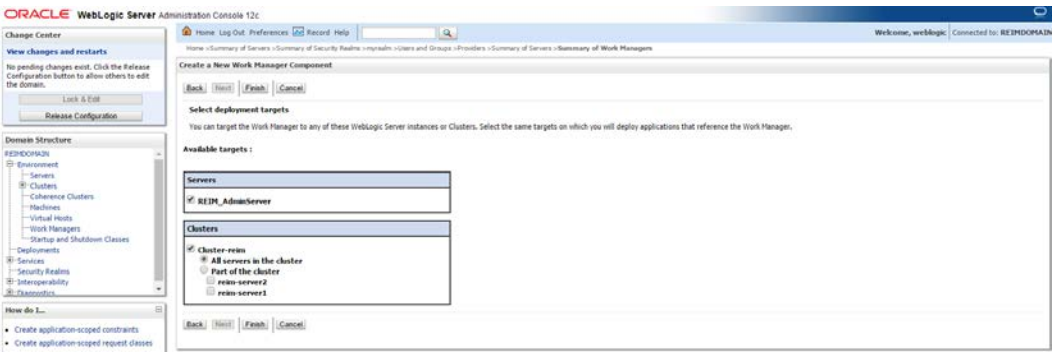
3. Click New. This will take us to the screen which allows us to create work managers and other related classes like constraints. Click **Next**.



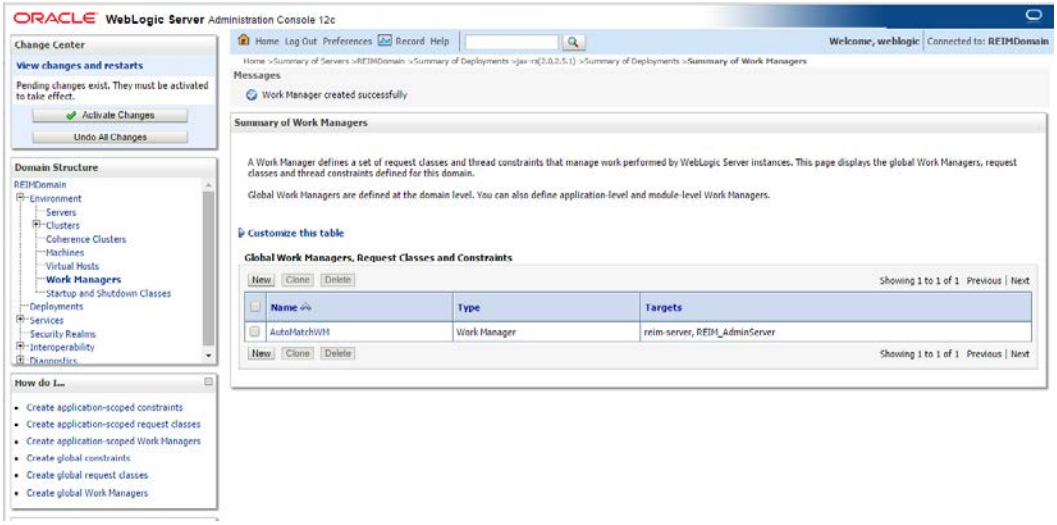
4. Provide the name of the work manager as mentioned in the table above.
   Example: AutoMatchWM



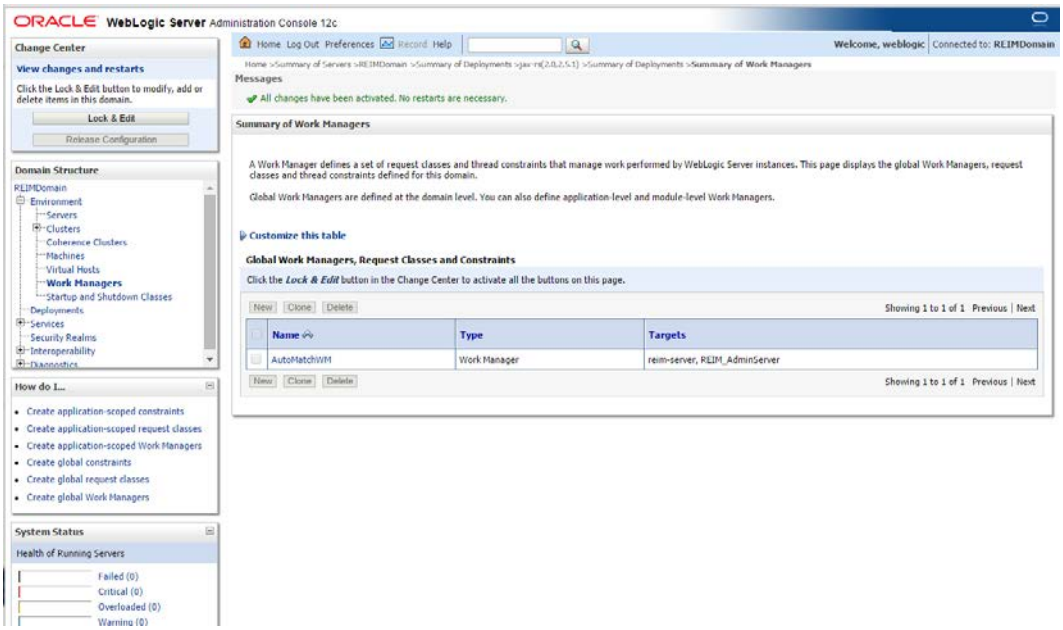
5. Target it to both Admin Server and the managed server (<Example>: REIM_AdminServer and Cluster-reim).



6. Click **Finish**.



7. Click **Activate Changes**.

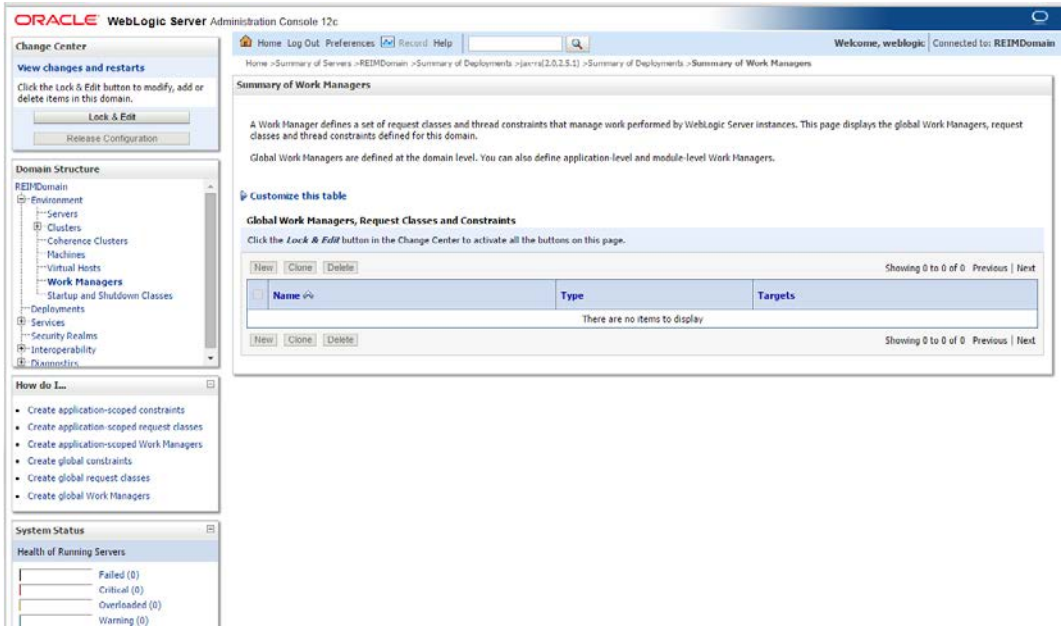


You can see the named work managers created in the list.

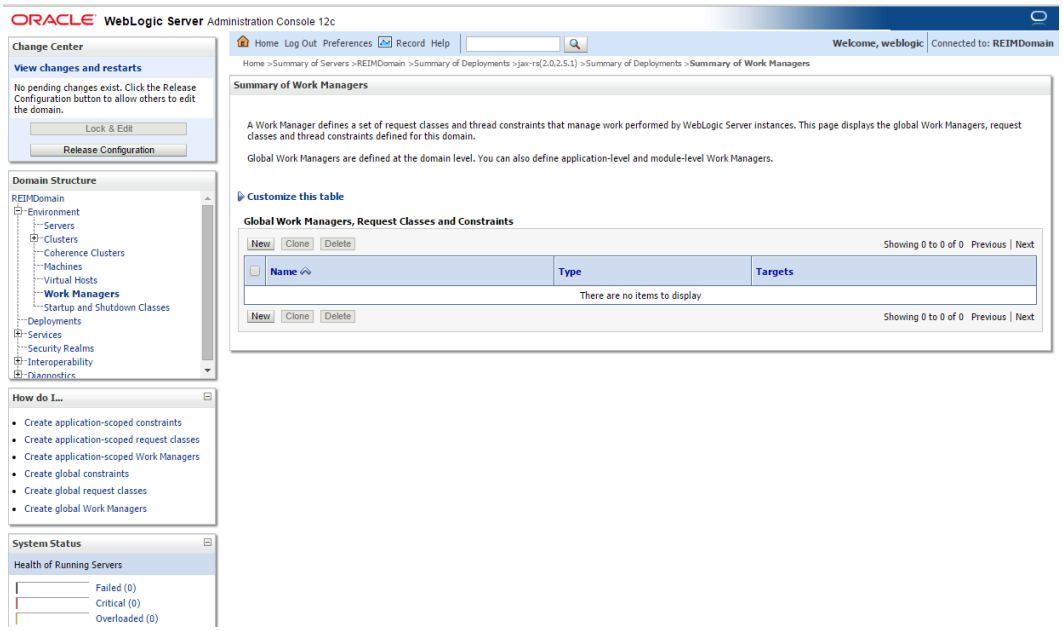
Steps to Create Maximum thread constraints

Maximum thread constraints can be assigned to work managers. Steps to create constraints and to assign them to work managers are as below:

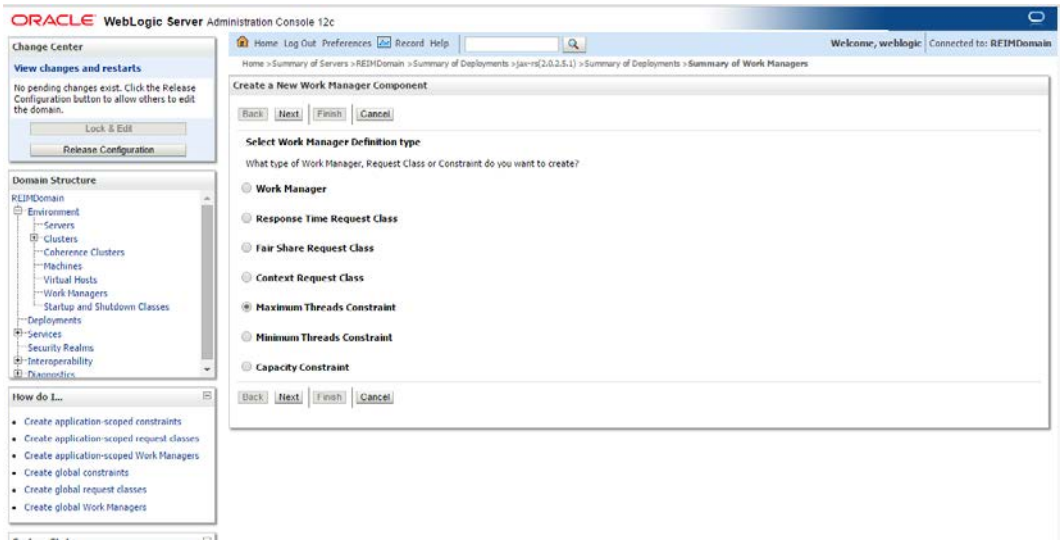
From WebLogic Console navigate to Work Manager pane (**Domain > Environment >Work Manager**)



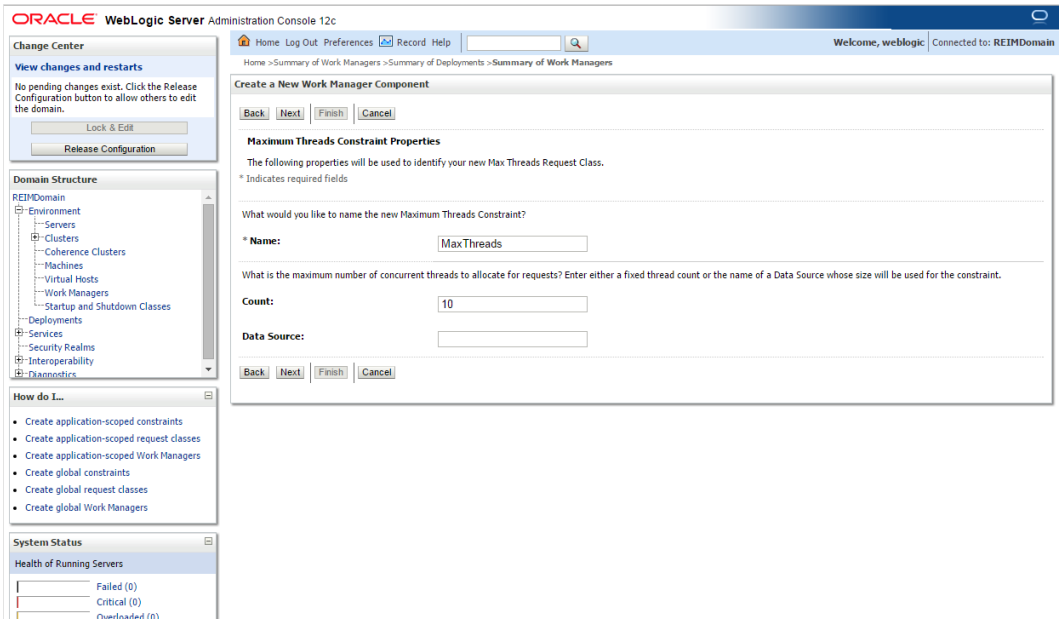
1. Click **Lock and Edit**.



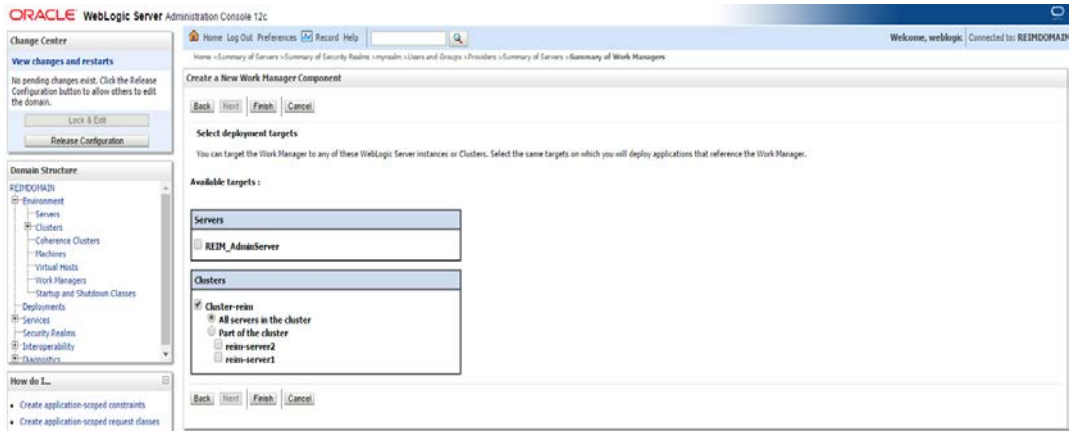
2. Click **New**. This will take us to the screen which allows us to create constraints.



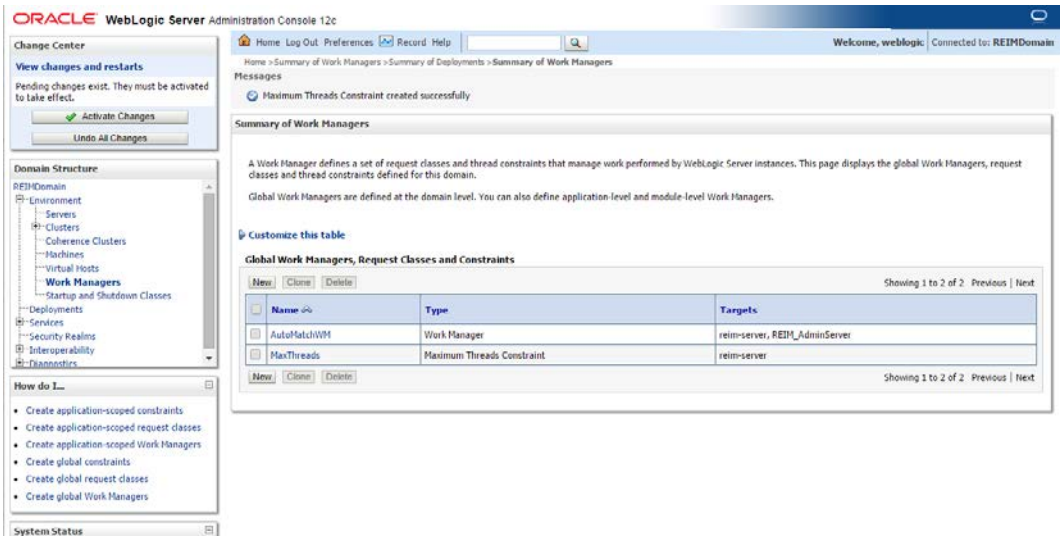
3. Select the **Maximum Thread Constraint** radio button, and click **Next**.
4. Give a Name (MaxThreads) and specify maximum number of consumers needed for your Application. Click **Next**.



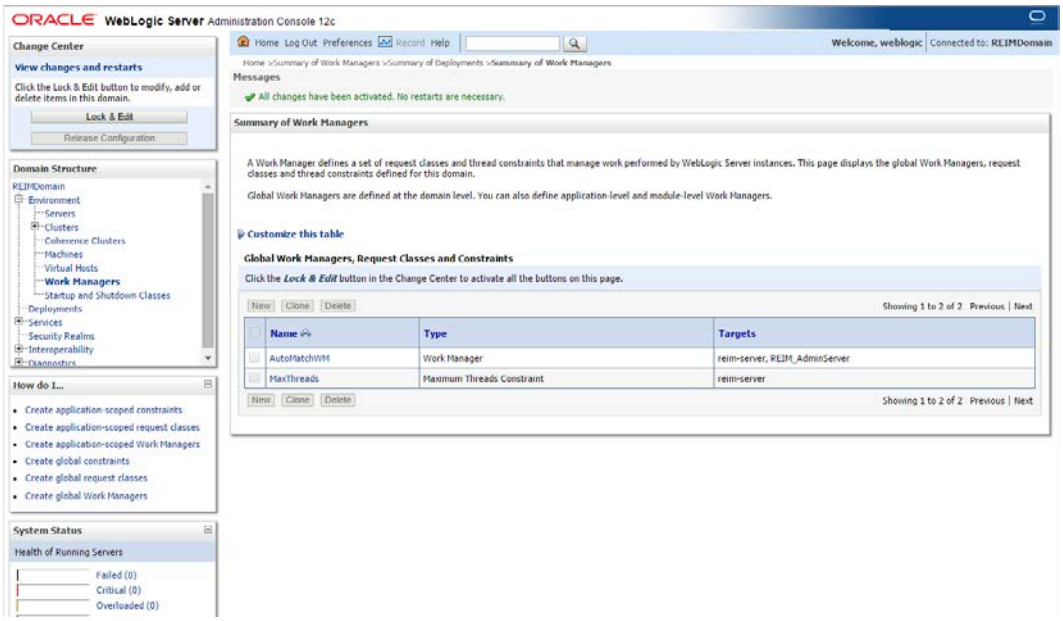
5. Select **Cluster-reim** from the Clusters box, and click **Finish**.



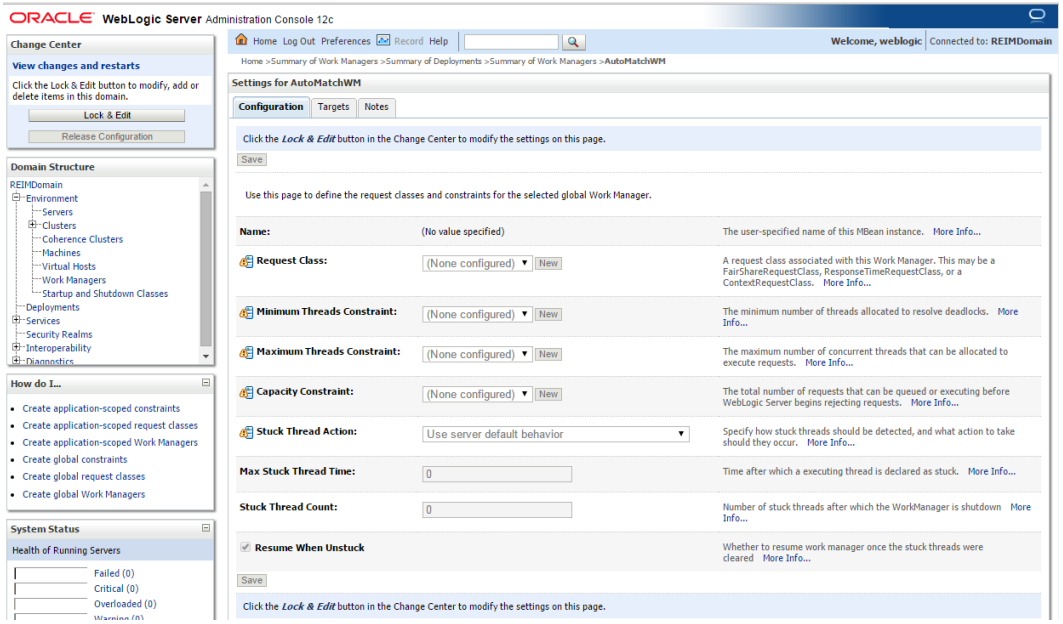
6. Click **Activate Changes**.



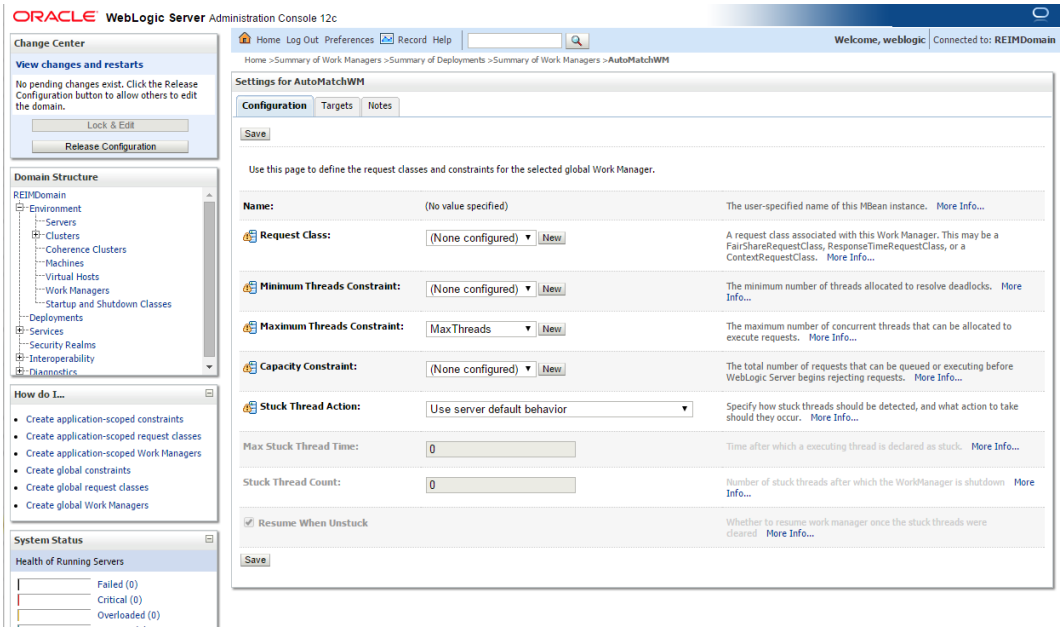
7. The Summary of the work managers window opens.



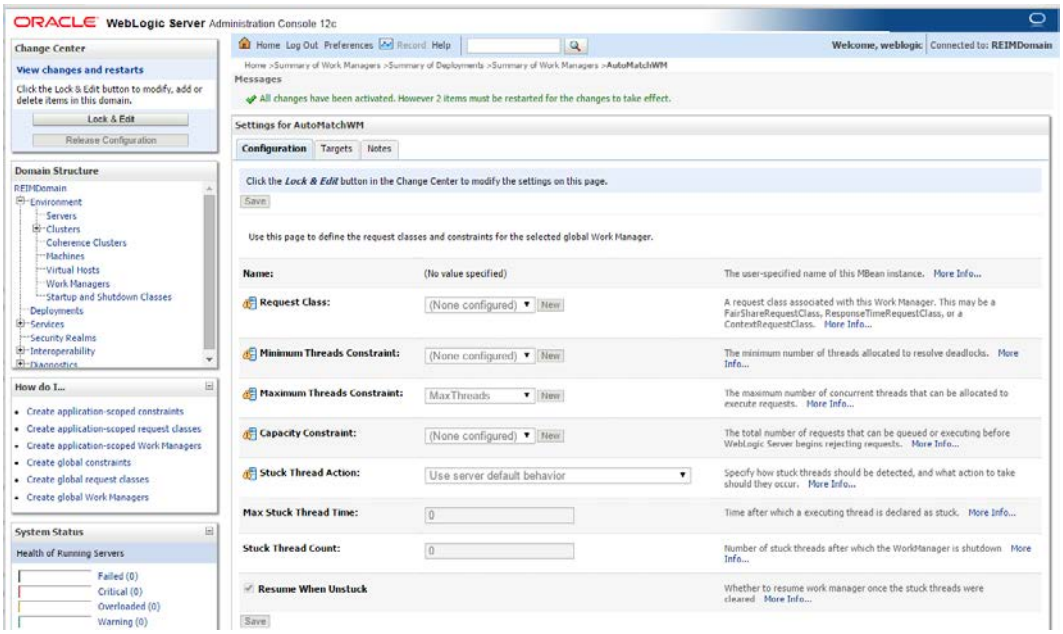
8. Click the work manager link from the Summary of work managers. Example: AutoBatchWM



9. Click **Lock and Edit**.
10. From the Maximum Thread Constraint dropdown, select the constraint you have created earlier.



11. Click **Save**.
12. Click **Activate Changes**.



13. Restart Weblogic Adminserver and Managed server.

Clustered Installations – Preinstallation Steps

Make sure that you are able to start and stop the managed servers that are part of the ReIM Cluster from the WebLogic Admin Console.

Expand the ReIM Application Distribution

To expand the ReIM application distribution, do the following.

1. Log in to the UNIX server as the user who owns the WebLogic installation. Create a new staging directory for the ReIM application distribution (reim15application.zip). There should be a minimum of 300 MB disk space available for the application installation files.

   Example: /u00/webadmin/media/REIM

   This location is referred to as INSTALL_DIR for the remainder of this chapter.
2. Copy reim15application.zip to INSTALL_DIR and extract its contents.

   Example: unzip reim15application.zip

Run the Oracle Retail Invoice Matching Installer

Once you have a managed server that is configured and started, you can run the Oracle Retail Invoice Matching application installer. This installer configures and deploys the Oracle Retail Invoice Matching application.

Note: See Appendix A: Oracle Retail Invoice Matching Application Installer Screens for details about every screen and field in the application installer.

Note: It is recommended that the installer be run as the same UNIX account which owns the application server ORACLE_HOME files.

1. Change directories to INSTALL_DIR/reim/application.
2. Set the ORACLE_HOME, JAVA_HOME, and WEBLOGIC_DOMAIN_HOME environment variables. ORACLE_HOME should point to your WebLogic installation. . JAVA_HOME should point to the Java JDK 1.7+. This is typically the same JDK which is being used by the WebLogic domain where Application is getting installed. WEBLOGIC_DOMAIN_HOME should point to the full path of the domain into which Allocation will be installed.
3. If you are using an X server such as Exceed, set the DISPLAY environment variable so that you can run the installer in GUI mode (recommended). If you are not using an X server, or the GUI is too slow over your network, unset DISPLAY for text mode.
4. Run the install.sh script. This launches the installer. After installation is completed, a detailed installation log file is created (reiminstall.<timestamp>.log). See Appendix A: Oracle Retail Invoice Matching Application Installer Screens for illustrations of installer screens and details about what information needs to be entered on each screen.
5. Once Installation is done follow below post installation steps.

Post-Installation Steps

Update the following settings in WebLogic:

Transaction Time Out

The transaction time out is set at the Domain Level in Weblogic console

1. Login to the WebLogic Console.
2. Navigate to REIMDomain/Configuration/JTA/Timeout Seconds.
3. Set Timeout Seconds to 1200000.

Data Source Capacity

Depending on your planned load, you may need to increase the capacity on the Allocation data sources to accommodate more concurrent connections. When increasing this setting, ensure that your Allocation database has processes setting large enough to accommodate the new maximum.

1. Login to the WebLogic Console.
2. Click the Data Sources link on the Home Screen. The Data Source window opens.
3. Under the list of Data Sources, click the ApplicationDBDS data source.
4. Click the Connection Pool tab.
5. Set the Maximum Capacity to 1000.
6. Repeat for all data sources.

Clustered Installations – Post-Installation Steps

In these instructions, the application server node with the ORACLE_HOME you used for the ReIM installer is referred to as the master server. All other nodes are referred to as the remote server.

1. The ReIM batch files should be copied from the master server to each of the remote servers under the same path as on the master server. You should take the <retailhome>/batch directory and copy it onto the remote servers under the same path.
2. The Oracle Retail Installation creates some security files on $WEBLOGIC_DOMAIN_HOME/retail/context root/config directory. Copy this directory to each remote node of the Cluster, matching the full path of the location of this directory on main node.
3. The Oracle Retail Installation creates some properties files on $WEBLOGIC_DOMAIN_HOME/retail/context root/ properties directory. Copy this directory to each remote node of the Cluster, matching the full path of the location of this directory on main node.

Test the ReIM Application

After the application installer completes you should have a working ReIM application installation. To launch the application, open a web browser and go to http://hostname:(managed_server_port)/<context_root>/index.jsp.

If you have configured a WebTier to a front end ReIM application, use http port instead of managed server port.

Example:
http://<vip_hostname>:<OHS_PORT>/reim15/index.jsp

ReIM Batch Scripts

The ReIM application installer configures and installs the batch scripts under <retailhome>/reim-batch.

Example: /u00/projects/j2ee/reim/rem-batch

The batch scripts are copies of the same generic file. Their file names determine which functionality is run. To run batch scripts, use the alias name provided in the installer when ReIM is installed, the one that is written out to the Java wallet (for example, reim_batchpgmname ADMIN).

For the scripts to run correctly, values for the following variables must be provided:

- ORACLE_HOME: WebLogic Home directory where the ReIM application has been deployed.
- JAVA_HOME: Java 7.0 (1.7.0) JDK installation that typically is being used by the WebLogic Application Server.

> **Example**: export ORACLE_HOME=/u00/webadmin/products/wls_retail
> export JAVA_HOME=/u00/webadmin/products/jdk_java
> export PATH=$JAVA_HOME/bin:$PATH

Online Help

The application installer automatically installs Online Help to the proper location. It is accessible from the help links within the application.

Single Sign-On

Skip this section if ReIM is not used within an Oracle Single Sign-On environment.

> **Note**: This section assumes the Oracle WebLogic Server has already been registered with the Oracle Access Manager (OAM) via the oamreg tool. See the Oracle Single Sign-On (OAM using webgate) documentation for details.

To set up single sign-on, complete the following steps.

1. If you are using Oracle Retail Invoice Matching in an Oracle Single Sign-On environment, then the Invoice Matching root context must be protected. Modify the following files
   a. mod_wl_ohs.conf located in <WEBLOGIC_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1

```
LoadModule weblogic_module
"<WEBLOGIC_HOME>/Oracle_WT1/ohs/modules/mod_wl_ohs.so"
<IfModule weblogic_module>
      WebLogicHost <WEBLOGIC_HOST>
      WebLogicPort <WEBLOGIC_PORT>
      Debug ON
      WLLogFile /tmp/weblogic.log
      MatchExpression *.jsp
</IfModule>

<Location /ReimViewController >
SecureProxy ON
WebLogicHost <WEBLOGIC_HOST>
WebLogicPort <WEBLOGIC_PORT>
SetHandler weblogic-handler
WLCookieName REIMSESSIONID
WLProxySSL ON
 WLProxySSLPassThrough ON
 WlSSLWallet
"${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/keystores/h
ost_name"
</Location>

<Location /RetailAppsAdminConsole-REIM >
WebLogicHost <WEBLOGIC_HOST>
WebLogicPort <WEBLOGIC_PORT>
SetHandler weblogic-handler
```

```
WLCookieName REIMSESSIONID
WLProxySSL ON
WLProxySSLPassThrough ON
SecureProxy ON
WlSSLWallet
"${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/keystores/h
ost_name"
```

Adding Logout URI

After checking that the default authenticator's control flag is set correctly as per the OAM documentation, and that the order of the providers is correct, add an OAM SSO provider and restart all servers as described below.

1. Connect to the WebLogic domain using WLST and run the following command:

   ```
   addOAMSSOProvider(loginuri="/<appcontextroot>/adfAuthentication",
   logouturi="/oamsso/logout.html")
   ```

   Example:

   <WEBLOGIC_HOME>/common/bin/wlst.sh

   Connect() and proceed with the above step

5

Installing the Allocation Application

This Chapter describes the Pre-installation task, on how to install the alloc application and how to perform post installation for Cluster configuration. And also describes on WebTier settings for ALLOC.

Clustered Installations – Preinstallation Steps

Make sure that you are able to start and stop the managed servers that are part of the Allocation Cluster from the WebLogic Admin Console.

There are no additional steps before running the installer for Allocation.

Expand the Oracle Retail Allocation Application Distribution

To expand the Oracle Retail Allocation application distribution, complete the following steps.

1. Log into the UNIX server as the user who owns the WebLogic installation. Create a new staging directory for the Oracle Retail Allocation application distribution (alloc15application.zip).

   Example: /u00/webadmin/media/alloc

   This location is referred to as INSTALL_DIR for the remainder of this chapter.

2. Copy alloc15application.zip to INSTALL_DIR and extract its contents.

   Example: unzip alloc15application.zip

Run the Oracle Retail Allocation Application Installer

Once you have a managed server that is configured and started, you can run the Oracle Retail Allocation application installer. This installer configures and deploys the Oracle Retail Allocation application.

Note: See Appendix: Oracle Retail Allocation Application Installer Screens for details about every screen and field in the application installer.

Note: It is recommended that the installer be run as the same UNIX account which owns the application server ORACLE_HOME files.

1. Change directories to INSTALL_DIR/alloc/application.
2. Set the ORACLE_HOME, JAVA_HOME, and WEBLOGIC_DOMAIN_HOME environment variables. ORACLE_HOME should point to your WebLogic installation. . JAVA_HOME should point to the Java JDK 1.7+. This is typically the same JDK which is being used by the WebLogic domain where Application is getting

installed. WEBLOGIC_DOMAIN_HOME should point to the full path of the domain into which Allocation will be installed.

3. If you are using an X server such as Exceed, set the DISPLAY environment variable so that you can run the installer in GUI mode (recommended). If you are not using an X server, or the GUI is too slow over your network, unset DISPLAY for text mode.
4. Run the install.sh script. This launches the installer. After installation is completed, a detailed installation log file is created (allocinstall.<timestamp>.log). See Appendix B: Oracle Retail Allocation Application Installer Screens for illustrations of installer screens and details about what information needs to be entered on each screen.

Post-Installation Steps

Update the following settings in WebLogic:

Transaction Time Out

The transaction time out is set at the Domain Level in Weblogic console

1. Login to the WebLogic Console.
2. Navigate to AllocDomain/JTA/Timeout Seconds.
3. Set Timeout Seconds to 1200000.

WebLogic Redelivery Limit

1. Login to the WebLogic Console.
2. Click the **JMS Modules** link on the Home Screen. The JMS Module window opens.
3. Under the list of JMS Modules, click **allocJMSModule**. The Queue List is displayed.
4. Click **calcQueue**.
5. Click the **Delivery Failure** tab.
6. Set the Redelivery Limit to **0** instead of -1.

RAFAsyncTaskDBDS Timeout

1. Login to the WebLogic Console.
2. Click the **Data Sources** link on the Home Screen. The Data Source window opens.
3. Under the list of Data Sources, click the **RAFAsyncTaskDBDS** data source.
4. Click the **Connection Pool** tab.
5. Expand the Advanced divider.
6. Click the **Transaction** tab.
7. Check the **Set XA Transaction Timeout** checkbox.
8. Set the XA Transaction Timeout to **162000**.

Data Source Capacity

Depending on your planned load, you may need to increase the capacity on the Allocation data sources to accommodate more concurrent connections. When increasing this setting, ensure that your Allocation database has processes setting large enough to accommodate the new maximum.

1. Login to the WebLogic Console.

2. Click the Data Sources link on the Home Screen. The Data Source window opens.
3. Under the list of Data Sources, click the ApplicationDBDS data source.
4. Click the Connection Pool tab.
5. Set the Maximum Capacity to 1000.
6. Repeat for all data sources.

Increase Max JMS messages

The following steps are not mandatory, but only intended to use as per your environment needs if required.

WebLogic uses the Work Manager to execute the Java Messages. Work Manager prioritizes tasks in queue and allocates the thread based on an execution model. To optimize the Java Messaging Services it is highly recommended that the Work Manager is configured most effectively per each customer expected user volumes. The maximum number of threads constraint should be set to a number that is appropriate for the maximum number of anticipated Allocation users on the system at any given time.

Steps to Configure WebLogic Work Manager

From WebLogic Console navigate to Work Manager pane (**Domain >Environment >Work Manager**)

Create Maximum thread constraint

1. Click **New**.
2. Select the Maximum Thread Constraint radio button, and click **Next**.
3. Give a Name (MaxThreads) and specify maximum number of consumers needed for your Application. Click **Next**.
4. Select Target as <alloc-server>, and click **Finish**.

Create Work Manager

1. Click **New**.
2. Select the **Work Manager** radio button, and click **Next**.
3. Give a Name (AllocWorkManager), and click **Next**.
4. Select Target as <alloc-server>, and click **Finish**.
5. Go back to Domain-Environments->Work Manager, choose and edit the work manager you just created: AllocWorkManager.
6. Assign Max thread constraint to –MaxThreads as configured above.

Clustered Installations – Post-Installation Steps

If you are installing the Oracle Retail Allocation application to a clustered WebLogic environment, extra steps are required to complete the installation. In these instructions, the application server node with the ORACLE_HOME you used for the Oracle Retail Allocation installer is referred to as the master node. All other nodes are referred to as remote nodes.

The Oracle Retail Installation creates security, batch, and configuration files in the $WEBLOGIC_DOMAIN_HOME/retail/<alloc_application_name>/directory. Copy this directory to each remote node of the cluster, matching the full path of the location of this directory on the master node.

Test the Oracle Retail Allocation Application

After the application installer completes you should have a working Oracle Retail Allocation application installation. To launch the application, open a web browser and go to http://host:httpport/contextroot/faces/pages_home

> **Examples**:
>
> http://<vip_hostname>:<OHS_PORT>//alloc15/faces/home
>
> myhost is the hostname and Port is the port of alloc-server where Allocation application has been deployed.

- You should use a user/password that you built in the previous section of this install guide "Load LDIF files in LDAP".

The default, preloaded user supplied in the LDIF scripts for testing this installed application is BENNY_ANDERSON; the password is <the password which you have given in the LDIF file RGBU-oid-create-users.ldif as part of loading LDIF files into the LDAP>.

Allocation Batch Scripts

The Allocation application installer configures and installs the batch scripts under <RETAIL_HOME>/alloc-batch/batch.).

Batch user is entered as part of the install and the user (Example: Alex Administrator) gets created in the wallet (<retail_ home>/orpatch/config/javaapp_alloc)

at the time of install.

Verify the entry was created in the wallet under the "retail_installer" partition by running the dump_credentials.sh script in directory < retail_home>/orpatch/deploy/retail-public-security-api/bin and passing in the batch wallet location.

Example:

./dump_credentials.sh <retail_ home>/orpatch/config/javaapp_alloc

Application level key partition name:retail_installer

User Name Alias:dsallocAlias User Name:RMSUSER

User Name Alias:alloc15 User Name: ALLOCATION_ADMIN

User Name Alias:wlsAlias User Name:weblogic

You will need the alias for running the batch scripts.

You must run the batch script with a Java wallet in the form of <allocbatchscript>.ksh <ALLOCATION_ADMIN alias>, where <ALLOCATION_ADMIN alias> is the alias given in the 'Batch Details' screen of the Appinstaller. For example: ./ AllocScheduleBatch.ksh alloc15

> **Note**: The JAVA_HOME used by batch is configured in the AllocBatch.ksh script by the Oracle Retail Allocation application installer using the JAVA_HOME of the installer.

