

Cifrado Seguro en Servidores Tomcat 8 y anteriores

Para activar el Cifrado Seguro en servidores Tomcat (sea Windows o Linux), tendremos que acceder al archivo de configuración del Connector 443 u 8443.

El archivo se ubica en la carpeta de Tomcat /conf/server.xml

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
  maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
  clientAuth="false" sslProtocol="TLS" keystoreFile="/etc/tomcat/keystore.jks"
  keyAlias="server" keystorePass="123456"/>
```

En este archivo, deberemos hacer 2 configuraciones:

1. Buscar el atributo sslProtocol y modificar a: sslEnabledProtocols="TLSv1.2". En servidores con Java8 actualizado se puede colocar:
sslEnabledProtocols="TLSv1.2,TLSv1.3"
2. Agregar el atributo ciphers y colocarlo de la siguiente manera:

```
ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TL
S_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256"
```

En servidores con Java8 actualizado se puede colocar:

```
ciphers="TLS_AES_128_GCM_SHA256,TLS_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM
_SHA384,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TL
S_DHE_RSA_WITH_AES_128_GCM_SHA256"
```

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11Protocol"
  maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
  clientAuth="false" sslEnabledProtocols="TLSv1.2,TLSv1.3" keystoreFile="/etc/tomcat/keystore.jks"
  keyAlias="server" keystorePass="123456"
  ciphers="TLS_AES_128_GCM_SHA256,TLS_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256" />
```

Luego de estas configuraciones, se reinicia el servicio Tomcat y los cambios serán aplicados.

Notas:

- Java 6 no soporta TLS 1.1 o TLS 1.2, por lo que se recomienda actualizar.
- Java 7 no soporta cifrados con AEAD (Authenticated Encryption with Associated Data), por lo que se recomienda actualizar.

HSTS en Servidores Tomcat

Si quieres activar HSTS, debes hacer lo siguiente:

1. En la misma carpeta del archivo server.xml, acceder al archivo web.xml
2. Buscar el siguiente bloque de código por la línea 480 - 500 y descomentarlo.

```
<filter>
  <filter-name>httpHeaderSecurity</filter-name>
  <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
  <async-supported>true</async-supported>
</filter>
```

3. Editarlo con el siguiente código:

```
<filter>
  <filter-name>httpHeaderSecurity</filter-name>
  <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
  <async-supported>true</async-supported>
  <init-param>
    <param-name>hstsEnabled</param-name>
    <param-value>true</param-value>
  </init-param>
  <init-param>
    <param-name>hstsMaxAgeSeconds</param-name>
    <param-value>31536000</param-value>
  </init-param>
  <init-param>
    <param-name>hstsIncludeSubDomains</param-name>
    <param-value>true</param-value>
  </init-param>
</filter>
```

Deberá quedar así:

```
<filter>
  <filter-name>httpHeaderSecurity</filter-name>
  <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
  <async-supported>true</async-supported>
  <init-param>
    <param-name>hstsEnabled</param-name>
    <param-value>true</param-value>
  </init-param>
  <init-param>
    <param-name>hstsMaxAgeSeconds</param-name>
    <param-value>31536000</param-value>
  </init-param>
  <init-param>
    <param-name>hstsIncludeSubDomains</param-name>
    <param-value>true</param-value>
  </init-param>
</filter>
```

4. Buscar el siguiente bloque de código por la línea 570 - 600 y descomentarlo.

```
<filter-mapping>  
  <filter-name>httpHeaderSecurity</filter-name>  
  <url-pattern>/*</url-pattern>  
  <dispatcher>REQUEST</dispatcher>  
</filter-mapping>
```

Luego de un reinicio del servicio Tomcat, el subdominio incluirá las cabeceras de HSTS en los paquetes que viajen desde el servidor.