Oracle® Banking Corporate Lending

Weblogic Configuration

Release 14.7.6.0.0
G32296-01
April 2025

ORACLE

Oracle Banking Corporate Lending Weblogic Configuration, Release 14.7.6.0.0

G32296-01

Contents

Preface

This topic contains the following sub-topics:

Purpose

This guide is designed to help acquaint you to configure SSL on Oracle Weblogic application server. This guide helps the user with the installation of Oracle Banking Application.

Audience

This manual is intended for the following User/User Roles:

Table 1 Audience

Role	Function
Administrator	Who controls the system and application parameters and ensures smooth functionality and flexibility of the banking application.
Implementation team	Implementation of Oracle Banking Corporate Lending Solution
Pre-sales team	Install Oracle Banking Corporate Lending for demo purpose
Bank personnel	Who installs Oracle Banking Corporate Lending

The user of this manual is expected to have basic understanding of Oracle Banking Application installation.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://www.oracle.com/corporate/accessibility/.

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.

Related Resources

For more information on any related features, refer to the following documents:

- Oracle Banking Corporate Lending User Guides.
- Oracle Banking Corporate Lending Installation Guides.

Conventions

The following text conventions are used in this document:

Table 2 Conventions

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
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.

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.

Acronyms and Abbreviations

The list of the acronyms and abbreviations used in this guide are as follows:

Table 3 Acronyms and Abbreviations

Abbreviation	Description
CA	Certificate Authority
CSR	Certificate Signing Request
CN	Common Name
DN	Distinguished name
HTTP	Hypertext Transfer Protocol
JDBC	Java Database Connectivity
JDK	Java Development Kit
JKS	Java keystore
JNDI	Java Naming and Directory Interface
JRE	Java Runtime Environment
OHS	Oracle HTTP Server
RSA	Rivest–Shamir–Adleman
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security

1

Configure SSL on Oracle Weblogic

This topic contains the following sub-topics:

- Set up SSL on Oracle Weblogic
  This topic describes tasks to set up SSL on Oracle Weblogic application server.
- Certificates and Keypairs
  This topic explains the certificates and keypairs used for validating the authenticity of the server.

1.1 Set up SSL on Oracle Weblogic

This topic describes tasks to set up SSL on Oracle Weblogic application server.

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

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

1.2 Certificates and Keypairs

This topic explains the certificates and keypairs used for validating the authenticity of the server.

Certificates are used for validating the authenticity of the server. Certificates contain the name of the owner, certificate usage, duration of validity, resource location, or distinguished name (DN), which includes the common name (CN - website address or e-mail address depending on the usage) and the certificate ID of the person who certified (signs) this 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 key tool 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, the 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 the Oracle Weblogic server to configure SSL.

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

2

Choose the Identity and Trust Stores

This topic explains to choose the identity and trust stores.

Oracle Financial Services Software recommends that the choice of Identity and Trust stores be made upfront. 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 are located in the `JAVA_HOME/jre/lib/security` directory. It is highly recommended to change the default Java standard trust store password from `change the password` (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 to the Oracle Weblogic Server documentation on Securing Oracle Weblogic Server.

3
Obtain the Identity Store

This topic contains the following sub-topics:

- Create Identity Store with Self-Signed Certificates
  This topic describes the creation of identity store along with Self-signed certificates.
- Create Identity Store with Trusted Certificates Issued by CA
  This topic explains to create identity store with trusted certificates issued by CA.

3.1 Create Identity Store with Self-Signed Certificates

This topic describes the creation of identity store along 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.

To create a self-signed certificate, the genkey pair option provided by the keytool utility of Sun Java 6 needs to be utilized.

This topic contains the following sub-topic:

- Creation of Self-Signed Certificate
  This topic describes the creation of self-signed certificate.

3.1.1 Creation of Self-Signed Certificate

This topic describes the creation of self-signed certificate.

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

Table 3-1 Attributes of the certificate and Keystore

Attributes	Description
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.

Table 3-1 (Cont.) Attributes of the certificate and Keystore

Attributes	Description
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 the Oracle Weblogic Server.
First and Last Name (CN)	Enter the domain name of the machine used to access Oracle Banking Corporate Lending, for instance, www.example.com
Name of your Organizational Unit	The name of the department or unit making the request, for example, BPD. Use this field to identify the SSL Certificate you are creating, for example, by department or by the physical server.
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.
Name of your City or Locality	The city in which your organization is physically located, for example, Mumbai.
Name of your State or Province	The state/province in which your organization is physically located, for example, Maharashtra.
Two-Letter Country Code for this Unit	The country in which your organization is physically located, for example, US, UK, IN, etc.

Note:

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 the Oracle Weblogic Server.

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 Create Identity Store with Trusted Certificates Issued by CA

This topic explains to create identity store with trusted certificates issued by CA.

This topic contains the following sub-topics:

- Creation of Public and Private Key Pair
  This topic provides the detailed information on creation of public and Private Key Pair.
- Generate CSR
  This topic provides the information to generate CSR.
- Obtain Trusted Certificate from CA
  This topic explains to obtain trusted certificate from CA.
- Import Certificate into Identity Store
  This topic describes the information on importing certificate into identity store.

3.2.1 Creation of Public and Private Key Pair

This topic provides the detailed information on creation of public and Private Key Pair.

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

Table 3-2 Attributes of the certificate and Keystore

Attributes	Description
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.
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 the Oracle Weblogic Server.
First and Last Name (CN)	Enter the domain name of the machine used to access Oracle Banking Corporate Lending, for instance, www.example.com
Name of your Organizational Unit	The name of the department or unit making the request, for example, BPD. Use this field to identify the SSL Certificate you are creating, for example, by department or by the physical server.
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.
Name of your City or Locality	The city in which your organization is physically located, for example, Mumbai.
Name of your State or Province	The state/province in which your organization is physically located, for example, Maharashtra.
Two-Letter Country Code for this Unit	The country in which your organization is physically located, for example, US, UK, IN, etc.

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 Generate CSR

This topic provides the information to generate 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.

> **Note:**
>
> 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.

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 -
keystoreD:\keystores\FCUBSKeyStore.jks

Enter keystore password:[Enter the password used to access the keystore]
Enter key password for <cvrhp0729>
(RETURN if same as keystore password):[Enter the password used to access the
key in the keystore]
```

3.2.3 Obtain Trusted Certificate from CA

This topic explains to obtain 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 Import Certificate into Identity Store

This topic describes the information on 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 is 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.

This topic contains the following sub-topics:

- Import Intermediate CA certificate
  This topic provides detailed information on importing Intermediate CA certificate into keystore.
- Import Identity Certificate
  This topic describes the information on importing identity certificate into keystore.

3.2.4.1 Import Intermediate CA certificate

This topic provides detailed information on importing Intermediate CA certificate into keystore.

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 -
fileD:\keystores\VerisignIntermediateCA.cer -trustcacerts -
keystoreD:\keystoreworkarea\FCUBSKeyStore.jks

Enter keystore password:<Enter the password used to access the keystore>
```

Certificate was added to keystore.

3.2.4.2 Import Identity Certificate

This topic describes the information on importing identity certificate into keystore.

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 was added to 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 the identity store, depending on factors including the trustworthiness of the CA, the necessity of transporting the trust store across the machine, among others.

4

Configure Identity and Trust Stores for Weblogic

This topic contains the following sub-topics:

4.1 Enable SSL on Oracle Weblogic Server

This topic explains the systematic instructions to enable SSL on Oracle Weblogic Server.

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

1. Click the **Lock & Edit** button under **Change Center**.
2. Expand the **Servers** node.
3. Select the name of the server for which you want to enable SSL (example - exampleserver).
4. Go to **Configuration** and select the **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 Configure Identity and Trust Stores

This topic provides the systematic instructions to configure identity and trust stores.

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

1. Click the **Lock & Edit** button under **Change Center**.
2. Expand the **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 the **Keystores** tab.
5. In the field **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:
   a. **Custom Identity Keystore File Name:** Fully qualified path to the Identity keystore.

b. **Custom Identity Keystore Type:** Set this attribute to JKS, the type of the keystore. If left blank, it defaults to JKS (Java KeyStore).

c. **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 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:

   a. **Custom Trust Keystore**: The fully qualified path to the trust keystore.

   b. **Custom Trust Keystore Type**: Set this attribute to JKS, the type of the keystore. If left blank, it defaults to JKS (Java KeyStore).

   c. **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 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.

   > **Note:**
   >
   > When identity and trust stores are of the JKS format, the passphrases are not required.

5

Configure SSL Attributes for Managed Servers

This topic explains to set SSL attributes for managed servers.

This topic contains the following sub-topics:

- Set SSL Attributes for Private Key Alias and Password
  This topic explais the systematic instruction to set SSL attributes for private key alias and password.

5.1 Set SSL Attributes for Private Key Alias and Password

This topic explais the systematic instruction to set SSL attributes for private key alias and password.

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

1. Click the **Lock & Edit** button under **Change Center**.
2. Expand the **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 the **SSL** tab.
5. Select **Keystores** from **Identity and Trust Locations**.
6. Under **Identity** section, specify the following details:
   a. **Private Key Alias:** Set this attribute to the alias name defined for the key pair when creating the key pair in the Identity keystore.
   b. **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. Click **Activate Changes** button under **Change Center**.
9. Go to the **controls** tab, check the appropriate server, and click **Restart SSL**. Confirm when it prompts.

6
Test Configuration

This topic explains to test the application after configuring with Oracle Weblogic for SSL.

Once the Oracle Weblogic has been configured for SSL, deploy the application in the usual manner. The application can be tested in SSL mode after deployment. To launch the application in SSL mode, enter the URL in the following format:

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

It is recommended that the Oracle Banking Corporate Lending web application be accessed via the HTTPS channel instead of the HTTP channel.

7

Create Resources on Weblogic

This topic explains the steps to deploy the Oracle Banking Corporate Lending application and gateway application in the application server.

This topic contains the following sub-topics:

- Resource Administration
  This topic explains the process of resource administration on Oracle Weblogic.
- Configure Weblogic for PMGateway
  This topic explains to configure Weblogic for PMGateway.
- Configure Weblogic for Oracle Banking Corporate Lending
  This topic provides the systematic instructions to configure the Oracle WebLogic application server for Oracle Banking Corporate Lending.
- Configure Mail Session in Weblogic
  This topic describes the set of configurations changes required in the Oracle Weblogic Server when Oracle Banking Corporate Lending is configured to generate and send passwords to users via e-mail.

7.1 Resource Administration

This topic explains the process of resource administration on Oracle Weblogic.

All the resources are mentioned in the *Resources To be Created* guide that need to be created before deployment.

One example for each category is explained in the following sub-topics.

- Create Data Source
  This topic explains methods to create data sources.
- Create JMS Server
  This topic explains the systematic instructions to create the JMS server in the Weblogic application server.
- Create JMS Modules
  This topic explains the systematic instructions to create the JMS Modules in the Weblogic application server.
- Create Subdeployment
  This topic explains the systematic instructions to create the subdeployment in the Weblogic application server.
- Create JMS Queue
  This topic provides the systematic instructions to create the JMS Queue in the Weblogic application server.
- Create JMS Connection Factory
  This topic explains the systematic instructions to create the JMS Connection Factory in the Weblogic application server.

7.1.1 Create Data Source

This topic explains methods to create data sources.

This topic contains the following sub-topics:

- Prerequisites
  This topic explains the prerequities details to create data source.
- XA Enabled Data Source
  This topic provides the systematic instructions to create the XA enabled data source in the Weblogic application server.
- Non-XA Enabled Data Source
  This topic provides the systematic instructions to create the Non-XA enabled data source in the Weblogic application server.

7.1.1.1 Prerequisites

This topic explains the prerequities details to create data source.

To create the data source, the OCI needs to be enabled. For this, download Oracle Instant Client and install it. The details are given below:

Table 7-1 Oracle Instant Client

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, the user needs to provide the directory path where Instant Client is installed.

The user needs to do the data source configuration with the 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 **setDomainEnv.bat**. This must be the directory path 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 **setDomainEnv.sh**. This must be the directory path 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 **setDomainEnv.sh**.

If the target database is Autonomous Database then configure the TNS_ADMIN in the DB client of the Application server with the Autonomous Database Wallet given by the Database Administrator.

7.1.1.2 XA Enabled Data Source

This topic provides the systematic instructions to create the XA enabled data source in the Weblogic application server.

To create the XA enabled data source, follow the steps below:

1. Start the Administrative Console of the WebLogic application server. Enter the Oracle WebLogic Admin Console URL in the address bar in an internet browser. For example: http://10.10.10.10:1001/console

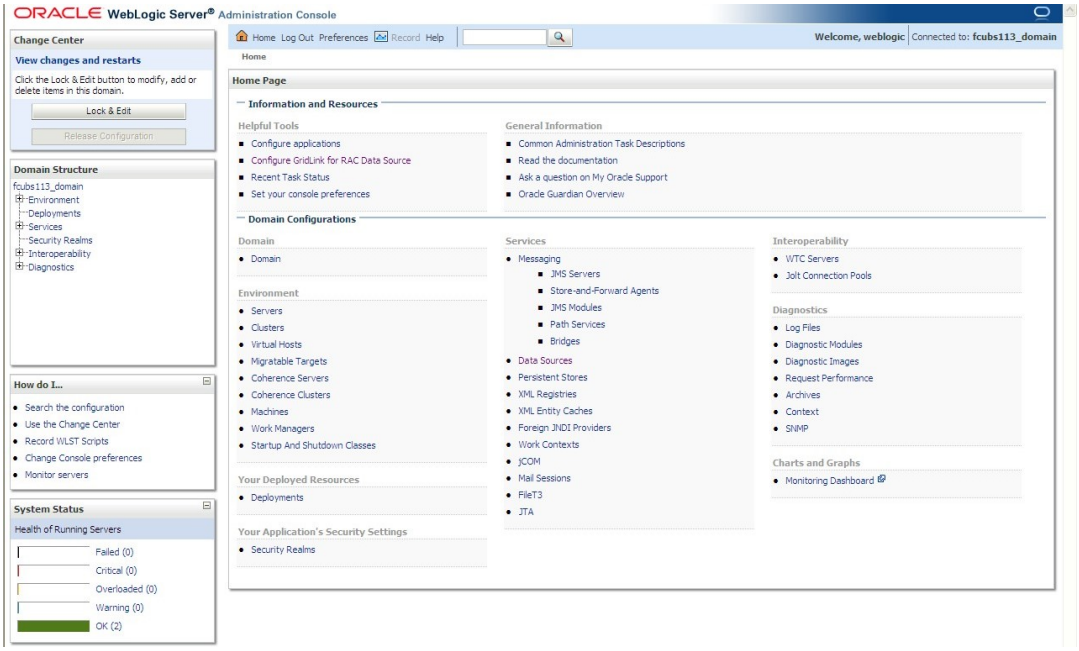
   The **Oracle Weblogic Server - Welcome** screen displays.

Figure 7-1 Oracle Weblogic Server - Welcome

2. Specify the WebLogic administrator **Username**, **Password** and click **Log In**.

   The **Oracle Weblogic Server - Home Page** screen displays.

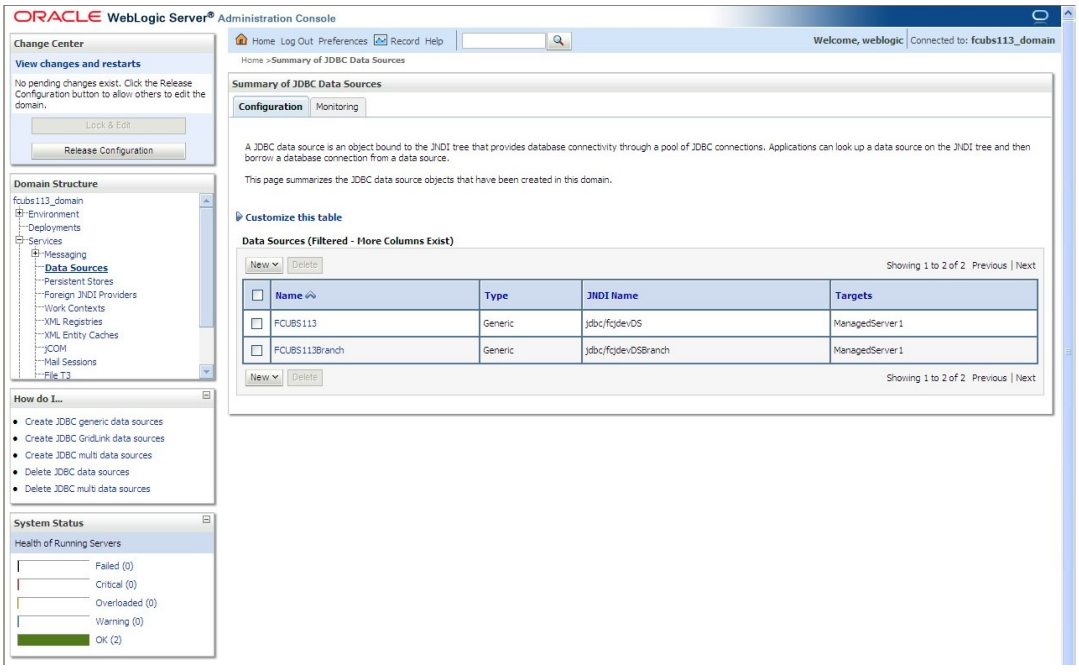
Figure 7-2 Oracle Weblogic Server - Home Page



3. Under the **Change Center**, click on the **Lock & Edit** button.
4. Go to **Data Sources**.

   The **Summary of JDBC Data Sources** screen displays.

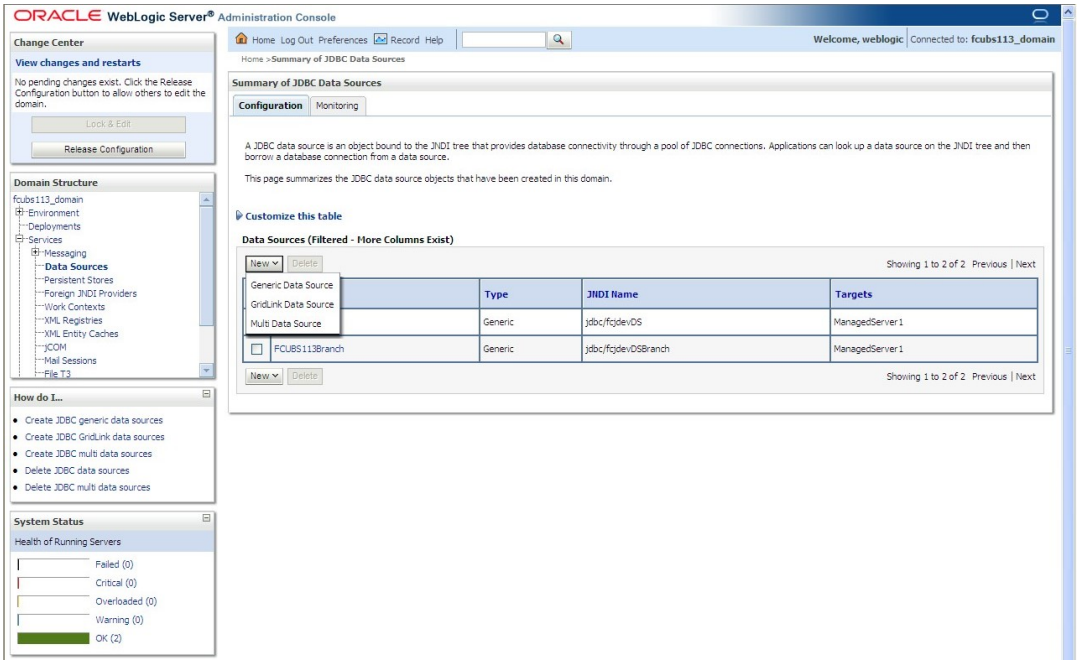
Figure 7-3 Summary of JDBC Data Sources



5. On the left pane, under **Domain Structure**, expand **Services** and then **Data Sources** under it. Click the **Lock & Edit** button.

   The **Summary of JDBC Data Sources - Configuration** screen displays.

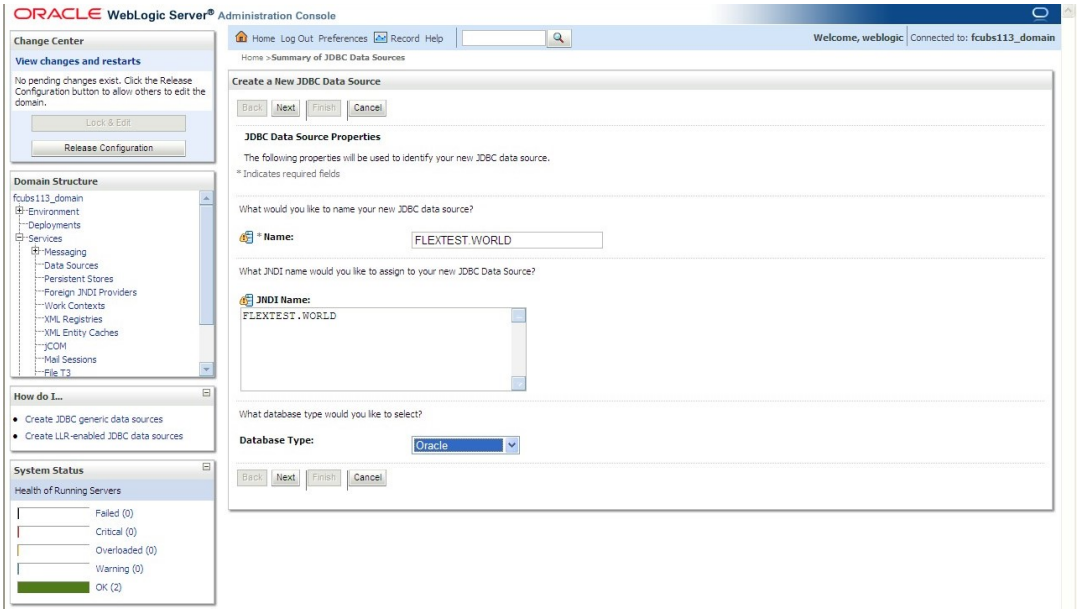
Figure 7-4 Summary of JDBC Data Sources - Configuration



6. To create a new data source, click **New** and select **Generic Data Source** from the drop-down.

   The **Create a New JDBC Data Source** screen displays.

Figure 7-5 Create a New JDBC Data Source



For more information on fields, refer to the field description table.

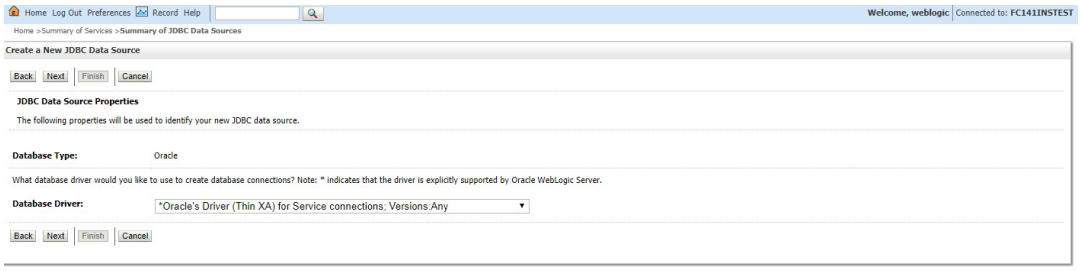
Table 7-2 Create a New JDBC Data Source

Field	Description
JDBC Datasource Name	Name of the data source.
JNDI Name	JNDI name which will be used for lookup.
Database Type	Specify the database type as Oracle from the drop-down list.

7. Click **Next**.

   The **JDBC Data Source Properties** screen displays.

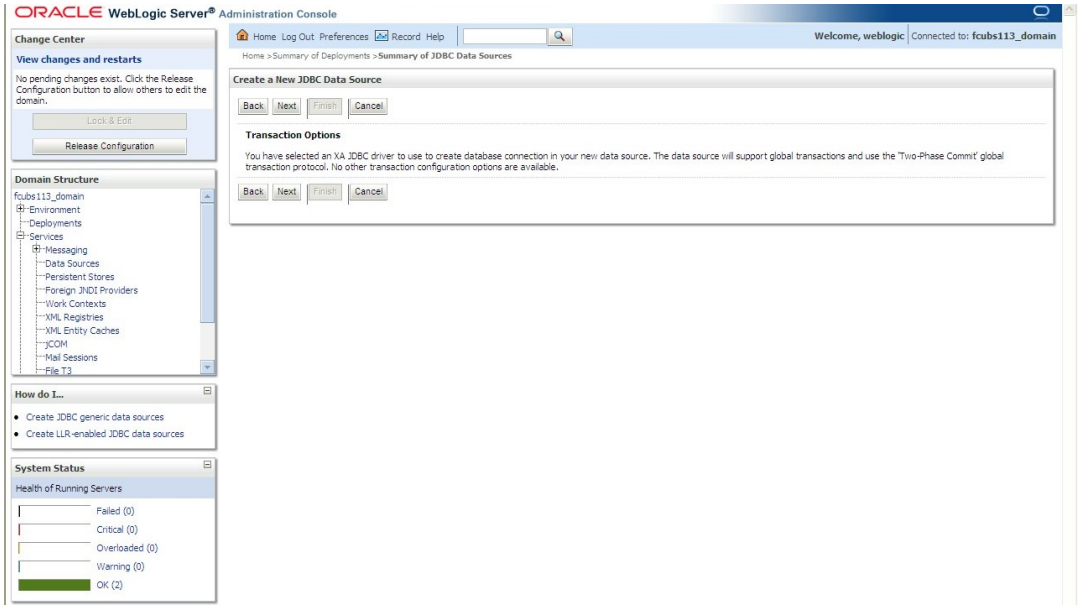
Figure 7-6 JDBC Data Source Properties



8. Select the database driver from the drop-down list and click **Next**.

   The **Create a New JDBC Data Source - Transaction Options** screen displays.

