

Application Installation Guide

# **Oracle Financial Services Lending and Leasing**

Release 14.9.0.0.0

**Part No. F27106-01**

May 2020

Application Installation Guide  
May 2020  
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>

Copyright © 2007, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

## **Send Us Your Comments**

### Oracle Financial Services Lending and Leasing User Documentation

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document. Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

Note: Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the Oracle Documentation available at [www.docs.oracle.com](http://www.docs.oracle.com) which contains the most current Documentation Library plus all documents revised or released recently.

Send your comments using the electronic mail address: [financialservices\\_ww@oracle.com](mailto:financialservices_ww@oracle.com)

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at [www.oracle.com](http://www.oracle.com).

---

# Table of Contents

<b>1. Preface</b>	<b>1-1</b>
1.1 Prerequisites	1-1
1.2 Audience	1-2
1.3 Conventions Used	1-2
<b>2. Installing Software</b>	<b>2-1</b>
2.1 Installing Oracle WebLogic Server 12c	2-1
<b>3. Creating Domains, Repositories, Data Sources</b>	<b>3-1</b>
3.1 Creating Schemas using Repository Creation Utility	3-1
3.2 Creating Domain and Servers	3-9
3.3 Creating Metadata Repository	3-21
3.4 Creating Data Source	3-24
3.5 Creating SQL Authentication Provider	3-30
3.6 Creating User Groups and Users	3-36
3.6.1 <i>Creating Users</i>	3-36
3.6.2 <i>Creating User Groups</i>	3-38
3.6.3 <i>Assigning Users to Groups</i>	3-39
3.6.4 <i>Resetting password via weblogic console</i>	3-39
3.7 Implementing JMX Policy for Change Password	3-40
<b>4. Configuring Policies</b>	<b>4-1</b>
4.1 Configuring Password Policy for SQL Authenticator	4-1
4.2 Configuring User Lockout Policy	4-2
<b>5. Deploying Application</b>	<b>5-1</b>
5.1 Deploying Application	5-1
<b>6. Enabling SSL</b>	<b>6-1</b>
<b>7. Mapping Enterprise Group with Application Role</b>	<b>7-1</b>
<b>8. Configuring JNDI name for HTTP Listener</b>	<b>8-1</b>
<b>9. Configure AQ-JMS Bridge</b>	<b>9-1</b>
9.1 Create Data Sources for AQ-JMS Bridge	9-1
9.2 Configure MDB Flow	9-7
9.3 AQ-JMS Topic Setup	9-13
9.3.1 <i>Create AQ-JMS Topic Bridge</i>	9-14
9.4 JMS Queue Configuration	9-17
9.4.1 <i>Create JMS Server</i>	9-18
9.4.2 <i>Create JMS Module</i>	9-20
9.4.3 <i>Subdeployment</i>	9-21
9.4.4 <i>Create JMS Connection Factory</i>	9-23
9.4.5 <i>Create JMS Queue</i>	9-25
9.5 Configure External Client Certificates	9-27
9.6 Create Credentials and System Policies	9-32
9.7 Deploy MDB EJB	9-38
<b>10. Configuring Oracle Analytics Publisher for Application</b>	<b>10-1</b>
<b>11. Launching Application</b>	<b>11-1</b>

---

# 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, OAS (Oracle Analytic Server) 5.5.0.

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 Analytics Publisher for Application](#)
- [Launching Application](#)

## 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 jdk1.8.0\_241 or above (<https://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>)
  2. Oracle WebLogic Server 12c Version 12.2.1.4.0 (<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.

---

### 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

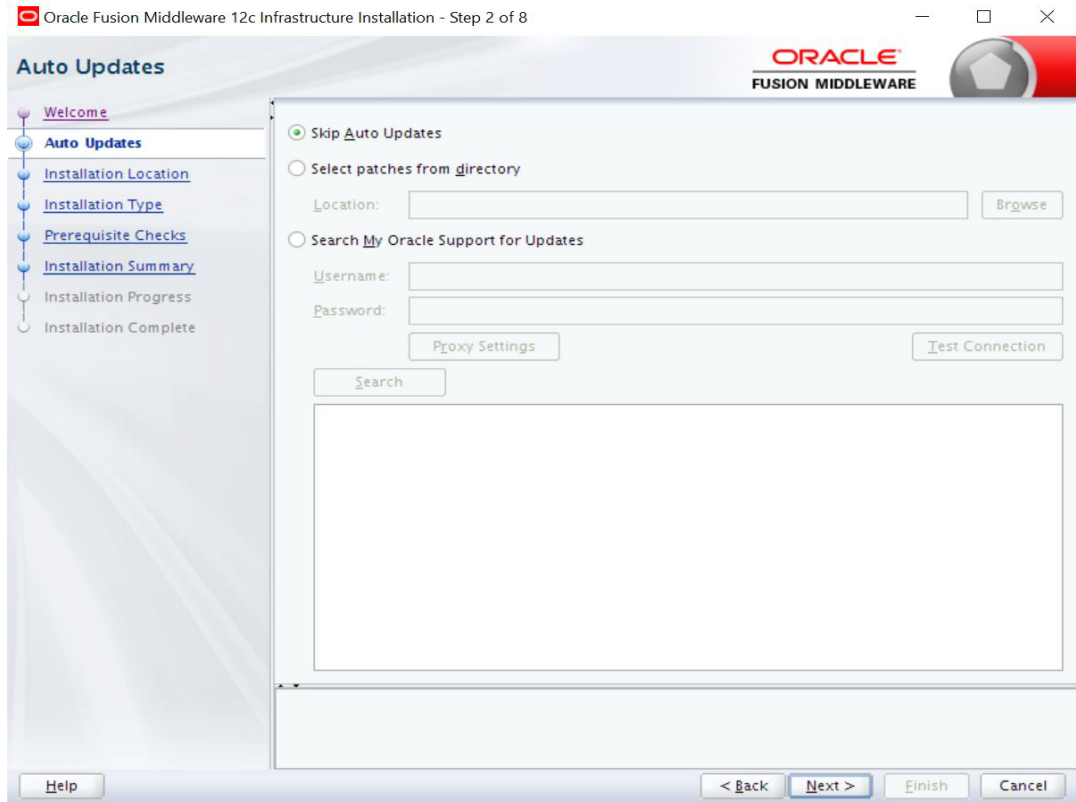
### 2.1 Installing Oracle WebLogic Server 12c

#### To install using generic Weblogic installer

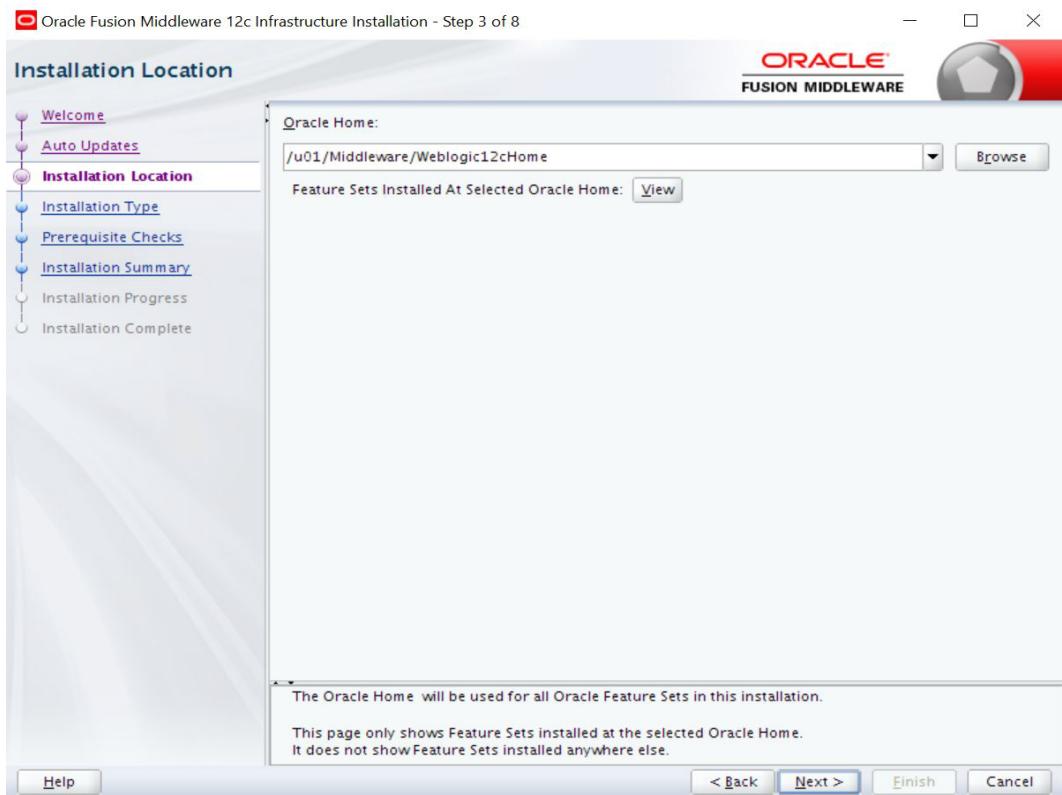
1. Run the command `> java -jar fmw_12.2.1.4.0_infrastructure.jar`
2. Welcome screen is displayed as shown below. Click Next.



3. The following window is displayed.



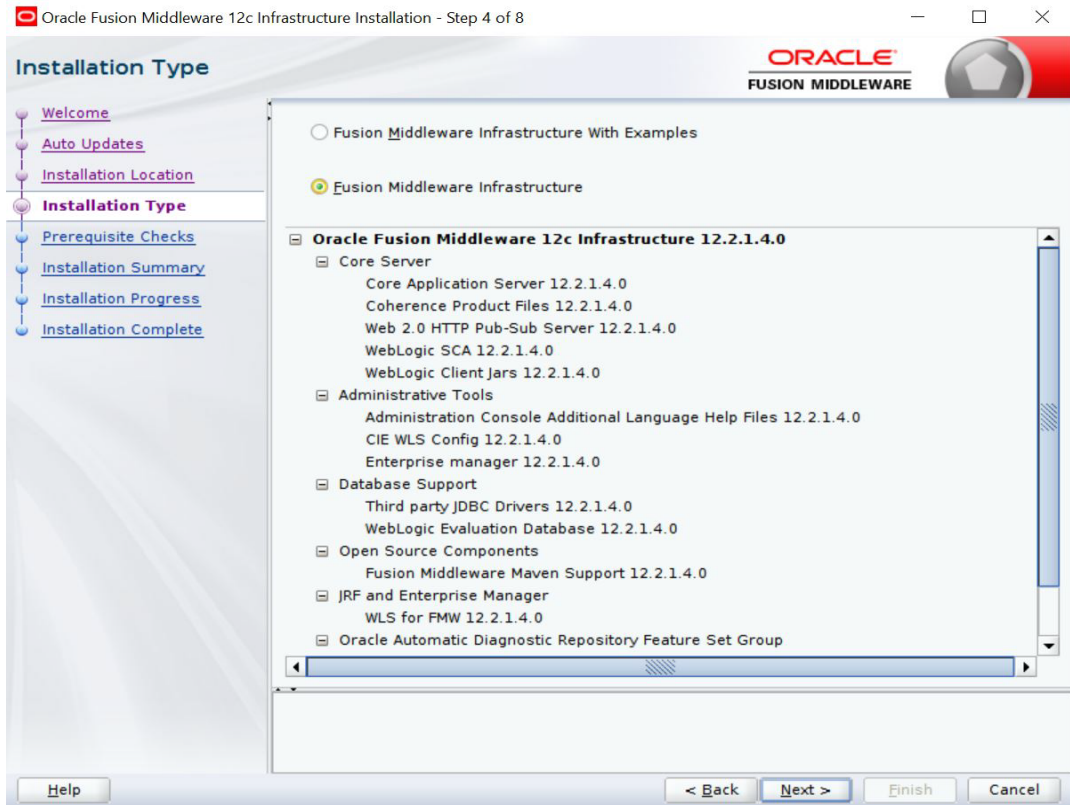
4. Select 'Skip Auto Updates' and Click 'Next'.



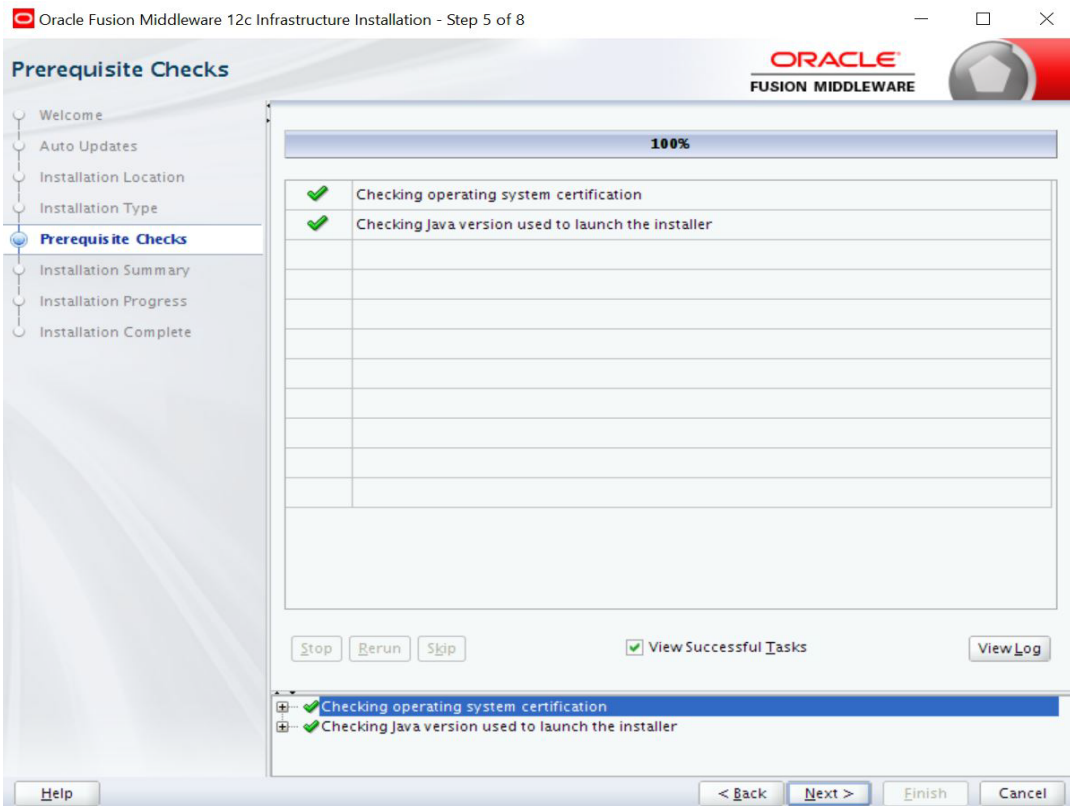
5. Specify the path for Middleware Home Directory.



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



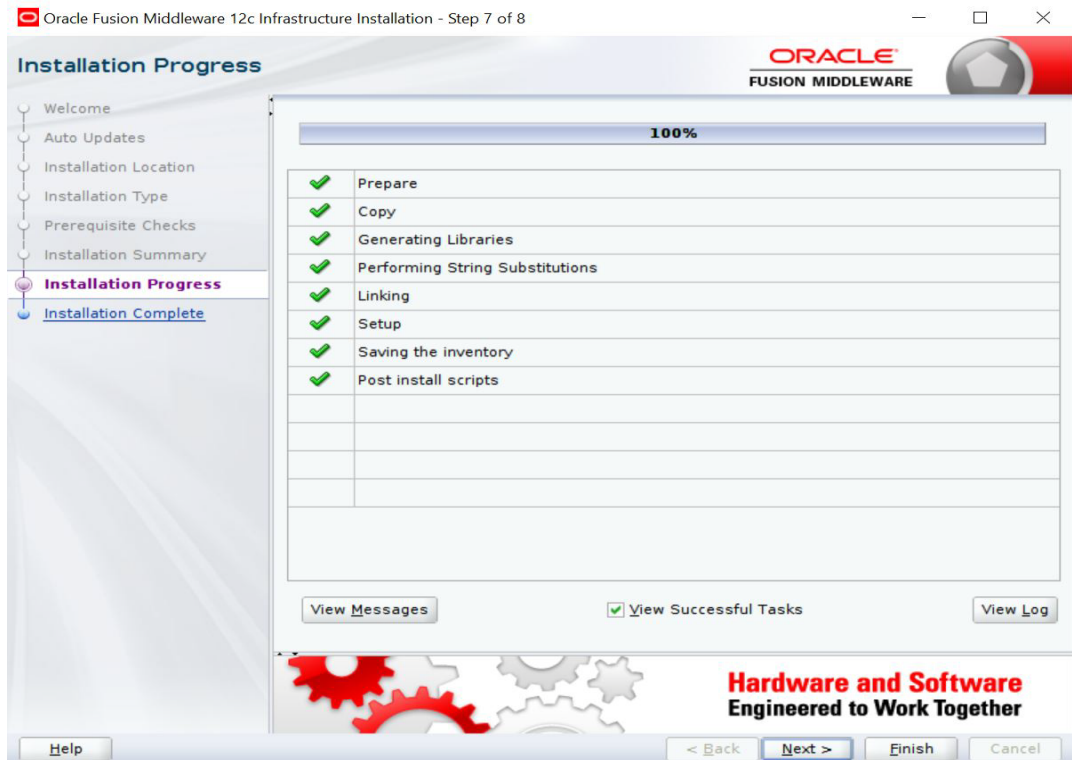
7. Select the option 'Fusion Middleware Infrastructure'. Click 'Next'.



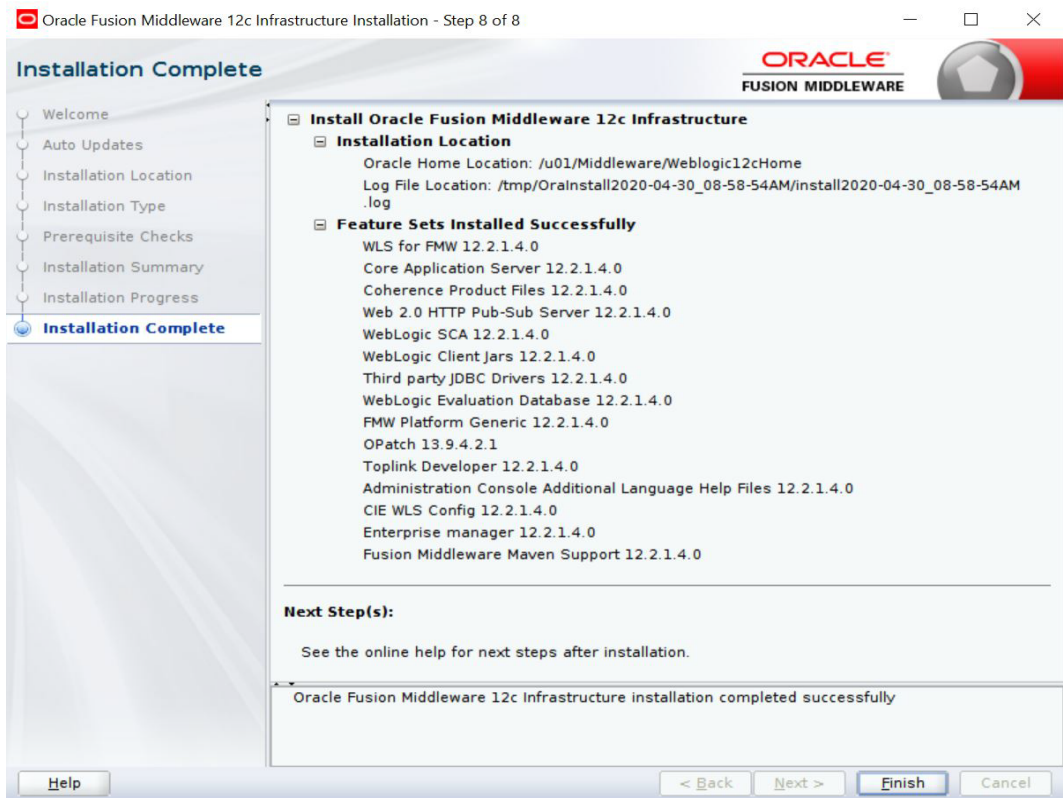
8. Click 'Next'. The following window is displayed.



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



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



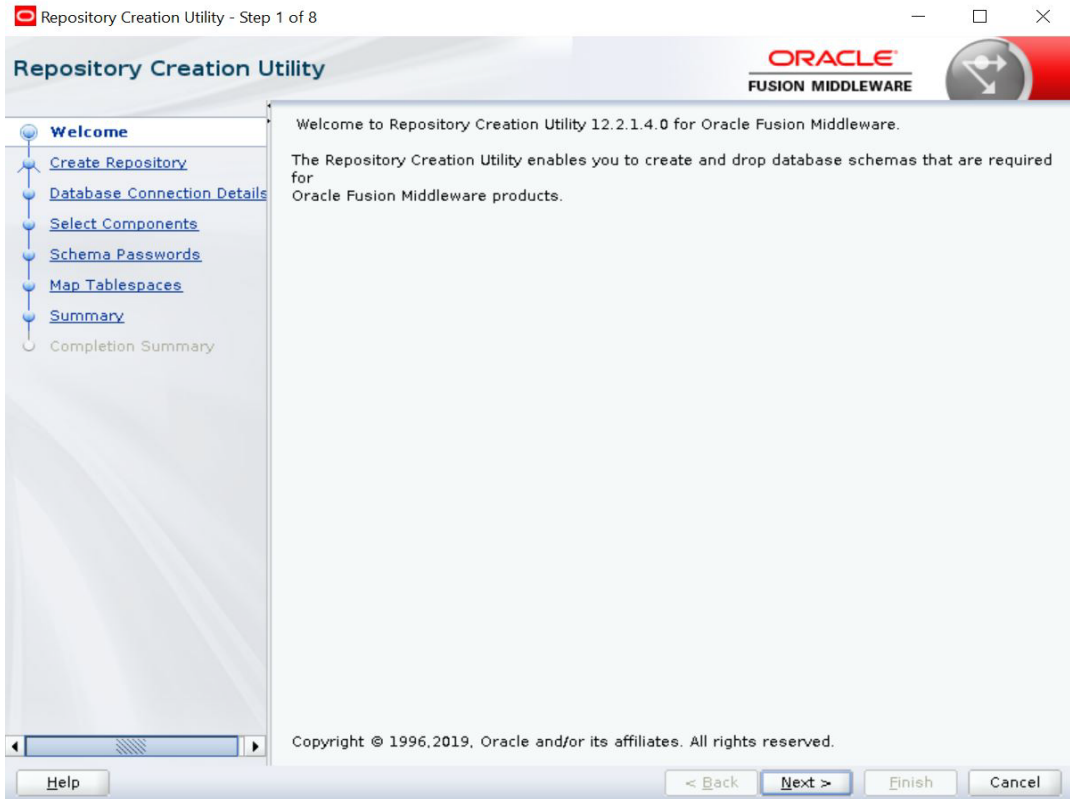
11. Click 'Finish' to close the window.

---

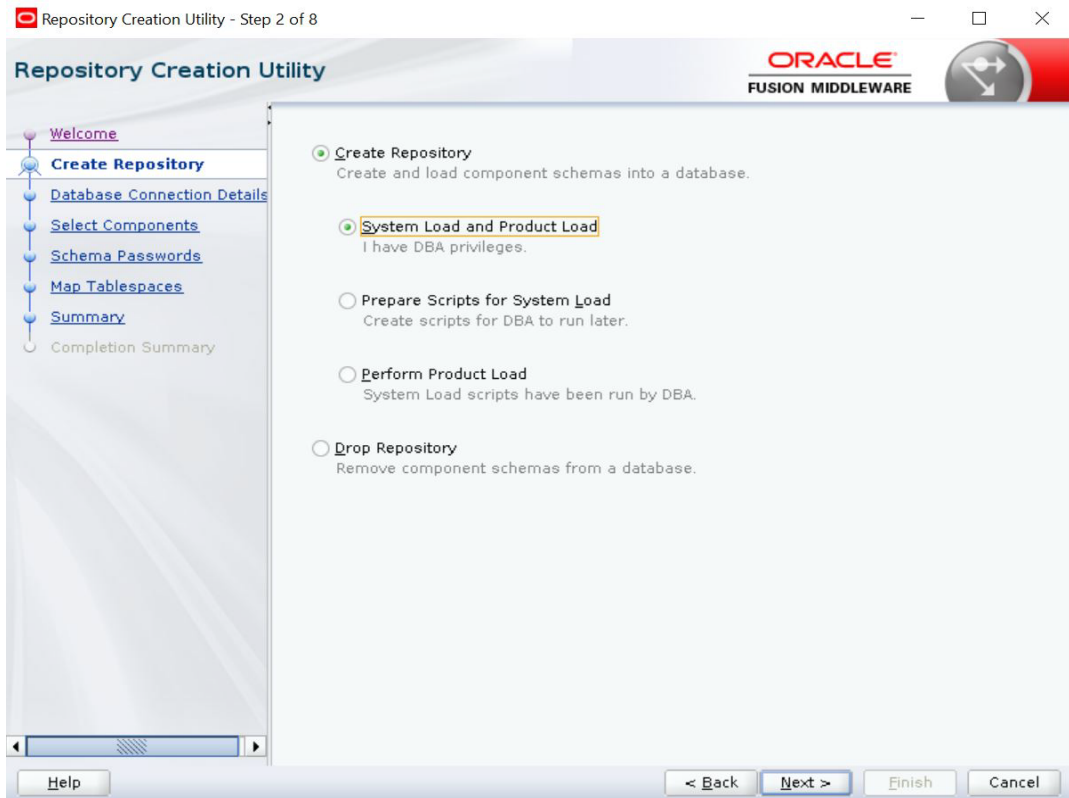
## 3. Creating Domains, Repositories, Data Sources

### 3.1 Creating Schemas using Repository Creation Utility

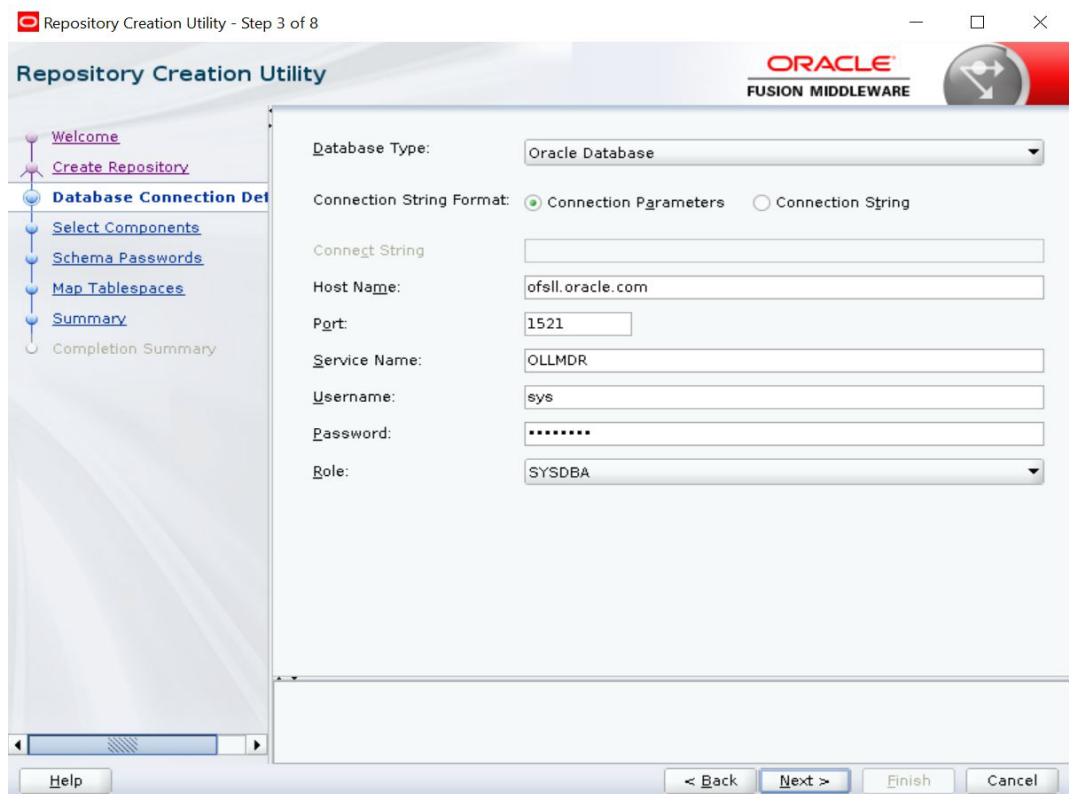
1. Open command prompt on Unix and browse to <WL\_HOME>/oracle\_common/bin and run ./rcu. The following window is displayed.



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.

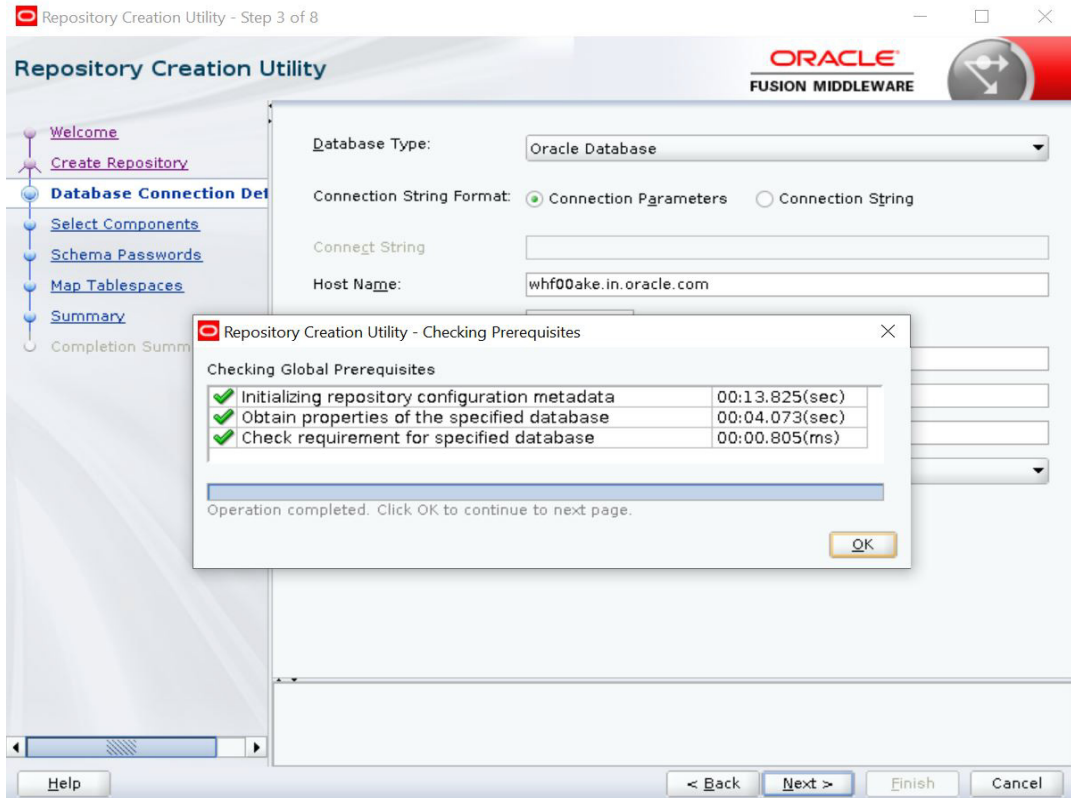
---

**Note**

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

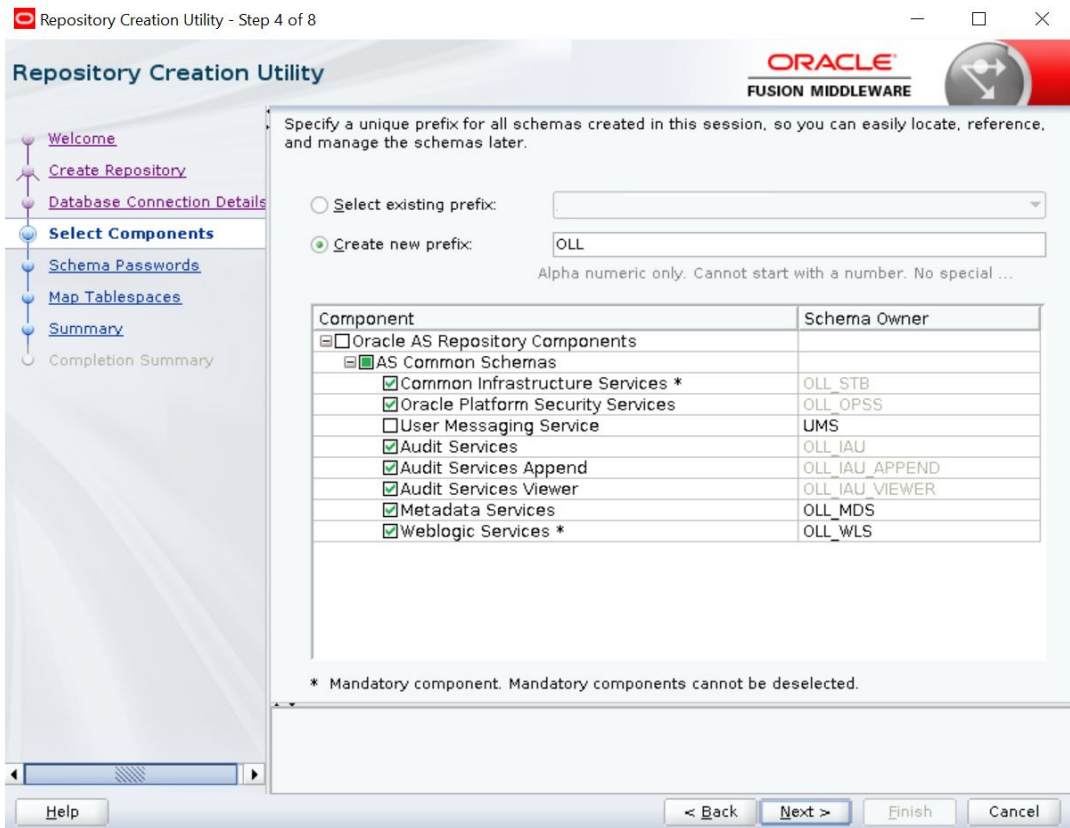
---

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



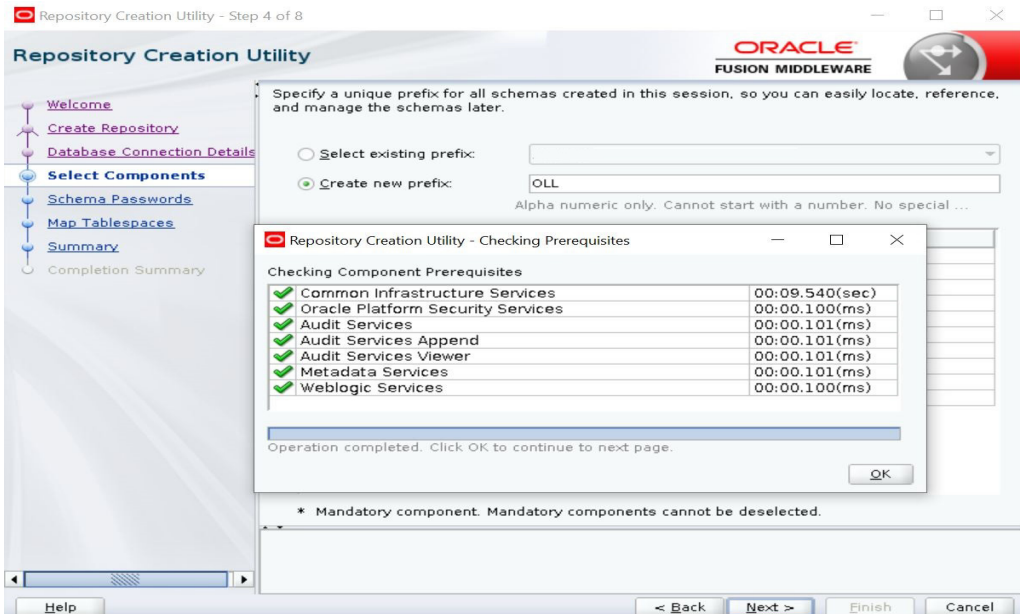
6. Click 'OK' in the confirmation dialog.

7. Click 'Next' the following window is displayed.

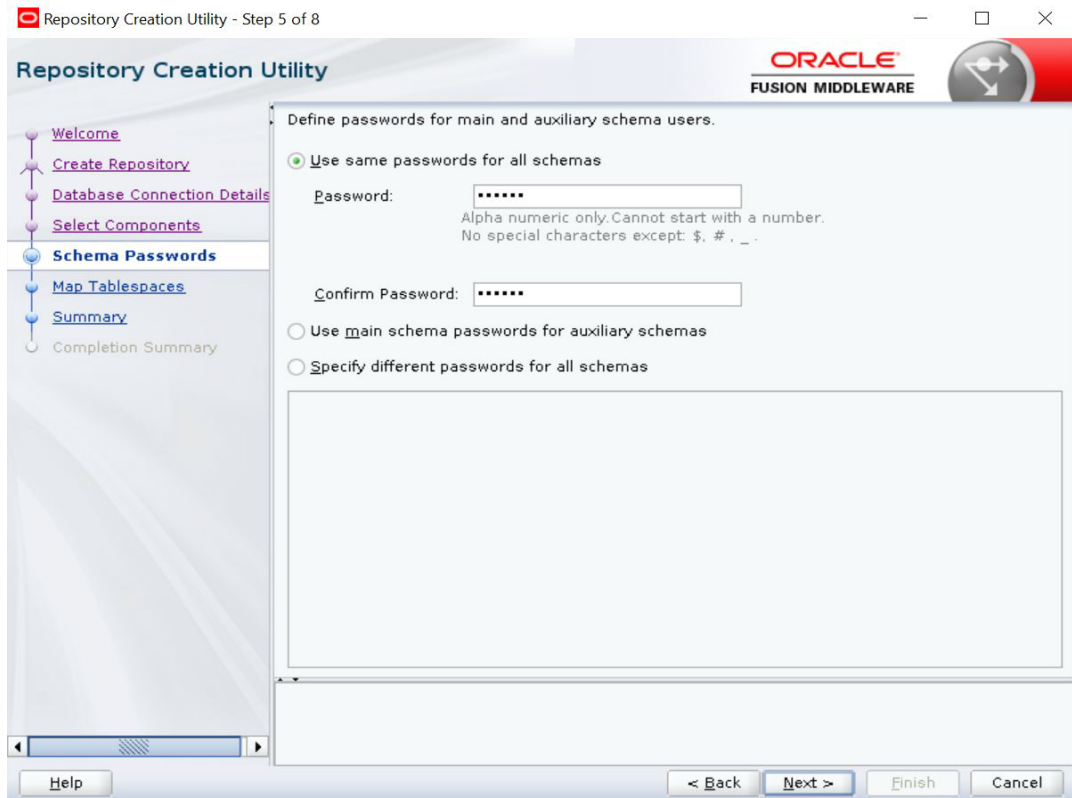


8. Select 'Create new Prefix' option and specify the value. For example, OLL.

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.

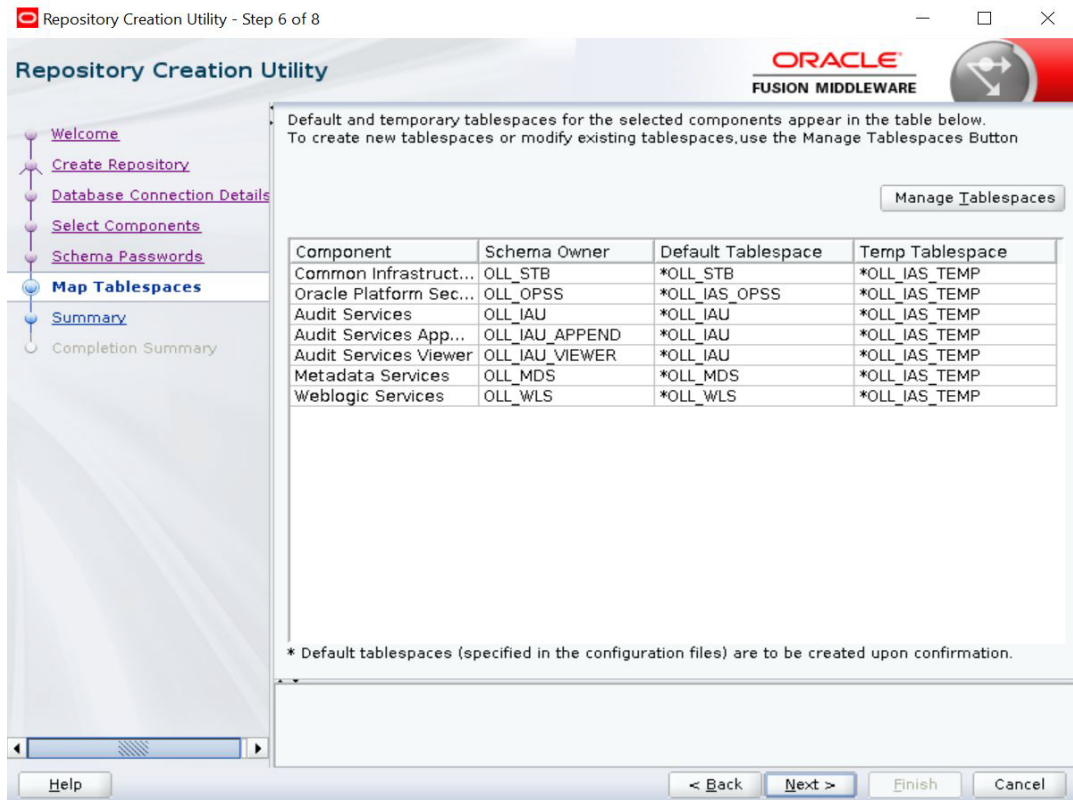


11. You can select one of the following:

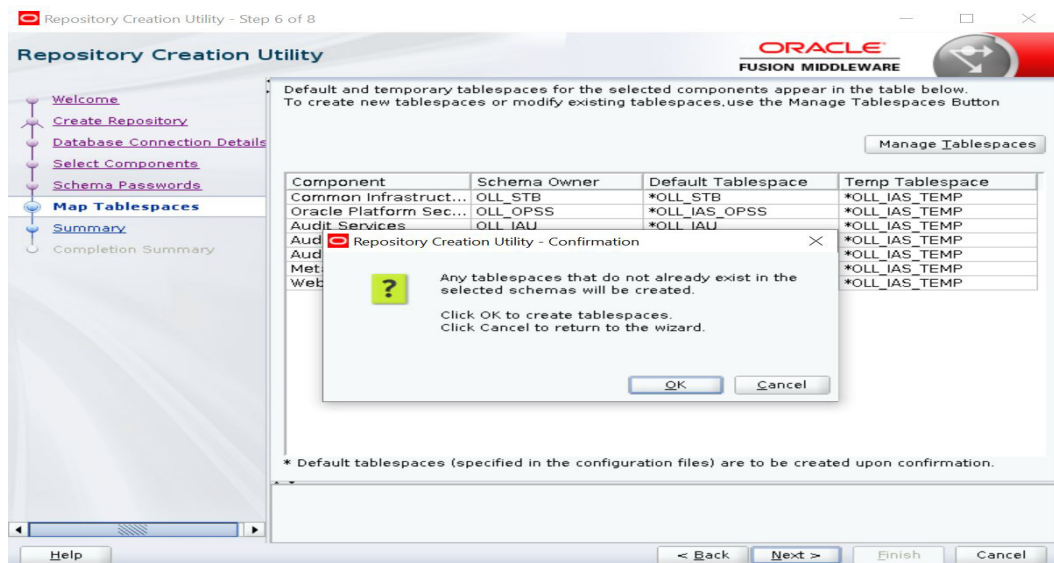
- Select 'Use same password for all schemas' and specify the password.
- Select 'Specify different passwords for all schemas' and specify Schema Passwords for each schema.



