匯智資訊 cloudmax

SSL 數位憑證

Tomcat 5.x / 6.x / 7.x 安裝說明

匯智資訊 cloudmax

匯智 資訊股份有限公司
10058 台灣台北市八德路一段 23 號 6 樓
6F, No.23, Sec. 1, Bade Rd., Taipei City 100, Taiwan
T. +886-2-2718-7200
F. +886-2-2718-1922

目錄

一、產生憑證請求檔

1. 執行下列命令產生 Keystore file

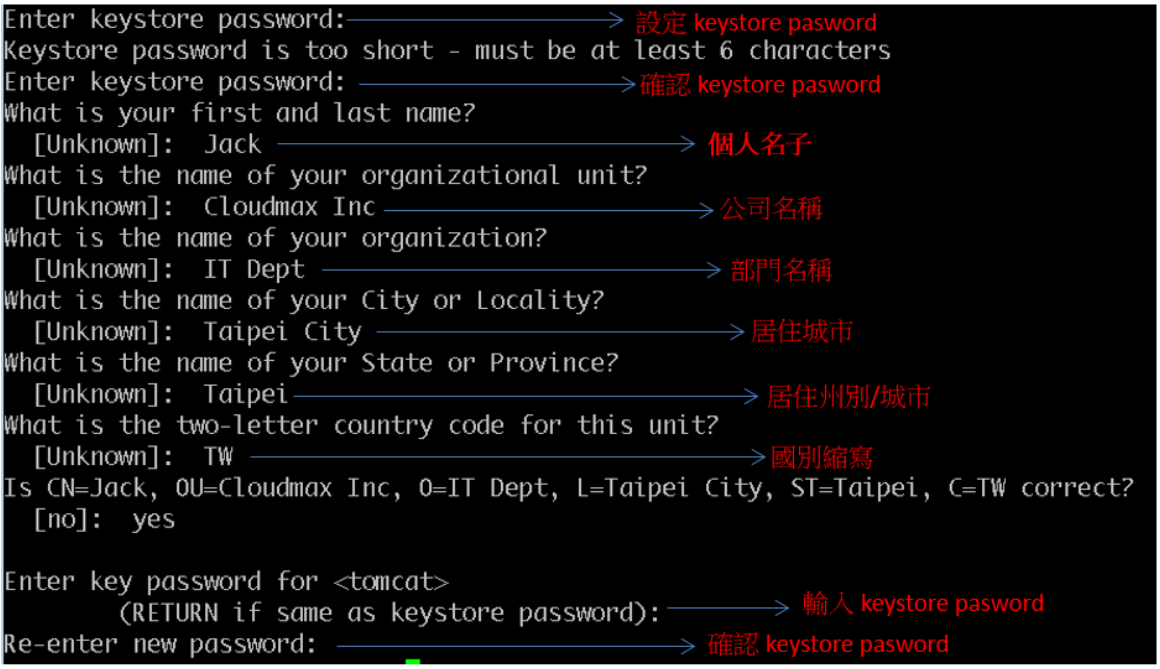
[Windows]

%JAVA_HOME%\bin\keytool -genkey -alias <your_keystore_filename> -keyalg RSA -keysize 2048 –keystore <your_keystore_filename>

[CentOS or RedHat]

$JAVA_HOME/bin/keytool -genkey -alias <your_keystore_filename> -keyalg RSA -keysize 2048 –keystore <your_keystore_filename>

2. 輸入憑證資訊



3. 產生憑證請求檔(CSR)

[Windows]

%JAVA_HOME%\bin\keytool -certreq -keyalg RSA -alias <your_domain_name> -file <your_csr_name> -keystore <your_keystore_filename>

[CentOS or RedHat]

$JAVA_HOME/bin/keytool -certreq -keyalg RSA -alias <your_domain_name> -file <your_csr_name> -keystore <your_keystore_filename>

二、憑證安裝

1. 安裝憑證 – 由 CSR 申請的憑證

1.1 安裝根憑證

[Windows]

%JAVA_HOME%\bin\keytool-import –alias <your_root_ca_name>-keystore <your_keystore_filename>-trustcacerts-file <your_root_filename>

[CentOS or RedHat]

$JAVA_HOME/bin/keytool –import –alias <your_root_ca_name>-keystore <your_root_ca_name>-trustcacerts-file <your_root_filename>

1.2 安裝中繼憑證

[Windows]

%JAVA_HOME%\bin\keytool –import-alias "intermed"-keystore <your_keystore_filename>-trustcacerts-file <your_intermediate_certificate_filename>

[CentOS or RedHat]

$JAVA_HOME/bin/keytool-import-alias " intermed "-keystore <your_keystore_filename>-trustcacerts-file <your_intermediate_certificate_filename>

1.3 安裝伺服器憑證

[Windows]

%JAVA_HOME%\bin\keytool-import-keystore <your_keystore_filename>-trustcacerts-file <your_name_of_the_certificate_filename>

[CentOS or RedHat]

$JAVA_HOME/bin/keytool-import-keystore <your_keystore_filename>-trustcacerts-file <your_name_of_the_certificate_filename>

2. 安裝憑證 - 由線上申請的憑證

2.1 將憑證資料轉換成 PKCS12 格式

openssl pkcs12 -export -in <your_server_cert>-inkey <your_server_key> -certfile <your_root_ca_cert> poc.cludmax.com.tw.p12

2.2 將 PKCS12 轉成 JKS 檔案格式

keytool -importkeystore -srckeystore <your_cert_p12_filepath> -destkeystore <your_keystore_filepath> -srcstoretype pkcs12

3. 設定 server.xml 設定檔

<

Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="<your_keystore_filepath>" keystorePass=" your_keystore_password"

/>

4. 重啟 tomcat service

三、憑證匯出（伺服器憑證匯出）

1. Windows

   %JAVA_HOME%/bin/keytool-export-keystore <your_keystore_filename>-alias <your_name_of_the_certificate>-file <your_ certificate_filename>

2. UNIX

   $JAVA_HOME/bin/keytool-export-keystore <your_keystore_filename>-alias <your_name_of_the_certificate>-file <your_ certificate_filename>