List the modified as below:

1. Change the 8005port.

Status: modify

Operation:

Change ’<Server port="8005" shutdown="SHUTDOWN">’ to ‘<Server port="8005" shutdown="telenavPassword ">’ in conf/server.xml, if anyone telnet the tomcat server for 8005 port, it must input the “telenavPassword” to shut down the tomcat server.

1. Increase the firewall:

Status: propose

Operation:

inser rules: iptables -A INPUT -p tcp -m tcp --dport 8005 -j DROP save rules: service iptables save reload rules: service iptables save

1. Clear the conf/tomcat-user.xml.

Status: modify

Operation:

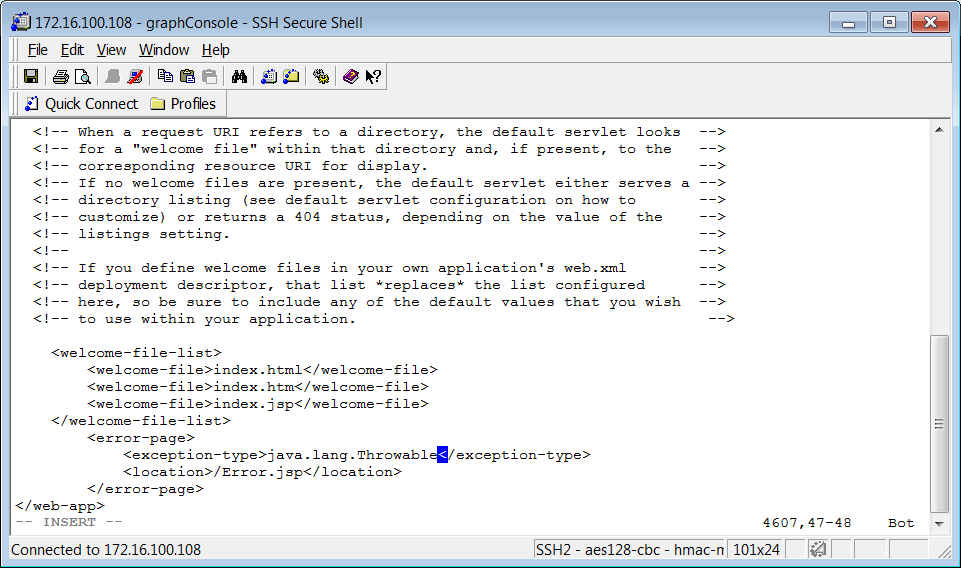
remove the webapp/manage directory

1. Add the customer error page, modified /conf.web as below:

Status: modify

Operation1:

cd /usr/local/apache-tomcat-7.0.42/conf/



Restart tomcat.

Operation2:

Status: testing

Chang the /lib/catalina/valves/ErrorReportValves.

1. Reduce the permission to start tomcat

Status: propose

Operation:

Root permission

[root@tomcat ~]# cd /usr/local/tomcat/bin/

[root@tomcat bin]# tar xf commons-daemon-native.tar.gz

[root@tomcat bin]# cd commons-daemon-1.0.15-native-src/unix

[root@tomcat unix]# ./configure –with-java=/usr/java/jdk1.8.0\_45/

[root@tomcat unix]# make

[root@tomcat unix]# cp jsvc /usr/local/tomcat/bin/

[root@tomcat bin]# cd /usr/local/tomcat/bin/

1. Close the 8009 need to disscuss.

Status: propose

Operation:

port 8009/tcp open ajp13

Reference : <http://blog.csdn.net/m8396017/article/details/51559739> (in eighth point)

1. Hide the version information.

Status: modify

Operation1:

<Connector port="8080" protocol="HTTP/1.1" server="DEV" connectionTimeout="20000"redirectPort="8443" />

Status: propose

Operation2:

[root@localhost ~]# cd /usr/local/apache-tomcat-7.0.53/lib

[root@localhost lib]# mkdir -p org/apache/catalina/util

[root@localhost lib]# cd org/apache/catalina/util

[root@localhost util]# vim ServerInfo.properties

server.info=nolinux //change the version to nolinux.

1. Shield directory files are automatically listed.

Status: modify

Operation:

<servlet>

        <servlet-name>default</servlet-name>

        <servlet-class>org.apache.catalina.servlets.DefaultServlet</servlet-class>

        <init-param>

            <param-name>debug</param-name>

            <param-value>0</param-value>

        </init-param>

        <init-param>

            <param-name>listings</param-name>

            <param-value>false</param-value>

        </init-param>

        <load-on-startup>1</load-on-startup>

    </servlet>

<param-value>false</param-value>

1. Set the session timeout.(default 30 minutes)

Status: propose

1. Close the auto deploy

Status: propose

Operaton:

<Host name="localhost" appBase=""unpackWARs="false" autoDeploy="false">

1. Set the tomcat connectionTimeOut.(default 20000)

Status : propose

1. Use customer hander protection.s

Status : not test.

Operation :

Reference the url:

<https://help.hana.ondemand.com/help/frameset.htm?e5be9994bb571014b575a785961062db.html>

https://help.sap.com/viewer/65de2977205c403bbc107264b8eccf4b/Cloud/enUS/3756f3fc7b4342d39db1bbe57d1b2d57.html

Reference the document as following :

<http://www.cnblogs.com/xiaoming279/p/6113781.html>

<http://blog.csdn.net/m8396017/article/details/51559739>

<https://www.owasp.org/index.php/Securing_tomcat>