Oracle WebLogic Server

Integration Guide

gemalto
security to be free

Document Number: 007-012420-001, Rev. M

Release Date: May 2018

Contents

Preface

This document is intended to guide administrators through the steps for Oracle WebLogic Server and SafeNet Luna HSM integration, and also covers the necessary information to install, configure, and integrate Oracle WebLogic Server with SafeNet Luna HSM.

Scope

This guide provides instructions for setting up a small test lab with Oracle WebLogic Server running with SafeNet Luna HSM for securing the SSL private keys. It explains how to install and configure software that is required for setting up a SSL on Oracle WebLogic Server while storing private key on SafeNet Luna HSM.

This guide is intended for experienced administrators responsible for the planning, implementation, and deployment of WebLogic Server. Administrators are expected to understand WebLogic Server concepts and be familiar with Administrative Console.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION: Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

WARNING: Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following: • Command-line commands and options (Type **dir /p**.) • Button names (Click **Save As**.) • Check box and radio button names (Select the **Print Duplex** check box.) • Window titles (On the **Protect Document** window, click **Yes**.) • Field names (**User Name:** Enter the name of the user.) • Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) • User input (In the **Date** box, type **April 1**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
`Consolas`	Denotes syntax, prompts, and code examples.

Support Contacts

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1
Introduction

Overview

SafeNet Luna HSM integrates with the Oracle WebLogic Server to provide significant performance improvements by off-loading cryptographic operations from the Server to SafeNet Luna HSM. In addition, SafeNet Luna HSM provides extra security by protecting and managing the server's high value SSL private key within a FIPS 140-2 certified hardware security module.

Understanding the Oracle WebLogic Server

Oracle WebLogic Server is a scalable, enterprise-ready Java Platform, Enterprise Edition (Java EE) application server. The WebLogic Server infrastructure supports the deployment of many types of distributed applications and is an ideal foundation for building applications based on Service Oriented Architectures (SOA). SOA is a design methodology aimed at maximizing the reuse of application services.

The WebLogic Server complete implementation of the Java EE 6.0 specification provides a standard set of APIs for creating distributed Java applications that can access a wide variety of services, such as databases, messaging services, and connections to external enterprise systems. End-user clients access these applications using Web browser clients or Java clients. It also supports the Spring Framework, a programming model for Java applications which provides an alternative to aspects of the Java EE model.

In addition to the Java EE implementation, WebLogic Server enables enterprises to deploy mission-critical applications in a robust, secure, highly available, and scalable environment. These features allow enterprises to configure clusters of WebLogic Server instances to distribute load, and provide extra capacity in case of hardware or other failures.

3rd Party Application Details

- Oracle WebLogic Server

Supported Platforms

SafeNet Luna HSM (v7.x)

Oracle WebLogic Server	Platforms Tested	SafeNet Luna HSM Appliance version and Firmware	SafeNet Luna HSM Client Software version	JDK
WLS 12.2.1.3	RHEL 7(64 bit)	7.2.0 f/w 7.2.0	7.2.0	Oracle JDK 1.8_131
WLS 12.2.1.1	RHEL 7(64 bit)	7.1.0 f/w 7.1.0	7.1.0	Oracle JDK 1.8_91
WLS 12.2.1.1	RHEL 7(64 bit)	7.0.0 f/w 7.0.1	7.0.0	Oracle JDK 1.8_91

SafeNet Luna HSM (v5.x/6.x)

Oracle WebLogic Server	Platforms Tested	SafeNet Luna HSM Appliance version and Firmware	SafeNet Luna HSM Client Software version	JDK
WLS 12.2.1	RHEL 7.0(64 bit)	6.3.0 f/w 6.27.0 and 6.10.9	6.x (v6.3.0)	Oracle JDK 1.8.0_91
WLS 12.2.1	RHEL 6.5(64 bit)	6.2.2 f/w 6.24.3 and 6.10.9	6.x (v6.2.2)	Oracle JDK 1.8.0_91
WLS 12.2.1	RHEL 6.5(64 bit)	6.2.1 f/w 6.24.2 and 6.10.9	6.x (v6.2.1)	Oracle JDK 1.8.0_91
WLS 12.1.2	RHEL 6.5(64 bit)	6.2.0 f/w 6.24.0 and 6.10.9	6.x (v6.2)	Oracle JDK 1.7.0_79
WLS 12.1.2	RHEL 7.0(64 bit)	6.0.0 f/w 6.22.0	6.x (v6.1)	Oracle JDK 1.7.0_79

