CHECKLIST

APACHE TOMCAT 8

1 Remove Extraneous Resources

2 Limit Server Platform Information Leaks

3 Protect the Shutdown Port

4 Protect Tomcat Configurations

5 Configure Realms

6 Connector Security

7 Establish and Protect Logging Facilities

8 Configure Catalina Policy

9 Application Deployment

10 Miscellaneous Configuration Settings

1.1 Remove extraneous files and directories

Audit:

Perform the following to determine the existence of extraneous resources:
1. List all files extraneous files. The following should yield no output:

```
$ ls -l $CATALINA_HOME/webapps/docs \ $CATALINA_HOME/webapps/examples
```

Remediation:

Perform the following to remove extraneous resources:
1. The following should yield no output:

```
$ rm -rf $CATALINA_HOME/webapps/docs \ $CATALINA_HOME/webapps/examples
```

If the Manager application is not utilized, also remove the following resources:

```
$ rm –rf $CATALINA_HOME/webapps/host-manager \ $CATALINA_HOME/webapps/manager
\ $CATALINA_HOME/conf/Catalina/localhost/manager.xml
```

1.2 Disable Unused Connectors

Audit:

Perform the following to identify configured `Connectors`:
1. Execute the following command to find configured Connectors. Ensure only those required are present and not commented out:

```
$ grep “Connector” $CATALINA_HOME/conf/server.xml
```

Remediation:

Perform the following to disable unused Connectors: 1. Within `$CATALINA_HOME/conf/server.xml`, remove or comment each unused `Connector`. For example, to disable an instance of the `HTTPConnector`, remove the following:

```
<Connector className="org.apache.catalina.connector.http.HttpConnector" ...
connectionTimeout="60000"/>
```

2.1 Alter the Advertised server.info String

Audit:

Perform the following to determine if the server.info value has been changed:
1. Extract the ServerInfo.properties file and examine the server.info attribute.

```
$ cd $CATALINA_HOME/lib $ jar xf catalina.jar
org/apache/catalina/util/ServerInfo.properties $ grep server.info
org/apache/catalina/util/ServerInfo.properties
```

Remediation:

Perform the following to alter the server platform string that gets displayed when clients connect to the tomcat server.
1. Extract the ServerInfo.properties file from the catalina.jar file:

```
$ cd $CATALINA_HOME/lib $ jar xf catalina.jar
org/apache/catalina/util/ServerInfo.properties
```

2. Navigate to the util directory that was created

```
cd org/apache/catalina/util
```

3. Open ServerInfo.properties in an editor
4. Update the server.info attribute in the ServerInfo.properties file.

```
server.info=<SomeWebServer>
5. Update the catalina.jar with the modified ServerInfo.properties file.
$ jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

2.2 Alter the Advertised server.number String

Audit:

Perform the following to determine if the server.number value has been changed:

1. Extract the ServerInfo.properties file and examine the server.number attribute.

```
$ cd $CATALINA_HOME/lib $ jar xf catalina.jar
org/apache/catalina/util/ServerInfo.properties $ grep server.number
org/apache/catalina/util/ServerInfo.properties
```

Remediation:

Perform the following to alter the server version string that gets displayed when clients connect to the server.

1. Extract the `ServerInfo.properties` file from the `catalina.jar` file:

```
$ cd $CATALINA_HOME/lib $ jar xf catalina.jar
org/apache/catalina/util/ServerInfo.properties
```

2. Navigate to the `util` directory that was created

```
$ cd org/apache/Catalina/util
```

3. Open `ServerInfo.properties` in an editor

4. Update the `server.number` attribute

```
server.number=<someversion>
```

5. Update the `catalina.jar` with the modified `ServerInfo.properties` file.

```
$ jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

2.3 Alter the Advertised server.built Date

Audit:

Perform the following to determine if the server.built value has been changed:

1. Extract the ServerInfo.properties file and examine the server.built attribute.

```
$ cd $CATALINA_HOME/lib $ jar xf catalina.jar
org/apache/catalina/util/ServerInfo.properties $ grep server.built
org/apache/catalina/util/ServerInfo.properties
```

Remediation:

Perform the following to alter the server version string that gets displayed when clients connect to the server.

