

Application Installation Guide
Oracle Financial Services Lending and Leasing
Release 14.3.0.0.0

Part No. E72985-01

March 2016

Application Installation Guide
March 2016
Oracle Financial Services Software Limited

Oracle Park

Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India
Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax: +91 22 6718 3001
www.oracle.com/financialservices/

Copyright © 2007, 2016, Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

Table of Contents

1. Preface	1-1
1.1 Prerequisites.....	1-1
1.2 Audience.....	1-2
1.3 Conventions Used	1-2
2. Installing Software	2-1
2.1 Installing Oracle WebLogic Server 12c	2-1
3. Creating Domains, Repositories, Data Sources	3-1
3.1 Creating Domain and Servers	3-1
3.2 Creating Schemas using Repository Creation Utility.....	3-11
3.3 Creating Metadata Repository.....	3-18
3.4 Creating Data Source	3-21
3.5 Creating SQL Authentication Provider.....	3-27
3.6 Creating User Groups and Users	3-33
3.6.1 <i>Creating Users</i>	3-33
3.6.2 <i>Creating User Groups</i>	3-34
3.6.3 <i>Assigning Users to Groups</i>	3-35
3.6.4 <i>Resetting password via weblogic console</i>	3-36
3.7 Implementing JMX Policy for Change Password.....	3-36
4. Configuring Policies	4-1
4.1 Configuring Password Policy for SQL Authenticator	4-1
4.2 Configuring User Lockout Policy	4-2
5. Deploying Application	5-1
5.1 Deploying Application	5-1
6. Enabling SSL	6-1
7. Mapping Enterprise Group with Application Role	7-1
8. Configuring JNDI name for HTTP Listener	8-1
9. Configuring Oracle BI Publisher for Application	9-1
10. Launching Application	10-1
11. Installing Upgrade	11-1

1. Preface

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

For recommendations on security configuration, refer Security Configuration Guide.

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

Application installation is a nine step process.

1. [Installing Software](#)
2. [Creating Domains, Repositories, Data Sources](#)
3. [Configuring Policies](#)
4. [Deploying Application](#)
5. [Enabling SSL](#)
6. [Launching Application](#)
7. [Mapping Enterprise Group with Application Role](#)
8. [Configuring Oracle BI Publisher for Application](#)
9. [Configuring JNDI name for HTTP Listener](#)

1.1 **Prerequisites**

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

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

1. Sun JDK Version 1.8.0_66 or above <http://www.oracle.com/technetwork/java/javase/downloads/index.html>
2. Oracle WebLogic Server 12c Version 12.2.1.0.0
(<http://www.oracle.com/technetwork/middleware/weblogic/downloads/index.html>)

Navigate to Fusion Middleware Infrastructure Installer.

JVM/JDK are to be downloaded and installed prior to installing the Weblogic Server.

Note

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

1.2 Audience

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

1.3 Conventions Used

Term	Refers to
Application	Oracle Financial Services Lending and Leasing

2. Installing Software

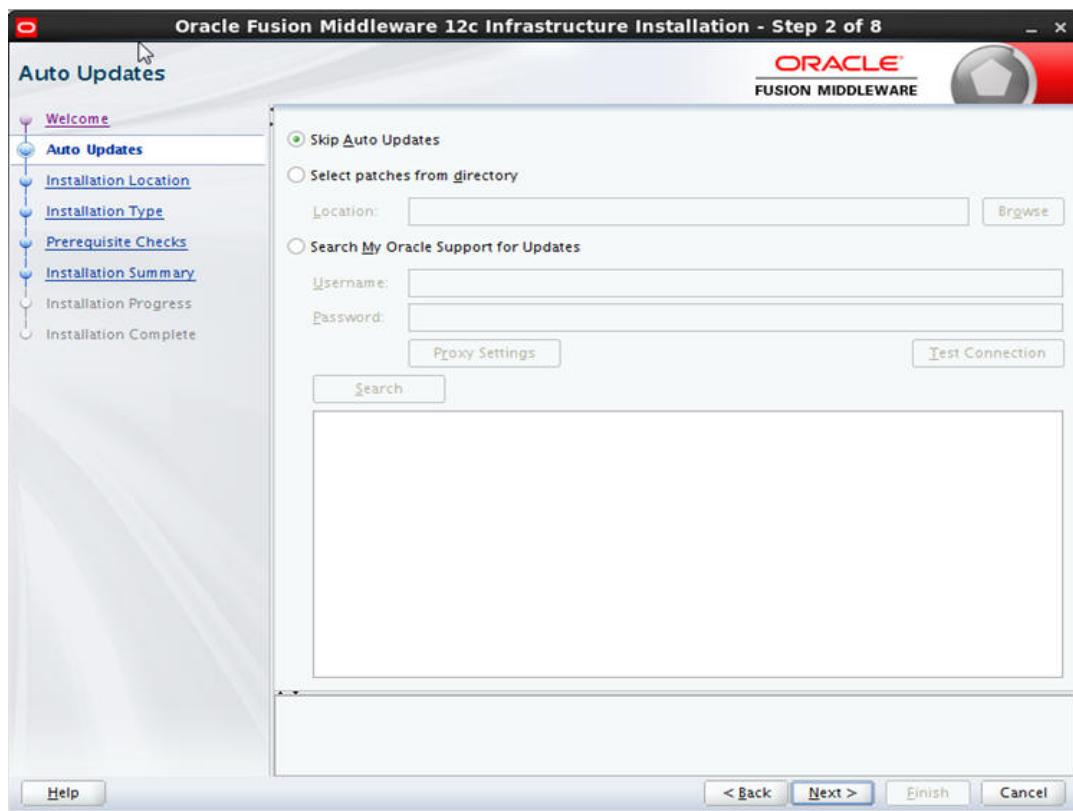
2.1 Installing Oracle WebLogic Server 12c

To install using generic Weblogic installer -

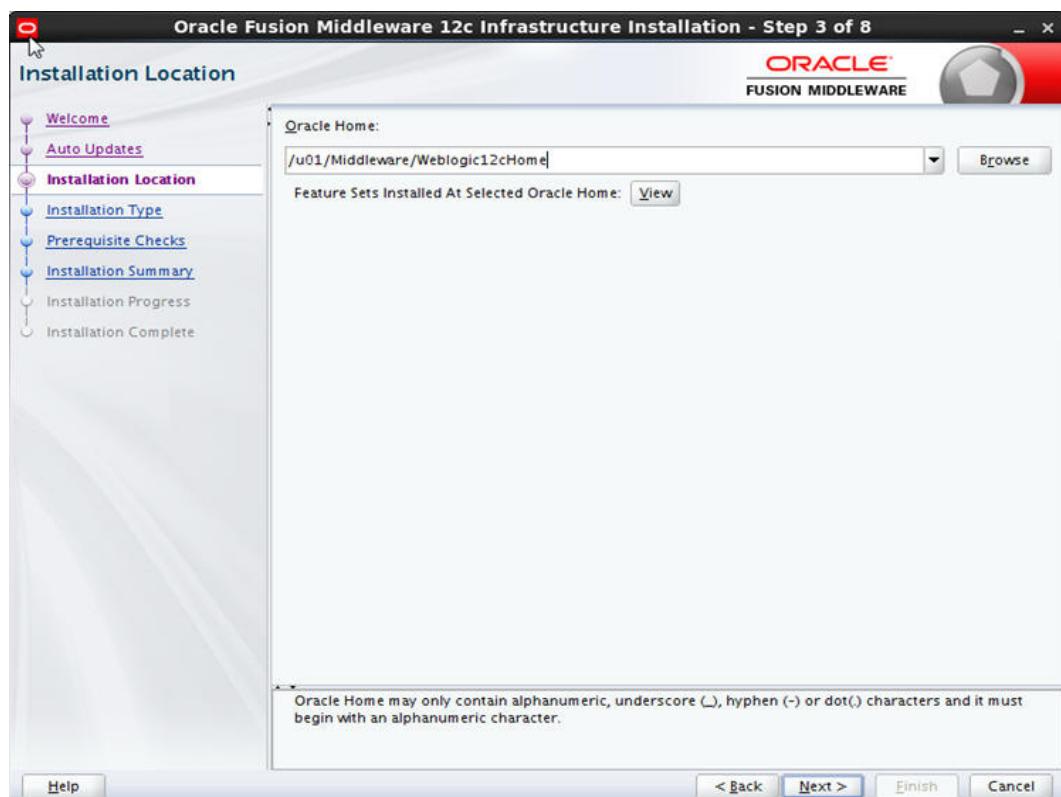
1. Run the command → `java -jar fmw_12.2.1.0.0_infrastructure.jar`
2. Welcome screen is displayed as shown below.



3. Click **Next** to continue.

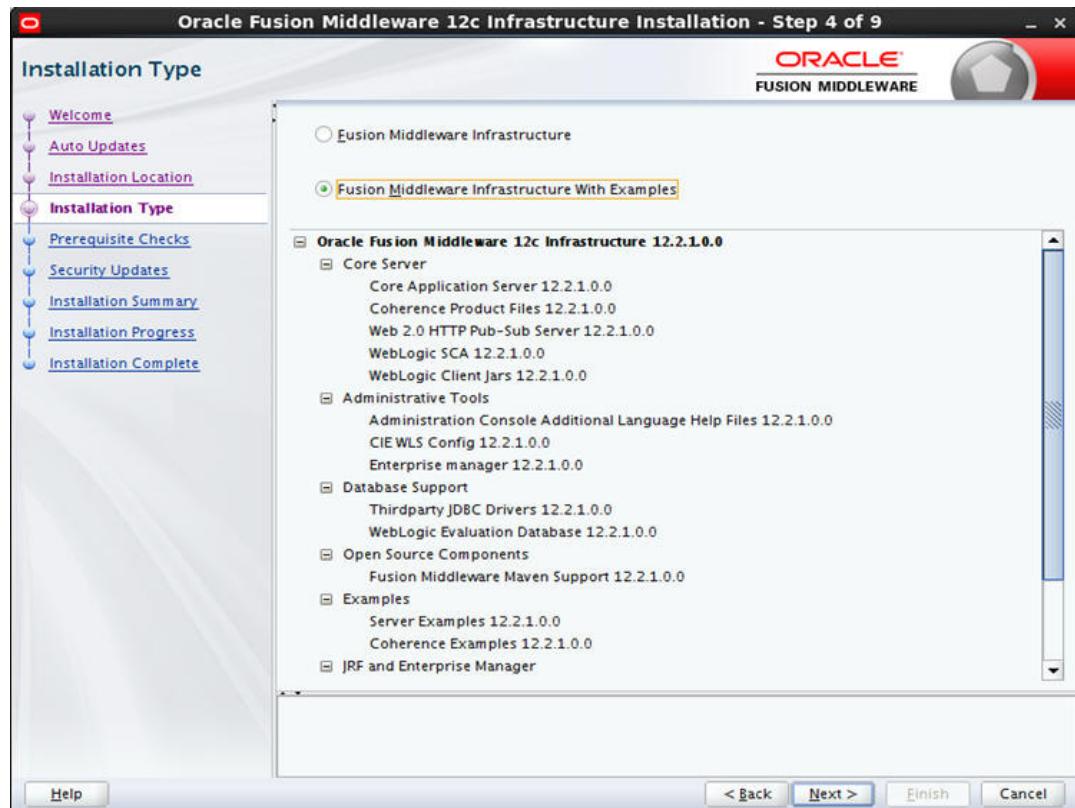


4. Select **Skip Auto Updates** and Click **Next**.



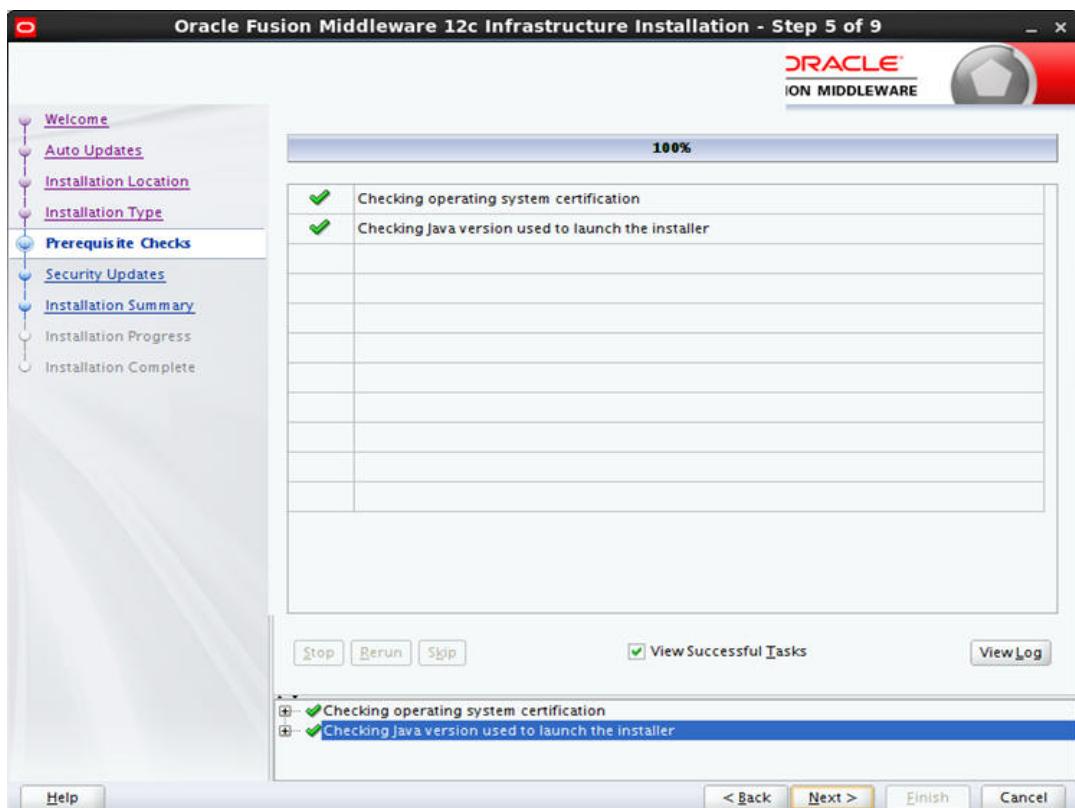
5. Specify the path for **Middleware Home Directory**, and then click **Next**.

6. The following window is displayed..

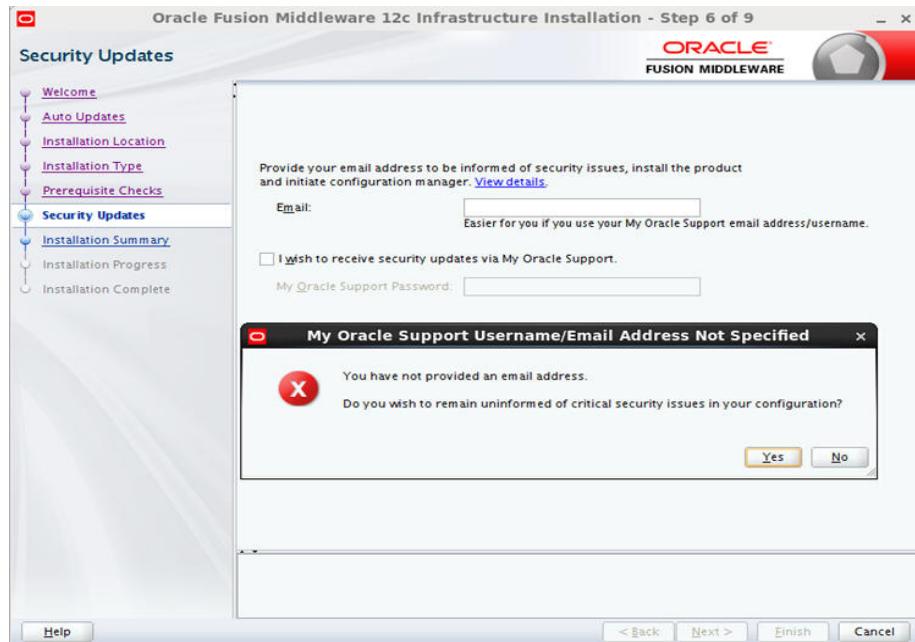


7. Select Fusion Middleware Infrastructure with Examples.

8. Click **Next** to continue.

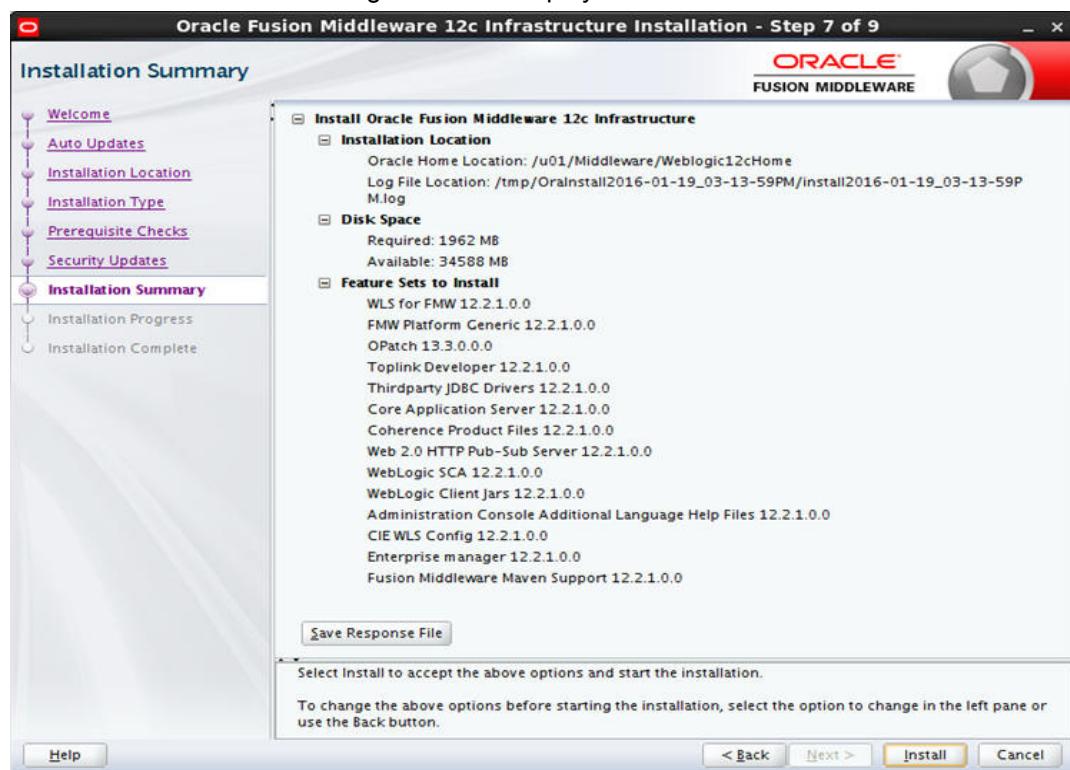


9. Click **Next** to continue..

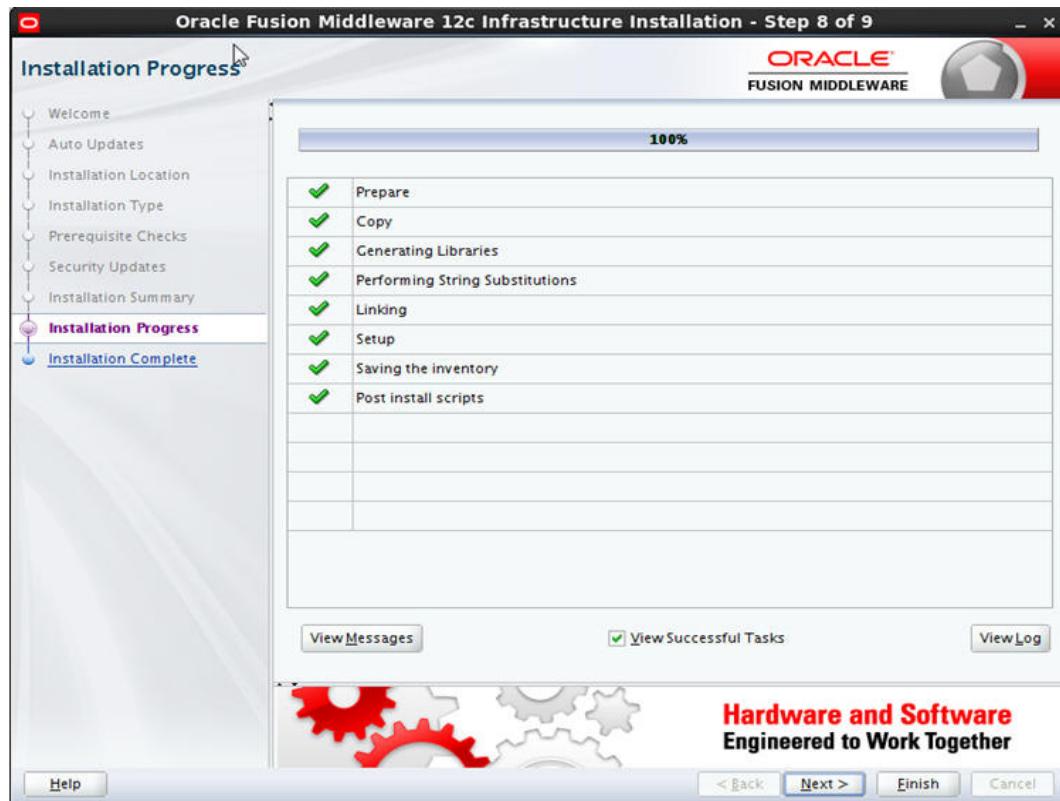


10. Uncheck the check box as in the above screen and click Next. Confirmation window is displayed. Click on Yes.

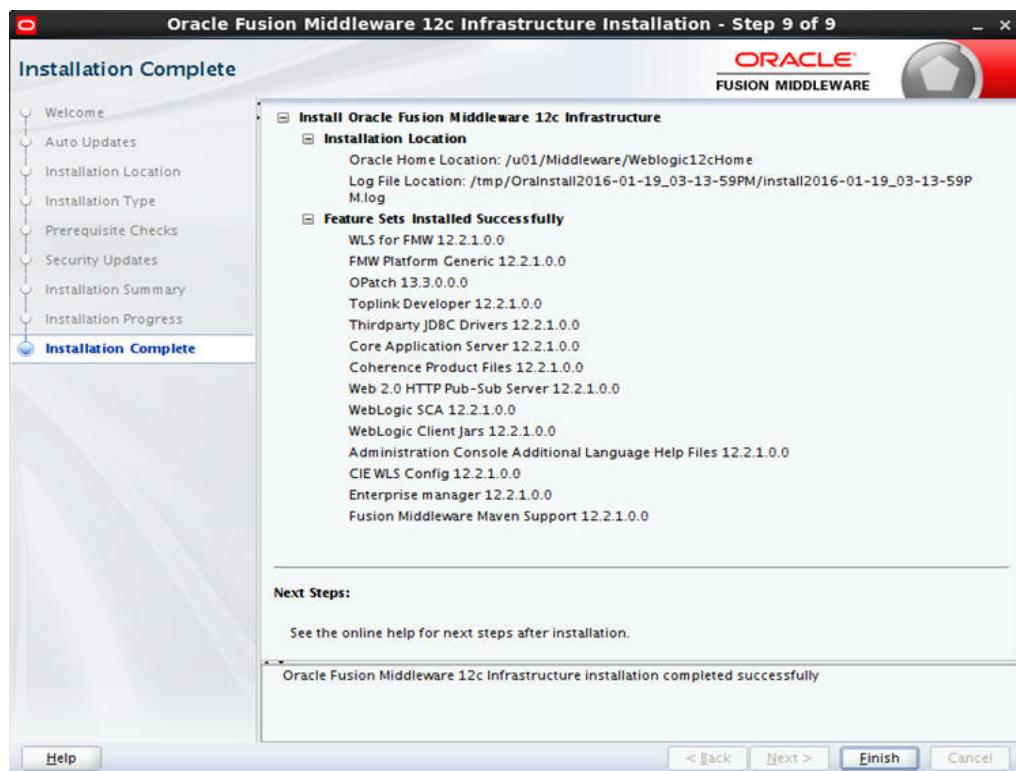
11. Click on Next. The following window is displayed.



12. Click on **Install**. The weblogic installation starts. After it is done the following window is displayed..



13. Click on **Next...**



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

3. Creating Domains, Repositories, Data Sources

3.1 Creating Domain and Servers

1. In Unix/Linux machine, once the Oracle WebLogic Server is installed, navigate to the following path.

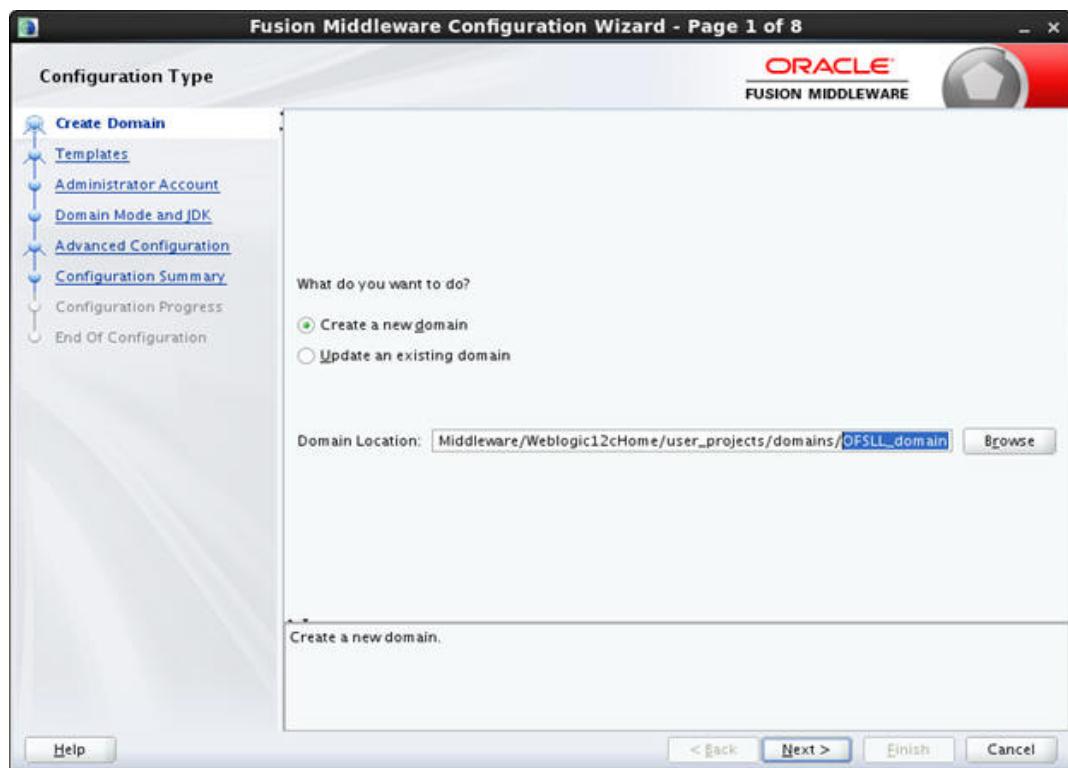
<WL_HOME>/wlserver/common/bin

Note

Use XManager for remote UNIX/LINUX machine. Refer [XManager Usage](#).

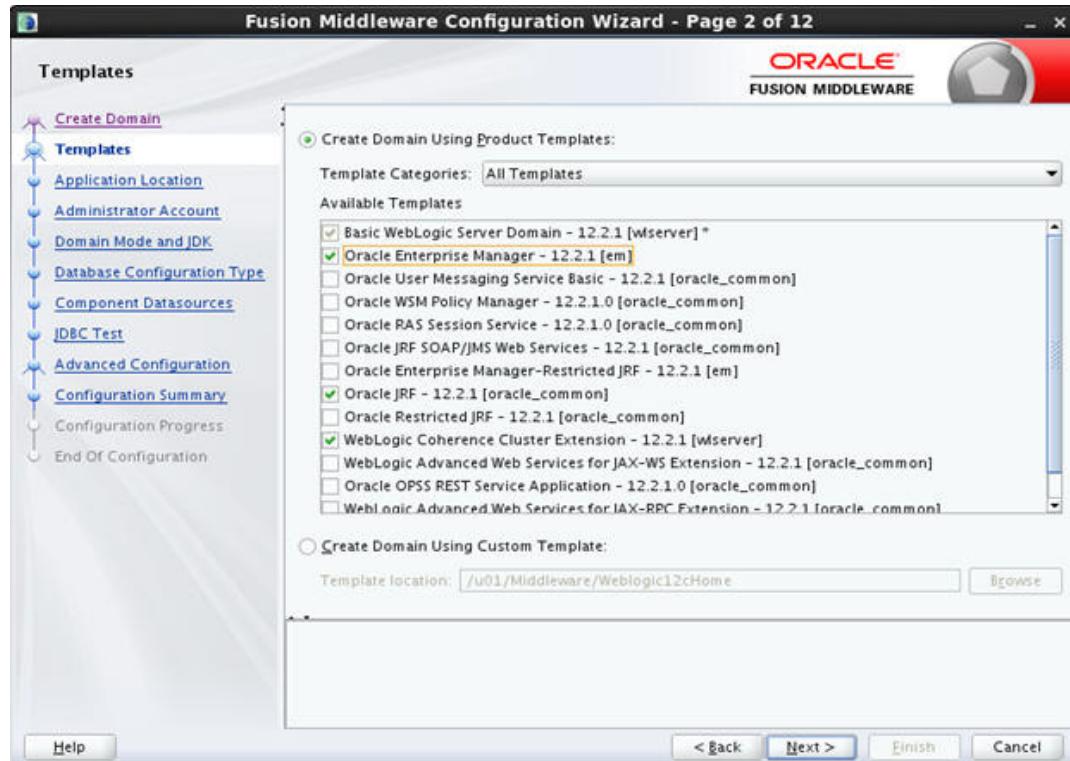
Here, WL_HOME is **/home/Oracle/Middleware**.

