Oracle® Banking Trade Finance

Weblogic Configuration

Release 14.8.0.0.0
G29256-01
April 2025

Oracle Banking Trade Finance Weblogic Configuration, Release 14.8.0.0.0

G29256-01

Copyright © 2007, 2025, Oracle and/or its affiliates.

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.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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 fail-safe, 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.

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

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Purpose v
Audience v
Documentation Accessibility v
Critical Patches v
Diversity and Inclusion v
Conventions vi
Related Resources vi
Screenshot Disclaimer vi

1 CONFIGURING SSL ON ORACLE WEBLOGIC

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 Introduction 2-1

3 OBTAINING THE IDENTITY STORE

3.1 Creating Identity Store with Self-Signed Certificates 3-1
3.1.1 Creation of Self-signed Certificate 3-1
3.2 Topic 3-3
3.2.1 Topic 3-3
3.2.2 Topic 3-3
3.2.3 Obtaining Trusted Certificate from CA 3-3
3.2.4 Topic 3-3

4 CONFIGURING IDENTITY AND TRUST STORES FOR WEBLOGIC

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 Setting SSL Attributes for Private Key Alias and Password 5-1

6 TESTING CONFIGURATION

6.1 Testing Configuration 6-1

7 CREATING RESOURCES ON WEBLOGIC

7.1 Introduction 7-1
7.2 Resource Administration 7-1
7.2.1 Creating Data Source 7-1
7.2.1.1 Prerequisites 7-1
7.2.1.2 XA Enabled Data Source 7-2
7.2.1.3 Non-XA Enabled Data Source 7-9
7.2.2 JMS Server Creation 7-18
7.2.3 JMS Modules Creation 7-23
7.2.4 Subdeployment Creation 7-27
7.2.5 JMS Queue Creation 7-31
7.2.6 JMS Connection Factory Creation 7-35
7.3 Configuring Weblogic for PMGateway 7-40
7.4 Configuring Weblogic for Oracle Banking Trade Finance 7-41
7.5 Setup/Configure Mail Session in Weblogic 7-44
7.5.1 Creating JavaMail Session 7-44
7.5.2 Configuration of the TLS/SSL Trust Store for Weblogic Server 7-48

Preface

- Purpose
- Audience
- Documentation Accessibility
- Critical Patches
- Diversity and Inclusion
- Conventions
- Related Resources
- Screenshot Disclaimer

Purpose

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

Audience

This guide is intended for anyone responsible for installing Oracle Banking Application.

Documentation Accessibility

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

Access to Oracle Support

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

Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at Critical Patches, Security Alerts and Bulletins. All critical patches should be applied in a timely manner to ensure effective security, as strongly recommended by Oracle Software Security Assurance.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners,

we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Related Resources

For more information, see these Oracle Banking Trade Finance resources:

- Oracle Banking Trade Finance Release Notes
- Oracle Banking Trade Finance Install & Upgrade

Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes.

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.

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

- Creation of Self-signed Certificate
  This topic explains creation of Self-signed Certificate.

3.1.1 Creation of Self-signed Certificate

This topic explains 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. ***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 Oracle Banking Trade Finance, 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

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 Topic

Enter a short description of your topic here (optional).

This is the start of your topic.

- Topic
  Enter a short description of your topic here (optional).
- Topic
  Enter a short description of your topic here (optional).
- Obtaining Trusted Certificate from CA
- Topic
  Enter a short description of your topic here (optional).

3.2.1 Topic

Enter a short description of your topic here (optional).

This is the start of your topic.

3.2.2 Topic

Enter a short description of your topic here (optional).

This is the start of your topic.

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 Topic

Enter a short description of your topic here (optional).

This is the start of your topic.

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 Banking Trade Finance 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.

- Creating Data Source
- JMS Server Creation
- JMS Modules Creation
- Subdeployment Creation
- JMS Queue Creation
- JMS Connection Factory Creation

7.2.1 Creating Data Source

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

- Prerequisites
- XA Enabled Data Source
- Non-XA Enabled Data Source

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	https://www.oracle.com/database/technologies/instant-client/downloads.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*.

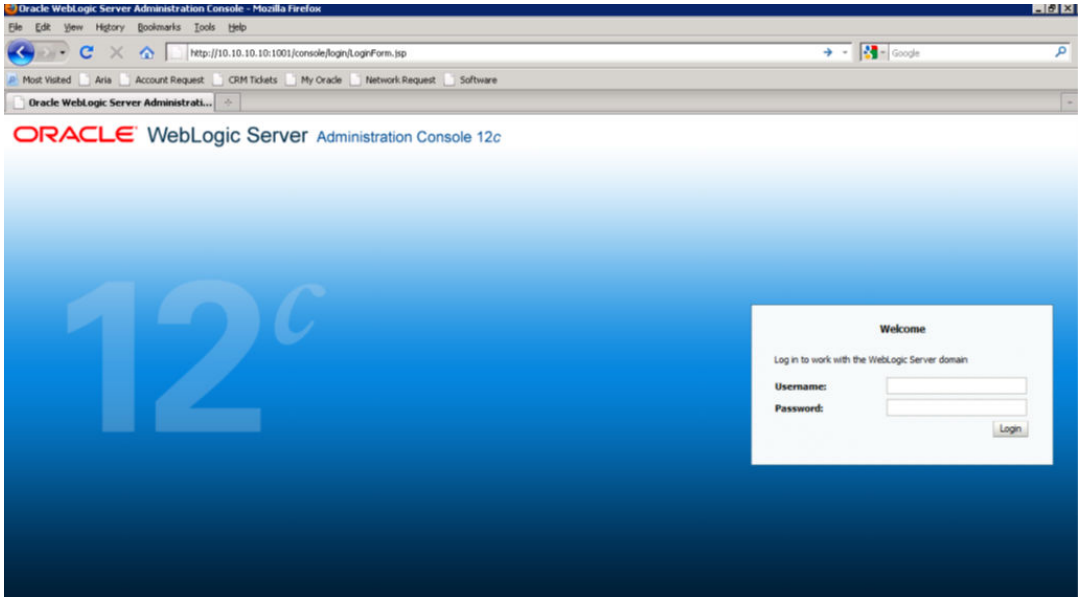
  This is required to load all the *.dll* files.
  - Ensure that the *ojdbc*.jar* file in *{WL_HOME}/server/lib/ojdbc*.*jar is the same as the file *{ORACLE_HOME}/jdbc/lib/ojdbc*.jar*. This is required for ensuring compatibility.
  - Update PATH in *StartWebLogic.bat or in setDomainEnv.bat*. This must 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:

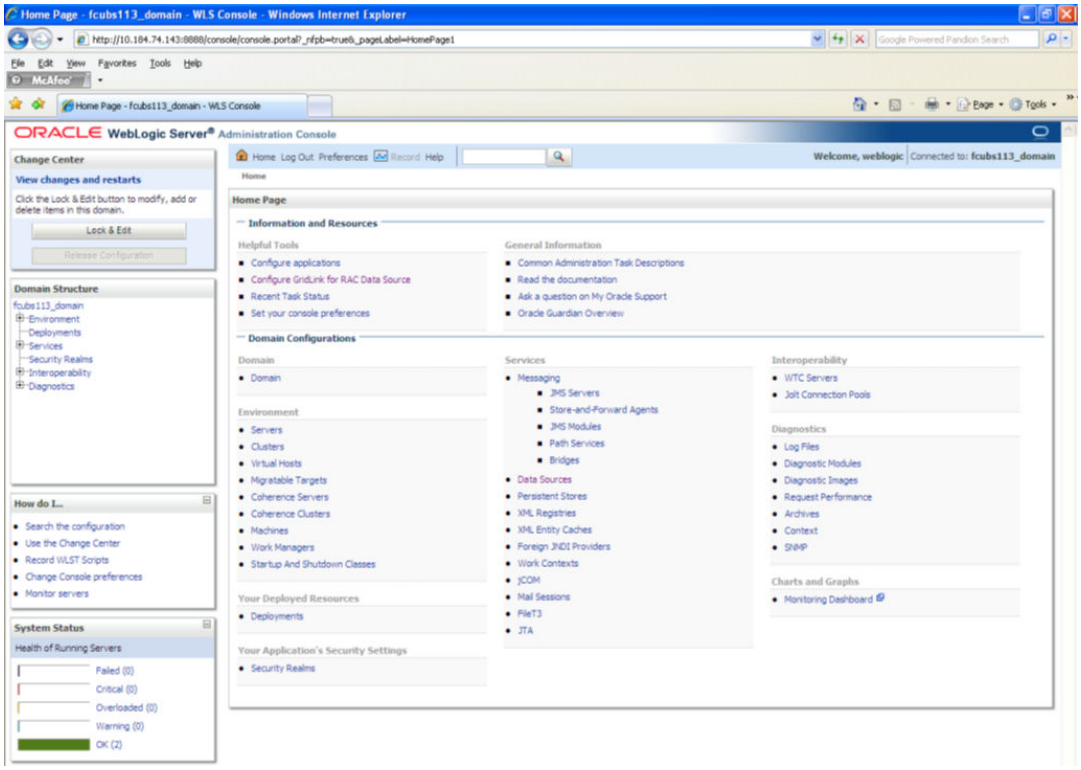
1. Start the Administrative Console of Weblogic application server. You can start this by entering Oracle Weblogic Admin Console URL in the address bar in an internet browser. http://10.10.10.10:1001/console

   Eg: http://10.10.10.10:1001/console

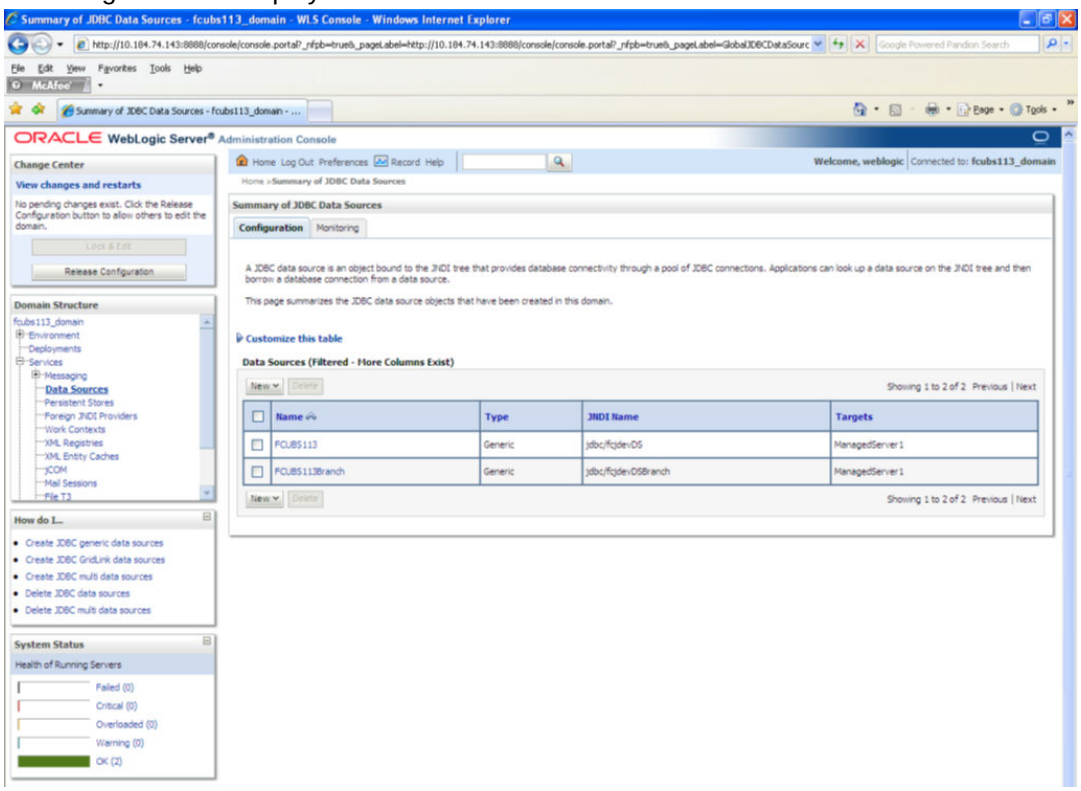


2. Specify the Weblogic administrator user name and password. Click ‘Log In’.

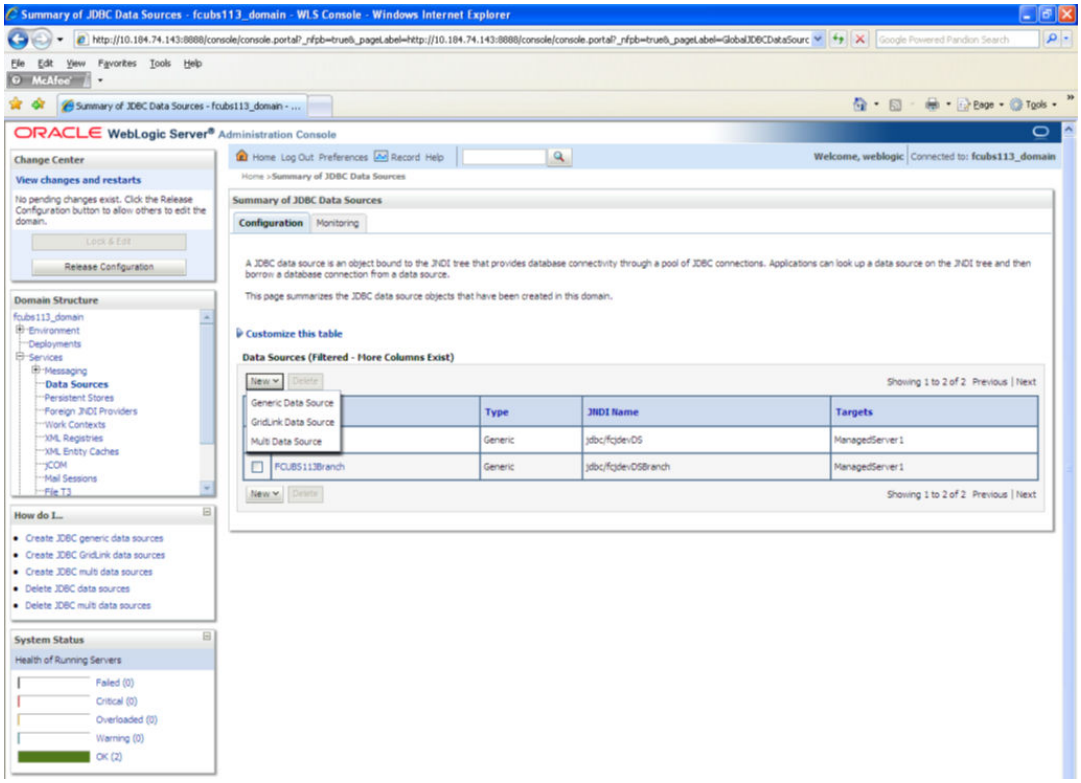
3. Navigate to Oracle Weblogic home page.



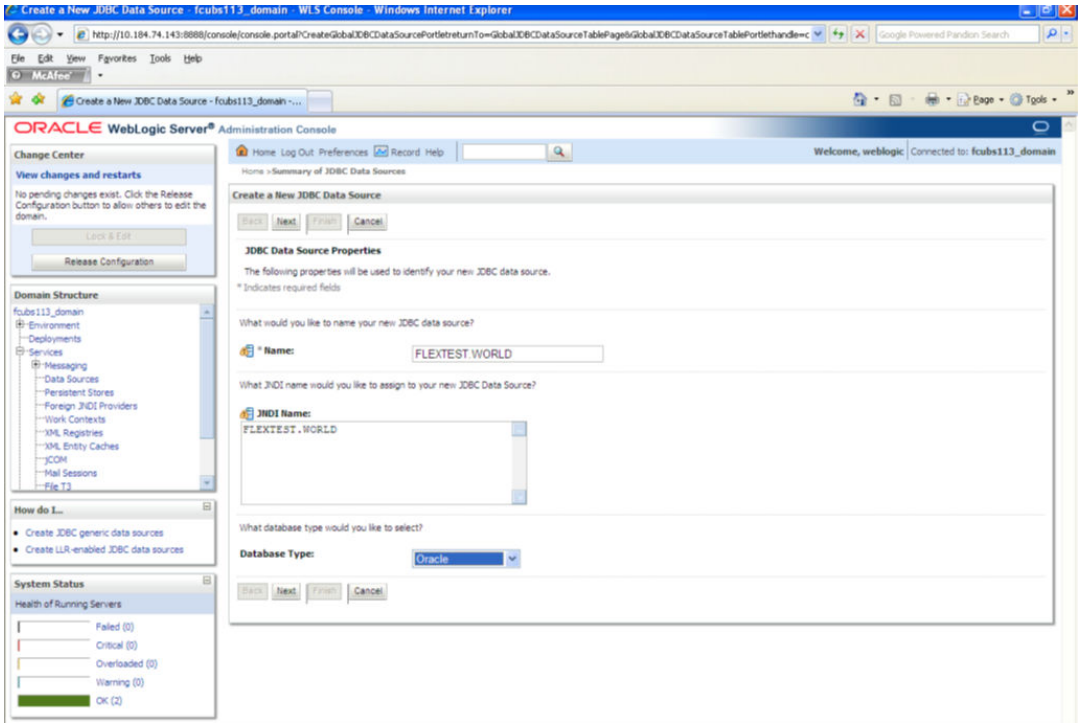
4. Click ‘LOCK & EDIT’.
Following screen is displayed:



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



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

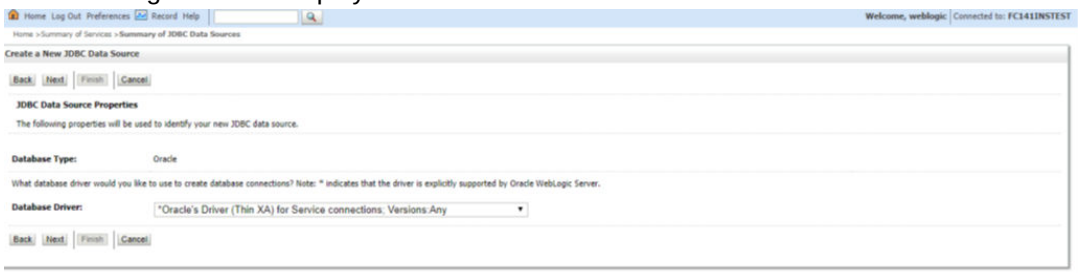


7. Specify the following details:

JDBC Datasource Name	Name of the data source
JNDI Name	JNDI name which will be used for lookup

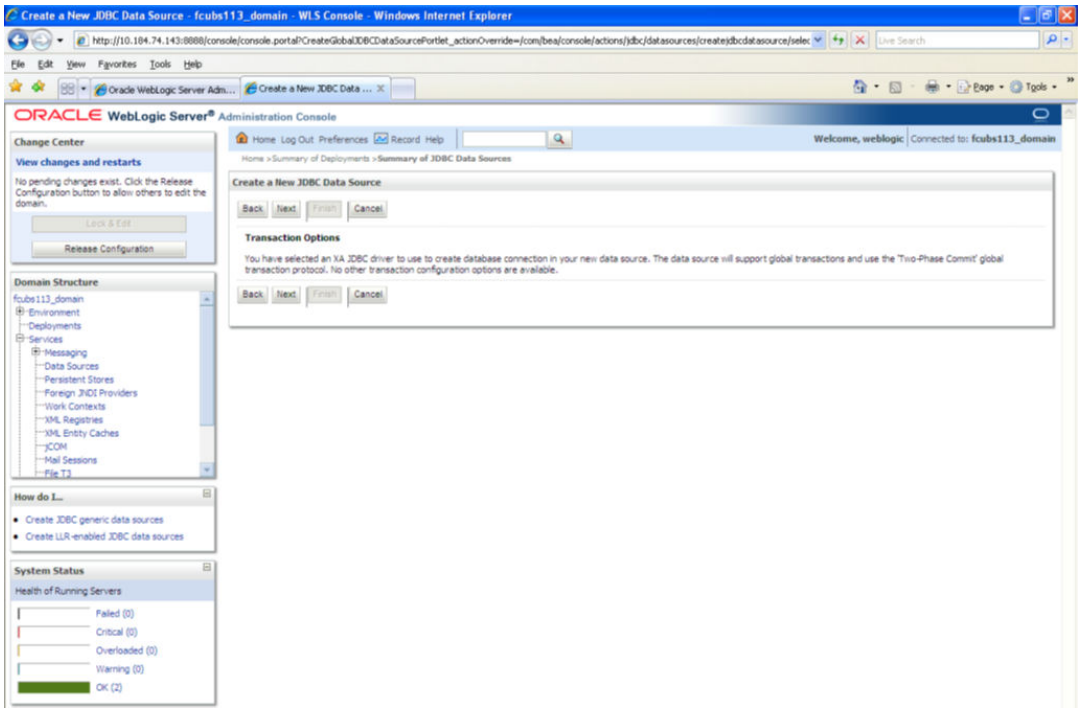
Database Type	Type of the database which is Oracle

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

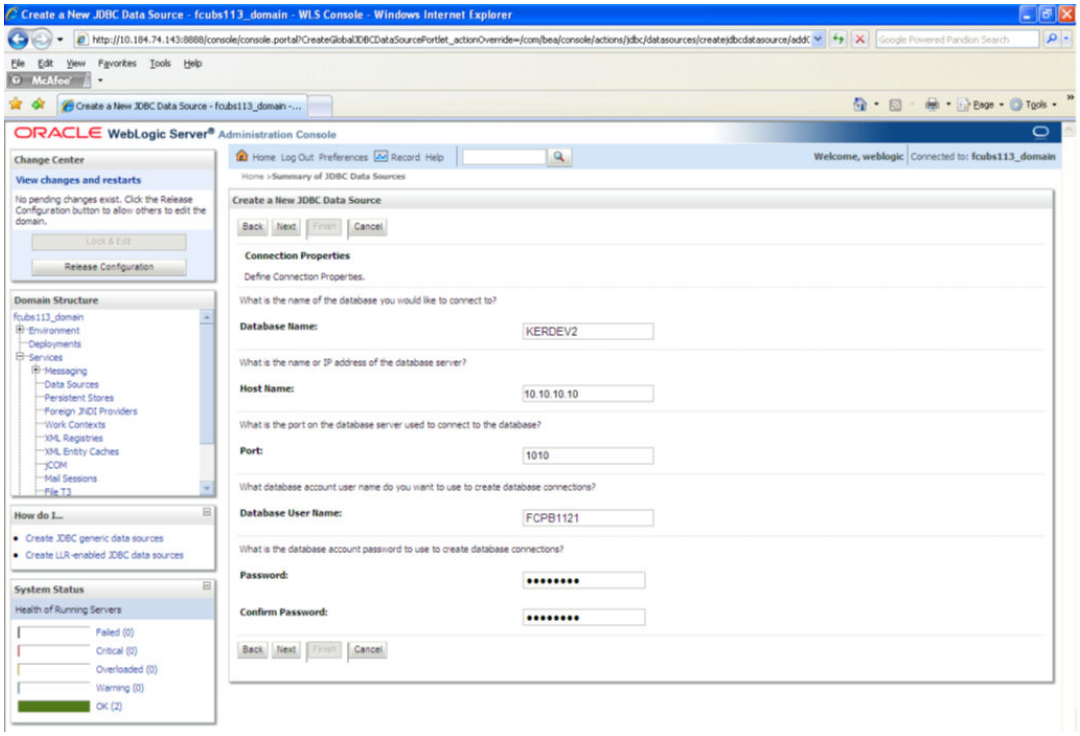


Click next.

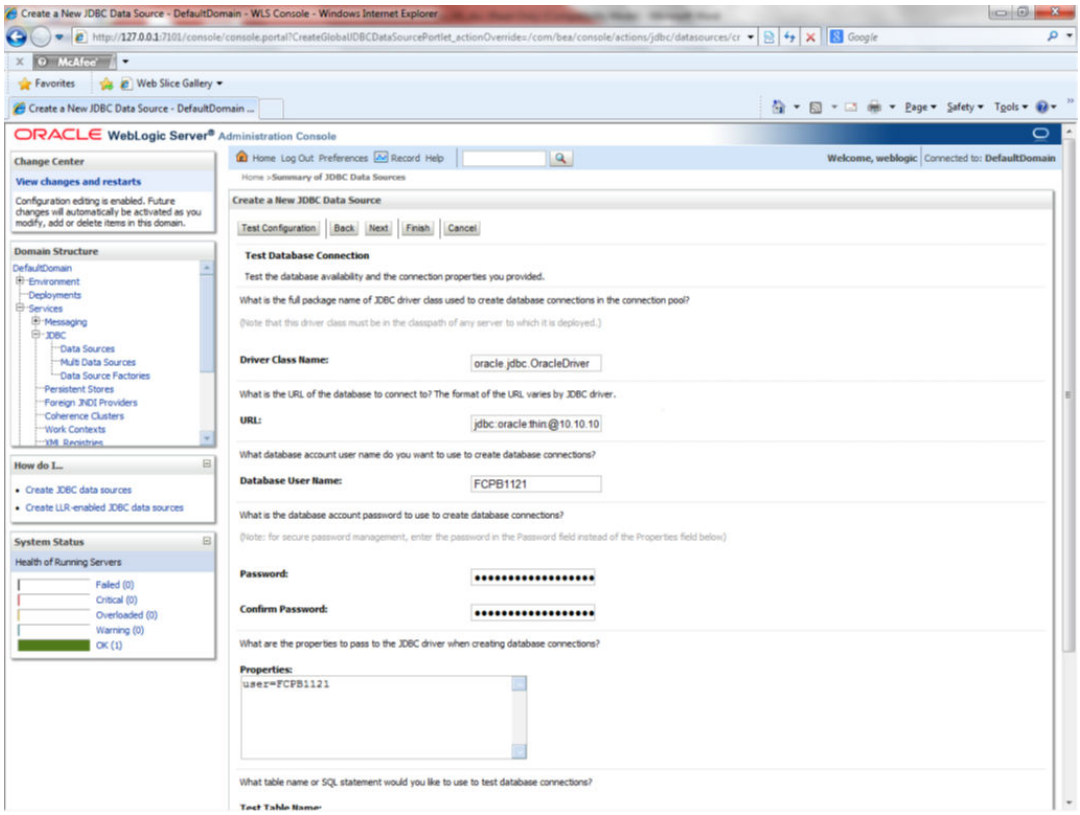
9. Select the database driver as shown in the figure. Click ‘Next’.



