Oracle® Financial Services Lending and Leasing

Application Installation Guide

Release 14.12.0.0.0
F81933-01
August 2024

Oracle Financial Services Lending and Leasing Application Installation Guide, Release 14.12.0.0.0

F81933-01

Contents

Preface

Prerequisites vi
Audience vii
Documentation Accessibility vii
Diversity and Inclusion vii
Conventions vii

1 Install Software

1.1 Installing Oracle WebLogic Server 12c 1-1

2 Create Domains, Repositories, Data Sources

2.1 Creating Schemas using Repository Creation Utility 2-1
2.2 Creating Domain and Servers 2-14
2.3 Creating Metadata Repository 2-36
2.4 Creating Data Source 2-40
2.5 Creating SQL Authentication Provider 2-52
2.6 Creating User Groups and Users 2-62
2.6.1 Creating Users 2-62
2.6.2 Creating User Groups 2-65
2.6.3 Assigning Users to Groups 2-66
2.6.4 Resetting password via weblogic console 2-67
2.7 Implementing JMX Policy for Change Password 2-68

3 Configure Policies

3.1 Configuring Password Policy for SQL Authenticator 3-1
3.2 Configuring User Lockout Policy 3-3

4 Deploy Application

4.1 Deploying Application 4-1

5 Enable SSL

5.1 Enabling SSL 5-1

6 Map Enterprise Group with Application Role

6.1 Mapping Enterprise Group with Application Role 6-1

7 Configure JNDI name for HTTP Listener

7.1 Configuring JNDI name for HTTP Listener 7-1

8 Configure JMS Queue

8.1 Create Data Sources for JMS Queue 8-1
8.1.1 Create Data Sources for JMS Queue 8-1
8.2 AQ-JMS Queue Configuration 8-9
8.2.1 Create JMS Server 8-10
8.2.2 Create JMS Module 8-13
8.2.3 Subdeployment 8-16
8.2.4 Create JMS Connection Factory 8-18
8.2.5 Create JMS Queue 8-24
8.3 Outbound Queue Configuration 8-28
8.3.1 Create Persistent Stores 8-28
8.3.2 Create JMS Server for Outbound Queue 8-35
8.3.3 Create JMS Module for Outbound Queue 8-40
8.3.4 SubDeployment for Outbound Queue 8-43
8.3.5 Create JMS Connection Factory for Outbound Queue 8-46
8.3.6 Create JMS Queue for Outbound Queue 8-50
8.4 Configure External Client Certificates 8-54
8.4.1 Configure External Client Certificates 8-54
8.5 Create Credentials and System Policies 8-62
8.5.1 Create Credentials and System Policies 8-62
8.6 Deploy MDB EJB 8-73
8.6.1 Deploy MDB EJB 8-73

9 Configure Oracle Analytics Publisher for Application

9.1 Configuring Oracle Analytics Publisher for Application 9-1
9.2 Configuring JNDI Name for http Listener 9-11

10 Launch Application

10.1 Launching Application 10-1

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) 5.9.0.

Application installation consists of following steps.

- Install Software
- Create Domains, Repositories, Data Sources
- Configure Policies
- Deploy Application
- Enable SSL
- Map Enterprise Group with Application Role
- Configure JNDI name for HTTP Listener
- Configure JMS Queue
- Configure Oracle Analytics Publisher for Application
- Launch Application

This section consists of the following topics:

- Prerequisites
- Audience
- Documentation Accessibility
- Diversity and Inclusion
- Conventions

Prerequisites

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

- Oracle Software Delivery Cloud (`http://edelivery.oracle.com/`)

- Oracle Technology Network (OTN)
  1. JDK Version 1.8.0_281 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/wls-main-097127.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.

Audience

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following conventions are used in this document:

Table 1 Conventions used

Term	Refers to
Application	Oracle Financial Services Lending and Leasing

1

Install Software

The following section details the steps to be followed to install weblogic server.

- Installing Oracle WebLogic Server 12c

1.1 Installing Oracle WebLogic Server 12c

Please follow below steps to install oracle weblogic server 12c.

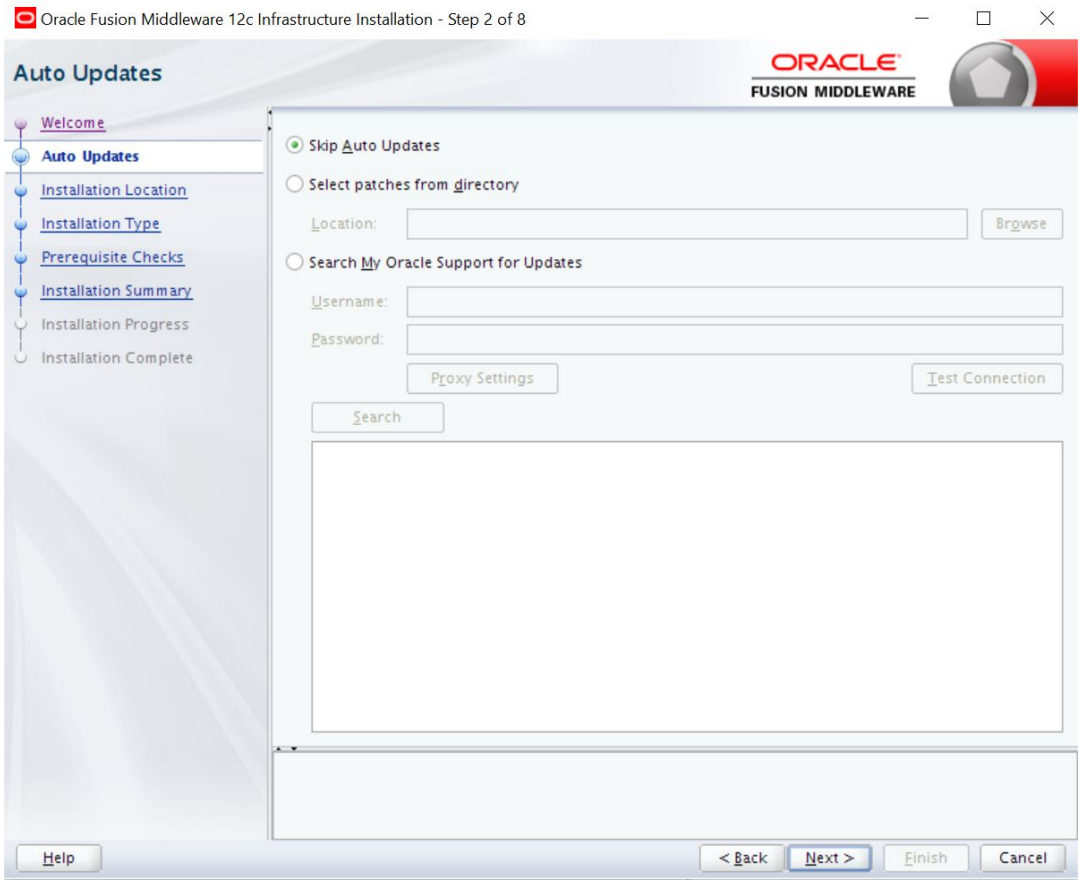
To install using generic Weblogic installer

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

Figure 1-1 Oracle Fusion Middleware infrastructure installer window

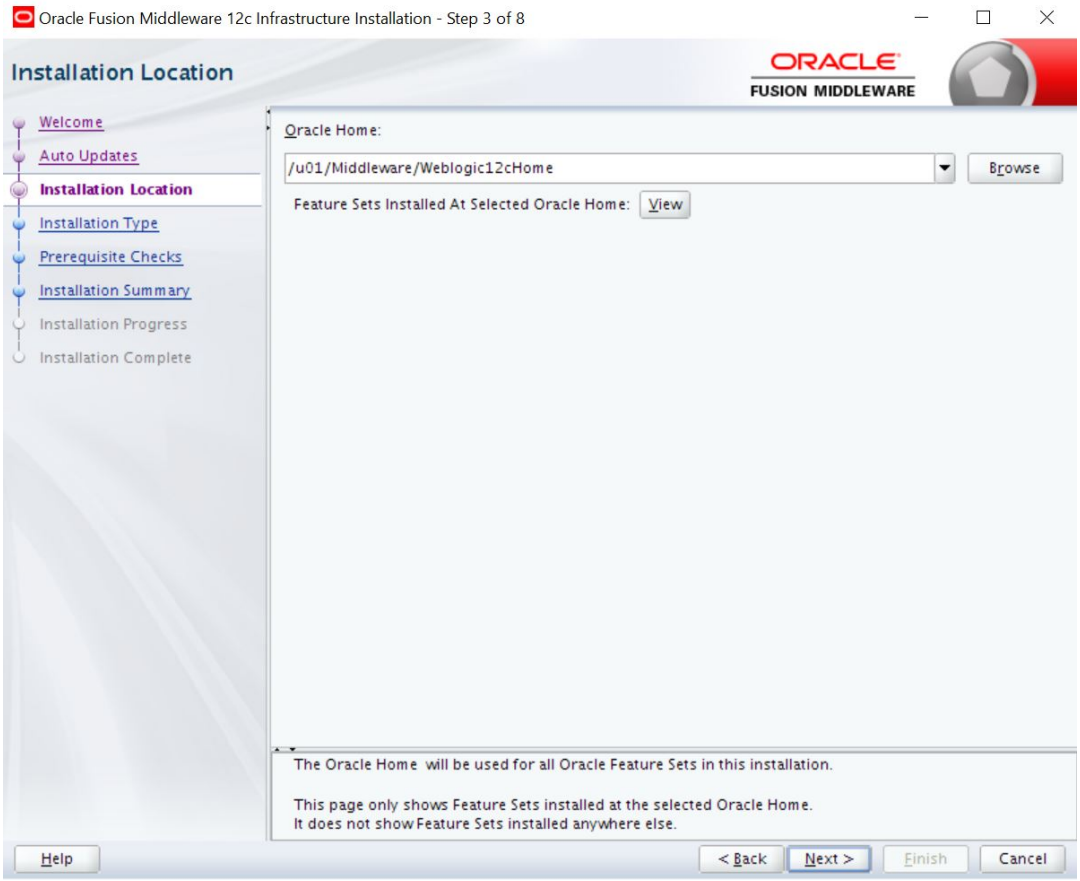
3. The following window is displayed.

Figure 1-2 Auto Updates window



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

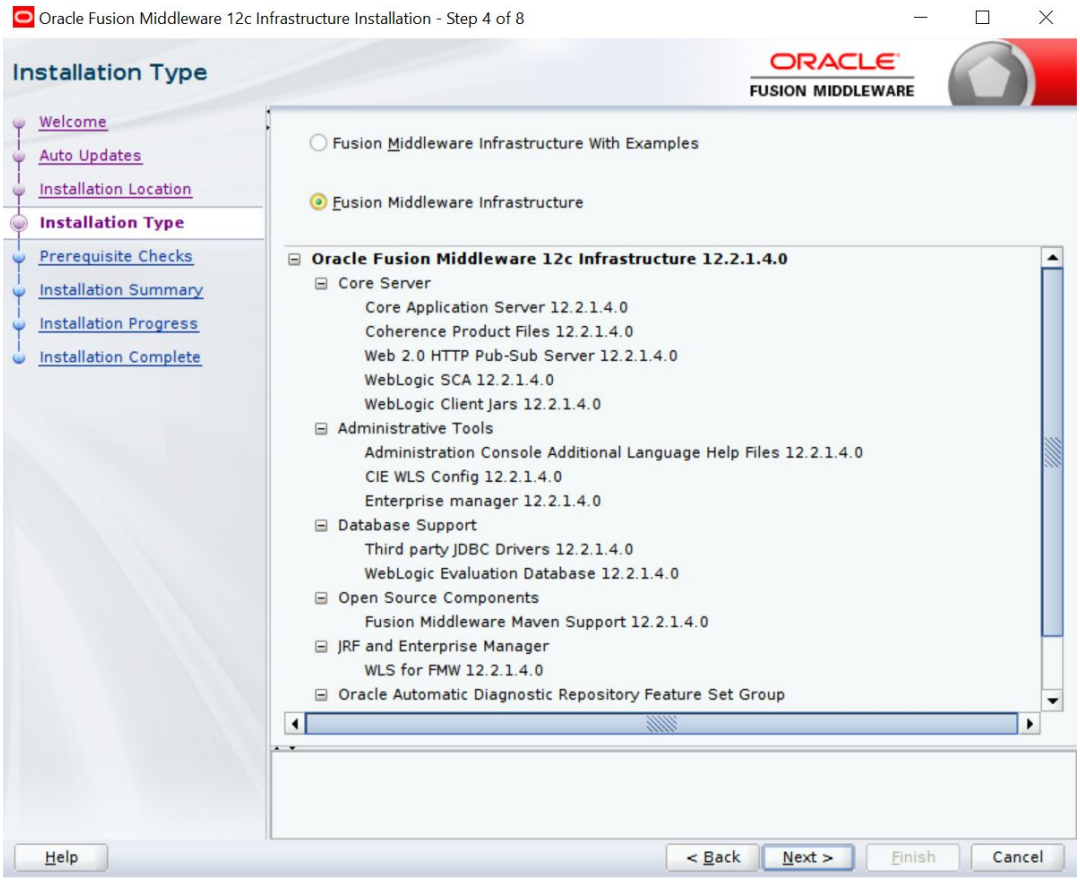
Figure 1-3 Installation Location window



5. Specify the path for Middleware Home Directory. Click **Next**.

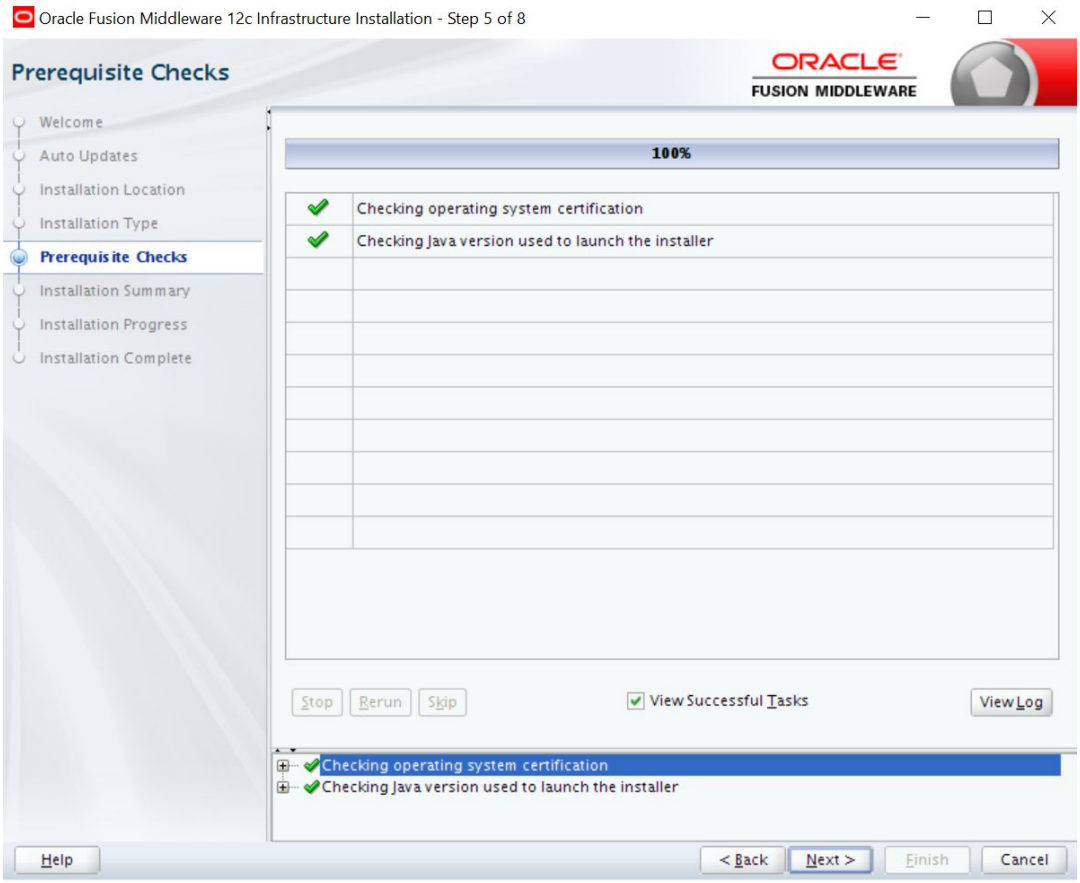
   The following window is displayed.

Figure 1-4 Installation Type window



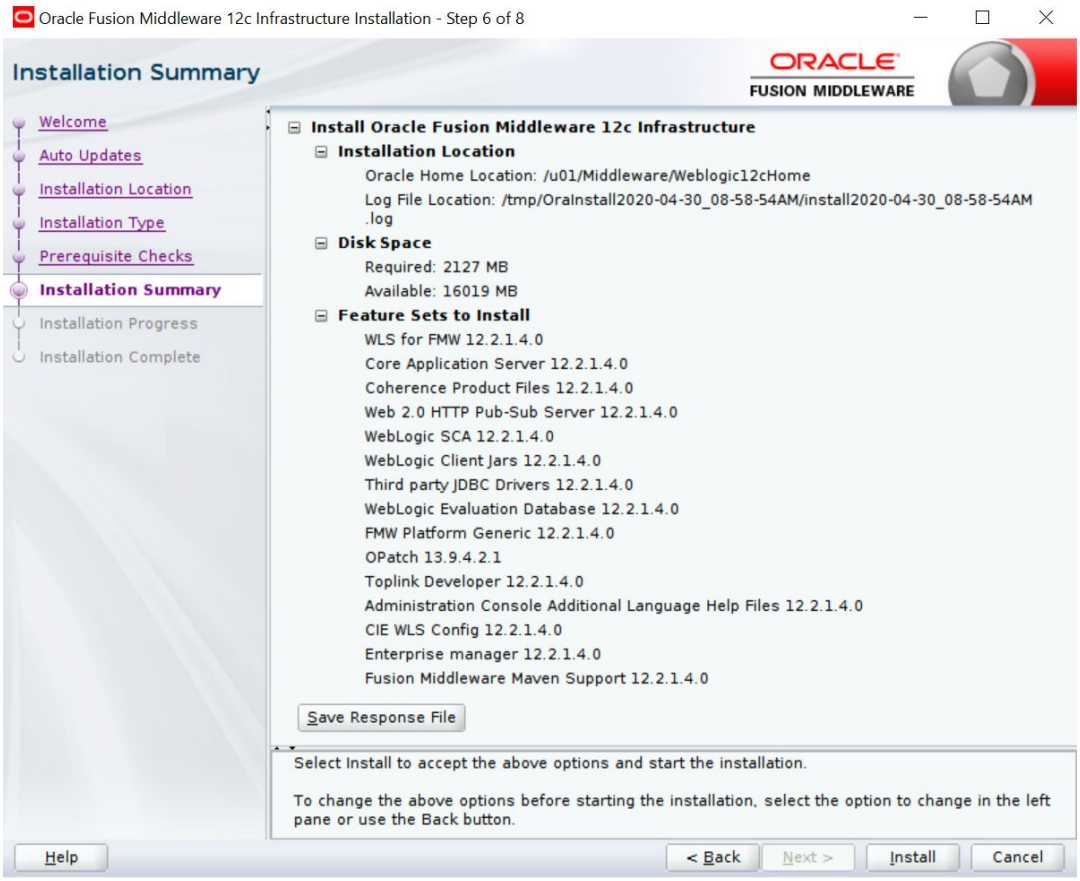
6. Select the option **Fusion Middleware Infrastructure**. Click **Next**.

Figure 1-5 Prerequisite Checks window



7. Click **Next** to continue.

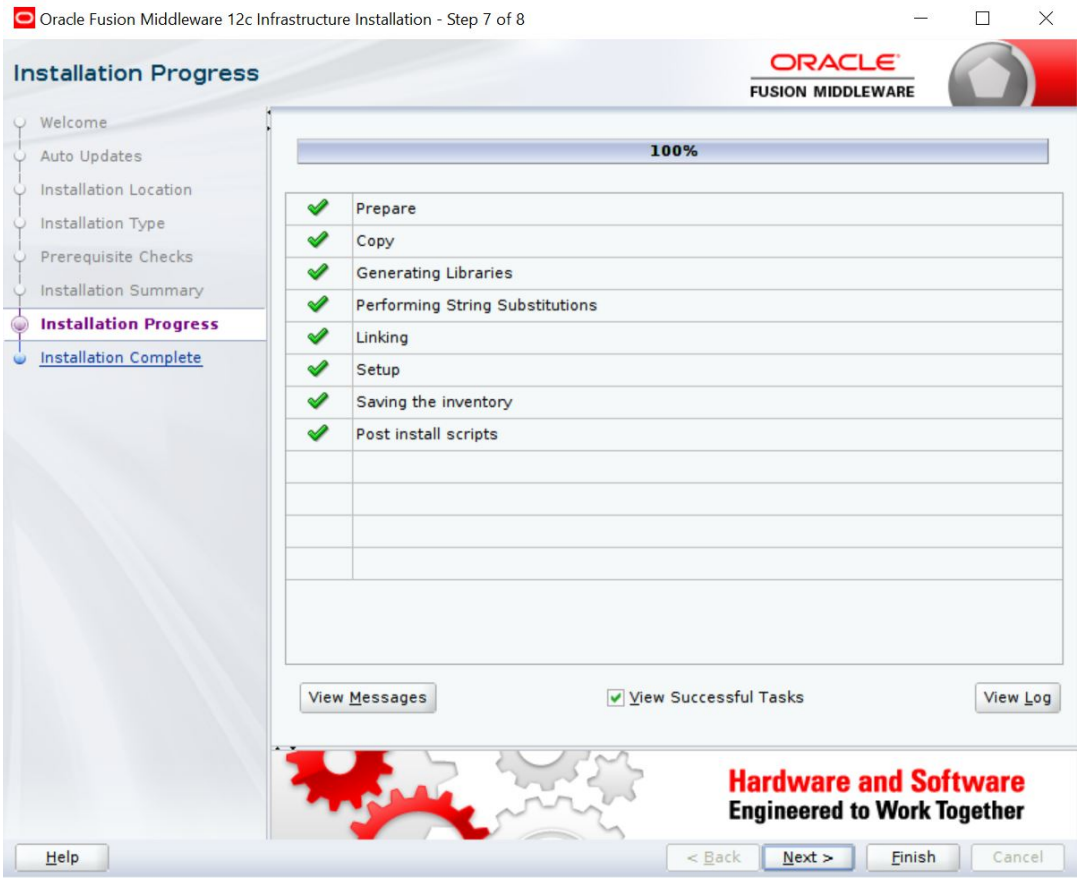
Figure 1-6 Installation Summary window



8. Click **Next**.

   The following window is displayed.

Figure 1-7 Installation Progress window



9. Click **Install**. The weblogic installation starts. Once done, the following window is displayed.

Figure 1-8 Installation Complete window

10. Click **Finish** to close the window.

2

Create Domains, Repositories, Data Sources

The following section details how to create domains, repositories, data sources.

- Creating Schemas using Repository Creation Utility
- Creating Domain and Servers
- Creating Metadata Repository
- Creating Data Source
- Creating SQL Authentication Provider
- Creating User Groups and Users
- Implementing JMX Policy for Change Password

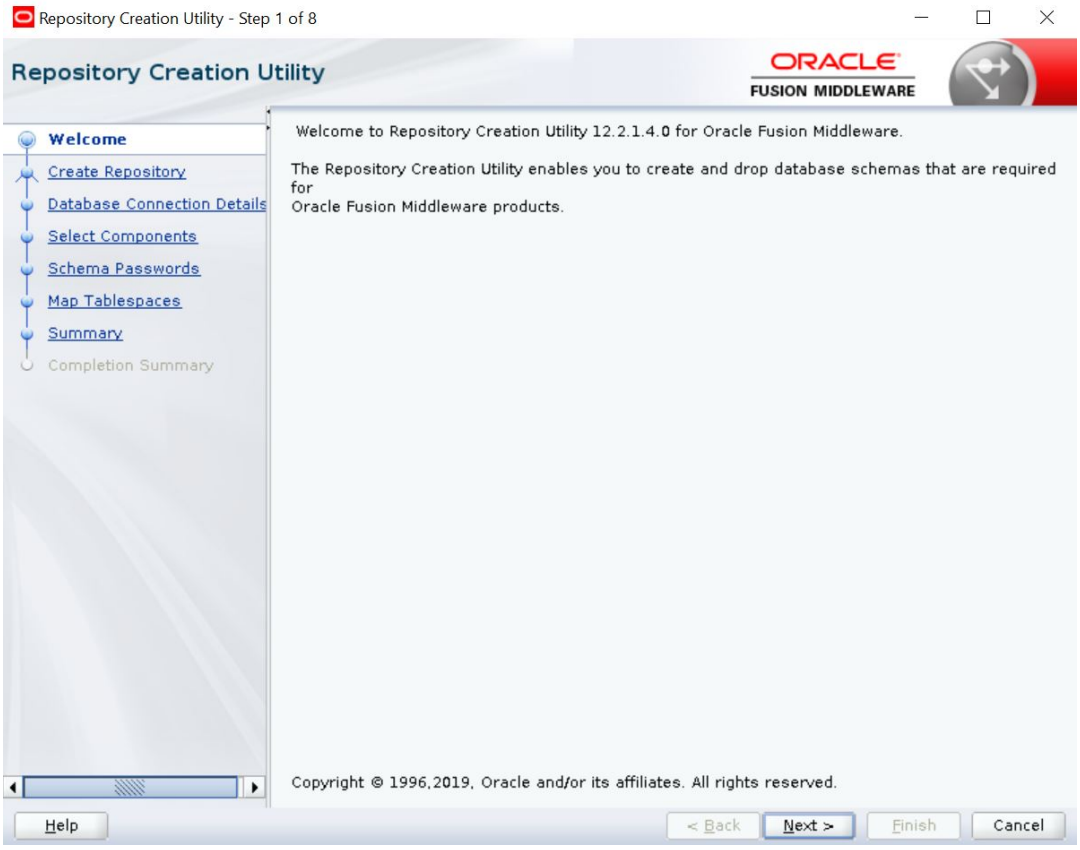
2.1 Creating Schemas using Repository Creation Utility

The following section details the steps to create 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.

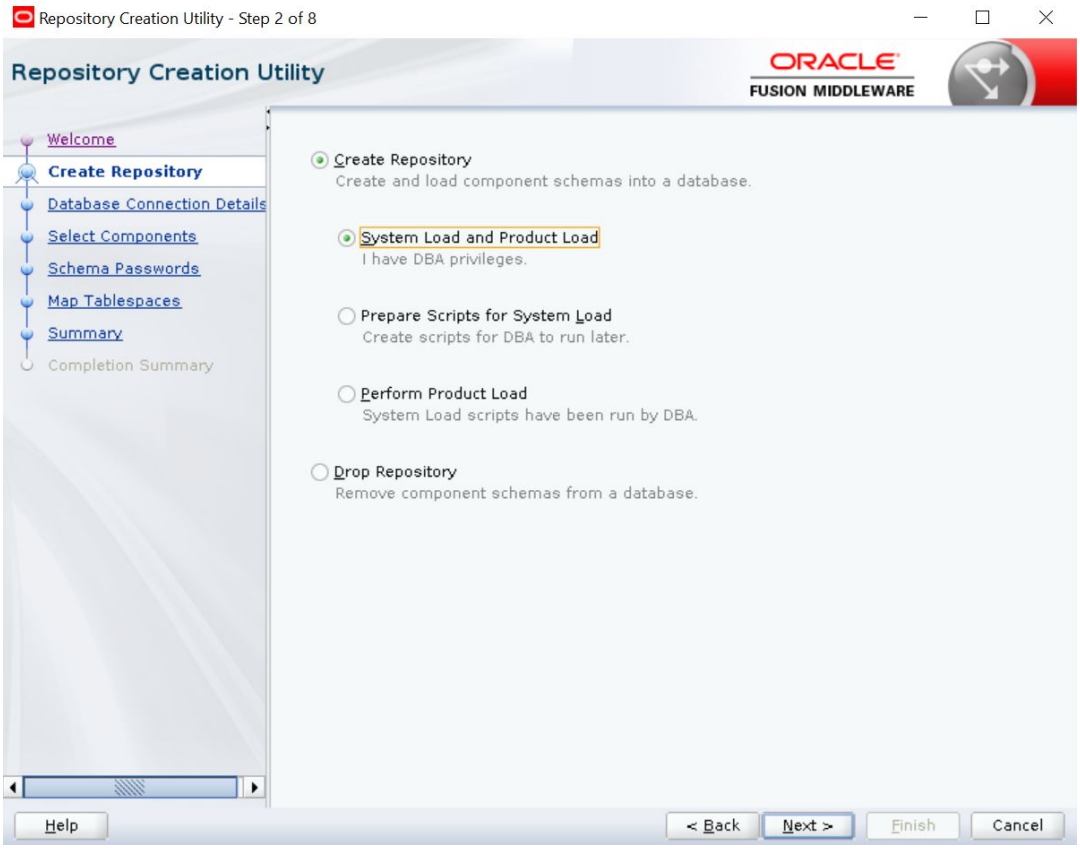
Figure 2-1 Repository Creation Utility 1



2. Click **Next**.

   The following window is displayed.

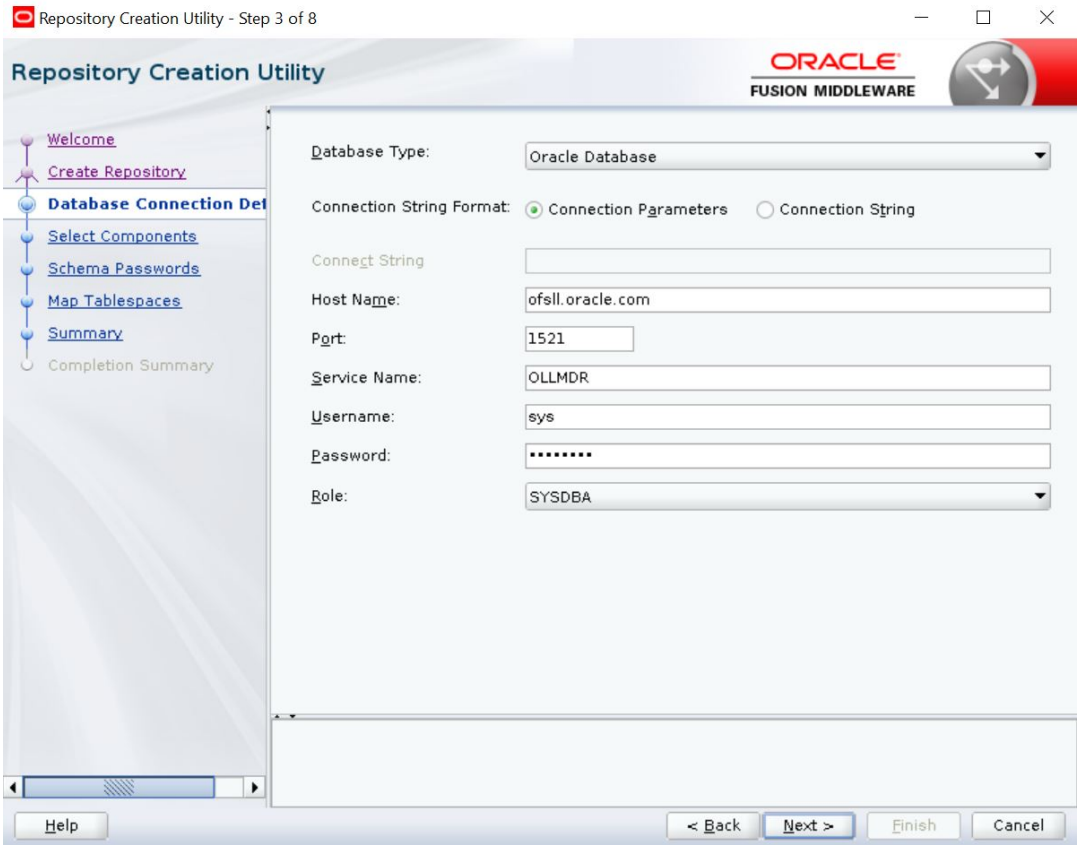
Figure 2-2 Repository Creation Utility 2



3. Select **Create Repository** and select **System Load and Product Load**. Click **Next**.

   The following screen is displayed.

Figure 2-3 Repository Creation Utility 3



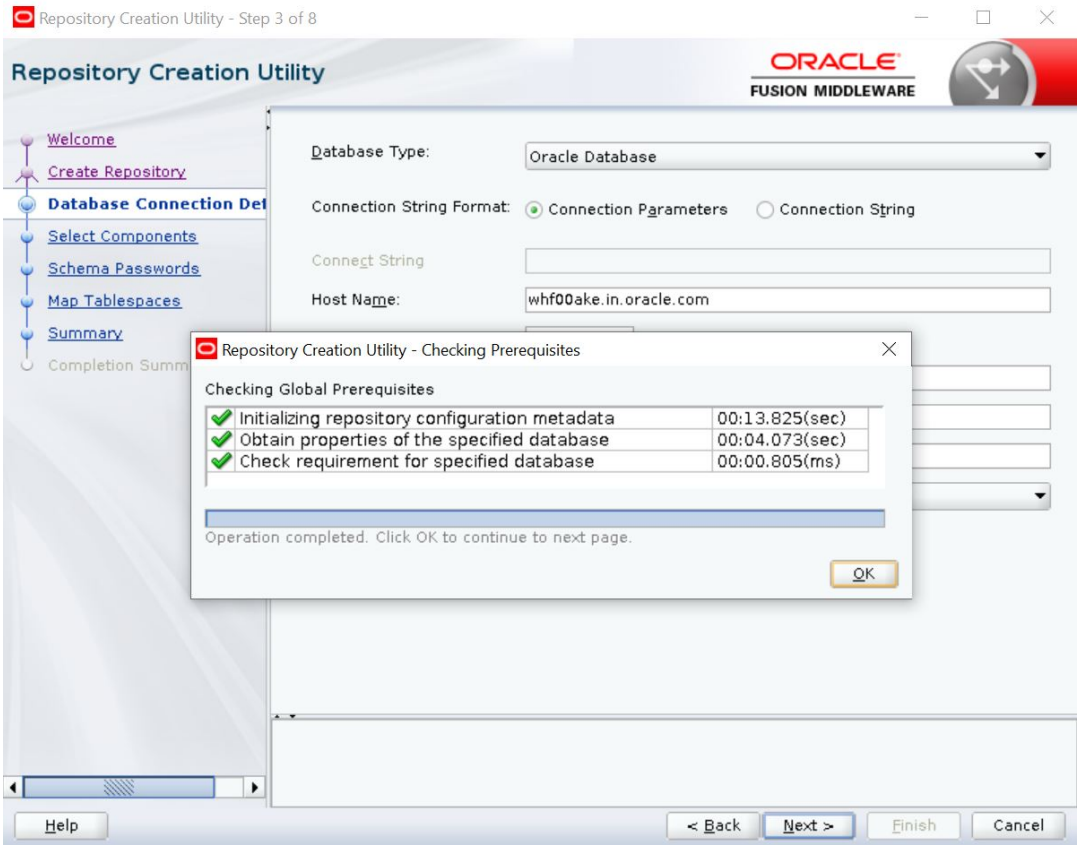
4. Provide database details where you want to create schemas, as shown in the above screen.

> **Note:**
>
> You will require a user with SYSDBA role to create schemas.

5. Click **Next**.

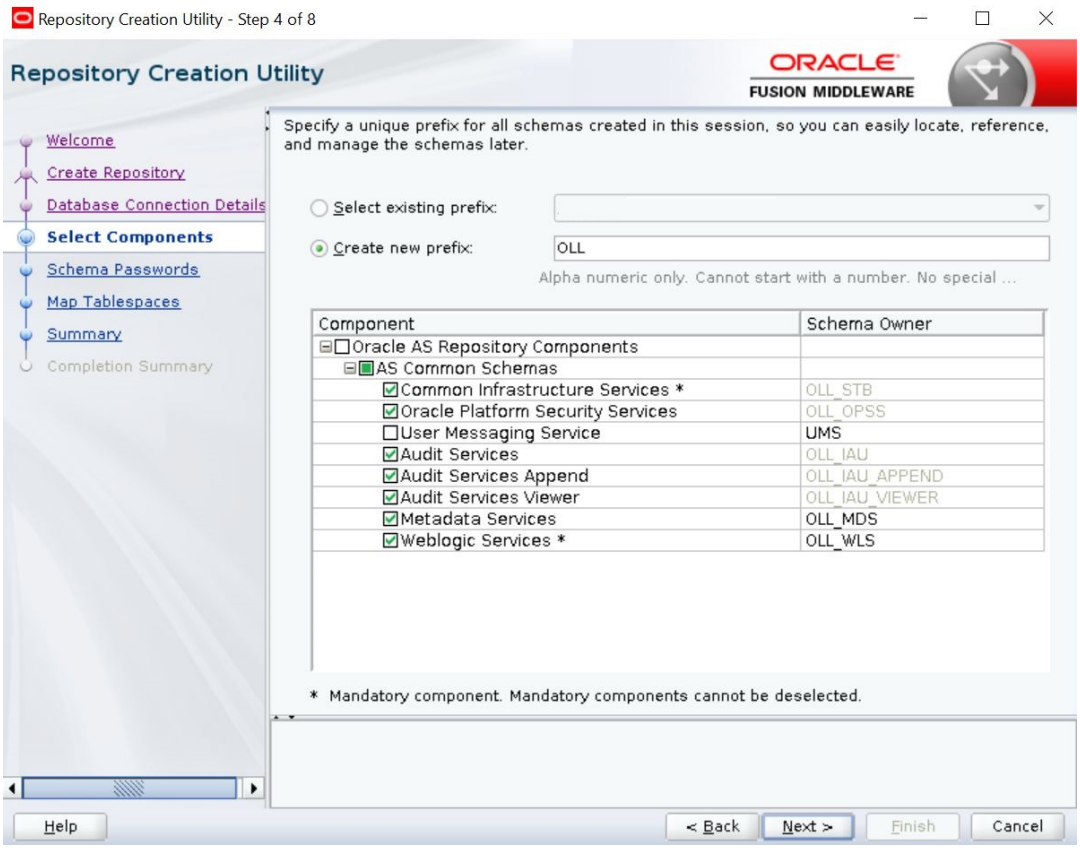
   The following window is displayed.

Figure 2-4 Repository Creation Utility 4



6. Click **OK** in the confirmation dialog.
7. Click **Next** the following window is displayed.

Figure 2-5 Repository Creation Utility 5



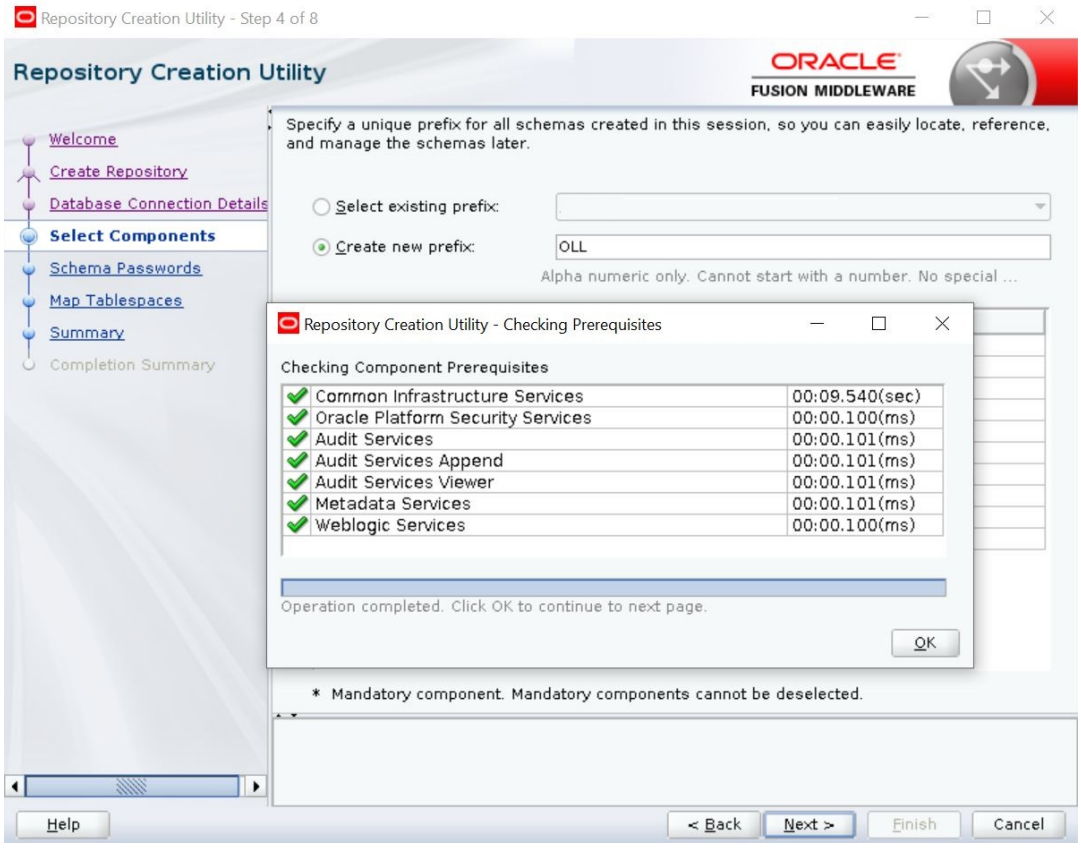
8. Select **Create new Prefix** option and specify the value.

   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.

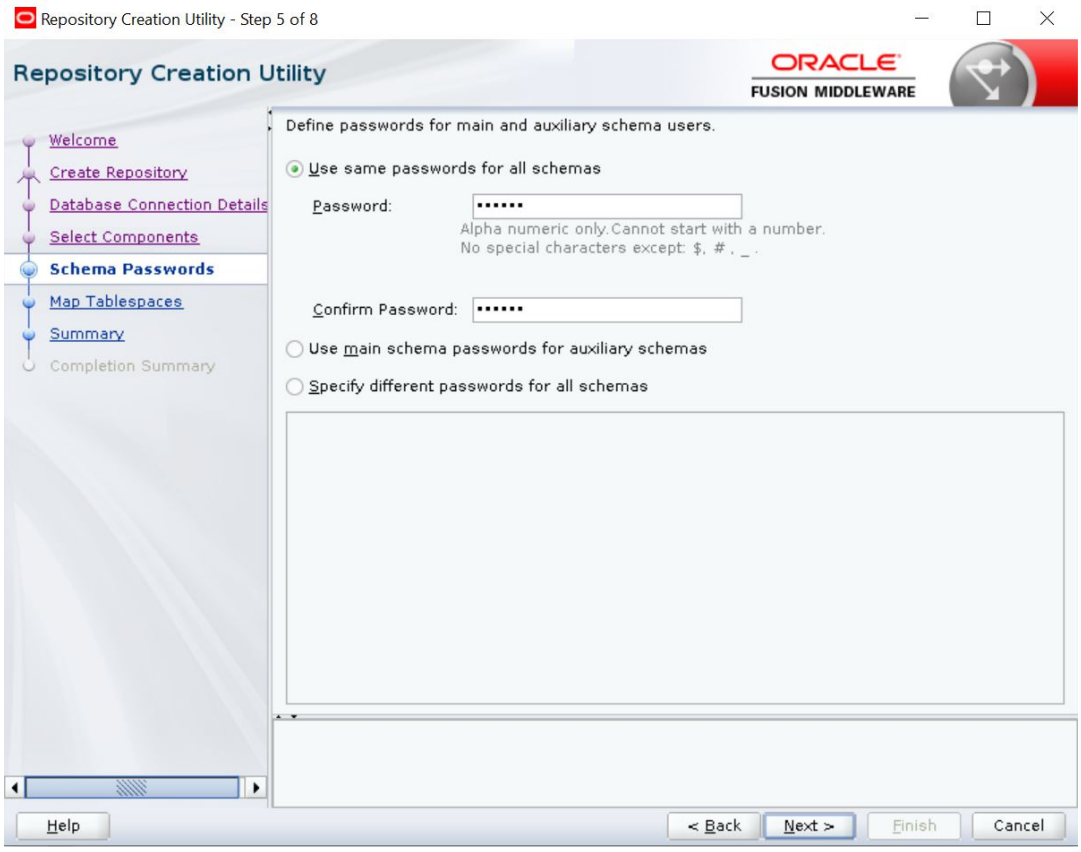
Figure 2-6 Repository Creation Utility 6



10. Click **Next**.

    The following window is displayed.

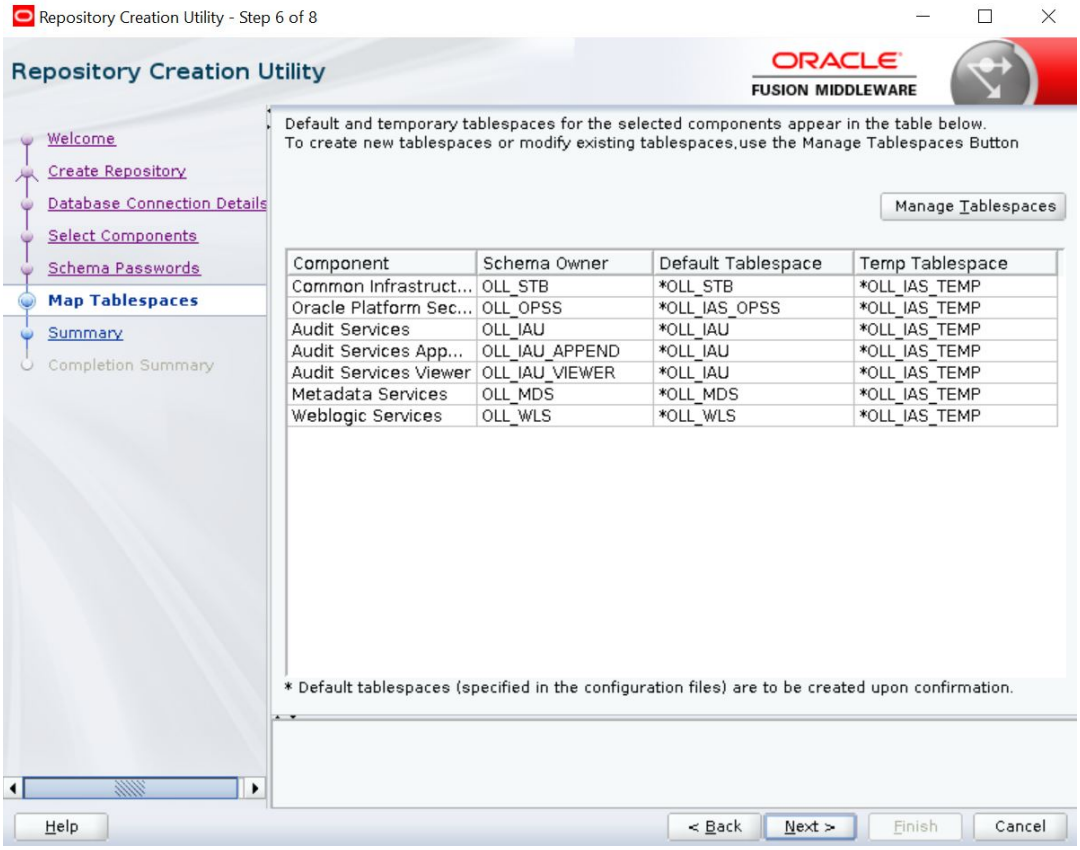
Figure 2-7 Repository Creation Utility 7



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.

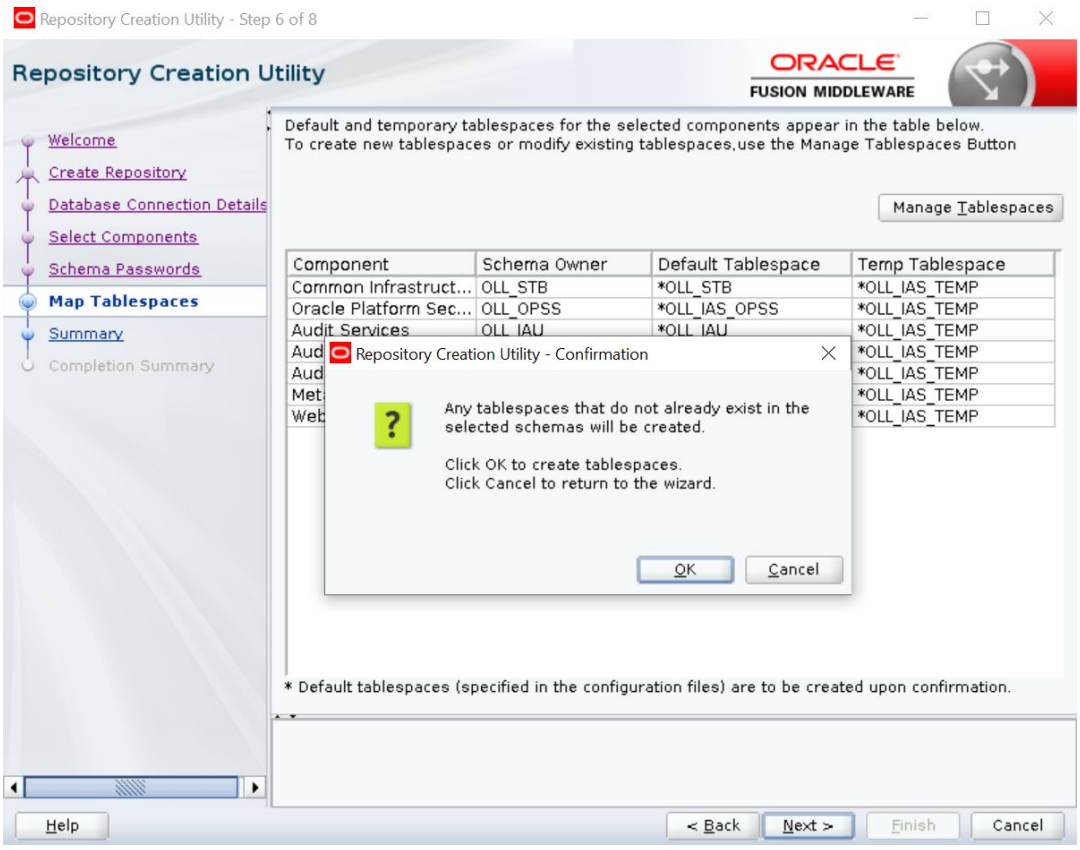
Figure 2-8 Repository Creation Utility 8



13. Click **Next**.

    The following window is displayed.

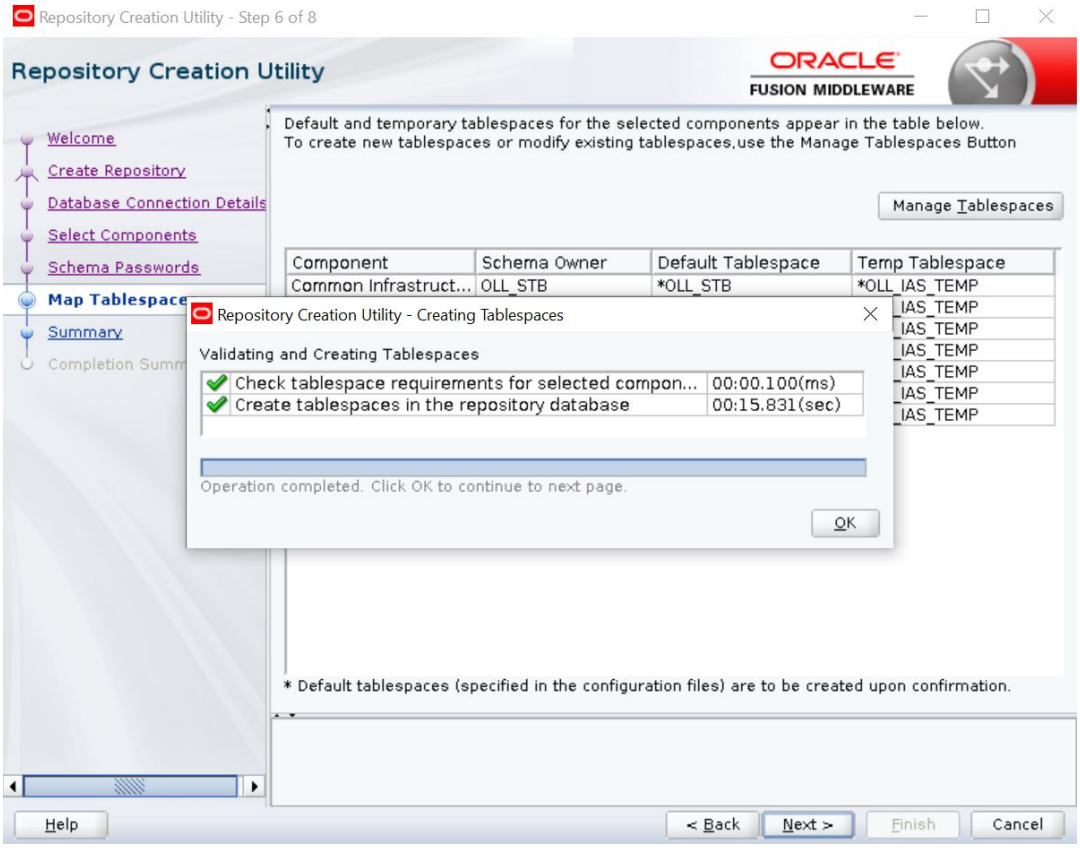
Figure 2-9 Repository Creation Utility 9



14. Click **OK** in the confirmation dialog.

    The following window is displayed.

Figure 2-10 Repository Creation Utility 10



15. Click **OK** in the confirmation dialog.

    The following window is displayed.

Figure 2-11 Repository Creation Utility 11

16. Click **Create**.

    The following windows are displayed.

Figure 2-12 Repository Creation Utility 12

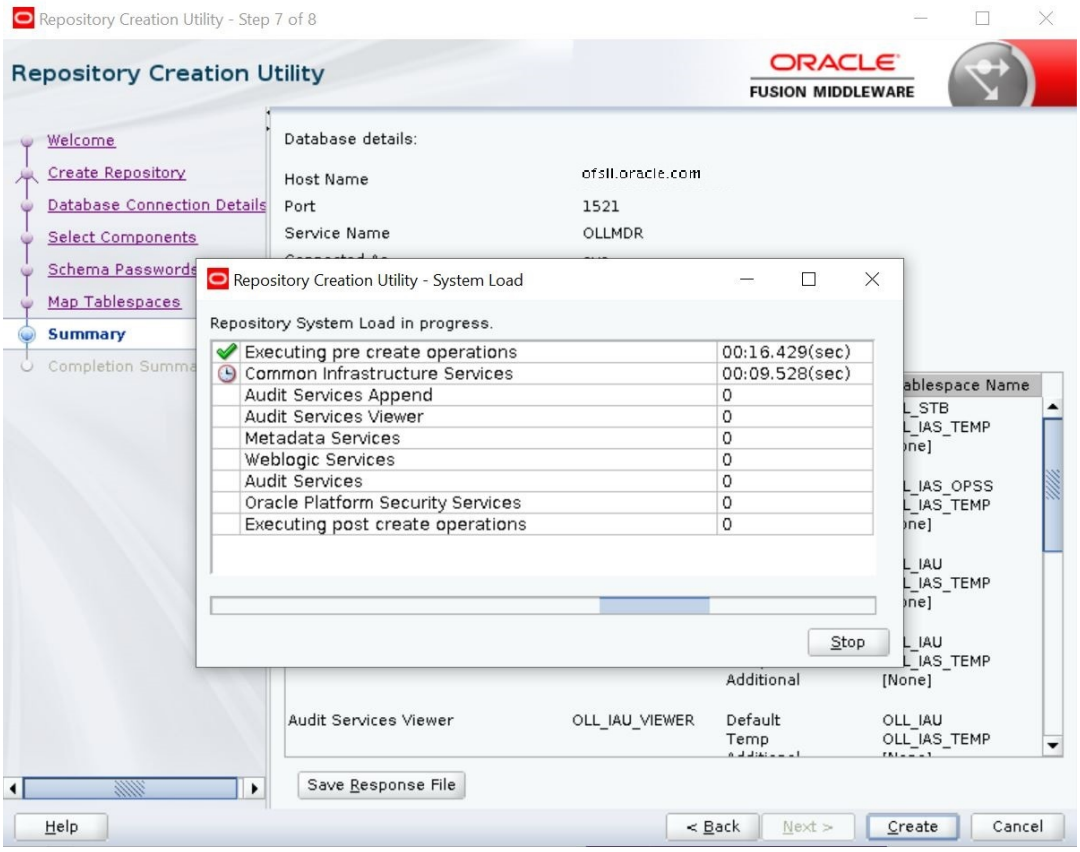
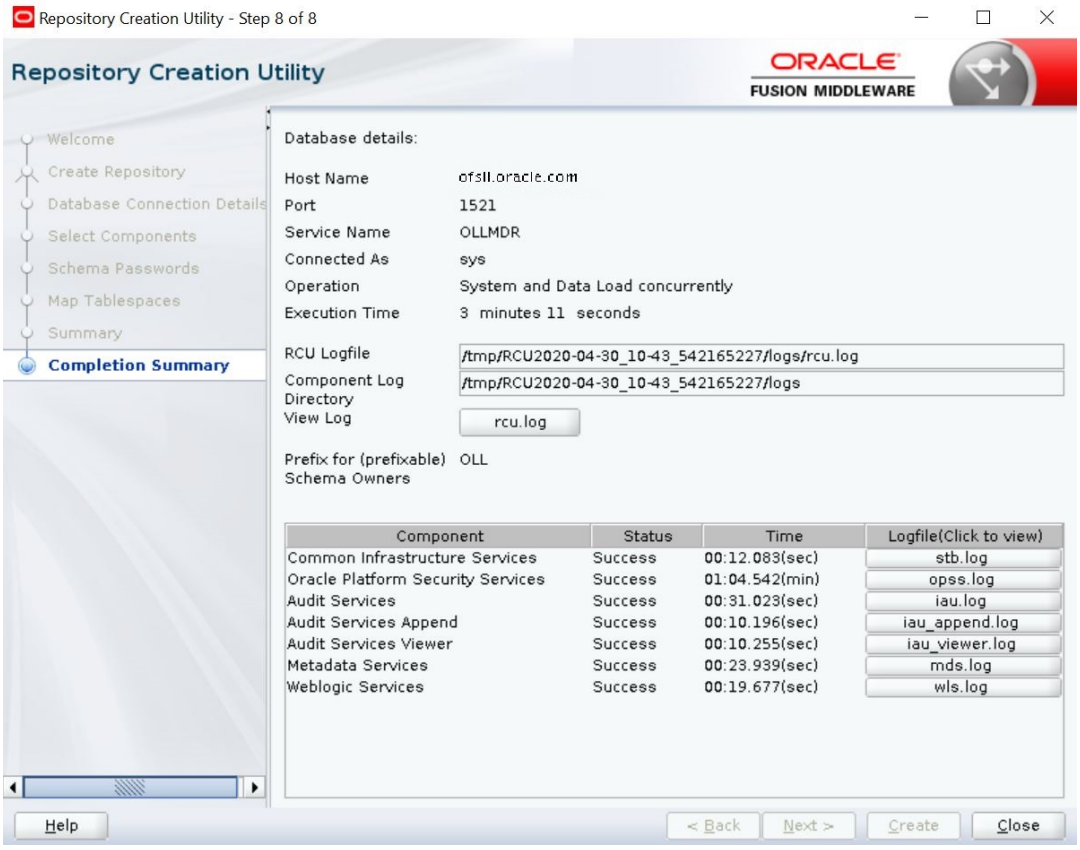


Figure 2-13 Repository Creation Utility 13



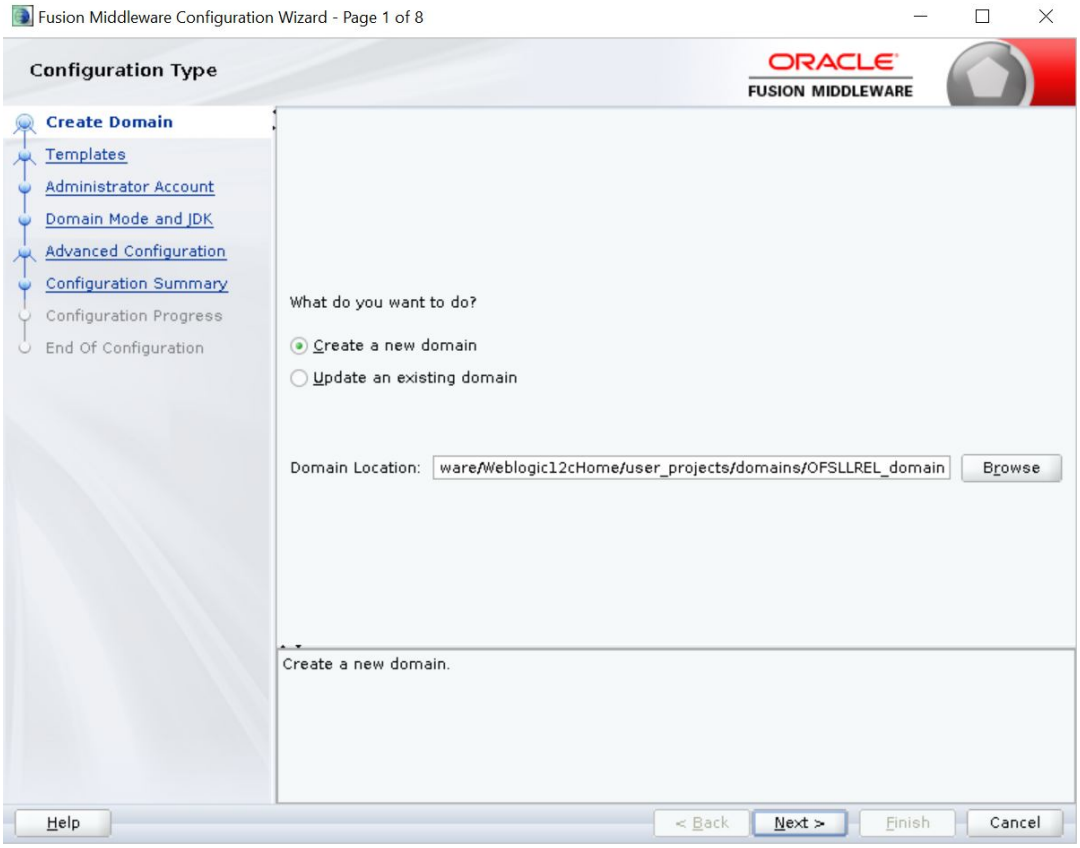
17. Click **Close** to close the window.

2.2 Creating Domain and Servers

The following section details the steps to create 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**

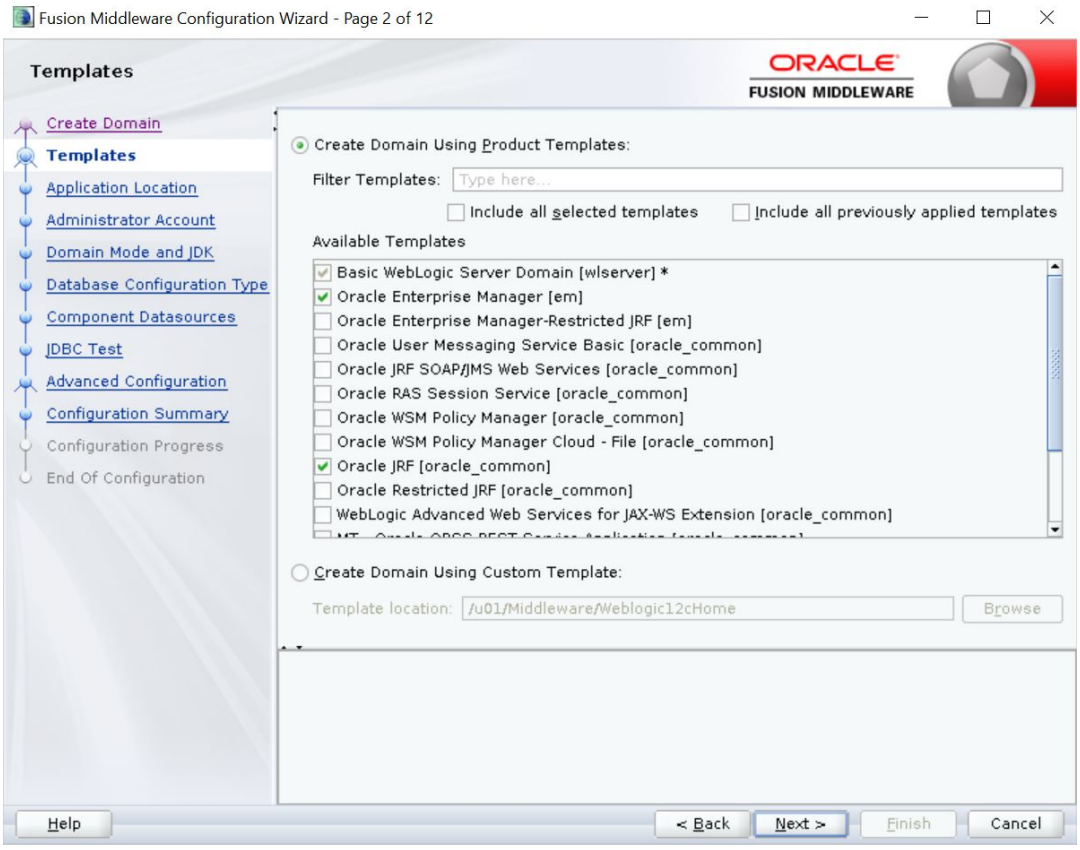
Figure 2-14 Weblogic Domain Creation 1



3. Select **Create a new domain** and specify the Domain Location.
4. Click **Next** to continue.

   The following window is displayed.

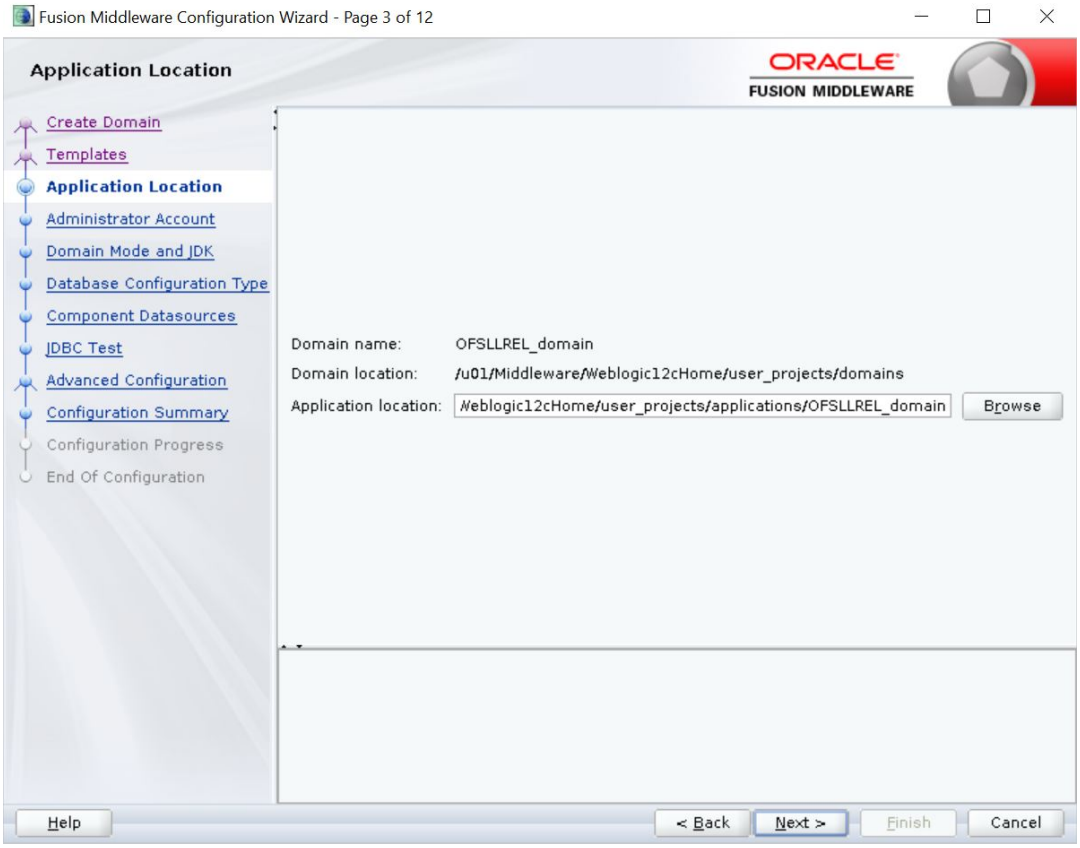
Figure 2-15 Weblogic Domain Creation 2



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

   The following window is displayed.

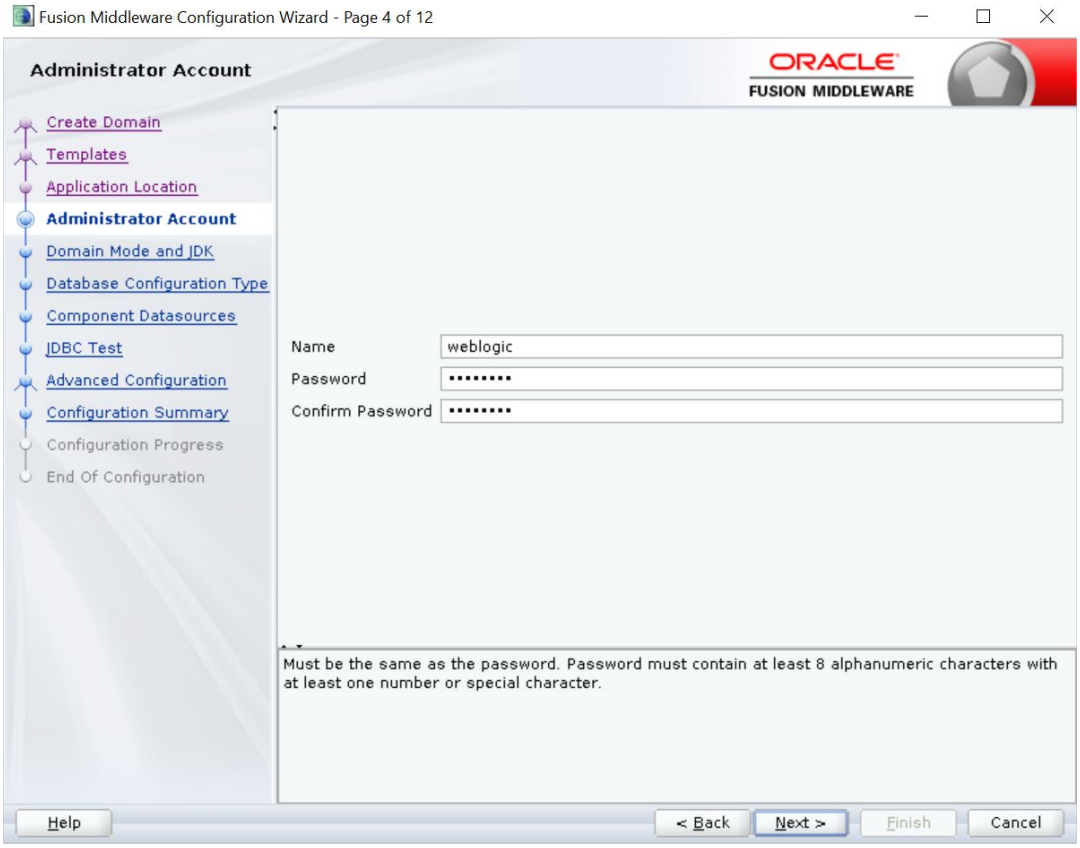
Figure 2-16 Weblogic Domain Creation 3



7. Specify the Domain Name in the **Application location** field. You can click browse to directly select the path (if required). Click **Next**.

   The following window is displayed.

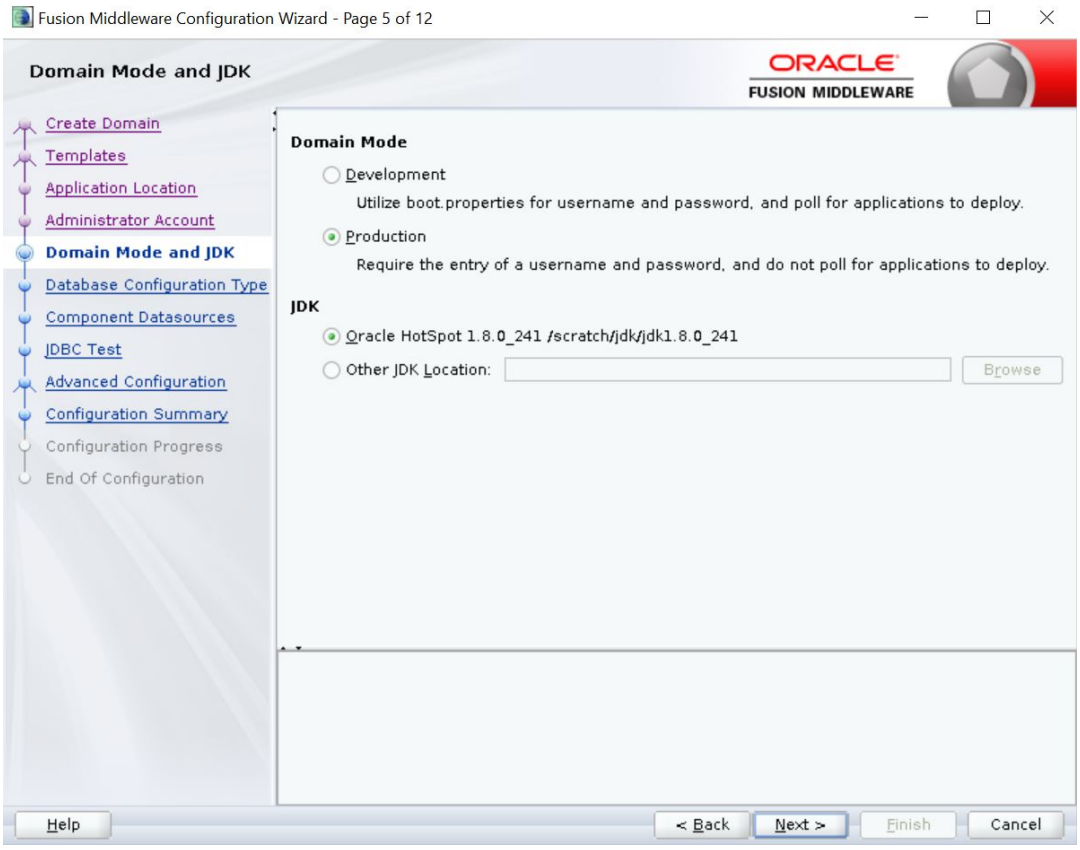
Figure 2-17 Weblogic Domain Creation 4



8. Enter credentials for the following:
   - Name
   - Password
   - Confirm Password
9. Click **Next**.

   The following window is displayed.

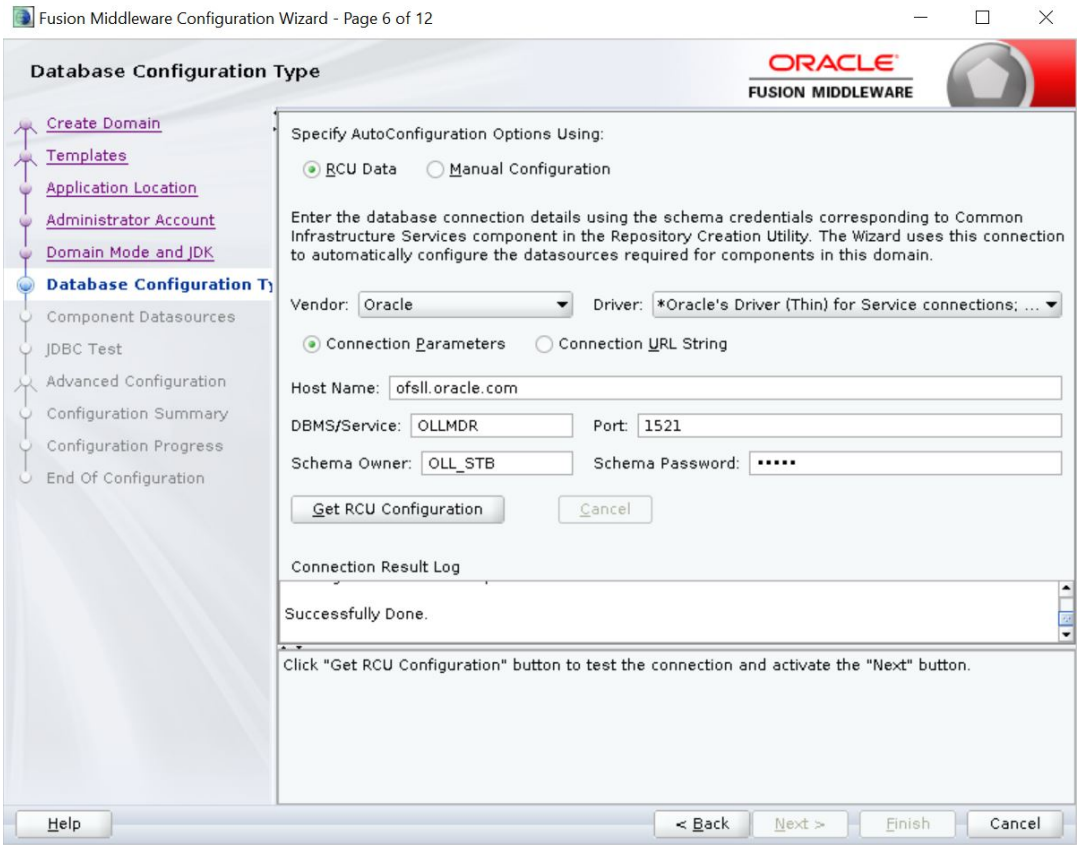
Figure 2-18 Weblogic Domain Creation 5



10. Select the Domain Mode as **Production** and **JDK** from Available JDKs. You can also select any other JDK by selecting **Other JDK Location**option. Click **Next**.

    The following window is displayed.

