

Weblogic Configuration
Oracle FLEXCUBE Universal Banking
Release 14.4.0.0.0
[May] [2020]



Table of Contents

1. CONFIGURING SSL ON ORACLE WEBLOGIC	1-1
1.1 INTRODUCTION	1-1
1.2 SETTING UP SSL ON ORACLE WEBLOGIC	1-1
1.3 CERTIFICATES AND KEYPAIRS	1-1
2. CHOOSING THE IDENTITY AND TRUST STORES.....	2-1
2.1 INTRODUCTION.....	2-1
3. OBTAINING THE IDENTITY STORE	3-1
3.1 CREATING IDENTITY STORE WITH SELF-SIGNED CERTIFICATES	3-1
3.1.1 <i>Creation of Self-signed Certificate</i>	<i>3-1</i>
3.2 CREATING IDENTITY STORE WITH TRUSTED CERTIFICATES ISSUED BY CA.....	3-3
3.2.1 <i>Creation of Public and Private Key Pair.....</i>	<i>3-3</i>
3.2.2 <i>Generating CSR.....</i>	<i>3-5</i>
3.2.3 <i>Obtaining Trusted Certificate from CA</i>	<i>3-5</i>
3.2.4 <i>Importing Certificate into Identity Store.....</i>	<i>3-5</i>
4. CONFIGURING IDENTITY AND TRUST STORES FOR WEBLOGIC	4-1
4.1 ENABLING SSL ON ORACLE WEBLOGIC SERVER.....	4-1
4.2 CONFIGURING IDENTITY AND TRUST STORES.....	4-1
5. SETTING SSL ATTRIBUTES FOR MANAGED SERVERS	5-1
5.1 SETTING SSL ATTRIBUTES FOR PRIVATE KEY ALIAS AND PASSWORD.....	5-1
6. TESTING CONFIGURATION.....	6-1
6.1 TESTING CONFIGURATION	6-1
7. CREATING RESOURCES ON WEBLOGIC	7-1
7.1 INTRODUCTION	7-1
7.2 RESOURCE ADMINISTRATION	7-1
7.2.1 <i>Creating Data Source</i>	<i>7-1</i>
7.2.2 <i>JMS Server Creation.....</i>	<i>7-23</i>
7.2.3 <i>JMS Modules Creation</i>	<i>7-29</i>
7.2.4 <i>Subdeployment Creation.....</i>	<i>7-34</i>
7.2.5 <i>JMS Queue Creation.....</i>	<i>7-38</i>
7.2.6 <i>JMS Connection Factory Creation</i>	<i>7-44</i>
7.3 CONFIGURING WEBLOGIC FOR PMGATEWAY	7-53
7.4 CONFIGURING WEBLOGIC FOR ORACLE FLEXCUBE	7-53
7.5 SETUP/CONFIGURE MAIL SESSION IN WEBLOGIC	7-58
7.5.1 <i>Creating JavaMail Session</i>	<i>7-58</i>
7.5.2 <i>Configuration of the TLS/SSL Trust Store for Weblogic Server</i>	<i>7-63</i>

1. Configuring SSL on Oracle Weblogic

1.1 Introduction

This chapter details out the configurations for SSL on Oracle Weblogic application server.

1.2 Setting up SSL on Oracle Weblogic

To setup SSL on Oracle Weblogic application server, you need to perform the following tasks:

1. Obtain an identity (private key and digital certificates) and trust (certificates of trusted certificate authorities) for Oracle Weblogic application server.
2. Store the identity and trust. Private keys and trust CA certificates are stored in keystores.
3. Configure the identity and trust the keystores for Oracle Weblogic application server in the administration console.
4. Set SSL attributes for the private key alias and password in Oracle Weblogic administration console.

1.3 Certificates and Keypairs

Certificates are used for validating the authenticity of the server. Certificates contains the name of the owner, certificate usage, duration of validity, resource location or distinguished name (DN), which includes the common name (CN - web site address or e-mail address depending of the usage) and the certificate ID of the person who certified (signs) these information. It also contains the public key and a hash to ensure that the certificate has not been tampered with. A certificate is insecure until it is signed. Signed certificates cannot be modified.

A certificate can be self signed or obtained from a reputable certificate authority such as Verisign, Inc., Entrust.net, Thawte, GeoTrust or InstantSSL.

SSL uses a pair of cryptographic keys - a **public key** and a **private key**. These keys are similar in nature and can be used alternatively. What one key encrypts can be decrypted by the other key of the pair. The private key is kept secret, while the public key is distributed using the certificate.

A **keytool** stores the keys and certificates in a **keystore**. The default keystore implementation implements it as a file. It protects private keys with a password. The different entities (key pairs and the certificates) are distinguished by a unique 'alias'. Through its keystore, Oracle Weblogic server can authenticate itself to other parties.

In Java, a keystore is a 'java.security.KeyStore' instance that you can create and manipulate using the **keytool** utility provided with the Java Runtime.

There are two keystores to be managed by Oracle Weblogic server to configure SSL.

- o Identity Keystore: Contains the key pairs and the Digital certificate. This can also contain certificates of intermediate CAs.
- o Trust Keystore: Contains the trusted CA certificates.

2. Choosing the Identity and Trust Stores

2.1 Introduction

Oracle Financial Services Software recommends that the choice of Identity and Trust stores be made up front. Oracle Weblogic server supports the following combinations of Identity and Trust stores:

- Custom Identity and Command Line Trust
- Custom Identity and Custom Trust
- Custom Identity and Java Standard Trust
- Demo Identity and Demo Trust

Oracle Financial Services does not recommend choosing Demo Identity and Demo Trust for production environments.

It is recommended to separate the identity and trust stores, since each Weblogic server tends to have its own identity, but might have the same set of trust CA certificates. Trust stores are usually copied across Oracle Weblogic servers, to standardize trust rules; it is acceptable to copy trust stores since they contain public keys and certificates of CAs. Unlike trust stores, identity stores contain private keys of the Oracle Weblogic server, and hence should be protected against unauthorized access.

Command Line Trust, if chosen requires the trust store to be specified as a command line argument in the Weblogic Server startup script. No additional configuration of the trust store is required in the Weblogic Server Administration Console.

Java Standard Trust would rely on the cacerts files provided by the Java Runtime. This file contains the list of trust CA certificates that ship with the Java Runtime, and is located in the 'JAVA_HOME/jre/lib/security' directory. It is highly recommended to change the default Java standard trust store password from 'changeit' (without quotes), and the default access permission of the file. Certificates of most commercial CAs are already present in the Java Standard Trust store. Therefore, it is recommended to use the Java Standard Trust store whenever possible. The rest of the document will assume the use of Java Standard Trust, since most CA certificates are already present in it.

One can also create custom trust stores containing the list of certificates of trusted CAs.

For further details on identity and trust stores, please refer the Oracle Weblogic Server documentation on Securing Oracle Weblogic Server.

3. Obtaining the Identity Store

3.1 Creating Identity Store with Self-Signed Certificates

Self-signed certificates are acceptable for use in a testing or development environment. Oracle Financial Services does not recommend the use of self-signed certificates in a production environment.

In order to create a self-signed certificate, the genkeypair option provided by the keytool utility of Sun Java 6 needs to be utilized.

3.1.1 Creation of Self-signed Certificate

Browse to the bin folder of JRE from the command prompt and type the following command.



The items highlighted in blue are placeholders, and should be replaced with suitable values when running the command.

```
keytool -genkeypair -alias alias -keyalg RSA -keysize 1024 -sigalg  
SHA1withRSA -validity 365 -keystore keystore
```

In the above command,

1. **alias** is used to identify the public and private key pair created. This alias is required later when configuring the SSL attributes for the managed servers in Oracle Weblogic Server.
2. **keystore** is used to specify the location of the JKS file. If no JKS file is present in the path provided, one will be created.

The command will prompt for the following attributes of the certificate and keystore:

1. **Keystore Password:** Specify a password that will be used to access the keystore. This password needs to be specified later, when configuring the identity store in Oracle Weblogic Server.
2. **Key Password:** Specify a password that will be used to access the private key stored in the keystore. This password needs to be specified later, when configuring the SSL attributes of the managed server(s) in Oracle Weblogic Server.
3. **First and Last Name (CN):** Enter the domain name of the machine used to access FLEXCUBE UBS, for instance, www.example.com
4. **Name of your Organizational Unit:** The name of the department or unit making the request, for example, BPD. Use this field to further identify the SSL Certificate you are creating, for example, by department or by physical server.
5. **Name of your Organization:** The name of the organization making the certificate request, for example, Oracle Financial Services. It is recommended to use the company or organization's formal name, and this name entered here must match the name found in official records.

6. **Name of your City or Locality:** The city in which your organization is physically located, for example Mumbai.
7. **Name of your State or Province:** The state/province in which your organization is physically located, for example Maharashtra.
8. **Two-Letter Country Code for this Unit:** The country in which your organization is physically located, for example US, UK, IN etc.



The key generation algorithm has been specified as RSA, the key size as 1024 bits, the signature algorithm as SHA1withRSA, and the validity days as 365. These can be changed to suitable values if the need arises. For further details, please refer to the documentation of the keytool utility in the JDK utilized by Oracle Weblogic Server.

Example

Listed below is the result of a sample execution of the command:

```
D:\Oracle\weblogic11g\jrockit_160_05_R27.6.2-20\bin>keytool -  
genkeypair -alias selfcert -keyalg RSA -keysize 1024 -sigalg  
SHA1withRSA -validity 365 -keystore D:\keystores\FCUBSKeyStore.jks  
Enter keystore password:<Enter a password to protect the keystore>  
Re-enter new password:<Confirm the password keyed above>  
What is your first and last name?  
[Unknown]: cvrhp0729.i-flex.com  
What is the name of your organizational unit?  
[Unknown]: BPD  
What is the name of your organization?  
[Unknown]: Oracle Financial Services  
What is the name of your City or Locality?  
[Unknown]: Mumbai  
What is the name of your State or Province?  
[Unknown]: Maharashtra  
What is the two-letter country code for this unit?  
[Unknown]: IN  
Is CN=cvrhp0729.i-flex.com, OU=BPD, O=Oracle Financial Services,  
L=Mumbai, ST=Maharashtra, C=IN correct?  
[no]: yes  
  
Enter key password for <selfcert>  
(RETURN if same as keystore password):<Enter a password to  
protect the key>  
Re-enter new password:<Confirm the password keyed above>
```

3.2 Creating Identity Store with Trusted Certificates Issued by CA

3.2.1 Creation of Public and Private Key Pair

Browse to the bin folder of JRE from the command prompt and type the following command.



The items highlighted in blue are placeholders, and should be replaced with suitable values when running the command.

```
keytool -genkeypair -alias alias -keyalg keyalg -keysize keysize -  
sigalg sigalg -validity valDays -keystore keystore
```

In the above command,

1. ***alias*** is used to identify the public and private key pair created. This alias is required later when configuring the SSL attributes for the managed servers in Oracle Weblogic Server.
2. ***keyalg*** is the key algorithm used to generate the public and private key pair. The RSA key algorithm is recommended.
3. ***keysize*** is the size of the public and private key pairs generated. A key size of 1024 or more is recommended. Please consult with your CA on the key size support for different types of certificates.
4. ***sigalg*** is the algorithm used to generate the signature. This algorithm should be compatible with the key algorithm and should be one of the values specified in the Java Cryptography API Specification and Reference.
5. ***valdays*** is the number of days for which the certificate is to be considered valid. Please consult with your CA on this period.
6. ***keystore*** is used to specify the location of the JKS file. If no JKS file is present in the path provided, one will be created.

The command will prompt for the following attributes of the certificate and keystore:

1. **Keystore Password:** Specify a password that will be used to access the keystore. This password needs to be specified later, when configuring the identity store in Oracle Weblogic Server.
2. **Key Password:** Specify a password that will be used to access the private key stored in the keystore. This password needs to be specified later, when configuring the SSL attributes of the managed server(s) in Oracle Weblogic Server.
3. **First and Last Name (CN):** Enter the domain name of the machine used to access FLEXCUBE UBS, for instance, www.example.com
4. **Name of your Organizational Unit:** The name of the department or unit making the request, for example, BPD. Use this field to further identify the SSL Certificate you are creating, for example, by department or by physical server.

5. **Name of your Organization:** The name of the organization making the certificate request, for example, Oracle Financial Services. It is recommended to use the company or organization's formal name, and this name entered here must match the name found in official records.
6. **Name of your City or Locality:** The city in which your organization is physically located, for example Mumbai.
7. **Name of your State or Province:** The state/province in which your organization is physically located, for example Maharashtra.
8. **Two-letter Country Code for this Unit:** The country in which your organization is physically located, for example US, UK, IN etc.

Example

Listed below is the result of a sample execution of the command:

```
D:\Oracle\weblogic11g\jrockit_160_05_R27.6.2-20\bin>keytool -  
genkeypair -alias cvrhp0729 -keyalg RSA -keysize 1024 -sigalg  
SHA1withRSA -validity 365 -keystore D:\keystores\FCUBSKeyStore.jks  
Enter keystore password:<Enter a password to protect the keystore>  
Re-enter new password:<Confirm the password keyed above>  
What is your first and last name?  
[Unknown]: cvrhp0729.i-flex.com  
What is the name of your organizational unit?  
[Unknown]: BPD  
What is the name of your organization?  
[Unknown]: Oracle Financial Services  
What is the name of your City or Locality?  
[Unknown]: Mumbai  
What is the name of your State or Province?  
[Unknown]: Maharashtra  
What is the two-letter country code for this unit?  
[Unknown]: IN  
Is CN=cvrhp0729.i-flex.com, OU=BPD, O=Oracle Financial Services,  
L=Mumbai, ST=Maharashtra, C=IN correct?  
[no]: yes  
  
Enter key password for <cvrhp0729>  
(RETURN if same as keystore password):<Enter a password to  
protect the key>  
Re-enter new password:<Confirm the password keyed above>
```

3.2.2 Generating CSR

To purchase an SSL certificate, one needs to generate a Certificate Signing Request (CSR) for the server where the certificate will be installed.

A CSR is generated from the server and is the server's unique "fingerprint". The CSR includes the server's public key, which enables server authentication and secure communication.



If the keystore file or the password is lost and a new one is generated, the SSL certificate and the private key will no longer match. A new SSL Certificate will have to be requested.

The CSR is created by running the following command in the bin directory of the JRE:

```
keytool -certreq -alias alias -file certreq_file -keystore keystore
```

In the above command,

1. **alias** is used to identify the public and private key pair. The private key associated with the alias will be utilized to create the CSR. Specify the alias of the key pair created in the previous step.
2. **certreq_file** is the file in which the CSR will be stored.
3. **keystore** is the location of the keystore containing the public and private key pair.

Example

Listed below is the result of a sample execution of the command

```
D:\Oracle\Weblogic11g\jrockit_160_05_R27.6.2-20\bin>keytool -certreq -  
alias cvrhp0729 -file D:\keystores\certreq.csr -keystore  
D:\keystores\FCUBSKeyStore.jks  
Enter keystore password: [Enter the password used to access the  
keystore]  
Enter key password for <cvrhp0729> [Enter the password used to access  
the key in the keystore]
```

3.2.3 Obtaining Trusted Certificate from CA

The processes of obtaining a trusted certificate vary from one CA to another. The CA might perform additional offline verification. Consult the CA issuing the certificate for details on the process to be followed for submission of the CSR and for obtaining the certificate.

3.2.4 Importing Certificate into Identity Store

Store the certificate obtained from the CA in the previous step, in a file, preferably in PEM format. Other formats like the p7b file format would require conversion to the PEM format. Details on performing the conversion are not listed here. Please refer to the Oracle Weblogic Server documentation on Securing Oracle Weblogic Server, for details on converting a Microsoft p7b file to the PEM format.

The command to be executed for importing a certificate into the identity store depend on whether the trust store chosen (in the earlier step; see section 2 of this document). It is highly recommended to verify the trust path when importing a certificate into the identity store. The commands provided below assume the use of the Java Standard Trust store.

Importing the Intermediate CA certificate

Most Certificate Authorities do not use the root CA certificates to issue identity certificates for use by customers. Instead, Intermediate CAs issue identity certificates in response to the submitted CSRs.

If the Intermediate CA certificate is absent in the Java Standard Trust store, the trust path for the certificate will be incomplete for the certificate, resulting in warnings issued by Weblogic Server during runtime. To avoid this, the intermediate CA certificate should be imported into the identity keystore. Although the intermediate CA certificate can be imported into the Java Standard Trust store, this is not recommended unless the intermediate CA can be trusted.

The following command should be executed to import the intermediate CA certificate into the keystore.

```
keytool -importcert -alias alias -file cert_file -trustcacerts -keystore  
keystore
```

In the above command,

1. ***alias*** is used to identify the public and private key pair. Specify the alias of the key pair used to create the CSR in the earlier step.
2. ***cert_file*** is the location of the file containing the intermediate CA certificate in a PKCS#7 format (PEM or DER file).
3. ***keystore*** is the location of the keystore containing the public and private key pair.

 The trustcacerts flag is used to consider other certificates (higher intermediaries and the root CA) in the chain of trust. If no chain of trust is established during verification, the certificate will be displayed and one would be prompted to verify it. It is recommended that due diligence be observed, when the prompt is displayed to verify a certificate when a chain of trust is absent.

Listed below is a sample execution of the command

```
D:\Oracle\weblogic11g\jrockit_160_05_R27.6.2-20\bin>keytool -  
importcert -alias verisigntrialintermediateca -file  
D:\keystores\VerisignIntermediateCA.cer -trustcacerts -keystore  
D:\keystoreworkarea\FCUBSKeyStore.jks  
Enter keystore password:<Enter the password used to access the  
keystore>  
Certificate was added to keystore
```

Importing the Identity certificate

The following command should be executed to import the identity certificate into the keystore.

```
keytool -importcert -alias alias -file cert_file -trustcacerts -keystore  
keystore
```

In the above command,

1. ***alias*** is used to identify the public and private key pair. Specify the alias of the key pair used to create the CSR in the earlier step.

2. ***cert_file*** is the location of the file containing the PKCS#7 formatted reply from the CA, containing the signed certificate.
3. ***keystore*** is the location of the keystore containing the public and private key pair.

The trustcacerts flag is used to consider other certificates (intermediate CAs and the root CA) in the chain of trust. If no chain of trust is established during verification, the certificate will be displayed and one would be prompted to verify it. It is recommended that due diligence be observed, when the prompt is displayed to verify a certificate when a chain of trust is absent.

Listed below is a sample execution of the command

```
D:\Oracle\weblogic11g\jrockit_160_05_R27.6.2-20\bin>keytool -  
importcert -alias cvrhp0729 -file D:\keystores\cvrhp0729.cer -  
trustcacerts -keystore D:\keystoreworkarea\FCUBSKeyStore.jks  
Enter keystore password:<Enter the password used to access the  
keystore>  
Enter key password for <cvrhp0729>:<Enter the password used to access  
the private key>  
Certificate reply was installed in keystore
```

 The previous set of commands assumed the presence of the appropriate root CA certificate (in the chain of trust) in the Java Standard Trust store, i.e. in the cacerts file. If the CA issuing the identity certificate (for the Weblogic Server) does not have the root CA certificate in the Java Standard Trust store, one can opt to import the root CA certificate into cacerts, or into the identity store, depending on factors including trustworthiness of the CA, necessity of transporting the trust store across machine, among others.