1. Extract the ServerInfo.properties file from the catalina.jar file:

```
$ cd $CATALINA_HOME/lib $ jar xf catalina.jar
org/apache/catalina/util/ServerInfo.properties
```

2. Navigate to the util directory that was created

```
$ cd org/apache/Catalina/util
```

3. Open ServerInfo.properties in an editor

4. Update the server.built attribute in the ServerInfo.properties file.

```
server.built=
```

5. Update the catalina.jar with the modified ServerInfo.properties file.

```
$ jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

2.4 Disable X-Powered-By HTTP Header and Rename the Server Value for all Connectors

```
<Connector

 ...

 xpoweredBy="false" />
```

3.1 Set a nondeterministic Shutdown command value

Audit:

Perform the following to determine if the shutdown port is configured to use the default shutdown command:
1. Ensure the shutdown attribute in $CATALINA_HOME/conf/server.xml is not set to SHUTDOWN.

```
$ cd $CATALINA_HOME/conf $ grep ‘shutdown[[:space:]]*=[[:space:]]*″SHUTDOWN‶′
server.xml
```

Remediation:

Perform the following to set a nondeterministic value for the shutdown attribute.
1. Update the shutdown attribute in $CATALINA_HOME/conf/server.xml as follows:

```
<Server port="8005" shutdown="NONDETERMINISTICVALUE">
```

Note: NONDETERMINISTICVALUE should be replaced with a sequence of random characters.

3.2 Disable the Shutdown port

Audit:

Perform the following to determine if the shutdown port has been disabled:
1. Ensure the port attribute in $CATALINA_HOME/conf/server.xml is set to -1.

```
$ cd $CATALINA_HOME/conf/ $ grep
'<Server[[:space:]]\+[^>]*port[[:space:]]*=[[:space:]]*"-1"' server.xml
```

Remediation:

Perform the following to disable the Shutdown port.
1. Set the port to -1 in the $CATALINA_HOME/conf/server.xml file:

```
<Server port="-1" shutdown="SHUTDOWN">
```

4.1 Restrict access to $CATALINA_HOME

Audit:

Perform the following to ensure the permission on the $CATALINA_HOME directory prevent unauthorized modification.

```
$ cd $CATALINA_HOME $ find . -follow -maxdepth 0 \( -perm /o+rwx,g=w -o ! -
user tomcat_admin -o ! -group tomcat \) -ls
```

The above command should not emit any output.

Remediation:

Perform the following to establish the recommended state:
1. Set the ownership of the $CATALINA_HOME to tomcat_admin:tomcat.
2. Remove read, write, and execute permissions for the world
3. Remove write permissions for the group. 29 | P a g e

```
# chown tomcat_admin.tomcat $CATALINA_HOME # chmod g-w,o-rwx $CATALINA_HOME
```

4.2 Restrict access to $CATALINA_BASE

Audit:

Perform the following to ensure the permission on the $CATALINA_BASE directory prevent unauthorized modification.

```
$ cd $CATALINA_BASE $ find . -follow -maxdepth 0 \( -perm /o+rwx,g=w -
o ! -user tomcat_admin -o ! -group tomcat \) -ls
```

The above command should not emit any output.

Remediation:

Perform the following to establish the recommended state:
1. Set the ownership of the $CATALINA_BASE to **tomcat_admin:tomcat.**
2. Remove read, write, and execute permissions for the world
3. Remove write permissions for the group.

```
# chown tomcat_admin.tomcat $CATALINA_BASE # chmod g-w,o-rwx $CATALINA_BASE
```

4.3 Restrict access to Tomcat configuration directory

Audit:

Perform the following to determine if the ownership and permissions on $CATALINA_HOME/conf are securely configured.
1. Change to the location of the $CATALINA_HOME/conf and execute the following:

```
# cd $CATALINA_HOME/conf # find . -maxdepth 0 \( -perm /o+rwx,g=w -o ! -user
tomcat_admin -o ! -group tomcat \) -ls
```

Note: If the ownership and permission are set correctly, no output should be displayed when executing the above command.

Remediation:

Perform the following to restrict access to Tomcat configuration files:
1. Set the ownership of the $CATALINA_HOME/conf to **tomcat_admin:tomcat.**
2. Remove read, write, and execute permissions for the world
3. Remove write permissions for the group.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf # chmod g-w,o-rwx $CATALINA_HOME/conf
```

4.4 Restrict access to Tomcat logs directory

Audit:

Perform the following to determine if the ownership and permissions on $CATALINA_HOME/logs are securely configured.
1. Change to the location of the $CATALINA_HOME/logs and execute the following:

```
# cd $CATALINA_HOME # find logs -follow -maxdepth 0 \( -perm /o+rwx -o ! -
user tomcat_admin -o ! -group tomcat \) -ls
```

Note: If the ownership and permission are set correctly, no output should be displayed when executing the above command.

