Oracle GlassFish Server
Integration Guide

SafeNet. THE DATA PROTECTION COMPANY

Document Information

Document Part Number	007-012348-001 (Rev A)
Release Date	August 2013

Trademarks

Limitations

This document does not include the steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to Luna SA documentation for general Luna setup procedures.

Disclaimer

The foregoing integration was performed and tested only with the specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Email	support@safenet-inc.com	

Contents

CHAPTER 1
Introduction

This document is intended to guide administrators through the steps for Oracle GlassFish Server and Luna HSM integration, and also covers the necessary information to install, configure and integrate Oracle GlassFish Server with SafeNet Luna Hardware Security Modules (HSMs).

The Luna HSMs integrates with the Oracle GlassFish Server to provide significant performance improvements by off-loading cryptographic operations from the Server to the Luna HSMs. In addition, the Luna HSMs 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 GlassFish Server

Oracle GlassFish Server is the world's first implementation of the Java Platform, Enterprise Edition (Java EE) 6 specification. Built using the GlassFish Server Open Source Edition, Oracle GlassFish Server delivers a flexible, lightweight, and production-ready Java EE application server. GlassFish Server Open Source Edition provides a server for developing and deploying Java Platform Enterprise Edition (Java EE) applications and web Java Web Services.

As an administrator of GlassFish Server, your main responsibilities are to establish a secure GlassFish Server environment and to oversee the services, resources, and users that participate in that environment. Your key tasks include configuring resources and services, managing GlassFish Server at runtime, and fixing problems that are associated with the server. You might also be involved in installing software, integrating add-on components, and deploying applications.

Scope

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

3rd Party Application Details

- Oracle GlassFish Server 3.1.1.2
- Oracle GlassFish Server 4.0

You can download the Oracle GlassFish Server from Oracle Support site:

http://www.oracle.com/technetwork/middleware/glassfish/downloads/index.html
http://glassfish.java.net/

Supported Platforms

The following platforms are supported for Luna HSM:

Operating System	SafeNet Luna HSM	Oracle Glassfish Server Version	Java Version
Red Hat Enterprise Linux 6.0 (64 bit)	Luna SA v5.2.1	4.0	JDK 1.7.0_25
Red Hat Enterprise Linux 6.0 (64 bit)	Luna G5	3.1.2.2	JDK 1.6.0_30 JDK 1.7.0_25

HSM and Firmware Support

We did this integration with the following:

- Luna SA v5.2.1 f/w 6.10.1 with Luna Client s/w v5.2.1 (64-bit)
- Luna G5 f/w 6.10.1 with Luna Client s/w v5.2.1 (64 bit)

Prerequisites

Luna SA Setup

Please refer to the Luna SA documentation for installation steps and details regarding configuring and setting up the box on UNIX operating systems. Before you get started ensure the following:

- Luna SA appliance and a secure admin password
- Luna SA, and a hostname, suitable for your network
- Luna SA network parameters are set to work with your network
- Initialized the HSM on the Luna SA appliance.
- Created and exchanged certificates between the Luna SA and your Client system.
- Created a partition on the HSM, remember the partition password that will be later used by Oracle GlassFish Server. Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from Luna SA. The general form of command is /usr/safenet/lunaclient/bin/vtl verify for UNIX.
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Luna G5 Setup

Please refer the Luna G5 documentation for installation steps and details regarding configuring and setting up the box on UNIX Operating system.

Oracle GlassFish Server Setup

You should familiarize yourself with Oracle GlassFish Server. Refer to the Oracle documentation for more information to install and pre-installation requirements.

http://www.oracle.com/technetwork/middleware/glassfish/documentation/index.html
http://glassfish.java.net/documentation.html

CHAPTER 2
Integrating Oracle GlassFish Server with Luna

Setting up Luna with Oracle GlassFish Server

To set up Luna SA for Oracle GlassFish Server, kindly perform the following steps:

Configuring the Oracle GlassFish Server

Install the JDK (refer the oracle documentation for supported JDK version for GlassFish Server) and export the JAVA_HOME and PATH variables to use the supported JDK:

 # export JAVA_HOME=<Path to the JDK Installation Directory>

For example: export JAVA_HOME=/opt/jdk1.7.0_25

 # export PATH=$JAVA_HOME/bin:$PATH

Configuring an Oracle GlassFish Server for Luna required the following tasks:

Task 1: Configuring the Luna Provider

Task 2: Generate the Certificate

Task 3: Enabling SSL in GlassFish Server

Configuring the Luna Provider

a) Copy the following files from

/usr/safenet/lunaclient/jsp/lib/libLunaAPI.so

/usr/safenet/lunaclient/jsp/lib/LunaProvider.jar

To

$JAVA_HOME/jre/lib/ext/

 # cp /usr/lunasa/jsp/lib/libLunaAPI.so $JAVA_HOME/jre/lib/ext/

 # cp /usr/lunasa/jsp/lib/LunaProvider.jar $JAVA_HOME/jre/lib/ext/

b) Modify the java.security file to include the Luna Provider. Open the java.security file and do the following changes:

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

security.provider.1=com.safenetinc.luna.provider.LunaProvider

security.provider.2=sun.security.provider.Sun

security.provider.3=sun.security.rsa.SunRsaSign

security.provider.4=sun.security.ec.SunEC

security.provider.5=com.sun.net.ssl.internal.ssl.Provider

security.provider.6=com.sun.crypto.provider.SunJCE

security.provider.7=sun.security.jgss.SunProvider

security.provider.8=com.sun.security.sasl.Provider

security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSigRI

security.provider.10=sun.security.smartcardio.SunPCSC

com.safenetinc.luna.provider.createExtractableKeys=true

Default keystore type.

#

keystore.type=luna

Generate the Certificate

a) Modify the /etc/Chrystoki.conf to include the following:

Misc = {

AppIdMajor=1

AppIdMinor=1

}

b) Open the session on Luna SA using application ID 1:1 with salogin utility

 # /usr/safenet/lunaclient/bin/salogin -o -i 1:1 -s <slot id> -v -p <password>

NOTE: Slot id is the slot number and password is Luna SA partition password.

c) Change the directory where you want to create your key store, if you want to use the GlassFish configuration directory then

 # cd <Path to the glassfish instance directory>/glassfish/domains/domain1/config

d) Change the GlassFish admin password.

 # <Path to the glassfish instance directory>/bin/asadmin change-master-password

For example: /opt/glassfish3/bin/asadmin change-master-password

It will prompt for current password, enter “changeit” and then type new password for GlassFish Server Admin.

e) Generate a new key store using the java keytool utility that uses the luna provider to generate key and certificate

 # keytool -genkeypair -keyalg RSA -alias lunakey -keypass password -keystore keystore.luna -storepass password -storetype luna -validity 3600

NOTE: It will ask you to provide the details to generate the self signed certificate. Provide the details and your key and certificate will be generated in the Luna SA and key store in the current directory. Provide the same password for keypass and storepass that you have set for admin in the previous step.

f) Create a Certificate Signing Request (CSR) using the generated key

 # keytool -certreq -alias lunakey -file certreq_file -storetype luna -keystore keystore.luna

g) Copy the contents of the generated CSR and submit it to the CA to sign the certificate request.

h) Obtain the signed certificate and root certificate from the Certificate Authority and import it to the key store.

i) Import the CA root certificate in the key store

 # keytool -importcert -trustcacerts -alias safeca -file SafeCA.cer -keystore keystore.luna

Where SafeCA.cer is root certificate of CA who signed the server certificate.

j) Import the signed certificate in the key store.

 # keytool -importcert -trustcacerts -alias lunakey -file MyCert.cer -keystore keystore.luna

Where MyCert.cer is signed certificate request.

NOTE: Before importing the certificate in key store you must import the CA Root certificate and Intermediate certificate also if any.

