## **BM Tech** Instalación SSL Glassfish

## Requisito: Tener java instalado

Si no cuenta con java lo puede descargar mediante este enlace: <a href="https://www.java.com/es/download/">https://www.java.com/es/download/</a>

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



< Back

Next >

Cancel

## **BM**Tech

👸 KeyStore Explorer 5.3.2 S	Setup		_		$\times$
A Contraction	Choose Install L Choose the folde	<b>.ocation</b> r in which to install Ki	eyStore Explo	orer 5.3.2	
Choose a directory to inst Destination Folder	all to:				
C:\Program Files (x86	)KeyStore Explorer	5.3.2\	Brow	/se	
Space available: 379.6GB					
Copyright 2004 - 2013 Wayn	e Grant, 2013 - 2017	Kai Kramer	Install	Canc	el

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

## **BM**Tech

		– 🗆 ×
		~ 🕐
	ں ^	Buscar en 🔎
Nombre	Fecha de modifica	Тіро
🗞 bmcert.jks	12/12/2018 11:28	Archivo JKS
Intermediate.cer	12/12/2018 11:26	Certificado de seg
🗞 keystore.jks	23/03/2017 16:20	Archivo JKS
Root.cer	12/12/2018 11:26	Certificado de seg
🔄 ServerCertificate.cer	12/12/2018 11:26	Certificado de seg
🗋 tomcat.key	12/12/2018 11:26	Archivo KEY

Nos pedirá una contraseña:

Unlock KeyStore 'keystore.jks'				
Enter Password:				
OK Cance	:I			

Contraseña por defecto: changeit

Nos muestra el contenido del keystore.jks

keyst	ore.jk	s Ж		
Ι		E	Entry Name	Algorithm
17		۲	glassfish-instance	RSA
T		۲	slas	RSA

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



T E Entry	Name	•	Algorithm	
🃅 💼 💿 glassfi	sh-ins	tance	RSA	
🎢 🖆 🧧 s1as			RSA	
	Q	View Detail	s	>
	$\ge$	Cut		Ctrl+X
	L)	Сору		Ctrl+C
	1	Export		>
		Generate C	SR	
	*	Import CA	Reply	>
	9	Edit Certific	ate Chain	>
	2	Sign		>
	л£	Unlock		
	00	Set Passwo	rd	
	X	Delete		
	Ť	Rename		

Lo renombramos como s1as-old y aceptamos

New Entry Alias	
Enter Alias: s1as-old	
ОК	Cancel

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



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

Import Key Pair Type	×
Select the type of key pair import requi	red:
O PKCS #12	
O PKCS #8	
⊖ рук	
OpenSSL	
OK Cance	4



Seleccionamos la ruta de nuestra llave privada y nuestro certificado ServerCertificate

Le damos a Import, desactivando la casilla Encrypted Private Key

Import OpenSSL Key Pair		×
Encrypted Private Key:		
Decryption Password:		
OpenSSL Private Key File:	Browse	Details
Certificate(s) File:	Browse	Details
	Import	Cancel

De alias, le colocamos: s1as (OBLIGATORIO)

New Key Pair Entry Alias		
Enter Alias: s1as		
OK Cancel		

De contraseña: changeit (OBLIGATORIO)

New Key Pair Entry Password		
Enter New Password:		
Confirm New Password:		
ОК Са	ncel	

Click derecho > Edit Certificate Chain > Append Certificate





opend Certificate					
→ × ↑ 📙 > Este equipo > Esc	critorio > Conversion certificado		✓ כ Buscar er	n Conversion cer	tific 🎾
Organizar 🔻 Nueva carpeta					
aneDrive	Nombre	Fecha de modifica	Tipo	Tamaño	
Esta anuina	🗞 bmcert.jks	12/12/2018 11:28	Archivo JKS	5 KB	
	🔄 Intermediate.cer	12/12/2018 11:26	Certificado de seg	2 KB	
🔶 Descargas	💊 keystore.jks	23/03/2017 16:20	Archivo JKS	5 KB	
Documentos	Root.cer	12/12/2018 11:26	Certificado de seg	2 KB	
🔜 Escritorio	ServerCertificate.cer	12/12/2018 11:26	Certificado de seg	3 KB	
📰 Imágenes	tomcat.key	12/12/2018 11:26	Archivo KEY	2 KB	
👌 Música					
🗊 Objetos 3D					
Vídeos					
Lisco local (C:)					
🔜 ILUZOS (D:)					
	¥				
Nombre: Intermediat	te.cer		✓ All Files	(*.*)	`
			Ab	rir Ca	ancelar

Realizamos el mismo procedimiento, y agregamos Root

Click derecho > Edit Certificate Chain > Append Certificate





Seleccionamos el Root

Append Certificate					×
← → · · ↑ → Este equipo >	Escritorio > Conversion cert	ificado	ٽ ~	Buscar en Conversi	ion certific 🔎
Organizar 👻 Nueva carpeta					• 🔳 🕐
🝊 OneDrive	^ Nombre	^ Fecha de	e modifica Tipo	Tamaño	>
Este equino	💊 bmcert.jks	12/12/20	)18 11:28 Archivo J	KS	5 KB
	🔄 Intermediate.ce	r 12/12/20	018 11:26 Certificad	lo de seg	2 KB
Descargas	💊 keystore.jks	23/03/20	)17 16:20 Archivo J	KS	5 KB
Documentos	📮 Root.cer	12/12/20	)18 11:26 Certificad	lo de seg	2 KB
Escritorio	ServerCertificate	e.cer 12/12/20	)18 11:26 Certificad	lo de seg	3 KB
📰 Imágenes	tomcat.key	12/12/20	)18 11:26 Archivo k	(EY	2 KB
👌 Música					
🧊 Objetos 3D					
🗃 Vídeos					
🏪 Disco local (C:)					
ILUZOS (D:)					
11170C (D.)	¥				
Nombre: Root.ce	er		~	All Files (*.*)	~
				Abrir	Cancelar

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



[root@localhost config]# l	•	
admin-keyfile 🛛 🖉	Intermediate.cer	log in . conf
cacerts.jks	javaee.server.policy	pid
default-logging.properties	keufile	pid.prev
default-web.xml	keystore.jks	restrict.server.policy
domain-passwords	кеуstore.jкs.bak	server.policy
domain.xml	local-password	wss-server-config-1.0.xml
domain.xml.bak	lockfile	wss-server-config-2.0.xml
glassfish-acc.xml	logging.properties	

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

Iroot@localhost config1# keytool -import -trustcacerts -keystore cacerts.jks -st
orepass changeit -alias int -import -file Intermediate.cer \_

Nos saldrá un mensaje de confirmación

Se ha agregado el certificado al almacén de claves

Apagamos el glassfish

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

Ejecutamos: ./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]#
```

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

[root@localhost bin]# ./asadmin enable-secure-admin

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

]							
Do	you	trust	the	above	certificate	[y¦N]	>y_

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.