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

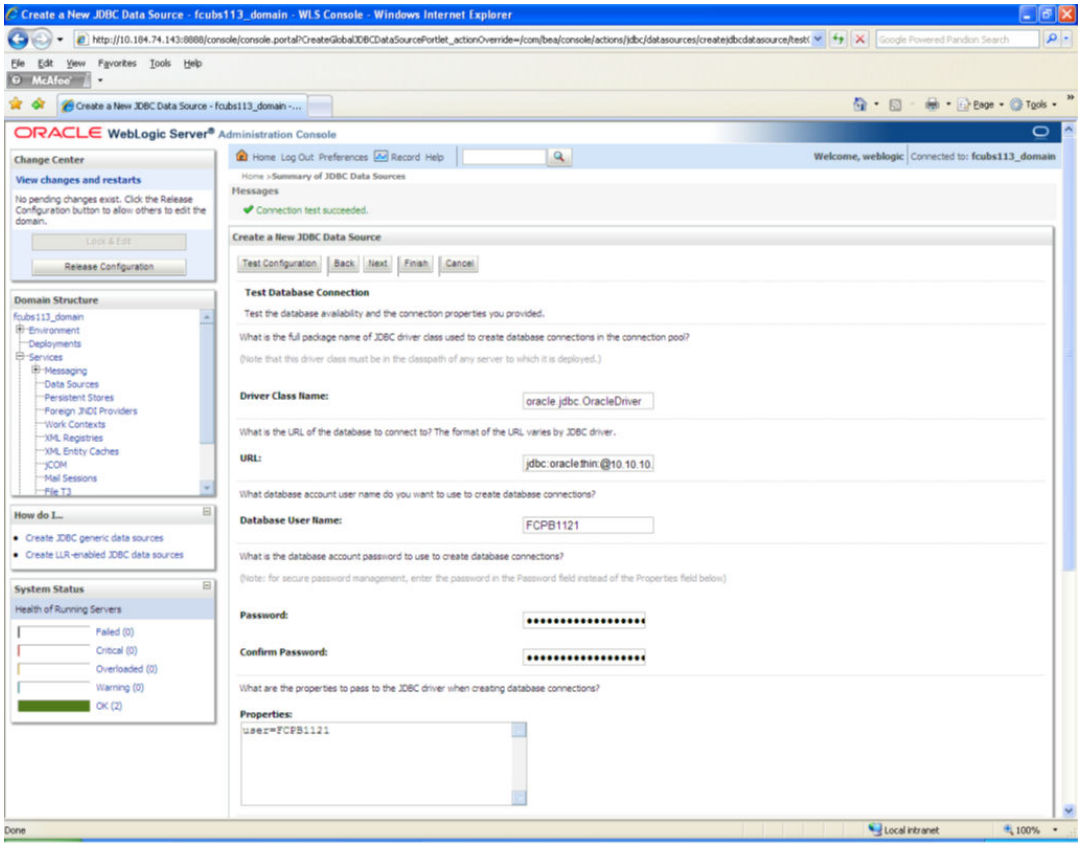


11. Click ‘Next’.
The following screen is displayed.



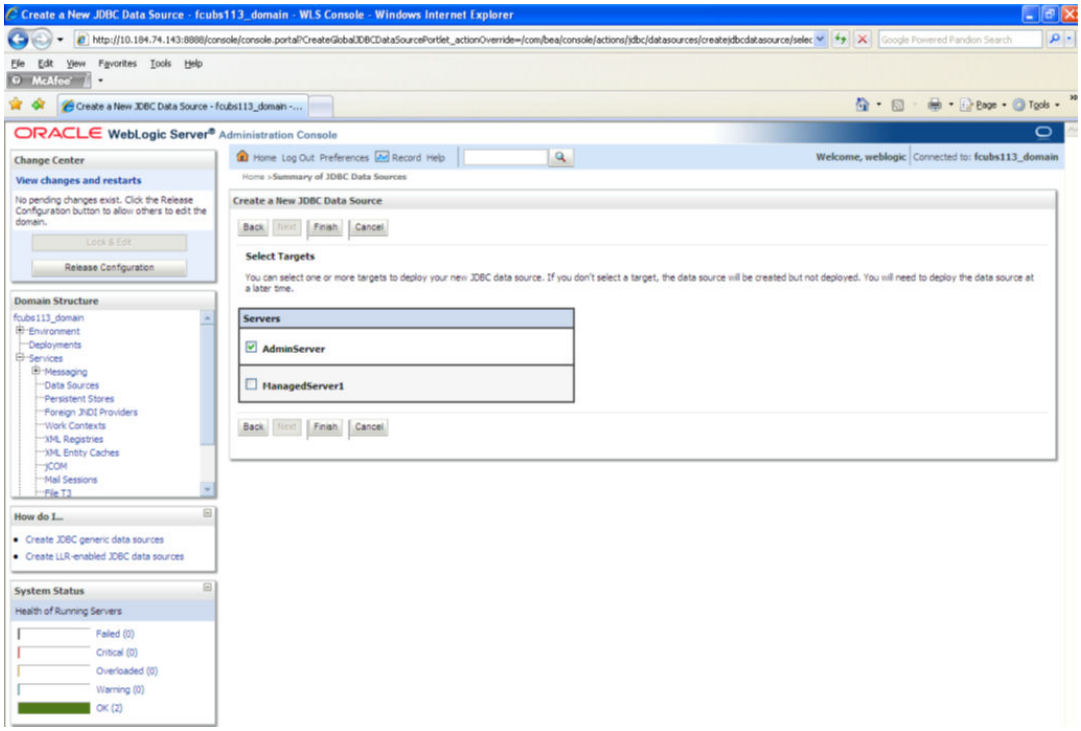
12. Specify the Driver Class Name (Eg: oracle.jdbc.OracleDriver).
13. Specify the URL.

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.

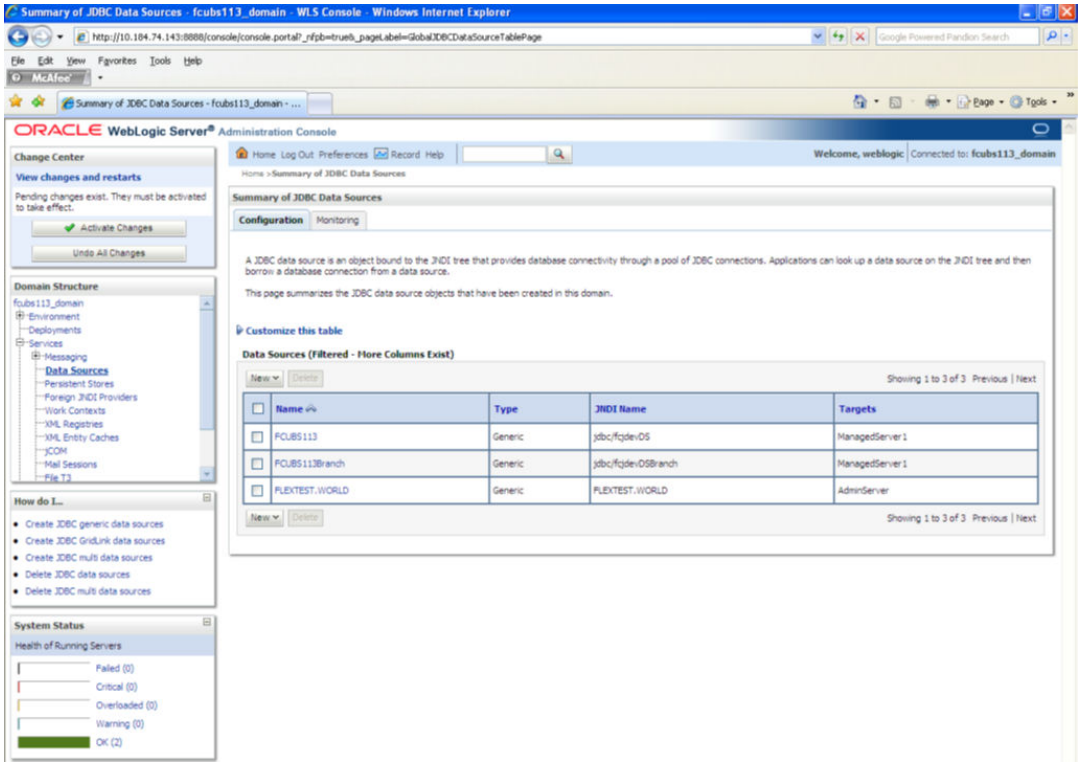


17. Click ‘Next’.

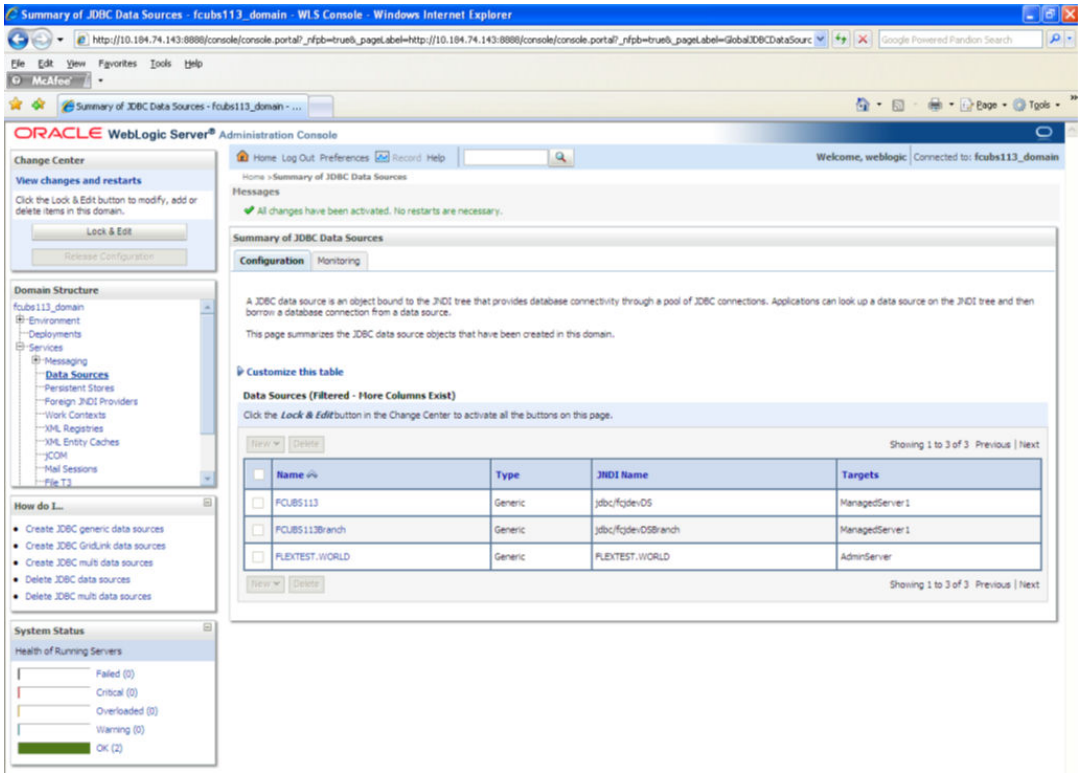
The following screen is displayed:



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.

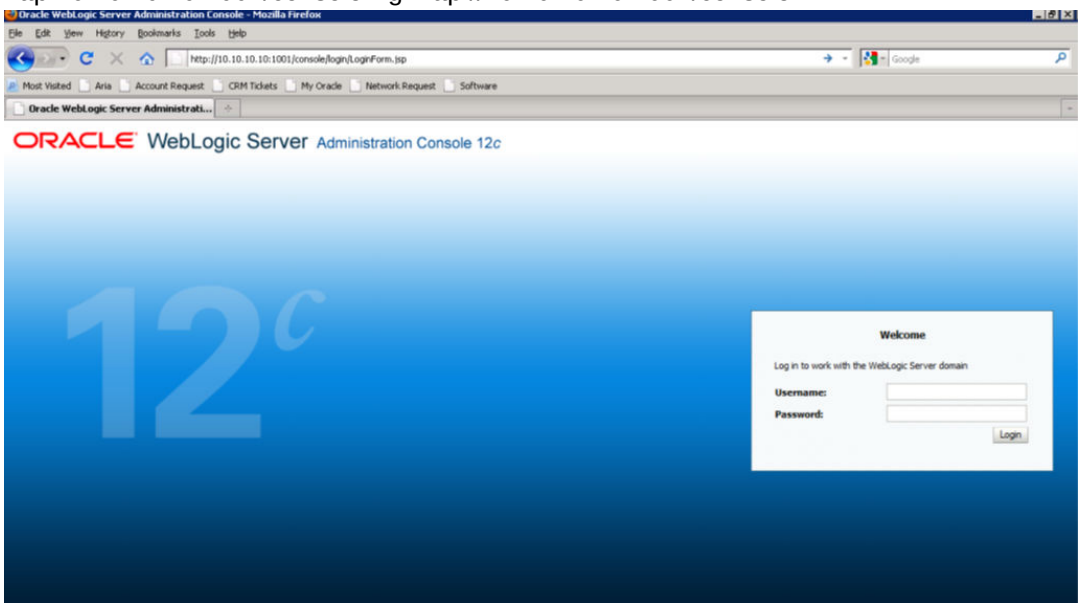


20. The datasource has been created.

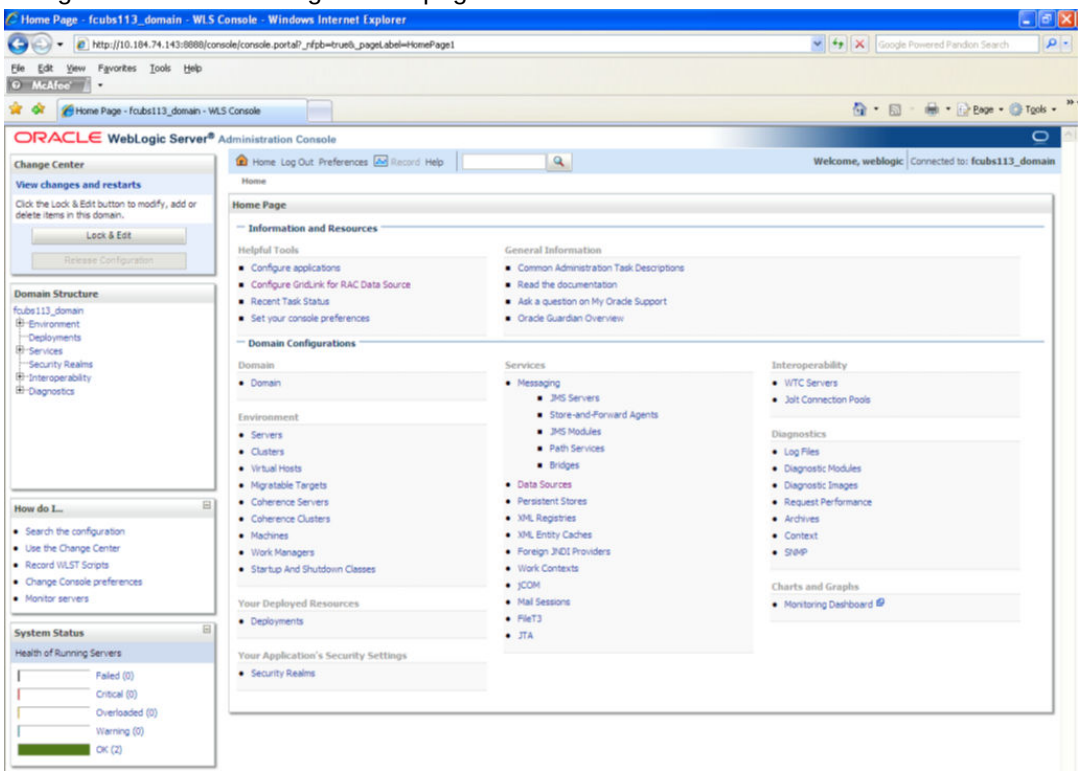
21. Refer to “Resources_To_ Be_Created.doc” for the list of XA datasources to be created.

7.2.1.3 Non-XA Enabled Data Source

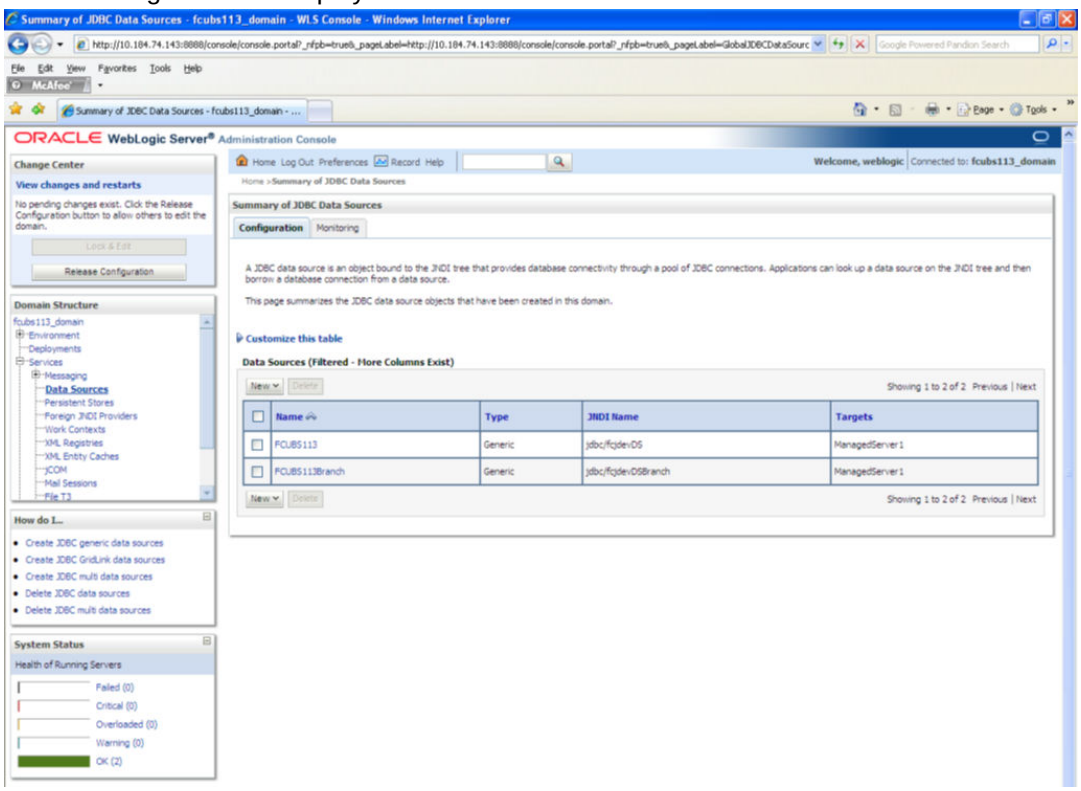
1. Follow the steps given below:Start the Administrative Console of Weblogic application server. You can start this by entering Oracle Weblogic Admin Console URL in the address bar in an internet browser.
http:10.10.10.10:1001/console Eg: http://10.10.10.10:1001/console



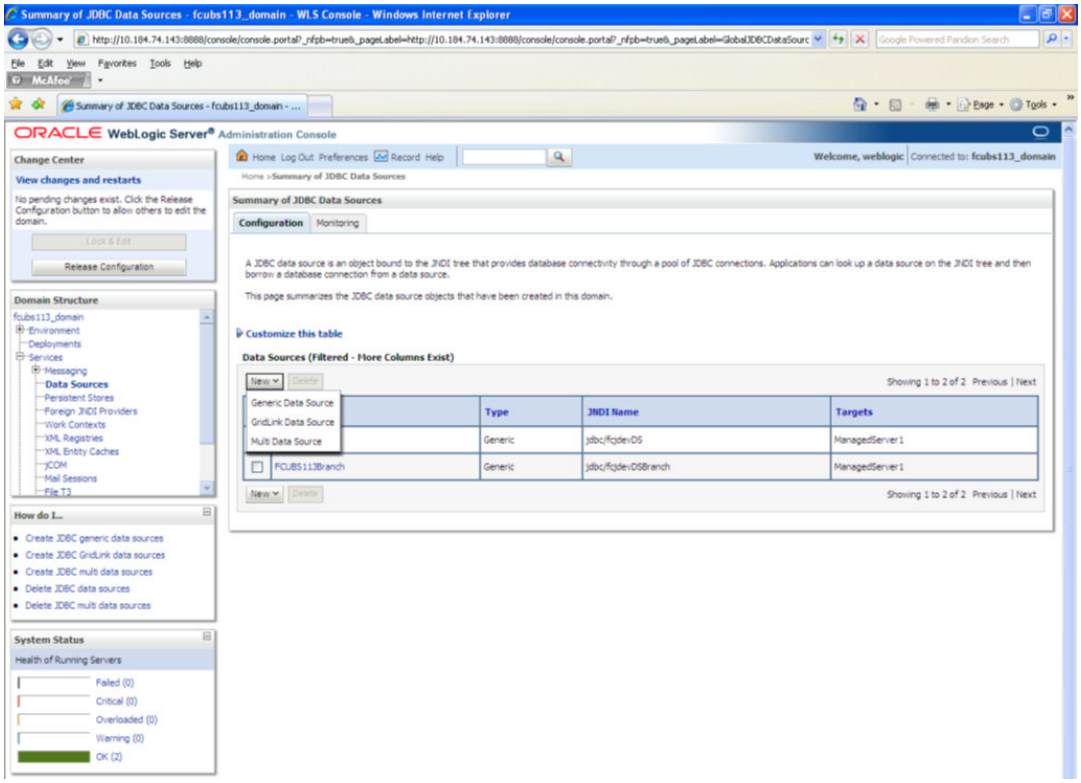
2. Specify the Weblogic administrator user name and password. Click ‘Log In’.
3. Navigate to Oracle Weblogic home page.



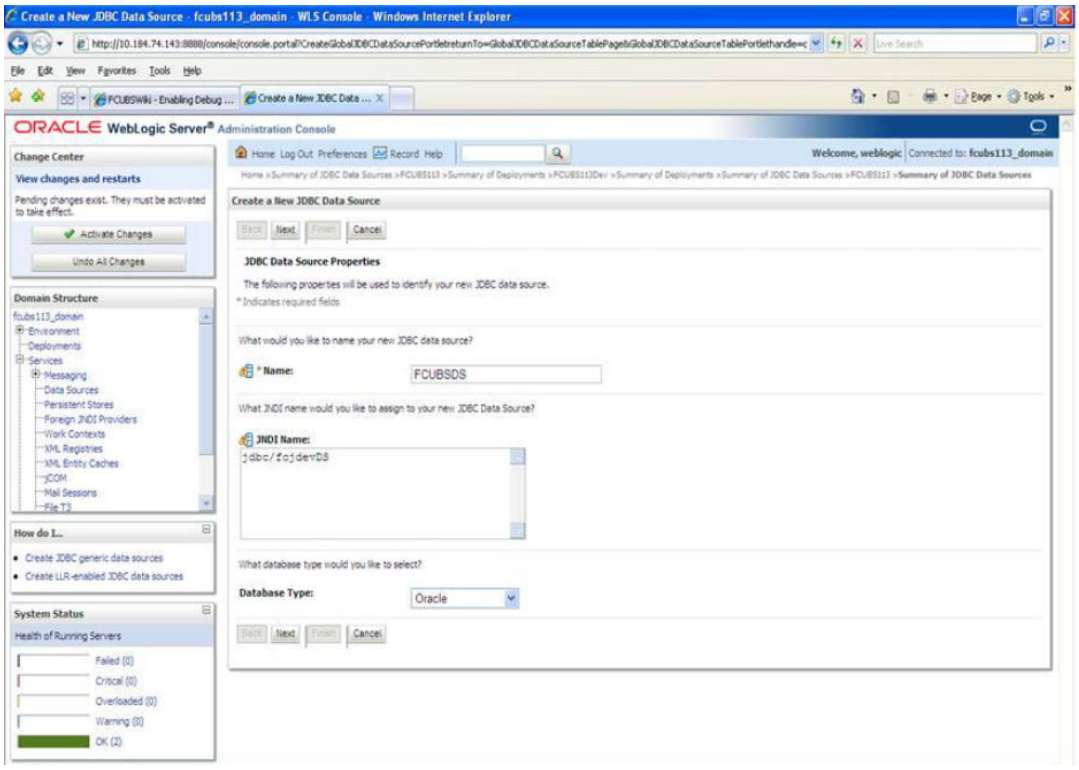
The following screen is displayed:



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



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

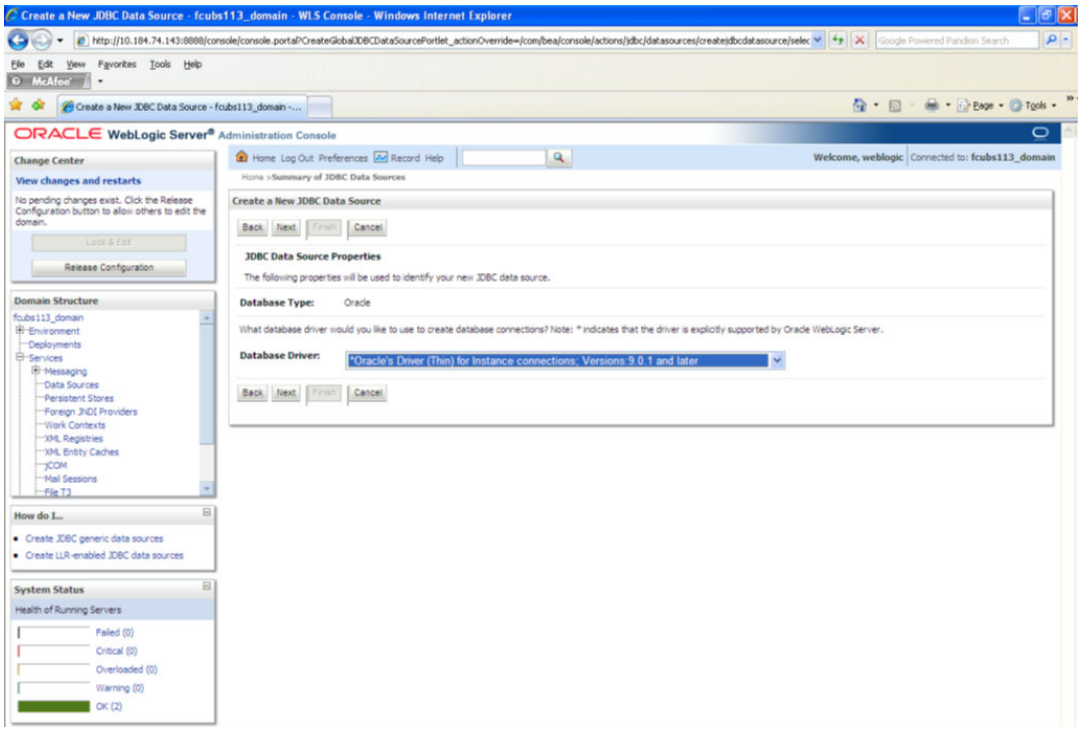


6. Specify the following details:

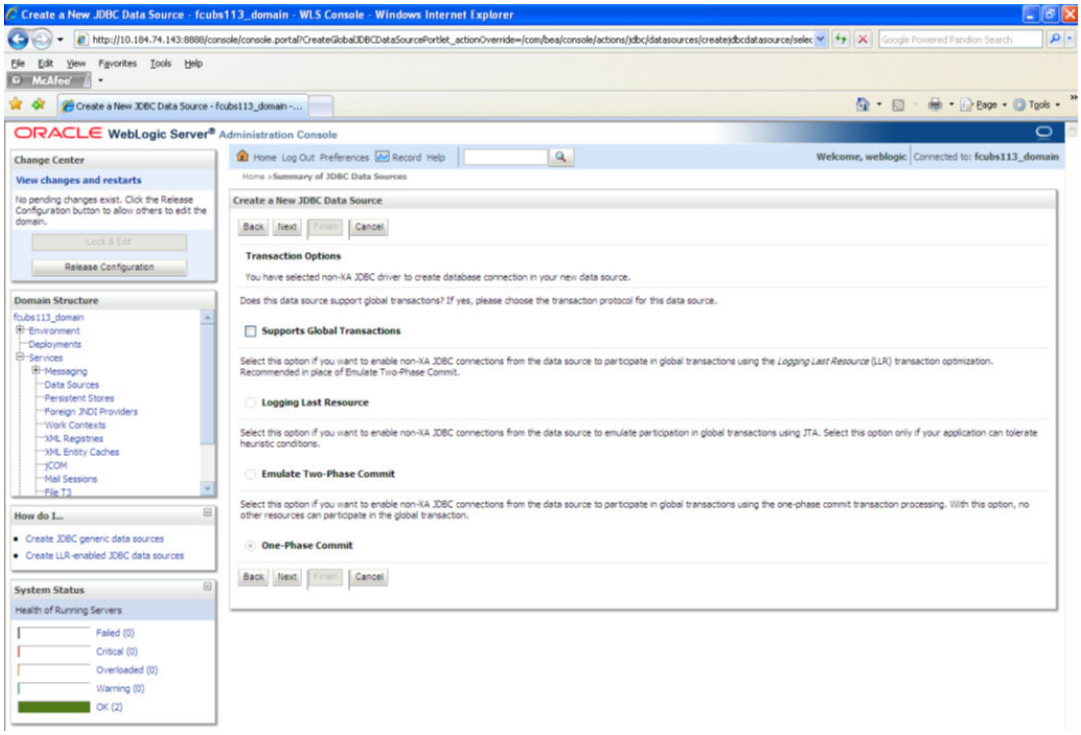
JDBC Datasource Name	Name of the Datasource
JNDI Name	JNDI for lookup

