Configure Negoserver

==========

Install the .net framework v2.0 Redistribuable at least. The c# code use the class NegotiateStream.

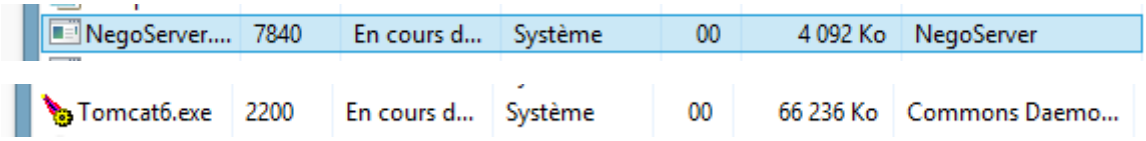
- ⇨ I've donwloaded http://www.microsoft.com/fr-fr/download/confirmation.aspx?id=6523

Copy the directory negoserver

Install the service with install.bat. For instance type "install.bat negoserver".

- ⇨ Done !

If Tomcat is running on Windows, the service NegoServer must be running on the same computer and NegoServer must be running with the account SYSTEM or Network Service.



You can configure in the file Negoserver.exe.conf

1) To log: You change the value of SourceSwitch

2) You can change the port. By default 21000

3) You can define an IP . By default it is Any Address

3) You can use only Kerberos(and not NTLM). But before to do that, test.

4) You can change the number of the threads in the pool. By default 4 (So 4 worker threads and 4 completion port threads)

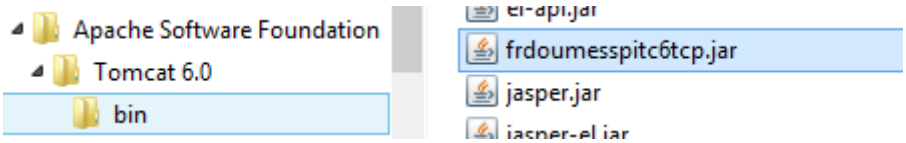
5) You van use SSL. An example will be given in a futur release

- ⇨ I didn't change anythning in Negoserver.exe.con !

Configure Tomcat 6

==========

1. Copy in the directory /lib of tomcat the file jar/tomcat6/frdoumesspitc6tcp.jar



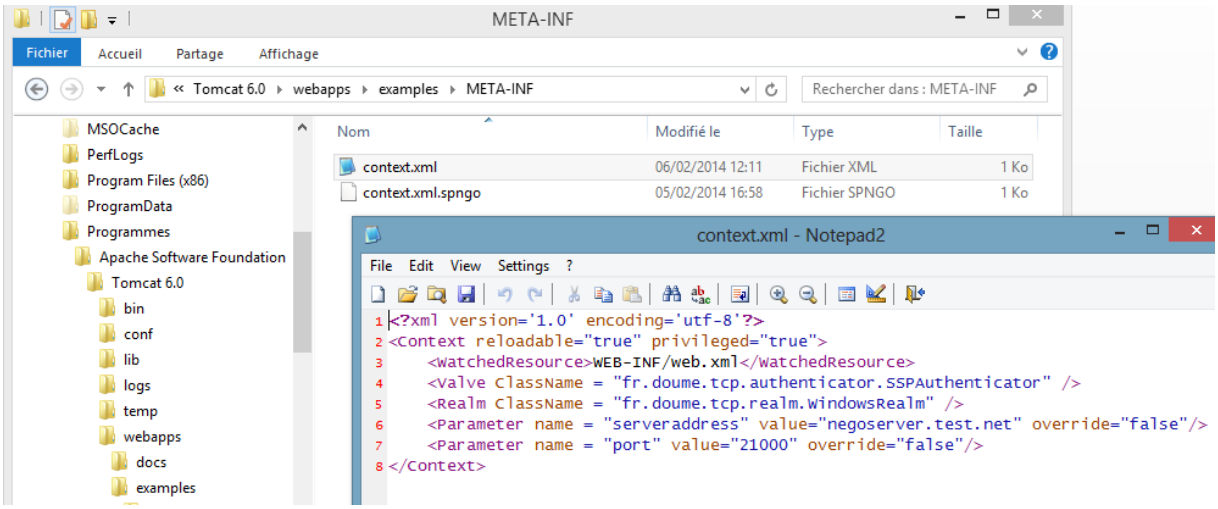
2. webapps/<application>/META-INF/context.xml file must contain:

<Valve ClassName="fr.doume.tcp.authenticator.SSPAuthenticator" />

<Realm ClassName ="fr.doume.tcp.realm.WindowsRealm" />

<Parameter name="serveraddress" value="negoserver.test.net" override="false"/>

<Parameter name="port" value="21000" override="false"/>



Configure web.xml

Web.xml must contain information on the protected area of the application. For example:

```
<security-constraint>
 <display-name>Managers Security Constraint</display-name>
 <web-resource-collection>
   <web-resource-name>Protected Area Utilisateurs</web-resource-name>
   <url-pattern>/gestion/*</url-pattern>
 </web-resource-collection>
 <auth-constraint>
   <role-name>DOMAINNAME\Managers</role-name>
   <role-name>DOMAINNAME\pipo</role-name>
 </auth-constraint>
</security-constraint>
<login-config>
 <auth-method>BASIC</auth-method>
 <realm-name>Example Windows Authentication Area</realm-name>
```

```
</login-config>
<security-role>
  <role-name>users</role-name>
</security-role>
<security-role>
  <role-name>tomcat</role-name>
</security-role>
<security-role>
  <role-name>DOMAINNAME\Domain users</role-name>
</security-role>
<security-role>
  <role-name>DOMAINNAME\Managers</role-name>
</security-role>
<security-role>
  <role-name>DOMAINNAME\Directors</role-name>
</security-role>
<security-role>
  <role-name>DOMAINNAME\pipo</role-name>
</security-role>
```

Comment: You can use the example of Tomcat 6 (examples/jsp/security/protected/index.jsp)

You should modify the tags auth-constraint and security-role in the file web.xml

⇨ See my web.xml

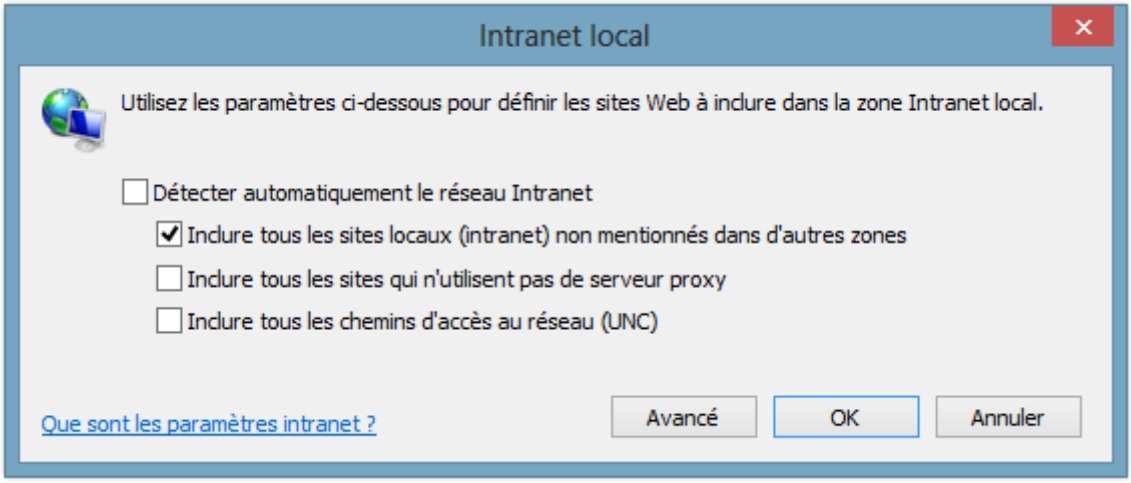
Configure IE:

==========

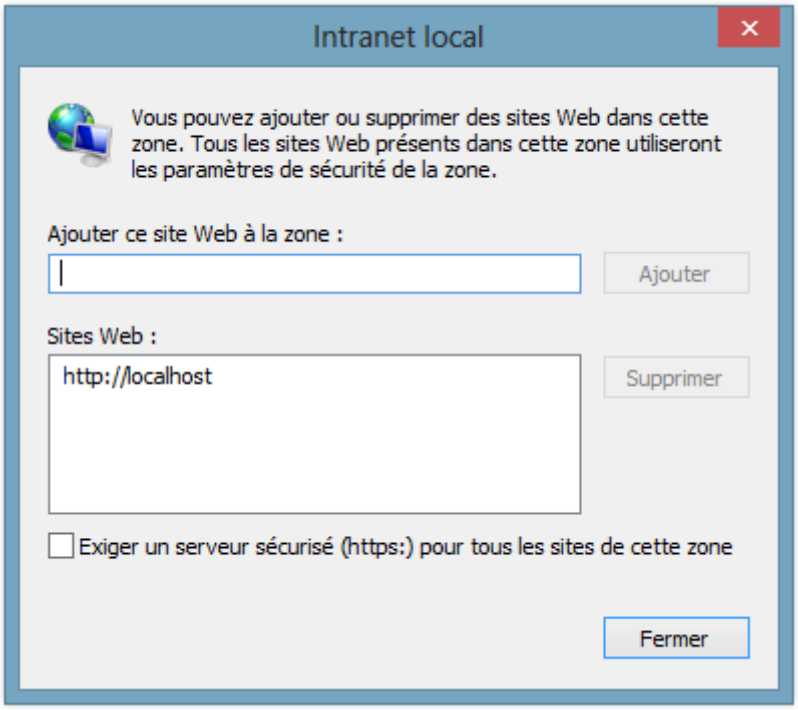
In the Internet Explorer window, click Tools > Internet Options > Security tab.

Select the Local intranet icon and click ***Sites***.

In the Local intranet window, ensure that the check box to ***include all local (intranet) not listed in other zones*** is selected, then click ***Advanced***.



In the Local intranet window, fill in the ***Add this Web*** site to the zone field with the Web address of the host name so that the single sign-on (SSO) can be enabled to the list Web sites shown in the Web sites field.



Your site information technology staff provides this information.

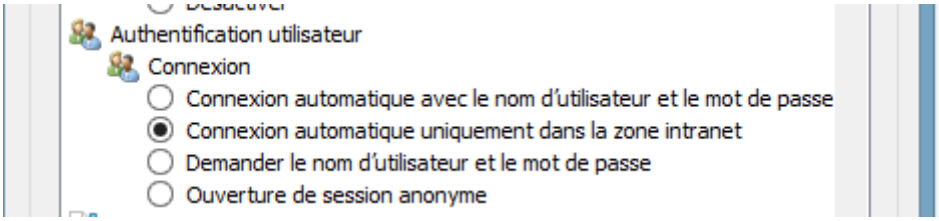
⇨ What does that mean ?

Click ***OK*** to complete this step and close the Local intranet window.

On the Internet Options window, click the ***Advanced*** tab and scroll to Security settings.

IE Menu Tools/Internet Options, Tab Security. Button Advanced…

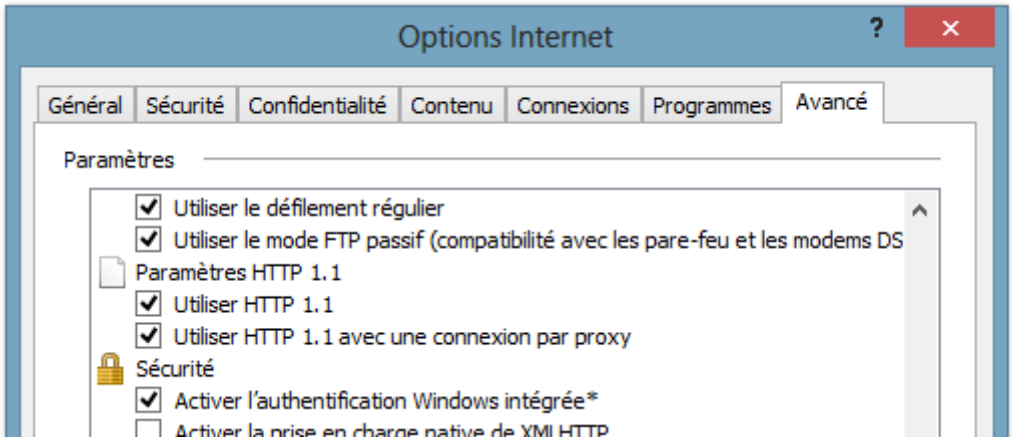
User authentication:/logon/Automatic logon only on intranet zone



