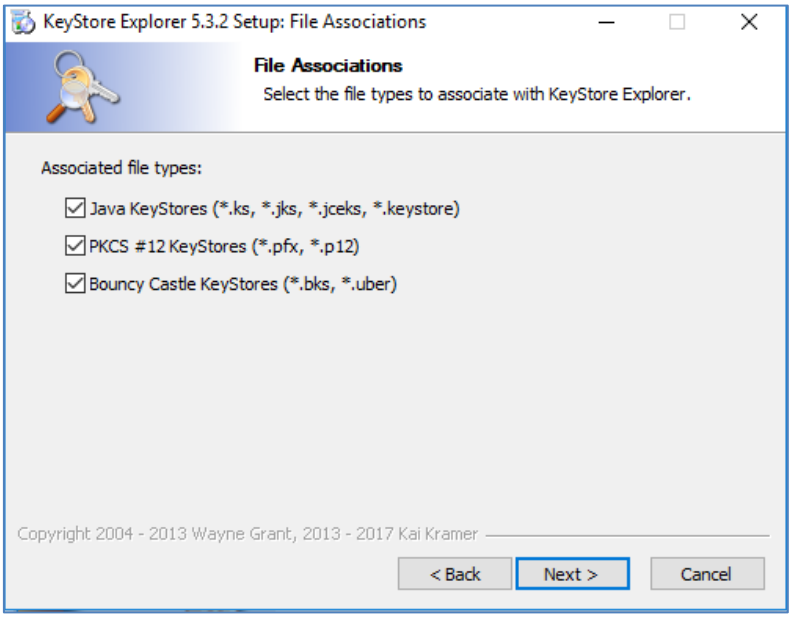
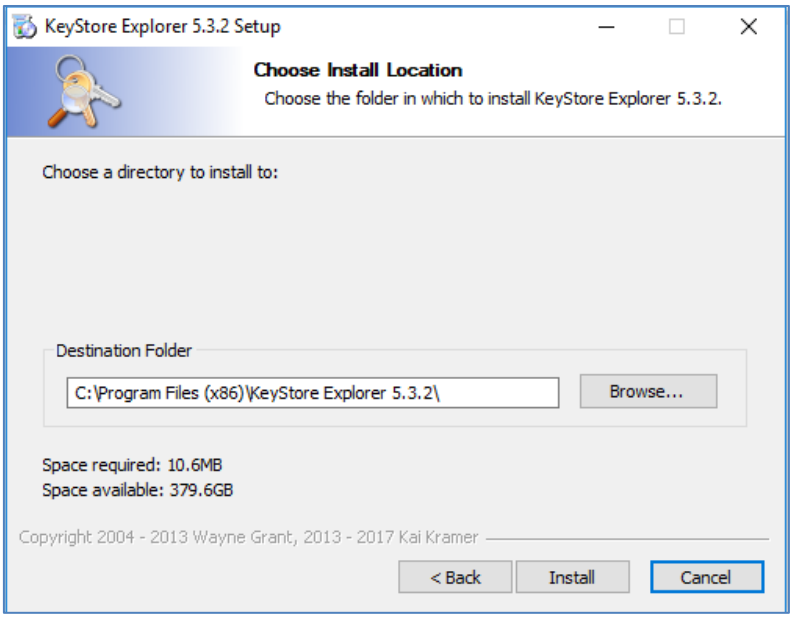
Instalación SSL Glassfish

Requisito: Tener java instalado

Si no cuenta con java lo puede descargar mediante este enlace:
https://www.java.com/es/download/

