Tomcat trên Linux: Cài ??t SSL

admin Sun, Apr 14, 2019 Chứng Chỉ Số SSL Certificates 0 1799

?? cài ??t SSL cho Tomcat trên Linux b?n th?c hi?n nh? sau:

Nh?p SSL ???c c?p vào keystore:

1. Gi?i nén t?p tin ?ính kèm mà b?n nh?n ???c qua email ho?c t?i trên website và upload lên server (g?m 2 t?p tin tenmien.crt và tenmien.ca-bundle), l?u trong th? m?c /usr/local/ssl/keystore (th? m?c ?ã t?o ra trong lúc t?o CSR)
2. ??ng nh?p vào server v?i quy?n root qua ssh. Sau ?ó di chuy?n ??n th? m?c Java/bin
3. Ch?y l?nh:

```
keytool -import -trustcacerts -alias EVIntermediate -keystore
/usr/local/ssl/keystore/server.jks -file
/usr/local/ssl/keystore/tenmien.ca-bundle
```

4. Nh?p vào m?t kh?u là “**changeit**” khi ???c h?i.
5. Ch?y l?nh:

```
keytool -import -trustcacerts -alias tomcat -keystore
/usr/local/ssl/keystore/server.jks -file
/usr/local/ssl/keystore/tenmien.crt
```

6. Nh?p vào m?t kh?u là “**changeit**” khi ???c h?i.
7. Ch?ng th? s? ?ã ???c cài ??t thành công vào Keystore. B?n có th? ch?y l?nh sau ?? ki?m tra thông tin keystore:

```
keytool -list -keystore /usr/local/ssl/keystore/server.jks -v
```

C?u hình SSL cho Tomcat

1. Chuy?n ??n th? m?c Tomcat. Tìm t?p tin server.xml mà Tomcat ?ang s? d?ng và m? ra ?? ch?nh s?a.
2. C?p nh?t l?i ???ng d?n trong ?o?n sau ?ây:

```
clientAuth="false" sslProtocol="TLSv1" keyAlias="tomcat"
keystoreFile="/usr/local/ssl/keystore/server.jks"
keystorePass="your_keystore_password" />
```

3. L?u ý s?a port 8443 thành port 443
4. N?u b?n mu?n h? tr? TLS 1.1 và TLS 1.2 (n?u server c?a b?n là Tomcat >=7), b?n có th? thay ??i ph?n sslProtocols phía trên thành: sslProtocols="TLSv1,TLSv1.1,TLSv1.2"
5. M? port 443 trên Firewall (N?u b?n dùng software firewall nh? iptables ch?ng h?n thì có th? tìm th?y file config t?i: /etc/sysconfig/iptables)
6. Kh?i ??ng l?i Tomcat.

```
M?o: Dùng PFX
```

C?u hình dùng PFX trong Tomcat

T?i phiên b?n PFX trên máy ch? c?a chúng tôi ho?c t? chuy?n ??i sang PFX

C?p nh?t tham s? sau ? t?p tin server.xml

```
<Connector port="443" maxHttpHeaderSize="8192" maxThreads="150"
```

```
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https"
secure="true" SSLEnabled="true" clientAuth="false" sslProtocol="TLS"
keystoreFile="conf/mydomain.pfx"
keystorePass="your_keystore_password" keystoreType="PKCS12"/>
```