Remediation:

Perform the following to restrict access to Tomcat log files:
1. Set the ownership of the $CATALINA_HOME/logs to **tomcat_admin:tomcat.**
2. Remove read, write, and execute permissions for the world

```
# chown tomcat_admin:tomcat $CATALINA_HOME/logs # chmod o-rwx $CATALINA_HOME/logs
```

4.5 Restrict access to Tomcat temp directory

Audit:

Perform the following to determine if the ownership and permissions on $CATALINA_HOME/temp are securely configured.
1. Change to the location of the $CATALINA_HOME/temp and execute the following:

```
# cd $CATALINA_HOME # find temp -follow -maxdepth 0 \( -perm /o+rwx -o ! -
user tomcat_admin -o ! -group tomcat \) -ls
```

Note: If the ownership and permission are set correctly, no output should be displayed when executing the above command.

Remediation:

Perform the following to restrict access to Tomcat temp directory:
1. Set the ownership of the $CATALINA_HOME/temp to tomcat_admin:tomcat.
2. Remove read, write, and execute permissions for the world

```
# chown tomcat_admin:tomcat $CATALINA_HOME/temp # chmod o-rwx $CATALINA_HOME/temp
```

4.6 Restrict access to Tomcat binaries directory

Audit:

Perform the following to determine if the ownership and permissions on $CATALINA_HOME/bin are securely configured.
1. Change to the location of the $CATALINA_HOME/bin and execute the following:

```
# cd $CATALINA_HOME # find bin -follow -maxdepth 0 \( -perm /o+rwx,g=w -o ! -
user tomcat_admin -o ! -group tomcat \) -ls
```

Note: If the ownership and permission are set correctly, no output should be displayed when executing the above command.

Remediation:

Perform the following to restrict access to Tomcat bin directory:
1. Set the ownership of the $CATALINA_HOME/bin to tomcat_admin:tomcat.
2. Remove read, write, and execute permissions for the world

```
# chown tomcat_admin:tomcat $CATALINA_HOME/bin # chmod g-w,o-rwx $CATALINA_HOME/bin
```

4.7 Restrict access to Tomcat web application directory

Audit:

Perform the following to determine if the ownership and permissions on $CATALINA_HOME/webapps are securely configured.
1. Change to the location of the $CATALINA_HOME/webapps and execute the following:

```
# cd $CATALINA_HOME # find webapps -follow -maxdepth 0 \( -perm /o+rwx,g=w -o
! -user tomcat_admin -o ! -group tomcat \) -ls
```

Note: If the ownership and permission are set correctly, no output should be displayed when executing the above command.

Remediation:

Perform the following to restrict access to Tomcat webapps directory:
1. Set the ownership of the $CATALINA_HOME/webapps to tomcat_admin:tomcat.
2. Remove read, write, and execute permissions for the world.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/webapps # chmod g-w,o-rwx
$CATALINA_HOME/webapps
```

4.8 Restrict access to Tomcat catalina.policy

Audit:

Perform the following to determine if the ownership and permissions on $CATALINA_HOME/conf/catalina.policy care securely configured.
1. Change to the location of the $CATALINA_HOME/ and execute the following:

```
# cd $CATALINA_HOME/conf/ # find catalina.policy -follow -maxdepth 0 \( -perm
/o+rwx -o ! -user tomcat_admin -o ! -group tomcat \) -ls
```

Note: If the ownership and permission are set correctly, no output should be displayed when executing the above command.

Remediation:

Perform the following to restrict access to $CATALINA_HOME/conf/catalina.policy.
1. Set the owner and group owner of the contents of $CATALINA_HOME/conf/catalina.policy to tomcat_admin and tomcat, respectively.

