Manual para autenticação no domínio em iFlow sobre Tomcat

Nota: este guia serve apenas ambiente Windows.

**Administração do Domínio**

1º Confirmar que a máquina servidor (onde reside o Tomcat) está no domínio.

2º Criar conta de utilizador de domínio que será usada para executar Tomcat

3º Obter o endereço do Key Distribution Service (KDC), o Tomcat irá conectar-se a este para processar a autenticação.

4º Registar Service Principal Names(SPN) para o utilizador criado em 3 de todos os alias de acesso ao site iFlow. Segue exemplo para instância de desenvolvimento, o <user> é o criado no passo 2:

setspn.exe -A HTTP/10.10.2.114 <user>

**Configuração do Tomcat**

5º Na raíz do Tomcat (ou local alcançável pela JVM) colocar os ficheiros de configuração krb5.conf e login.conf.

O ficheiro krb5.conf deve ser alterado com o DOMAIN e REALM correspondentes da seguinte forma:

*[libdefaults]*

*default\_realm = <REALM>*

*default\_tkt\_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc*

*default\_tgs\_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc*

*permitted\_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc*

*[realms]*

*<REALM> = {*

*kdc = <DOMAIN>*

*default\_domain = <REALM>*

*}*

*[domain\_realm]*

*.<REALM>= <REALM>*

O ficheiro login.conf não necessita de alterações adicionais.

6º Na pasta lib do Tomcat adicionar a biblioteca spnego-r9.jar.

**Configuração do iFlow**

7º Em <iflow.home>\config\iflow.properties adicionar/descomentar a propriedade AUTHENTICATION\_WINDOWS=true

8º Em <tomcat>\webapps\iFlow\WEB-INF\web.xml adicionar/descomentar as linhas, alterar onde indicado para o utilizador criado em 2º:

*<filter>*

*<filter-name>SpnegoHttpFilter</filter-name>*

*<filter-class>net.sourceforge.spnego.SpnegoHttpFilter</filter-class>*

*<init-param>*

*<param-name>spnego.allow.basic</param-name>*

*<param-value>true</param-value>*

*</init-param>*

*<init-param>*

*<param-name>spnego.allow.localhost</param-name>*

*<param-value>true</param-value>*

*</init-param>*

*<init-param>*

*<param-name>spnego.allow.unsecure.basic</param-name>*

*<param-value>true</param-value>*

*</init-param>*

*<init-param>*

*<param-name>spnego.login.client.module</param-name>*

*<param-value>spnego-client</param-value>*

*</init-param>*

*<init-param>*

*<param-name>spnego.krb5.conf</param-name>*

*<param-value>krb5.conf</param-value>*

*</init-param>*

*<init-param>*

*<param-name>spnego.login.conf</param-name>*

*<param-value>login.conf</param-value>*

*</init-param>*

*<init-param>*

*<param-name>spnego.preauth.username</param-name>*

*<param-value><USER></param-value>*

*</init-param>*

*<init-param>*

*<param-name>spnego.preauth.password</param-name>*

*<param-value><PASSWORD></param-value>*

*</init-param>*

*<init-param>*

*<param-name>spnego.login.server.module</param-name>*

*<param-value>spnego-server</param-value>*

*</init-param>*

*<init-param>*

*<param-name>spnego.prompt.ntlm</param-name>*

*<param-value>true</param-value>*

*</init-param>*

*<init-param>*

*<param-name>spnego.logger.level</param-name>*

*<param-value>1</param-value>*

*</init-param>*

*</filter>*

*<filter-mapping>*

*<filter-name>SpnegoHttpFilter</filter-name>*

*<url-pattern>\*</url-pattern>*

*</filter-mapping>*

9º Em <tomcat>\webapps\iFlow\WEB-INF\classes adicionar o patch fornecido

10º O processo está concluído pode-se reiniciar tomcat.