Application Installation Guide

Oracle Financial Services Lending and Leasing

Release 14.7.0.0.0

Part No. F16599-01

May 2019

ORACLE

Application Installation Guide
May 2019
Oracle Financial Services Software Limited

Oracle Park

Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India
Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax:+91 22 6718 3001
https://www.oracle.com/industries/financial-services/index.html

Table of Contents

1. Preface

This document contains notes and installation steps needed to install and setup Oracle Financial Services Lending and Leasing. Oracle Financial Services Lending and Leasing relies on several pieces of Oracle software in order to run and this document is in no way meant to replace Oracle documentation supplied with these Oracle products or available via Oracle technical support. The purpose of this document is only meant to supplement the Oracle documentation and to provide Oracle Financial Services Lending and Leasing specific installation instructions.

For recommendations on security configuration, refer Security Configuration Guide.

It is assumed that anyone installing Oracle Financial Services Lending and Leasing will have a thorough knowledge and understanding of Oracle Weblogic Server 12c, Oracle BI Publisher 12c.

Application installation consists of following steps.

- Installing Software
- Creating Domains, Repositories, Data Sources
- Configuring Policies
- Deploying Application
- Enabling SSL
- Mapping Enterprise Group with Application Role
- Configuring JNDI name for HTTP Listener
- Configure AQ-JMS Bridge
- Configuring Oracle BI Publisher for Application
- Launching Application
- Installing Upgrade

1.1 Prerequisites

The following software are required to install Oracle Financial Services Lending and Leasing application and they are available from the following sources:

- Oracle Software Delivery Cloud (http://edelivery.oracle.com/)
- Oracle Technology Network (OTN)

1. JDK Version 1.8.0_202 or above (https://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html)
2. Oracle WebLogic Server 12c Version 12.2.1.3.0 (http://www.oracle.com/technetwork/middleware/weblogic/downloads/index.html)
   Navigate to Fusion Middleware Infrastructure Installer.
3. JVM/JDK are to be downloaded and installed prior to installing the Weblogic Server.
4. The patches for Fusion Middleware 12.2.1.3.0 with the following patch numbers are to be applied - 23741897, 27438258 and 28561620.

Note

Please use all 64-bit software's for machine hosted with 64-bit O/S.

1.2 Audience

This document is intended for system administrators or application developers who are installing Oracle Financial Services Lending and Leasing Application.

1.3 Conventions Used

Term	Refers to
Application	Oracle Financial Services Lending and Leasing

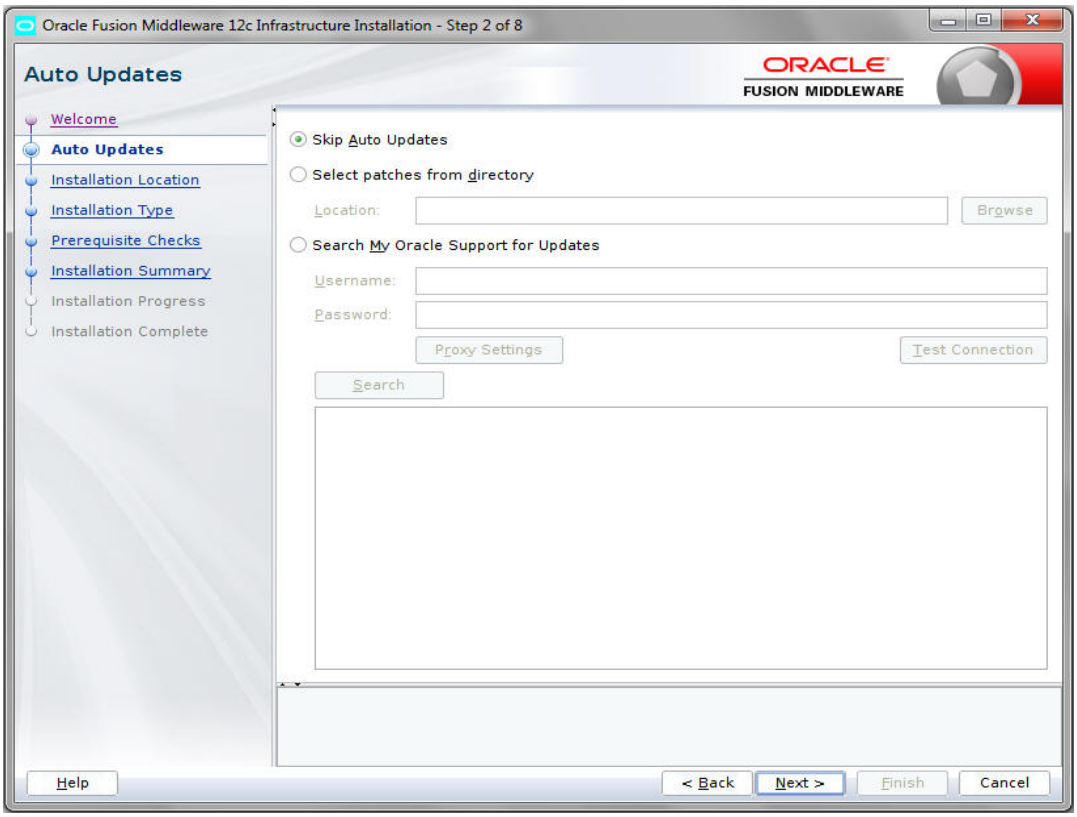
2. Installing Software

2.1 Installing Oracle WebLogic Server 12c

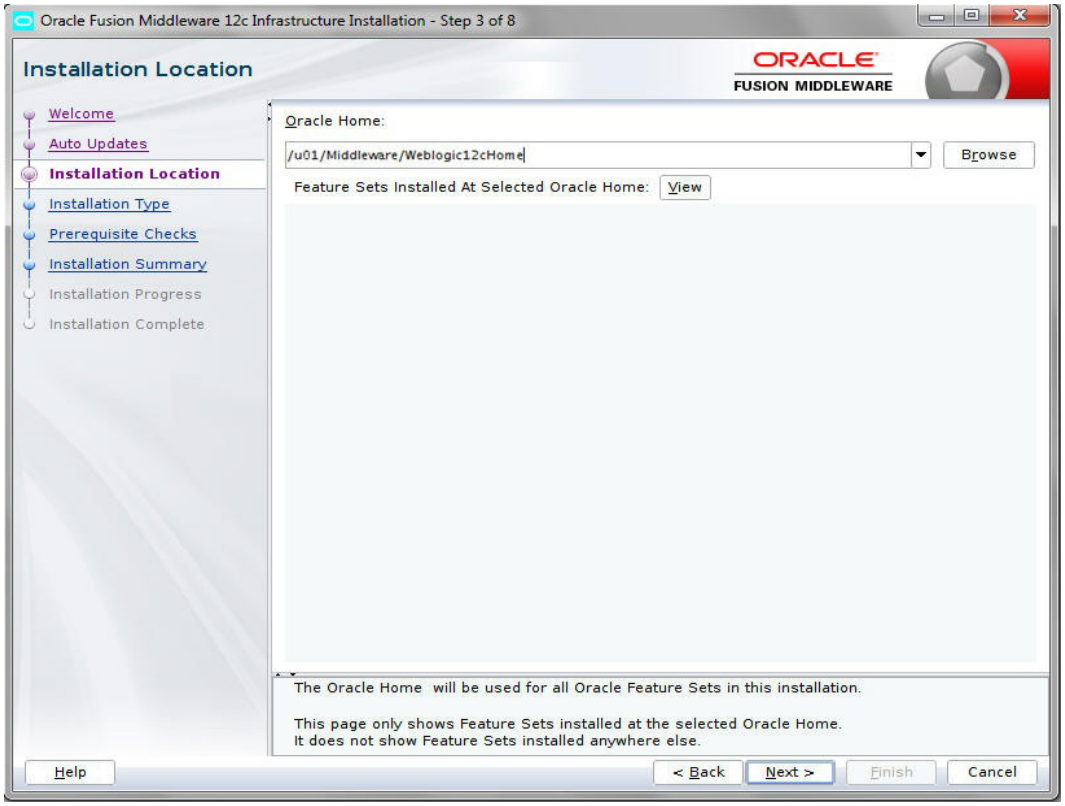
To install using generic Weblogic installer

1. Run the command > java -jar fmw_12.2.1.3.0_infrastructure.jar
2. Welcome screen is displayed as shown below. Click Next.

3. The following window is displayed.

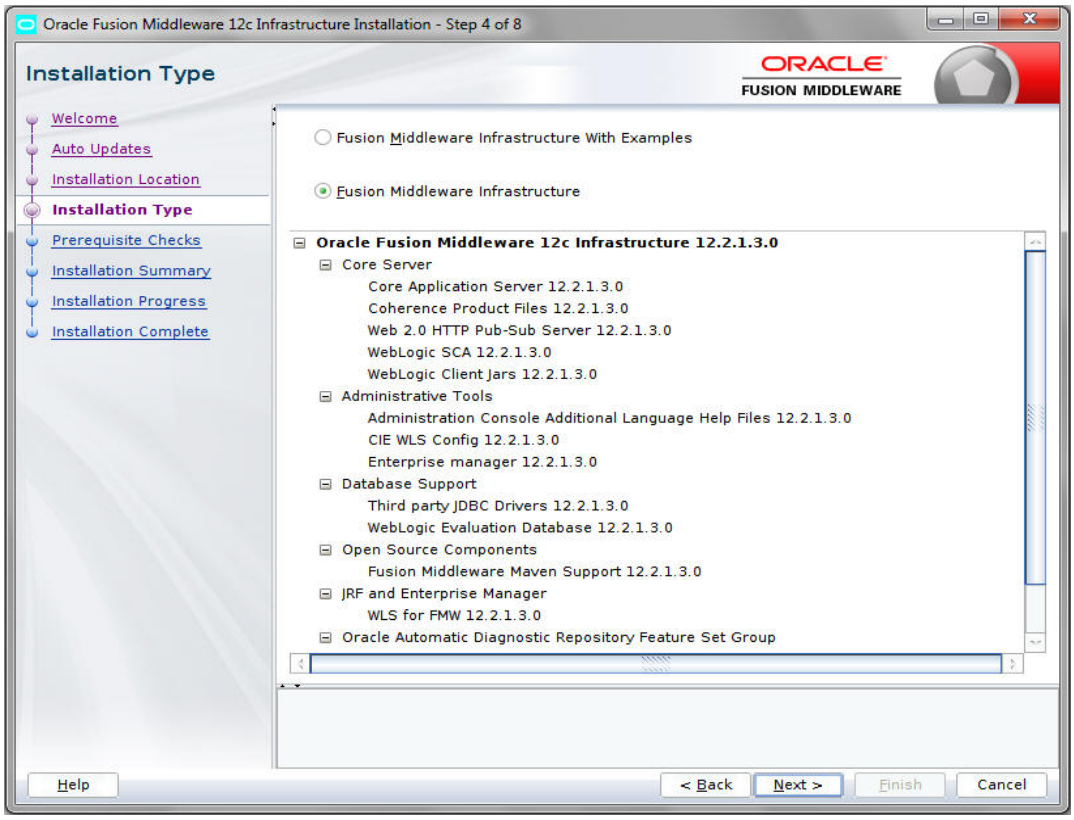


4. Select ‘Skip Auto Updates’ and Click ‘Next’.

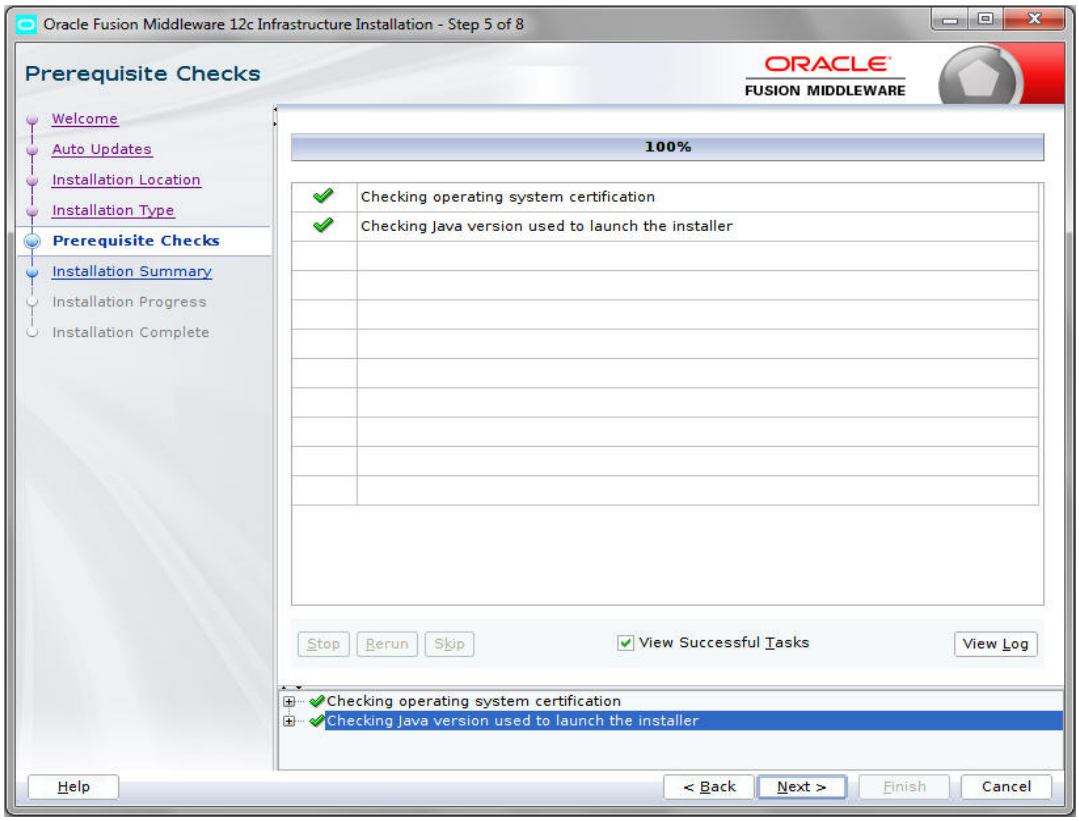


5. Specify the path for Middleware Home Directory.

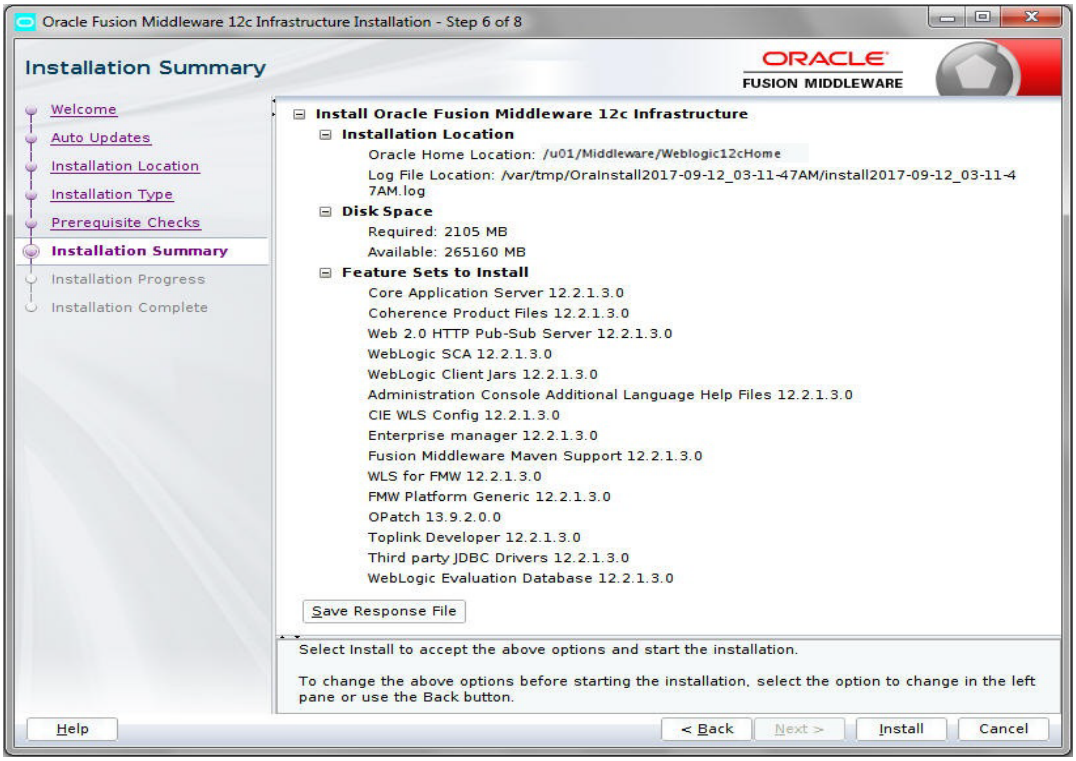
6. Click ‘Next’. The following window is displayed.



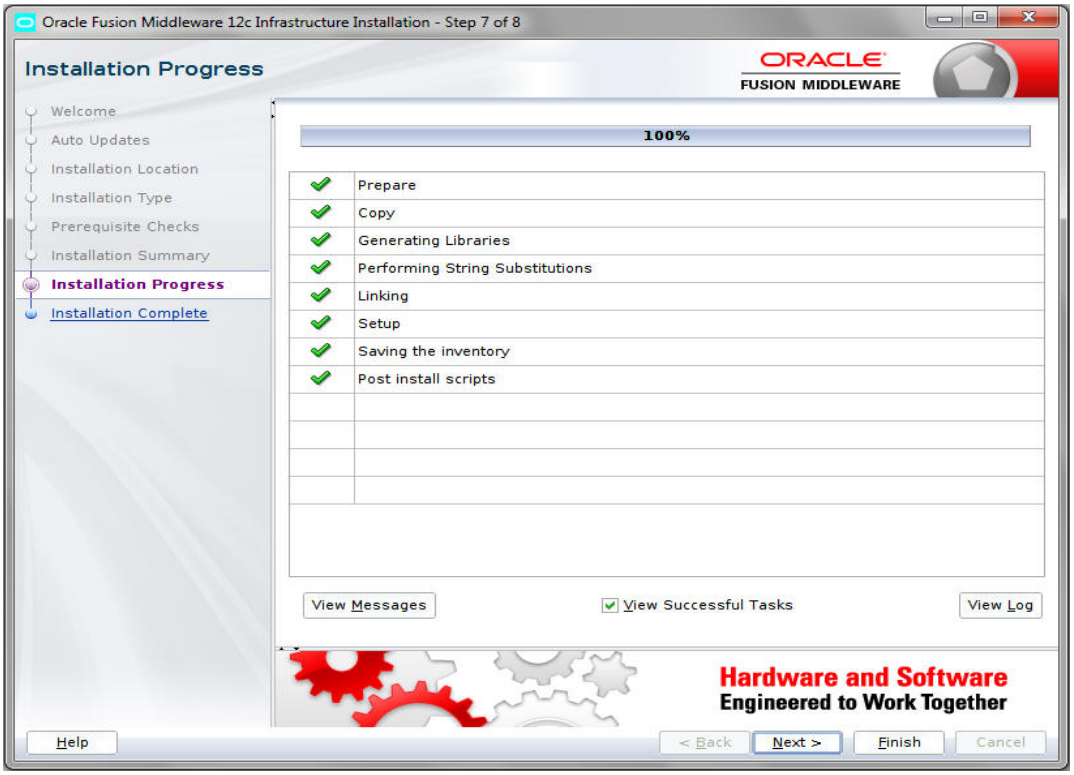
7. Select the option ‘Fusion Middleware Infrastructure’. Click ‘Next’.



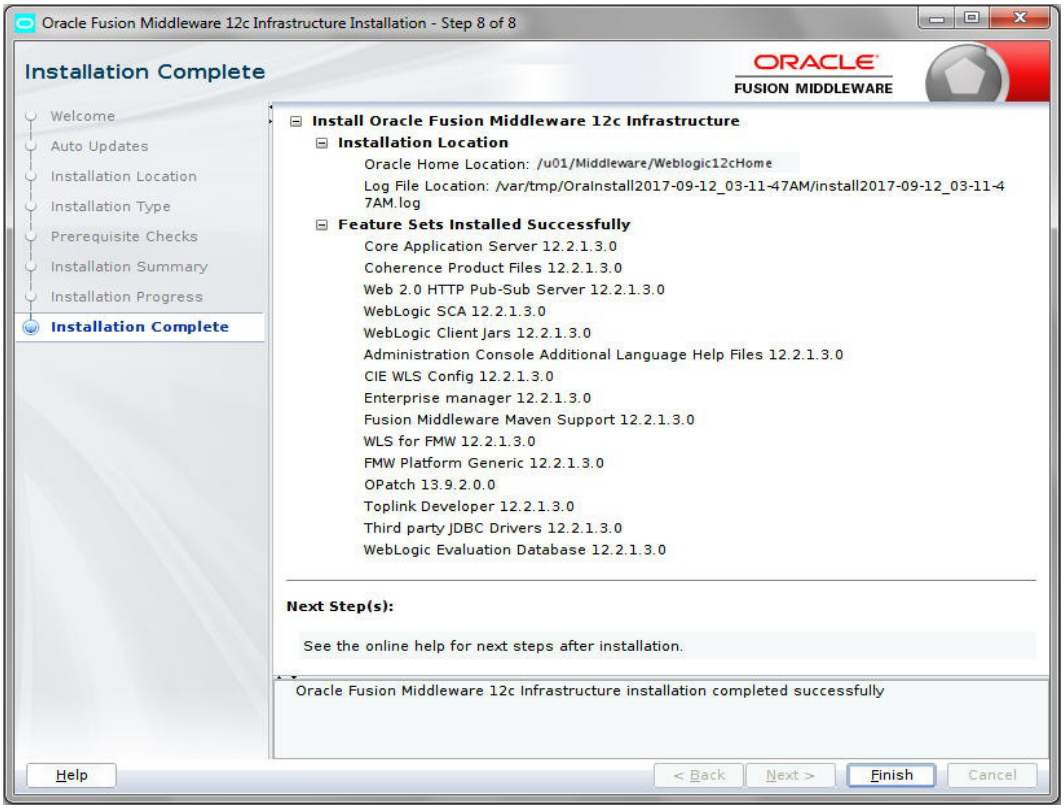
8. Click ‘Next’. The following window is displayed.



9. Click ‘Next’. The following window is displayed.



10. Click ‘Install’. The weblogic installation starts. Once done, the following window is displayed.

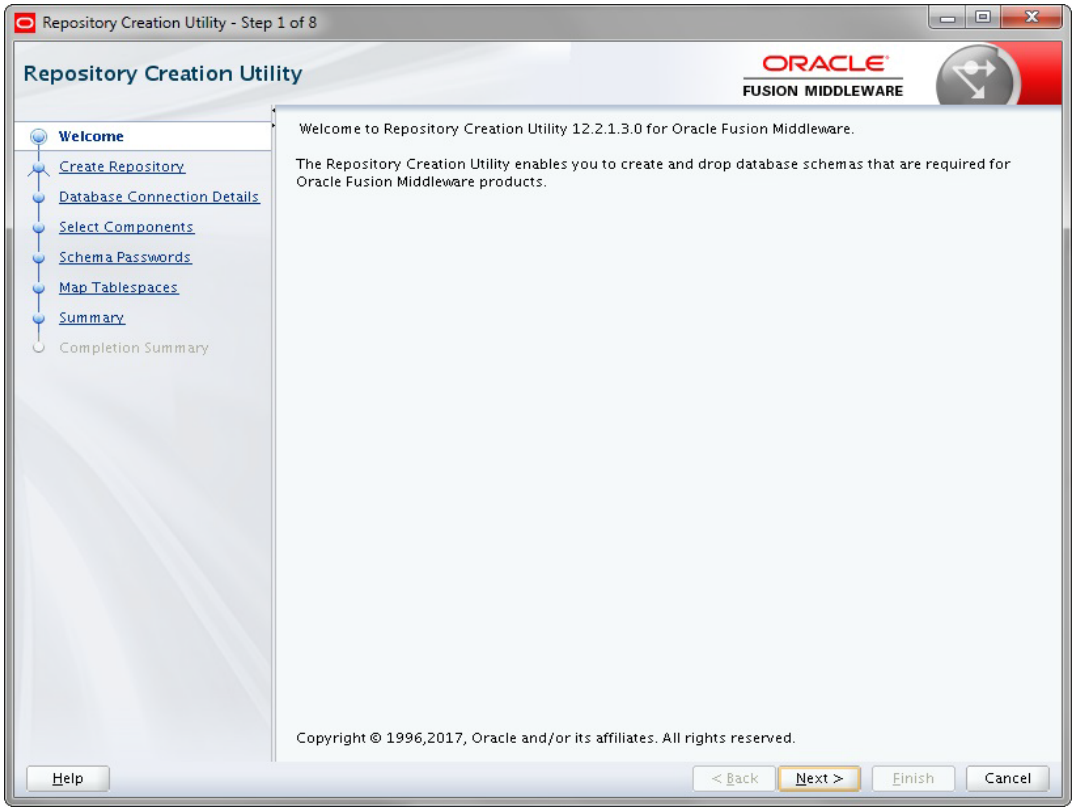


11. Click ‘Finish’ to close the window.

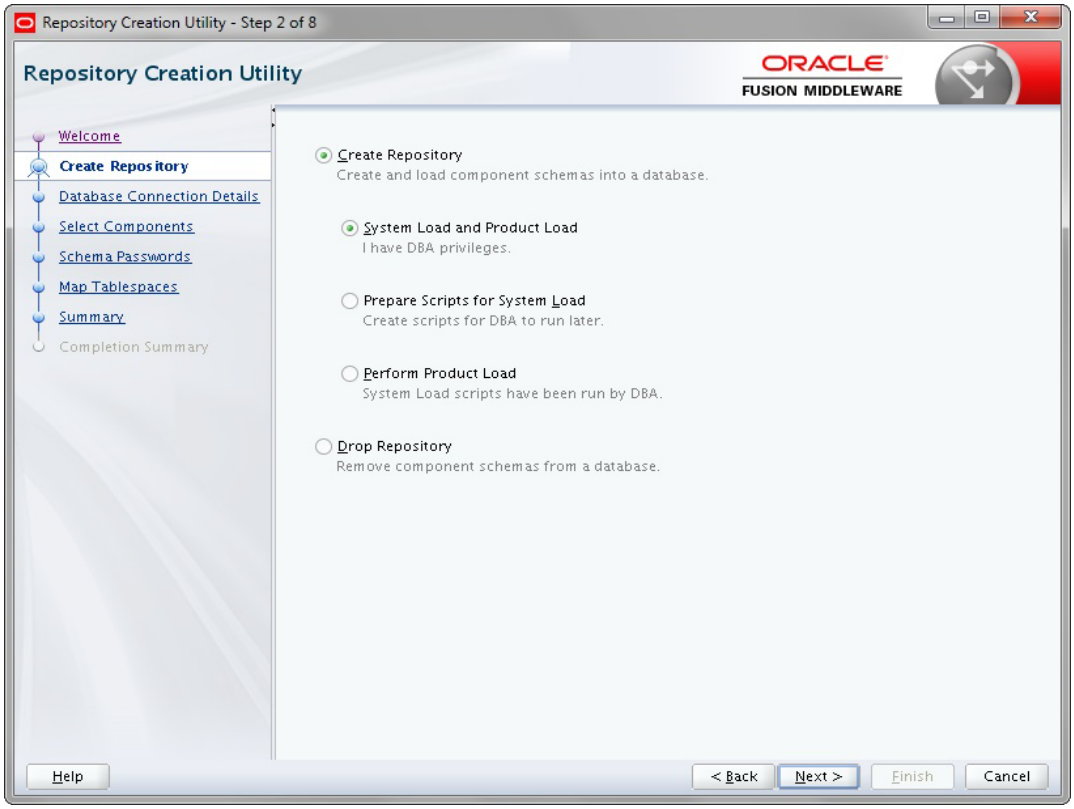
3. Creating Domains, Repositories, Data Sources

3.1 Creating Schemas using Repository Creation Utility

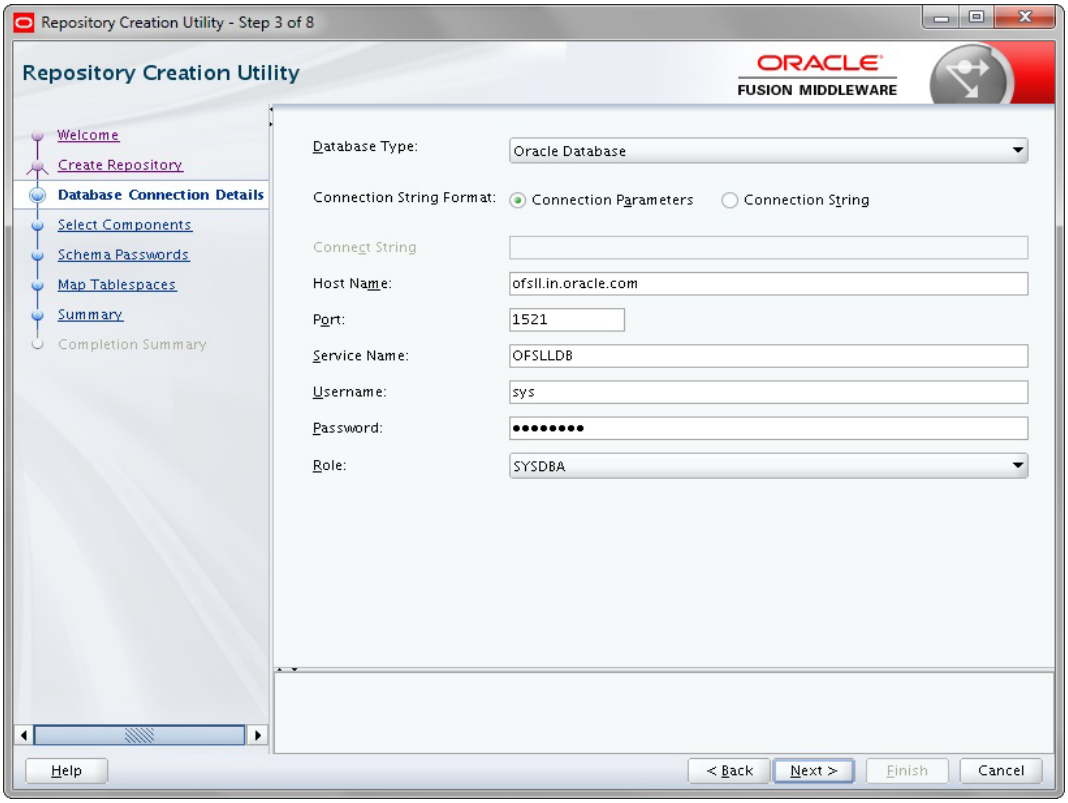
1. Open command prompt on Unix and browse to <WL_HOME>/oracle_common/bin and run ./rcu. The following window is displayed.



2. Click ‘Next’. The following window is displayed.



3. Select ‘Create Repository’ and select ‘System Load and Product Load’. Click ‘Next’. The following window is displayed.

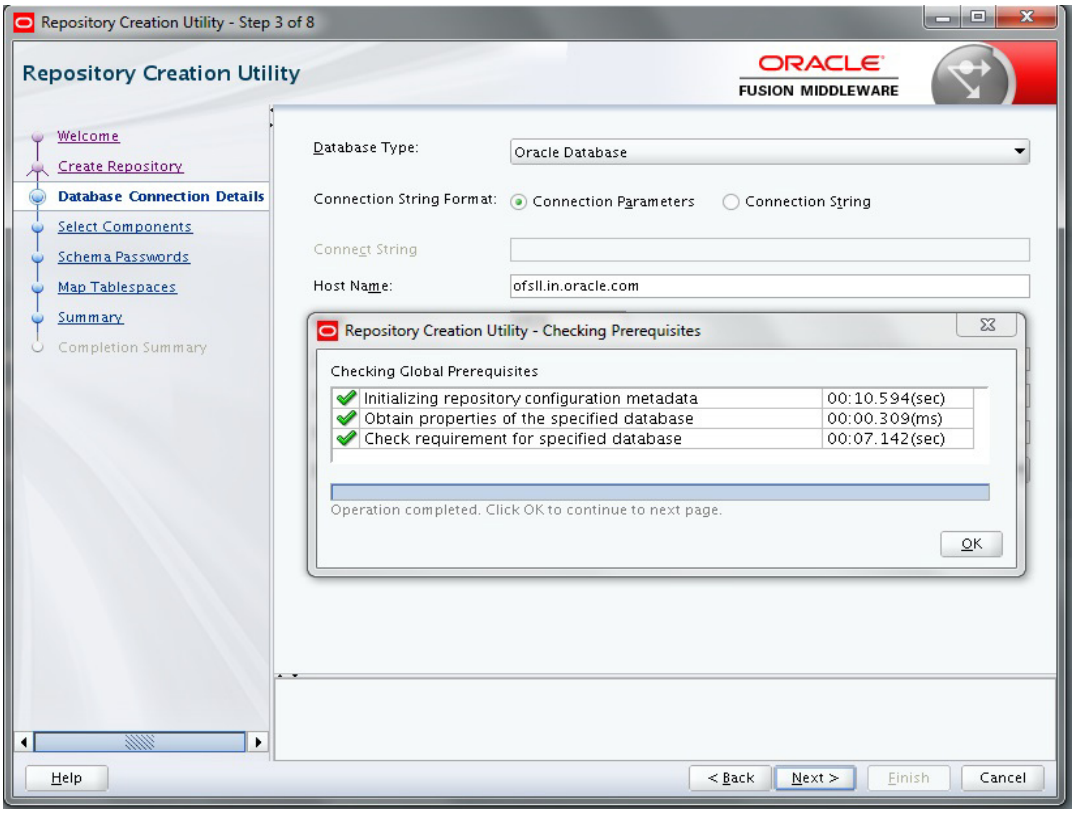


4. Provide database details where you want to create schemas, as shown in the above screen.

Note

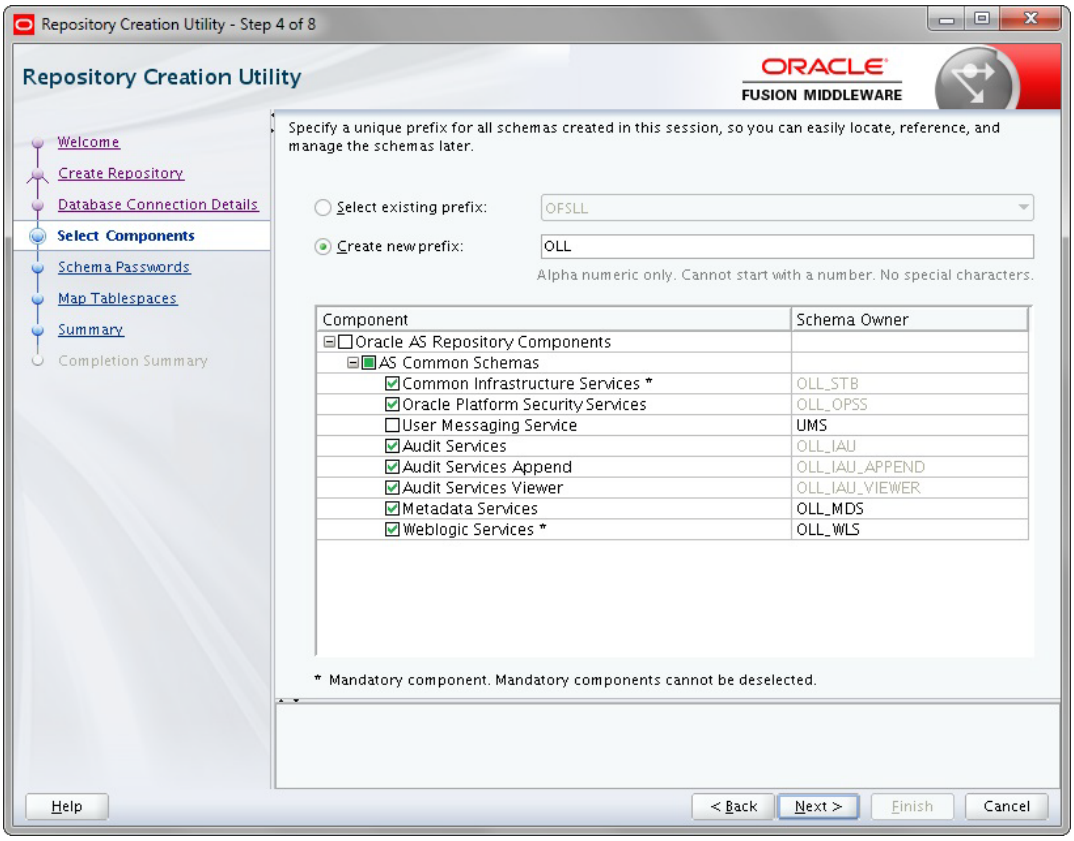
You will require a user with SYSDBA role to create schemas.

5. Click ‘Next’. The following window is displayed.

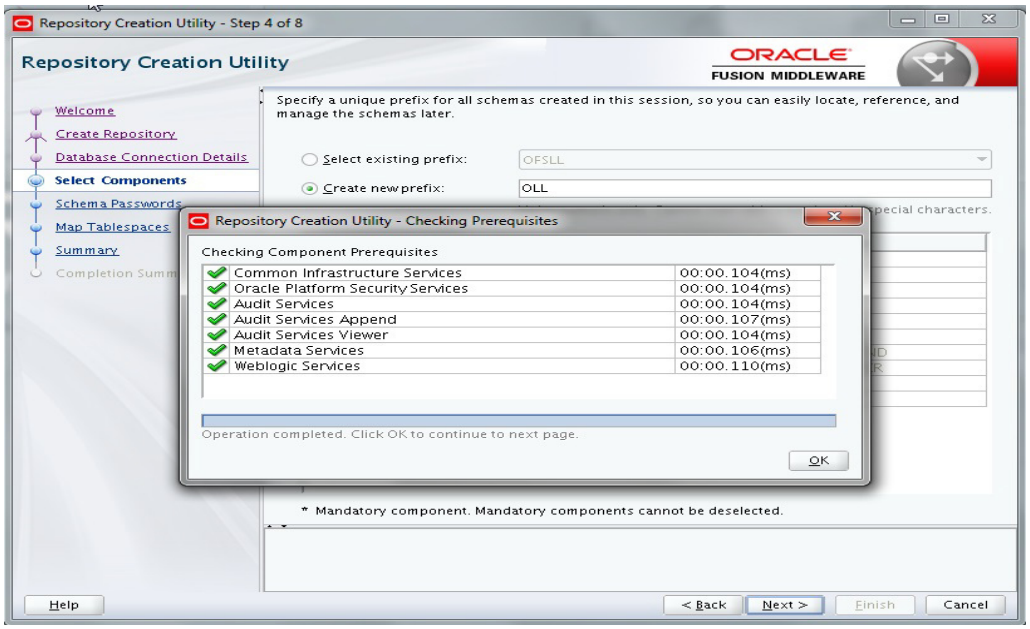


6. Click ‘OK’ in the confirmation dialog.

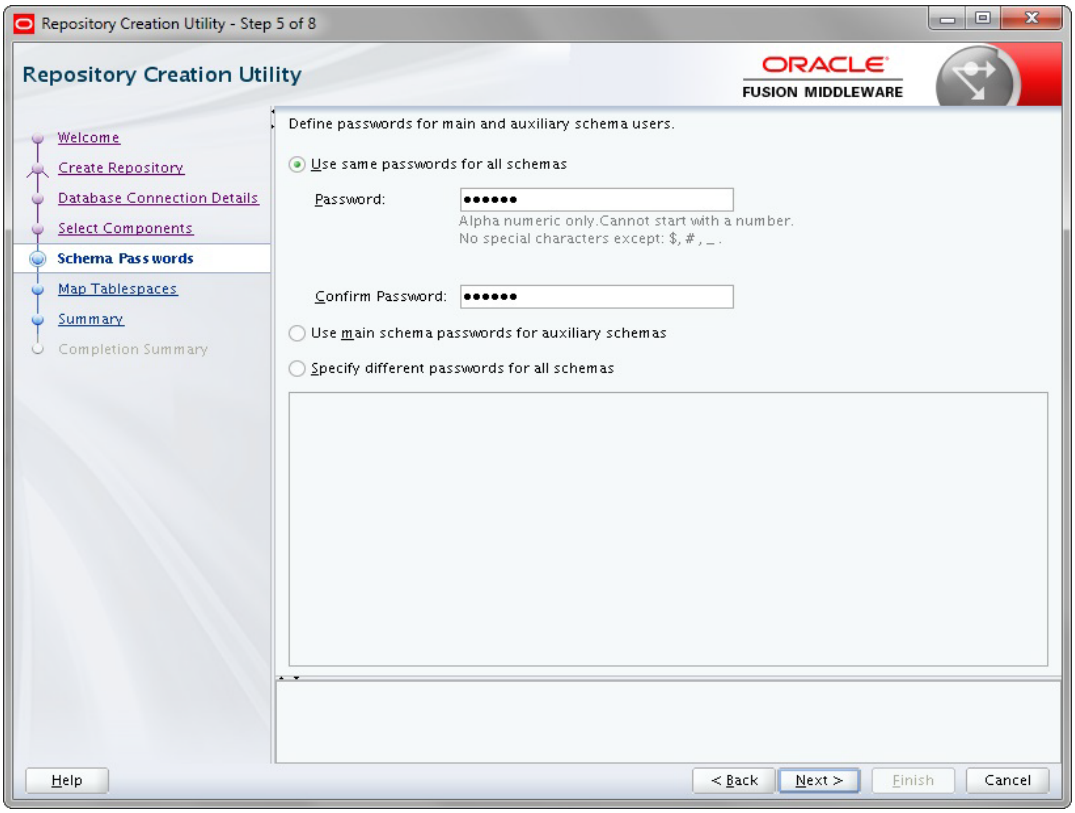
7. Click ‘Next’ the following window is displayed.



8. Select ‘Create new Prefix’ option and specify the value. For example, OLL.
9. Select the options ‘Metadata Services’ and ‘Oracle Platform Security Services’ as shown in the above screen. Click ‘Next’. The following window is displayed.

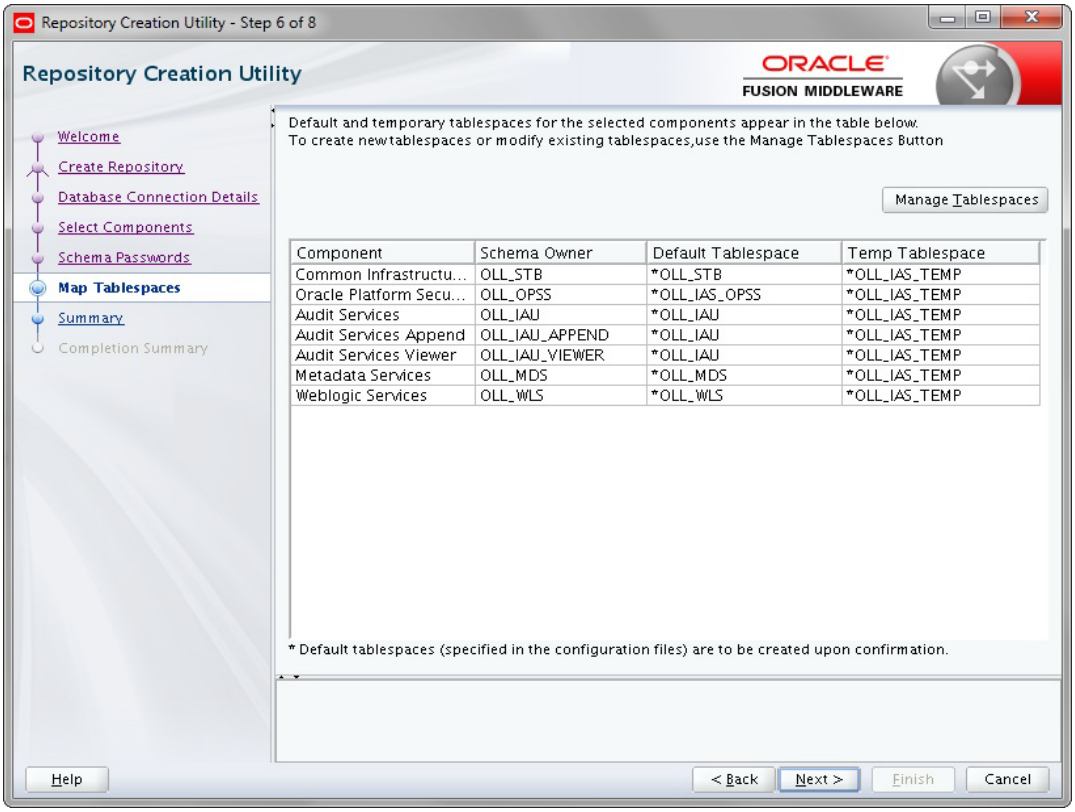


10. Click ‘Next’. The following window is displayed.

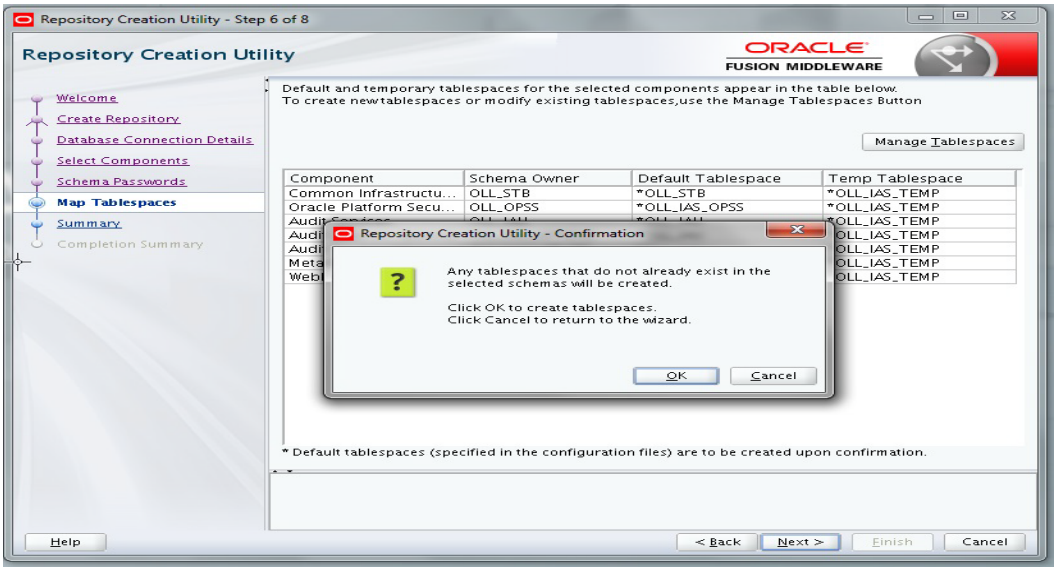


11. You can select one of the following:
    - Select ‘Use same password for all schemas’ and specify the password.
    - Select ‘Specify different passwords for all schemas’ and specify Schema Passwords for each schema.

12. Click ‘Next’. The following window is displayed.

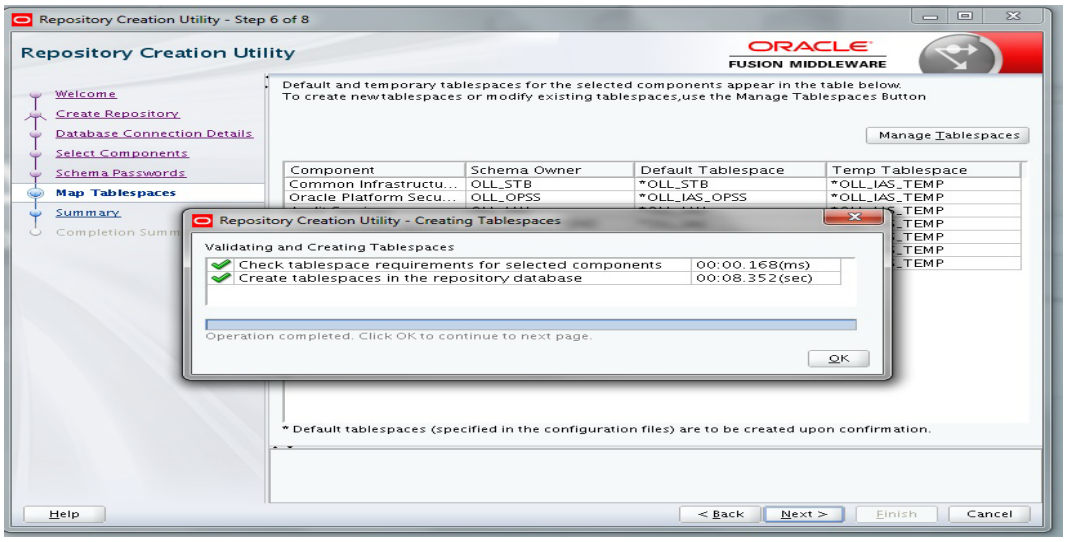


13. Click ‘Next’. The following window is displayed.

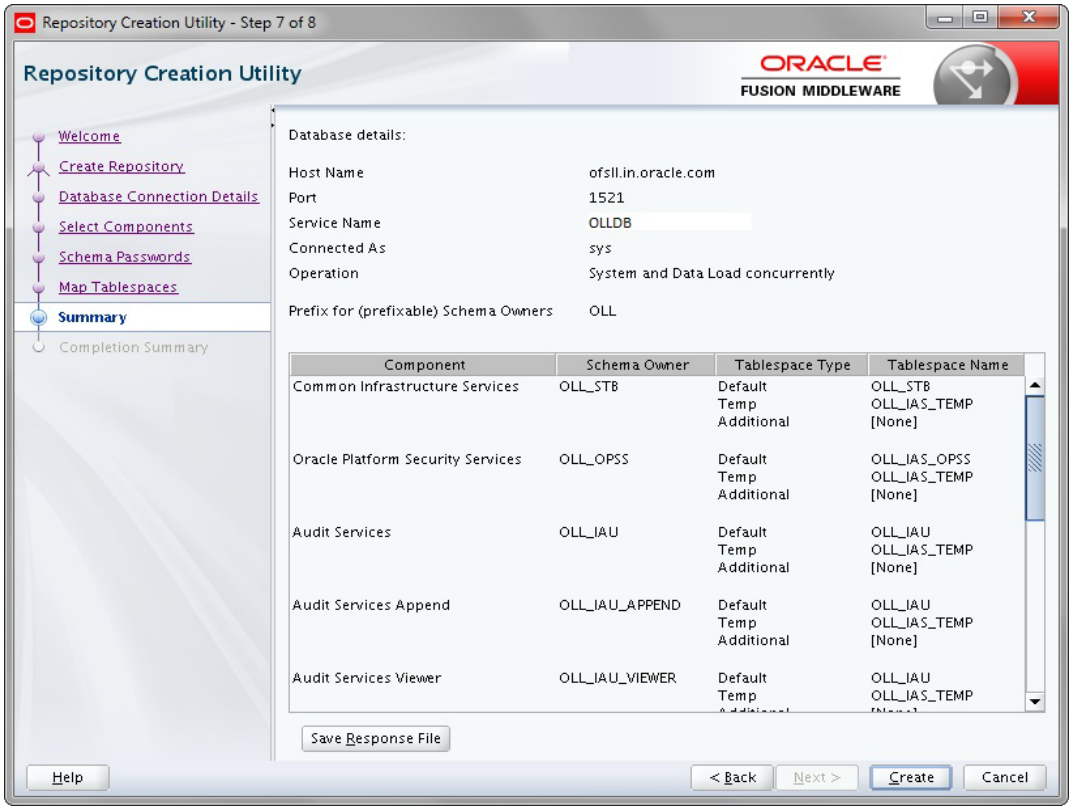


14. Click ‘OK’ in the confirmation dialog.

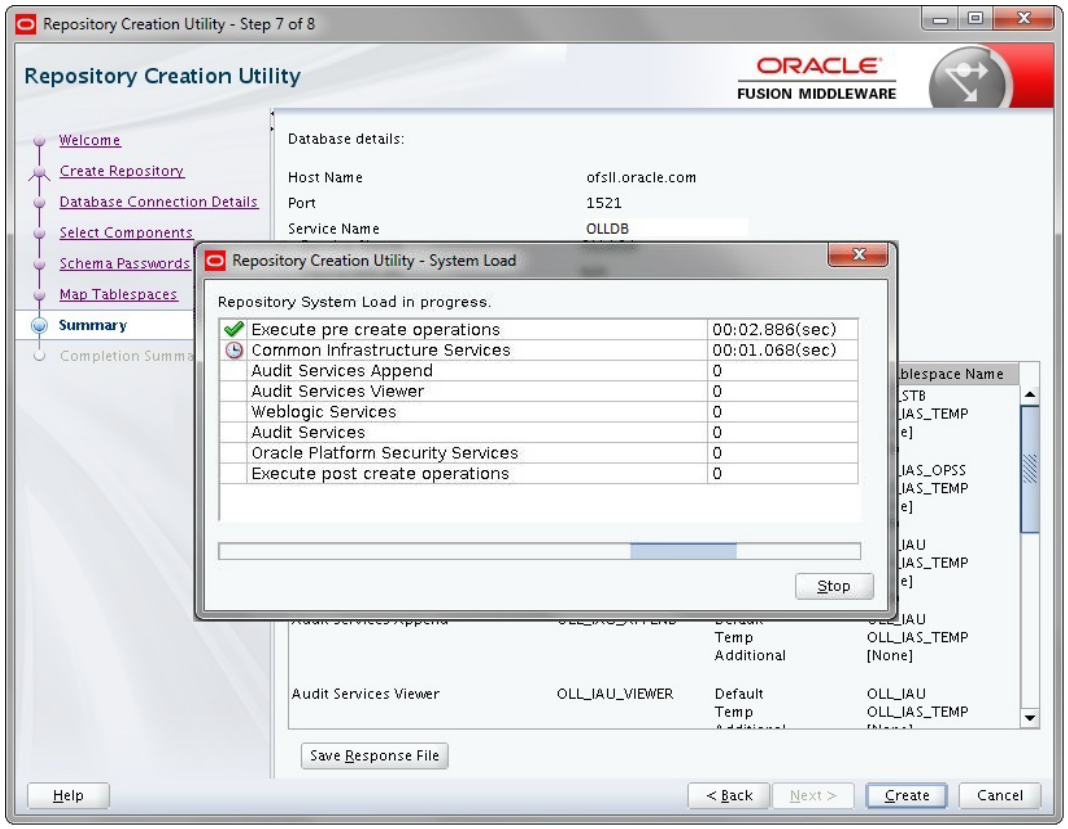
15. Click ‘Next’. The following window is displayed.

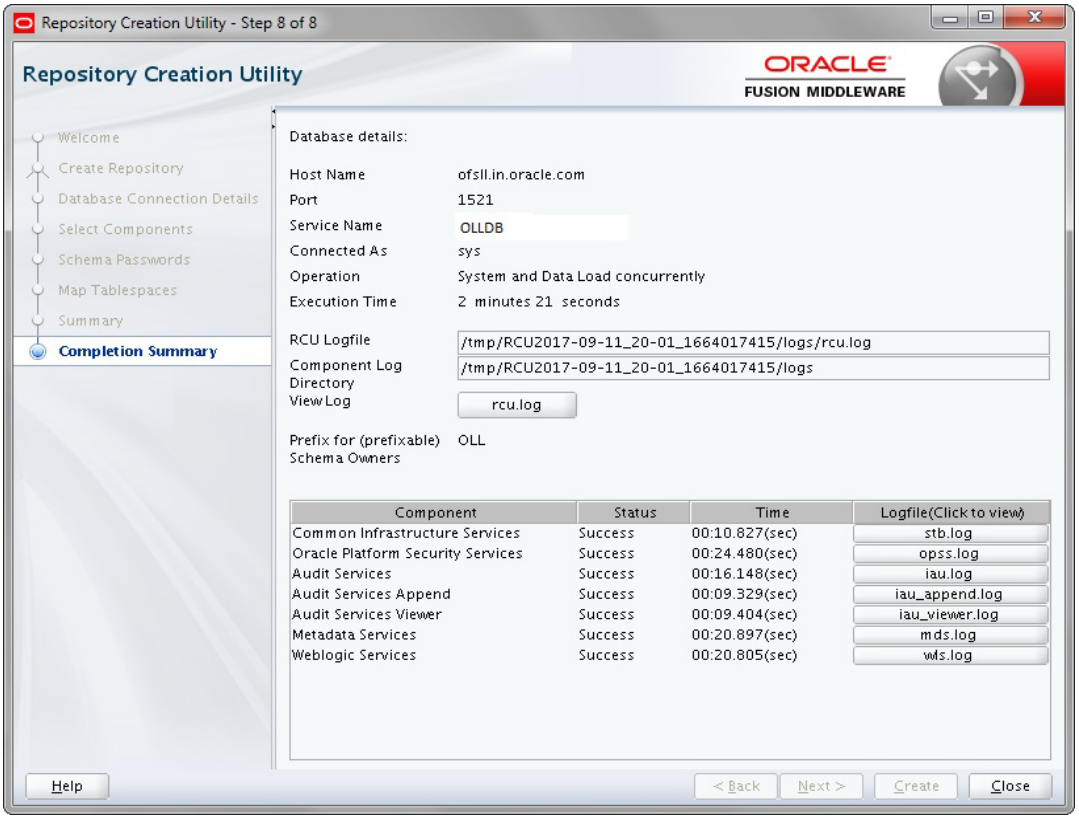


16. Click ‘OK’ in the confirmation dialog. The following window is displayed.



17. Click ‘Create’. The following windows are displayed.



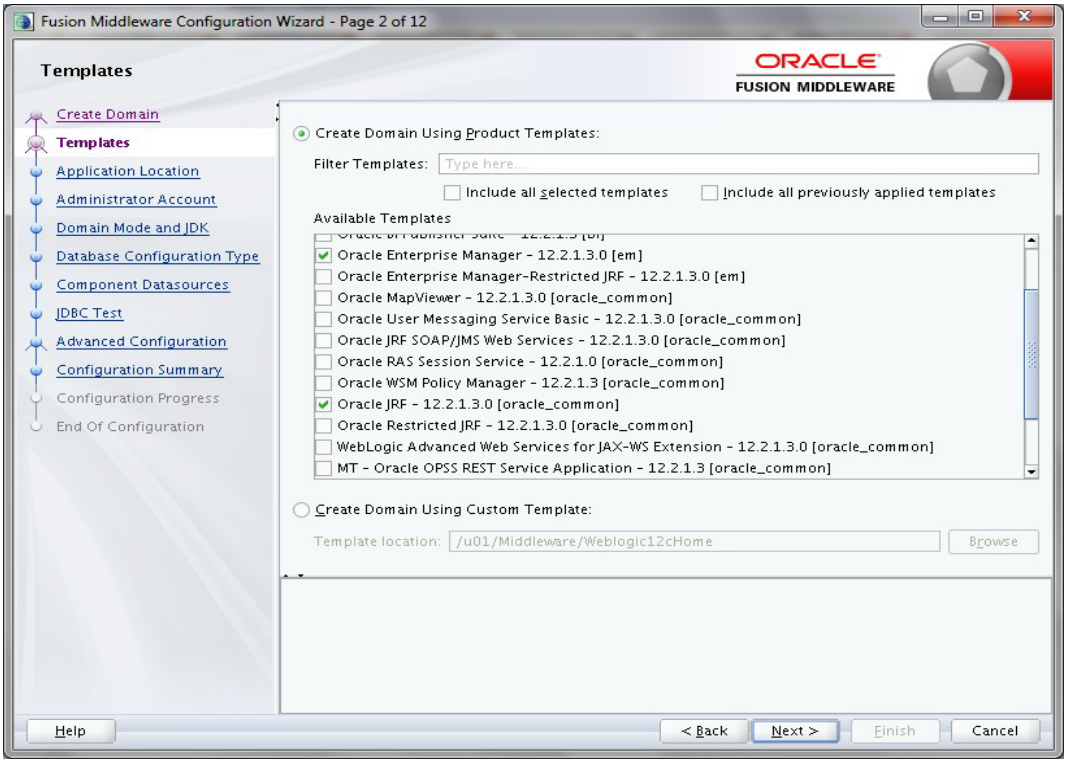


18. Click ‘Close’ to close the window.

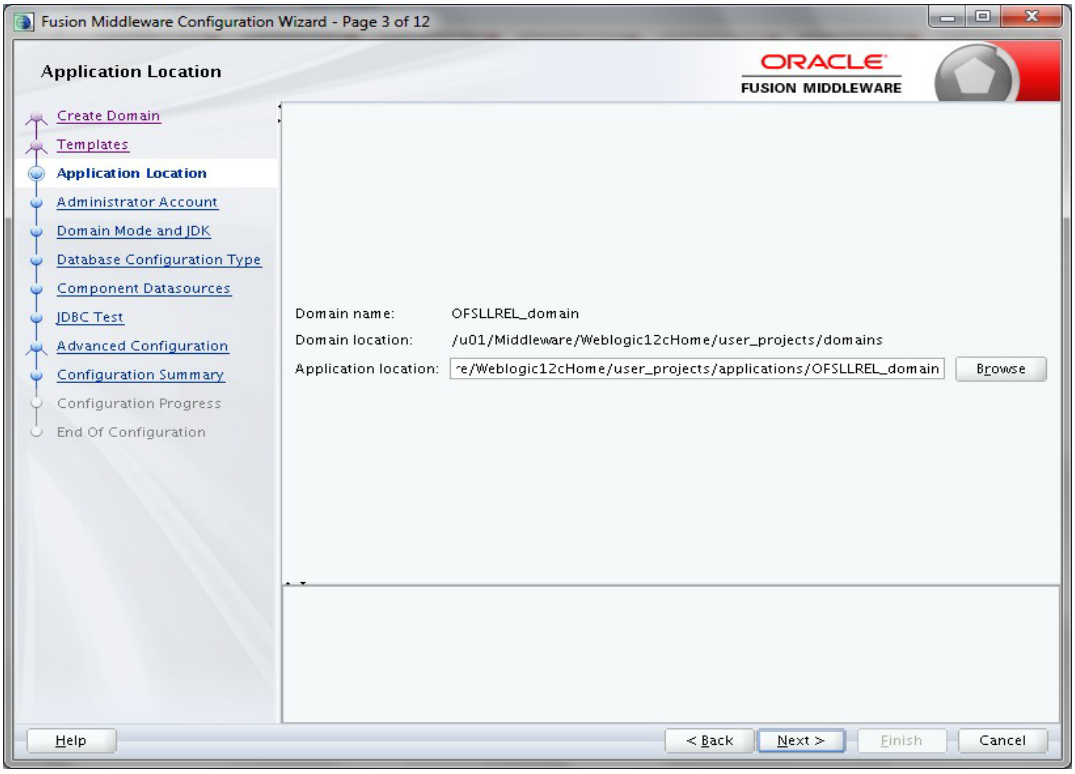
3.2 Creating Domain and Servers

1. In Unix/Linux machine, once the Oracle WebLogic Server is installed, navigate to the following path - <WL_HOME>/oracle_common/common/bin.
2. In Unix, run ‘config.sh’

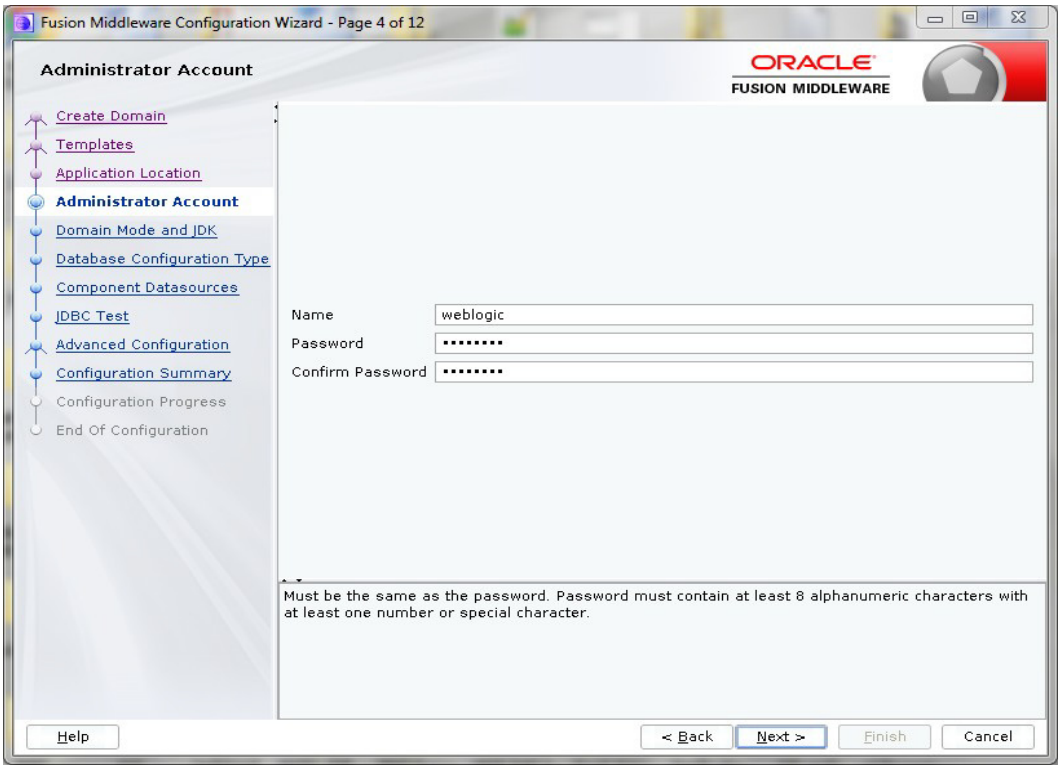
3. Select ‘Create a new domain’ and specify the Domain Location.
4. Click ‘Next’. The following window is displayed.