Enabling SSL in GlassFish Server

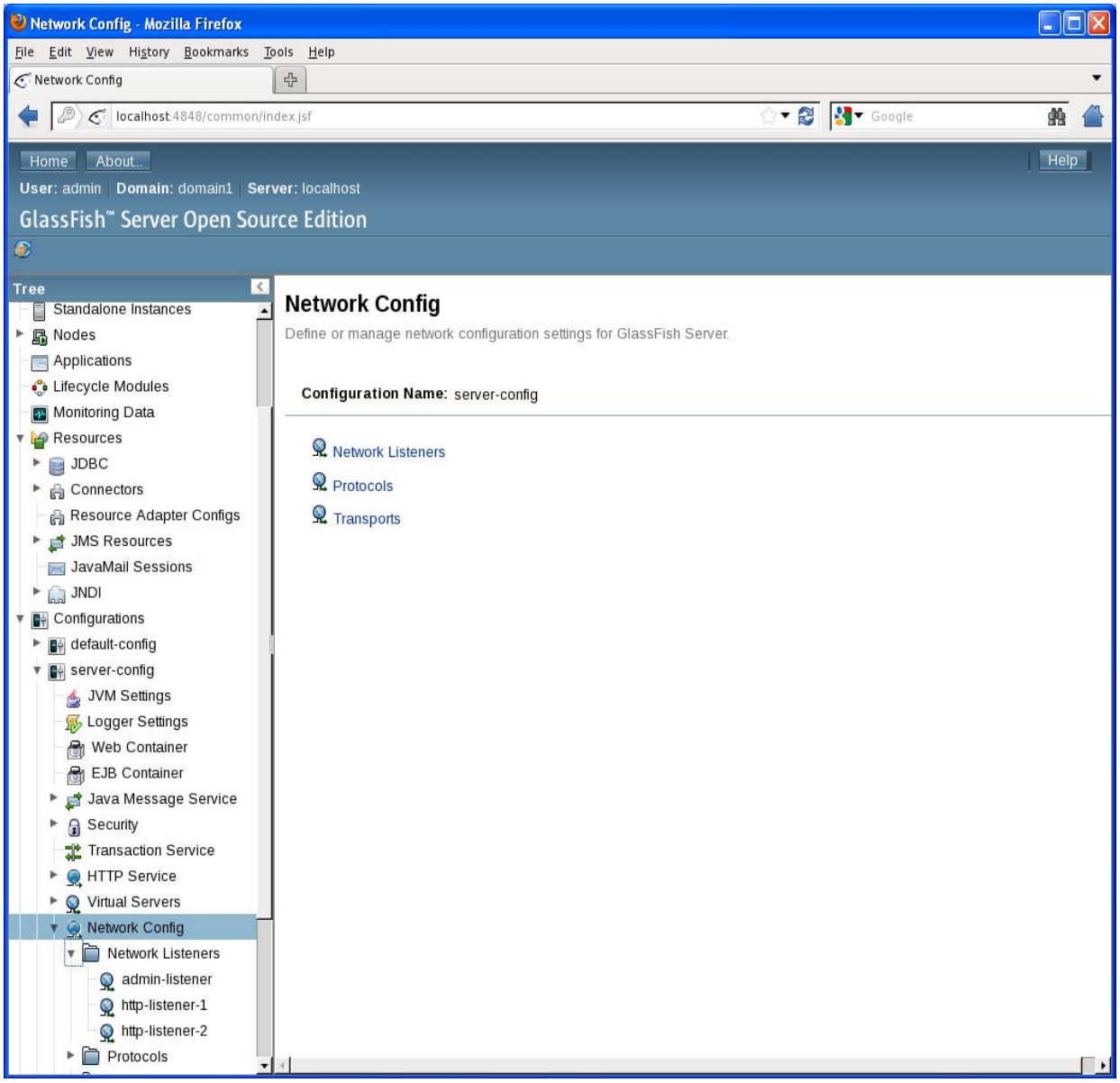
a) Start the glassfish admin server.