4. Configuring Identity and Trust Stores for Weblogic

4.1 Enabling SSL on Oracle Weblogic Server

To configure SSL on Oracle Weblogic server, login in to the Admin Console and follow the steps given below:

1. Under 'Change Center', click the button 'Lock & Edit'.
2. Expand 'Servers' node.
3. Select the name of the server for which you want to enable SSL (example - exampleserver).
4. Go to 'Configuration' and select General' tab.
5. Select the option 'SSL Listen Port Enabled' and specify the SSL listen port.
6. Against 'Listen Address', specify the hostname of the machine in which the application server is installed.

4.2 Configuring Identity and Trust Stores

To configure the Identity and Trust stores in Oracle Weblogic Server, log in to the Admin Console of Weblogic Server.

1. Under 'Change Center', click the button 'Lock & Edit'.
2. Expand 'Servers' node.
3. Select the name of the server for which you want to configure the keystores (example - exampleserver).
4. Go to 'Configuration' and select 'Keystores' tab.
5. In the filed 'Keystores', select the method for storing and managing private keys/digital certificate pairs and trusted CA certificates. This choice should match the one made in Section 2 of this document (Choosing the Identity and Trust Stores).
6. In the 'Identity' section, provide the following details:
 - **Custom Identity Keystore File Name:** Fully qualified path to the Identity keystore.
 - **Custom Identity Keystore Type:** Set this attribute to JKS, the type of the keystore. If left blank, it is defaulted to JKS (Java KeyStore).
 - **Custom Identity Keystore PassPhrase:** The password you enter when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. Oracle Weblogic server only reads from the keystore. So whether or not you define this property depends on the requirements of the keystore.
7. In the 'Trust' section, provide the following details:

If you choose **Java Standard Trust**, specify the password used to access the trust store.

If you choose **Custom Trust**, the following attributes have to be provided:

- **Custom Trust Keystore:** The fully qualified path to the trust keystore.
- **Custom Trust Keystore Type:** Set this attribute to JKS, the type of the keystore. If left blank, it defaults to JKS (Java KeyStore).
- **Custom Trust Keystore Passphrase:** The password you enter when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. Oracle Weblogic Server only reads from the keystore. So, whether or not you define this property depends on the requirements of the keystore.



When identity and trust stores are of the JKS format, the passphrases are not required.

5. Setting SSL attributes for Managed Servers

5.1 Setting SSL Attributes for Private Key Alias and Password

To configure the private key alias and password, log in to the Oracle Weblogic Server Admin Console.

1. Under '**Change Center**', click the button 'Lock & Edit'.
2. Expand '**Servers**' node.
3. Select the name of the server for which you want to configure keystores (example - exampleserver).
4. Go to '**Configuration**' and select '**SSL**' tab.
5. Select 'Keystores' from '**Identity and Trust Locations**'.
6. Under 'Identity' section, specify the following details:
 - **Private Key Alias:** set this attribute to the alias name defined for the key pair when creating the key pair in the Identity keystore.
 - **Private Key Passphrase:** The password defined for the key pair (alias_password), at the time of its creation. . Confirm the password.
7. Click '**Save**'.
8. Under '**Change Center**', click '**Activate changes**'.
9. Go to **controls** tab, check the appropriate server and click '**Restart SSL**'. Confirm when it prompts.

6. Testing Configuration

6.1 Testing Configuration

Once the Oracle Weblogic has been configured for SSL, deploy the application in the usual manner. After deployment, you can test the application in SSL mode. To launch the application in SSL mode you need to enter the URL in the following format:

https://(Machine Name):(SSL_Listener_port_no)/(Context_root)



It is recommended that the Oracle FLEXCUBE UBS web application be accessed via the HTTPS channel, instead of the HTTP channel.

7. Creating Resources on Weblogic

7.1 Introduction

This document explains the steps to be executed to deploy the FCUBS application and gateway application in application server.

7.2 Resource Administration

This section deals with the process of resource administration on Oracle Weblogic.

All the resources mention in “Resources To be Created” document are need to be created before deployment. One example for each category is explained in the following subsections.

7.2.1 Creating Data Source

The method for creating data sources is explained under the following headings.

7.2.1.1 Prerequisites

You need to create the data source with OCI enabled. For this, download Oracle Instant Client and install it. The details are given below.

Package	Download Location	Remarks
Oracle Instant Client Package	http://www.oracle.com/technetwork/database/features/instant-client/index-097480.html	Install Oracle Instant Client in a local directory. While configuring Weblogic for Windows or Unix/Linux box, you need to provide the directory path where Instant Client is installed.

You need to do the data source configuration with OCI driver enabled. The configurations are given below.

- Oracle Weblogic on Windows Box:
 - Set `{ORACLE_HOME}` in the environment variable.
 - Update the Environment Variable Path as `{ORACLE_HOME}/Instance Client`. This is required to load all the `.dll` files.
 - Ensure that the `ojdbc*.jar` file in `{WL_HOME}/server/lib/ojdbc*.jar` is the same as the file `{ORACLE_HOME}/jdbc/lib/ojdbc*.jar`. This is required for ensuring compatibility.
 - Update PATH in `StartWebLogic.bat` or in `setDomainEnv.bat`. This must be the path of directory where Oracle Instant Client is installed.
 - Oracle Weblogic on Unix/Linux Box:

- Set `{ORACLE_HOME}` in the environment variable.
- Update the environment variable `LD_LIBRARY_PATH` as `{ORACLE_HOME}/lib`. This is to load all the .so files.
- Ensure that the `ojdbc*.jar` file in `{WL_HOME}/server/lib/ojdbc*.jar` is the same as the file `{ORACLE_HOME}/jdbc/lib/ojdbc*.jar`. This is to ensure compatibility.
- Update `LD_LIBRARY_PATH` in `StartWeblogic.sh` or in `setDomainEnv.sh`. This must be the path of directory where Oracle Instant Client is installed.
- If you are still not able to load the .so files, then you need to update the `EXTRA_JAVA_PROPERTIES` by setting `Djava.library.path` as `{ORACLE_HOME}/lib` in `StartWebLogic.sh` or in `setDomainEnv.sh`.

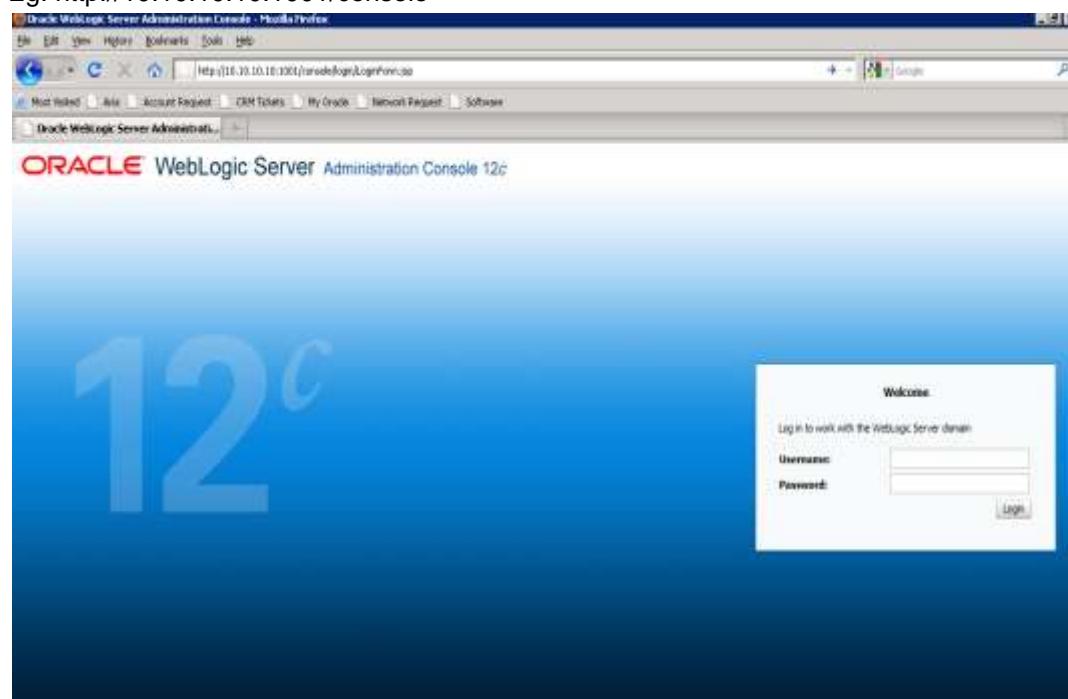
7.2.1.2 XA Enabled Data Source

Follow the steps given below:

1. Start the Administrative Console of Weblogic application server. You can start this by entering Oracle Weblogic Admin Console URL in the address bar in an internet browser.

`http://10.10.10.10:1001/console`

Eg: `http://10.10.10.10:1001/console`



2. Specify the Weblogic administrator user name and password. Click 'Log In'.

3. Navigate to Oracle Weblogic home page.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The title bar reads "Home Page - tru113_domain - WLSCoreConsole - Microsoft Internet Explorer". The main content area is titled "Home Page" and contains several sections:

- Information and Resources**: Includes links to "Configure applications", "Configure GridLink for RAC Data Source", "Reset Task Status", "Set user profile preferences", "Common Administrative Task Descriptions", "Read the documentation", "Ask a question on My Oracle Support", and "Oracle Guardian Overview".
- Domain Structure**: Shows the domain structure with nodes like "Environment", "Deployments", "Services", "Security Realms", "Interoperability", and "Diagnostics".
- Next Step**: Lists actions such as "Search the configuration", "Use the Change Center", "Revert MDT Setup", "Change Coherence preferences", and "Monitor servers".
- System Status**: Displays the "Health of Running Services" with categories: Failed (0), Critical (1), Overloaded (0), Warning (0), and OK (0).
- Your Application's Security Settings**: Includes a link to "Security Realms".
- General Information**: Links to "WLS Configuration", "WLS Modules", "WLS Services", "Bridges", "Data Sources", "Persistent Stores", "WLS Registry", "WLS Shady Caches", "Foreign JNDI Providers", "Mail Connectors", "JNDI", "Mail Destinations", "File I/O", and "JMS".
- Interoperability**: Links to "WTC Servers" and "JMS Connection Pools".
- Diagnostic**: Links to "Log Files", "Diagnostic Modules", "Diagnostic Dumper", "Request Performance", "Archives", "Corset", and "OMF".
- Charts and Graphs**: A link to "Monitoring Dashboard".

4. Click 'LOCK & EDIT'.

Following screen is displayed:

The screenshot shows the Oracle WebLogic Server Administration Console interface. The title bar reads "Summary of JDBC Data Sources - Eclat111_domain - WLSC Console - Microsoft Internet Explorer". The main content area is titled "Summary of JDBC Data Sources". It displays a table of data sources with the following columns: Name, Type, JNDI Name, and Targets. There are two entries in the table:

Name	Type	JNDI Name	Targets
PCDB111	Generic	jdbc:PointOfSale	ManagedServer1
PCDB111Branch	Generic	jdbc:PointOfSaleBranch	ManagedServer1

Below the table, there are sections for "Change Center" (with a note about pending changes), "Domain Structure" (showing the domain structure with nodes like Environment, Deployments, etc.), and "System Status" (listing managed servers with their status: Failed (0), Down (0), Disconnected (0), Running (0), and OK (2)).

5. Expand 'Services' and then 'Data Sources' under it. Click 'Lock & Edit' button.

Name	Type	JNDI Name	Targets
Generic Data Source	Generic	java:comp/env/jdbc/DS1	ManagerServer
Multitenant Data Source	Generic	java:comp/env/jdbc/MDS	ManagerServer
FLEXTESTDB	Generic	java:comp/env/jdbc/FLEXTESTDB	ManagerServer

6. To create a new data source, click 'New' and select 'Generic Data Source'. The following screen is displayed.

7. Specify the following details:

JDBC Datasource Name	Name of the data source
JNDI Name	JNDI name which will be used for lookup
Database Type	Type of the database which is Oracle

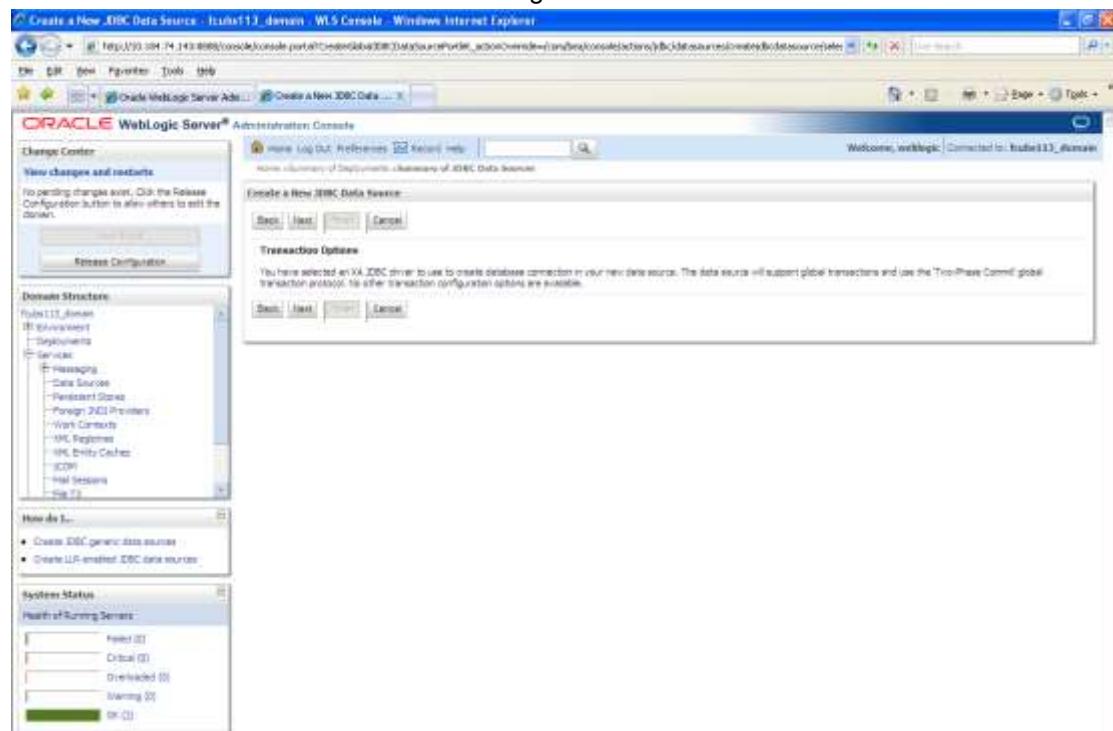
8. Click 'Next'.

The following screen is displayed:

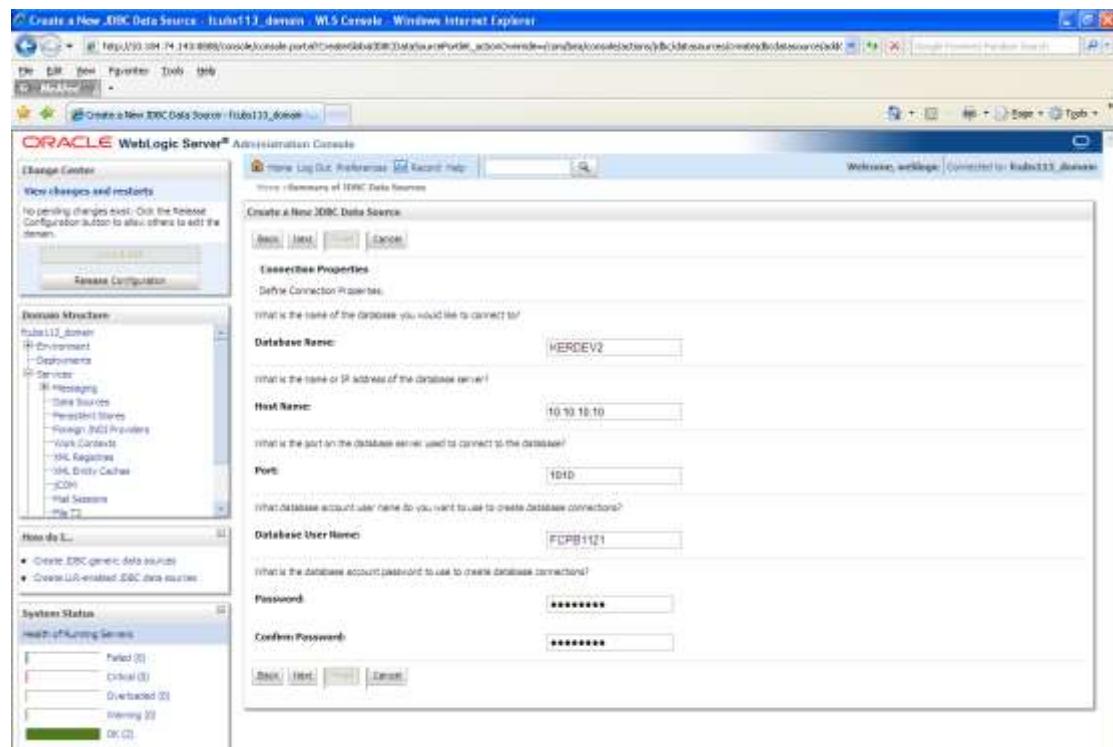
The screenshot shows a web-based configuration interface for creating a new JDBC data source. At the top, there's a navigation bar with links for Home, Log Out, Preferences, Record, Help, and a search bar. Below the navigation is a breadcrumb trail: Home > Summary of Services > Summary of JDBC Data Sources. The main title is "Create a New JDBC Data Source". Below the title, there are four buttons: Back, Next, Finish, and Cancel. The first section is titled "JDBC Data Source Properties" and contains the instruction: "The following properties will be used to identify your new JDBC data source." It shows two entries: "Database Type: Oracle" and "Database Driver: *Oracle's Driver (Thin XA) for Service connections; Versions: Any". At the bottom of this section are the same four buttons: Back, Next, Finish, and Cancel.

Click next.

