Assignment - Security

Creating directories for certificate installation

```
root@ubuntu:/home/nevil# mkdir -p ca/root-ca/private ca/root-ca/db crl certs
root@ubuntu:/home/nevil# chmod 700 ca/root-ca/private
root@ubuntu:/home/nevil#
```

Creating the database and installing ntp

```
root@ubuntu:/home/nevil# cp /dev/null ca/root-ca/db/root-ca.db
root@ubuntu:/home/nevil# cp /dev/null ca/root-ca/db/root-ca.db.attr
root@ubuntu:/home/nevil# echo 01 > ca/root-ca/db/root-ca.crt.srl
root@ubuntu:/home/nevil#
root@ubuntu:/home/nevil#
root@ubuntu:/home/nevil# apt-get install ntp
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ntp is already the newest version (1:4.2.8p12+dfsg-3ubuntu4.1).
0 upgraded, 0 newly installed, 0 to remove and 177 not upgraded.
root@ubuntu:/home/nevil#
```

```
root@ubuntu:/home/nevil# cd /root/ca
root@ubuntu:~/ca# ls -lart
total 52
drw------- 2 root root 4096 Nov 20 17:10 crl
drw------- 2 root root 4096 Nov 20 17:13 private
-rw------- 1 root root    0 Nov 20 18:56 index.txt.old
-rw------- 1 root root    5 Nov 20 18:57 serial.old
-rw------- 1 root root 2082 Nov 20 19:01 cacert.pem
-rw-r--r-- 1 root root    5 Nov 20 19:13 serial
drw------- 2 root root 4096 Nov 20 19:13 requests
drw------- 2 root root 4096 Nov 20 19:13 newcerts
-rw-r--r-- 1 root root   21 Nov 20 19:13 index.txt.attr
-rw-r--r-- 1 root root  101 Nov 20 19:13 index.txt
drw------- 2 root root 4096 Nov 20 20:11 certs
drw------- 8 root root 4096 Nov 20 23:51 .
drwxr-xr-x 3 root root 4096 Nov 20 23:51 opt
drwx------ 9 root root 4096 Nov 22 12:01 ..
```

Generating the private key(cakey.pem) File and Set the Pass phrase

```
root@ubuntu:~/ca# cd requests/
root@ubuntu:~/ca/requests# ls -alrt
total 8
drw------- 2 root root 4096 Nov 20 17:10 .
drw------- 7 root root 4096 Nov 20 17:18 ..
root@ubuntu:~/ca/requests# pwd
/root/ca/requests
root@ubuntu:~/ca/requests# openssl genrsa -aes256 -out webserver.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
...........+++++
.....................................................+++++
e is 65537 (0x010001)
Enter pass phrase for webserver.pem:
Verifying - Enter pass phrase for webserver.pem:
root@ubuntu:~/ca/requests#
```

Creating root certificate(cacert.pem) with private key(cakey.pem) as input:

```
root@ubuntu: ~/ca
root@ubuntu:~/ca# openssl req -new -x509 -key /root/ca/private/cakey.pem -out cacert.pem -days 3650
Enter pass phrase for /root/ca/private/cakey.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:ca
Locality Name (eg, city) []:sjsu
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:SJSU
Common Name (e.g. server FQDN or YOUR name) []:nevil
Email Address []:nevilviplavbhai.shah@sjsu.edu
root@ubuntu:~/ca#
```