```
# chmod 770 $CATALINA_HOME/conf/catalina.policy # chown tomcat_admin:tomcat
$CATALINA_HOME/conf/catalina.policy
```

4.9 Restrict access to Tomcat catalina.properties

Audit:

Perform the following to determine if the ownership and permissions on $CATALINA_HOME/conf/catalina.properties care securely configured.
1. Change to the location of the $CATALINA_HOME/ and execute the following:

```
# cd $CATALINA_HOME/conf/ # find catalina.properties -follow -maxdepth 0 \( -
perm /o+rwx,g=w -o ! -user tomcat_admin -o ! -group tomcat \) -ls
```

Note: If the ownership and permission are set correctly, no output should be displayed when executing the above command.

Remediation:

Perform the following to restrict access to catalina.properties:
1. Set the ownership of the $CATALINA_HOME/conf/catalina.properties to **tomcat_admin:tomcat.**
2. Remove read, write, and execute permissions for the world.
3. Remove write permissions for the group.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/catalina.properties # chmod
g-w,o-rwx $CATALINA_HOME/conf/catalina.properties
```

4.10 Restrict access to Tomcat context.xml

Audit:

Perform the following to determine if the ownership and permissions on $CATALINA_HOME/conf/context.xml care securely configured.
1. Change to the location of the $CATALINA_HOME/conf and execute the following:

```
# cd $CATALINA_HOME/conf # find context.xml -follow -maxdepth 0 \( -perm
/o+rwx,g=w -o ! -user tomcat_admin -o ! -group tomcat \) -ls
```

Note: If the ownership and permission are set correctly, no output should be displayed when executing the above command.

Remediation:

Perform the following to restrict access to context.xml:

1. Set the ownership of the $CATALINA_HOME/conf/context.xml to tomcat_admin:tomcat.
2. Remove read, write, and execute permissions for the world.
3. Remove write permissions for the group.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/context.
```

4.11 Restrict access to Tomcat logging.properties

Audit:

Perform the following to determine if the ownership and permissions on $CATALINA_HOME/conf/logging.properties care securely configured.

1. Change to the location of the $CATALINA_HOME/conf and execute the following:

```
# cd $CATALINA_HOME/conf/ # find logging.properties -follow -maxdepth 0 \( -
perm /o+rwx,g=w -o ! -user tomcat_admin -o ! -group tomcat \) -ls
```

Note: If the ownership and permission are set correctly, no output should be displayed when executing the above command.

Remediation:

Perform the following to restrict access to logging.properties:

1. Set the ownership of the $CATALINA_HOME/conf/logging.properties to **tomcat_admin:tomcat.**
2. Remove read, write, and execute permissions for the world.
3. Remove write permissions for the group.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/logging.properties # chmod g-
w,o-rwx $CATALINA_HOME/conf/logging.properties
```

4.12 Restrict access to Tomcat server.xml

Audit:

Perform the following to determine if the ownership and permissions on $CATALINA_HOME/conf/server.xml care securely configured.

1. Change to the location of the $CATALINA_HOME/conf and execute the following:

```
# cd $CATALINA_HOME/conf/ # find server.xml -follow -maxdepth 0 \( -perm
/o+rwx,g=w -o ! -user tomcat_admin -o ! -group tomcat \) -ls
```

Note: If the ownership and permission are set correctly, no output should be displayed when executing the above command.

Remediation:

Perform the following to restrict access to server.xml:

1. Set the ownership of the $CATALINA_HOME/conf/server.xml to **tomcat_admin:tomcat.**
2. Remove read, write, and execute permissions for the world.
3. Remove write permissions for the group.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/server.xml # chmod g-
w,o-rwx $CATALINA_HOME/conf/server.xml
```

4.13 Restrict access to Tomcat tomcat-users.xml

Audit:

Perform the following to determine if the ownership and permissions on $CATALINA_HOME/conf/tomcat-users.xml care securely configured.
1. Change to the location of the $CATALINA_HOME/conf and execute the following:

```
# cd $CATALINA_HOME/conf/ # find tomcat-users.xml -follow -maxdepth 0 \( -
perm /o+rwx,g=w -o ! -user tomcat_admin -o ! -group tomcat \) -ls
```

Note: If the ownership and permission are set correctly, no output should be displayed when executing the above command.

Remediation:

Perform the following to restrict access to tomcat-users.xml:
1. Set the ownership of the $CATALINA_HOME/conf/tomcat-users.xml to **tomcat_admin:tomcat**.
2. Remove read, write, and execute permissions for the world.
3. Remove write permissions for the group.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/tomcat-users.xml # chmod g-
w,o-rwx $CATALINA_HOME/conf/tomcat-users.xml
```

4.14 Restrict access to Tomcat web.xml

Audit:

Perform the following to determine if the ownership and permissions on $CATALINA_HOME/conf/web.xml care securely configured.
1. Change to the location of the $CATALINA_HOME/conf and execute the following:

```
# cd $CATALINA_HOME/conf/ # find web.xml -follow -maxdepth 0 \( -perm
/o+rwx,g=w -o ! -user tomcat_admin -o ! -group tomcat \) -ls
```

Note: If the ownership and permission are set correctly, no output should be displayed when executing the above command.