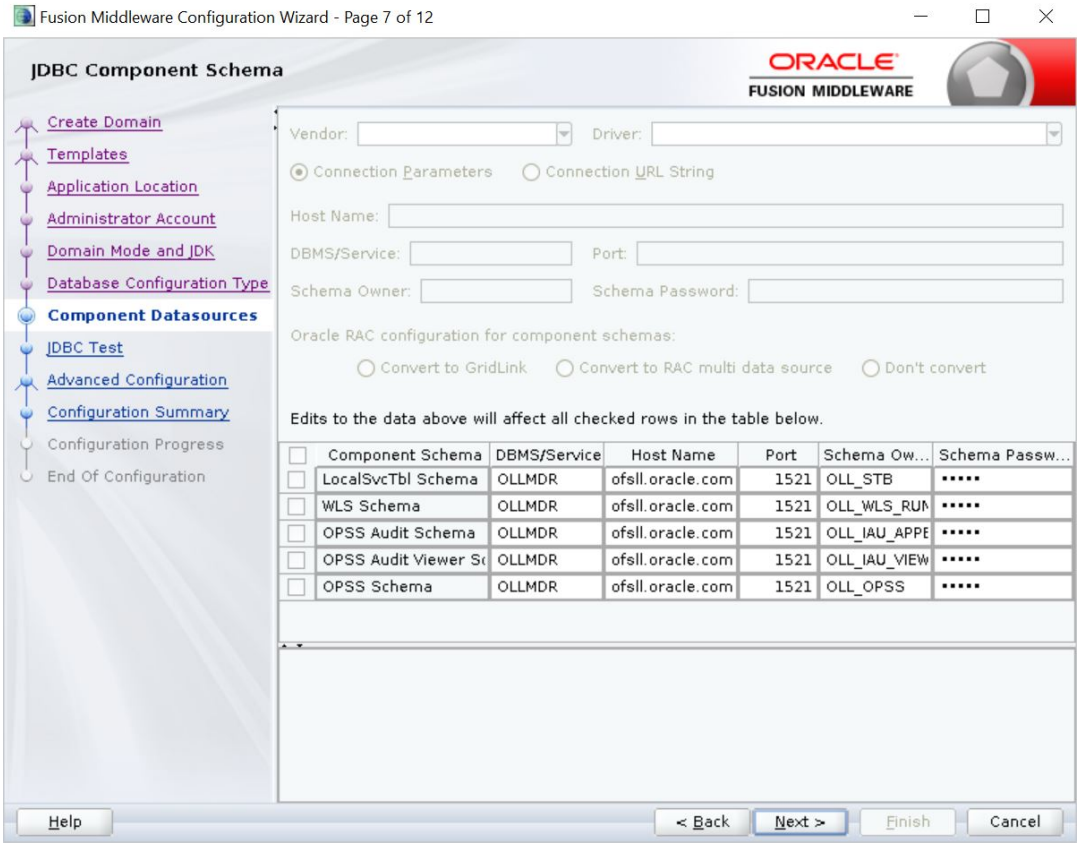
Figure 2-19 Weblogic Domain Creation 6



11. Specify the RCU data and click on **Get RCU Configuration**.

    The following window is displayed.

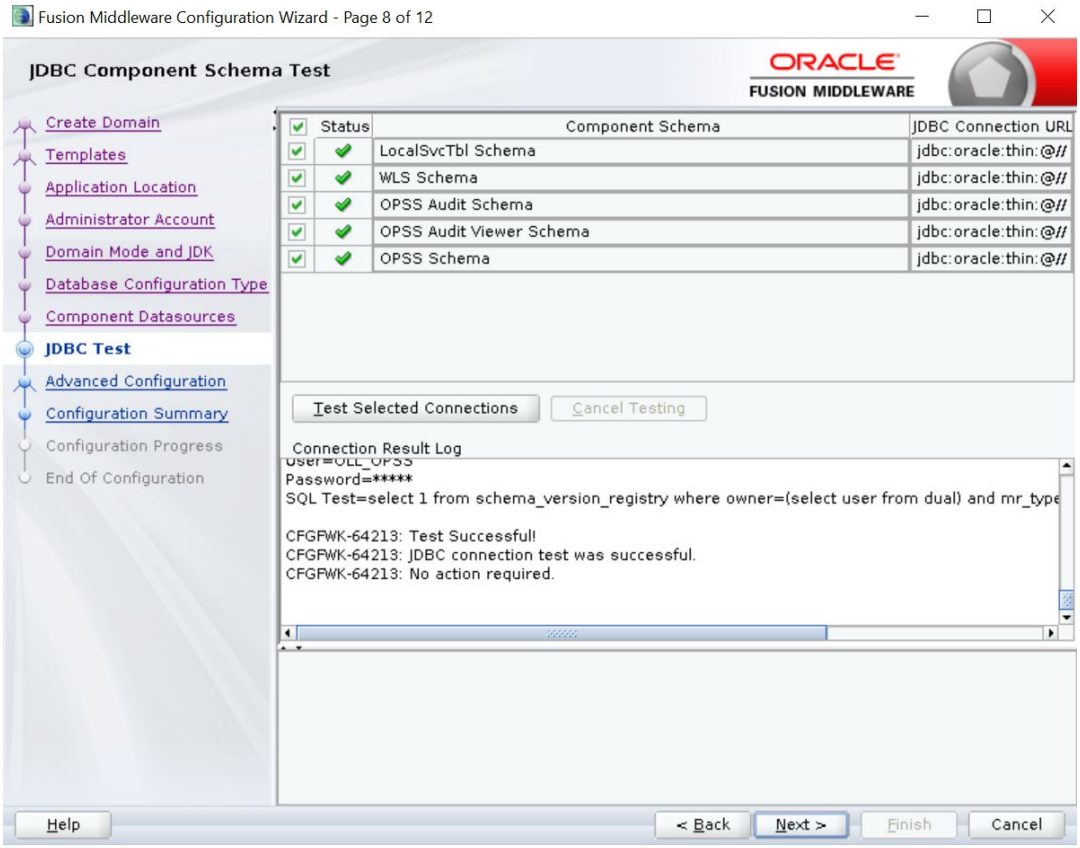
Figure 2-20 Weblogic Domain Creation 7



12. Click **Next**.

    The following window is displayed.

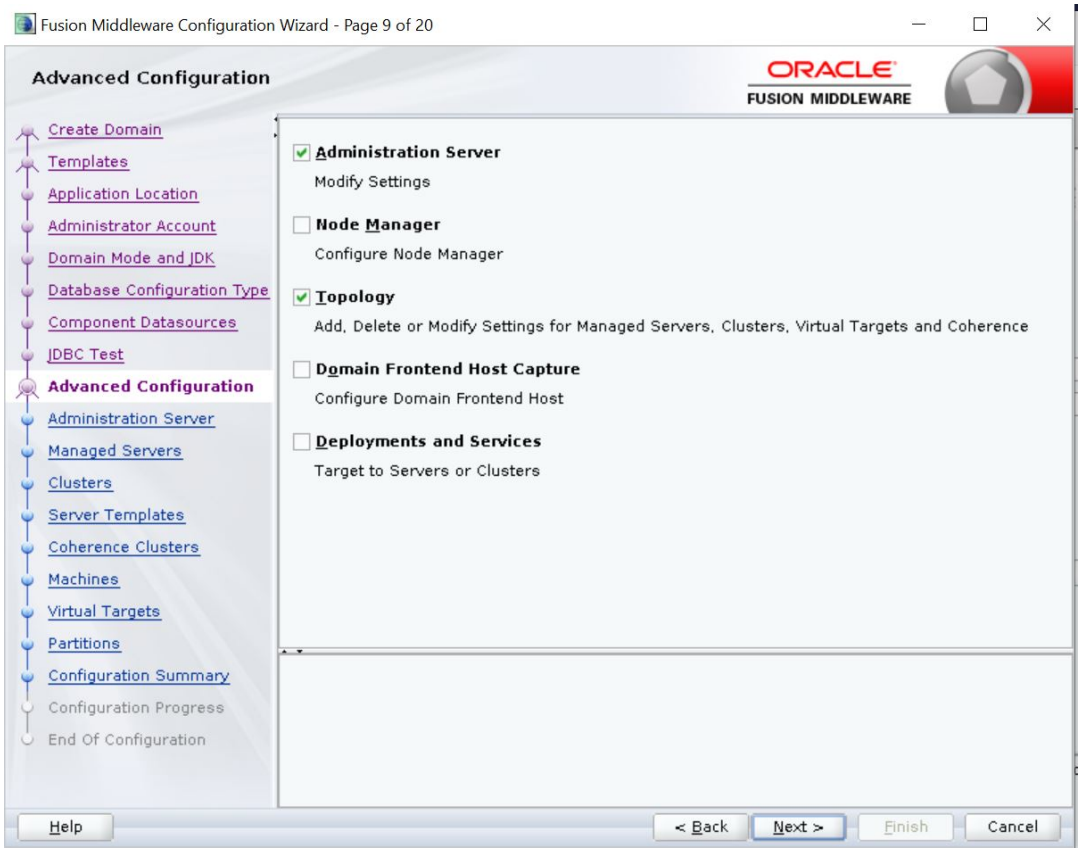
Figure 2-21 Weblogic Domain Creation 8



13. Click **Next**.

    The following window is displayed.

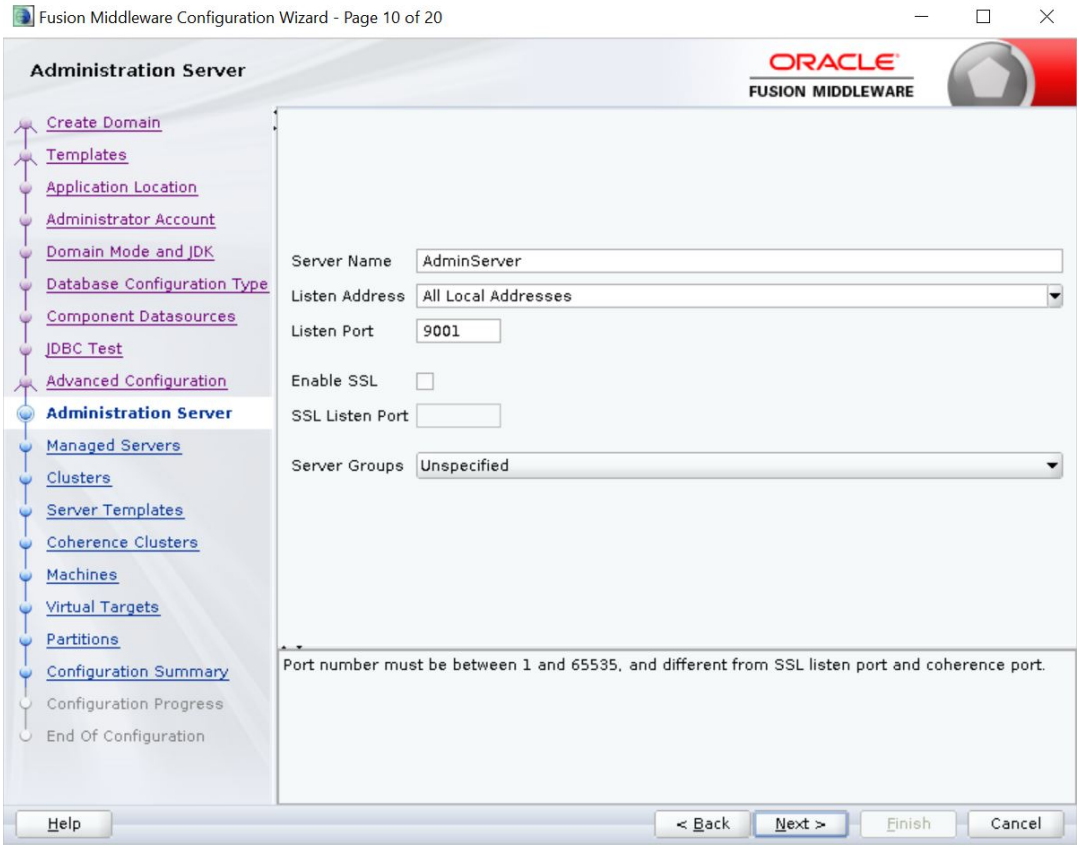
Figure 2-22 Weblogic Domain Creation 9



14. Select **Administration Server** and **Topology** and click **Next**.

    The following window is displayed.

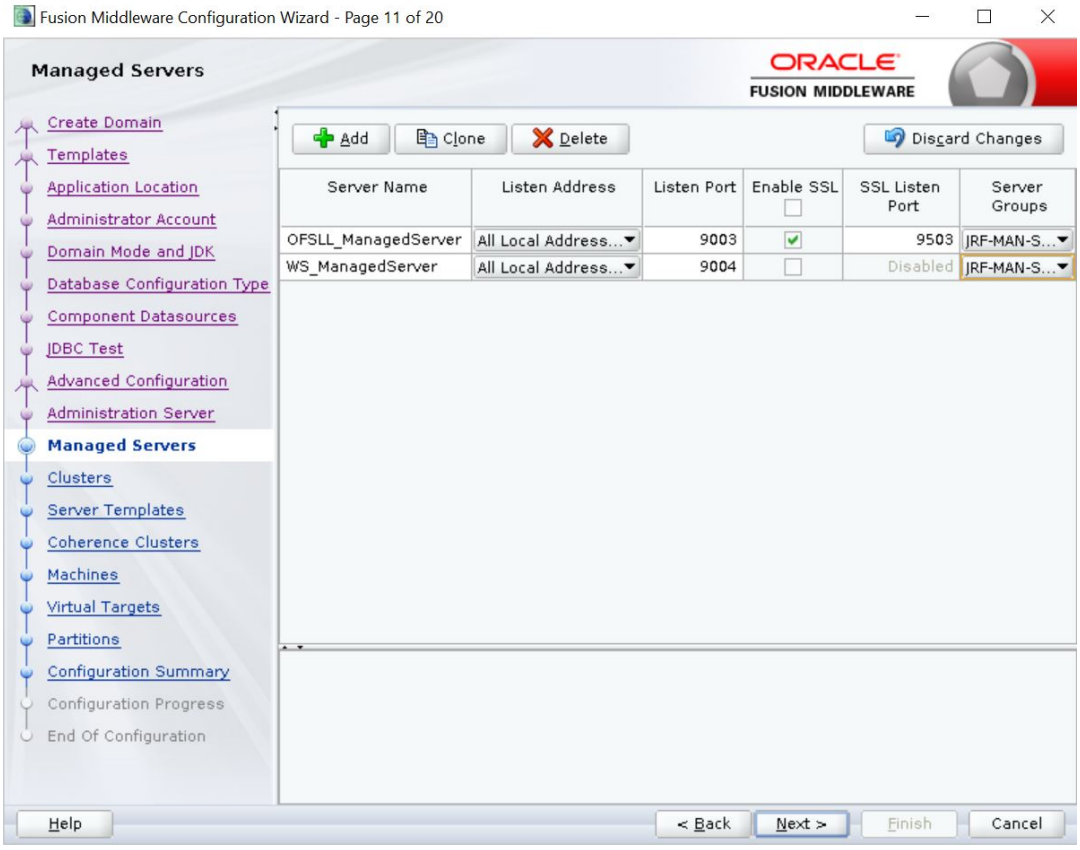
Figure 2-23 Weblogic Domain Creation 10



15. Enter Administration **Server Name** and **Listen Port** details. Click **Next**.

    The following window is displayed.

Figure 2-24 Weblogic Domain Creation 11



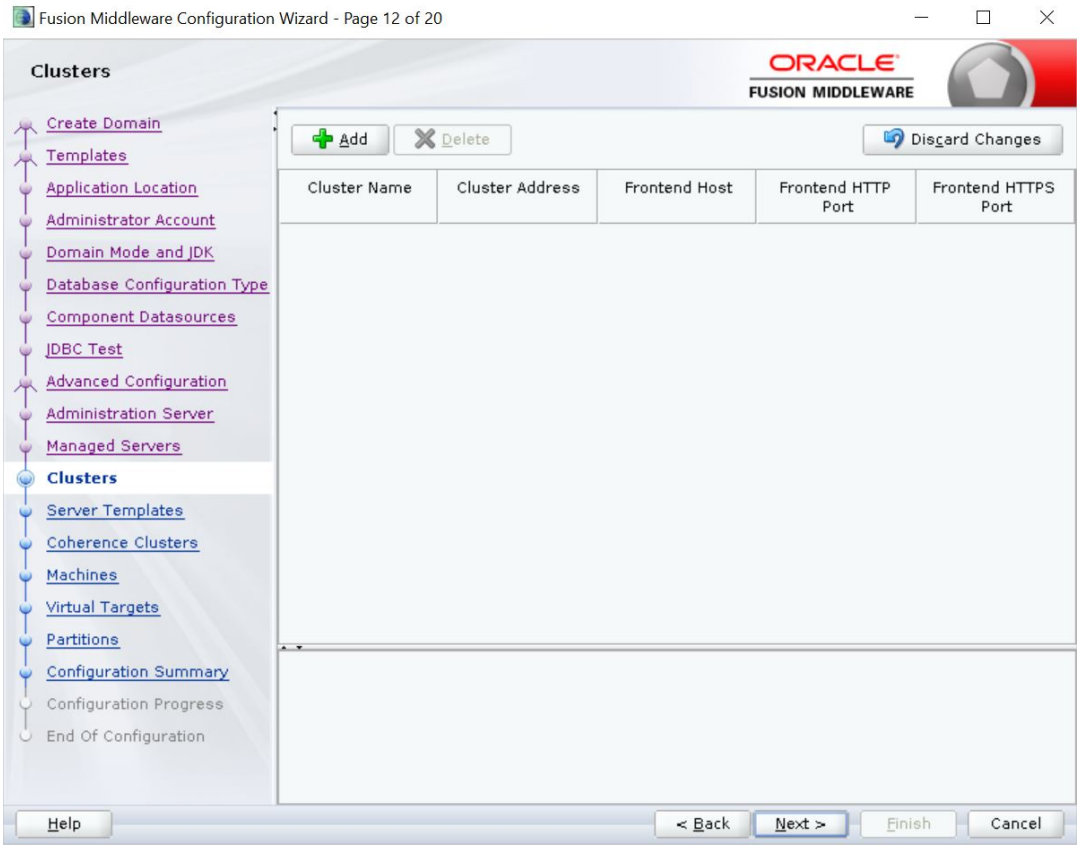
16. Click **Add** button to create **ManagedServer**.
17. Select the Server Group as **JRF-MAN-SVR**. Selecting this server group ensures that the Oracle JRF services are targeted to the specific Managed Servers created.

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

18. Click **Next**.

    The following window is displayed.

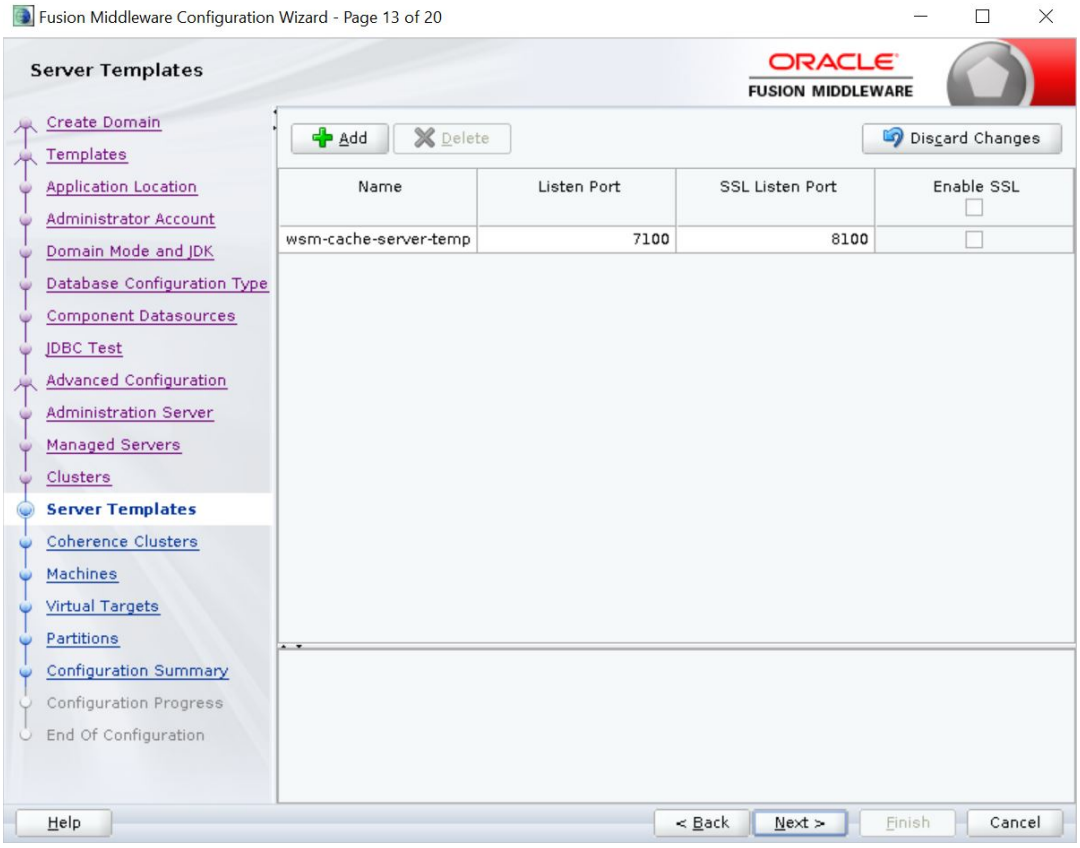
Figure 2-25 Weblogic Domain Creation 12



19. Configure as required and click **Next**.

    The following window is displayed.

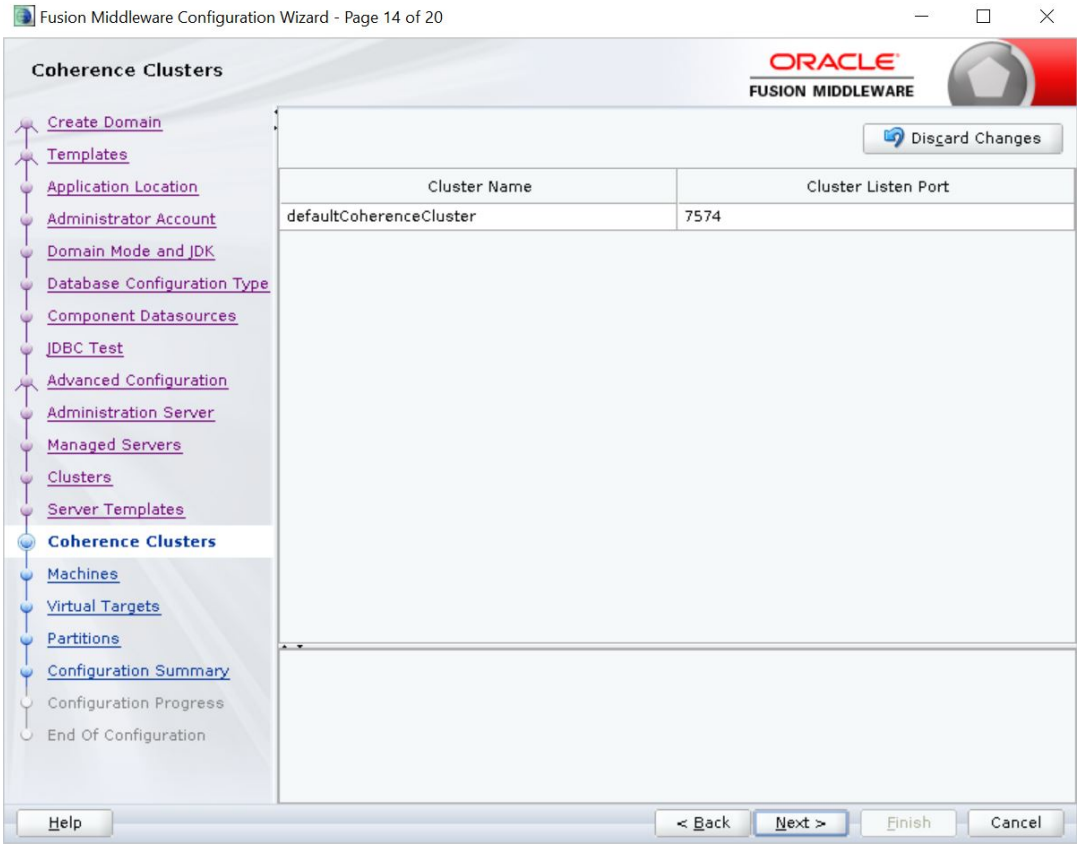
Figure 2-26 Weblogic Domain Creation 13



20. Configure as required and click **Next**.

    The following window is displayed.

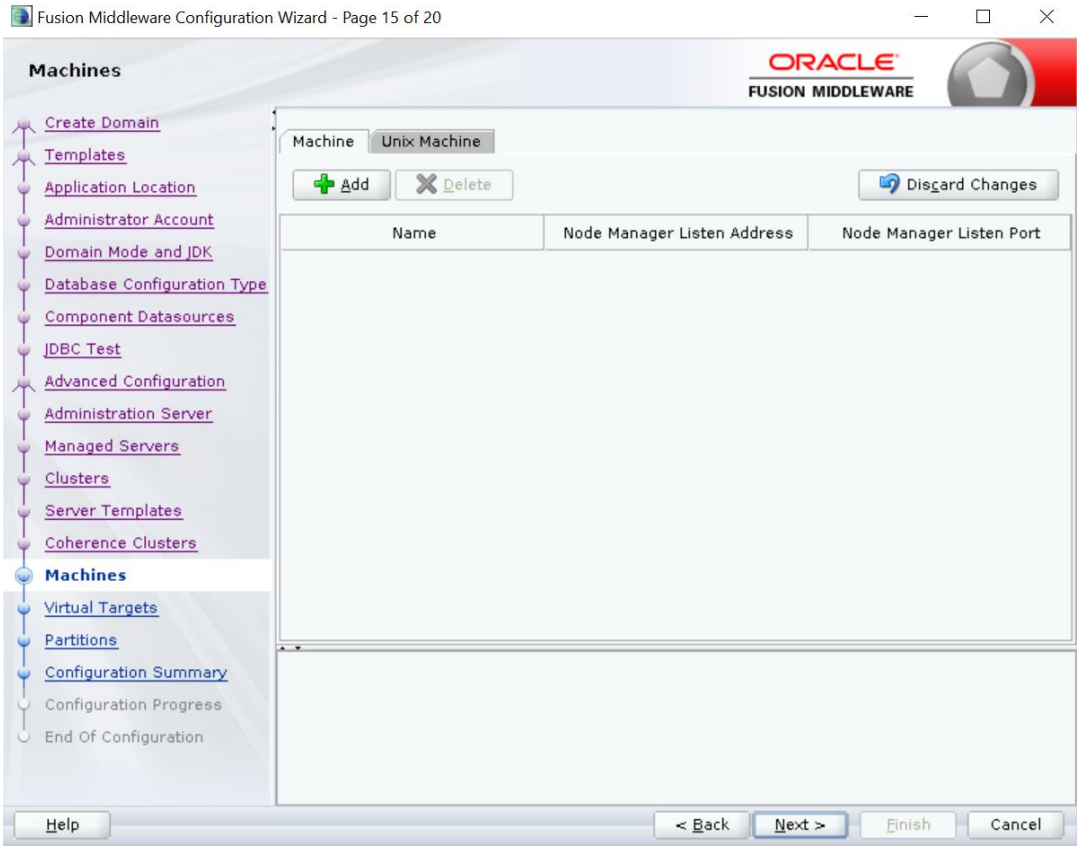
Figure 2-27 Weblogic Domain Creation 14



21. Configure as required and click **Next**.

    The following window is displayed.

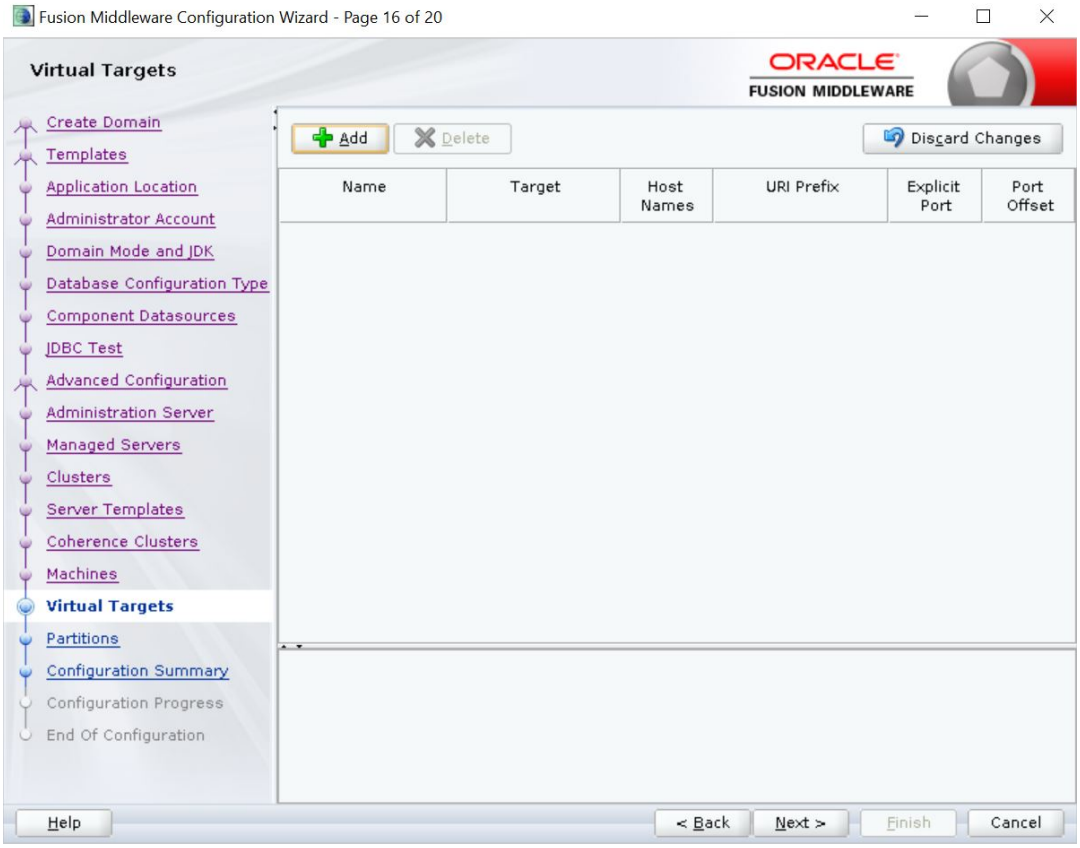
Figure 2-28 Weblogic Domain Creation 15



22. Click **Create**.

    The following window is displayed.

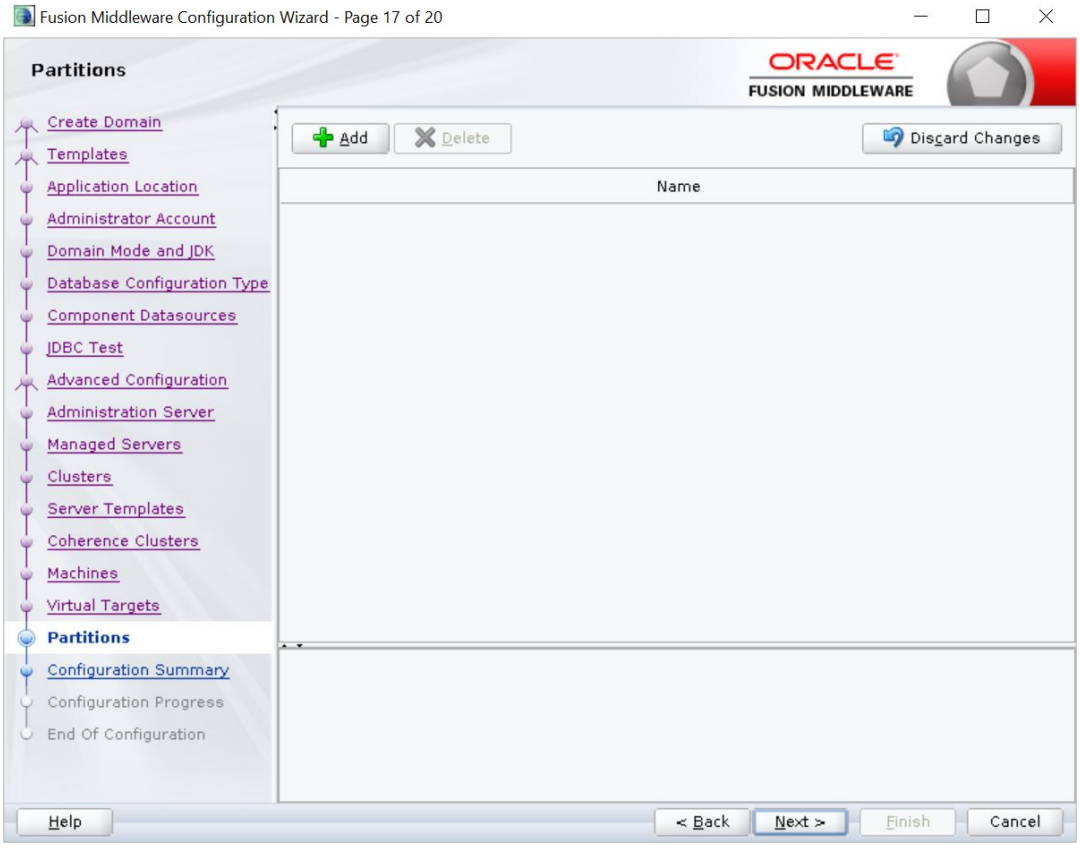
Figure 2-29 Weblogic Domain Creation 16



23. Click **Next**.

    The following window is displayed.

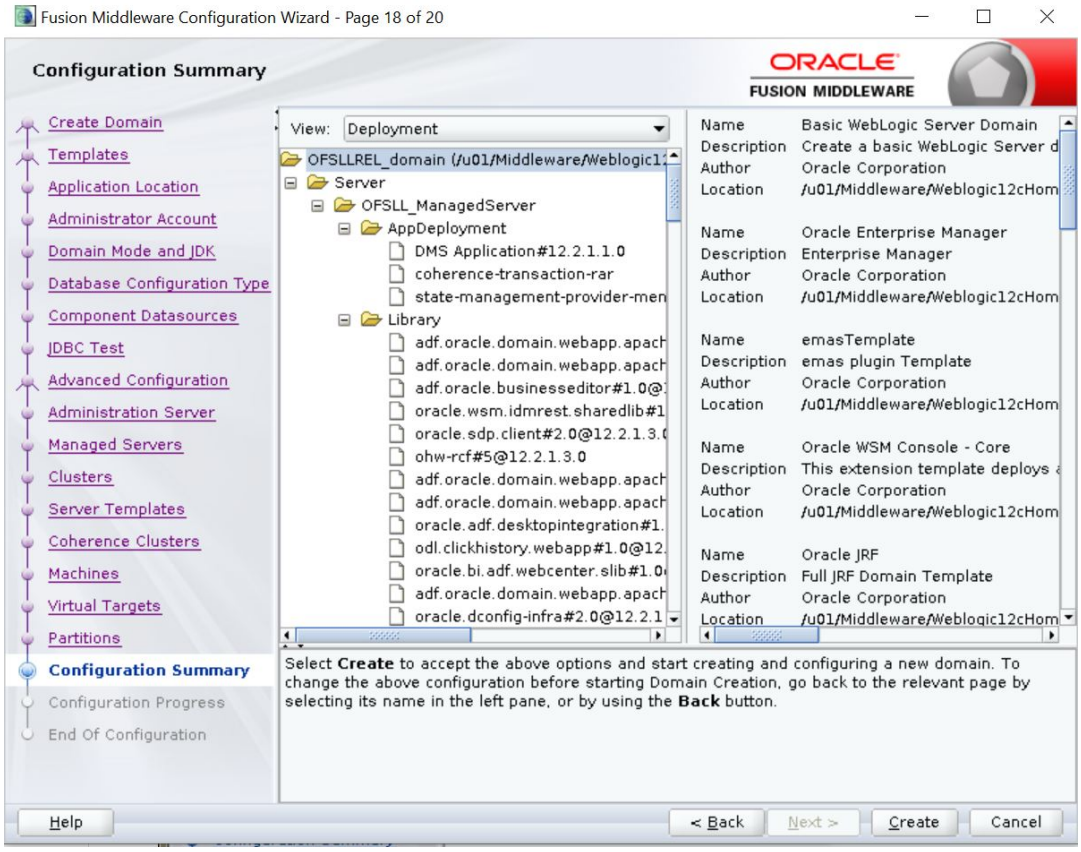
Figure 2-30 Weblogic Domain Creation 17



24. Click **Next**.

    The following window is displayed.

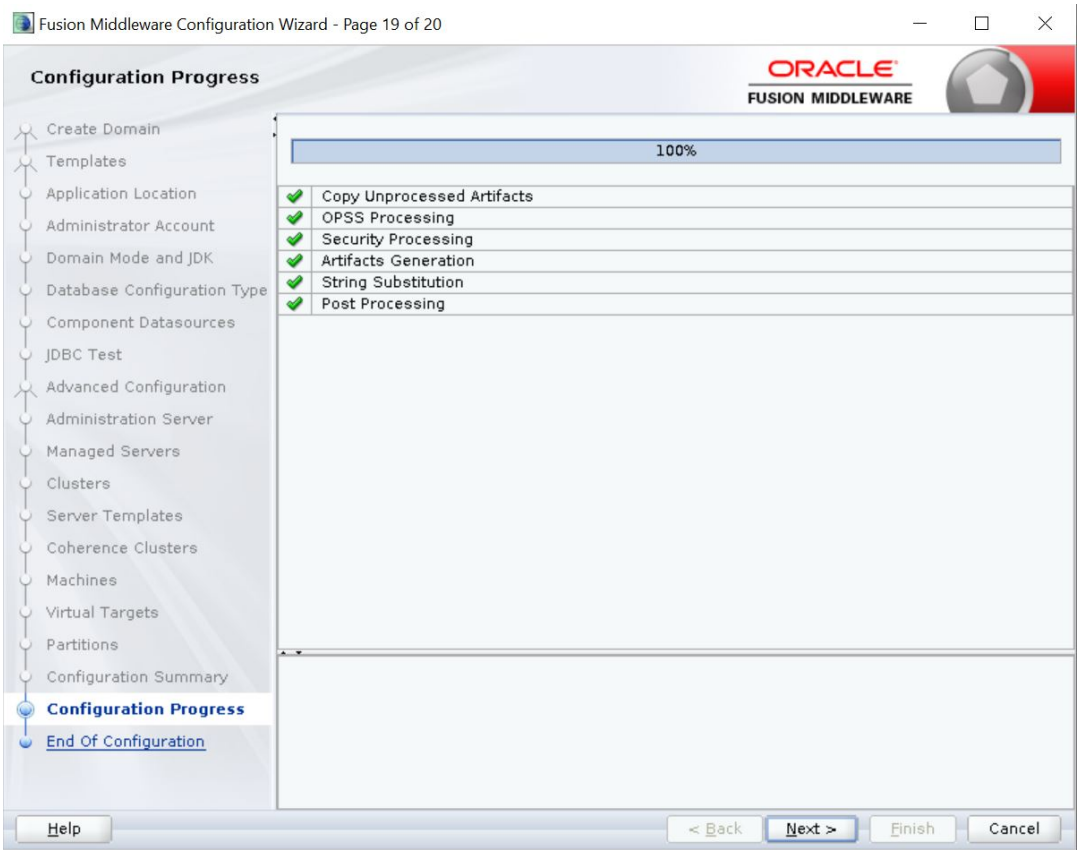
Figure 2-31 Weblogic Domain Creation 18



25. Click **Next**.

    The following window is displayed.

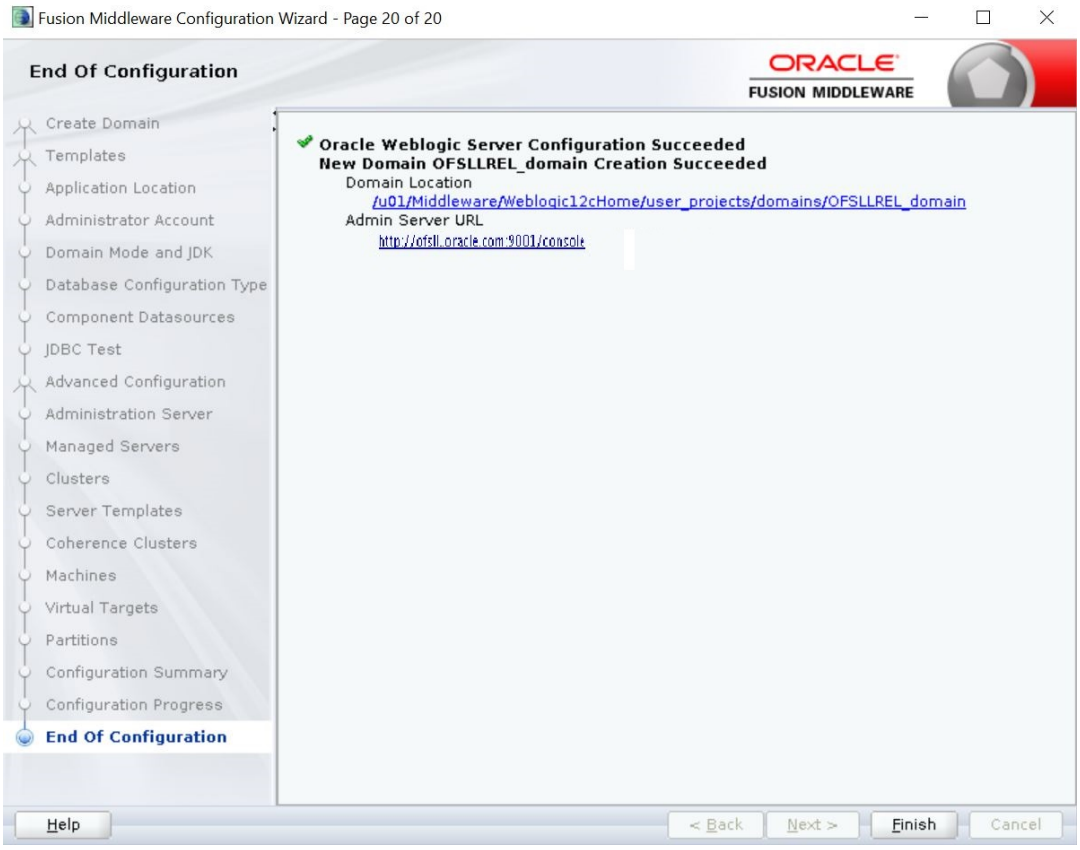
Figure 2-32 Weblogic Domain Creation 19



26. Click **Next**.

    The following window is displayed.

Figure 2-33 Weblogic Domain Creation 20



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

> **Note:**
>
> The default Weblogic installation will be running JVM with 512MB, this has to be increased for the ADF managed server. Say, for a 2 CPU Quad Core with 16 GB it could have the JVM running at 8 GB as:
> USER_MEM_ARGS="-Xms8192m –Xmx8192m -XX:PermSize=2048m -XX:Max-PermSize=2048m"

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

    - $ cd $MW_HOME/user_projects/domains/<mydomain>/bin
    - $ ./startWebLogic.sh

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

    $ nohup ./startWebLogic.sh &

29. To Start Managed Server

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

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

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

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

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

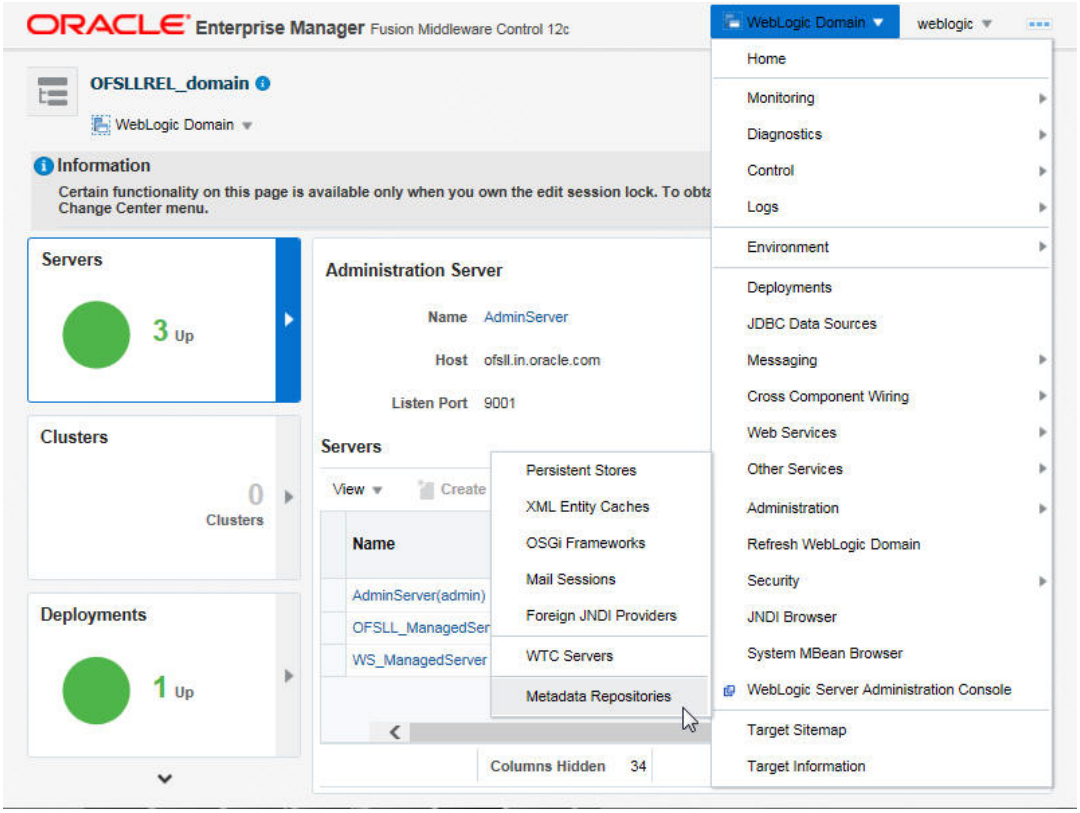
2.3 Creating Metadata Repository

The following section details the steps to create 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.

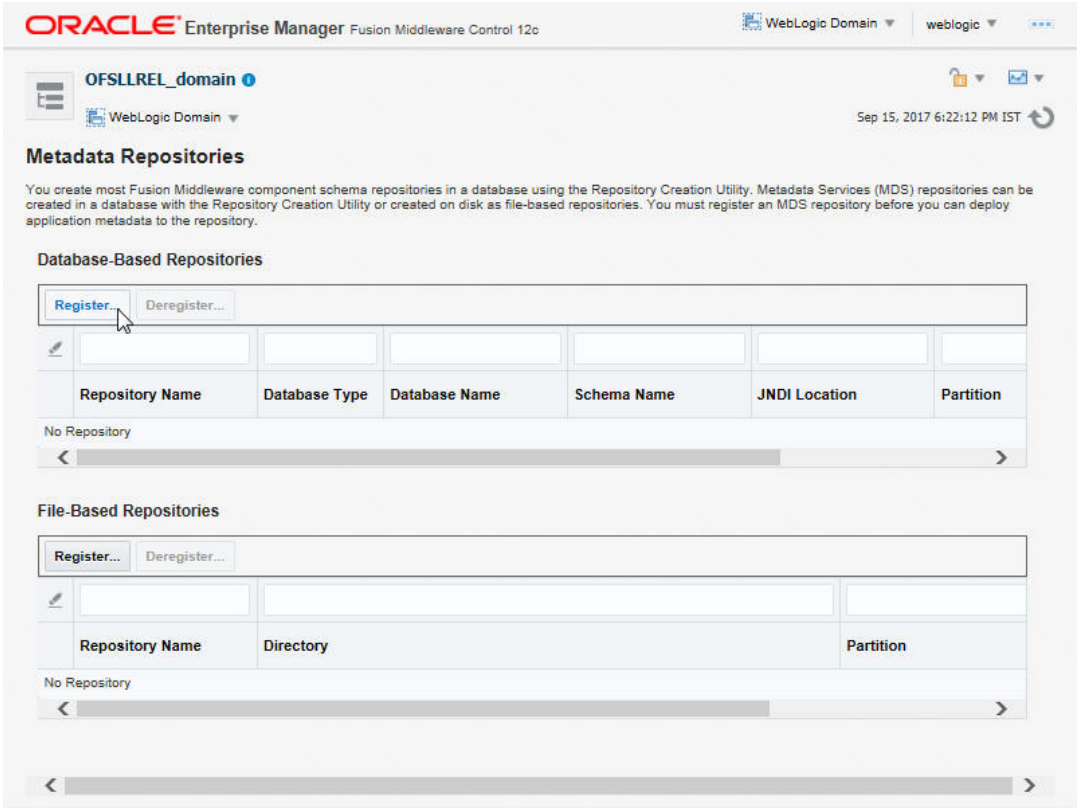
1. Login to Oracle Enterprise Manager 12c console (`http://hostname:port/em`).

Figure 2-34 Metadata Repository 1



2. Click on domain name OFSLLREL_domain on the left side panel.
3. Expand Weblogic domain OFSLLREL_domain and click **Metadata Repositories** option, as shown in the above screen.
4. The following window is displayed.

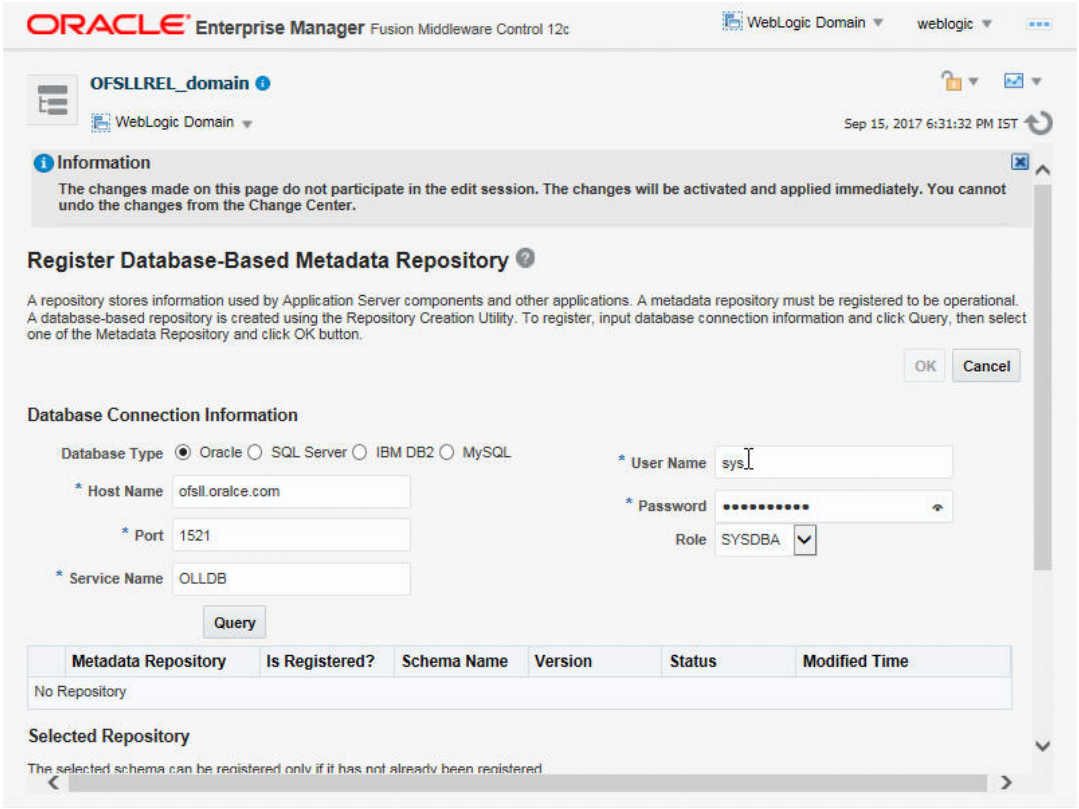
Figure 2-35 Metadata Repository 2



5. Click **Register** button.

   The following window is displayed.

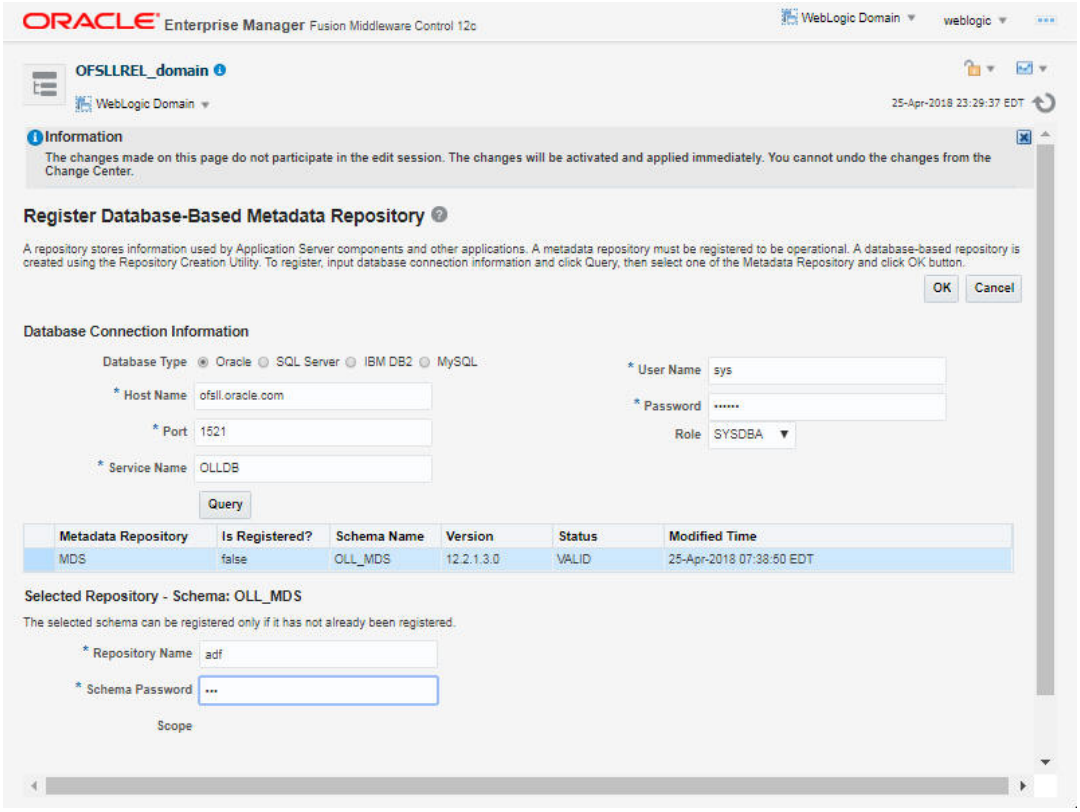
Figure 2-36 Metadata Repository 3



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**.

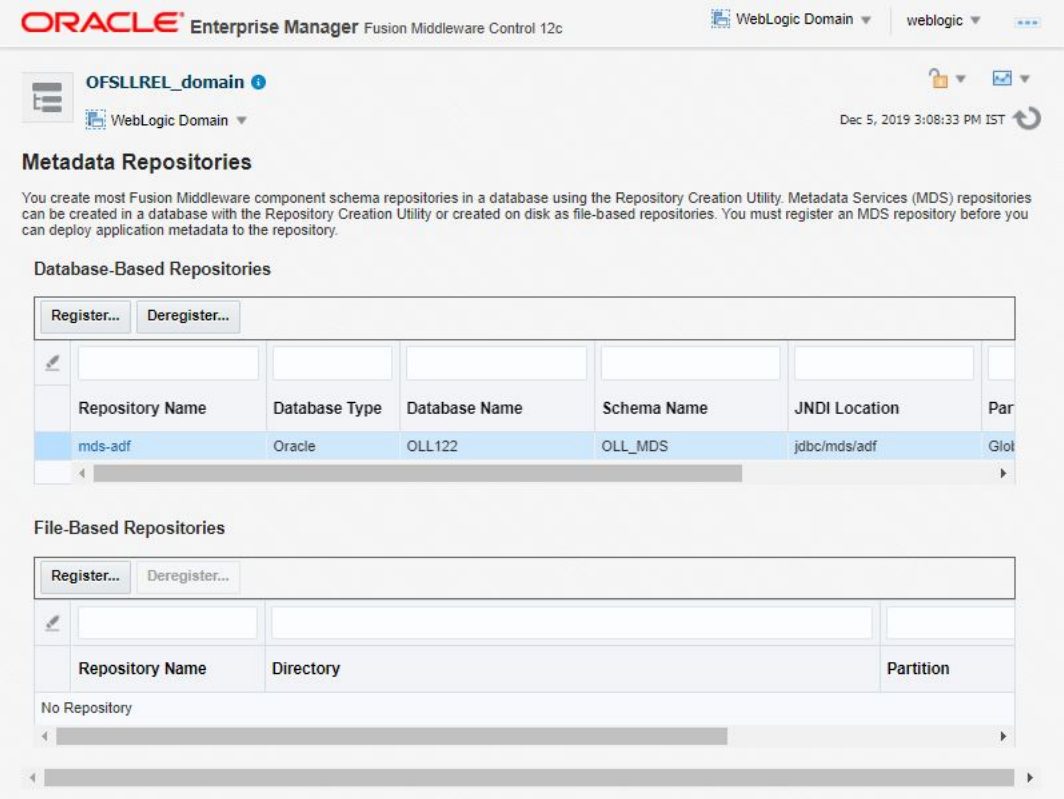
   The following window is displayed.

Figure 2-37 Metadata Repository 4



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

Figure 2-38 Metadata Repository 5



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

2.4 Creating Data Source

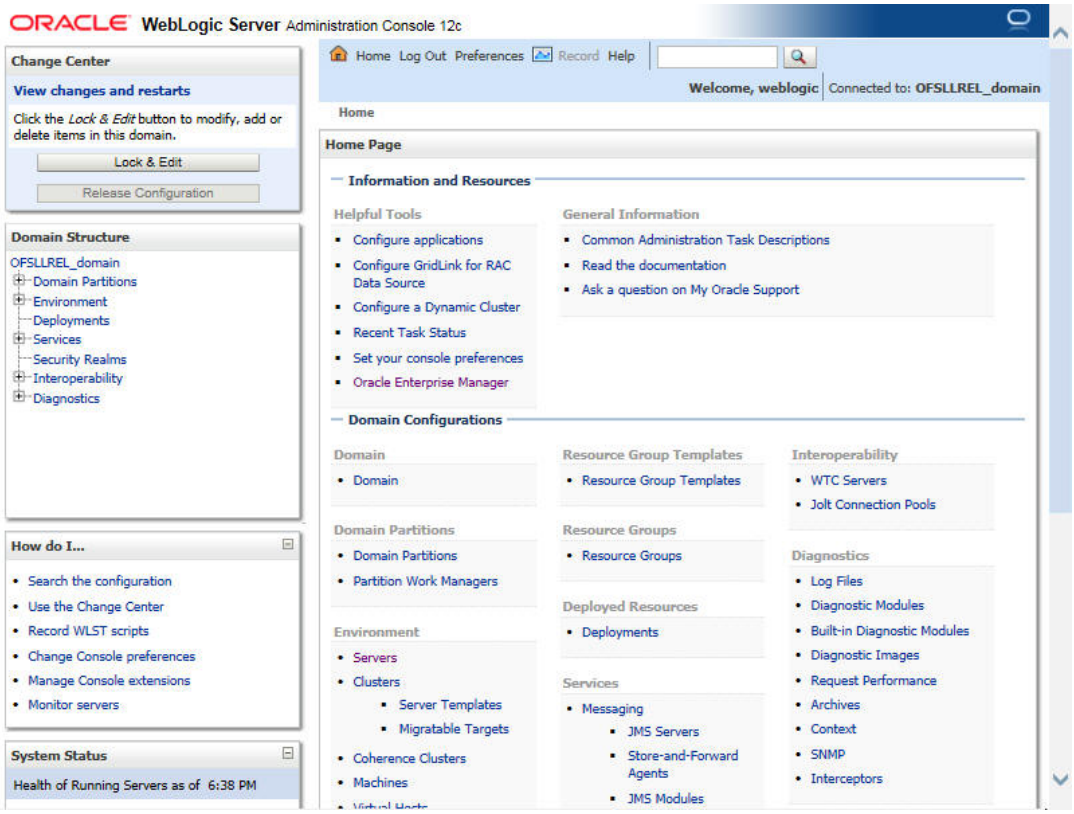
The following section details the steps to create data source.

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

Figure 2-39 Create Data Source 1

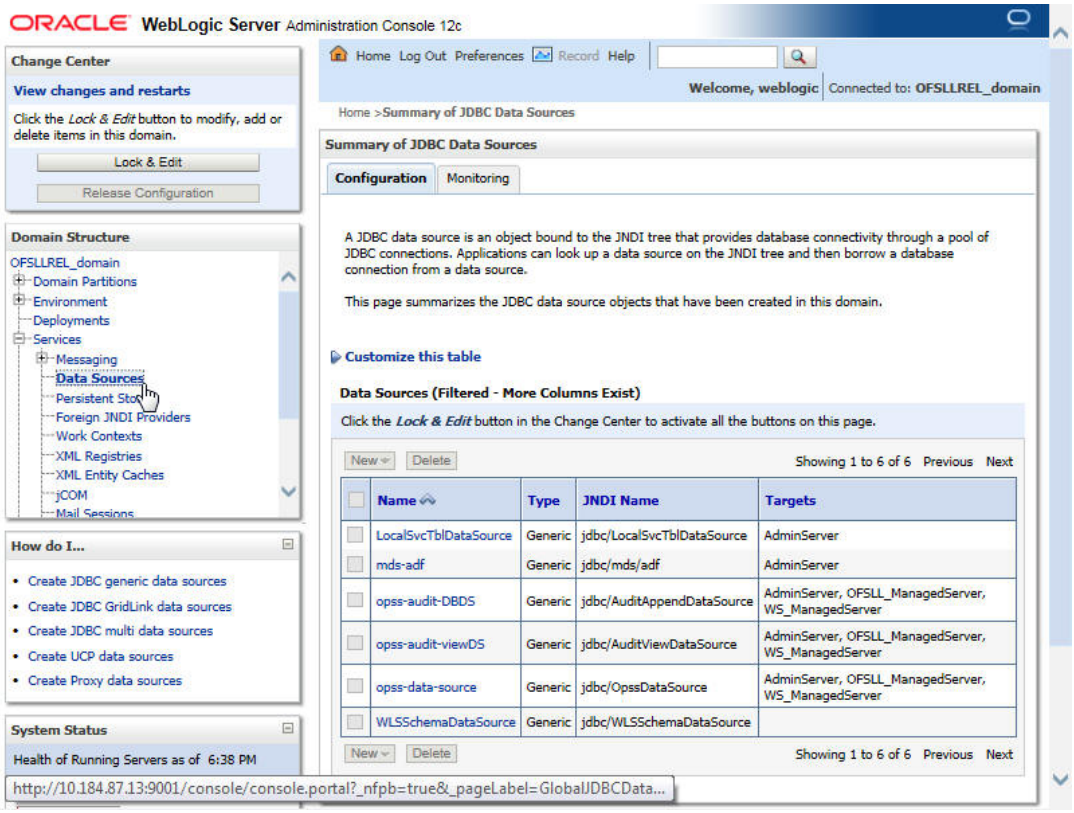
2. The following window is displayed.

Figure 2-40 Create Data Source 2



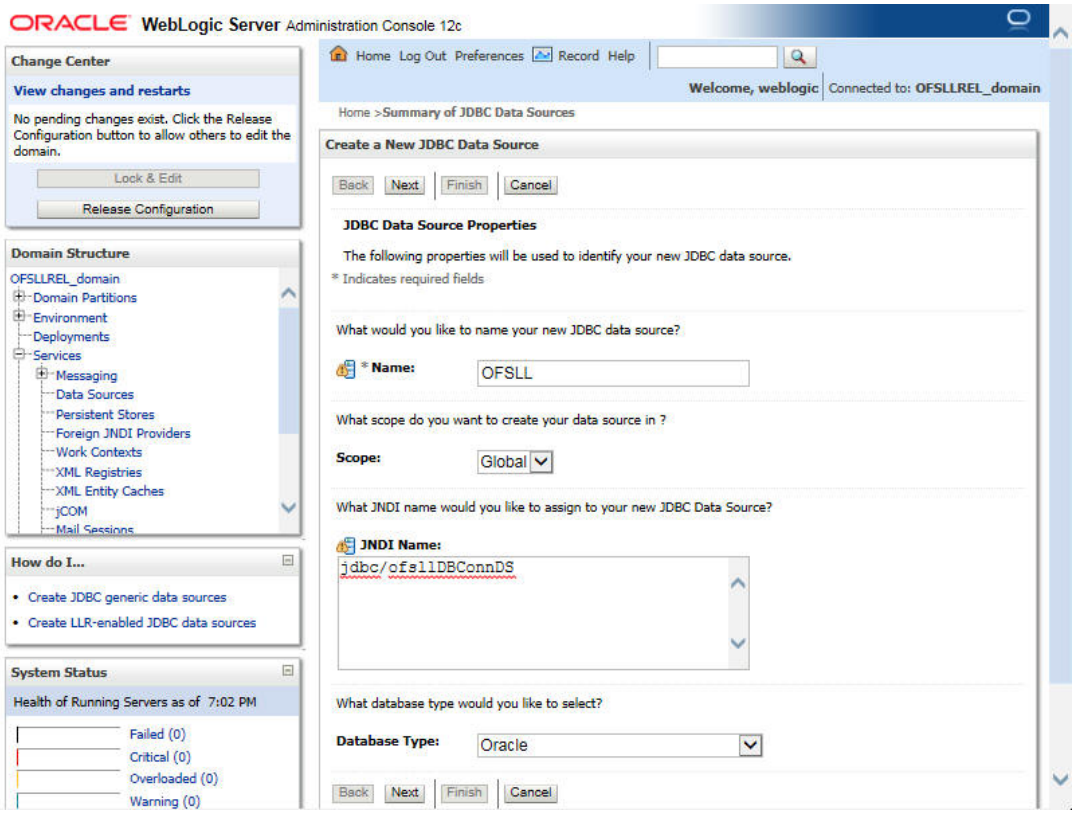
3. Click Domain Name > Services > Data Sources.
4. The following window is displayed.

Figure 2-41 Create Data Source 3



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

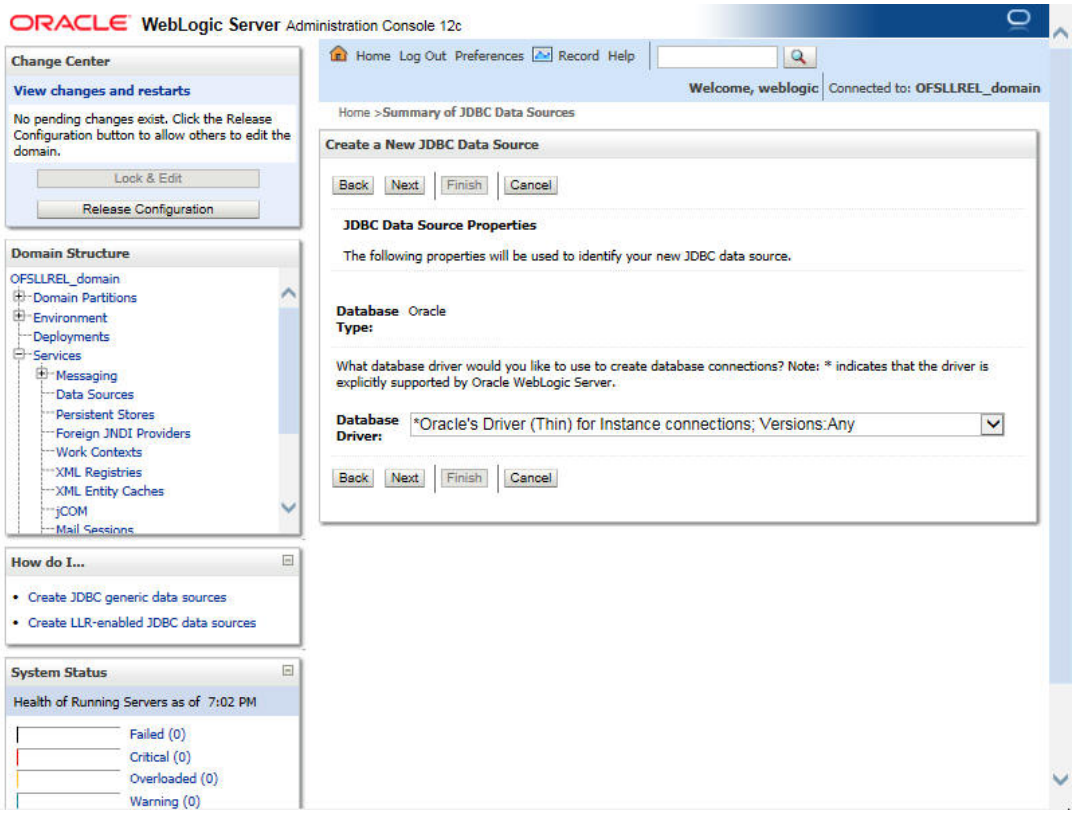
Figure 2-42 Create Data Source 4



6. Enter Data source **Name**, JNDI Name as **jdbc/ofsllDBConnDS** and select **Oracle** as Database Type.
7. Click **Next**.

   The following window is displayed.

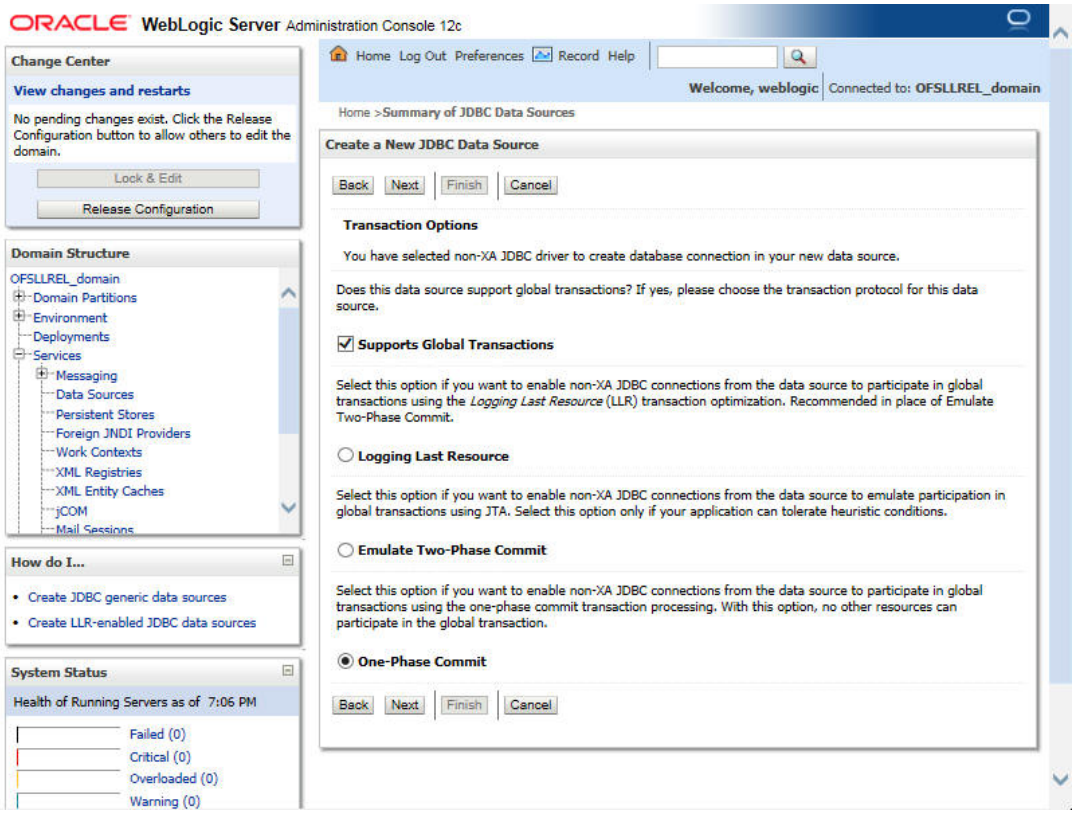
Figure 2-43 Create Data Source 5



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.

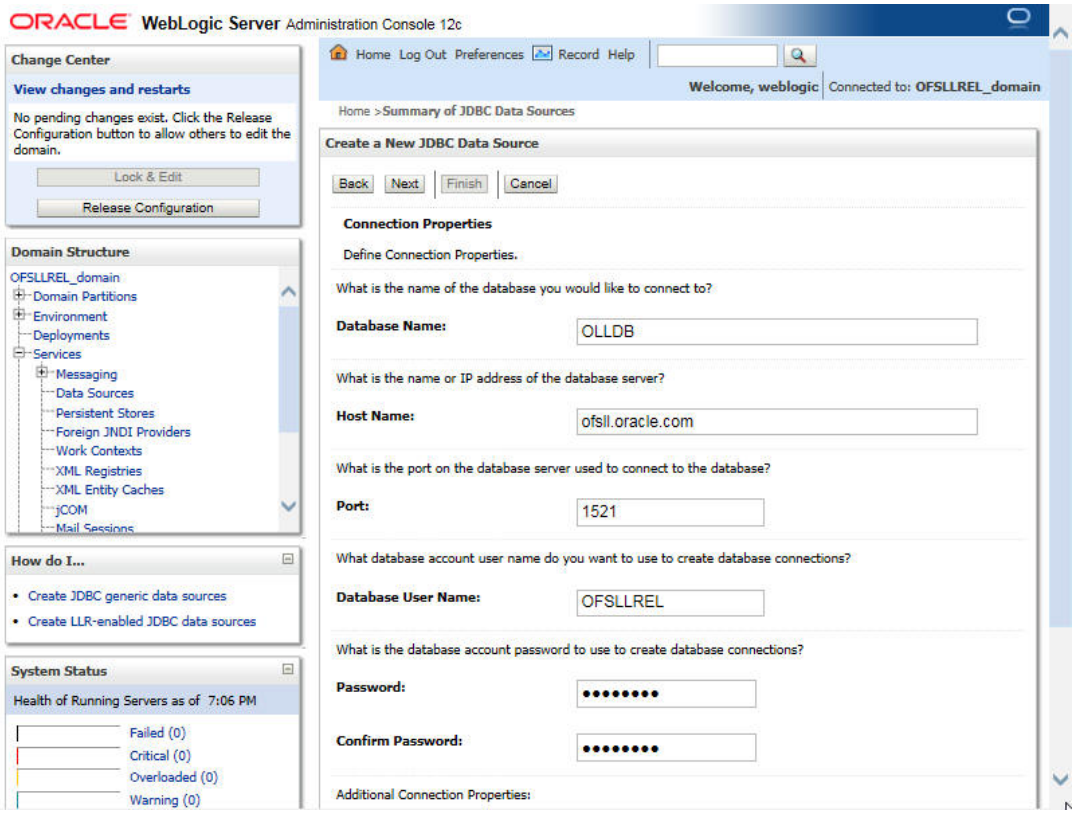
Figure 2-44 Create Data Source 6



10. Click **Next**.

    The following window is displayed.

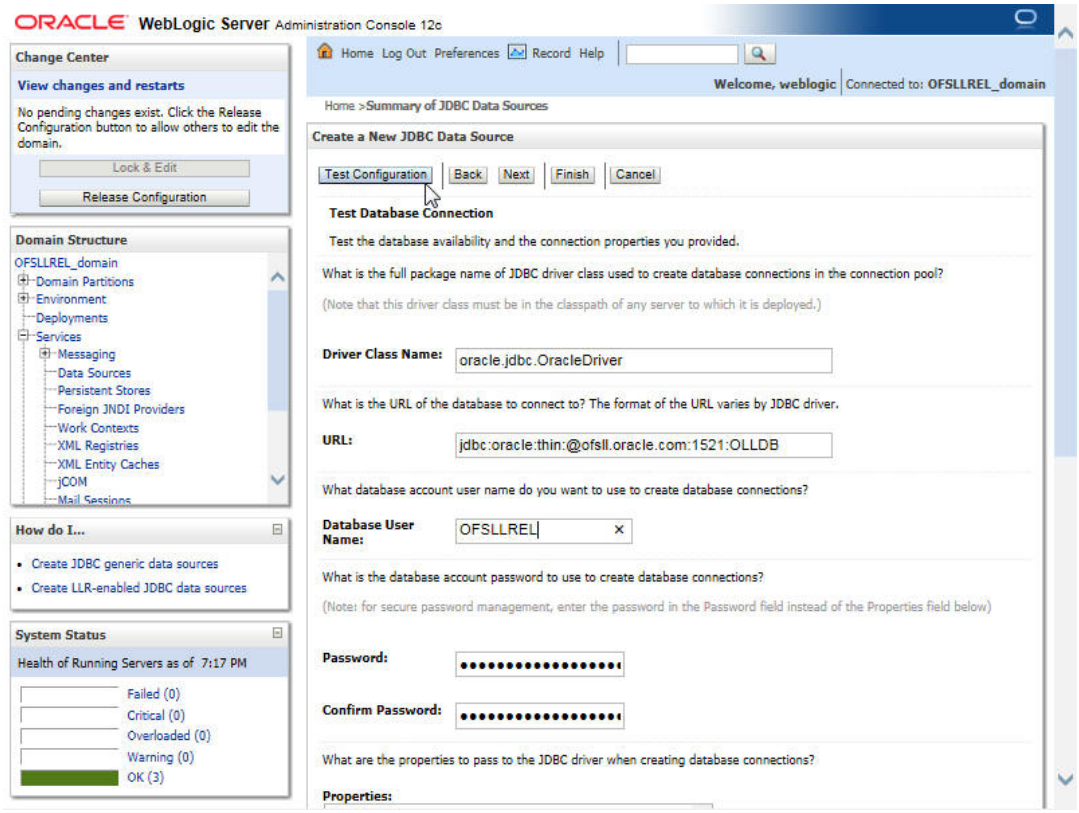
Figure 2-45 Create Data Source 7



11. Enter Database details click **Next**.

    The following window is displayed.