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

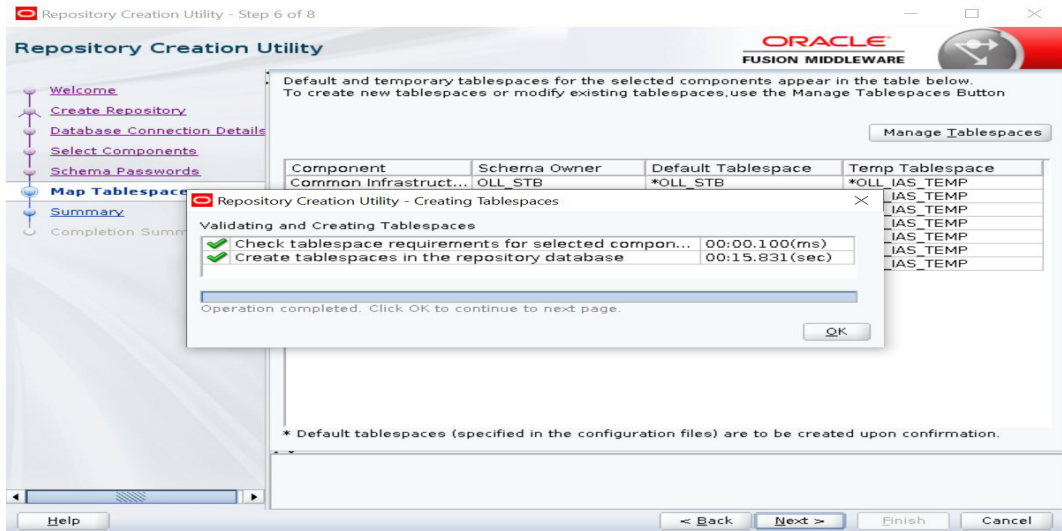


13. Click 'Next'. The following window is displayed.

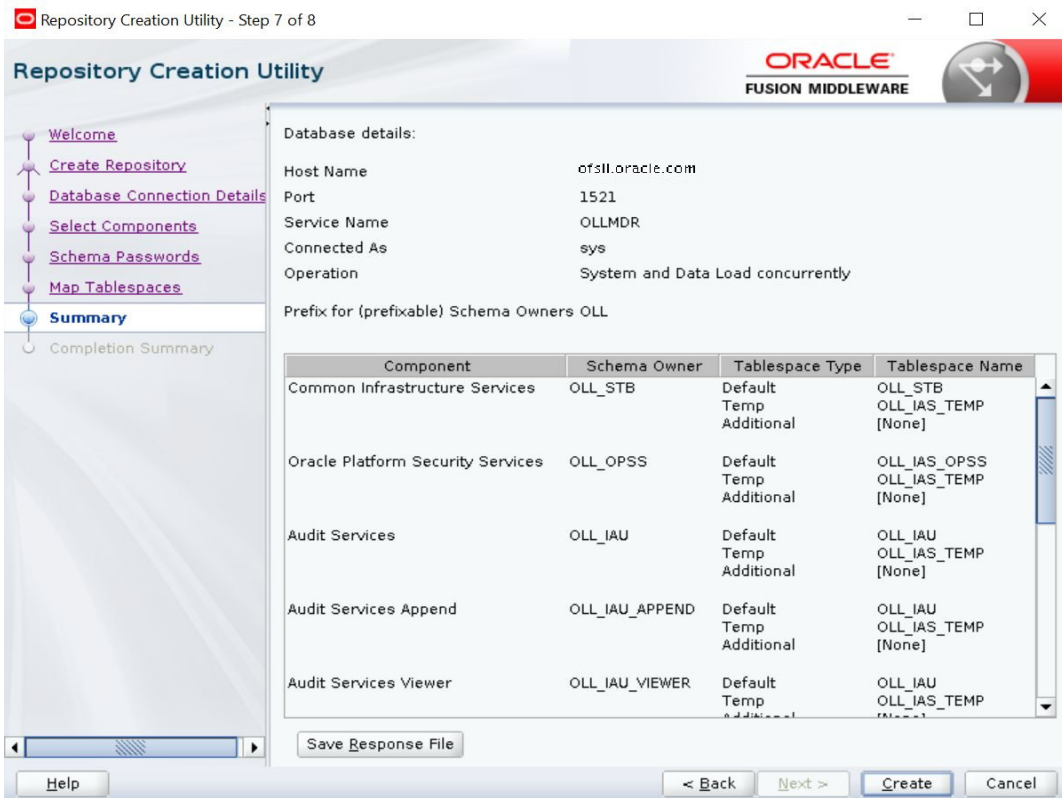


14. Click 'OK' in the confirmation dialog.

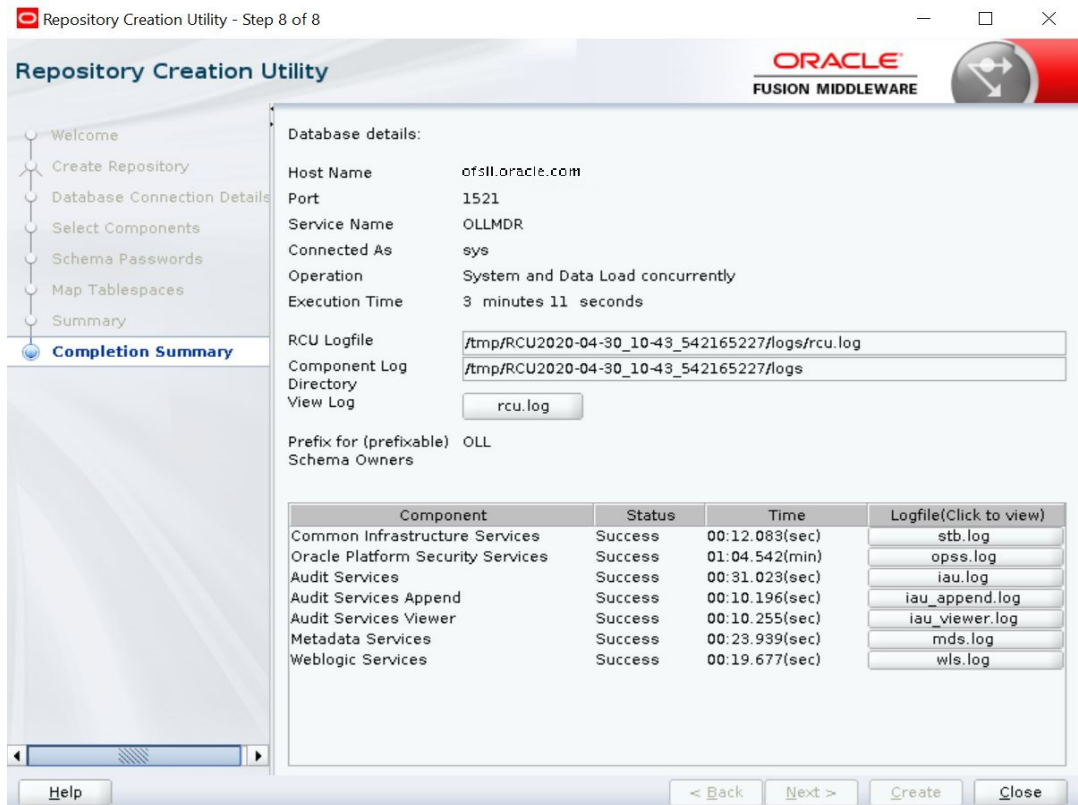
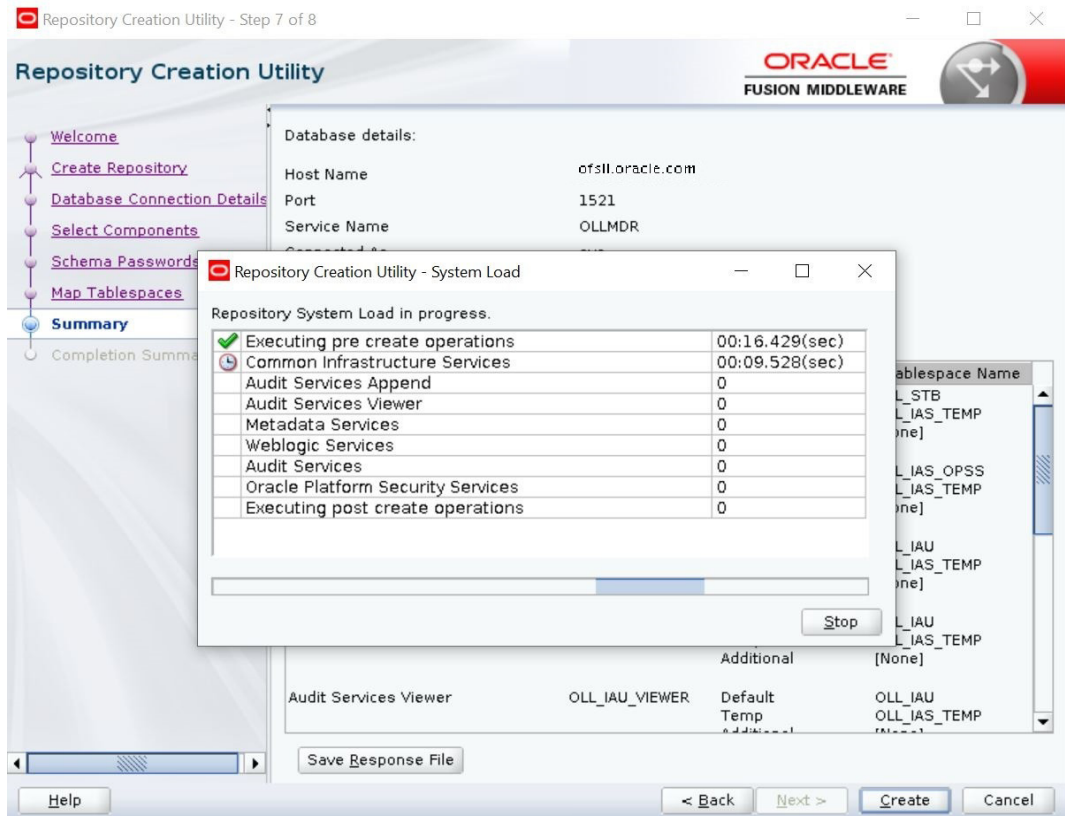
15. Click 'Next'. The following window is displayed.



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



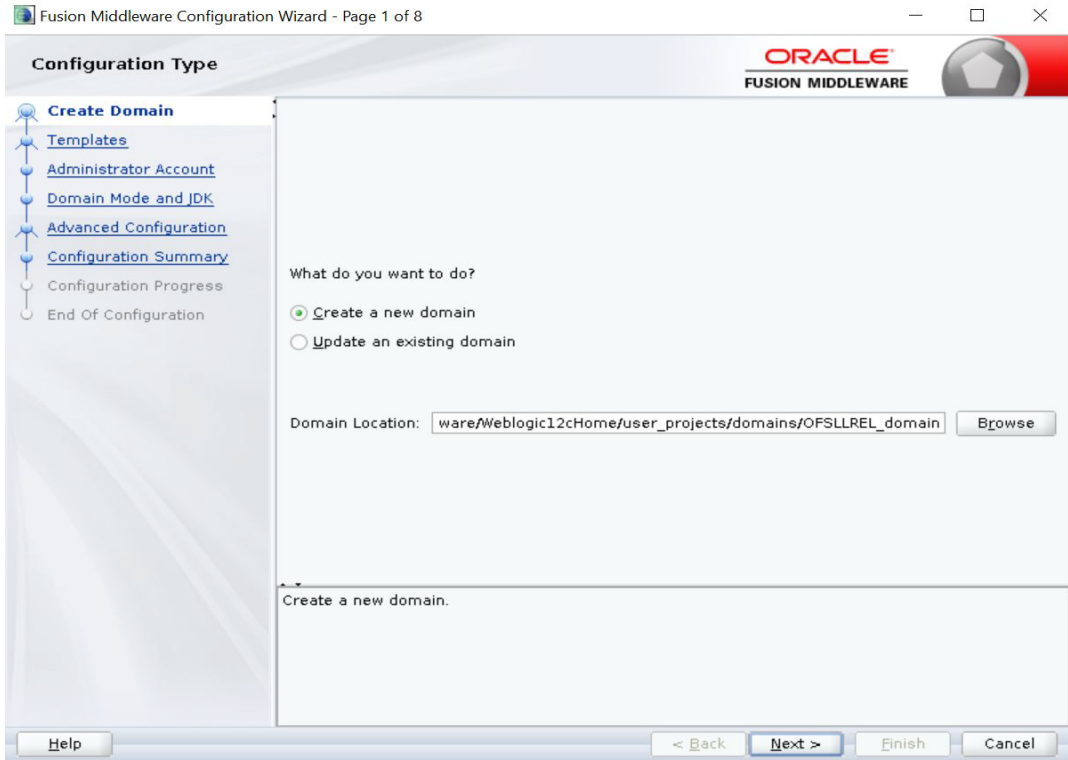
17. Click 'Create'. The following windows are displayed.



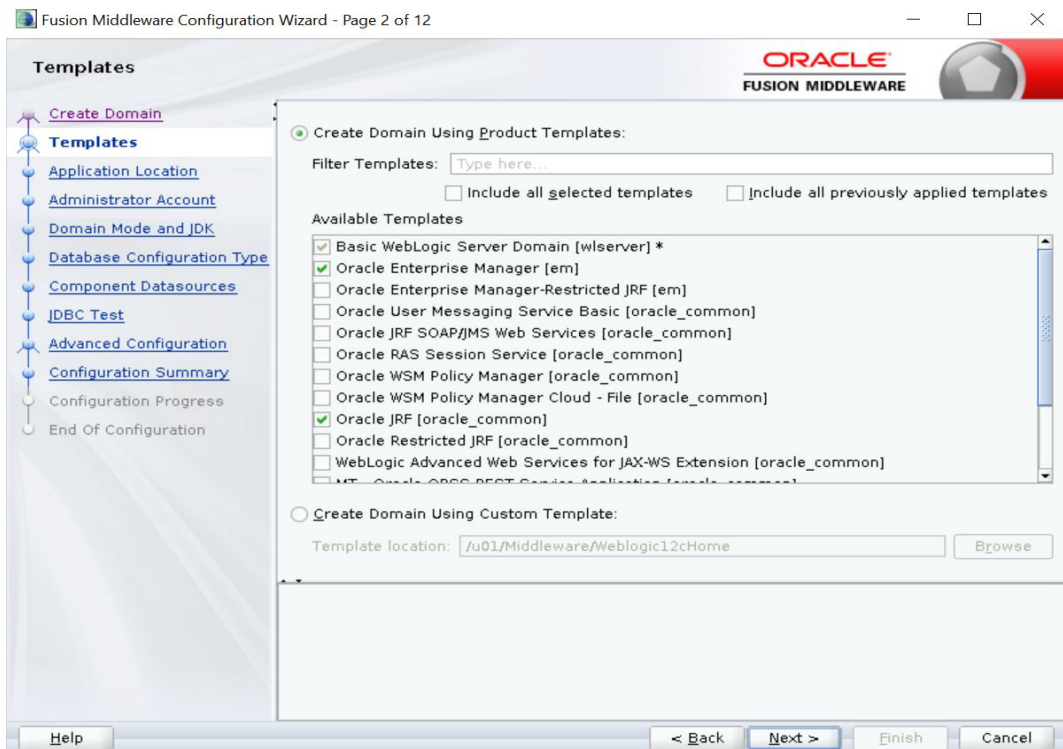
18. Click 'Close' to close the window.

## 3.2 Creating Domain and Servers

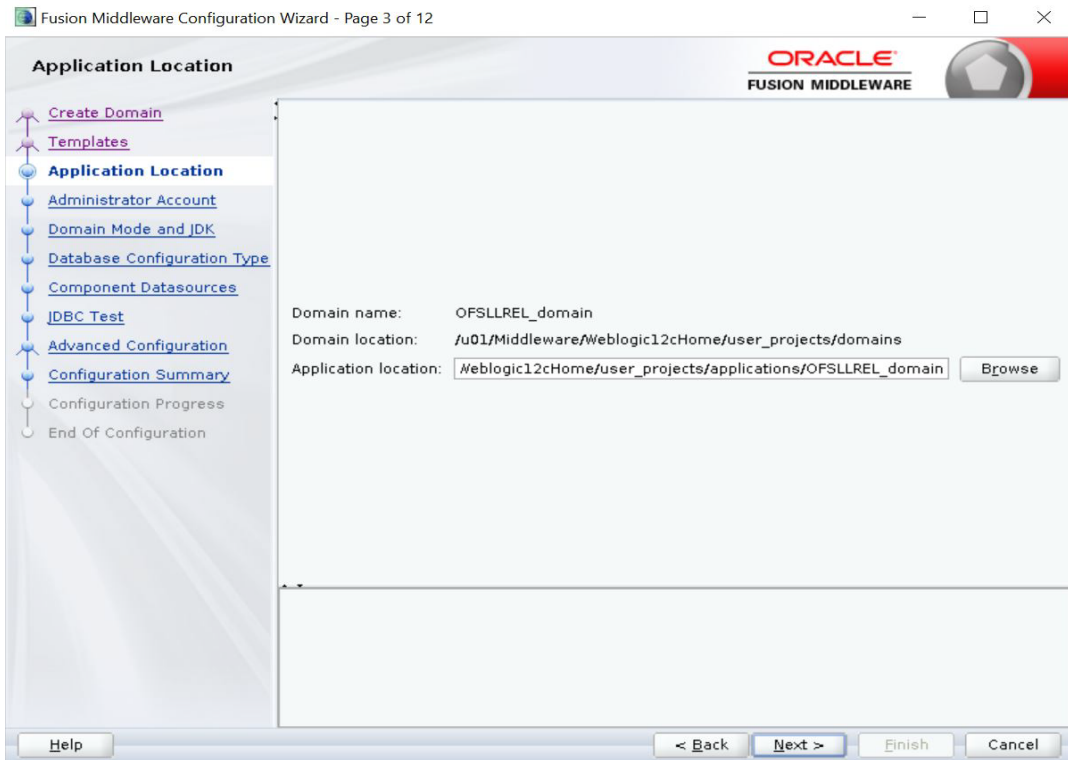
1. In Unix/Linux machine, once the Oracle WebLogic Server is installed, navigate to the following path - <WL\_HOME>/oracle\_common/common/bin.
2. In Unix, run 'config.sh'



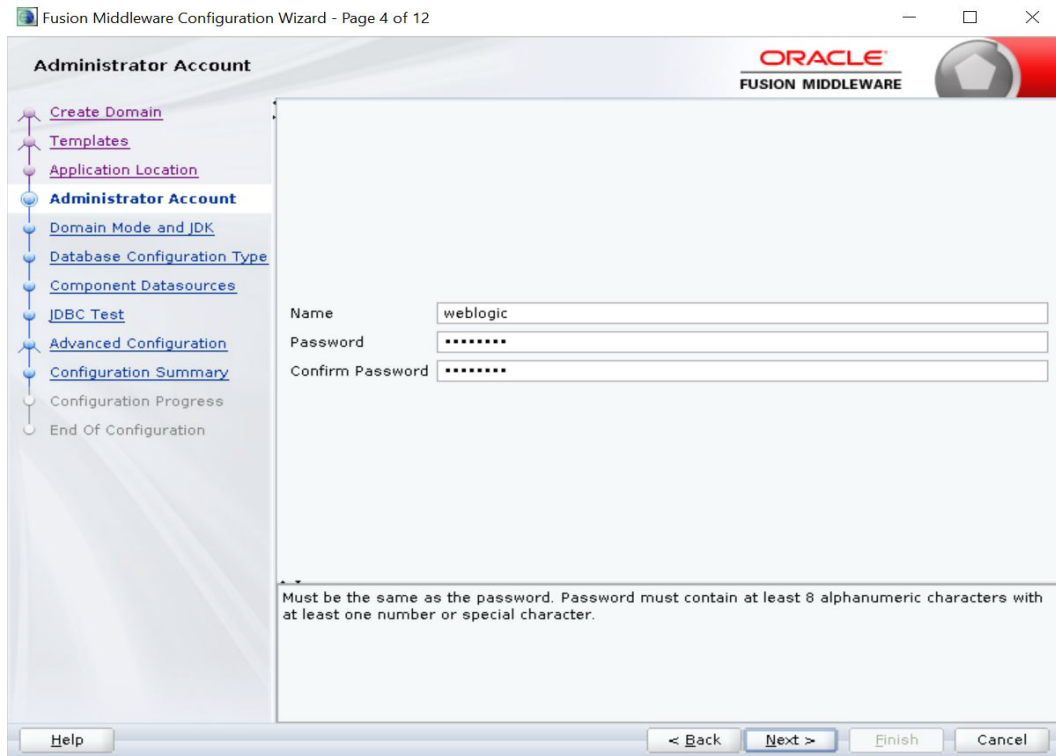
3. Select 'Create a new domain' and specify the Domain Location.
4. Click 'Next'. The following window is displayed.



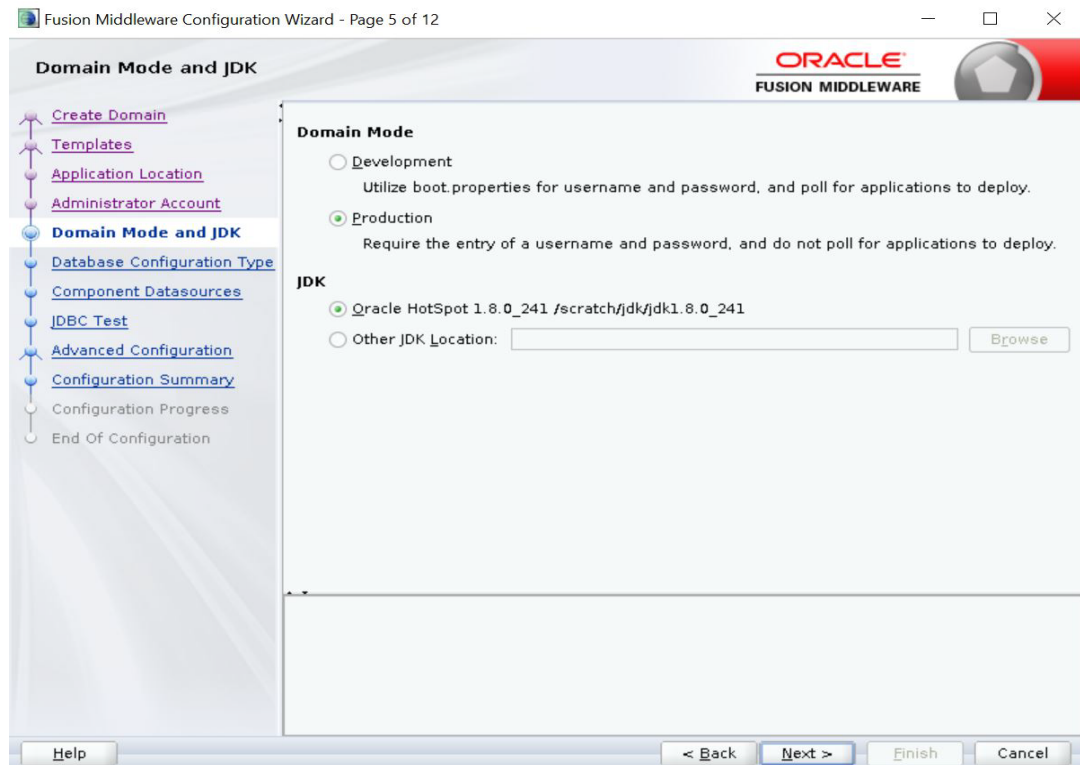
5. Select the option 'Create Domain Using Product Templates' in the list of available templates and select 'Oracle Enterprise Manager - 12.2.1.3.0 [em]'. On selection, the following options are auto-selected:
  - Oracle JRF - 12.2.1.3.0 [oracle\_common]
  - Weblogic coherence cluster Extension-12.2.1.3.0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



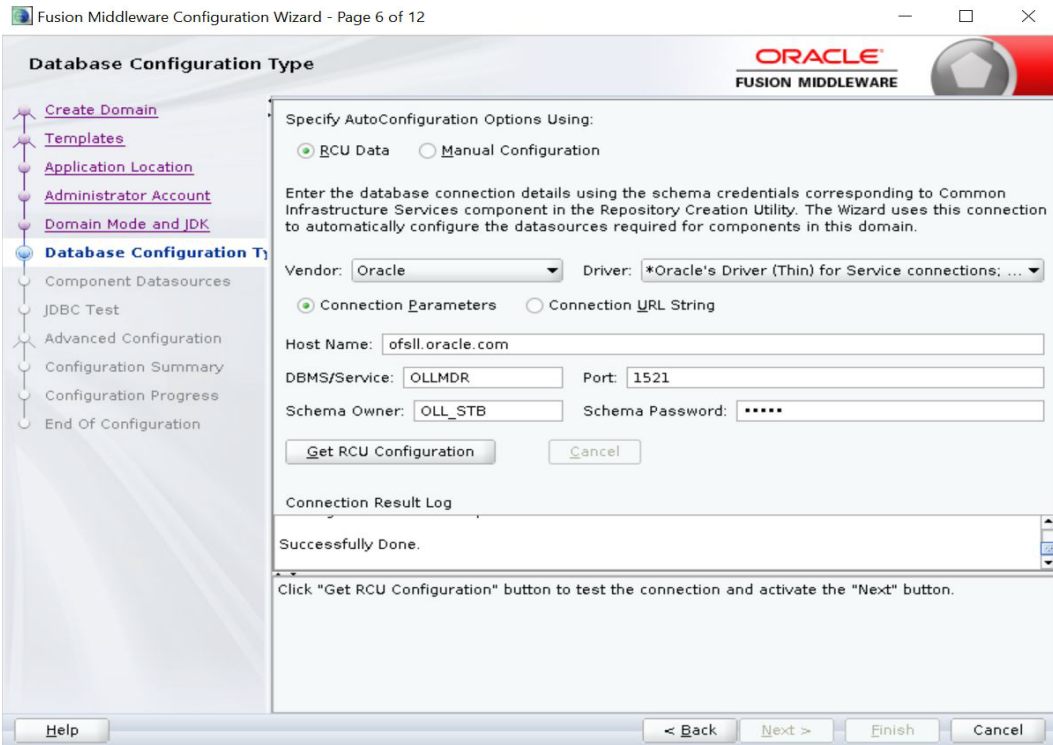
- Specify the Domain Name in the 'Application location' field. You can click browse to directly select the path (if required). Click 'Next'. The following window is displayed.



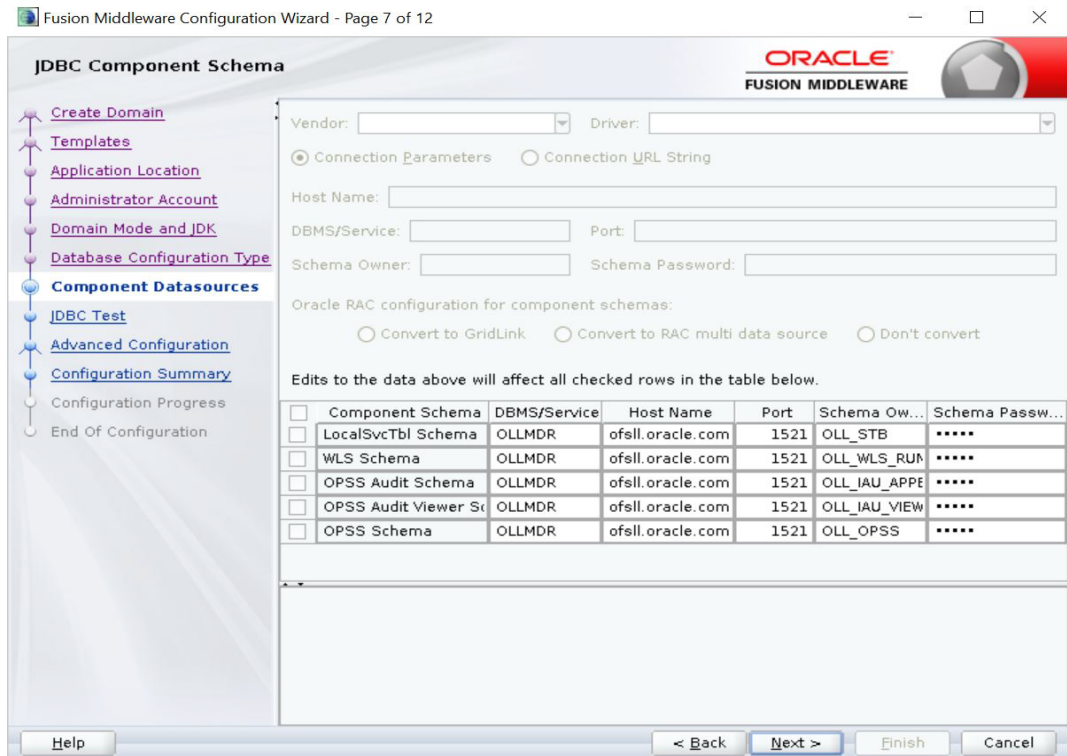
- Enter credentials for the following:
  - Name
  - Password
  - Confirm Password
- Click 'Next'. The following window is displayed.



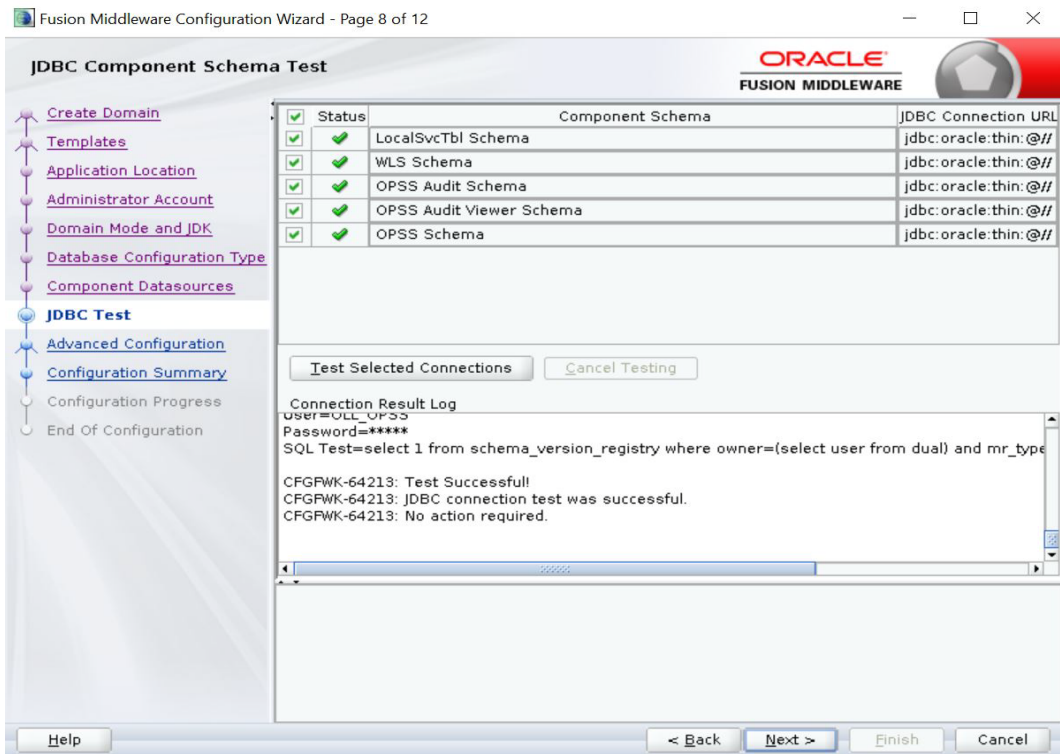
- Select the Domain Mode as 'Production' and 'JDK' from Available JDKs. You can also select any other JDK by selecting 'Other JDK Location' option. Click 'Next'. The following window is displayed.



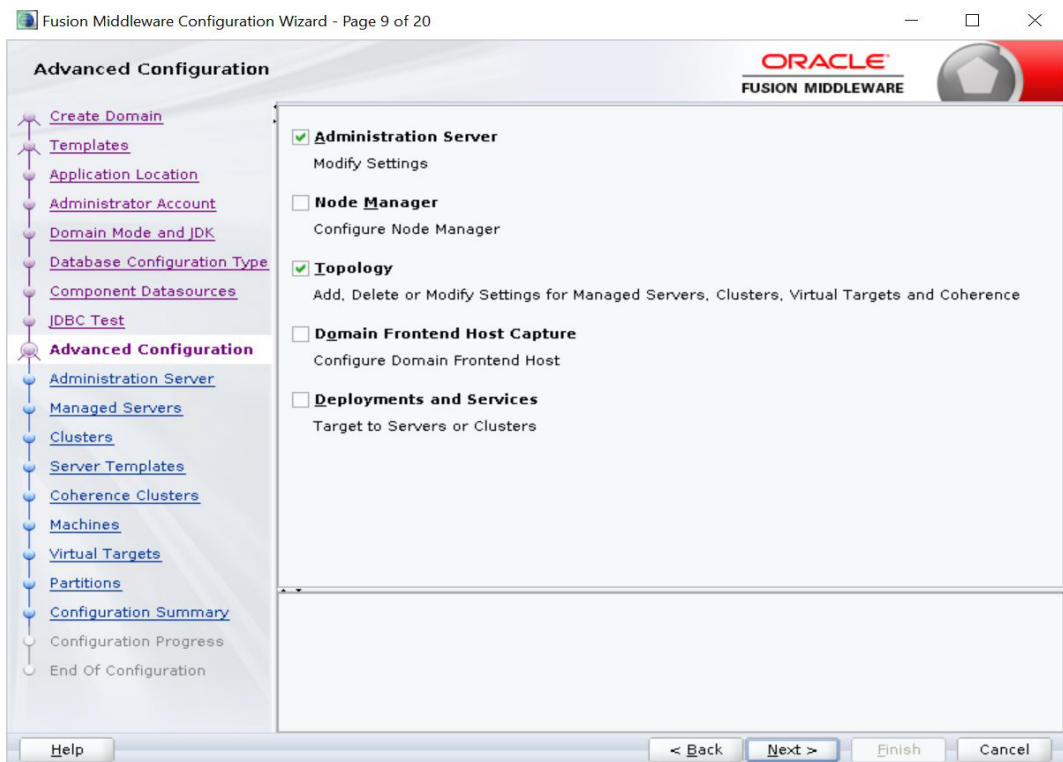
- Specify the RCU data and click on 'Get RCU Configuration'. The following window is displayed.



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



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

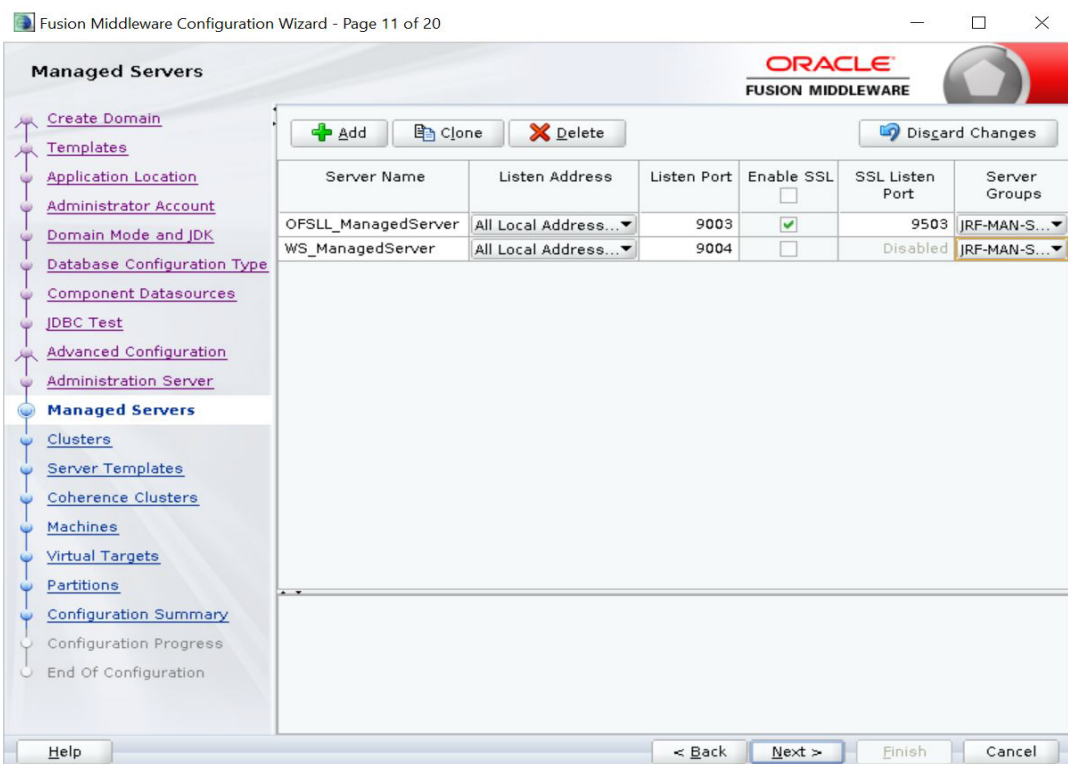




- Select 'Administration Server' and 'Topology' and click 'Next'. The following window is displayed.



- Enter Administration 'Server Name' and 'Listen Port' details. Click 'Next'. The following window is displayed.



- Click 'Add' button to create 'ManagedServer'.
- 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.*

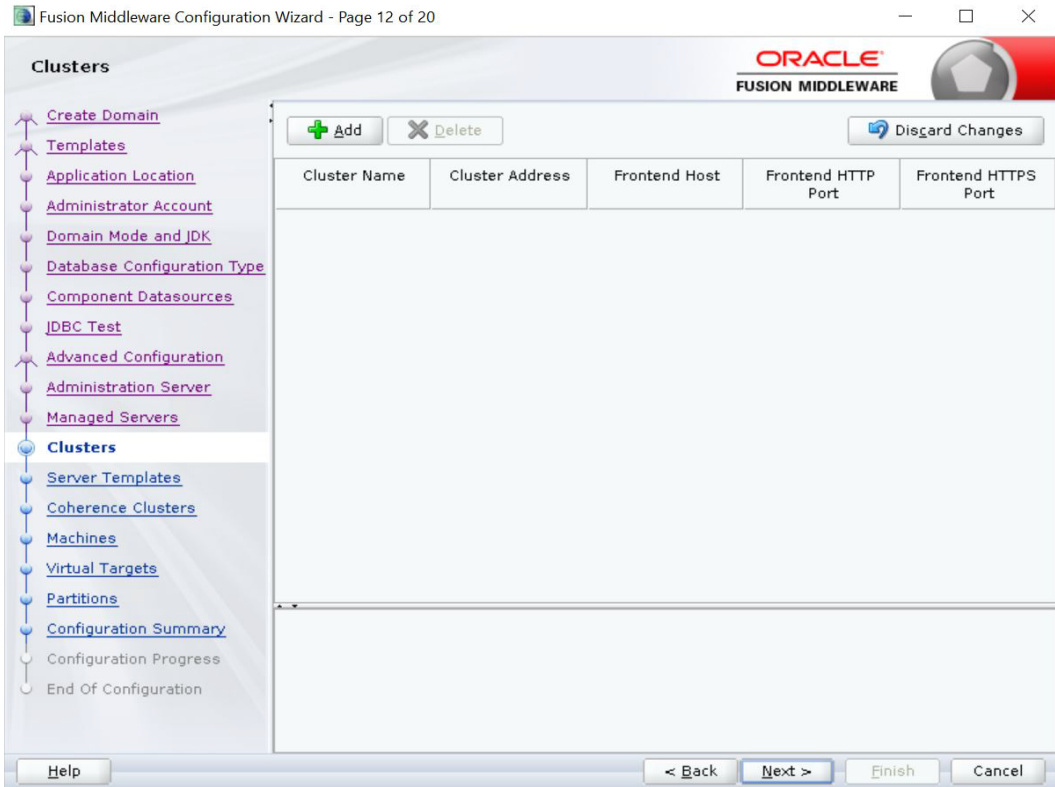
---

**Note**

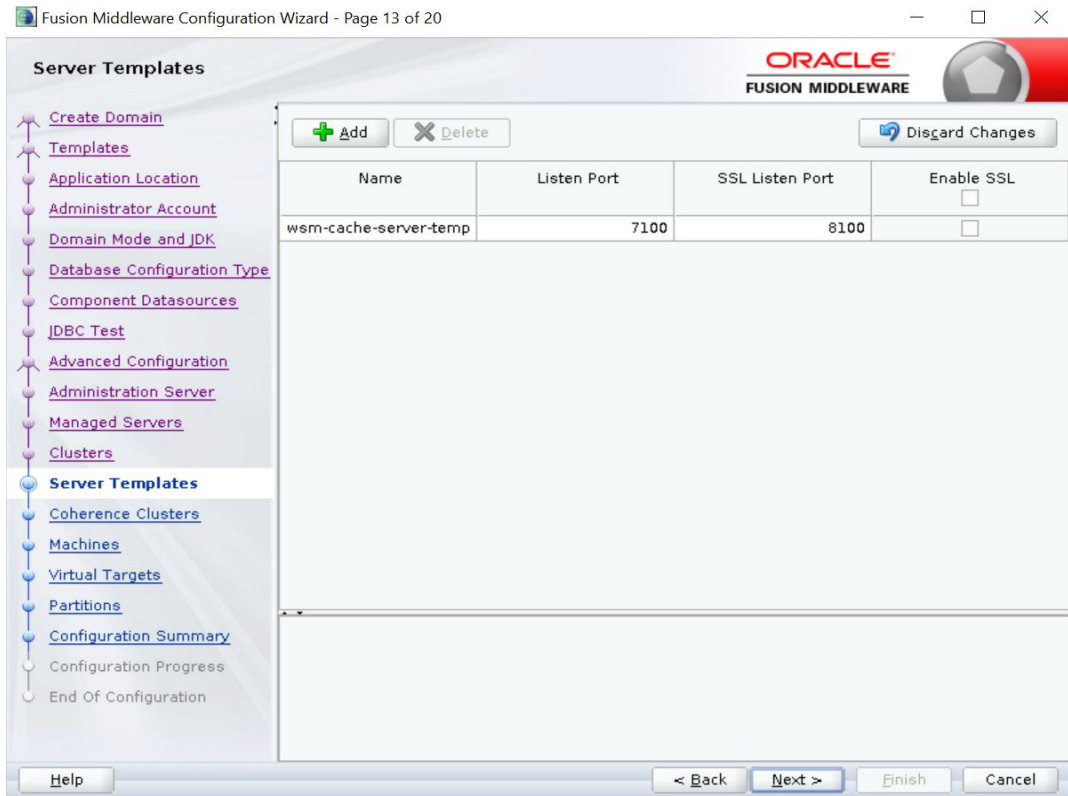
It is recommended to create two managed servers, one each for UI and Web Services.

---

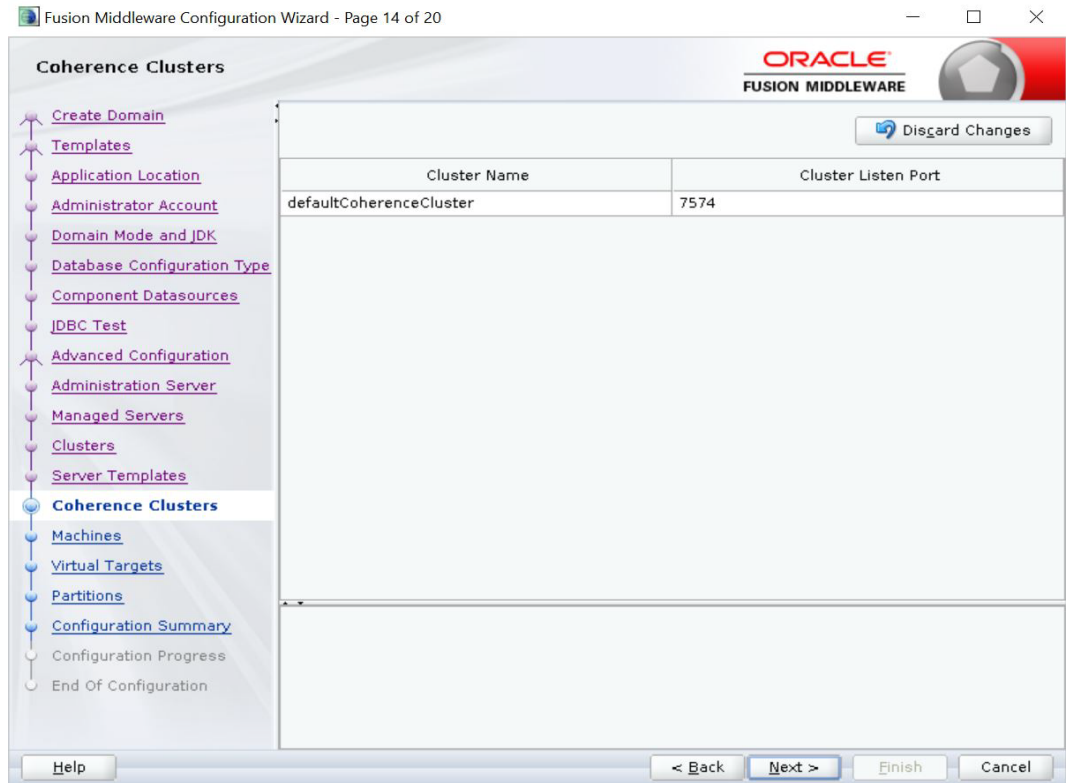
18. Click 'Next'. The following window is displayed.



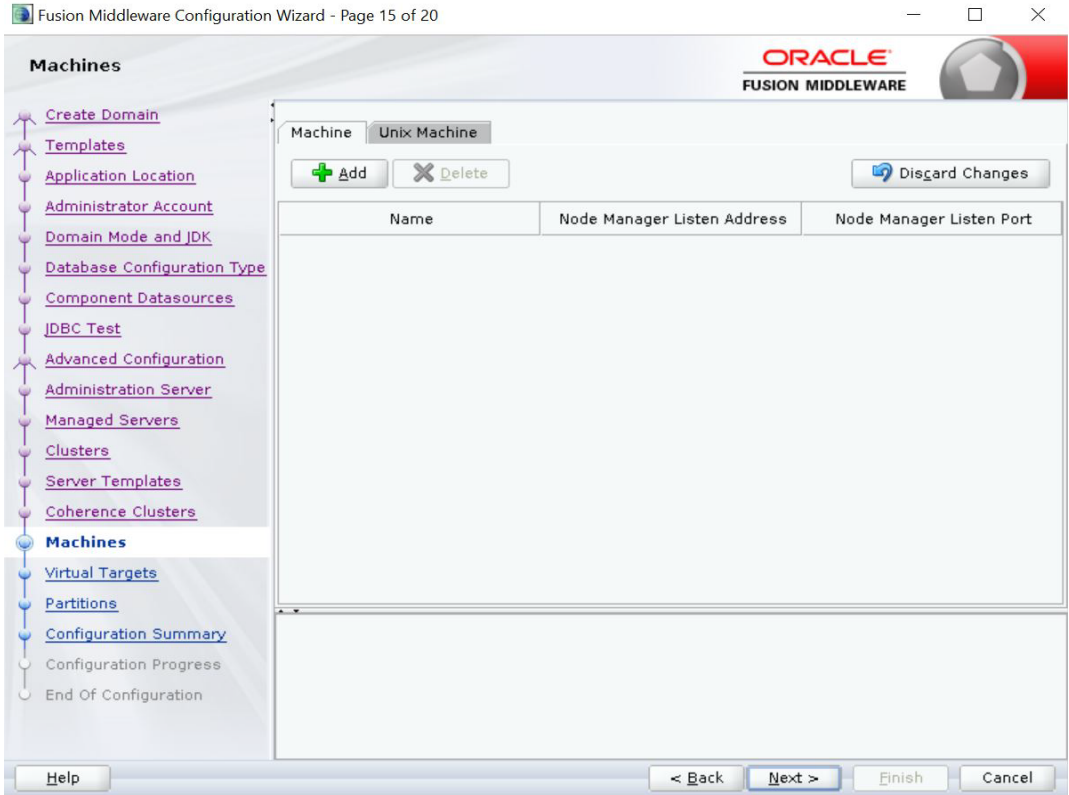
19. Configure as required and click 'Next'. The following window is displayed.



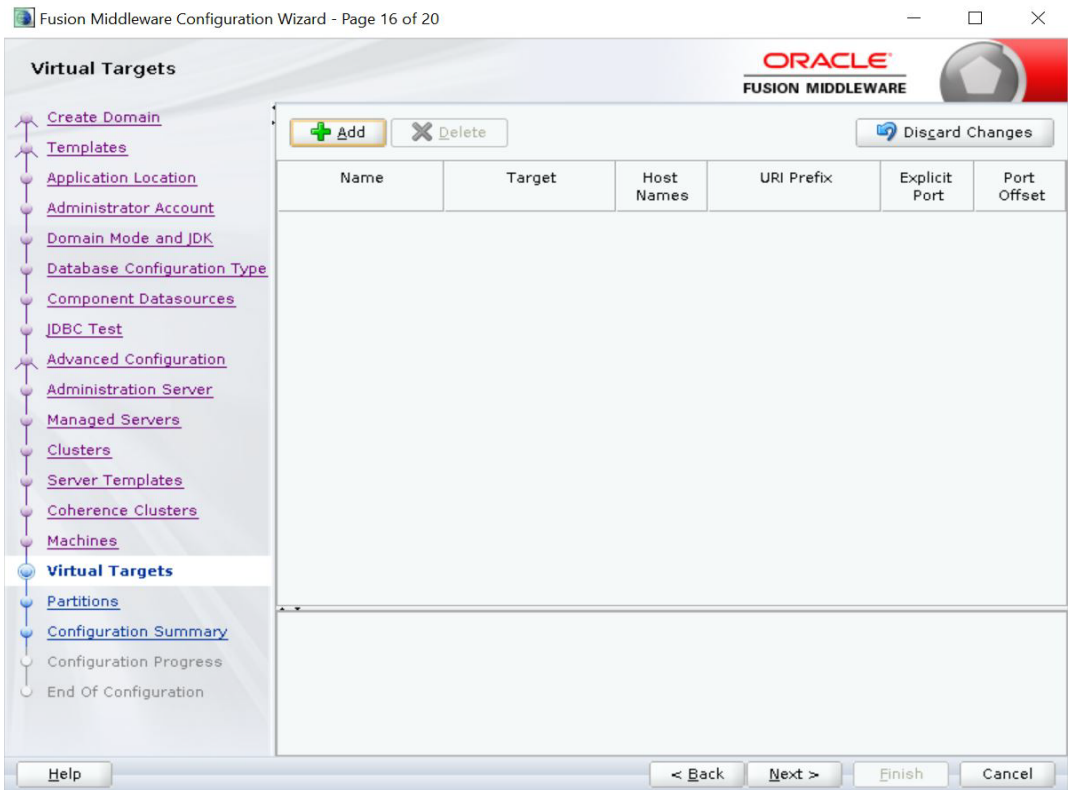
20. Configure as required and click 'Next'. The following window is displayed.



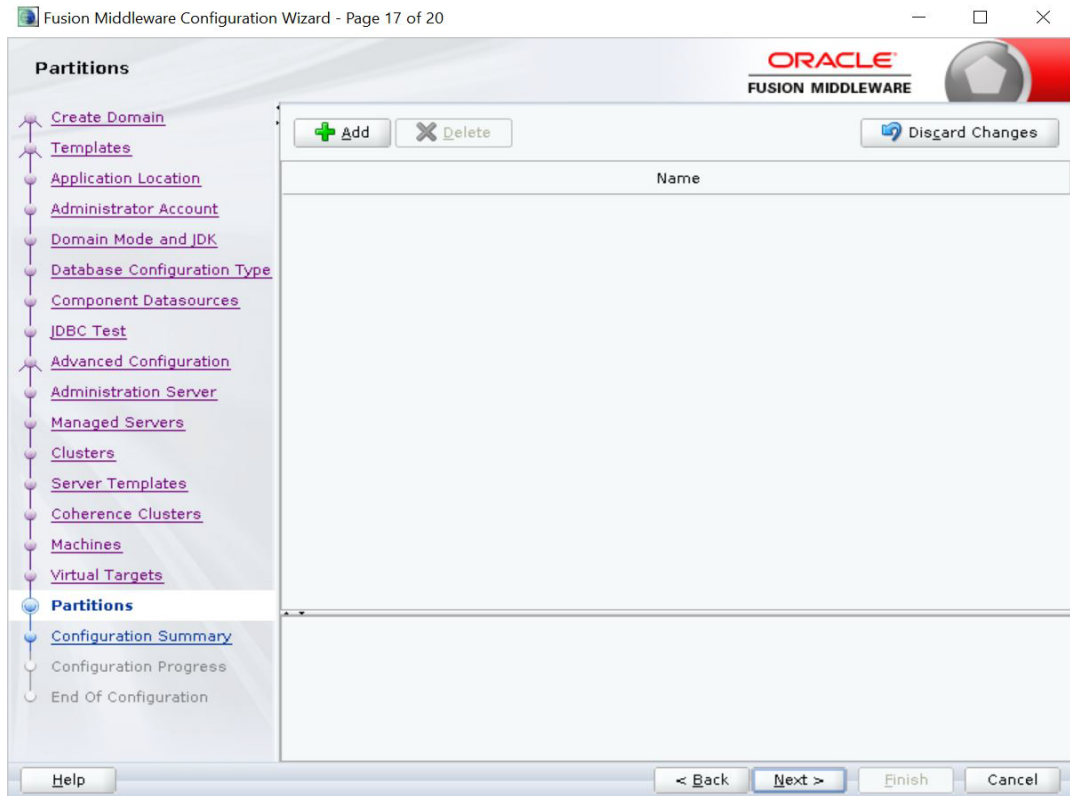
21. Configure as required and click 'Next'. The following window is displayed.



