Apache Server Configuration for FLEXCUBE

Oracle FLEXCUBE Universal Banking

Release 14.3.0.0.0

[May] [2019]

Table of Contents

1. INSTALLATION AND CONFIGURATION OF APACHE 2.2.25 1-1

1.1 PURPOSE 1-1
1.2 INTRODUCTION 1-1

2. INSTALLATION OF APACHE 2-1

3. CONFIGURE APACHE SERVER INFRONT OF WEBLOGIC SERVER 3-1

4. CONFIGURING SSL FOR APACHE SERVER 4-1

4.1 SSL CONFIGURATION FOR INBOUND REQUEST TO APACHE 4-1
4.2 CONFIGURING SSL BETWEEN APACHE AND ORACLE WEBLOGIC SERVER 4-3

5. STARTING, STOPPING, AND RESTARTING APACHE 5-1

6. DEBUGGING 6-1

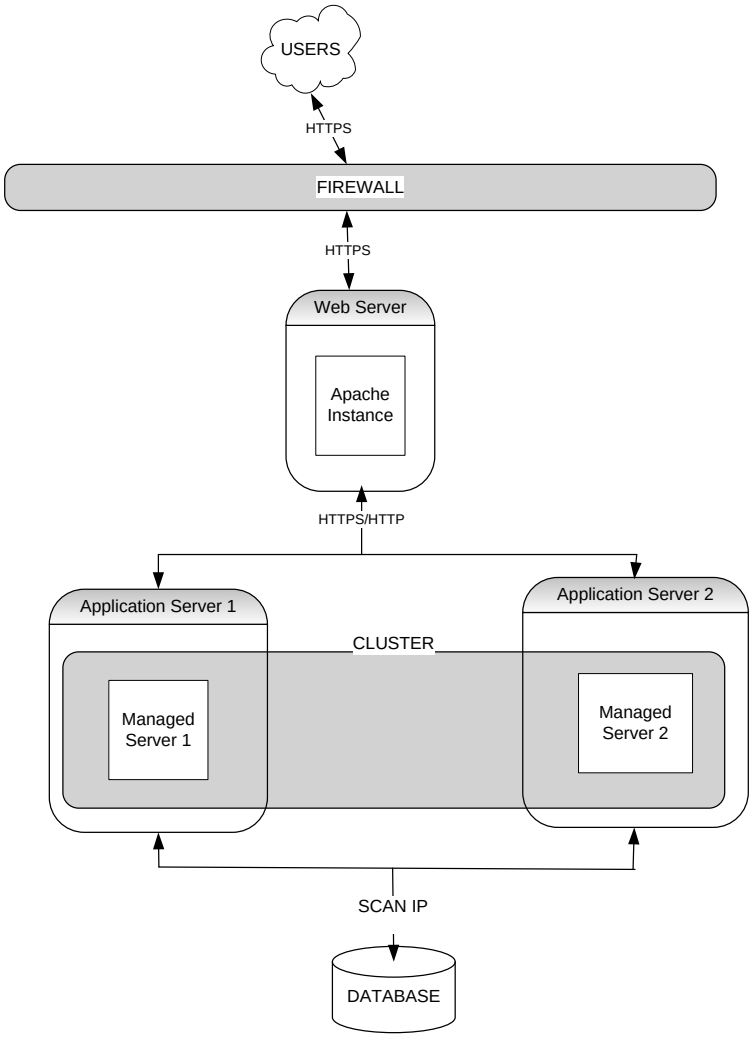
1. Installation and Configuration of Apache 2.2.25

1.1 Purpose

The objective of this document is to explain the installation and configuration of Apache 2.2.25. This includes setting up of server details and enabling SSL.

1.2 Introduction

Below is the typical deployment diagram and this document covers the setup for Apache Webserver Instance.



2. Installation of Apache

Unzip the Apache software, in this example the unzipped location is /scratch/oracle/software/httpd-2.2.25. Below steps should be executed from inside this directory location.