Editing the openssl file to change the directory (dir = /root/ca)

```
root@ubuntu:~/ca#
root@ubuntu:~/ca# chmod 600 -R /root/ca
root@ubuntu:~/ca#
root@ubuntu:~/ca# vim /usr/lib/ssl/openssl.cnf
```

```
####################################################################
[ CA_default ]

dir             = /root/ca              # Where everything is kept
certs           = $dir/certs            # Where the issued certs are kept
crl_dir         = $dir/crl              # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
#unique_subject = no                    # Set to 'no' to allow creation of
                                        # several certs with same subject.
new_certs_dir   = $dir/newcerts         # default place for new certs.

certificate     = $dir/cacert.pem       # The CA certificate
serial          = $dir/serial           # The current serial number
crlnumber       = $dir/crlnumber        # the current crl number
                                        # must be commented out to leave a V1 CRL
crl             = $dir/crl.pem          # The current CRL
private_key     = $dir/private/cakey.pem# The private key

x509_extensions = usr_cert              # The extensions to add to the cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt        = ca_default            # Subject Name options
cert_opt        = ca_default            # Certificate field options
```

Signing the certificate by initiating the requests.

```
root@ubuntu:/home/nevil# cd /root/ca
root@ubuntu:~/ca# cd requests/
root@ubuntu:~/ca/requests# ls -alrt
total 8
drw------- 2 root root 4096 Nov 20 17:10 .
drw------- 7 root root 4096 Nov 20 17:18 ..
root@ubuntu:~/ca/requests# pwd
/root/ca/requests
root@ubuntu:~/ca/requests# openssl genrsa -aes256 -out webserver.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.........+++++
.....................................................+++++
e is 65537 (0x010001)
Enter pass phrase for webserver.pem:
Verifying - Enter pass phrase for webserver.pem:
root@ubuntu:~/ca/requests# openssl req -new -key webserver.pem -out webserver.csr
```

Creating and saving the certificate requests in .csr format.

```
root@ubuntu:~/ca/requests# openssl req -new -key webserver.pem -out webserver.csr
Enter pass phrase for webserver.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SJSU
Organizational Unit Name (eg, section) []:SJSU
Common Name (e.g. server FQDN or YOUR name) []:Nevil
Email Address []:nevilviplavbhai.shah@sjsu.edu

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:root
An optional company name []:SJSU
root@ubuntu:~/ca/requests#
```

Signing the request certificate.

```
root@ubuntu:~/ca/requests#
root@ubuntu:~/ca/requests# openssl ca -in webserver.csr -out webserver.crt
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for /root/ca/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4660 (0x1234)
        Validity
            Not Before: Nov 21 03:12:51 2021 GMT
            Not After : Nov 21 03:12:51 2022 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = CA
            organizationName          = SJSU
            commonName                = nevil
            emailAddress              = nevilviplavbhai.shah@sjsu.edu
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                90:CB:A7:CF:30:E4:5A:77:1C:21:AD:65:27:52:47:24:E4:16:E8:27
            X509v3 Authority Key Identifier:
                keyid:B0:7A:D5:07:5D:CC:36:E2:1D:DA:EF:5A:04:A5:01:3E:64:23:4A:42

Certificate is to be certified until Nov 21 03:12:51 2022 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
root@ubuntu:~/ca/requests#
```

Installing Tomcat 9 and downloading the packages required for running tomcat services on the server

```
root@ubuntu:~/ca# apt install tomcat9 tomcat9-admin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tomcat9 is already the newest version (9.0.43-1).
tomcat9-admin is already the newest version (9.0.43-1).
0 upgraded, 0 newly installed, 0 to remove and 177 not upgraded.
root@ubuntu:~/ca# wget https://dlcdn.apache.org/tomcat/tomcat-9/v9.0.54/bin/apache-tomcat-9.0.54.tar.gz
--2021-11-22 13:14:54--  https://dlcdn.apache.org/tomcat/tomcat-9/v9.0.54/bin/apache-tomcat-9.0.54.tar.gz
Resolving dlcdn.apache.org (dlcdn.apache.org)... 151.101.2.132, 2a04:4e42::644
Connecting to dlcdn.apache.org (dlcdn.apache.org)|151.101.2.132|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11576317 (11M) [application/x-gzip]
Saving to: 'apache-tomcat-9.0.54.tar.gz'

apache-tomcat-9.0.54.tar.gz                     100%[=============================================================================================================>]  11.04M  17.3MB/s    in 0.6s

2021-11-22 13:14:56 (17.3 MB/s) - 'apache-tomcat-9.0.54.tar.gz' saved [11576317/11576317]

root@ubuntu:~/ca#
```