Database Type	Oracle

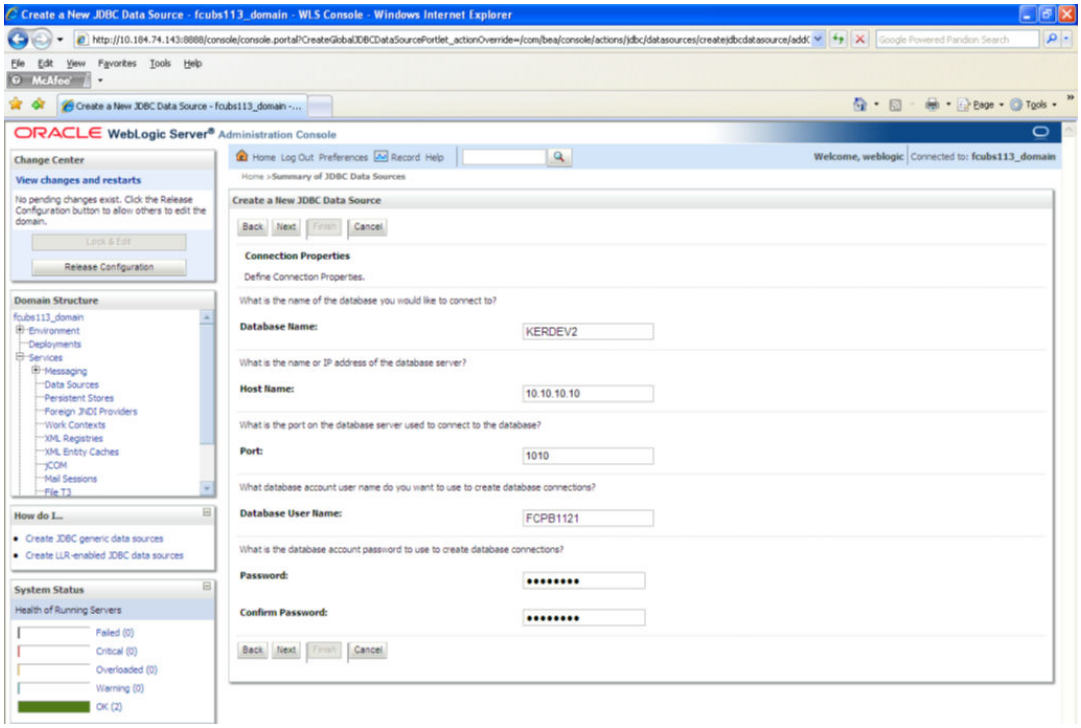
7. Click ‘Next’.



8. Select the database driver as shown in the figure. Click ‘Next’.
Following screen is displayed:



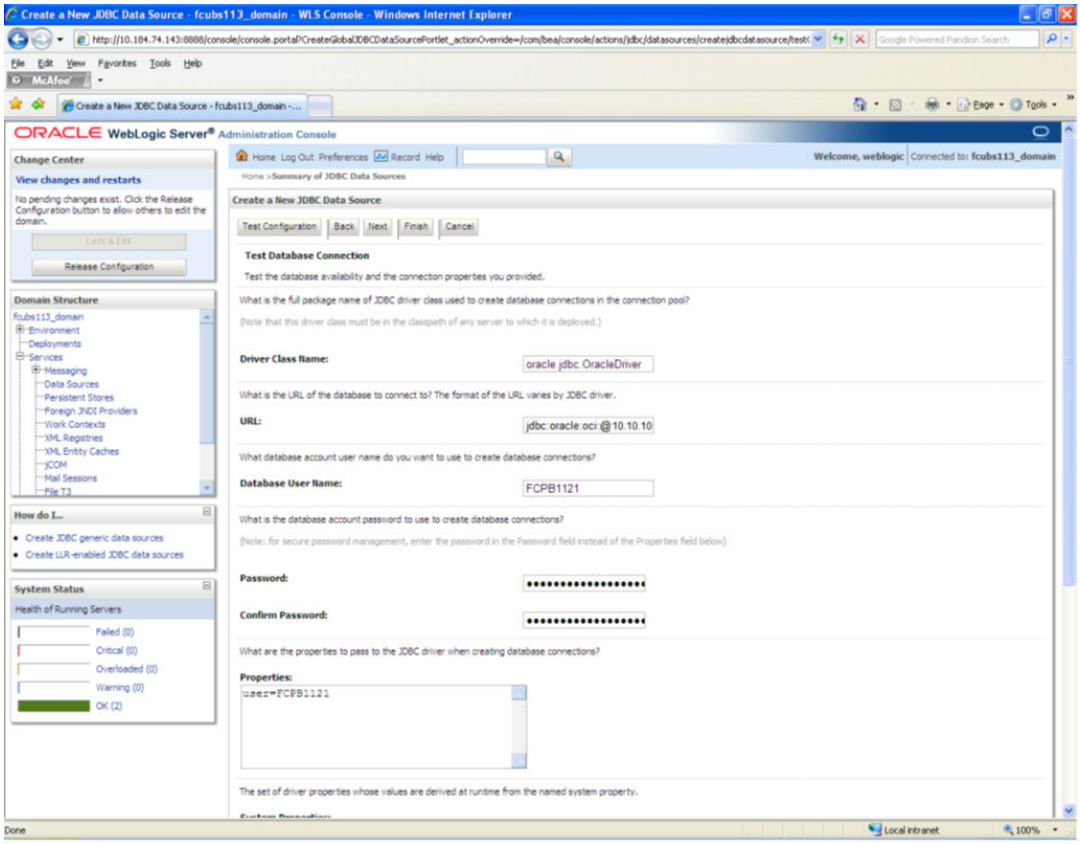
9. Select Logging Last Resource then uncheck ‘Support Global Transactions’. Click ‘Next’. The following screen is displayed:



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.

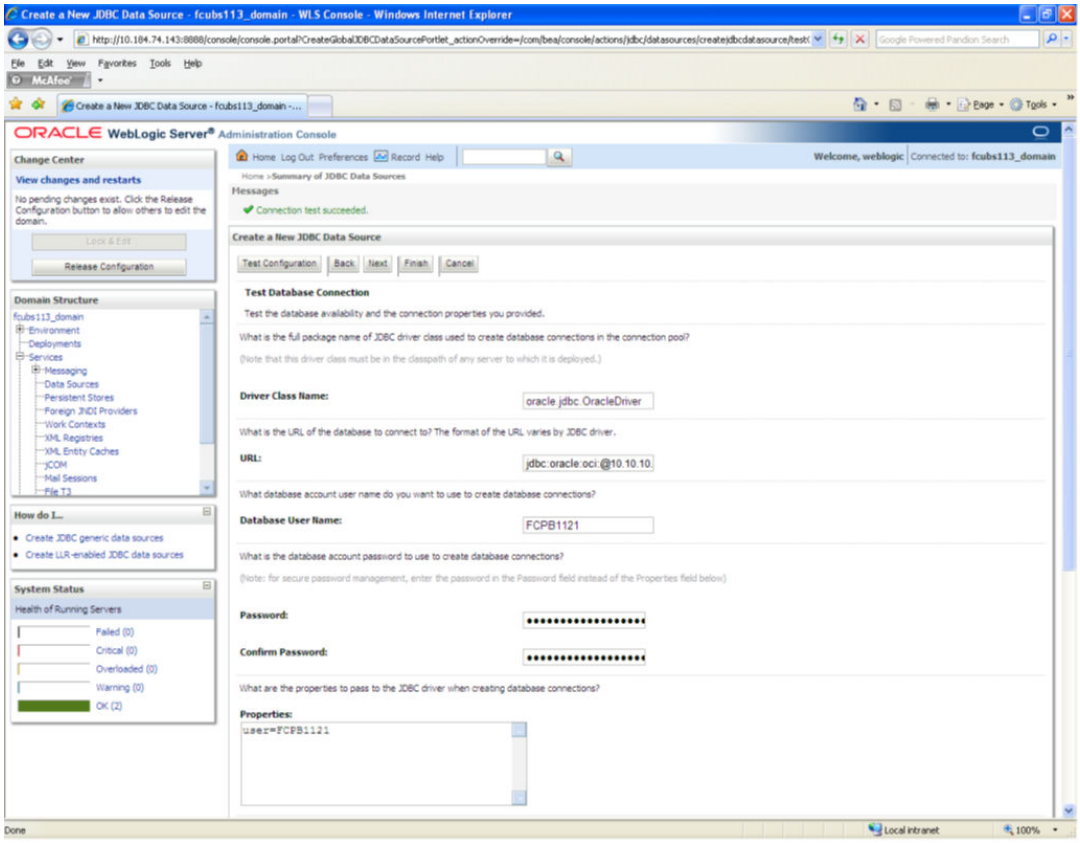
12. Click ‘Next’. The following screen is displayed.



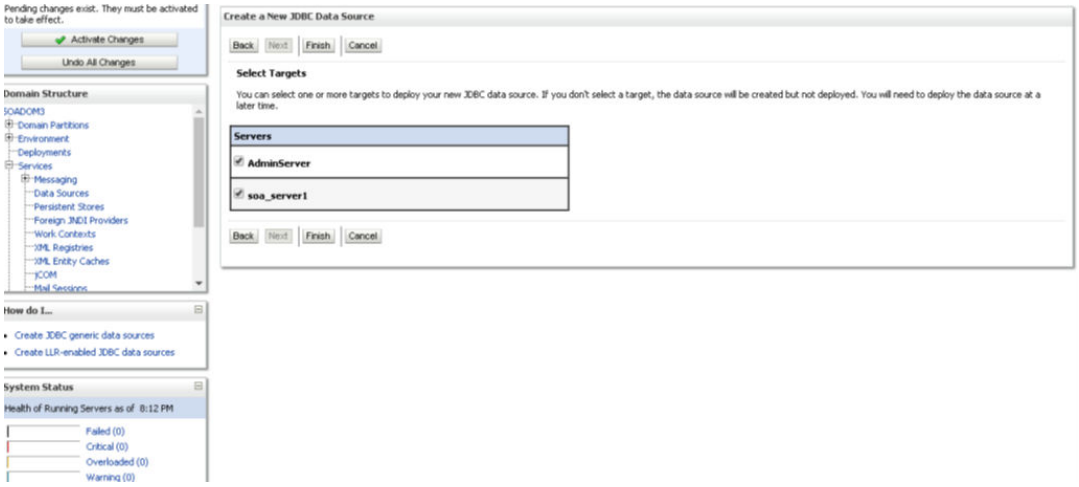
13. Specify the Driver Class Name (Eg: oracle.jdbc.OracleDriver)
14. Specify the URL.
    Default URL: jdbc:oracle:thin:@10.10.10.10:1001:<INSTANCE_NAME>.

    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.

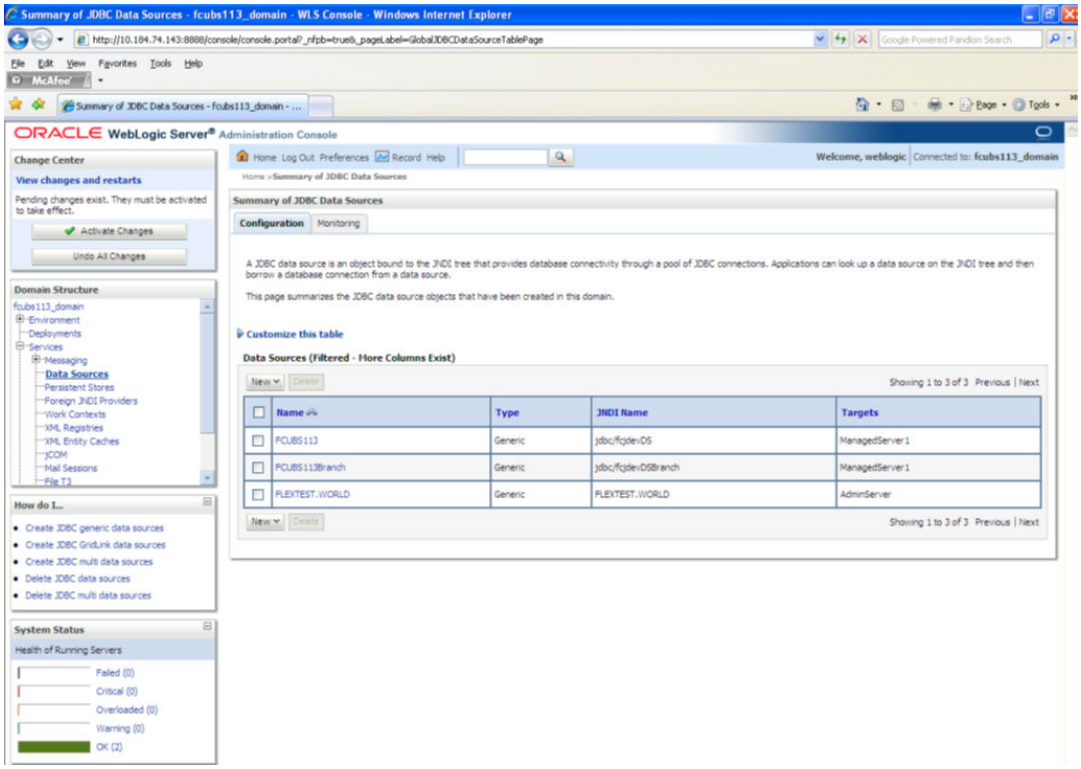


19. Click ‘Next’. The following screen is displayed:

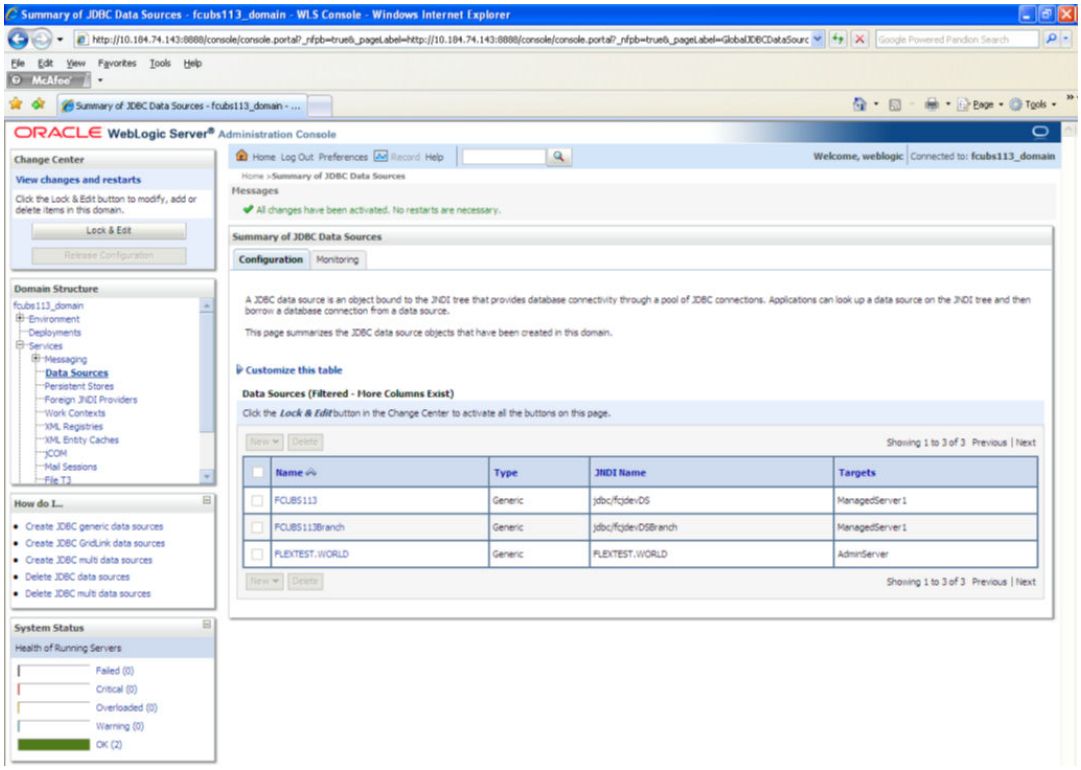


20. Check the boxes against the required servers(for data source jdbc/fcjdevDS, it is mandatory to check the admin server as well as application-deployed server). Click

'Finish'. The following screen is displayed:

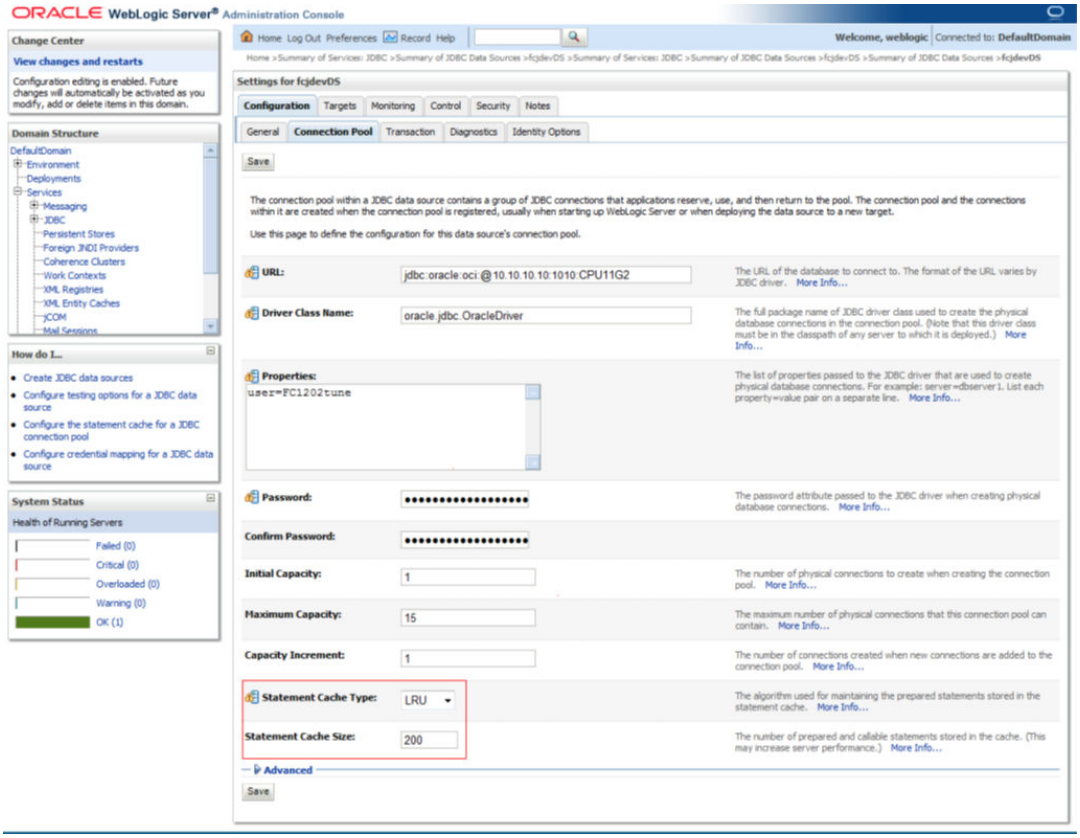


21. Click 'Activate Changes' button. Click 'Activate Changes' button on the left pane. The message 'All the changes have been activated. No restarts are necessary' is displayed.



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.

STOP Note the following

- 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’.
- 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’.
- 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 -

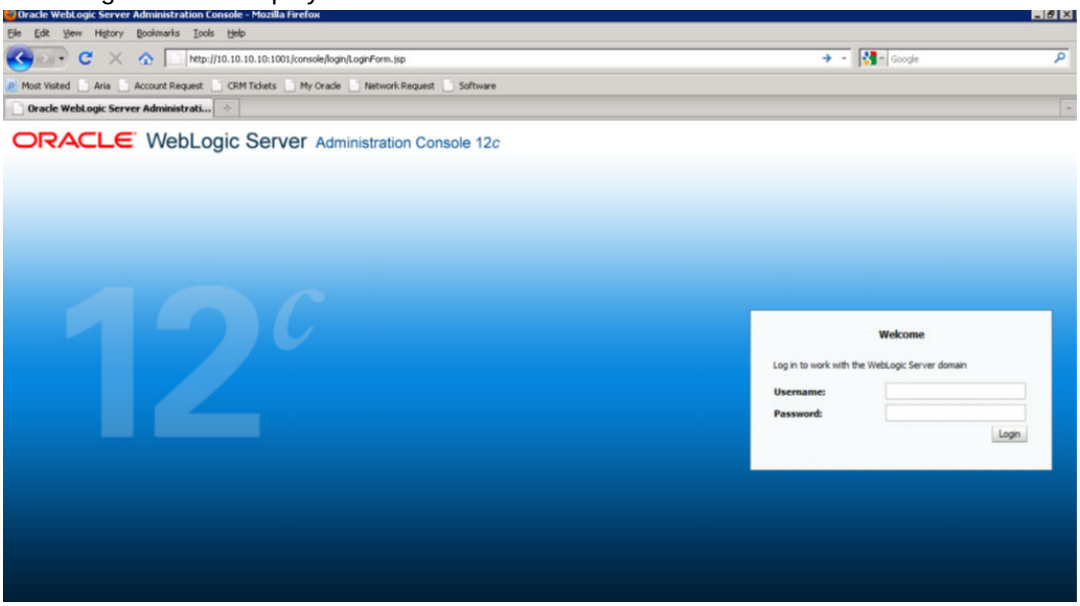
Purpose	Datasource Name	JNDI Name
FCUBS	FCUBS Data source	jdbc/fcjdevDS
SMS	SMS_Datasource	jdbc/fcjdevDSSMS
VAMS	VAMS_DATASOURCE	jdbc/fcvamDS
Gateway	FLEXTEST.WORLD	FLEXTEST.WORLD
Async data source	FCUBS DS_ASYNC	jdbc/fcjdevDS_ASYNC
Scheduler	Scheduler_Datasource	jdbc/fcjSchedulerDS

7.2.2 JMS Server Creation

Follow the steps given below:

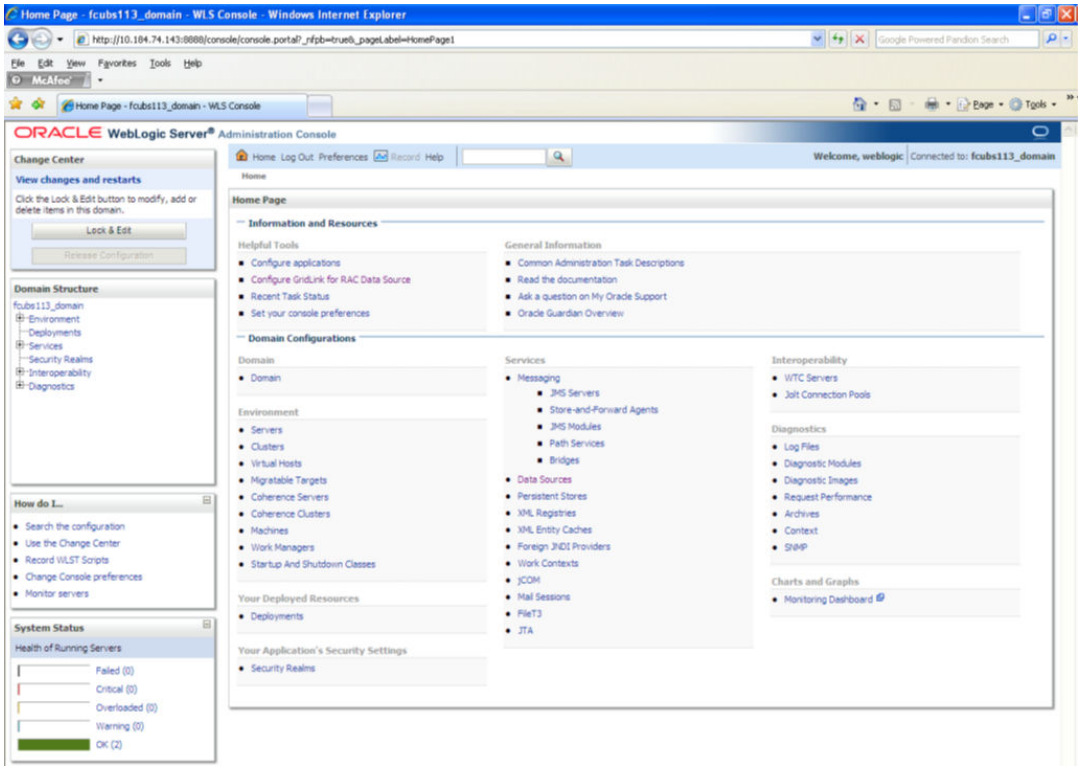
1. Start the Administrative Console of Weblogic application server. You can start this by entering Oracle Weblogic Admin Console URL in the address bar in an internet browser. http://10.10.10.10:1001/console Eg: http://10.10.10.10:1001/console

   Following screen is displayed:

