**Документация по настройке взаимодействия MQ c Weblogic.**

1. **Генерация binding-файла:**

Необходимо для генерации binding-файла, который будет использоваться в дальнейшем для подключения Weblogic по JMS-технологии к КСШ (MQ) передать файл с настройками генерации:

define xaqcf(«имя менеджера очередей») qmgr(«имя менеджера очередей») host(«имя/ip-адрес сервера») port(«порт соединения») tran(CLIENT) chan(«имя канала») CCSID(1208) SSLCIPHERSUITE(SSL\_RSA\_WITH\_RC4\_128\_MD5)

DEFINE Q(«имя очереди - входящая») QUEUE((«имя очереди - входящая») ) QMGR(«имя менеджера») CCSID(1208) TARGCLIENT(JMS) MSGBODY(UNSPECIFIED) MDREAD(YES)

DEFINE Q( «имя очереди - исходящая») QUEUE(«имя очереди - исходящая») QMGR() CCSID(1208) TARGCLIENT(JMS) MSGBODY(UNSPECIFIED) MDWRITE(YES)

END

После выполнения стандартных команд на генерацию должен получится файл «.binding».

1. **Генерация и подпись SSL-сертификатов.** 
   1. Генерация личных сертификатов.

Для генерации личного сертификата необходимо знать его DN.

Например:

DN сертификата: <CN=”\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*”, OU=”\*\*\*\*”, O=”\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*”, C=”\*\*”>

Для создания хранилища на сервере с Weblogic выполняем:

keytool -genkey -keyalg RSA -keysize 2048 -dname "DN сертификата" -alias «имя алиаса» -keypass "пароль" -keystore «путь до файла хранилища ключей .jks(пример: c:/app/sec/keystoretest.jks)» -storepass "пароль"

Для генерации запроса на подписание сертификата на сервере с Weblogic выполняем:

keytool -certreq -alias «имя алиса личного сертификата» -file «путь к файлу на подпись .pem» -keypass "пароль" -keystore «путь до файла хранилища ключей .jks» -storepass "пароль"

Отправляем на подпись полученный файл \*.pem

Получаем подписанный личный сертификат:\*.pem и импортируем его в хранилище сертификатов:

keytool -import -alias «имя алиса личного сертификата» -file «путь к подписанному сертификату .pem» -keypass "пароль" -keystore « путь до файла хранилища ключей .jks »-storepass "пароль"

* 1. Импорт доверенных сертификатов (trust).

При подписании сертификатов необходимо от администраторов MQ-сервера получить несколько доверенных сертификатов (trusted) и выполнить их импорт в общее хранилище ключей на Weblogic поочередно:

keytool -import -trustcacerts -alias «имя алиса доверенного сертификата» -file «путь к доверенному сертификату .cer» -keypass "пароль" -keystore « путь до файла хранилища ключей .jks »-storepass "пароль"

1. **Настройка файла файла java.security.**

Файл находится на сервере с Weblogic:

JDK\_HOME/jre/lib/security/java.security

В данном файле необходимо закомментировать следующие строки:

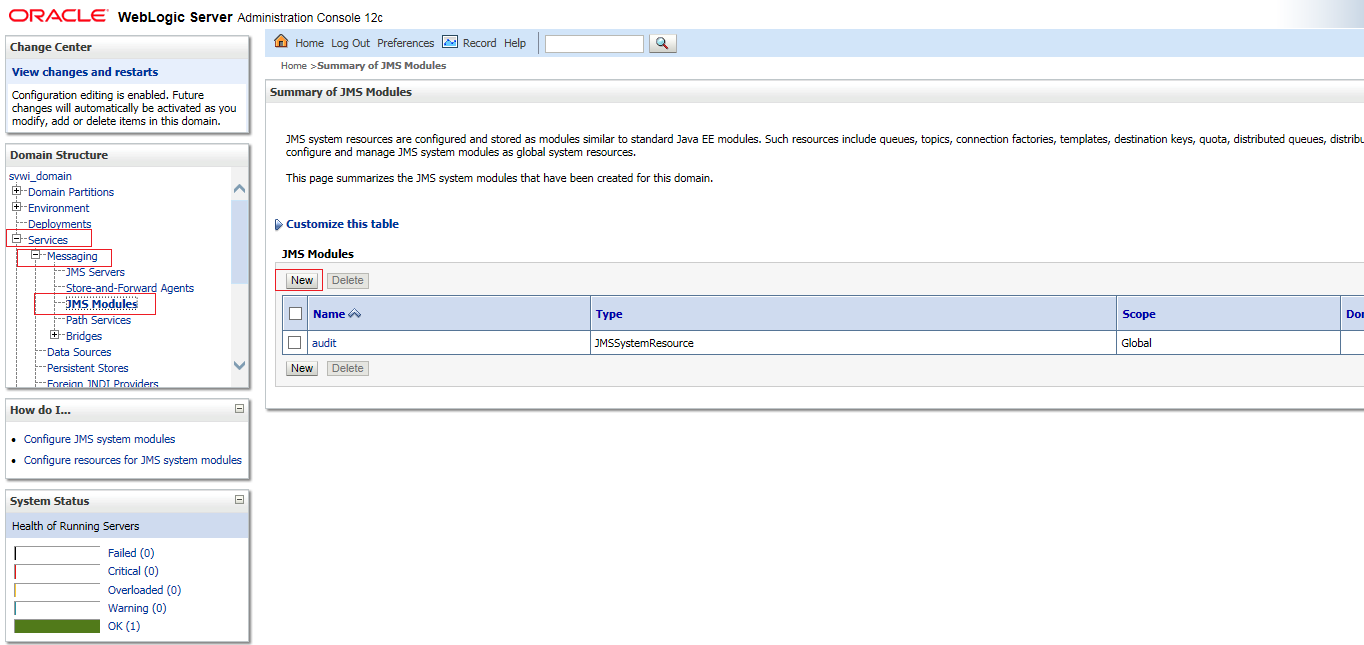
jdk.certpath.disabledAlgorithms=MD2\*

jdk.tls.disabledAlgorithms=MD5\*

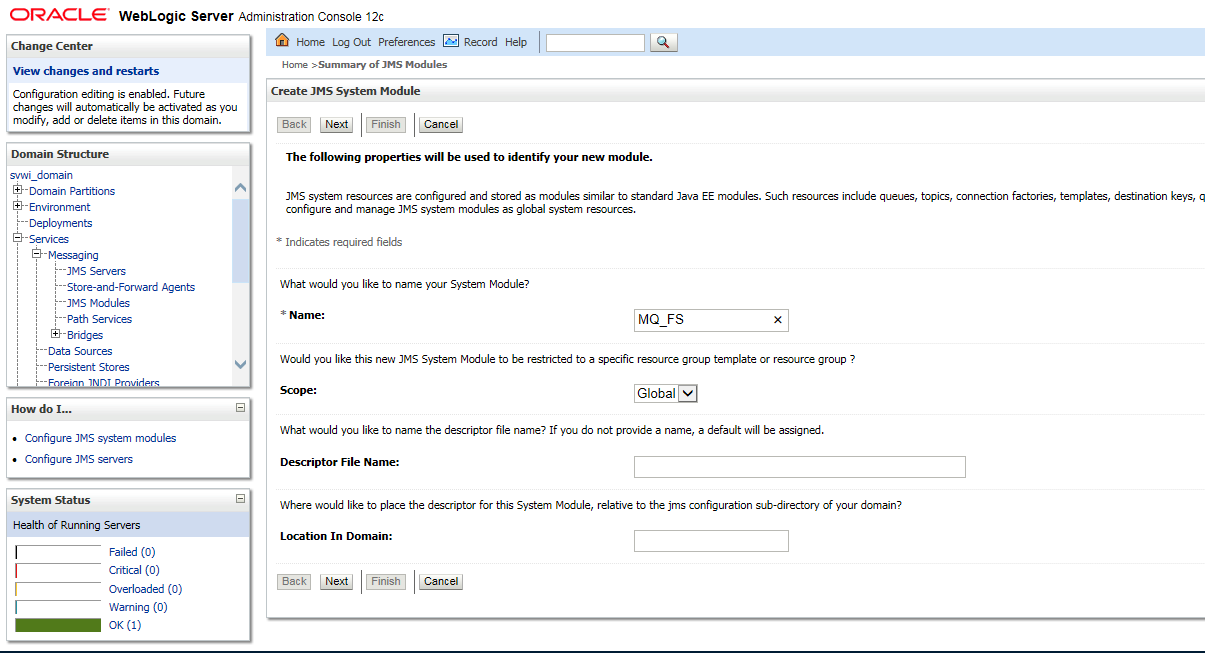
jdk.tls.disabledAlgorithms=SSLv3

1. **Настройка Weblogic**
   1. Создание JMS-модуля

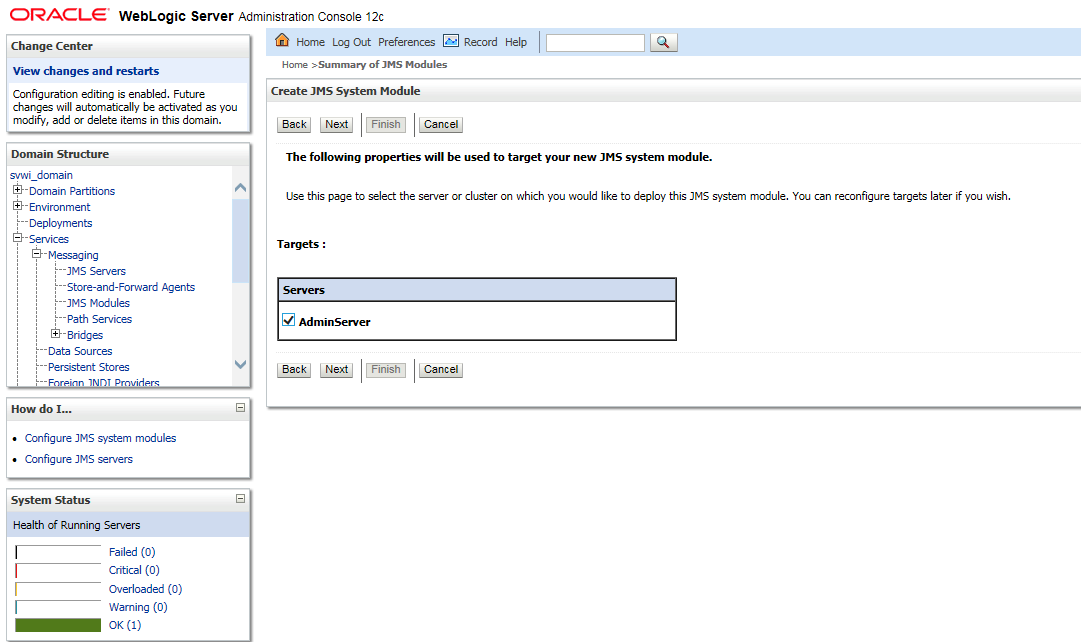
Необходимо перейти в консоли администратора Weblogic в Services -> Messaging -> JMS Modules и нажать New:



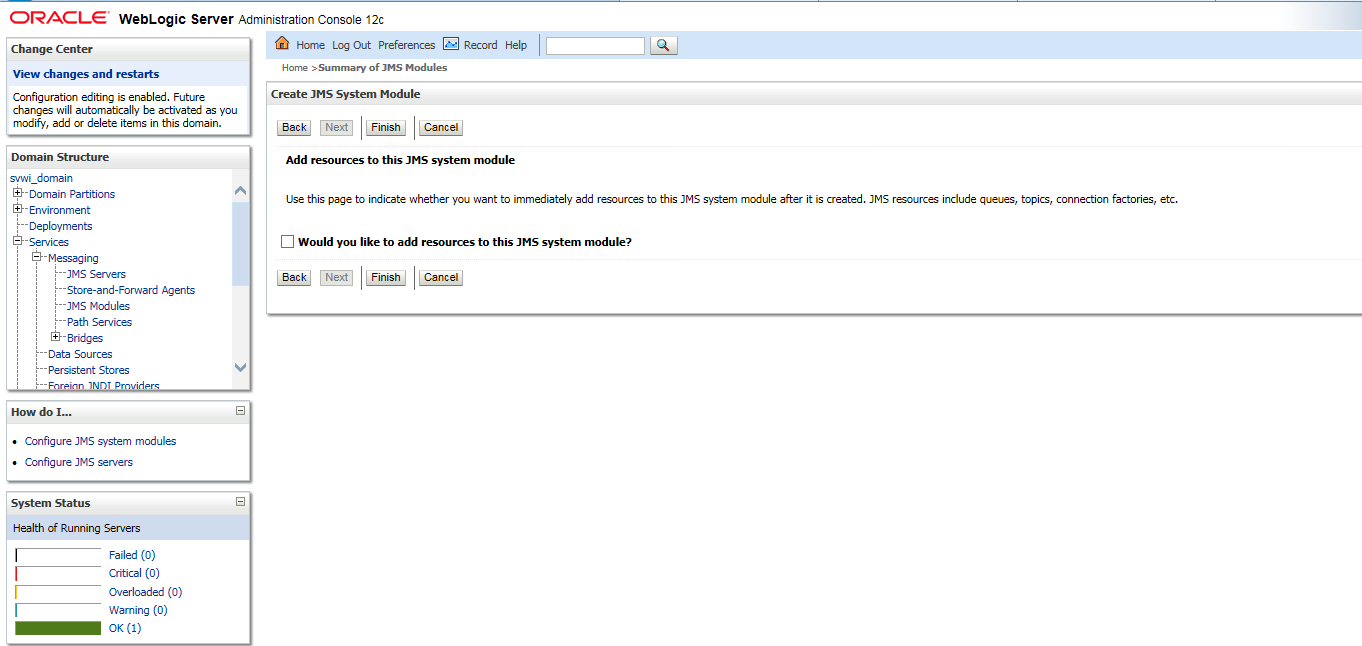
Указать имя (Name), например «MQ\_FS»:



Указать Target, например AdminServer и нажать Next:

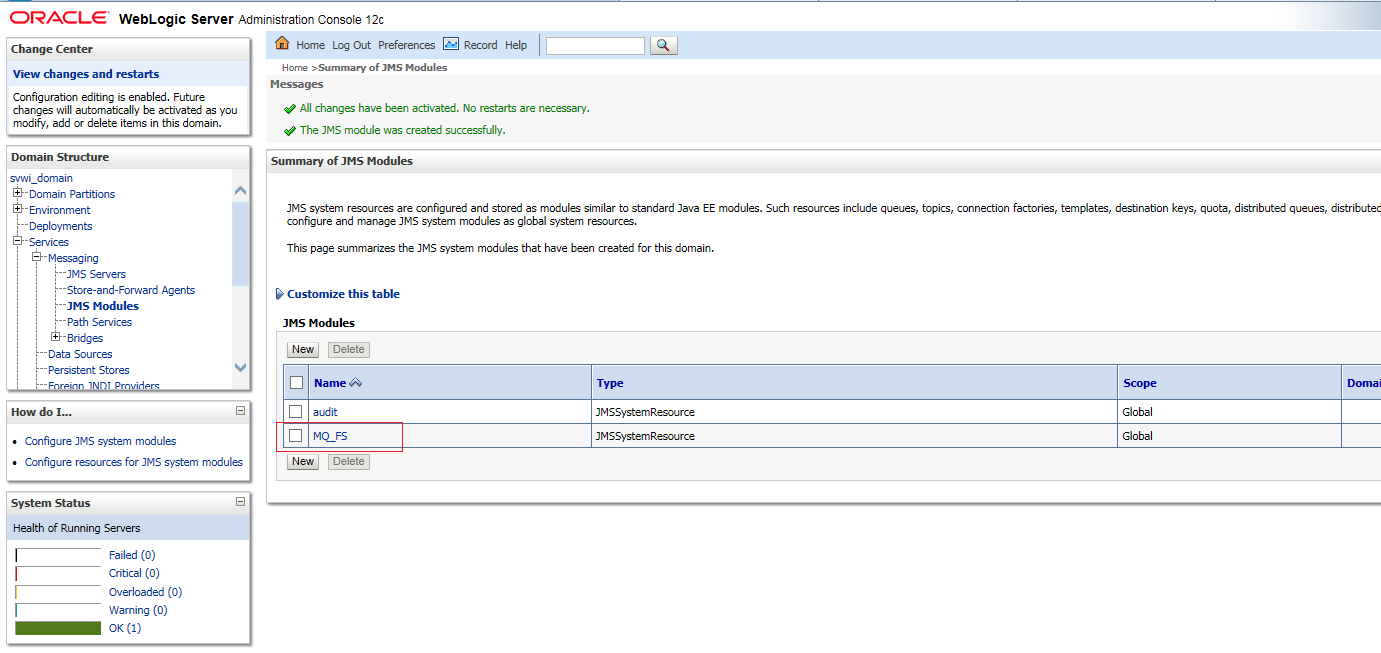


Нажать Finish:

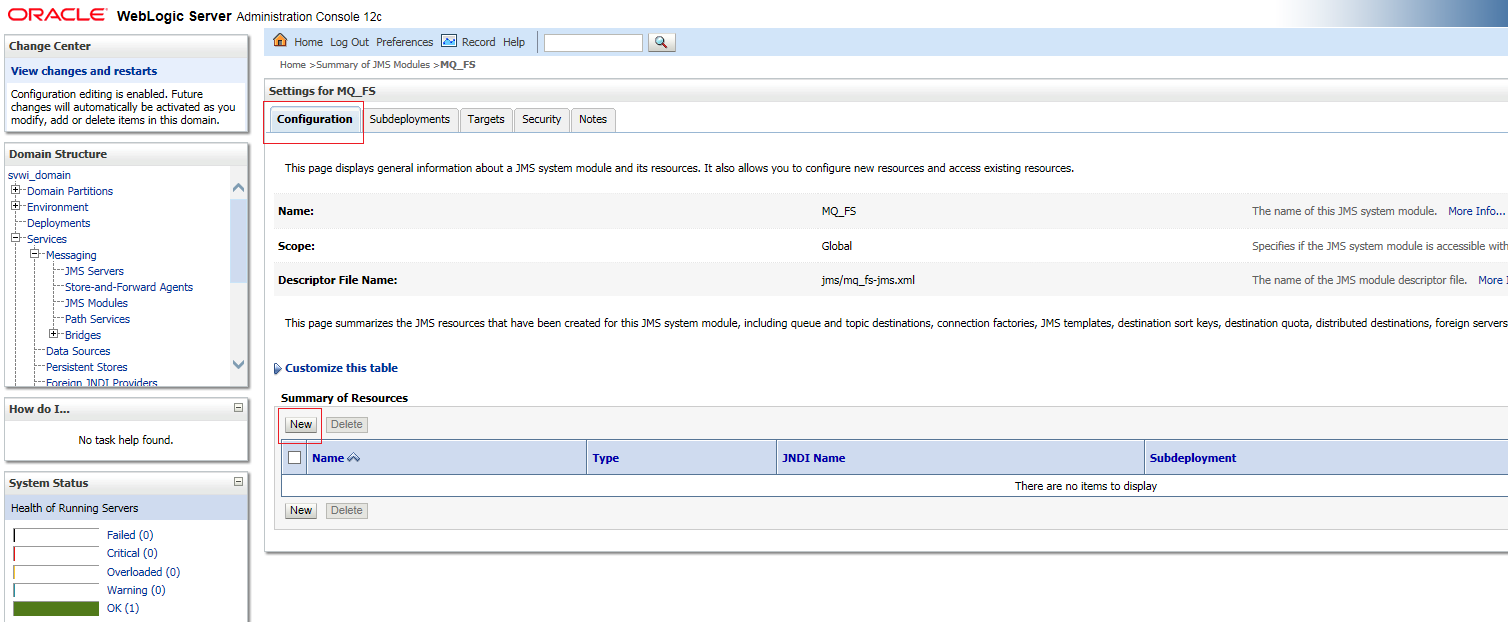


* 1. Создание JMS-ресурса

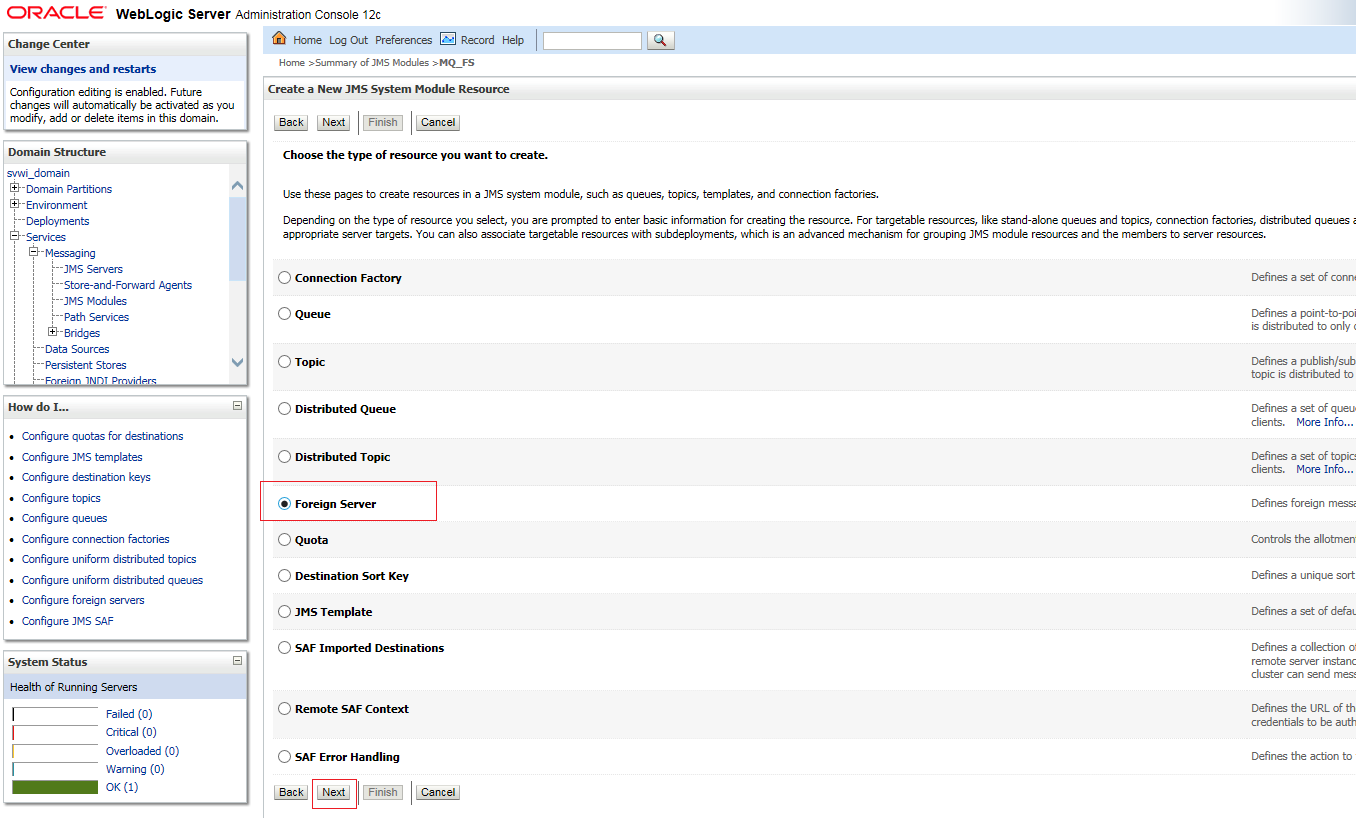
Выбрать, созданный в пункте 4.1. модуль “MQ\_FS”:



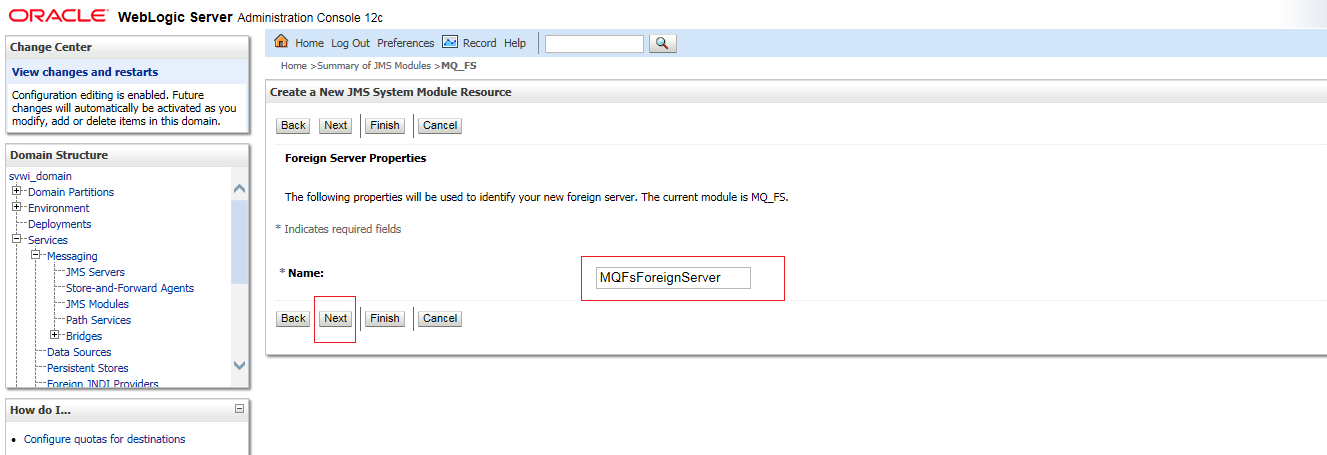
На вкладке «Configuration» нажать New:



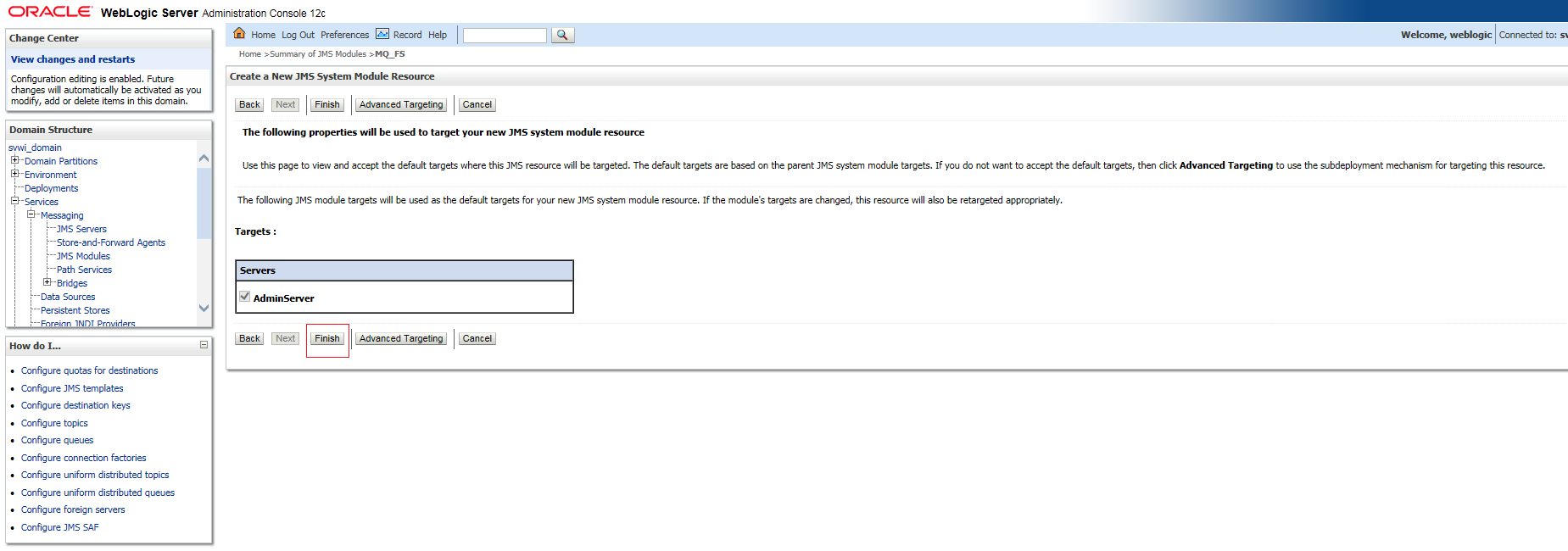
Выбрать Foreign Server и нажать Next:



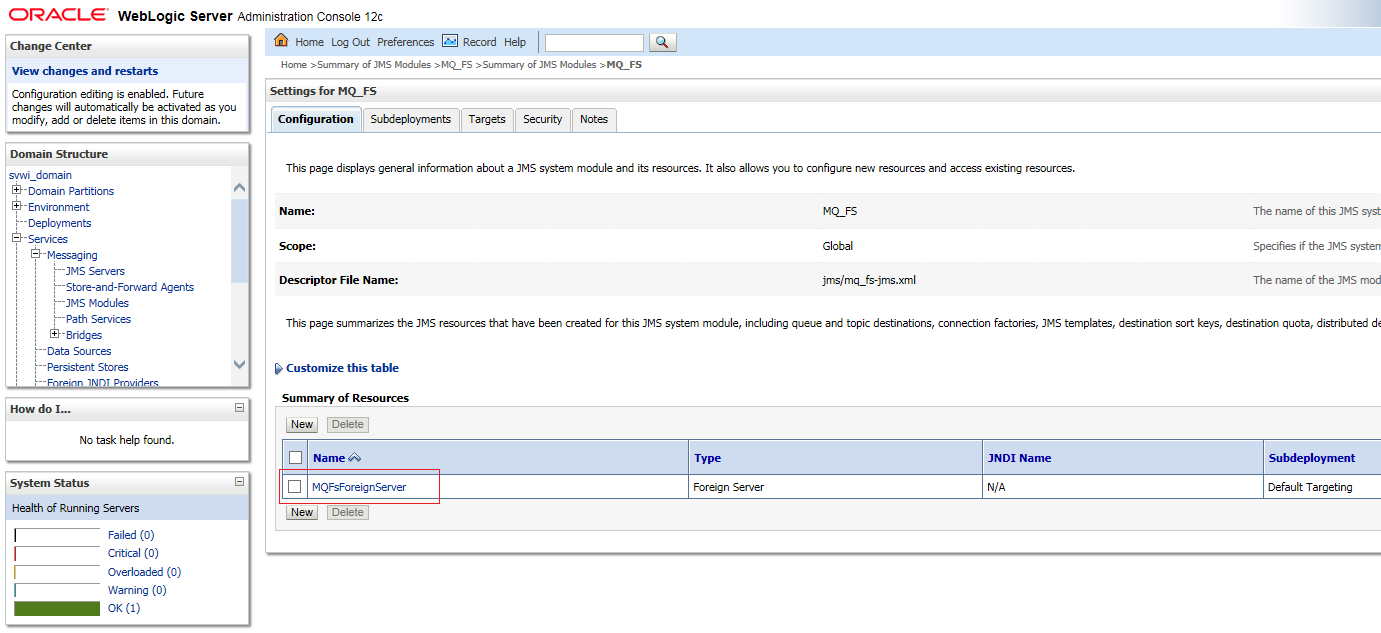
Ввести Name, например “MQFsForeignServer” и нажать Next:



Нажать Finish:



Выбрать только что созданный ресурс:

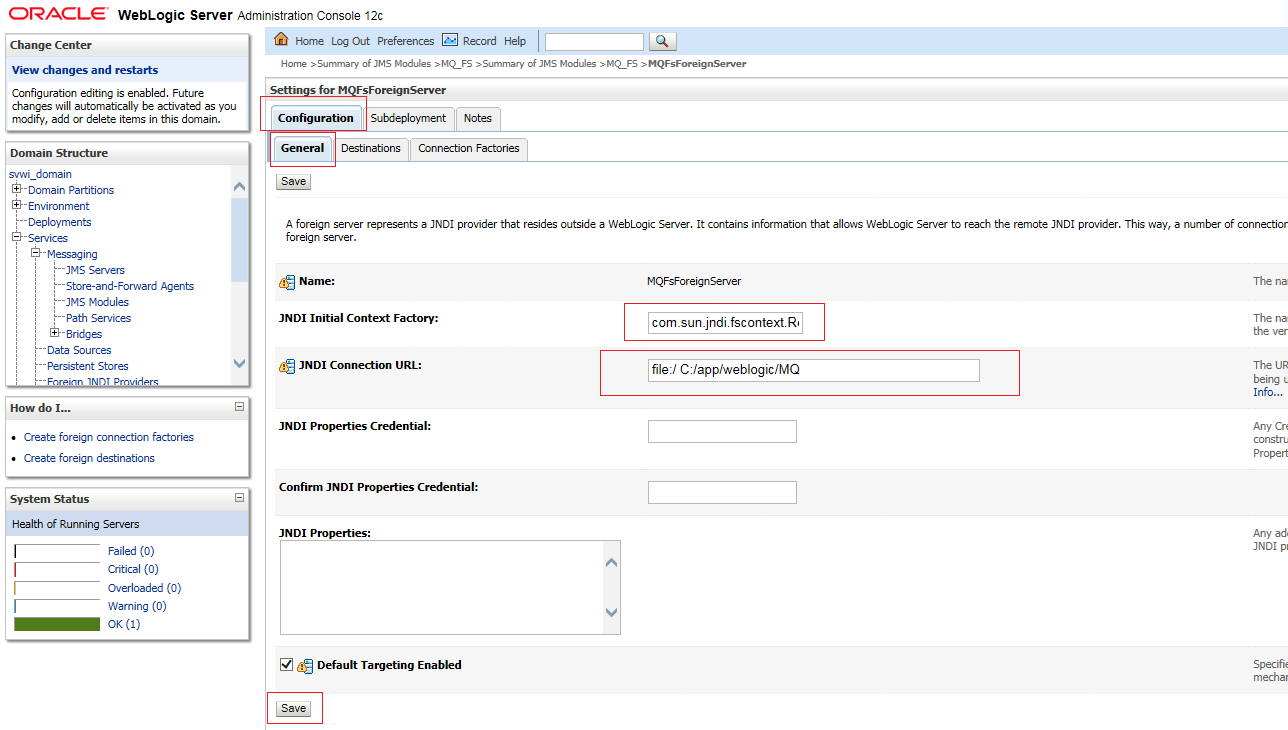


Во вкладке Configuration -> General заполнить следующие поля:

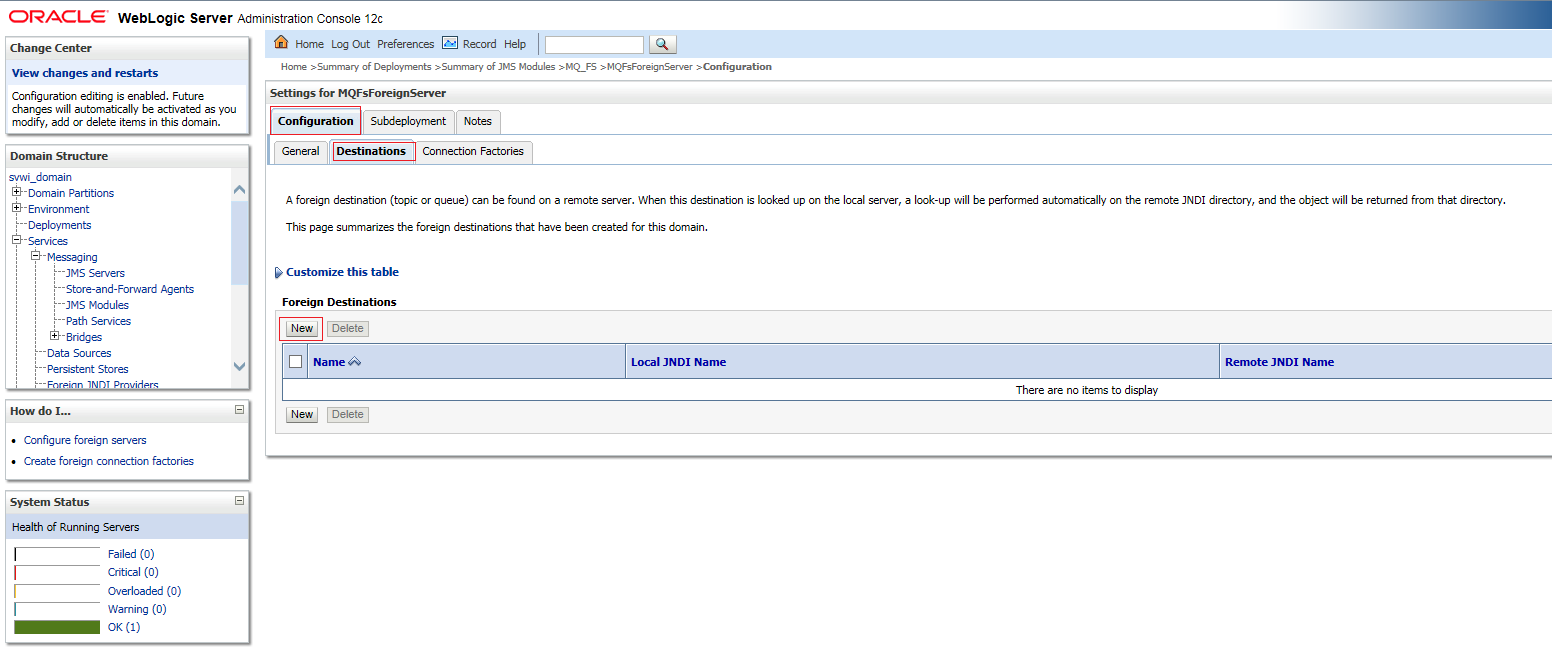
JNDI Initial Context Factory: “com.sun.jndi.fscontext.RefFSContextFactory”

Необходимо поместить в папку на сервере с Weblogic файл “.bindings”, полученный в пункте 1 и указать в следующем параметре:

JNDI Connection URL: “file:/ C:/app/weblogic/MQ” (в данном случае указан пример папки расположения файла). Нажать Save:



Перейти на вкладку Destination:



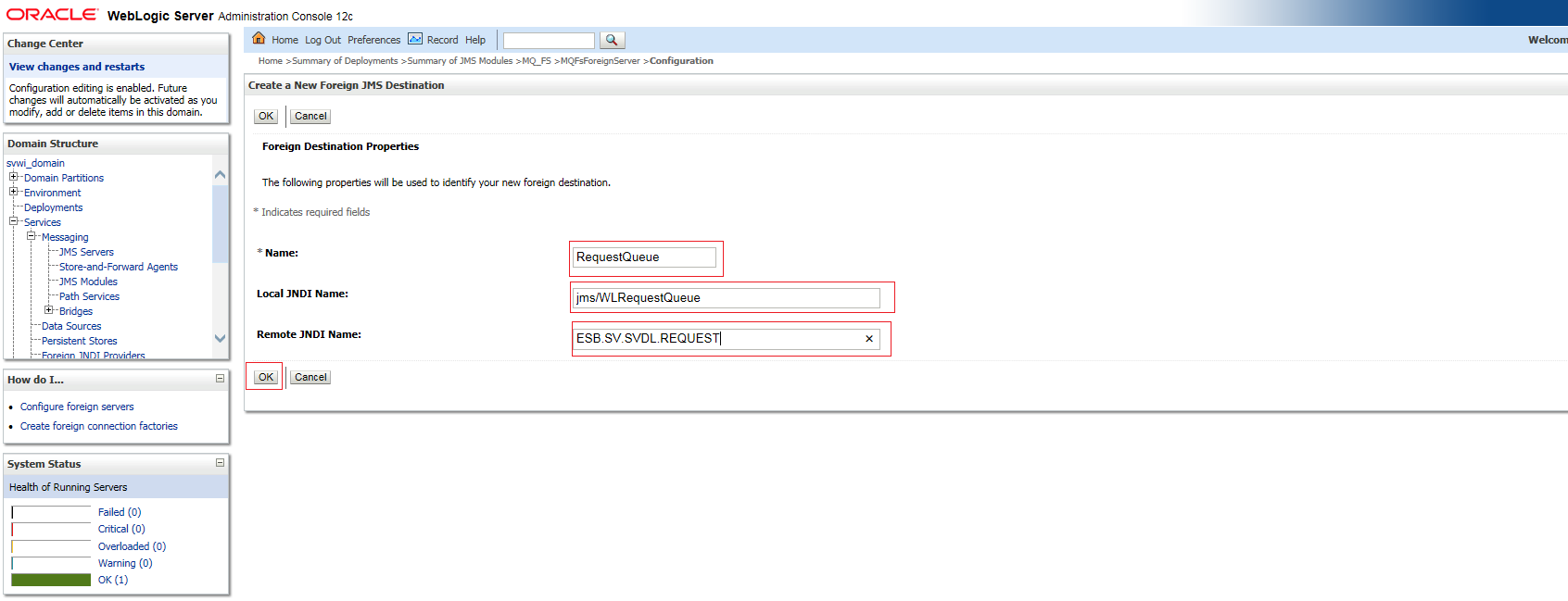
На страннице создания очереди заполнить поля:

Name: Имя очереди

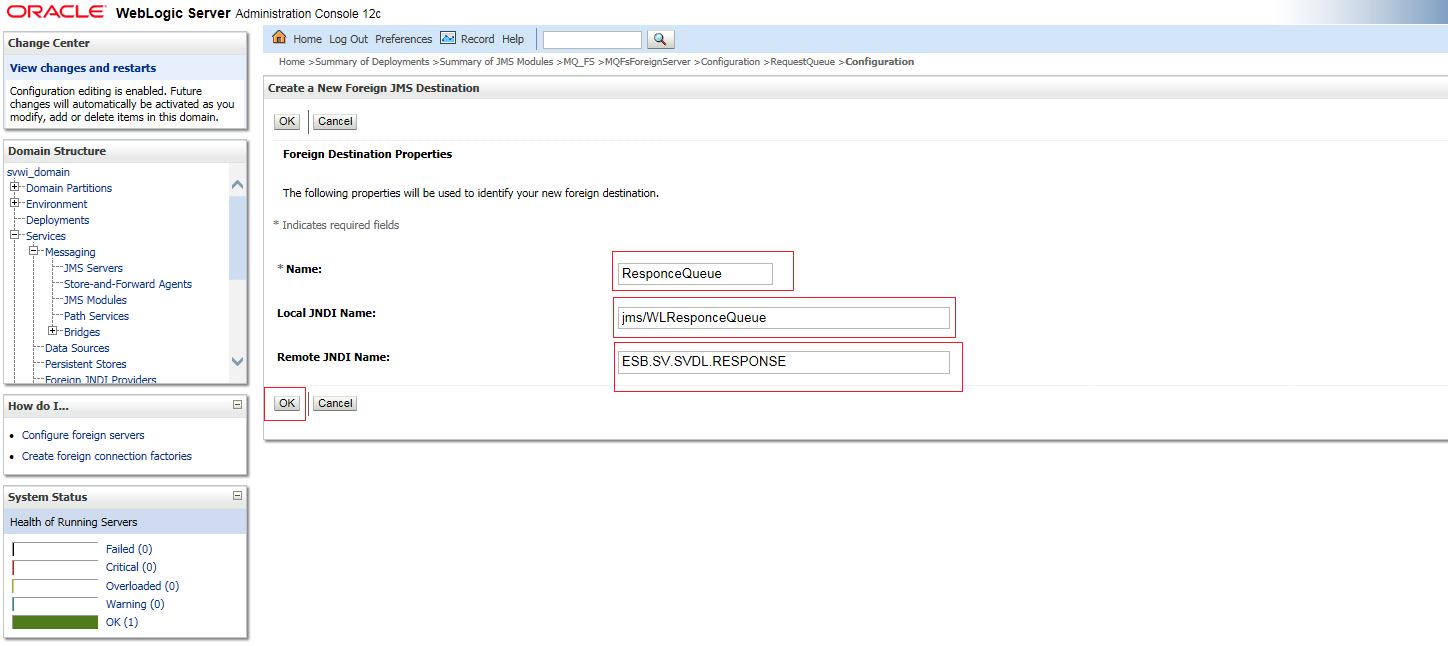
Local JNDI Name: Локальное JNDI имя, используемое приложением

Remote JNDI Name: имя очереди в .binding-файле (параметр «Q» в пункте 1).

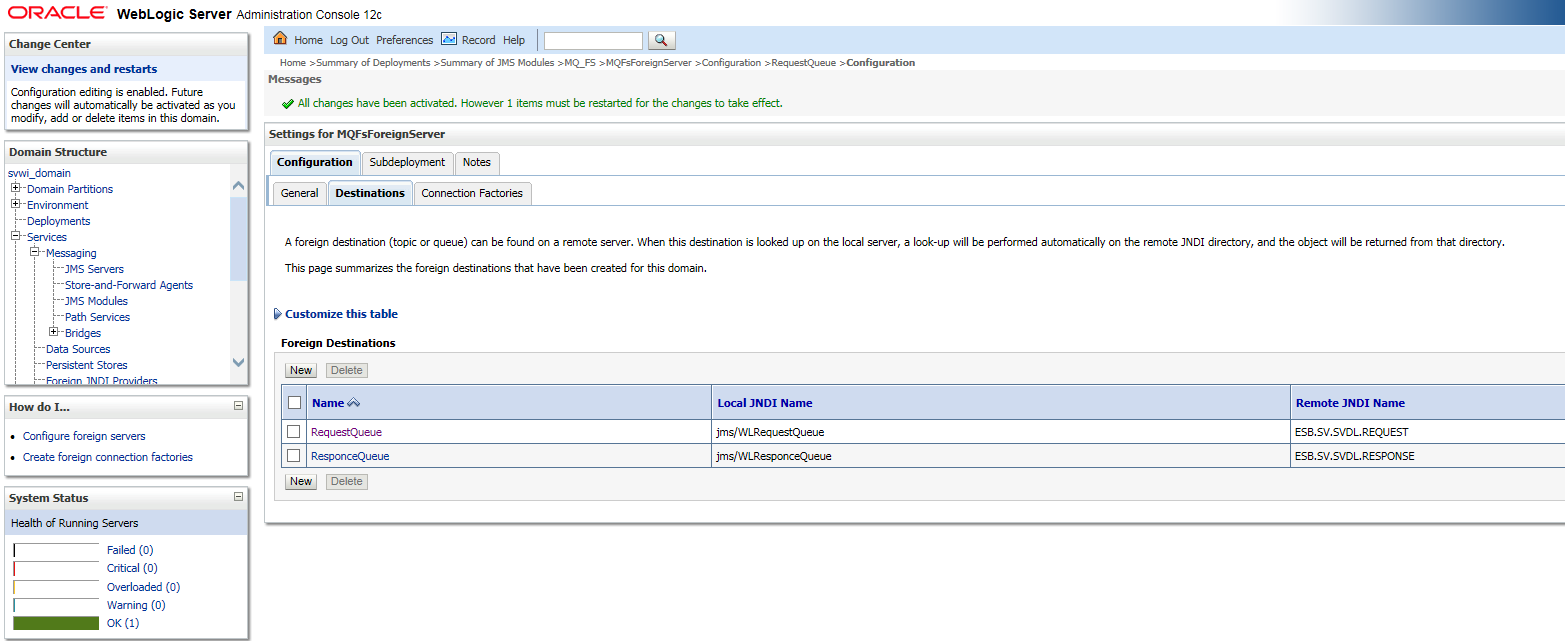
Нажать Ок:



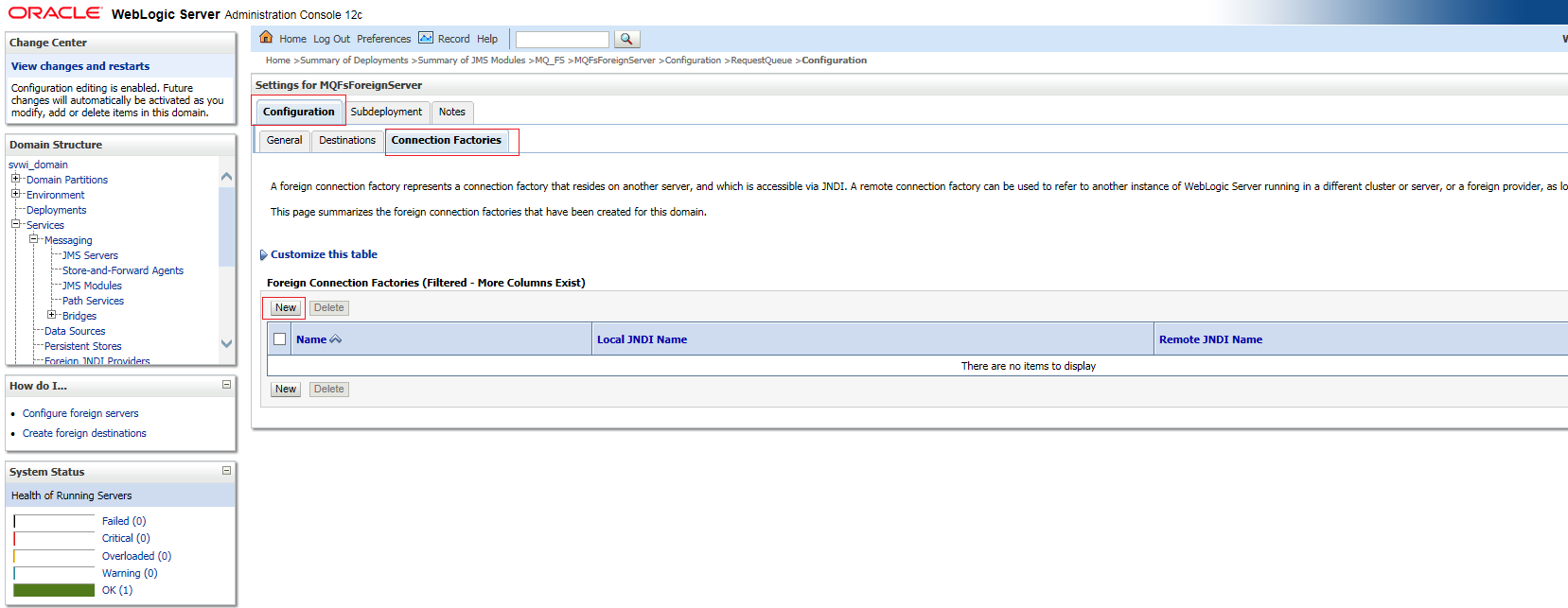
Аналогичным образом создать очередь для ответа:



Получаем 2 очереди:



После этого переходим на вкладку Connection Factories и нажимаем New:



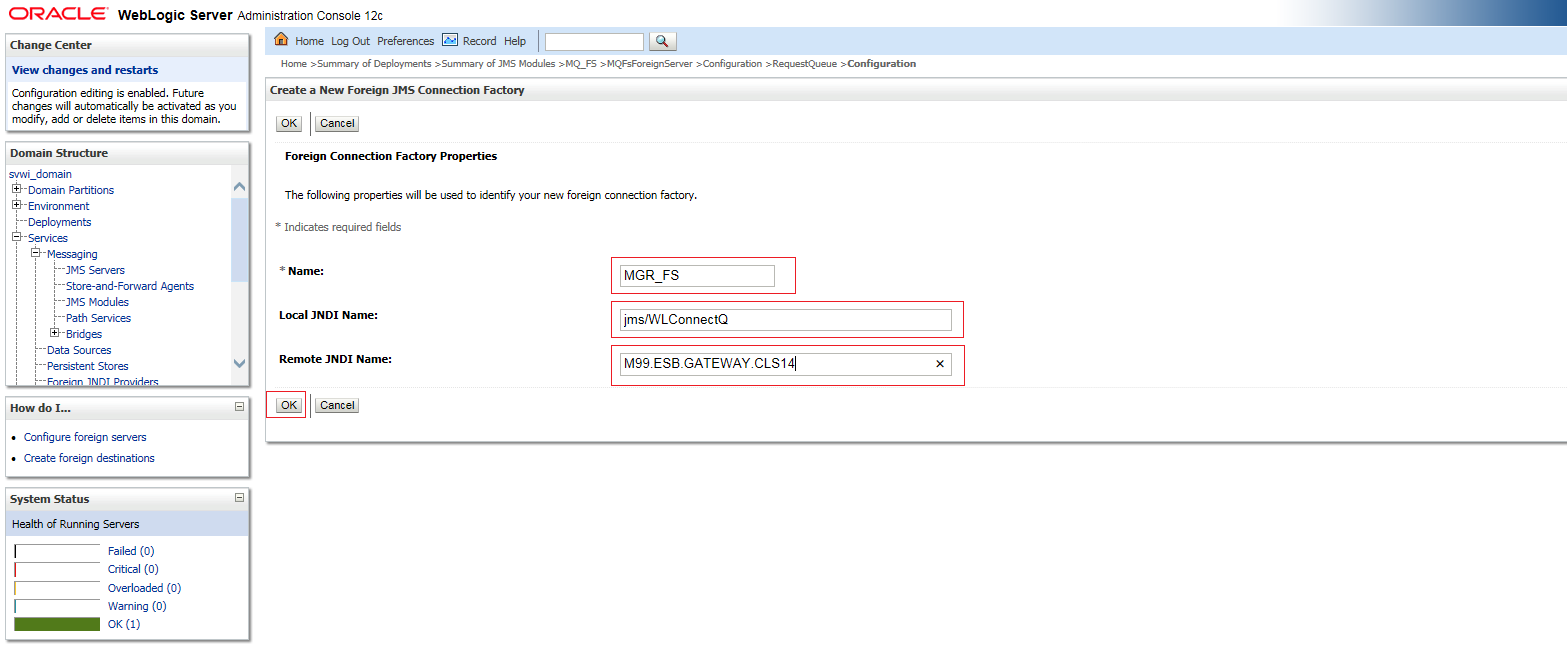
В окне создания фабрики соединений необходимо заполнить следующие поля:

Name: Имя фабрики соединений

Local JNDI Name: локальное JNDI имя для использования приложением

Remote JNDI Name: имя менеджера очередей из .bindings-файла (имя параметра” xacqf” пункт 1).

Нажимаем Ок:



* 1. Прописывание библиотек.

Из MQ-сервера необходимо собрать следующие библиотеки:

com.ibm.mq.allclient.jar

com.ibm.mq.commonservices.jar

com.ibm.mq.jar

com.ibm.mq.jmqi.jar

com.ibm.mqetclient.jar

com.ibm.mqjms.jar

dhbcore.jar

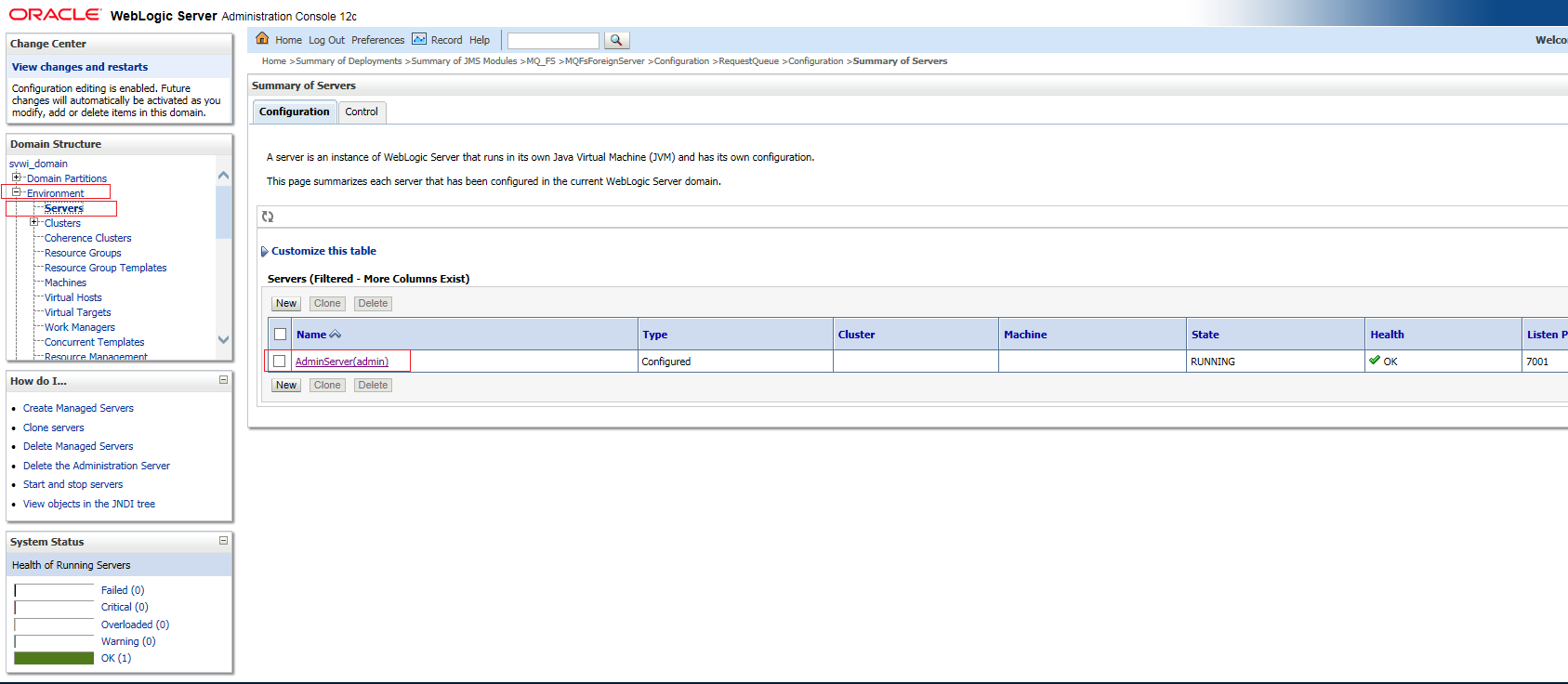
fscontext.jar

providerutil-1.2.1.jar

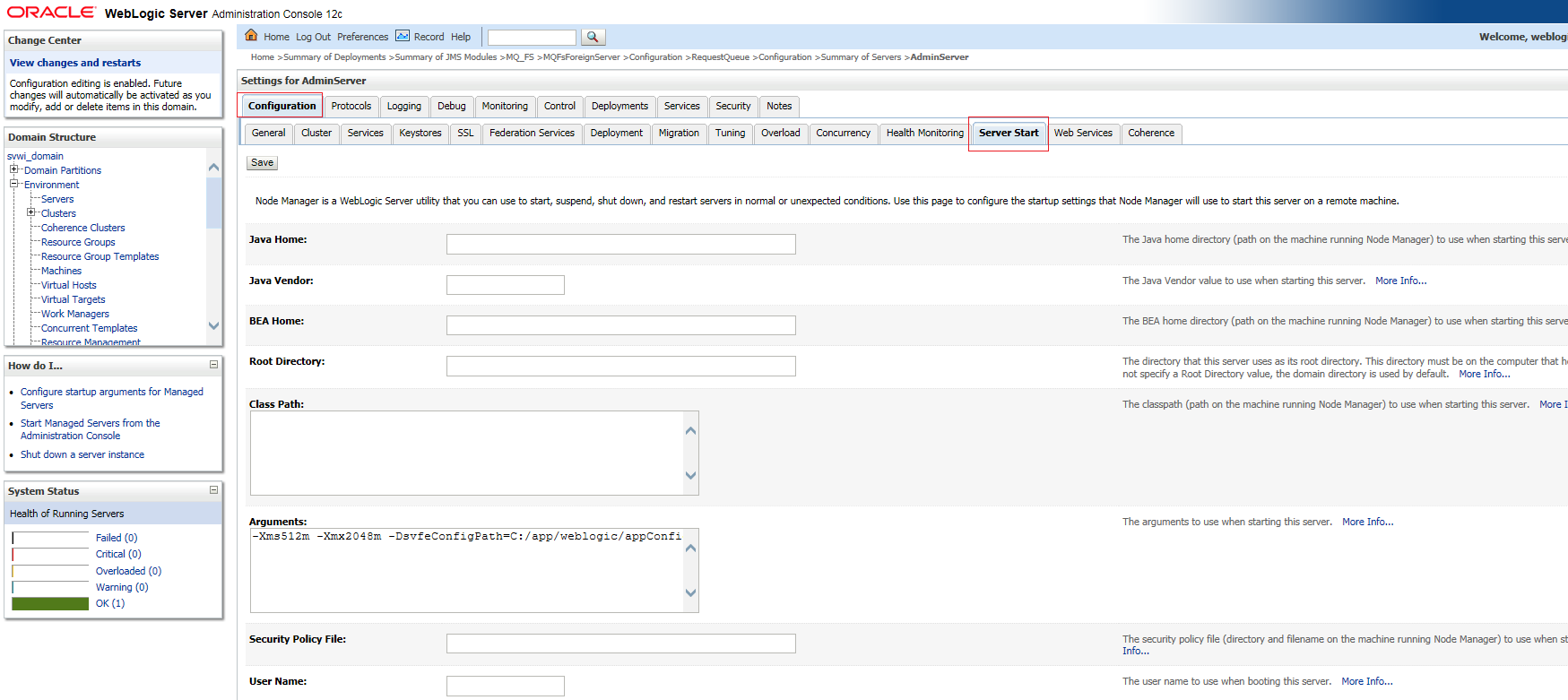
После получения их необходимо расположить на сервере с Weblogic в любой заданной директории.

Затем необходимо прописать пути до этих библиотек.

Для этого необходимо в консоли администратора weblogic перейти в Environment -> Servers и нажать на нужный нам сервер:



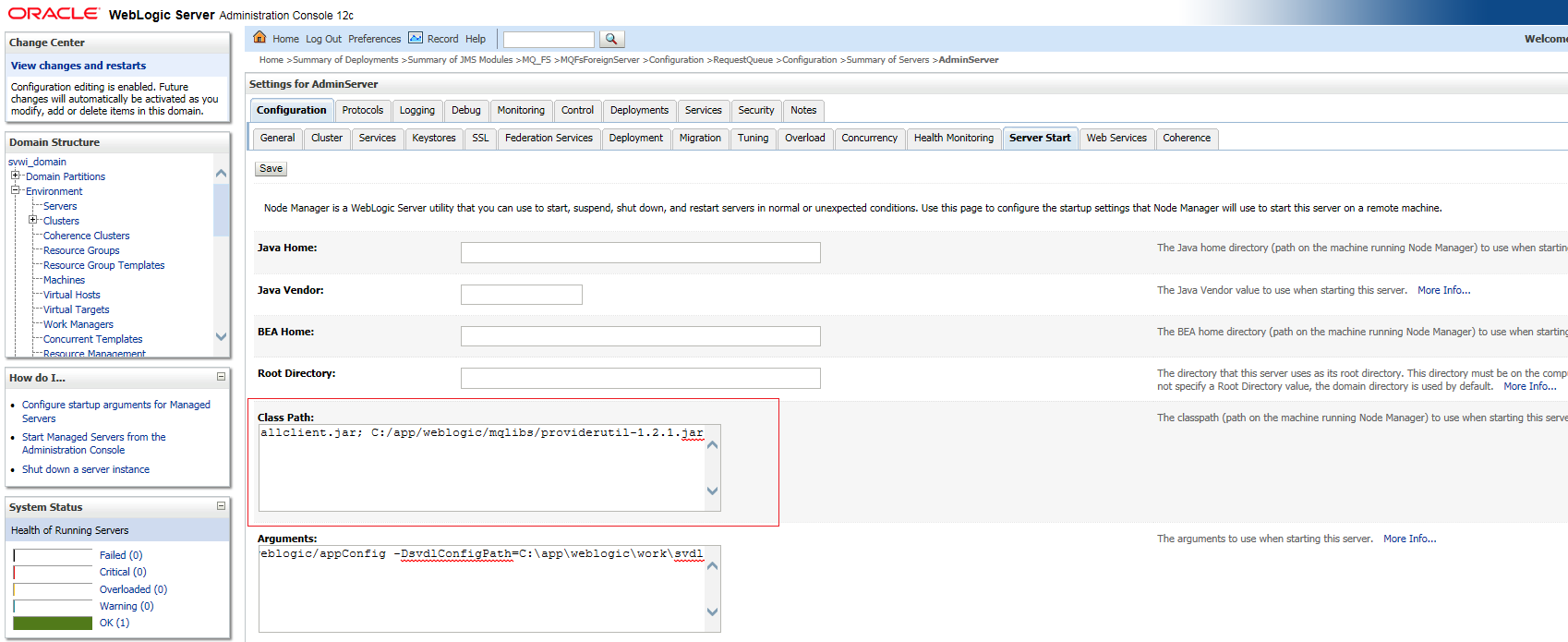
После этого необходимо перейти во вкладку Configuration -> Server Start:



В параметре Class Path необходимо прописать пути до библиотек следующим образом:

C:/app/weblogic/mqlibs/com.ibm.mq.jar; C:/app/weblogic/mqlibs/com.ibm.mqjms.jar; C:/app/weblogic/mqlibs/dhbcore.jar; C:/app/weblogic/mqlibs/fscontext.jar; C:/app/weblogic/mqlibs/com.ibm.mqetclient.jar; C:/app/weblogic/mqlibs/com.ibm.mq.commonservices.jar; C:/app/weblogic/mqlibs/com.ibm.mq.jmqi.jar; C:/app/weblogic/mqlibs/com.ibm.mq.allclient.jar; C:/app/weblogic/mqlibs/providerutil-1.2.1.jar

И нажать Save:



* 1. Параметры запуска Java.

В той же вкладке, в которой закончили работу в пункте 4.3. необходимо задать дополнительные параметры в поле Arguments:

-Dweblogic.security.SSL.protocolVersion=TLS1 -Dweblogic.security.SSL.nojce=true -Dweblogic.security.SSL.minimum.ProtocolVersion=TLSv1 -Djavax.net.ssl.trustStore=”путь до хранилища ключей из пункта 2”-Djavax.net.ssl.keyStore=” путь до хранилища ключей из пункта 2” -Djavax.net.ssl.keyStorePassword=”пароль для хранилища”

После нажать Save.

После выполнения всех настроек необходимо перезапустить сервер с Weblogic.

Подключение к очередям выполняем по параметрам:

Connection Factory: jms/WLConnectQ

Queue Req: jms/WLRequestQueue

Queue Res: jms/WLResponceQueue