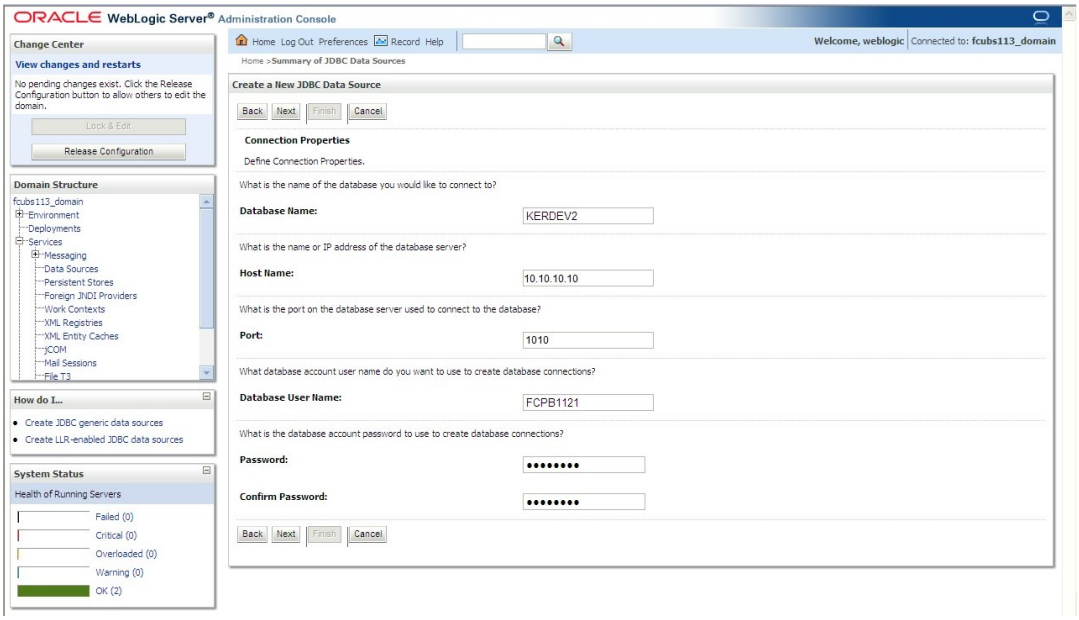
Figure 7-7 Create a New JDBC Data Source - Transaction Options



9. On the **Create a New JDBC Data Source - Connection Properties** screen, specify the Database Name, Host Name, Port of the database server to connect, Database User Name, Password. and Confirm password.

   The **Create a New JDBC Data Source - Connection Properties** screen displays.

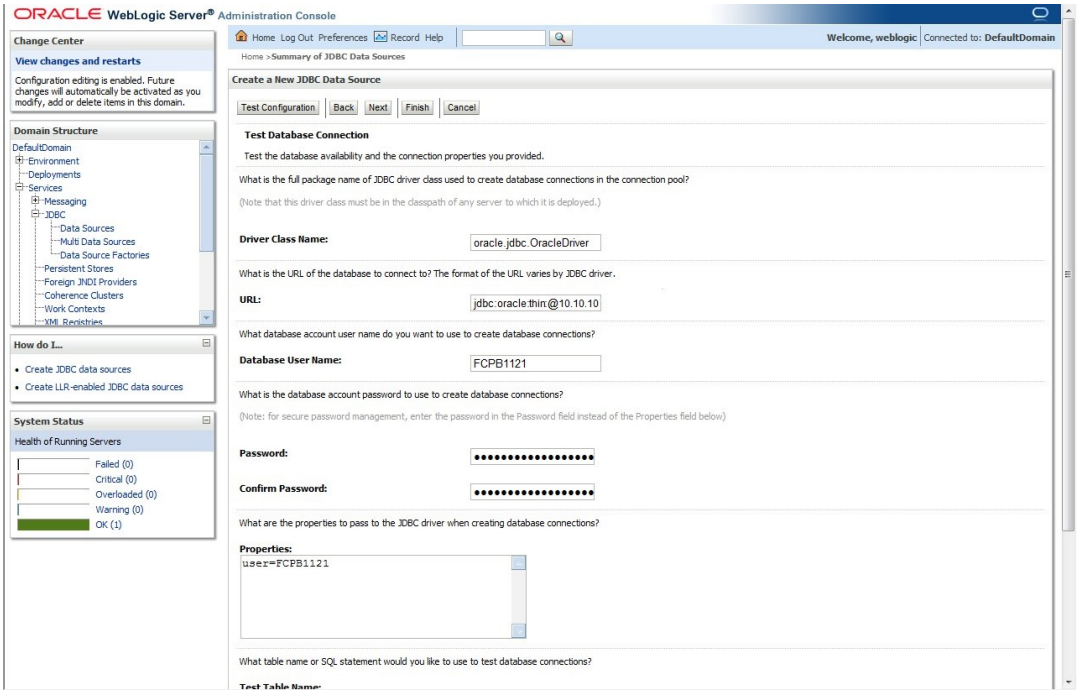
Figure 7-8 Create a New JDBC Data Source - Connection Properties



10. Click **Next**.

    The **Create a New JDBC Data Source - Test Database Connection** screen displays.

Figure 7-9 Create a New JDBC Data Source - Test Database Connection



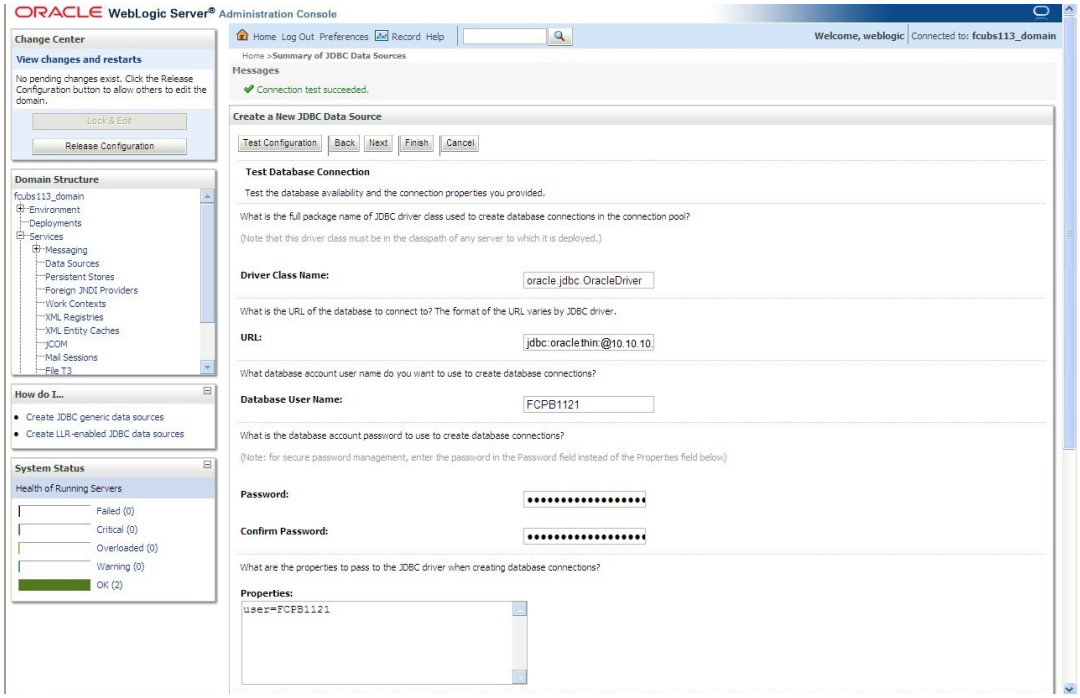
11. Specify the **Driver Class** Name (Eg: oracle.jdbc.OracleDriver).
12. Specify the URL as jdbc:oracle:thin:@10.10.10.10:1001<INSTANCE_NAME>.

    If the target database is Autonomous Database then, the URL Format to connect to Autonomous Database must be as follows: Jdbc:oracle:thin:@<Database Service Connect string >?TNS_ADMIN=<TNS ADMIN PATH>

13. Specify the Database username (Eg: FCPB1121) and password.
14. Confirm the password.
15. Click the **Test Configuration** button.
16. If the connection is established successfully,

    A message displays on the **Create a New JDBC Data Source** screen confirming that `Connection test succeeded`.

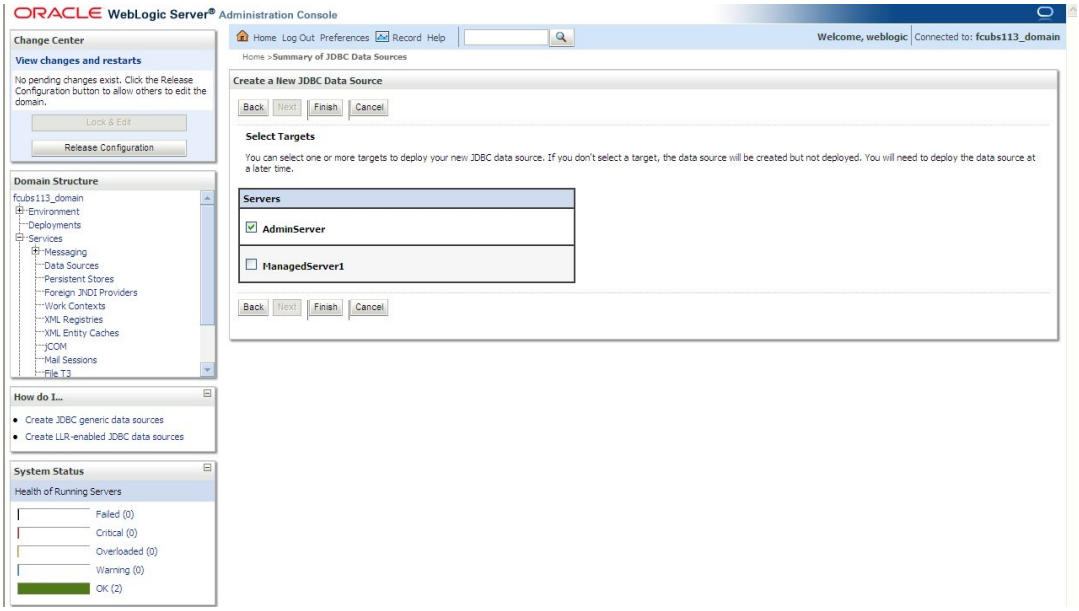
Figure 7-10 Create a New JDBC Data Source - Message



17. Click **Next**.

    The **Create a New JDBC Data Source - Select Targets** screen displays.

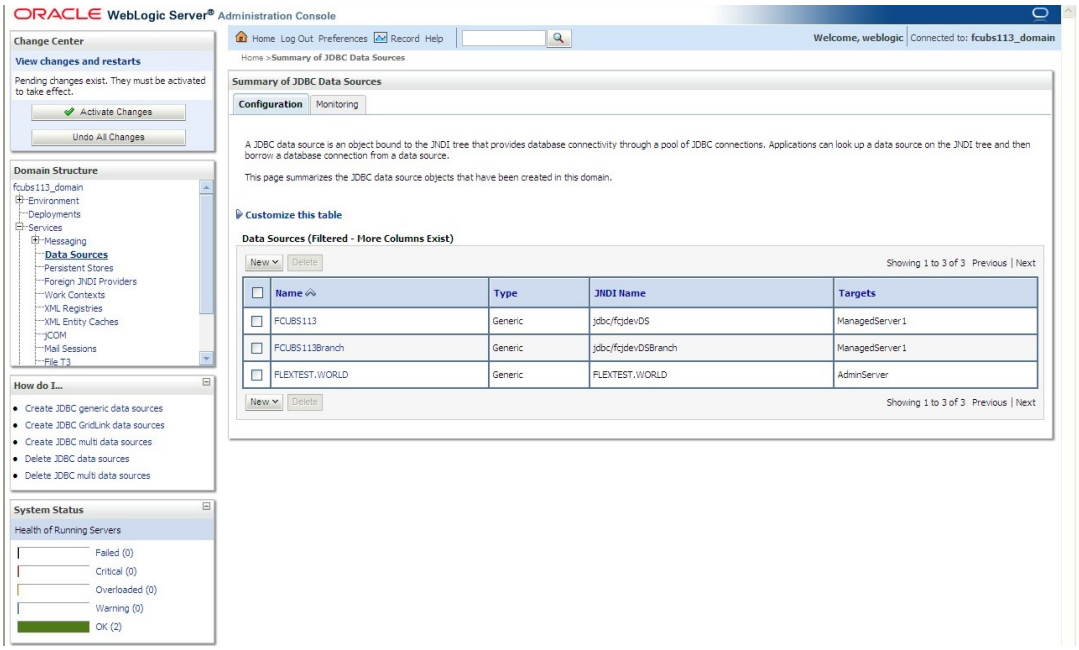
Figure 7-11 Create a New JDBC Data Source - Select Targets



18. Check the boxes against the required servers and click **Finish**.

    The **Summary of JDBC Data Sources - New Data Source** screen displays.

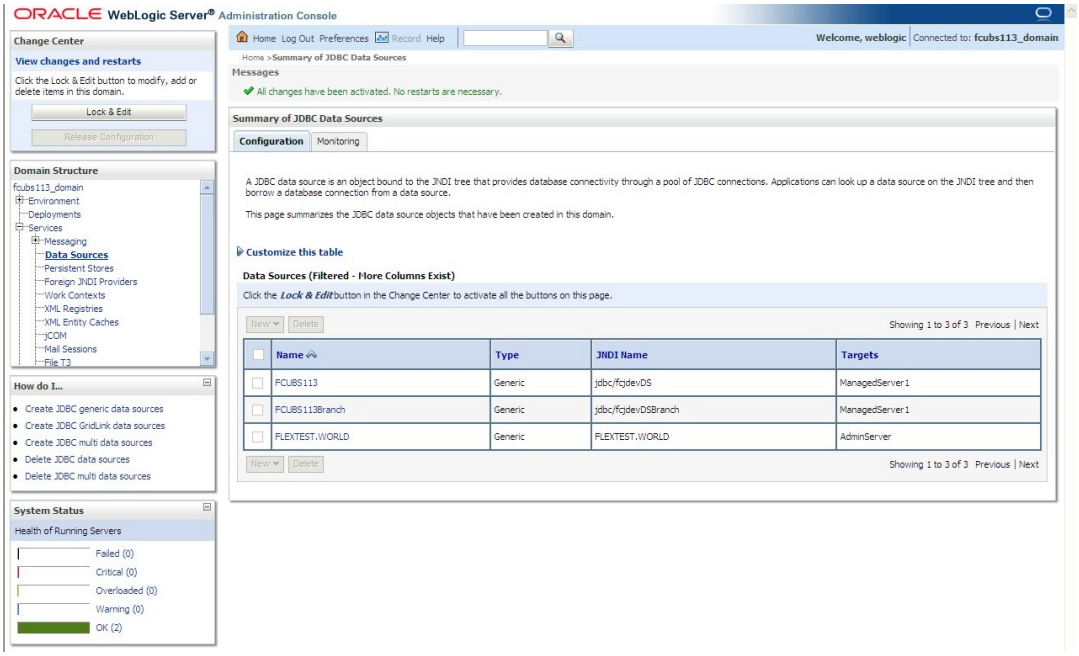
Figure 7-12 Summary of JDBC Data Sources - New Data Source



19. Click the **Activate Changes** button on the left pane.

    The message displays on the **Summary of JDBC Data Sources** screen confirming that `All the changes have been activated. No restarts are necessary.`

Figure 7-13 Summary of JDBC Data Sources - Activate Changes Message



Refer to *Resources_To_ Be_Created* guide for the list of XA data sources to be created.

A new **Data Source** is created.

7.1.1.3 Non-XA Enabled Data Source

This topic provides the systematic instructions to create the Non-XA enabled data source in the Weblogic application server.

To create the Non-XA enabled data source, follow the steps given below:

1. Start the Administrative Console of the WebLogic application server. Enter the Oracle WebLogic Admin Console URL in the address bar in an internet browser. For example: http://10.10.10.10:1001/console.

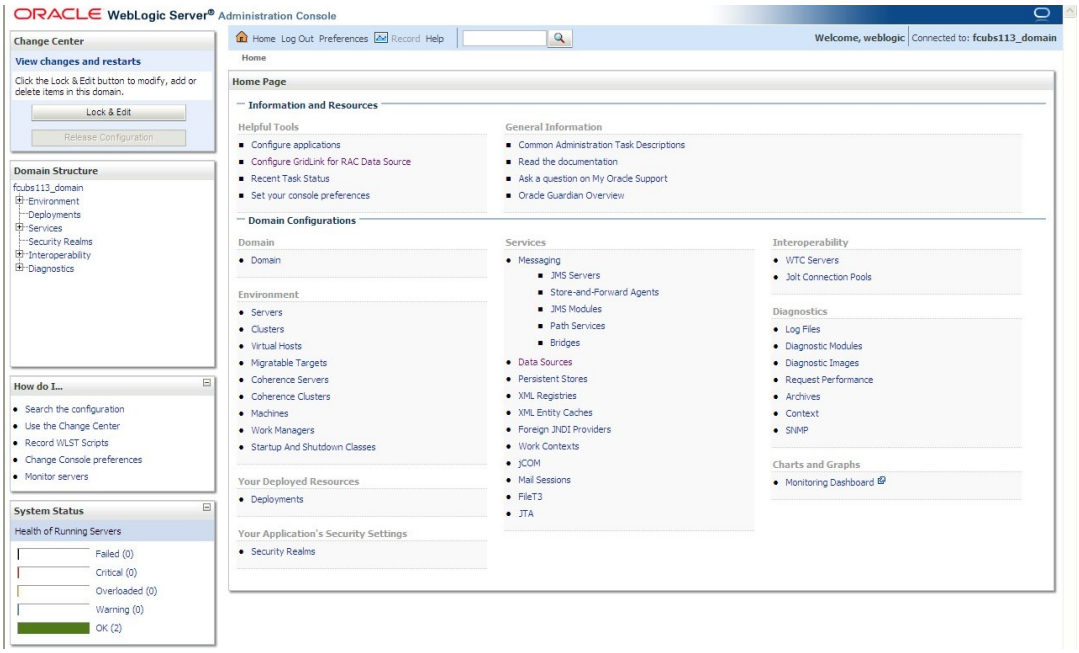
   The **Oracle Weblogic Server - Welcome** screen displays.

Figure 7-14 Oracle Weblogic Server - Welcome

2. Specify the WebLogic administrator **Username**, **Password** and click **Log In**.

   The **Oracle Weblogic Server - Home Page** screen displays.

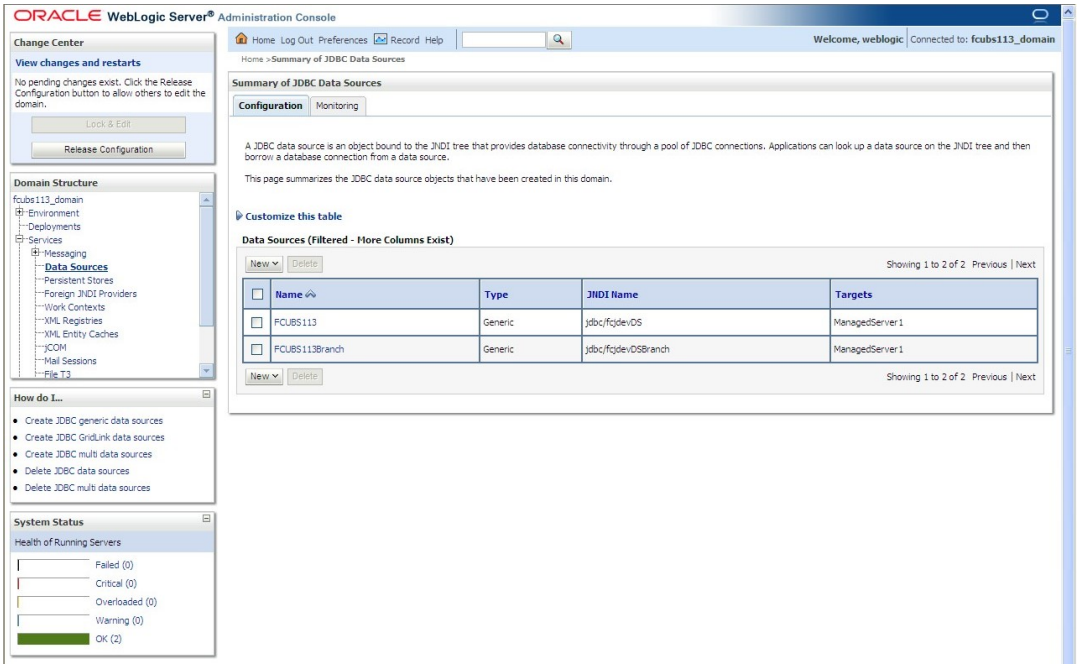
Figure 7-15 Oracle Weblogic Server - Home Page



3. Go to **Data Sources**.

   The **Summary of JDBC Data Sources** screen displays.

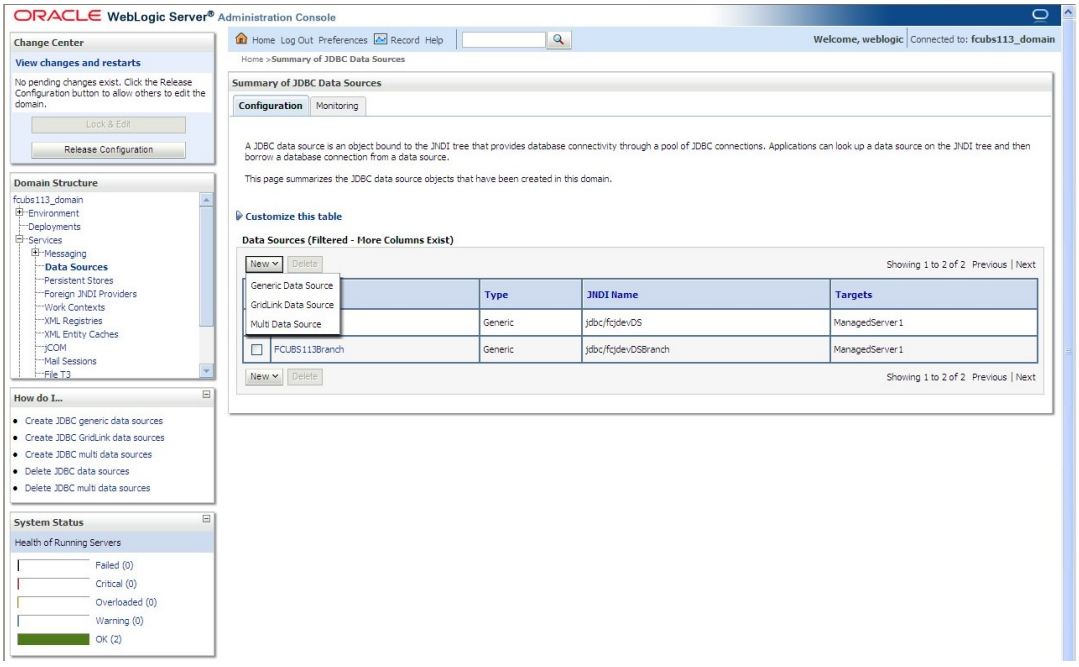
Figure 7-16 Summary of JDBC Data Sources



4. On the left pane, under **Domain Structure**, expand **Services** and then **Data Sources** under it. Click the **Lock & Edit** button.

   The **Summary of JDBC Data Sources - Configuration** screen displays.

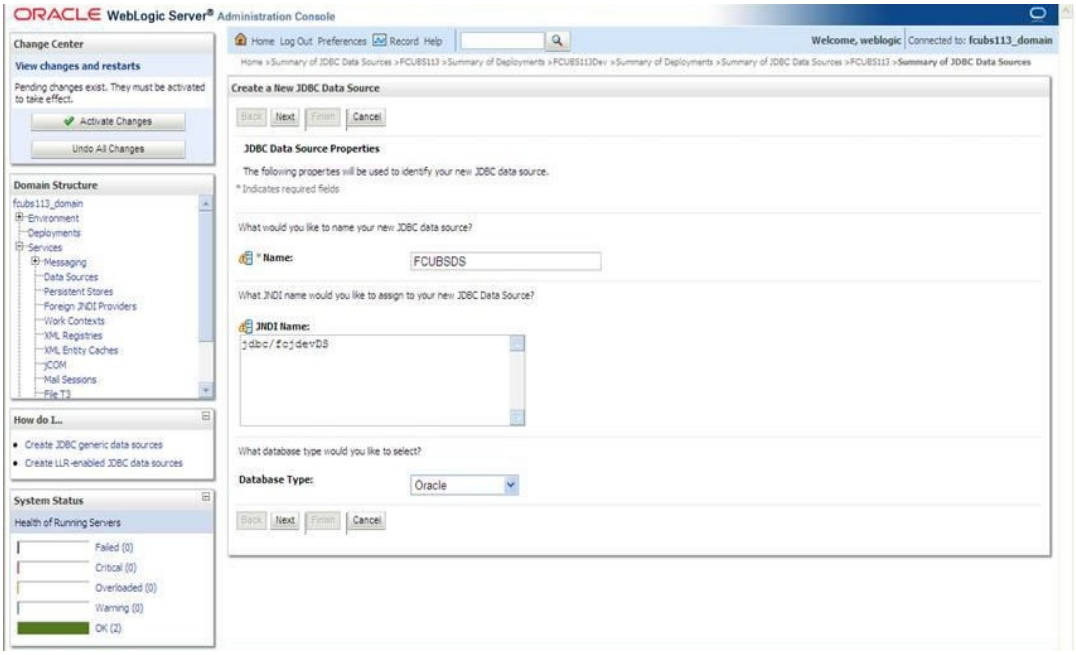
Figure 7-17 Summary of JDBC Data Sources - Configuration



5. To create a new data source, click **New** and select **Generic Data Source** from the drop-down.

   The **Create a New JDBC Data Source** screen displays.

