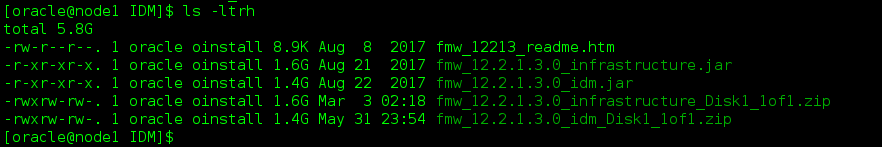
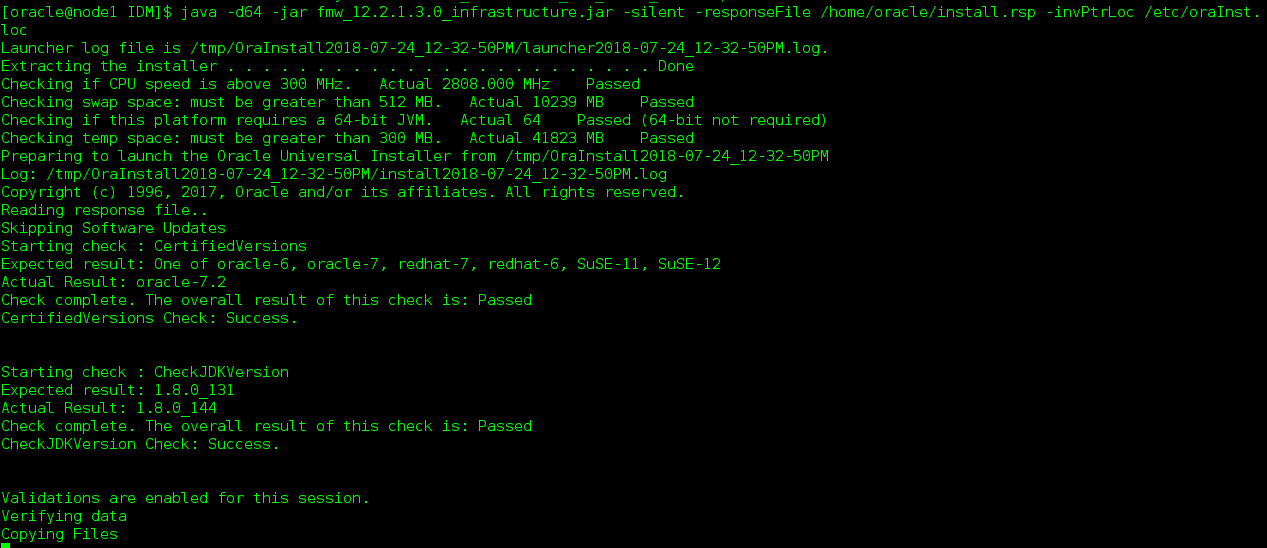
OAM INSTALLATION