Software Directory: /scratch/oracle/software/httpd-2.2.25

1. $ ./configure --prefix=/scratch/oracle/apache --enable-ssl --with-included-apr

   Where / scratch/oracle/apache is the apache home directory

2. $ make

3. $ make install

ORACLE

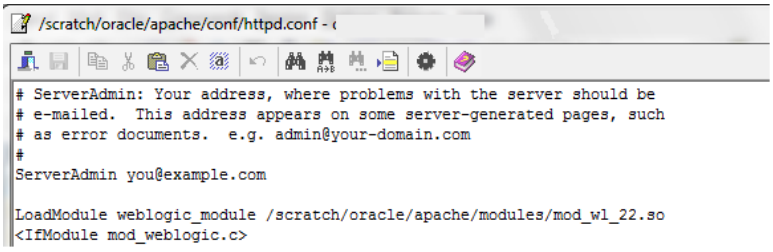
3. Configure Apache Server infront of Weblogic Server

1. Copy mod_wl_22.so from any weblogic Server ($WLS_HOME/server/plugin/linux/x_86_64) to $PREFIX/modules/ location in Apache Server.

NOTE: In this example the OS is linux, copy the file from appropriate folder according to the weblogic installed directory.

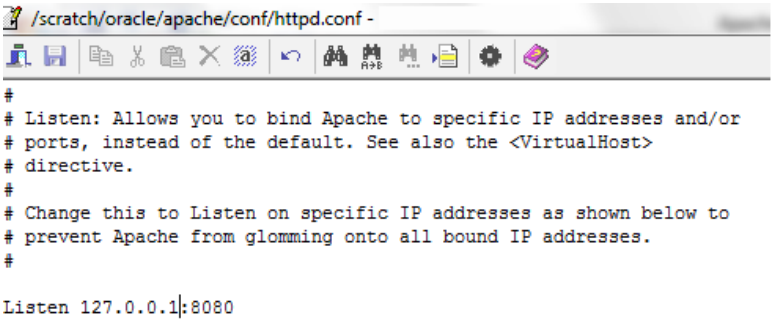
2. Edit http.conf located under folder $PREFIX/conf to include mod_wl_22.conf file.

LoadModule weblogic_module /scratch/oracle/apache/modules/mod_wl_22.so



3. Modify http.conf file for the required listen port

Listen <HOST NAME>:<PORT>



NOTE: This port is for http protocol and not for https

4. Modify the http.conf file to include the weblogic server details

   a. For WebLogic in single instance

<Location /<<context/url>> >

SetHandler weblogic-handler

ORACLE

WebLogicHost <<server name>>

WeblogicPort <<port>>

</Location>

Example:

<Location /FCJNeoWeb>

SetHandler weblogic-handler

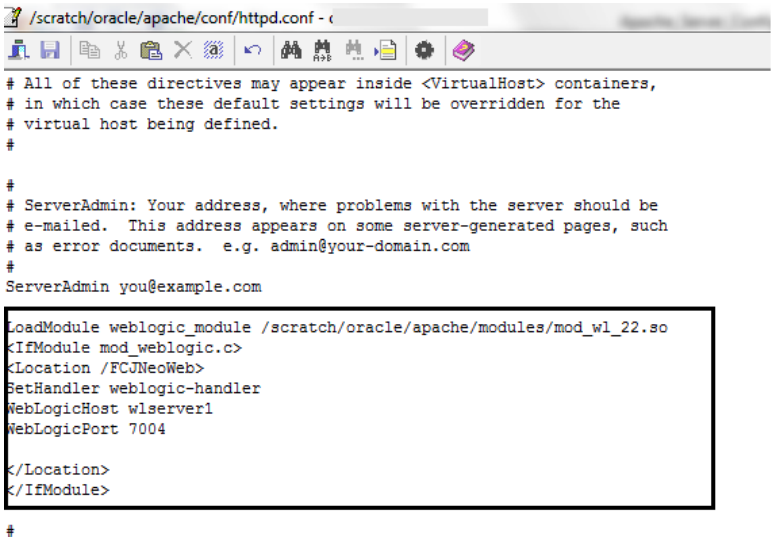
WebLogicHost wlserver1

WeblogicPort 7004

</Location>

This will forward /FCJNeoWeb from Apache server to /FCJNeoWeb on WebLogic Server wlserver1: 7004