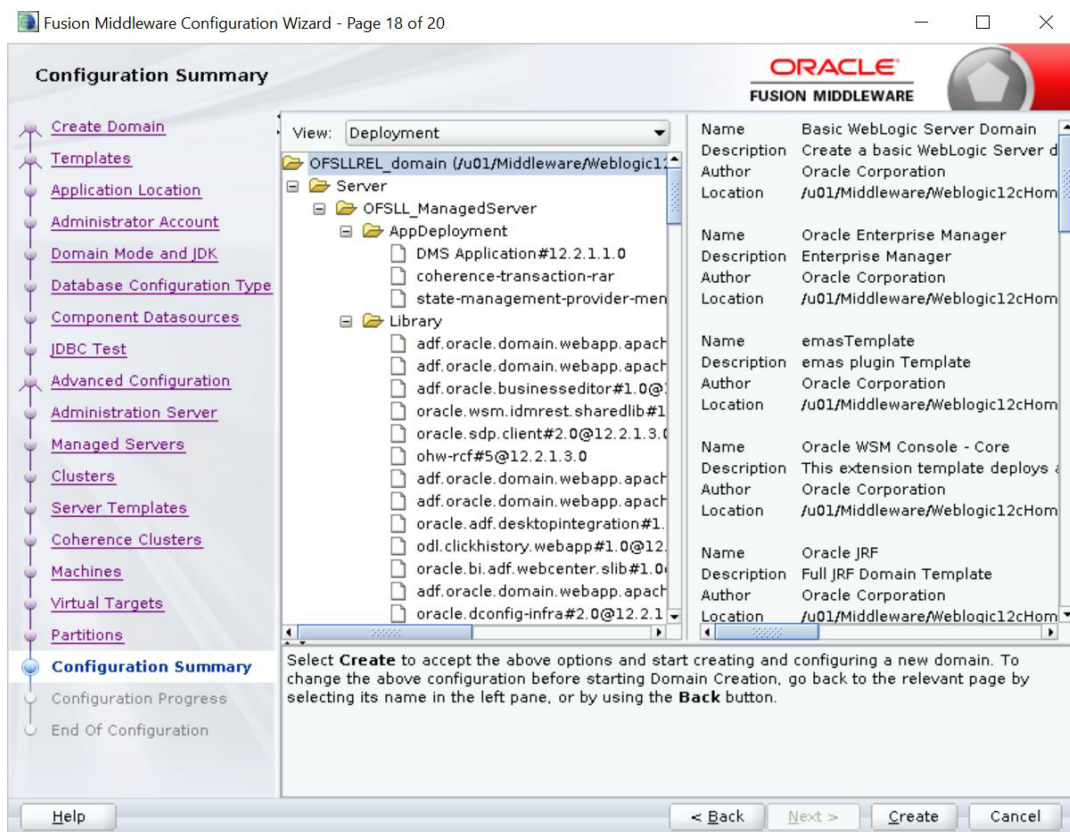
22. Click 'Create'. The following window is displayed.



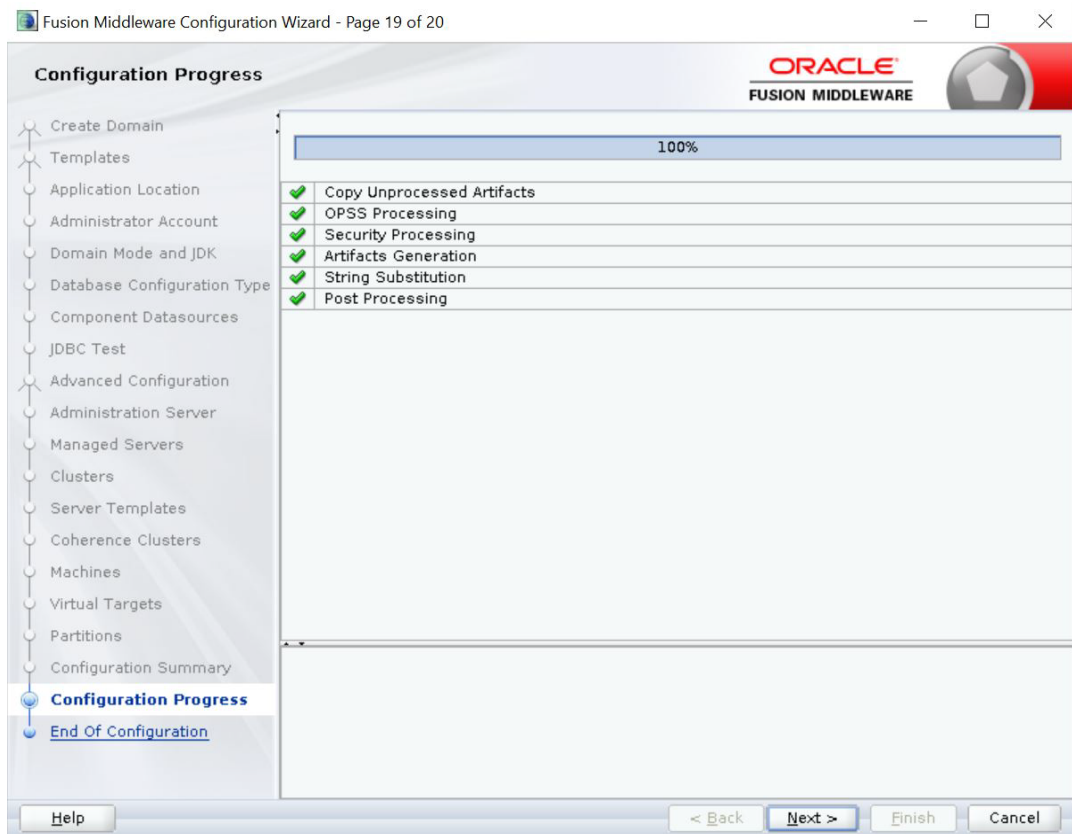
23. Click 'Next'. The following window is displayed.



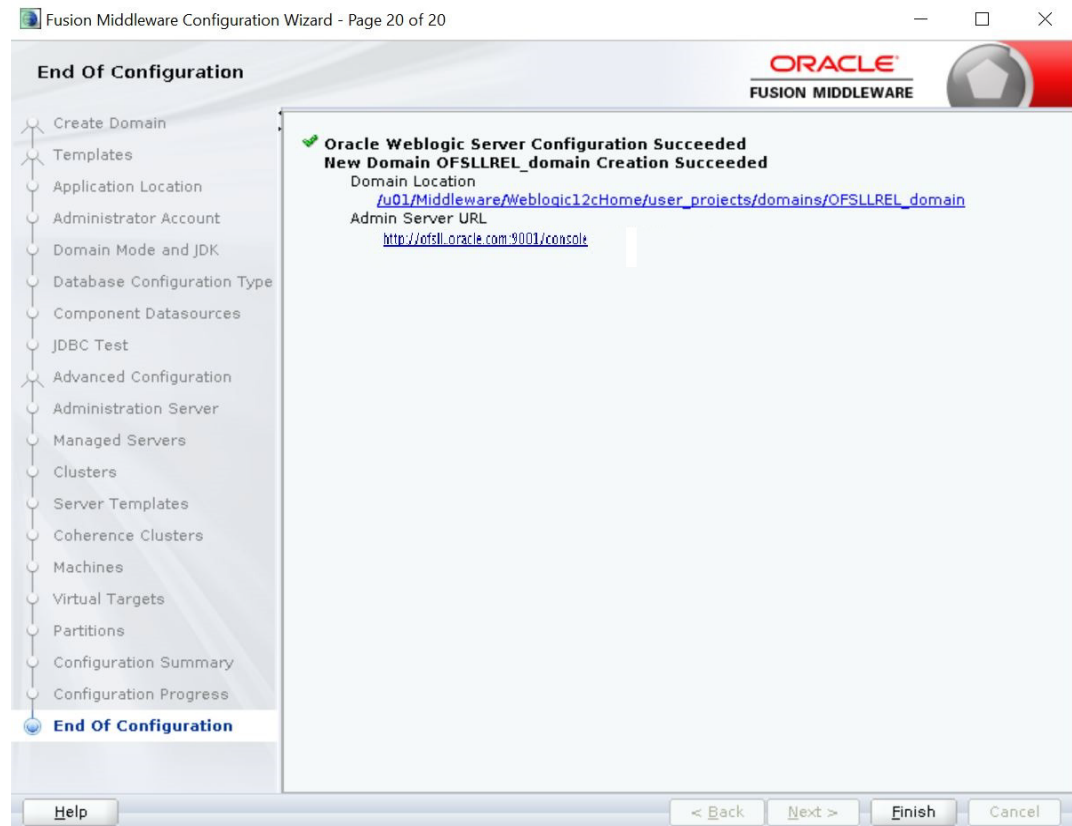
24. Click 'Next'. The following window is displayed.



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.specjds1=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

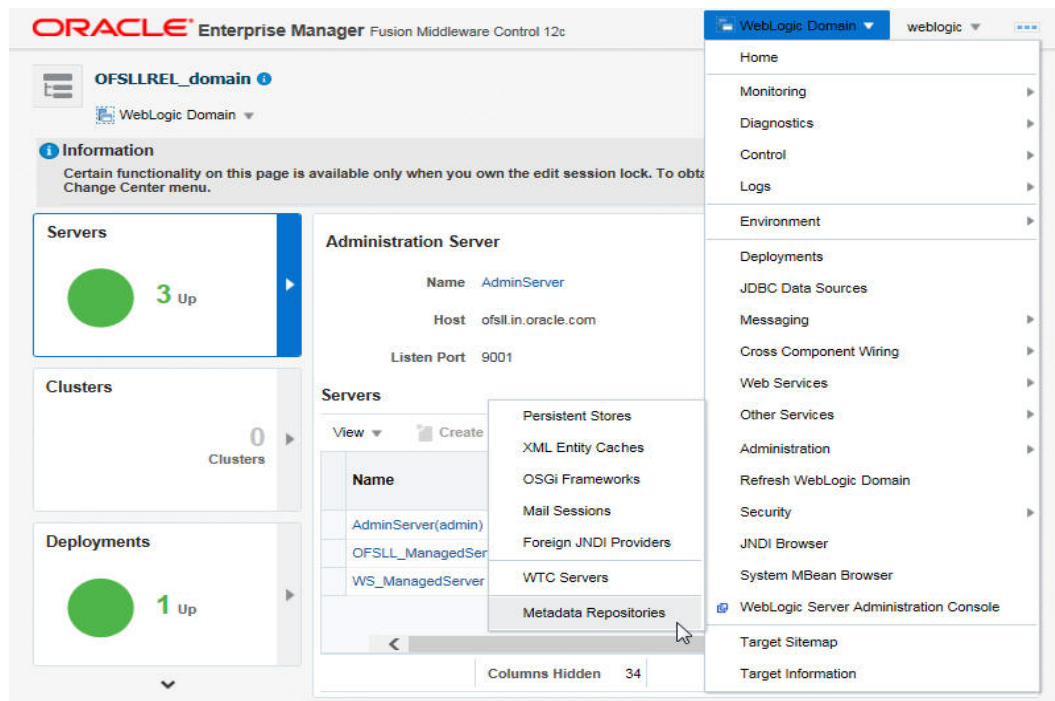
- For managed server where web services are deployed:

-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.specjds=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.

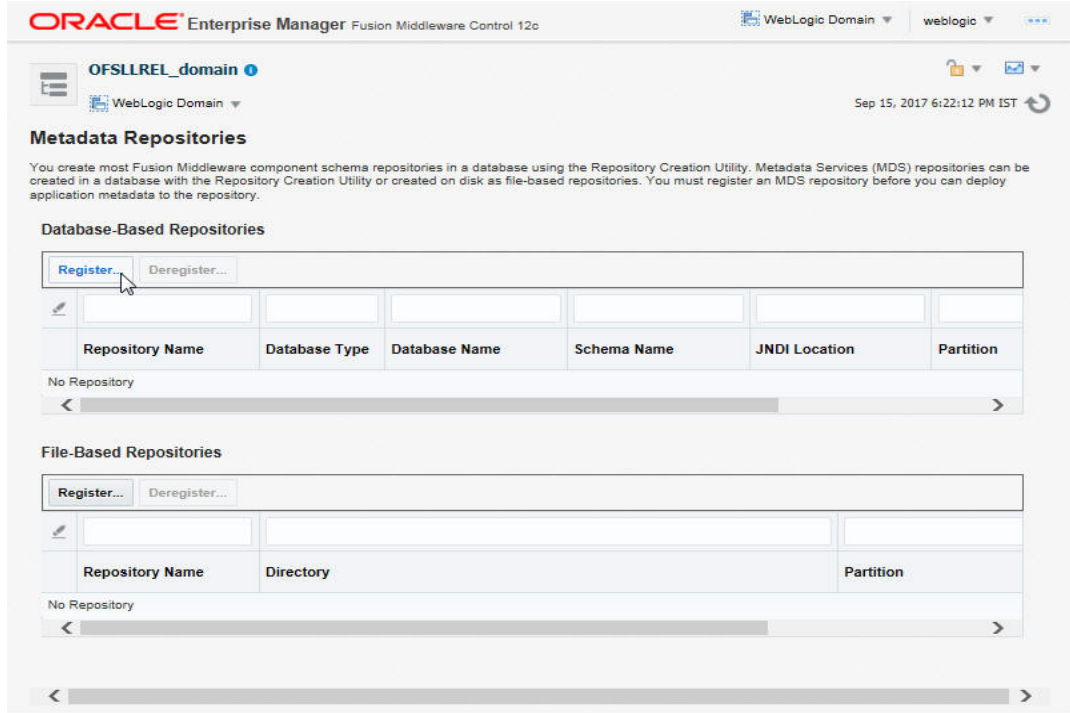
1. Login to Oracle Enterprise Manager 12c console (<http://hostname:port/em>).



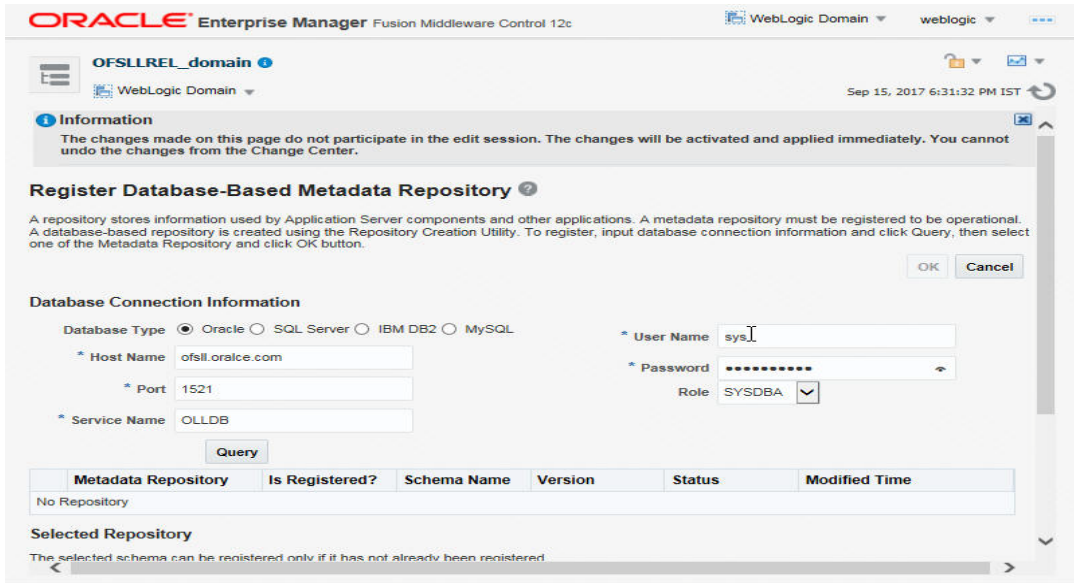
2. Click on domain name OFSSLREL\_domain on the left side panel.
3. Expand Weblogic domain OFSSLREL\_domain and click 'Metadata Repositories' option, as shown in the above screen.



4. The following window is displayed.



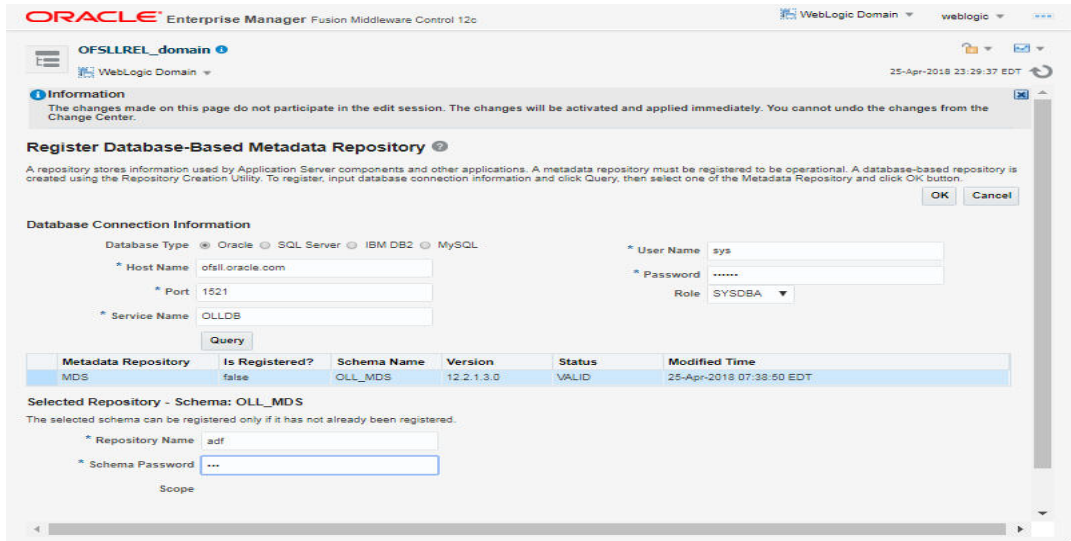
5. Click 'Register' button. The following window is displayed.



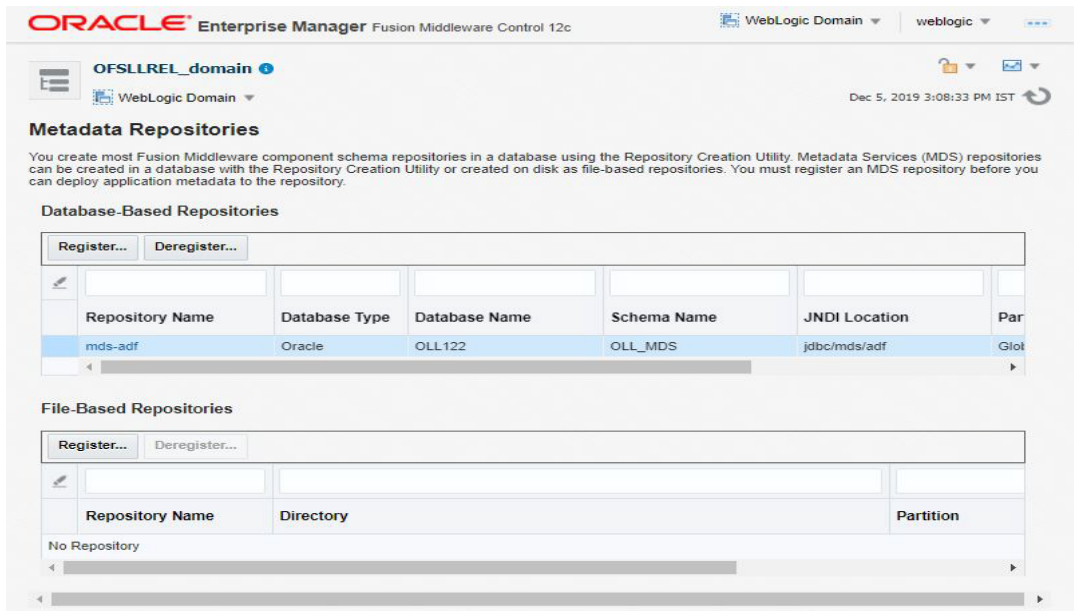
6. Enter database instance details under Database Connection Information section and click 'Query'. All available schemas in the given database instance are listed.

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.



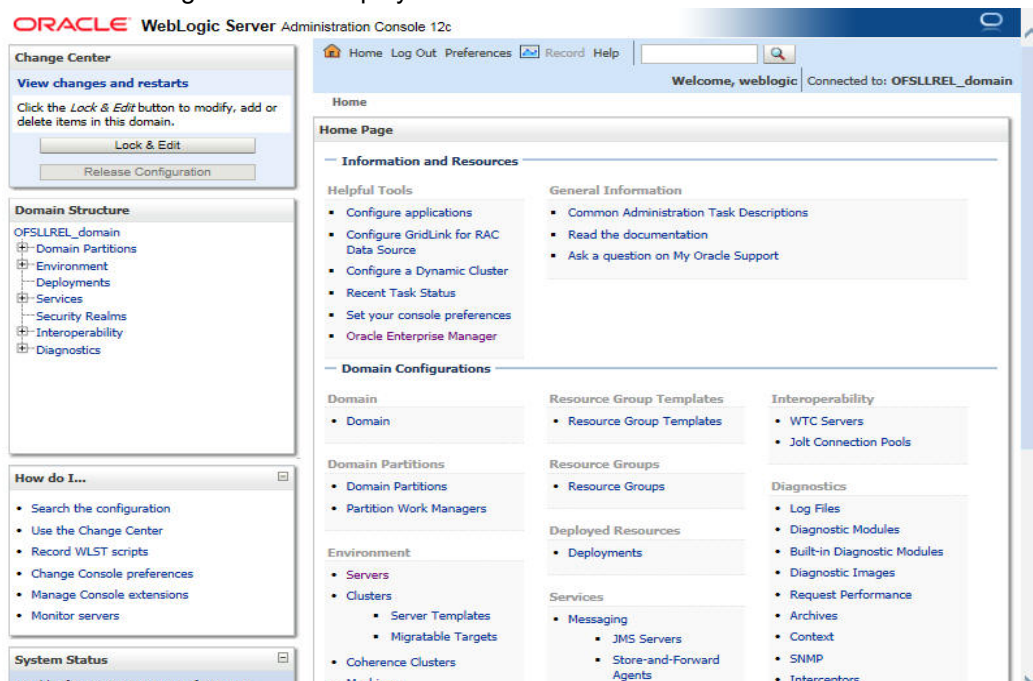
10. Click 'Add' and target to AdminSever and OFSLL\_ManagedServer as on right panel.

## 3.4 Creating Data Source

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

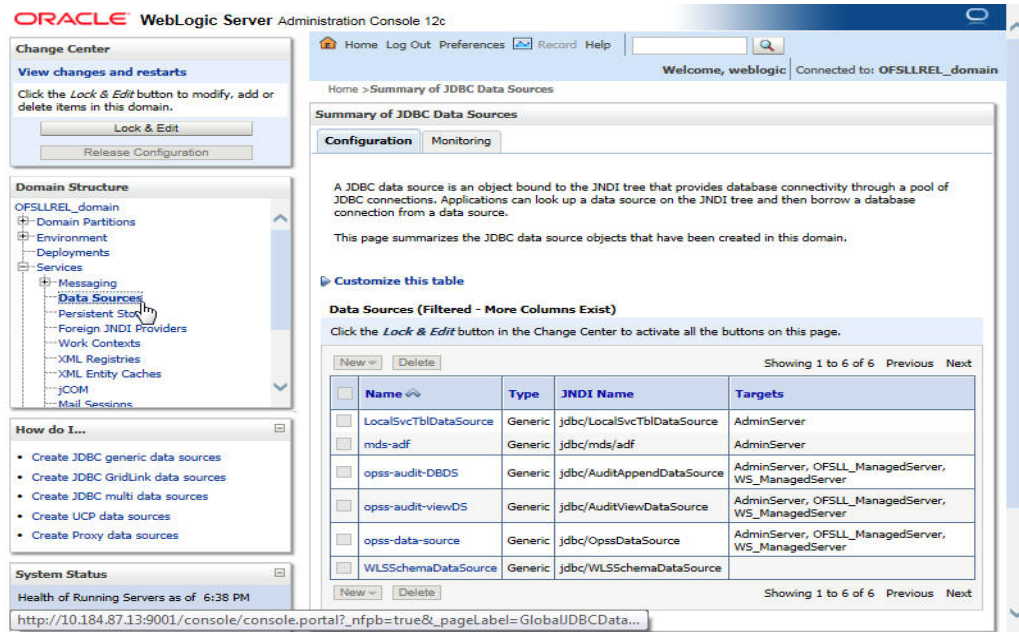


2. The following window is displayed.

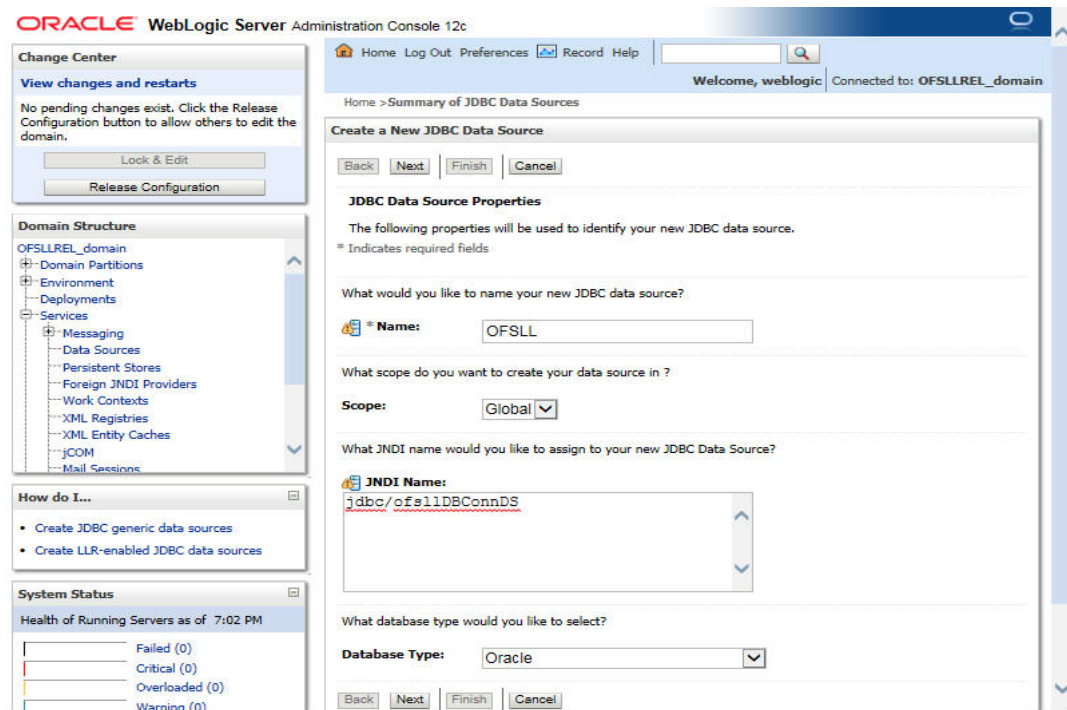


3. Click Domain Name > Services > Data Sources.

4. The following window is displayed.

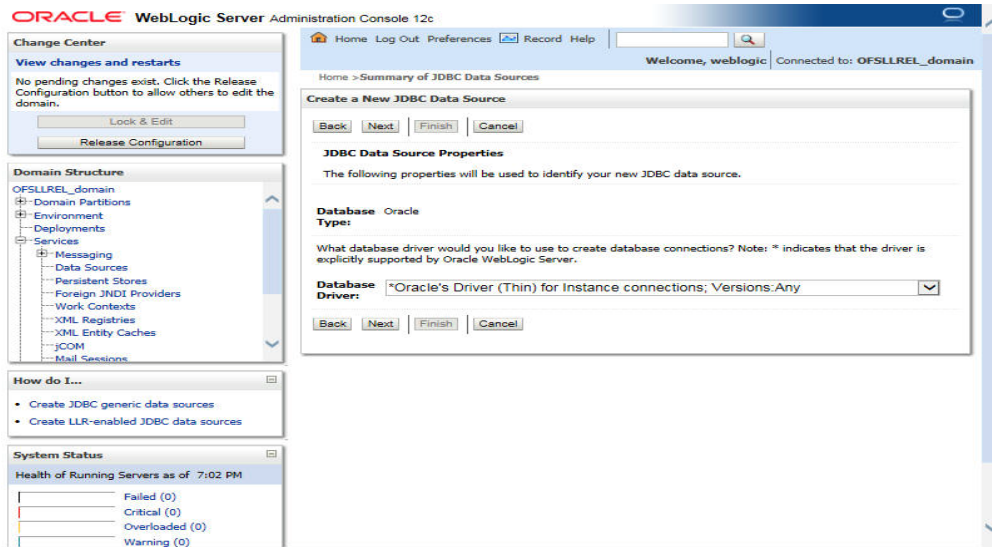


5. Click 'Lock & Edit' button on the left panel. Click 'New' on right panel and select Generic Data Source.



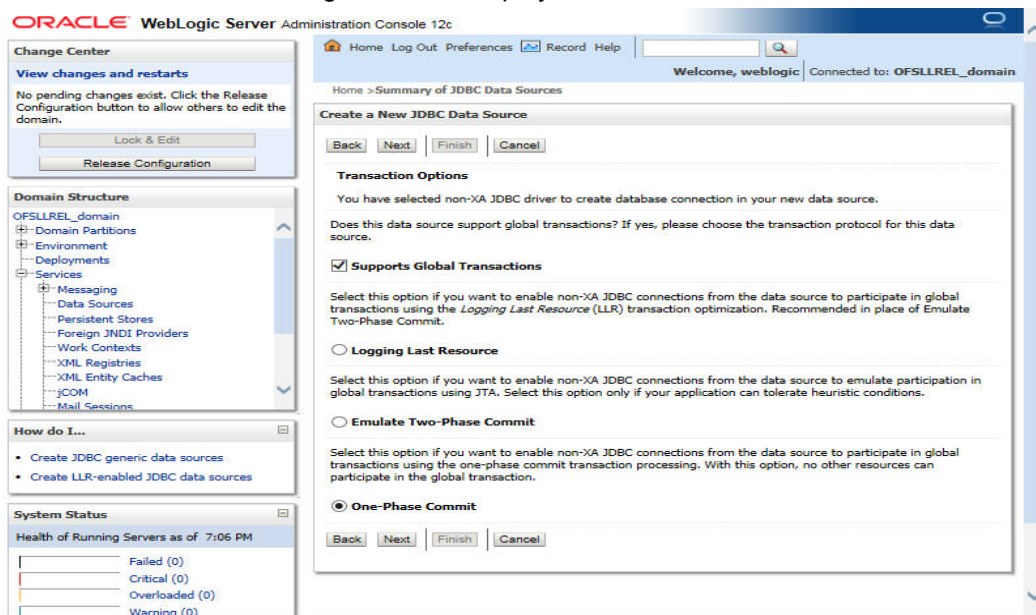
6. Enter Data source 'Name', JNDI Name as 'jdbc/ofslIDBConnDS' and select 'Oracle' as Database Type.

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.

**ORACLE WebLogic Server Administration Console 12c**

Home > Summary of JDBC Data Sources

Welcome, weblogic | Connected to: OFSSLREL\_domain

### Create a New JDBC Data Source

Back | **Next** | Finish | Cancel

**Connection Properties**

Define Connection Properties.

What is the name of the database you would like to connect to?

**Database Name:**

What is the name or IP address of the database server?

**Host Name:**

What is the port on the database server used to connect to the database?

**Port:**

What database account user name do you want to use to create database connections?

**Database User Name:**

What is the database account password to use to create database connections?

**Password:**

**Confirm Password:**

Additional Connection Properties:

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

**ORACLE WebLogic Server Administration Console 12c**

Home > Summary of JDBC Data Sources

Welcome, weblogic | Connected to: OFSSLREL\_domain

### Create a New JDBC Data Source

**Test Configuration** | Back | Next | Finish | Cancel

**Test Database Connection**

Test the database availability and the connection properties you provided.

What is the full package name of JDBC driver class used to create database connections in the connection pool?  
(Note that this driver class must be in the classpath of any server to which it is deployed.)

**Driver Class Name:**

What is the URL of the database to connect to? The format of the URL varies by JDBC driver.

**URL:**

What database account user name do you want to use to create database connections?

**Database User Name:**

What is the database account password to use to create database connections?  
(Note: for secure password management, enter the password in the Password field instead of the Properties field below)

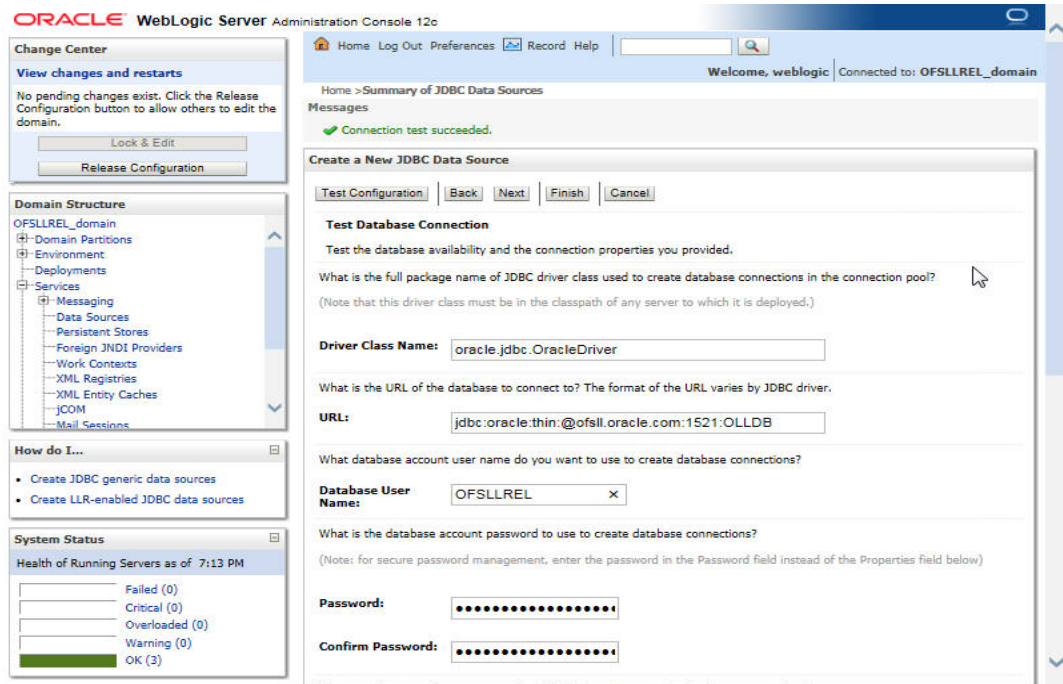
**Password:**

**Confirm Password:**

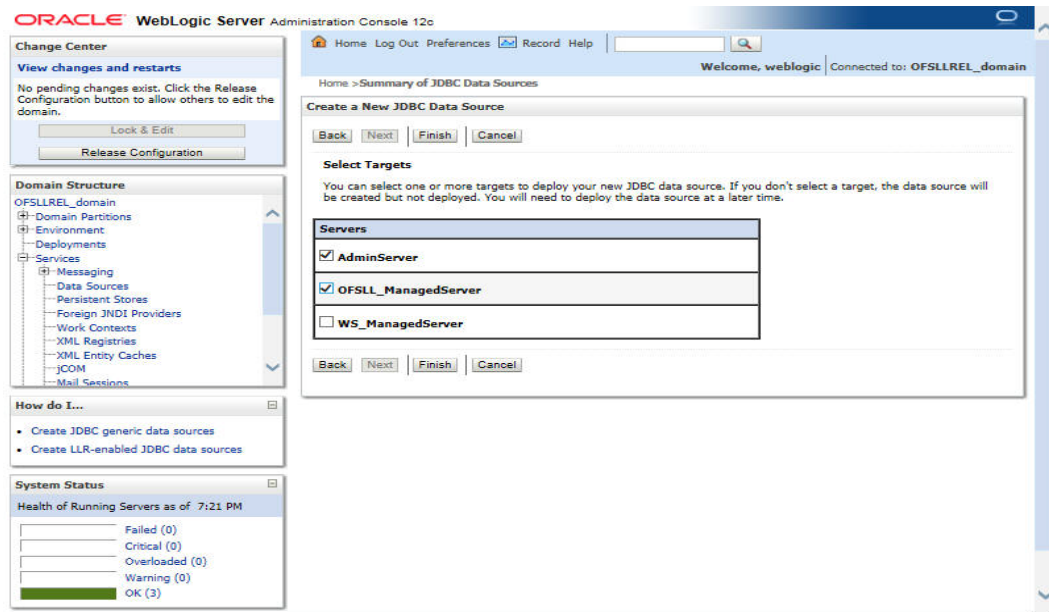
What are the properties to pass to the JDBC driver when creating database connections?

**Properties:**

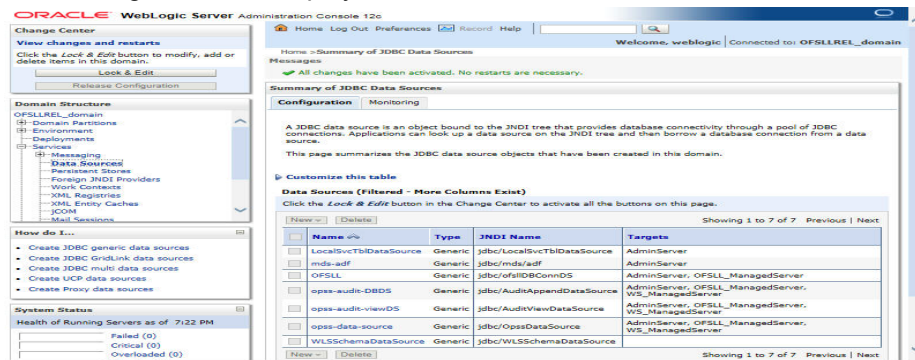
12. Click 'Test Configuration'. The following window is displayed.



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**

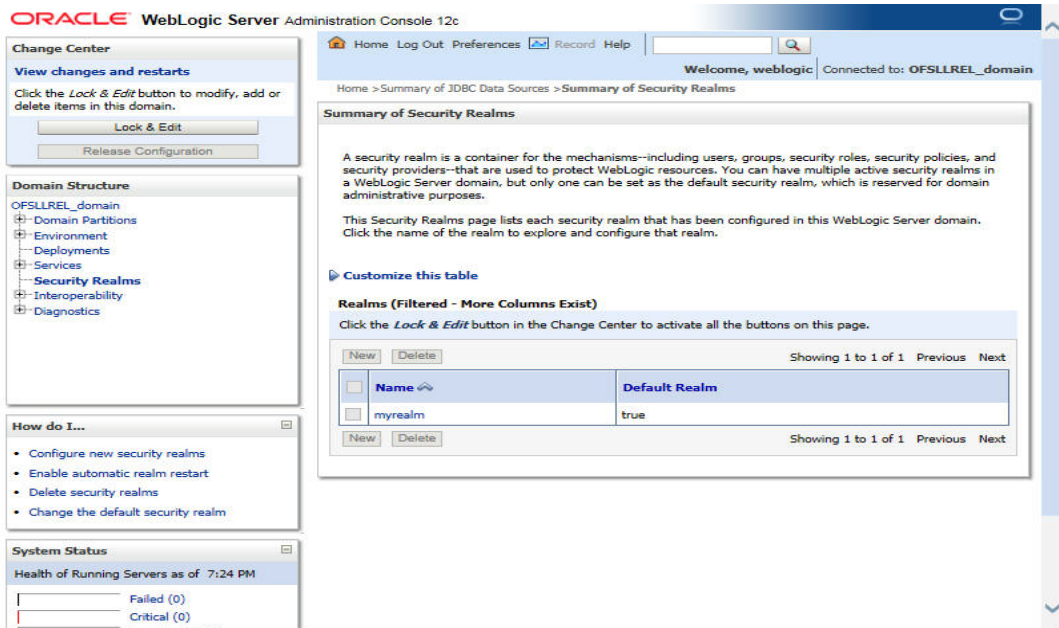
User Authentication and Management is outside of Oracle Financial Services Lending and Leasing application. Organizations can use an LDAP implementation for authentication. For Development and Testing purpose, the following sections can be configured for authentication:

- 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
-

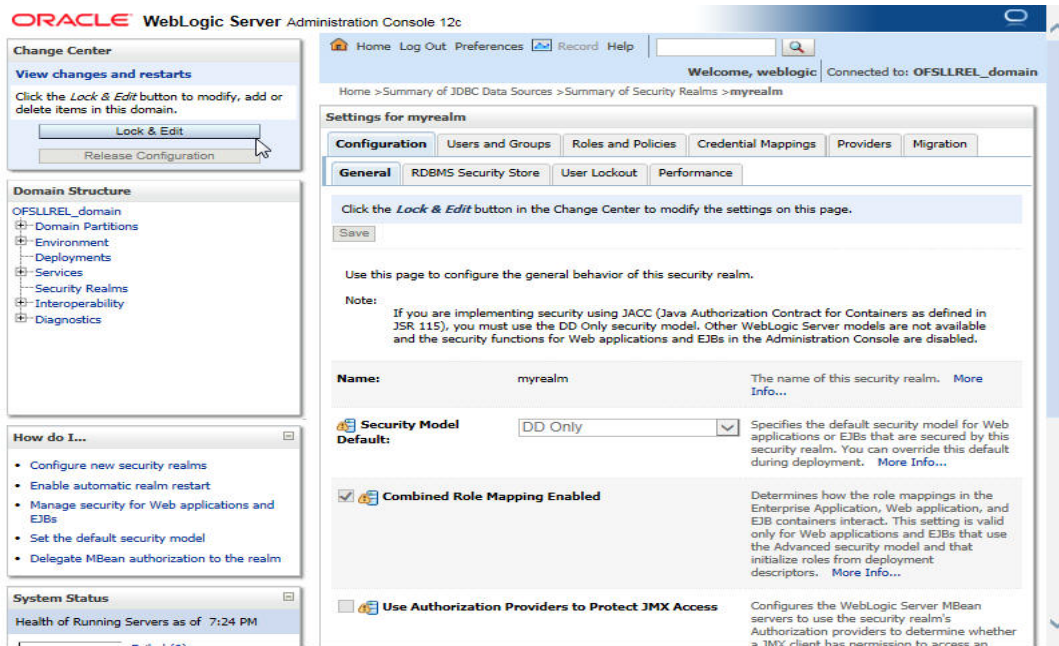


## 3.5 Creating SQL Authentication Provider

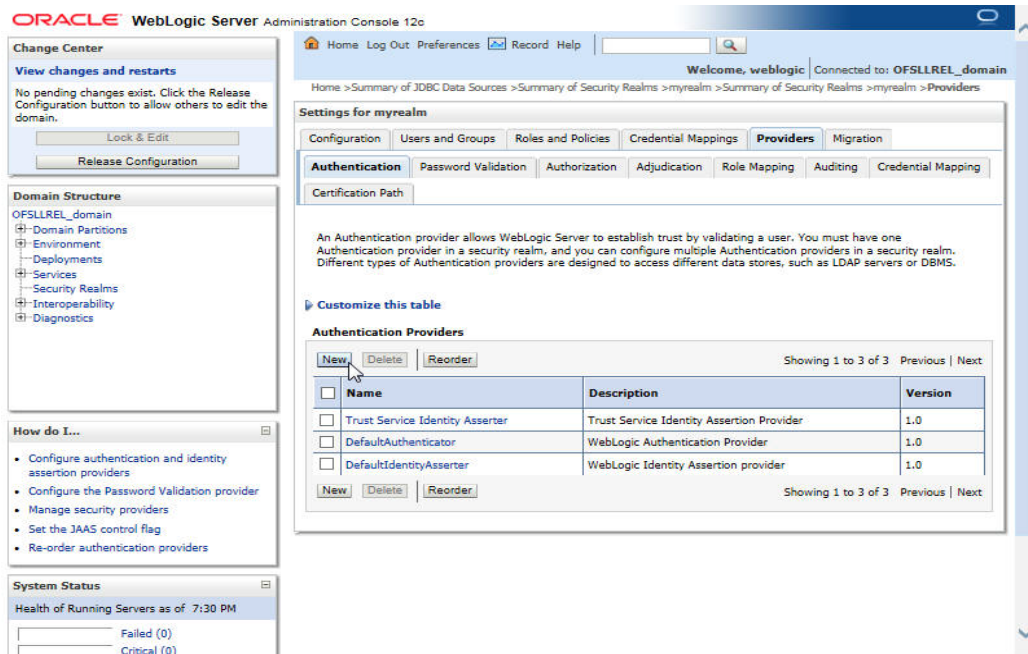
1. Login to WebLogic server administration console and click 'Security Realms' in left panel. The following window is displayed.



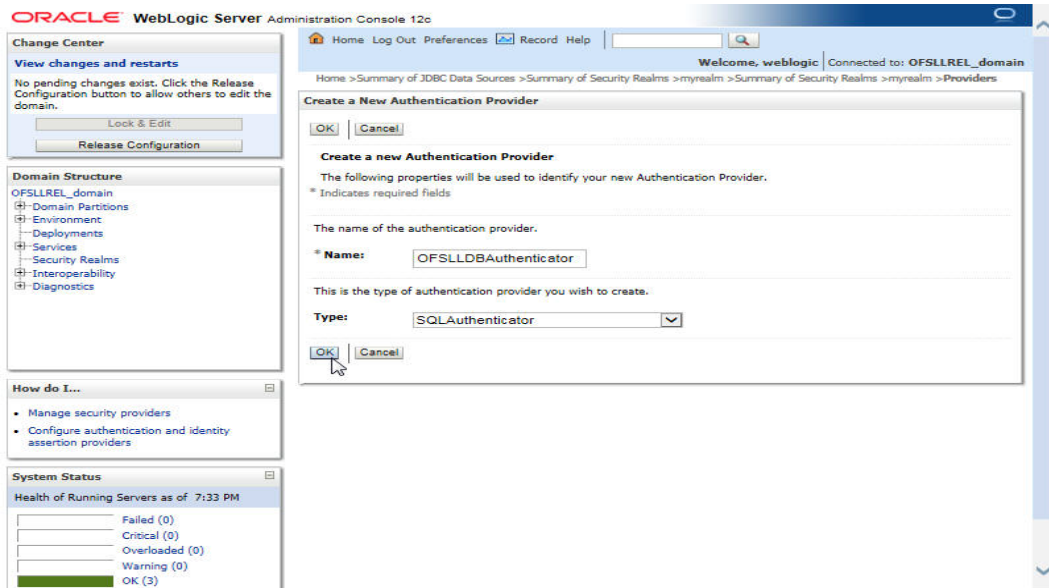
2. Click 'myrealm' on right panel. The following window is displayed.



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



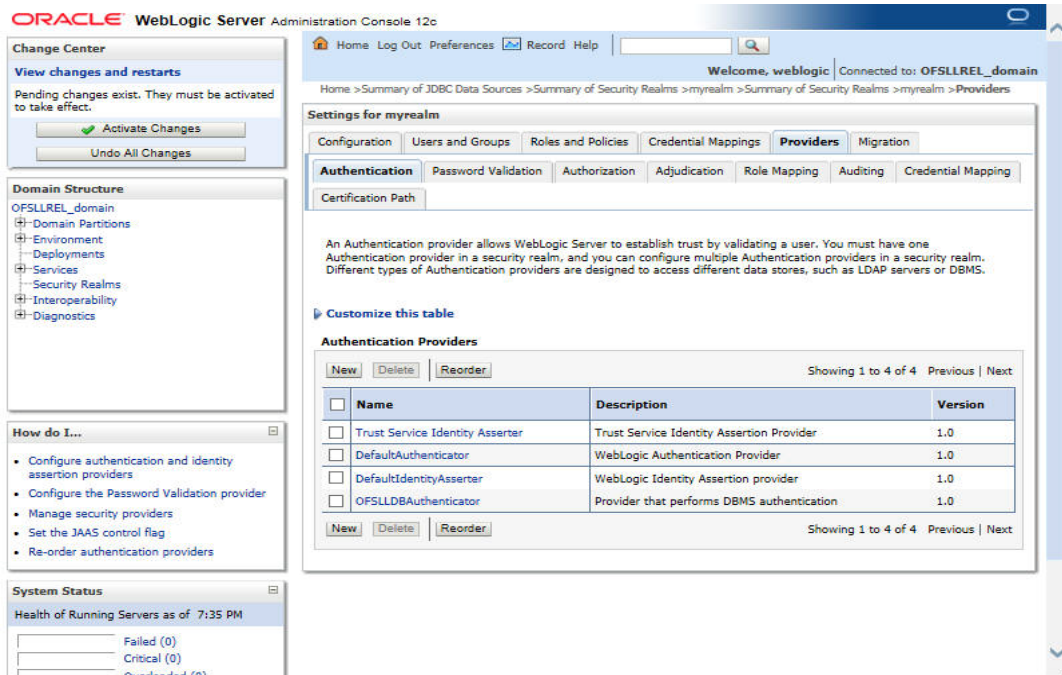
4. Click 'Lock & Edit' to unlock the screen and click 'New' button in Authentication Providers sub tab. The following window is displayed.