If a new batch user needs to be created in the wallet, follow the procedure below.

Run the save_credential.sh script, passing in a unique alias, the location to the batch wallet (<retail_ home>/orpatch/config/javaapp_alloc), "retail_installer" for the partition name, and the username which needs to be created. This user must be in LDAP and must

have valid roles in LDAP. Please refer the *Oracle Retail Allocation Operations Guide* for more information on the batch user.

You will need the alias you chose when you are running the batch scripts.

Example:

```
./save_credential.sh -a alloc15 -l <retail_ home>/orpatch/config/javaapp_alloc
 -p alloc15 -u ALLOCATION_ADMIN
```

In the above, 'alloc15' is the new alias (this needs to be unique), 'retail_installer' is the partition name and 'ALLOCATION_ADMIN' is the new user.

Single Sign-On

Note: This section assumes the Oracle WebLogic Server has already been registered with the Oracle Access Manager (OAM) via the oamreg tool. See the Oracle Single Sign-On (OAM using webgate) documentation for details.

If you are using Oracle Retail Allocation in an Oracle Single Sign-On environment, then the Allocation root context must be protected. Modify the following files.

- mod_wl_ohs.conf located in <WEBLOGIC_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1
- LoadModule weblogic_module "${ORACLE_HOME}/ohs/modules/mod_wl_ohs.so"
- <IfModule weblogic_module>
- </IfModule>

```
<Location /console>
        WebLogicHost <weblogichostname>
        WebLogicPort <AdminServerPort>
        SetHandler weblogic-handler
</Location>

<Location /alloc15 >
WebLogicHost <weblogichostname>
WebLogicPort <AdminServerPort>
SetHandler weblogic-handler
WLCookieName ALC_CORESESSIONID
</Location>


<Location /RetailAppsAdminConsole-ALLOC >
WebLogicHost <weblogichostname>
WebLogicPort <AdminServerPort>
SetHandler weblogic-handler
WLCookieName ALC_CORESESSIONID
</Location>
```

Note: In the above, modify 'alloc15' with the context root name used for installing Allocation application.

Adding Logout URI

After checking that the default authenticator's control flag is set correctly as per the OAM documentation, and that the order of the providers is correct, add an OAM SSO provider and restart all servers as described below.

Connect to the WebLogic domain using WLST and run the following command:

```
addOAMSSOProvider(loginuri="/<appcontextroot>/adfAuthentication",
logouturi="/oamsso/logout.html")
```

Example:

<WEBLOGIC_HOME>/common/bin/wlst.sh

Connect() and proceed with the above step

6

Installing the SIM

This Chapter describes the Pre-installation task, on how to install the sim application and how to perform post installation for Cluster configuration. And also describes on WebTier settings for SIM.

Expand the SIM Application Distribution

To expand the SIM application distribution, do the following.

1. Log in to the UNIX server as the user who owns the Web Logic installation. Create a new staging directory for the SIM application distribution (sim15-application.zip). There should be a approximately 1 GB disk space available for the application media and installation files.

   This location is referred to as INSTALL_DIR for the remainder of this chapter.
2. Copy sim15-application.zip to <INSTALL_DIR> and extract its contents.

Set the Environment Variables for the SIM Installer

1. Set the following environment variables for the SIM installer (the following are just examples, use values for appropriate for your environment):

```
ORACLE_HOME=/u00/webadmin/products/wls_retail
WEBLOGIC_DOMAIN_HOME=/u00/webadmin/config/domains/wls_retail/SIMDomain
JAVA_HOME=/u00/webadmin/product/jdk_java
PATH=$JAVA_HOME/bin:$PATH
export ORACLE_HOME WEBLOGIC_DOMAIN_HOME JAVA_HOME PATH
```

Run the SIM Application Installer

This installer configures and deploys the SIM application and Java WebStart client files.

1. If you are using an X server such as Exceed, set the DISPLAY environment variable so that you can run the installer in GUI mode (recommended). If you are not using an X server, or the GUI is too slow over your network, unset DISPLAY for text mode.
2. Verify that the managed server to which SIM will be installed is currently running.
3. Run the install.sh script. This launches the installer. After installation is completed, a detailed installation log file is created: <INSTALL_DIR>/sim/application/logs/sim-install-app.<timestamp>.log.

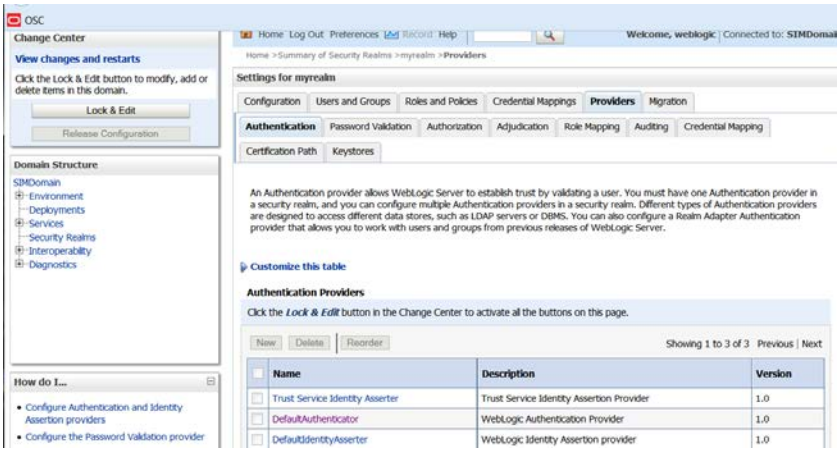
Note: The manual install option in the installer is not functional for this release.

Note: See Appendix C: SIM Application WebLogic Server Installer Screens for details on every screen and field in the WebLogic application installer.

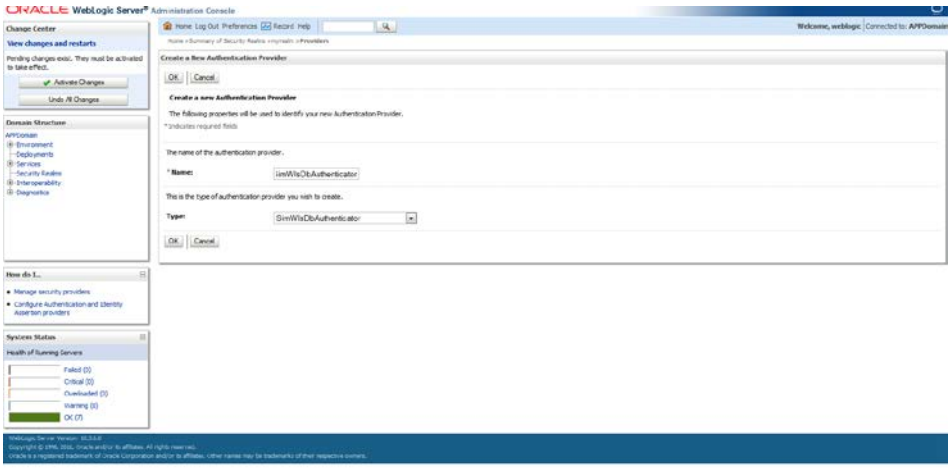
SIM Database Authentication Provider set up (to be done after the application deploy)

> **Note**: This procedure is only needed if you plan on using database authentication for the SIM application. This can be skipped if LDAP is going to be used for authentication.

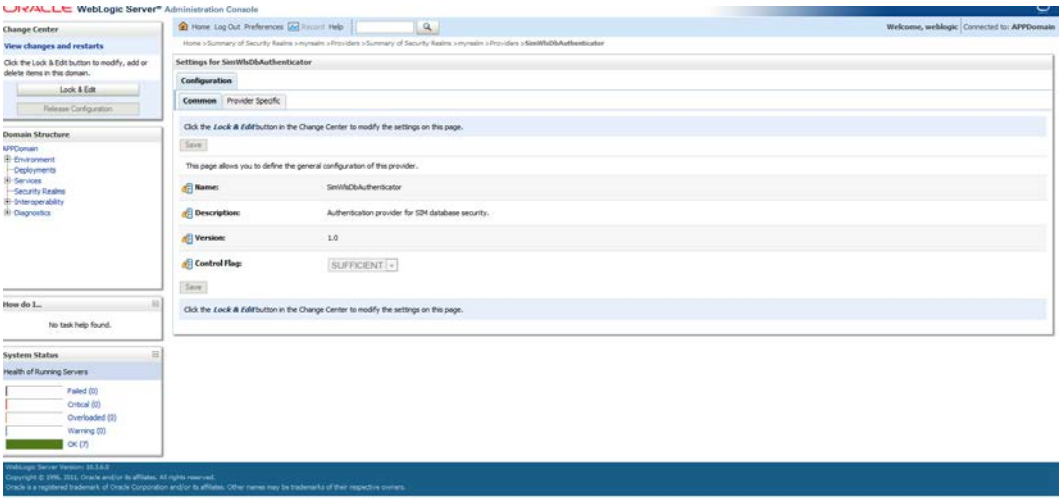
1. Shut down all the servers of the WebLogic Domain created.
2. Once you extract the SIM installer to <INSTALL_DIR> copy the sim-security.zip present in <INSTALL_DIR>/sim/application/sim15 to the <WEBLOGIC_DOMAIN_HOME>/lib and extract it contents in the folder.
3. Start the domain admin server.
4. Log into the WebLogic console.
5. Navigate to: security realms -> myrealm (default realm) -> providers.



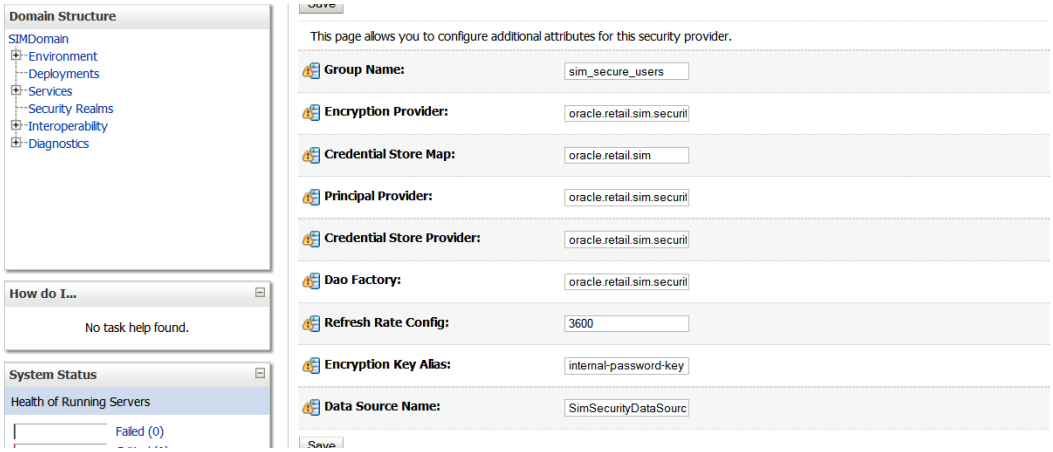
1. Click **Lock & Edit** in the change center.
2. Click **New provider**.
3. Select the provider type from the list: **SimWlsDbAuthenticator**.
4. Set the provider name (Default: SimWlsDbAuthenticator).



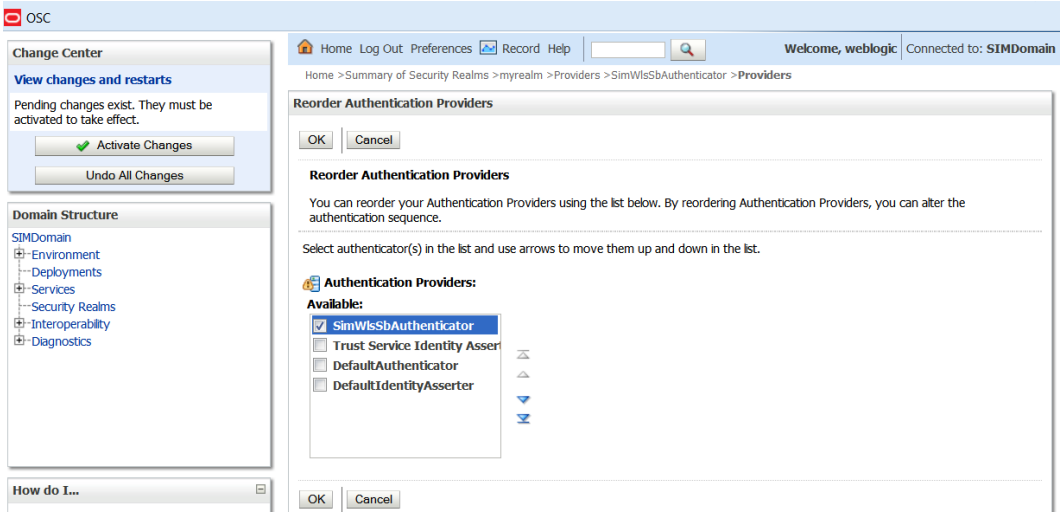
5. Click **OK**.
6. Open the new provider configuration.
7. From the **Common** tab, set the Control Flag to **SUFFICIENT**.
8. Click **Save**.



9. Click the **Provider Specific** tab.
10. The SIM Data Source Name defaults to SimDataSource which is what the SIM installer creates. It should be left to the default value. The Group Name defaults to sim_secure_user. If this was changed during the SIM installation then it also needs to be changed here.



11. Click **Save**.
12. Back on the provider tab, click **Reorder**.
13. Move the SimDbAuthenticator to the top of the list, or above the DefaultAuthenticator.



14. Click **OK**.
15. Click **Activate Changes**.
16. Shutdown the SIMDomain (The adminserver and the managed servers).
17. Start the admin and managed servers for the domain.

Review and/or Configure Oracle Single Sign-On

Note: This procedure is only needed if you plan on setting up the SIM application using Single Sign On (SSO) authentication. This can be skipped if SSO is not going to be configured for this environment. The Oracle Access Manager must be configured and the Oracle http server (Webtier and webgate) must be registered into the Oracle Access Manager.

Create the SIM SSO provider in the SIMDomain

1. Shut down all the servers of the WebLogic Domain created.
2. Once you copy the contents to <INSTALL_DIR> copy the sim-security.zip present in <INSTALL_DIR>/sim/application/sim15 to the <WEBLOGIC_DOMAIN_HOME>/lib and extract it contents in the folder.
3. Start the domain admin server.
4. Log into the WebLogic console
5. Navigate to: security realms -> myrealm (default realm) -> providers.
6. Click **Lock & Edit** in the change center.
7. Click **New**.
8. Select the provider type from the list: **SimWlsSsoAuthenticator**.
9. Set the provider name (Default: SimSsoAuthenticator).
10. Click **OK**.
11. Click on the newly created **SimSsoAuthenticator**.
12. From the **Common** tab, set the Control Flag to **SUFFICIENT**, and click **Save**.
13. Click **Provider Specific** tab.
14. Check that the GroupName is set to the name of the group used for SIM secure users (sim_secure_users by default).

15. All other values under the Provider Specific tab can be left as the default value.
16. Click **Save**.
17. On the provider list, click **Reorder**.
18. Move the SimWlsSsoAuthenticator to the top of the list.
19. Click **OK**.
20. Click **Activate Changes** in the control center.
21. Shutdown the domain.
22. Start the admin and managed servers for the domain.

After the SSO provider is created in the SIMDomain, you will also have to set the protection of the SIM application resources correctly in the Application Domain that has been registered in the Oracle Access Manager.

In the Webtier/Webgate http server you need to set the mod_wl_ohs.conf file to redirect the http call to the where the SIM application has been deployed.

For example, in mod_wl_ohs.conf set:

```
<Location /sim-client >
 WebLogicCluster orapphost1:orapphost2
 SetHandler weblogic-handler
</Location>

Ex:
<Location /sim-client >
WebLogicCluster msp00acs.us.oracle.com:7143,msp00acf.us.oracle.com:7143
SetHandler WebLogic-handler
</Location>
```

Then in Oracle Access Manager, set the protection of the resources in the Application Domain that has been registered for the SIM application. You must protect the /sim-client/launch resource and exclude the rest:

Resource URL: /sim-client/launch

Protection Level: Protected

Authentication Policy: Protected Resource Policy

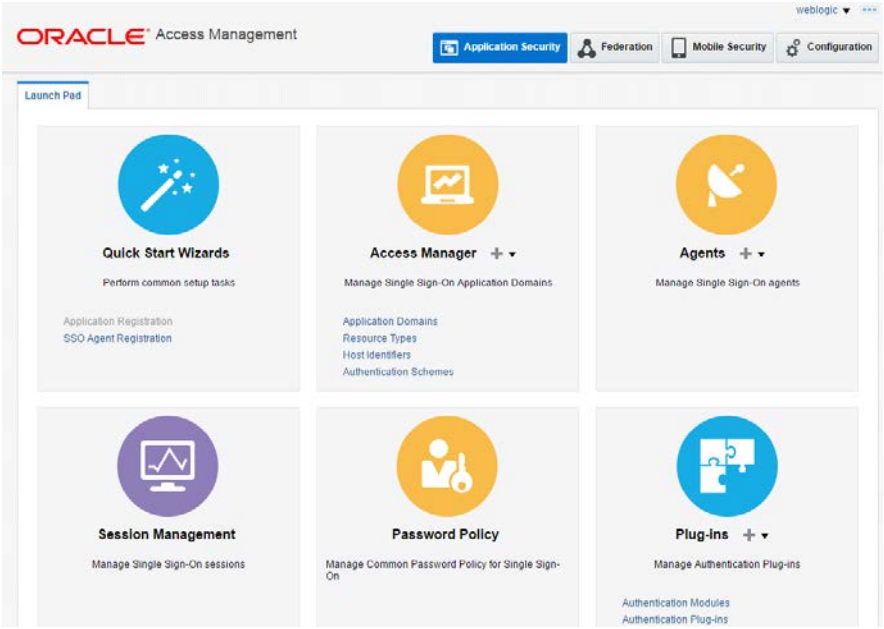
Authorization Policy: Protected Resource Policy

Resource URL: /sim-client/.../*

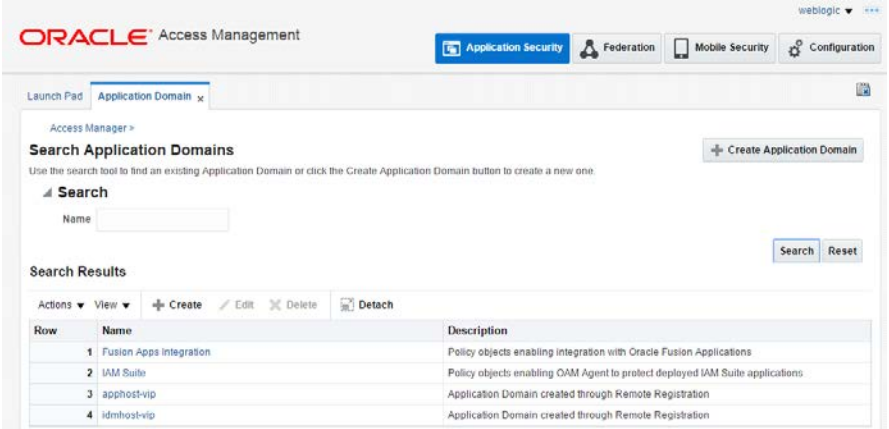
Protection Level: Excluded

Steps to add resource url is below:

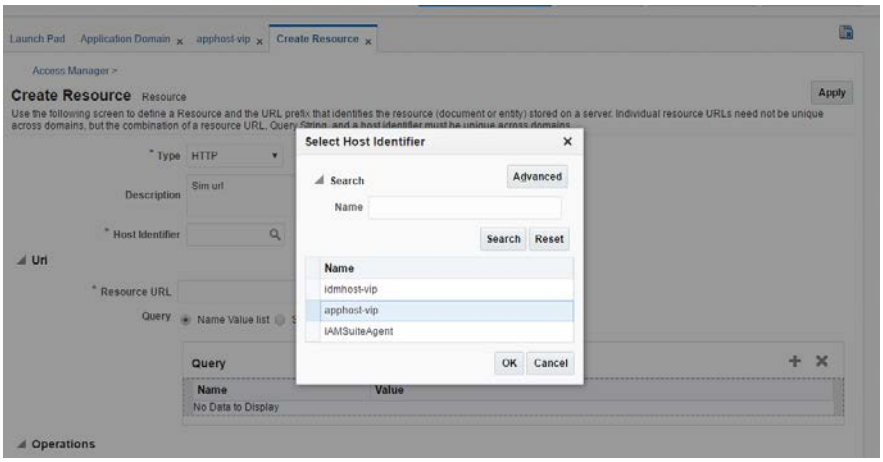
- Login to OAMCONSOLE and click Applications Domains under Access Manager.



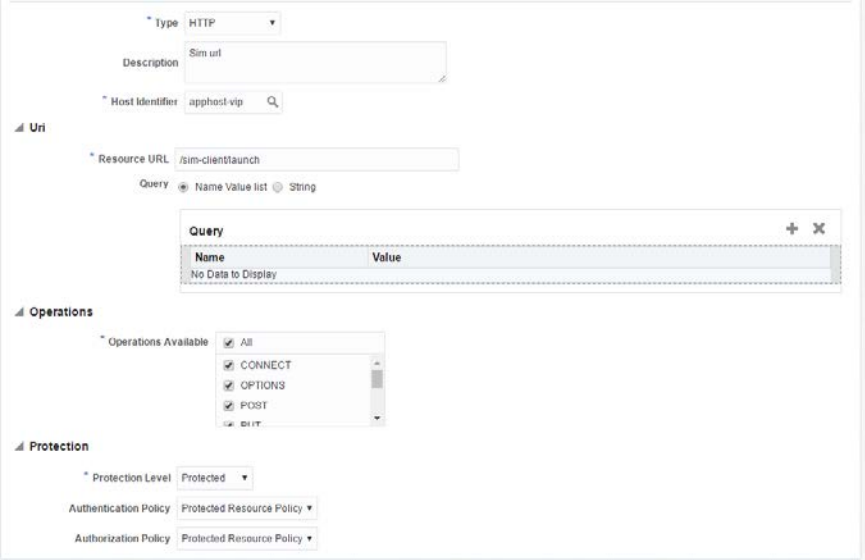
- In Application Domains screen, just click **Search** and select the appropriate domain(apphost-vip).



- Traverse to Resources Tab and click **Create**.
- Update the details and Search the host Identifier, select and click **OK**.



- Add the Resource URL and Protection level.

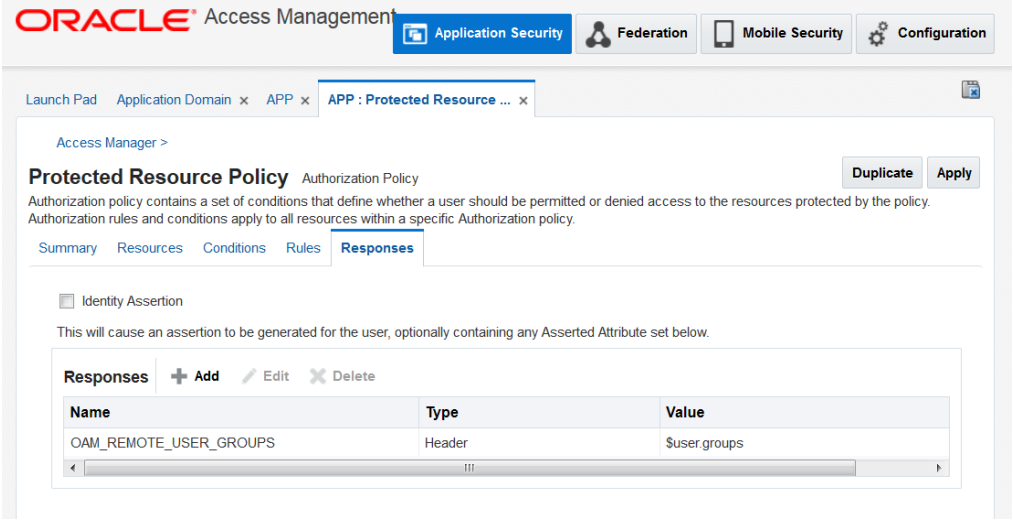


- Click **Apply.** You can now see the resource URL that you added, in the Resource tab. Please follow the above steps to add other resource URL of SIM and RPM also.

In the OAM you need to add a response to the Protected Resource Policy:

- Under Access Manager click **Application Domains**.
- Search and click on the domain used for your SIM deployment.
- Click **Authorization Policies**.
- Click **Protected Resource Policy**.
- Click **Responses**.
- Click Add and enter the following values:
  - Type: Header
  - Name: OAM_REMOTE_USER_GROUPS
  - Value: $user.groups

It will look similar to the following:



SIM Batch Scripts

The SIM batch programs are installed into the WEBLOGIC_DOMAIN_HOME location that was specified during application installation.

The batch programs can be run from a different location if you cannot run them from under the application server <WEBLOGIC_DOMAIN_HOME>.. To install the batch files in a different location just copy the entire batch folder to the appropriate destination.

The batch directory is assumed to be located on the same server as the application server. If you copy the SIM batch directory to a location on a different server, then you need to configure the file path to the sim-batch.log file, which is defined in batch/resources/log4j.xml.

See the "Batch Detail" section of the Oracle Retail Store Inventory Management Operations Guide for information about how to run batches.

Starting and Stopping the Wavelink Server

In order to use handheld wireless devices with SIM, the Wavelink server must be running. The SIM application installer installs, configures, and starts the Wavelink server for you, so once the SIM application install is complete, the Wavelink server is ready to be used.

> **Note**: Even if you use the AdminServer to restart SIM, you will still need to restart the Wavelink server manually.

The Wavelink server scripts are installed into the <sim-wireless-directory>/bin.

The following is an example for stopping and starting the Wavelink server:

```
# cd /u00/webadmin/config/domains/wls_retail/SIMDomain/retail/sim15/wireless/bin
# ./wavelink-shutdown.sh
# ./wavelink-startup.sh
```

> **Note**: This is clustered environment so need to start in both the nodes.

Test the SIM Application

Once SIM database and application are installed, foundation data is imported into SIM, you should have a working SIM application installation. To launch the application client, open a web browser and go to the client URL. You can find the URL in the **Next** steps section of the log file that was produced by the installer.

> **Example**:
>
> WLS: http://<vip_hostname>:<OHS_PORT>/sim-client/launch

7

Installing the RPM Application

This Chapter describes the Pre-installation task, on how to install the rpm application and how to perform post installation for Cluster configuration. And also describes on WebTier settings for RPM.

Expand the RPM Application Distribution

To expand the RPM application distribution, do the following.

1. Log into the UNIX server as the user who owns the WebLogic installation. Create a new staging directory for the RPM application distribution (rpm15application.zip). There should be a minimum of 2 GB disk space available for the application installation files.

   Example: /u00/webadmin/media/rpm

   This location is referred to as STAGING_DIR for the remainder of this chapter.
2. Copy rpm15application.zip to STAGING_DIR and extract its contents.

Clustered Installations – Preinstallation Steps

Skip this section if you are not clustering the application server.

If you are installing the RPM application to a clustered WebLogic Application Server environment, there are some extra steps you need to take before running the RPM application installer. In these instructions, the application server node with the ORACLE_HOME you used for the RPM installer is referred to as the master node. All other nodes are referred to as the remote nodes.

1. Before starting the RPM Application Installer, make sure that you are able to start and stop the managed servers that are part of the RPM Application Cluster from the WebLogic Administration Console.
2. When the RPM Application Installer displays the screen in which it asks for the information related to the JMS Provider, we recommend entering these values:
   input.jms.module = rpmJMSModule

   input.taskqueue.name = taskQueue

   input.chunkqueue.name = chunkQueue

   input.chunkControllerQueue.name = chunkControllerQueue
3. Insert into all remote nodes <MW_HOME>/wlserver/server/lib/weblogic.policy file changes, the same RPM entries for java security permissions you entered on the master node.

Provide the Hibernate4.3.10 Jar File

The RPM application requires hibernate4 jar files to be installed. These files should be downloaded from http://www.hibernate.org.

Older releases can be downloaded here
http://sourceforge.net/projects/hibernate/files/hibernate4/4.3.10.Final

Extract the required Hibernate 4.3.10 jar files and place them within the application servers STAGING_DIR/rpm/application/hibernate4 directory before running the installer. The installer will then install the jar files within the application for you.

The required jars are as follows:

- hibernate-commons-annotations-4.0.*.jar
- hibernate-core-4.3.*.jar
- hibernate-ehcache-4.3.*.jar
- hibernate-jpa-2.1-api-1.0.*.jar
- jboss-logging-3.1.*.jar
- jboss-transaction-api_1.2_spec-1.0.*.jar
- The required jar files are located in the <HIBERNATE_EXTRACT_DIR>\hibernate-release-4.3.5.Final.tgz\hibernate-release-4.3.5.Final.tar\hibernate-release-4.3.5.Final\lib\required\directory.

Run the RPM Application Installer

Once you have a WebLogic instance that is configured and started, you can run the RPM application installer. This installer configures and deploys the RPM application and Java WebStart client files.

> **Note**: See Appendix D: RPM Application Installer Screens for details on every screen and field in the application installer. The screenshots contain instructions that are necessary to result in a working application.

1. Change directories to STAGING_DIR/rpm/application.
2. Set the ORACLE_HOME, DOMAIN_HOME and JAVA_HOME environment variables. ORACLE_HOME should point to your WebLogic installation. JAVA_HOME should point to the Java 7.0 (1.7.) JDK . DOMAIN_HOME should point to your WebLogic domain.
3. If you are using an X server such as Exceed, set the DISPLAY environment variable so that you can run the installer in GUI mode (recommended). If you are not using an X server, or the GUI is too slow over your network, unset DISPLAY for text mode.
4. Run the install.sh script. This launches the installer. After installation is complete, a detailed installation log file is created (rpm15install.<timestamp>.log).

   > **Note**: The values you enter in the installer screen, "Setup Application Users," have specific requirements for RPM to work properly. See the screen description in Appendix D: RPM Application Installer Screens for more details. The screenshots contain instructions that are necessary to result in a working application.

5. The installer has an 'analyze' mode that will evaluate all files in the patch against the environment and report on the files that will be updated based on the patch. To run the installer in analyze mode, set the variable ORPATCH_ANALYZE to 'true'.
6. After clicking "install", the Analyze tool will generate a report of the files that will be patched if you apply this patch to the selected RETAIL_HOME. A high level report can be found in the log file: STAGING_DIR/rpm/application/log/rpminstall.<timestamp>analyze. Log

The detailed list of patch files can be found in RETAIL_HOME/orpatch/logs/detail_logs/analyze/details/

7. If you are using an X server such as Exceed, set the DISPLAY environment variable so that you can run the installer in GUI mode (recommended). If you are not using an X server, or the GUI is too slow over your network, unset DISPLAY for text mode.
8. Run the install.sh script. This launches the installer. After installation is completed, a detailed installation log file is created (rpminstall.<timestamp>.log).

Clustered Installations – Post-Installation Steps

If you are installing the RPM application to a clustered WebLogic Server environment, there are some extra steps you need to take to complete the installation. In these instructions, the application server with the ORACLE_HOME you used for the RPM installer is referred to as the master server. All other nodes are referred to as the remote servers.

1. The RPM batch files should be copied from the master node to each of the remote nodes under the same path as on the master node. You should take the $DOMAIN_HOME/retail/<rpmdir>/rpm-batch directory and copy it onto the remote nodes under the same path.
2. For retailers who install batch on either node of the cluster, launchRpmBatch.sh script should be modified on each remote node to point to the local RPM instance. The RPM URL is set in the PROVIDER_URL variable. This script is located at $DOMAIN_HOME/retail/<rpmdir>/rpm-batch/scripts/launchRpmBatch.sh.
3. The Oracle Retail Installation creates some security files on $DOMAIN_HOME/retail/<rpm_application_name>/config directory. Copy this directory to each remote node of the Cluster, matching the full path of the location of this directory on main node.
4. The Oracle Retail Installation creates some properties files on $DOMAIN_HOME/retail/<rpm_application_name>/properties directory. Copy this directory to each remote node of the Cluster, matching the full path of the location of this directory on main node.

Review and/or Configure Oracle Single Sign-On

Note: This step is only needed if you plan on setting up the RPM application using Single Sign On (SSO) authentication. This can be skipped if SSO is not going to be configured for this environment. The Oracle Access manager must be configured and the Oracle http server (Webtier and webgate) must be registered into the Oracle Access Manager.

Create the RPM SSO provider in the RPMdomain:

1. Shut down all the servers of the Weblogic Domain created.
2. Once you copy the contents to <INSTALL_DIR> copy the rpm15-security.zip present in <INSTALL_DIR>/ rpm/application/rpm15 to the DOMAIN_HOME/lib and extract its contents in the folder.
3. Start the domain admin server.
4. Log into the WebLogic console.
5. Navigate to: security realms -> myrealm (default realm) -> providers.
6. Start a Lock and Edit session.

7. Click **New provider**.
8. Select the provider type from the list: RpmWlsSsoAuthenticator.
9. Set the provider name (Default: RpmSsoAuthenticator).
10. Click **OK**.
11. Open the new provider configuration.
12. Under Common, set the Control Flag to **SUFFICIENT**.
13. Click **Provider Specific**.
14. Check that the GroupName is set to the name of the group used for RPM secure users (rpm_secure_users by default).
15. All other values under the Provider Specific tab can be left as the default value.
16. Click **OK**.
17. On the provider list, click **Reorder**.
18. Move the RpmWlsSsoAuthenticator to the top of the list, or above the DefaultAuthenticator.
19. Click **OK**.
20. Click **Activate Changes**.
21. Shutdown the domain.
22. Start the admin and managed servers for the domain.

After the SSO provider is created in the RPMdomain, you will also have to set the protection of the RPM application resources correctly in the Application Domain that has been registered in the Oracle Access Manager.

In the Webtier/Webgate http server you need to set the mod_wl_ohs.conf file to redirect the http call to where the RPM application has been deployed.

For example, in mod_wl_ohs.conf set:

```
<Location /rpm-client >
 WebLogicCluster <RPMServerhost>:<RPMServerport>
 SetHandler weblogic-handler
 ErrorPage downtime.html
</Location>
```

Example:

```
<Location /rpm-client>
 WebLogicCluster msp00acs.us.oracle.com:7133,msp00acf.us.oracle.com:7133
 SetHandler weblogic-handler
</Location>
```

Then in Oracle Access Manager, set the protection of the resources in the Application Domain that has been registered for the RPM application. You must protect the /rpm-client/launch resource and unprotect the rest:

Resource URL: / rpm-client/launch

Protection Level: Protected

Authentication Policy: Protected Resource Policy

Authorization Policy: Protected Resource Policy

Resource URL: / rpm-client/.../*

Protection Level: Excluded

Note: Follow same steps as SIM to add resource URL.

Sign the RPM Client Configuration Jar File

There is some client-side configuration that the installer performs which results in a modified rpm_client_config.jar file after installation. Because of this, the jar file cannot be pre-signed by Oracle. The installer now provides an option to sign the jar by asking some details but if decide not to do it using the installer, the user must sign this jar file after the installer has completed.

The rpm_client_config.jar file is located in $DOMAIN_HOME/servers/<rpm-managedserver>/tmp/_WL_user/rpm/<38o5n1 >/war/lib. Use the jarsigner utility to sign the rpm_client_config.jar file using your alias and keystore, .

Example: jarsigner $DOMAIN_HOME/servers/rpm-managedserver/tmp/_WL_user/rpm/<38o5n1> /war/lib/rpm_client_config.jar foo

If you are clustering the application server you need to copy the signed rpm_client_config.jar file to the same path under $ORACLE_HOME on all remote nodes.

Consult the jarsigner documentation from Sun for further information on the JAR signing process.

You also need to sign in same jar file inside WebLaunchServlet.war which can be found in the rpm15.ear location in the stage directory of the managed server. Copy the ear file in a temporary location extract the ear files sign the jar file and compress them again and replace it with the one in the staging directory. The above is needed to avoid unsigned entries in jar after restarting the server in the future. Once you restart the weblogic server, files will re-loaded from the once in stage directory. Hence these steps are needed.

Transaction Timeout

This section describes how to establish settings for a transaction timeout. A transaction timeout is the maximum duration, in seconds, for transactions on the application server. Any transaction that is not required to complete before this timeout is rolled back.

To set up transaction timeouts, complete these steps:

1. Log in to the WebLogic Server 12.1.3 Administration Console.
2. Click the **Domain** link.
3. Under Configuration, click **JTA**.
4. Click **Lock and Edit**.
5. Set the Timeout Seconds (for example, 600 seconds).
6. Click **Activate Changes**.

Test the RPM Application

After the application installer finishes, a working RPM application installation should result, if the users were created properly.

For LDAP authentication, the application will not log you in properly unless you have a row for the users in question in the database on the rsm_user_role table. The following is an example of how to add rows if they have not been added.

```
insert into rsm_user_role
(id, user_id, role_id, start_date_time, end_date_time)
select rsm_user_role_seq.Nextval,
       'retail.user',
       -1001,
       nvl(get_vdate,sysdate) - 365,
       null
  from dual;
```

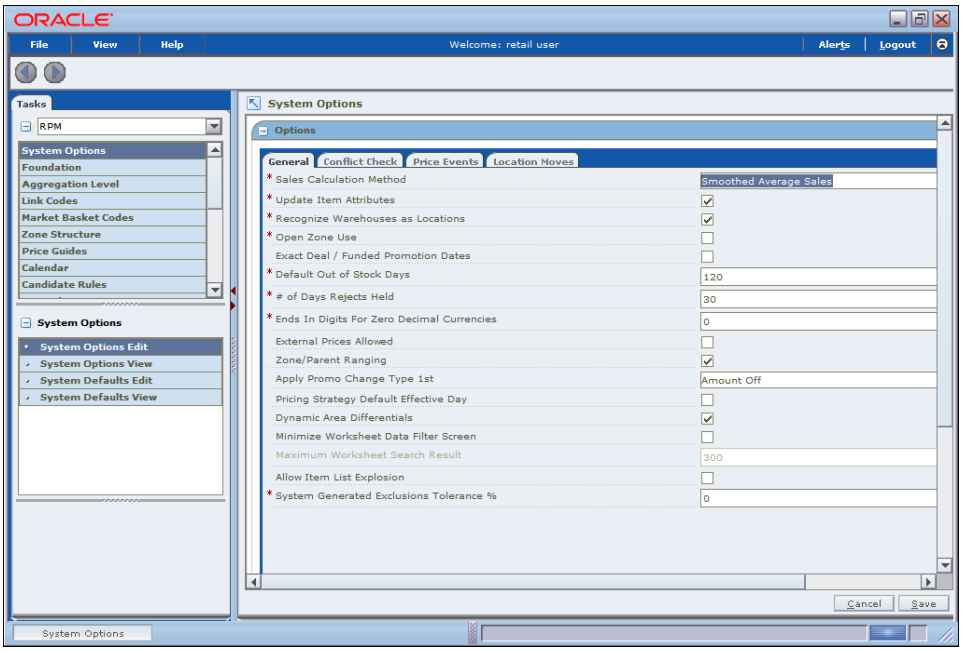
If problems occur when trying to start the RPM application, ensure proxies are turned off.

To launch the application client, open a Web browser and access the JnlpLaunchServlet, naming the RPM JNLP template file (rpm_jnlp_template.vm).

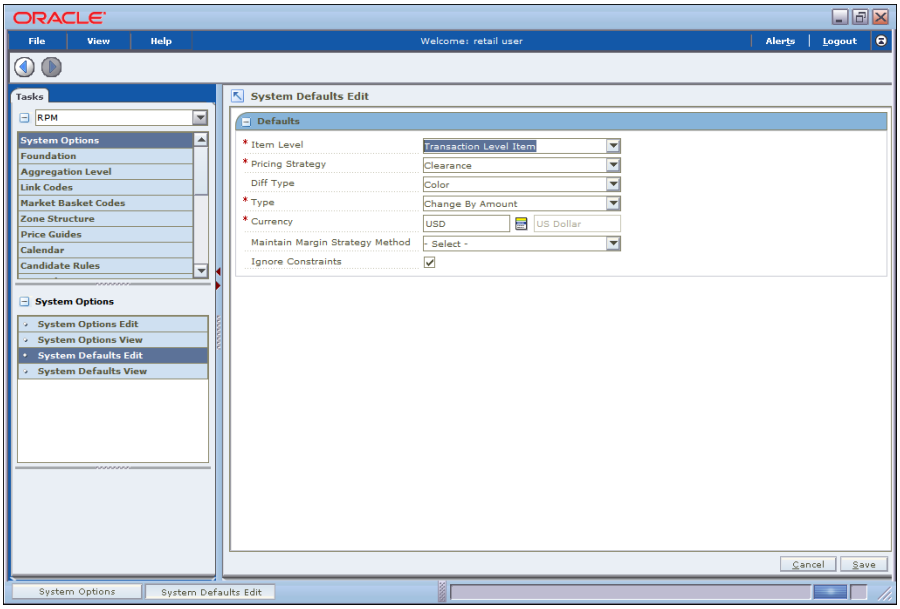
Example: http://VIP_URL:OHS_PORT/rpm-client/launch?template=rpm_jnlp_template.vm

When you are in the RPM application, do the following to add a rpm_system_options row required by RPM for system use.