NOTE: If you want to allow more than one context root, then either add different Location entries for each context root eg: <Location /FCJNeoWeb>, <Location /FCJWebServices>, etc or Add <Location /> which will all the context roots.



b. For Weblogic instances in cluster

<Location /<<context/url>> >

SetHandler weblogic-handler

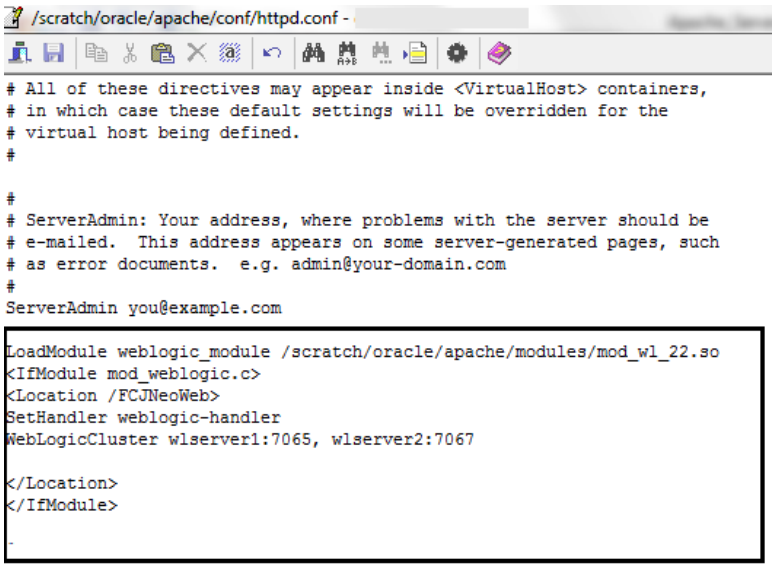
WebLogicCluster <server1>:<port1>,<server2>:<port2>

</Location>

Example

<Location / FCJNeoWeb >
SetHandler weblogic-handler
WebLogicCluster wlserver1:7065, wlserver2:7067
</Location>

This will forward /FCJNeoWeb from Apache server to /FCJNeoWeb on WebLogic Cluster wlserver1:7065 and wlserver2:7067



5. Enable “WebLogic Plug-In Enabled” flag in weblogic

This flag needs to be enabled in weblogic if it is accessed through proxy plugins. When the WebLogic plugin is enabled, a call to getRemoteAddr will return the address of the browser client from the proprietary WL-Proxy-Client-IP header instead of the web server.

a. Plugin flag at managed server level

i. Click on ‘Environment’- > 'Servers' -> '<ManagedServer>' -> 'General' -> 'Advanced'

ii. Check the 'WebLogic Plug-In Enabled' box.

iii. Click 'Save'

iv. Restart the Server.

b. Plugin flag at domain level

i. Click on <Domain> -> 'Web Applications'

ii. Check the 'WebLogic Plug-In Enabled' box.

iii. Click 'Save'

iv. Restart the server.

6. Restart the apache server and application can be accessed using link

http://<hostname>:<port>/FCJNeoWeb/

4. Configuring SSL for Apache Server

Secure Sockets Layer (SSL) is required to run any Web site securely. Secure Sockets Layer (SSL) is an encrypted communication protocol that is designed to securely send messages across the Internet.

Reading of "**SSL_Configuration on Weblogic**" document provided as part of FCUBS installation is recommended before proceeding with further setup.