Figure 7-18 Create a New JDBC Data Source



For more information on fields, refer to the field description table.

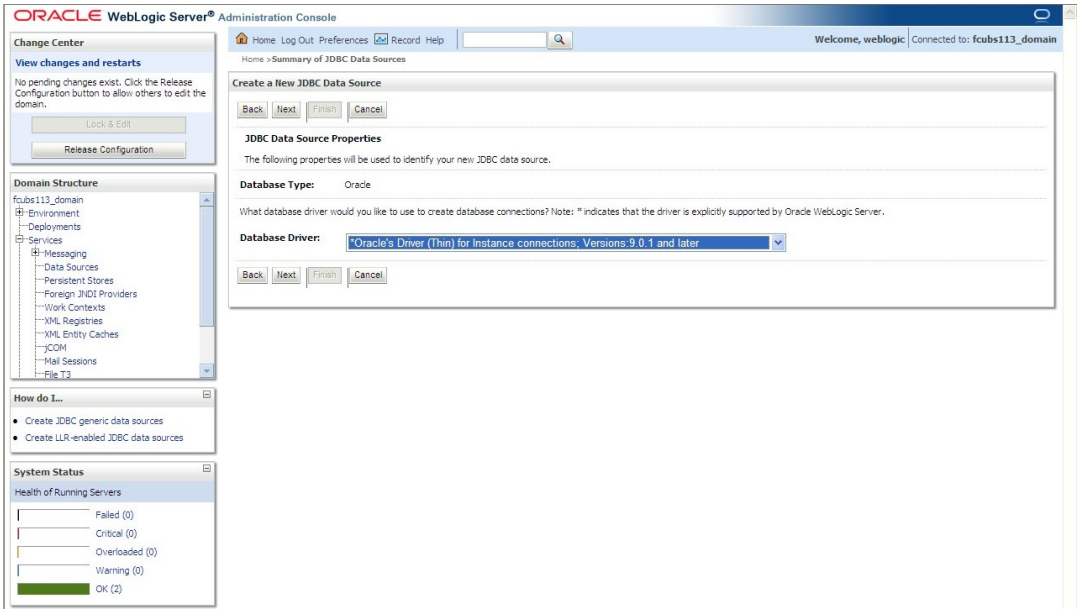
Table 7-3 Create a New JDBC Data Source

Field	Description
JDBC Datasource Name	Name of the Datasource.
JNDI Name	JNDI for lookup.
Database Type	Oracle

6. Click **Next**.

The **Create a New JDBC Data Source - JDBC Data Source Properties** screen displays.

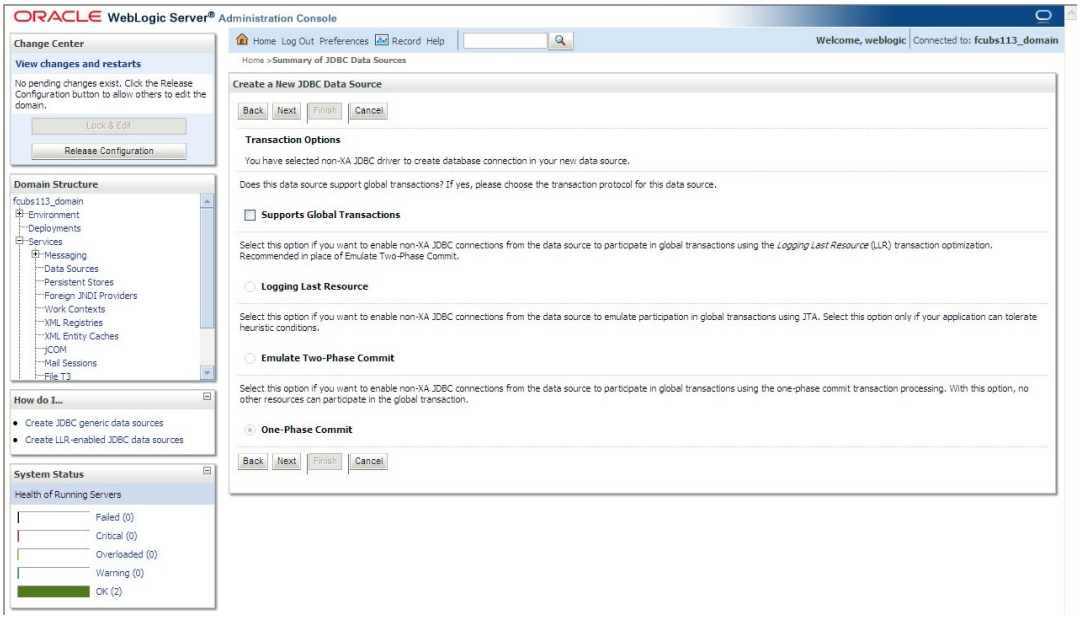
Figure 7-19 Create a New JDBC Data Source - JDBC Data Source Properties



7. Select the database driver from the drop-down list and click **Next**.

   The **Create a New JDBC Data Source - Transaction Options** screen displays.

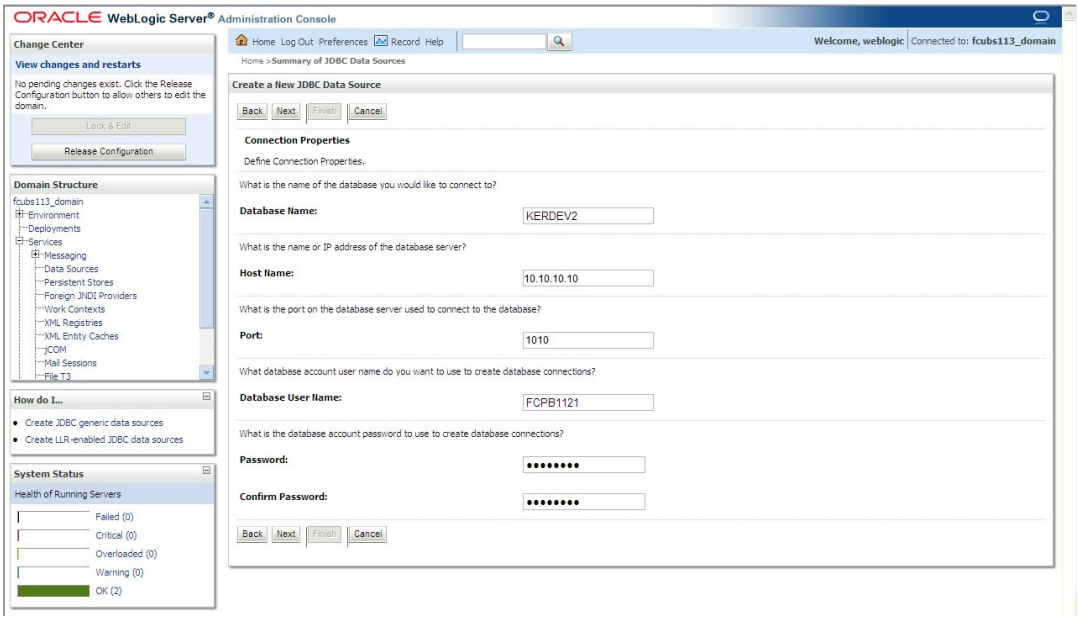
Figure 7-20 Create a New JDBC Data Source - Transaction Options



8. Select **Logging Last Resource** then, uncheck **Support Global Transactions** and Click **Next**.

   The **Create a New JDBC Data Source - Connection Properties** screen displays.

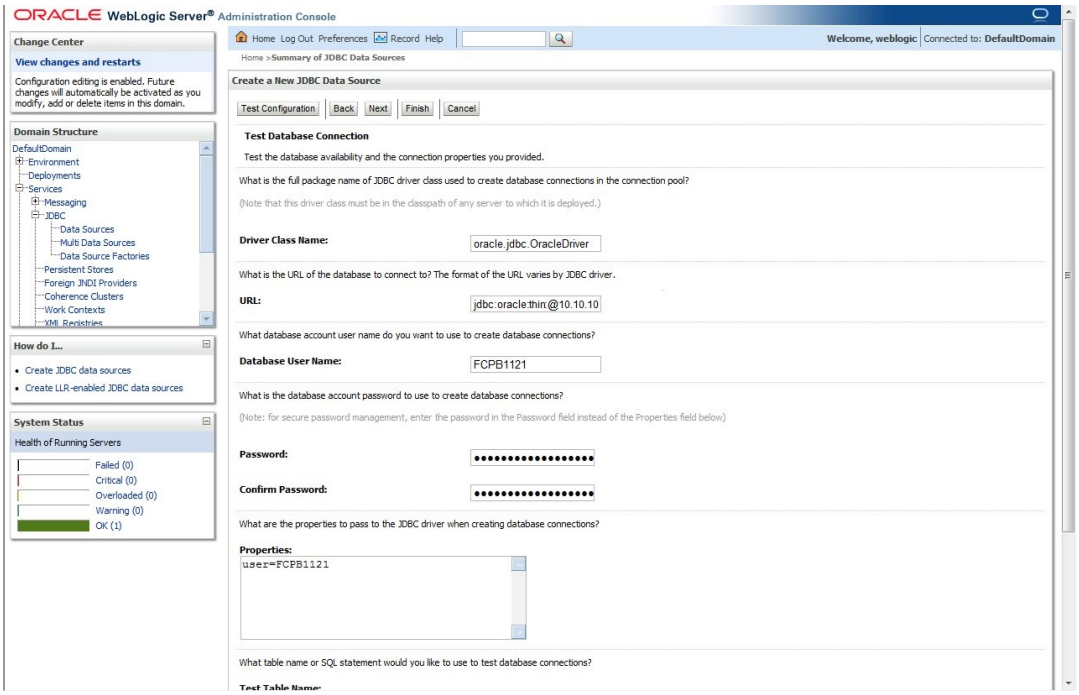
Figure 7-21 Create a New JDBC Data Source - Connection Properties



9. The **Create a New JDBC Data Source - Connection Properties** defines the connection properties.
10. Specify the Database Name, Host Name, Port of the database server to connect, Database User Name, Password, and Confirm the password.
11. Click **Next**.

    The **Create a New JDBC Data Source - Test Database Connection** screen displays.

Figure 7-22 Create a New JDBC Data Source - Test Database Connection

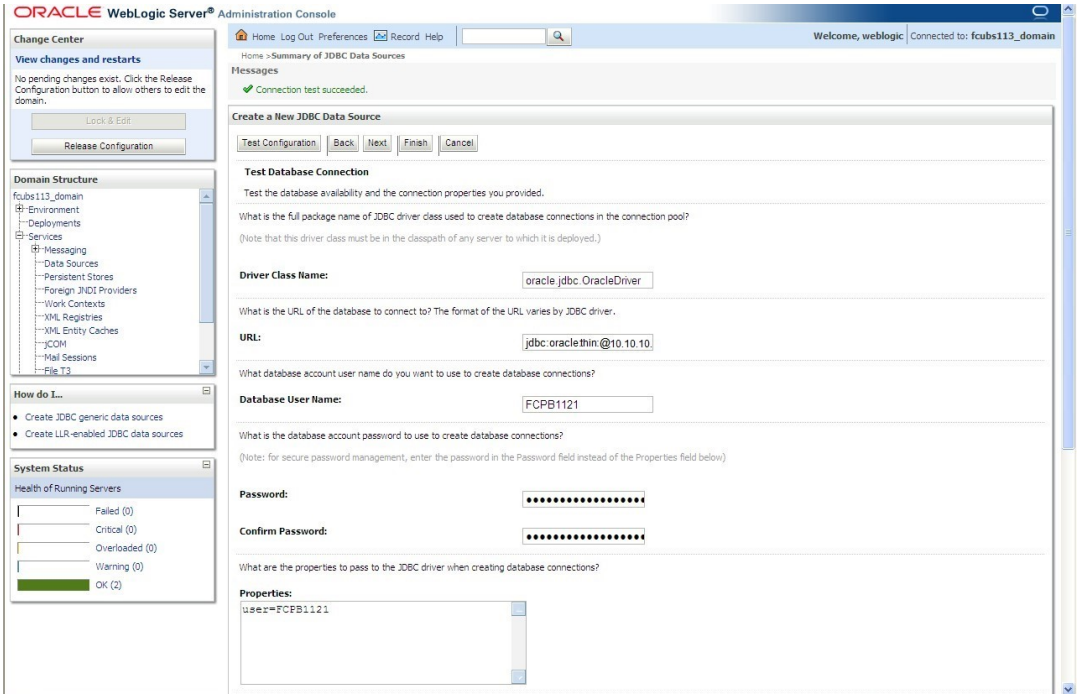


12. Specify the **Driver Class Name** (Eg: oracle.jdbc.OracleDriver).
13. Specify the URL as jdbc:oracle:oci:@10.10.10.10:1010:<INSTANCE_NAME> from jdbc:oracle:thin:@10.10.10.10:1001<INSTANCE_NAME>.

    If the target database is Autonomous Database then, the URL Format to connect to Autonomous Database must be as follows: Jdbc:oracle:thin:@<Database Service Connect string >?TNS_ADMIN=<TNS ADMIN PATH>
14. Specify the Database Username (Eg: testdb) and password.
15. Confirm the password.
16. Click on **Test Configuration** button.

    If the connection is established successfully, a message displays on the **Create a New JDBC Data Source - Messages** screen confirming that `Connection test succeeded`.

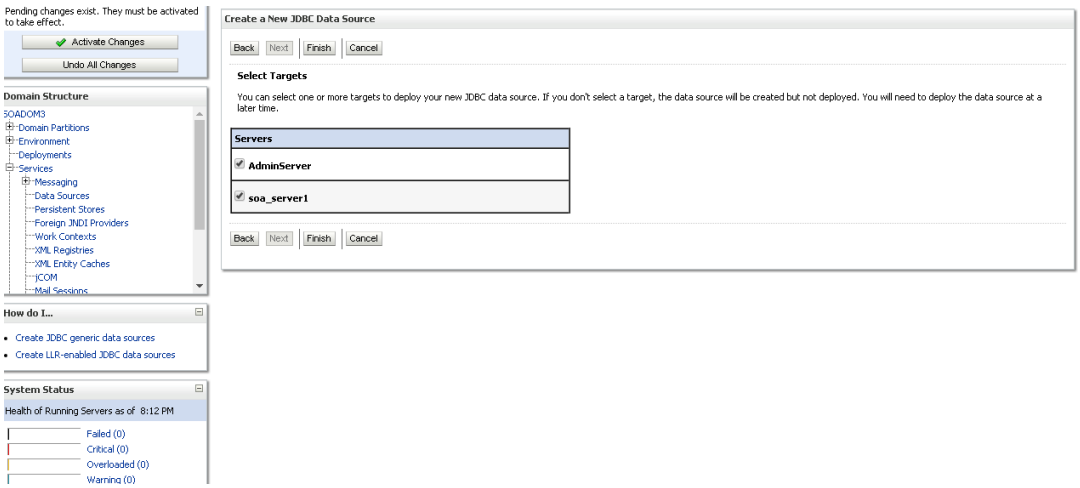
Figure 7-23 Create a New JDBC Data Source - Message



17. Click **Next**.

    The **Create a New JDBC Data Source - Select Targets** screen displays.

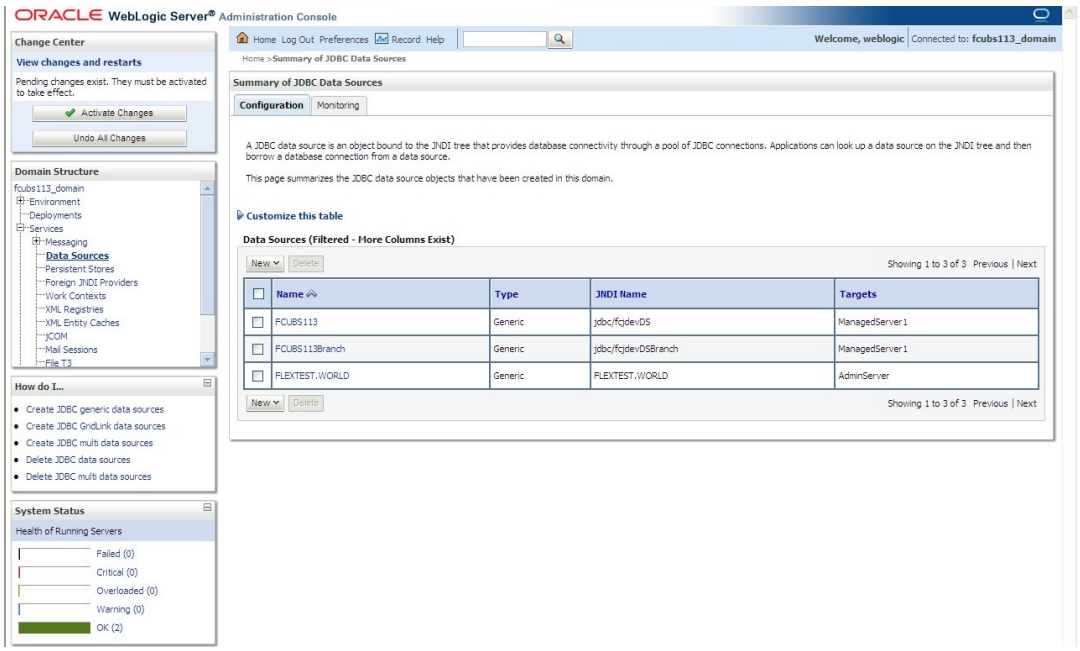
Figure 7-24 Create a New JDBC Data Source - Select Targets



18. Select the check boxes against the required servers(for data source jdbc/fcjdevDS, it is mandatory to select the admin server check box as well as the application-deployed server) and click **Finish**.

    The **Summary of JDBC Data Sources - New Data Source** screen displays.

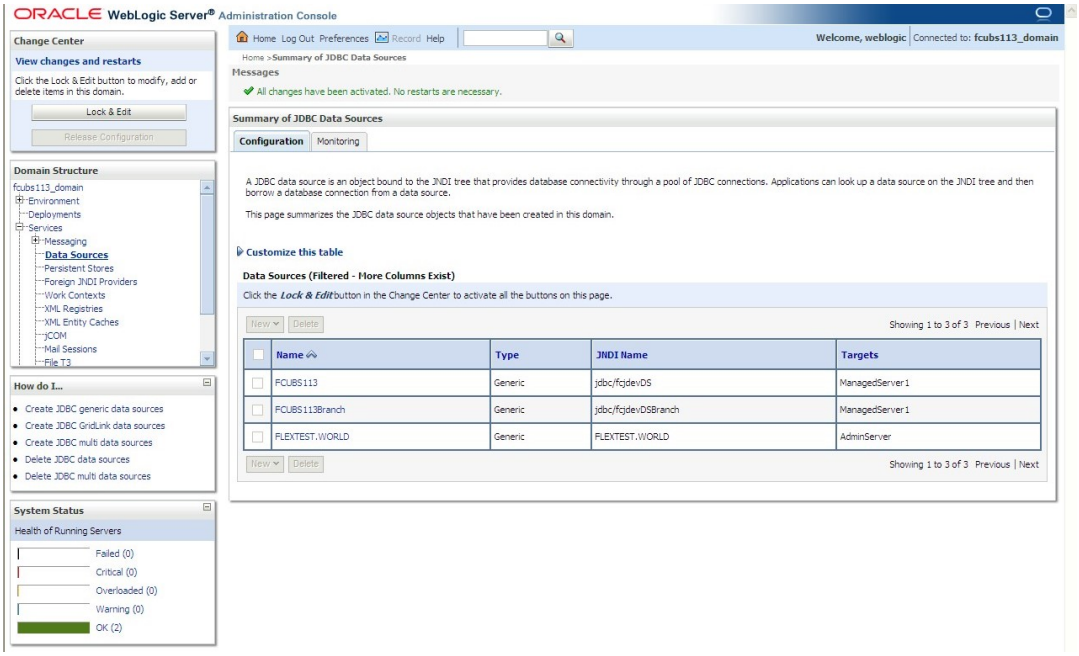
Figure 7-25 Summary of JDBC Data Sources - New Data Source



19. Click the **Activate Changes** button on the left pane.

    The message displays on the **Summary of JDBC Data Sources - Activate Changes Message** screen confirming that `All the changes have been activated. No restarts are necessary`.

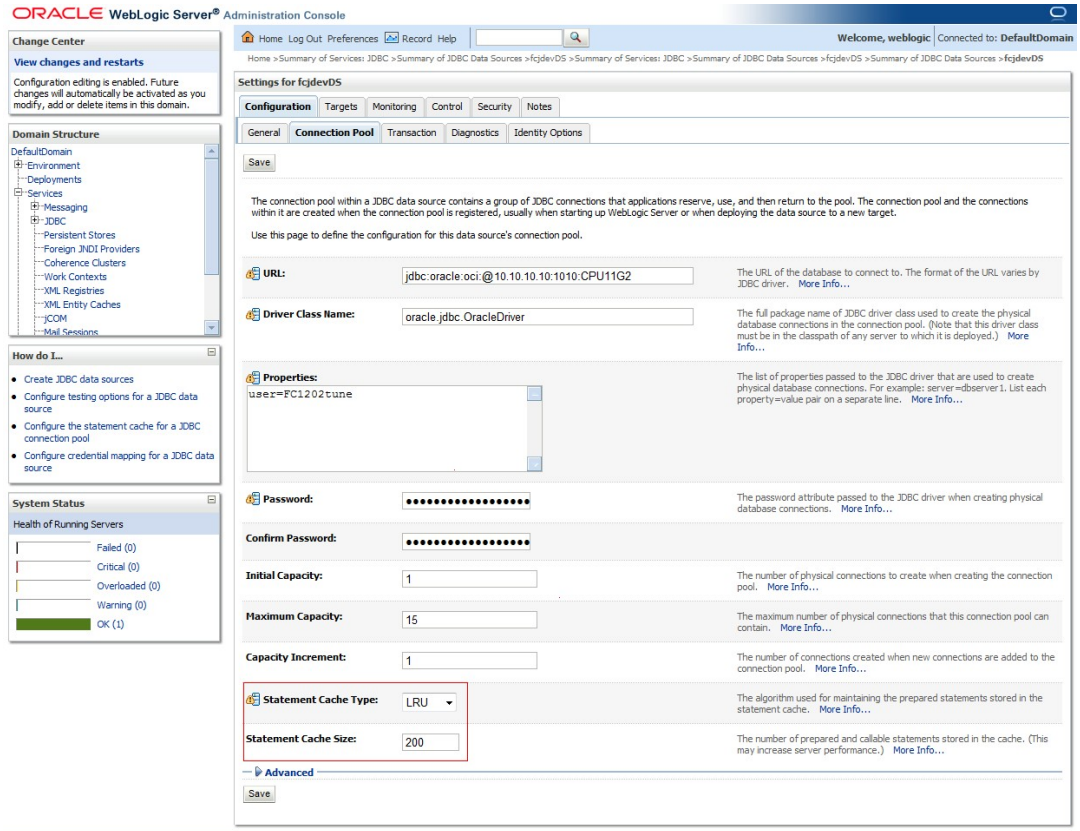
Figure 7-26 Summary of JDBC Data Sources - Activate Changes Message



20. Click the Datasource, and then click on the **Connection Pool** tab.

The **Settings for fcjdevDS - Connection Pool** screen displays.

Figure 7-27 Settings for fcjdevDS - Connection Pool



21. On the **Settings for fcjdevDS - Connection Pool** screen, select the statement cache type as **LRU** from the drop-down list.
22. Specify the statement cache size as **200**.
23. Click **Save** button.
24. Refer to the *Resources to be created* guide for the list of Non-XA data sources to be created.

> **Note:**
>
> - You need to create another data source for Oracle FCUBS with the JNDI name '_ASYNC' for the 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 **_ASYNC**.
> - You need to create another data source for Oracle ELCM with the 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 the ELCM data source.

The following is the list of data sources that can be created depending on the requirement. For more information, refer to the *Resources to be created* guide.

Table 7-4 List of Data Sources

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

The Oracle Banking Corporate Lending data source is created.

7.1.2 Create JMS Server

This topic explains the systematic instructions to create the JMS server in the Weblogic application server.

To create the JMS server, follow the steps given below:

1. Start the Administrative Console of the WebLogic application server. Enter the Oracle WebLogic Admin Console URL in the address bar in an internet browser. For example: http://10.10.10.10:1001/console.