Remediation:

Perform the following to restrict access to web.xml:
1. Set the ownership of the $CATALINA_HOME/conf/web.xml to tomcat_admin:tomcat.
2. Remove read, write, and execute permissions for the world.
3. Remove write permissions for the group.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/web.xml # chmod g-w,o-
rwx $CATALINA_HOME/conf/web.xml
```

5.1 Use secure Realms

Audit:

Perform the following to ensure improper realm is not in use:

```
# grep "Realm className" $CATALINA_HOME/conf/server.xml | grep MemoryRealm #
grep "Realm className" $CATALINA_HOME/conf/server.xml | grep JDBCRealm
# grep "Realm className" $CATALINA_HOME/conf/server.xml | grep
UserDatabaseRealm
# grep "Realm className" $CATALINA_HOME/conf/server.xml | grep JAASRealm
```

The above commands should not emit any output.

5.2 Use LockOut Realms

Audit:

Perform the following to check to see if a LockOut realm is being used:

```
# grep "LockOutRealm" $CATALINA_HOME/conf/server.xml
```

Remediation:

Create a lockout realm wrapping the main realm like the example below:

```
<Realm className="org.apache.catalina.realm.LockOutRealm" failureCount="3"
lockOutTime="600" cacheSize="1000" cacheRemovalWarningTime="3600"> <Realm
className="org.apache.catalina.realm.DataSourceRealm" dataSourceName=... />
</Realm>
```

6.1 Setup Client-cert Authentication

Audit:

Review the Connector configuration in server.xml and ensure the clientAuth parameter is set to true.

Remediation:

In the Connector element, set the clientAuth parameter to true.

```
<-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 --> <Connector
port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
disableUploadTimeout="true" acceptCount="100" debug="0" scheme="https"
```

6.2 Ensure SSLEnabled is set to True for Sensitive Connectors

Audit:

Review server.xml and ensure all Connectors sending or receiving sensitive information have the SSLEnabled attribute set to true.

Remediation:

In server.xml, set the SSLEnabled attribute to true for each Connector that sends or receives sensitive information

```
<Connector
...
SSLEnabled="true"
...
/>
```

6.3 Ensure scheme is set accurately

Audit:

Review server.xml to ensure the Connector's scheme attribute is set to http for Connectors operating over HTTP. Also ensure the Connector's scheme attribute is set to https for Connectors operating over HTTPS.

Remediation:

In server.xml, set the Connector's scheme attribute to http for Connectors operating over HTTP. Set the Connector's scheme attribute to https for Connectors operating of HTTPS.

```
<Connector
  ...
scheme="https"
...
/>
```

6.4 Ensure secure is set to true only for SSL-enabled Connectors

Audit:

Review server.xml and ensure the secure attribute is set to true for those Connectors having SSLEnabled set to true. Also, ensure the secure attribute set to false for those Connectors having SSLEnabled set to false.

Remediation:

For each Connector defined in server.xml, set the secure attribute to true for those Connectors having SSLEnabled set to true. Set the secure attribute set to false for those Connectors having SSLEnabled set to false.

```
<Connector SSLEnabled="true"
  ...
 secure="true"
...
/>
```

6.5 Ensure SSL Protocol is set to TLS for Secure Connectors

Audit:

Review server.xml to ensure the sslProtocol attribute is set to TLS for all Connectors having SSLEngine set to on.

Remediation:

In server.xml, set the sslProtocol attribute to "TLS" for Connectors having SSLEnabled set to true.

```
<Connector
  ...
sslProtocol="TLS"
  ...
/>
```

7.2 Specify file handler in logging.properties files

Audit:

Review each application's logging.properties file located in the applications $CATALINA_BASE\webapps\<app name>\WEB-INF\classes directory and determine if the file handler properties are set.