1. Ingresar al siguiente link y descargar el Keystore Explorer:
   https://www.bmtech.pe/certs/kse-532-setup.exe





2. Agregar nuestro certificado al keystore.jks

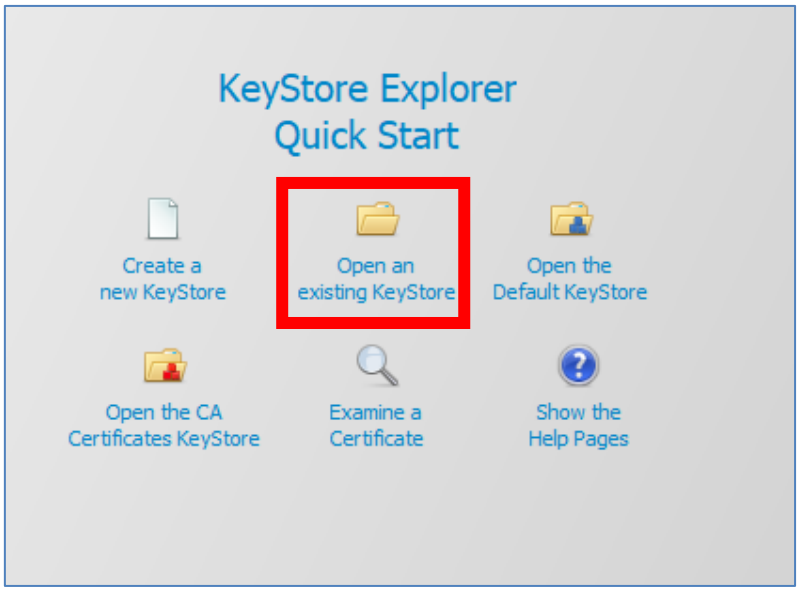
Archivos necesarios:

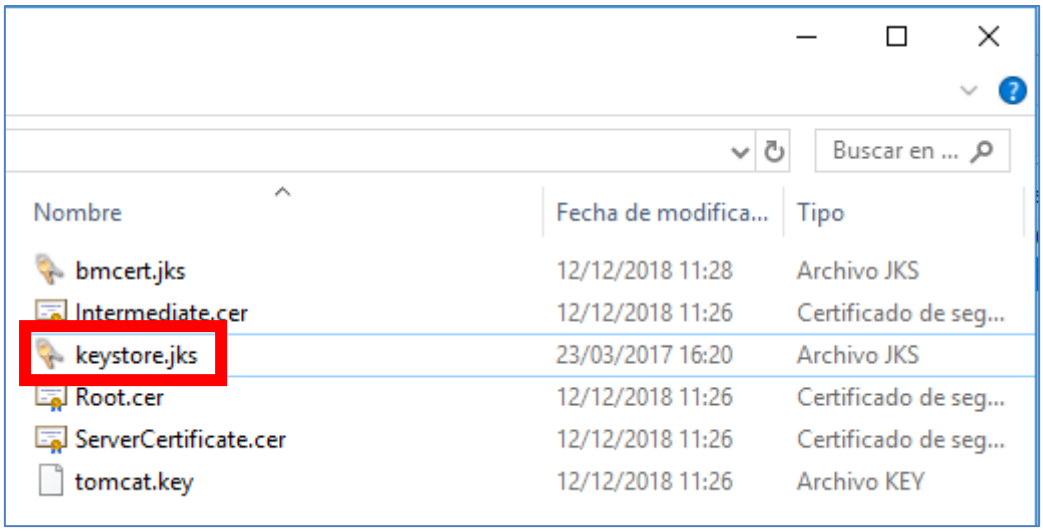
- Nuestros certificados: ServerCertificate, Intermediario y Root con extensión .crt o .cer
- Llave privada de nuestro certificado

También deberemos copiar el archivo keystore.jks desde el servidor del Glassfish,este se encuentra dentro de la carpeta config, ejm: /opt/glassfish5/glassfish/domains/domain1/config

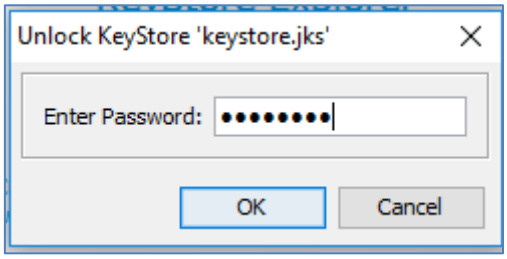
Una vez ubicado el archivo, lo copiamos a una carpeta en Windows donde se pueda modificar.