2. In Unix run **config.sh**.
3. Click Configuration Wizard icon.

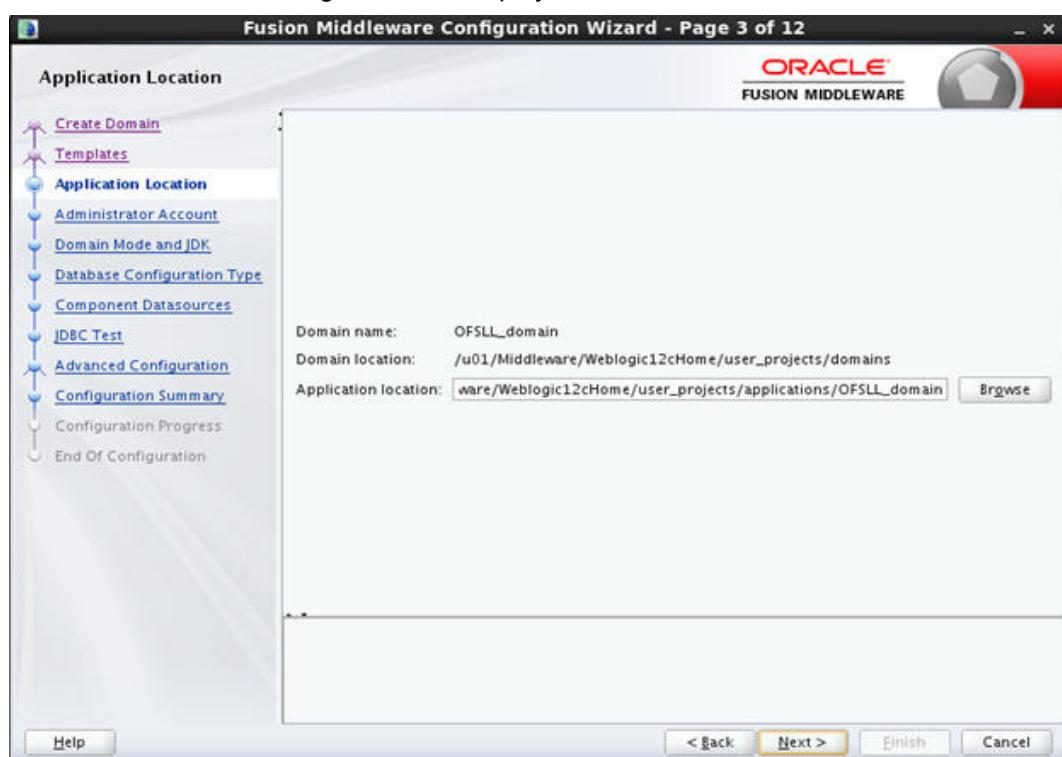


4. Select **Create a new domain** and give the Domain Location.

5. Click **Next** to continue. The following window is displayed.

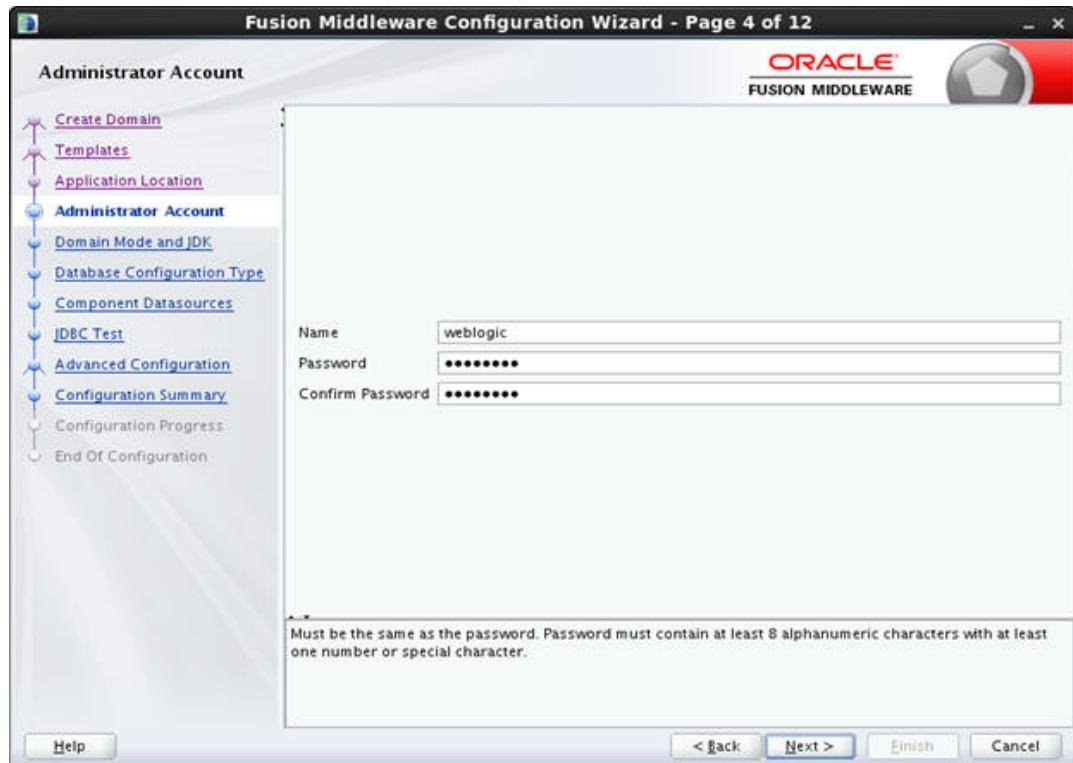


6. Select **Create Domain Using Product Templates** option.
7. Select **Oracle Enterprise Manager - 12.2.1 [em]** check box.
8. Select **Oracle JRF - 12.2.1 [oracle_common]** check box.
9. Click **Next**. The following window is displayed.



10. Enter **Domain Name** and click **Next**. The following window is displayed.

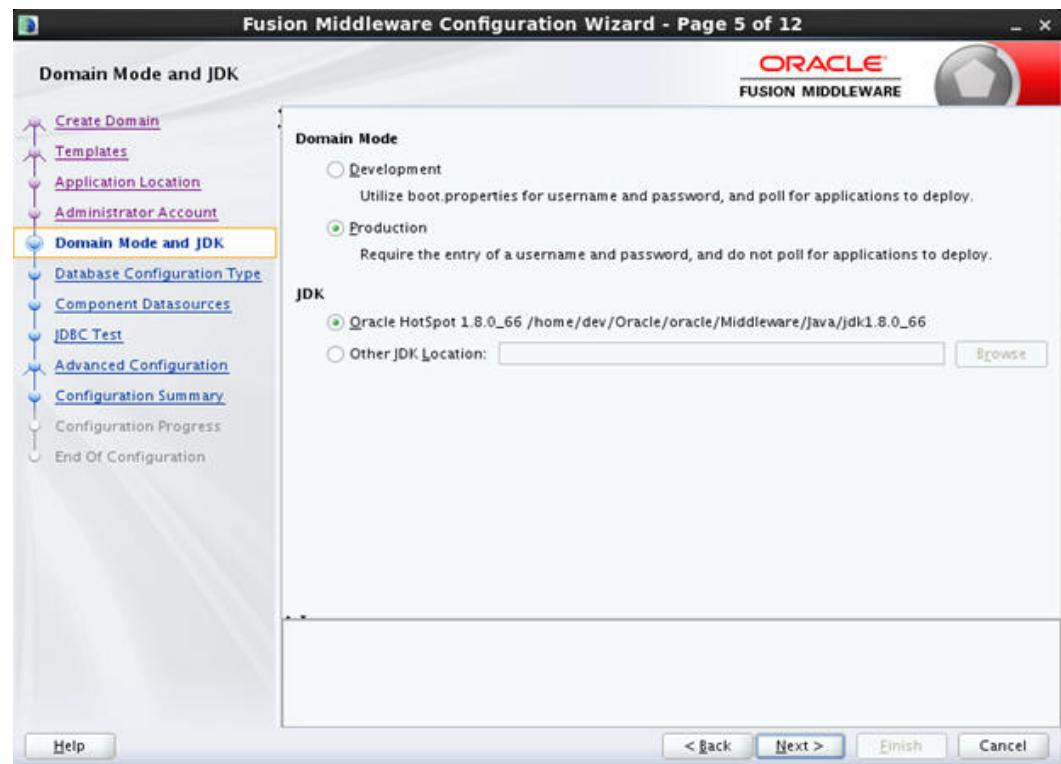
11. Edit Domain Location, if needed.



12. Enter credentials for the following:

- Name
- User password
- Confirm user password
- Description

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

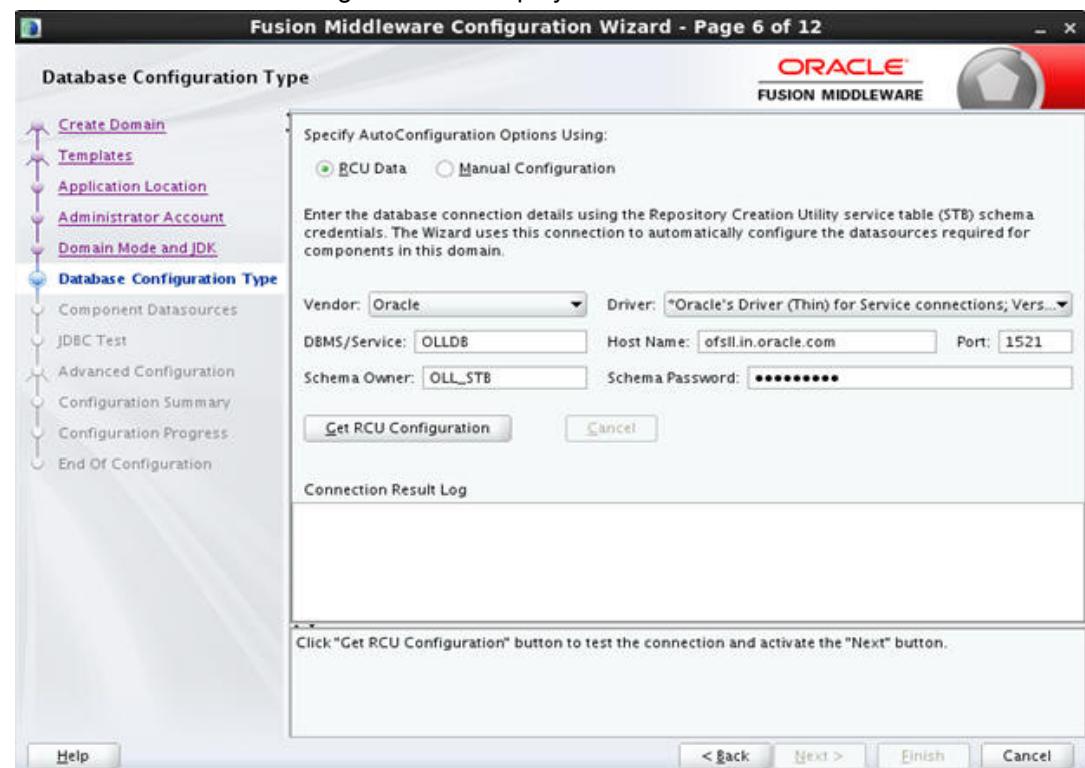


14. Select **Production** Mode and **JDK** from Available **JDKs**

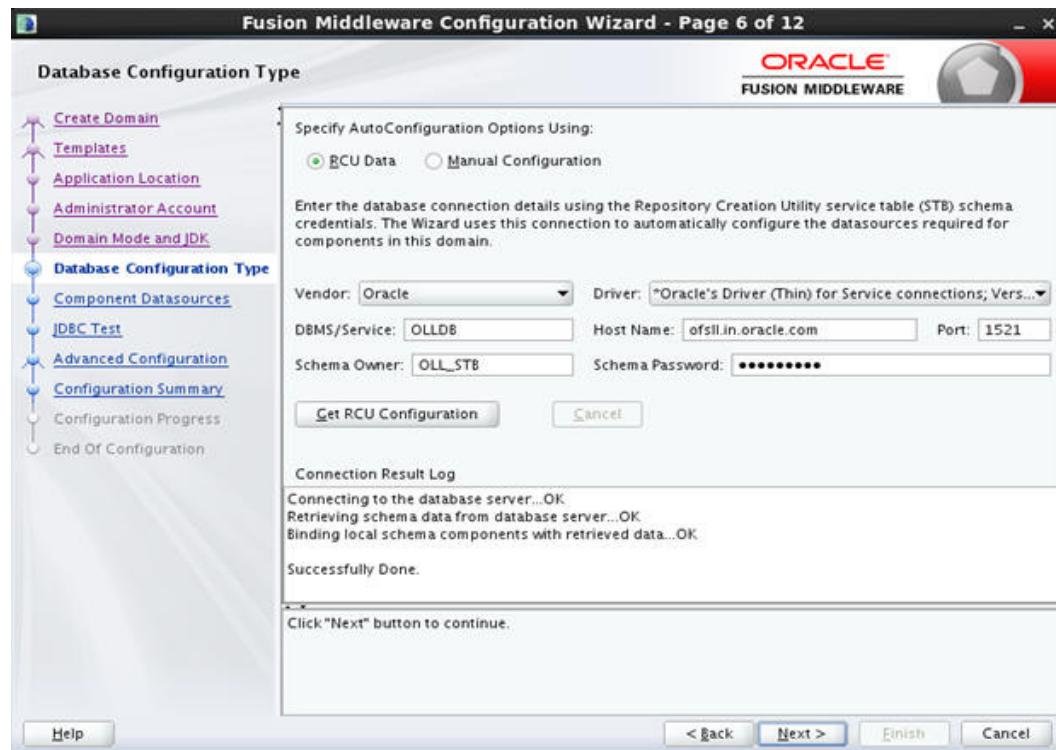
OR

Select **Other JDK** option to select any other **JDK**.

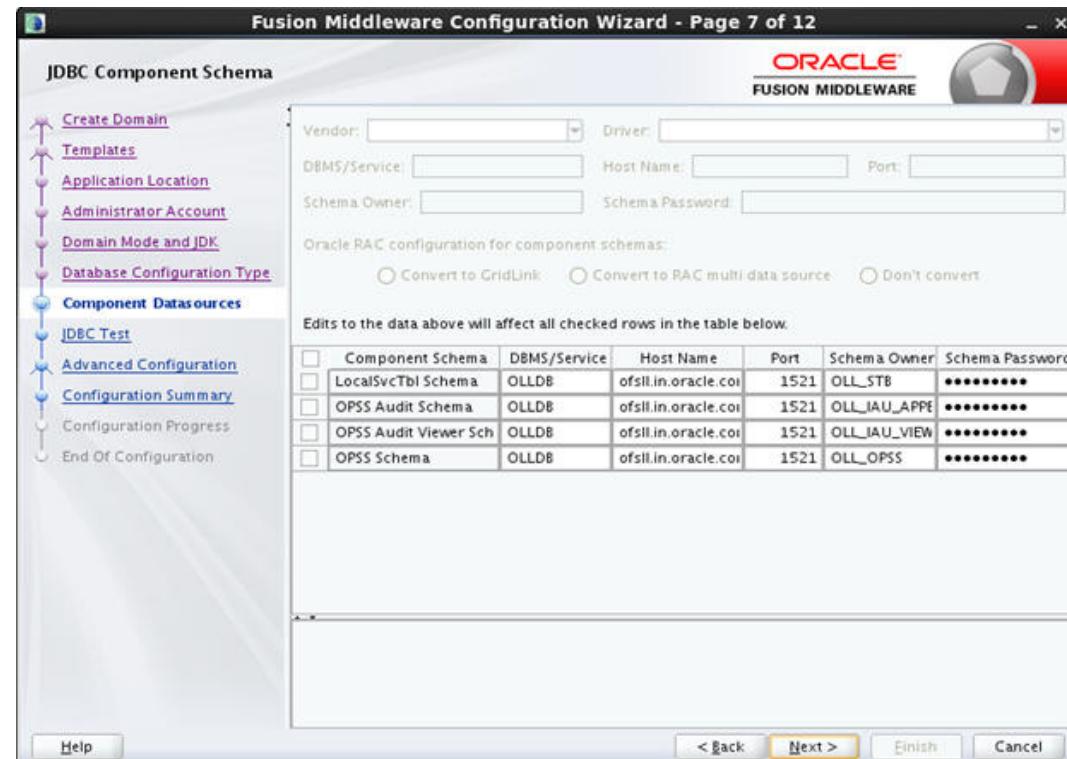
15. Click **Next**. The following window is displayed.



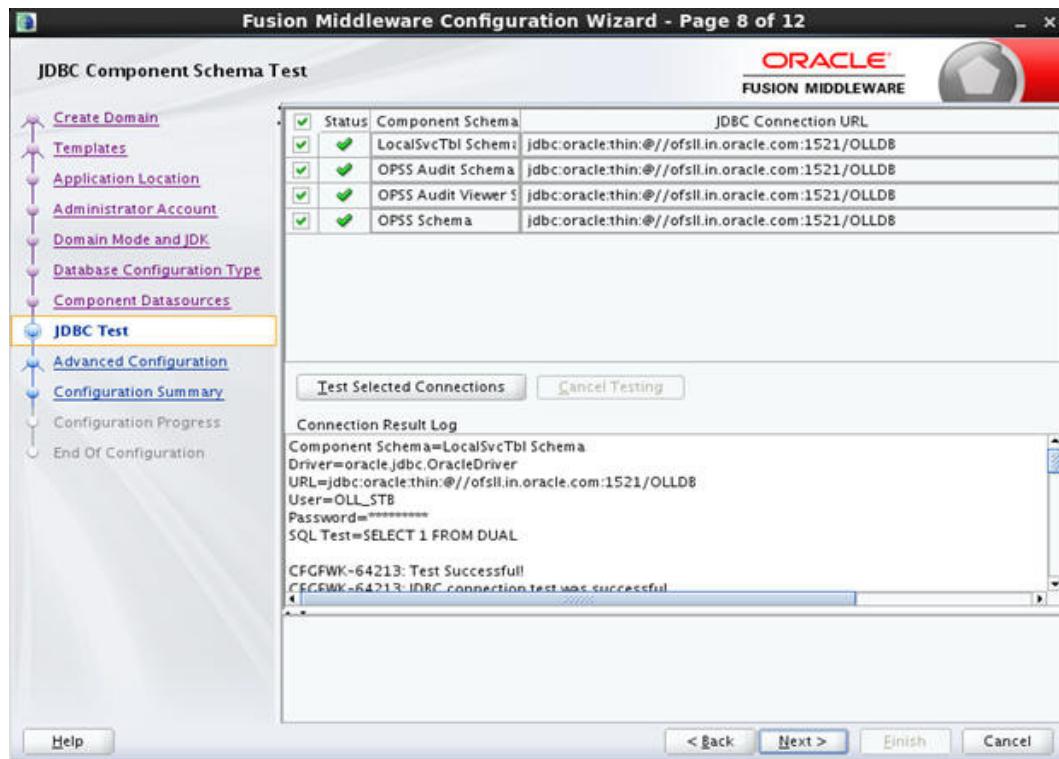
16. Provide the RCU data and click on Get RCU Configuration. The following window is displayed.



17. Click on **Next** to continue..



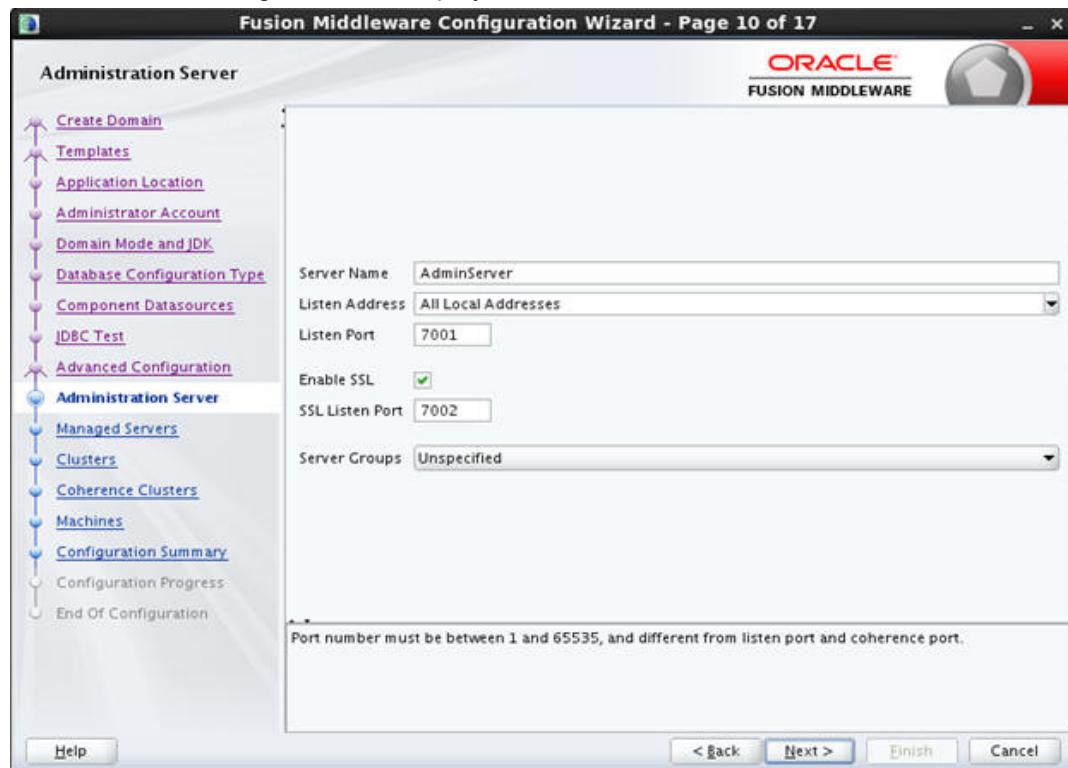
18. . Click on **Next** to continue..



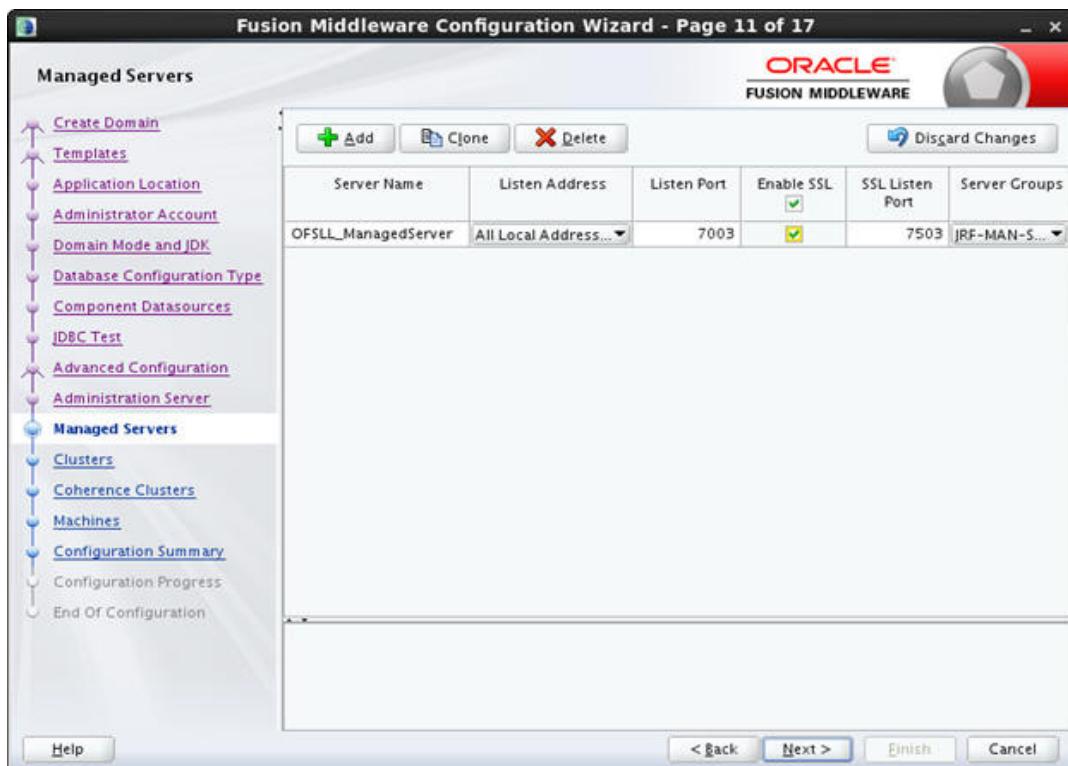
19. Click on **Next** to continue.



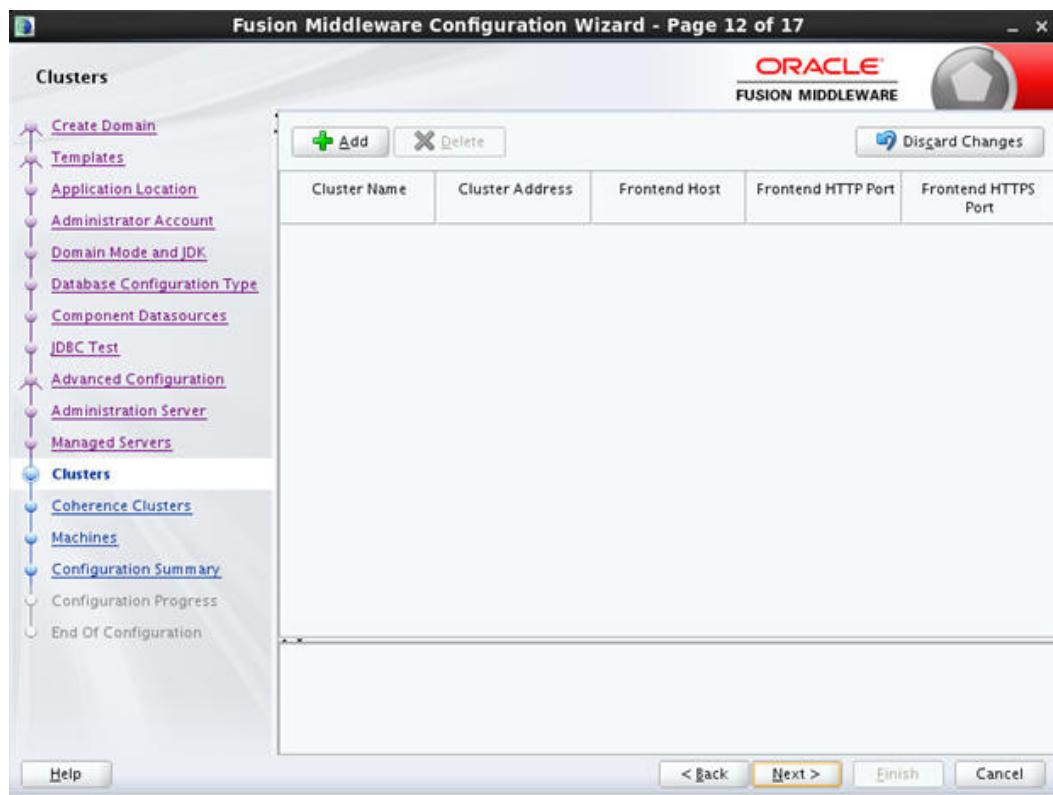
20. Select Administration Server and Managed Servers, Clusters and Machines and click Next. The following window is displayed..



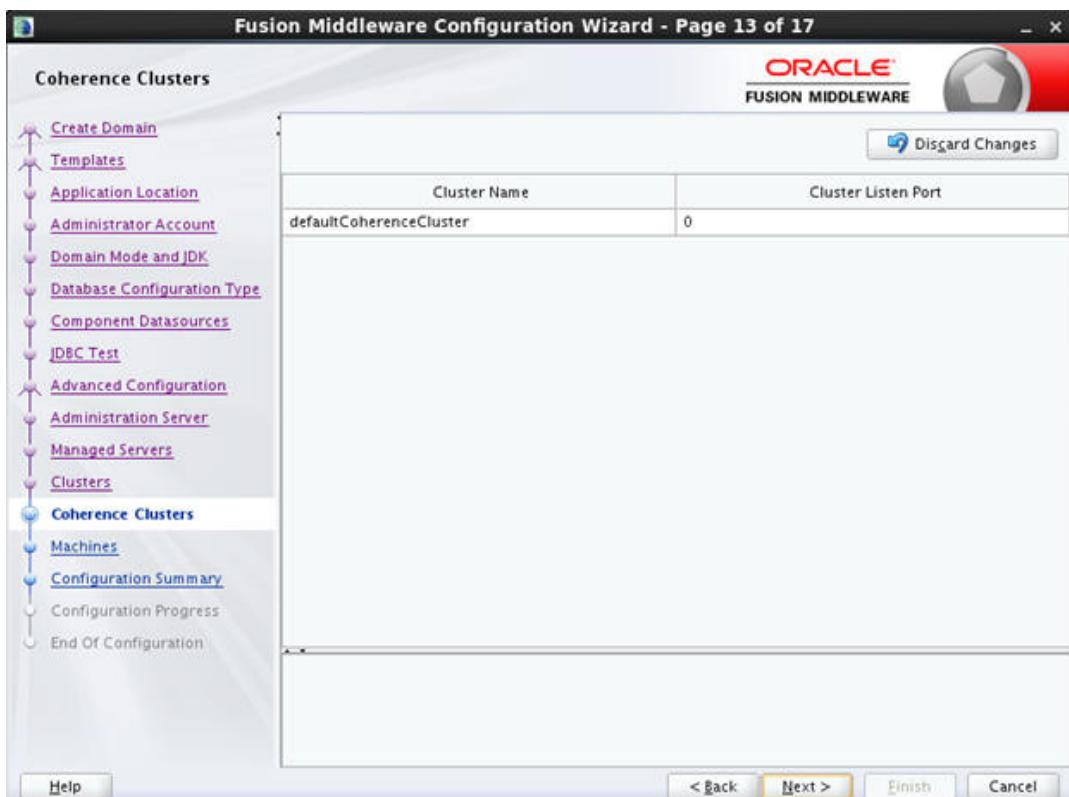
21. Enter Administration Server Name and Listen Port details. Check the SSL port and click Next. The following window is displayed.



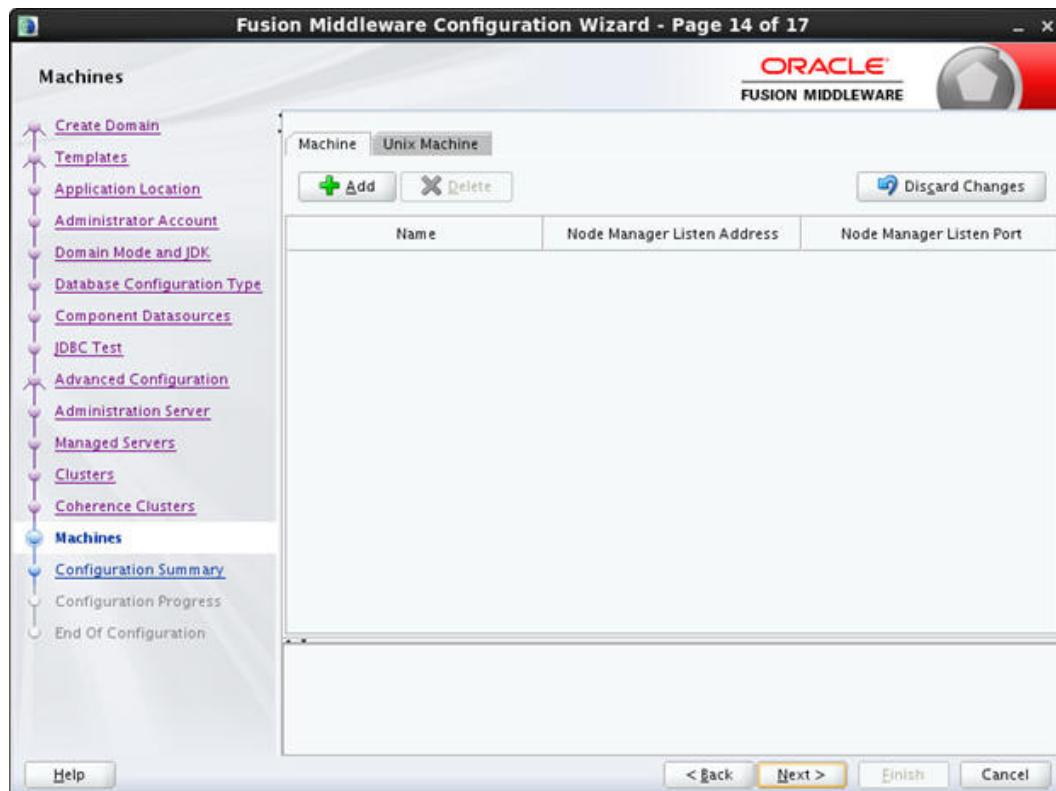
22. Click Add button. Enter Name and Listen Port details in Configure Managed Servers window. Check the SSL port and click Next. The following window is displayed.