```
$ grep handlers \ $CATALINA_BASE\webapps\<app name>\WEB-INF\classes\logging.properties
```

In the instance where an application specific logging has not been created, the logging.properties file will be located in $CATALINA_BASE\conf

```
$ grep handlers $CATALINA_BASE\conf\logging.properties
```

Remediation:

Add the following entries to your logging.properties file if they do not exist.

```
handlers=org.apache.juli.FileHandler, java.util.logging.ConsoleHandler
```

Ensure logging is not off and set the logging level to the desired level such as:

```
org.apache.juli.FileHandler.level=FINEST
```

7.3 Ensure className is set correctly in context.xml

Audit:

Execute the following to ensure className is set properly:

```
# grep org.apache.catalina.valves.AccessLogValve $CATALINA_BASE\webapps\<app
name>\META-INF\context.xml
```

Remediation:

Add the following statement into the $CATALINA_BASE\webapps\<app name>\META-INF\context.xml file if it does not already exist.

```
<Valve className="org.apache.catalina.valves.AccessLogValve"
directory="$CATALINA_HOME/logs/" prefix="access_log" fileDateFormat="yyyy-MM-
dd.HH" suffix=".log" pattern="%t %H cookie:%{SESSIONID}c
request:%{SESSIONID}r %m %U %s %q %r" />
```

7.4 Ensure directory in context.xml is a secure location

Audit:

Review the permissions of the directory specified by the directory setting to ensure the permissions are o-rwx and owned by tomcat_admin:tomcat:

```
# grep directory context.xml # ls –ld <log location>
```

Remediation:

Perform the following:

1. Add the following statement into the $CATALINA_BASE\webapps\<app-name>\META-INF\context.xml file if it does not already exist.

```
<Valve
className="org.apache.catalina.valves.AccessLogValve"
directory="$CATALINA_HOME/logs/" prefix="access_log" fileDateFormat="yyyy-MM-
dd.HH" suffix=".log"
pattern="%t %H cookie:%{SESSIONID}c request:%{SESSIONID}r %m %U %s %q %r"
/>
```

2. Set the location pointed to by the directory attribute to be owned by tomcat_admin:tomcat with permissions of o-rwx.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/logs # chmod o-rwx $CATALINA_HOME/logs
```

7.5 Ensure pattern in context.xml is correct

Audit:

Review the pattern settings to ensure it contains all the variables required by the installation.

```
# grep pattern $CATALINA_BASE\webapps\<app-name>\META-INF\context.xml
```

Remediation:

Add the following statement into the $CATALINA_BASE\webapps\<app-name>\META-INF\context.xml file if it does not already exist.

```
<Valve
className="org.apache.catalina.valves.AccessLogValve"
directory="$CATALINA_HOME/logs/" prefix="access_log"
fileDateFormat="yyyy-MM-dd.HH" suffix=".log"
pattern="%h %t %H cookie:%{SESSIONID}c request:%{SESSIONID}r %m %U %s
%q %r"
/>
```

7.6 Ensure directory in logging.properties is a secure location

Audit:

Review the permissions of the directory specified by the directory setting to ensure the permissions are o-rwx and owned by **tomcat_admin:tomcat:**

```
# grep directory logging.properties # ls –ld <log_location>
```

Remediation:

Perform the following:

1. Add the following properties into your logging.properties file if they do not exist

```
<application_name>.org.apache.juli.FileHandler.directory=<log_location>
<application_name>.org.apache.juli.FileHandler.prefix=<application_name>
```

2. Set the location pointed to by the directory attribute to be owned by tomcat_admin:tomcat with permissions of o-rwx.

```
# chown tomcat_admin:tomcat <log_location>
# chmod o-rwx <log_location>
```

7.7 Configure log file size limit

Audit:

Validate the max file limit is not greater than the size of the partition where the log files are stored.

Remediation:

Create the following entry in your logging.properties file. This field is specified in bytes.

```
java.util.logging.FileHandler.limit=10000
```

8.1 Restrict runtime access to sensitive packages

Audit:

Review package.access list in $CATALINA_BASE/conf/catalina.properties to ensure only allowed packages are defined.