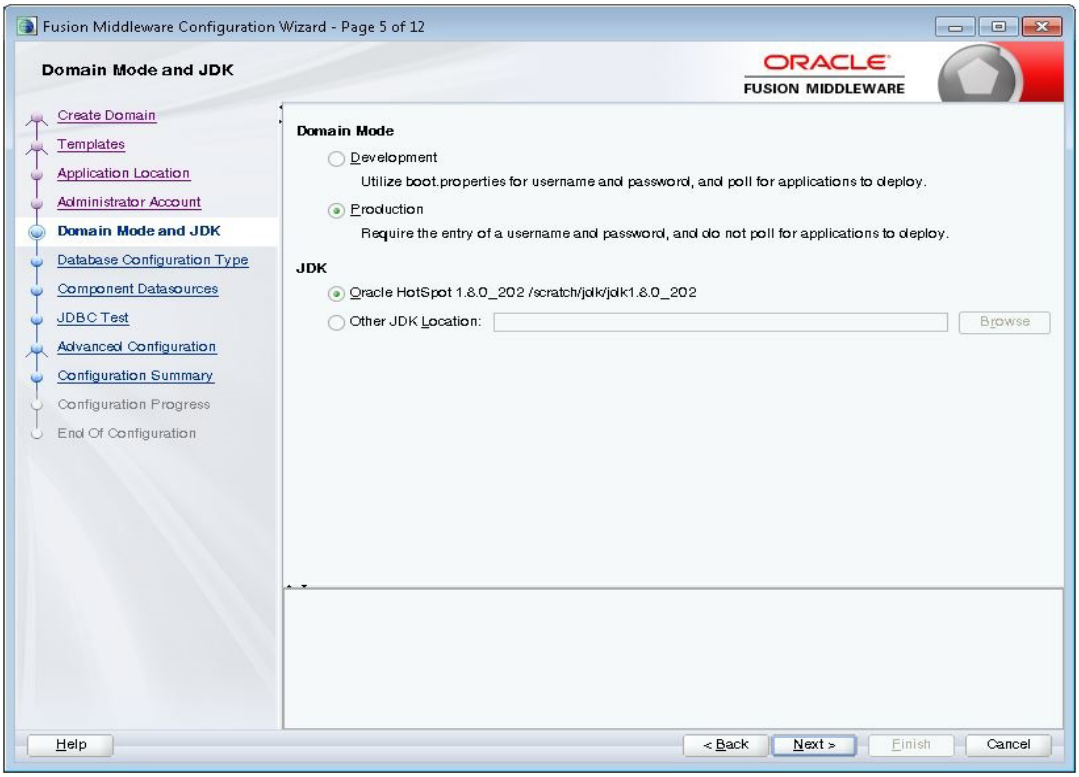
5. Select the option ‘Create Domain Using Product Templates’ in the list of available templates and select ‘Oracle Enterprise Manager - 12.2.1.3.0 [em]’. On selection, the following options are auto-selected:
   – Oracle JRF - 12.2.1.3.0 [oracle_common]
   – Weblogic coherence cluster Extension-12.2.1.3.0 [wlserver]
6. Click ‘Next’. The following window is displayed.



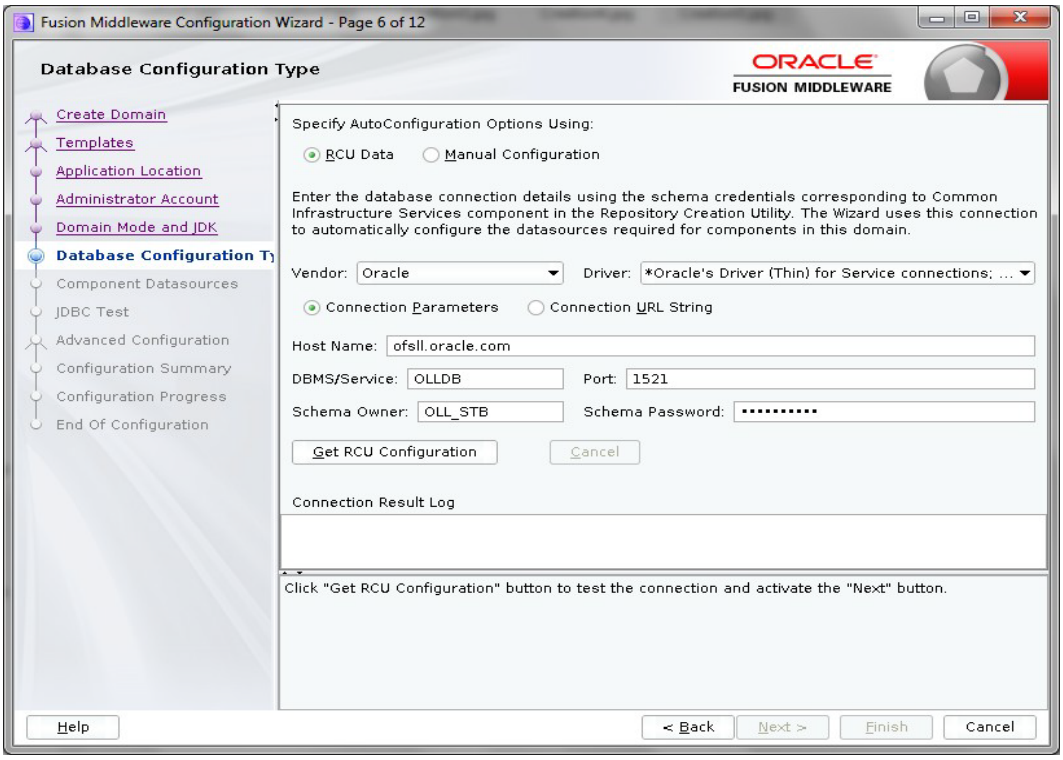
7. Specify the Domain Name in the ‘Application location’ field. You can click browse to directly select the path (if required). Click ‘Next’. The following window is displayed.



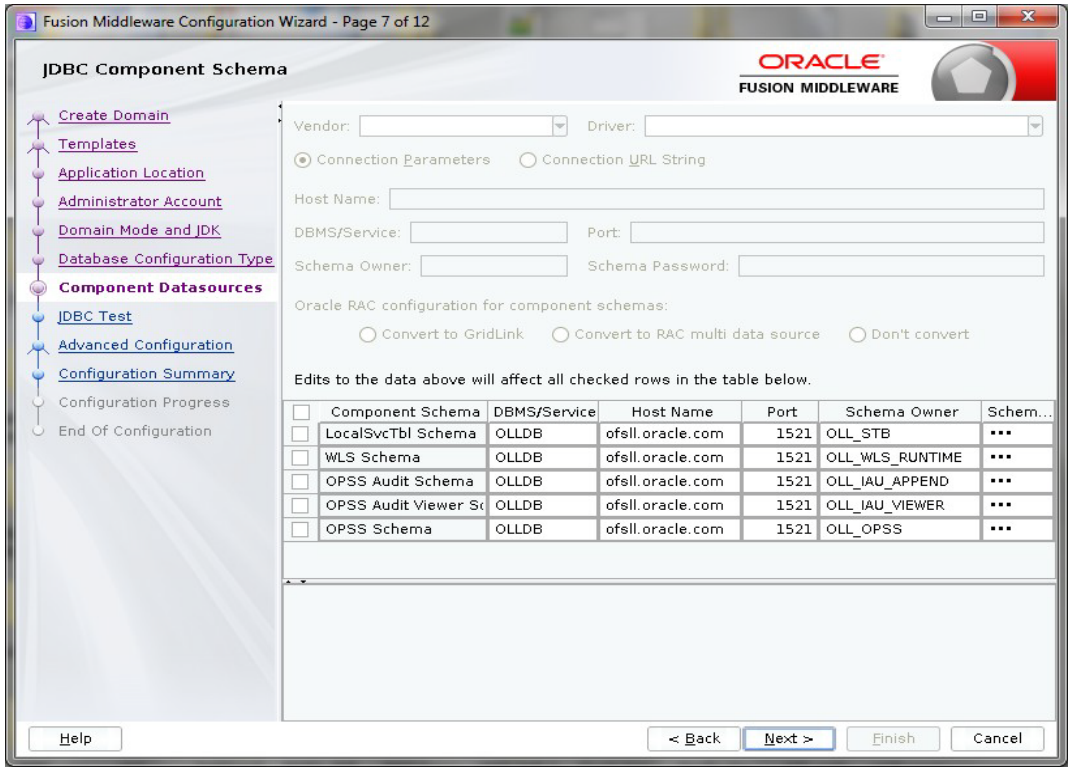
8. Enter credentials for the following:
   - Name
   - Password
   - Confirm Password
9. Click ‘Next’. The following window is displayed.



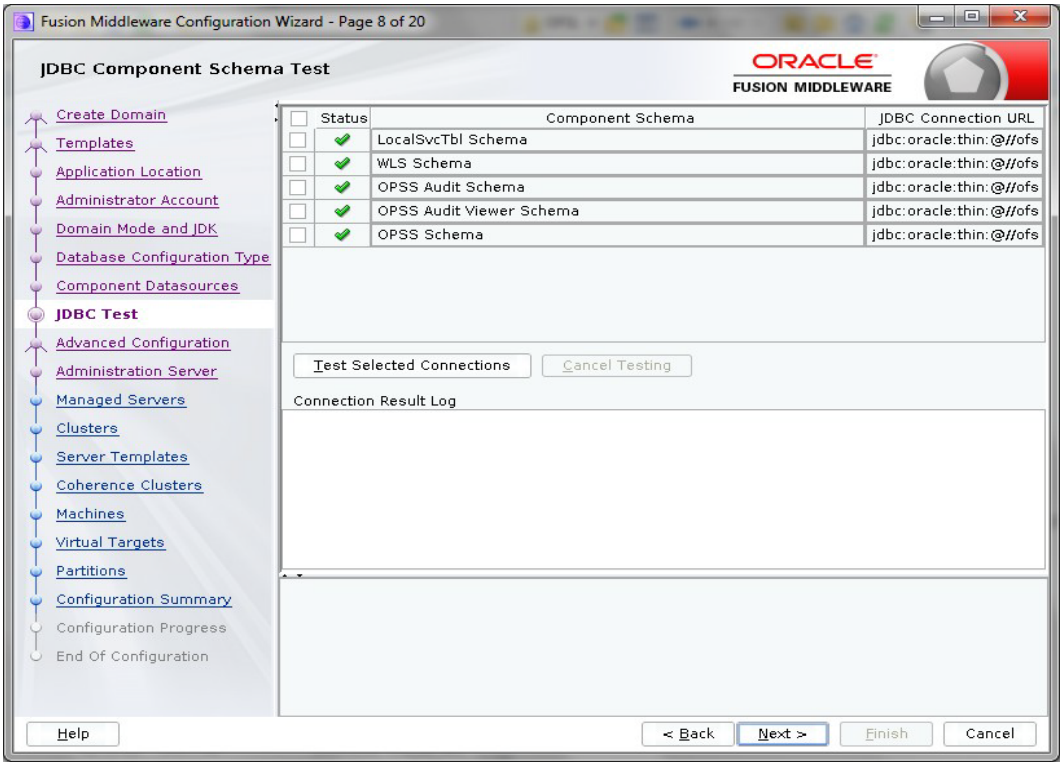
10. Select the Domain Mode as ‘Production’ and ‘JDK’ from Available JDKs. You can also select any other JDK by selecting ‘Other JDK Location’ option. Click ‘Next’. The following window is displayed.



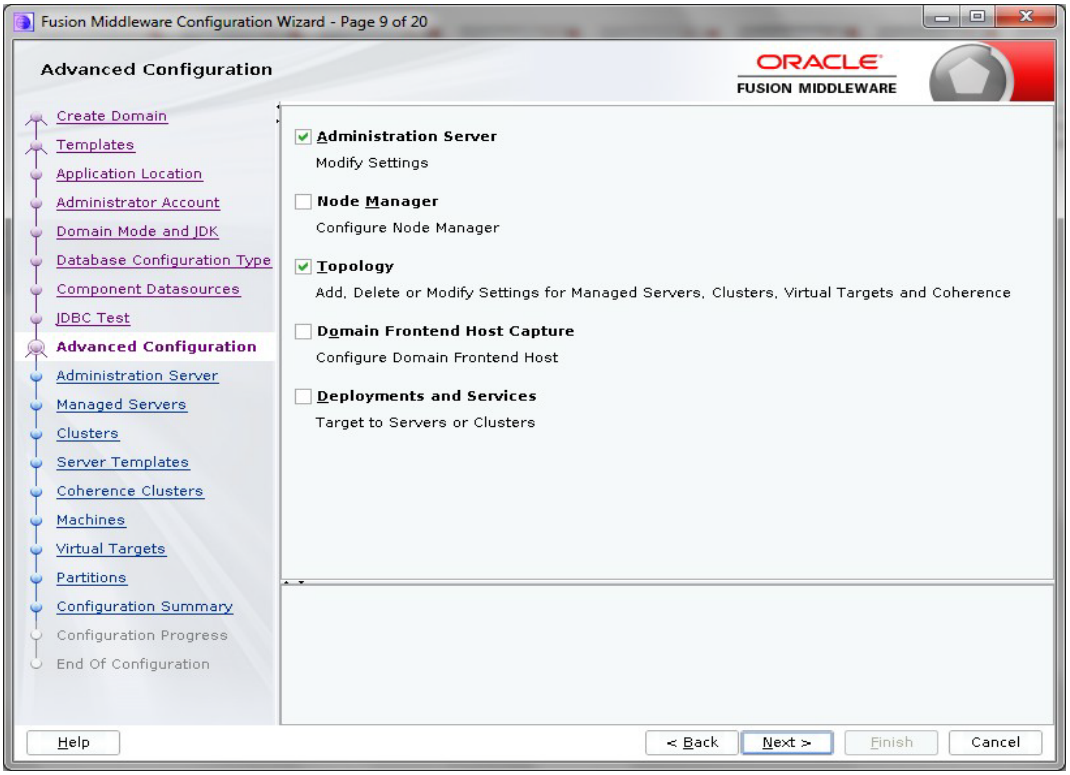
11. Specify the RCU data and click on ‘Get RCU Configuration’. The following window is displayed.



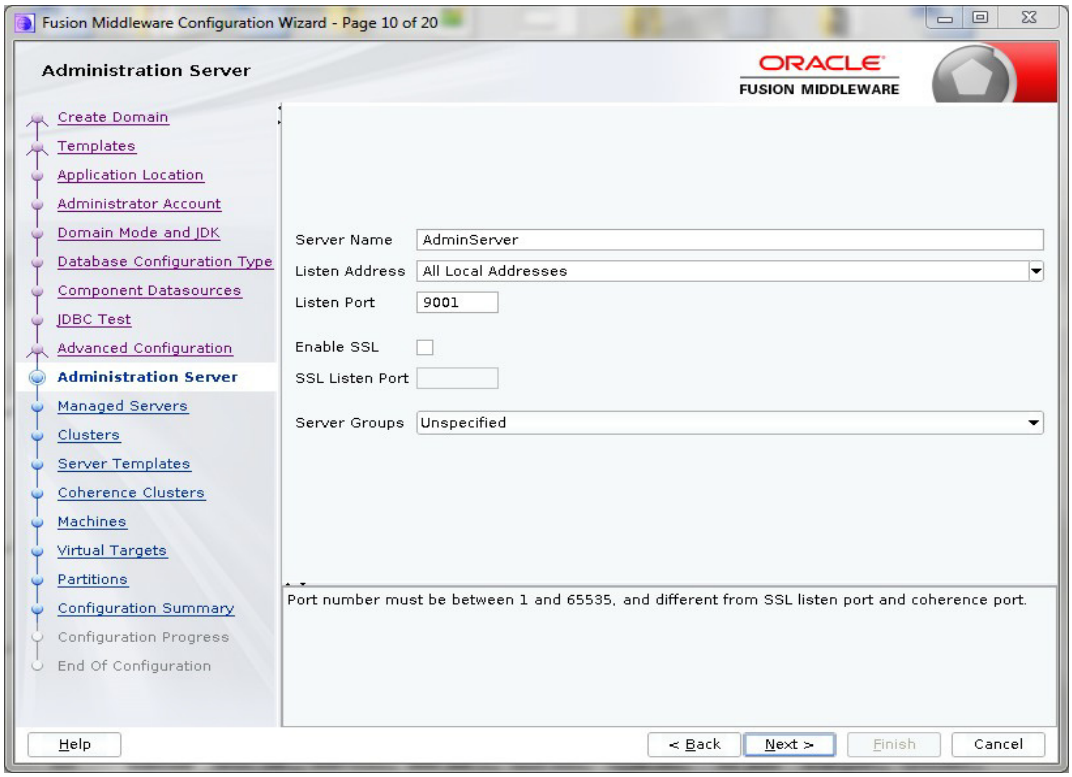
12. Click ‘Next’. The following window is displayed.



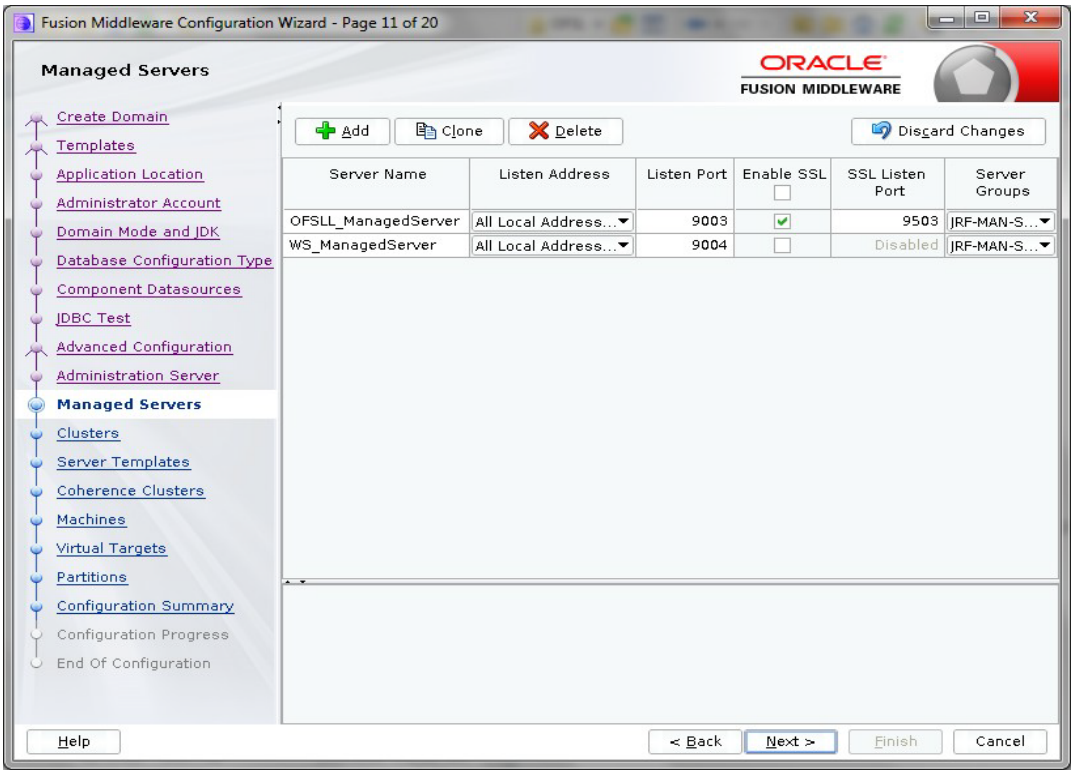
13. Click ‘Next’. The following window is displayed.



14. Select ‘Administration Server’ and ‘Topology’ and click ‘Next’. The following window is displayed.



15. Enter Administration ‘Server Name’ and ‘Listen Port’ details. Click ‘Next’. The following window is displayed.



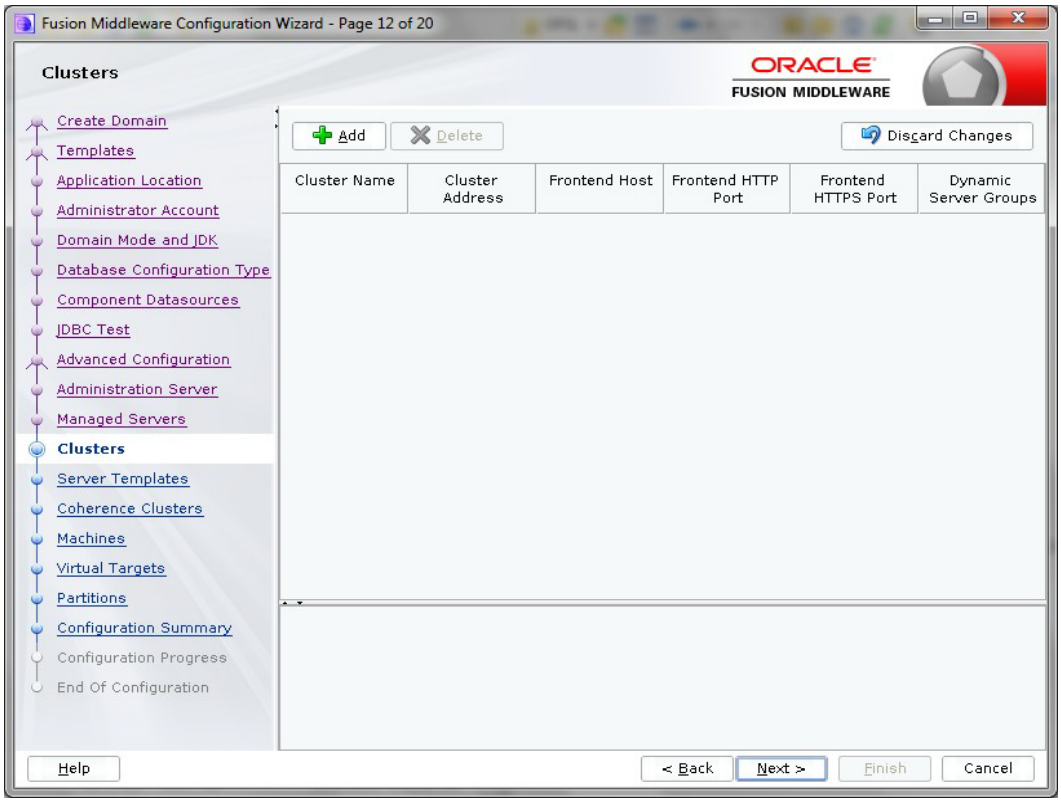
16. Click ‘Add’ button to create ‘ManagedServer’.

17. Select the Server Group as ‘JRF-MAN-SVR’. *Selecting this server group ensures that the Oracle JRF services are targeted to the specific Managed Servers created*.

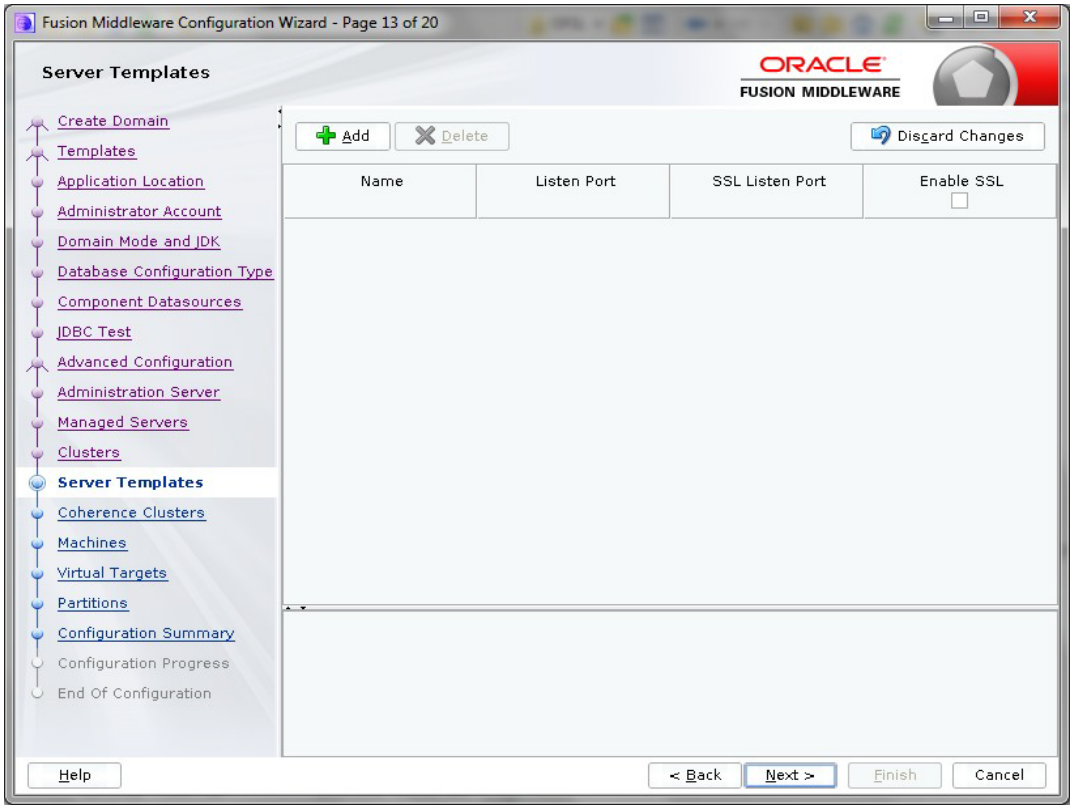
Note

It is recommended to create two managed servers, one each for UI and Web Services.

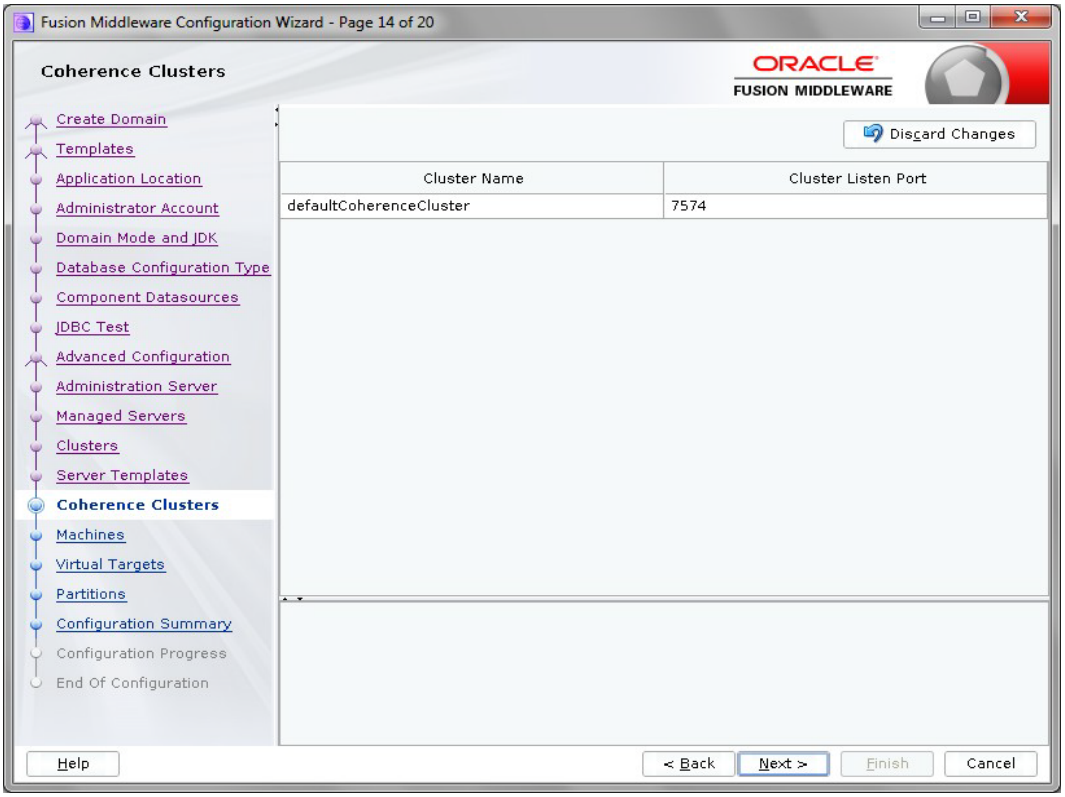
18. Click ‘Next’. The following window is displayed.



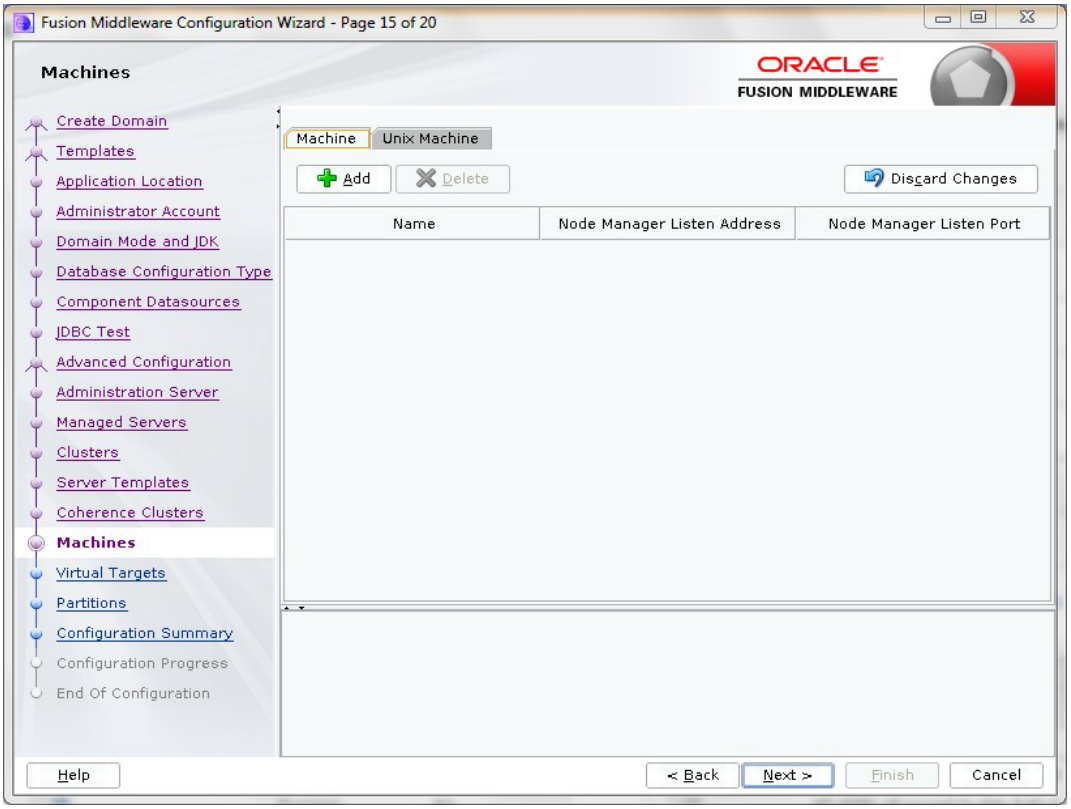
19. Configure as required and click ‘Next’. The following window is displayed.



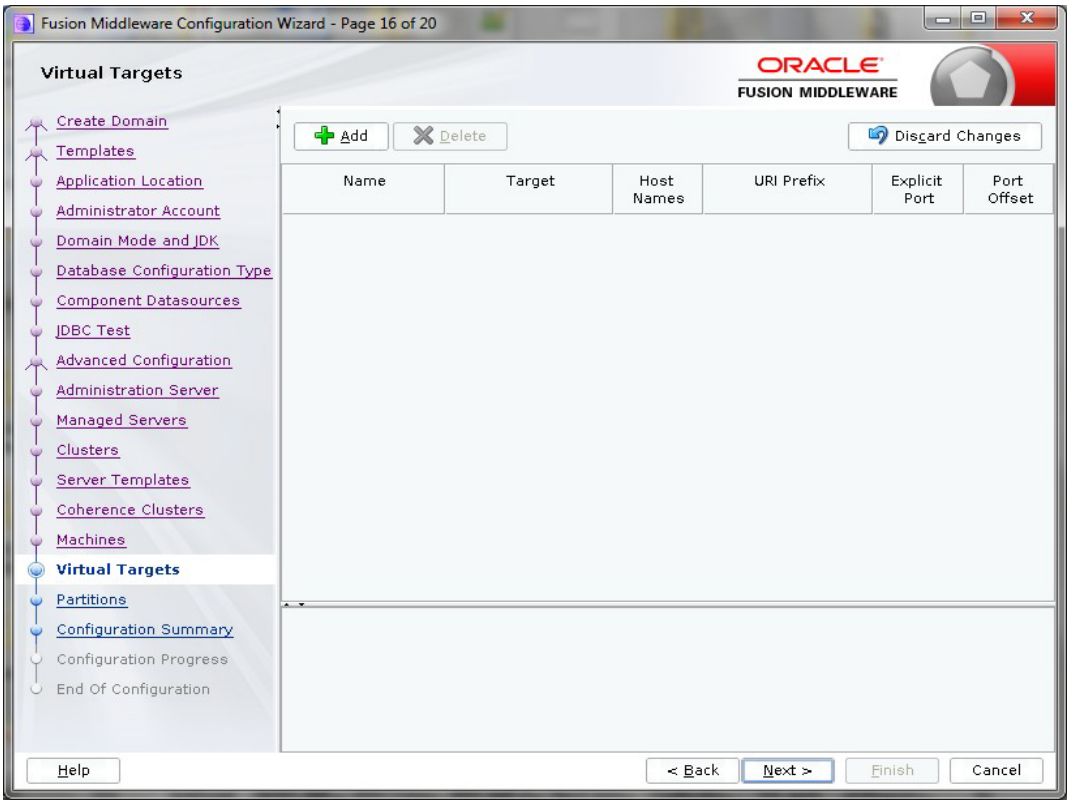
20. Configure as required and click ‘Next’. The following window is displayed.



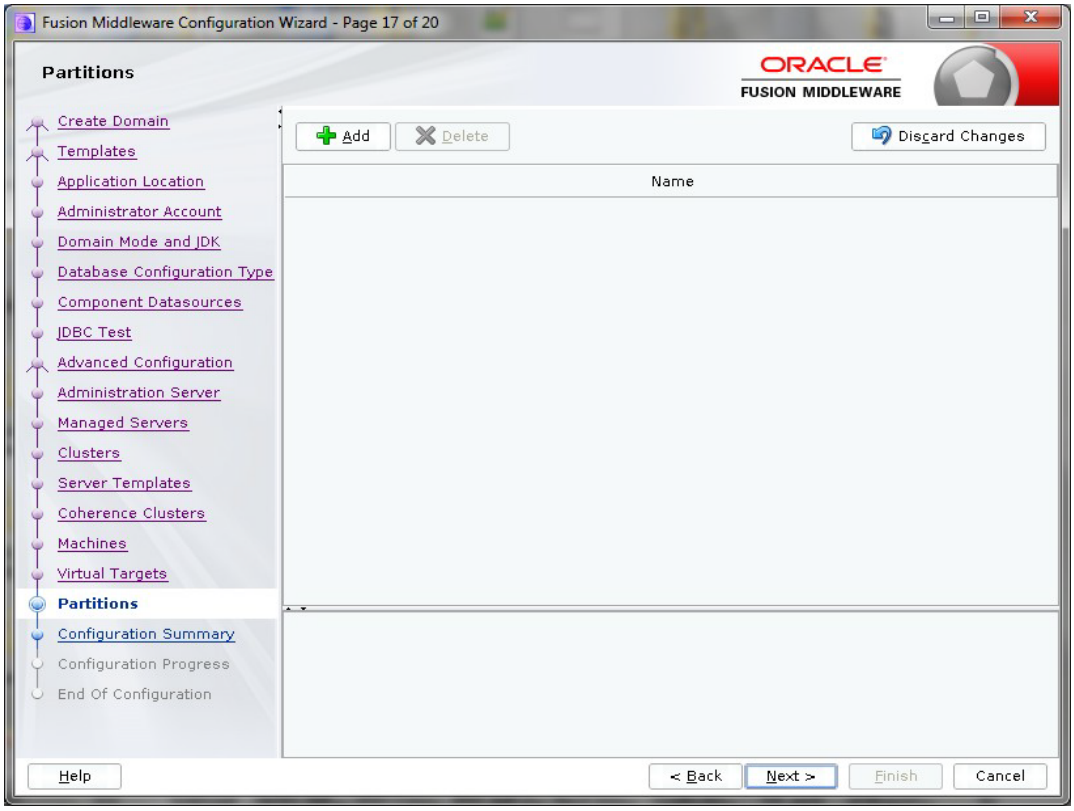
21. Configure as required and click ‘Next’. The following window is displayed.



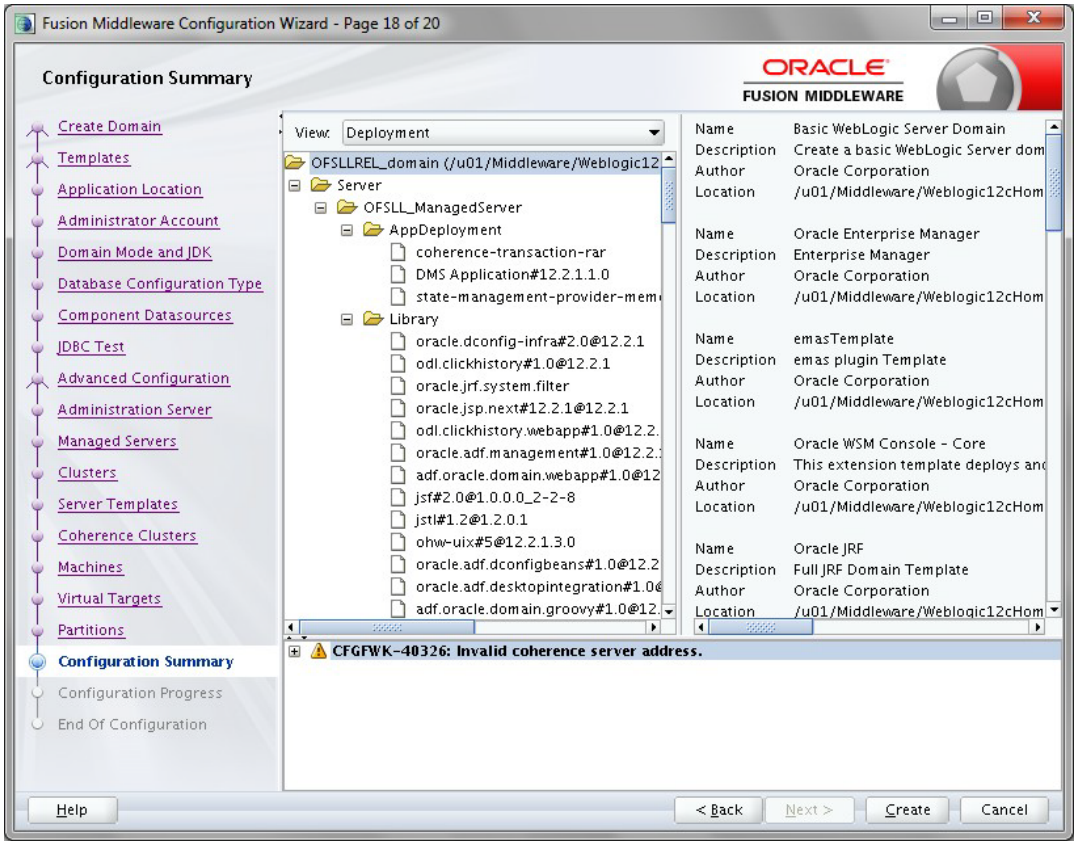
22. Click ‘Create’. The following window is displayed.



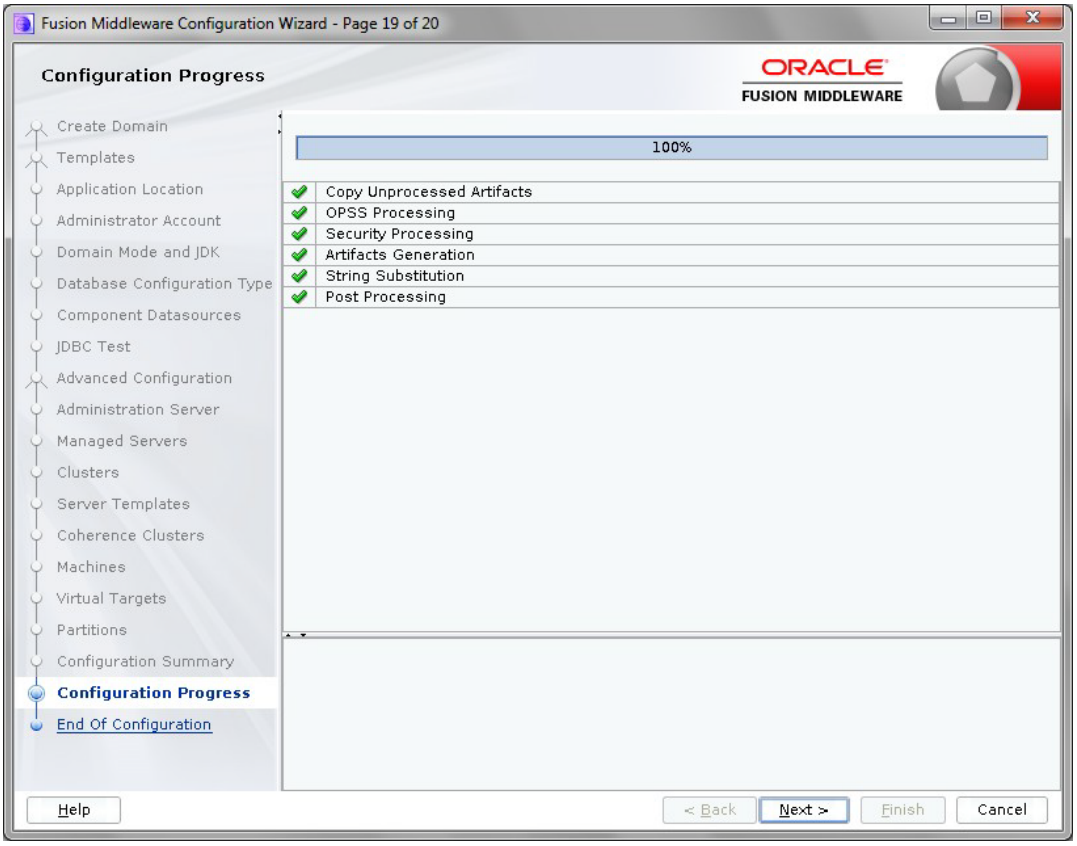
23. Click ‘Next’. The following window is displayed.



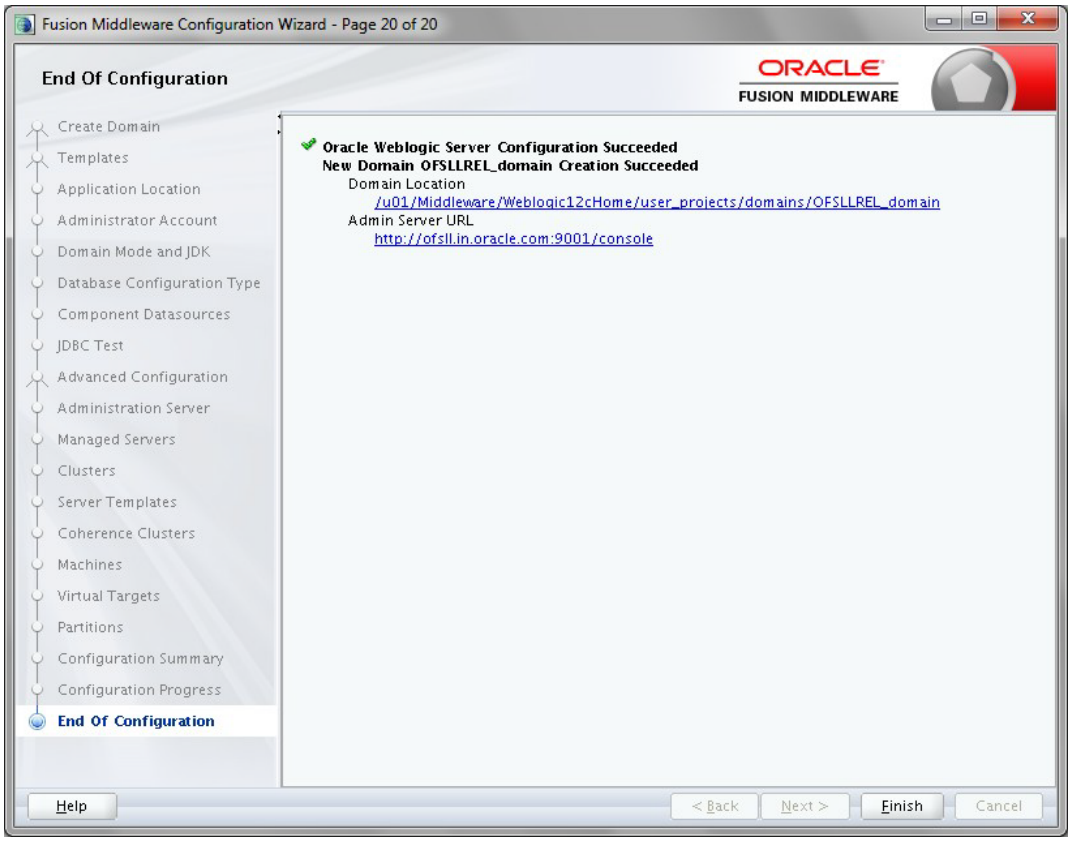
24. Click ‘Next’. The following window is displayed.



25. Click ‘Next’. The following window is displayed.



26. Click ‘Next’. The following window is displayed.



27. Once the creation of the Domain is complete, click ‘Finish’ to close the window.

Note

The default Weblogic installation will be running JVM with 512MB, this has to be increased for the ADF managed server. Say, for a 2 CPU Quad Core with 16 GB it could have the JVM running at 8 GB as:

USER_MEM_ARGS="-Xms8192m –Xmx8192m -XX:PermSize=2048m -XX:Max-PermSize=2048m"

28. The "$MW_HOME/user_projects/domains/<mydomain>" directory contains a script that can be used to start the Admin server.
    - $ cd $MW_HOME/user_projects/domains/<mydomain>/bin
    - $ ./startWebLogic.sh

    If the server is required to be running and access to command line needs to be returned use "nohup" and "&"

    $ nohup ./startWebLogic.sh &

29. To Start Managed Server
    - $ cd $MW_HOME/user_projects/domains/<mydomain>/bin
    - $ ./$MW_HOME/user_projects/domains/<mydomain>/bin/ startManagedWebLogic.sh {ManagedServer_name} {AdminServer URL}

    If the server is required to be running and access to command line needs to be returned use "nohup" and "&".

    $ nohup ./$MW_HOME/user_projects/domains/<mydomain>/bin/ startManagedWebLogic.sh {ManagedServer_name} {AdminServer URL} &

The recommended parameters for each Managed Server for application and web services are as follows:

- For managed server where application is deployed:

  -Xms8g -Xmx8g -XX:NewRatio=3 -XX:HeapDumpPath=/tmp -Dweblogic.threadpool.MinPoolSize=40 -Dweblogic.threadpool.MaxPoolSize=150 -XX:SoftRefLRUPolicyMSPerMB=10 -Dweblogic.diagnostics.debug.DebugLogger.DISABLED=true -Dweblogic.management.discover=false -Dweblogic.llr.table.specjdsl=wl_llr_jent31_1 -Dweblogic.llr.table.specjds2=wl_llr_jent31_2 -Dsun.net.inetaddr.ttl=0 -Dnetworkaddress.cache.ttl=0 -XX:AllocatePrefetchDistance=256 -XX:AllocatePrefetchStyle=1 -XX:+AggressiveOpts -XX:+UseConcMarkSweepGC -XX:+UseParNewGC -XX:MaxTenuringThreshold=4 -XX:-UseCMSInitiatingOccupancyOnly -XX:CMSInitiatingOccupancyFraction=60 -XX:CMSTriggerRatio=60 -XX:+CMSParallelRemarkEnabled -XX:+UseCMSCompactAtFullCollection -XX:+CMSCompactWhenClearAllSoftRefs -XX:PrintCMSStatistics=1 -XX:+PrintClassHistogram -XX:-UseParallelGC -XX:ParallelGCThreads=10 -XX:-TraceClassUnloading -XX:-UseParallelOldGC -XX:+UseCompressedOops -XX:+UseBiasedLocking -XX:+AlwaysPreTouch -XX:-UseAdaptiveSizePolicy -Djbo.load.components.lazily=true -Djbo.ampool.initpoolsize=100 -Djbo.recyclethreshold=200 -Djbo.ampool.minavailablesize=200 -Djbo.ampool.maxavailablesize=200 -Djbo.ampool.timetolive=-1 -Djbo.locking.mode=optimistic -Djbo.doconnectionpooling=true -Djbo.txn.disconnect_level=1 -Djbo.ampool.doampooling=true -Djbo.dofailover=false -Djbo.ampool.maxinactiveage=3600000 -Djbo.ampool.monitorsleepinterval=360000 -Doracle.multitenant.enabled=false -Dweblogic.mdb.message.MinimizeAQSessions=true -Dweblogic.ejb.container.MDBDestinationPollIntervalMillis=6000 -XX:StringTableSize=100003 -XX:ReservedCodeCacheSize=1g -XX:+UseStringCache

-XX:+OptimizeStringConcat -XX:+UnlockCommercialFeatures -XX:+FlightRecorder -Doracle.adfm.useSharedTransactionForFrame=false

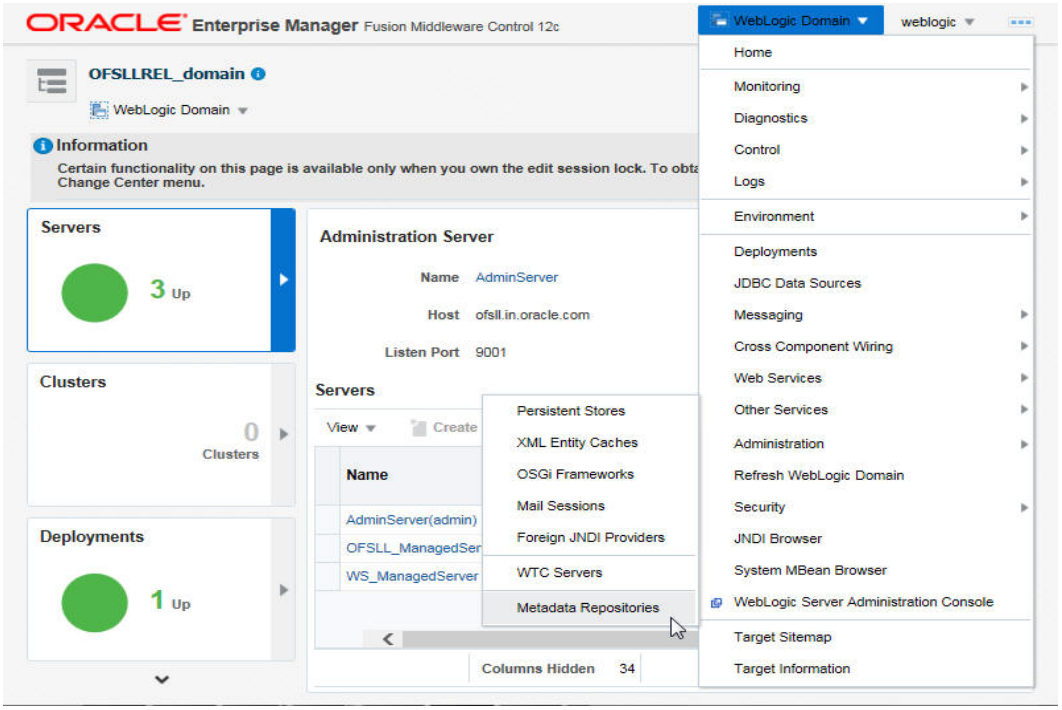
- For managed server where web services are deployed:

  -Xms8g -Xmx8g -XX:NewRatio=3 -XX:HeapDumpPath=/tmp -Dweblogic.threadpool.MinPoolSize=40 -Dweblogic.threadpool.MaxPoolSize=150 -XX:SoftRefLRUPolicyMSPerMB=10 -Dweblogic.diagnostics.debug.DebugLogger.DISABLED=true -Dweblogic.management.discover=false -Dweblogic.llr.table.specjdsl=wl_llr_jent31_1 -Dweblogic.llr.table.specjds2=wl_llr_jent31_2 -Dsun.net.inetaddr.ttl=0 -Dnetworkaddress.cache.ttl=0 -XX:AllocatePrefetchDistance=256 -XX:AllocatePrefetchStyle=1 -XX:+AggressiveOpts -XX:+UseConcMarkSweepGC -XX:+UseParNewGC -XX:MaxTenuringThreshold=4 -XX:-UseCMSInitiatingOccupancyOnly -XX:CMSInitiatingOccupancyFraction=60 -XX:CMSTriggerRatio=60 -XX:+CMSParallelRemarkEnabled -XX:+UseCMSCompactAtFullCollection -XX:+CMSCompactWhenClearAllSoftRefs -XX:-UseParallelGC -XX:ParallelGCThreads=10 -XX:-TraceClassUnloading -XX:-UseParallelOldGC -XX:+UseCompressedOops -XX:+UseBiasedLocking -XX:+AlwaysPreTouch -XX:-UseAdaptiveSizePolicy -Doracle.multitenant.enabled=false -XX:StringTableSize=100003 -XX:ReservedCodeCacheSize=1g -XX:+UseStringCache -XX:+OptimizeStringConcat -XX:+UnlockCommercialFeatures -XX:+FlightRecorder

3.3 Creating Metadata Repository

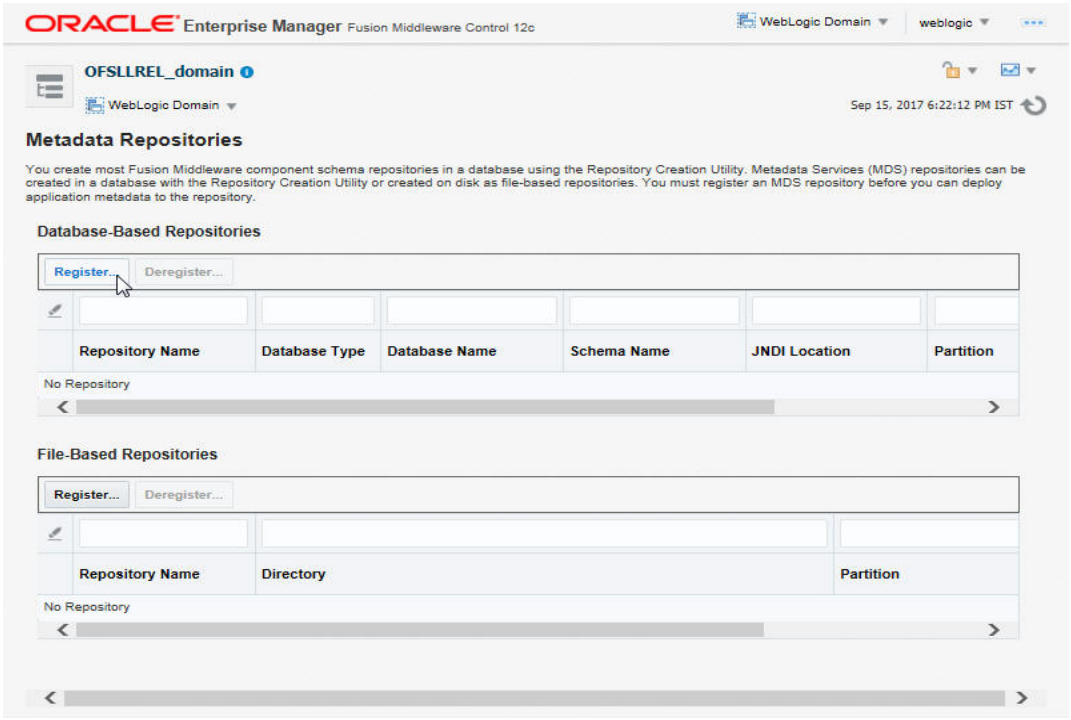
Assuming that **OLL_MDS** schema is created using Oracle Repository Creation Utility (RCU) as mentioned in Creating Schemas using Repository Creation Utility section, follow the below steps to create the repository.