Oracle WebLogic Server	Platforms Tested	SafeNet Luna HSM Appliance version and Firmware	SafeNet Luna HSM Client Software version	JDK
WLS 12.1.2	RHEL 6.0(64 bit) RHEL 6.2(64 bit)	5.4.1 f/w 6.21.0	5.x (v5.0.x, 5.1.x, 5.2.x, 5.3.x, 5.4.x)	Oracle JDK 1.7.0_51
WLS 10.3.6	RHEL 5.5 (64 bit) RHEL 6.2 (64 bit) RHEL 6.0 (64 bit) Solaris 10 SPARC v9 (32 bit)	5.4.0 f/w 6.21.0	5.x (v5.0.x, 5.1.x, 5.2.x, 5.3.x, 5.4.x)	Oracle JRockit 1.6.0_45 Oracle JDK 1.6.0_45 Oracle JDK 1.7.0_25 Oracle JDK 1.7.0_72
WLS 10.3.5	RHEL 5.8(64 bit) RHEL 6.2(64 bit)	5.2.1 f/w 6.10.1	5.x (v5.0.x, 5.1.x, 5.2.x, 5.3.x, 5.4.x)	Oracle JDK 1.6.0_45

NOTE: This integration is tested with Luna Clients in HA and FIPS Mode also.

Prerequisites

Configuring SafeNet Luna Network HSM 7.x

SafeNet Luna Network HSM allows to create Per-Partition Security Officer (PPSO) partition. HSM Administrator is not Security Officer (SO) for PPSO partitions. The HSM SO/Administrator elects to create a partition as PPSO-type, which creates an empty structure that is handed to the new owner, who initializes the partition to create the Partition Security Officer (PSO) role or identity for management functions. The PSO in turn creates the partition Crypto Officer (CO) to control client cryptographic operations on the partition.

Refer to the SafeNet Luna HSM documentation for installation steps and details regarding the configuration and setup of the box on UNIX/Windows systems. Before you get started ensure the following:

- SafeNet Luna Network HSM appliance and a secure admin password.
- SafeNet Luna Network HSM, and a hostname, suitable for your network.
- SafeNet Luna Network HSM network parameters are set to work with your network.
- Initialize the HSM on the SafeNet Luna Network HSM appliance.
- Create and exchange certificates between the SafeNet Luna Network HSM and your Client system.
- Create a partition on the HSM that will be later used by Weblogic Server.

- Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from SafeNet Luna HSM. The general form of command is "`C:\Program Files\SafeNet\LunaClient> vtl verify`" for Windows and "`/usr/safenet/lunaclient/bin/vtl verify`" for Unix.
- Initialize the Partition as mentioned in steps below for Password/PED based respectively.
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Luna Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Initialize the Partition SO and Crypto Officer Roles on a PW-Auth Partition

These instructions assume a password-authenticated SafeNet Luna Network HSM that has been initialized, and an application partition has been created, capable of having its own Security Officer.

- **Initialize the Partition SO role**

  Set the active slot to the created, uninitialized, application partition.
  Type **slot set -slot <slot number>**

```
lunacm:> slot set -slot 0
Current Slot Id:    0     (Luna User Slot 7.0.0 (Password) Signing With Cloning Mode)
Command Result : No Error
```

  Initialize the application partition, to create the partition's Security Officer (SO).
  Type **partition init -label <partition label>**

```
lunacm:> par init -label <part_label> –password <part_password>
         You are about to initialize the partition.
         All partition objects will be destroyed.
         Are you sure you wish to continue?
         Type 'proceed' to continue, or 'quit' to quit now -> proceed
Command Result: No Error
```

- **Initialize the Crypto Officer role**

  a. The SO of the application partition can now assign the first operational role within the new partition.
  Type **role login -name Partition SO**.

```
lunacm:> role login -name Partition SO
```

  b. Type **role init -name Crypto Officer**.

```
lunacm:> role init -name Crypto Officer
```

  c. The application partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, the SO must log out to allow the Crypto Officer to log in.
  Type **role logout**.

```
lunacm:> role logout
```

Initialize the Partition SO and Crypto Officer Roles on a PED-Auth Partition

These instructions assume a PED-authenticated SafeNet Luna Network HSM that has been initialized, and an application partition has been created, capable of having its own Security Officer.