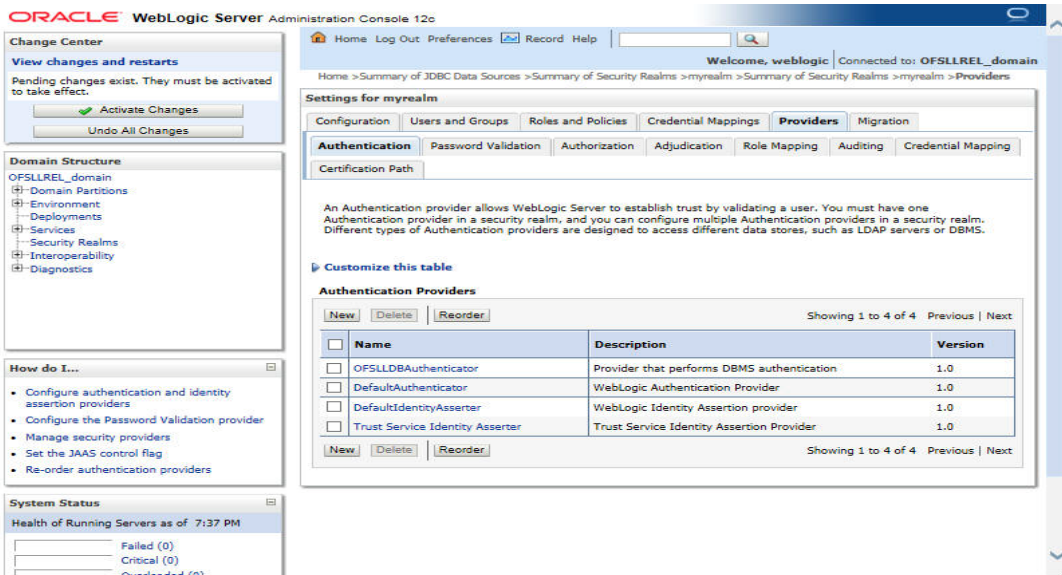
5. Create Authentication provider with following values:

- Name: OFSLLDAuthenticator
- Type: SQLAuthenticator

6. Click 'OK'. The following window is displayed.

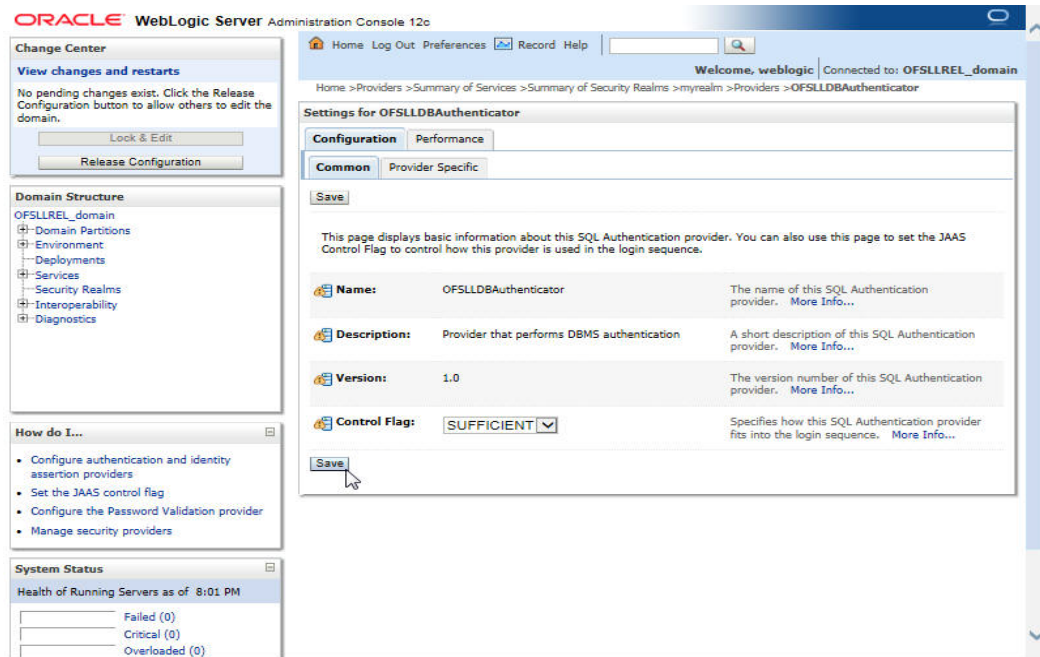


7. Click on 'Activate Changes'. The following window is displayed.



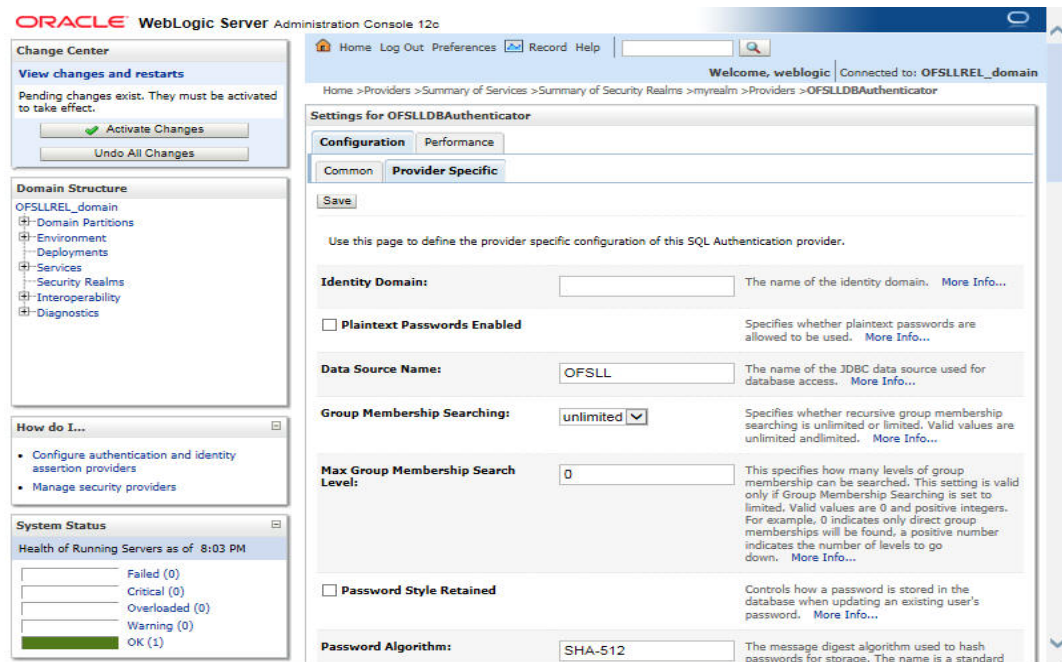
Authentication order should be maintained as mentioned in the above screen. 'OFSLDDBAuthenticator' will be displayed as above.

8. Click on 'OFSLDBAuthenticator'. 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: OFSSL
- 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 Webllogic	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 Webllogic	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 = ?
SQL Set 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	

<b>SQL Remove Member From Group:</b>	EMBER_USR_CODE= ?	The SQL statement used to remove a member from a group. The SQL statement requires two parameters: the group name and the group member being deleted from the group. <a href="#">More Info...</a>
<b>SQL Remove Group Member:</b>	DELETE FROM USER_([	The SQL statement used to remove a member from a group. The SQL statement requires a single parameter: the username or group name being removed. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> <b>Descriptions Supported</b>		Indicates whether user and group descriptions are supported by the database used by the authentication provider. <a href="#">More Info...</a>
<b>SQL Get User Description:</b>	E UAU_USR_CODE = ?	The SQL statement used to retrieve the description of a specific user. Only valid if Descriptions Supported is enabled. The SQL statement requires a single parameter for the username and must return a resultSet containing at most a single record containing the user description. <a href="#">More Info...</a>
<b>SQLSet User Description:</b>	RE UAU_USR_CODE = ?	
<b>SQL Get Group Description:</b>	JGR_GROUP_CODE = ?	The SQL statement used to retrieve the description of a group. Only valid if Descriptions Supported is enabled. The SQL statement requires a single parameter for the group name and must return a resultSet containing at most a single record containing the group description. <a href="#">More Info...</a>
<b>SQL Set Group Description:</b>	JGR_GROUP_CODE = ?	The SQL statement used to specify a description for a group. Only valid if Descriptions Supported attribute is enabled. The SQL statement requires two parameters: the group description and the group name. <a href="#">More Info...</a>
<input type="button" value="Save"/>		

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 OFSSL 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: OFSSLREL
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 OFSSL 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..

The screenshot displays the Oracle WebLogic Server Administration Console. The main content area is titled 'Summary of Security Realms' and contains a table with the following data:

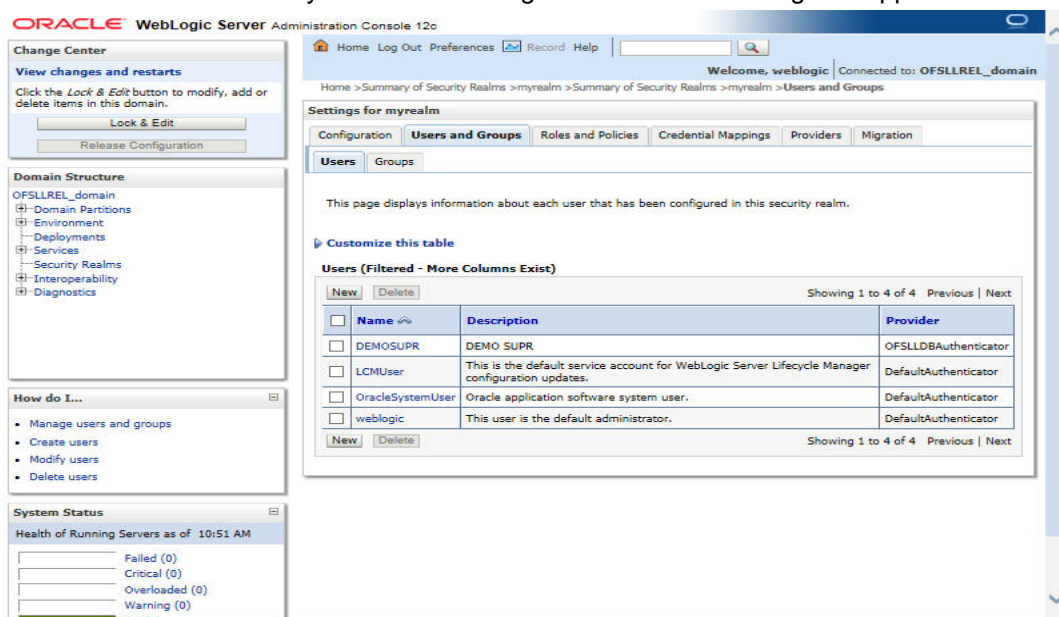
Name	Default Realm
myrealm	true

The left sidebar shows the 'Domain Structure' tree with 'Security Realms' selected. Below it, the 'How do I...' section lists tasks like 'Configure new security realms' and 'Change the default security realm'. The 'System Status' section shows the health of running servers as of 10:49 AM.

4. Select 'Users' tab under Users and Groups.

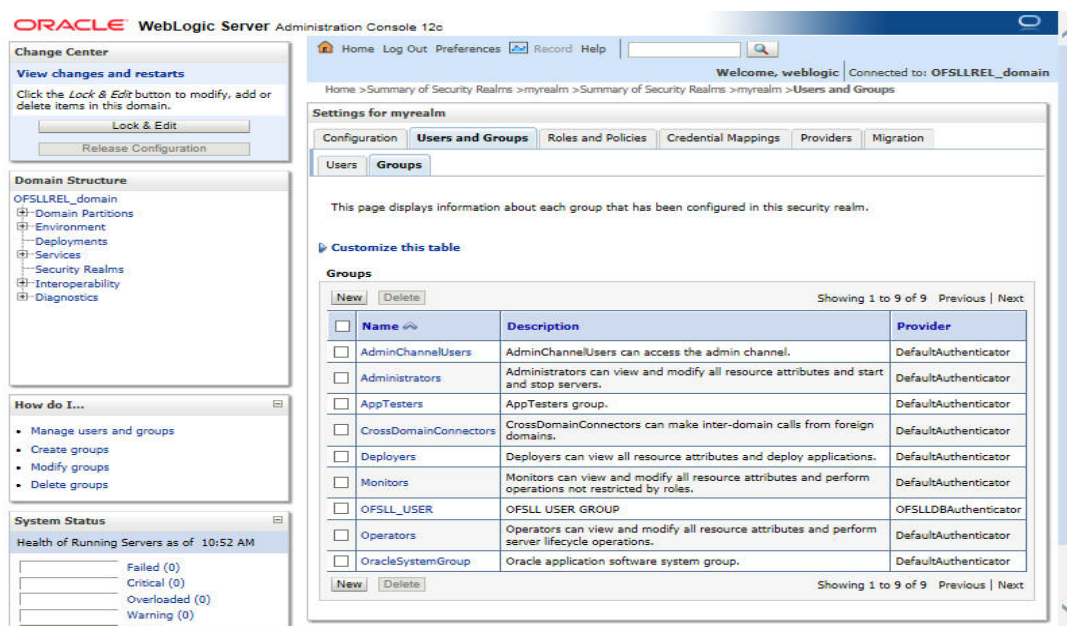


- If SQLAuthenticator is configured as a Security Provider for the OFSLL application, the Users are automatically created in weblogic when created through an application.



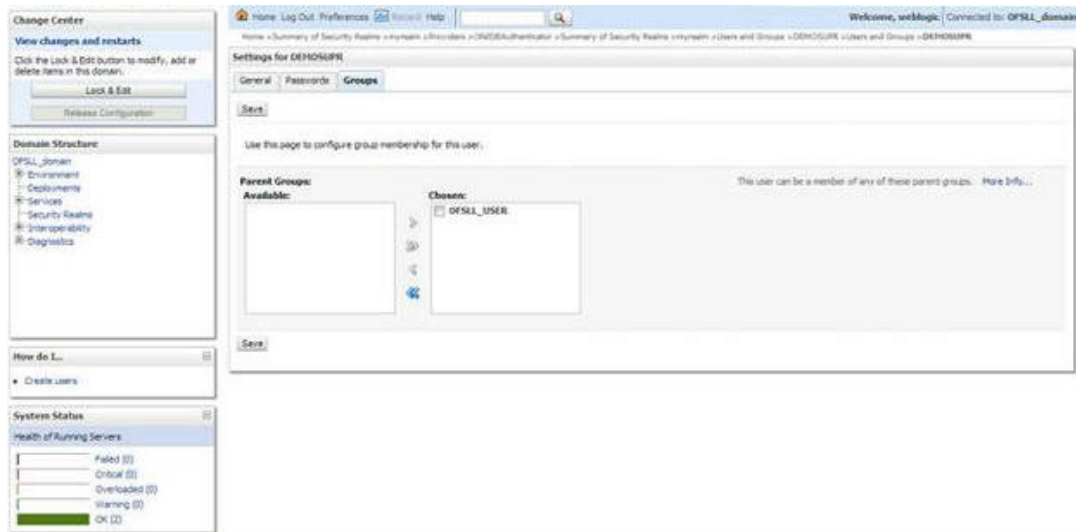
### 3.6.2 Creating User Groups

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



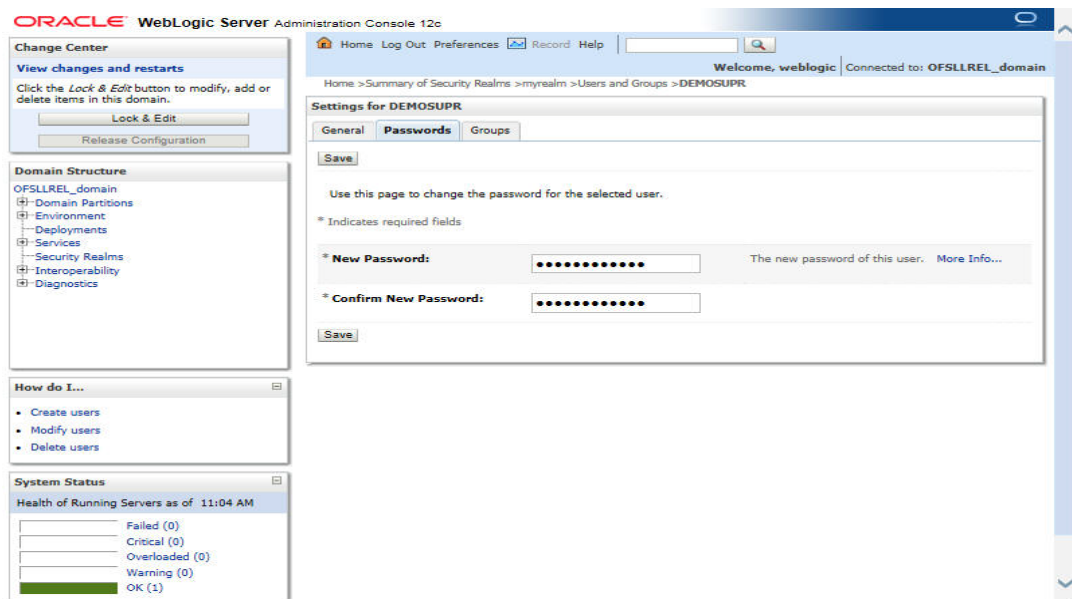
### 3.6.3 Assigning Users to Groups

The USERS are automatically mapped to default application group - OFSLL\_USER.

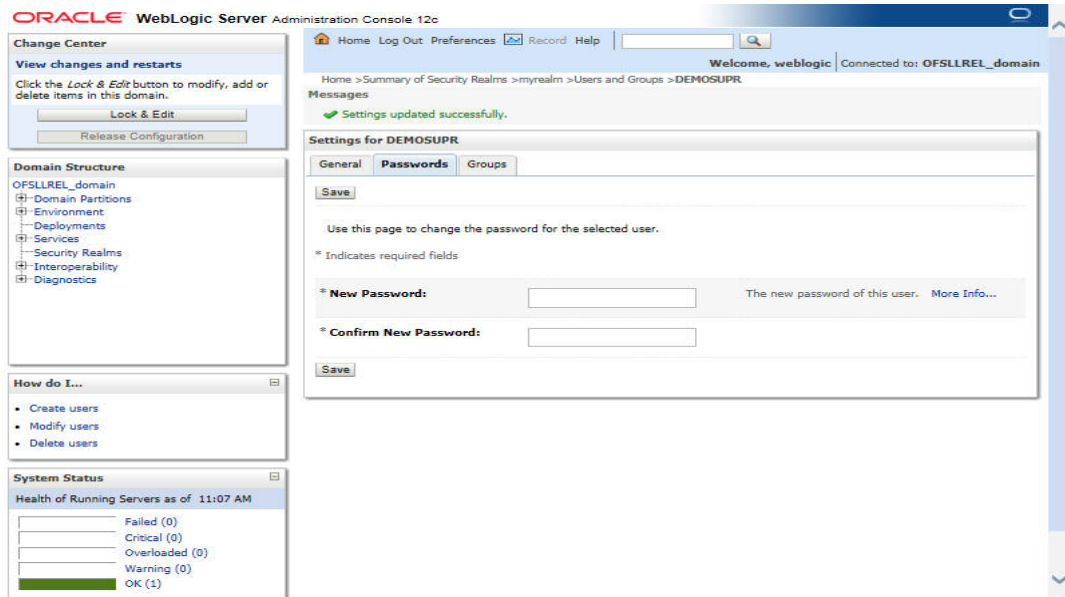


### 3.6.4 Resetting password via weblogic console

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



2. Click 'Save'. The following window displayed.



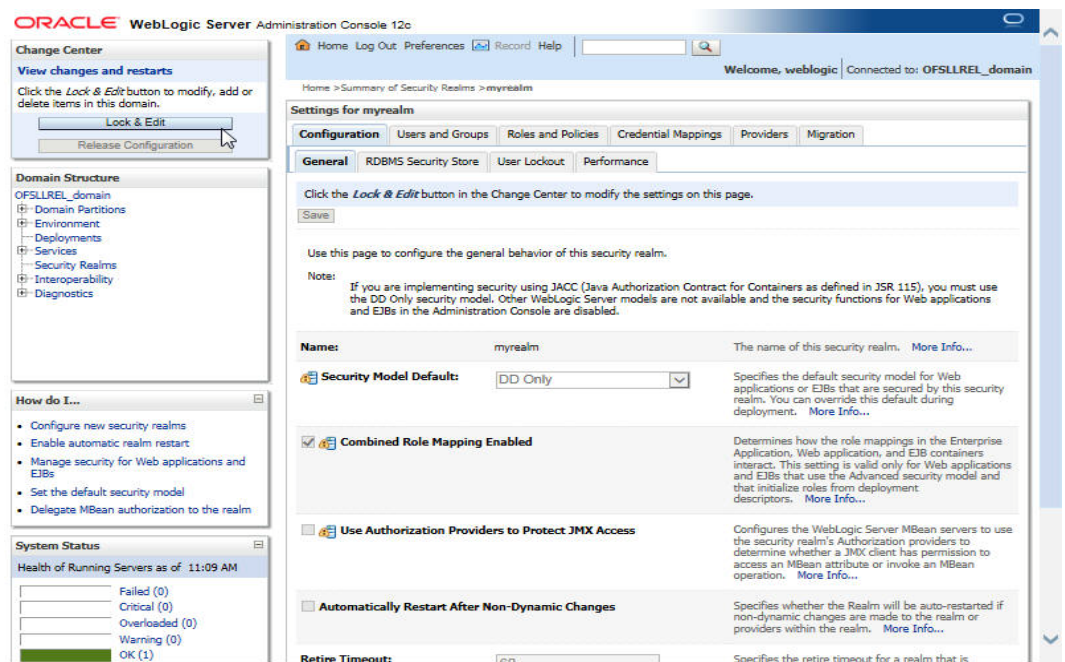
### 3.7 Implementing JMX Policy for Change Password

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**



- To enable JMX policy select the 'Use Authorization Providers to Protect JMX Access' check box on the right panel

The screenshot shows the Oracle WebLogic Server Administration Console. The main content area is titled 'Settings for myrealm' and includes a 'Configuration' tab. Under the 'Configuration' tab, the 'General' sub-tab is active. The 'Security Model Default' is set to 'DD Only'. The 'Combined Role Mapping Enabled' checkbox is checked. The 'Use Authorization Providers to Protect JMX Access' checkbox is also checked. The 'Automatically Restart After Non-Dynamic Changes' checkbox is unchecked. The 'Retire Timeout' is set to 60. The left sidebar shows the 'Domain Structure' and 'System Status' sections.

- Click 'Save' and restart the server.
- Re-login to console.
- Click Domain > Security > myrealm > Roles and Policies > Realm Policies

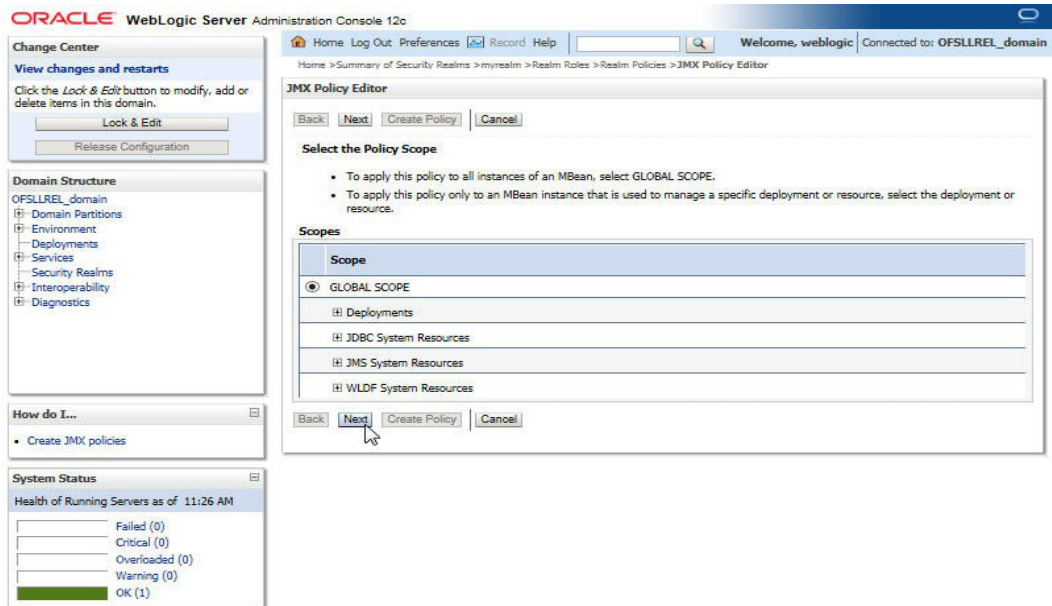
## Note

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

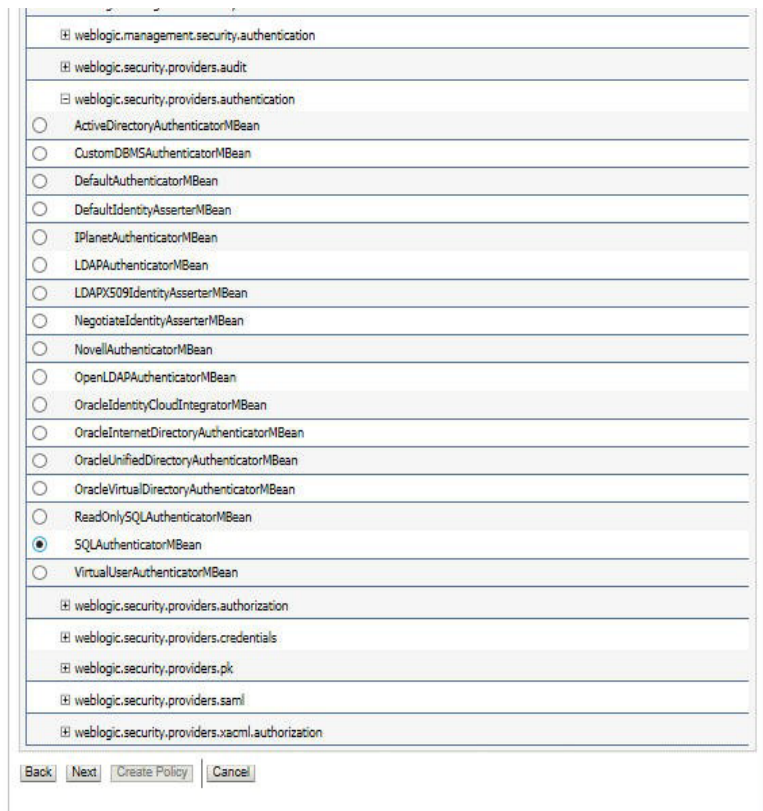
The screenshot shows the Oracle WebLogic Server Administration Console. The main content area is titled 'Settings for myrealm' and includes a 'Roles and Policies' tab. Under the 'Roles and Policies' tab, the 'Realm Policies' sub-tab is active. The page displays a table of policies for the realm. The 'JMX Policy Editor' option is visible in the table. The left sidebar shows the 'Domain Structure' and 'System Status' sections.

Name	Resource Type	Policy
Coherence Clusters		
Deployments		
Domain		
JCOM		
JDBC		
JMS		
JMX Policy Editor		
Root Level Policies		

7. Click on JMX Policy Editor to configure

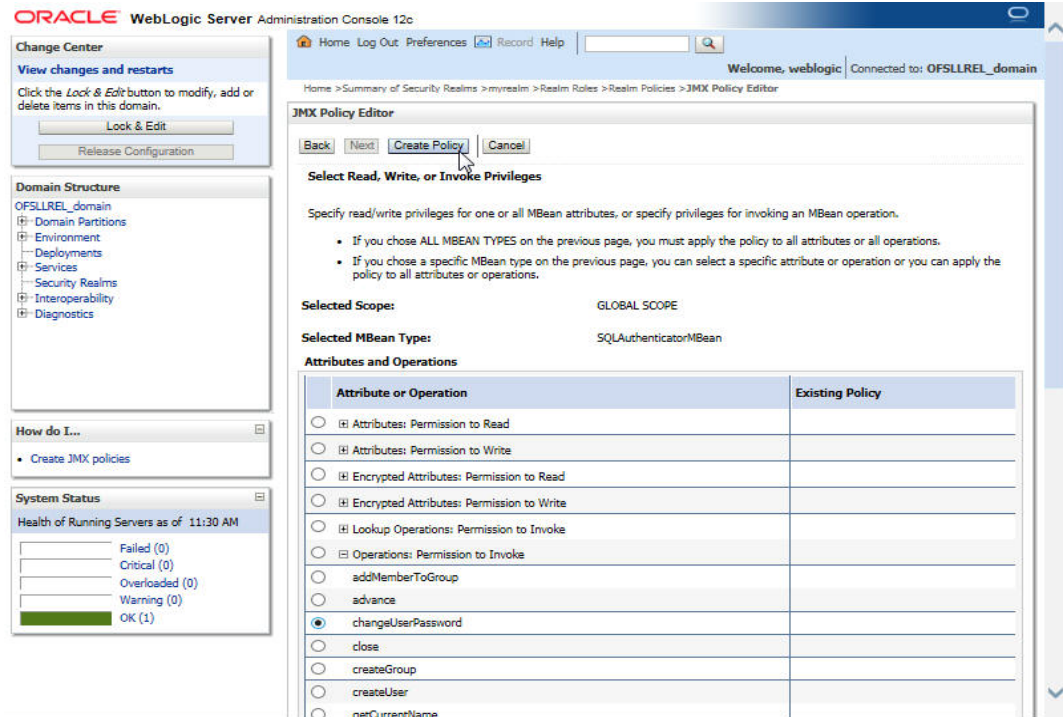


8. Select 'GLOBAL SCOPE' and click 'Next'.



9. Select weblogic.security.providers.authentication.

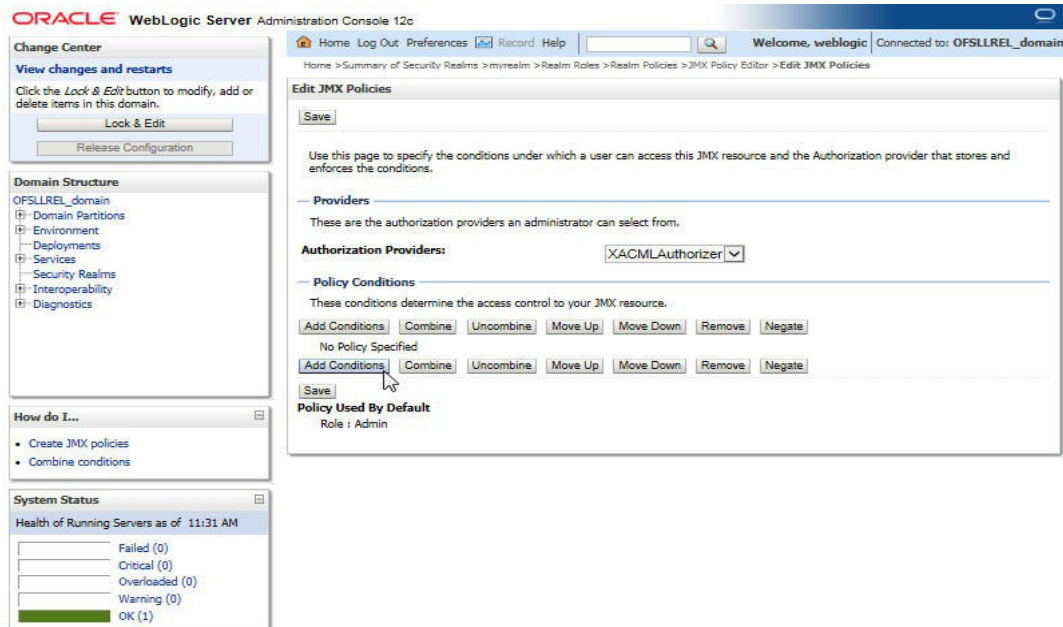
10. Select 'SQLAuthenticatorMBean'. Click 'Next'.



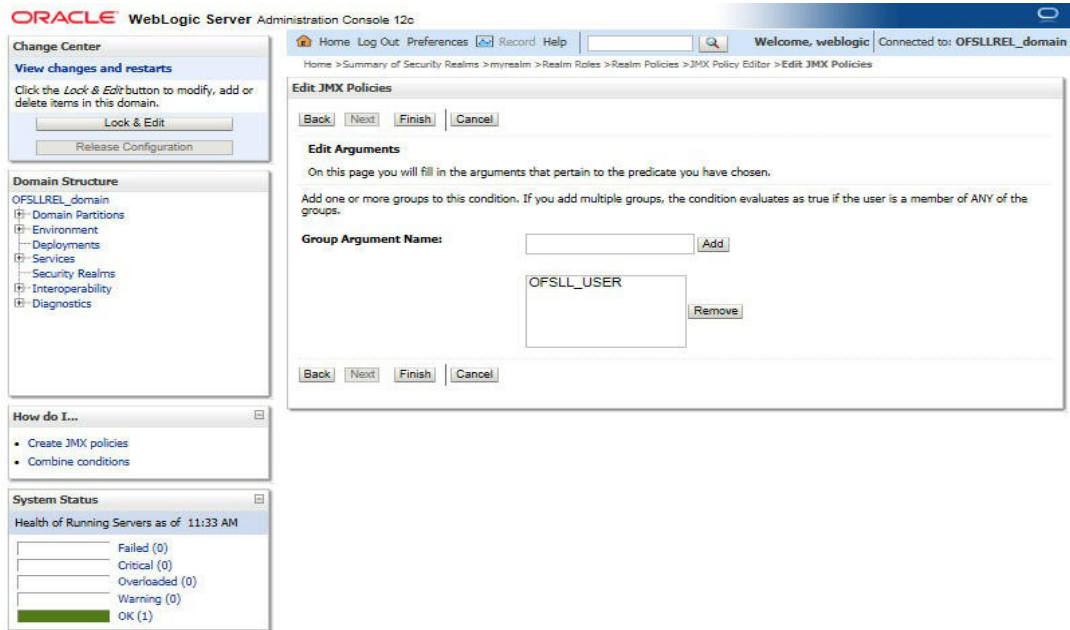
11. Expand 'Operations: Permissions to Invoke' and select 'ChangeUserPassword'.

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.

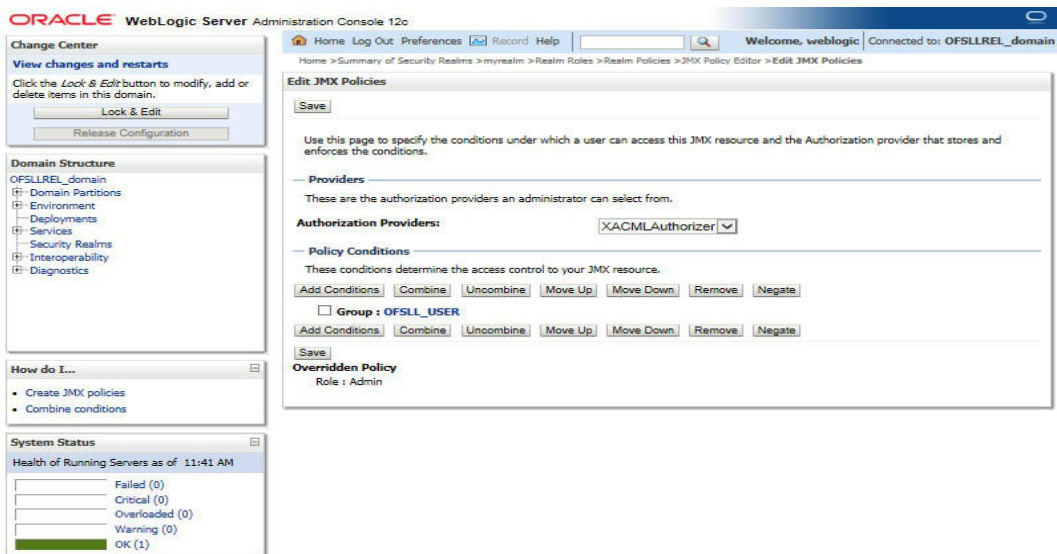


14. For Predicate List, select Group for configuration. Click 'Next'.



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

The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar contains sections for Change Center, Domain Structure, How do I..., and System Status. The main content area is titled 'Settings for myrealm' and includes tabs for Configuration, Users and Groups, Roles and Policies, Credential Mappings, Providers, and Migration. Under the Providers tab, the 'Password Validation' sub-tab is active. A table lists the Password Validation Providers:

Name	Description	Version
SystemPasswordValidator	Password composition checks	1.0

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

The screenshot shows the configuration page for the SystemPasswordValidator provider. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Settings for SystemPasswordValidator' and includes tabs for Configuration, Common, and Provider Specific. The 'Common' tab is active, displaying basic information about the provider:

Name:	SystemPasswordValidator	The name of this System Password Validation provider. <a href="#">More Info...</a>
Description:	Password composition checks	A short description of the System Password Validator provider. <a href="#">More Info...</a>
Version:	1.0	The version number of the System Password Validator provider. <a href="#">More Info...</a>

4. Click **Provider Specific** Tab.



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

**Reject if Password Contains the User Name Reversed** To determine whether the password can contain or be equal to the reverse username. This check will be case insensitive. If the value is "true", the password must not contain or be equal to the reverse username. [More Info...](#)

**Password Length Policies**

**Minimum Password Length:**  Specifies the minimum number of characters that the password may contain. Note: If the Default Authentication provider is configured in the realm, make sure that this number is consistent with the one configured for that provider. [More Info...](#)

**Maximum Password Length:**  Specifies the maximum number of characters that the password may contain. To be accepted, the password may not contain a greater number of characters than the value specified. Specifying 0 results in no restriction on password length. [More Info...](#)

**Character Policies**

**Maximum Instances of Any Character:**  Specifies the maximum number of times any one character may appear in the password. [More Info...](#)

**Maximum Consecutive Characters:**  Specifies the maximum number of times that a character may appear consecutively in the password. [More Info...](#)

**Minimum Number of Alphabetic Characters:**  Specifies the minimum number of alphabetic characters that a password must contain. [More Info...](#)

**Minimum Number of Numeric Characters:**  Specifies the minimum number of numeric characters that must appear in the password. [More Info...](#)

**Minimum Number of Lower Case Characters:**  Specifies the minimum number of lowercase characters that a password must contain. [More Info...](#)

**Minimum Number of Upper Case Characters:**  Specifies the minimum number of uppercase characters that a password must contain. [More Info...](#)

**Minimum Number of Non-Alphanumeric Characters:**  Specifies the minimum number of non-alphanumeric characters (also known as special characters, such as %, \*, #, or ;) that must appear in the password. [More Info...](#)

**Minimum Number of Non-Alphabetic Characters:**  Specifies the minimum number of numeric or special characters (such as %, \*, #, or ;) that a password must contain. [More Info...](#)

- Click 'Save'.

## 4.2 Configuring User Lockout Policy

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

**ORACLE WebLogic Server Administration Console 12c**

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: OFSLLREL\_domain

Home > Summary of Security Realms > myrealm

**Settings for myrealm**

Configuration Users and Groups Roles and Policies Credential Mappings Providers Migration

General RDBMS Security Store **User Lockout** Performance

Click the **Lock & Edit** button in the Change Center to modify the settings on this page.

Password guessing is a common type of security attack. In this type of attack, a hacker attempts to log in to a computer using various combinations of usernames and passwords. WebLogic Server provides a set of attributes to protect user accounts from intruders. This page allows us to define how user lockouts will be handled in this security realm.

**Lockout Enabled** Specifies whether the server locks users out when there are invalid login attempts on their account. [More Info...](#)

**Lockout Threshold:**  The maximum number of consecutive invalid login attempts that can occur before a user's account is locked out. [More Info...](#)

**Lockout Duration:**  The number of minutes that a user's account is locked out. [More Info...](#)

**Lockout Reset Duration:**  The number of minutes within which consecutive invalid login attempts cause a user's account to be locked out. [More Info...](#)

**Lockout Cache Size:**  The maximum number of invalid login records that the server can place in a cache. [More Info...](#)

**Lockout GC Threshold:**  The maximum number of invalid login records that the server keeps in memory. [More Info...](#)

- 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>)



Domain Domain\_OFSSLREL\_domain

\* User Name weblogic

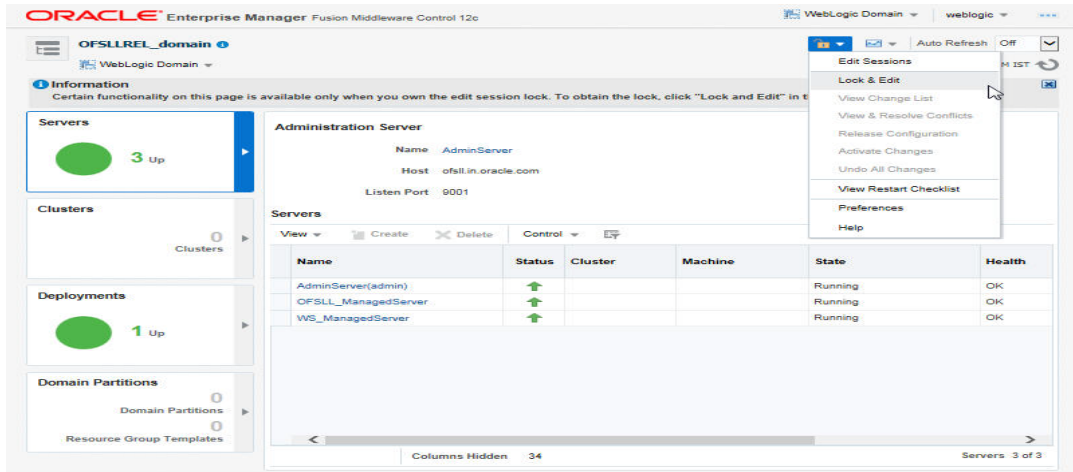
\* Password \*\*\*\*\*

Login to Partition

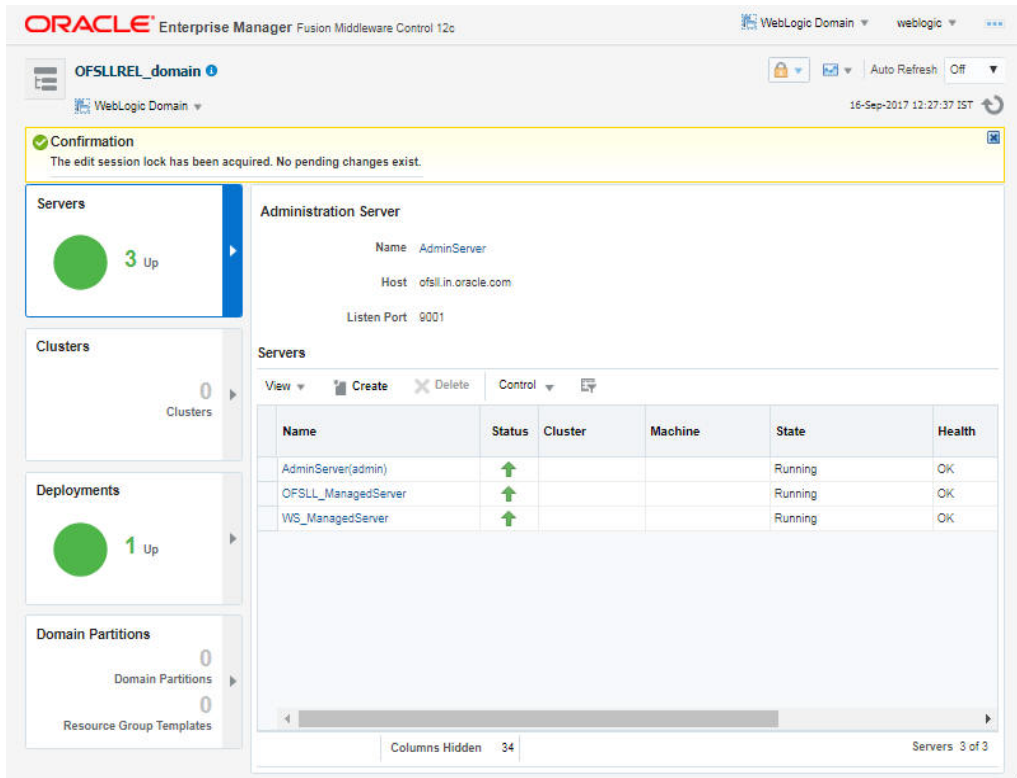
Sign in



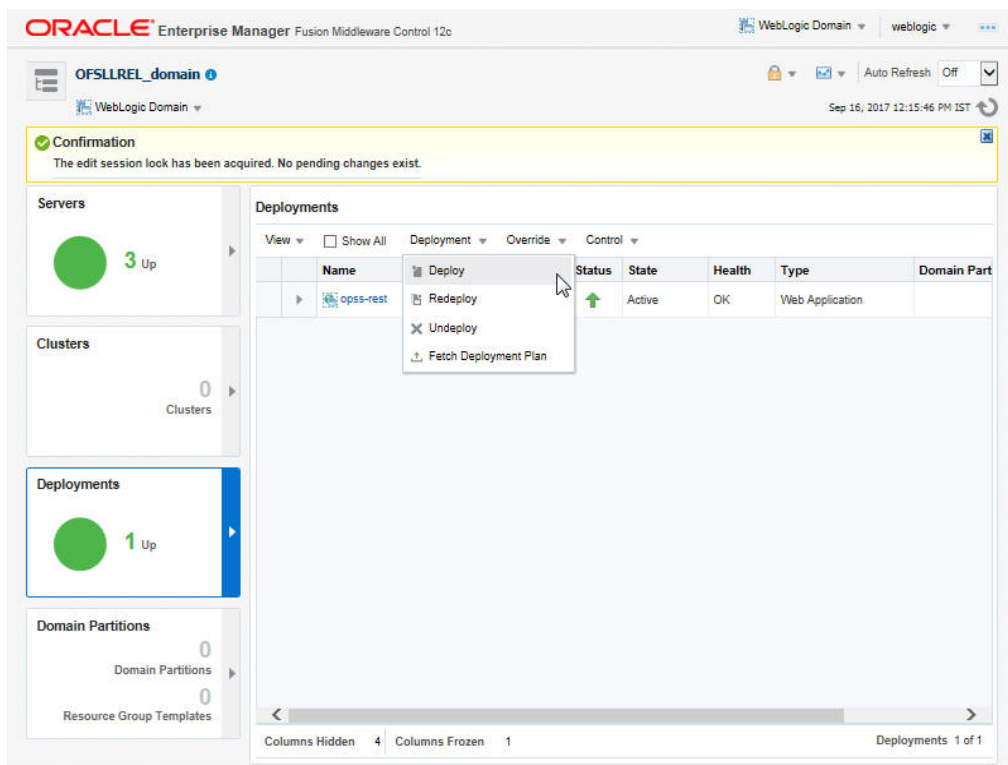
2. Click on 'Lock and Edit' as shown below.



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. ofssl\_149.ear. Choose the 'Deployment Plan' (if any).

**ORACLE** Enterprise Manager Fusion Middleware Control 12c weblogic ▾

**OFSLLREL\_domain**

Select Archive    Select Target    Application Attributes    Deployment Settings

**Deploy Java EE Application: Select Archive** Back Step 1 of 4 Next Cancel

**Scope**  
Select a scope that you want to deploy this application to Global ▾

**Archive or Explored Directory**  
Java EE archives, Web Modules (WAR files), EJB Modules (EJB JAR files), Resource Adapter Modules (RAR files), Coherence Archives (GAR files), JDBC Modules, JMS Modules, and library files (Jar files) can be deployed. You can also deploy an exploded archive that is present on the server where Enterprise Manager is running.

Archive is on the machine where this Web browser is running. Archive Location

ofssl\_149.ear

Archive or exploded directory is on the server where Enterprise Manager is running.

**Deployment Plan**  
The deployment plan is a file that contains the deployment settings for an application. You can use a previously saved deployment plan for this application. Later in the deployment process, you can optionally edit the deployment plan and save it for a future deployment of this application. If you do not have a deployment plan, one will be created automatically during the deployment process when deployment configuration is done. The deployment plan is not applicable when you deploy a library.

Create a new deployment plan when deployment configuration is done.

Deployment plan is on the machine where this Web browser is running.

No file chosen

Deployment plan is on the server where Enterprise Manager is running.