1. On the left side of the screen, select **System Options**.
2. Select **System Options Edit**.
3. In the lower right part of the screen, click **Save**.



4. To add an rpm_system_options_def row required by RPM needs for system use, do the following.
   a. Select **System Defaults Edit**.
5. In the lower right part of the screen, click **Save**.



RPM Batch Scripts

The RPM application installer configures and installs the batch scripts under <retail_home>/rpm-batch. . You will run the RPM java batch pgms with a java wallet alias (for example, RETAIL.USER1) that you created in the installer screens. The following is an example execution of a RPM java batch script.

```
./<RPMbatchscriptname>.sh RETAIL.USER1
```

Note: Make sure that JAVA_HOME is set to the appropriate Java JDK (the same JDK that has been used by WebLogic Server) and ORACLE_HOME is set to weblogic installation before running the RPM batch programs.

Adding a User to the RPM Application

For LDAP authentication, complete the following steps.

Build/copy existing RPM user in LDAP to the new user name you desire. User in LDAP for RPM must have objectclass, retailUser, as there is a search filter on that objectclass name of retailUser.

Insert row to database table:

```
insert into rsm_user_role
(id, user_id, role_id, start_date_time, end_date_time)
select rsm_user_role_seq.Nextval,
       'retail.user1',
       -1001,
       nvl(get_vdate,sysdate) - 365,
       null
  from dual;
```

8

Installing the ReSA Application

This Chapter describes the Pre-installation task, on how to install the ReSA application and how to perform post installation for Cluster configuration. And also describes on WebTier settings for ReSA.

Clustered Installations – Preinstallation Steps

Make sure that you are able to start and stop the managed servers that are part of the ReSA Cluster from the WebLogic Admin Console.

There are no additional steps before running the installer for Retail Sales Audit.

Expand the ReSA Application Distribution

To expand the ReSA application distribution, complete the following steps.

1. Log into the UNIX server as the user who owns the WebLogic installation. Create a new staging directory for the ReSA application distribution (resa15application.zip).

   Example: /u00/webadmin/media/resa

This location is referred to as INSTALL_DIR for the remainder of this chapter.

2. Copy resa15application.zip to INSTALL_DIR and extract its contents.

   Example: unzip resa15application.zip

Run the ReSA Application Installer

Once you have a managed server that is configured and started, you can run the ReSA application installer. This installer configures and deploys the ReSA application.

Note: See Appendix E: Oracle Retail Sales Audit Application Installer Screens for details about every screen and field in the application installer.

Note: It is recommended that the installer be run as the same UNIX account which owns the application server ORACLE_HOME files.

- Change directories to INSTALL_DIR/resa/application.
- Set the ORACLE_HOME, JAVA_HOME, and WEBLOGIC_DOMAIN_HOME environment variables. ORACLE_HOME should point to your WebLogic installation. JAVA_HOME should point to the Java JDK 1.7+. This is typically the same JDK which is being used by the WebLogic domain where Application is getting installed. WEBLOGIC_DOMAIN_HOME should point to the full path of the domain into which ReSA will be installed.

  The installer has an 'analyze' mode that will evaluate all files in the patch against the environment and report on the files that will be updated based on the patch.

To run the installer in analyze mode, set the variable ORPATCH_ANALYZE to 'true'.

After clicking "install", the Analyze tool will generate a report of the files that will be patched if you apply this patch to the selected RETAIL_HOME. A high level report can be found in the log file: STAGING_DIR/resa/application/log/ReSAinstall.<timestamp>analyze. Log

The detailed list of patch files can be found in RETAIL_HOME/orpatch/logs/detail_logs/analyze/details/

- If you are using an X server such as Exceed, set the DISPLAY environment variable so that you can run the installer in GUI mode (recommended). If you are not using an X server, or the GUI is too slow over your network, unset DISPLAY for text mode.
- Run the install.sh script. This launches the installer. After installation is completed, a detailed installation log file is created (ReSAinstall.<timestamp>.log).

Test the ReSA Application

After the application installer completes you should have a working ReSA application installation. To launch the application, open a web browser and go to http://host:httpport/ResaPortal

Examples:

- http://<vip_hostname>:<OHS_PORT>/ResaPortal/faces/HomeYou should use a user/password that you built in the previous Case study guide to Load LDIF files in LDAP.

  The default, preloaded user supplied in the LDIF scripts for testing this installed application is RESA_SU; the password is <the password which you have given in the LDIF file RGBU-oid-create-users.ldif as part of loading LDIF files into the LDAP>.

REST Web Service Disable/Re-enable

If you want to disable or enable RST web services for Merchandising Mobile, perform the following procedures.

Disable REST Web Services war

- Login to the WebLogic Administration console with username/password.
- Click the Deployments in the domain structure panel which will list all the applications deployed under that domain.
- In Summary of Deployments click resa15 application.
- Click the Target tab and click **Lock & Edit**.
- Check the ResaReSTServices under Target Assignments and click **Change Targets**.
- Uncheck the server and click **Yes**.
- Click **Activate Changes** for the changes to become effective.

Re-enable REST Web Services war

- Login to the WebLogic Administration console with username/password.
- Click the Deployments in the domain structure panel which will list all the applications deployed under that domain.
- In Summary of Deployments, click **resa15** application.
- Click the Target tab and click Lock & Edit.
- Check the **ResaReSTServices** under Target Assignments, and click **Change** Targets.
- Check the server, and click **Yes**.
- Click **Activate Changes** for the changes to become effective.

Single Sign-On

Note: This section assumes the Oracle WebLogic Server has already been registered with the Oracle Access Manager (OAM) via the oamreg tool. See the Oracle Single Sign-On (OAM using webgate) documentation for details.

If you are using ReSA in an Oracle Single Sign-On environment, then the ReSA root context must be protected. Modify the following files.

- mod_wl_ohs.conf located in <WEBLOGIC_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1
- LoadModule weblogic_module "${ORACLE_HOME}/ohs/modules/mod_wl_ohs.so"
- <IfModule weblogic_module>
- </IfModule>

```
<Location /console>
        WebLogicHost <weblogichostname>
        WebLogicPort <AdminServerPort>
        SetHandler weblogic-handler
</Location>

<Location / ResaPortal-Portal-context-root />
        WebLogicHost <weblogichostname>
        WebLogicPort <resaserverport>
         WLCookieName RESASESSIONID
        SetHandler weblogic-handler
</Location>

<Location /adfAuthentication>
        WebLogicHost <weblogichostname>
        WebLogicPort <resaserverport>
         WLCookieName RESASESSIONID
        SetHandler weblogic-handler
</Location>
```

Note: In the above, modify 'ResaPortal-Portal-context-root' with the context root name used for installing the ReSA Application.

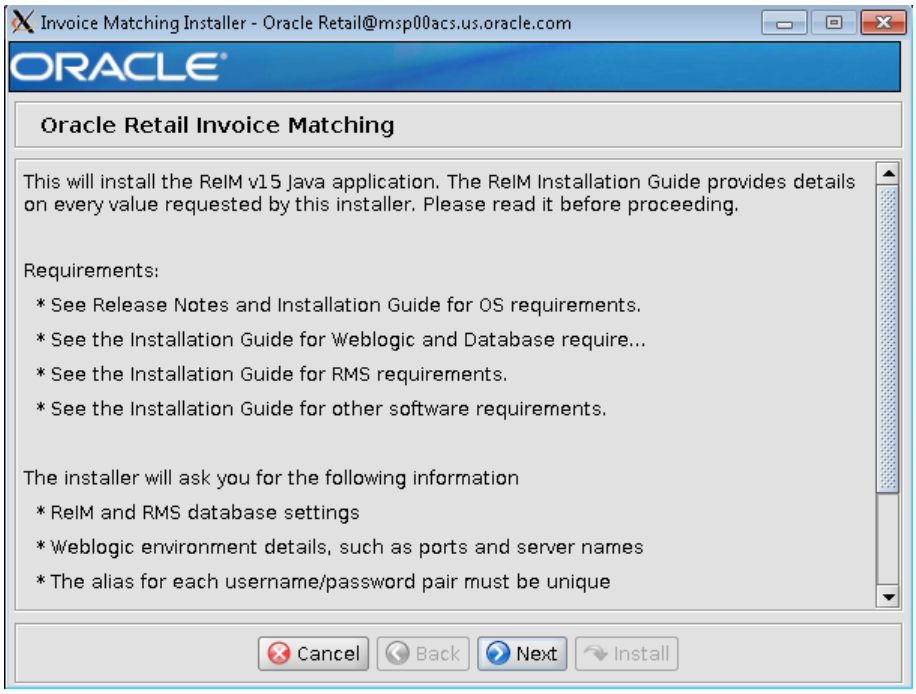
A

Appendix: REIM Application Installer Screens

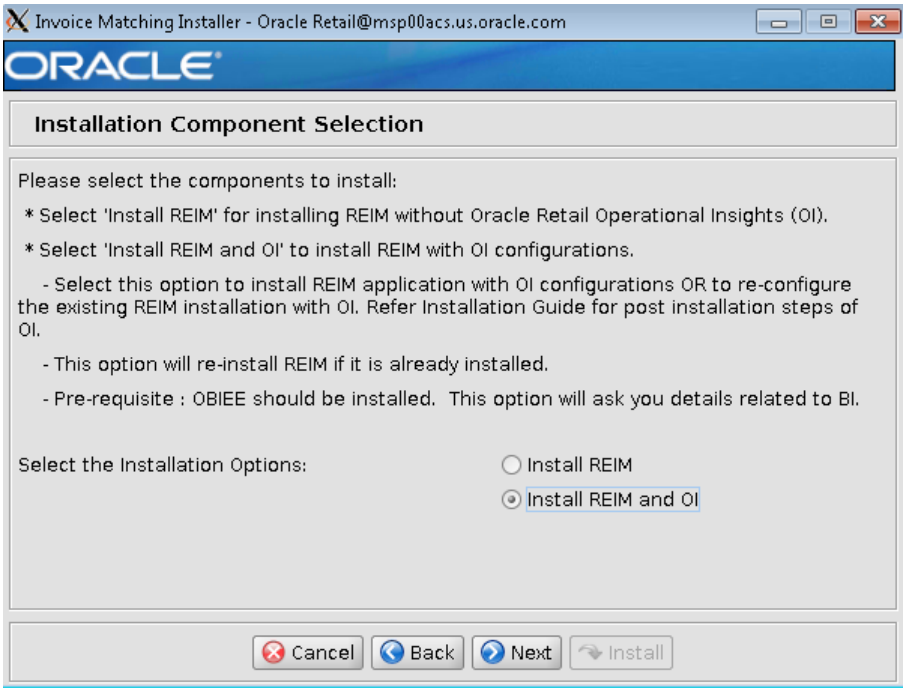
Below are the details of Application installer screens for REIM.

You need the following details about your environment for the installer to successfully deploy the SIM application. Depending on the options you select, you may not see some screens.

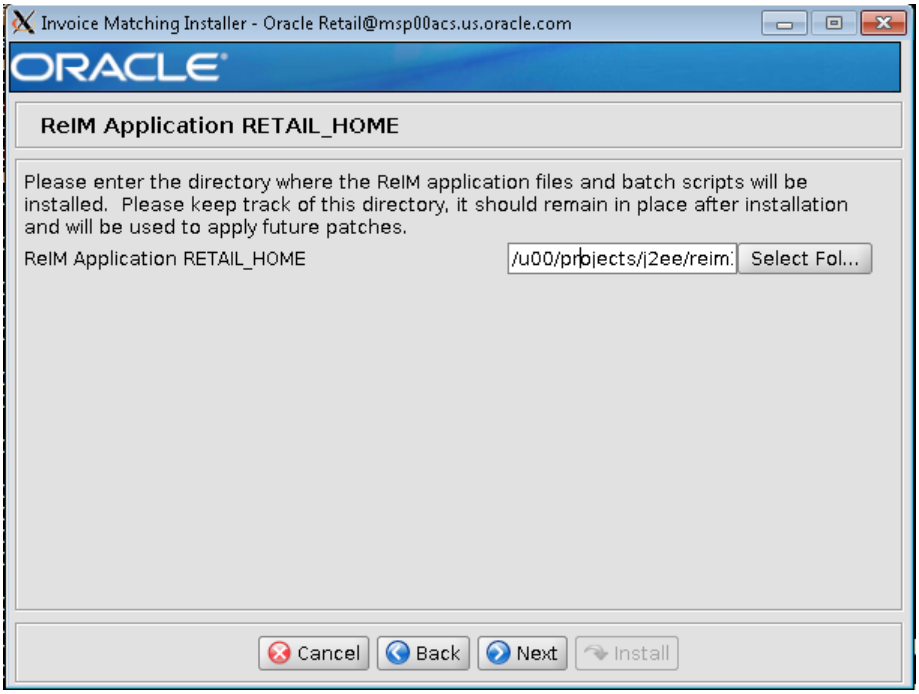
- Starup Screen

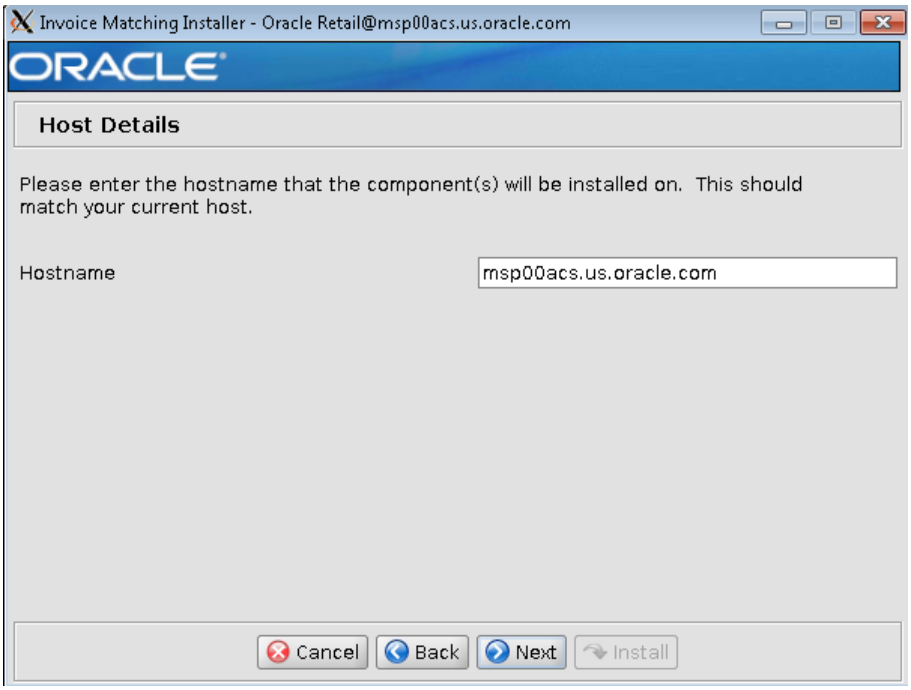


- The Installation Component Selection window opens.

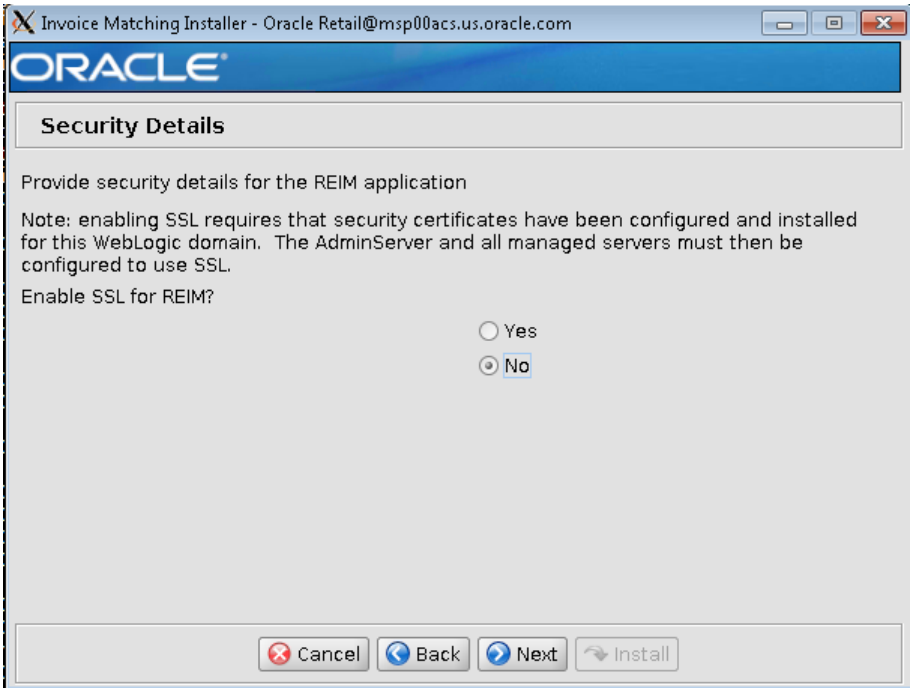


- The ReIM Application RETAIL_HOME opens. Update host details.

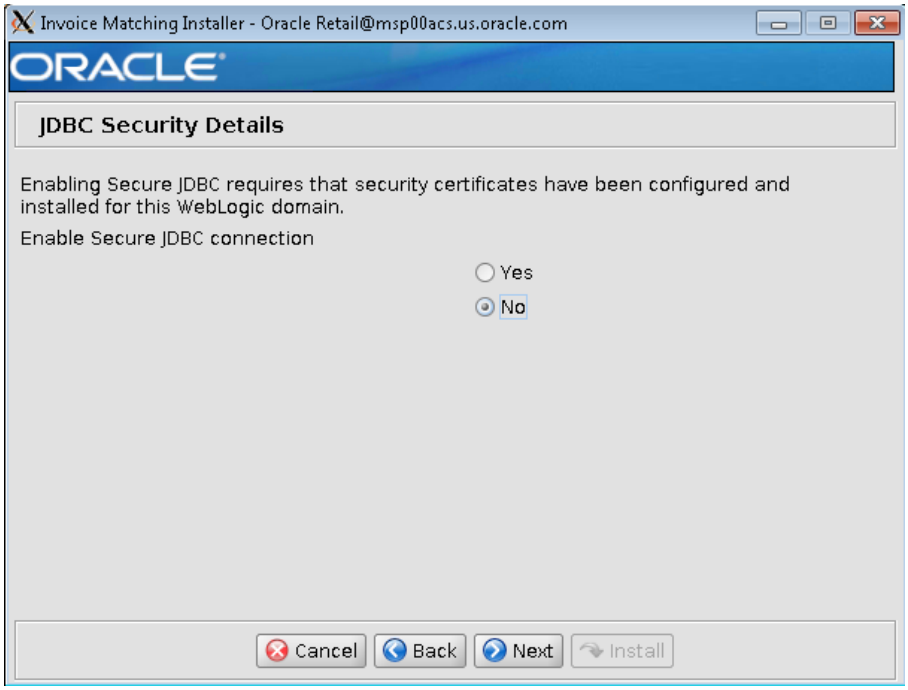




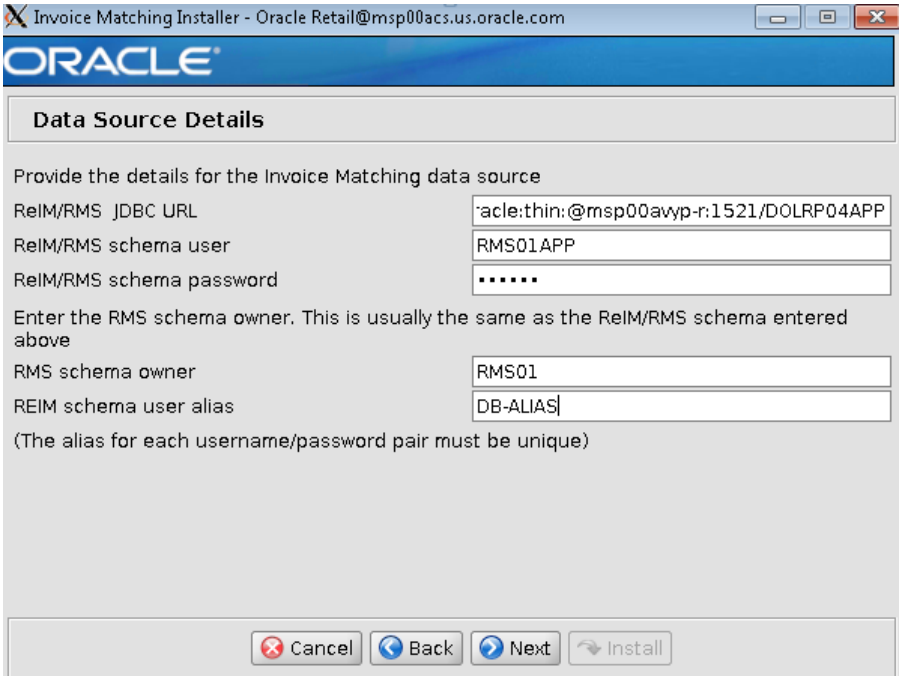
- Security Details



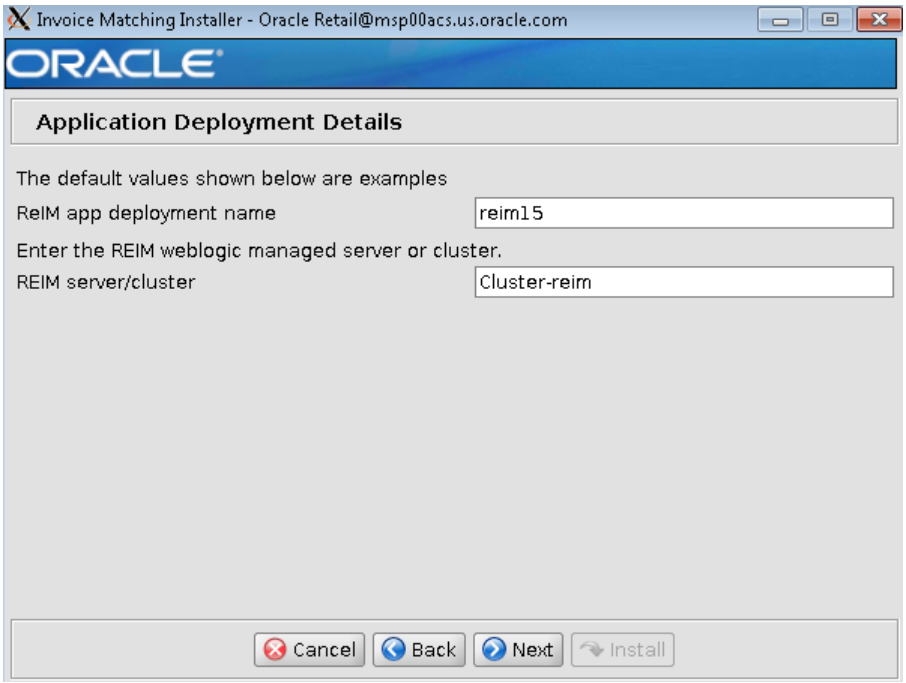
- JDBC Security Details



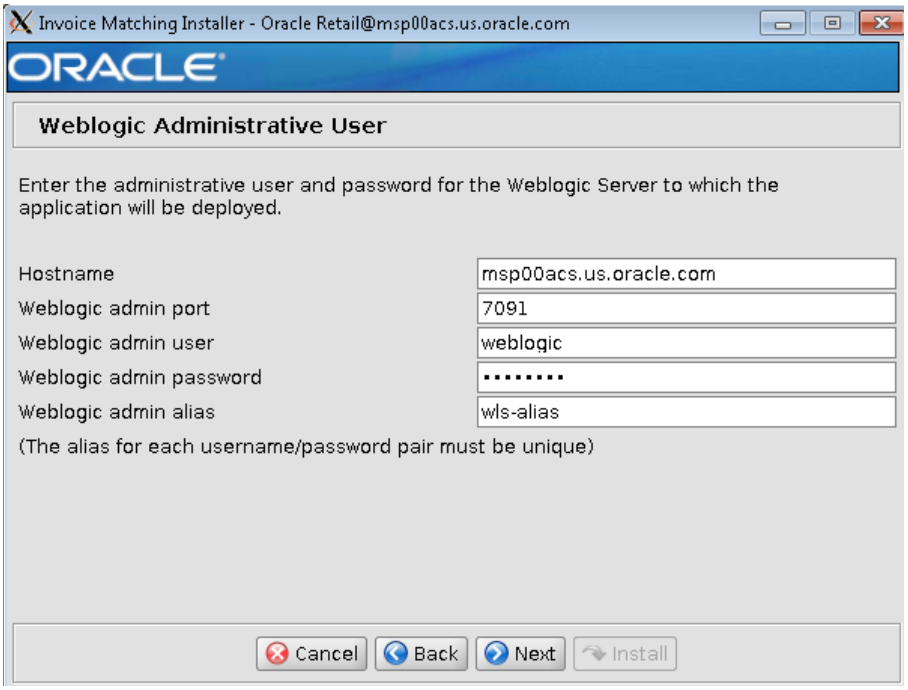
- Data Source Details



- Application Deployment Details

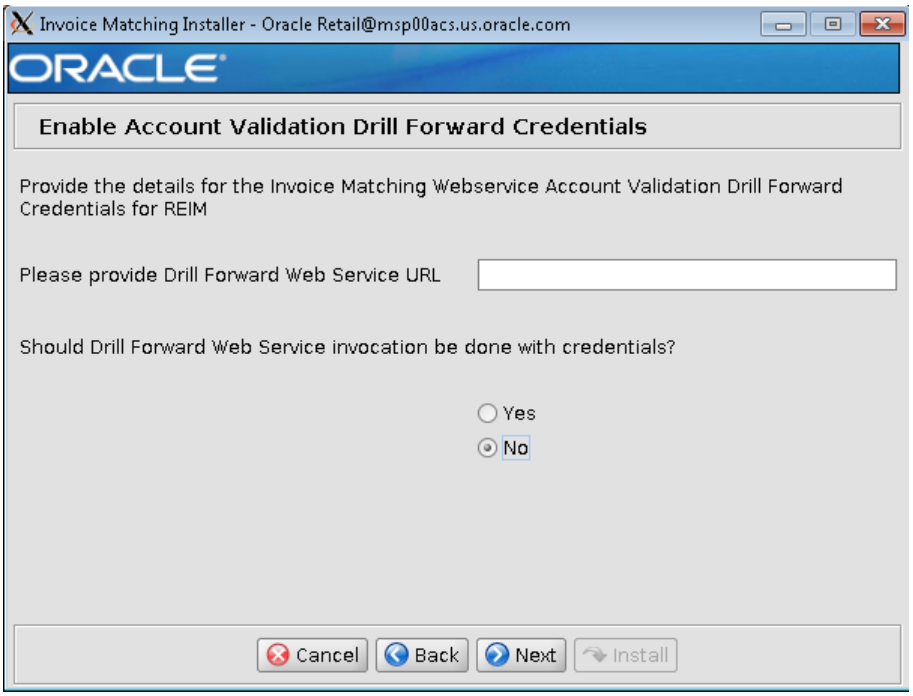


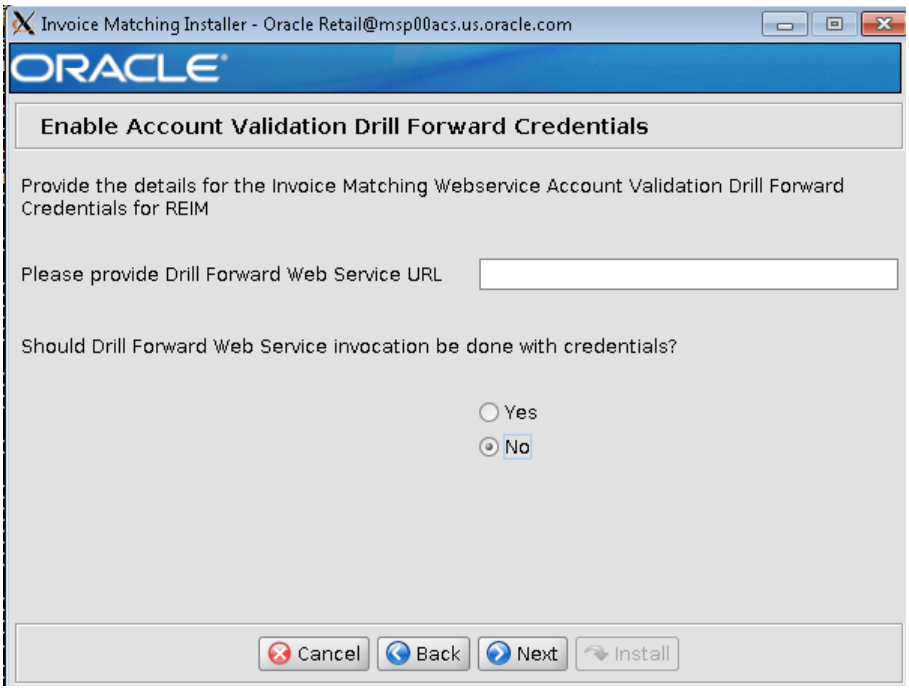
- Update WebLogic Administrative User



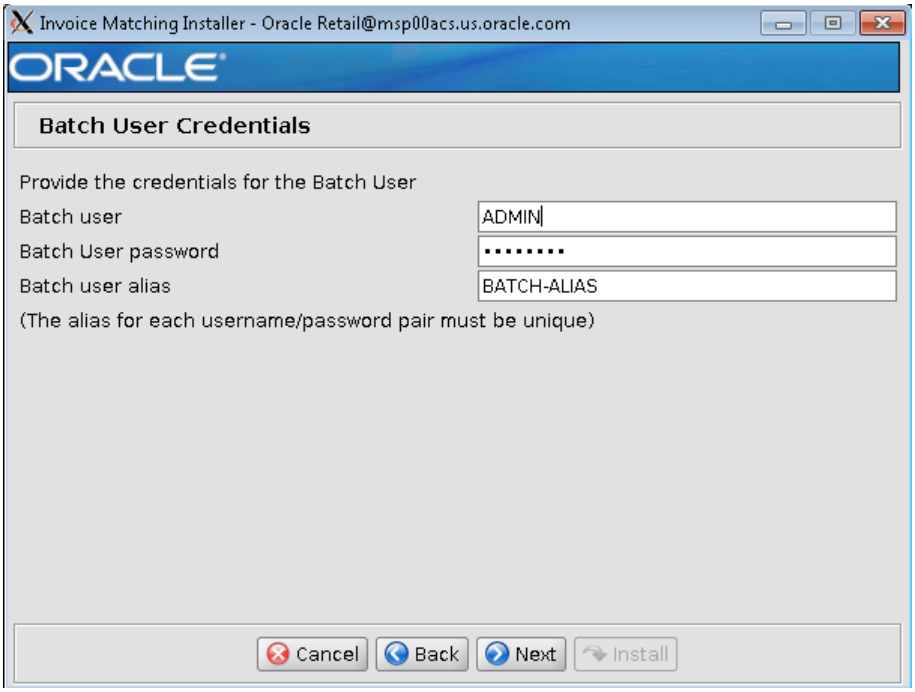
- You can also update the Webservice Account validation.

The Web service provider URL used for drilling forward from the ReIM application. This information is from the financial application to which you are integrating (for example, Oracle E-Business Suite). Leave this field blank if there is no integration with a financial application.

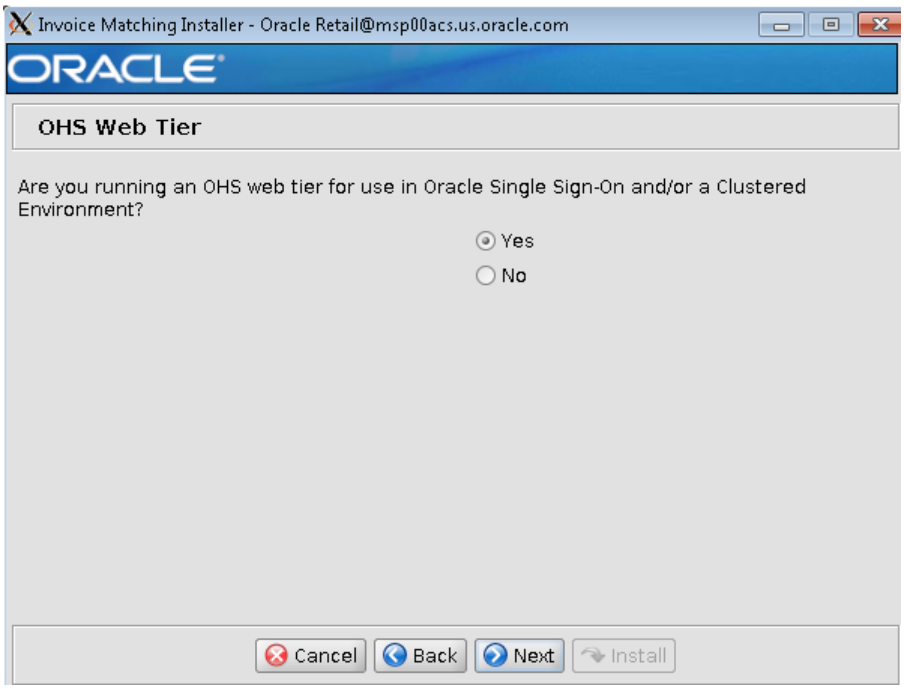


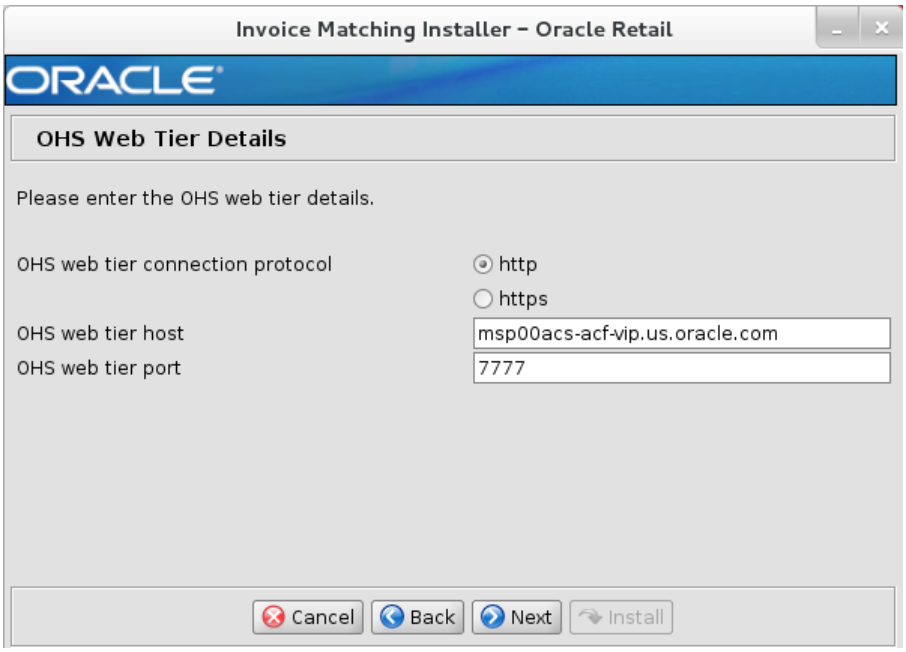


- The Batch User Credentials window opens.

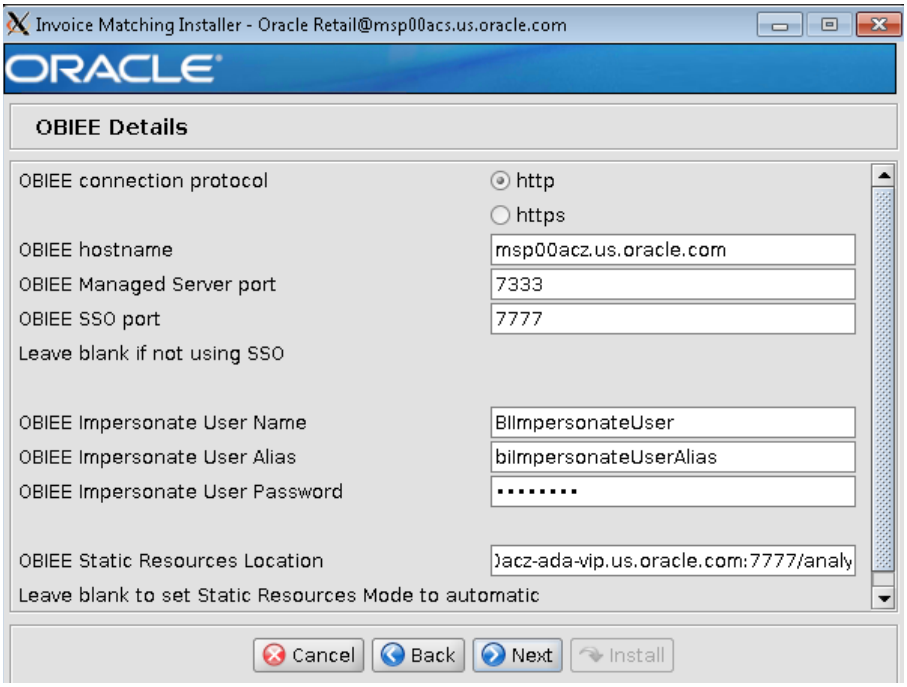


- Update OHS Webtier details

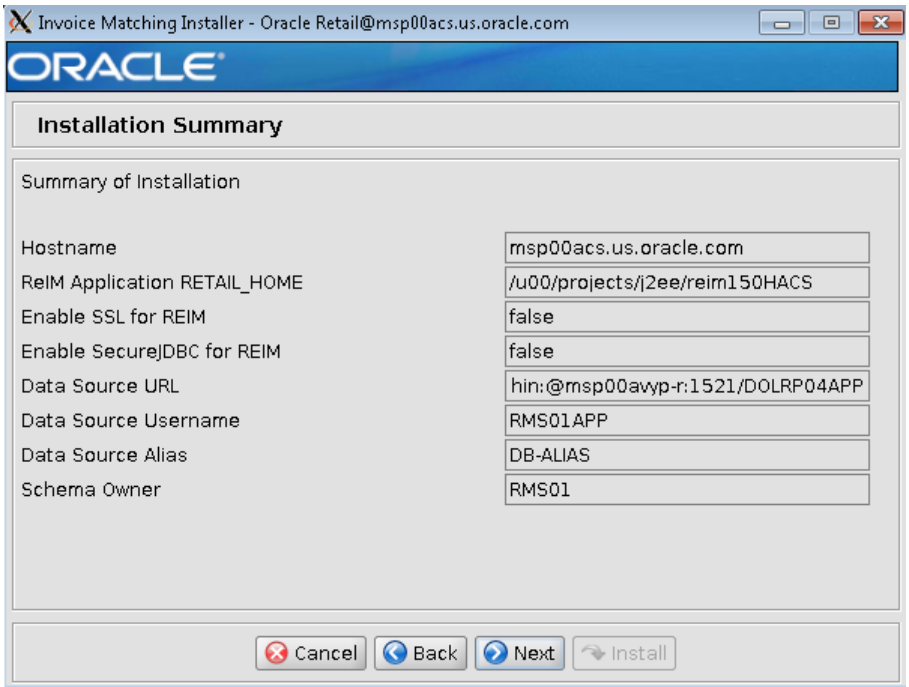


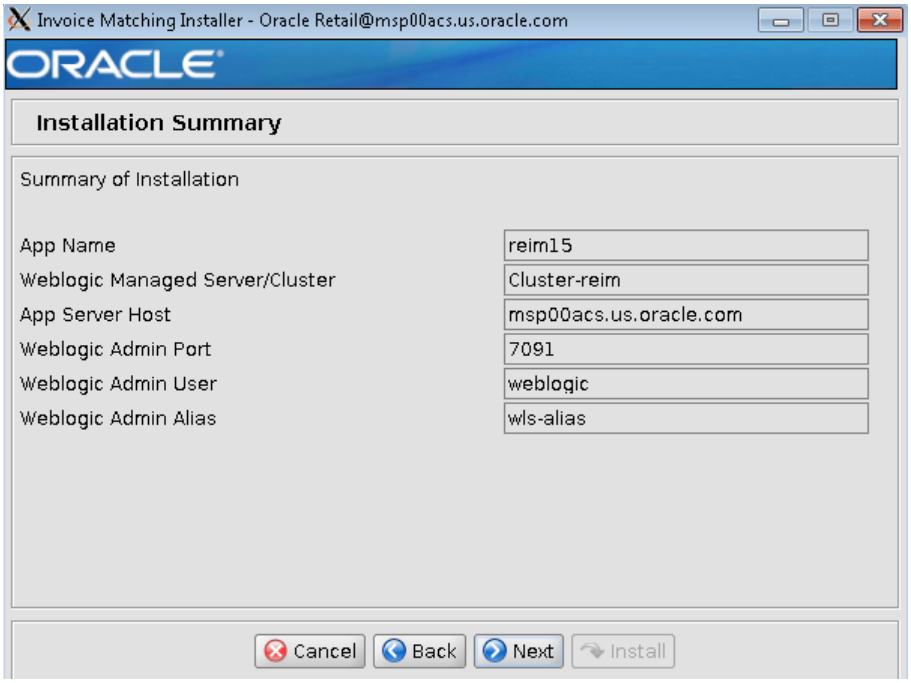


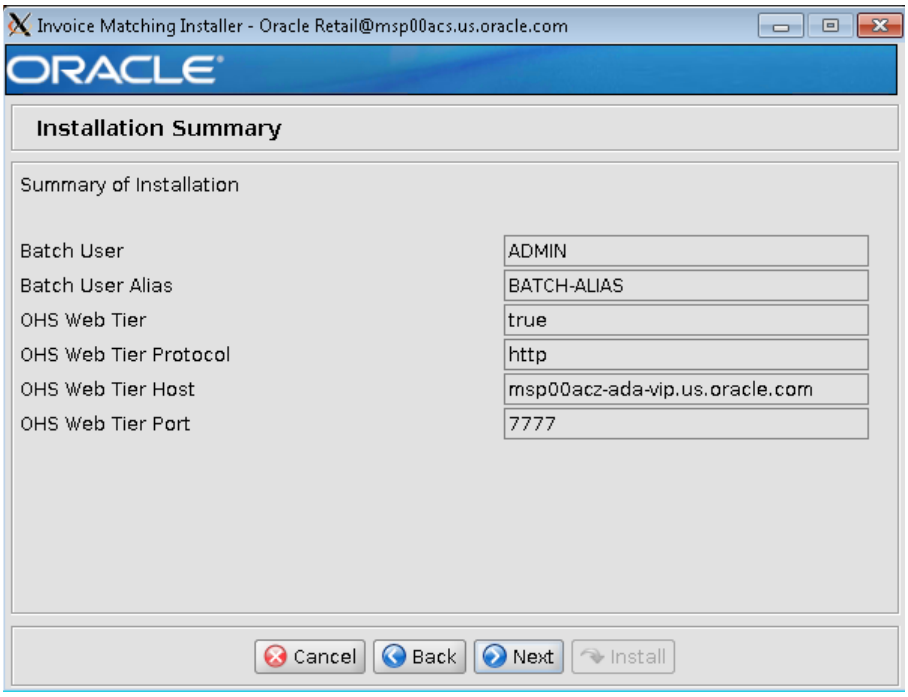
- OBIEE Details

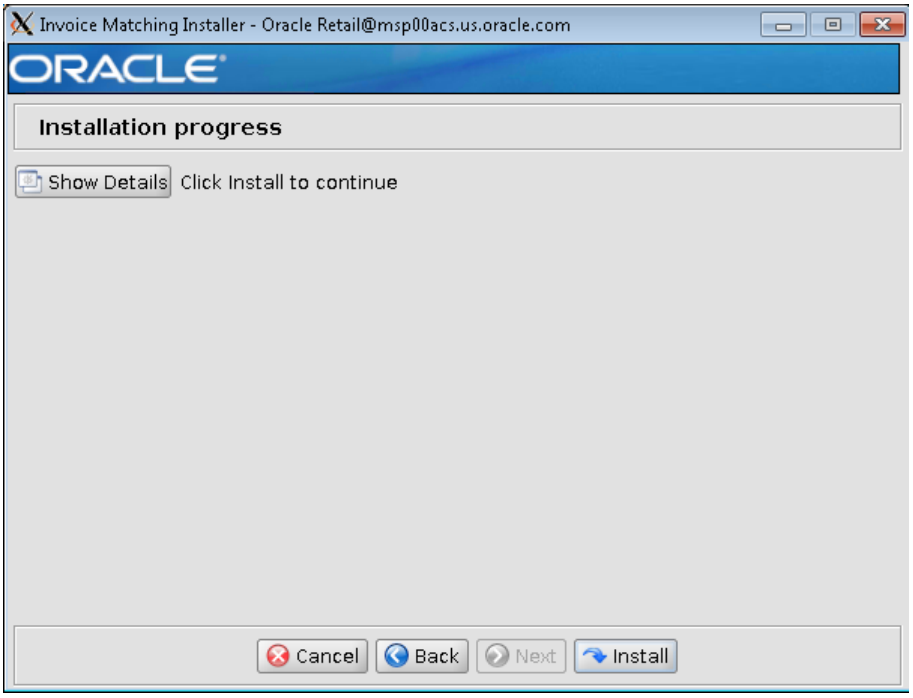


- Installation Summary.