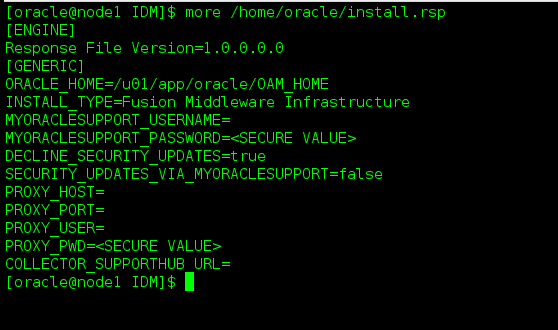
Unzip the SW



Install FMW in silent mode



Install.rsp file

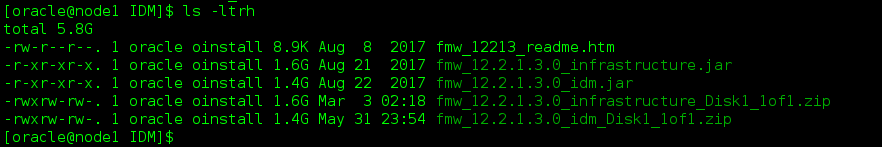


FMW is installed in below location

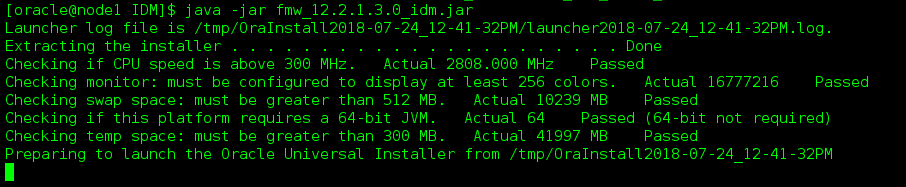


Install OAM software

Unzip the SW

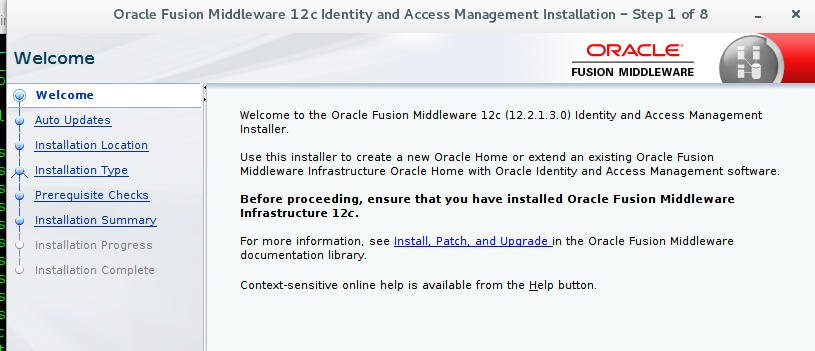


Launch OAM

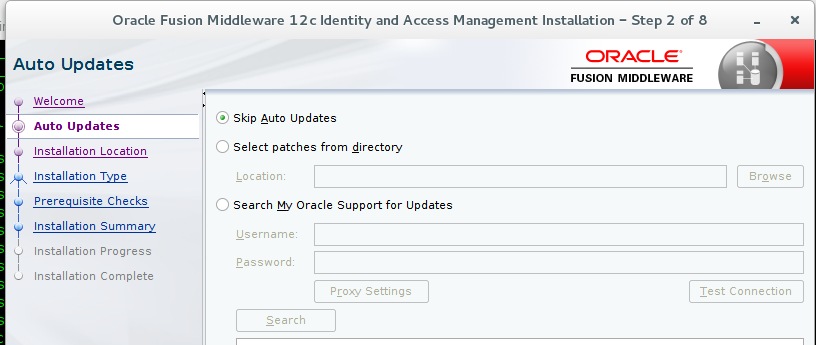




Click on next



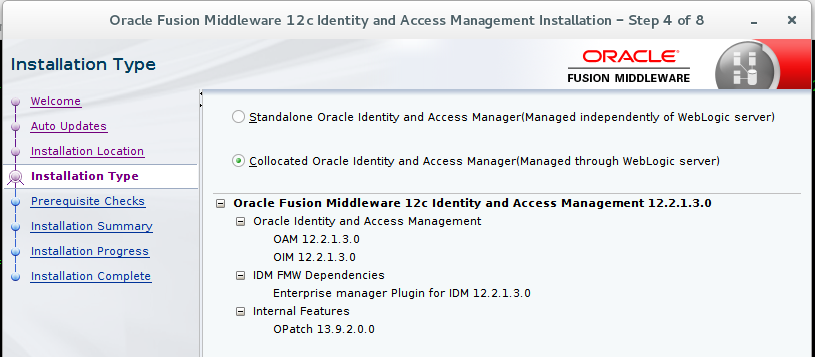
Skip Auto updates



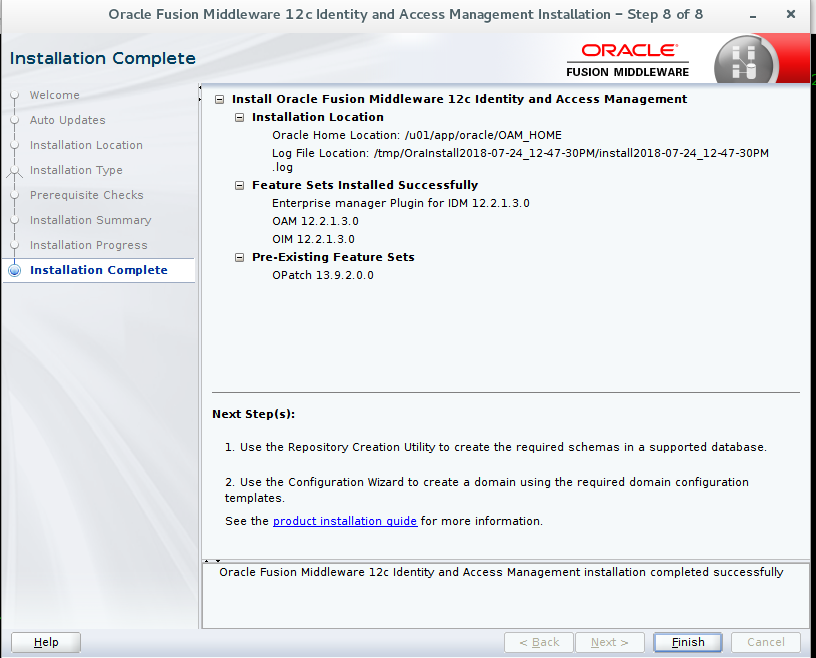
MW home location



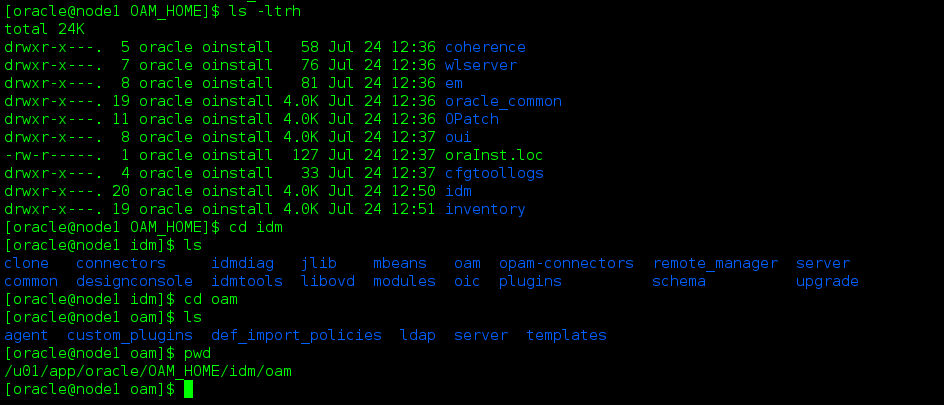
Collocated Mode



Installation completed successfully

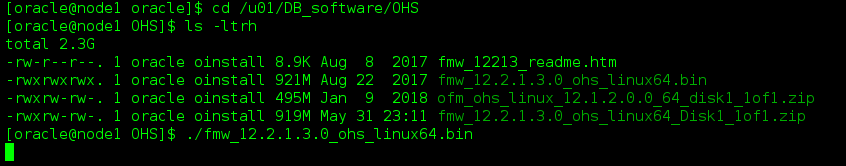


OAM and IDM binaries

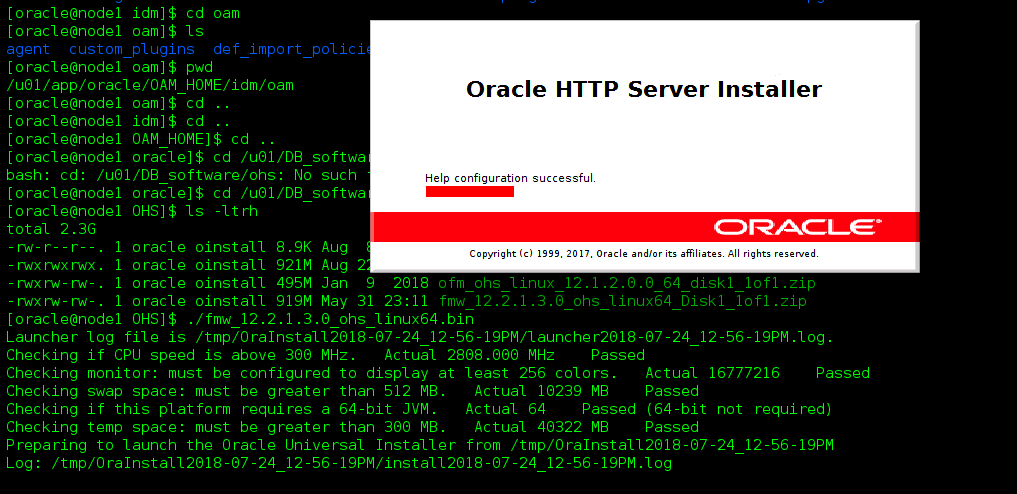


Install OHS

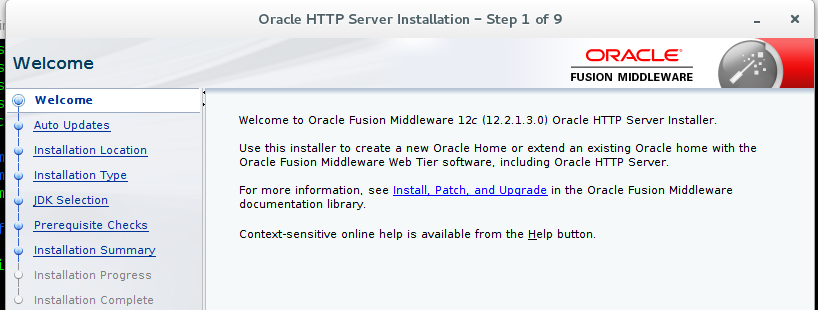
Unzip the Sw



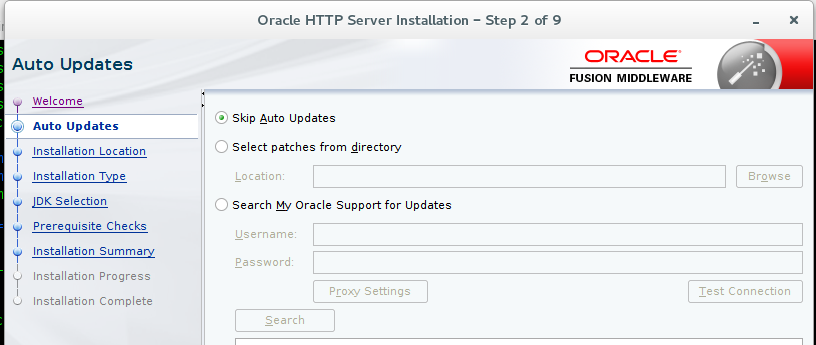
Launch OHS



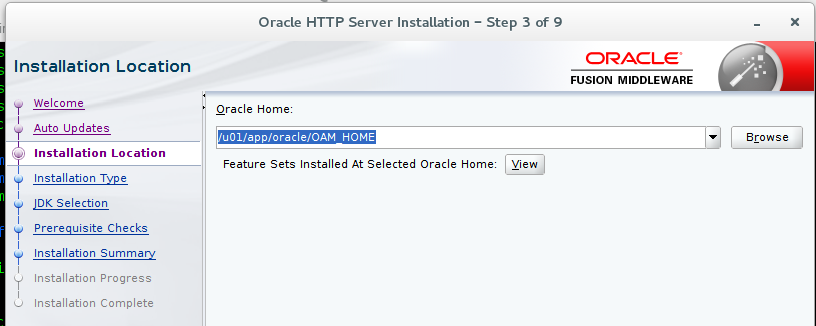
Click Next



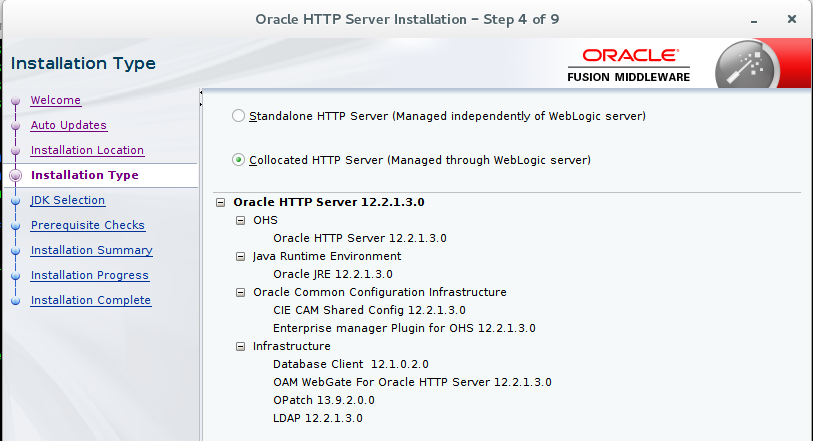
Skip Auto updates



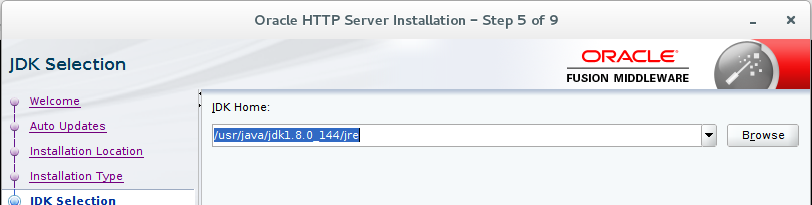