1. Login to Oracle Enterprise Manager 12c console (http://hostname:port/em).

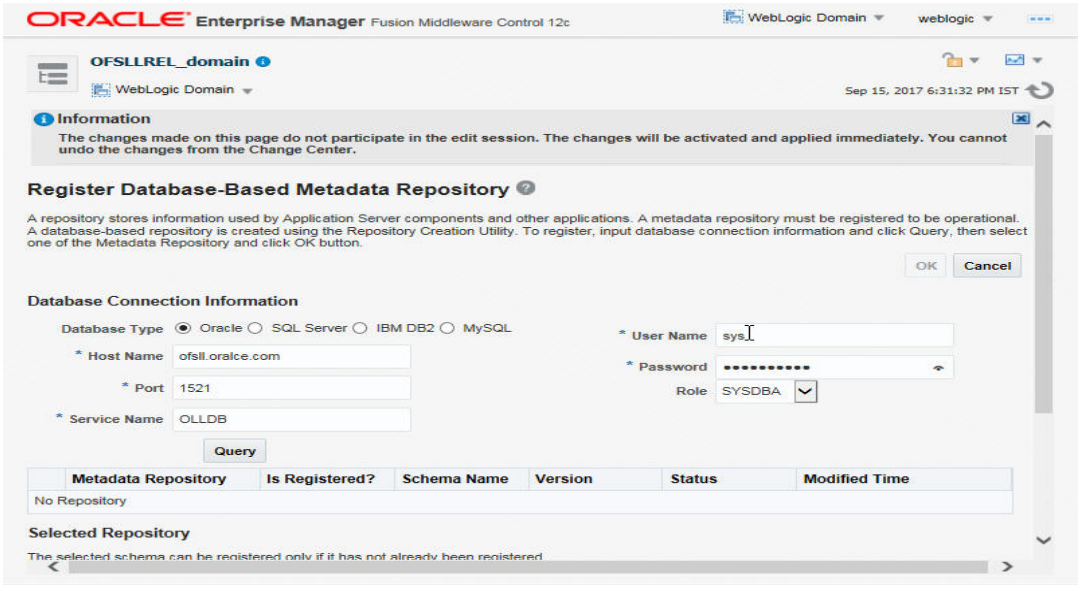


2. Click on domain name OFSLLREL_domain on the left side panel.
3. Expand Weblogic domain OFSLLREL_domain and click ‘Metadata Repositories’ option, as shown in the above screen.

4. The following window is displayed.

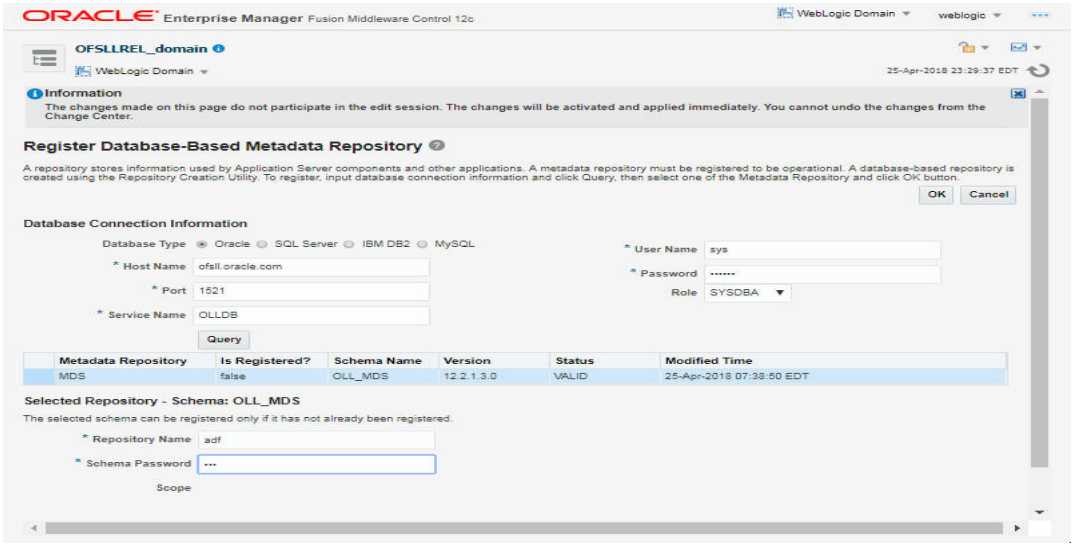


5. Click ‘Register’ button. The following window is displayed.

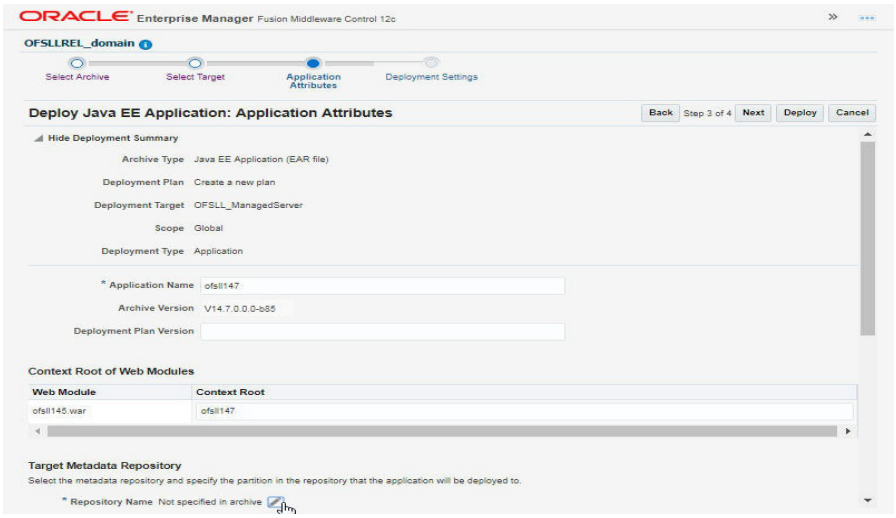


6. Enter database instance details under Database Connection Information section and click ‘Query’. All available schemas in the given database instance are listed.
7. Select the schema you require and in the Selected Repository – Schema OLL_MDS section, enter ‘Repository Name’ (adf) and the password.

8. Click ‘OK’. The following window is displayed.



9. Click Repository name ‘mds-adf’ on left panel. You can even select it from right panel.

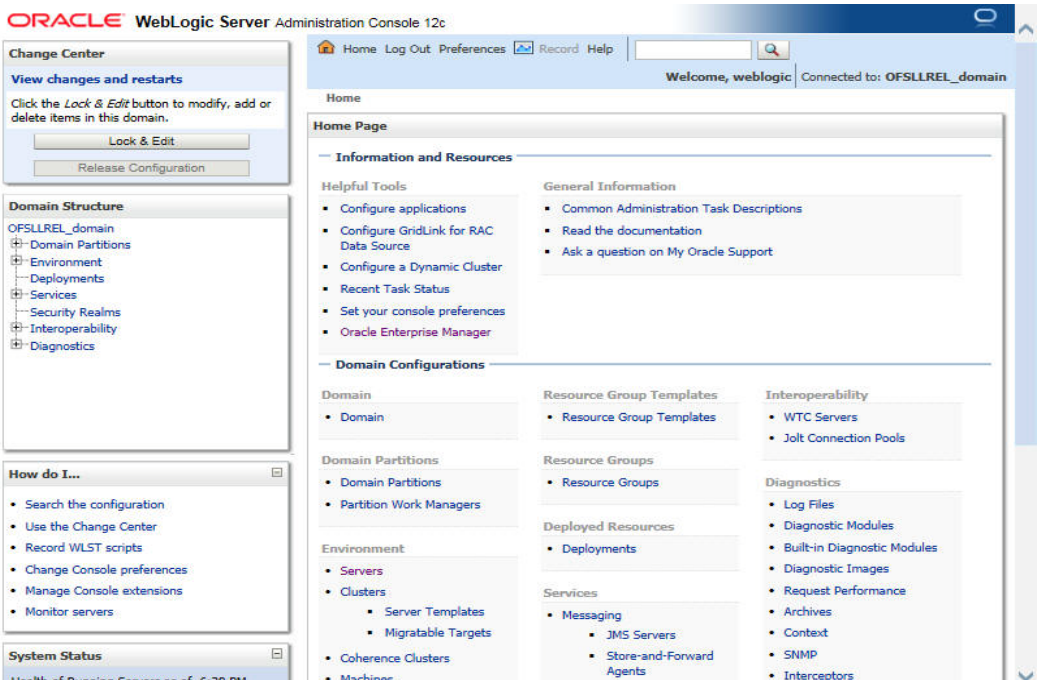


10. Click ‘Add’ and target to AdminSever and OFSLL_ManagedServer as on right panel.

3.4 Creating Data Source

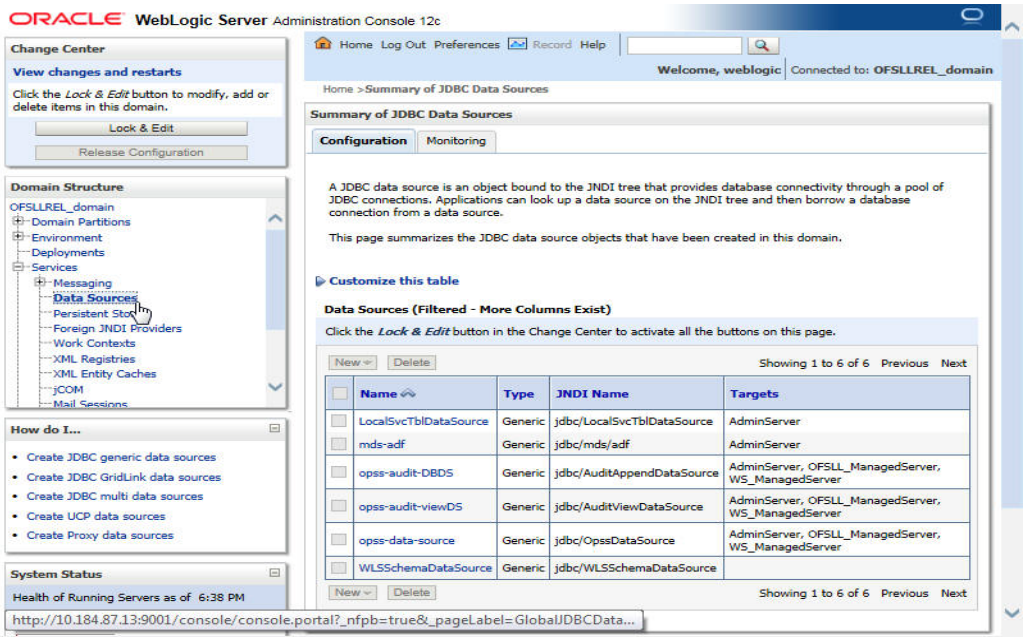
1. Login to WebLogic Server 12c console (http://hostname:port/console).

2. The following window is displayed.

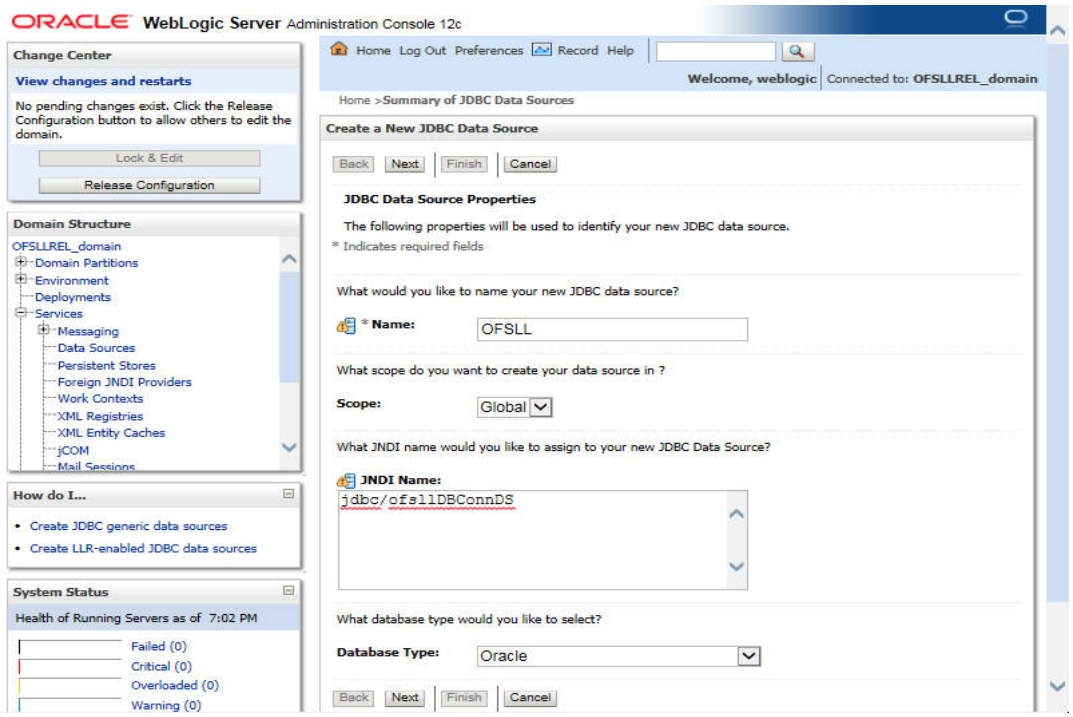


3. Click Domain Name > Services > Data Sources.

4. The following window is displayed.

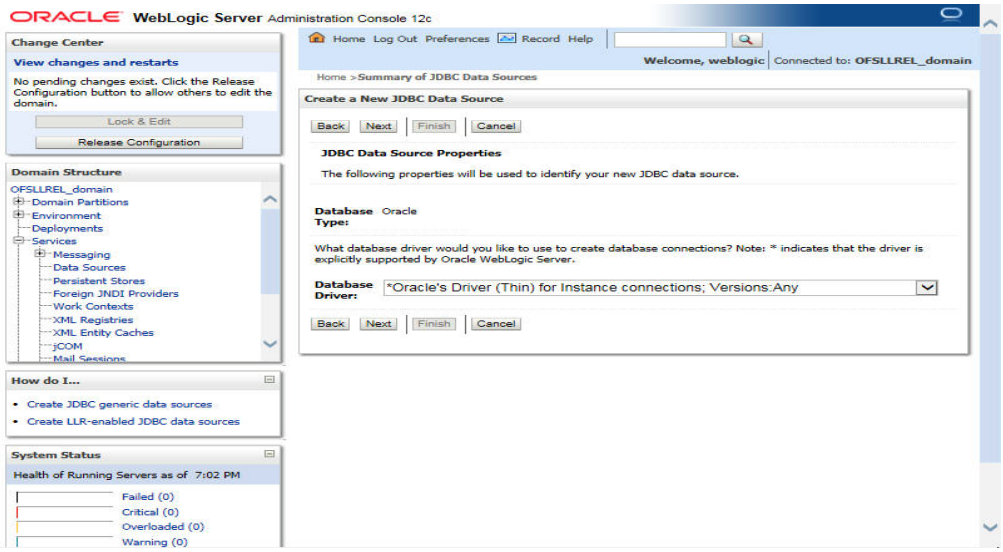


5. Click ‘Lock & Edit’ button on the left panel. Click ‘New’ on right panel and select Generic Data Source.



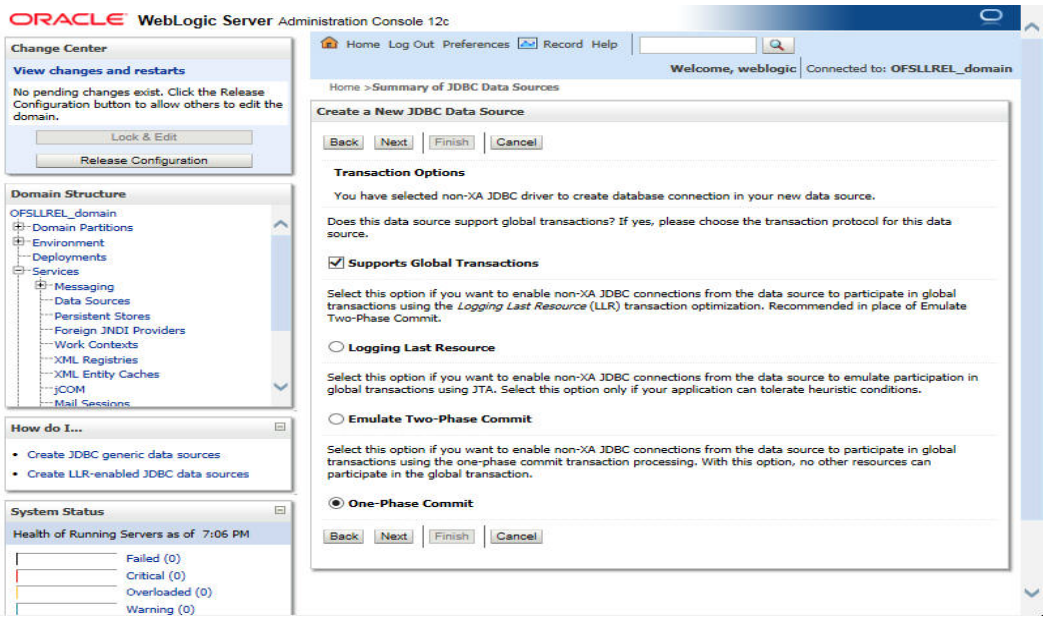
6. Enter Data source ‘Name’, JNDI Name as ‘jdbc/ofsllDBConnDS’ and select ‘Oracle’ as Database Type.

7. Click ‘Next’. The following window is displayed.

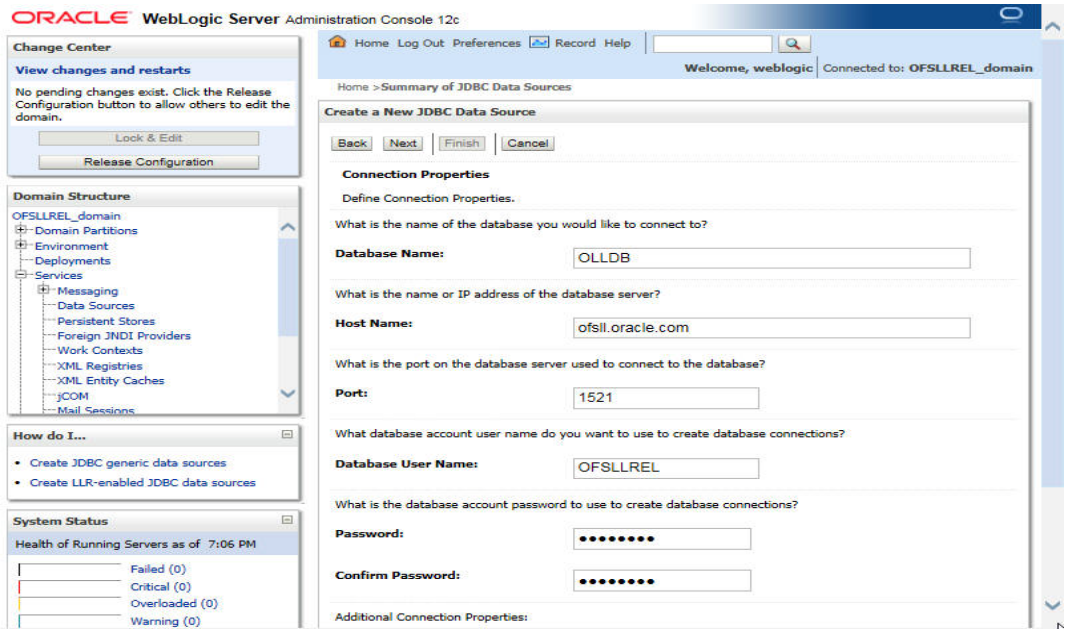


8. Select the Database Driver ‘Oracle's Driver(Thin) for Instance connections; Versions:Any’ as shown above.

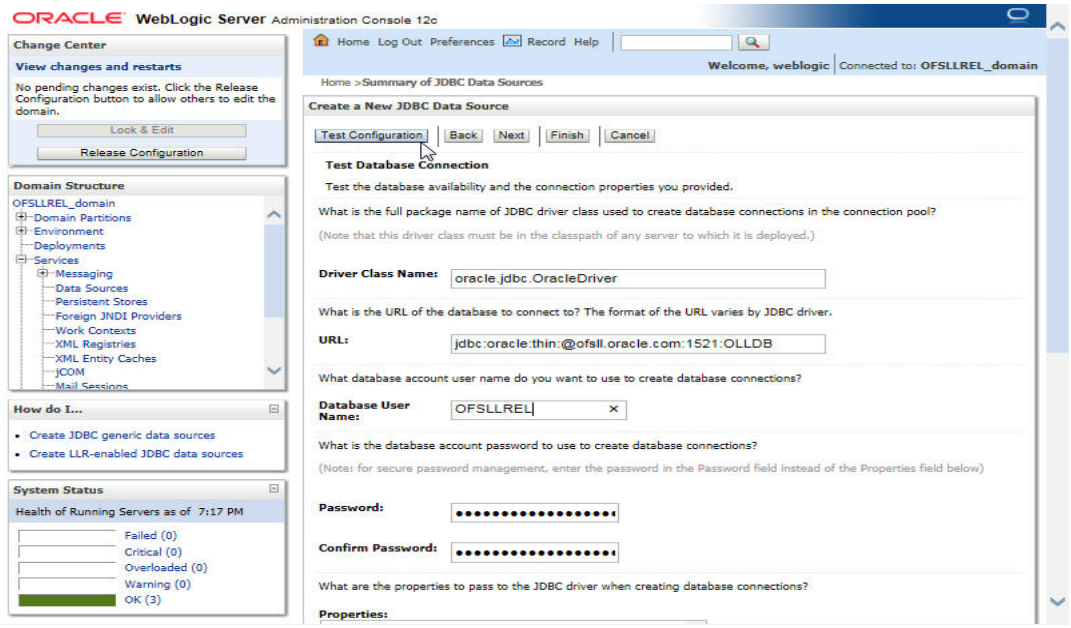
9. Click ‘Next’. The following window is displayed.



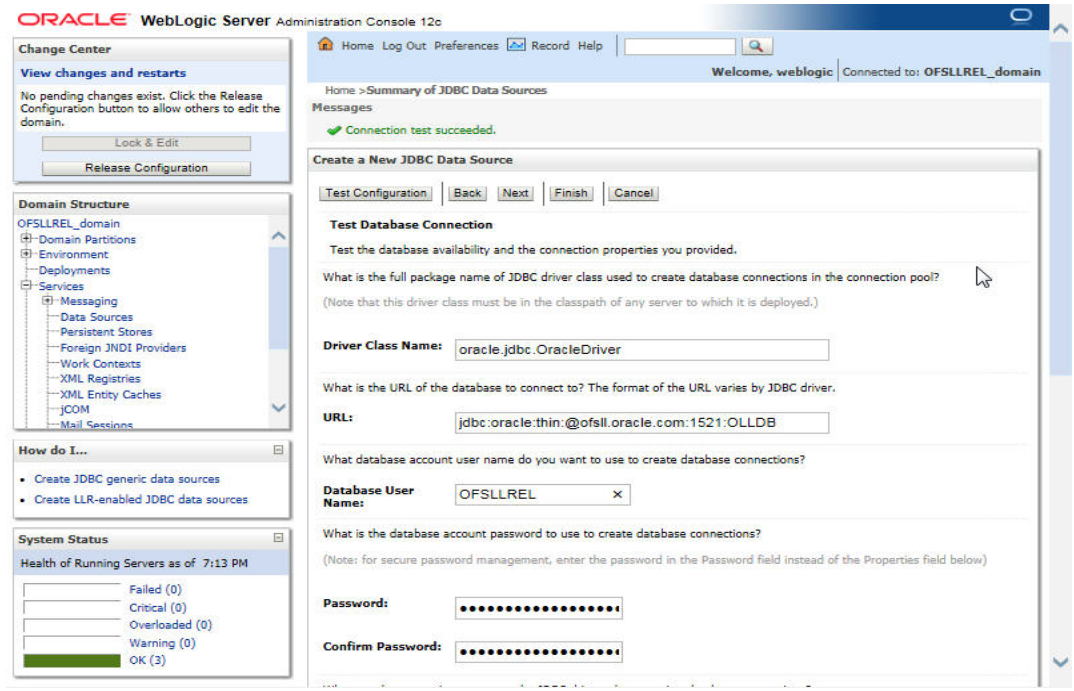
10. Click ‘Next’. The following window is displayed.



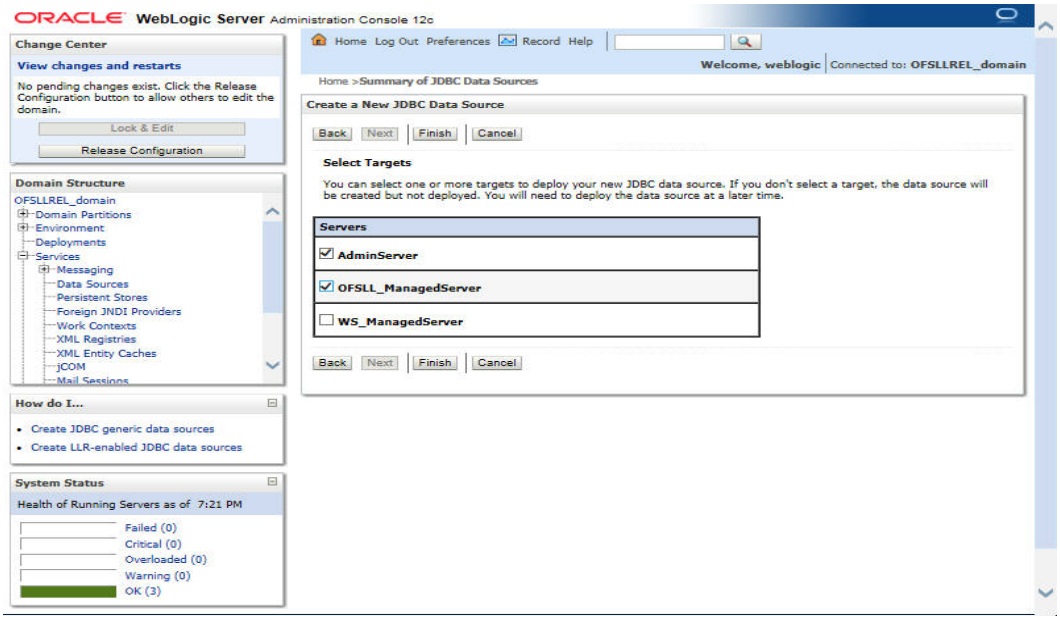
11. Enter Database details click ‘Next’. The following window is displayed.



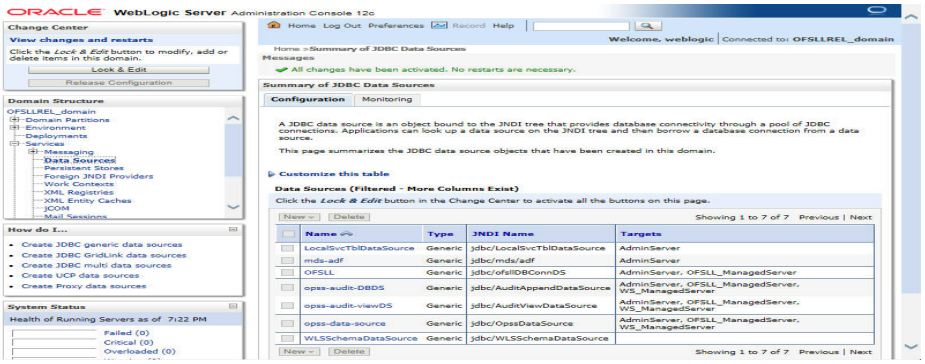
12. Click ‘Test Configuration’. The following window is displayed.



13. Displays confirmation message as ‘Connection test succeeded’. Click ‘Next’. The following window is displayed.



14. Select target Servers ‘AdminServer’ and ‘OFSLL_ManagedServer’ and click ‘Finish’. The following window is displayed.



15. Click ‘Activate Changes’ on the left panel.

Update the following parameters in JDBC data source connection pool:

1. Select Services > Data Sources > select the OFSLL data source > Connection Pool.
2. Initial capacity and Maximum capacity is defaulted to 15, if the number of concurrent users are more this needs to be increased.
3. Click Advanced button and update the following:
   - Inactive Connection Timeout=900
   - Uncheck the ‘Wrap Data Types’ parameter for better performance.
4. Click ‘Save’.

Note

User Authentication and Management is outside of Oracle Financial Services Lending and Leasing application. Organizations can use an LDAP implementation for authentication. For Development and Testing purpose, the following sections can be configured for authentication:

3.5 Creating SQL Authentication Provider

3.6 Creating User Groups and Users

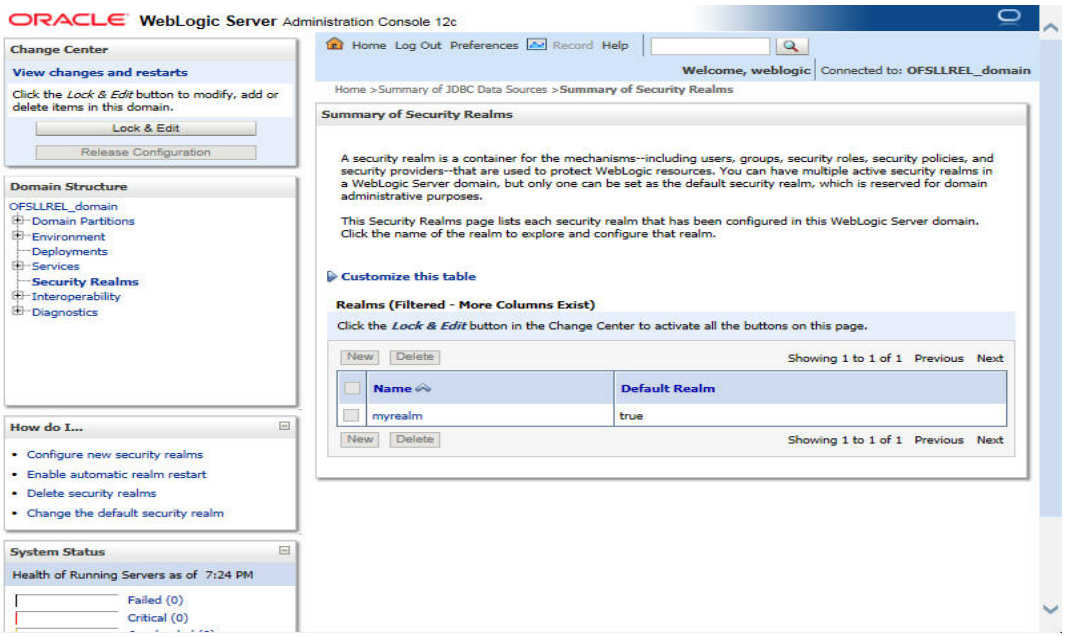
3.7 Implementing JMX Policy for Change Password

4.1 Configuring Password Policy for SQL Authenticator

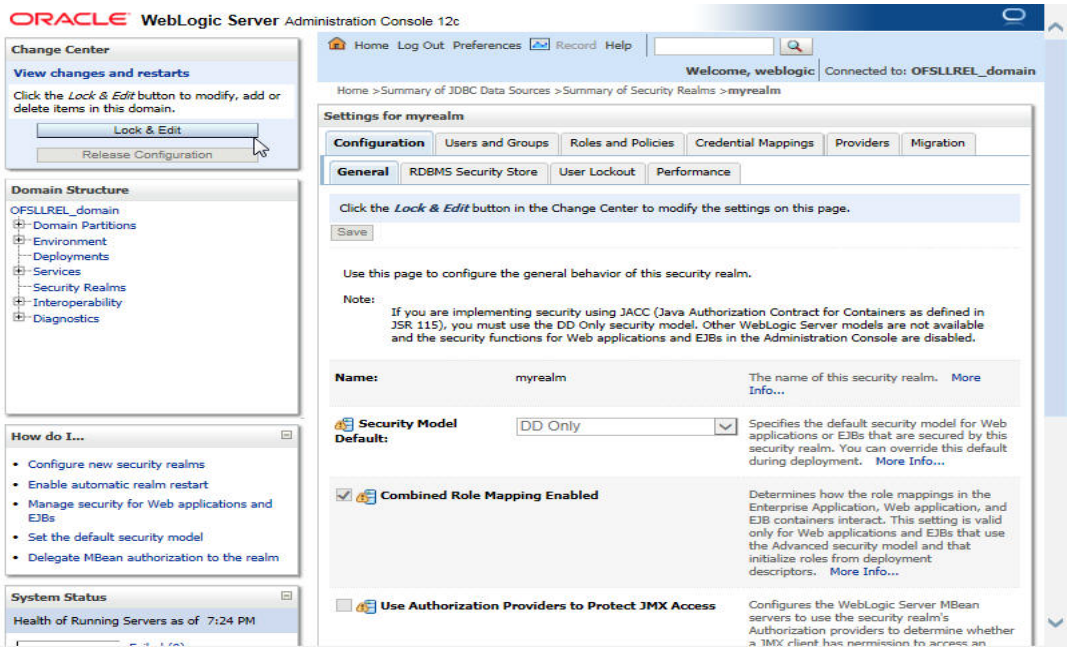
4.2 Configuring User Lockout Policy

3.5 Creating SQL Authentication Provider

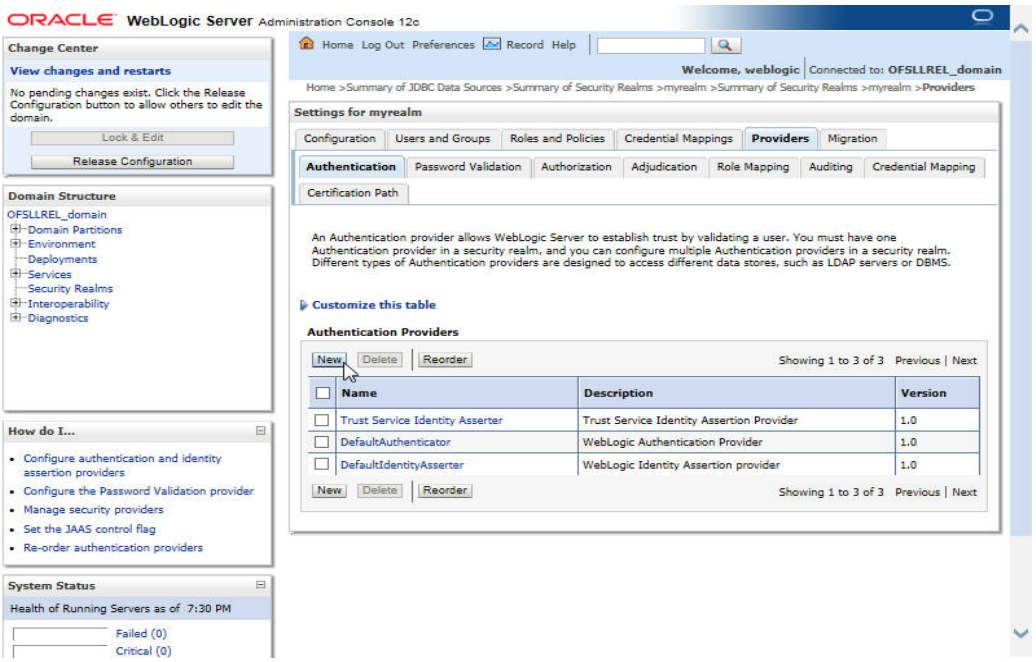
1. Login to WebLogic server administration console and click ‘Security Realms’ in left panel. The following window is displayed.



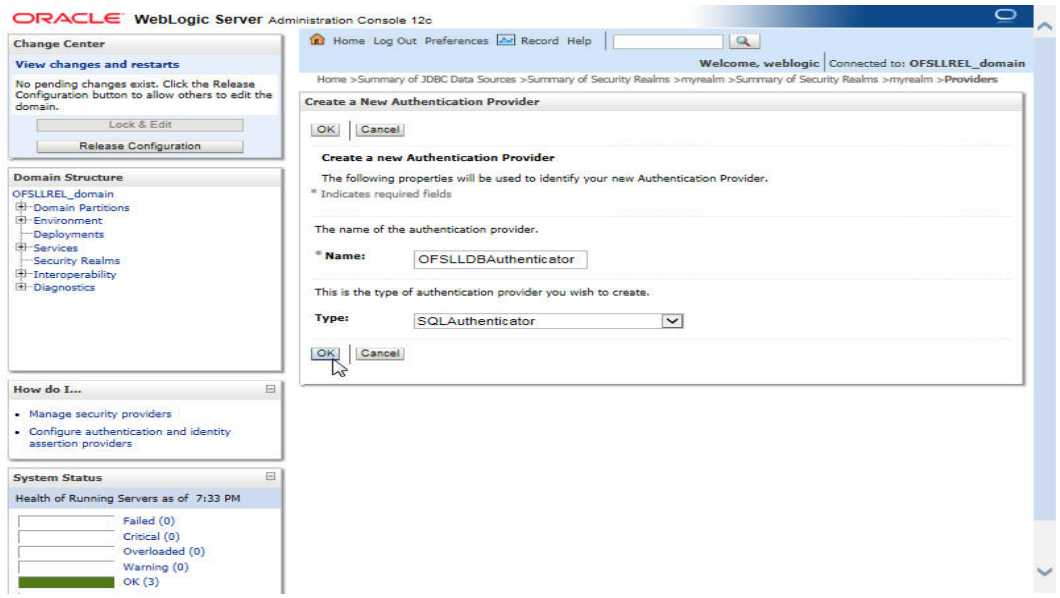
2. Click ‘myrealm’ on right panel. The following window is displayed.



3. Click on Providers tab. The following window is displayed.

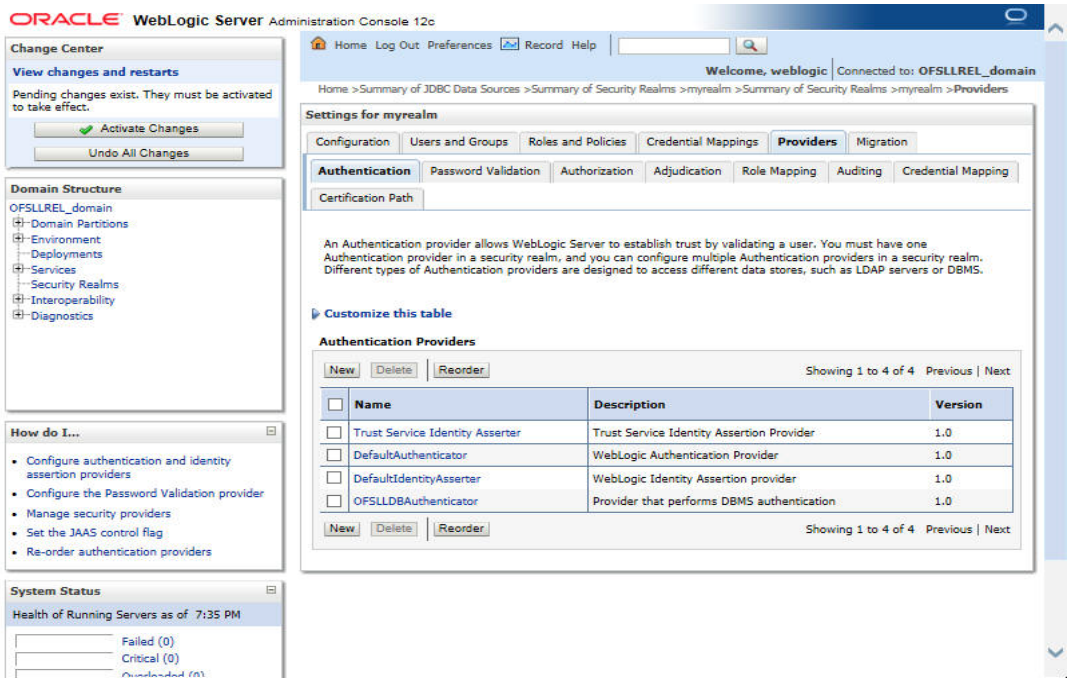


4. Click 'Lock & Edit' to unlock the screen and click 'New' button in Authentication Providers sub tab. The following window is displayed.

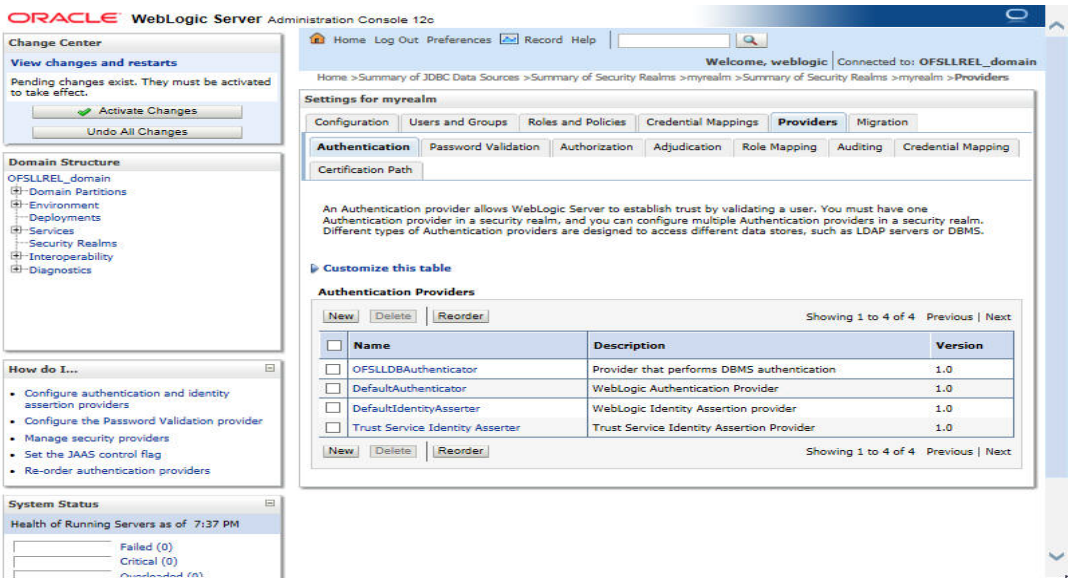


5. Create Authentication provider with following values:
   - Name: OFSLLDBAuthenticator
   - Type: SQLAuthenticator

6. Click ‘OK’. The following window is displayed.

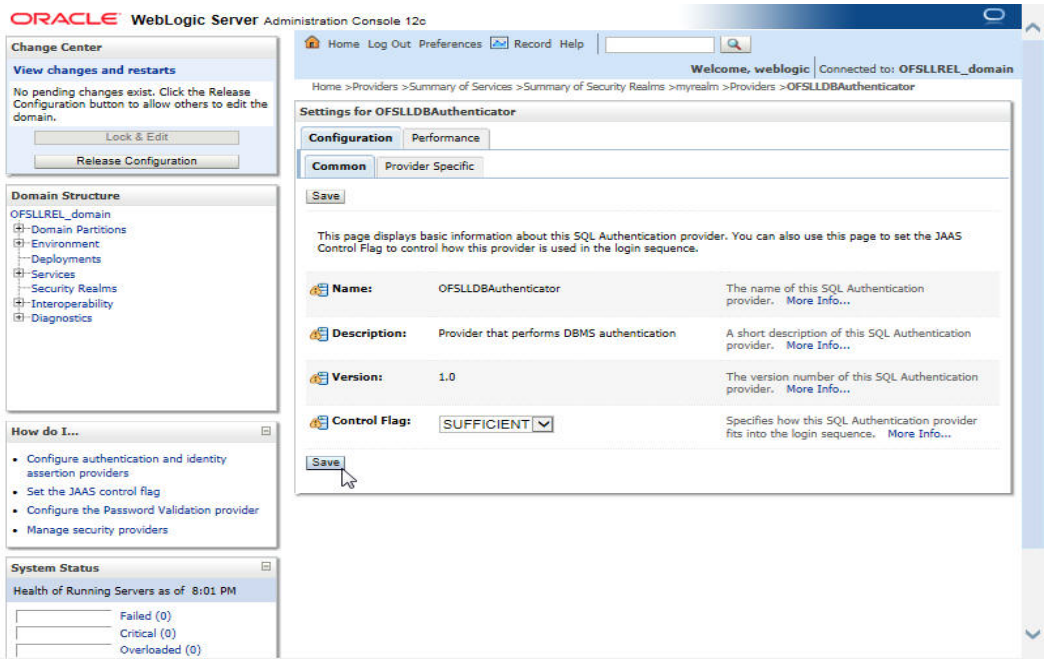


7. Click on ‘Activate Changes’. The following window is displayed.

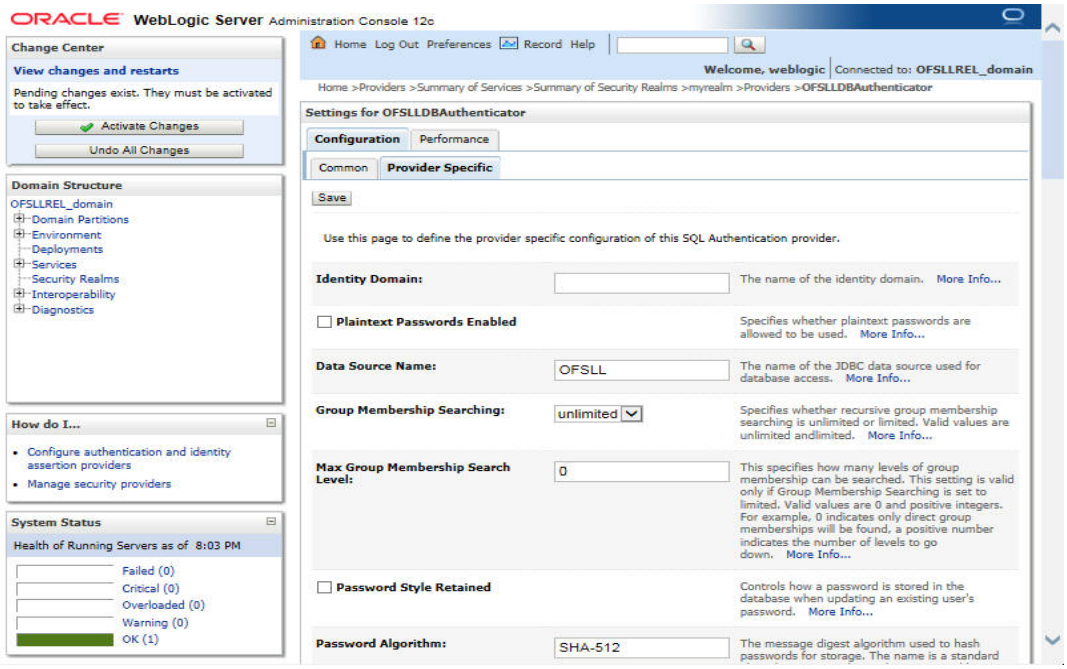


Authentication order should be maintained as mentioned in the above screen. ‘OFSLLDBAuthenticator’ will be displayed as above.

8. Click on ‘OFSLLDBAuthenticator’. The following window is displayed.



9. Select ‘SUFFICIENT’ as the Control Flag and click ‘Save’.
10. Click Provider Specific sub tab under Configuration tab. The following window is displayed.

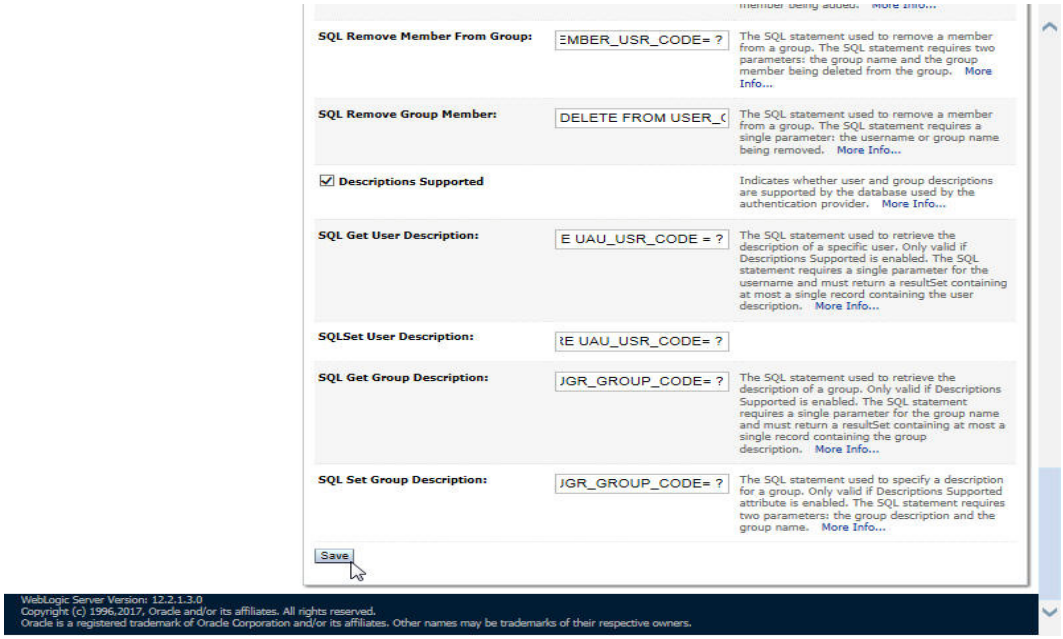


11. Specify the following values in corresponding fields:
    - Data Source Name: OFSLL
    - Password Style Retained: Uncheck
    - Password Algorithm: SHA-512
    - Password Style: SALTEDHASHED

– Provide the SQL Queries from the column Corresponding SQL Queries as per OFSLL Tables as given below.

Operation	Default SQL Query from Weblogic	Corresponding SQL Queries as per our Tables
SQL Get Users Password:	SELECT U_PASSWORD FROM USERS WHERE U_NAME = ?	SELECT UAU_USR_PASSWORD FROM USER_AUTHORISATIONS WHERE UAU_USR_CODE = ?
SQL Set User Password:	UPDATE USERS SET U_PASSWORD = ? WHERE U_NAME = ?	UPDATE USER_AUTHORISATIONS SET UAU_USR_PASSWORD = ? WHERE UAU_USR_CODE = ?
SQL User Exists:	SELECT U_NAME FROM USERS WHERE U_NAME = ?	SELECT UAU_USR_CODE FROM USER_AUTHORISATIONS WHERE UAU_USR_CODE = ?
SQL List Users:	SELECT U_NAME FROM USERS WHERE U_NAME LIKE ?	SELECT UAU_USR_CODE FROM USER_AUTHORISATIONS WHERE UAU_USR_CODE LIKE ?
SQL Create User:	INSERT INTO USERS VALUES (? , ? , ?)	INSERT INTO USER_AUTHORISATIONS(UAU_USR_CODE, UAU_USR_PASSWORD,UAU_DESC) VALUES(?,?,?)
SQL Remove User:	DELETE FROM USERS WHERE U_NAME = ?	DELETE FROM USER_AUTHORISATIONS WHERE UAU_USR_CODE= ?
SQL List Groups:	SELECT G_NAME FROM GROUPS WHERE G_NAME LIKE ?	SELECT UGR_GROUP_CODE FROM USER_GROUPS WHERE UGR_GROUP_CODE LIKE ?
SQL Group Exists:	SELECT G_NAME FROM GROUPS WHERE G_NAME = ?	SELECT UGR_GROUP_CODE FROM USER_GROUPS WHERE UGR_GROUP_CODE = ?
SQL Create Group:	INSERT INTO GROUPS VALUES (? , ?)	INSERT INTO USER_GROUPS(UGR_GROUP_CODE,UGR_GROUP_DESC) VALUES(?,?)
SQL Remove Group:	DELETE FROM GROUPS WHERE G_NAME = ?	DELETE FROM USER_GROUPS WHERE UGR_GROUP_CODE = ?
SQL Is Member:	SELECT G_MEMBER FROM GROUPMEMBERS WHERE G_NAME = ? AND G_MEMBER = ?	SELECT UGM_MEMBER_USR_CODE FROM USER_GROUP_MEMBERS WHERE UGM_MEMBER_GROUP_CODE= ? AND UGM_MEMBER_USR_CODE = ?
SQL List Member Groups:	SELECT G_NAME FROM GROUPMEMBERS WHERE G_MEMBER = ?	SELECT UGM_MEMBER_GROUP_CODE FROM USER_GROUP_MEMBERS WHERE UGM_MEMBER_USR_CODE= ?

Operation	Default SQL Query from Weblogic	Corresponding SQL Queries as per our Tables
SQL List Group Members:	SELECT G_MEMBER FROM GROUPMEMBERS WHERE G_NAME = ? AND G_MEMBER LIKE ?	SELECT UGM_MEMBER_USR_CODE FROM USER_GROUP_MEMBERS WHERE UGM_MEMBER_GROUP_CODE= ? AND UGM_MEMBER_USR_CODE LIKE ?
SQL Remove Group Memberships:	DELETE FROM GROUPMEMBERS WHERE G_MEMBER = ? OR G_NAME = ?	DELETE FROM USER_GROUP_MEMBERS WHERE UGM_MEMBER_USR_CODE= ? OR UGM_MEMBER_GROUP_CODE= ?
SQL Add Member To Group:	INSERT INTO GROUPMEMBERS VALUES(?, ?)	INSERT INTO USER_GROUP_MEMBERS (UGM_MEMBER_GROUP_CODE,UGM_MEMBER_USR_CODE) VALUES(?,?)
SQL Remove Member From Group:	DELETE FROM GROUPMEMBERS WHERE G_NAME = ? AND G_MEMBER = ?	DELETE FROM USER_GROUP_MEMBERS WHERE UGM_MEMBER_GROUP_CODE= ? AND UGM_MEMBER_USR_CODE= ?
SQL Remove Group Member:	DELETE FROM GROUPMEMBERS WHERE G_NAME = ?	DELETE FROM USER_GROUP_MEMBERS WHERE UGM_MEMBER_GROUP_CODE= ?
SQL Get User Description:	SELECT U_DESCRIPTION FROM USERS WHERE U_NAME = ?	SELECT UAU_DESC FROM USER_AUTHORISATIONS WHERE UAU_USR_CODE = ?
SQLSet User Description:	UPDATE USERS SET U_DESCRIPTION = ? WHERE U_NAME = ?	UPDATE USER_AUTHORISATIONS SET UAU_DESC= ? WHERE UAU_USR_CODE= ?
SQL Get Group Description:	SELECT G_DESCRIPTION FROM GROUPS WHERE G_NAME = ?	SELECT UGR_GROUP_DESC FROM USER_GROUPS WHERE UGR_GROUP_CODE= ?
SQL Set Group Description:	UPDATE GROUPS SET G_DESCRIPTION = ? WHERE G_NAME = ?	UPDATE USER_GROUPS SET UGR_GROUP_DESC= ? WHERE UGR_GROUP_CODE= ?
Provider Name	OFSLLDBAuthenticator	



12. Click ‘Save’.

Note

Application server needs to be restarted for these changes to take effect.

3.6 Creating User Groups and Users

3.6.1 Creating Users

Create an OFSLL application super user to login to the application.

A script is provided in the distribution media in the dba_utils folder to create an user.

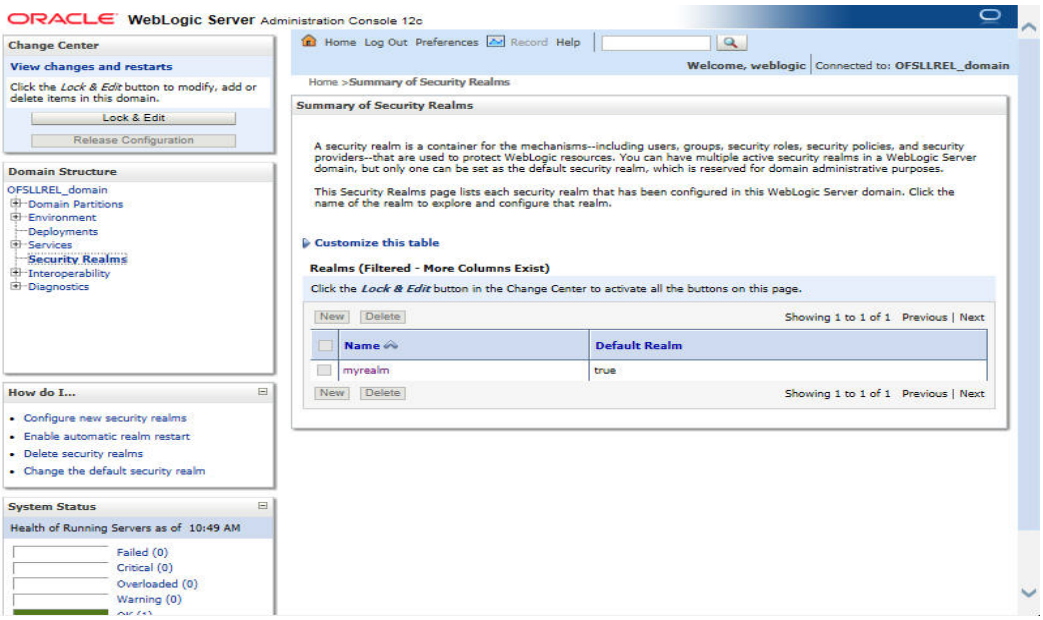
Note

By default there are no users created to login to OFSLL application.

Login as application schema owner and run the script ‘crt_app_user.sql script’ to create OFSLL application user.

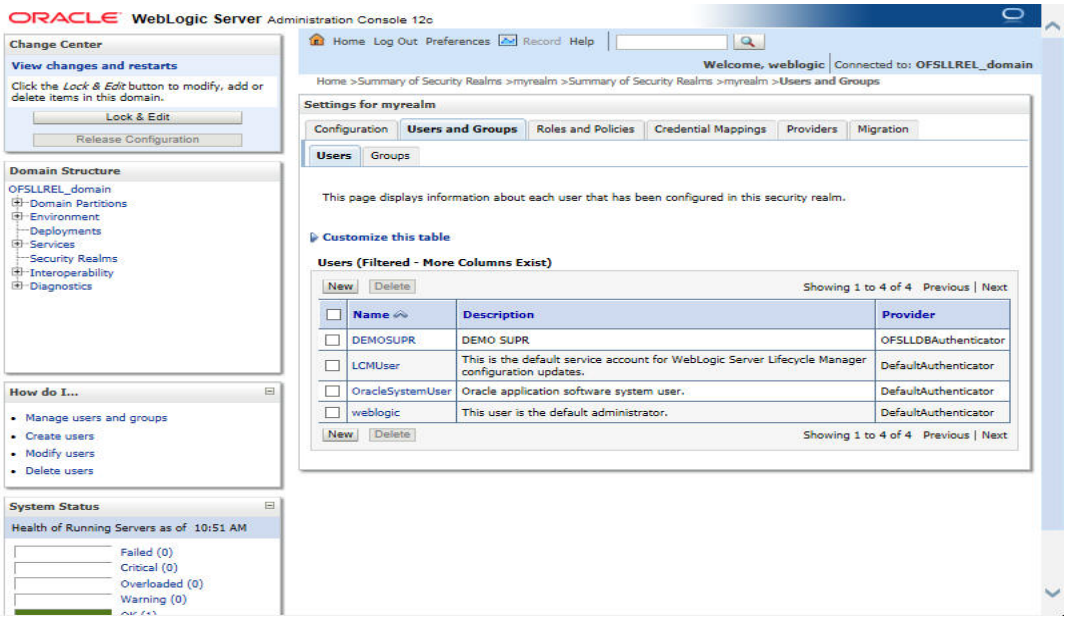
```
SQL*Plus: Release 12.1.0.2.0 Production on Sat Sep 16 10:35:29 2017

Copyright (c) 1982, 2014, Oracle.  All rights reserved.

Enter user-name: OFSLLREL
Enter password:
Last Successful login time: Sat Sep 16 2017 10:38:03 +05:30
Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options

SQL> @crt_app_user.sql
Enter the name of the OFSLL App user Id you
Want to create user: DEMOSUPR
Enter the First Name for this user: DEMO
Enter the Last Name for this user: SUPR
Enter the Phone Number for this user: 9997778886
Enter the Fax Number for this user: 6655544422

1 row created.


1 row created.


1 row created.

SQL> commit;

Commit complete.

SQL>
```

1. Login into WebLogic server console.
2. Click ‘Security Realms’ on the left panel.
3. Click ‘myrealm’ on the right panel..



