

Websphere Configuration

Oracle Banking Treasury Management

Release 14.5.4.0.0

Part No. F53253-01

[February] [2022]



Table of Contents

1.	CONFIGURING SSL ON WEBSPHERE.....	1-3
1.1	INTRODUCTION	1-3
1.2	CERTIFICATES.....	1-3
1.2.1	Creating SSL Connection between Application Server and Client	1-3
1.2.2	Creating Self Signed Certificate	1-3
1.2.3	Path Details	1-5
1.3	ADDING KEY STORE TO APPLICATION SERVER	1-5
1.4	CREATING SSL CONFIGURATION	1-8
1.5	MANAGING ENDPOINT SECURITY CONFIGURATIONS.....	1-10
1.6	SSL SETTINGS AT APPLICATION SERVER LEVEL	1-11
1.7	RUNNING APPLICATION WITH SSL	1-14
1.8	CERTIFICATE EXCHANGE FOR TWO WAYS SSL.....	1-14
1.8.1	Extracting Certificate for Server1	1-14
1.8.2	Extracting Certificate for Server2	1-15
1.8.3	Importing Certificate into Keystore for Server1	1-15
1.8.4	Importing Certificate into Keystore for Server2	1-17
1.8.5	Importing Certificate into Truststore for Server1	1-18
1.8.6	Importing Certificate into Truststore for Server2.....	1-20
1.9	MANAGING ENDPOINT SECURITY CONFIGURATIONS.....	1-21
1.10	PROTECTION QUALITY	1-23
1.11	IMPORTING OR ADDING SERVER CERTIFICATES USING BATCH.....	1-25
1.11.1	Default JAXRS provider settings	1-26
2.	CREATING RESOURCES ON WEBSPHERE	2-1
2.1	INTRODUCTION	2-1
2.2	CREATING QUEUES ON WEBSPHERE MQ SERVER	2-1
2.2.1	Creating Queue Manager through Console.....	2-1
2.2.2	Creating Queues	2-10
2.3	CREATING QUEUE MANAGER AND QUEUE USING UNIX COMMANDS.....	2-13
2.3.1	Creating Queue Manager	2-13
2.3.2	Starting Queue Manager	2-14
2.3.3	Starting MQ Service to Create Queues under FC_QMGR.....	2-14
2.3.4	Creating Queues	2-14
2.3.5	Creating Channel.....	2-14
2.3.6	Ending MQSC.....	2-14
2.3.7	Creating Bindings.....	2-15
2.3.8	Creating QCF	2-15
2.3.9	MQ Channel Authentication	2-18
2.4	VIEWING IBM MQ QUEUES	2-18
3.	CREATING JDBC RESOURCES ON WEB SPHERE	3-1
3.1	INTRODUCTION	3-1
3.2	PREREQUISITE:	3-1
3.3	CREATING JDBC SOURCES	3-1
3.3.1	Creating Global Security	3-1
3.3.2	JDBC Provider for Non XA Data Source	3-4
3.3.3	Creating Non XA Data Source.....	3-8
3.3.4	Testing Data Source.....	3-16
3.3.5	JDBC Provider for XA Data Source	3-19
3.3.6	Creating XA Data Source	3-23
3.3.7	Testing Data Source.....	3-30

3.4	CREATING JMS RESOURCES.....	3-31
3.4.1	<i>Creating Queue Connection Factory</i>	3-31
3.4.2	<i>Creating Queues</i>	3-40
3.5	CREATING MESSAGE LISTENER.....	3-44
4.	DEFAULT SETTINGS FOR WEB SPHERE.....	4-1
4.1	LIBRARIES FOR PMGATEWAY APPLICATION.....	4-1
5.	CONFIGURING MAIL SESSION ON WEBSPHERE	5-1
5.1	INTRODUCTION.....	5-1
5.2	CREATING JAVA MAIL SESSION.....	5-1
6.	ANNEXURE.....	6-1
6.1	IBM WEBSPHERE SERVER - INCREASING HEAP SIZE.....	6-1
6.2	IBM WEBSPHERE SERVER - TRANSACTION SERVICE PROPERTIES.....	6-1
6.3	IBM WEBSPHERE SERVER – ORB SERVICE CONFIGURATION	6-1

1. Configuring SSL on Websphere

1.1 Introduction

This chapter guides you through the process of configuring SSL on IBM Websphere application server.

1.2 Certificates

1.2.1 Creating SSL Connection between Application Server and Client

To establish SSL connection between Websphere and client work stations, follow the steps given below:

- Create SSL certificate (this certificate is required during real time production)
- Self signed certificate (SSL) will be used for testing purpose

1.2.2 Creating Self Signed Certificate

To create a self signed certificate, you may use various tools including IBM (Keyman). For illustration purpose, this guide explains the method of generating SSL using a tool available in JAVA. The keytool is available in the folder 'JAVA_HOME\jdk\bin'.

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

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



The texts highlighted in blue are placeholders. You need to replace them with the suitable values while running the command.

In the above command,

- ***alias*** is used to identify the public and private key pair created. This *alias* is required for configuring the SSL attributes for the managed servers in Oracle WebLogic application server.
- ***keyalg*** is the key algorithm to generate the public and private key pair. The RSA key algorithm is recommended.
- ***keysize*** is the size of the public and private key pair generated. A key size of 1024 or more is recommended. Consult your CA on the key size support for different types of certificates.
- ***sigalg*** is the algorithm used to generate the signature. This algorithm must be compatible with the key algorithm. This has to be one of the values specified in the Java Cryptography API Specification and Reference.
- ***valdays*** is the number of days for which the certificate is considered to be valid. Consult your CA on this period.

- **keystore** is to specify the location of the JKS file. If JKS file is not present in the path provided, this will create it.

