

Appeler un web service Soap sécurisé depuis un programme web

La problématique

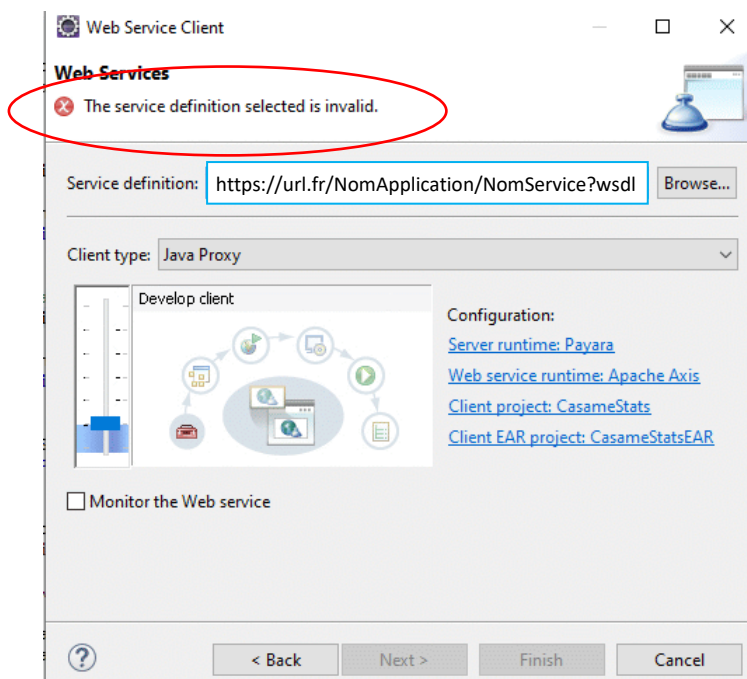
Les webservices accessibles via une url sécurisée sont un peu plus difficile à interroger. C'est à la fois un problème de l'IDE Eclipse, mais aussi du certificat qu'il convient d'importer dans le serveur utilisé (Glassfish dans cette documentation).

Il y a donc 2 problèmes à résoudre :

- 1ère problème : Créer l'accès client du WS sous Eclipse
- 2e problème : Corriger l'erreur d'accès au certificat pour le programme java

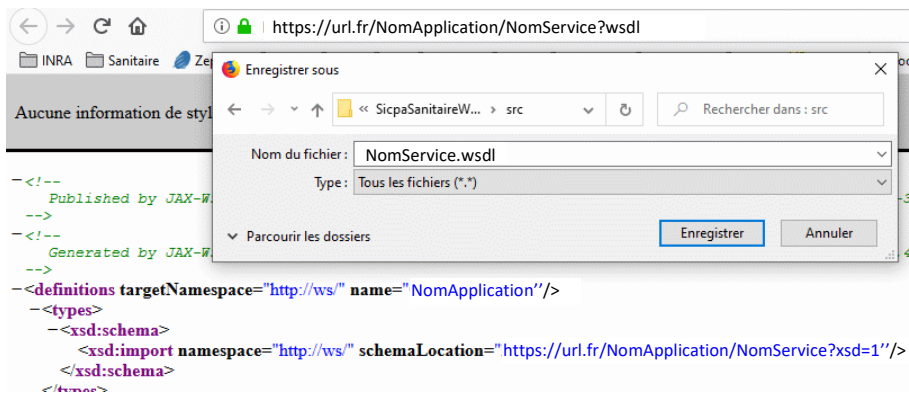
1ère problème : Créer l'accès client du WS sous Eclipse

Quand on utilise l'assistant pour l'accès client d'un WS existant, l'adresse est considérée comme invalide.