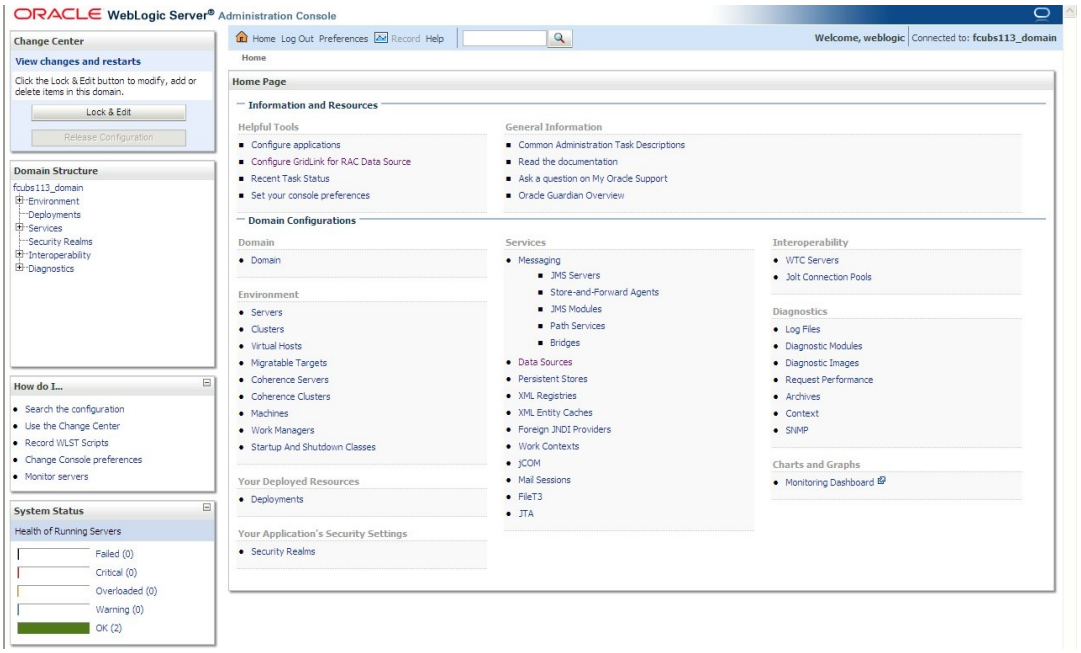
   The **Oracle Weblogic Server - Welcome** screen displays.

Figure 7-28 Oracle Weblogic Server - Welcome

2. Specify the WebLogic administrator **Username**, **Password** and click **Log In**.
3. Navigate to Oracle Weblogic home page.

   The **Oracle Weblogic Server - Home Page** screen displays.

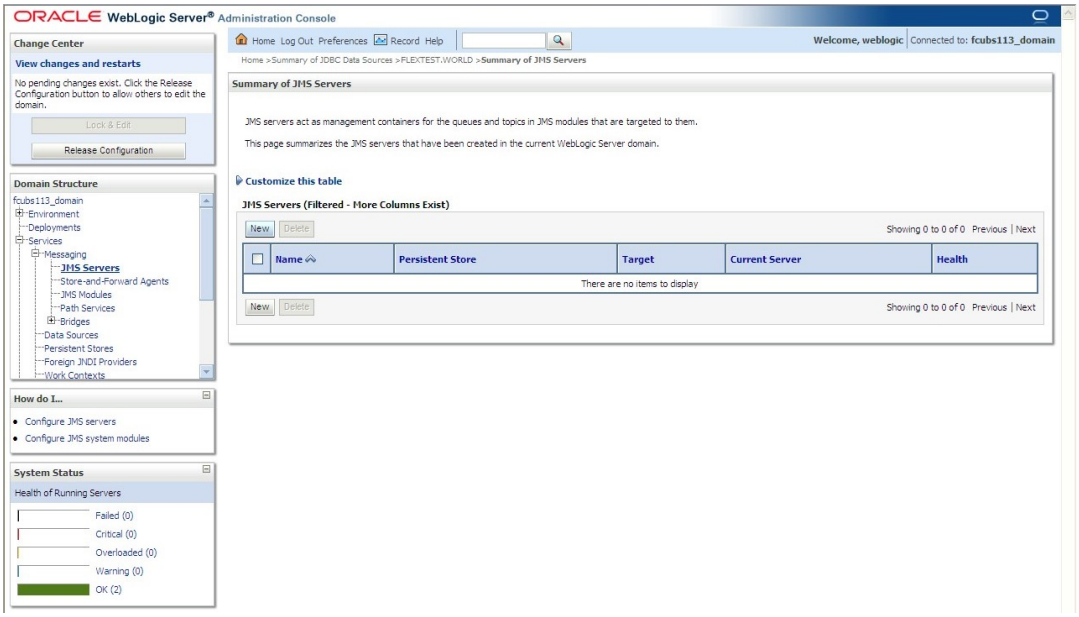
Figure 7-29 Oracle Weblogic Server - Home Page



4. On the left pane, under **Domain Structure**, expand **Services**, **Messaging** and **JMS Server** under it. Click the **Lock & Edit** button.

   The **Summary of JMS Servers** screen displays.

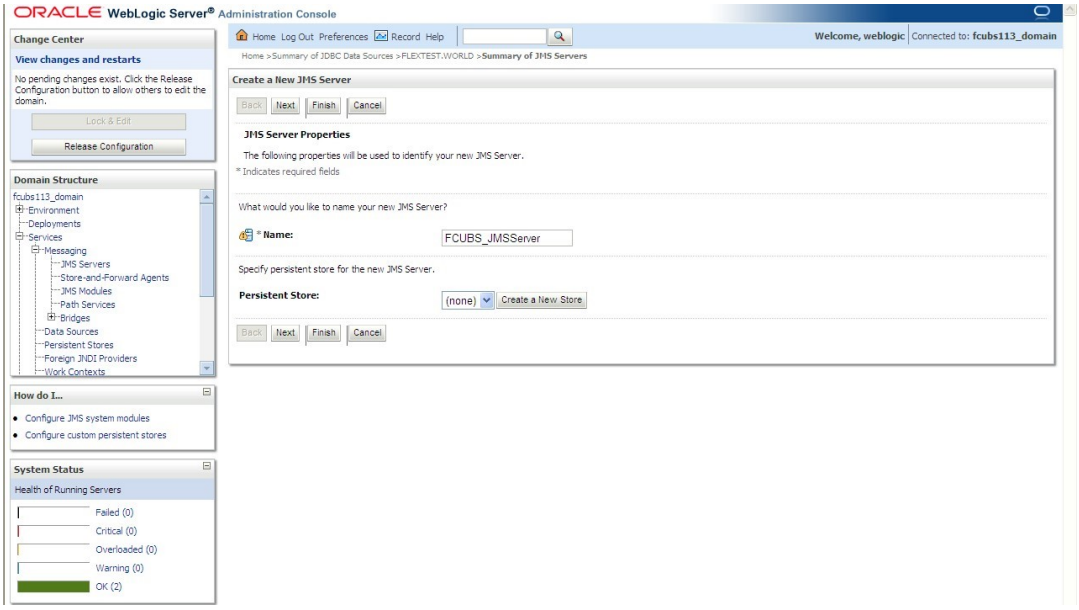
Figure 7-30 Summary of JMS Servers



5. Click **New**.

The **Create a New JMS Server - JMS Server Properties** screen displays.

Figure 7-31 Create a New JMS Server - JMS Server Properties



For more information, refer to the fields description table.

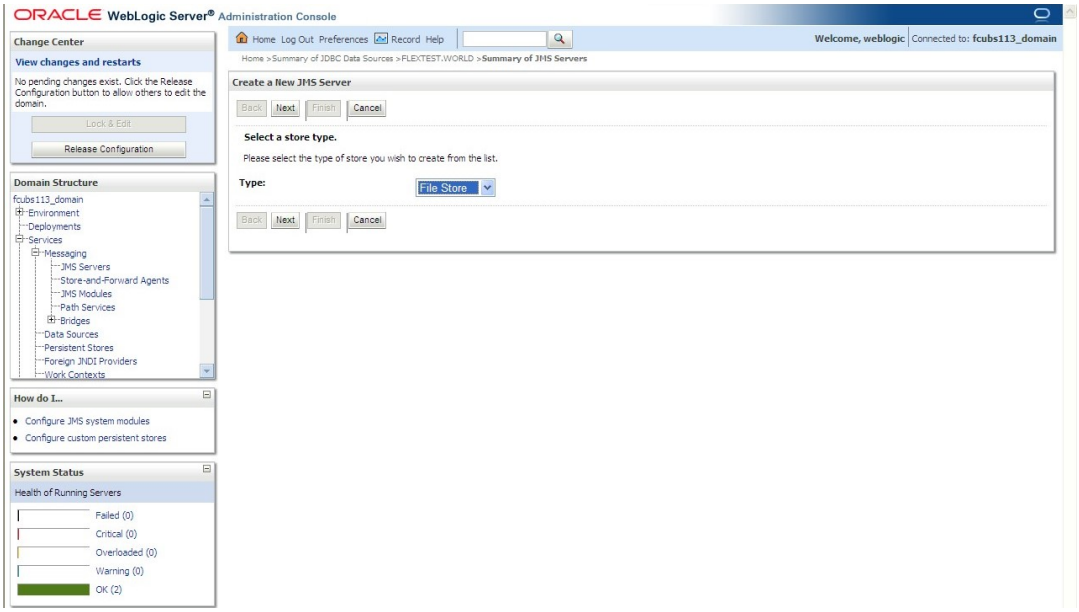
Table 7-5 Create a New JMS Server

Field	Description
JMS Server Name	Specify the name of JMS Server.

6. Click **Create a new Store** button.

   The **Create a New JMS Server - Select store type** screen displays.

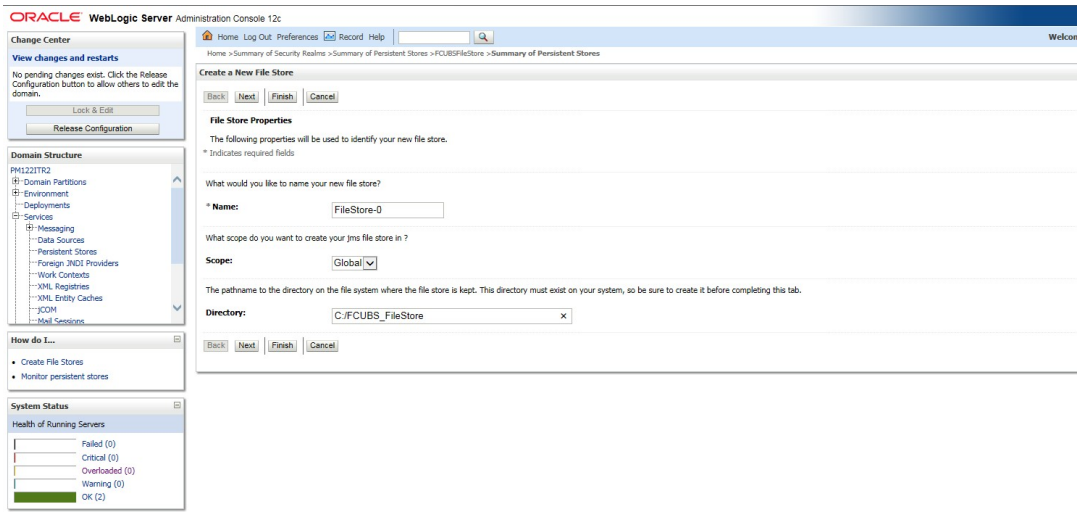
Figure 7-32 Create a New JMS Server - Select store type



7. Select the **Type** as **File Store** from the drop-down.
8. Click **Next**.

   The **Create a New JMS Server - File Store Properties** screen displays.

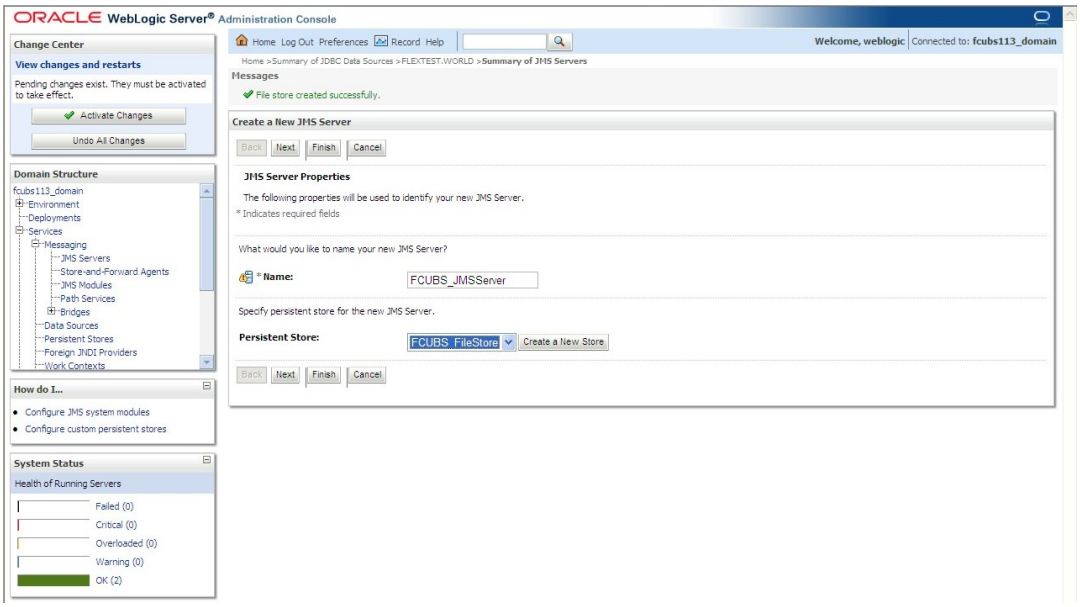
Figure 7-33 Create a New JMS Server - File Store Properties



9. To identify the new **File Store**, specify the following properties:
   a. Specify the file store name as **FCUBS_FileStore**.
   b. Select a server. For this file store, you may select **ManagedServer1** (created by the user).
   c. Specify the **File store** Directory path as `C:/FCUBS_FileStore`.
   d. Click **OK**.
10. Click **Next** and the message `File store created successfully` displays.

    The **Create a New JMS Server - Messages** screen displays.

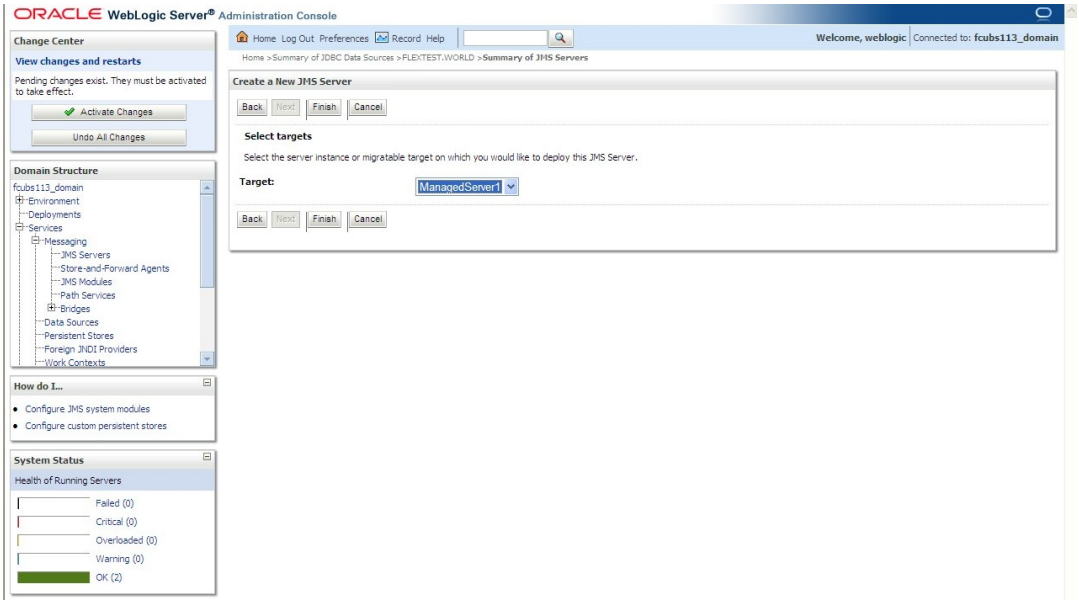
Figure 7-34 Create a New JMS Server - Messages



11. Click **Next**.

    The **Create a New JMS Server - Select Targets** screen displays.

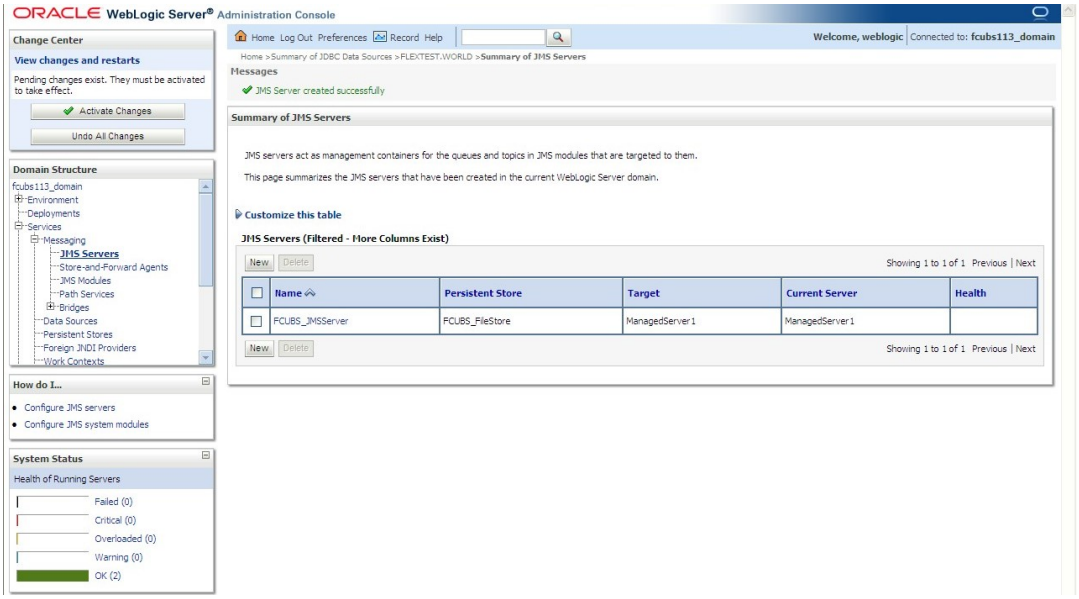
Figure 7-35 Create a New JMS Server - Select Targets



12. Select the **Target** as **ManagedServer1**.
13. Click on **Finish** and the message `JMS Server created successfully` displays.

    The **Summary of JMS Servers - Messages** screen displays.

Figure 7-36 Summary of JMS Servers - Messages



14. Click the **Activate Changes** button under **Change Center**.

    The message `All the changes have been activated. No restarts are necessary` displays.

The **JMS Server** is created.

7.1.3 Create JMS Modules

This topic explains the systematic instructions to create the JMS Modules in the Weblogic application server.

To create the JMS Modules, follow the steps given below:

1. Start the Administrative Console of the WebLogic application server. Enter the Oracle WebLogic Admin Console URL in the address bar in an internet browser. For example: http://10.10.10.10:1001/console.

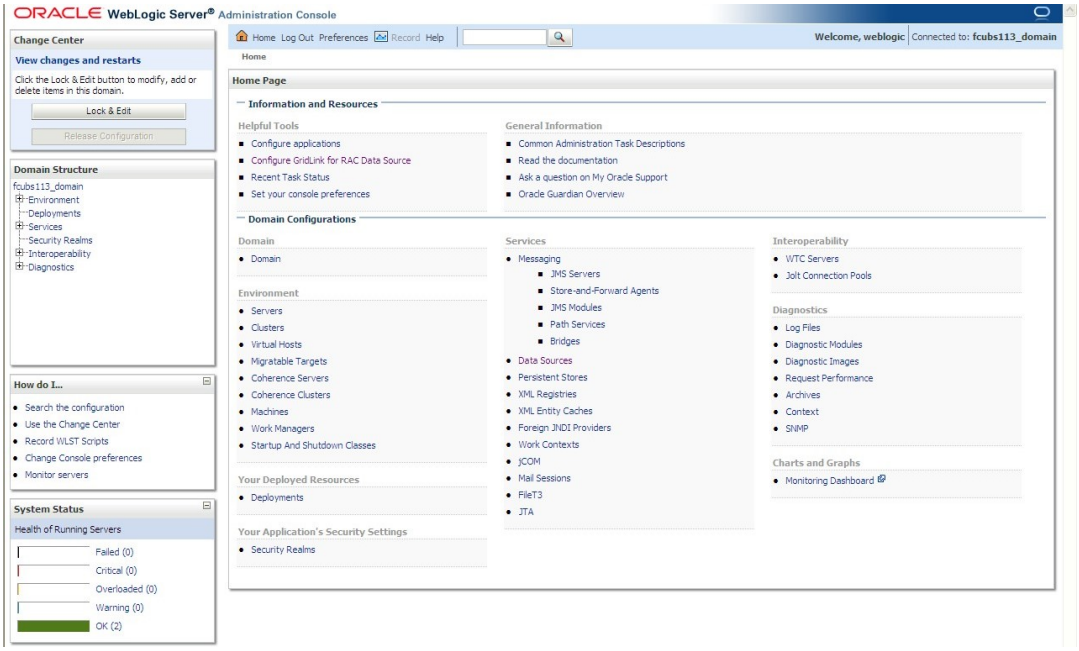
   The **Oracle Weblogic Server - Welcome** screen displays.

Figure 7-37 Oracle Weblogic Server - Welcome

2. Specify the WebLogic administrator **Username**, **Password** and click **Log In**.
3. Navigate to Oracle Weblogic home page.

   The **Oracle Weblogic Server - Home Page** screen displays.

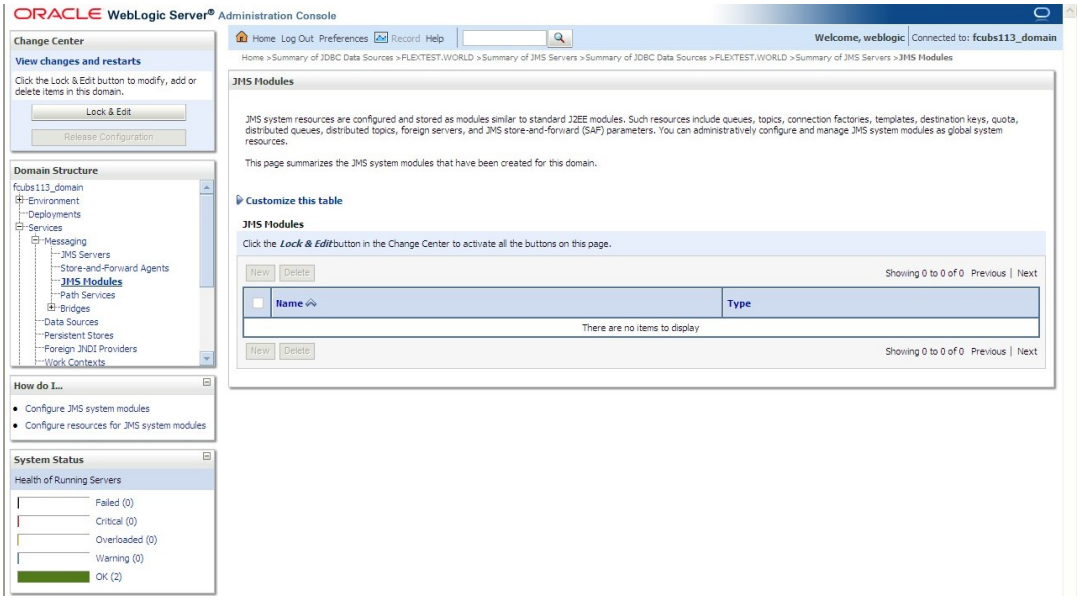
Figure 7-38 Oracle Weblogic Server - Home Page



4. On the left pane, under **Domain Structure**, expand **Services**, **Messaging** and **JMS Modules** under it.

   The **JMS Modules** screen displays.

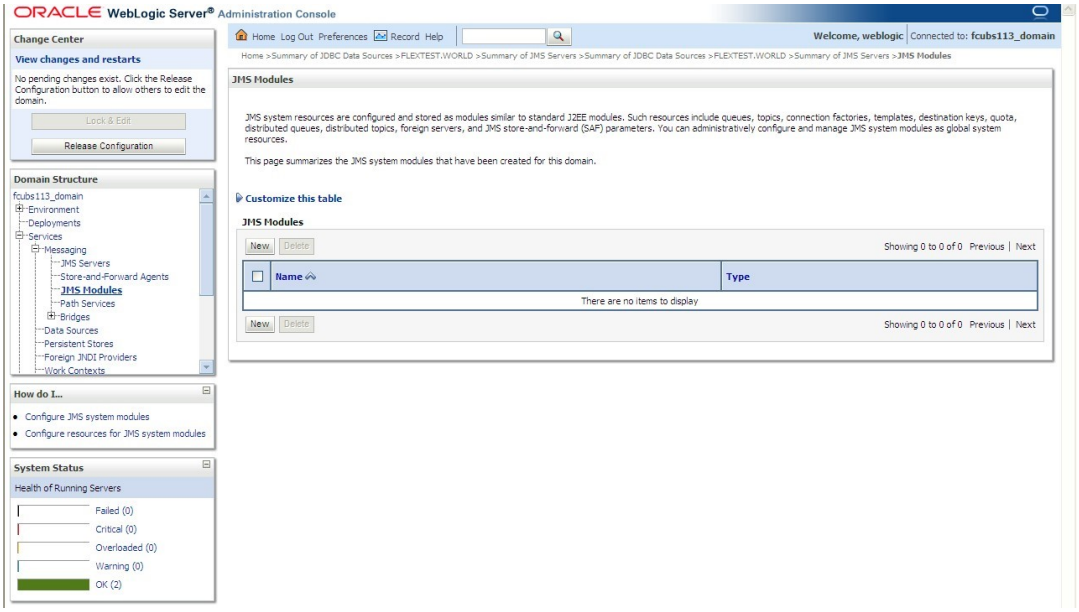
Figure 7-39 JMS Modules



5. To create new **JMS Module**, click the **Lock & Edit** button under the **Change Center**.

   The **JMS Modules - New** screen displays.