Take the following steps to initialize the PSO and CO roles:

- **Initialize the Partition SO role**

  Set the active slot to the created, uninitialized, application partition.
  Type **slot set -slot <slot number>**

```
lunacm:> slot set -slot 0
```

```
Current Slot Id:    0     (Luna User Slot 7.0.0 (PED) Signing With Cloning Mode)

Command Result : No Error
```

Initialize the application partition, to create the partition's Security Officer (SO).
Type **partition init -label <partition label>**

```
lunacm:> par init -label <part_label>
         You are about to initialize the partition.
         All partition objects will be destroyed.
         Are you sure you wish to continue?
         Type 'proceed' to continue, or 'quit' to quit now -> proceed
         Please attend to the PED.
         Respond to SafeNet PED prompts...
Command Result : No Error
```

- **Initialize the Crypto Officer role**

  The SO of the application partition can now assign the first operational role within the new partition.

  Type **role login -name Partition SO**.

  Type **role init -name Crypto Officer**.

```
lunacm:> role init -name Crypto Officer
         Please attend to the PED.
         Respond to SafeNet PED prompts...

Command Result: No Error
```

The application partition SO can create the Crypto Officer, but only the Crypto Officer can create the Crypto User. Therefore, the SO must log out to allow the Crypto Officer to log in.

Type **role logout**.

Now, the Crypto Officer, or an application using the CO's challenge secret/password can perform cryptographic operations in the partition, as soon as the Crypto Officer logs in with **role login -name Crypto Officer**. However, the Crypto Officer can create, modify and delete crypto objects within the partition, in addition to merely using existing crypto objects (sign/verify). You can also create a limited-capability role called Crypto User that can use the objects created by the Crypto Officer, but cannot modify them.

NOTE: The black Crypto Officer PED key/Crypto Officer Password (In case of PW-Auth) is valid for the initial login only. You must change the initial credential on the key using the command **role changepw** during the initial login session, or a subsequent login. Failing to change the credential will result in a CKR_PIN_EXPIRED error while performing role-dependent actions.

Controlling User Access to the HSM

By default, only the root user has access to the HSM. You can specify a set of non-root users that are permitted to access the HSM, by adding them to the **hsmusers** group. The client software installation automatically creates the hsmusers group. The hsmusers group is retained when you uninstall the client software, allowing you to upgrade your client software while retaining your hsmusers group configuration.

Adding users to hsmusers group

To allow non-root users or applications access to the HSM, assign the users to the **hsmusers** group. The users you assign to the hsmusers group must exist on the client workstation. Users you add to the hsmusers group are able to access the HSM. Users who are not part of the hsmusers group are not able to access the HSM.

- **Adding a user to hsmusers group**

  a. Ensure that you have **sudo** privileges on the client workstation.

  b. Add a user to the hsmusers group.

  ```
  sudo gpasswd --add <username> hsmusers
  ```

  where `<username>` is the name of the user you want to add to the hsmusers group.

Removing users from hsmusers group

To revoke a user's access to the HSM, you can remove them from the hsmusers group.

- **Removing a user from hsmusers group**

  a. Ensure that you have **sudo** privileges on the client workstation.

  b. Remove a user from the hsmusers group.

  ```
  sudo gpasswd -d <username> hsmusers
  ```

  Where `<username>` is the name of the user you want to remove from the hsmusers group. You must log in again to see the change.

NOTE: The user you delete will continue to have access to the HSM until you reboot the client workstation.

Configuring SafeNet Luna Network HSM (v5.x/6.x)

Refer to the SafeNet Luna HSM documentation for installation steps and details regarding the configuration and setup of the box on UNIX systems. Before you get started ensure the following:

- SafeNet Luna Network HSM appliance and a secure admin password.
- SafeNet Luna Network HSM, and a hostname, suitable for your network.
- SafeNet Luna Network HSM network parameters are set to work with your network.
- Initialize the HSM on the SafeNet Luna Network HSM appliance.
- Create and exchange certificates between the SafeNet Luna Network HSM and your Client system.
- Create a partition on the HSM, remember the partition password that will be later used by Oracle WebLogic Server.
- Register the Client with the partition. And run the `"vtl verify"` command on the client system to display a partition from SafeNet Luna Network HSM. The general form of command is `"C:\Program Files\SafeNet\LunaClient> vtl verify"` for Windows and `"/usr/safenet/lunaclient/bin/vtl verify"` for Unix.
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Luna Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

NOTE: For Ped based SafeNet Luna HSM make sure ProtectedAuthenticationPathFlagStatus is set to '1' in Misc Section of Chrystoki.conf file.