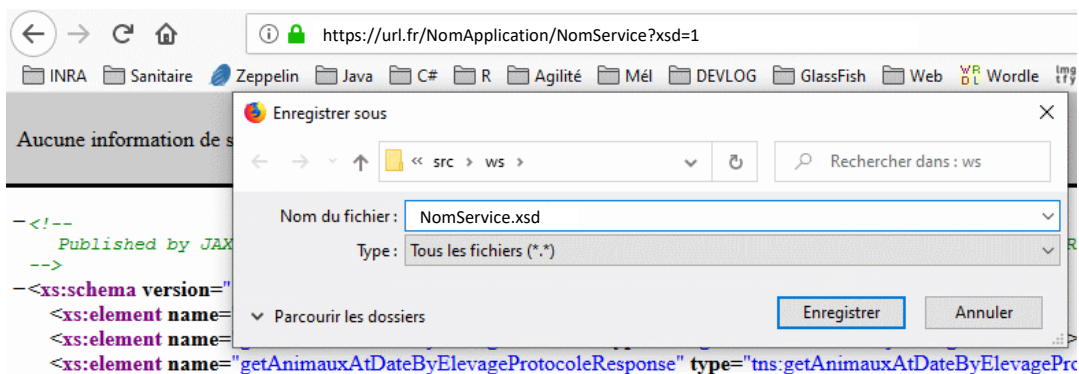


Solution pour résoudre ce problème

1. Lancer un navigateur et renseigner l'adresse wsdl du webservice



2. Enregistrer en local le fichier .wsdl
3. Renseigner, maintenant, l'adresse du xsd

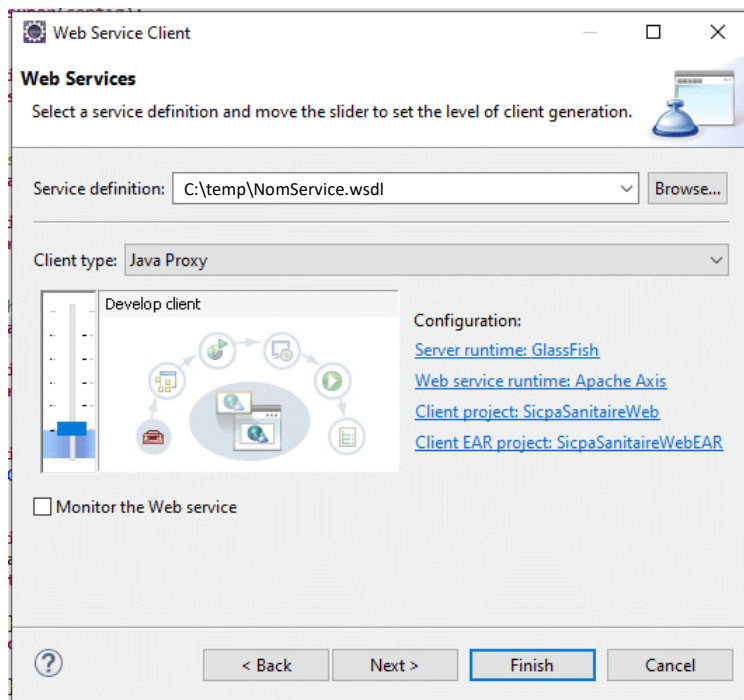


4. Enregistrer en local le fichier .xsd
5. Ouvrir le fichier .wsdl et renommer l'appel du fichier xsd

```

1 <?xml version='1.0' encoding='UTF-8'?><!-- Published by JAX-WS
2 <types>
3 <xsd:schema>
4 <xsd:import namespace="http://ws/" schemaLocation="NomService.xsd"/>
5 </xsd:schema>
6 </types>
  
```

6. Pour finir, dans l'assistant pour l'accès client d'un WS existant, renseigner le fichier wsdl



2^e problème : erreur d'accès au certificat

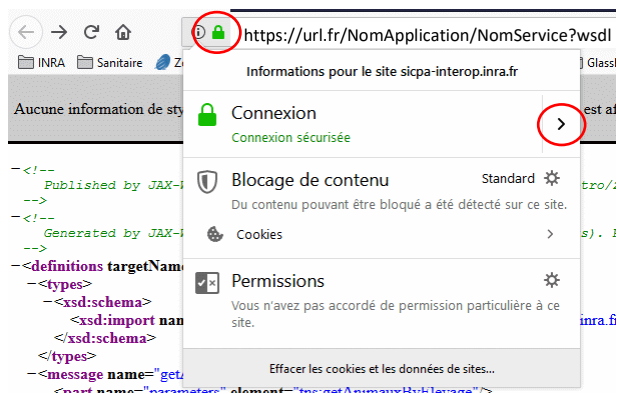
L'appel du WS depuis le programme java, génère l'erreur suivante :

```
javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building
failed: sun.security.provider.certpath.SunCertPathBuilderException:
unable to find valid certification path to requested target
```

Solution pour résoudre ce problème

Le certificat n'est pas reconnu comme valide. Il faut donc l'intégrer dans le magasin des certificats reconnus.

1. Dans un navigateur, renseigner l'adresse du wsdl du webservice.
2. Pour récupérer le certificat, cliquer sur le cadenas.



3. Puis, cliquer sur « Afficher le certificat »
4. Dans les « Détails » cliquer sur « Exporter »
5. Enregistrer le certificat au format *.crt ou *.cer
6. Ensuite, il faut importer le certificat dans le keystore de la JVM du serveur web (ici Glassfish)