Allowing other ports to be enabled for tomcat service to run.

```
root@ubuntu:~/ca#
root@ubuntu:~/ca# sudo ufw allow from any to any port 8080 proto tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
root@ubuntu:~/ca#
```

Generating the keystore file

```
root@ubuntu:/home/nevil# keytool -genkey -keystore /home/nevil/.keystore -alias ALIAS -keyalg RSA -keysize 4096 -validity 720
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  nevil shah
What is the name of your organizational unit?
  [Unknown]:  SJSU
What is the name of your organization?
  [Unknown]:  SJSU
What is the name of your City or Locality?
  [Unknown]:  san jose
What is the name of your State or Province?
  [Unknown]:  california
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=nevil shah, OU=SJSU, O=SJSU, L=san jose, ST=california, C=US correct?
  [no]:
What is your first and last name?
  [nevil shah]:  nevil shah
What is the name of your organizational unit?
  [SJSU]:  SJSU
What is the name of your organization?
  [SJSU]:  SJSU
What is the name of your City or Locality?
  [san jose]:  san jose
What is the name of your State or Province?
  [california]:  california
What is the two-letter country code for this unit?
  [US]:  US
Is CN=nevil shah, OU=SJSU, O=SJSU, L=san jose, ST=california, C=US correct?
  [no]:  yes

root@ubuntu:/home/nevil#
```

Configuring Java environment for Tomcat service script

```
root@ubuntu:~/ca# cd ..
root@ubuntu:~# cd /etc/systemd/system
root@ubuntu:/etc/systemd/system# cat tomcat.service
[Unit]
Description=Apache Tomcat Web Application Container
After=network.target

[Service]
Type=forking

Environment=JAVA_HOME=/usr/lib/jvm/java-1.11.0-openjdk-amd64
Environment=CATALINA_PID=/opt/tomcat/temp/tomcat.pid
Environment=CATALINA_HOME=/opt/tomcat
Environment=CATALINA_BASE=/opt/tomcat
Environment='CATALINA_OPTS=-Xms512M -Xmx1024M -server -XX:+UseParallelGC'
Environment='JAVA_OPTS=-Djava.awt.headless=true -Djava.security.egd=file:/dev/./urandom'

ExecStart=/opt/tomcat/bin/startup.sh
ExecStop=/opt/tomcat/bin/shutdown.sh

User=tomcat
Group=tomcat
UMask=0007
RestartSec=10
Restart=always

[Install]
WantedBy=multi-user.target
root@ubuntu:/etc/systemd/system#
```

Verifying if port 8080 is enabled.

```
root@ubuntu:/etc# ss -ltn
State               Recv-Q              Send-Q                           Local Address:Port                           Peer Address:Port              Process
LISTEN              0                   4096                          127.0.0.53%lo:53                                  0.0.0.0:*
LISTEN              0                   128                               127.0.0.1:631                                 0.0.0.0:*
LISTEN              0                   1                          [::ffff:127.0.0.1]:8005                                  *:*
LISTEN              0                   100                                   *:8080                                        *:*
LISTEN              0                   128                                [::1]:631                                     [::]:*
root@ubuntu:/etc#
```