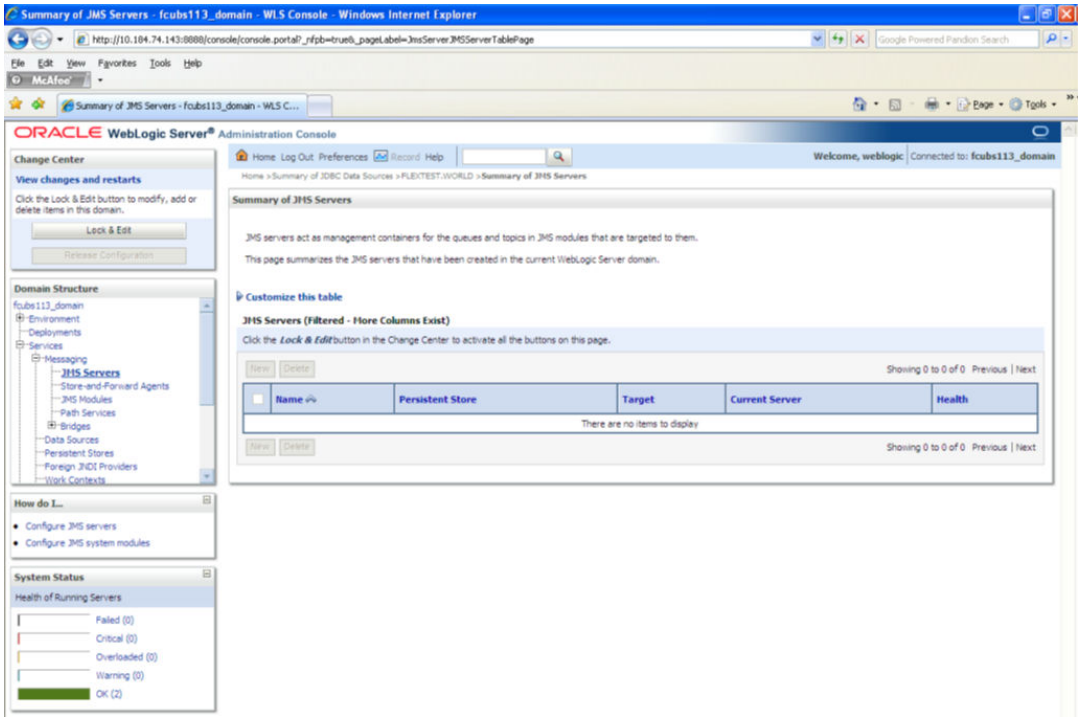


2. Specify the Weblogic administrator user name and password. Click ‘Log In’.

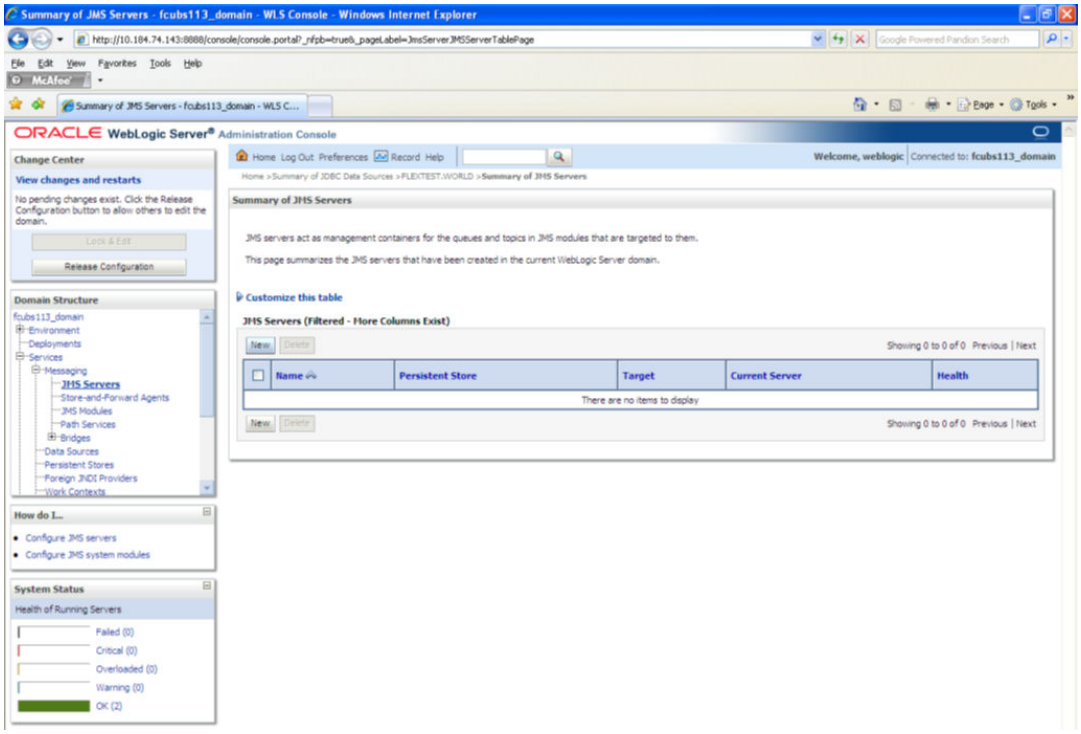
3. Navigate to Oracle Weblogic home page.



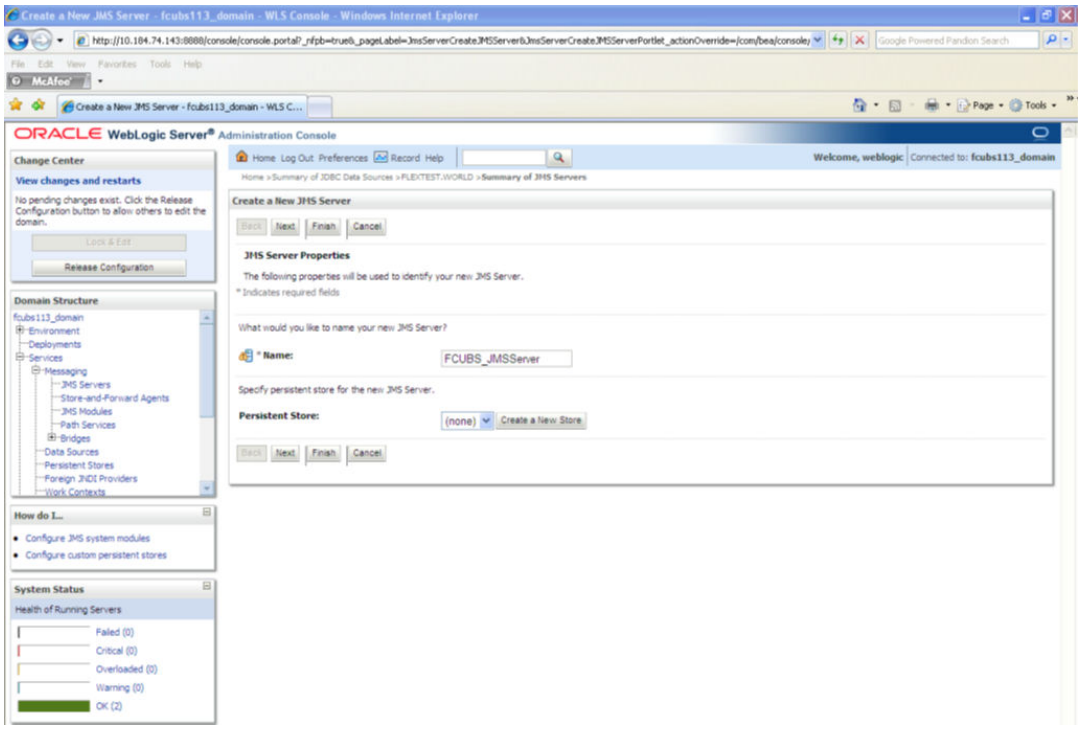
4. Following screen is displayed:



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



6. Click ‘New’.

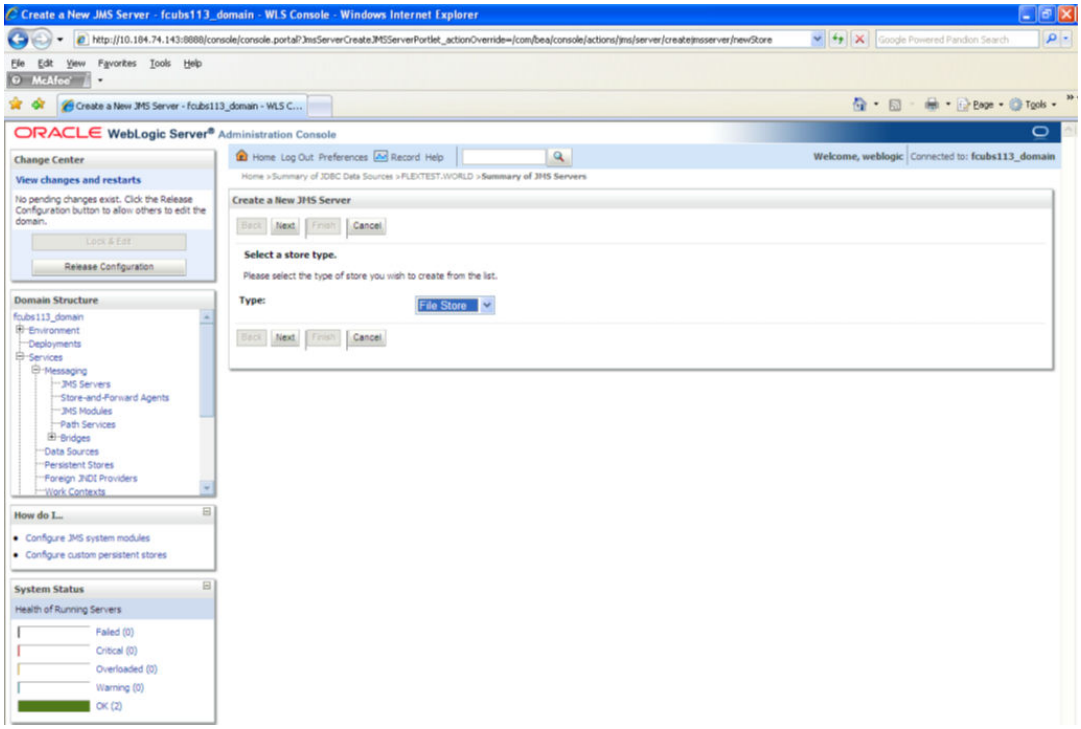


7. Specify the following details:

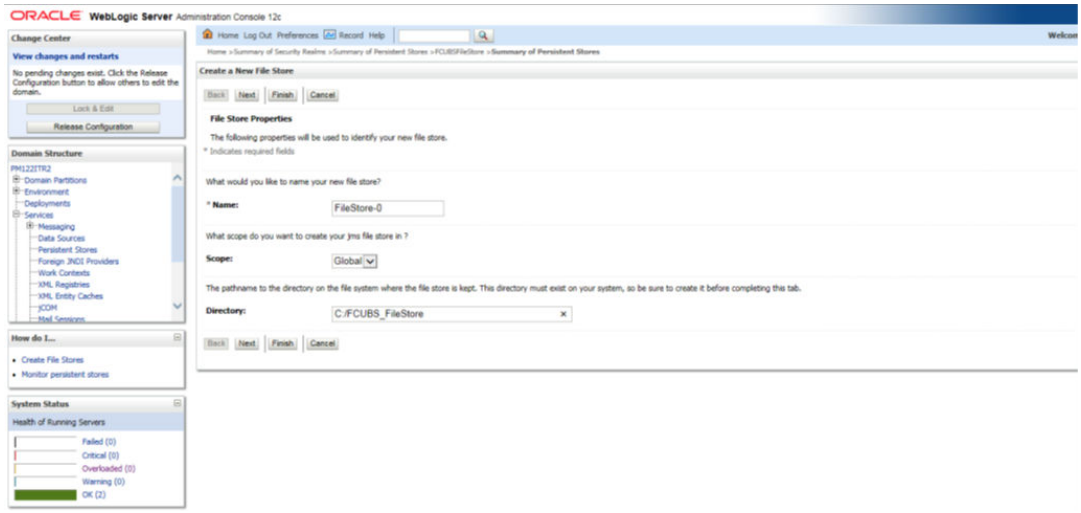
JMS Server Name	Specify the name of JMS Server.

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

9. Select ‘File Store’ as the type and click ‘Next’.



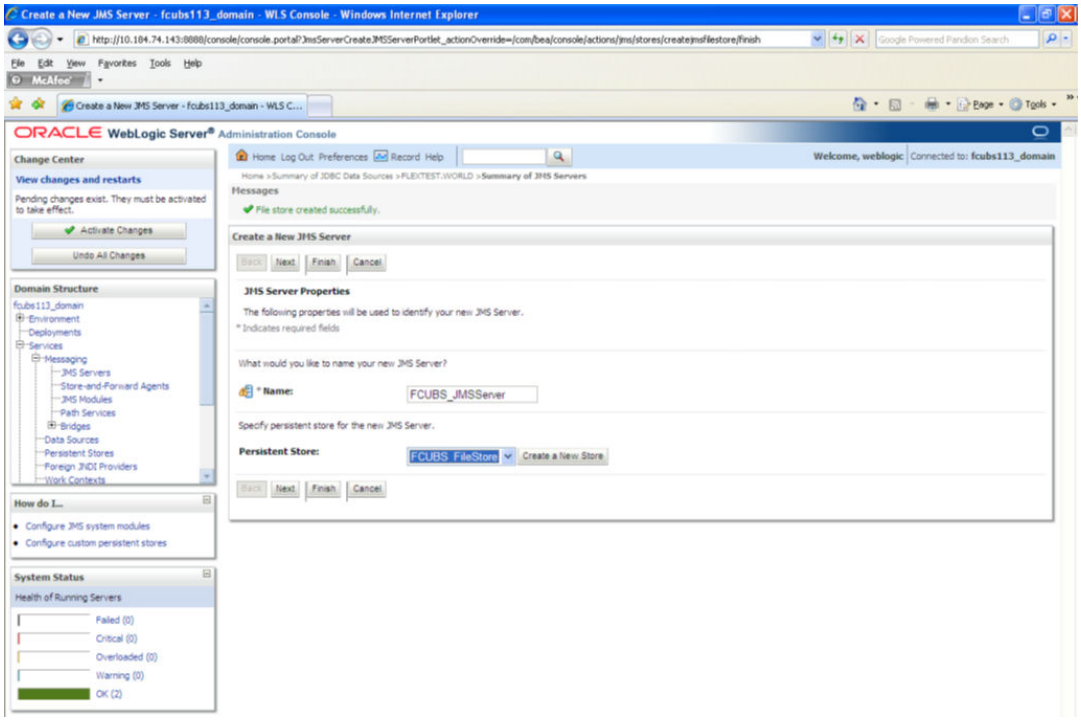
Following screen is displayed:

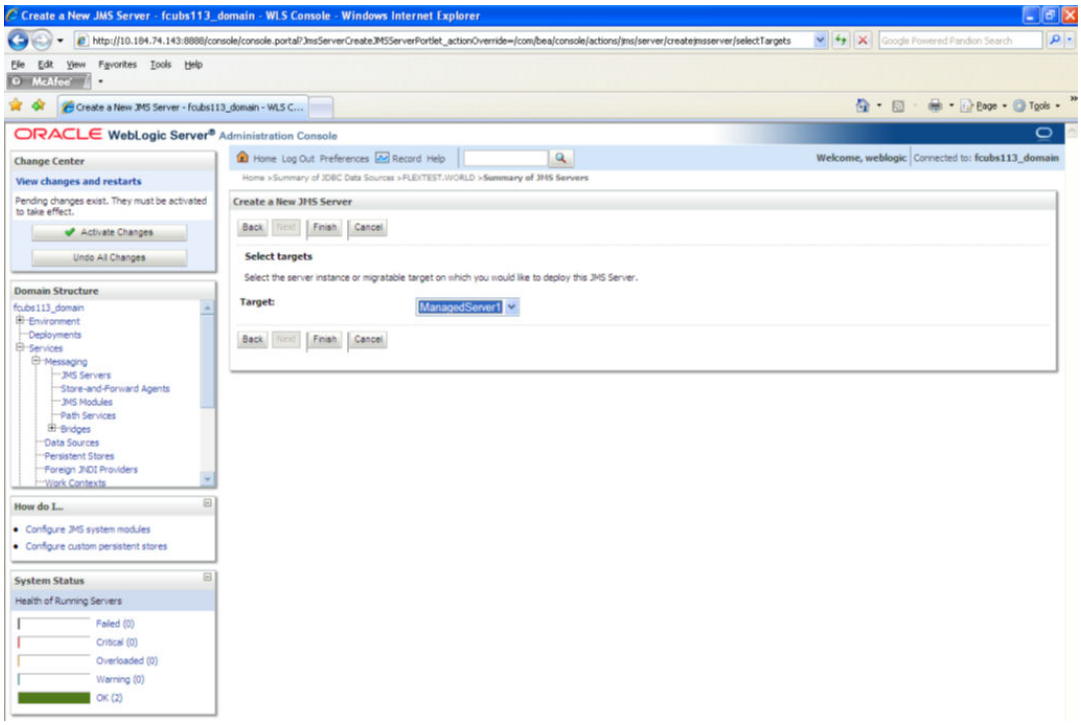


10. To identify the new File Store, specify the following properties:

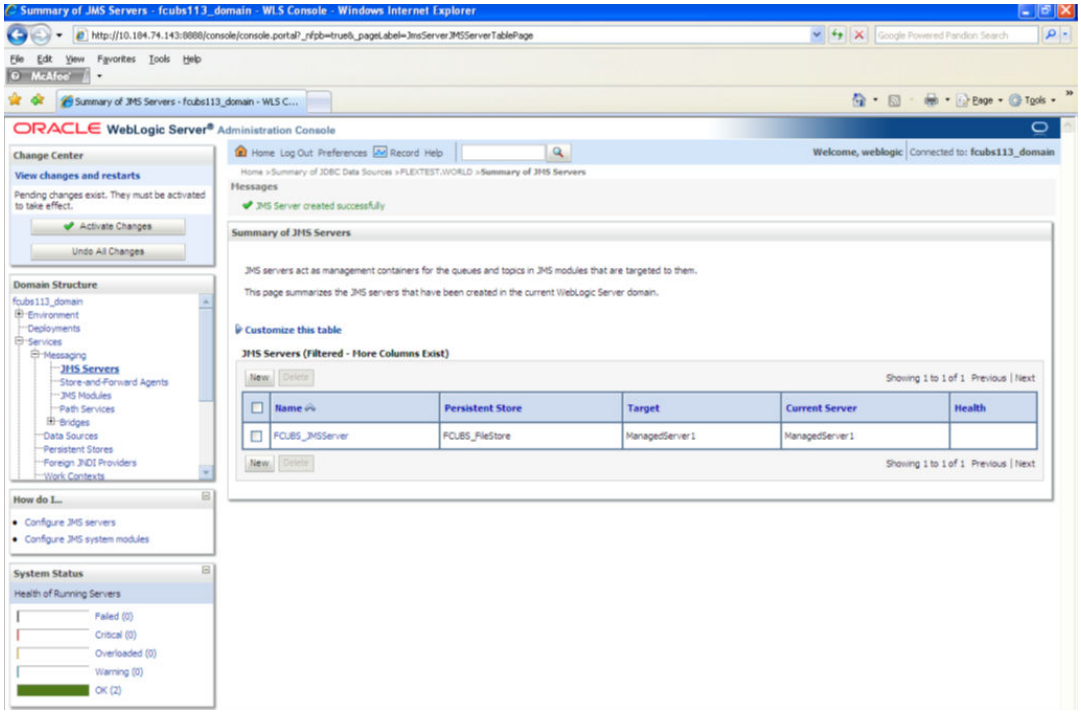
- Specify the file store name as FCUBS_FileStore.
- Select a server. For this file store, you may select ManagedServer1 (created by the user).
- Specify the Filestore Directory path as C:/FCUBS_FileStore.
- Click ‘OK’
  The following screen is displayed with message ‘File store created successfully’.

11. Click ‘Next’.





12. Select the target managed server. Click ‘Finish’.



13. The message ‘JMS Server created successfully’ is displayed.

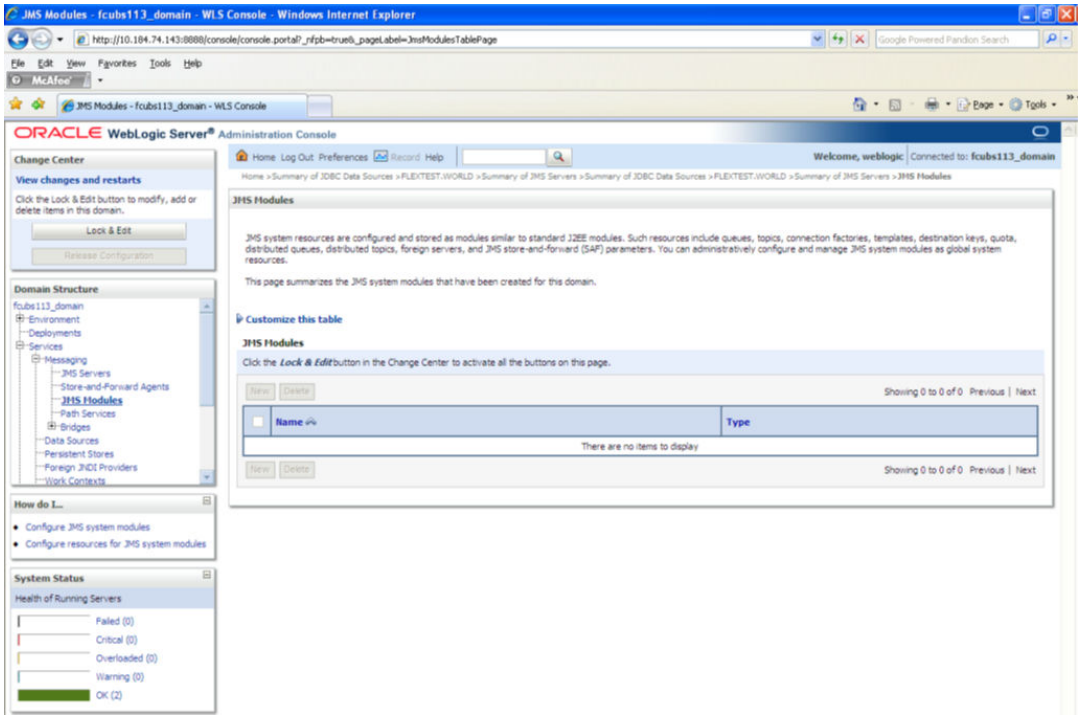
14. Click ‘Activate Changes’ under Change Center. The message ‘All changes have been activated. No restarts are necessary’ is displayed.

7.2.3 JMS Modules Creation

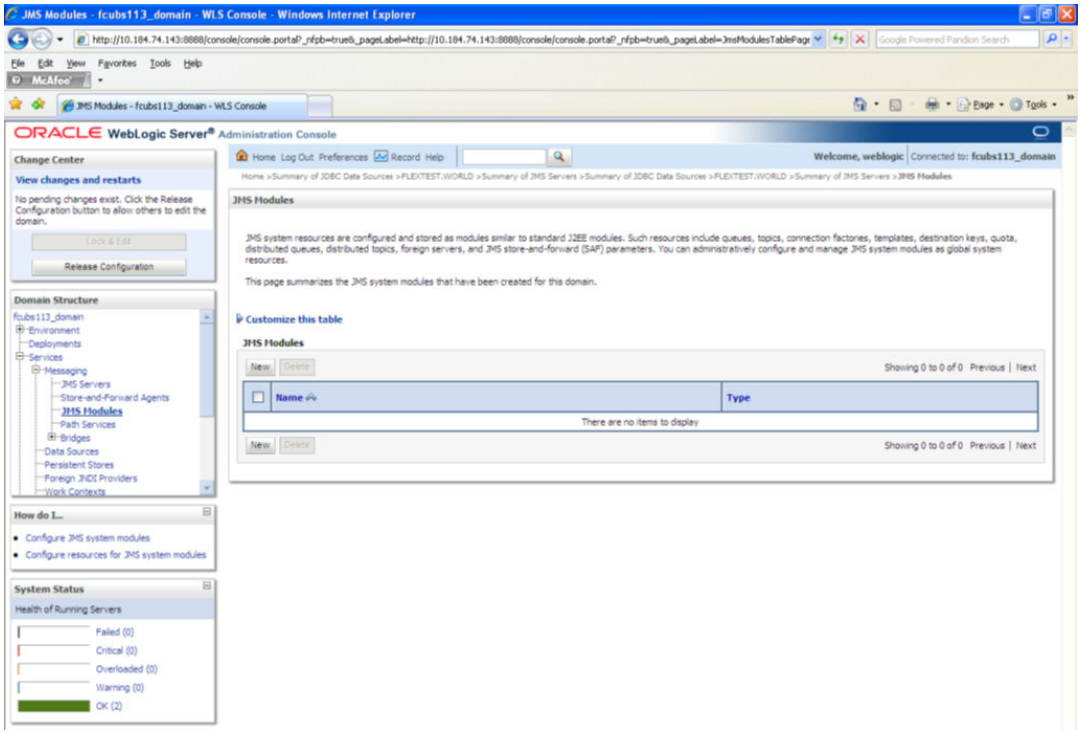
Follow the steps given below:

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

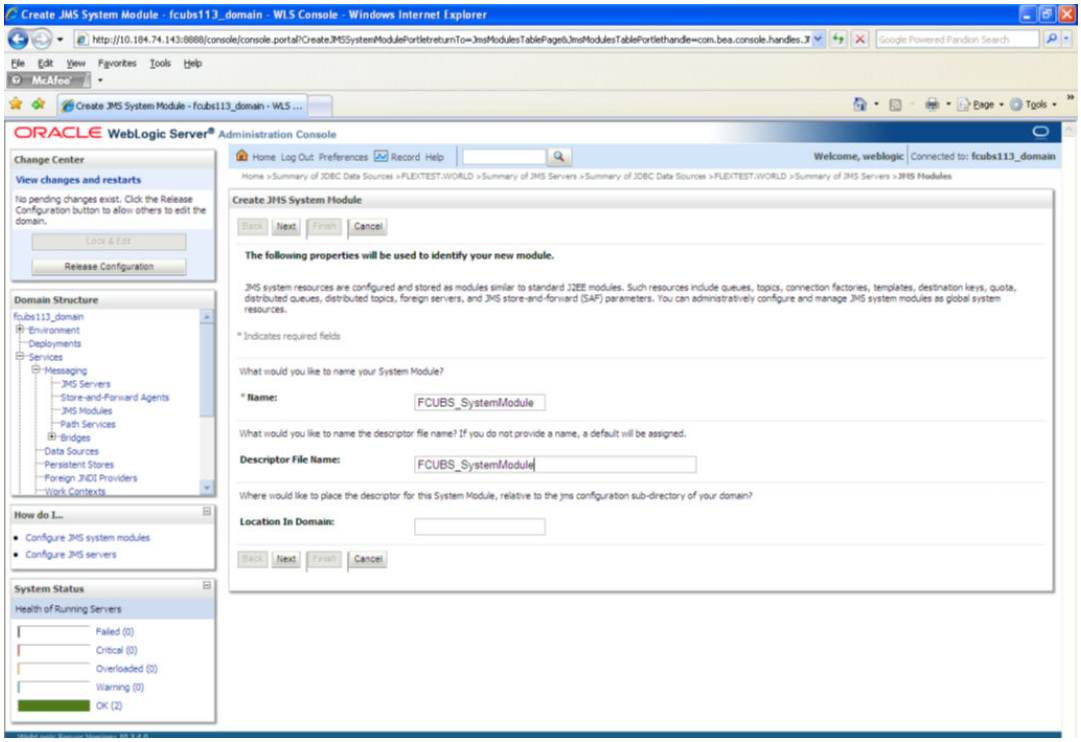
The following screen is displayed:



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



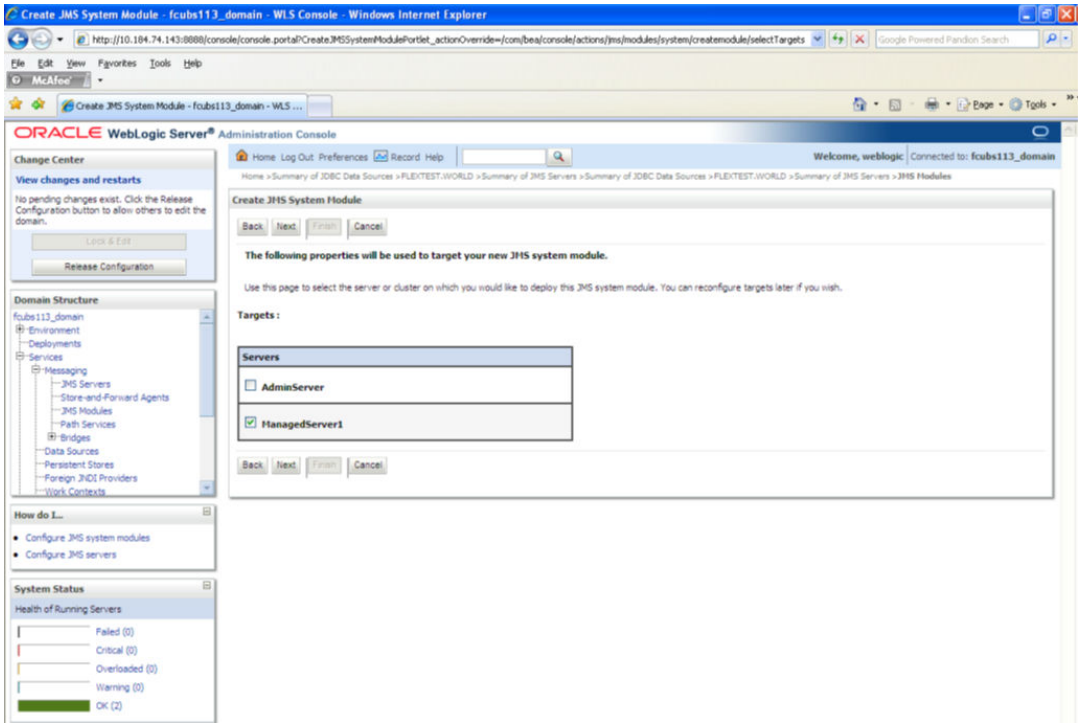
3. Click ‘New’ button. The following screen is displayed.