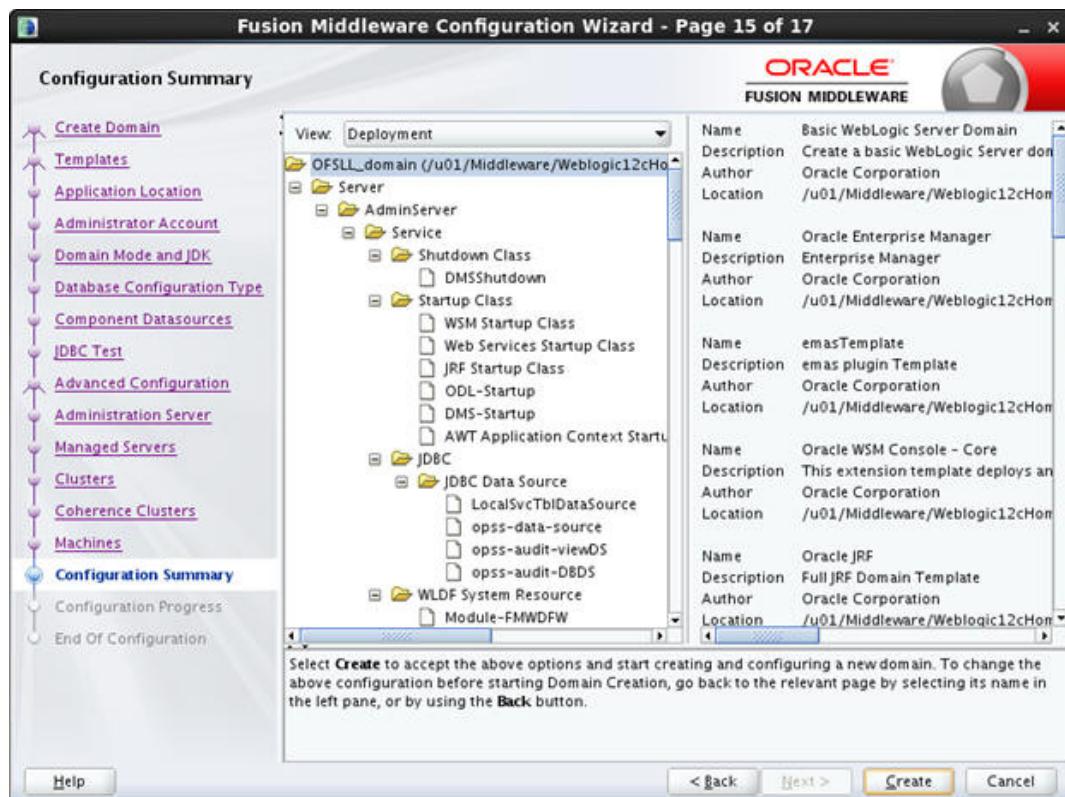
23. Configure as required and click **Next**. The following window is displayed.



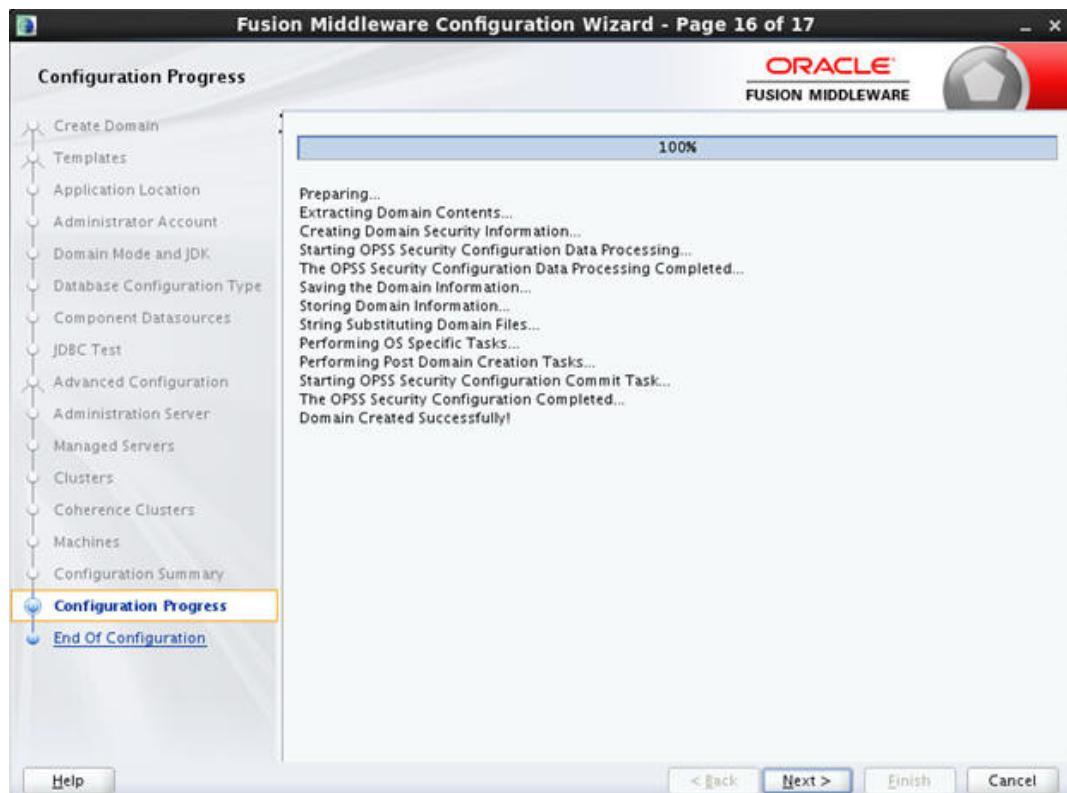
24. Configure as required and click Next. The following window is displayed.



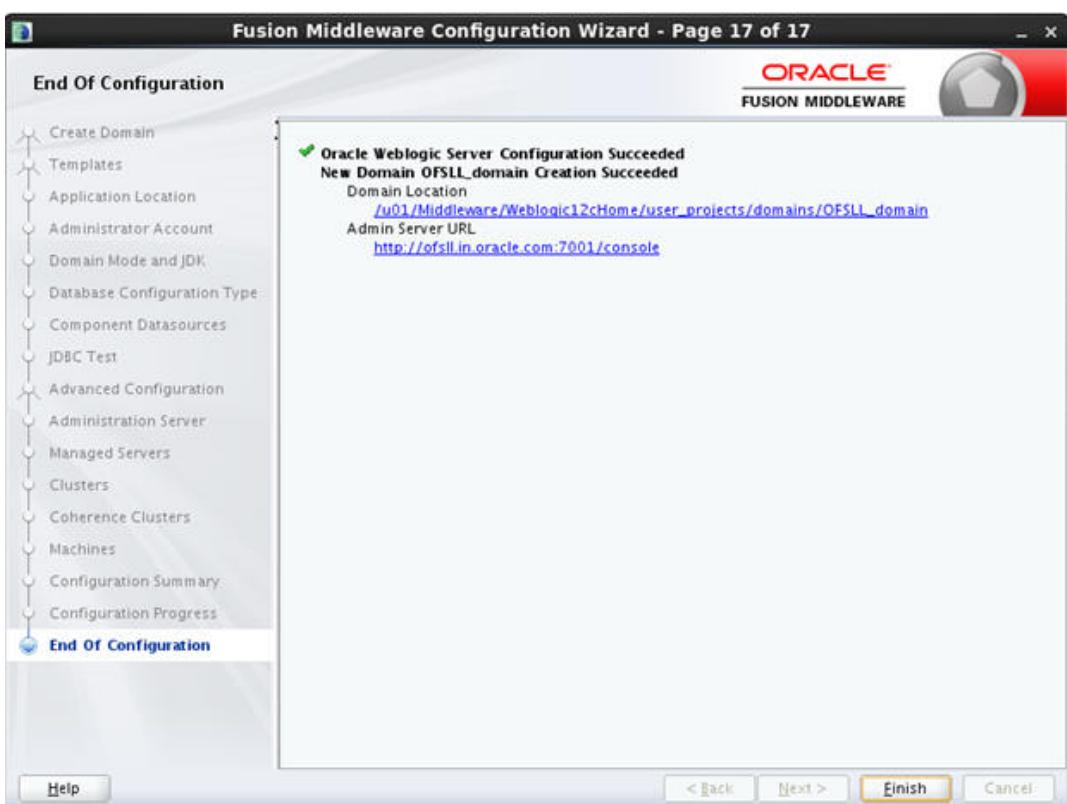
25. Configure as required and click Next. The following window is displayed.



26. Click **Create**. The following window is displayed.



27. Click **Next** to continue.



28. 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"
```

29. 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 &
```

30. To Start Managed Server

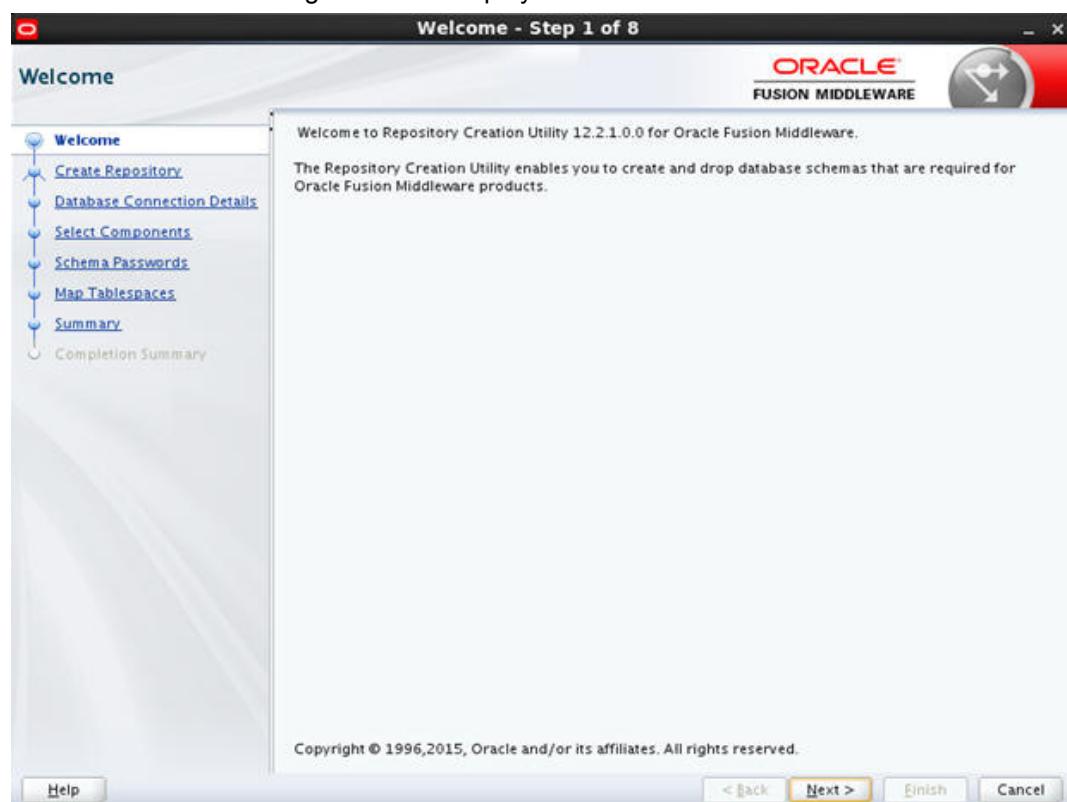
```
$ cd $MW_HOME/user_projects/domains/mydomain/bin  
$ ./$MW_HOME/user_projects/domains/mydomain/bin/startManagedWebLogic.sh  
{ManagedServer_name} {AdminServer URL}
```

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

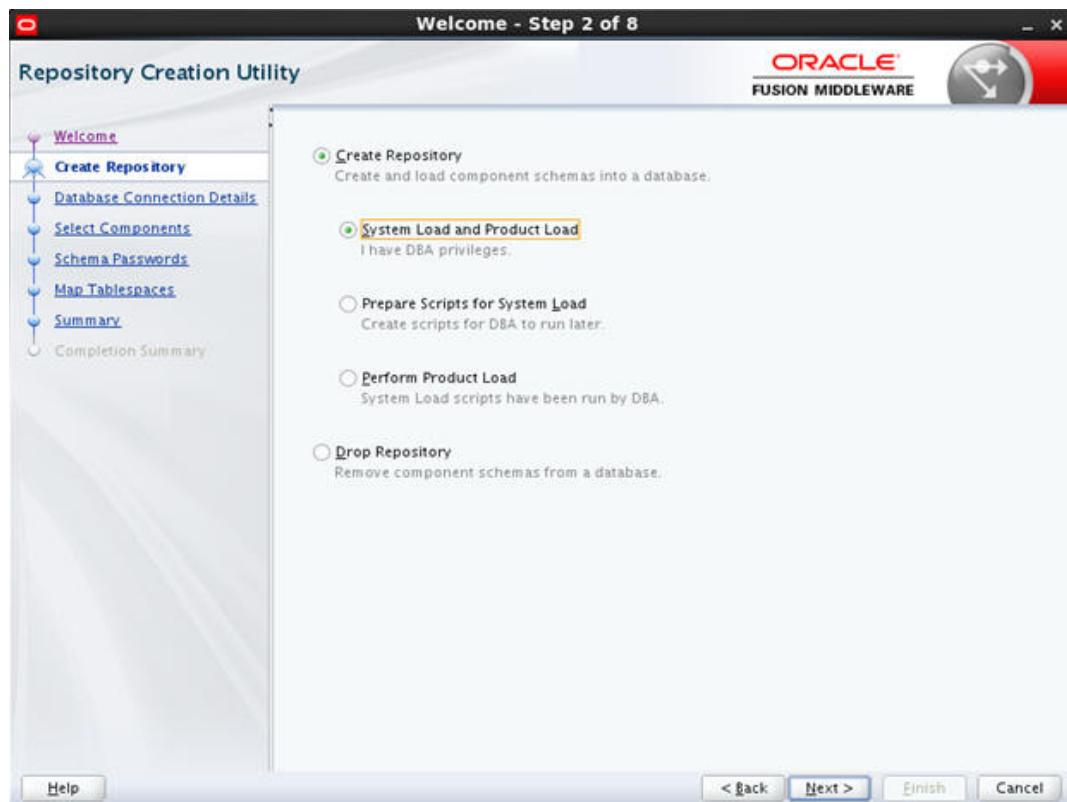
```
$ nohup ./$MW_HOME/user_projects/domains/mydomain/bin/  
startManagedWebLogic.sh {ManagedServer_name} {AdminServer URL} &
```

3.2 **Creating Schemas using Repository Creation Utility**

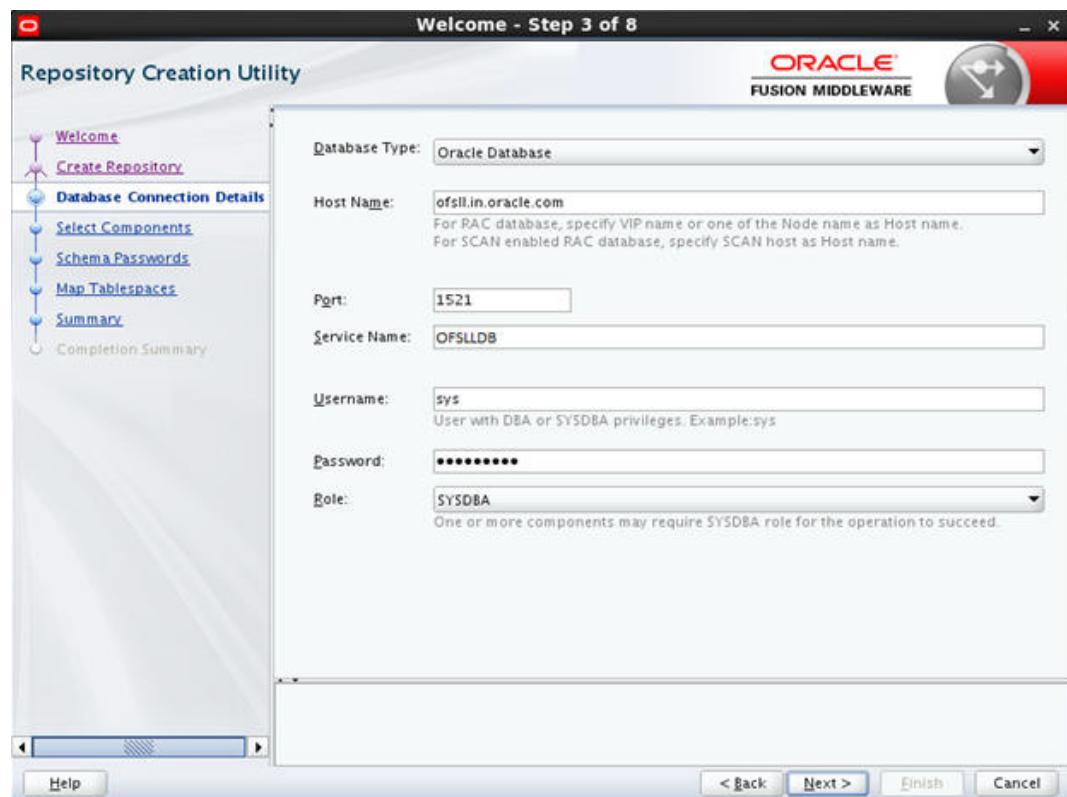
1. Open command prompt on Unix and browse to <WL_HOME>/oracle_common/bin and run ./rcu. The following window is displayed.



2. Click on **Next** to continue..



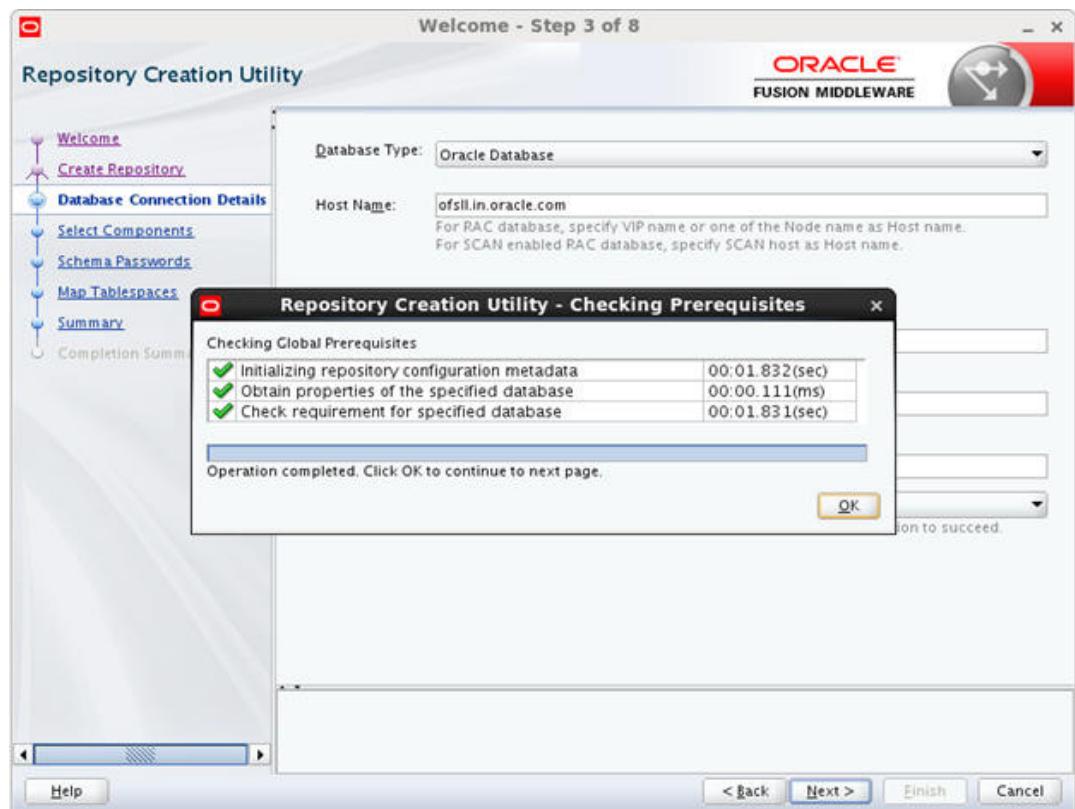
3. Select **Create Repository** and **System Load and Product Load** and click **Next**. The following screen is displayed..



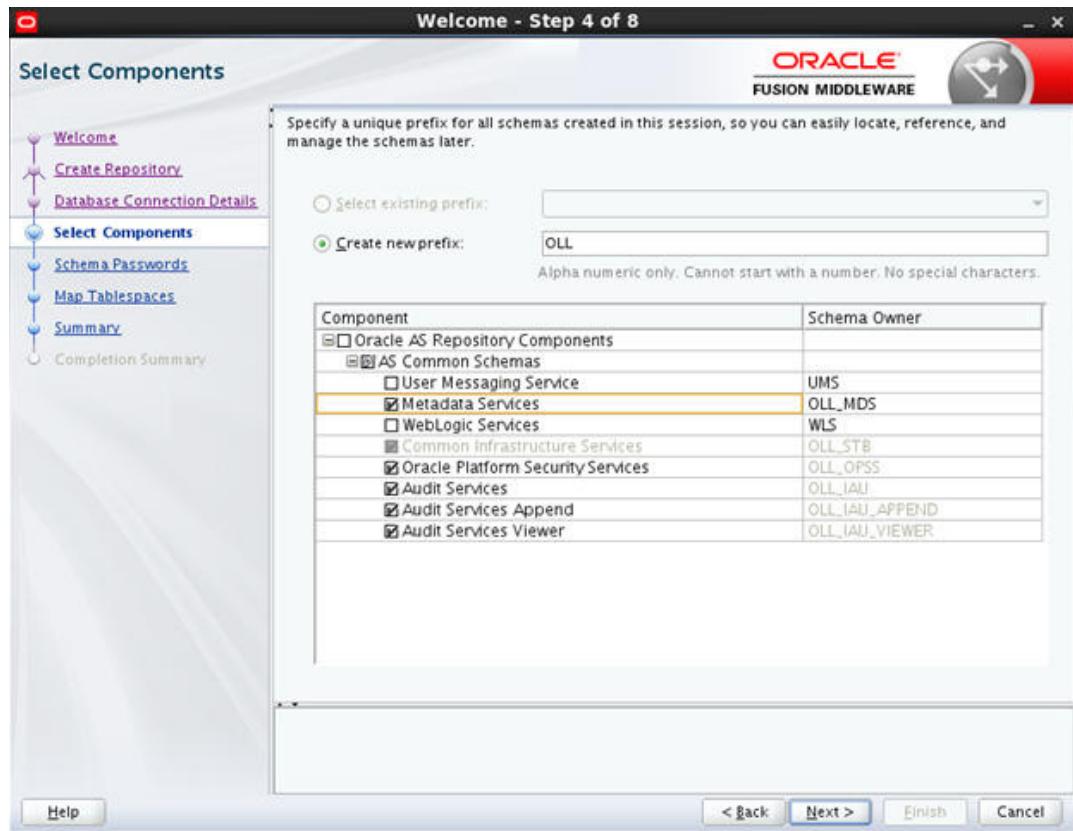
4. Provide database details where you want to create schemas, as shown in the above screen. Click on Next. The following window is displayed.

Note

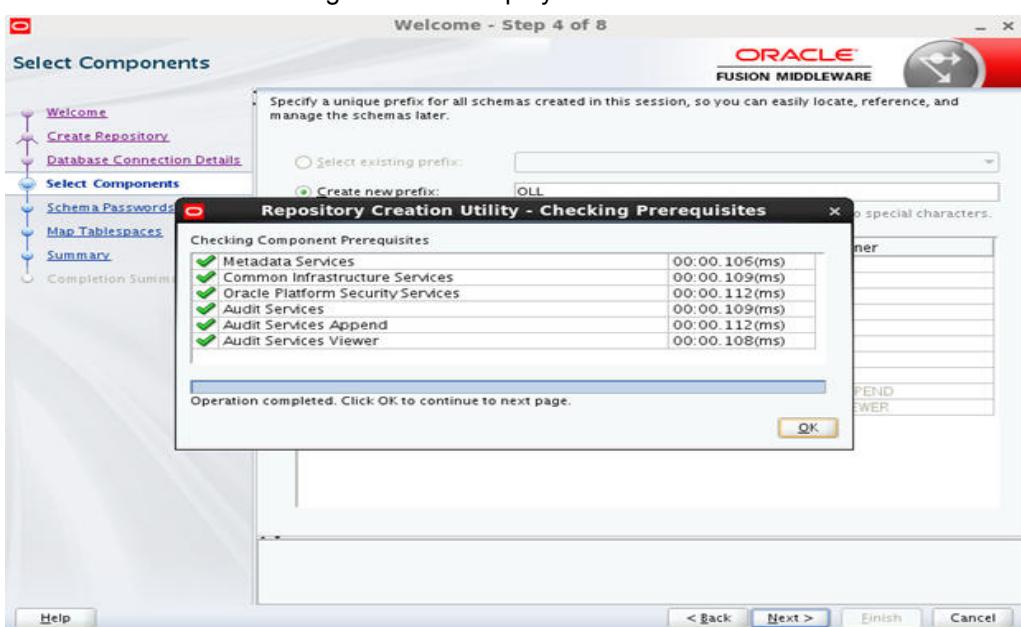
You will require a user with SYSDBA role to create schemas.



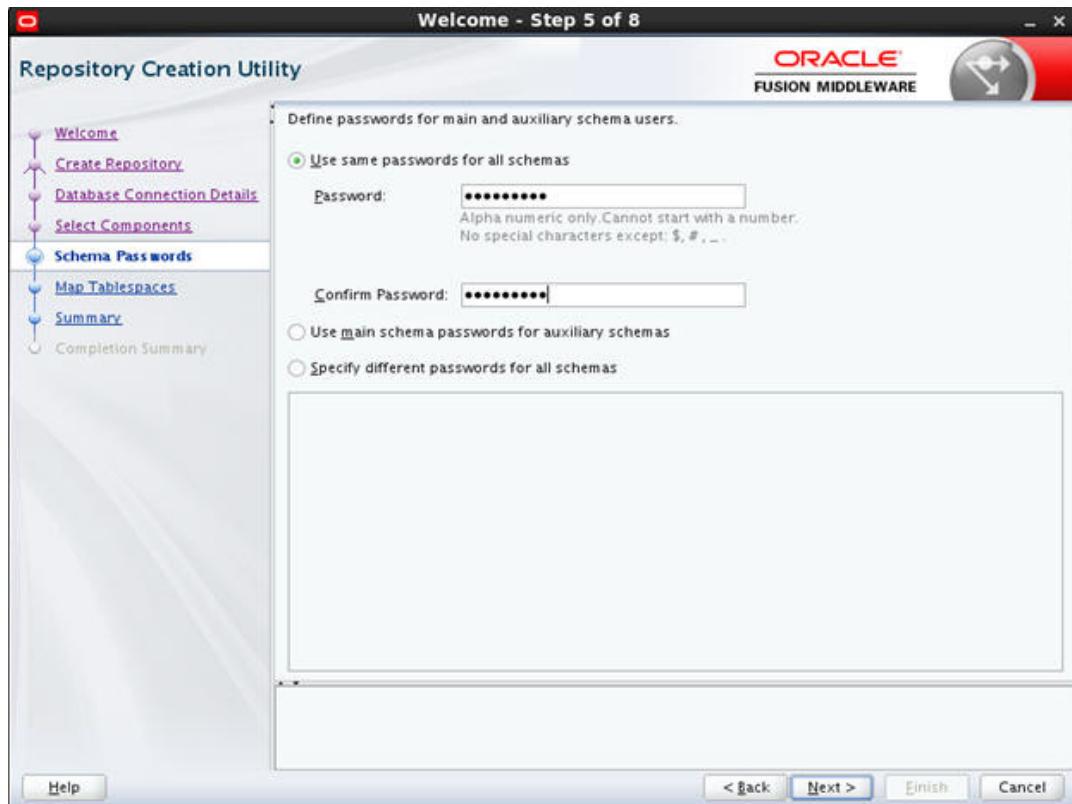
5. Click on OK. Click on Next to continue.



6. Select **Create a new Prefix** option and specify value. For example, OLL. Check **Metadata Services** and **Oracle Platform Security Services** as shown in the above screen.
7. Click **Next**. The following window is displayed.

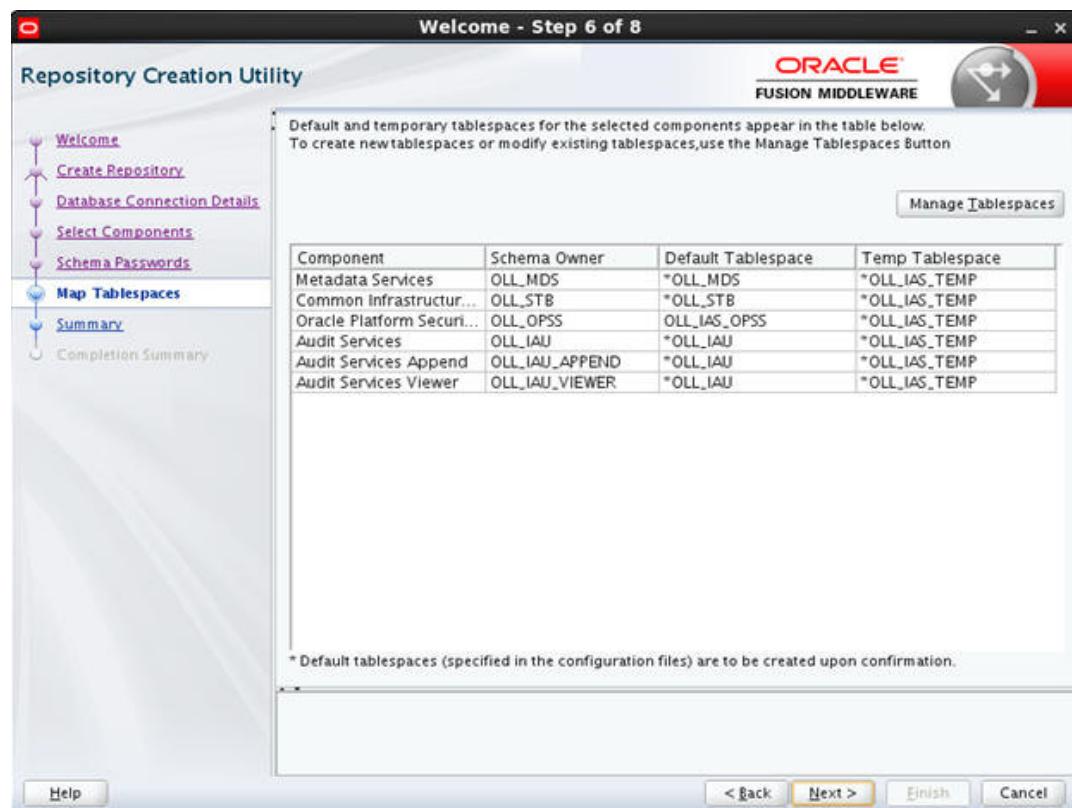


8. Click **Next..**

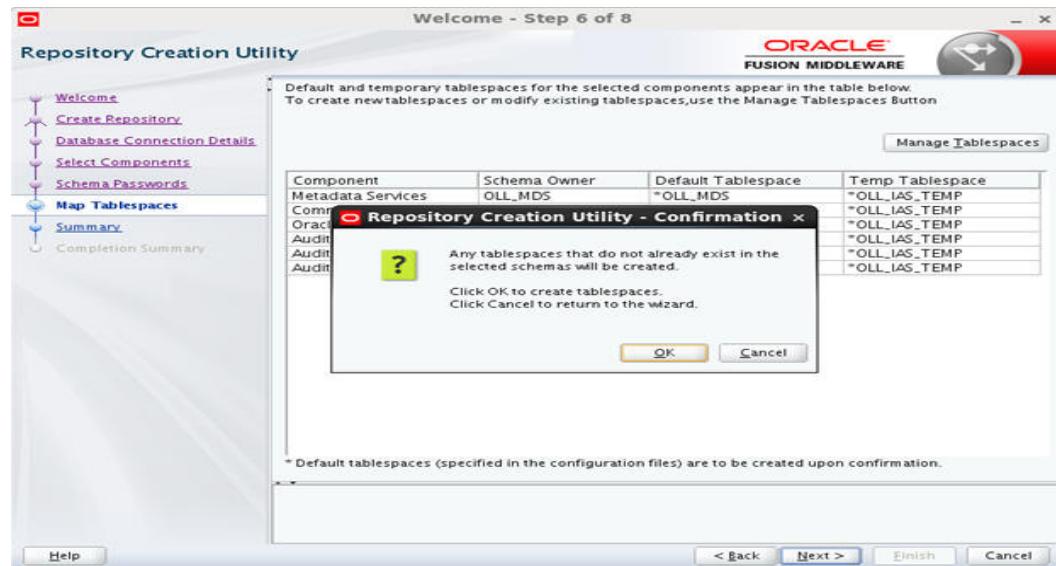


9. Select **Use Same Password for all schemas** and provide the Password OR **Select Specify different passwords for all schemas** and provide Schema Passwords for each server.