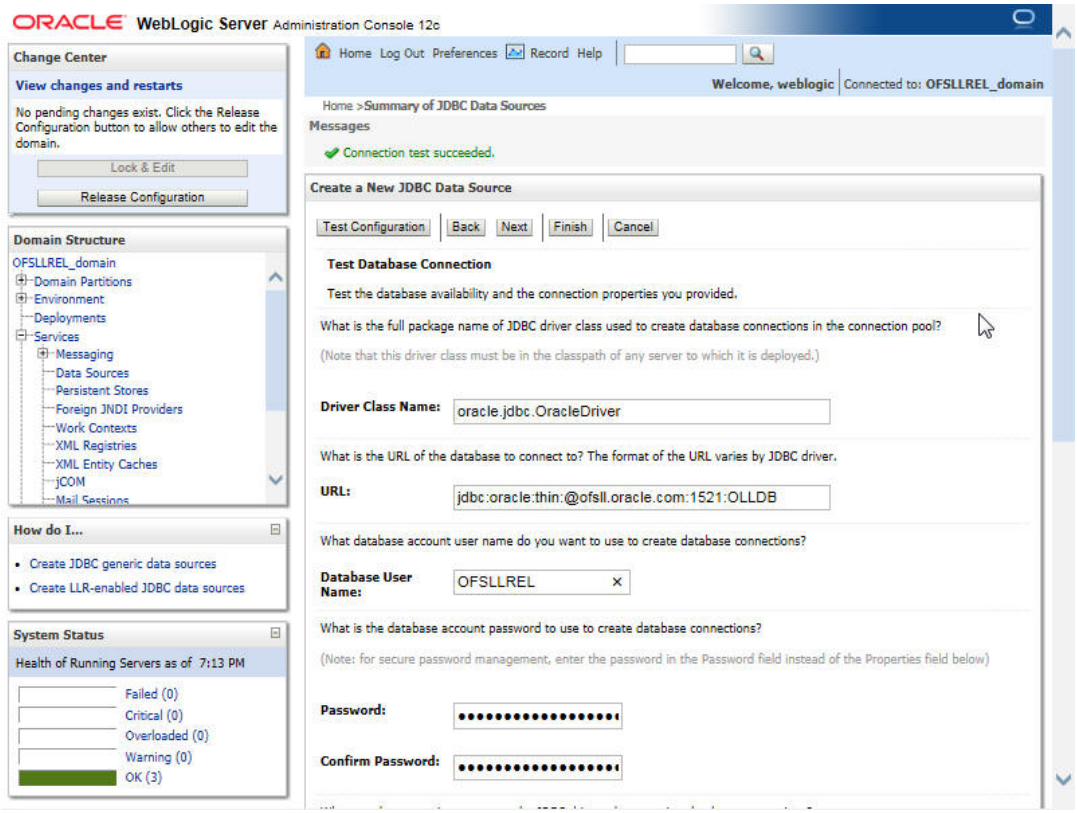
Figure 2-46 Create Data Source 8



12. Click **Test Configuration**.

    The following window is displayed.

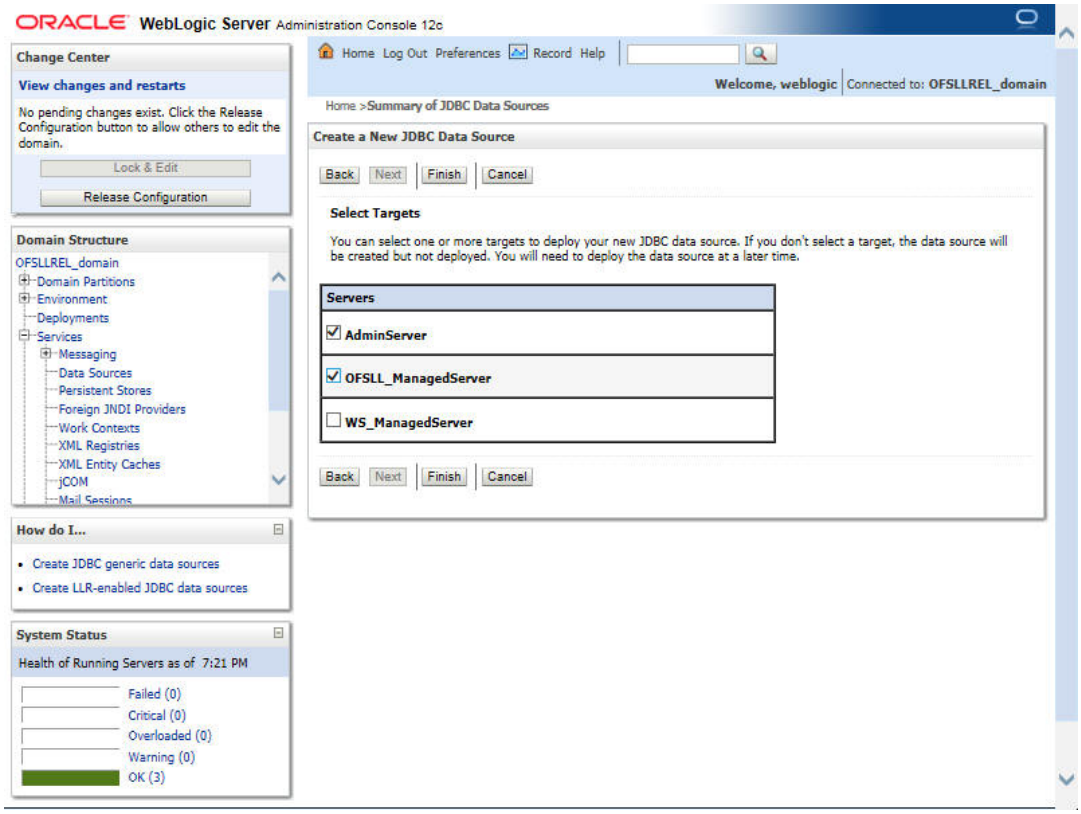
Figure 2-47 Create Data Source 9



13. Displays confirmation message as **Connection test succeeded**. Click **Next**.

    The following window is displayed.

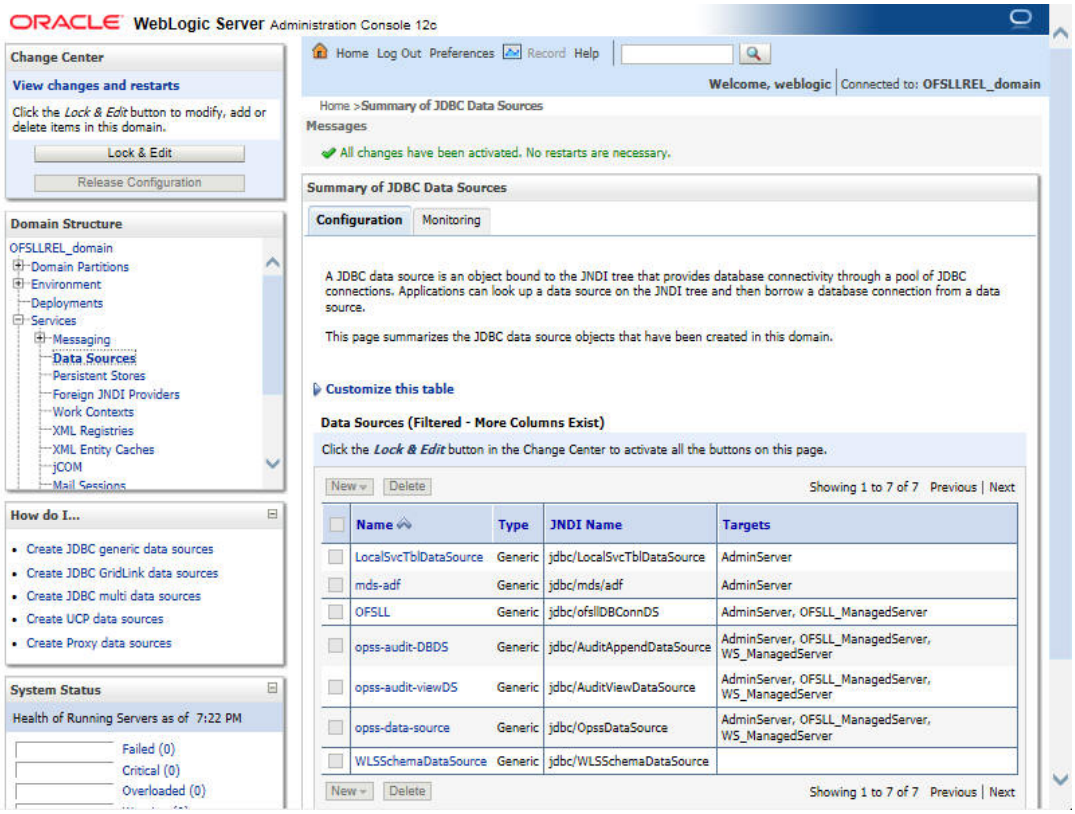
Figure 2-48 Create Data Source 10



14. Select target Servers **AdminServer** and **OFSLL_ManagedServer** and click **Finish**.

    The following window is displayed.

Figure 2-49 Create Data Source 11



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

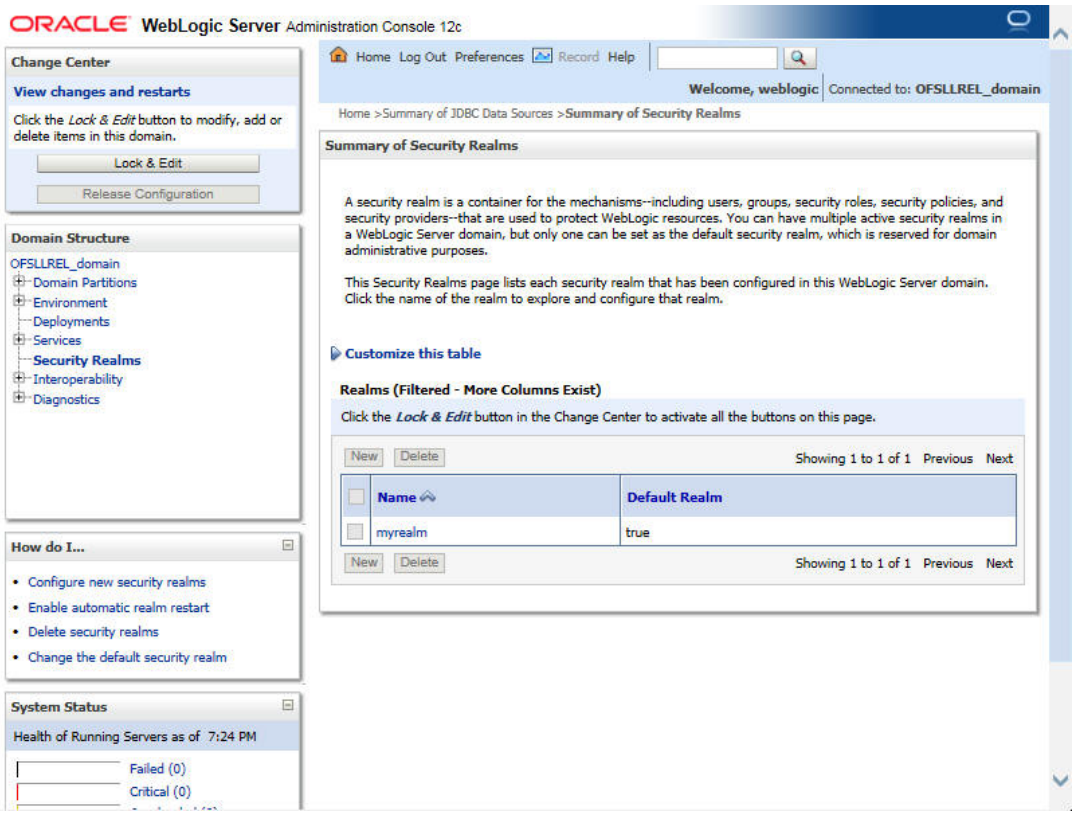
2.5 Creating SQL Authentication Provider

The following section details the steps to create SQL authentication provider.

1. Login to WebLogic server administration console and click **Security Realms** in left panel.

   The following window is displayed.

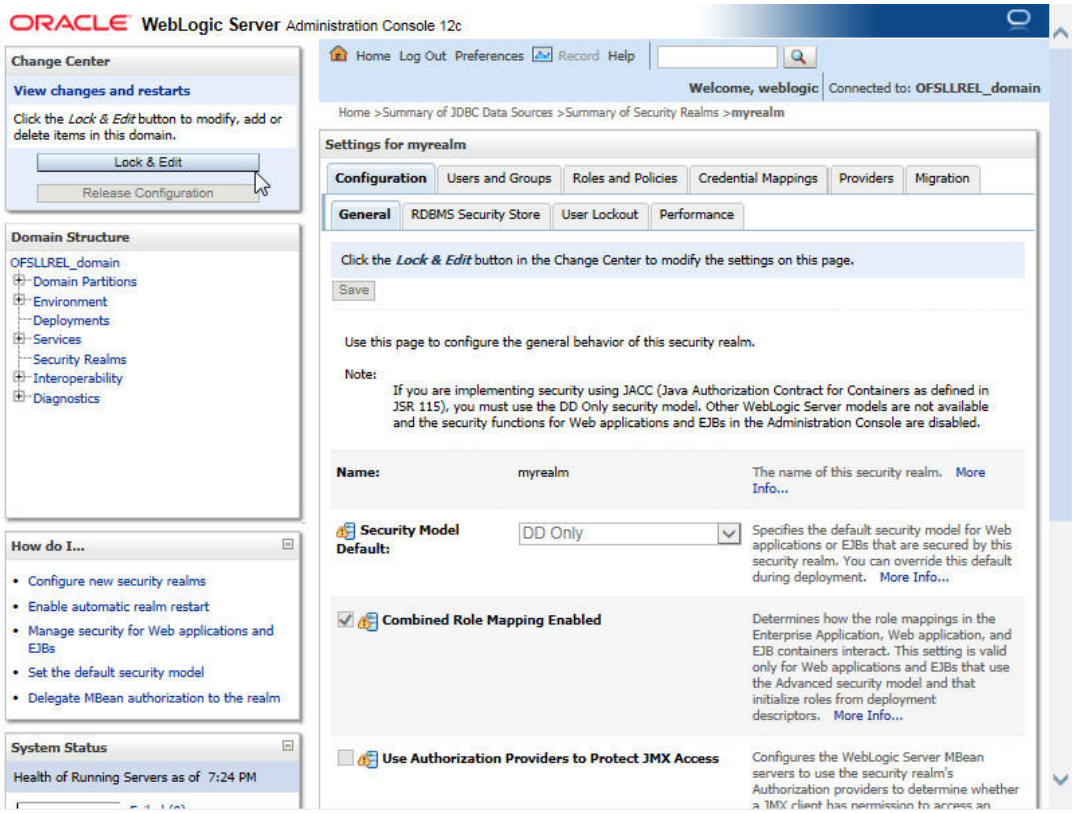
Figure 2-50 SQL Authentication 1



2. Click **myrealm** on right panel.

   The following window is displayed.

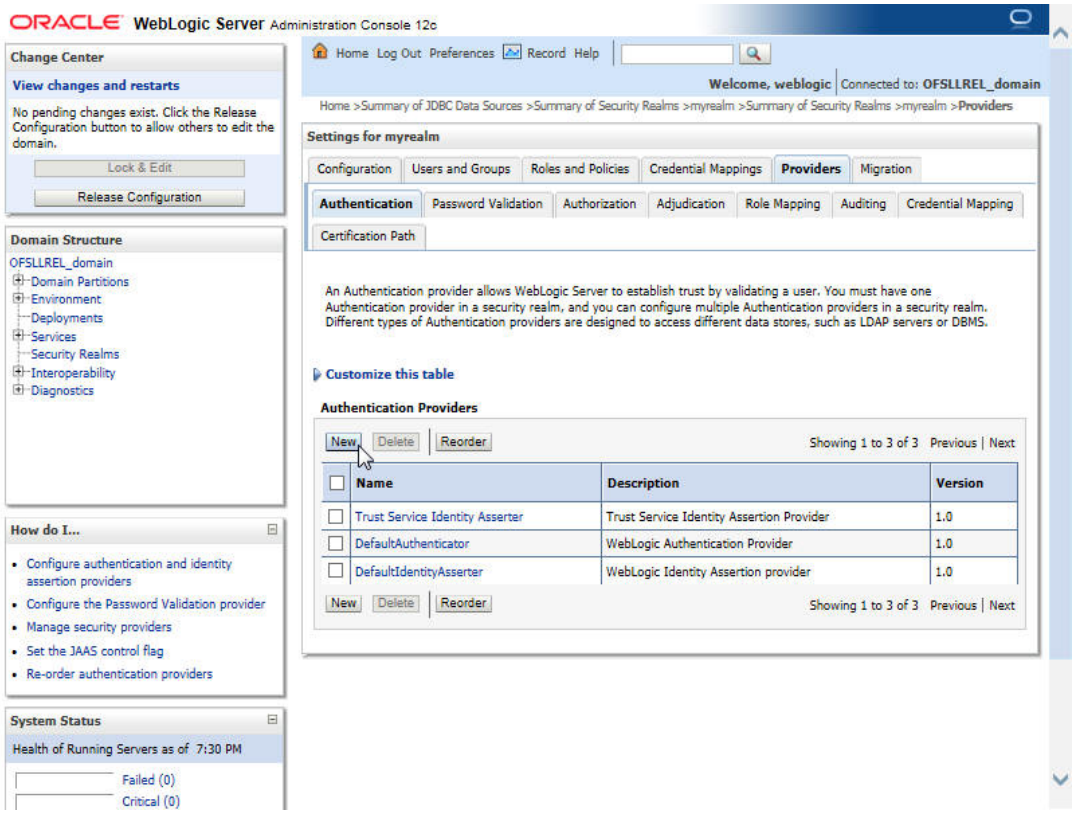
Figure 2-51 SQL Authentication 2



3. Click on **Providers tab**.

   The following window is displayed.

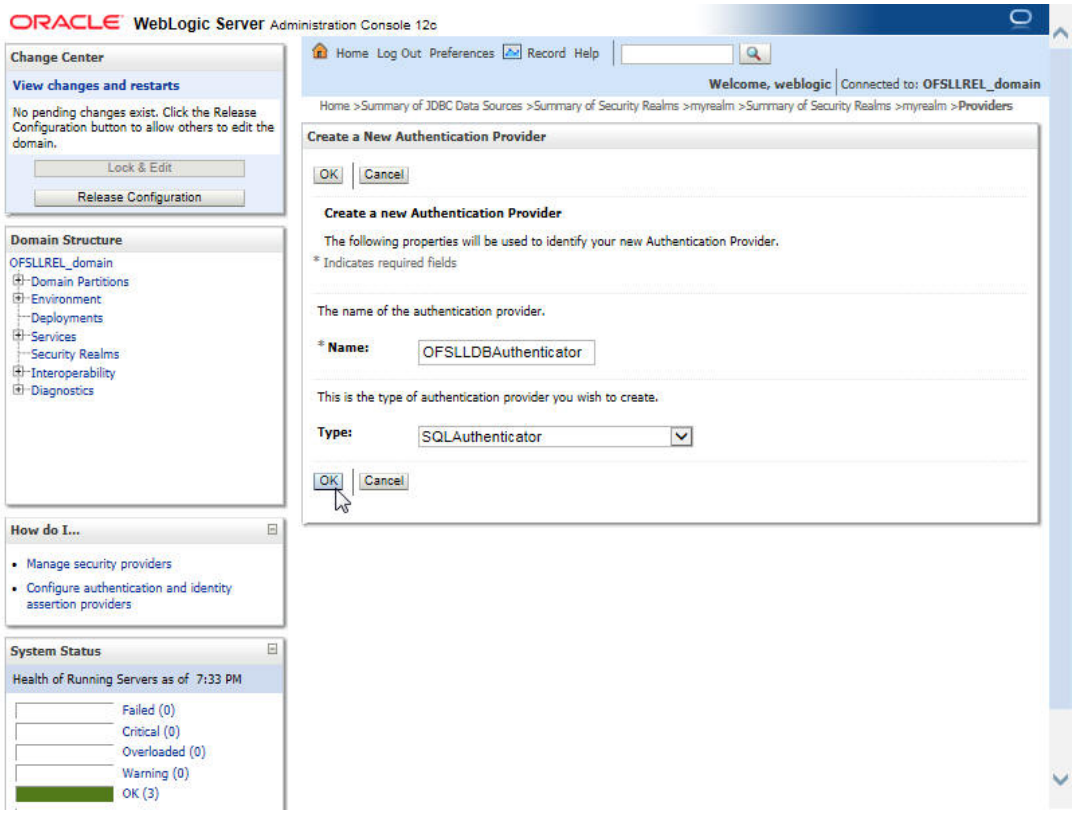
Figure 2-52 SQL Authentication 3



4. Click **Lock & Edit** to unlock the screen and click **New** button in Authentication Providers sub tab.

   The following window is displayed.

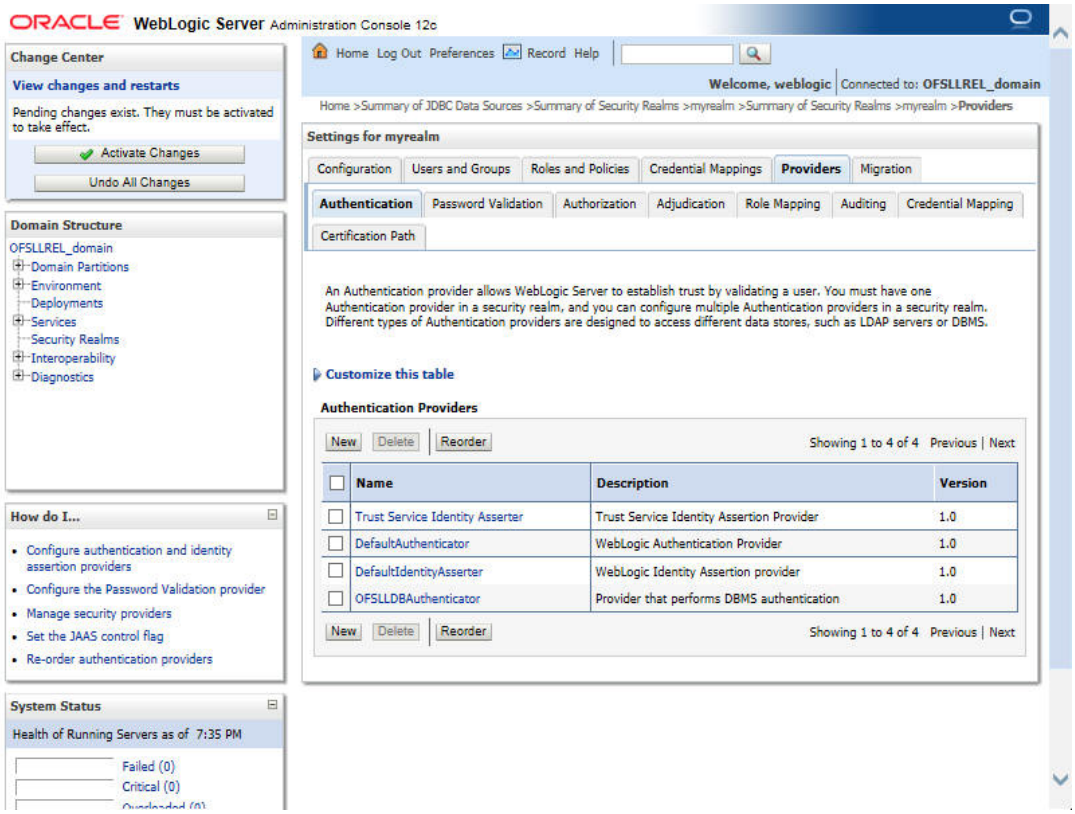
Figure 2-53 SQL Authentication 4



5. Create Authentication provider with following values:
   - Name: OFSLLDBAuthenticator
   - Type: SQLAuthenticator
6. Click **OK**.

   The following window is displayed.

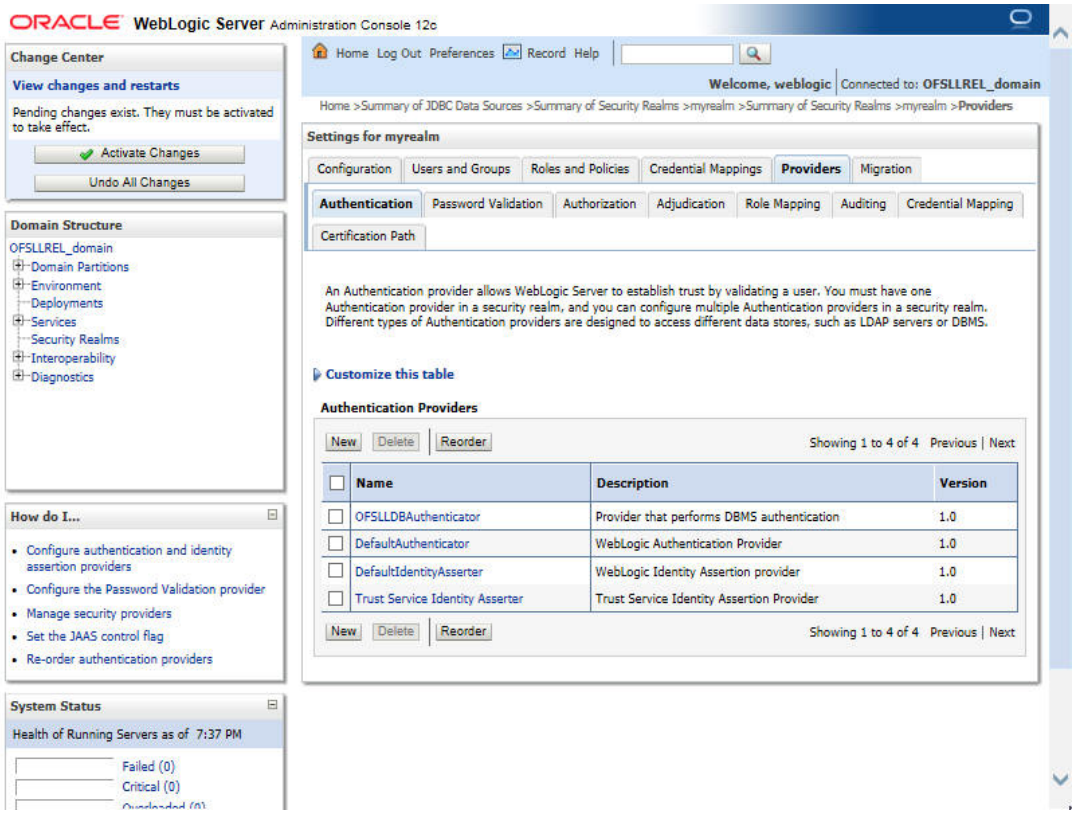
Figure 2-54 SQL Authentication 5



7. Click on **Activate Changes**.

   The following window is displayed.

Figure 2-55 SQL Authentication 6

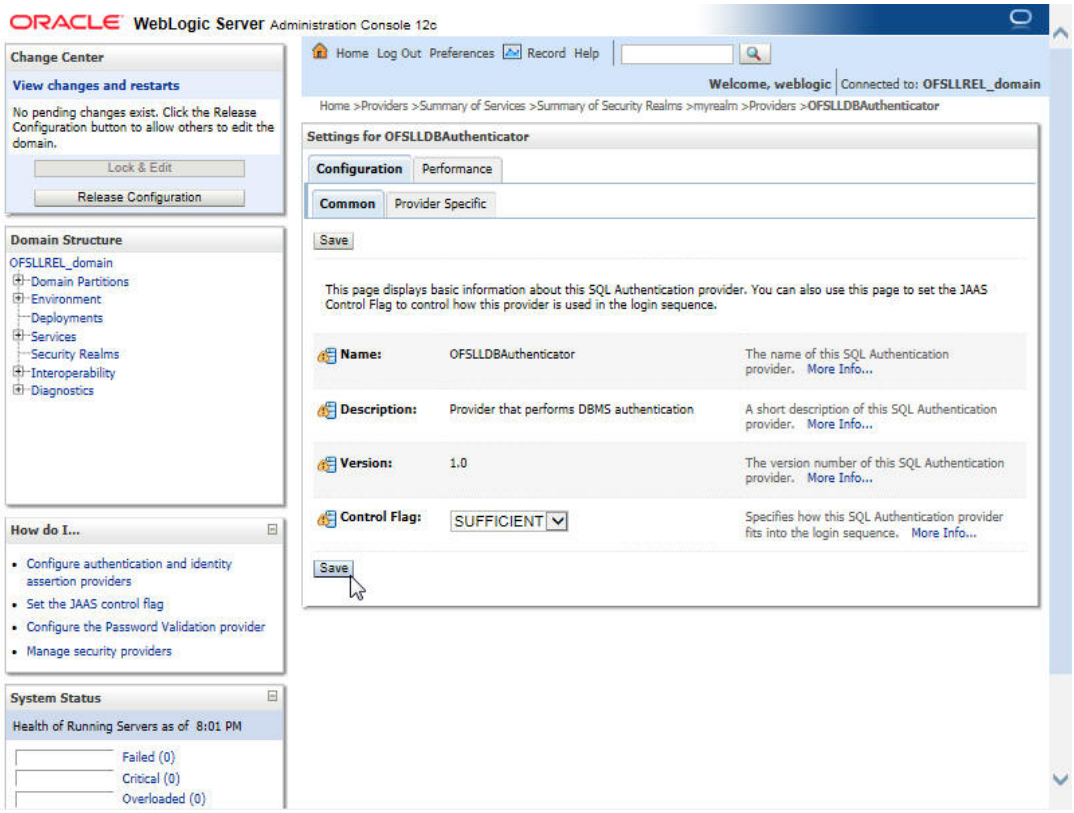


Authentication order should be maintained as mentioned in the above screen. ‘OFSLLDBAuthenticator’ will be displayed as above.

8. Click on **OFSLLDBAuthenticator**.

   The following window is displayed.

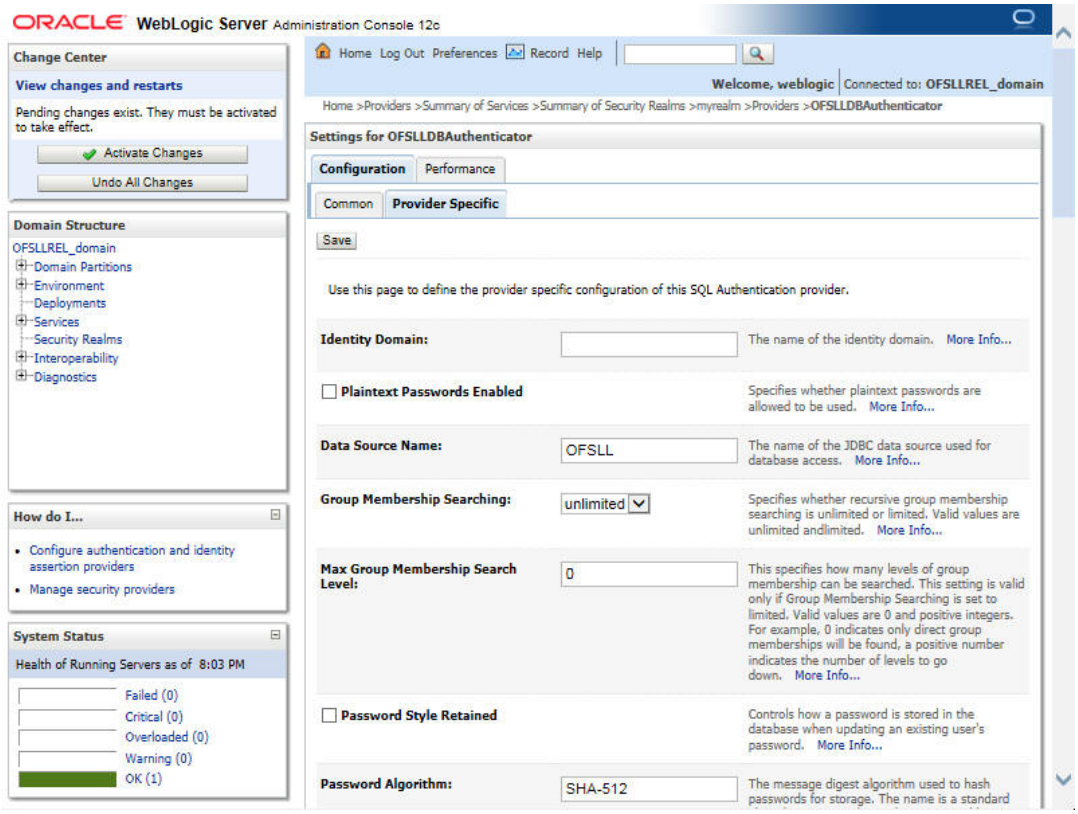
Figure 2-56 SQL Authentication 7



9. Select **SUFFICIENT** as the Control Flag and click **Save**.
10. Click **Provider Specific** sub tab under Configuration tab.

    The following window is displayed.

Figure 2-57 SQL Authentication 8



11. Specify the following values in corresponding fields:
    - Data Source Name: OFSLL
    - Password Style Retained: Uncheck
    - Password Algorithm: SHA-512
    - Password Style: SALTEDHASHED
    - Provide the SQL Queries from the column Corresponding SQL Queries as per OFSLL Tables as given below.

Table 2-1 SQL Queries

Operation	Default SQL Query from Weblogic	Corresponding SQL Queries as per our Tables
SQL Get Users Password:	SELECT U_PASSWORD FROM USERS WHERE U_NAME = ?	SELECT UAU_USR_PASSWORD FROM USER_AUTHORISATIONS WHERE UAU_USR_CODE = ?
SQL Set User Password:	UPDATE USERS SET U_PASSWORD = ? WHERE U_NAME = ?	UPDATE USER_AUTHORISATIONS SET UAU_USR_PASSWORD = ? WHERE UAU_USR_CODE = ?
SQL User Exists:	SELECT U_NAME FROM USERS WHERE U_NAME = ?	SELECT UAU_USR_CODE FROM USER_AUTHORISATIONS WHERE UAU_USR_CODE = ?

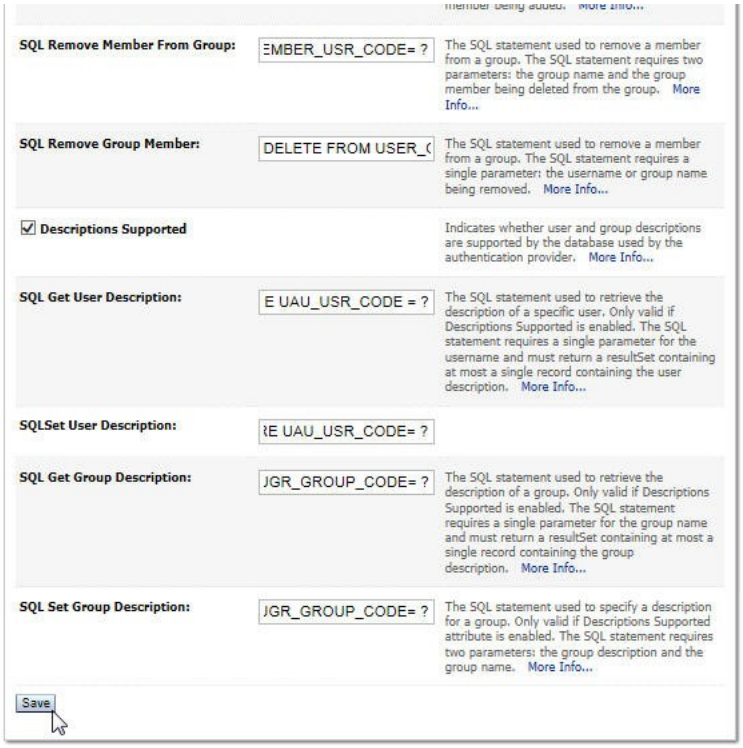
Table 2-1 (Cont.) SQL Queries

Operation	Default SQL Query from Weblogic	Corresponding SQL Queries as per our Tables
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= ?
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 ?

Table 2-1 (Cont.) SQL Queries

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

Figure 2-58 SQL Authentication 9



12. Click **Save**.

> **Note:**
>
> Application server needs to be restarted for these changes to take effect.

2.6 Creating User Groups and Users

The following section details the steps to create user groups and users.

- Creating Users
- Creating User Groups
- Assigning Users to Groups
- Resetting password via weblogic console

2.6.1 Creating Users

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

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

> **Note:**
>
> By default there are no users created to login to OFSLL application.

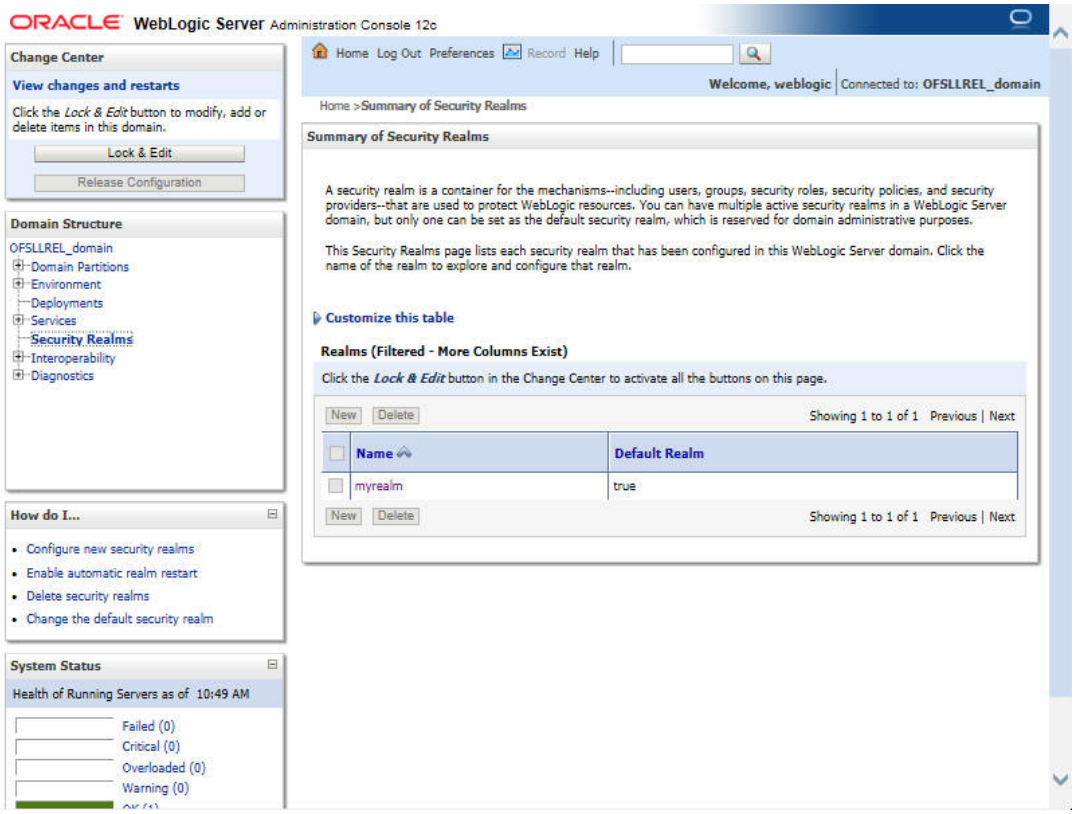
Login as application schema owner and run the script crt_app_user.sql script to create OFSLL application user.

Figure 2-59 User group Script

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

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

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

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

1 row created.


1 row created.


1 row created.

SQL> commit;

Commit complete.