**Information**  
Use this page to deploy Java EE applications that require Oracle Metadata Services (MDS) or that take advantage of the Oracle Application Development Framework (Oracle ADF).  
If your application is a SOA composite, use the SOA Compos deployment wizard.  
If your application is not a SOA composite or it does not require a MDS repository or ADF connections, then you can deploy your application using this wizard or the Oracle WebLogic Server Administration Console.

---

### Note

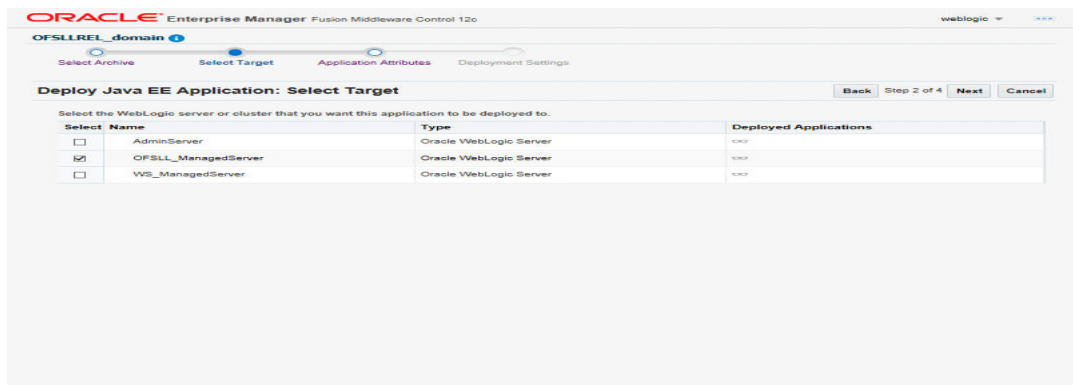
A deployment plan can be used to easily change an application's WebLogic Server configuration for a specific environment without modifying existing deployment descriptors.

---

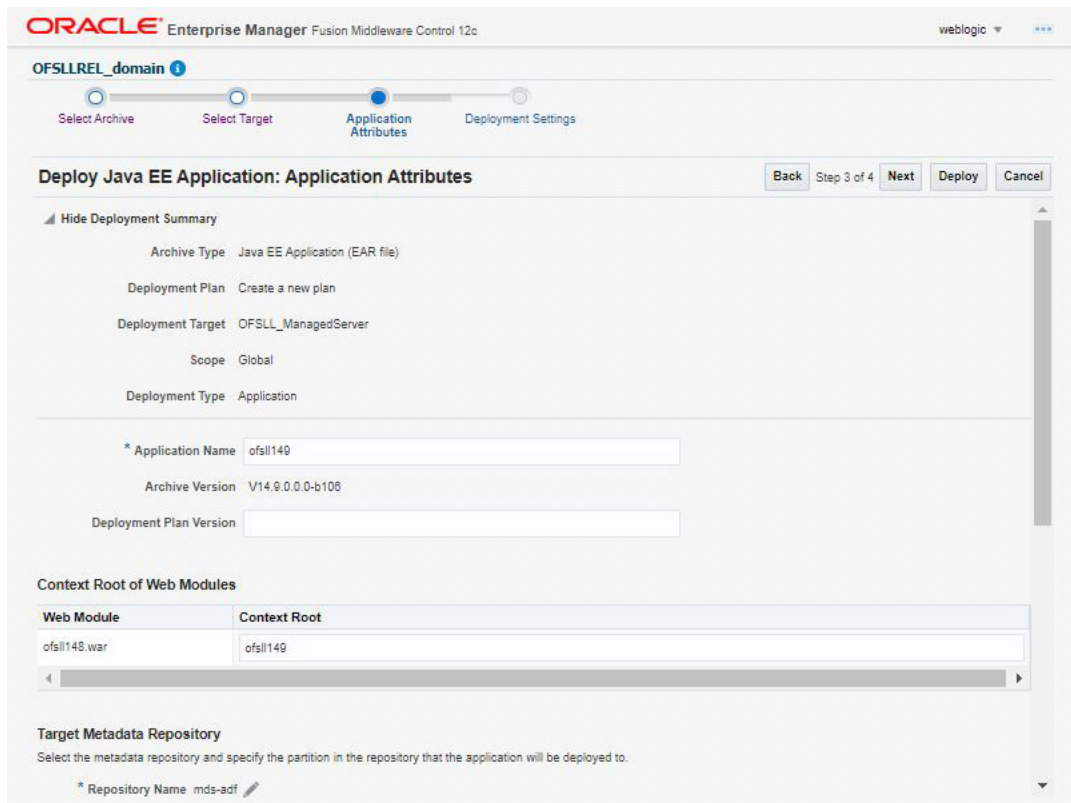
## Sample plan.xml

```
<?xml version='1.0' encoding='UTF-8'?>
<deployment-plan xmlns="http://xmlns.oracle.com/weblogic/deployment-plan" xmlns:xsi="http://www.w3.org/2001/XMLSchema"
<application-name>ofsslrel</application-name>
<variable-definition>
  <variable>
    <name>Web_ofsslrel_contextRoot</name>
    <value>ofsslrel</value>
  </variable>
</variable-definition>
<module-override>
  <module-name>ofsslrel.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_ofsslrel_contextRoot</name>
      <xpath>/application/module/web/[context-root="ofsslrel"]/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>ofsslrel.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>
</deployment-plan>
```

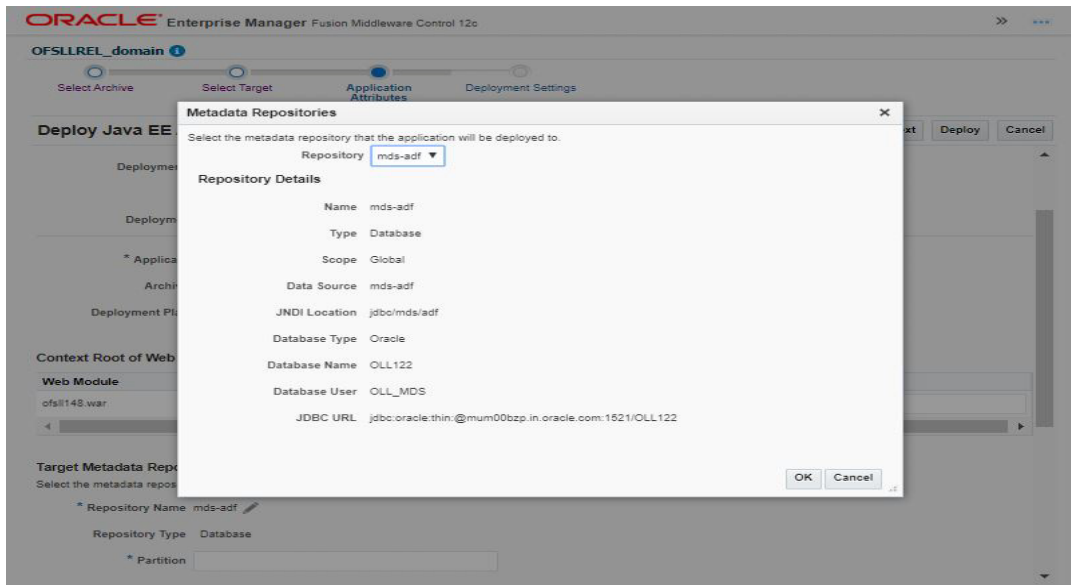
6. Click 'Next'. The following window is displayed.



7. Check target server as per the requirement 'OFSSL\_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'.

**ORACLE** Enterprise Manager Fusion Middleware Control 12c weblogic ▾ ⋮

OFSLLREL\_domain ⓘ

Select Archive    Select Target    **Application Attributes**    Deployment Settings

**Deploy Java EE Application: Application Attributes** Back Step 3 of 4 Next Deploy Cancel

**Target Metadata Repository**  
Select the metadata repository and specify the partition in the repository that the application will be deployed to.

\* Repository Name  ✎

Repository Type Database

\* Partition

**Distribution**

Install and start application (servicing all requests)  
 Install and start application in administration mode (servicing only administration requests)  
 Install only. Do not start.

▲ **Other Options**

**Application Source Accessibility**

Use the defaults defined by the deployment's targets. Recommended selection.  
 Copy this application onto every target. During deployment, the files will be copied automatically to the managed servers to which the application is targeted.  
 Make the application accessible from the source location that it will be deployed on. You must ensure that each target can reach the location.

**Deployment Plan Source Accessibility**

Use the same accessibility as the application.  
 Copy the deployment plan onto every target. During deployment, the files will be copied automatically to the managed servers to which the application is targeted.  
 Make the deployment plan accessible from the source location that it will be deployed on. You must ensure that each target can reach the location.

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

**ORACLE** Enterprise Manager Fusion Middleware Control 12c weblogic ▾ ⋮

OFSLLREL\_domain ⓘ

Select Archive    Select Target    Application Attributes    **Deployment Settings**

**Deploy Java EE Application: Deployment Settings** Back Step 4 of 4 Next Deploy Cancel

▲ **Hide Deployment Summary**

Archive Type Java EE Application (EAR file)

Deployment Plan Create a new plan

Deployment Target OFSLL\_ManagedServer

Scope Global

Deployment Type Application

Application Name ofsl149

Version V14.9.0.0.0-b108

Context Root ofsl149

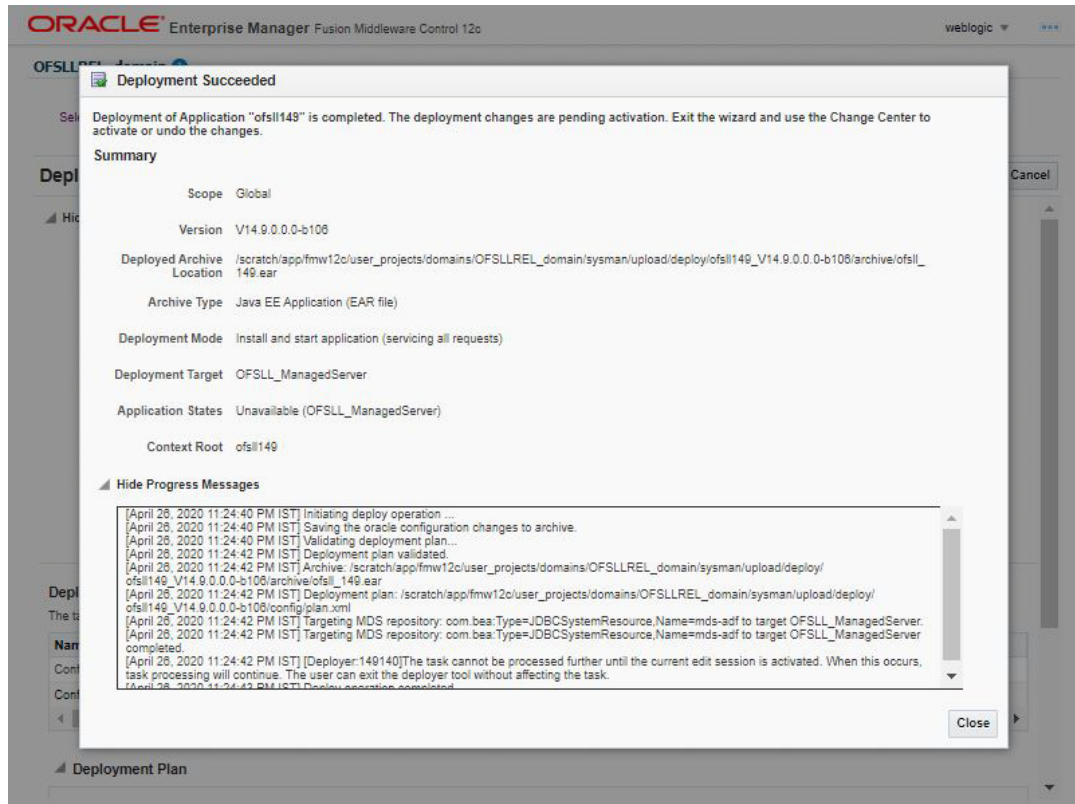
Deployment Mode Install and start application (servicing all requests)

**Deployment Tasks**  
The table below lists common tasks that you may wish to do before deploying the application.

Name	Go To Task	Description
Configure Web Modules	<span style="font-size: small;">✎</span>	Configure the Web modules in your application.
Configure Application Security	<span style="font-size: small;">✎</span>	Configure application policy migration, credential migration and other security behavior.

▲ **Deployment Plan**

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.

The screenshot displays the 'Settings for OFSSL\_ManagedServer' configuration page. The 'General' tab is selected, and the 'SSL' sub-tab is active. The 'Listen Port Enabled' checkbox is checked, and the 'SSL Listen Port' is set to 9503. The 'Listen Port' is set to 9003. The 'Client Cert Proxy Enabled' checkbox is unchecked.

Property	Value	Description
Name	OFSSL_ManagedServer	An alphanumeric name for this server instance. <a href="#">More Info...</a>
Template	(No value specified) <a href="#">Change</a>	The template used to configure this server. <a href="#">More Info...</a>
Machine	(None)	The WebLogic Server host computer (machine) on which this server is meant to run. <a href="#">More Info...</a>
Cluster	(Stand-Alone)	The cluster, or group of WebLogic Server instances, to which this server belongs. <a href="#">More Info...</a>
Listen Address		The IP address or DNS name this server uses to listen for incoming connections. For example, enter 12.34.5.67 or mymachine, respectively. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> Listen Port Enabled		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. <a href="#">More Info...</a>
Listen Port	9003	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. <a href="#">More Info...</a>
<input checked="" type="checkbox"/> SSL Listen Port Enabled		Indicates whether the server can be reached through the default SSL listen port. <a href="#">More Info...</a>
SSL Listen Port	9503	The TCP/IP port at which this server listens for SSL connection requests. <a href="#">More Info...</a>
<input type="checkbox"/> Client Cert Proxy Enabled		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. <a href="#">More Info...</a>

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

---

### Note

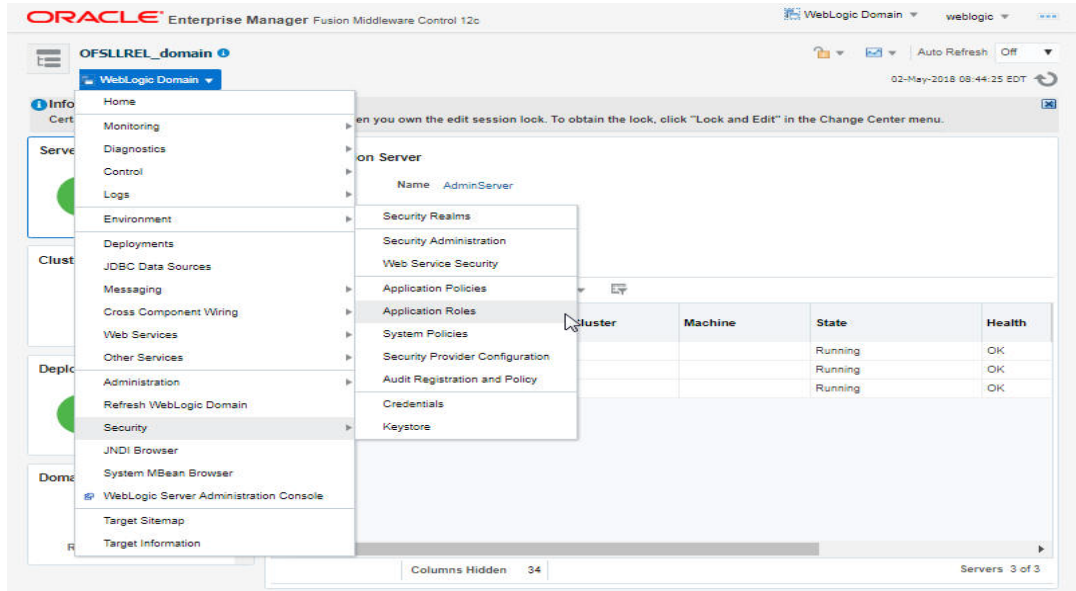
It is recommended to disable http protocol.

---

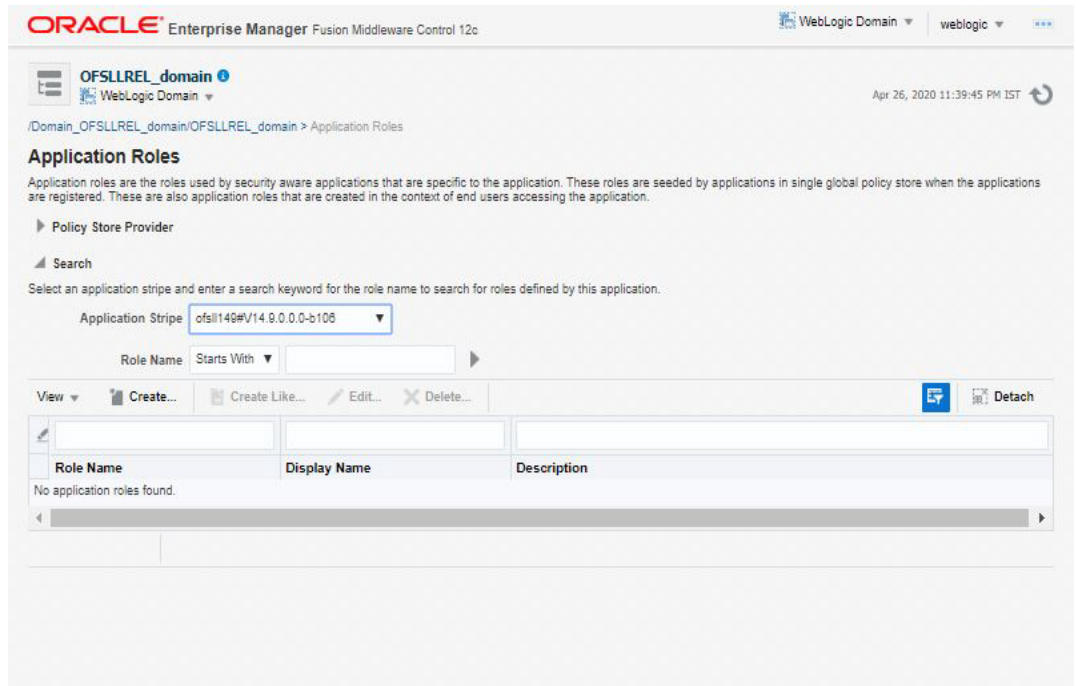
# 7. Mapping Enterprise Group with Application Role

**Follow the below steps to add a 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:



- Select the 'Role Name'. Membership details of the selected Role Name are displayed under Membership for "role\_name"..

**Application Roles**

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in single global policy store when the applications are registered. These are also application roles that are created in the context of end users accessing the application.

Policy Store Provider

Search

Select an application stripe and enter a search keyword for the role name to search for roles defined by this application.

Application Stripe: ofsl149#V14.9.0.0.0-b106

Role Name: Starts With

Role Name	Display Name	Description
OFSSL_USER	OFSLL USER	

Membership for OFSLL\_USER

Principal	Display Name	Type	Description
DEMOSUPR		User	

- Click 'Edit'. The following window is displayed.

**Edit Application Role : OFSLL\_USER**

Role (or Enterprise Role) is the group of users designed at the enterprise level and typically used to assign a privilege or permission. A role can also contain other roles as members.

General

Application Stripe: ofsl149#V14.9.0.0.0-b106

Role Name: OFSLL\_USER

Display Name: OFSLL USER

Description:

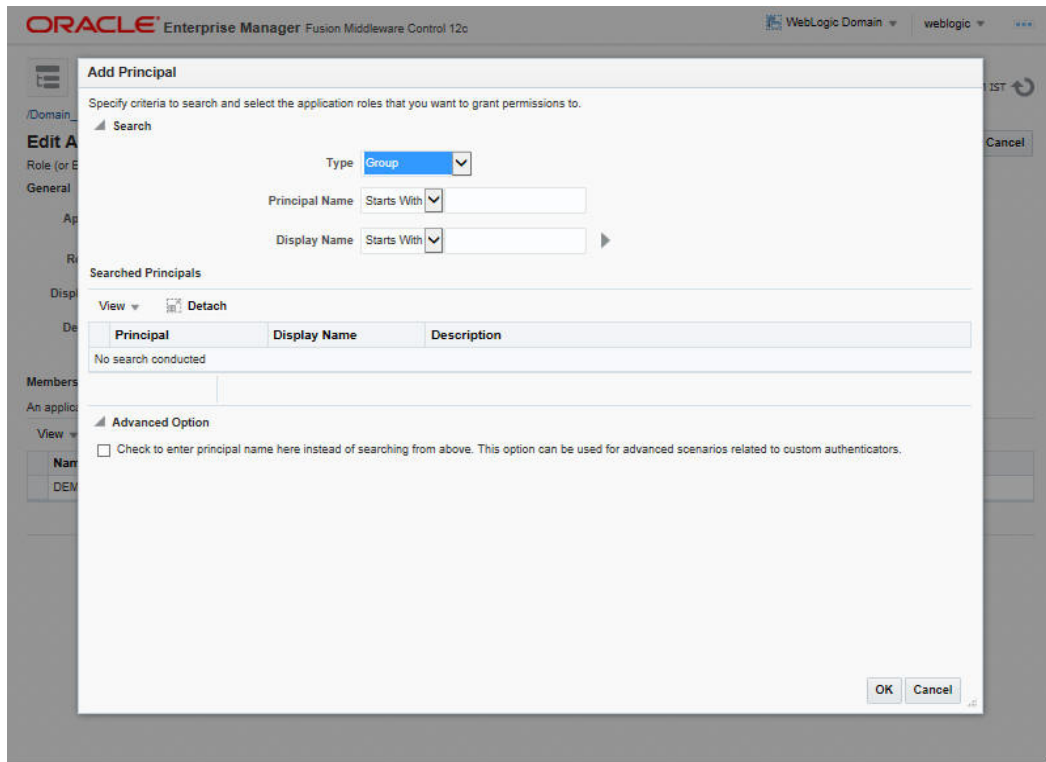
Members

An application role may need to be mapped to users or groups defined in enterprise LDAP server, or the role can be mapped to other application roles.

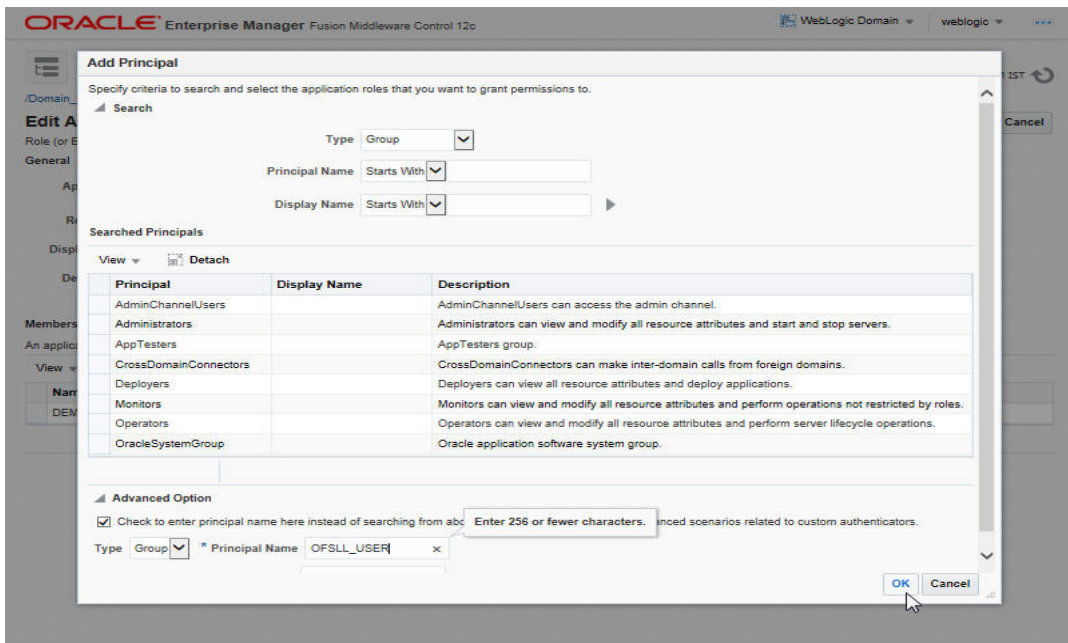
Name	Display Name	Type
DEMOSUPR		User

- 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'.

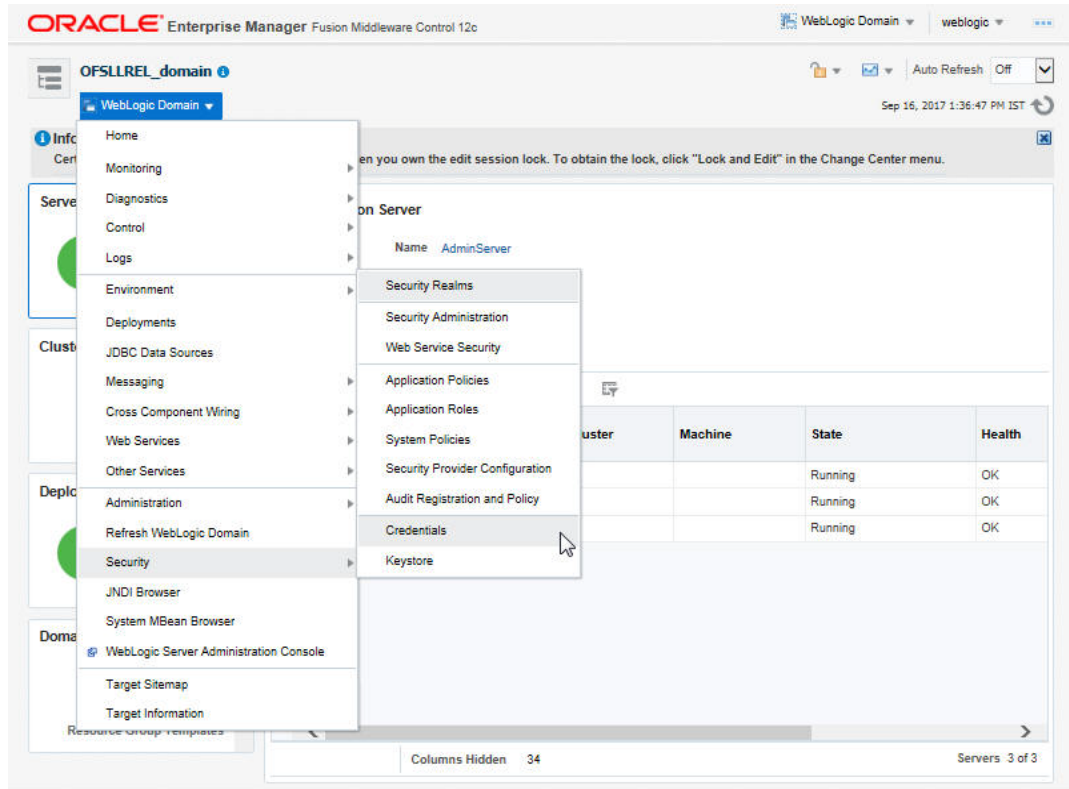
The screenshot shows the 'Edit Application Role' page for 'OFSSL\_USER' in the 'OFSLLREL\_domain'. The page includes a breadcrumb trail, a title bar with 'OK' and 'Cancel' buttons, and a description of the role. The 'General' section contains fields for 'Application Stripe' (ofssl149#V14.9.0.0.0-b106), 'Role Name' (OFSSL\_USER), 'Display Name' (OFSSL USER), and a 'Description' text area. The 'Members' section includes a table with columns 'Name', 'Display Name', and 'Type', listing 'DEMOSUPR' (User) and 'OFSSL\_USER' (Group).

11. The following window is displayed with the confirmation message as 'The Application role of 'group\_name' has been updated'.

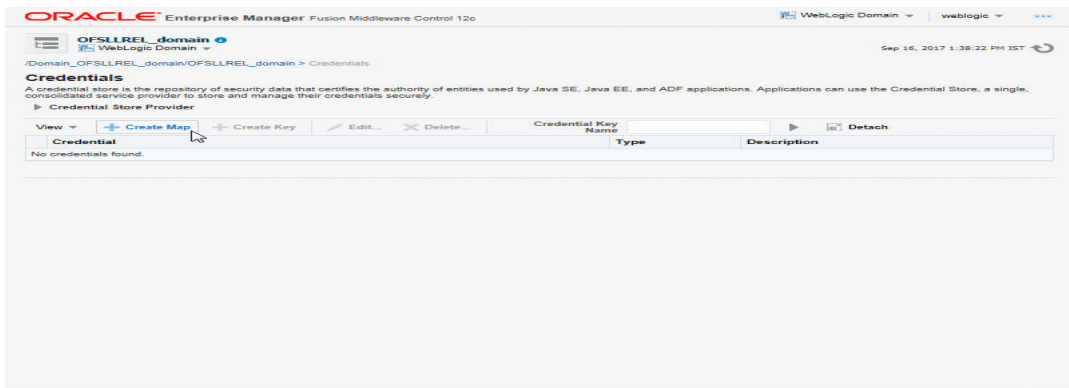
The screenshot shows the 'Application Roles' page for 'OFSSL\_USER' in the 'OFSLLREL\_domain'. A yellow information banner at the top states: 'An application role OFSSL\_USER has been updated.' Below this, the 'Application Roles' section includes a search area with 'Application Stripe' (ofssl149#V14.9.0.0.0-b106) and 'Role Name' (Starts With) fields. A table below the search area lists the role 'OFSSL\_USER' with 'Display Name' 'OFSSL USER' and 'Description'. The 'Membership for OFSSL\_USER' section contains a table with columns 'Principal', 'Display Name', 'Type', and 'Description', listing 'DEMOSUPR' (User) and 'OFSSL\_USER' (Group).

## 8. Configuring JNDI name for HTTP Listener

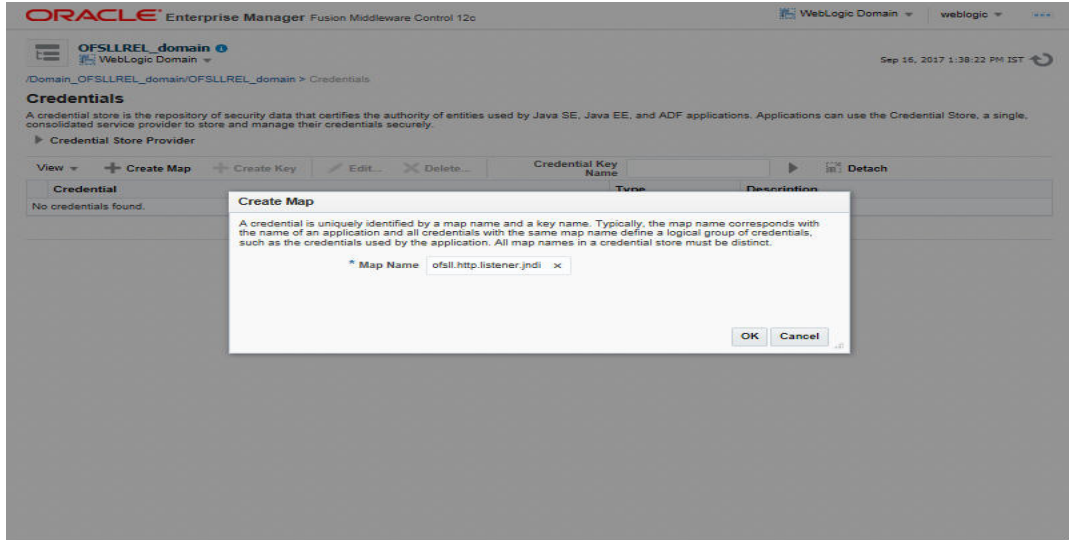
1. Click 'WebLogic Domain' on the right panel. Select Security > Credentials.



2. Click 'Credentials'. The following window is displayed.

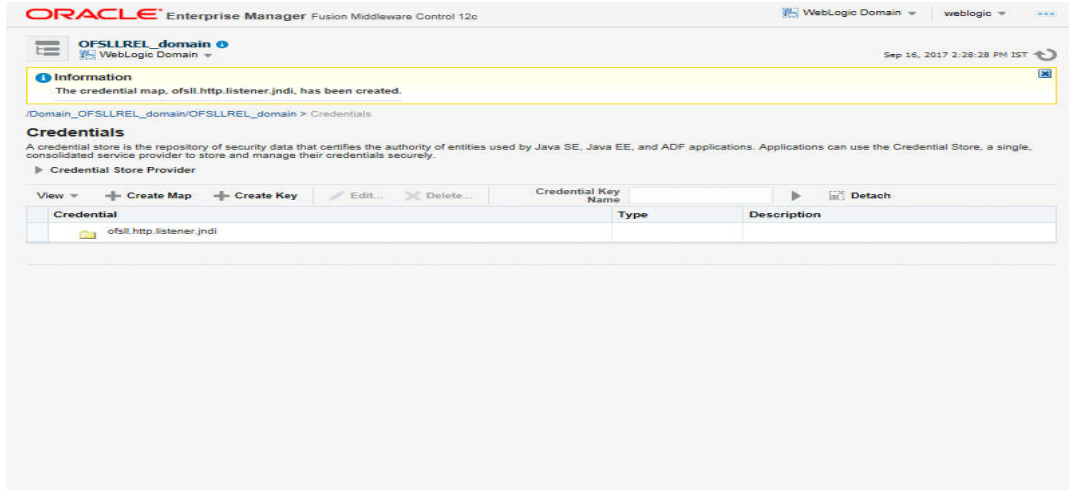


3. Click 'Create Map'. The following window is displayed.

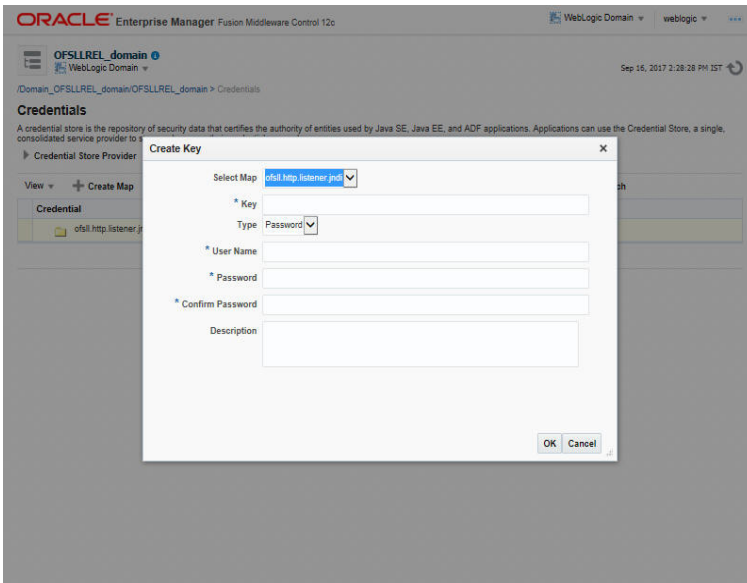


4. Enter Map name as 'ofssl.http.listener.jndi'.

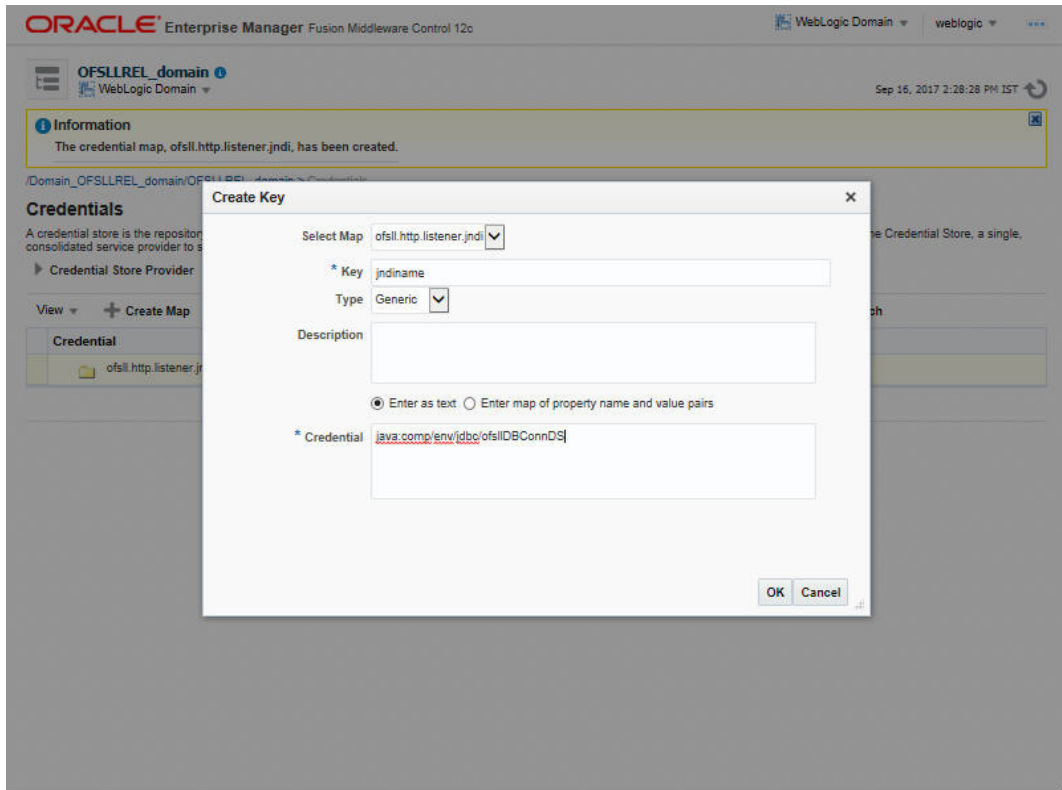
5. Click 'OK'. The following window is displayed.



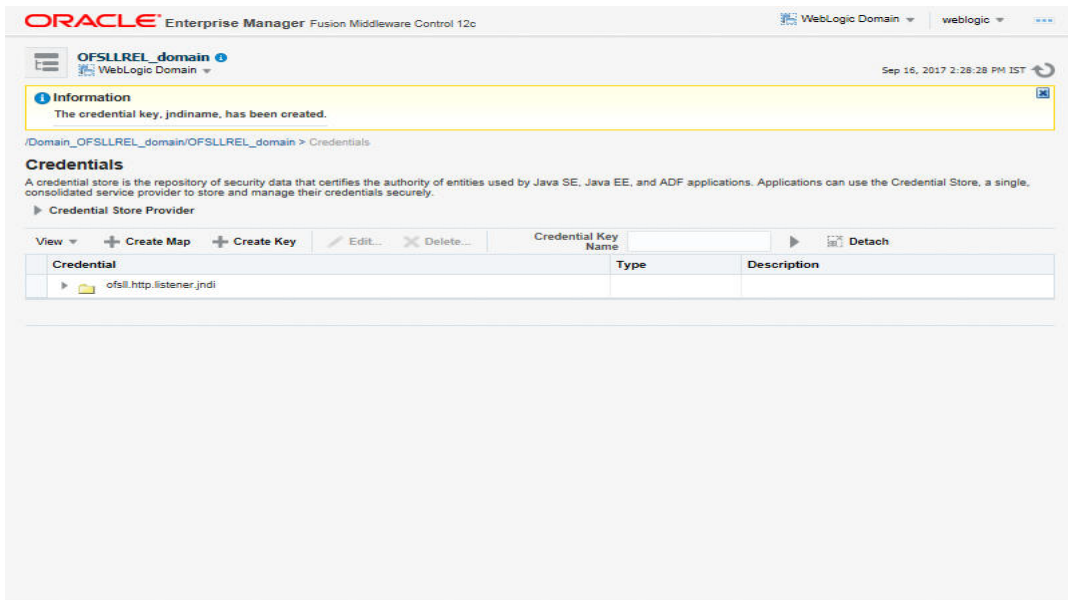
6. Click 'Create Key' Button. The following window is displayed.



7. Enter the following details as per your requirement.
  - Key: jndiname
  - Credential: java:comp/env/jdbc/ofslIDBConnDS
  - 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](#)

---

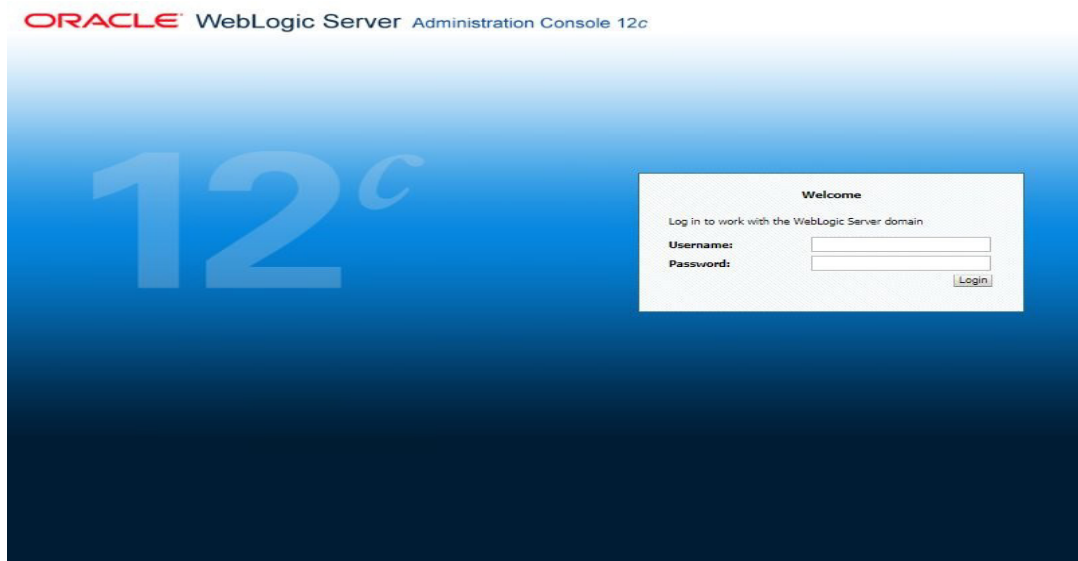
### Note

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

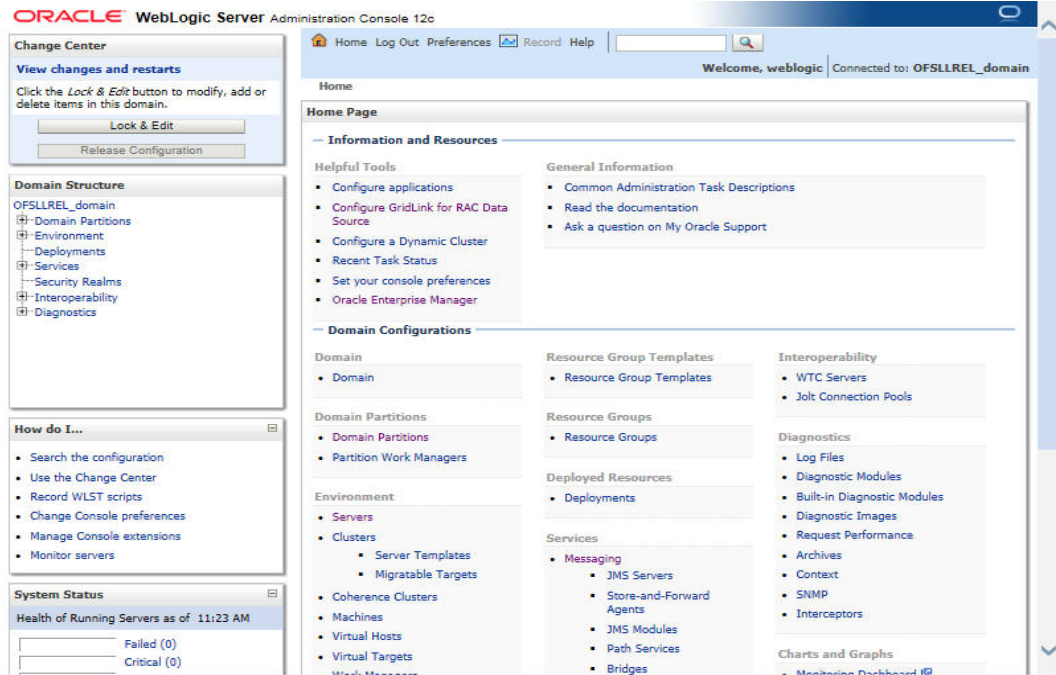
---

### 9.1 Create Data Sources for AQ-JMS Bridge

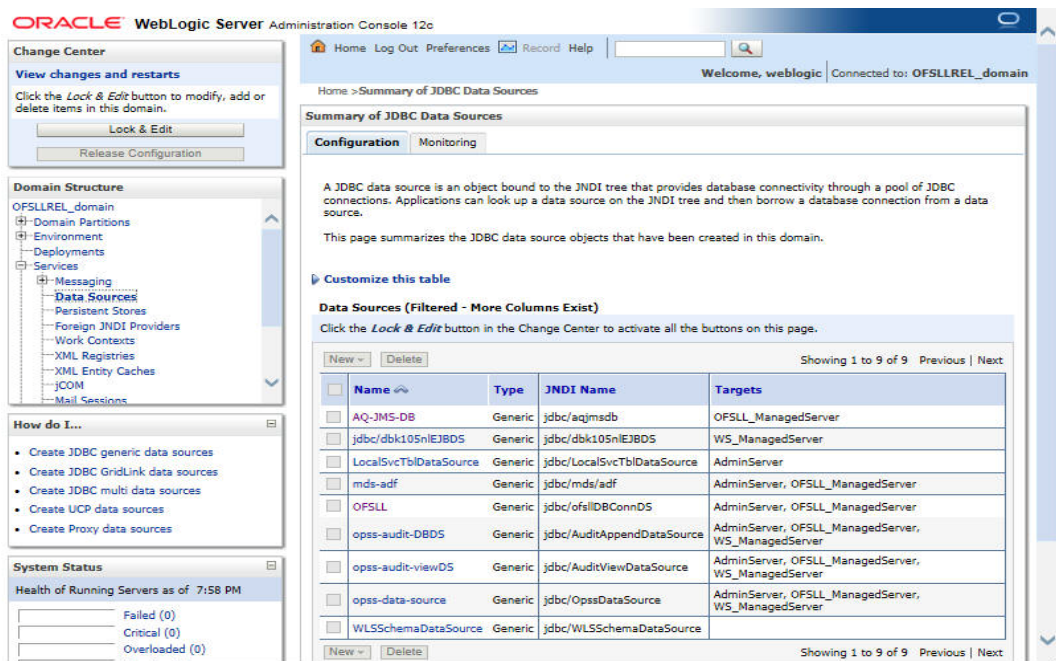
1. Login to Oracle Weblogic 12c console (<http://hostname:port/console>).



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



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



- Click 'Lock & Edit' button on the left panel. Click 'New' on right panel and select 'Generic Data Source'.

The screenshot shows the Oracle WebLogic Server Administration Console. On the left, the 'Change Center' panel has 'Lock & Edit' selected. The 'Domain Structure' tree shows 'Data Sources' expanded. The main area displays the 'Summary of JDBC Data Sources' page with a table of existing data sources. A tooltip is visible over the 'Generic Data Source' row in the table.

Generic Data Source	Type	JNDI Name	Targets
GridLink Data Source	Generic	jdbc/aqjmsdb	OFSLL_ManagedServer
Multi Data Source	Generic	jdbc/dbk105n1EJBDS	WS_ManagedServer
Proxy Data Source	Generic	jdbc/LocalSvcTblDataSource	AdminServer
UCP Data Source	Generic	jdbc/mds/adf	AdminServer, OFSLL_ManagedServer
OFSLL	Generic	jdbc/ofslDBConnDS	AdminServer, OFSLL_ManagedServer
opss-audit-DBDS	Generic	jdbc/AuditAppendDataSource	AdminServer, OFSLL_ManagedServer, WS_ManagedServer
opss-audit-viewDS	Generic	jdbc/AuditViewDataSource	AdminServer, OFSLL_ManagedServer, WS_ManagedServer
opss-data-source	Generic	jdbc/OpssDataSource	AdminServer, OFSLL_ManagedServer, WS_ManagedServer
WLSSchemaDataSource	Generic	jdbc/WLSSchemaDataSource	

- The following window is displayed.