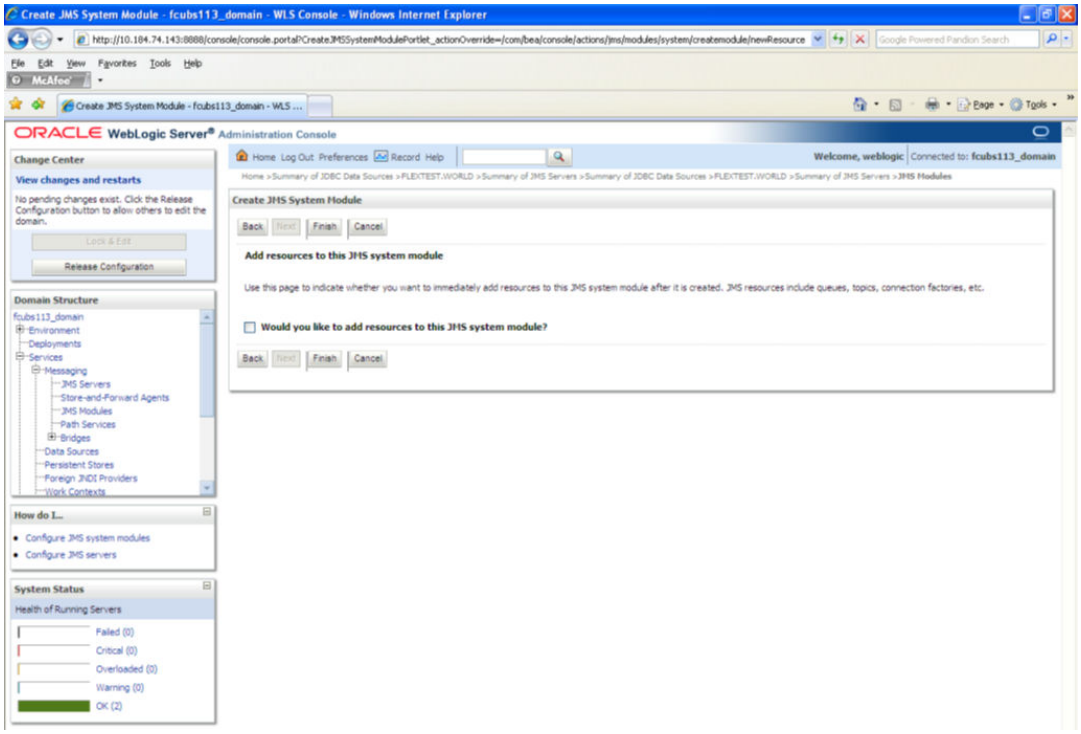
Enter the System Module Name as FCUBS_SystemModule.

Enter the Description File Name as FCUBS_SystemModule.

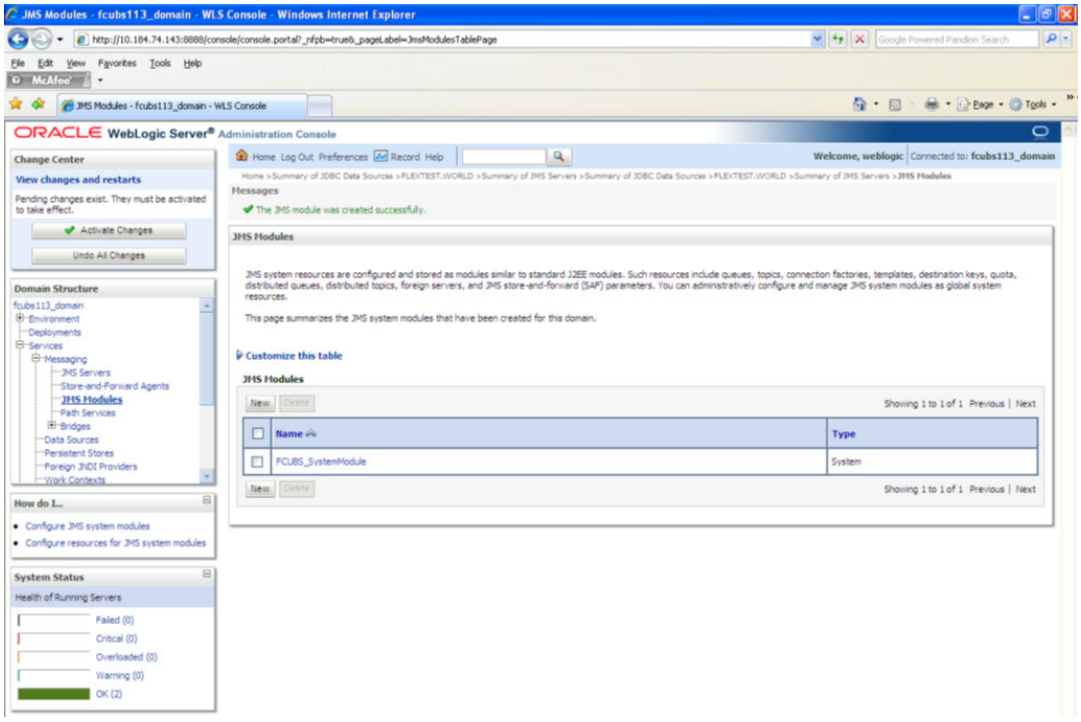
4. Click ‘Next’.
The following screen is displayed.



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

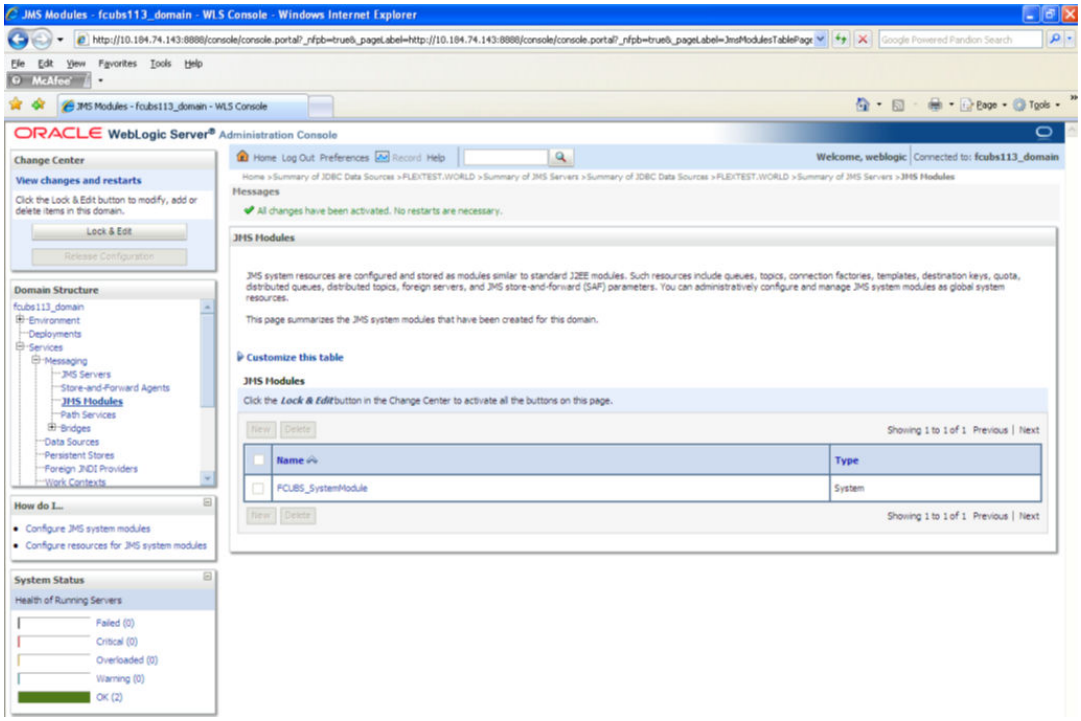


6. Click ‘Finish’ button. The following screen is displayed.



7. Click ‘Activate Changes’ button on the left pane.

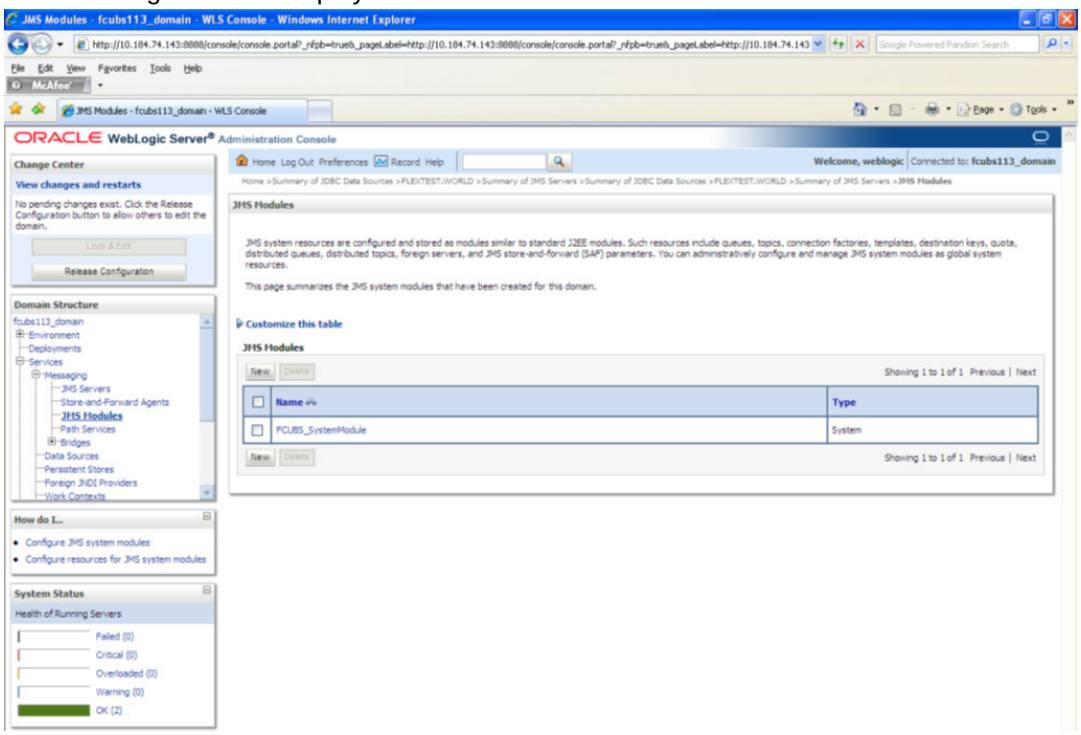
The message ‘All the changes have been activated. No restarts are necessary’ is displayed.



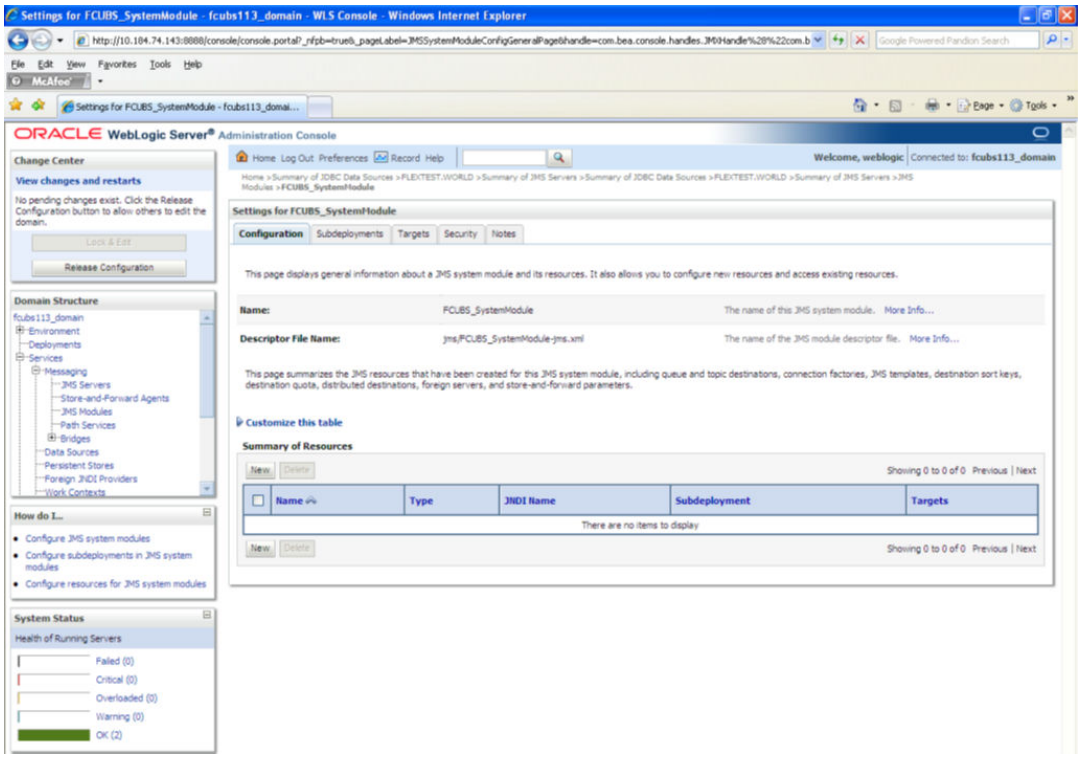
7.2.4 Subdeployment Creation

Follow the steps given below:

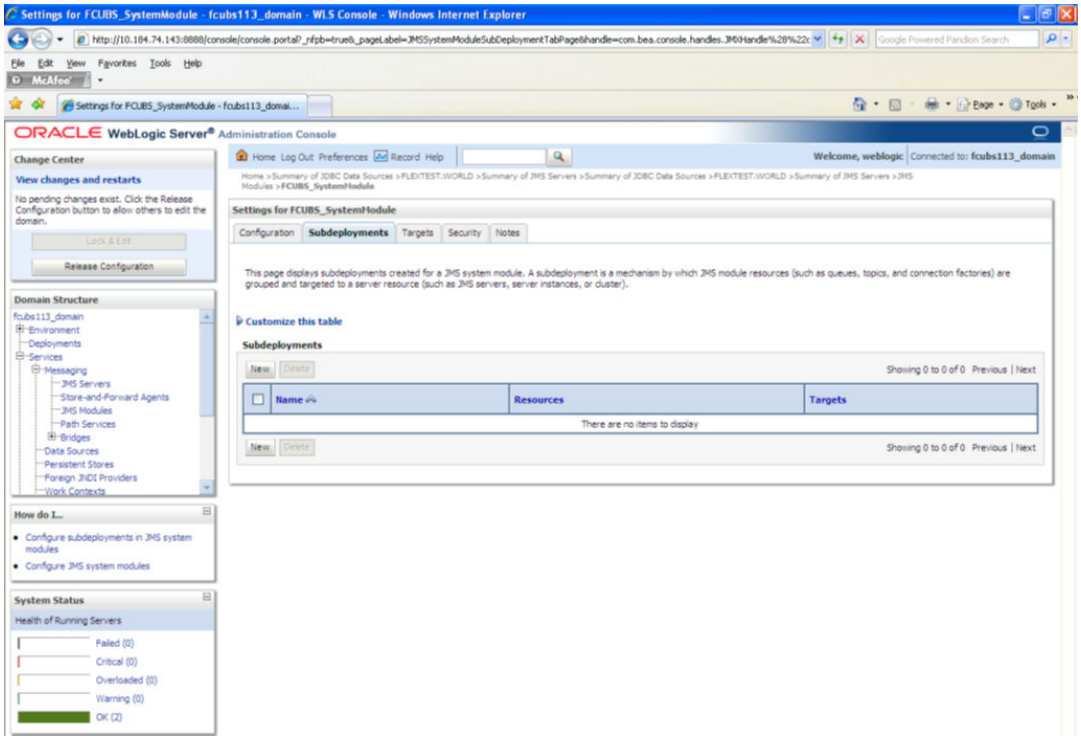
1. Navigate to the WEBLOGIC Home Page. Click ‘JMS Modules’ on domain structure by expanding ‘Messaging’.
   The following screen is displayed:



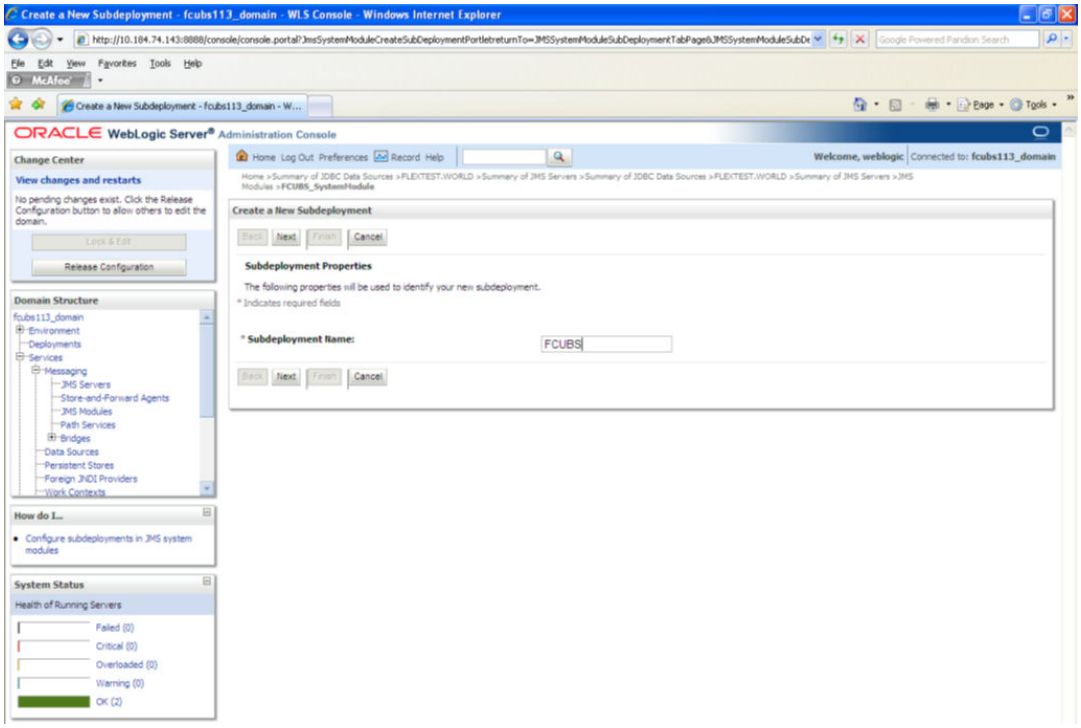
2. Click ‘Lock & Edit’ button.
3. Select the JMS module created earlier.



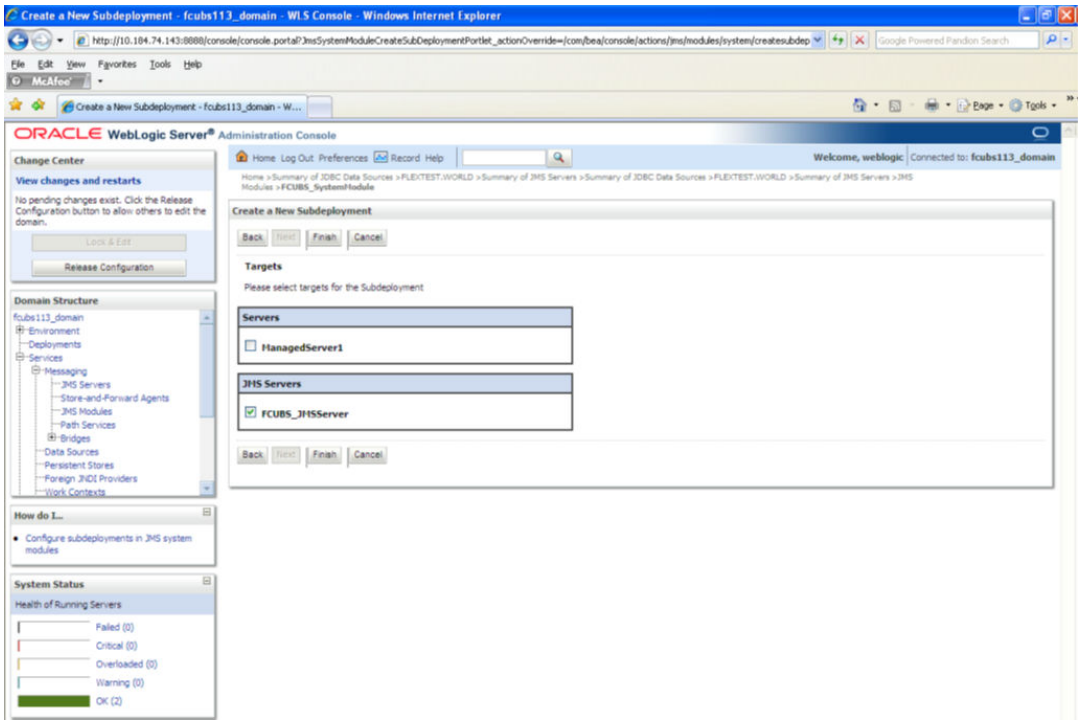
4. Click ‘Subdeployments’ tab.