SQL>
```

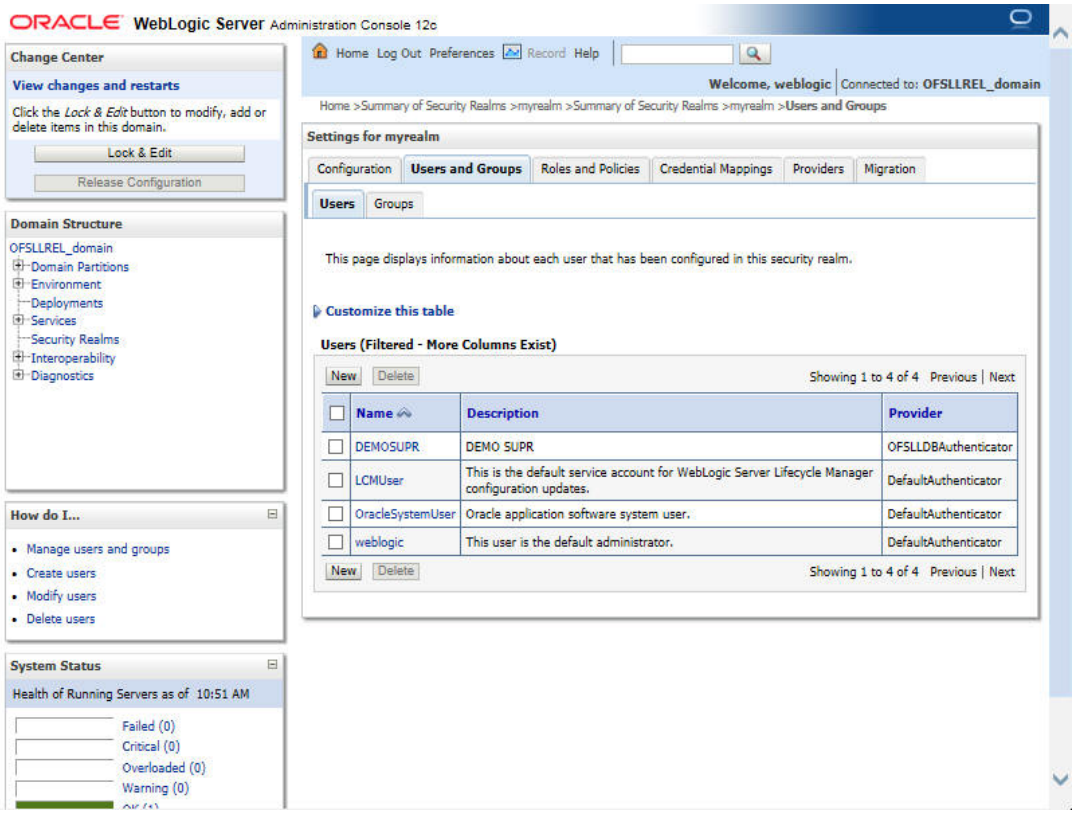
1. Login into WebLogic server console.
2. Click **Security Realms** on the left panel.
3. Click **myrealm** on the right panel.

Figure 2-60 User group 1



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

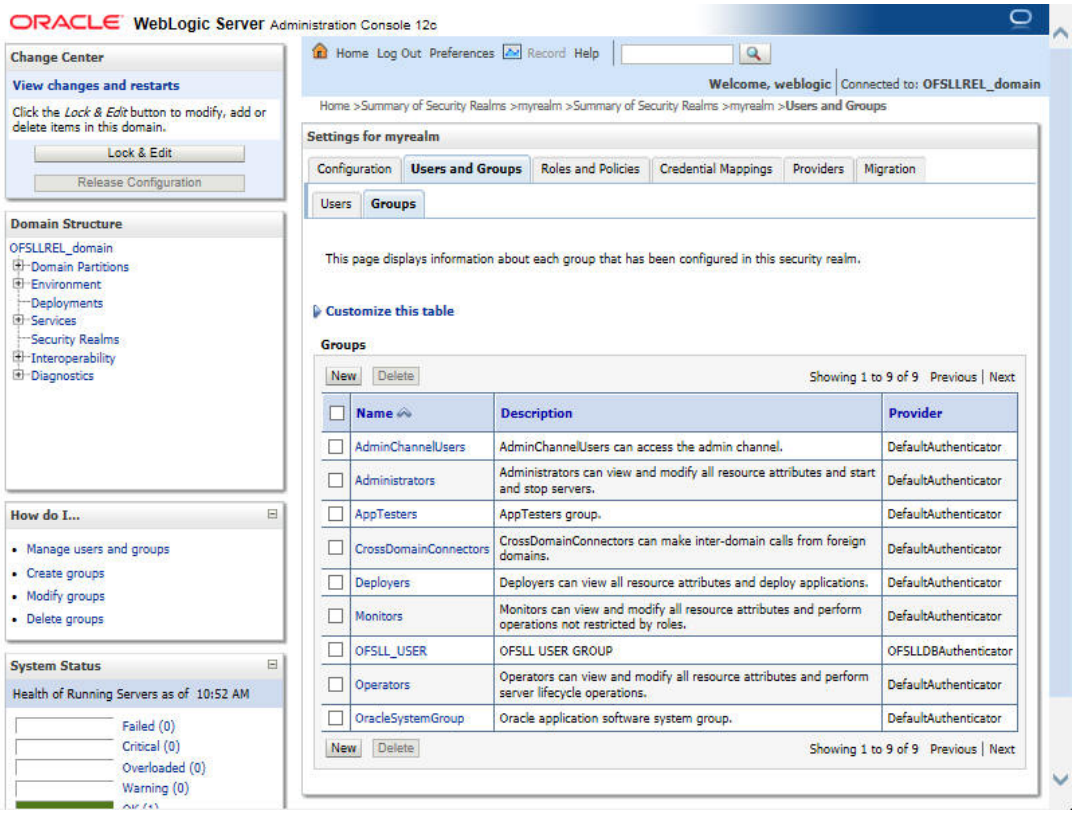
Figure 2-61 User group 2



2.6.2 Creating User Groups

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

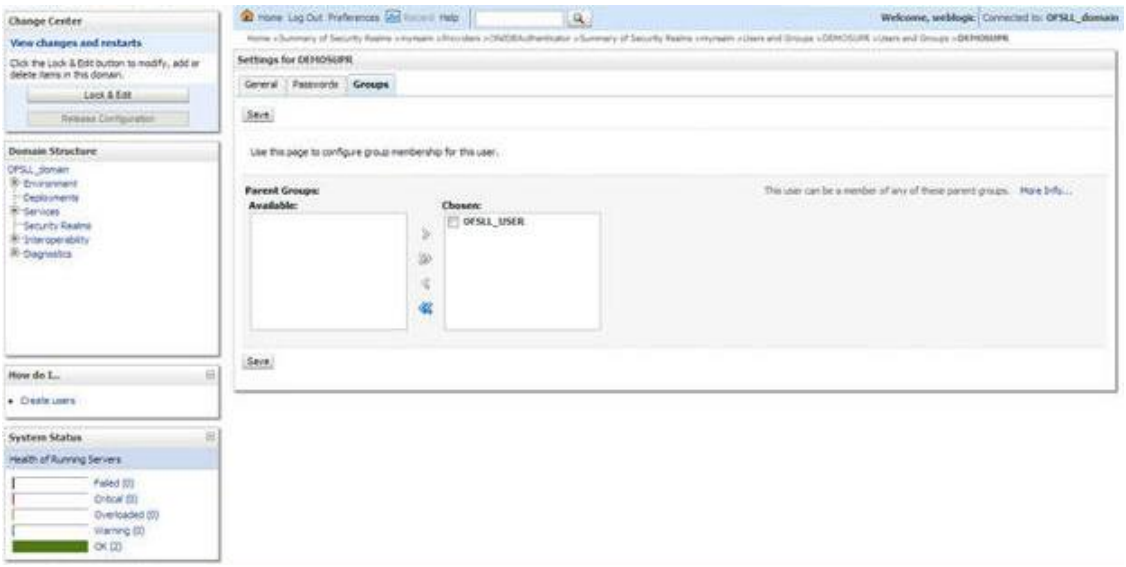
Figure 2-62 User group 3



2.6.3 Assigning Users to Groups

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

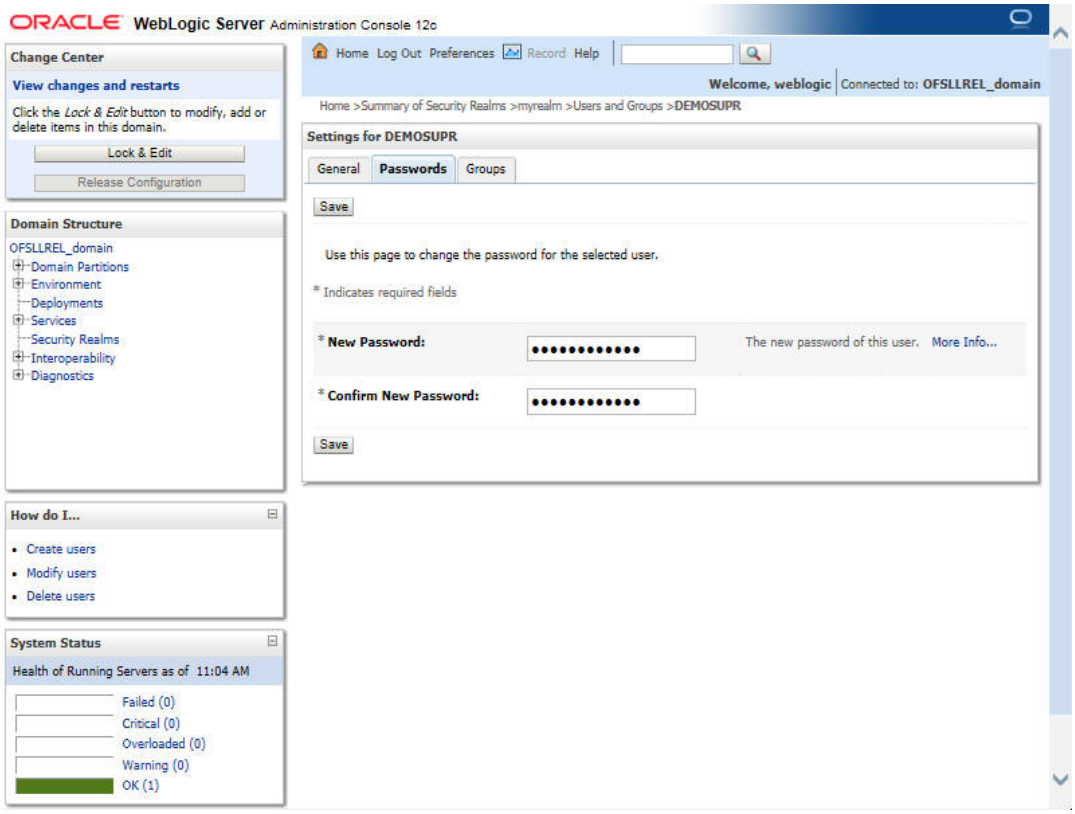
Figure 2-63 User group 4



2.6.4 Resetting password via weblogic console

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

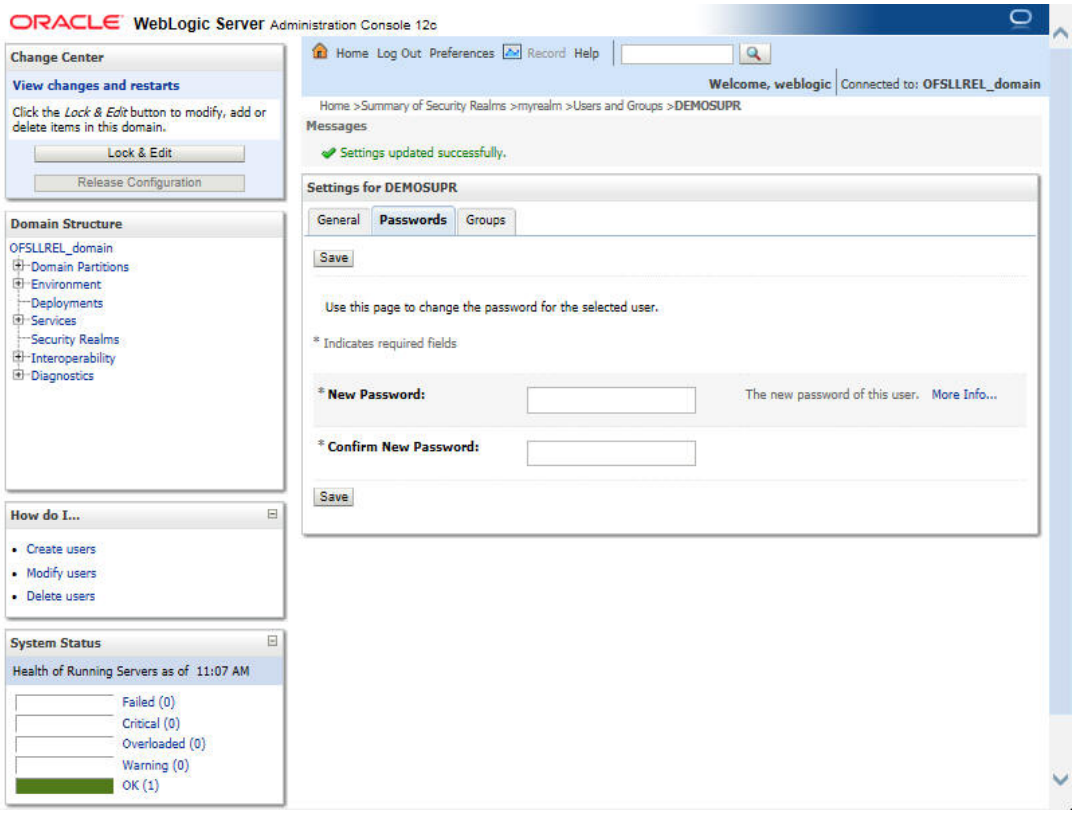
Figure 2-64 User Group 5



2. Click **Save**.

   The following window displayed.

Figure 2-65 User Group 6



2.7 Implementing JMX Policy for Change Password

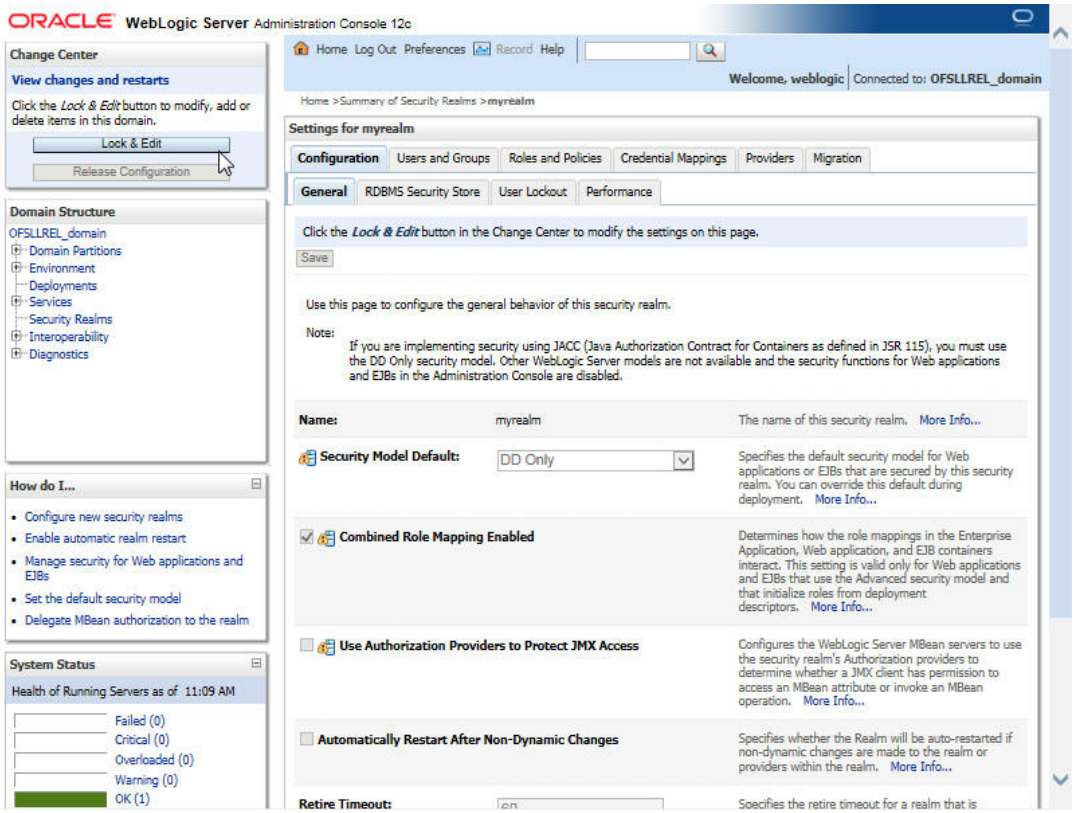
The following section details the steps to implement JMX Policy for Change Password.

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.

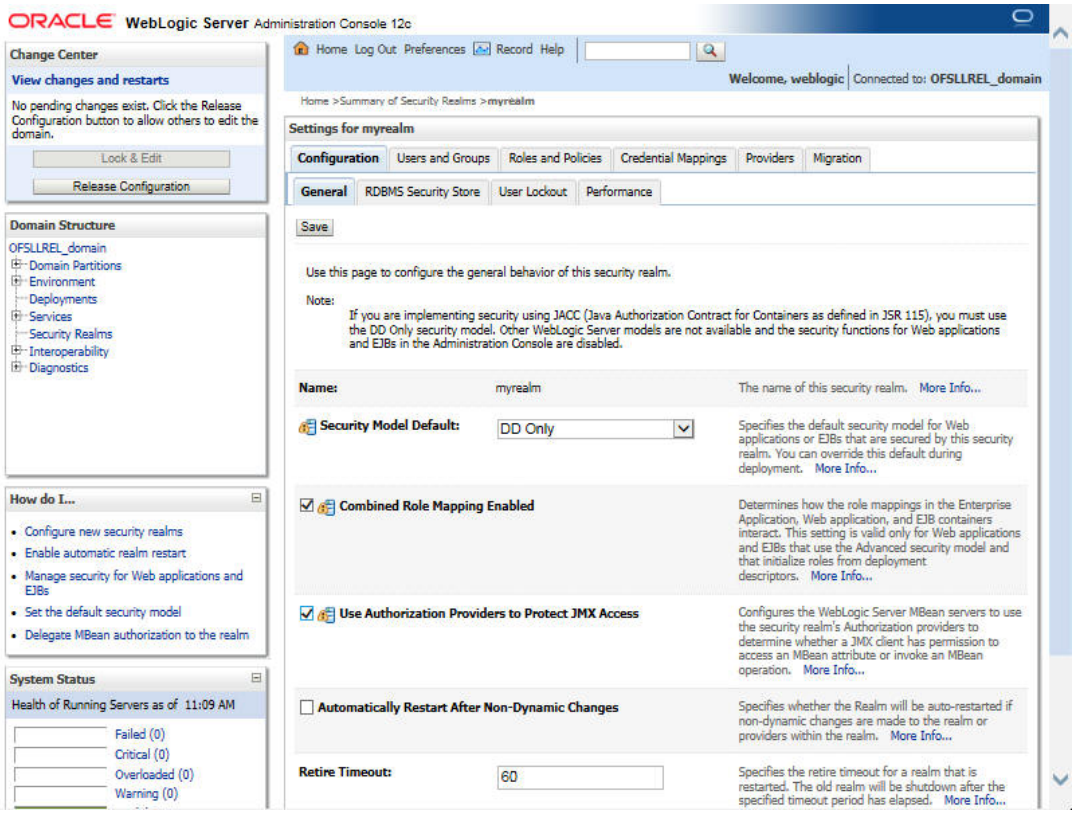
2. Click Domain > Security > myrealm > Configuration.

Figure 2-66 Implement JMX Policy 1



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

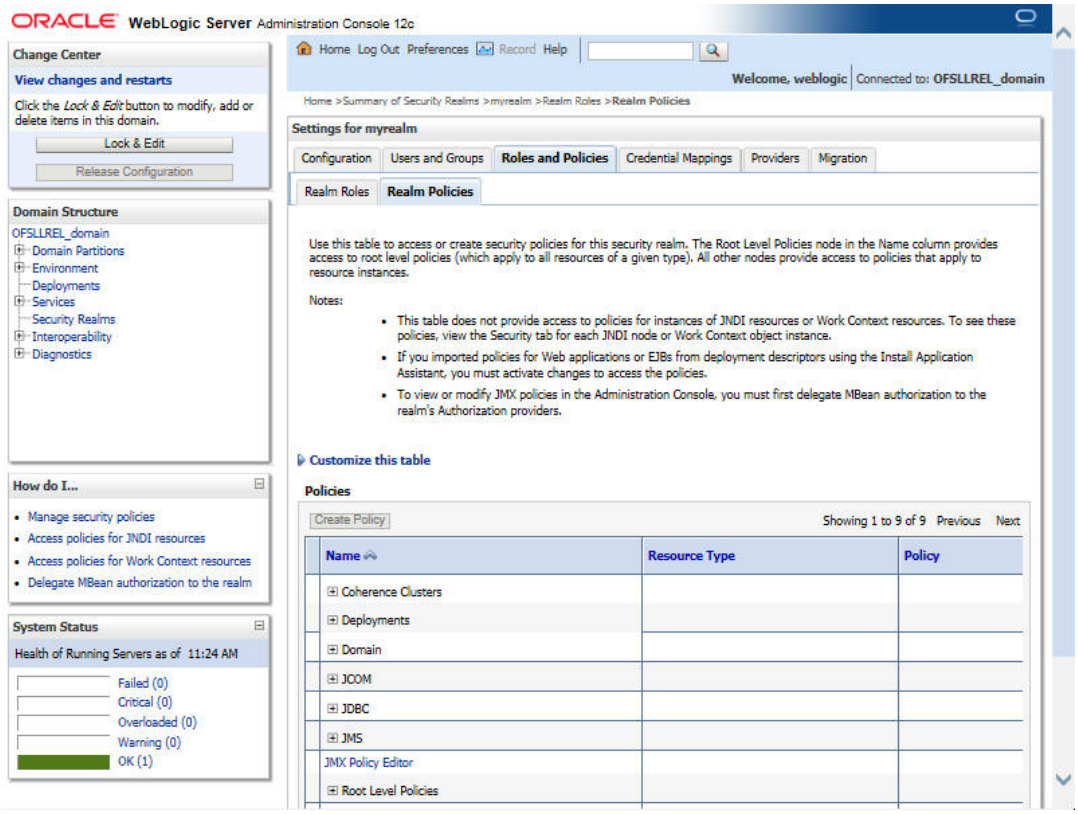
Figure 2-67 Implement JMX Policy 2



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

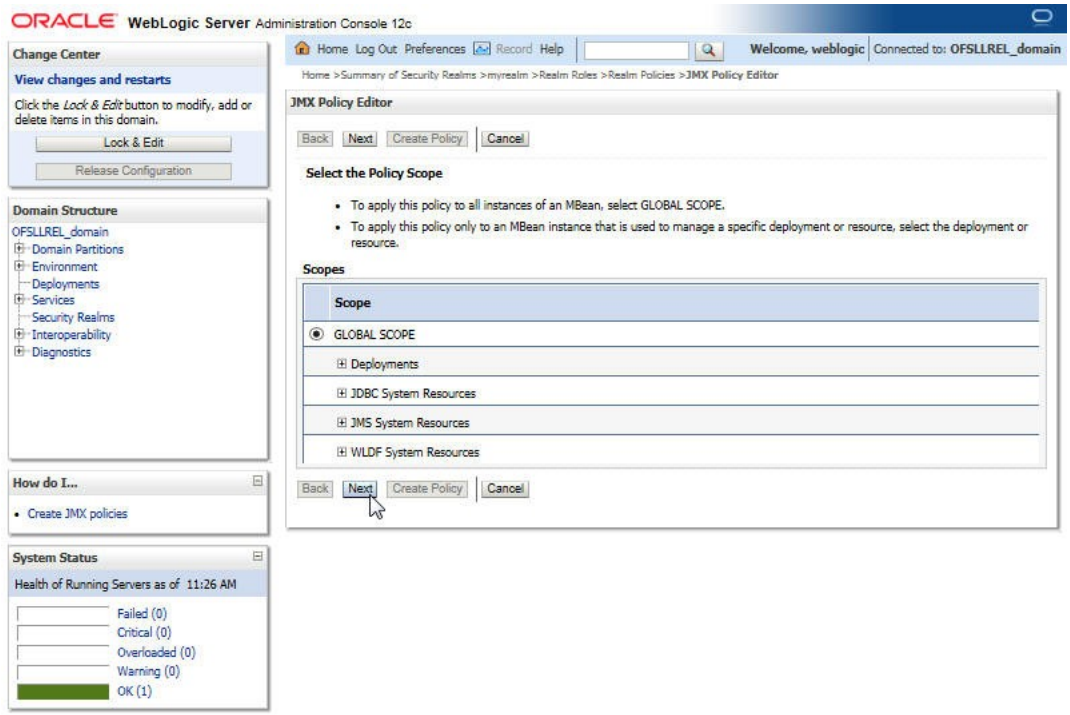
> **Note:**
>
> If server is not restarted, JMX Policy Editor option will not appear.

Figure 2-68 Implement JMX Policy 3



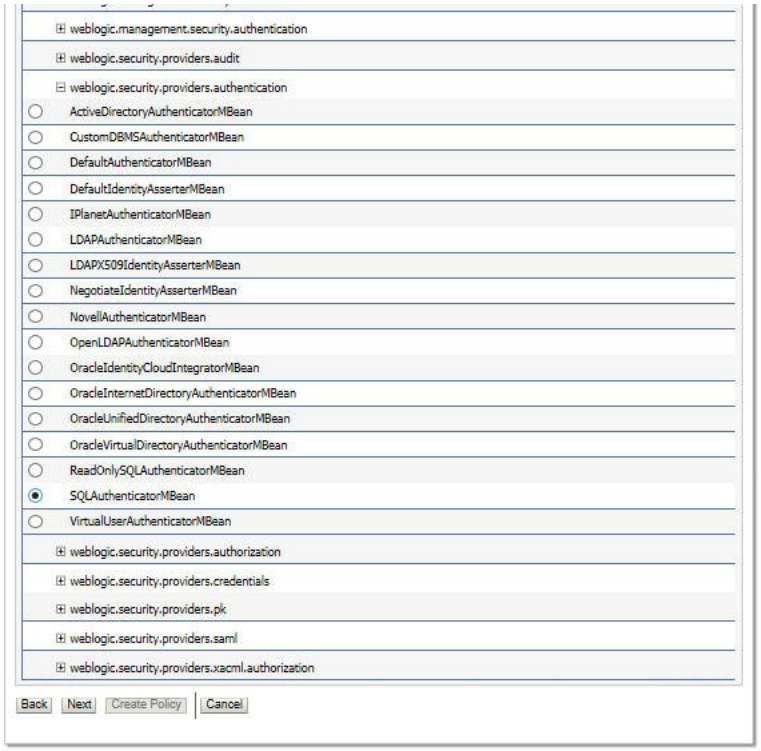
7. Click on JMX Policy Editor to configure.

Figure 2-69 Implement JMX Policy 4



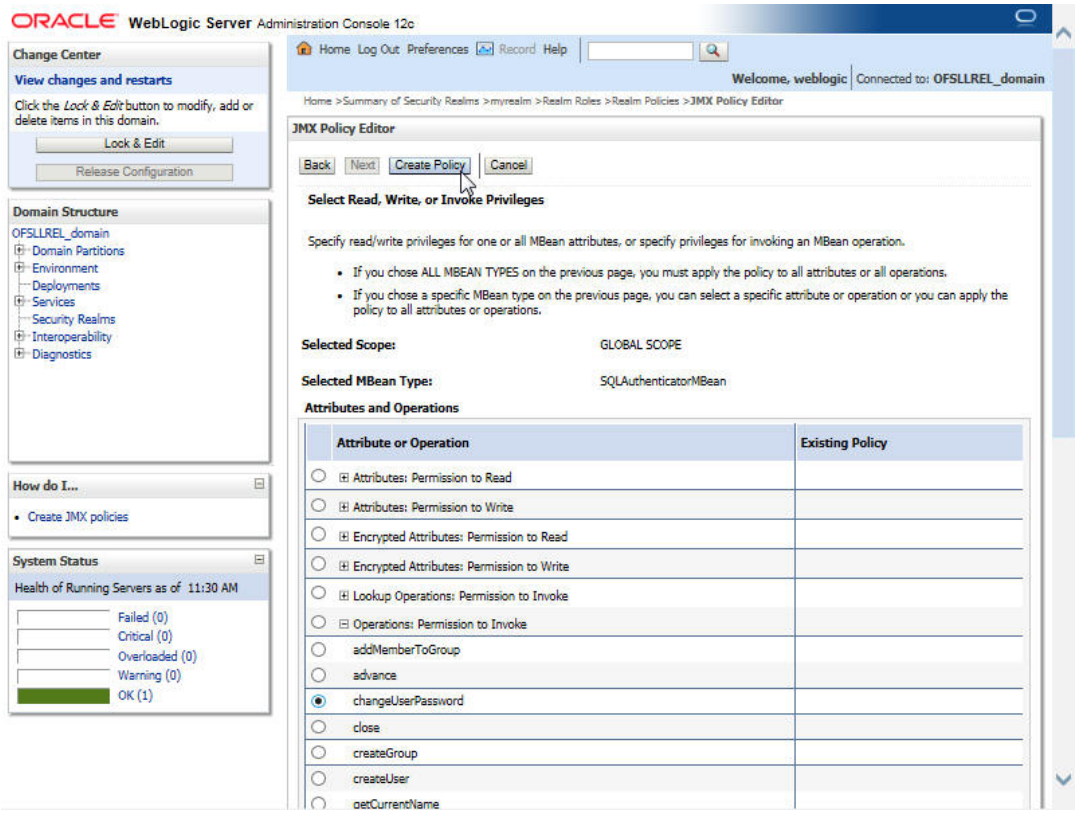
8. Select **GLOBAL SCOPE** and click **Next**.

Figure 2-70 Implement JMX Policy 5



9. Select **weblogic.security.providers.authentication**.
10. Select **SQLAuthenticatorMBean**. Click **Next**.

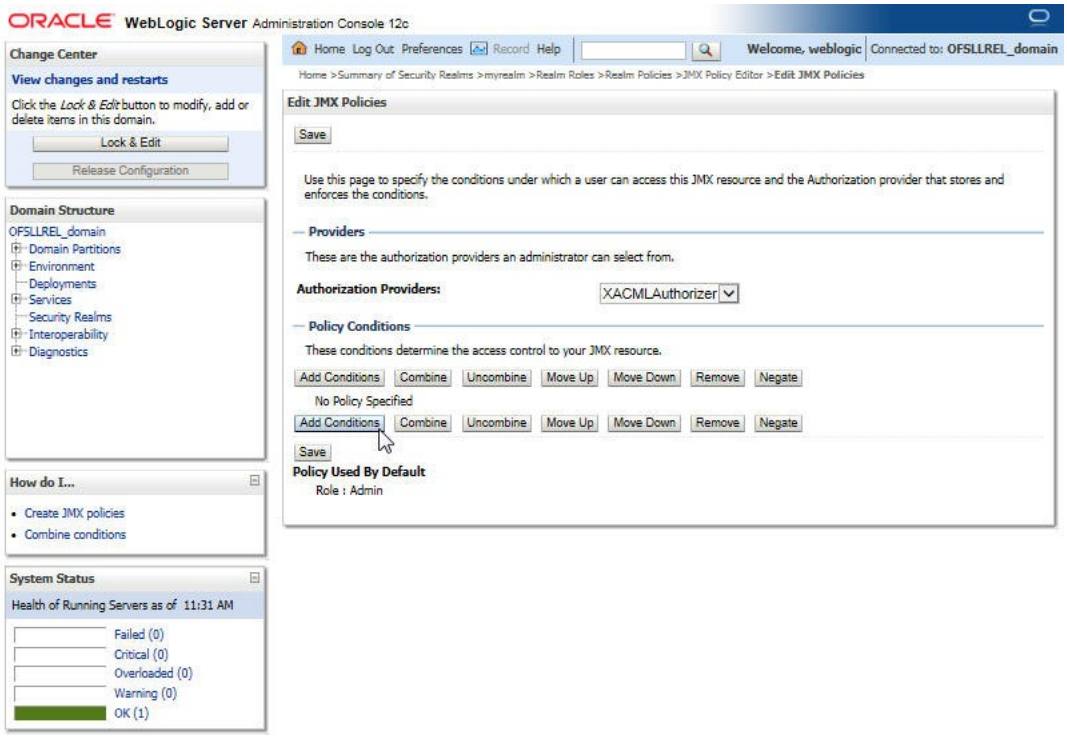
Figure 2-71 Implement JMX Policy 6



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**.

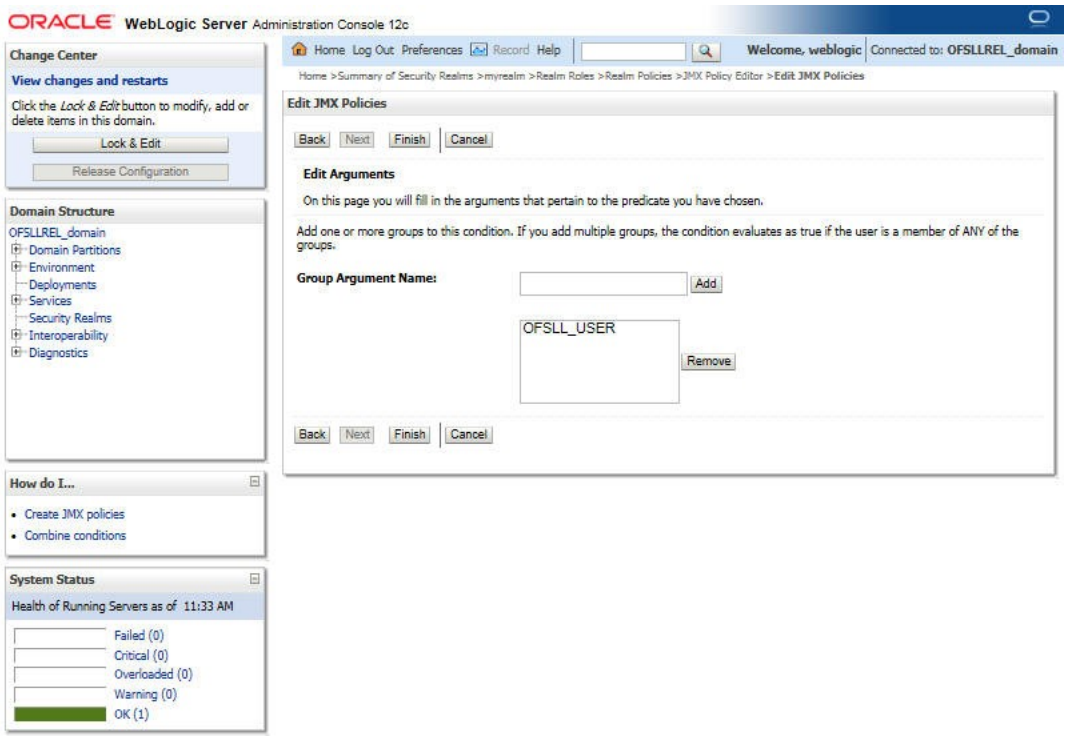
    The below screen will be displayed.

Figure 2-72 Implement JMX Policy 7



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

Figure 2-73 Implement JMX Policy 8

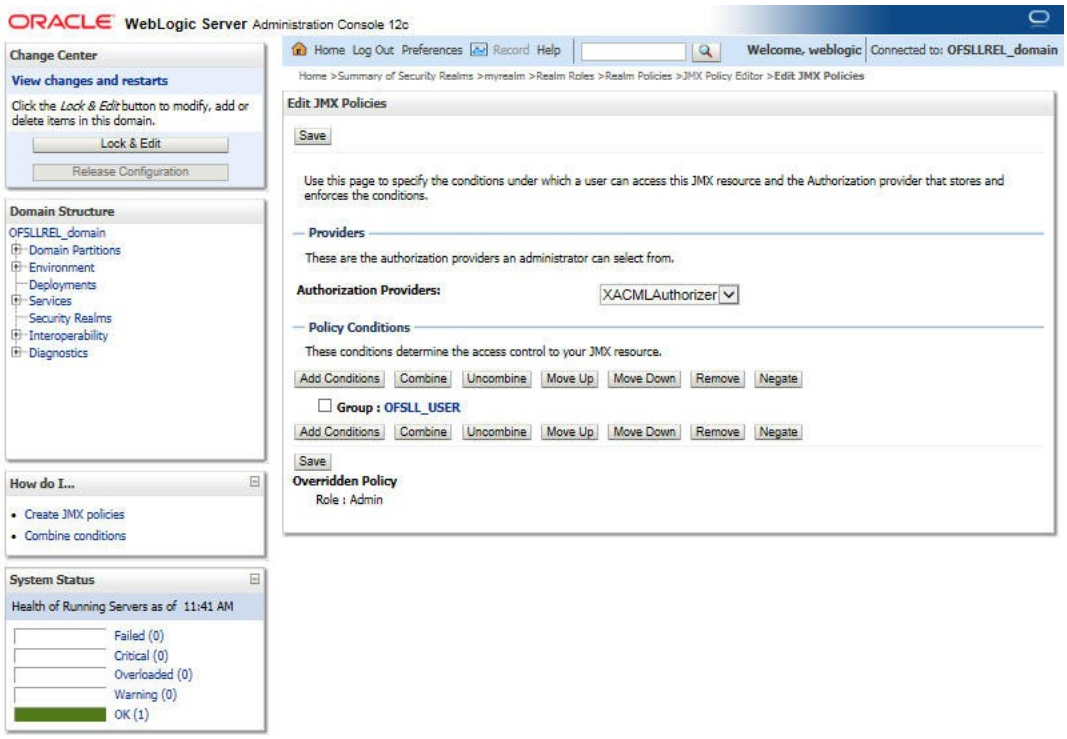


15. Select user roles for application.

16. Click **Finish**. Click on Save to complete the configuration.

    The following window will be displayed.

Figure 2-74 Implement JMX Policy 9



3
Configure Policies

The following sections details the steps to configure password policy for SQL Authenticator and configure user lockout policy .

- Configuring Password Policy for SQL Authenticator
- Configuring User Lockout Policy

3.1 Configuring Password Policy for SQL Authenticator

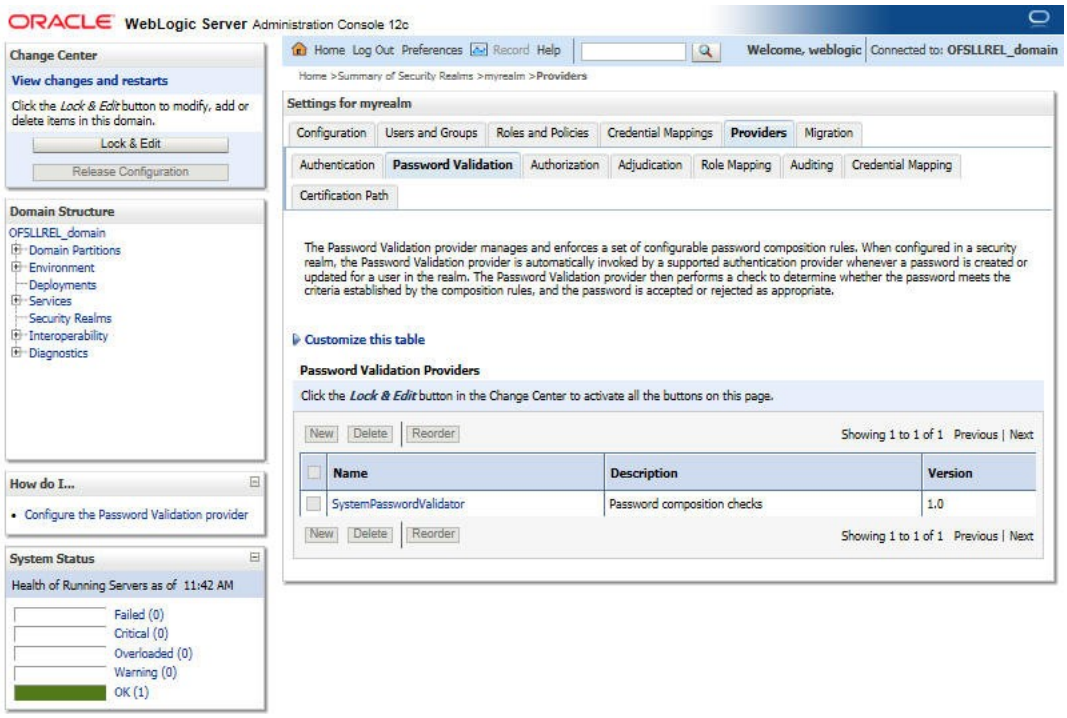
1. Login to the WebLogic server administration console with user login credentials.

   (Optional) Enter the result of the step here.

2. Browse to Security Realms > myrealm > Providers > Password Validation as shown below.

   The following window is displayed.

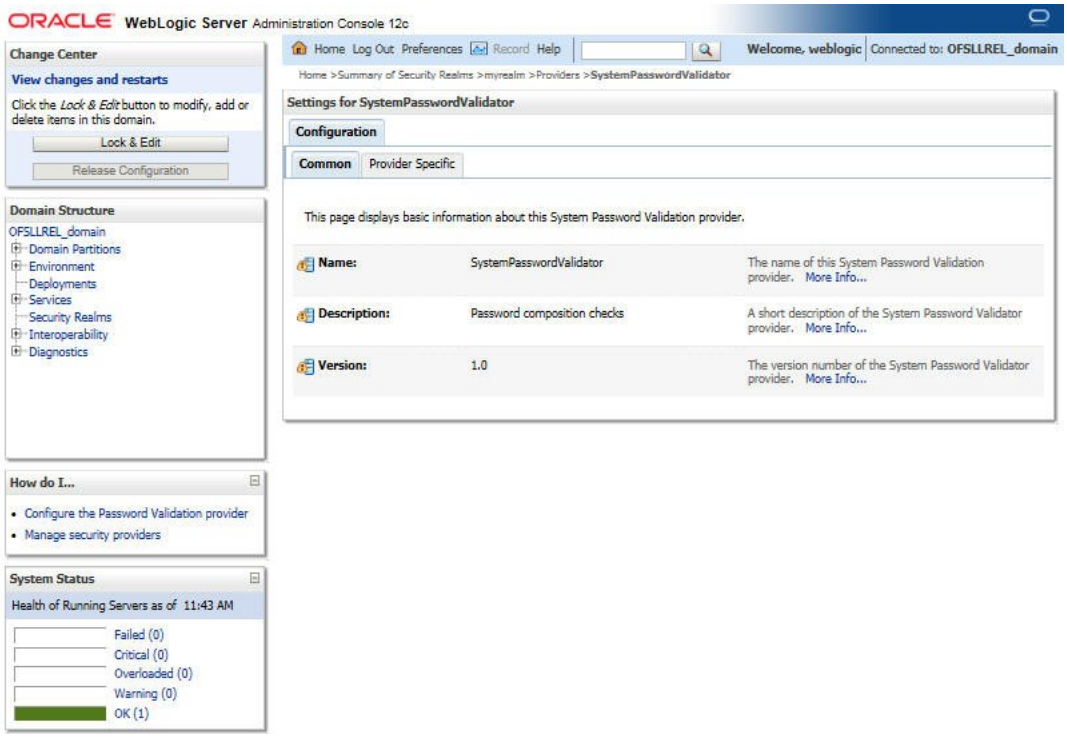
Figure 3-1 Configuring Password Policy 1



3. Click **SystemPasswordValidator** link.

   The following window is displayed.

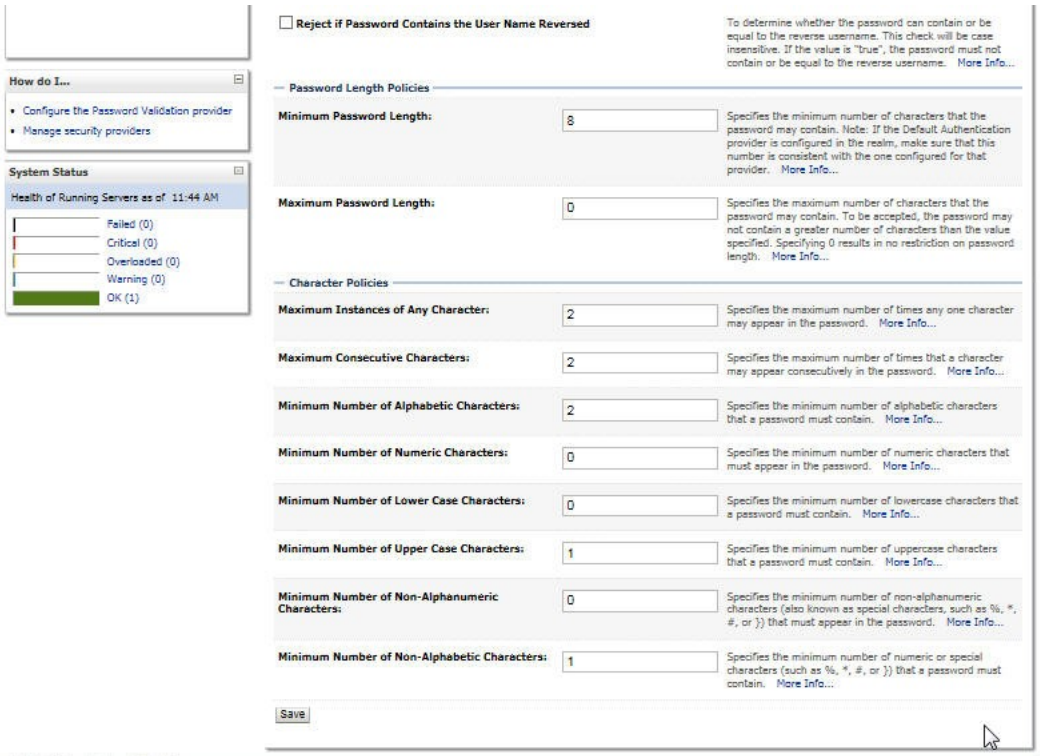
Figure 3-2 Configuring Password Policy 2



4. Click Provider Specific Tab.
5. Configure the password policy as per the requirement.

   An example is provided in the following window.

Figure 3-3 Configuring Password Policy 3



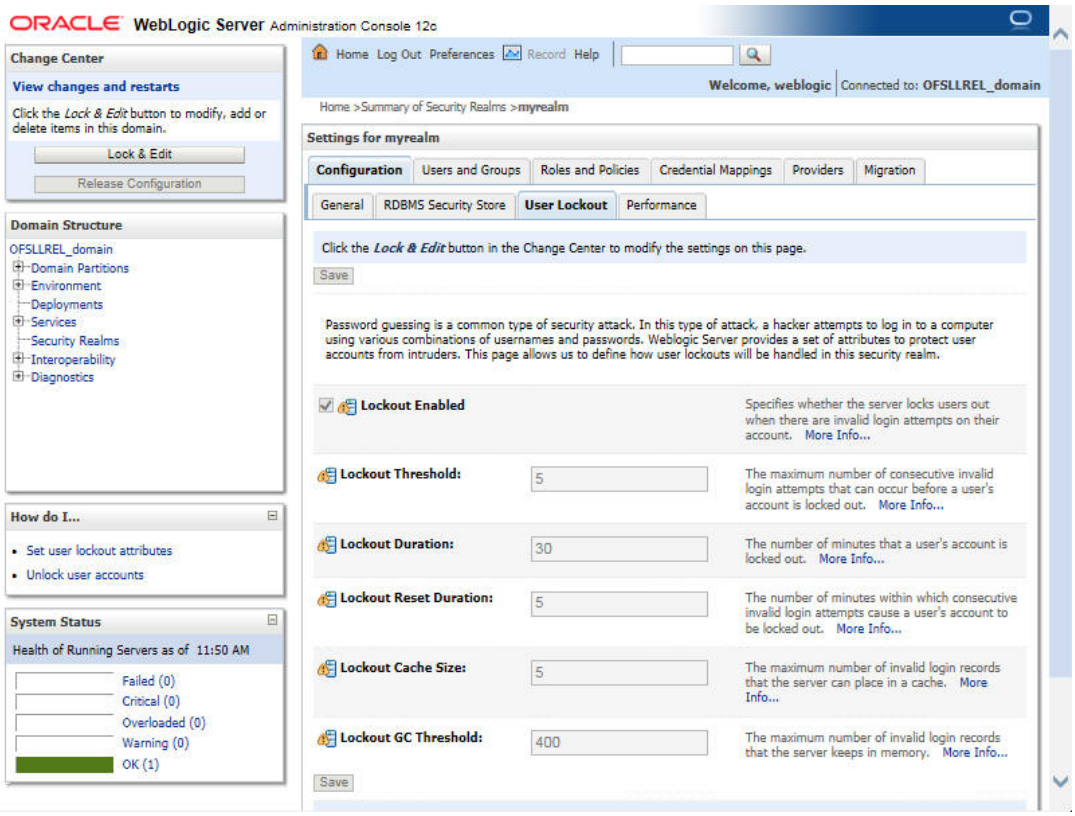
6. Click **Save**.

3.2 Configuring User Lockout Policy

1. To Change User lockout policy, browse to Security Realms > myrealm > Configuration Tab > User Lockout Tab.

   The following window is displayed.

Figure 3-4 Configuring User Lockout Policy



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

4
Deploy Application

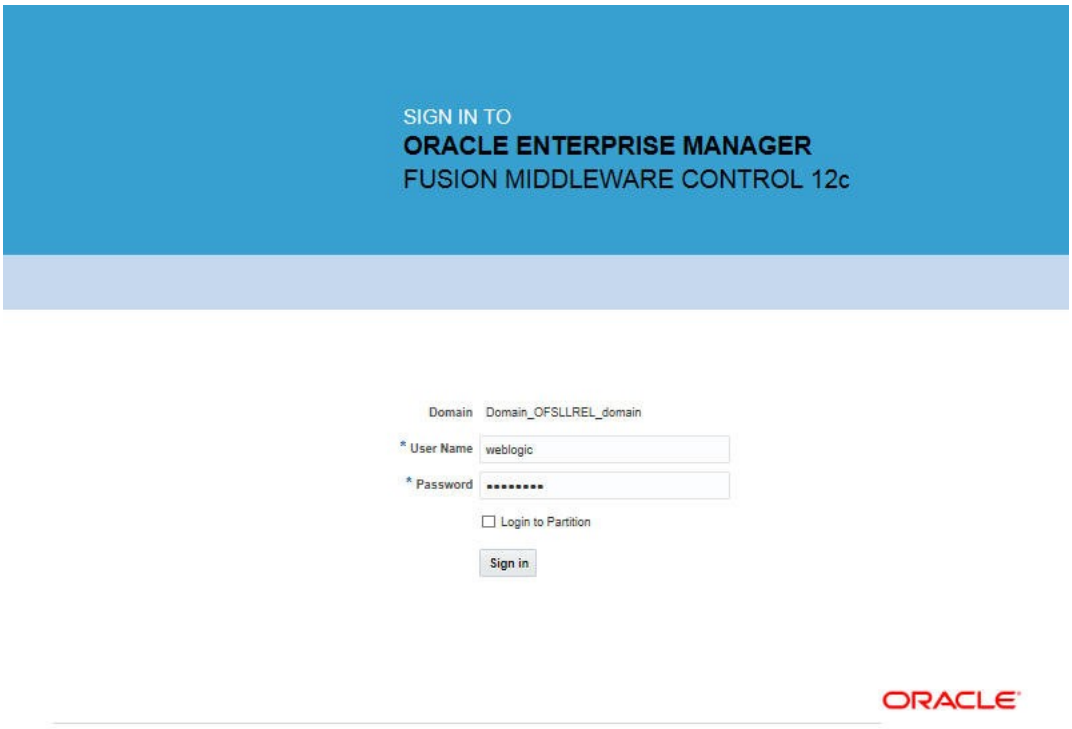
The following section details the steps to deploy Application.

- Deploying Application

4.1 Deploying Application

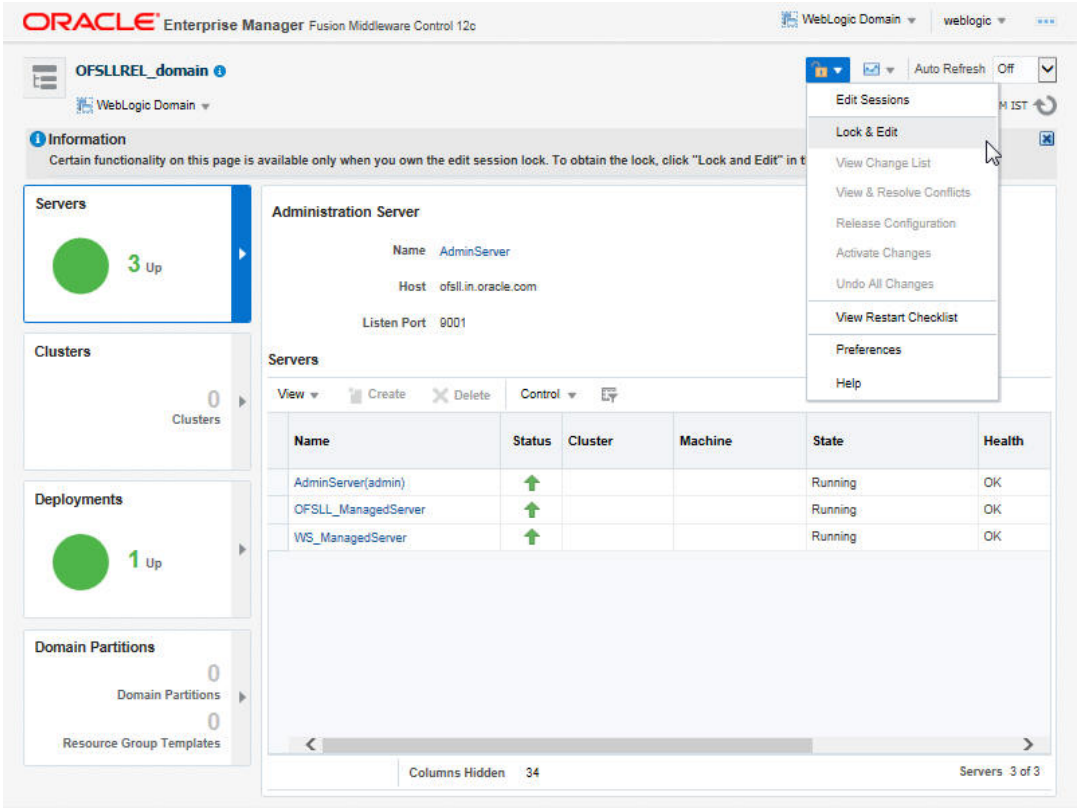
1. Login to the Oracle Enterprise Manager 12c console . (i.e. `http://hostname:port/em`)

Figure 4-1 Deploying Application 1



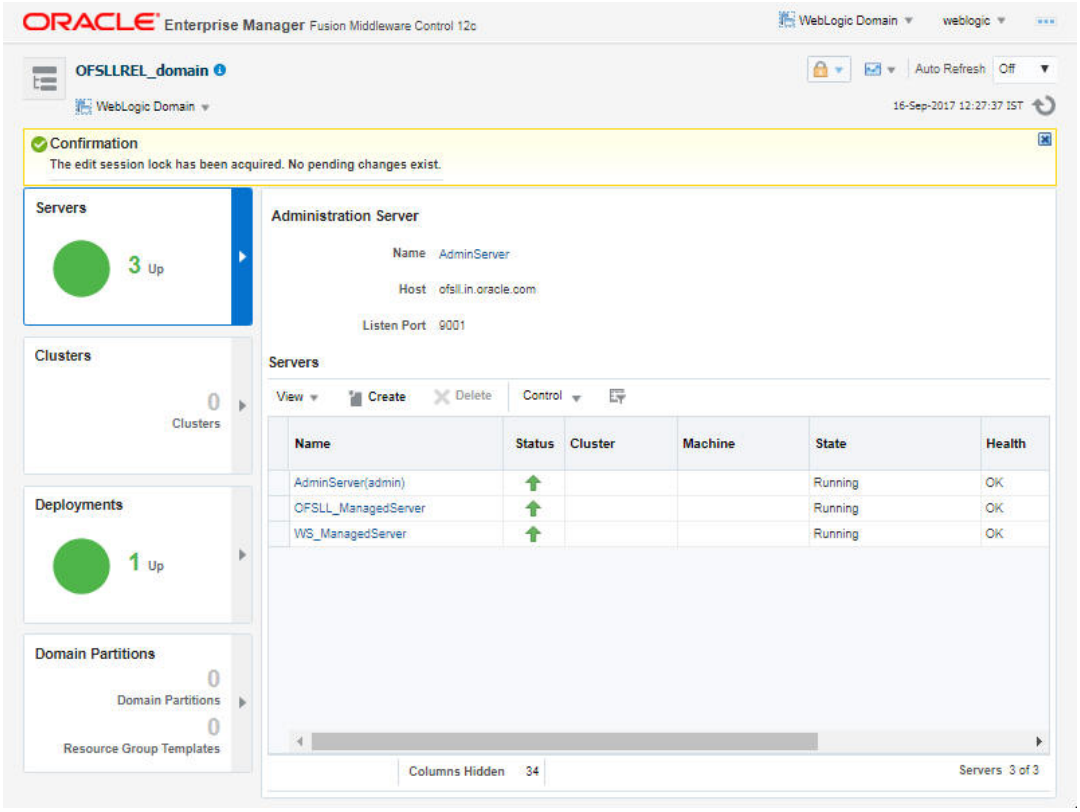
2. Click on **Lock and Edit** as shown below.

Figure 4-2 Deploying Application 2



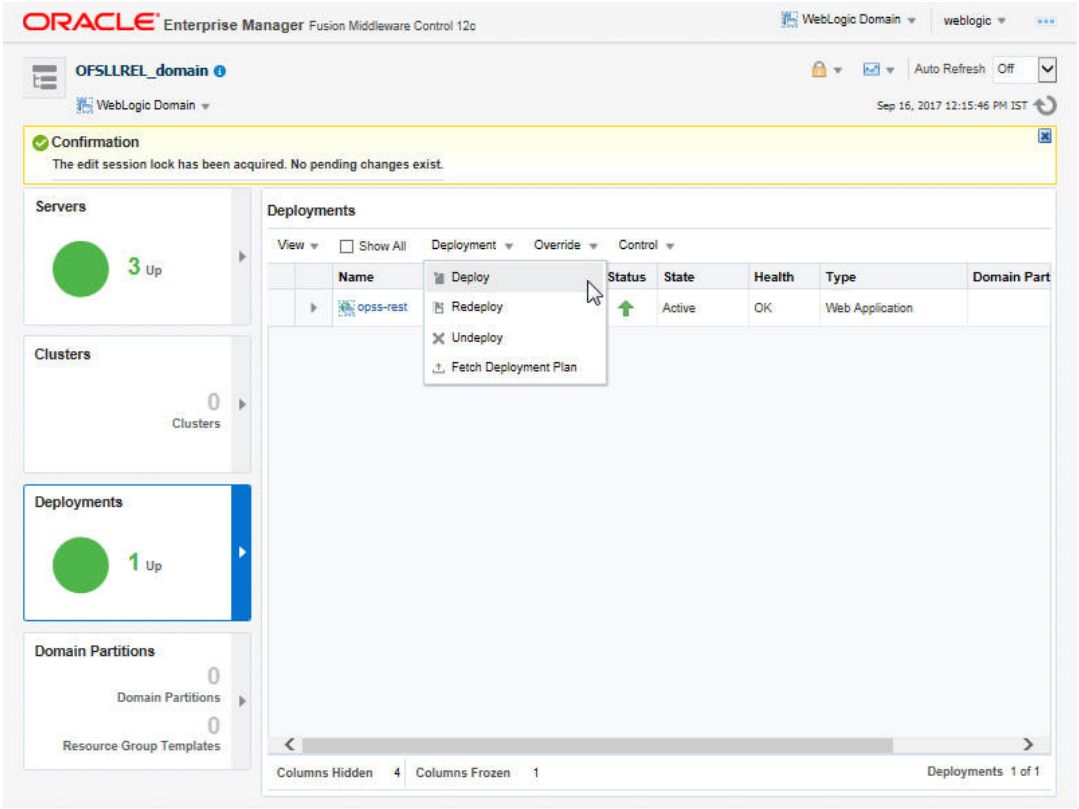
3. The following window is displayed.

Figure 4-3 Deploying Application 3



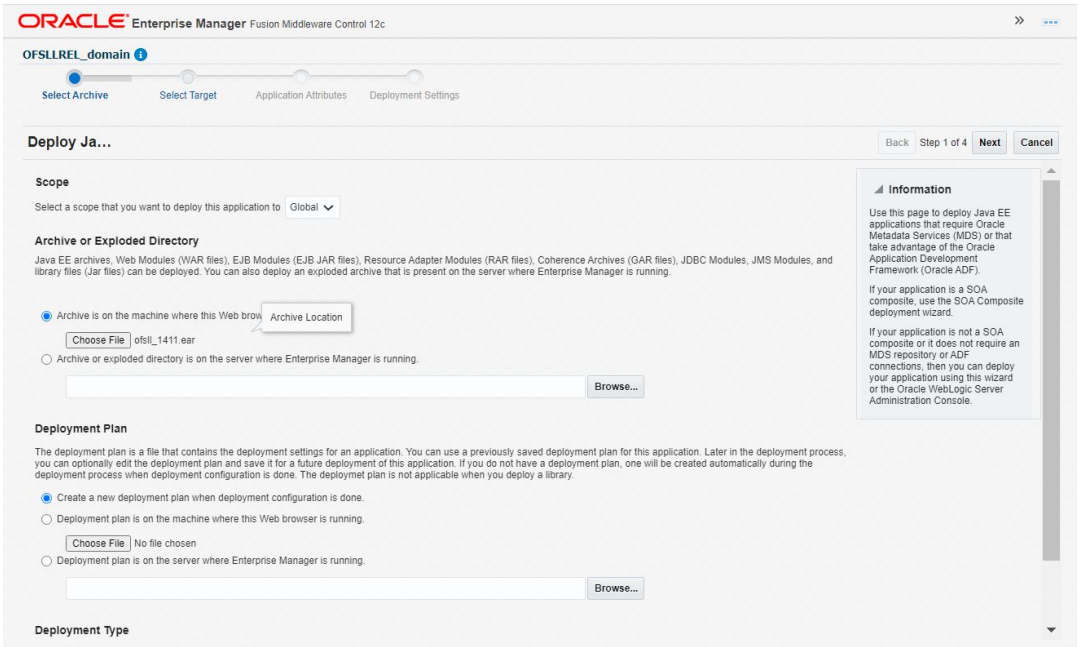
4. Click on **Deployments** in the left panel. To deploy go to Deployments option in the menu as shown below.

Figure 4-4 Deploying Application 4



5. Click **Choose File** button and select OFSLL application archive file i.e. `ofsll_1411.ear`. Choose the **Deployment Plan** (if any).

Figure 4-5 Deploying Application 5



> **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

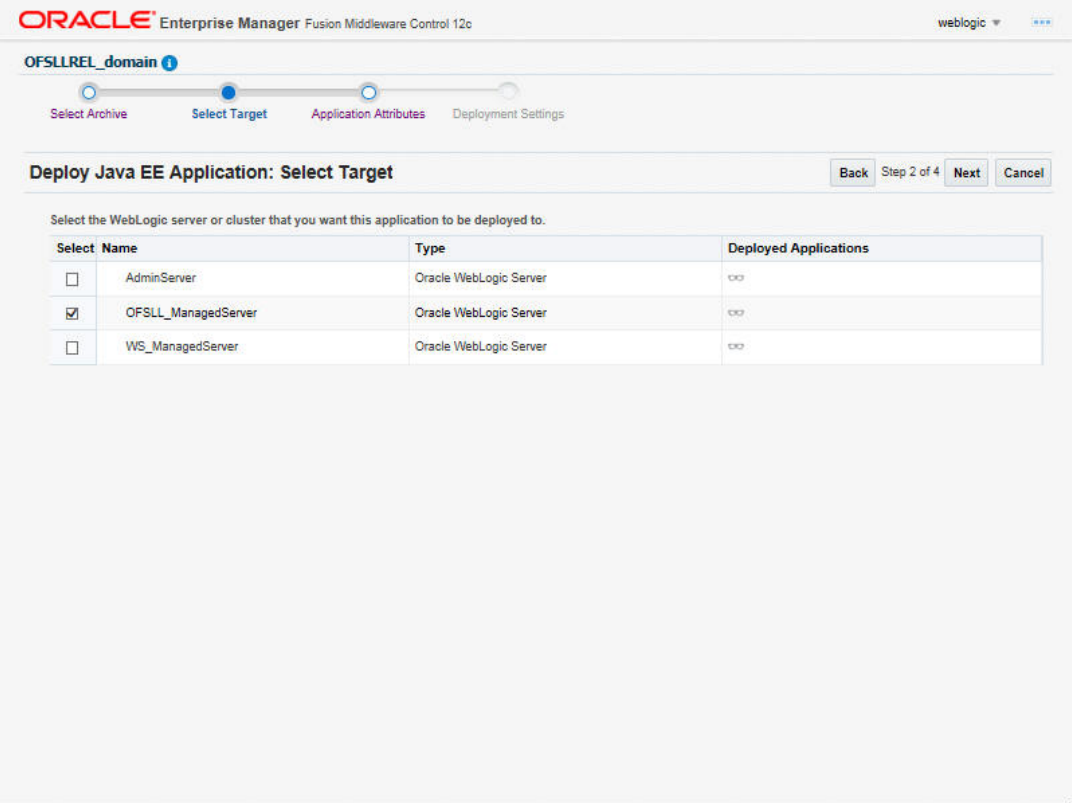
Figure 4-6 Deploying Application 6

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

6. Click **Next**.

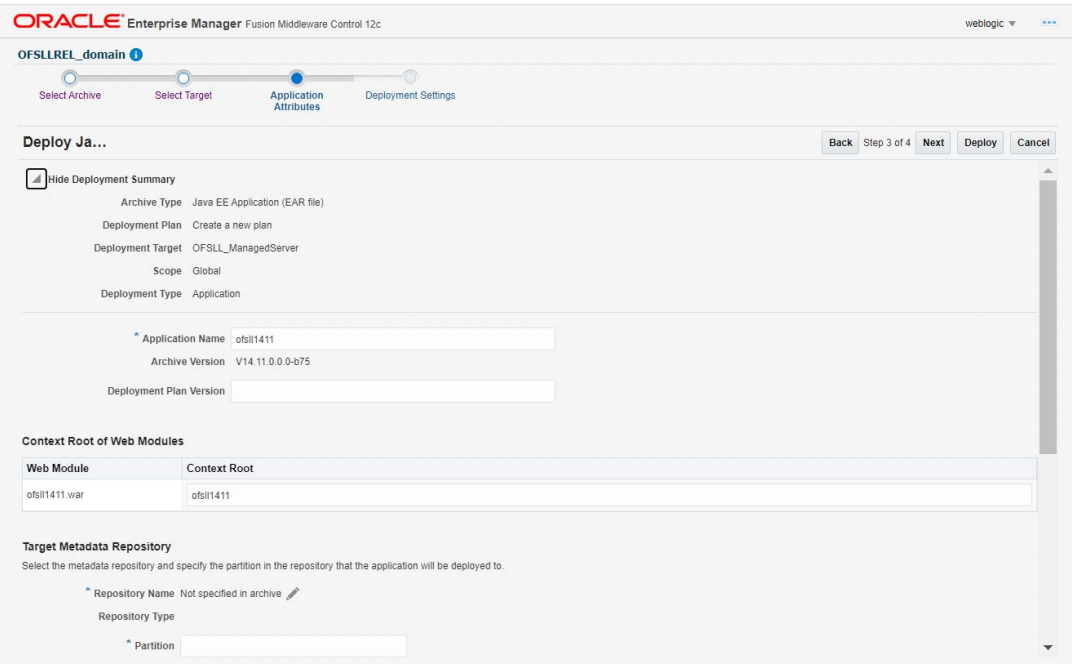
   The following window is displayed.

Figure 4-7 Deploying Application 7



7. Check target server as per the requirement **OFSLL_ManagedServer** and click **Next**.

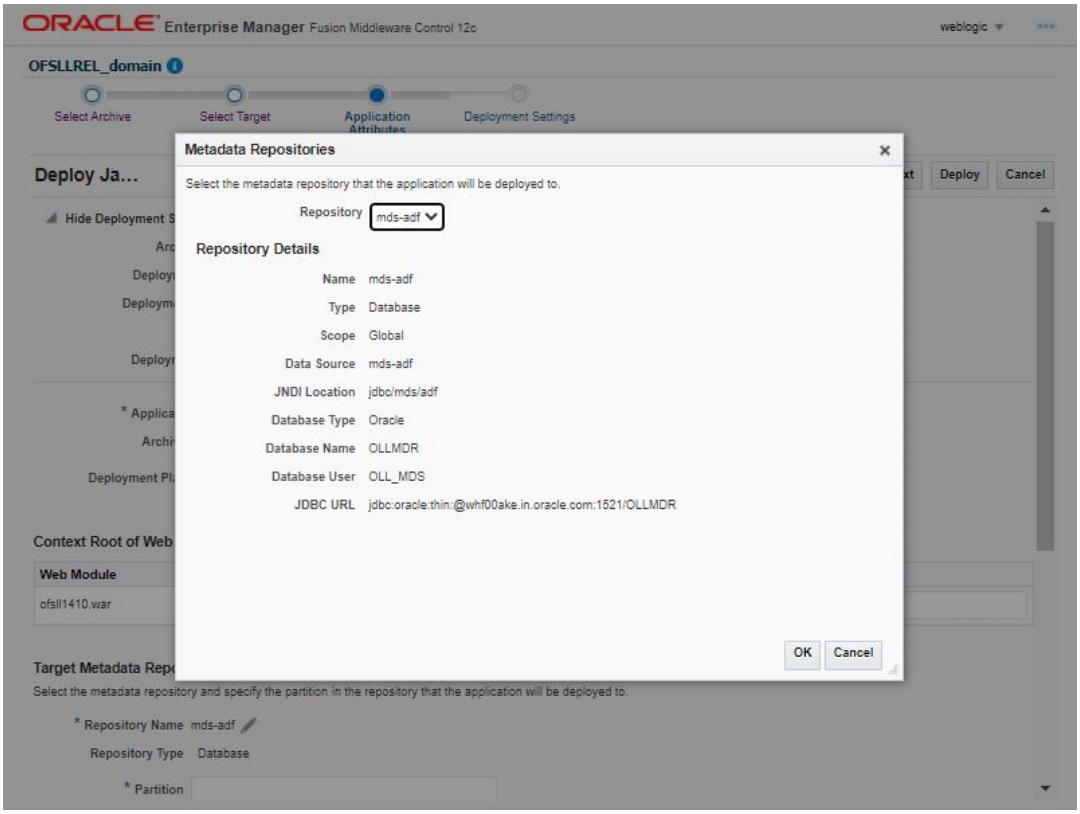
Figure 4-8 Deploying Application 8



8. Click button to select Repository Name.

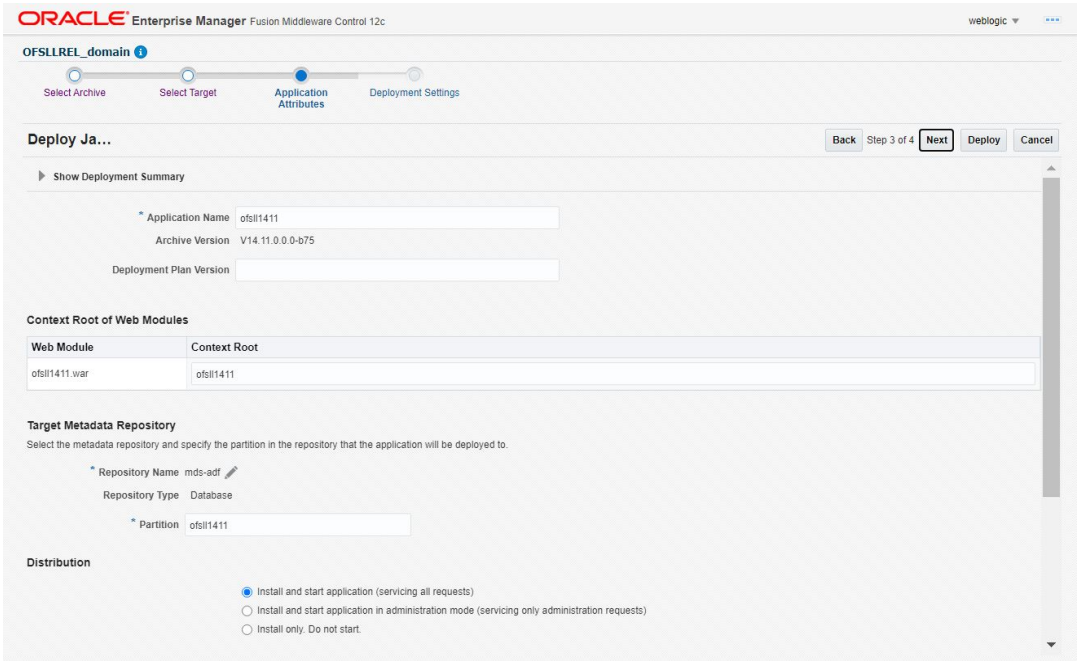
   The following window is displayed.

Figure 4-9 Deploying Application 9



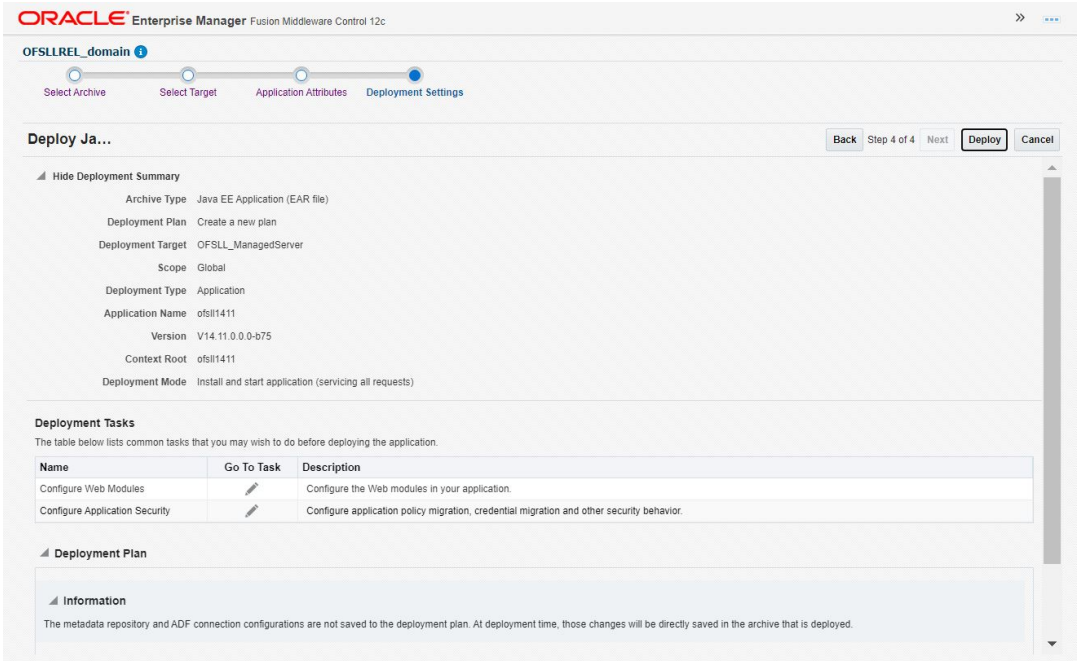
9. Select Repository as per requirement and click **OK**.

Figure 4-10 Deploying Application 10



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

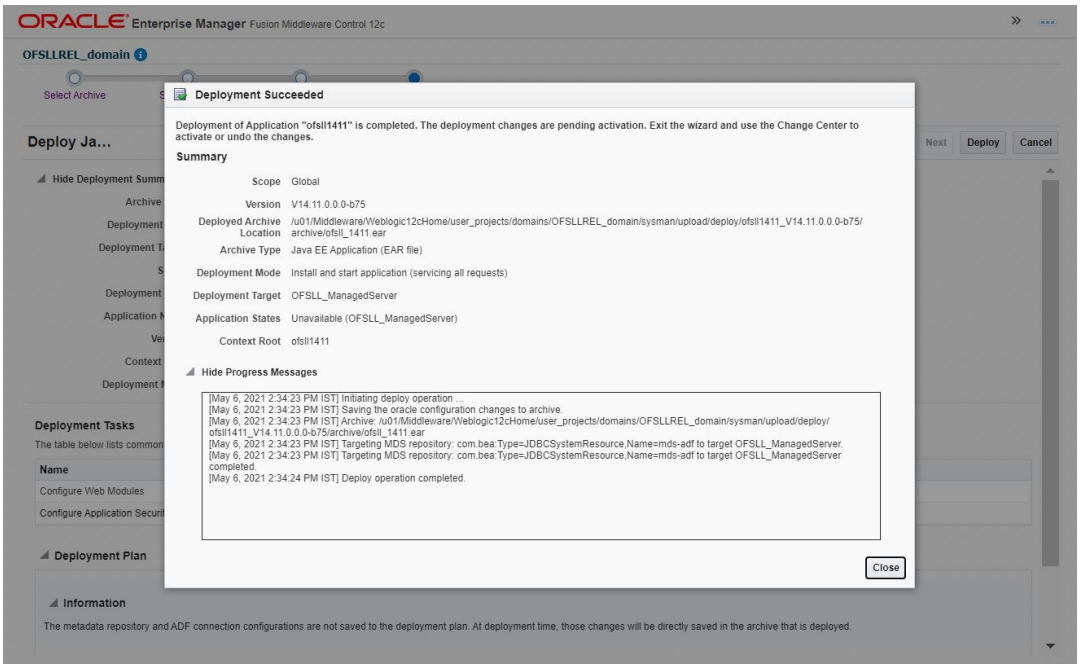
Figure 4-11 Deploying Application 11



11. Click **Deploy**.

    The following window is displayed.

Figure 4-12 Deploying Application 12



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

5

Enable SSL

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

- Enabling SSL

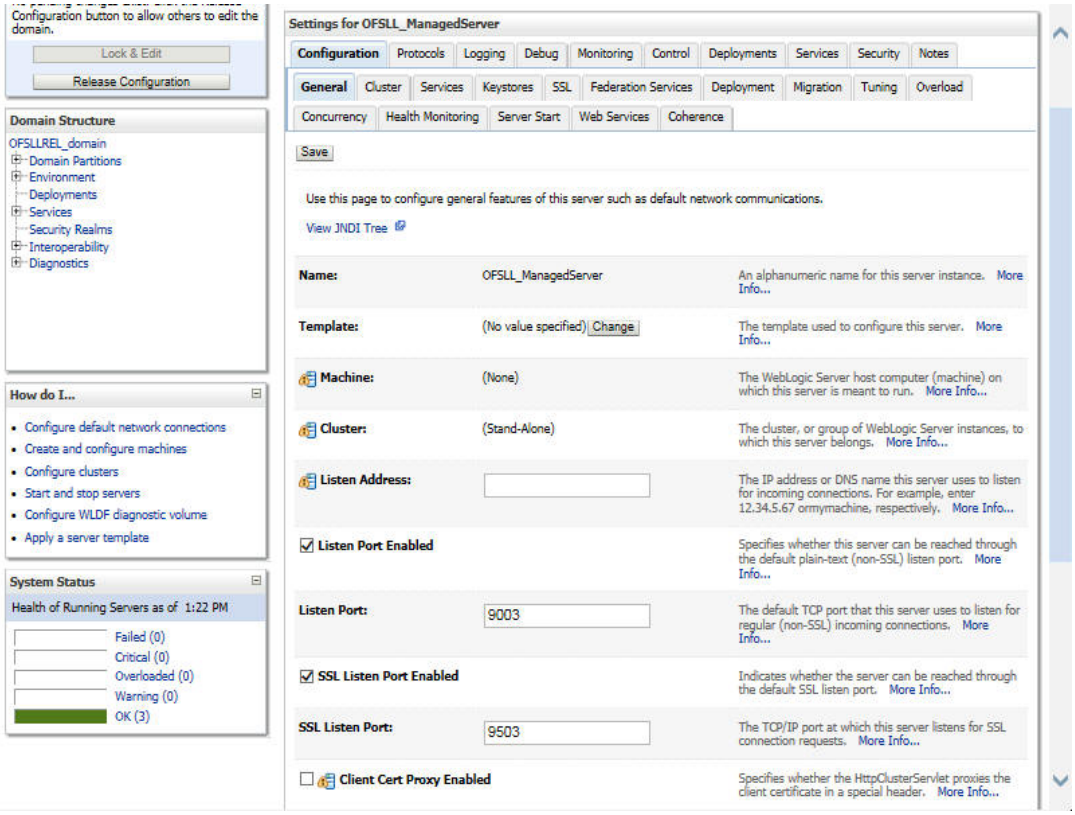
5.1 Enabling SSL

To enable SSL

1. Login to console.
2. $Domain_Home > Servers > Manage Servers > Configuration > General.

   The below screen is displayed.

Figure 5-1 Enable SSL



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.

6
Map Enterprise Group with Application Role

The following section details the steps to be followed to map enterprise group with application role.

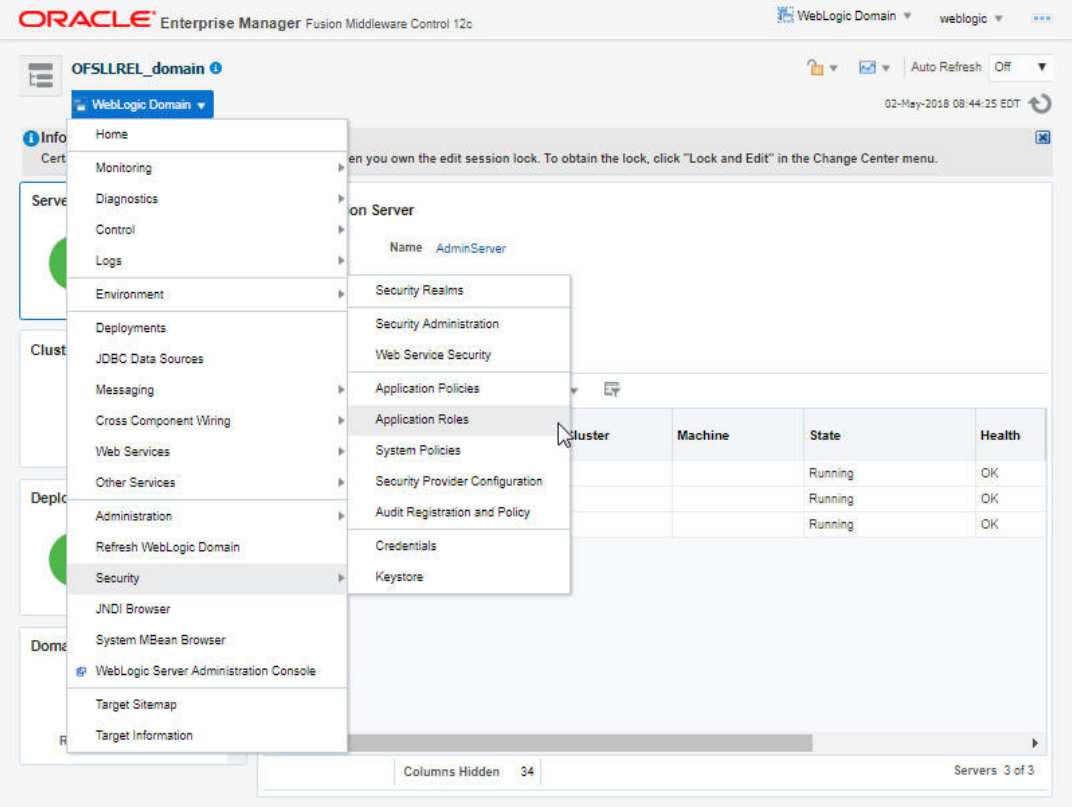
- Mapping Enterprise Group with Application Role

6.1 Mapping Enterprise Group with Application Role

Follow the below steps to add an user to the group:

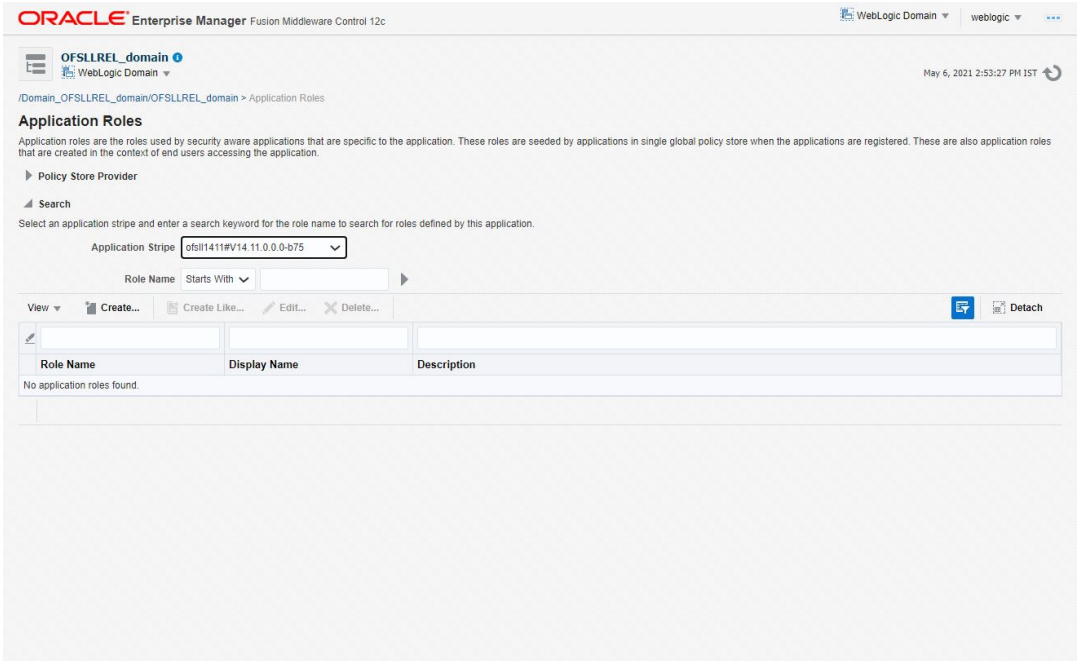
1. Login to Oracle Enterprise Manager 12c console (`http://hostname:port/em`).
2. Click WebLogic Domain > Security > Application Roles on the right panel.

Figure 6-1 Mapping Enterprise Group 1



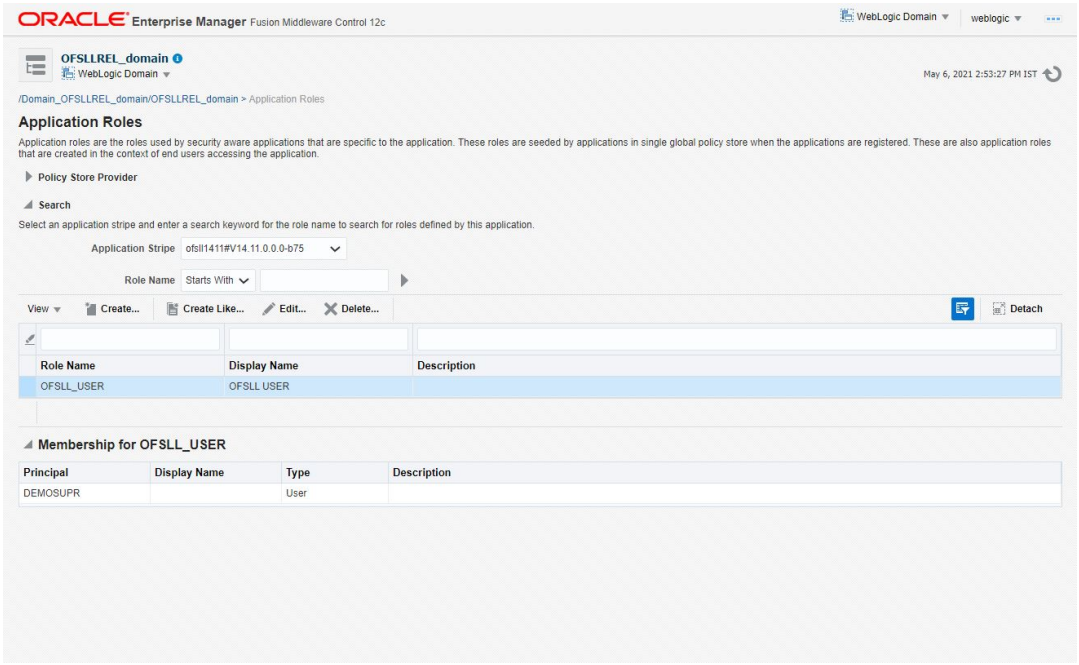
3. Select Application Stripe from the drop-down menu.
4. Click the arrow head button. Details of the existing Roles are displayed below:

Figure 6-2 Mapping Enterprise Group 2



5. Select the **Role Name**. Membership details of the selected Role Name are displayed under Membership for **role_name**.

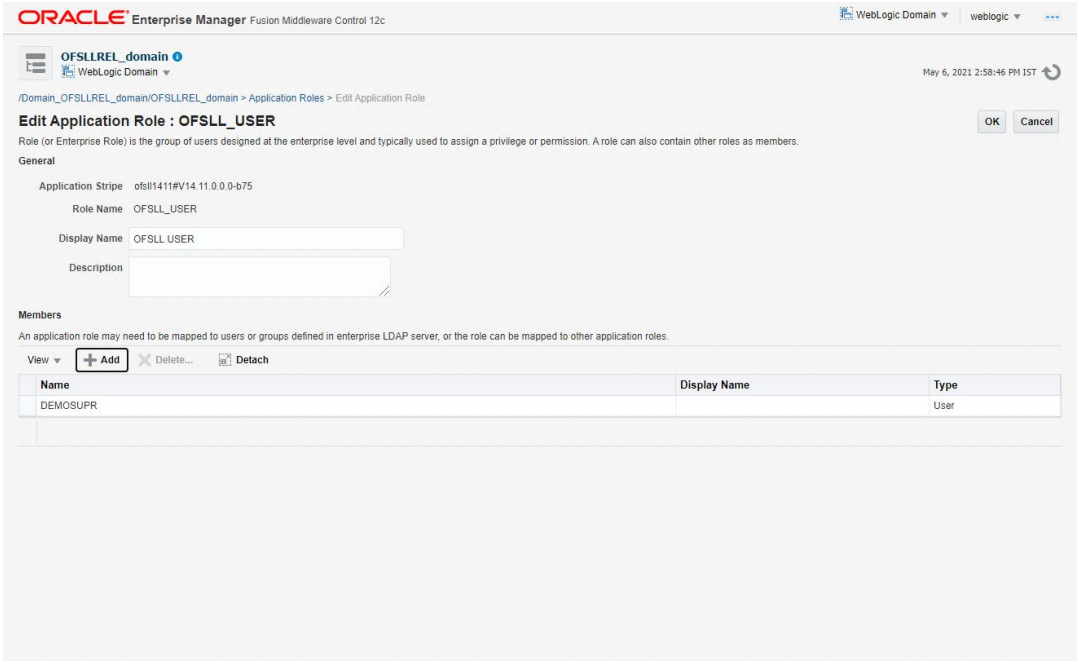
Figure 6-3 Mapping Enterprise Group 3



6. Click **Edit**.

   The following window is displayed.

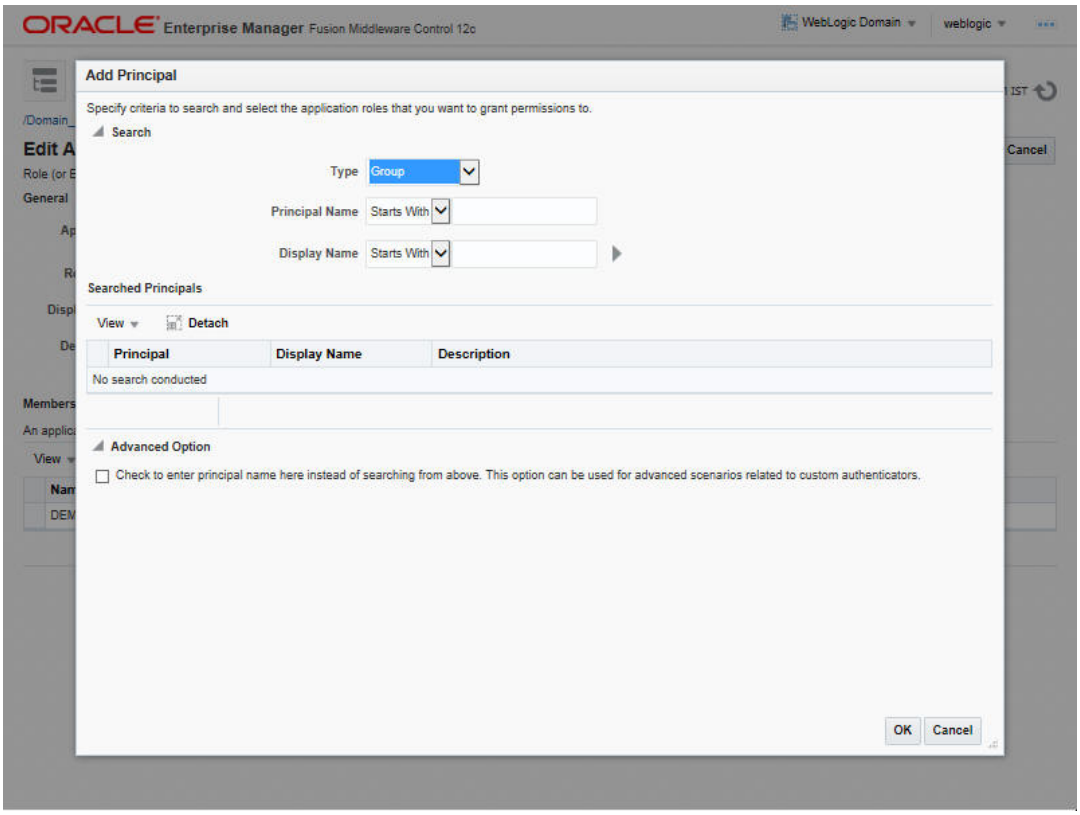
Figure 6-4 Mapping Enterprise Group 4



7. Click **Add**. Select type as Group. Click on the arrow head button.
8. Follow the given steps to select the Principal **OFSLL_USER** to add and click **OK**.

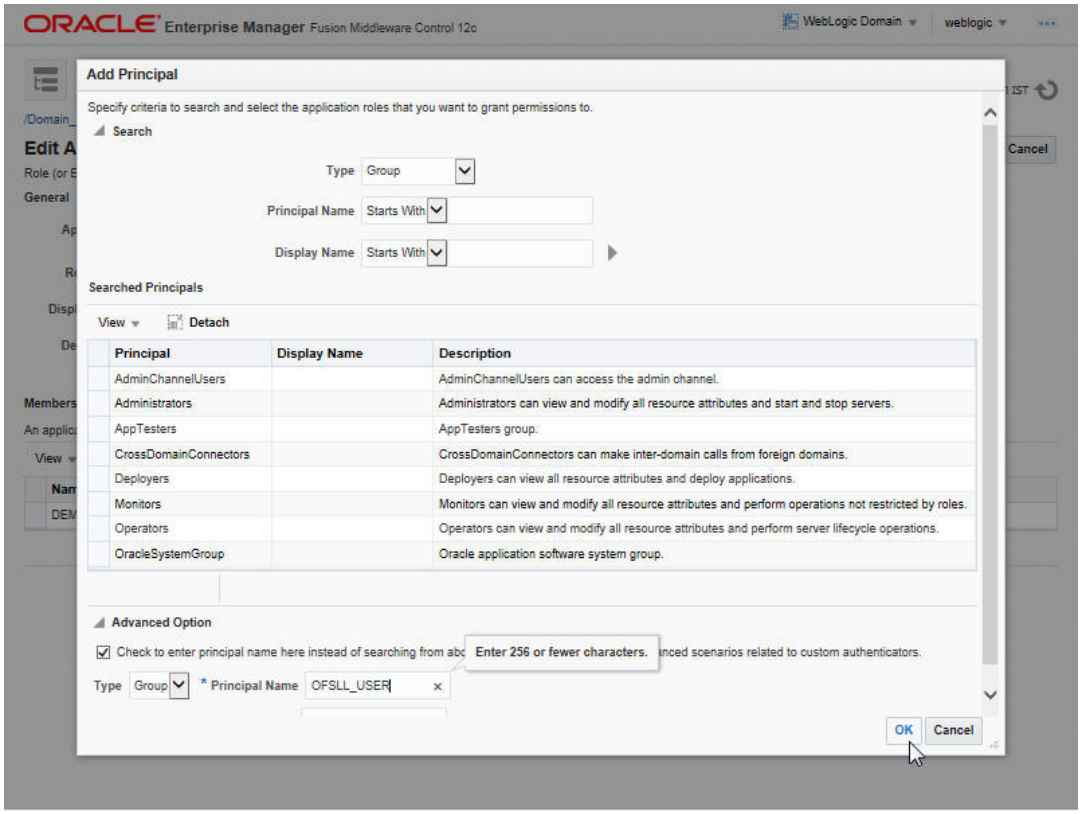
   The following window is displayed.

Figure 6-5 Mapping Enterprise Group 5



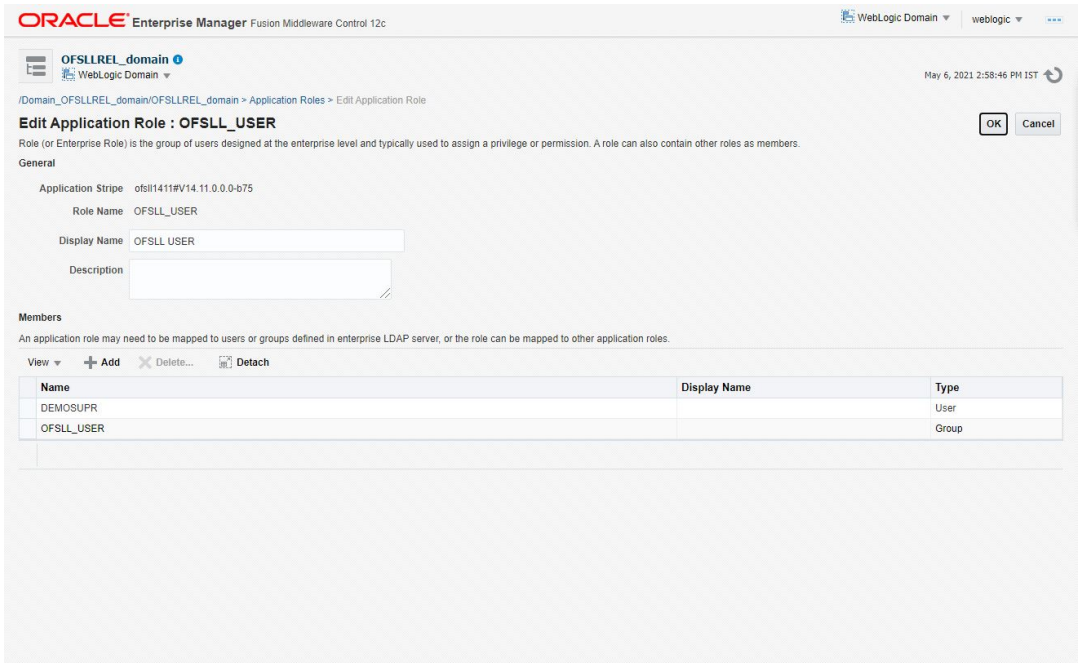
9. Check the check box in Advanced options. Enter the name of Group manually.

Figure 6-6 Mapping Enterprise Group 6



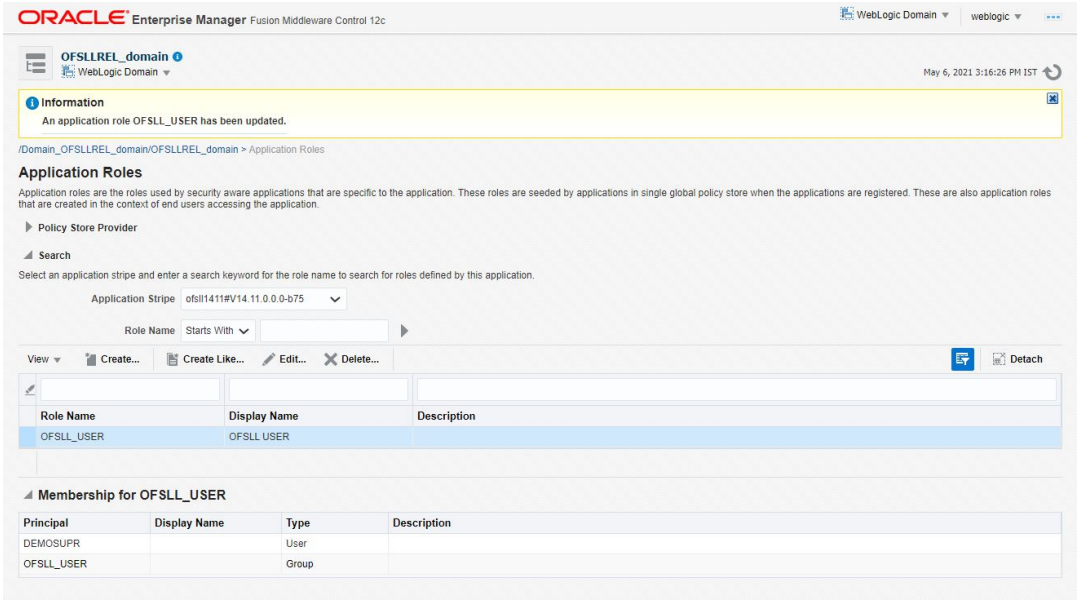
10. Click **OK**.