Abrimos el keystore.jks con el Keystore Explorer



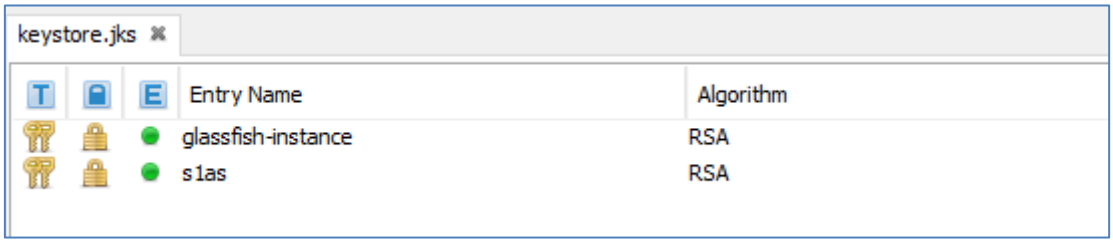


Nos pedirá una contraseña:

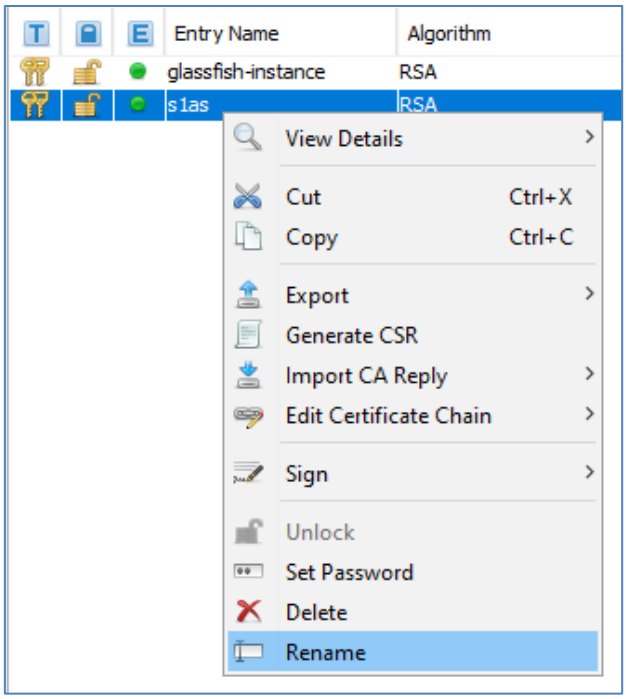


Contraseña por defecto: changeit

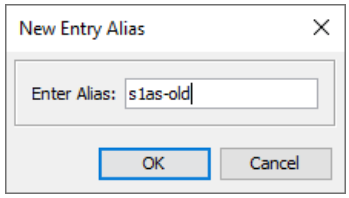
Nos muestra el contenido del keystore.jks



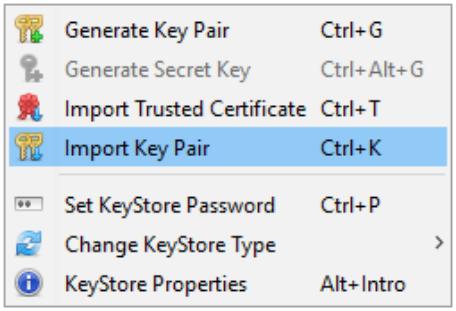
Lo que haremos será renombrar el certificado de alias **s1as** e importar el nuestro con el mismo alias.



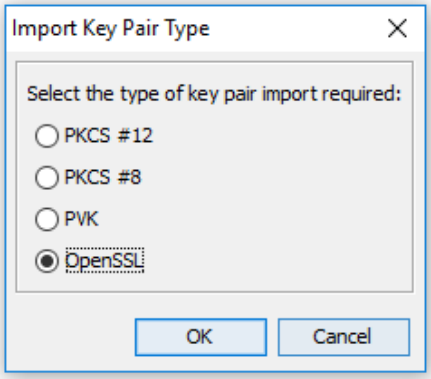
Lo renombramos como s1as-old y aceptamos



Ahora importaremos nuestro certificado: Click derecho en cualquier parte de la pantalla