The screenshot shows the 'Create a New JDBC Data Source' dialog box. The 'JDBC Data Source Properties' section contains the following information:

- Name:** AQ-JMS-DB
- Scope:** Global
- JNDI Name:** jdbc/aqjmsdb
- Database Type:** Oracle

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

---

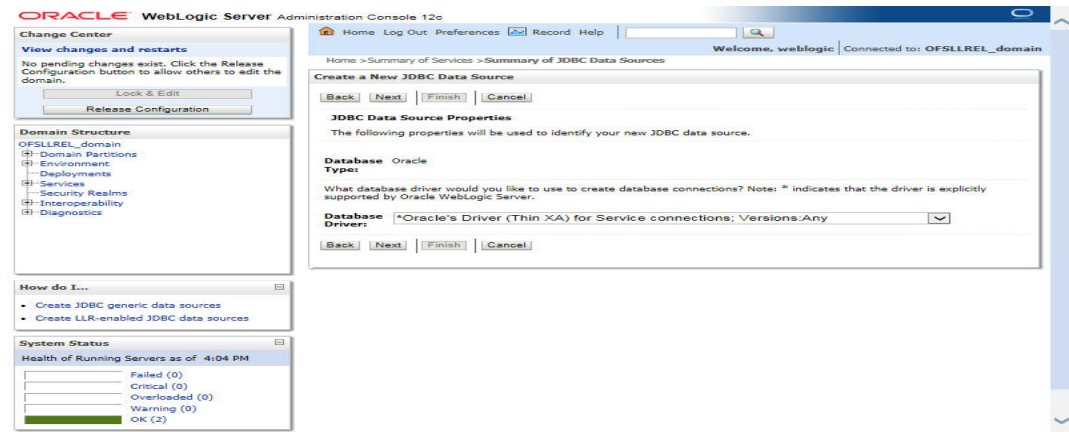
## Note

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

---

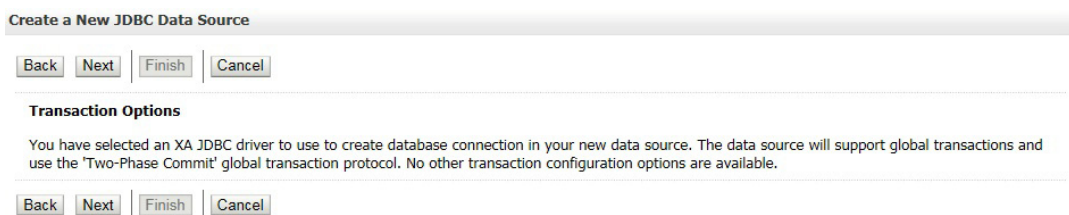
- Select 'Oracle' as Database Type.

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.

The screenshot displays the Oracle WebLogic Server Administration Console interface. The main window is titled "Create a New JDBC Data Source" and is part of the "Summary of JDBC Data Sources" page. The interface includes a navigation bar at the top with "Home", "Log Out", "Preferences", "Record", and "Help" options. A search bar and user information "Welcome, weblogic | Connected to: OFSSLREL\_domain" are also present. On the left side, there are several panels: "Change Center" with "View changes and restarts" and "Release Configuration" buttons; "Domain Structure" showing a tree view of the domain hierarchy; "How do I..." with links to "Create JDBC generic data sources" and "Create LLR-enabled JDBC data sources"; and "System Status" showing the health of running servers as of 8:07 PM, with 3 servers in an "OK" state. The main content area is a wizard with "Back", "Next", "Finish", and "Cancel" buttons. The "Connection Properties" section is active, with the following fields: "Database Name" (OLLDB), "Host Name" (ofssl.oracle.com), "Port" (1521), "Database User Name" (OFSSLREL), and "Password" (masked with dots). The "Additional Connection Properties" section shows "oracle.jdbc.DRCPConnectionClass" in a text box.

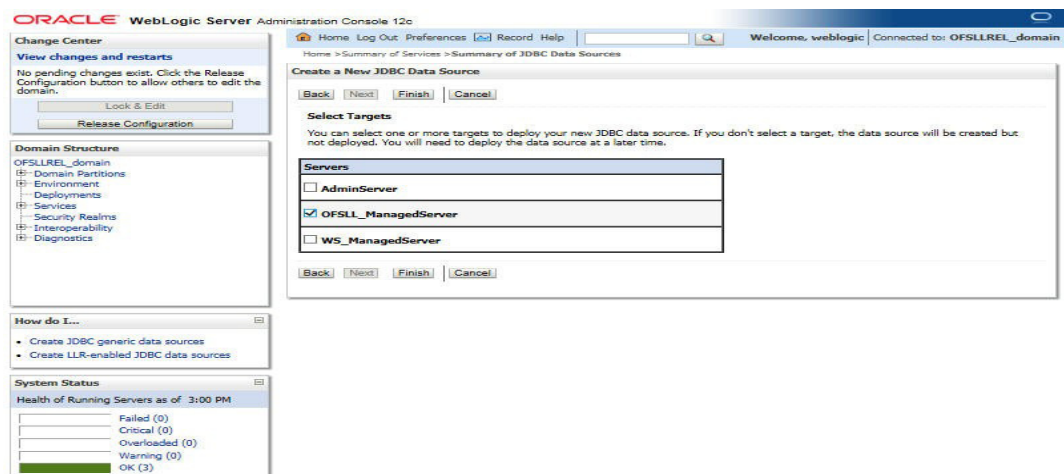
11. Enter the Database details.

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 'OFSSL\_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.

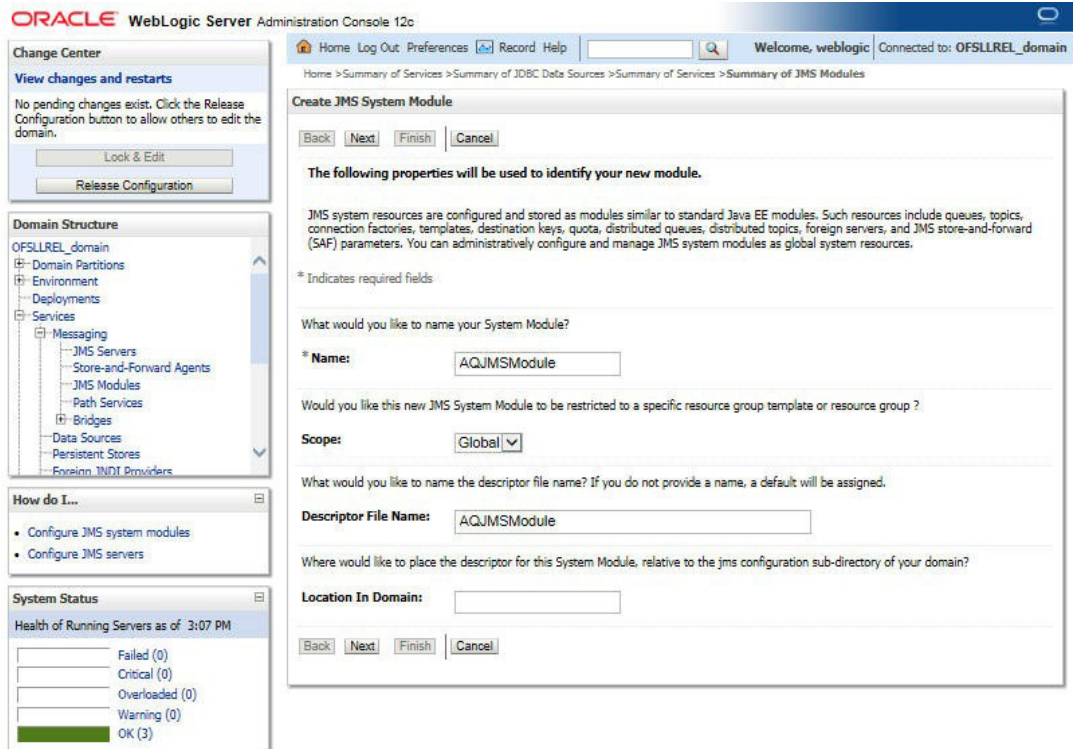
## 9.2 Configure MDB Flow

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.

The screenshot displays the Oracle WebLogic Server Administration Console 12c interface. The main content area shows the 'Summary of JMS Modules' page. The breadcrumb navigation is: Home > Summary of Services > Summary of JDBC Data Sources > Summary of Services > Summary of JMS Modules. The page title is 'Summary of JMS Modules'. Below the title, there is a paragraph explaining that JMS system resources are configured and stored as modules similar to standard Java EE modules. A 'Customize this table' link is present. Below that, there is a section titled 'JMS Modules (Filtered - More Columns Exist)' with a 'Lock & Edit' button. A table with columns 'Name' and 'Type' is shown, but it is empty with the message 'There are no items to display'. The left sidebar contains several panels: 'Change Center' with 'Lock & Edit' and 'Release Configuration' buttons; 'Domain Structure' showing a tree view with 'JMS Modules' selected; 'How do I...' with links to 'Configure JMS system modules' and 'Configure resources for JMS system modules'; and 'System Status' showing 'Health of Running Servers as of 3:03 PM' with a bar chart indicating 0 Failed, 0 Critical, 0 Overloaded, 0 Warning, and 3 OK servers.

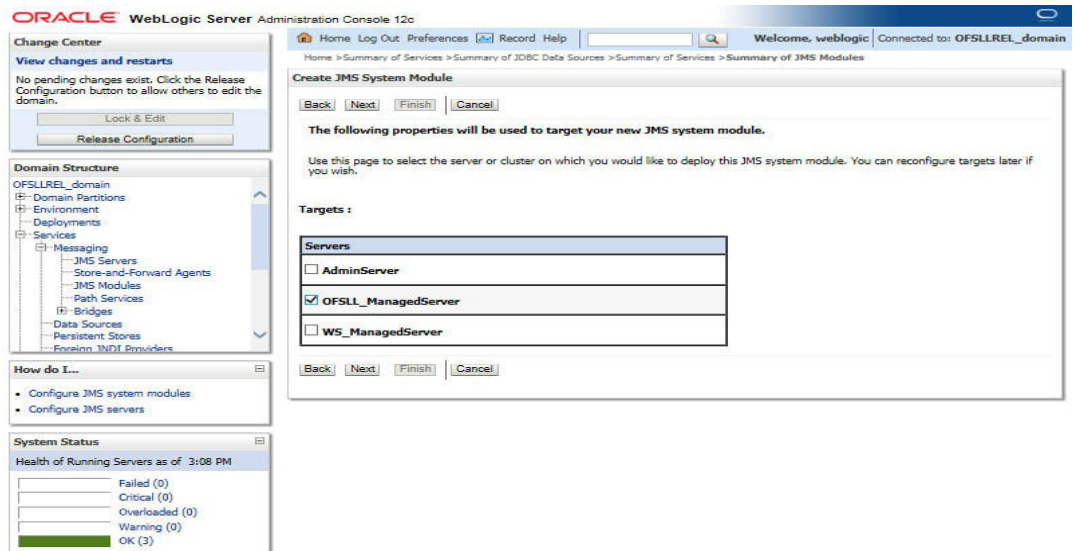
4. Click 'New'. The following screen is displayed.



5. Specify the following details:

- Name: AQJMSModule
- Descriptor File Name: AQJMSModule

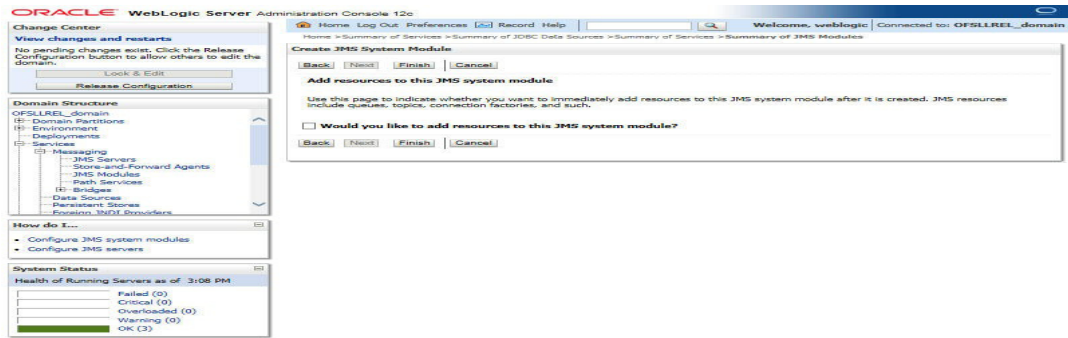
6. Click 'Next'. The following window is displayed.



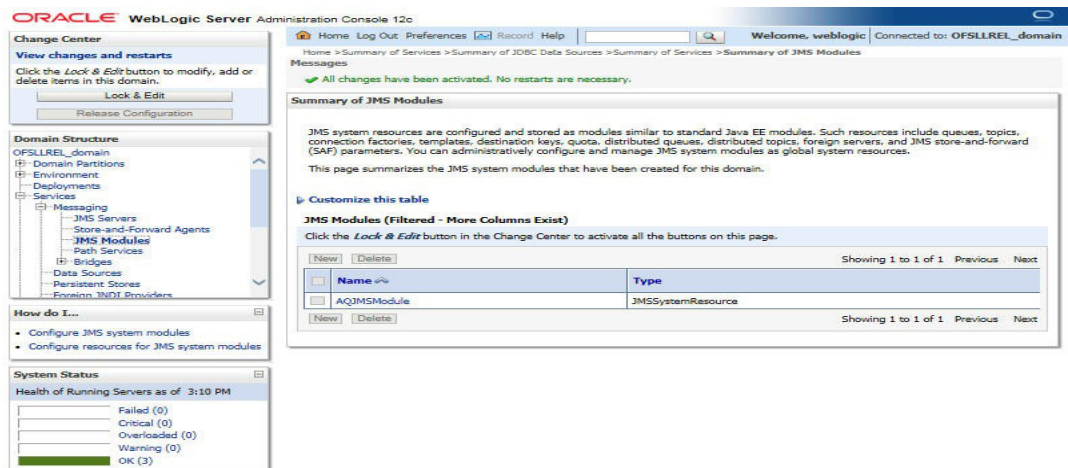
7. Select target servers as 'OFSLL\_ManagedServer'.



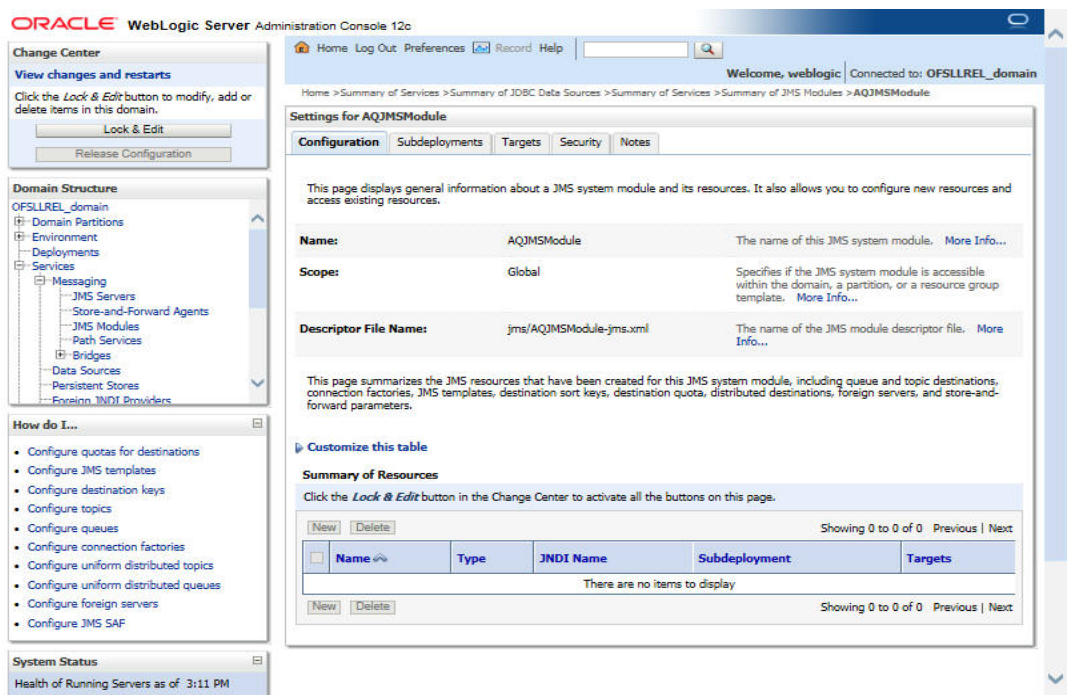
8. Click 'Next'. The following window is displayed.



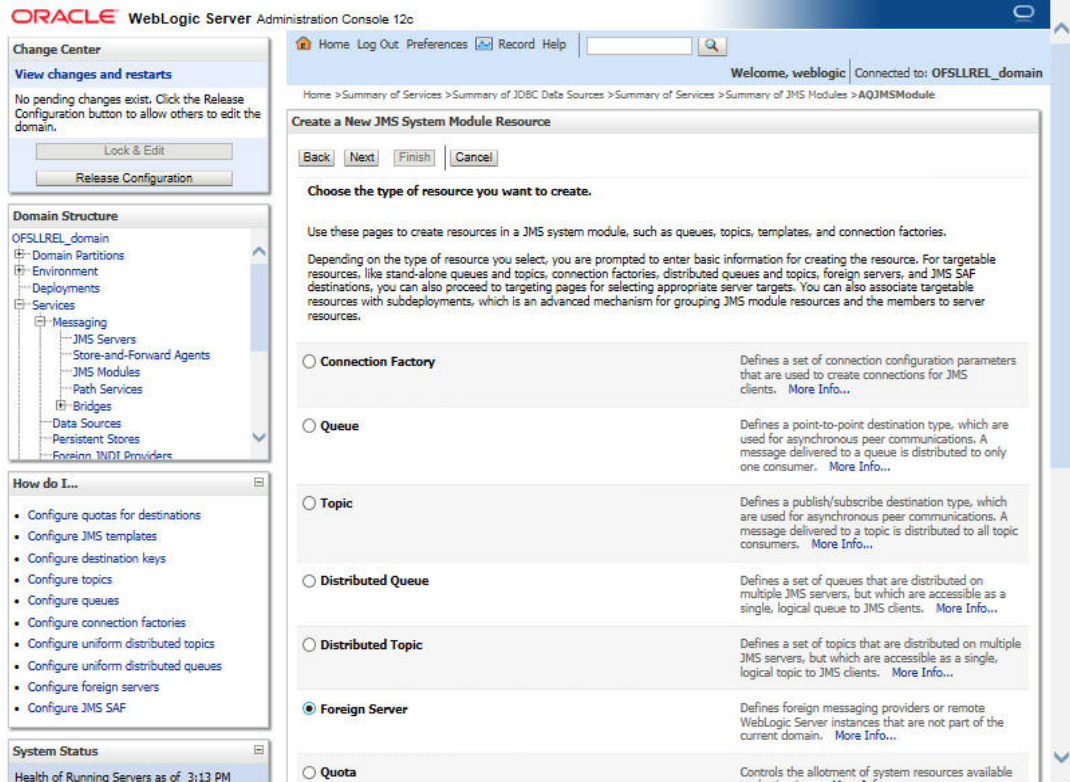
9. Click 'Finish' to activate the changes. The following window is displayed.



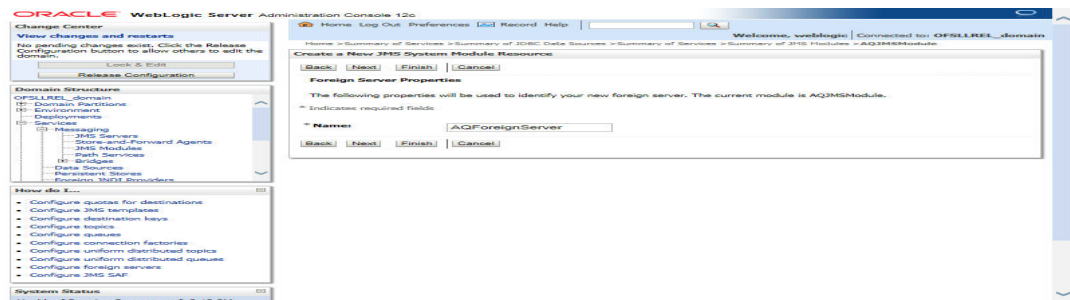
10. Click on the JMS Module that you created. The following window is displayed.



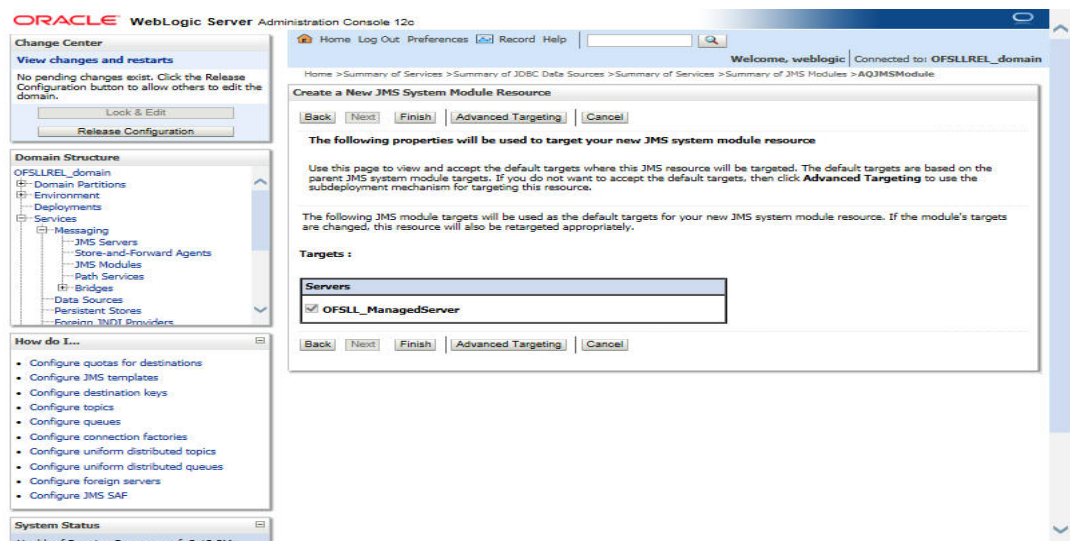
11. Click 'New' in 'Summary of Resources' section. The following window is displayed.



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.

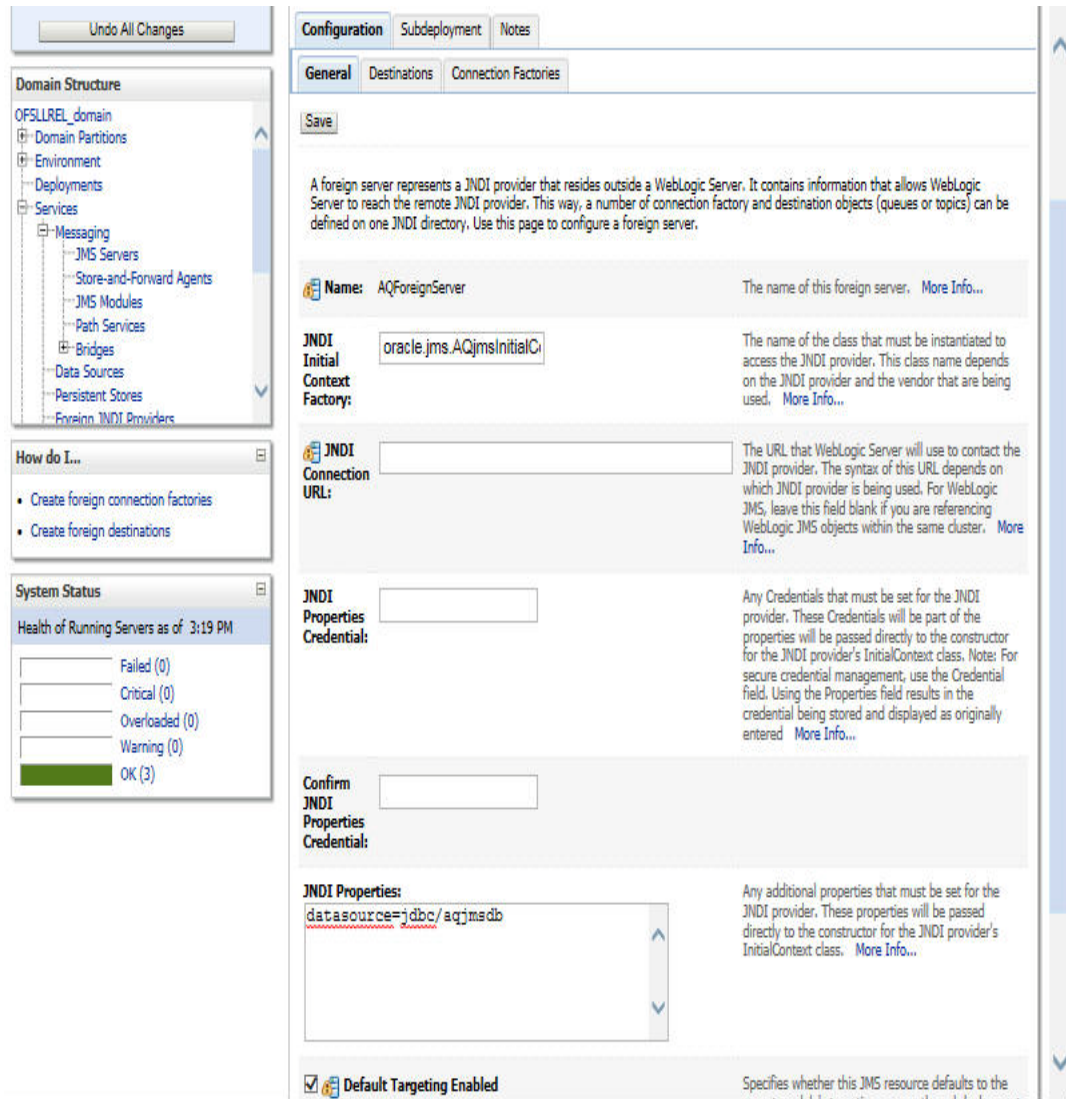


14. Click 'Finish' and activate the changes. The following window is displayed.

The screenshot shows the Oracle WebLogic Server Administration Console. The main content area is titled 'Settings for AQJMSModule' and includes a 'Configuration' tab. A message states: 'The foreign server was created successfully.' Below this, there is a 'Summary of Resources' table.

Name	Type	JNDI Name	Subdeployment	Targets
AQForeignServer	Foreign Server	N/A	Default Targeting	OFSLM_ManagedServer

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

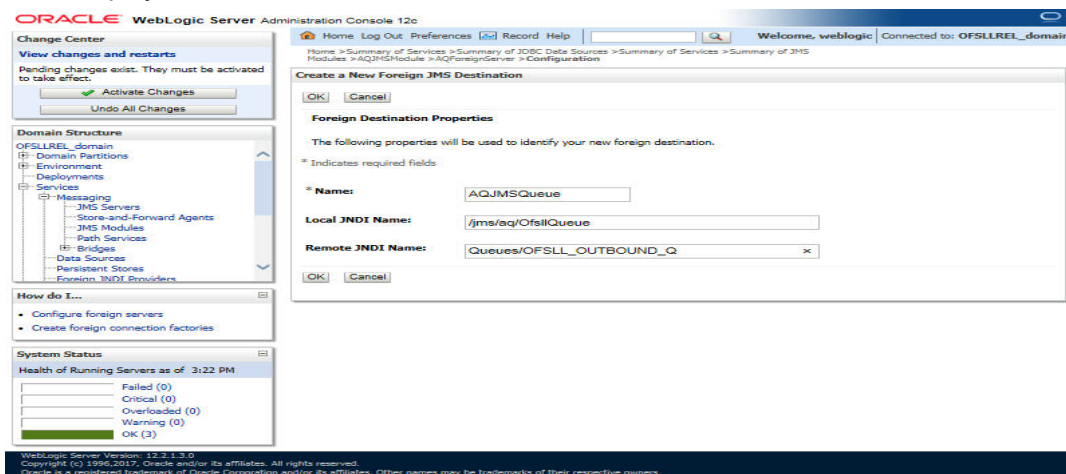


16. Specify the following details:

- Enter JNDI Initial Context Factory as 'oracle.jms.AQjmsInitialContextFactory'.
- JNDI Properties as 'datasource=jdbc/aqjmsdb'.
- Ensure 'Default Targeting Enabled' option is selected.

17. Click 'Save'.

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

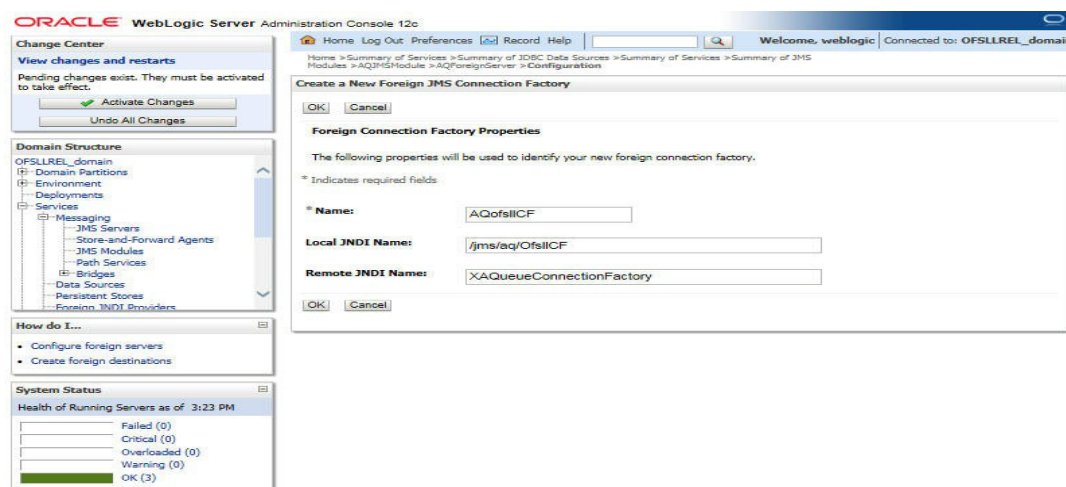


19. Specify the following details:

- 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.

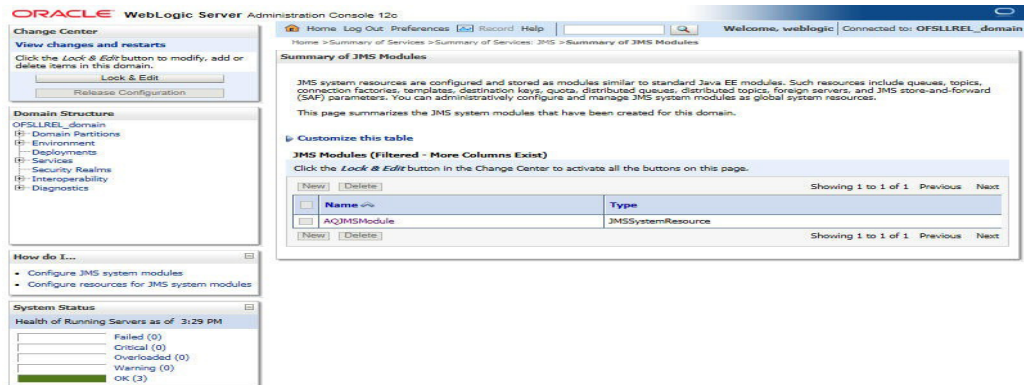
## 9.3 AQ-JMS Topic Setup

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.

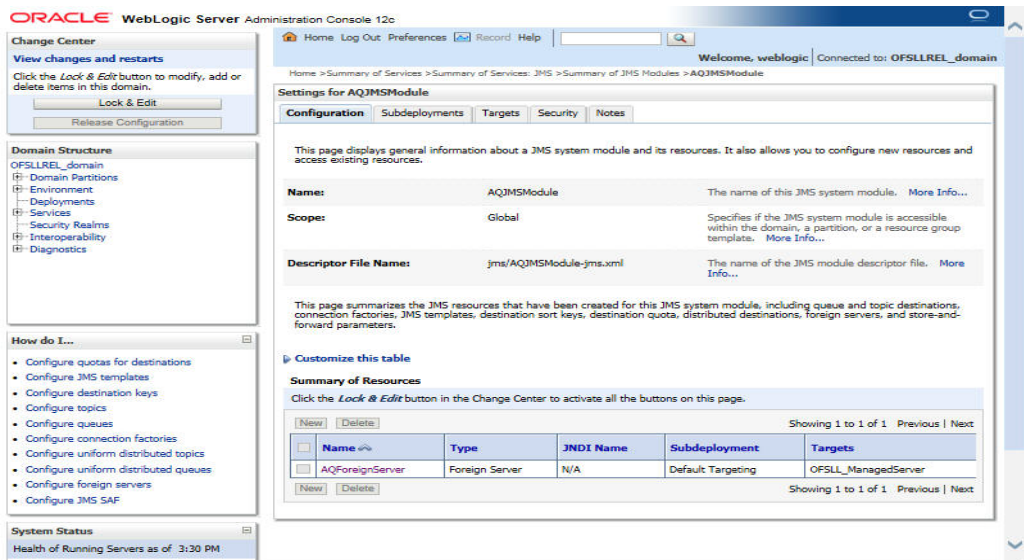
### 9.3.1 Create AQ-JMS Topic Bridge

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

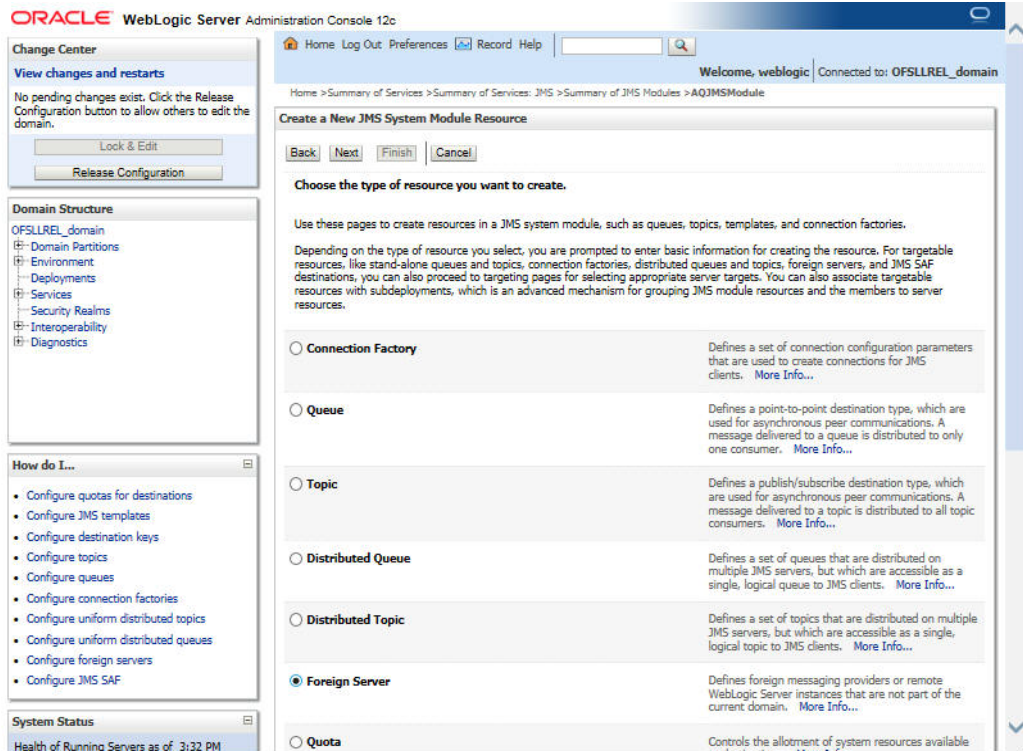
1. Login to Oracle Weblogic 12c console (<http://hostname:port/console>).
2. On the left pane, select Services > Messaging > JMS Modules. The following window is displayed.



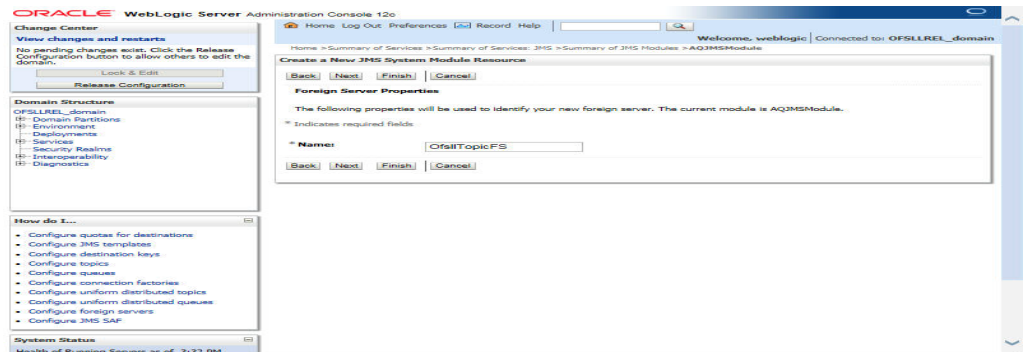
3. Click 'AQJMSModule'. The following window is displayed.



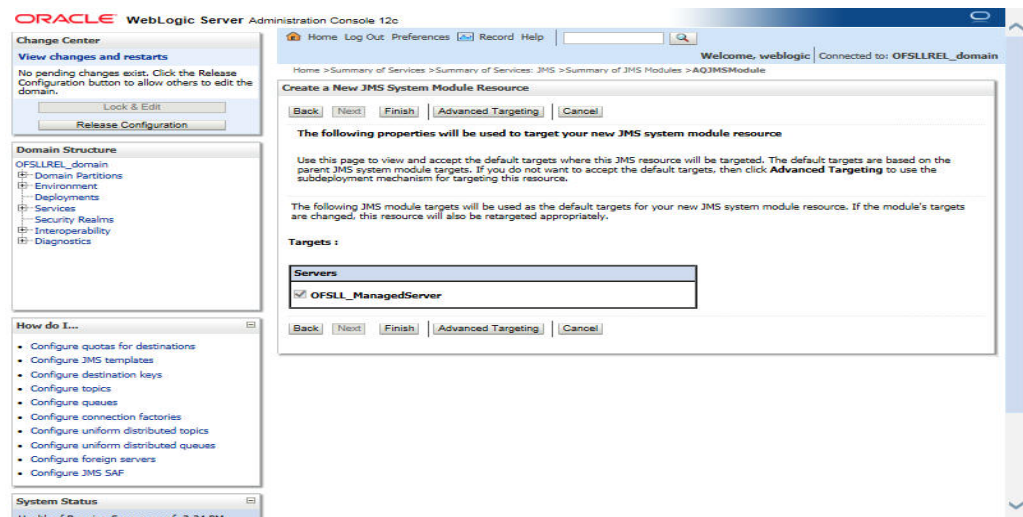
- In the Summary of Resources section, click 'New'. The following window is displayed.



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



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



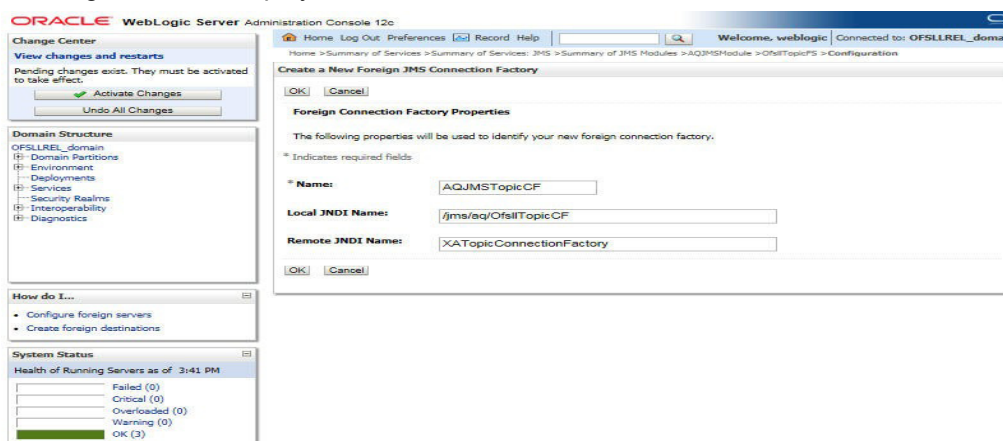
7. Click 'Finish' and activate the changes.
8. Click on the Foreign Server that you created. The following window is displayed.

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 Targeting 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

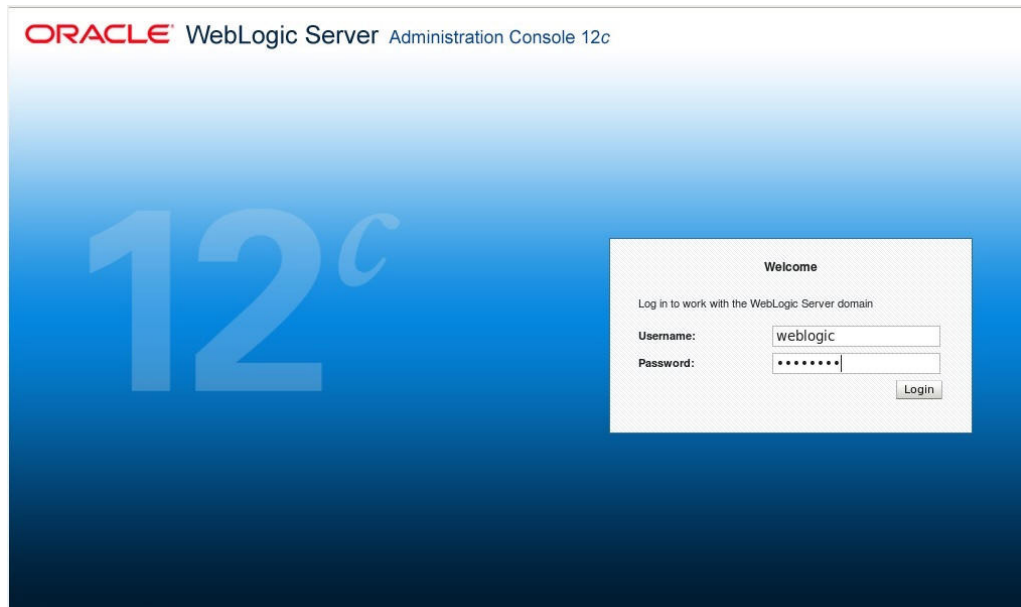
JMS queue is used to hold webservice invocation exception messages. It provides a mechanism for third parties to handle communication related failures.

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

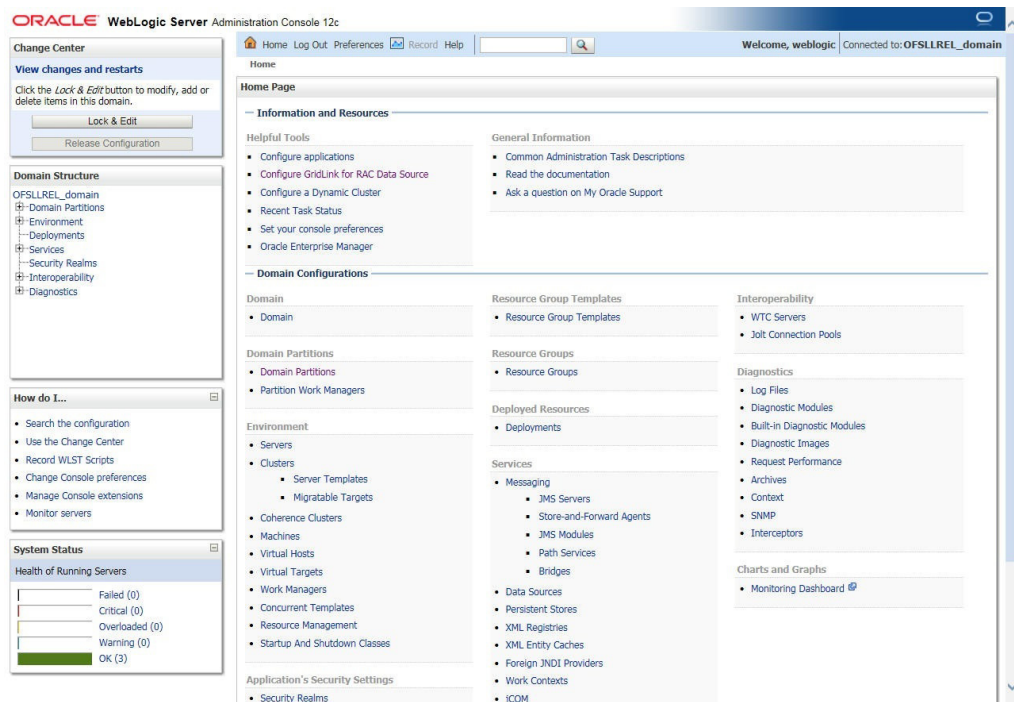
- [Create JMS Server](#)
- [Create JMS Module](#)
- [Subdeployment](#)
- [Create JMS Connection Factory](#)
- [Create JMS Queue](#)

## 9.4.1 Create JMS Server

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

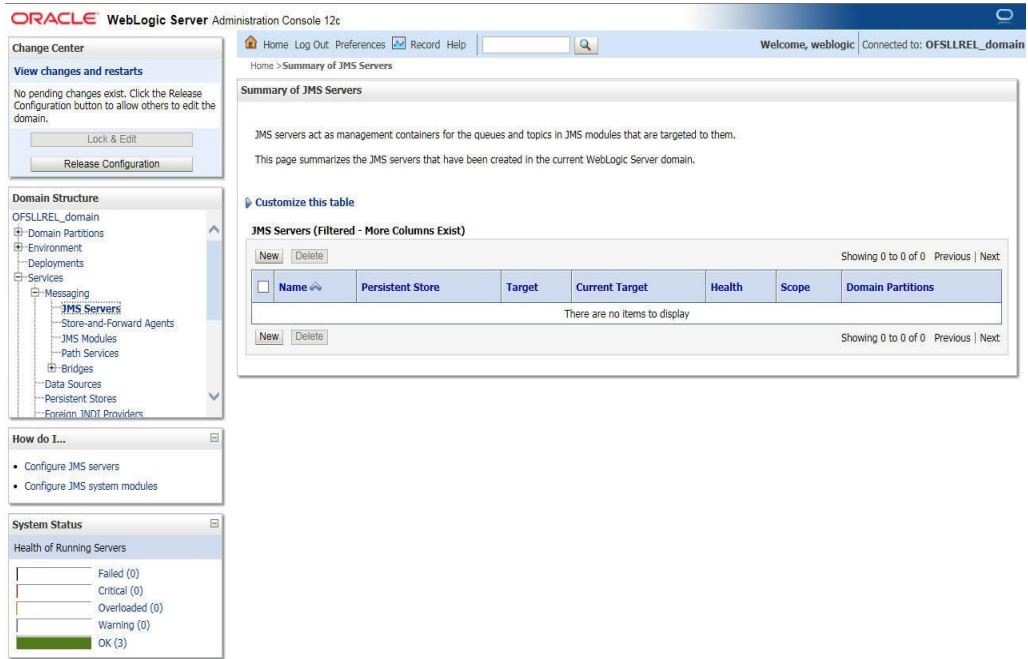


2. Specify the Weblogic administrator user name and password and click 'Log In'. The Oracle Weblogic home page is displayed.

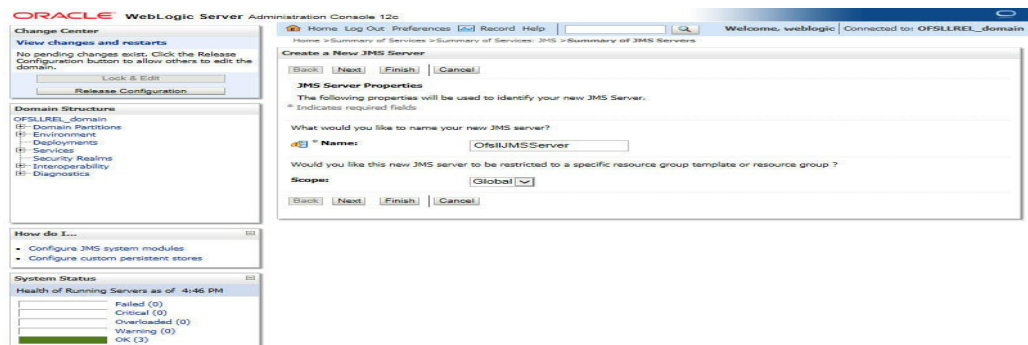


3. Click Domain Name > Services > Messaging > JMS Server.

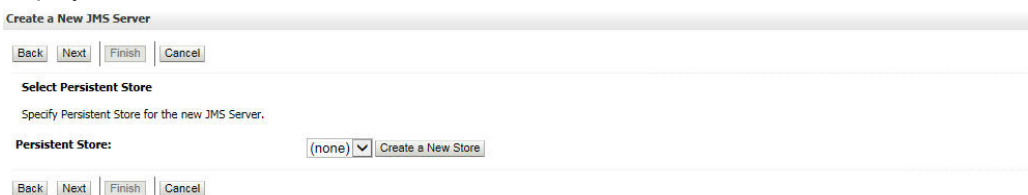
- In the main window, click 'Lock & Edit'. The following window is displayed.