MW home



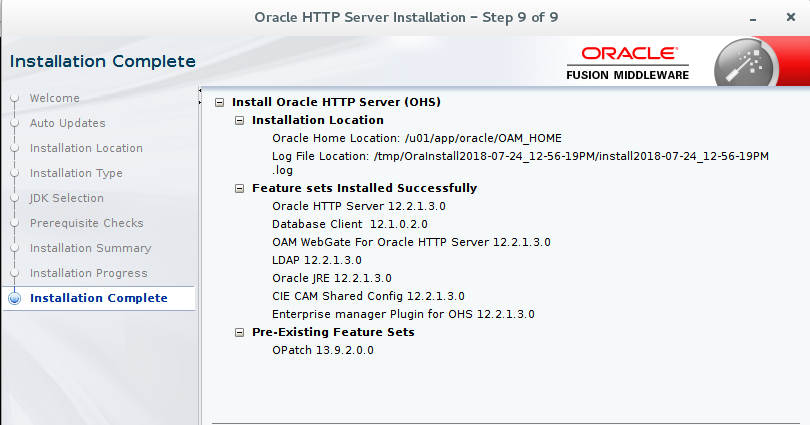
Collocated mode



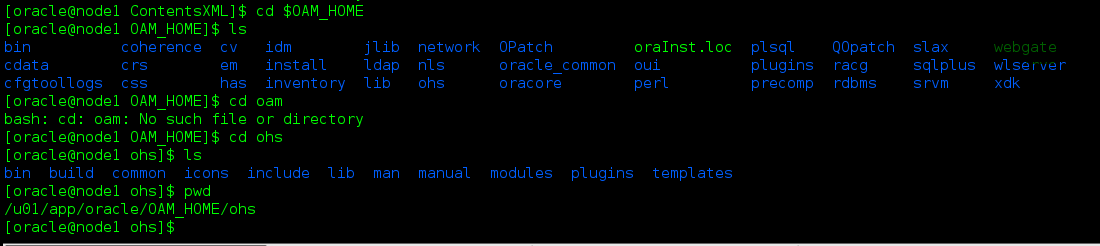
JDK home



Installation Summary

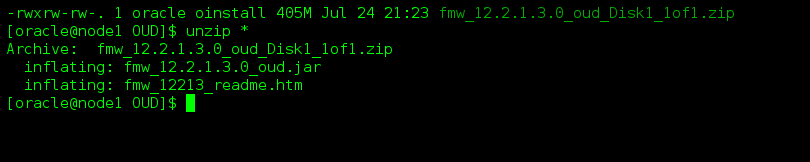


Location of OHS

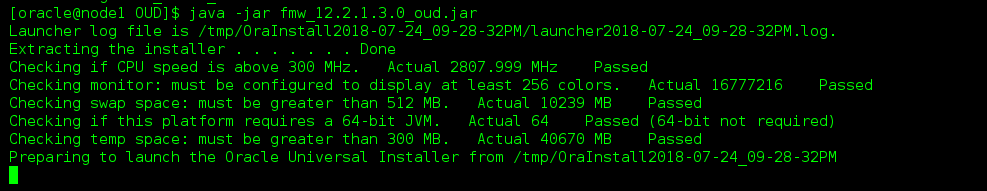


Install OUD

Unzip the SW

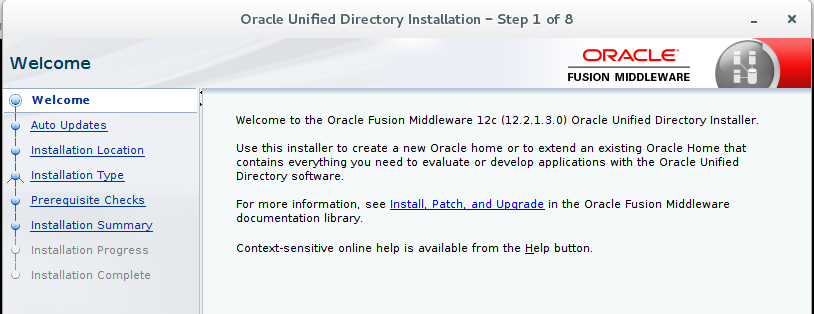


Launch OUD

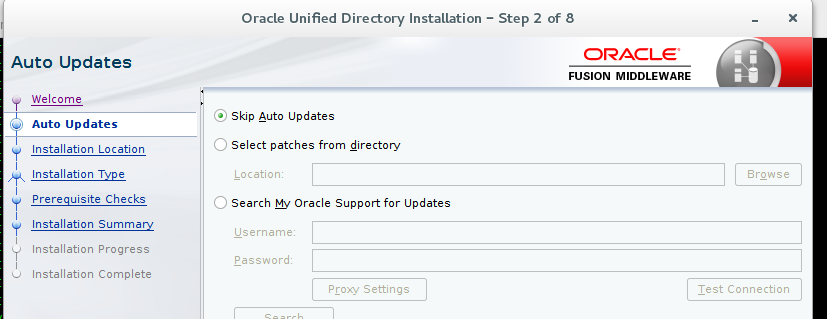




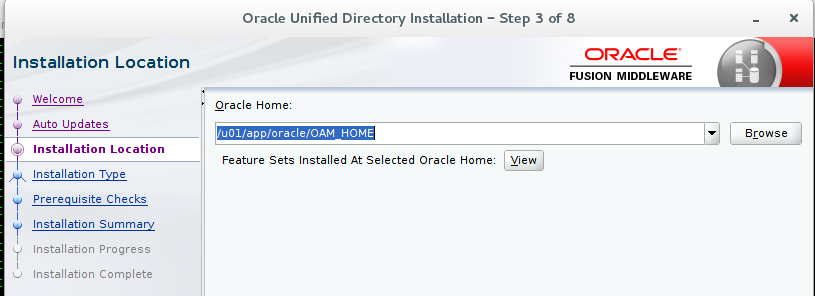
Click Next



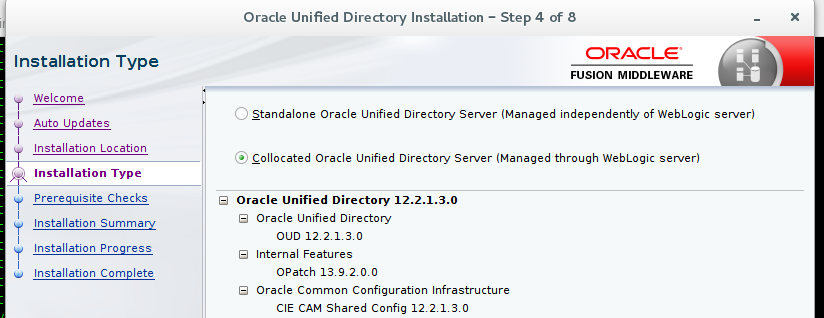
Skip Auto updates



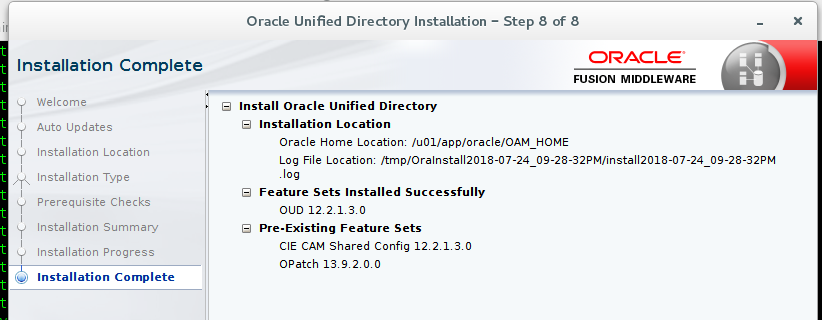
MW Home Location



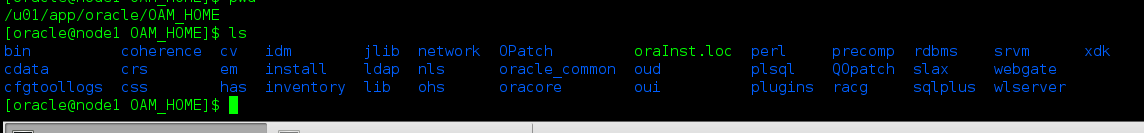
Collocated mode



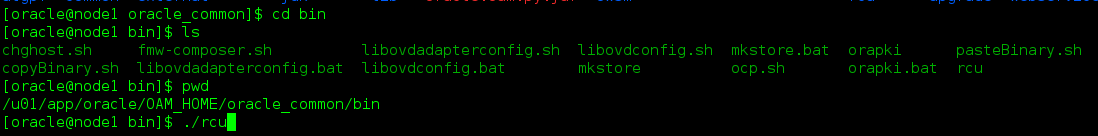
Installation Complete



OUD Installed Location



Create RCU for OAM, OUD, OHS



Welcome



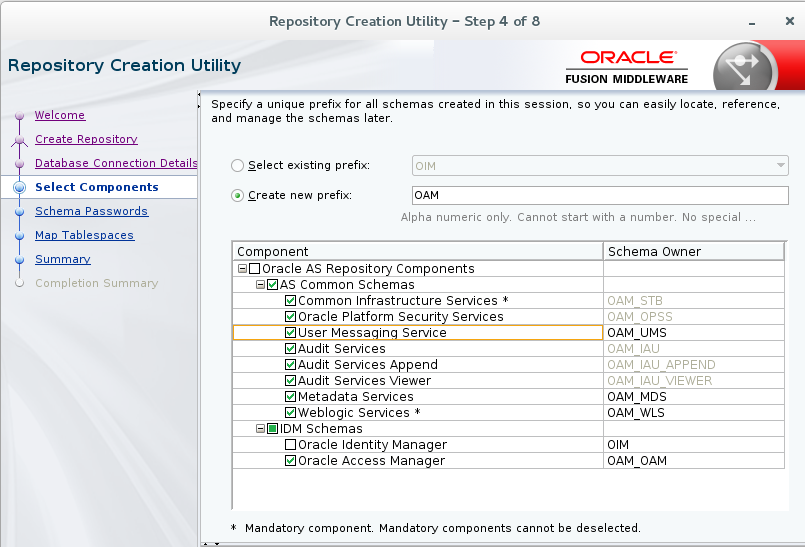
Create repository



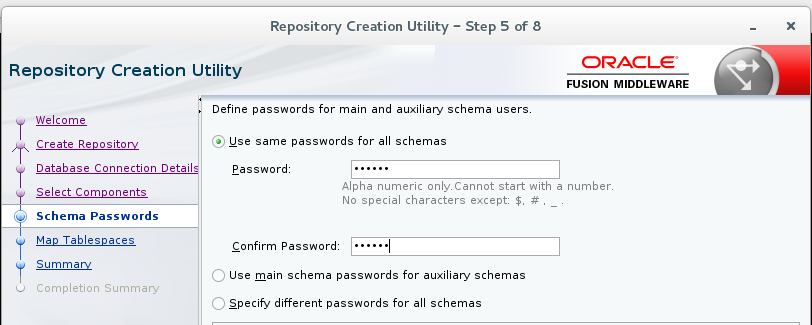
DB connection details



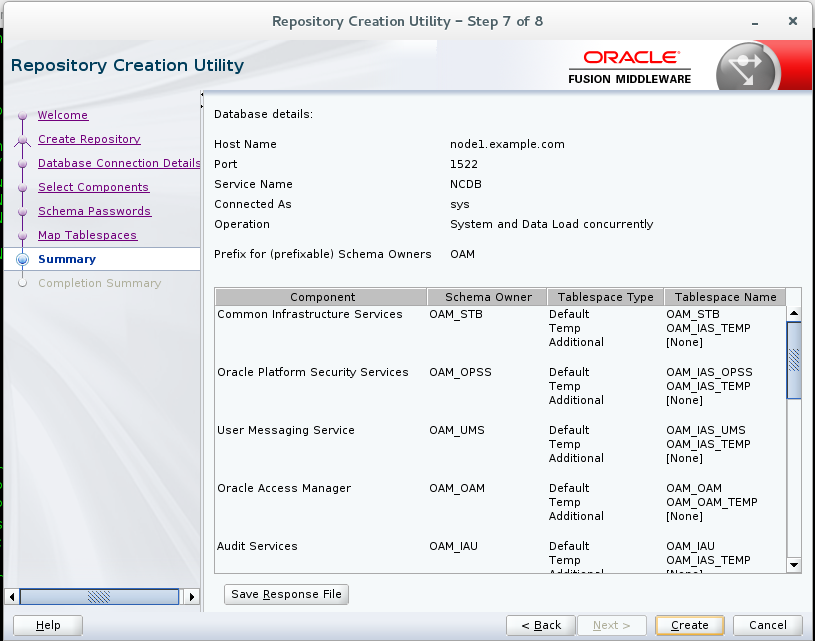
Select components



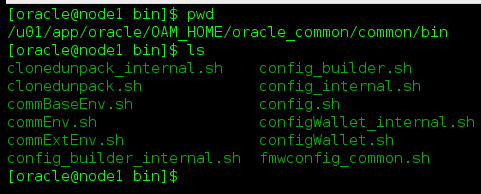
Choose Passwords



