SAMBA : Partage de fichiers pour Windows sous Linux

Contributeurs : (SISR2-2017) Patrice Cypre

Principes

SAMBA est une transposition sous Linux du protocole **SMB** assurant le partage de fichiers dans un environnement Windows. Il est aussi utilisé pour assurer les rôles de contrôleurs de domaine équivalent à AD, mais qui n'est pas l'objet de cette page.

Pour fonctionner, SAMBA nécessite :

- les services smbd et nmbd installés par ***apt install samba***
- des dossiers présents sur le disque de la machine Samba, auxquels des droits sont définis selon des utilisateurs Linux
- des utilisateurs Linux intégrés à Samba par ***smbpasswd***
- des partages définis dans les ***sections*** du fichier smb.cnf, auxquels sont associés des restrictions

Fonctionnement des droits

Lors d'un accès à un partage par le voisinage réseau Windows ou par l'accès smb:/ /, le serveur étudiera :

- les restrictions définies dans la section de partage : browseable, read_only, writeable, etc
- les permissions éventuelles définies dans la section : write_users, read_users, etc
- les permissions éventuelles appliquées directement sur le dossier Linux avec ***chown/chmod***

il appliquera les restrictions les plus strictes :

- pour l'utilisateur s'il a des permissions définies
- pour son groupe s'il y a des permissions associées
- pour l'ensemble des utilisateurs

Installation en serveur autonome

Installation

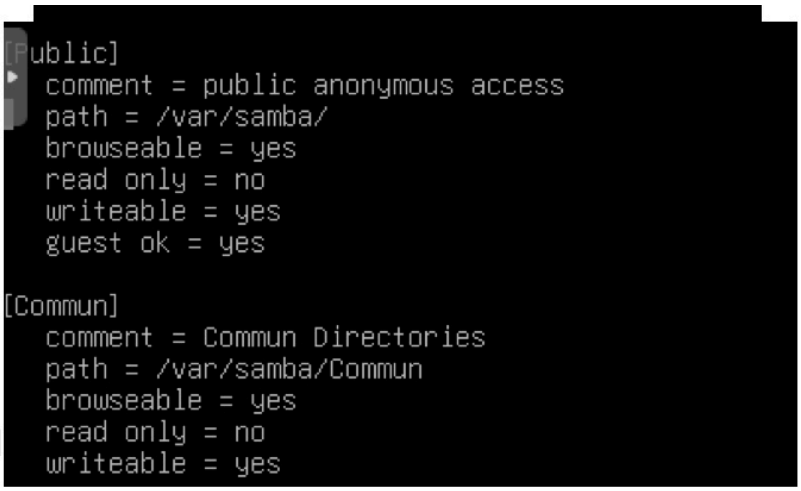
Installation des paquet et des dépendances :

```
apt-get install samba
```

Configuration du fichier smb.conf

Pour chaque élément que l'on veut rendre accessible par le réseau, on doit créer une ***[section]*** qui définira les accès.

Configuration du fichier /etc/samba/smb.conf



Les options à configurer sont les suivantes :

- ***[<nom_partage>]*** : définit le nom qui sera visible à travers le réseau
- ***path*** : chemin d'accès local au dossier à partager
- ***browseable*** : le partage est visible (*yes*) ou masqué (*no*)
- ***readonly*** : le partage est accessible en lecture seule (*yes*) ou pas (*no*)
- ***writeable*** : le partage est accessible en écriture (*yes*) ou pas (*no*)
- ***guest ok*** : le partage est accessible sans authentification (*yes*) ou pas (*no*)
- ***valid users*** : liste des utilisateurs et groupes autorisés pour l'accès (comptes et groupes Linux)
- ***write_users*** : liste des utilisateurs et groupes autorisés en écriture

Redémarrage du service

A chaque modification des fichiers de configuration, on redémarrera le service :

```
systemctl restart smbd
```

Gestion des utilisateurs

La gestion des utilisateurs passe par deux étapes :

- **Création des comptes pour Linux**

```
adduser <nomUtilisateur>
```

- **Création d'un utilisateur Samba** :

Le compte de l'utilisateur Linux doit être ajouté à Samba. Les mots de passe peuvent différer.

```
smbpasswd -a <nomUtilisateur>
```

Commandes Windows pour l'accès aux partages

Pour visualiser les partages d'une machine :

```
net view <adresse_serveur>
```

Monter un partage vers un dossier distant sur un lecteur local :

```
net use [<lettre_lecteur>:] \\<adresse_serveur>\nom_partage
[/user:<nom_utilisateur>]
```