#<Path to the glassfish Instance directory>/bin/asadmin start-domain

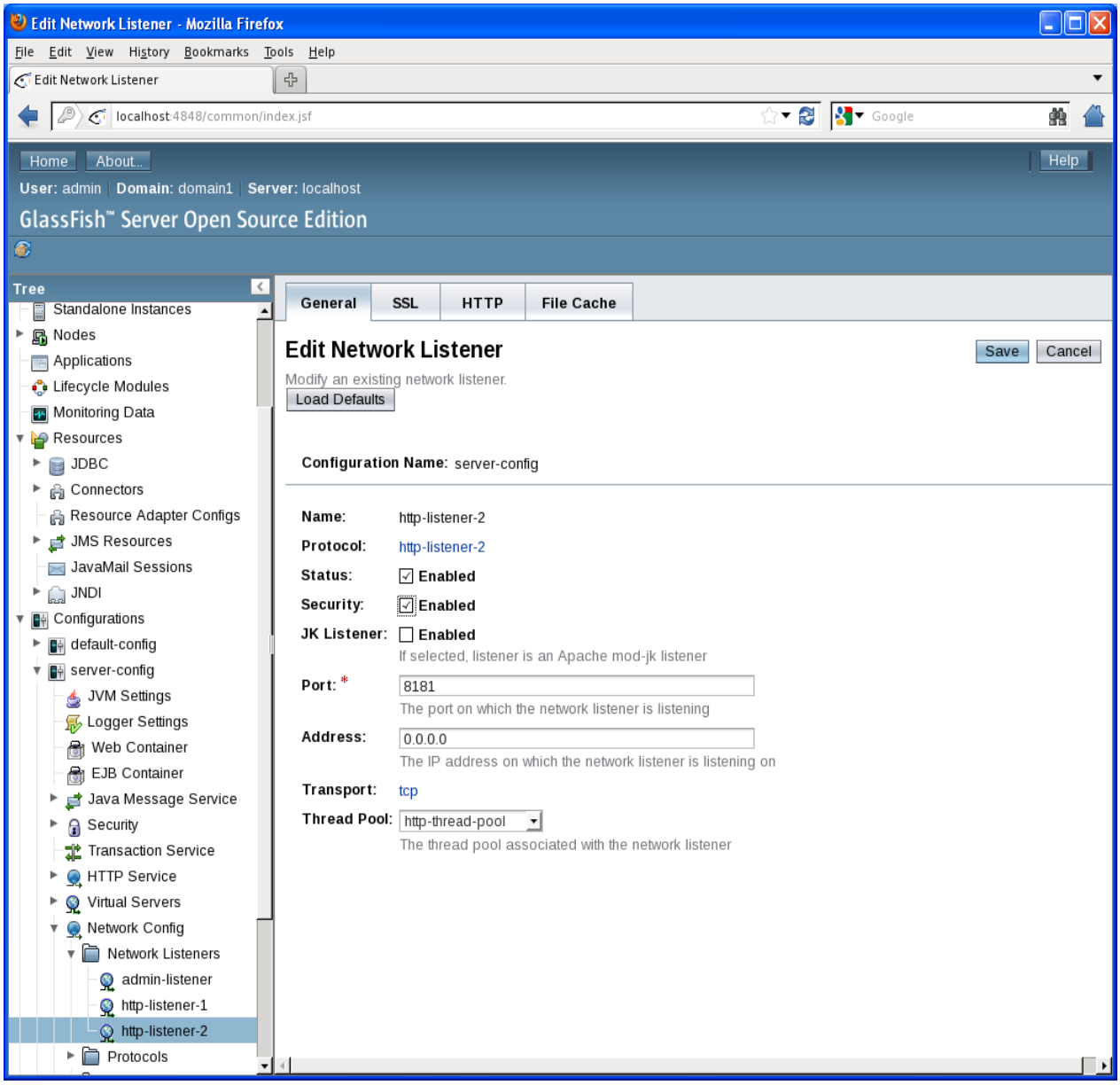
For Example: /opt/glassfish3/bin/asadmin start-domain

