# Utilisation d'un volume CIFS dans Linux avec kerberos

Ce document s'applique à un serveur Red Hat Enterprise Linux 7.

Le but est de permettre à un serveur Linux et Samba, d'accéder à un partage de fichier de type CIFS distant par une connexion sécurisée, en utilisant une authentification par kerberos et le protocole SMB2 ou supérieure.

Pour cela le serveur Linux doit être joint même domaine Active Directory que le serveur de fichiers (Windows, Linux ou Baie NAS).

## *Prérequis*

Il est recommander de de disposer d'un serveur Linux à jours.

> Si des versions inferieurs Samba peuvent fonctionner, la version recommandé est la 4.6.2 au minimum.
> **Les versions précédents sont exposées à plusieurs failles de sécurité.**

Dans le reste du document les variables suivantes seront utilisées.

| Variable | Description |
|---|---|
| AD_DOMAIN | Nom court du domaine Active directory. |
| AD_REALM | Nom du royaume Kerberos de domaine Active directory en majuscule. |
| AD_FQDN_DOMAIN | Nom FQDN du domaine Active directory. |
| AD_ADMIN | Compte AD disposant des droits pour joindre une machine à l'AD. |
| AD_USER | Compte utilisateur dand l'AD. |
| AD_HOST | Nom fqdn d'un serveur Active directory du domaine. |
| SAMBA_HOST | Nom fqdn du serveur Linux Samba. |
| FILER_HOST | Nom fqdn du serveur de fichiers. |
| SHARE | Partage sur le FILER_HOST. |
| MNT_POINT | Point de montage sur SAMBA_HOST. |
| SMB_PROTO | Version du protocole SMB à utiliser lors du montage. |

## Packages nécessaires

Installer les packages suivants :

```
# yum install winbind samba
# yum install samba-winbind samba-winbind samba-winbind-clients samba-
winbind-modules
# yum install samba-client
# yum install keyutils cifs-utils autofs
# yum install krb5-workstation
# yum install ntpdate
```

## Vérification NTP

L'utilisation d'un serveur NTP est recommandé sur l'ensemble des serveurs.

Vérifier qu'il n'y a pas plus de **5 minutes** (offset) entre le serveur Samba et l'Active Directory.

> Ne pas faire pointer les serveurs NTP d'un linux vers un serveur AD Windows. Windows n'implémente pas le protocle NTP mais une version simplifiée SNTP, non compatible avec Linux.
> Pour une mise à jour ponctuelle, arrêter le service NTP et utiliser la commande **ntpdate**

```
# ntpdate -q AD_HOST
server XXX.XXX.XXX.XXX, stratum 1, offset 0.000241, delay 0.04170
23 Oct 15:33:14 ntpdate[2201]: adjust time server XXX.XXX.XXX.XXXX
offset 0.000241 sec
```

## Vérification DNS

Vérifier que les adresses suivantes sont déclarées dans les DNS utilisés. Ces valeurs sont normalement présentes par défaut dans les DNS des Active Directory.

Les adresses sont de type **SRV** et non A ou CNAME

```
# nslookup <AD_HOST>
# nslookup <SAMBA_HOST>
# nslookup <FILER_HOST>
# nslookup -q=SRV _kerberos._tcp.<AD_FQDN_DOMAIN>
# nslookup -q=SRV _ldap._tcp.<AD_FQDN_DOMAIN>
```

> En cas d'erreur vérifier les adresses IP des serveurs DNS dans /etc/resolv.conf.
> Faire déclarer les adresses manquantes dans les DNS.
> Vérifier la résolution inverse des adresses IP vers les fqdn

## Vérification du service kerberos

Ce chapitre permet de tester le bon fonctionnement de kerberos.

Si kerberos ne fonctionne pas, samba et winbind risque de disfonctionner.

### *Utilisation des DNS pour kerberos*

Configurer kerberos pour utiliser la résolution DNS. Dans le fichier /etc/krb5.conf, dans la section **libdefaults**, vérifier que dns_lookup_realm et default_realm sont configurés comme suit:

```
.../...
[libdefaults]
.../...
 dns_lookup_realm = true
```

```
 default_realm = <AD_REALM>
../...
```

- Obtenir un ticket du serveur kerberos :

```
kinit <USER>@<AD_REALM>
```

- Afficher le ticket obtenu

```
klist
```

- Supprimer le ticket obtenu

```
kdestroy
```

### *Configurer l'authentification par Winbind*

Activer l'authentification par winbind sur le système :

```
authconfig --enablewinbindauth  --enablemkhomedir --update
```

## Fichier nsswitch

Vérifier que le fichier /etc/nsswitch.conf prend winbind en compte.

```
# vi /etc/nsswitch.conf
.../...
passwd:     files winbind
shadow:     files winbind
group:      files winbind
.../...
```

## Configuration Samba

> Les lignes idmap config AD_DOMAIN ... sont très importantes. Elles définissent le backend (méthode d'accès) AD (Active Directory), et la plage des identifiants numériques pour les utilisateurs et groupes du domaine AD_DOMAIN. Cette plage doit être définie dans la politique du domaine. Afin d'éviter des usurpations d'identité et de droits, il faut garantir que ces numéros soient uniques. Ils ne peuvent donc pas être utilisés localement (sur aucune machine du domaine).
>
> Samba utiliser le backend **rid**. Ce backend se base sur le SID d'un utilisateur : S-1-5-XX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXX-RID, prend le RID et l'additionne au range défini.