SSL configuration can be done between

1. Browser to Apache Server(Mandatory)

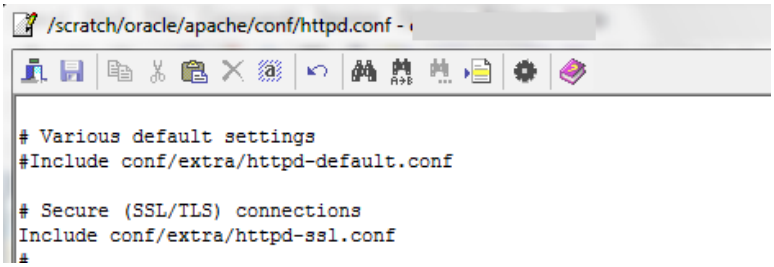
2. Apache to Oracle Weblogic Server(If required)

4.1 SSL configuration for Inbound Request to Apache

Perform these tasks to enable and configure SSL between browser and Apache Server.

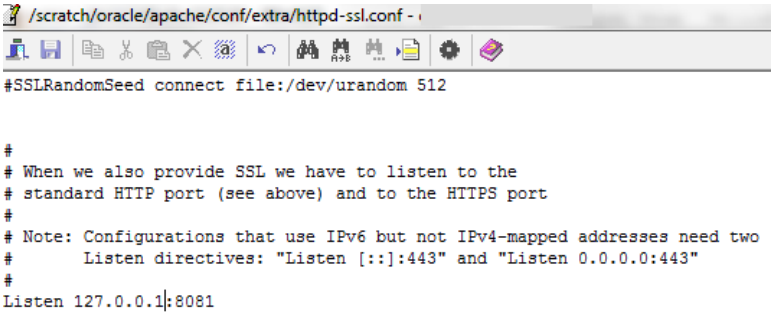
1. In httpd.conf, uncomment the below line

   Include conf/extra/httpd-ssl.conf



2. Edit httpd-ssl.conf file located in $PREFIX/conf/extra/ to give the server address and port as below

   Listen <hostname>:<port>



NOTE: This is the https port and not for http

3. Obtain a certificate from CA or create a self signed certificate using openSSL

    a. Steps to create certificate using openSSL

    openssl genrsa -des3 -out test.key 1024

    openssl req -new -key test.key -out test.csr

    openssl x509 -req -days 365 -in test.csr -signkey test.key -out test.crt

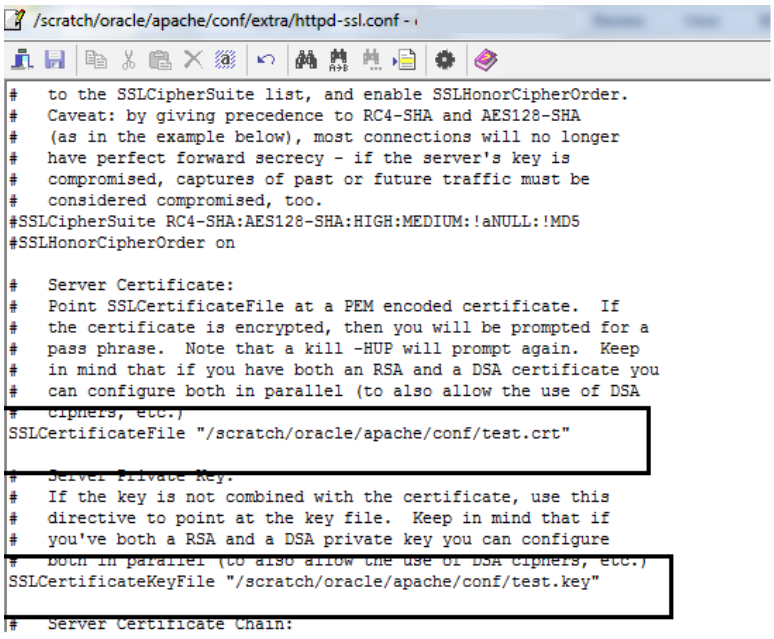
    This will generate 3 files named test.key, test.csr, test.crt