5. Click ‘New’. The following screen is displayed.

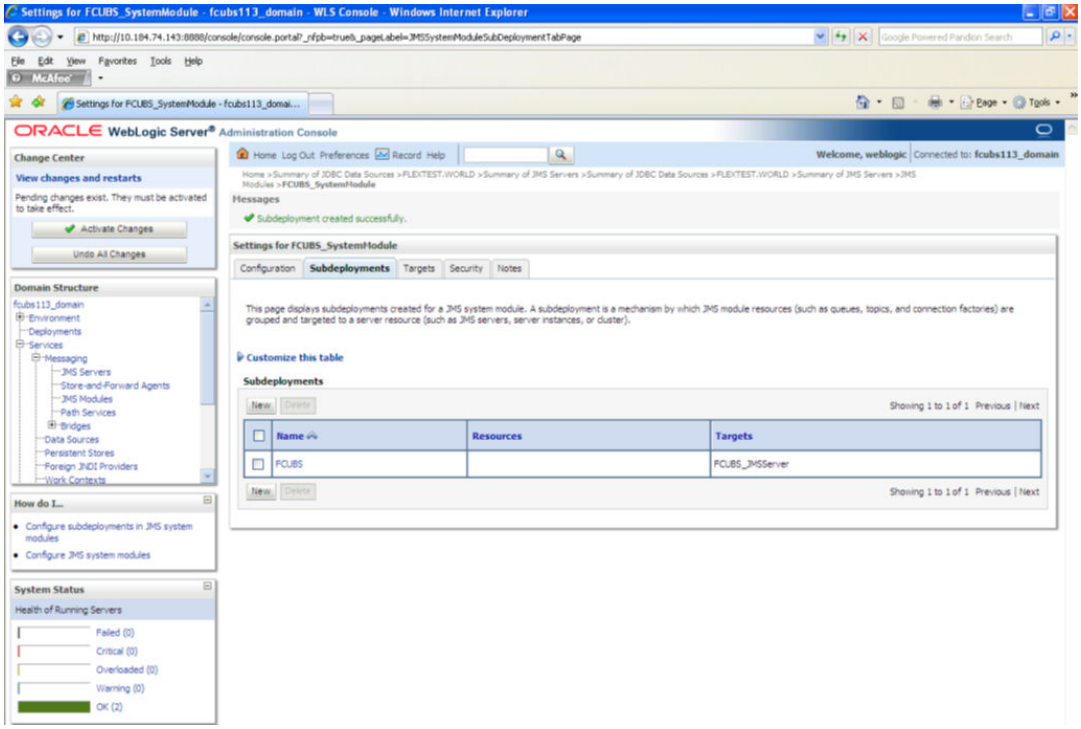


6. Specify the Subdeployment Name as ‘FCUBS’. Then click ‘Next’.
The following screen will be displayed.

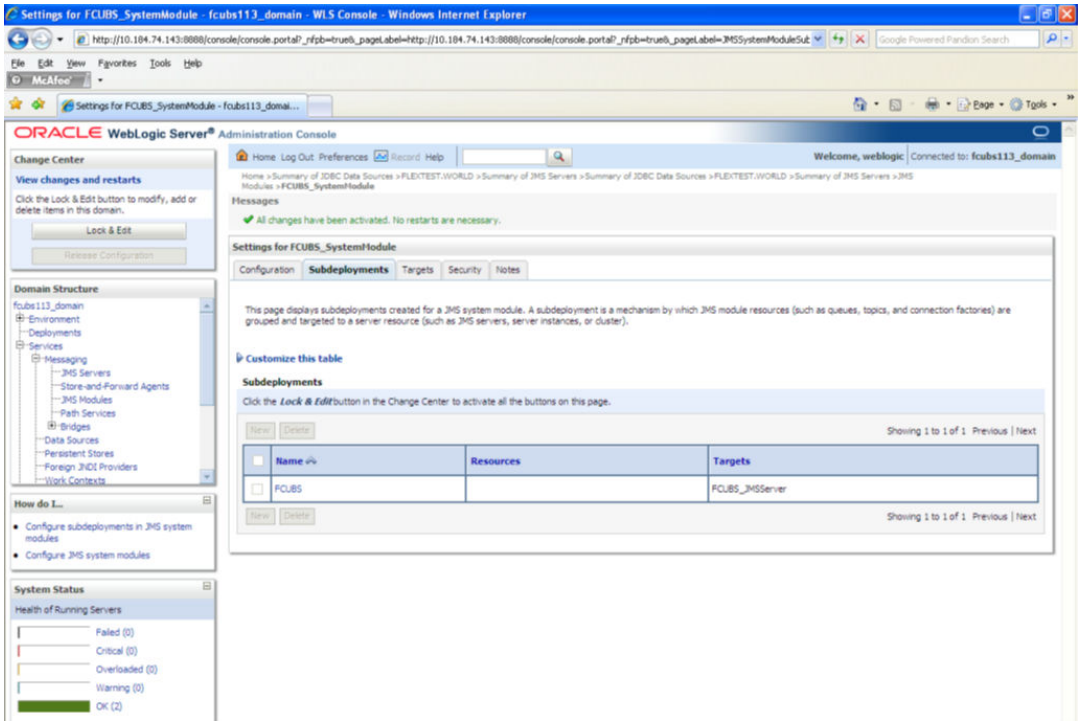


7. Select the JMS Server (as created by the user).
8. Click ‘Finish’ button.

9. Following screen is displayed.

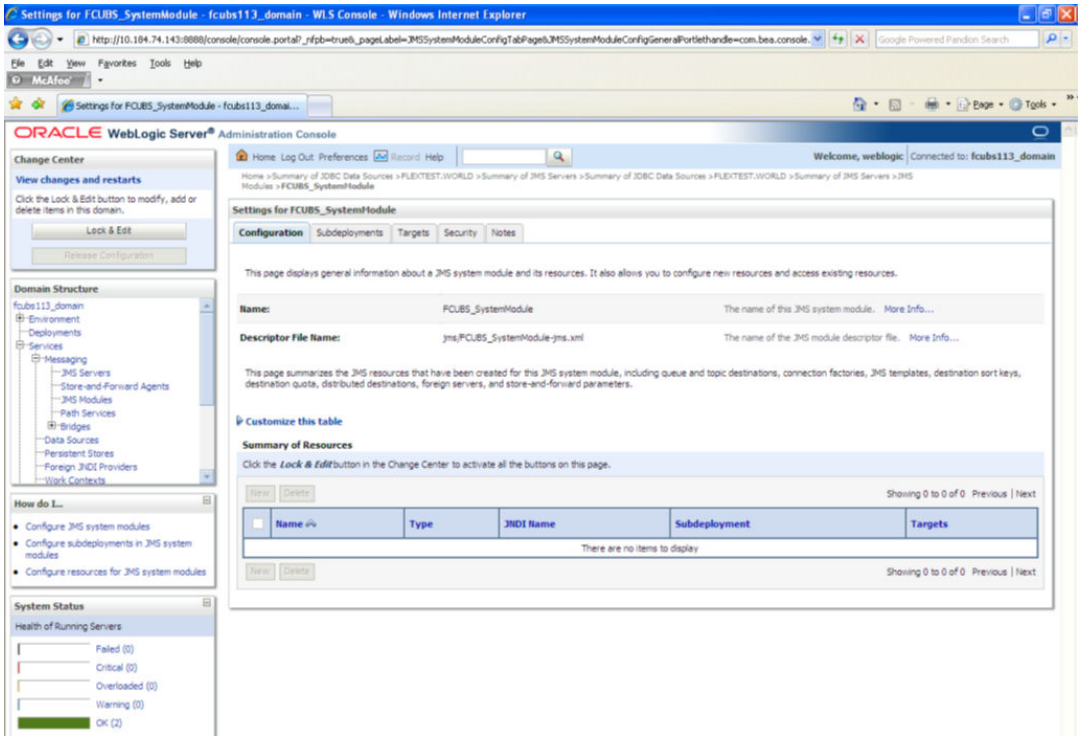


10. Click ‘Activate Changes’. Following screen is displayed.

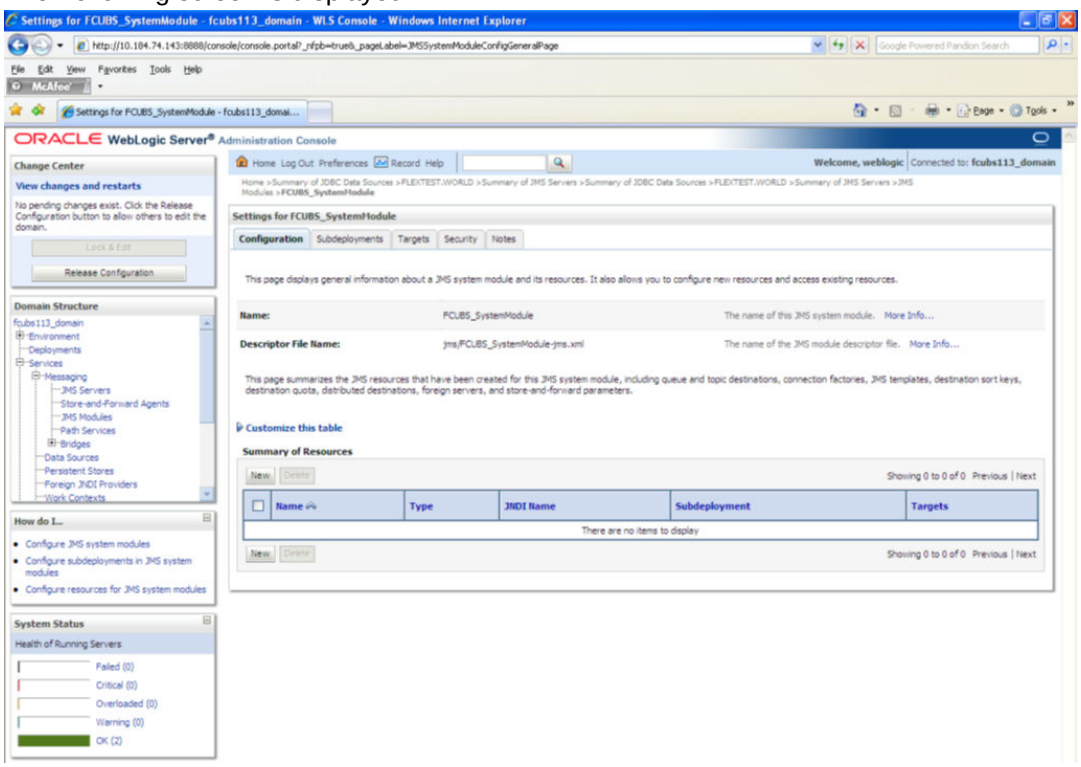


7.2.5 JMS Queue Creation

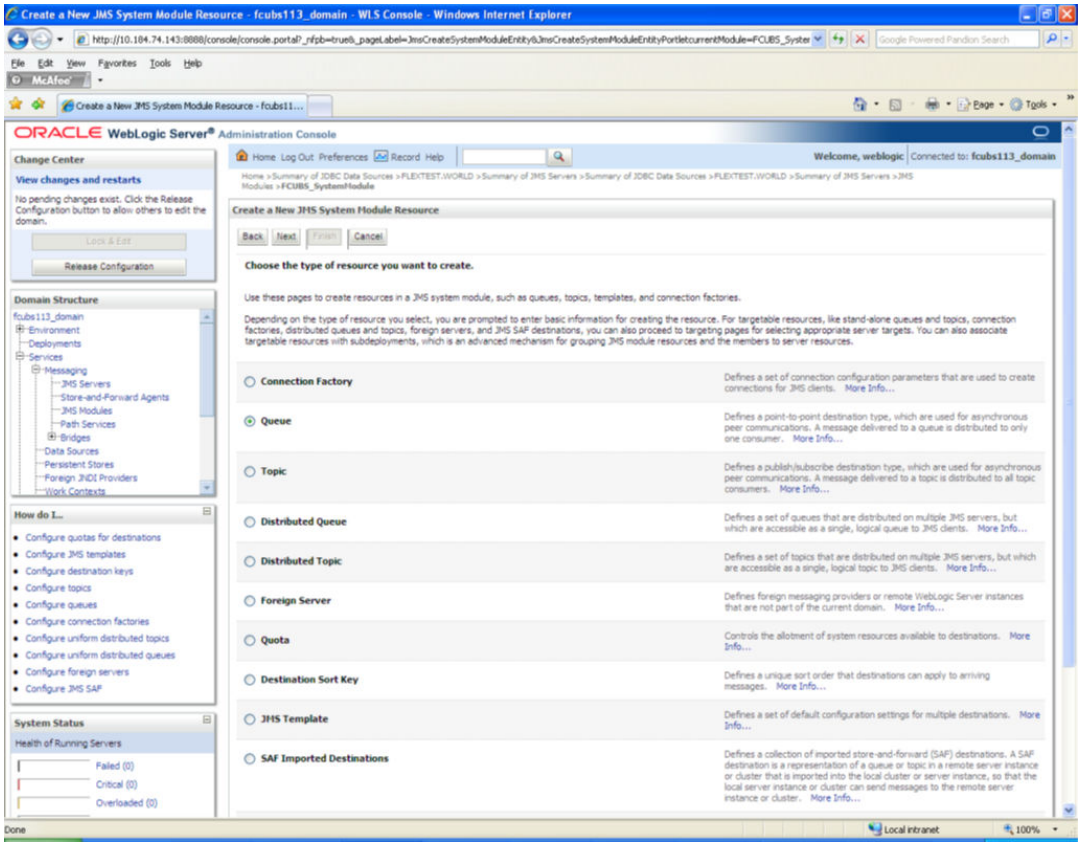
1. Select the JMS Module created earlier.



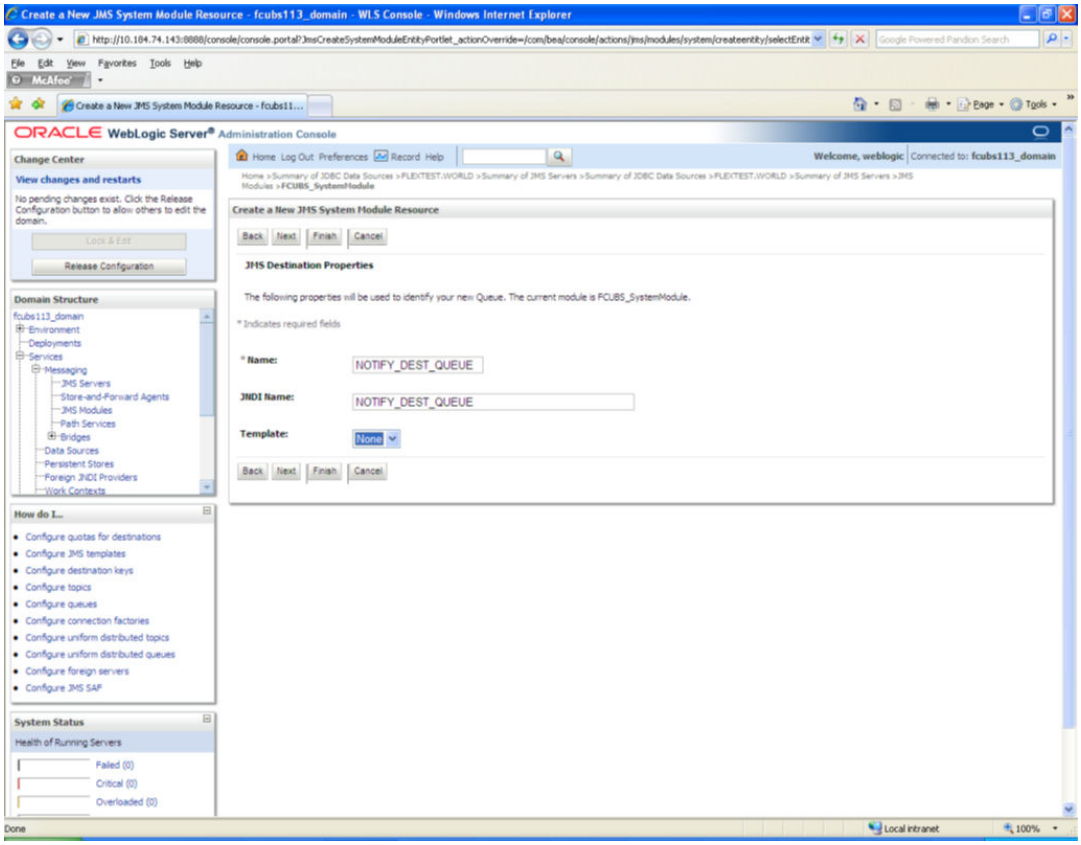
2. You need to set the configuration for FCUBS_SystemModule is to be set.
3. Click ‘Configuration’. Then click ‘Lock & Edit’.
   The Following screen is displayed.



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



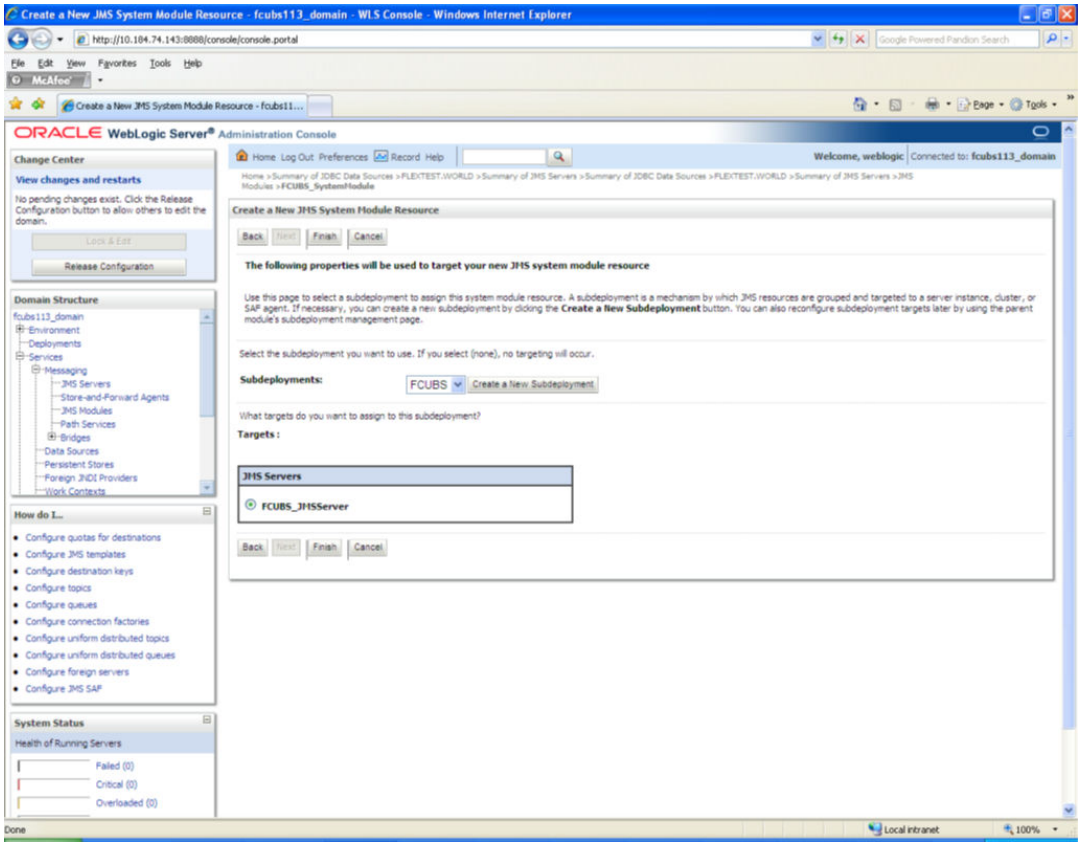
5. Select the ‘Queue’ option. Then click ‘Next’.



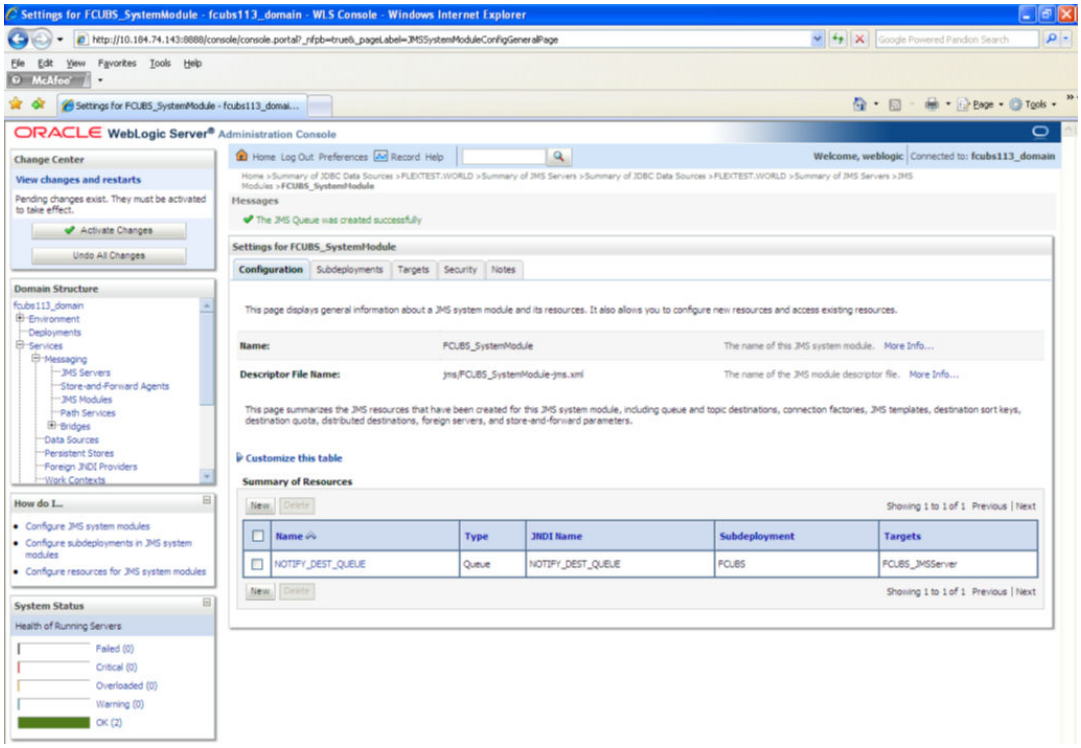
For creating new JMS System Module Resources, follow the steps given below:

- 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’.

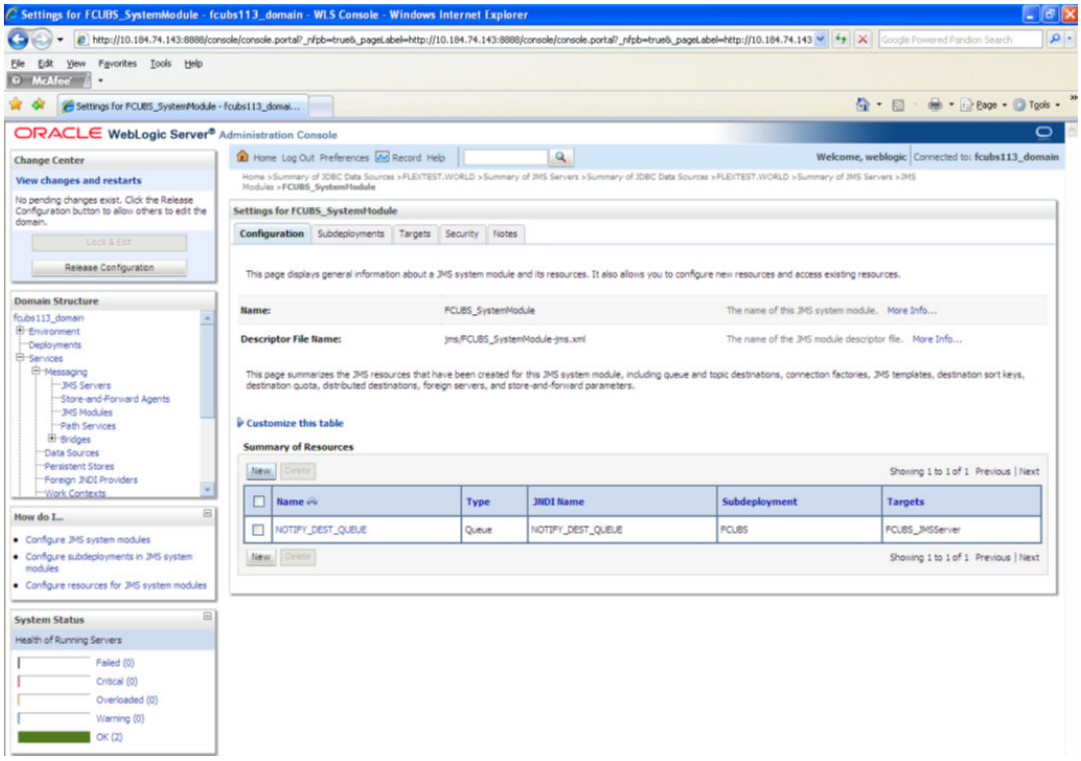
Following screen is displayed.



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



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

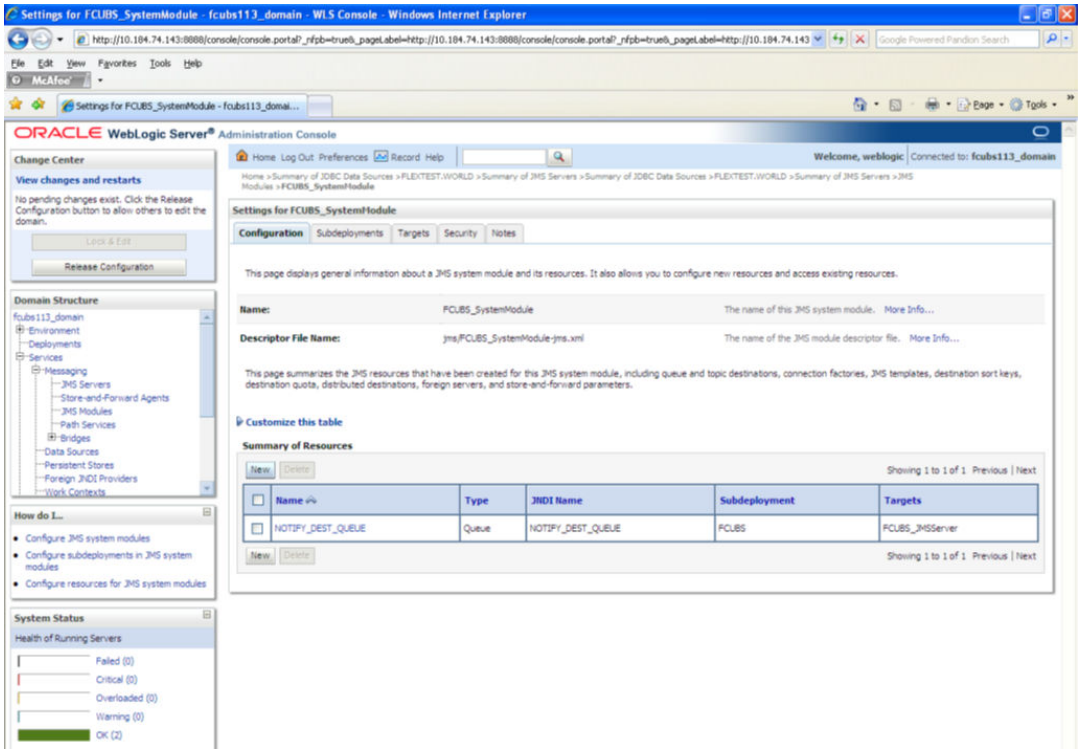


8. Click ‘New ‘to create more Queues. You may follow the same steps to create other queues.

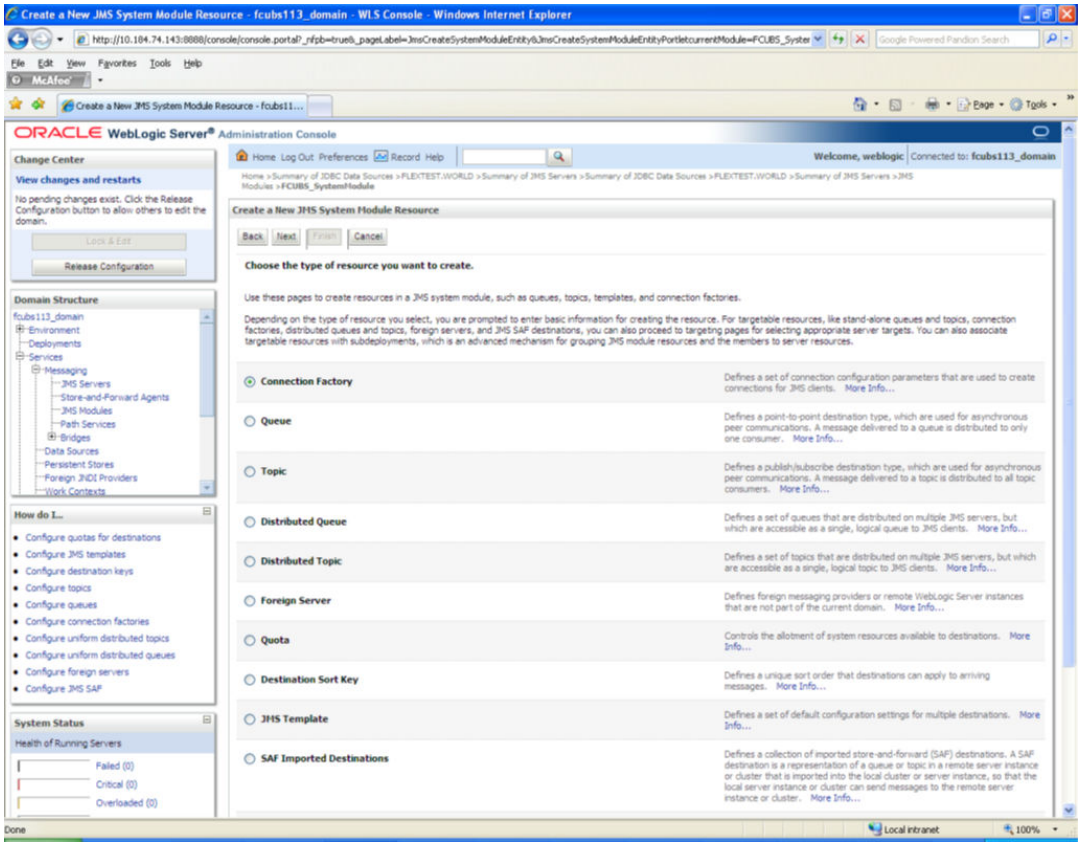
7.2.6 JMS Connection Factory Creation

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

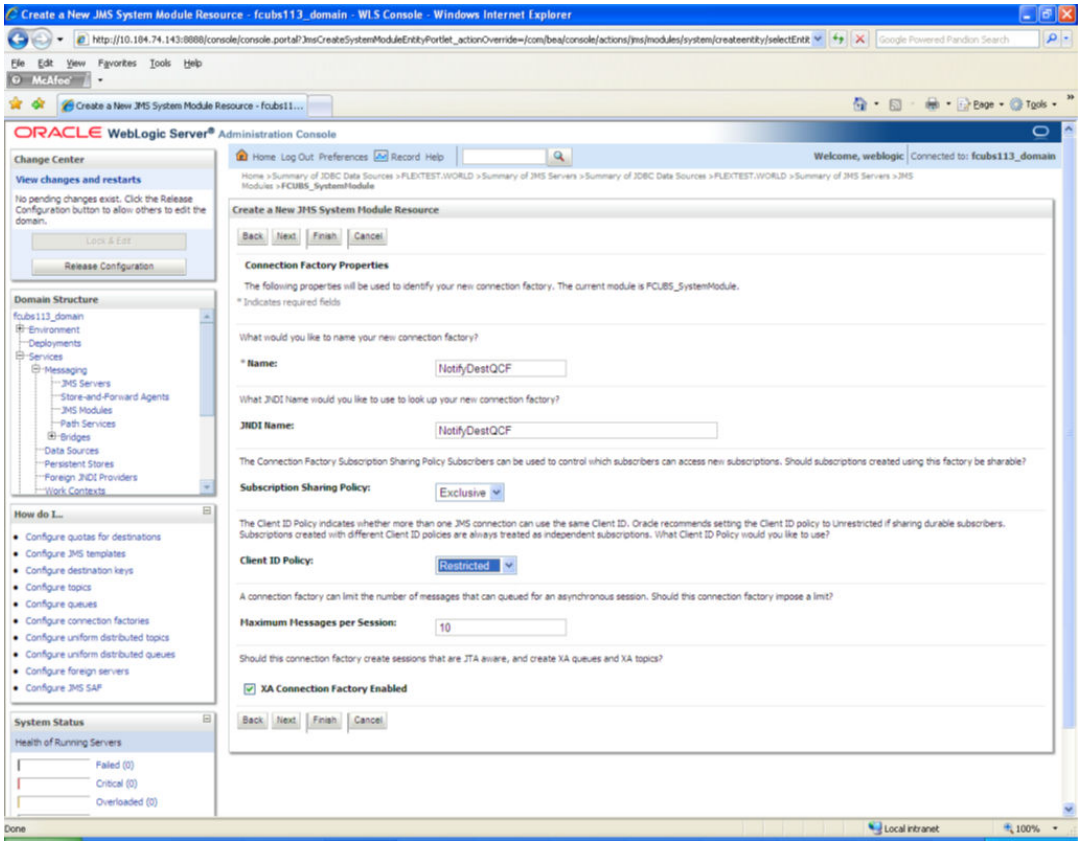
1. Click ‘New’.