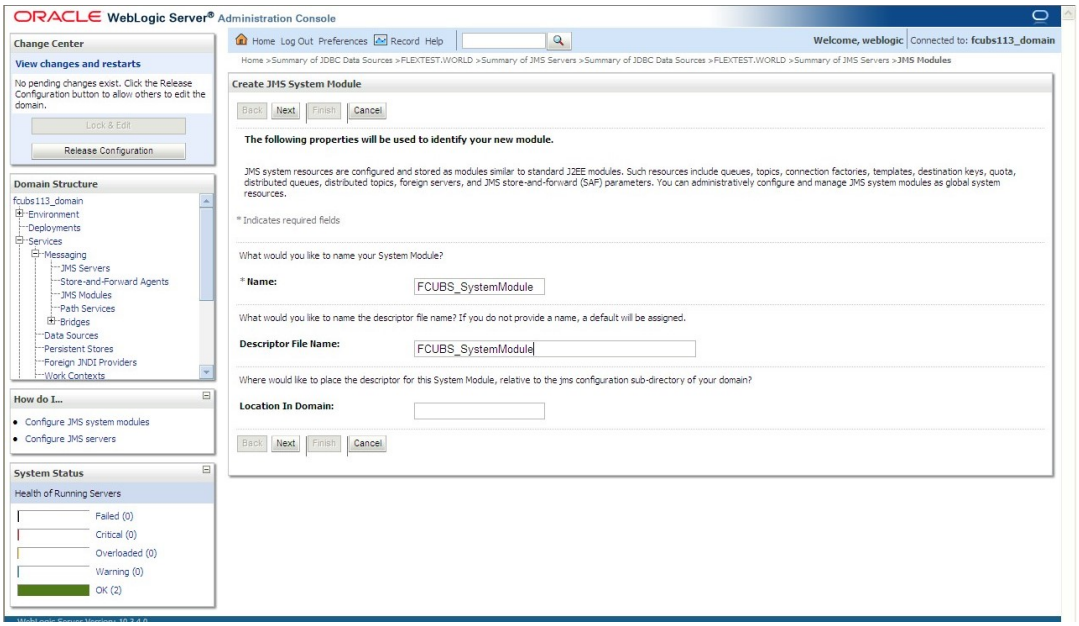
Figure 7-40 JMS Modules - New



6. On the **JMS Modules** screen, click **New**.

   The **Create JMS System Module** screen displays.

Figure 7-41 Create JMS System Module



For more information on fields, refer to the field description table.

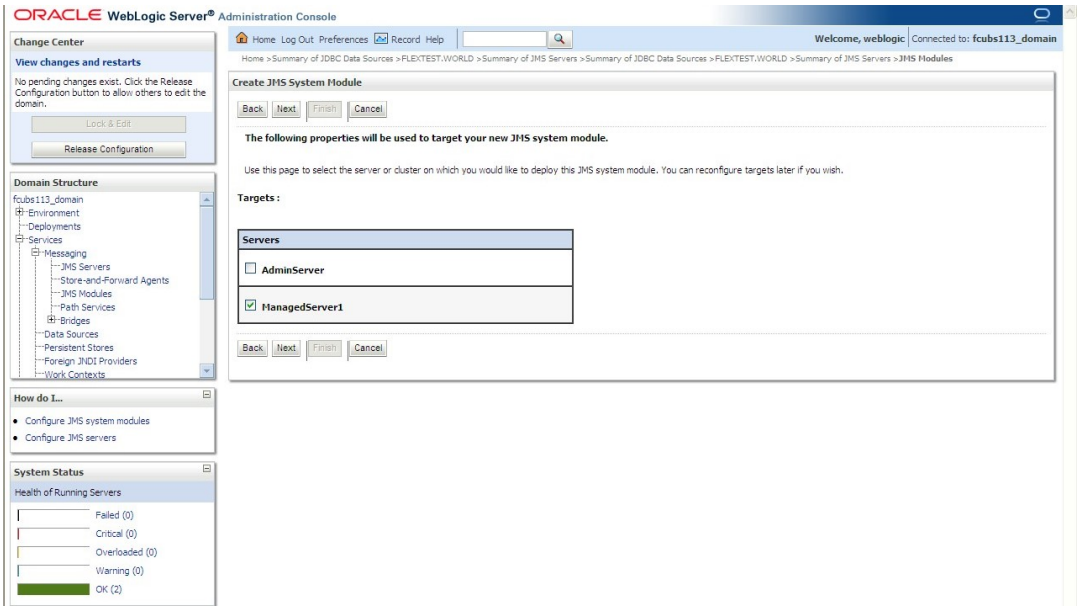
Table 7-6 Create JMS System Module

Field	Description
Name	Enter the System Module Name as **FCUBS_SystemModule**.
Description File Name	Enter the Description File Name as **FCUBS_SystemModule**.

7. Click **Next**.

   The **Create JMS System Module - Targets** screen displays.

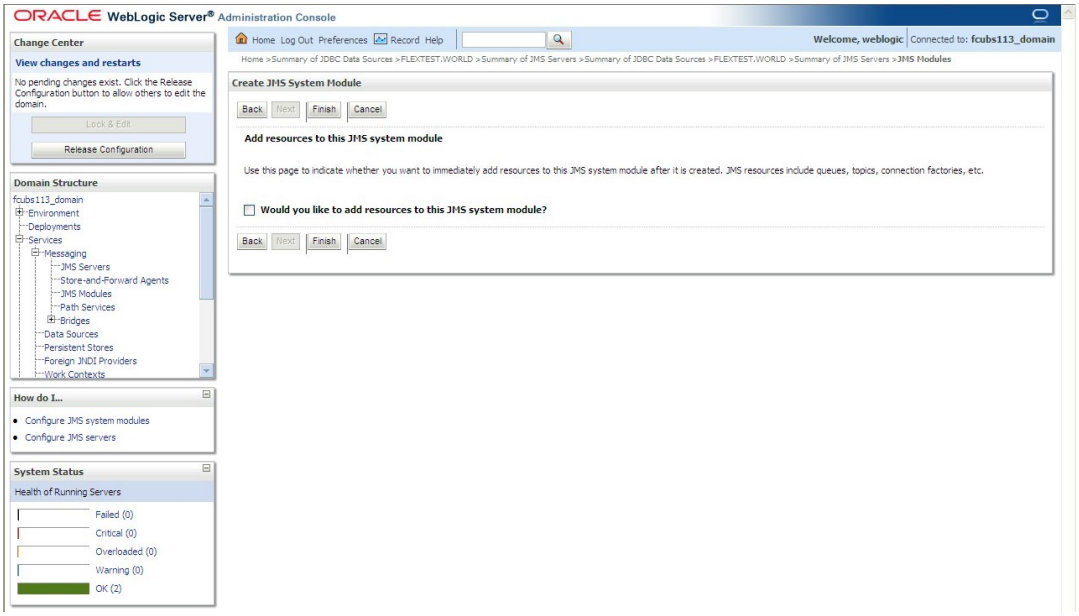
Figure 7-42 Create JMS System Module - Targets



8. Select the check box against the server created and click **Next**.

   The **Create JMS System Module - Add Resources** screen displays.

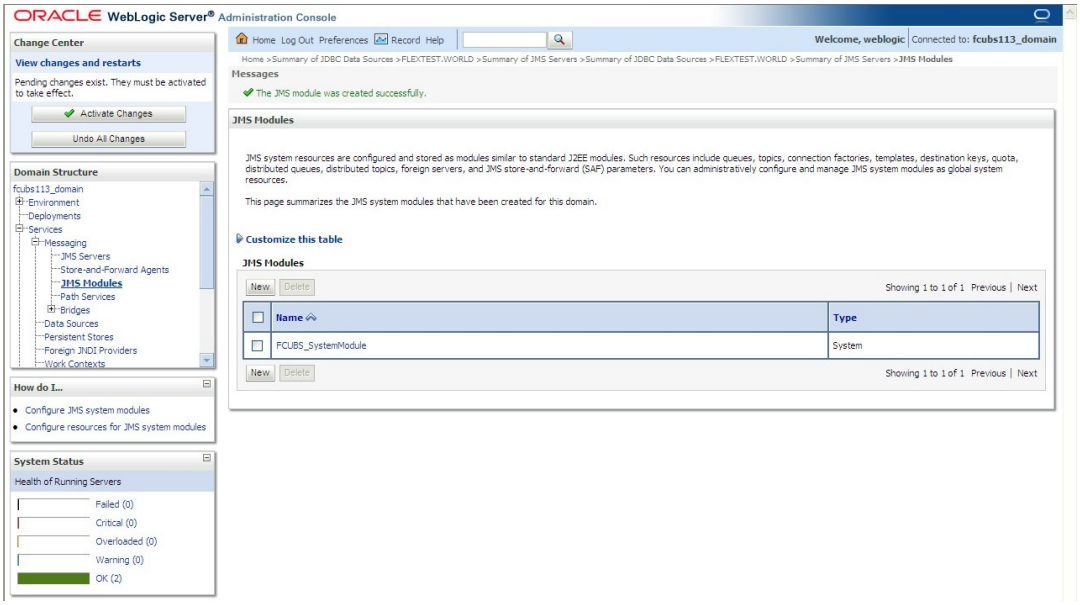
Figure 7-43 Create JMS System Module - Add Resources



9. Click the **Finish** button.

   The message displays on the **JMS Modules - Message** screen confirming that `JMS was created successfully`

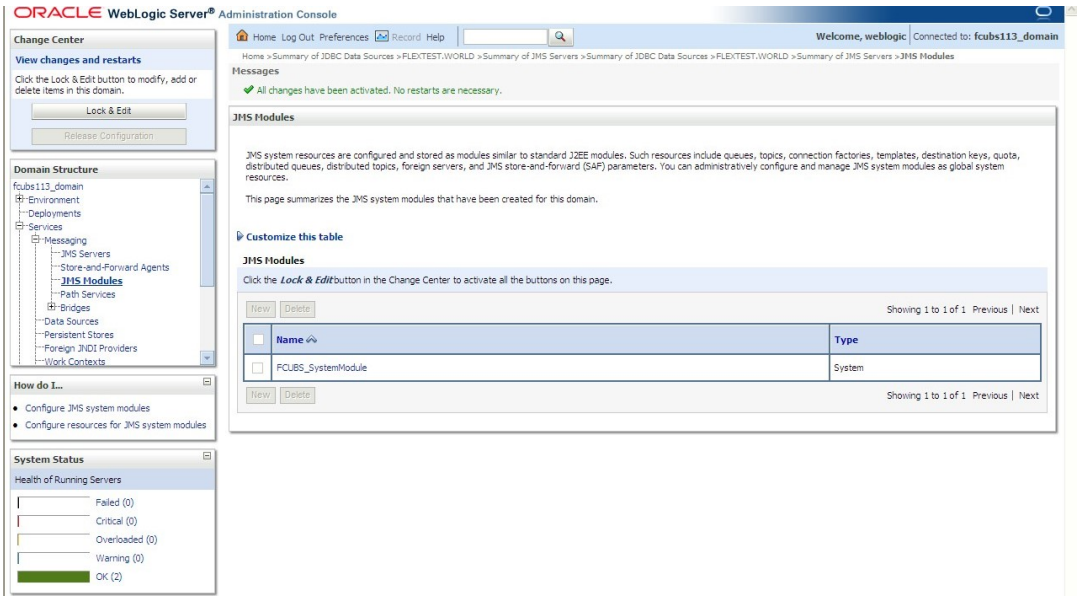
Figure 7-44 JMS Modules - Message



10. Click the **Activate Changes** button under **Change Center**. The message `All the changes have been activated. No restarts are necessary` displays.

    The **JMS Modules - Activate Changes** screen displays.

Figure 7-45 JMS Modules - Activate Changes Message



The **JMS Module** is created.

7.1.4 Create Subdeployment

This topic explains the systematic instructions to create the subdeployment in the Weblogic application server.

To create the subdeployments, follow the steps given below:

1. Start the Administrative Console of the WebLogic application server. Enter the Oracle WebLogic Admin Console URL in the address bar in an internet browser. For example: http://10.10.10.10:1001/console.

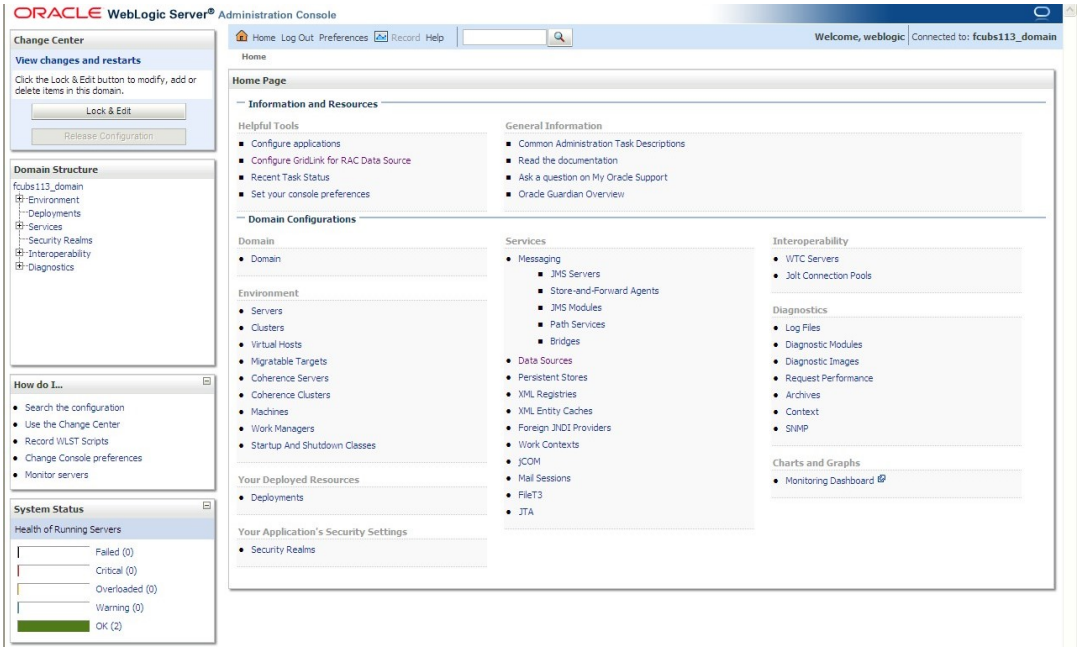
   The **Oracle Weblogic Server - Welcome** screen displays.

Figure 7-46 Oracle Weblogic Server - Welcome

2. Specify the WebLogic administrator **Username**, **Password** and click **Log In**.
3. Navigate to Oracle Weblogic home page.

   The **Oracle Weblogic Server - Home Page** screen displays.

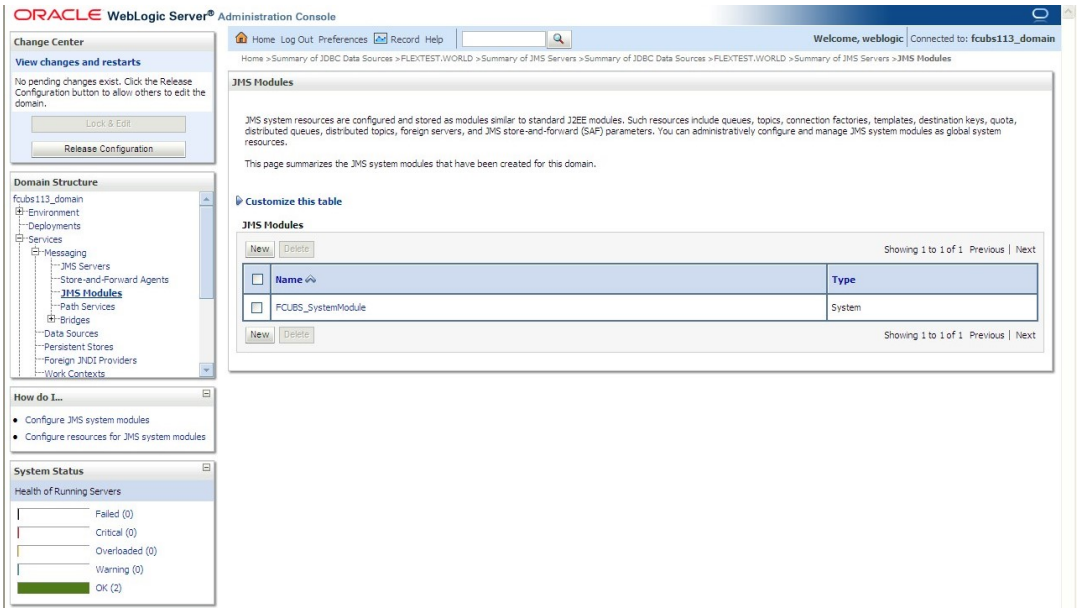
Figure 7-47 Oracle Weblogic Server - Home Page



4. On the left pane, under **Domain Structure**, **expand Services**, **Messaging** and **JMS Modules** under it.
5. Click the **Lock & Edit** button under the **Change Center**.

   The **JMS Modules** screen displays.

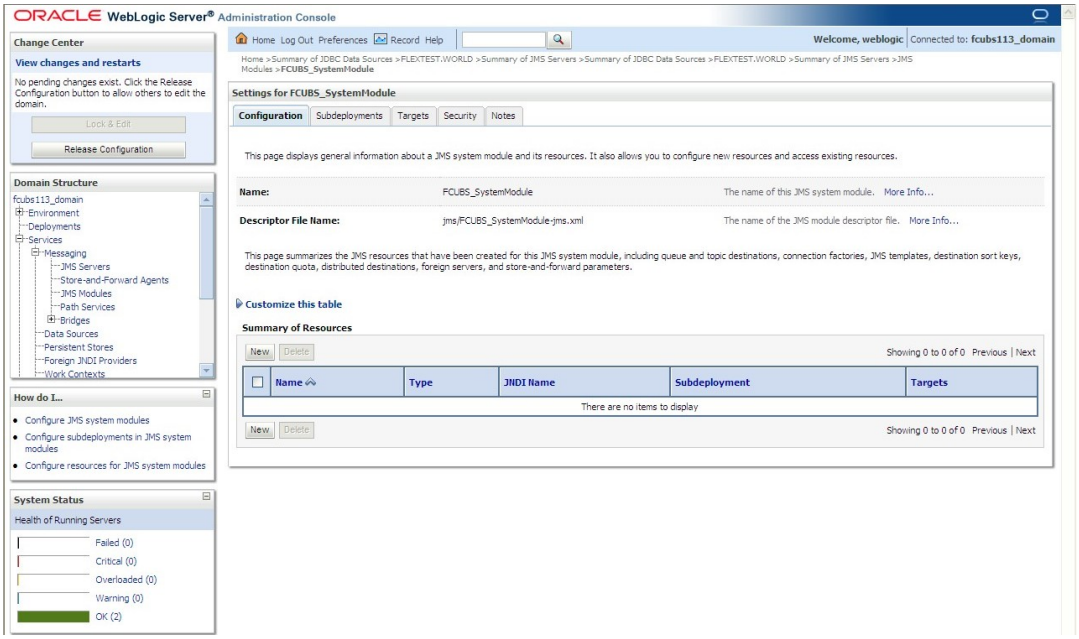
Figure 7-48 JMS Modules



6. Select the JMS module created earlier.

   The **Settings for FCUBS_SystemModule** screen displays.

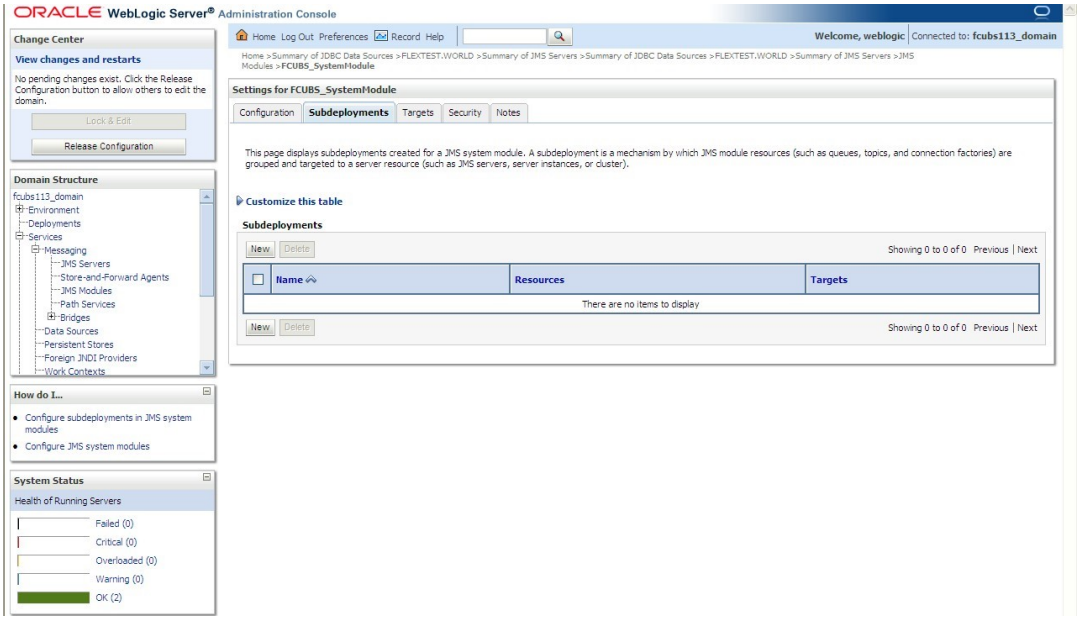
Figure 7-49 Settings for FCUBS_SystemModule



7. Click on **Subdeployments** tab.

   Settings for FCUBS_SystemModule - Subdeployments tab displays.

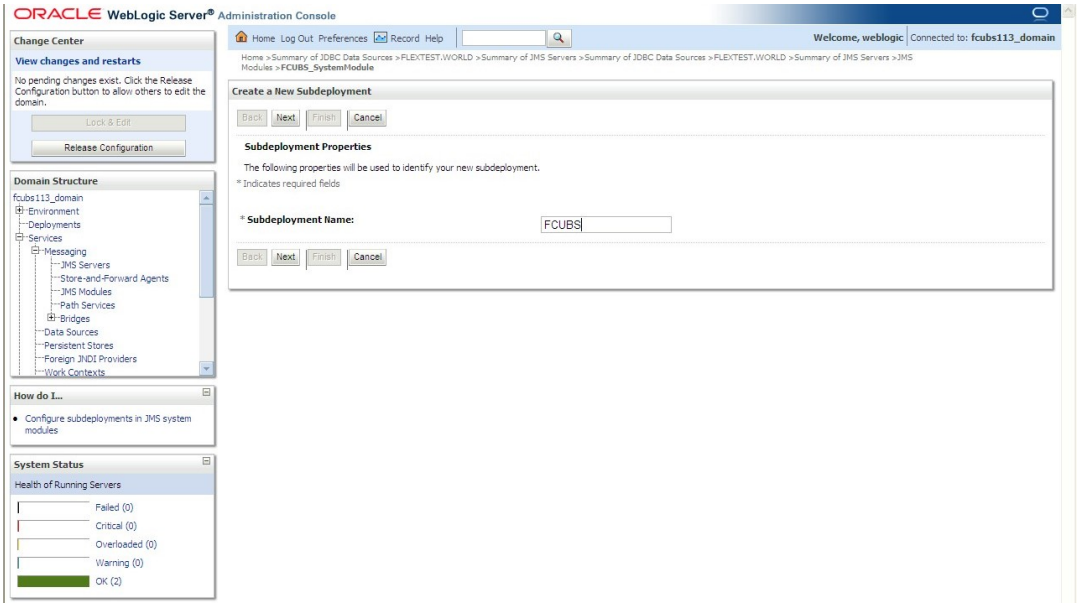
Figure 7-50 Settings for FCUBS_SystemModule - Subdeployments tab



8. On the **Subdeployments** tab, click **New**.

   The **Create a New Subdeployment** screen displays.