Invoice Matching Installer - Oracle Retail@msp00acs.us.oracle.com
ORACLE
Installation Summary
Summary of Installation
App Name
reim15
Weblogic Managed Server/Cluster
Cluster-reim
App Server Host
msp00acs.us.oracle.com
Weblogic Admin Port
7091
Weblogic Admin User
weblogic
Weblogic Admin Alias
wls-alias
Cancel
Back
Next
Install


Invoice Matching Installer - Oracle Retail@msp00acs.us.oracle.com
ORACLE
Installation Summary
Summary of Installation
Batch User
ADMIN
Batch User Alias
BATCH-ALIAS
OHS Web Tier
true
OHS Web Tier Protocol
http
OHS Web Tier Host
msp00acz-ada-vip.us.oracle.com
OHS Web Tier Port
7777
Cancel
Back
Next
Install



- Click **Install** and once it is completed click **Finish**.

> **Note:** Copy the Retail_Home content from APPHOST1 to APPHOST2 after installation is completed. This Note is valid for all the Clustered application Installation. Ex ReSA, ReIM, Alloc, SIM and RPM

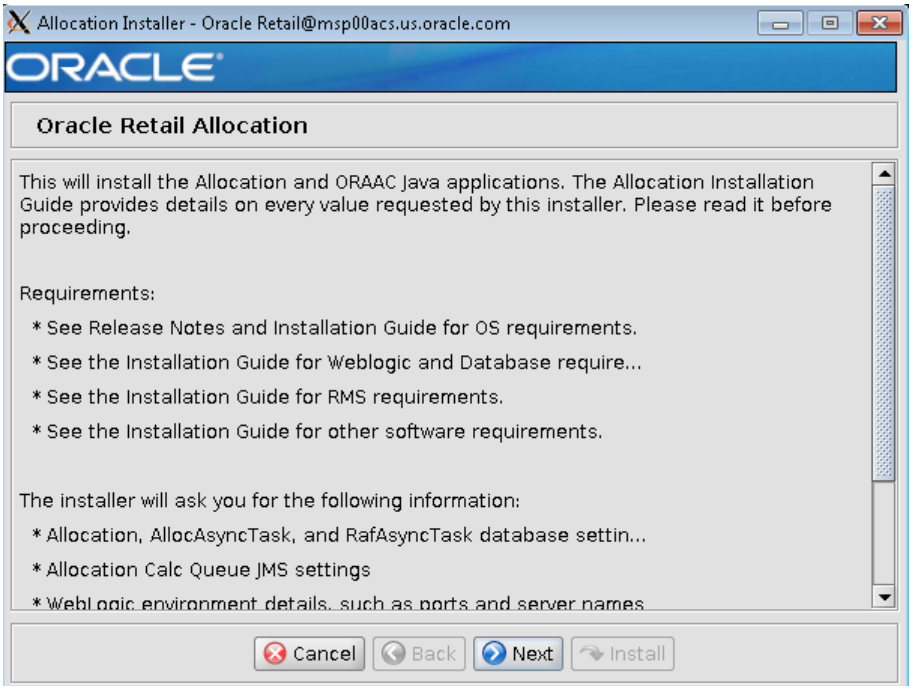
B

Appendix: Oracle Retail Allocation Application Installer Screens

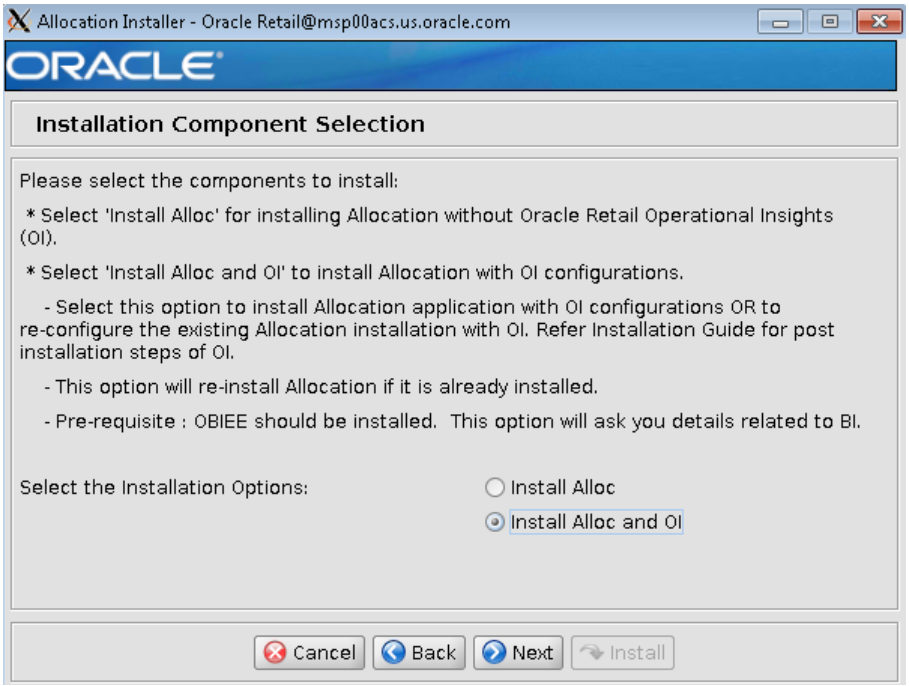
Below are the details of Application installer screens for ALLOCATION.

You need the following details about your environment for the installer to successfully deploy the Oracle Retail Allocation application. Depending on the options you select, you may not see some screens or fields.

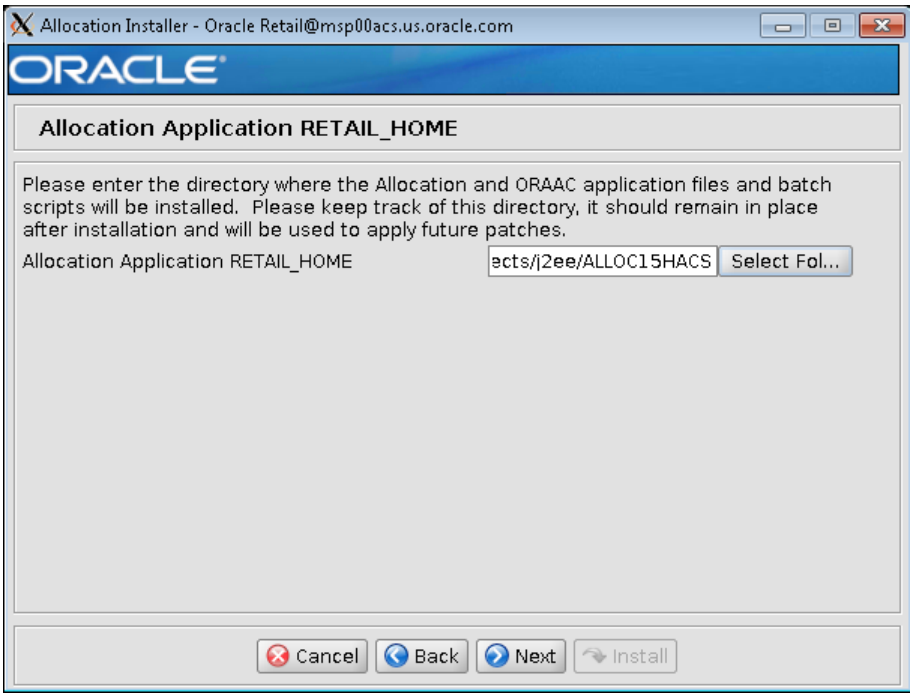
- Installation startup screen



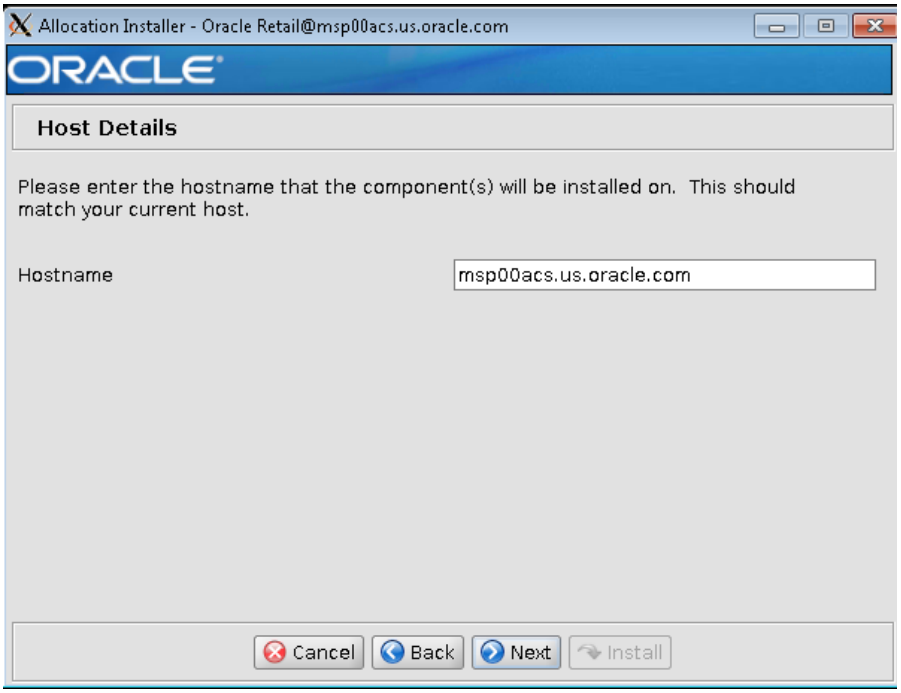
- Installation Component Selection.



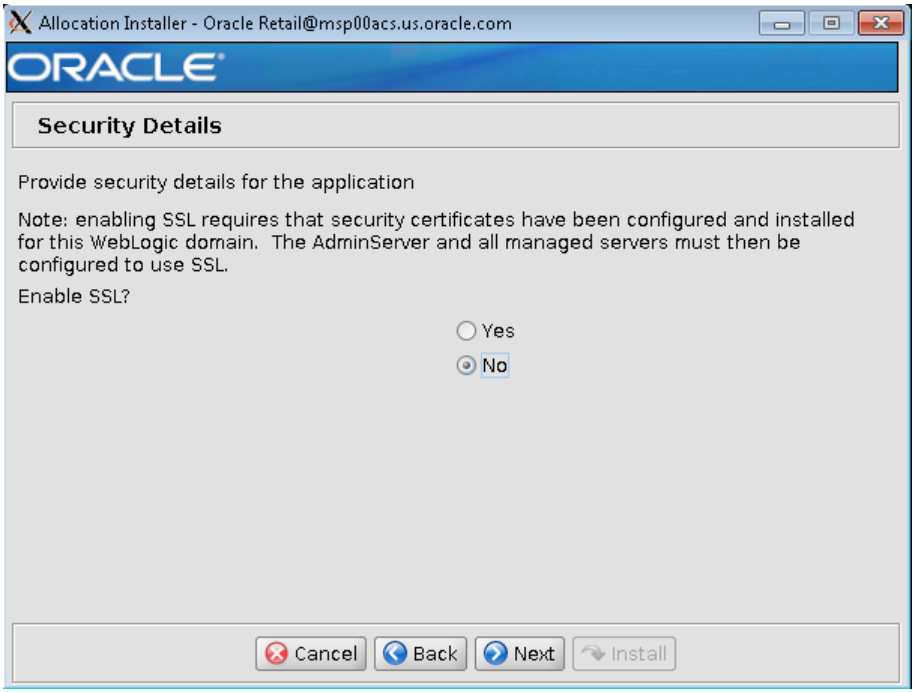
- Update Allocation Application RETAIL_HOME



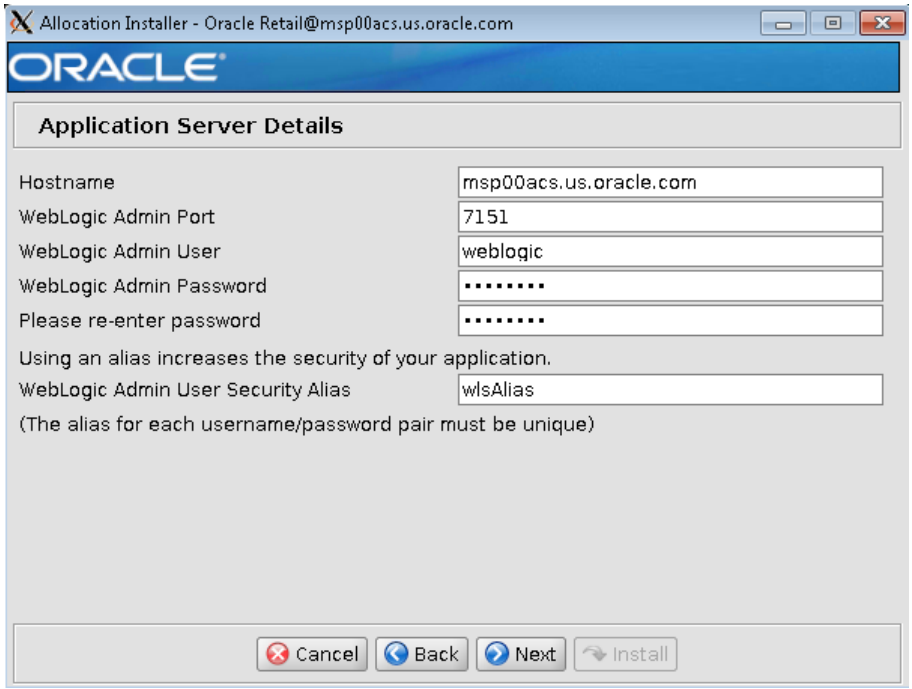
- Update Host details.



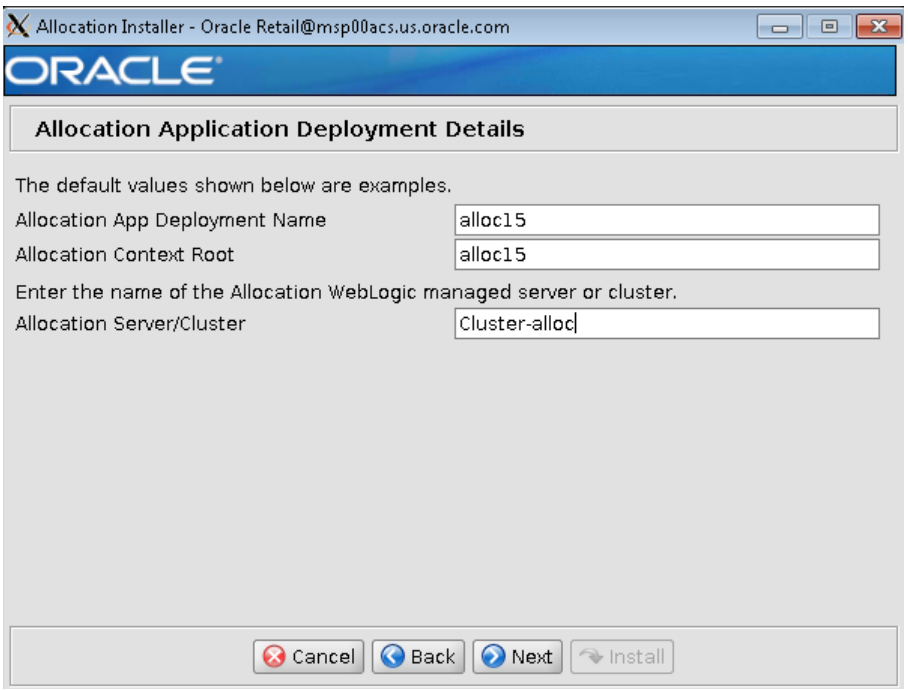
- Security details for application



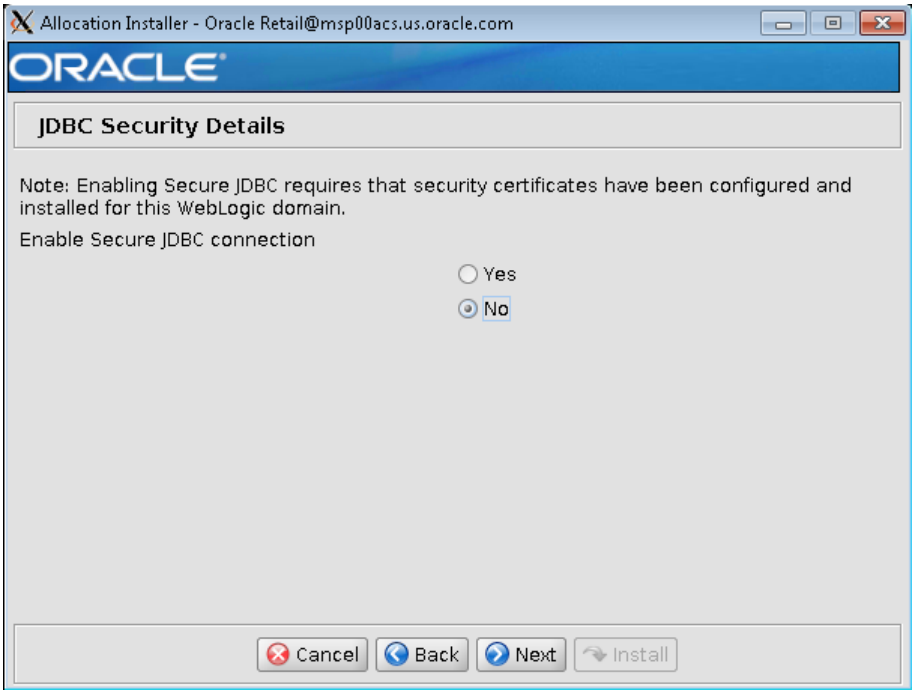
- Update with Application server details.



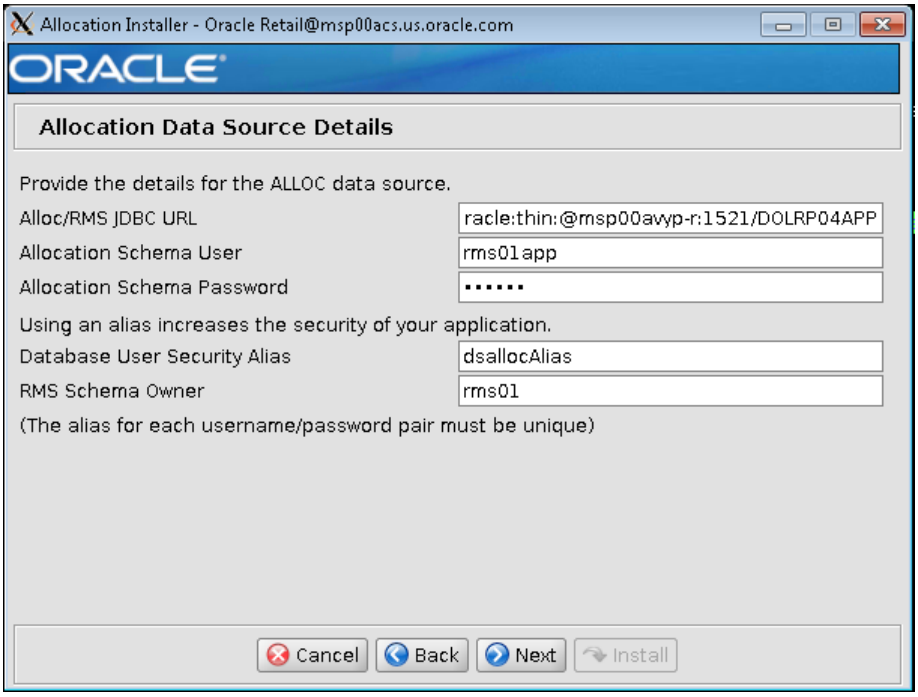
- Update Application Deployment details.



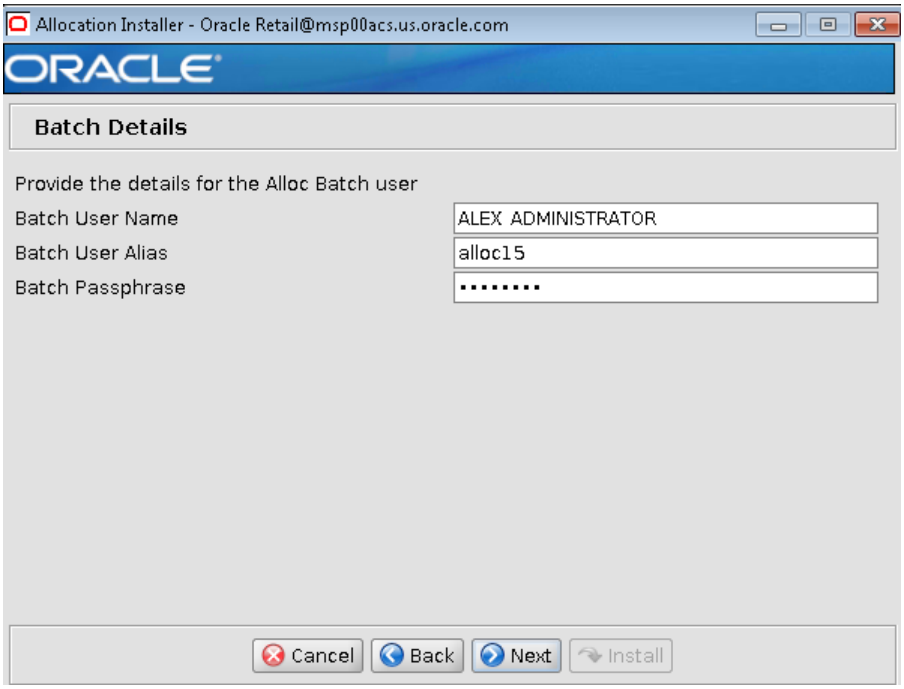
- The JDBC Security details window opens.



- Update Allocation datasource details.

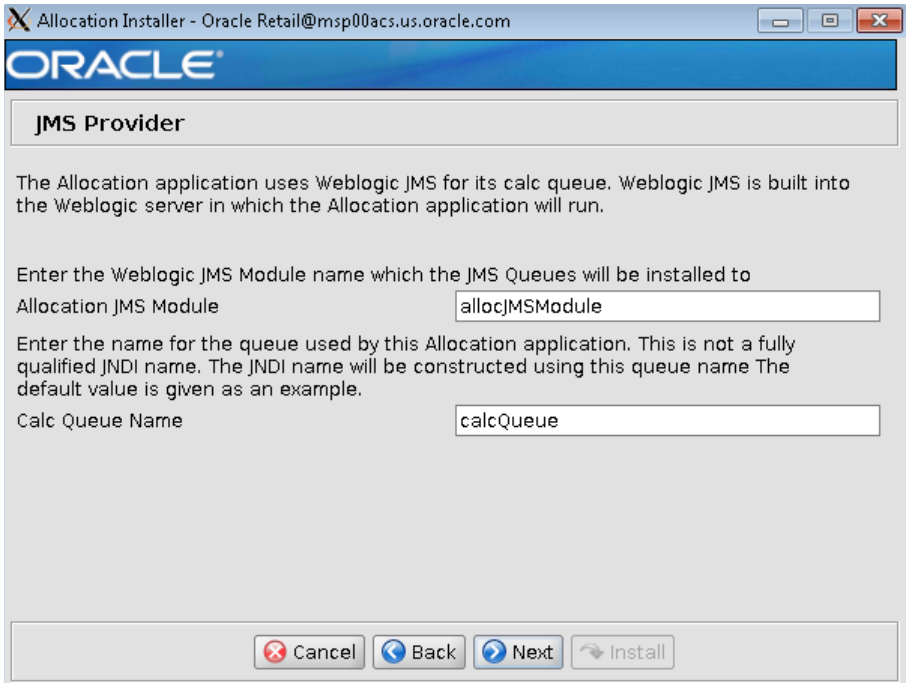


- Update Batch Details.

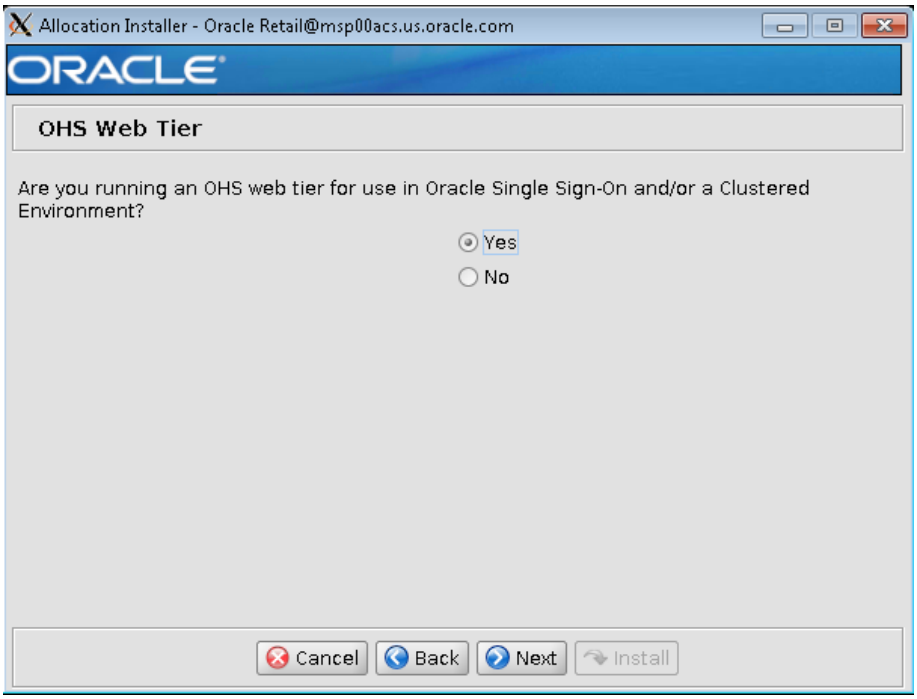


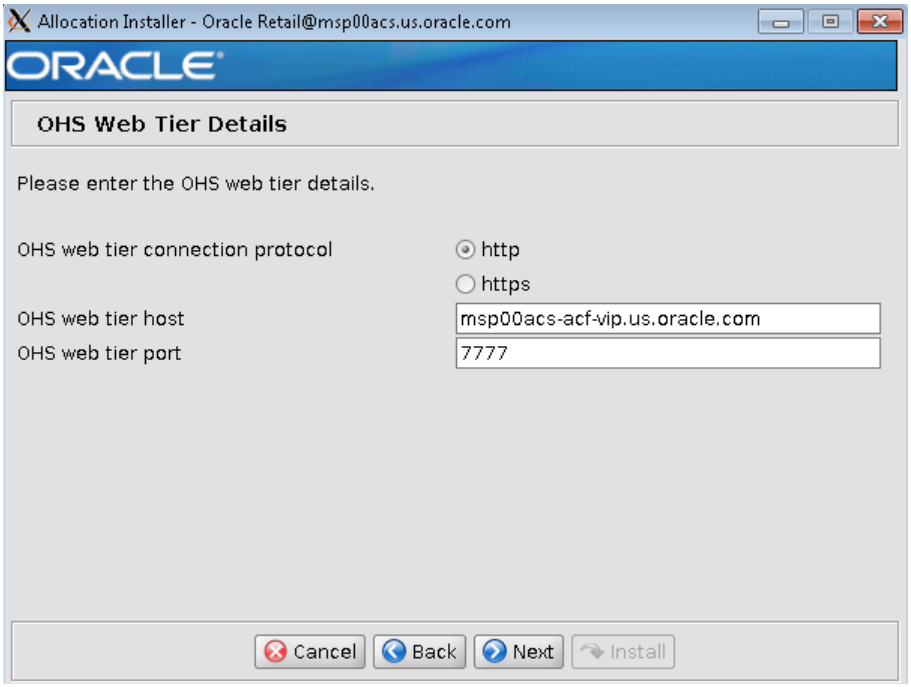
Update Batch user name as Admin user (Ex: ALLOCATION_ADMIN)

- JMS Provider details.

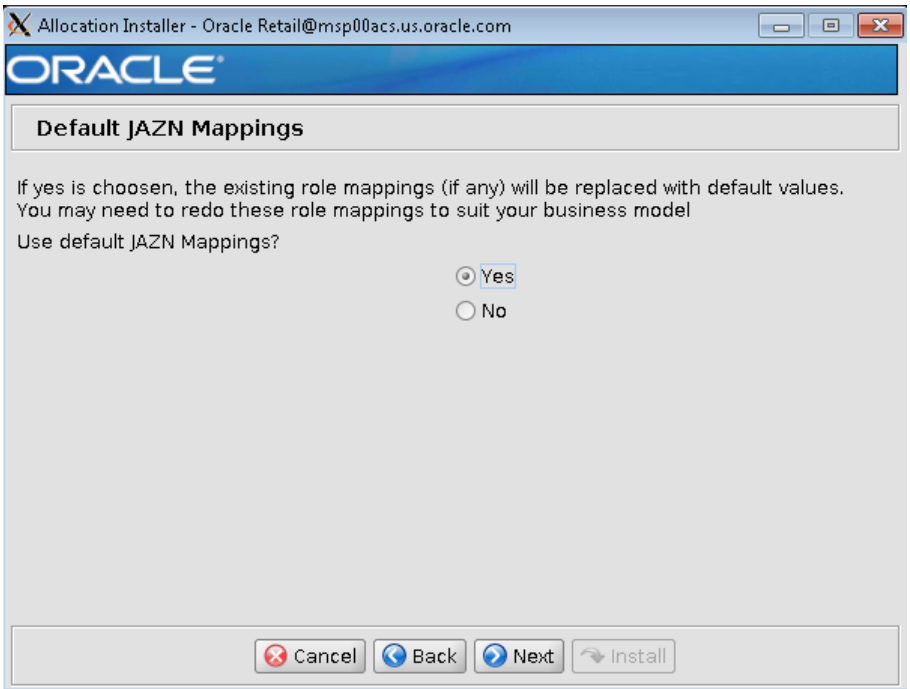


- Enable OHS Webtier and update details

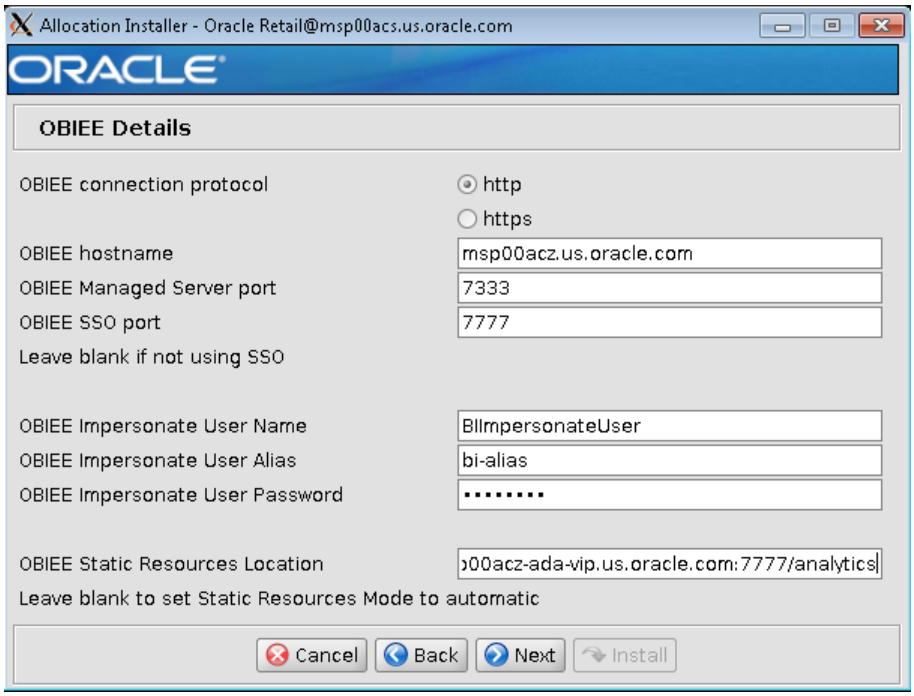




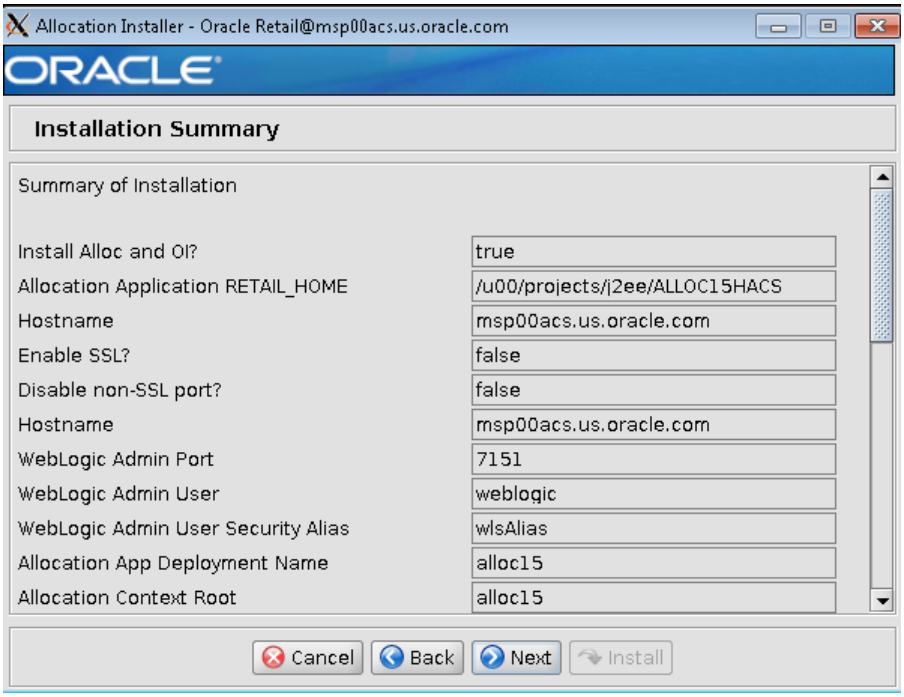
- Set default JAZN mapping to Yes.



- The OBIEE Details window opens.



- The Installation Summary window opens.



- Click **Install** and click **Finish** once the deployment is completed.

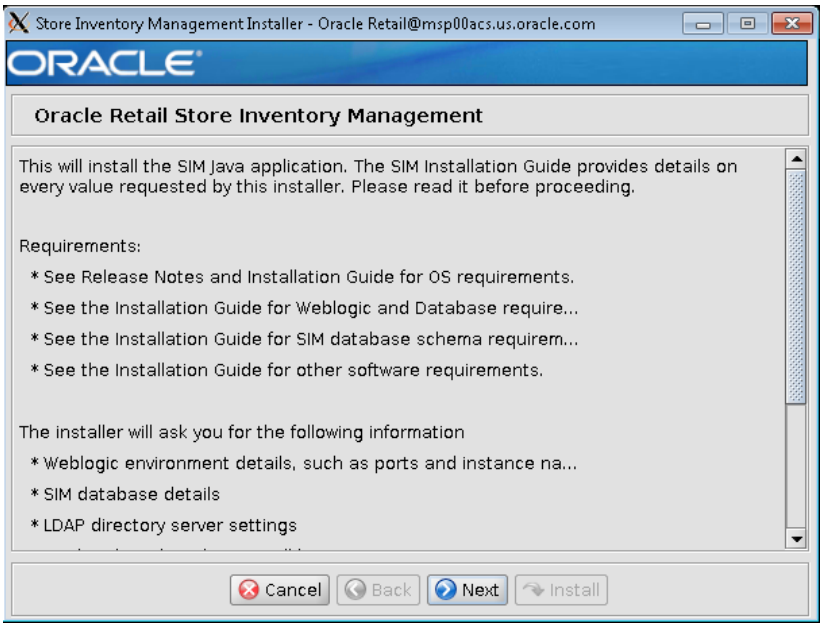
C

Appendix: SIM Application Installer Screens

Below are the details of Application installer screens for SIM.