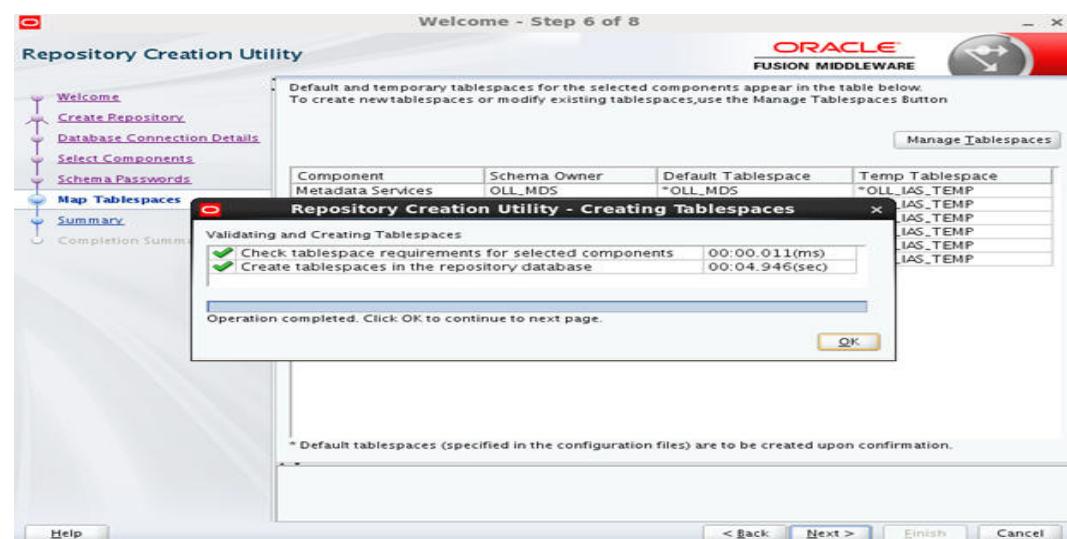
10. Click on Next to continue..



11. Click **Next**. The following window is displayed.



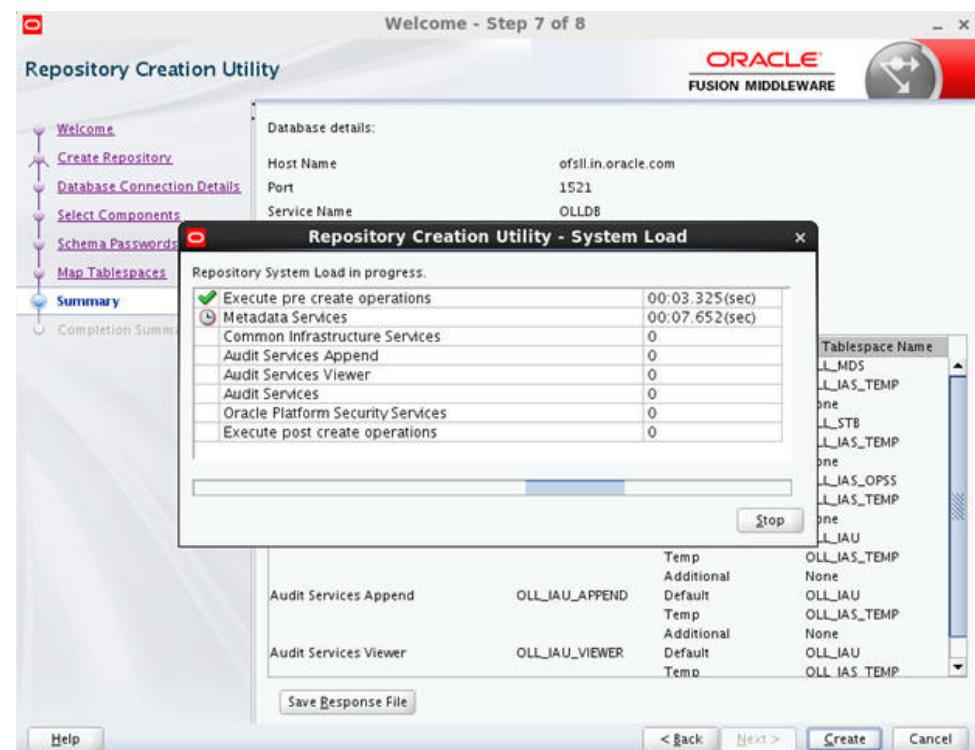
12. Click **OK**. The following window is displayed.

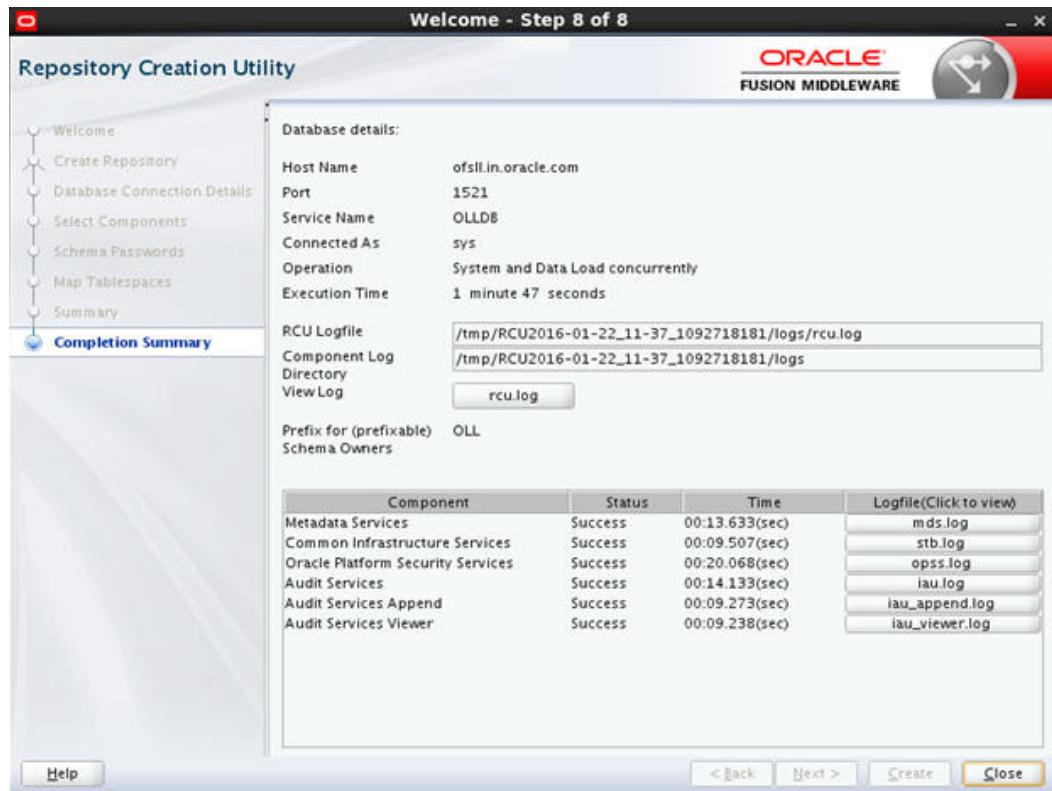


13. Click **OK**. The following window is displayed.



14. Click **Create**. The following windows are displayed.





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

3.3 Creating Metadata Repository

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

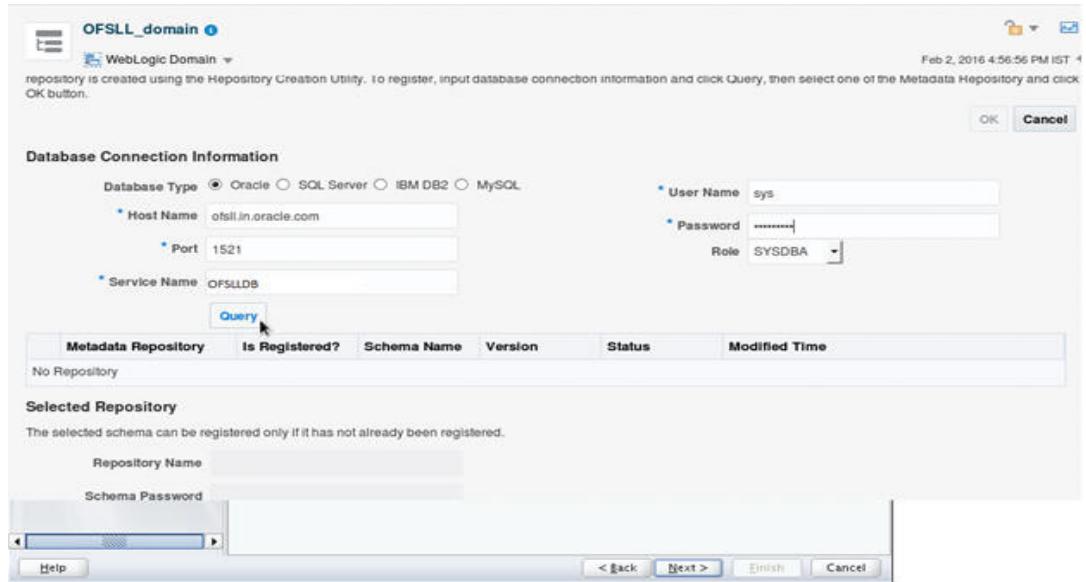
1. Login to Oracle Enterprise Manager 12c console (<http://hostname:port/em>).

The screenshot shows the Oracle Enterprise Manager interface. The left sidebar lists domains: 'OFSLL_domain' (selected), 'WebLogic Domain' (selected), 'Cluster', 'Deployment', 'Server', 'Logs', 'Environment', 'Deployments', 'JDBC Data Sources', 'Messaging', 'Cross Component Wiring', 'Web Services', 'Other Services' (selected), 'Administration', 'Refresh WebLogic Domain', 'Security', and 'System MBean Browser'. The right panel shows 'Domain Server' details: Name: AdminServer, Host: ofssl.in.oracle.com, Admin Port: 7001, Listen Port: 7002. Below this is a table of 'Metadata Repositories' with columns: Cluster, Machine, State. One entry is visible: Machine: Machine-0, State: Running. At the bottom, it says 'Columns Hidden: 33' and 'Servers: 2 of 2'.

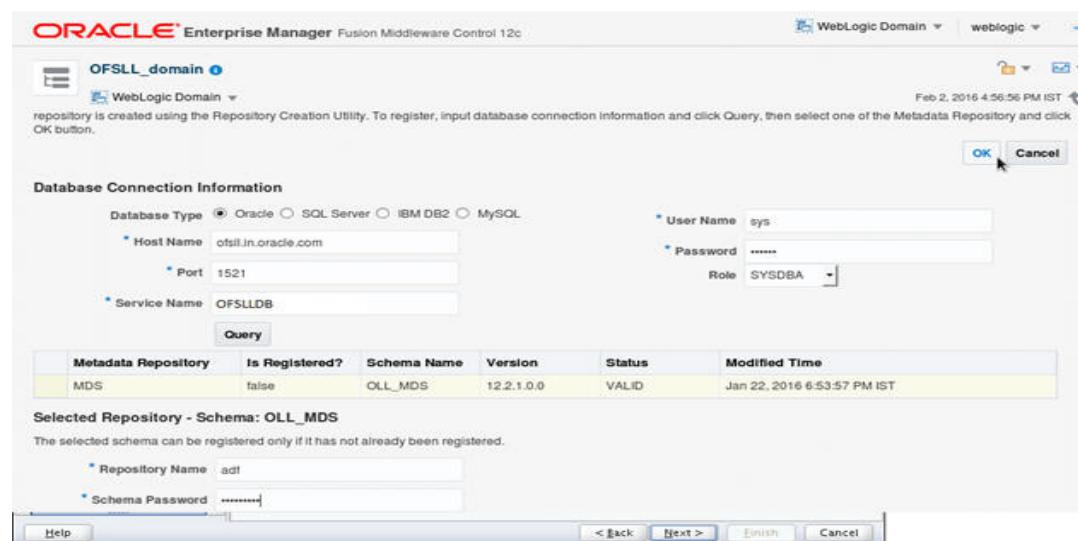
2. Click on domain name OFSLL_domain on the left side panel.
3. Expand Weblogic domain OFSLL_domain and click Metadata Repositories on right side panel, as shown above screen.
4. The following window is displayed.

The screenshot shows the 'Metadata Repositories' page. At the top, it says: 'You create most Fusion Middleware component schema repositories in a database using the Repository Creation Utility. Metadata Services (MDS) repositories can be created in a database with the Repository Creation Utility or created on disk as file-based repositories. You must register an MDS repository before you can deploy application metadata to the repository.' Below this are two sections: 'Database-Based Repositories' and 'File-Based Repositories'. Both sections have 'Register...' and 'Deregister...' buttons. The 'Database-Based Repositories' section shows a table with columns: Repository Name, Database Type, Database Name, Schema Name, JNDI Location, Partition, and Scope. The table is empty, showing 'No Repository'. The 'File-Based Repositories' section shows a similar table with columns: Repository Name, Directory, Partition, and Scope. It also shows 'No Repository'.

- Click Register button. The following window is displayed.



- Enter database instance details under Database Connection Information section and click **Query**.
- All available schemas in the given database instance are listed.
- Select the schema you require and enter **Repository Name (adf)** and the password under Selected Repository – Schema **OLL_MDS** section.
- Click OK. The following window is displayed.



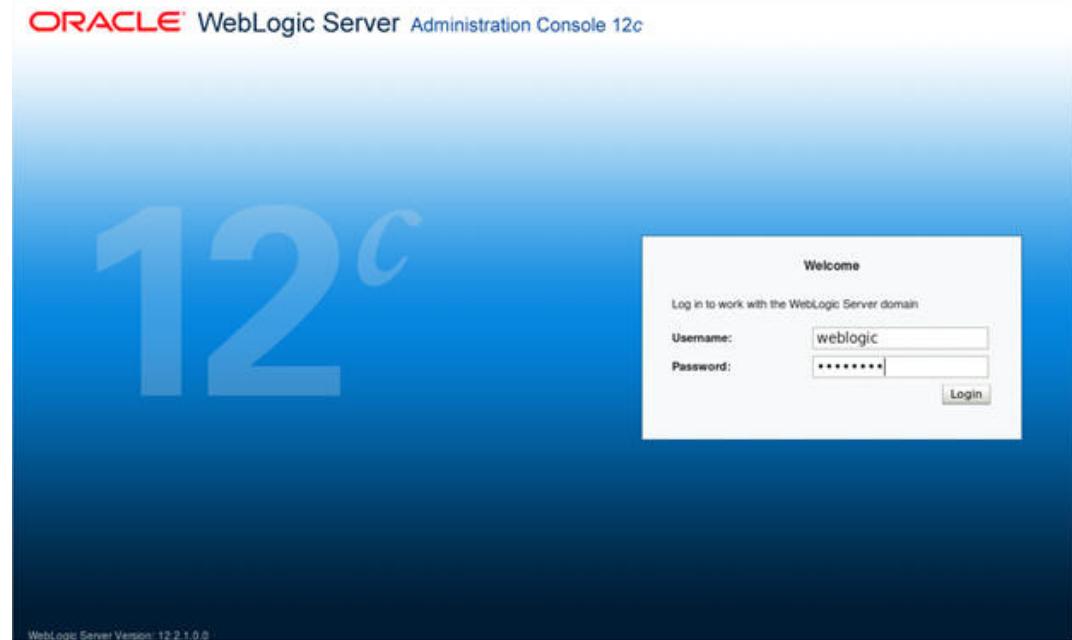
10. Click Repository name **mds-adf** on left panel. You can even select it from right panel.

Repository Name	Database Type	Database Name	Schema Name	JNDI Location	Partition	Scope
mds-adf	Oracle	OLLDB	OLL_MDS	jdbc/mds/adf	Global	Global

11. Click Add and target to OFSLL_AdminSever and OFSLL_ManagedServer as on right panel.

3.4 Creating Data Source

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



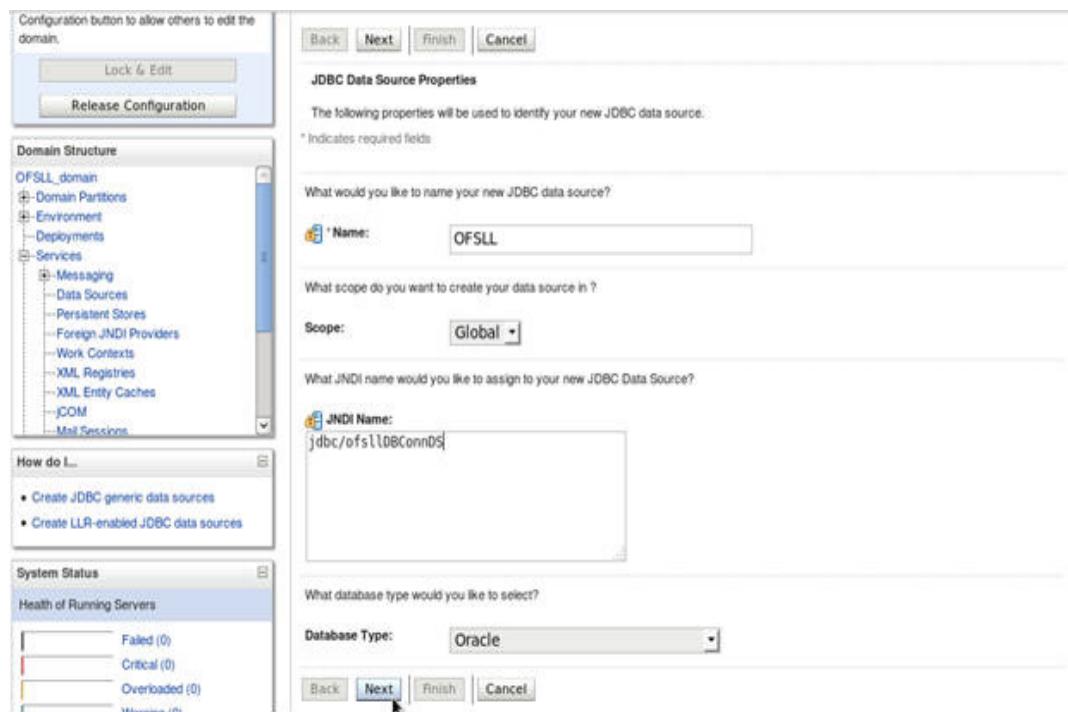
2. The following window is displayed.

3. Click Domain Name → Services → Data Sources.

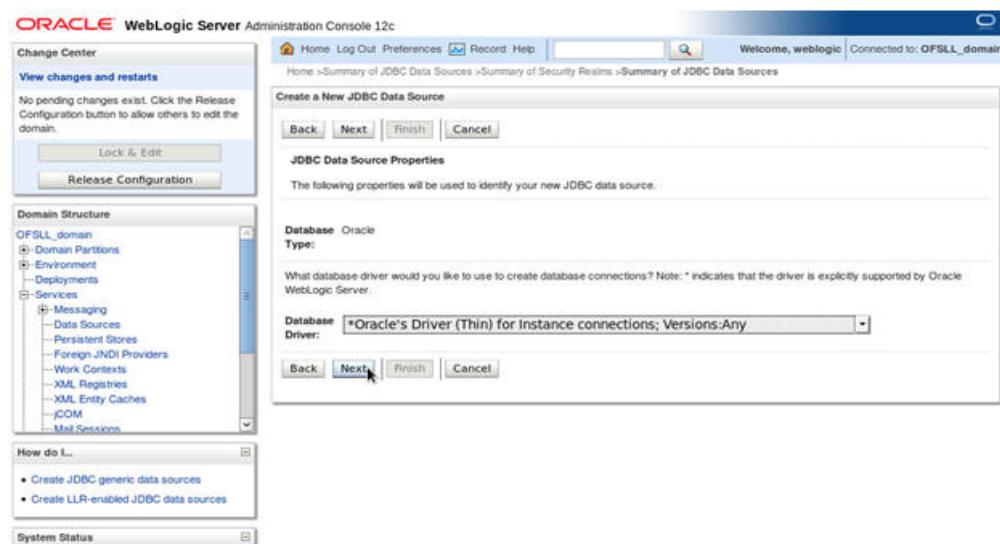
4. The following window is displayed.

New	Name	Type	JNDI Name	Targets	Scope	Domain Partitions
<input type="checkbox"/>	LocalSrvTbDataSource	Generic	jdbc/LocalSrvTbDataSource	AdminServer	Global	
<input type="checkbox"/>	ops-audit-DBDS	Generic	jdbc/AuditAppendDataSource	AdminServer, OFSLL_ManagedServer	Global	
<input type="checkbox"/>	ops-audit-viewDS	Generic	jdbc/AuditViewDataSource	AdminServer, OFSLL_ManagedServer	Global	
<input type="checkbox"/>	ops-data-source	Generic	jdbc/OpsDataSource	AdminServer, OFSLL_ManagedServer	Global	

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

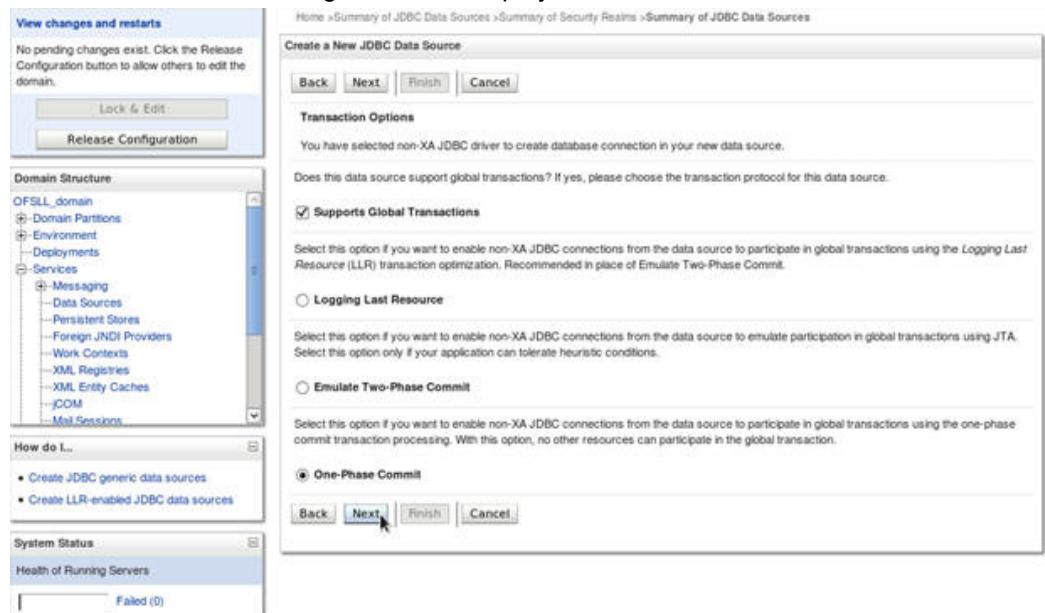


- Enter Data source Name
- Enter JNDI Name as **jdbc/ofsllDBConnDS**.
- Select Oracle as Database Type and click **Next**. The following window is displayed.

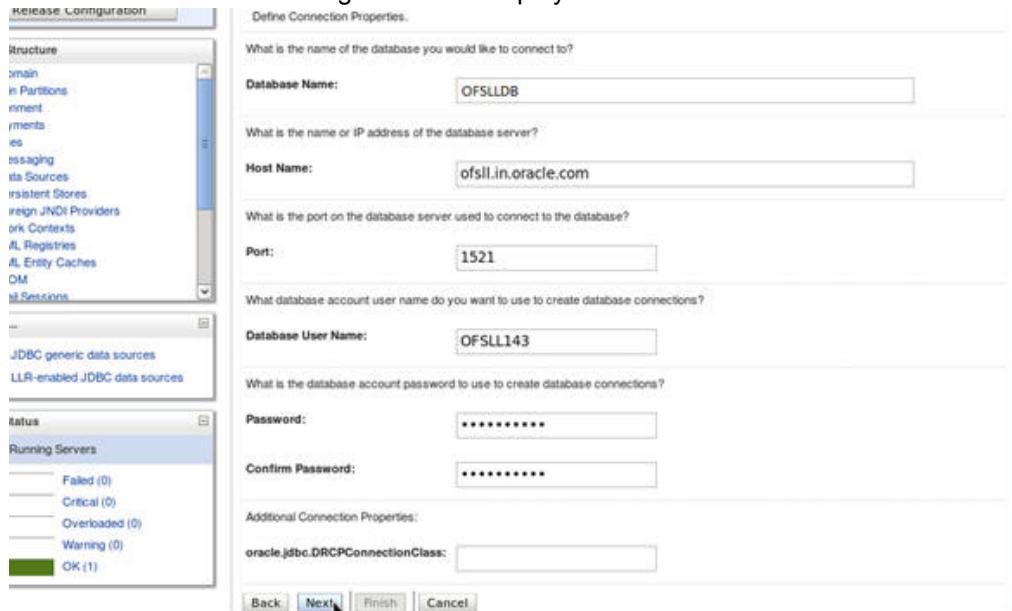


- Select the Database Driver "Oracle's Driver(Thin) for Instance connections; Versions:Any and later" as shown above.

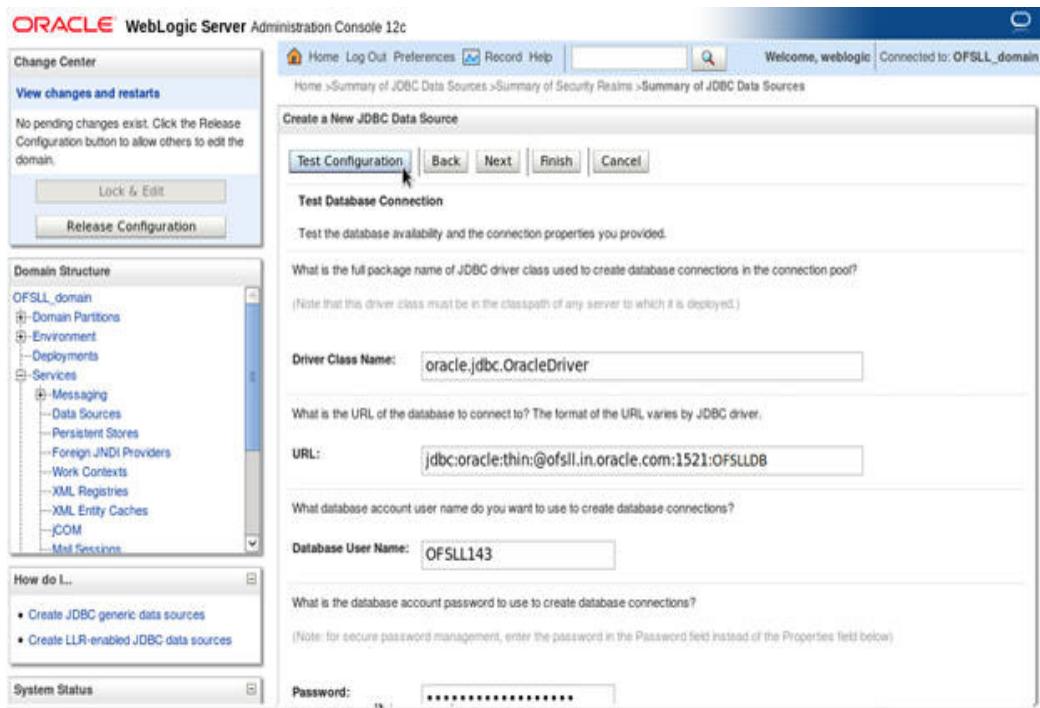
10. Click **Next**. The following window is displayed.



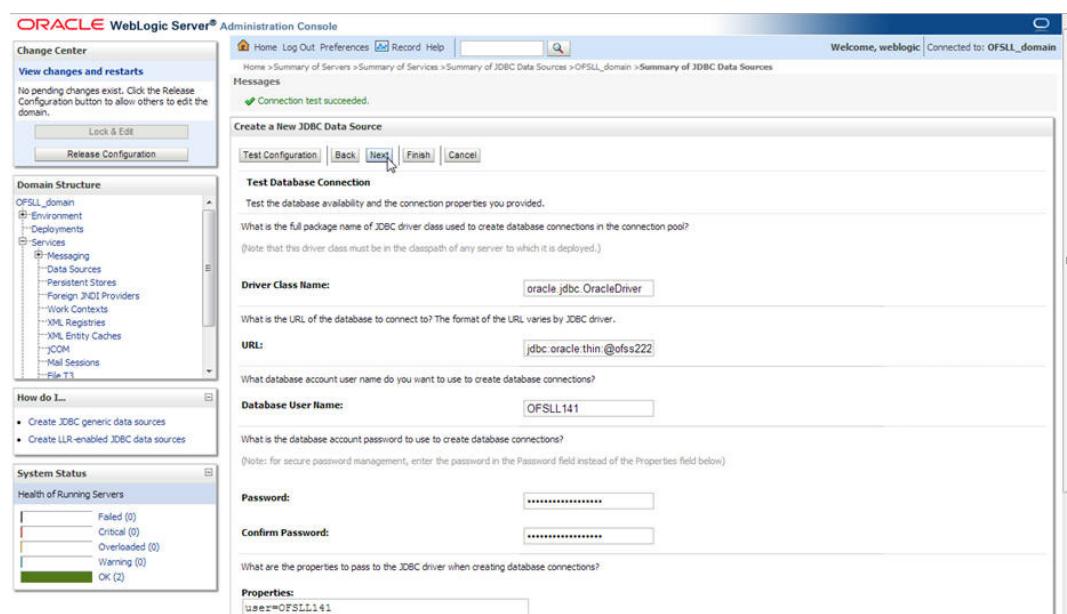
11. Click **Next**. The following window is displayed.



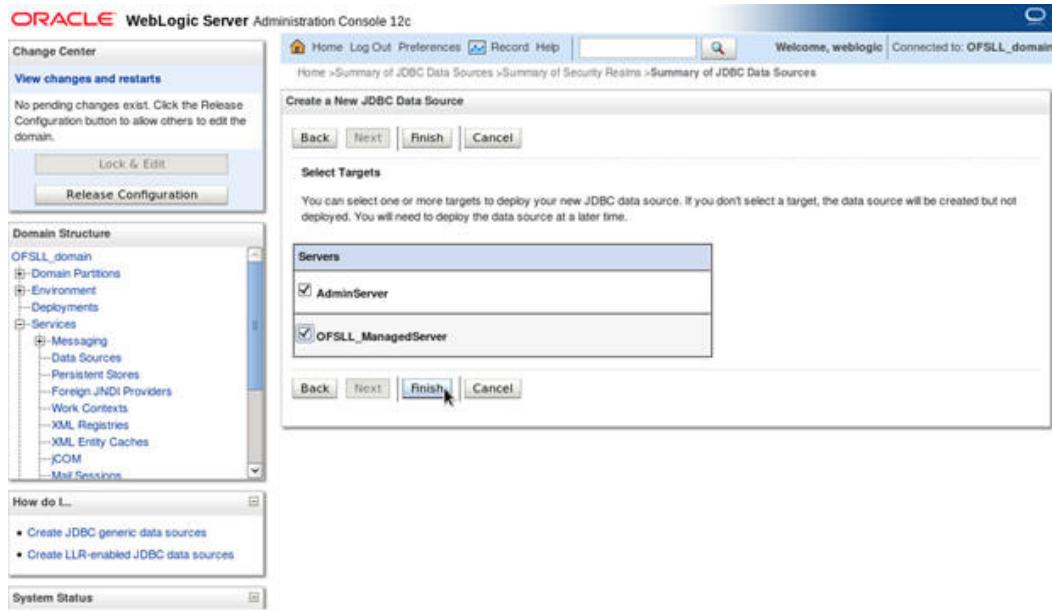
12. Enter Database details click **Next**. The following window is displayed.