9. Select the database driver as shown in the figure. Click 'Next'.

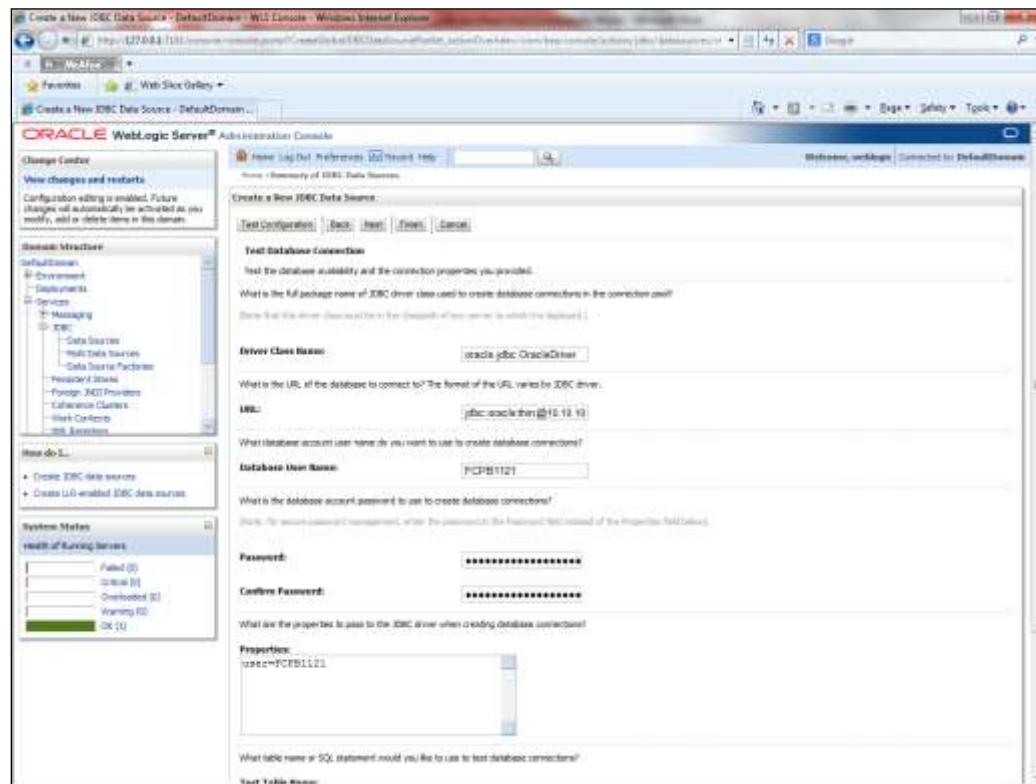


10. Specify the Database Name, Host Name, Port of the database server to connect, Database User Name and Password. Confirm the password.



11. Click 'Next'.

The following screen is displayed.



12. Specify the Driver Class Name (Eg: oracle.jdbc.OracleDriver).

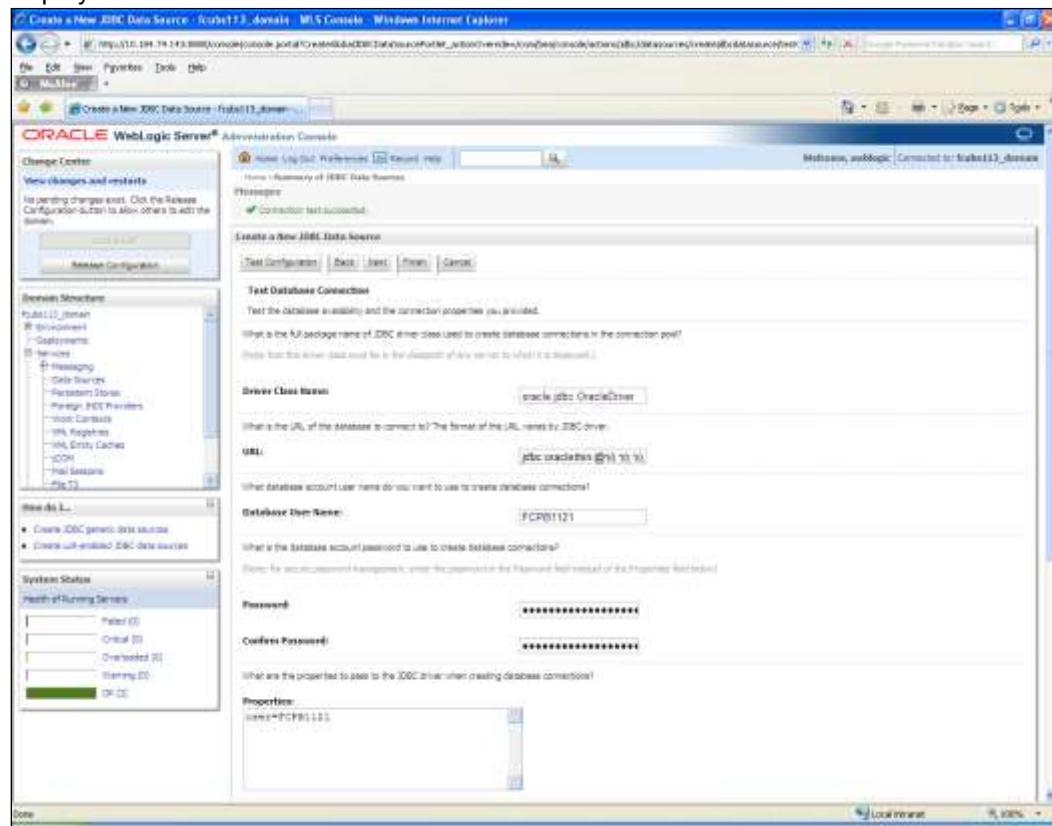
13. Specify the URL.

14. jdbc:oracle:thin:@10.10.10.10:1001<INSTANCE_NAME>Specify the Database Username (Eg: FCPB1121) and password.

15. Confirm the password.

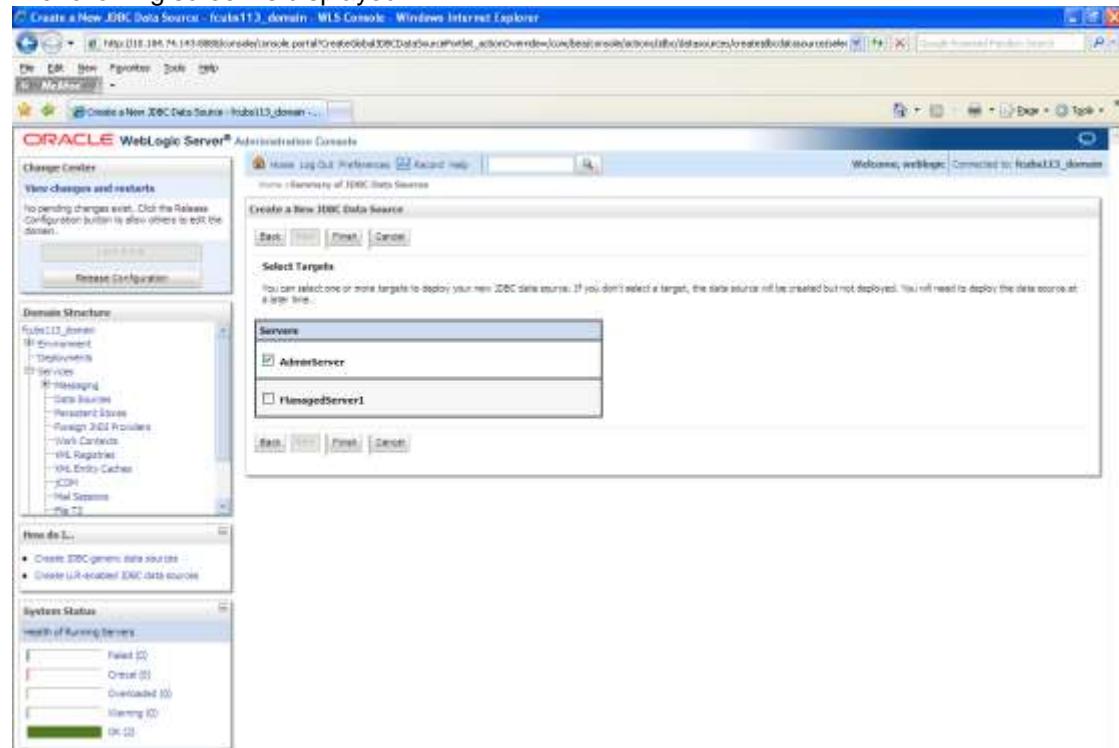
16. Click 'Test Configuration' tab.

If the connection is established successfully, the message 'Connection test succeeded' is displayed.

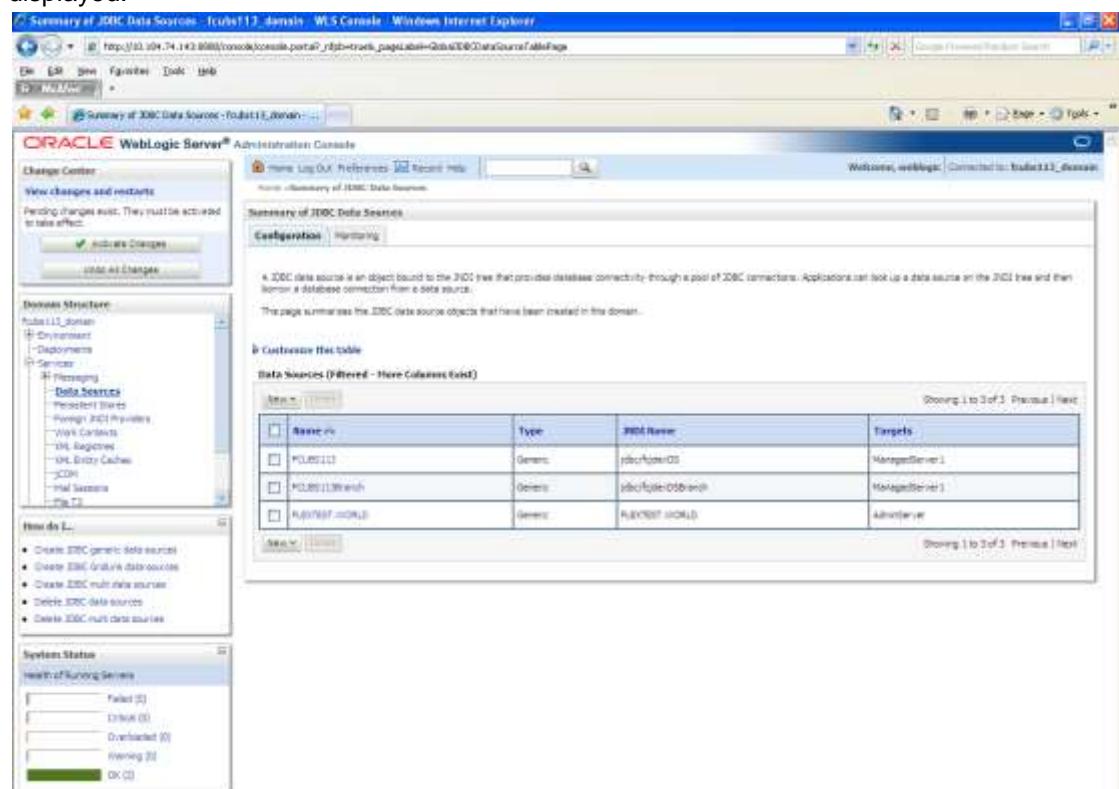


17. Click 'Next'.

The following screen is displayed:



18. Check the boxes against the required servers. Click 'Finish'. The following screen is displayed:



19. Click 'Activate Changes' button. Click 'Activate Changes' button on the left pane. The message 'All the changes have been activated. No restarts are necessary' is displayed.

The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar has a 'Change Center' section with a 'View changes and restarts' link and a 'Lock & Edit' button. Below it is a 'Domain Structure' tree with 'Fuchs113_domain' expanded, showing 'Universal', 'Deployments', and 'Services' nodes. Under 'Services', 'Data Sources' is selected, showing sub-options like 'Persistent Conn', 'Foreign JNDI Providers', 'Work Connect', 'IML Required', 'IML Write Cache', 'JNDI', 'IML Session', and 'Log TS'. A 'How do I...' link provides instructions for creating generic, multi-link, and multi-data sources, as well as deleting them. The main content area is titled 'Summary of JDBC Data Sources' and shows a table of data sources:

Name	Type	JDBC Name	Target
PCDBTEST	Generic	pcdbtestds	ManagerServer1
PCDBTEST-BRANCH	Generic	pcdbtest-branch	ManagerServer1
PCDBTEST-WORLD	Generic	pcdbtest-world	AdminServer

Below the table, there are 'Previous' and 'Next' navigation links. The bottom of the page shows a 'System Status' section with a 'Health of Running Services' table:

Health	Count
Fixed	0
Critical	0
Overloaded	0
Warning	0
OK	0

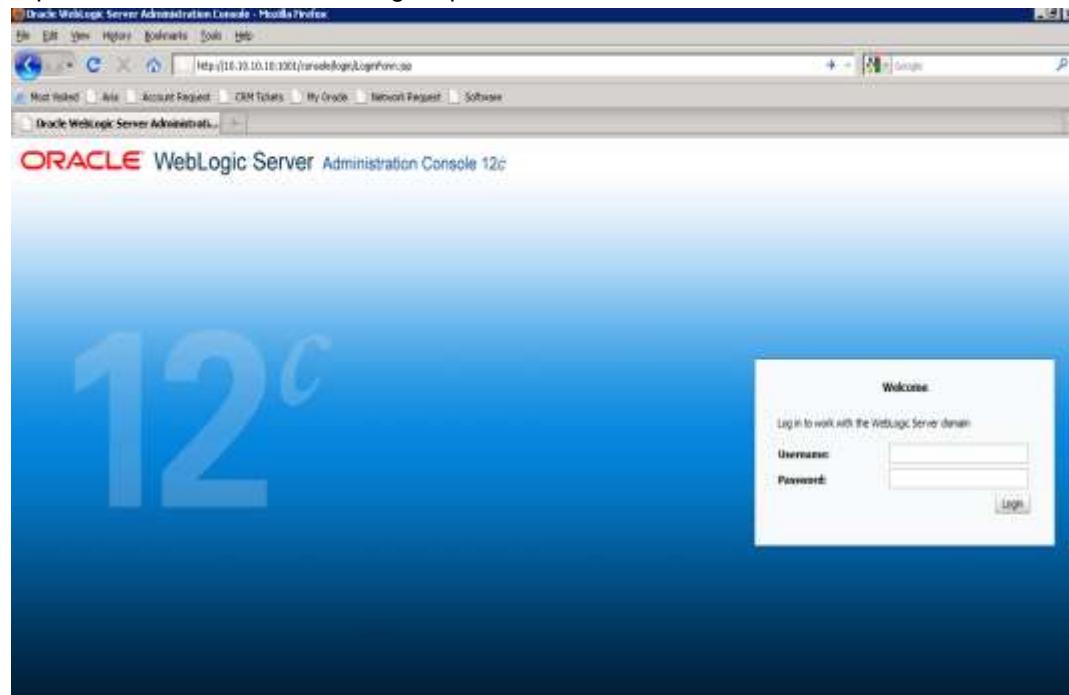
20. The datasource has been created.

21. Refer to "Resources_To_Be_Created.doc" for the list of XA datasources to be created.

7.2.1.3 Non-XA Enabled Data Source

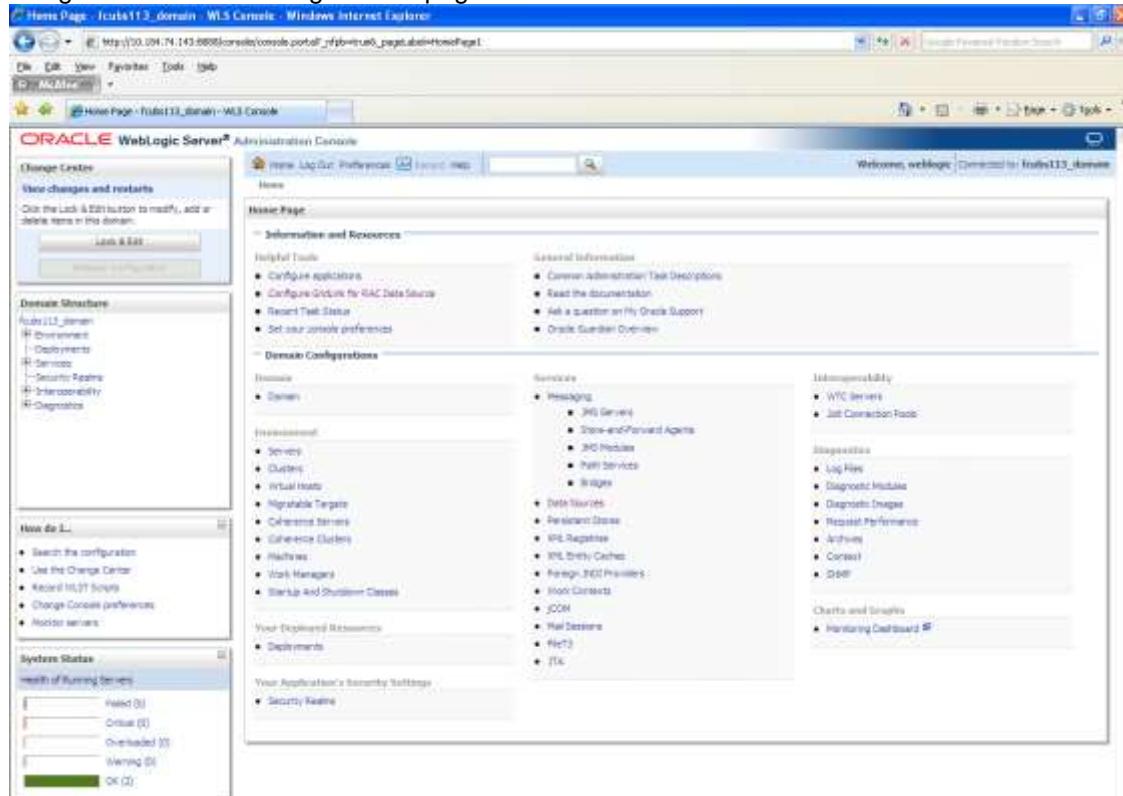
1. Follow the steps given below: Start the Administrative Console of Weblogic application server. You can start this by entering Oracle Weblogic Admin Console URL in the address bar in an internet browser.

http://10.10.10.10:1001/console Eg: http://10.10.10.10:1001/console



2. Specify the Weblogic administrator user name and password. Click 'Log In'.

3. Navigate to Oracle Weblogic home page.



The following screen is displayed:

This screenshot shows the Oracle WebLogic Server Administration Console interface. The left sidebar contains a navigation tree with nodes like 'Domain Structure' (including 'WebLogic Domain', 'Environment', 'Deployments', 'Services', 'JMS', 'Messaging', 'Data Sources', 'Persistent Stores', 'Work Contexts', 'XML Repositories', 'CDH', 'Mail Session', 'File T2'), 'How do I...' (with options for creating generic, JNDI, or multi-data sources), and 'System Status' (listing services like 'Health of Admin Services' with status 'OK'). The main content area is titled 'Summary of JDBC Data Sources' and displays a table of data sources. The table has columns: 'Name' (checkbox), 'Name (i18n)', 'Type', 'JNDI Name', and 'Targets'. It lists two entries: 'PCDBS113' (Generic, jndi:PicewDS, ManagedServer1) and 'PCDBS113Branch' (Generic, jndi:PicewDBBranch, ManagedServer1). A note at the bottom of the table states: 'A JDBC data source is an object bound to the JNDI tree that provides database connections through a pool of JDBC connections. Applications can look up a data source in the JNDI tree and then obtain a database connection from a data source.' Below the table are links for 'Create New Table' and 'Data Sources (Filtered - More Columns Exist)'.