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

- **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 Oracle WebLogic Server.
- **First and last name (CN):** Specify the domain name of the machine used to access Oracle Banking Treasury Management. For instance, www.example.com.
- **Name of your organizational unit:** Specify 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 physical server.
- **Name of your organization:** Specify the name of the organization making the certificate request. For example, Oracle Financial Services Software. It is recommended to use the formal name of the company or organization. This name must match the name in the official records.
- **Name of your City or Locality:** Specify the name of the city in which your organization is physically located. For example Mumbai.
- **Name of your State or Province:** Specify the state/province in which your organization is physically located. For example Maharashtra.
- **Two-letter country code for this unit:** Specify 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:

```
C:\Program Files\IBM\WebSphere\AppServer\bin>keytool -
genkeypair -alias cvrhp0729 -keyalg RSA -keysize 1024 -sigalg
SHA1withRSA -validity 365 -keystore
D:\keystores\OBTRMKeyStore.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>

The self signed certificate needs to be added to the web server.

1.2.3 **Path Details**

You need to copy or move the keystore file *<name of the file>.jks* to the application server location given below:

/oracle1/WAS61/Appserver_ND/profiles/AppSrv01/config/cells/ips014dorCell01/nodes/ips014dorNode02

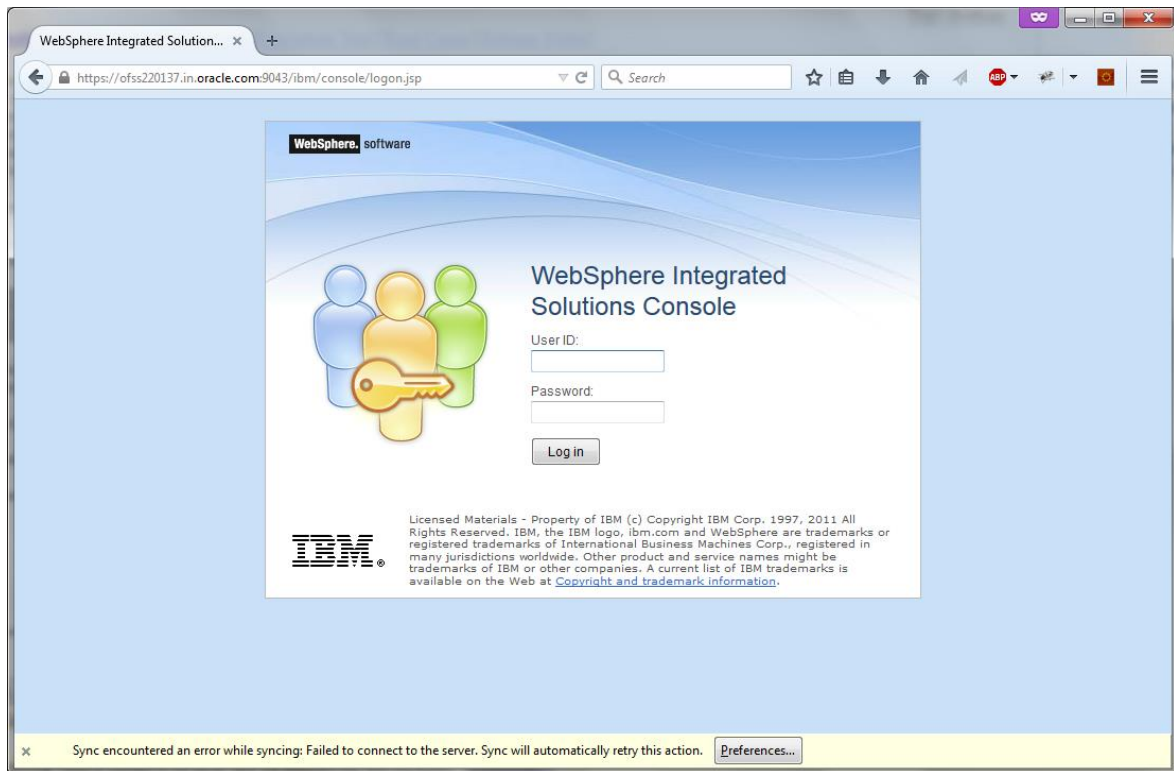
ips014dorCell01 --> <ips014dor> name of the machine and < Cell01>

ips014dorNode02 --> < ips014dorNode > name of the machine and <Node02>

1.3 **Adding Key Store to Application Server**

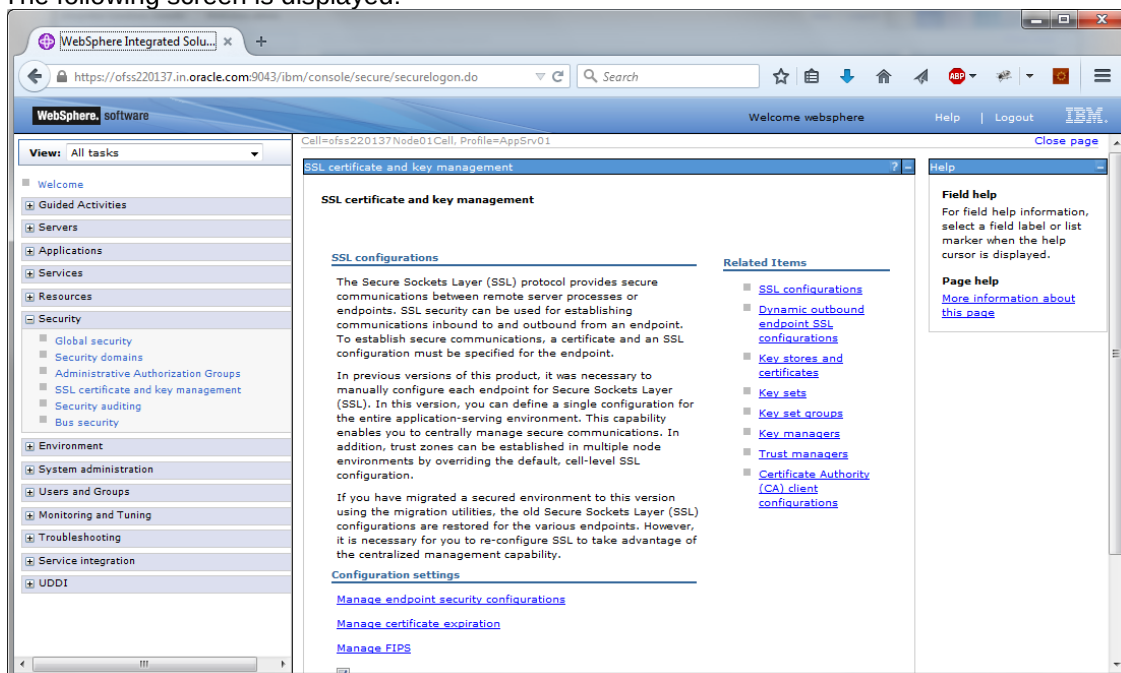
To add keystore to the Websphere application server, follow the instructions given below.

1. Log in to the WAP console as the user 'admin'.



2. Specify the user ID of the administrator and the password set while installing the software. Click 'Log In'.

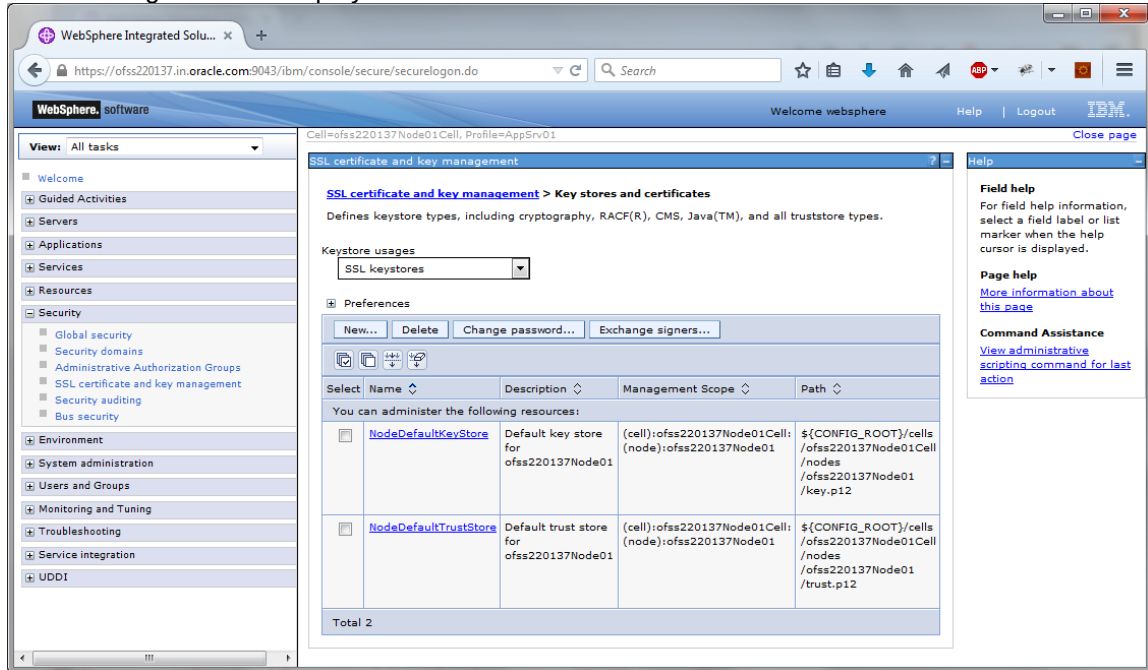
The following screen is displayed:



On the left pane, expand 'Security' and click 'SSL certificate and key management'. The screen displays the details of SSL.

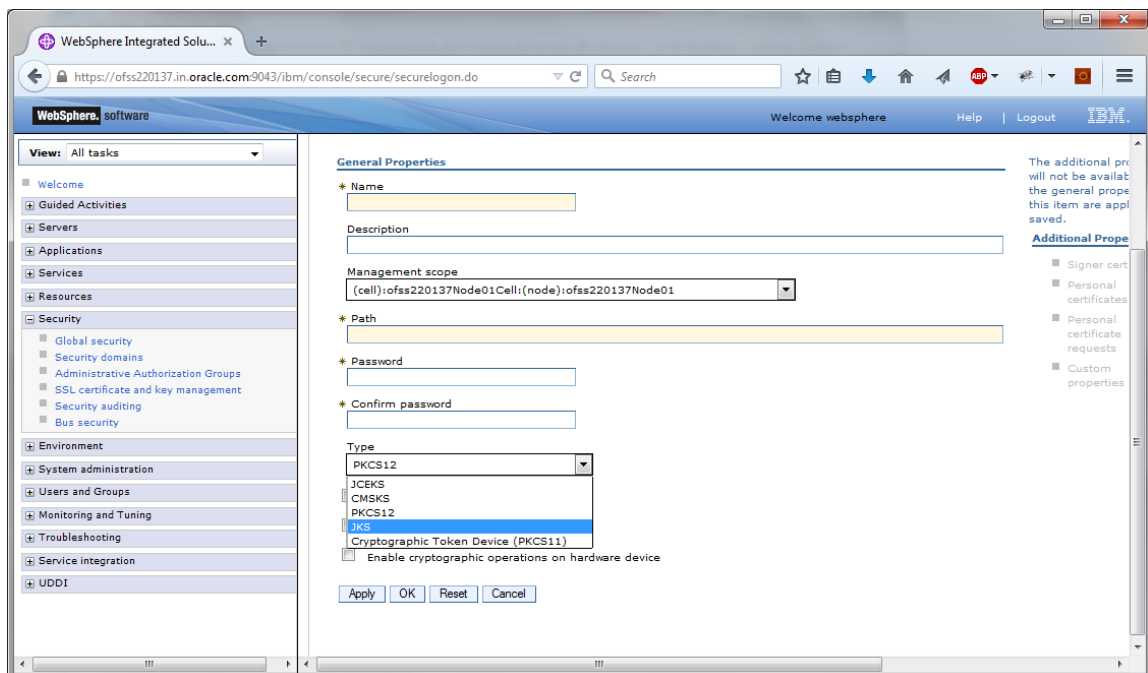
3. Under 'Related items' on the right side, click 'Key stores and certificates'.

The following screen is displayed:



This screen is used for attaching the key store to the application server.

4. Click 'New' button to add a new key to store.



5. Specify the following details:

Name

Specify the key store name.

Path

Specify the location of the key store generated.

This has to be a relative path.

Example

`${CONFIG_ROOT}/cells/ips014dorCell01/nodes/ips014dorNode02/jf3sslstore.jks`

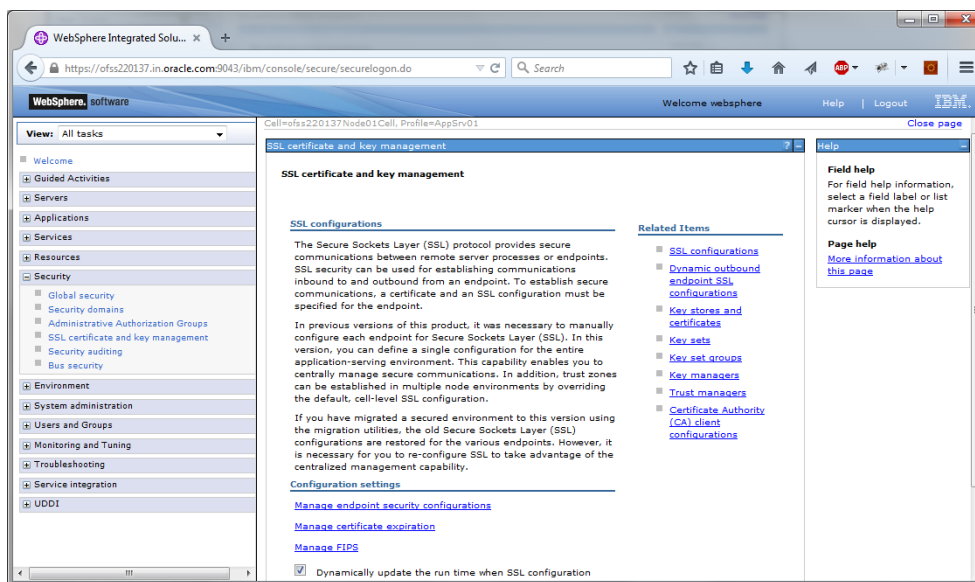
Password

Specify the password given in the 'store pass' parameter during key store generation.

6. Click 'Apply' and save the changes.

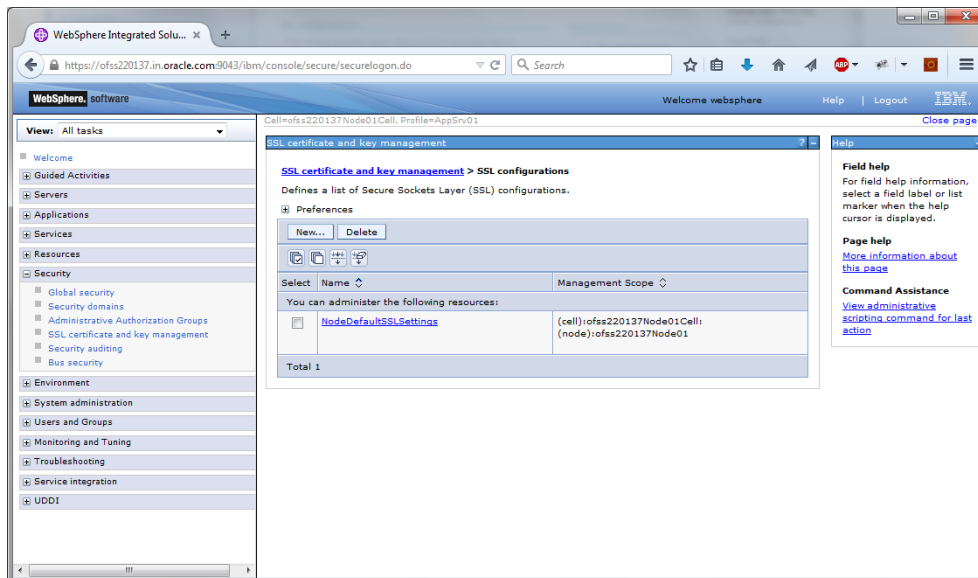
1.4 Creating SSL Configuration

To create SSL configuration, on the left pane, click 'SSL certificate and key management'.

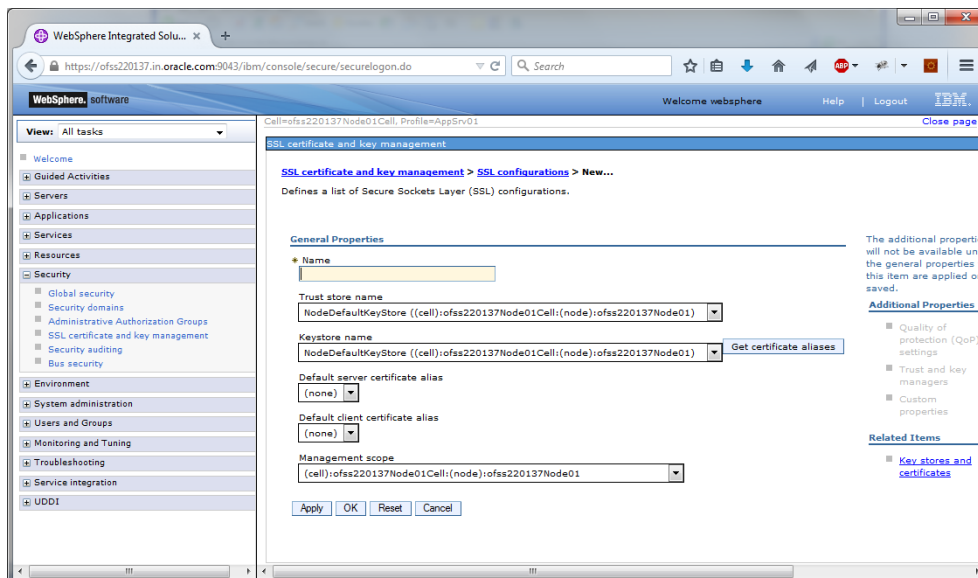


1. Under the section 'Related items', click 'SSL configurations'.

The following screen is displayed:



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



3. Specify the following details:

Name

Specify the name of the SSL configuration.

Trusted Store Name

Select the added key store.

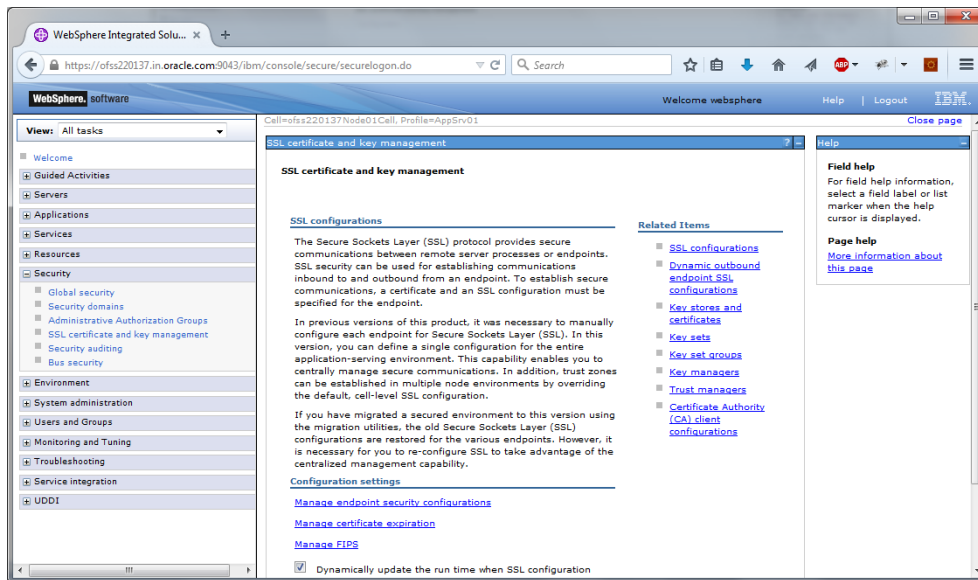
Key Store Name

Select the added key store.

4. Click the button 'Get Certificate aliases'. Further, click 'Apply' and save the changes.

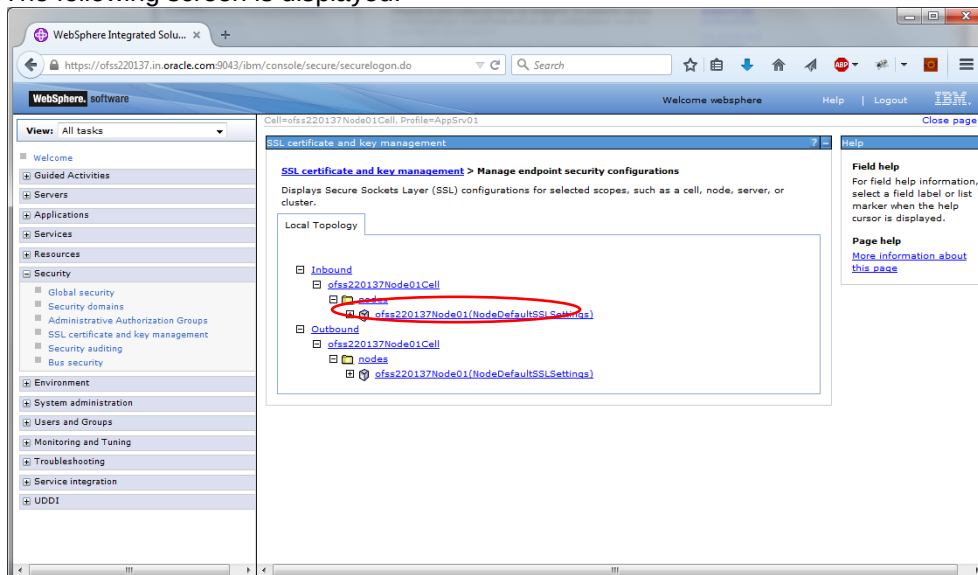
1.5 Managing Endpoint Security Configurations

This section explains the process of managing endpoint security configurations.

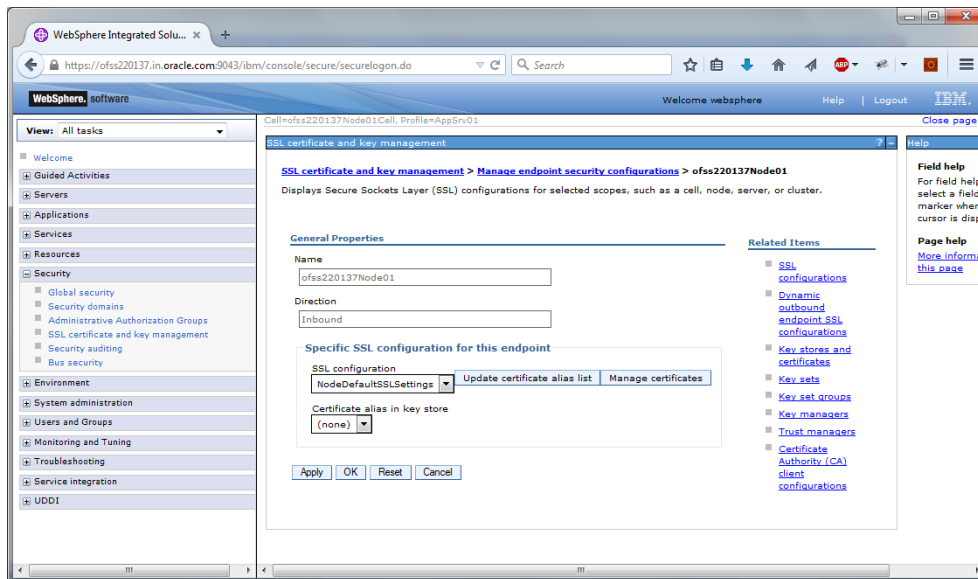


1. On the left pane, expand 'Security' and click 'SSL certificate and key management'. Under 'Configuration settings', click 'Manage endpoint security configurations'.

The following screen is displayed:



2. Click the first link under 'Inbound tree'. The following screen is displayed:

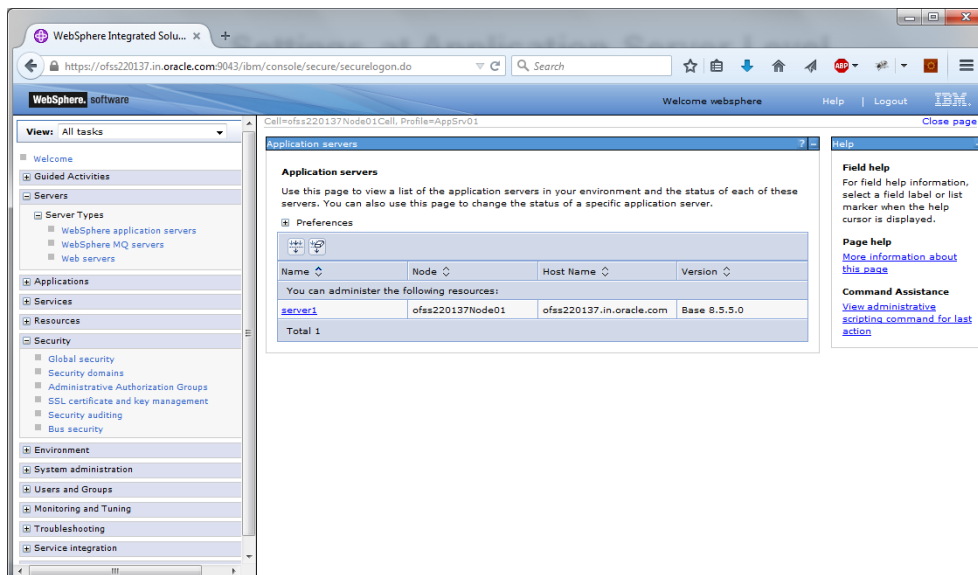


Under SSL configurations, select the configured SSL from the drop-down list.

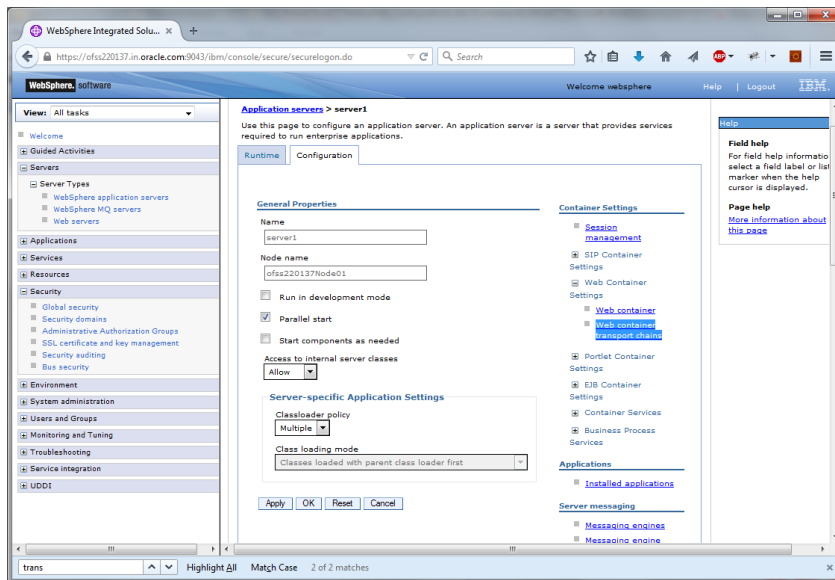
3. Click the button 'Update certificate alias list'. Click 'Apply' and save the changes.

1.6 SSL Settings at Application Server Level

Go to the servers available on the left and click the application servers link which will refresh the window on the right side to display the details pertaining to application servers

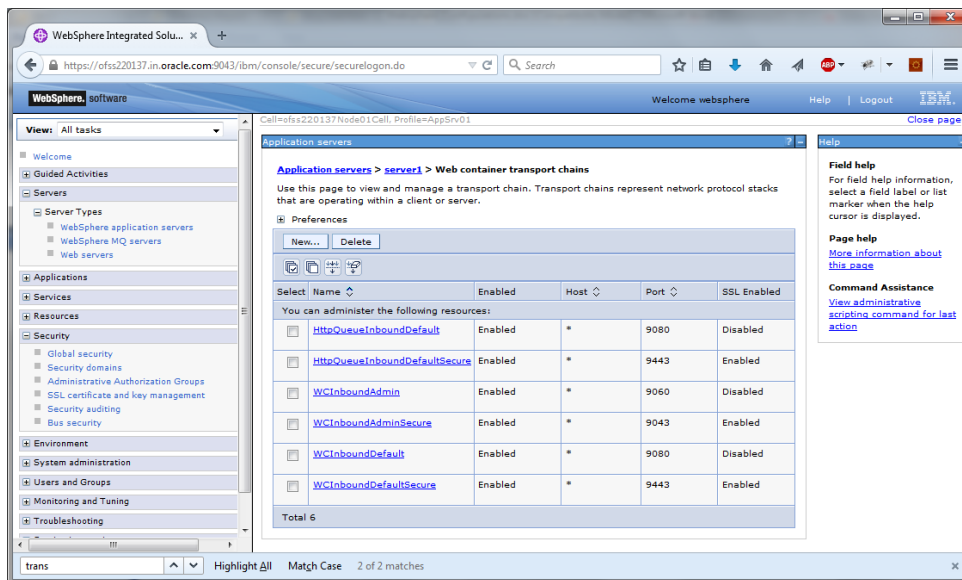


1. Click the server to which SSL configuration has to be applied. The following screen is displayed.



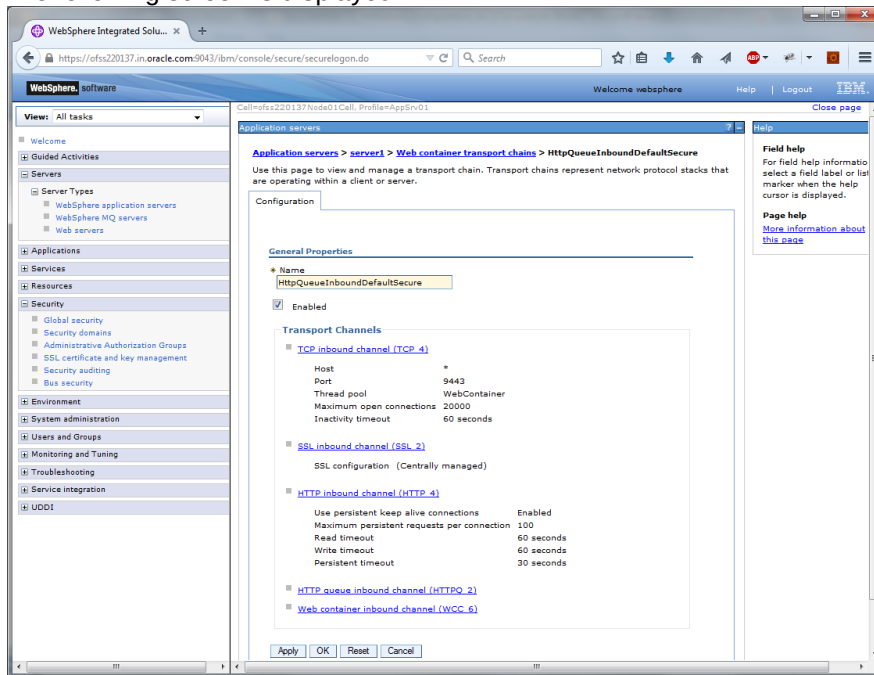
2. Go to Configuration tab and click 'Web container transport chains' under 'Container settings'.

The following screen is displayed.

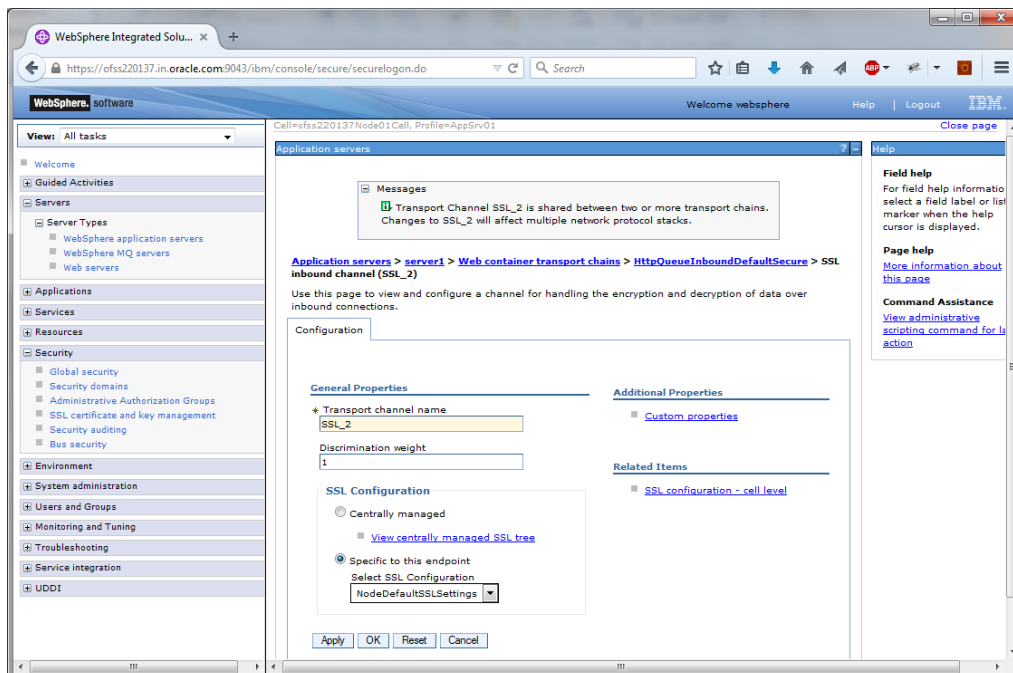


3. Against their respective names, the secured connection is available under the column 'SSL Enabled'. Click 'WCInboundDefaultSecure'.

The following screen is displayed:



4. Click 'SSL Inbound channel (SSL 2)'.



5. Select the configured SSL from the list of SSL configurations. Click 'Apply' and save the changes.

1.7 Running Application with SSL

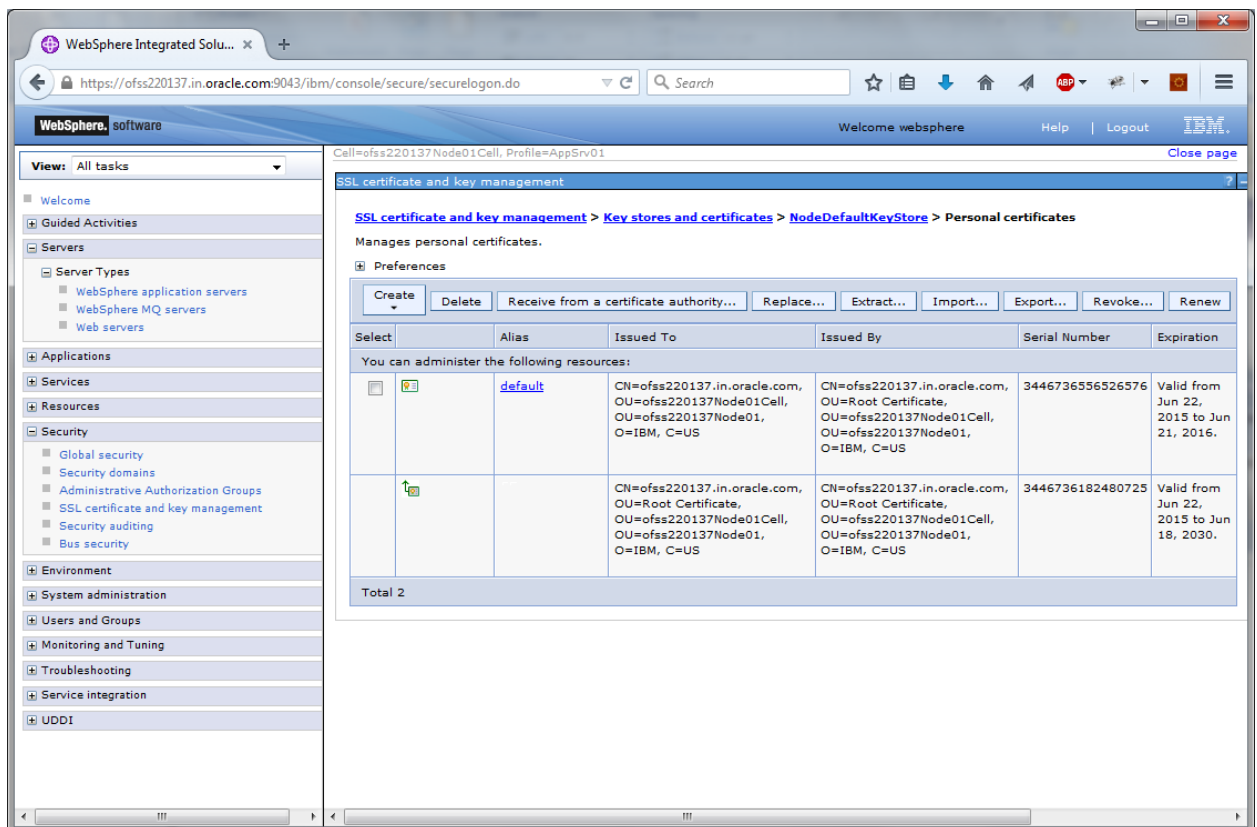
To run the application with SSL, use the following syntax:

https://<<ip address or host name>>:<<port number>>/<<context>>>

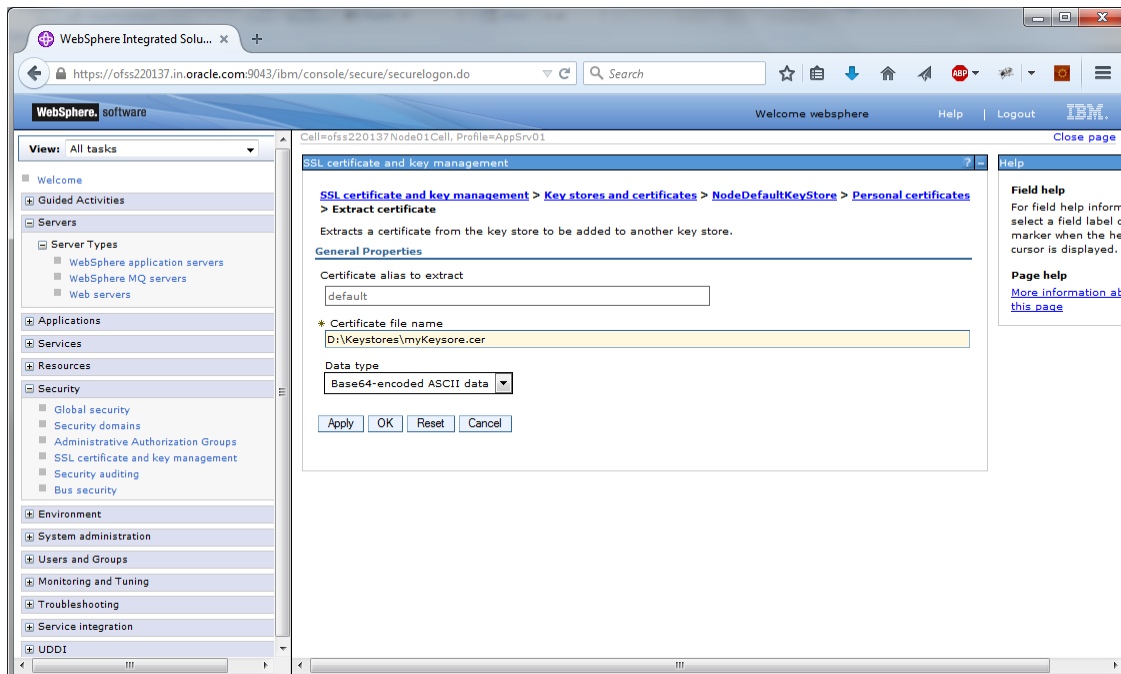
1.8 Certificate Exchange for Two Ways SSL

1.8.1 Extracting Certificate for Server1

The process of extracting certificate for Server 1 is described below.



1. On the left pane of the screen, expand 'Security'. Go to 'SSL certificate and key management > Key stores and certificates > {YOUR KEYSTORE NAME} > Personal certificates.
2. Select the installed certificate and click 'Extract' button.



3. Specify the location to save the certificate. This will be used to add in the other server.
Ensure that the file has been created in the location.

Eg: \<localfolder>\<server1.cer>

4. Similarly extract the certificate for the second server.

Eg: \<localfolder>\<server2.cer>

1.8.2 Extracting Certificate for Server2

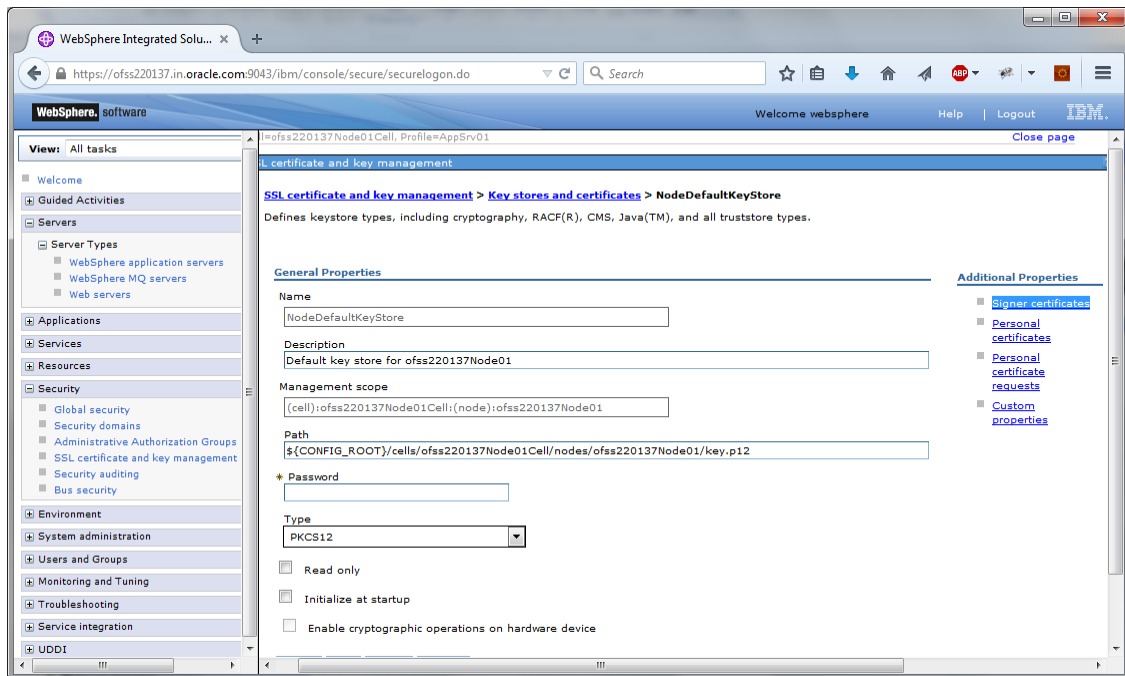
You can follow the steps for server 1 described under 'Extracting Certificate for Server1' to extract the certificate for Server2.

1.8.3 Importing Certificate into Keystore for Server1



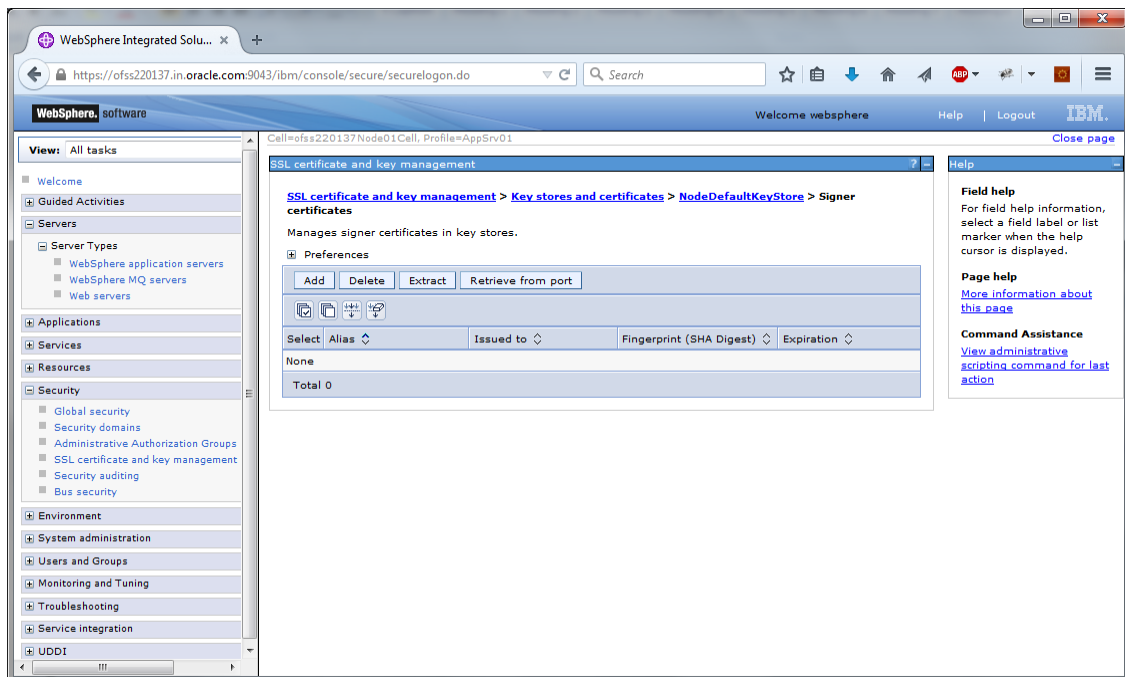
Note: The trust certificates also needs to be added in the **cacerts** of the Java Runtime Environment

Go to the other server. Expand 'Security > SSL certificate and key management > Key stores and certificates > Server7Keystore (which is created now).

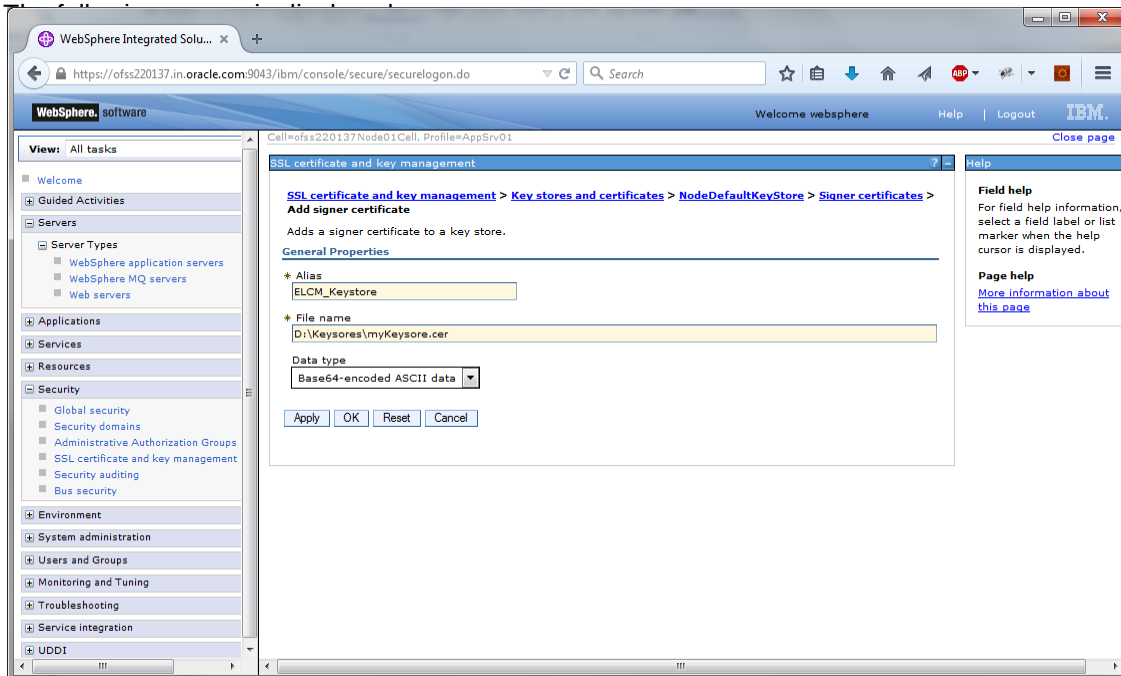


1. Click 'Signer Certificates'.

The following screen is displayed:



2. Click 'Add' button to add the certificate of the other server.



3. The extracted certificate of the second server has to be imported to the key-store and trust-store of first server. This has to be done using the same local path where the extract certificate was generated for the first server.

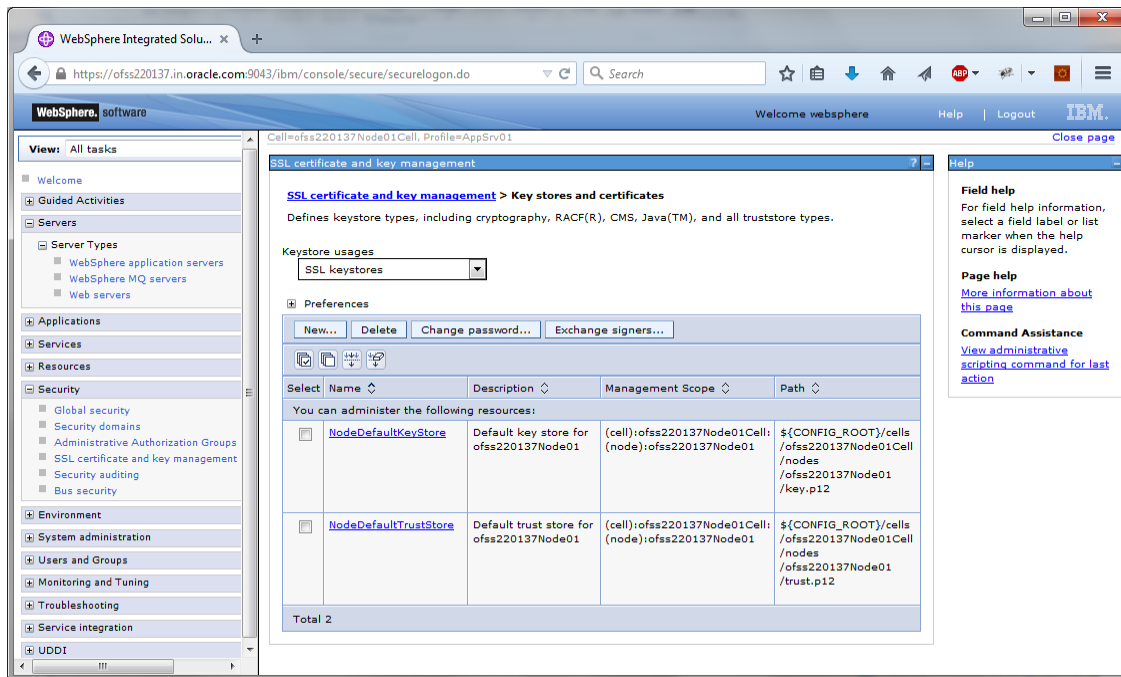
Eg: \<localfolder>\<server1.cer>

1.8.4 **Importing Certificate into Keystore for Server2**

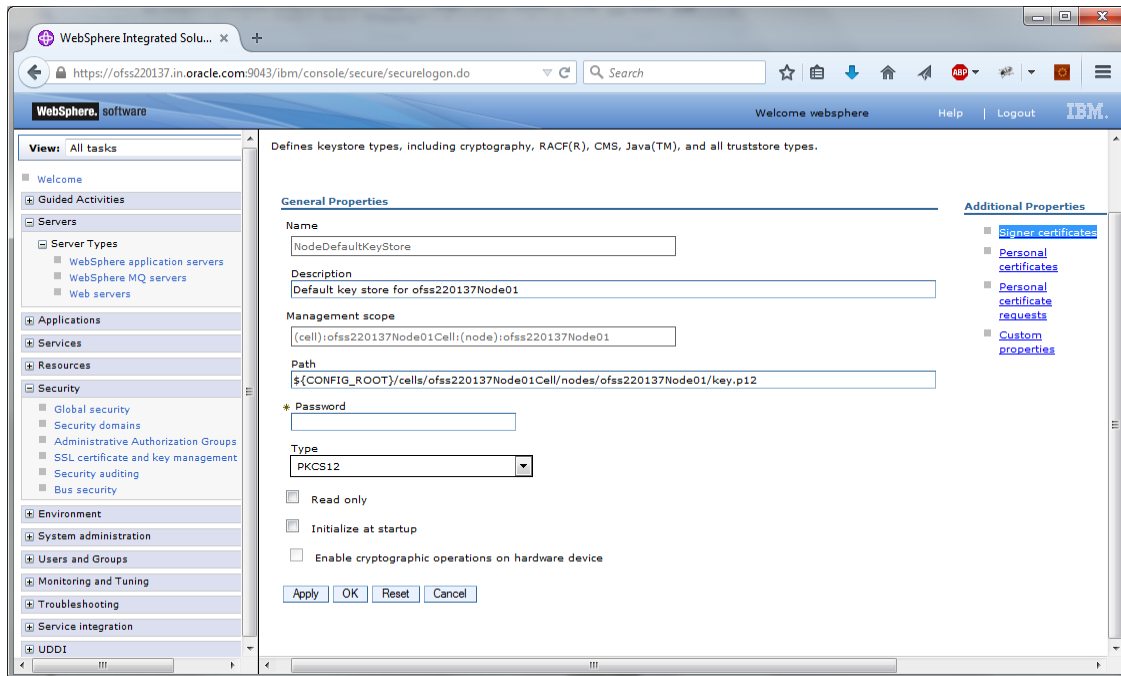
You can follow the steps for server 1 described under 'Importing Certificate into Keystore for Server1' to import the certificate into keystore for Server2.

1.8.5 Importing Certificate into Truststore for Server1

Expand 'SSL certificate and key management > Key stores and certificates and click 'NodeDefaultTrustStore'.

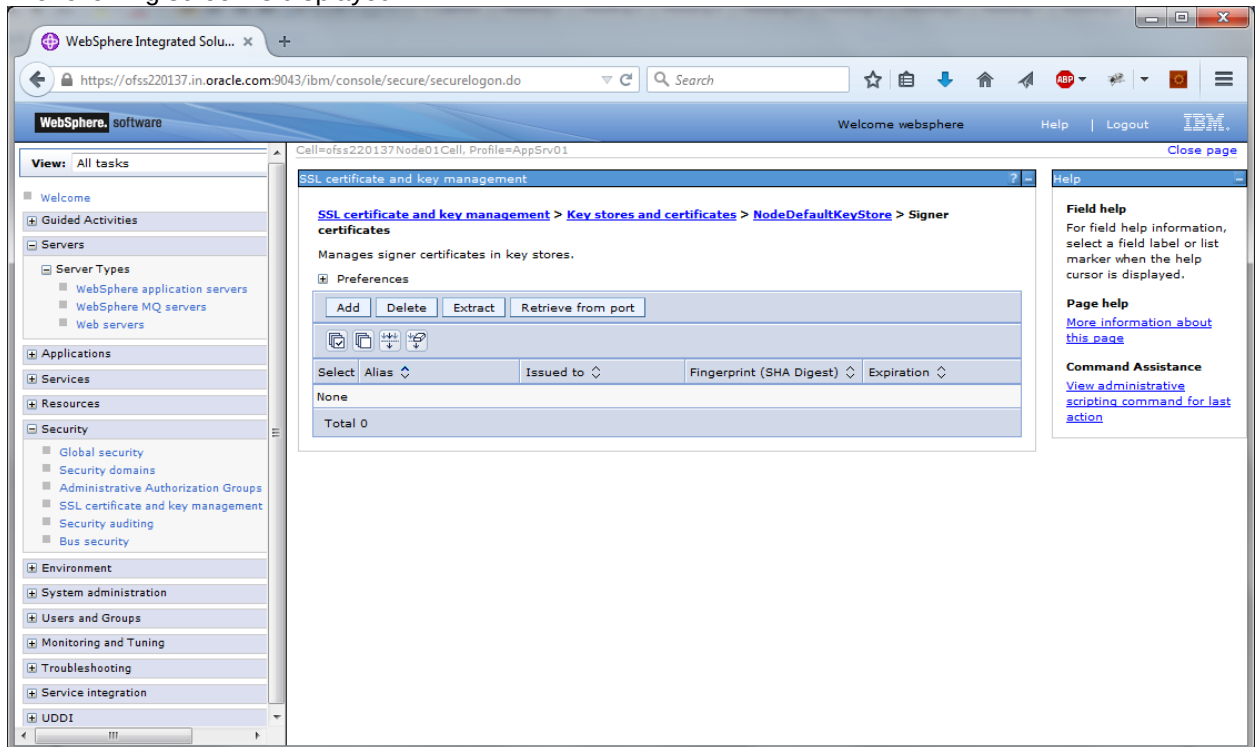


The following screen is displayed.



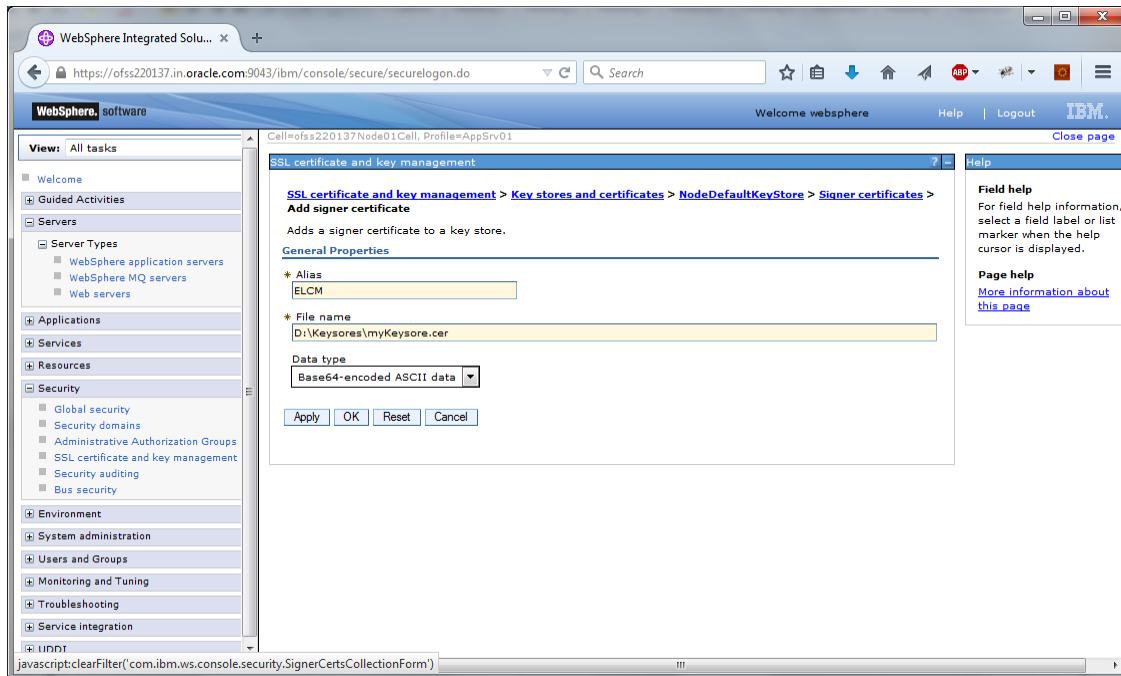
1. Click 'Signer Certificates'.

The following screen is displayed.



2. Click 'Add' button to add the extracted certificate of the second server.

The following screen is displayed.



3. Specify the 'alias' name to identify the other server.

Eg: For server1, you can give the alias name 'server2Alias'.

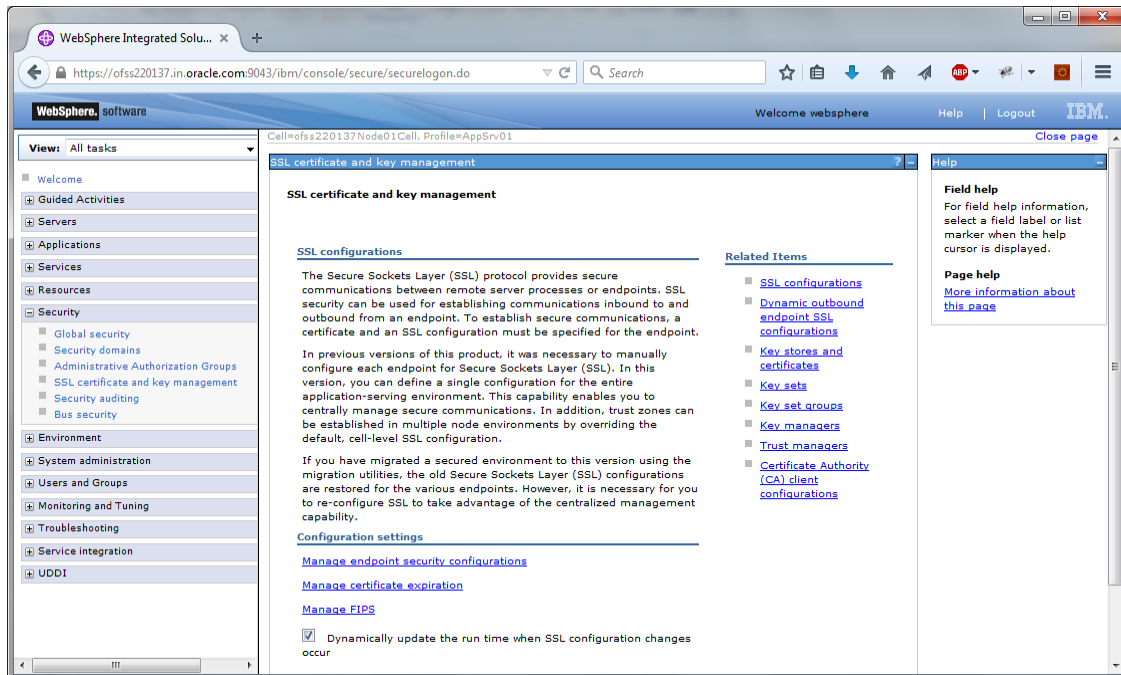
4. Further, specify the location of the extracted certificate.

1.8.6 Importing Certificate into Truststore for Server2

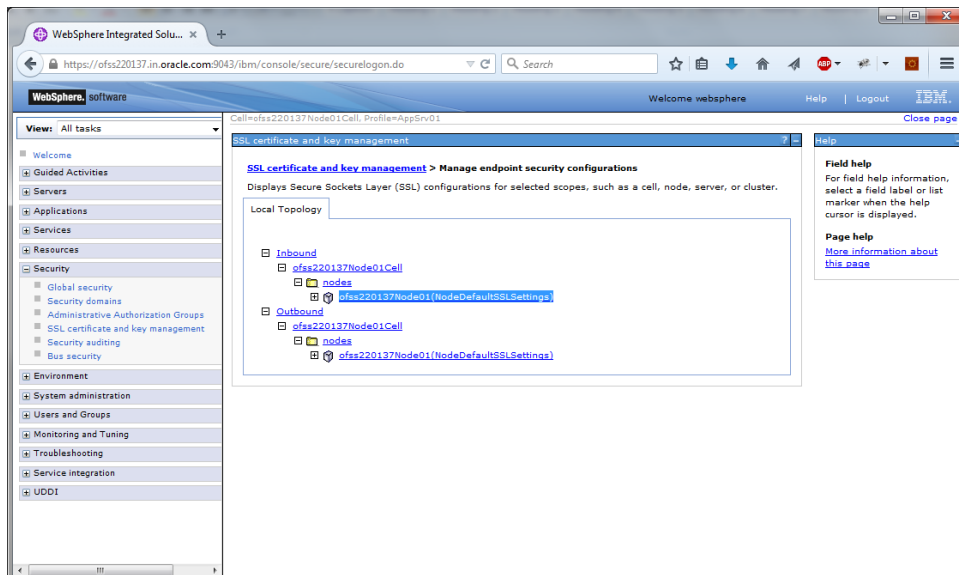
You can follow the steps for server 1 described under 'Importing Certificate into Truststore for Server2' to import the certificate into Truststore for Server2.

1.9 Managing Endpoint Security Configurations

To manage the endpoint security configurations, follow the instructions given below.

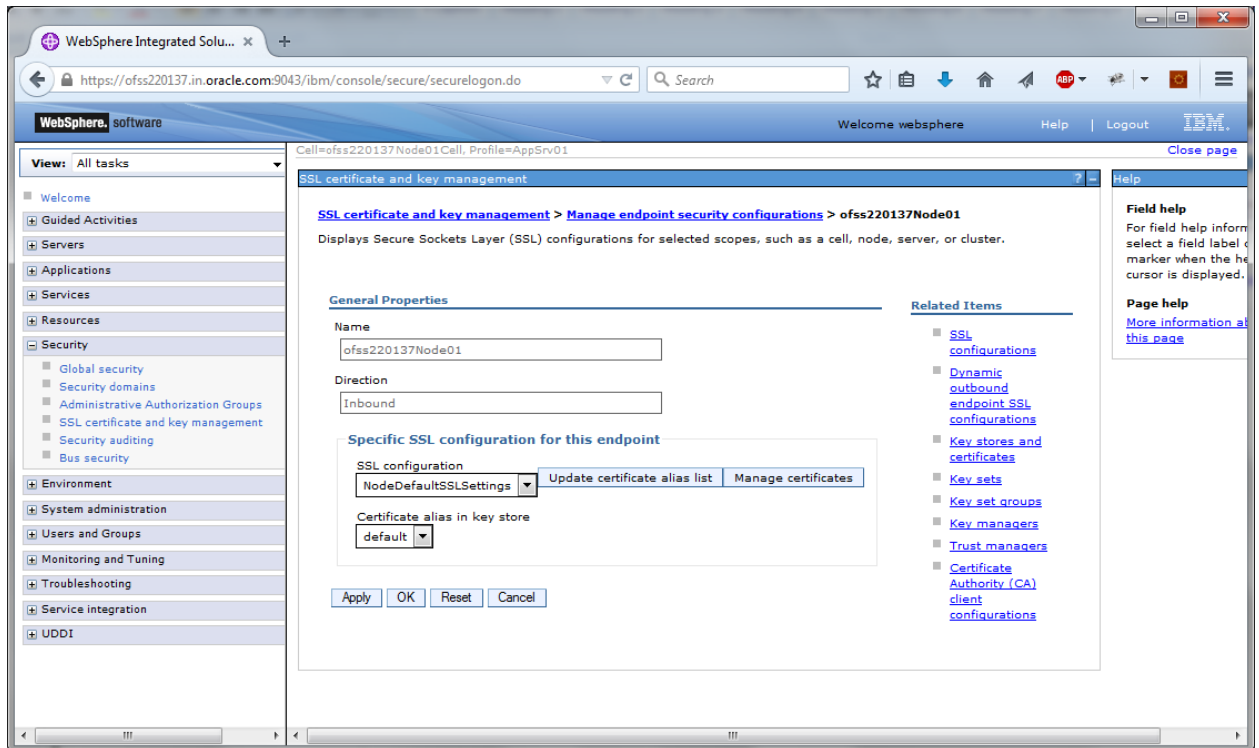


1. Expand 'Security > SSL certificate and key management' and click 'Manage endpoint security configurations'.



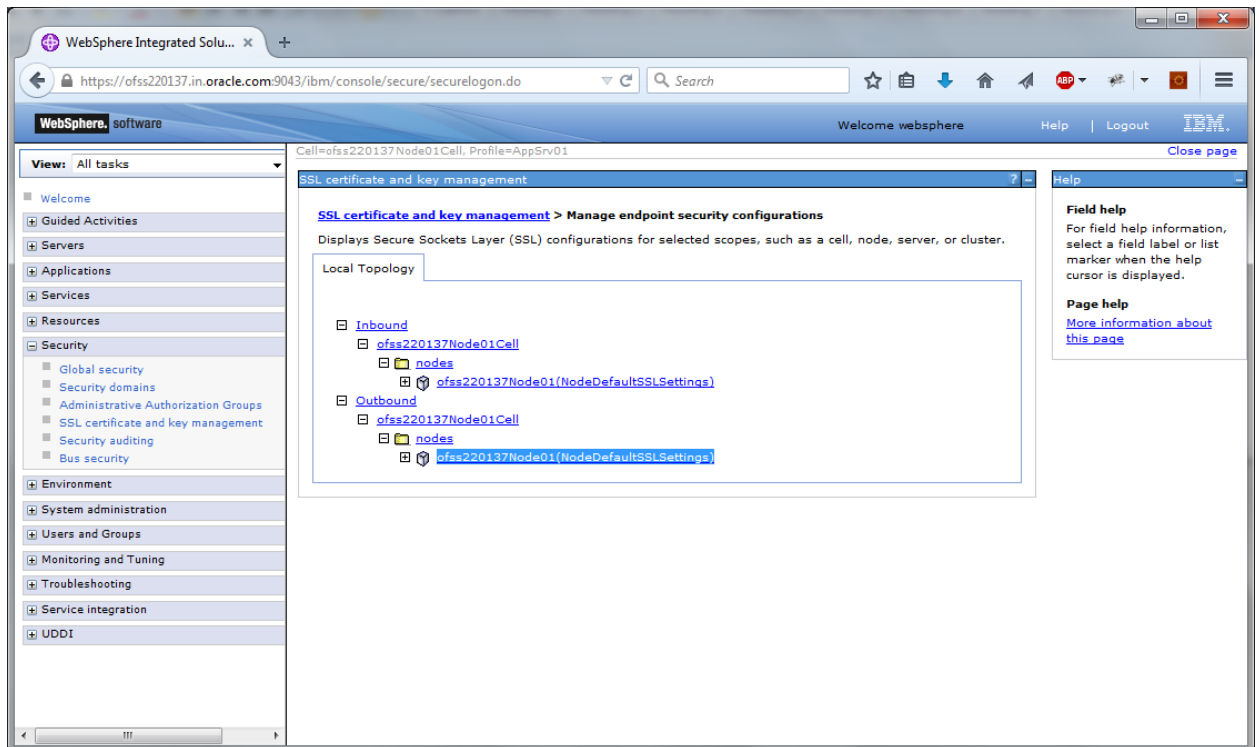
2. Change the inbound node settings. Expand 'Inbound' and click link highlighted in blue color.

The following screen is displayed.



3. Select the 'SSL Configuration' created which you just created. Click 'Update certificate alias list' button.
4. Ensure that the proper certificate and SSL configuration are selected. Further, click 'Apply' and save the settings.

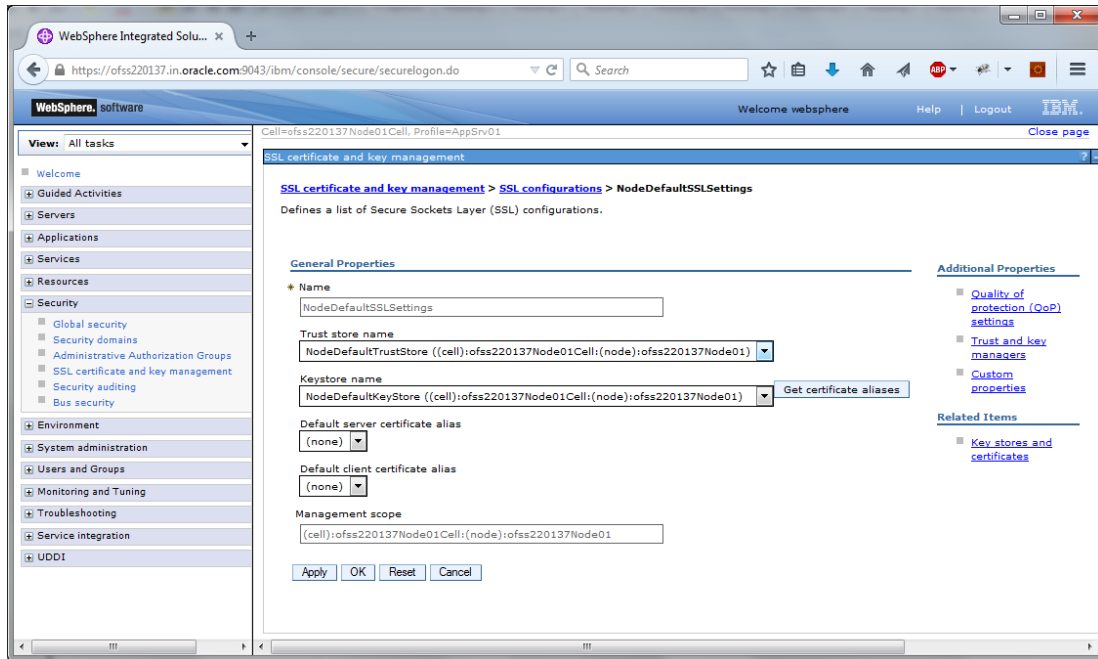
You can view the settings under 'Inbound'.



5. Repeat the above steps for 'Outbound' as well.
6. You need to repeat the above steps for server2 also.

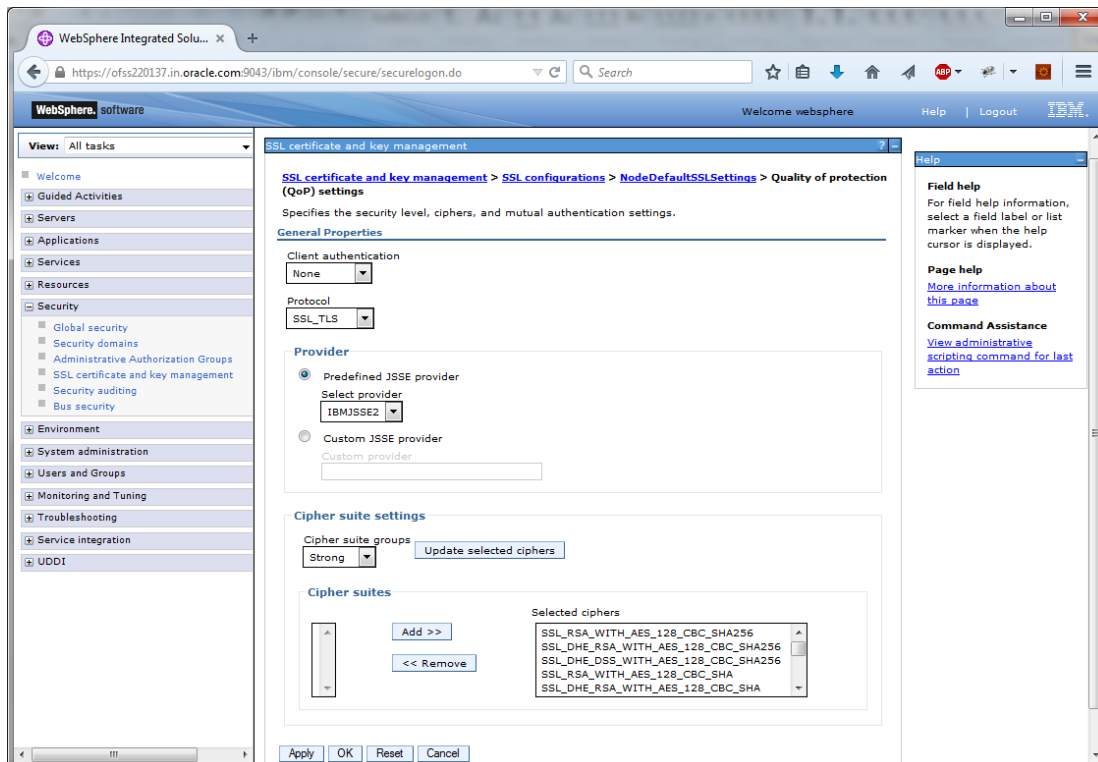
1.10 Protection Quality

1. Expand 'SSL certificate and key management > SSL configurations > {YOUR SERVER CONFIG }'.



2. On the right side, click 'Quality of protection (QoP) settings'.

The following screen is displayed.



3. Under 'Client authentication' choose 'Supported' from the drop-down list.

4. Click 'Apply' and save the changes.
5. You need to repeat these steps for the second server. Once you have made the changes to both the servers, restart the servers. It is recommended to restart the servers after making the changes.

// New Changes

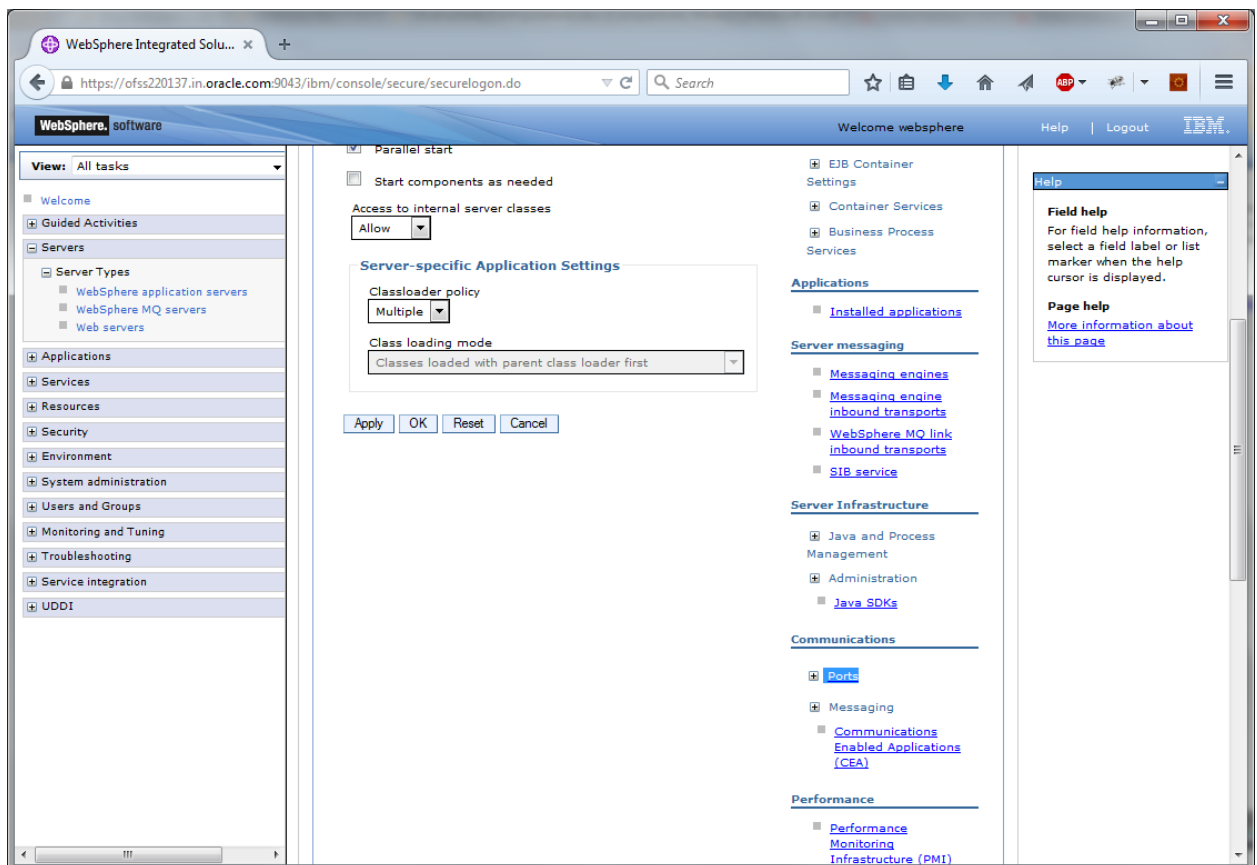