b) Open the Administrator Console in the web browser. Type http://localhost:4848

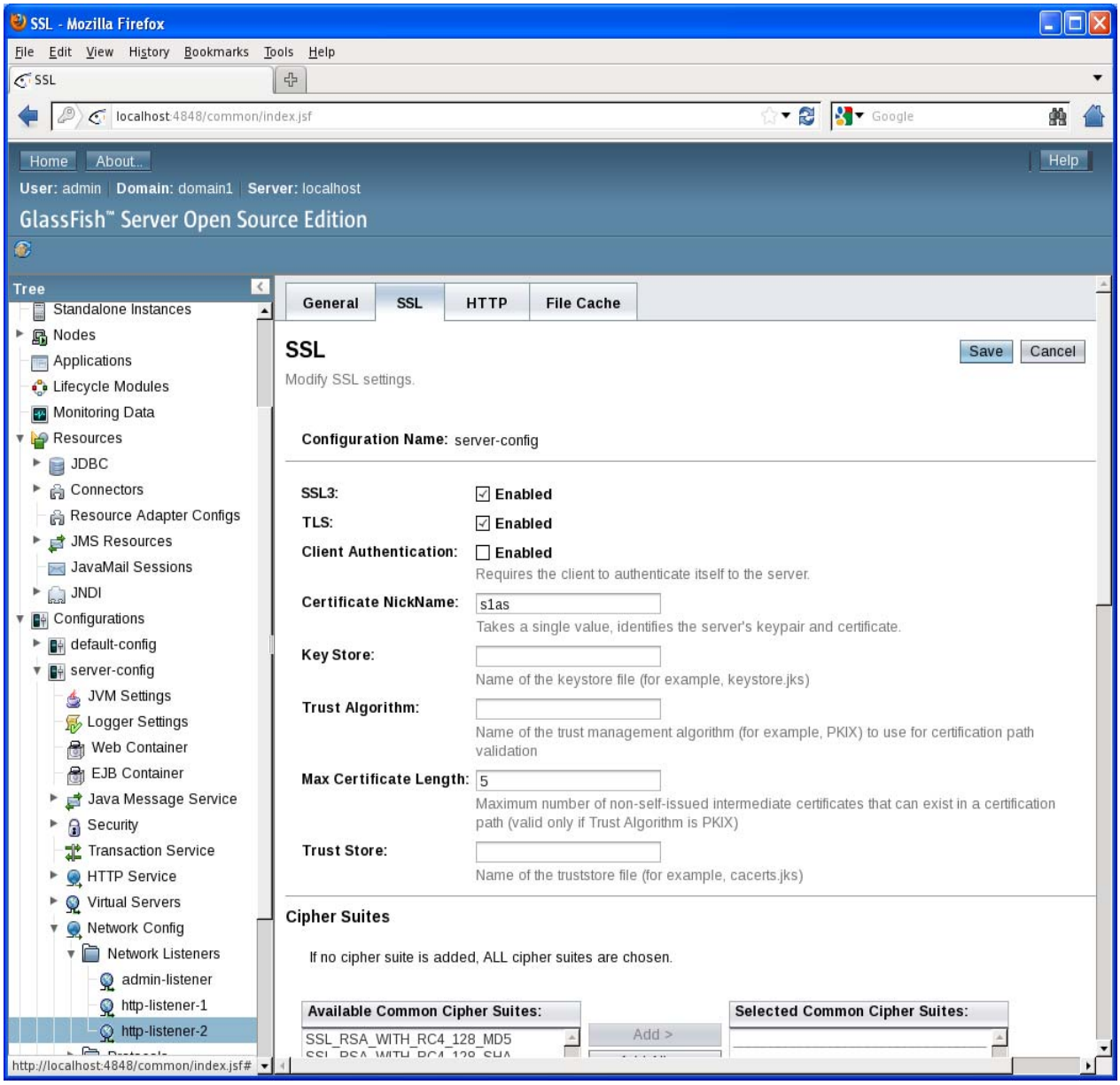
c) Click on the Configurations -> server-config -> Network Config -> Network Listeners.