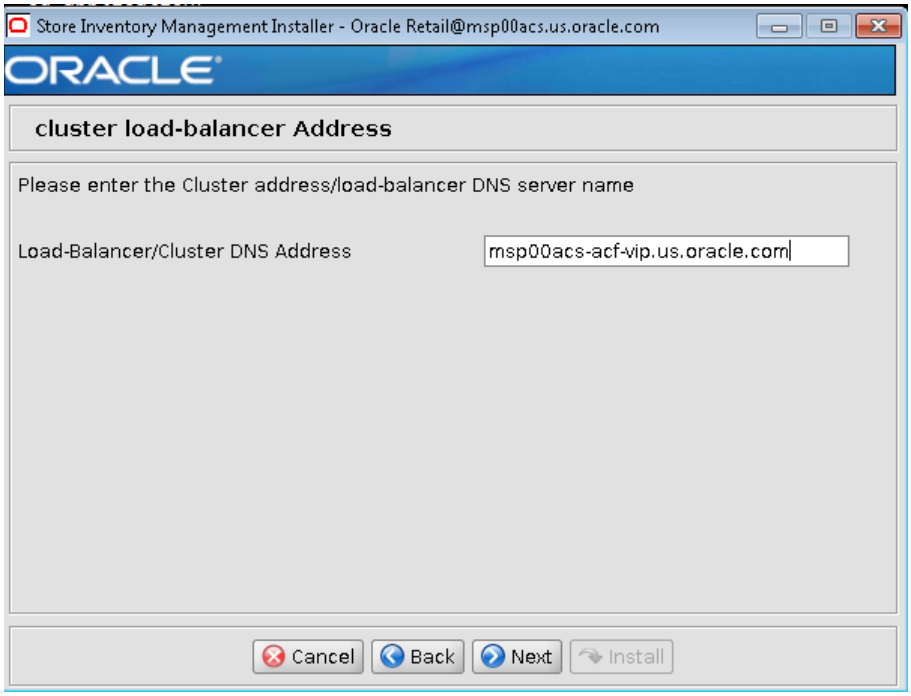
You need the following details about your environment for the installer to successfully deploy the SIM application. Depending on the options you select, you may not see some screens.

- SIM startup application Screen

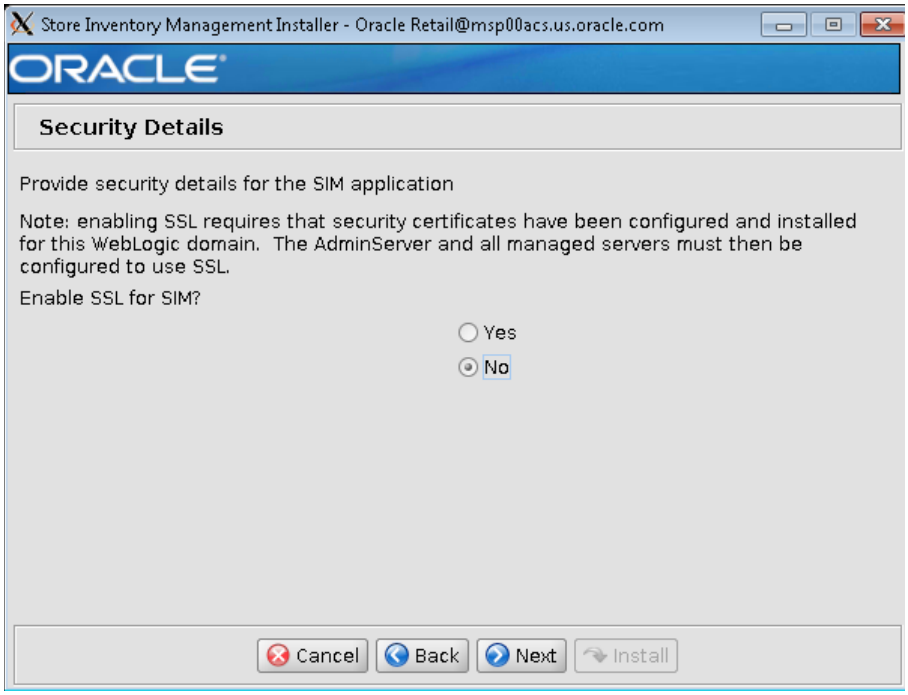


- Installation Type

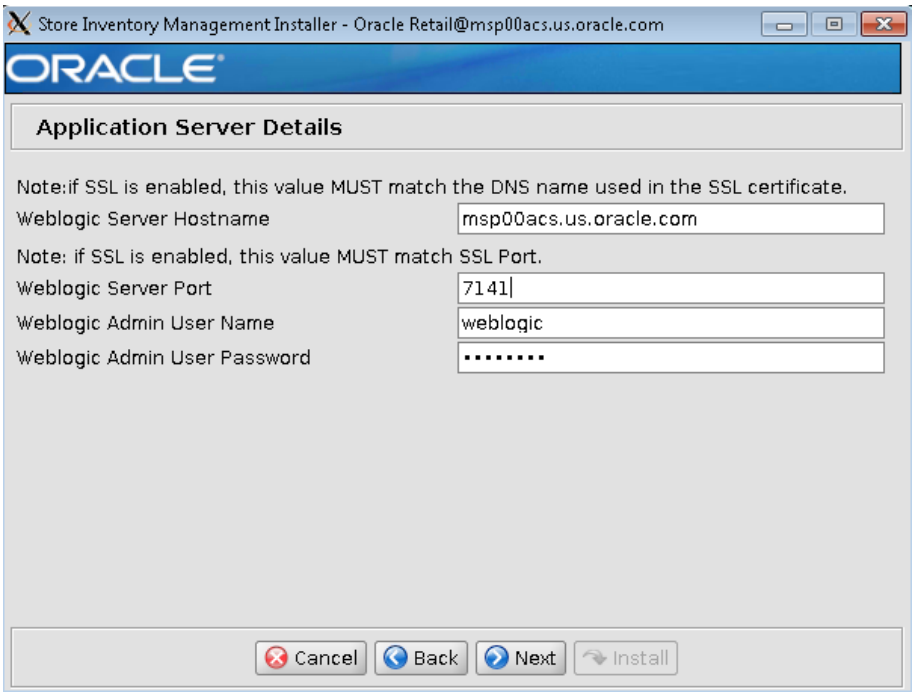
- Update Cluster Load – balancer Address.



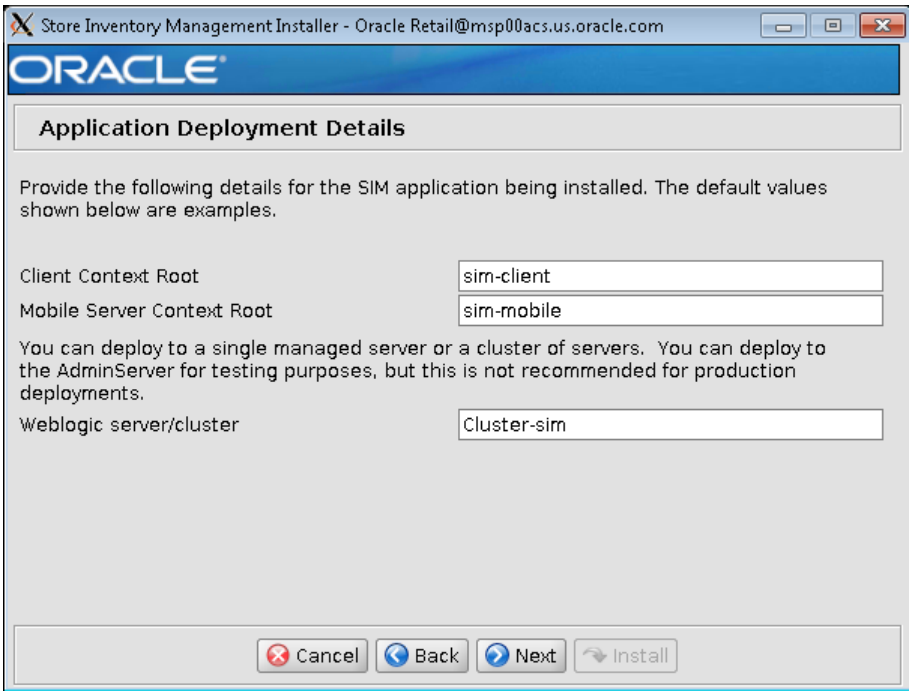
- Security Details for SIM



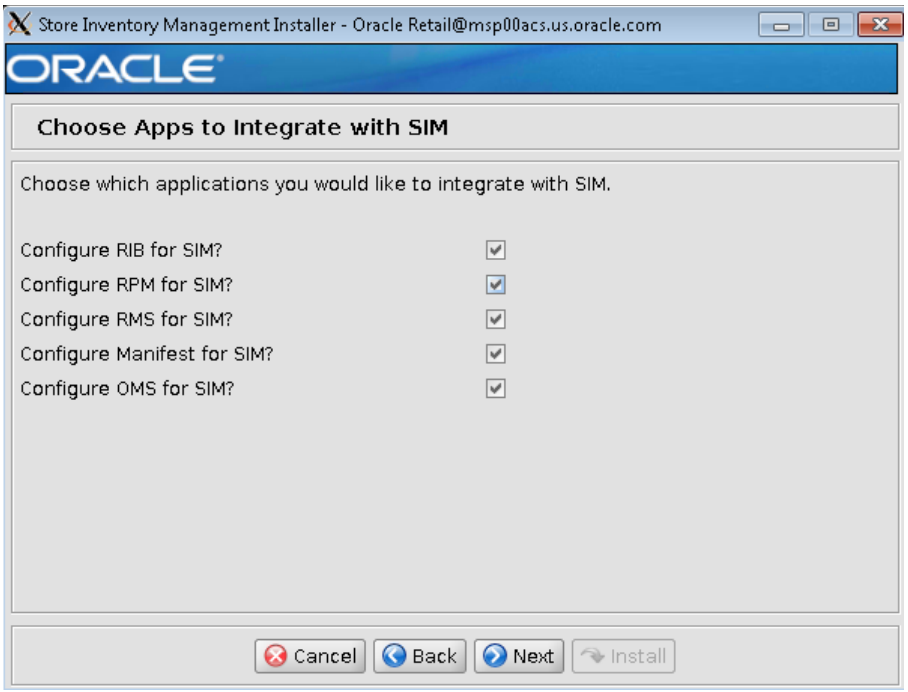
- Update Application Server Details



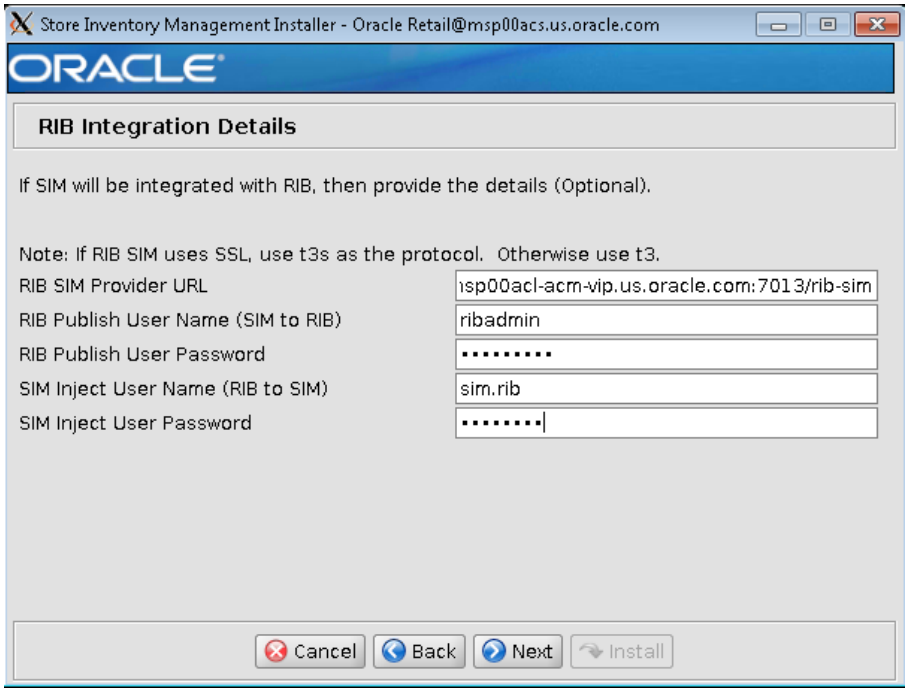
- Update Application Deployment Details

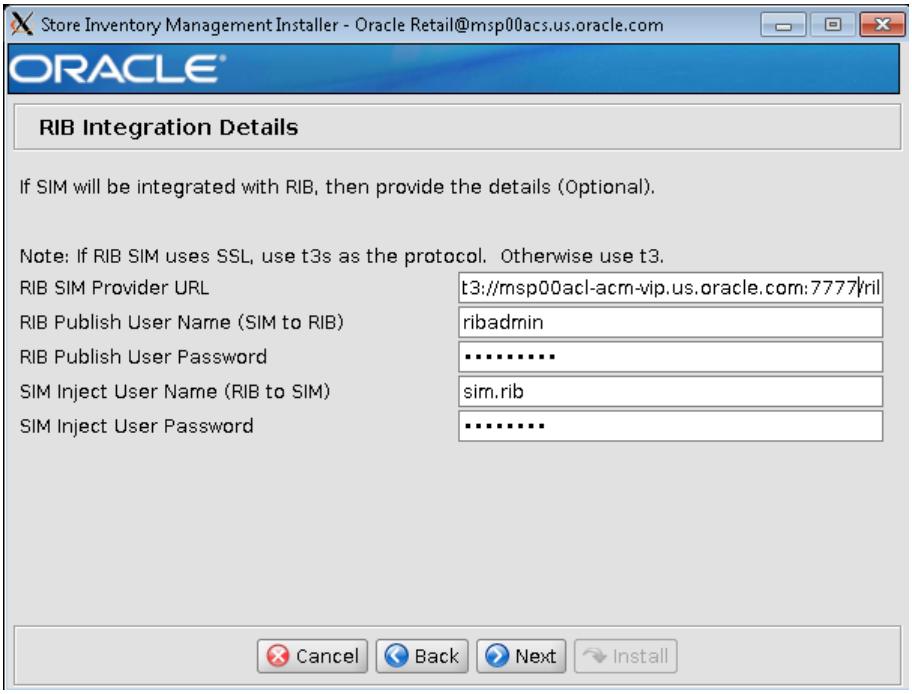


- Choose Apps to Integrate with SIM.



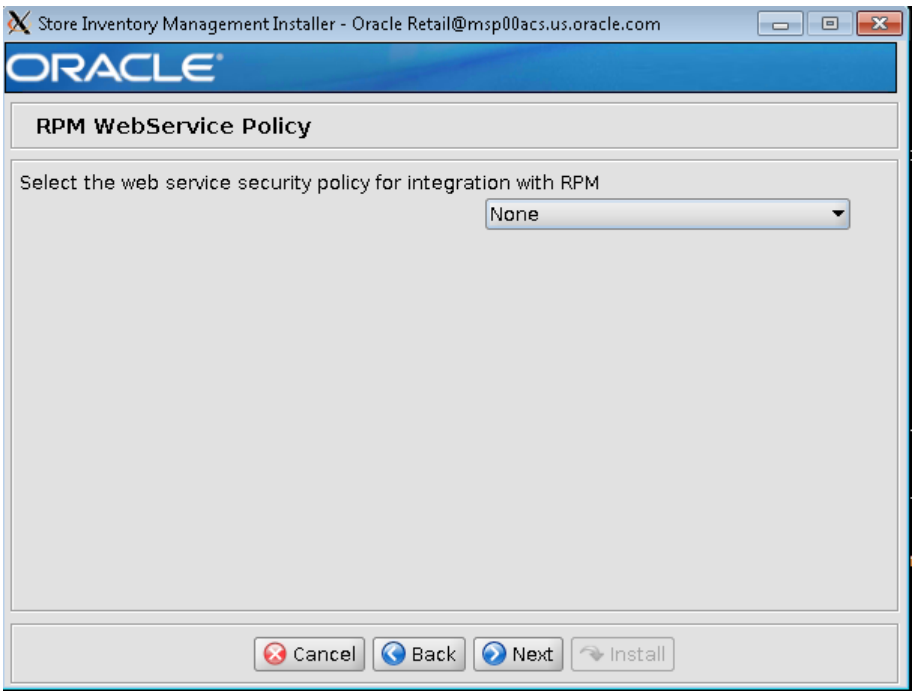
- Update RIB Integration Details





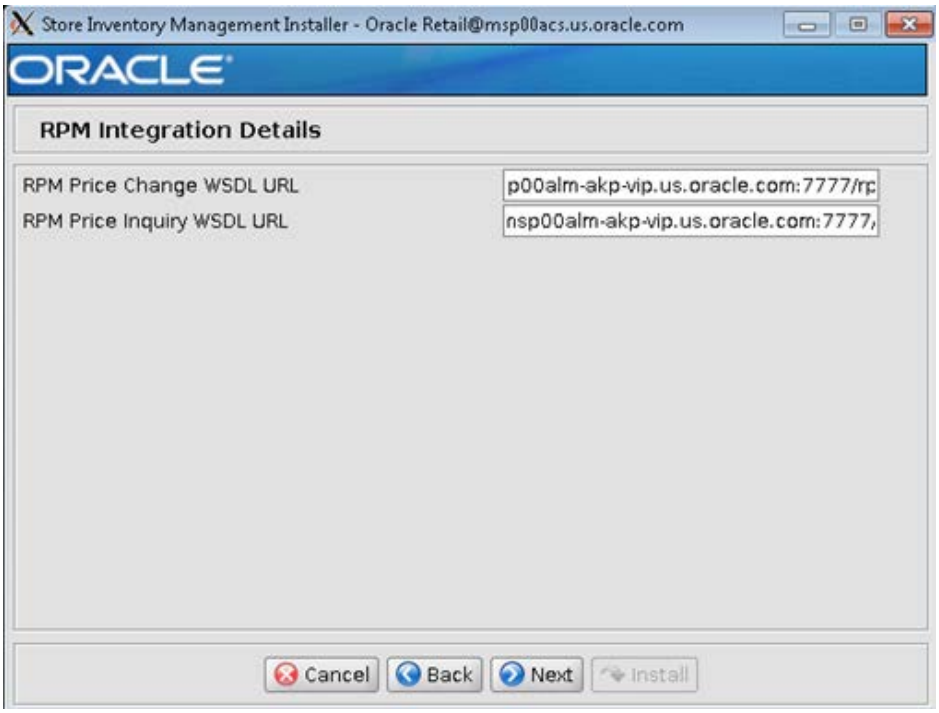
- RPM Webservice policy.

  Please refer to the *Oracle Retail Store Inventory Management Security Guide* to learn more about Policy A and Policy B. Here I have not selected the POLICY.



- **RPM Integration Details**

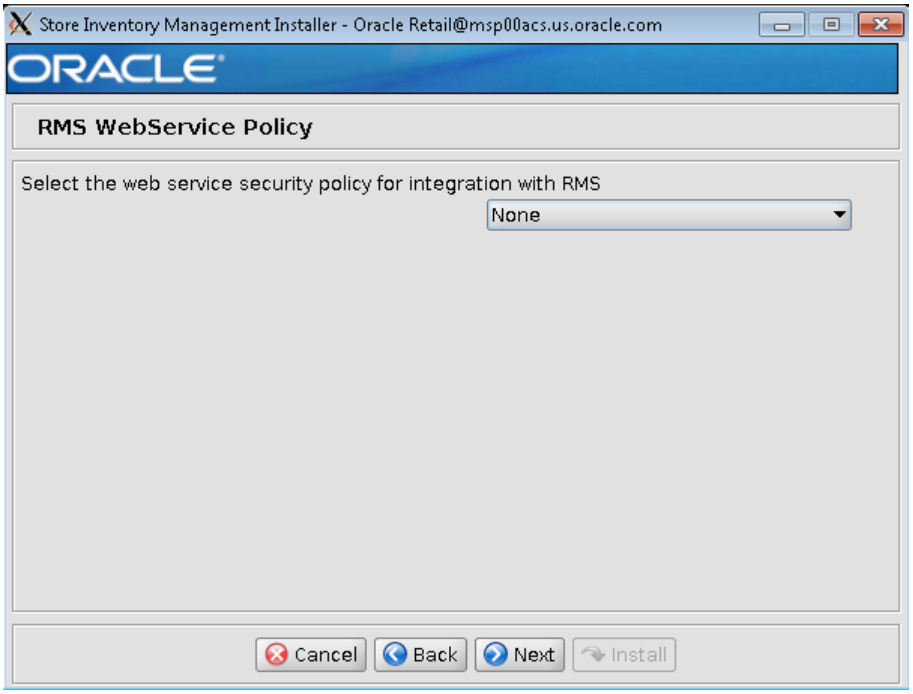
  This screen will be displayed if the Configure RPM for SIM option is checked on the Choose Apps to Integrate with SIM screen.



Note: If the user chooses to integrate SIM with RPM then RPM installation is a pre-requisite to installing SIM.

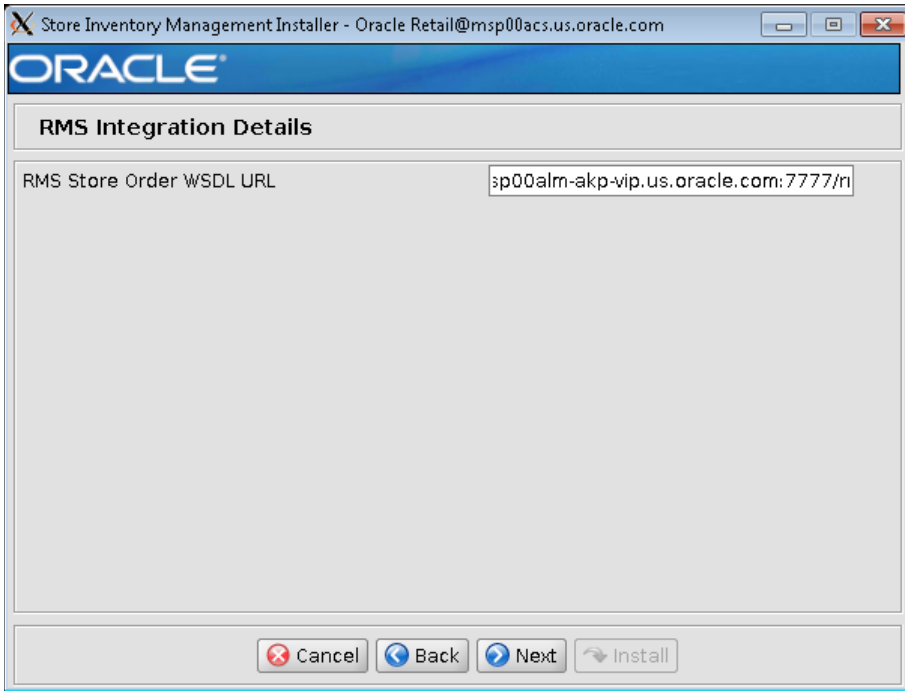
- **RMS Web service Policy**

This screen will be displayed if the Configure RMS for SIM option is checked on the Choose Apps to Integrate with SIM screen.



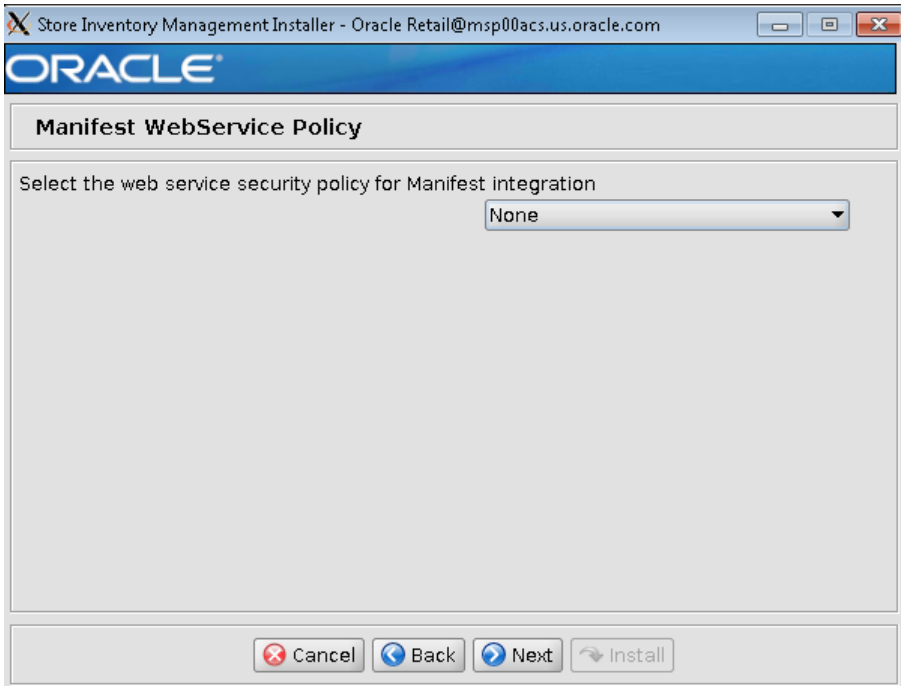
- **Screen: RMS Integration Details**

  This screen will be displayed if the Configure RMS for SIM option is checked on the Choose Apps to Integrate with SIM screen.



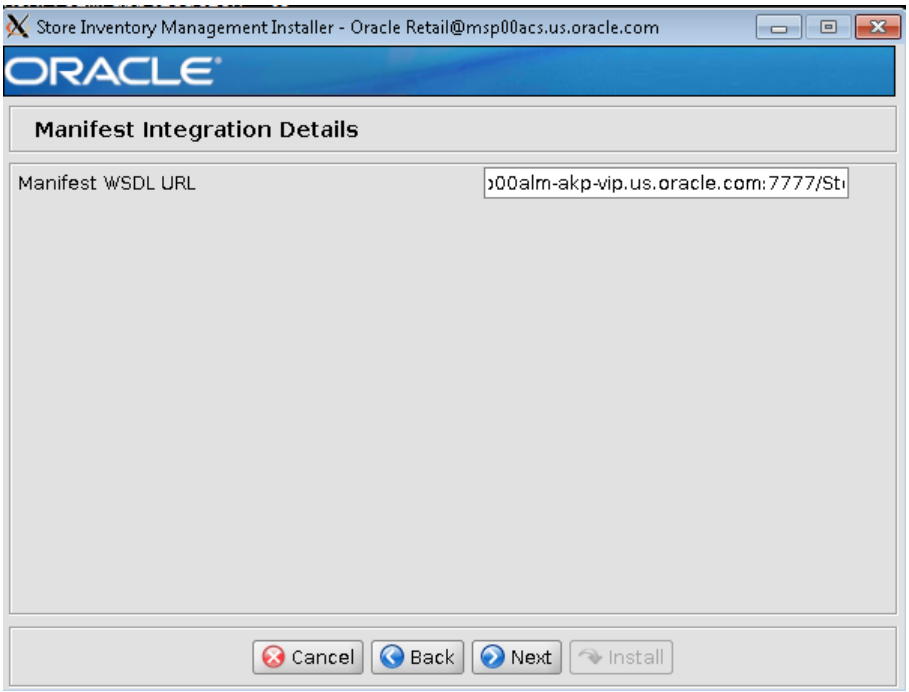
Note: If there are no policies, then the above screen can be left blank.

- Screen: Manifest Web service Policy



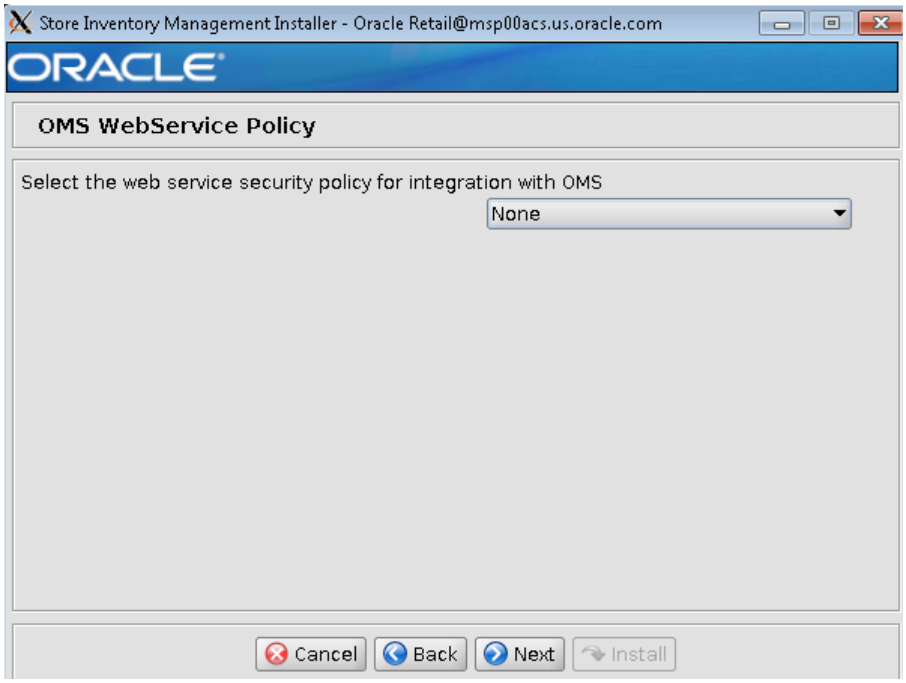
- **Screen: Manifest Integration Details**

  This screen will be displayed if the Configure Manifest for SIM option is checked on the Choose Apps to Integrate with SIM screen.



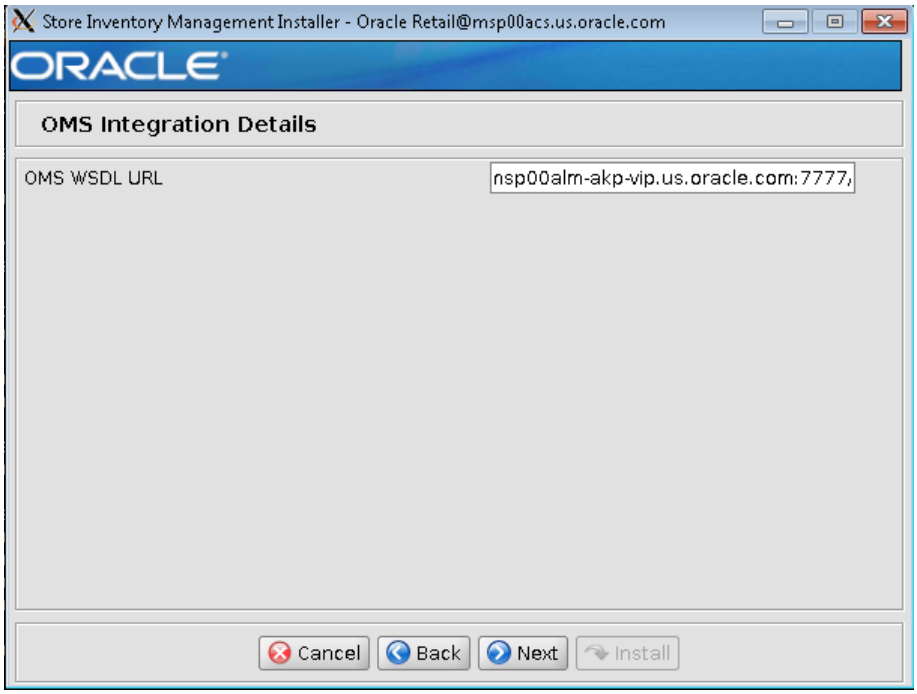
- **Screen: OMS Web service Policy**

  This screen will be displayed, if Configure OMS for SIM option is checked on the Choose Apps to Integrate with SIM screen.

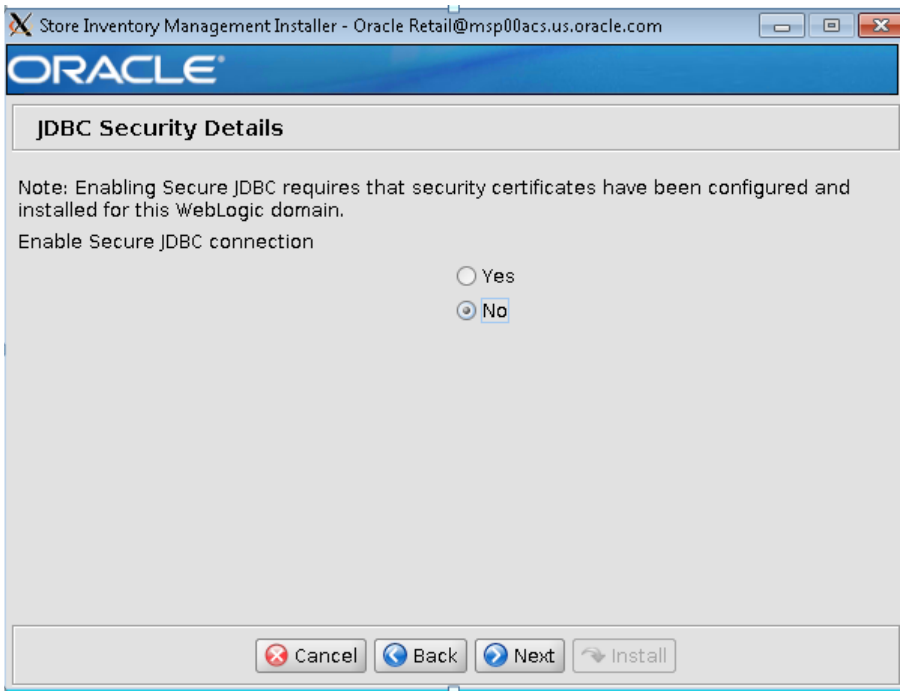


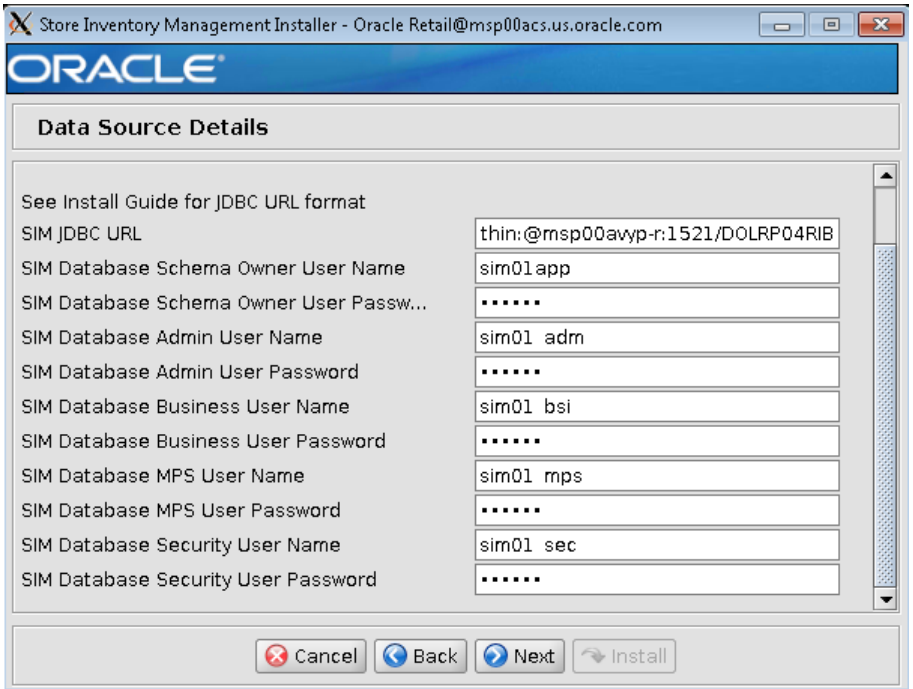
- **Screen: OMS Integration Details**

  This screen will be displayed if the Configure OMS for SIM option is checked on the Choose Apps to Integrate with SIM screen.

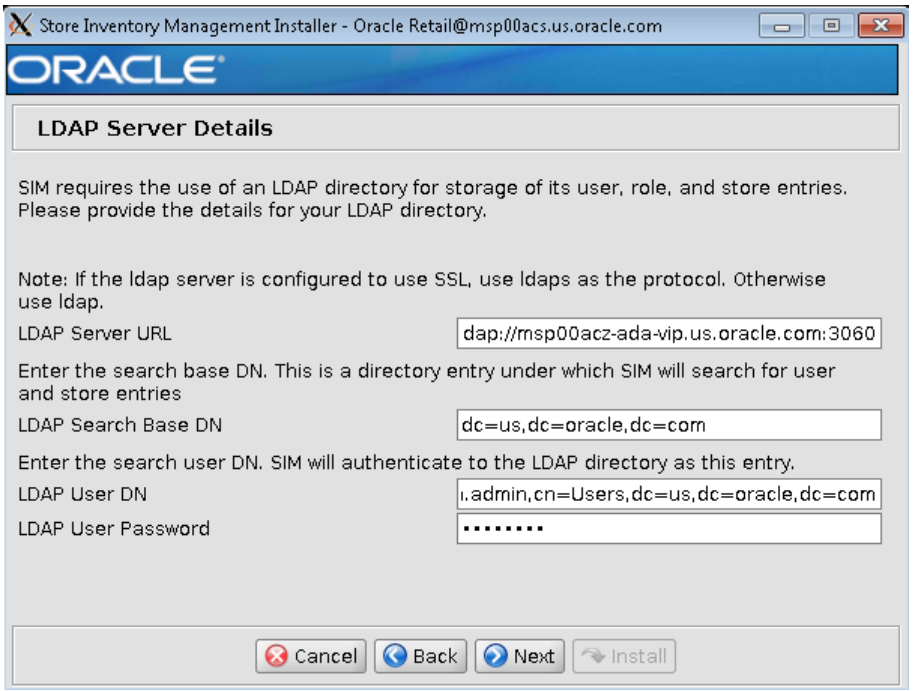


JDBC Security Details and Datasource details.

