rôle active directory domain controller

Qui ne n'a jamais assisté à une discussion avec des pro Windows, vous racontent Linux c'est bien, mais 100% des entreprises ont au moins un serveur Windows et il parle de l'Active Directory de Windows.

Depuis décembre 2012 cela est fini, l'arrivée de samba 4 change tout, en effet, il est ainsi possible de joindre complètement des clients Windows à un domaine et effectuer des opérations d'ouverture de session.

Et la cerise sur le gâteau, pour ceux qui seraient habitués a manipulé cela avec les outils d'administration de serveur distant RSAT de Windows, c'est possible.

Vous l'aurez bien compris, je vais vous montrer comment fabriquer non pas un, mais 2 serveurs samba active directory domain controller, oui parce qu'un réseau avec un serveur DC cela ne n'existe pas, ou sinon c'est que vous avez préparé une petite place sous votre moquette de bureau, le jour ou cela tombe.
Donc je récapitule :

- un Serveur DC samba 4 master
- un Serveur DC samba 4 secondaire

Pour l'installation, regardé Installation d'un serveur SAMBA 4, car l'article est basé dessus.

Tout d'abord, il faut vérifier le fichier **/etc/hosts**, Si cela n'est pas déjà fait.

```
127.0.0.1       localhost
XXX.XXX.XXX.XXX    nom.domaine.loc nom
```

Ou

- nom.domaine.loc représente le nom de votre serveur sur le réseau.
- xxx.xxx.xxx.xxx représente son IP

Modifier le fichier `/etc/network/interfaces` pour lui donner une configuration IP static, Si cela n'est pas déjà fait.

```
allow-hotplug eth0
auto eth0
iface eth0 inet static
      address XXX.XXX.XXX.XXX
      netmask XXX.XXX.XXX.XXX
      gateway XXX.XXX.XXX.XXX
```

mettre la machine dans le future domaine avec comme DNS lui même Editer /etc/resolv.conf

```
domain domaine.loc
search domaine.loc
nameserver 127.0.0.1
```

Fichier kerberos client

```
rm /etc/krb5.conf
cp /usr/local/samba/share/setup/krb5.conf /etc/
vim /etc/krb5.conf
```

On ajoute ce qui suit :

```
[libdefaults]
      default_realm = DOMAINE.LOC
      dns_lookup_realm = false
      dns_lookup_kdc = true
```

Création du domaine

```
samba-tool domain provision --use-rfc2307 --interactive
```

Répondez aux questions, mais normalement vous avez renseigné tous vos fichiers.
Les plus importantes sont:

- `DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:`, bon pour le test, j'ai choisi `SAMBA_INTERNAL`, Je fais une rapide description des modes :
  - **SAMBA_INTERNAL** : Le serveur DNS interne est intégré dans Samba et utilise AD comme backend.
    Il est la solution DNS par défaut lors de l'approvisionnement d'un nouveau Samba AD DC.
  - **BIND9_DLZ** :BIND 9.8 et 9.9 peut être configuré pour fournir la résolution DNS pour gérées les zones.
    Ils sont accessible à partir de BIND à travers les DLZ (zones chargeables dynamiquement) plugin.
    Noter que le serveur BIND doit fonctionner sur la même machine que le Samba AD DC.
  - **BIND9_FLATFILE** : Ne pas utiliser BIND9_FLATFILE! Il n'est pas documenté ou soutenu.
  - **NONE** : pas de DNS
- `DNS forwarder IP address (write 'none' to disable forwarding)` : Une IP réseau utilisé pour transférer des requêtes DNS pour des noms DNS externes vers des serveurs DNS situés à l'extérieur de ce réseau.
  Pour le test j'ai mis 8.8.8.8.

Si, vous penser vous être trompé dans le questionnaire ce n'est pas grave, sauf pour le mot de passe `administrator`.

Pour effacer la configuration de Samba :

```
rm -f /usr/local/samba/etc/smb.conf
rm -rf /usr/local/samba/private/*
```

Sinon, votre fichier de configuration `smb.conf` a été créé dans `/usr/local/samba/etc` en l'éditant vous obtenez ce qui suit :

```
# Global parameters
[global]
      workgroup = DOMAINE
      realm = DOMAINE.LOC
      netbios name = NOM
      server role = active directory domain controller
      dns forwarder = 8.8.8.8 8.8.4.4 #j'ai ajouté un DNS secondaire de
google ^^
      idmap_ldb:use rfc2307 = yes

[netlogon]
      path = /usr/local/samba/var/locks/sysvol/mondomaine.loc/scripts
      read only = No

[sysvol]
      path = /usr/local/samba/var/locks/sysvol
      read only = No
```

Votre DC est prêt a fonctionné vous pouvez donc lancer le service

```
/etc/init.d/samba start
```

Création d'un serveur secondaire

Pour la suite, les étapes sont presque similaires, je vais donner ce qui change.
Fichier kerberos :

```
[libdefaults]
      default_realm = DOMAINE.LOC
      dns_lookup_realm = true
      dns_lookup_kdc = true
```

Commande samba pour joindre le domaine :

```
samba-tool domain join domaine.loc DC -U administrator
```

Pour activer le DNS sur le serveur secondaire, `dns forwarder = 8.8.8.8 8.8.4.4` dans le fichier `smb.conf`

Administration

Donc, il y a les outils d'administration de serveur distant RSAT de Windows.
Sinon, sous Linux la commande `samba-tool` sert pour tout.
exemple :

- enlevé la complexité du mot de passe :
  `samba-tool password settings set –complexity=off –min-pwd-lengt=0`

`–store-plaintext=off`

- ajouter un enregistrement A (Adresse) dans le DNS backend :`samba-tool dns add <IP OU NOM DU CONTRÔLEUR DE DOMAIN> <domaine.loc> <nom> A XXX.XXX.XXX.XXX`
- ajouter un enregistrement PTR (pointer) dans le DNS backend :`samba-tool dns add <IP OU NOM DU CONTRÔLEUR DE DOMAIN> X.X.X.in-addr.arpa XX PTR <nom.domaine.loc>`
- ajouter un login : `samba-tool user add <USERNAME>`

Je vous renvoi vers samba.org pour plus d'information sur la commande

installation d'un service NTP

Moi, j'aime bien mettre en place un petit service ntp sur les serveurs DCs, car ils peuvent servir de serveur de temps pour les autres machines et c'est logique. Installation de `ntp`:

```
aptitude install ntp ntpdate
```

Nous allons éditer la configuration de `ntp` qui est dans le fichier `ntp.conf`

```
 vim /etc/ntp.conf
```

Ajouter la ligne suivante :

```
 restrict  <@IP network>
```

```
 dans mon exemple :
 restrict 192.168.1.0/24
```

Dans le même fichier ajouté ce qui suit :

```
server 127.127.1.0
fudge  127.127.1.0 stratum 10

restrict default kod nomodify notrap nopeer mssntp
```

Relancer le service `ntp` pour prendre en compte la modification.

```
 /etc/init.d/ntp restart
```

autres

Quelques test pour s'assurer, que les serveurs soient bien entrés dans le domaine

```
host -t srv _ldap._tcp.<domaine.loc>
host -t srv _kerberos._tcp.<domaine.loc>
hots -t A <dc.domaine.loc>
```

Pour effacer toutes la configuration de samba (fichier de configuration et base local)

```
rm -f /usr/local/samba/etc/smb.conf
rm -rf /usr/local/samba/private/*
```

Affiché les connexions actives via Samba :

```
smbstatus -v
```

sources : samba.org