Name	Name (i18n)	Type	JNDI Name	Targets
<input type="checkbox"/>	PCDBS113	Generic	jndi:PicewDS	ManagedServer1
<input type="checkbox"/>	PCDBS113Branch	Generic	jndi:PicewDBBranch	ManagedServer1

4. Expand 'Services' and then 'Data Sources' under it. Click 'Lock & Edit' button.

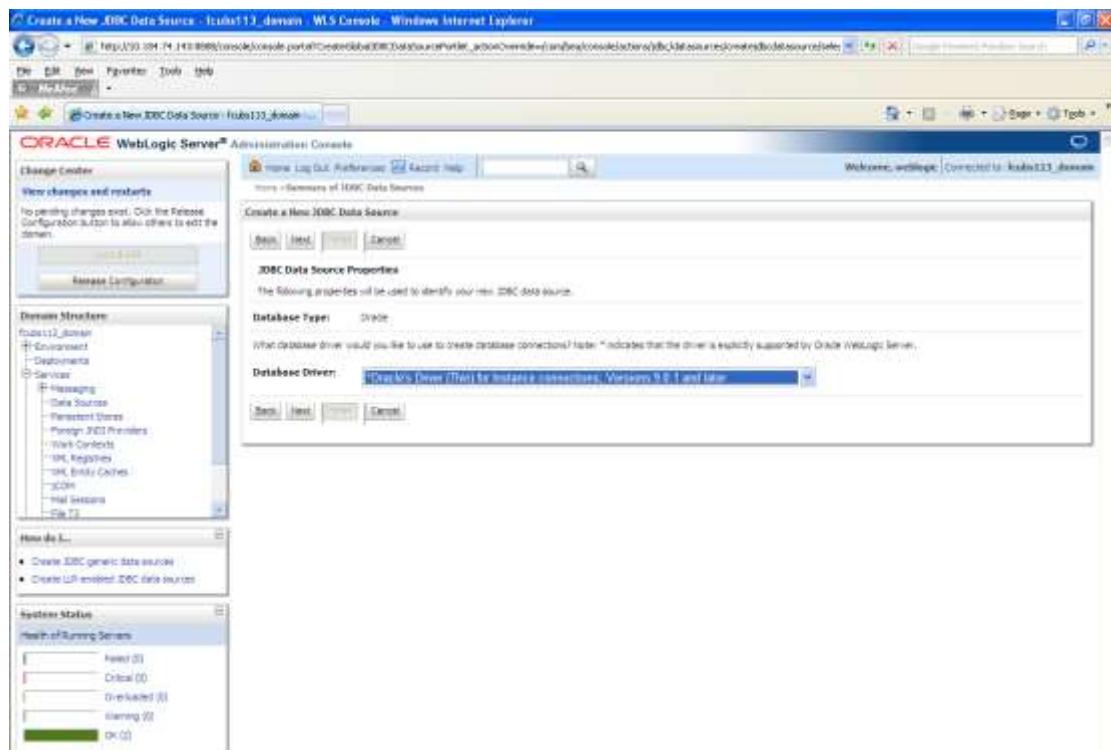
Name	Type	JNDI Name	Targets
FCUBS113DS	Generic	jdbc/fojdevDS	ManagerServer1
Multitenant Data Source	Generic	jdbc/TNS-DB-DS	ManagerServer1
FCUBS113DS	Generic	jdbc/fojdevDS	ManagerServer1

5. To create a new data source, click 'New' and select 'Generic Data Source'.

6. Specify the following details:

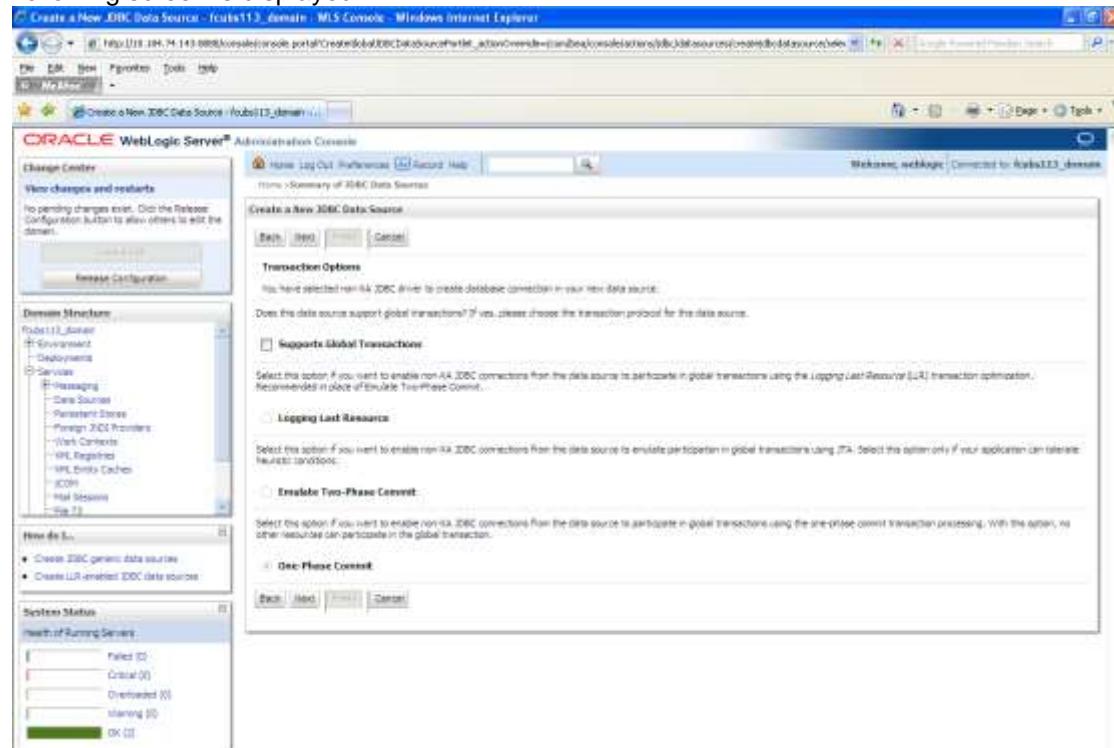
JDBC Datasource Name	Name of the Datasource
JNDI Name	JNDI for lookup
Database Type	Oracle

7. Click 'Next'.

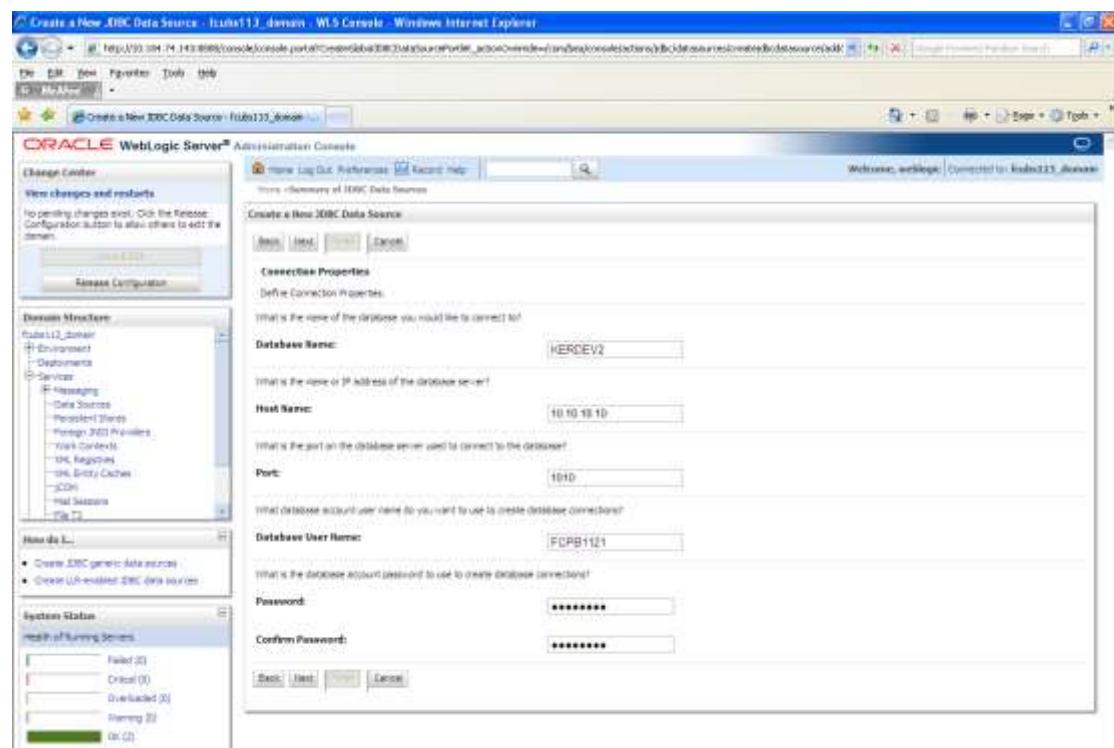


8. Select the database driver as shown in the figure. Click 'Next'.

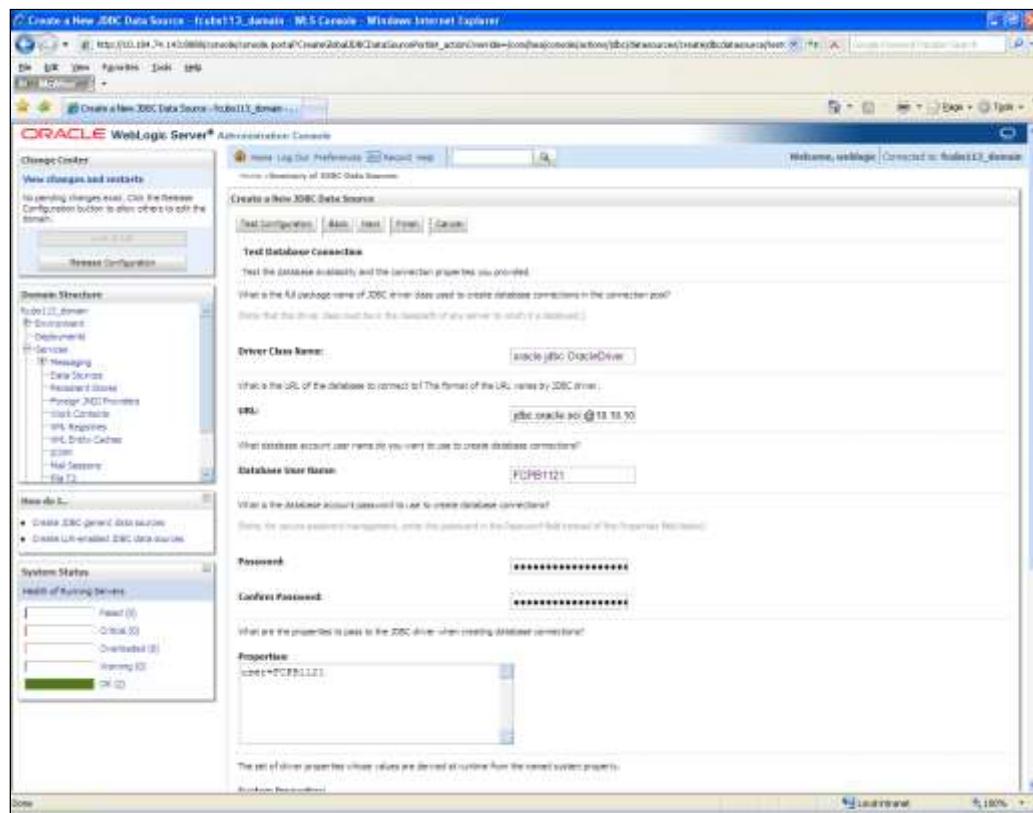
Following screen is displayed:



9. Select Logging Last Resource then uncheck 'Support Global Transactions'. Click 'Next'. The following screen is displayed:



10. This screen defines the connection properties. Set the details as given below:
11. Specify the Database Name, Host Name, Port of the database server to connect, Database User Name and Password. Confirm the password.
12. Click 'Next'. The following screen is displayed.

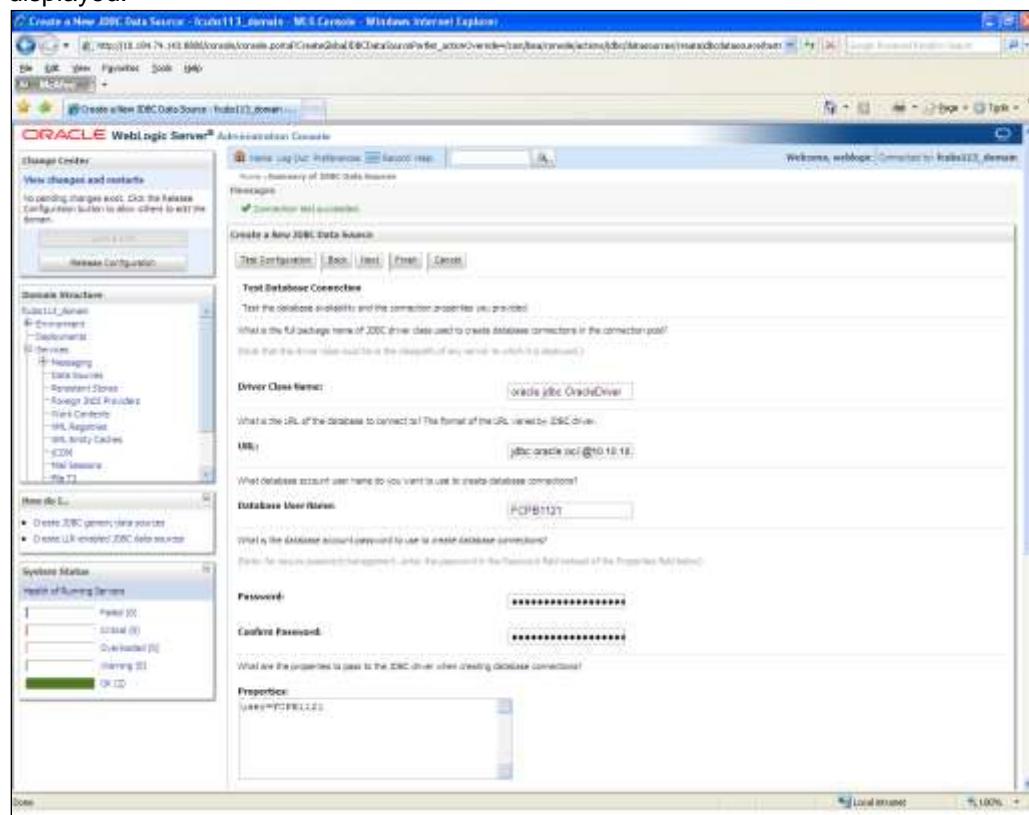


13. Specify the Driver Class Name (Eg: oracle.jdbc.OracleDriver)
14. Specify the URL.

Default URL: `jdbc:oracle:thin:@10.10.10.10:1001:<INSTANCE_NAME>`.
 Change the default URL to: `jdbc:oracle:oci:@10.10.10.10:1010:<INSTANCE_NAME>`

15. Specify the Database Username (Eg: testdb) and password.
16. Confirm the password.
17. Click 'Test Configuration' tab.

18. If the connection is established successfully, the message ‘Connection test succeeded’ is displayed.



19. Click ‘Next’. The following screen is displayed:



- 20.** Check the boxes against the required servers(for data source jdbc/fcjdevDS, it is mandatory to check the admin server as well as application-deployed server). Click 'Finish'. The following screen is displayed:

Name	Type	JNDI Name	Targets
POLESL11	General	jdbc/fcjdevDS	ManageServer1
POLESL11Branch	General	jdbc/fcjdevDSBranch	ManageServer1
PLETEST.WORLD	General	PLETEST.WORLD	AdminServer

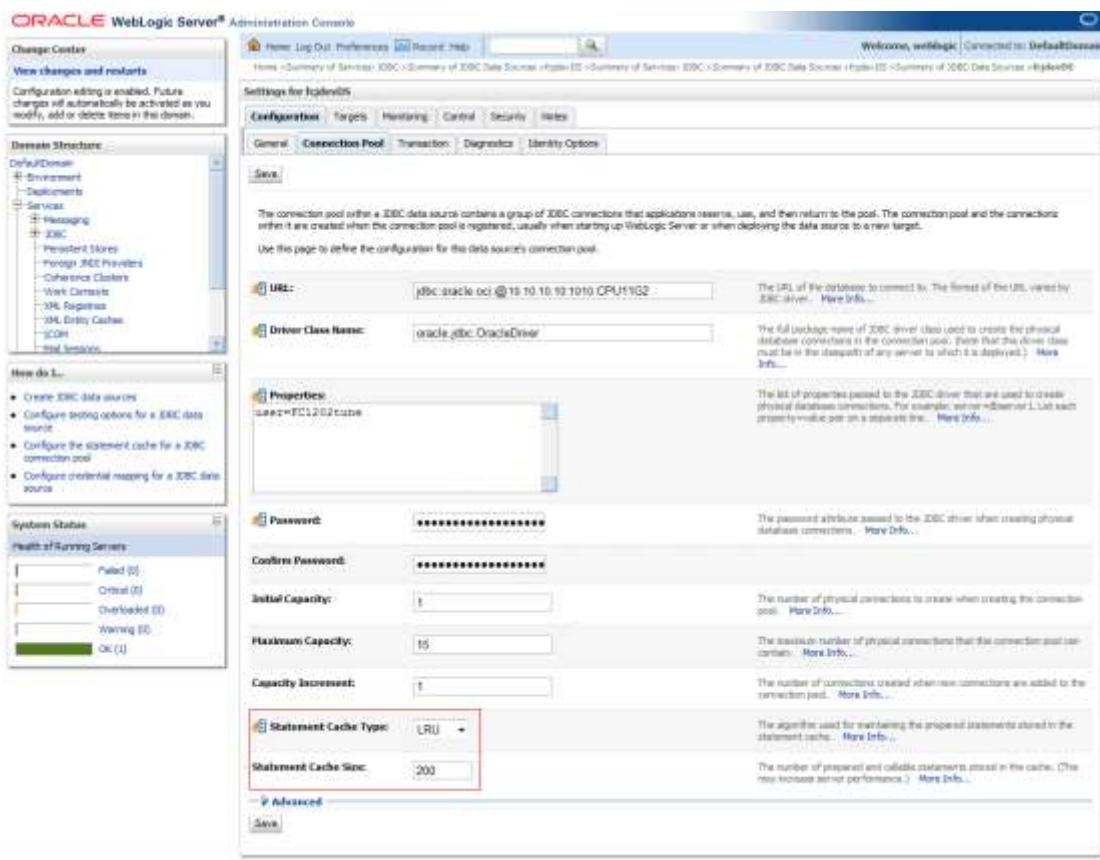
- 21.** Click 'Activate Changes' button. Click 'Activate Changes' button on the left pane.

The message 'All the changes have been activated. No restarts are necessary' is displayed.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The title bar reads "Summary of JDBC Data Sources - Fcube13_domain - WLSCore - Windows Internet Explorer". The main content area displays the "Summary of JDBC Data Sources" page. On the left, there is a navigation tree under "Change Center" with sections like "View changes and restarts", "Domain Structure", "How do I...", and "System Status". The right side has tabs for "Configuration" and "Monitoring". A message at the top states "All changes have been activated. No restarts are necessary." Below this, a table lists three data sources:

Name	Type	JNDI Name	Targets
FCUBSDS	Generic	jdbc/fcubds	ManagedServer1
FCUBSDSadmin	Generic	jdbc/fcubds-admin	ManagedServer1
PLEXTEST_WORLDS	Generic	PLEXTEST_WORLD	AdminServer

22. 'FCUBSDS' datasource is created.
23. Click the datasource, and then click on the Connection Pool tab.



24. Select the statement cache type as 'LRU'.
25. Specify the statement cache size as '200'.
26. Click 'Save'.
27. Refer to "Resources_To_Be_Created.doc" for the list of Non-XA datasources to be created.