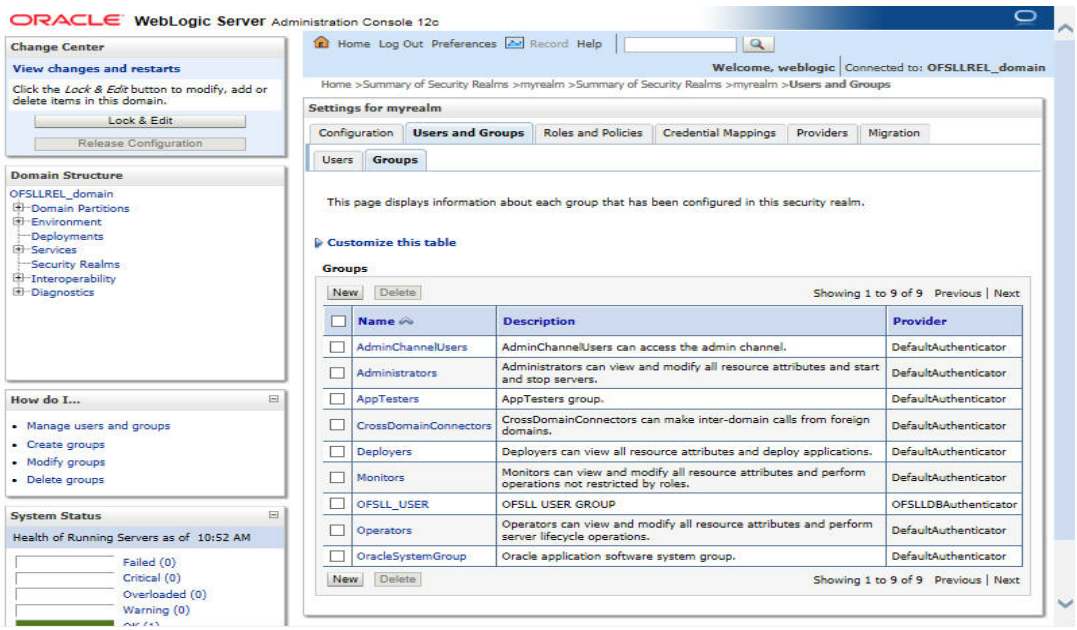
4. Select ‘Users’ tab under Users and Groups.

5. If SQLAuthenticator is configured as a Security Provider for the OFSLL application, the Users are automatically created in weblogic when created through an application.



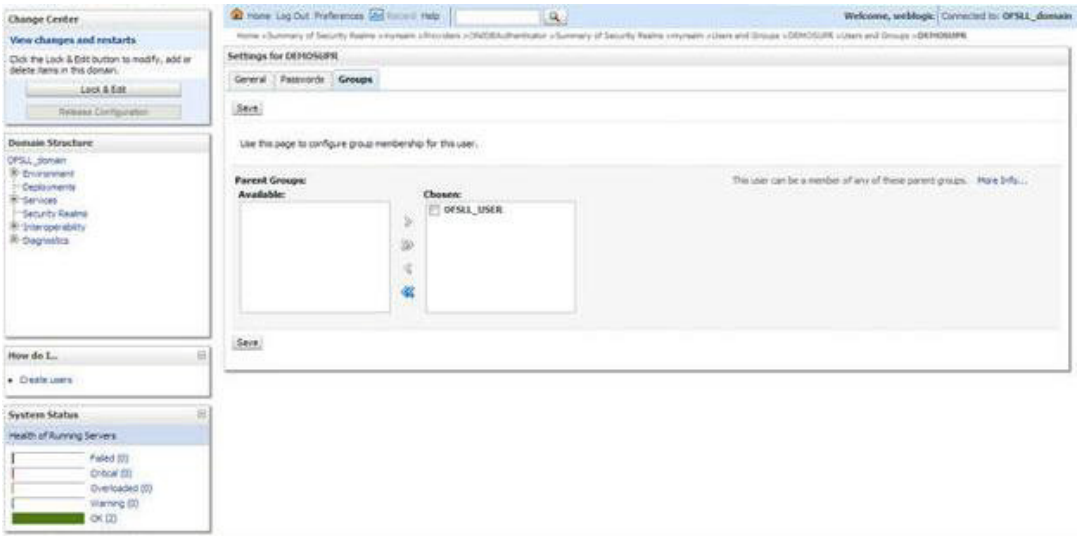
3.6.2 Creating User Groups

1. Select ‘Groups’ tab under Users and Groups.
2. If SQLAuthenticator is configured as a Security Provider for the OFSLL application, the Groups are automatically created in weblogic when created through an application.



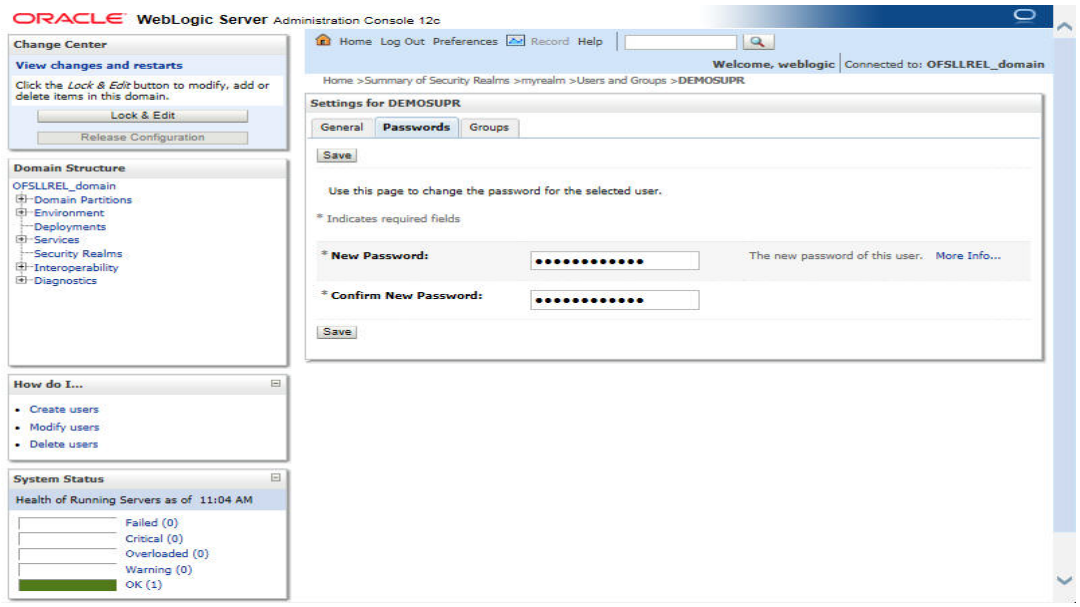
3.6.3 Assigning Users to Groups

The USERS are automatically mapped to default application group - OFSLL_USER.

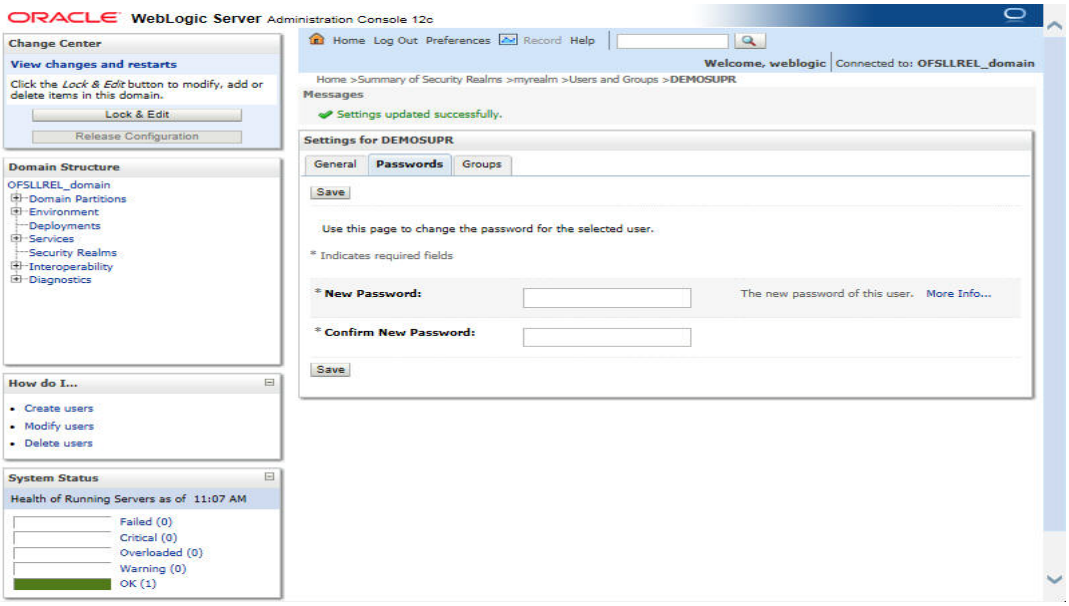


3.6.4 Resetting password via weblogic console

1. Click on 'User'. Select Passwords tab and enter new password and confirm password.



2. Click ‘Save’.The following window displayed.



3.7 Implementing JMX Policy for Change Password

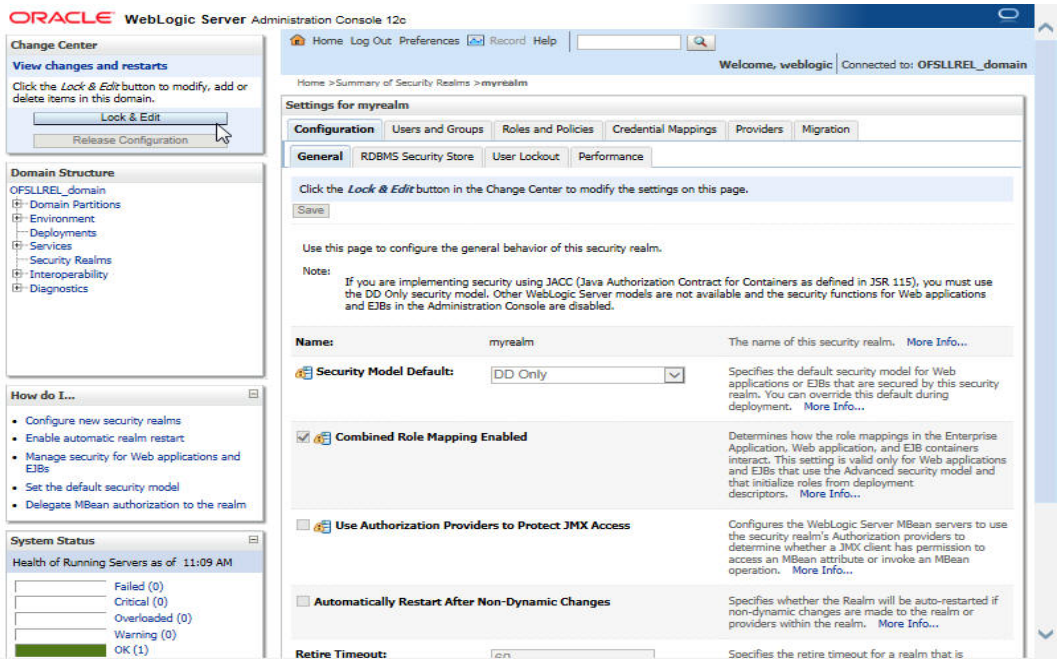
1. Login to Oracle WebLogic Server 12c console (http://hostname:port/console)

Note

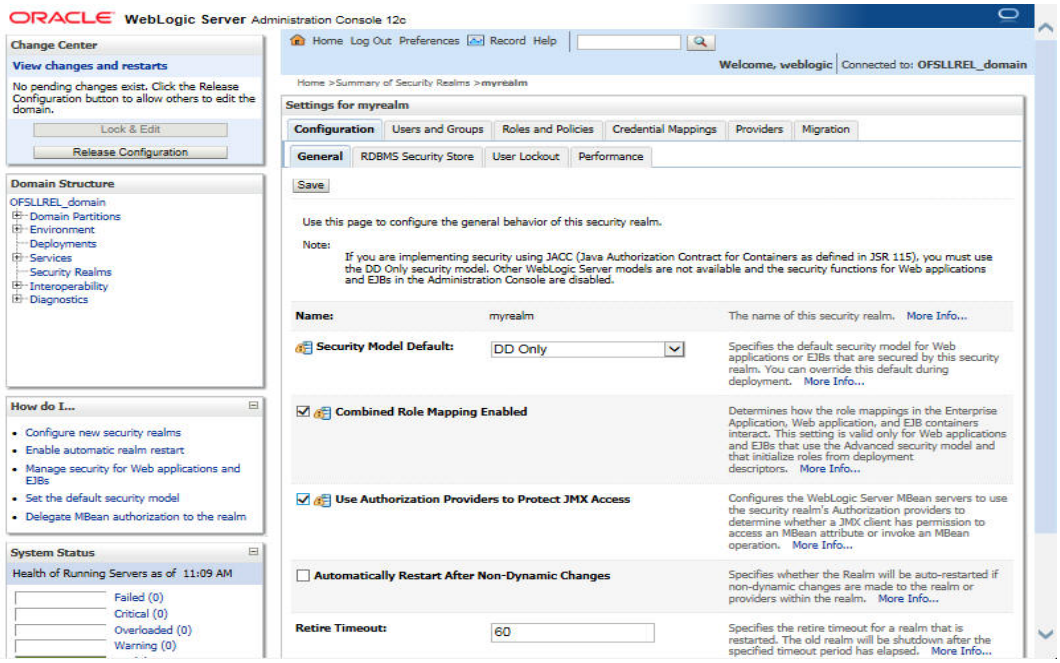
The Change Password feature uses the JMX Policy configured on the domain. Hence, the AdminServer is required to be up and running to enable this.

---

2. Click **Domain > Security > myrealm > Configuration**



3. To enable JMX policy select the ‘Use Authorization Providers to Protect JMX Access’ check box on the right panel



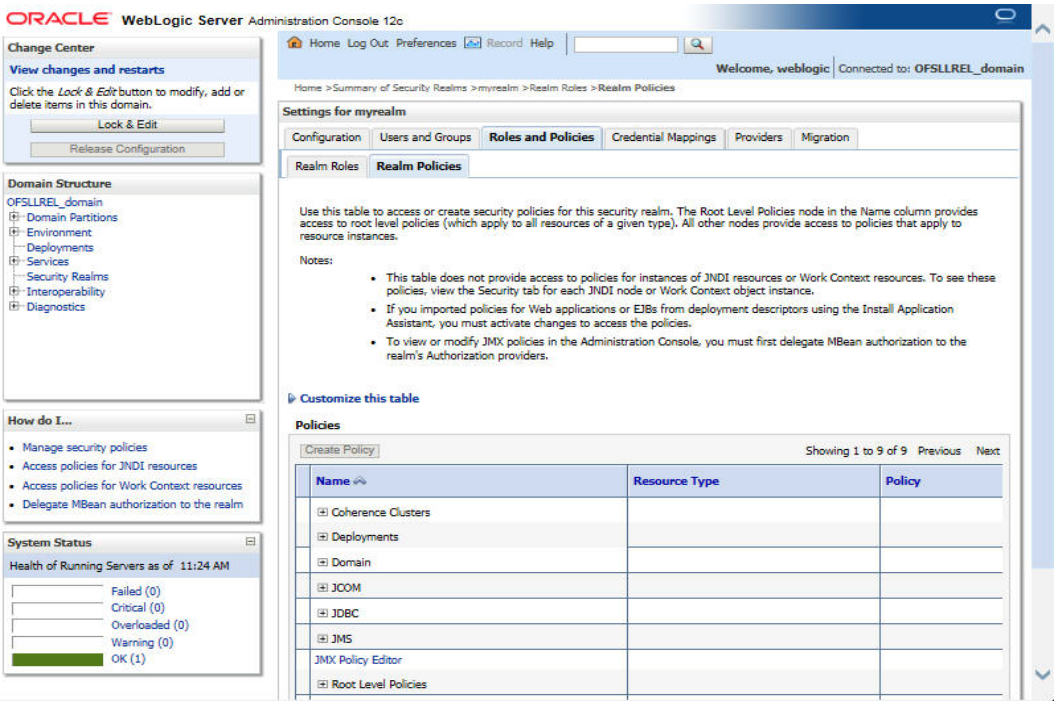
4. Click ‘Save’ and restart the server.
5. Re-login to console.
6. Click Domain > Security > myrealm > Roles and Policies > Realm Policies

---

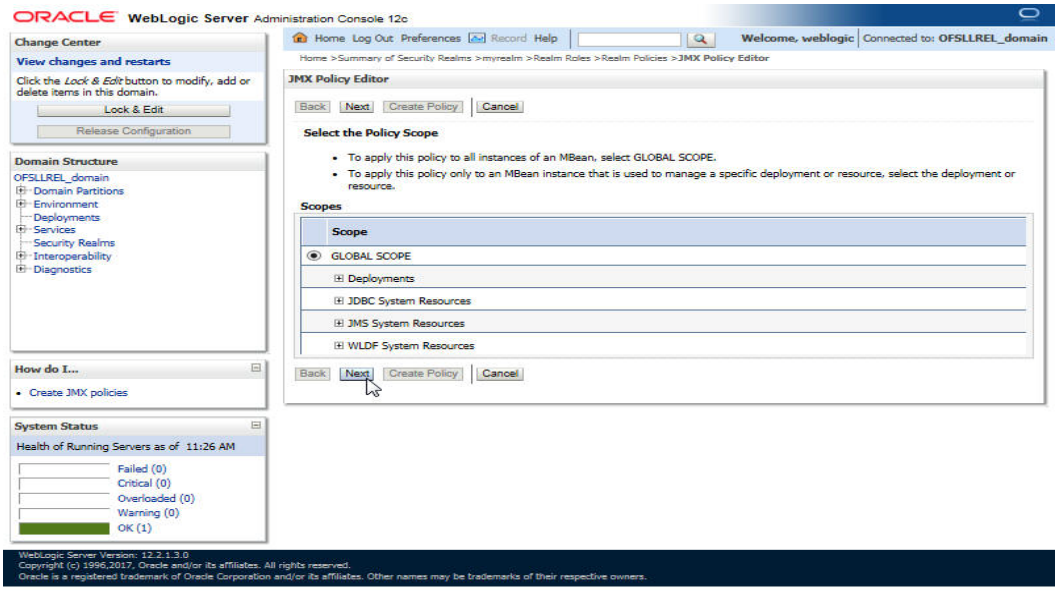
Note

If server is not restarted, JMX Policy Editor option will not appear

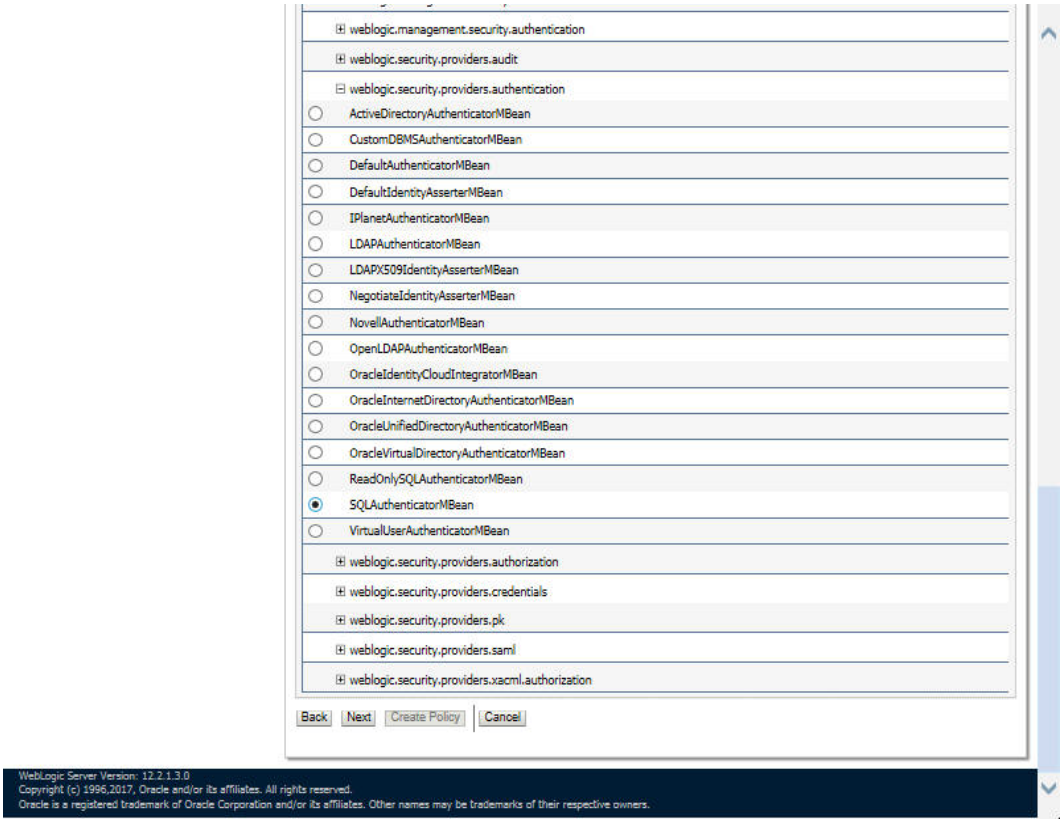
---



7. Click on JMX Policy Editor to configure

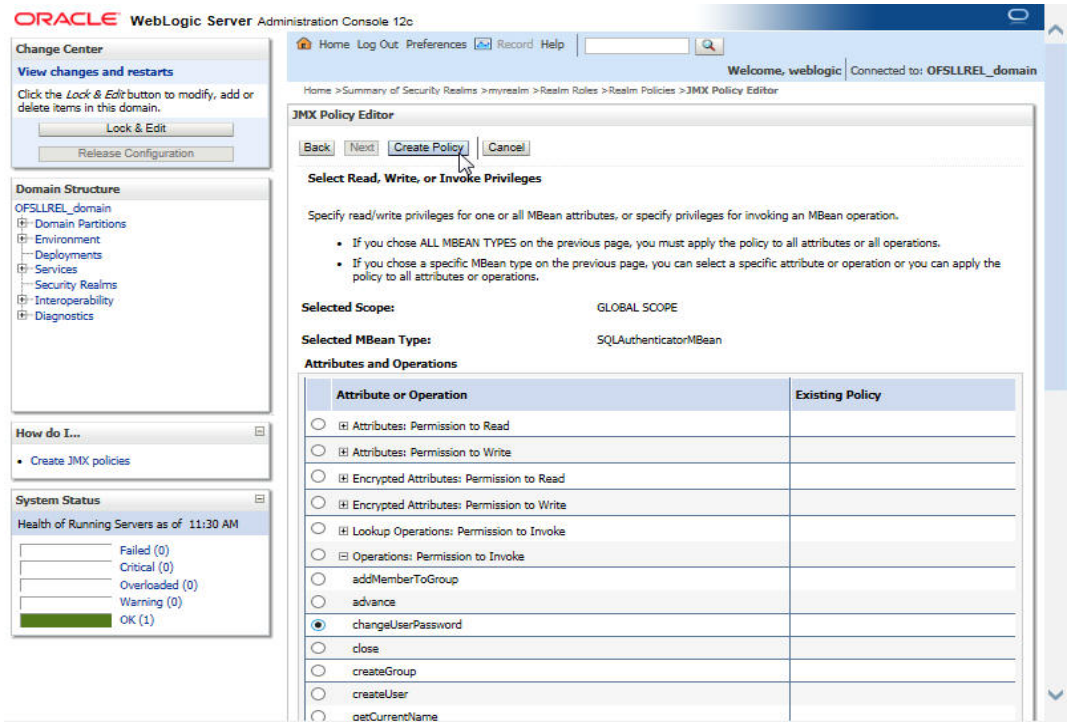


8. Select ‘GLOBAL SCOPE’ and click ‘Next’.

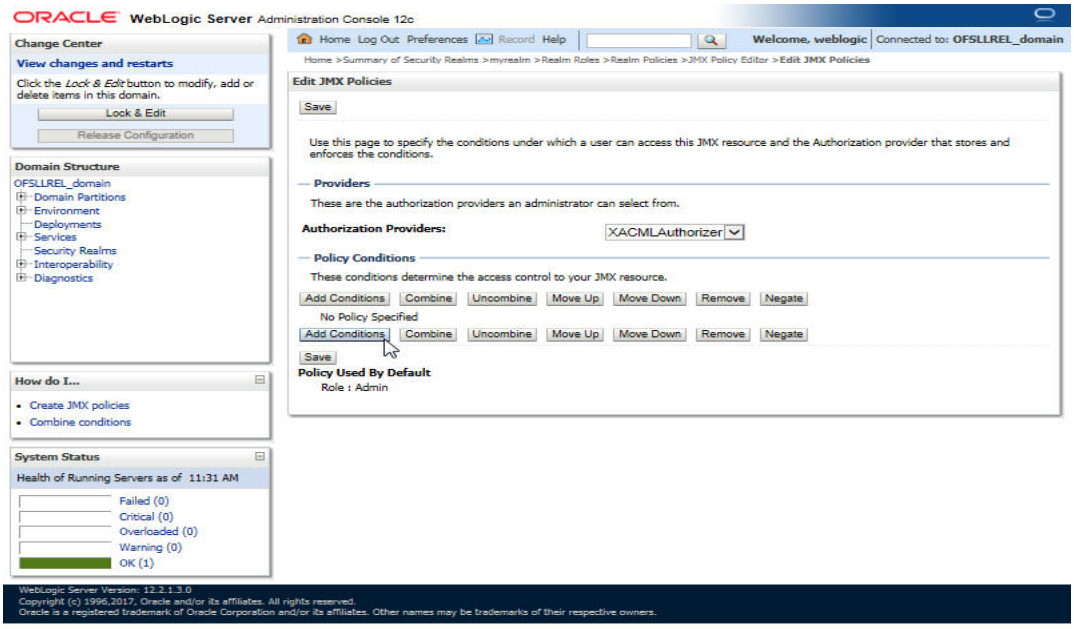


9. Select weblogic.security.providers.authentication.

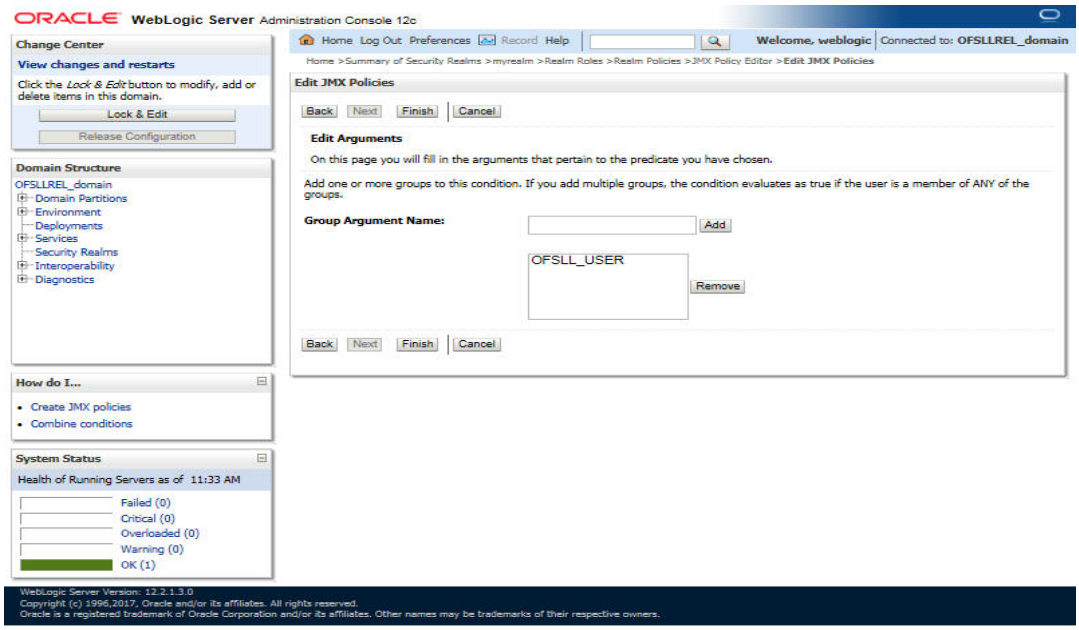
10. Select ‘SQLAuthenticatorMBean’. Click ‘Next’.



11. Expand ‘Operations: Permissions to Invoke’ and select ‘ChangeUserPassword’.
12. Click ‘Create Policy’. The following window is displayed for Authorization providers where you can add conditions to setup the policy.
13. Click ‘Add Condition’. The below screen will be displayed.

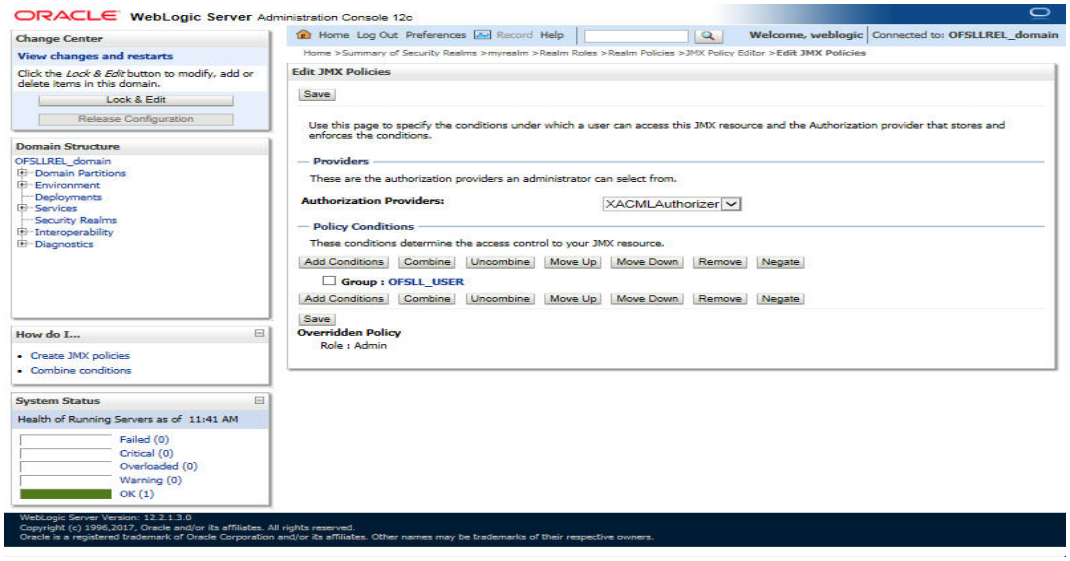


14. For Predicate List, select Group for configuration. Click ‘Next’.



15. Select user roles for application.

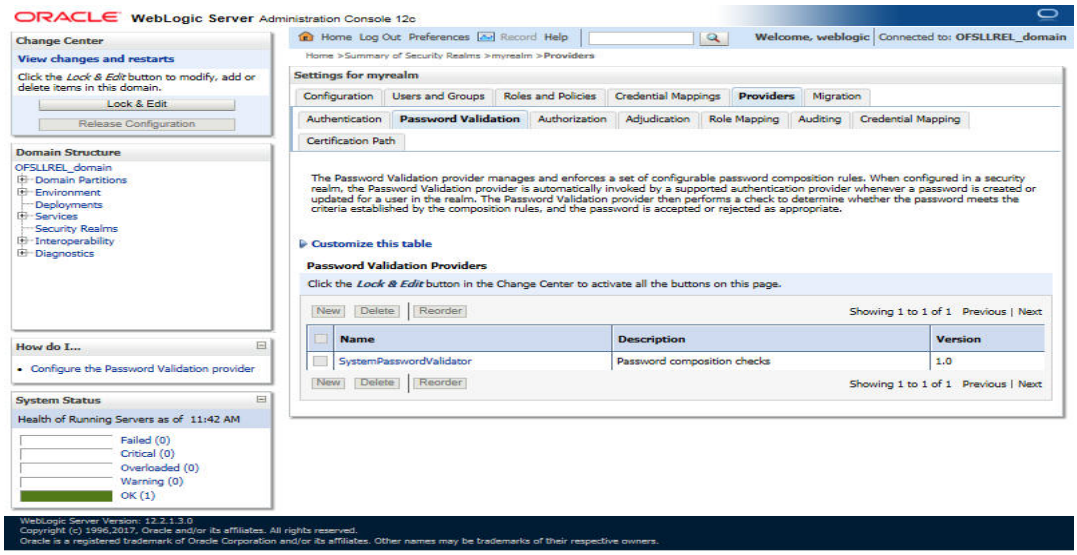
16. Click ‘Finish’. Click ‘Save’ to complete the configuration. The following window will be displayed.



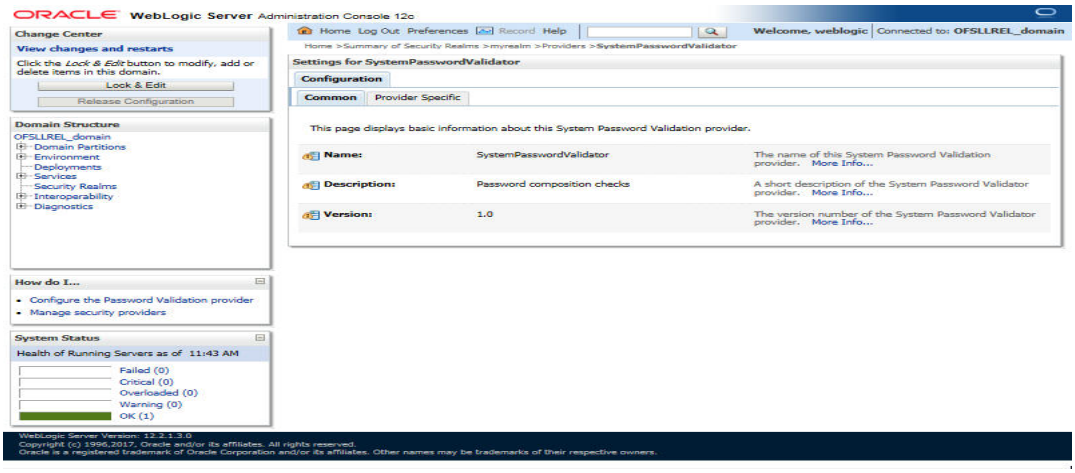
4. Configuring Policies

4.1 Configuring Password Policy for SQL Authenticator

1. Login to the WebLogic server administration console with user login credentials.
2. Browse to Security Realms > myrealm > Providers > Password Validation as shown below. The following window is displayed

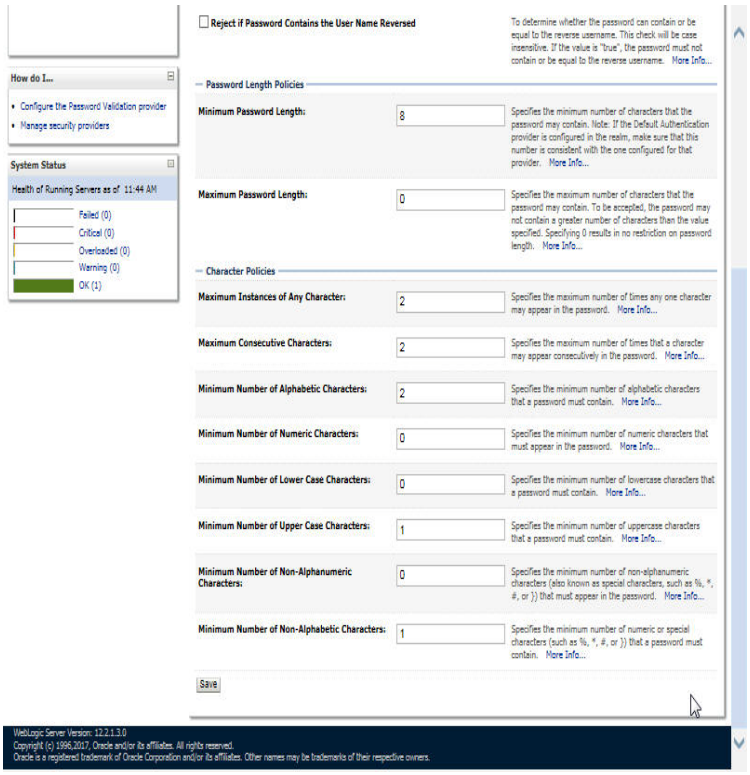


3. Click 'SystemPasswordValidator' link. The following window is displayed.



4. Click **Provider Specific** Tab.

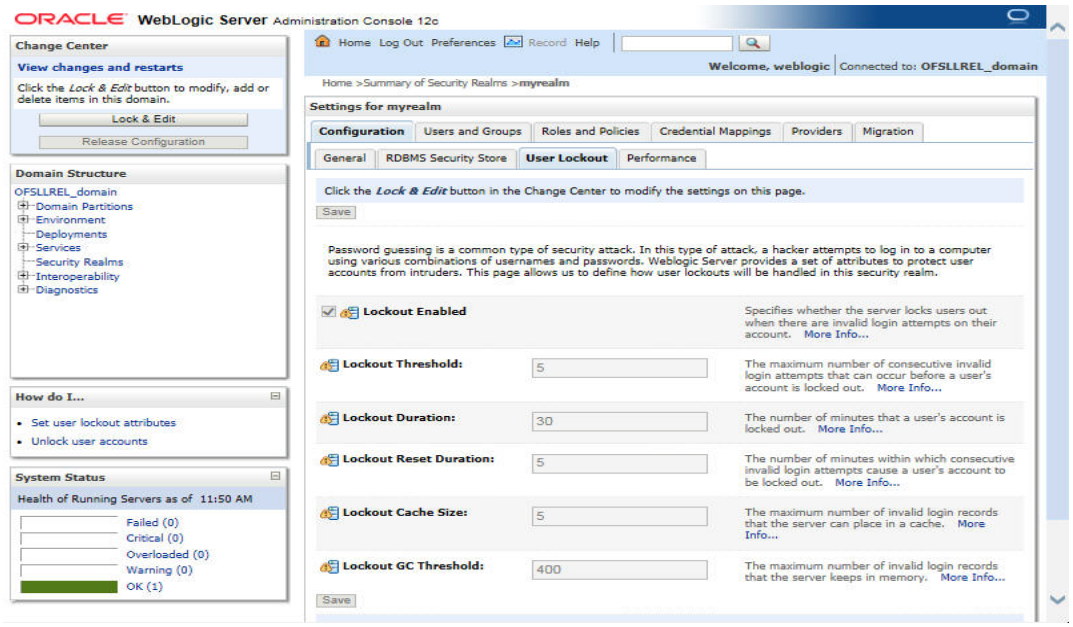
5. Configure the password policy as per the requirement. An example is provided in the following window.



6. Click ‘Save’.

4.2 Configuring User Lockout Policy

1. To Change User lockout policy, browse to **Security Realms > myrealm > Configuration** Tab **> User Lockout** Tab. The following window is displayed



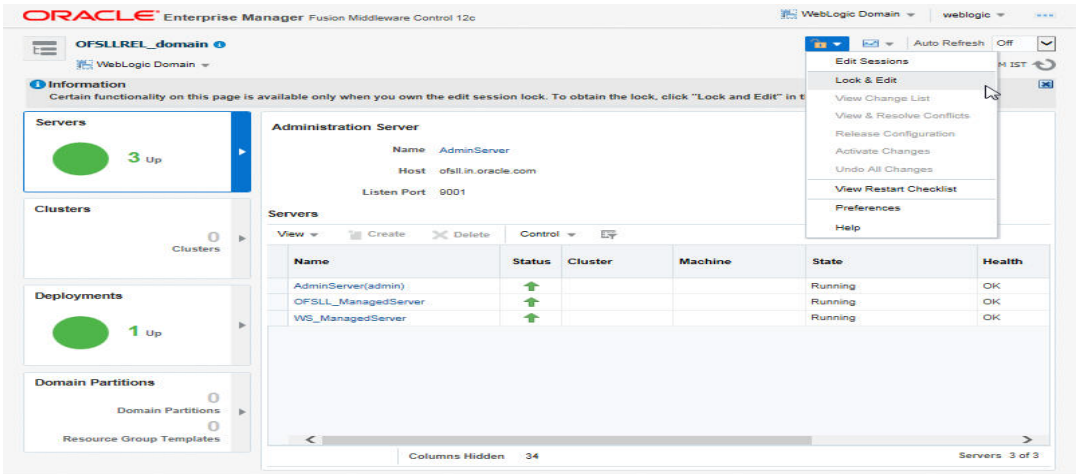
2. Configure the User Lockout details as per the requirement. An example is provided above.

5. Deploying Application

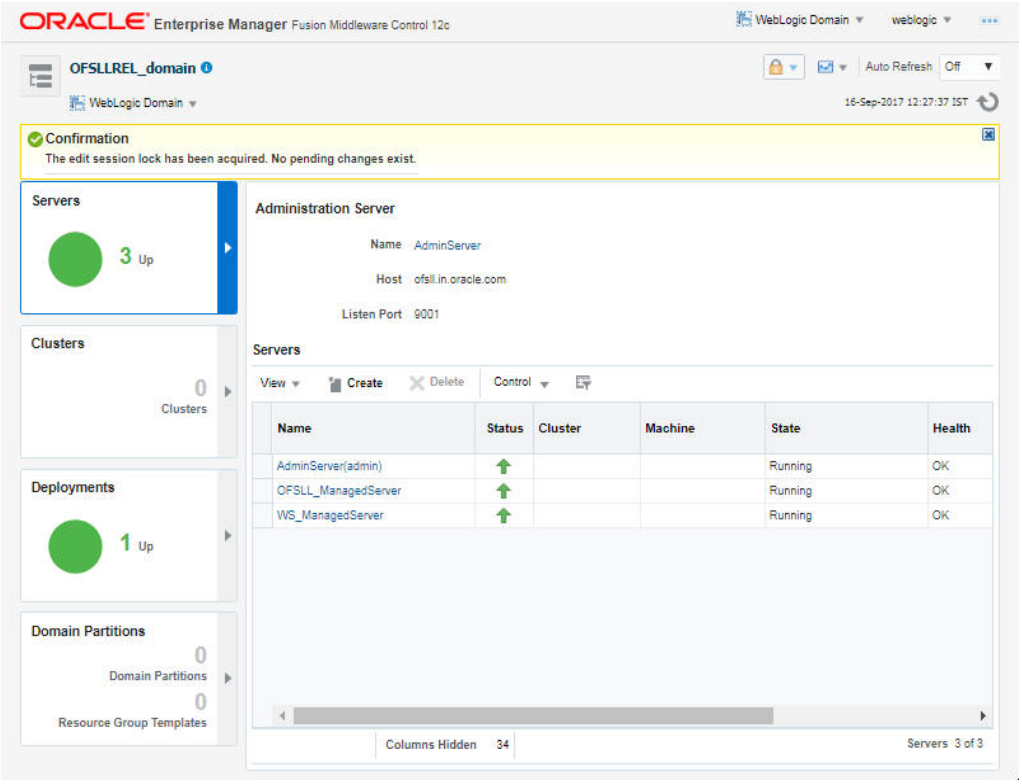
5.1 Deploying Application

1. Login to the Oracle Enterprise Manager 12c console . (i.e. http://hostname:port/em)

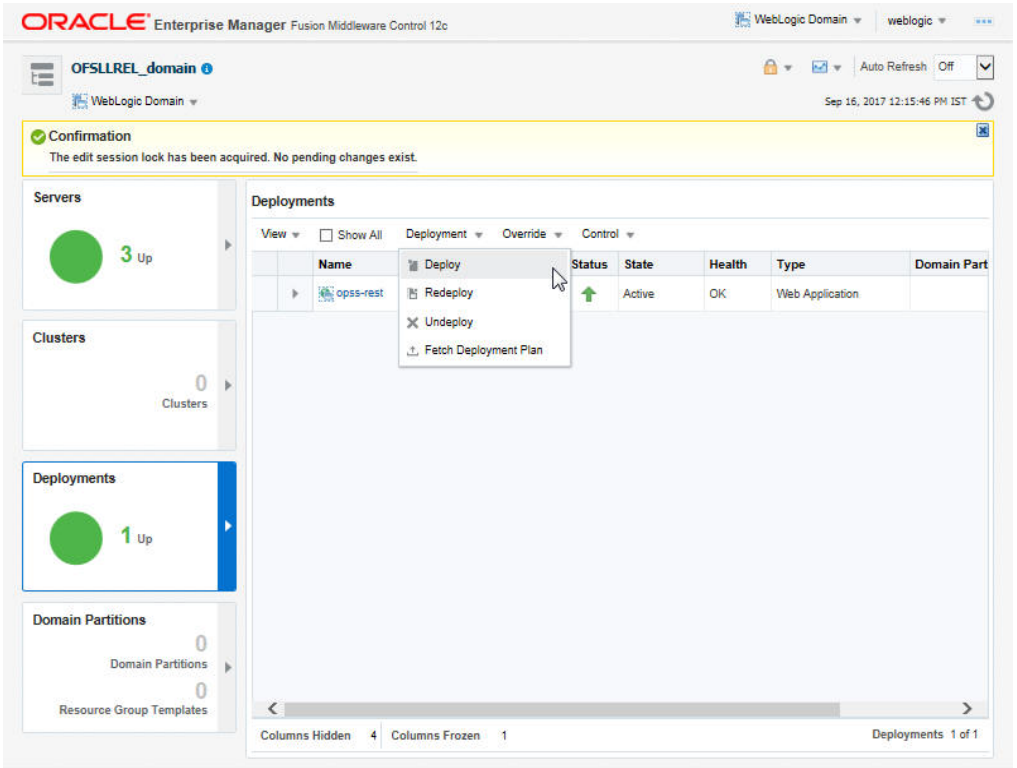
2. Click on 'Lock and Edit' as shown below.



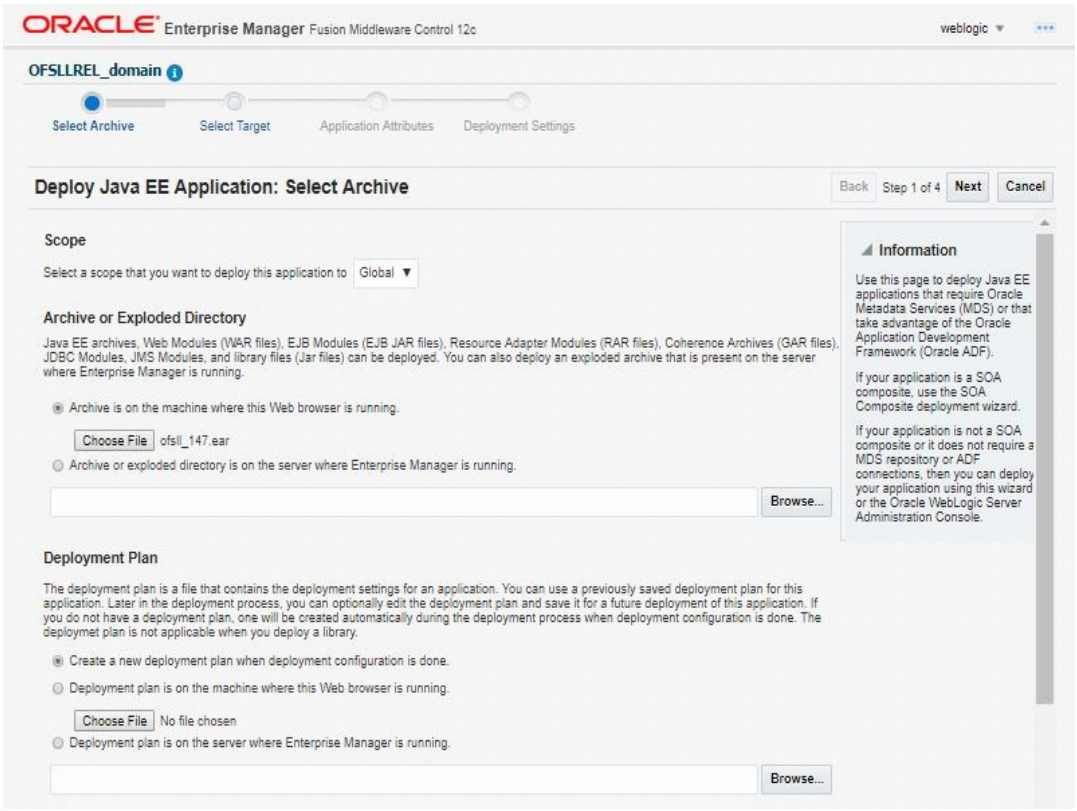
3. The following window is displayed.



4. Click on Deployments in the left panel. To deploy go to Deployments option in the menu as shown below.



5. Click ‘Choose File’ button and select OFSLL application archive file i.e. ofsll_146.ear. Choose the ‘Deployment Plan’ (if any).



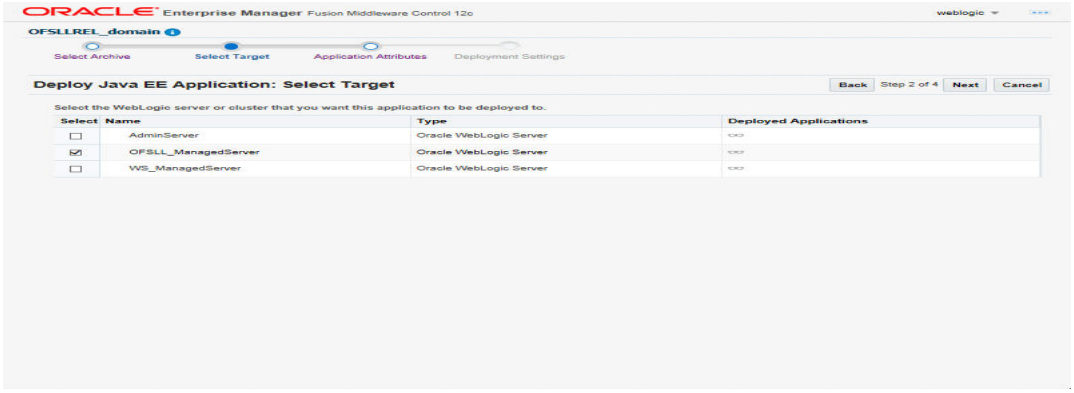
Note

A deployment plan can be used to easily change an application's WebLogic Server configuration for a specific environment without modifying existing deployment descriptors.

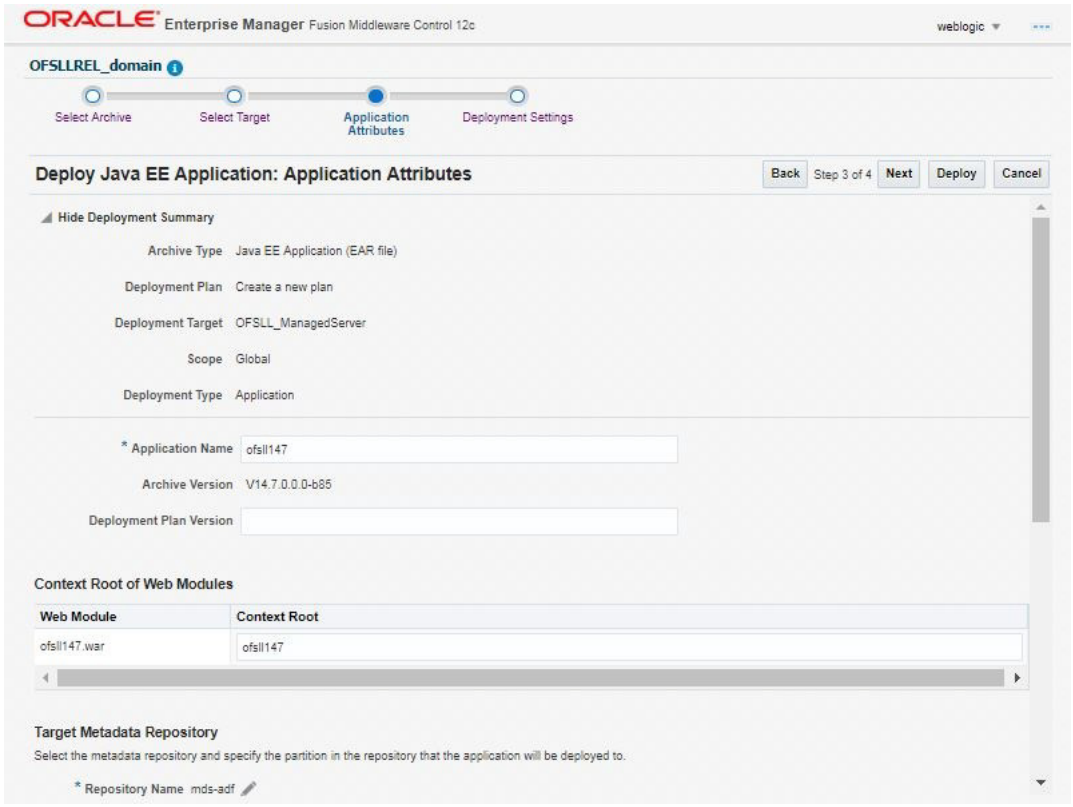
Sample plan.xml

```
<?xml version='1.0' encoding='UTF-8'?>
<deployment-plan xmlns="http://xmlns.oracle.com/weblogic/deployment-plan" xmlns:xsi="http://www.w3.org/2001/XMLSch
  <application-name>ofsllrel</application-name>
  <variable-definition>
    <variable>
      <name>Web_ofsllrel_contextRoot</name>
      <value>ofsllrel</value>
    </variable>
  </variable-definition>
  <module-override>
    <module-name>ofsllrel.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>
      <variable-assignment>
        <name>Web_ofsllrel_contextRoot</name>
        <xpath>/application/module/web/[context-root="ofsllrel"]/context-root</xpath>
        <operation>replace</operation>
      </variable-assignment>
    </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>ofsllrel.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>
    </module-descriptor>
    <module-descriptor external="false">
      <root-element>web-app</root-element>
      <uri>WEB-INF/web.xml</uri>
    </module-descriptor>
  </module-override>
  <module-override>
    <module-name>empty.jar</module-name>
    <module-type>car</module-type>
    <module-descriptor external="true">
      <root-element>weblogic-application-client</root-element>
      <uri>META-INF/weblogic-application-client.xml</uri>
    </module-descriptor>
    <module-descriptor external="false">
      <root-element>application-client</root-element>
      <uri>META-INF/application-client.xml</uri>
    </module-descriptor>
  </module-override>
```

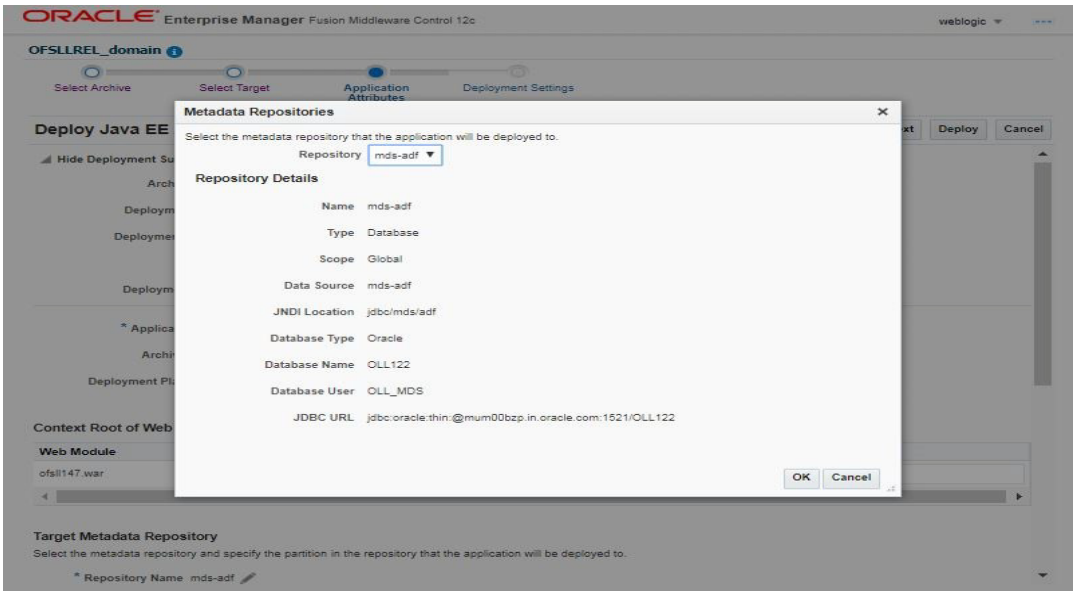
6. Click ‘Next’. The following window is displayed.



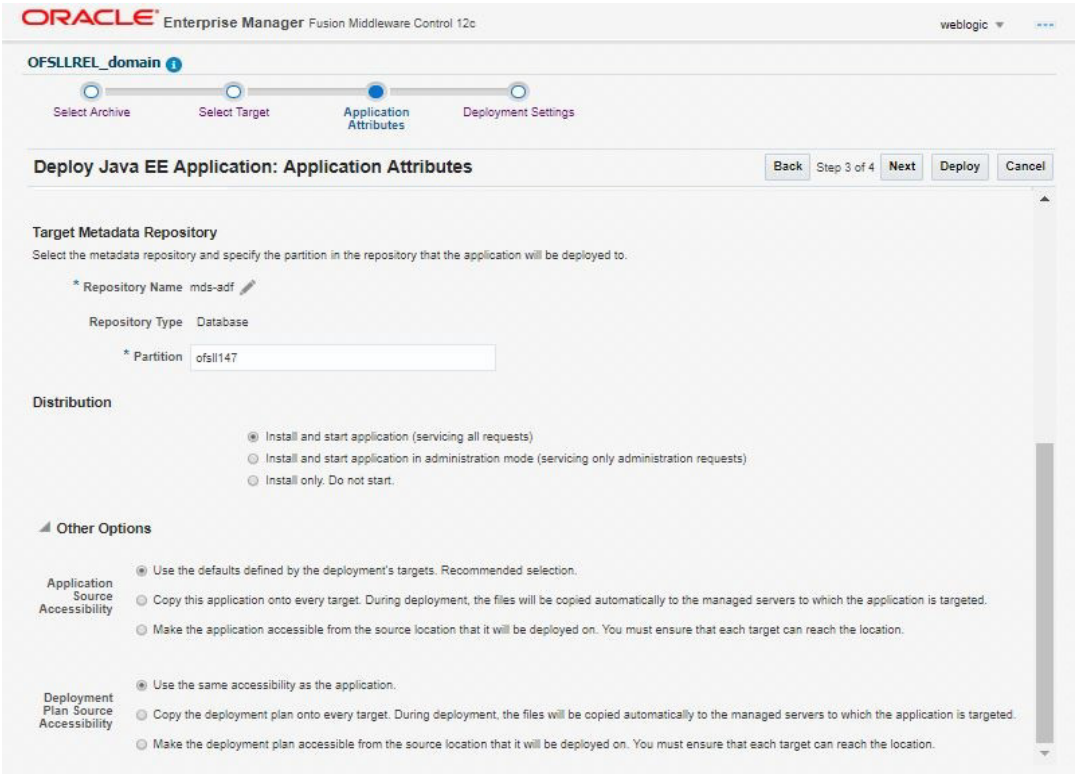
7. Check target server as per the requirement ‘OFSLL_ManagedServer’ and click ‘Next’. The following window is displayed.