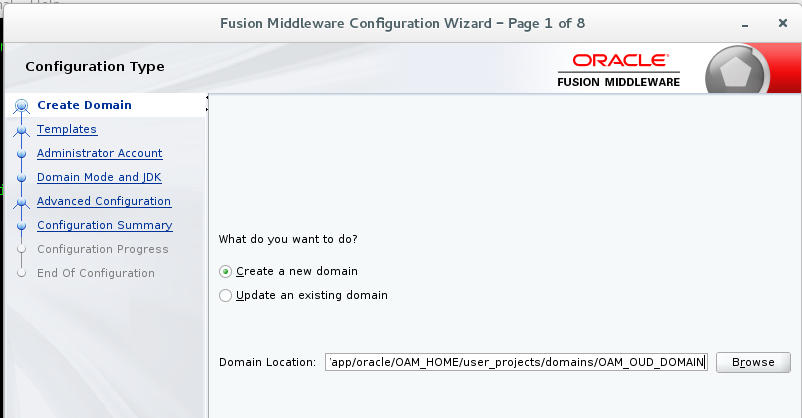
Summary



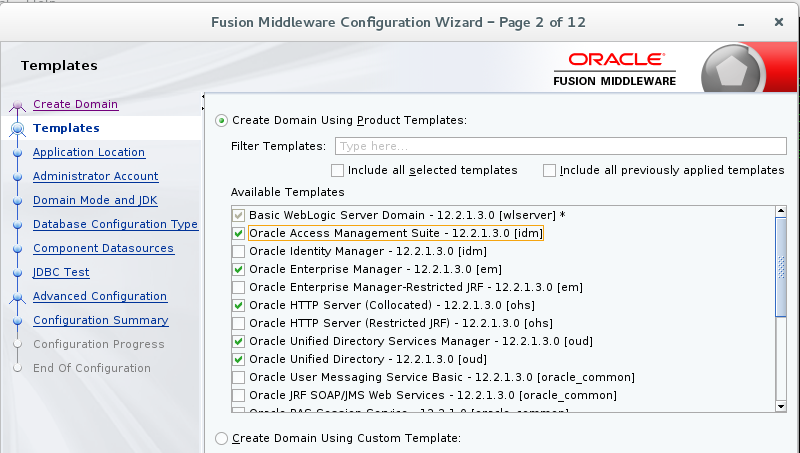
Creating a domain for OAM



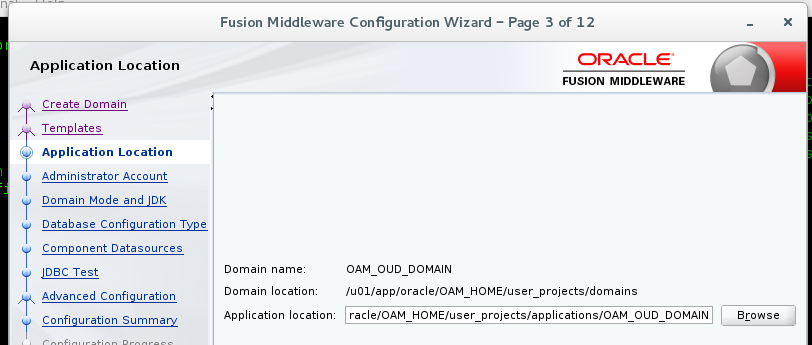
Launch config.sh



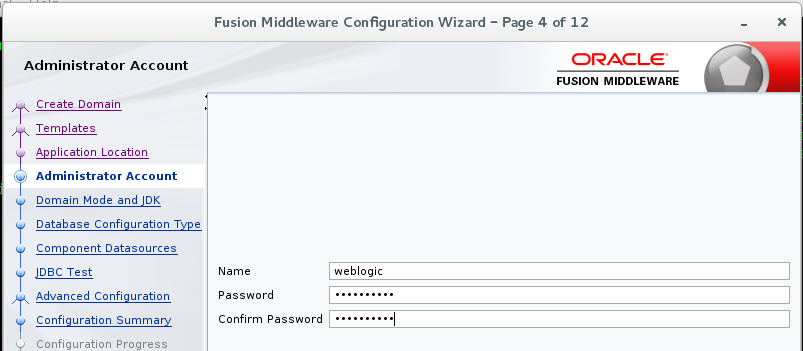
Select component



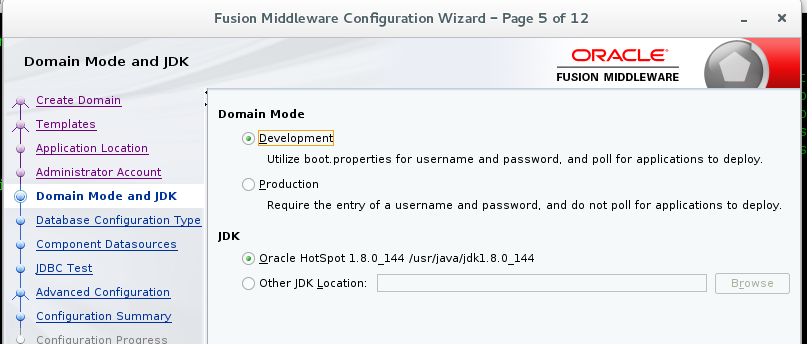
APP location



Admin Acc



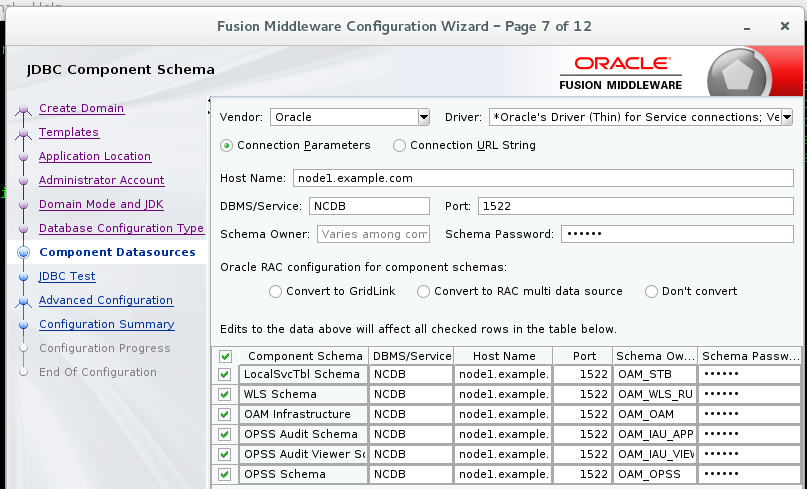
Dev mode



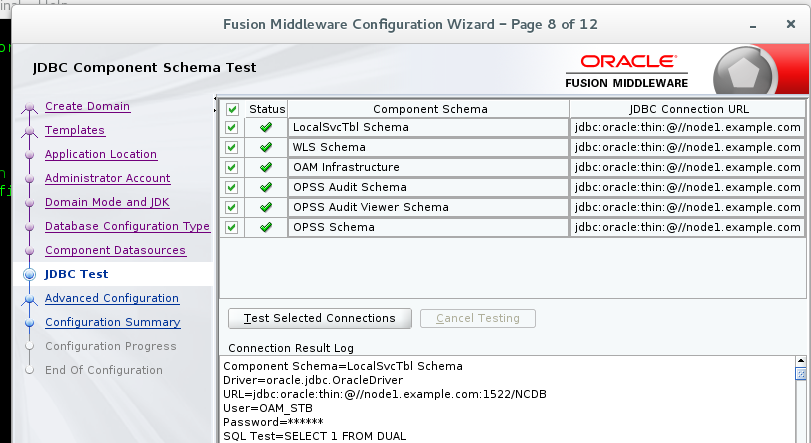
RCU information



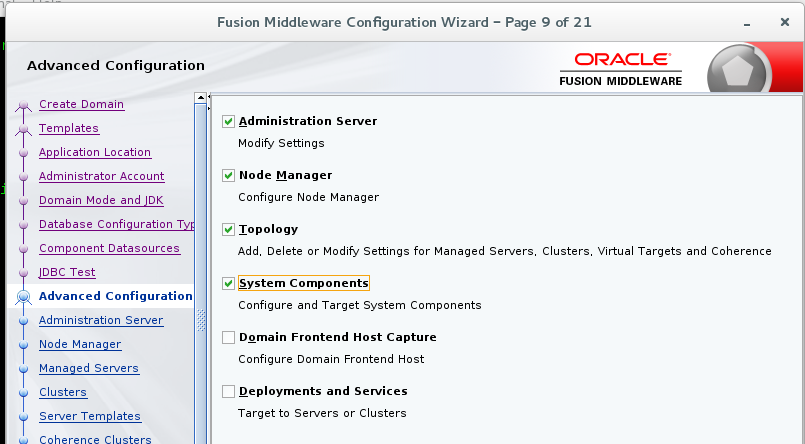
Component information



JDBC TEST



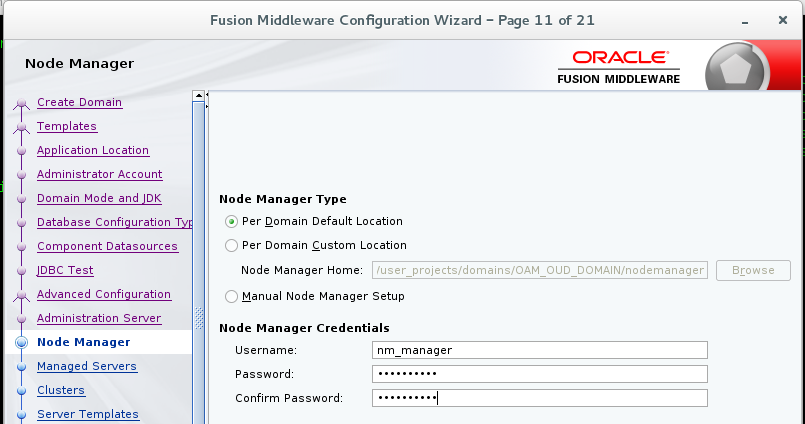
Advanced configuration



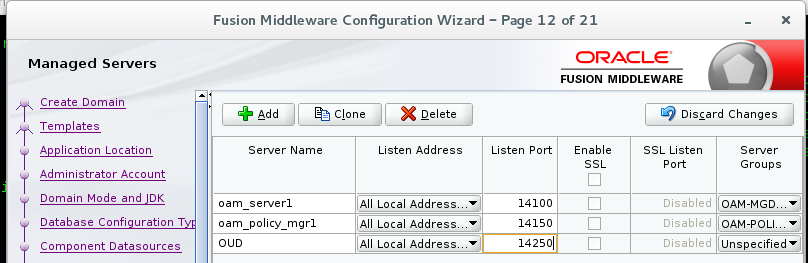
Admin Server Port details



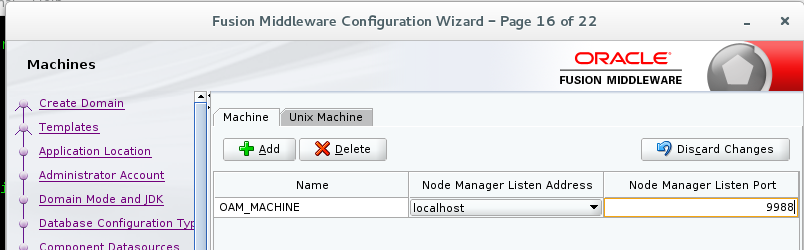
NM Manager Location



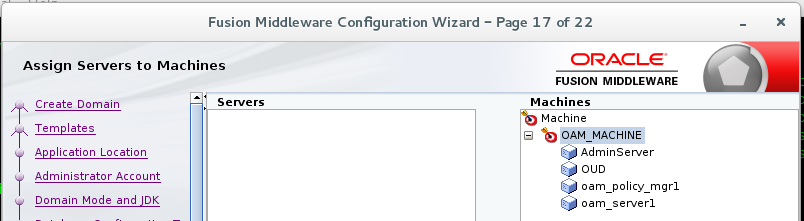
MS server details



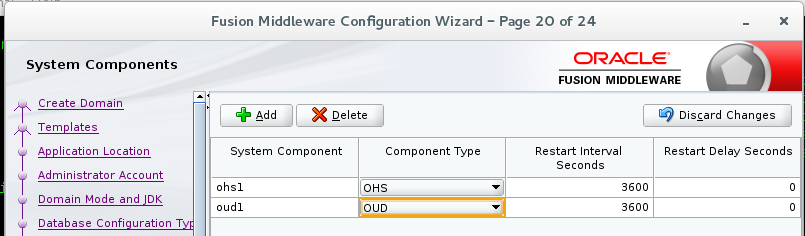
Machine details



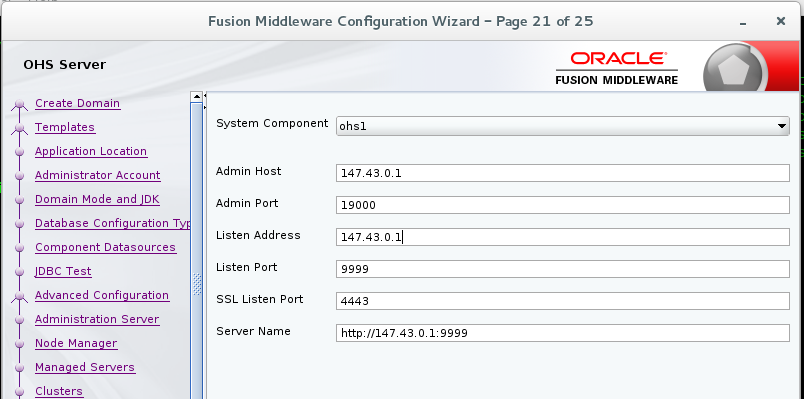
Assign Servers to Machines



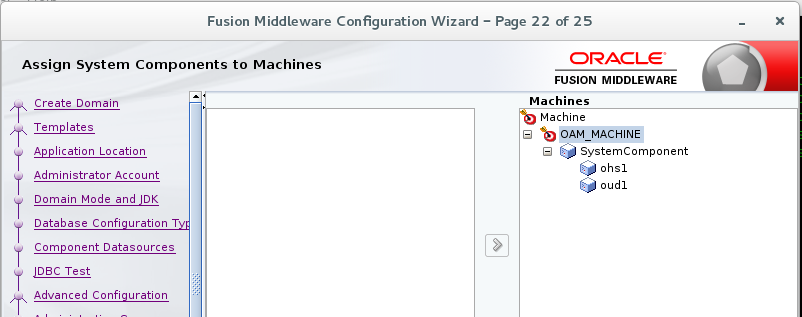
System component information for OHS and OUD