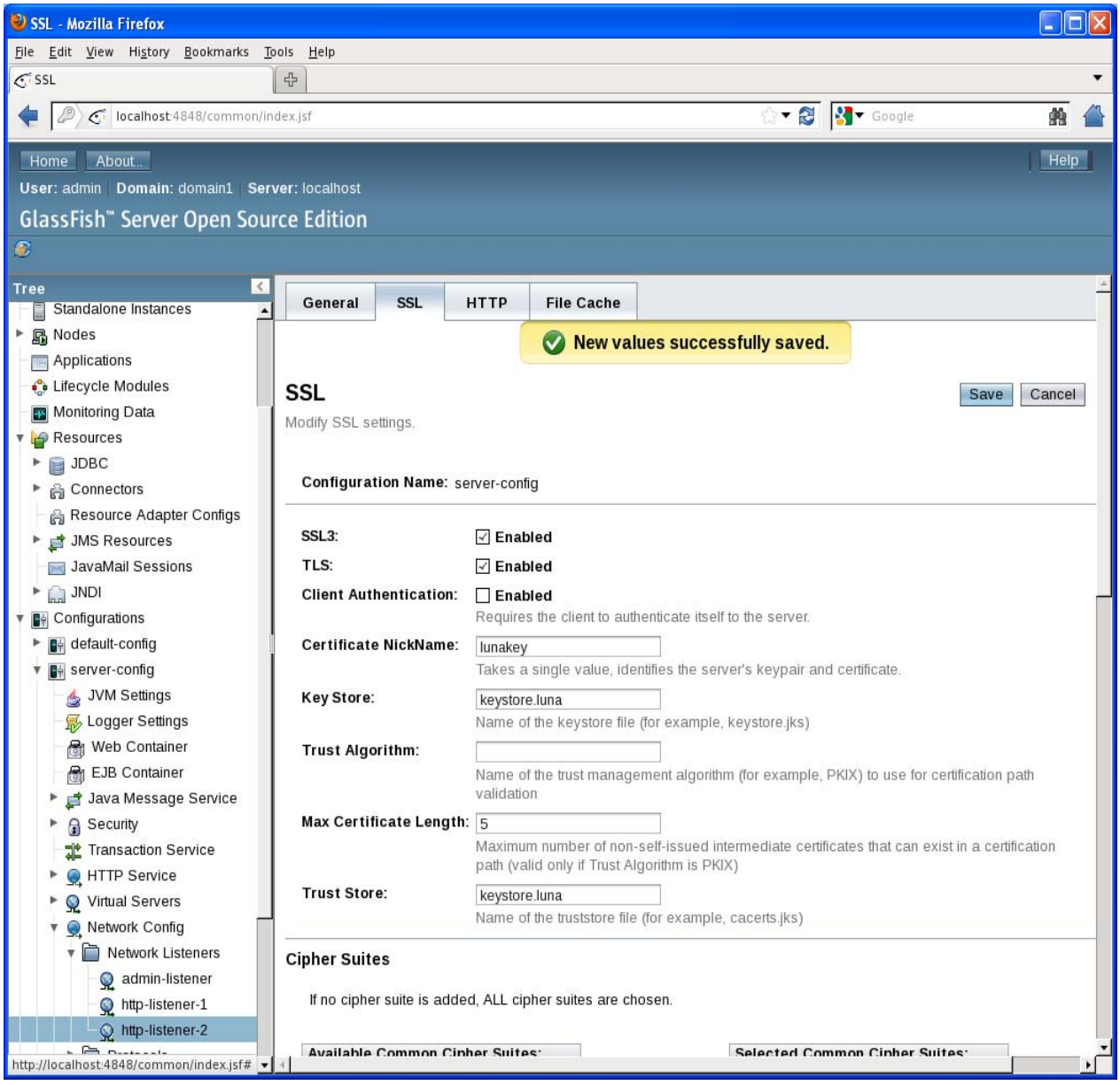
d) Click on http-listener-2, click on General tab and select Security Enable check box.



e) Click on SSL tab, and select SSL3 and TLS checkbox to enable it.



f) Enter the Certificate NickName, Key Store and Trust Store that you have created using keytool. Click the Save button to save the configuration.



g) Close the browser and change the preference of security provider in the file $JAVA_HOME/jre/lib/security/java.security

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

security.provider.1=sun.security.provider.Sun

security.provider.2=sun.security.rsa.SunRsaSign

security.provider.3=sun.security.ec.SunEC

security.provider.4=com.sun.net.ssl.internal.ssl.Provider

security.provider.5=com.sun.crypto.provider.SunJCE

security.provider.6=com.safenetinc.luna.provider.LunaProvider

security.provider.7=sun.security.jgss.SunProvider

security.provider.8=com.sun.security.sasl.Provider

security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSigRI

security.provider.10=sun.security.smartcardio.SunPCSC

com.safenetinc.luna.provider.createExtractableKeys=true

NOTE: Make sure that Luna Provider is below the com.sun.crypto.provider.SunJCE provider.

h) Save the changes and restart the glassfish admin server

#<Path to the glassfish Instance directory>/bin/asadmin restart-domain

For Example: /opt/glassfish3/bin/asadmin restart-domain

i) Open the Firefox or any web browser.