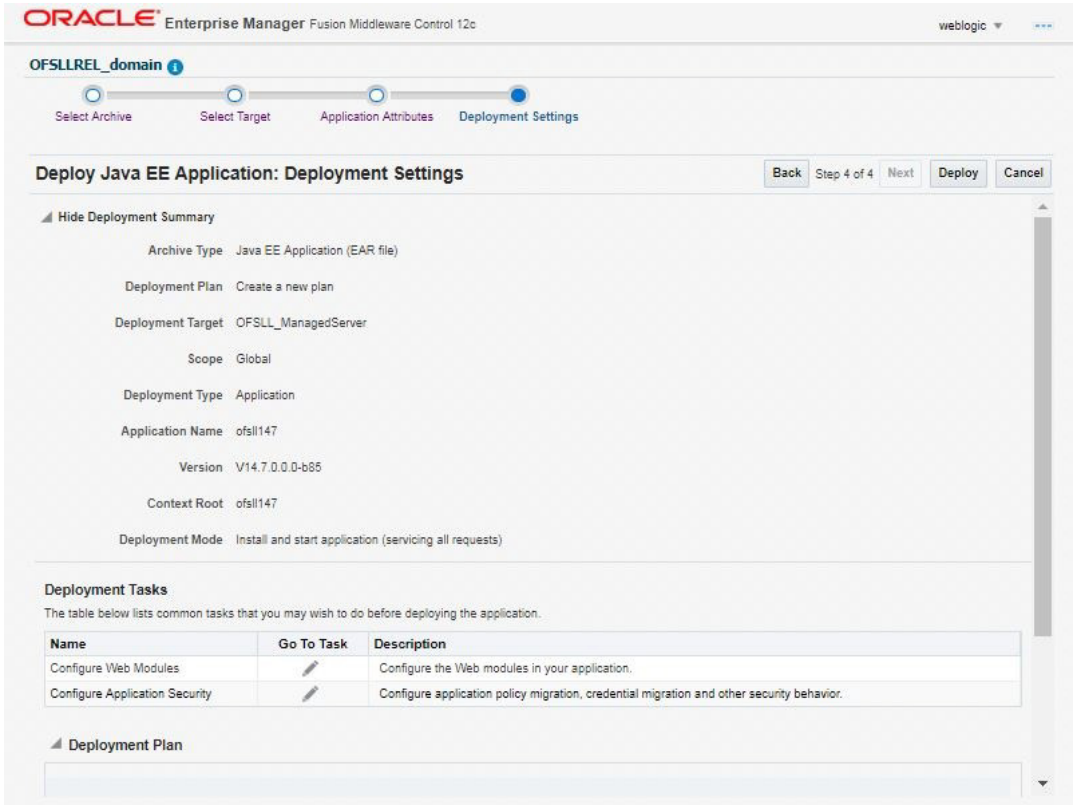
8. Click button to select Repository Name. The following window is displayed.



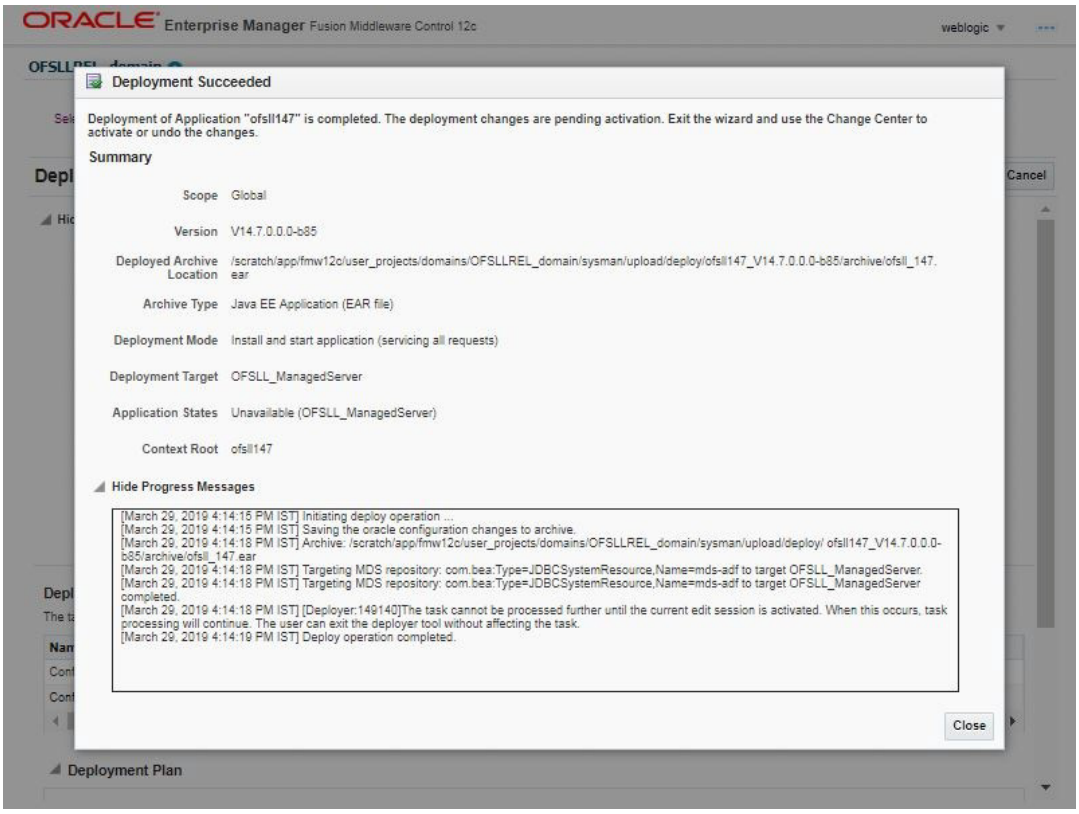
9. Select Repository as per requirement and click ‘OK’.



10. Enter Partition name as per the requirement and click ‘Next’.



11. Click ‘Deploy’. The following window is displayed



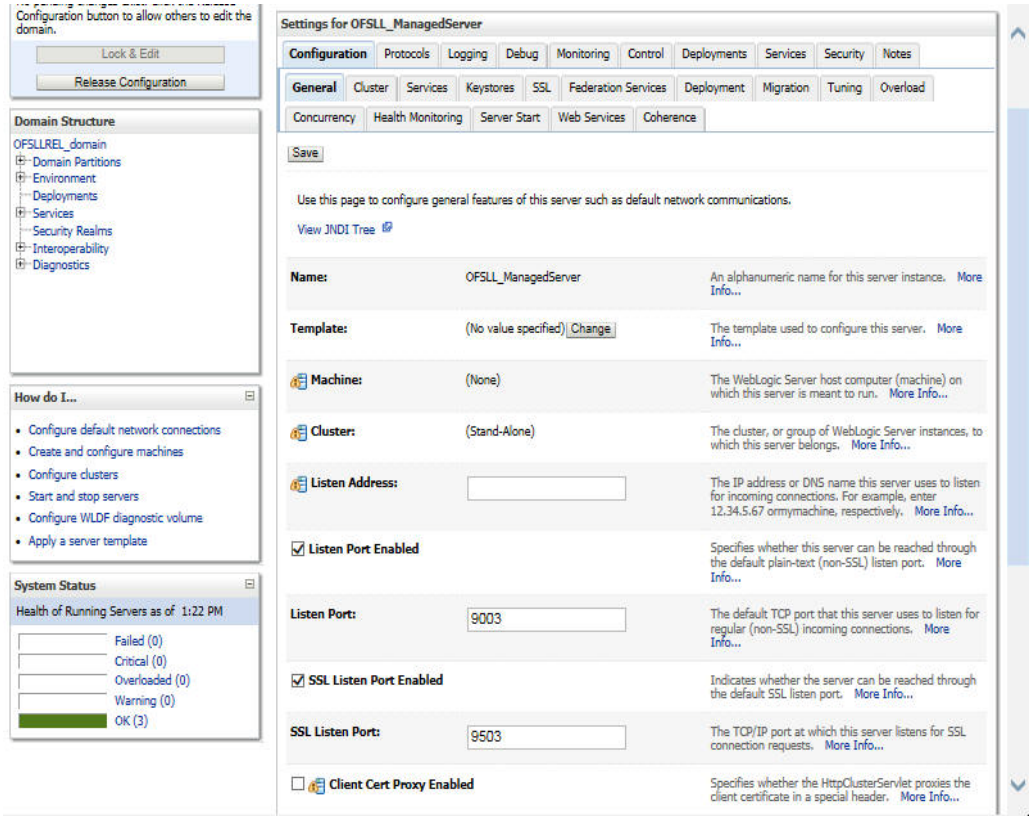
12. Click Close once the message ‘Deploy operation completed’ is displayed.

6. Enabling SSL

The application is accessible only via https protocol; hence, after the deployment of the application, you need to enable SSL.

To enable SSL

1. Login to console.
2. $Domain_Home > Servers > Manage Servers > Configuration > General. The below screen is displayed.



3. Check the ‘SSL Listen Port Enabled’ check box.
4. Specify the port for ‘SSL Listen Port’.

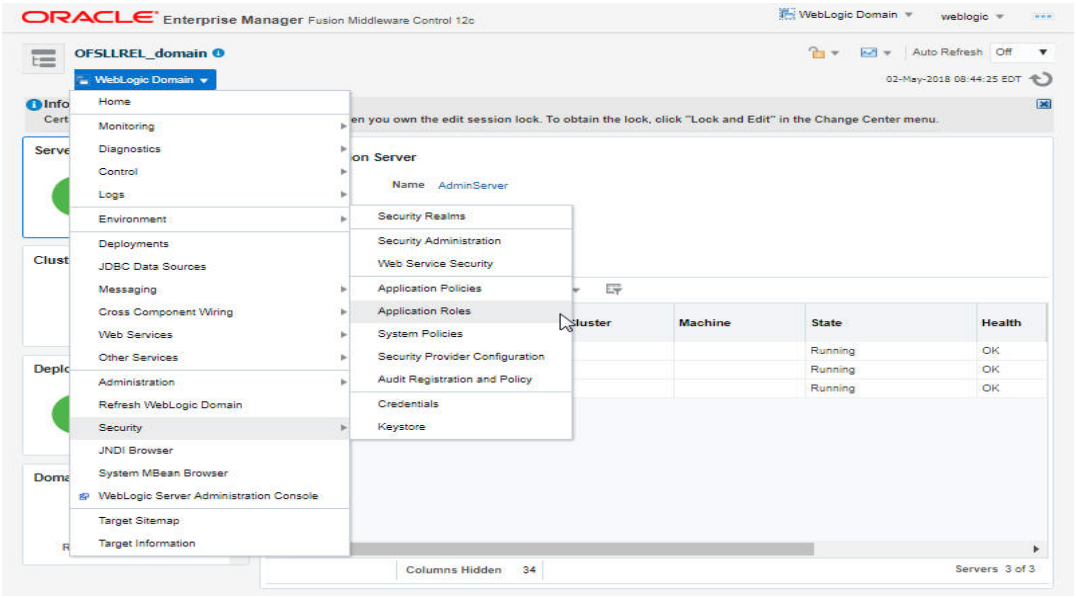
Note

It is recommended to disable http protocol.

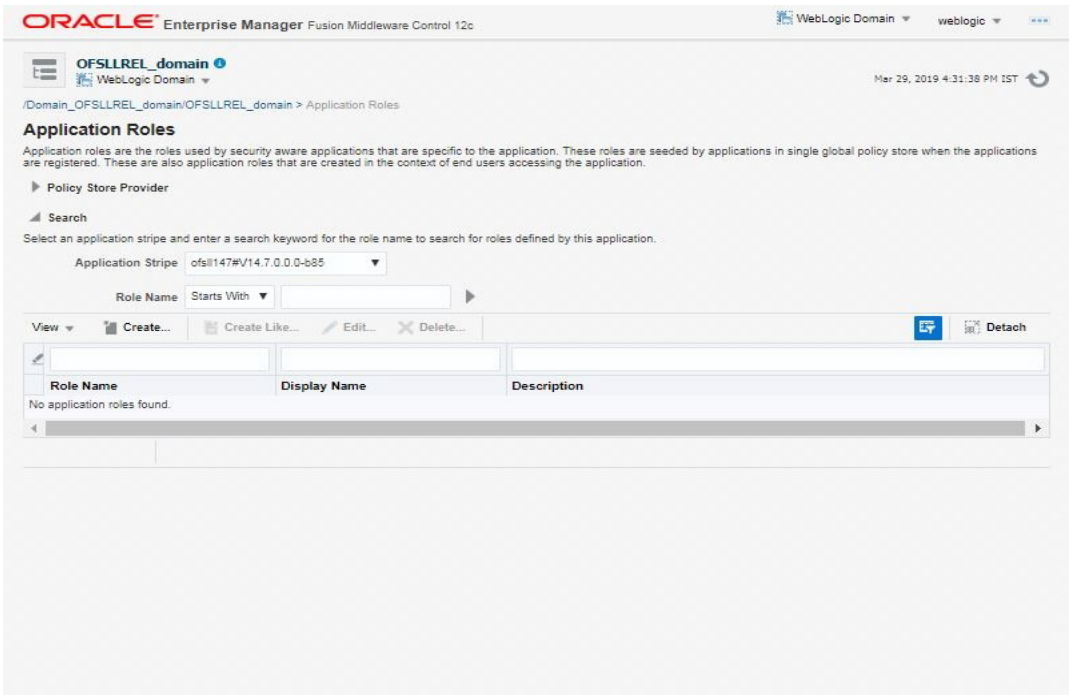
7. Mapping Enterprise Group with Application Role

Follow the below steps to add an user to the group

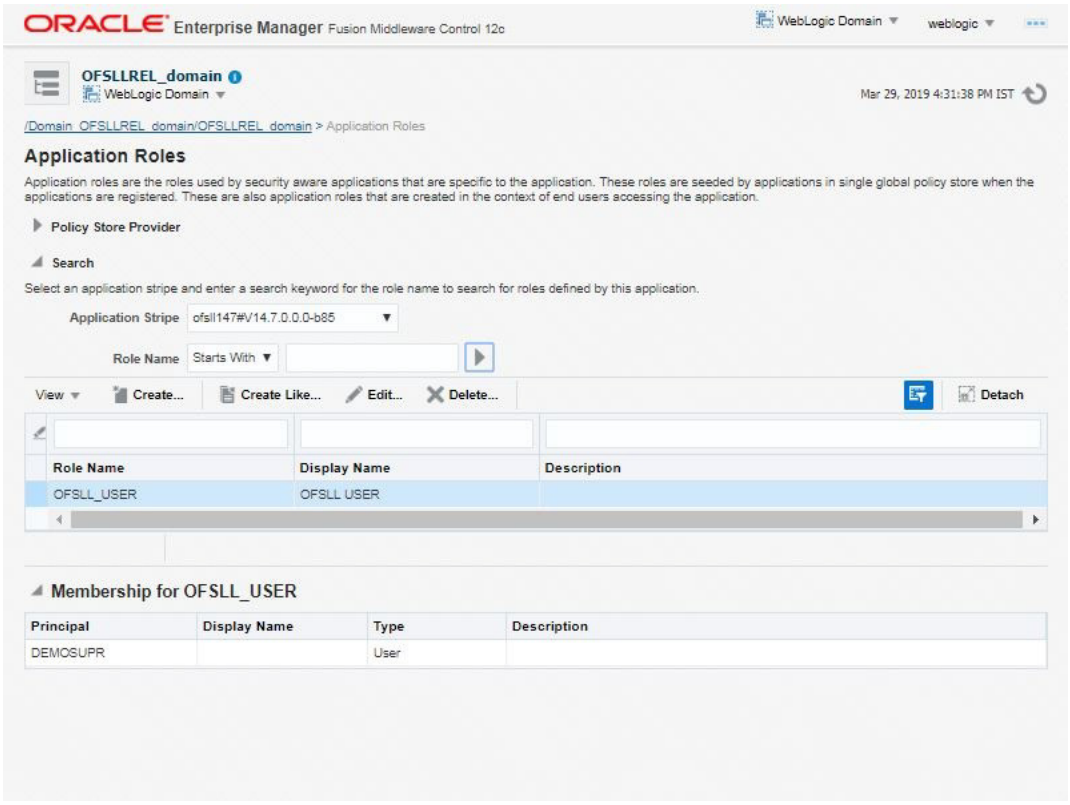
1. Login to Oracle Enterprise Manager 12c console (http://hostname:port/em).
2. Click WebLogic Domain > Security > Application Roles on the right panel.



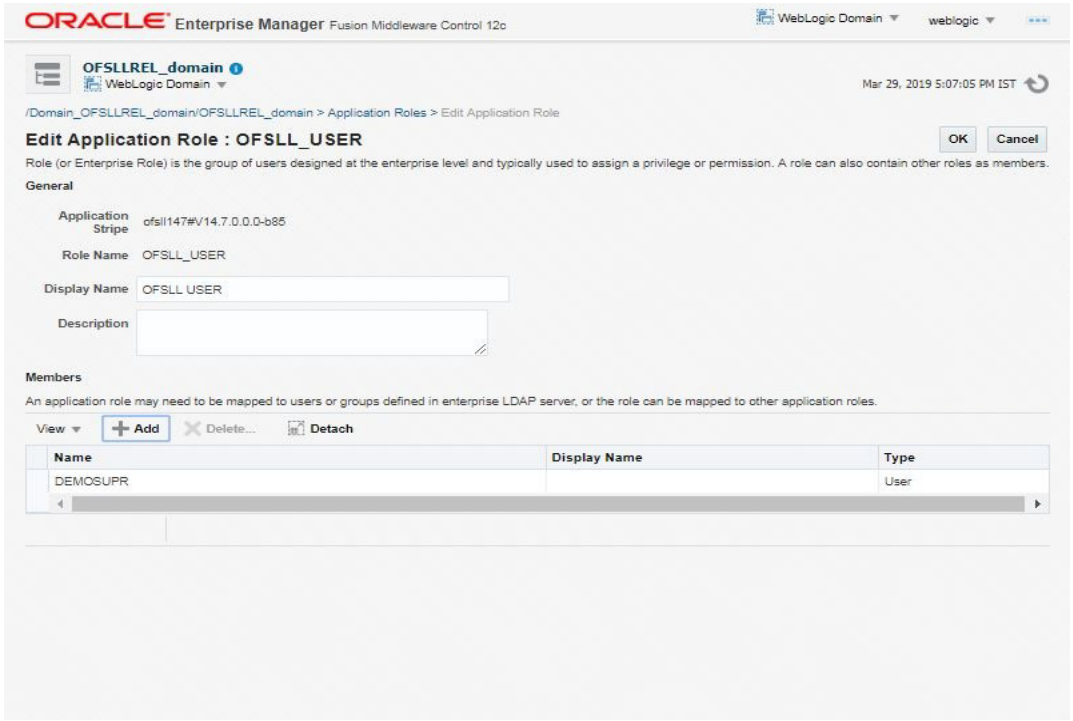
3. Select Application Stripe from the drop-down menu.
4. Click the arrow head button. Details of the existing Roles are displayed below:



5. Select the ‘Role Name’. Membership details of the selected Role Name are displayed under Membership for "role_name"..

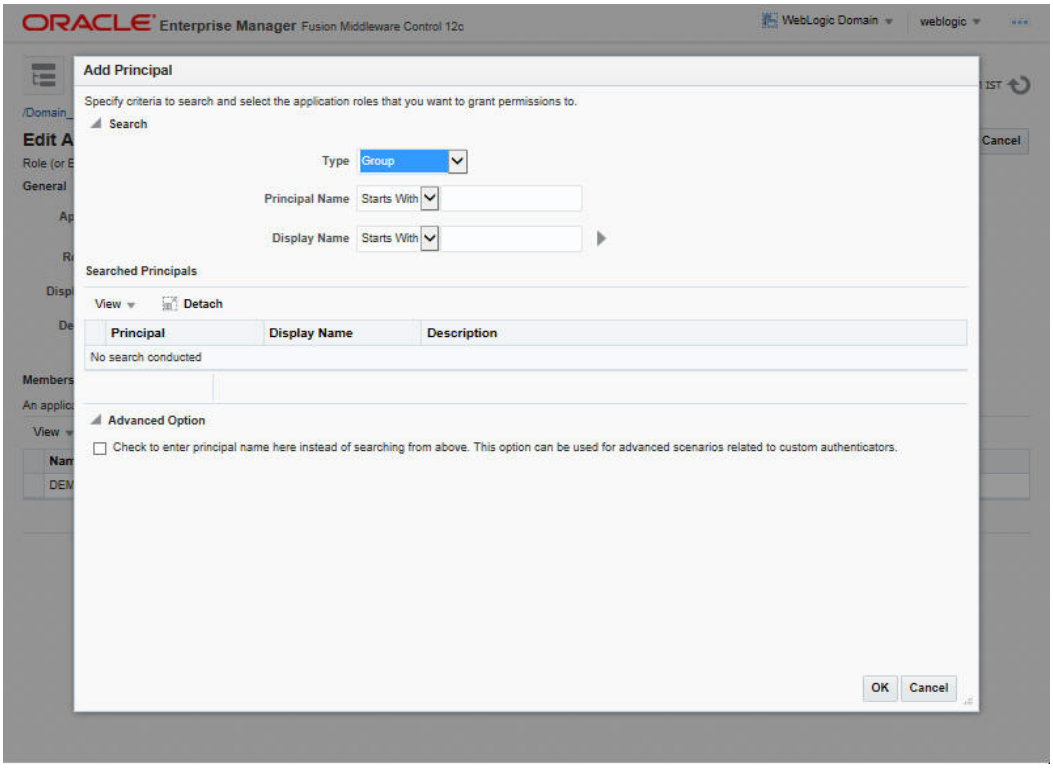


6. Click ‘Edit’. The following window is displayed.

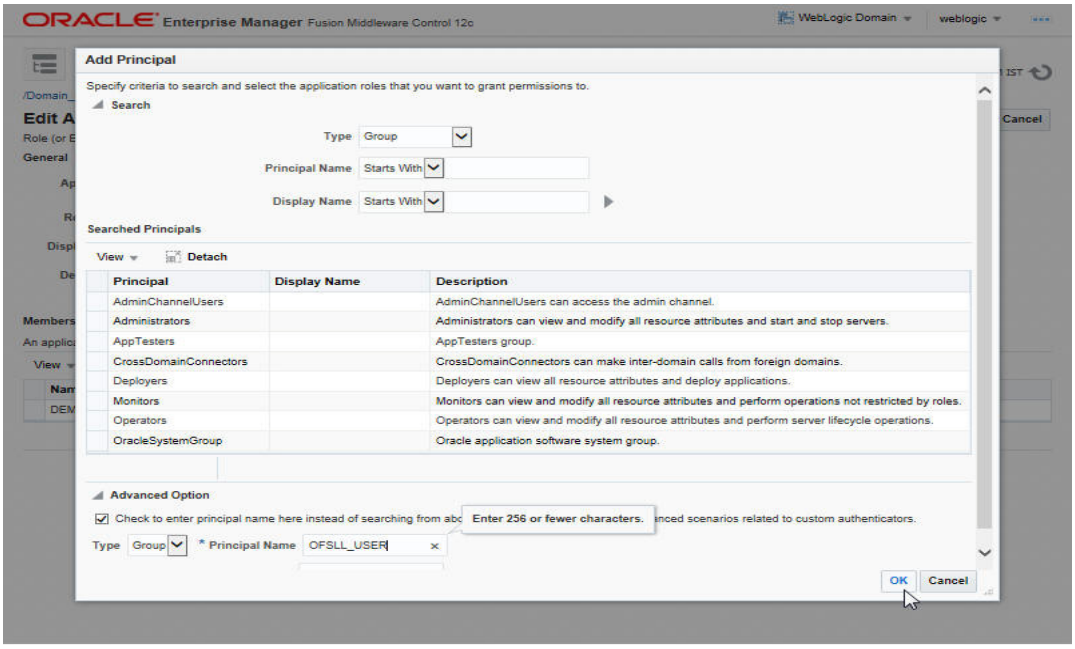


7. Click ‘Add”. Select type as Group. Click on the arrow head button.

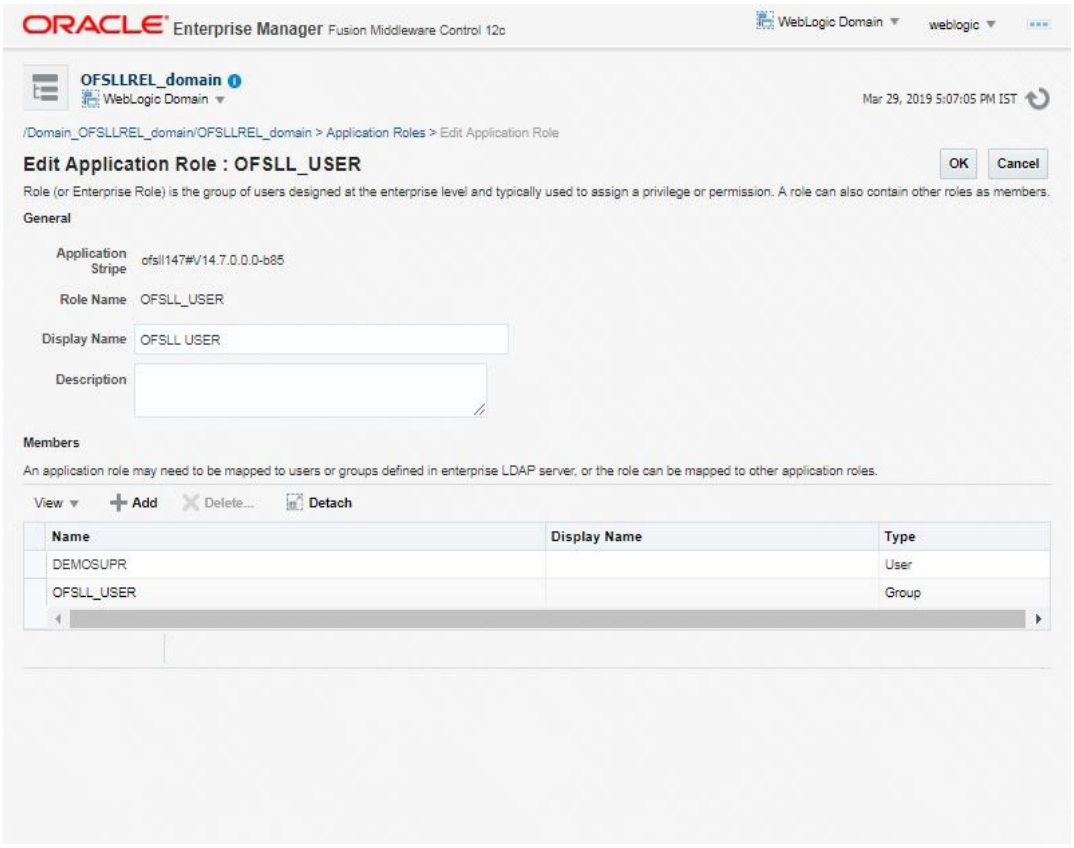
8. Follow the given steps to select the Principal ‘OFSLL_USER’ to add and click OK. The following window is displayed.



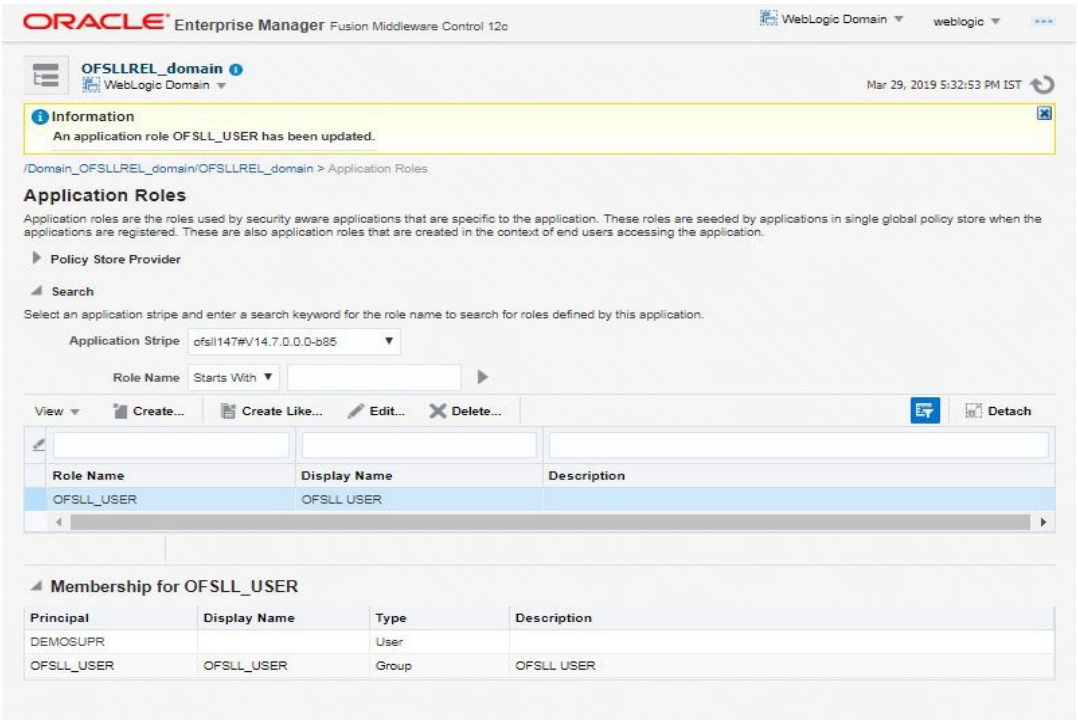
9. Check the check box in Advanced options. Enter the name of Group manually.



10. Click ‘OK’.

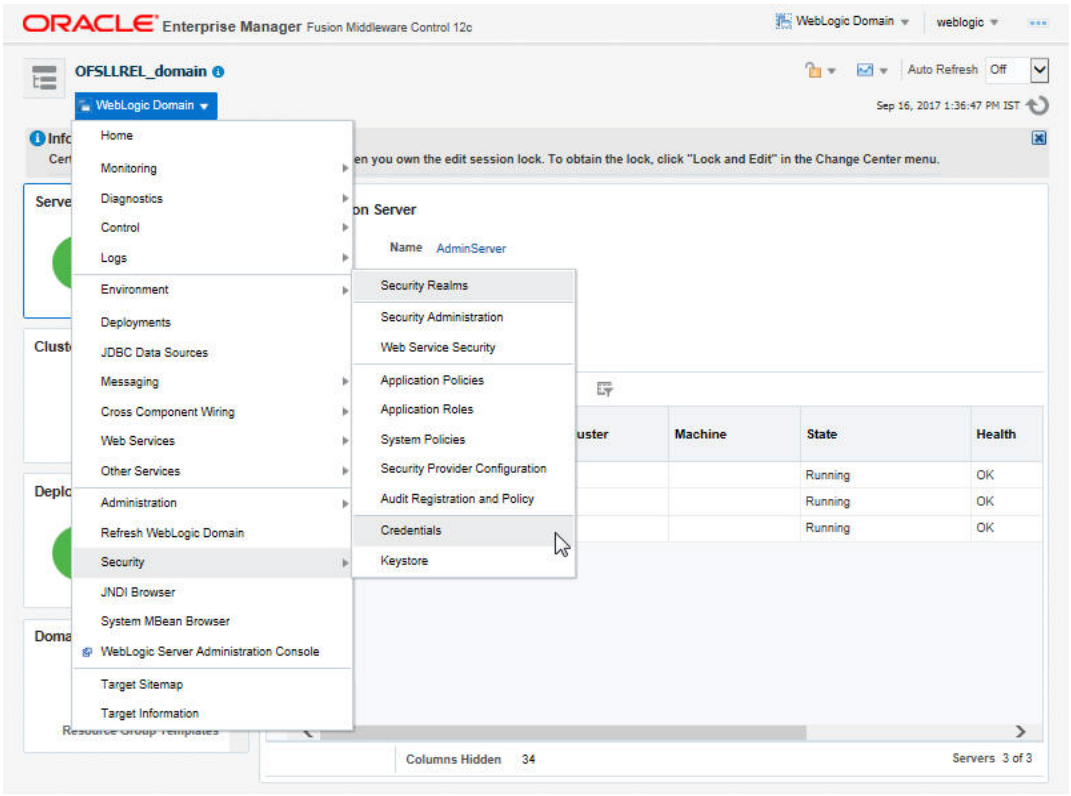


11. The following window is displayed with the confirmation message as ‘The Application role of 'group_name' has been updated’.

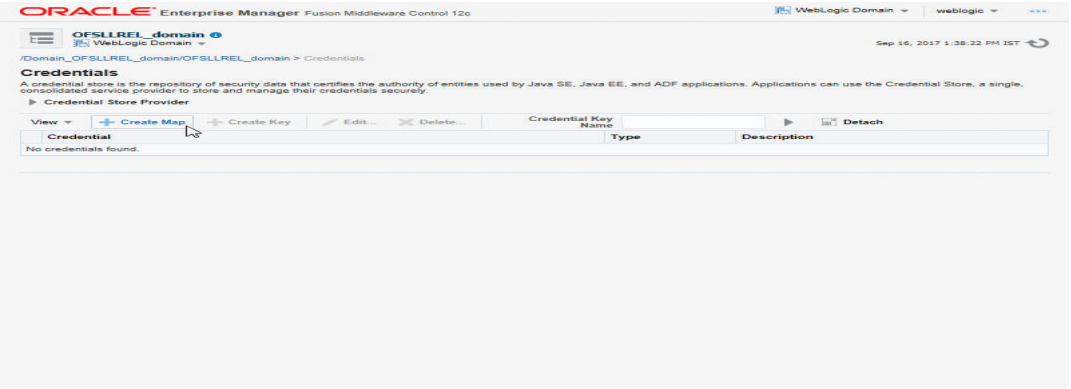


8. Configuring JNDI name for HTTP Listener

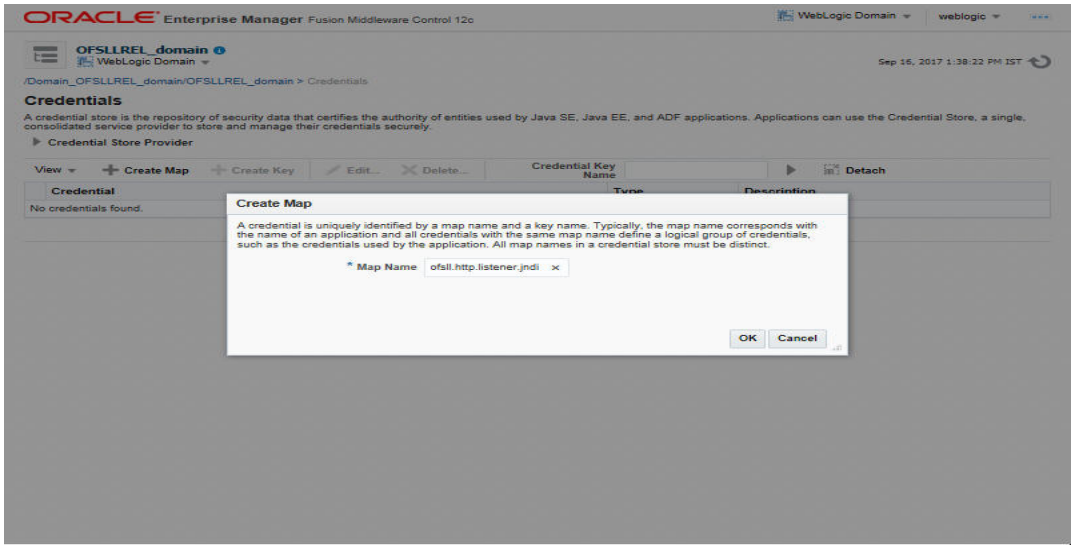
1. Click ‘WebLogic Domain’ on the right panel. Select Security > Credentials.



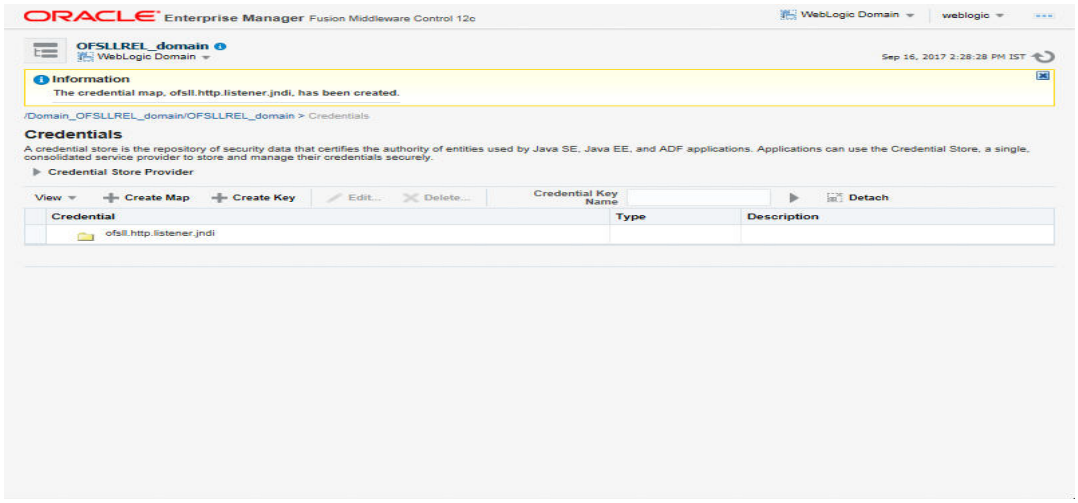
2. Click ‘Credentials’. The following window is displayed.



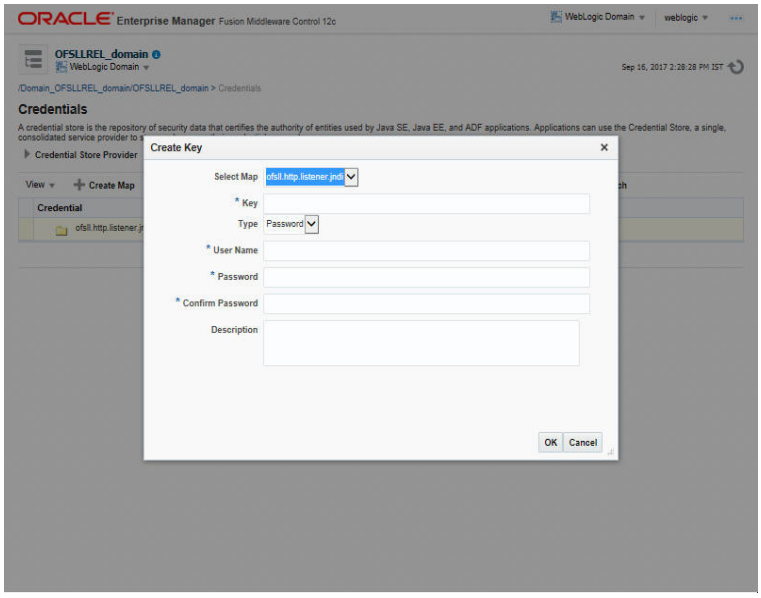
3. Click ‘Create Map’. The following window is displayed.



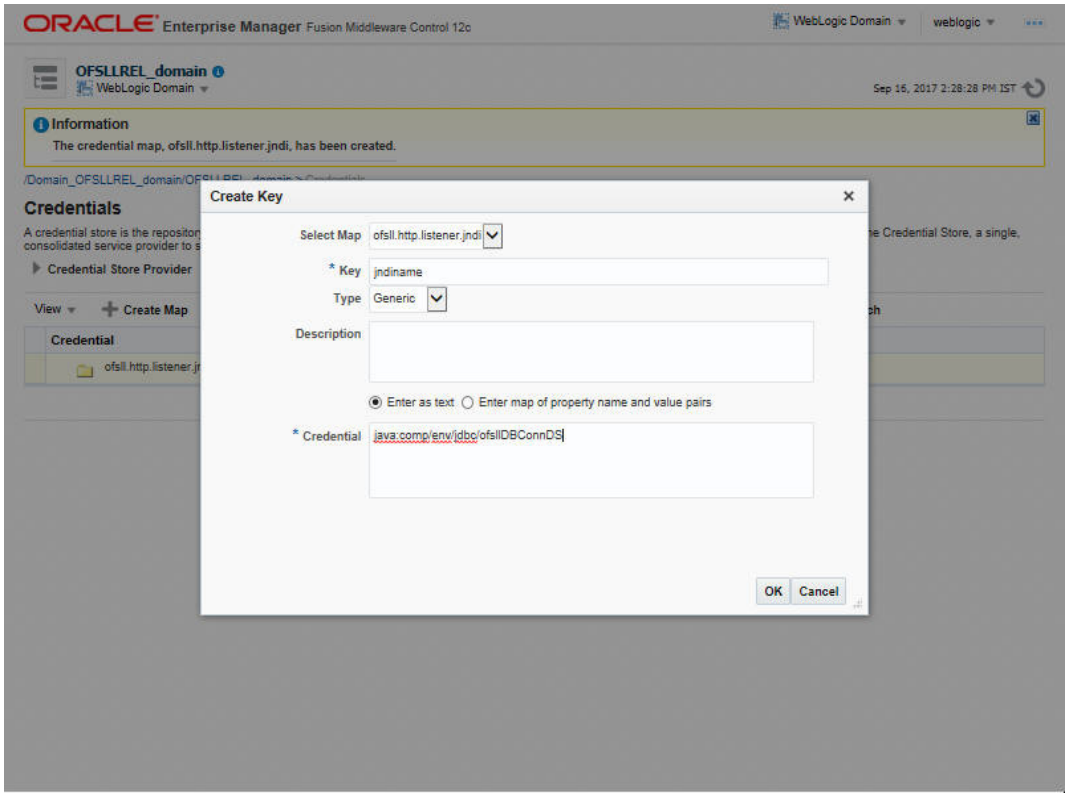
4. Enter Map name as 'ofsll.http.listener.jndi'.
5. Click ‘OK’. The following window is displayed.



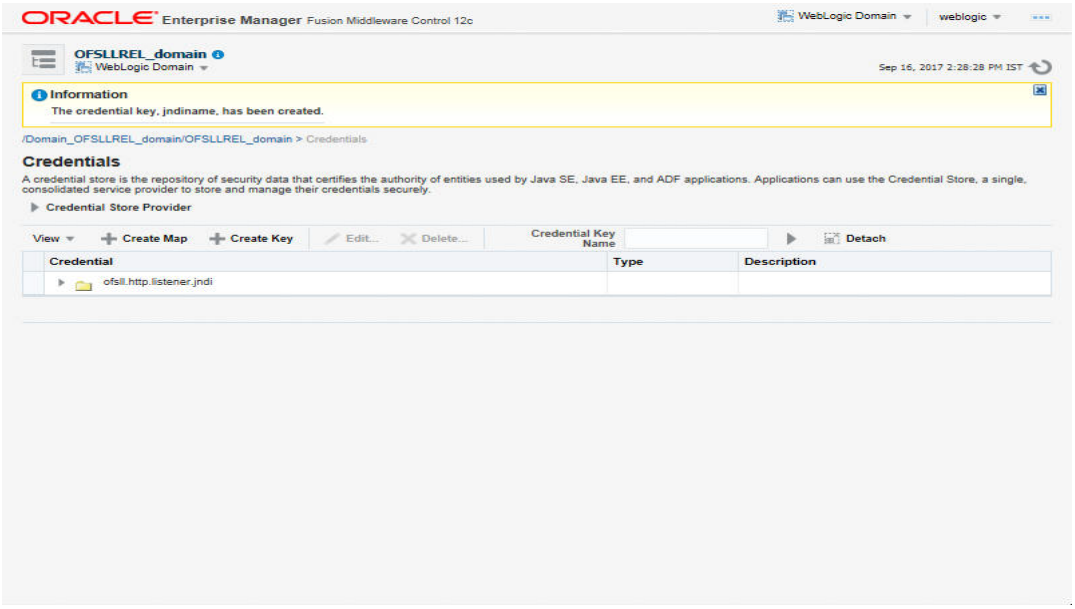
6. Click ‘Create Key’ Button. The following window is displayed.



7. Enter the followng details as per your requirement.
   - Key: jndiname
   - Credential: java:comp/env/jdbc/ofsllDBConnDS
   - Type:Generic



8. Click ‘OK’. The following window is displayed.



9. Configure AQ-JMS Bridge

The following steps are to be performed to configure the AQ-JMS Bridge through the Weblogic Console:

- Create Data Sources for AQ-JMS Bridge
- Configure MDB Flow
- AQ-JMS Topic Setup
- JMS Queue Configuration
- Configure External Client Certificates
- Create Credentials and System Policies
- Deploy MDB EJB

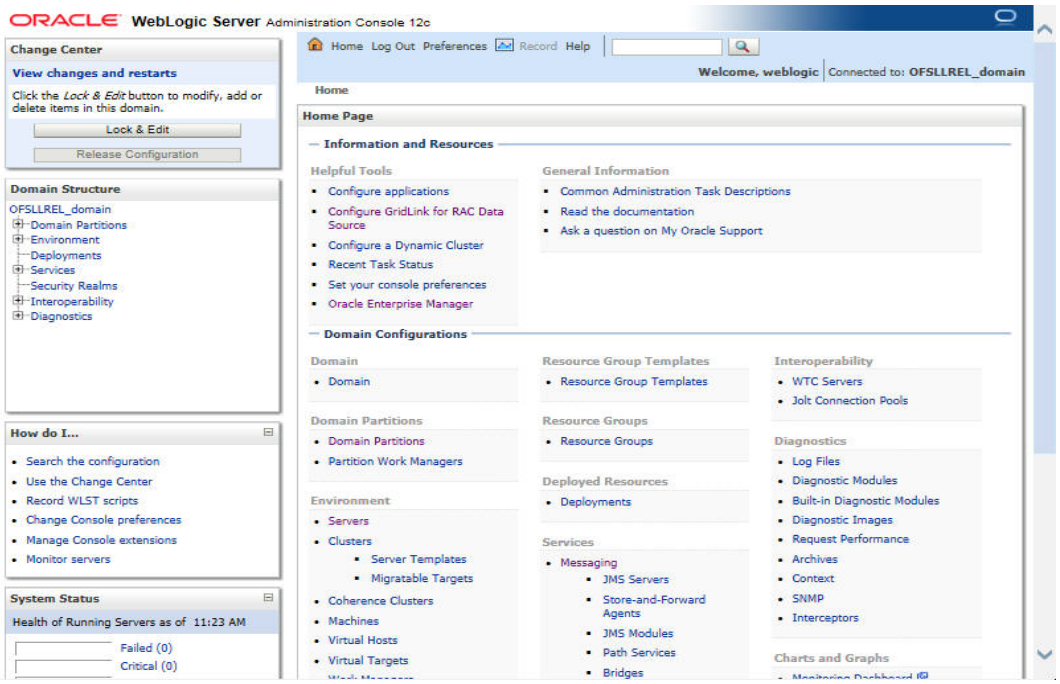
Note

Ensure that MDB EJB is not configured and deployed (i.e. OfsllAppQueue.ear deployment) on the same server on which the other WebServices are deployed.

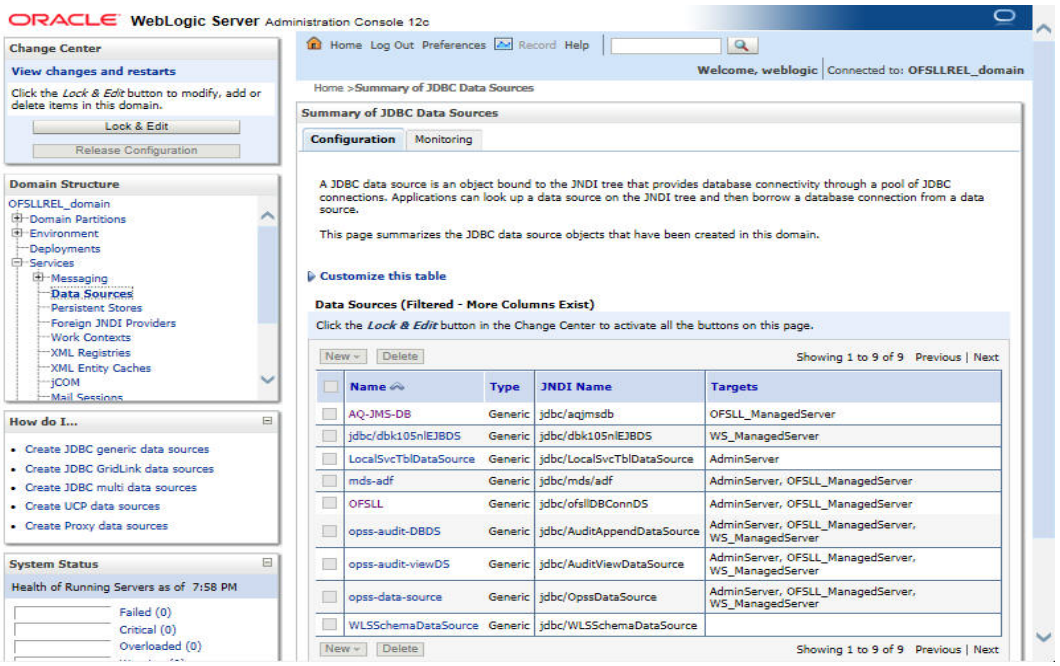
9.1 Create Data Sources for AQ-JMS Bridge

1. Login to Oracle Weblogic 12c console (http://hostname:port/console).

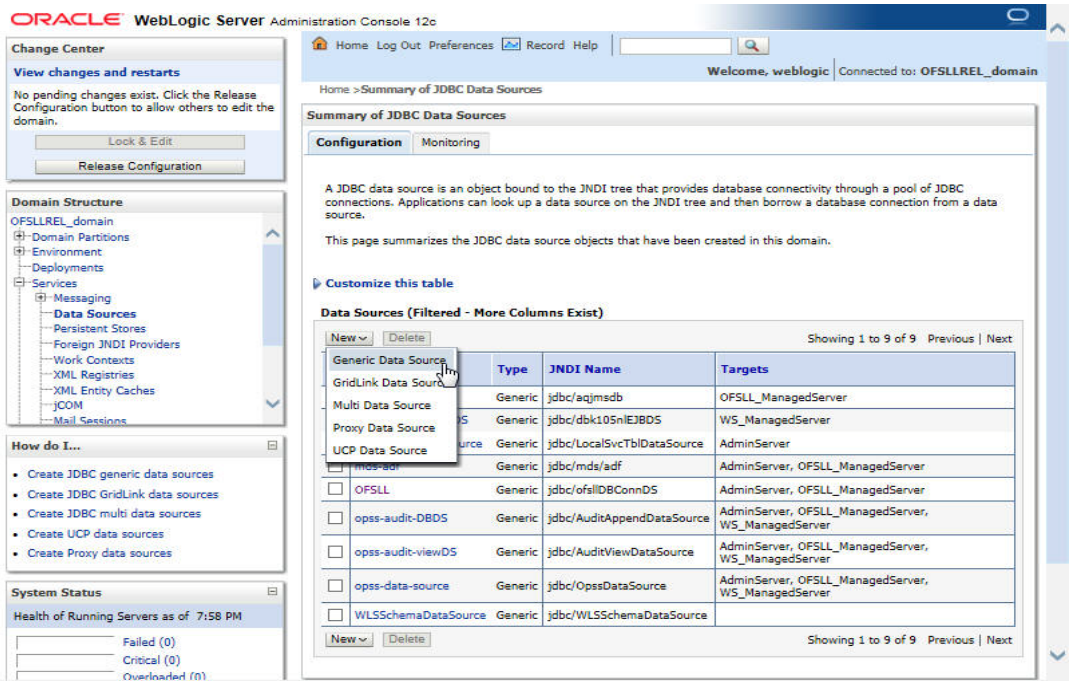
2. On successful login, the following window is displayed.



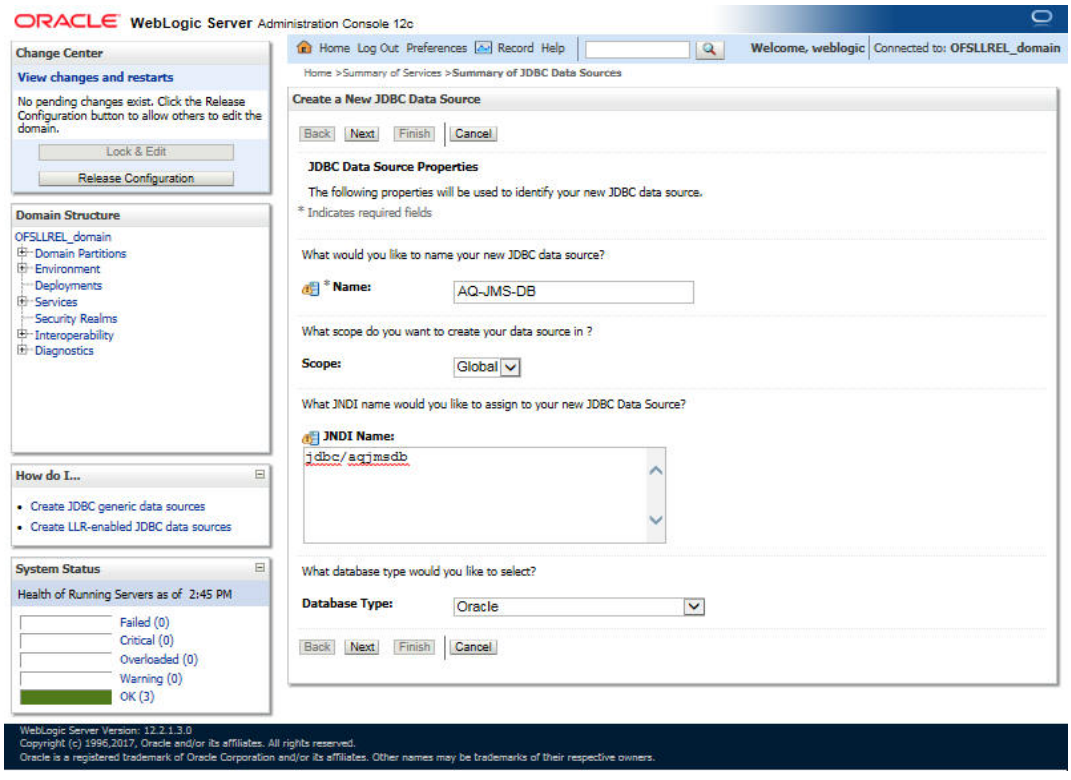
3. Click Domain Name > Services > Data Sources. The following window is displayed.



4. Click ‘Lock & Edit’ button on the left panel. Click ‘New’ on right panel and select ‘Generic Data Source’.



5. The following window is displayed.



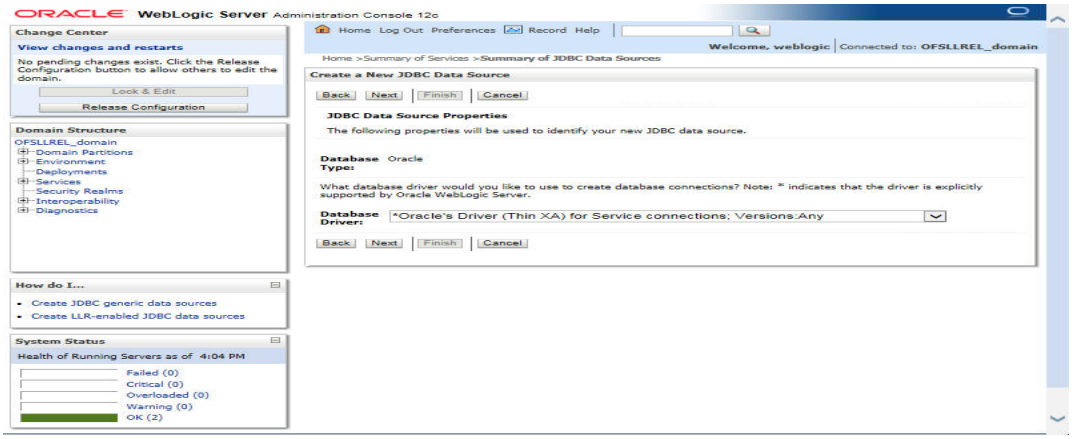
6. Specify the following details:
   - Enter Data source Name
   - Enter the JNDI Name as ‘jdbc/aqjmsdb’.

Note

If required, you may specify any other JNDI name, but ensure to use the same JNDI name during other configuration steps.

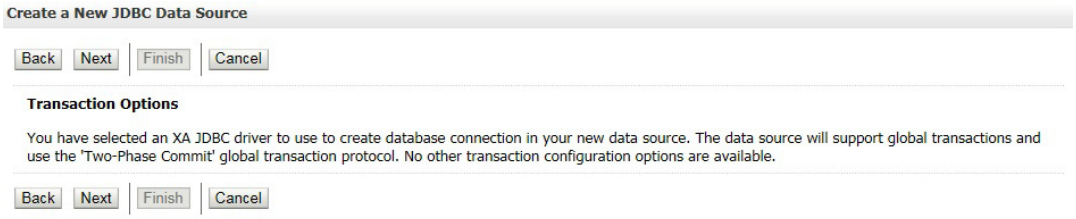
– Select ‘Oracle’ as Database Type.