Figure 6-7 Mapping Enterprise Group 7



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

Figure 6-8 Mapping Enterprise Group 8



7

Configure JNDI name for HTTP Listener

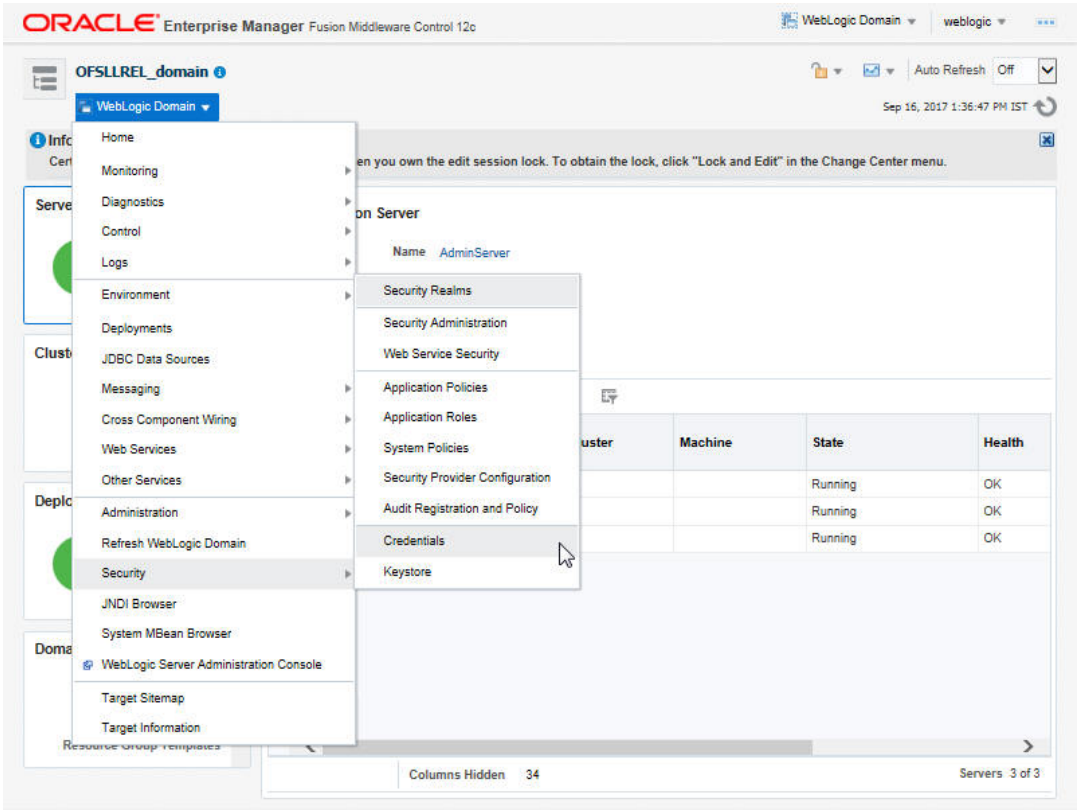
The following section details the steps to be followed to configure JNDI name for HTTP listener.

- Configuring JNDI name for HTTP Listener

7.1 Configuring JNDI name for HTTP Listener

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

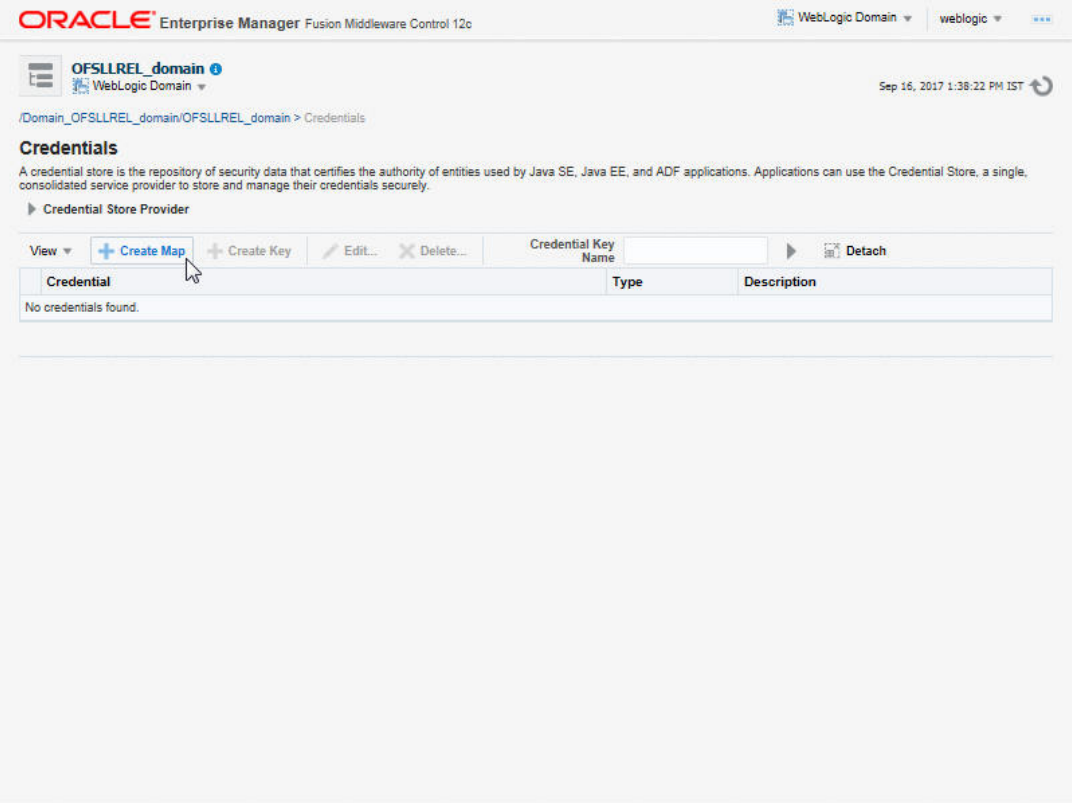
Figure 7-1 JNDI for HTTP Listener 1



2. Click **Credentials**.

   The following window is displayed.

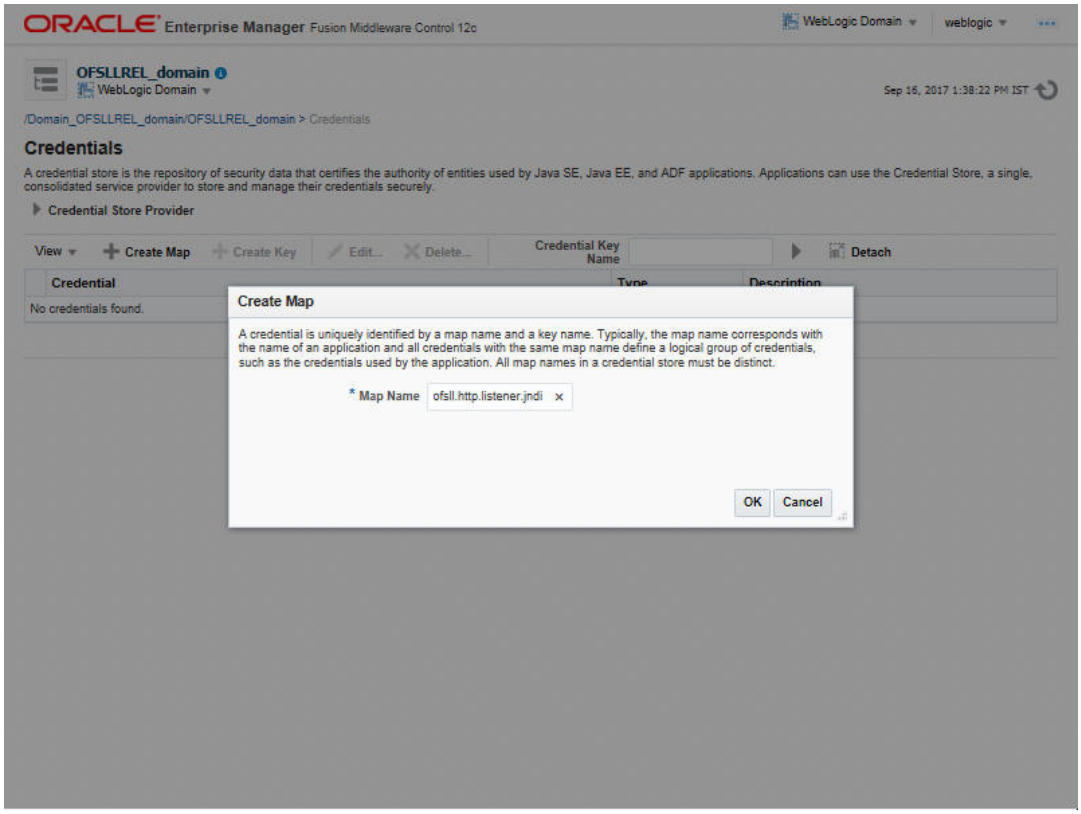
Figure 7-2 JNDI for HTTP Listener 2



3. Click **Create Map**.

   The following window is displayed.

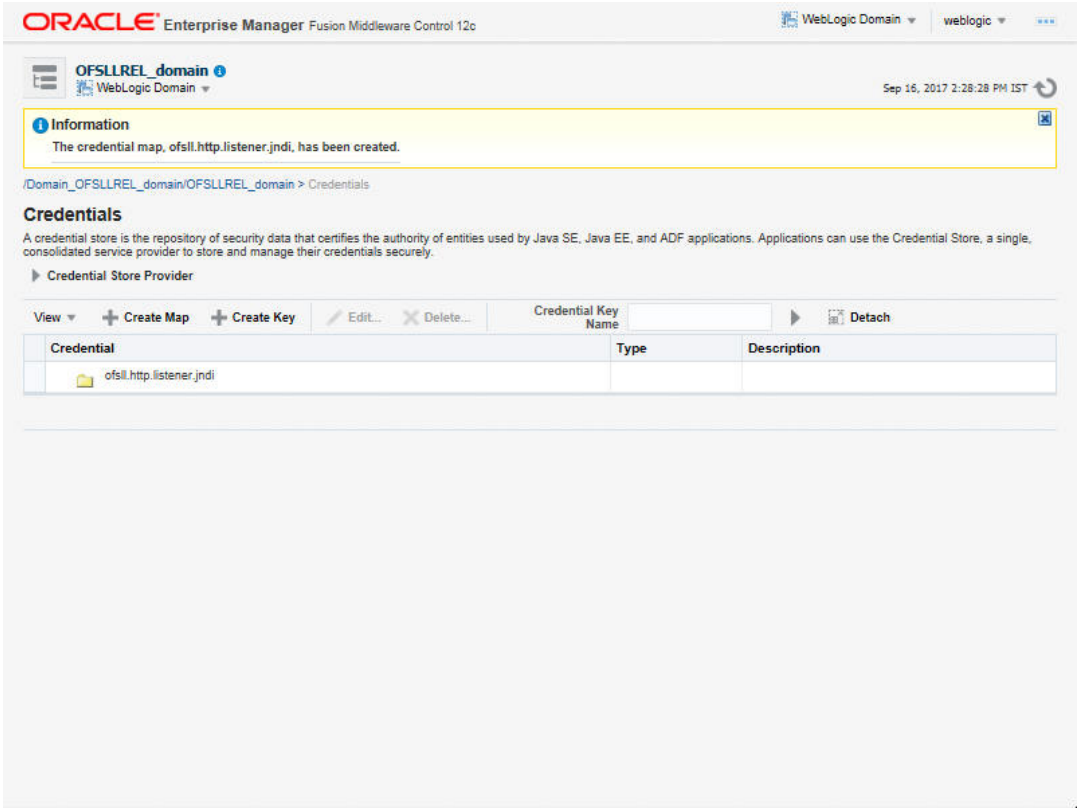
Figure 7-3 JNDI for HTTP Listener 3



4. Enter Map name as **ofsll.http.listener.jndi**.
5. Click **OK**.

   The following window is displayed.

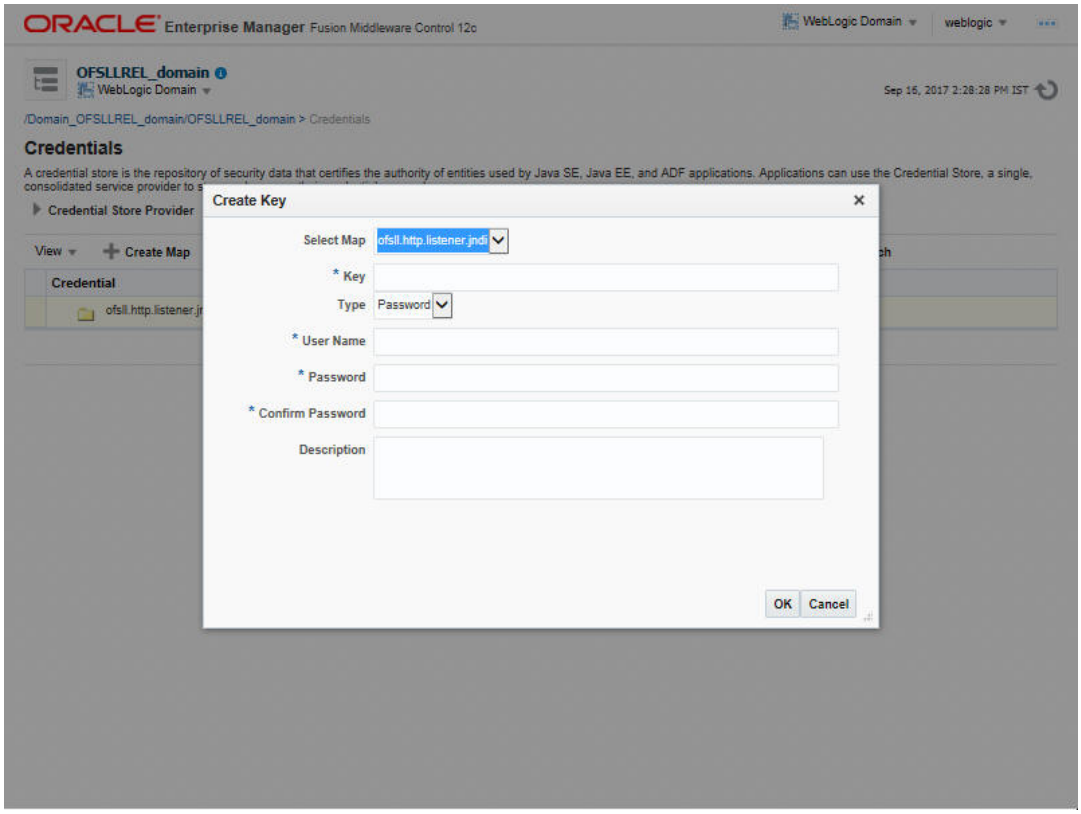
Figure 7-4 JNDI for HTTP Listener 4



6. Click **Create Key** Button.

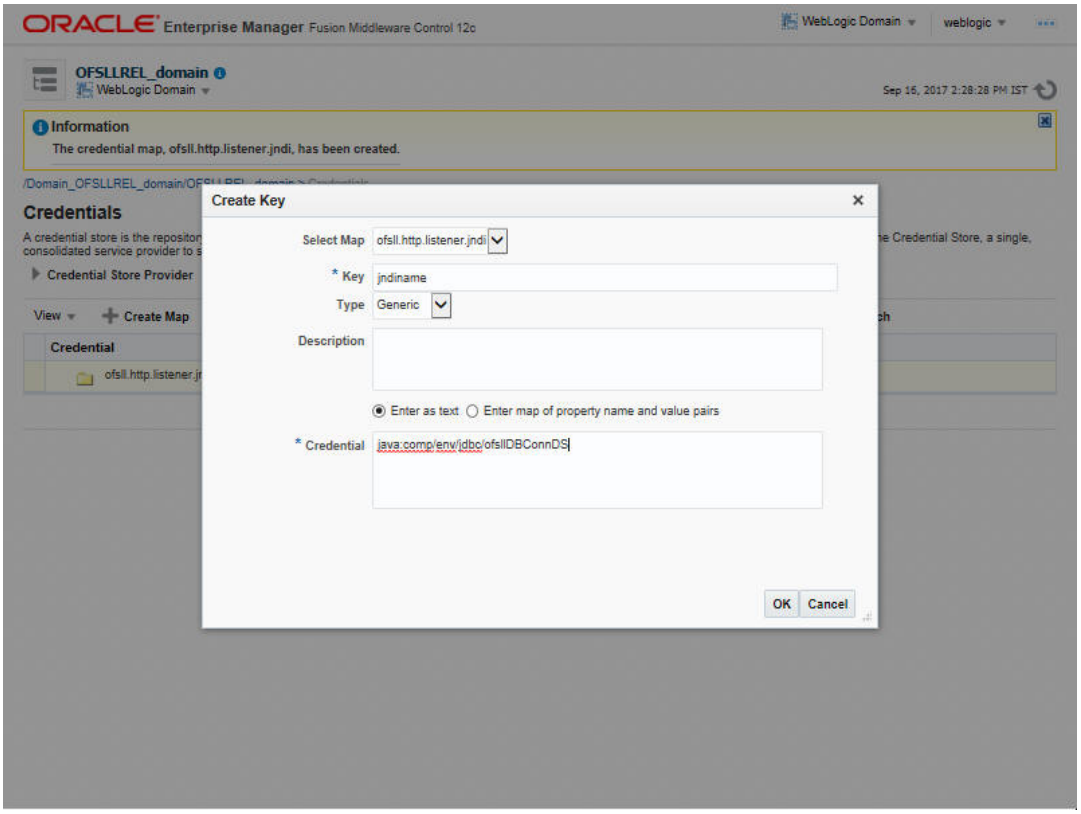
   The following window is displayed.

Figure 7-5 JNDI for HTTP Listener 5



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

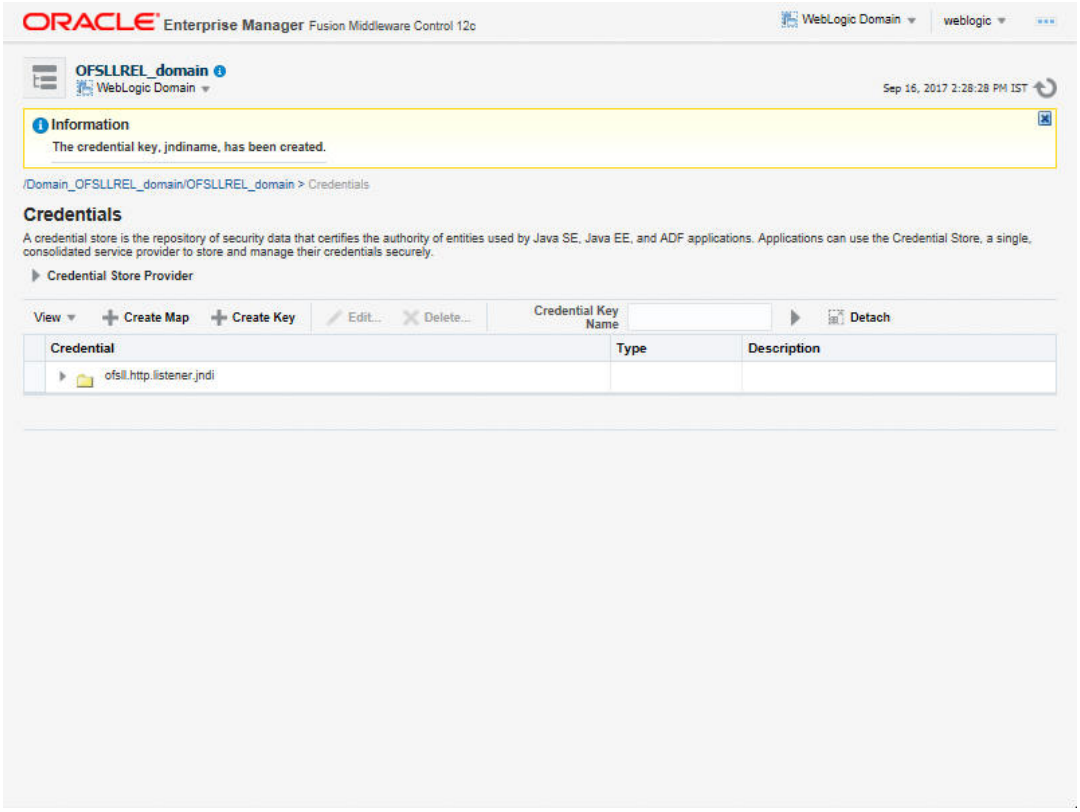
Figure 7-6 JNDI for HTTP Listener 6



8. Click **OK**.

   The following window is displayed.

Figure 7-7 JNDI for HTTP Listener 7



8
Configure JMS Queue

The following steps are to be performed to configure the JMS Queue through the Weblogic Console:

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

8.1 Create Data Sources for JMS Queue

Follow the below steps to create data sources for JMS queue.

- Create Data Sources for JMS Queue

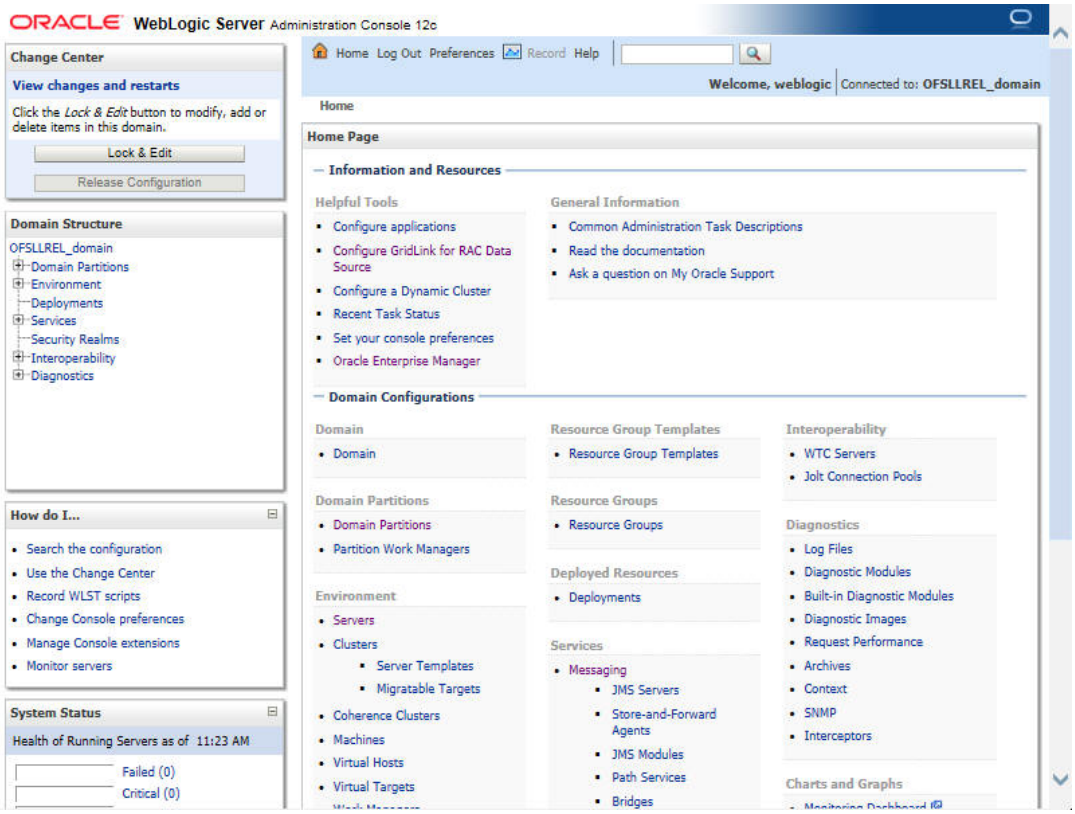
8.1.1 Create Data Sources for JMS Queue

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

Figure 8-1 Data Sources for JMS Queue 1

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

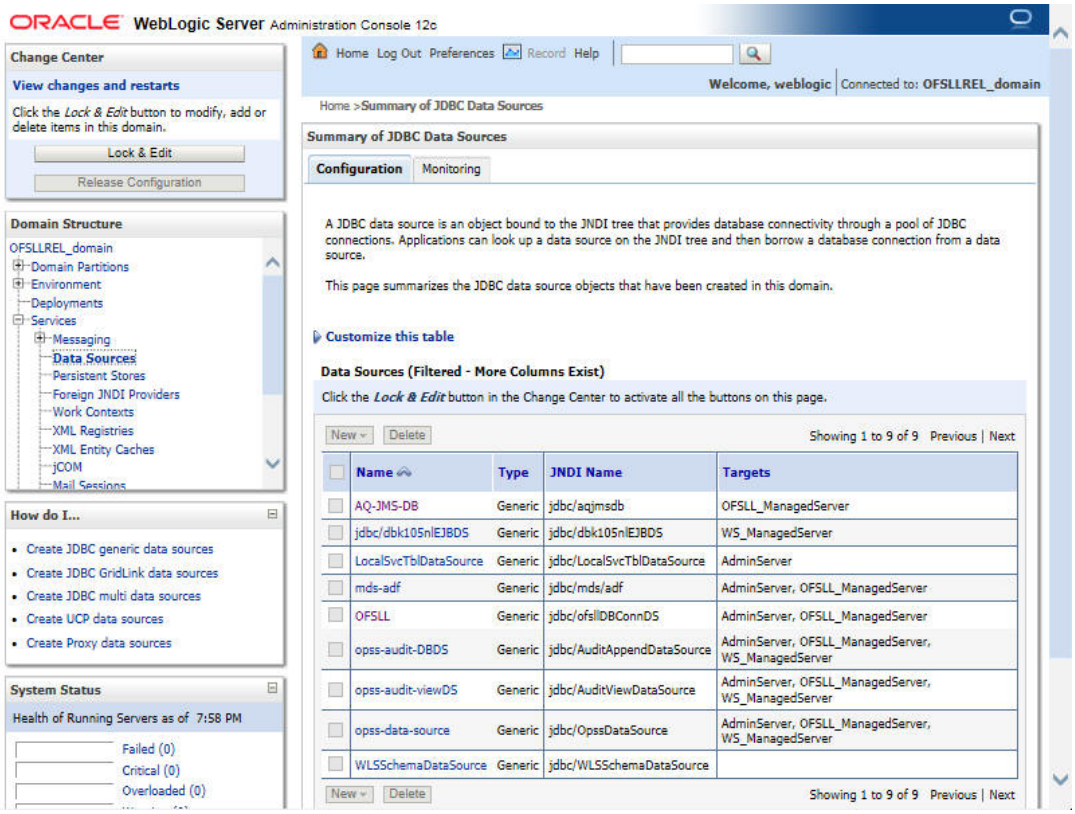
Figure 8-2 Data Sources for JMS Queue 2



3. Click Domain Name > Services > Data Sources.

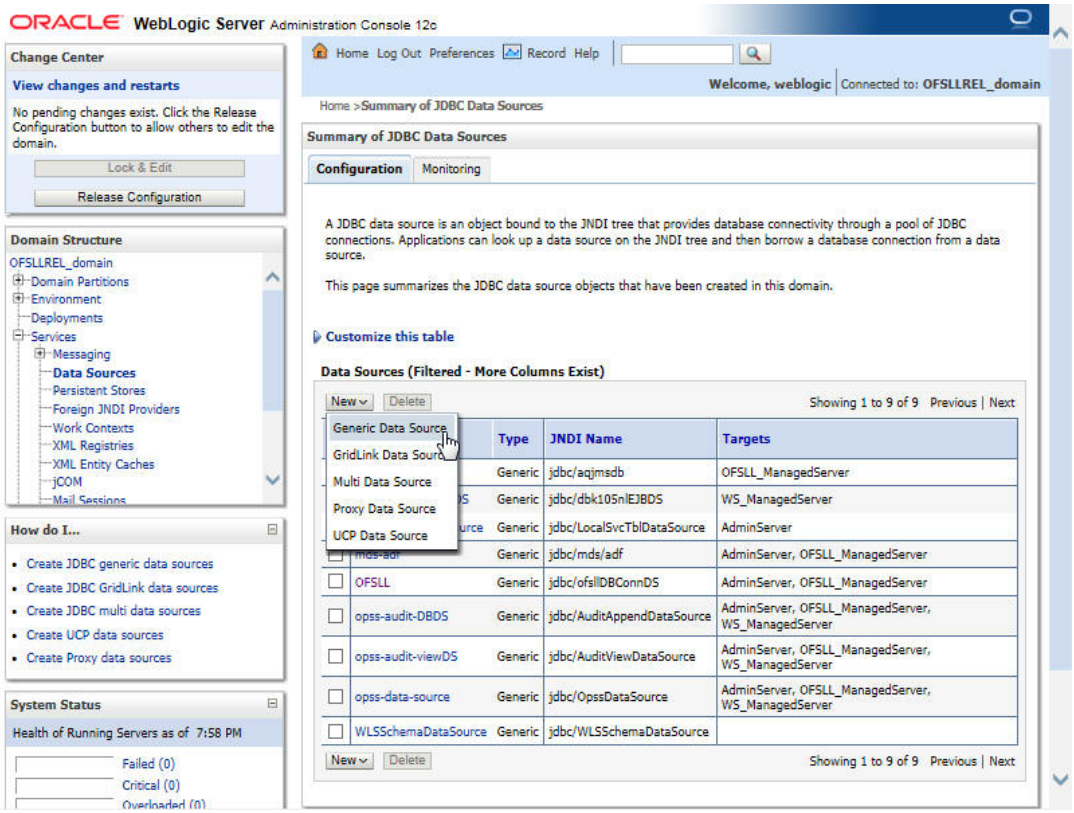
   The following window is displayed.

Figure 8-3 Data Sources for JMS Queue 3



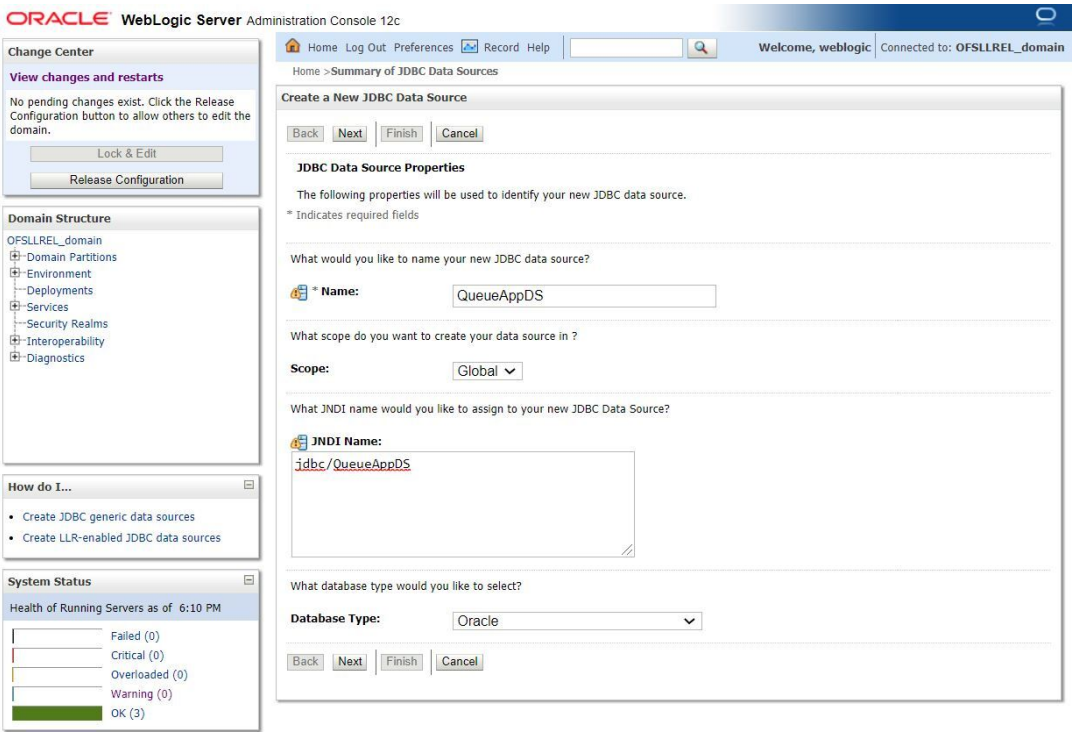
4. Click **Lock & Edit** button on the left panel. Click **New** on right panel and select **Generic Data Source**.

Figure 8-4 Data Sources for JMS Queue 4



5. The following window is displayed.

Figure 8-5 Data Sources for JMS Queue 5



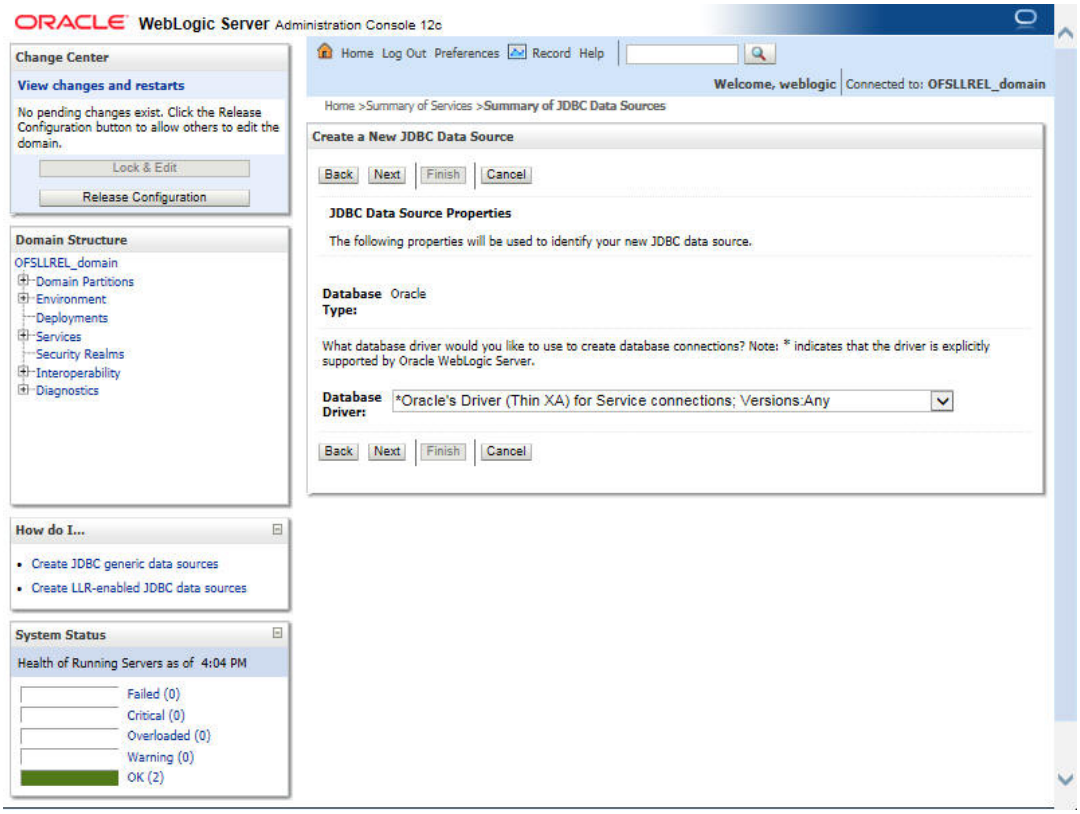
6. Specify the following details:
   - Enter Data source Name: **QueueAppDS**
   - Enter the JNDI Name as **jdbc/QueueAppDS**.

   > **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.

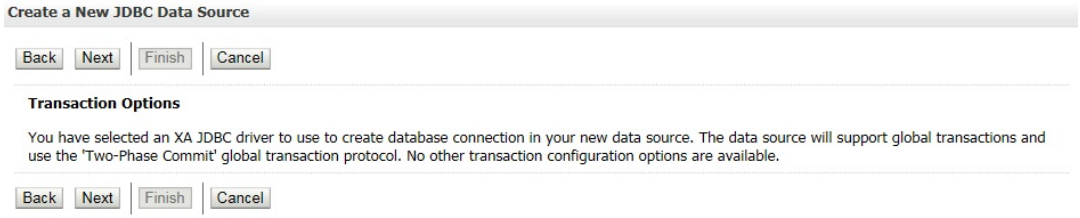
Figure 8-6 Data Sources for JMS Queue 6



8. Select the Database Driver **Oracle's Driver(Thin XA) for Services connections;Versions:Any**.
9. Click **Next**.

   The following window is displayed.

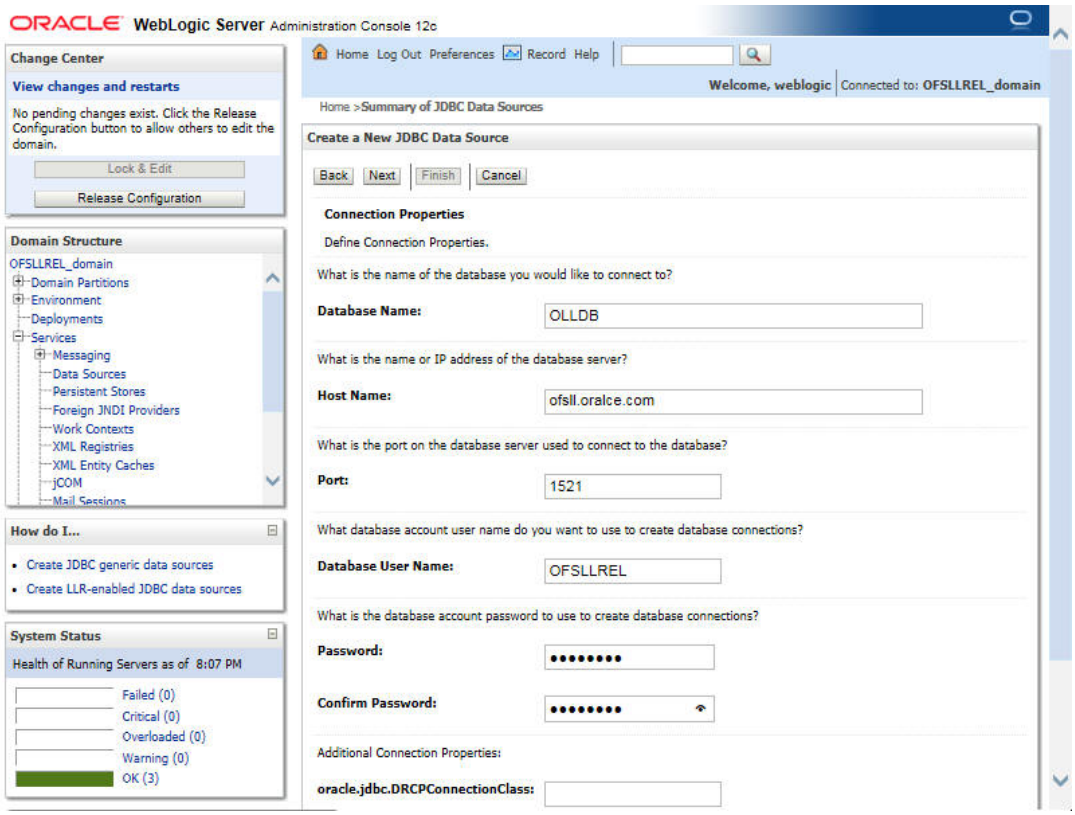
Figure 8-7 Data Sources for JMS Queue 7



10. Click **Next**.

    The following window is displayed.

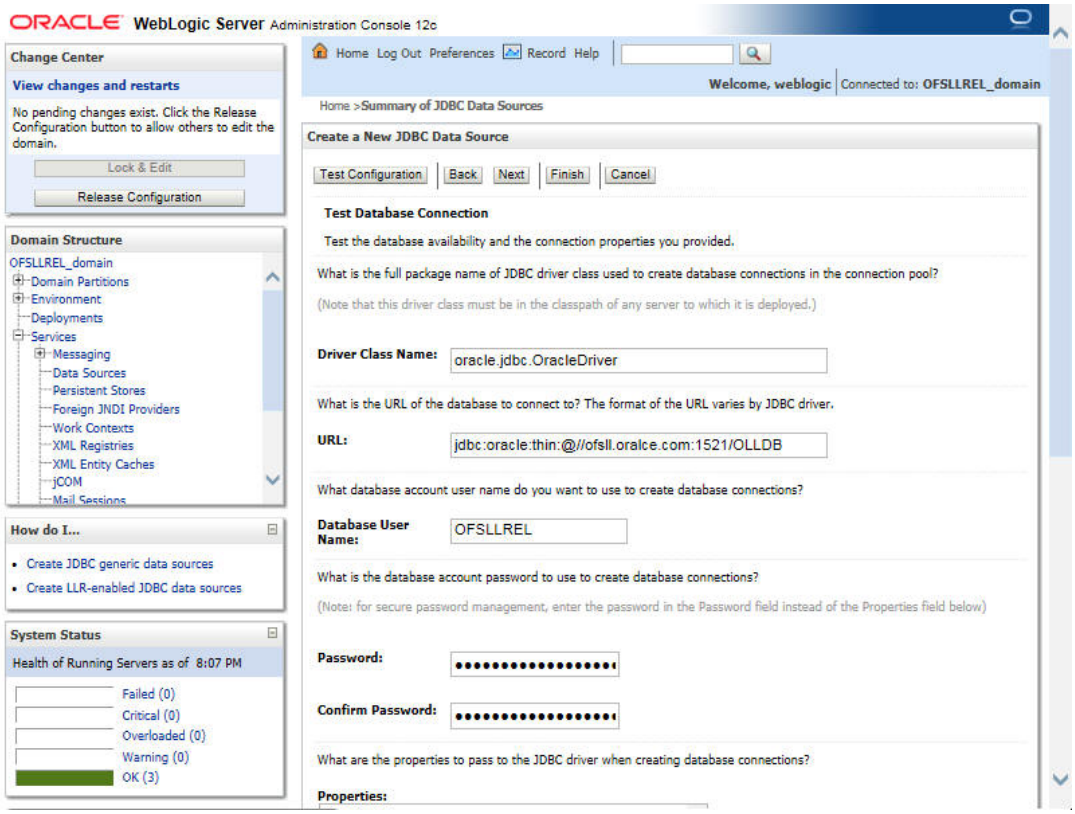
Figure 8-8 Data Sources for JMS Queue 8



11. Enter the Database details.
12. Click **Next**.

    The following window is displayed.

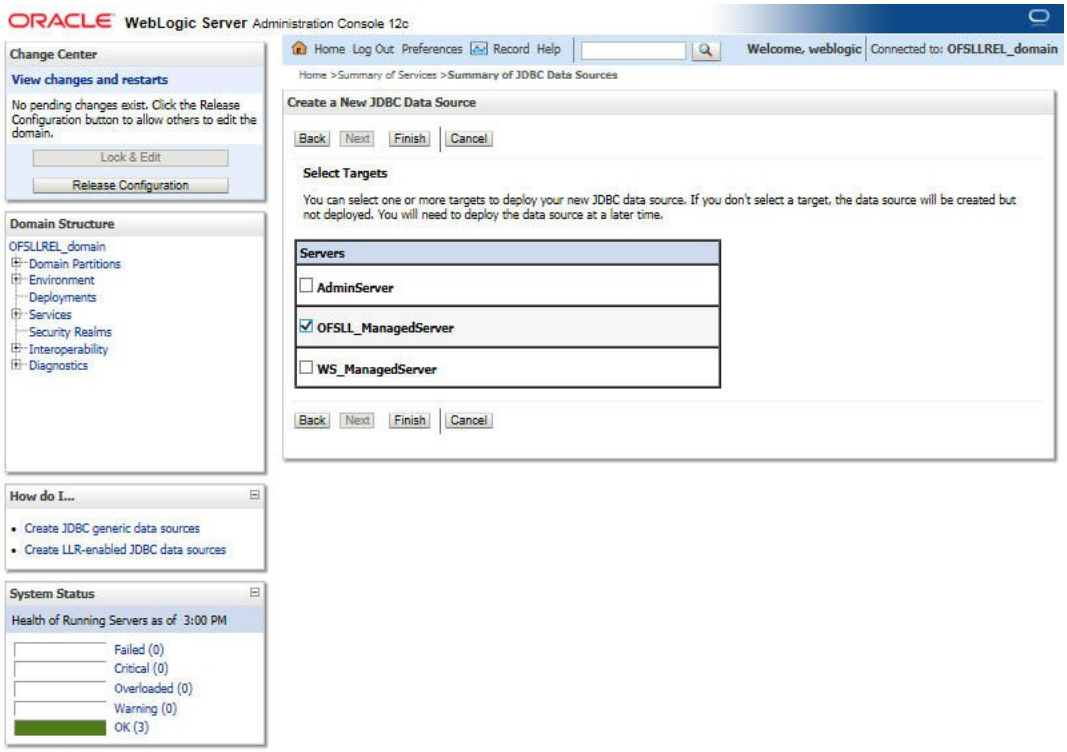
Figure 8-9 Data Sources for JMS Queue 9



13. Click **Test Configuration**. On completion, displays a confirmation message as **Connection test succeeded**.
14. Click **Next**.

    The following window is displayed.

Figure 8-10 Data Sources for JMS Queue 10



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

Update the following parameters in JDBC data source connection pool:

1. Select Services > Data Sources > select the QueueAppDS 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. To Enable GRI (Generic Recovery Interface) CLOB logging from MDB to DB, click **Advanced button** and deselect the **Wrap Data Types** check box.
4. Click **Advanced button** and update the **Inactive Connection Timeout** to 300 seconds.
5. Click **Save** and restart the Data source.

8.2 AQ-JMS Queue Configuration

AQ-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 AQ-JMS queue in application server.

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

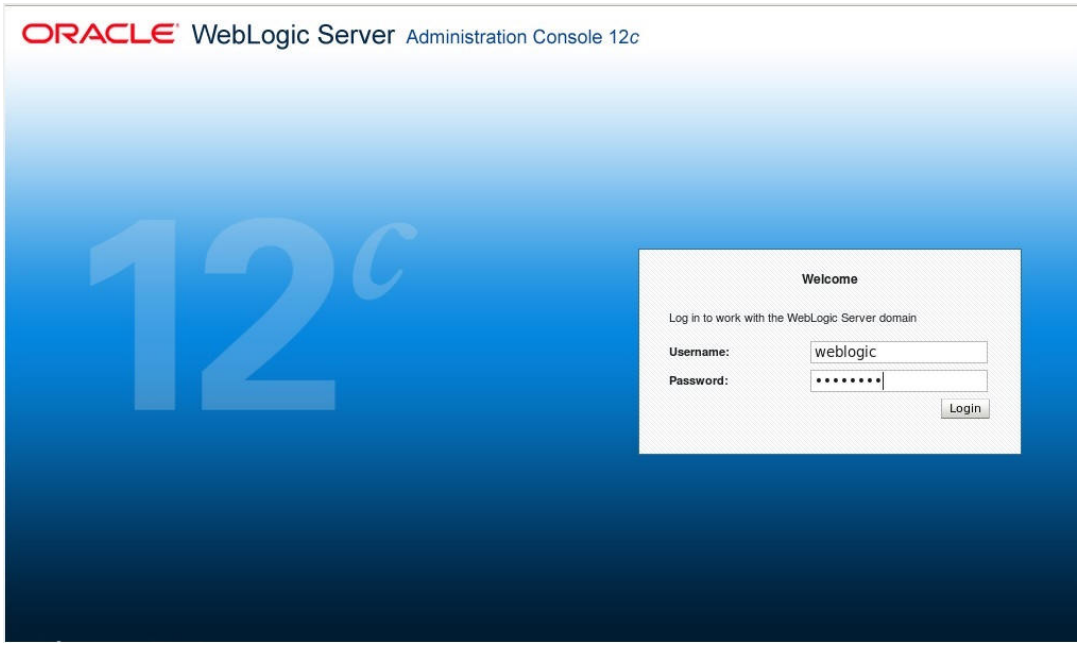
8.2.1 Create JMS Server

Follow the below steps to create JMS server.

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

   The following screen is displayed.

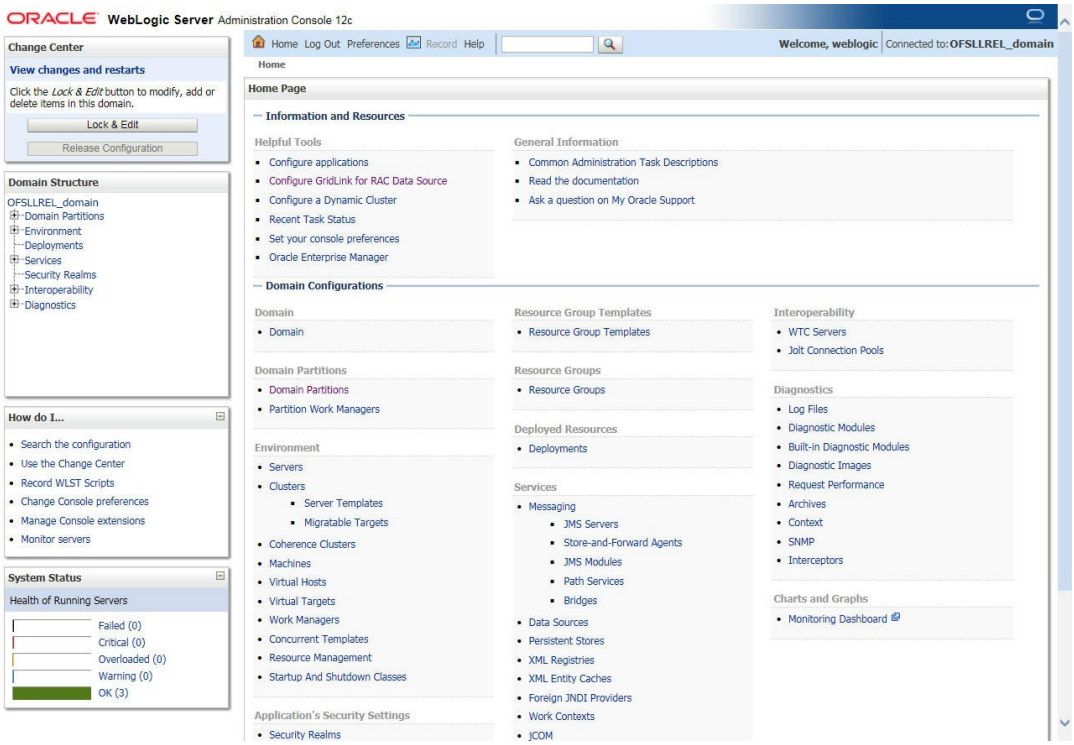
Figure 8-11 Create JMS Server 1



2. Specify the Weblogic administrator user name and password and click **Log In**.

   The Oracle Weblogic home page is displayed.

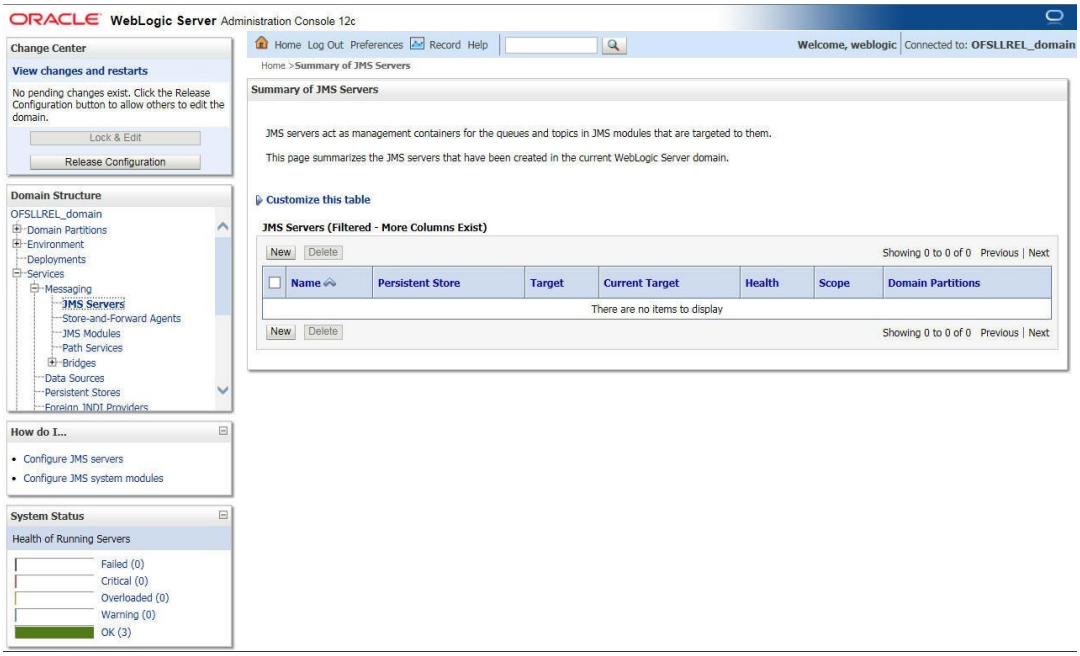
Figure 8-12 Create JMS Server 2



3. Click Domain Name > Services > Messaging > JMS Server.
4. In the main window, click **Lock & Edit**.

   The following window is displayed.

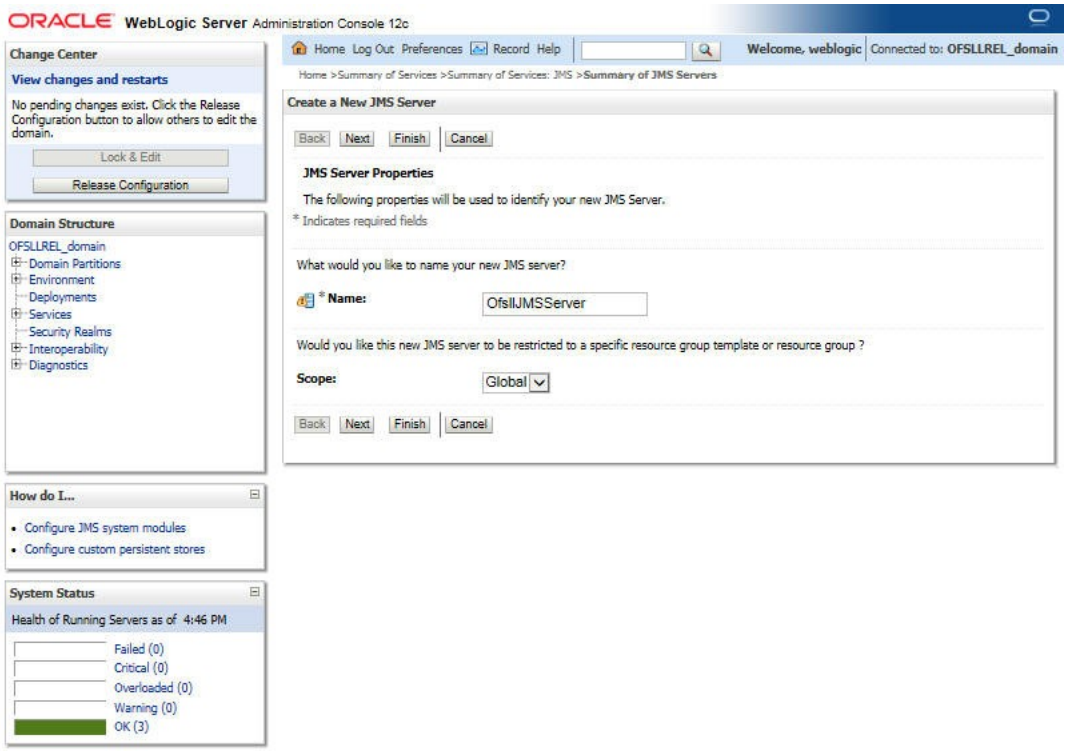
Figure 8-13 Create JMS Server 3



5. Click **New**.

   The following window is displayed.

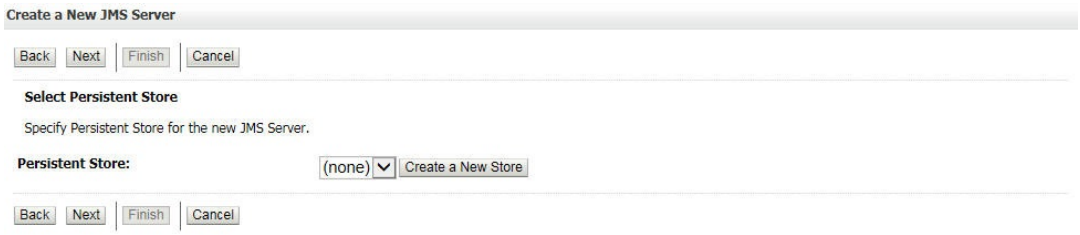
Figure 8-14 Create JMS Server 4



6. Specify the JMS Server Name as **OfsllJMSServer**. Click Next.

   The following window is displayed.

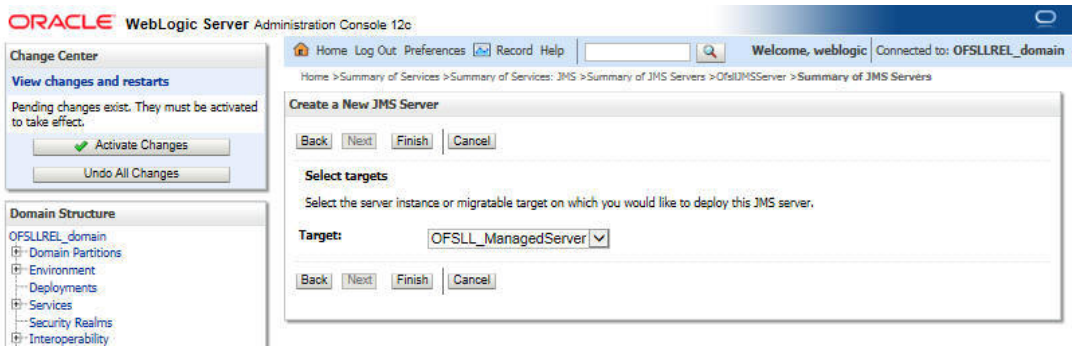
Figure 8-15 Create JMS Server 4



7. Select **None** as the Persistent Store type. Click **Next**.

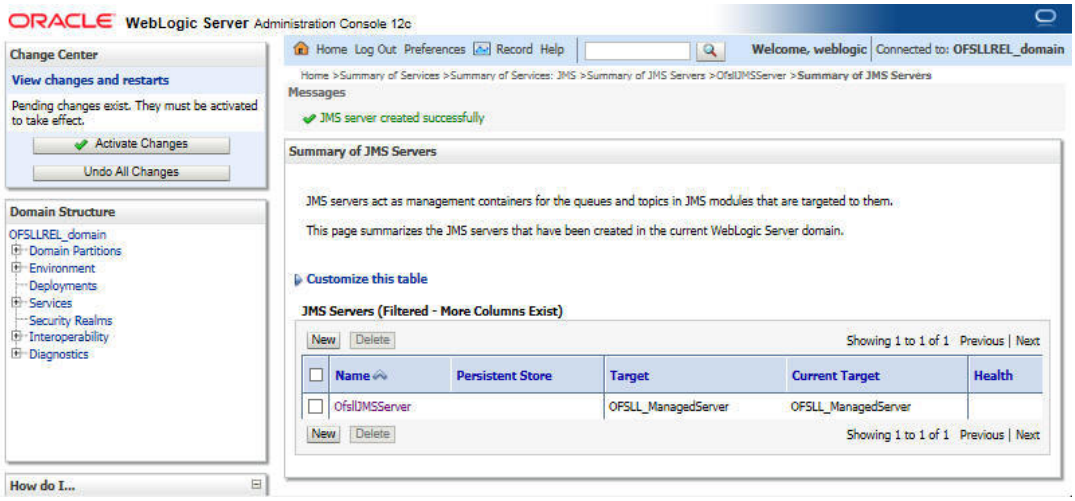
   The following window is displayed.

Figure 8-16 Create JMS Server 5



8. Select the target managed server and click **Finish**.
9. Click **Activate Changes** under Change Center. Once done, the following window is displayed:

Figure 8-17 Create JMS Server 6



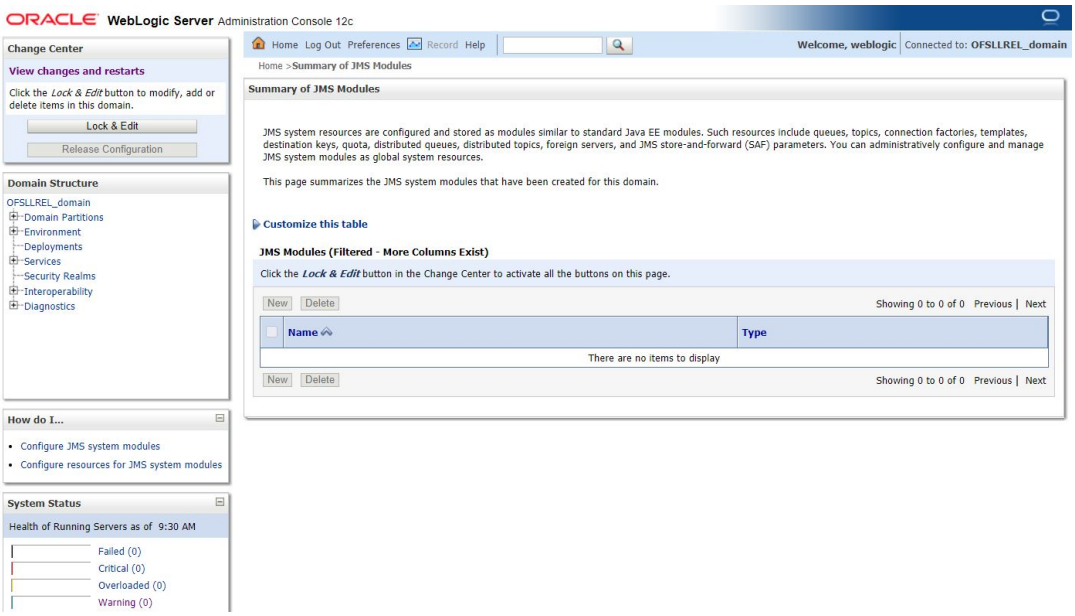
8.2.2 Create JMS Module

Follow the below steps to create JMS module.

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

   The following window is displayed.

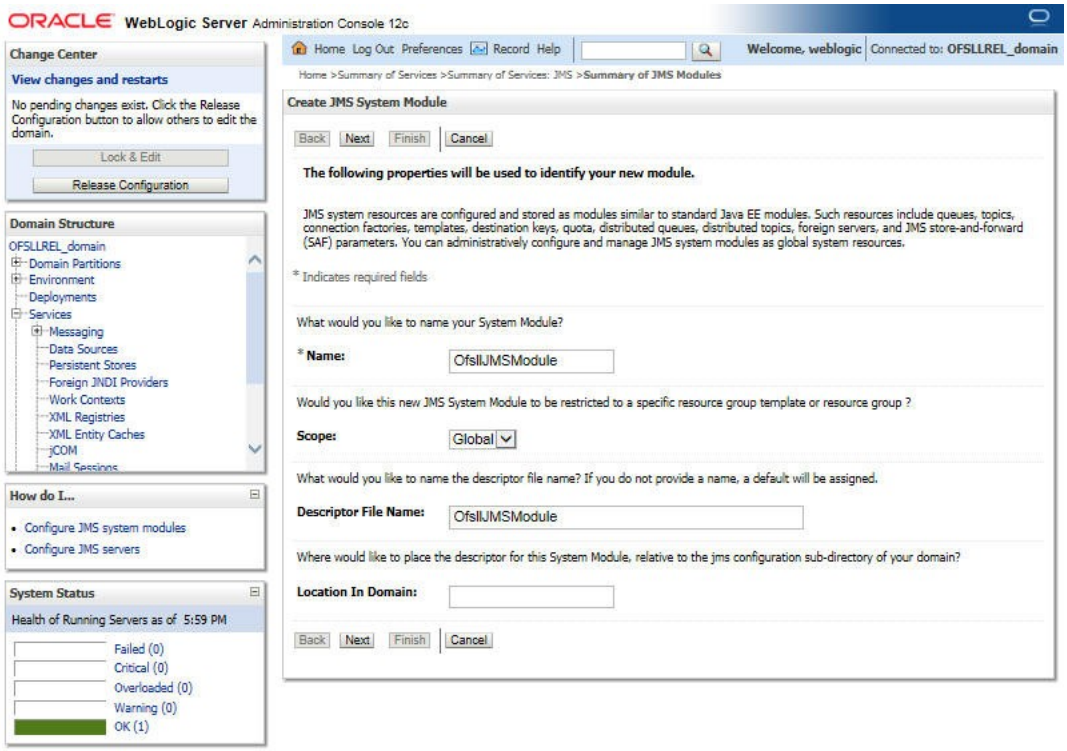
Figure 8-18 Create JMS Module 1



3. Click **New**.

   The following screen is displayed.

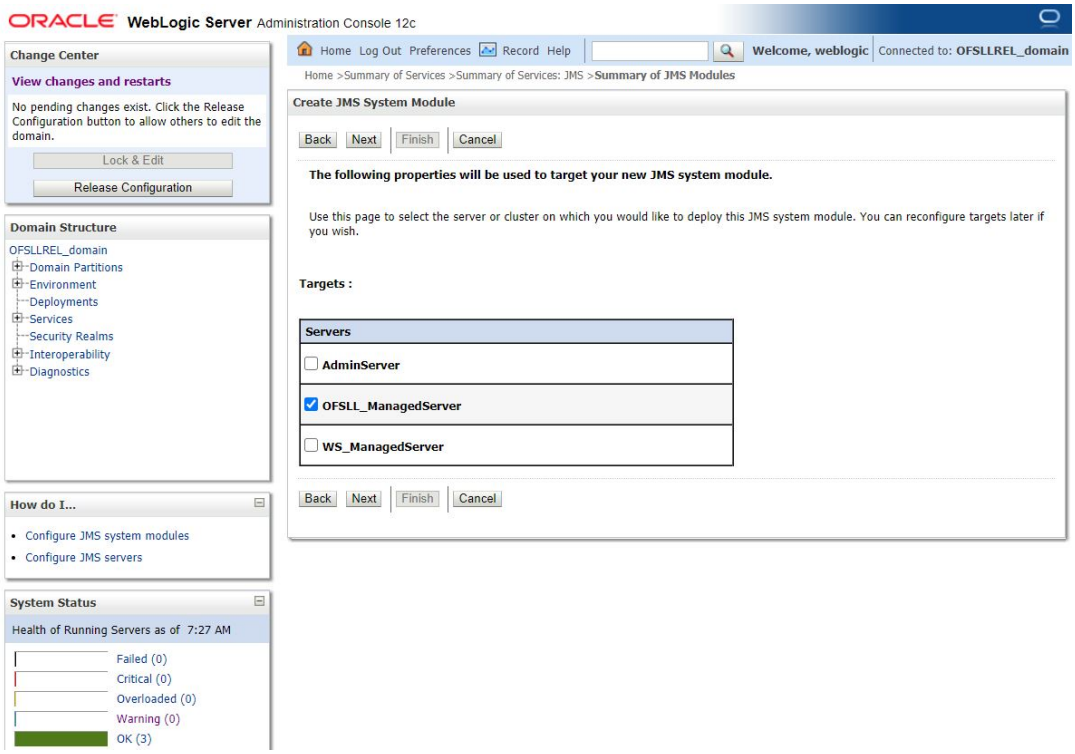
Figure 8-19 Create JMS Module 2



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.

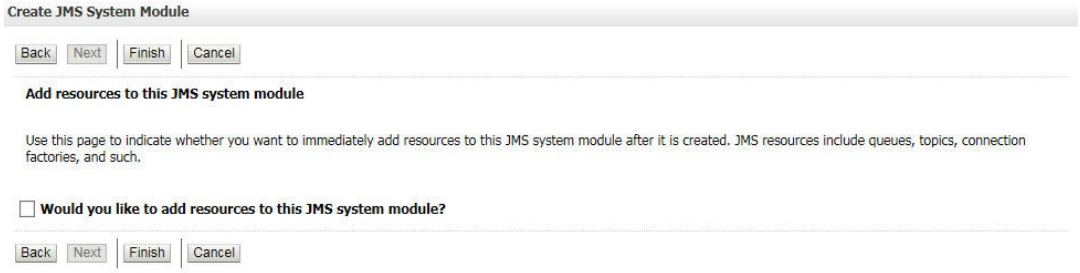
Figure 8-20 Create JMS Module 3



6. Select the target server and click **Next**.

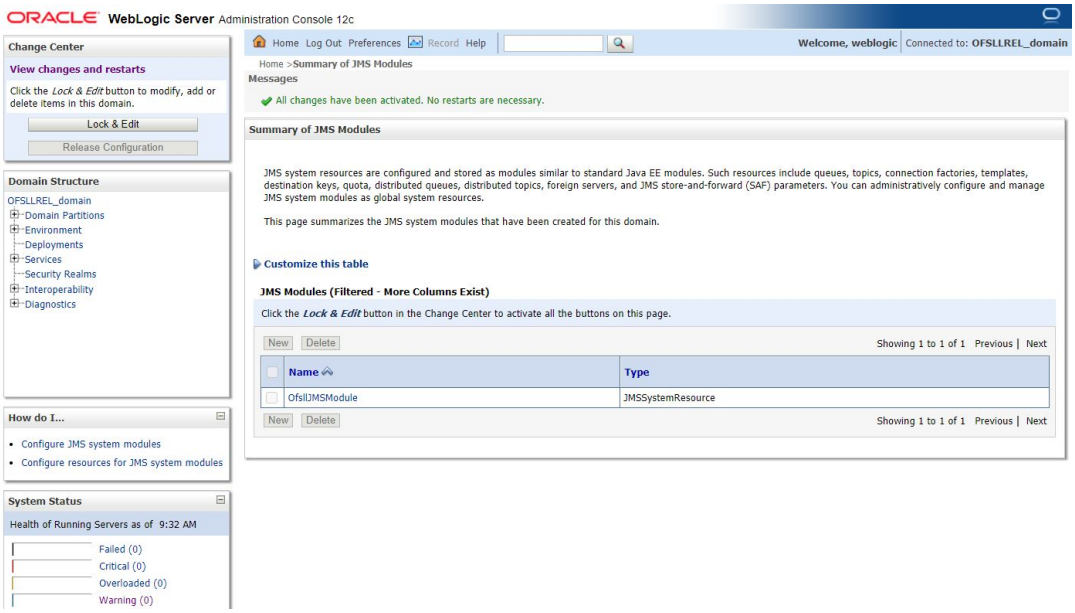
   The following window is displayed.

Figure 8-21 Create JMS Module 4



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

Figure 8-22 Create JMS Module 5



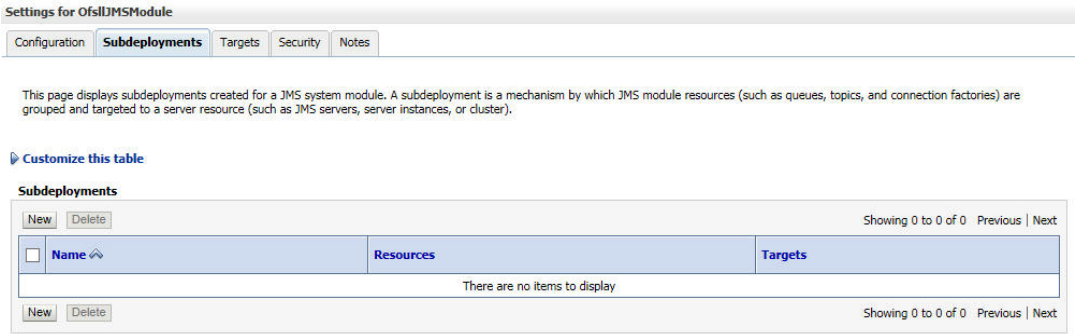
8.2.3 Subdeployment

Follow the below steps to do subdeployment.

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

   The following window is displayed.

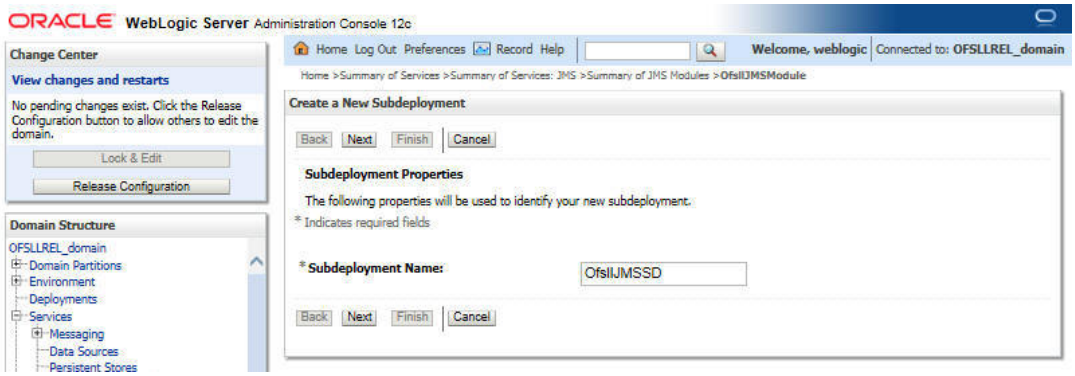
Figure 8-23 Subdeployment 1



4. Click **New**.

   The following screen is displayed.

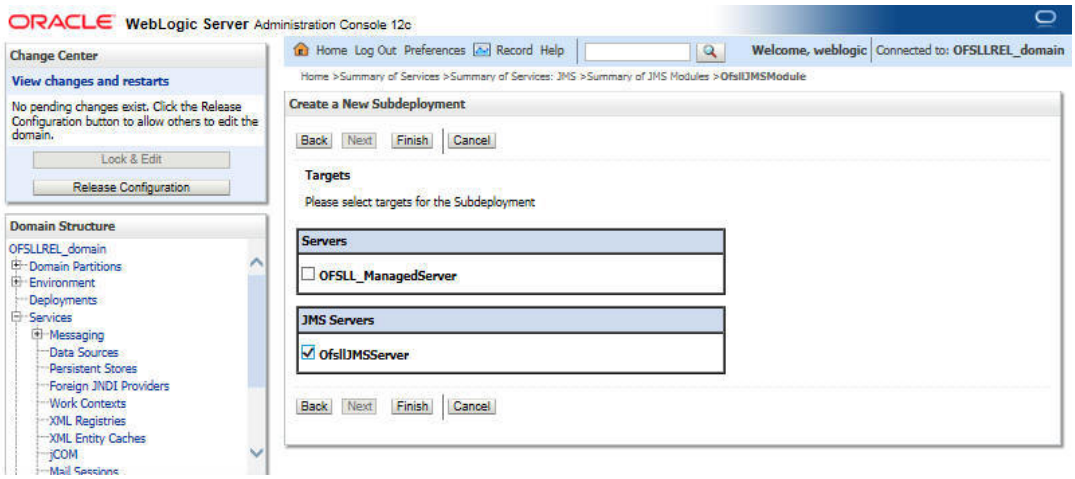
Figure 8-24 Subdeployment 2



5. Specify the Subdeployment Name as **OfsllJMSSD**. Click **Next**.

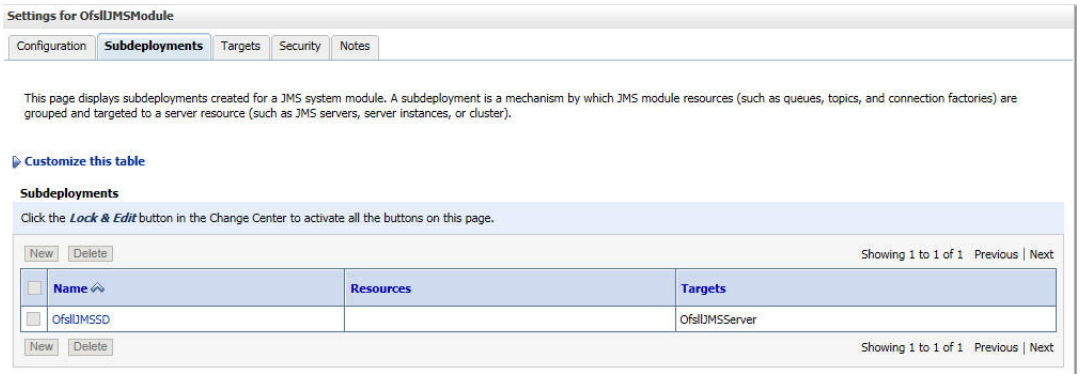
   The following window is displayed.

Figure 8-25 Subdeployment 3



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

Figure 8-26 Subdeployment 4



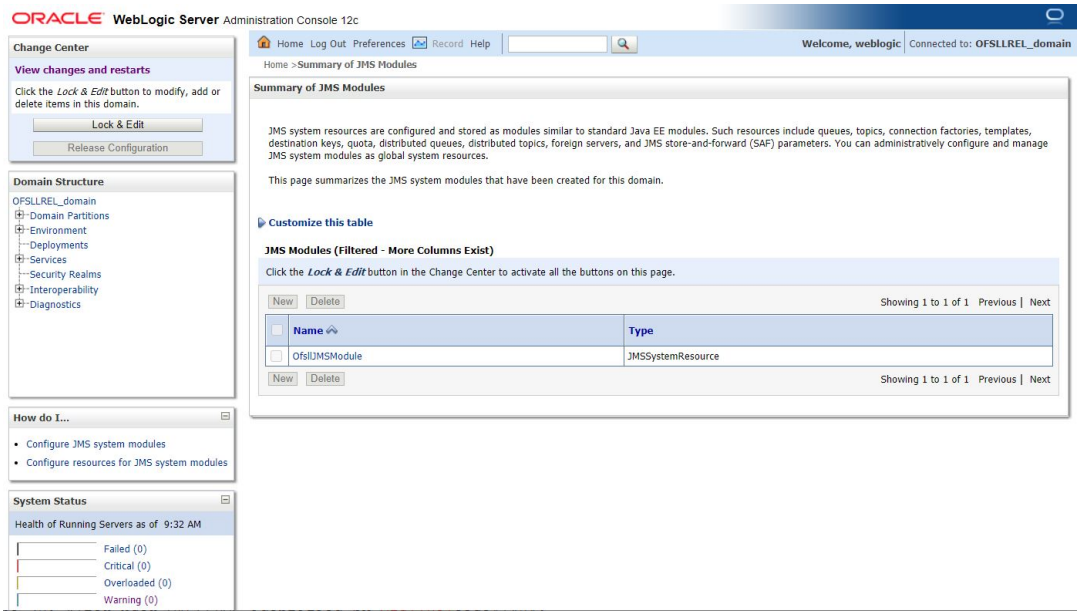
8.2.4 Create JMS Connection Factory

Follow the below steps to 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.

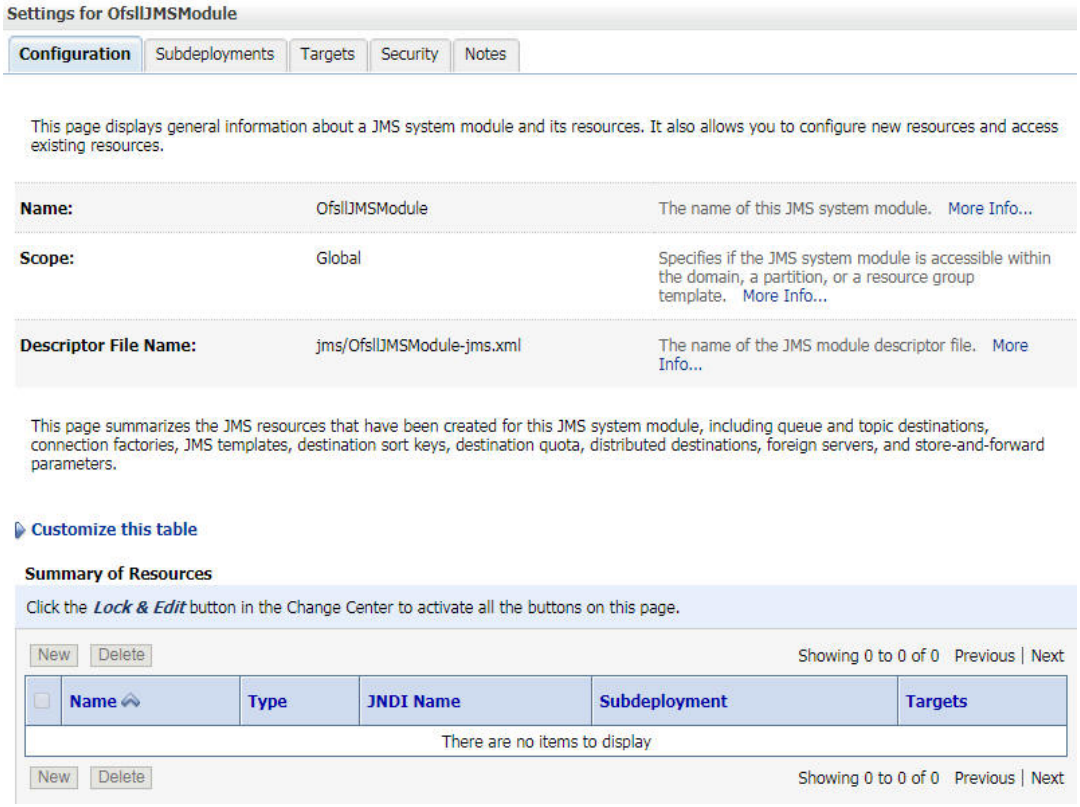
Figure 8-27 JMS Connection Factory 1



4. Click **New**.

   The following window is displayed.

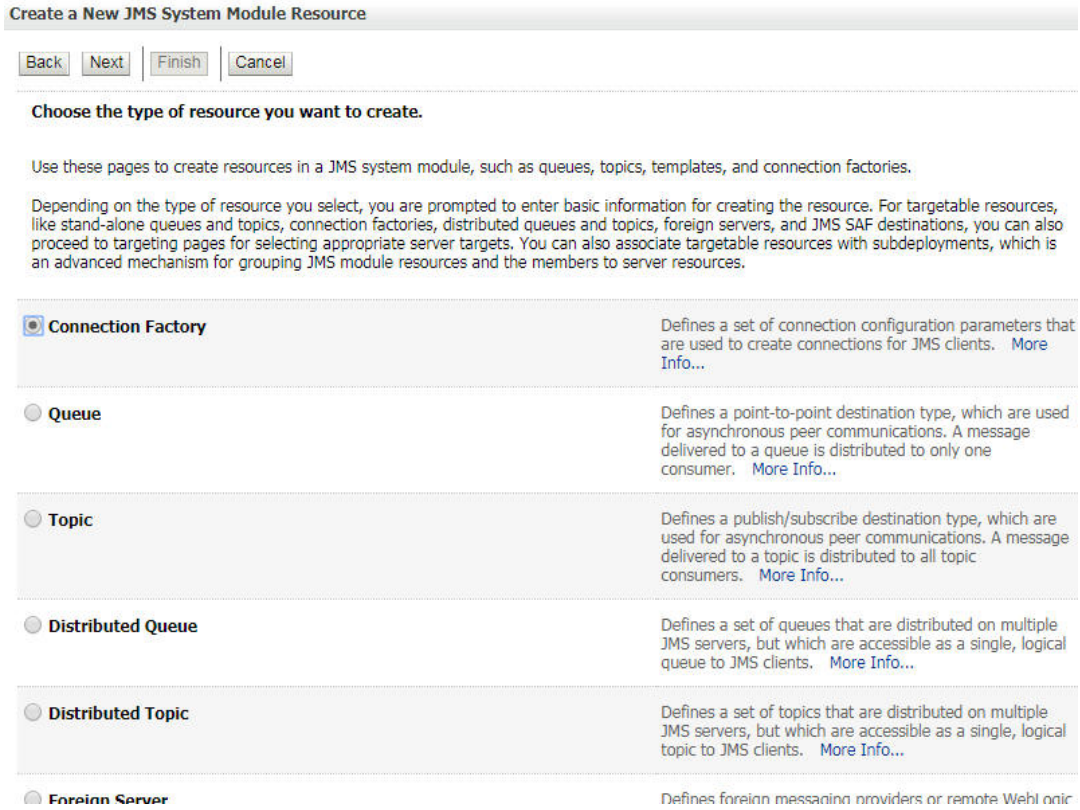
Figure 8-28 JMS Connection Factory 2



5. Click **Next**.

   The following window is displayed.

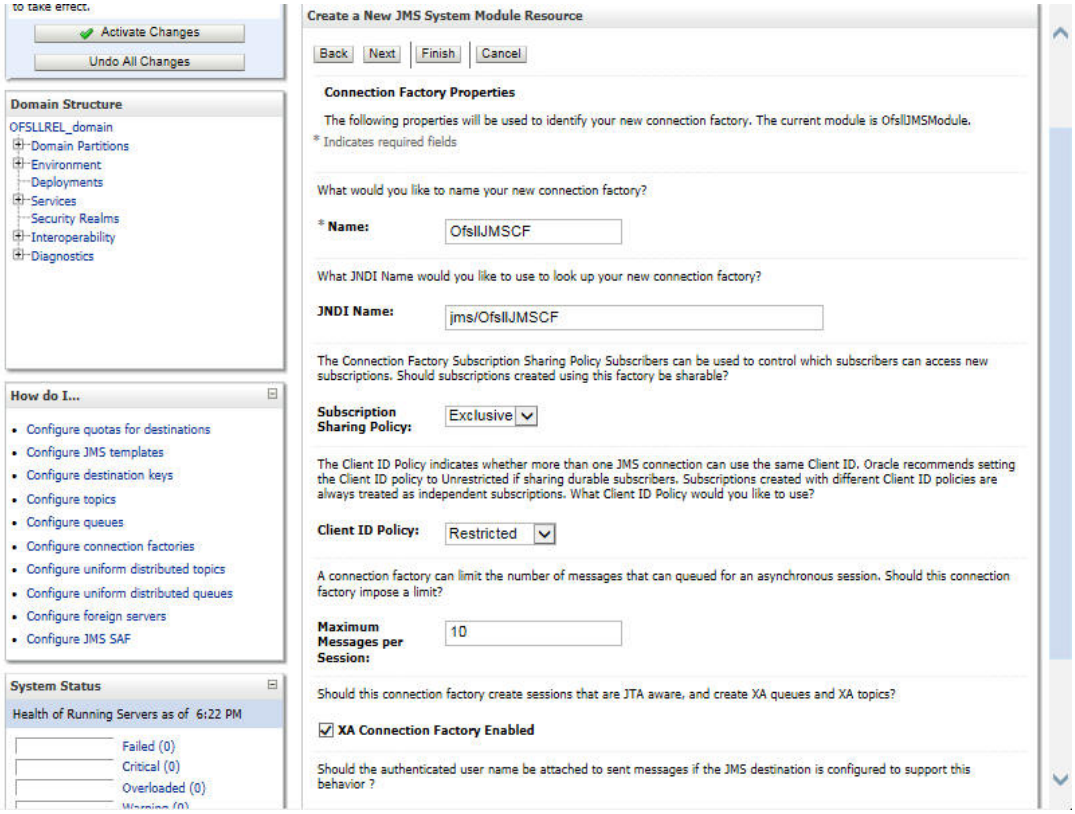
Figure 8-29 JMS Connection Factory 3



6. Select **Connection Factory** option and click **Next**.

   The following window is displayed.

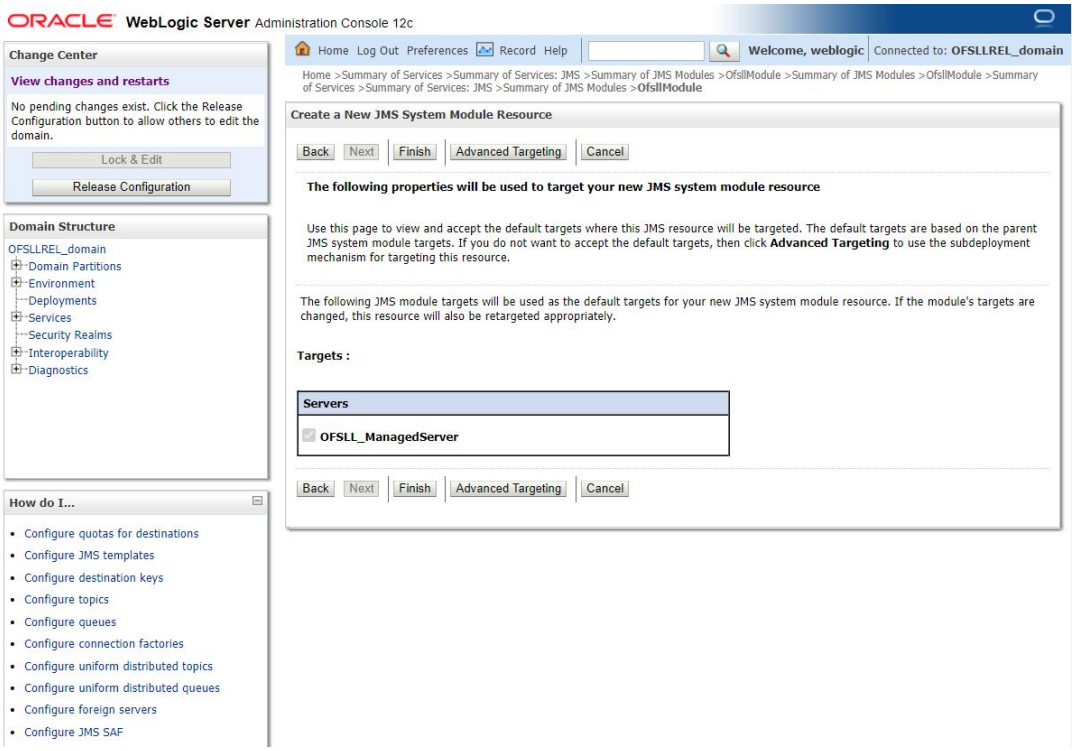
Figure 8-30 JMS Connection Factory 4



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

   The following window is displayed.

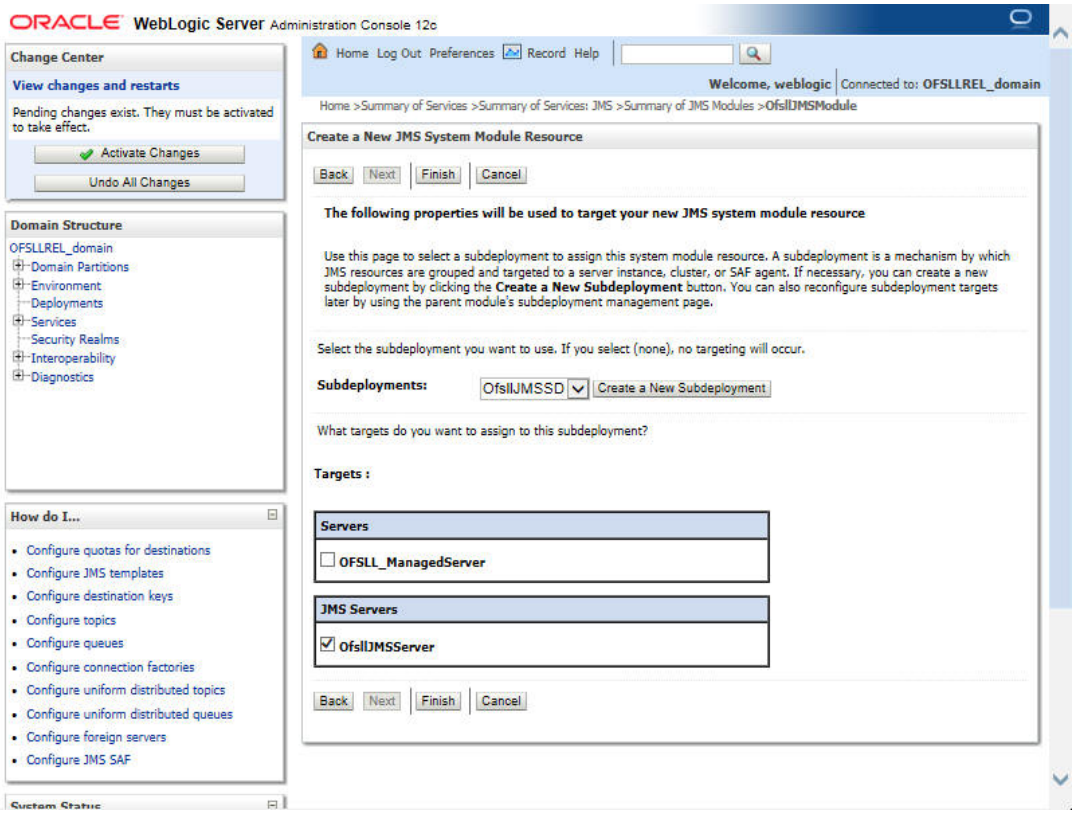
Figure 8-31 JMS Connection Factory 5