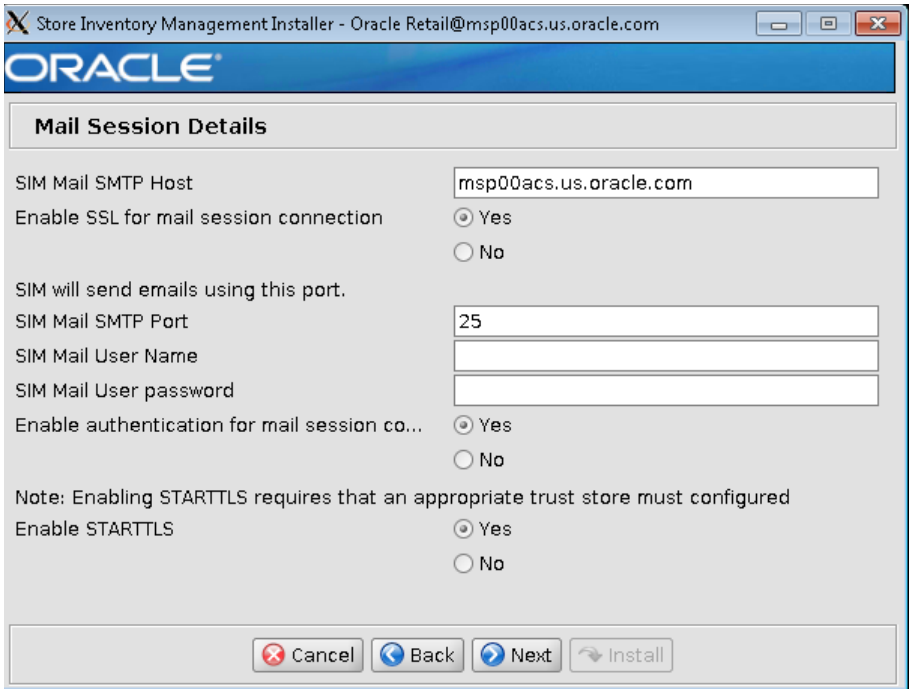




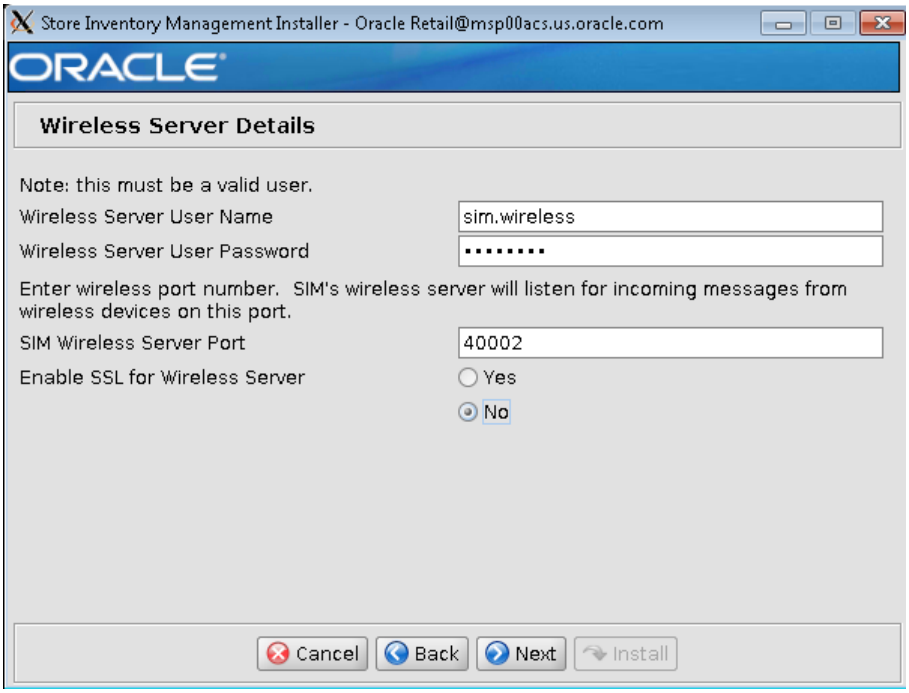
- Update LDAP Server Details



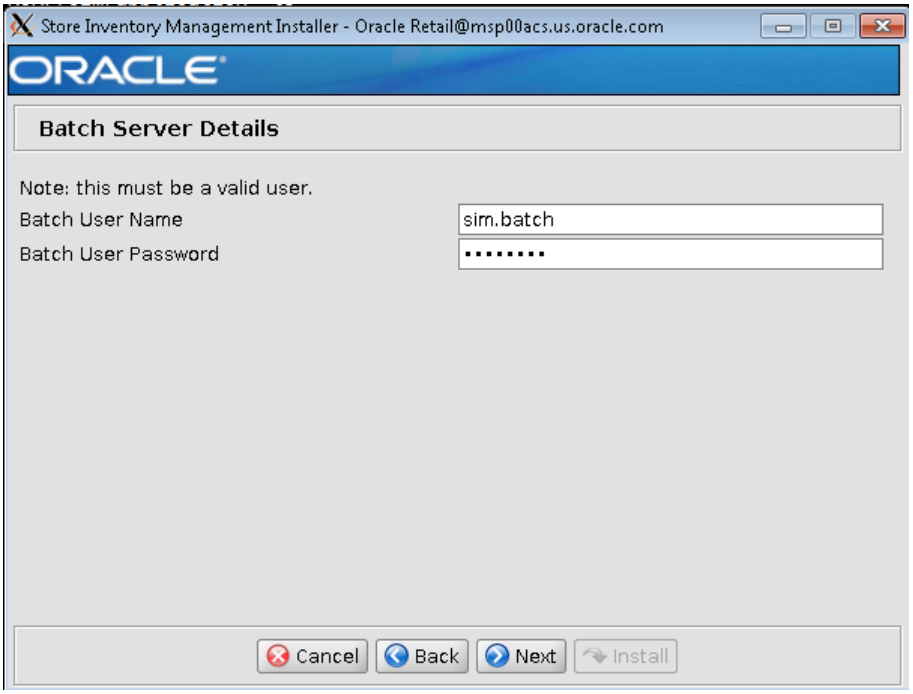
- Mail Session Details



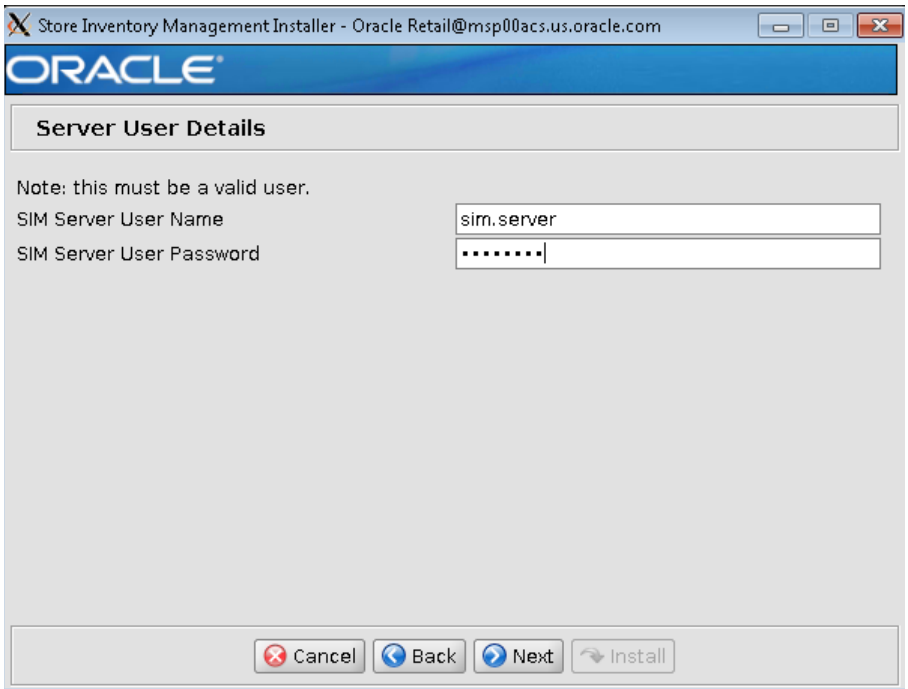
- Wireless Server Details



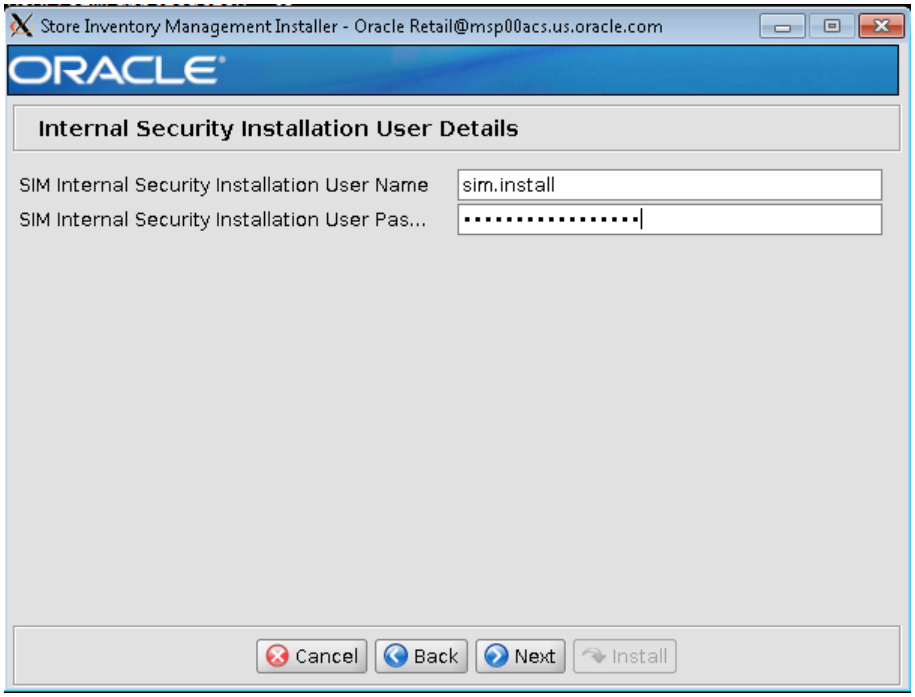
- Batch Server Details



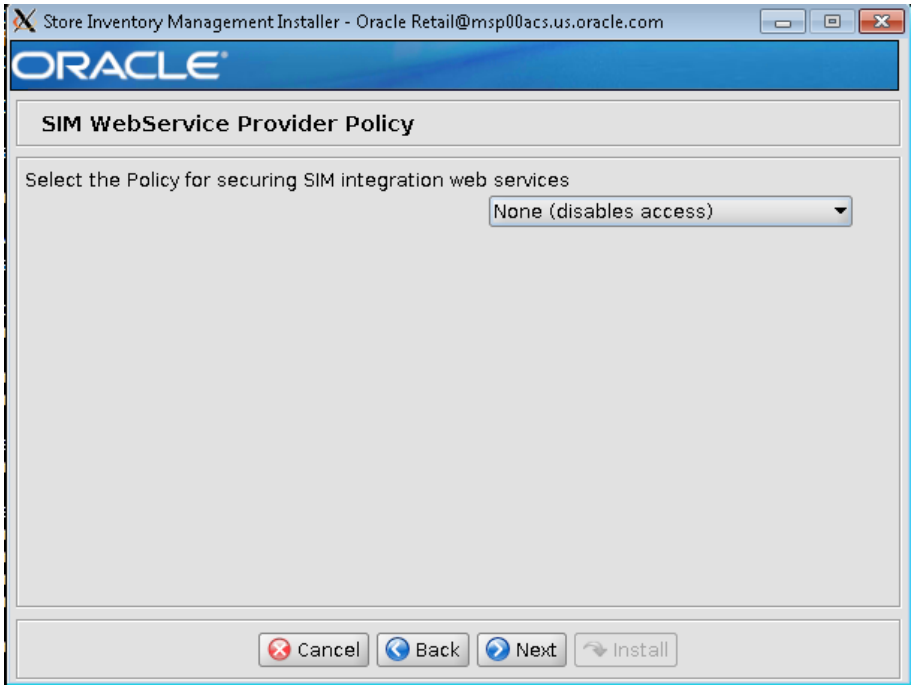
- Server User Details



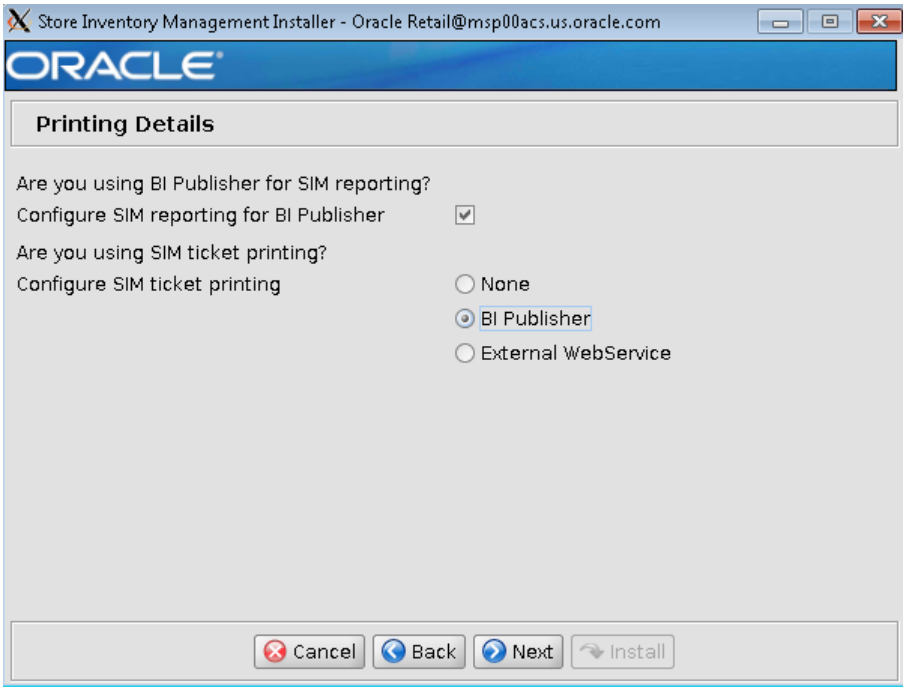
- Internal Security Installation User Details



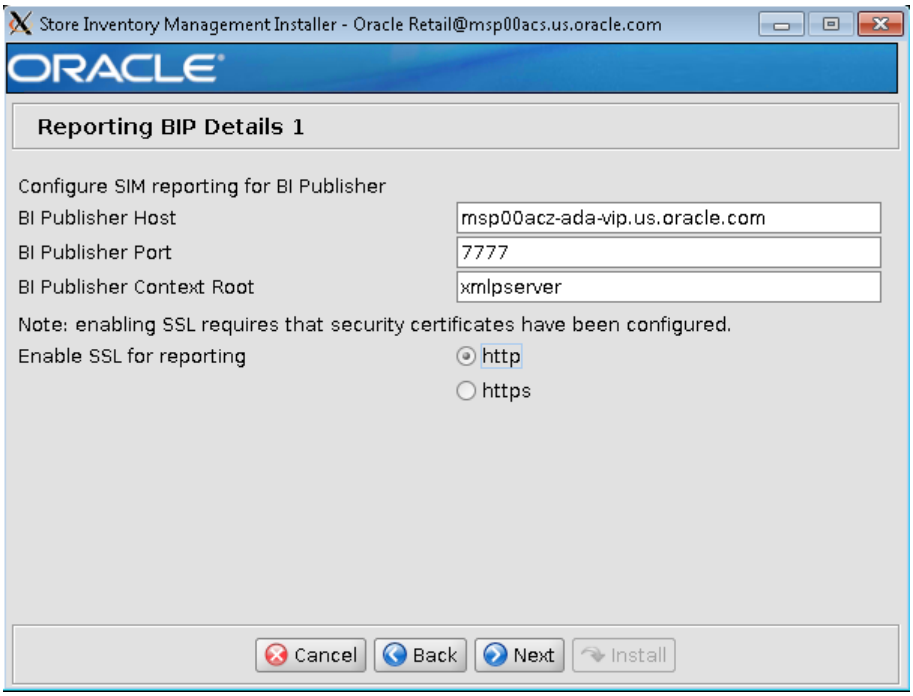
- SIM Webservice Provider Policy

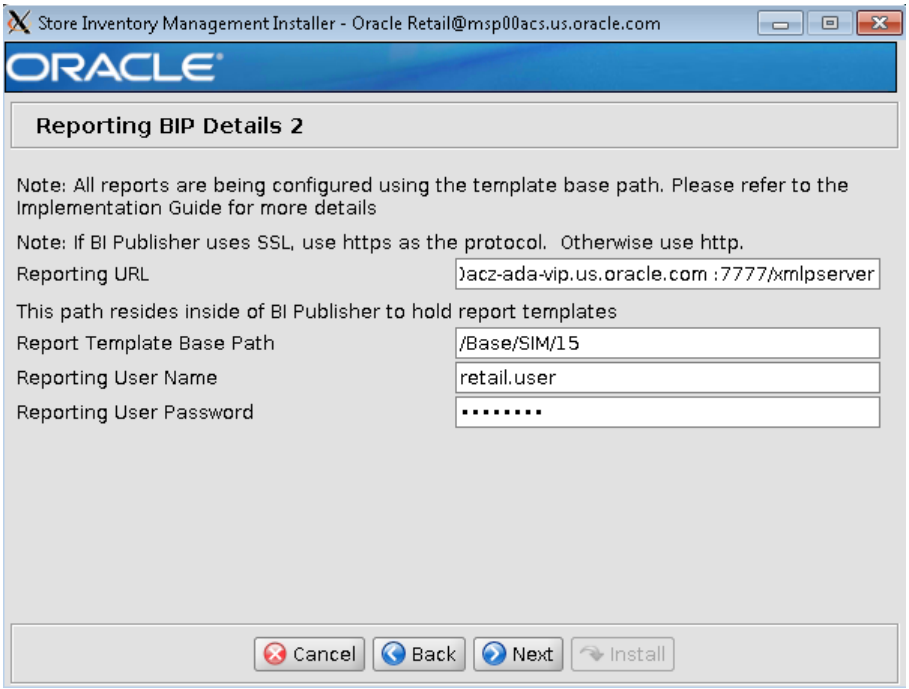


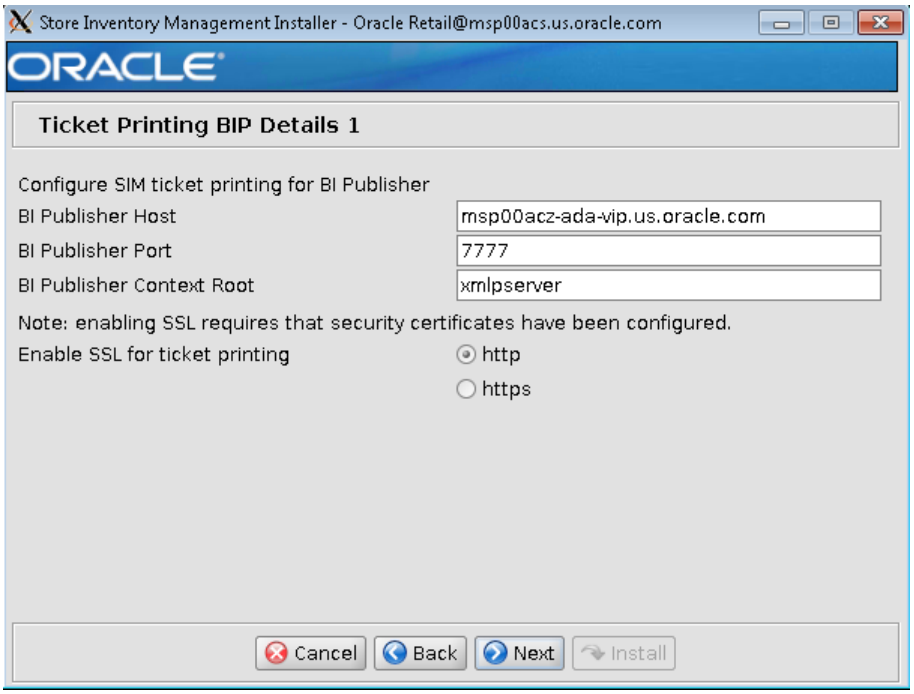
- Printing Details

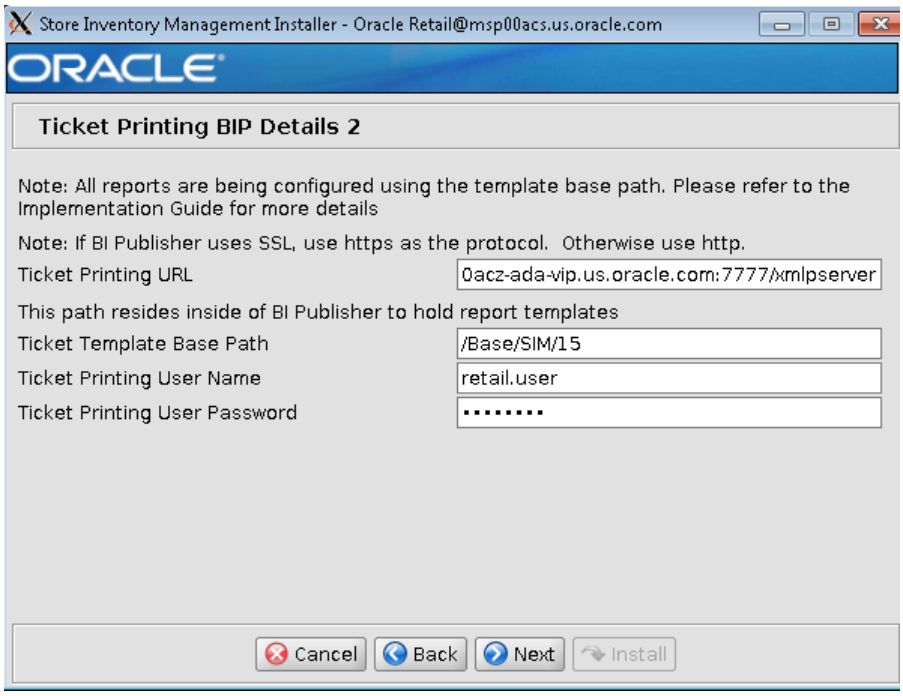


- OBIEE Details.



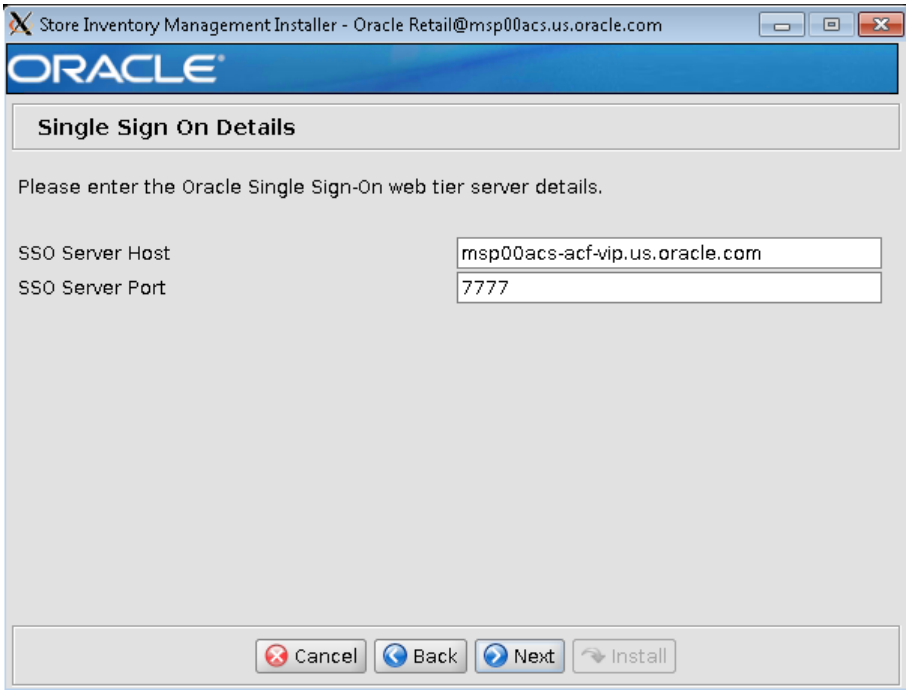

Store Inventory Management Installer - Oracle Retail@msp00acs.us.oracle.com
ORACLE
Reporting BIP Details 2
Note: All reports are being configured using the template base path. Please refer to the Implementation Guide for more details
Note: If BI Publisher uses SSL, use https as the protocol. Otherwise use http.
Reporting URL
)acz-ada-vip.us.oracle.com :7777/xmlpserver
This path resides inside of BI Publisher to hold report templates
Report Template Base Path
/Base/SIM/15
Reporting User Name
retail.user
Reporting User Password
Cancel
Back
Next
Install


Store Inventory Management Installer - Oracle Retail@msp00acs.us.oracle.com
ORACLE
Ticket Printing BIP Details 1
Configure SIM ticket printing for BI Publisher
BI Publisher Host
msp00acz-ada-vip.us.oracle.com
BI Publisher Port
7777
BI Publisher Context Root
xmlpserver
Note: enabling SSL requires that security certificates have been configured.
Enable SSL for ticket printing
http
https
Cancel
Back
Next
Install

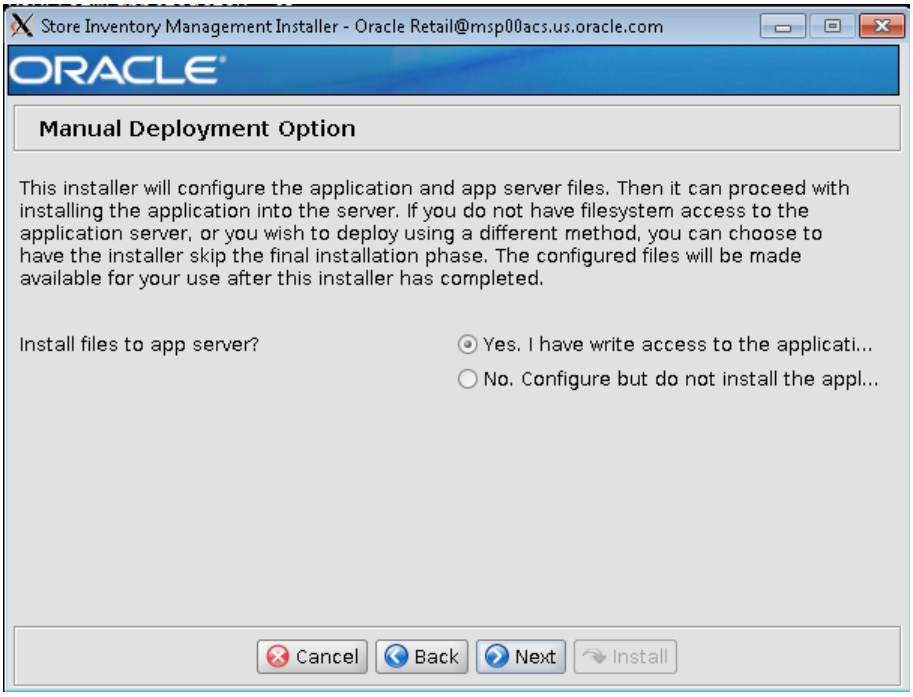

Store Inventory Management Installer - Oracle Retail@msp00acs.us.oracle.com
ORACLE
Ticket Printing BIP Details 2
Note: All reports are being configured using the template base path. Please refer to the Implementation Guide for more details
Note: If BI Publisher uses SSL, use https as the protocol. Otherwise use http.
Ticket Printing URL
0acz-ada-vip.us.oracle.com:7777/xmlpserver
This path resides inside of BI Publisher to hold report templates
Ticket Template Base Path
/Base/SIM/15
Ticket Printing User Name
retail.user
Ticket Printing User Password
Cancel
Back
Next
Install

- Enable SSO

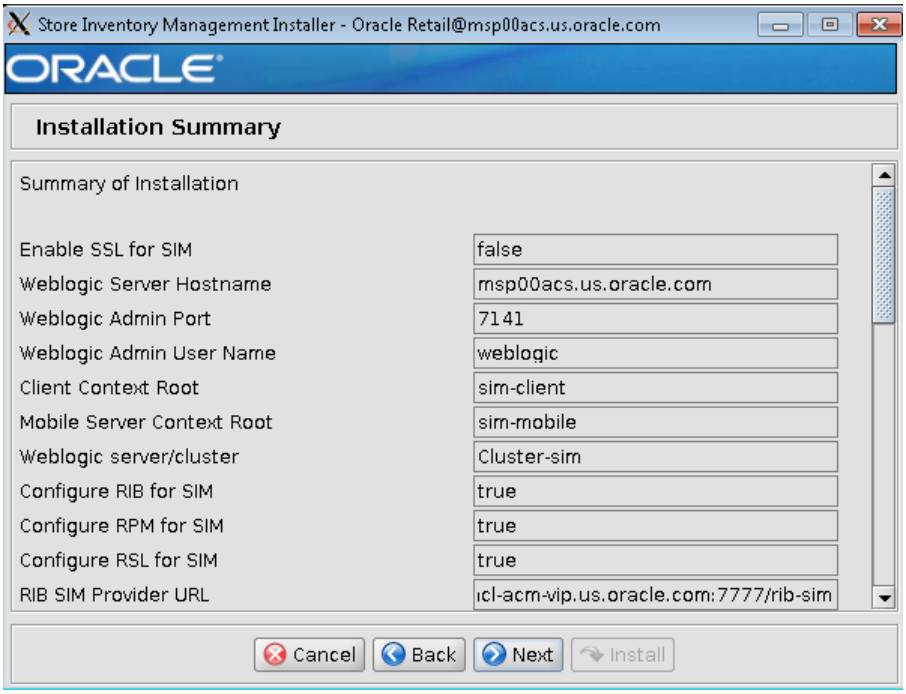
Store Inventory Management Installer - Oracle Retail@msp00acs.us.oracle.com
ORACLE
Enable SSO in SIM
Oracle Single Sign-On must be installed separately. You should only check the box below if you have already set up and configured Oracle SSO.
Use Oracle Single Sign On for user identification and authentication?
Enable Single Sign On in SIM?
Cancel
Back
Next
Install



- Update Manual Deployment.



- Installation Summary:



- Click **Next,** and Click **Finish** once it is done.

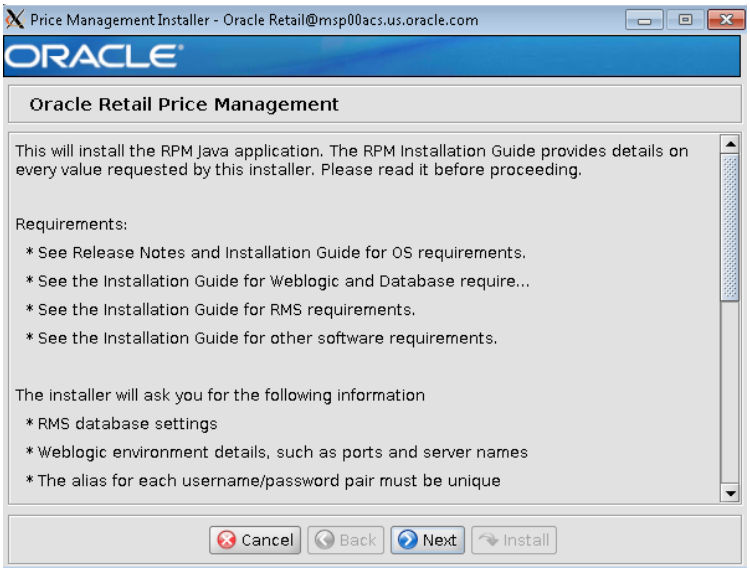
D

Appendix: RPM Application Installer Screens

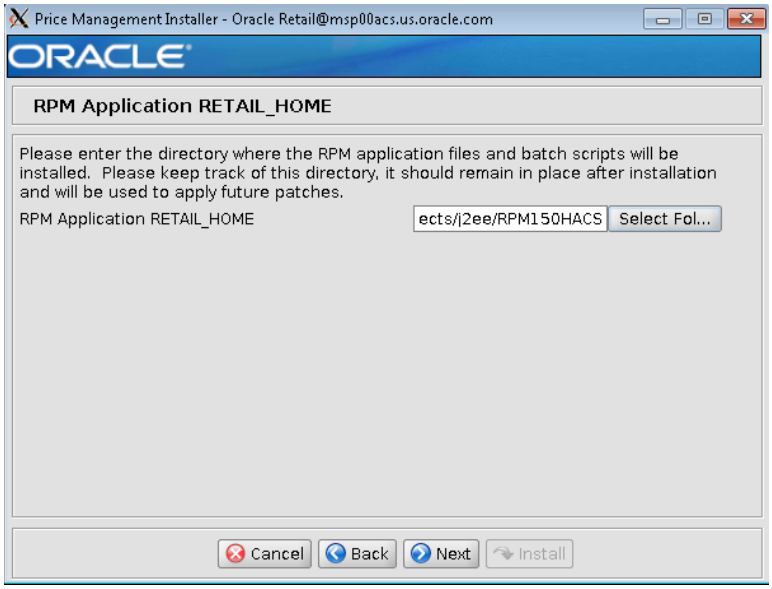
Below are the details of Application installer screens for RPM.

You need the following details about your environment for the installer to successfully deploy the RPM application. Depending on the options you select, you may not see some screens or fields.

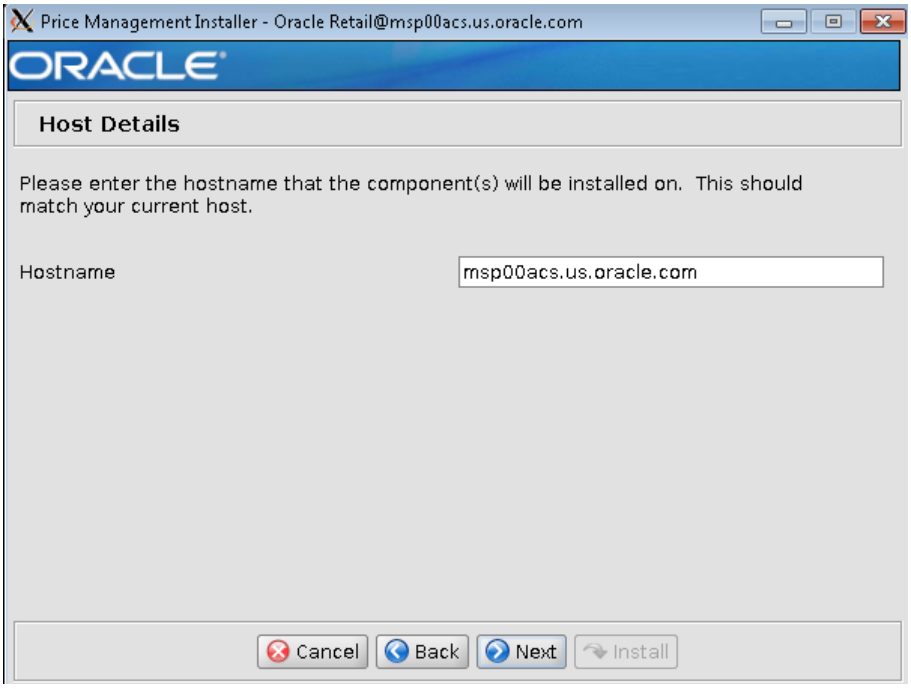
- Installation Introduction Screen



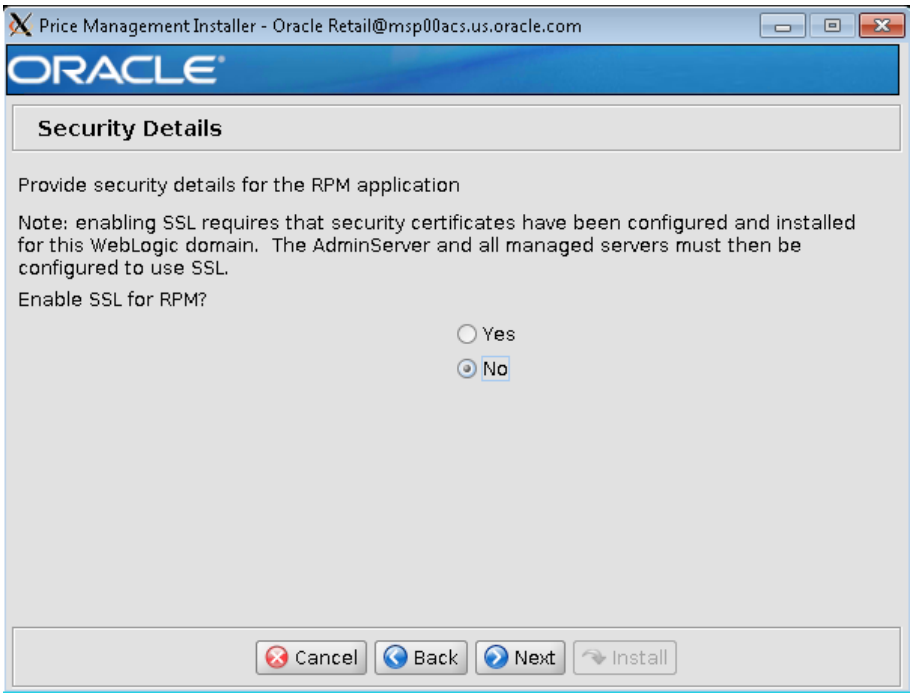
- RPM Application RETAIL HOME



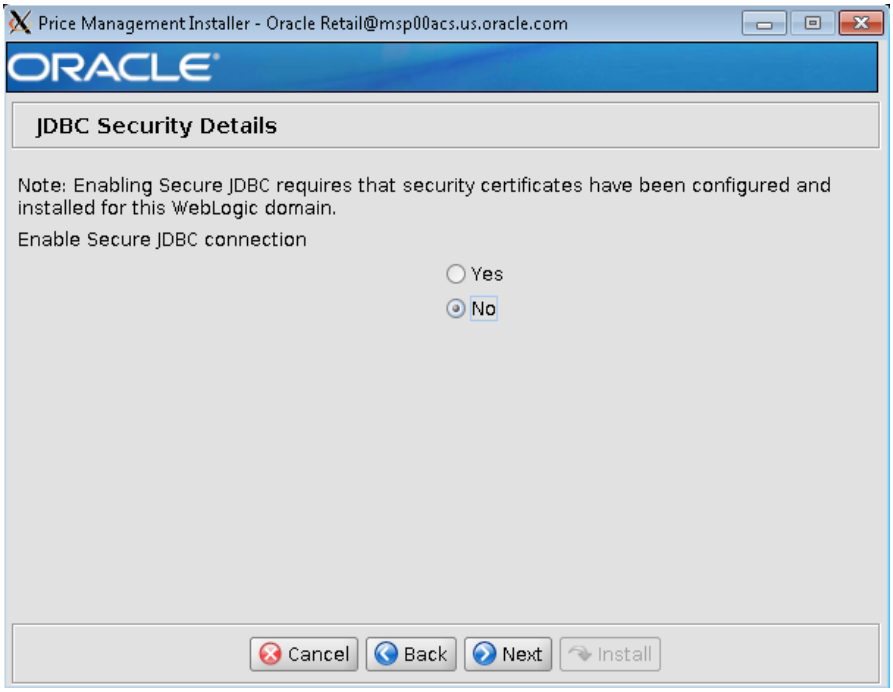
- Update Host Details.



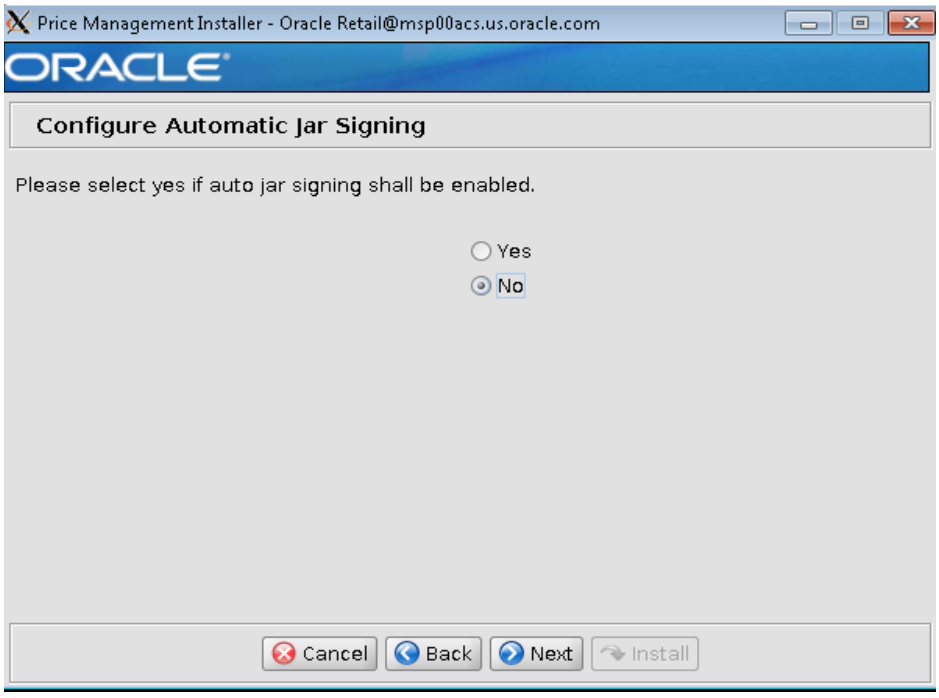
- Input the security details.