7. Click ‘Next’. The following window is displayed.

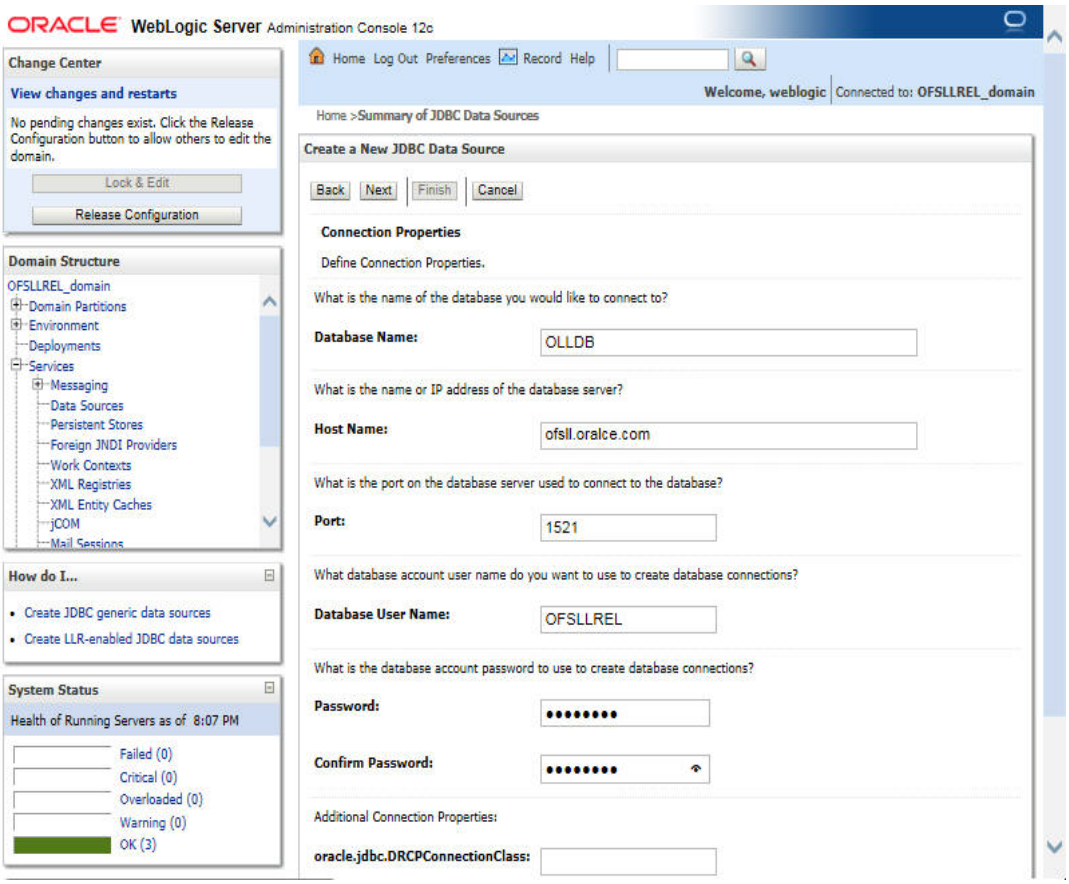


8. Select the Database Driver ‘Oracle's Driver(Thin XA) for Services connections;Versions:Any’.

9. Click ‘Next’. The following window is displayed.

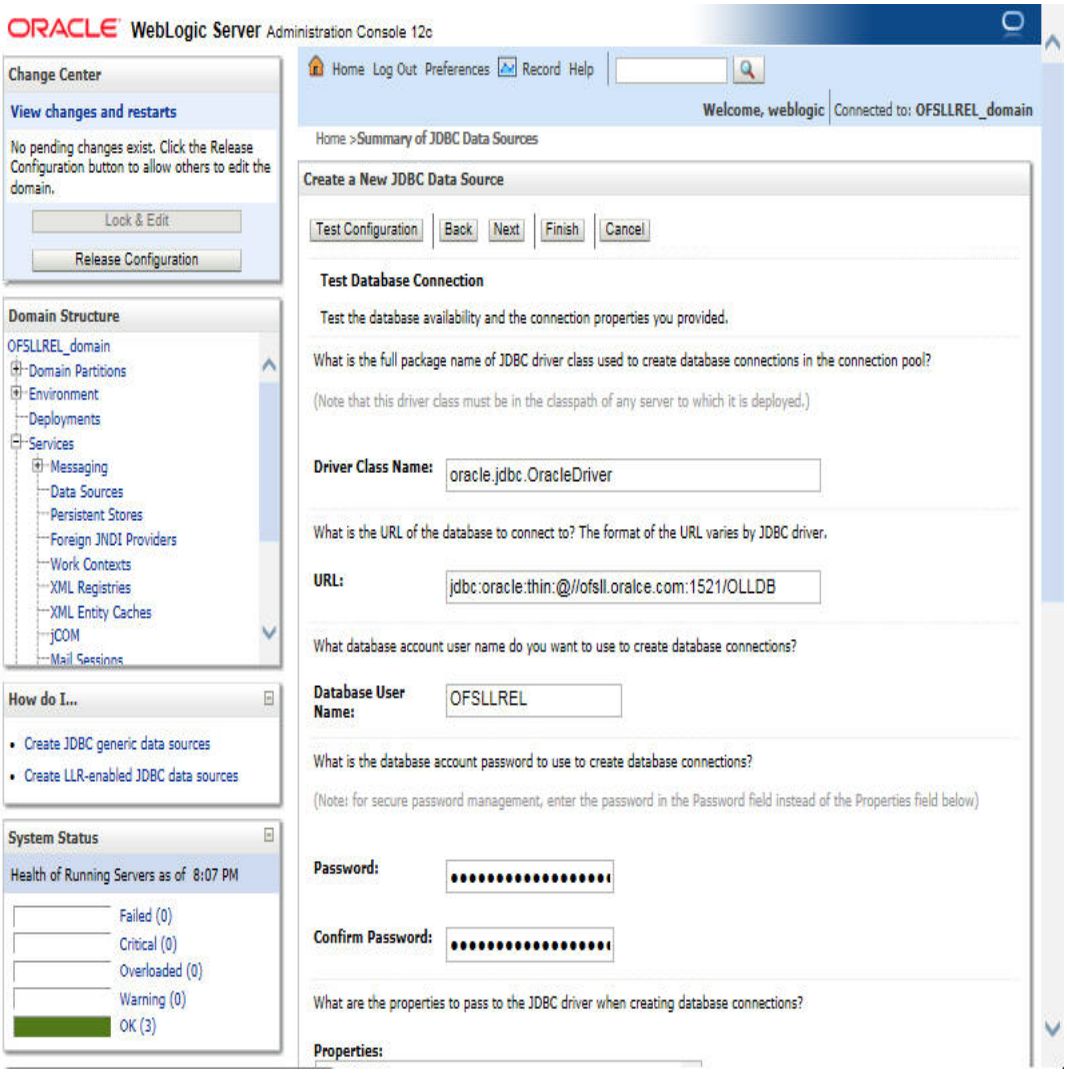


10. Click ‘Next’. The following window is displayed.

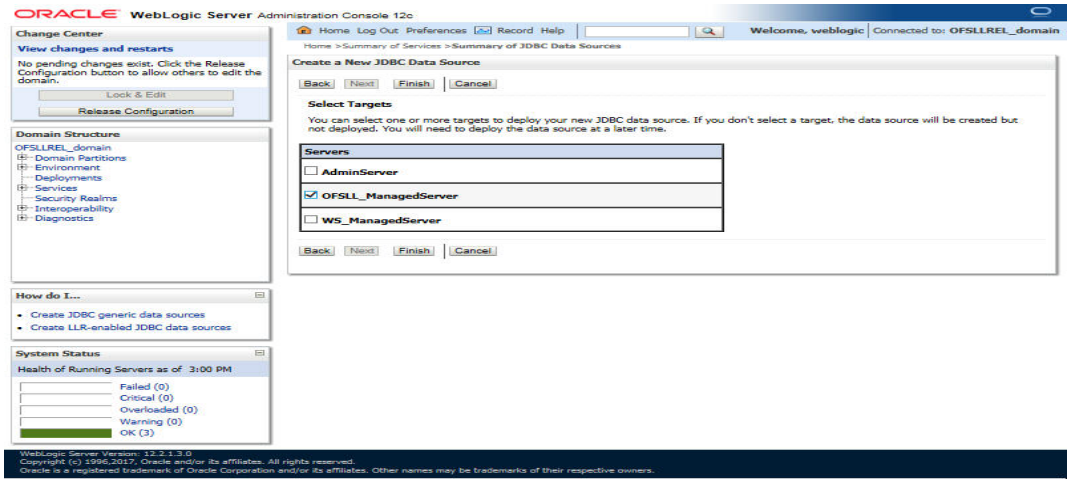


11. Enter the Database details.

12. Click ‘Next’. The following window is displayed.



13. Click ‘Test Configuration’. On completion, displays a confirmation message as ‘Connection test succeeded’.
14. Click ‘Next’. The following window is displayed.



15. Select target Server as ‘OFSLL_ManagedServer’.
16. Click ‘Finish’ to activate the changes.

Update the following parameters in JDBC data source connection pool:

1. Select Services > Data Sources > select the AQ_JMS_DB data source > Connection Pool.
2. Initial capacity and Maximum capacity is defaulted to 30, if the number of concurrent users are more this needs to be increased.
3. Click Advanced button and update the ‘Inactive Connection Timeout’ to 300 seconds.
4. Click 'Save' and restart the Data source.

Similarly create ‘QueueAppDS’ data sources which is used by MDB for all database related operations by following the steps mentioned in above section (Create Data Sources for AQ-JMS Bridge).

- Create data source name as QueueAppDS
- Update the JNDI as jdbc/QueueAppDS

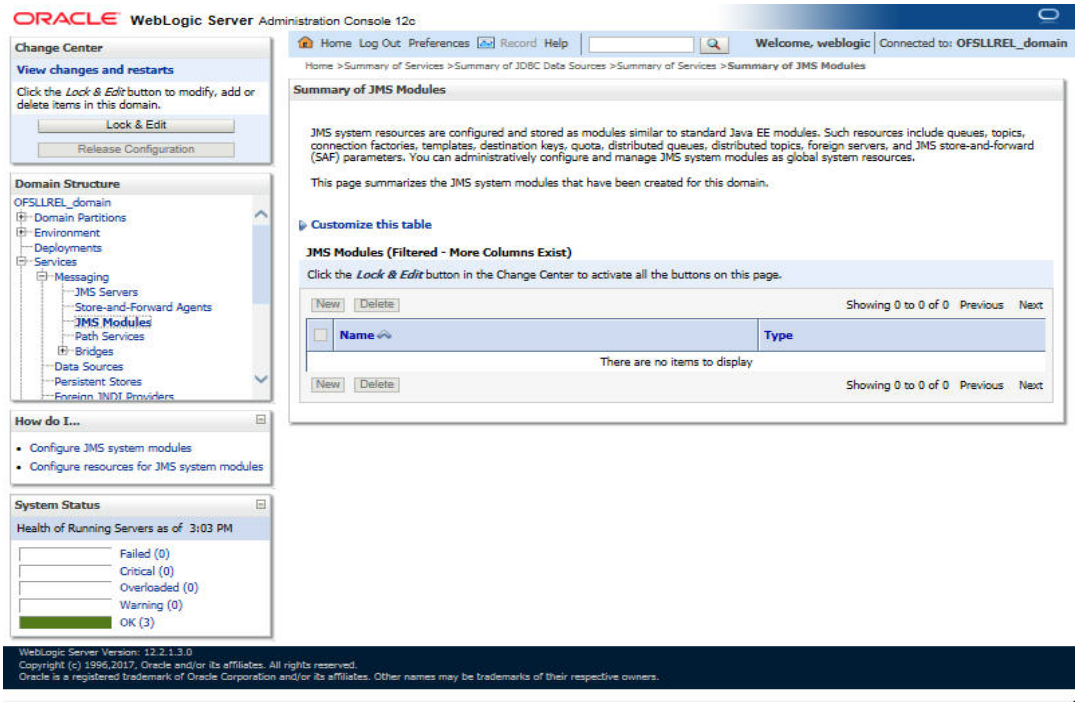
Do not perform the JDBC data source update and instead follow the below steps to configure the created ‘QueueAppDS’ data source:

- To Enable GRI (Generic Recovery Interface) CLOB logging from MDB to DB, click Advanced button and deselect the 'Wrap Data Types' check box.
- Set the ‘Inactive Connection Timeout’ to 300 seconds.

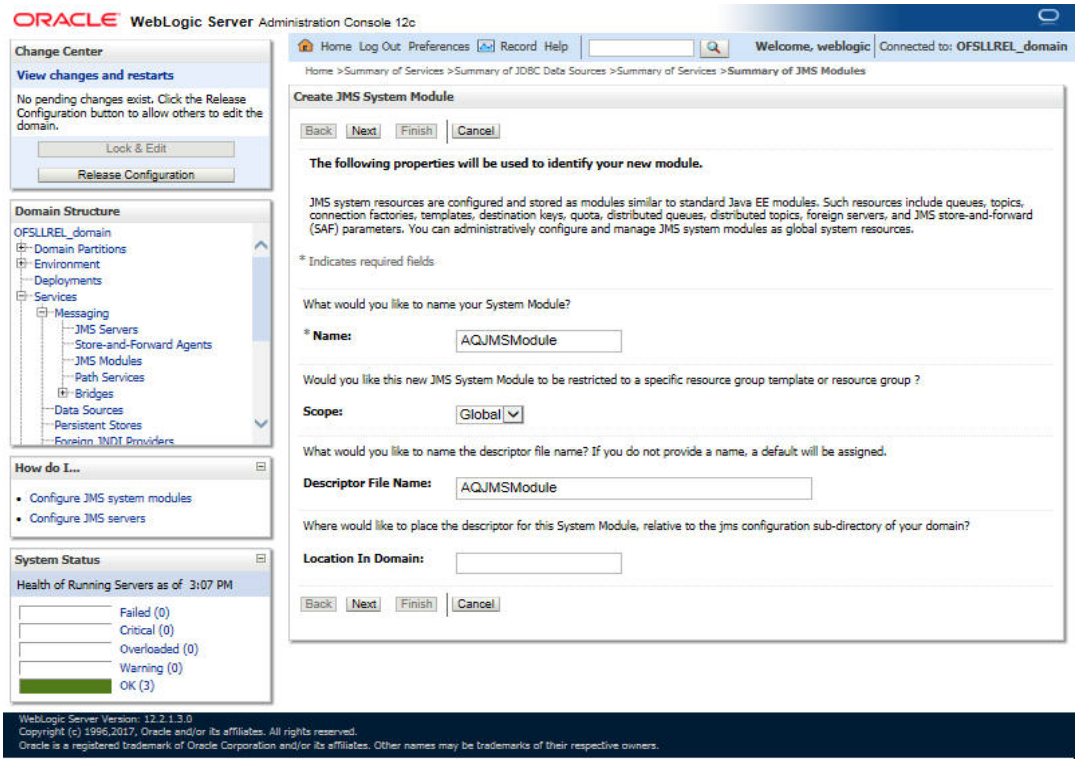
9.2 Configure MDB Flow

To configure the MDB Flow from Weblogic Console, do the following:

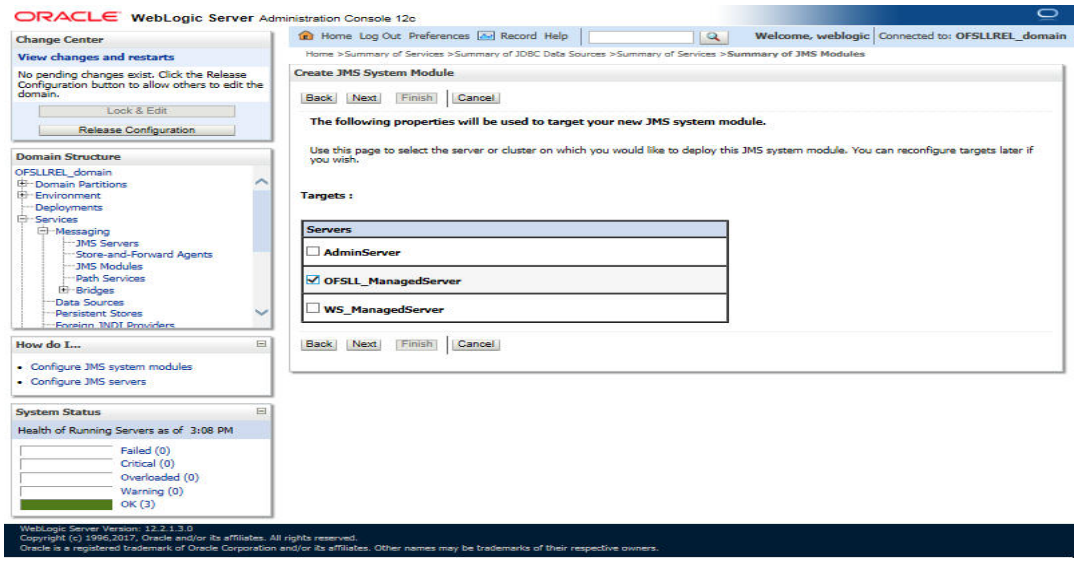
1. Login to Oracle Weblogic 12c console (http://hostname:port/console).
2. On the left pane, click 'Services'.
3. In Messaging tree click ‘JMS Modules’. The following window is displayed.



4. Click 'New'. The following screen is displayed.

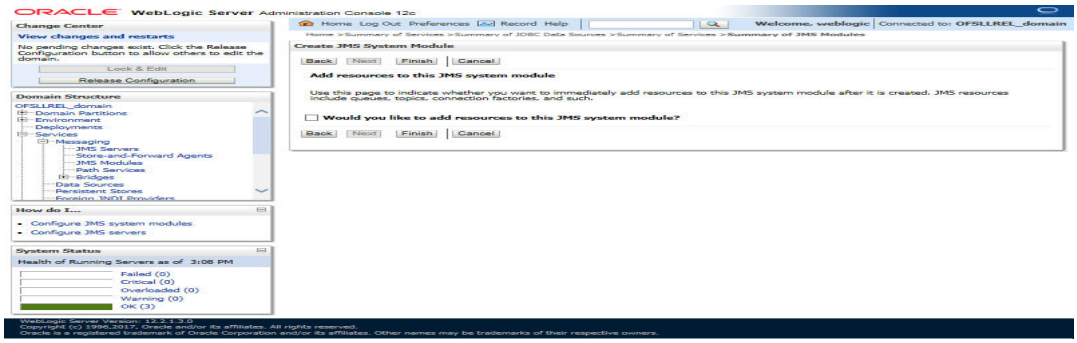


5. Specify the following details:
   - Name: AQJMSModule
   - Descriptor File Name: AQJMSModule
6. Click ‘Next’. The following window is displayed.

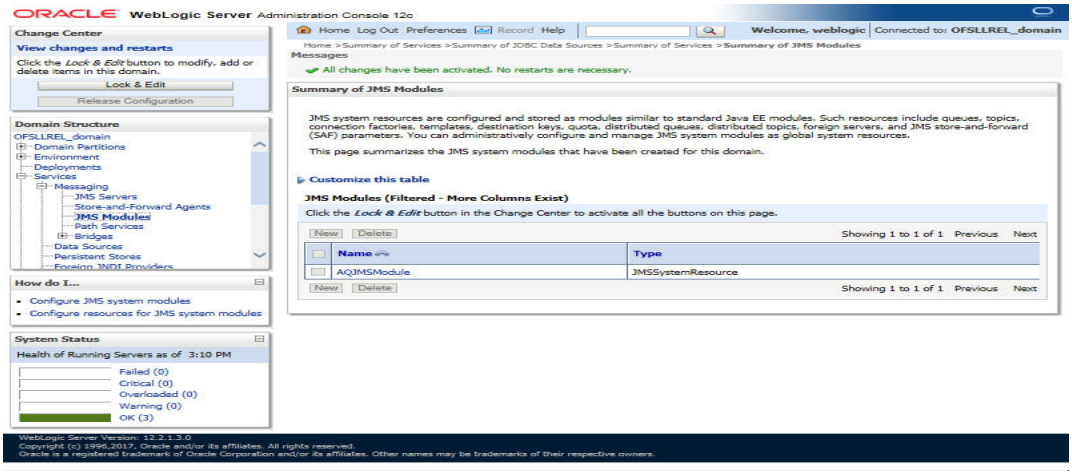


7. Select target servers as ‘OFSLL_ManagedServer’.

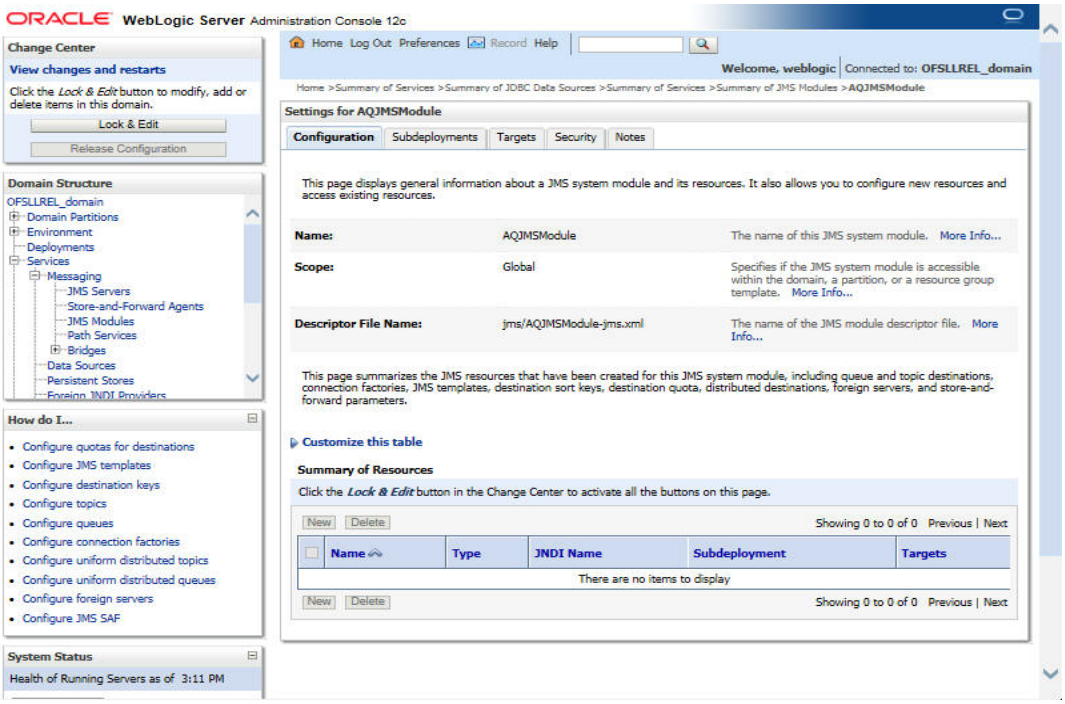
8. Click ‘Next’. The following window is displayed.



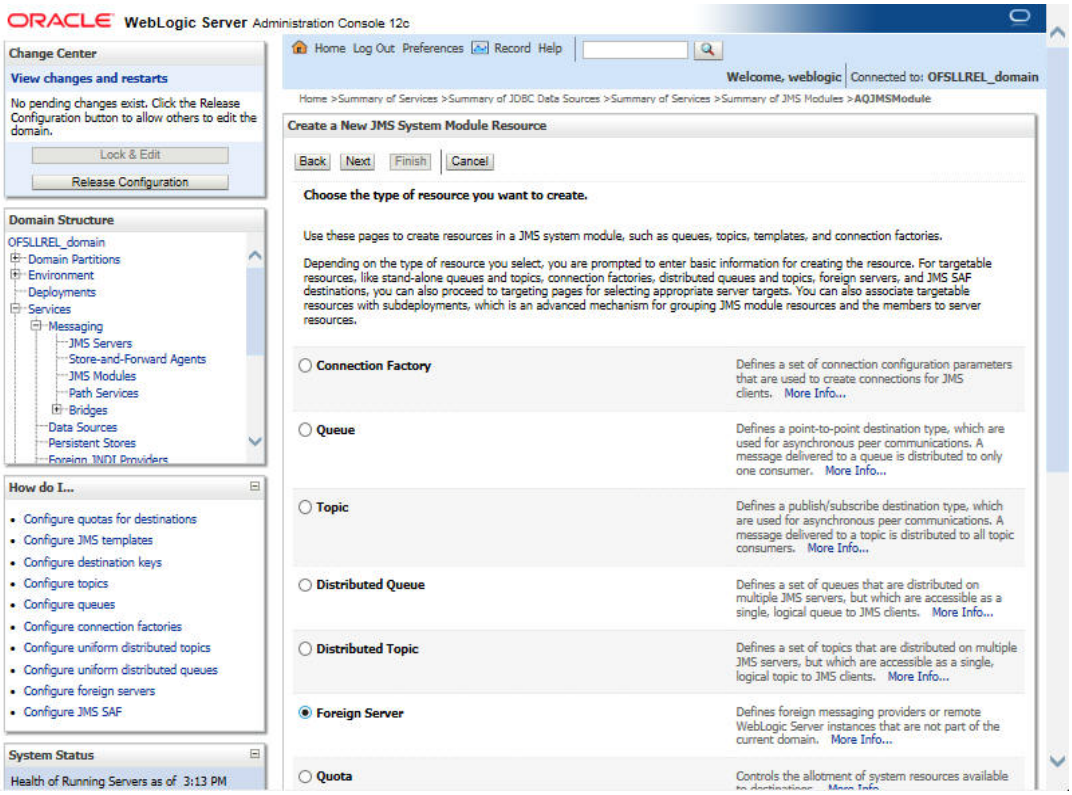
9. Click ‘Finish’ to activate the changes. The following window is displayed.



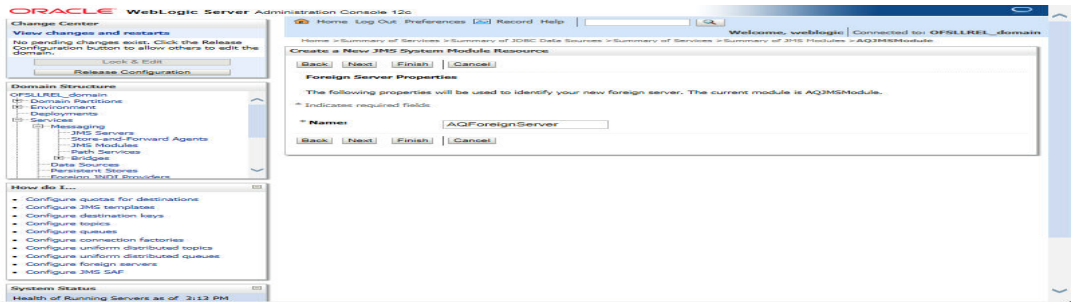
10. Click on the JMS Module that you created. The following window is displayed.



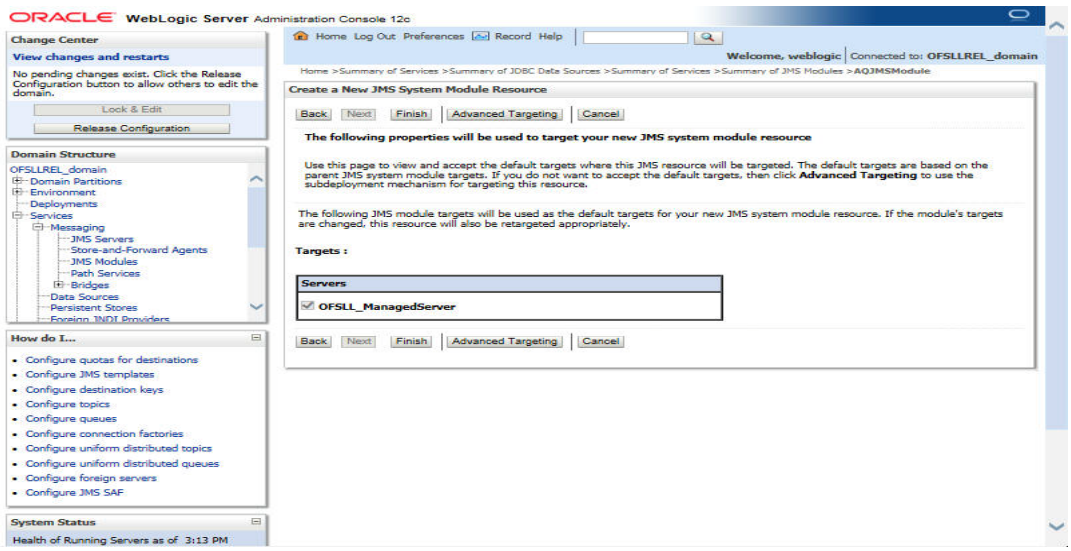
11. Click ‘New’ in ‘Summary of Resources’ section. The following window is displayed.



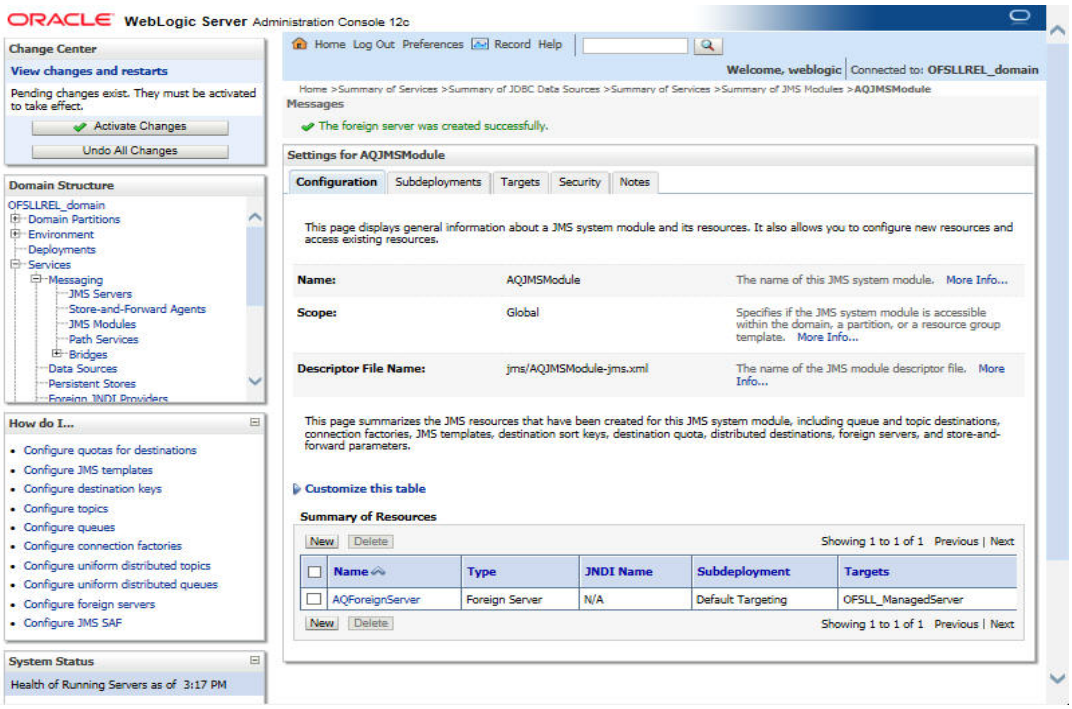
12. Select ‘Foreign Server’ as the option for type of resource to be created and click ‘Next’. The following window is displayed.



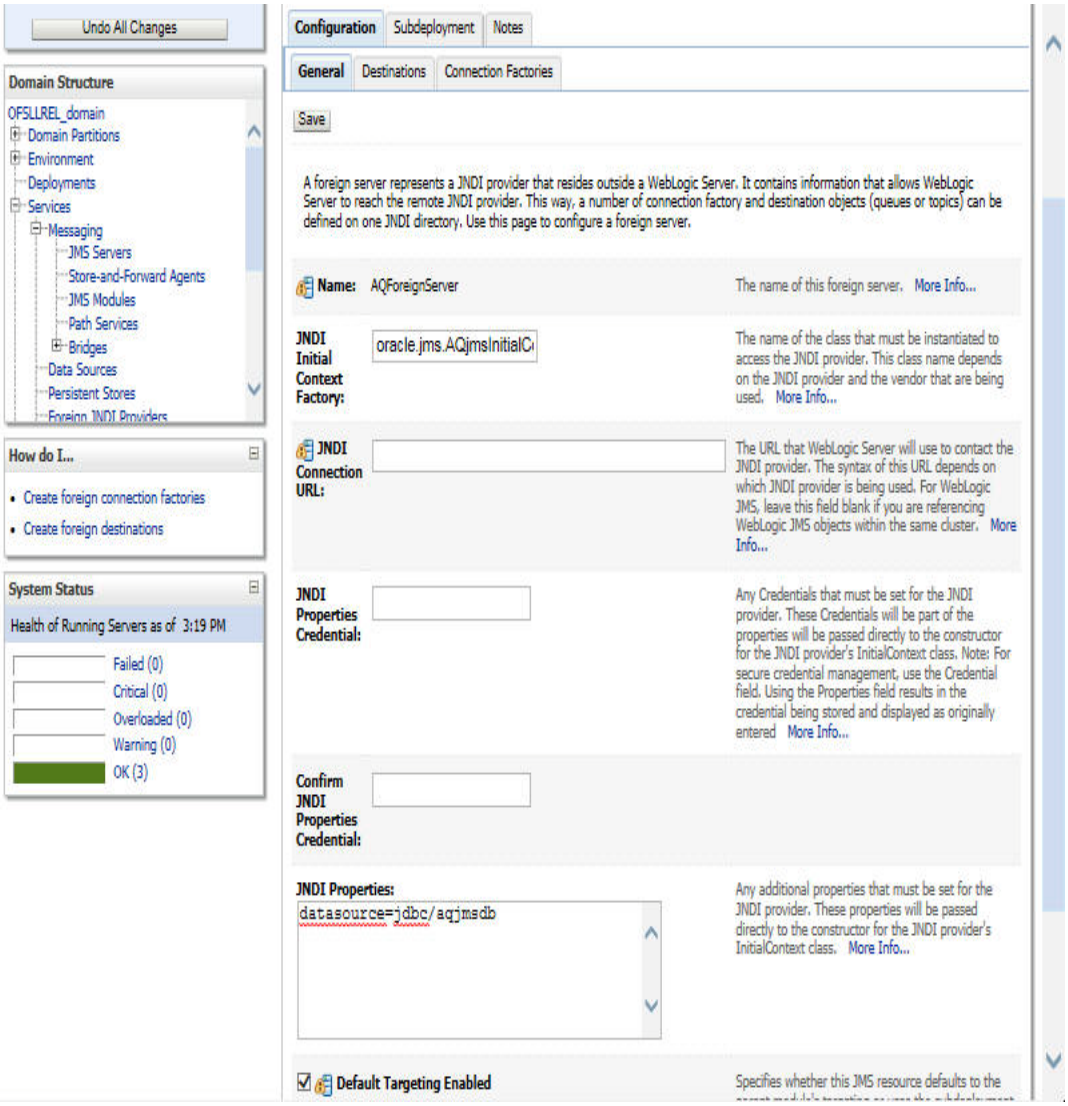
13. Specify the name of the Foreign Server as ‘AQForeignServer’ and click 'Next'. The following window is displayed.



14. Click ‘Finish’ and activate the changes. The following window is displayed.

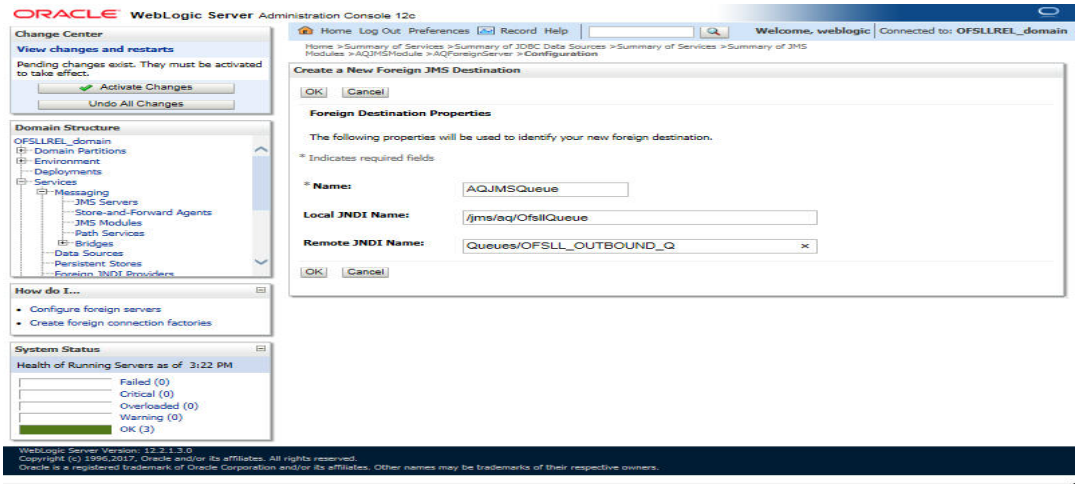


15. Click on the Foreign Server that you created. The following window is displayed.

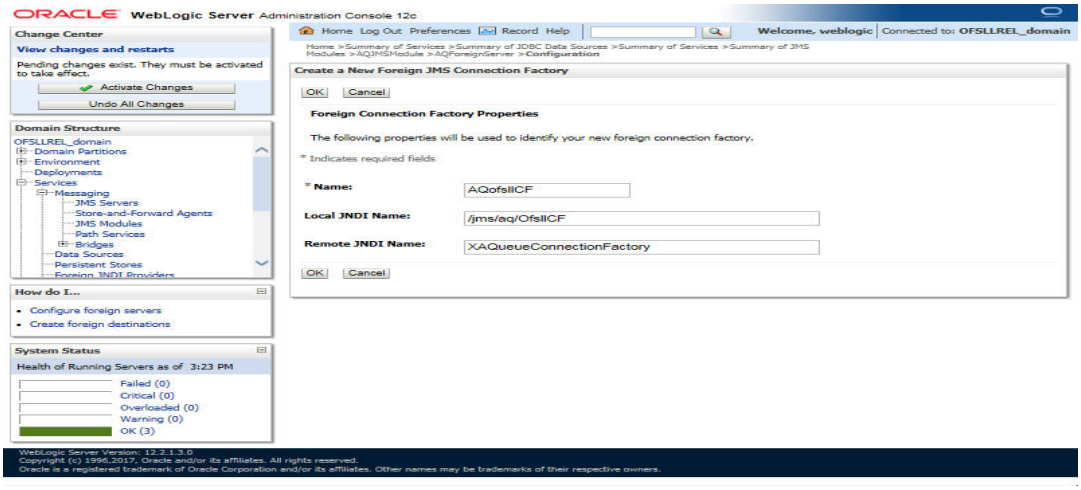


16. Specify the following details:
    - Enter JNDI Initial Context Factory as ‘oracle.jms.AQjmsInitialContextFactory’.
    - JNDI Properties as ‘datasource=jdbc/aqjmsdb’.
    - Ensure ‘Default Targetting Enabled’ option is selected.
17. Click ‘Save’.

18. Select ‘Destinations’ Tab and click ‘New’ to create new destination. The following window is displayed.



19. Specify the following details:
    - Name: AQJMSQueue
    - LocalJNDI Name: /jms/aq/OfsllQueue
    - Remote JNDI Name: Queues/OFSLL_OUTBOUND_Q
20. Click ‘OK’ and save the changes.
21. Select ‘Connection Factories’ Tab and click ‘New’ to add new connection factory. The following window is displayed.



22. Specify the following details:
    - Name: AQofsllCF
    - Local JNDI Name: /jms/aq/OfsllCF
    - Remote JNDI Name: XAQueueConnectionFactory
23. Click ‘OK’ and save the changes.

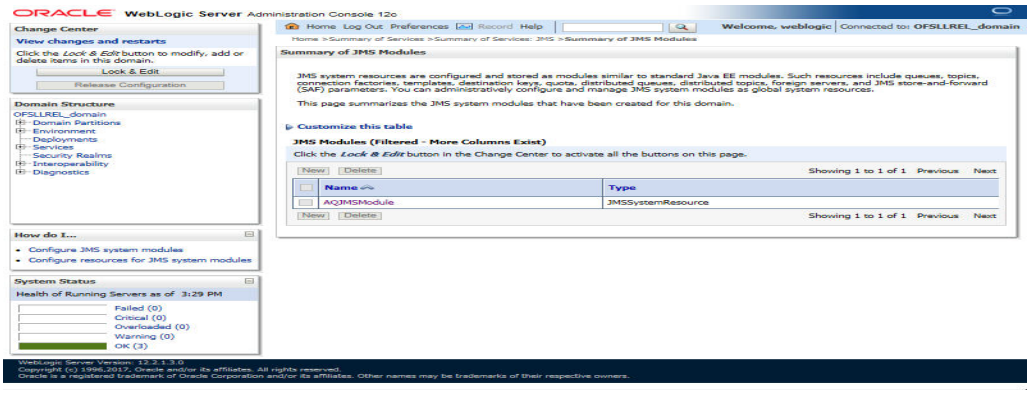
9.3 AQ-JMS Topic Setup

AQ-JMS Topic Bridge facilitates for group publishing to set of subscribed users. In a configured setup, a published message is sent to all the interested subscribers. Accordingly zero to many subscribers will receive a copy of the same message.

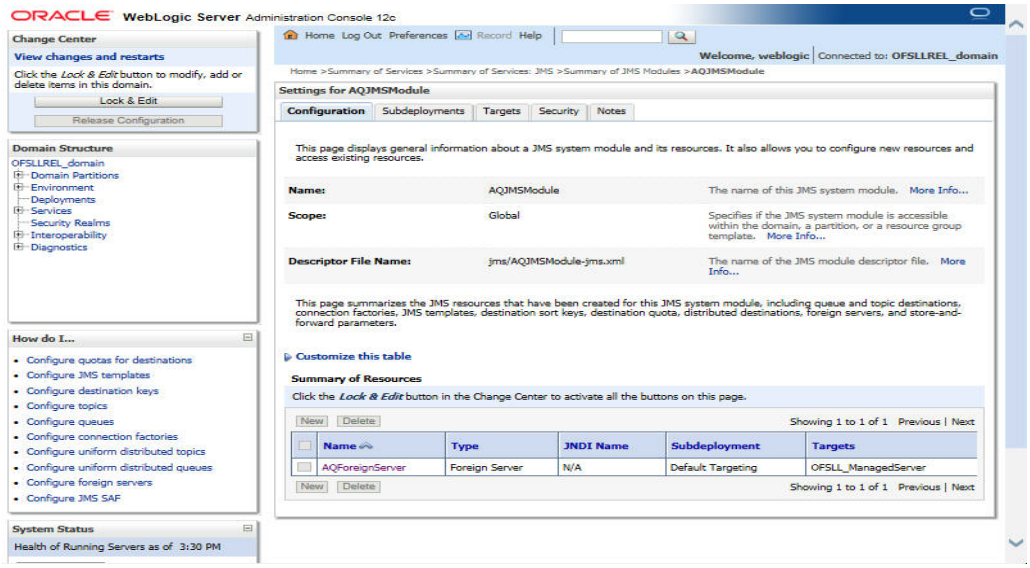
9.3.1 Create AQ-JMS Topic Bridge

To configure the AQ JMS Topic from Weblogic console, do the following:

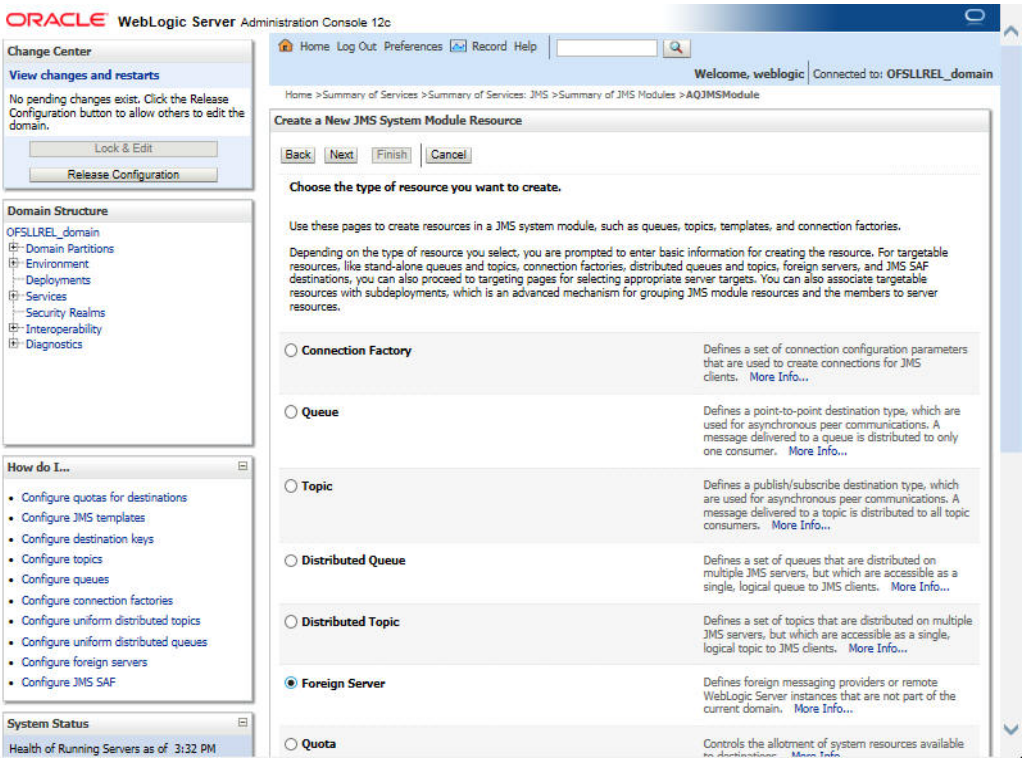
1. Login to Oracle Weblogic 12c console (http://hostname:port/console).
2. On the left pane, select Services > Messaging > JMS Modules. The following window is displayed.



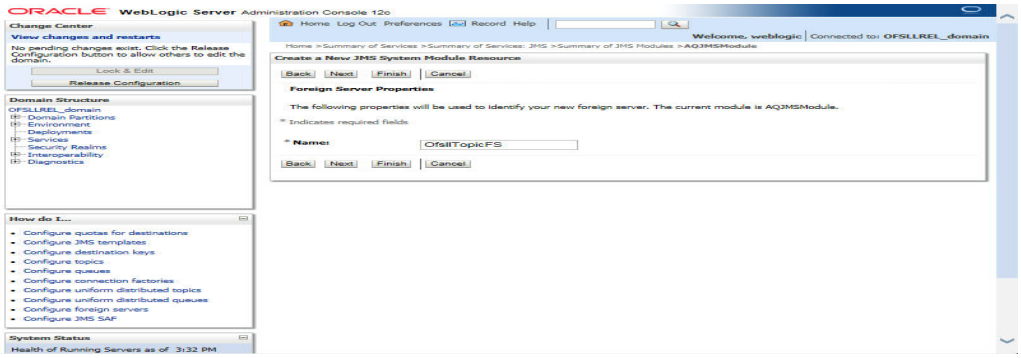
3. Click 'AQJMSModule'. The following window is displayed.



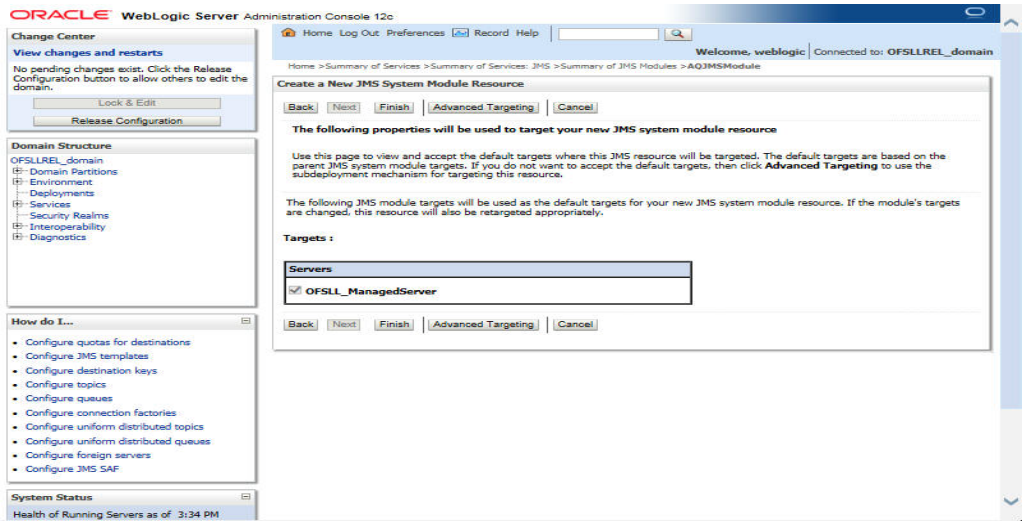
4. In the Summary of Resources section, click 'New'. The following window is displayed.



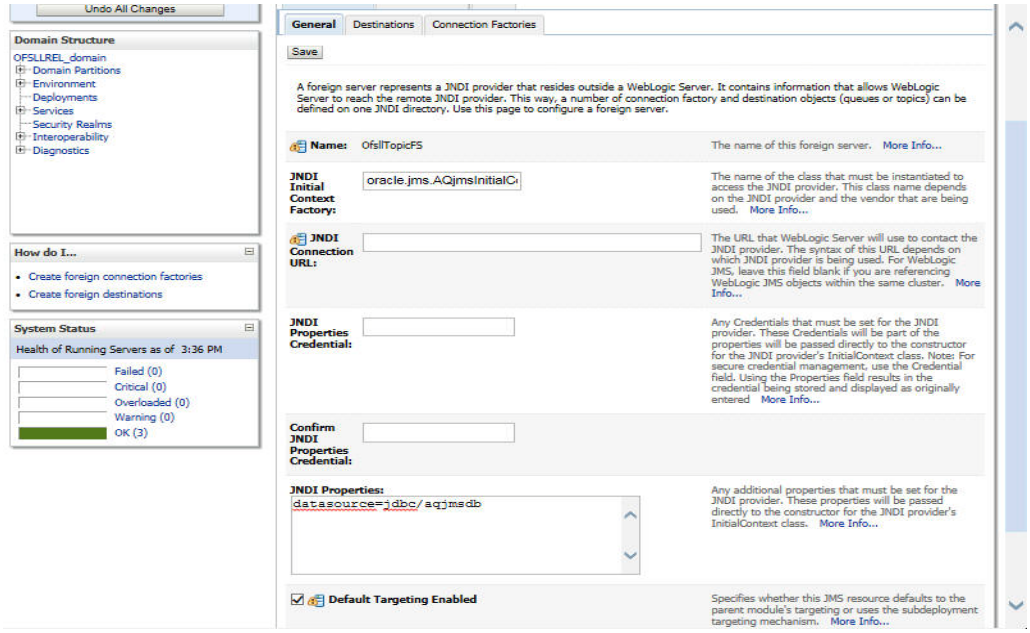
5. Select 'Foreign Server' as the option for type of resource to be created and click 'Next'. The following window is displayed.



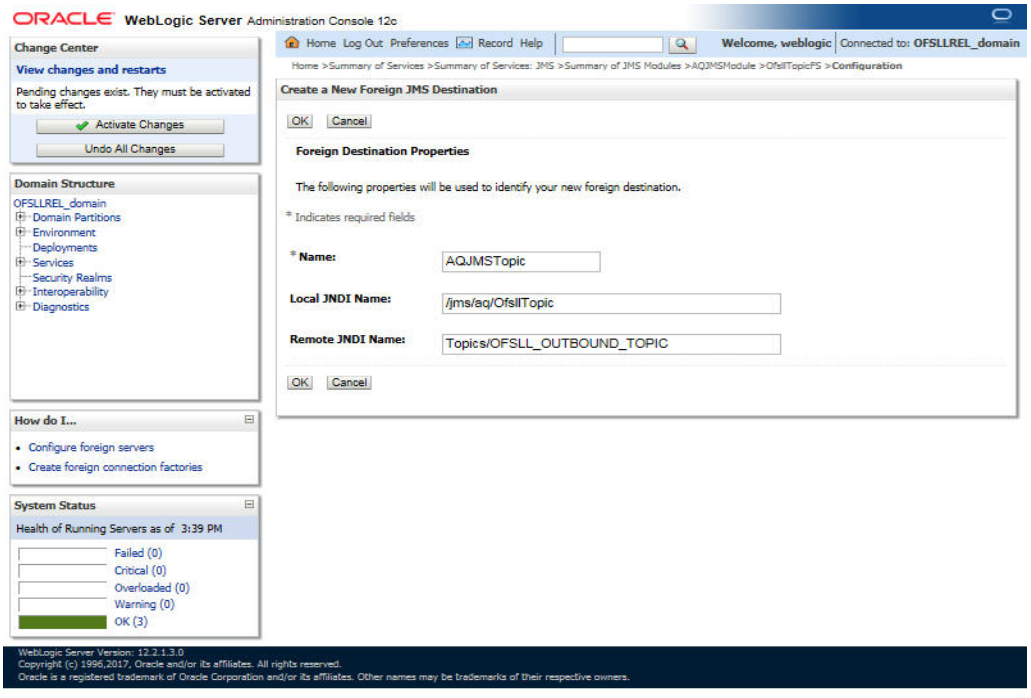
6. Specify the name of the Foreign Server as ‘OfsllTopicFS’ and click 'Next'. The following window is displayed.



7. Click 'Finish' and activate the changes.
8. Click on the Foreign Server that you created. The following window is displayed.

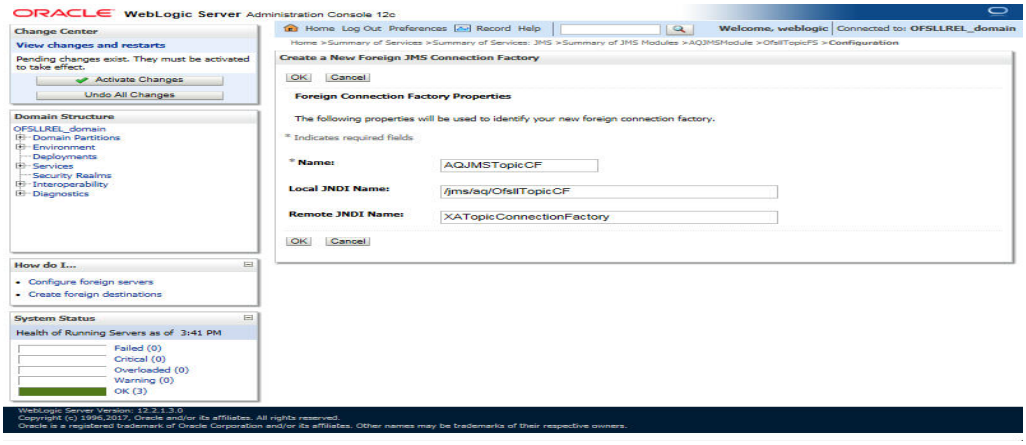


9. Specify the following details and click 'Save'.
   - Enter JNDI Initial Context Factory as 'oracle.jms.AQjmsInitialContextFactory'.
   - JNDI Properties as 'datasource=jdbc/aqjmsdb'.
   - Ensure 'Default Targetting Enabled' checkbox is selected.
10. Select 'Destinations' tab and click 'New' to create new destination. The following window is displayed.



11. Specify the following details and click 'OK' to save the changes.
    - Name: AQJMSTopic
    - LocalJNDI Name: /jms/aq/OfsllTopic
    - Remote JNDI Name: Topics/OFSLL_OUTBOUND_TOPIC

12. Select 'Connection Factories' tab and click 'New' to add new connection factory. The following window is displayed.



13. Specify the following details and Click 'OK' to save the changes.
    - Name: AQJMSTopicCF
    - Local JNDI Name: /jms/aq/OfsllTopicCF
    - Remote JNDI Name: XATopicConnectionFactory

9.4 JMS Queue Configuration

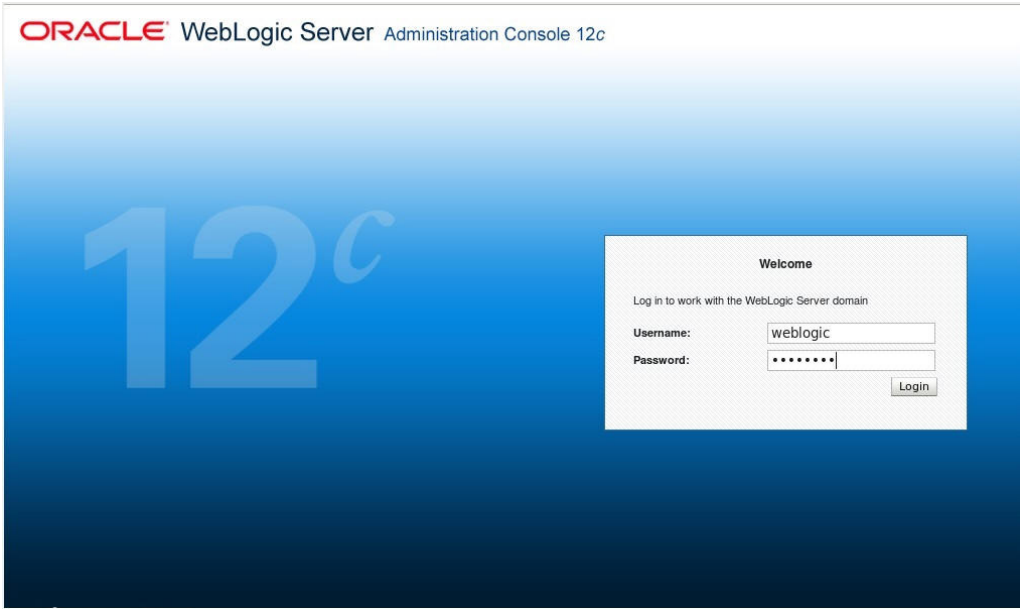
JMS queue is used to hold webservice invocation exception messages. It provides a mechanism for third parties to handle communication related failures.

Perform the following steps to configure JMS queue in application server.

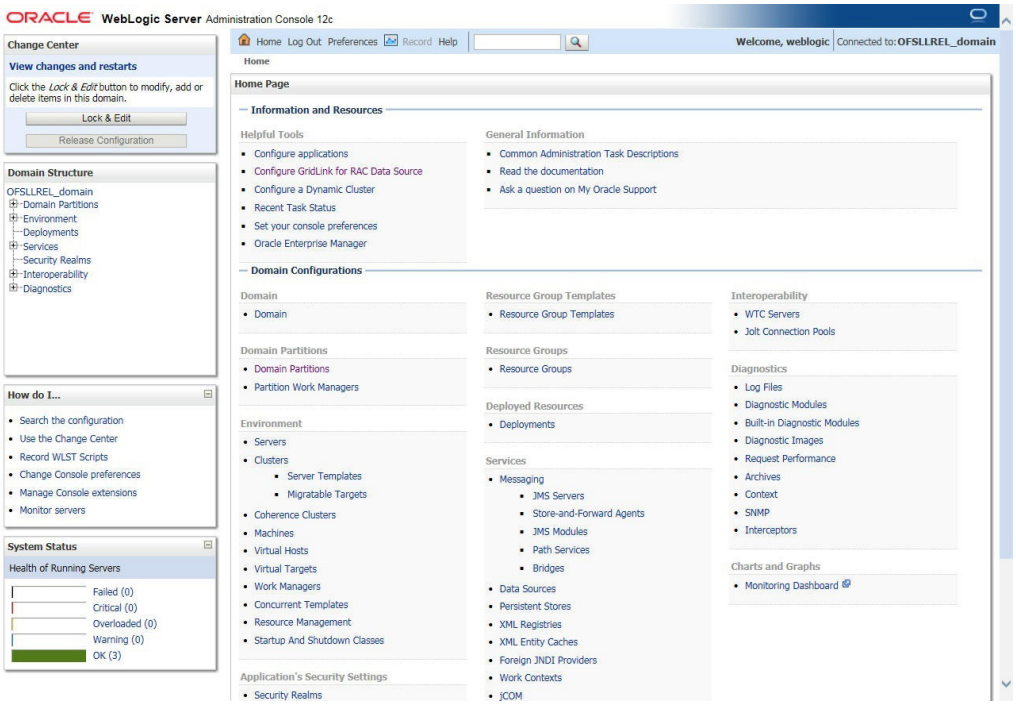
- Create JMS Server
- Create JMS Module
- Subdeployment
- Create JMS Connection Factory
- Create JMS Queue

9.4.1 Create JMS Server

1. Login to WebLogic Server 12c console (http://hostname:port/console). The following screen is displayed.

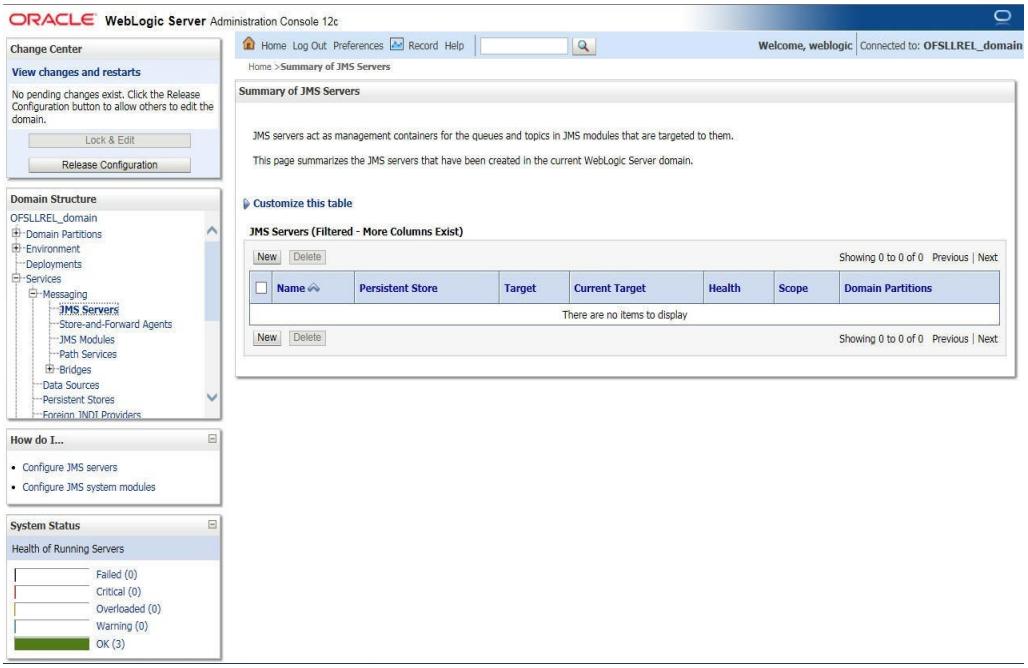


2. Specify the Weblogic administrator user name and password and click 'Log In'. The Oracle Weblogic home page is displayed.

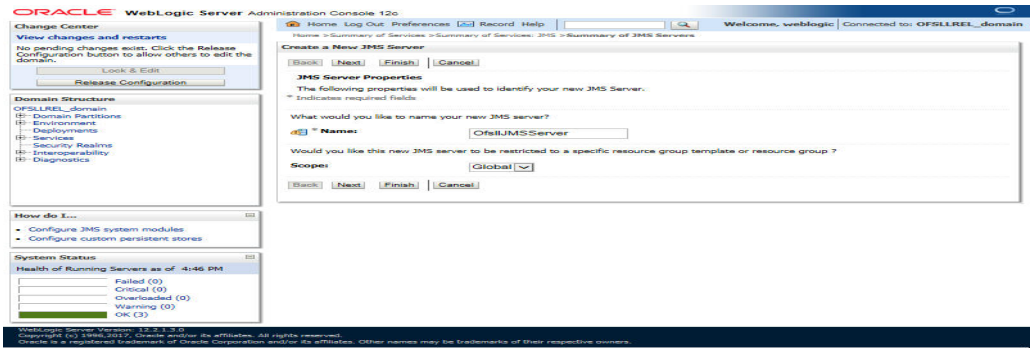


3. Click Domain Name > Services > Messaging > JMS Server.

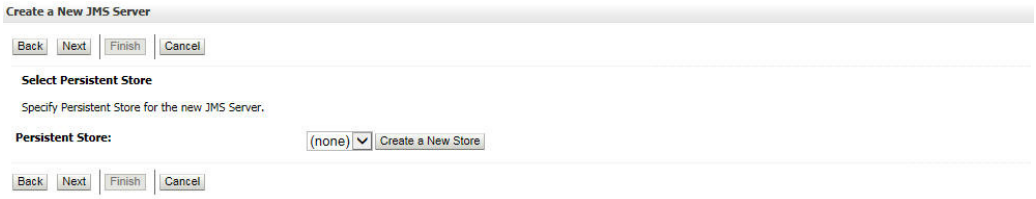
4. In the main window, click 'Lock & Edit'. The following window is displayed.