1.11 Importing or Adding Server Certificates using Batch

Alternatively, you can import or add the server certificates using *ikeyman.bat*. This batch is available at the following location:

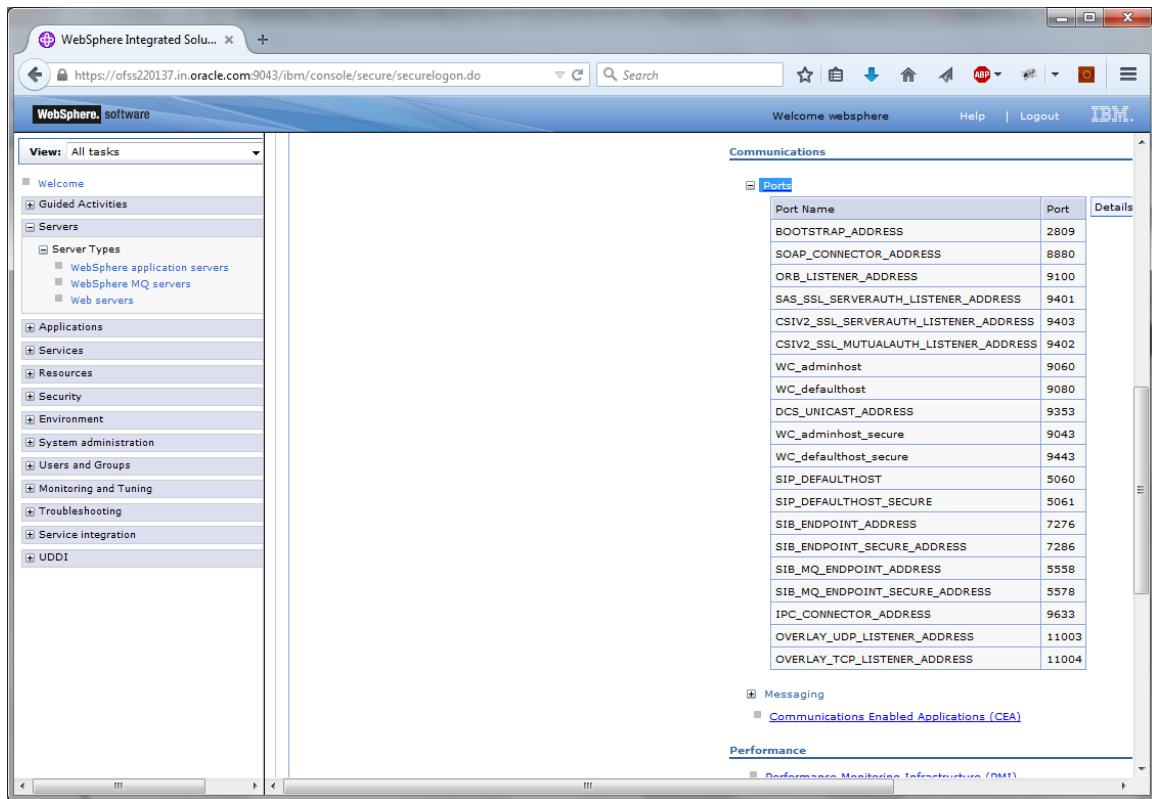
<InstalledLocatio>\IBM\WebSphere\AppServer\bin

For security reasons, change the password for 'defaultTruststore' (trust.p12). The default password is 'WebAS'.

SSL port information is available in the following screens.

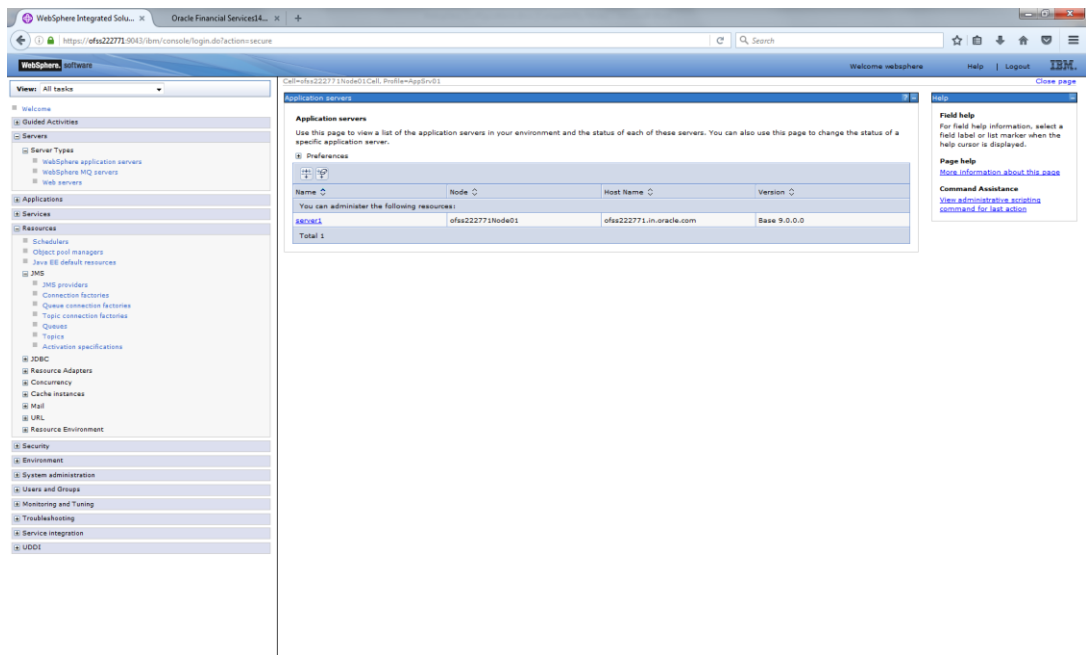


1. Click 'Ports'.
2. The details are displayed as follows.



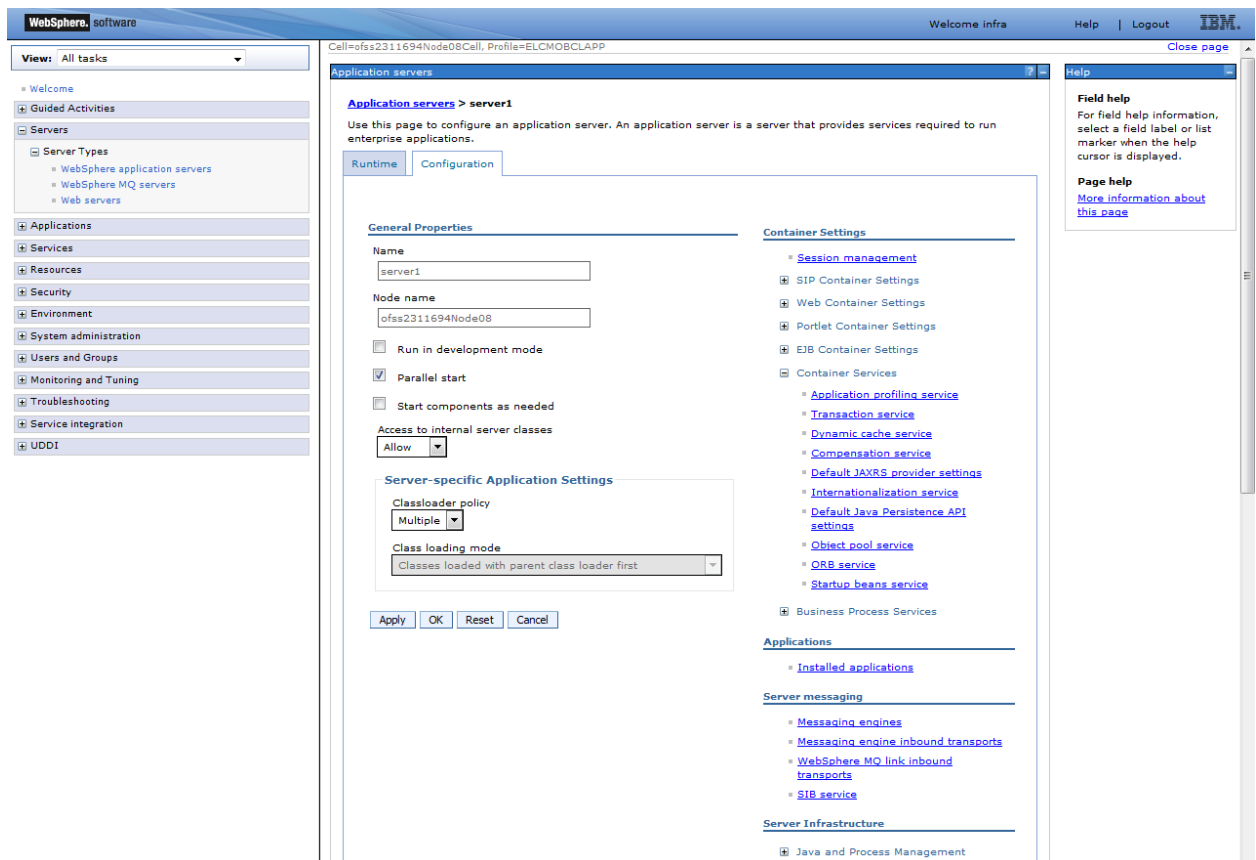
1.11.1 Default JAXRS provider settings

1. Navigate to Websphere home page.
2. Expand Servers > Server Types and click 'Websphere application servers'.



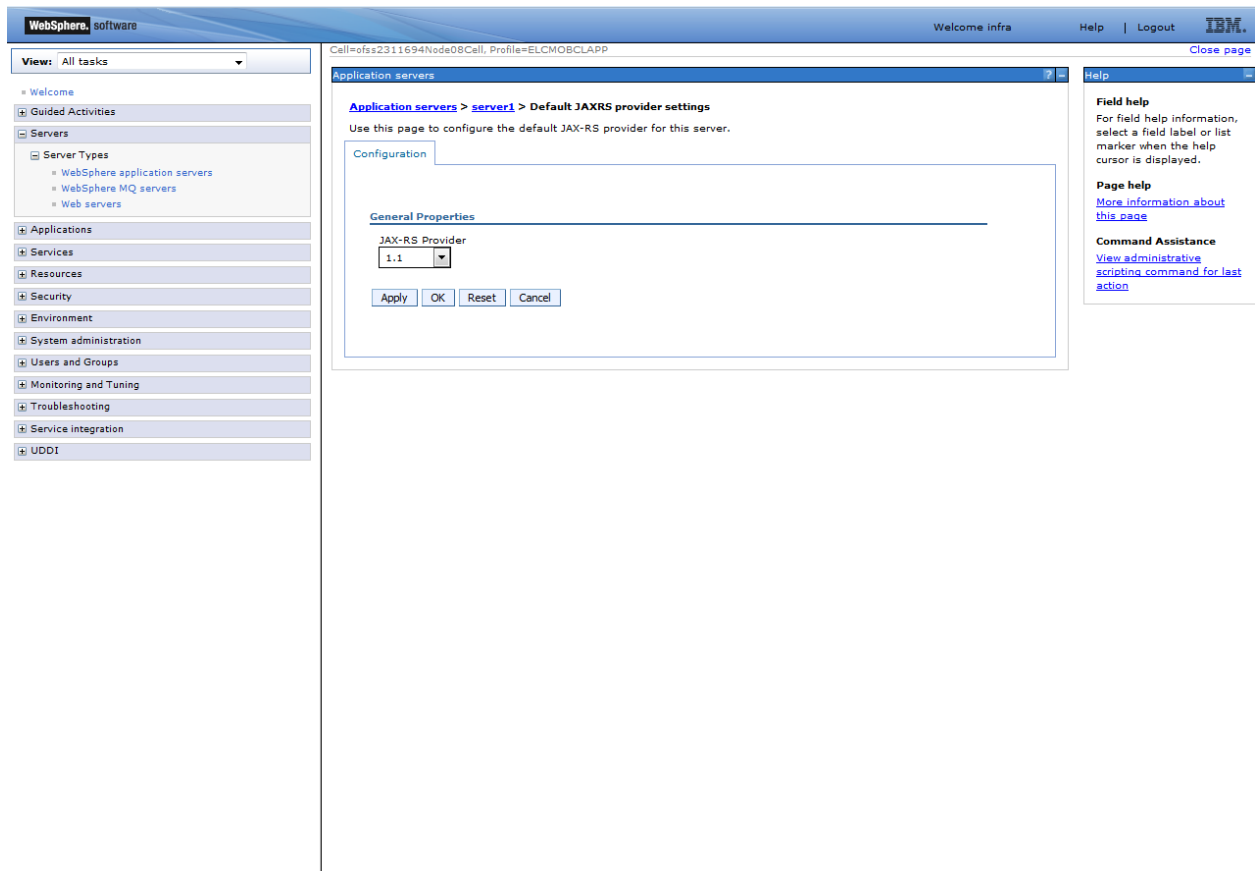
3. Click 'server1'.

The following screen is displayed.



4. Expand 'Container Services' under Communications and select 'default JAX-RS provider settings'.

The following screen is displayed.



5. Select JSX_RS Provider version 1.1 from the drop-down list.
6. Click 'Apply' and 'Save' the changes. It is recommended to restart the servers after making the changes.

2. Creating Resources on Websphere

2.1 Introduction

This document explains the steps to create resources on Websphere application server and Queues in Websphere MQ server.

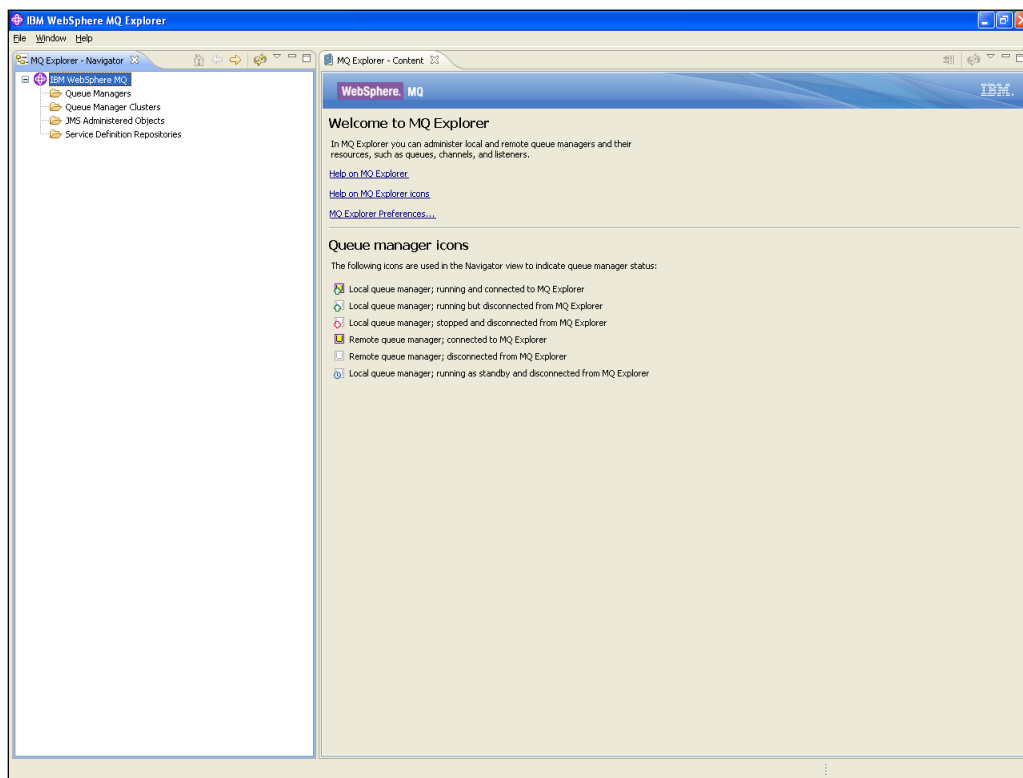
2.2 Creating Queues on Websphere MQ Server

The process of creation of queues on Websphere is explained under the following headings.

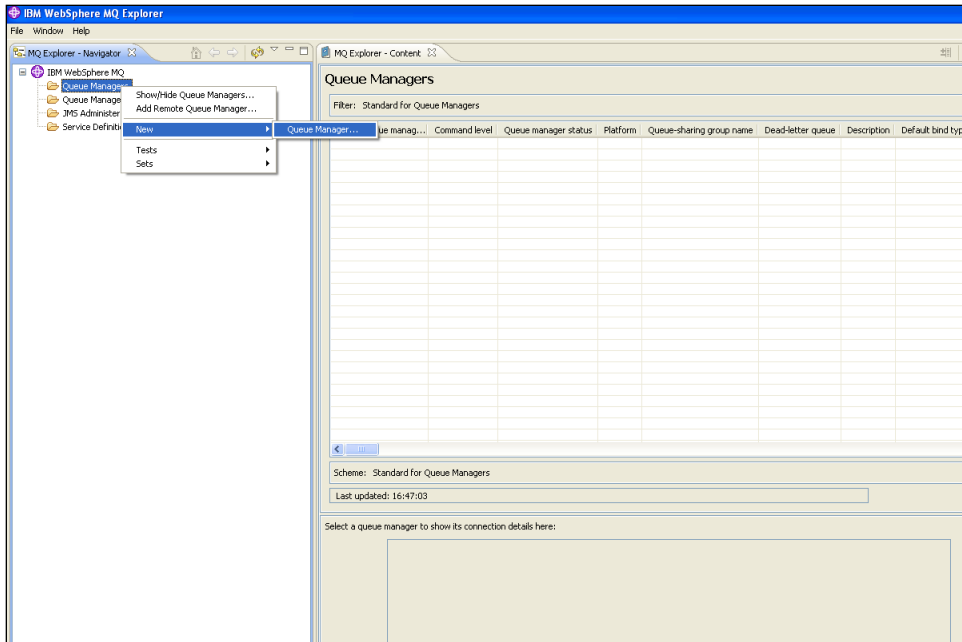
2.2.1 Creating Queue Manager through Console

To create queue manager through console, follow the steps given below:

1. Start MQ server console.



2. On the left pane, go to 'IBM Websphere MQ > Queue Manager > New > Queue Manager' as shown below:



The following screen is displayed:

Create Queue Manager

Queue Manager
Enter basic values

Queue manager name: QM_DDHP0520

☒ Make this the default queue manager

Default transmission queue:

Dead-letter queue:

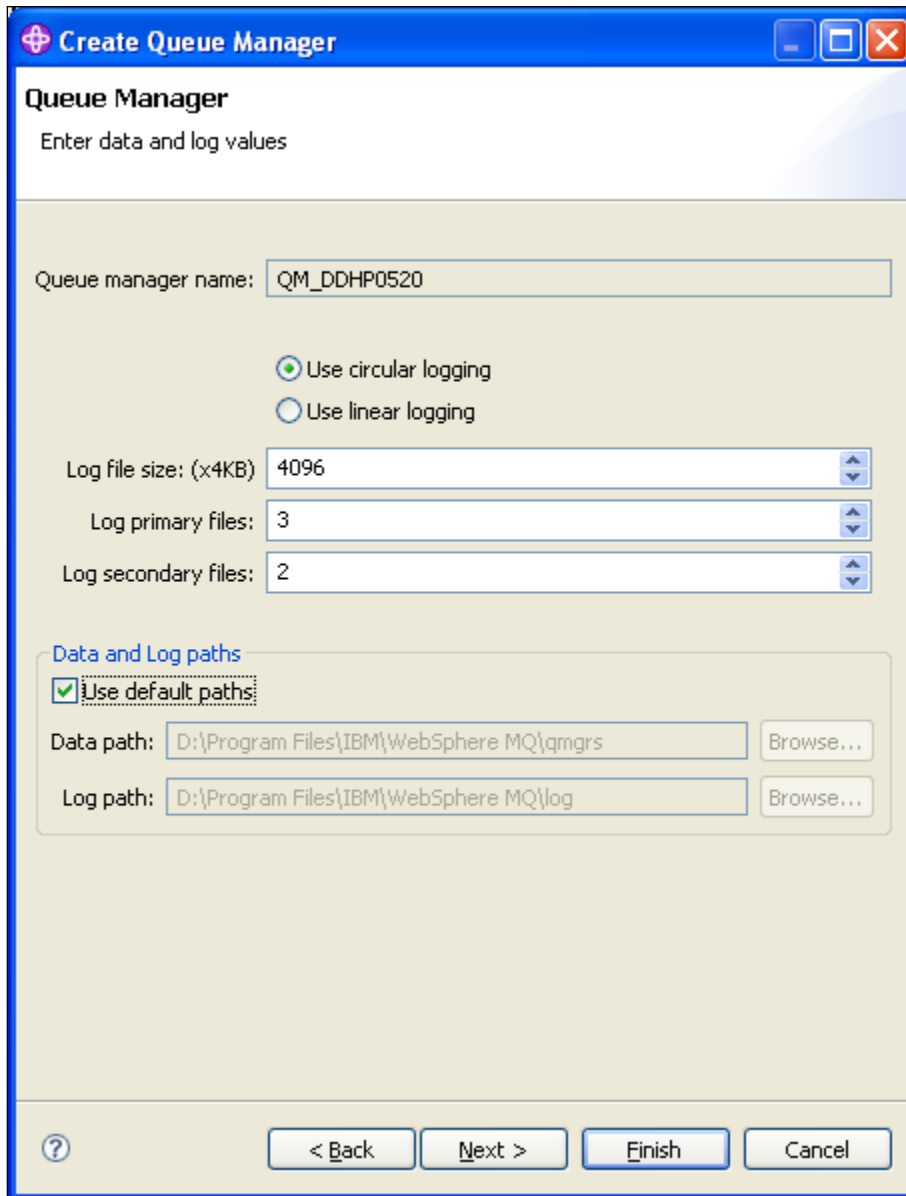
Max handle limit: 256

Trigger interval: 999999999

Max uncommitted messages: 10000

? < Back Next > Finish Cancel

3. Specify the 'Queue manager name'. Check the box 'Make this the default queue manager'.
4. Click 'Next'. The following screen is displayed:



The image shows a Windows-style dialog box titled "Create Queue Manager". The subtitle is "Queue Manager" and the instruction is "Enter data and log values". The dialog has a blue title bar with standard window controls. The main area is light beige. It contains a text field for "Queue manager name" with the value "QM_DDHP0520". Below this are two radio buttons: "Use circular logging" (selected) and "Use linear logging". There are three spinners: "Log file size: (x4KB)" set to 4096, "Log primary files" set to 3, and "Log secondary files" set to 2. A section titled "Data and Log paths" contains a checked checkbox "Use default paths:". Below this are two text fields: "Data path" with the value "D:\Program Files\IBM\WebSphere MQ\qmgrs" and "Log path" with the value "D:\Program Files\IBM\WebSphere MQ\log". Each text field has a "Browse..." button to its right. At the bottom, there is a help icon (question mark) and four buttons: "< Back", "Next >", "Finish", and "Cancel".

Create Queue Manager

Queue Manager
Enter data and log values

Queue manager name: QM_DDHP0520

☒ Use circular logging
☐ Use linear logging

Log file size: (x4KB) 4096

Log primary files: 3

Log secondary files: 2

Data and Log paths

☒ Use default paths:

Data path: D:\Program Files\IBM\WebSphere MQ\qmgrs Browse...

Log path: D:\Program Files\IBM\WebSphere MQ\log Browse...

? < Back Next > Finish Cancel

5. Click 'Next'.

The following screen is displayed:

Create Queue Manager

Queue Manager
Enter configuration options

Queue manager name: QM_DDHP0520

☒ Start queue manager after it has been created

Multi-instance Queue Manager:

☐ Permit a standby instance

Select type of queue manager startup

☒ Automatic
☐ Service (manual)
☐ Interactive (manual)

Configures the queue manager to start automatically when the machine starts up.

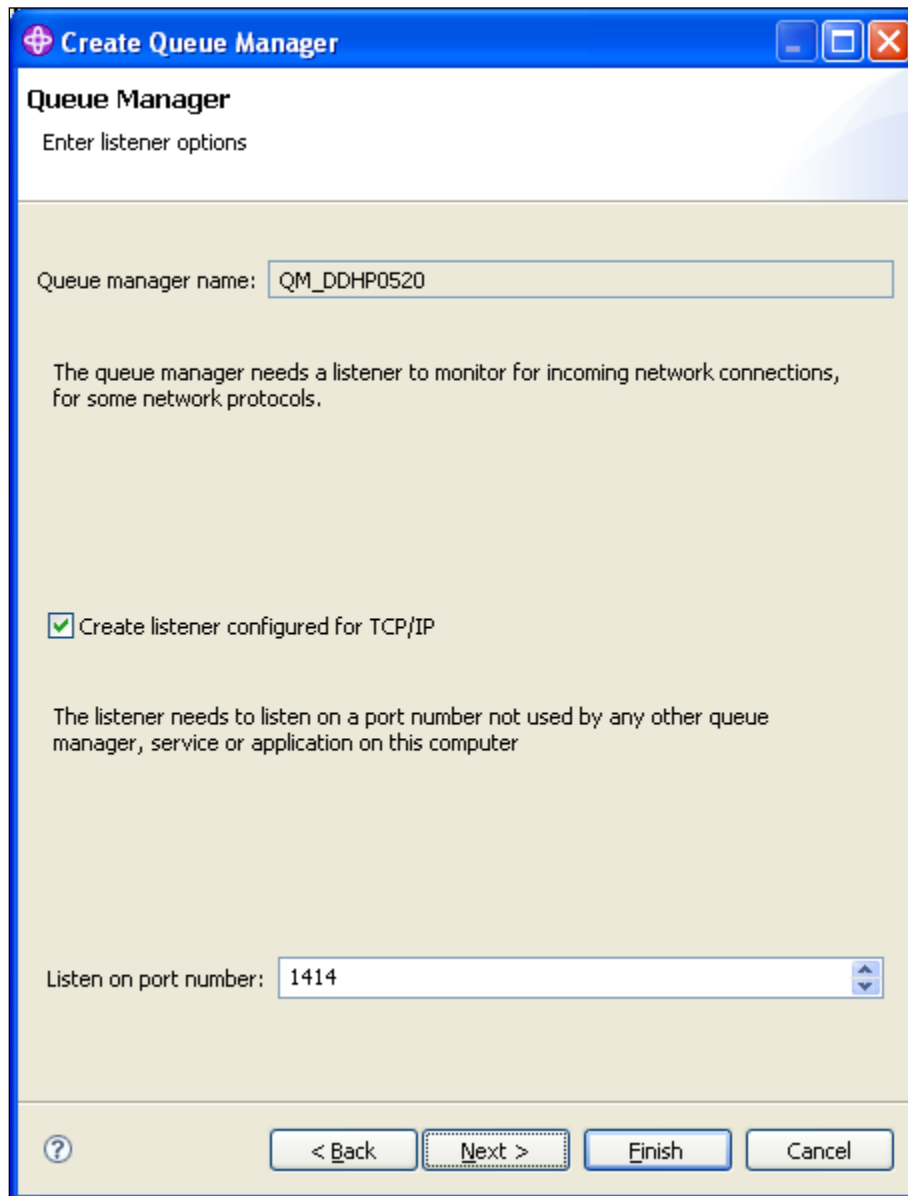
Create server-connection channel to allow remote administration of the queue manager over TCP/IP

☐ Create server-connection channel

? < Back Next > Finish Cancel

6. Click 'Next'.

The following screen is displayed:



The image shows a Windows-style dialog box titled "Create Queue Manager". The window has a blue title bar with standard minimize, maximize, and close buttons. The main content area has a light beige background. At the top, the text "Queue Manager" is displayed, followed by the instruction "Enter listener options". Below this, there is a text input field labeled "Queue manager name:" containing the text "QM_DDHP0520". A paragraph of text follows: "The queue manager needs a listener to monitor for incoming network connections, for some network protocols." Below this is a checked checkbox labeled "Create listener configured for TCP/IP". Another paragraph of text follows: "The listener needs to listen on a port number not used by any other queue manager, service or application on this computer". At the bottom of the main area, there is a text input field labeled "Listen on port number:" containing the value "1414". The bottom of the dialog box contains a row of buttons: a help button (question mark icon), "< Back", "Next >", "Finish", and "Cancel".

Create Queue Manager

Queue Manager
Enter listener options

Queue manager name: QM_DDHP0520

The queue manager needs a listener to monitor for incoming network connections, for some network protocols.

☒ Create listener configured for TCP/IP

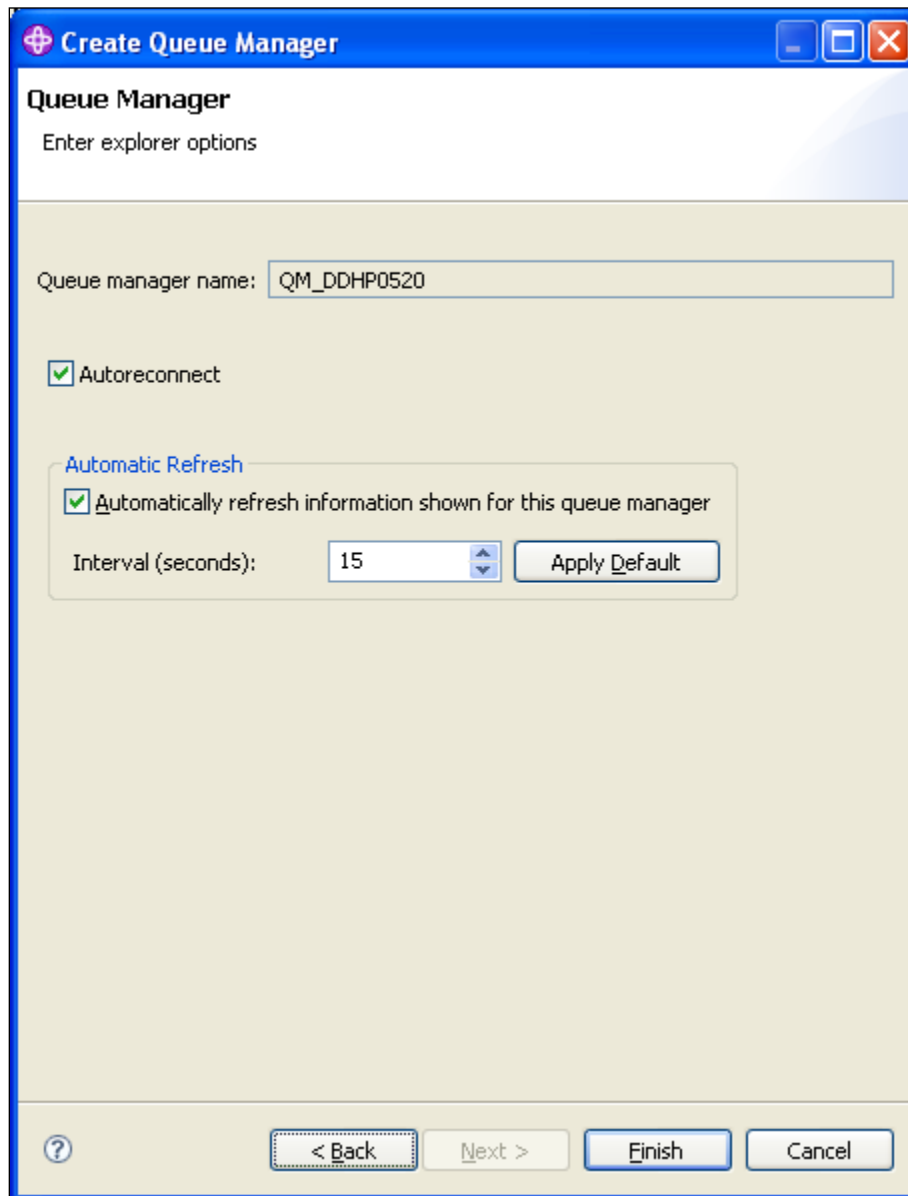
The listener needs to listen on a port number not used by any other queue manager, service or application on this computer

Listen on port number: 1414

? < Back Next > Finish Cancel

7. Specify the 'Listen on port number' as '1414' (default). Click 'Next'

The following screen is displayed:



The image shows a Windows-style dialog box titled "Create Queue Manager". The title bar is blue with standard minimize, maximize, and close buttons. Below the title bar, the text "Queue Manager" is displayed in bold, followed by the instruction "Enter explorer options". The main area of the dialog is light beige. It contains a text input field for "Queue manager name:" with the value "QM_DDHP0520". Below this is a checked checkbox for "Autoreconnect". A section titled "Automatic Refresh" in blue text contains a checked checkbox for "Automatically refresh information shown for this queue manager". Below this checkbox is a label "Interval (seconds):" followed by a spin box set to "15" and an "Apply Default" button. At the bottom of the dialog, there is a row of buttons: a help button (question mark icon), "< Back", "Next >", "Finish", and "Cancel".

Create Queue Manager

Queue Manager

Enter explorer options

Queue manager name: QM_DDHP0520

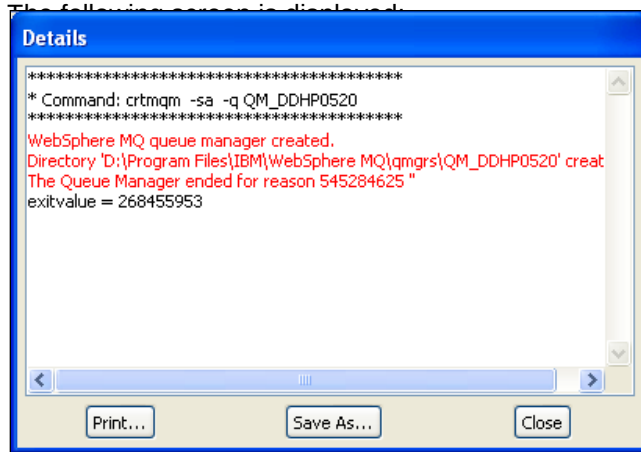
☒ Autoreconnect

Automatic Refresh

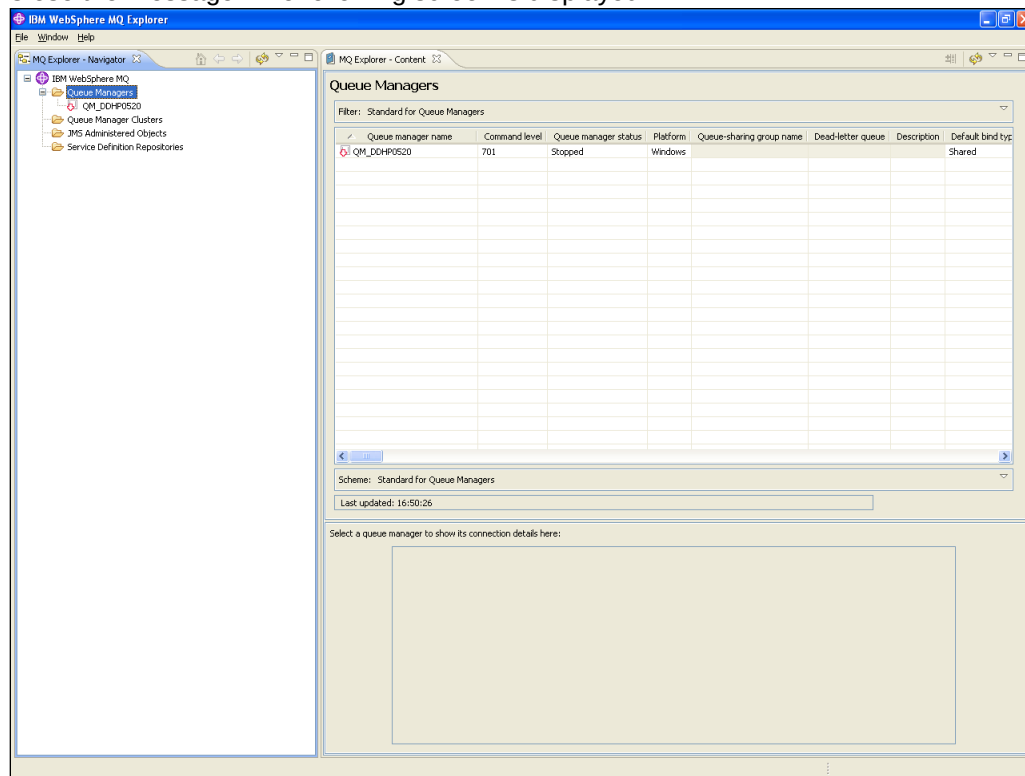
☒ Automatically refresh information shown for this queue manager

Interval (seconds): 15

8. Click 'Finish'.

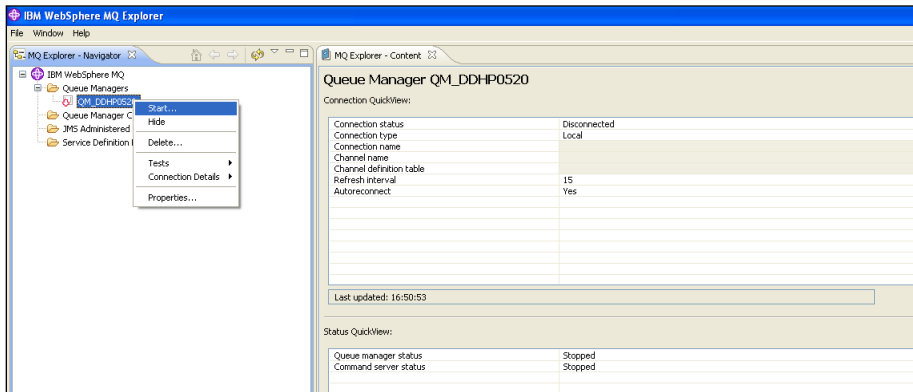


Close the message. The following screen is displayed:

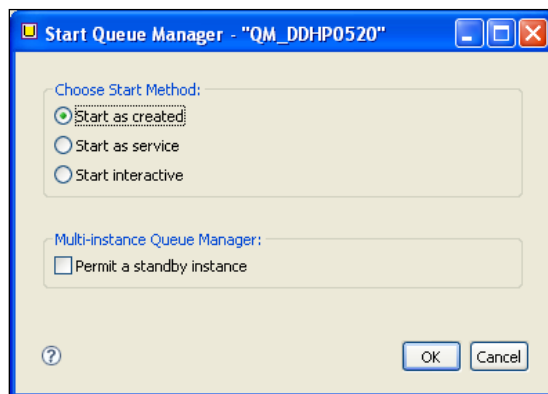


9. Right click 'Queue Manager' and select 'Start'.

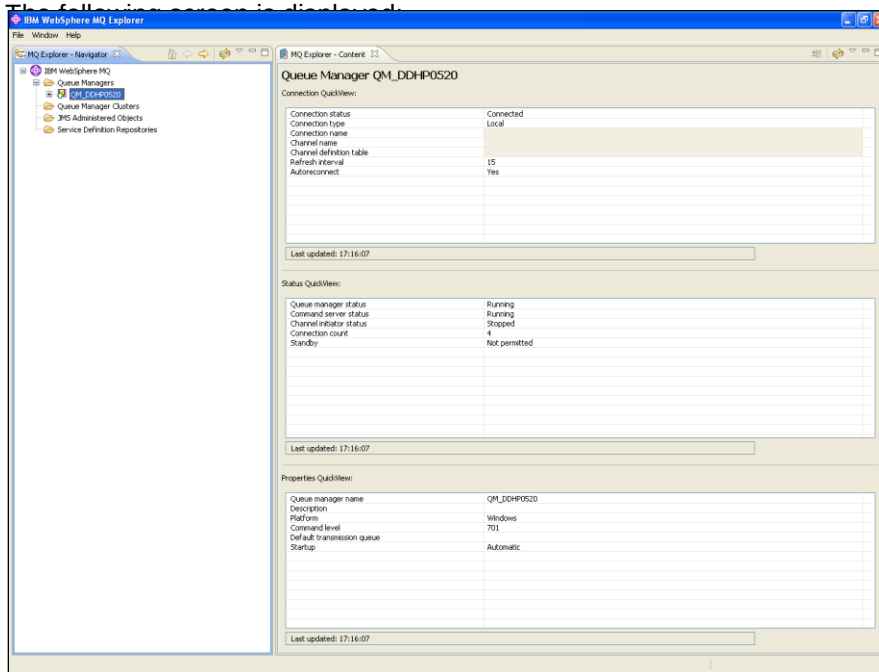
The following screen is displayed:



10. Right click 'Queue Manager QM_DDHP0520' and select 'Start'. The following screen is displayed:



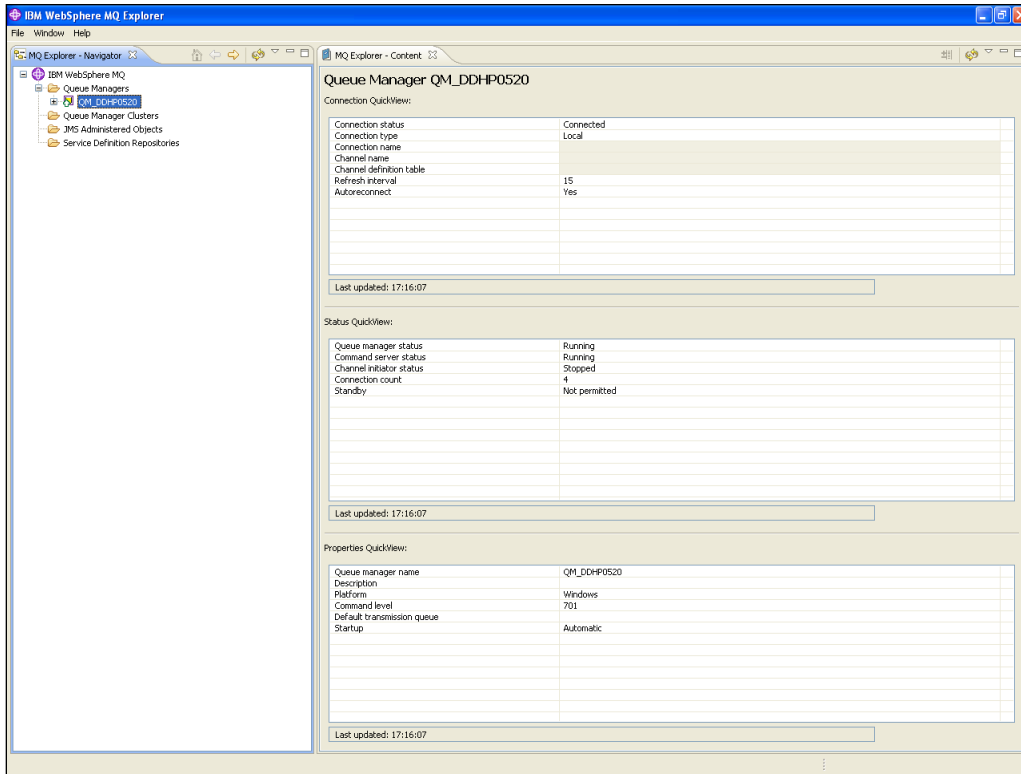
11. Click 'OK'.



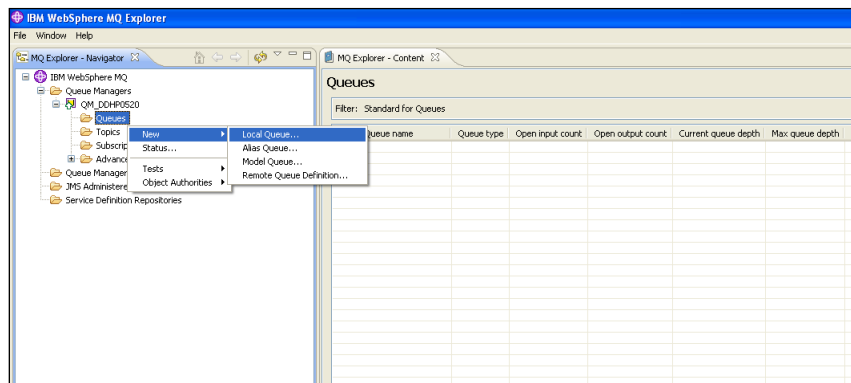
2.2.2 Creating Queues

To create queues, follow the steps given below:

1. Start MQ server console.

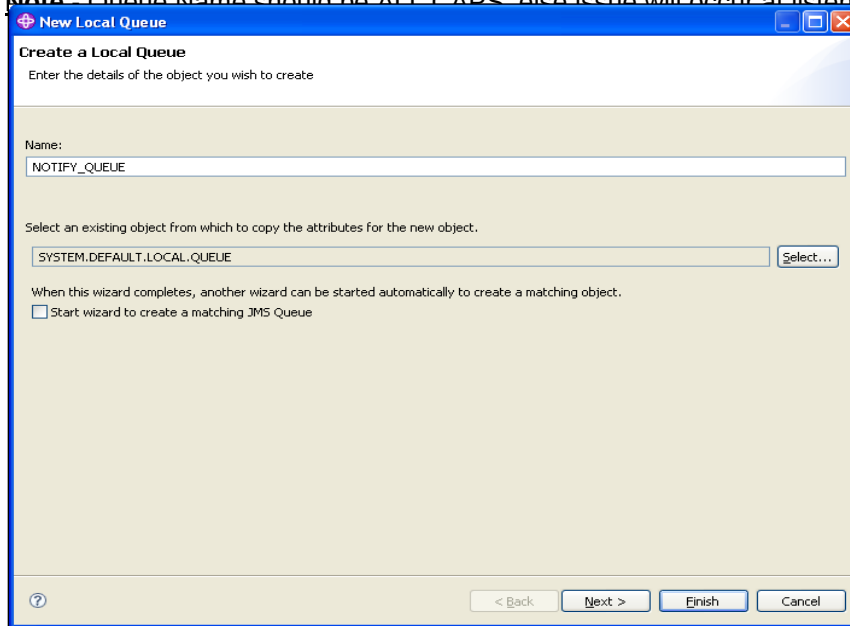


- On the left pane, go to 'IBM Websphere MQ > Queue Managers > QM_DDHP0520 > Queues > New > Local Queue' as shown below.



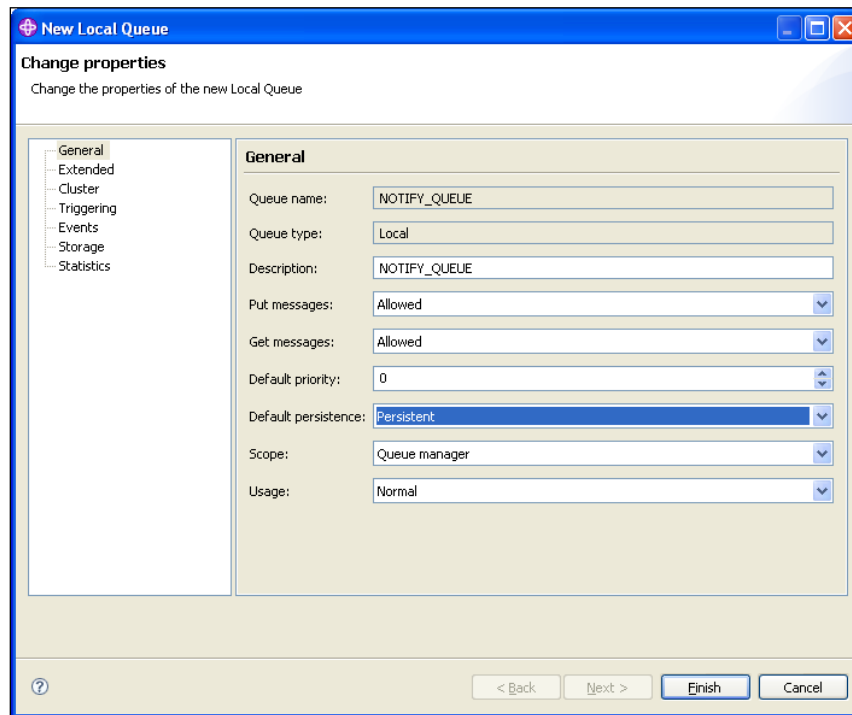
The following screen is displayed:

Note: Queue Name should be ALL CAPS, else issue will occur at listener level in WAS.



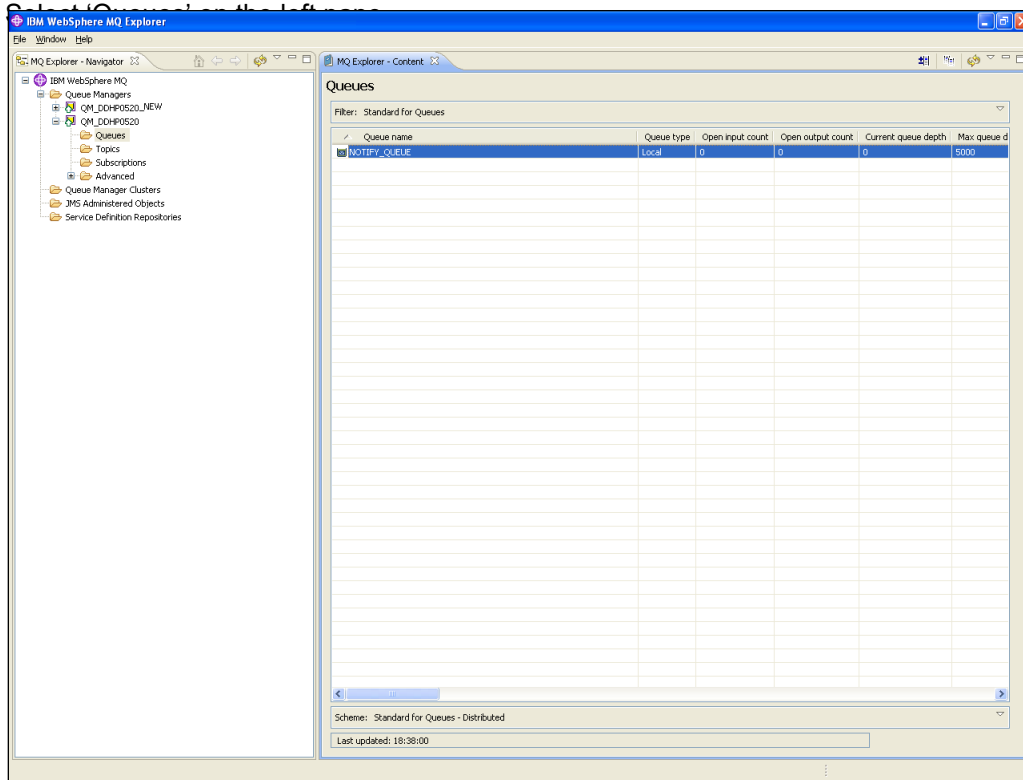
The screenshot shows the 'New Local Queue' wizard, specifically the 'Create a Local Queue' step. The window title is 'New Local Queue'. The main heading is 'Create a Local Queue' with the instruction 'Enter the details of the object you wish to create'. The 'Name:' field contains 'NOTIFY_QUEUE'. Below it, there is a section 'Select an existing object from which to copy the attributes for the new object.' with a dropdown menu showing 'SYSTEM.DEFAULT.LOCAL.QUEUE' and a 'Select...' button. A checkbox 'Start wizard to create a matching JMS Queue' is present and unchecked. At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

3. Specify the queue name. Click 'Next'. The following screen is displayed:



The screenshot shows the 'New Local Queue' wizard, specifically the 'Change properties' step. The window title is 'New Local Queue'. The main heading is 'Change properties' with the instruction 'Change the properties of the new Local Queue'. On the left, there is a tree view with 'General' selected. The 'General' tab is active, showing various properties: 'Queue name:' (NOTIFY_QUEUE), 'Queue type:' (Local), 'Description:' (NOTIFY_QUEUE), 'Put messages:' (Allowed), 'Get messages:' (Allowed), 'Default priority:' (0), 'Default persistence:' (Persistent), 'Scope:' (Queue manager), and 'Usage:' (Normal). At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

4. Specify the description. Select 'Persistent' as the 'Default persistence'.



5. You can find the new queue name in the list.

2.3 Creating Queue Manager and Queue using UNIX Commands

You need to create, configure, post and view messages in IBM MQ queues. The method is described under the following headings.

For this, first you need to open 'Putty' and connect it to the MQ server installed box.

2.3.1 Creating Queue Manager

Change the directory to '<Websphere_MQ_HOME>'. Here, 'Websphere_MQ_HOME' is the MQ server software installation directory.

The command to create Queue Manager is given below:

```
crtmqm <queue_manager_name>
```

Example

```
crtmqm FC_QMGR
```

This command creates the queue manager 'FC_QMGR' in the MQ server.

2.3.2 **Starting Queue Manager**

Once the queue manager is created, you need to start the queue manager using the following command:

```
strmqm <queue_manager_name>
```

Example

```
strmqm FC_QMGR
```

This command starts the 'FC_QMGR' queue manager.

2.3.3 **Starting MQ Service to Create Queues under FC_QMGR**

After starting the queue manager, run the MQSC service (for creating queues and other objects) of queue manager. You can use the following command:

```
runmqsc <queue_manager_name>
```

Example

```
runmqsc FC_QMGR
```

This command starts the MQ service for 'FC_QMGR'.

2.3.4 **Creating Queues**

After starting the MQSC issue, you need to create the required queues using the following command:

```
DEFINE QLOCAL (<QUEUE_NAME>)
```

Example

```
DEFINE QLOCAL (EMSOUT_QUEUE)
```

This command creates all the necessary queues.

2.3.5 **Creating Channel**

After creating the queues, you need to create a channel for queue manager using the following command:

```
DEFINE CHANNEL (<CHNL_NAME>) CHLTYPE(<CHANNEL_TYPE>)
```

Here, 'CHNL_NAME' is the name of the channel and 'CHANNEL_TYPE' is the type of channel such as server connection, sender, receiver, etc. You can create the server connection channel using the following command:

```
DEFINE CHANNEL (FC_CNL) CHLTYPE (SVRCONN)
```

Here, SVRCONN stands for the 'Server Connection' channel type.

2.3.6 **Ending MQSC**

You can use the command 'END' to end the MQSC service.

2.3.7 Creating Bindings

After creating the queues and the channel, you need to bind them using the JMSAdmin. To do this, start Putty and connect it to the MQ server installed box.

Move to the directory '<Websphere_MQ_HOME>/java/bin'. Here, 'Websphere_MQ_HOME' is the MQ server software installation path.

In this folder, you will find the file 'JMSAdmin.config'. You need to give the PROVIDER_URL to which the .bindings files need to be created.