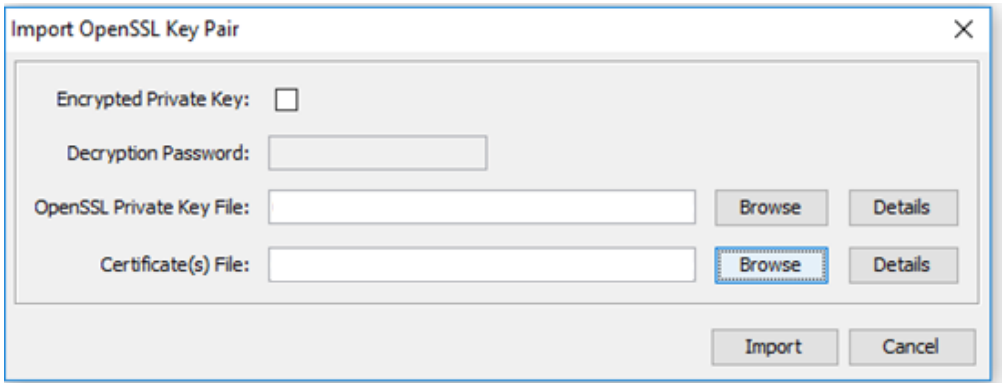


Escogemos el tipo de nuestra llave, si no estás seguro, elige OpenSSL

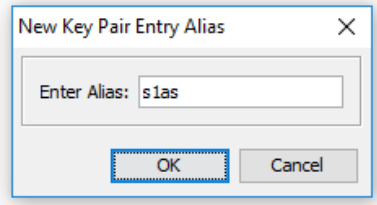


Seleccionamos la ruta de nuestra llave privada y nuestro certificado ServerCertificate

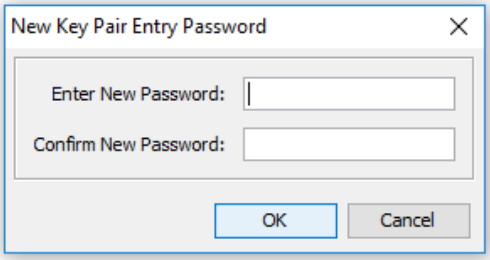
Le damos a Import, **desactivando** la casilla **Encrypted Private Key**



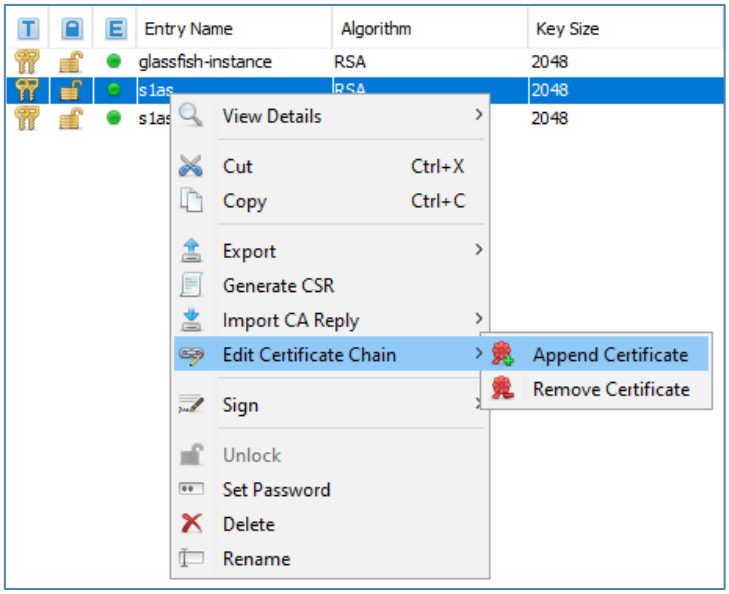
De alias, le colocamos: s1as **(OBLIGATORIO)**



