

Tomcat trên Linux: Cài đặt SSL

admin Sun, Apr 14, 2019 [Chứng Chỉ Số SSL Certificates](#) 0 2097

Để cài đặt SSL cho Tomcat trên Linux bạn thực hiện như sau:



Nhập SSL chứng chỉ vào keystore:

1. Tải về tệp tin đính kèm mà bạn nhận được qua email hoặc tải trên website và upload lên server (gồm 2 tệp tin `tenmien.crt` và `tenmien.ca-bundle`), lưu trong thư mục `/usr/local/ssl/keystore` (thư mục chưa tồn tại trong lúc tạo CSR)
2. Đăng nhập vào server với quyền root qua ssh. Sau đó di chuyển đến thư mục `Java/bin`
3. Chạy lệnh:

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

4. Nhập vào mật khẩu là **“changeit”** khi được hỏi.
5. Chạy lệnh:

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

6. Nhập vào mật khẩu là **changeit** khi được hỏi.
7. Chọn thế nào để cài đặt thành công vào Keystore. Bạn có thể chạy lệnh sau để kiểm tra thông tin keystore:

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

Cấu hình SSL cho Tomcat

1. Chuyển tên thư mục Tomcat. Tìm tệp tin server.xml mà Tomcat đang sử dụng và mở ra để chỉnh sửa.
2. Copy nhúng nội dung dưới đây:

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

3. Lưu ý sửa port 8443 thành port 443
4. Nếu bạn muốn hỗ trợ TLS 1.1 và TLS 1.2 (nếu server của bạn là Tomcat >=7), bạn có thể thay đổi phần sslProtocols phía trên thành:
sslProtocols="TLSv1,TLSv1.1,TLSv1.2"
5. Mở port 443 trên Firewall (Nếu bạn dùng software firewall như iptables chọn hướng thì có thể tìm thấy file config tại: /etc/sysconfig/iptables)
6. Khởi động lại Tomcat.

Mẹo: Dùng PFX

Cấu hình dùng PFX trong Tomcat

Tệp phiên bản PFX trên máy chủ của chúng tôi hoặc tải xuống từ sang PFX

Copy nhúng tham số sau vào tệp 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"/>
```

Online URL: <https://huongdan.maxserver.com/article-73.html>