```
PROVIDER_URL=file: <Websphere_MQ_HOME>/JNDI
```

Example

```
PROVIDER_URL=file: /var/mqm/JNDI
```

Below environment variables need to be set before creating queue/connection factory configurations.

```
PATH=$PATH:$HOME/bin
export MQ_JAVA_INSTALL_PATH=/opt/mqm/java
export MQ_JAVA_DATA_PATH=/var/mqm
export MQ_JAVA_LIB_PATH=/opt/mqm/java/lib
L=$MQ_JAVA_INSTALL_PATH/lib
CLASSPATH=$CLASSPATH:$L/com.ibm.mq.jar:$L/com.ibm.mqjms.jar
export
CLASSPATH=$CLASSPATH:/opt/mqm/samp/jms/samples:/opt/mqm/samp/wmqjava/samp
export PATH
```

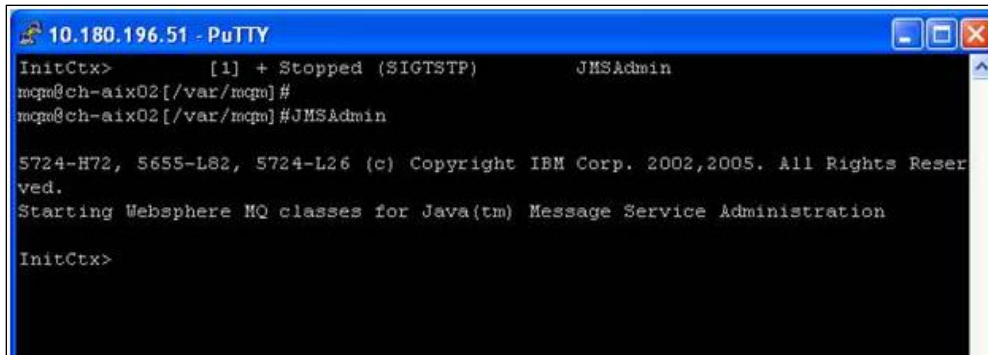
Launch JMSAdmin



You should have read-write access on this folder.

2.3.8 Creating QCF

After creating the queues and channel, you need to create a queue connection factory in the MQ server. Complete the above steps and make above changes to the 'JMSAdmin.config' file. Move to the directory '<Websphere_MQ_HOME>/java/bin' in Putty. Type 'JMSAdmin' as shown in the figure.



```
10.180.196.51 - PuTTY
InitCtx> [1] + Stopped (SIGTSTP) JMSAdmin
mqpn@ch-aix02[/var/mqpn]#
mqpn@ch-aix02[/var/mqpn]#JMSAdmin

5724-H72, 5655-L82, 5724-L26 (c) Copyright IBM Corp. 2002,2005. All Rights Reserved.
Starting Websphere MQ classes for Java(tm) Message Service Administration

InitCtx>
```

This will take you to the 'InitCtx>' section. Use the following command to create queue connection factory:

```
define qcf (<qcf_name>) qmgr(<queue_mgr_name>) host (<ip-address>) port(1010)
tran(CLIENT)
```

Example

```
define qcf (fc_qcf) qmgr(FC_QMGR) host (10.10.10.10) port(1010) tran(CLIENT)
```

This creates the queue connection factory for the queue manager 'FC_QMGR' in 10.10.10.10 server.

Now, you need to create the bindings for each queue. Use the following command in 'InitCtx>'.

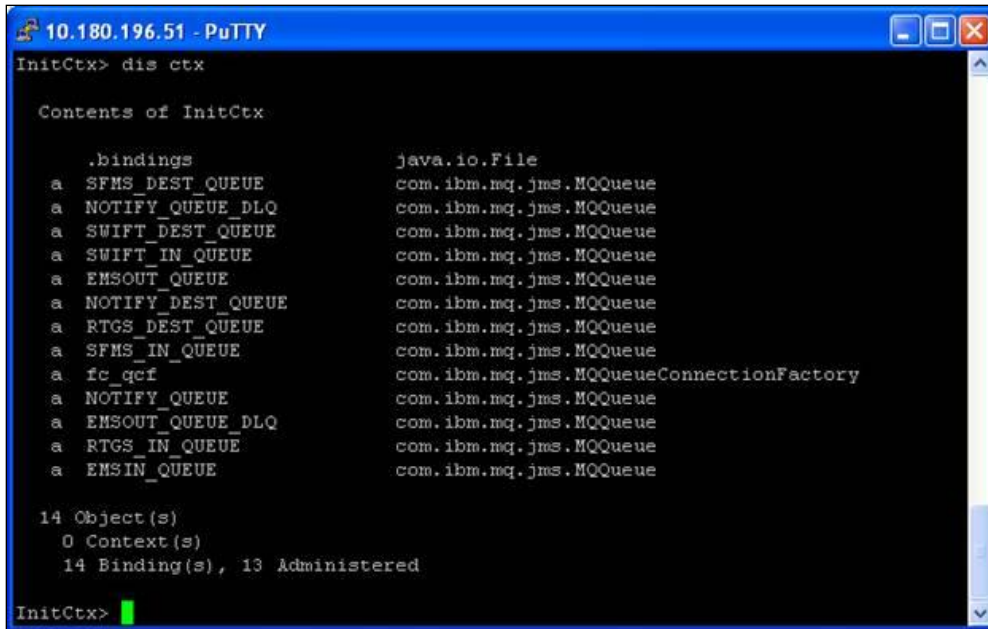
```
DEFINE Q(EMSOUT_QUEUE) QUEUE(EMSOUT_QUEUE) QMGR(FC_QMGR)
```

Use the same command for other queues also.

You can use the following command to view the binding details:

```
InitCtx> display ctx
```

The binding details are displayed as shown in the figure below.



```
10.180.196.51 - PuTTY
InitCtx> dis ctx

Contents of InitCtx

    .bindings
a SFMS_DEST_QUEUE      com.ibm.mq.jms.MQQueue
a NOTIFY_QUEUE_DLQ    com.ibm.mq.jms.MQQueue
a SWIFT_DEST_QUEUE     com.ibm.mq.jms.MQQueue
a SWIFT_IN_QUEUE       com.ibm.mq.jms.MQQueue
a EMSOUT_QUEUE         com.ibm.mq.jms.MQQueue
a NOTIFY_DEST_QUEUE   com.ibm.mq.jms.MQQueue
a RTGS_DEST_QUEUE     com.ibm.mq.jms.MQQueue
a SFMS_IN_QUEUE       com.ibm.mq.jms.MQQueue
a fc_qcf              com.ibm.mq.jms.MQQueueConnectionFactory
a NOTIFY_QUEUE        com.ibm.mq.jms.MQQueue
a EMSOUT_QUEUE_DLQ    com.ibm.mq.jms.MQQueue
a RTGS_IN_QUEUE       com.ibm.mq.jms.MQQueue
a EMSIN_QUEUE         com.ibm.mq.jms.MQQueue