9. Click **Advanced Targeting**.

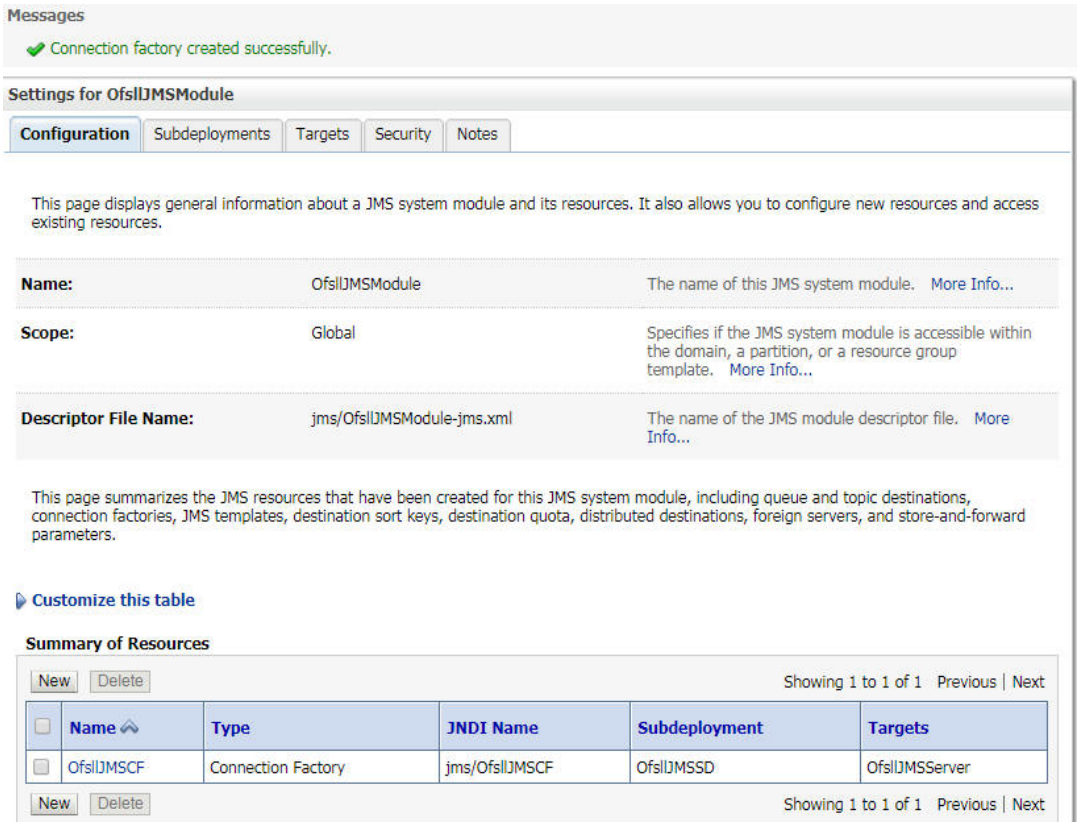
   The following window is displayed.

Figure 8-32 JMS Connection Factory 6



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

Figure 8-33 JMS Connection Factory 7



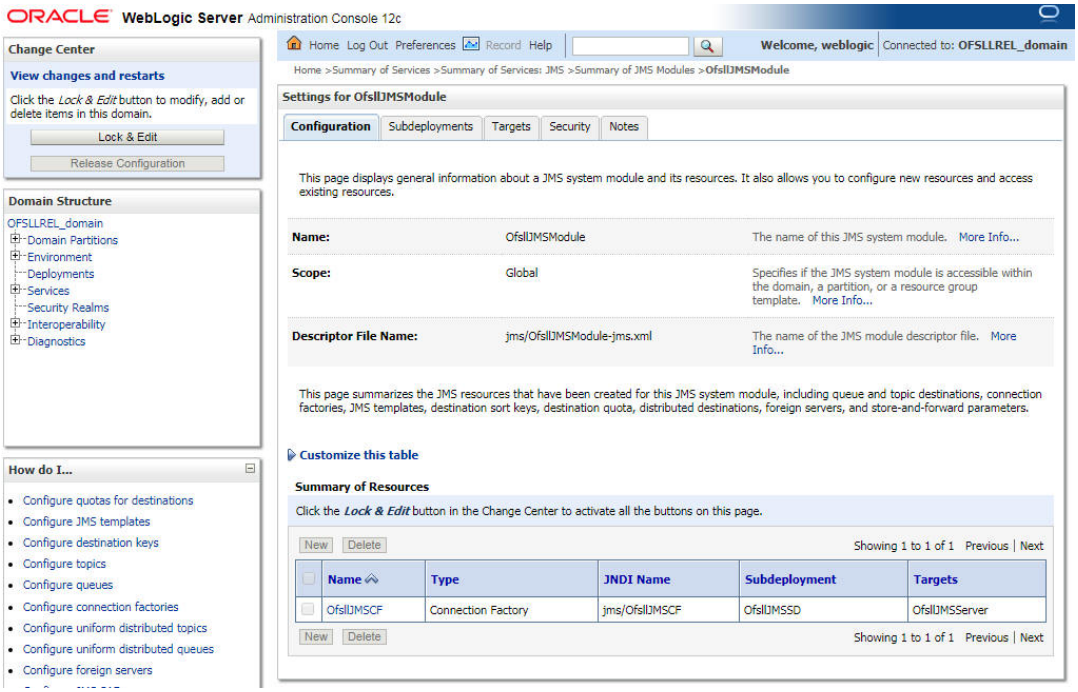
8.2.5 Create JMS Queue

Follow the below steps to create JMS queue.

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

   The following window is displayed.

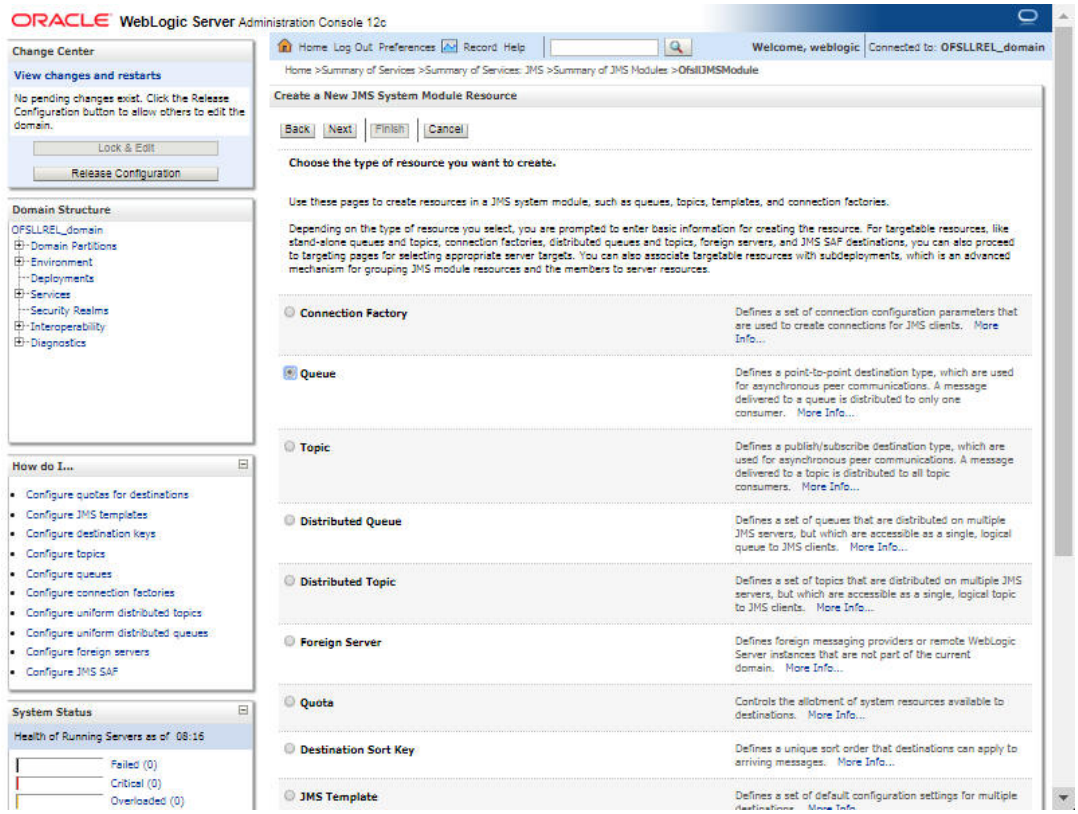
Figure 8-34 JMS Queue 1



4. Click **New**.

The following window is displayed.

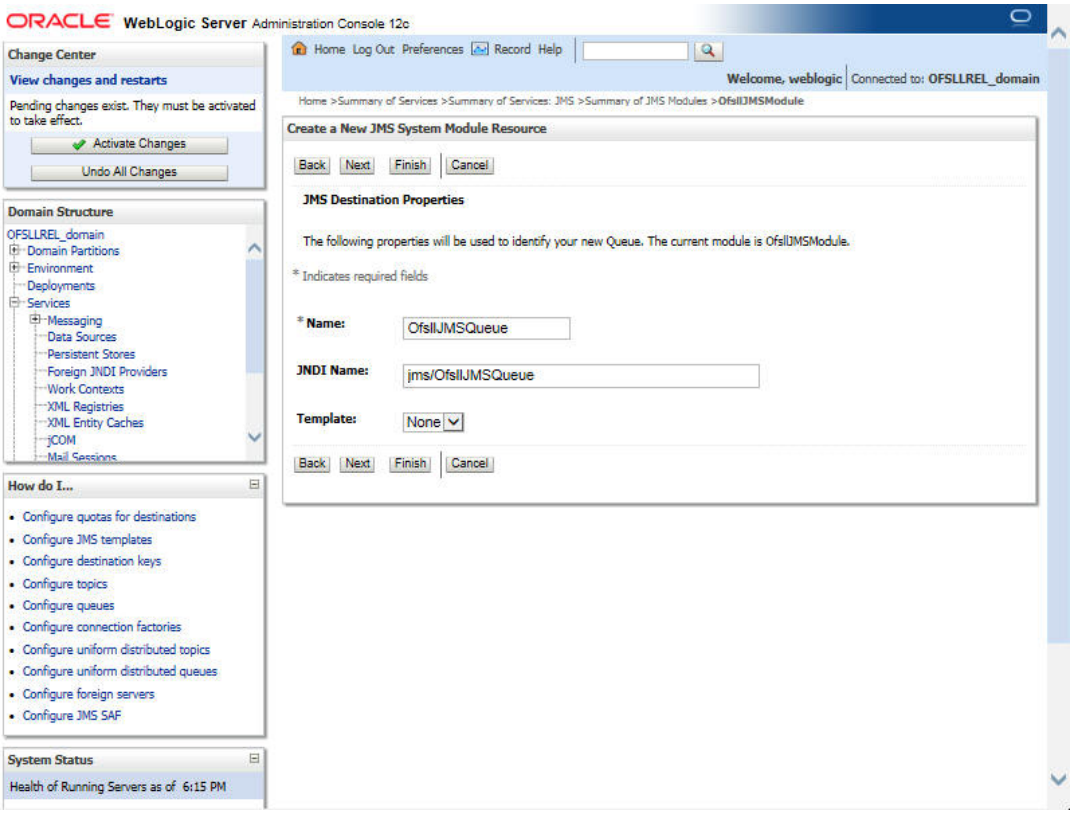
Figure 8-35 JMS Queue 2



5. Select the **Queue** option and click **Next**.

   The following window is displayed.

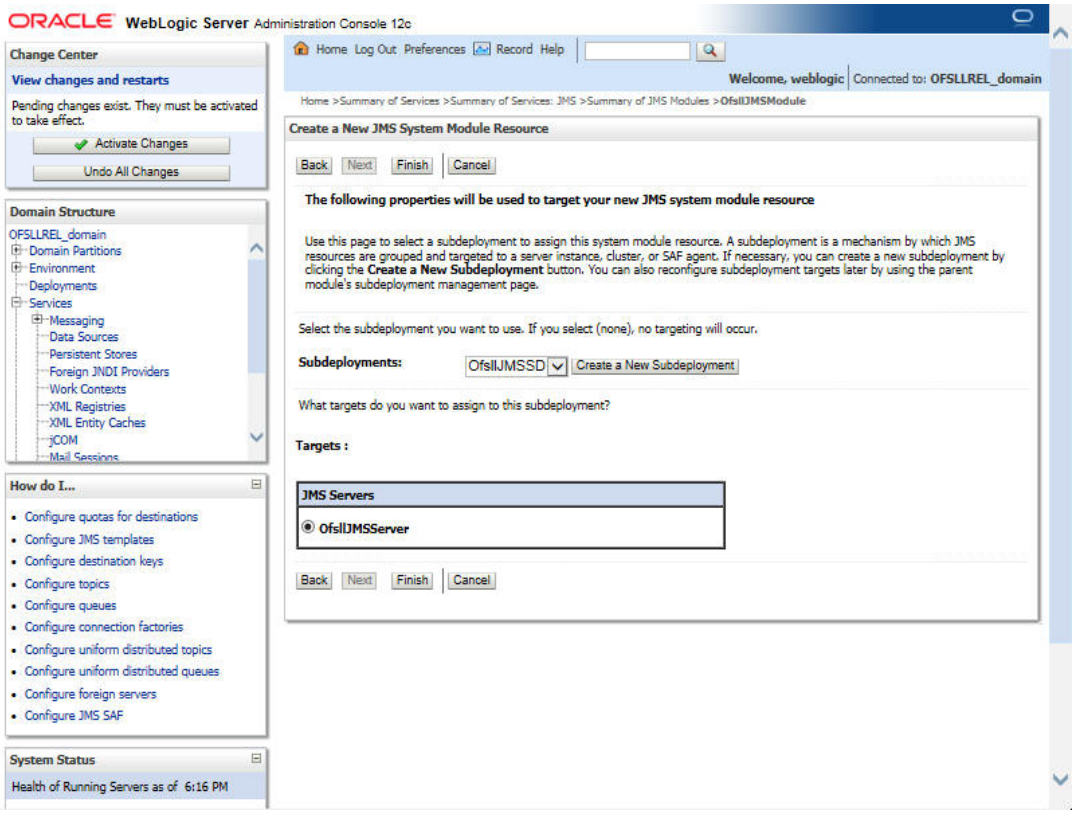
Figure 8-36 JMS Queue 3



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**.

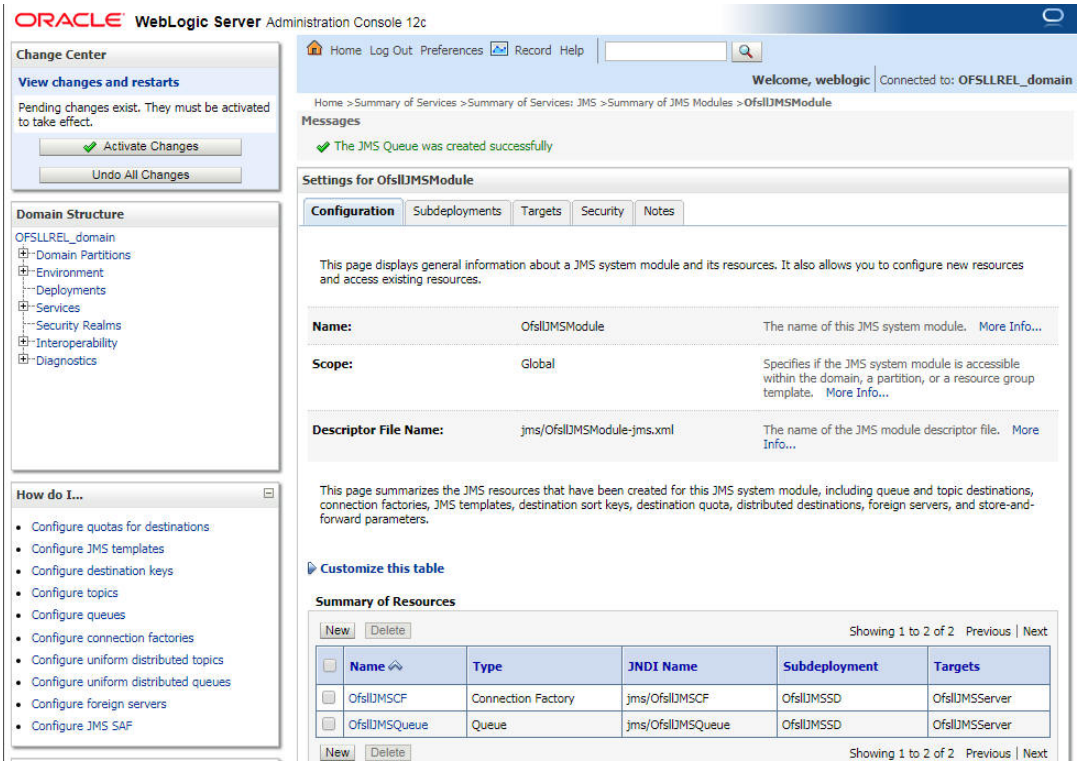
   The following window is displayed.

Figure 8-37 JMS Queue 4



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.

Figure 8-38 JMS Queue 5



8.3 Outbound Queue Configuration

Outbound Queue provides a mechanism to consume AQ messages from the database and send those messages to MDBs.

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

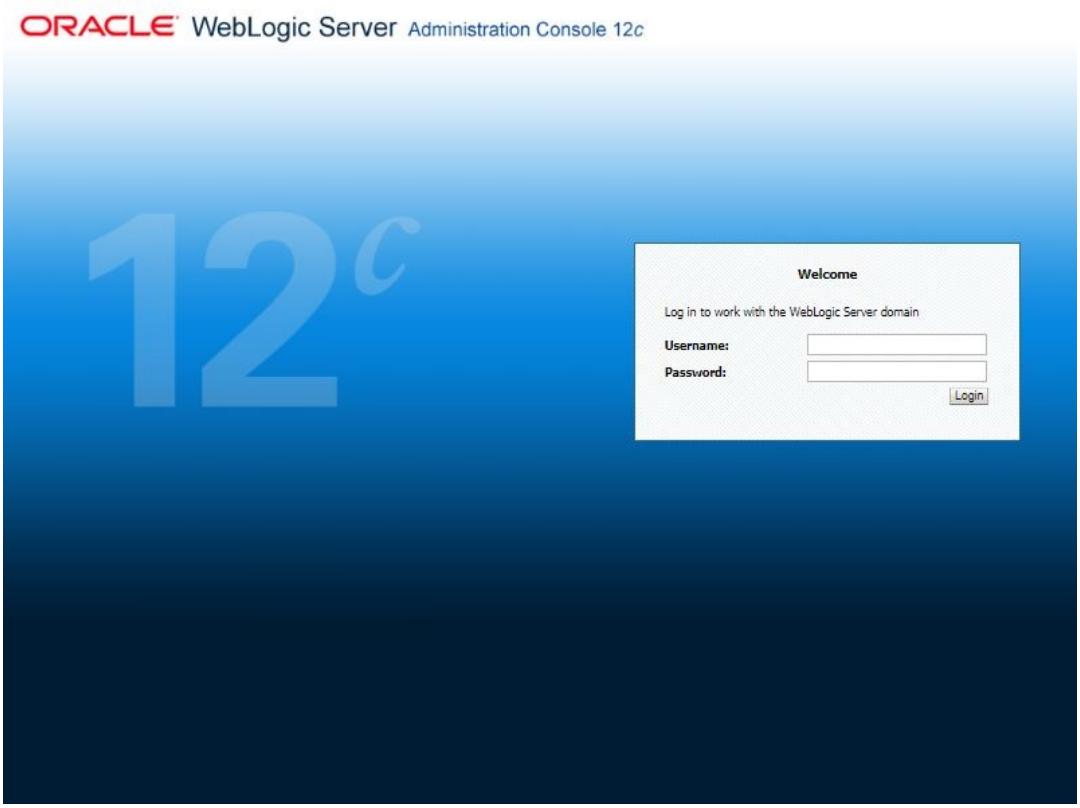
- Create Persistent Stores
- Create JMS Server for Outbound Queue
- Create JMS Module for Outbound Queue
- SubDeployment for Outbound Queue
- Create JMS Connection Factory for Outbound Queue
- Create JMS Queue for Outbound Queue

8.3.1 Create Persistent Stores

Follow the below steps to create persistent stores.

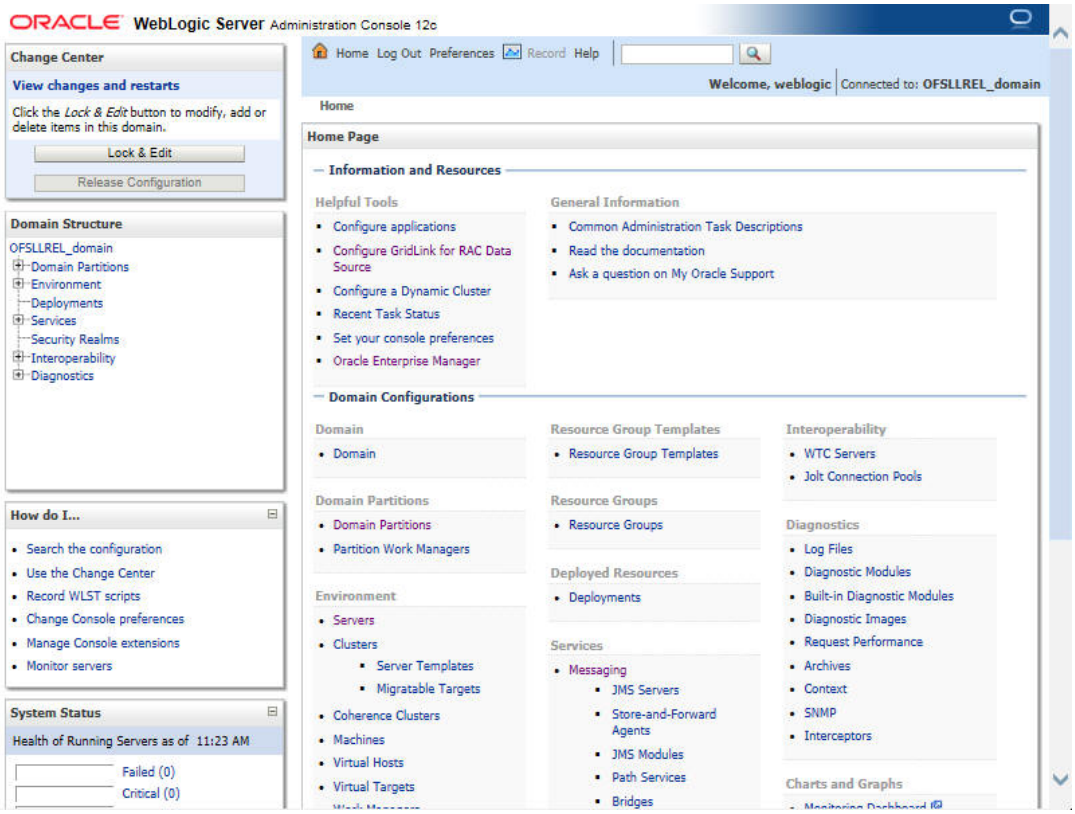
1. Login to Oracle Weblogic 12c console (`http://hostname:port/console`).

Figure 8-39 Create Persistent Stores 1



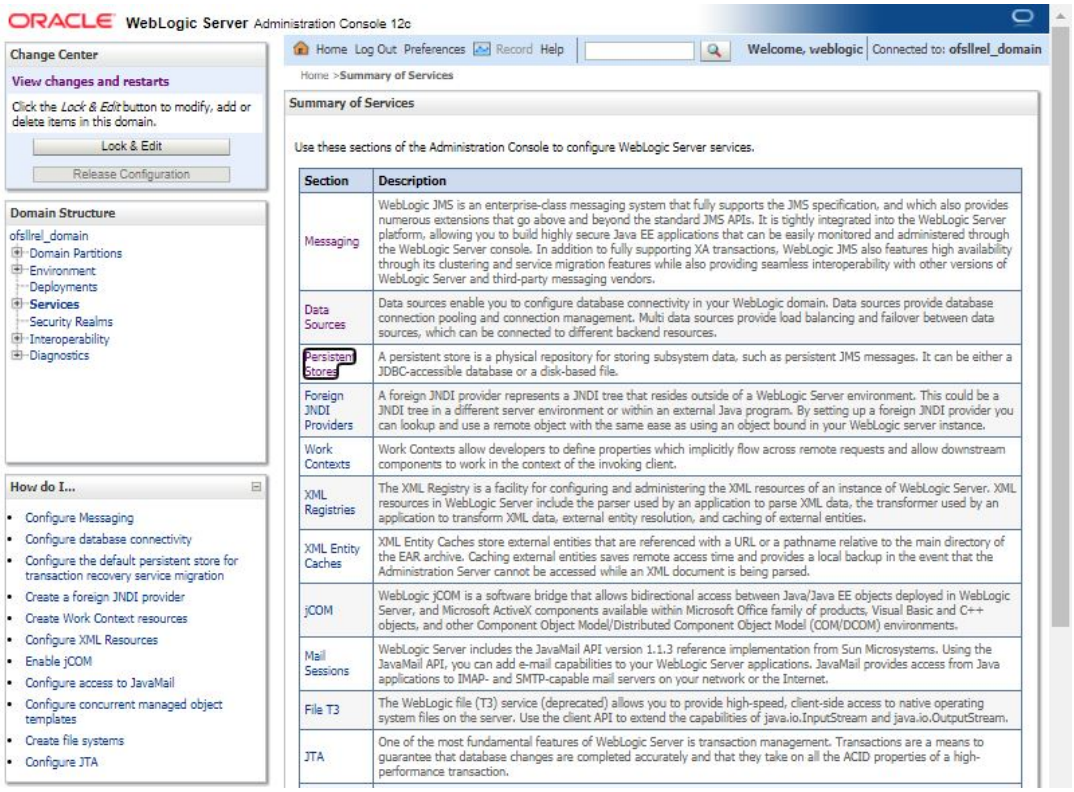
2. On successful login, the following window is displayed.

Figure 8-40 Create Persistent Stores 2



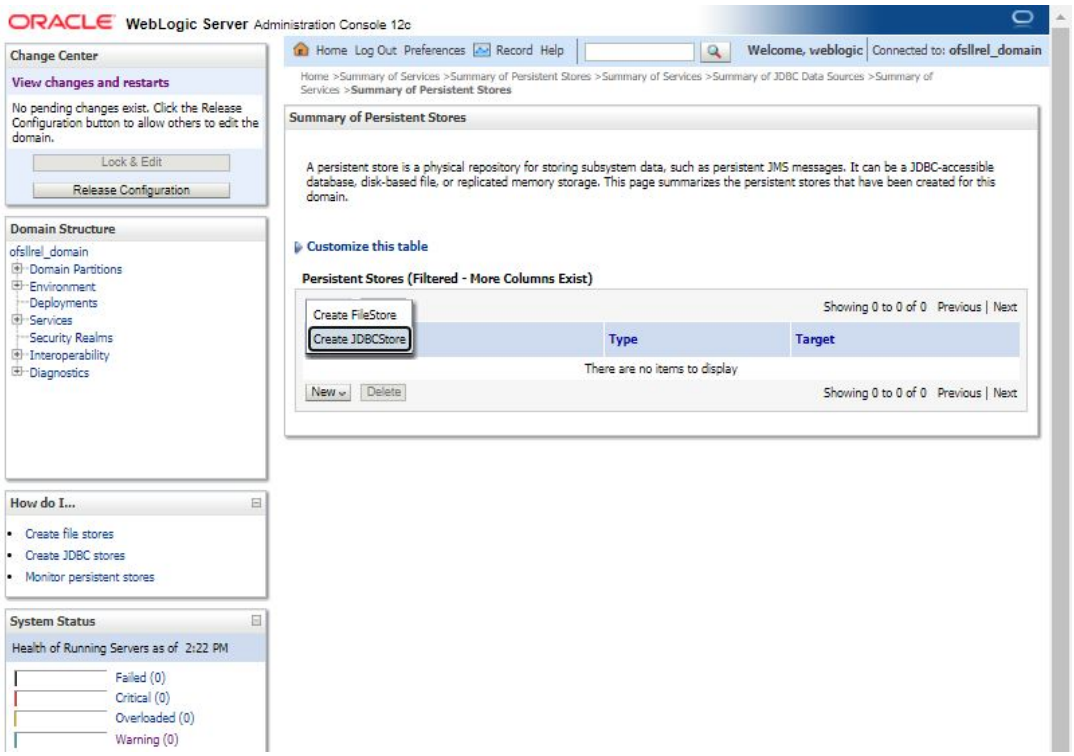
3. Click Domain Name > Services > Persistent Stores.

Figure 8-41 Create Persistent Stores 3



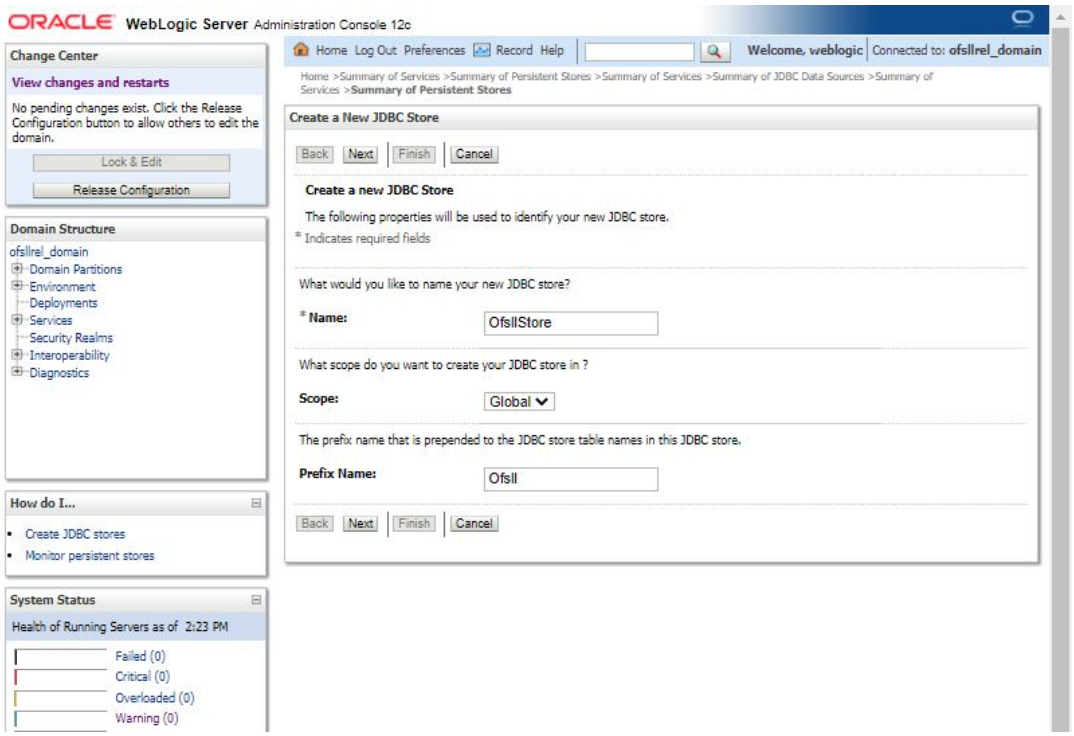
4. Click **Lock & Edit** button on the left panel. Click **New** on right panel and select **Create JDBCStore**.

Figure 8-42 Create Persistent Stores 4



5. Specify the following details:
   - Name: OfsllStore
   - Prefix Name: Ofsll

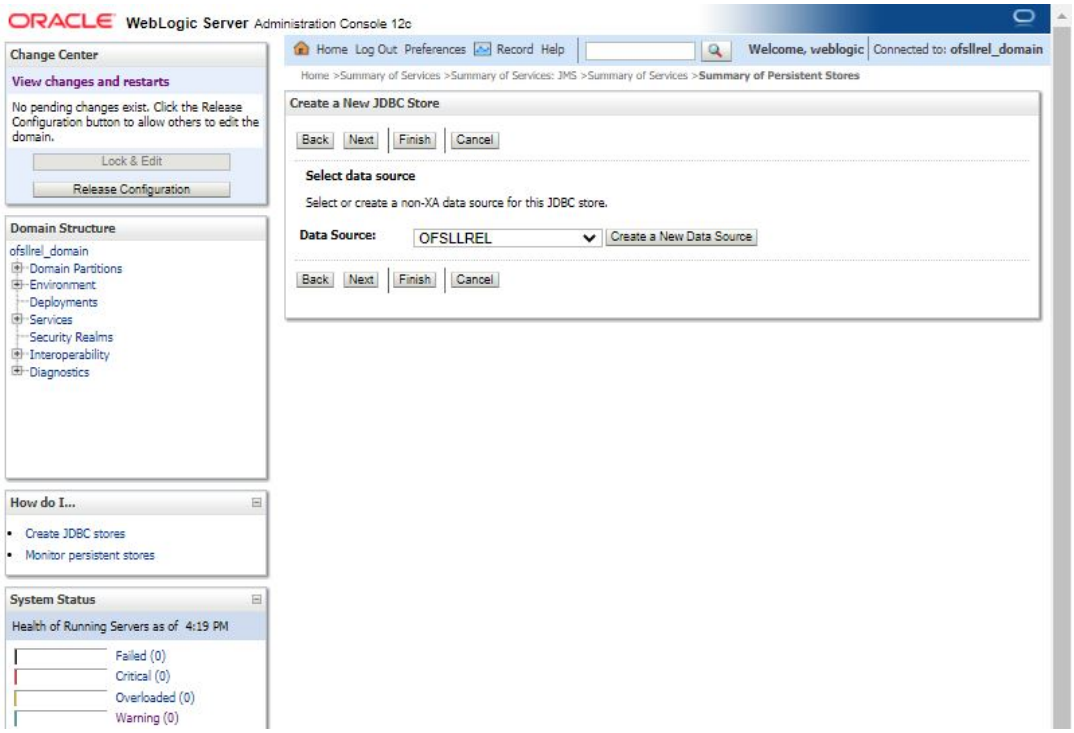
Figure 8-43 Create Persistent Stores 5



6. Click **Next**.

   The following window is displayed.

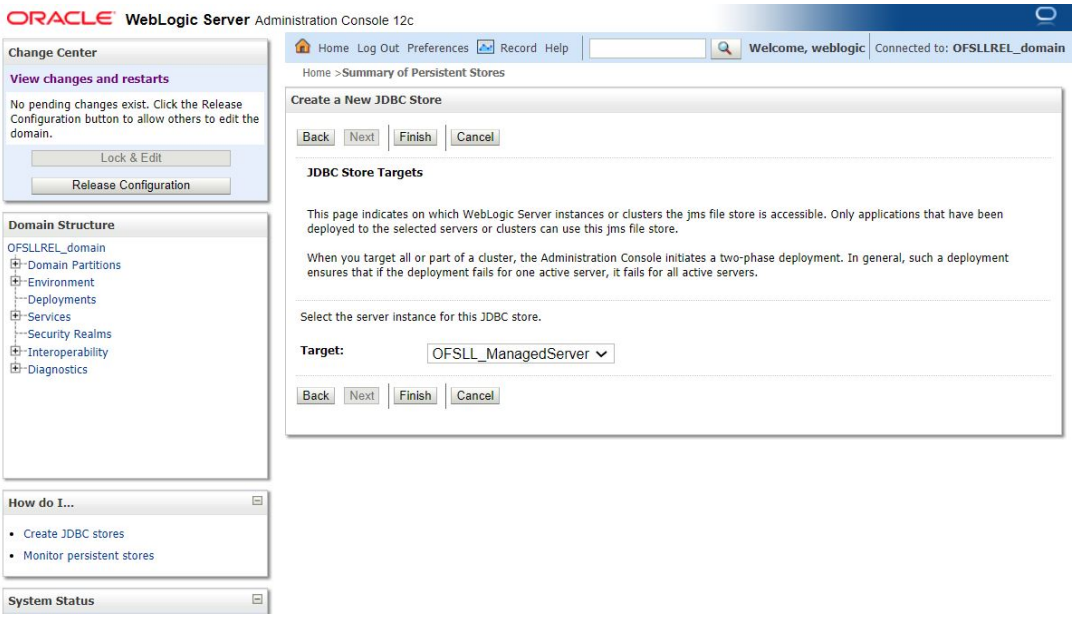
Figure 8-44 Create Persistent Stores 6



7. Select **OFSLLREL** Data source from the drop-down list. Click **Next**.

   The following window is displayed.

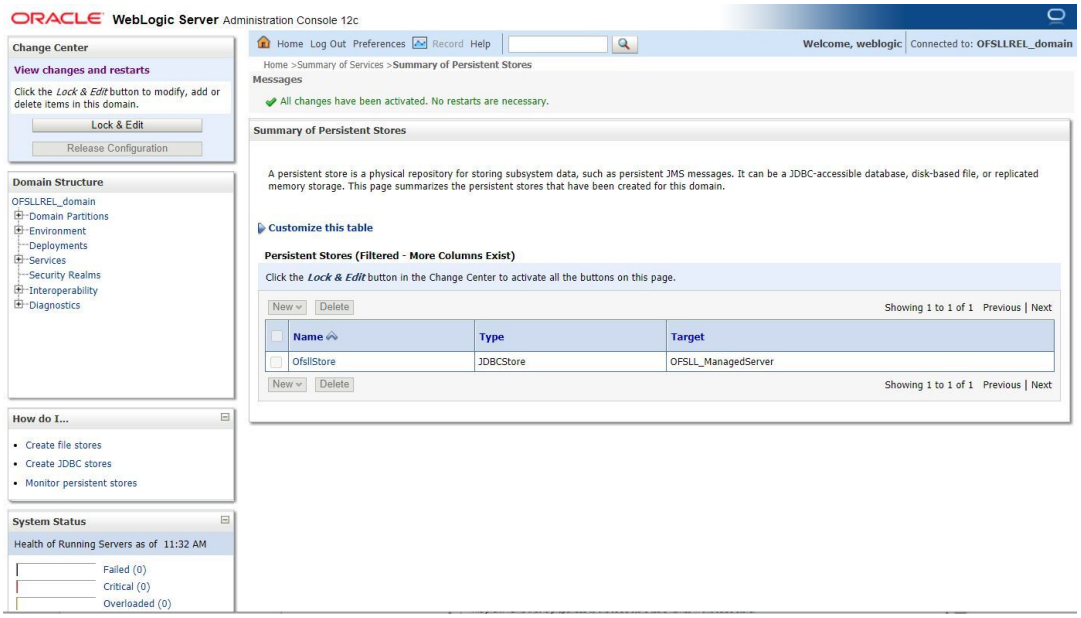
Figure 8-45 Create Persistent Stores 7



8. Select the Target as **OFSLL_ManagedServer** from the drop-down list. Click **Next**.

   The following window is displayed.

Figure 8-46 Create Persistent Stores 8



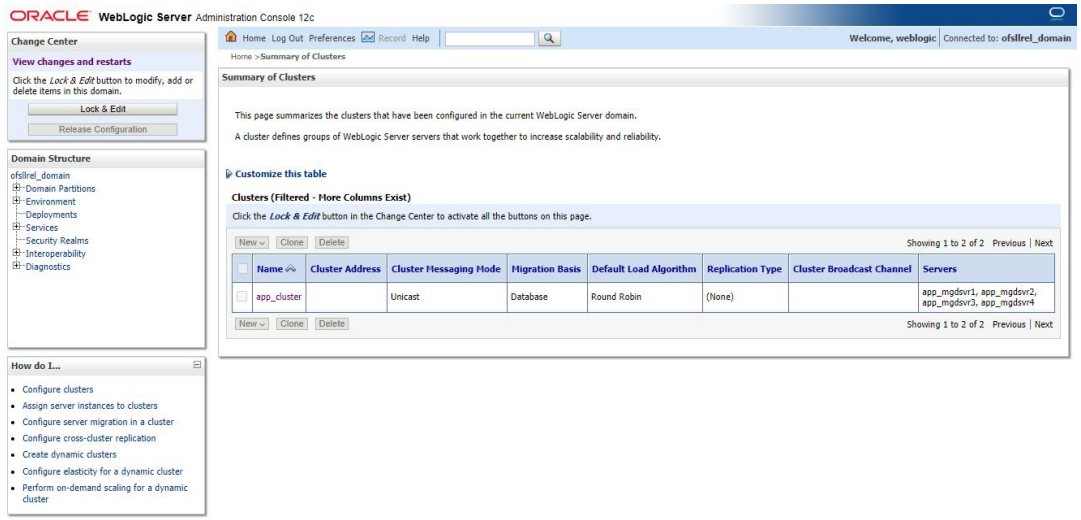
9. Click **Finish** to activate the changes.

In case you are creating a cluster setup, continue the below steps:

10. Click Domain Name > Environment > Clusters.

The following window is displayed.

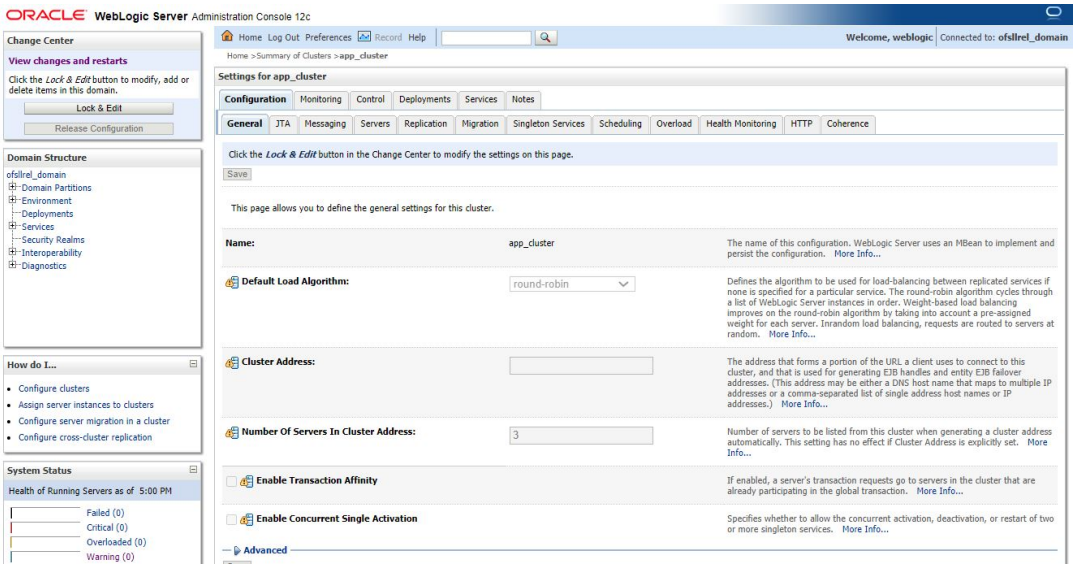
Figure 8-47 Create Persistent Stores 9



11. Click **app_cluster**.

The following window is displayed.

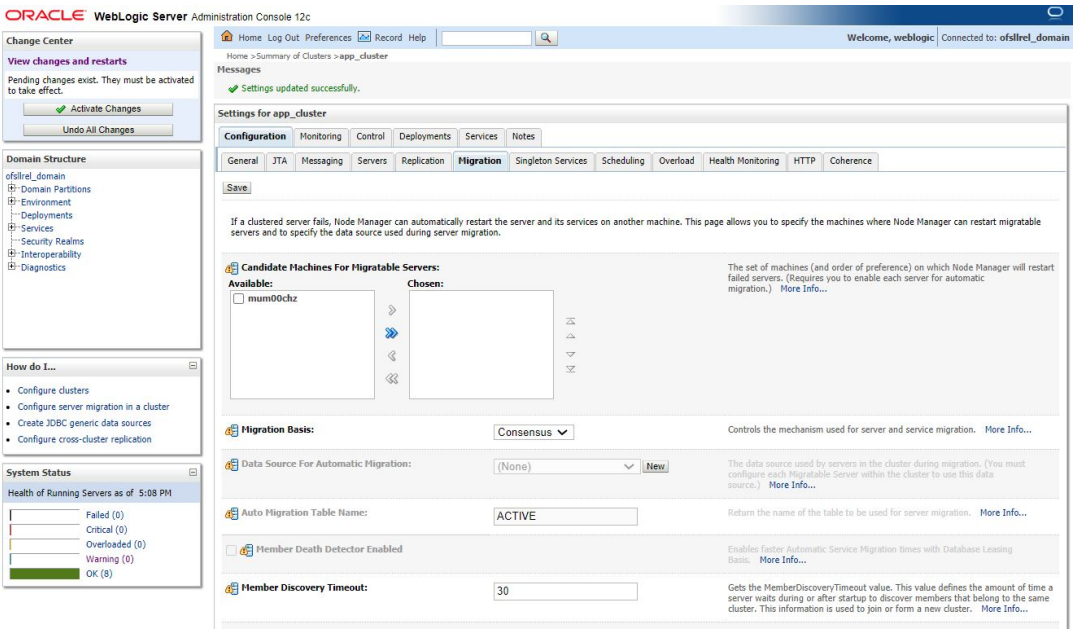
Figure 8-48 Create Persistent Stores 10



12. Click **Lock & Edit** button on the left panel.

    The following window is displayed.

Figure 8-49 Create Persistent Stores 11



13. Click **Migration** tab and choose Migration Basis as **Consensus** from the drop-down list.
14. Click **Save** to activate the changes.

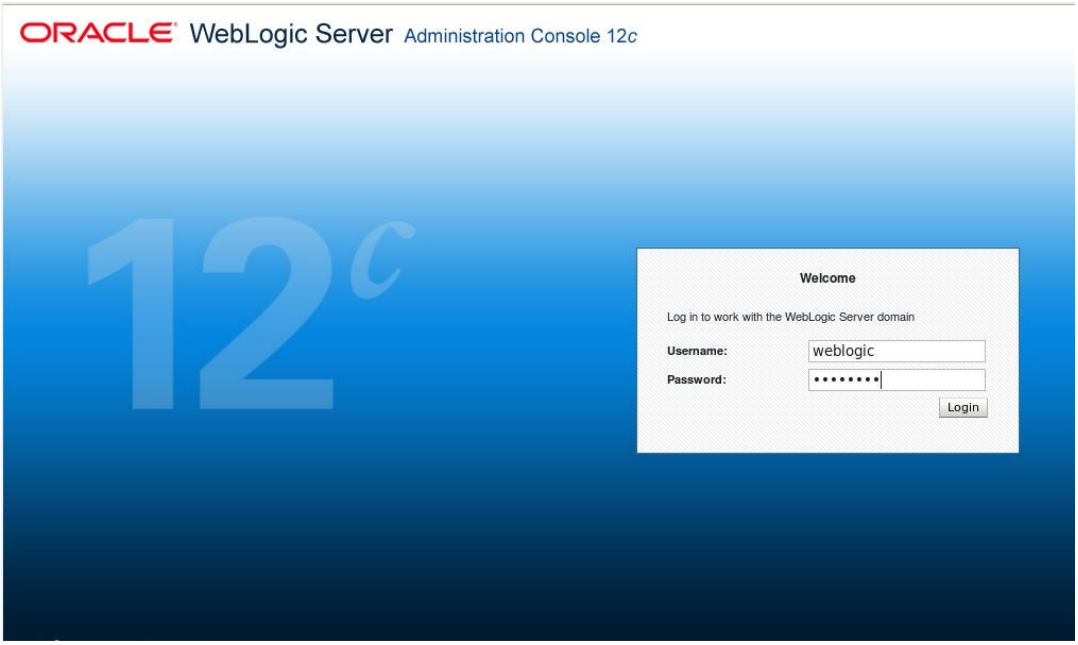
8.3.2 Create JMS Server for Outbound Queue

Follow the below steps to create JMS server for outbound queue.

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

   The following screen is displayed.

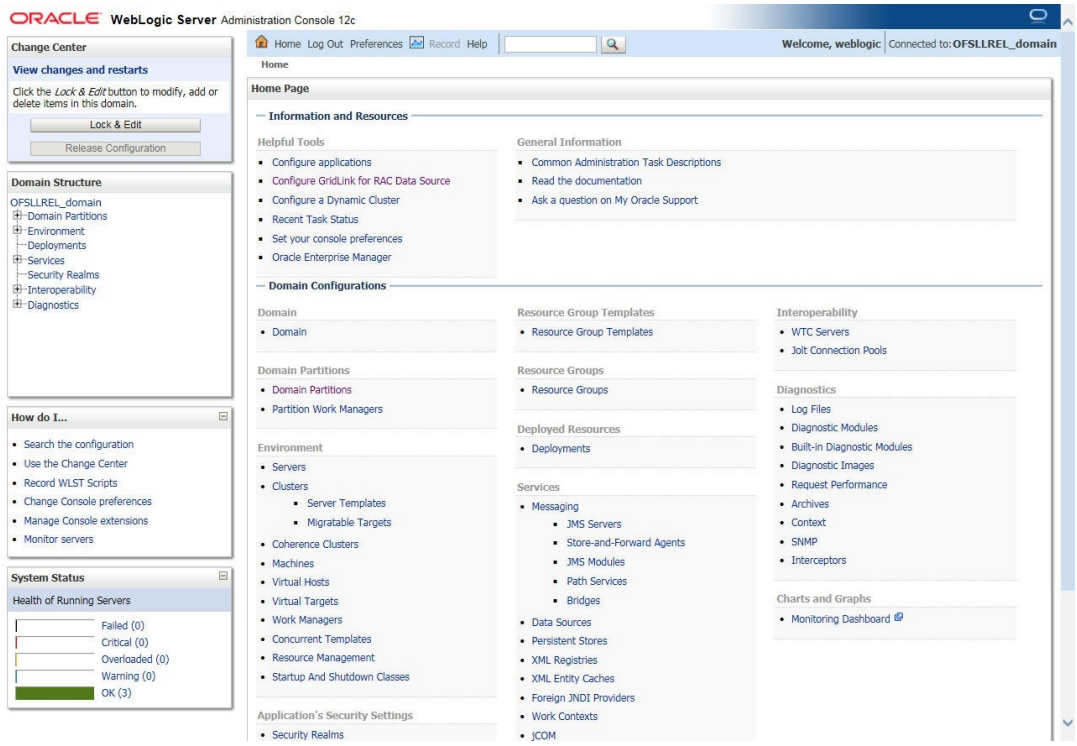
Figure 8-50 JMS Server for Outbound Queue 1



2. Specify the Weblogic administrator user name and password and click **Log In**.

   The Oracle Weblogic home page is displayed.

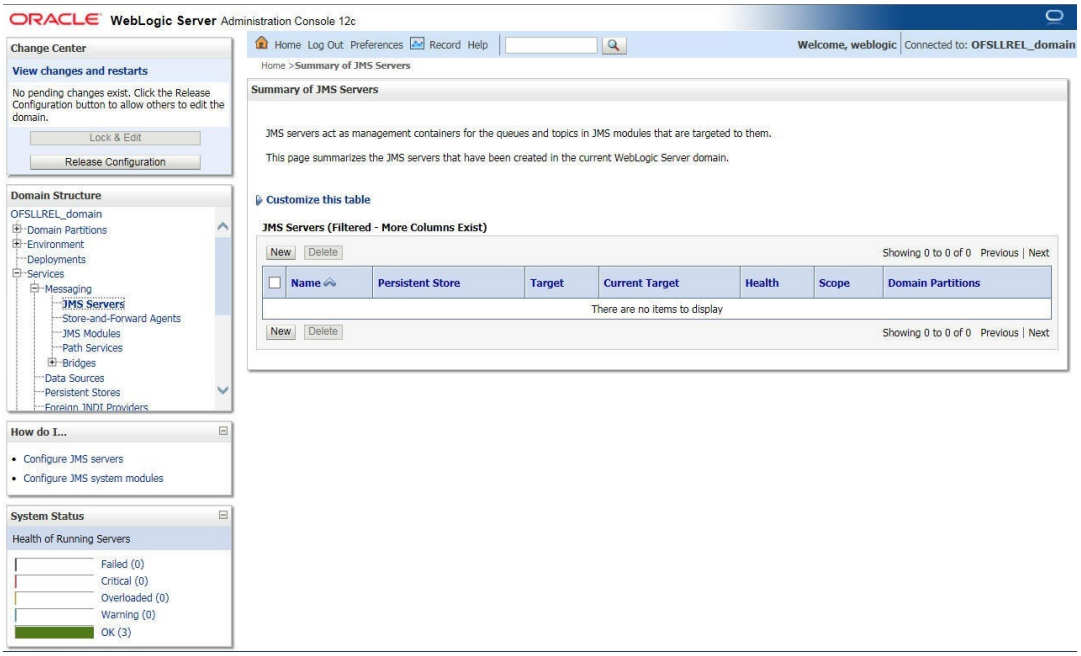
Figure 8-51 JMS Server for Outbound Queue 2



3. Click Domain Name > Services > Messaging > JMS Server.
4. In the main window, click **Lock & Edit**.

   The following window is displayed.

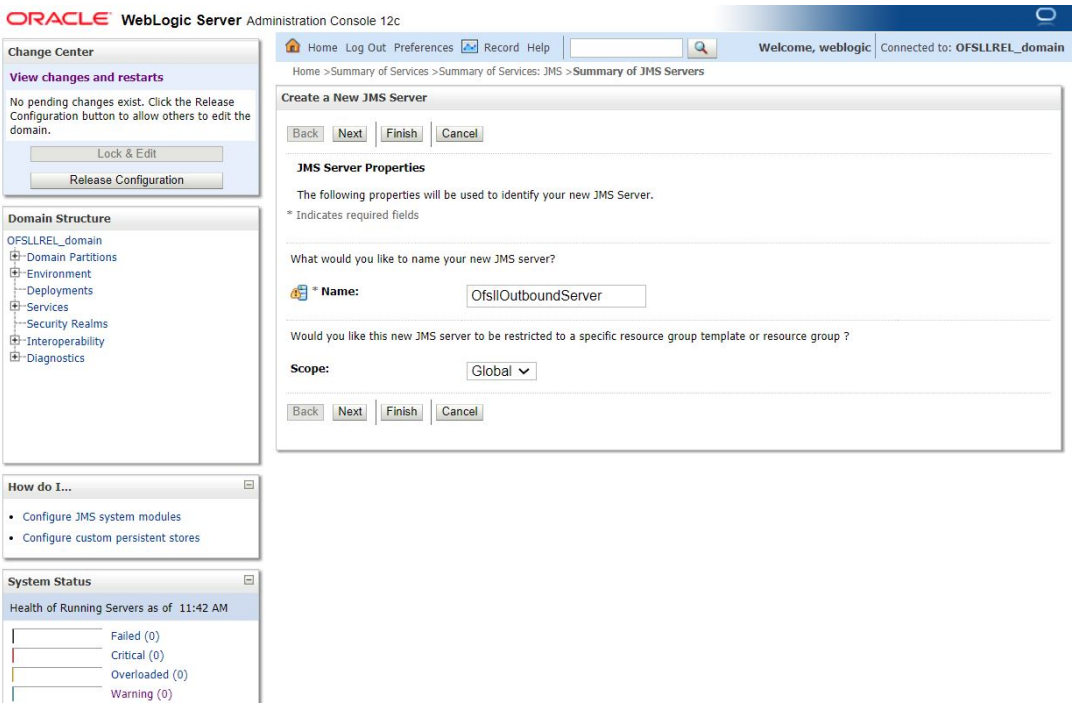
Figure 8-52 JMS Server for Outbound Queue 3



5. Click **New**.

   The following window is displayed.

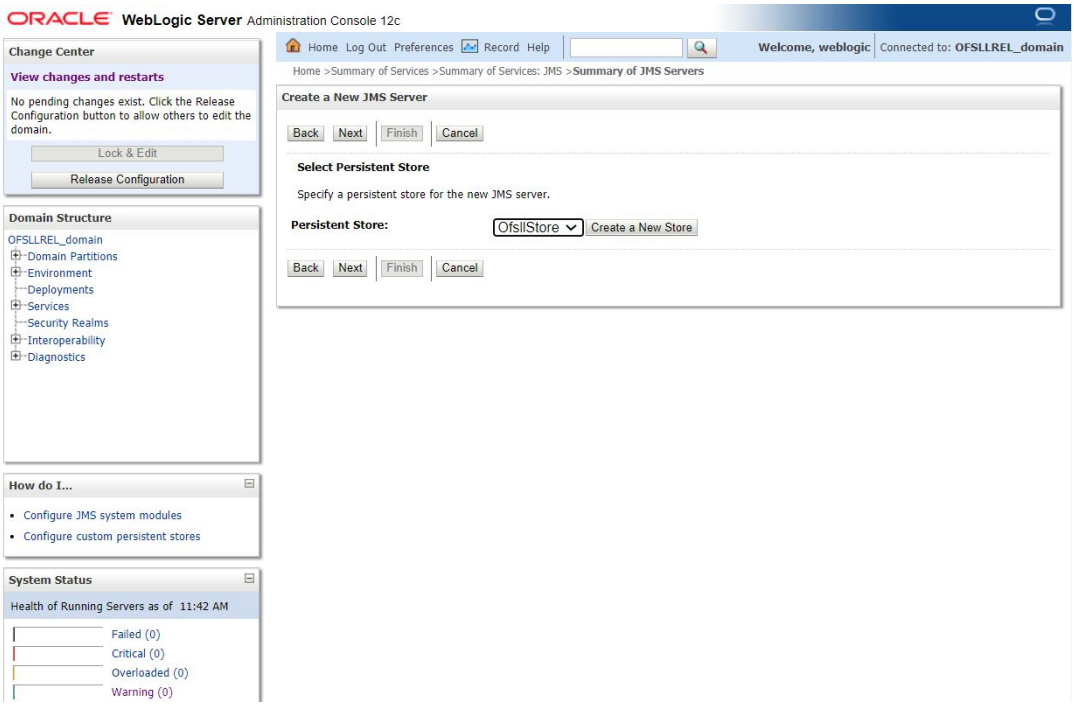
Figure 8-53 JMS Server for Outbound Queue 4



6. Specify the JMS Server Name as **OfsllOutboundServer**. Click **Next**.

   The following window is displayed.

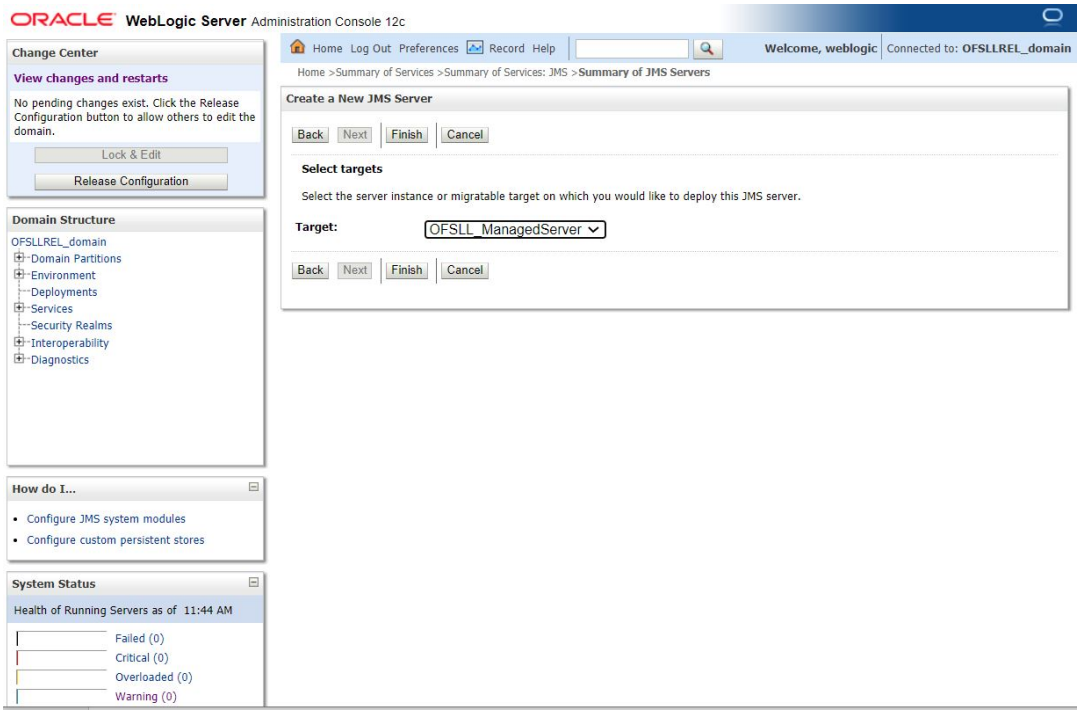
Figure 8-54 JMS Server for Outbound Queue 5



7. Select **OfsllStore** as the Persistent Store type. Click **Next**.

   The following window is displayed.

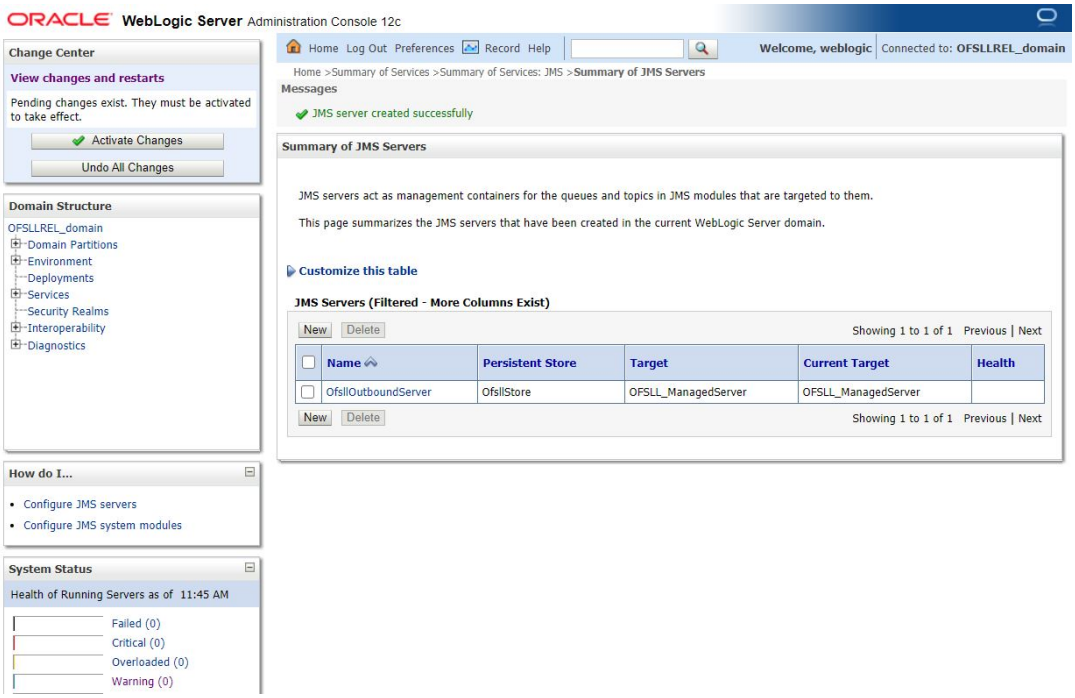
Figure 8-55 JMS Server for Outbound Queue 6



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

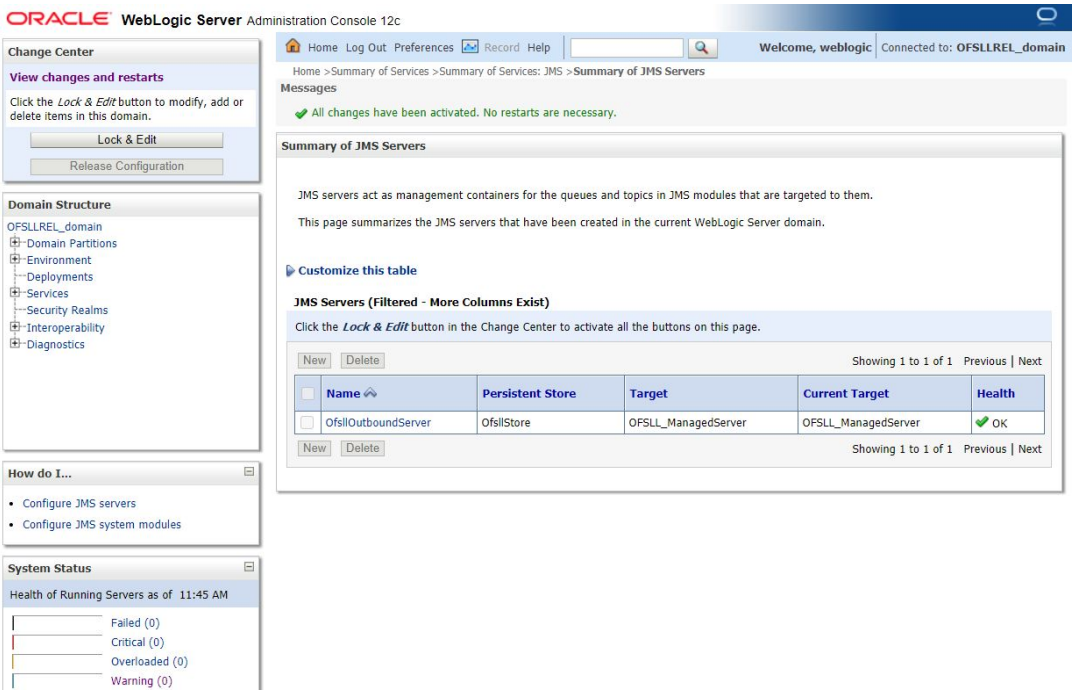
9. Click **Activate Changes** under Change Center section in LHS menu. Once done, the following window is displayed.

Figure 8-56 JMS Server for Outbound Queue 7



10. Once done the following window is displayed.

Figure 8-57 JMS Server for Outbound Queue 8



8.3.3 Create JMS Module for Outbound Queue

Follow the below steps to create JMS module for outbound queue.

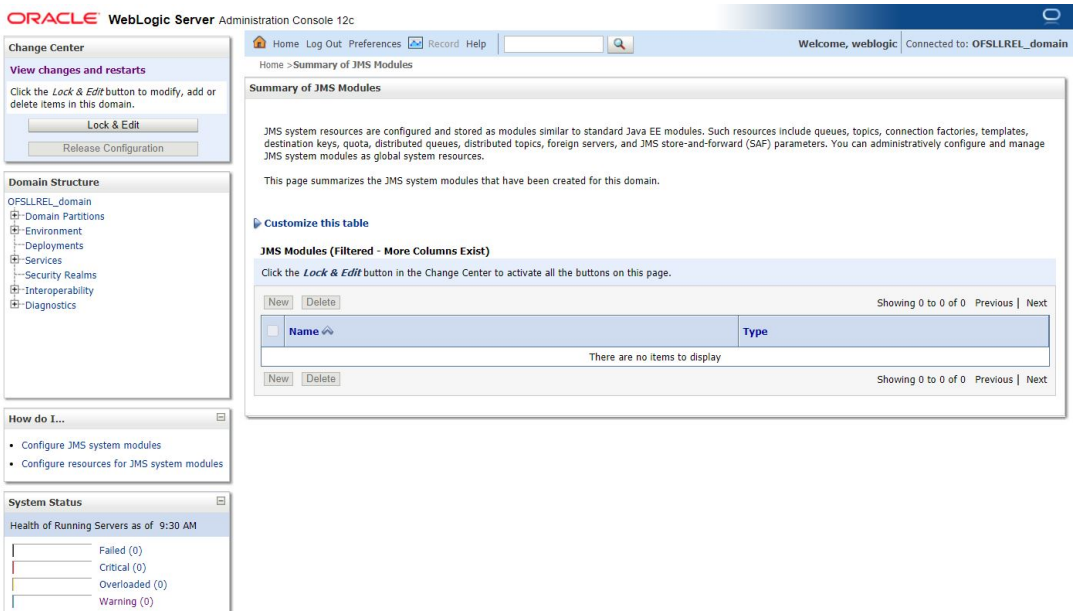
1. Login to WebLogic Server 12c console (`http://hostname:port/console`) by specifying the Weblogic administrator user name and password.

   (Optional) Enter the result of the step here.

2. Click Domain Name > Services > Messaging > JMS Modules.

   The following window is displayed.

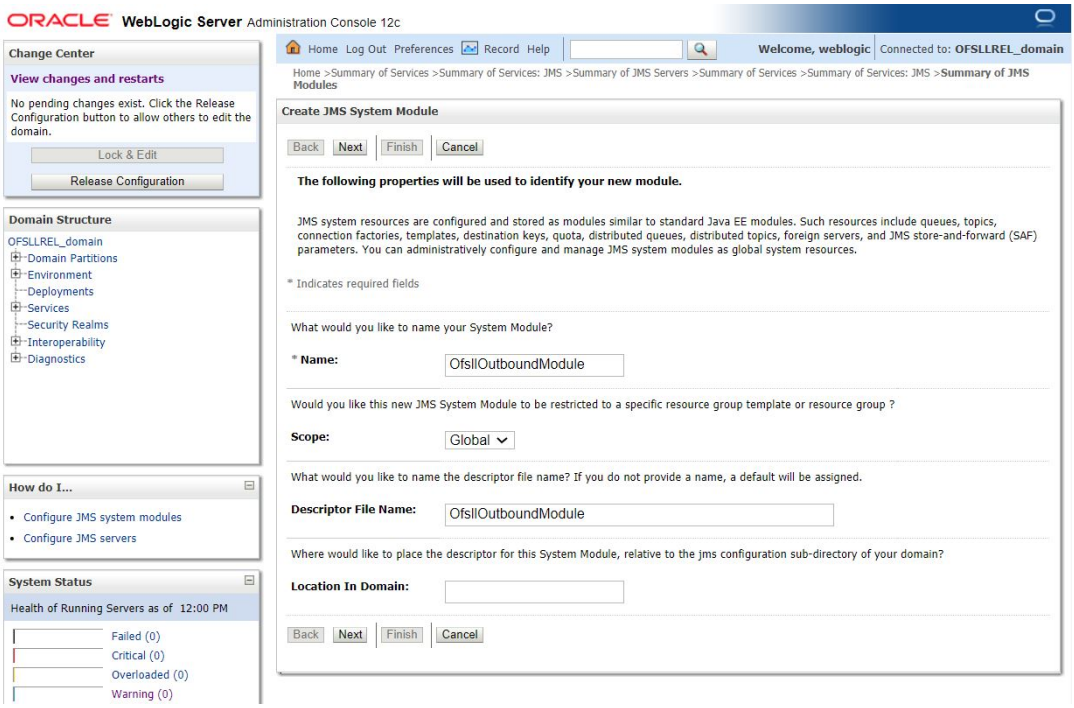
Figure 8-58 JMS Module for Outbound Queue 1



3. Click **New**.

   The following screen is displayed.

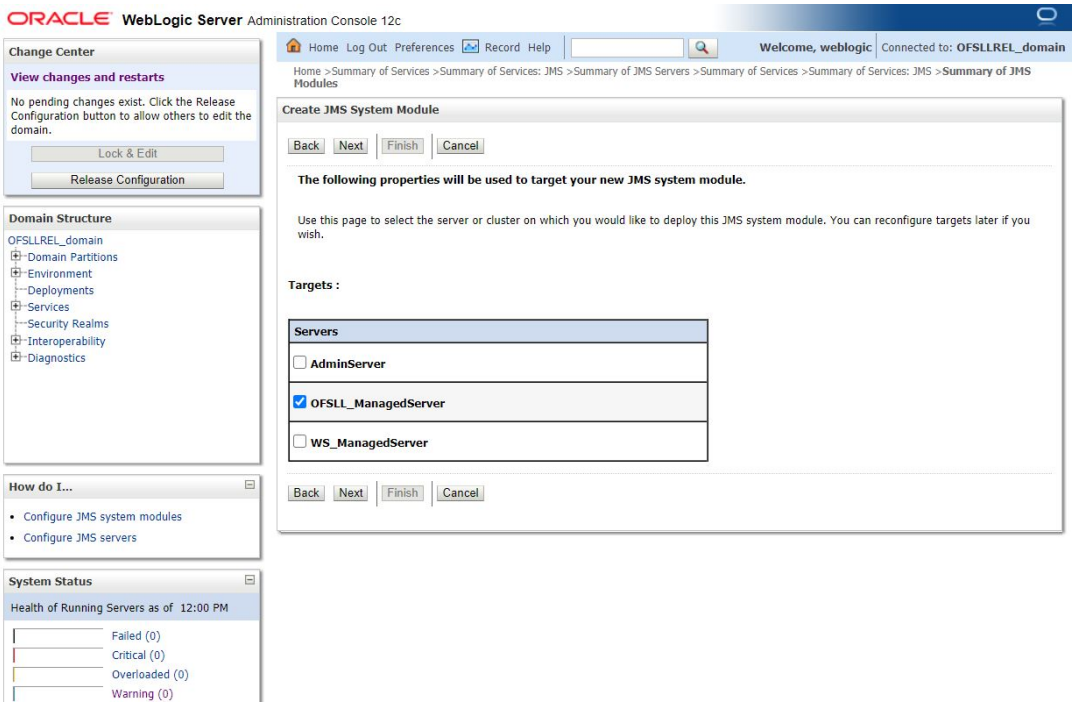
Figure 8-59 JMS Module for Outbound Queue 2



4. Specify the following details:
   - Enter the System Module Name as **OfsllOutboundModule**.
   - Enter the Description File Name as **OfsllOutboundModule**.
5. Click **Next**.

   The following screen is displayed.

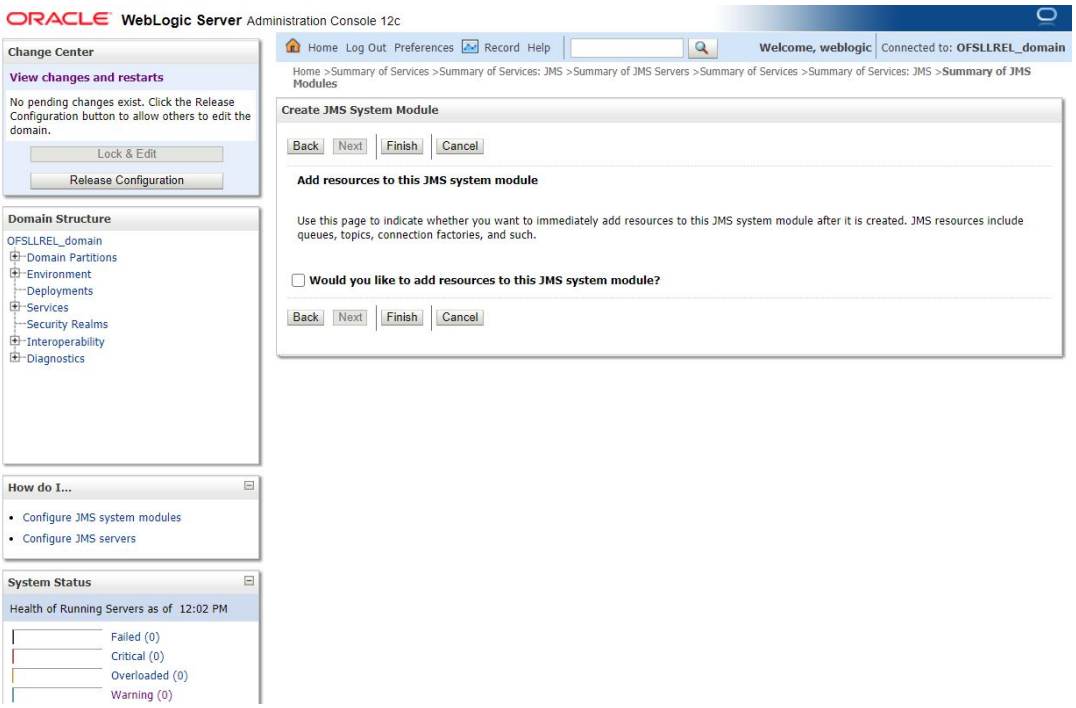
Figure 8-60 JMS Module for Outbound Queue 3



6. Select the target server and click **Next**.

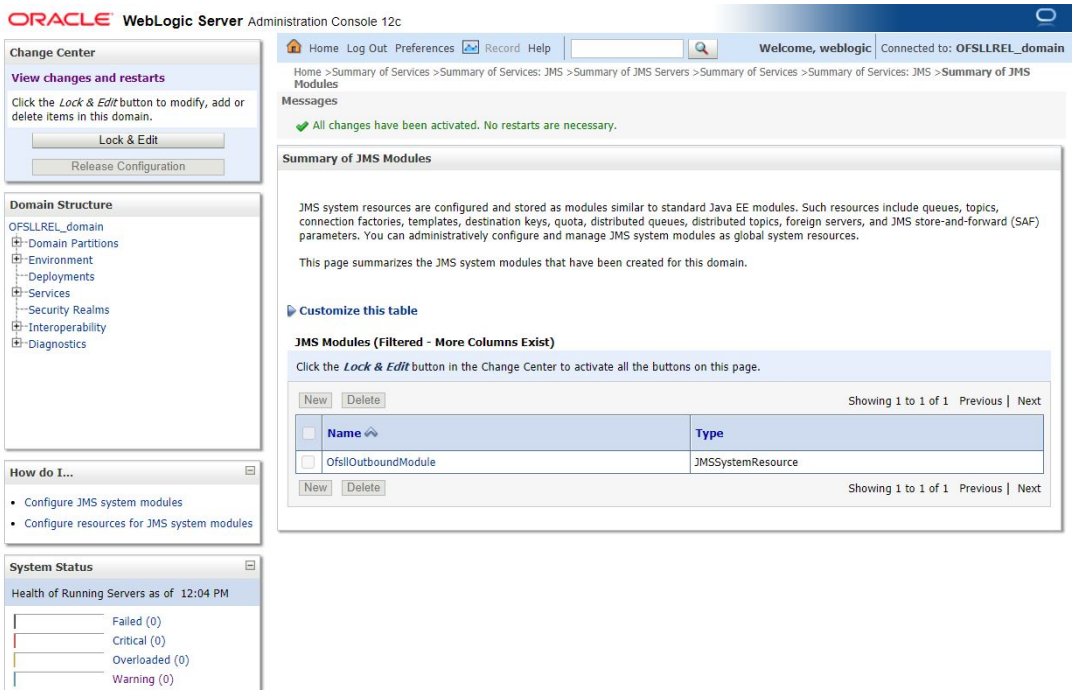
   The following window is displayed.

Figure 8-61 JMS Module for Outbound Queue 4



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

Figure 8-62 JMS Module for Outbound Queue 5



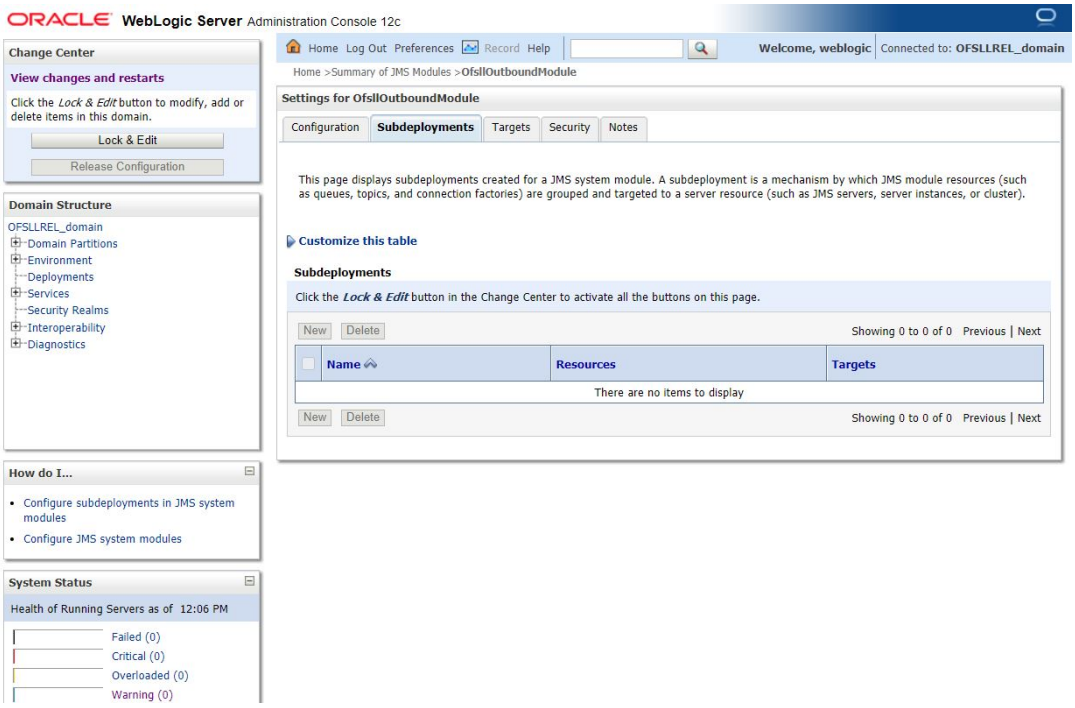
8.3.4 SubDeployment for Outbound Queue

Follow the below steps to do subdeployment for outbound queue.

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

   The following window is displayed.

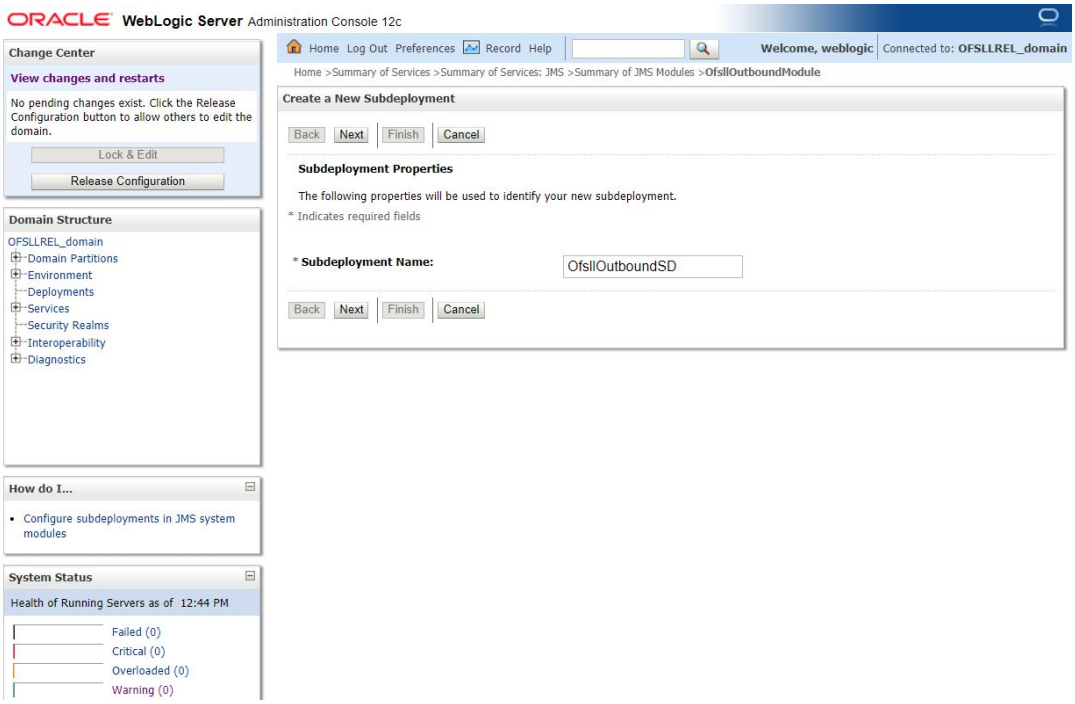
Figure 8-63 SubDeployment for Outbound Queue 1



4. Click **New**.

The following screen is displayed.

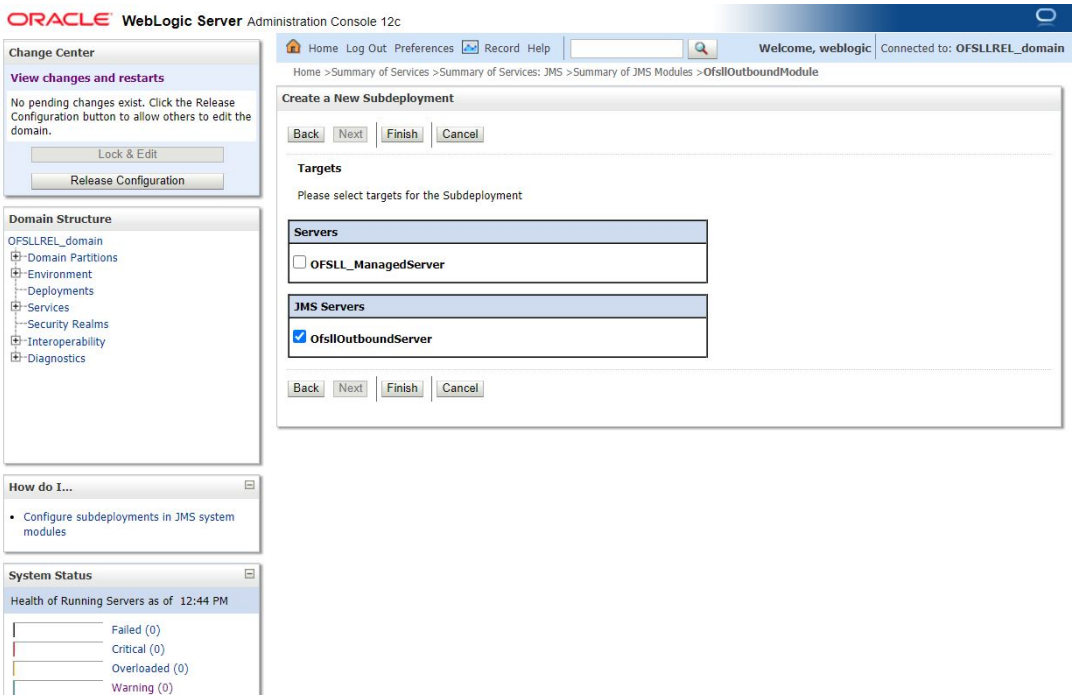
Figure 8-64 SubDeployment for Outbound Queue 2



5. Specify the Subdeployment Name as **OfsllOutboundSD**. Click **Next**.

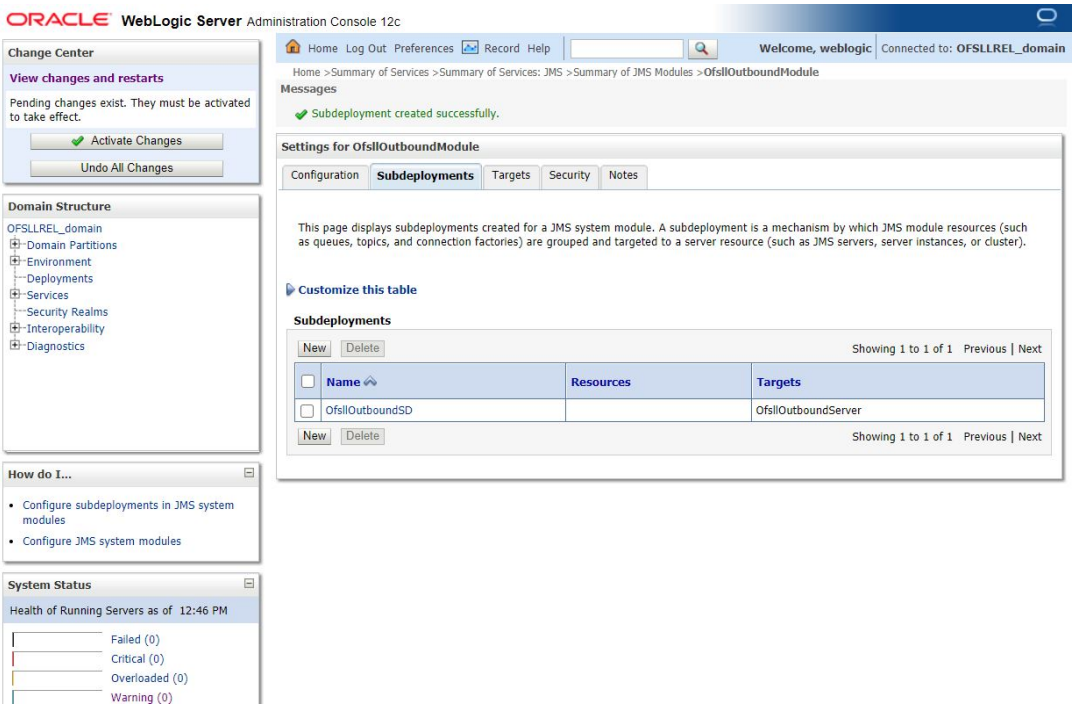
The following window is displayed.

Figure 8-65 SubDeployment for Outbound Queue 3



6. Select the check box against the newly created OfsllOutboundServer and click **Finish**.
7. Once done, the following window is displayed.

Figure 8-66 SubDeployment for Outbound Queue 4



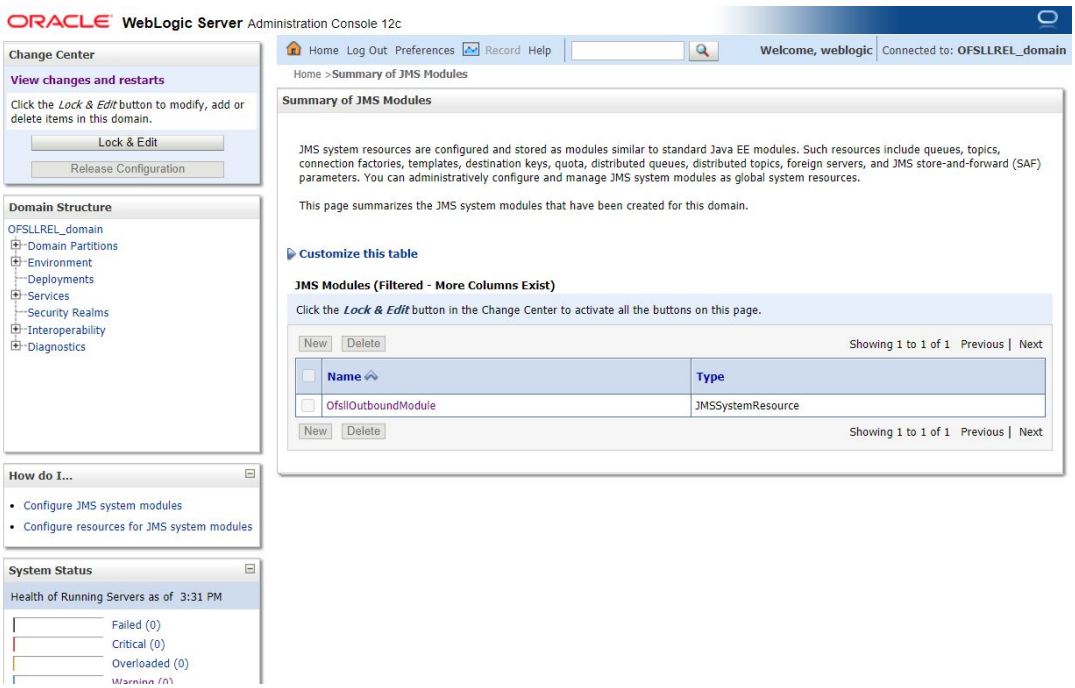
You can further click **New** to create more Queues and repeat the steps explained above.

8.3.5 Create JMS Connection Factory for Outbound Queue

Follow the below steps to create JMS connection factory for outbound queue.

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

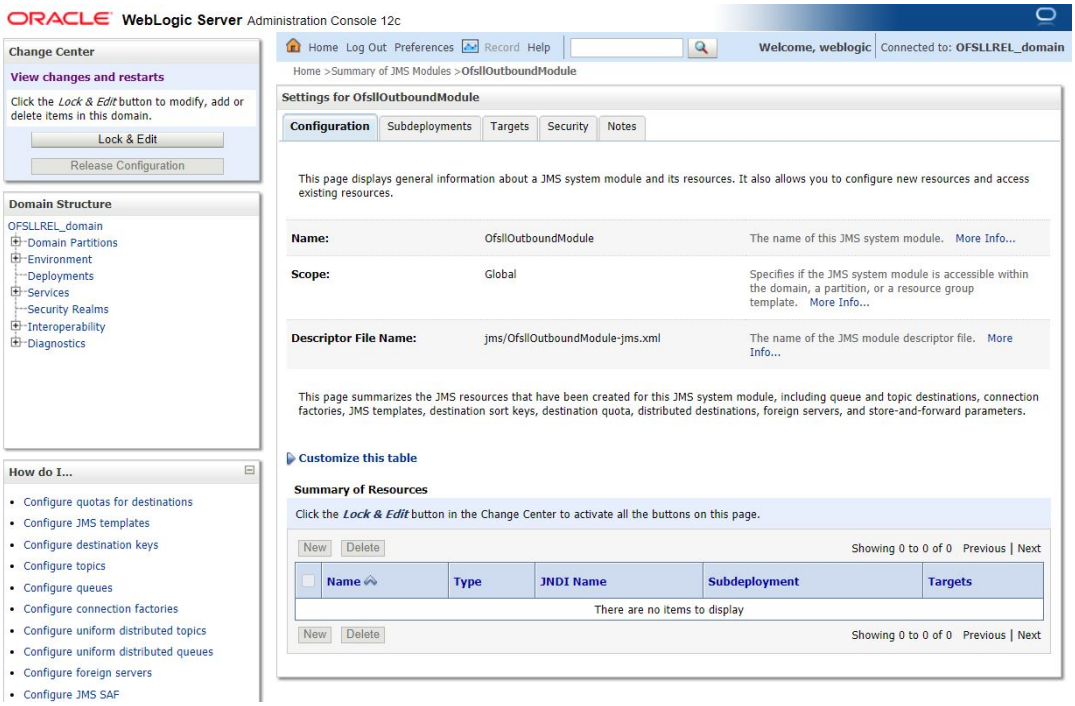
Figure 8-67 JMS Connection Factory for Outbound Queue 1



3. Select the newly created JMS module **OfsllModule**.

   The following window is displayed.

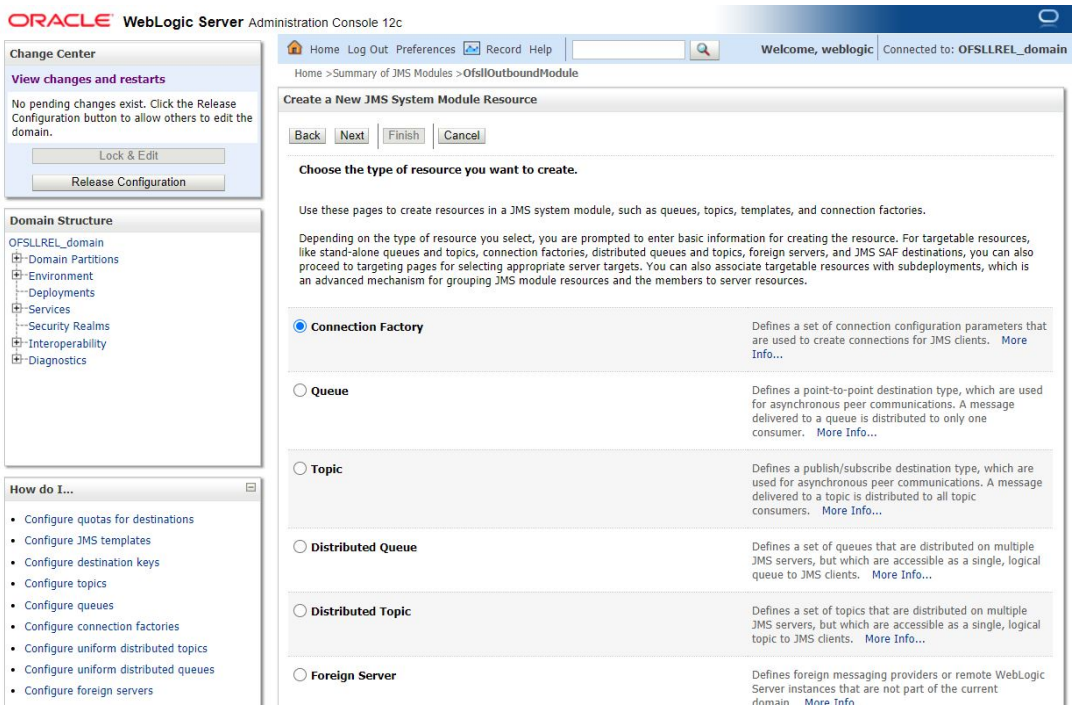