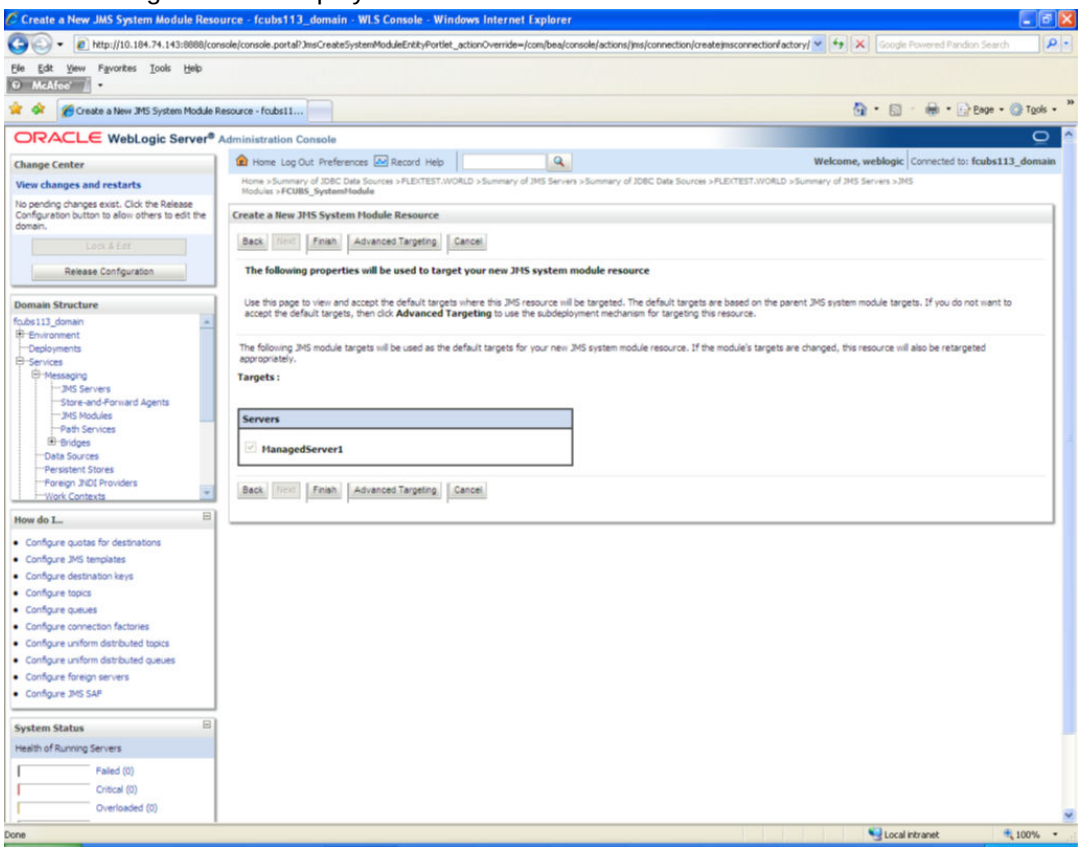
The following screen is displayed:



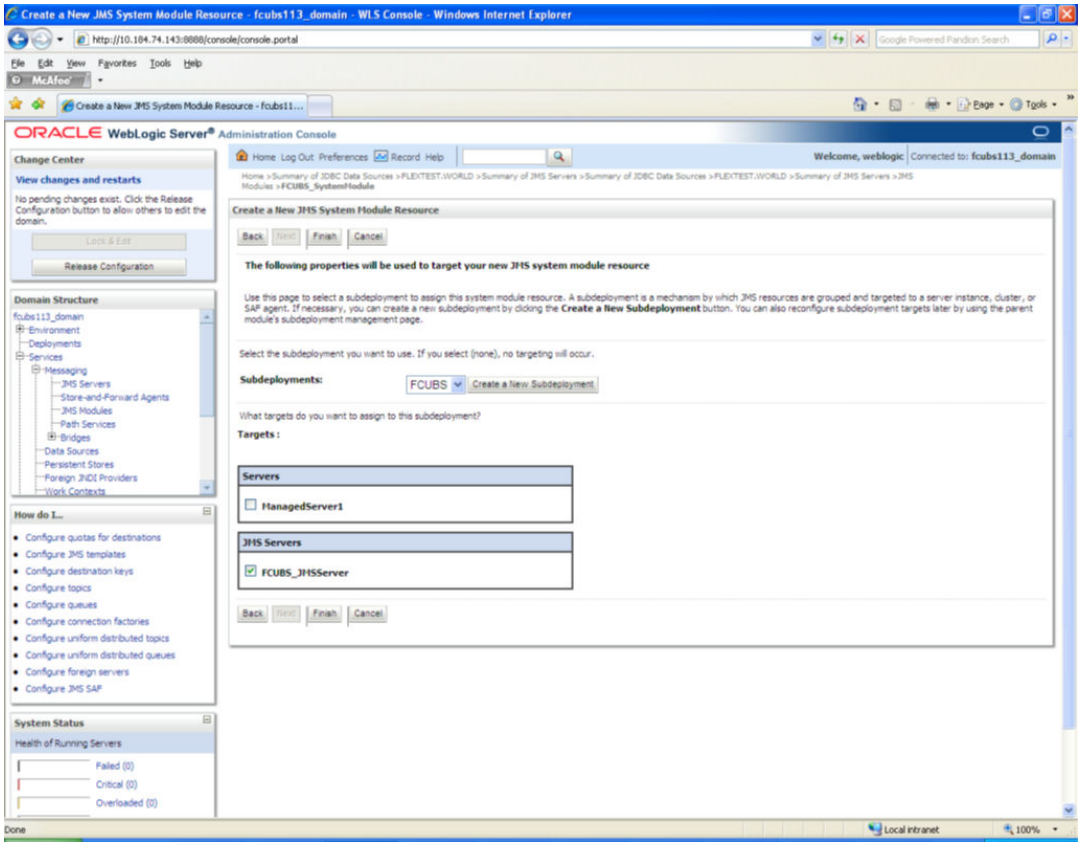
2. Select ‘Connection Factory’. Click ‘Next’.



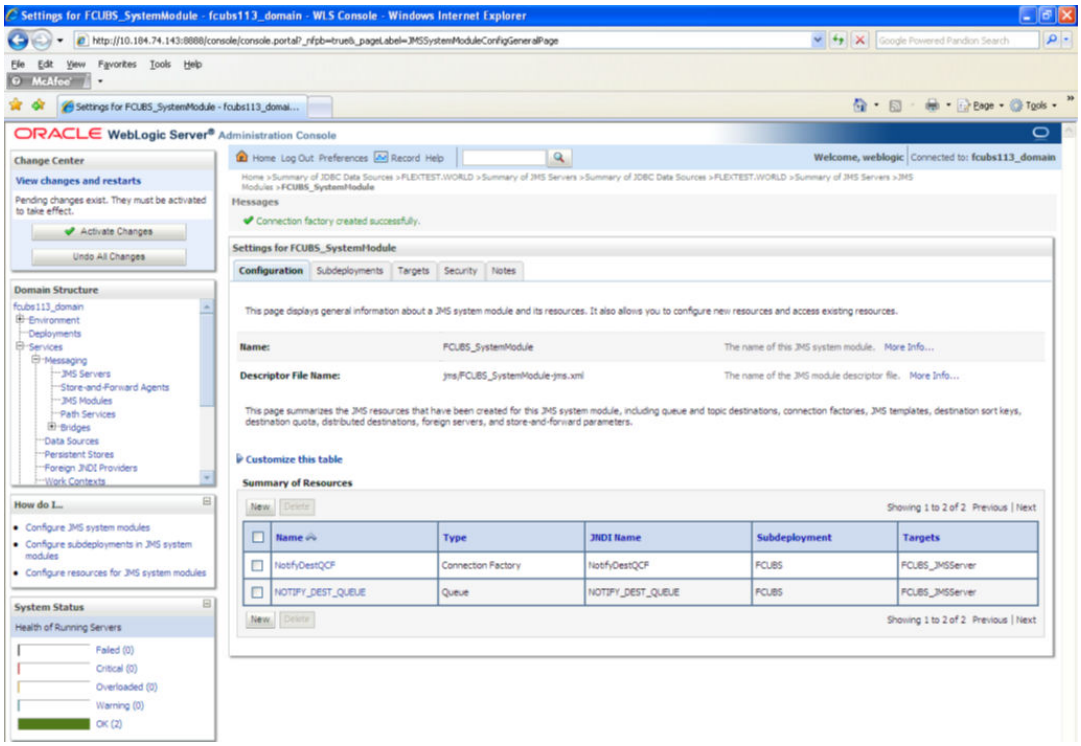
3. Enter the Name of the Connection Factory as ‘NotifyDestQCF’.
4. Enter the JNDI Name as ‘NotifyDestQCF’.
5. Check the box ‘XA Connection Factory Enabled’.
6. Click ‘Next’.
   The following screen is displayed:



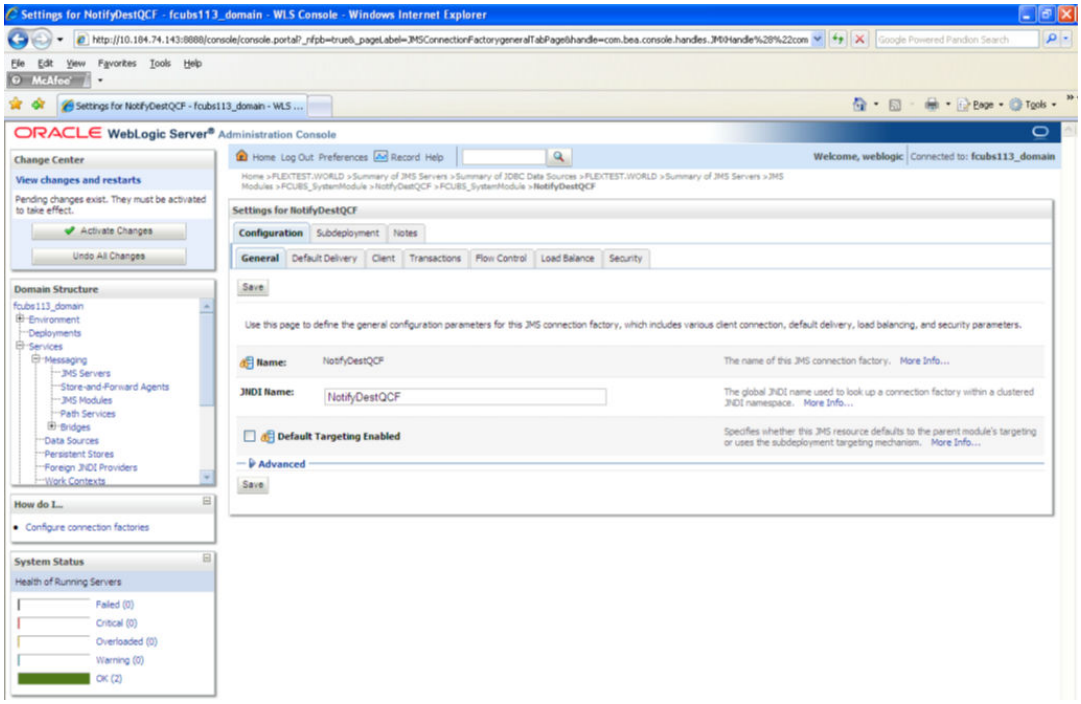
7. Click ‘Advanced Targeting’. The following screen is displayed.



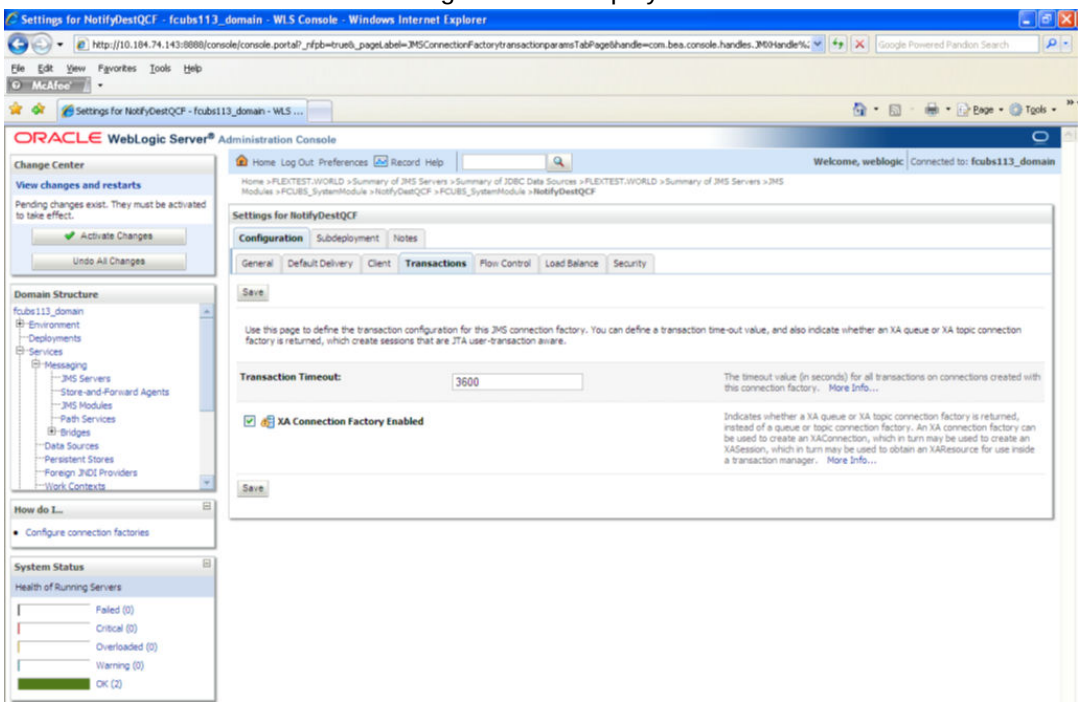
8. Select the ‘Subdeployments’ as FCUBS.
9. Under JMS Servers, check the box against ‘Managed Server’.
10. Click ‘Finish’. The following screen is displayed:



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.

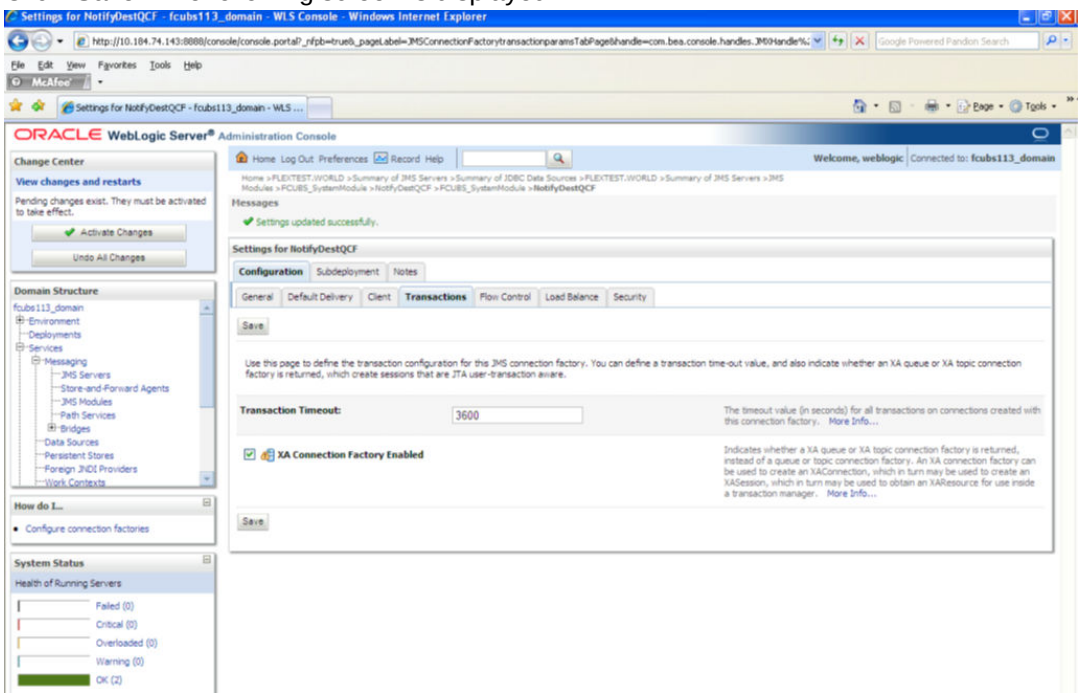


13. Click ‘Transactions’ Tab. The following screen is displayed.



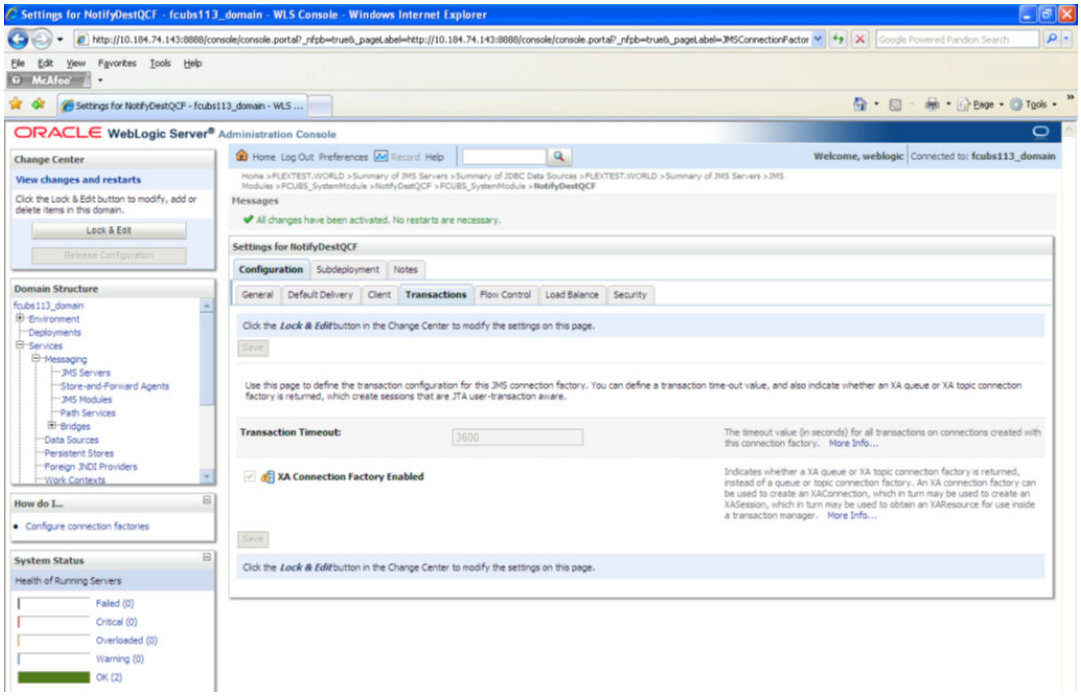
14. Check the box ‘XA Connection Factory Enabled’.

15. Click ‘Save’. The following screen is displayed.



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.



7.3 Configuring Weblogic for PMGateway

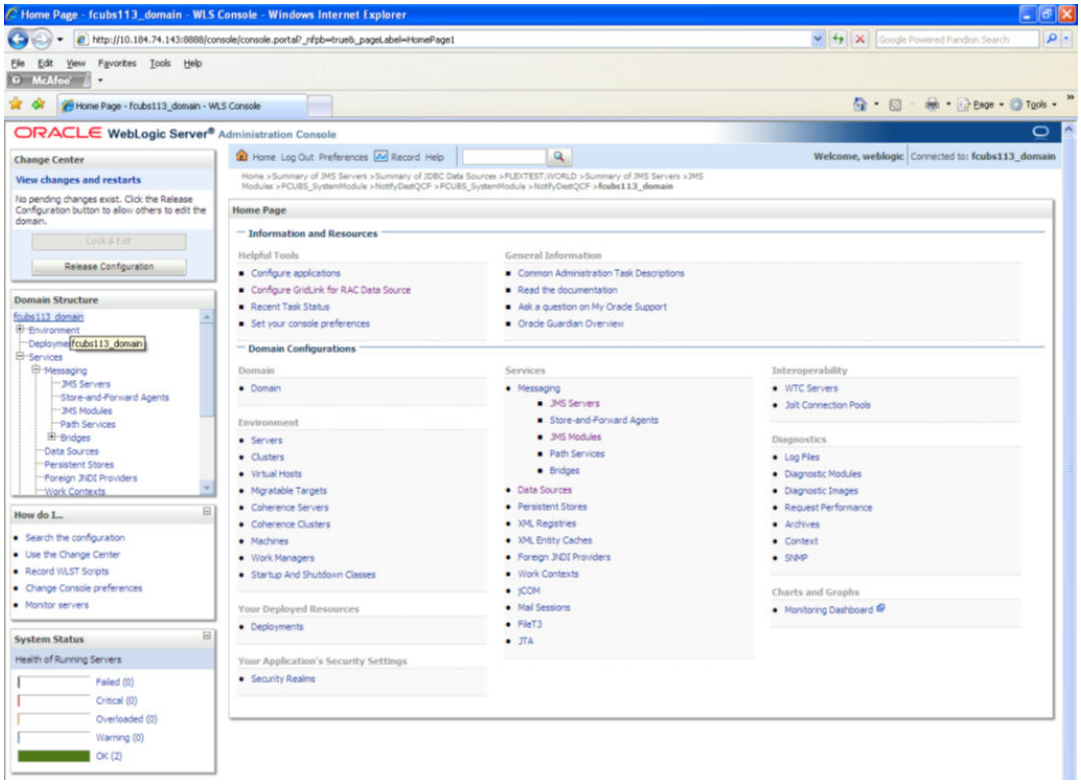
To deploy and run PMGateway application in weblogic server following configuration needs to be done

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

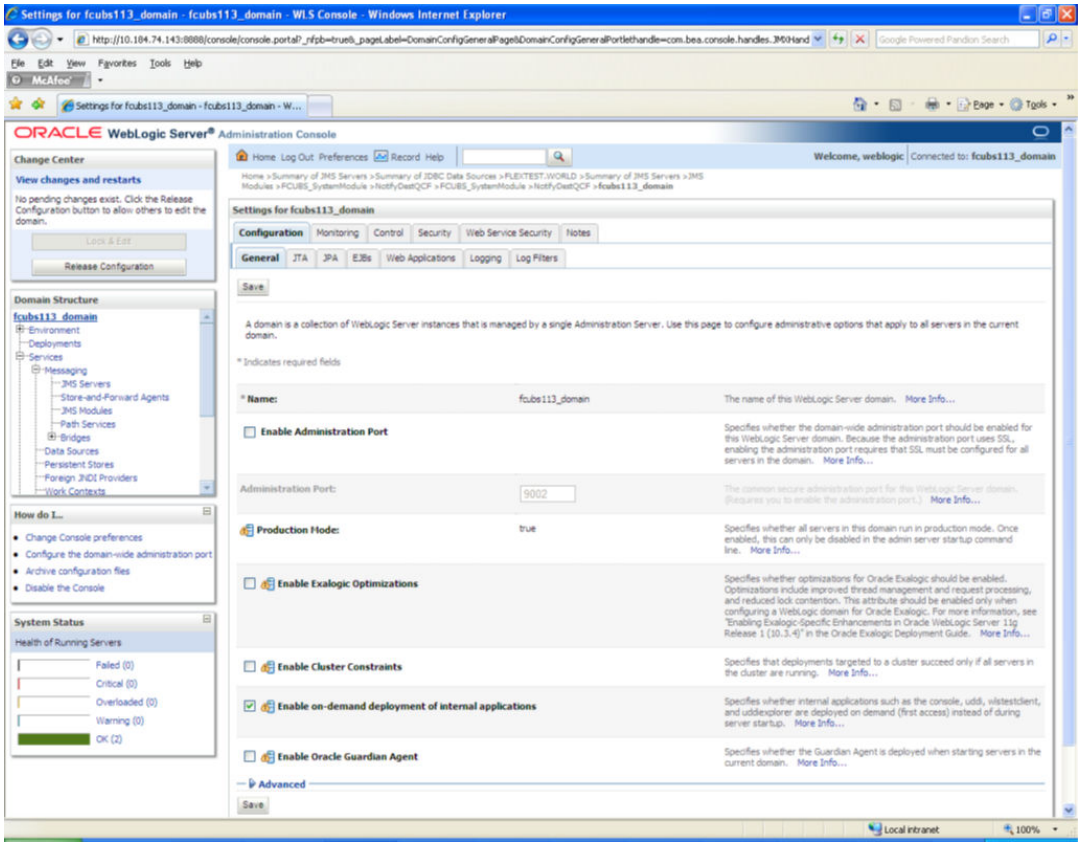
7.4 Configuring Weblogic for Oracle Banking Trade Finance

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

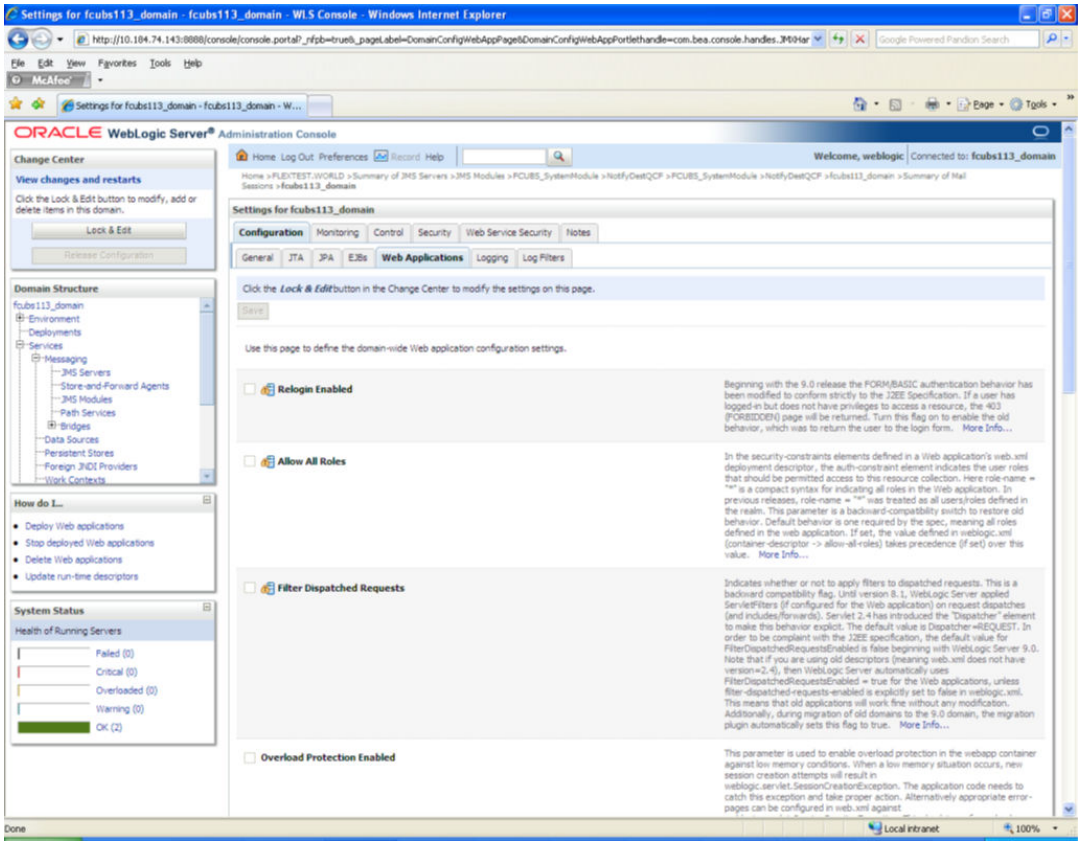
1. Select the domain from the domain structure as shown below. (Eg: fcubs113_domain).



