Seguridad SSL
Introducción

- Es posible configurar *Tomcat* para que sirva contenidos seguros usando el protocolo **SSL.**
- Existen dos posibilidades de configuración:
  - Utilizar la implementación SSL de Java (*Java SSL*).
  - Utilizar la implementación nativa ARP (*OpenSSL*).

	Java Blocking Connector BIO	Java Nio Blocking Connector NIO	APR/native Connector APR
Classname	Http11Protocol	Http11NioProtocol	Http11AprProtocol
Tomcat Version	3.x onwards	6.x onwards	5.5.x onwards
Support Polling	NO	YES	YES
Polling Size	N/A	maxConnections	maxConnections
Read HTTP Request	Blocking	Non Blocking	Blocking
Read HTTP Body	Blocking	Sim Blocking	Blocking
Write HTTP Response	Blocking	Sim Blocking	Blocking
Wait for next Request	Blocking	Non Blocking	Non Blocking
SSL Support	Java SSL	Java SSL	OpenSSL
SSL Handshake	Blocking	Non blocking	Blocking
Max Connections	maxConnections	maxConnections	maxConnections

Seguridad SSL
Introducción

- Web
  - http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html

Seguridad SSL
Implementación SSL de Java

- 1) Crear un almacén de claves con un certificado SSL (usando la herramienta **`Keytool`**)

```
alumno@ServidorLinux01:/var/lib/tomcat7$ sudo keytool -genkey -alias tomcat -key
alg RSA -keystore /var/lib/tomcat7/daw01keystore
Introduzca la contraseña del almacén de claves:
Volver a escribir la contraseña nueva:
¿Cuáles son su nombre y su apellido?
  [Unknown]:  servidorlinux01.daw01.net
¿Cuál es el nombre de su unidad de organización?
  [Unknown]:  tomcat
¿Cuál es el nombre de su organización?
  [Unknown]:  daw01.net
¿Cuál es el nombre de su ciudad o localidad?
  [Unknown]:  Madrid
¿Cuál es el nombre de su estado o provincia?
  [Unknown]:  Madrid
¿Cuál es el código de país de dos letras de la unidad?
  [Unknown]:  ES
¿Es correcto CN=servidorlinux01.daw01.net, OU=tomcat, O=daw01.net, L=Madrid, ST=
Madrid, C=ES?
  [no]:  si

Introduzca la contraseña de clave para <tomcat>
        (INTRO si es la misma contraseña que la del almacén de claves):
alumno@ServidorLinux01:/var/lib/tomcat7$
```

Seguridad SSL
Implementación SSL de Java

- 2) Configurar un conector SSL en *Tomcat*.

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
     This connector uses the JSSE configuration, when using APR, the
     connector should be using the OpenSSL style configuration
     described in the APR documentation -->

<Connector
    port="8443"
    protocol="HTTP/1.1"
    SSLEnabled="true"
    maxThreads="150"
    scheme="https" secure="true"
    clientAuth="false"
    sslProtocol="TLS"
    keystoreFile="/var/lib/tomcat7/daw01keystore" keystorePass="despliegue"
    keyAlias="tomcat" keyPass="despliegue"
  />
```

Seguridad SSL
Aplicaciones con HTTPS obligatorio

- Para obligar a que una aplicación solo responda a peticiones HTTPS hay que realizar la siguiente configuración en su descriptor de despliegue.

```
<security-constraint>
    <web-resource-collection>
        <web-resource-name>MemoryRealm</web-resource-name>
        <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <role-name>curso</role-name>
    </auth-constraint>
    <user-data-constraint>
        <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
</security-constraint>
```

Práctica

- Práctica 7.18
  - Seguridad SSL.

```
alumno@ServidorLinux01:/var/lib/tomcat7$ sudo keytool -genkey -alias tomcat -key
alg RSA -keystore /var/lib/tomcat7/daw01keystore
Introduzca la contraseña del almacén de claves:
Volver a escribir la contraseña nueva:
¿Cuáles son su nombre y su apellido?
  [Unknown]:  servidorlinux01.daw01.net
¿Cuál es el nombre de su unidad de organización?
  [Unknown]:  tomcat
¿Cuál es el nombre de s
  [Unknown]:  daw01.net
¿Cuál es el nombre de s
  [Unknown]:  Madrid
¿Cuál es el nombre de s
  [Unknown]:  Madrid
¿Cuál es el código de p
  [Unknown]:  ES
¿Es correcto CN=servido
Madrid, C=ES?
  [no]:  si

Introduzca la contraseñ
        (INTRO si es la
alumno@ServidorLinux01:
```

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
     This connector uses the JSSE configuration, when using APR, the
     connector should be using the OpenSSL style configuration
     described in the APR documentation -->

<Connector
    port="8443"
    protocol="HTTP/1.1"
    SSLEnabled="true"
    maxThreads="150"
    scheme="https" secure="true"
    clientAuth="false"
    sslProtocol="TLS"
    keystoreFile="/var/lib/tomcat7/daw01keystore" keystorePass="despliegue"
    keyAlias="tomcat" keyPass="despliegue"
  />
```

Biblografía

- *Apache Tomcat 7. Aleksa Vukotic y James Goodwill. Editorial Apress.*
- http://tomcat.apache.org
- http://wiki.apache.org/tomcat
- http://www.jguru.com/faq/java-tools/tomcat