⇨ OK

IE Menu Tools/Internet Options, Tab Advanced

Enable Integrated Windows Authentication



Click ***OK***.

Do not forget : You must populate the list of web sites that are in your organization's intranet

⇨ Useless for testing purpose, no ?

==========

If you have an forest Active Directory mycompany.intra, and others domains like domaina.mycompany.intra and domainb.mycompany.intra, you can add *.mycompany.intra to this list.

To add go to IE/ menu Tools/Internet Options, Tab Security,

Button sites

Advanced

Add this web site

⇨ Useless for testing purpose, no ?

If you have unix servers, you often use an Bind DNS. Your Windows servers can also be in this Bind DNS. If the domain is mycompany.net,

you add to the list *.mycompany.net

If you use the addresses 10.*.*.* in your organization, you also add 10.*.*.* to the list.

Compilation of the source Java

==========

I used the JDK 5. So it can be used with the JDK 5 or 6.

Comment:

The Java classes used to log with Tomcat 5.5 are present in common/lib/commons-logging-api.jar,

but are not included for Tomcat6.

So, for Tomcat 6, you have two solutions:

- Either, in the source of the Java's files,

  you comment the two lines

  import org.apache.commons.logging.Log;

  import org.apache.commons.logging.LogFactory;

  you decomment the two lines

  import org.apache.juli.logging.Log;

  import org.apache.juli.logging.LogFactory;

  and you recompile the sources. The result is the

  file frinseespsttc6.jar

- Either you add commons-logging-api.jar in the directory

  /lib of Tomcat 6,after having downloaded this file

  from htp://commons.apache.org.

  In this case, you use the jar file frdoumesspitc5.jar

I used the JDK 6 for tomcat 7. The classes GenericPrincipal and AuthenticatorBase are not the same in tomcat 6 and tomcat 7. So the java code is not the same.

Example

==========

You have an example in the directory example

The Tomcat's account:

==========

Tomcat must be running as a service with the account SYSTEM or better Network Service

To install tomcat as a service, download tomcat from htpp://tomcat.apache.org

Tomcat 55: goto core and download the zip

tomcat 6 and tomcat 7: download 32 bits or 64 bits download zip

Add a file setenv.bat in the directory /bin of tomcat

Oen this file and add:

set JAVA_HOME=...

set PAT=%JAVA_HOME%\bin;%PATH%

save the file.

open cmd.exe

CD <directory /bin od tomcat>

setenv.bat

service -install nameofyourservice

You can change the account used with tomcat. It is SYSTEM by default. You can use Network Service, but you must give the rights on the directory of tomcat to this account.

net start nameofyourservice

rename tomcat6w.exe into nameofyourservice.exe. So, you can change the configuration of the tomcat service.

Remarks : You can Define groups in an Realm:

==========

You can use another realm to search the tomcat roles.

To do that, comment the WindowsRealm in the context.xml and dd another Realm. Uncomment the Parameter nogroupsinad

With SPNEGO, the server does not know the password of the user. So SSPAuthenticator sends the user name as password to the Realm.

When you use JNDIRealm, you do not use the bind mode but the comparison mode

You can define the parameter userPassword, so there is no bind but only a search and compare in the ldap directory.cf doc tomcat

With JDBCRealm, you can map the name and the password to the same column:

(userNameCol="user_name" userCredCol="user_name") cf doc tomcat

With the UserDatabaseRealm, you define the same value to the name and password in the file conf/tomcat-users.xml. cf doc tomcat

You can also use the parameter usernamewithoutdomainasprefix

==========