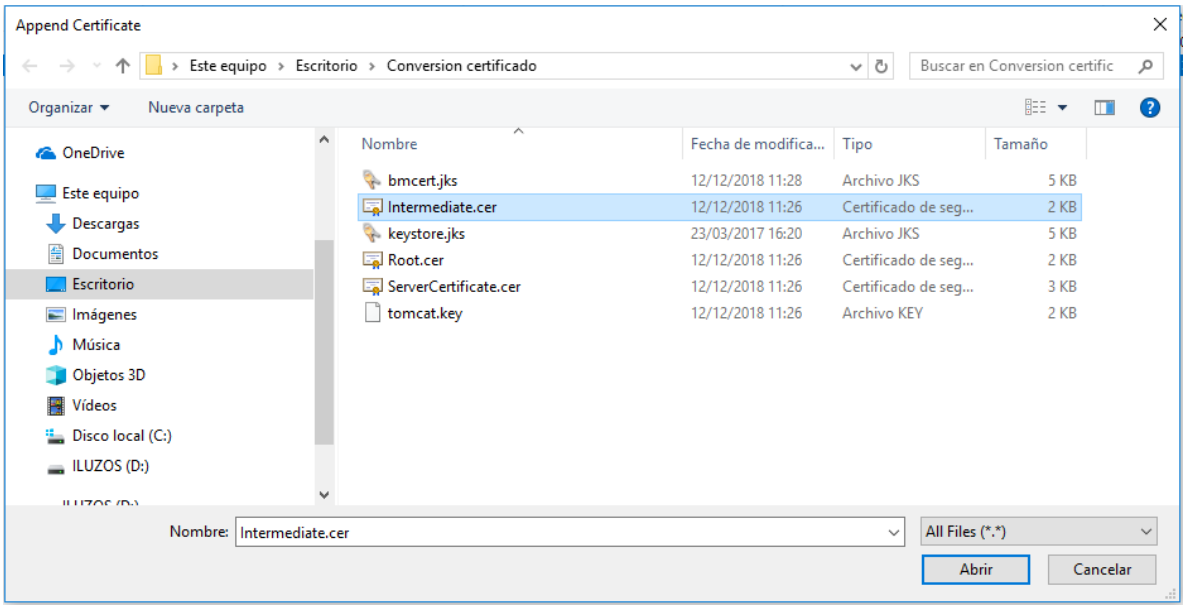
De contraseña: changeit **(OBLIGATORIO)**