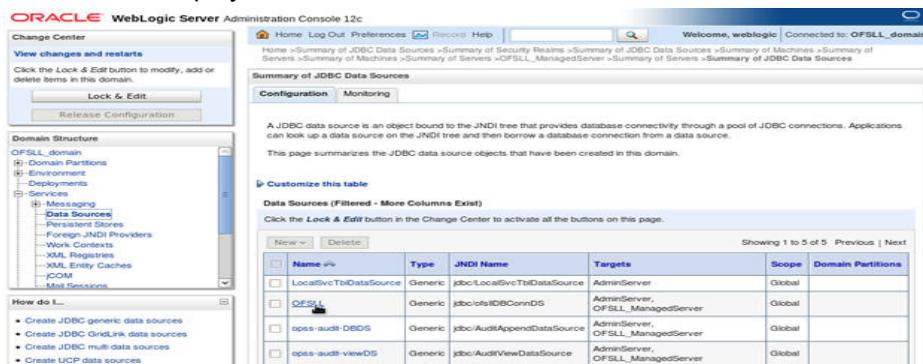
13. Click **Test Configuration**. The following window is displayed.



14. Displays confirmation message as "Connection test succeeded". Click **Next**. The following window is displayed.



15. Select target Servers **AdminServer** and **ManagedServer** and click **Finish**. The following window is displayed.



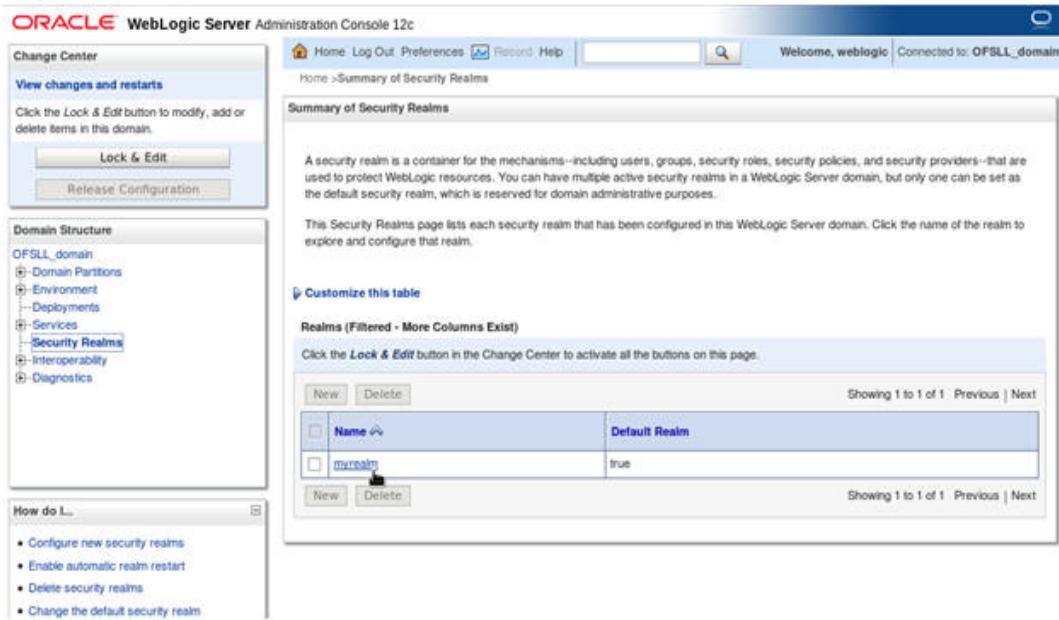
16. Click **Activate Changes** on the left panel.

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**.

3.5 Creating SQL Authentication Provider

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



ORACLE WebLogic Server Administration Console 12c

Change Center

View changes and restarts

Click the Lock & Edit button to modify, add or delete items in this domain.

Lock & Edit

Release Configuration

Domain Structure

OFSLI_domain

- Domain Partitions
- Environment
- Deployments
- Services
- Security Realms**
- Interoperability
- Diagnostics

How do I...

- Configure new security realms
- Enable automatic realm restart
- Delete security realms
- Change the default security realm

Summary of Security Realms

A security realm is a container for the mechanisms—including users, groups, security roles, security policies, and security providers—that are used to protect WebLogic resources. You can have multiple active security realms in a WebLogic Server domain, but only one can be set as the default security realm, which is reserved for domain administrative purposes.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

Customize this table

Realms (Filtered - More Columns Exist)

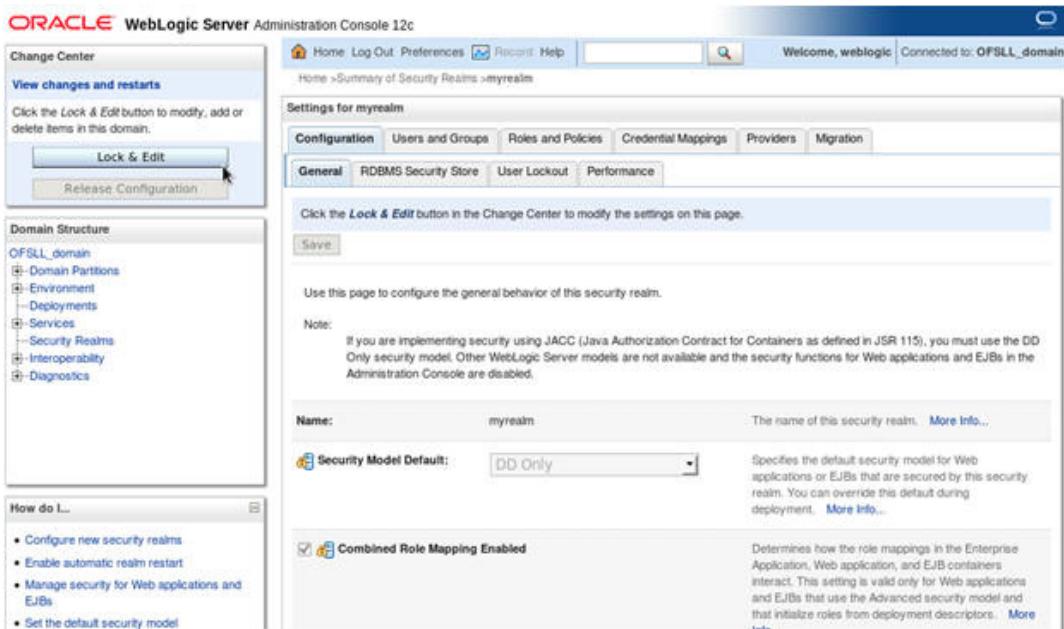
Click the Lock & Edit button in the Change Center to activate all the buttons on this page.

New	Delete	Name	Default Realm
New	Delete	myrealm	true

Showing 1 to 1 of 1 Previous | Next

Showing 1 to 1 of 1 Previous | Next

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



ORACLE WebLogic Server Administration Console 12c

Change Center

View changes and restarts

Click the Lock & Edit button to modify, add or delete items in this domain.

Lock & Edit

Release Configuration

Domain Structure

OFSLI_domain

- Domain Partitions
- Environment
- Deployments
- Services
- Security Realms
- Interoperability
- Diagnostics

How do I...

- Configure new security realms
- Enable automatic realm restart
- Manage security for Web applications and EJBs
- Set the default security model

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings Providers Migration

General RDBMS Security Store User Lockout Performance

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

Name: myrealm

Save

Note: If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.

Name: myrealm

Security Model Default: DD Only

Specifies the default security model for Web applications or EJBs that are secured by this security realm. You can override this default during deployment. [More Info...](#)

Combined Role Mapping Enabled

Determines how the role mappings in the Enterprise Application, Web application, and EJB containers interact. This setting is valid only for Web applications and EJBs that use the Advanced security model and that initialize roles from deployment descriptors. [More Info...](#)

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

ORACLE WebLogic Server Administration Console 12c

Change Center

View changes and restarts

No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Lock & Edit

Release Configuration

Domain Structure

OFSLL_domain

- Domain Partitions
- Environment
- Deployments
- Services
- Security Realms
- Interoperability
- Diagnostics

How do I...

- Configure Authentication and Identity Assertion providers
- Configure the Password Validation provider
- Manage security providers

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings Providers Migration

Authentication Password Validation Authorization Adjudication Role Mapping Auditing Credential Mapping Certification Path

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS.

Customize this table

Authentication Providers

New	Delete	Reorder	Showing 1 to 3 of 3 Previous Next		
Name	Description		Version		
Trust Service Identity Asserter	Trust Service Identity Assertion Provider		1.0		
DefaultAuthenticator	WebLogic Authentication Provider		1.0		
DefaultIdentityAssertor	WebLogic Identity Assertion provider		1.0		

New Delete Reorder Showing 1 to 3 of 3 Previous | Next

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

ORACLE WebLogic Server Administration Console 12c

Change Center

View changes and restarts

No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Lock & Edit

Release Configuration

Domain Structure

OFSLL_domain

- Domain Partitions
- Environment
- Deployments
- Services
- Security Realms
- Interoperability
- Diagnostics

How do I...

- Manage security providers
- Configure Authentication and Identity Assertion providers

System Status

Health of Running Servers

Create a New Authentication Provider

OK Cancel

Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.

* Indicates required fields

The name of the authentication provider.

* Name: OFSLLDBAuthenticator

This is the type of authentication provider you wish to create.

Type: SQLAuthenticator

OK Cancel

5. Create Authentication provider with following values.

Name: **OFSLLDBAuthenticator**

Type: **SQLAuthenticator**

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

The screenshot shows the Oracle WebLogic Server Administration Console 12c. The left sidebar shows the 'Domain Structure' with 'OFSLL_domain' selected. The main content area is titled 'Settings for myrealm' and shows the 'Providers' tab selected. A table lists four authentication providers:

Name	Description	Version
Trust Service Identity Assembler	Trust Service Identity Assertion Provider	1.0
DefaultAuthenticator	WebLogic Authentication Provider	1.0
DefaultIdentityAssembler	WebLogic Identity Assertion provider	1.0
OFSLLDBAuthenticator	Provider that performs DBMS authentication	1.0

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

The screenshot shows the Oracle WebLogic Server Administration Console 12c. The left sidebar shows the 'Domain Structure' with 'OFSLL_domain' selected. The main content area is titled 'Settings for myrealm' and shows the 'Providers' tab selected. A table lists four authentication providers:

Name	Description	Version
OFSLLDBAuthenticator	Provider that performs DBMS authentication	1.0
DefaultAuthenticator	WebLogic Authentication Provider	1.0
DefaultIdentityAssembler	WebLogic Identity Assertion provider	1.0
Trust Service Identity Assembler	Trust Service Identity Assertion Provider	1.0

Authentication order should be maintained as mentioned in the above screen.

8. **OFSLLDBAuthenticator** will be displayed as above.

9. Click on **OFSLLDBAuthenticator**.

10. The following window is displayed.

The screenshot shows the Oracle WebLogic Server Administration Console. The title bar says 'ORACLE WebLogic Server Administration Console 12c'. The main content area is titled 'Settings for OFSLLDBAuthenticator' under the 'Configuration' tab. It shows the following configuration details:

- Name:** OFSLLDBAuthenticator
- Description:** Provider that performs DBMS authentication
- Version:** 1.0
- Control Flag:** SUFFICIENT

A 'Save' button is visible at the bottom of the configuration panel. A 'How do I...' sidebar on the left provides links for managing authentication providers and security providers.

11. Select **SUFFICIENT** as the **Control Flag** and click **Save**.

12. Click Provider Specific sub tab under Configuration tab. The following window is displayed.

The screenshot shows the 'Provider Specific' configuration for the OFSLLDBAuthenticator provider. The configuration tabs are 'Configuration' (selected) and 'Performance'. The 'Provider Specific' sub-tab is selected. The configuration fields are:

- Identity Domain:** (empty text field)
- Data Source Name:** OFSLL
- Group Membership Searching:** unlimited
- Max Group Membership Search Level:** 0
- Password Style Retained:** (unchecked checkbox)
- Password Algorithm:** SHA-512

A 'Save' button is visible at the top of the configuration panel. A 'How do I...' sidebar on the left provides links for managing authentication providers and security providers. A 'System Status' sidebar on the left shows the health of running servers.

13. Provide the following values in corresponding fields.

Data Source Name: OFSLL

Password Style Retained: Uncheck

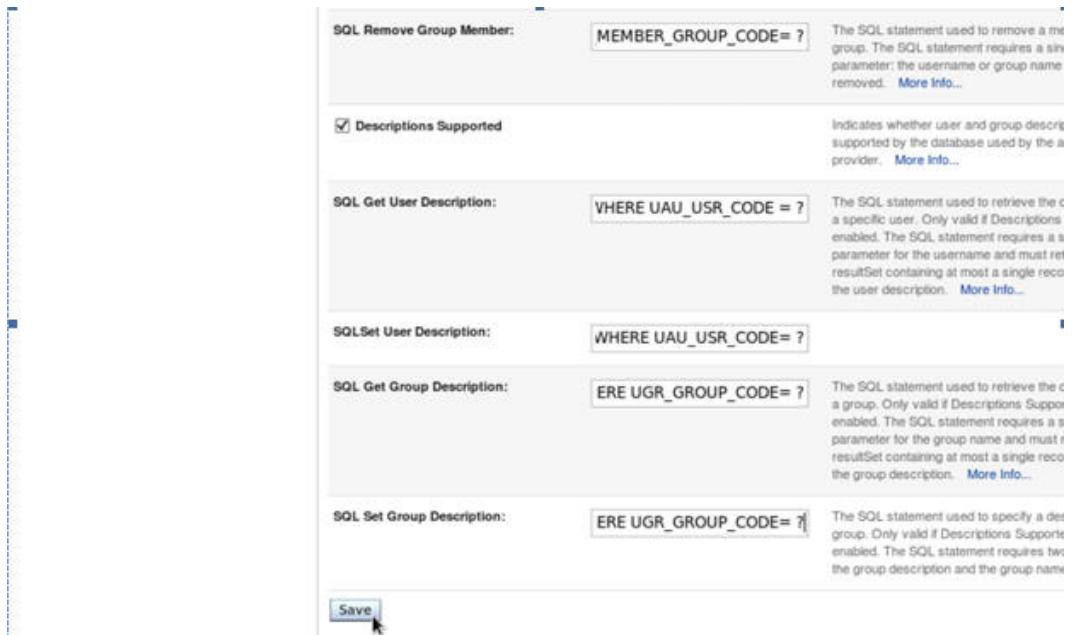
Password Algorithm: SHA-512

Password Style: SALTEDHASHED

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

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

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



14. Click Save.

Note

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

3.6 Creating User Groups and Users

3.6.1 Creating Users

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

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

Note

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

Run the script "crt_app_user.sql" script" as a OFSLL application owner user.

```

SQL*Plus: Release 12.1.0.2.0 Production on Thu Feb 4 12:47:05 2016
Copyright (c) 1982, 2014, Oracle. All rights reserved.

Enter user-name: OFSLI143TEST1
Enter password:
Last Successful login time: Thu Feb 04 2016 12:02:37 +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> @/home/dev/Desktop/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: 99999777321
Enter the Fax Number for this user: 9999888321
1 row created.

1 row created.

1 row created.

SQL> ■

```

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

ORACLE WebLogic Server Administration Console 12c

Home >Summary of Security Realms

Summary of Security Realms

A security realm is a container for the mechanisms—including users, groups, security roles, security policies, and security providers—that are used to protect WebLogic resources. You can have multiple active security realms in a WebLogic Server domain, but only one can be set as the default security realm, which is reserved for domain administrative purposes.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

Customize this table

Realms (Filtered - More Columns Exist)

Click the Lock & Edit button in the Change Center to activate all the buttons on this page.

<input type="checkbox"/>	Name ↗	Default Realm
<input type="checkbox"/>	myrealm	true

Showing 1 to 1 of 1 Previous | Next

How do I...

- Configure new security realms
- Enable automatic realm restart
- Delete security realms
- Change the default security realm

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

ORACLE WebLogic Server Administration Console 12c

Home >Summary of Security Realms >myrealm >Users and Groups >Summary of Security Realms >myrealm >OFSLL_USER >myrealm >Users and Groups >DEMOUSR >Users and Groups

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings Providers Migration

Users Groups

This page displays information about each user that has been configured in this security realm.

Customize this table

Users (Filtered - More Columns Exist)

<input type="checkbox"/>	Name ↗	Description	Provider
<input type="checkbox"/>	DEMOUSR	DEMO SUPR	OFSLLDBAuthenticator
<input type="checkbox"/>	LCMUser	This is the default service account for WebLogic Server Lifecycle Manager configuration updates.	DefaultAuthenticator
<input type="checkbox"/>	OracleSystemUser	Oracle application software system user.	DefaultAuthenticator
<input type="checkbox"/>	TESTUSER	TEST USER	OFSLLDBAuthenticator
<input type="checkbox"/>	weblogic	This user is the default administrator.	DefaultAuthenticator

Showing 1 to 5 of 5 Previous | Next

How do I...

- Manage users and groups
- Create users
- Modify users
- Delete users

3.6.2 Creating User Groups

1. Select **Groups** tab under **Users and Groups**.

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

Name	Description	Provider
AdminChannelUsers	AdminChannelUsers can access the admin channel.	DefaultAuthenticator
Administrators	Administrators can view and modify all resource attributes and start and stop servers.	DefaultAuthenticator
AppTesters	AppTesters group.	DefaultAuthenticator
CrossDomainConnectors	CrossDomainConnectors can make inter-domain calls from foreign domains.	DefaultAuthenticator
Deployers	Deployers can view all resource attributes and deploy applications.	DefaultAuthenticator
Monitors	Monitors can view and modify all resource attributes and perform operations not restricted by roles.	DefaultAuthenticator
OFSLL_USER	Operators can view and modify all resource attributes and perform server lifecycle operations.	OFSLLDAuthenticator
Operators	Operators can view and modify all resource attributes and perform server lifecycle operations.	DefaultAuthenticator
OracleSystemGroup	Oracle application software system group.	DefaultAuthenticator

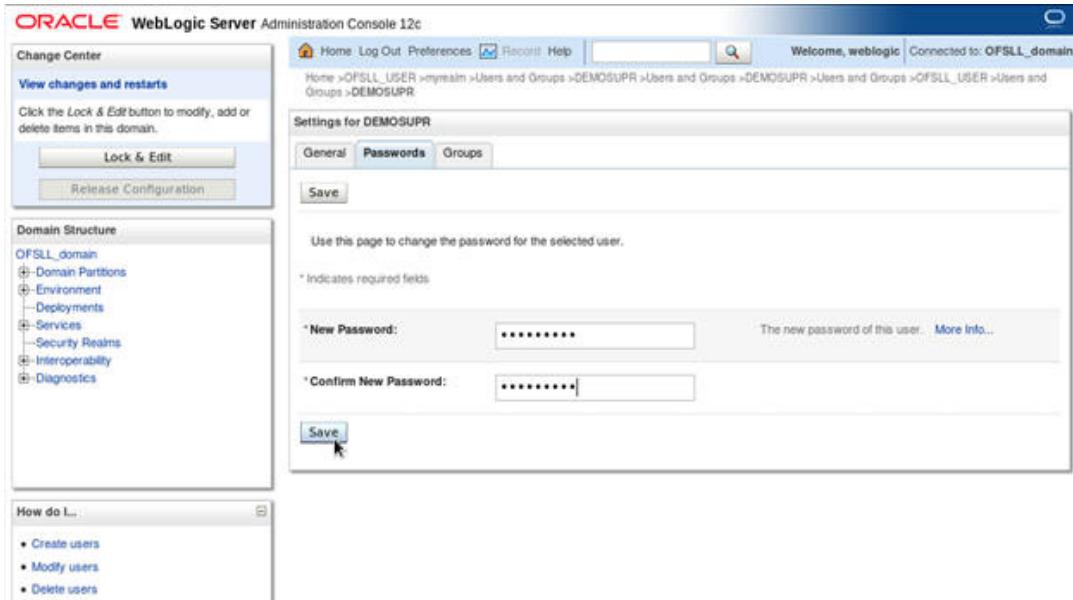
3.6.3 Assigning Users to Groups

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

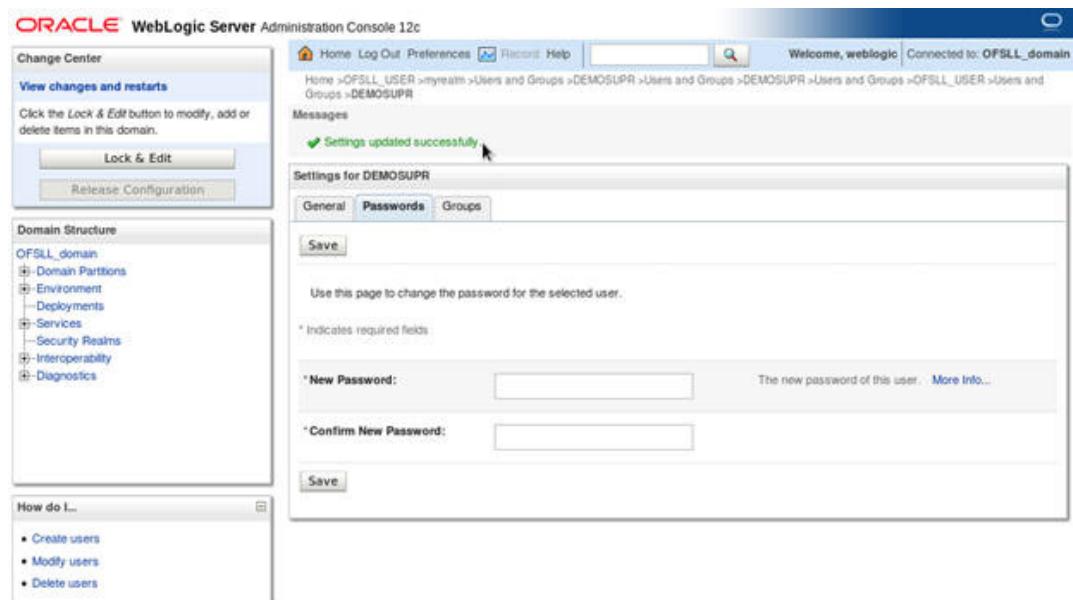
The screenshot shows the 'Groups' tab in the 'Users and Groups' section. In the 'Available' list, there is one item: 'OFSLL_USER'. In the 'Chosen' list, there is one item: 'OFSLL_USER'. A tooltip indicates that the user can be a member of any of these parent groups.

3.6.4 Resetting password via weblogic console

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



2. Click on **Save**. The following window displayed.



3.7 Implementing JMX Policy for Change Password

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

Note

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

2. Click Domain → Security → myrealm → Configuration

The screenshot shows the Oracle WebLogic Server Administration Console 12c. The left sidebar shows a 'Domain Structure' with 'OFSLL_domain' expanded, containing 'Domain Partitions', 'Environment', 'Deployments', 'Services', 'Security Realms', 'Interoperability', and 'Diagnostics'. A 'Change Center' section with 'View changes and restarts' and a 'Lock & Edit' button is present. A 'How do I...' panel lists tasks like 'Configure new security realms', 'Enable automatic realm restart', and 'Manage security for Web applications and EJBs'. A 'System Status' panel shows 'Health of Running Servers' with 2 OK servers. The main right panel is titled 'Settings for myrealm' and has a 'Configuration' tab selected. It shows the 'Name' as 'myrealm'. Under 'Security Model Default', 'DD Only' is selected. The 'Combined Role Mapping Enabled' checkbox is checked. The 'Use Authorization Providers to Protect JMX Access' checkbox is checked. A note at the bottom states: 'If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.' A 'Save' button is at the bottom.

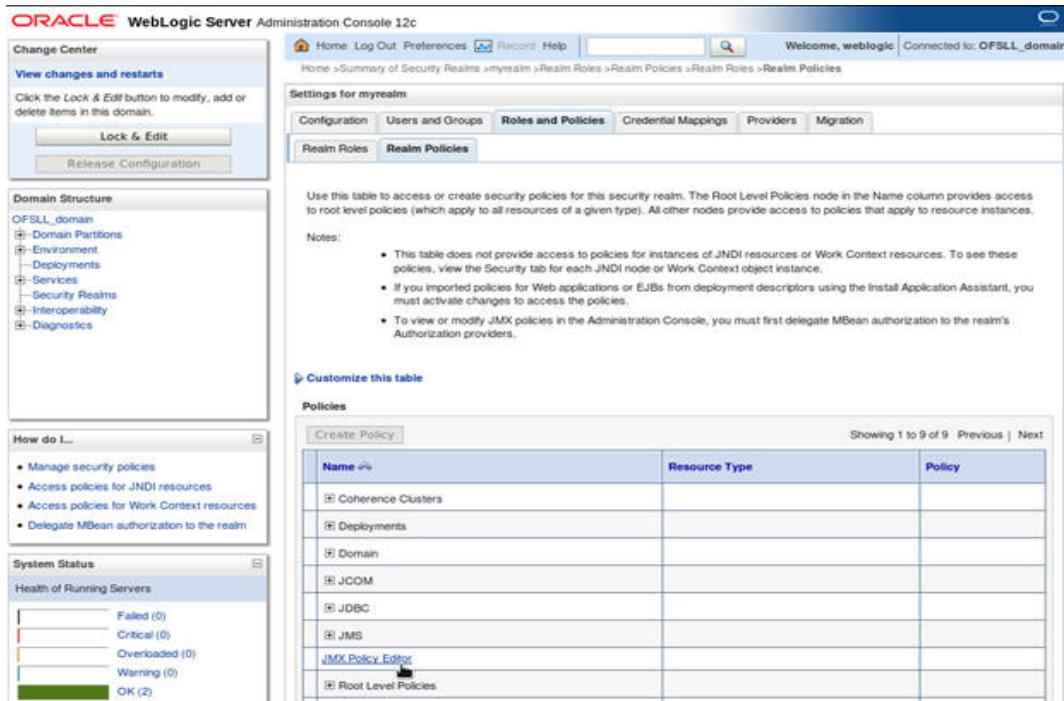
3. To enable JMX policy select the "Use Authorization Providers to Protect JMX Access" check box on the right panel

The screenshot shows the Oracle WebLogic Server Administration Console 12c. The left sidebar and 'Change Center' are identical to the previous screenshot. The main right panel is titled 'Settings for myrealm' and has a 'Configuration' tab selected. It shows the 'Name' as 'myrealm'. Under 'Security Model Default', 'DD Only' is selected. The 'Combined Role Mapping Enabled' checkbox is checked. The 'Use Authorization Providers to Protect JMX Access' checkbox is checked. A note at the bottom states: 'If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.' A 'Save' button is at the bottom.

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

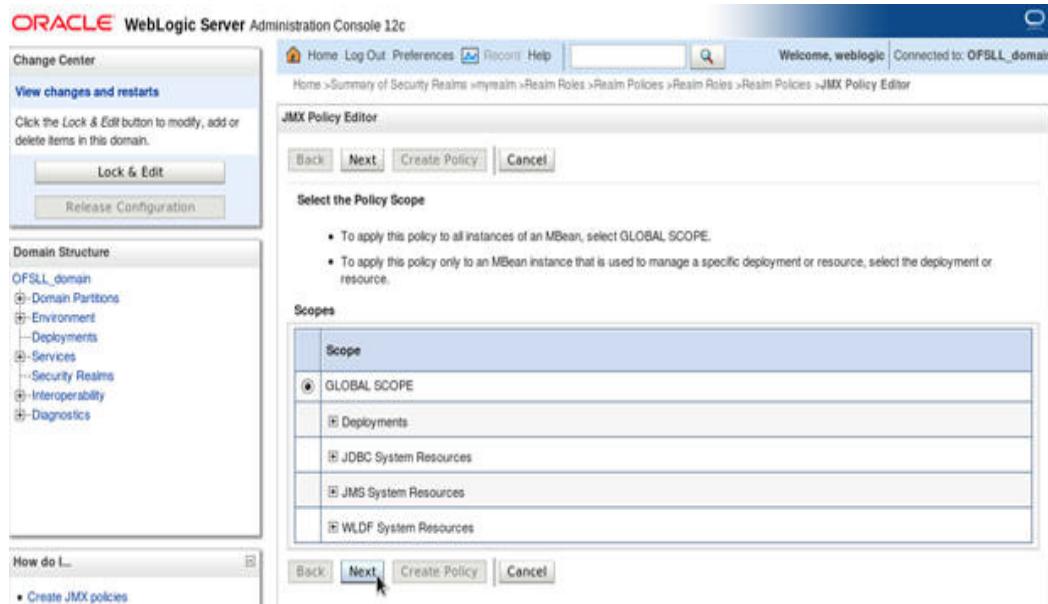
Note

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



The screenshot shows the Oracle WebLogic Server Administration Console 12c interface. The main title bar reads "ORACLE WebLogic Server Administration Console 12c". The top navigation bar includes "Home", "Log Out", "Preferences", "Record", "Help", "Welcome, weblogic", and "Connected to: OFSLL_domain". The current page is "Home >Summary of Security Realms >myrealm >Realm Roles >Realm Policies >Realm Policies >Realm Policies". The left sidebar has sections for "Change Center", "View changes and restarts", "Domain Structure" (listing "OFSLL_domain" with sub-nodes: "Domain Partitions", "Environment", "Deployments", "Services", "Security Realms", "Interoperability", and "Diagnostics"), "How do I..." (with options: "Manage security policies", "Access policies for JNDI resources", "Access policies for Work Context resources", and "Delegate MBean authorization to the realm"), and "System Status" (listing "Health of Running Servers" with categories: "Failed (0)", "Critical (0)", "Overloaded (0)", "Warning (0)", and "OK (2)"). The main content area is titled "Settings for myrealm" and shows tabs for "Configuration", "Users and Groups", "Roles and Policies", "Credential Mappings", "Providers", and "Migration". The "Roles and Policies" tab is selected, showing sub-tabs "Realm Roles" and "Realm Policies". A note states: "Use this table to access or create security policies for this security realm. The Root Level Policies node in the Name column provides access to root level policies (which apply to all resources of a given type). All other nodes provide access to policies that apply to resource instances." Below this is a list of notes: "This table does not provide access to policies for instances of JNDI resources or Work Context resources. To see these policies, view the Security tab for each JNDI node or Work Context object instance.", "If you imported policies for Web applications or EJBs from deployment descriptors using the Install Application Assistant, you must activate changes to access the policies.", and "To view or modify JMX policies in the Administration Console, you must first delegate MBean authorization to the realm's Authorization providers." A "Customize this table" link is present. The "Policies" table has columns: "Name", "Resource Type", and "Policy". The table lists several items: "Coherence Clusters", "Deployments", "Domain", "JCOM", "JDBC", "JMS", "JMX Policy Editor" (which is highlighted with a black box), and "Root Level Policies". The "JMX Policy Editor" row is selected. The table shows 9 items in total, with "Showing 1 to 9 of 9".

7. Click on JMX Policy Editor to configure



The screenshot shows the "JMX Policy Editor" configuration dialog. The title bar reads "ORACLE WebLogic Server Administration Console 12c". The top navigation bar is the same as the previous screenshot. The current page is "Home >Summary of Security Realms >myrealm >Realm Roles >Realm Policies >Realm Policies >JMX Policy Editor". The left sidebar is identical to the previous screenshot. The main content area is titled "JMX Policy Editor". It has buttons for "Back", "Next", "Create Policy", and "Cancel". A sub-section titled "Select the Policy Scope" contains the following text: "To apply this policy to all instances of an MBean, select GLOBAL SCOPE. To apply this policy only to an MBean instance that is used to manage a specific deployment or resource, select the deployment or resource." Below this is a "Scopes" section with a table. The table has columns: "Scope" and "GLOBAL SCOPE". The "GLOBAL SCOPE" row is selected. Other rows include "Deployments", "JDBC System Resources", "JMS System Resources", and "WLDF System Resources". The "Next" button is highlighted with a black box.