Figure 8-68 JMS Connection Factory for Outbound Queue 2



4. Click **New**.

The following window is displayed.

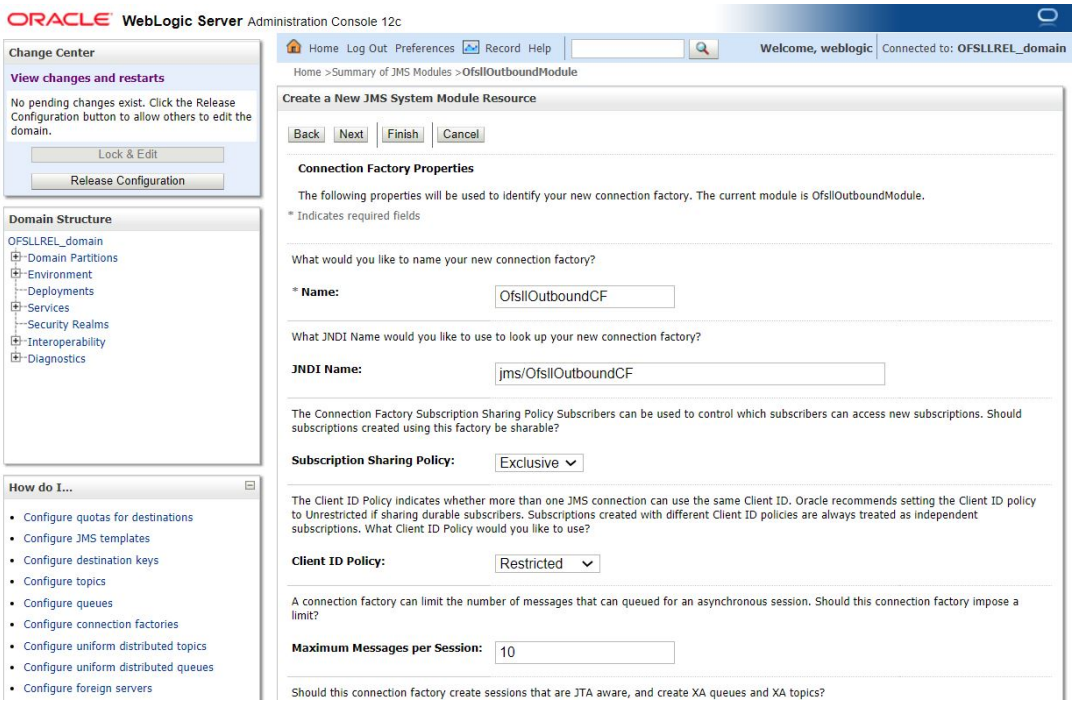
Figure 8-69 JMS Connection Factory for Outbound Queue 3



5. Select **Connection Factory** option and click **Next**.

The following window is displayed.

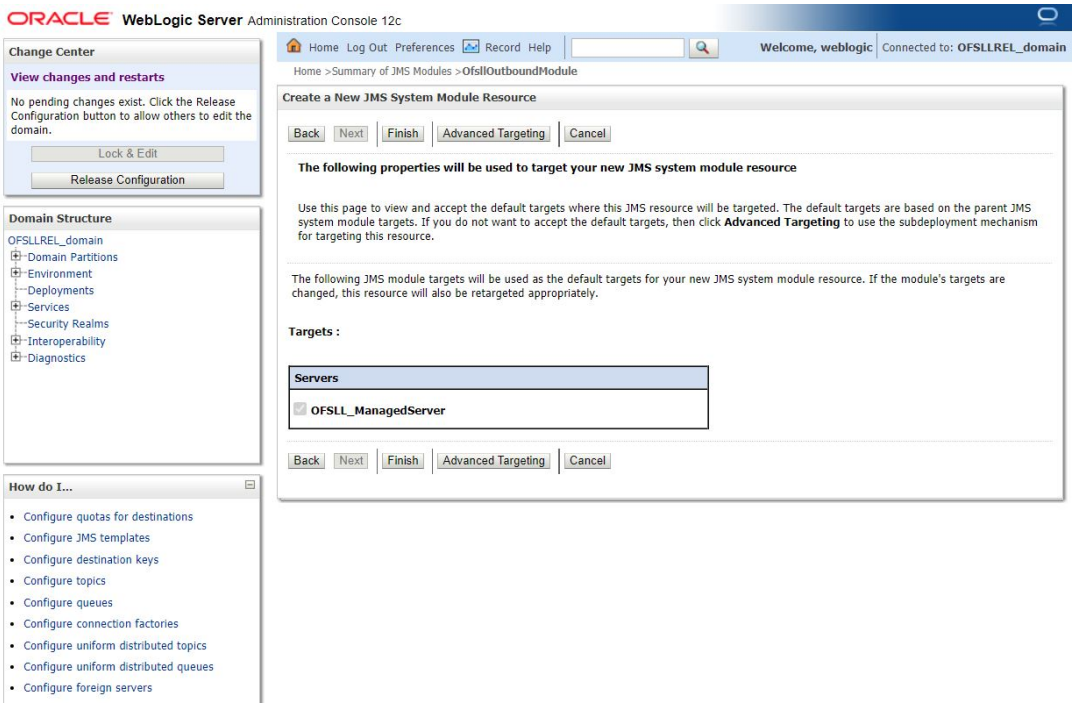
Figure 8-70 JMS Connection Factory for Outbound Queue 4



6. Specify the following details:
   - Enter the Name of the Connection Factory as **OfsllOutboundCF**.
   - Enter the JNDI Name as **jms/OfsllOutboundCF**.
   - Select the check box **XA Connection Factory Enabled**
7. Click **Next**.

   The following window is displayed.

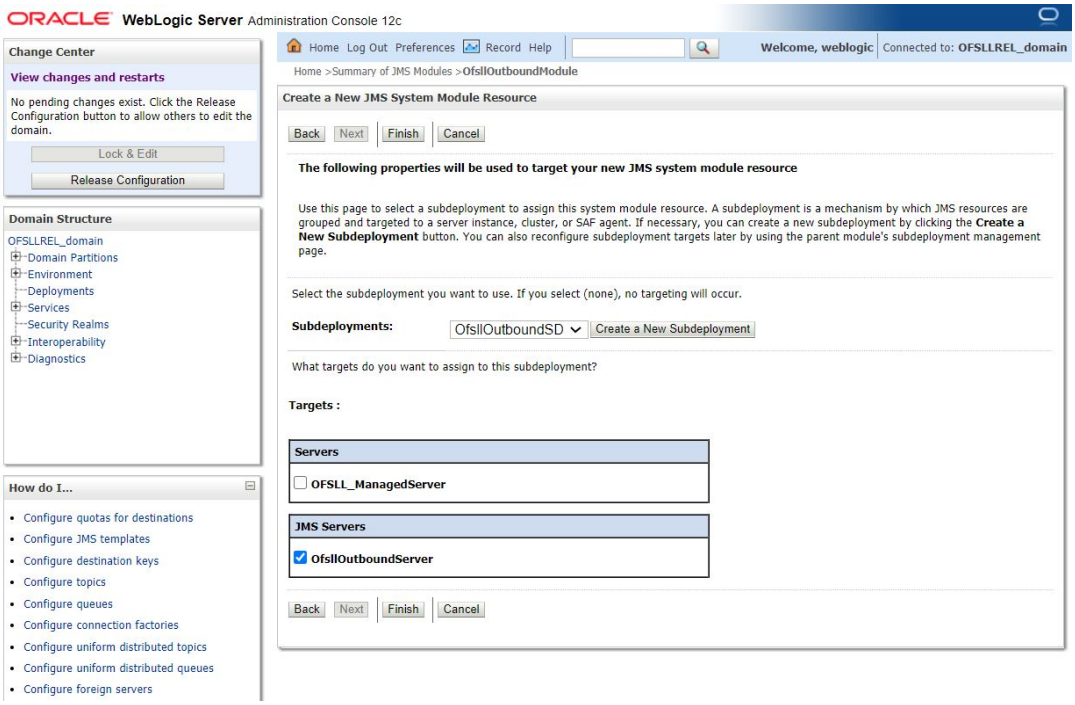
Figure 8-71 JMS Connection Factory for Outbound Queue 5



8. Click **Advanced Targeting** button.

   The following window is displayed.

Figure 8-72 JMS Connection Factory for Outbound Queue 6



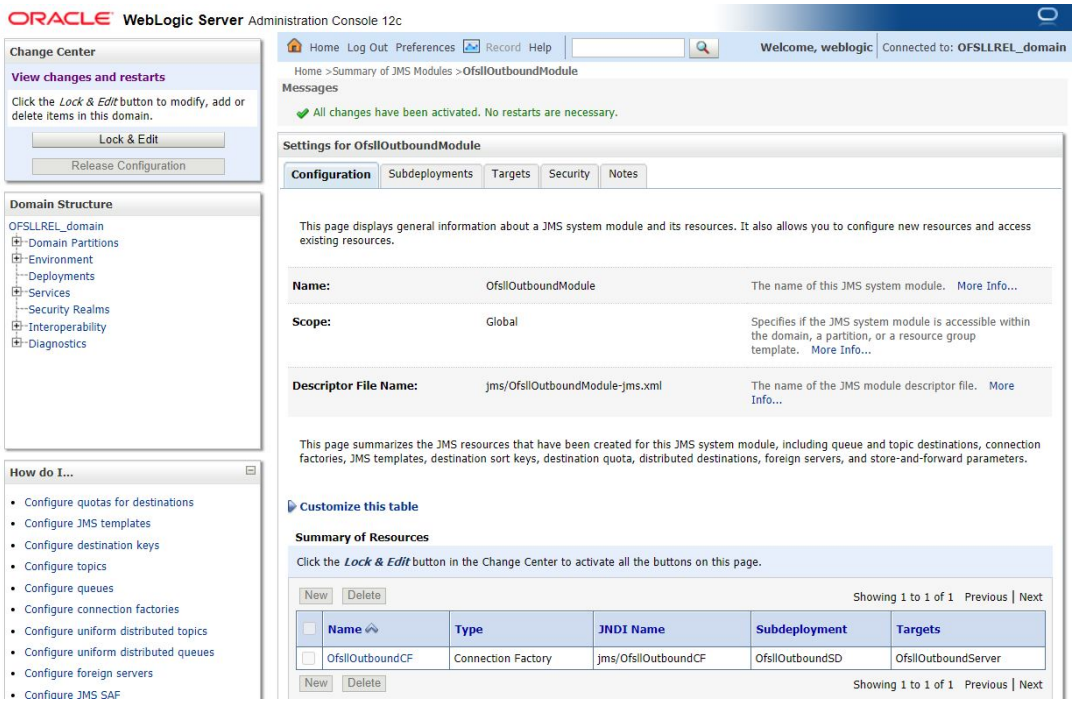
9. Do the following:

   - Select the Subdeployments as **OfsllOutboundSD** from the drop down list.

- Under JMS Servers, select the check box against **OfsllOutboundServer**.

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

Figure 8-73 JMS Connection Factory for Outbound Queue 7



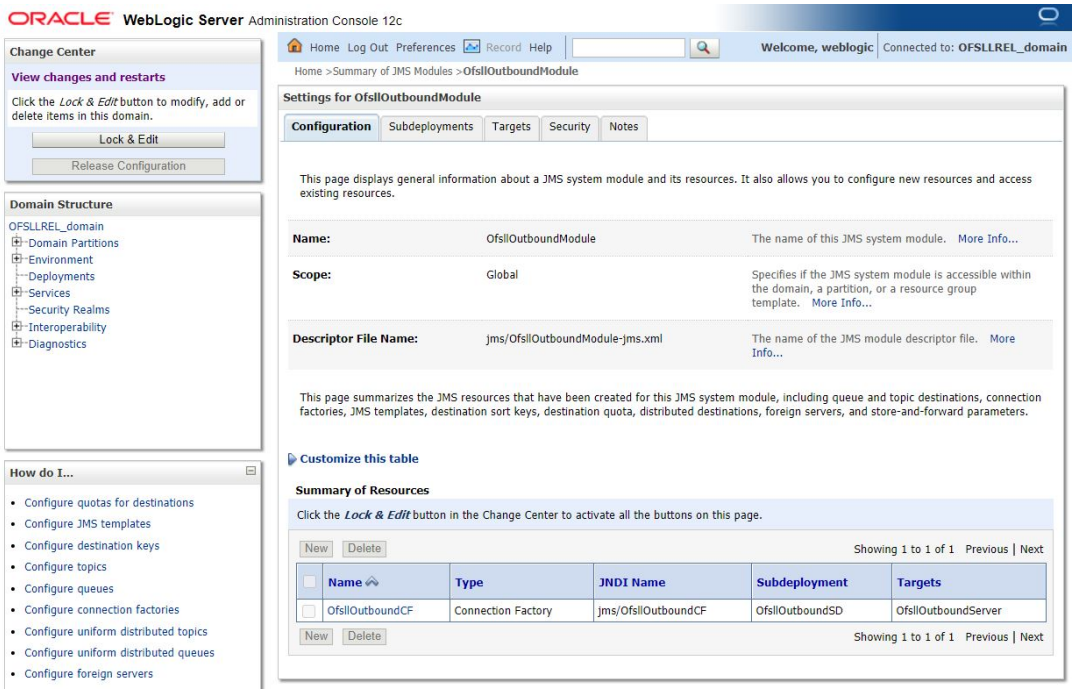
8.3.6 Create JMS Queue for Outbound Queue

Follow the below steps to create JMS Queue for outbound queue.

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

   The following window is displayed.

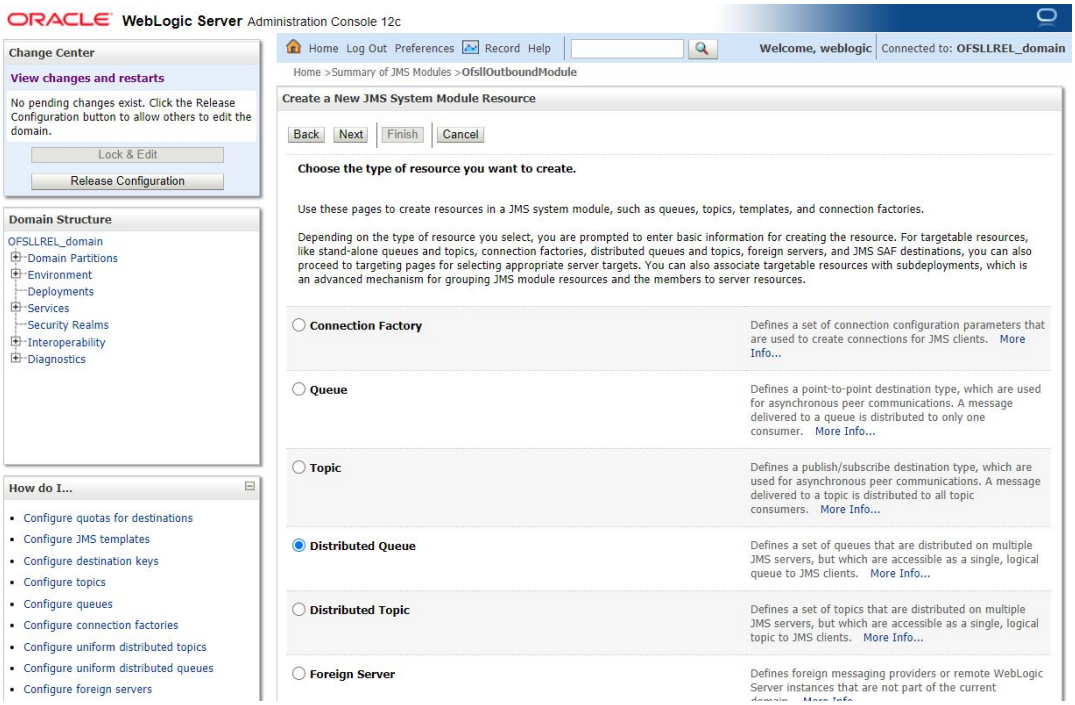
Figure 8-74 JMS Queue for Outbound Queue 1



4. Click **New**.

   The following window is displayed.

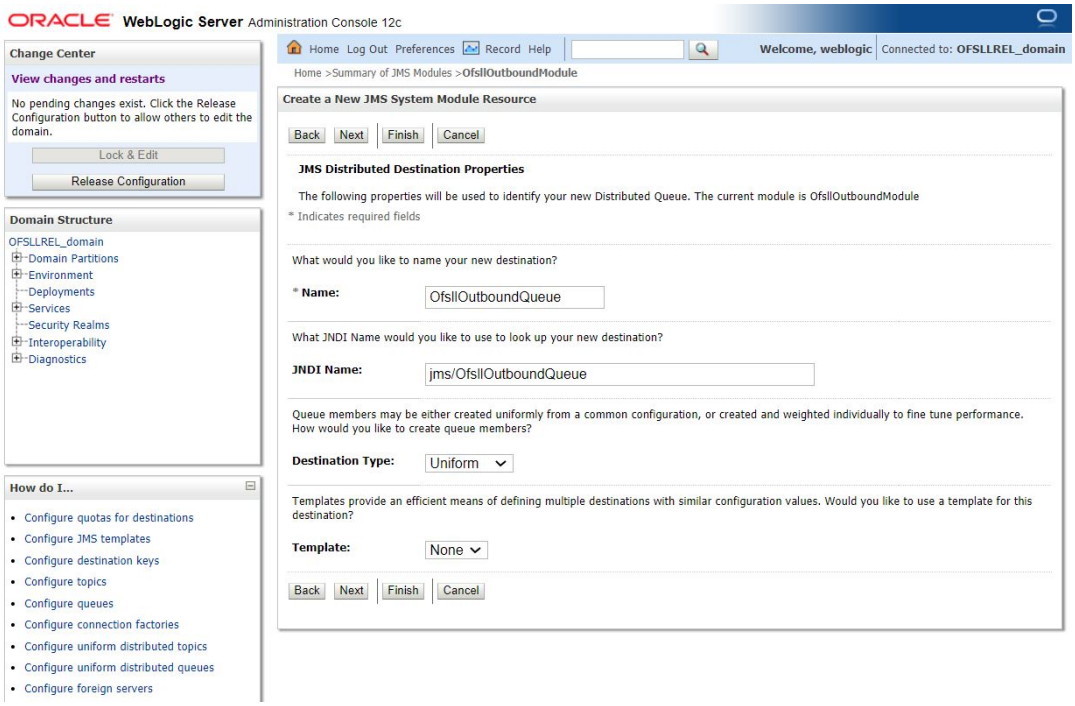
Figure 8-75 JMS Queue for Outbound Queue 2



5. Select the **Distributed Queue** option and click **Next**.

   The following window is displayed.

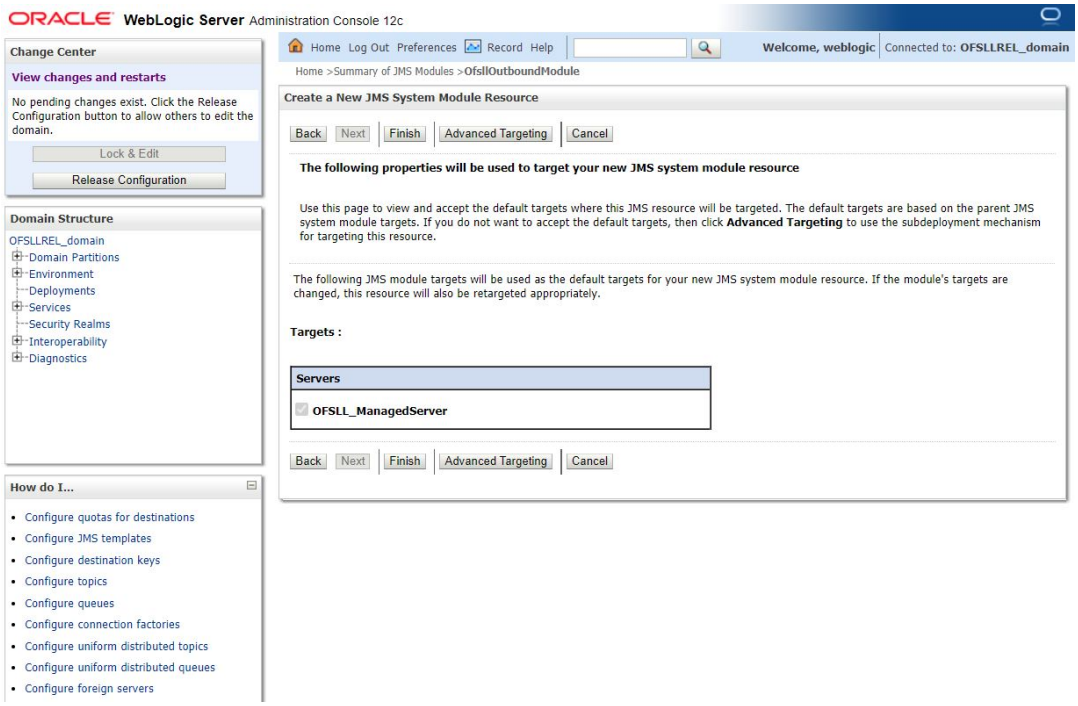
Figure 8-76 JMS Queue for Outbound Queue 3



6. Specify the following details while creating new JMS System Module Resources:
   - Enter the Name of the Queue as **OfsllOutboundQueue**
   - Enter the JNDI Name as **jms/OfsllOutboundQueue**
   - Select the Template as **None**
7. Click **Next**.

   The following window is displayed.

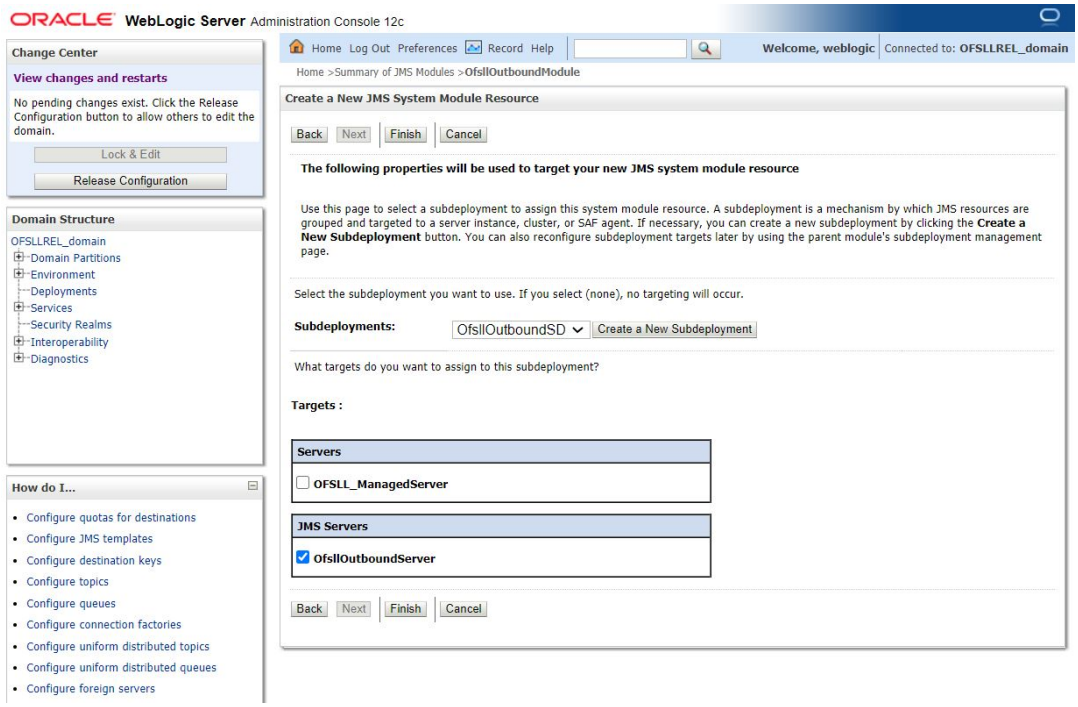
Figure 8-77 JMS Queue for Outbound Queue 4



8. Click **Advanced Targeting** button.

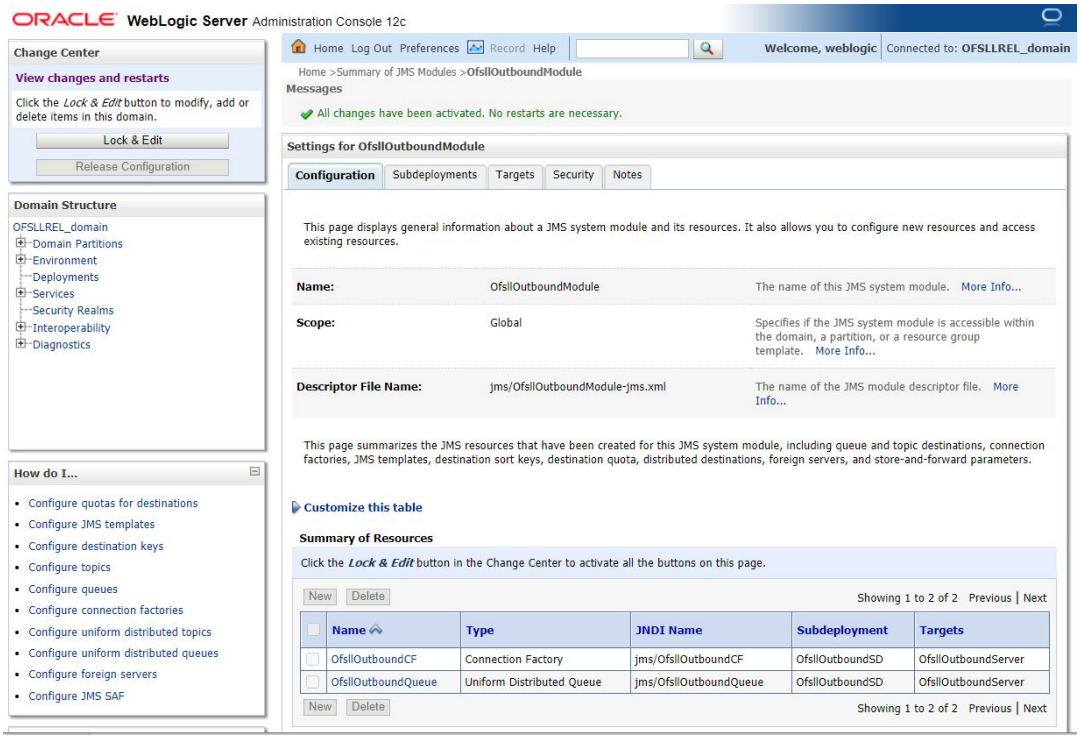
   The following window is displayed.

Figure 8-78 JMS Queue for Outbound Queue 5



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

Figure 8-79 JMS Queue for Outbound Queue 6



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

8.4 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.

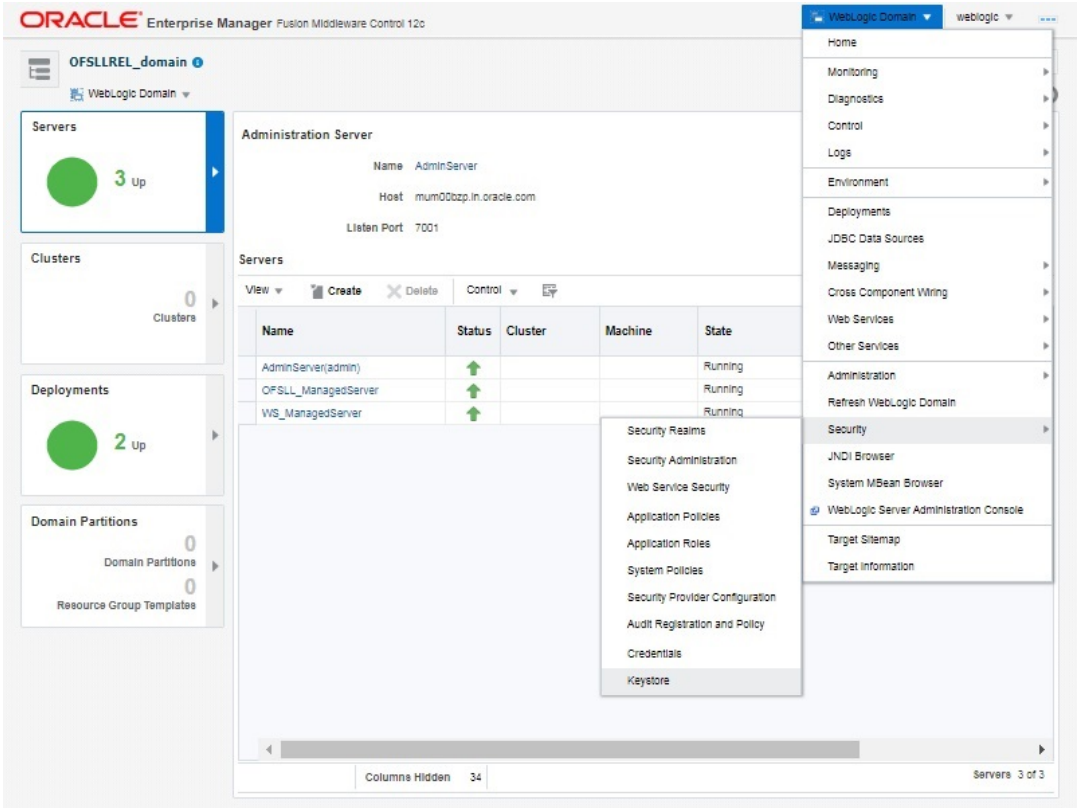
- Configure External Client Certificates

8.4.1 Configure External Client Certificates

Follow the below steps to import the certificates.

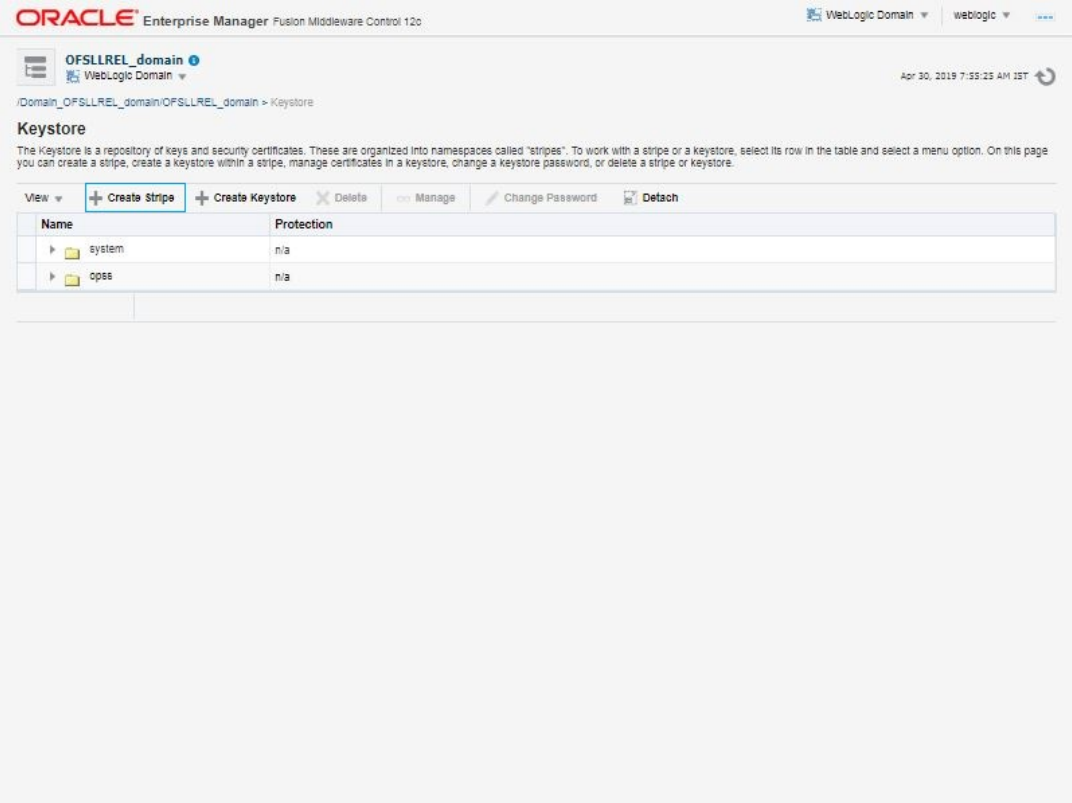
1. Login to the Oracle Enterprise Manager 12c console. (i.e. `http://hostname:port/em`)
2. Click on **Weblogic Domain** drop-down list and navigate to Security > Keystore.

Figure 8-80 Configure Client certificates 1



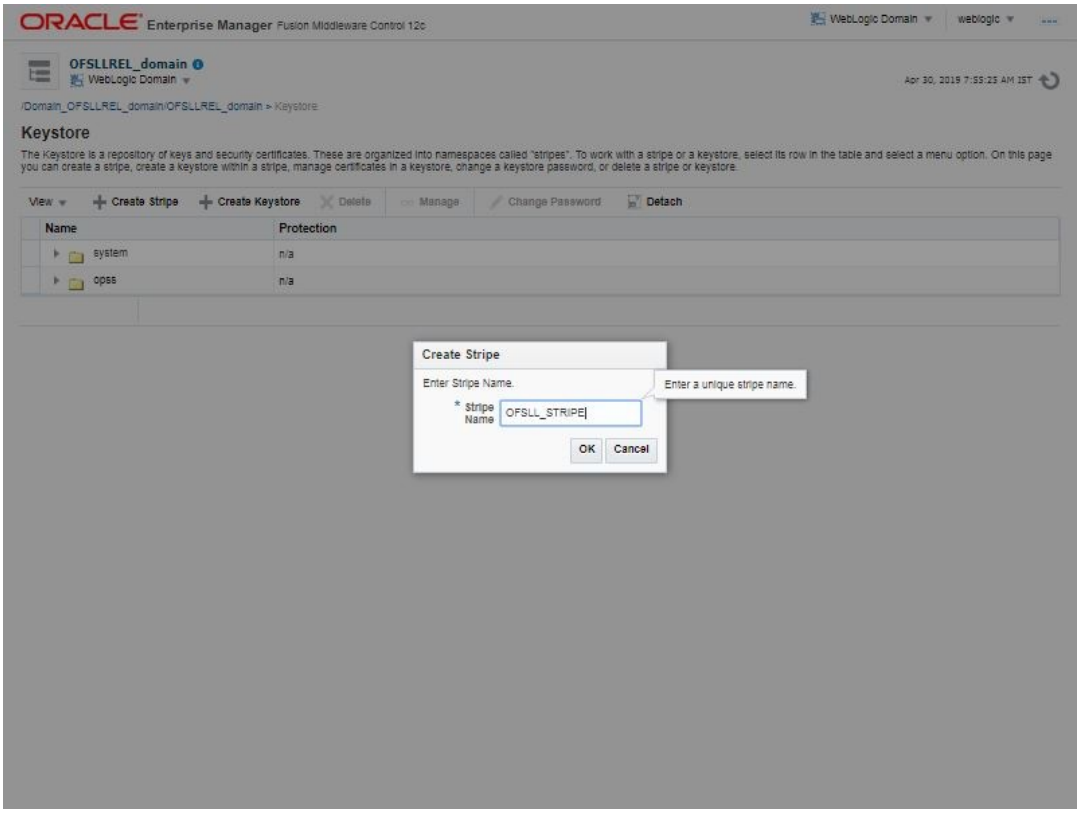
3. Click on **Create Stripe**.

Figure 8-81 Configure Client certificates 2



4. Enter the Stripe Name as **OFSLL_STRIPE**.

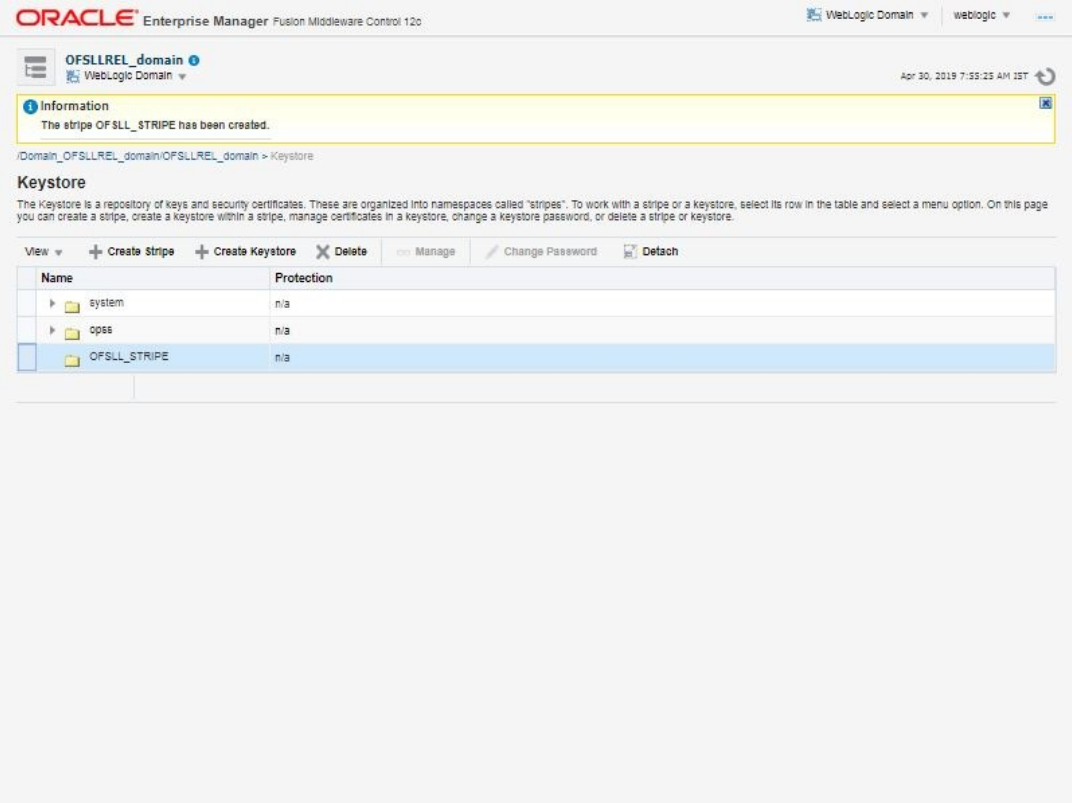
Figure 8-82 Configure Client certificates 3



5. Click **OK**.

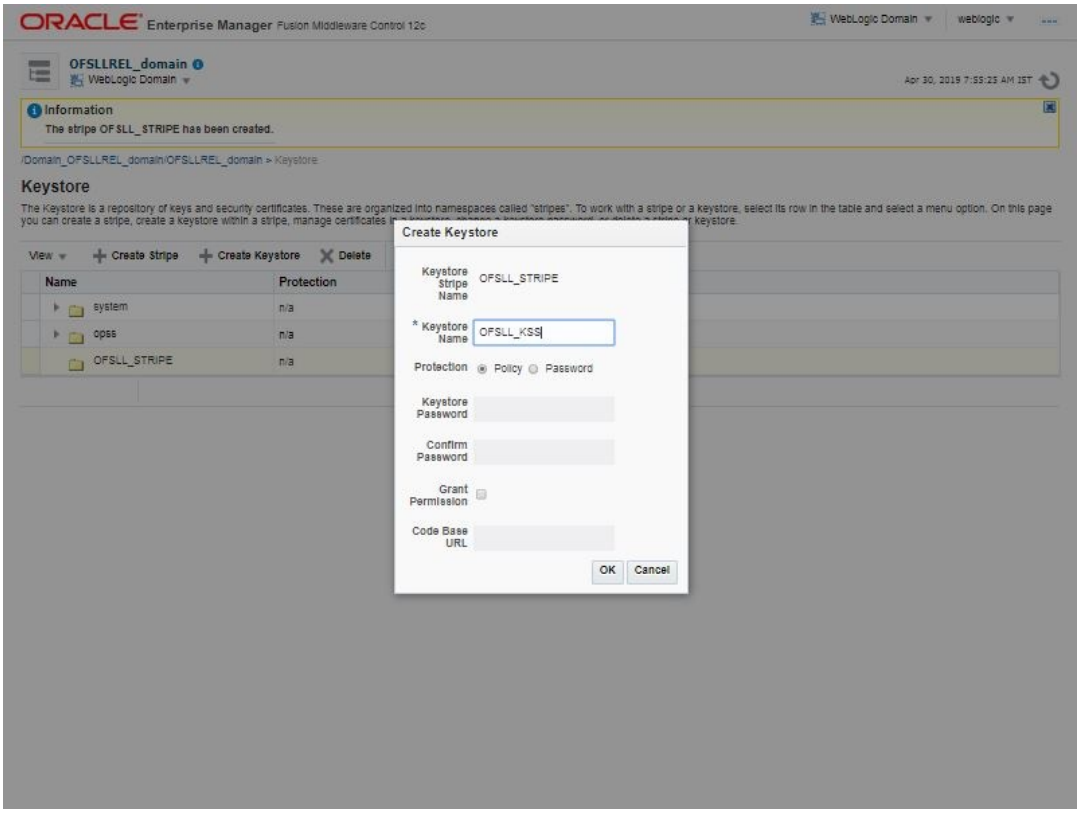
   The following OFSLL_STRIPE is created.

Figure 8-83 Configure Client certificates 4



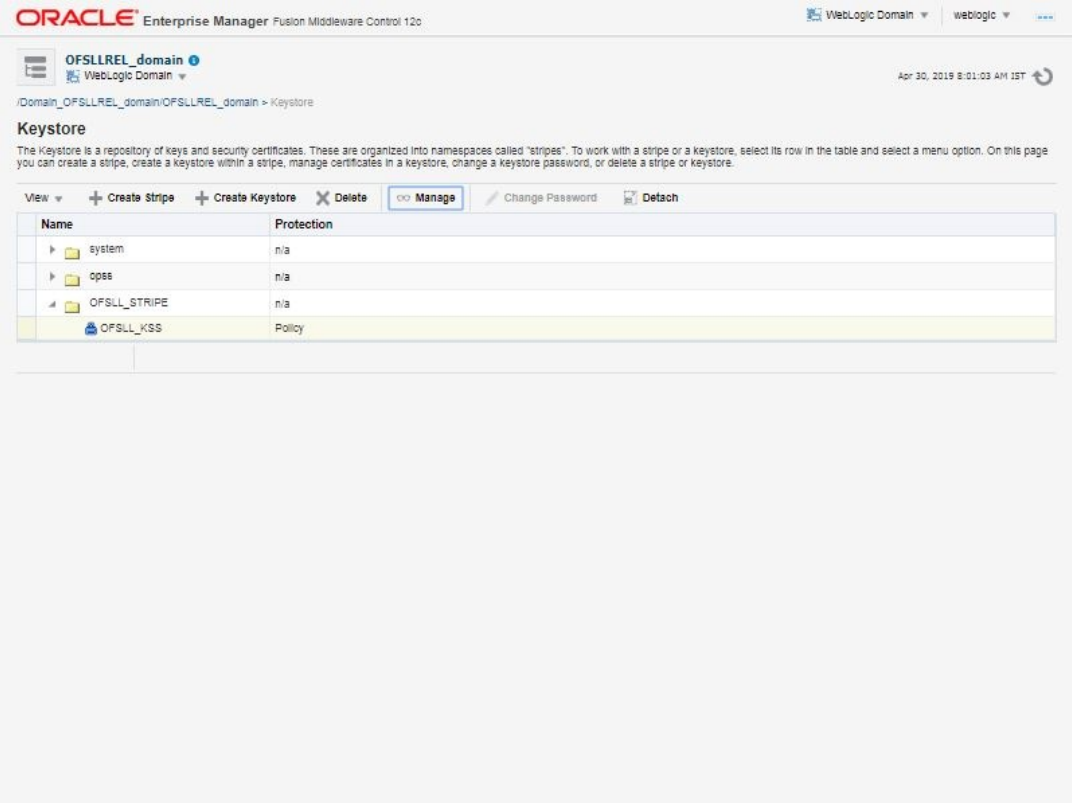
6. Select the newly created **OFSLL_STRIPE** and click **Keystore**.
7. Enter the Keystore Name as **OFSLL_KSS** and click **OK**.

Figure 8-84 Configure Client certificates 5



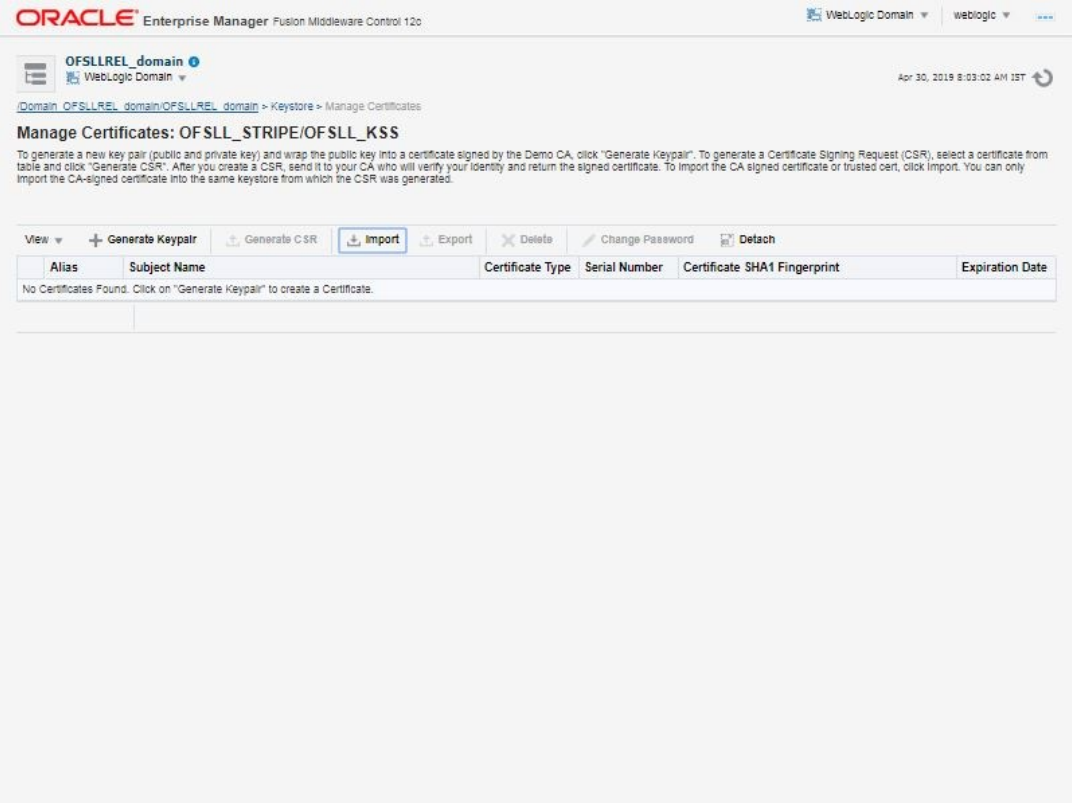
8. Select **OFSLL_KSS** and click **Manage**.

Figure 8-85 Configure Client certificates 6



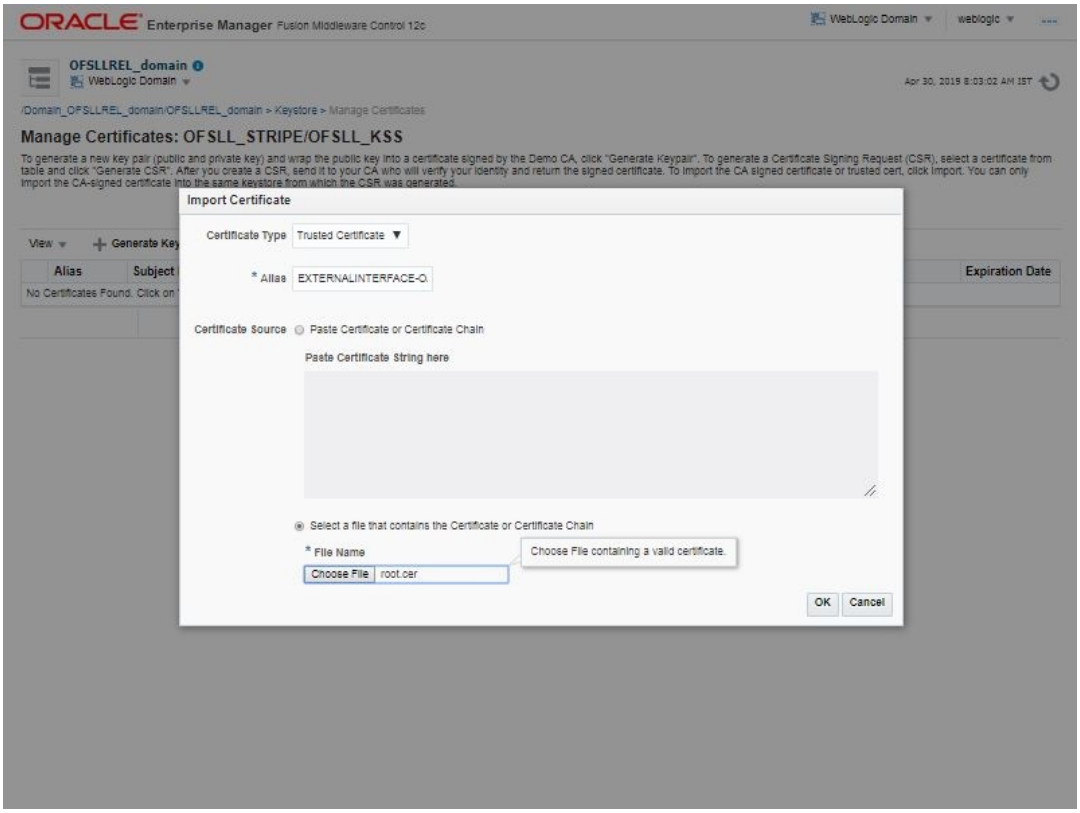
9. Click **Import**.

Figure 8-86 Configure Client certificates 7



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

Figure 8-87 Configure Client certificates 8



11. Click **OK**.

8.5 Create Credentials and System Policies

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

- Create Credentials and System Policies

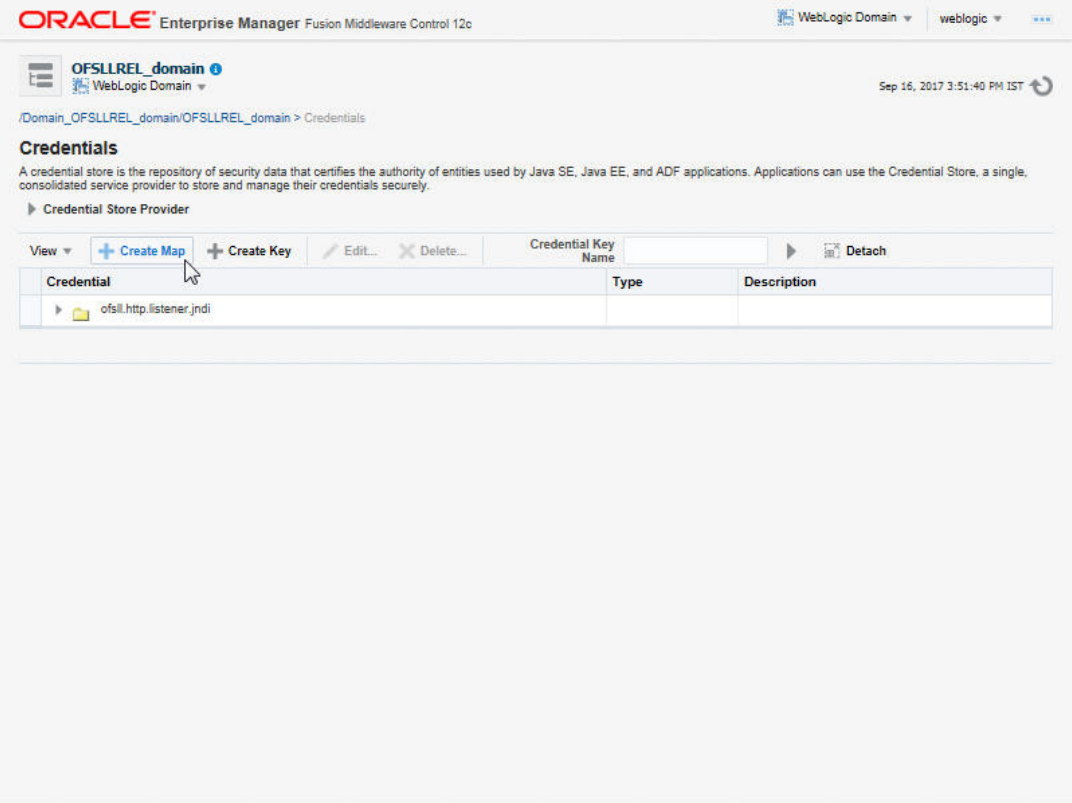
8.5.1 Create Credentials and System Policies

Follow the below steps to create credentials and system policies.

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.

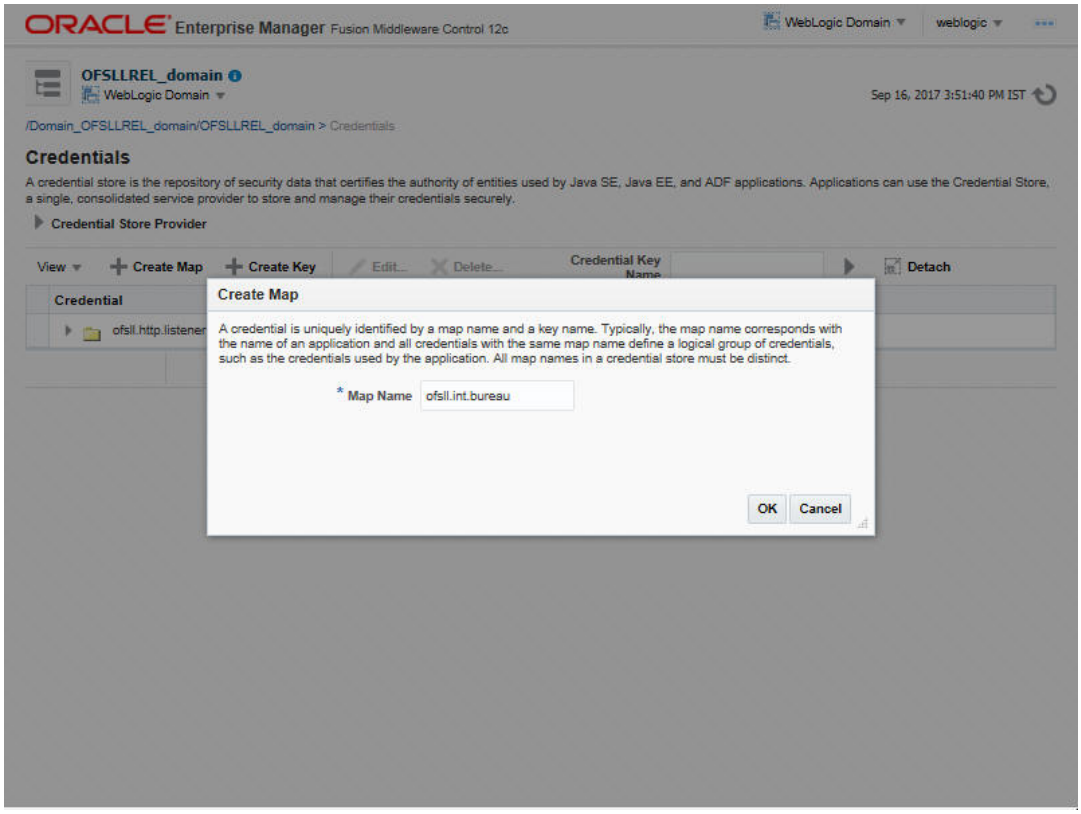
Figure 8-88 Credentials page



3. Click **Create Map**.

   The following window is displayed.

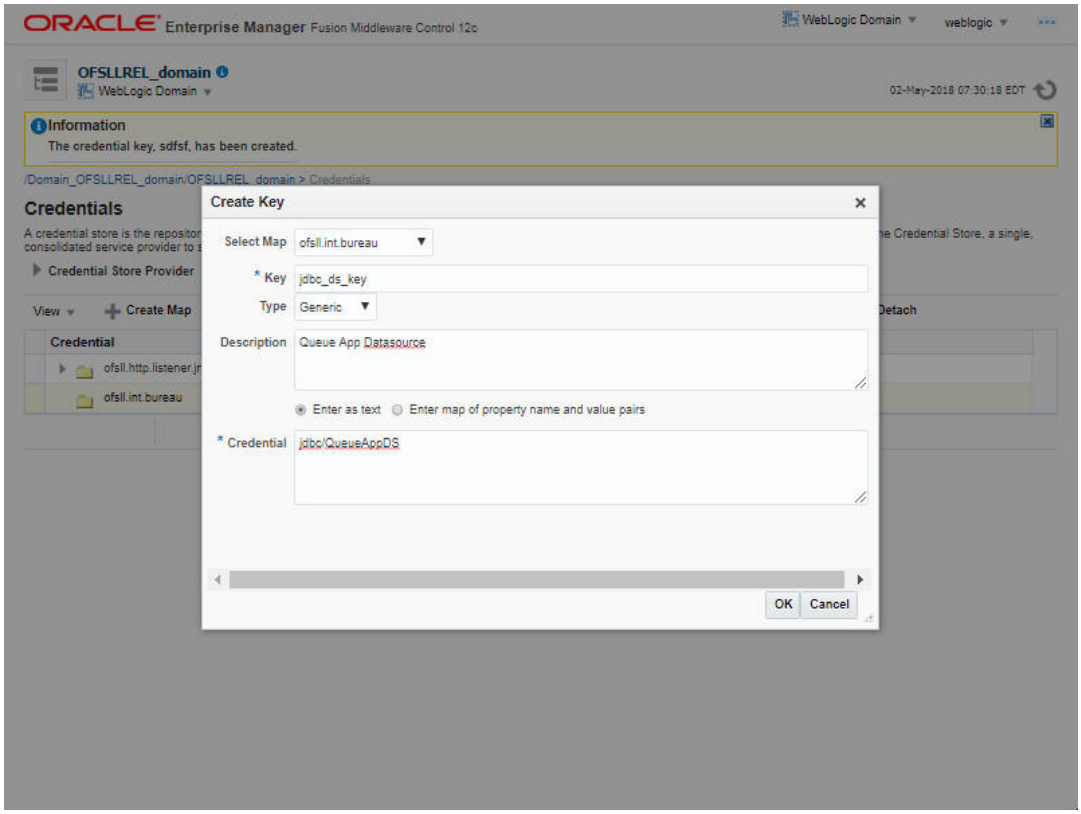
Figure 8-89 Create Map



4. Enter Map Name as **ofsll.int.bureau** and click **OK**.
5. Click **Create Key**.

   The following window is displayed.

Figure 8-90 Create Key



6. Specify the following details:
   - Select Map as **ofsll.int.bureau** from the drop down list.
   - Specify Key as **jdbc_ds_key**
   - Select Type as **Generic** from the drop down list.
   - Specify the Credential as **jdbc/QueueAppDS**
7. Click **OK**.
8. Similarly you need to create the following Maps and corresponding keys as indicated in following table.

Table 8-1 Maps and corresponding keys

Maps	Keys	Description
ofsll.int.bureau		This map is used to setup keys for all credit bureau interfaces
	ProxyServer	Name of the proxyServer to be configured
	ProxyPort	Port to which ProxyServer is running.
	ExpEcalsURL	The Experian Connection URL to be configured.
	ExpDirectExperianEnabled	If you set value as true, then you would be setting ecals response URL. Else, the Ecals request URL

Table 8-1 (Cont.) Maps and corresponding keys

Maps	Keys	Description
	ExpCertPath	The location of `.jks` file which contains the valid certificate for Experian Credit Bureau.
	ExpBusUserNamePassword	Login Credentials to be configured for Experian Business reports.
	ExpConUserNamePassword	Login Credentials to be configured for Experian Consumer reports.
	EfxURL	The Equifax Connection URL to be configured.
	EfxCertPath	The location of `.jks` file which contains the valid certificate for Equifax Credit Bureau.
	EfxUserNamePassword	Login credentials to be configured for accessing Equifax Reports.
	TucCertPath	The location of `.jks` file which contains valid certificate for Transunion Bureau .
	TucCertPassword	The password that requires to read the valid `.jks`certificate for the Transunion Bureau.
	TucUserNamePassword	Login credentials to be configured for accessing Transunion reports
	TucConnectionURL	The Transunion URL to be configured.
	jdbc_ds_key	Datasource configured to retrieve data for bureau.
	source	Configured as EXTERNAL for actual call.
ofsll.int.outbound		This map is used to setup keys for the RouteOne and Dealer track call back from OFSLL.
	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 outbound Resources.
	roPostDealerUsernamePasswd	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

Table 8-1 (Cont.) Maps and corresponding keys

Maps	Keys	Description
	dtPostDealerUsernamePasswd	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
	TorqueItsUserNamePassword	Credentials required to connect to TorqueIts web service
	TorqueItsURL	TorqueIts Decision service URL
	ProxyHost	Name of the proxyServer to be configured.
	ProxyPort	Port to which ProxyServer is running.
ofsll.int.bip		This Map is used to setup all the Keys required to setup interface with BIP to generate reports.
	local_top_dir	Define the path of the local BIP server where you would like place the generated BIP reports.
	email_from_addr	Define the From Email address to be used while sending email for the generated BIP reports.
	emailBodyContentPath	The path for `file.properties`file that contains the content of the subject and body required while sending letter, report or correspondence as mail to the applicant or producer. For example; /tmp/file.properties *Refer to note below for details on `file.properties`file creation for email configuration.
	fax_server	Configure the name of Fax server to be used to fax the generated BIP reports.