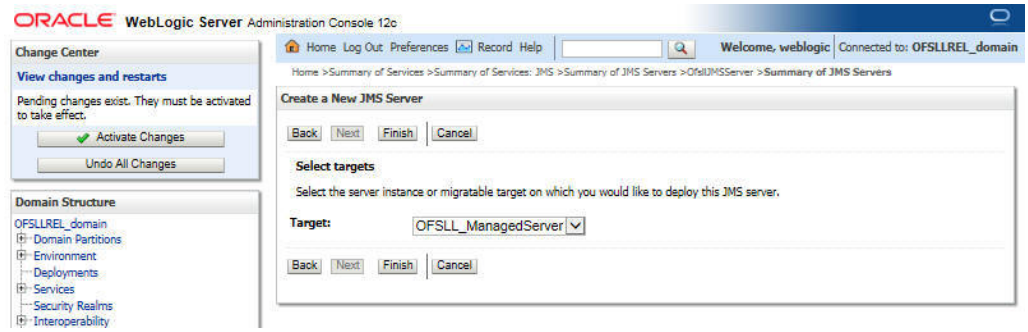
5. Click 'New'. The following window is displayed.



6. Specify the JMS Server Name as ‘OfsllJMSServer’. Click ‘Next’, the following window is displayed.

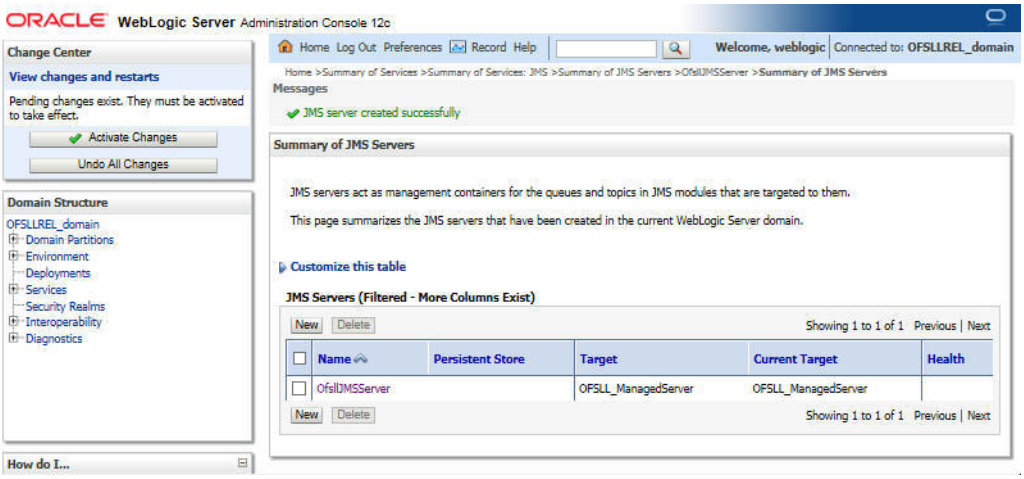


7. Select 'None' as the Persistent Store type. Click 'Next', the following window is displayed.



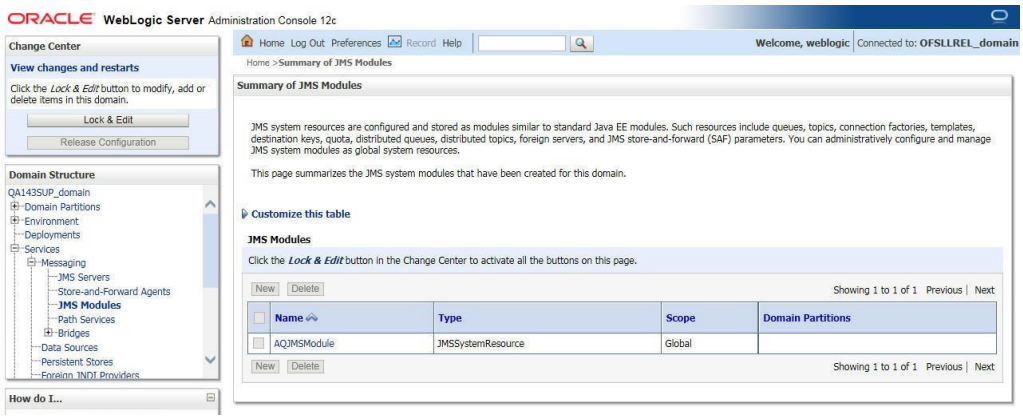
8. Select the target managed server and click 'Finish'.

9. Click 'Activate Changes' under Change Center. Once done, the following window is displayed:

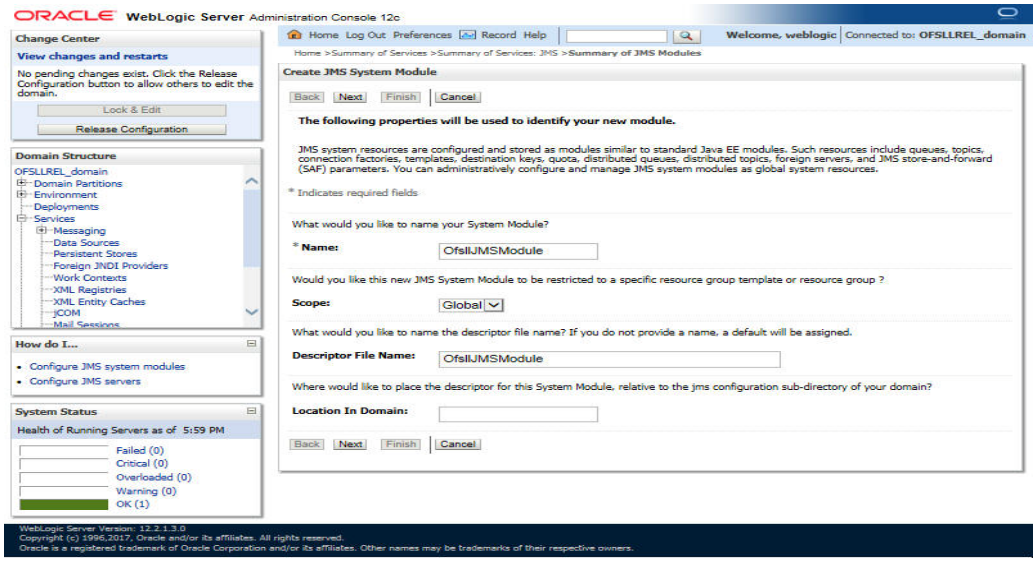


9.4.2 Create JMS Module

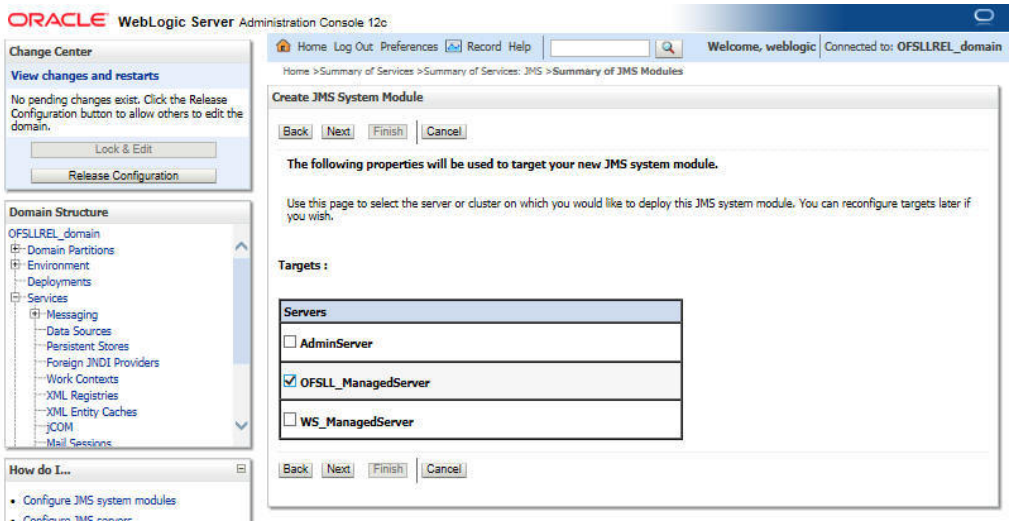
1. Login to WebLogic Server 12c console (http://hostname:port/console) by specifying the Weblogic administrator user name and password.
2. Click Domain Name > Services > Messaging > JMS Modules. The following window is displayed.



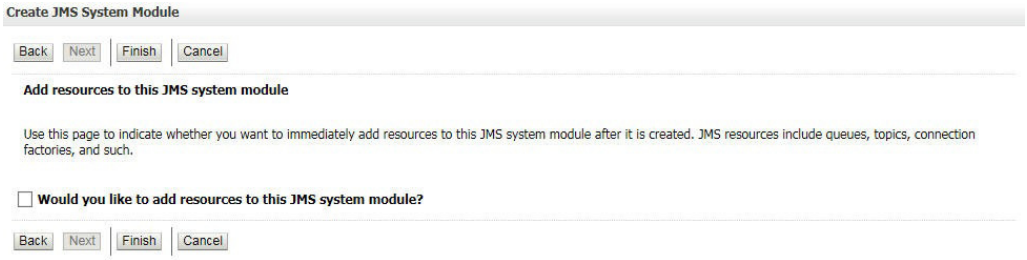
3. Click 'New'. The following screen is displayed.



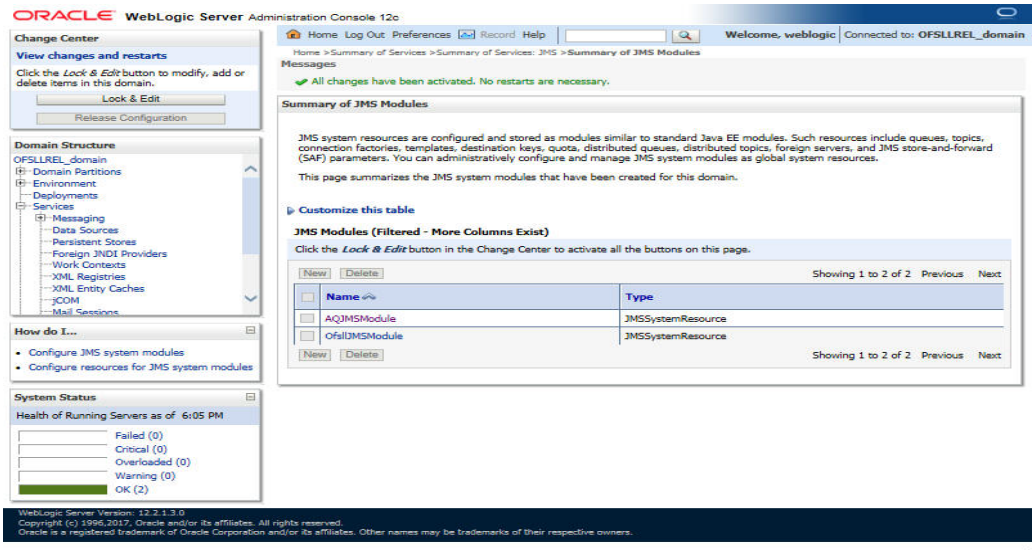
4. Specify the following details:
   - Enter the System Module Name as ‘OfsllJMSModule’
   - Enter the Description File Name as ‘OfsllJMSModule’
5. Click ‘Next’. The following screen is displayed.



6. Select the target server and click 'Next'. The following window is displayed.



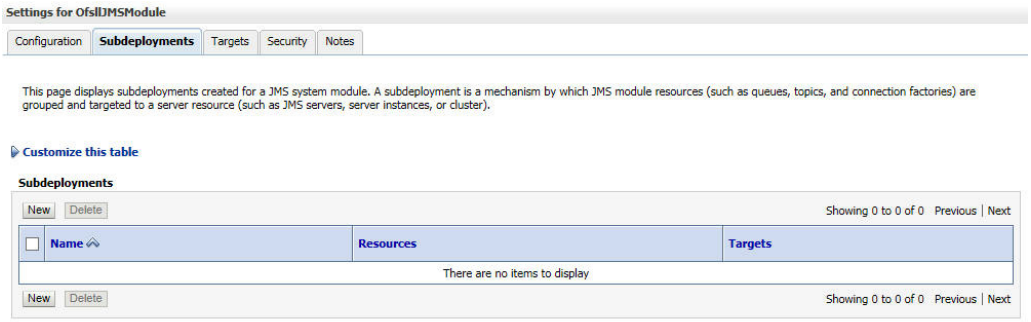
7. Click 'Finish' to save and activate the changes. Once done, the following window is displayed.



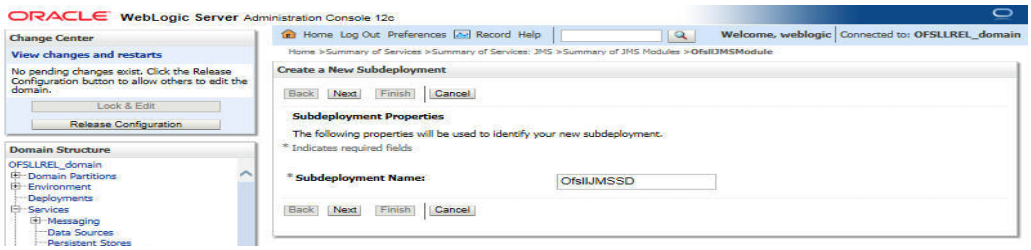
9.4.3 Subdeployment

1. Login to WebLogic Server 12c console (http://hostname:port/console) by specifying the Weblogic administrator user name and password.

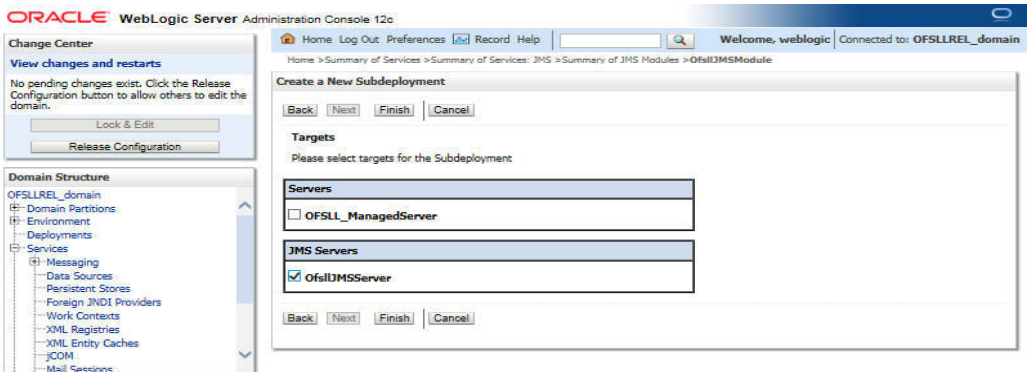
2. Click Domain Name > Services > Messaging > JMS Modules. The main window displays the list of JMS modules available.
3. Select the created JMS module ‘OfsllJMSModule’ and click 'Subdeployments' tab. The following window is displayed.



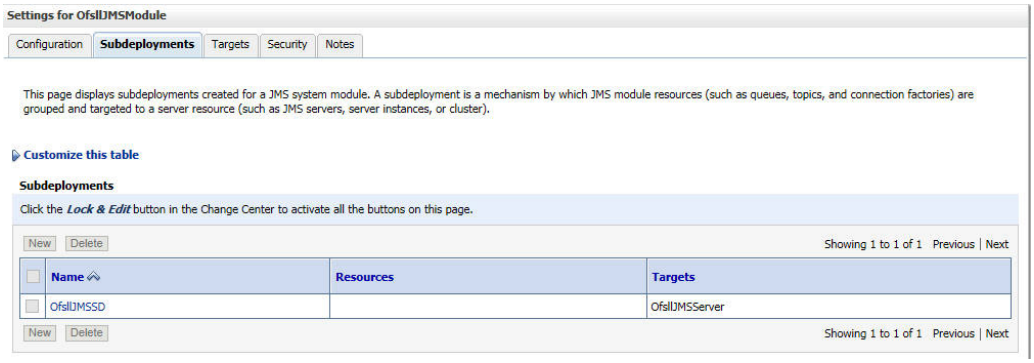
4. Click 'New'. The following screen is displayed.



5. Specify the Subdeployment Name as ‘OfsllJMSSD’. Click 'Next', the following window is displayed.



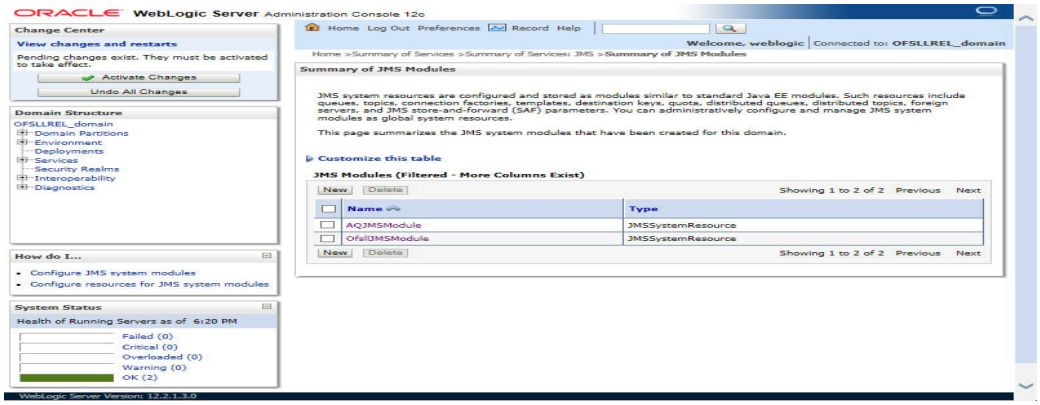
6. Select the check box against the newly created JMS Server and click ‘Finish’. Once done, the following window is displayed.



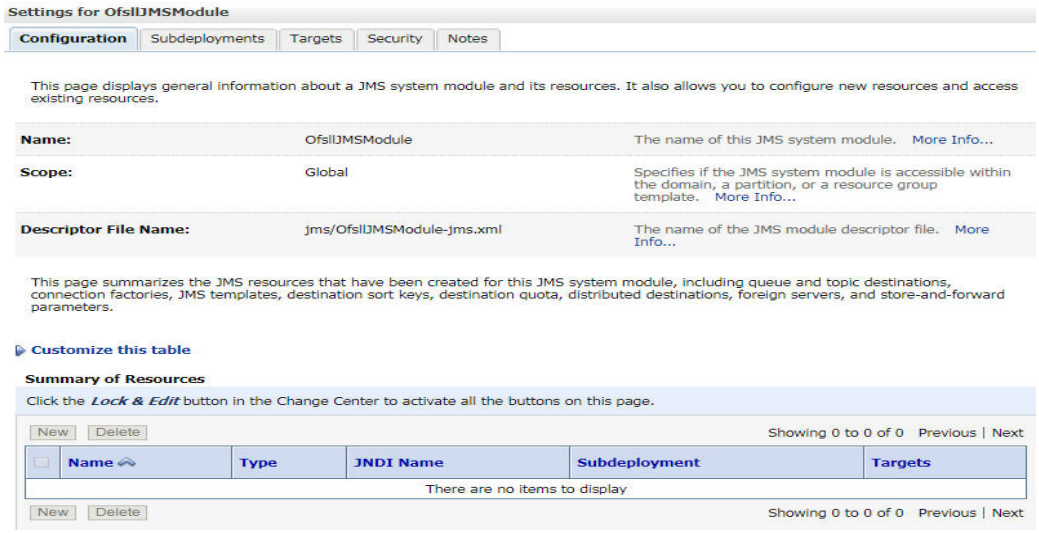
You can further click 'New 'to create more Queues and repeat the steps explained above.

9.4.4 Create JMS Connection Factory

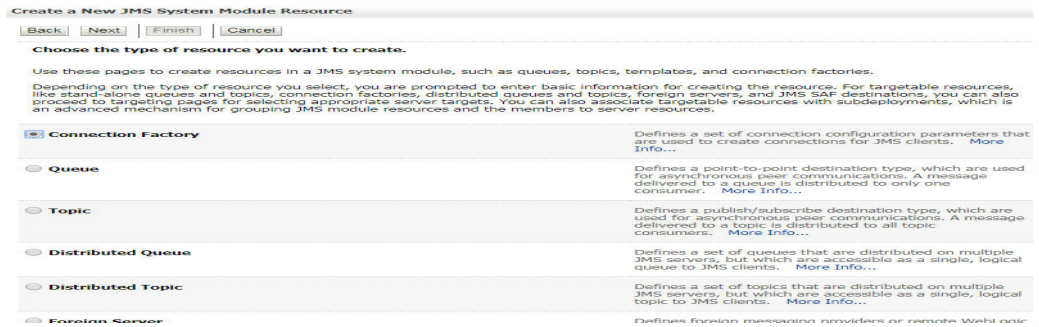
1. Login to WebLogic Server 12c console (http://hostname:port/console) by specifying the Weblogic administrator user name and password.
2. Click Domain Name > Services > Messaging > JMS Modules. The main window displays the list of JMS modules available.
3. Select the newly created JMS module ‘OfsllJMSModule’. The following window is displayed.



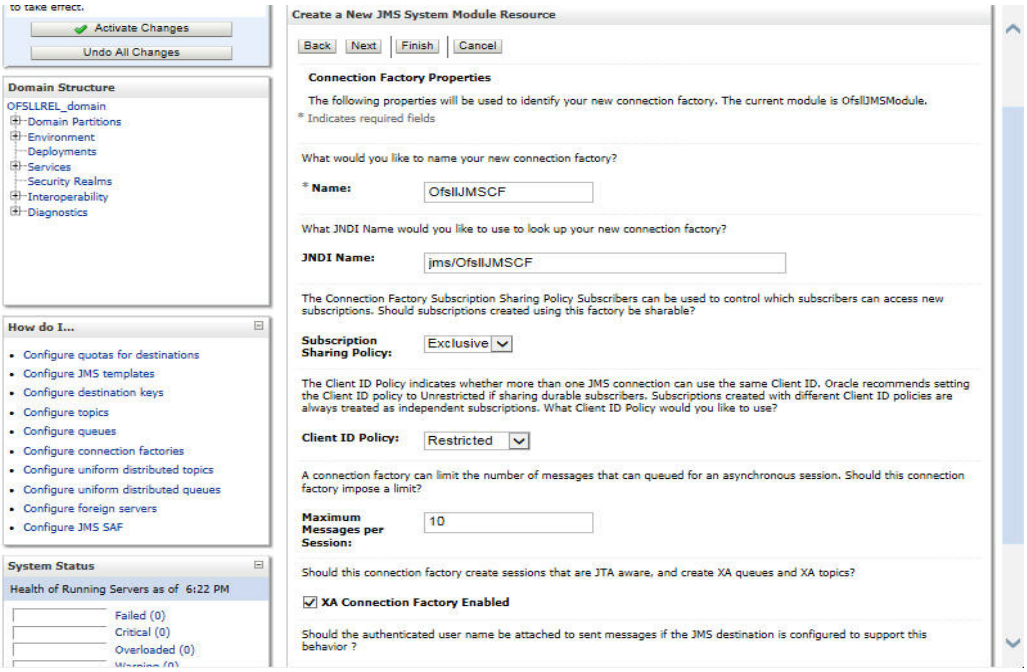
4. Click 'New’. The following window is displayed.



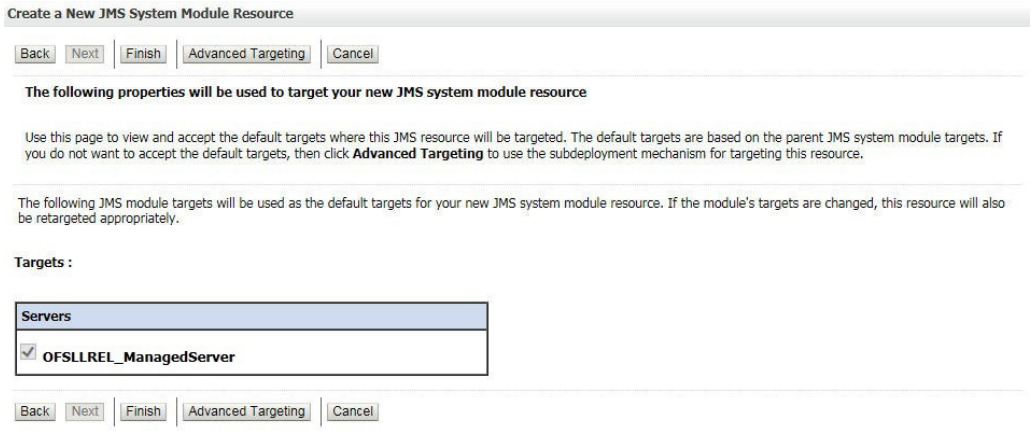
5. Click 'Next'. The following window is displayed.



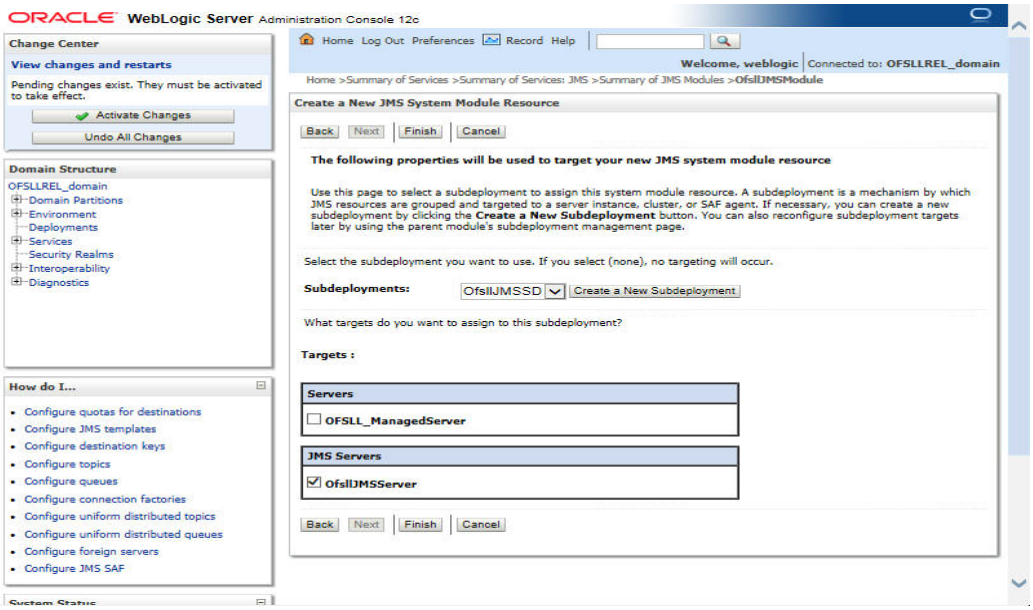
6. Select 'Connection Factory' option and click 'Next'. The following window is displayed.



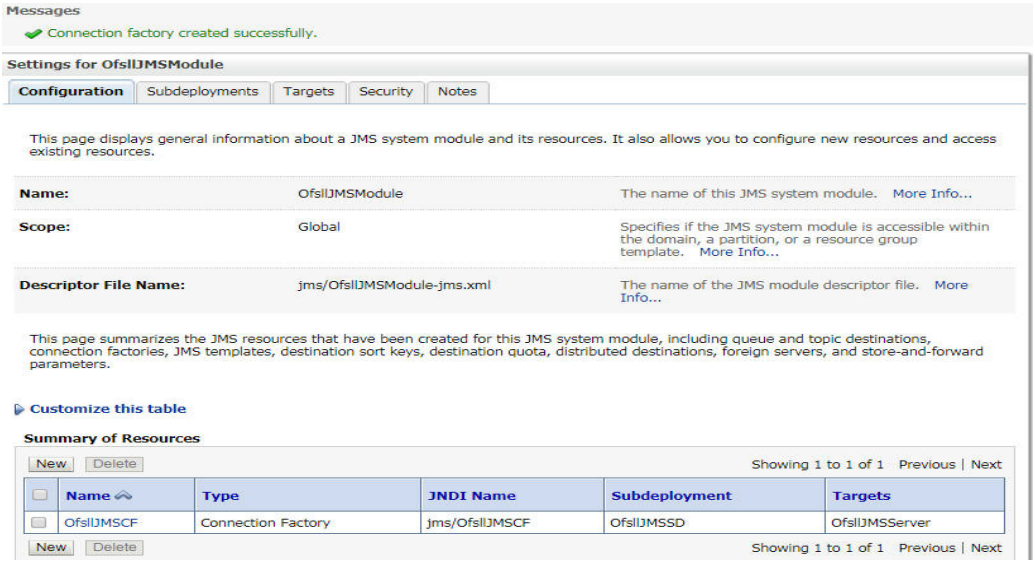
7. Specify the following details:
   - Enter the Name of the Connection Factory as 'OfsllJMSCF'
   - Enter the JNDI Name as 'jms/OfsllJMSCF'
   - Select the check box 'XA Connection Factory Enabled'
8. Click 'Next'. The following window is displayed.



9. Click 'Advanced Targeting'. The following window is displayed.



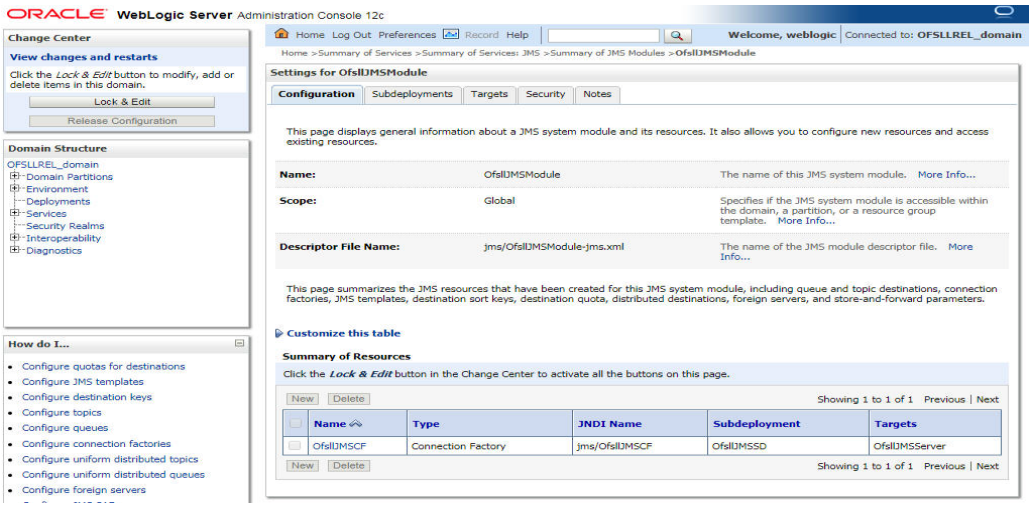
10. Select the Subdeployments as ‘OfsllJMSSD’ from the drop down list.
11. Under JMS Servers, select the check box against 'OfsllJMSServer'.
12. Click 'Finish' to save and activate the changes. Once done, the following window is displayed.



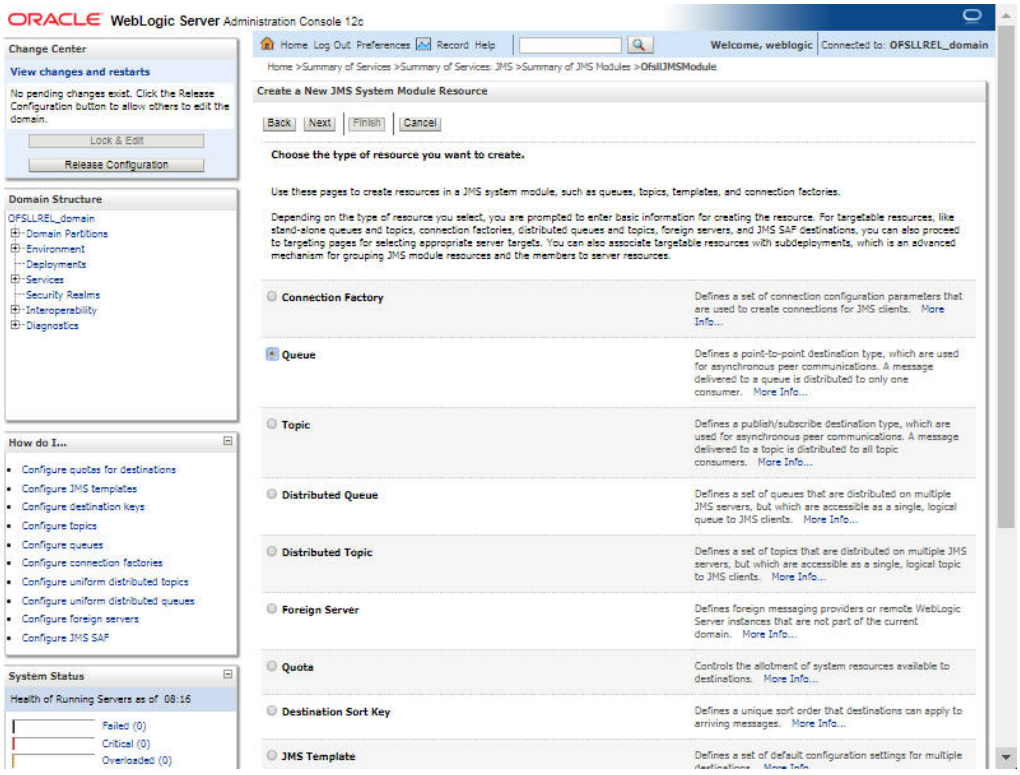
9.4.5 Create JMS Queue

1. Login to WebLogic Server 12c console (http://hostname:port/console) by specifying the Weblogic administrator user name and password.
2. Click Domain Name > Services > Messaging > JMS Modules. The main window displays the list of JMS modules available.

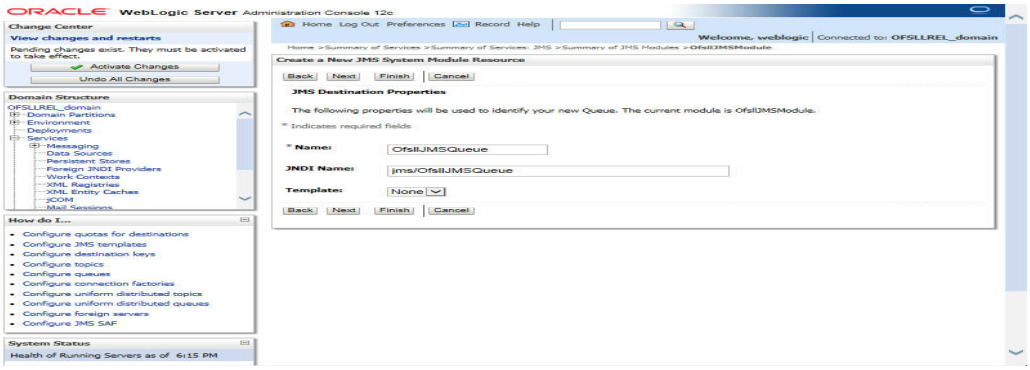
3. Select the newly created JMS module ‘OfsllJMSModule’. The following window is displayed.



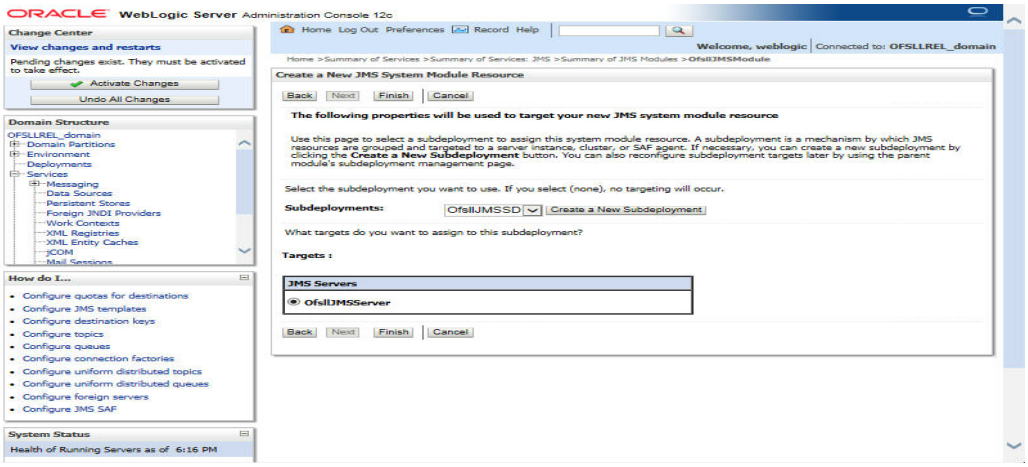
4. Click ‘New’. The following window is displayed.



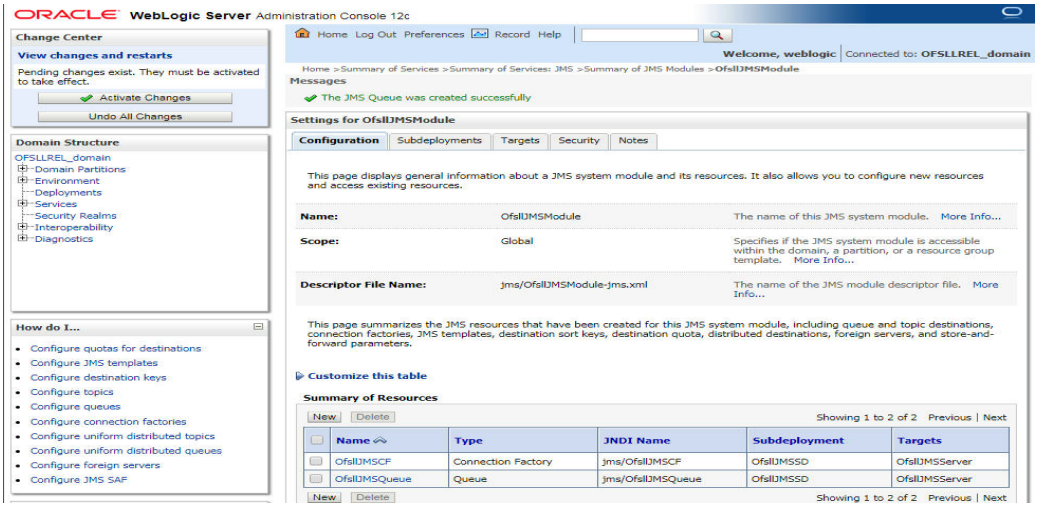
5. Select the 'Queue' option and click 'Next'. The following window is displayed.



6. Specify the following details while creating new JMS System Module Resources:
   - Enter the Name of the Queue as 'OfsllJMSQueue'
   - Enter the JNDI Name as 'jms/OfsllJMSQueue'
   - Select the Template as 'None'
7. Click 'Next'. The following window is displayed.



8. Select the Subdeployments as 'OfsllJMSSD' from the drop-down list.
9. Click 'Finish' to save and activate the changes. Once done, the following window is displayed.



You can further click 'New 'to create more Queues and repeat the steps explained above.

9.5 Configure External Client Certificates

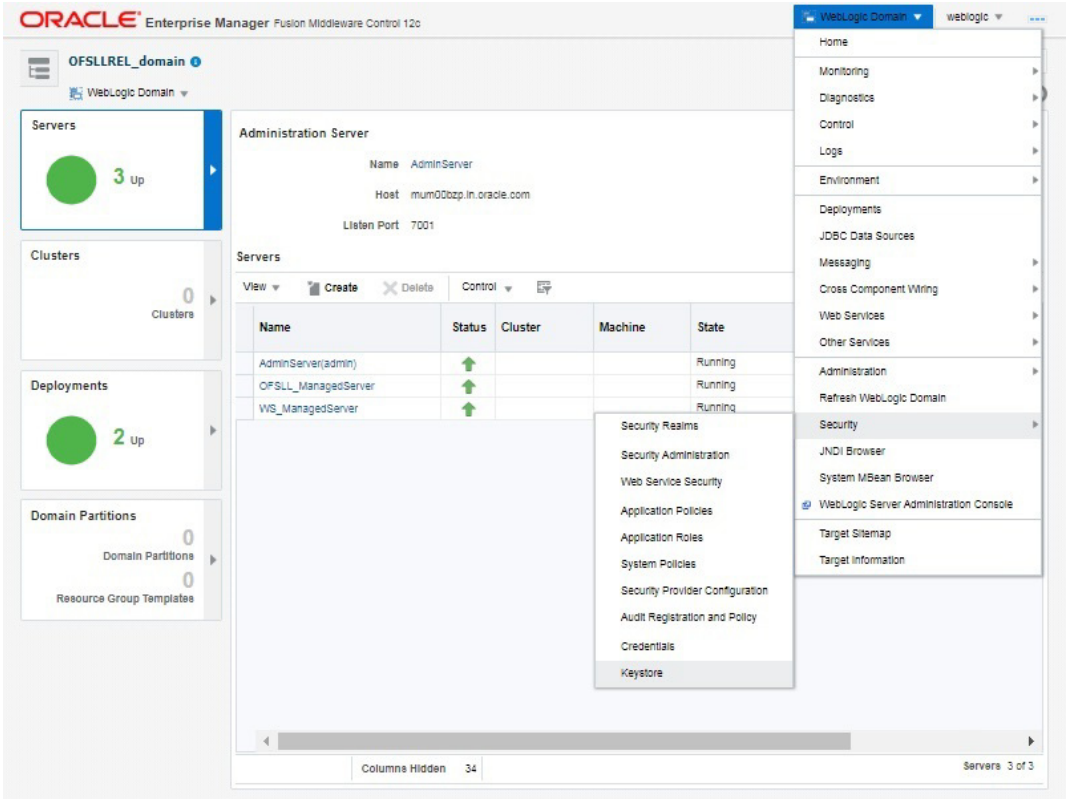
The Webhook option in OFSLL extends the support of interfacing with third-party applications by sending REST API based notifications of changes through system generated Webhook event actions.

In a Webhook setup you can notify the changes that are done in OFSLL by triggering Webhook request as an event action and propagate the information to the dependant third-party applications (client) through specific https communication channel.

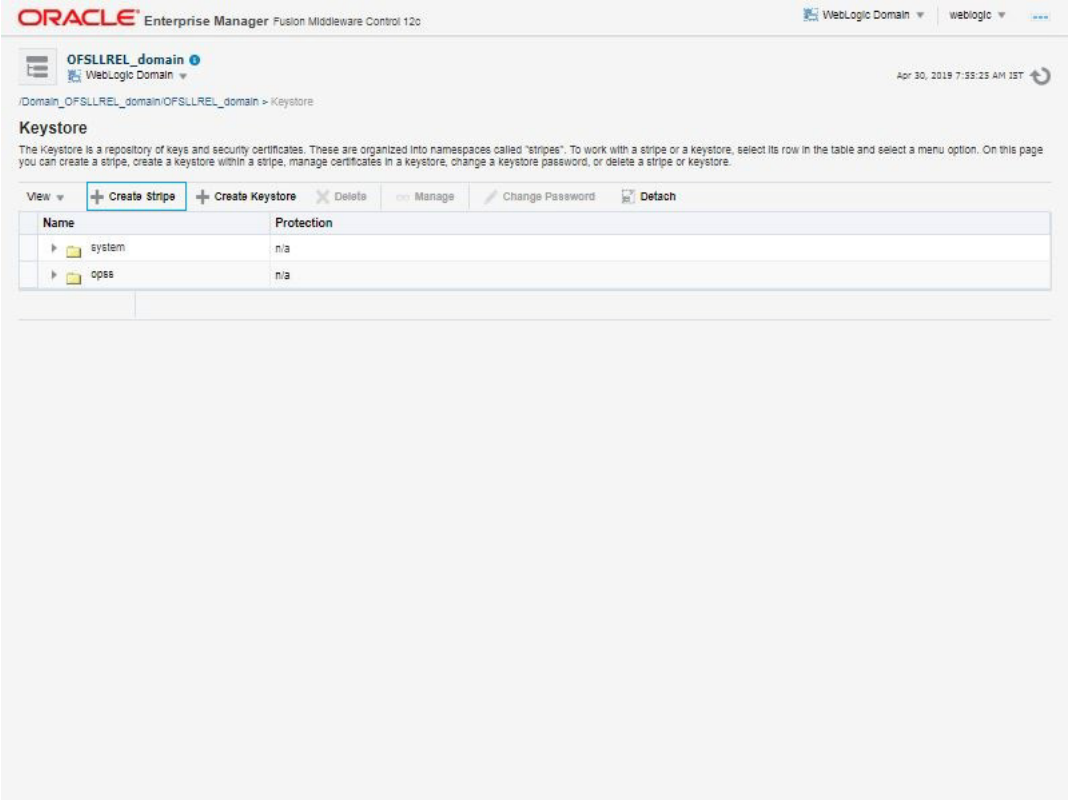
For webhook HTTPS communication, client certificates are to be imported in Weblogic OPSS keystore for each channel.

Follow the below steps to import the certificates.

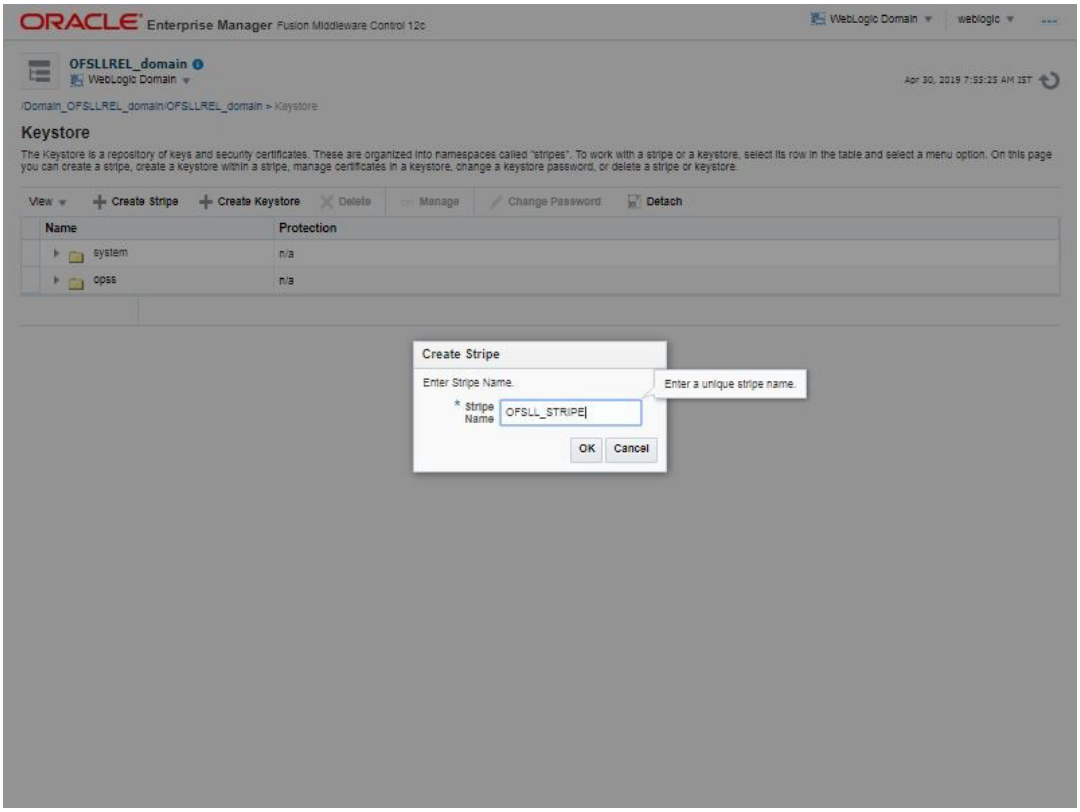
1. Login to the Oracle Enterprise Manager 12c console. (i.e. http://hostname:port/em)
2. Click on ‘Weblogic Domain’ drop-down list and navigate to Security > Keystore.



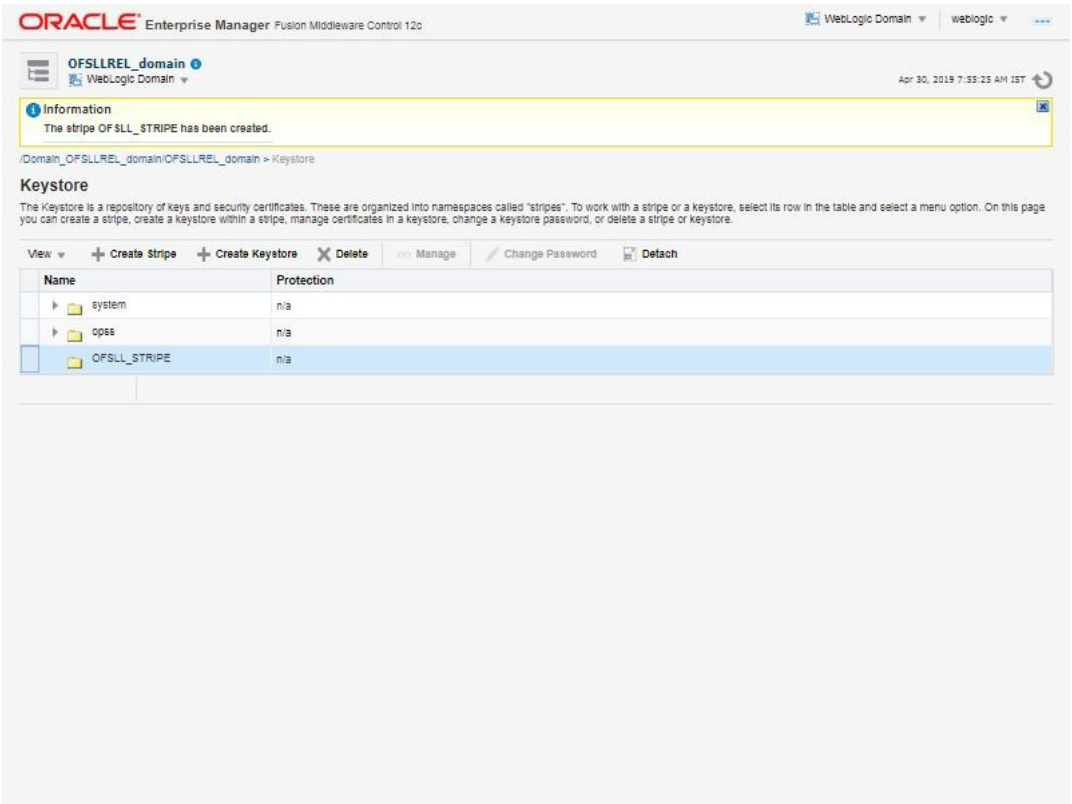
3. Click on ‘Create Stripe’.



4. Enter the Stripe Name as ‘OFSLL_STRIPE’.

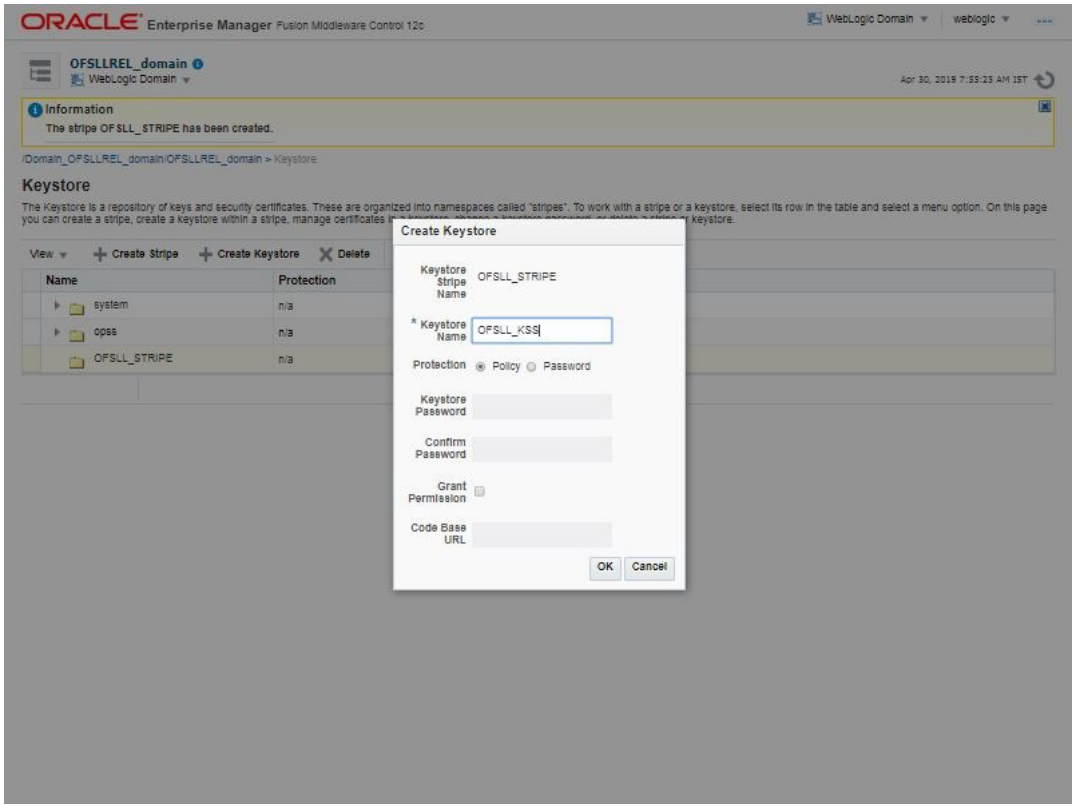


5. Click ‘OK’. The following OFSLL_STRIPE is created.

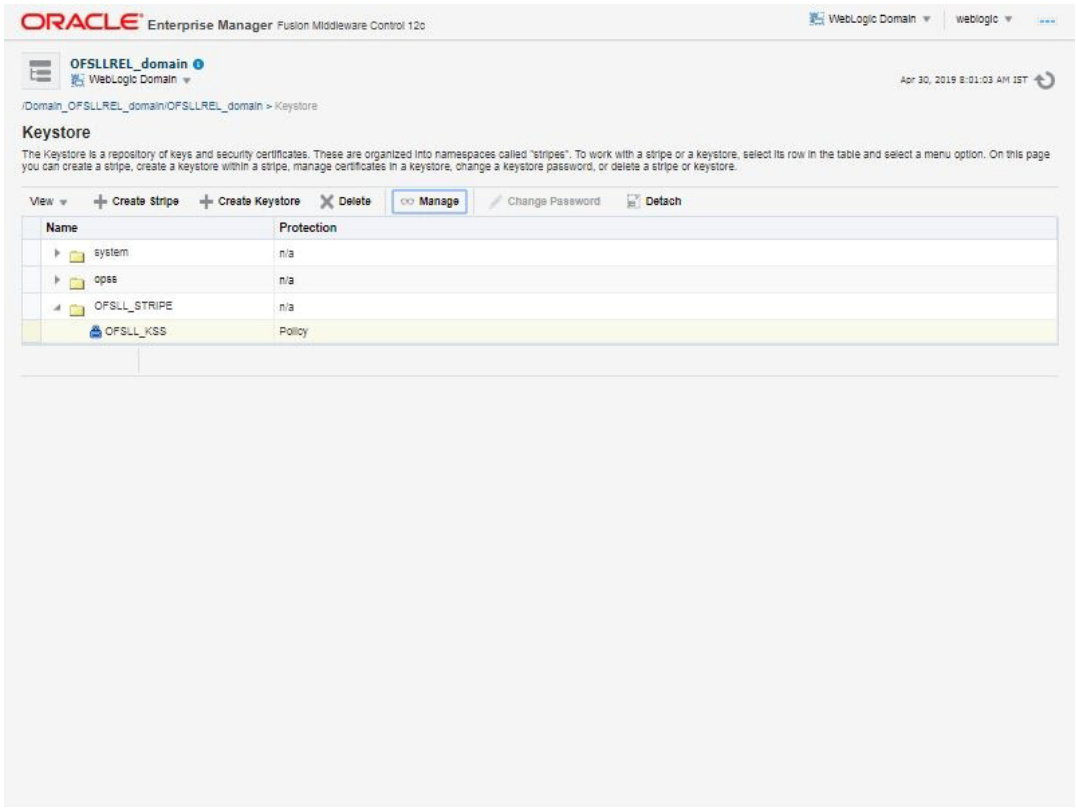


6. Select the newly created ‘OFSLL_STRIPE’ and click ‘Keystore’.

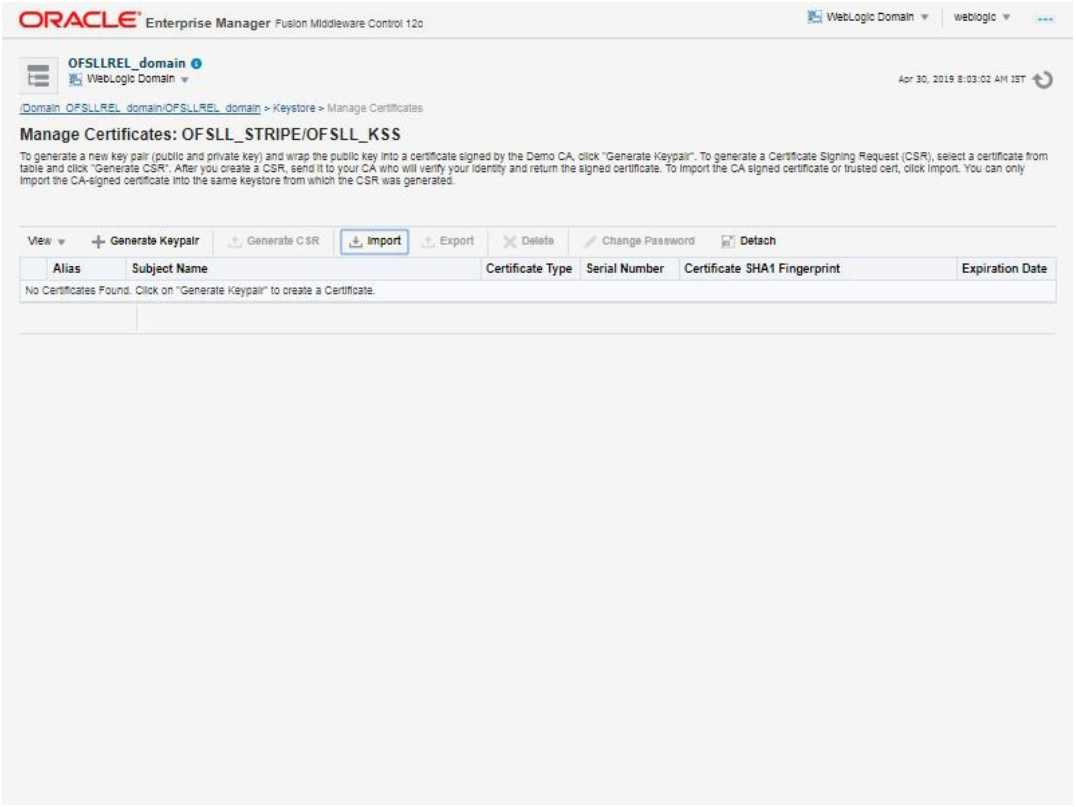
7. Enter the Keystore Name as ‘OFSLL_KSS’ and click ‘OK’.