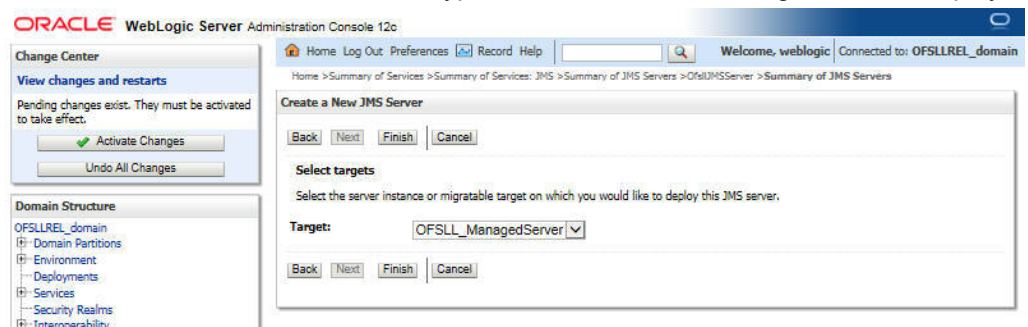
- Click 'New'. The following window is displayed.



- Specify the JMS Server Name as 'OfsllJMSServer'. Click 'Next', the following window is displayed.

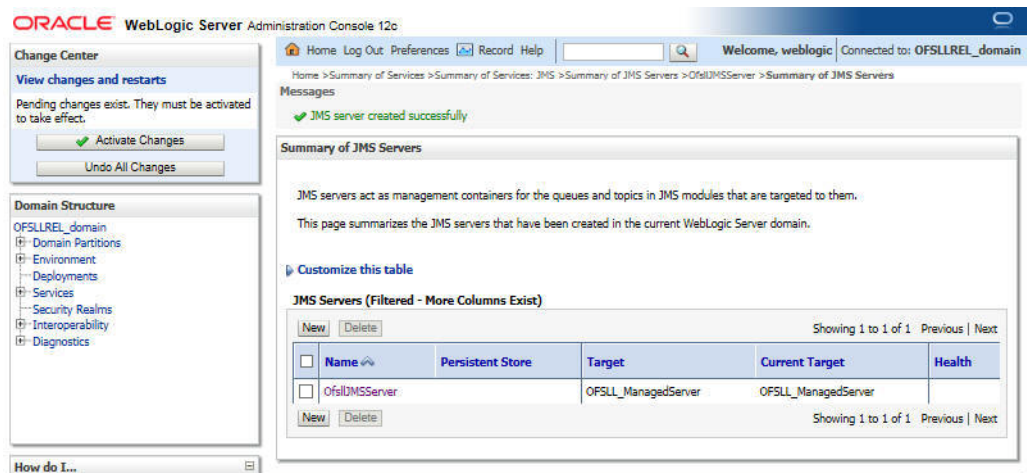


- Select 'None' as the Persistent Store type. Click 'Next', the following window is displayed.



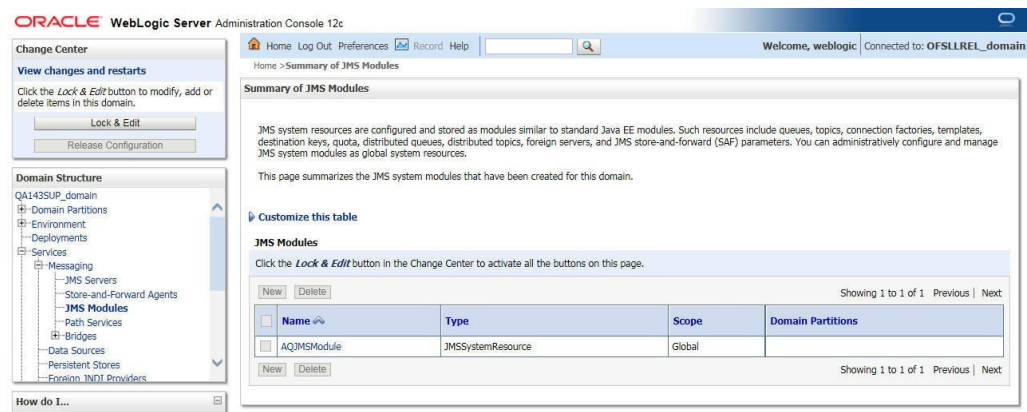
- Select the target managed server and click 'Finish'.

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

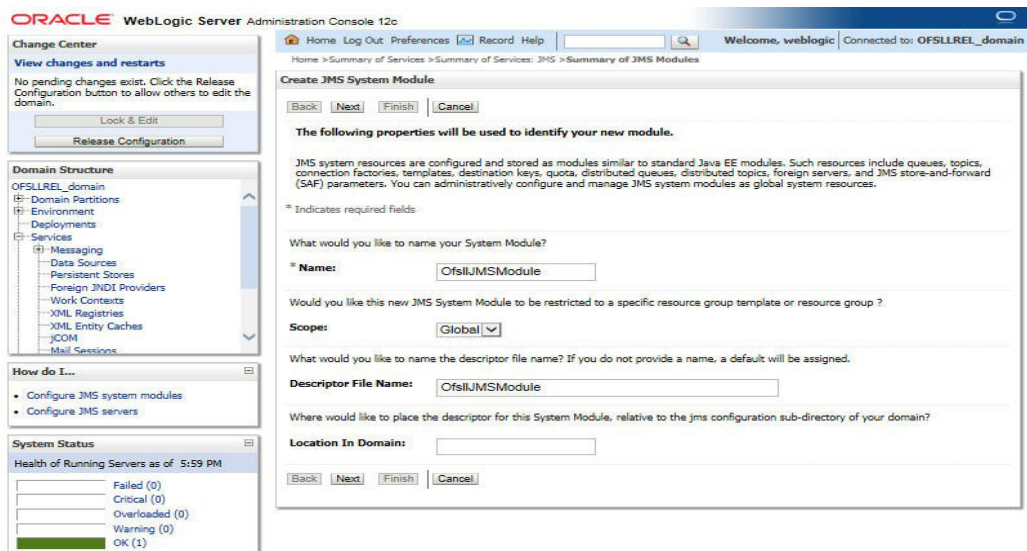


## 9.4.2 Create JMS Module

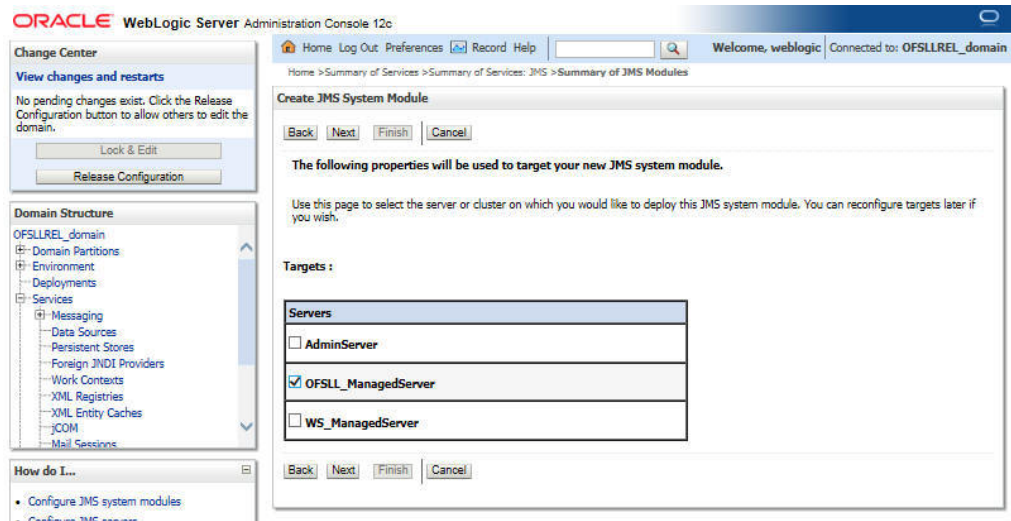
- Login to WebLogic Server 12c console (<http://hostname:port/console>) by specifying the Weblogic administrator user name and password.
- Click Domain Name > Services > Messaging > JMS Modules. The following window is displayed.



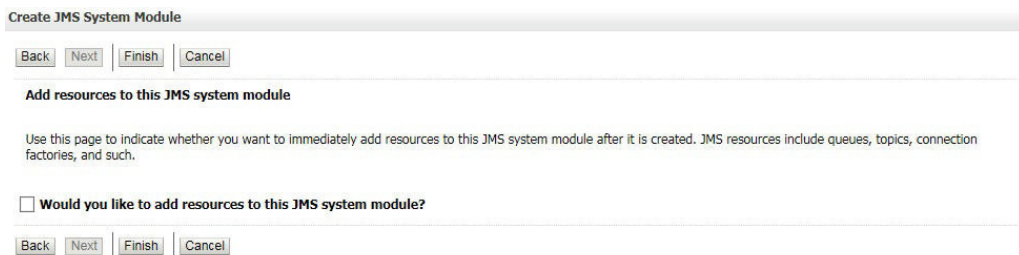
- Click 'New'. The following screen is displayed.



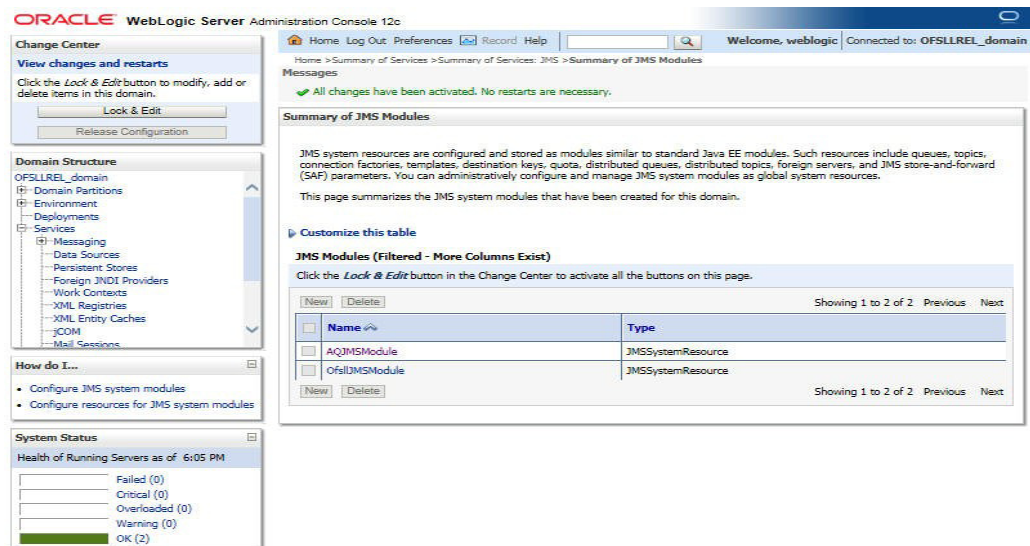
4. Specify the following details:
  - Enter the System Module Name as 'OfsllJMSModule'
  - Enter the Description File Name as 'OfsllJMSModule'
5. Click 'Next'. The following screen is displayed.



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



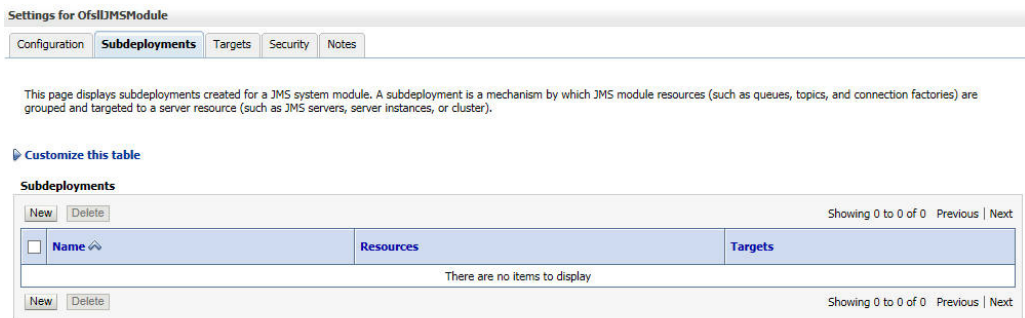
7. Click 'Finish' to save and activate the changes. Once done, the following window is displayed.



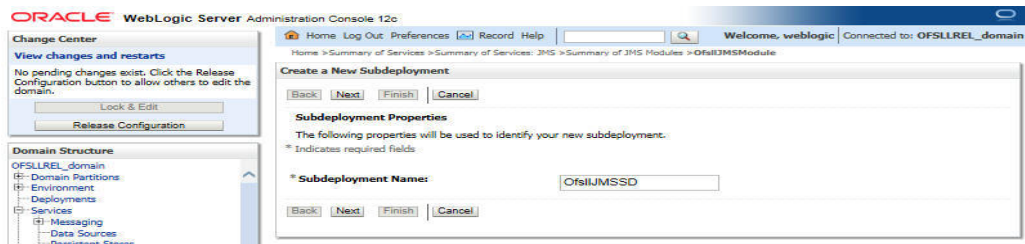
## 9.4.3 Subdeployment

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

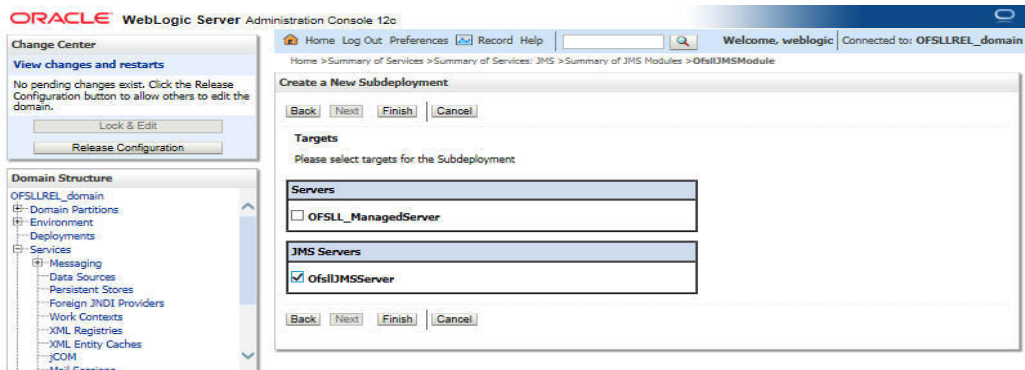
- Click Domain Name > Services > Messaging > JMS Modules. The main window displays the list of JMS modules available.
- Select the created JMS module 'OfsllJMSModule' and click 'Subdeployments' tab. The following window is displayed.



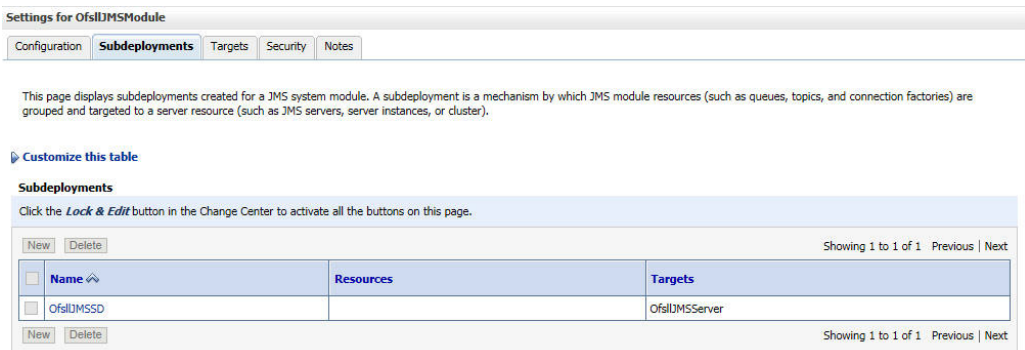
- Click 'New'. The following screen is displayed.



- Specify the Subdeployment Name as 'OfsllJMSSD'. Click 'Next', the following window is displayed.



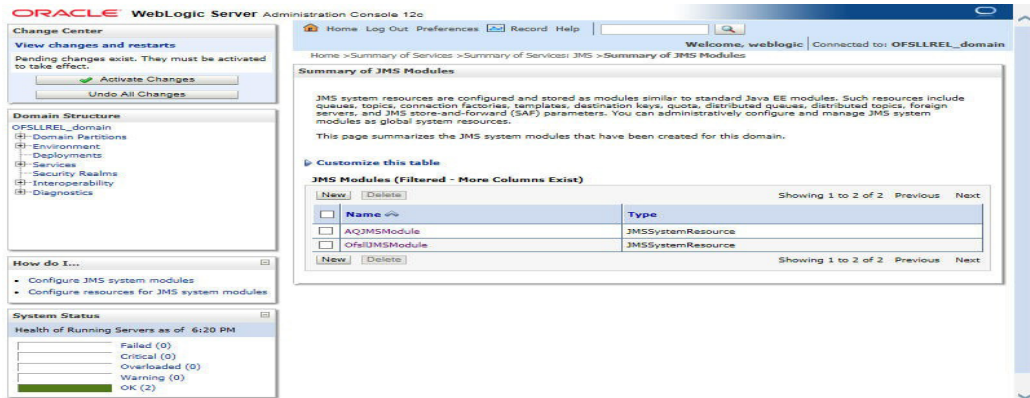
- Select the check box against the newly created JMS Server and click 'Finish'. Once done, the following window is displayed.



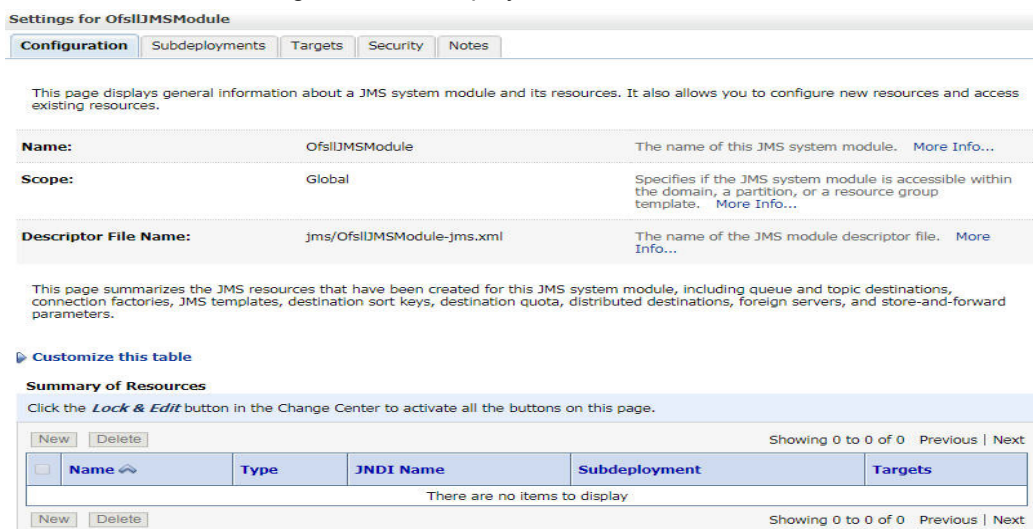
You can further click 'New' to create more Queues and repeat the steps explained above.

## 9.4.4 Create JMS Connection Factory

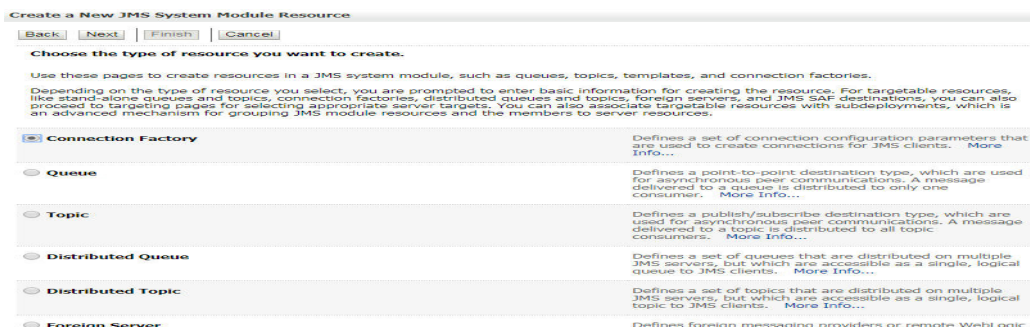
1. Login to WebLogic Server 12c console (<http://hostname:port/console>) by specifying the Weblogic administrator user name and password.
2. Click Domain Name > Services > Messaging > JMS Modules. The main window displays the list of JMS modules available.
3. Select the newly created JMS module 'OfsllJMSModule'.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

The screenshot shows the 'Create a New JMS System Module Resource' window. On the left, there is a 'Domain Structure' tree with 'OFSLLEL\_domain' selected, and a 'How do I...' section with 'Configure connection factories' highlighted. The main area is titled 'Connection Factory Properties' and contains the following fields and options:

- Name:** OfslIJMSCF
- JNDI Name:** jms/OfslIJMSCF
- Subscription Sharing Policy:** Exclusive
- Client ID Policy:** Restricted
- Maximum Messages per Session:** 10
- XA Connection Factory Enabled**

7. Specify the following details:

- Enter the Name of the Connection Factory as 'OfslIJMSCF'
- Enter the JNDI Name as 'jms/OfslIJMSCF'
- Select the check box 'XA Connection Factory Enabled'

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

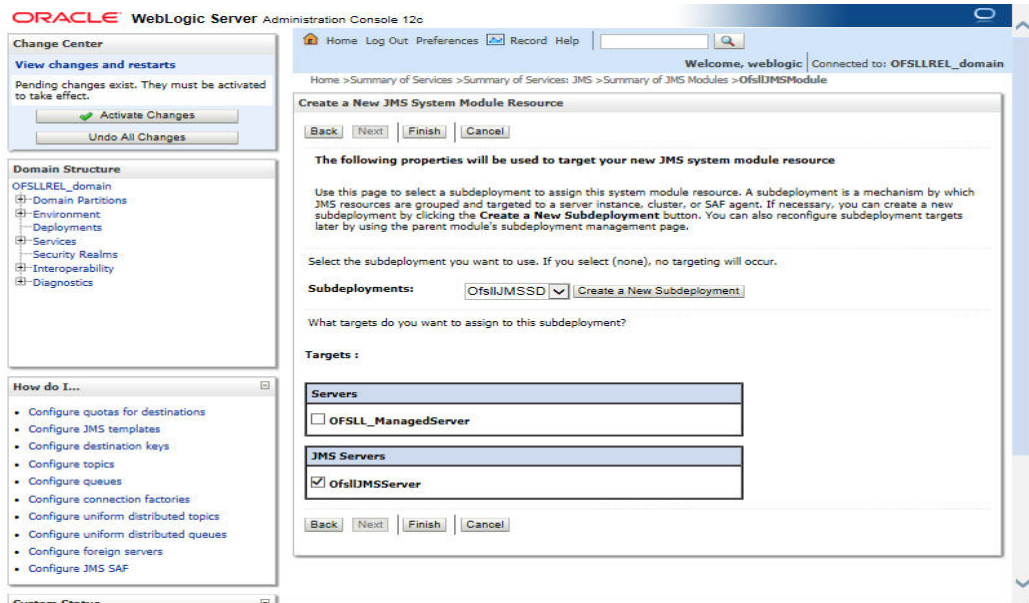
The screenshot shows the 'Advanced Targeting' window. It contains the following information:

- Targets :**
- A table with the following content:
 

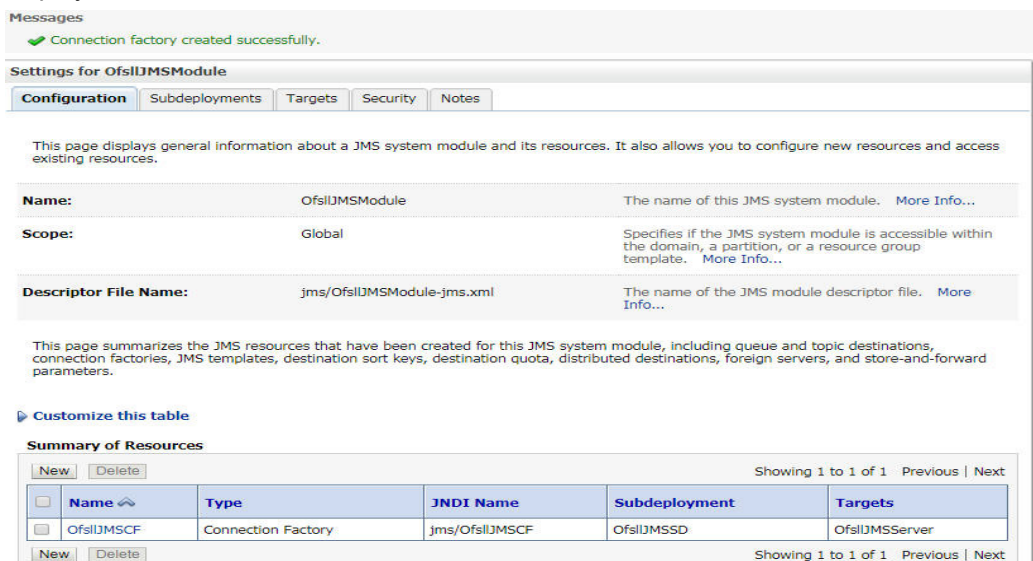
Servers
<input checked="" type="checkbox"/> OFSLLEL_ManagedServer



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



- Select the Subdeployments as 'OfslIJMSSD' from the drop down list.
- Under JMS Servers, select the check box against 'OfslIJMSServer'.
- Click 'Finish' to save and activate the changes. Once done, the following window is displayed.



### 9.4.5 Create JMS Queue

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

- Select the newly created JMS module 'OfsllJMSModule'. The following window is displayed.

The screenshot shows the Oracle WebLogic Server Administration Console. The main content area is titled 'Settings for OfsslJMSModule'. It features a 'Configuration' tab and a 'Summary of Resources' table. The table lists the following resource:

Name	Type	JNDI Name	Subdeployment	Targets
OfsslJMSSCF	Connection Factory	jms/OfsslJMSSCF	OfsslJMSSD	OfsslJMSServer

Below the table, there are 'New' and 'Delete' buttons for each resource. The page also includes a 'Customize this table' section and a 'Summary of Resources' section with a 'Lock & Edit' button.

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

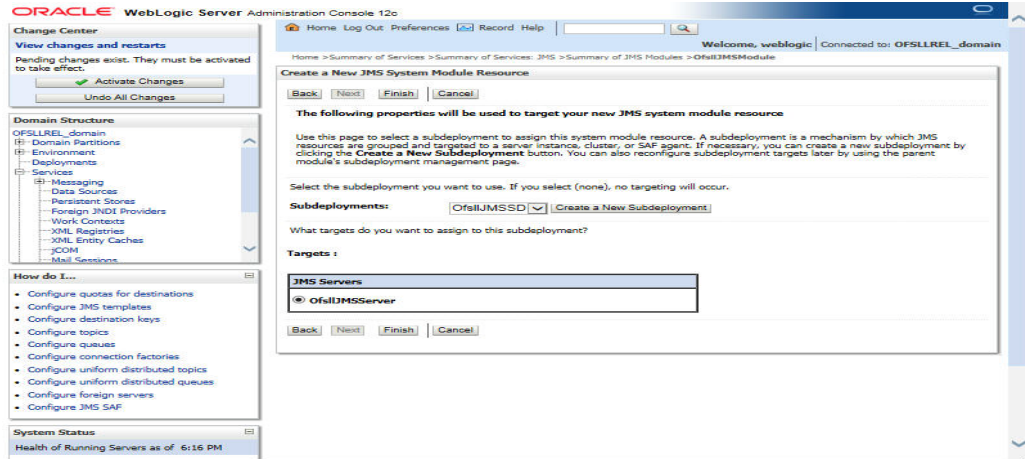
The screenshot shows the 'Create a New JMS System Module Resource' dialog. The 'Queue' option is selected. The dialog provides a list of resource types with their descriptions:

- Connection Factory**: Defines a set of connection configuration parameters that are used to create connections for JMS clients.
- Queue**: Defines a point-to-point destination type, which are used for asynchronous peer communications. A message delivered to a queue is distributed to only one consumer.
- Topic**: Defines a publish/subscribe destination type, which are used for asynchronous peer communications. A message delivered to a topic is distributed to all topic consumers.
- Distributed Queue**: Defines a set of queues that are distributed on multiple JMS servers, but which are accessible as a single, logical queue to JMS clients.
- Distributed Topic**: Defines a set of topics that are distributed on multiple JMS servers, but which are accessible as a single, logical topic to JMS clients.
- Foreign Server**: Defines foreign messaging providers or remote WebLogic Server instances that are not part of the current domain.
- Quota**: Controls the allotment of system resources available to destinations.
- Destination Sort Key**: Defines a unique sort order that destinations can apply to arriving messages.
- JMS Template**: Defines a set of default configuration settings for multiple destinations.

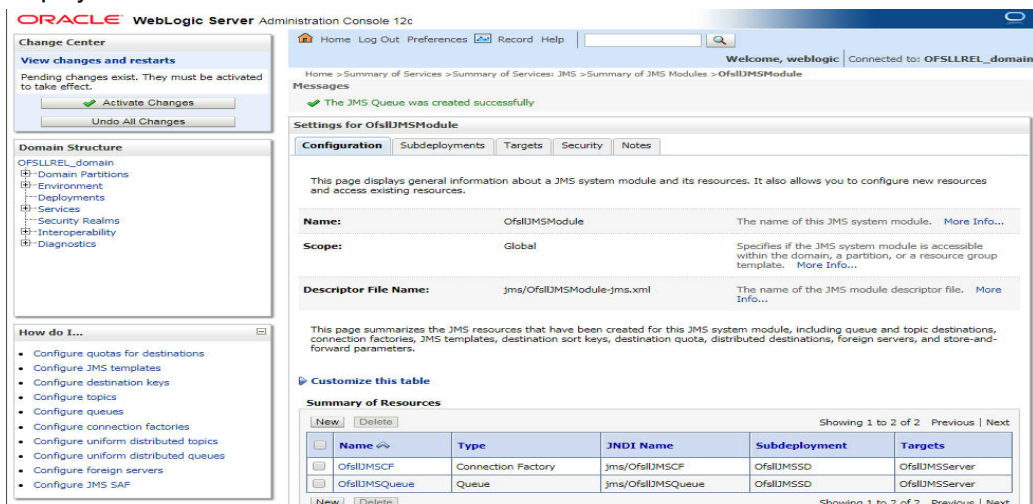
- Select the 'Queue' option and click 'Next'. The following window is displayed.

The screenshot shows the 'JMS Destination Properties' dialog. The 'Name' field is 'OfsslJMSQueue'. The 'JNDI Name' field is 'jms/OfsslJMSQueue'. The 'Template' dropdown is set to 'None'. The dialog includes 'Back', 'Next', 'Finish', and 'Cancel' buttons.

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

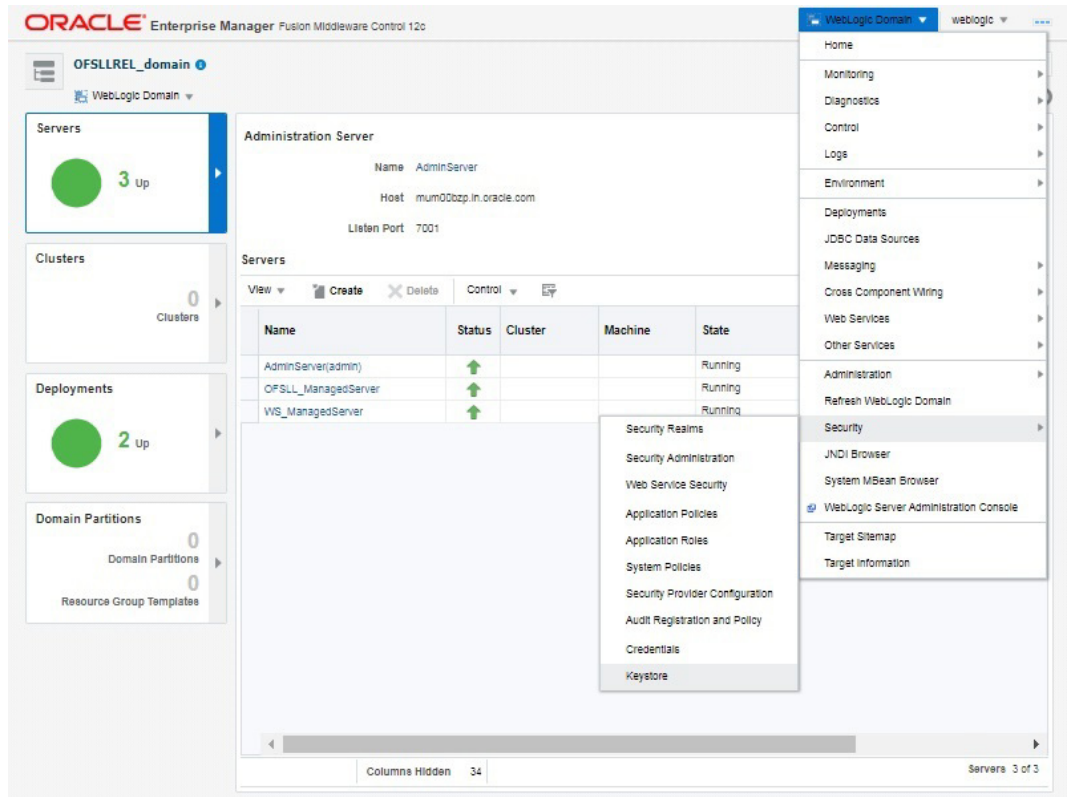
The Webhook option in OFSLL extends the support of interfacing with third-party applications by sending REST API based notifications of changes through system generated Webhook event actions.

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.

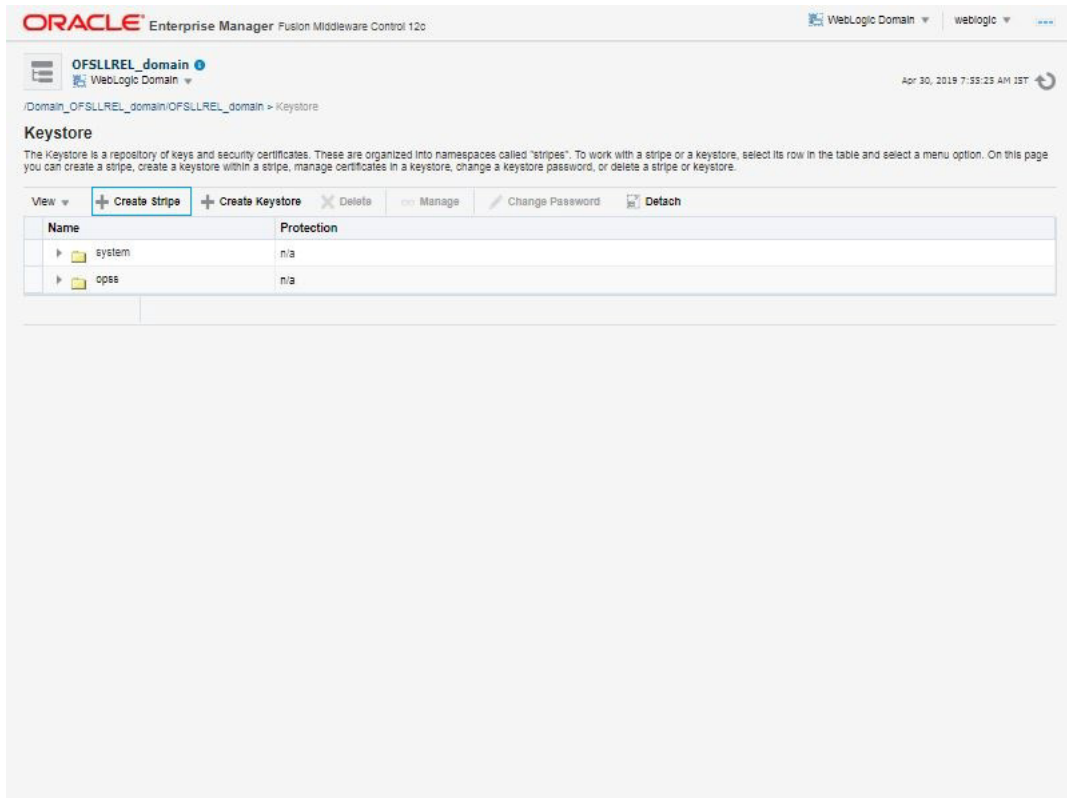
For webhook HTTPS communication, client certificates are to be imported in Weblogic OPSS keystore for each channel.

Follow the below steps to import the certificates.

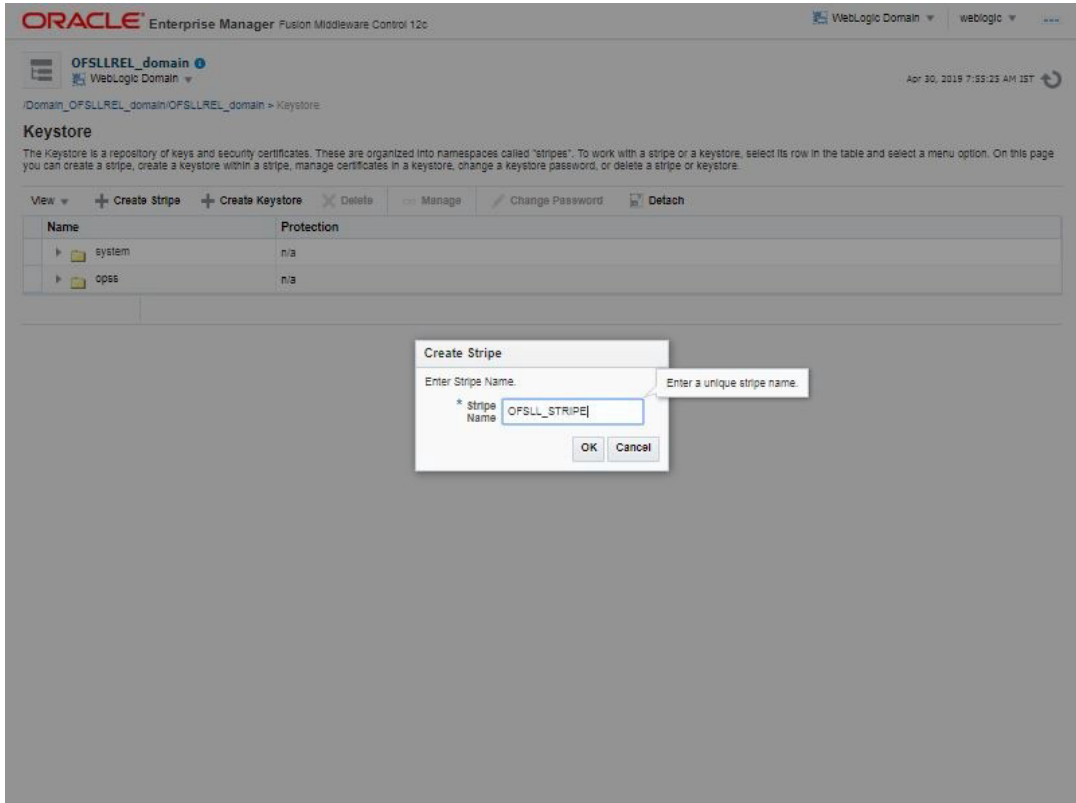
1. Login to the Oracle Enterprise Manager 12c console. (i.e. <http://hostname:port/em>)
2. Click on 'Weblogic Domain' drop-down list and navigate to Security > Keystore.



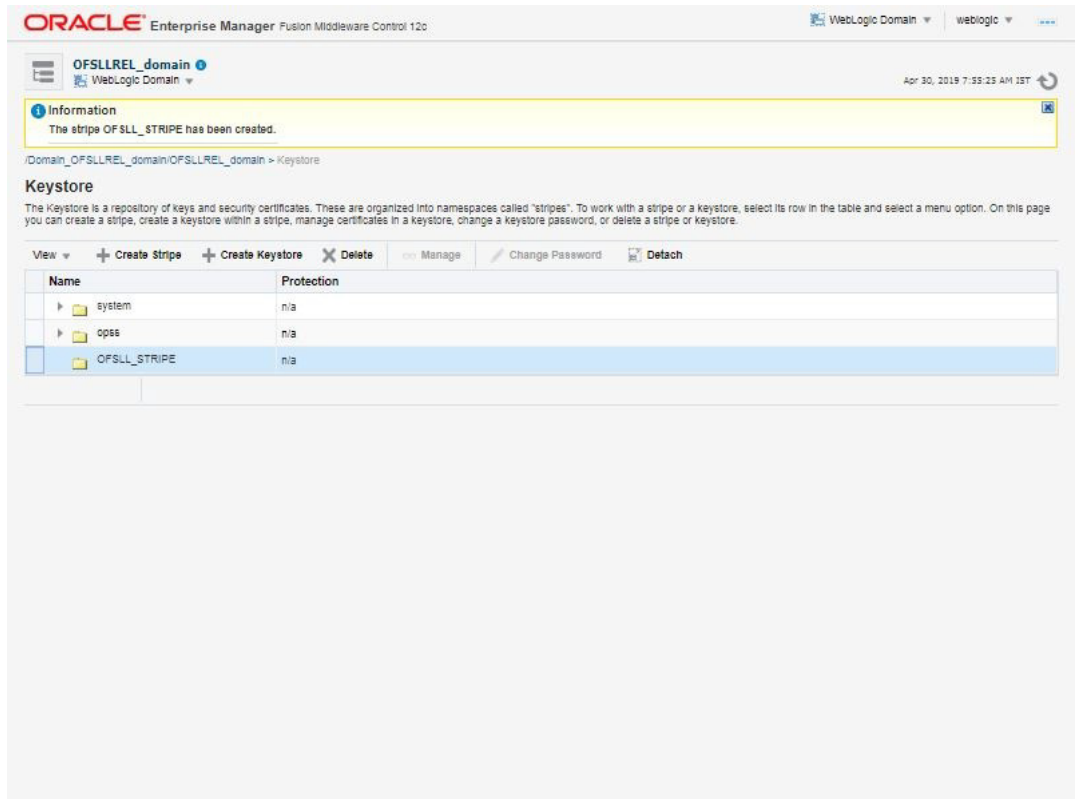
3. Click on 'Create Stripe'.



4. Enter the Stripe Name as 'OFSSL\_STRIPE'.



5. Click 'OK'. The following OFSSL\_STRIPE is created.



6. Select the newly created 'OFSSL\_STRIPE' and click 'Keystore'.

7. Enter the Keystore Name as 'OFSSL\_KSS' and click 'OK'.

The screenshot shows the Oracle Enterprise Manager interface for the 'OFSSLREL\_domain'. A 'Create Keystore' dialog box is open, allowing the user to create a new keystore. The dialog box contains the following fields and options:

- Keystore Stripe Name: OFSSL\_STRIPE
- \* Keystore Name: OFSSL\_KSS
- Protection:  Policy  Password
- Keystore Password: [Empty field]
- Confirm Password: [Empty field]
- Grant Permission:
- Code Base URL: [Empty field]

The background shows a table of existing keystores:

Name	Protection
system	n/a
ops	n/a
OFSSL_STRIPE	n/a

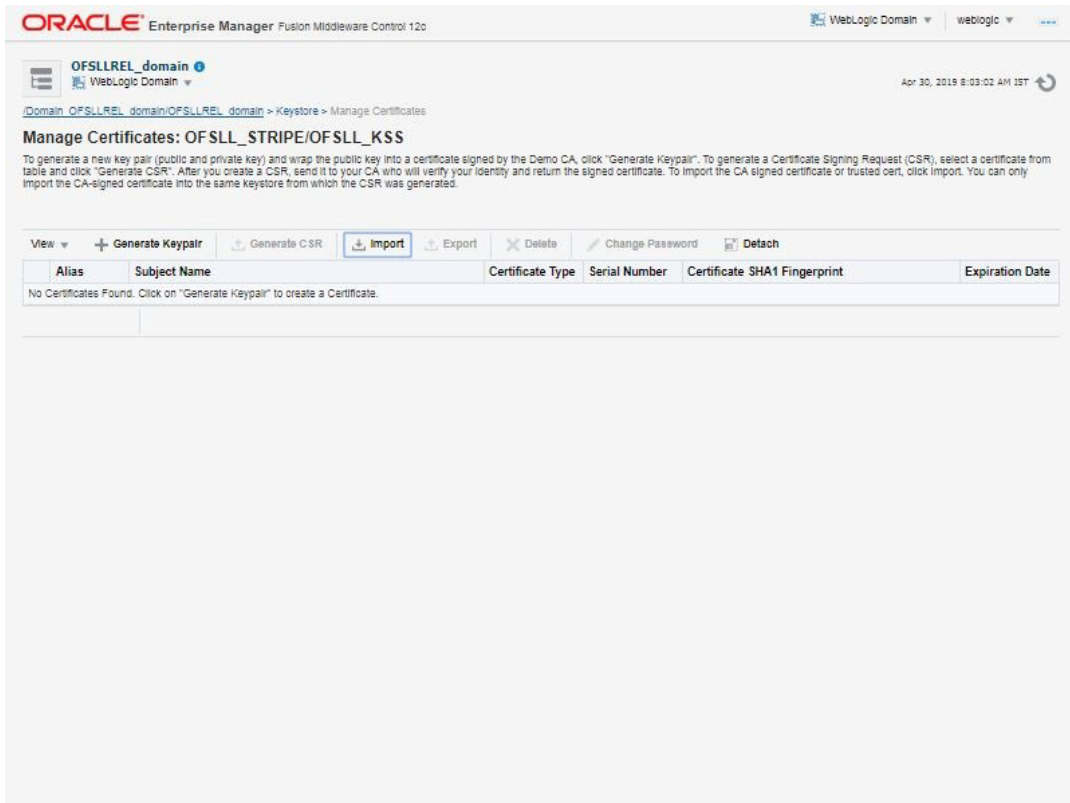
8. Select 'OFSSL\_KSS' and click 'Manage'.

The screenshot shows the Oracle Enterprise Manager interface for the 'OFSSLREL\_domain'. The 'Keystore' table is displayed, and the 'OFSSL\_KSS' keystore is selected. The 'Manage' button is highlighted in the toolbar above the table.

The background shows the 'Keystore' table with the following data:

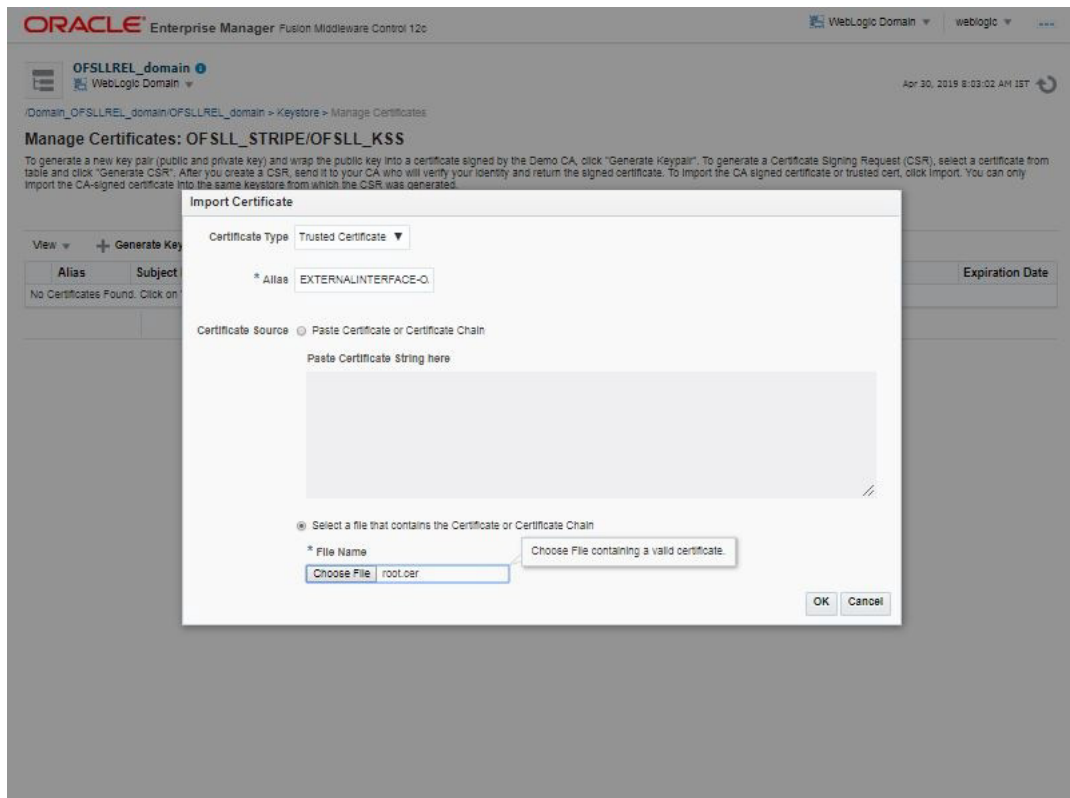
Name	Protection
system	n/a
ops	n/a
OFSSL_STRIPE	n/a
OFSSL_KSS	Policy

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

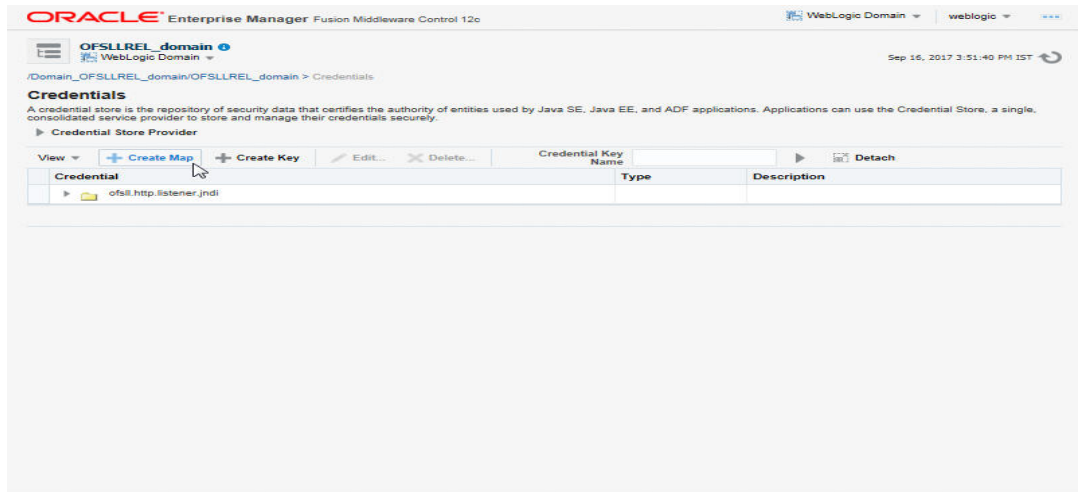


11. Click 'OK'.

## 9.6 Create Credentials and System Policies

In order to 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.