14 Object(s)
0 Context(s)
14 Binding(s), 13 Administered

InitCtx>
```

Once this is created, you need to check whether the *.bindings* file is available in the path given in 'JMSAdmin.config' (PROVIDER_URL).

Now, you need to create JMS queues for DIRECT queues to post messages. DIRECT queues require connection to Oracle Banking Treasury Management application.

Example

Following are the DIRECT queues:

- NOTIFY_QUEUE
- EMSIN_QUEUE
- EMSOUT_QUEUE
- SFMS_INQUEUE
- SFMSOUT_QUEUE
- RTGS_INQUEUE
- INTERNAL_BIPREPORT_QUEUE
- INTERNAL_BIP_QUEUE_DLQ
- INTERNAL_BIPADVREPORT_QUEUE
- INTERNAL_BIP_ADVICE_QUEUE_DLQ
- INTERNAL_GI_UPLOAD_QUEUE
- INTERNAL_GI_UPLOAD_DLQ
- EMS_QUEUE_DLQ

You need to create JMS queues for the above queues as shown in the figure:

Queue name	Queue type	Open input count	Open output count	Current queue depth
DEFERRED_DEST_QUEUE	Local	0	0	0
EL_NOTIFY_DLQ	Local	0	0	0
EL_NOTIFY_REQ_Q	Local	0	0	0
EL_NOTIFY_RES_Q	Local	0	0	0
ELMDB_DLQ	Local	0	0	0
ELMDB_REQ_Q	Local	0	0	0
ELMDB_RES_Q	Local	0	0	0
EMS_EXTQUEUE	Local	0	0	0
EMS_INQUEUE	Local	2	0	0
EMS_OUTQUEUE	Local	1	0	0
MDB_QUEUE	Local	0	0	0
MDB_QUEUE_DLQ	Local	0	0	0
MDB_QUEUE_RESPONSE	Local	0	0	0
NOTIFY_DEST_QUEUE	Local	0	0	0
NOTIFY_QUEUE	Local	1	0	0
NOTIFY_QUEUE_DLQ	Local	0	0	0
RTGS_INQUEUE	Local	1	0	0
SFMS_INQUEUE	Local	1	0	0

2.3.9 MQ Channel Authentication

MQ Channel Authentication can be managed using following set of MQSC Commands

- Enable Channel Authentication

>ALTER QMGR CHLAUTH(ENABLE)

- b) Allow MQ Privileged Users to access Channel

>SET CHLAUTH(*) TYPE(BLOCKUSER) USERLIST(*MQADMIN) ACTION(REMOVE)

- c) Allow all client addresses to access Channel

>SET CHLAUTH(SYSTEM.*) TYPE(ADDRESSMAP) ADDRESS(*) ACTION(REMOVE)

2.4 Viewing IBM MQ Queues

Through MQ explorer, you can view the queues created in IBM MQ. If the IBM MQ server sits on a Unix box, an MQ client needs to be setup in a client machine in Windows operating system.

Follows the below steps to view the queues created in server, from an MQ client:

1. Install IBM MQ client in a client terminal.
2. Open the client MQ explorer.
3. Right click 'Queue Managers' on the left pane and select 'Show/Hide Queue Managers'.
4. Click 'Add' in the Show/Hide Queue Managers window.
5. Specify the name of Queue Manager which is created in the MQ server. Click 'Next'.
6. Specify the IP address of the IBM MQ server in the Host name or IP address field.

7. Specify the Port number in which the Queue manager is created in MQ server.
8. Specify the server connection channel created in the MQ server. Click 'Finish'.

Under the Queue Manager menu, the queue manger created in the server is displayed with its IP address and port number in braces.

Queue name	Queue type	Definition type	Open input count	Open output count	Current queue depth	Max queue depth	Put messages
EMSIIN_QUEUE	Local	Predefined	1	0	0	5000	Allowed
EMSIOUT_QUEUE	Local	Predefined	1	0	12	5000	Allowed
EMSIOUT_QUEUE_DLQ	Local	Predefined	0	0	0	5000	Allowed
FCQMGR	Local	Predefined	0	0	0	5000	Allowed
MDB_QUEUE	Local	Predefined	1	0	0	999999999	Allowed
MDB_QUEUE_DLQ	Local	Predefined	0	0	6	999999999	Allowed
MDB_QUEUE_RESPONSE	Local	Predefined	0	0	12	999999999	Allowed
NOTIFY_DEST_QUEUE	Local	Predefined	0	0	1	5000	Allowed
NOTIFY_QUEUE	Local	Predefined	3	0	0	5000	Allowed
NOTIFY_QUEUE_DLQ	Local	Predefined	0	0	19	5000	Allowed
RTGS_DEST_QUEUE	Local	Predefined	0	0	0	5000	Allowed
RTGS_DL_QUEUE	Local	Predefined	1	0	0	5000	Allowed
SPMS_DEST_QUEUE	Local	Predefined	0	0	32	5000	Allowed
SPMS_IN_QUEUE	Local	Predefined	1	0	3	5000	Allowed
SPMSOUT_QUEUE	Local	Predefined	1	0	3	5000	Allowed

3. Creating JDBC Resources on Web Sphere

3.1 Introduction

This chapter guides you through the process of JDBC resource creation on IBM Websphere application server.

3.2 Prerequisite:

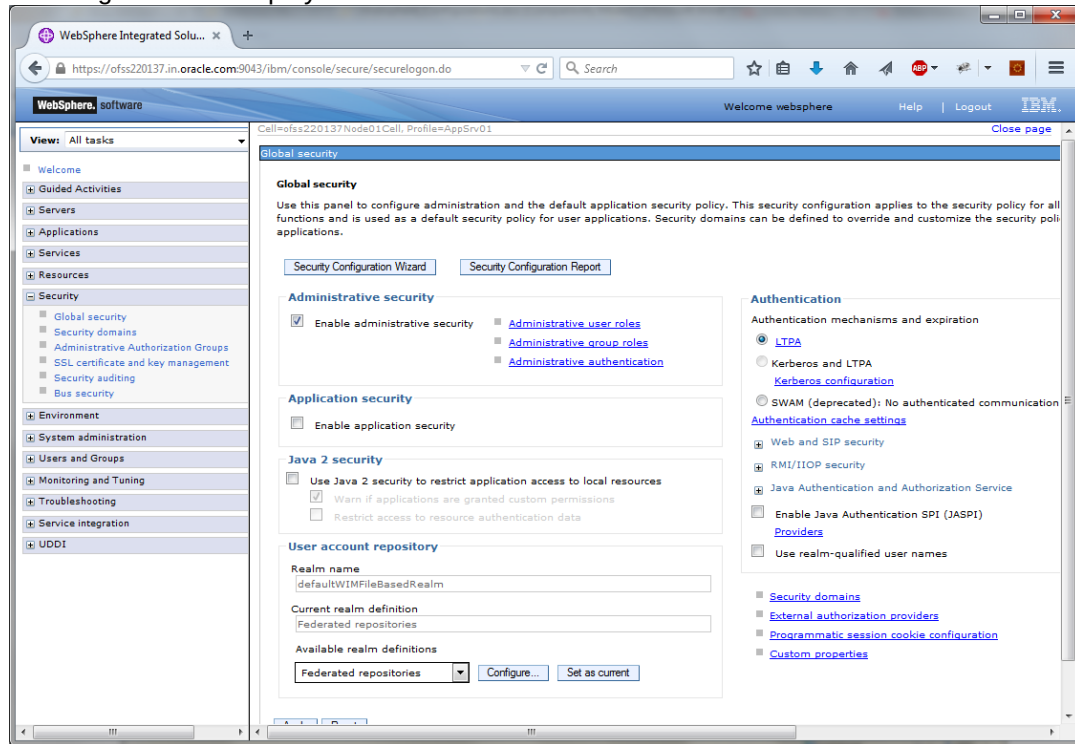
If OCI configuration needs to be used in data sources, please refer the vendor specific support manual and make the configuration changes before creating datasources.

3.3 Creating JDBC Sources

3.3.1 Creating Global Security

1. Specify the Websphere administrator username and password.
2. Click 'Log In'.

4. Navigate to the Websphere home page . Expand 'Security' and select 'Global Security'. The following screen is displayed.



5. Expand 'Java Authentication and Authorization Service' and click 'J2C authentication data'.

The following screen is displayed.

WebSphere Integrated Solu...

<https://ofss220137.in.oracle.com:9043/ibm/console/secure/securelogin.do>

WebSphere, software

Welcome websphere

Help | Logout

IBM.

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
- Security
 - Global security
 - Security domains
 - Administrative Authorization Groups
 - SSL certificate and key management
 - Security auditing
 - Bus security
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Cell=ofss220137/Node01Cell, Profile=AppSrv01

Global security

Global security > JAAS - J2C authentication data

Specifies a list of user identities and passwords for Java(TM) 2 connector security to use.

☒ Prefix new alias names with the node name of the cell (for compatibility with earlier releases)

Apply

Preferences

New...

Delete

Select

Alias

User ID

Description

You can administer the following resources:

☐	ofss220137/Node01/FC121ASK	FC121ASK	FC121ASK
☐	ofss220137/Node01/FCUBS121_DEV	FCUBS121_DEV	FCUBS121_DEV

Total 2

Field help

For field help information, select a field label or list marker when the help cursor is displayed.

Page help

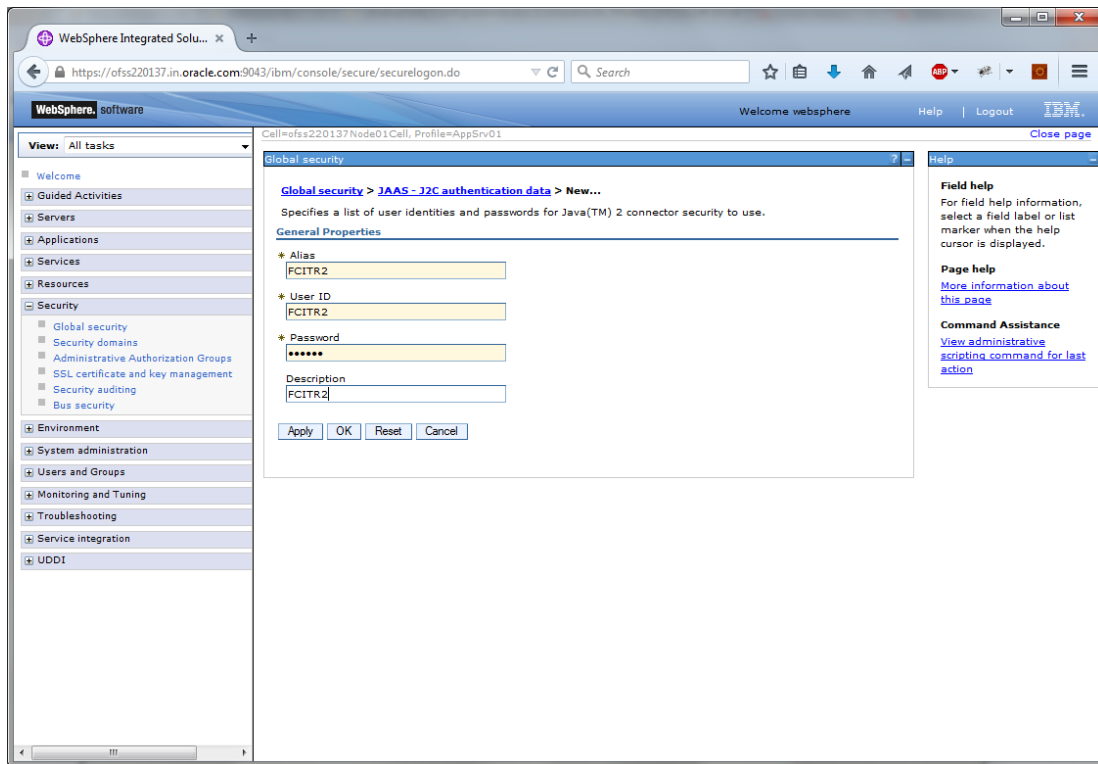
[More information about this page](#)

Command Assistance

[View administrative scripting command for last action](#)

6. Click 'New'.

The following screen is displayed.



7. You need to define the connection properties. Specify the following details.

- Alias
- User ID of the Database
- Password of the Database
- Description

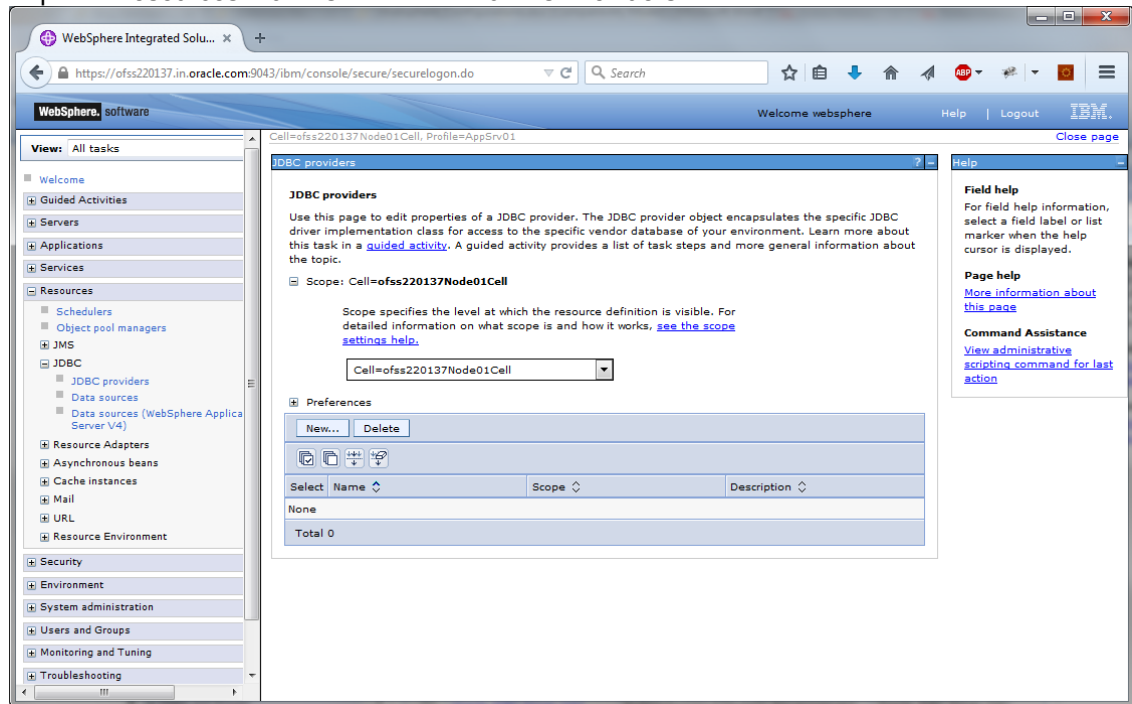
8. Once you have specified the above details, click 'Apply' and then click 'Save' link appears in the top.

3.3.2 JDBC Provider for Non XA Data Source

Follow the steps given below:

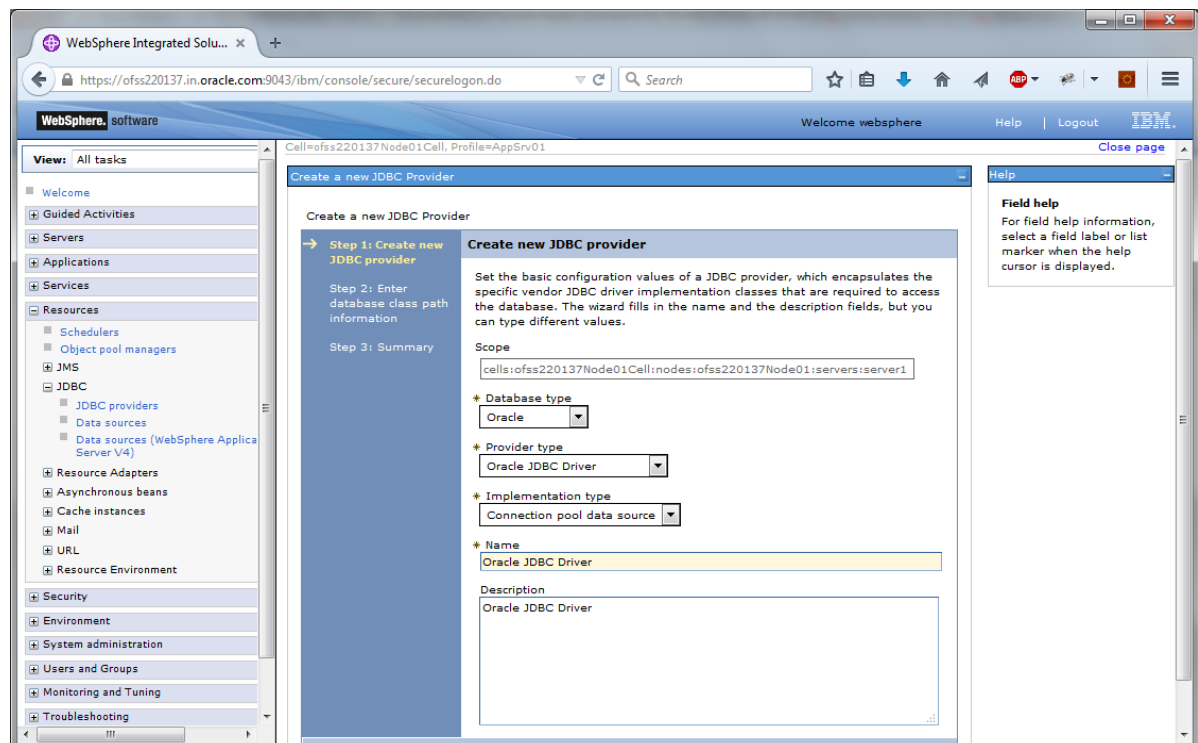
1. Login to the application server administration console.

2. Expand 'Resources > JDBC' and select 'JDBC Providers'.



3. Select 'Node' from the dropdown list.

Click New, The following screen is displayed:

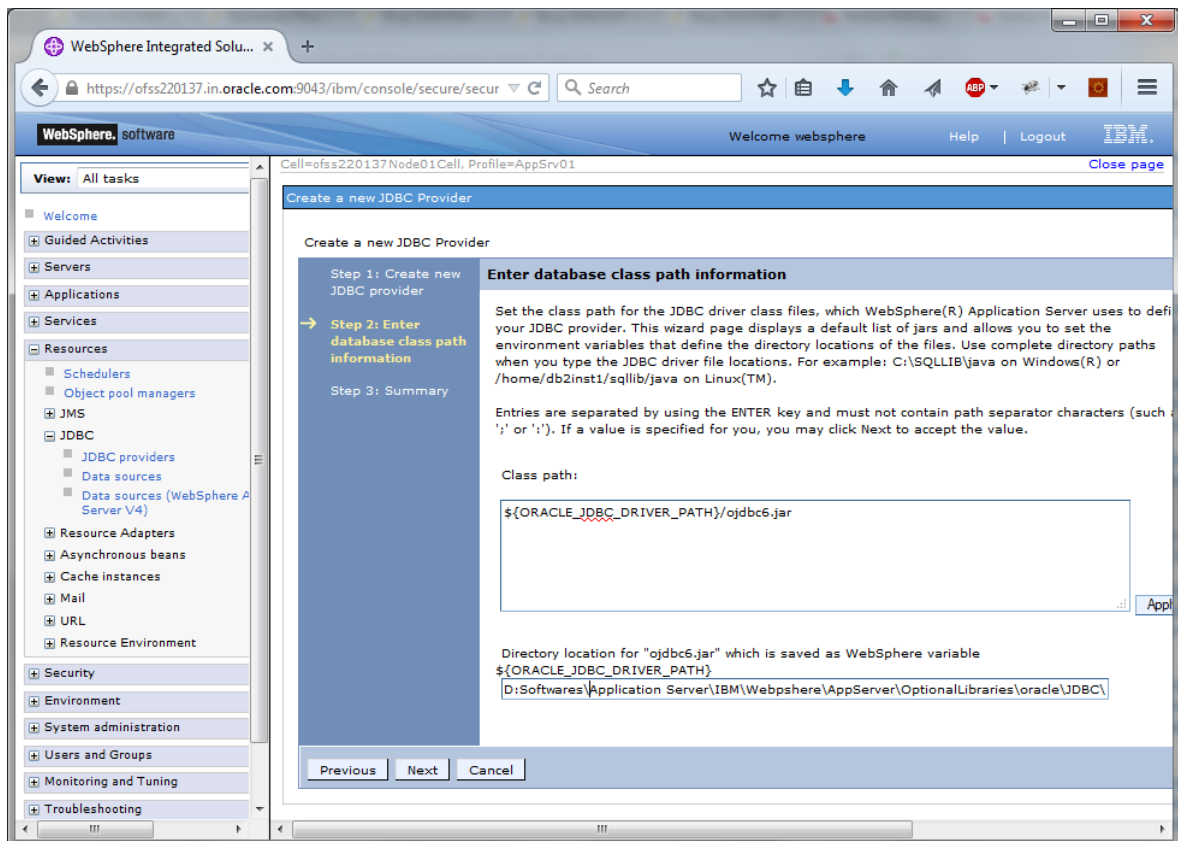


4. Specify the following details:

Database Type	Oracle
Provider Type	Oracle JDBC Driver
Implementation Type	Connection pool data source
Name	OBTR
Description	OBTR JDBC Driver

5. Click 'Next'.

The following screen is displayed:



6. Provide the location of ojdbc6.jar. Click 'Next'.

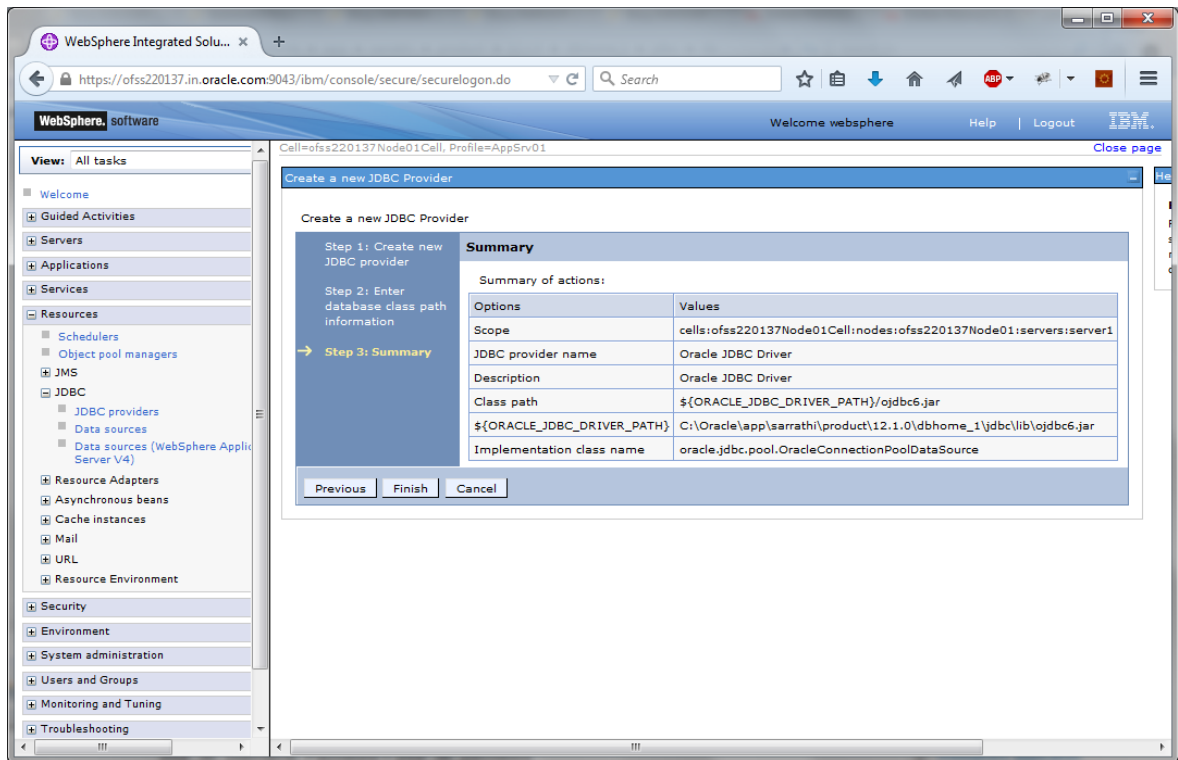
Note :If ojdbc6.jar is not available at your Websphere server, then copy them into your server (eg: path: /scratch/app/WAS9/lib) and run an export of the jar .

(Eg.in putty run a command

export ORACLE_JDBC_DRIVER_PATH=/scratch/app/WAS9/lib;)Then give the "Directory location for ojdbc6.jar which is saved as Websphere variable

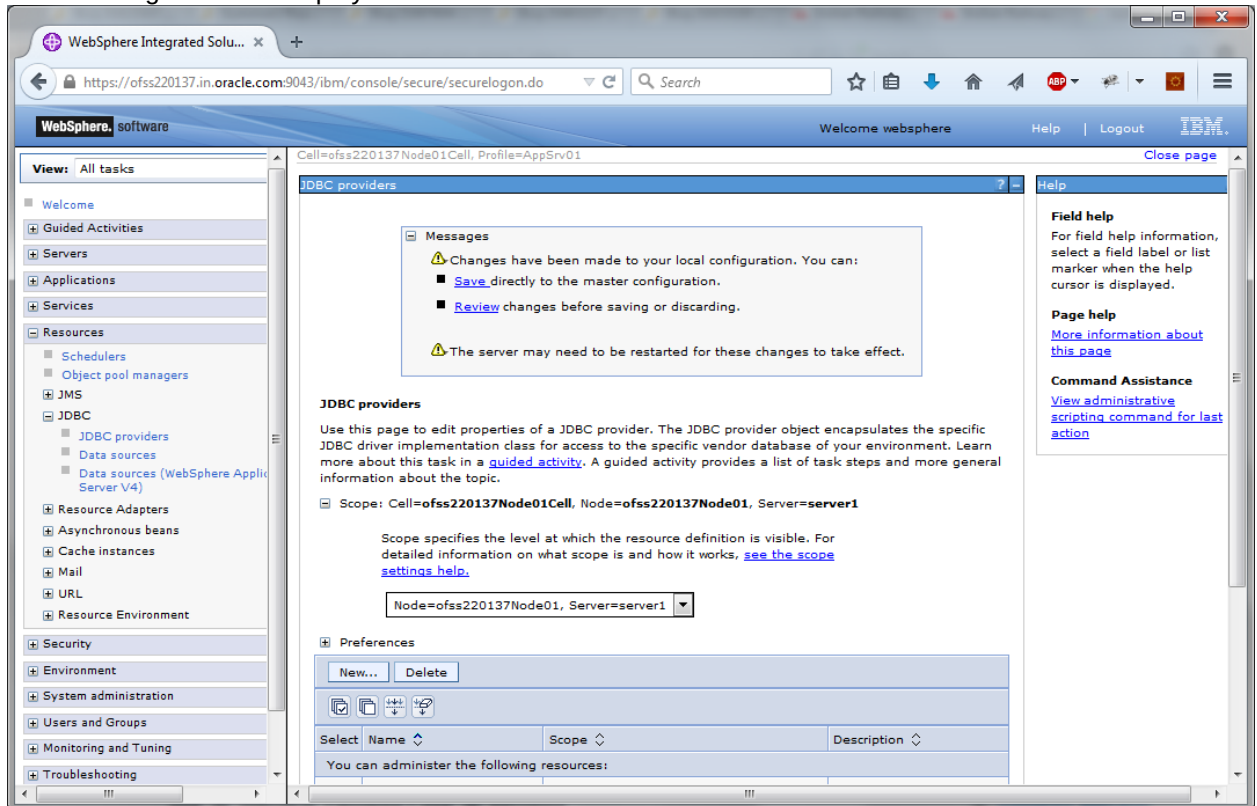
`${ORACLE JDBC DRIVER_PATH}`" as `/scratch/app/WAS9/lib`

The following screen is displayed.



7. Click 'Finish'.

The following screen is displayed.



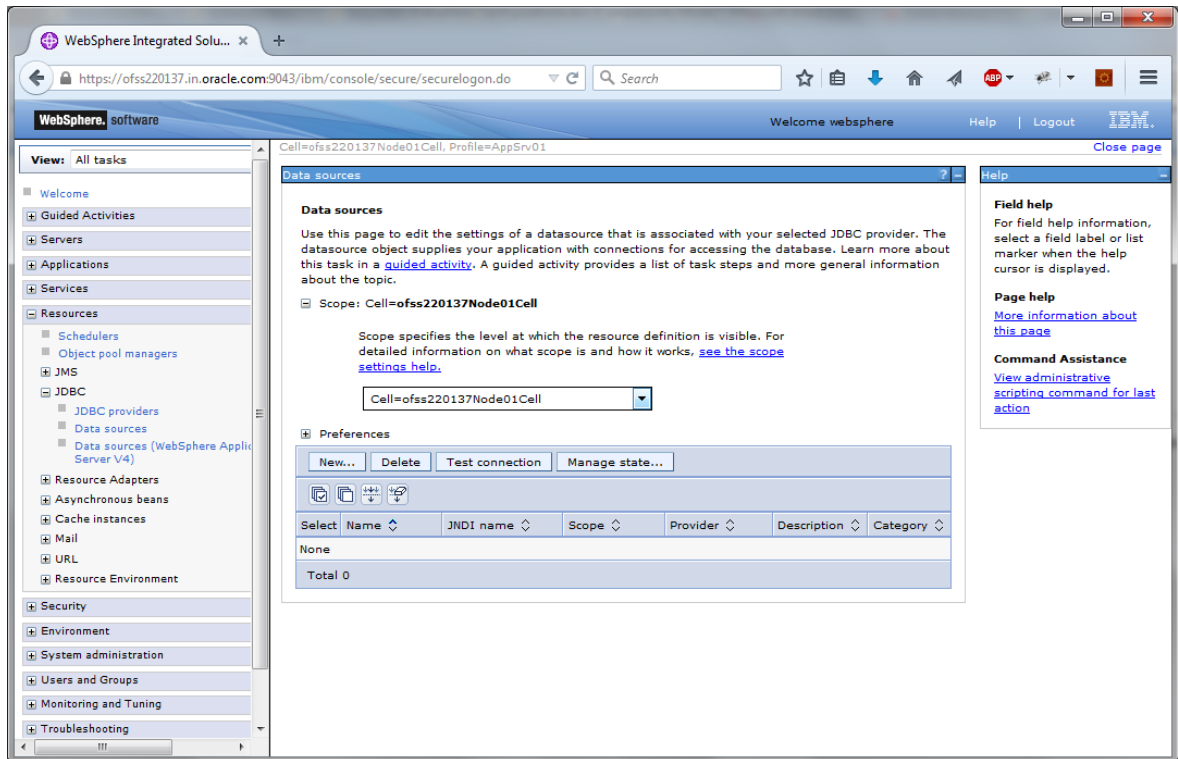
8. Click 'Save'.

3.3.3 Creating Non XA Data Source

Follow the steps given below:

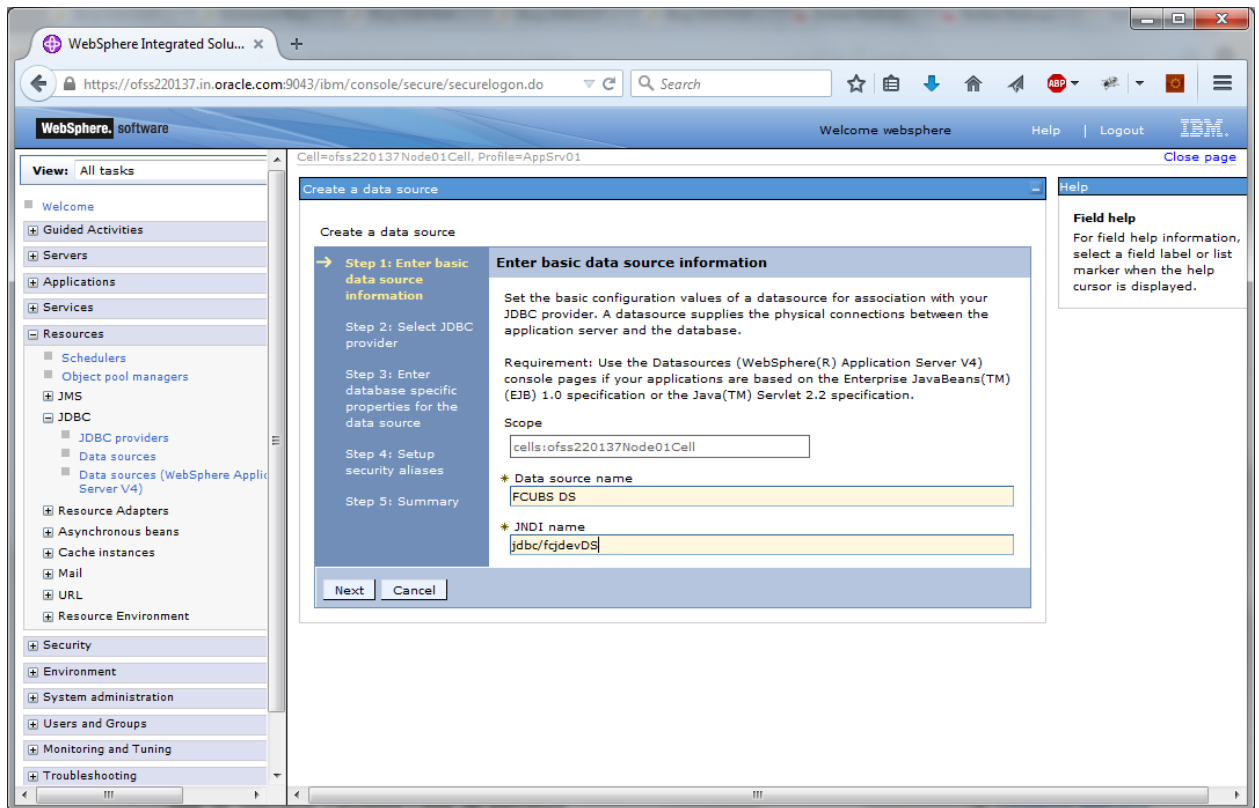
9. Login to the application server administration console.
10. Expand 'Resources > JDBC' and click 'Data sources'.

The following screen is displayed.



11. Select "Scope" from the drop-down list.

Click New, The following screen is displayed.

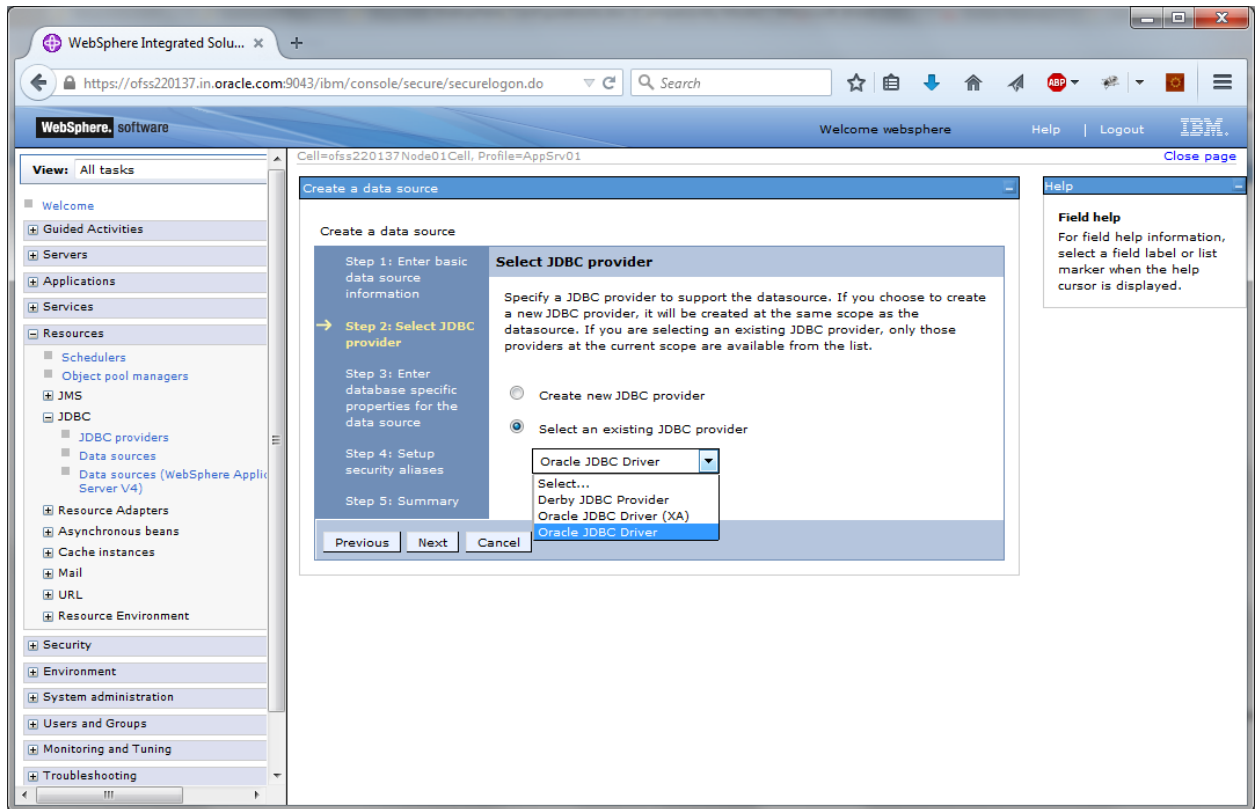


12. Specify the data source name as 'OBTR DS'.

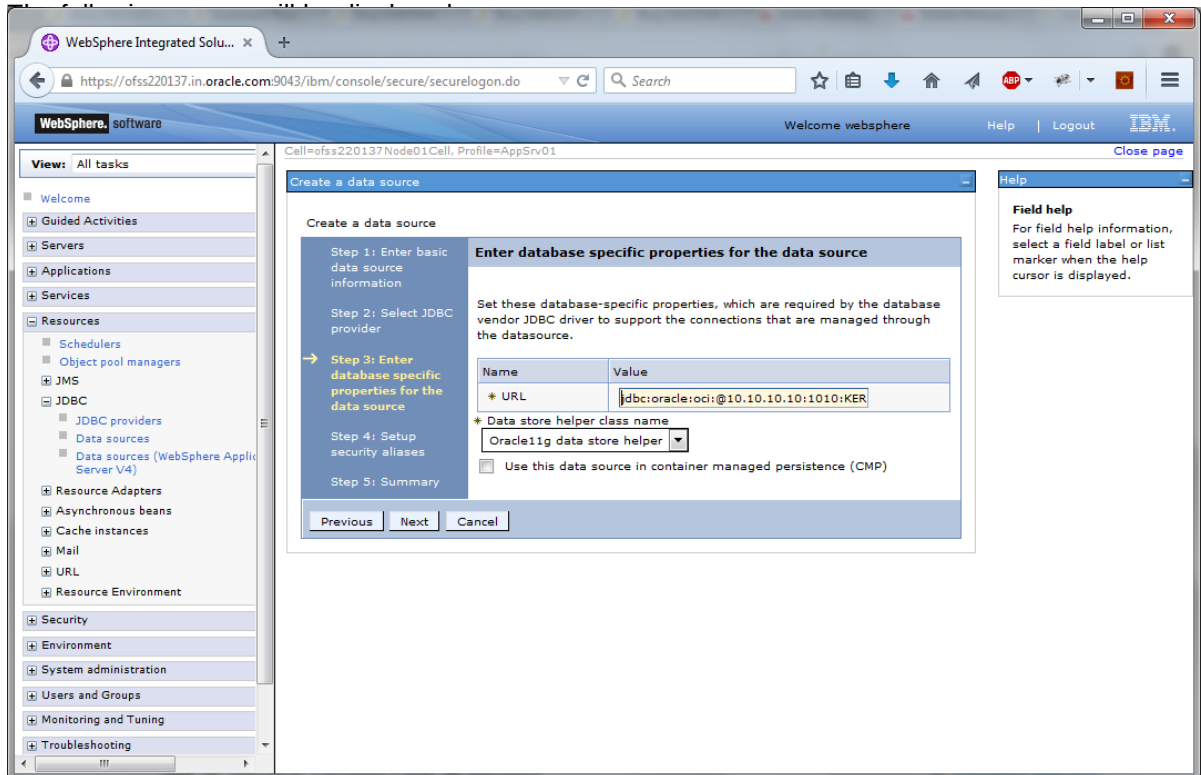
13. Specify the JNDI name as 'jdbc/fcdevDS'.

14. Click 'Next'.

The following screen is displayed.



15. Select the option 'Select an existing JDBC provider'. From the drop-down list, choose 'Oracle JDBC Driver' and click next.



16. Specify the URL of the Database

Uncheck "Use this data source in container managed persistence (CMP)"

Example

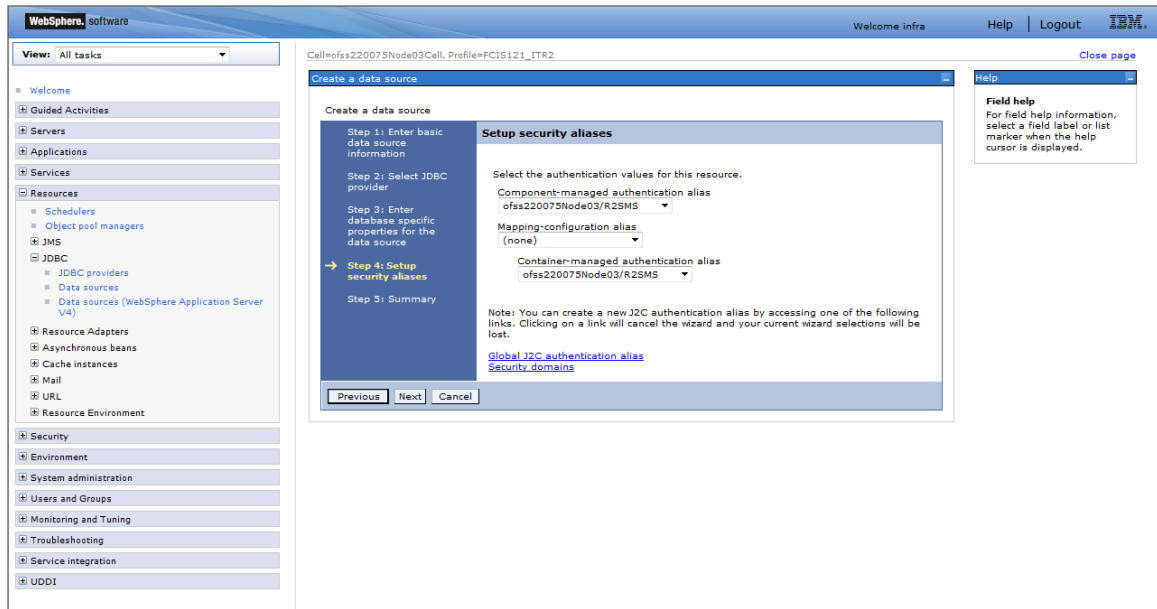
`jdbc:oracle:thin:@10.10.10.10:1010:KERDEV2`

Here, `10.10.10.10` is the *hostname* where the database is installed, `1010` the *port number* and `KERDEV2` the *instance name*.

17. Select the data store helper class as 'Oracle11g data store helper'.

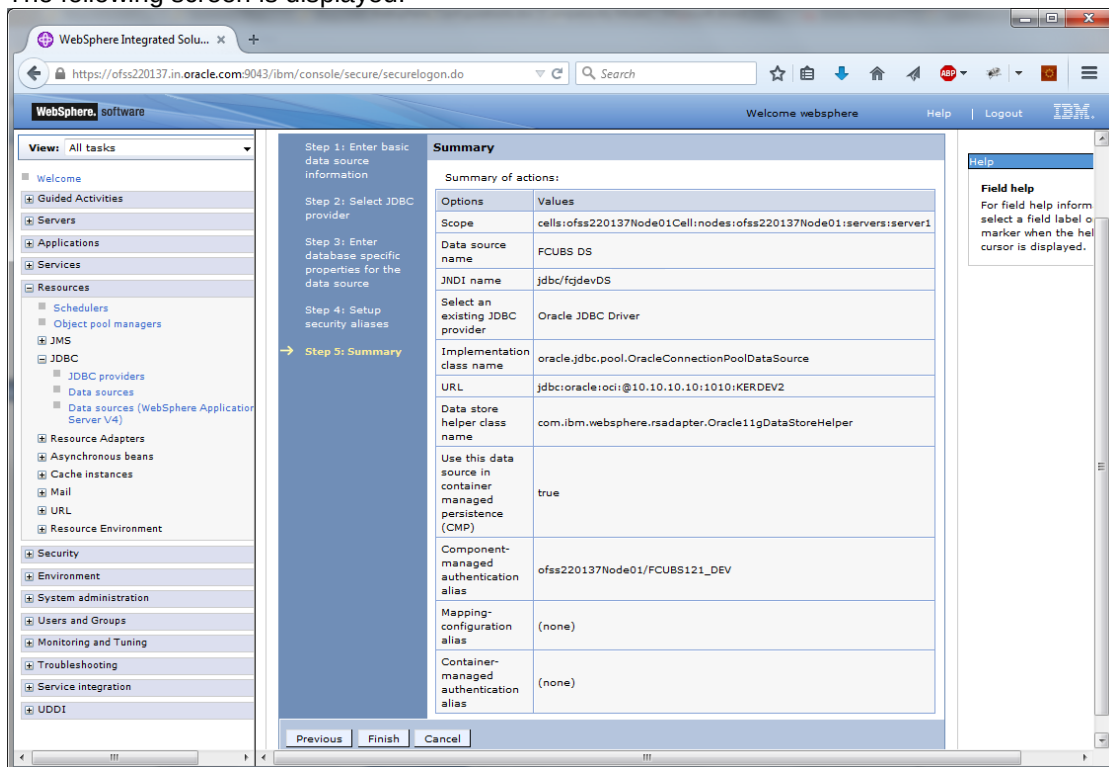
18. Click 'Next'. The following screen is displayed.

Select user alias from Component-managed authentication alias and Container-managed authentication alias dropdown.

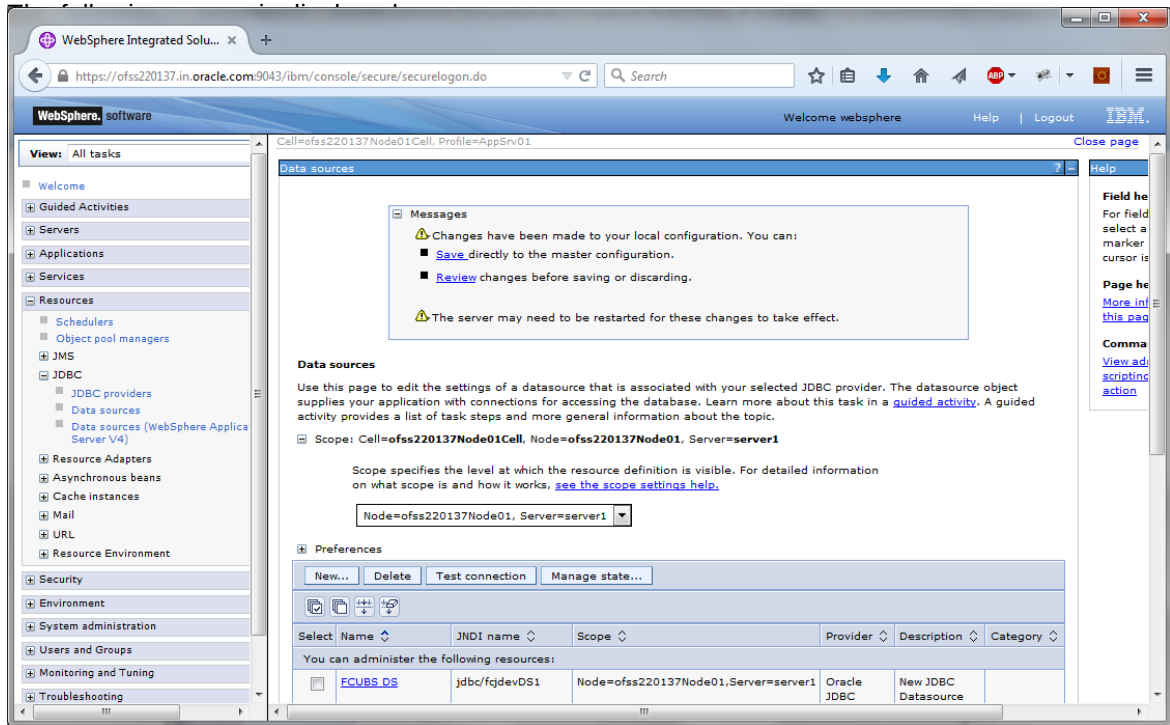


19. Click 'Next'.

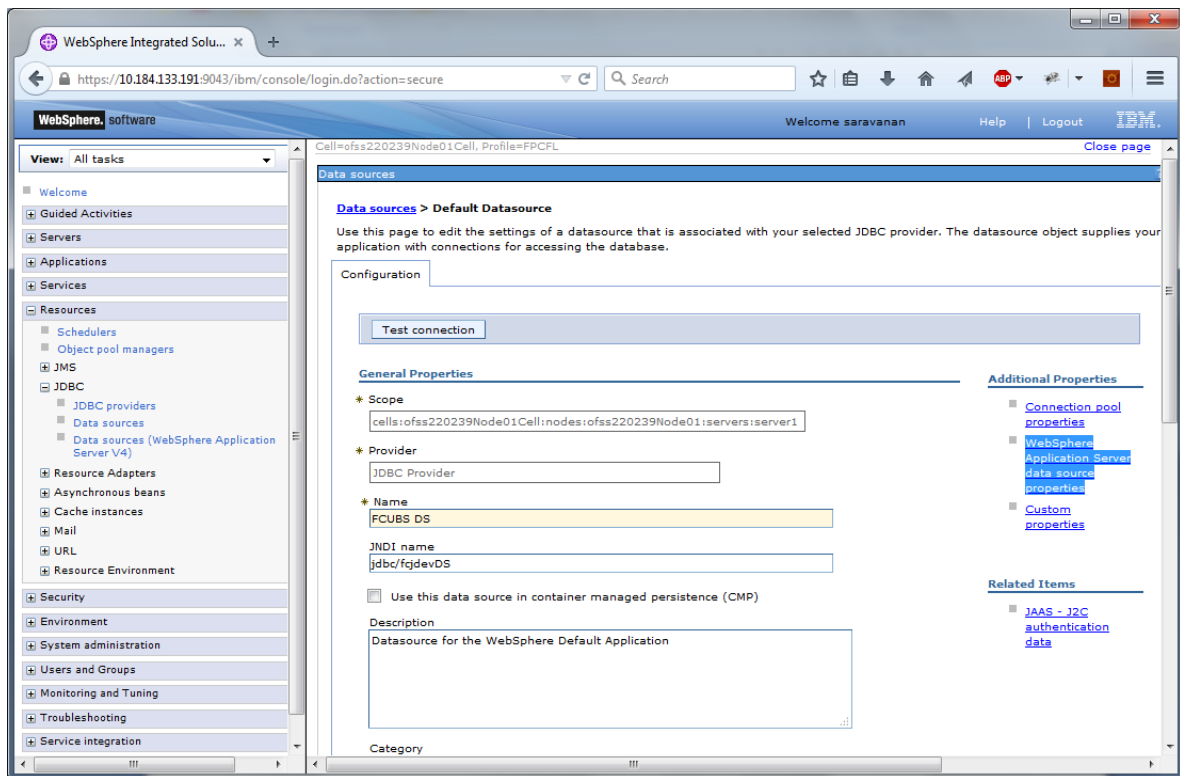
The following screen is displayed.



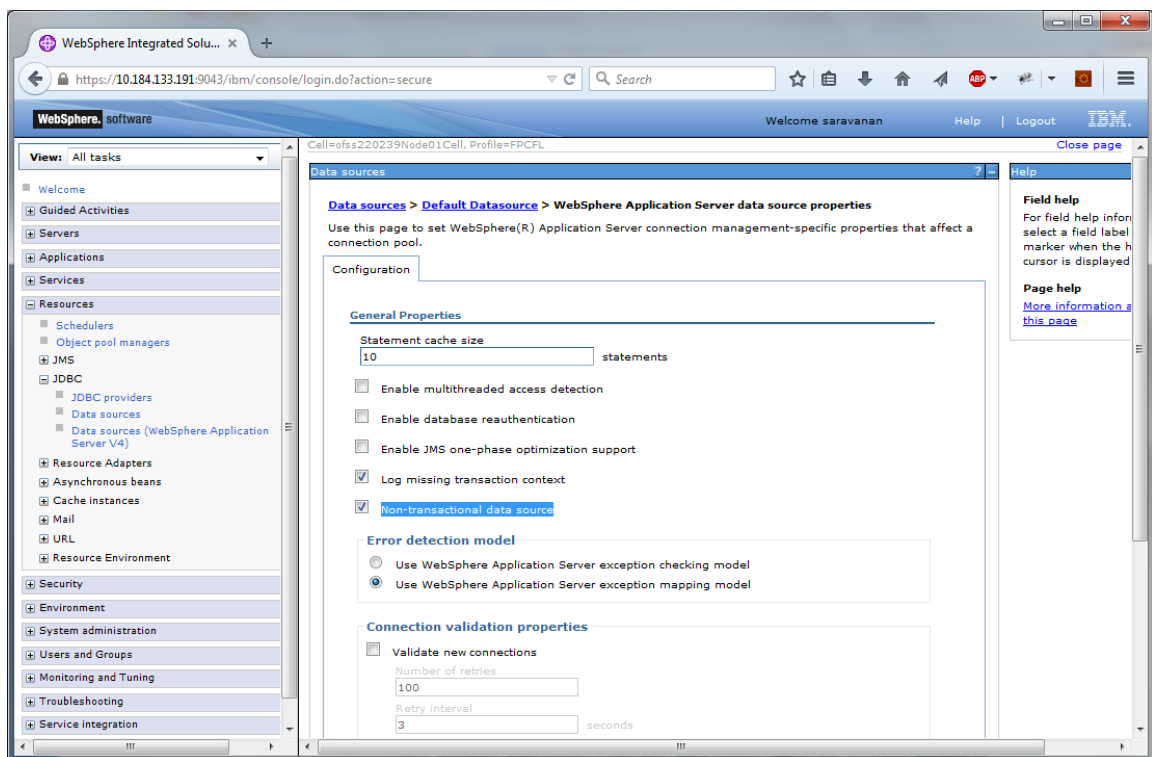
20. Click 'Finish'.



21. Click 'Save'.
22. Following steps needs to be followed only for Non-XA datasources
23. Click on the newly created Non-XA datasource, in our example "OBTR DS". The following screen is displayed



24. Make sure that the checkbox “Use this data source in container managed persistence (CMP)” is unchecked. Then click on the link “Webpsphere Application Server data source properties” on the right side.



25. Select the checkbox “Non-transactional data source”.

26. Click Apply button and Click Save link.



Note the following

- You need to create another data source for Oracle OBTR with the JNDI name '<Non-XA OBTR HOST JNDI name>_ASYNC'. For example, if the Oracle OBTR HOST Non XA data source JNDI name is 'jdbc/fcjdevDS', then you need to create another data source for OBTR 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 OBTR 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 OBTR HOST Non XA data source JNDI name is 'jdbc/fcjdevDS', then you need to create another data source for OBTR with the JNDI name 'jdbc/fcjdevDS_EL'. Ensure that the check box “Non-transactional data source” is unchecked 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 -

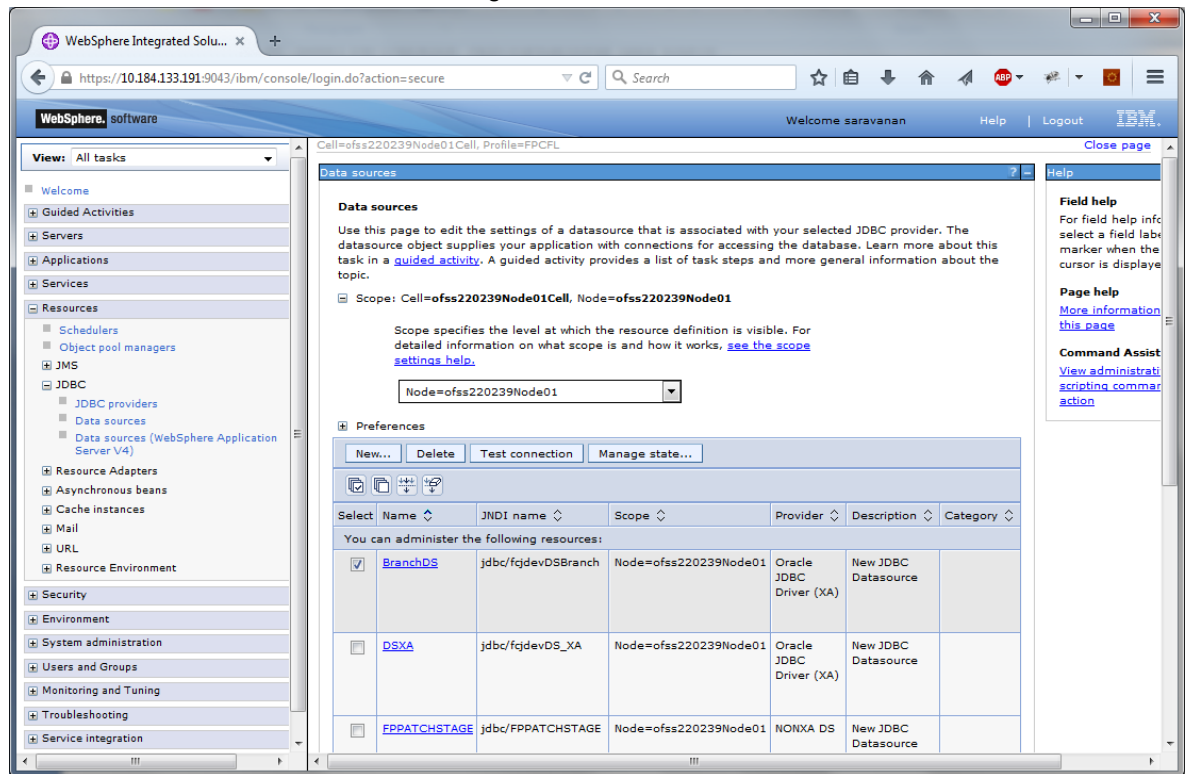
Purpose	Datasource Name	JNDI Name
OBTR	OBTR Data source	jdbc/fcjdevDS
SMS	SMS Datasource	jdbc/fcjdevDSSMS
Gateway	FLEXTEST.WORLD	FLEXTEST.WORLD
Async data source	OBTR DS_ASYNC	jdbc/fcjdevDS_ASYNC
Scheduler	Scheduler_Datasource	jdbc/fcjSchedulerDS

•

3.3.4 Testing Data Source

Follow the steps given below:

1. Select the data source as shown in the figure.



2. Click 'Test connection' button.

On successful creation, the following message is displayed.

WebSphere Integrated Solu... x

<https://10.184.133.191:9043/ibm/console/login.do?action=secure>

Search

WebSphere, software

Welcome saravanan Help Logout IBM

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
 - Schedulers
 - Object pool managers
 - JMS
 - JDBC
 - JDBC providers
 - Data sources
 - Data sources (WebSphere Application Server V4)
 - Resource Adapters
 - Asynchronous beans
 - Cache instances
 - Mail
 - URL
 - Resource Environment
- Security
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration

Cell=ofss220239Node01Cell, Profile=FPCFL

Close page

Data sources

Messages

The test connection operation for data source BranchDS on server server1 at node ofss220239Node01 was successful.

Data sources

Use this page to edit the settings of a datasource that is associated with your selected JDBC provider. The datasource object supplies your application with connections for accessing the database. Learn more about this task in a [guided activity](#). A guided activity provides a list of task steps and more general information about the topic.

Scope: Cell=ofss220239Node01Cell, Node=ofss220239Node01

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, [see the scope settings help](#).

Node=ofss220239Node01

Preferences

New... Delete Test connection Manage state...

Select Name JNDI name Scope Provider Description Category

You can administer the following resources:

☐	BranchDS	jdbc/fjdevDSBranch	Node=ofss220239Node01	Oracle JDBC Driver (XA)	New JDBC Datasource	
☐	DSXA	jdbc/fjdevDS_XA	Node=ofss220239Node01	Oracle	New JDBC	

Field help

For field help info select a field label marker when the cursor is displayed

Page help

[More information this page](#)

Command Assist

[View administrative scripting command action](#)

3-18

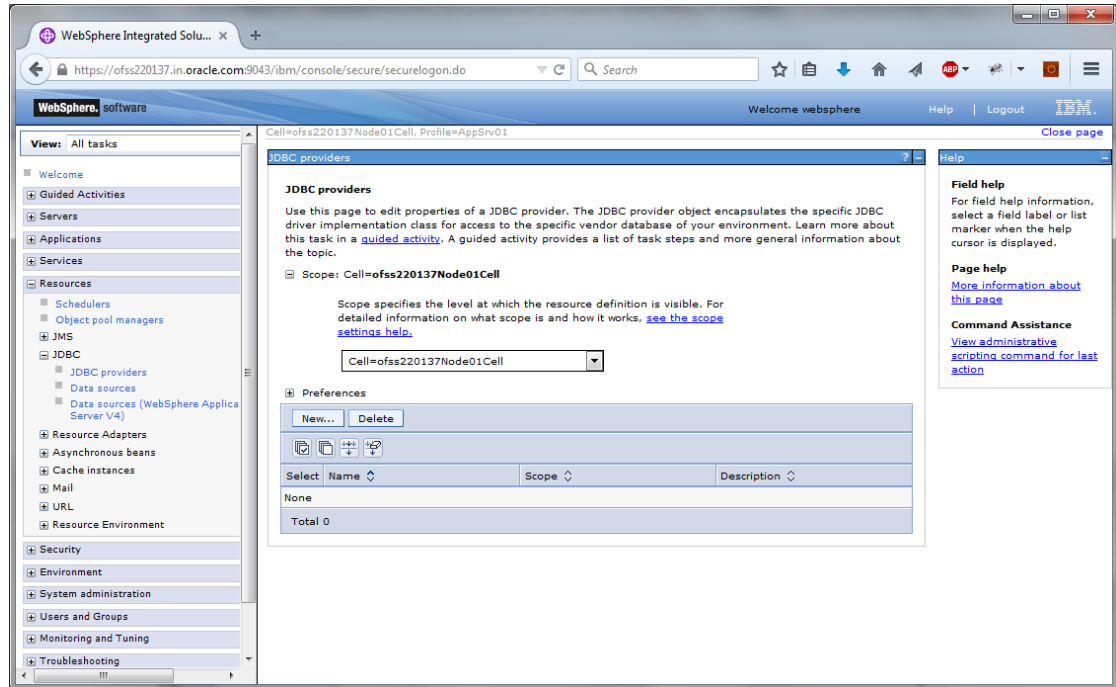
ORACLE®

3.3.5 JDBC Provider for XA Data Source

Follow the steps given below:

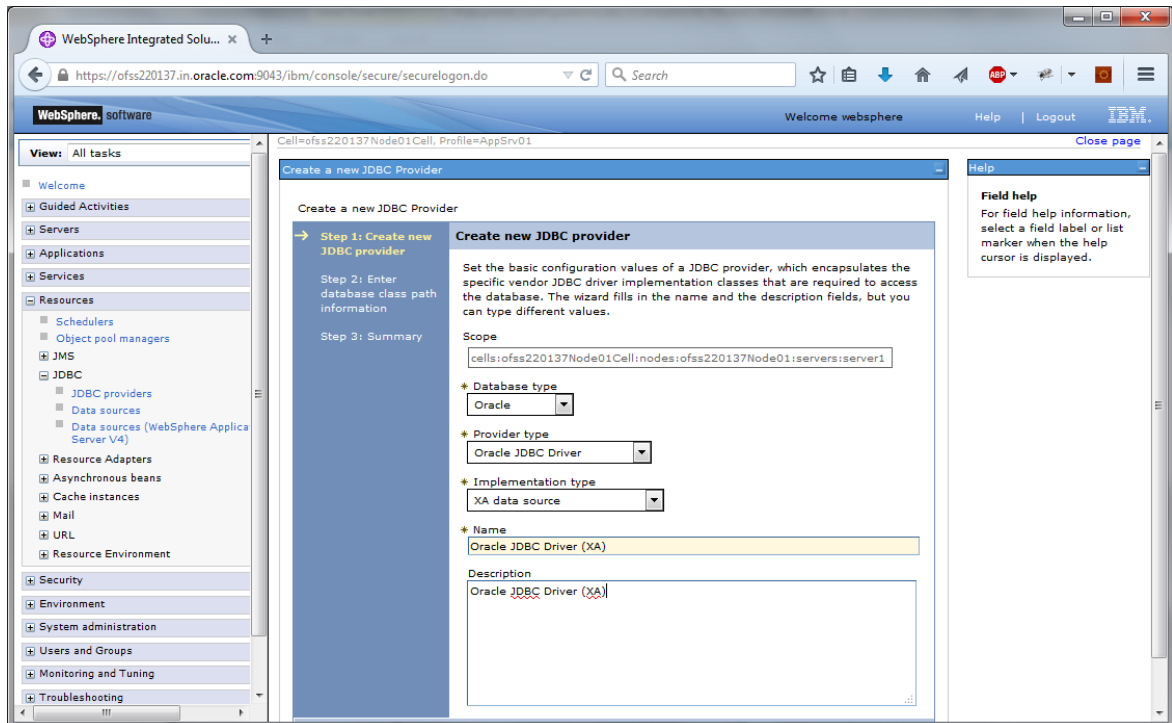
1. Login to the application server administration console.
2. Expand 'Resources > JDBC' and click 'JDBC Providers'.

The following screen is displayed.



3. Select 'Node' from the drop-down list and click 'New' button.

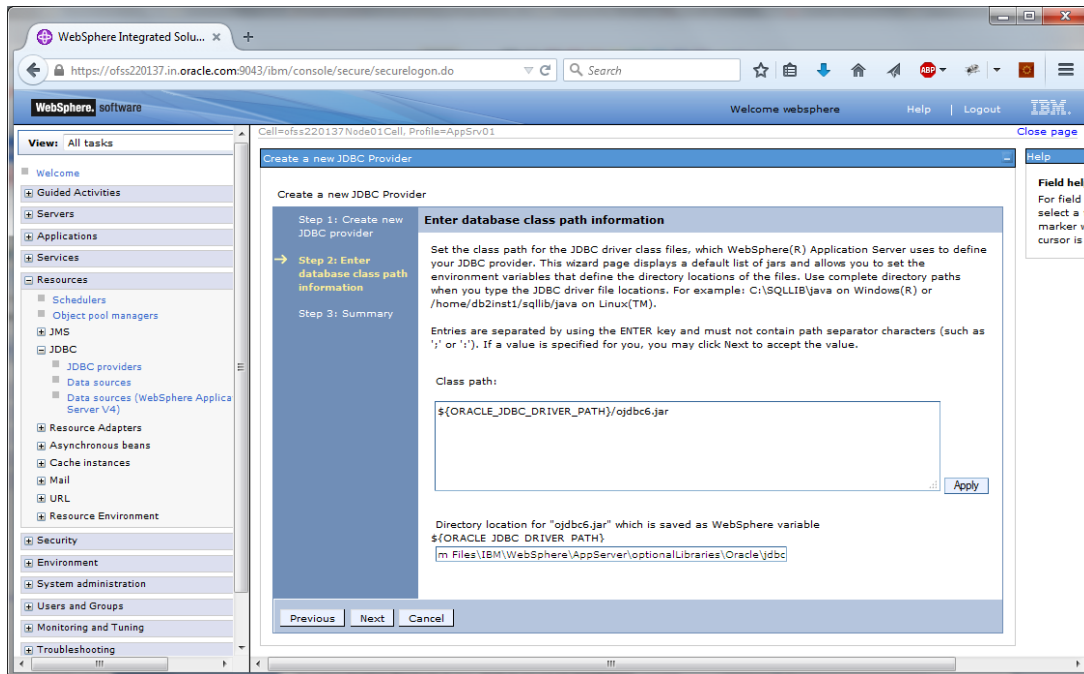
The following message is displayed.



4. Specify the following details:

Database Type	Oracle
Provider Type	Oracle JDBC Driver
Implementation Type	XA data source
Name	OBTR Oracle JDBC Driver (XA)
Description	OBTR Oracle JDBC Driver (XA)

Click next, the following message is displayed.



5. Specify the location of ojdbc6.jar and click next.

Note :If ojdbc6.jar is not available at your Websphere server, then copy them into your server (path: /scratch/app/WAS9/lib) and run an export of the jar .

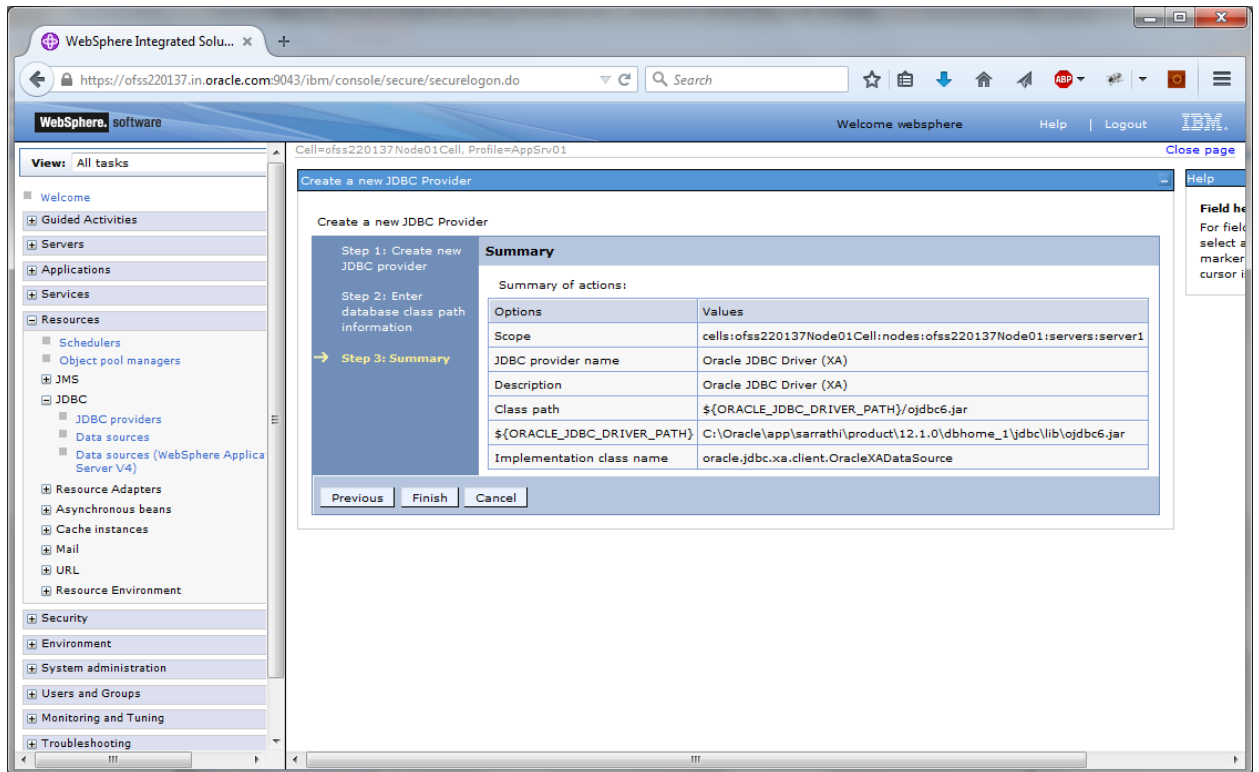
(Eg.in putty run a command