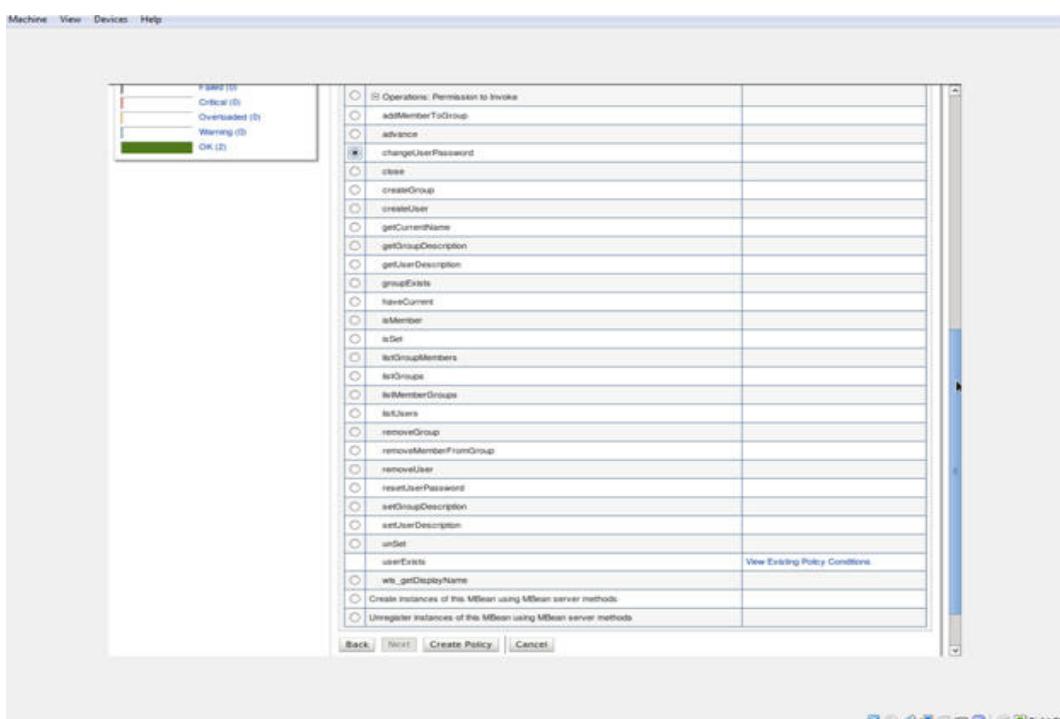
8. Select GLOBAL SCOPE

9. Click Next



10. Select `weblogic.security.providers.authentication`.

11. Select "SQLAuthenticatorMBean". Click **Next**.



12. Expand "Operations: Permissions to Invoke" and select "ChangePassword"

13. Click "Create Policy"

14. It opens the below screen for Authorization providers where you can add conditions to setup the policy.

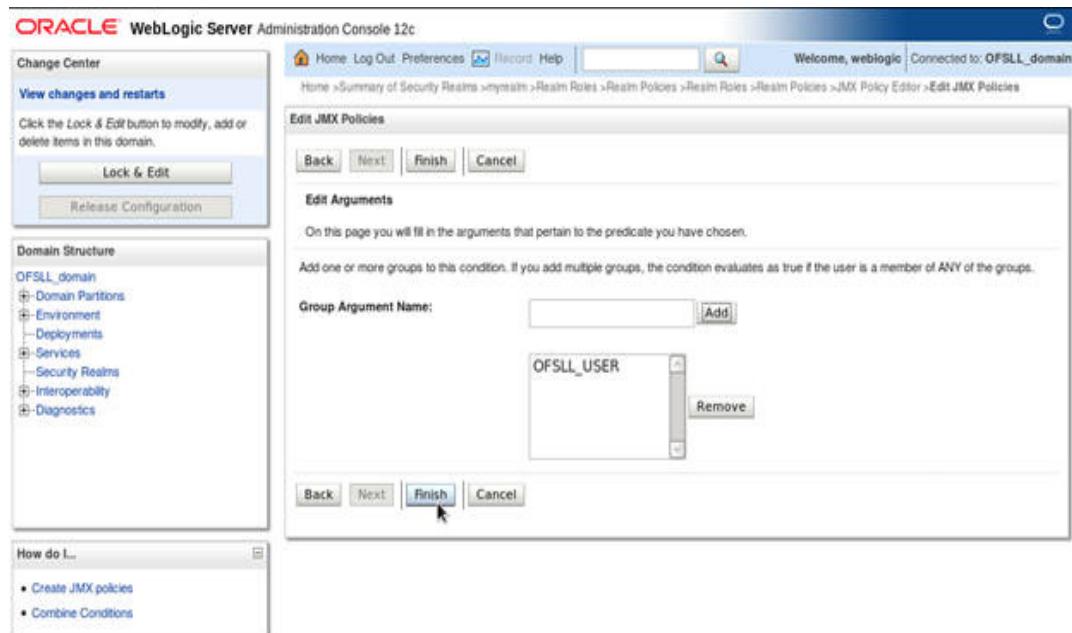
The screenshot shows the Oracle WebLogic Server Administration Console 12c interface. The title bar reads 'ORACLE WebLogic Server Administration Console 12c'. The left sidebar shows a 'Domain Structure' with 'OFSLL_domain' expanded, containing 'Domain Partitions', 'Environment', 'Deployments', 'Services', 'Security Realms', 'Interoperability', and 'Diagnostics'. A 'Change Center' section with 'View changes and restarts' and 'Lock & Edit' buttons is also present. The main content area is titled 'Edit JMX Policies' with a 'Save' button. It contains a section for 'Providers' (selected 'XACMLAuthorizer') and 'Policy Conditions' (with buttons for 'Add Conditions', 'Combine', 'Uncombine', 'Move Up', 'Move Down', 'Remove', and 'Negate'). A 'Policy Used By Default' section shows 'Role : Admin'. A 'How do I...' sidebar lists 'Create JMX policies' and 'Combine Conditions'.

15. Click **Add Condition**. The below screen will be displayed.

This screenshot is identical to the previous one, showing the 'Edit JMX Policies' page. The 'Add Conditions' button is highlighted with a cursor, indicating it is the next step to be clicked.

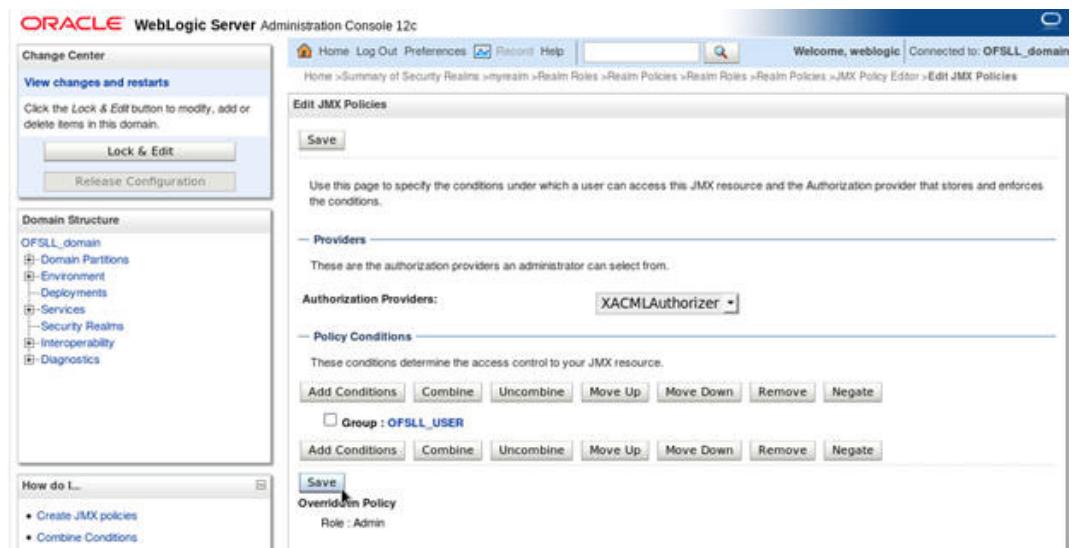
16. For **Predicate List**, select **Group** for configuration.

17. Click Next.



18. Select user roles for application.

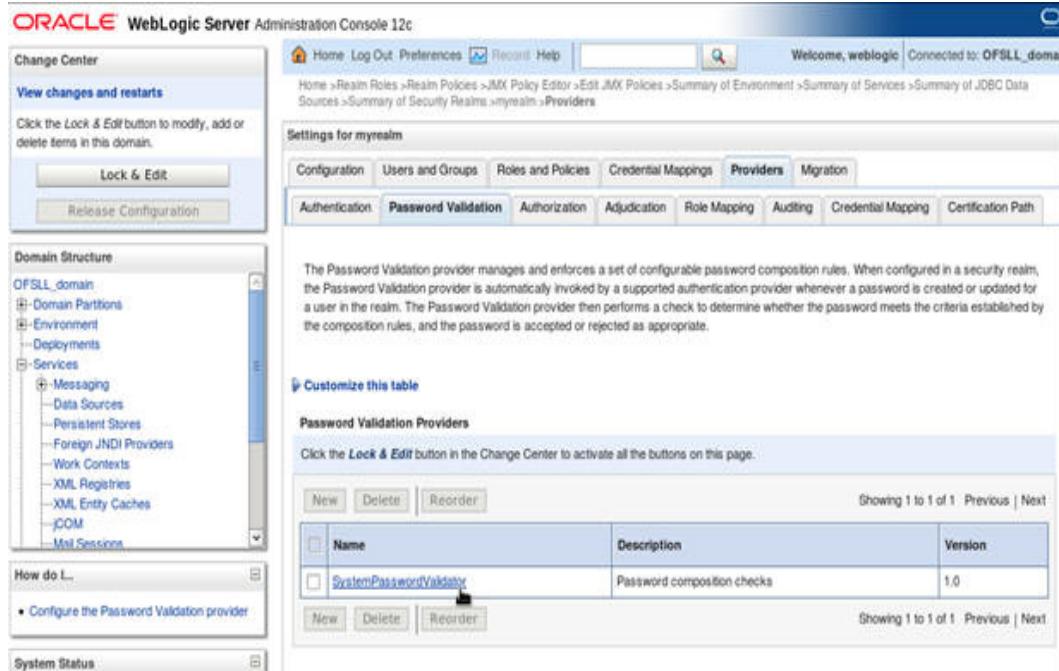
19. Click Finish. Click on Save to complete the configuration. The following window will be displayed.



4. Configuring Policies

4.1 Configuring Password Policy for SQL Authenticator

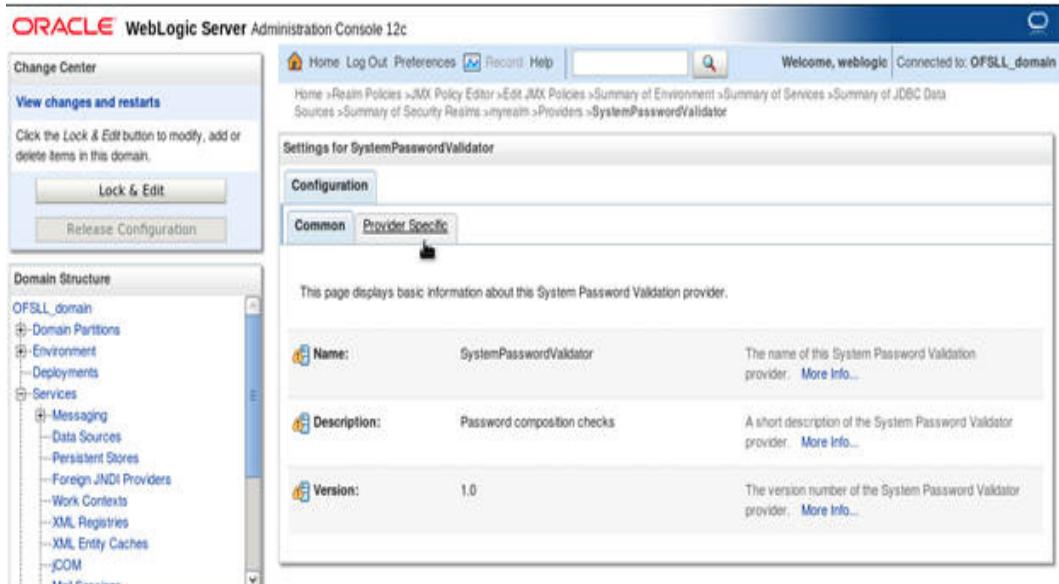
1. Login to the WebLogic server administration console with user login credentials.
2. Browse to **Security Realms** → **myrealm** → **Providers** as shown below. The following window is displayed



The screenshot shows the Oracle WebLogic Server Administration Console 12c. The left sidebar shows the 'Domain Structure' for 'OFSL_domain' with 'Services' expanded, showing 'Messaging', 'Data Sources', 'Persistent Stores', 'Foreign JNDI Providers', 'Work Contexts', 'XML Registries', 'XML Entity Caches', 'JCOM', and 'Mail Sessions'. The main content area is titled 'Settings for myrealm' and has a 'Providers' tab selected. Below the tabs, a table lists 'Password Validation Providers' with one entry: 'SystemPasswordValidator'.

Name	Description	Version
SystemPasswordValidator	Password composition checks	1.0

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



The screenshot shows the 'Settings for SystemPasswordValidator' page. The 'Provider Specific' tab is selected. The page displays basic information about the System Password Validation provider, including its name, description, and version.

Name:	SystemPasswordValidator	The name of this System Password Validation provider. More Info...
Description:	Password composition checks	A short description of the System Password Validator provider. More Info...
Version:	1.0	The version number of the System Password Validator provider. More Info...

4. Click **Provider Specific** Tab.
5. Configure the password policy as per the requirement. The following window is displayed. Click Save.

4.2 Configuring User Lockout Policy

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

The screenshot shows the Oracle WebLogic Server Administration Console 12c interface. On the left, the 'Change Center' sidebar includes 'View changes and restarts', 'Domain Structure' (listing OFSLL_domain, Domain Partitions, Environment, Deployments, Services, and Messaging), 'How do I...' (Set user lockout attributes, Unlock user accounts), and 'System Status' (Health of Running Servers). The main content area is titled 'Settings for myrealm' and has tabs for Configuration, Users and Groups, Roles and Policies, Credential Mappings, Providers, and Migration. The 'User Lockout' tab is selected. A sub-tab bar at the bottom of the content area includes General, RDBMS Security Store, User Lockout (selected), and Performance. A descriptive text box explains the purpose of the User Lockout settings. Below this are five configuration fields with their current values and descriptions:

Setting	Value	Description
Lockout Enabled	<input checked="" type="checkbox"/>	Specifies whether the server locks users out when there are invalid login attempts on their account. More Info...
Lockout Threshold	5	The maximum number of consecutive invalid login attempts that can occur before a user's account is locked out. More Info...
Lockout Duration	30	The number of minutes that a user's account is locked out. More Info...
Lockout Reset Duration	5	The number of minutes within which consecutive invalid login attempts cause a user's account to be locked out. More Info...
Lockout Cache Size	5	The maximum number of invalid login records that the server can place in a cache. More Info...
Lockout GC Threshold	400	The maximum number of invalid login records that the server keeps in memory. More Info...

A 'Save' button is located at the bottom of the configuration area.

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

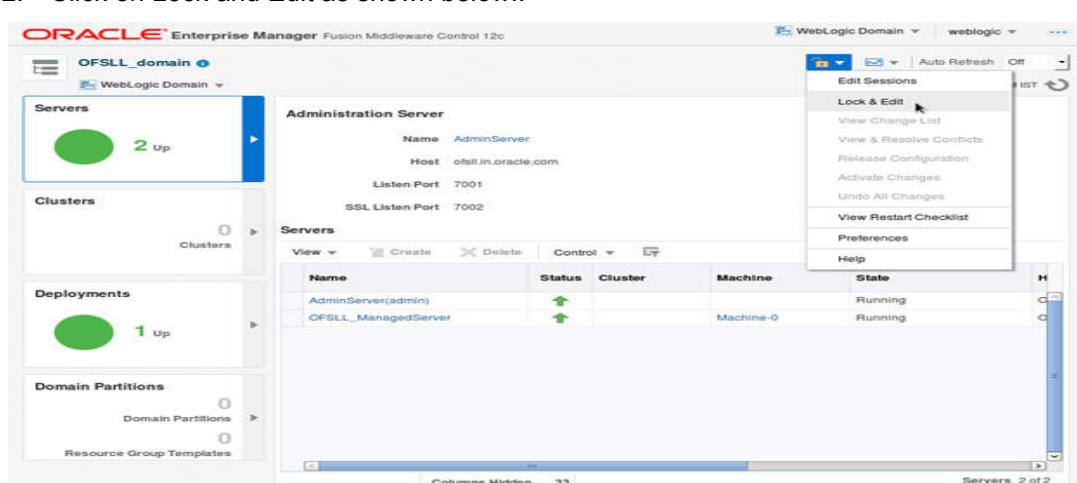
5. Deploying Application

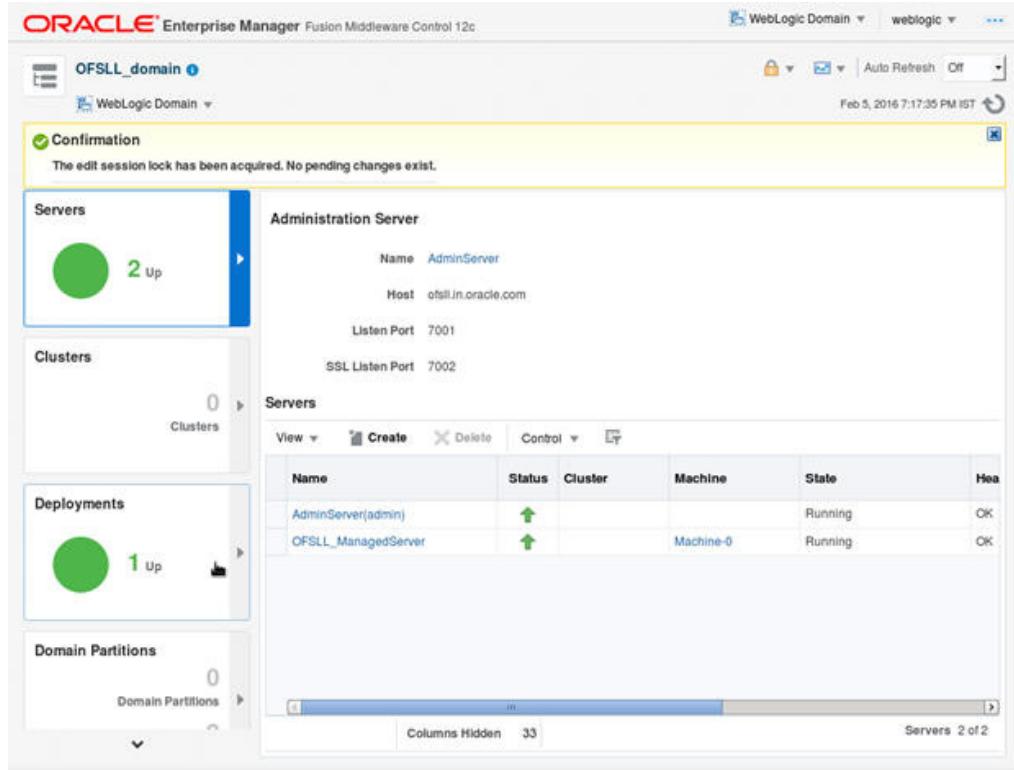
5.1 Deploying Application

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

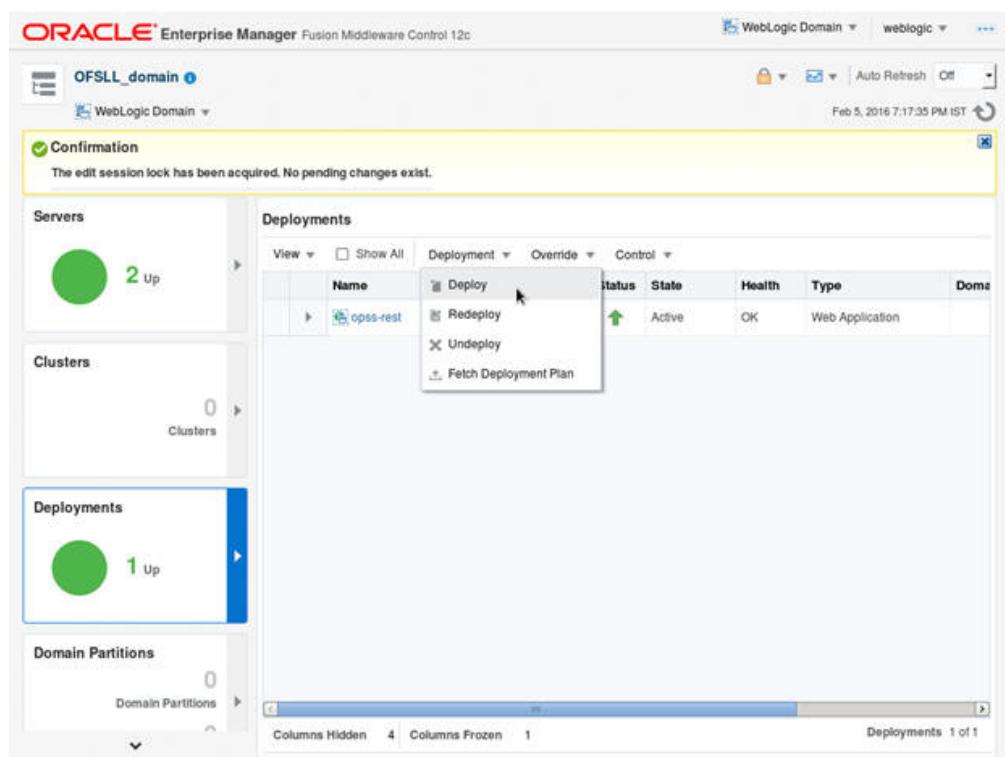


2. Click on Lock and Edit as shown below..

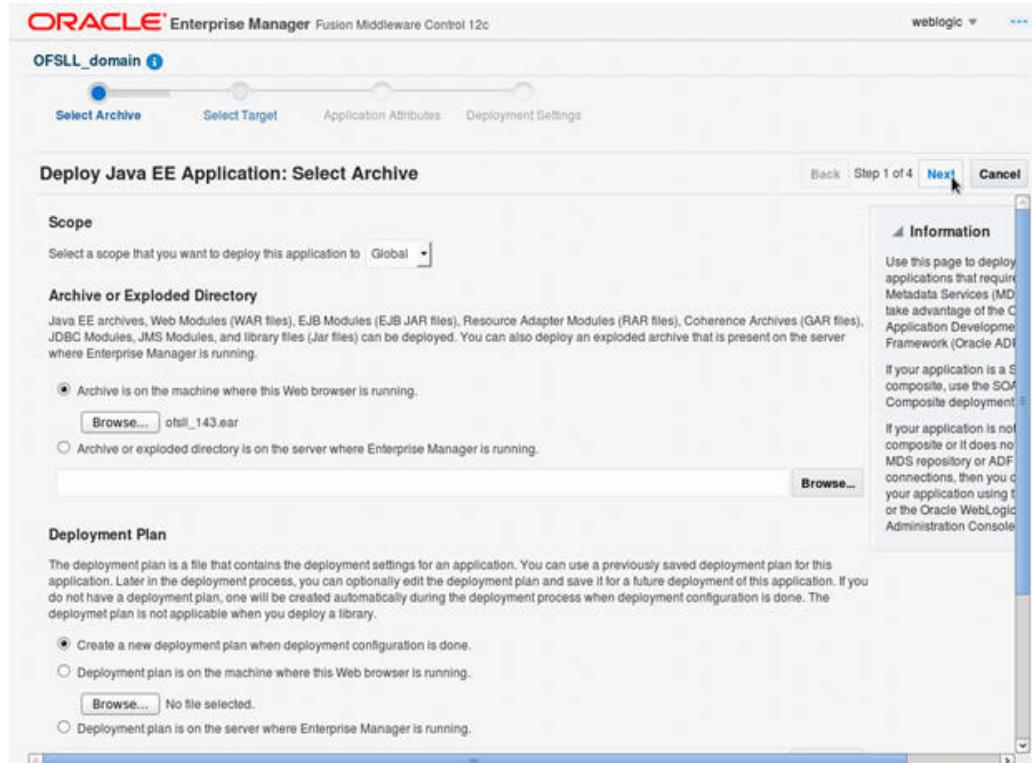




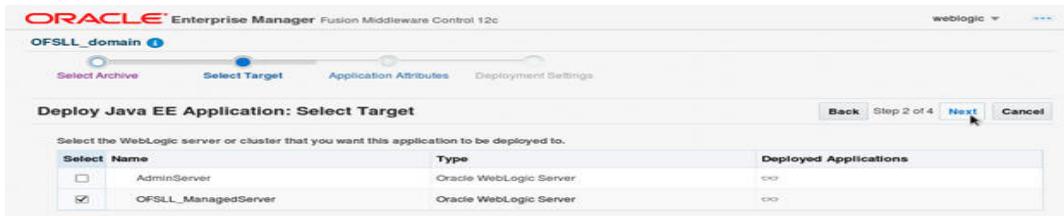
- Click on Deployments in the left panel. To deploy go to Deployments option in the menu as shown below.



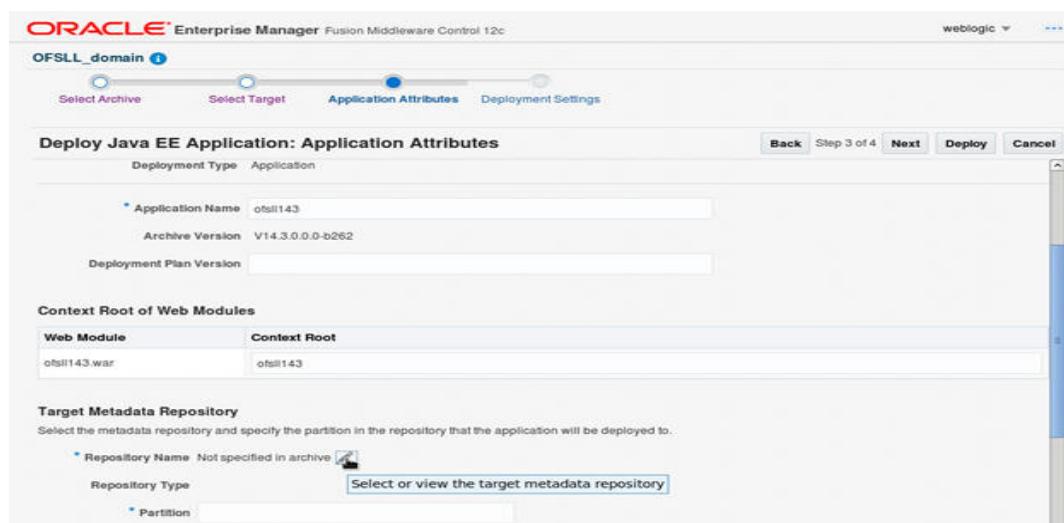
- Click Choose File button and select OFSLL application archive file i.e. ofssl_143.ear.



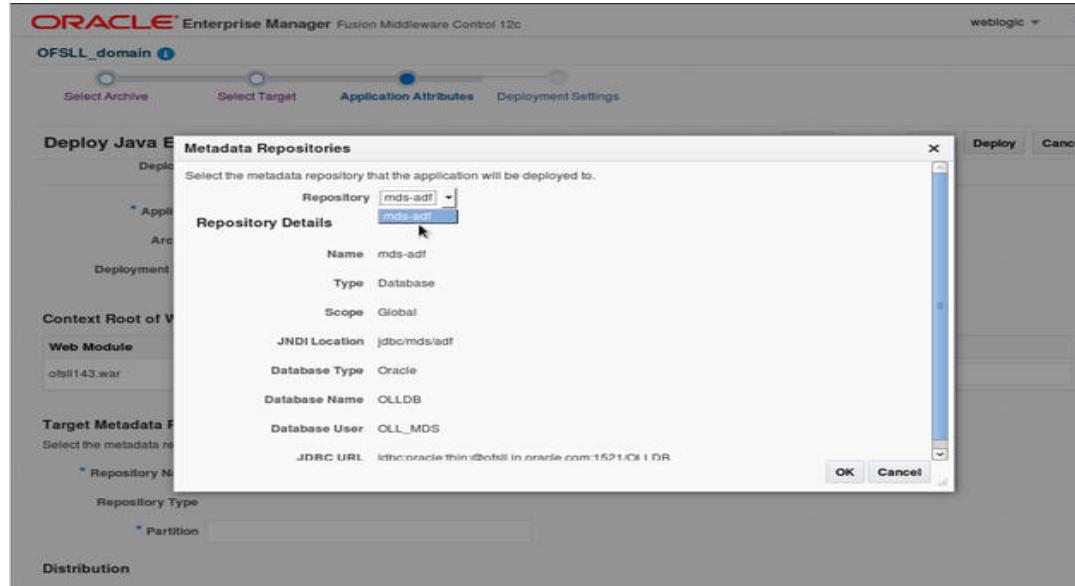
5. Click **Next**. The following window is displayed



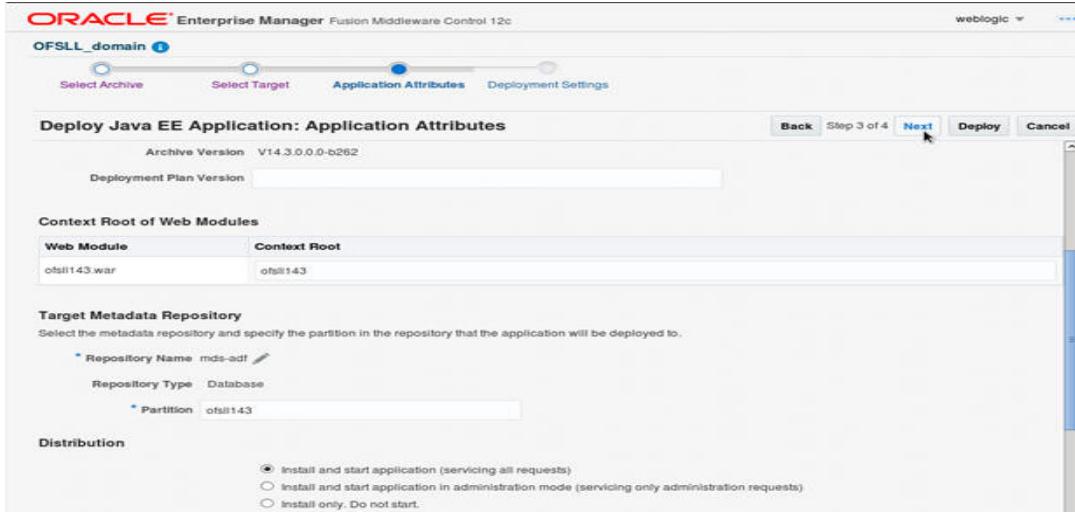
6. Check target server as per the requirement **OFSLL_ManagedServer** and click **Next**.
 7. The following window is displayed.