4. Copy the files with extenstion.crt and .key to $PREFIX/conf/ folder.

5. Edit httpd-ssl.conf to give the location and name for .crt and .key as below

```
SSLCertificateFile "/scratch/oracle/apache/conf/test.crt"

SSLCertificateKeyFile "/scratch/oracle/apache/conf/test.key"
```



6. Restart apache and application can be accessed using URL

    https://<hostname>:<port>/FCJNeoWeb/

NOTE: When apache is started with SSL enabled it will ask for pass phrase: here enter the pass phrase used during creation of certificate

4.2 Configuring SSL between Apache and Oracle Weblogic Server

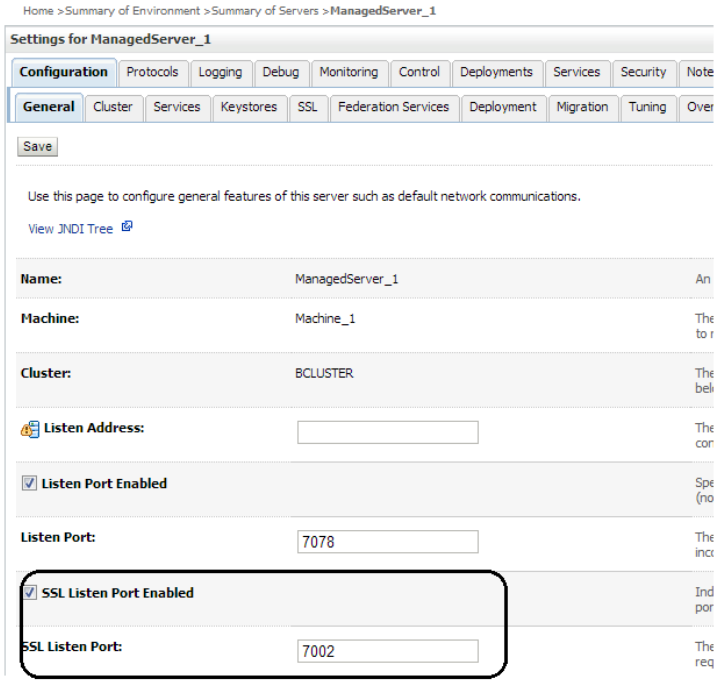
1. Obtain a certificate from CA or create a self signed certificate using Keytool

   keytool -genkeypair -alias testselfcert -keyalg RSA -keypass admin123 -validity 365 -keystore testidentity.jks

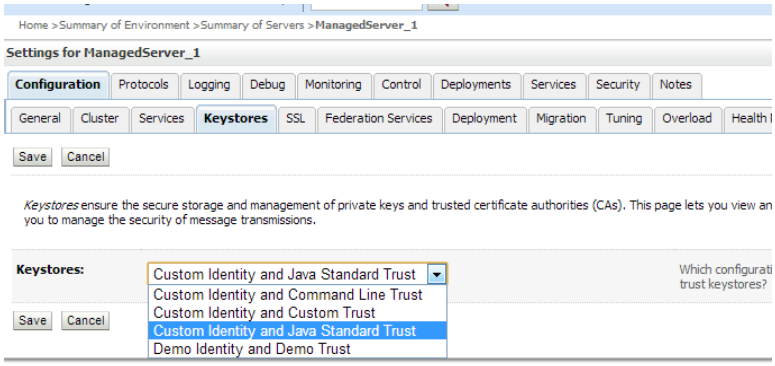
   keytool -export -alias testselfcert -file test.cer -keystore testidentity.jks