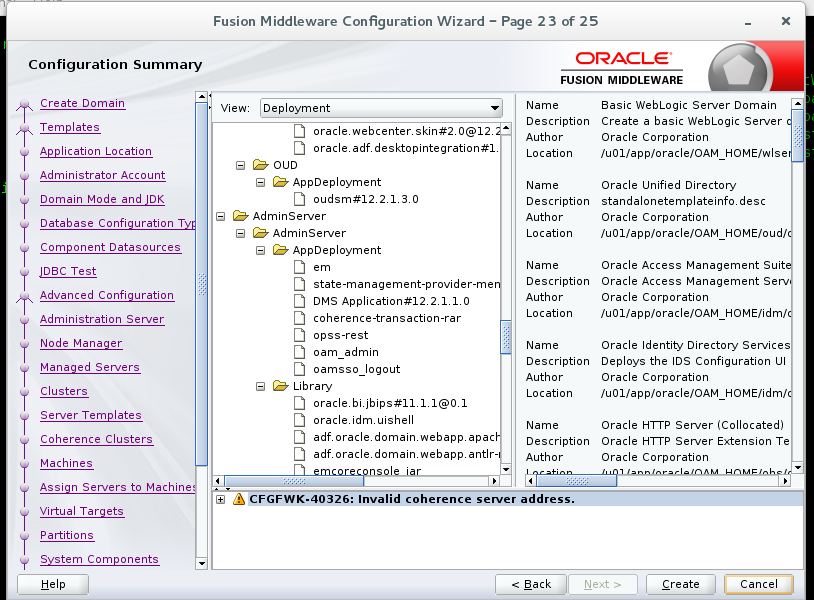
OHS Server details



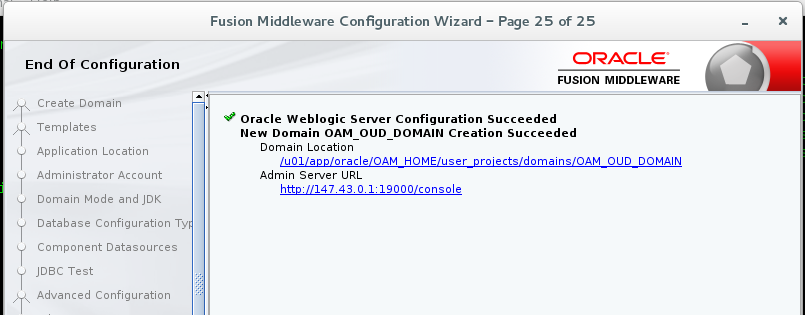
Assign System component to machines



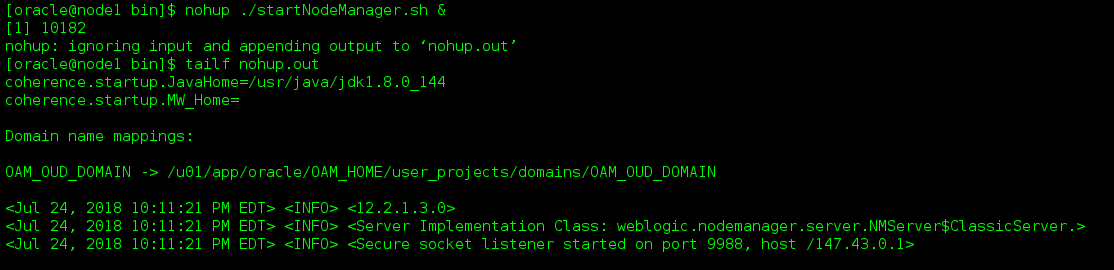
Configuration summary



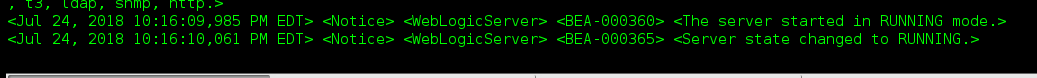
Installation summary

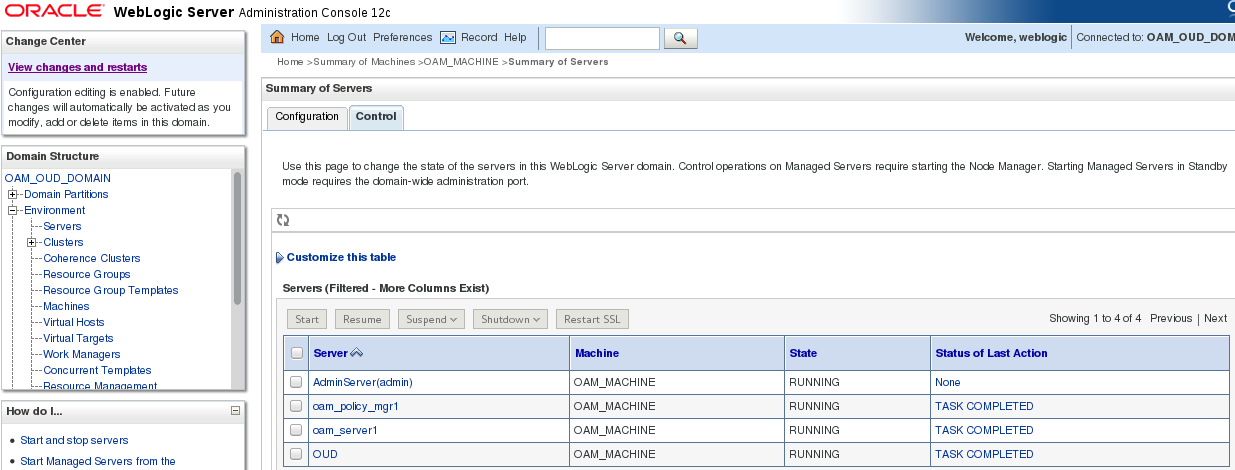


Start Node Manager

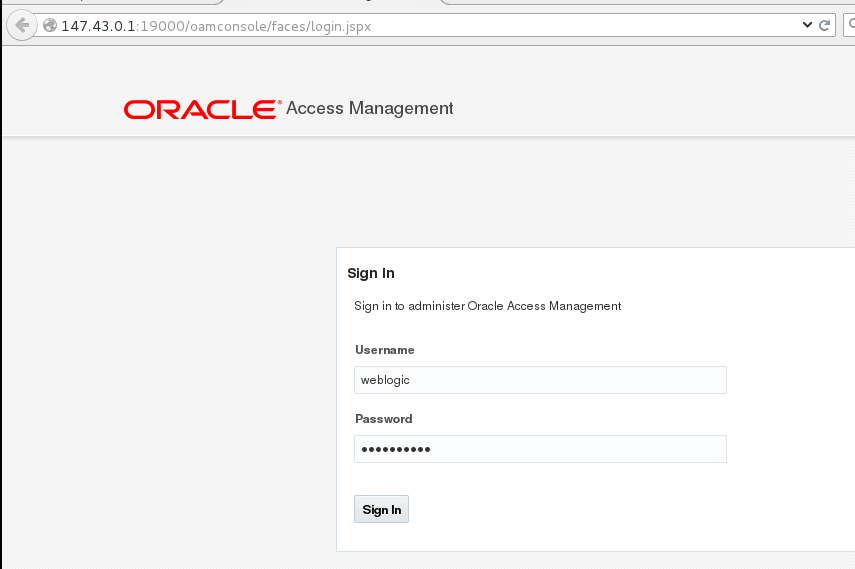


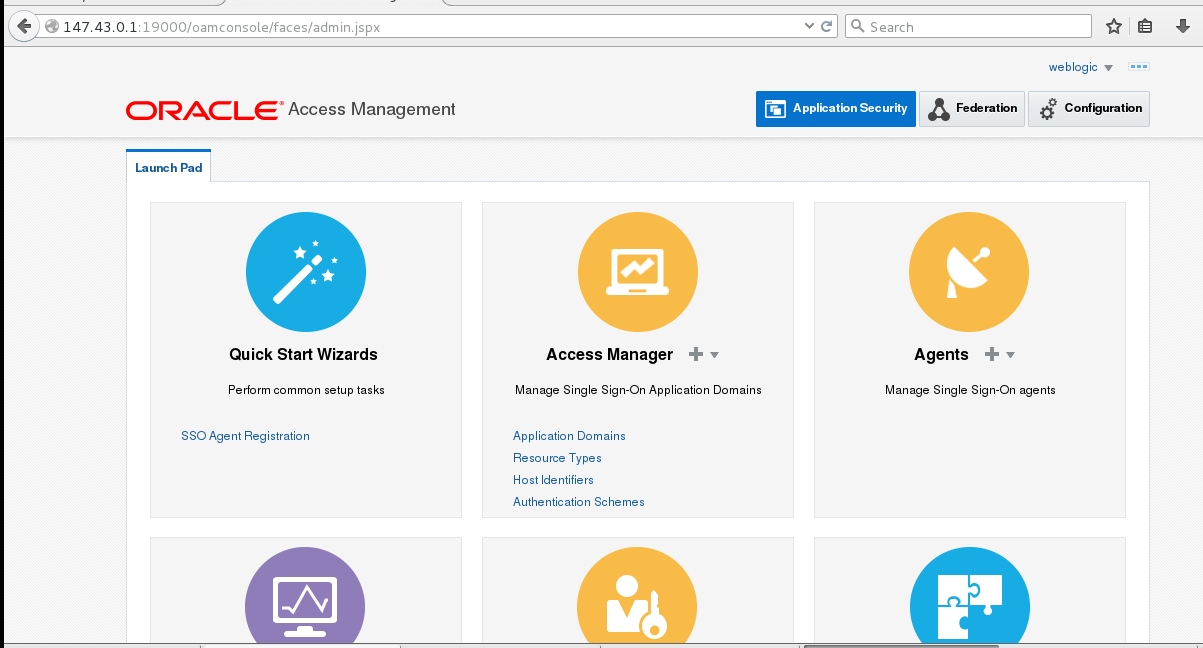
Start Weblogic.sh





OAM Console

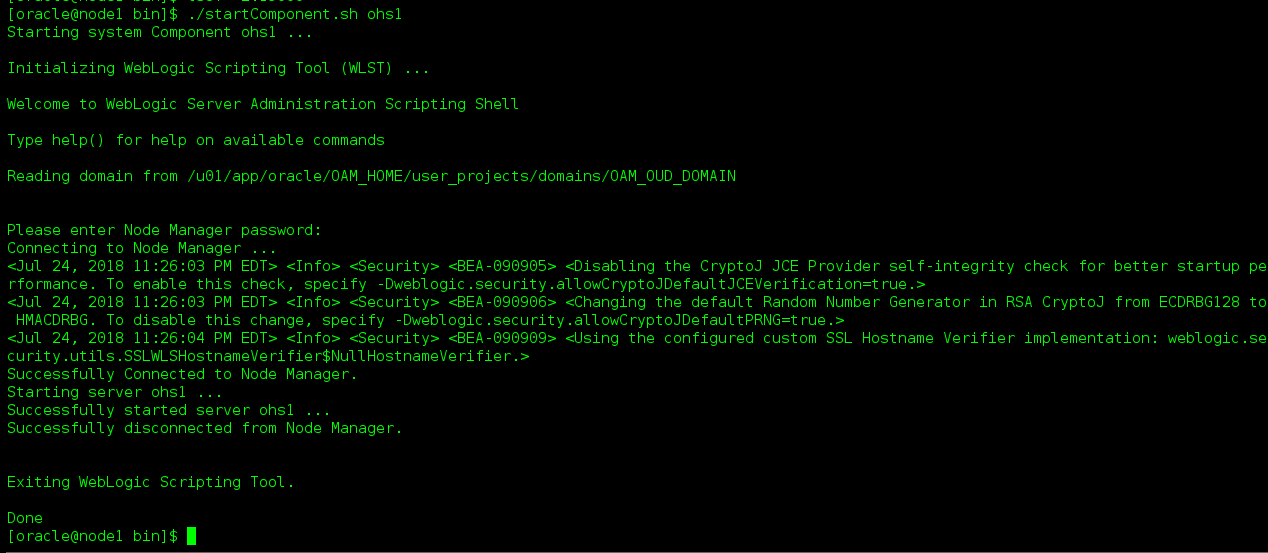




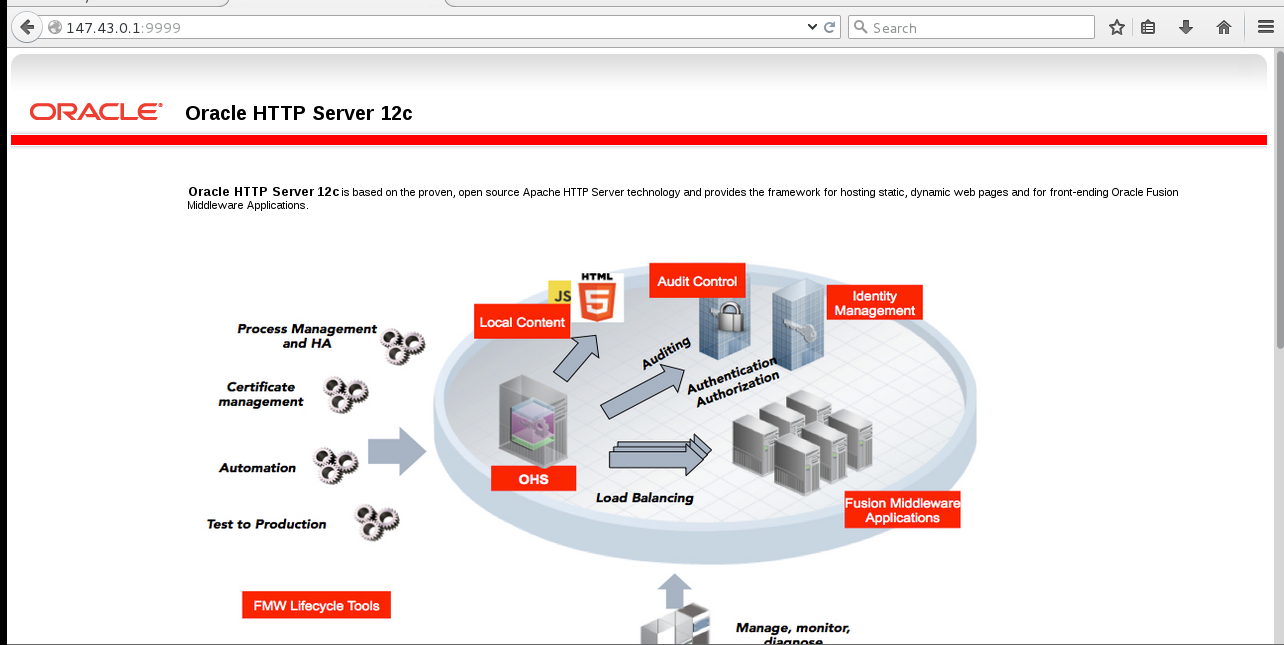
You can also access OAM console from oam\_policy\_mgr1 MS port( 11g2PS3 feature)



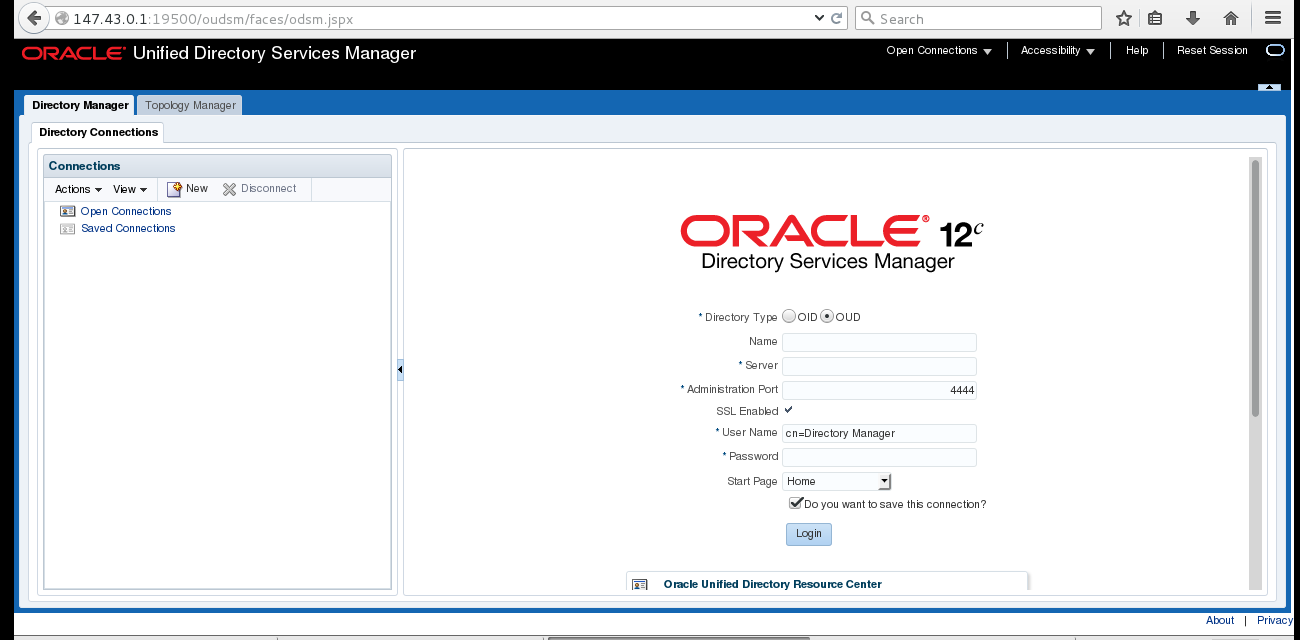
Start OHS( node manager should always be in SSL mode to start OHS1)