Vérifier la configuration du serveur samba dans le fichier /etc/smb.conf.

Vérifier les variables workgroup, realm, id config sont bien renseignées.

```
# vi /etc/samba/smb.conf
[global]
   workgroup = <AD_DOMAIN>
   security = ads
   realm = <AD_REALM>
   kerberos method = secrets and keytab
   client NTLMv2 auth = Yes
   min protocol = SMB2
```

```
   winbind enum users = Yes
   winbind enum groups = Yes
   winbind use default domain = true
   winbind separator = +

   idmap config * : backend = rid
   idmap config * : range = 100000-19999999

   idmap config <AD_DOMAIN> : rangesize = 1000000
   idmap config <AD_DOMAIN> : backend = rid
   idmap config <AD_DOMAIN> : range = 30000000-39999999
   idmap config <AD_DOMAIN> : unix_nss_info = yes
   template shell = /bin/bash

   log level = 1

   .../...
```

## Joindre le domaine

Pour joindre le serveur samba au domaine AD_DOMAIN, il faut disposer d'un compte de domaine (AD_ADMIN) avec les droits suffisants pour intégrer un serveur.

```
# net ads join osName="Red Hat Enterprise Linux" -osVersion="7" --no-
dns-updates -U <AD_ADMIN>@<AD_REALM>
```

## Service Winbind

Démarrer le service winbind en tant que root :

```
# systemctl enable winbind
# systemctl start winbind
```

### *Tests de connections*

## Connexion Winbind

Vérifier le fonctionnement de Winbind.

- Les commandes suivantes listent les utilisateurs et les groupes Windows.

```
# wbinfo -u
# wbinfo -g
```

- Vérifier le mapping SID vers UID/GID.

```
# wbinfo -n <AD_USER>
S-1-5-21-2047507078-2512947033-3780000690-1106 SID_USER (1)
# wbinfo -S S-1-5-21-2047507078-2512947033-3780000690-110630001106
 30001106
# wbinfo -i <AD_USER>
<AD_USER>:*:30001106:30000513:AD USER:/home///bin/bash
# wbinfo -r <AD_USER>
30001106 30000513 30001107
# wbinfo -G 30001106
S-1-5-21-2047507078-2512947033-3780000690-1106
```

- Vérifier le compte sous Linux et la liste des groupes qui lui sont associés.

```
# su - <DOMAIN_AD>\\<AD_USER>
$ id
uid=30001106(<AD_USER>) gid=30000513(utilisateurs du domaine)
groupes=30000513(utilisateurs du
domaine),30001106(<AD_USER>),30001107(it)
contexte=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

## *Montage d'un volume*

Version des protocoles SMB supportés en fonction des versions des OS.

> La version 1.0 du protocole est à éviter.
> La version 2.1 est la version minimale préconisée
> La version 3 est la version recommandée.

| OS | W8.1/WS2k 12R2 | W8.1/WS2k 12 | W7/WS2k8 R2 | WVista/WS 2k8 | WXP/W2k3 |
|---|---|---|---|---|---|
| **RHEL7.4/W8.1/WS2k12R2** | 3.02 | 3.0 | 2.1 | 2.0 | 1.0 |
| **W8.1/WS2k12** | 3.0 | 3.0 | 2.1 | 2.0 | 1.0 |
| **W7/WS2k8R2** | 2.1 | 2.1 | 2.1 | 2.0 | 1.0 |
| **WVista/WS2k8** | 2.0 | 2.0 | 2.0 | 2.0 | 1.0 |
| **WXP/W2k3** | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 |

Ajouter le point de montage dans /etc/fstab et choisir le protocole SMB à utiliser.

```
# vi /etc/fstab
.../...
//<FILER_HOST>/<SHARE> <MNT_POINT> cifs
sec=krb5,multiuser,file_mode=0660,dir_mode=0770,nounix,noserverino,vers=
<SMB_PROTO> 0 0
.../...
```

Pour éviter de saisir le mot de passe kerberos, on utilise un fichier keytab.

```
# ktutil
ktutil:  addent -password -p <AD_USER>@<AD_REALM> -k 1 -e aes256-cts
Password for <AD_USER>@<AD_REALM>:
ktutil:  wkt <AD_USER>.keytab
ktutil:  quit
```

Obtenir le ticket kerberos pour le user AD_USER :

```
# kinit <AD_USER>@<AD_REALM> -k -t <AD_USER>.keytab
```

Vérifier le ticket obtenu :

```
# klist
```

Monter le volume :

```
# mount <MNT_POINT>
```

> Il est possible de vérifier le protocole SMB utilisé entre le client Linux et le poste windows par la commande :
> **Get-SmbSession | Select-Object -Property Dialect**