Remediation:

Edit $CATALINA_BASE/conf/catalina.properties by adding allowed packages to the package.access list:

```
package.access =
sun.,org.apache.catalina.,org.apache.coyote.,org.apache.tomcat.,
org.apache.jasper
```

9.1 Starting Tomcat with Security Manager

Audit:

Review the startup configuration in /etc/init.d for Tomcat to ascertain if Tomcat is started with the -security option

Remediation:

The security policies implemented by the Java SecurityManager are configured in the $CATALINA_HOME/conf/catalina.policy file. Once you have configured the catalina.policy file for use with a SecurityManager, Tomcat can be started with a SecurityManager in place by using the --security option:

```
$ $CATALINA_HOME/bin/catalina.sh start -security (Unix) C:\>
%CATALINA_HOME%\bin\catalina start -security (Windows)
```

9.2 Disabling auto deployment of applications

Audit:

Perform the following to ensure autoDeploy is set to false.

```
# grep "autoDeploy" $CATALINA_HOME/conf/server.xml
```

Remediation:

In the $CATALINA_HOME/conf/server.xml file, change autoDeploy to false.

```
autoDeploy="false"
```

9.3 Disable deploy on startup of applications

Audit:

Perform the following to ensure deployOnStartup is set to false.

```
# grep "deployOnStartup" $CATALINA_HOME/conf/server.xml
```

Remediation:

In the $CATALINA_HOME/conf/server.xml file, change deployOnStartup to false.

```
deployOnStartup="false"
```

10.1 Ensure Web content directory is on a separate partition from the Tomcat system files

Audit:

Locate the Tomcat system files and web content directory. Review the system partitions and ensure the system files and web content directory are on separate partitions.

```
# df $CATALINA_HOME/webapps # df $CATALINA_HOME
```

Note: Use the default value "webapps" which is defined by "appBase" attribute here.

10.2 Restrict access to the web administration

Audit:

Review $CATALINA_HOME/conf/server.xml to ascertain that the RemoteAddrValve option is uncommented and configured to only allow access to systems required to connect.

Remediation:

For the administration application, edit $CATALINA_HOME/conf/server.xml and uncomment the following:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve" allow="127\.0\.0\.1"/>
```

Note: The RemoteAddrValve property expects a regular expression, therefore periods and other regular expression meta-characters must be escaped.

10.3 Restrict manager application

Remediation:

For the manager application, edit $CATALINA_BASE/conf/[enginename]/[hostname]/manager.xml, and add the bolded line:

```
<Context path="/manager" docBase="${catalina.home}/webapps/manager" debug="0"
privileged="true"> <Valve className="org.apache.catalina.valves.RemoteAddrValve"
allow="127\.0\.0\.1"/> <!-- Link to the user database we will get roles from -->
<ResourceLink name="users" global="UserDatabase"
type="org.apache.catalina.UserDatabase"/>
</Context>
```

10.4 Force SSL when accessing the manager application

Audit:

Ensure $CATALINA_HOME/webapps/manager/WEB-INF/web.xml has the <transport-guarantee> attribute set to CONFIDENTIAL.

```
# grep transport-guarantee $CATALINA_HOME/webapps/manager/WEB-INF/web.xml
```

Remediation:

Set $CATALINA_HOME/webapps/manager/WEB-INF/web.xml:

```
<security-constraint> <user-data-constraint> <transport-
guarantee>CONFIDENTIAL</transport-guarantee> <user-data-constraint>
</security-constraint>
```

10.5 Rename the manager application

Remediation:

Perform the following to rename the manager application:
1. Rename the manager application XML file:

```
# mv $CATALINA_HOME/webapps/host-manager/manager.xml \
$CATALINA_HOME/webapps/host-manager/new-name.xml
```

2. Update the docBase attribute within $CATALINA_HOME/webapps/host-manager/new-name.xml to ${catalina.home}/webapps/new-name
3. Move $CATALINA_HOME/webapps/manager to $CATALINA_HOME/webapps/new-name

```
# mv $CATALINA_HOME/webapps/manager $CATALINA_HOME/webapps/new-name
```

10.6 Enable strict servlet Compliance

Audit:

Ensure the above parameter is added to the startup script which by default is located at $CATALINA_HOME/bin/catalina.sh.

Remediation:

Start Tomcat with strict compliance enabled. Add the following to your startup script.

```
-Dorg.apache.catalina.STRICT_SERVLET_COMPLIANCE=true
```

10.7 Turn off session façade recycling

Audit:

Ensure the above parameter is added to the startup script which by default is located at $CATALINA_HOME/bin/catalina.sh.

Remediation:

Start Tomcat with RECYCLE_FACADES set to true. Add the following to your startup script.