2. Configure in weblogic to use the generated keyStore

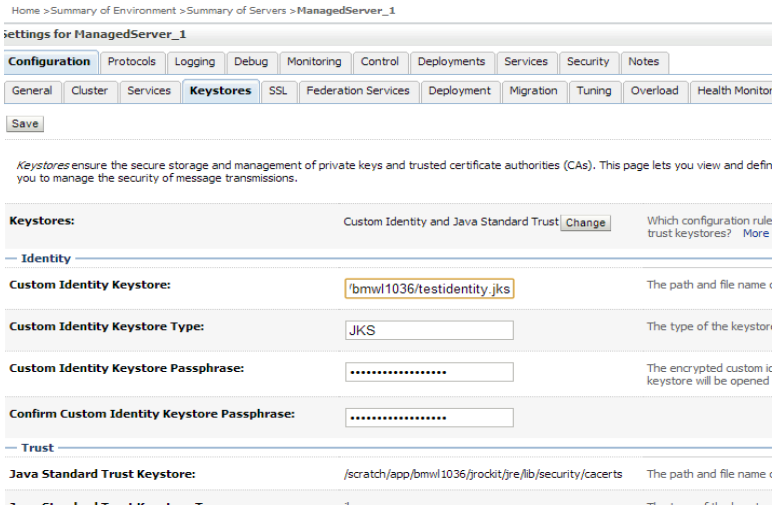
   a. Enable the enable SSL port for the managed server



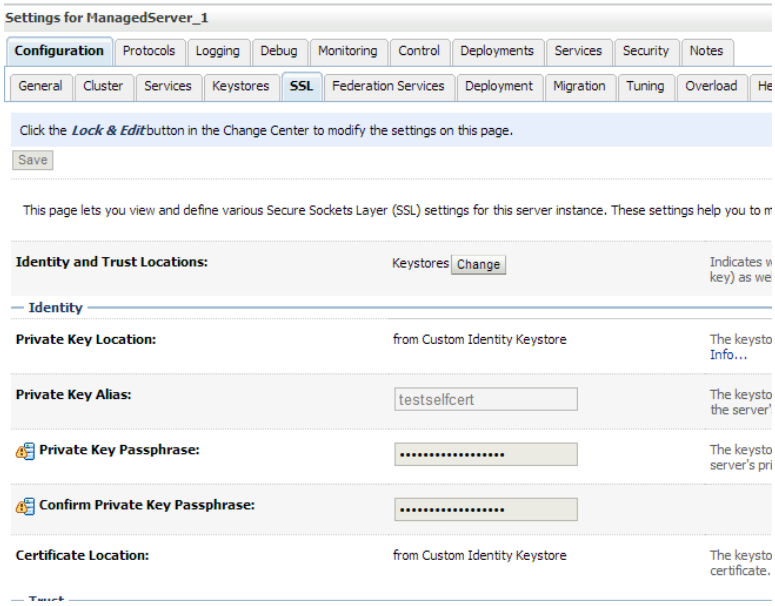
   b. In KeyStores tab select Custom Identity and Java Standard Trust



c. Enter the Path where KeyStore generated is stored and then Enter the passphrase



d. Under SSL tab Enter the Alias and the key Passphrase



Certificate displayed by Weblogic needs to be copied to apache, below steps needs to be followed