147.43.0.1:9999



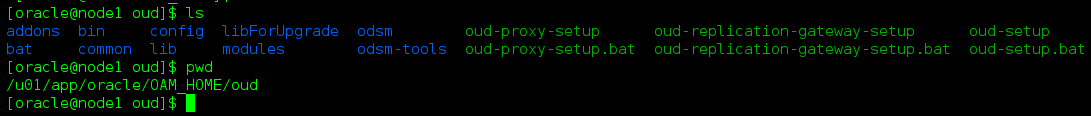
OUDSM



OUDSM was not launching as the OUDSM app was not targeted to Admin Server



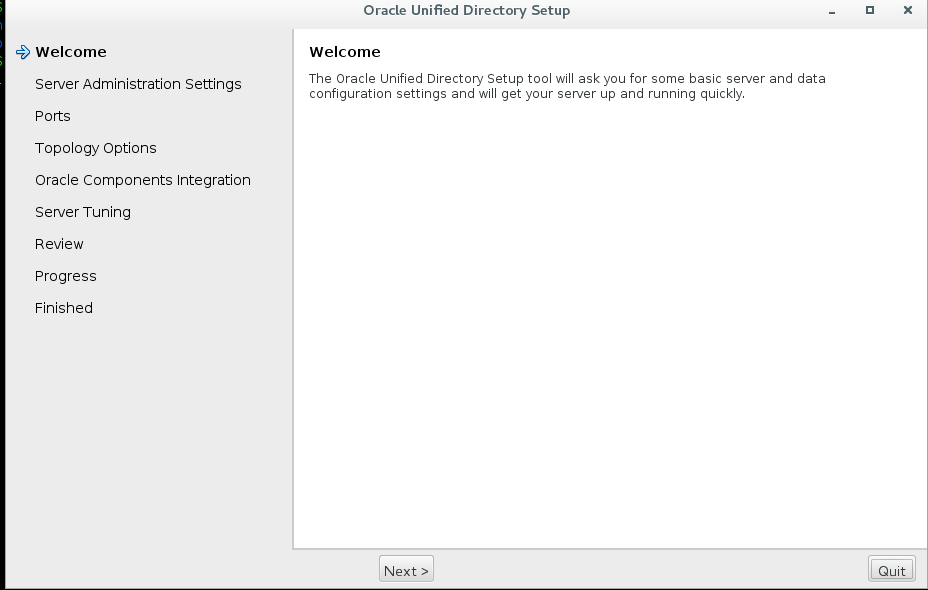
How to Configure OUD



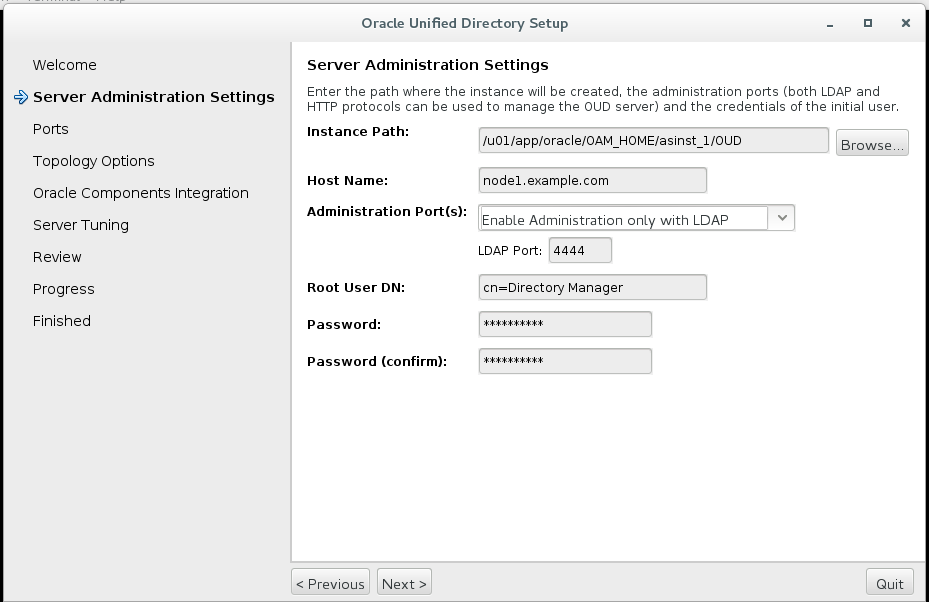
Launch OUD-Setup



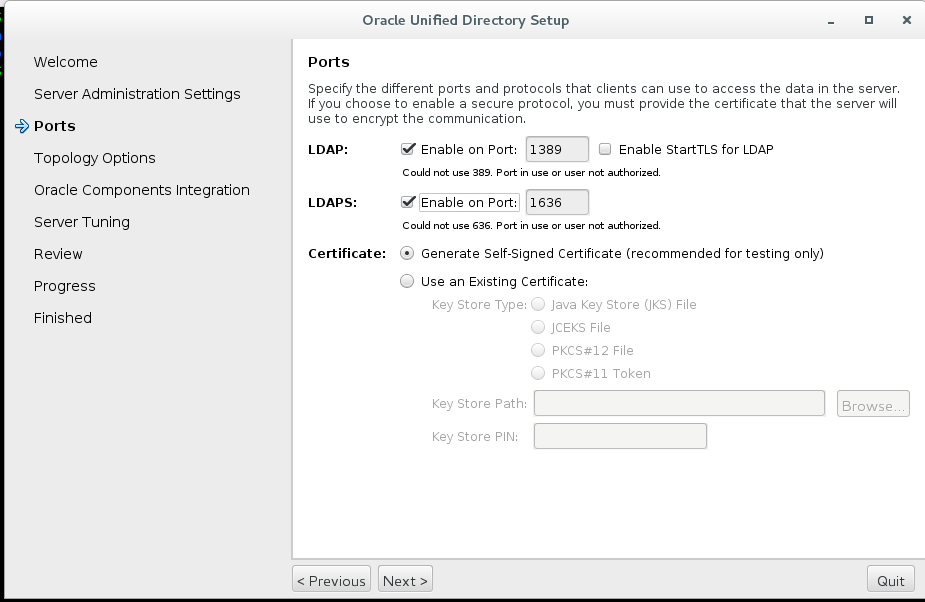
Next



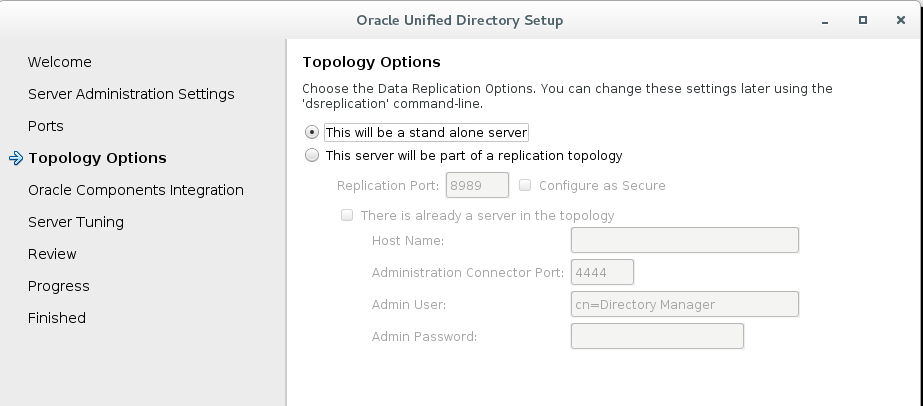
Server Admin Settings



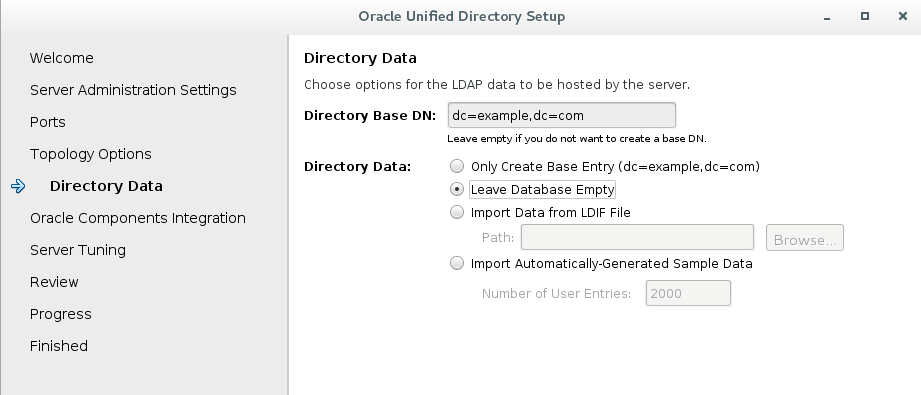
Ports



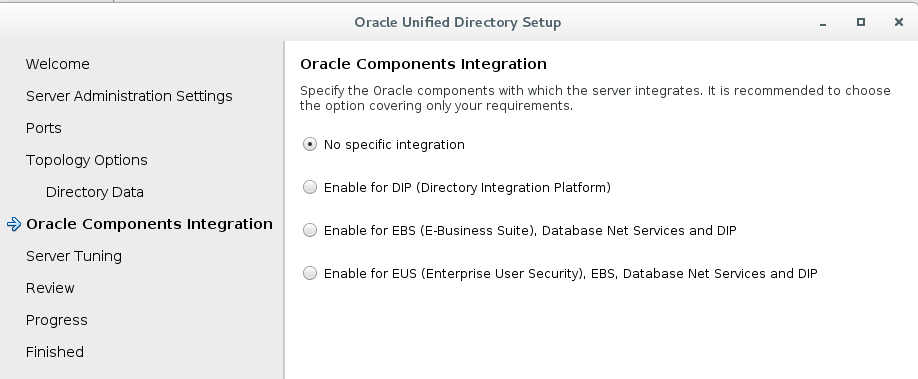
Standalone Server



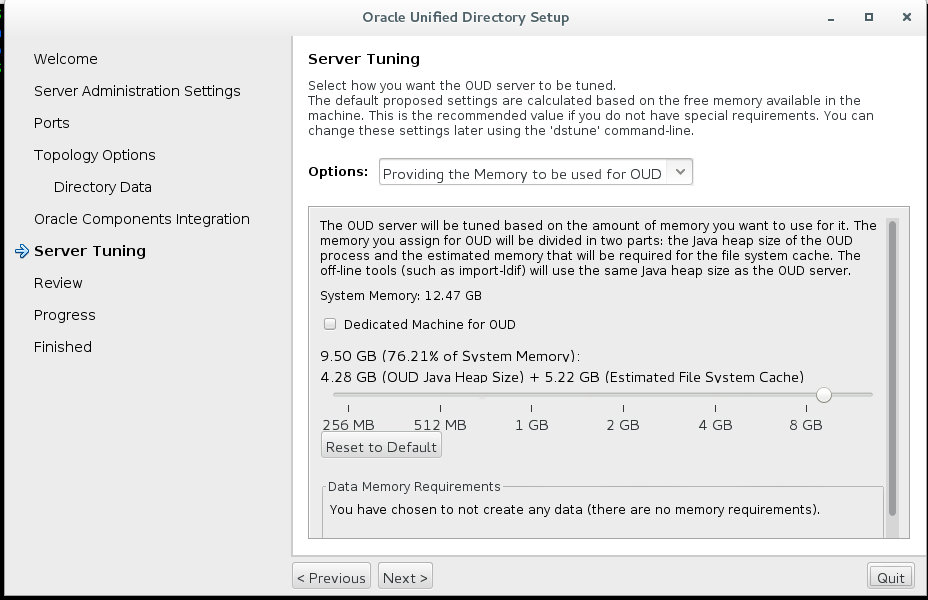
Leave Database empty



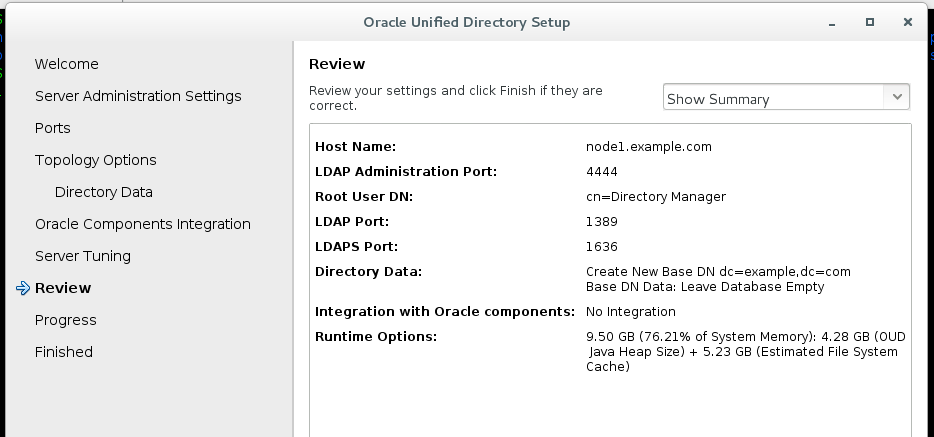
No Specific Integeration



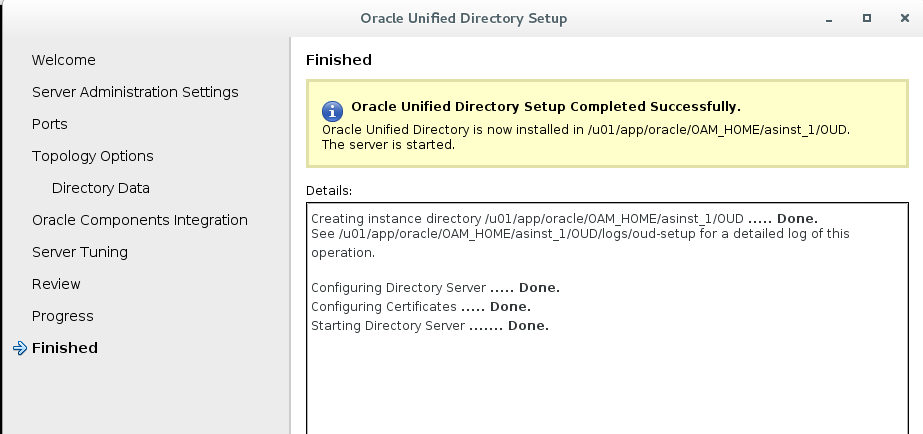
Memory



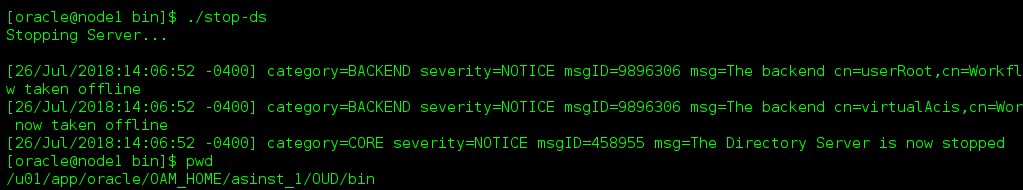
Run Time information



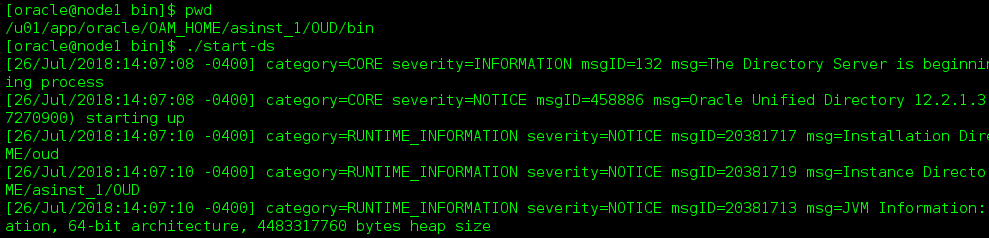
Summary



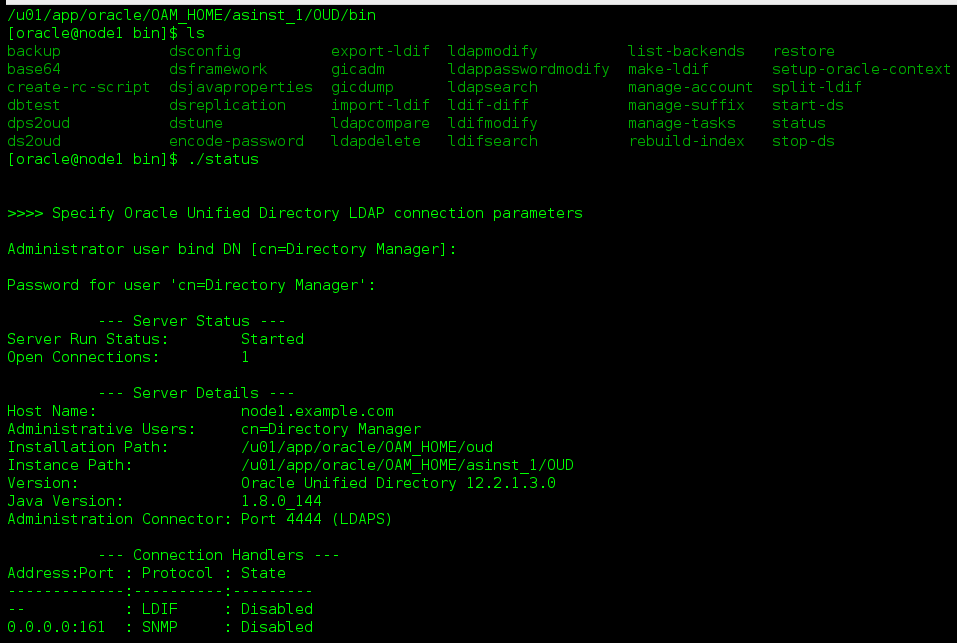
Stop Directory Server



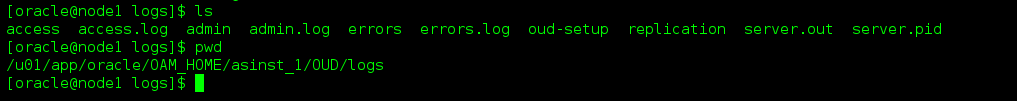
Start Directory Server



Check the status



Logs for OUD



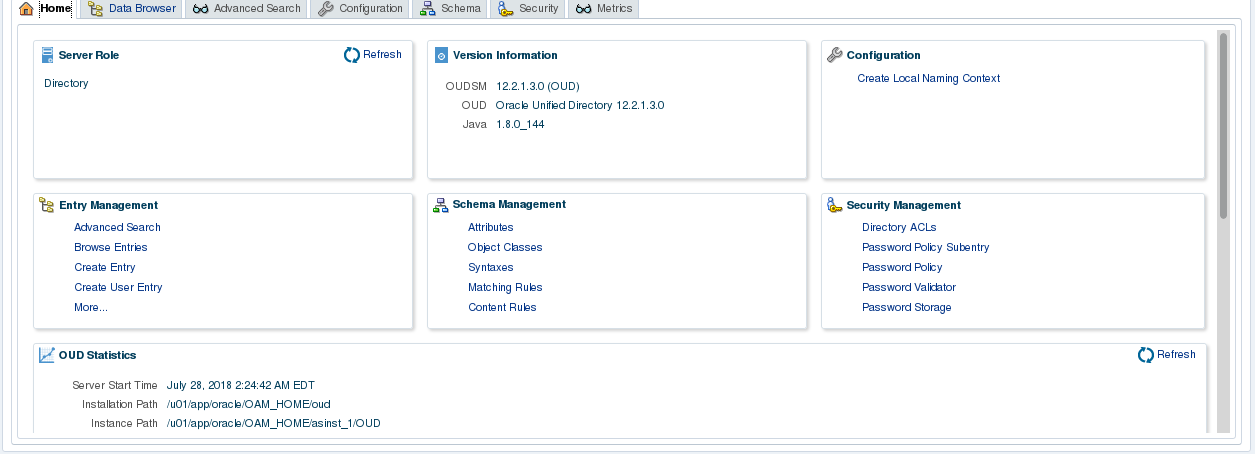
How to import Sample Data



Login to OUDSM after starting Directory server

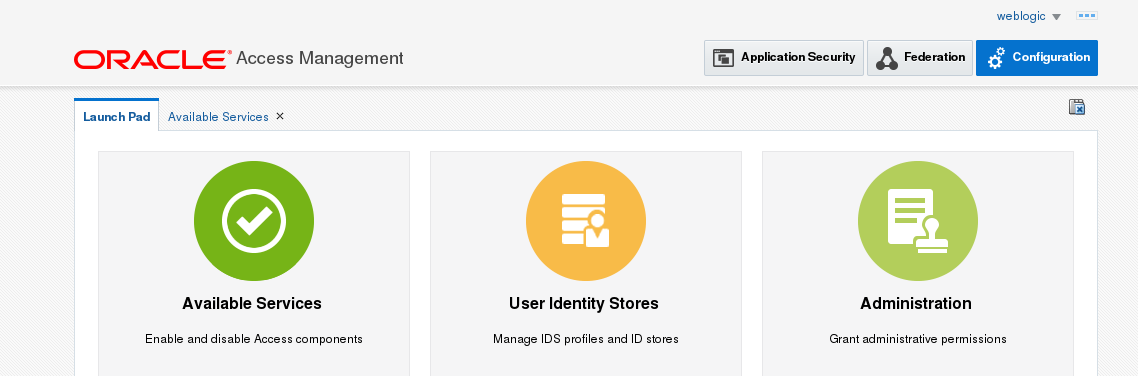


Welcome Page

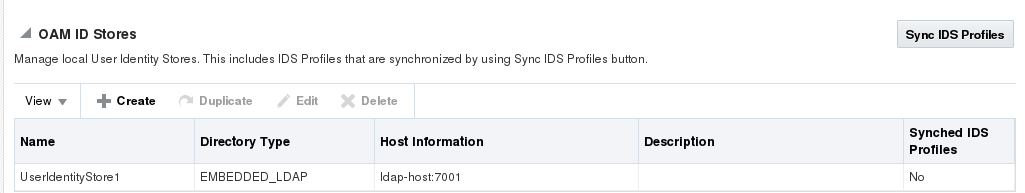


Configure OUD as the Identity Store in OAM

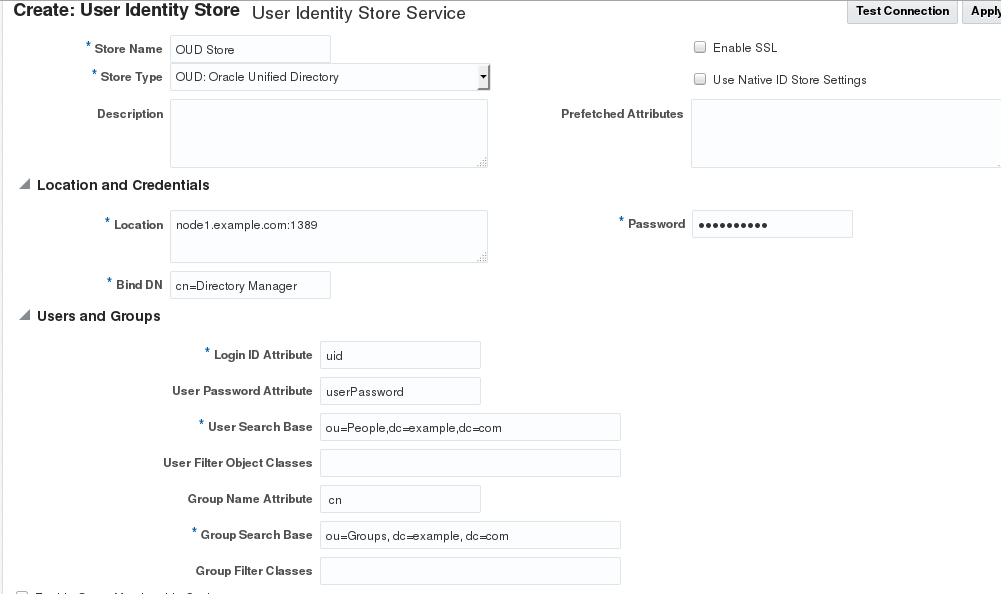
Go to configuration -> User Identity store



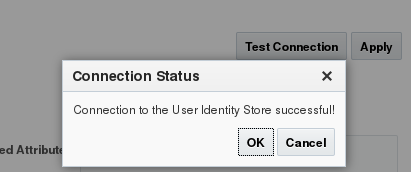
Click create in the OAM ID Store



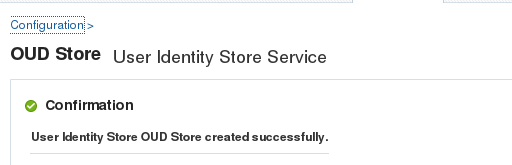
Fill the attributes



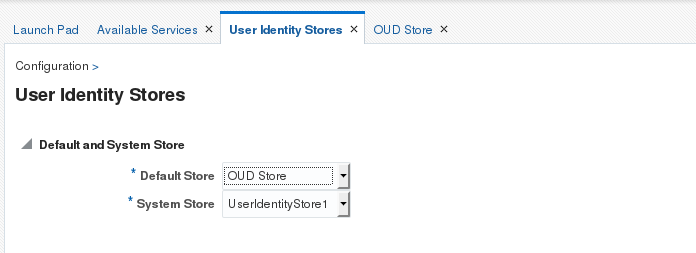
Click Test Connection



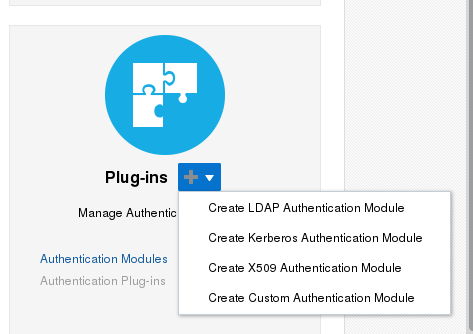