Note the following

- o You need to create another data source for Oracle FCUBS with the JNDI name '<Non-XA FCUBS HOST JNDI name>_ASYNC' for batch process. For example, if the Oracle FCUBS HOST Non XA data source JNDI name is 'jdbc/fcjdevDS', then you need to create another data source for FCUBS with the JNDI name 'jdbc/fcjdevDS_ASYNC'.
- o While creating a branch using the 'Branch Parameters Maintenance' (STDBRANC) screen, if you have created a data source for the branch, then you need to create a corresponding ASYNC data source with the JNDI name '<Non-XA FCUBS BRANCH JNDI name>_ASYNC'.
- o You need to create another data source for Oracle ELCM with the JNDI name '<ENTITY_ID JNDI name>_EL'. For example, if the Oracle FCUBS HOST Non XA data source JNDI name is 'jdbc/fcjdevDS', then you need to create another data source for FCUBS with the JNDI name 'jdbc/fcjdevDS_EL'. Ensure that the checkbox "Support Global Transaction" is checked and select "Emulate Two-Phase Commit" for ELCM data source.

- The following are the list of datasources that can be created depending on the requirement. Please refer to the document Resources_to_be_created.docx for more information -

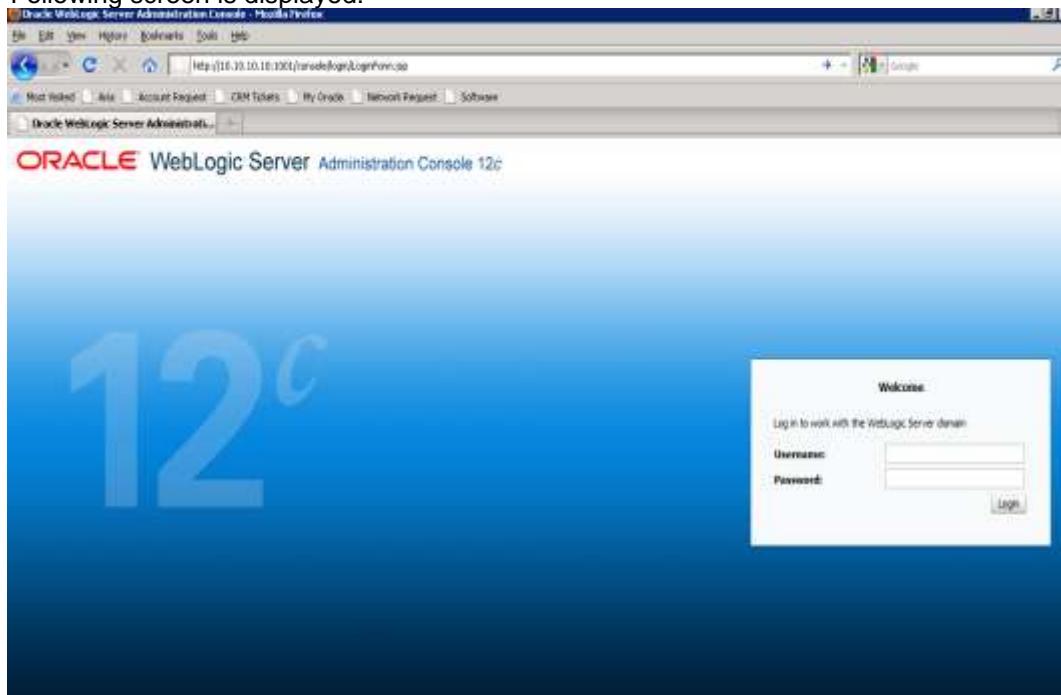
Purpose	Datasource Name	JNDI Name
FCUBS	FCUBS Data source	jdbc/fcjdevDS
SMS	SMS Datasource	jdbc/fcjdevDSSMS
VAMS	VAMS_DATASOURCE	jdbc/fcvamDS
Gateway	FLEXTEST.WORLD	FLEXTEST.WORLD
Async data source	FCUBS DS_ASYNC	jdbc/fcjdevDS_ASYNC
Scheduler	Scheduler_Datasource	jdbc/fcjSchedulerDS

7.2.2 JMS Server Creation

Follow the steps given below:

- Start the Administrative Console of Weblogic application server. You can start this by entering Oracle Weblogic Admin Console URL in the address bar in an internet browser.
<http://10.10.10.10:1001/console> Eg: http://10.10.10.10:1001/console

Following screen is displayed:



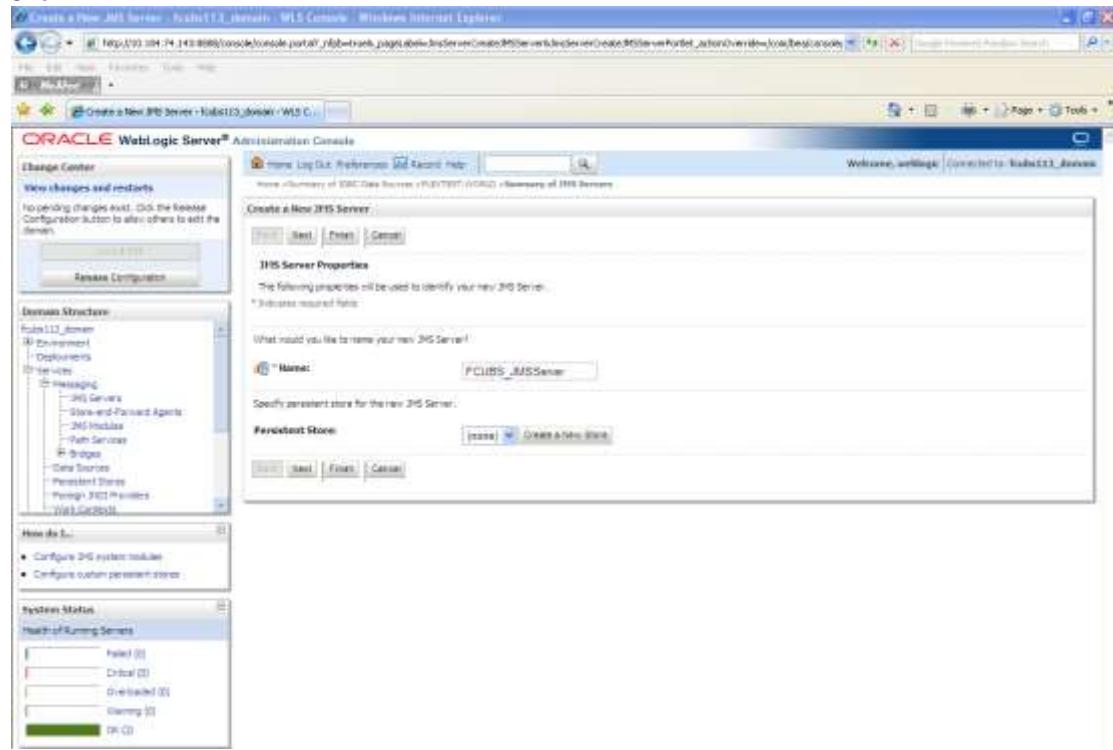
- Specify the Weblogic administrator user name and password. Click 'Log In'.
- Navigate to Oracle Weblogic home page.

The screenshot shows the Oracle WebLogic Server Administration Console interface. At the top, the URL is http://10.10.113.143:8080/console/console.portal?_nfpb=true&_pageLabel=HomePage. The left sidebar includes sections for Change Center, Domain Structure, Help, and System Status. The main content area displays the Home Page with sections for Information and Resources, General Information, Domain Configuration, Resources, Services, Interoperability, Diagnostic Modules, and Monitoring Dashboard.

4. Following screen is displayed:

5. Expand 'Services' and then 'Messaging' and 'JMS Server' under it. Click 'Lock & Edit' button.

6. Click 'New'.

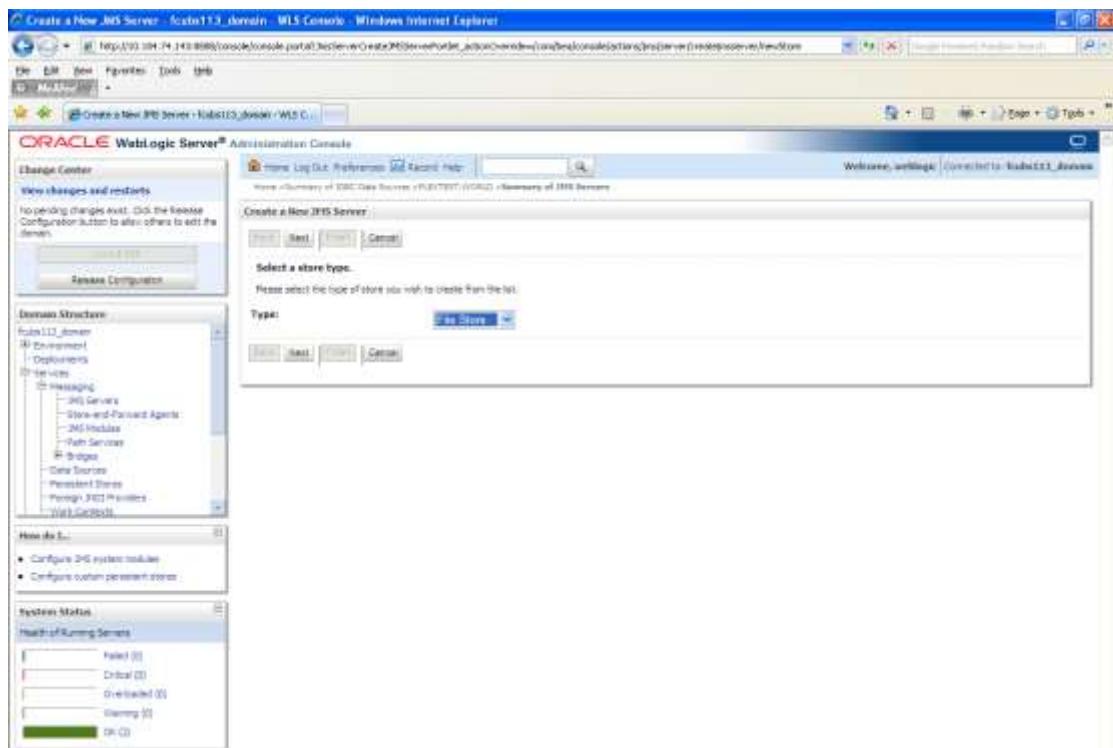


7. Specify the following details:

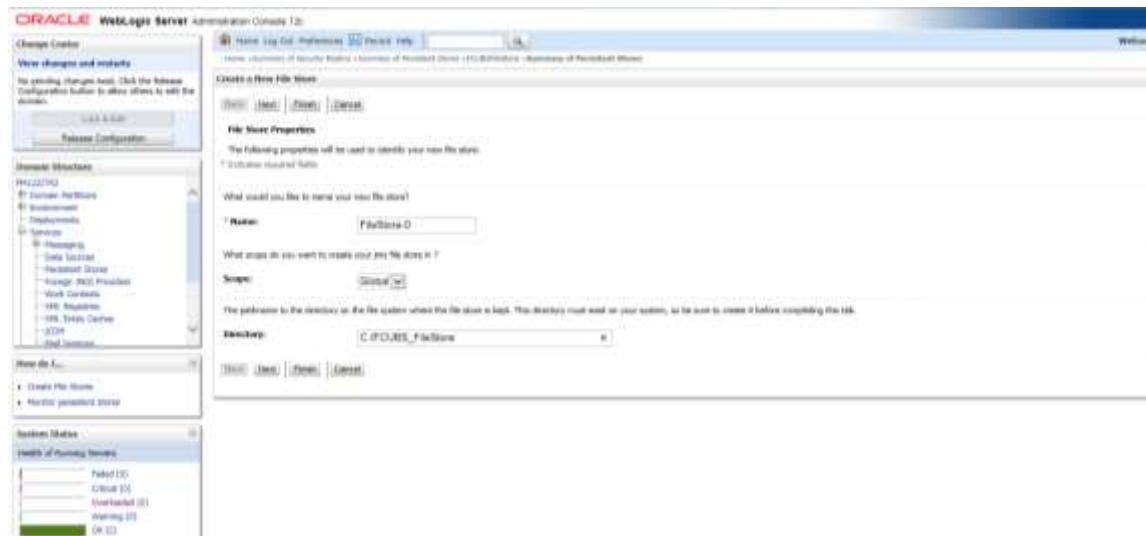
JMS Server Name	Specify the name of JMS Server.
-----------------	---------------------------------

8. Click 'Create a new Store' button. The following screen is displayed.

9. Select 'File Store' as the type and click 'Next'.



Following screen is displayed:

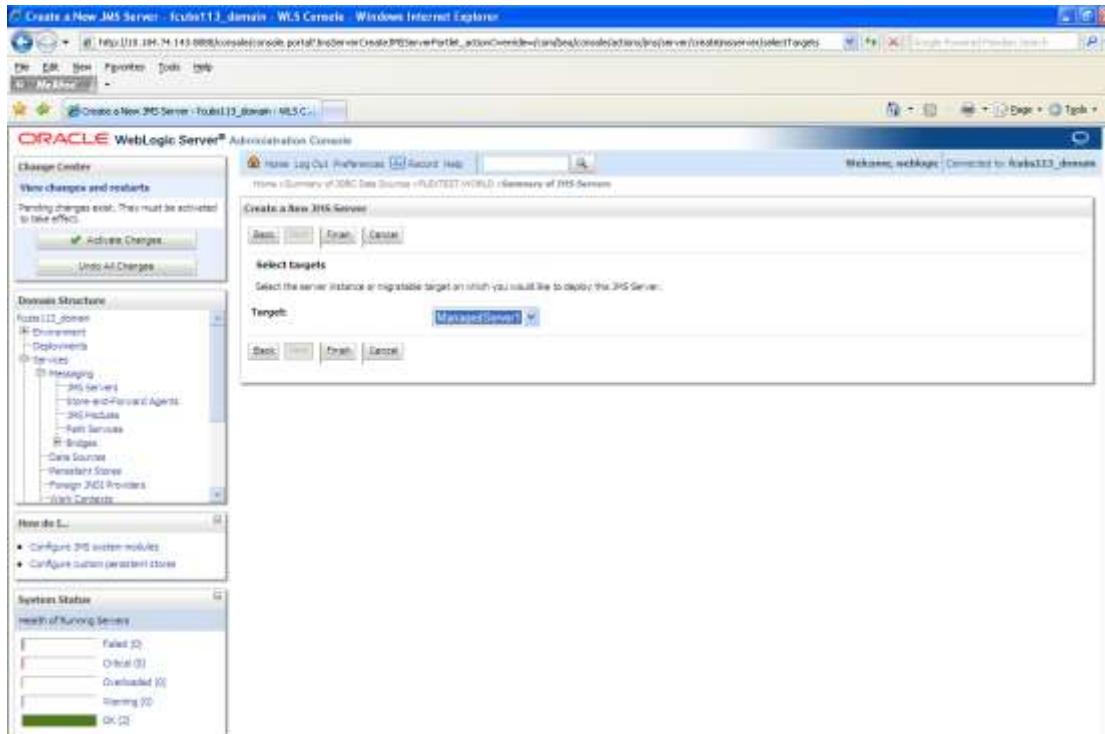
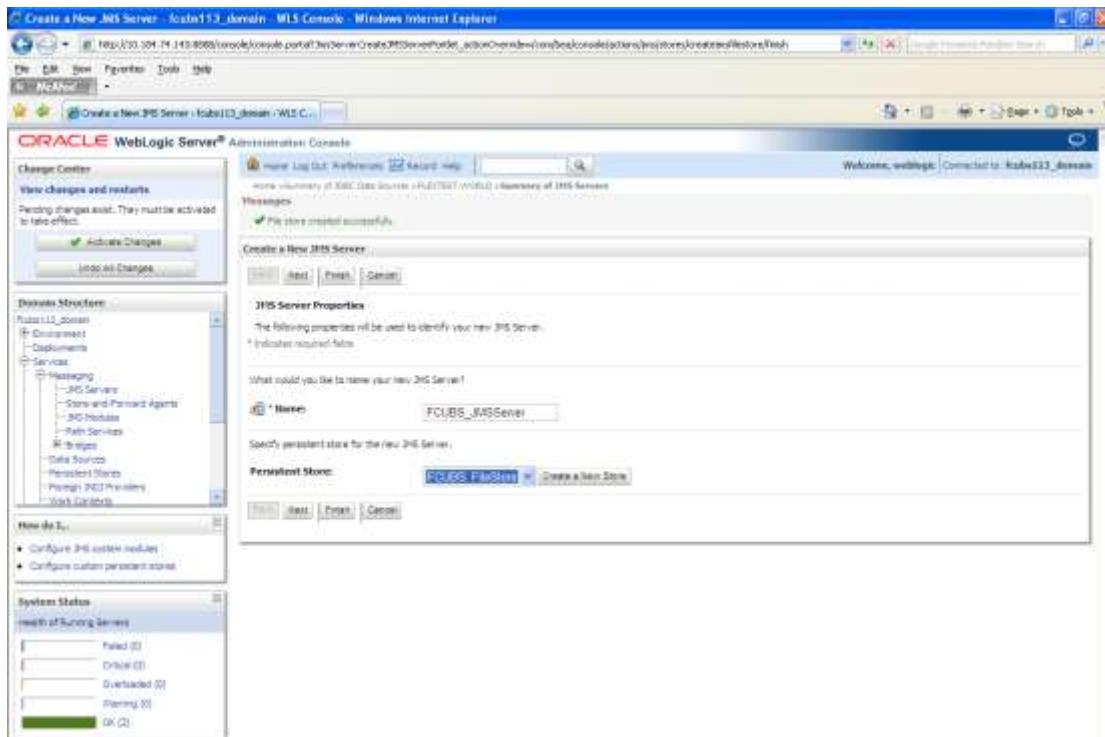


10. To identify the new File Store, specify the following properties:

- Specify the file store name as FCUBS_FileStore.
- Select a server. For this file store, you may select ManagedServer1 (created by the user).
- Specify the Filestore Directory path as C:/FCUBS_FileStore.
- Click 'OK'.

The following screen is displayed with message 'File store created successfully'.

11. Click 'Next'.



12. Select the target managed server. Click 'Finish'.

Name	Persistent Store	Target	Current Server	Health
WLSDJMServer	WLSD_PlistStore	ManagerServer1	ManagerServer2	OK (0)

13. The message 'JMS Server created successfully' is displayed.
14. Click 'Activate Changes' under Change Center. The message 'All changes have been activated. No restarts are necessary' is displayed.