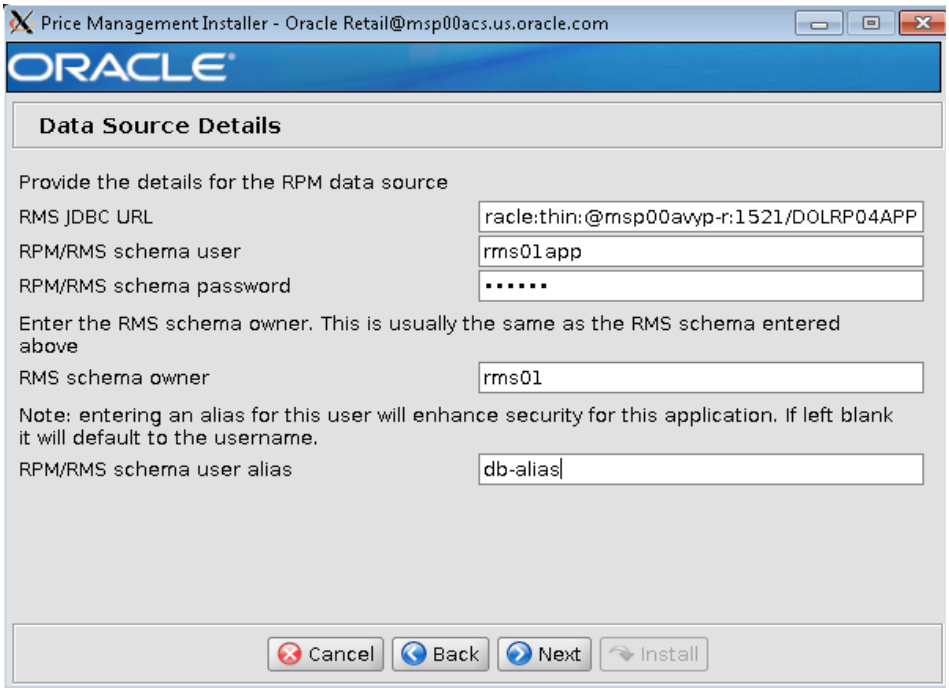
- Update JDBC security detail



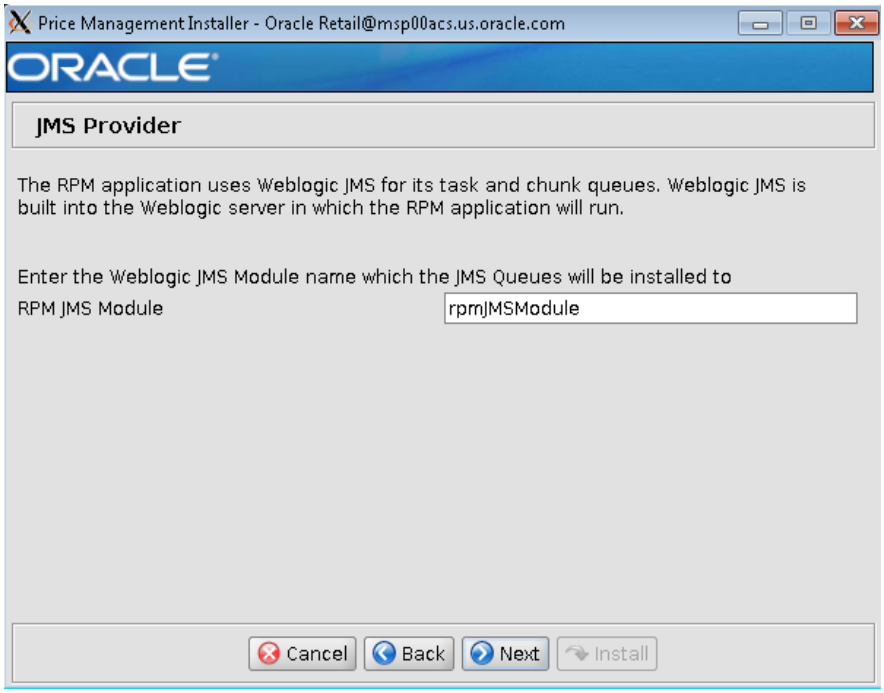
- Update Automatic Jar Signing



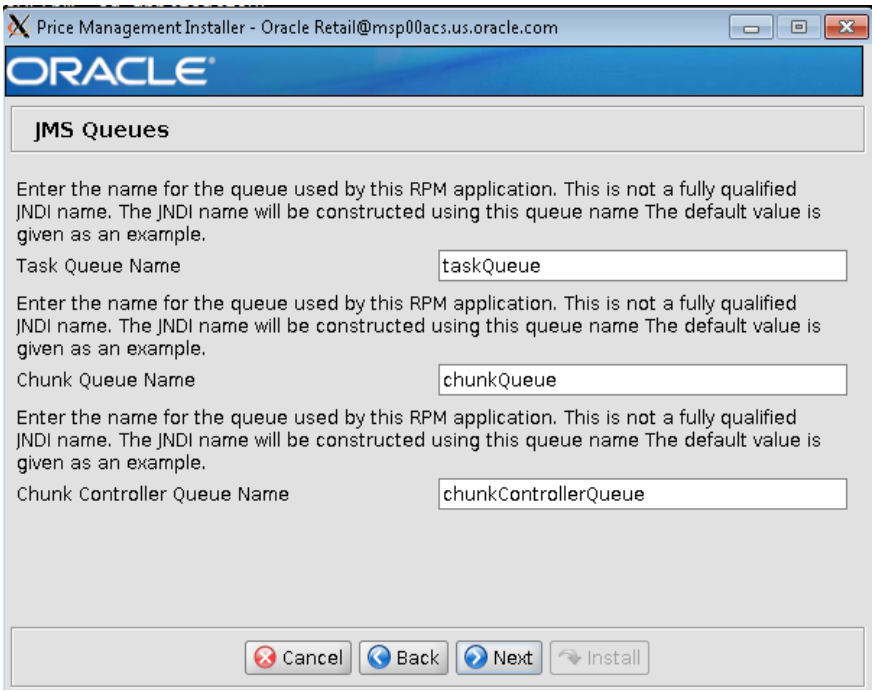
- Update Datasource details.



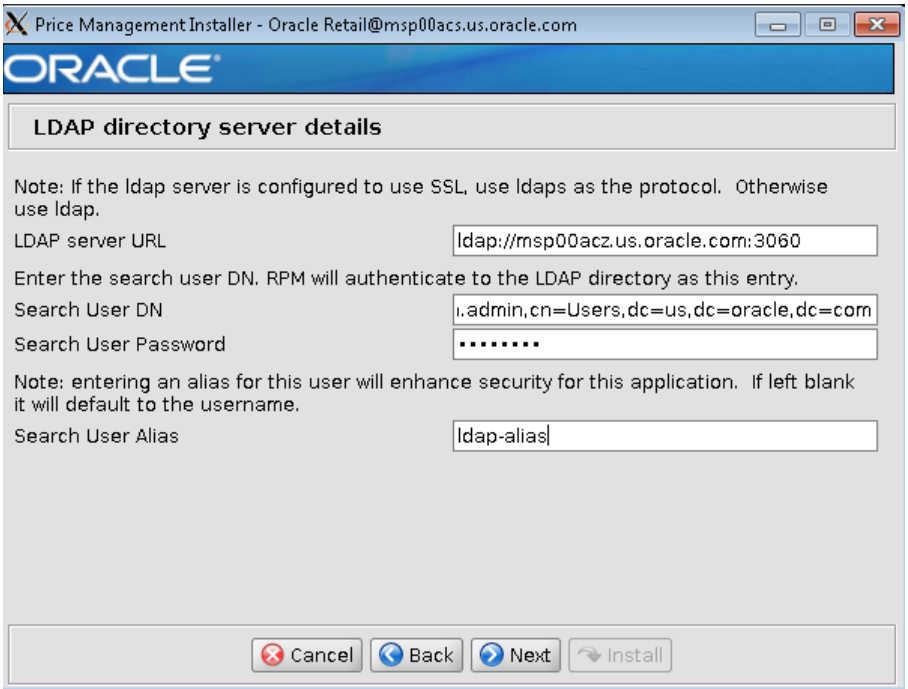
- Default JMS provider details

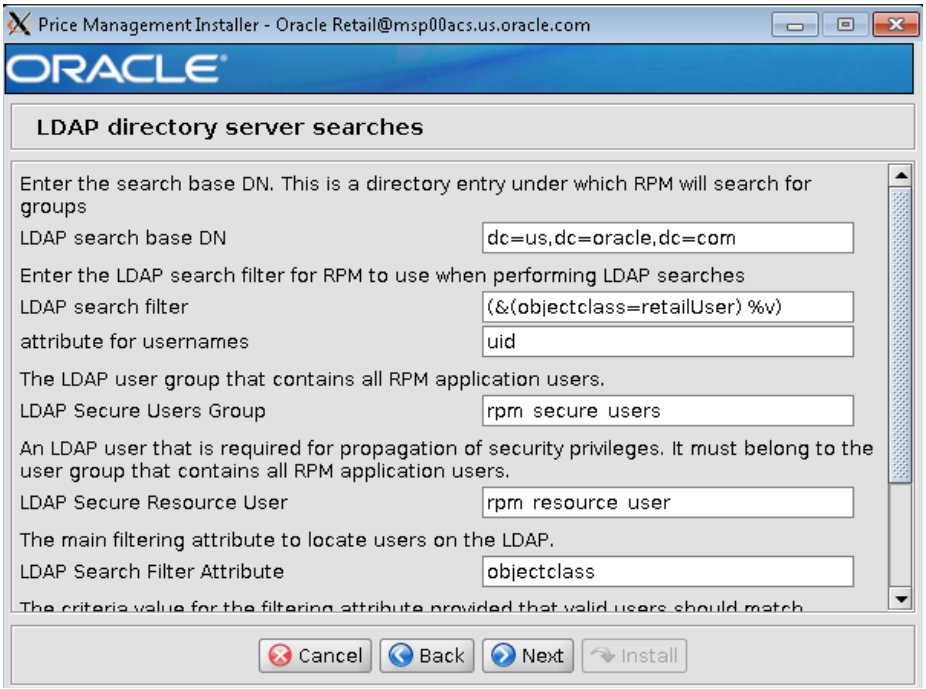


- Default JMS Queues details.

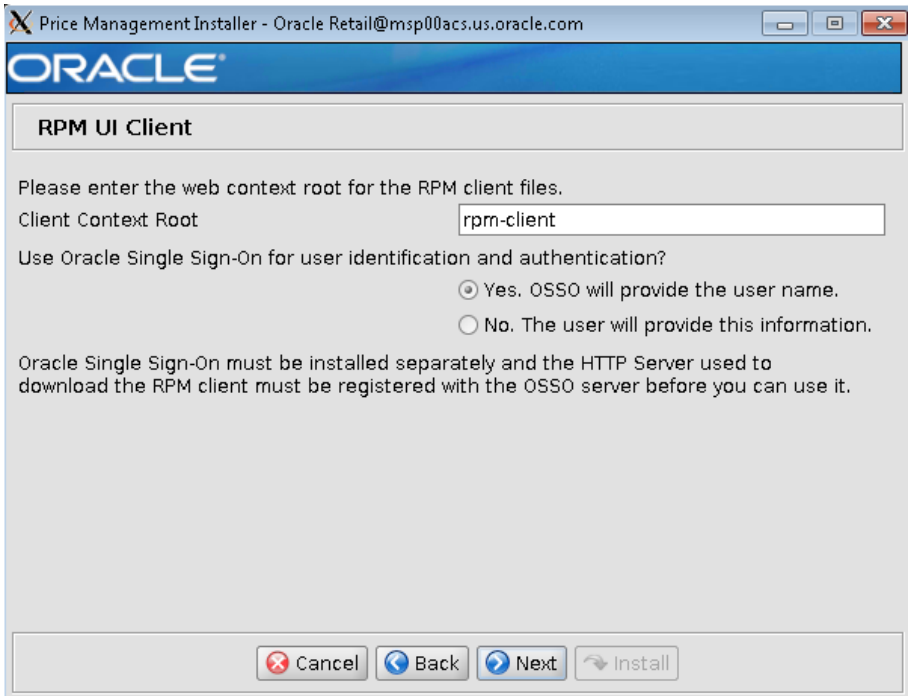


- Update LDAP Details.

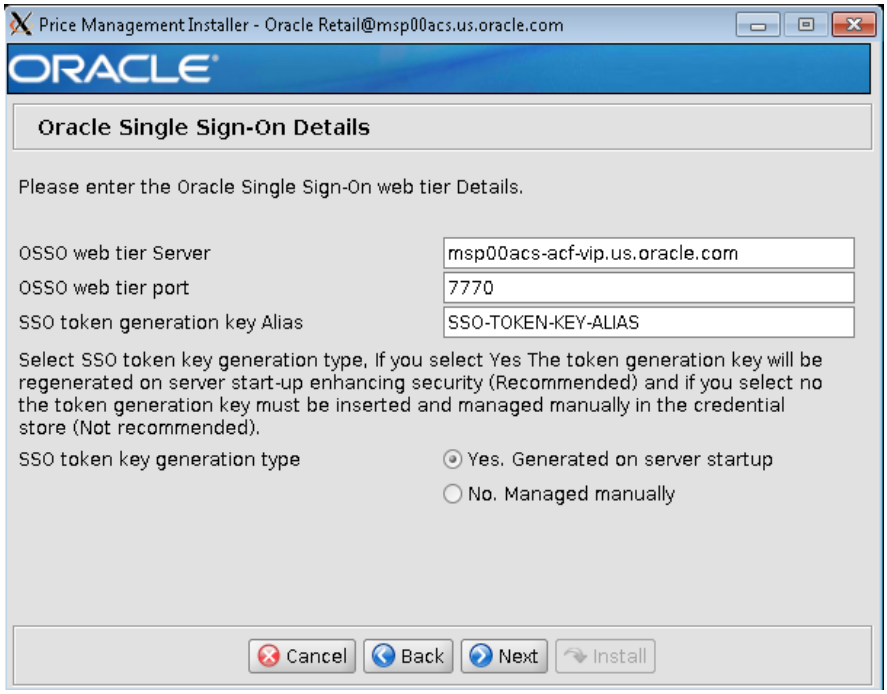




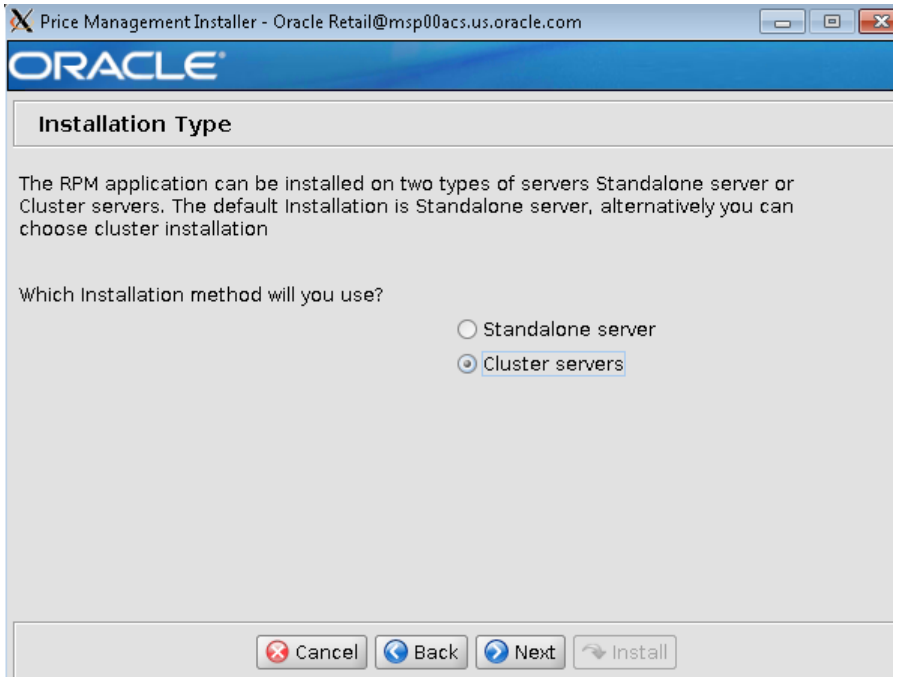
- Update RPM UI client



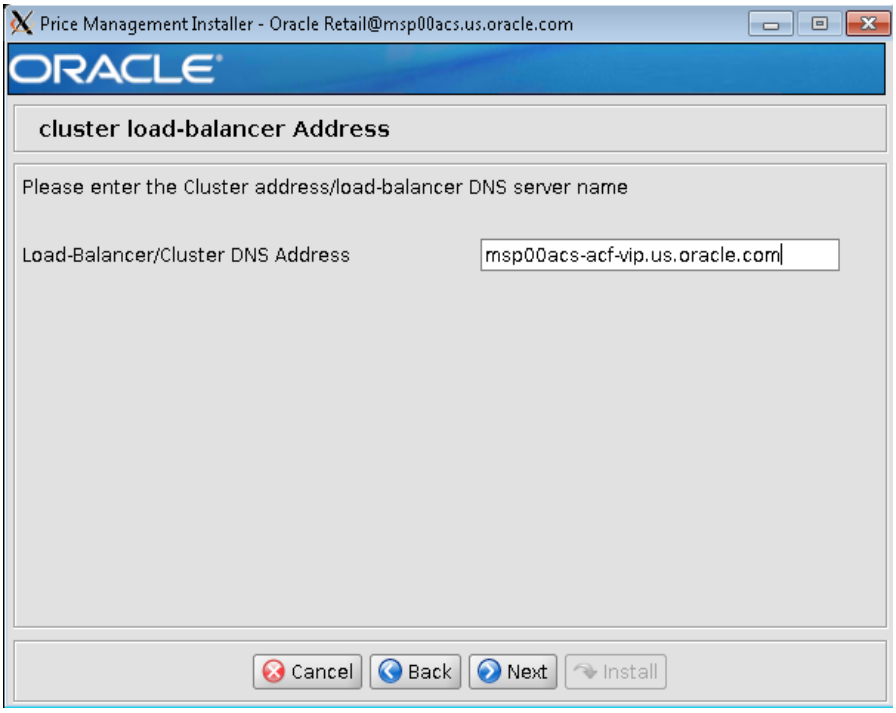
- Oracle SSO Details



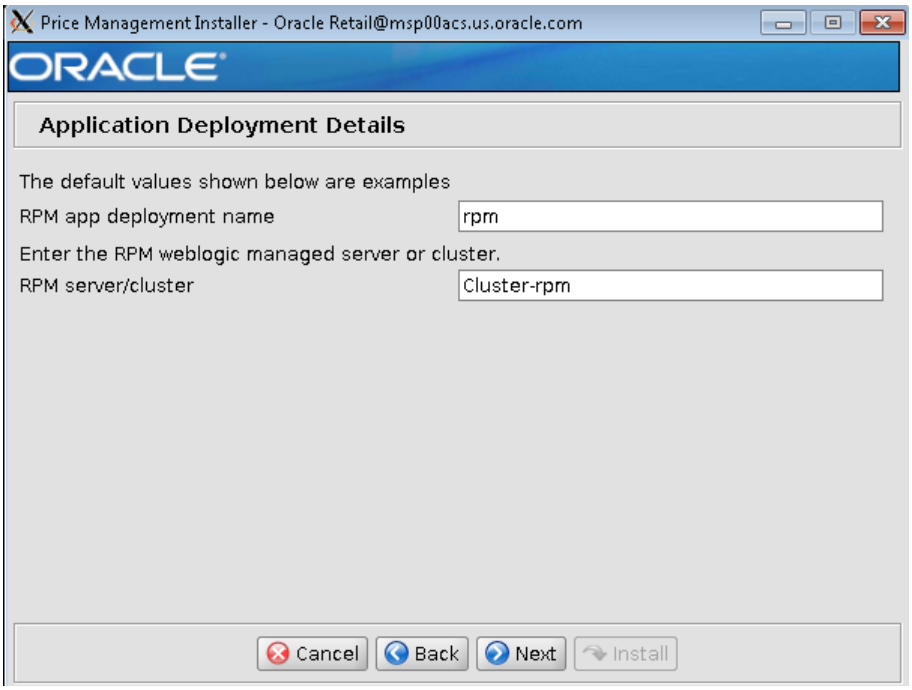
- Installation Type



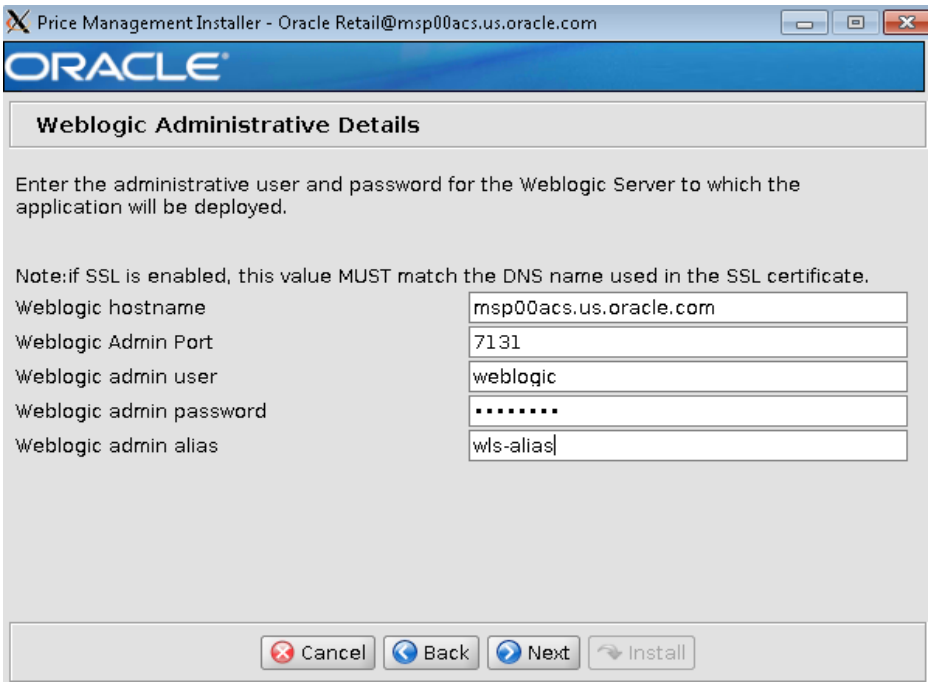
- Update Cluster Address



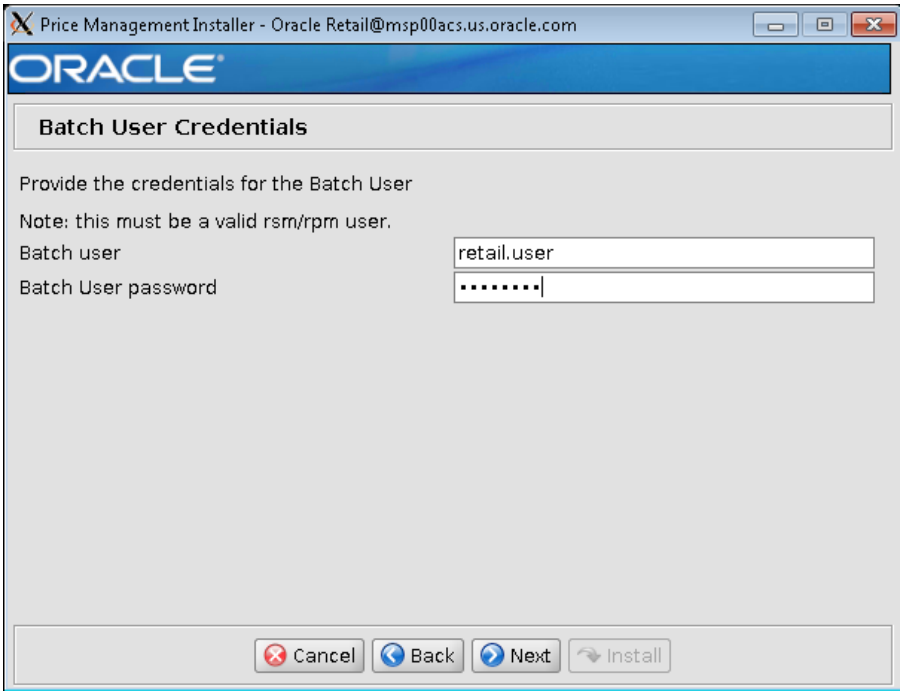
- Application Deployment Details



- Weblogic Administrative details

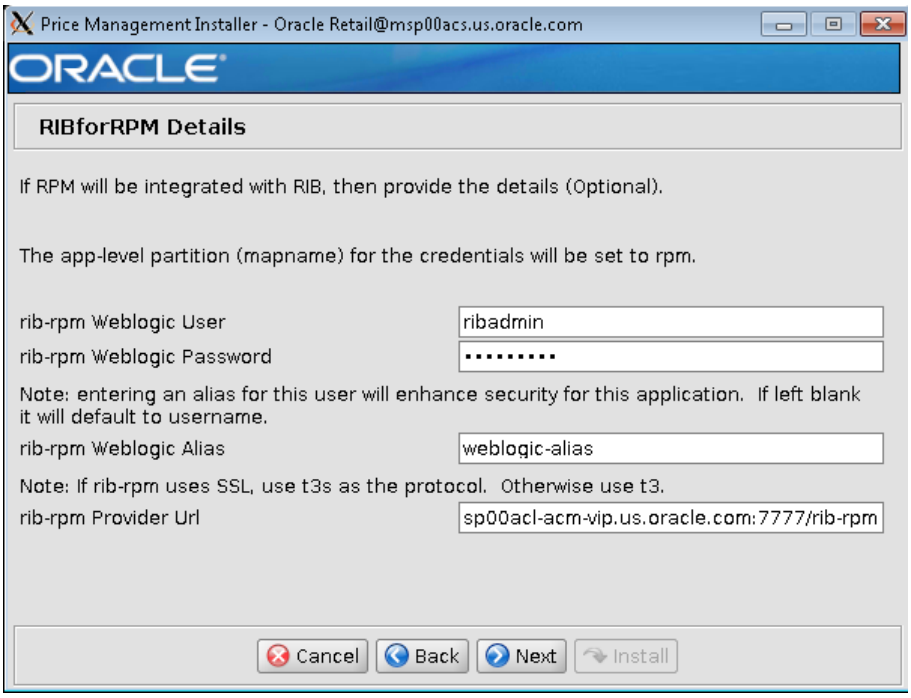


- Update Batch Credentials

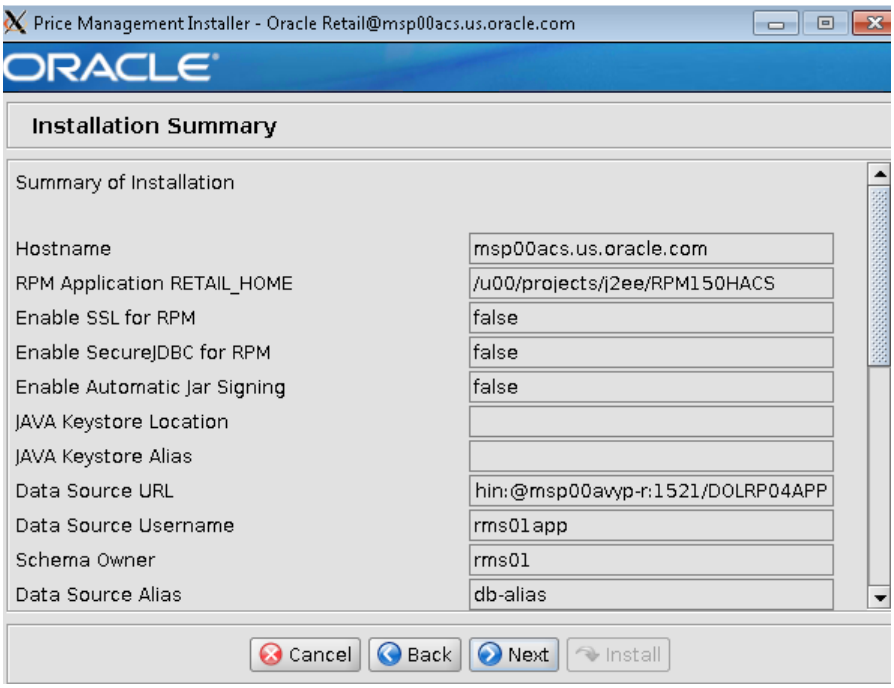


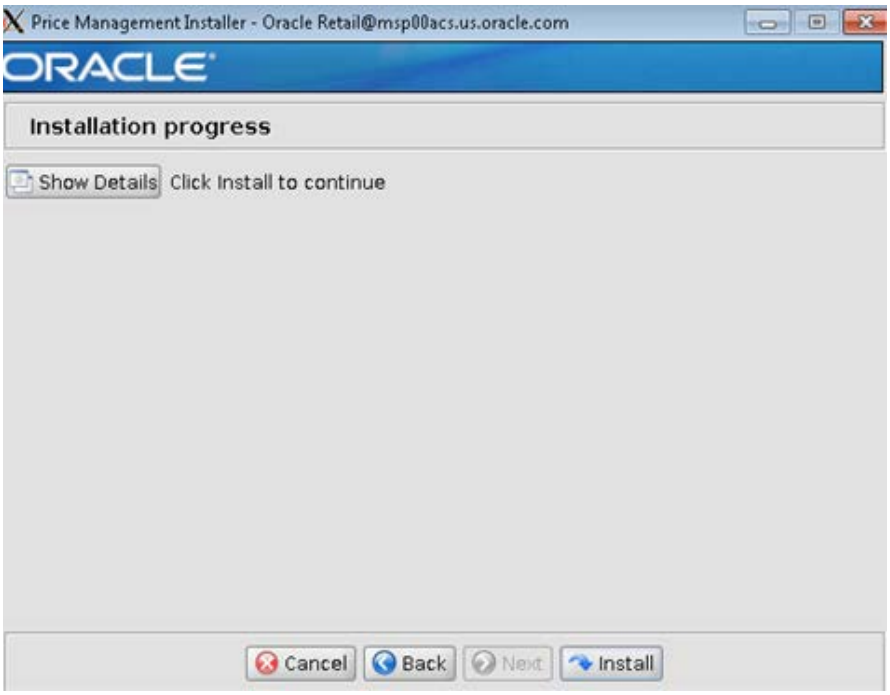
- Chose Apps to Integrate with RPM

- Update RIB for RPM details



- Installation Summary





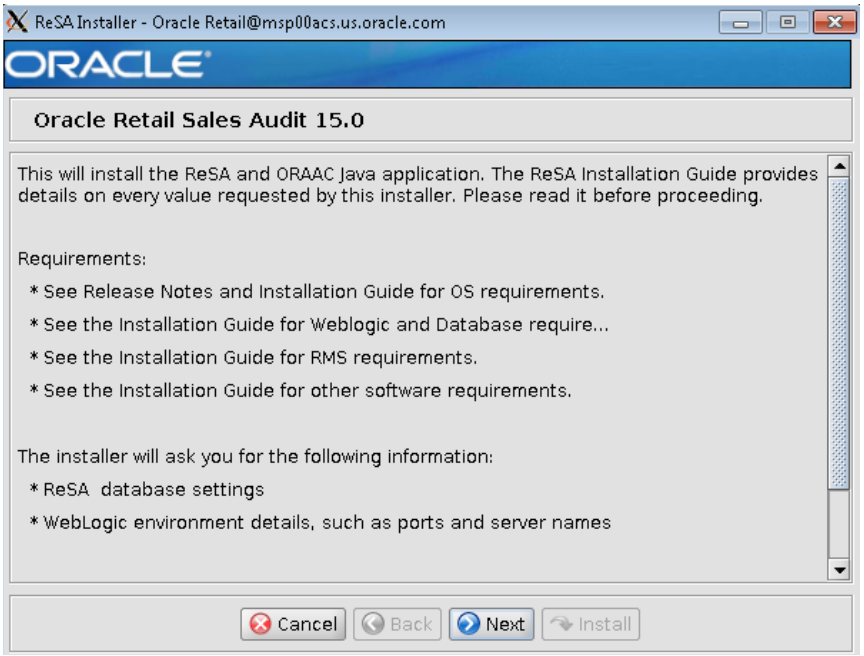
- Click **Install,** and once Installation is completed click **OK**.

E

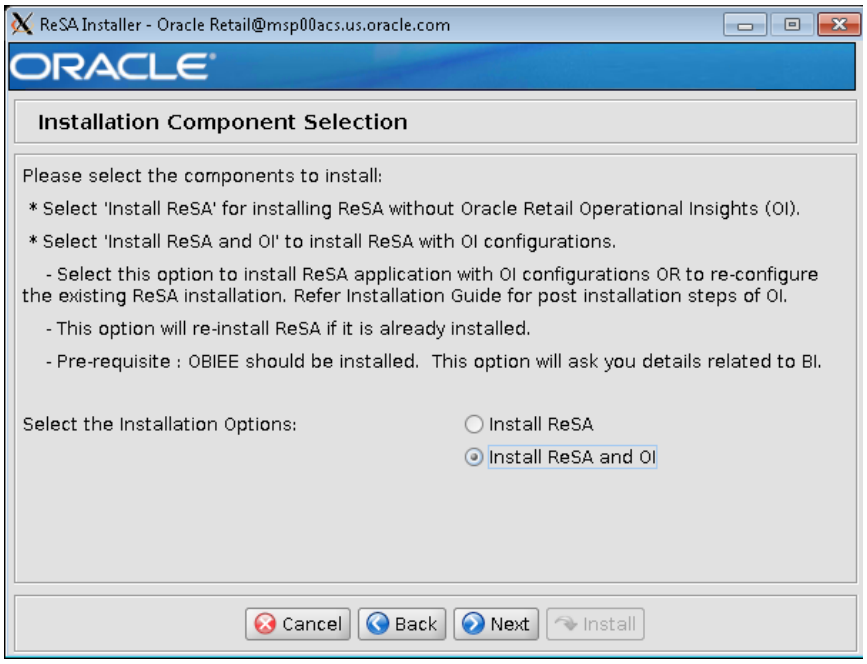
Appendix: ReSA Installer Screens

Below are the details of Application installer screens for ReSA.

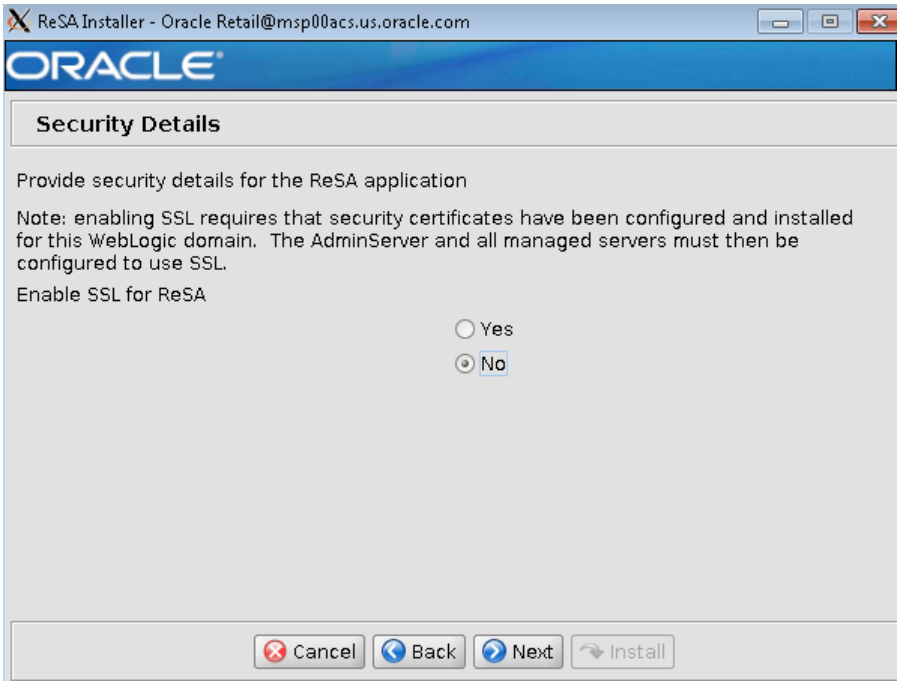
- ReSA Startup screen



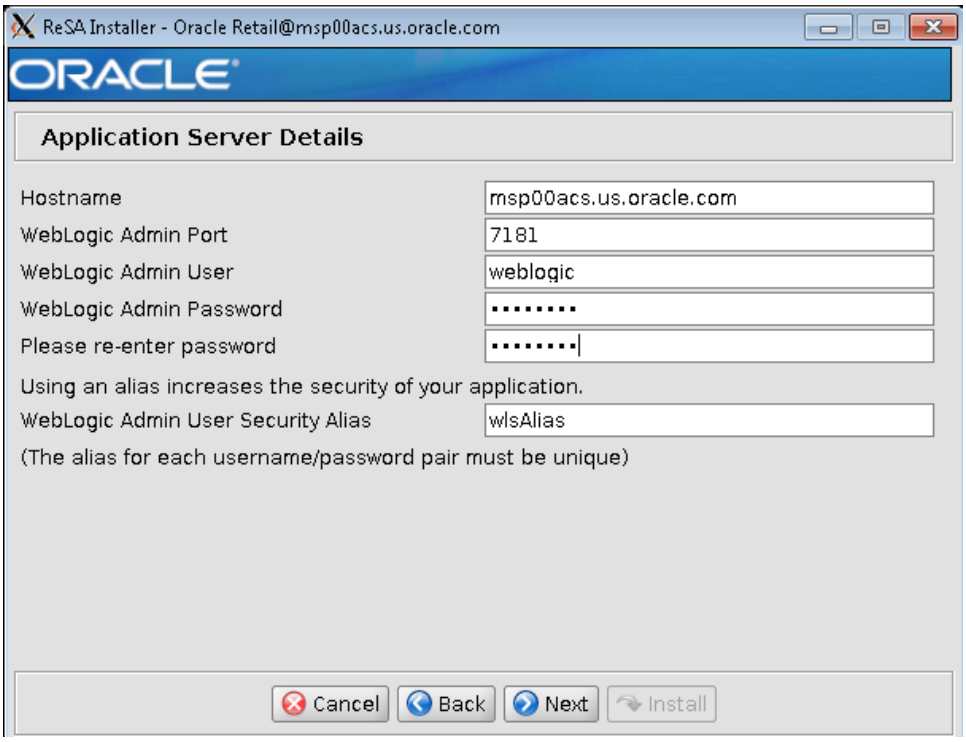
- Installation Component Selection



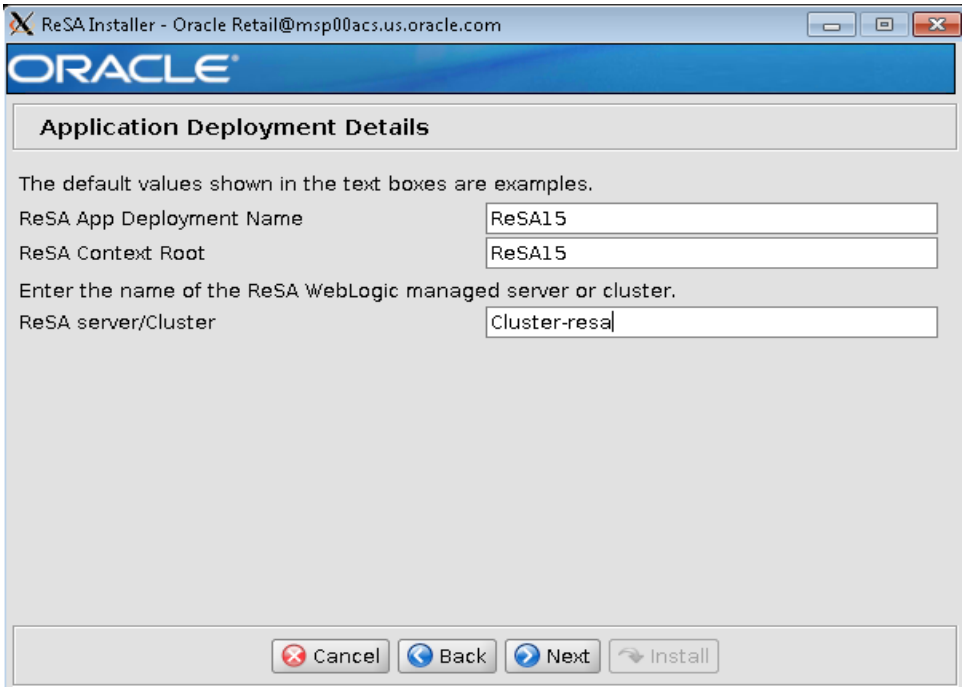
- Update Security details



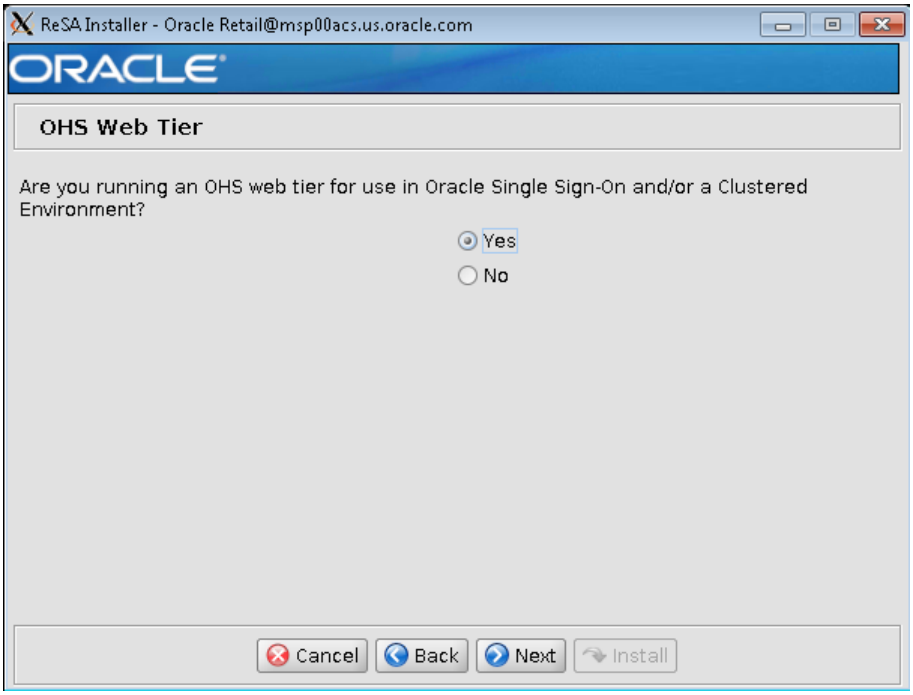
- Update Application Server details

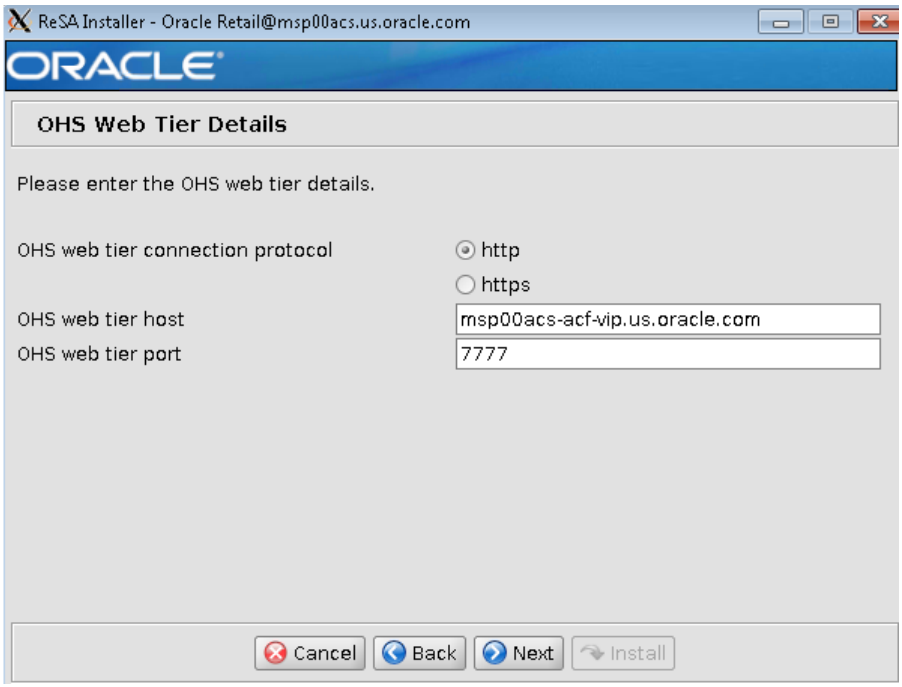


- Update Deployment details

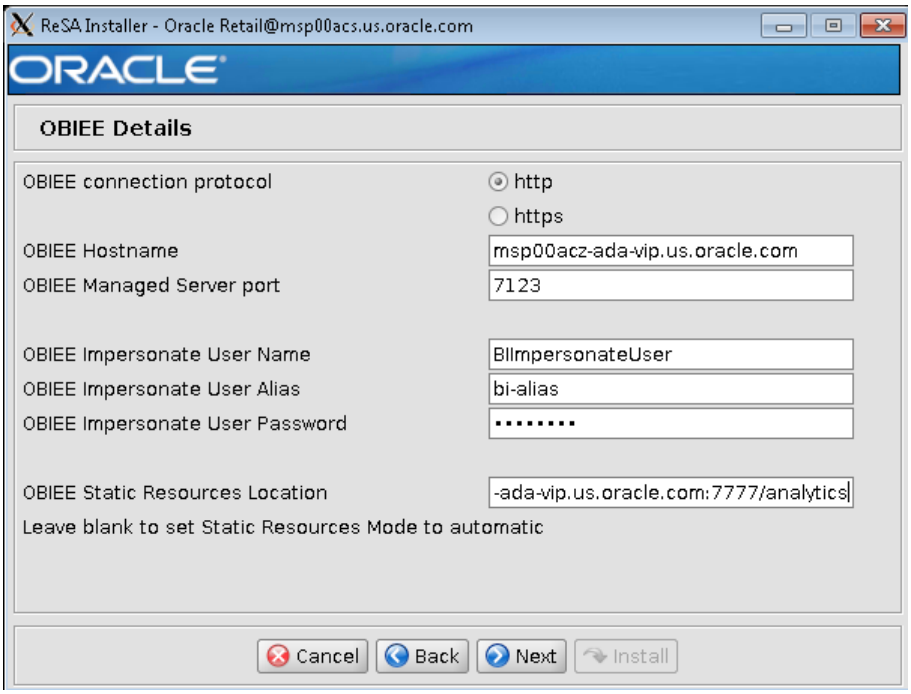

ReSA Installer - Oracle Retail@msp00acs.us.oracle.com
ORACLE
Application Deployment Details
The default values shown in the text boxes are examples.
ReSA App Deployment Name
ReSA15
ReSA Context Root
ReSA15
Enter the name of the ReSA WebLogic managed server or cluster.
ReSA server/Cluster
Cluster-resa
Cancel
Back
Next
Install