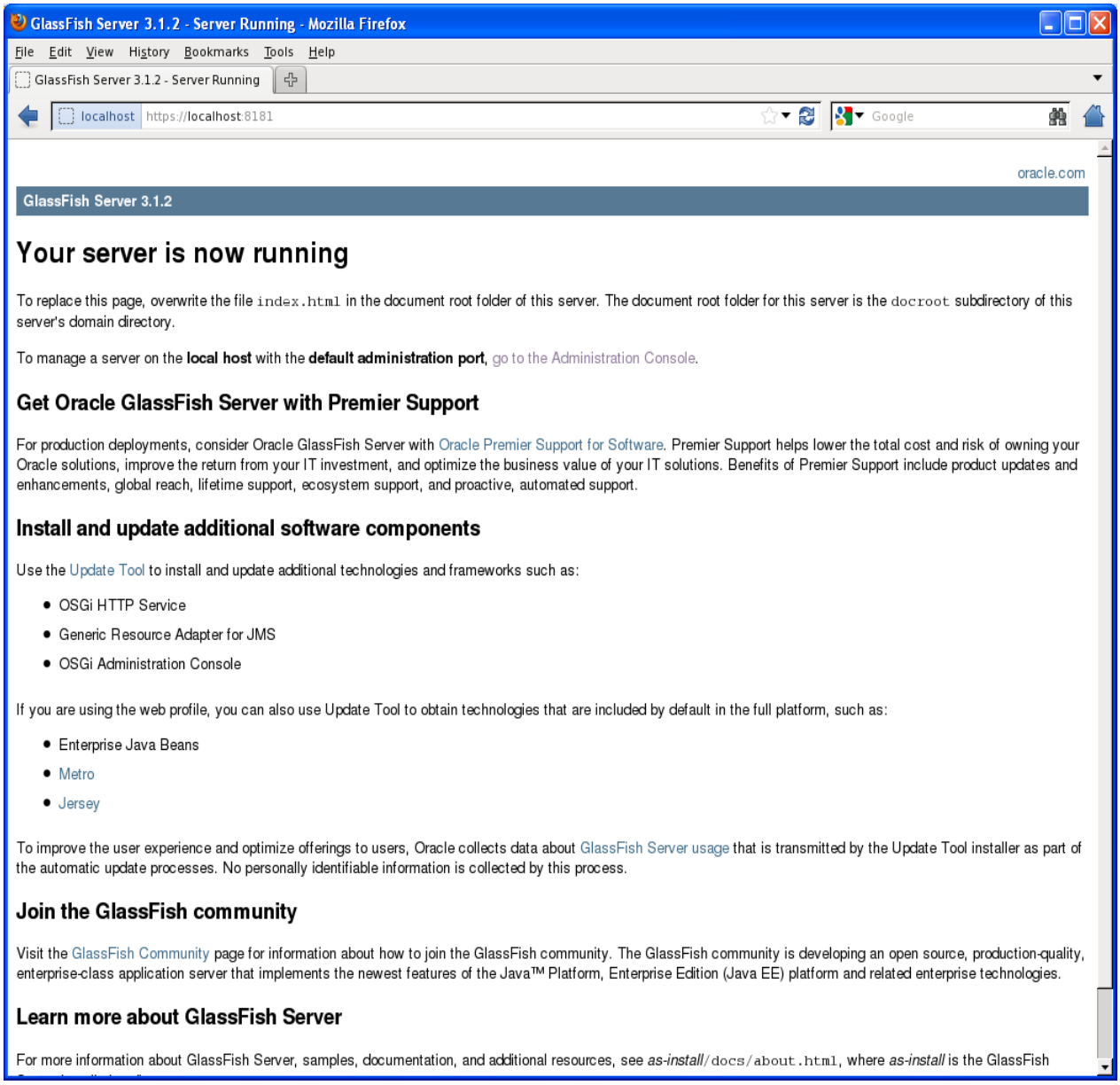
j) In the address bar, type https://<fully qualified domain name or IP>:8181

For example: https://localhost:8181

k) On the certificate navigation, click on add exception.

l) Click on Get Certificate and View to check the certificate details. Verify that the certificate is same that you have created using keytool and whose private key is saved on Luna.

m) Click on confirm security exception and the oracle glassfish web server page will display.



We have successfully created the SSL connection using the certificate whose private key is stored on the Luna.