Passage de l'authentification Kerberos aux applications web (mod_auth_kerb) (archive)

Nous montrons dans cette partie comment configurer le couple Apache/mod_auth_kerb pour faire passer le SSO de l'authentification système jusqu'aux applications web.

Les tests sont fait sur la machine **cas.ifsic.univ-rennes1.fr**, sur laquelle on installe Apache et mod_auth_kerb. Cette partie ne sert pas pour les applications CASifiées, mais elle peut être envisagée pour des application dont on ne dispose pas des sources et qui seraient capable de s'appuyer sur une authentification externe de type **REMOTE_USER**.

Authentification

Il n'est pas nécessaire de configurer l'authentification des utilisateurs avec **system-config-authentication** sur ce serveur (les utilisateurs n'ont pas à se connecter sur le serveur CAS). Il faut néanmoins installer le fichier **/etc/krb5.conf** :

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = UNIV-RENNES1.FR
 default_etypes = des3-hmac-sha1 des-cbc-crc
 default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc
 default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc
 permitted_enctypes = des3-hmac-sha1 des-cbc-crc rc4-hmac
 ticket_lifetime = 24h
 forwardable = yes

[realms]
 UNIV-RENNES1.FR = {
  kdc = kerb.ifsic.univ-rennes1.fr:88
  admin_server = kerb.ifsic.univ-rennes1.fr:749
  default_domain = univ-rennes1.fr
 }

[domain_realm]
 .univ-rennes1.fr = UNIV-RENNES1.FR
 univ-rennes1.fr = UNIV-RENNES1.FR

[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
 }
```

Installation basique Apache

Installer httpd (Apache) et mod_auth_kerb et démarrer Apache :

```
[root@cas ~]# chkconfig httpd on
[root@cas ~]# service httpd start
Starting httpd:                            [OK]
[root@cas ~]#
```

Création d'un script de test

Ecrire un simple script **test.php** dans le répertoire **/var/www/html/kerb** :

```
<?php
echo "<p>REMOTE_USER=[".$_SERVER['REMOTE_USER']."]</p>";
echo "<p>PHP_AUTH_USER=[".$_SERVER['PHP_AUTH_USER']."]</p>";
phpinfo();
?>
```

Debuggage

Modifier la directive **LogLevel** du fichier **/etc/httpd/conf/httpd.conf** :

```
LogLevel debug
```

Les logs sont dans le répertoire **/var/log/httpd**.

Test

Tester en accédant à http://cas.ifsic.univ-rennes1.fr/kerb/test.php .

Installation mod_auth_kerb

Configuration Kerberos

Déclarer le client Kerberos :

```
[root@cas ~]# kadmin
Authenticating as principal root/admin@UNIV-RENNES1.FR with password.
Password for root/admin@UNIV-RENNES1.FR:
kadmin:  addprinc -randkey HTTP/cas.ifsic.univ-rennes1.fr
WARNING: no policy specified for HTTP/cas.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR; defaulting to no policy
Principal "HTTP/cas.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR" created.
kadmin:  exit
[root@cas ~]#
```

Configuration mod_auth_kerb

Exporter la clé du client dans le fichier le fichier **/etc/httpd/conf/mod_auth_kerb.keytab** (ce fichier sera utilisé par mod_auth_kerb) :

```
[root@cas ~]# kadmin
Authenticating as principal root/admin@UNIV-RENNES1.FR with password.
Password for root/admin@UNIV-RENNES1.FR:
kadmin:  ktadd -k /etc/httpd/conf/mod_auth_kerb.keytab HTTP/cas.ifsic.univ-rennes1.fr
Entry for principal HTTP/cas.ifsic.univ-rennes1.fr with kvno 3, encryption type AES-256 CTS mode with 96-bit
SHA-1 HMAC added to keytab WRFILE:/etc/httpd/conf/mod_auth_kerb.keytab.
Entry for principal HTTP/cas.ifsic.univ-rennes1.fr with kvno 3, encryption type AES-128 CTS mode with 96-bit
SHA-1 HMAC added to keytab WRFILE:/etc/httpd/conf/mod_auth_kerb.keytab.
Entry for principal HTTP/cas.ifsic.univ-rennes1.fr with kvno 3, encryption type Triple DES cbc mode with HMAC
/sha1 added to keytab WRFILE:/etc/httpd/conf/mod_auth_kerb.keytab.
Entry for principal HTTP/cas.ifsic.univ-rennes1.fr with kvno 3, encryption type ArcFour with HMAC/md5 added to
keytab WRFILE:/etc/httpd/conf/mod_auth_kerb.keytab.
Entry for principal HTTP/cas.ifsic.univ-rennes1.fr with kvno 3, encryption type DES with HMAC/sha1 added to
keytab WRFILE:/etc/httpd/conf/mod_auth_kerb.keytab.
Entry for principal HTTP/cas.ifsic.univ-rennes1.fr with kvno 3, encryption type DES cbc mode with RSA-MD5 added
to keytab WRFILE:/etc/httpd/conf/mod_auth_kerb.keytab.
kadmin:  exit
[root@cas ~]#
```

Modifier les permissions de la clé :

```
[root@cas ~]# chown apache /etc/httpd/conf/mod_auth_kerb.keytab
[root@cas ~]# chmod 640 /etc/httpd/conf/mod_auth_kerb.keytab
[root@cas ~]#
```

Protéger un répertoire par Kerberos en éditant **/etc/httpd/conf.d/auth_kerb.conf** :

```
<Location /kerb>
  #SSLRequireSSL
  AuthType KerberosV5
  AuthName "Kerberos Login"
  KrbMethodNegotiate On
  KrbMethodK5Passwd Off
  KrbAuthRealms UNIV-RENNES1.FR
  Krb5KeyTab /etc/httpd/conf/mod_auth_kerb.keytab
  require valid-user
</Location>
```

Test

Avant de tester, ne pas oublier d'ouvrir le port 80 entrant (**system-config-firewall**).

Tester en accédant http://cas.ifsic.univ-rennes1.fr/kerb/test.php. Le nom de l'utilisateur doit apparaître dans les variables **$_SERVER["REMOTE_USER"]** et **$_SERVER["PHP_AUTH_USER"]** (quelque chose comme **paubry@IFSIC.UNIV-RENNES1.FR**).

Note : il faut configurer les navigateurs clients pour que l'authentification kerberos soit transmise au serveur web.

- Configuration de Firefox (archive)
- Configuration de Internet Explorer (archive)

Il est possible de supprimer le domaine Kerberos de l'identifiant renvoyé par mod_auth_kerb en ajoutant l'option suivante à **mod_auth_kerb** :

```
KrbLocalUserMapping On
```