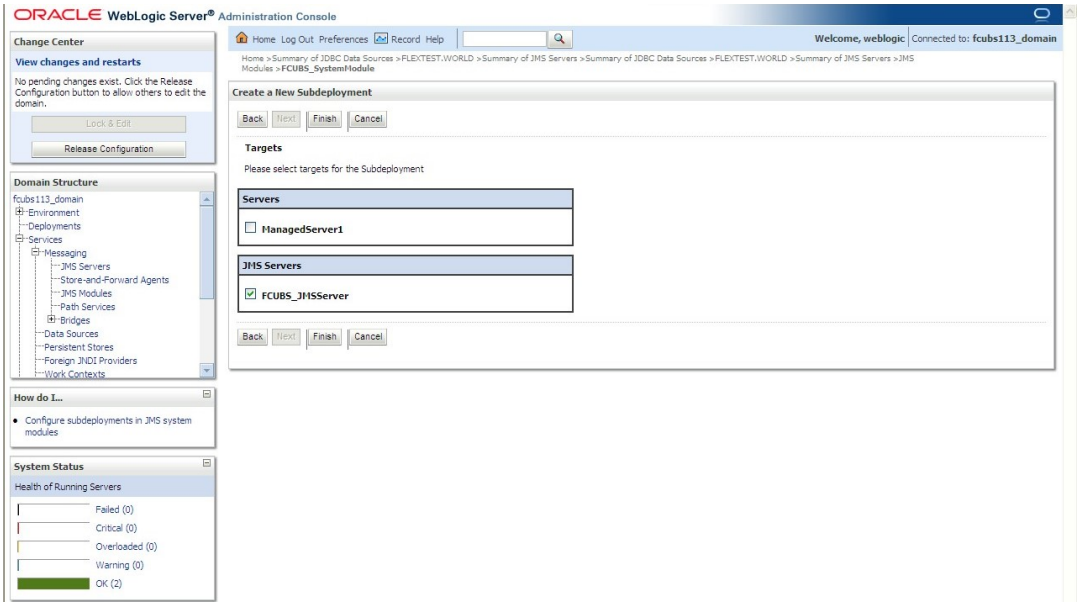
Figure 7-51 Create a New Subdeployment



9. On **Create a New Subdeployment** screen, specify the Subdeployment Name as **FCUBS** and click **Next**.

   The **Create a New Subdeployment - Targets** screen displays.

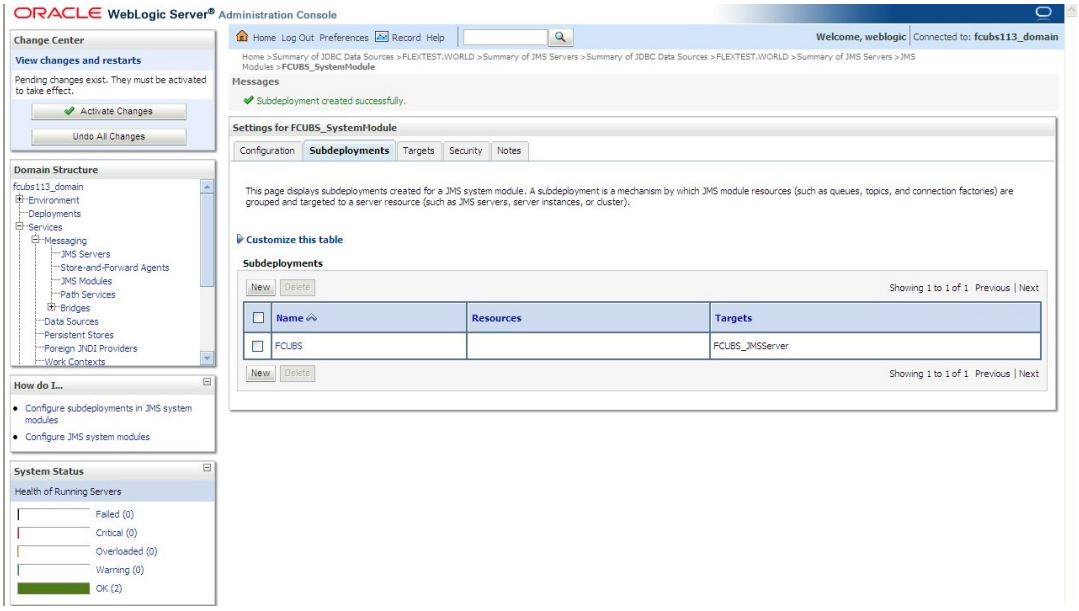
Figure 7-52 Create a New Subdeployment - Targets



10. Select the **JMS Server** (as created by the user).
11. Click the **Finish** button.

    The **FCUBS** subdeployment displays in the **Settings for FCUBS_SystemModule - Messages** screen.

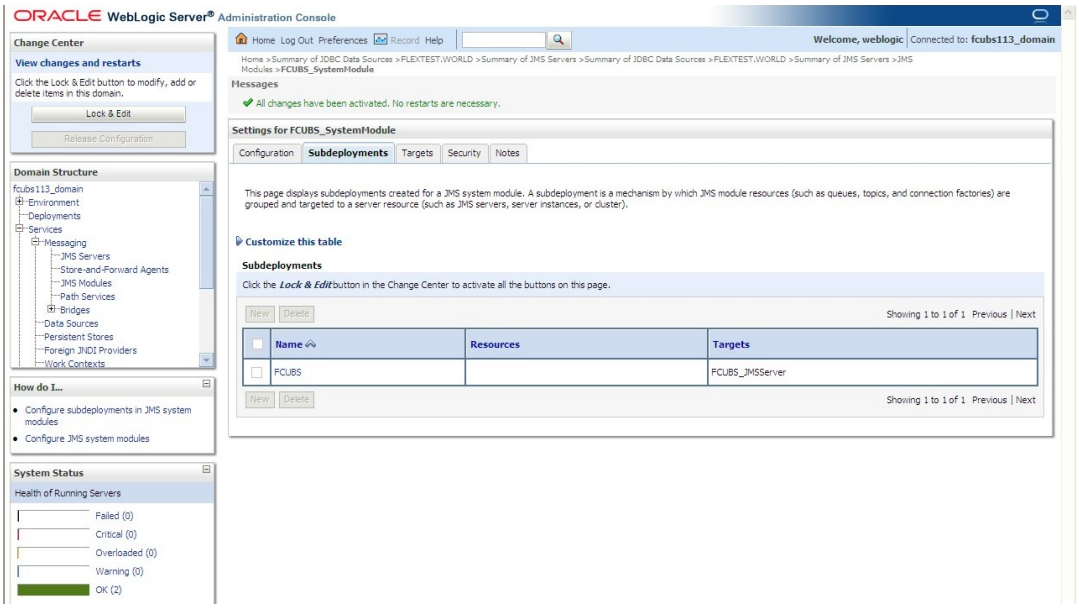
Figure 7-53 Settings for FCUBS_SystemModule - Messages



12. Click the **Activate Changes** button under **Change Center**. The message `All the changes have been activated. No restarts are necessary` displays.

    The **Settings for FCUBS_SystemModule - Activate changes Messages** screen displays.

Figure 7-54 Settings for FCUBS_SystemModule - Activate Changes Messages



The **Subdeployment** is created.

7.1.5 Create JMS Queue

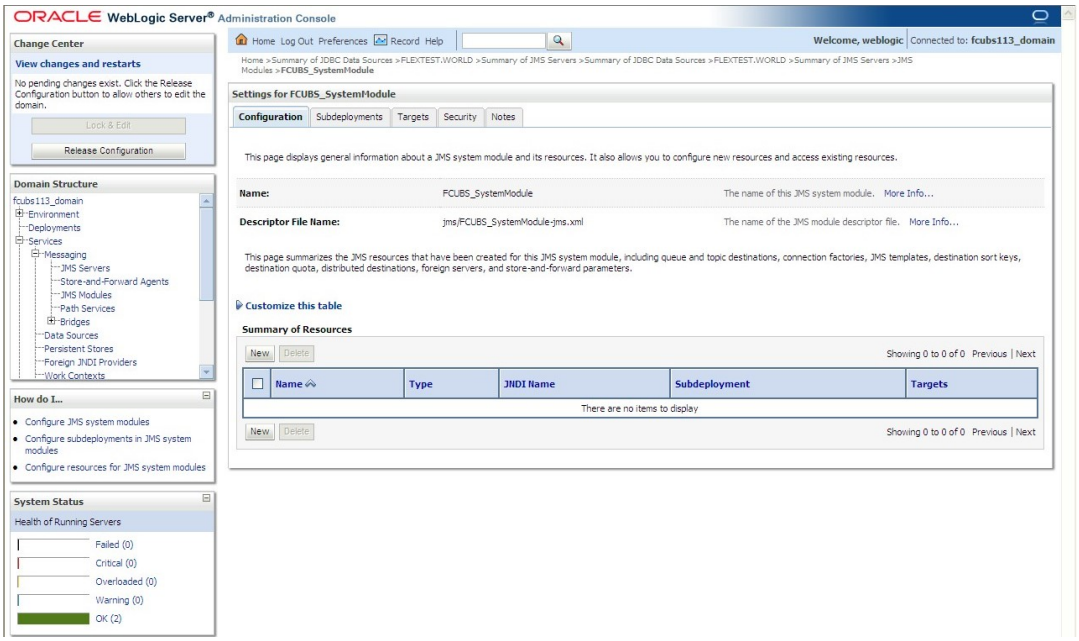
This topic provides the systematic instructions to create the JMS Queue in the Weblogic application server.

To create the JMS Queue, follow the steps given below:

1. Select the JMS Module created earlier.
2. Click on the **Configuration** tab and then click **Lock & Edit** button under **Change Center**.

   The **Settings for FCUBS_SystemModule - Configuration** tab displays.

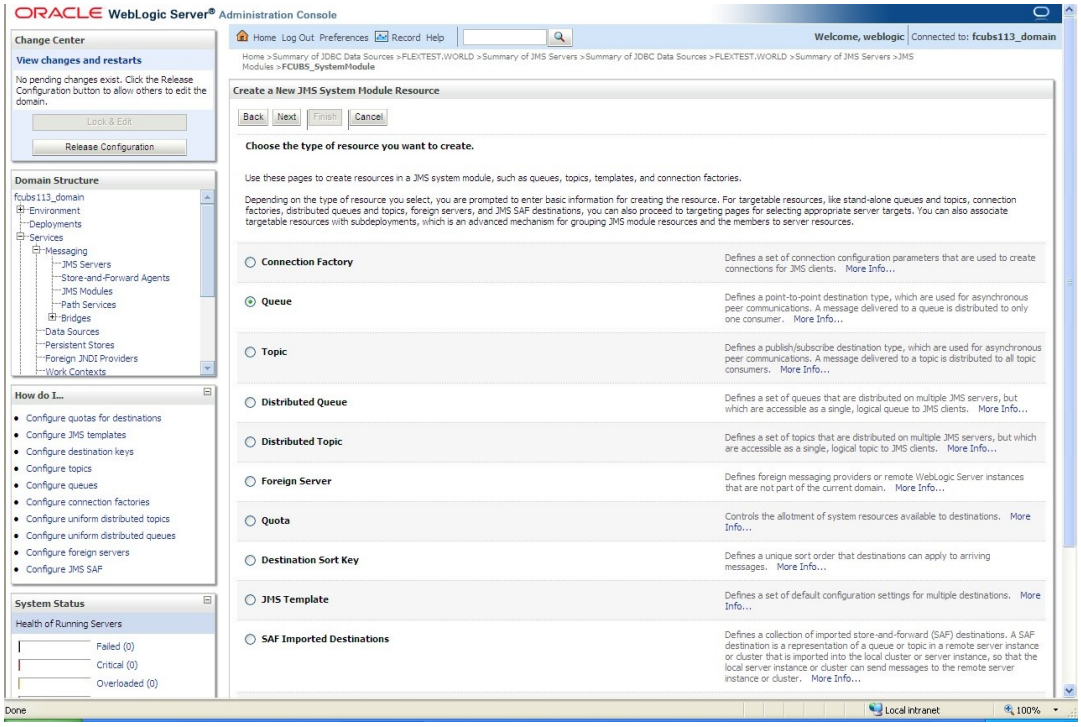
Figure 7-55 Settings for FCUBS_SystemModule



3. On the **Settings for FCUBS_SystemModule - Configuration** tab, click **New**.

   The **Create a New JMS System Module Resource** screen displays.

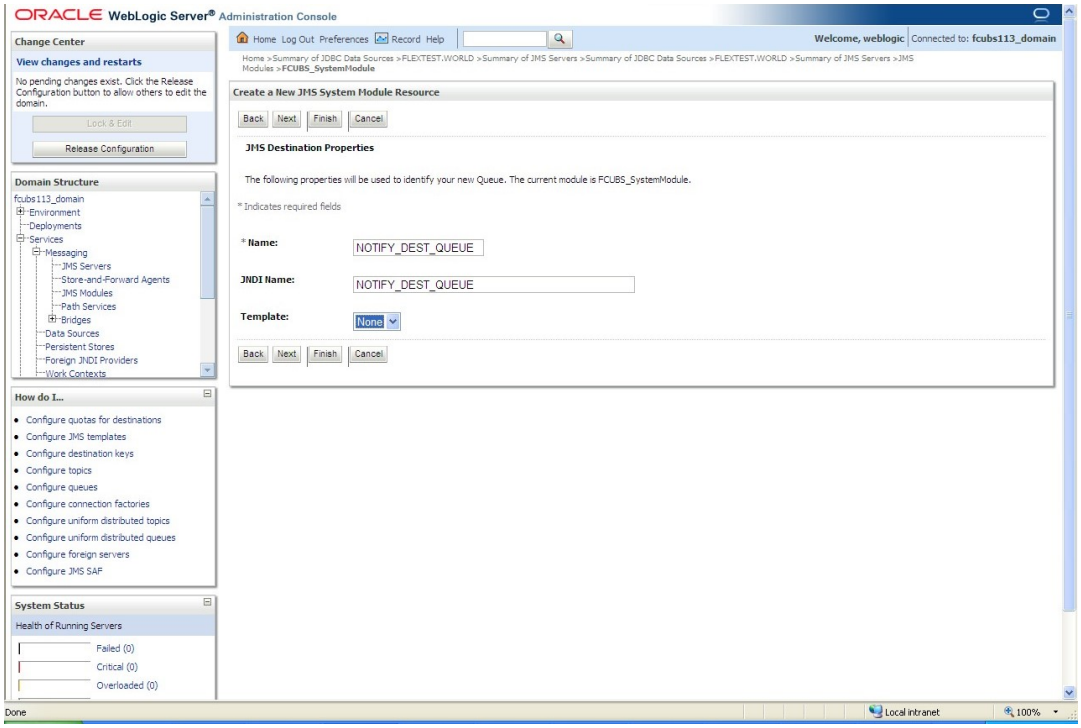
Figure 7-56 Create a New JMS System Module Resource



4. Select the **Queue** option and then click **Next**.

   The **Create a New JMS System Module Resource - JMS Destination Properties** screen displays.

Figure 7-57 Create a New JMS System Module Resource - JMS Destination Properties



For more information, refer to the fields description table.

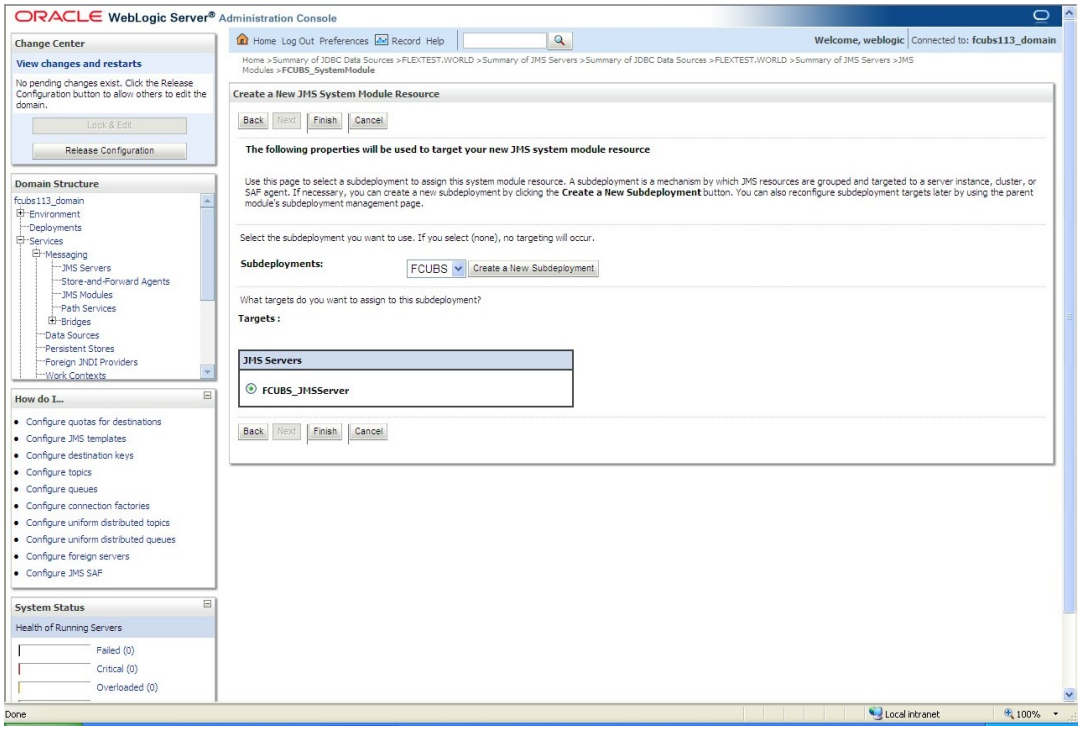
Table 7-7 JMS Destination Properties

Filed	Description
Name	Specify the Name of the Queue as **NOTIFY_DEST_QUEUE**.
JNDI Name	Specify the JNDI Name as **NOTIFY_DEST_QUEUE**
Template	Select the Template as **None** from the drop-down.

5. Click **Next**.

The **Create a New JMS System Module Resource - Select Subdeployment** screen displays.

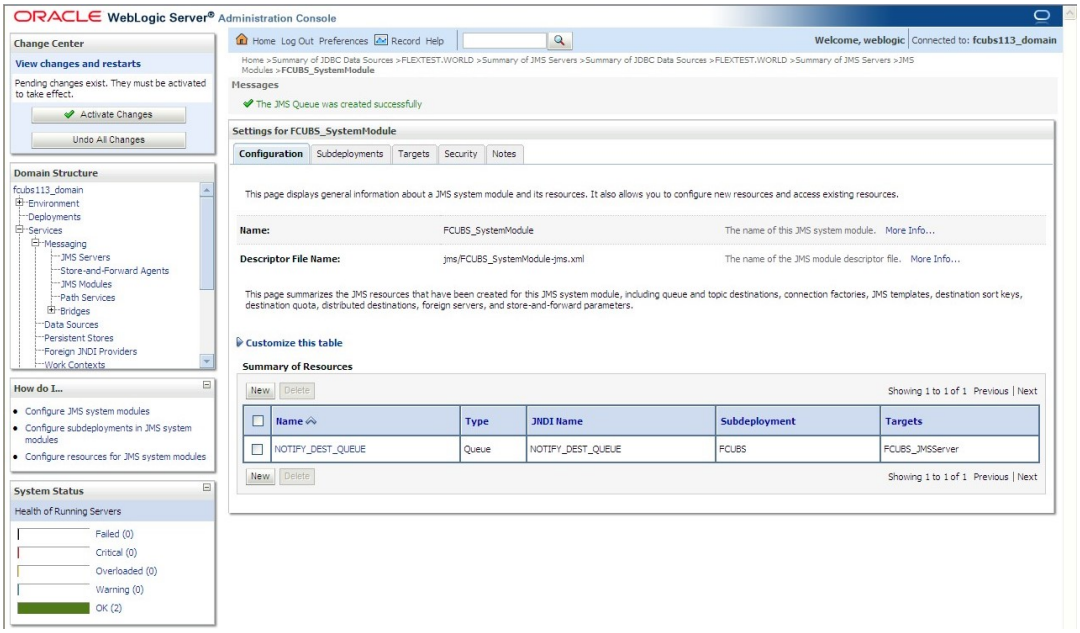
Figure 7-58 Create a New JMS System Module Resource - Select Subdeployment



6. Select the managed server created and click **Finish** button.

The new **JMS System Module Resource** is created and displays a message on the **Setting for FCUBS_SystemModule** screen confirming that `JMS Queue are created successfully`.

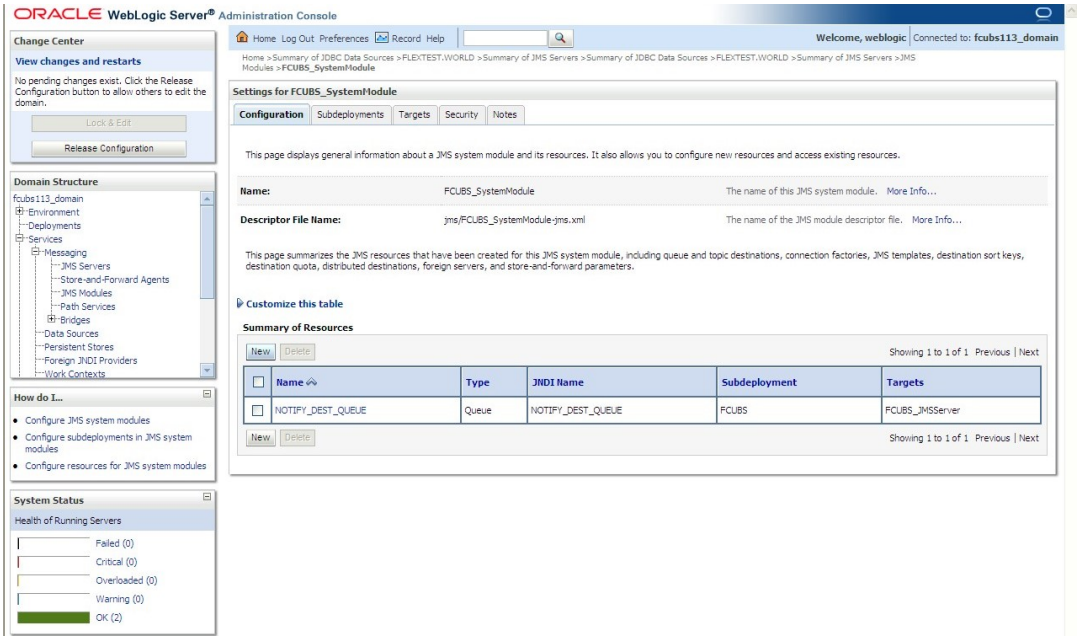
Figure 7-59 Settings for FCUBS_SystemModule - JMS Queue Messages



7. Click the **Activate Changes** button under **Change Center**.

   The message displays on the **Settings for FCUBS_SystemModule** screen confirming that `All the changes have been activated. No restarts are necessary.`

Figure 7-60 Settings for FCUBS_SystemModule - JMS Queue Activate changes Messages



8. Click **New** to create more Queues. Follow the steps from 3 to 7.

The **JMS Queue** has been created successfully.

7.1.6 Create JMS Connection Factory

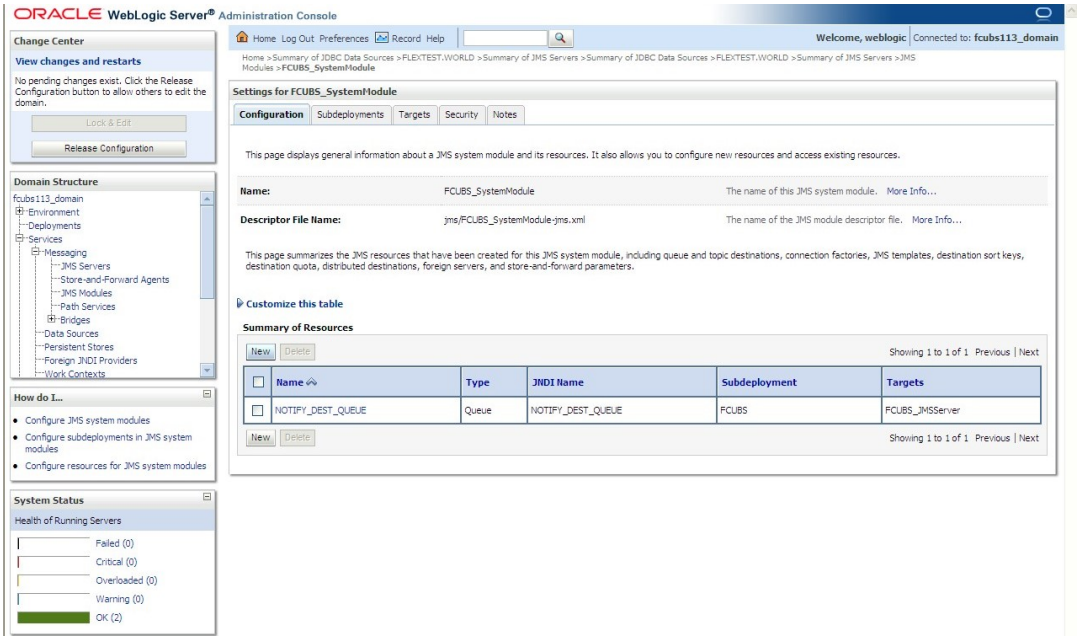
This topic explains the systematic instructions to create the JMS Connection Factory in the Weblogic application server.

After creating the queues, you need to create the connection factory. To create the JMS Connection Factory, follow the steps given below:

1. On the **Settings for FCUBS_SystemModule - Configuration** tab, select the newly created JMS Queue module.

   The **Settings for FCUBS_SystemModule - Configuration** tab displays.