Running the tomcat service using startup script

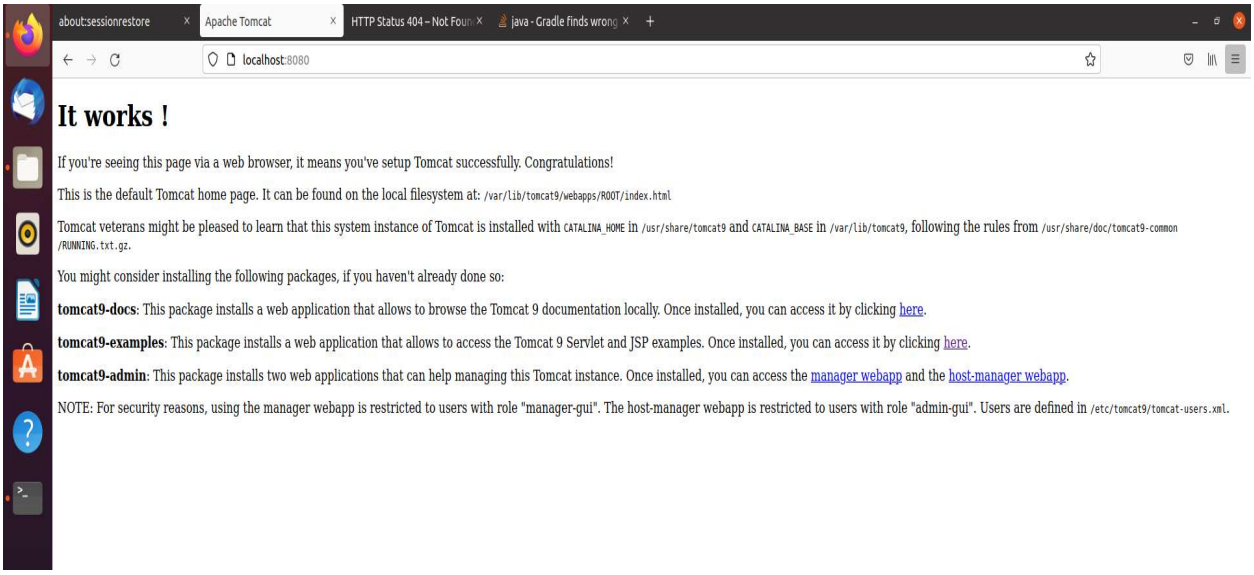
```
root@ubuntu:/etc#
root@ubuntu:/etc# cd /opt/tomcat/bin
root@ubuntu:/opt/tomcat/bin# ls
bootstrap.jar  catalina-tasks.xml  commons-daemon.jar            configtest.sh  digest.sh     setclasspath.bat  shutdown.sh  tomcat-juli.jar       tool-wrapper.sh
catalina.bat   ciphers.bat         commons-daemon-native.tar.gz  daemon.sh      makebase.bat  setclasspath.sh   startup.bat  tomcat-native.tar.gz  version.bat
catalina.sh    ciphers.sh          configtest.bat                digest.bat     makebase.sh   shutdown.bat      startup.sh   tool-wrapper.bat      version.sh
root@ubuntu:/opt/tomcat/bin# ./startup.sh
Using CATALINA_BASE:   /opt/tomcat
Using CATALINA_HOME:   /opt/tomcat
Using CATALINA_TMPDIR: /opt/tomcat/temp
Using JRE_HOME:        /usr
Using CLASSPATH:       /opt/tomcat/bin/bootstrap.jar:/opt/tomcat/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
root@ubuntu:/opt/tomcat/bin#
```

Here, the tomcat service has started .

Displaying Apache Tomcat on the Localhost:8080

```
status: unrecognized service
nevil@ubuntu:/etc/systemd/system$ service tomcat status
● tomcat.service - Apache Tomcat Web Application Container
     Loaded: loaded (/etc/systemd/system/tomcat.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2021-11-22 11:59:00 PST; 420ms ago
    Process: 89089 ExecStart=/opt/tomcat/bin/startup.sh (code=exited, status=0/SUCCESS)
   Main PID: 89099 (java)
      Tasks: 15 (limit: 4596)
     Memory: 28.4M
     CGroup: /system.slice/tomcat.service
             └─89099 /usr/lib/jvm/java-1.11.0-openjdk-amd64/bin/java -Djava.util.logging.config.file=/opt/tomcat/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager

Nov 22 11:59:00 ubuntu systemd[1]: Starting Apache Tomcat Web Application Container...
Nov 22 11:59:00 ubuntu startup.sh[89089]: Existing PID file found during start.
Nov 22 11:59:00 ubuntu startup.sh[89089]: Removing/clearing stale PID file.
Nov 22 11:59:00 ubuntu startup.sh[89089]: Tomcat started.
Nov 22 11:59:00 ubuntu systemd[1]: Started Apache Tomcat Web Application Container.
lines 1-15/15 (END)
```