e. Execute the openSSL command, openssl s_client -connect <WL host: Port>

Eg: openssl s_client -connect wlserver1:7004.
It will give output as below

```
-bash-4.1$ openssl s_client  -connect wlserver1:7004
CONNECTED(00000003)
depth=0 C = IN, ST = IN, L = IN, O = IN, OU = IN, CN = IN
verify error:num=18:self signed certificate
verify return:1
depth=0 C = IN, ST = IN, L = IN, O = IN, OU = IN, CN = IN
verify return:1
---
Certificate chain
 0 s:/C=IN/ST=IN/L=IN/O=IN/OU=IN/CN=IN
   i:/C=IN/ST=IN/L=IN/O=IN/OU=IN/CN=IN
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICEzCCAXygAwIBAgIEUigrQTANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJJ
TjELMAkGA1UECBMCSU4xCzAJBgNVBAcTAklOMQswCQYDVQQKEwJJTjELMAkGA1UE
CxMCSU4xCzAJBgNVBAMTAklOMB4XDTEzMDkwNTA2NTcwNVoXDTE0MDkwNTA2NTcw
NVowTjELMAkGA1UEBhMCSU4xCzAJBgNVBAgTAklOMQswCQYDVQQHEwJJTjELMAkG
A1UEChMCSU4xCzAJBgNVBAsTAklOMQswCQYDVQQDEwJJTjCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEAita2L8q7cA+aMbnCIWIjXO+2If+1/Oz3tiLJiC2ulhD/
kd7Q+TxjPS5qsGDhK4jgLOTk4wwNzjawvQVUBY+s5XGwSQatujkgk9kmu+d1zP29
5Hwer0wvA/mRH3k4tj9Os1ueJaHgIdI1eS16bhadMV1C7Z9Tr1M+2fdjzGWSl0UC
AwEAATANBgkqhkiG9w0BAQUFAAOBgQA62+BFGN5CMQJkX3YUf1l0KhLJveWQwwGl
OHnW2lchW3YK4YyKsl5b4HdNuBeGjINn47wnujhqPjh6BI8pqbHOYlPjKpNwjTVn
5qkxKZhC5WCMdA3lyyGSQrmUIxJBatw2fVhGaMxdQRy7WujPL5Vf5N+TpedTwXWY
ampTtc+4cw==
```

-----END CERTIFICATE-----
subject=/C=IN/ST=IN/L=IN/O=IN/OU=IN/CN=IN
issuer=/C=IN/ST=IN/L=IN/O=IN/OU=IN/CN=IN

No client certificate CA names sent

SSL handshake has read 665 bytes and written 295 bytes

New, TLSv1/SSLv3, Cipher is RC4-MD5
Server public key is 1024 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : RC4-MD5
Session-ID: EF4D92AFB99069ADF35DB9B16E8B36C9
Session-ID-ctx:
Master-Key:
3B9AD7E1F72C0A50FF4C10458F392C763331CDD5313832A8BF28EDEBFFCD8E6D928944D
4698FC302F3A490116DC6E320
Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1378442902
Timeout : 300 (sec)
Verify return code: 18 (self signed certificate)

f. The section highlighted in red above is the certificate presented by weblogic. This needs to be copied to new file and name this file as server.pem under location $PREFIX/conf/