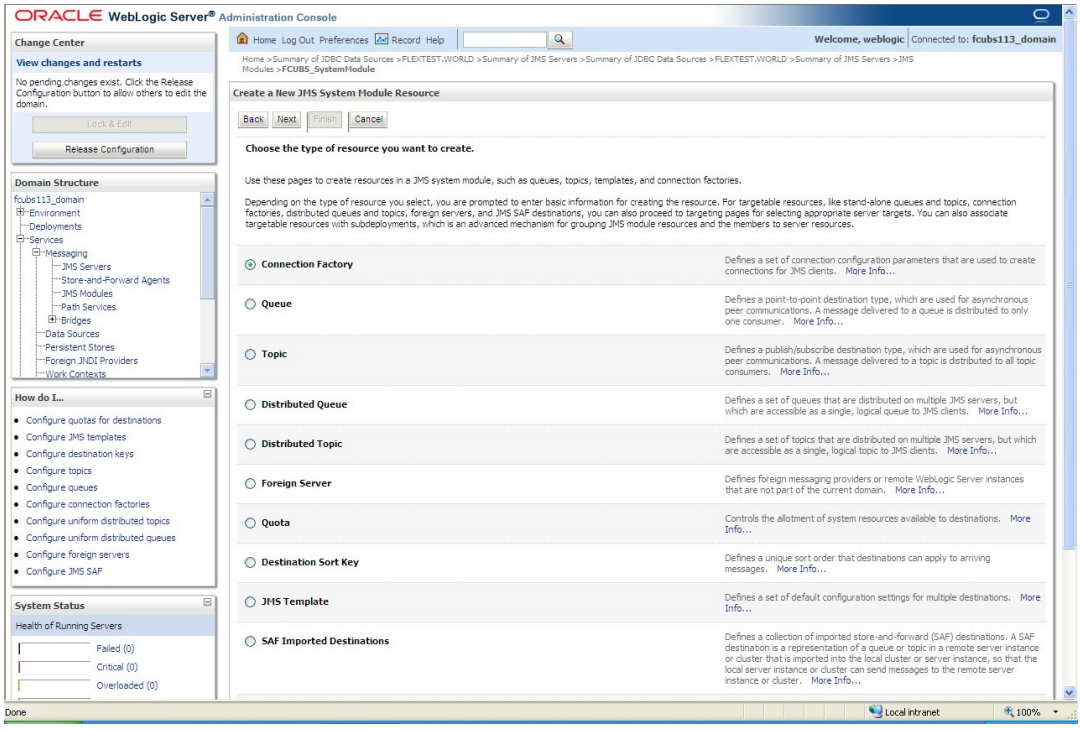
Figure 7-61 Settings for FCUBS_SystemModule



2. Click **New**.

   The **Create a New JMS System Module Resource** screen displays.

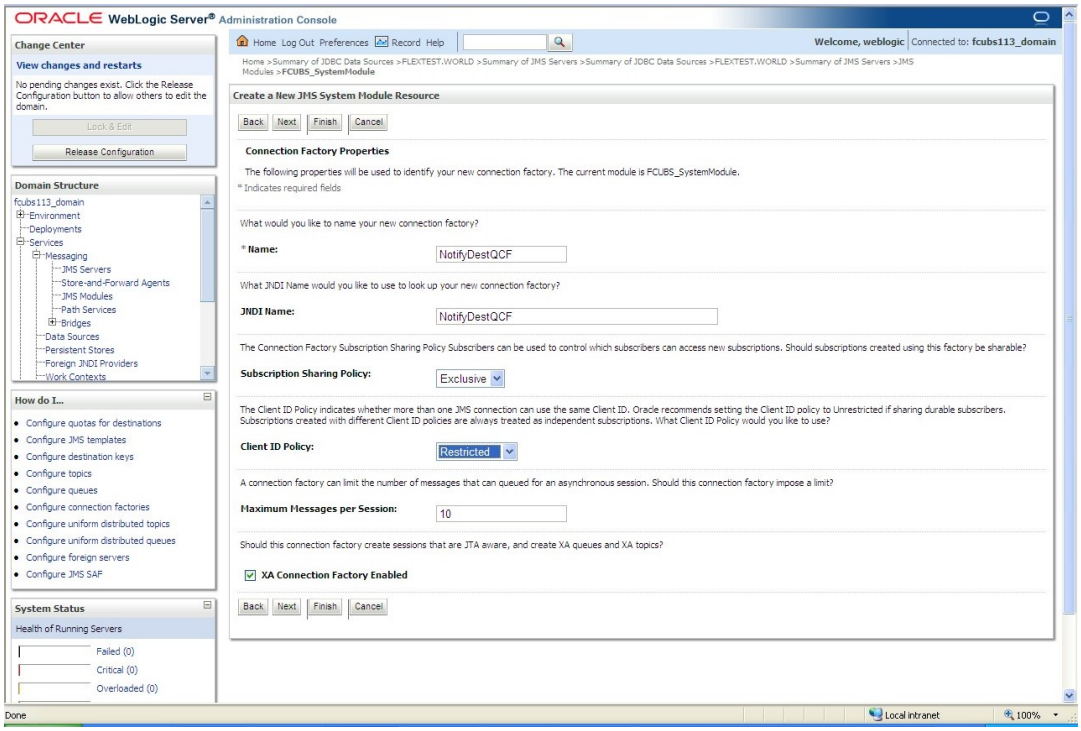
Figure 7-62 Create a New JMS System Module Resource



3. Select the **Connection Factory** option and then click **Next**.

   The **Create a New JMS System Module Resource - Connection Factory Properties** screen displays.

Figure 7-63 Create a New JMS System Module Resource - Connection Factory Properties



For more information, refer to the fields description table.

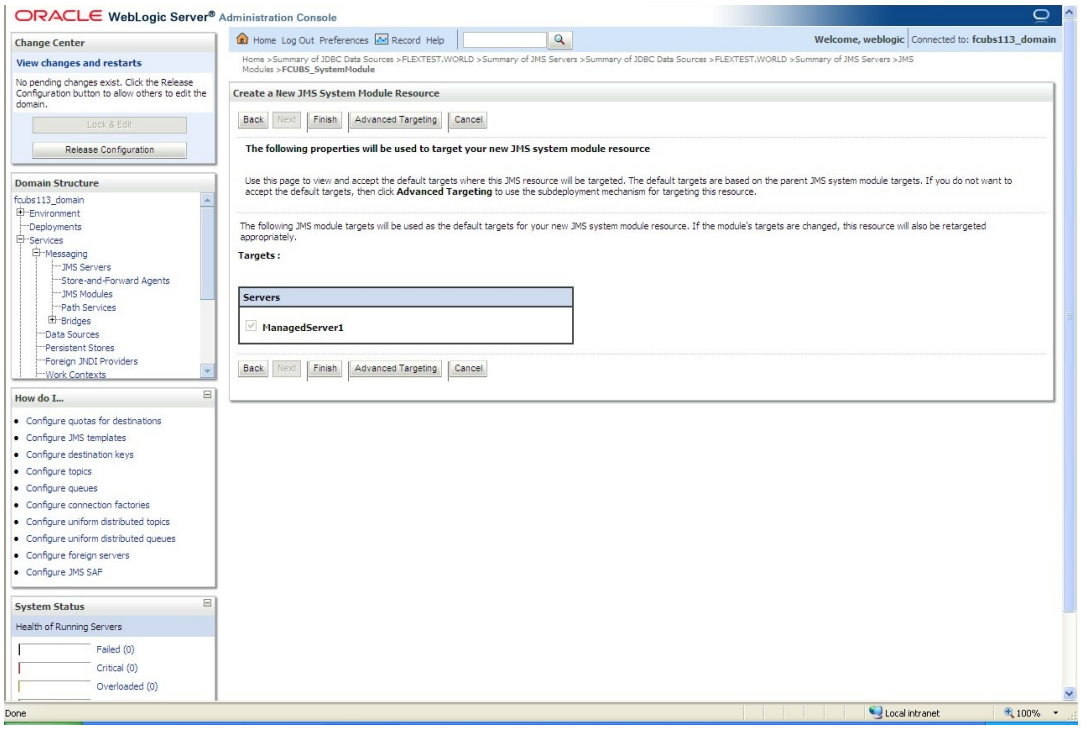
Table 7-8 Connection Factory Properties

Filed	Description
Name	Specify the Name of the Connection factory as**NotifyDestQCF**.
JNDI Name	Specify the JNDI Name as **NotifyDestQCF**
Client ID Policy	Select the Client ID policy as **Restricted** from the drop-down.

4. Select the **XA Connection Factory Enabled** check box and click **Next**.

   The **Create a New JMS System Module Resource - Targets** screen displays.

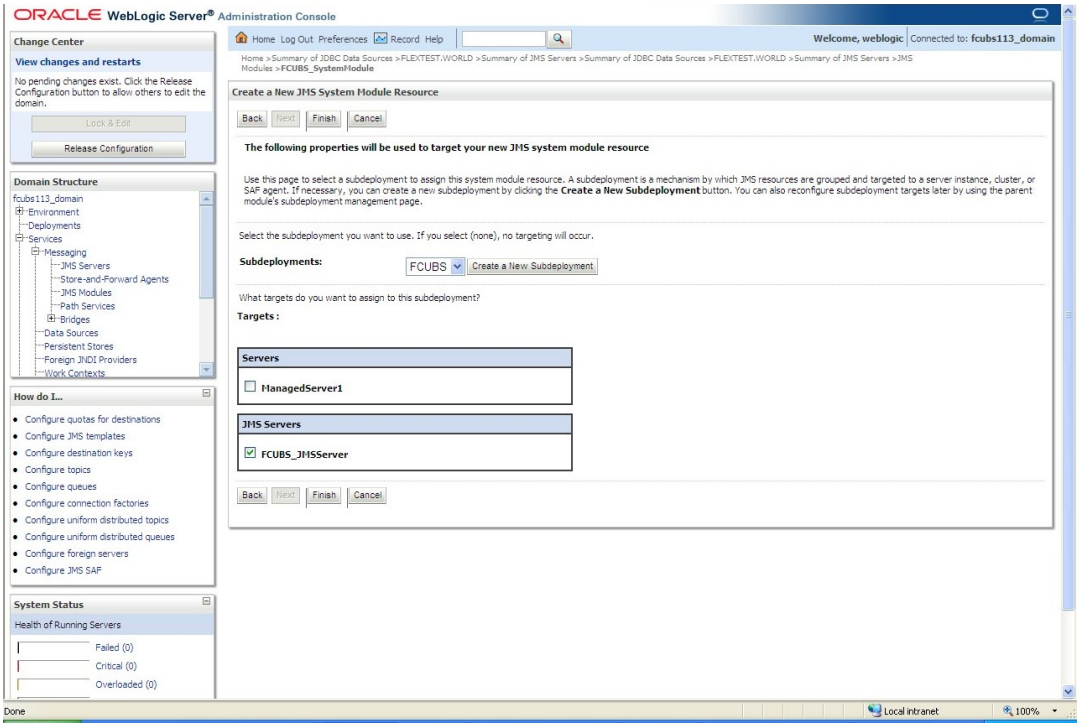
Figure 7-64 Create a New JMS System Module Resource - Targets



5. Click on the **Advanced Targeting**.

   The **Create a New JMS System Module Resource - Advance Targeting** screen displays.

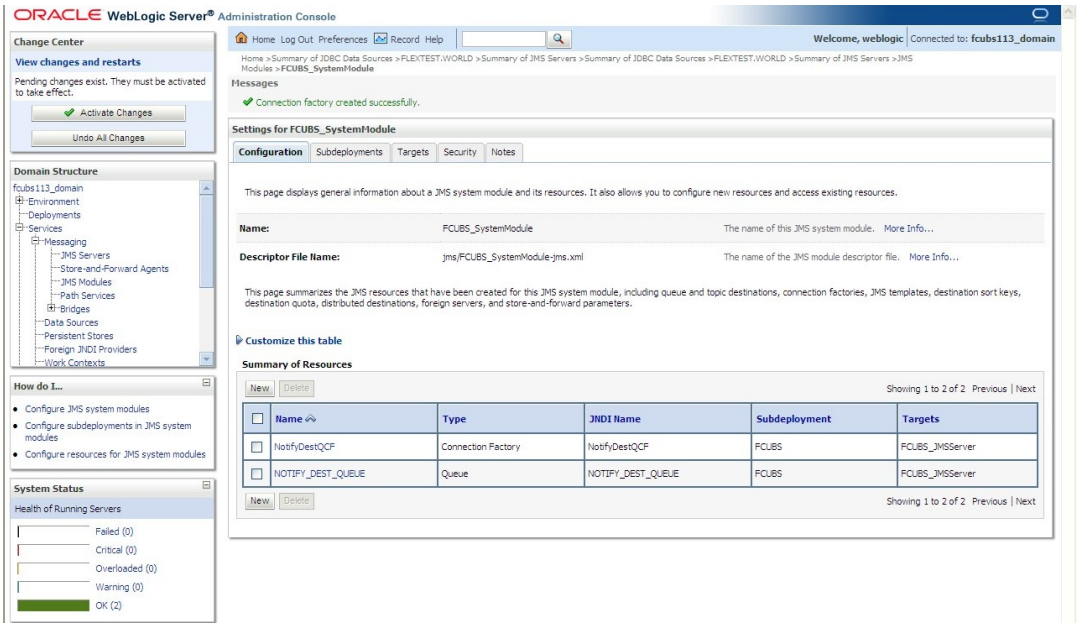
Figure 7-65 Create a New JMS System Module Resource - Advance Targeting



6. Select the **Subdeployments** as **FCUBS** from the drop-down list.
7. Under the JMS Servers, select the check box against **Managed Server**.
8. Click **Finish**.

   The message displays on the **Settings for FCUBS_SystemModule** screen confirming that `Connection Factory created successfully`.

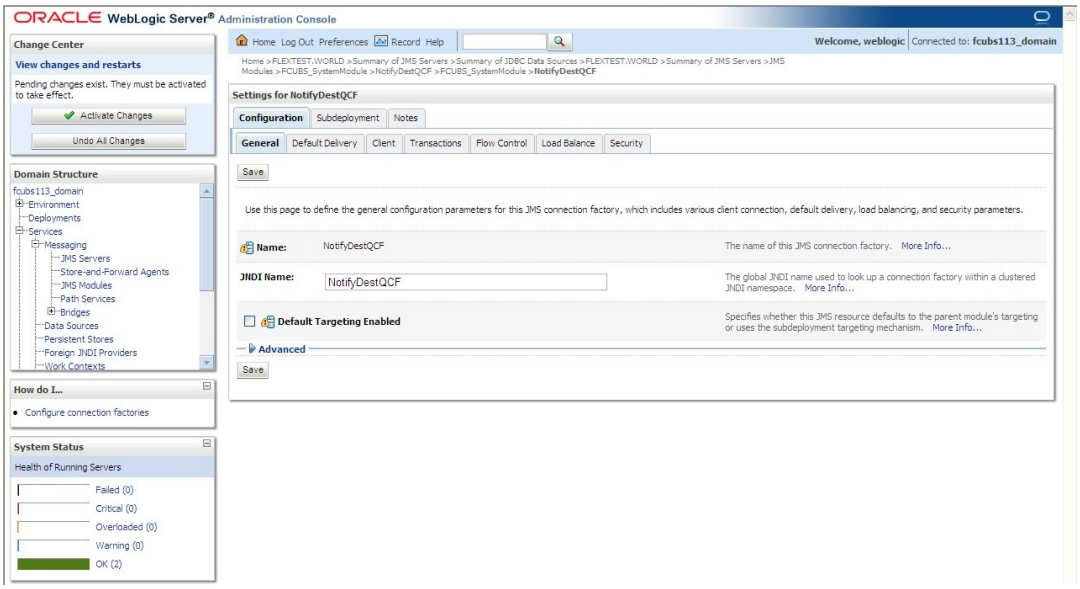
Figure 7-66 Settings for FCUBS_SystemModule - Connection Factory Messages



9. To have the XA Connection Factory enabled, click the Connection Factory **NotifyDestQCF** from the **Summary of Resources** table.

   The **Settings for NotifyDestQCF** screen displays.

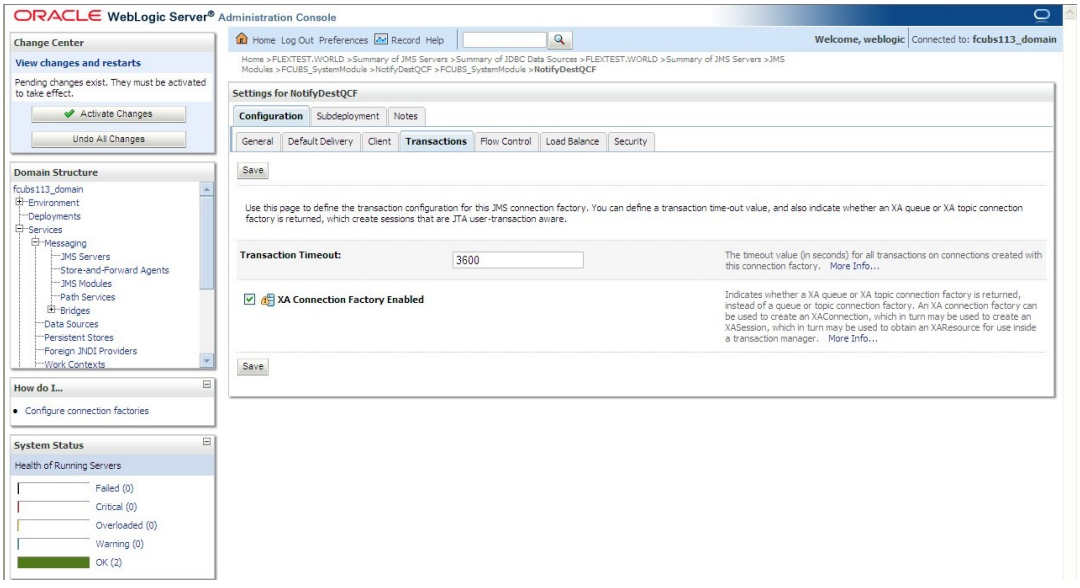
Figure 7-67 Settings for NotifyDestQCF



10. Click the **Transactions** tab.

    The **Settings for NotifyDestQCF - Transactions** tab displays.

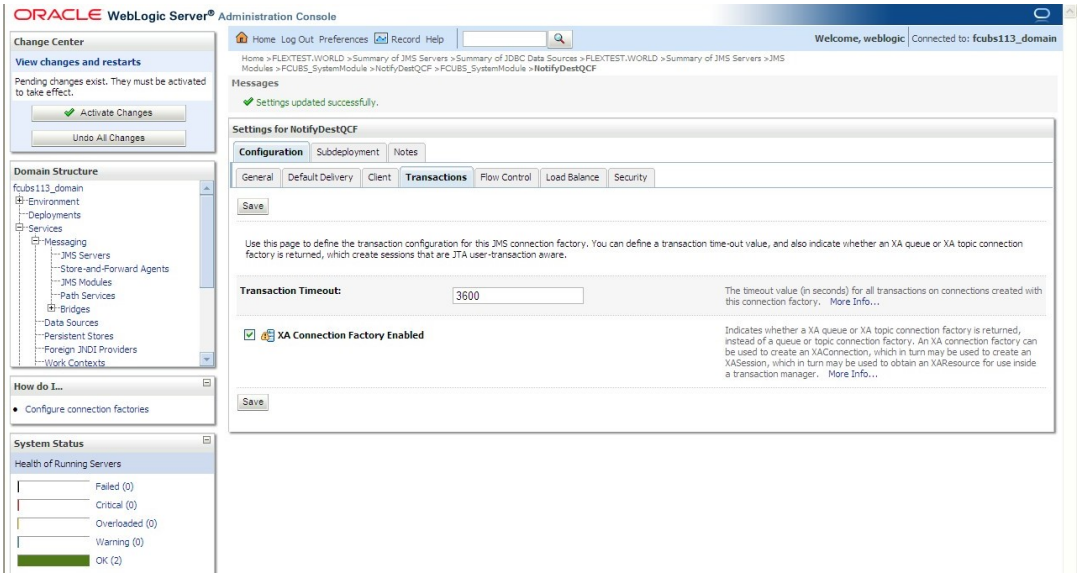
Figure 7-68 Settings for NotifyDestQCF - Transactions



11. Select the **XA Connection Factory Enabled** check box.
12. Click the **Save** button.

    The message displays on the **Settings for NotifyDestQCF - Messages** screen confirming that `Settings updated successfully`.

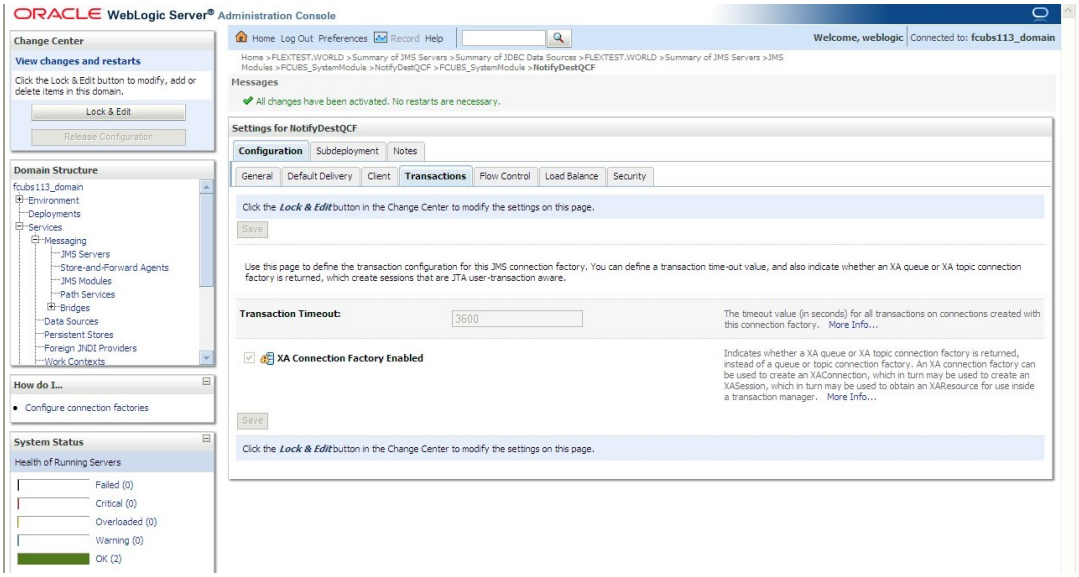
Figure 7-69 Settings for NotifyDestQCF - Messages



13. Click the **Activate Changes** button under **Change Center**.

    The message displays on the **Settings for NotifyDestQCF** screen confirming that `All the changes have been activated. No restarts are necessary.`

Figure 7-70 Settings for NotifyDestQCF - Activate Changes



The **JMS Connection Factory** is created.

7.2 Configure Weblogic for PMGateway

This topic explains to configure Weblogic for PMGateway.

To deploy and run the PMGateway application in the 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`.

7.3 Configure Weblogic for Oracle Banking Corporate Lending

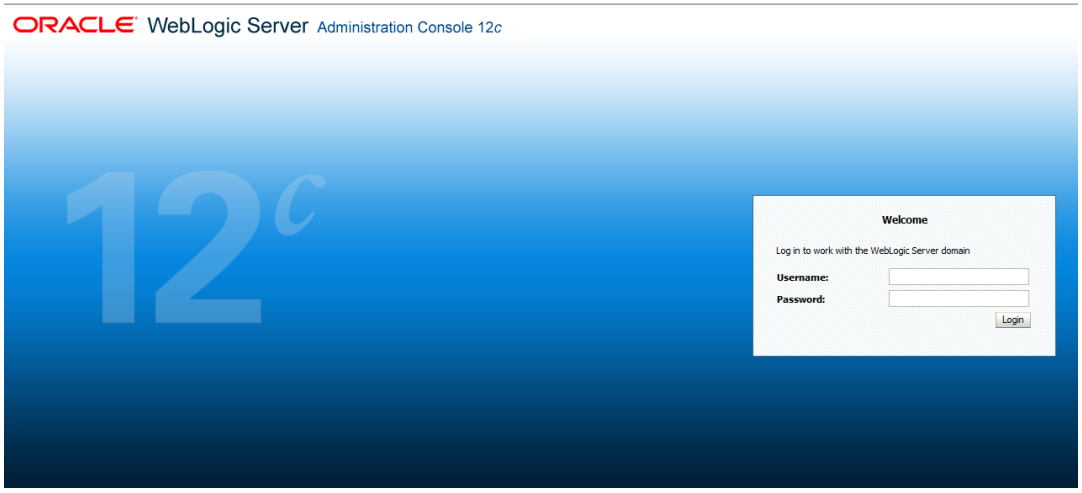
This topic provides the systematic instructions to configure the Oracle WebLogic application server for Oracle Banking Corporate Lending.

To configure the Oracle WebLogic application server, follow the steps below:

1. Start the Administrative Console of the WebLogic application server. Enter the Oracle WebLogic Admin Console URL in the address bar in an internet browser. For example: http://10.10.10.10:1001/console

   The **Oracle Weblogic Server - Welcome** screen displays.