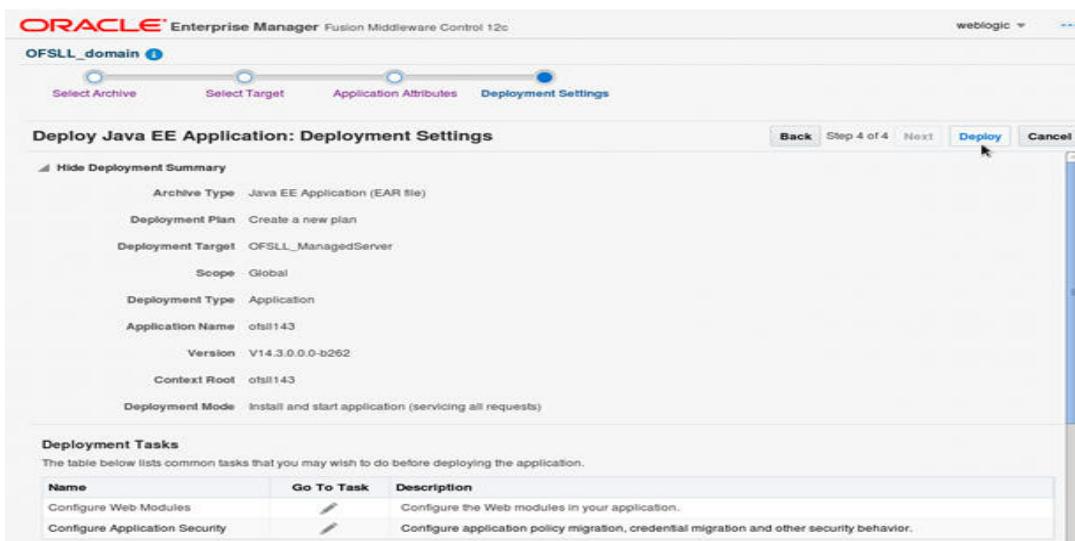
8. Click  button to select Repository Name. The following window is displayed.



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



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



11. Click **Deploy**. The following window is displayed



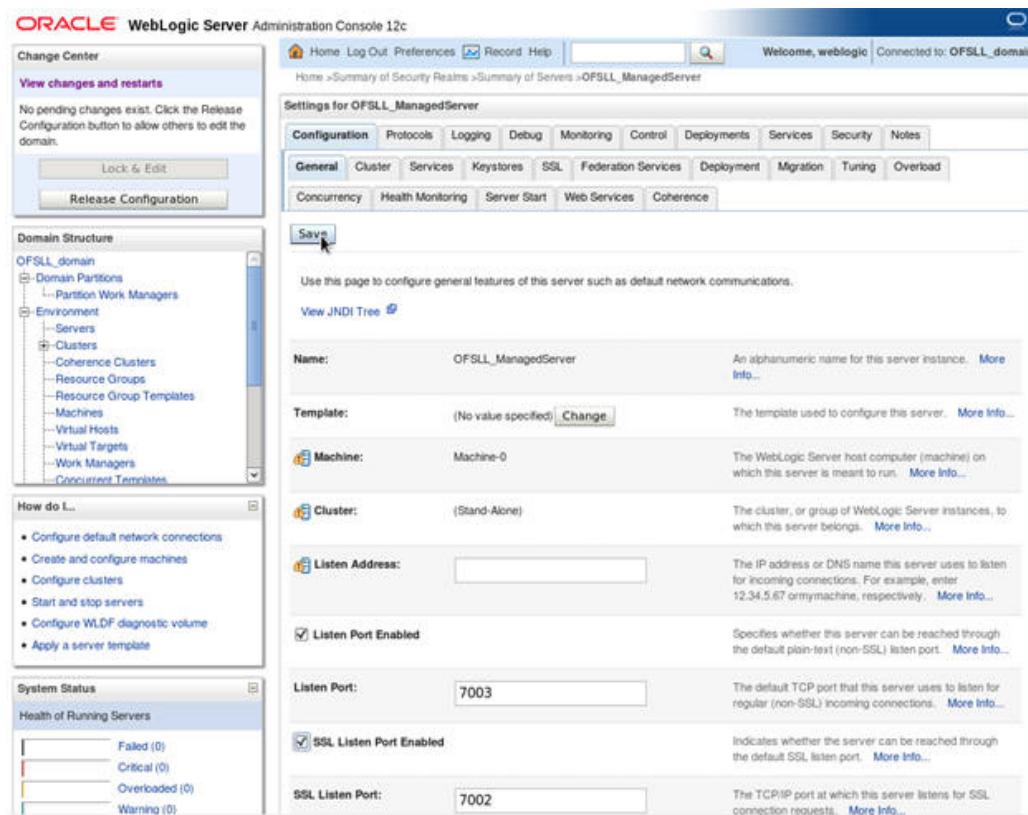
12. Click Close once the message “Deploy operation completed” is displayed.

6. Enabling SSL

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

To enable SSL:

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



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

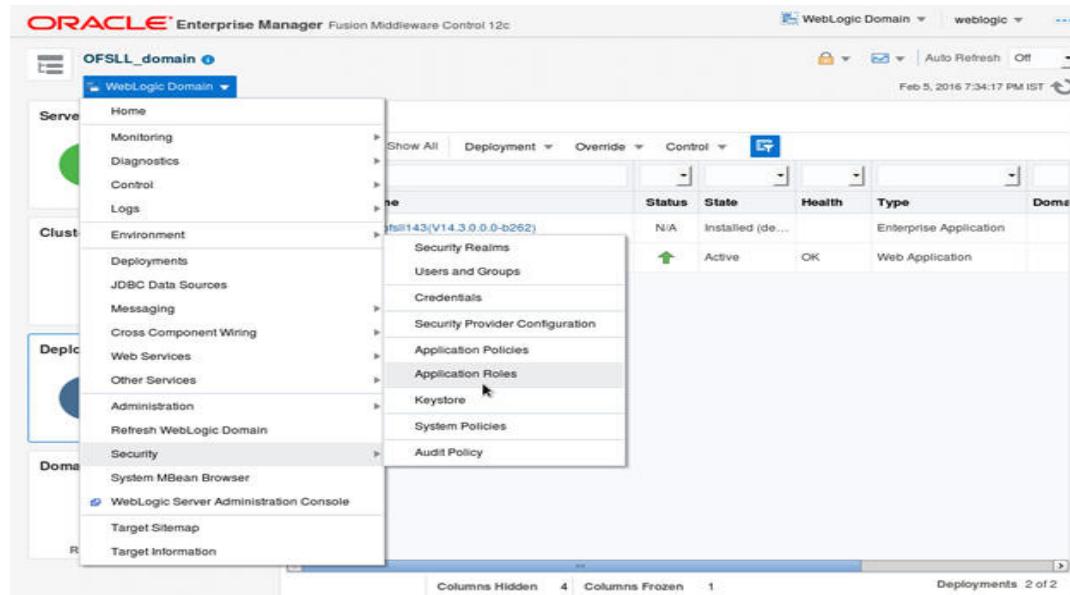
Note

It is recommended to disable http protocol.

7. Mapping Enterprise Group with Application Role

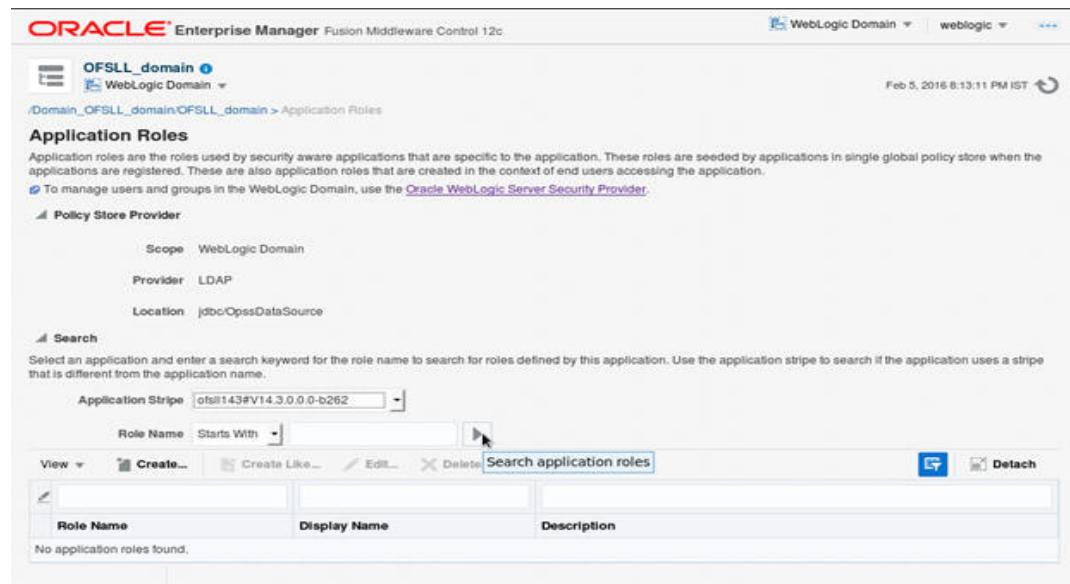
Follow the below steps to add an user to the group

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



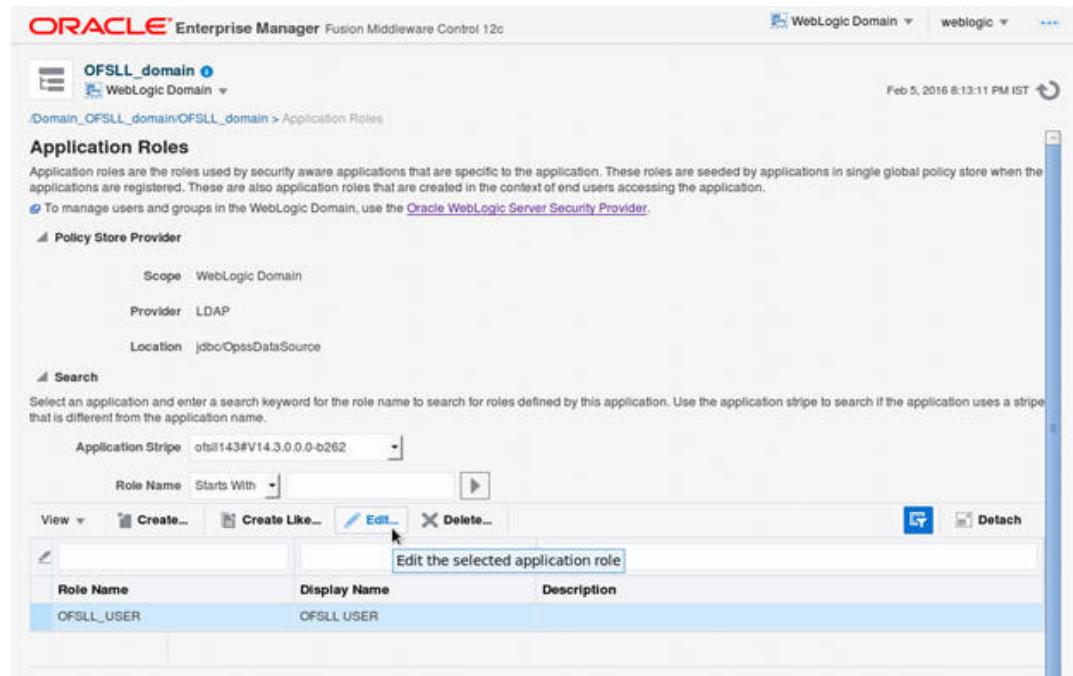
The screenshot shows the Oracle Enterprise Manager interface for a WebLogic Domain. The left sidebar shows the navigation path: OFSLL_domain > WebLogic Domain > Security > Application Roles. The right panel displays a table of application roles. One row is selected, showing 'ofssl143(V14.3.0.0.0-b262)' with status 'N/A', state 'Installed (de...', health 'OK', and type 'Enterprise Application'. Below the table are buttons for 'Active' and 'OK'.

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



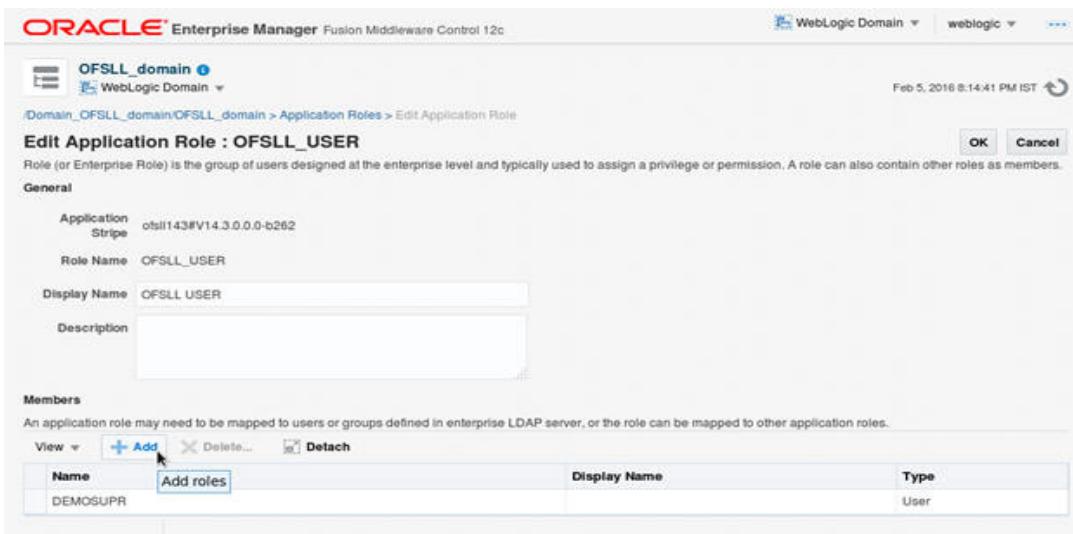
The screenshot shows the 'Application Roles' page within the Oracle Enterprise Manager interface. The left sidebar shows the navigation path: OFSLL_domain > WebLogic Domain > Application Roles. The main content area displays the 'Application Roles' section, which includes a description of what application roles are and how they are used. It shows a table with the message 'No application roles found.' Below this is a search section with fields for 'Application Stripe' (set to 'ofssl143#V14.3.0.0.0-b262'), 'Role Name' (set to 'Starts With'), and a search button. There are also buttons for 'Create...', 'Create Like...', 'Edit...', 'Delete', and 'Search application roles'.

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



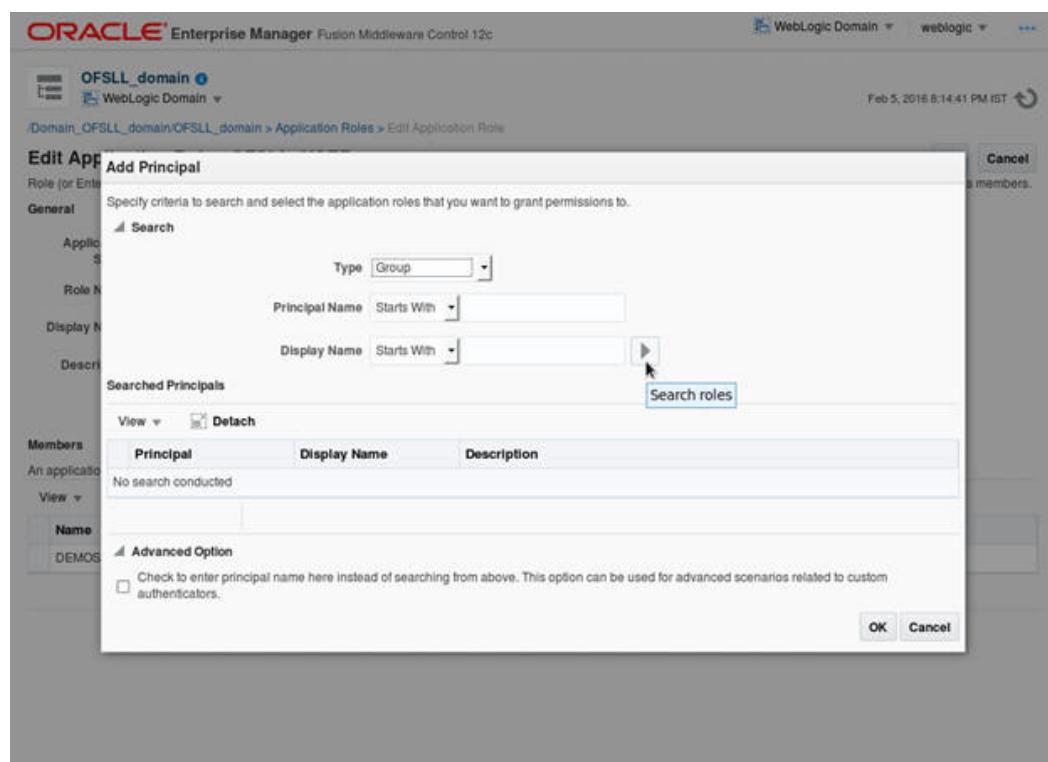
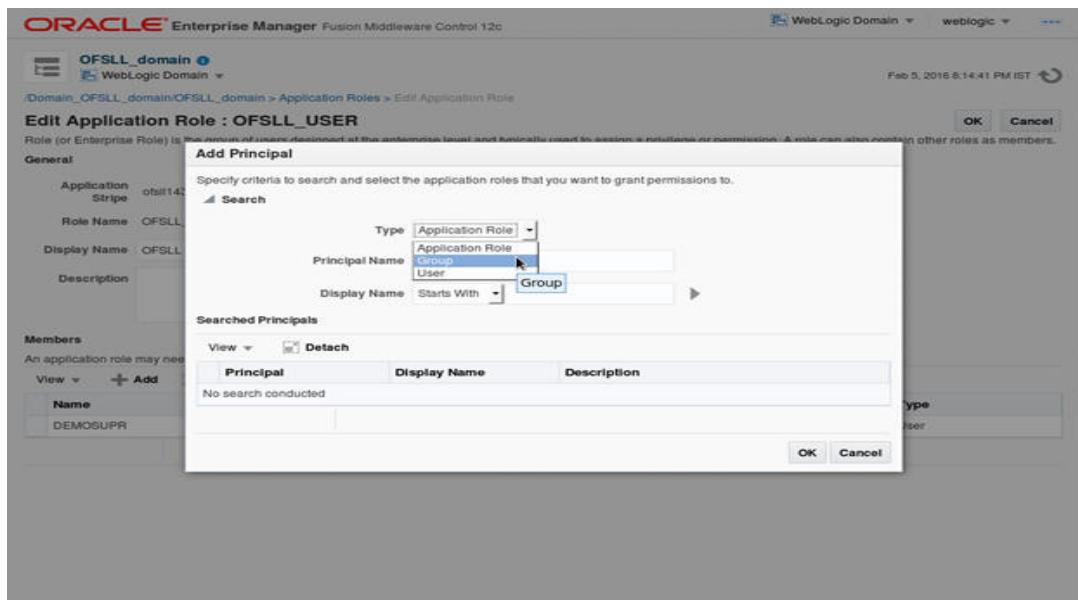
The screenshot shows the Oracle Enterprise Manager Fusion Middleware Control 12c interface. The top navigation bar shows 'WebLogic Domain' and 'weblogic'. The main title is 'ORACLE Enterprise Manager Fusion Middleware Control 12c'. The current page is 'Domain_OFSLL_domain/OFSLL_domain > Application Roles'. The 'Application Roles' section is displayed, showing a table with one row: 'Role Name' (OFSLL_USER), 'Display Name' (OFSLL USER), and 'Description' (empty). The 'Edit' button for this row is highlighted with a mouse cursor. The 'Scope' is set to 'WebLogic Domain', 'Provider' to 'LDAP', and 'Location' to 'jdbc/OpsxDataSource'. A 'Search' section is also visible.

6. Click **Edit**. The following window is displayed.

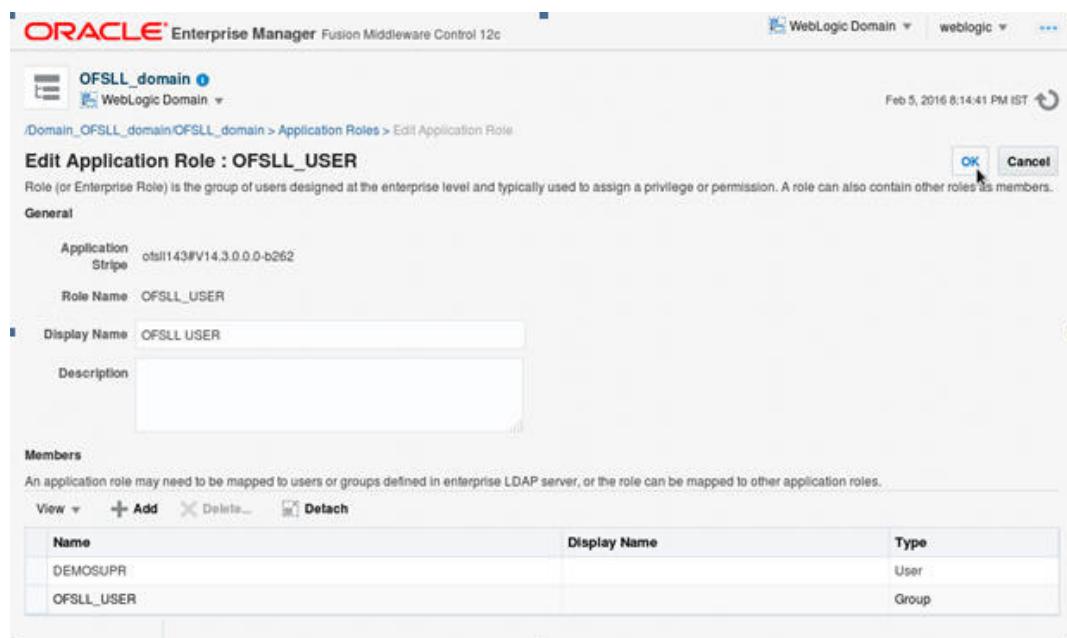
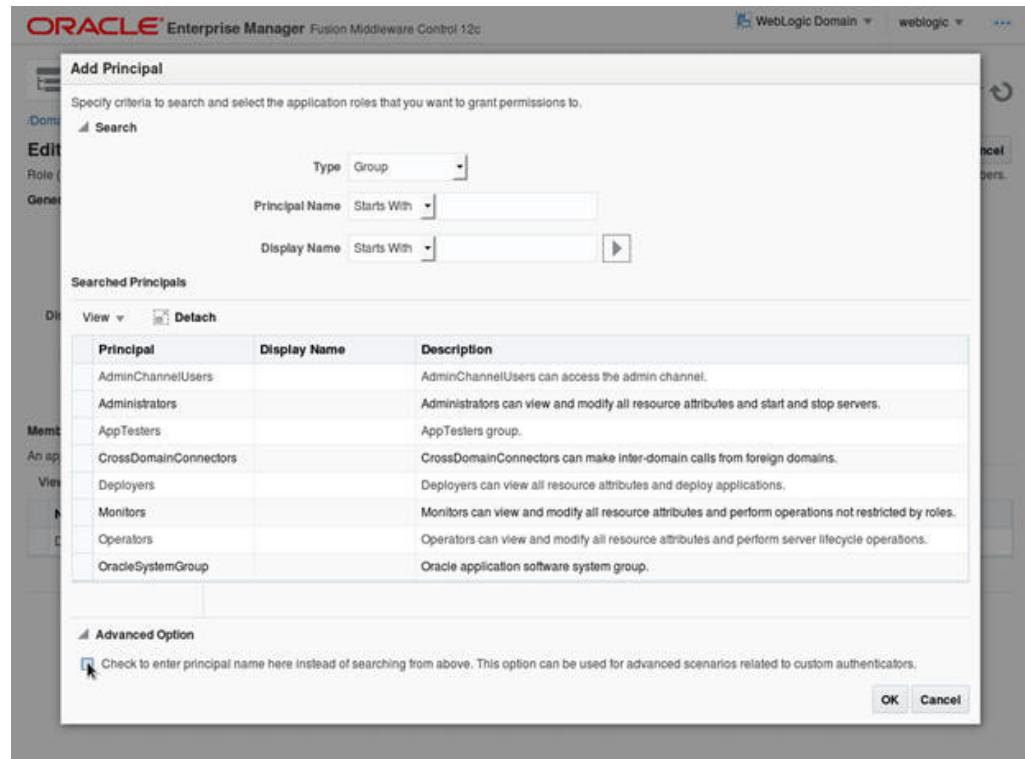


The screenshot shows the 'Edit Application Role : OFSLL_USER' dialog box. The 'General' tab is selected. The 'Role Name' is OFSLL_USER and the 'Display Name' is OFSLL USER. The 'Description' field is empty. The 'Members' section has a table with one row: 'Name' (DEMOUSPR) and 'Type' (User). The 'Add' button in the 'Members' section is highlighted with a mouse cursor. The 'OK' and 'Cancel' buttons are visible at the top right.

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



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



10. Click OK. The following window is displayed with the confirmation message as "The Application role of 'group_name' has been updated".

ORACLE Enterprise Manager Fusion Middleware Control 12c

WebLogic Domain weblogic ...

OFSSL_domain WebLogic Domain

Feb 5, 2016 8:20:15 PM IST

Information

An application role OFSSL_USER has been updated.

/Domain_OFSSL_domain/OFSSL_domain > Application Roles

Application Roles

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

To manage users and groups in the WebLogic Domain, use the [Oracle WebLogic Server Security Provider](#).

Policy Store Provider

Scope WebLogic Domain

Provider LDAP

Location jdbc/OpsxDataSource

Search

Select an application and enter a search keyword for the role name to search for roles defined by this application. Use the application stripe to search if the application uses a stripe that is different from the application name.

Application Stripe ofssl143#V14.3.0.0-b262

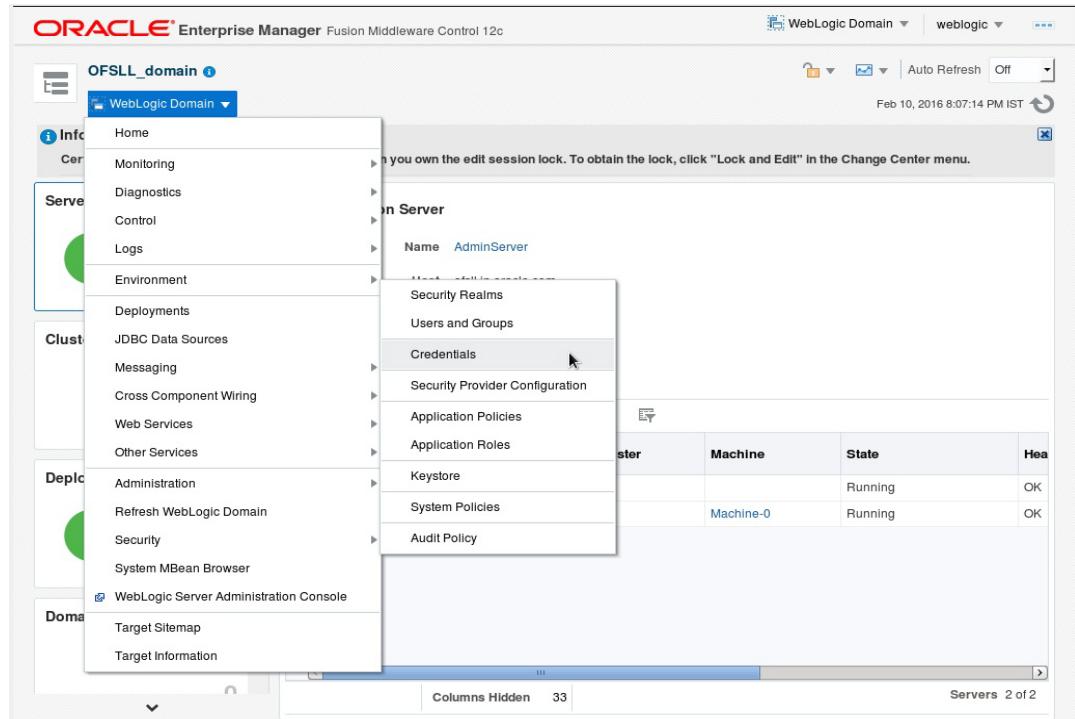
Role Name Starts With

View Create... Create Like... Edit... Delete...

Role Name	Display Name	Description
OFSSL_USER	OFSSL USER	

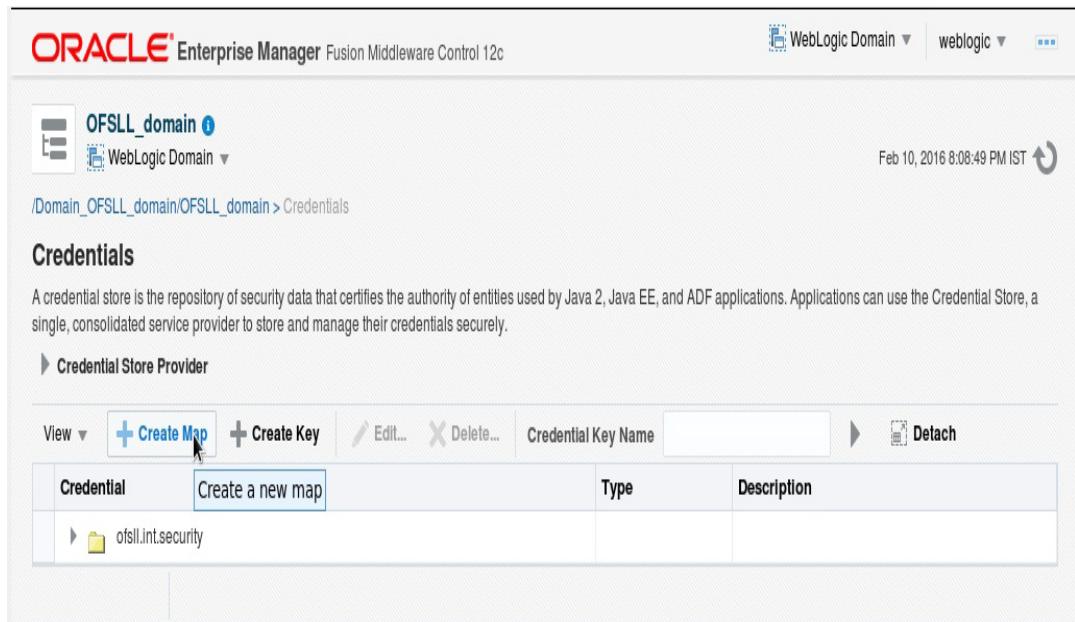
8. Configuring JNDI name for HTTP Listener

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



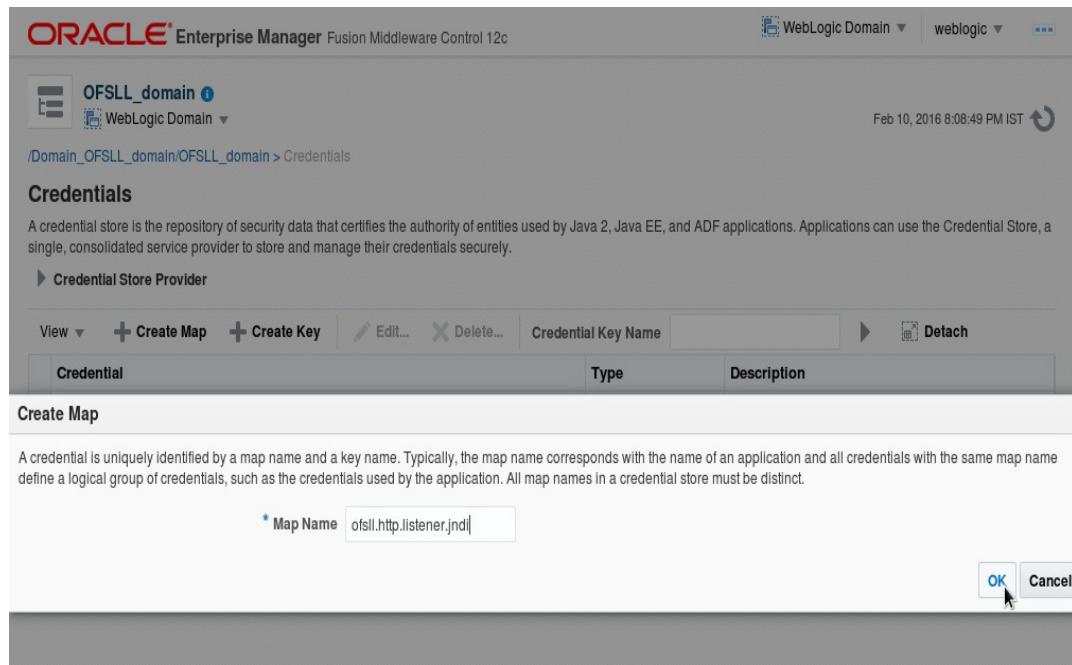
The screenshot shows the Oracle Enterprise Manager Fusion Middleware Control 12c interface. The left sidebar has sections for Infrastructure, Servers, Clusters, Deployments, and Domains. Under 'WebLogic Domain', there are sub-options: Home, Monitoring, Diagnostics, Control, Logs, Environment, Deployments, JDBC Data Sources, Messaging, Cross Component Wiring, Web Services, Other Services, Administration, Refresh WebLogic Domain, Security, System MBean Browser, and WebLogic Server Administration Console. A context menu is open over 'WebLogic Domain', with 'Credentials' highlighted. The main panel shows a table of servers with columns: Server, Machine, State, and Health. The table has two rows: one for 'Machine-0' which is 'Running' and 'OK', and another for 'Machine-1' which is also 'Running' and 'OK'. The status bar at the bottom indicates 'Servers 2 of 2'.

