Table of contents

1.Introduction

Using SPNEGO protocol to allow web applications to authenticate users with their windows login id needs a bit of configuration on the Active Directory domain controller to be used.

2.Identifying your Application Server in Active Directory

You need to create a user in Active Directory to represent your Application Server. The name chosen does not matter. However, two restrictions applies :

- the user password must never expire
- the user must not need to change its password at next login

3.Configuring DNS

To allow SPNEGO to function properly, you must configure your DNS server to name the host on which resides the Application Server. The reverse DNS must be configured too. Usually, you will name the host using the domain name, for example if your host is named myappserver, and you are in the domain MY.DOMAIN.COM, you will name it myappserver.my.domain.com.

Be aware that this is this name that clients will have to use, and no other name in order to allow SPNEGO protocol to function. This is a restriction on how web browsers implements SPNEGO. When a web server requires SPNEGO authentication, the web browser constructs a service name which it sends to the domain controller to verify the authenticity of the web server. This name looks like *HTTP/host_name*. In our sample, this name will be *HTTP/myappserver.my.domain.com*.

4.Mapping your Application Server ID in Kerberos

The service principal name (SPN) used in SPNEGO looks like *HTTP/hostname@realm*, where realm is the capitalized active directory domain name. The mapping between the service's user name and its SPN is done using the "**ktpass**" command. This utility is available in the *support tools* of windows 2003 or windows 2000 server.

```
> ktpass -princ SPN -pass password -mapuser user_name
```

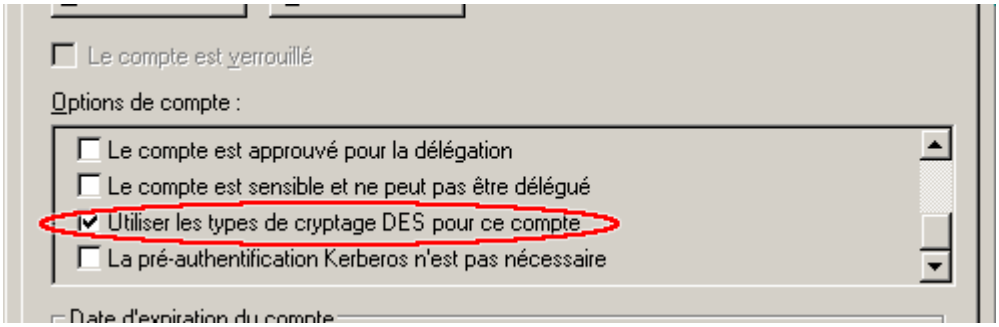
In our sample, the SPN will be *HTTP/myappserver.my.domain.com@MY.DOMAIN.COM*.

5. Application Server dependent configuration

The ktpass generates Kerberos password using a particular encryption. Support for encryption types vary between tomcat and Websphere.

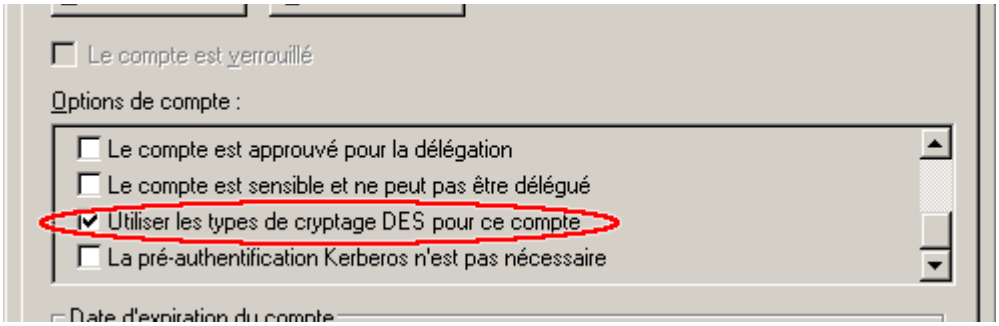
1. Tomcat settings

Under active directory users, open the "**Account configuration**" panel for the application server user. Select the "**Account**" tab and uncheck the entry "**Use DES encryption for this account**" under the section "**Account options**". Reset account password to ensure proper encryption by Kerberos.



2. Websphere settings

Under active directory users, open the "**Account configuration**" panel for the application server user. Select the "**Account**" tab and check the entry "**Use DES encryption for this account**" under the section "**Account options**". Reset account password to ensure proper encryption by Kerberos.



6. Client configuration

Web browsers must be configured to consider that the host on which the application server runs resides on the local intranet.

Under *Internet Explorer*, this is done by opening the "*Internet Options*" page, then selecting the "*Security*" tab. Select the "*Local intranet*" zone then click "*Sites...*". On the message box, click "*Advanced...*". From here you can add the address (either http://myserver.domain.com or https://myserver.domain.com) of the host. Restart *Internet Explorer* for the changes to take effect.

Under *Firefox*, this is done by opening the configuration window. Type *about:config* in the address bar. Then search for *network.negotiate-auth.trusted-uris* add the address of the host here. Restart *Firefox* for the changes to take effect.