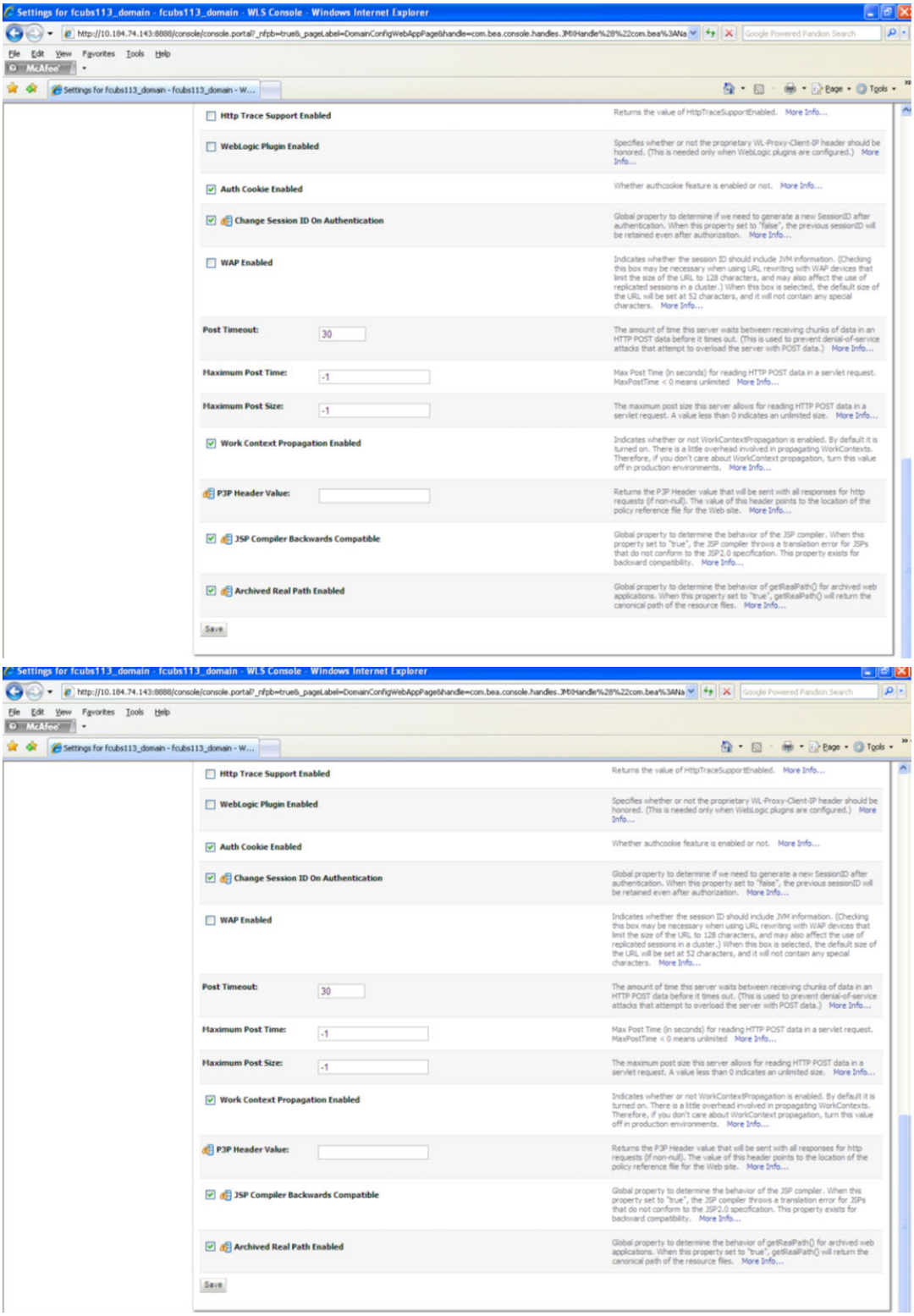
The following screen is displayed:



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



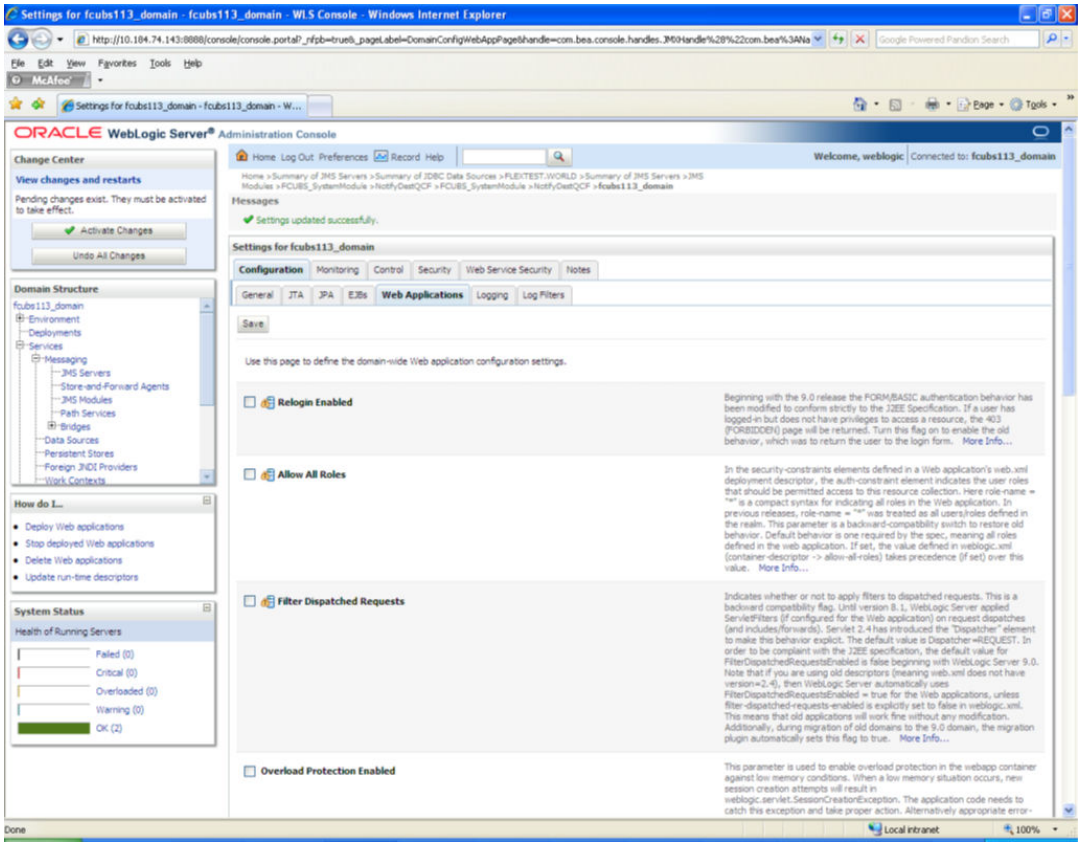
3. Scroll down and ensure that the details are as shown in the figure. The remaining portion of the screen is given below:



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

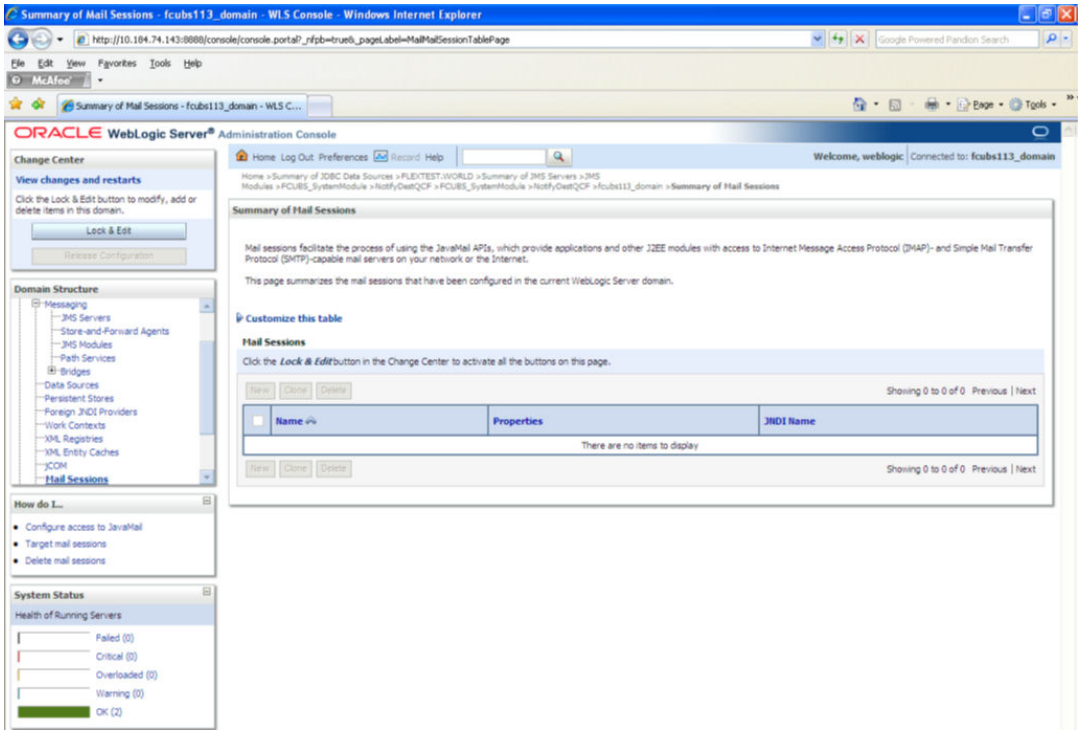
This section describes the set of configurations changes required in Oracle Weblogic Server when Oracle Banking Trade Finance is configured to generate and send passwords to users via e-mail.

- Creating JavaMail Session
- Configuration of the TLS/SSL Trust Store for Weblogic Server

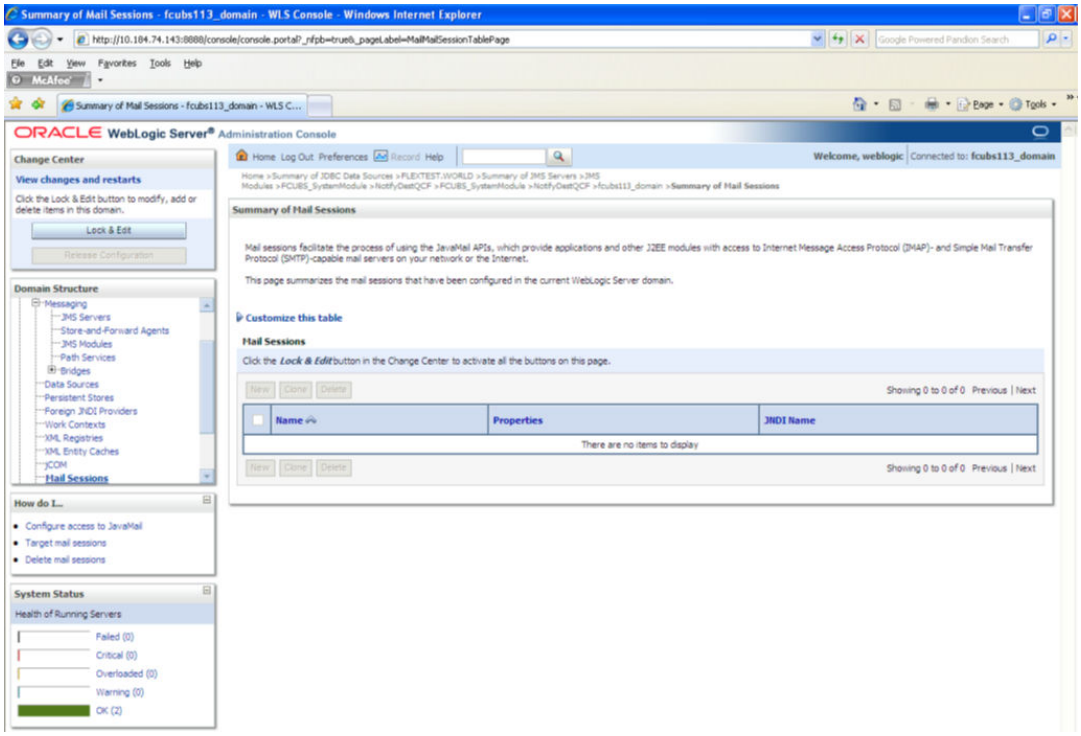
7.5.1 Creating JavaMail Session

To configure mail session, follow the steps below.

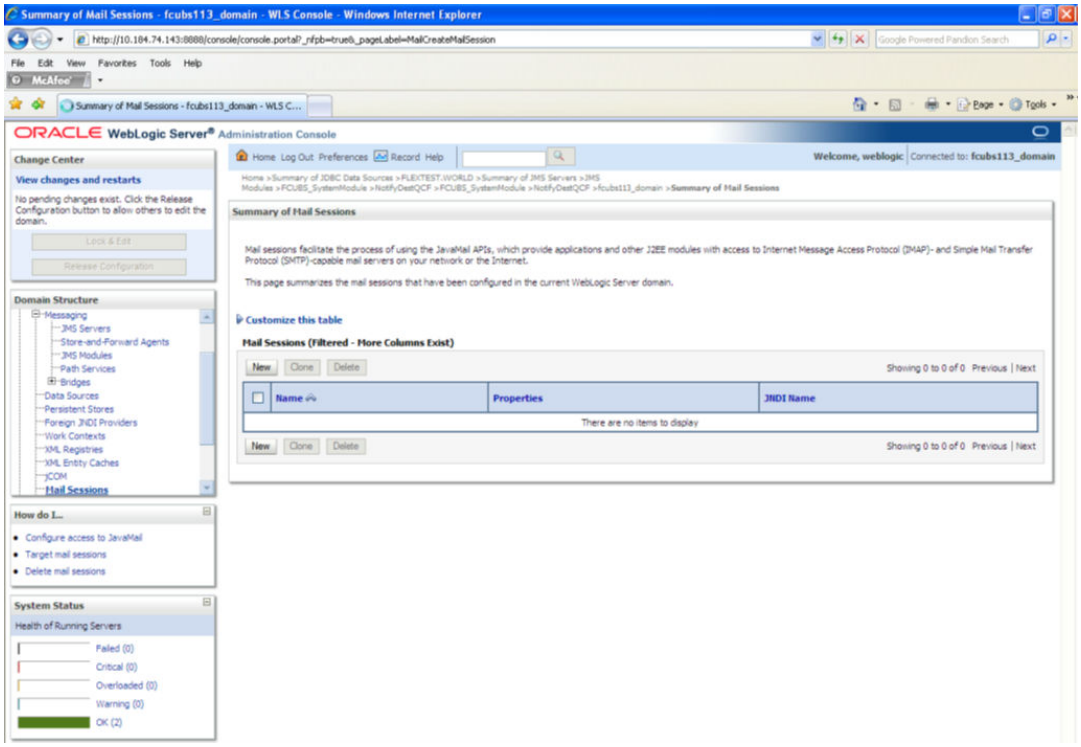
1. Expand ‘Services’ on the left pane of the application server. Click ‘Mail Sessions’.



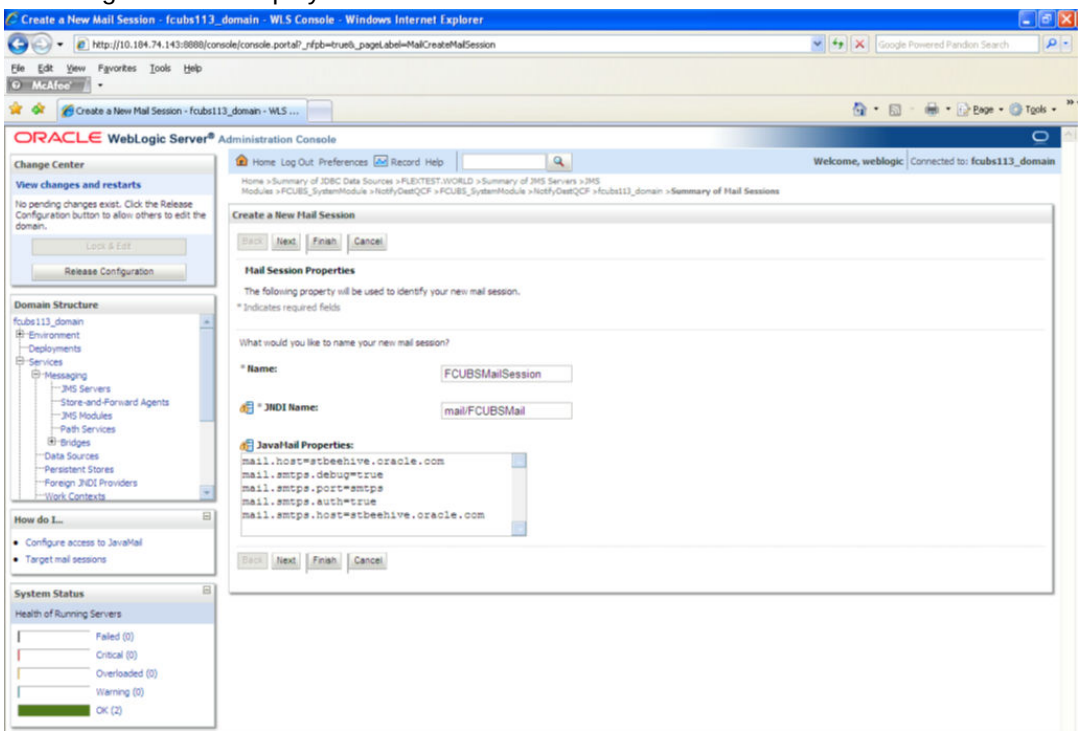
2. Click ‘Lock & Edit’.



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>

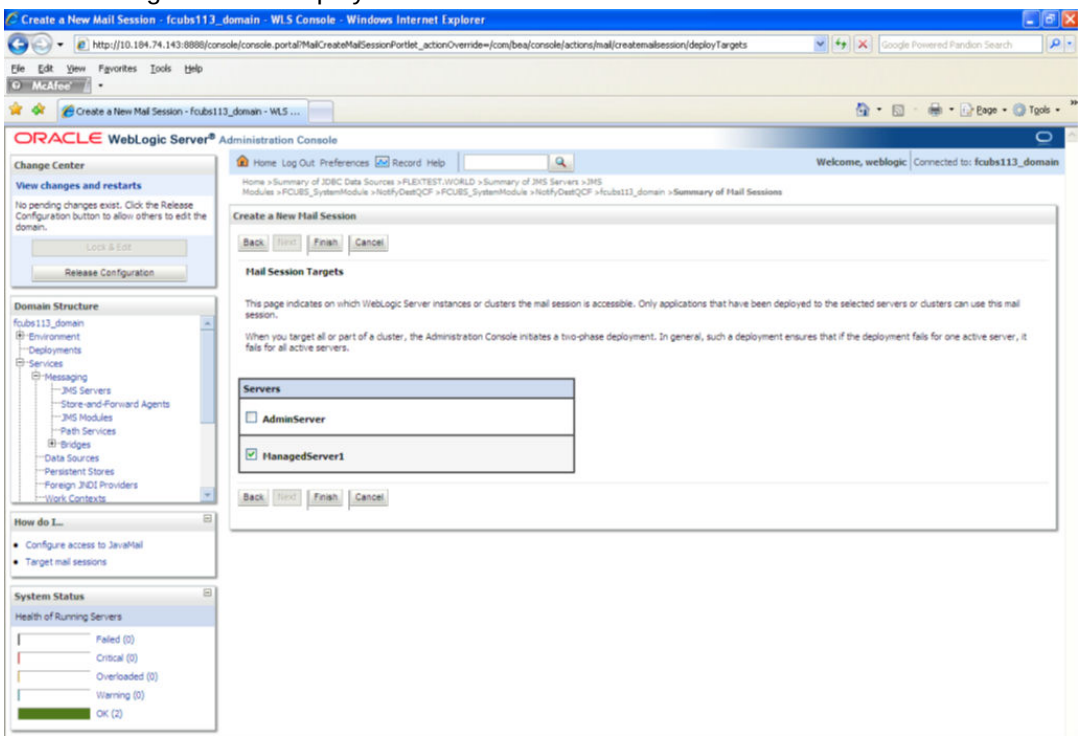
Eg: smtps

mail.smtps.auth=true

mail.smtps.host==<HOST_SMTPS_MAIL_SERVER>

Eg: samplename.mail.com

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



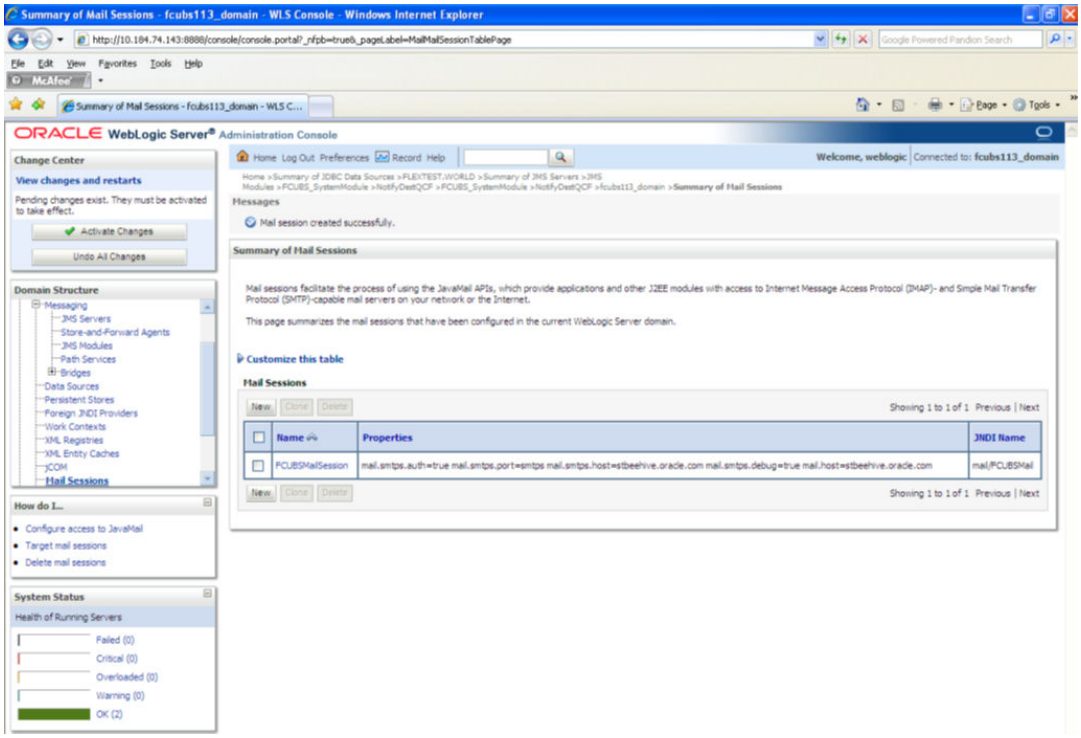
7. Check the box against the required servers and click ‘Finish’ to complete the configuration.

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

- SMTP_HOST
- SMTP_USER
- SMTP_PASSWORD
- SMTP_JNDI

This can be achieved using the Oracle Banking Trade Finance Installer.

8. Click ‘Active Changes’ button to activate the current mail session settings.



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

As described in the previous section, Oracle Banking Trade Finance 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 Banking Trade Finance 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 Banking Trade Finance 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).