

Instalar/renovar certificado Jenkins

Para poder configurar que Jenkins vaya por HTTPS, tenemos que seguir los siguientes pasos.

Si ya tenemos un fichero **.pfx** o **.p12**, podemos saltarnos estos pasos.

- Para crear el fichero **.p12**, necesitamos el certificado, la key y la CA. Con ellos generaremos el fichero con el siguiente comando, donde `<password>` es la contraseña que queremos poner:

```
1 openssl pkcs12 -export -out b_pecunpay_es.p12 -passout 'pass:<password>' -inkey star_b_pecunpay_es.key -in STA
```

- Una vez creado, tendremos que generar el fichero **.jks**, que tendremos que tener instalado **keytool** para poder hacerlo. Con el siguiente comando generaremos el fichero, donde `<password>` es la contraseña que queremos poner:

```
1 keytool -importkeystore -srckeystore b_pecunpay_es.p12 -srcstorepass '<password>' -srcstoretype PKCS12 -srcali
```

- En el jenkins tendremos que configurar el fichero `/etc/sysconfig/jenkins`, en el caso de los CentOS y tendremos que añadir/modificar estos parametros para activar HTTPS, si ya lo tenemos activado y queremos renovar el certificado, sólo tendremos que sustituir el certificado de la ruta que indica.

```
1 JENKINS_PORT="-1"
2 JENKINS_HTTPS_PORT="8443"
3 JENKINS_HTTPS_KEYSTORE="/etc/jenkins/b_pecunpay_es.jks"
4 JENKINS_HTTPS_KEYSTORE_PASSWORD="<password>"
5 JENKINS_HTTPS_LISTEN_ADDRESS="0.0.0.0"
```

Con estos parametros deshabilitaremos que se puedan conectar por HTTP, indicaremos el puerto de HTTPS, la ruta del certificado, la contraseña del mismo y la dirección IP dónde se va a levantar el puerto HTTPS.