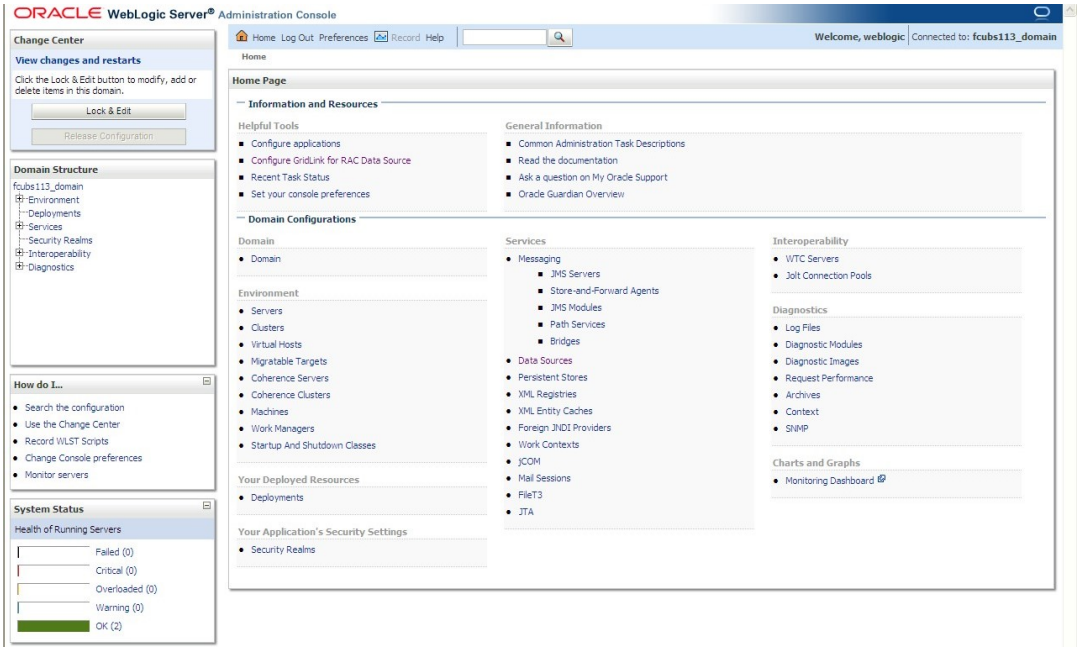
Figure 7-71 Oracle Weblogic Server - Welcome



2. Specify the WebLogic administrator **Username**, **Password** and click **Log In**.

   Oracle Weblogic Server - Home Page screen displays.

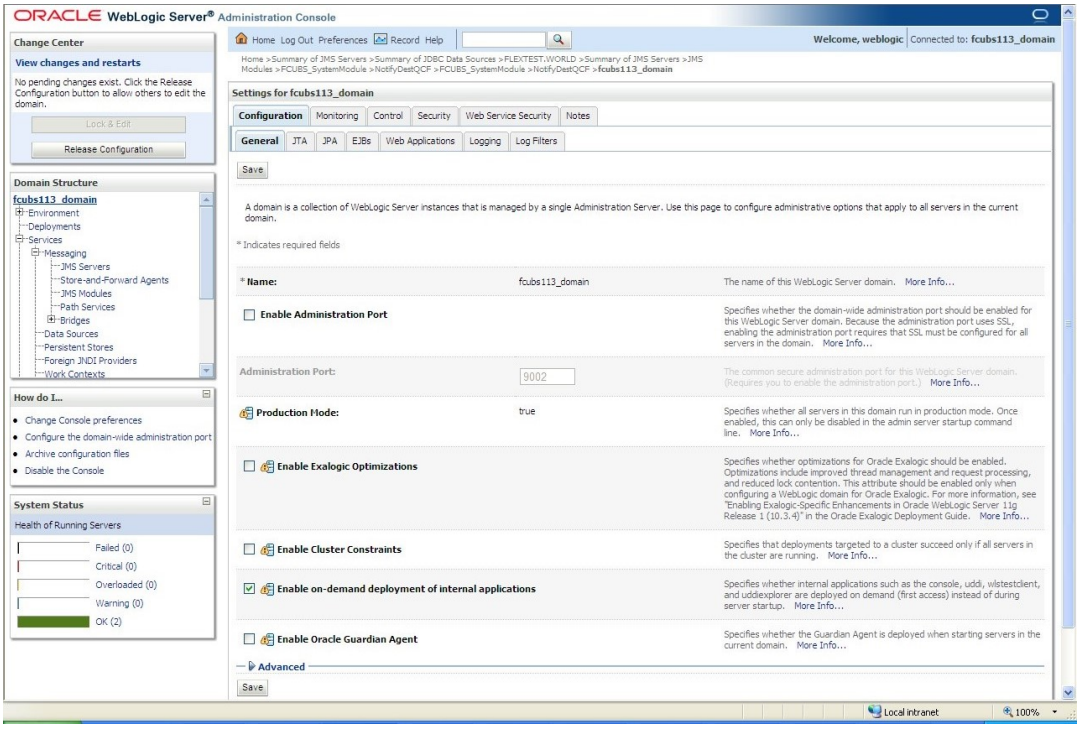
Figure 7-72 Oracle Weblogic Server - Home Page



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

Settings for fcubs113_domain screen displays.

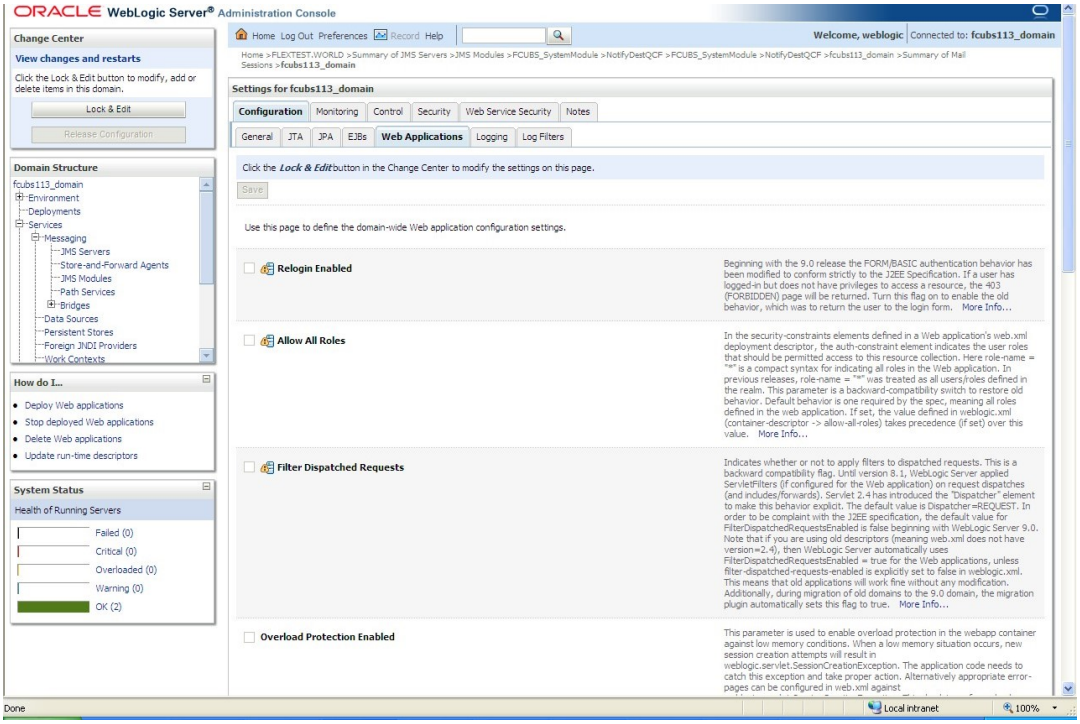
Figure 7-73 Settings for fcubs113_domain



4. Under the **Configuration** tab, select **Web Applications**.

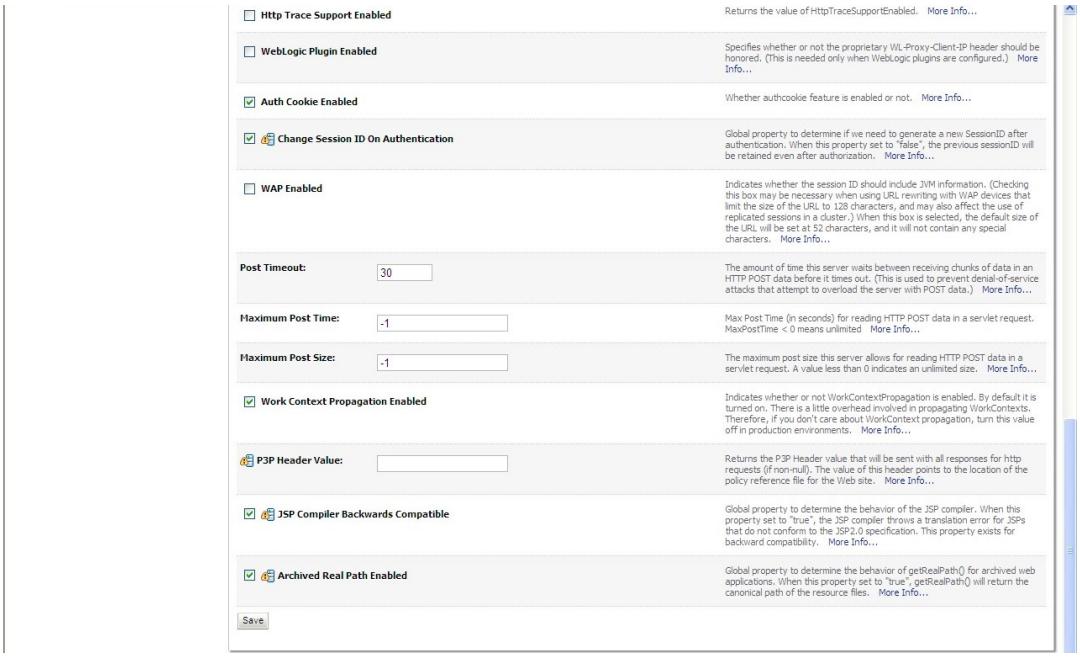
Settings for fcubs113_domain - Web Applications tab displays.

Figure 7-74 Settings for fcubs113_domain - Web Applications



5. Check the options **JSP Compiler Backwards Compatible** and **Archived Real Path Enabled**.

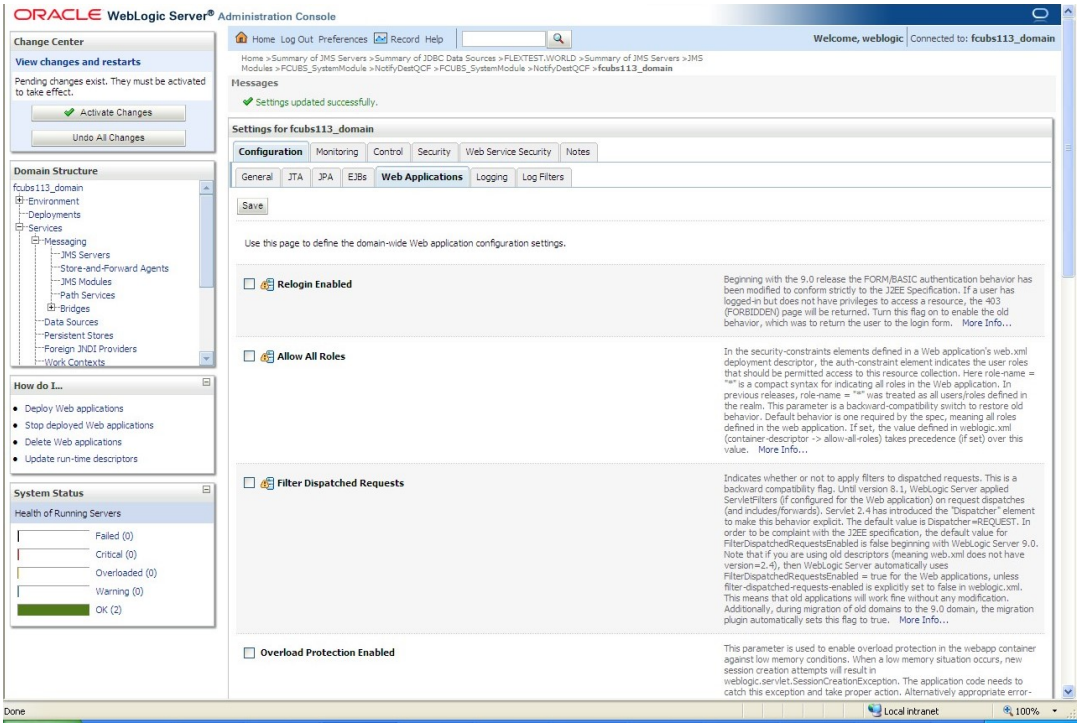
Figure 7-75 Settings for fcubs113_domain - Web Applications 2



6. Click **Save**.

   A message displays on the **Settings for fcubs113_domain** screen confirming that settings are updated successfully.

Figure 7-76 Settings for fcubs113_domain - Messages



7. Click the **Activate Changes** button under the **Change Center**.

   The message displays on the Settings for fcubs113_domain screen confirming that `All the changes have been activated. No restarts are necessary.`

7.4 Configure Mail Session in Weblogic

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

This topic contains the following sub-topics:

- Create JavaMail Session
  This topic explains the systematic instructions to create JavaMail session.
- Configuration of the TLS/SSL Trust Store for Weblogic Server
  This topic explains the configuration of the TLS/SSL Trust Store for Weblogic Server.

7.4.1 Create JavaMail Session

This topic explains the systematic instructions to create JavaMail session.

To configure the JavaMail session, follow the steps below:

1. Start the Administrative Console of the WebLogic application server. Enter the Oracle WebLogic Admin Console URL in the address bar in an internet browser. For example: http://10.10.10.10:1001/console.

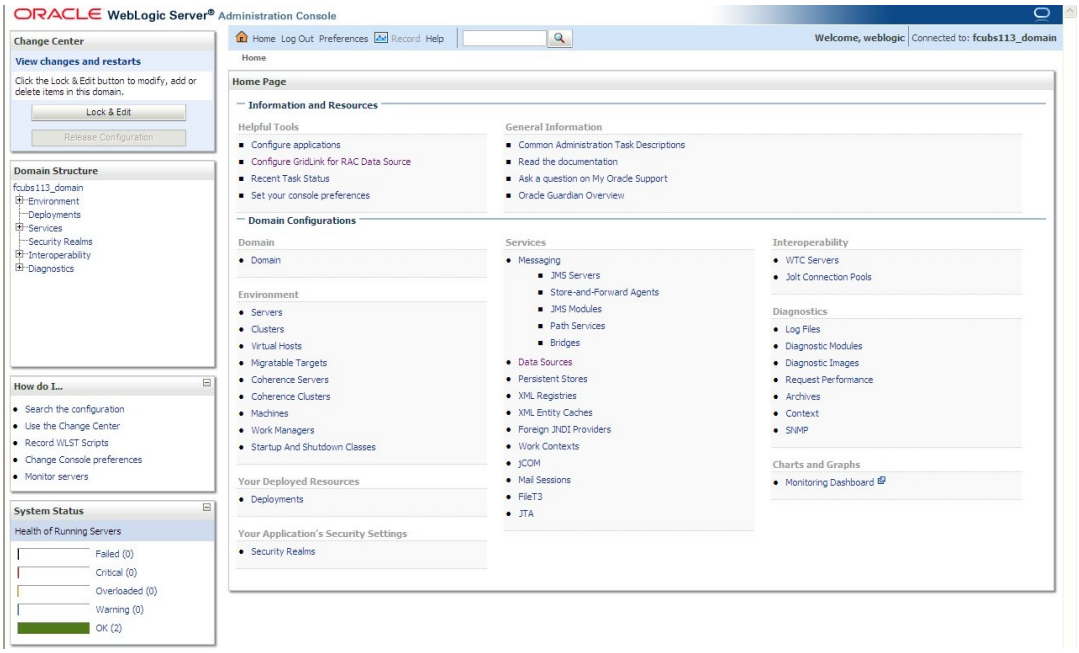
   The **Oracle Weblogic Server - Welcome** screen displays.

Figure 7-77 Oracle Weblogic Server - Welcome

2. Specify the WebLogic administrator **Username**, **Password** and click **Log In**.

   The **Oracle Weblogic Server - Home Page** screen displays.

Figure 7-78 Oracle Weblogic Server - Home page

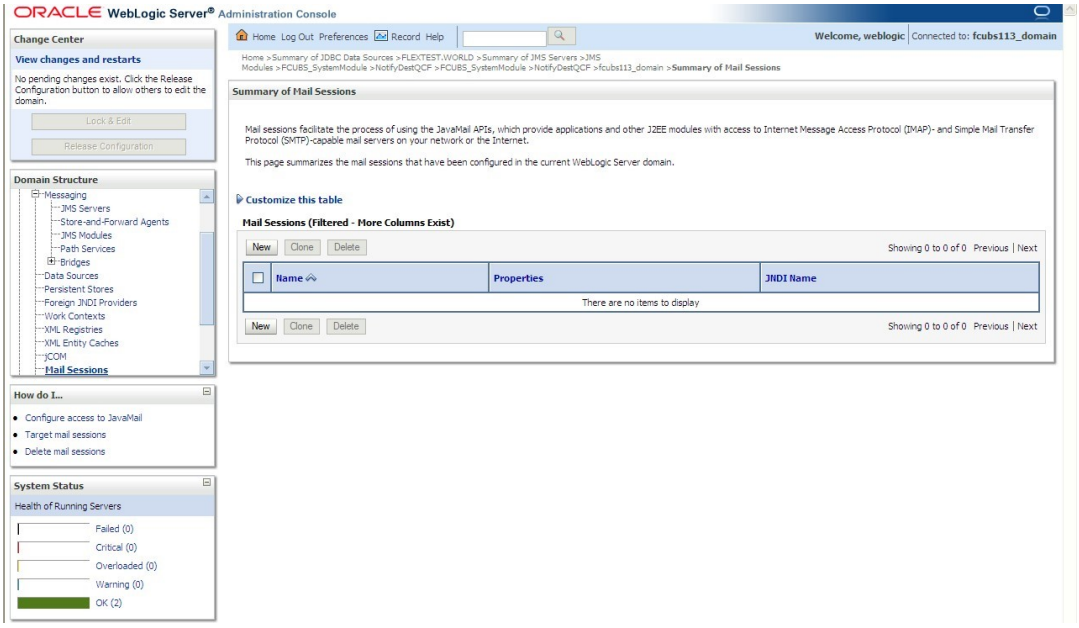


3. On the left pane, under **Domain Structure**, expand **Services** and Click **Mail Sessions** under it.

4. Click the **Lock & Edit** button.

   The **Summary of Mail Sessions** screen displays.

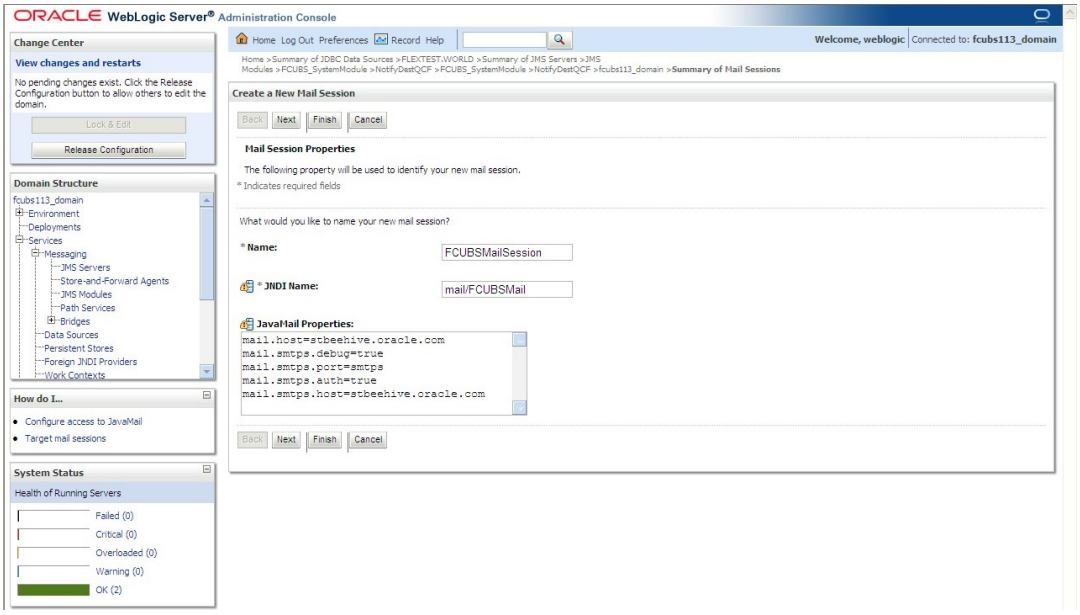
Figure 7-79 Summary of Mail Sessions



5. Click the **New** button.

   The **Create a New Mail Session** screen displays.

Figure 7-80 Create a New Mail Session

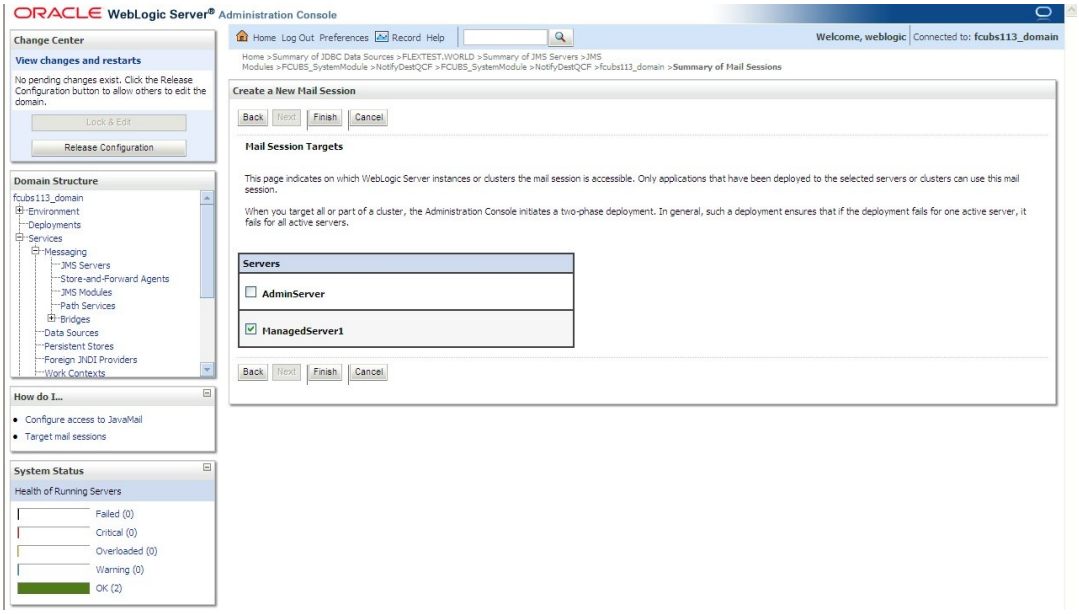


For more information, refer to the fields description table.

6. Click **Next**.

   Create a New Mail Session - Targets screen displays.

Figure 7-81 Create a New Mail Session - Targets



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

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

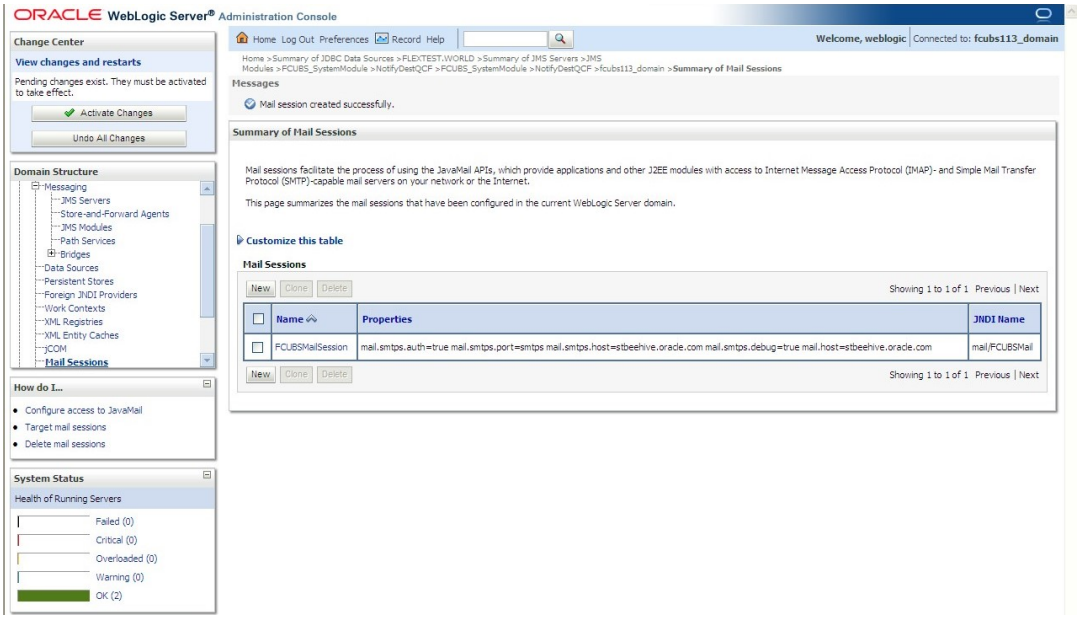
   - SMTP_HOST
   - SMTP_USER
   - SMTP_PASSWORD
   - SMTP_JNDI

   This can be achieved using the Oracle Universal Banking Installer.

8. Click the **Activate Changes** button under the **Change Center** to activate the current mail session settings.

   The message displays on the **Summary of JDBC Data Sources - Activate Changes Message** confirming that `All the changes have been activated. No restarts are necessary.`

Figure 7-82 Summary of Mail Sessions - Activate Changes Message



The **JavaMail Session** is created.

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

This topic explains the configuration of the TLS/SSL Trust Store for Weblogic Server.

As described in the previous topic, Oracle Banking Corporate Lending 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 Corporate Lending 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 Corporate Lending 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).