```
-Dorg.apache.catalina.connector.RECYCLE_FACADES=true
```

10.8 Do not allow additional path delimiters

Remediation:

Start Tomcat with ALLOW_BACKSLASH set to false and ALLOW_ENCODED_SLASH set to false. Add the following to your startup script.

```
-Dorg.apache.catalina.connector.CoyoteAdapter.ALLOW_BACKSLASH=false
-Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=false
```

10.9 Do not allow custom header status messages

Audit:

Ensure the above parameter is added to the startup script which by default is located at $CATALINA_HOME/bin/catalina.sh.

Remediation:

Start Tomcat with USE_CUSTOM_STATUS_MSG_IN_HEADER set to false. Add the following to your startup script.

```
-Dorg.apache.coyote.USE_CUSTOM_STATUS_MSG_IN_HEADER=false
```

10.10 Configure connectionTimeout

Audit:

Locate each connectionTimeout setting in $CATALINA_HOME/conf/server.xml and verify the setting is correct.

```
# grep connectionTimeout $CATALINA_HOME/conf/server.xml
```

Remediation:

Within $CATALINA_HOME/conf/server.xml ensure each connector is configured to the connectionTimeout setting that is optimal based on hardware resources, load, and number of concurrent connections.

```
connectionTimeout="60000"
```

10.11 Configure maxHttpHeaderSize

Audit:

Locate each maxHttpHeaderSize setting in $CATALINA_HOME/conf/server.xml and verify that they are set to 8192.

```
# grep maxHttpHeaderSize $CATALINA_HOME/conf/server.xml
```

Remediation:

Within $CATALINA_HOME/conf/server.xml ensure each connector is configured to the appropriate maxHttpHeaderSize setting.

```
maxHttpHeaderSize=”8192”
```

10.12 Force SSL for all applications

Audit:

Ensure $CATALINA_HOME/conf/web.xml has the attribute set to CONFIDENTIAL.

```
# grep transport-guarantee $CATALINA_HOME/conf/web.xml
```

Remediation:

In $CATALINA_HOME/conf/web.xml, set the following:

```
<user-data-constraint> <transport-guarantee>CONFIDENTIAL</transport-
guarantee> <user-data-constraint>
```

10.13 Do not allow symbolic linking

Audit:

Ensure all context.xml have the allowLinking attribute set to false or allowLinking does not exist.

```
# find . -name context.xml | xargs grep "allowLinking"
```

Remediation:

In all context.xml, set the allowLinking attribute to false:

```
<Context ... <Resources ... allowLinking=″false″ /> ... </Context>
```

10.14 Do not run applications as privileged

Audit:

Ensure all context.xml have the privileged attribute set to false or privileged does not exist.

```
# find . -name context.xml | xargs grep "privileged"
```

Remediation:

In all context.xml, set the privileged attribute to false unless it is required like the manager application:

```
<Context ... privileged=″false″ />
```

10.15 Do not allow cross context requests

Audit:

Ensure all context.xml have the crossContext attribute set to false or crossContext does not exist.

```
# find . -name context.xml | xargs grep "crossContext"
```

Remediation:

In all context.xml, set the crossContext attribute to false:

```
<Context ... crossContext=″false″ />
```

10.16 Do not resolve hosts on logging valves

Audit:

Ensure Connector elements have the enableLookups attribute set to false or enableLookups does not exist.

```
# grep enableLookups $CATALINA_HOME/conf/server.xml
```

Remediation:

In Connector elements, set the enableLookups attribute to false or remove it.

```
<Connector ... enableLookups="false" />
```

10.17 Enable memory leak listener

Remediation:

Uncomment the JRE Memory Leak Prevention Listener in $CATALINA_HOME/conf/server.xml

```
<Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />
```

10.18 Setting Security Lifecycle Listener

```
<Listener className="org.apache.catalina.security.SecurityListener" checkedOsUsers="alex,bob"
minimumUmask="0007" />
```

10.19 use the logEffectiveWebXml and metadata-complete settings for deploying applications in production

Audit:

1. Review each application’s web.xml file located in the applications $CATALINA_BASE\<app name>\WEB-INF\web.xml and determine if the metadata-complete property is set.

```
<web-app
...
metadata-complete="true"
...
 >
```

2. Review each application’s context.xml file located in the applications $CATALINA_BASE\<app name>\META-INF\context.xml and determine if the metadata-complete property is set.

```
<Context
 ...
logEffectiveWebXml="true"
...
>
```