Supprimer les connexions existantes :

```
net use \\<adresse_serveur>\nom_partage /delete
```

```
net use * /delete
```

Intégration de samba à Active Directory

1-Installer des services

Il faut installer le service ***ntp*** et paramétrer le serveur AD dans les DNS du serveur Samba.

```
apt-get install ntp
vi /etc/ntp.conf
```

Dans le fichier, on ajoute la ligne :

```
server <NomADServer>.<domaine>.<tld>
```

2 - Installer Kerberos

<Kerberos est le service d'authentification d'AD.

```
apt-get install krb5-user
```

On adaptera l fichier **// /etc/krb5.conf //** (attention à la casse) :

```
[libdefaults]
default_realm = <nomDomaine>
[realms]
```

```
<nomDomaine> = {
kdc = <serveurAD>.<nomDomaine>
admin_server =  <serveurAD>.<nomDomaine>
default_domain = <nomDomaine>
}
[domain_realm]
. <serveurAD>.<nomDomaine> = <serveurAD>.<nomDomaine>
[login]
krb4_convert = true
krb4_get_tickets = false
```

Pour créer le compte machine et faire partie de Active Directory de Windows Server 2012, Kerberos doit tout d'abord être initialisé comme serveur membre faisant partie du domaine AD Pour créer un ticket administratif pour Kerberos : (à vérifier)

```
[root@/home/tux] Administrateur@SIO-VOYAGES.FR
Password for Administrateur@SIO-VOYAGES.FR:
[root@/home/tux]
```

3- configuration de /etc/samba/smb.conf

```
[global]
workgroup =<nomDomaine> #Nom de Domaine
password server = <serveurAD><nomDomaine>
realm = <nomDomaine>
security = ADS
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind separator = /
template shell = /bin/bash
winbind use default domain = true
#on peut se passer de l'authentification \\domaine\login
winbind offline logon = false
netbios name = DEBIAN
preferred master = no
server string = Samba Server version %v
encrypt passwords = yes
log level = 3
log file = /var/log/samba/%m
max log size = 50
printcap name = cups
printing = cups
winbind enum users = Yes
#samba doit faire appel à Winbind pour gérer ses users
winbind enum groups = Yes
#samba doit faire appel à Winbind pour gérer ses groupes
template homedir = /home/%D/%U
```

4- Editer /etc/nsswitch

/etc/nsswitch permet d'indiquer comment et dans quel ordre la résolution des noms des machines va se faire

```
passwd: files winbind
shadow: files winbind
group: files winbind
```

5- les règles d'authentification PAM-Pluggable Authenfication Module

Accéder aux fichiers de configuration PAM qui sont stockés dans /etc/pam.d/

Mise a jour des règles d'authentification

```
 pam-auth-update

cat common-account
account [success=2 new_authtok_reqd=done default=ignore] pam_unix.so
account [success=1 new_authtok_reqd=done default=ignore] pam_winbind.so
account requisite pam_deny.so
account required pam_permit.so

cat common-auth
auth [success=2 default=ignore] pam_unix.so nullok_secure
auth [success=1 default=ignore] pam_winbind.so krb5_auth
krb5_ccache_type=FILE cached_login try_first_pass
auth requisite pam_deny.so
auth required pam_permit.so
auth optional pam_cap.so

cat common-password
password [success=2 default=ignore] pam_unix.so obscure sha512
password [success=1 default=ignore] pam_winbind.so use_authtok
try_first_pass
password requisite pam_deny.so
password required pam_permit.so
password optional pam_gnome_keyring.so

cat common-session
session [default=1] pam_permit.so
session requisite pam_deny.so
session required pam_permit.so
session required pam_unix.so
session optional pam_winbind.so
session optional pam_ck_connector.so nox11
session required pam_mkhomedir.so skel=/etc/skel

==== 6- Redémarrer les serveurs winbind et samba ====
```

```
==== 7- Intégration de la machine Linux au domaine AD ====

<code lscript>net join -U Administrateur
wbinfo -u #afin d'afficher les utilisateurs présent dans l'active directory
```

8- Home directory

La mise en place des lecteurs personnel à chaque utilisateur se fait grâce a la configuration suivante :

```
[homes]
        comment = Home Directories
        valid user =%S
        read only = No
        browseable = No
        directory mask = 0700
        create mask = 0700
```

From:
https://wiki.sio.bts/ - **WIKI SIO : DEPUIS 2017**

Permanent link:
https://wiki.sio.bts/doku.php?id=samba&rev=1677498849

Last update: **2023/02/27 11:54**