Using Luna v6.x/7.x in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the SafeNet Luna HSM in FIPS mode, you have to make the following change in configuration file:

```
Misc = {
RSAKeyGenMechRemap = 1;
}
```

The above setting redirects the older calling mechanism to a new approved mechanism when SafeNet Luna HSM is in FIPS mode.

NOTE: The above configuration is valid for Luna 7.x and Luna 6.x (F/W Version 6.22.0 and above only).

Oracle WebLogic Server Setup

Post installing WebLogic Server apply a patch to support SafeNet Luna HSM.Patch information for the WebLogic Server is provided below:

- For Oracle WebLogic Server 12.1.2

  p17436068_121200_Generic.zip

- For Oracle WebLogic Server 10.3.6

  p17436068_1036_Generic.zip

- For Oracle WebLogic Server 10.3.5

  p17436068_1035_Generic.zip

NOTE: Refer to the ReadMe.txt for installing the patch or Oracle documentation to use smart update utility for applying the patch.

Before you install

Before installing the WebLogic Server you need to install the JDK. Download the JDK software from Oracle support site and install it. You can use the following JDK software available at Oracle Technology Network:

- Java Development Kit 8
- Java Development Kit 7

- Java Development Kit 6
- JRockit

After installing the JDK the following actions should be performed by the "root" user:

- Create a new group and user.

```
# groupadd -g 1000 oinstall
# useradd -u 1100 -g oinstall oracle
# passwd oracle
```

- Create the directories in which the Oracle software will be installed.

```
# mkdir -p /u01/app/oracle/middleware
# chown -R oracle:oinstall /u01
# chmod -R 775 /u01/
```

After creating the user/group and directories for WebLogic Server, logged in as “oracle” user and run the installer. Create the WebLogic domain and apply the appropriate patch to support SafeNet Luna HSM.

2

Integrate SafeNet Luna HSM with Oracle WebLogic Server

Configuring SafeNet Luna HSM with Oracle WebLogic Server

To configure SafeNet Luna HSM for Oracle WebLogic Server, perform the following steps:

1. Copy the **libLunaAPI.so** and **LunaProvider.jar** file from the **<Luna Installation Directory>** to appropriate extension folder under **<JDK Installation directory>**.

   For Example:

   ```
   # cp /usr/safenet/lunaclient/jsp/lib/libLunaAPI.so <JAVA_HOME>/jre/lib/ext/
   # cp /usr/safenet/lunaclient/jsp/lib/LunaProvider.jar <JAVA_HOME>/jre/lib/ext/
   ```

2. Edit the Java Security Configuration file **`java.security`** located in the security directory under **<JDK Installation directory>**.

   For Example:

   ```
   # vi $JAVA_HOME/jre/lib/security/java.security
   ```

   Add the Luna Provider in **java.security** file as shown below:

   ```
   security.provider.1=sun.security.provider.Sun
   security.provider.2=sun.security.rsa.SunRsaSign
   security.provider.3=com.sun.net.ssl.internal.ssl.Provider
   security.provider.4=com.sun.crypto.provider.SunJCE
   security.provider.5=sun.security.jgss.SunProvider
   security.provider.6=com.sun.security.sasl.Provider
   security.provider.7=org.jcp.xml.dsig.internal.dom.XMLDSigRI
   security.provider.8=sun.security.smartcardio.SunPCSC
   security.provider.9=com.safenetinc.luna.provider.LunaProvider
   ```

   Save the changes in the **java.security** file.

   NOTE: If using SafeNet Luna HSM 5.2.1 and above, skip the step 3, 4 and proceed with step 5.