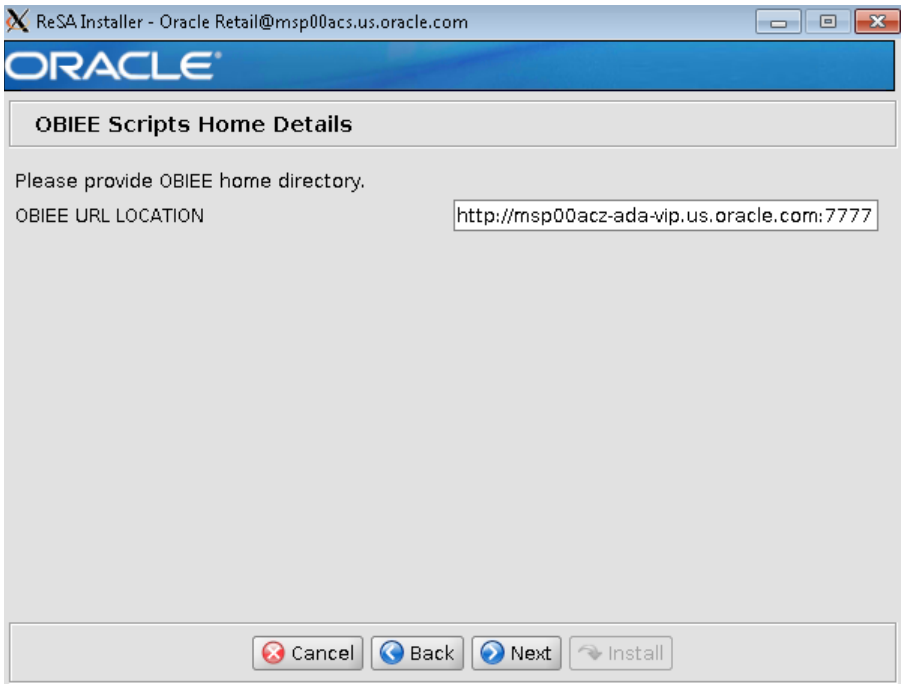
- OHS details

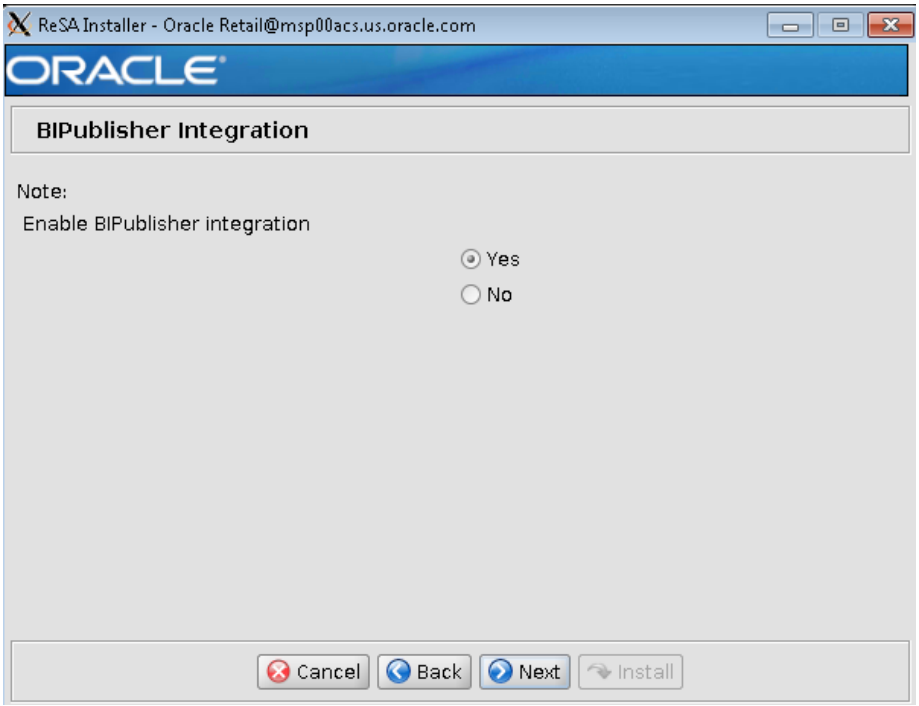

ReSA Installer - Oracle Retail@msp00acs.us.oracle.com
ORACLE
OHS Web Tier
Are you running an OHS web tier for use in Oracle Single Sign-On and/or a Clustered Environment?
Yes
No
Cancel
Back
Next
Install



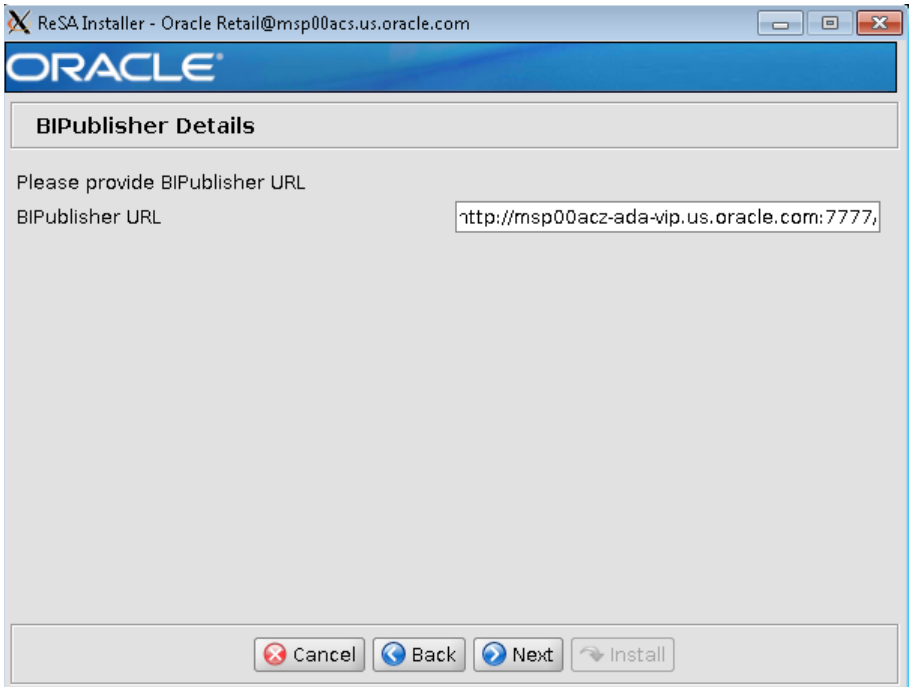
- OBIEE Details



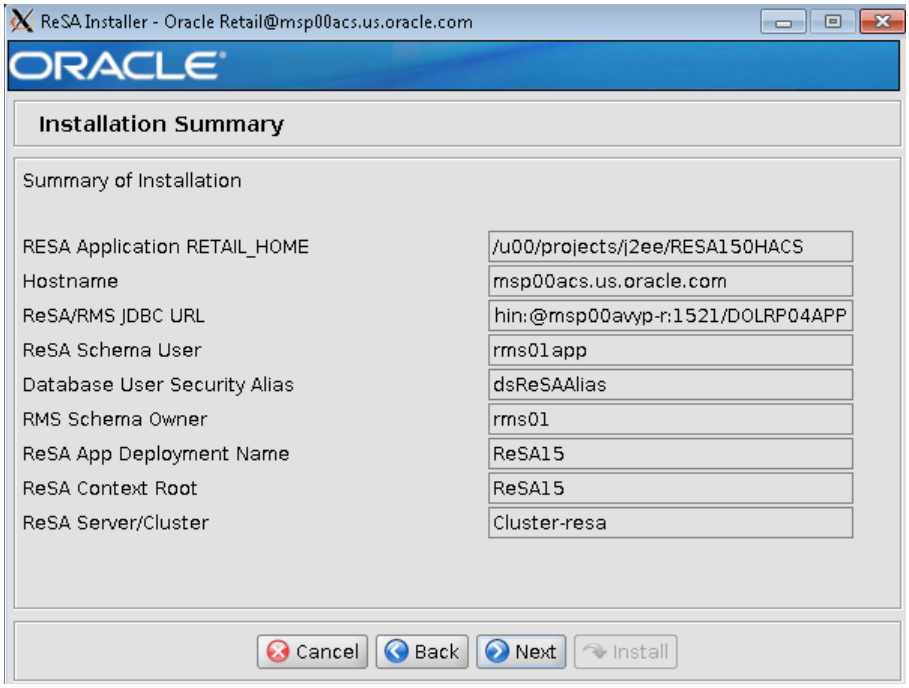

ReSA Installer - Oracle Retail@msp00acs.us.oracle.com
ORACLE
OBIEE Scripts Home Details
Please provide OBIEE home directory.
OBIEE URL LOCATION
http://msp00acz-ada-vip.us.oracle.com:7777
Cancel
Back
Next
Install

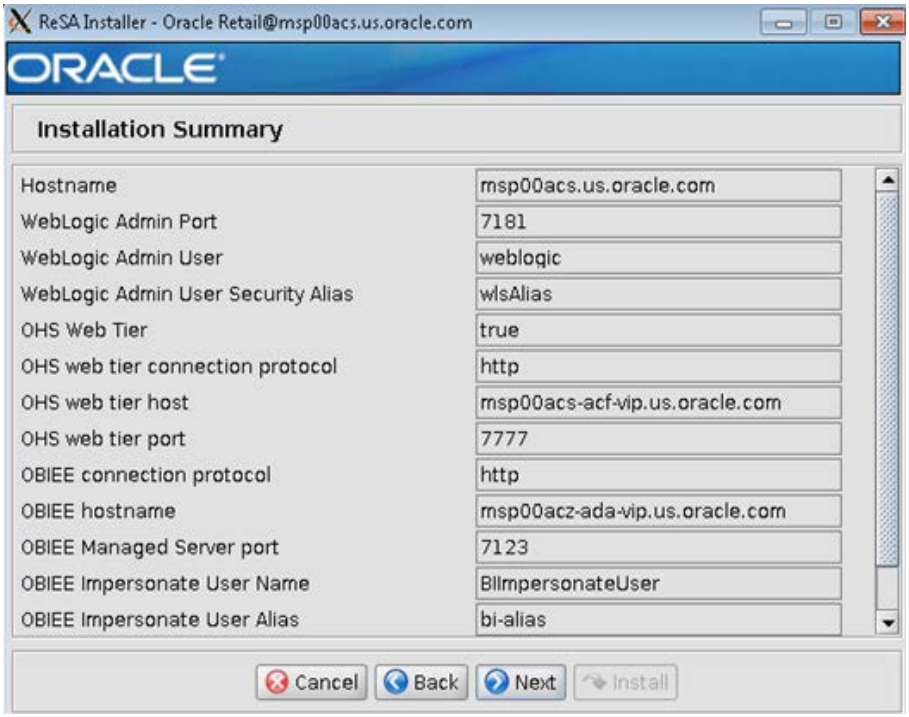

ReSA Installer - Oracle Retail@msp00acs.us.oracle.com
ORACLE
BIPublisher Integration
Note:
Enable BIPublisher integration
Yes
No
Cancel
Back
Next
Install

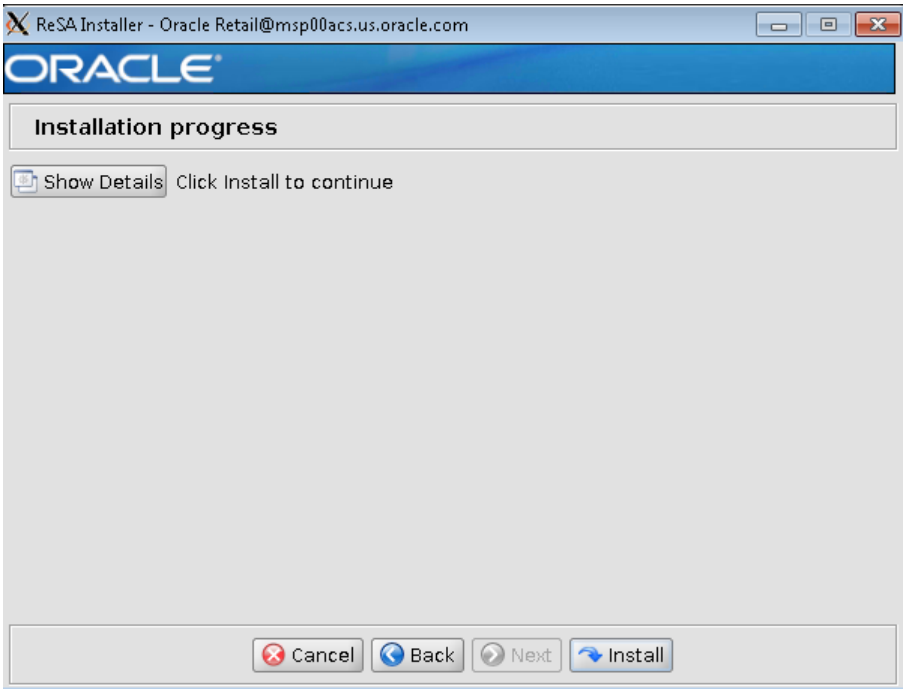
- Bipublisher Details



- Installation Summary







- Click **Install,** and once it is completed Click **OK** and Launch application.

F

Appendix: ant.install.properties - ReIM

Below is the sample of ant.install.properties file generated during installation of ReIM

Ant Installer - properties auto generated on Tue\ May\ 24\ 20:50:36\ PDT\ 2016

```
basedir = /scratch/u00/webadmin/media/REIM/CDROM/reim/application/.
ant.install.config.version = 1.0
## Properties from Page:Introduction
input.datasource.keyStore.user =
input.datasource.keyStoreType =
input.datasource.trustStore.user =
input.datasource.trustStoreType =

## Properties from Page:SelectComponent
input.enable.obiee.integration = true
## Properties from Page:init-prop
input.obiee.protocol = http
input.obiee.host = msp00acz.us.oracle.com
input.obiee.managed.server.port = 7333
input.obiee.sso.port = 7777
input.obiee.impersonate.user = BIImpersonateUser
input.obiee.impersonate.user.alias = bi-alias
input.obiee.static.resources.location = http://msp00acz-ada-
vip.us.oracle.com:7777/analytics

## Properties from Page:ReIMAPPRETAILHOME

input.retail.home = /u00/projects/j2ee/reim150HACS

## Properties from Page:HostDetails

input.host = msp00acs.us.oracle.com

## Properties from Page:Security

input.enable.ssl = false

## Properties from Page:SecureJDBC

input.enable.securejdbc = false

## Properties from Page:DataSourceDetails
input.datasource.url = jdbc:oracle:thin:@msp00avyp-r:1521/DOLRP04APP
input.datasource.username = RMS01APP
input.schema.owner = RMS01
input.datasource.alias = DB-ALIAS

## Properties from Page:ValidateDataSource

## Properties from Page:AppDeploymentDetails
input.app.name = reim15
input.wls.target = Cluster-reim

## Properties from Page:WLSAdminUser
```

```
input.appserver.host = msp00acs.us.oracle.com
input.appserver.admin.port = 7091
input.admin.user = weblogic
input.admin.alias = wls-alias

## Properties from Page:WWAV Details
input.webservice.account.validation =
input.enable.webservice.account.validation.credentials = false

## Properties from Page:initWWAVDrillFwd
input.webservice.drill.forward.alias =
input.webservice.drill.forward.username =
input.webservice.drill.forward =
input.webservice.account.validation =
input.webservice.account.validation.username =
input.webservice.account.validation.alias =

## Properties from Page:Drill Forward Details
input.webservice.drill.forward =
input.enable.webservice.drill.forward.credentials = false

## Properties from Page:WWAV Credentials Skip
input.webservice.account.validation.username =
input.webservice.account.validation.alias =

## Properties from Page:Batch User Credentials
input.batch.user = ADMIN
input.batch.user.alias = BATCH-ALIAS

## Properties from Page:OHSWebTier
input.use.ohs.web.tier = true

## Properties from Page:OHSWebTierDetails
input.ohs.web.tier.protocol = http
input.ohs.web.tier.host = msp00acs-acf-vip.us.oracle.com
input.ohs.web.tier.port = 7777

## Properties from Page:OBIEEDetails
input.obiee.protocol = http
input.obiee.host = msp00acz.us.oracle.com
input.obiee.managed.server.port = 7333
input.obiee.sso.port = 7777
input.obiee.impersonate.user = BIImpersonateUser
input.obiee.impersonate.user.alias = bi-alias
input.obiee.static.resources.location = http://msp00acz-ada-vip.us.oracle.com:7777

## Properties from Page:Summary
input.do.install.oraac = true

## Properties from Page:Summary

## Properties from Page:Summary

## Properties from Page:Summary

## Properties from Page:Summary

## Properties from Page:progress
# Targets selected for page
progress-targets = install,
```

G

Appendix: ant.install.properties - ALLOC

Below is the ant install properties file for Alloc application.

Ant Installer - properties auto generated on Wed\ Jun\ 08\ 21:48:15\ PDT\ 2016

```
basedir = /scratch/u00/webadmin/media/ALLOC/alloc/application/.
ant.install.config.version = 1.1


## Properties from Page:Introduction
input.turnoffnonssl.port = false

## Properties from Page:SelectComponent
input.enable.obiee.integration = true

## Properties from Page:AllocAppRetailHome
input.retail.home = /u00/projects/j2ee/ALLOC15HACS

## Properties from Page:HostDetails
input.host = msp00acs.us.oracle.com

## Properties from Page:Security
input.enable.ssl.alloc.admin.server = false

## Properties from Page:AppServerDetails
input.appserver.host = msp00acs.us.oracle.com
input.appserver.admin.port = 7151
input.admin.user = weblogic
input.admin.alias = wlsAlias

## Properties from Page:AllocAppDeploymentDetails
input.app.name = alloc15
input.context.root = alloc15
input.wls.target = Cluster-alloc

## Properties from Page:SecureJDBC
input.enable.securejdbc = false

## Properties from Page:AllocDataSourceDetails
input.alloc.datasource.url = jdbc:oracle:thin:@msp00avyp-r:1521/DOLRP04APP
input.alloc.datasource.username = rms01app
input.alloc.datasource.alias = dsallocAlias
input.alloc.datasource.schema.owner = rms01

## Properties from Page:AllocValidateDataSourcea

## Properties from Page:SecureDataSourceDetails
input.datasource.keyStore =
input.datasource.keyStoreType =
input.datasource.keyStorePassword =
input.datasource.trustStore =
input.datasource.trustStoreType =
input.datasource.trustStorePassword =


## Properties from Page:ALLOCBatchInput
```

```
input.batch.user.name = ALLOCATION_ADMIN
input.batch.user.alias = alloc15

## Properties from Page:JMSProvider
input.jms.module = allocJMSModule
input.calcqueue.name = calcQueue

## Properties from Page:OHSWebTier
input.use.ohs.web.tier = true

## Properties from Page:OHSWebTierDetails
input.ohs.web.tier.protocol = http
input.ohs.web.tier.host = msp00acs-acf-vip.us.oracle.com
input.ohs.web.tier.port = 7777

## Properties from Page:DefaultJaznMappings
input.use.default.jazn.mappings = true

## Properties from Page:OBIEEDetails
input.obiee.protocol = http
input.obiee.host = msp00acz.us.oracle.com
input.obiee.managed.server.port = 7333
input.obiee.sso.port = 7777
input.obiee.impersonate.user = BIImpersonateUser
input.obiee.impersonate.user.alias = bi-alias
input.obiee.static.resources.location = http://msp00acz-ada-
vip.us.oracle.com:7777/analytics

## Properties from Page:Summary
input.admin.alias = wlsAlias
input.alloc.datasource.alias = dsallocAlias

## Properties from Page:progress
# Targets selected for page
progress-targets = install,
```

H

Appendix: ant.install.properties - SIM

Below is the sample of ant.install.properties file generated during installation of SIM.

Ant Installer - properties auto generated on Thu\ May\ 19\ 22:31:51\ PDT\ 2016

```
basedir = /scratch/u00/webadmin/media/SIM/sim/application/.
ant.install.config.version = 1.0


## Properties from Page:Introduction

## Properties from Page:Installation Type
input.deploy.clustered = true

## Properties from Page:Cluster Details
input.installation.url = msp00acs-acf-vip.us.oracle.com

## Properties from Page:Security Details
input.enable.ssl = false

## Properties from Page:Application Server Details
input.admin.host = msp00acs.us.oracle.com
input.admin.port = 7141
input.admin.user = weblogic

## Properties from Page:App Deployment Details
input.client.context.root = sim-client
input.mobile.server.context.root = sim-mobile
input.wls.instance = Cluster-sim

## Properties from Page:Choose Integration Apps
input.sim.integration.rib.enabled = true
input.sim.integration.rpm.enabled = true
input.sim.integration.rms.enabled = true
input.sim.integration.manifest.enabled = true
input.sim.integration.oms.enabled = true

## Properties from Page:RIB Integration Details
input.sim.integration.rib.url = t3://msp00acl-acm-vip.us.oracle.com:7777/rib-sim
input.sim.integration.rib.user.name = ribadmin
input.sim.integration.rib.inject.user.name = sim.rib

## Properties from Page:RPM WebService Policy
input.sim.integration.rpm.policy =

## Properties from Page:RPM Integration Details
input.sim.integration.rpm.pricechange.wsdl.url = http:///msp00alm-akp-
vip.us.oracle.com:7777/rpm-PriceChange-
AppServiceDecorator/ProxyService/PriceChangeAppServiceProxy?wsdl
input.sim.integration.rpm.priceinquiry.wsdl.url = http://msp00alm-akp-
vip.us.oracle.com:7777/rpm-PriceInquiry-
AppServiceDecorator/ProxyService/PriceInquiryAppServiceProxy?wsdl
input.sim.integration.rpm.user.name =
input.sim.integration.rpm.client.keystore.name =
```

```
input.sim.integration.rpm.client.key.name =
input.sim.integration.rpm.server.key.name =

## Properties from Page:RMS WebService Policy
## Properties from Page:RMS Integration Details
input.sim.integration.rms.storeorder.wsdl.url = http:/msp00alm-akp-
vip.us.oracle.com:7777/rms-StoreOrder-
AppServiceDecorator/ProxyService/StoreOrderAppServiceProxy?wsdl
input.sim.integration.rms.user.name =
input.sim.integration.rms.client.keystore.name =
input.sim.integration.rms.client.key.name =
input.sim.integration.rms.server.key.name =

## Properties from Page:Manifest WebService Policy
input.sim.integration.manifest.policy =

## Properties from Page:Manifest Integration Details
input.sim.integration.manifest.wsdl.url = http://msp00alm-akp-
vip.us.oracle.com:7777/StoreShipmentManifestBean/StoreShipmentManifestService?WSDL
input.sim.integration.manifest.user.name =
input.sim.integration.manifest.client.keystore.name =
input.sim.integration.manifest.client.key.name =
input.sim.integration.manifest.server.key.name =

## Properties from Page:OMS WebService Policy
input.sim.integration.oms.policy =

## Properties from Page:OMS Integration Details
input.sim.integration.oms.wsdl.url = http://msp00alm-akp-
vip.us.oracle.com:7777/oms-CustomerOrder-
AppServiceDecorator/ProxyService/CustomerOrderAppServiceProxy?wsdl
input.sim.integration.oms.user.name =
input.sim.integration.oms.client.keystore.name =
input.sim.integration.oms.client.key.name =
input.sim.integration.oms.server.key.name =

## Properties from Page:SecureJDBC
input.enable.securejdbc = false

## Properties from Page:Data Source Details
input.datasource.url = jdbc:oracle:thin:@msp00avyp-r:1521/DOLRP04APP
input.datasource.username = sim01
input.datasource.admin.username = sim01_adm
input.datasource.business.username = sim01_bsi
input.datasource.mps.username = sim01_mps
input.datasource.security.username = sim01_sec
input.datasource.keyStore =
input.datasource.keyStoreType =
input.datasource.trustStore =
input.datasource.trustStoreType =

## Properties from Page:ValidateDataSource

## Properties from Page:LDAP Server Details
input.ldap.url = ldap://msp00acz.us.oracle.com:3060
input.ldap.base.dn = dc=us,dc=oracle,dc=com
input.ldap.user = cn=sim.admin,cn=Users,dc=us,dc=oracle,dc=com

## Properties from Page:Mail Session Details
input.mail.host = msp00acs.us.oracle.com
input.mail.ssl.enable = true
input.mail.port = 25
input.mail.user.name =
```

```
input.mail.auth = true
input.mail.starttls.enable = true

## Properties from Page:Wireless Server Details
input.sim.wireless.user.name = sim.wireless
input.sim.wireless.port = 40002
input.sim.wireless.ssl.enabled = false

## Properties from Page:Wireless Server SSL Disabled
input.sim.wireless.keystore.type =
input.sim.wireless.keystore.name =
input.sim.wireless.key.name =

## Properties from Page:Batch Server Details
input.sim.batch.user.name = sim.batch

## Properties from Page:Server User Details
input.sim.server.user.name = sim.server

## Properties from Page:Internal Security Installation User Details
input.sim.security.internal.install.user.name = sim.install

## Properties from Page:SIM WebService Provider Policy
input.sim.integration.webservice.policy =

## Properties from Page:Reporting and Printing Details
input.sim.integration.report.enabled = true

## Properties from Page:Reporting BIP Details 1

## Properties from Page:Reporting BIP Details 2
input.sim.integration.report.wsdl.url = http://msp00acz-ada-
vip.us.oracle.com:7777/xmlpserver
input.sim.integration.report.template.root.folder = /Base/SIM/15
input.sim.integration.report.user.name = retail.user
input.sim.integration.report.bip.enabled = true

## Properties from Page:Ticket Printing Disabled
input.sim.integration.ticket.enabled = false
input.sim.integration.ticket.bip.enabled =
input.sim.integration.ticket.wsdl.url =
input.sim.integration.ticket.template.root.folder =
input.sim.integration.ticket.policy =
input.sim.integration.ticket.user.name =
input.sim.integration.ticket.client.keystore.name =
input.sim.integration.ticket.client.key.name =
input.sim.integration.ticket.server.key.name =
## Properties from Page:EnableSSO
input.sim.security.sso.enabled = true

## Properties from Page:Single Sign On Details
input.sim.security.sso.host = msp00acs-acf-vip.us.oracle.com
input.sim.security.sso.port = 7777

## Properties from Page:Manual Deployment Option
input.install.to.appserver = true

## Properties from Page:Summary

## Properties from Page:Summary2

## Properties from Page:progress
# Targets selected for page
```

```
progress-targets = install,
```

I

Appendix: ant.install.properties - RPM

Below is the sample of ant.install.properties file generated during installation of RPM

Ant Installer - properties auto generated on Wed\ Jun\ 08\ 00:21:42\ PDT\ 2016

```
basedir = /scratch/u00/webadmin/media/RPM/CDROM/rpm/application/.
ant.install.config.version = 1.1


## Properties from Page:Introduction
input.datasource.alias = db-alias
input.rib.jndi.username = ribadmin
input.rib.jndi.alias = weblogic-alias
input.rib.provider.url = t3://msp00acl-acm-vip.us.oracle.com:7777/rib-rpm
input.ldap.search.alias = ldap-alias
input.admin.alias = wls-alias
input.batch.user.alias = retail.user
input.installation.url = msp00acs-acf-vip.us.oracle.com
input.osso.web.tier.server = msp00acs-acf-vip.us.oracle.com
input.osso.web.tier.port = 7777
input.install.to.appserver = true
input.datasource.keyStore =
input.datasource.keyStoreType =
input.datasource.trustStore =
input.datasource.trustStoreType =
input.refresh.sso.token.key.startup = true
input.security.sso.token.key.alias = SSO-TOKEN-KEY-ALIAS

## Properties from Page:RPMAPPRETAILHOME
input.retail.home = /u00/projects/j2ee/RPM150HACS

## Properties from Page:HostDetails
input.host = msp00acs.us.oracle.com

## Properties from Page:Security
input.enable.ssl = false

## Properties from Page:SecureJDBC
input.enable.securejdbc = false

## Properties from Page:RPMAPPCONFIGUREAUTOJARSIGNING
input.enable.autojarsign = false

## Properties from Page:Jar Signing Details
input.autojarsign.keyStore =
input.autojarsign.keyStore.password =
input.autojarsign.keystore.private.pass =
input.autojar.signing.alias =

## Properties from Page:DataSourceDetails
input.datasource.url = jdbc:oracle:thin:@msp00avyp-r:1521/DOLRP04APP
input.datasource.username = rms01app
input.schema.owner = rms01
input.datasource.alias = db-alias
```

```
## Properties from Page:ValidateDataSource

## Properties from Page:JMSProvider
input.jms.module = rpmJMSModule

## Properties from Page:JMSQueue
input.taskqueue.name = taskQueue
input.chunkqueue.name = chunkQueue
input.chunkControllerQueue.name = chunkControllerQueue

## Properties from Page:LDAPDirectoryServerDetails
input.ldap.provider.url = ldap://msp00acz.us.oracle.com:3060
input.ldap.search.user = cn=rpm.admin,cn=Users,dc=us,dc=oracle,dc=com
input.ldap.search.alias = ldap-alias

## Properties from Page:LDAPDirectoryServerSearches
input.ldap.base.dn = dc=us,dc=oracle,dc=com
input.ldap.search.filter = (&(objectclass=person) %v)
input.ldap.attr.username = uid
input.rpm.secure.users.group = rpm_secure_users
input.rpm.secure.resource.user = rpm_resource_user
input.ldap.search.filter.attr = objectclass
input.ldap.search.filter.value = person
input.ldap.idstore.factory.class =
oracle.security.idm.providers.oid.OIDIdentityStoreFactory

## Properties from Page:RpmClient
input.client.context.root = rpm-client
input.use.osso = true

## Properties from Page:OSSODetails
input.osso.web.tier.server = msp00acs-acf-vip.us.oracle.com
input.osso.web.tier.port = 7777
input.security.sso.token.key.alias = SSO-TOKEN-KEY-ALIAS
input.refresh.sso.token.key.startup = true

## Properties from Page:InstallationType
input.installation.type = Cluster

## Properties from Page:ClusterDetails
input.installation.url = msp00acs-acf-vip.us.oracle.com

## Properties from Page:AppDeploymentDetails
input.app.name = rpm
input.wls.target = Cluster-rpm

## Properties from Page:WLSAdminDetails
input.appserver.host = msp00acs.us.oracle.com
input.appserver.admin.port = 7131
input.admin.user = weblogic
input.admin.alias = wls-alias
## Properties from Page:Batch User Credentials
input.batch.user = retail.user

## Properties from Page:ChooseApps
input.scope.rib-rpm = true

## Properties from Page:RIBforRPMDetails
input.rib.jndi.username = ribadmin
input.rib.jndi.alias = weblogic-alias
input.rib.provider.url = t3://msp00acl-acm-vip.us.oracle.com:7777/rib-rpm
```

```
## Properties from Page:Summary
input.rib.jndi.alias = weblogic-alias
input.ldap.search.alias = ldap-alias
input.admin.alias = wls-alias
input.batch.user.alias = retail.user

## Properties from Page:progress
# Targets selected for page
progress-targets = install,
```

J

Appendix: ant.install.properties - ReSA

Below is the sample of ant.install.properties file generated during installation of ReSA.

Ant Installer - properties auto generated on Tue\ May\ 24\ 00:29:37\ PDT\ 2016

```
basedir = /scratch/u00/webadmin/media/RESA/resa/application/.
ant.install.config.version = 1.1


## Properties from Page:Introduction
input.turnoffnonssl.port = false
input.do.install.oraac = true

## Properties from Page:SelectComponent
input.OBIEE.value = true

## Properties from Page:init-prop
input.obiee.protocol = http
input.obiee.host = msp00acz.us.oracle.com
input.obiee.managed.server.port = 7333
input.obiee.sso.port =
input.obiee.impersonate.user = BIImpersonateUser
input.obiee.impersonate.user.alias = bi-alias
input.obiee.static.resources.location = http://msp00acz-ada-
vip.us.oracle.com:7777/analytics

## Properties from Page:ReSAAppRetailHome
input.retail.home = /u00/projects/j2ee/RESA150HACS

## Properties from Page:HostDetails
input.host = msp00acs.us.oracle.com

## Properties from Page:Security
input.enable.ssl.ReSA.admin.server = false

## Properties from Page:AppServerDetails
input.appserver.host = msp00acs.us.oracle.com
input.appserver.admin.port = 7181
input.admin.user = weblogic
input.admin.alias = wlsAlias

## Properties from Page:AppDeploymentDetails
input.app.name = ReSA15
input.context.root = ReSA15
input.wls.target = Cluster-resa

## Properties from Page:ReSASecureJDBC
input.enable.securejdbc = false

## Properties from Page:ReSADataSourceDetails
input.ReSA.datasource.url = jdbc:oracle:thin:@msp00avyp-r:1521/DOLRP04APP
input.ReSA.datasource.username = rms01app
input.ReSA.datasource.alias = dsReSAAlias
input.ReSA.datasource.schema.owner = rms01
## Properties from Page:ReSAValidateDataSourcea
```

```
## Properties from Page:ReSASecureDataSourceDetails
input.ReSA.datasource.keyStore =
input.ReSA.datasource.keyStoreType =
input.ReSA.datasource.keyStorePassword =
input.ReSA.datasource.trustStore =
input.ReSA.datasource.trustStoreType =
input.ReSA.datasource.trustStorePassword =

## Properties from Page:OHSWebTier
input.use.ohs.web.tier = true

## Properties from Page:OHSWebTierDetails
input.ohs.web.tier.protocol = http
input.ohs.web.tier.host = msp00acs-acf-vip.us.oracle.com
input.ohs.web.tier.port = 7777

## Properties from Page:OBIEEDetails
input.obiee.protocol = http
input.obiee.host = msp00acz.us.oracle.com
input.obiee.managed.server.port = 7333
input.obiee.impersonate.user = BIImpersonateUser
input.obiee.impersonate.user.alias = bi-alias
input.obiee.static.resources.location = http://msp00acz-ada-
vip.us.oracle.com:7777/analytics

## Properties from Page:OBIEEHomeDetails
input.OBIEE.url.location = http://msp00acz-ada-vip.us.oracle.com:7777

## Properties from Page:BIPublisher
input.BIPublisher.value = true

## Properties from Page:BIPublisherDetails
input.BIPublisher.url = http://msp00acz-ada-
vip.us.oracle.com:7777/xmlpserver/Guest/RMS

## Properties from Page:Summary
input.admin.alias = wlsAlias
input.ReSA.datasource.alias = dsReSAAlias

## Properties from Page:Summary

## Properties from Page:progress
# Targets selected for page
progress-targets = install,
```

K

Appendix: Entries of mod_wl_ohs.conf File

LoadModule weblogic_module "${ORACLE_HOME}/ohs/modules/mod_wl_ohs.so"

This empty block is needed to save mod_wl related configuration from EM to this file when changes are made at the Base Virtual Host Level

```
<IfModule weblogic_module>
#      WebLogicHost <WEBLOGIC_HOST>
#      WebLogicPort <WEBLOGIC_PORT>
#      Debug ON
#      WLLogFile /tmp/weblogic.log
#      MatchExpression *.jsp
      MatchExpression /oam*
</IfModule>

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

<Location /forms/frmservlet?* >
WebLogicCluster msp00acs.us.oracle.com:9001,msp00acf.us.oracle.com:9001
SetHandler weblogic-handler
</Location>

<Location /sim-client >
WebLogicCluster msp00acs.us.oracle.com:7143,msp00acf.us.oracle.com:7143
SetHandler WebLogic-handler
</Location>

<LocationMatch ^/bea_wls_internal/>
SetHandler weblogic-handler
WebLogicCluster msp00acs.us.oracle.com:7143,msp00acf.us.oracle.com:7143
</LocationMatch>

<LocationMatch ^/bea_wls_internal/>
SetHandler weblogic-handler
WebLogicCluster msp00acs.us.oracle.com:9001,msp00acf.us.oracle.com:9001
</LocationMatch>

<Location /alloc15>
WebLogicCluster msp00acs.us.oracle.com:7153,msp00acf.us.oracle.com:7153
SetHandler WebLogic-handler
WLCookieName ALC_CORESESSIONID
</Location>

<Location /adfAuthentication>
WebLogicCluster msp00acs.us.oracle.com:7153,msp00acf.us.oracle.com:7153
SetHandler WebLogic-handler
</Location>

<Location /rpm-client >
WebLogicCluster msp00acs.us.oracle.com:7133,msp00acf.us.oracle.com:7133
```

```
SetHandler weblogic-handler
</Location>

<Location /ReimViewController>
 WebLogicCluster msp00acs.us.oracle.com:7093,msp00acf.us.oracle.com:7093
 SetHandler weblogic-handler
 WLCookieName REIMSESSIONID
</Location>

<Location /ResaPortal>
WebLogicCluster msp00acs.us.oracle.com:7183,msp00acf.us.oracle.com:7183
SetHandler WebLogic-handler
WLCookieName RESASESSIONID
</Location>

<Location /RetailAppsAdminConsole-REIM>
WebLogicCluster msp00acs.us.oracle.com:7093,msp00acf.us.oracle.com:7093
 SetHandler weblogic-handler
</Location>

<Location /RetailAppsAdminConsole-RESA>
WebLogicCluster msp00acs.us.oracle.com:7183,msp00acf.us.oracle.com:7183
SetHandler WebLogic-handler
</Location>

<Location /RetailAppsAdminConsole-ALLOC>
WebLogicCluster msp00acs.us.oracle.com:7153,msp00acf.us.oracle.com:7153
SetHandler WebLogic-handler
</Location>
```

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.