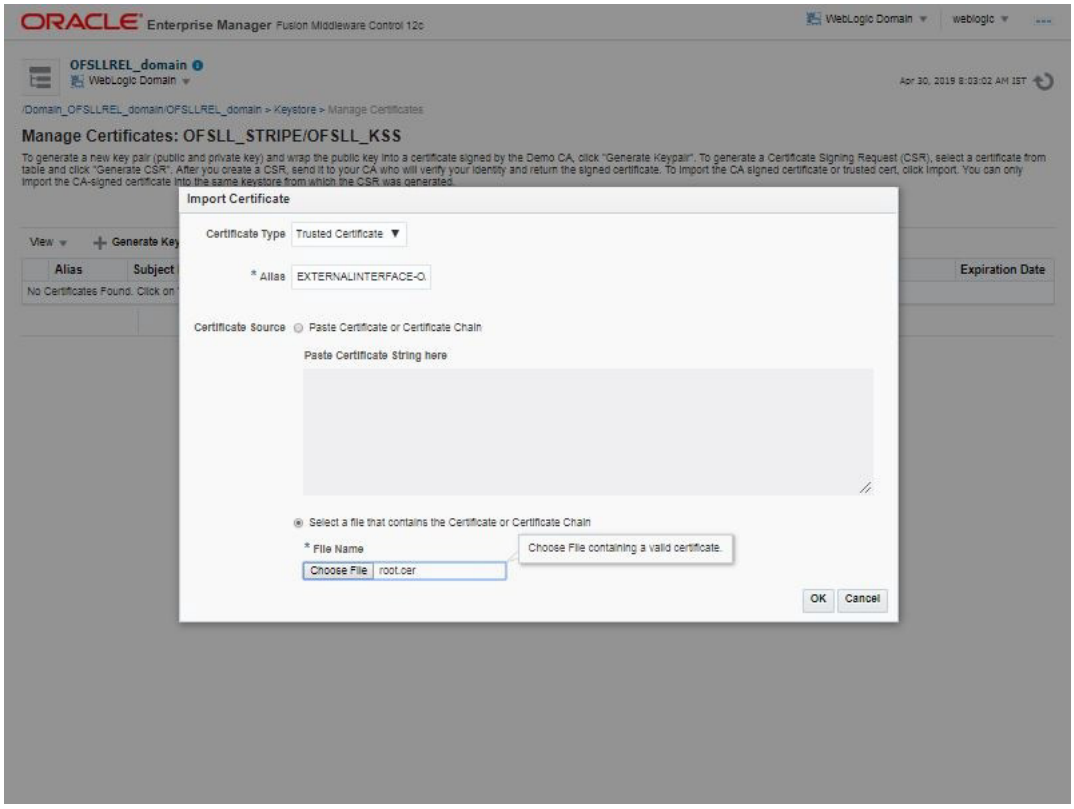
8. Select ‘OFSLL_KSS’ and click ‘Manage’..



9. Click ‘Import’.



10. In the below ‘Import Certificate’ screen, specify the following details:
    - Certificate Type: Trusted Certificate
    - Alias: webhook Channel Name
    - Choose file: webhook channel certificate

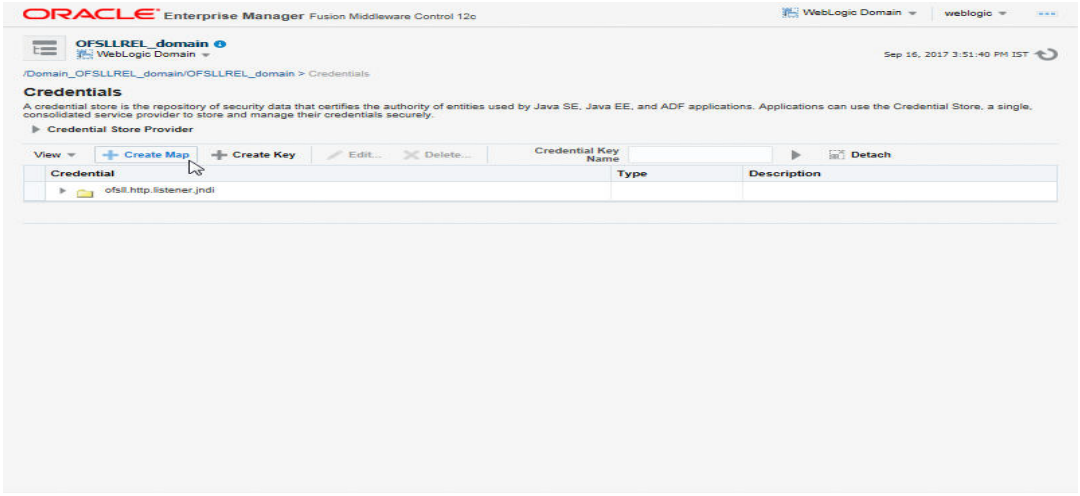


11. Click ‘OK’.

9.6 Create Credentials and System Policies

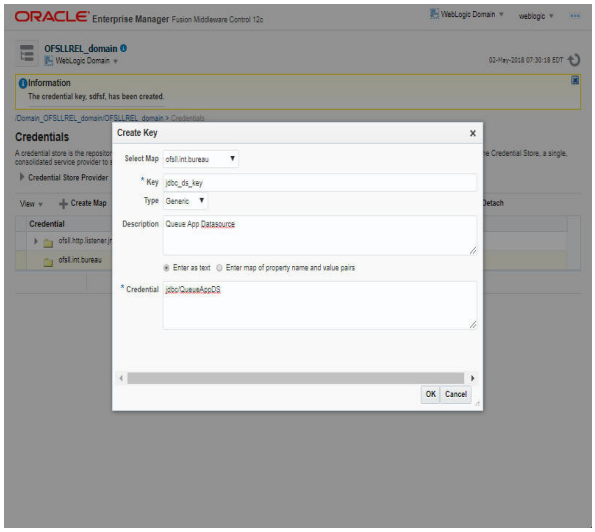
In order Configure MDB flow, you need to create credentials and system policies. The credentials are accessed through CSF framework which is managed by Oracle Weblogic Server. The keys are managed by Maps and Maps need to be given with Permissions.

1. Login to Oracle Enterprise Manager (http://hostname:port/em).
2. On the left panel, right click on OFSLLREL_domain and select Security > System Policies > Credentials. The following window is displayed.



3. Click ‘Create Map’. The following window is displayed.

4. Enter Map Name as ‘ofsll.int.bureau’ and click ‘OK’.
5. Click ‘Create Key’. The following window is displayed.



6. Specify the following details:
   - Select Map as ‘ofsll.int.bureau’ from the drop down list.
   - Specify Key as ‘jdbc_ds_key’

- Select Type as ‘Generic’ from the drop down list.
- Specify the Credential as ‘jdbc/QueueAppDS’.

7. Click ‘OK’.
8. Similarly you need to create the following Maps and corresponding keys as indicated in following table.

Maps	Keys	Description
ofsll.int.bureau		This map is used to setup keys for all credit bureau interfaces
	ProxyServer	Name of the proxyServer to be configured
	ProxyPort	Port to which ProxyServer is running.
	ExpEcalsURL	The Experian Connection URL to be configured.
	ExpDirectExperianEnabled	If you set value as true, then you would be setting ecals response URL. Else, the Ecals request URL
	ExpCertPath	The location of .jks file which contains the valid certificate for Experian Credit Bureau.
	ExpBusUserNamePassword	Login Credentials to be configured for Experian Business reports.
	ExpConUserNamePassword	Login Credentials to be configured for Experian Consumer reports.
	EfxURL	The Equifax Connection URL to be configured.
	EfxCertPath	The location of .jks file which contains the valid certificate for Equifax Credit Bureau.
	EfxUserNamePassword	Login credentials to be configured for accessing Equifax Reports.
	TucCertPath	The location of .jks file which contains valid certificate for Transunion Bureau.
	TucCertPassword	The password that requires to read the valid .jks certificate for the Transunion Bureau.
	TucUserNamePassword	Login credentials to be configured for accessing Transunion reports
	TucConnectionURL	The Transunion URL to be configured.
	jdbc_ds_key	Datasource configured to retrieve data for bureau.
	source	Configured as EXTERNAL for actual call.
ofsll.int.outbound		This map is used to setup keys for the RouteOne and Dealer track call back from OFSLL.

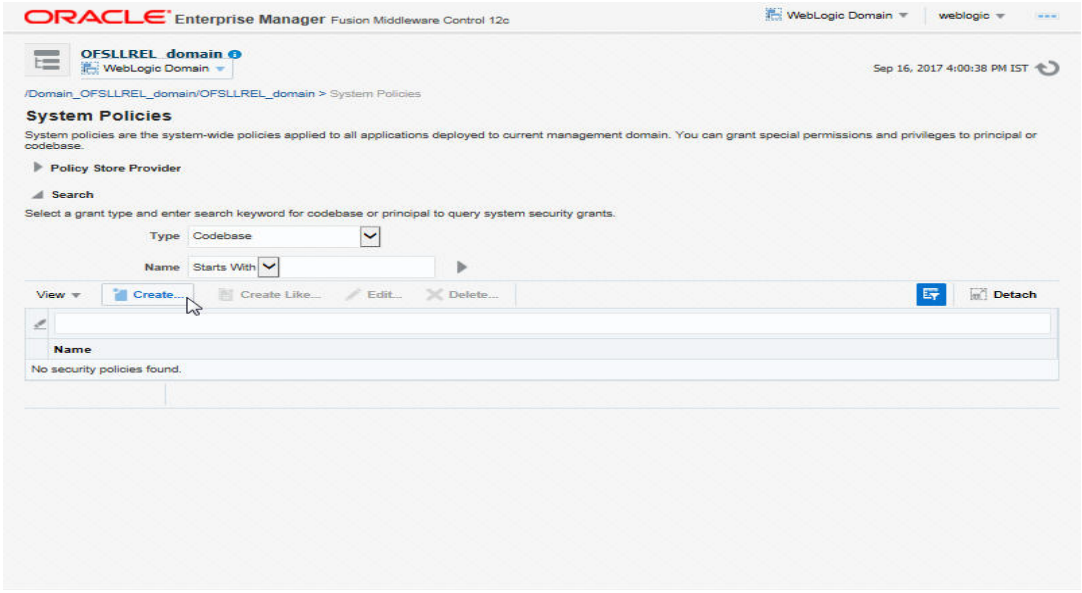
Maps	Keys	Description
	roUserNamePassword	Login Credentials used at the time of call back from OFSLL to RouteOne Interface.
	dtUsernamePassword	Login Credentials used at the time of Call back from OFSLL to Dealer Track Interface.
	jdbc_ds_key	Datasource configured to retrieve data for out-bound Resources.
	roPostDealerUsername-Passwd	Credentials required to upload the dealer details to Route One Portal
	roPostDealerWbsURL	Route One Post Dealer Web Service url
	roDealerUploadURL	Route One URL to upload the Dealer details
	dtPostDealerUsername-Passwd	Credentials required to upload the dealer details to Dealer Track Portal
	dtPostDealerWbsURL	Dealer Track Post Dealer Web Service url
	dtDealerUploadURL	Dealer Track URL to upload the Dealer details
	VertexUserNamePd	Credentials required to connect to VERTEX web service
	VertexTrustedId	ID required to connect to VERTEX web service
	TorqueItsUserName-Password	Credentials required to connect to TorqueIts web service
	TorqueItsURL	TorqueIts Decision service URL
	ProxyHost	Name of the proxyServer to be configured.
	ProxyPort	Port to which ProxyServer is running.
ofsll.int.bip		This Map is used to setup all the Keys required to setup interface with BIP to generate reports.
	local_top_dir	Define the path of the local BIP server where you would like place the generated BIP reports.
	email_from_addr	Define the From Email address to be used while sending email for the generated BIP reports.
	emailBodyContentPath	The path for 'file.properties' file that contains the content of the subject and body required while sending letter, report or correspondence as mail to the applicant or producer. For example; /tmp/file.properties *Refer to note below for details on 'file.properties' file creation for email configuration.
	fax_server	Configure the name of Fax server to be used to fax the generated BIP reports.

Maps	Keys	Description
	jdbc_ds_key	Datasource configured to retrieve data for BIP.
ofsll.int.file transfer		This map is used to setup keys for all credit bureau interfaces
	sftp_key	Credentials to login to SFTP server(Username/ Password)
	sftp_top_dir	Top root directory for SFFTP server
	sftp_servers	SFTP server names
ofsll.int.se curity	bip_key	This is BIP login credentials
ofsll.int.gri	GriURL	GRI web service URL to be configured.
	GriAPIKey	GRI API key to be configured
	ProxySet	System Level Proxy Enabled/Disabled. Value can be either true or false. True= proxy required False = proxy not required
	ProxyHost	Name of the proxyServer to be configured. Set only if ProxySet =true.
	ProxyPort	Port on which ProxyServer is running. Set only if ProxySet =true.
	jdbc_ds_key	Datasource configured to retrieve the request XML for GRI.
	GriCertPath	The location of .jks file which contains the valid certificate for GRI. Configure only when a valid certificate is available.
ofsll.int.co mmon		This map is used to setup keys for common JMS Queue
	OfsllJMSQueueJNDI	The JMS queue JNDI name to be configured
	OfsllJMSQueueCF	The JMS queue connection factory to be configured
	OfsllJMSServerURL	The JMS server url to be configured. Ex: t3://<JMS server host>:<JMS server port>
ofsll.int.we bhook	jdbc_ds_key	Datasource configured to retrieve data for Webhook.

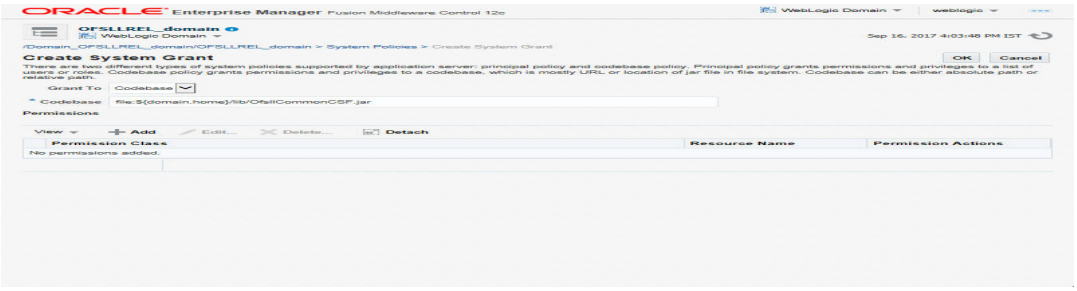
* A new file(file.properties) needs to be created and copied to the application server in the same path as mentioned in the value corresponding to the key 'emailBodyContentPath' under the map 'ofsll.int.bip'. The file should have the following contents:

- letter_subject='Text that is configurable and would be the subject of the mail'
- letter_body='Text that is configurable and would be the body of the mail'
- correspondence_subject='Text that is configurable and would be the subject of the mail'
- correspondence_body='Text that is configurable and would be the body of the mail'
- report_subject='Text that is configurable and would be the subject of the mail'
- report_body='Text that is configurable and would be the body of the mail'

9. On the left panel, right click on OFSLLREL_domain and select Security > System Policies. The following window is displayed.

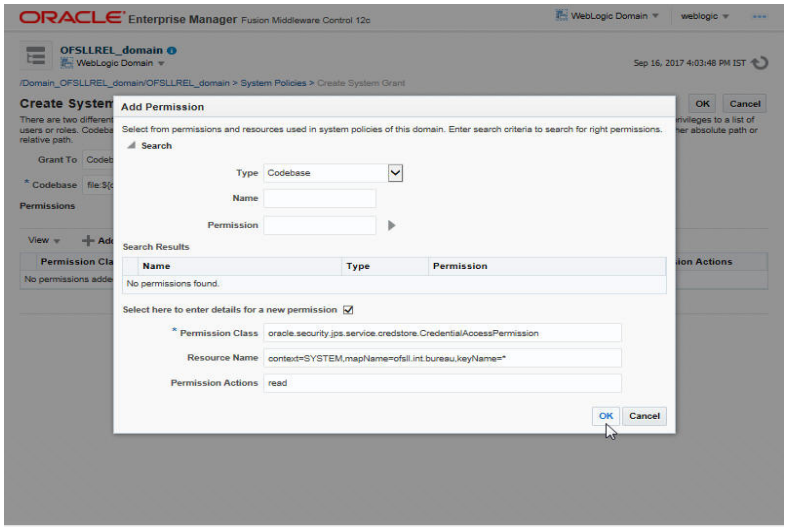


10. Click ‘Create’. The following window is displayed.



11. Enter the codebase as ‘file:${domain.home}/lib/OfsllCommonCSF.jar’

12. Click ‘Add’. The following window is displayed.



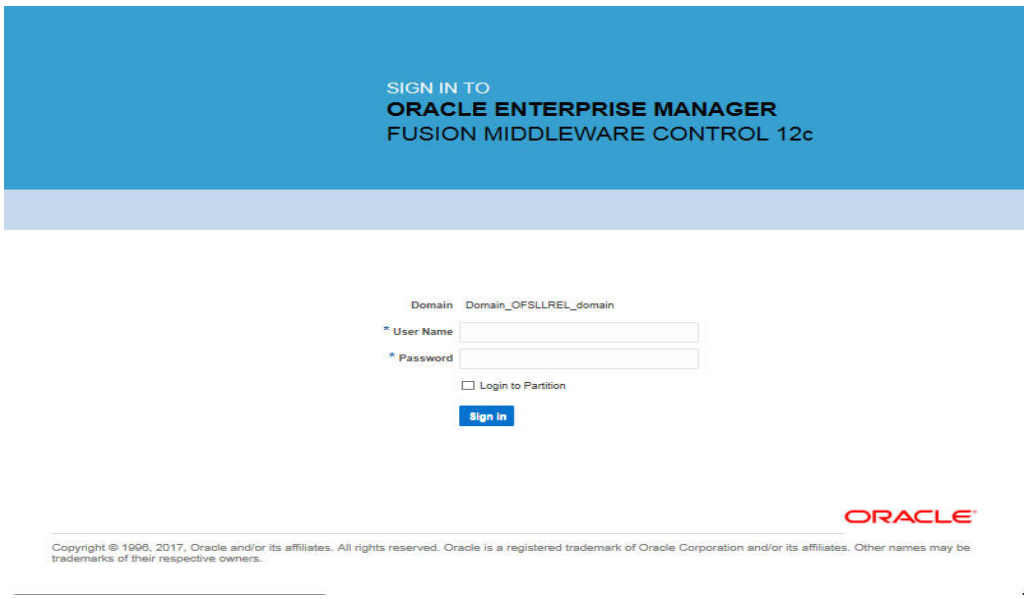
13. Select the check box 'Select here to enter details for a new permission'.
14. Specify the following details as the first permission class.

Permission Class	Resource Name	Permission Actions
oracle.security.jps.service.credstore.CredentialAccessPermission	context=SYSTEM,mapName=ofsll.int.bureau,keyName=*	read
oracle.security.jps.service.credstore.CredentialAccessPermission	context=SYSTEM,mapName=ofsll.int.filetransfer,keyName=*	read
oracle.security.jps.service.credstore.CredentialAccessPermission	context=SYSTEM,mapName=ofsll.int.outbound,keyName=*	read
oracle.security.jps.service.credstore.CredentialAccessPermission	context=SYSTEM,mapName=ofsll.int.bip,keyName=*	read
oracle.security.jps.service.credstore.CredentialAccessPermission	context=SYSTEM,mapName=ofsll.int.gri,keyName=*	read
oracle.security.jps.service.credstore.CredentialAccessPermission	context=SYSTEM,mapName=ofsll.int.common,keyName=*	read
oracle.security.jps.service.credstore.CredentialAccessPermission	context=SYSTEM,mapName=ofsll.http.listener.jndi,keyName=*	read
oracle.security.jps.service.credstore.CredentialAccessPermission	context=SYSTEM,mapName=ofsll.int.webhook,keyName=*	read, write, update
oracle.security.jps.service.keystore.KeyStoreAccessPermission	stripeName=OFSLL_STRIPE,keystoreName=OFSLL_KSS,alias=*	read

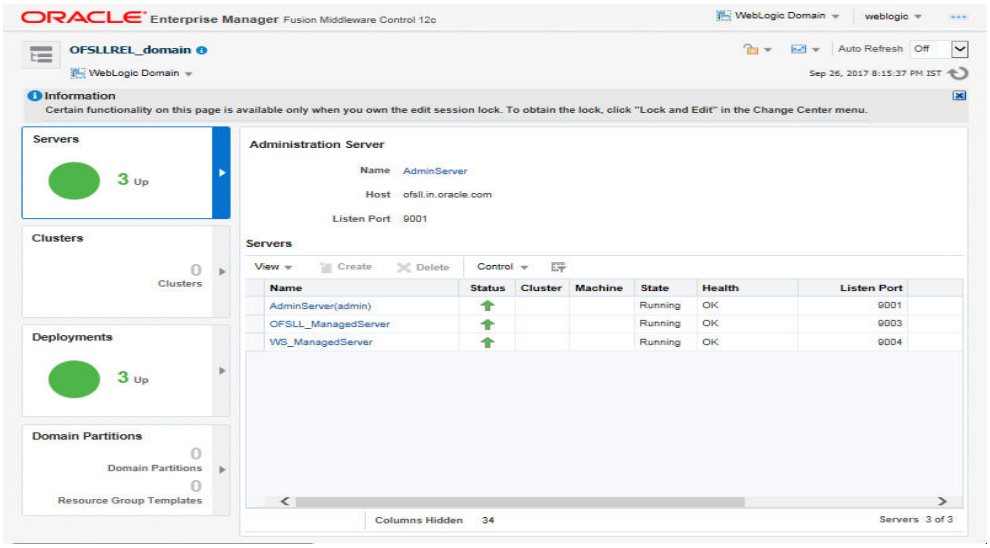
15. Click ‘OK’.

9.7 Deploy MDB EJB

1. Login to Web Logic application server enterprise manager (e.g.:http://hostname:port/em)

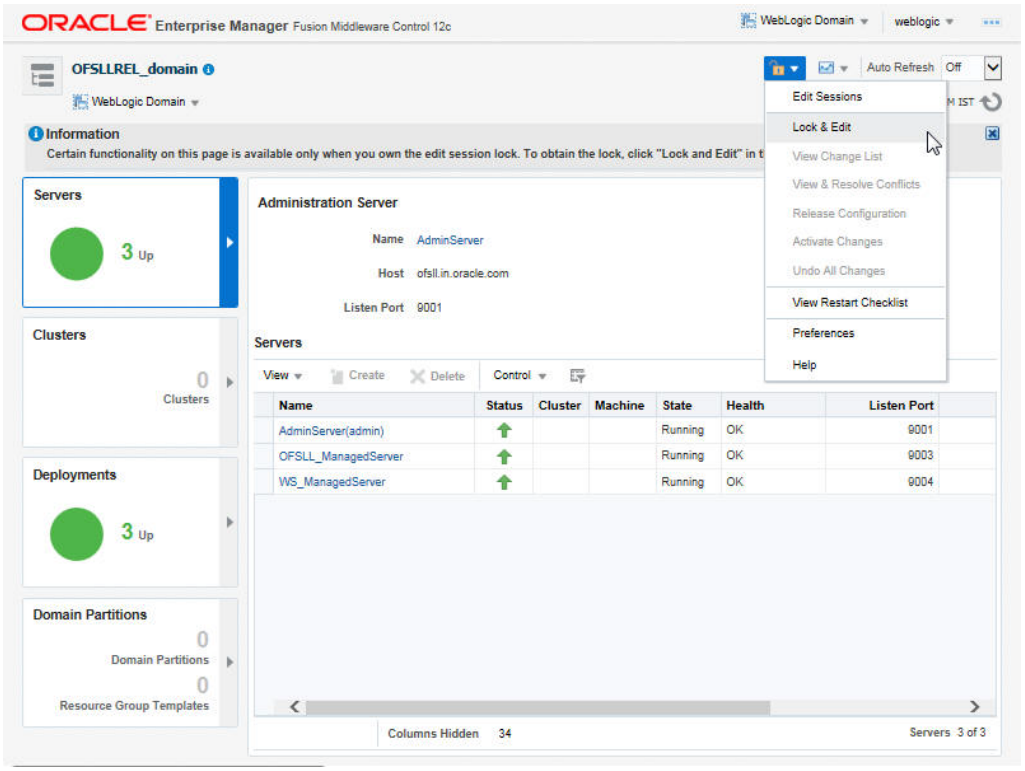


2. Enter valid login credentials. The following window is displayed.

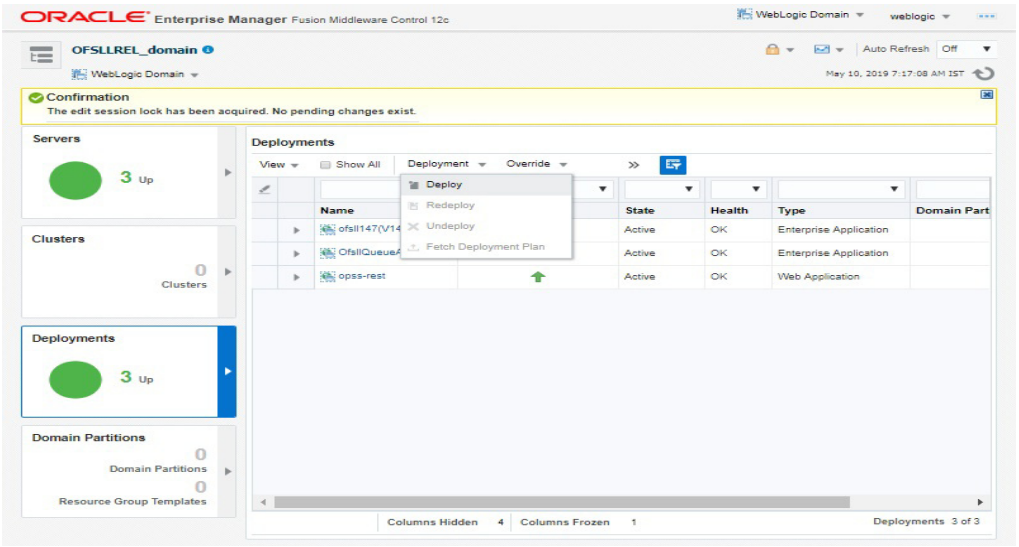


3. Select ‘Lock & Edit’ option in the lock drop-down list available in the header.

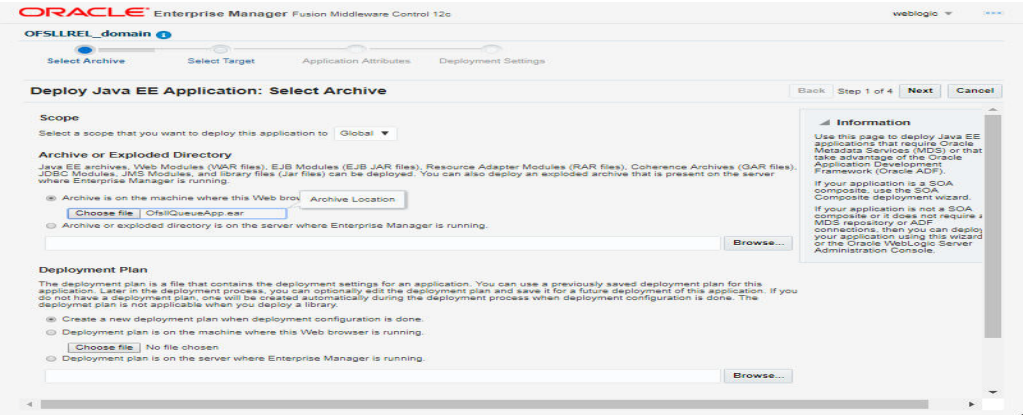
4. Click ‘Deployment’ in the left panel. The following window is displayed.



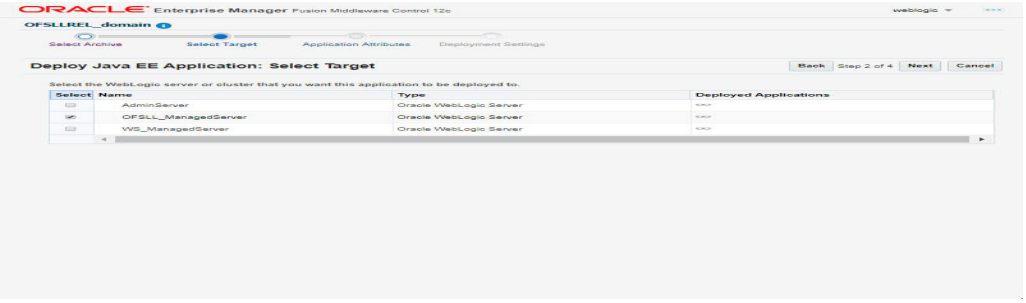
5. Select ‘Deploy’ from the Deployment drop-down list. The following window is displayed.



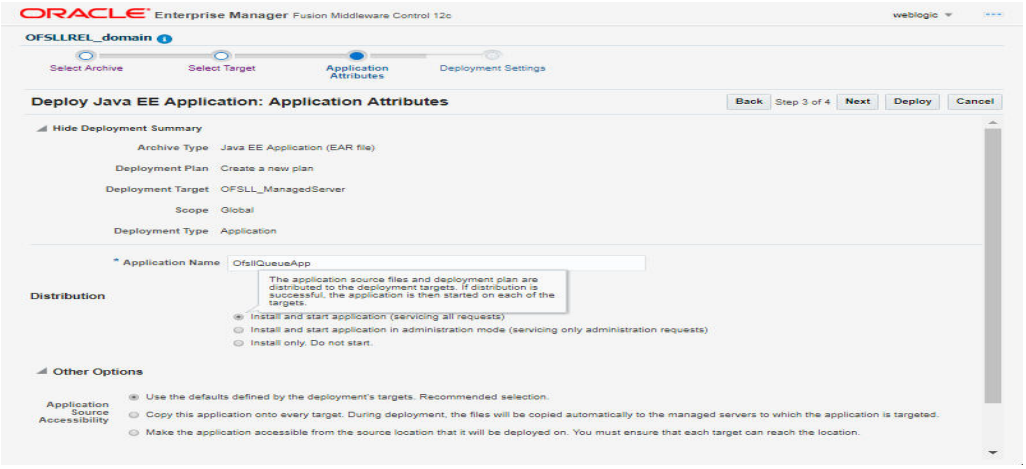
6. The following window is displayed.



7. Browse to the folder containing the MDB EJB. Eg: C:/OfsllQueueApp.ear
8. Click ‘Next’. The following window is displayed.

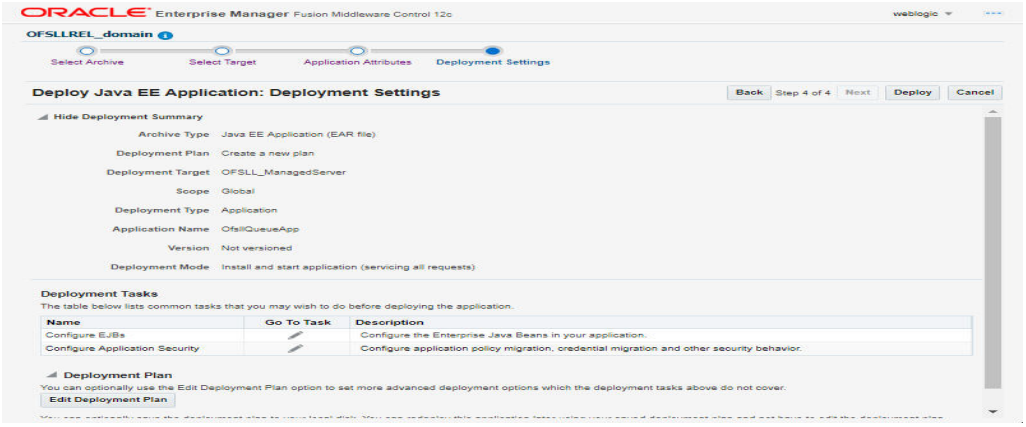


9. Select the server on which the MDB EJB needs to be deployed.
10. Click ‘Next’. The following window is displayed.

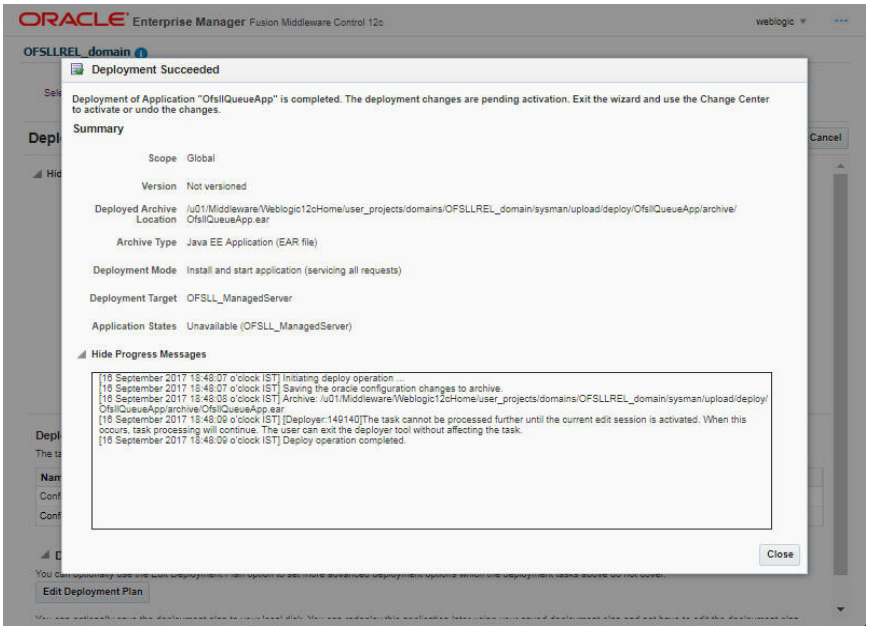


11. Select the option ‘Install and start application (servicing all requests)’.

12. Check the context root and click ‘Next’.The following window is displayed.



13. Click ‘Deploy’. On successful deployment, the following window is displayed.



14. Click ‘Close’. Post deployment, you need to activate the changes by selecting ‘Active Changes’ option from ‘Edit Session’ drop-down list as indicated in step 4 above.

Note

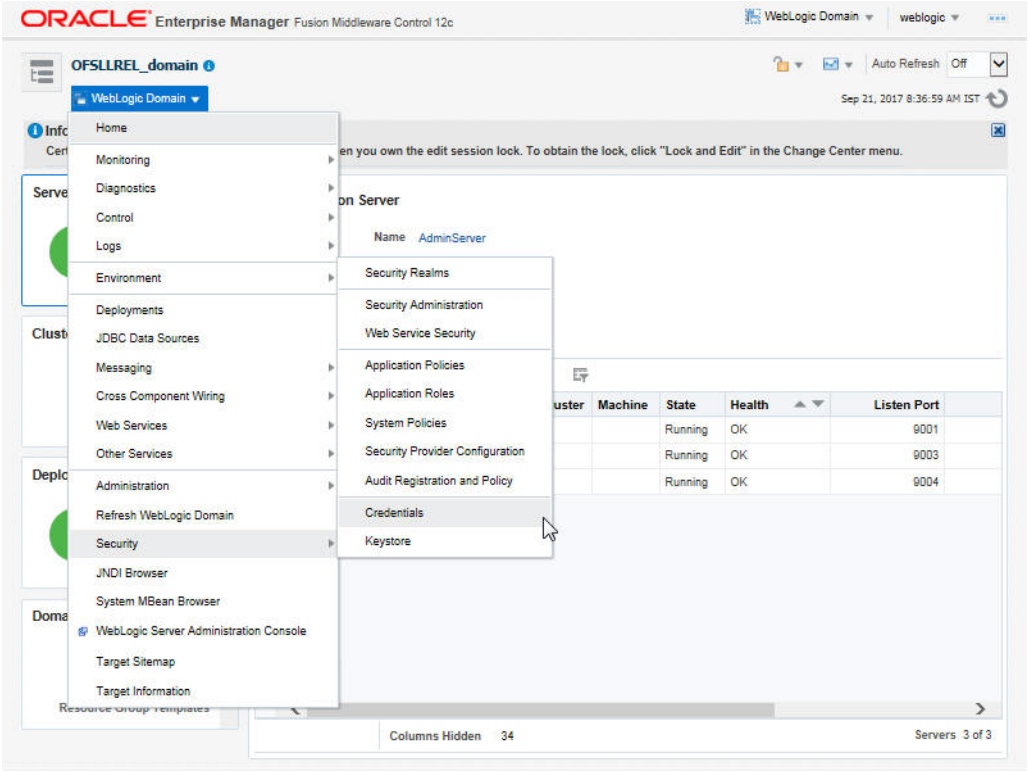
While starting the ‘OFSLLREL_ManagedServer’, always start with option ‘-DUseSun-HttpHandler=true’ to enforce the weblogic server to uses SUN SSL implementation.

10. Configuring Oracle BI Publisher for Application

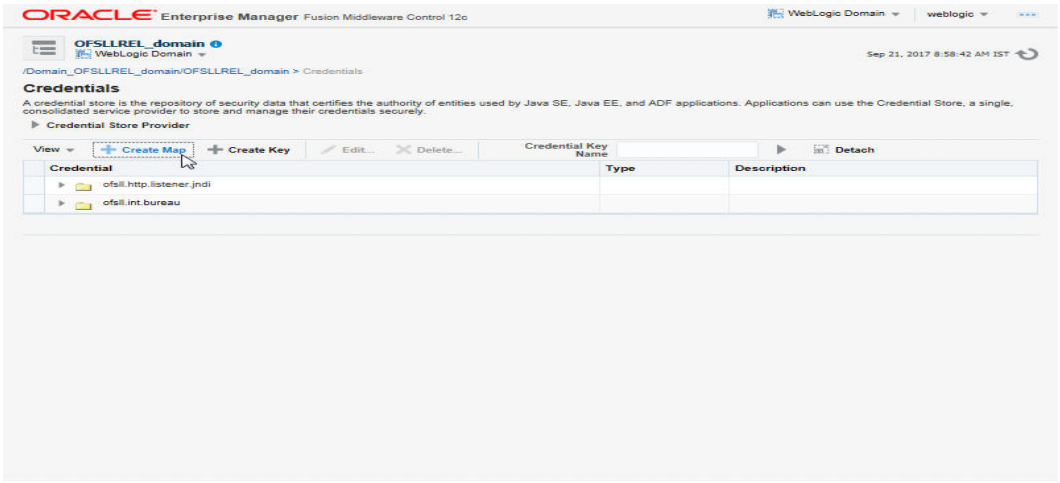
1. Copy the OfsllCommonCSF.jar from /WEB-INF/lib available in the staging area to $DOMAIN_HOME/lib
2. Update the setDomainEnv.sh file ($MW_HOME/user_projects/domains/mydomain/bin directory) by appending the above jar file path – EXTRA_JAVA_PROPERTIES="…….. ${EXTRA_JAVA_PROPERTIES} -Dofsll.csf.path=${DOMAIN_HOME}"
3. Configure Security via EMconsole

Note

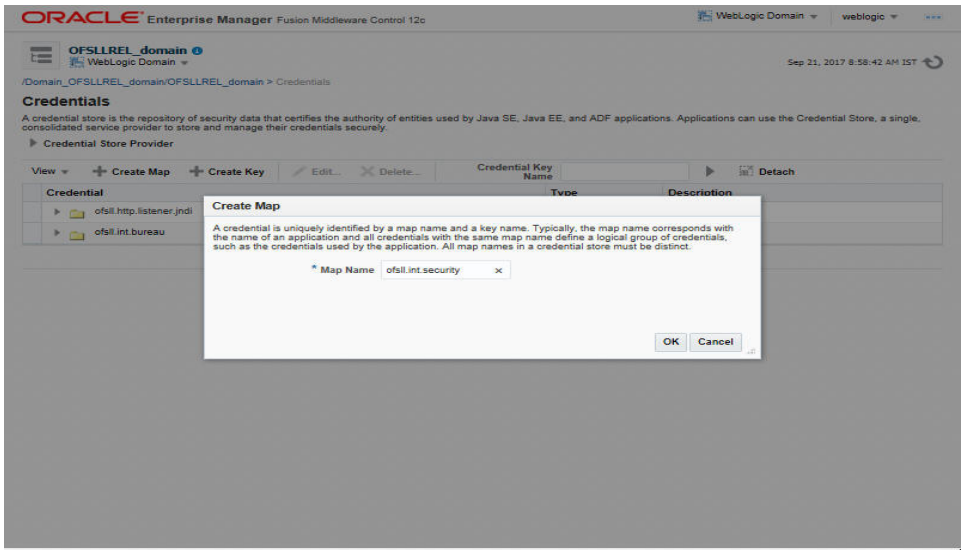
It is assumed that BI Publisher is installed and configured. Refer BI Publisher Guide for further details.



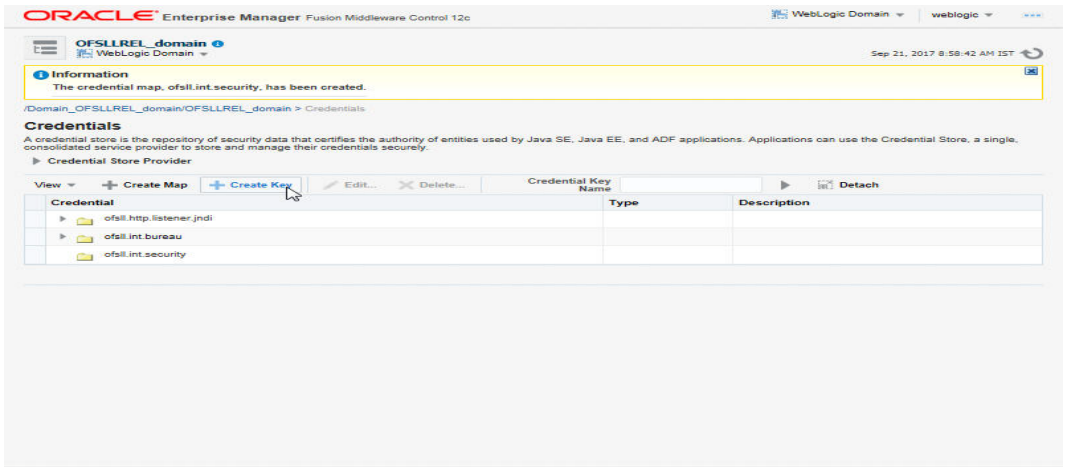
4. Click WebLogic Domain on the right panel. Select Security > Credentials. Click ‘Create Map’.



5. Enter the Map Name: ofsll.int.security.

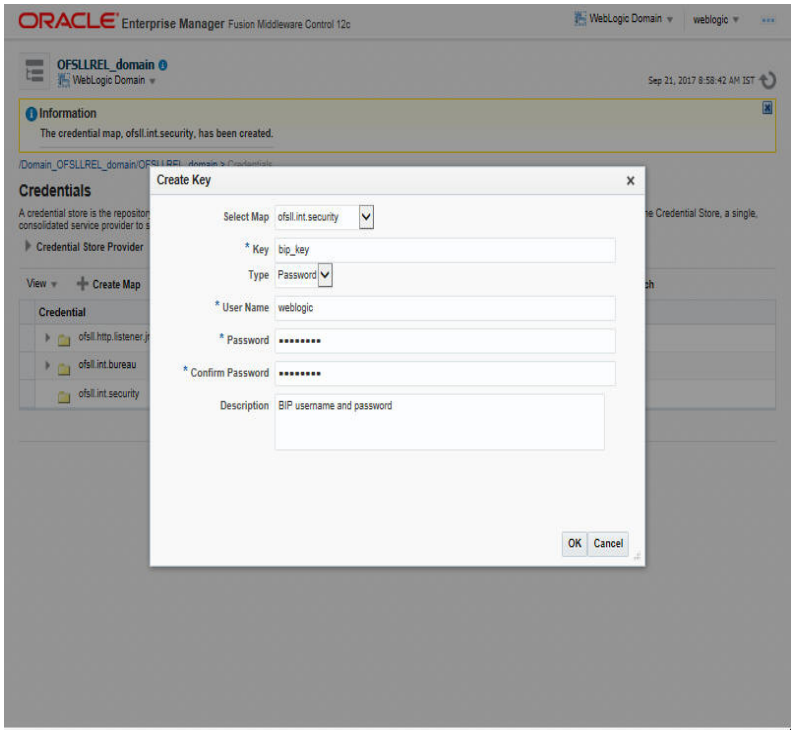


6. Click ‘OK’.

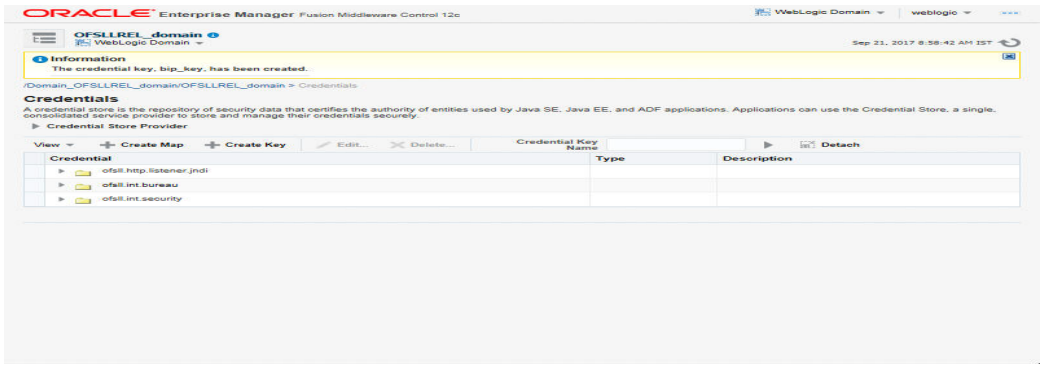


7. Click ‘Create Key’ Button.

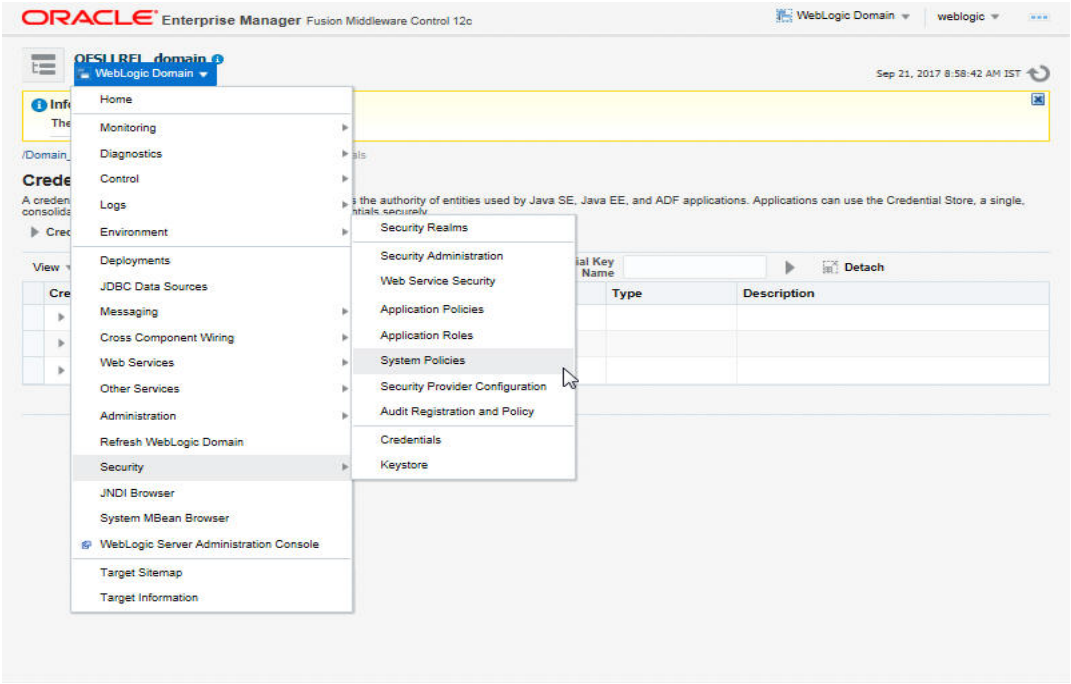
8. Enter the details as per your requirement. Specify ‘User Name’ and ‘Password’ of BI Publisher console.



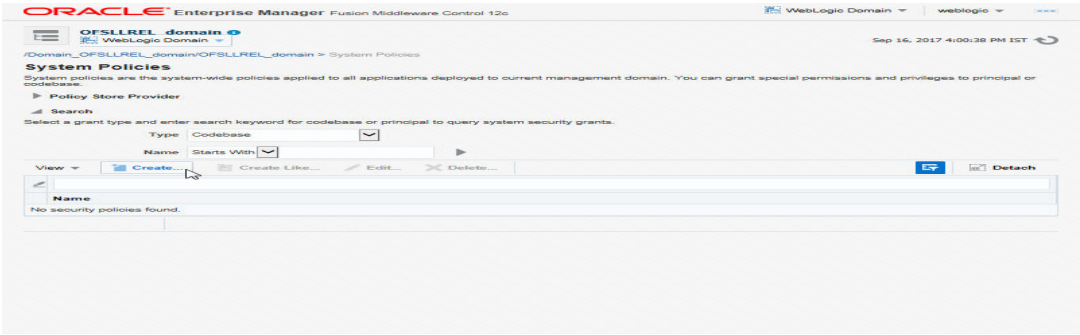
9. Click ‘OK’. The following window is displayed.



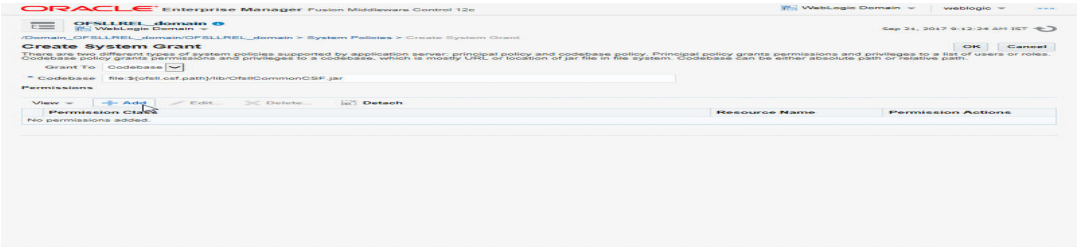
10. On the left panel, right click on the domain OFSLL_domain > Security > System Policies. The following window is displayed.



11. Click ‘Create’.

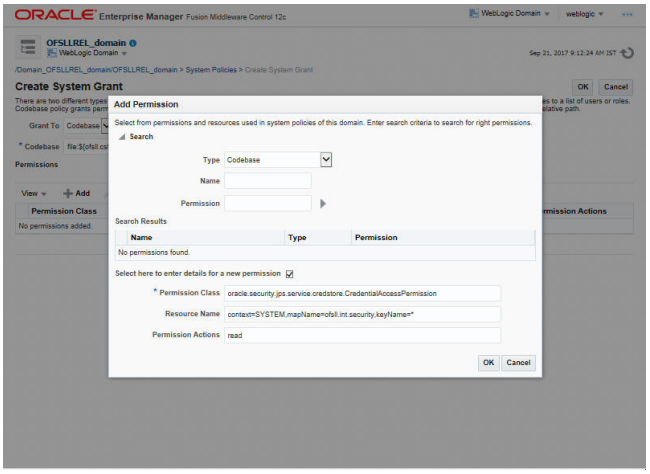


12. The following window is displayed. Enter the codebase as ‘file:${ofsll.csf.path}/lib/OfsllCommonCSF.jar’ and click ‘Add’.



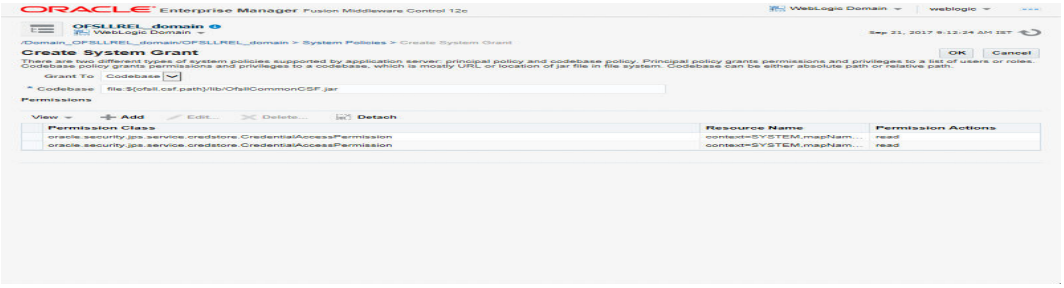
13. The following window is displayed. Select the checkbox 'Select here to enter details for a new permission' and enter the following details as the first permission class.
    - Permission Class: oracle.security.jps.service.credstore.CredentialAccessPermission
    - Resource Name: context=SYSTEM,mapName=ofsll.int.security,keyName=*

– Permission Actions: read

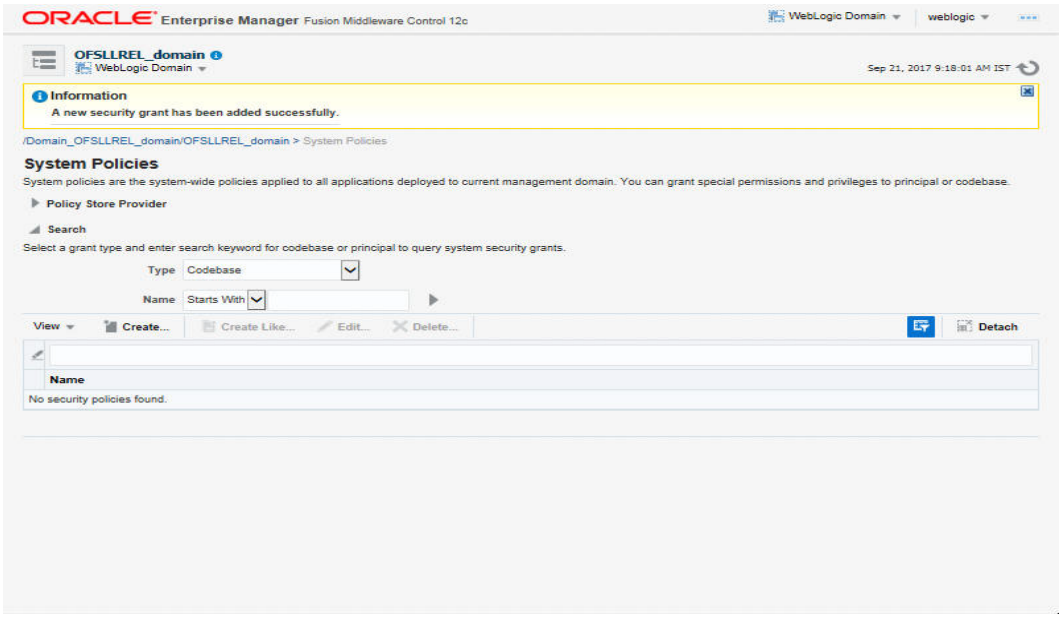


Configuring JNDI Name for http Listener

1. Similarly, click Add to add the second permission class. Select the check box 'Select here to enter details for a new permission' and enter the following details as the second permission class.
   – Permission Class: oracle.security.jps.service.credstore.CredentialAccessPermission
   – Resource Name: context=SYSTEM,mapName=ofsll.http.listener.jndi,keyName=*
   – Permission Actions: read
2. Click ‘OK’. The following window is displayed.



3. Click ‘OK’. The following window is displayed.



11. Launching Application

Verifying Successful Application Deployment and Launching Application

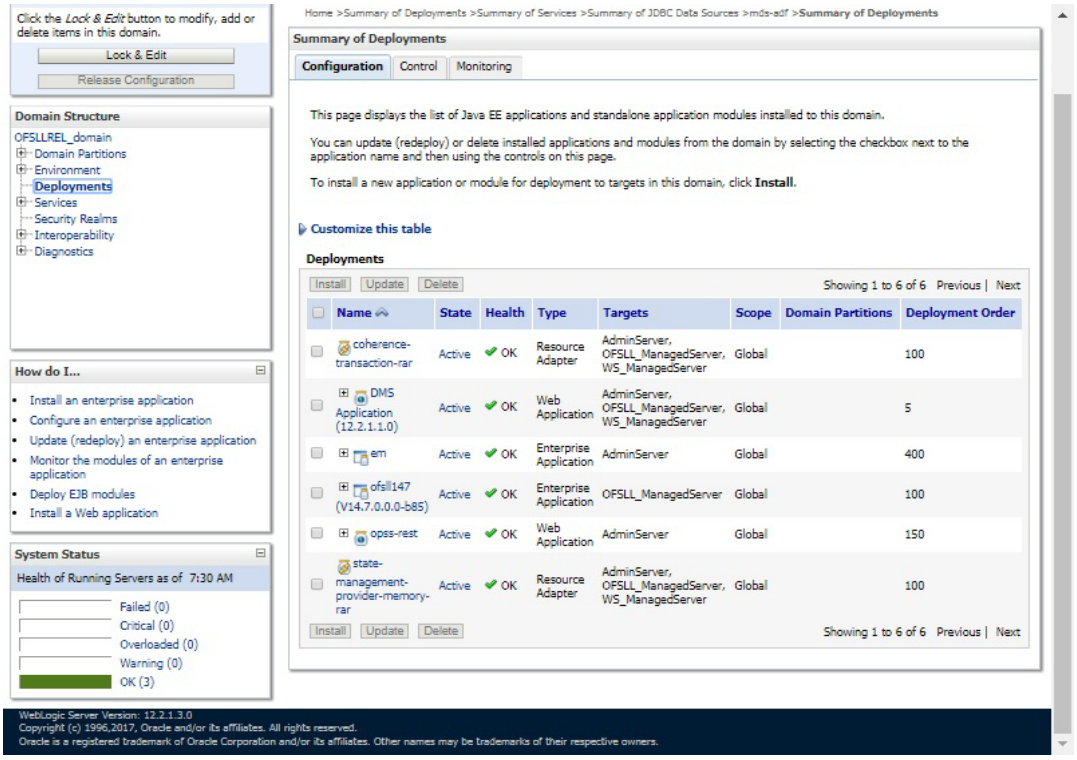
Successful Application deployment can be verified by following:

- Making sure that the state is ACTIVE and health is OK in the Weblogic.
- Access and log into the application.

After you enable SSL you can launch the application via https:\\ protocol.

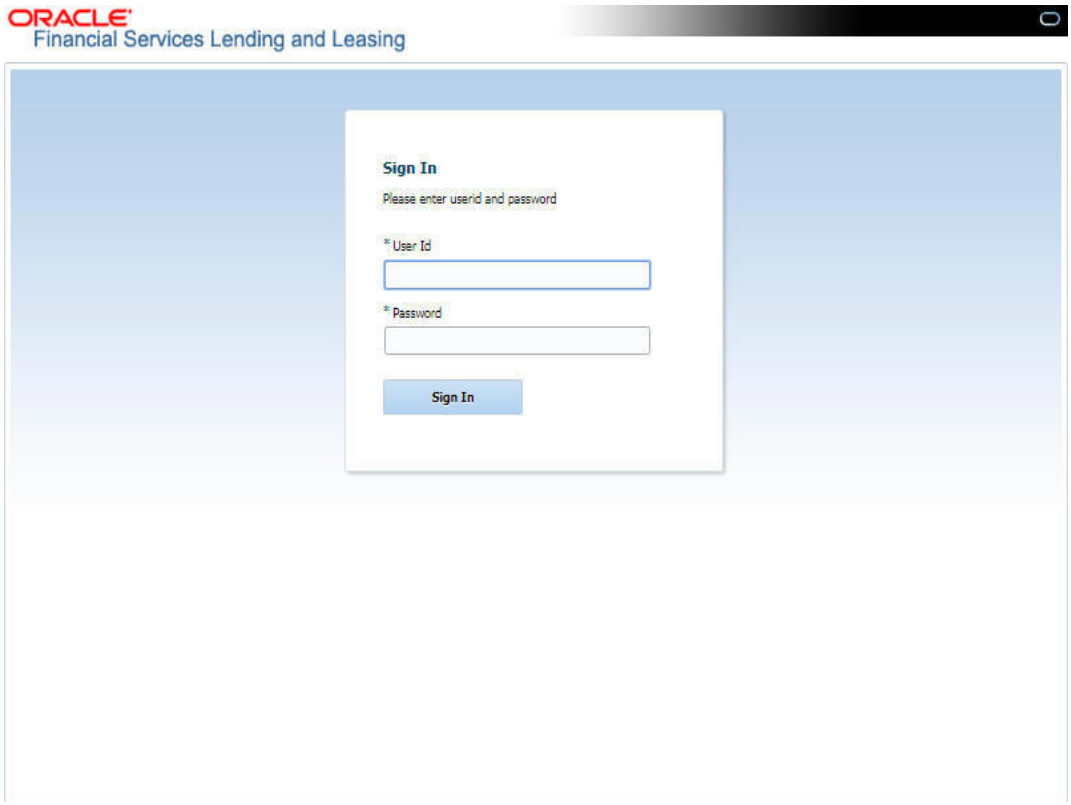
To launch application

1. Verify if the deployed OFSLL application is 'Active'.



2. The URL of the OFSLL application will be of the format - https://<hostname>:<Port>/<ContextName>/faces/pages/OfsllSignIn.jsf (Example: https://localhost:7003/ofsll/faces/pages/OfsllSignIn.jsf)

3. Login with the user credentials that was created in Users Creation.



4. After successful login, the following screen is displayed