7.2.3 JMS Modules Creation

Follow the steps given below:

1. Navigate to the WEBLOGIC Home Page. Click 'JMS Modules' on domain structure by expanding 'Messaging'.

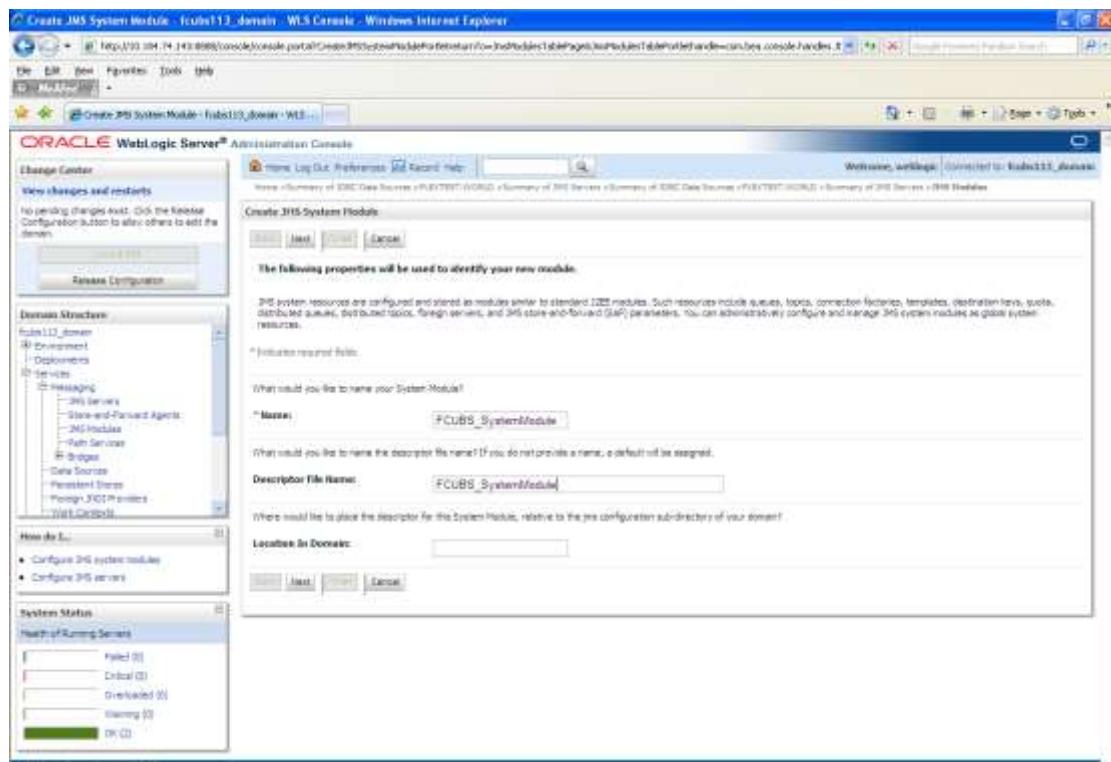
The following screen is displayed:

This screenshot shows the Oracle WebLogic Server Administration Console interface. The left sidebar displays a navigation tree with nodes like 'Domain Structure' (including 'Environment', 'Deployments', 'Services', 'Messaging' with 'JMS Services' and 'JMS Modules'), 'Data Sources', 'Ports', 'File Bridges', 'File Sources', 'Persistent Stores', 'Foreign JMS Providers', and 'Web Cache'. Below the tree are sections for 'How do I...' (with links to 'Configure JMS system modules' and 'Configure resources for JMS system modules') and 'System Status' (showing the 'Health of Running Servers' with four items: Failed (0), Critical (0), Overloaded (0), and Warning (0)). The main content area is titled 'JMS Modules' and contains a table with one row: 'Name: <empty>' and 'Type: <empty>'. A note below the table states 'There are no items to display.' At the bottom right of the table, there are 'Showing 0 to 0 of 0' and 'Previous | Next' buttons.

2. For creating New JMS System Modules, click 'Lock & Edit' button.

This screenshot shows the same Oracle WebLogic Server Administration Console interface as the previous one, but with a key difference: the 'Lock & Edit' button in the 'How do I...' section is now highlighted with a yellow background. The rest of the interface remains identical to the first screenshot, including the navigation tree, status bar, and the 'JMS Modules' table.

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

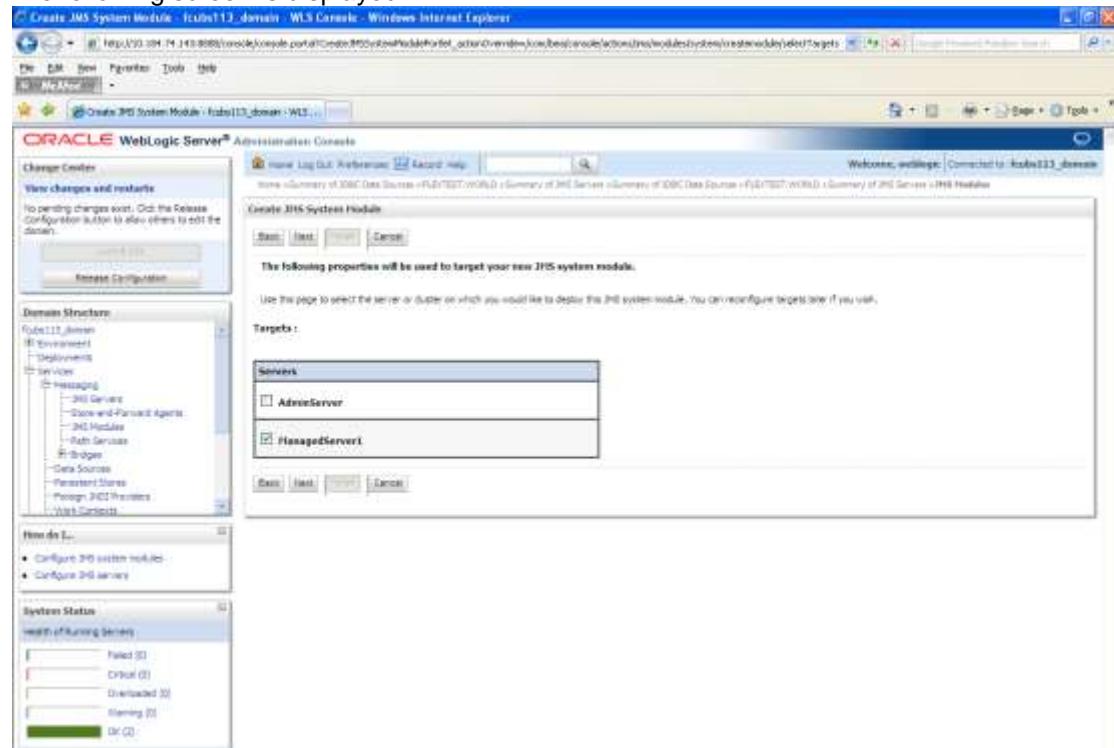


Enter the System Module Name as FCUBS_SystemModule.

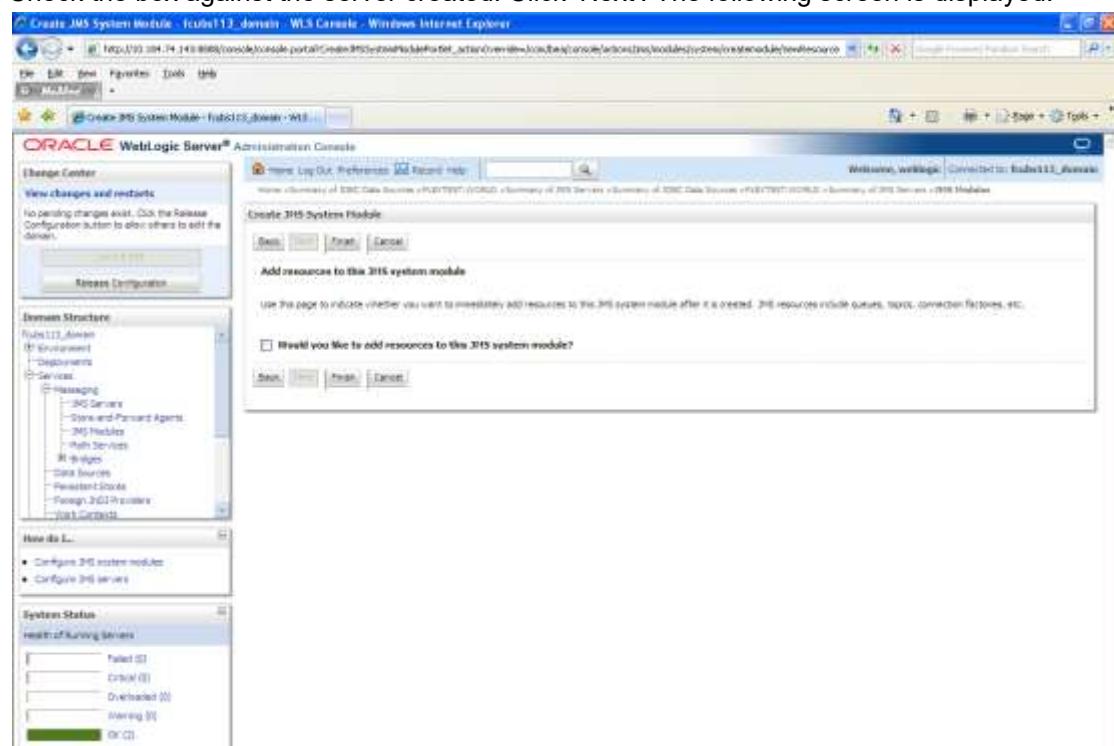
Enter the Description File Name as FCUBS_SystemModule.

4. Click 'Next'.

The following screen is displayed.



5. Check the box against the server created. Click 'Next'. The following screen is displayed.



- Click 'Finish' button. The following screen is displayed.

The JMS module has been created successfully.

Name	Type
Basic JMS	System
FCJMS_SystenModule	System

- Click 'Activate Changes' button on the left pane.

The message 'All the changes have been activated. No restarts are necessary' is displayed.

All changes have been activated. No restarts are necessary.

Name	Type
Basic JMS	System
FCJMS_SystenModule	System

7.2.4 Subdeployment Creation

Follow the steps given below:

1. Navigate to the WEBLOGIC Home Page. Click 'JMS Modules' on domain structure by expanding 'Messaging'.

The following screen is displayed:

The screenshot shows the Oracle WebLogic Server Administration Console interface. The title bar reads "JMS Modules - Fobit113_domain - WebLogic - Windows Internet Explorer". The left sidebar shows the "Domain Structure" with nodes like "Fobit113_domain", "Environment", "Deployments", and "Services". Under "Services", "Messaging" is expanded, showing "JMSServers", "JMS Modules", "JMSServices", "JMSSchemas", "Data Sources", "Persistent Stores", "Foreign JNDI Providers", and "JMSSystemModule". A "Release Changes" button is visible. The main content area is titled "JMS Modules" and contains a table with two rows:

Name	Type
Base JMS	Queue
PCJMS_SystemModule	Stream

Below the table, there are buttons for "Add", "Edit", and "Delete". On the right, there are links for "Previous" and "Next". The bottom left of the main area has a "Help" link. The bottom of the page shows the "Health of Running Services" status with categories: Failed (0), Critical (0), Deteriorated (0), Warning (0), and OK (1).

2. Click 'Lock & Edit' button.

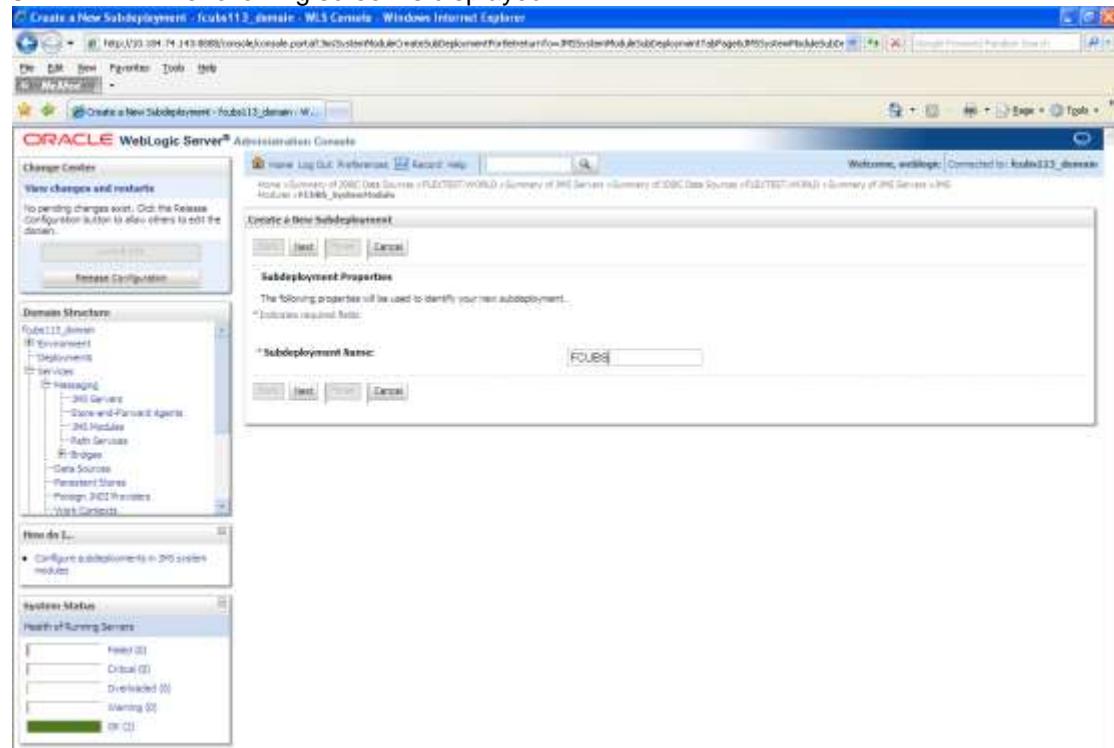
3. Select the JMS module created earlier.

The screenshot shows the Oracle WebLogic Server Administration Console. The title bar reads "Settings for FCUBS_SystemModule - fcub113_domain - WLS Console - Windows Internet Explorer". The main content area is titled "Settings for FCUBS_SystemModule". Below it, the "Configuration" tab is selected, showing a summary of the module's resources. A table titled "Summary of Resources" displays one item: "FCUBS_SystemModule" (Type: JMS Module). The left sidebar shows the domain structure under "Services" and a "How do I..." section with links for configuring JMS system modules. The bottom left shows the "System Status" with 0 failed servers.

4. Click 'Subdeployments' tab.

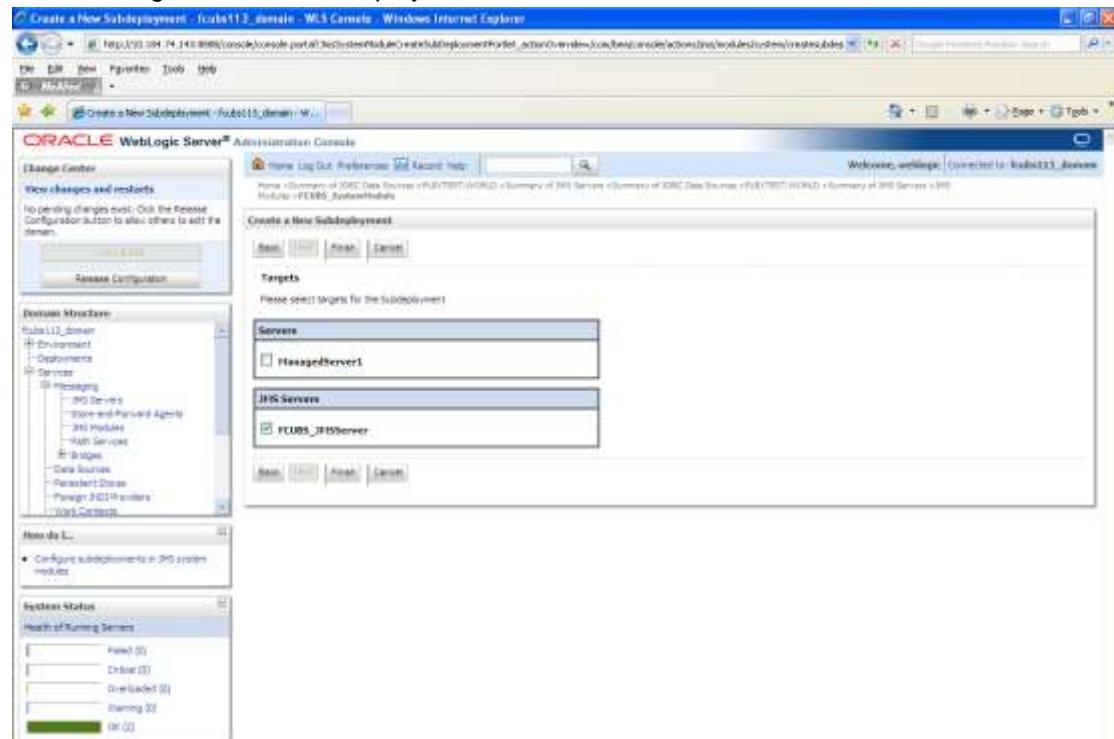
The screenshot shows the same Oracle WebLogic Server Administration Console interface, but the "Subdeployments" tab is now selected. This page is currently empty, displaying the message "There are no items to display". The left sidebar and bottom status bar remain the same as in the previous screenshot.

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



6. Specify the Subdeployment Name as 'FCUBS'. Then click 'Next'.

The following screen will be displayed.



7. Select the JMS Server (as created by the user).

- Click 'Finish' button.
- Following screen is displayed.

Subdeployments

Name	Resources	Targets
FCUBS		FCUBS_WebServer

- Click 'Activate Changes'. Following screen is displayed.

Subdeployments

Name	Resources	Targets
FCUBS		FCUBS_WebServer

7.2.5 JMS Queue Creation

1. Select the JMS Module created earlier.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The left sidebar displays the domain structure under 'Domain Structure' for 'FCUBS_domain'. The 'Messaging' section is expanded, showing 'JMS Servers', 'Store-and-Forward Agents', 'JMS Modules', 'Path Services', 'IP Bridges', 'Data Sources', 'Persistent Stores', 'Inbound JMS Providers', and 'Java Cache'. A 'How do I...' panel on the right provides links for 'Configure JMS system module', 'Configure subdeployment in JMS system module', and 'Configure resources for JMS system module'. The main content area is titled 'Settings for FCUBS_SystemModule' and shows the 'Configuration' tab selected. It displays general information about the JMS system module, including its name ('FCUBS_SystemModule'), descriptor file ('jms/FCUBS_SystemModule-jms.xml'), and a summary of resources. A table below lists resources, showing one entry: 'There are no items to display.' The bottom right corner of the table indicates 'Showing 0 to 0 of 0'.

2. You need to set the configuration for FCUBS_SystemModule is to be set.
3. Click 'Configuration'. Then click 'Lock & Edit'.