2. On clicking **Credentials** the following window is displayed.

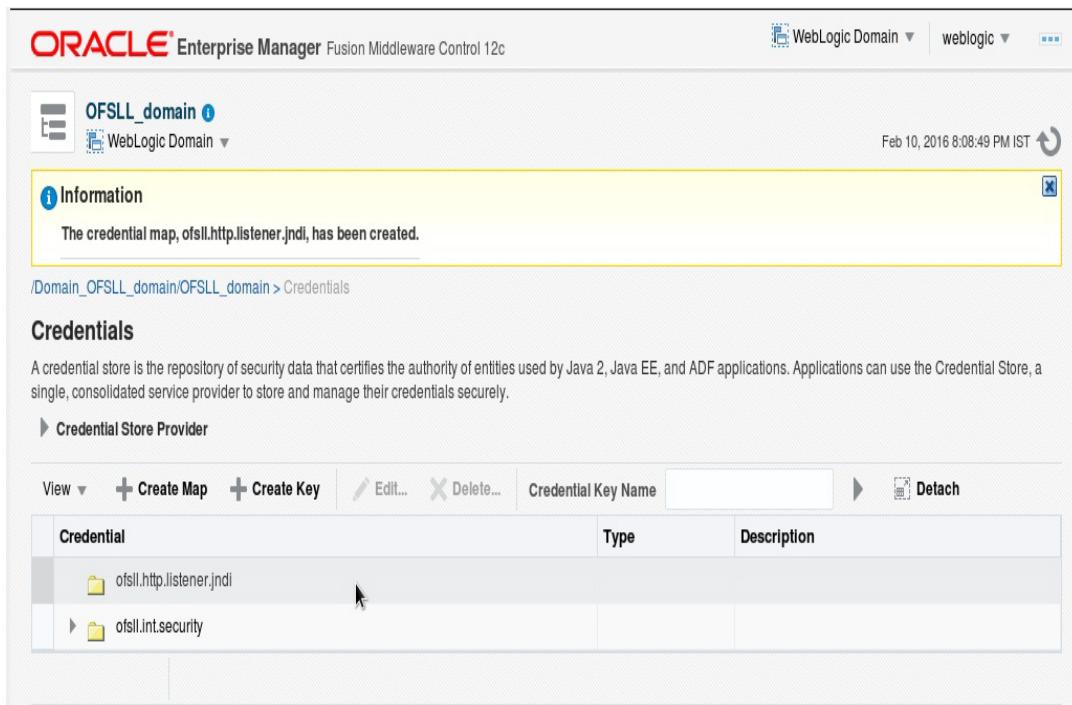


The screenshot shows the 'Credentials' page in Oracle Enterprise Manager. The top navigation bar includes 'WebLogic Domain' and 'weblogic'. The main content area shows the path '/Domain_OFSL_domain/OFSL_domain > Credentials'. The page title is 'Credentials'. A sub-section 'Credential Store Provider' is visible. At the top of the table are buttons: 'View', '+ Create Map' (which is highlighted in blue), '+ Create Key', 'Edit...', 'Delete...', 'Credential Key Name' (a search bar), and 'Detach'. The table has columns: 'Credential', 'Type', and 'Description'. There is one entry: 'Create a new map' with a sub-item 'ofsl.int.security'. The status bar at the bottom indicates 'Servers 2 of 2'.

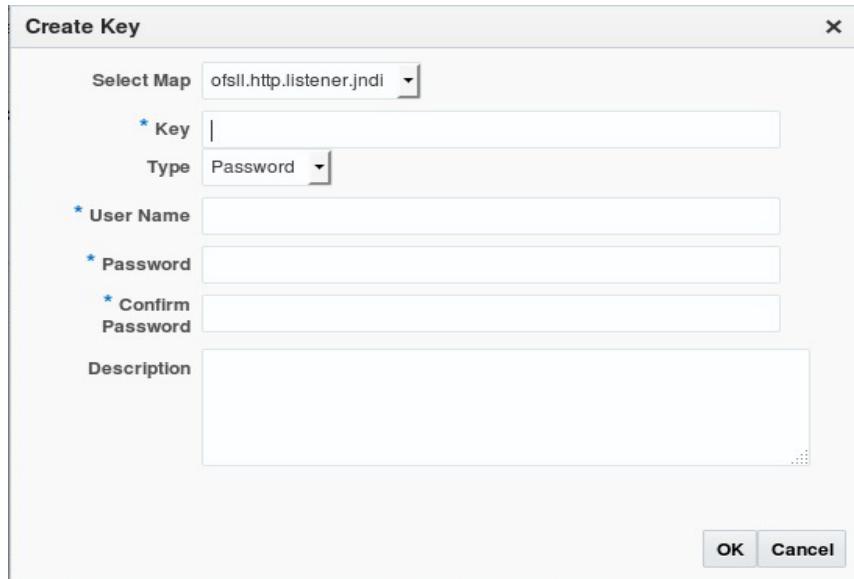
3. Click on **Create Map**. The following window is displayed.



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



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



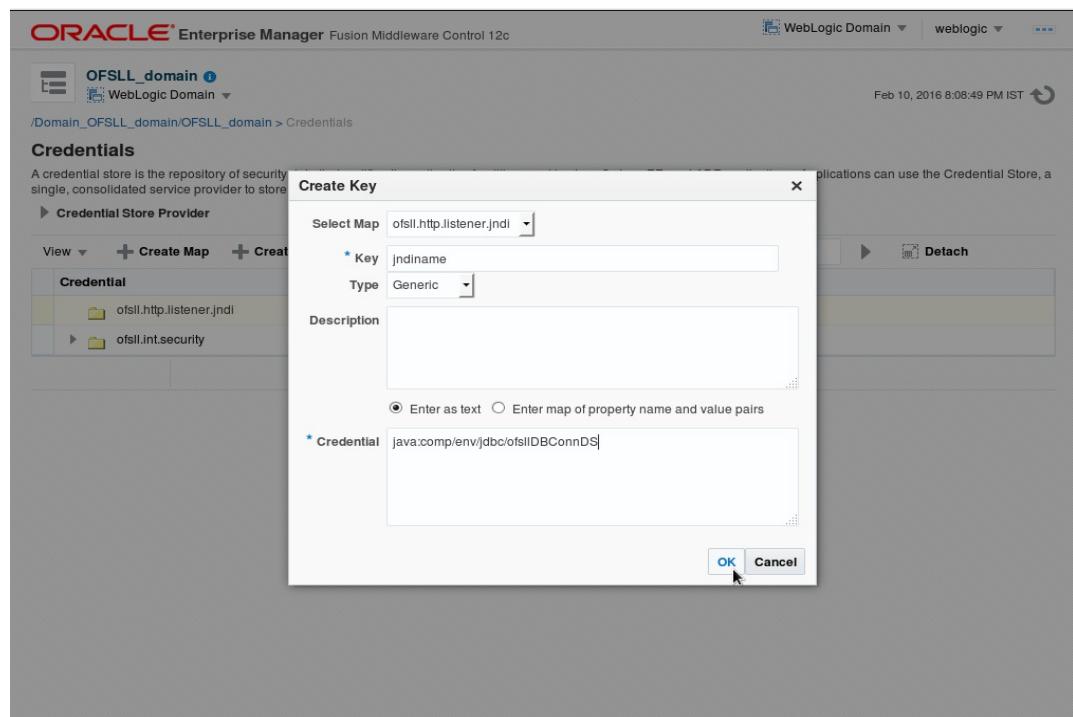
The dialog box is titled "Create Key". It has a dropdown menu "Select Map" set to "ofssl.http.listener.jndi". The "Key" field is empty. The "Type" dropdown is set to "Password". Below these are fields for "User Name", "Password", and "Confirm Password", all of which are empty. A "Description" text area is also empty. At the bottom are "OK" and "Cancel" buttons.

7. Enter the details as per your requirement.

Key: jndiname

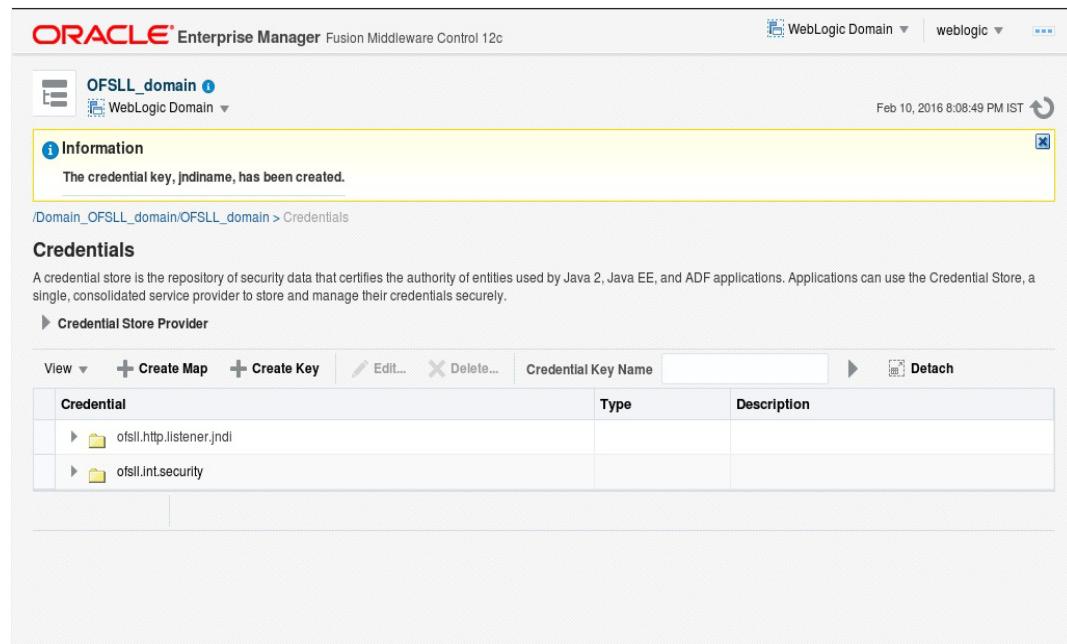
Credential: java:comp/env/jdbc/ofsslDBConnDS

Type:Generic



The screenshot shows the Oracle Enterprise Manager interface for a "WebLogic Domain" on "weblogic". The main window displays a "Credentials" list with items like "ofssl.http.listener.jndi" and "ofssl.int.security". A "Create Key" dialog box is overlaid on the screen. It has a "Select Map" dropdown set to "ofssl.http.listener.jndi". The "Key" field contains "jndiname", "Type" is set to "Generic", and the "Description" field is empty. Below the fields are two radio buttons: "Enter as text" (selected) and "Enter map of property name and value pairs". A "Credential" field contains the value "java:comp/env/jdbc/ofsslDBConnDS". At the bottom of the dialog are "OK" and "Cancel" buttons, with "OK" being highlighted.

8. Click **OK**. The following window is displayed.



The screenshot shows the Oracle Enterprise Manager Fusion Middleware Control 12c interface. The title bar reads 'ORACLE Enterprise Manager Fusion Middleware Control 12c'. The top navigation bar includes 'WebLogic Domain' and 'weblogic'. The date 'Feb 10, 2016 8:08:49 PM IST' and a refresh icon are also present. The main content area is titled 'Information' with the message 'The credential key, jndiname, has been created.' Below this, the 'Credentials' section is shown with the following table:

Credential	Type	Description
ofssl.http.listener.jndi		
ofssl.int.security		

9. Configuring Oracle BI Publisher for Application

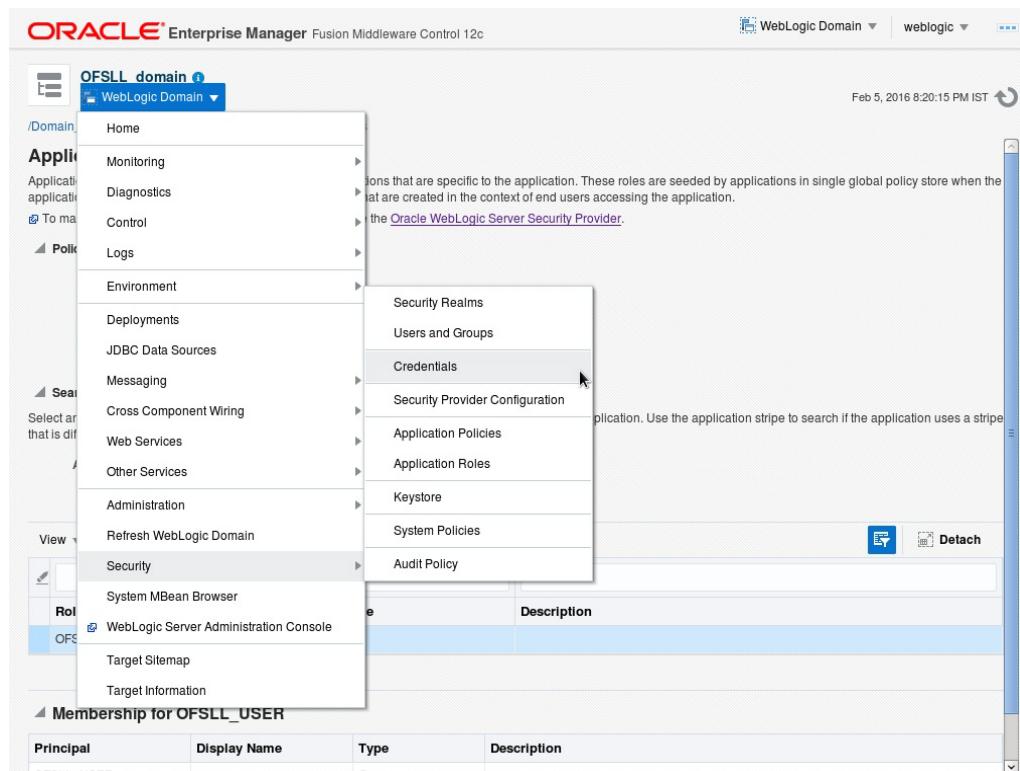
1. Copy the OfsllCommonCSF.jar from /WEB-INF/lib available in the staging area to \$DOMAIN_HOME/lib
2. Update the setDomainEnv.sh file (\$MW_HOME/user_projects/domains/mydomain/bin directory) by appending the above jar file path –

**EXTRA_JAVA_PROPERTIES="..... \${EXTRA_JAVA_PROPERTIES}
-Dofsll.csf.path=\${DOMAIN_HOME}"**

3. Configure Security via EMconsole

Note

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



The screenshot shows the Oracle Enterprise Manager Fusion Middleware Control 12c interface. The left sidebar shows the navigation tree with 'OFSLL domain' selected. The main content area is titled 'Security' and shows a sub-menu for 'Security Realms'. The 'Credentials' option is highlighted with a cursor. Below the menu, there is a table titled 'Membership for OFSLL_USER' with one row: 'OFSLL_USER'. The top right corner shows the date and time: 'Feb 5, 2016 8:20:15 PM IST'.

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

The screenshot shows the Oracle Enterprise Manager interface. The top navigation bar includes 'WebLogic Domain' and 'weblogic'. The main content area is titled 'Credentials' and contains a sub-section 'Credential Store Provider'. A toolbar at the top of the list table has a 'Create Map' button highlighted with a mouse cursor. The table below shows a single row with a 'Create a new map' button.

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

This screenshot shows a modal dialog box titled 'Create Map'. It contains a single input field labeled 'Map Name' with the value 'ofssl.int.security'. Below the input field are 'OK' and 'Cancel' buttons, with the 'OK' button being the target of a mouse cursor.

6. Click OK.

The screenshot shows the Oracle Enterprise Manager interface again. A yellow notification bar at the top displays the message: 'The credential map, ofssl.int.security, has been created.' Below this, the 'Credentials' page is visible, showing the newly created map 'ofssl.int.security' in the list.

7. Click **Create Key** Button.
8. Enter the details as per your requirement.

9. And provide User Name and Password of BI Publisher console.

Create Key

Select Map	ofssl.int.security
* Key	bip_key
Type	Password
* User Name	weblogic
* Password	*****
* Confirm Password	*****
Description	
OK Cancel	

10. Click **OK**. The following window is displayed.

ORACLE® Enterprise Manager Fusion Middleware Control 12c

OFSSL_domain WebLogic Domain Feb 10, 2016 11:20:55 AM IST

Information
The credential key, bip_key, has been created.

/Domain_OFSSL_domain/OFSSL_domain > Credentials

Credentials
A credential store is the repository of security data that certifies the authority of entities used by Java 2, Java EE, and ADF applications. Applications can use the Credential Store, a single, consolidated service provider to store and manage their credentials securely.

► Credential Store Provider

View **Create Map** **Create Key** Edit... Delete... Credential Key Name Detach

Credential	Type	Description
ofssl.int.security		

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

The screenshot shows the Oracle Enterprise Manager interface. The left sidebar has a tree structure with nodes like 'Info', 'Certificates', 'Server', 'Clusters', 'Deployments', 'Domain', and 'Domain'. The 'Domain' node is expanded, showing 'OFSLL_domain'. Under 'OFSLL_domain', the 'WebLogic Domain' node is selected and expanded, showing sub-options: Home, Monitoring, Diagnostics, Control, Logs, Environment, Deployments, JDBC Data Sources, Messaging, Cross Component Wiring, Web Services, Other Services, Administration, Refresh WebLogic Domain, Security, System MBean Browser, and WebLogic Server Administration Console. A context menu is open over the 'WebLogic Domain' node, with 'System Policies' highlighted. To the right, a table shows server status: AdminServer (Machine-0) is running, and Audit Policy is listed. The top right shows the date and time: Feb 10, 2016 11:30:43 AM IST.

12. Click Create.

The screenshot shows the 'System Policies' page. The left sidebar shows 'OFSLL_domain' selected. The main area has a heading 'System Policies' with a sub-instruction: 'System policies are the system-wide policies applied to all applications deployed to current management domain. You can grant special permissions and privileges to principal or codebase.' Below this are sections for 'Policy Store Provider' and 'Search'. A search bar is present with 'Type: Codebase' and 'Name: Starts With:'. Below the search bar is a button labeled 'Create...' with a tooltip 'Create...'. The main content area shows a table with one row: 'No security policies found.' The top right shows the date and time: Feb 10, 2016 12:02:47 PM IST.

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

The screenshot shows the 'Create System Grant' dialog. The top bar shows 'OFSLL_domain' and 'System Policies'. The main area has a heading 'Create System Grant' with a sub-instruction: 'Create two different types of system policies supported by application server: principal policy and codebase policy. Principal policy grants permissions and privileges to a list of users or roles. Codebase policy grants permissions and privileges to a codebase, which is mostly URL or location of jar file in file system. Codebase can be either absolute path or relative path.' Below this are sections for 'Grant To' (Codebase) and 'Codebase' (file:\${ofsll.csf.path}/lib/OfsllCommonCSF.jar). A 'Permissions' section has a 'Add' button. The bottom right has 'OK' and 'Cancel' buttons. The top right shows the date and time: Feb 10, 2016 7:45:05 PM IST.

14. The following window is displayed. Select the checkbox 'Select here to enter details for a new permission' and enter the following details as the first permission class.

- Permission Class: oracle.security.jps.service.credstore.CredentialAccessPermission
- Resource Name: context=SYSTEM,mapName=ofsll.int.security,keyName=*

- Permission Actions: read

Configuring JNDI Name for http Listener

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

3. Click OK. The following window is displayed.

10. Launching Application

Verifying Successful Application Deployment and Launching Application

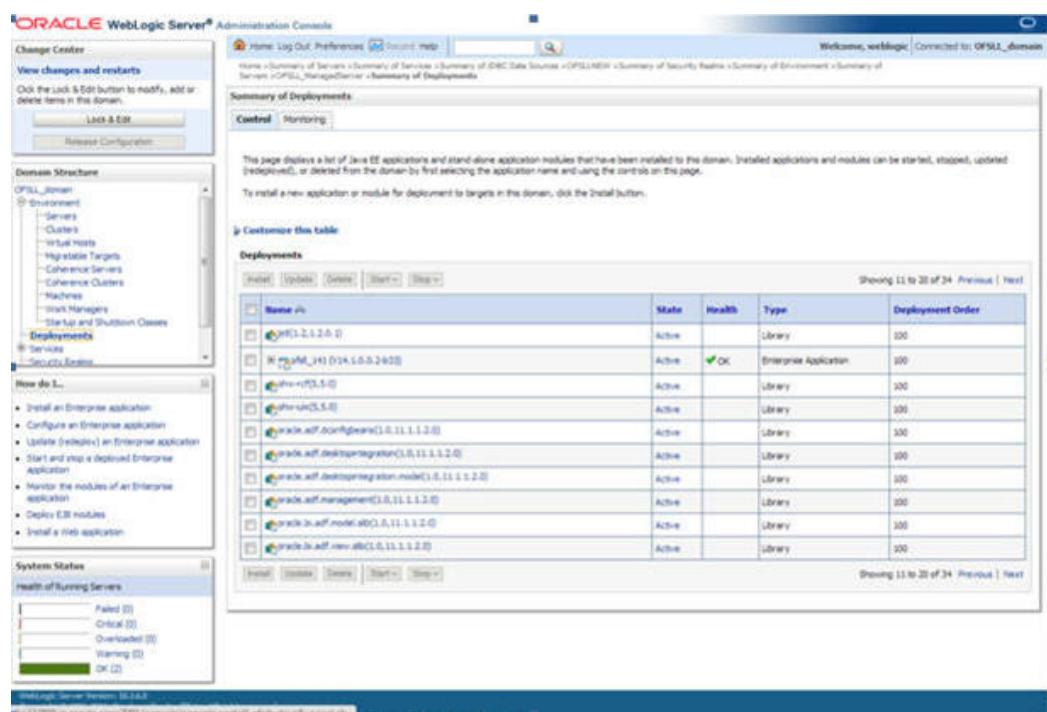
Successful Application deployment can be verified by following:

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

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

To launch application

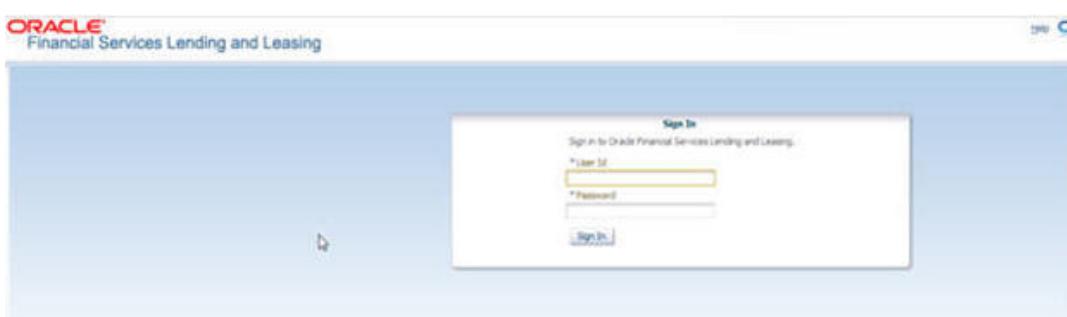
1. Verify if the deployed OFSLL application is **Active**.



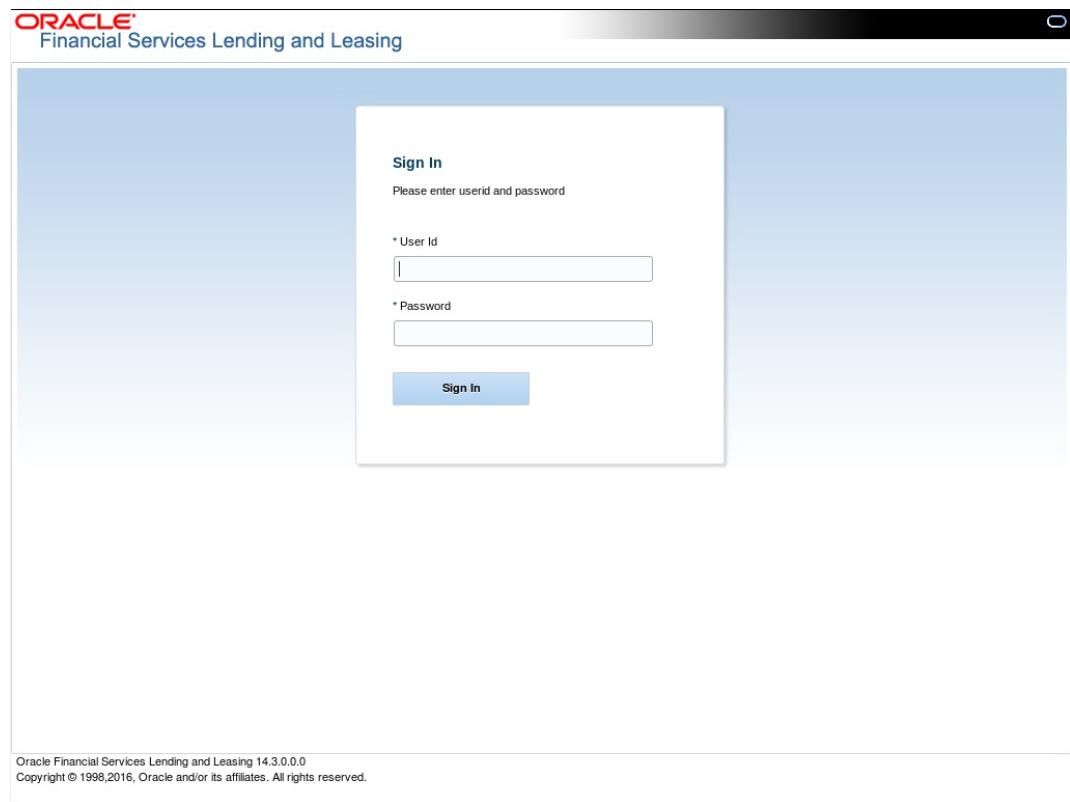
Name	State	Health	Type	Deployment Order
ofsl1-2.1.2.5-1	Active		Library	100
ofsl1-14 (v14.1.0.2.493)	Active	OK	Enterprise Application	100
ofsl1-v17(3.3-1)	Active		Library	100
ofsl1-v18(3.5-1)	Active		Library	100
oracle.adf.configuration(1.0.11.1.1.2.0)	Active		Library	100
oracle.adf.desktopIntegration(1.0.11.1.1.2.0)	Active		Library	100
oracle.adf.desktopIntegration.module(1.0.11.1.1.2.0)	Active		Library	100
oracle.adf.management(1.0.11.1.1.2.0)	Active		Library	100
oracle.adf.model(1.0.11.1.1.2.0)	Active		Library	100
oracle.adf.view(1.0.11.1.1.2.0)	Active		Library	100

2. The URL of the OFSLL application will be

<https://<hostname>:<Port>/<ContextName>/faces/pages/OfsllSignIn.jsf>
(Example: <https://localhost:7003/ofsl143/faces/pages/OfsllSignIn.jsf>)

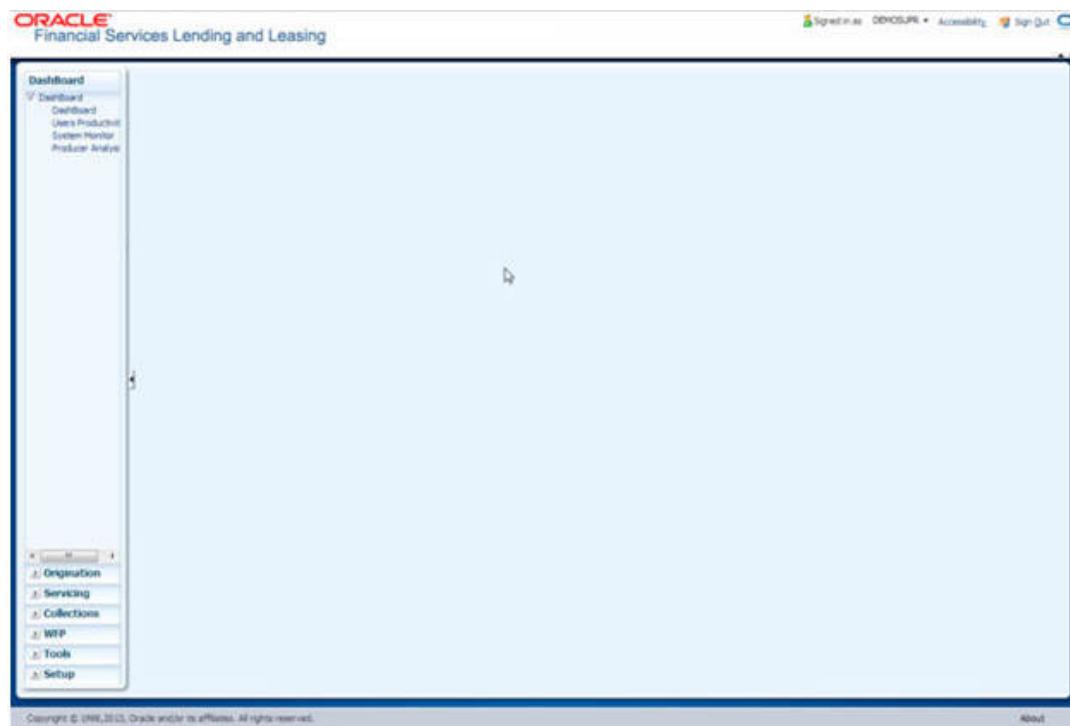


3. Login with the user credentials that was created in Users Creation.



The image shows the 'Sign In' page of the Oracle Financial Services Lending and Leasing application. The page has a light blue header with the 'ORACLE' logo and the text 'Financial Services Lending and Leasing'. Below the header is a large white 'Sign In' form. The form contains the following fields: 'User Id' (a text input field with a placeholder 'User Id'), 'Password' (a text input field with a placeholder 'Password'), and a 'Sign In' button. Below the form, a small note reads: 'Oracle Financial Services Lending and Leasing 14.3.0.0.0 Copyright © 1998,2016, Oracle and/or its affiliates. All rights reserved.'

4. After successful login, the following screen is displayed



The image shows the 'Dashboard' page of the Oracle Financial Services Lending and Leasing application. The page has a light blue header with the 'ORACLE' logo and the text 'Financial Services Lending and Leasing'. The top right corner shows 'Signed in as DEMOUSER' and 'Sign Out'. The left side features a vertical navigation menu with the following items: 'Dashboard' (selected), 'Dashboard', 'Ongoing', 'Servicing', 'Collections', 'WIP', 'Tools', and 'Setup'. The main content area is currently empty, showing a large white space with a cursor icon. At the bottom of the page, a footer bar contains the text 'Copyright © 1998,2016, Oracle and/or its affiliates. All rights reserved.' and a 'Help' link.

11. Installing Upgrade

There is an infrastructure upgrade required (from 11g fusion middleware to 12c fusion middleware) when upgrading from OFSLL 14.2.0.0.0 to OFSLL 14.3.0.0.0.

Hence, it is recommended to install a new 12c fusion middleware infrastructure and deploy the 14.3.0.0.0 OFSLL application.