	jdbc_ds_key	Datasource configured to retrieve data for BIP.
ofsll.int.filetransfer		This map is used to setup keys for all credit bureau interfaces
	sftp_key	Credentials to login to SFTP server(Username/Password)
	sftp_top_dir	Top root directory for SFFTP server
	sftp_servers	SFTP server names

Table 8-1 (Cont.) Maps and corresponding keys

Maps	Keys	Description
ofsll.int.security	bip_key	This is BIP login credentials
ofsll.int.gri	GriURL	GRI web service URL to be configured.
	GriAPIKey	GRI API key to be configured
	ProxySet	System Level Proxy Enabled/ Disabled. Value can be either true or false. True= proxy required False = proxy not required
	ProxyHost	Name of the proxyServer to be configured. Set only if ProxySet =true.
	ProxyPort	Port on which ProxyServer is running. Set only if ProxySet =true.
	jdbc_ds_key	Datasource configured to retrieve the request XML for GRI.
	GriCertPath	The location of `.jks` file which contains the valid certificate for GRI. Configure only when a valid certificate is available.
ofsll.int.common		This map is used to setup keys for common JMS Queue
	OfsllJMSQueueJNDI	The JMS queue JNDI name to be configured
	OfsllJMSQueueCF	The JMS queue connection factory to be configured
	OfsllJMSServerURL	The JMS server url to be configured. Ex: t3://<JMS server host>:<JMS server port>
	outbound_jms_queue_con_factory	The JMS connection factory to be configured. jms/OfsllOutboundCF
	outbound_jms_queue	The JMS queue to be configured. jms/OfsllOutboundQueue
	weblogic_cluster_ind	This is to be configured based on the environment i.e. for weblogic cluster environment set it as **Y**. Else, set it to **N**.

Table 8-1 (Cont.) Maps and corresponding keys

Maps	Keys	Description
	outbound_jms_queue_provider_url	The JMS server url to be configured. Ex: For non clustered environment - t3://<JMS server host>:<JMS server port> Ex: For clustered environment - t3://<JMS server host>:<JMS server port>,<JMS server host>:<JMS server port>
ofsll.int.webhook	jdbc_ds_key	Datasource configured to retrieve data for Webhook.

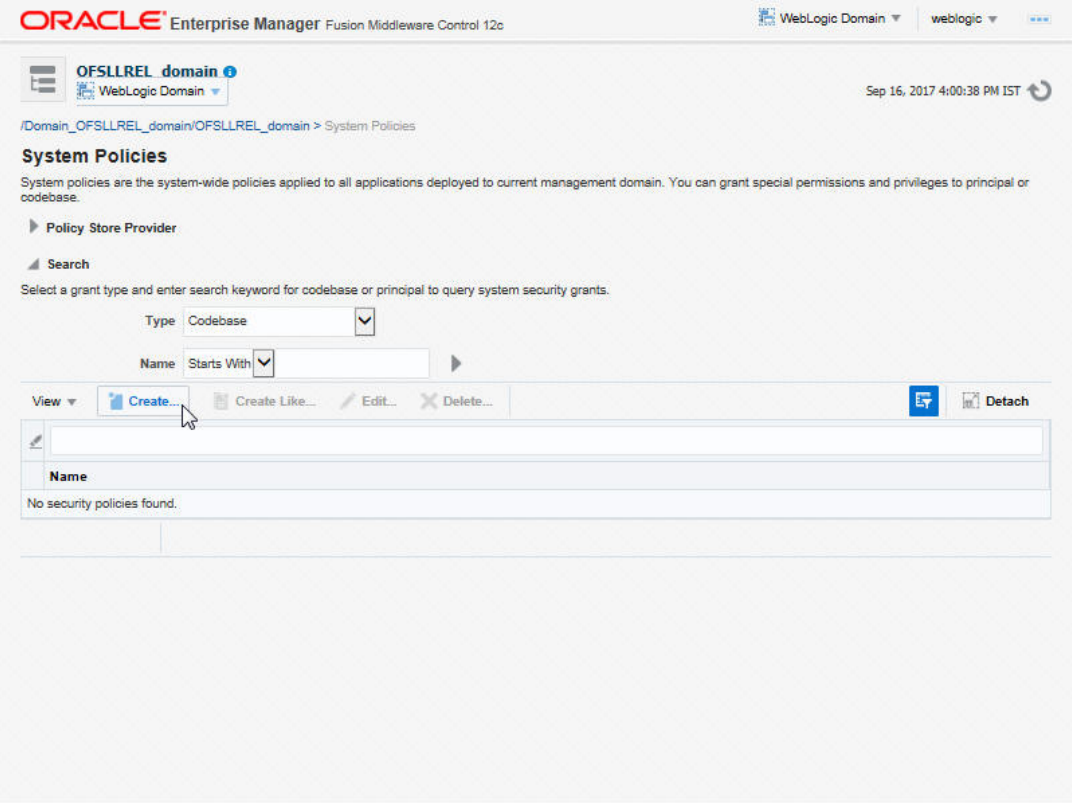
* A new file(`file.properties`) needs to be created and copied to the application server in the same path as mentioned in the value corresponding to the key **emailBodyContentPath** under the map **ofsll.int.bip**. The file should have the following contents:

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

9. On the left panel, right click on OFSLLREL_domain and select Security > System Policies.

   The following window is displayed.

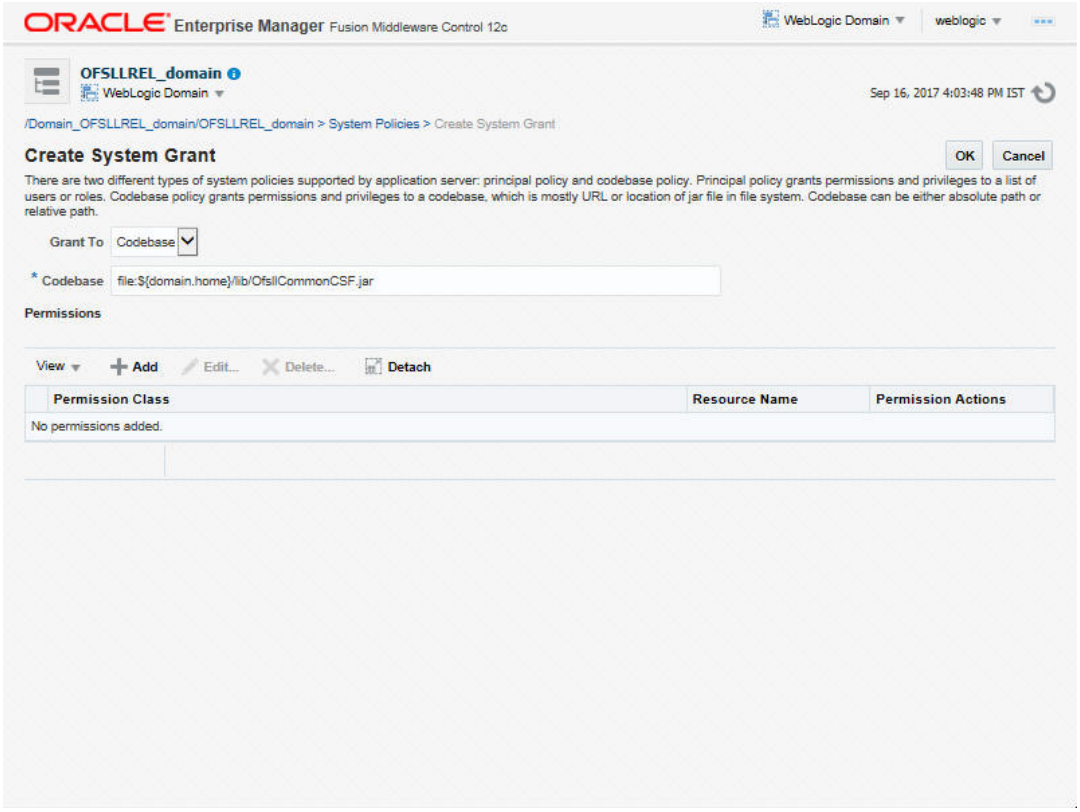
Figure 8-91 System Policies



10. Click **Create**.

    The following window is displayed.

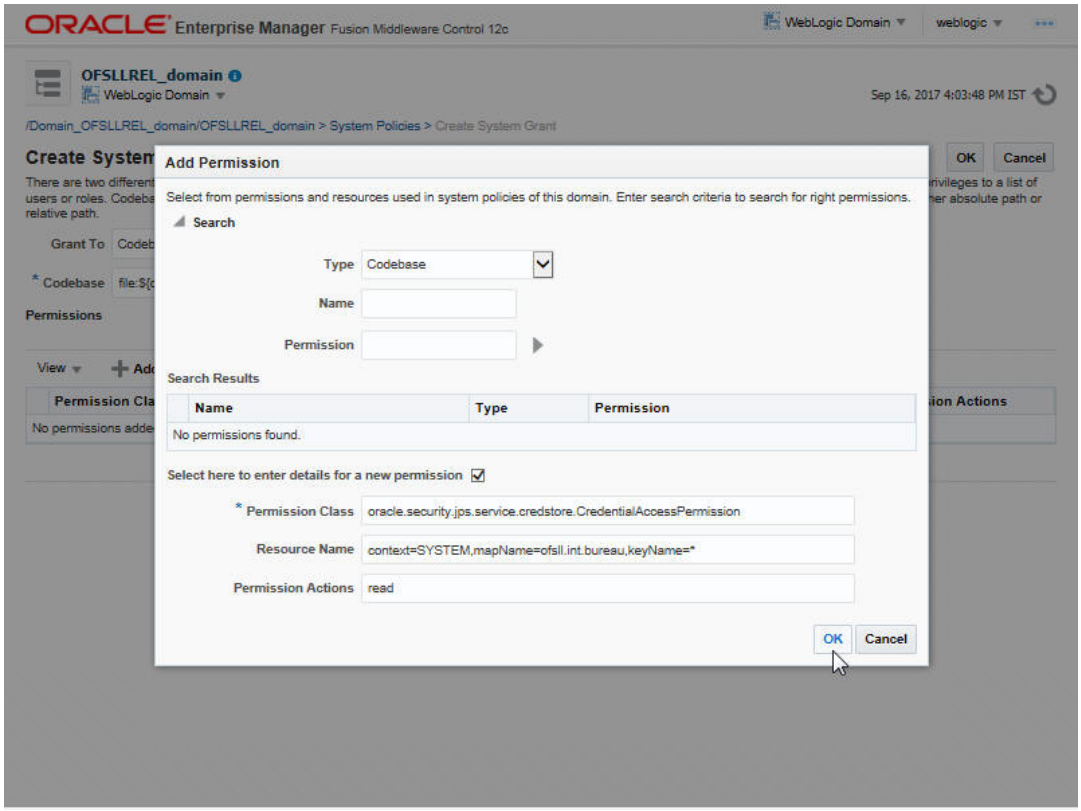
Figure 8-92 Create System Grant



11. Enter the codebase as `file:${domain.home}/lib/OfsllCommonCSF.jar`.
12. Click **Add**.

    The following window is displayed.

Figure 8-93 Add permission



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

Table 8-2 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

Table 8-2 (Cont.) Permission Class

Permission Class	Resource Name	Permission Actions
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**.

8.6 Deploy MDB EJB

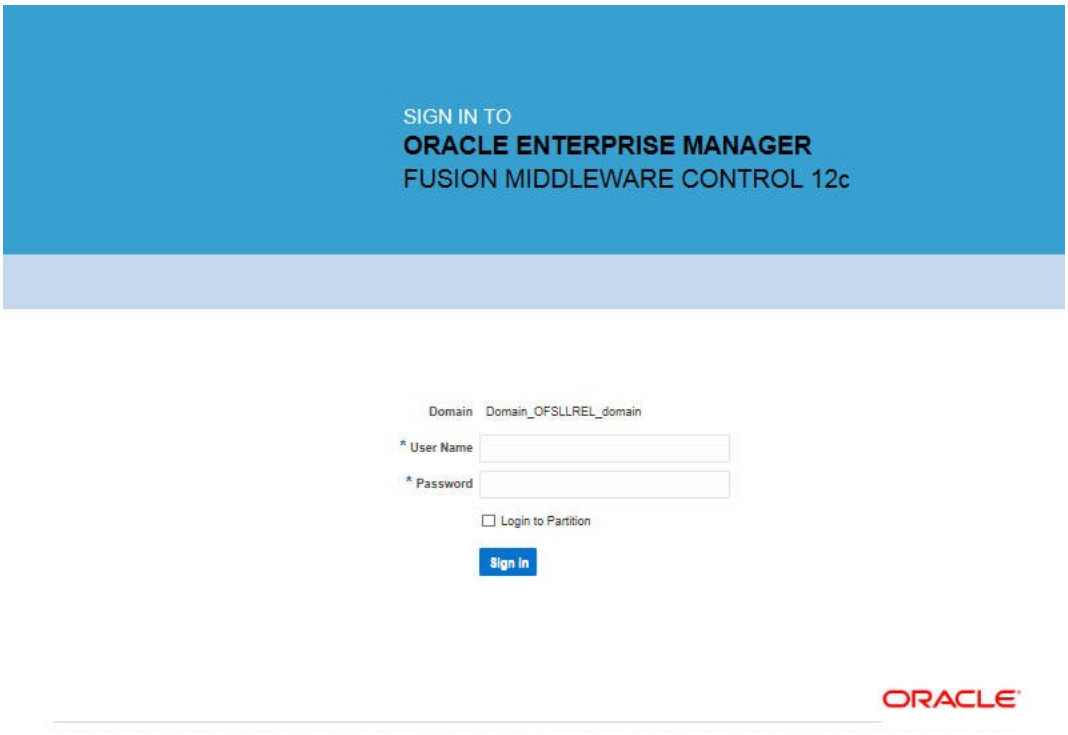
The following section details the steps to be followed to deploy MDB EJB.

- Deploy MDB EJB

8.6.1 Deploy MDB EJB

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

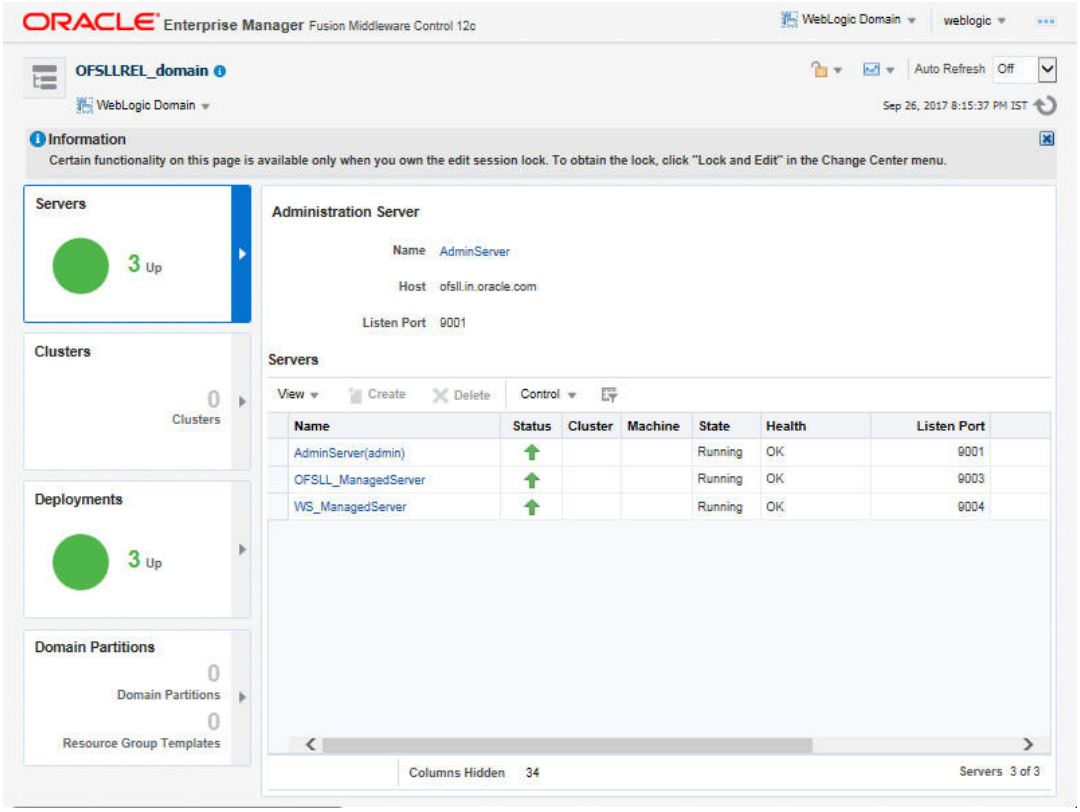
Figure 8-94 Deploy MDB EJB 1



2. Enter valid login credentials.

   The following window is displayed.

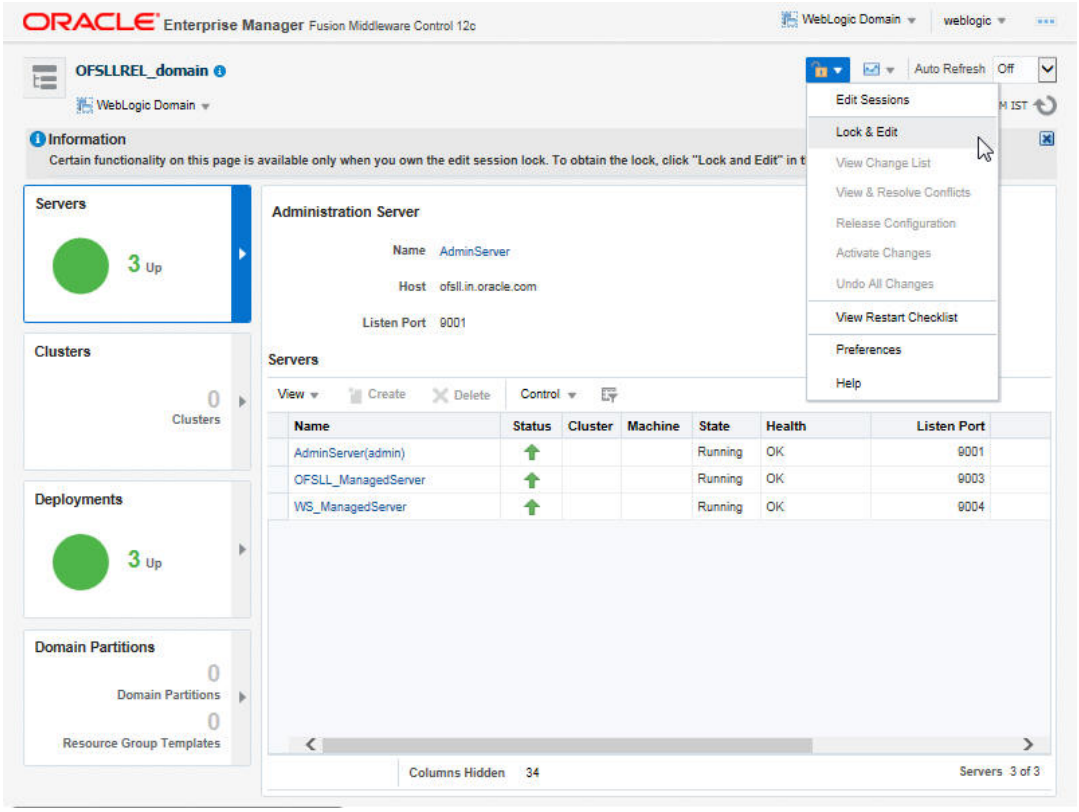
Figure 8-95 Deploy MDB EJB 2



3. Select **Lock & Edit** option in the lock drop-down list available in the header.
4. Click **Deployment** in the left panel.

   The following window is displayed.

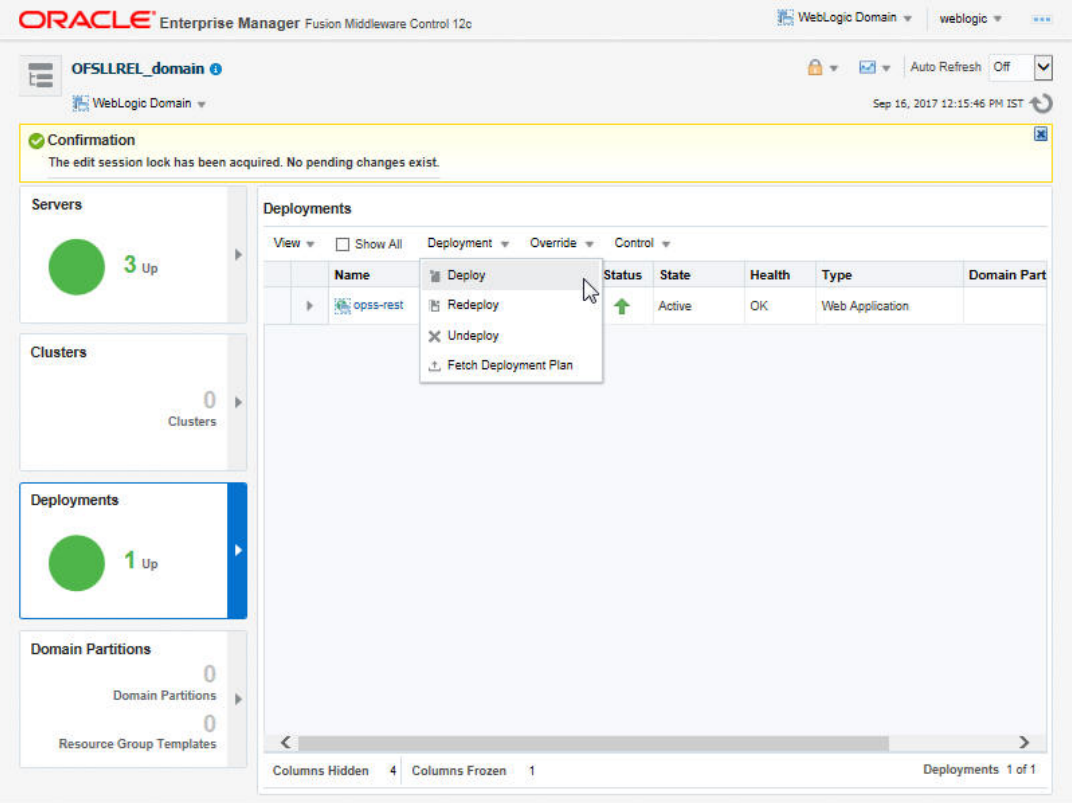
Figure 8-96 Deploy MDB EJB 3



5. Select **Deploy** from the Deployment drop-down list.

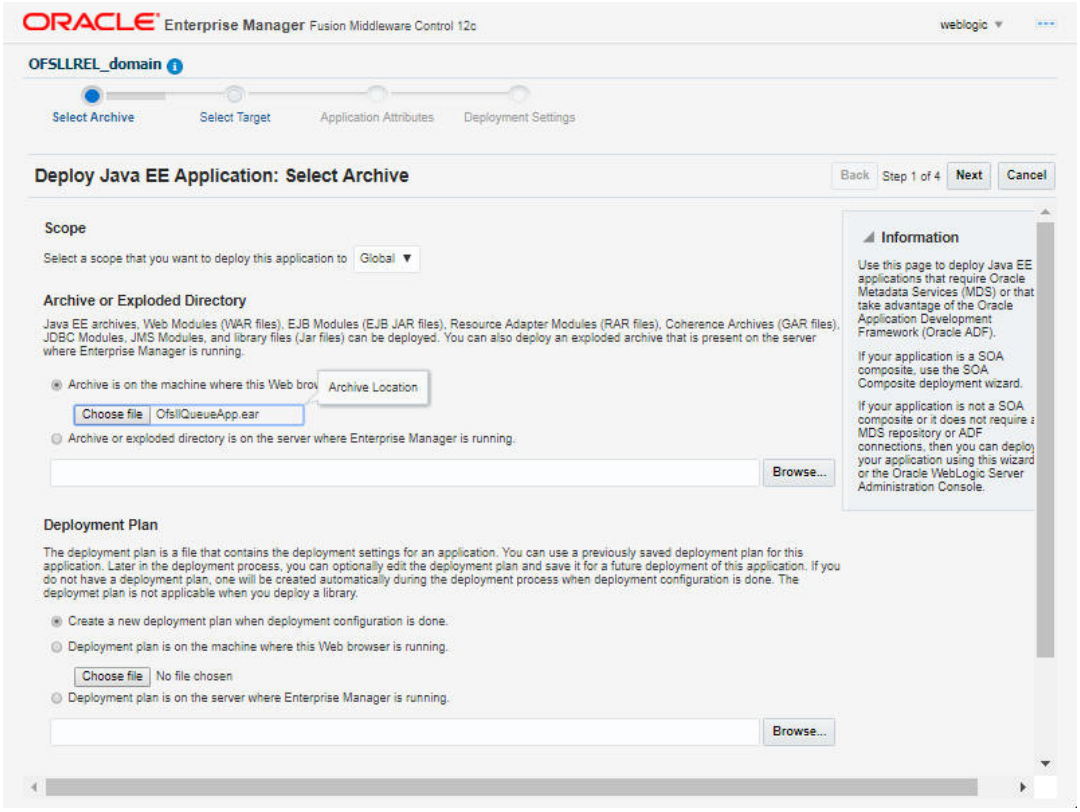
   The following window is displayed.

Figure 8-97 Deploy MDB EJB 4



6. The following window is displayed.

Figure 8-98 Deploy MDB EJB 5



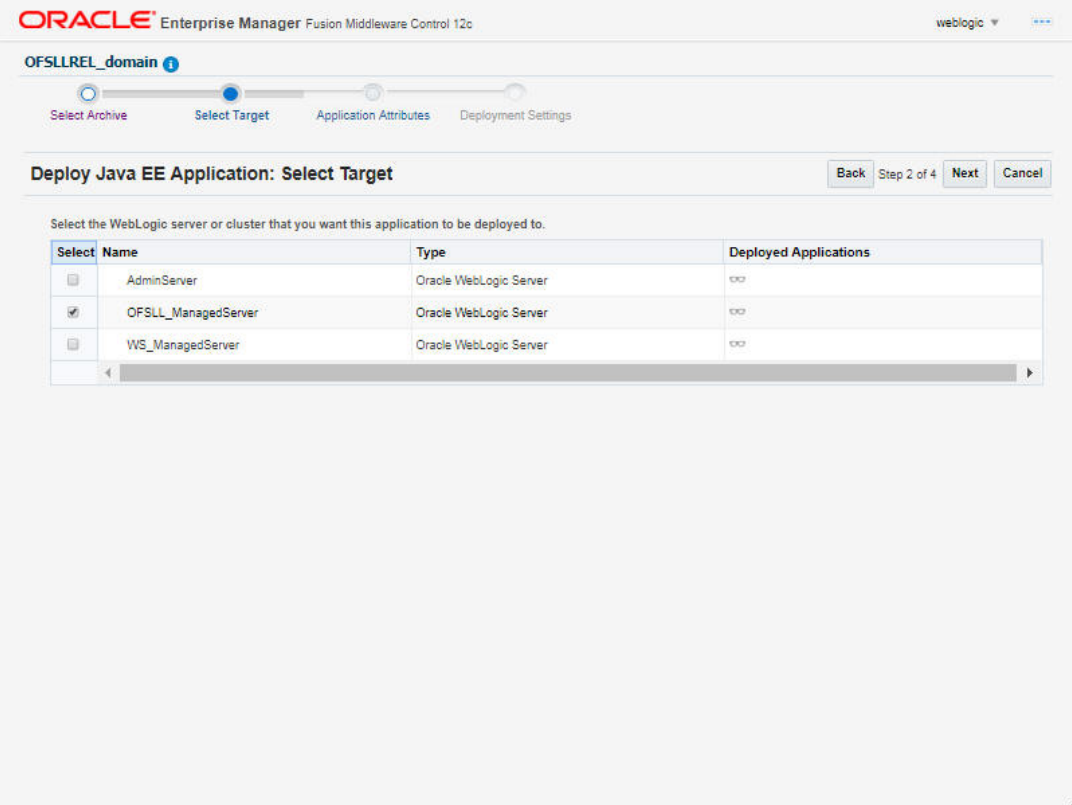
7. Browse to the folder containing the MDB EJB.

   Eg: `C:/OfsllQueueApp.ear`

8. Click **Next**.

   The following window is displayed.

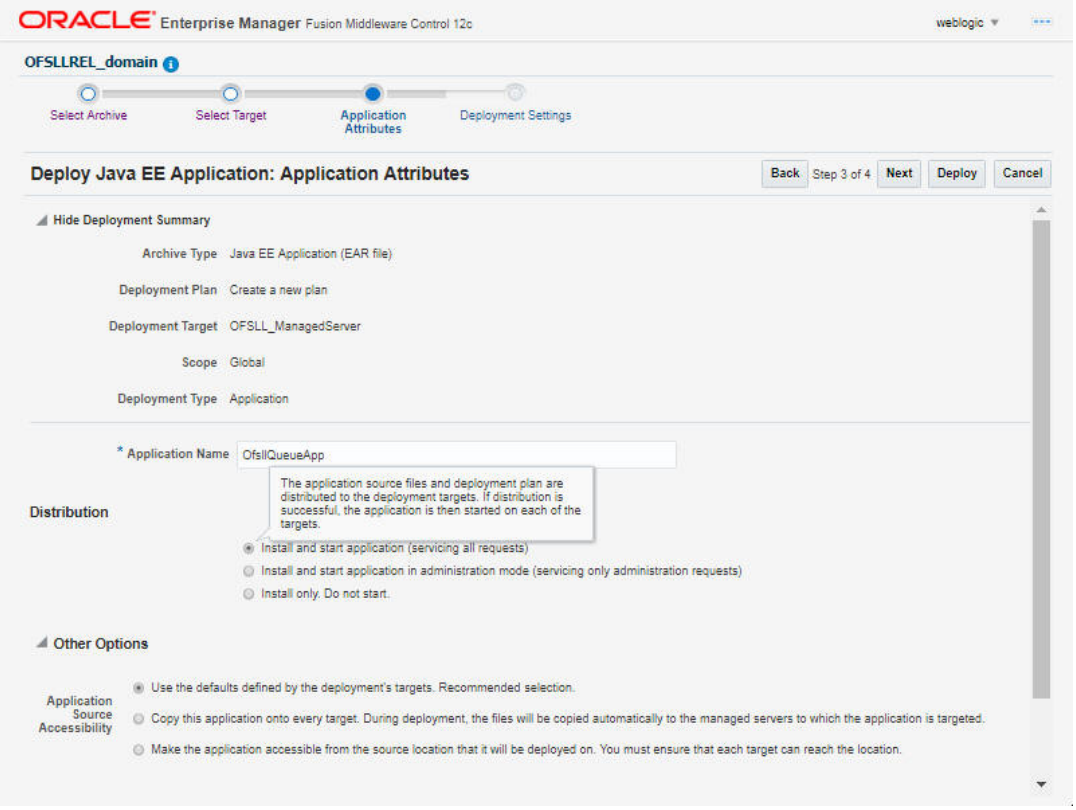
Figure 8-99 Deploy MDB EJB 6



9. Select the server on which the MDB EJB needs to be deployed.
10. Click **Next**.

    The following window is displayed.

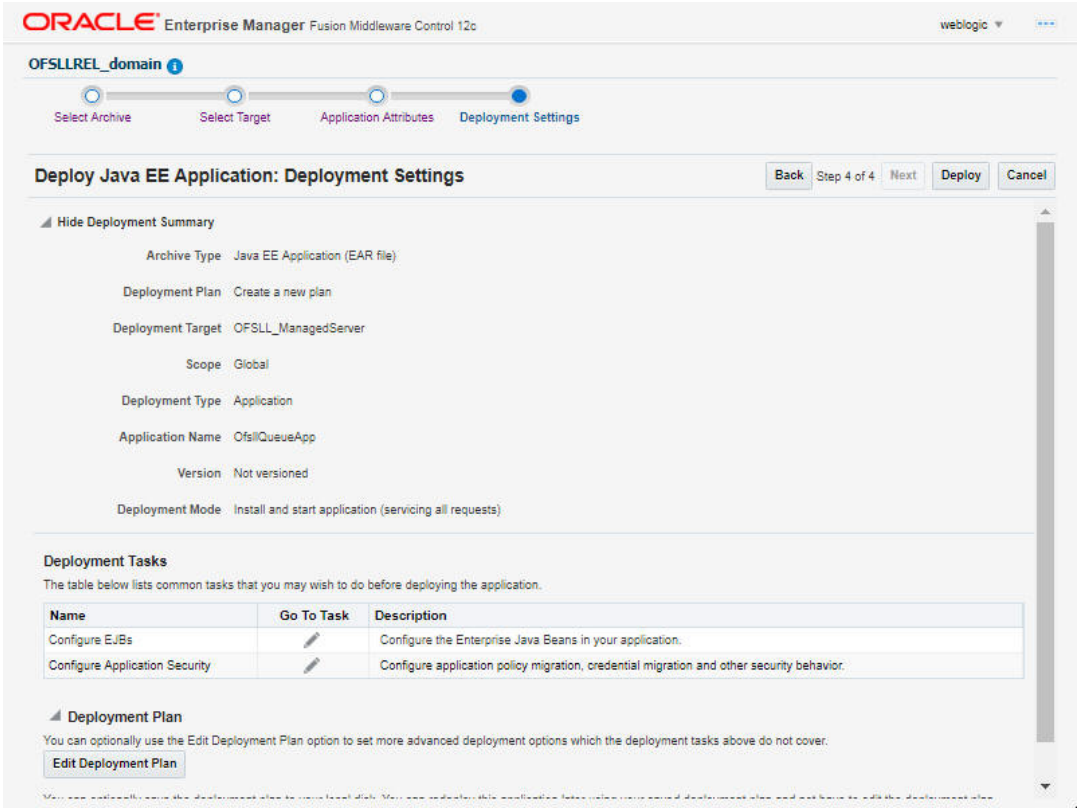
Figure 8-100 Deploy MDB EJB 7



11. Select the option **Install and start application (servicing all requests)**.
12. Check the context root and click **Next**.

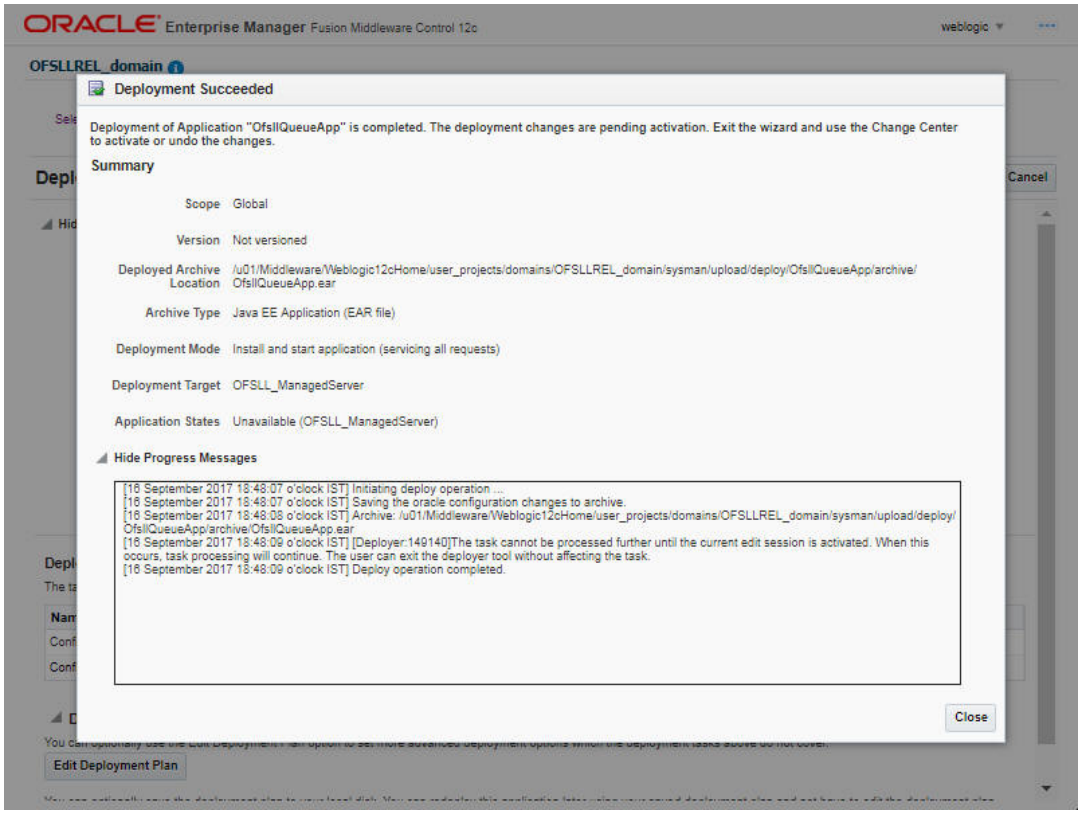
    The following window is displayed.

Figure 8-101 Deploy MDB EJB 8



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

Figure 8-102 Deploy MDB EJB 9



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 **-DUseSunHttpHandler=true** to enforce the weblogic server to uses SUN SSL implementation.

9

Configure Oracle Analytics Publisher for Application

The following sections details the steps to be followed to configure Oracle analytics publisher for application.

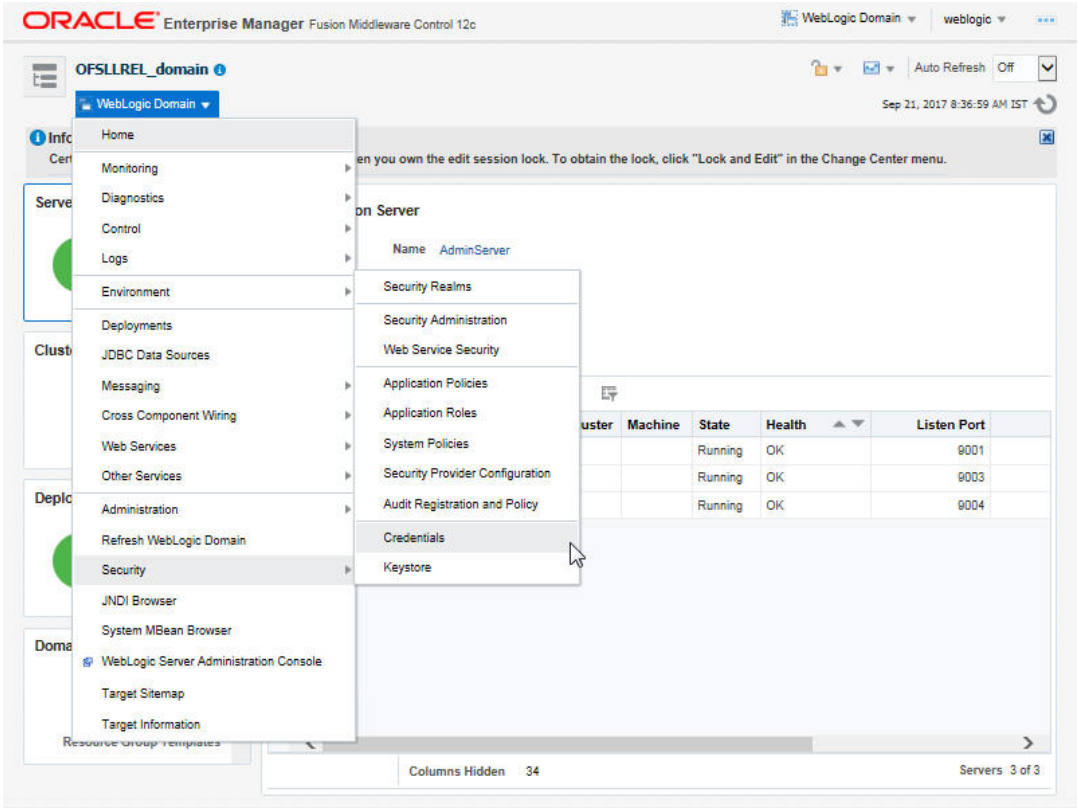
- Configuring Oracle Analytics Publisher for Application
- Configuring JNDI Name for http Listener

9.1 Configuring Oracle Analytics Publisher for Application

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

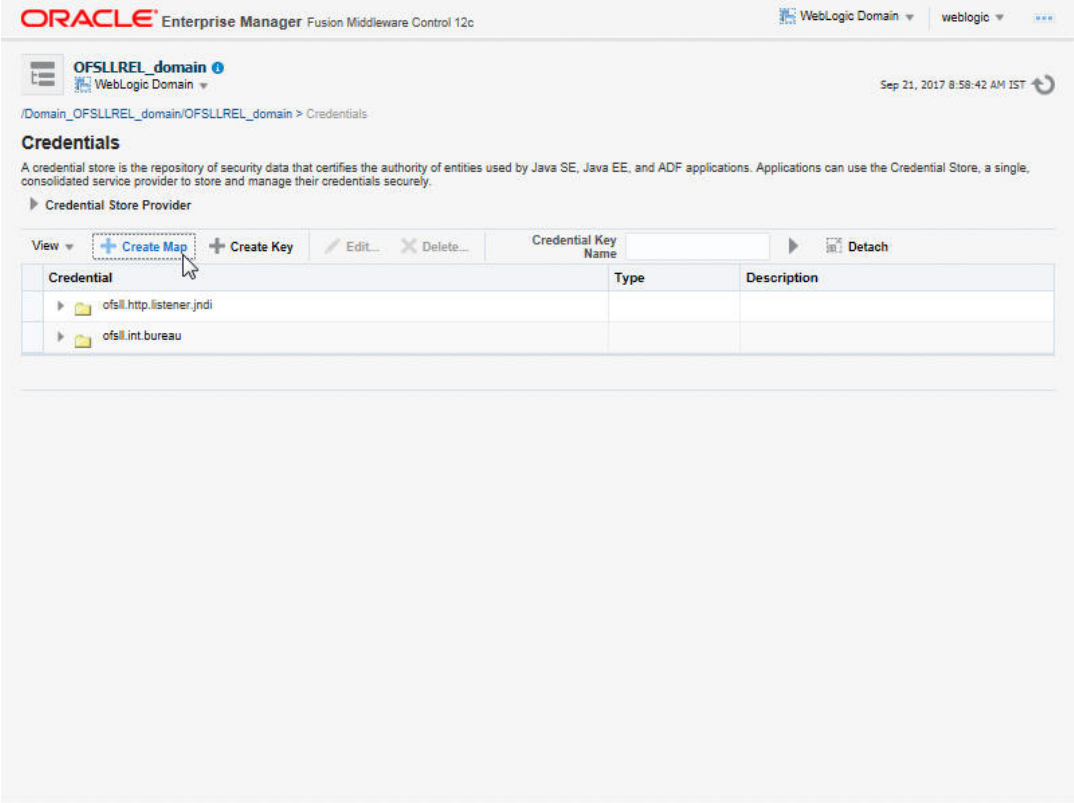
> **Note:**
>
> It is assumed that BI Publisher is installed and configured. Refer BI Publisher Guide for further details.

Figure 9-1 BI Publisher 1



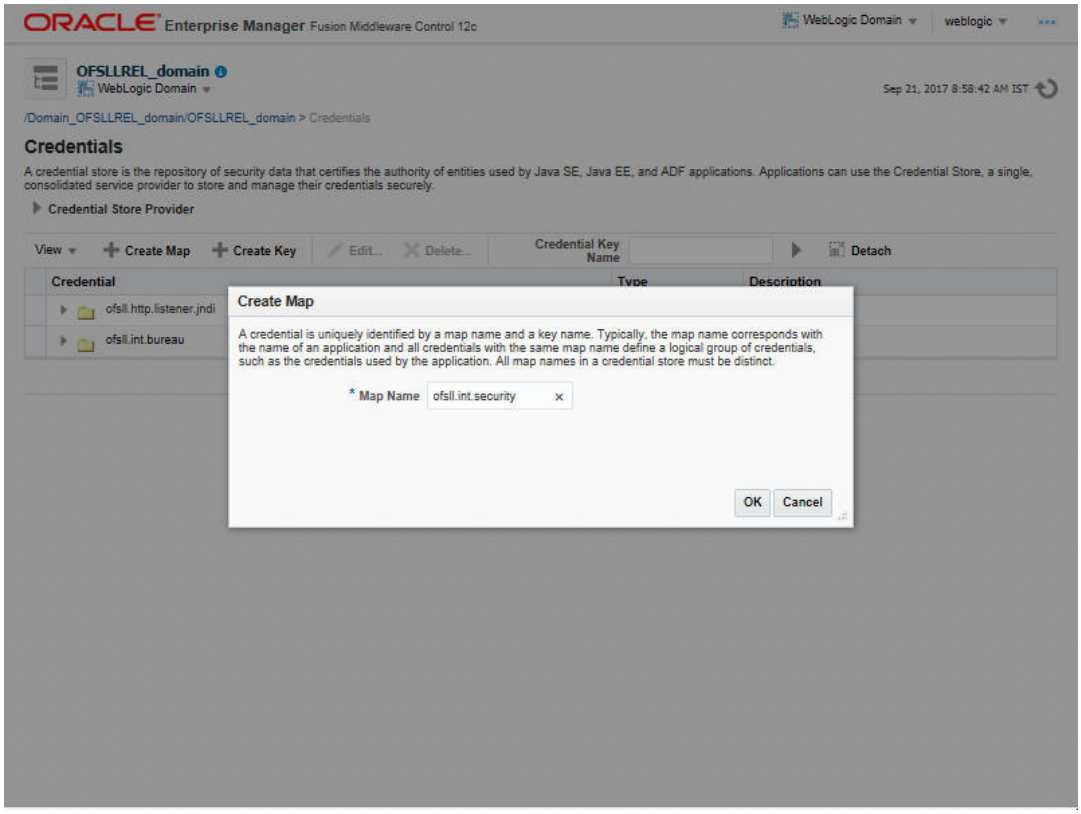
4. Click **WebLogic Domain** on the right panel. Select Security > Credentials. Click **Create Map**.

Figure 9-2 BI Publisher 2



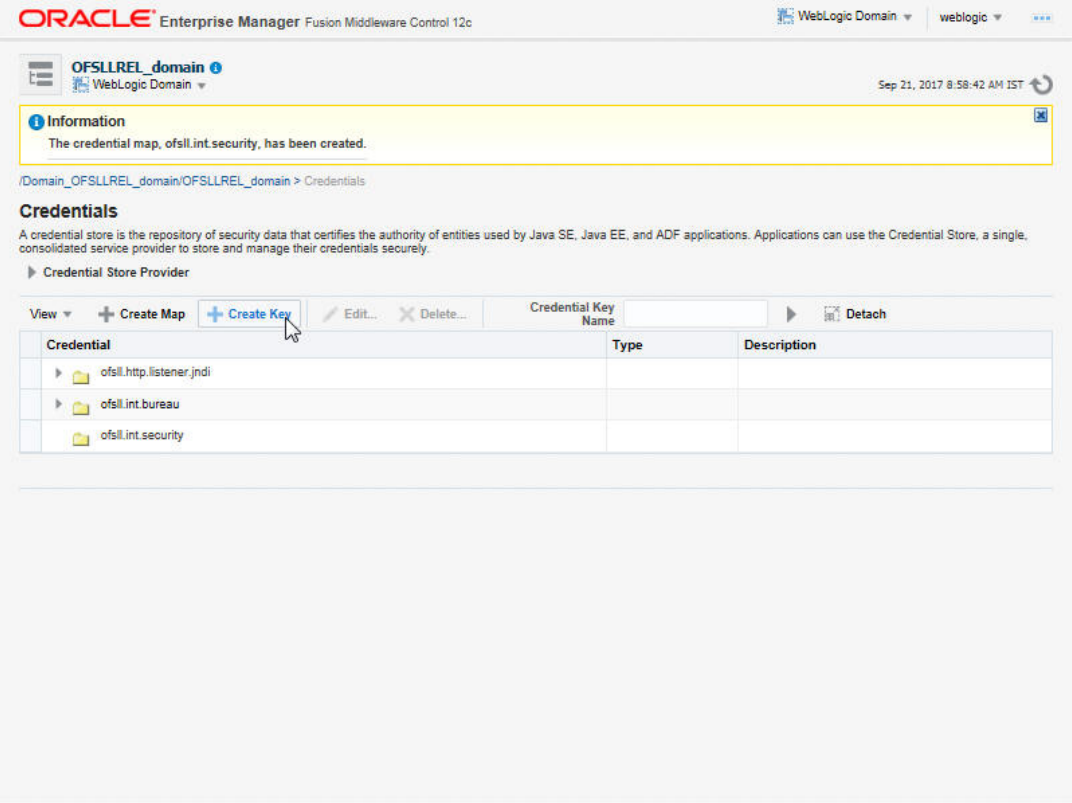
5. Enter the Map Name: ofsll.int.security.

Figure 9-3 BI Publisher 3



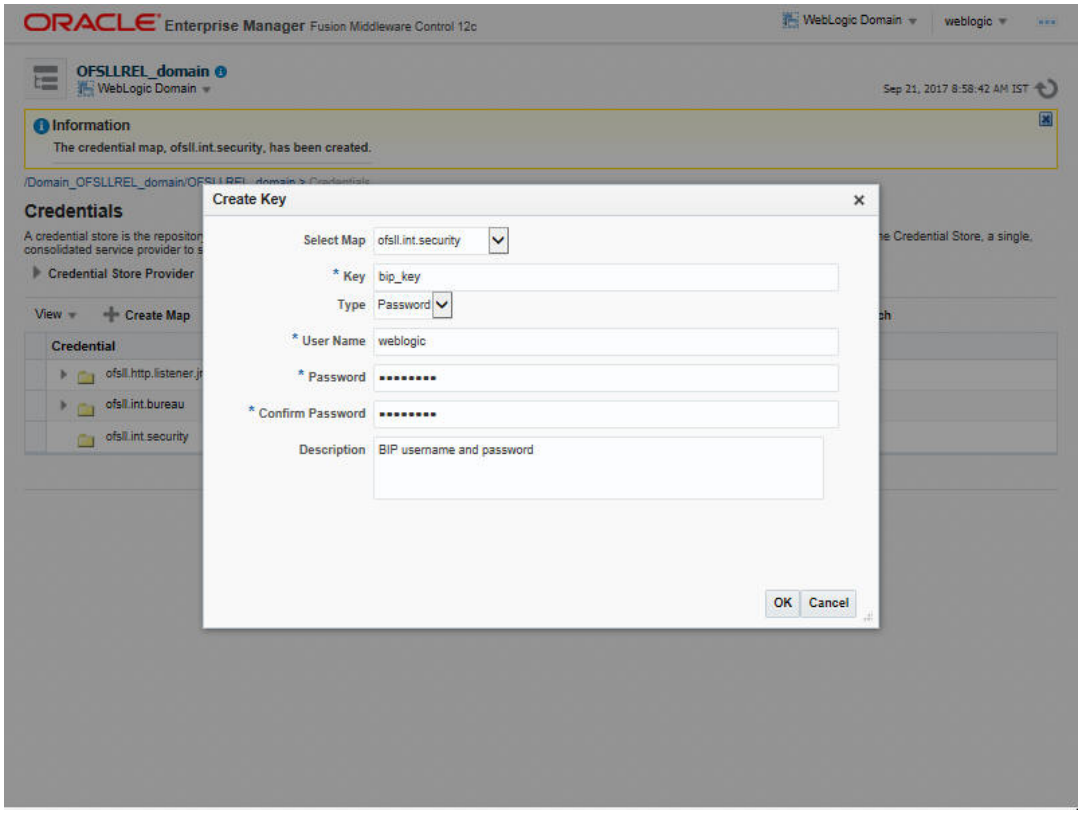
6. Click **OK**.

Figure 9-4 BI Publisher 4



7. Click **Create Key** Button.
8. Enter the details as per your requirement. Specify **User Name** and **Password** of BI Publisher console.

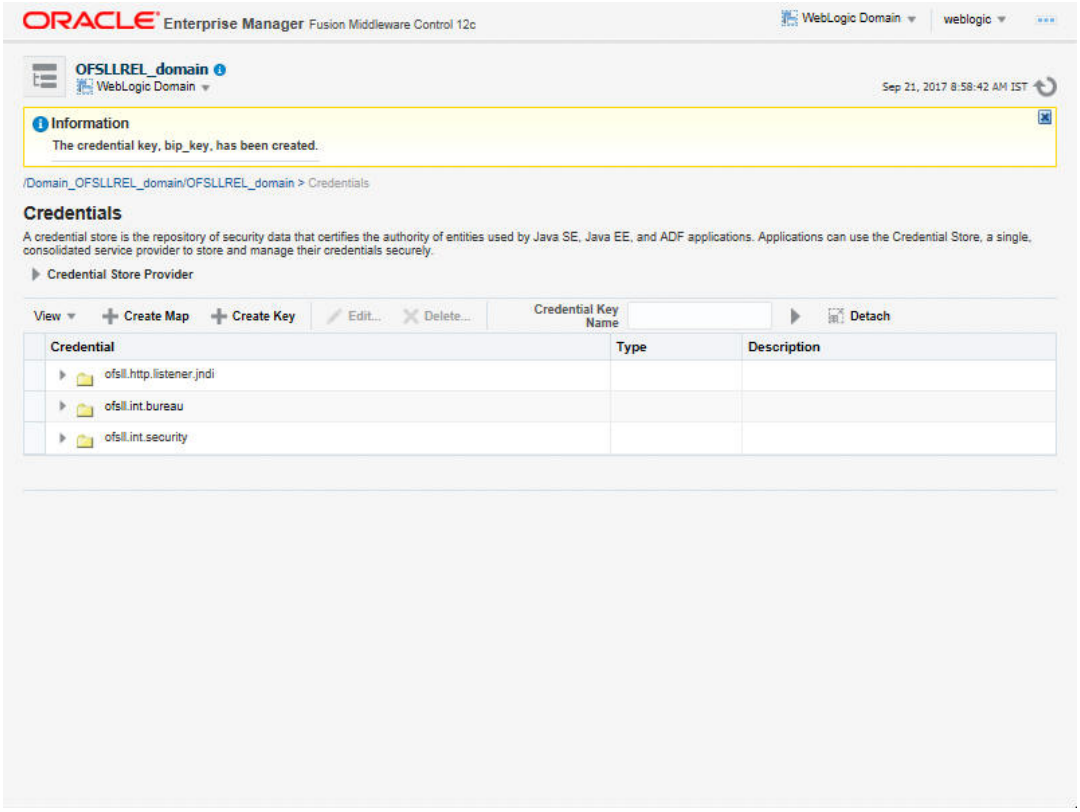
Figure 9-5 BI Publisher 5



9. Click **OK**.

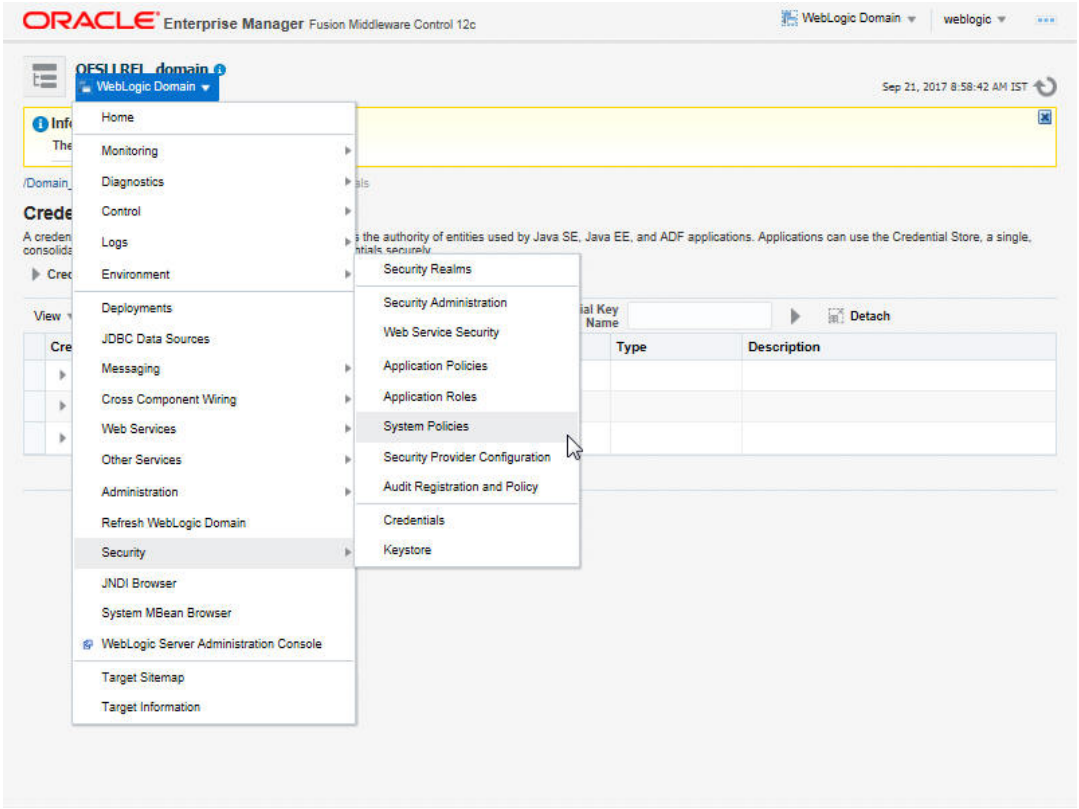
   The following window is displayed.

Figure 9-6 BI Publisher 6



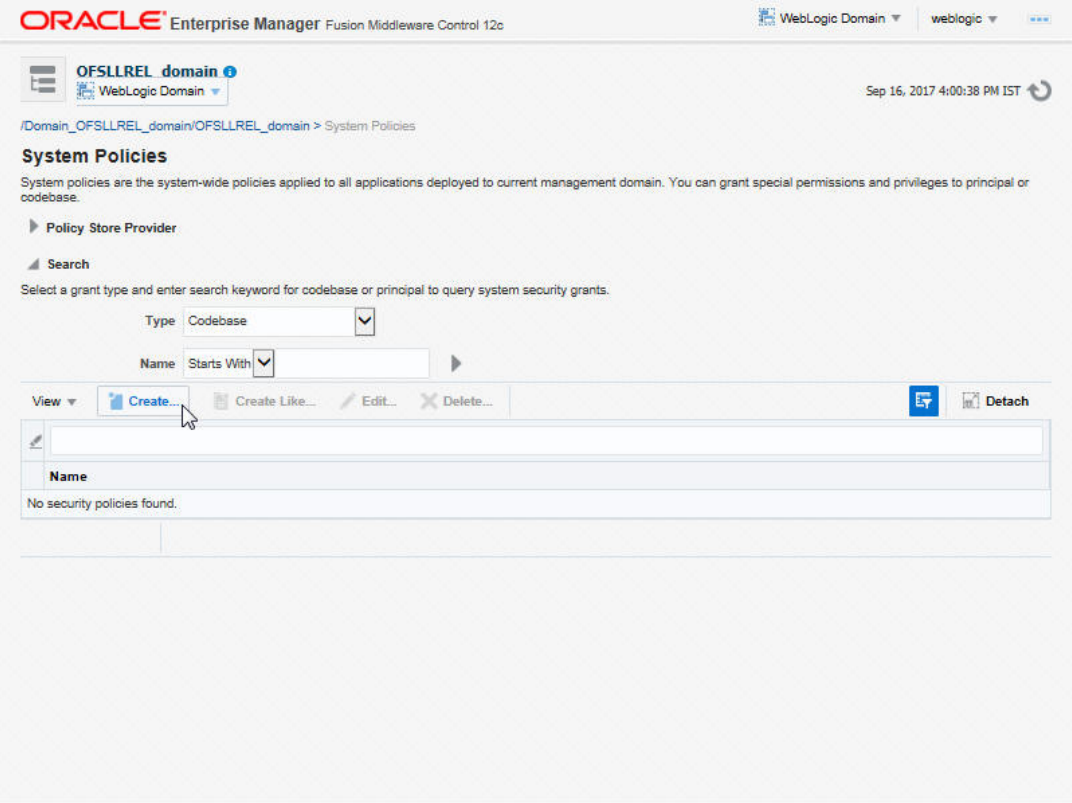
10. On the left panel, right click on the domain OFSLL_domain > Security > System Policies. The following window is displayed.

Figure 9-7 BI Publisher 7



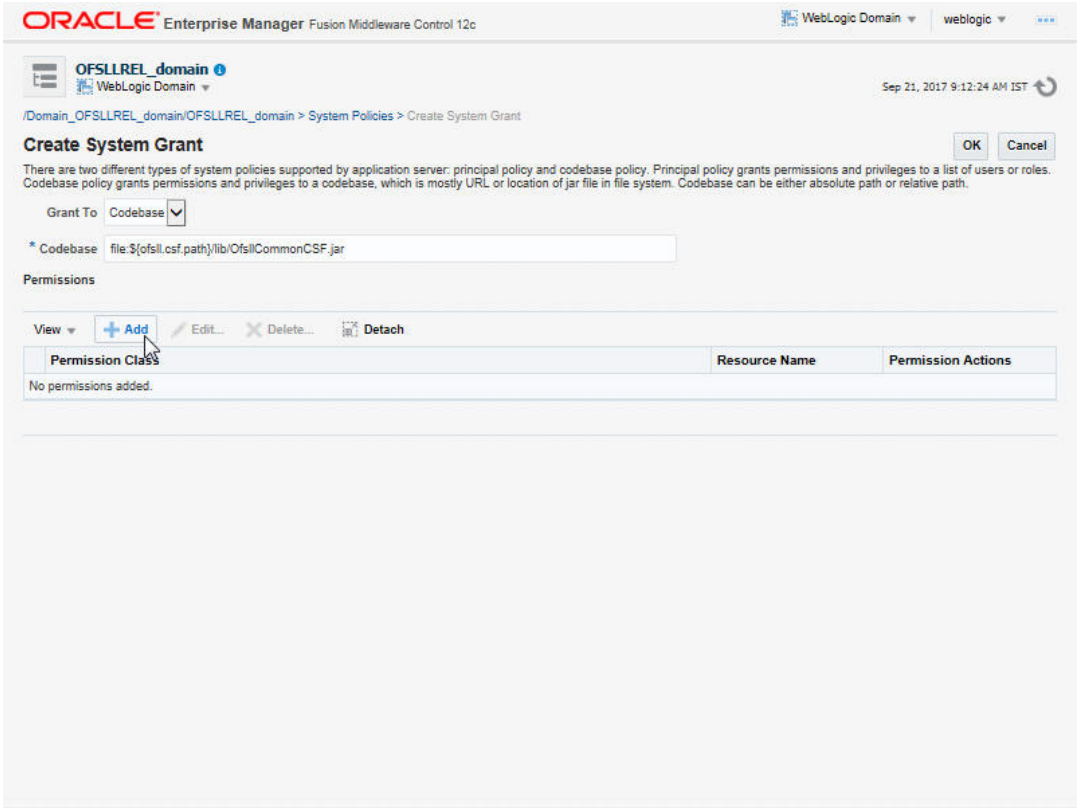
11. Click **Create**.

Figure 9-8 BI Publisher 8



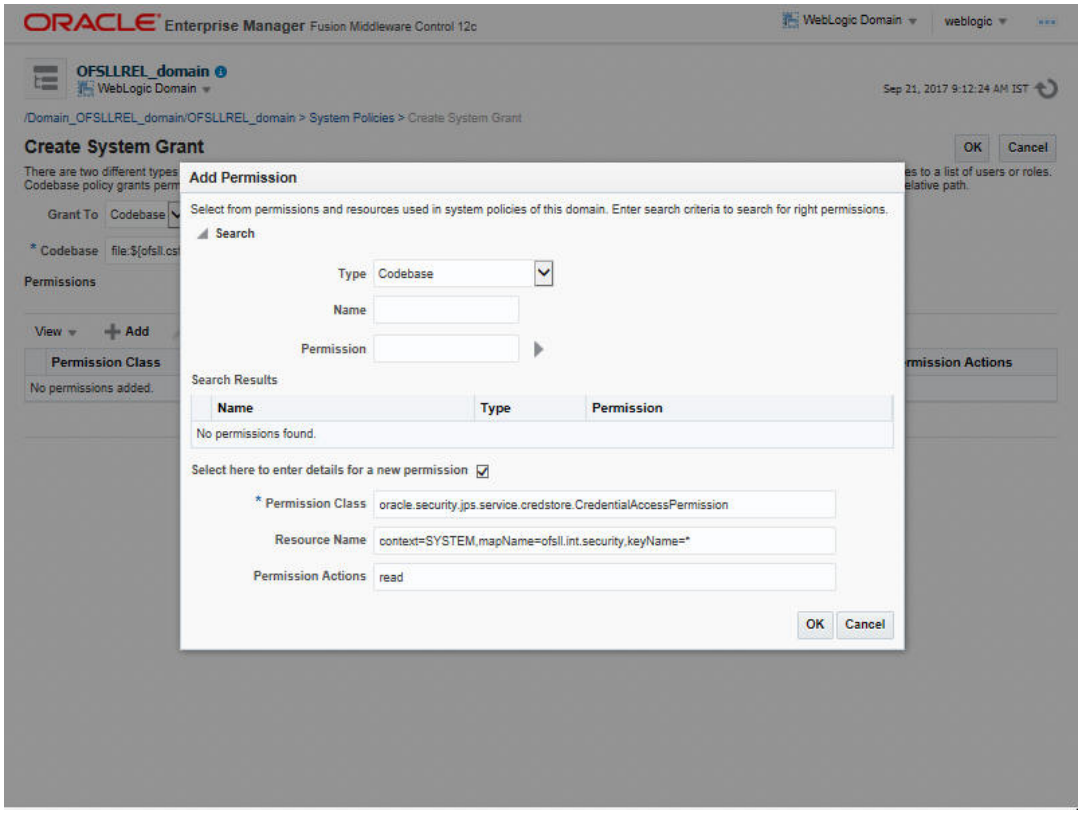
12. The following window is displayed. Enter the codebase as **file:${ofsll.csf.path}/lib/OfsllCommonCSF.jar** and click **Add**.

Figure 9-9 BI Publisher 9



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

Figure 9-10 BI Publisher 10

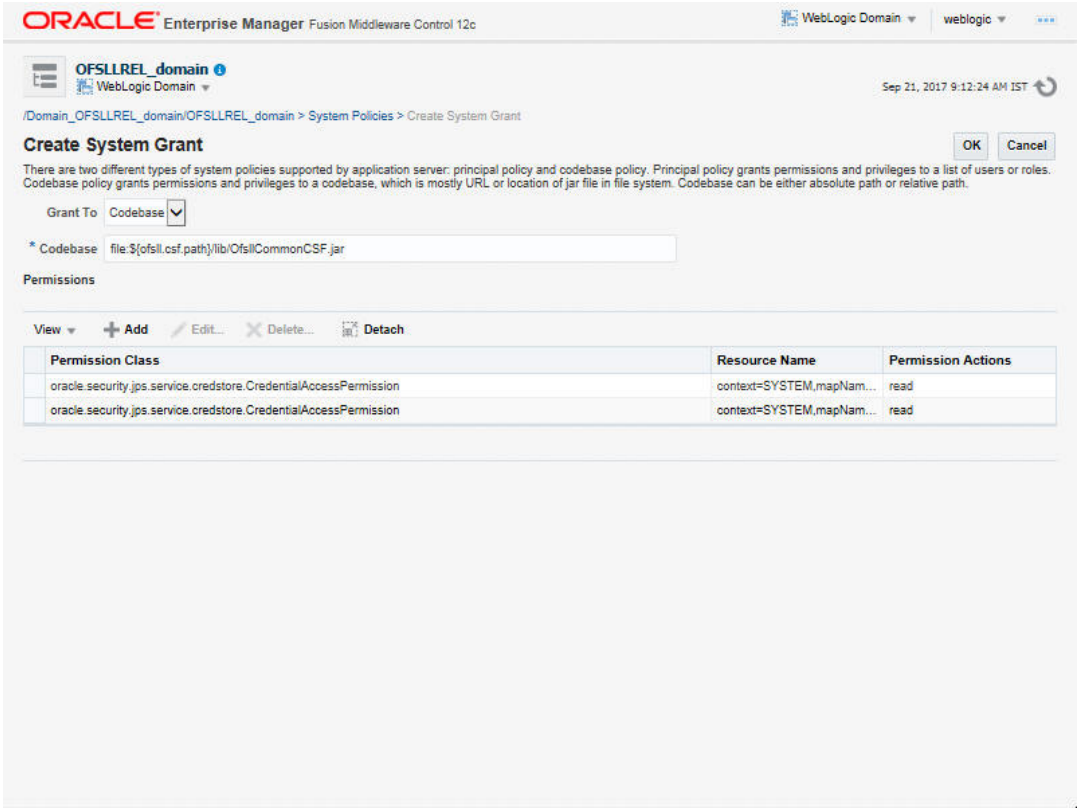


9.2 Configuring JNDI Name for http Listener

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

   The following window is displayed.

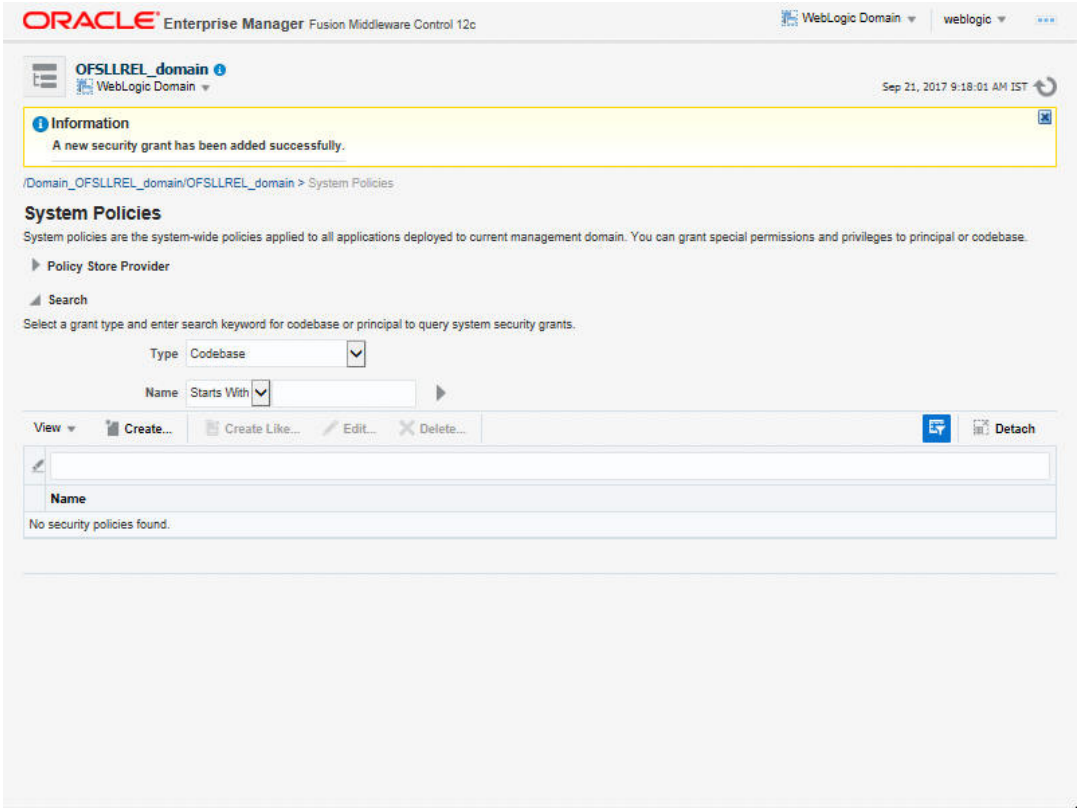
Figure 9-11 BI Publisher 10



3. Click **OK**.

   The following window is displayed.

Figure 9-12 BI Publisher 11



10

Launch 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.

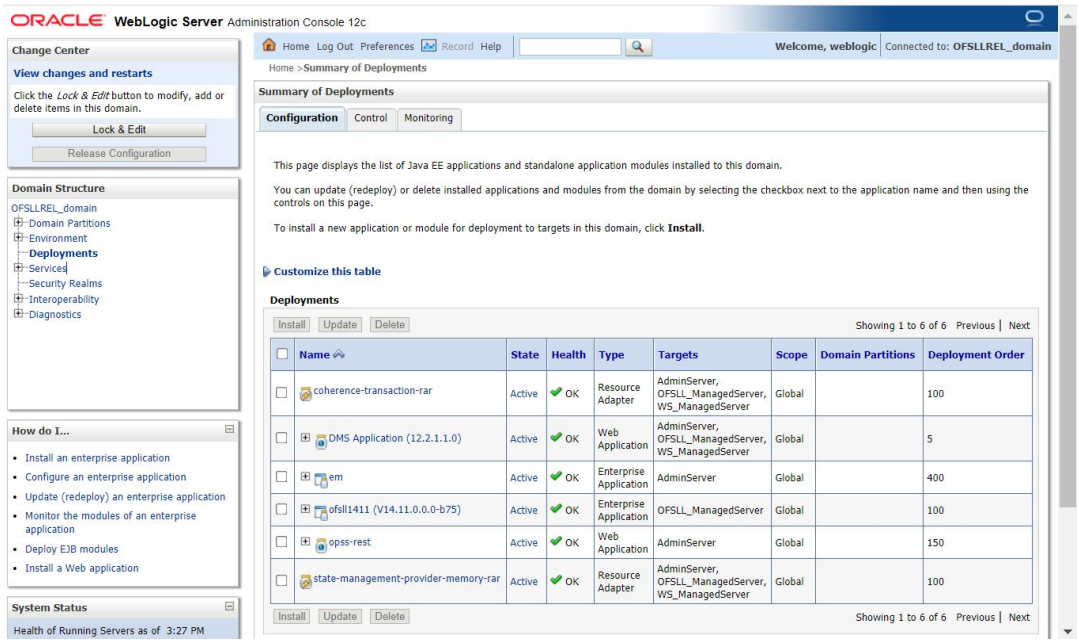
- Launching Application

10.1 Launching Application

To launch application

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

Figure 10-1 Launching Application 1

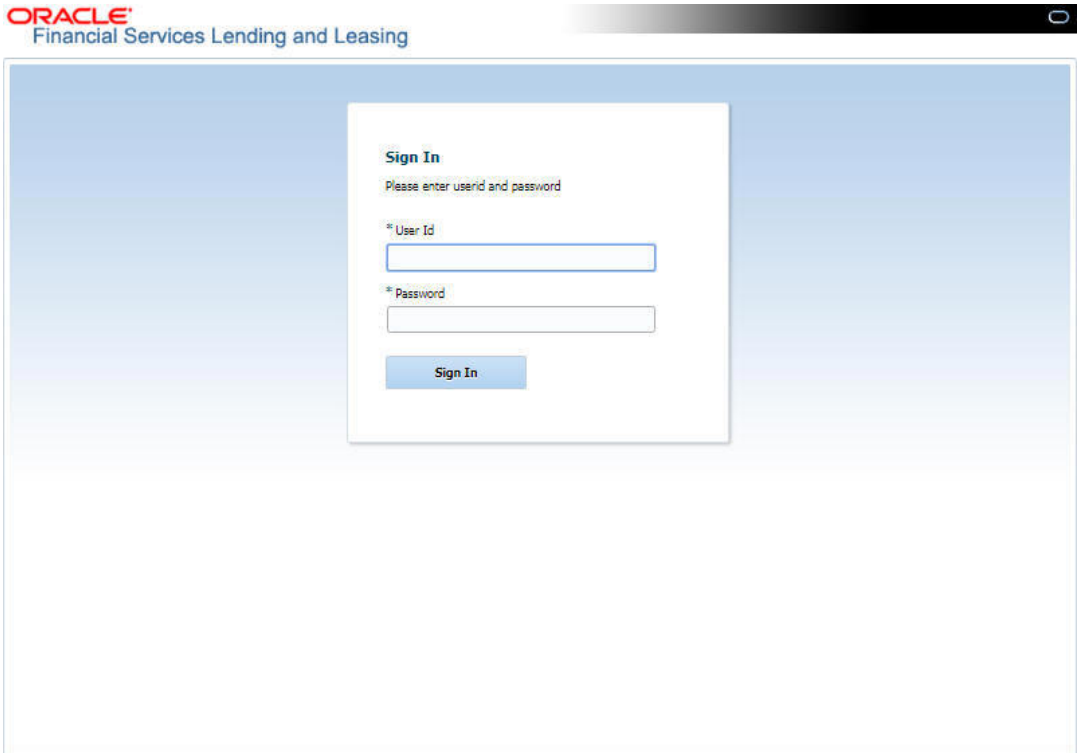


2. The URL of the OFSLL application will be of the format - https://<hostname>:<Port>/<ContextName>/faces/pages/OfsllSignIn.jsf

   (Example: https://localhost:7003/ofsll/faces/pages/OfsllSignIn.jsf)

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

Figure 10-2 Launching Application 2



4. After successful login, the following screen is displayed

Figure 10-3 Launching Application 3