Confirmation



Access the User Identity Stores tab, and set Default Store to OUD\_Store, and then Click Apply.



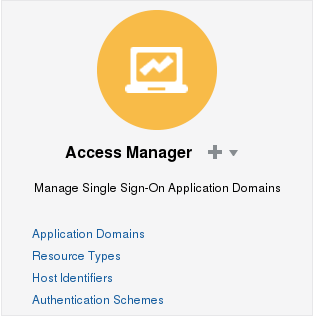
Click Application Security, and then Authentication Modules under the Plug-ins tile.



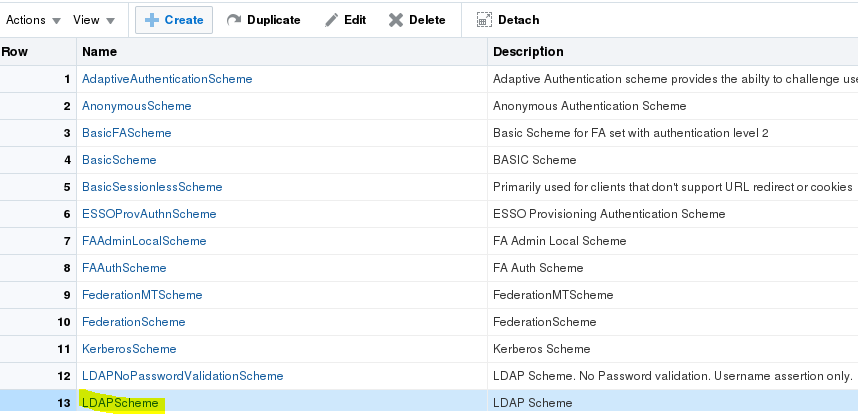


Click the Launch Pad tab, and click the Authentication Schemes link in the Access Manger tile. In the Search Authentication Schemes page, click Search. Select the LDAPScheme row in the search result and click Edit.  
In the LDAPScheme, click Duplicate. It creates a new scheme with the name 'Copy of LDAP Scheme'. Change this scheme as follows, and then click Apply.

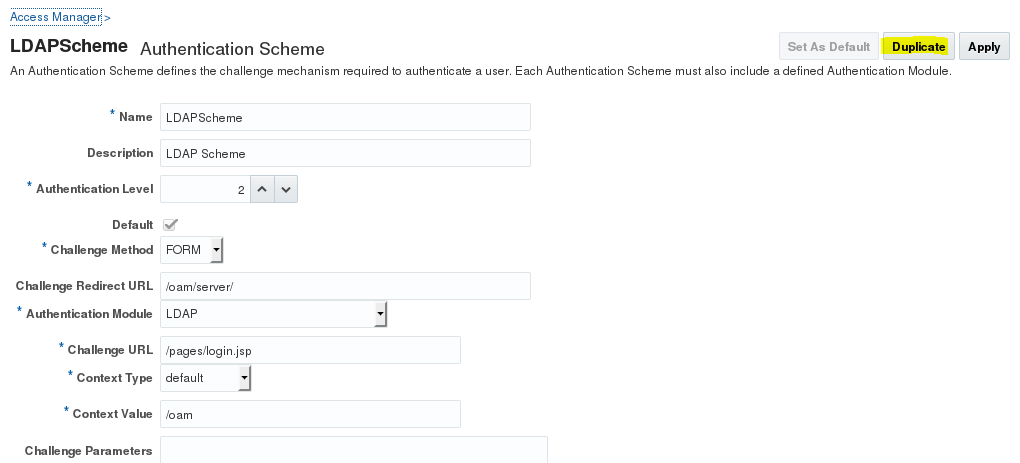
* Name: LDAPOUDScheme
* Description: LDAP Scheme Over OUD
* Authentication Module: LDAPOverOUD



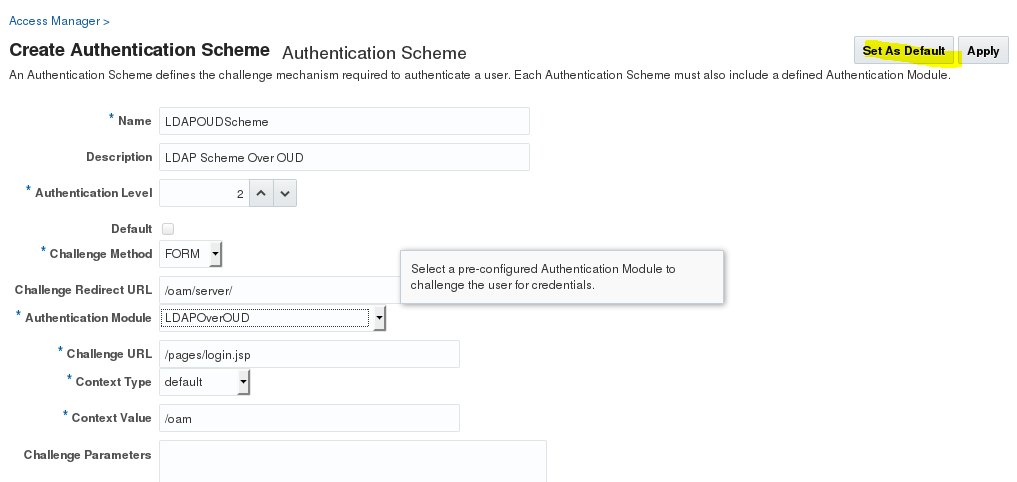
Click LDAP scheme and Edit



Click Duplicate



Change the scheme and set as default



## Configure the Oracle Access Management WebGate

## Navigate to Webgate

## 

## Deploy the Webgate

## 

## Run the command

## 

## Before running the command (Webgate configuration file is missing in OHS)

## 

## After running the command (Webgate configuration file is present in OHS)

## 

## Run the following command

## 

## Output for the above command

## 

## We are running the above command , just to add webgate in OHS configuration

## 

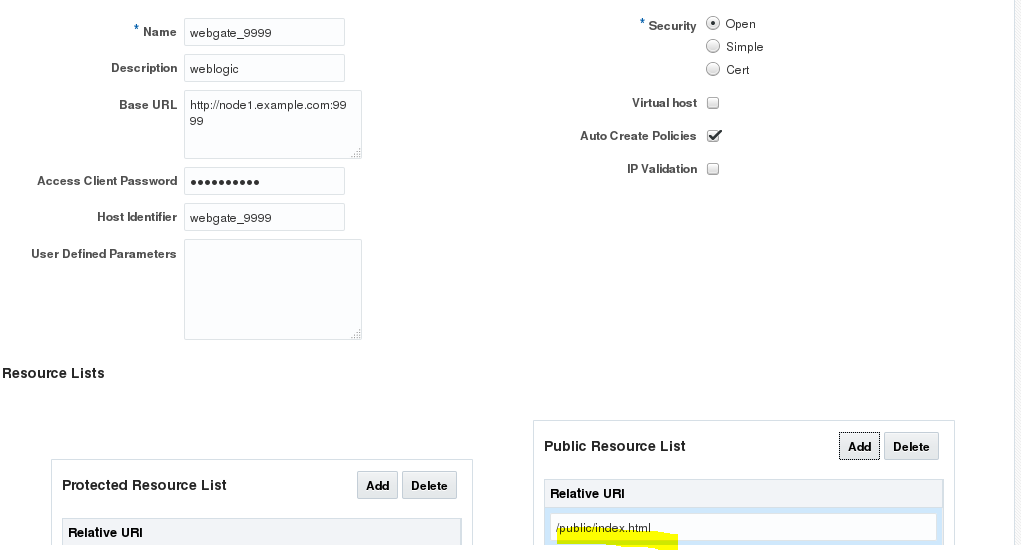
## Register the WebGate with OAM

## 

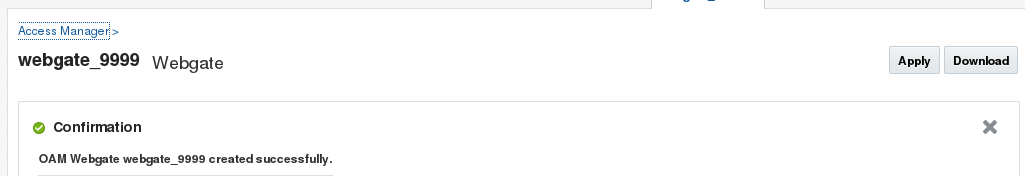
## Click agent type Webgate and click Next