Click derecho > Edit Certificate Chain > Append Certificate

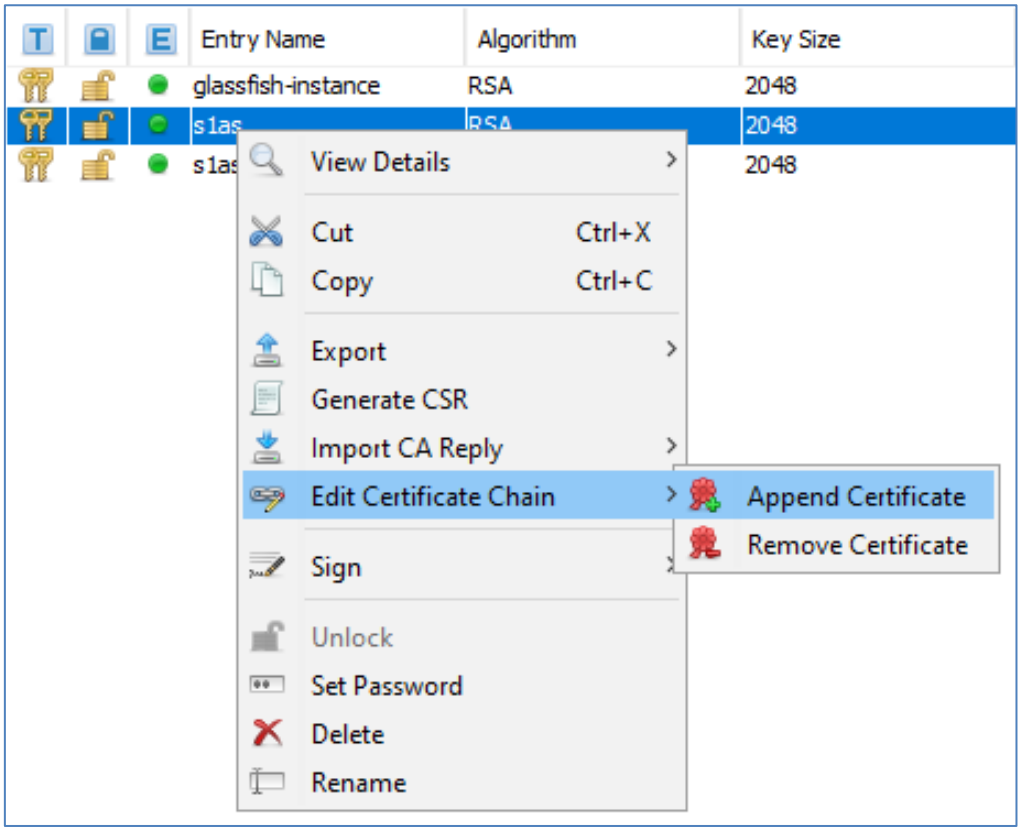


Seleccionamos el Intermediario

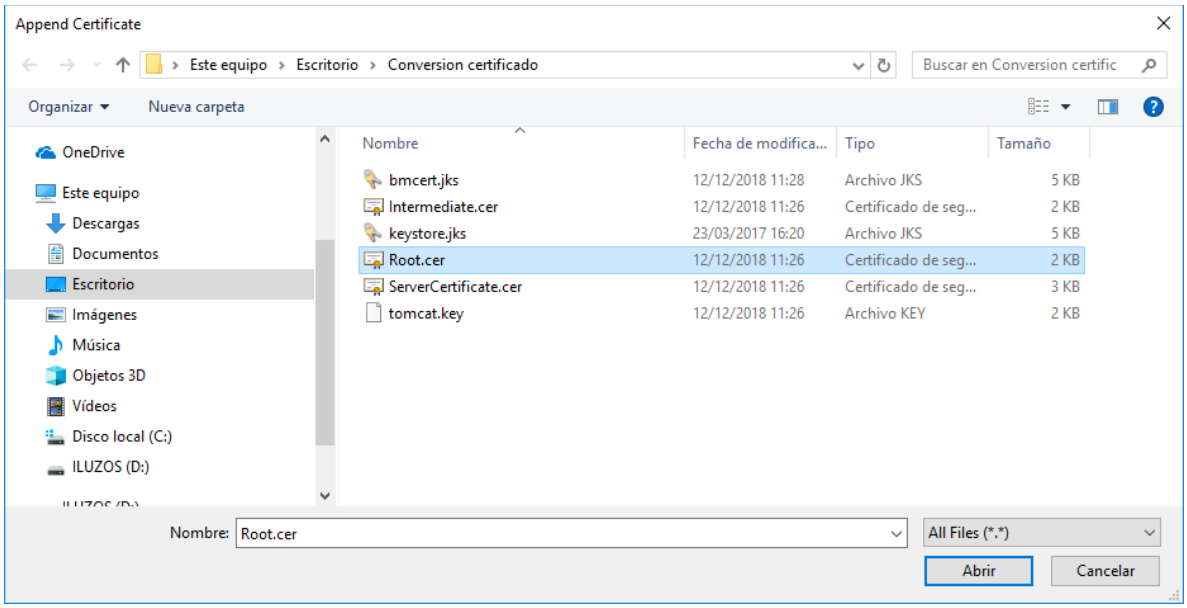


Realizamos el mismo procedimiento, y agregamos Root

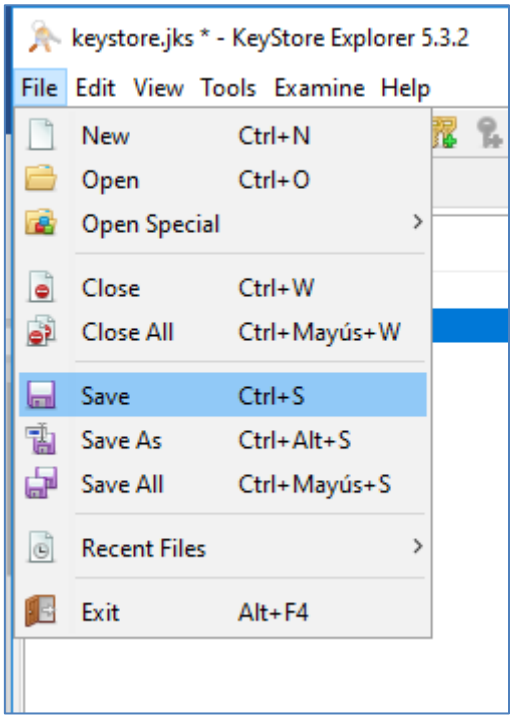
Click derecho > Edit Certificate Chain > Append Certificate