Changing the group and permissions of all the files and folders present in /opt/tomcat location.

```
root@ubuntu:/opt/tomcat# chgrp -R tomcat /opt/tomcat/
root@ubuntu:/opt/tomcat# chmod -R g+r conf
root@ubuntu:/opt/tomcat# chmod  g+x conf
root@ubuntu:/opt/tomcat# ls -lart
total 156
drwxr-x--- 7 tomcat tomcat  4096 Sep 28 06:51 webapps
-rw-r----- 1 root   tomcat 16507 Sep 28 06:51 RUNNING.txt
-rw-r----- 1 root   tomcat  6898 Sep 28 06:51 RELEASE-NOTES
-rw-r----- 1 root   tomcat  3372 Sep 28 06:51 README.md
-rw-r----- 1 root   tomcat  2333 Sep 28 06:51 NOTICE
-rw-r----- 1 root   tomcat 57092 Sep 28 06:51 LICENSE
-rw-r----- 1 root   tomcat  6210 Sep 28 06:51 CONTRIBUTING.md
-rw-r----- 1 root   tomcat 18970 Sep 28 06:51 BUILDING.txt
drwxr-xr-x 4 root   root    4096 Nov 20 20:53 ..
drwxr-x--- 2 root   tomcat  4096 Nov 22 11:16 lib
drwxr-xr-x 9 tomcat tomcat  4096 Nov 22 11:16 .
drwxr-x--- 3 tomcat tomcat  4096 Nov 22 11:16 work
drwxr-x--- 2 tomcat tomcat  4096 Nov 22 11:21 logs
drwxr-x--- 2 root   tomcat  4096 Nov 22 11:43 bin
drwxr-x--- 3 root   tomcat  4096 Nov 22 12:01 conf
drwxr-x--- 2 tomcat tomcat  4096 Nov 22 13:30 temp
root@ubuntu:/opt/tomcat#
```

```
root@ubuntu:/opt/tomcat# vi /etc/systemd/system/tomcat.service
root@ubuntu:/opt/tomcat# systemctl daemon reload
Unknown command verb daemon.
root@ubuntu:/opt/tomcat# systemctl daemon-reload
root@ubuntu:/opt/tomcat# systemctl start tomcat
root@ubuntu:/opt/tomcat# systemctl enable tomcat
root@ubuntu:/opt/tomcat#
```

```
root@ubuntu:/opt/tomcat# cd conf/
root@ubuntu:/opt/tomcat/conf# vi tomcat-users.xml
root@ubuntu:/opt/tomcat/conf#
root@ubuntu:/opt/tomcat/conf# systemctl restart tomcat
root@ubuntu:/opt/tomcat/conf#
```

Enable SSL and configure the keystore file for tomcat to run on 8443 port .

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
keystoreFile="/home/nevil/.keystore" keystorePass="nevil9998704361"
clientAuth="false" sslProtocol="TLS" sslVerifyClient="optional"
sslEnabledProtocols="TLSv1.2,TLSv1.1,SSLv2Hello"/>

<!-- Define an SSL/TLS HTTP/1.1 Connector on port 8443 with HTTP/2
     This connector uses the APR/native implementation which always uses
     OpenSSL for TLS.
     Either JSSE or OpenSSL style configuration may be used. OpenSSL style
     configuration is used below.
-->
<!--
```

Tomcat webpage is being displayed using https with SSL certificate being enabled over the port 8443.