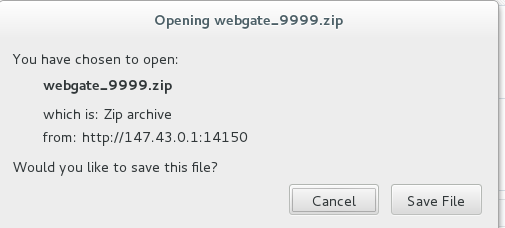
## 

Enter the Details and click Finish

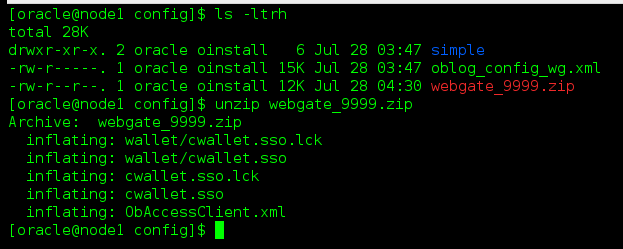


Download the File



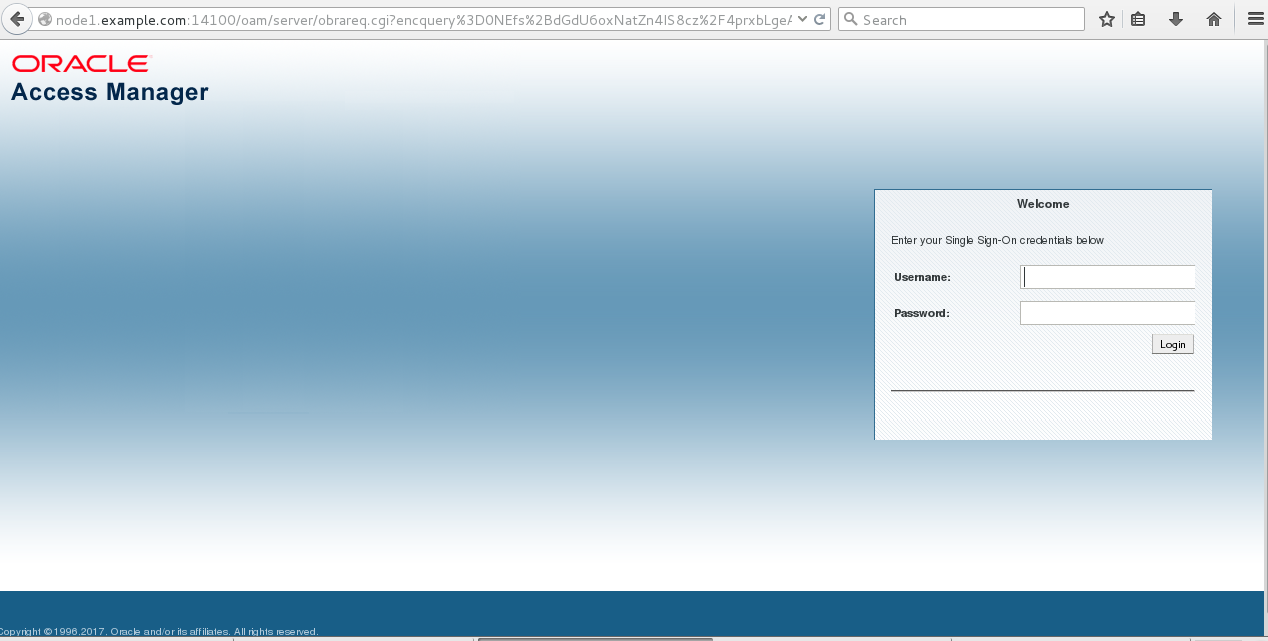


Move the Webgate file



Restart the Servers

Now 147.43.0.1:9999 redirects to OAM SSO console



Enter your credentials and login , you will redirect to OHS server

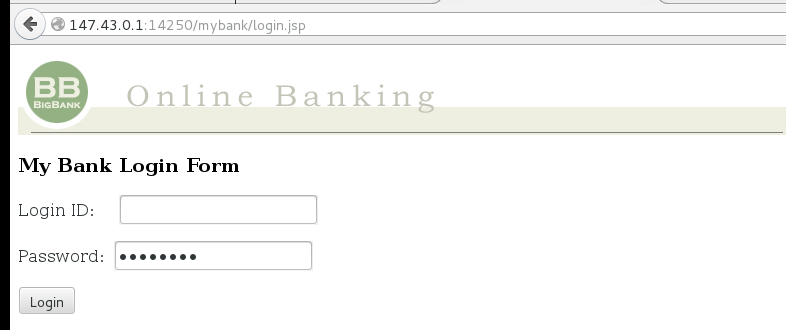


Webgate is protecting your application. Since OAM is registered with Webgate , you are getting OAM SSO page when you launch OHS server( 147.43.0.1:9999)

OHS🡪Webgate🡪OAM( Since webgate configuration is updated in OHS and Webgate is registered with OAM) thats why OAM SSO page

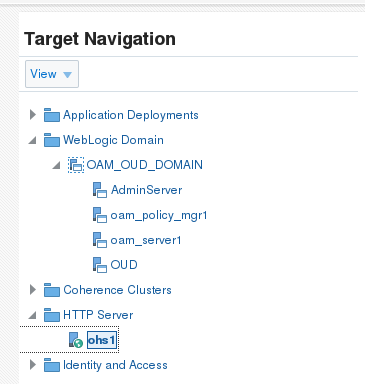
Protect the Application using Webgate

Deploy an application



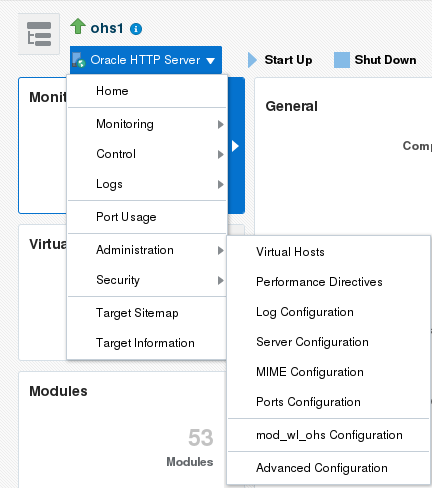
Instead of using MS port, the app must use Load Balancer port 9999

Log into EM and configure mod\_wl\_ohs

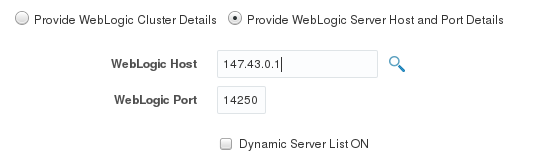


From the Oracle HTTP Server drop down menu select Administration > mod\_wl\_ohs Configuration.

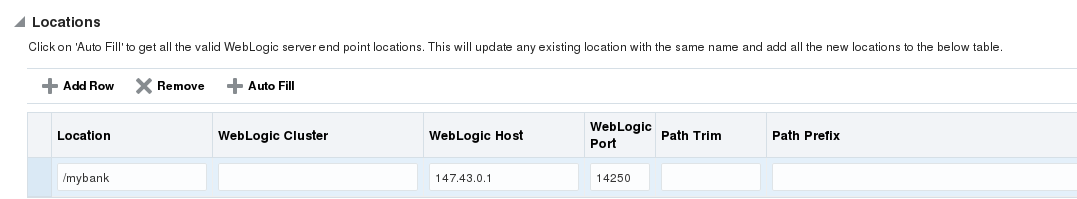
Click the unlocked padlock icon in the top right of the page and select Lock and Edit.



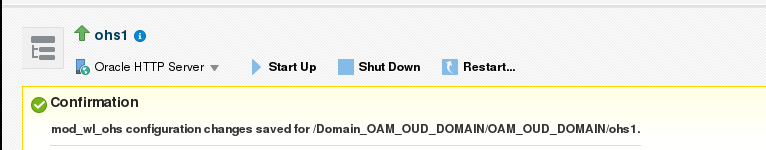
Enter web logic host and port details



Location details

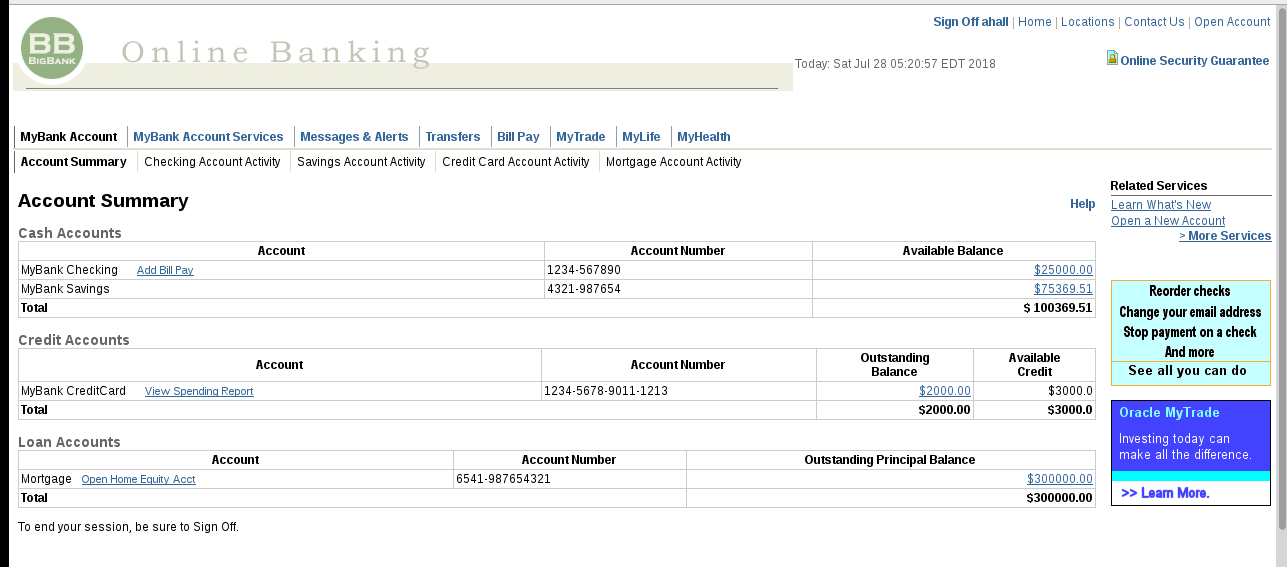


After applying, restart the OHS server



Now application is accessible via Load Balancer

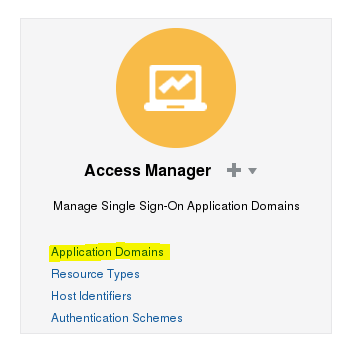
**Note**: As all OHS pages are currently protected via Oracle Access Management, you should be redirected to the OAM SSO login page (notice that the redirect URL now points to OAM server 14100 port hosted on the OAM machine).



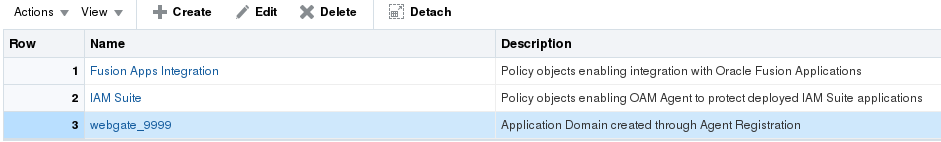
By default webgate protects all application that are accessible by OHS server( 147.43.0.1:9999)

Protect only mybank application

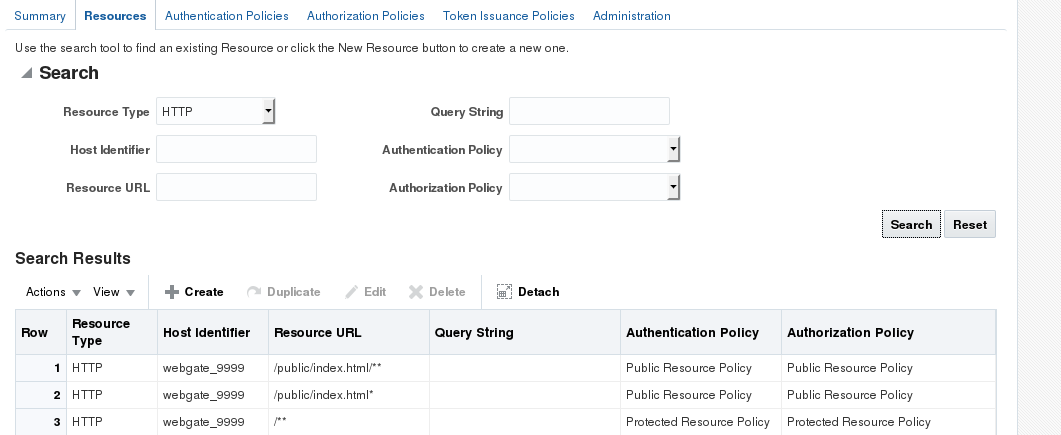
Login into OAM Console



Click Webgate



Then Resources

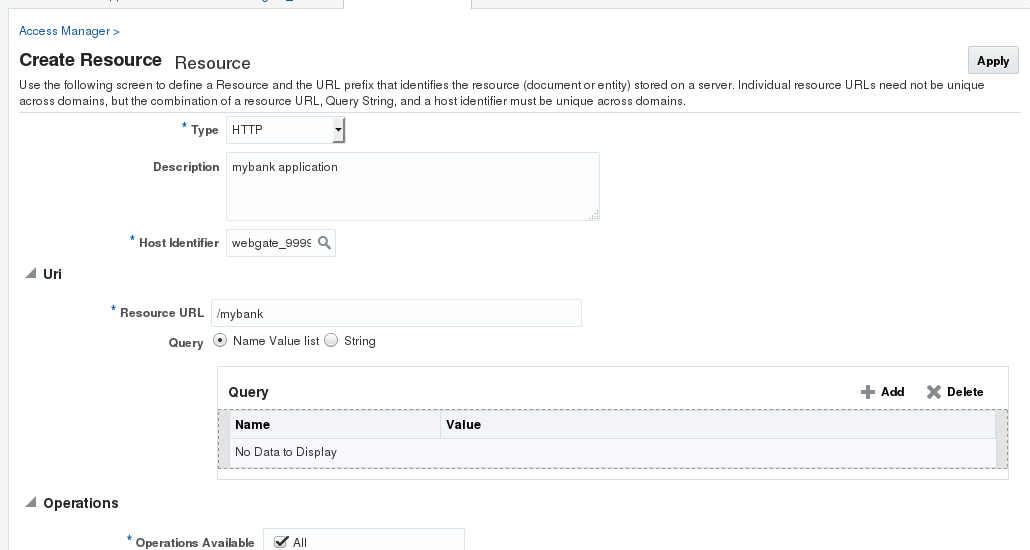


1. Under **Protection**, set **Protection Level** to **Excluded**. Click **Apply**.
2. On the **Resources** tab select the Resource URL **/\*\*** and click **Edit**. Change **Protection Level** to **Excluded** and then click **Apply**. Changing Protection Level to Excluded means that all URL's under http://oam.example.com:7777are now unprotected.
3. Close the current tabs to return to the **webgate\_7777**Resources tab.
4. Set up a policy to protect the mybank application /mybank, by clicking **Create**. Create the /mybank resource as follows and click **Apply**:

Set up a policy to protect the mybank application /mybank, by clicking **Create**. Create the /mybank resource as follows and click **Apply**:

|  |  |
| --- | --- |
| **Name** | **Value** |
| Type | HTTP |
| Description | mybank application |
| Host Identifier | webgate\_7777 |
| Resource URL | /mybank |
| Protection Level | Protected |
| Authentication Policy | Protected Resource Policy |
| Authorization Policy | Protected Resource Policy |

Create Resource to Protect Mybank app alone



And mybank is accessible