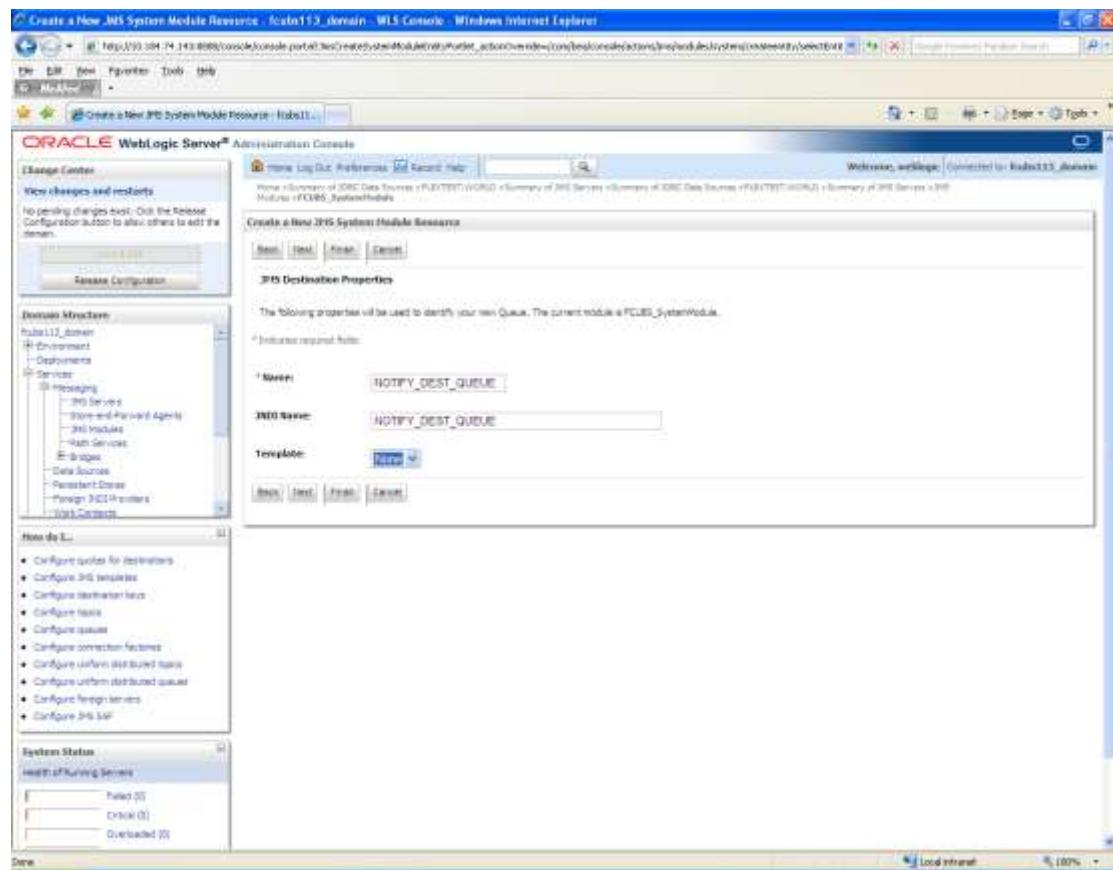
The Following screen is displayed.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The title bar reads "Settings for FCUBS_SystemModule - fcub112.domain - WLS Console - Windows Internet Explorer". The main content area is titled "Settings for FCUBS_SystemModule". It includes tabs for Configuration, Subenvironments, Targets, Security, and Help. The Configuration tab is selected. A sidebar on the left shows the "Domain Structure" with nodes like "fcub112.domain", "Environment", "Deployments", and "Services". Under Services, "Messaging" is expanded to show "JMS Servers", "Store-and-Foreward Agents", "JMSS Modules", "Auth Services", "Bridges", "Data Sources", "Persistent Stores", "Foreign JNDI Bindings", and "JMSS Connectors". A "How do I..." section provides links for configuring JMS system modules, subenvironments, and resources. The right side of the screen displays a "Summary of Resources" table with columns: Name, Type, JMS Status, Subdeployment, and Targets. The table is currently empty, showing the message "There are no items to display." Below the table, there are two buttons: "New" and "Delete". Navigation links at the bottom right say "Showing 1 to 0 of 0 | Previous | Next".

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

The screenshot shows the Oracle WebLogic Server Administration Console interface. The main title bar reads "Create a New JMS System Module Resource - Rols112_domain - WLSC Console - Windows Internet Explorer". Below the title bar, the URL is "http://192.168.14.143:8080/console/console.portal?_nfpb=true&_pageLabel=InstCreateSystemModule&_id=instCreateInstModuleUtilityForCurrentModule#JMS_Syst...". The left sidebar contains a "Domain Structure" tree with nodes like "Rols112_domain", "Environment", "Deployments", "Services", "Messaging", "JMS Servers", "Store-and-Foreward Agents", "JMS Modules", "Auth Services", "Browsers", "Data Sources", "Persistent Stores", "Foreign JMS Providers", and "Web Contexts". A "How do I..." section lists various configuration steps. The central panel is titled "Create a New JMS System Module Resource" and has tabs for "Basic", "Test", and "Details". The "Basic" tab is selected. It displays a list of resource types with "Queue" being the selected option. To the right of the selected option, there is a detailed description: "Defines a point-to-point destination topic, which are used for synchronous user communications. A message delivered to a queue is distributed to all topic consumers." Below this, there are "More Info..." links for each resource type. The bottom right corner of the window shows "Load Intranet" and "100%".

5. Select the 'Queue' option. Then click 'Next'.



For creating new JMS System Module Resources, follow the steps given below:

- Enter the Name of the Queue as 'NOTIFY_DEST_QUEUE'.
- Enter the JNDI Name as 'NOTIFY_DEST_QUEUE'.
- Select the Template as 'None'.
- Click 'Next'.

Following screen is displayed.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The title bar reads "Create a New JMS System Module Resource - Robust - WLSC Console - Windows Internet Explorer". The main content area is titled "Create a New JMS System Module Resource". It displays a summary of the properties being used to target the new JMS system module resource, specifically targeting the "FCU09_JMServer" subdeployment under the "FCU09" server. On the left, there is a navigation tree showing the domain structure, including Services > Messaging > JMS Servers. A sidebar on the left lists "How do I..." with various configuration options like "Configure quota for resources" and "Configure JMS targets". At the bottom, there is a "System Status" section showing the health of running servers. The status table has three rows: "Failed (0)", "Ok (0)", and "Overloaded (0)".

6. Select the managed server created by the user. Click 'Finish' button.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The title bar indicates the session is for 'Settings for FCUBS_SystemModule - host113_domain - WLS Console - Windows Internet Explorer'. The left sidebar shows the 'Domain Structure' for 'host113_domain' under 'JMS System Modules'. The main content area is titled 'Configuration' for 'FCUBS_SystemModule'. It displays general information about the module, including its name ('FCUBS_SystemModule'), description file ('jms/FCUBS_SystemModule/jms.xml'), and a summary of JMS resources. A table lists a single resource: 'HTTP_DEST_QUEUE' (Type: Queue, JNDI Name: 'HTTP_DEST_QUEUE', Subdeployment: 'FOSS', Target: 'FC_B2_JMServer'). The bottom section shows the 'System Status' with all services marked as 'Ok'.

Name	Type	JNDI Name	Subdeployment	Targets
HTTP_DEST_QUEUE	Queue	HTTP_DEST_QUEUE	FOSS	FC_B2_JMServer

7. The JMS Queue has been created successfully. Click 'Activate Changes' under 'Change Center'.

Name	Type	Subdeployment	Targets
HOSTED_DEBT_QUEUE	Queue	PCUES	PCUES_Instances

8. Click 'New' to create more Queues. You may follow the same steps to create other queues.

7.2.6 JMS Connection Factory Creation

After creating the queues, you need to create the connection factory. To perform this, follow the steps given below:

1. Click 'New'.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The title bar indicates the session is for 'Settings for FCUBS_SystemModule - fcub113_domain'. The main content area is titled 'Settings for FCUBS_SystemModule' under the 'Configuration' tab. On the left, there's a navigation tree for the domain structure, including Environment, Deployments, and Services (with sub-options like Messaging, JMS Servers, JMS Modules, JMS Bridges, Data Sources, Persistence Stores, and Foreign JNDI Lookups). A 'How do I...' section provides links for configuring JMS system modules, JMS destinations, and resources. The right side displays a table titled 'Summary of Resources' with one entry: 'HTTP_DEST_QUEUE' (Type: Queue, SubDeployment: FCUBS, Targets: FCUBS_MQServer). The status bar at the bottom shows 'Showing 1 to 1 of 1 | Previous | Next'.

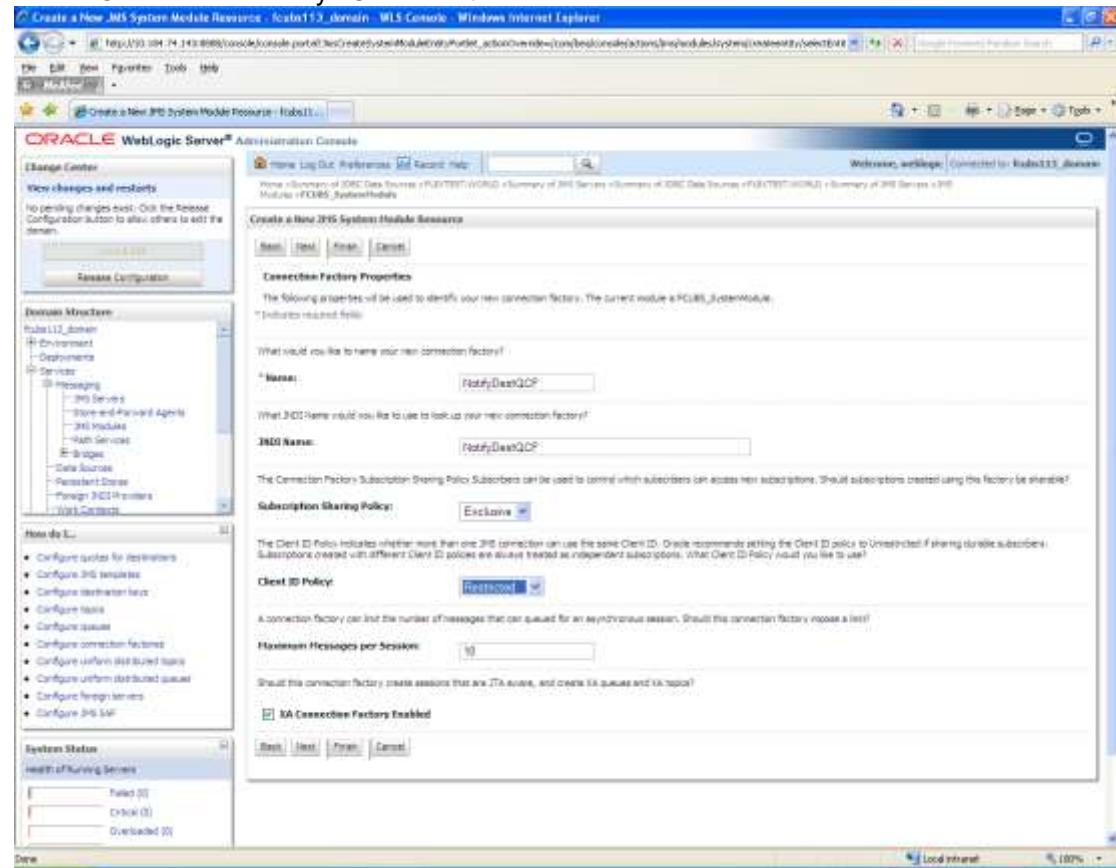
The following screen is displayed:

The screenshot shows the Oracle WebLogic Server Administration Console interface. The title bar reads "Create a New JMS System Module Resource - Robust... - Windows Internet Explorer". The main content area is titled "Create a New JMS System Module Resource". It displays a list of resource types to choose from, each with a brief description and a "More Info..." link. The visible options include:

- Connection Factory**: Defines a list of connection configuration parameters that are used to create connectors for JMS clients. [More Info...](#)
- Queue**: Defines a point-to-point destination topic, which are used for unidirectional user communications. A message delivered to a queue is distributed to all consumers. [More Info...](#)
- Topic**: Defines a publish-subscribe destination type, which are used for asynchronous user communications. A message delivered to a topic is distributed to all consumers. [More Info...](#)
- Distributed Queue**: Defines a list of queues that are distributed on multiple JMS servers, but which are accessible on a single, logical queue to JMS clients. [More Info...](#)
- Distributed Topic**: Defines a list of topics that are distributed on multiple JMS servers, but which are accessible as a single, logical topic to JMS clients. [More Info...](#)
- Foreign Server**: Defines foreign messaging providers or remote WebLogic Server instances that are not part of the current domain. [More Info...](#)
- Quota**: Controls the amount of system resources available to destinations. [More Info...](#)
- Destination Sort Key**: Defines a unique sort order that destinations can apply to arriving messages. [More Info...](#)
- JMS Template**: Defines a set of default configuration settings for multiple destinations. [More Info...](#)
- SAP Imported Destinations**: Defines a collection of imported store-and-forward (SAF) destinations. A SAF destination is a representation of a queue or topic in a remote server instance or cluster that is imported into the local cluster or server instance, so that the local server instance or cluster can send messages to the remote server instance or cluster. [More Info...](#)

On the left side, there is a sidebar with sections like "Domain Structure" (Robust12_domain), "How do I...", and "System Status". The "How do I..." section lists various configuration steps such as "Configure quota for destinations", "Configure JMS template", etc.

- Select 'Connection Factory'. Click 'Next'.



- Enter the Name of the Connection Factory as 'NotifyDestQCF'.
- Enter the JNDI Name as 'NotifyDestQCF'.
- Check the box 'XA Connection Factory Enabled'.
- Click 'Next'.

The following screen is displayed:

The screenshot shows the Oracle WebLogic Server Administration Console interface. The title bar reads "Create a New JMS System Module Resource - Admin113_domain - WebLogic Console - Microsoft Internet Explorer". The main content area is titled "Create a New JMS System Module Resource - Admin113...". On the left, there's a navigation tree under "Remote Structure" with nodes like "Admin Server", "Deployment", "Services", "Messaging", "Data Sources", "Resource Issues", "Foreign JNDI Providers", and "JMS Connectors". A context menu is open over the "Messaging" node with options such as "Configure queues for destination", "Configure JMS resources", "Configure destination topics", "Configure basic", "Configure queues", "Configure connector factories", "Configure uniform distributed topics", "Configure uniform distributed queues", "Configure foreign topic", and "Configure JMS SAT". Below the navigation tree, there's a "System Status" section showing "Health of Running Servers" with three entries: "Presto (0)", "Citrine (0)", and "Overlander (0)". The central panel displays the "Create a New JMS System Module Resource" dialog. It has tabs for "Basic", "Advanced Targeting", and "General". Under "Basic", it says "The following JMS module targets will be used to target your new JMS system module resource." and "Targets: ManagedServer1". At the bottom of the dialog, there are "Next Step" and "Cancel" buttons.

7. Click 'Advanced Targeting'. The following screen is displayed.

The screenshot shows the Oracle WebLogic Server Administration Console. The title bar reads "Create a New JMS System Module Resource - Admin113_domain - WebLogic Server - Microsoft Internet Explorer". The main content area is titled "Create a New JMS System Module Resource". A sidebar on the left lists various system components like JMS Servers, JMS Modules, and JMS Resources. The main panel has tabs for "Basic", "Advanced", and "Custom". The "Advanced" tab is selected. A note says "The following properties will be used to target your new JMS system module resource". Below this, it says "Select the subdeployment you want to use. If you select [None], no targeting will occur." A dropdown menu under "Subdeployments" shows "FCUBS" selected. A note below says "What targets do you want to assign to this subdeployment?" Under "Targets", there are two sections: "Servers" and "JMS Servers". In the "Servers" section, "ManagedServer1" is listed with an unchecked checkbox. In the "JMS Servers" section, "FCUBS_JMServer" is listed with a checked checkbox. At the bottom are "Edit", "Next", and "Cancel" buttons.

8. Select the 'Subdeployments' as FCUBS.
9. Under JMS Servers, check the box against 'Managed Server'.

10. Click 'Finish'. The following screen is displayed:

Name	Type	Queue Name	Subdeployment	Targets
NotifyDestQCF	Connection Factory	notifyDestQCF	FCUBS	FCUBS_Receiver
NOTIFY_DEST_QUEUE	Queue	NOTIFY_DEST_QUEUE	FCUBS	FCUBS_Receiver

11. The message 'Connection Factory created successfully' is displayed.
 12. Click on the Connection Factory 'NotifyDestQCF' to have XA Connection Factory enabled.

The following screen will be displayed.

This screenshot shows the Oracle WebLogic Server Administration Console. The URL in the address bar is `http://10.104.74.143:8080/console/console.portal?_nfpb=true&pagelet=JMSConnectionFactoryGeneralTab&pageHandle=consolehandles_#0&handle%28%22com.bea.console.handles_#0%29`. The title bar says "Settings for NotifyDestJCF - fcafb113_domain - WLS Console - Windows Internet Explorer". The left sidebar shows a "Domain Structure" tree with nodes like "fcafb113_domain", "Environment", "Deployments", "Services", and "Messaging". Under "Messaging", there are sub-nodes: "JMS Servers", "Store and Forward Agents", "JMS Modules", "Path Services", "Bridges", "Data Sources", "Persistent Stores", "Foreign JNDI Providers", and "Web Contracts". A "How do I..." section provides links for "Configure connection factories". The main content area is titled "Settings for NotifyDestJCF" and has tabs for "Configuration", "Deployment", and "Notes". The "Configuration" tab is selected, showing sub-tabs for "General", "Default Delivery", "Client", "Transactions", "Row Control", "Load Balance", and "Security". The "General" sub-tab is active, displaying fields for "Name" (set to "NotifyDestJCF") and "JNDI Name" (set to "NotifyDestJCF"). There is also a checkbox for "Default Targeting Enabled". Below these fields is an "Advanced" section with a "Save" button. The right side of the screen shows a "Welcome, weblogic" message and a "Connected to: fcafb113_domain" status bar.

13. Click 'Transactions' Tab. The following screen is displayed.

This screenshot shows the same Oracle WebLogic Server Administration Console interface, but the "Transactions" tab is now selected under the "Configuration" tab of the "NotifyDestJCF" settings. The URL in the address bar remains the same: `http://10.104.74.143:8080/console/console.portal?_nfpb=true&pagelet=JMSConnectionFactoryGeneralTab&pageHandle=consolehandles_#0&handle%28%22com.bea.console.handles_#0%29`. The left sidebar and general layout are identical to the previous screenshot. The main content area now displays the "Transactions" configuration for the JMS connection factory. It includes fields for "Transaction Timeout" (set to 3600) and a checkbox for "XA Connection Factory Enabled". Below these fields is an "Advanced" section with a "Save" button. The right side of the screen shows the same "Welcome, weblogic" message and "Connected to: fcafb113_domain" status bar.

14. Check the box 'XA Connection Factory Enabled'.

15. Click 'Save'. The following screen is displayed.

The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar shows the domain structure under 'NotifiyDestJCF' and a 'System Status' section with a green bar indicating all servers are running. The main panel is titled 'Settings for NotifiyDestJCF' and has tabs for Configuration, Subdeployment, Notes, General, Default Delivery, Client, Transactions, Flow Control, Load Balance, and Security. The 'Transactions' tab is selected. It contains fields for 'Transaction Timeout' (set to 3600) and a checkbox for 'XA Connection Factory Enabled' which is checked. A message below the checkbox states: 'Indicates whether a XA queue or XA topic connection factory is returned, instead of a queue or topic connection factory. An XA connection factory can be used to create an XAResource, which in turn may be used to create an XATransaction, which in turn may be used to obtain an XAResource for use inside a transaction manager...'. At the bottom is a 'Save' button.

16. The message 'Settings updated successfully' is displayed.

17. Click 'Activate Changes' button under 'Change Center'.

The message 'All the changes have been activated. No restarts are necessary' is displayed.