Seleccionamos el Root



Ahora guardamos el keystore.jks modificado



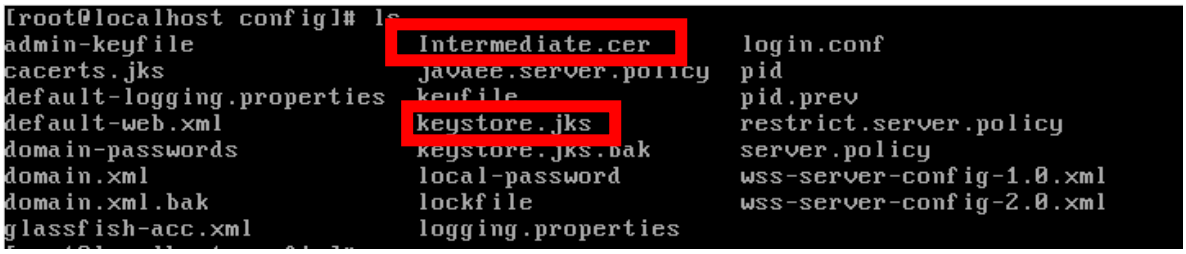
3. Configurar el Glassfish

Archivos necesarios:

- Nuevo keystore.jks (El cual acabamos de modificar)
- Certificado intermediario con extensión .crt o .cer

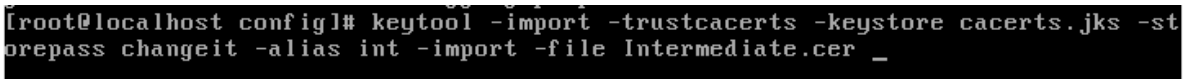
Copiamos los archivos indicados en la carpeta config donde se encuentre su dominio en el glassfish (se recomienda hacer backup del keystore.jks):

Por ejemplo: /opt/glassfish5/glassfish/domains/domain1/config



Ahora importamos nuestro certificado Intermediate en el cacerts.jks (Repositorio de confianza de java)

keytool -import -trustcacerts -keystore cacerts.jks -storepass changeit -alias int -file Intermediate.cer



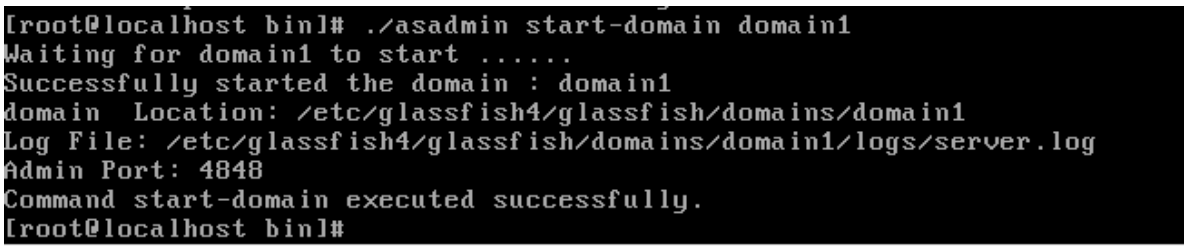
Nos saldrá un mensaje de confirmación

Apagamos el glassfish

Entramos a la carpeta bin del glassfish, ejemplo: glassfish5/bin

Ejecutamos: ./asadmin stop-domain domain1

Ahora lo iniciamos: ./asadmin start-domain domain1



Hecho esto, iniciará el glassfish pero no iniciará la consola del glassfish (que funciona por el puerto 4848), para que funcione ejecutamos: ./asadmin enable-secure-admin

Nos preguntará si confiamos en el certificado: Presionamos "**y**" para confirmar

Nos pide nuestras credenciales de la consola de glassfish

```
Enter admin user name>  admin
Enter admin password for user "admin"> _
```

Nos sale un mensaje de confirmación

```
You must restart all running servers for the change in secure admin to take effe
ct.
Command enable-secure-admin executed successfully.
```

Apagamos con: ./asadmin stop-domain domain1

```
[root@localhost config]# cd
[root@localhost ~]# cd /etc/glassfish4/bin/
[root@localhost bin]# ./asadmin stop-domain domain1
Waiting for the domain to stop .
Command stop-domain executed successfully.
[root@localhost bin]#
```

Ahora lo iniciamos: ./asadmin start-domain domain1

```
[root@localhost bin]# ./asadmin start-domain domain1
Waiting for domain1 to start ......
Successfully started the domain : domain1
domain  Location: /etc/glassfish4/glassfish/domains/domain1
Log File: /etc/glassfish4/glassfish/domains/domain1/logs/server.log
Admin Port: 4848
Command start-domain executed successfully.
[root@localhost bin]#
```

Y con esto queda listo, Glassfish debe funcionar con nuestro certificado.