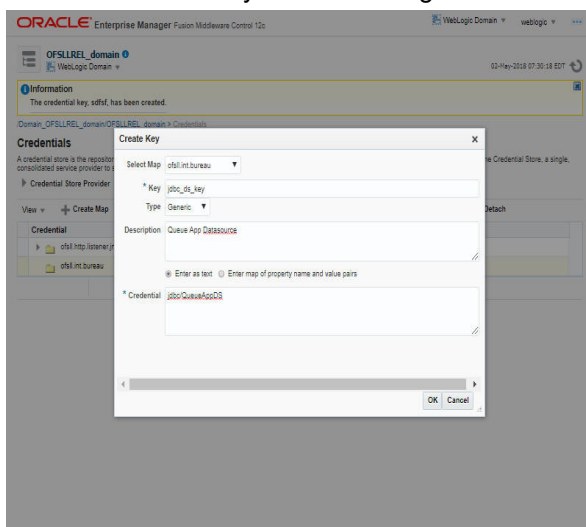
1. Login to Oracle Enterprise Manager (http://hostname:port/em).
2. On the left panel, right click on OFSLLREL\_domain and select Security > System Policies > Credentials. The following window is displayed.



3. Click 'Create Map'. The following window is displayed.



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



6. Specify the following details:
  - Select Map as 'ofssl.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
ofssl.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.
ofssl.int.outbound		This map is used to setup keys for the Route-One and Dealer track call back from OFSSL.

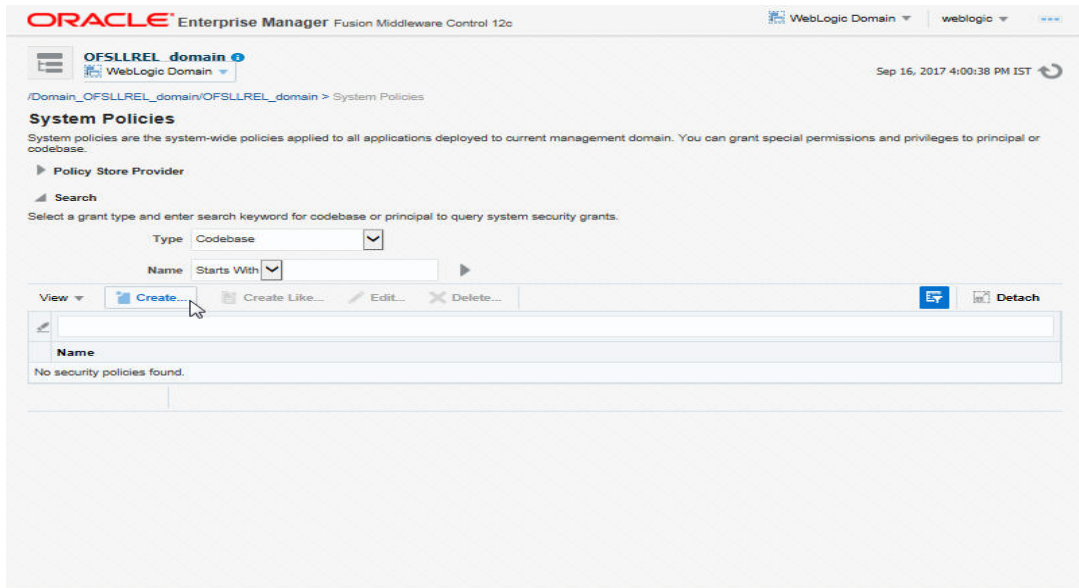
Maps	Keys	Description
	roUserNamePassword	Login Credentials used at the time of call back from OFSLL to RouteOne Interface.
	dtUsernamePassword	Login Credentials used at the time of Call back from OFSLL to Dealer Track Interface.
	jdbc_ds_key	Datasource configured to retrieve data for out-bound Resources.
	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
	TorqueltsUserName- Password	Credentials required to connect to Torquelts web service
	TorqueltsURL	Torquelts 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.
ofssl.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 SFTP server
	sftp_servers	SFTP server names
ofssl.int.se curity	bip_key	This is BIP login credentials
ofssl.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.
ofssl.int.co mmon		This map is used to setup keys for common JMS Queue
	OfsslJMSQueueJNDI	The JMS queue JNDI name to be configured
	OfsslJMSQueueCF	The JMS queue connection factory to be configured
	OfsslJMSServerURL	The JMS server url to be configured. Ex: t3://<JMS server host>:<JMS server port>
ofssl.int.we bhook	jdbc_ds_key	Datasource configured to retrieve data for Webhook.

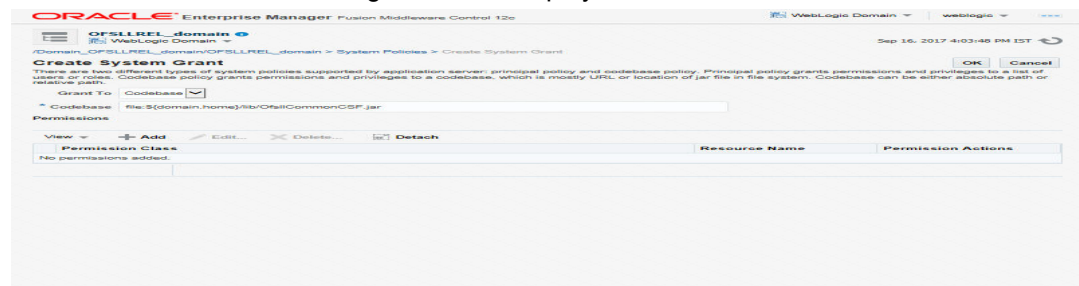
\* A new file(file.properties) needs to be created and copied to the application server in the same path as mentioned in the value corresponding to the key 'emailBodyContentPath' under the map 'ofssl.int.bip'. The file should have the following contents:

- 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.

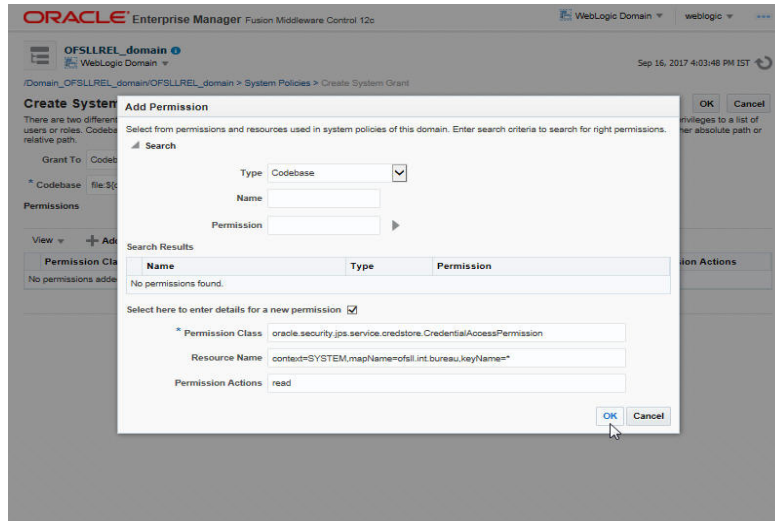


10. Click 'Create'. The following window is displayed.



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'.

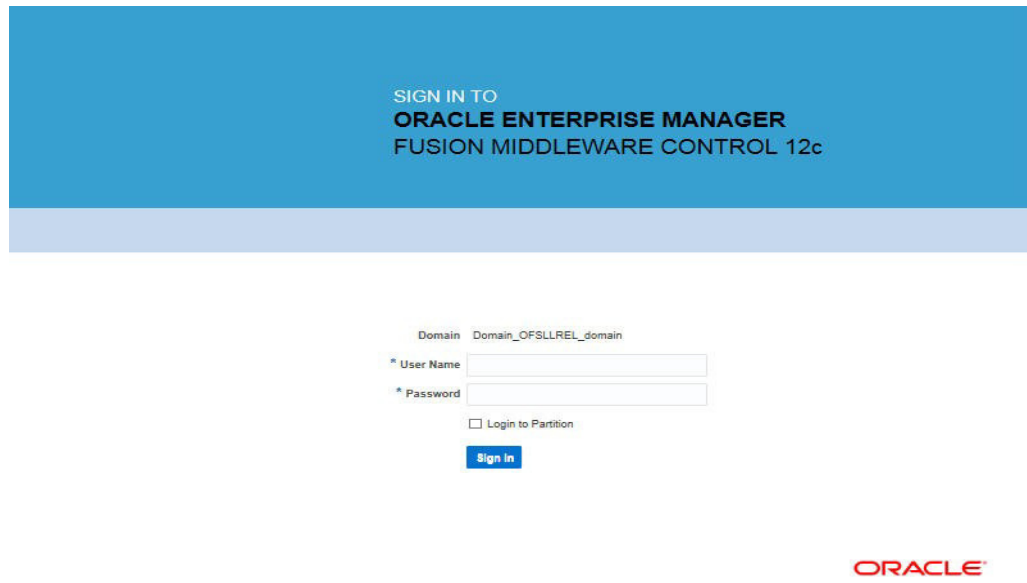
14. Specify the following details as the first permission class.

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

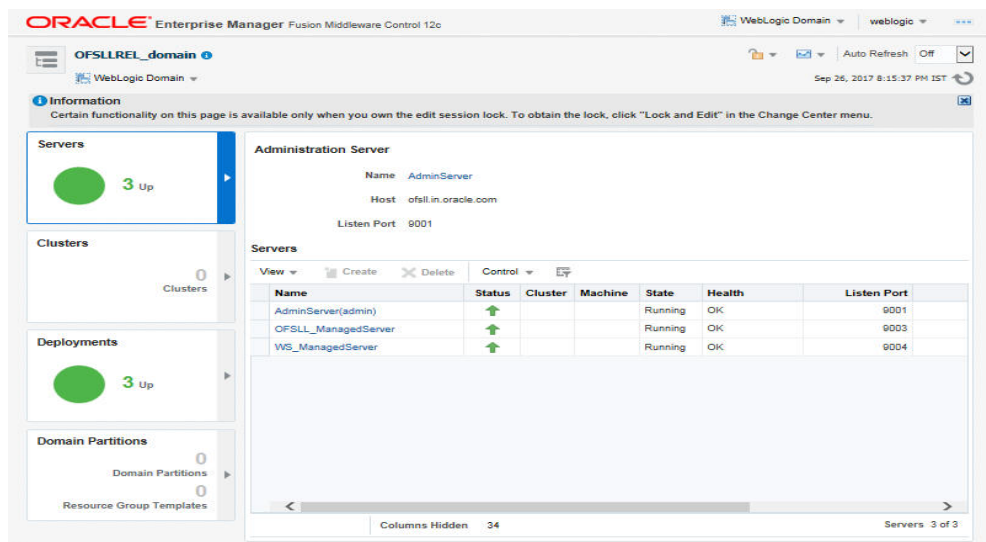
15. Click 'OK'.

## 9.7 Deploy MDB EJB

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



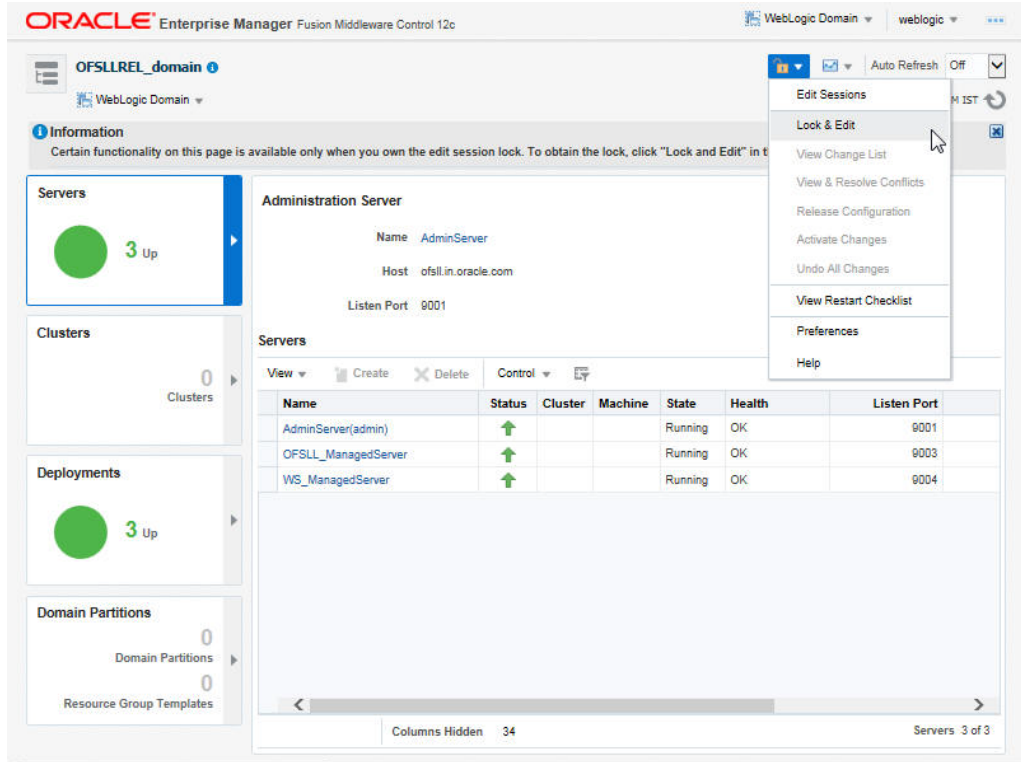
2. Enter valid login credentials. The following window is displayed.



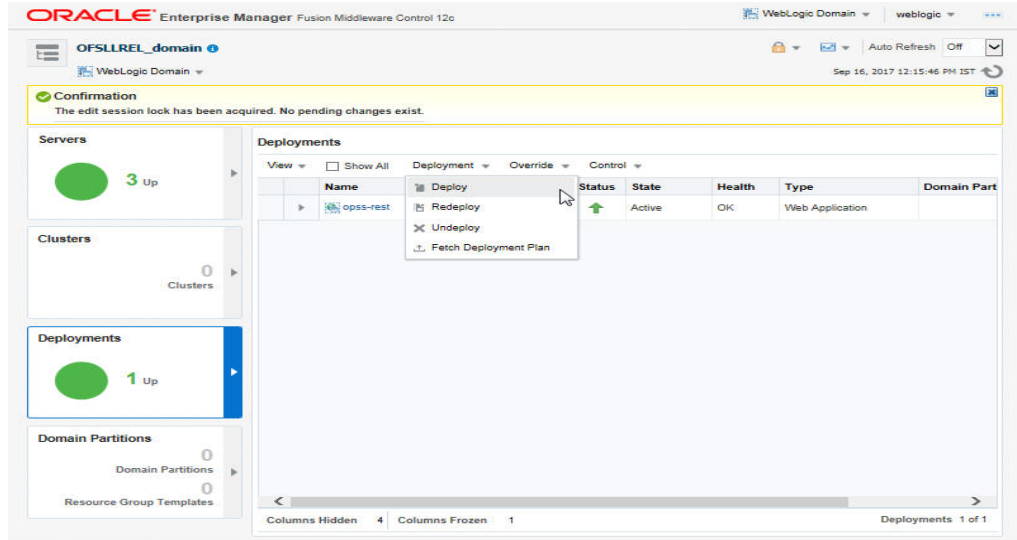
Name	Status	Cluster	Machine	State	Health	Listen Port
AdminServer(admin)	↑			Running	OK	9001
OFSSL_ManagedServer	↑			Running	OK	9003
WS_ManagedServer	↑			Running	OK	9004

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

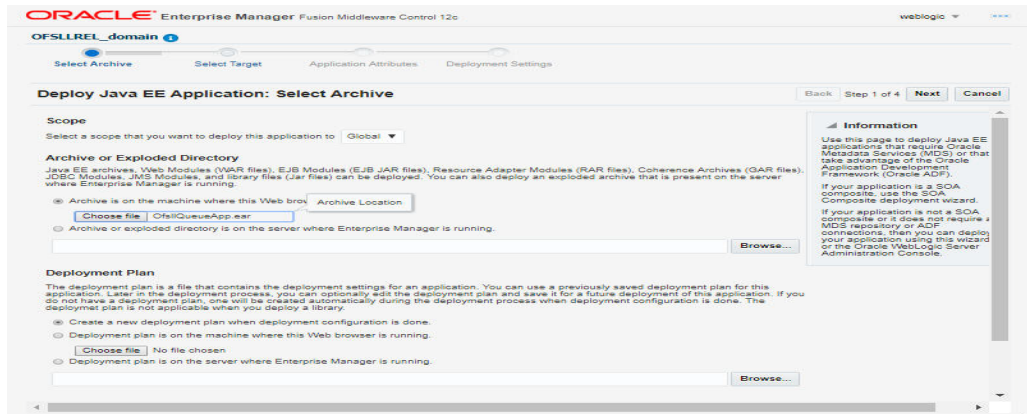
- Click 'Deployment' in the left panel. The following window is displayed.



- Select 'Deploy' from the Deployment drop-down list. The following window is displayed.

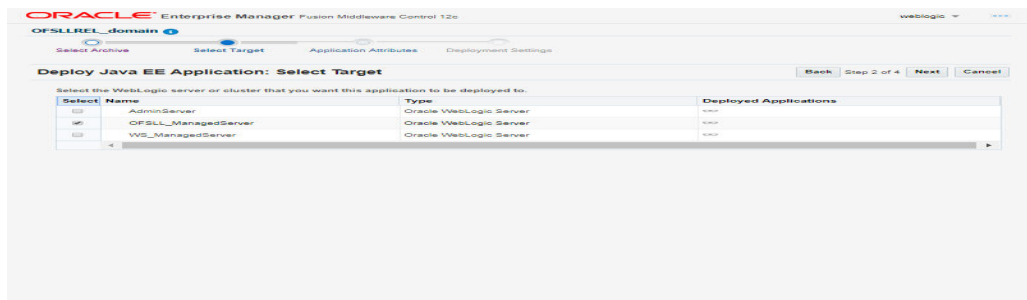


6. The following window is displayed.



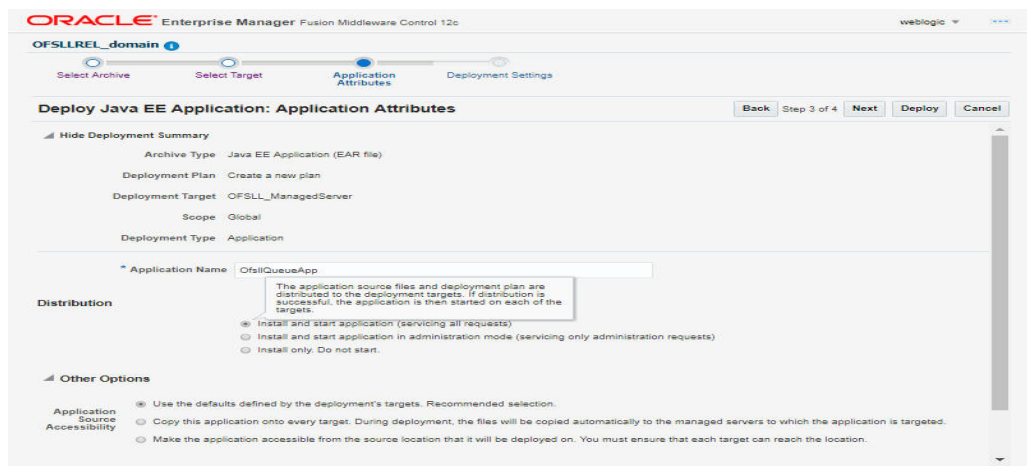
7. Browse to the folder containing the MDB EJB. Eg: C:/OfsllQueueApp.ear

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



9. Select the server on which the MDB EJB needs to be deployed.

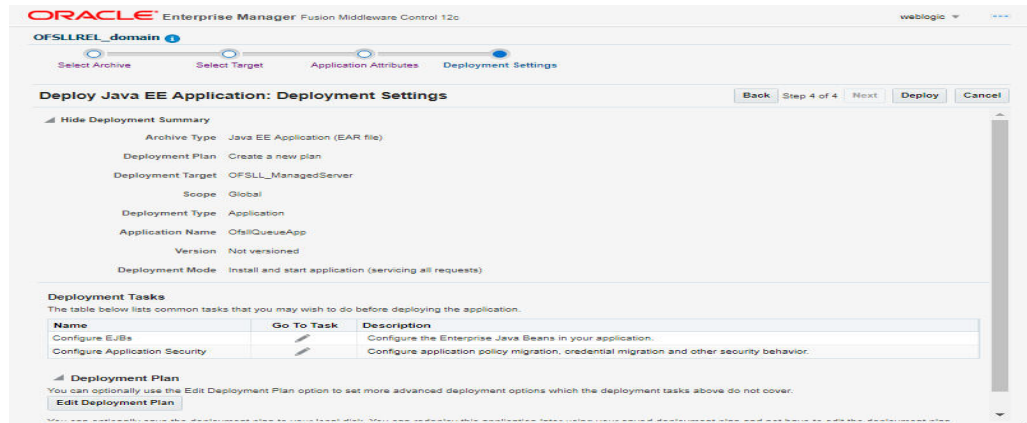
10. Click 'Next'. The following window is displayed.



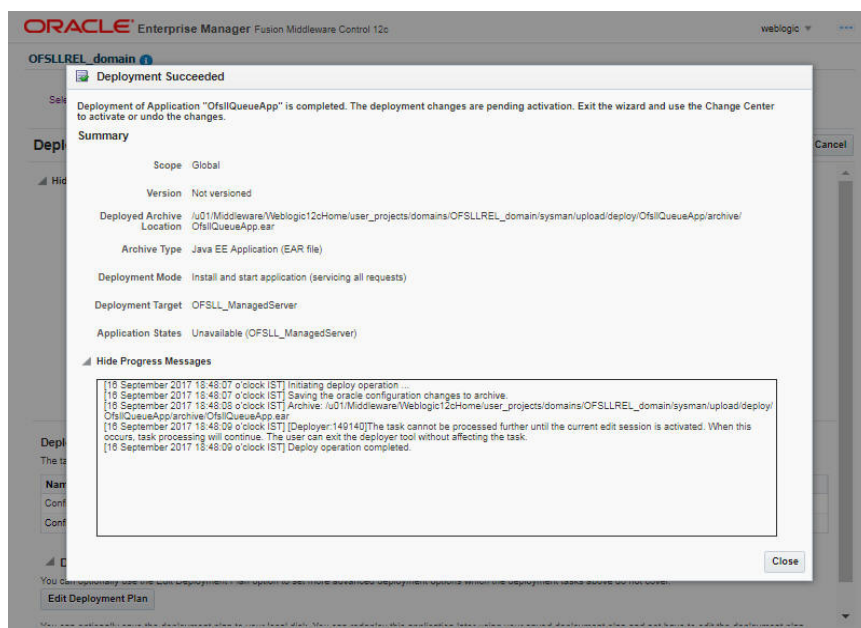
11. Select the option 'Install and start application (servicing all requests)'.



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.

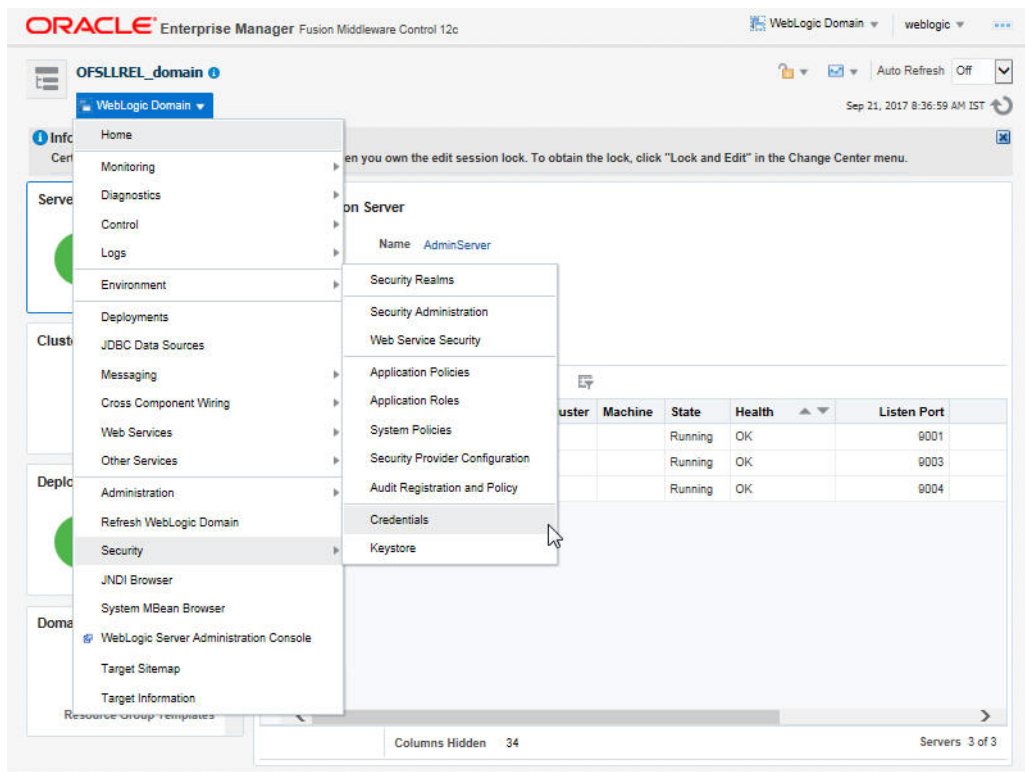
---

# 10. Configuring Oracle Analytics Publisher for Application

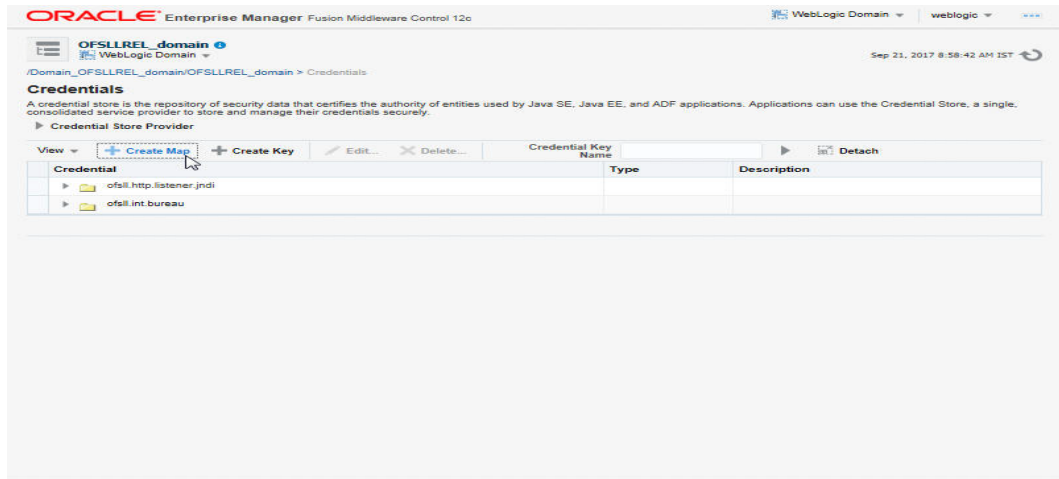
1. Copy the OfsslCommonCSF.jar from /WEB-INF/lib available in the staging area to \$DOMAIN\_HOME/lib
2. Update the setDomainEnv.sh file (\$MW\_HOME/user\_projects/domains/mydomain/bin directory) by appending the above jar file path – EXTRA\_JAVA\_PROPERTIES="..... \${EXTRA\_JAVA\_PROPERTIES} -Dofssl.csf.path=\${DOMAIN\_HOME}"
3. Configure Security via EMconsole

## Note

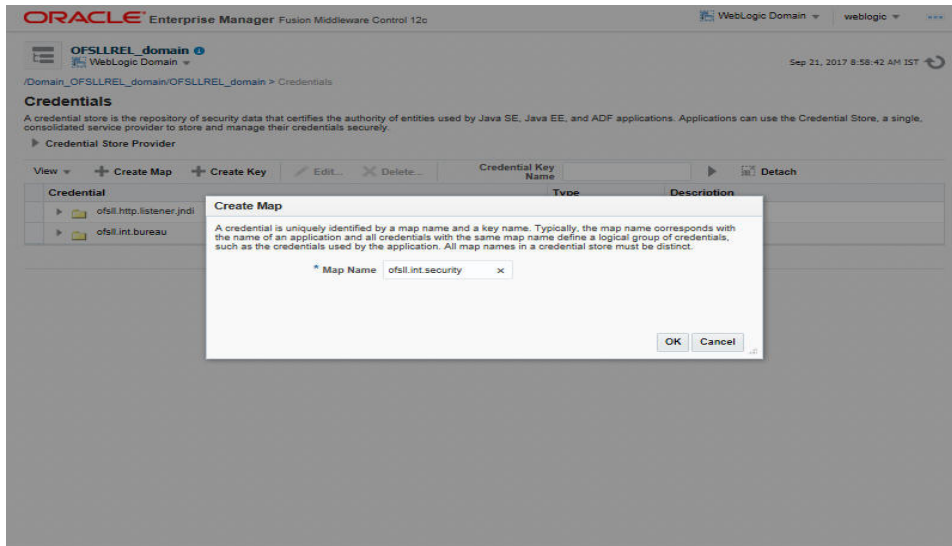
It is assumed that BI Publisher is installed and configured. Refer BI Publisher Guide for further details.



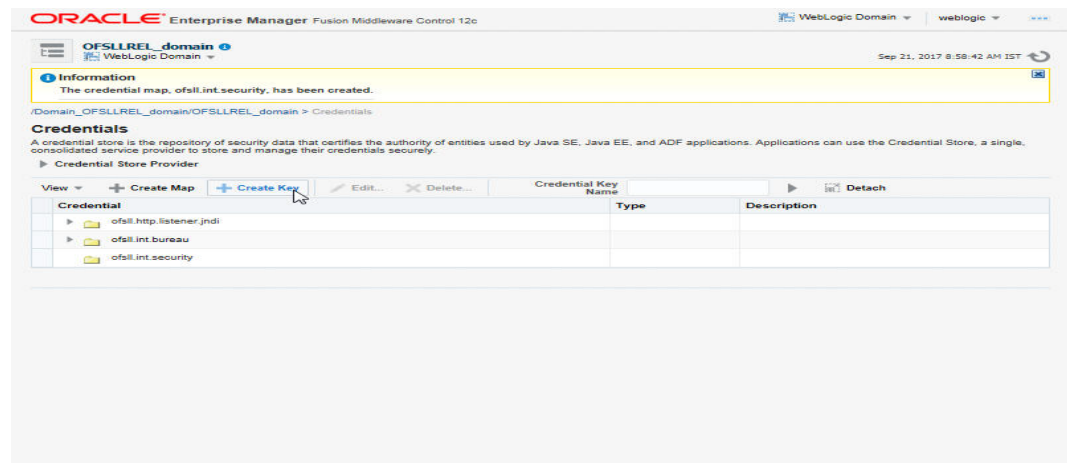
- Click WebLogic Domain on the right panel. Select Security > Credentials. Click 'Create Map'.



- Enter the Map Name: ofssl.int.security.

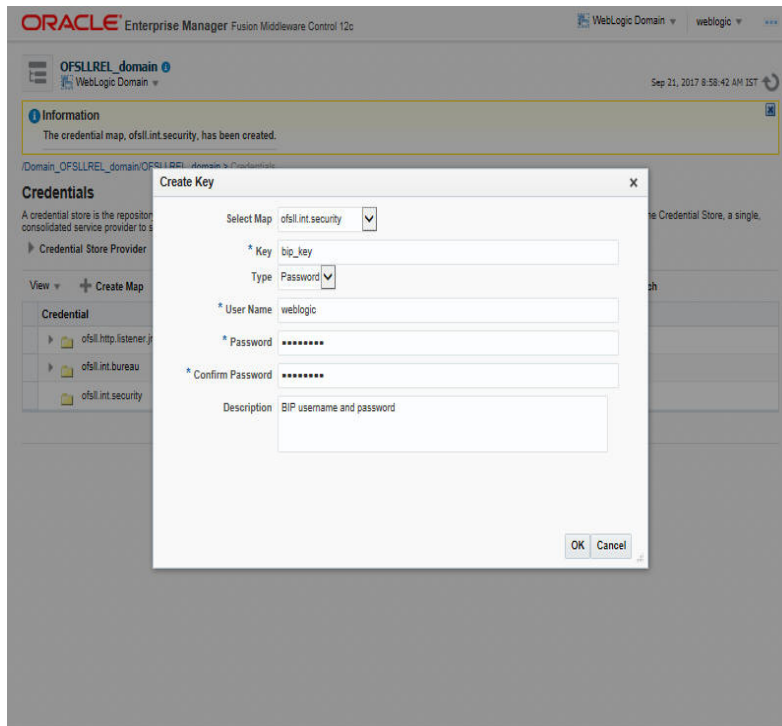


- Click 'OK'.

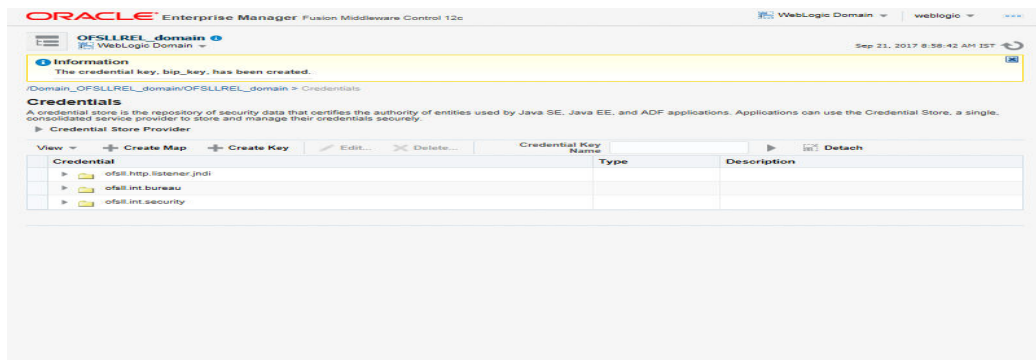


- Click 'Create Key' Button.

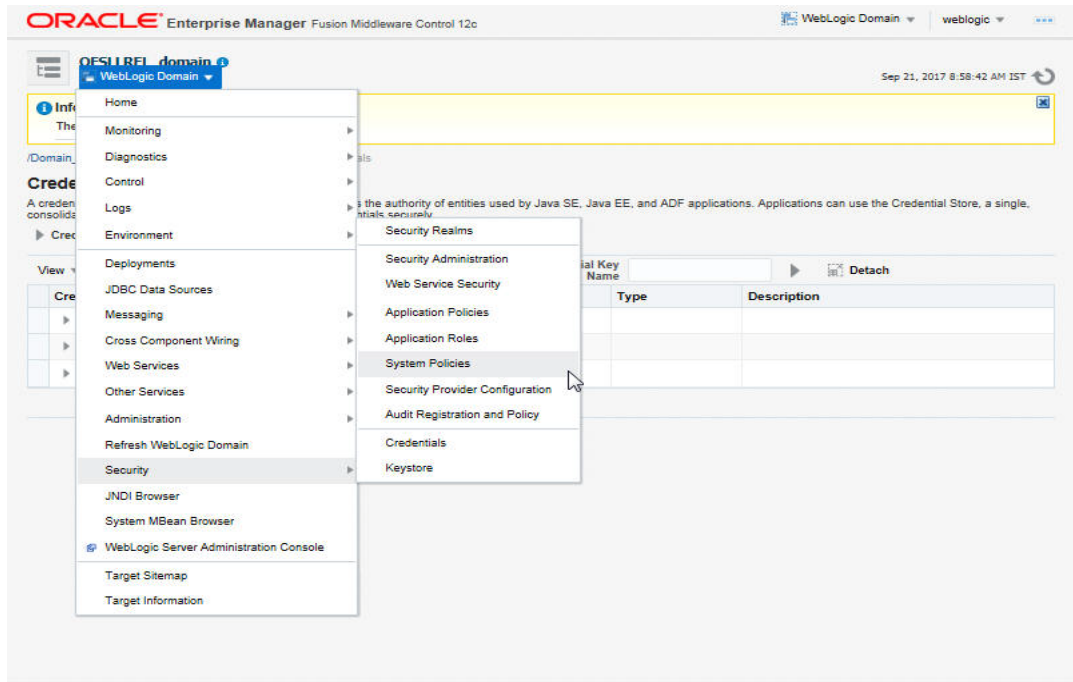
8. Enter the details as per your requirement. Specify 'User Name' and 'Password' of BI Publisher console.



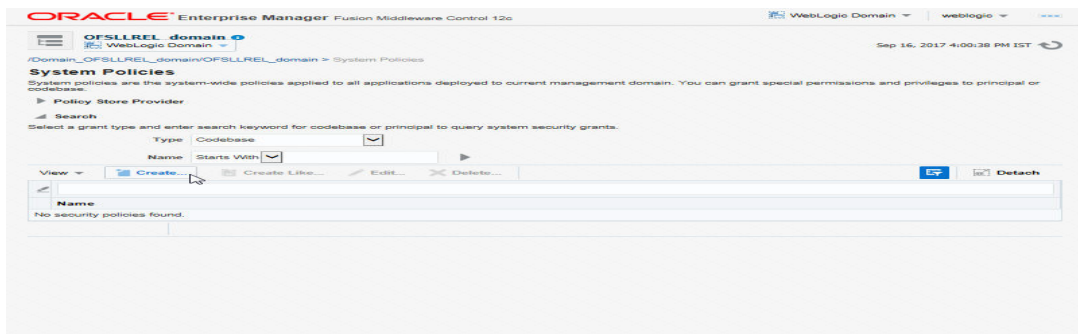
9. Click 'OK'. The following window is displayed.



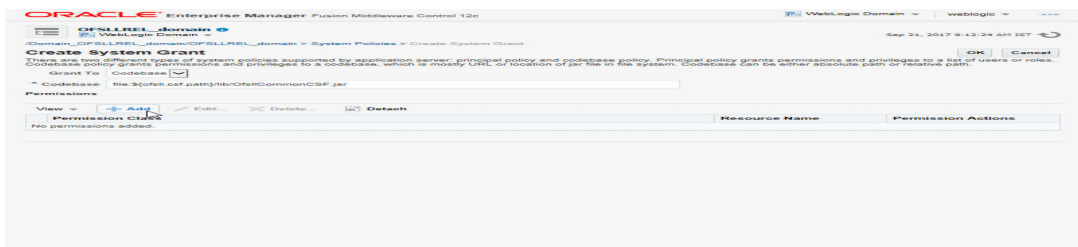
- On the left panel, right click on the domain OFSLL\_domain > Security > System Policies. The following window is displayed.



- Click 'Create'.

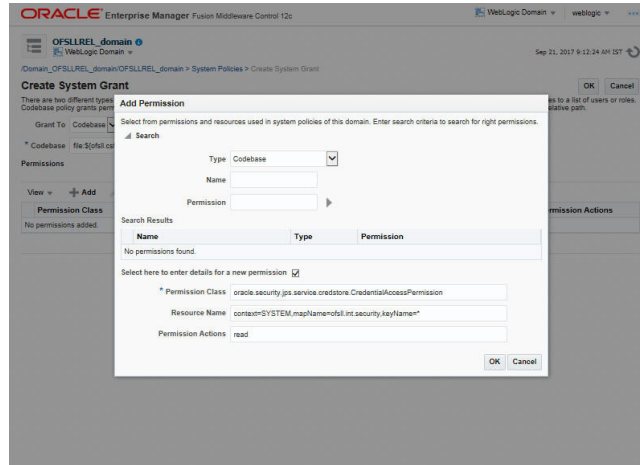


- The following window is displayed. Enter the codebase as 'file:\${ofssl.csf.path}/lib/OfsslCommonCSF.jar' and click 'Add'.



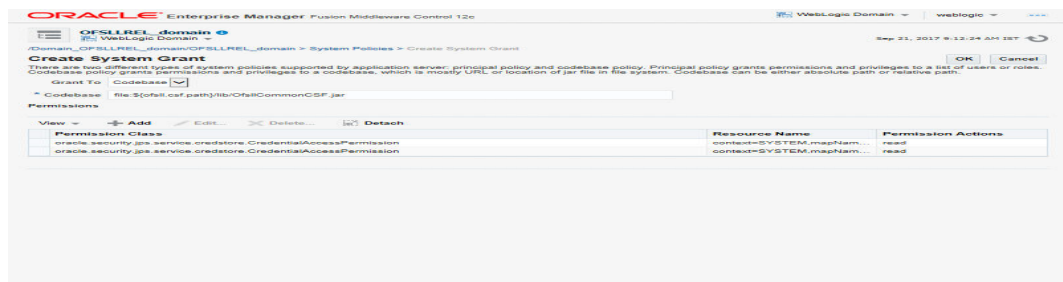
- The following window is displayed. Select the checkbox 'Select here to enter details for a new permission' and enter the following details as the first permission class.
  - Permission Class: oracle.security.jps.service.credstore.CredentialAccessPermission
  - Resource Name: context=SYSTEM,mapName=ofssl.int.security,keyName=\*

- Permission Actions: read

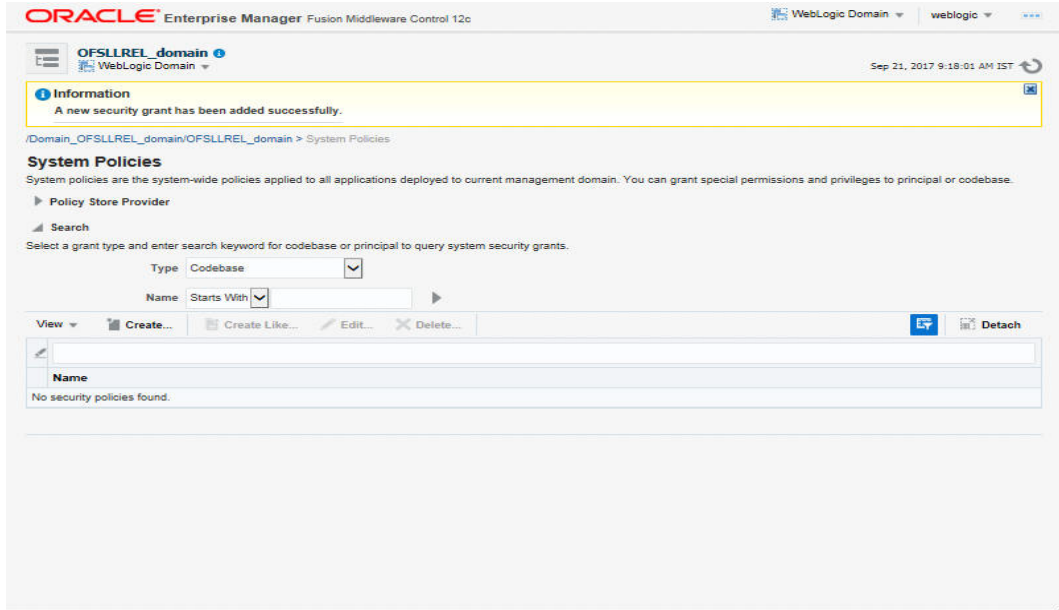


## Configuring JNDI Name for http Listener

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=ofsl.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'.

The screenshot displays the Oracle WebLogic Administration Console interface. On the left, a tree view shows the domain structure: OFSLLREL\_domain, Domain Partitions, Environment, Deployments, Services, Security Realms, Interoperability, and Diagnostics. Below the tree are three panels: 'How do I...' with a list of tasks (Install, Configure, Update, Monitor, Deploy, Install Web application), 'System Status' showing 'Health of Running Servers as of 5:07 AM' with 3 OK servers, and a 'Deployments' table.

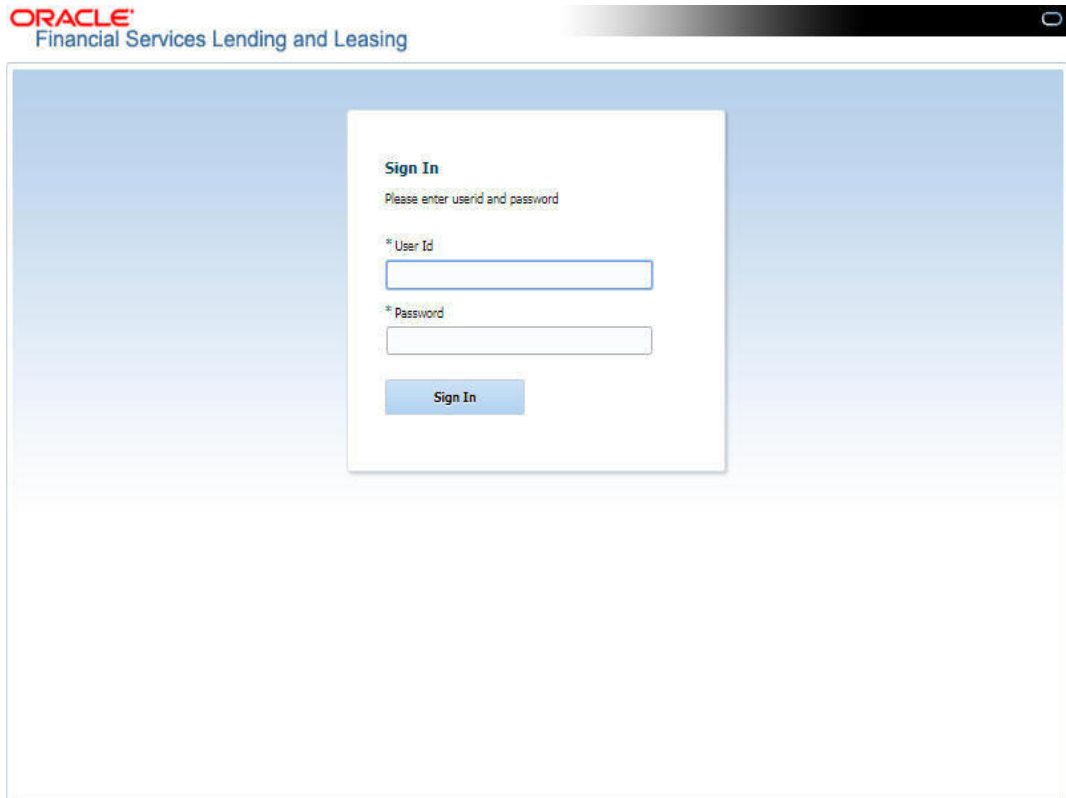
The 'Deployments' table lists the following applications:

Name	State	Health	Type	Targets	Scope	Domain Partitions	Deployment Size
coherence-transaction-rar	Active	OK	Resource Adapter	AdminServer, OFSLL_ManagedServer, WS_ManagedServer	Global		100
DMS Application (12.2.1.1.0)	Active	OK	Web Application	AdminServer, OFSLL_ManagedServer, WS_ManagedServer	Global		5
em	Active	OK	Enterprise Application	AdminServer	Global		400
ofsll149 (V14.9.0.0.0-b106)	Active	OK	Enterprise Application	OFSLL_ManagedServer	Global		100
opss-rest	Active	OK	Web Application	AdminServer	Global		150
state-management-provider-memory-rar	Active	OK	Resource Adapter	AdminServer, OFSLL_ManagedServer, WS_ManagedServer	Global		100

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