This screenshot shows the 'Change Center' page of the Oracle WebLogic Server Administration Console. A message at the top says 'All changes have been activated. No restarts are necessary.' Below this, a note says 'Click the 'Save & Exit' button in the Change Center to modify the settings on this page.' To the right, the 'Transactions' configuration screen for the 'NotifiyDestJCF' connection factory is shown, identical to the one in the previous screenshot. The 'XA Connection Factory Enabled' checkbox is checked, and the message below it is visible. The left sidebar shows the domain structure and system status.

7.3 Configuring Weblogic for PMGateway

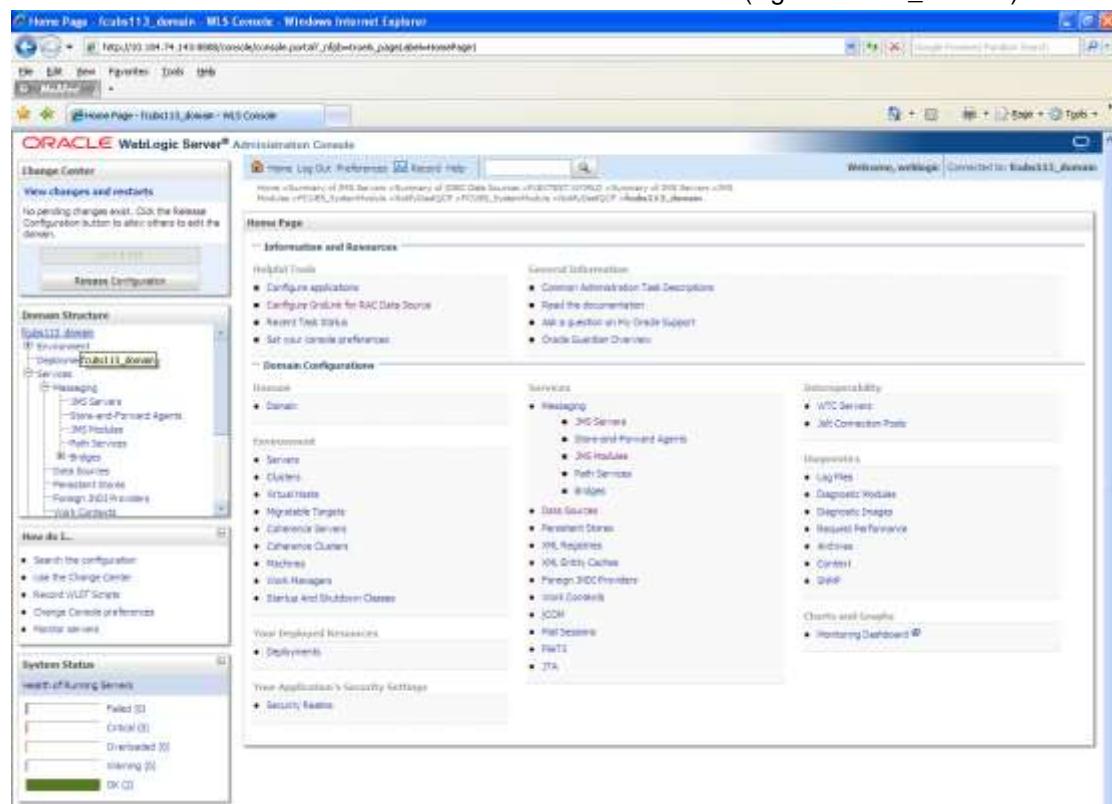
To deploy and run PMGateway application in weblogic server following configuration needs to be done

Copy runtime12.jar from database servers ORACLE_HOME/sqlj/lib to application servers library path WEBLOGIC_HOME/user_projects/domains/<app-domain>/lib

7.4 Configuring Weblogic for Oracle FLEXCUBE

This section explains the steps for configuring Oracle WebLogic application server for Oracle FLEXCUBE. Follow the steps given below:

1. Select the domain from the domain structure as shown below. (Eg: fcubs113_domain).



The following screen is displayed:

Settings for tobacco13.domain /tobacco13.domain - WebLogic - Microsoft Internet Explorer

File Edit View Favorites Book Help

ORACLE WebLogic Server® Administration Console

Change Center

View changes and restarts

No pending changes exist. Click the 'Restart' button to allow changes to take effect.

Configuration button to allow changes to edit this domain.

Logout Preferences Recent Help

Welcome, weblogic | Connect to: tobacco13.domain

Settings for tobacco13.domain

Configuration | Monitoring | Control | Security | Web Service Security | Home

General | JTA | JDB | Web Applications | Logging | Log Files

General

A domain is a collection of WebLogic Server instances that is managed by a single Administration Server. Use the tabs to configure administrative options that apply to all servers in the current domain.

* indicates required field

Name: tobacco13.domain

✓ Enable Administration Port.

Administration Mode: true

Production Mode: true

✓ Enable Oracle Coherence Optimizations

✓ Enable Cluster Constraints

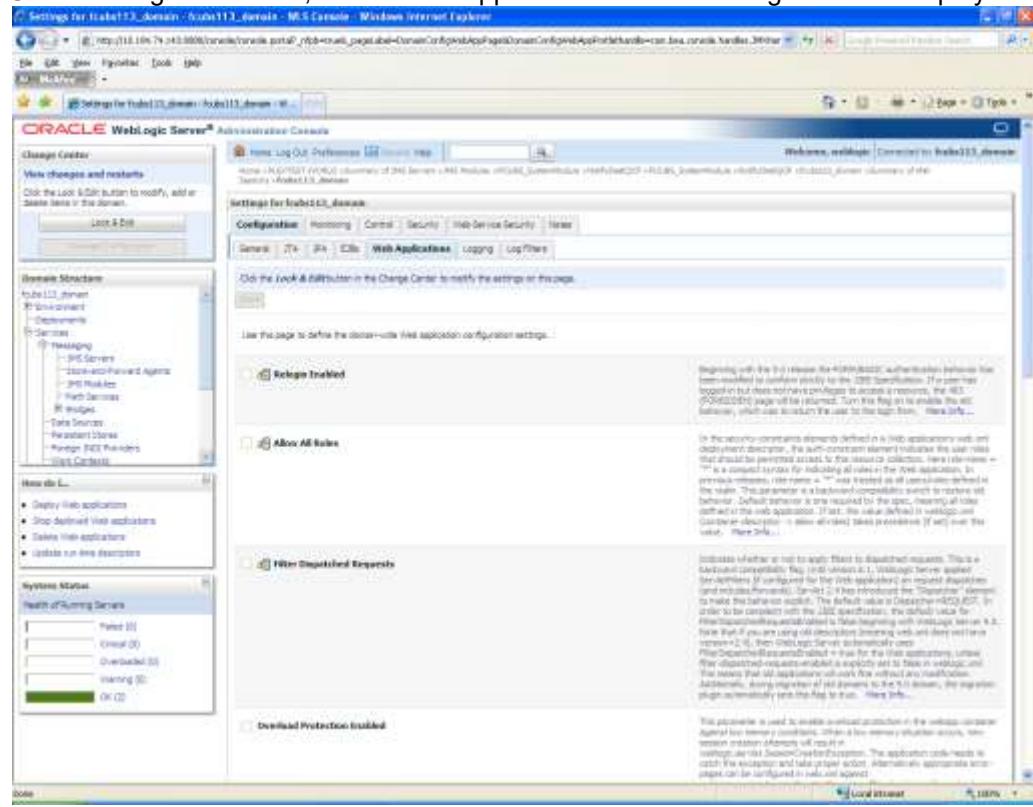
✓ Enable on-demand deployment of internal applications

✓ Enable Oracle GridLink Agent

Advanced

Last Update: 7/10/2013 10:45:00 AM

2. Under 'configuration' tab ,Select 'Web Applications'. The following screen is displayed.



3. Scroll down and ensure that the details are as shown in the figure. The remaining portion of the screen is given below:

Settings for fob113_domain - fob113_domain - MJS Console - Windows Internet Explorer

File Edit View Favorites Date Help

Settings for fob113_domain - fob113_domain - MJS Console

HTTP Trace Support Enabled

Specifies the value of the `httpTraceSupportEnabled`. [More Info...](#)

WebLogic Plugin Enabled

Specifies whether or not the proprietary WL-Proxy-Client header should be honored. (This is needed only when WebLogic plugins are configured.) [More Info...](#)

Auth Cookie Enabled

Whether automatic features are enabled or not. [More Info...](#)

Change Session ID On Authentication

Allows property to determine if we need to generate a new session ID after authentication. When this property set to "false", the previous session ID will be retained even after authentication. [More Info...](#)

WAP Enabled

Indicates whether the response should include WML information. (Checking this box may be necessary when using URLs containing short URLs because they limit the size of the URL to 256 characters, and may also affect the use of redirect statements in a location.) When this box is selected, the output size of the URL is limited to 256 characters, and it will not contain any special characters. [More Info...](#)

Post Timeout:

The amount of time the server waits between receiving chunks of data in an HTTP POST data before it times out. (This is used to prevent denial-of-service attacks that attempt to exhaust the server with POST data.) [More Info...](#)

Maximum Post Time:

Max Post Time (in seconds) for reading HTTP POST data in a certain request. MaxPostTime < 0 means unlimited. [More Info...](#)

Maximum Post Size:

The maximum post size this server allows for reading HTTP POST data in a certain request. A value less than 0 implies an unlimited size. [More Info...](#)

Work Context Propagation Enabled

Indicates whether or not `workContextPropagation` is enabled. By default it is turned on. There is a little overhead involved in propagating WebContext. Therefore, if you are certain that you don't need it, turn the value off to produce better performance. [More Info...](#)

CSP Header Value:

Defines the CSP header value that will be sent with all responses for HTTP requests (if non-null). The value of this header points to the location of the policy/resource file for the static site. [More Info...](#)

JSP Compiler Backwards Compatible

Allows property to determine the behavior of the JSP compiler. When this property set to "true", the JSP compiler throws a compilation error for JSPs that do not conform to the JSP 2.1 specification. This property exists for backward compatibility. [More Info...](#)

Archived Real Path Enabled

Allows property to determine the behavior of `getArchivedPath` for Archived resources. When this property set to "true", `getArchivedPath` will return the canonical path of the resource file. [More Info...](#)

Save

The screenshot shows the 'Settings' page for a domain in the Oracle WebLogic Server Administration Console. The page lists several configuration options with their current status and brief descriptions:

- Http Trace Support Enabled:** Unchecked. Returns the value of `HttpTraceSupportEnabled`. [More Info...](#)
- Weblogic Plugin Enabled:** Unchecked. Specifies whether or not the proprietary `WL-Plugin-Client-ID` header should be honored. (This is needed only when Weblogic plugins are configured.) [More Info...](#)
- Auth Cookie Enabled:** Checked. Whether authcookie feature is enabled or not. [More Info...](#)
- Change Session ID On Authentication:** Checked. Global property to determine if we need to generate a new `SessionID` after authentication. When this property set to "true", the previous `SessionID` will be returned even after authentication. [More Info...](#)
- WAP Enabled:** Unchecked. Indicates whether the session ID should include WAP information. (Checking this box may be necessary when using WAP, especially with WAP devices that limit the size of the URL to 128 characters, and may also affect the use of replaced sessions in a cluster.) When this box is selected, the default size of the URL will be set at 52 characters, and it will not contain any special characters. [More Info...](#)
- Post Timeout:** 30. The amount of time the server waits between receiving chunks of data in an HTTP POST data before it times out. (This is used to prevent denial-of-service attacks that attempt to overload the server with POST data.) [More Info...](#)
- Maximum Post Time:** -1. Max Post Time (in seconds) for reading HTTP POST data in a servlet request. MaxPostTime < 0 means unlimited. [More Info...](#)
- Maximum Post Size:** -1. The maximum post size this server allows for reading HTTP POST data in a servlet request. A value less than 0 indicates an unlimited size. [More Info...](#)
- Work Context Propagation Enabled:** Checked. Indicates whether or not `WorkContextPropagation` is enabled, by default it is turned on. There is a little overhead involved in propagating WorkContexts. Therefore, if you don't care about workContext propagation, turn the value off in production environments. [More Info...](#)
- HTTP Header Value:** [empty input field]. Returns the HTTP Header value that will be sent with all responses for http requests of non null. The value of this header points to the location of the policy reference file for the web site. [More Info...](#)
- JSP Compiler Backwards Compatible:** Checked. Global property to determine the behavior of the JSP compiler. When this property set to "true", the JSP compiler throws a translation error for JSPs that do not conform to the JSP 2.0 specification. This property exists for backward compatibility. [More Info...](#)
- Archived Real Path Enabled:** Checked. Global property to determine the behavior of `getRealPath()` for archived web applications. When the property set to "true", `getRealPath()` will return the canonical path of the resource files. [More Info...](#)

A 'Save' button is located at the bottom of the form.

4. Check the options 'JSP Compiler Backwards Compatible' and 'Archived Real Path Enabled'.
5. Click 'Save'.

6. The following screen is displayed:

7. Ensure that the message 'Settings are updated successfully' is displayed.
8. Click the button 'Active Changes'.

7.5 Setup/Configure Mail Session in Weblogic

This section describes the set of configurations changes required in Oracle Weblogic Server when Oracle FLEXCUBE UBS is configured to generate and send passwords to users via e-mail.

7.5.1 Creating JavaMail Session

To configure mail session, follow the steps below.

1. Expand 'Services' on the left pane of the application server. Click 'Mail Sessions'.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The left sidebar has a tree view under 'Domain Structure' with nodes like 'Messaging', 'Data Sources', and 'Mail Sessions'. The 'Mail Sessions' node is expanded. Below it is a 'How do I...' section with links for 'Configure access to JMS', 'Target mail sessions', and 'Delete mail sessions'. To the right is a table titled 'Summary of Mail Sessions' with the message 'There are no items to display.'

2. Click 'Lock & Edit'.

This screenshot is identical to the previous one, showing the 'Summary of Mail Sessions' page. The difference is that the 'LOCK & EDIT' button has been clicked, which has caused the page to refresh and show the same message again: 'There are no items to display.'

3. Following screen is displayed; Click 'New' for creating a new session.

4. Following screen is displayed.

5. Specify the required details to create a session. Sample details are given below:

Name

FCUBSMailSession

JNDI Name

mail/FCUBSMail



This JNDI name needs to be maintained in fcubs.properties file with encrypted format.

Java Mail Properties

mail.host=<HOST_MAIL_SERVER>

Eg: samplename.mail.com

mail.smtps.port=<SMTPS_SERVER_PORT>

Eg: 1010

mail.transport.protocol=<MAIL_TRANSFER_PROTOCOL>

Eg: smtps

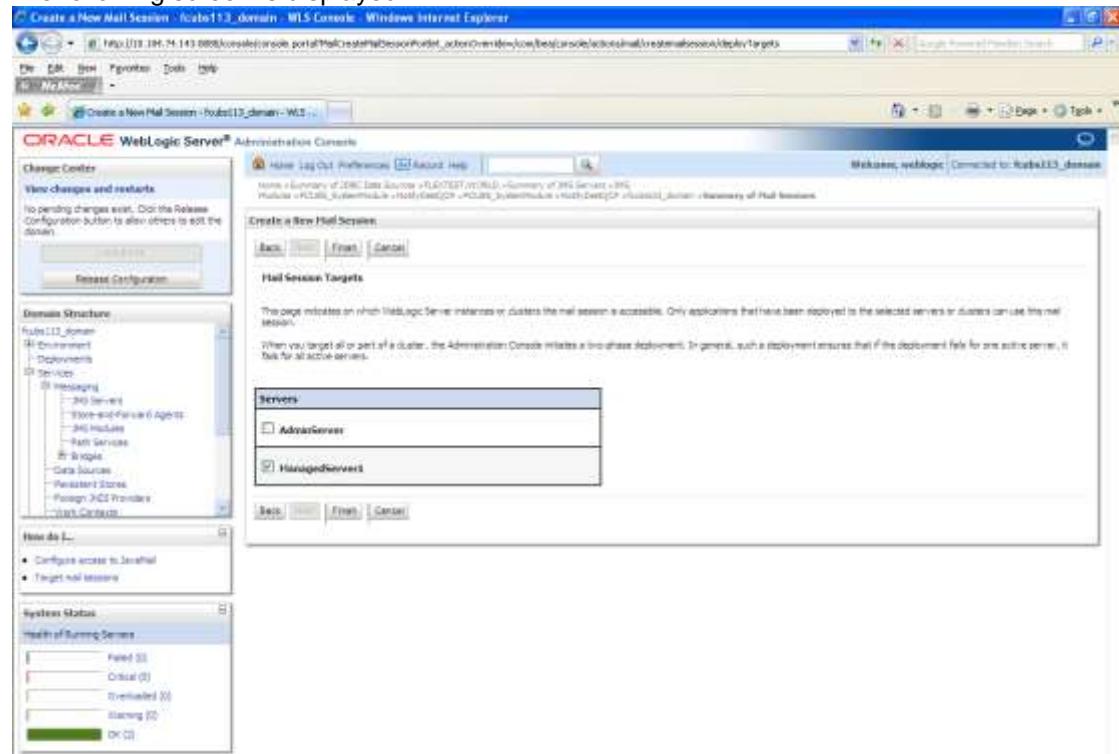
mail.smtps.auth=true

mail.smtps.host=<HOST_SMTPS_MAIL_SERVER>

Eg: samplename.mail.com

6. Click 'Next'.

The following screen is displayed.



7. Check the box against the required servers and click 'Finish' to complete the configuration.



'fcubs.properties' file needs to be updated with the encrypted values of

- o SMTP_HOST
- o SMTP_USER
- o SMTP_PASSWORD
- o SMTP_JNDI

This can be achieved using the Oracle FLEXCUBE UBS Installer.

- Click 'Active Changes' button to activate the current mail session settings.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The left sidebar has a tree view under 'Domain Structure' with nodes like 'Messaging', 'JMS', 'Web Services', and 'Mail Sessions'. A context menu is open over the 'Mail Sessions' node with options: 'Configure access to JMSMail', 'Target mail sessions', and 'Delete mail sessions'. The main content area is titled 'Summary of Mail Sessions' and contains a table with one row:

Name	Properties	JNDI Name
FCL20MailSession	mail.amps.auth=true;mail.amps.port=25;mail.amps.host=elba.amps.oracle.com;mail.amps.debug=true;mail.host=elba.amps.oracle.com	mail/JMSMail

7.5.2 Configuration of the TLS/SSL Trust Store for Weblogic Server

As described in the previous section, Oracle FLEXCUBE UBS uses SMTPS to send outgoing mails. SMTPS uses SSL to ensure transport-level security of the mail messages and hence, the certificate of the mail server needs to be imported into the trust store(s) of the Managed Servers where Oracle FLEXCUBE UBS is deployed.

The certificate of the mail server needs to be specifically imported into the trust store configured for the Managed Server(s), as configured in the Oracle FLEXCUBE UBS Installation guide titled 'SSL Configuration On Weblogic' (SSL_Configuration).

For further details on importing the certificate of the mail server into the trust store, refer to the documentation for the Sun Java keytool utility (Key and Certificate Management tool).



Weblogic Configuration
[May] [2020]
Version 14.4.0.0.0

Oracle Financial Services Software Limited
Oracle Park
Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India

Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax: +91 22 6718 3001
<https://www.oracle.com/industries/financial-services/index.html>

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

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

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

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

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

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

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