```
export ORACLE_JDBC_DRIVER_PATH=/scratch/app/WAS9/lib;)
```

Then give the “Directory location for ojdbc6.jar which is saved as Websphere variable

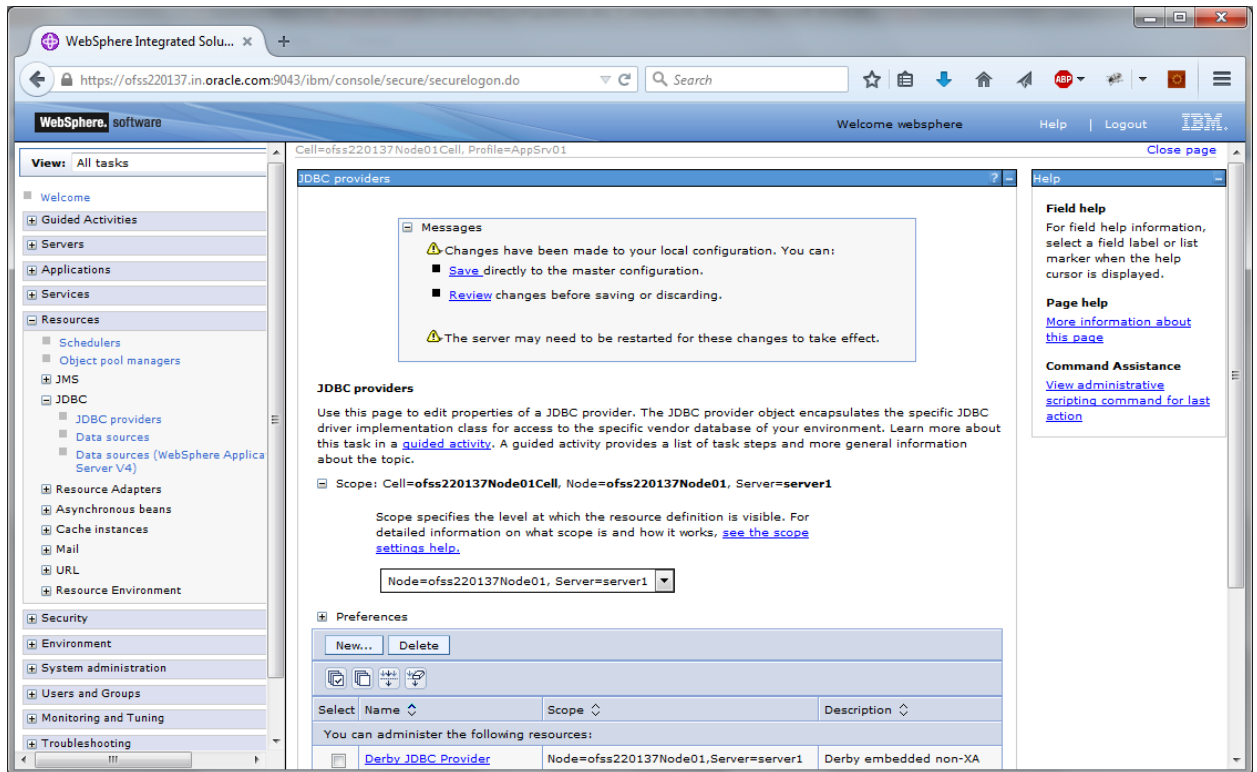
6. \${ORACLE JDBC DRIVER PATH}” as /scratch/app/WAS9/lib

The following screen is displayed.



7. Click 'Finish'.

The following screen is displayed.



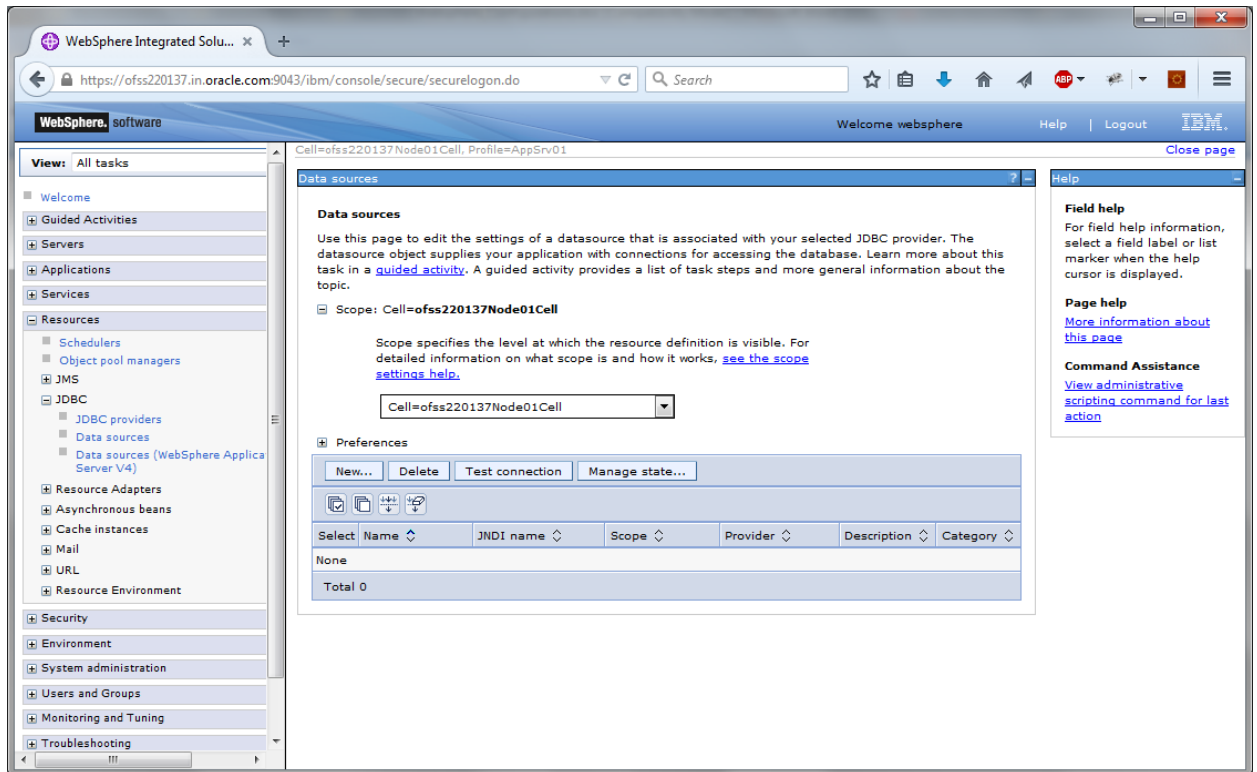
8. Click 'Save'.

3.3.6 Creating XA Data Source

Follow the steps given below:

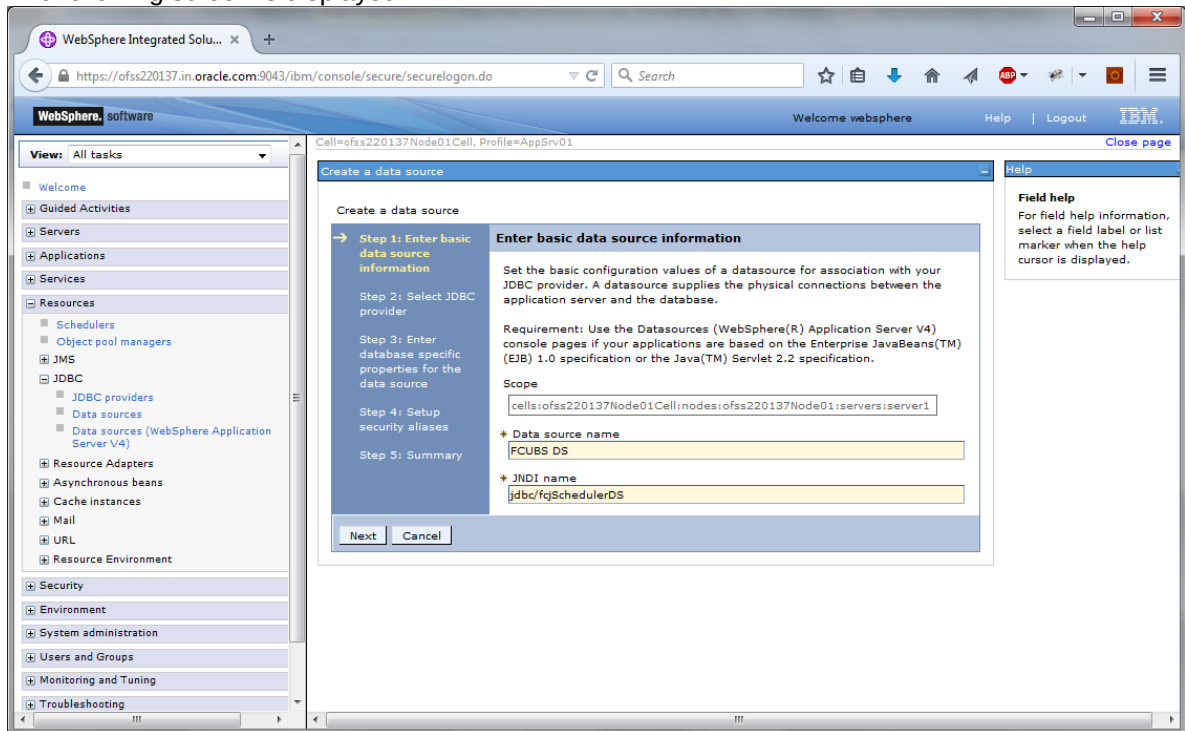
1. Login to the application server administration console.
2. Expand 'Resources > JDBC' and click 'Data sources'.

The following screen is displayed.



3. Select 'Scope' from the dropdown list and click 'New' button.

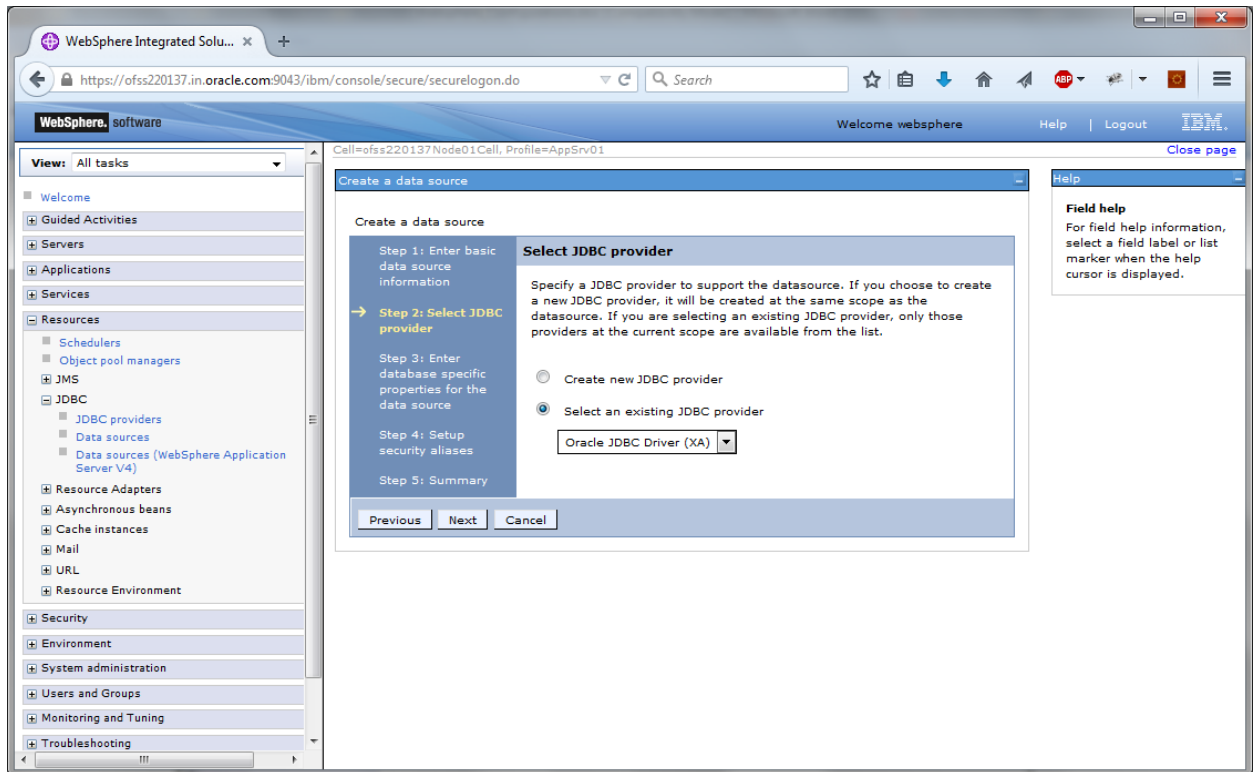
The following screen is displayed.



4. Specify the following details:

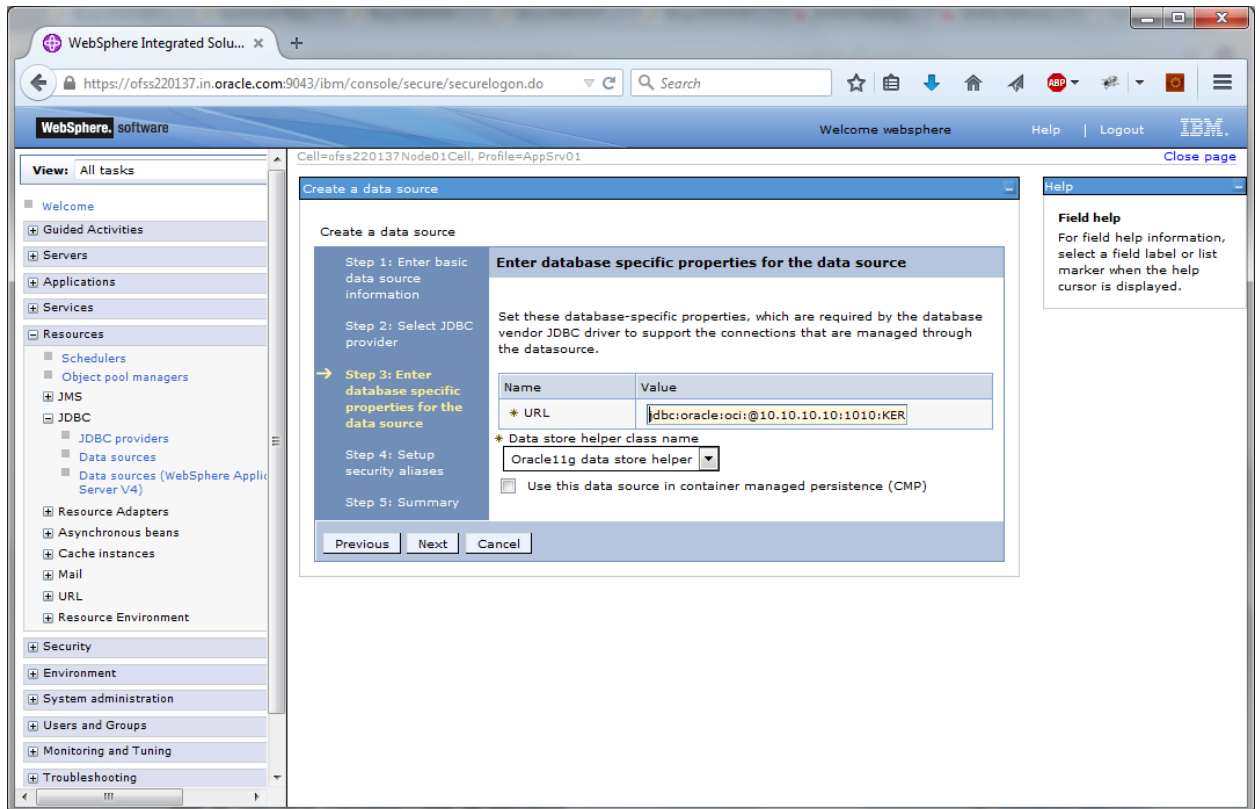
Data source name	OBTR Scheduler Data source
JNDI Name	jdbc/fcjSchedulerDS

Click next, the following screen is displayed.



5. Select the option 'Select an existing JDBC provider' and choose 'OBTR Oracle JDBC Deriver (XA)' from the drop-down list and click next.

The following screen is displayed.



6. Specify the URL of the Database

Uncheck "Use this data source in container managed persistence (CMP)"

Example

jdbc:oracle:thin:@10.10.10.10:1010:KERDEV2

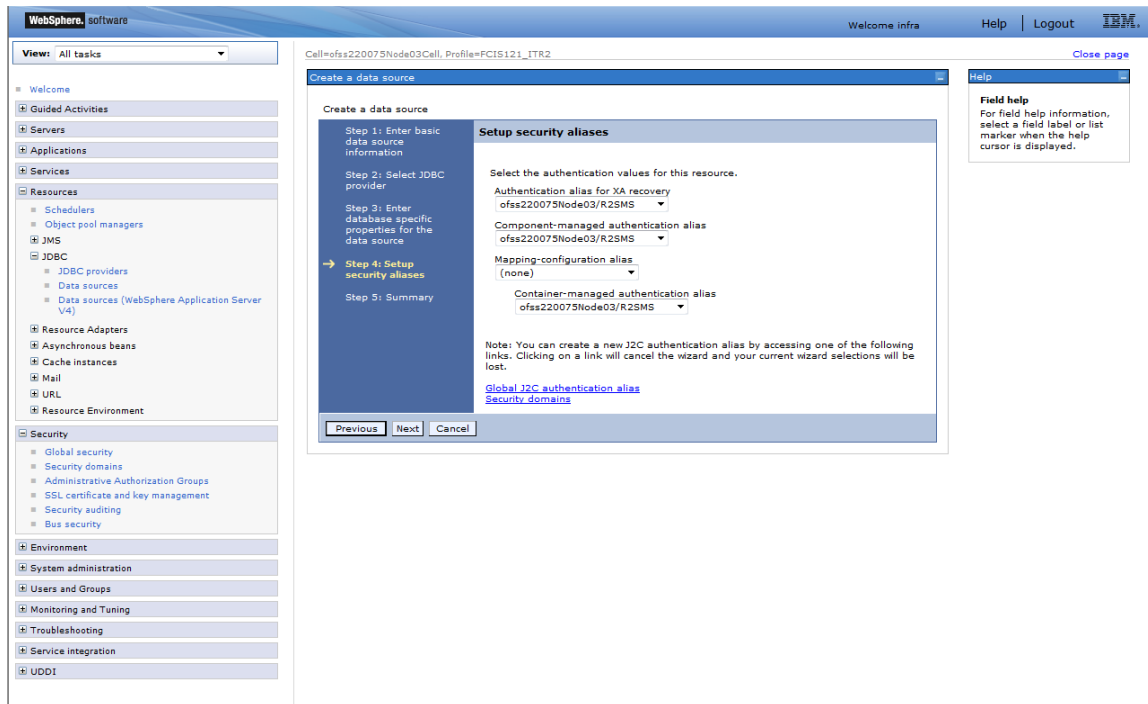
Here, 10.10.10.10 is the *hostname* where the database is installed, 1010 is the *port number*, KERDEV2 is the *instance name*.

7. Select the 'Data store helper class' as 'Oracle11g data store helper'.

8. Click 'Next'.

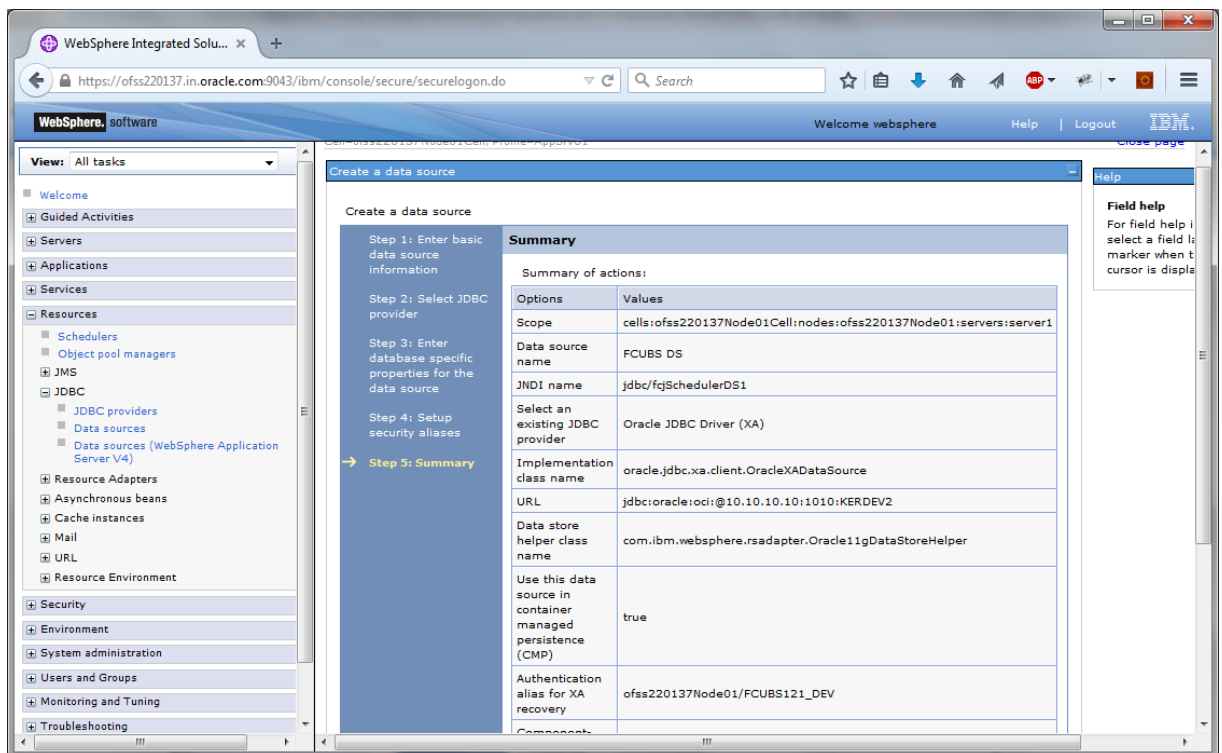
The following screen is displayed.

Select user alias from Authentication alias for XA Recovery, Component-managed authentication alias and Container-managed authentication alias dropdown.

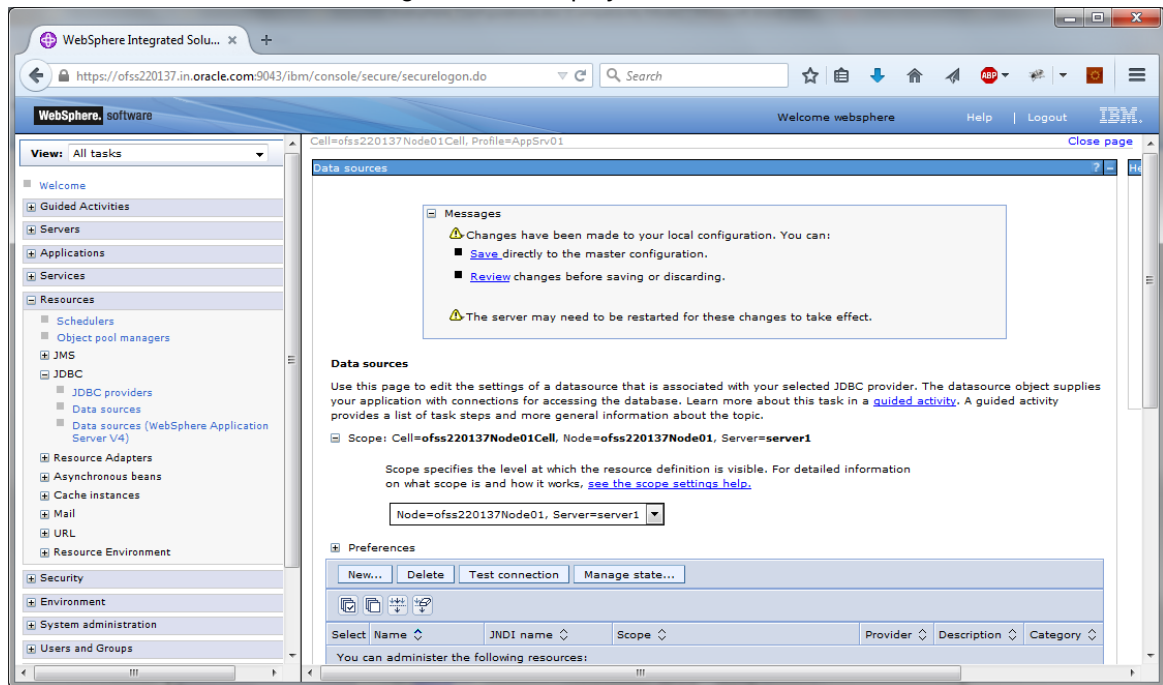


9. Click 'Next'.

The following screen is displayed.



10. Click 'Finish', the following screen is displayed.



11. Click 'Save'.

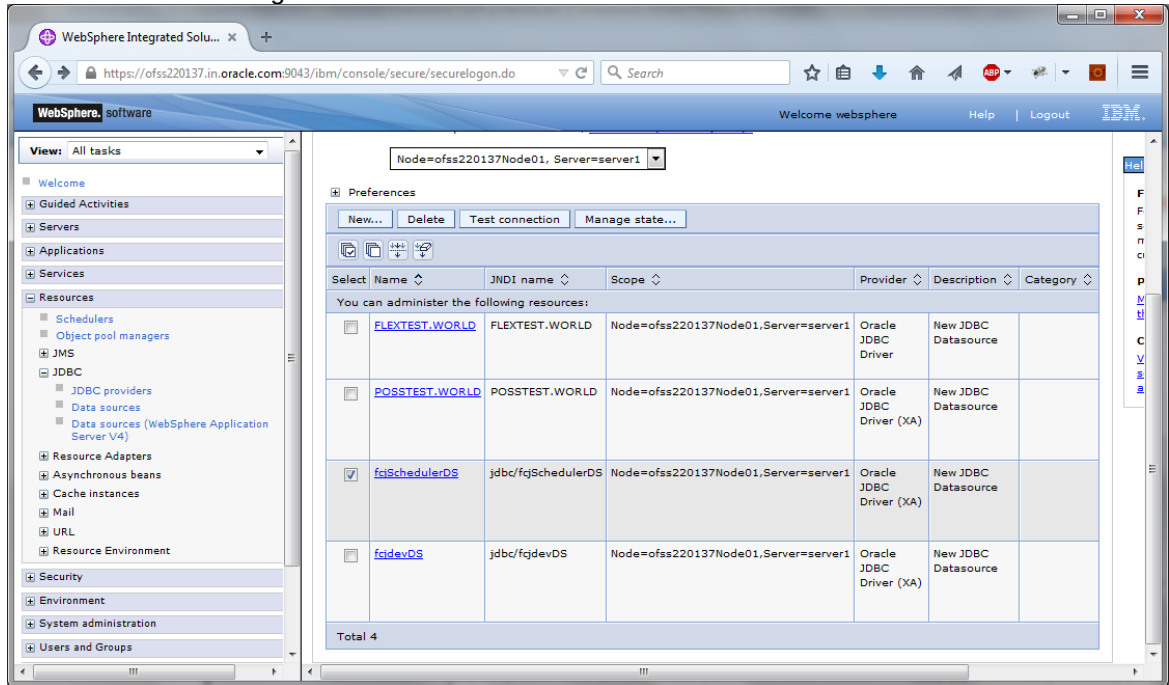
The following are the list of XA datasources that can be created depending on the requirement. Please refer to the document Resources_To_Be_Created.docx for more information-

Purpose	Datasource Name	JNDI Name
Scheduler	Scheduler_XA	jdbc/fcjSchedulerDS
OBTR	OBTR_DS_XA	jdbc/fcjdevDS_XA
Branch	OBTR DSBranch	jdbc/fcjdevDSBranch

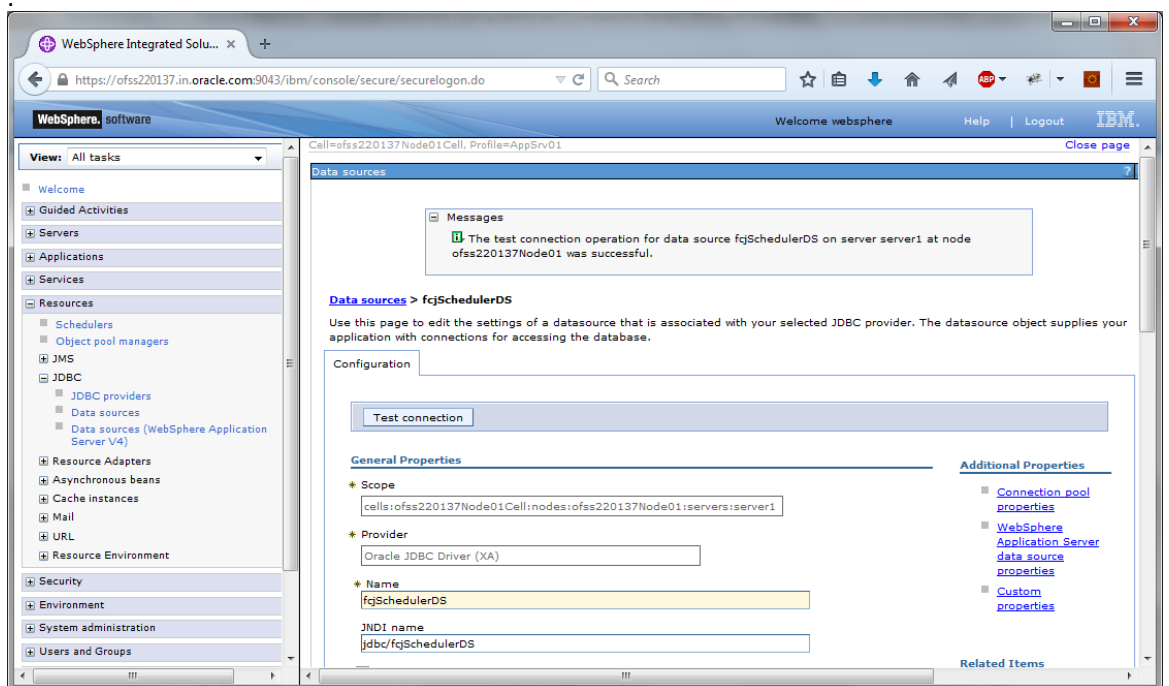
3.3.7 Testing Data Source

Follow the steps given below:

Select data source as given below.



Click 'Test connection' button. The following screen is displayed on successful creation



3.4 Creating JMS Resources

3.4.1 Creating Queue Connection Factory

Follow the steps given below:

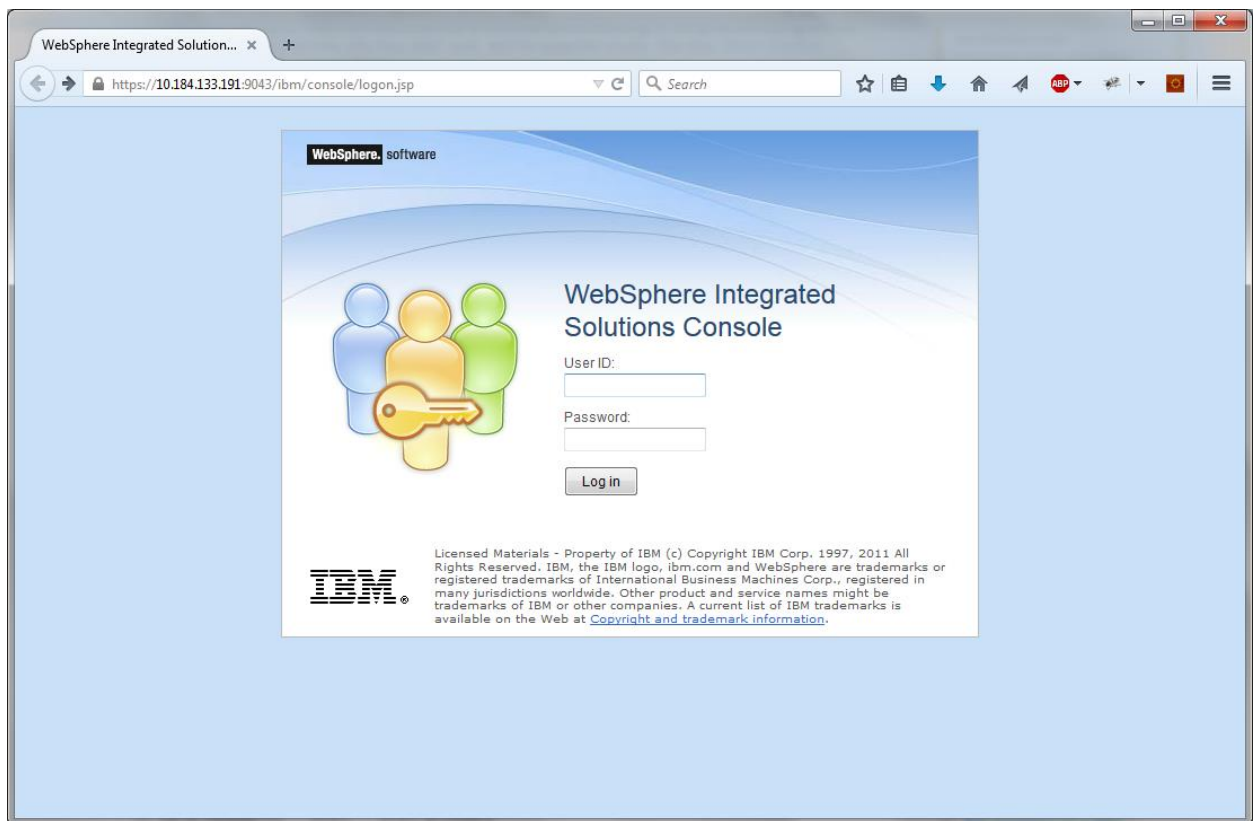
1. Start the administrative console of Websphere application server. Open an internet browser and enter the Websphere admin console URL.

`http://{Host}:{Port}/console`

Eg: `https://10.10.10.10:1010/console`

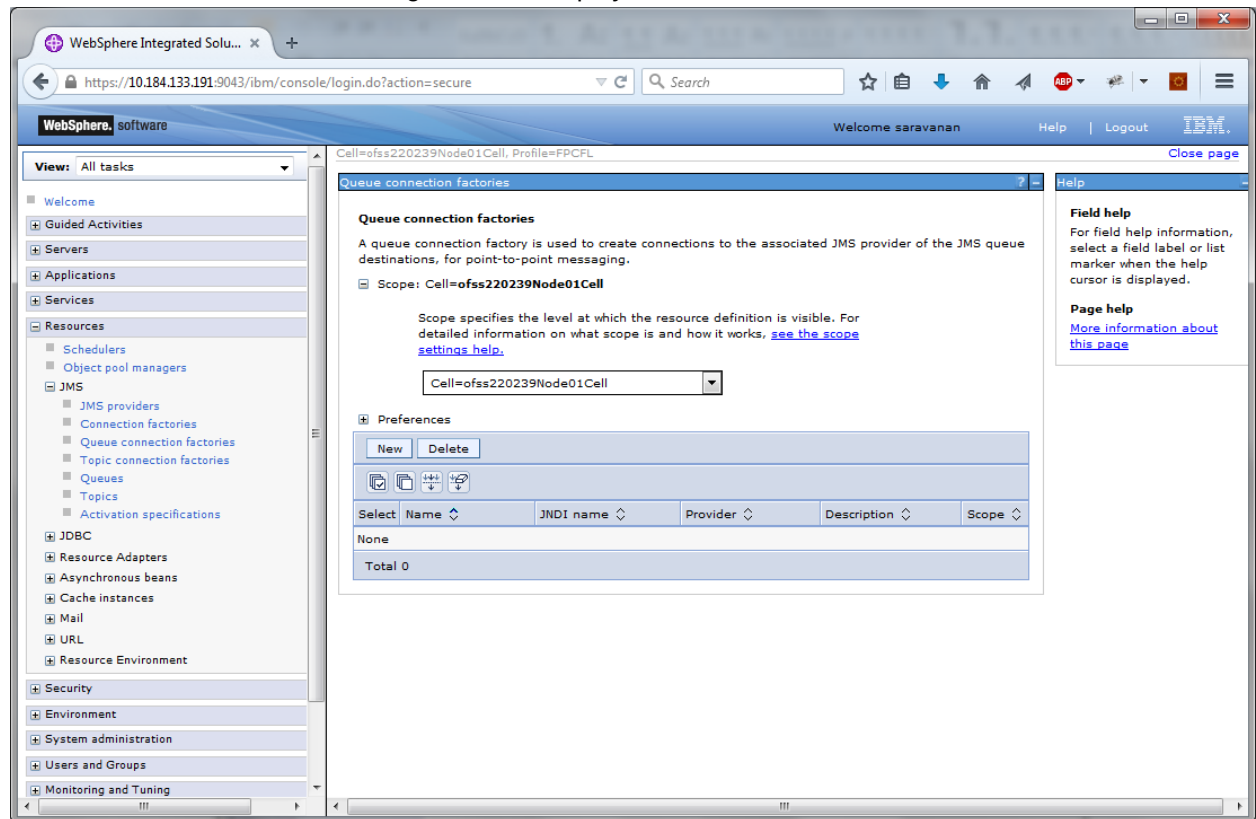
In this example, 10.10.10.10 is the machine IP address on which Websphere is running.

The following screen is displayed:



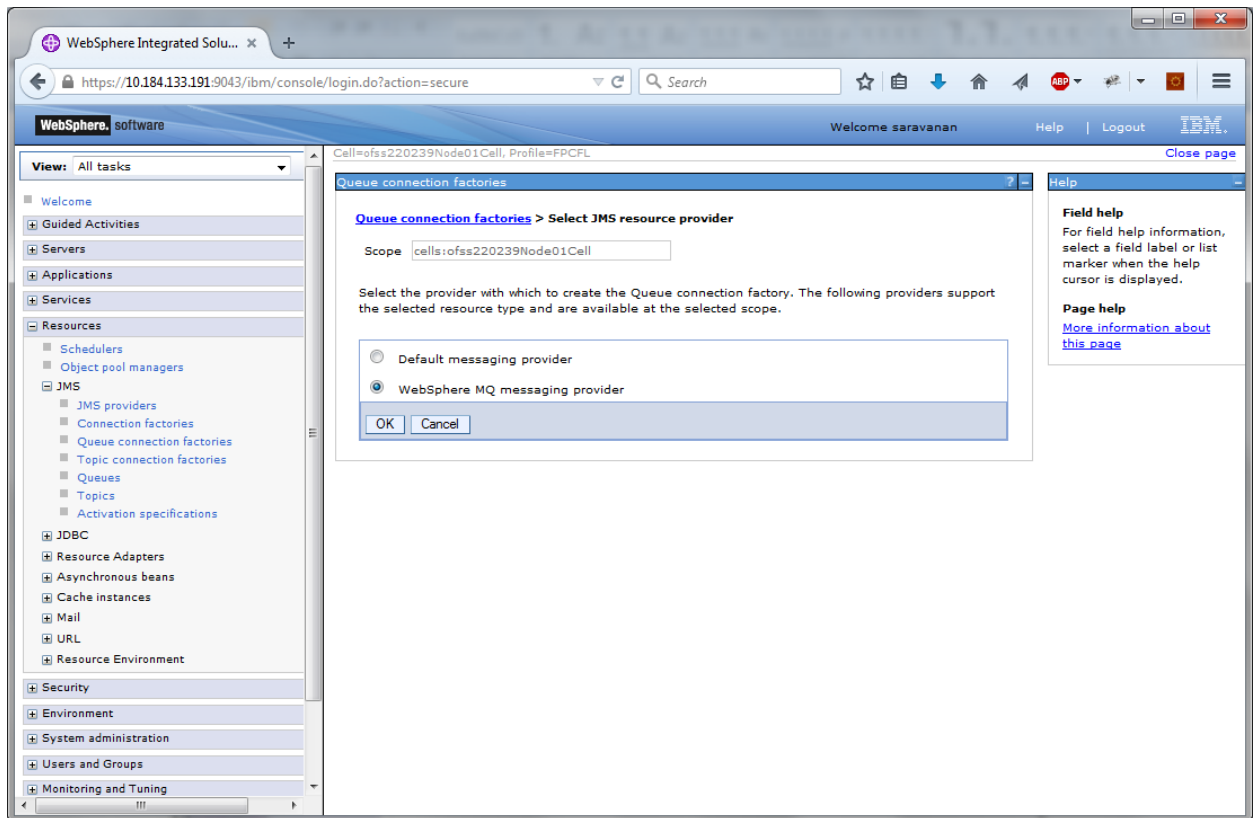
2. Specify the Websphere administrator username and password.
3. Click 'Log In'.

4. Navigate to Websphere Home page .Expand 'Resources' and select 'JMS'. Click 'Queue connection factories'. The following screen is displayed.



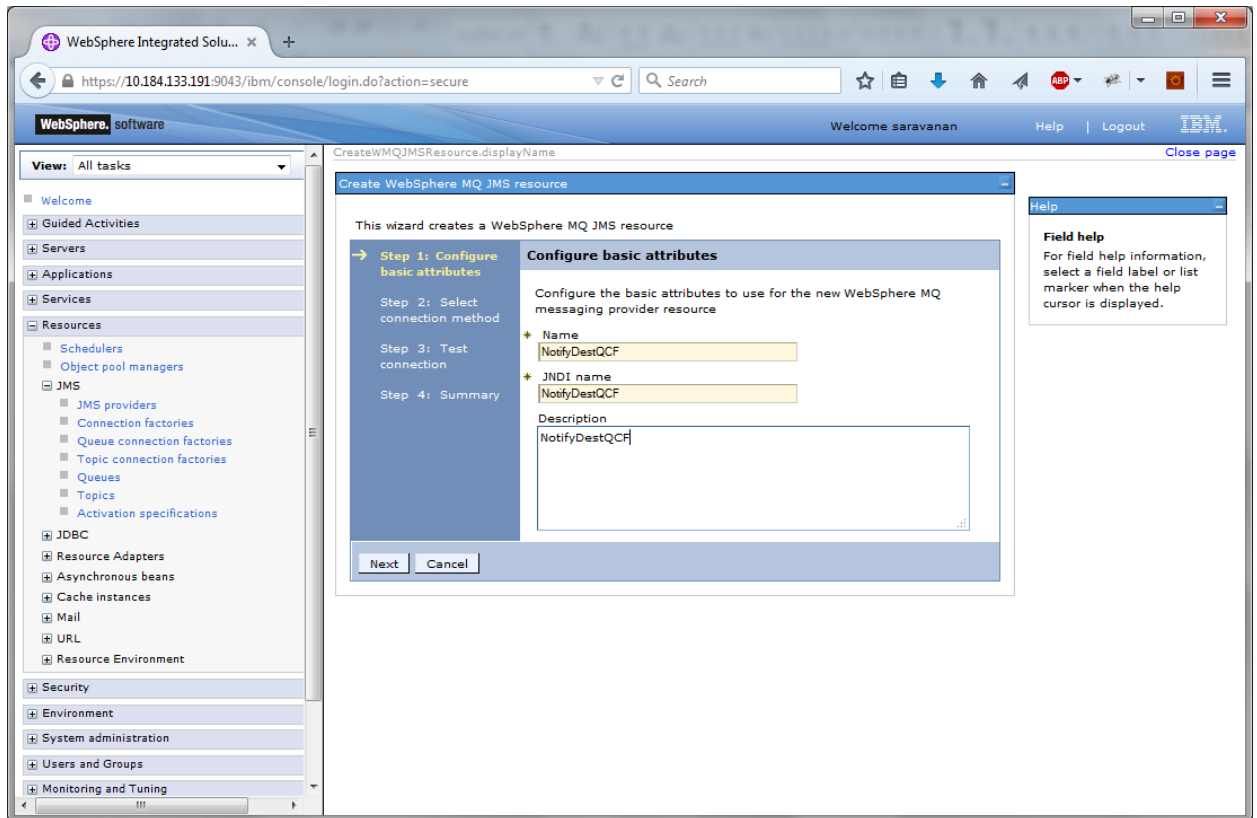
5. Select 'Scope' from the drop down list and click 'New' button.

The following screen is displayed.



6. Select 'WebSphere MQ messaging provider' and click 'OK'.

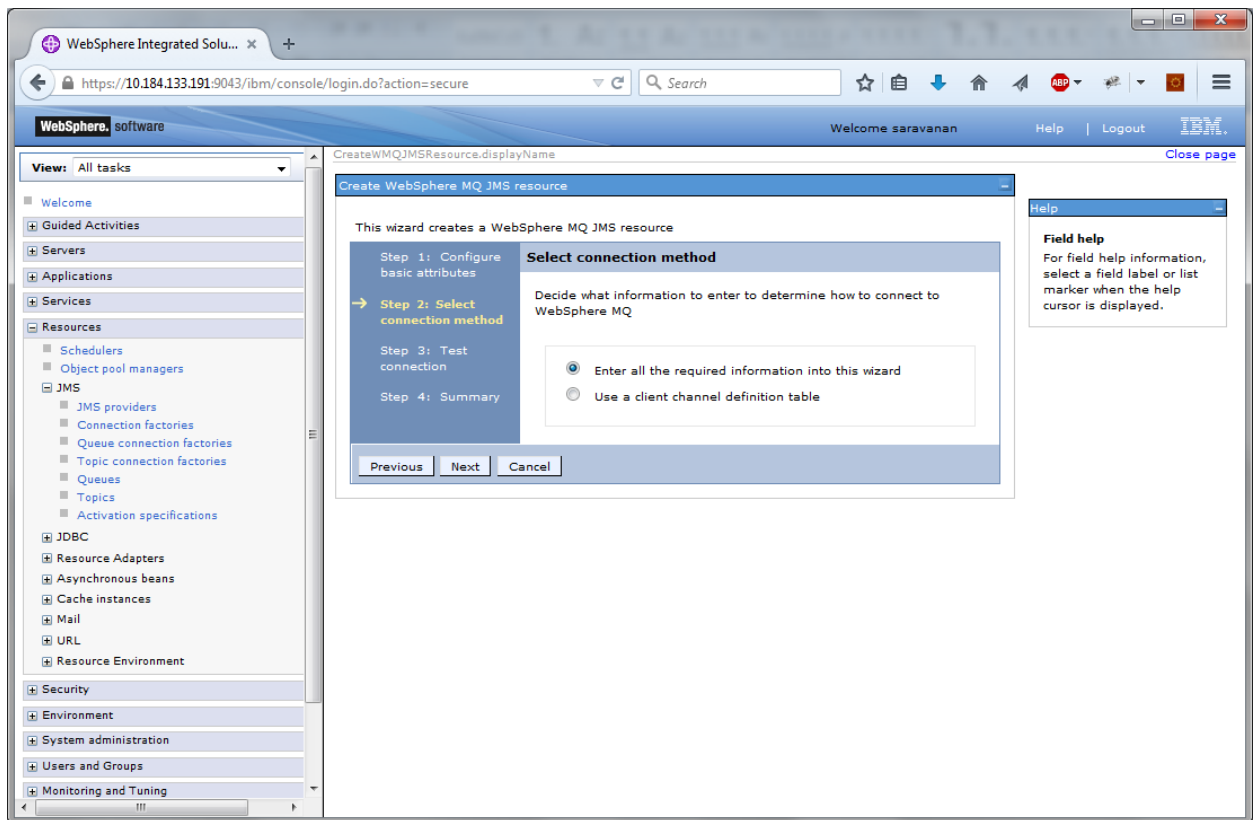
The following screen is displayed.



7. Specify the following details:

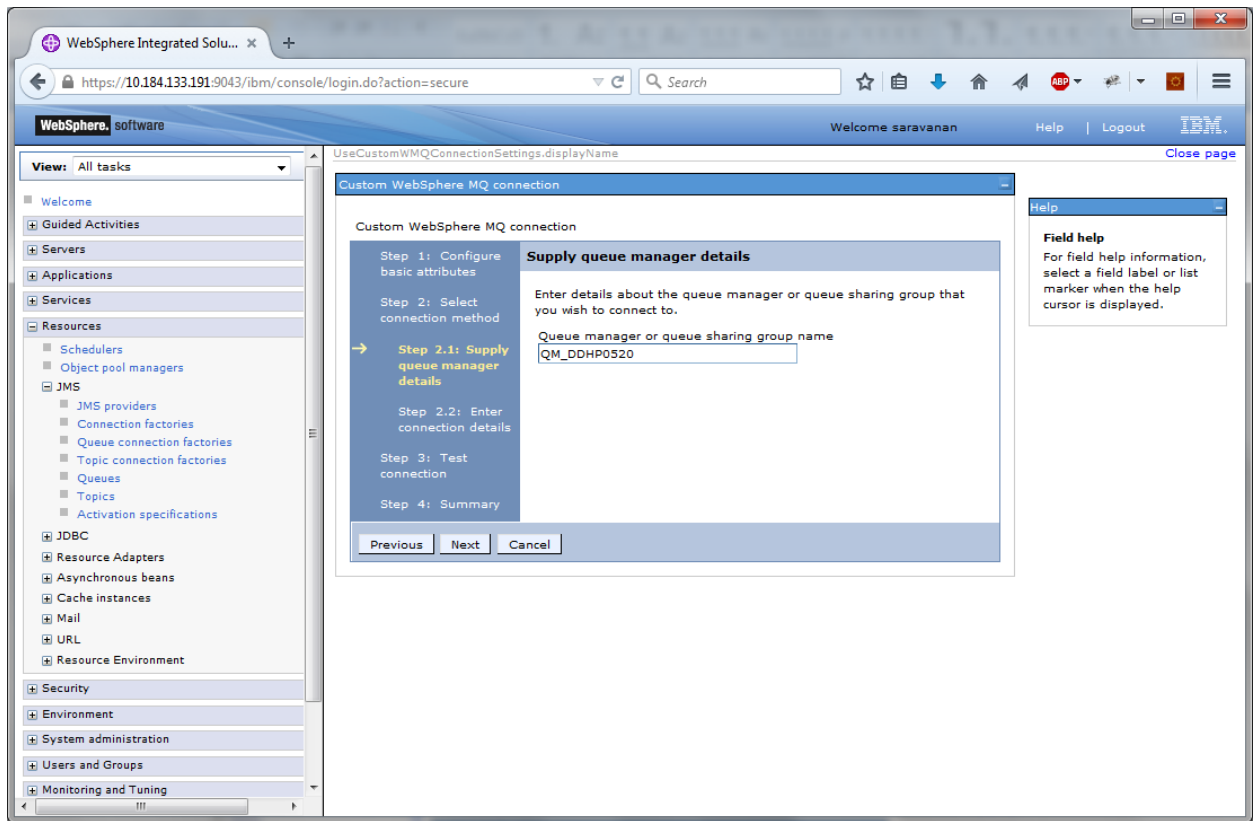
Name	NotifyDestQCF
JNDI Name	NotifyDestQCF
Description	NotifyDestQCF

Click 'Next'. The following screen is displayed.

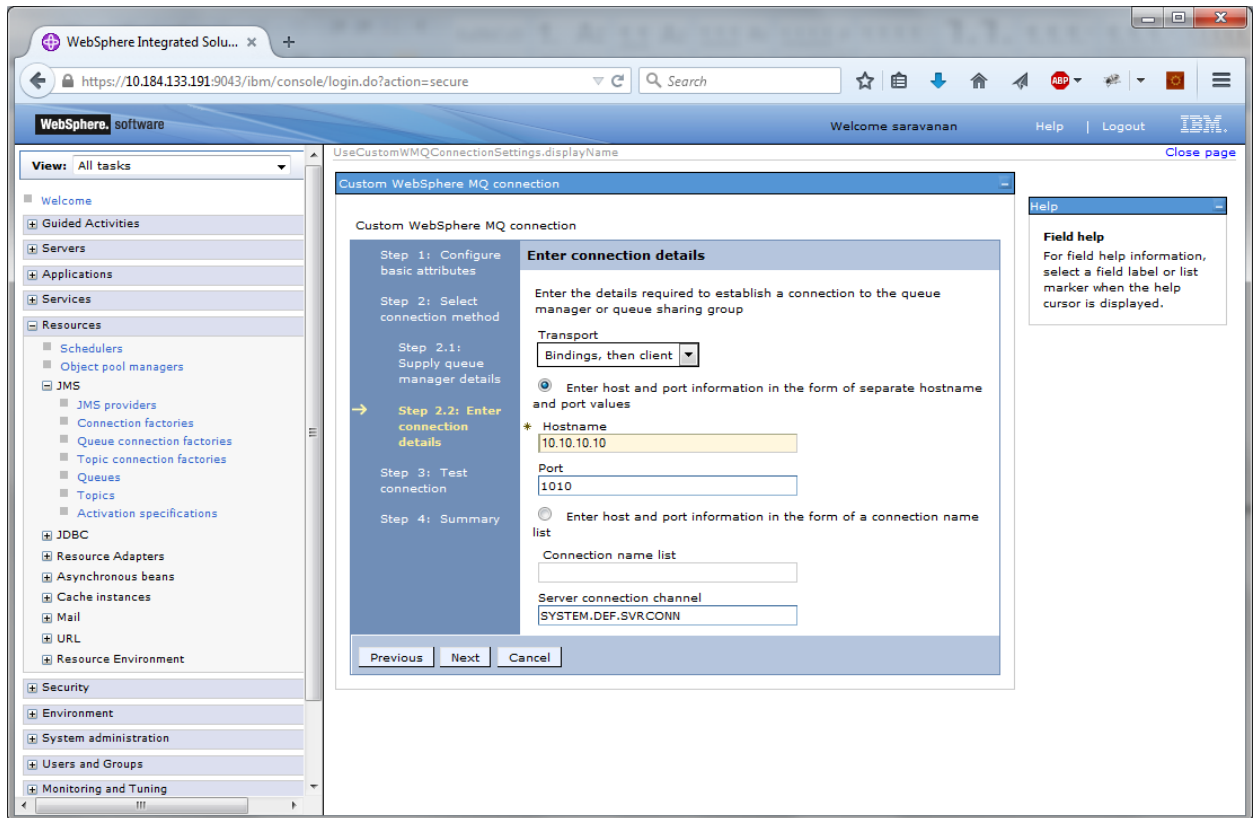


8. Set the options as shown in the figure. Click 'Next'.

The following screen is displayed.

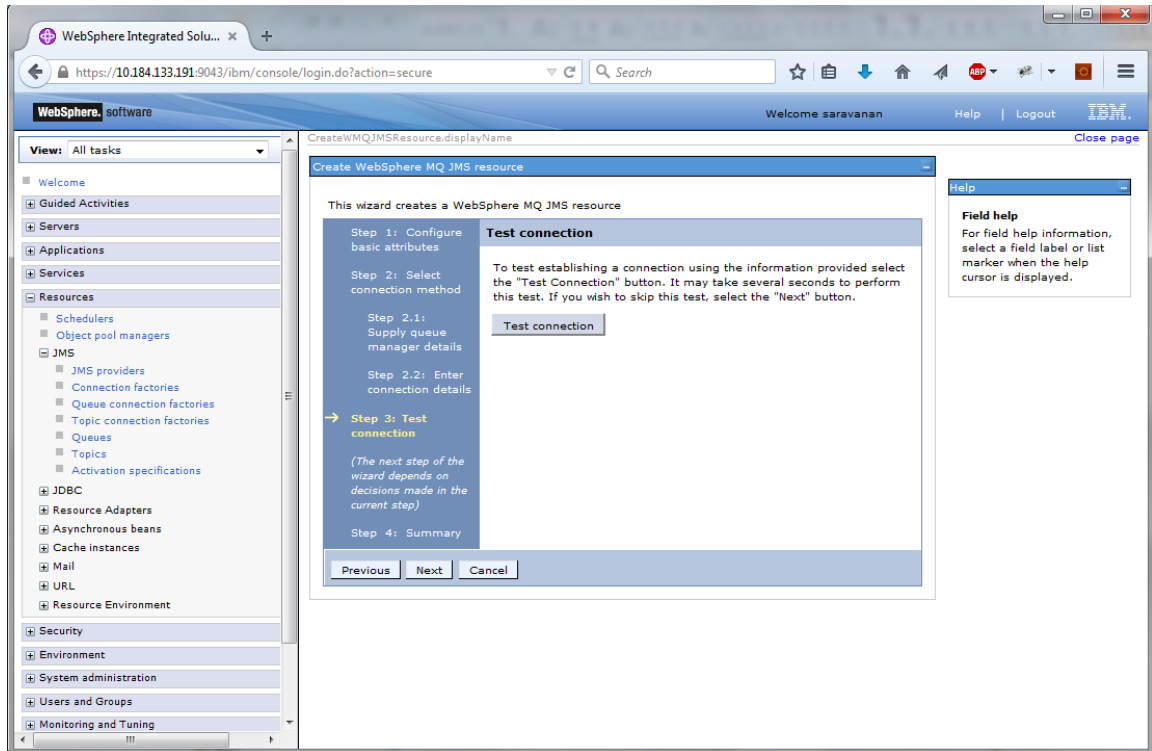


Specify the queue manager name 'QM_DDHP0520'. Click 'Next'.



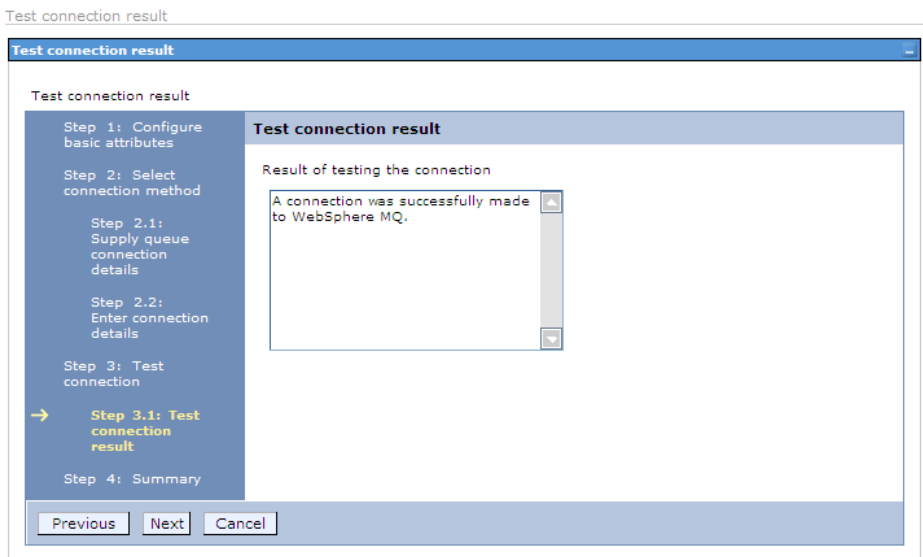
9. Specify the following details:

Host Name	10.10.10.10 (Host where Websphere MQ is installed)
Port	1010 (Web sphere MQ port)
Server Connection Channel	SYSTEM.DEF.SVRCONN

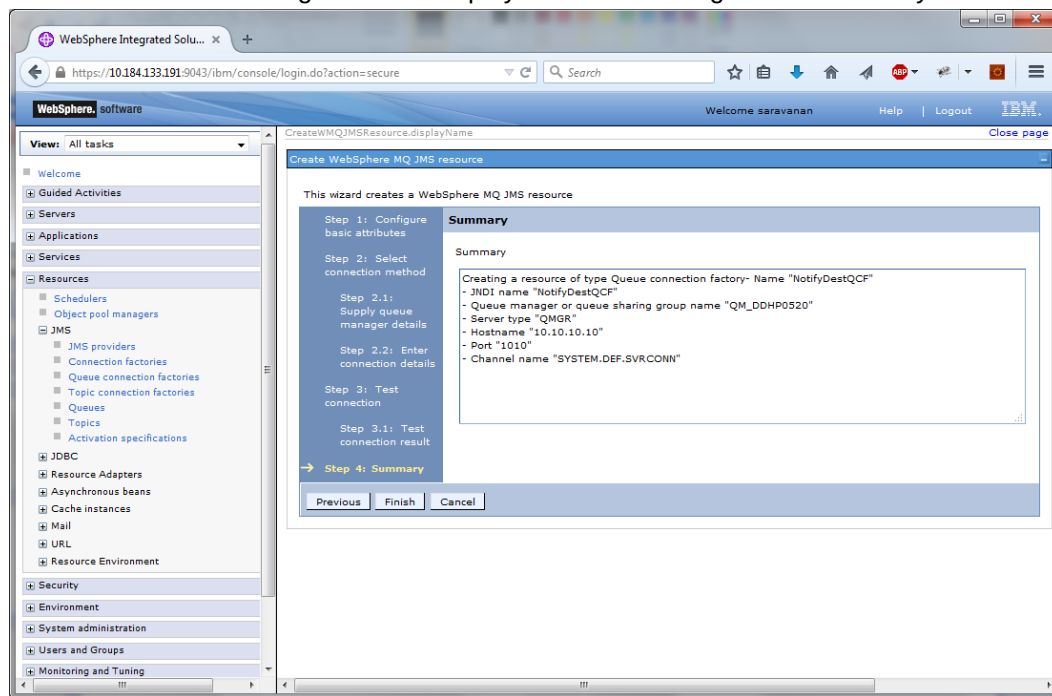


10. Click 'Test Connection' button.

The following screen is displayed:

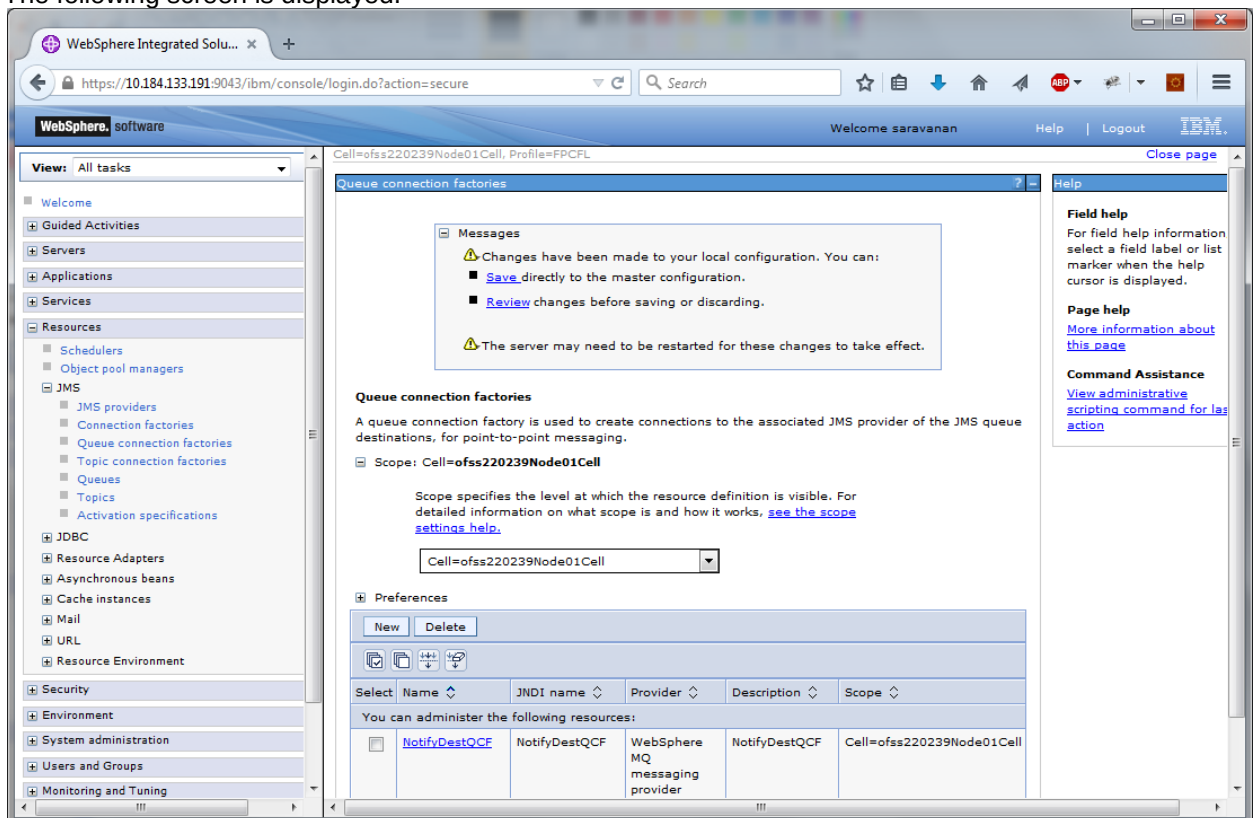


11. Click 'Next'. The following screen is displayed with a message in the summary field.



12. Click 'Finish'.

The following screen is displayed.

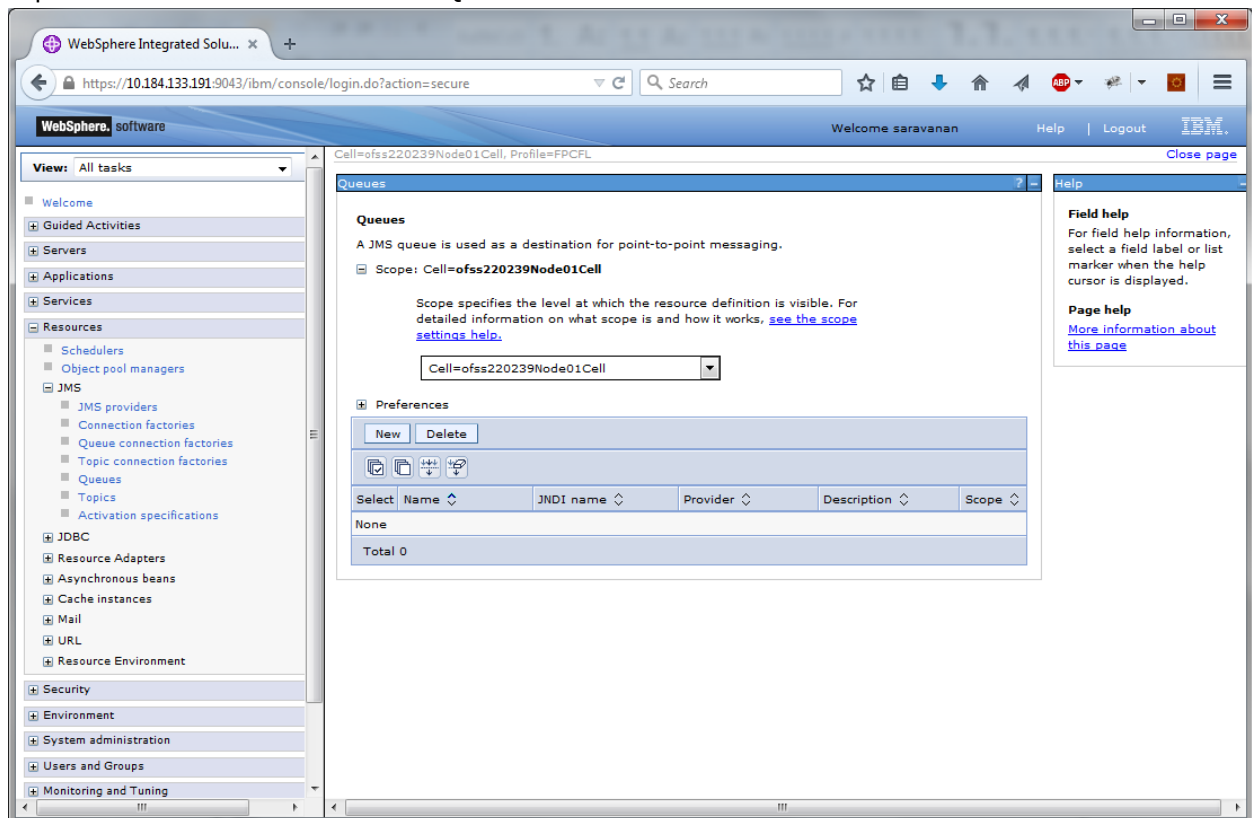


13. Click 'Save'.
14. Similarly, you need to create the all queue connection factories mentioned in the document "Resource To be Created"
15. Make sure that the checkbox "Support two phase commit protocol" is un-checked when creating FCM_QCF as JNDI name.

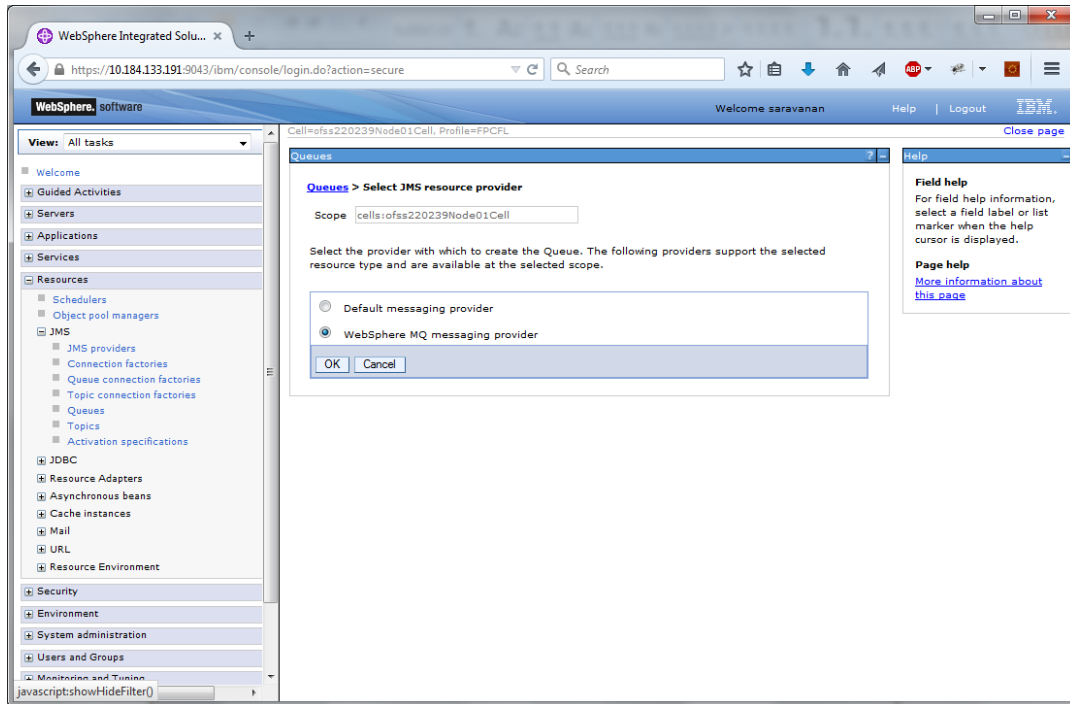
3.4.2 Creating Queues

Follow the steps given below:

1. Expand 'Resources > JMS' and click Queues.

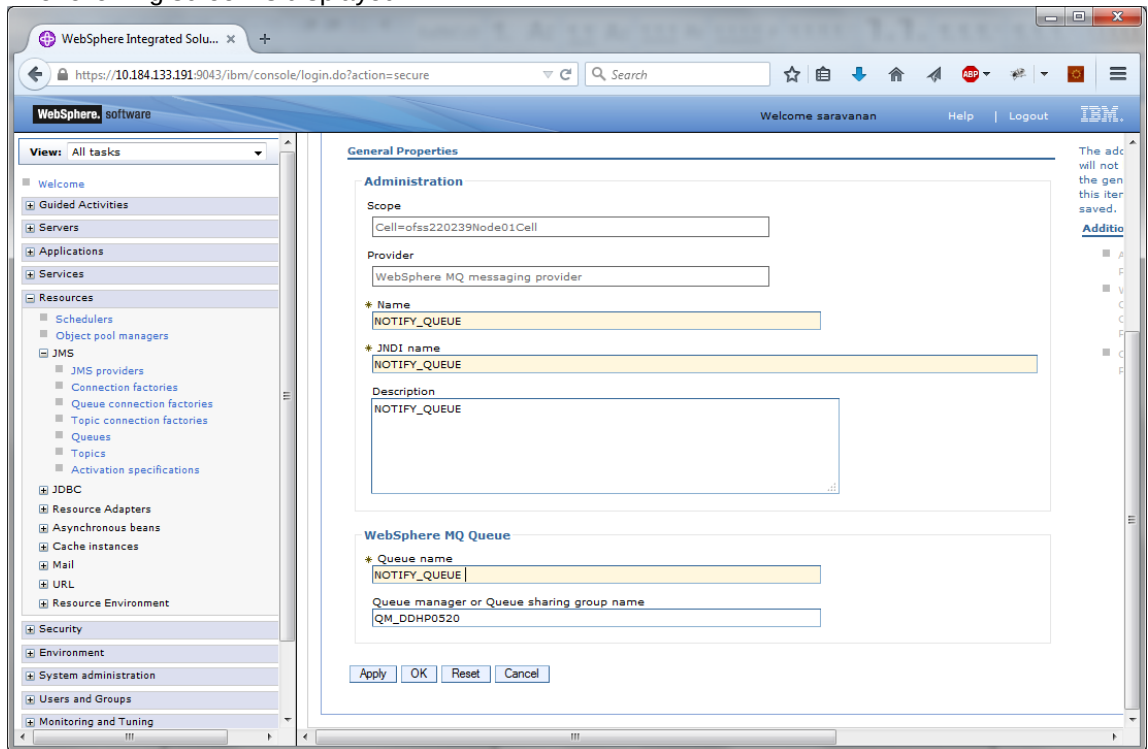


2. Select 'Scope' from the drop down list. Click 'New'.



3. Select 'Websphere MQ messaging provider'. Click 'OK'.

The following screen is displayed.

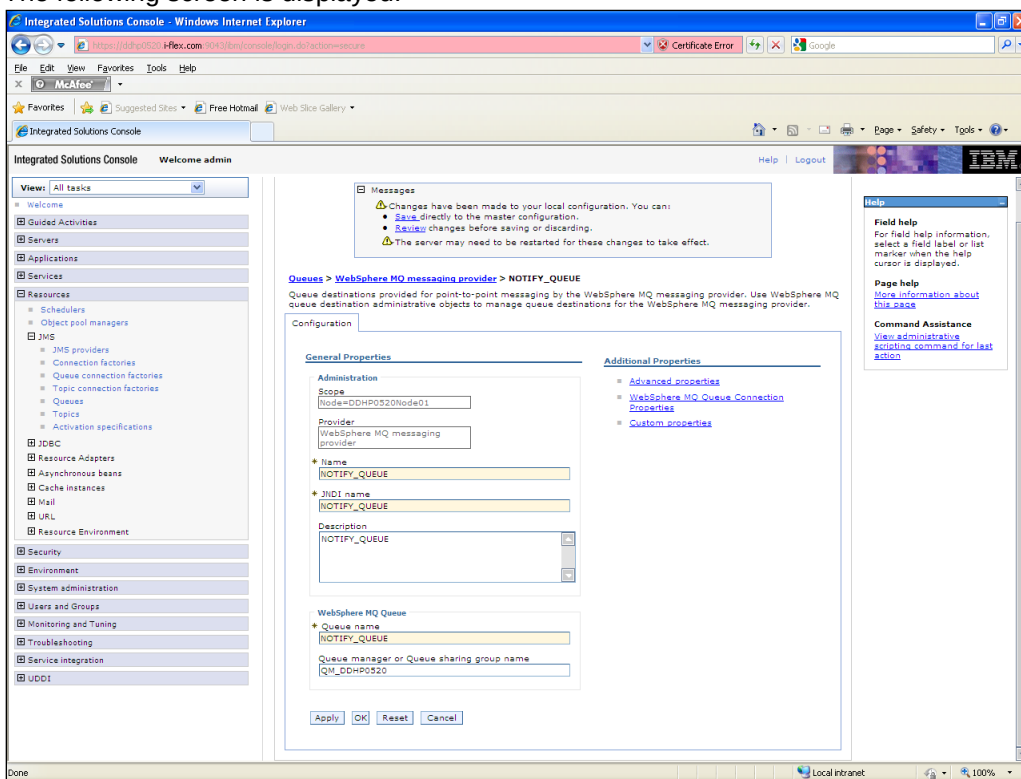


Specify the following details:

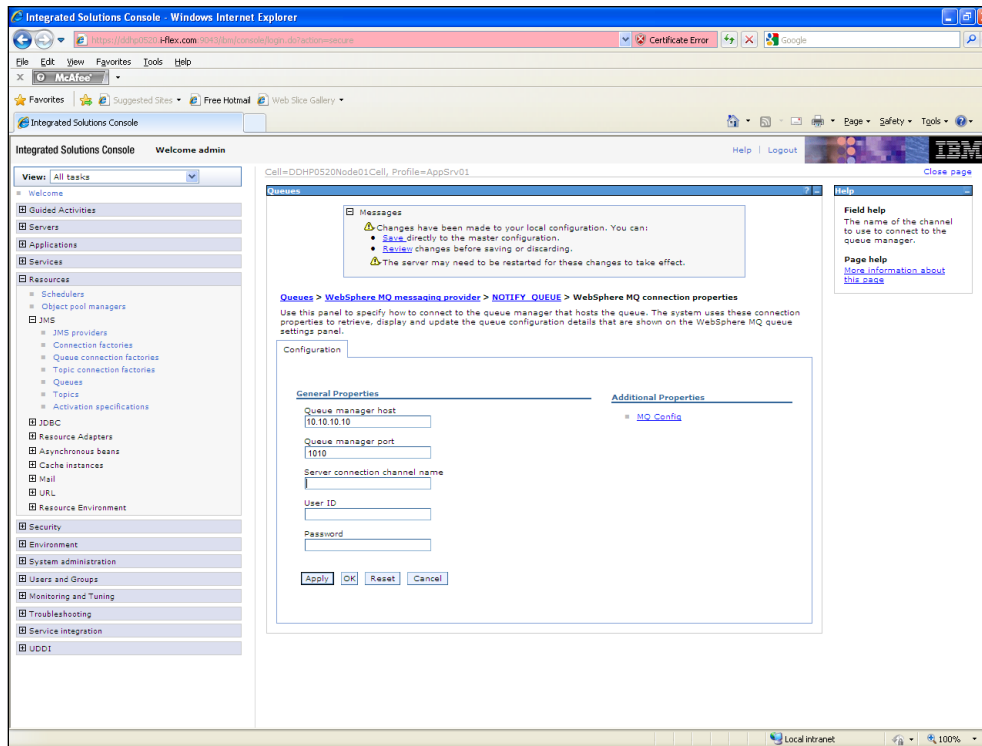
Name	NOTIFY_QUEUE
JNDI Name	NOTIFY_QUEUE
Description	NOTIFY_QUEUE
Queue Name	NOTIFY_QUEUE on Websphere MQ to which the queue needs to be mapped
Queue Manager or Queue sharing group name	QM_DDHP0520

4. Click 'Apply'.

The following screen is displayed.



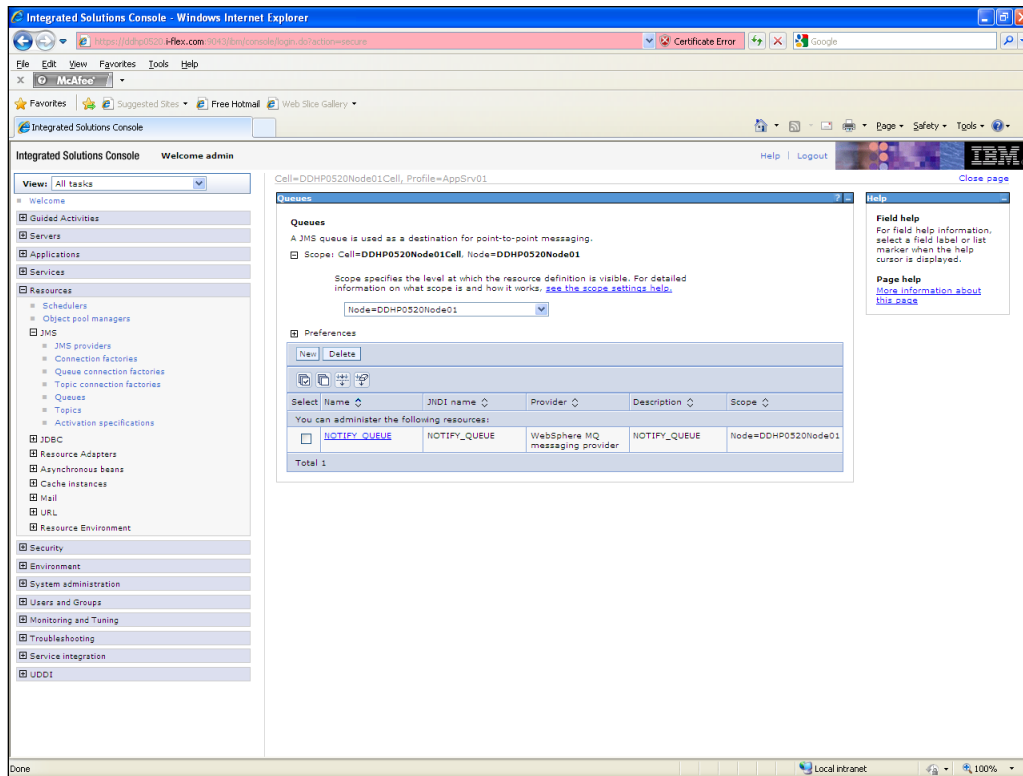
5. Click 'WebSphere MQ Queue Connection Properties'.



6. Specify the following details:

Queue manager host	10.10.10.10 (IP address of the MQ server)
Queue manager port	1010
Server Connection channel name	SYSTEM.DEF.SVRCONN

7. Click 'Save'.



8. Similarly, you need to create all the queues mentioned in the document “Resource To be Created”.

3.5 Creating Message Listener

Follow the steps given below:

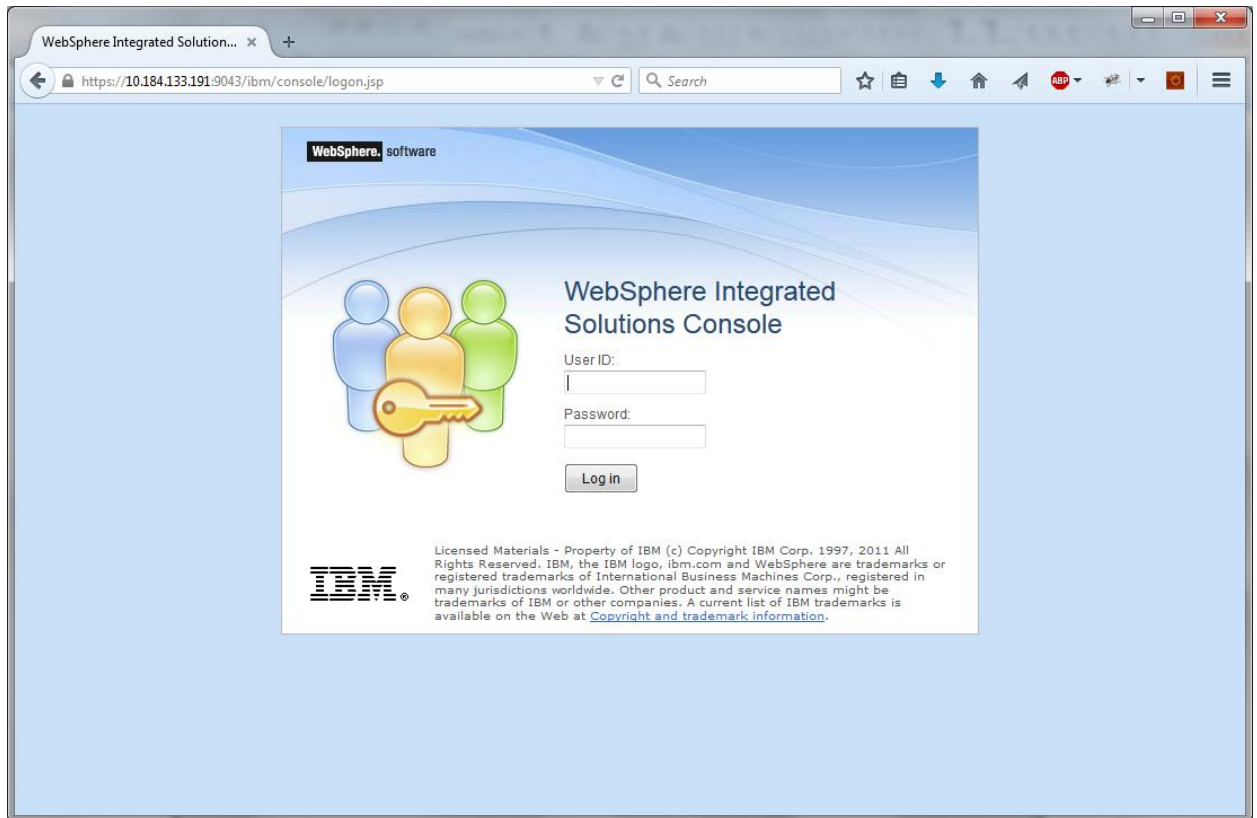
1. Start the administrative console of Websphere application server. Open an internet browser and enter the Websphere admin console URL.

http://{Host}:{Port}/console

Eg: https://10.10.10.10:1010/console

In this example, 10.10.10.10 is the machine IP address on which Websphere is running.

The following screen is displayed:



2. Specify the Websphere administrator username and password.
3. Click 'Log In'.

4. Navigate to Websphere home page .Expand 'Servers > Server Types' and click 'Websphere application servers'.

The following screen is displayed.

The screenshot shows the IBM WebSphere Integrated Solutions console. The left sidebar contains a tree view with the following structure:

- View: All tasks
- Welcome
- Guided Activities
- Servers
 - Server Types
 - WebSphere application servers
 - WebSphere MQ servers
 - Web servers
- Applications
- Services
- Resources
 - Schedulers
 - Object pool managers
 - Java EE default resources
 - JMS
 - JMS providers
 - Connection factories
 - Queue connection factories
 - Topic connection factories
 - Queues
 - Topics
 - Activation specifications
 - JDBC
 - Resource Adapters
 - Concurrency
 - Cache instances
 - Mail
 - URL
 - Resource Environment
- Security
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service Integration
- UDDI

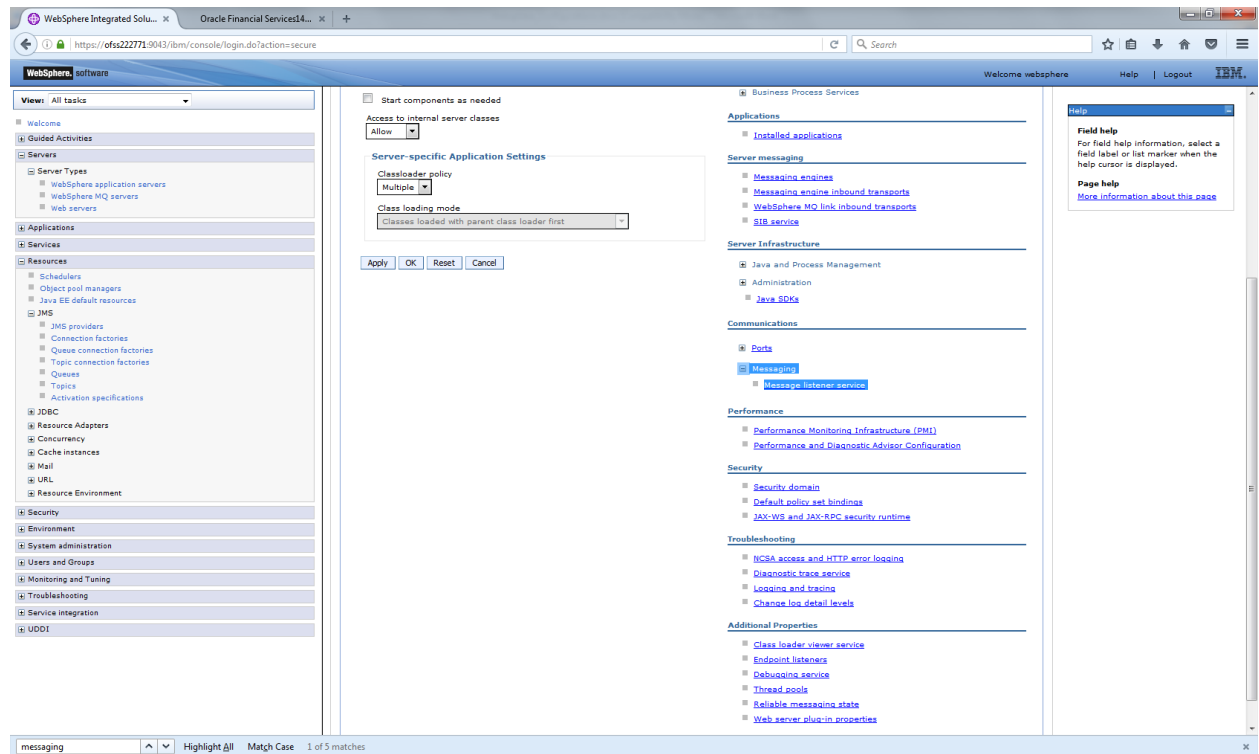