- a. Pour cela, repérer l'endroit où se trouve le store utilisé par Glassfish en ouvrant le fichier domain.xml (... \glassfish4\glassfish\domains\domain1\config\domain.xml)

```
<java-config classpath-suffix="" debug-options="-agentlib:jdwp=transport=dt_socket,server=y,suspend=n,address=9009" system-classpath="">
<jvm-options>-XX:MaxPermSize=192m</jvm-options>
<jvm-options>-client</jvm-options>
<jvm-options>-Djava.awt.headless=true</jvm-options>
<jvm-options>-Djdk.corba.allowOutputStreamSubclass=true</jvm-options>
<jvm-options>-Djavax.xml.accessExternalSchema=all</jvm-options>
<jvm-options>-Djavax.management.builder.initial=com.sun.enterprise.v3.admin.AppServerMBeanServerBuilder</jvm-options>
<jvm-options>-XX:+UnlockDiagnosticVMOptions</jvm-options>
<jvm-options>-Djava.endorsed.dirs=${com.sun.aas.installRoot}/modules/endorsed${path.separator}${com.sun.aas.installRoot}/lib/endorsed</jvm-options>
<jvm-options>-Djava.security.policy=${com.sun.aas.installRoot}/config/server.policy</jvm-options>
<jvm-options>-Djava.security.auth.login.config=${com.sun.aas.installRoot}/config/login.conf</jvm-options>
<jvm-options>-Dcom.sun.enterprise.security.httpsOutboundKeyAlias=slas</jvm-options>
<jvm-options>-Xmx512m</jvm-options>
<jvm-options>-Djavax.net.ssl.keyStore=${com.sun.aas.installRoot}/config/keystore.jks</jvm-options>
<jvm-options>-Djavax.net.ssl.trustStore=${com.sun.aas.installRoot}/config/cacerts.jks</jvm-options>
<jvm-options>
Djava.ext.dirs=${com.sun.aas.javaRoot}/lib/ext${path.separator}${com.sun.aas.javaRoot}/jre/lib/ext${path.separator}${com.sun.aas.installRoot}/lib/ext</jvm-options>
<jvm-options>-Djdbc.drivers=org.apache.derby.jdbc.ClientDriver</jvm-options>
<jvm-options>-DANTLR_USE_DIRECT_CLASS_LOADING=true</jvm-options>
<jvm-options>-Dcom.sun.enterprise.config.config_environment_factory_class=com.sun.enterprise.config.serverbeans.AppserverConfigEnvironmentFactory</jvm-options>
<jvm-options>-
Dorg.glassfish.additionalOSGiBundlesToStart=org.apache.felix.shell,org.apache.felix.gogo.runtime,org.apache.felix.gogo.shell,org.apache.felix.gogo.command,org.apache.felix.gogo.runtime,org.apache.felix.gogo.plugin</jvm-options>
<jvm-options>-Dorg.apache.felix.fileinstall</jvm-options>
<jvm-options>-Dosgi.shell.telnet.port=6666</jvm-options>
<jvm-options>-Dosgi.shell.telnet.maxconn=1</jvm-options>
<jvm-options>-Dosgi.shell.telnet.ip=127.0.0.1</jvm-options>
<jvm-options>-Dgosh.args=-noInteractive</jvm-options>
<jvm-options>-Dfelix.fileinstall.dir=${com.sun.aas.installRoot}/modules/autostart</jvm-options>
<jvm-options>-Dfelix.fileinstall.poll=5000</jvm-options>
<jvm-options>-Dfelix.fileinstall.log.level=2</jvm-options>
<jvm-options>-Dfelix.fileinstall.bundles.new.start=true</jvm-options>
<jvm-options>-Dfelix.fileinstall.bundles.startTransient=true</jvm-options>
<jvm-options>-Dfelix.fileinstall.disableConfigSave=false</jvm-options>
<jvm-options>-XX:NewRatio=2</jvm-options>
<jvm-options>-Dcom.ctc.wstx.returnNullForDefaultNamespace=true</jvm-options>
</java-config>
```

- b. Sur une console taper la commande ci-dessous :

```
keytool -import -J-Duser.language=en -alias aliasDuCertificat -file fichier.crt -keystore cacerts.jks
```

-J-Duser.language=en : Ceci est nécessaire uniquement en java8.

-alias aliasDuCertificat : Mettre un alias. Ce nom est nécessaire si on veut ensuite le supprimer

-file fichier.crt : Chemin et nom du fichier .crt enregistré dans l'étape 5.

-keystore cacerts.jks : Chemin et nom du store repérer en 6.a

La console va alors vous demande le mot de passe du store. Normalement, ce mot de passe est : changeit

Mes sources :

<https://stackoverflow.com/questions/6908948/java-sun-security-provider-certpath-suncertpathbuilderexception-unable-to-find>

http://magicmonster.com/kb/prg/java/ssl/pkix_path_building_failed.html

<https://docs.oracle.com/cd/E19226-01/821-0027/gevgn/index.html>

<https://stackoverflow.com/questions/45820060/installing-a-certificate-in-glassfish-v4-without-storing-password-in-config-file>

<https://www.ssls.com/knowledgebase/how-to-install-an-ssl-certificate-on-glassfish/>