Kerberos SPNEGO

SPNEGO Authentication for kerberos

Permet de s'authentifier directement avec Chrome, Firefox et autres avec un ticket Kerberos créer par windows ou par MIT Kerberos.

https://apereo.github.io/cas/5.2.x/installation/SPNEGO-Authentication.html

$home/cas/build.gradle

```
repositories {
    ...
    maven { url "http://developer.jasig.org/repo/content/groups/m2-legacy" }
}

dependencies {
    ...
    compile "org.apereo.cas:cas-server-support-spnego-webflow:${project.'cas.version'}"
}
```

Remplacez $home par vos paramètres personnalisés dans ce qui suit:

$home/etc/cas/config/cas.properties

```
# SPNEGO / KERBEROS / KDC
cas.authn.spnego.kerberosConf=$home/etc/cas/config/krb5.conf
# Permet d'utiliser soit le mode login page et le SPNEGO soit seulement le SPNEGO, renvoi par consequent vers
une page blanche
cas.authn.spnego.mixedModeAuthentication=true
# Ce champs ne supporte pas les CNAME, il doit être paramétrer avec le domaine principale du server, pas d'alias
cas.authn.spnego.jcifsServicePrincipal=HTTP/your-cas.fr@UNIV-PARIS.FR
cas.authn.spnego.ntlmAllowed=false
cas.authn.spnego.hostNamePatternString=.+
cas.authn.spnego.ipsToCheckPattern=.*
cas.authn.spnego.kerberosRealm=UNIV-PARIS.FR
cas.authn.spnego.principalWithDomainName=false
```

Remplacez $home par vos paramètres personnalisés dans ce qui suit:

$home/etc/cas/config/krb5.conf

```
[logging]
 default = FILE:/$home/log/krb5libs.log
 admin_server = FILE:/$home/log/kadmind.log

[libdefaults]
 ticket_lifetime = 24000
 default_realm = UNIV-PARIS.FR
 default_keytab_name = FILE:/$home/etc/cas/config/cas5.keytab
 dns_lookup_realm = true
 dns_lookup_kdc = true
```

Le fichier cas5.keytab doit avoir été paramétré préalablement avec les domaines enregistrés dans notre cas HTTP/your-cas.fr@UNIV-PARIS.FR

Paramètrage du client

Vous devez ensuite configurer votre navigateur

- Pour **Google Chrome**, créer le fichier `/etc/opt/chrome/policies/recommended/krb5.json` : **{ "AuthServerWhitelist": "*univ-paris.fr" }**
- Pour **Firefox**, entrer about:config et modifier **network.negotiate-auth.trusted-uris** : **"univ-paris.fr"**

Attention: Remplacer "univ-paris.fr" par votre nom de domaine kerberos

DEBUG

Vous pouvez débugger grâce au navigateur dans l'onglet Réseau, en sélectionnant l'options “Données persistante”. Vous verrez ainsi l'affiche d'une requête “401 Non-Autorisé”, si tout se passe bien, suivi d'une requête 302 Déplacé Temporairement