The main content area displays the 'Application servers' page. It includes a title bar 'Application servers' and a subtitle 'Application servers'. Below the subtitle, it states: 'Use this page to view a list of the application servers in your environment and the status of each of these servers. You can also use this page to change the status of a specific application server.' There is a 'Preferences' link. Below this, a table lists the application servers:

Name	Node	Host Name	Version
You can administer the following resources:			
server1	ofsa222771Node01	ofsa222771.in.oracle.com	Base 9.0.0.0
Total 1			

The right sidebar contains a 'Help' section with 'Field help' and 'Page help' links, and a 'Command Assistance' section with 'View administrative actions' and 'Command for last action' links.

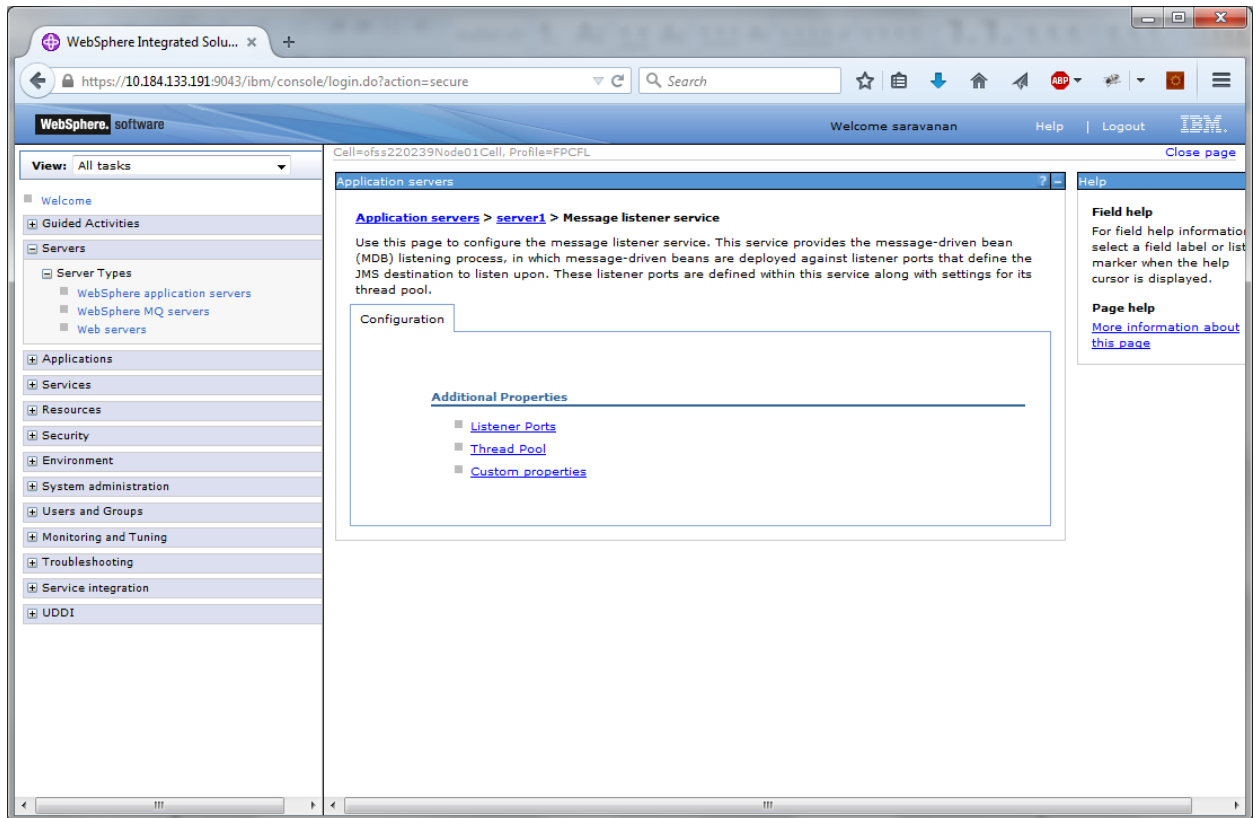
5. Click 'server1'.

The following screen is displayed.



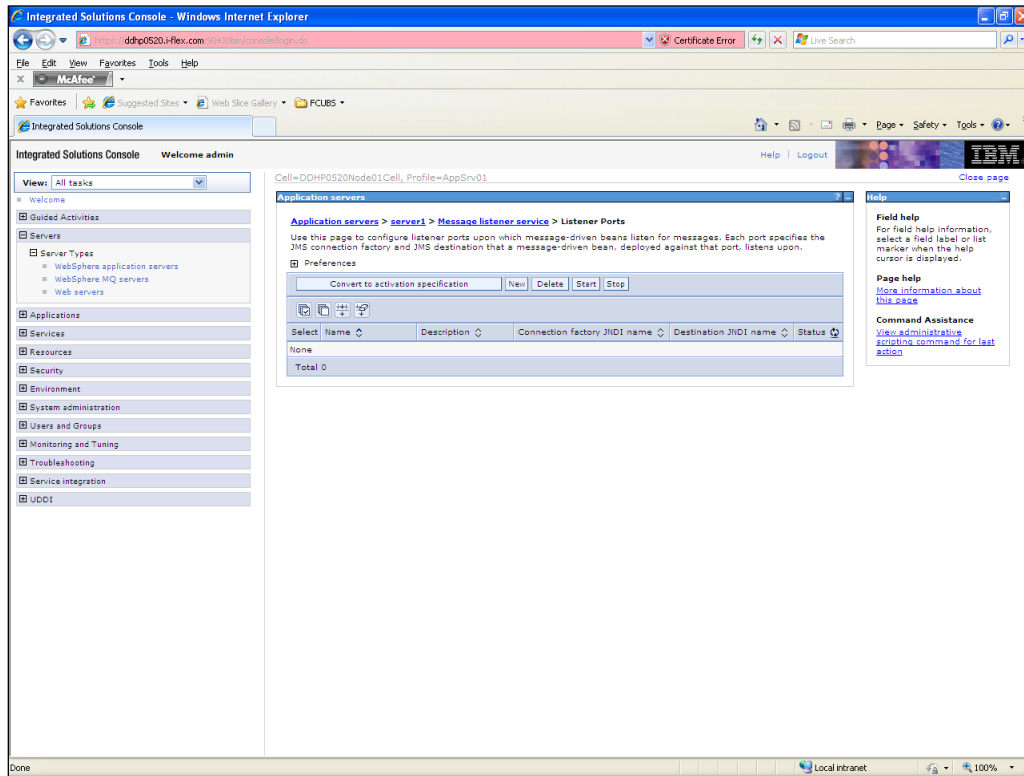
6. Expand 'Messaging' under Communications and select 'Message listener service'.

The following screen is displayed.



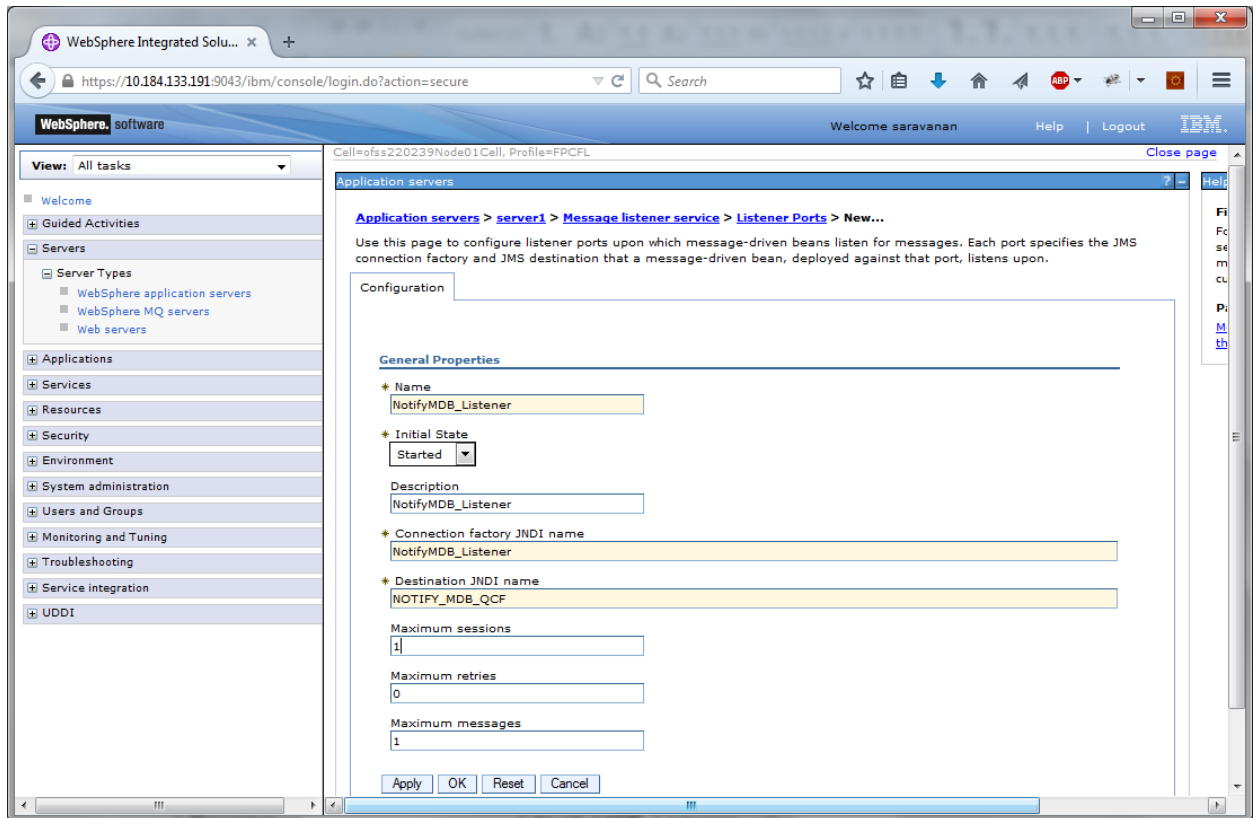
7. Click 'Listener Ports'.

The following screen is displayed.



8. Click 'New'.

The following screen is displayed.

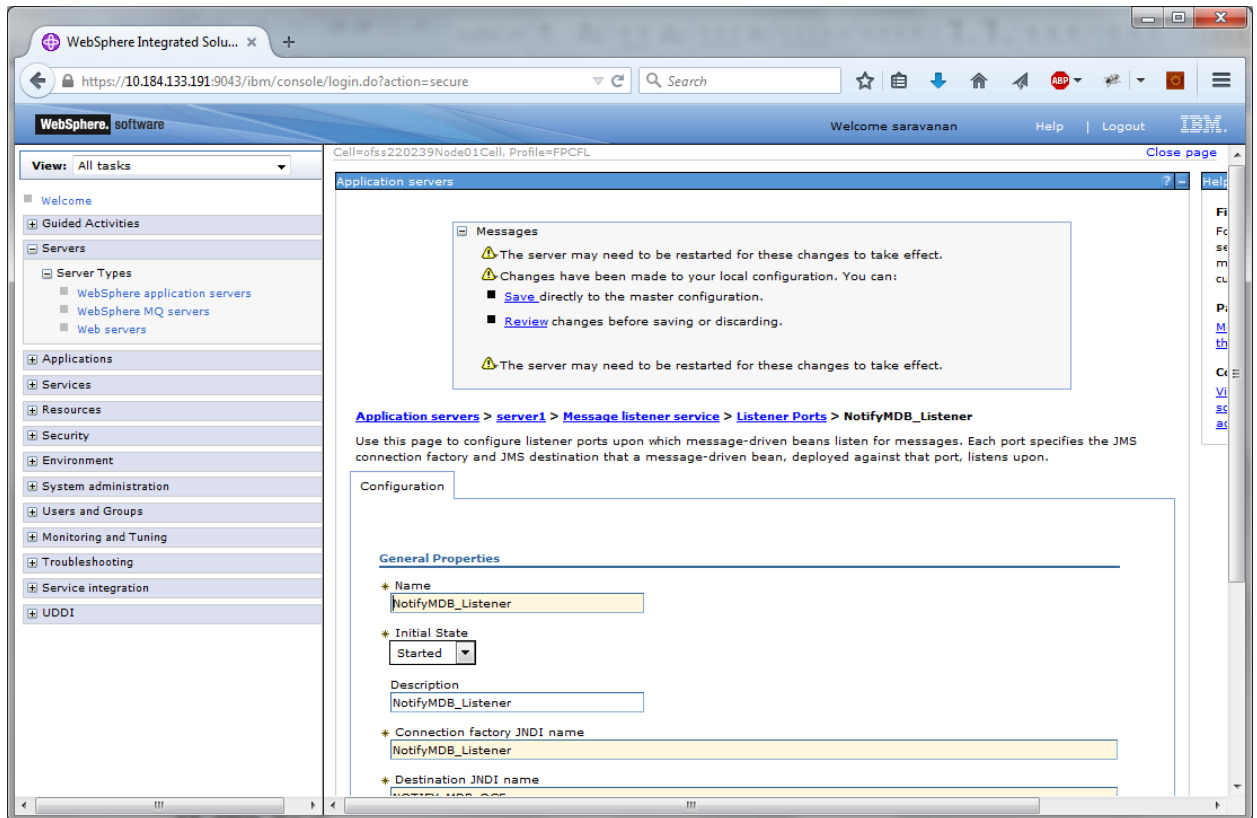


9. Specify the following details:

Name	NotifyMDB_Listener
Description	NotifyMDB_Listener
Connection factory JNDI name	NOTIFY_MDB_QCF
Destination JNDI name	NOTIFY_ QUEUE
Maximum retries	1

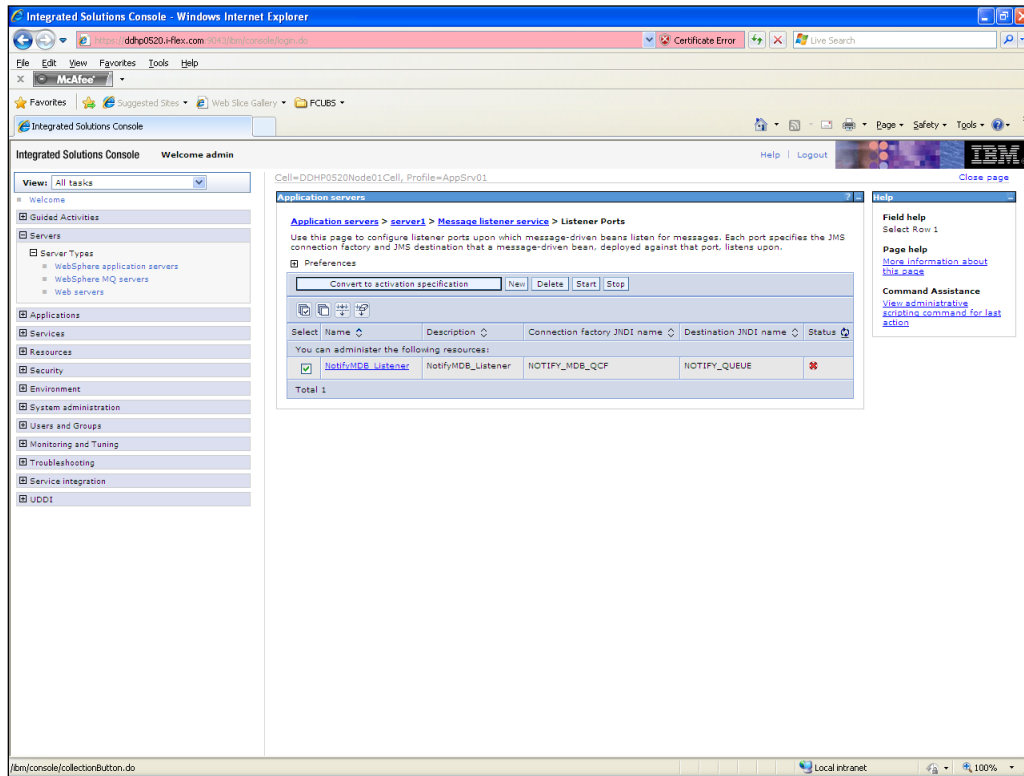
10. Click 'Apply'.

The following screen is displayed.



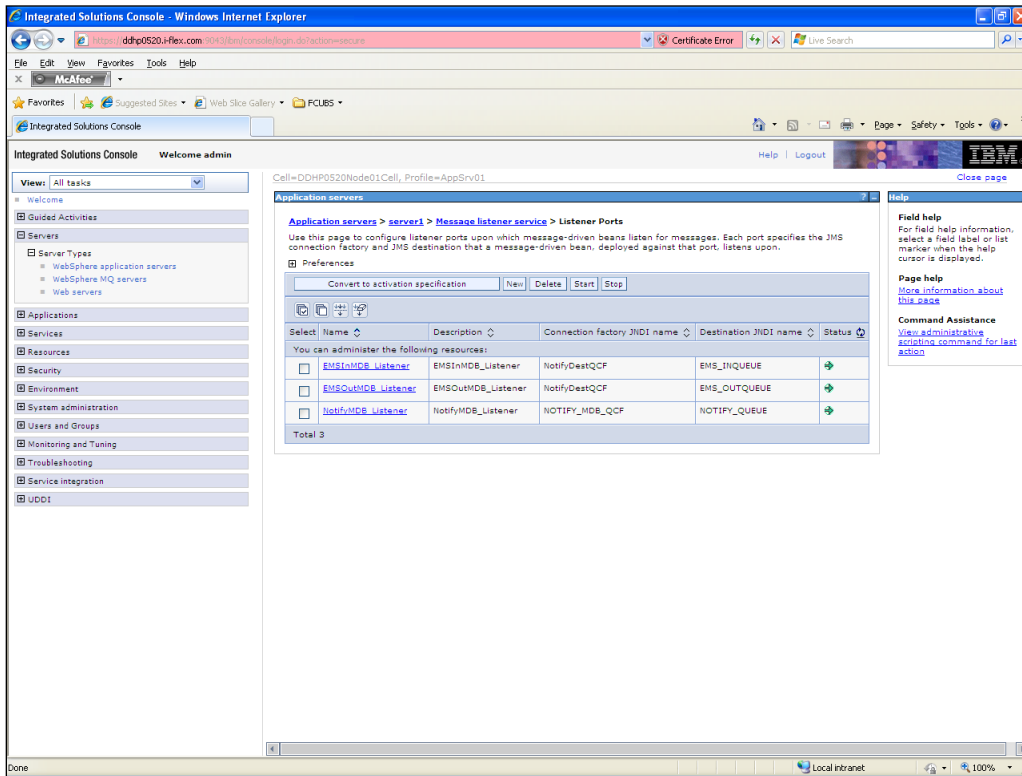
11. Click 'Save'.

The following screen is displayed.



12. Select 'Notify MDB_Listener'. Click 'Start'.

The following screen is displayed.



13. Similarly, you need to create the following listeners:

MDB_Listener
NotifyMDB_Listener
RecordingMDB_Listener
ELMDB_Listener
ELNotifyMDB_Listener

The complete list of listener queue and QCF to be created for Websphere is given below.

Application Name	Listener Name	Listener QCF	Listener QUEUE
<i>GWMDB</i>	<i>MDB_Listener</i>	<i>MDBQCF</i>	<i>MDB_QUEUE</i>
<i>GWNotifyMDB Bean</i>	<i>NotifyMDB_Listener</i>	<i>NOTIFY_MDB_QCF</i>	<i>NOTIFY_QUEUE</i>
<i>RTGSInMDB</i>	<i>RTGS_Listener</i>	<i>RTGSQCF</i>	<i>RTGS_INQUEUE</i>
<i>SFMSInMDB</i>	<i>SFMS_Listener</i>	<i>SFMSQCF</i>	<i>SFMS_INQUEUE</i>

<i>ELGWMDBBean</i>	<i>ELMDB_Listener</i>	<i>ELMDBQCF</i>	<i>ELMDB_REQ_Q</i>
<i>ELNotifyMDBBean</i>	<i>ELNotifyMDB_Listener</i>	<i>EL_NOTIFY_QCF</i>	<i>EL_NOTIFY_REQ_Q</i>
<i>EMSinMDB</i>	<i>EmsIn_Listener</i>	<i>EmsQcf</i>	<i>EMS_INQUEUE</i>
<i>EMSOOutMDB</i>	<i>EmsOut_Listener</i>	<i>EmsQcf</i>	<i>EMS_OUTQUEUE</i>
BipReportMDB	BipReport_Listener	BIPQCF	INTERNAL_BIPREPORT_QUEUE
BipAdviceMDB	BipAdvReport_Listener	BIPQCF	INTERNAL_BIPADVREPORT_QUEUE
GIUploadMDB	Gi_Upload_Listener	GI_UPLOAD_QCF	INTERNAL_GI_UPLOAD_QUEUE
PMScheduler	PMSCH_Listener	SchedulerQCF	SchedulerQueue
PMGateway	PMGW_Listener	PM_GW_QCF	PM_GW_REQ_QUEUE
FCMCore	FCM_RECEIVER_Listener	FCM_QCF	FCM_RECEIVER
FCMCore	FCM_BULKER_Listener	FCM_QCF	FCM_BULKER
FCMCore	FILE_PROCESSOR_Listener	FCM_QCF	FILE_PROCESSOR
FCMCore	pymtGatewayResQ_Listener	FCM_QCF	pymtGatewayResQ

Here,

- MDB_Listener is mandatory for Gateway MDB applications
- PMGW_Listener is mandatory for Payment Gateway MDB applications
- PMSCH_Listener is mandatory for Payment Job framework applications
- FCMCore related listeners are mandatory for FLEXCUBE Messaging.
- All others are required for FCJ Applications embedded with Scheduler and ELCM

4. Default Settings for Web Sphere

4.1 Libraries for PMGateway Application

To deploy the PMGateway application, Following steps need to be performed

1. Copy runtime12.jar from database servers ORACLE_HOME/sqlj/lib to application servers library path (WAS_HOME/lib/ext)
2. Create a global shared library containing the following file:
 - a. eclipselink.jar

Find this file in the

'TOPLINK_INSTALLATION\oracle_common\modules\oracle.toplink_ver_no' directory created by the TopLink quick installer.

- For step 2 Kindly Refer the document **Toplink_IBM_WAS_setup.doc**

5. Configuring Mail Session on Websphere

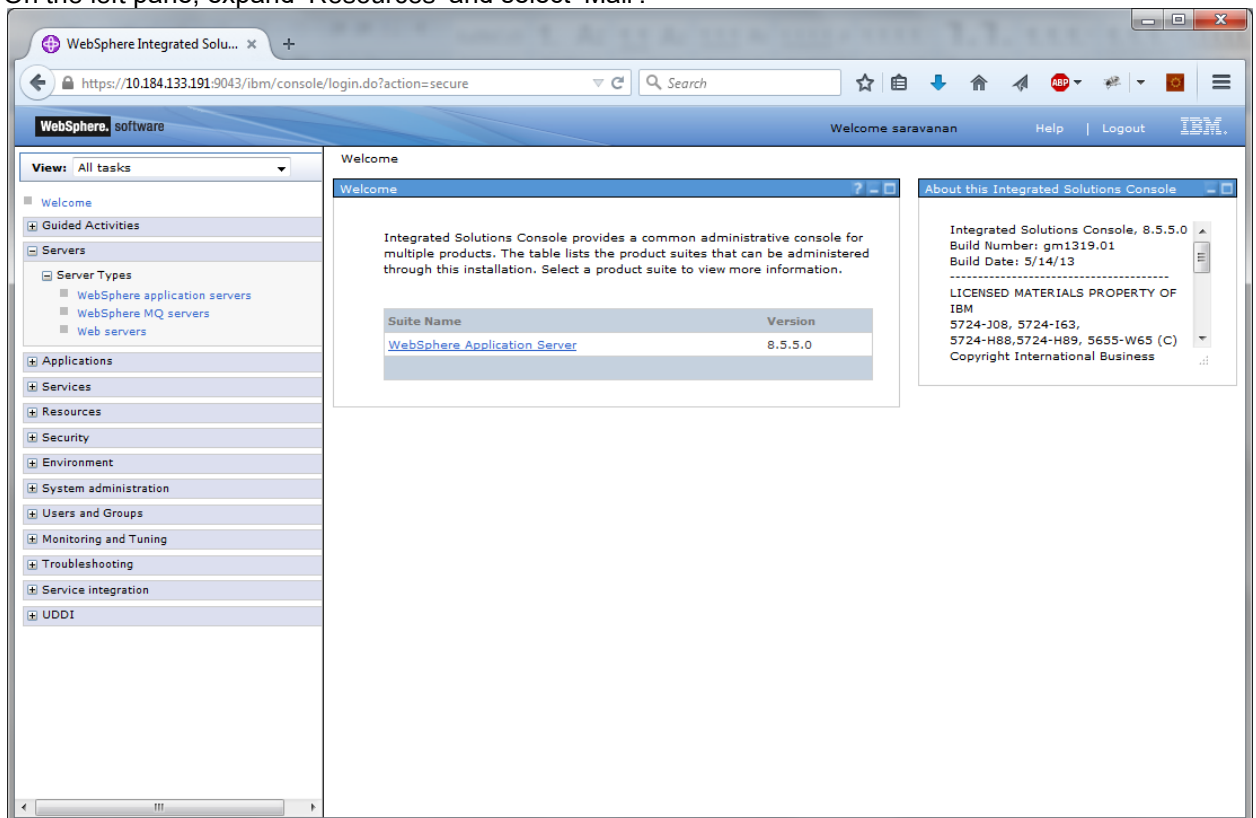
5.1 Introduction

This section describes the method to configure Websphere application server for Oracle FLEXCUBE to generate and send passwords to the users via e-mail.

5.2 Creating Java Mail Session

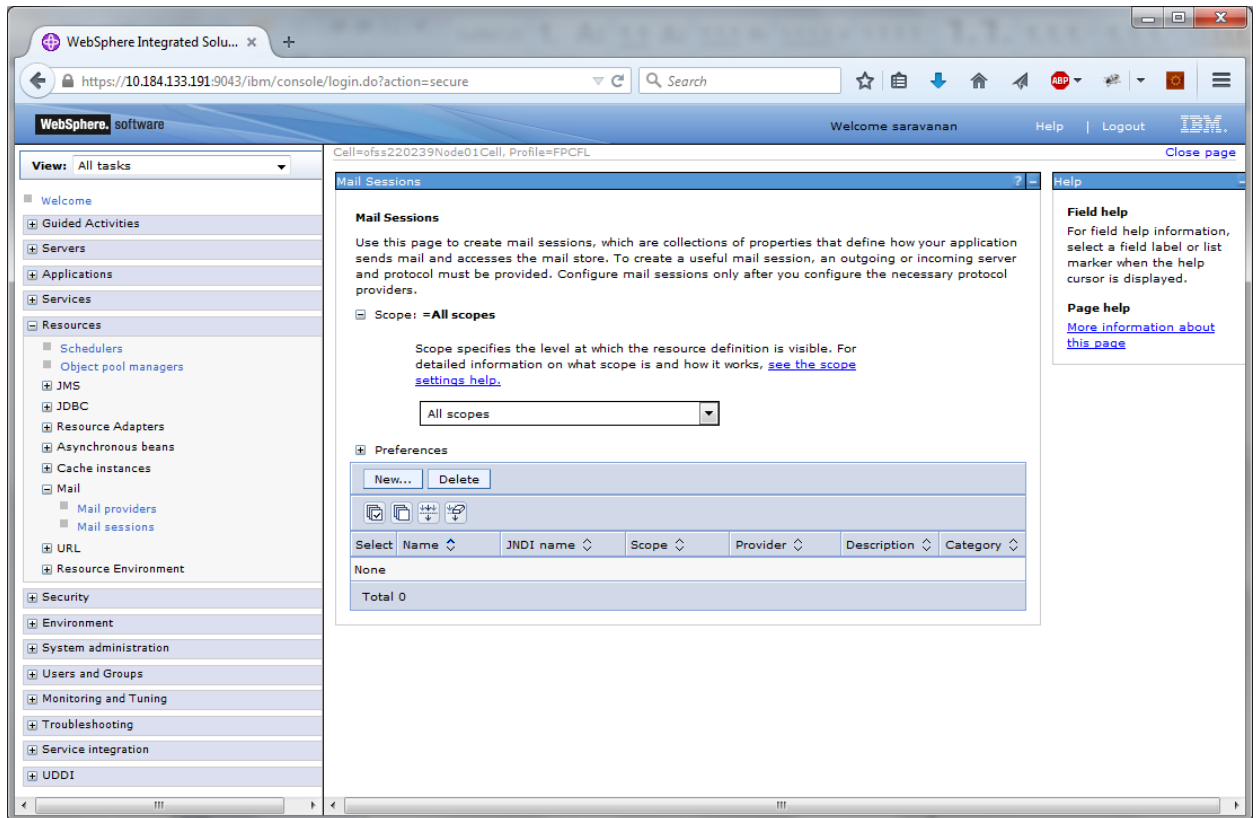
To create Java mail session, follow the steps given below:

On the left pane, expand 'Resources' and select 'Mail'.

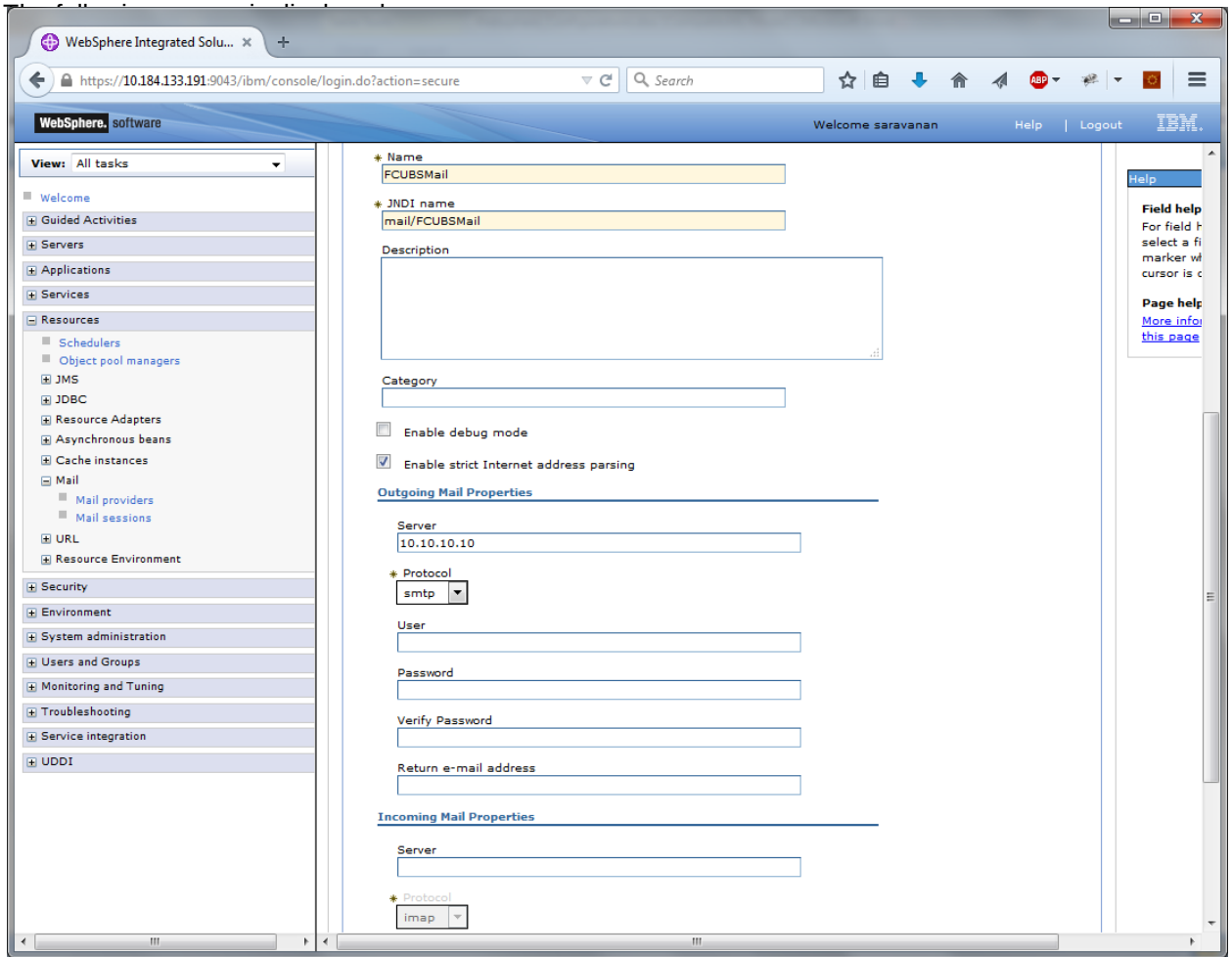


1. Click 'Mail Sessions' to invoke the 'Mail sessions' screen.

The following screen is displayed:



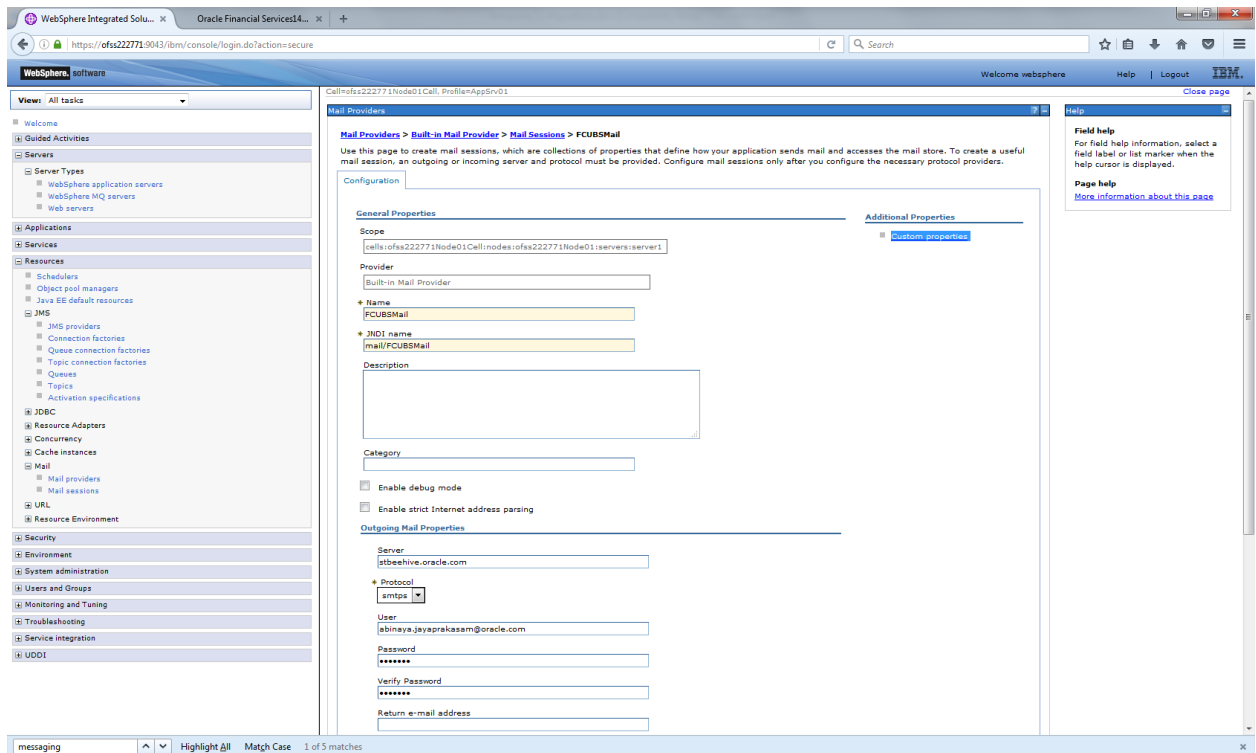
2. Click 'New' button to create a new mail session.



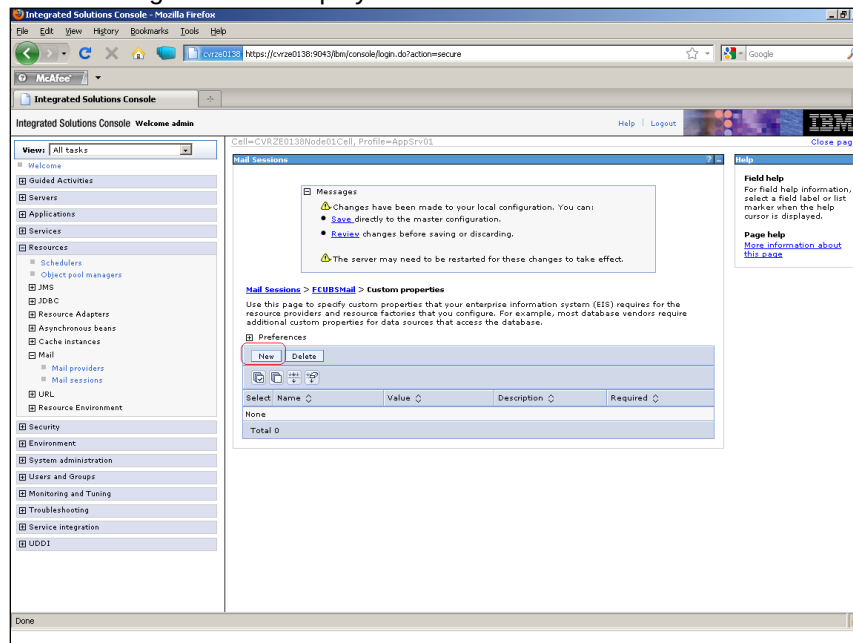
3. Provide the required information. Sample details are given below for your reference.

General Properties	
Name	OBTRMMail
JNDI Name	mail/OBTRMMail
Outgoing Mail Properties	
Server	< HOST_MAIL_SERVER >
Protocol	Smtps

4. Click 'Custom Properties' link to configure the custom properties.

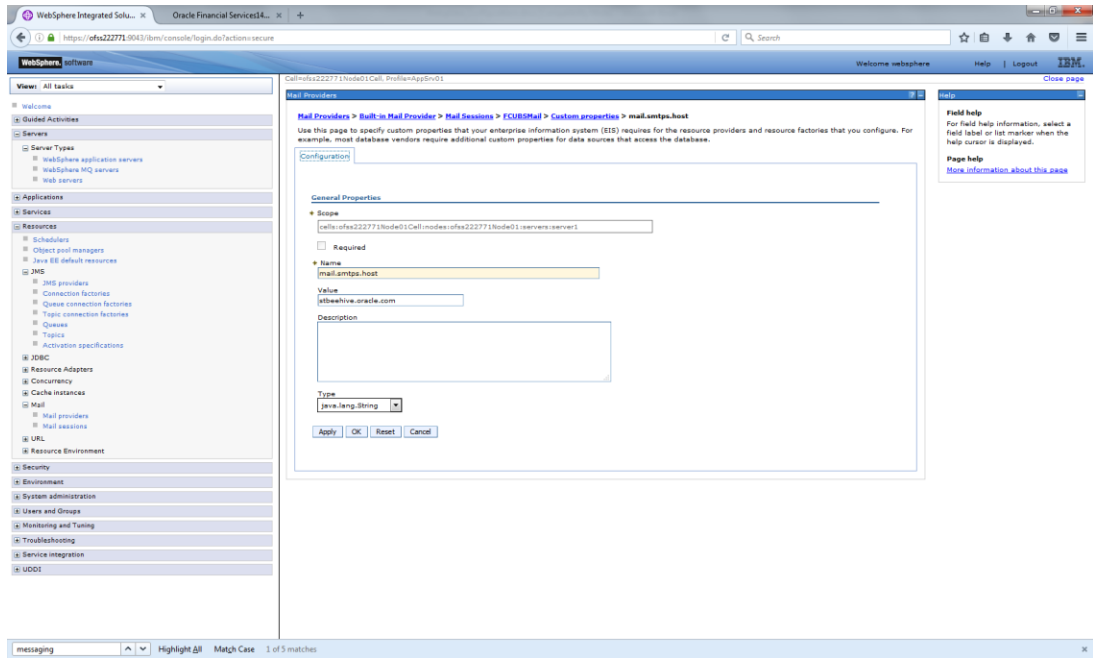


The following screen is displayed.



5. Click 'New' button to create new custom properties.

The following screen is displayed.

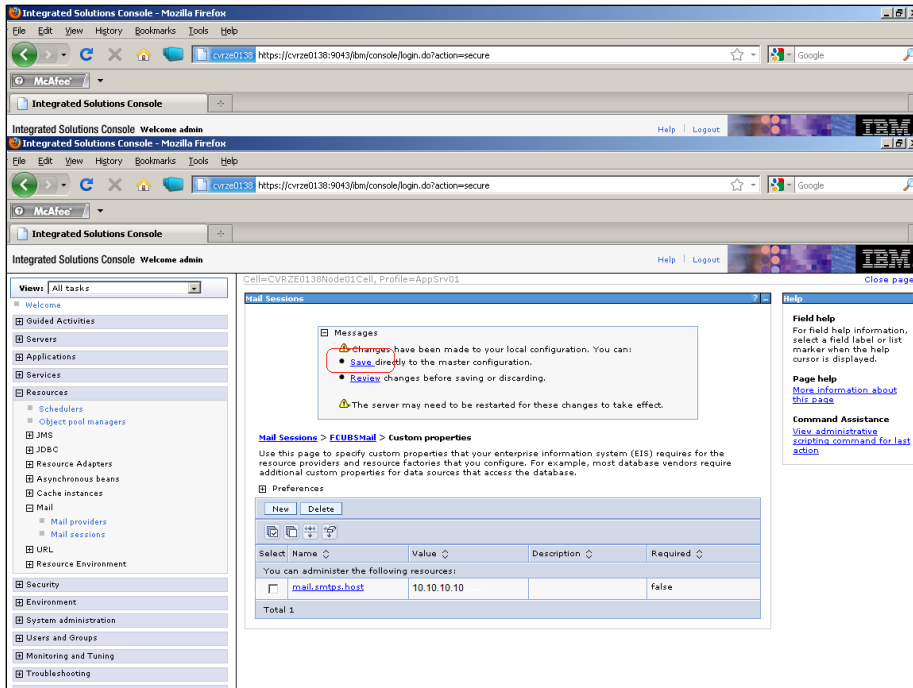


6. Specify the information required for creating custom properties. Sample details are given below:

Name	mail.smtps.host
Value	<HOST_SMTPS_MAIL_SERVER>
Type	java.lang.String

The custom properties are given below:

Name	Value	Type
mail.smtp.host	<HOST_SMTPS_MAIL_SERVER>	java.lang.String
mail.smtp.port	<SMTPS_SERVER_PORT>	java.lang.String
mail.host	<HOST_MAIL_SERVER>	java.lang.String
mail.smtps.auth	TRUE	java.lang.String



Click 'Save' to complete the configuration.



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

- SMTP_HOST
- SMTP_USER
- SMTP_PASSWORD
- SMTP_JNDI

You can update this using Oracle Banking Treasury Management Installer.

6. Annexure

Ensure the following settings before deploying the application:

6.1 IBM Websphere Server - Increasing Heap Size

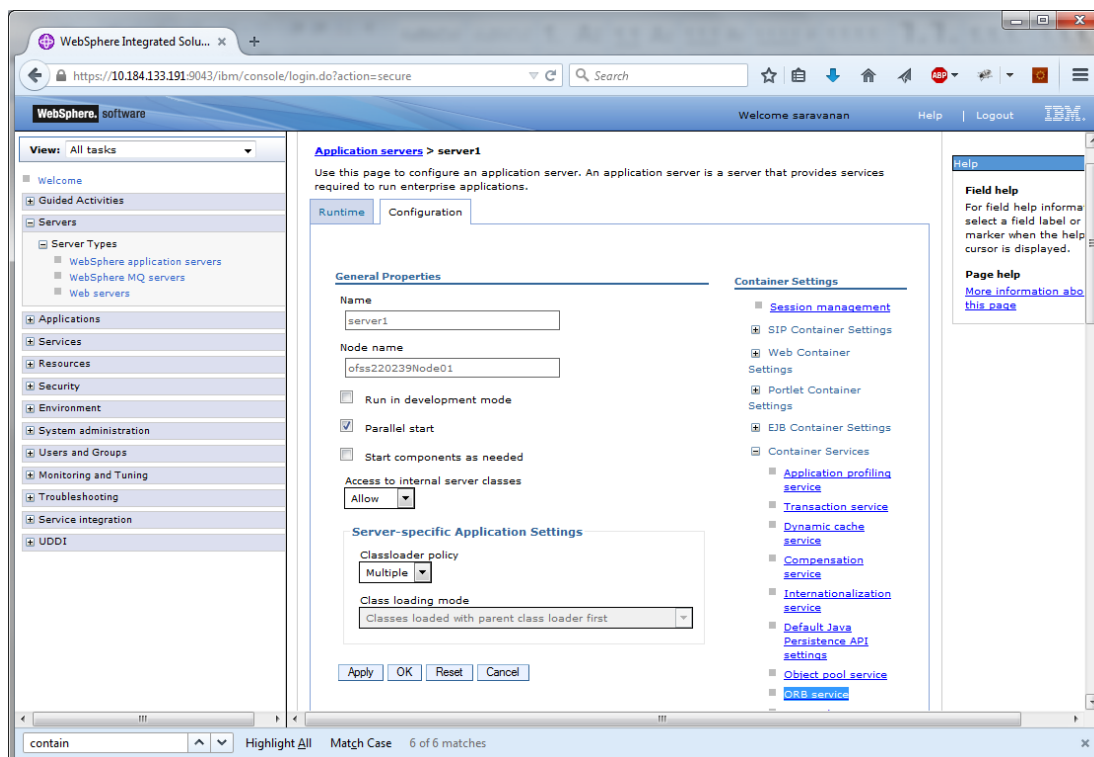
1. Go to 'Server > Application Servers' and select the 'server_name'
2. Under the Configuration tab, navigate to 'Server Infrastructure > Java(TM) and Process Management > Process Definition > Additional Properties: Java Virtual Machine'
3. Modify the initial heap size and maximum heap size appropriately based on the load size

6.2 IBM Websphere Server - Transaction Service Properties

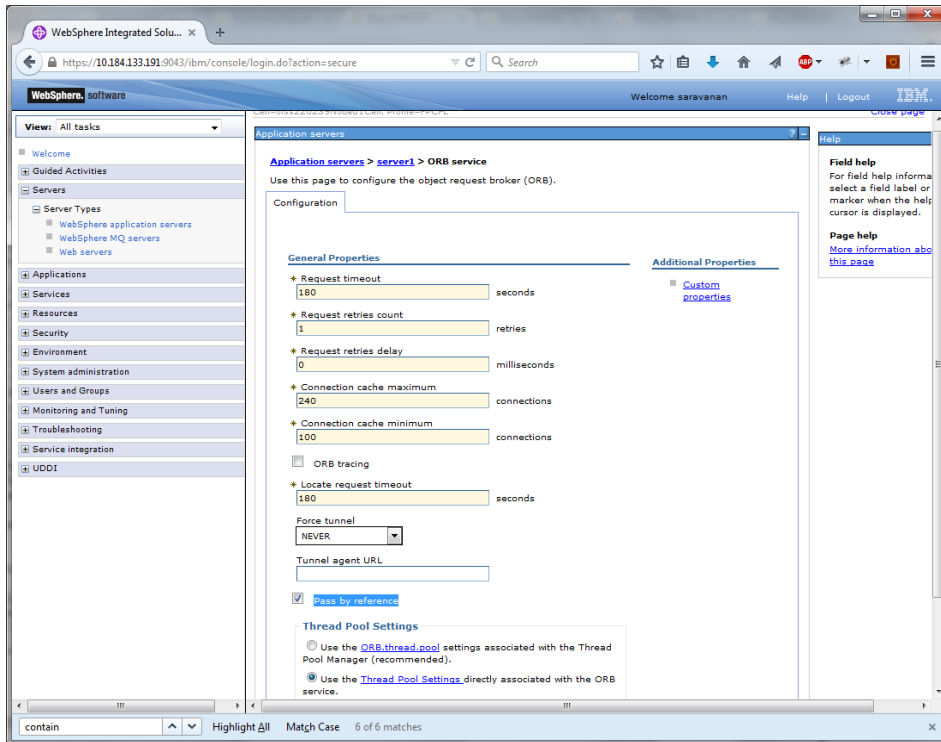
1. Go to 'Server > Application Servers' and select the 'server_name'
2. Choose 'Container Services > Transaction Service'
3. Change the total transaction lifetime timeout appropriately
4. Party content, products, or services.

6.3 IBM Websphere Server – ORB Service Configuration

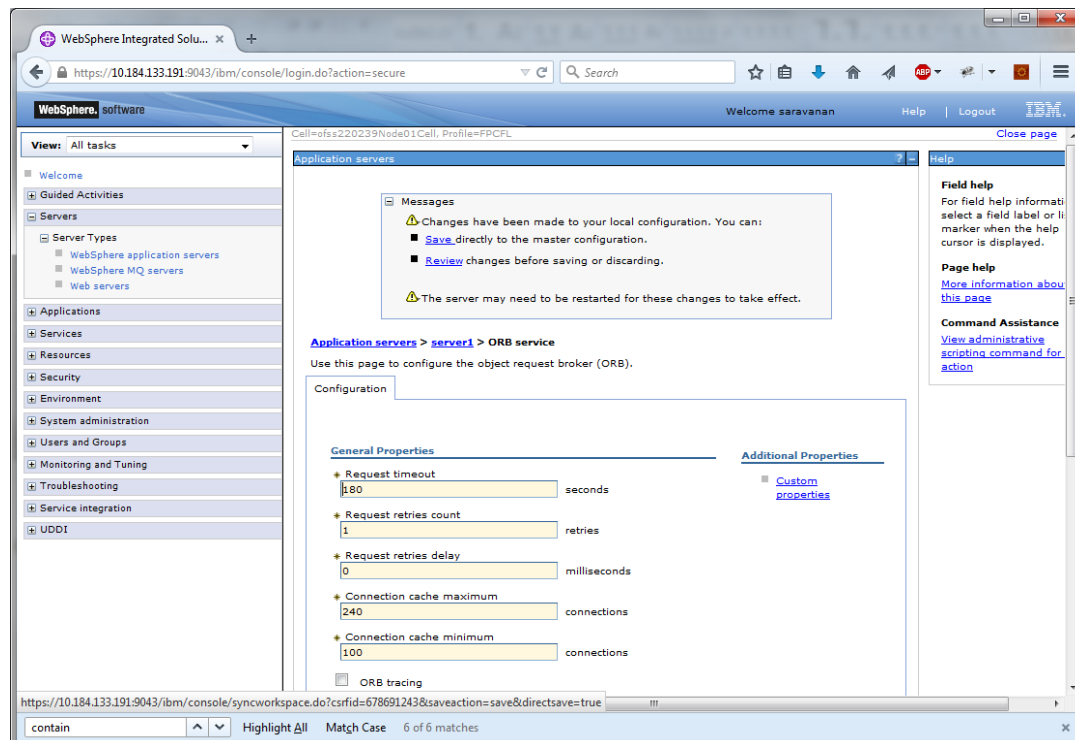
1. Go to 'Server > Application Servers' and select the 'server_name'



2. Expand 'Container Services' and click 'ORB Service'



3. Check 'Pass by reference' and click Apply



4. Click 'Save'.



Websphere Configuration

[February] [2022]

Version 14.5.4.0.0

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

Worldwide Inquiries:

Phone: +91 22 6718 3000

Fax: +91 22 6718 3001

www.oracle.com/financialservices/

Copyright © 2020, 2022 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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