3. Edit the Luna Configuration file make the following changes in the Misc section:

   ```
   Misc = {
       AppIdMajor=1;
       AppIdMinor=1;
   }
   ```

4. Use SALOGIN utility to open the session with Luna using Application ID defined in Luna Configuration file.

   For example:

   ```
   # /usr/safenet/lunaclient/bin/salogin -o -s 1 -i 1:1 -v -p <Partition Password>
   ```

5. Export the JAVA_HOME and PATH variables.

   For Example:

   ```
   # export JAVA_HOME=<JAVA_HOME>
   # export PATH=$JAVA_HOME/bin:$PATH
   ```

6. Go to the WebLogic Server Domain directory.

   For Example:

   ```
   # cd /u01/app/oracle/middleware/user_projects/domains/base_domain/bin/
   ```

7. Set the domain environment variables by executing the setDomainEnv.sh

   For Example:

   ```
   # . ./setDomainEnv.sh
   ```

8. Create a **lunastore** file and made following entry:

   ```
   tokenlabel:<Partition Name>
   ```

   And place it at "/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain" directory.

9. Generate a new keystore and key pair using Java Keytool utility.

   ```
   # keytool -genkeypair -alias lunakey -keyalg RSA -sigalg SHA256withRSA -keypass temp123# -
   keysize 2048 -keystore lunastore -storepass temp123# -storetype luna
   ```

   For Example:

   ```
   # keytool -genkeypair -alias lunakey -keyalg RSA -sigalg SHA256withRSA -keypass temp123# -
   keysize 2048 -keystore lunastore -storepass temp123# -storetype luna

   What is your first and last name?
   [Unknown]: Hostname
   What is the name of your organizational unit?
   [Unknown]: Testing Only
   What is the name of your organization?
   [Unknown]: My Org
   What is the name of your City or Locality?
   [Unknown]: My City
   What is the name of your State or Province?
   [Unknown]: My State
   What is the two-letter country code for this unit?
   [Unknown]: UK
   Is CN= Hostname, OU= Testing Only, O= My Org, L= My City, ST= My State, C=
   UK correct?
   [no]: yes
   ```

   A new key pair will be generated on Luna HSM.

10. Generate a certificate request from a key in the keystore.

    ```
    # keytool -certreq -alias lunakey -sigalg SHA256withRSA -file certreq_file -storetype luna -
    keystore lunastore
    ```

11. Submit the CSR file to a CA such as VeriSign, Entrust, and so on. The CA authenticates the request and returns a signed certificate or a certificate chain. Save the reply in the current working directory.

12. Import the CA's Root certificate and signed certificate or a certificate chain in to the keystore.
    - To import the CA root certificate execute the following:

      ```
      # keytool -trustcacerts -importcert -alias rootca -file root.cer -keystore lunastore -storetype luna
      ```

    - To import the signed certificate reply or certificate chain execute the following:

      ```
      # keytool -trustcacerts -importcert -alias lunakey -file mycert.cer -keystore lunastore -storetype luna
      ```