3. Apache to be configured to use the SSL

In httpd.conf add the below directive

<Location /FCJNeoWeb>

SetHandler weblogic-handler

SecureProxy ON

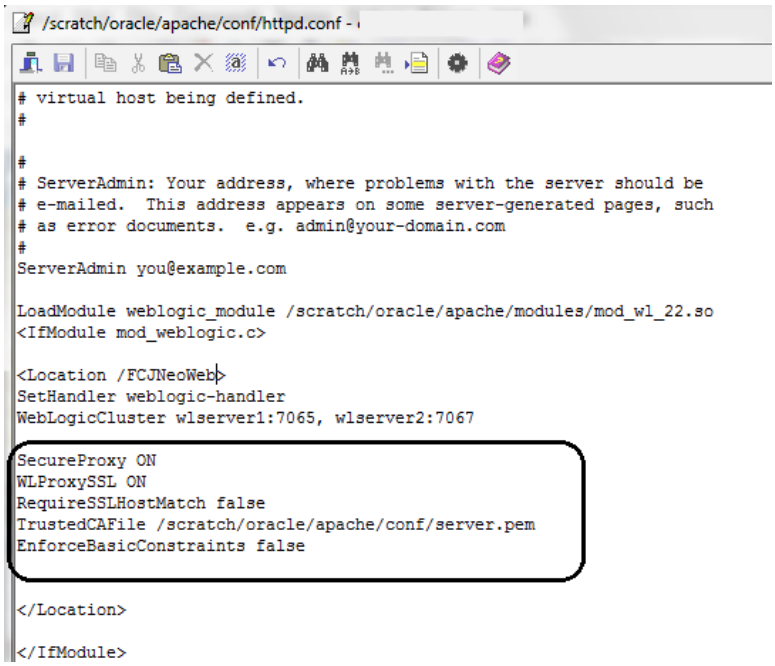
WLProxySSL ON

RequireSSLHostMatch false

TrustedCAFile /scratch/oracle/apache/conf/server.pem

EnforceBasicConstraints false

</Location>



4. Restart Apache and access using the URL

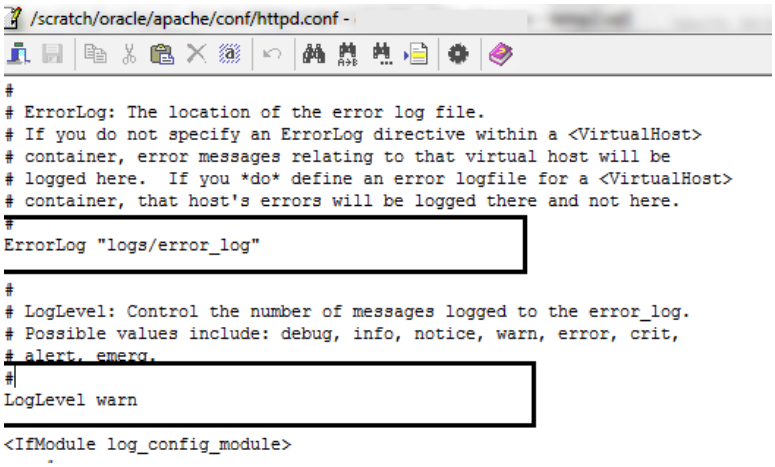
   https://<hostname>:<port>/FCJNeoWeb/

5. Starting, Stopping, and Restarting Apache

Run below commands

- $PREFIX/bin/apachectl start
- $PREFIX/bin/apachectl stop
- $PREFIX/bin/apachectl restart

1. LogLevel and ErrorLog directives in httpd.conf file control the location and log file severity.

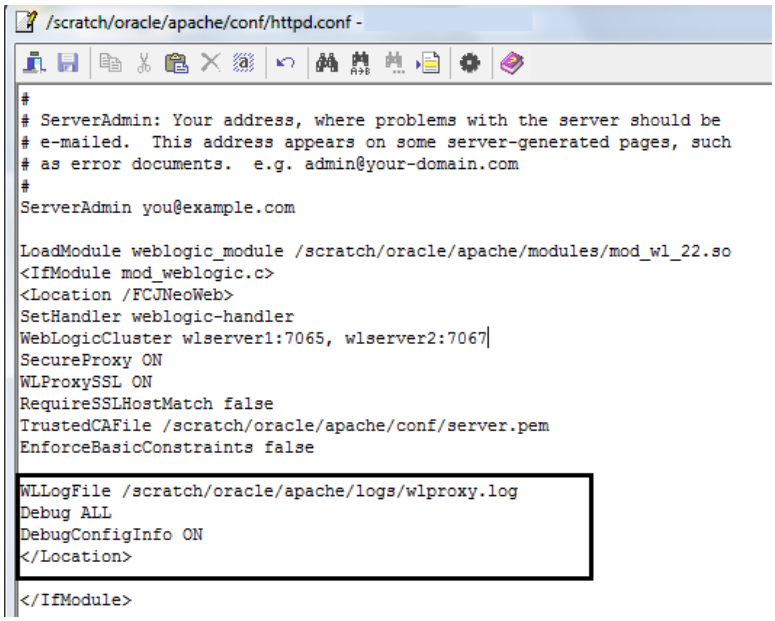


2. To enable debugging for communication between apache and weblogic add the following directives under Location tag

   WLLogFile <File path>

   Debug ALL

   DebugConfigInfo ON



Apache_Server_Configuration
[May] [2019]
Version 14.3.0.0.0

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 © 2007, 2019, 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.