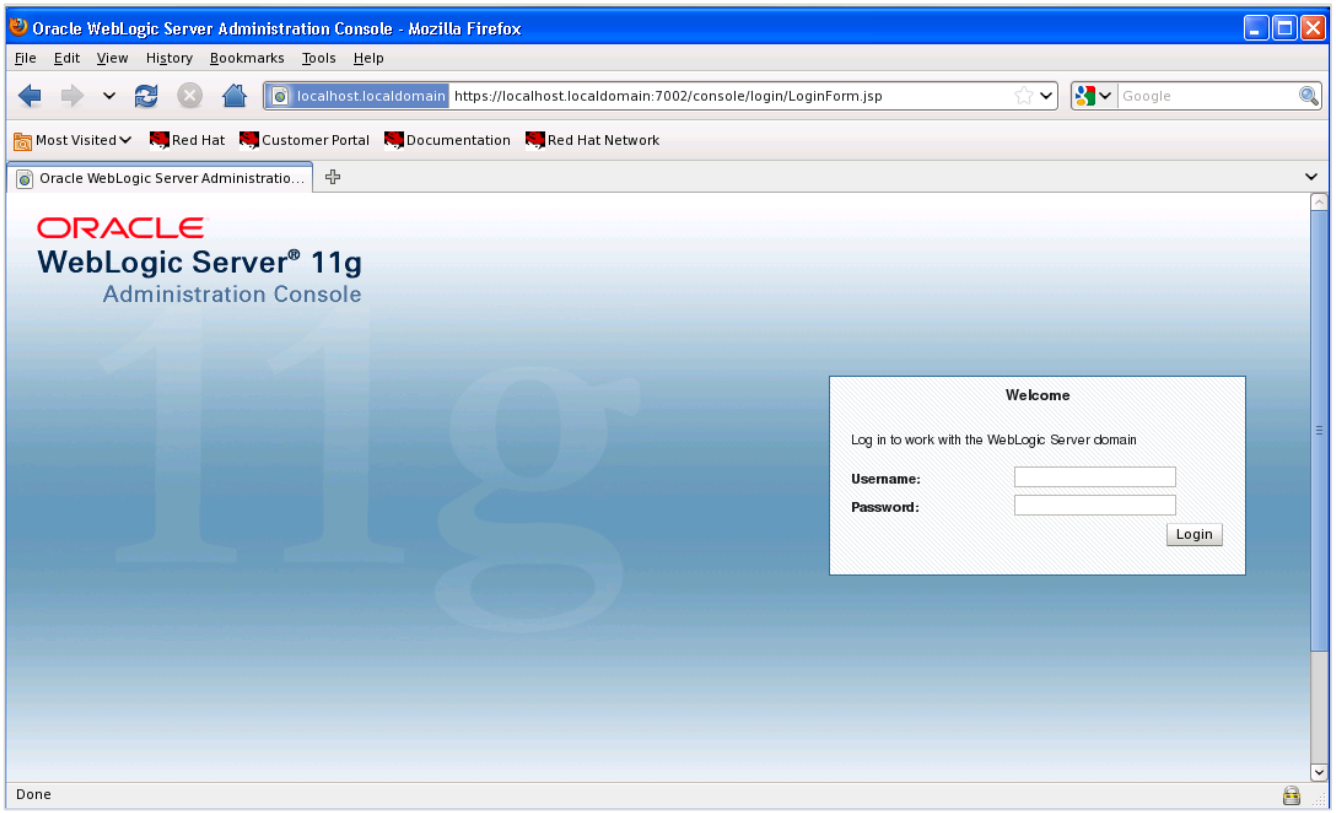
      `root.cer` and `mycert.cer` are the CA Root Certificate and Signed Certificate request respectively.
13. Start the WebLogic Server with below command:

    ```
    # ./startWebLogic.sh
    ```
14. Open the Administration Console **http://hostname:7001/console**
15. Navigate to **Domain Structure** > **Environment** and complete the following steps:
    a. Click **Servers**.
    b. Click **AdminServer**.
    c. Click **Lock & Edit.**
    d. Select the **SSL Listen Port Enabled** check box.
    e. Click **Save**.
16. Open the **Keystores** tab and then complete the following steps:
    a. Click **Change**.
    b. From the drop-down menu, select **Custom Identity and Custom Trust**.
    c. Click **Save**.
    d. In the **Custom Identity Keystore** field, enter **lunastore**.
    e. In the **Custom Identity Keystore Type** field, enter **luna.**
    f. In the **Custom Identity Keystore Passphrase** field, enter **<part_password>**. Confirm the passphrase.
    g. In the **Custom Trust Keystore** field, enter **lunastore.**
    h. In the **Custom Trust Keystore Type** field, enter **luna**.
    i. In the **Custom Trust Keystore Passphrase** field, enter **<part_password>**. Confirm the passphrase.
    j. Click **Save**.
17. Open the **SSL** tab.
    a. In the **Private Key Alias** field, enter lunakey.
    b. In the **Private Key Passphrase** field, enter **<part_password>**. Confirm the passphrase.
    c. Click **Save**.
18. Click **Advanced**.
    a. Select the **Use JSSE SSL** check box.

       In Oracle Weblogic 12c, **USE JSSE SSL** option would not be available.
    b. Click **Save**.
19. Click **Activate Changes**.
20. **Logout** from the **Administration** console.

21. Restart the WebLogic Server.

    Open the **Administration** console using **https://hostname:7002/console**.



3
Troubleshooting

Troubleshooting

Problem

SSL_BAD_MAC_ALERT message received when accessing the Administration Console using **https://hostname:7002/console**.

Solution

Ensure that you have applied the appropriate patch for SafeNet Luna HSM support and selected the **Use JSSE SSL** check box under the **SSL > Advanced tab** in the Administration Console.