Active Directory avec des Contrôleurs de Domaine sous Linux avec Samba

Superviseur : Patrice Krzanik

Tunui Franken

Table des matières

1 But de la manœuvre

Nous allons implémenter une forêt Active Directory, mais avec des contrôleurs de domaines sous Linux. Il faut avoir des serveurs qui prennent le rôle du contrôleur de domaine. Nous allons utiliser pour cela des serveurs Samba.

Nous aurons deux contrôleurs AD Samba pour la redondance et un client à ajouter au domaine.

2 Prérequis

— Deux VM pour faire les contrôleurs de domaine, contenant une installation simple mais fonctionnelle de Debian 10 (Buster).
— Une VM pour pour le client, sous Windows XP.

On donne à toutes les machines une configuration réseau par pont.

On ne va pas couvrir l'installation des VM à proprement parler, mais nous configurons les machines de la façon suivante :

	Serveur Debian 1	**Serveur Debian 2**
RAM	1 Go	1 Go
Disque dur	8 Go	8 Go
Nom de l'ordinateur	debian-server-1	debian-server-2
Domaine	afpa.fr	afpa.fr
Mot de passe root	afpa	afpa
Utilisateur	Tunui Franken	Tunui Franken
Identifiant	administrateur	administrateur
Mot de passe utilisateur	afpa	afpa
Adresse IP	192.168.0.11/24	192.168.0.12/24
Passerelle	192.168.0.1	192.168.0.1
DNS	ceux du FAI, que l'on va changer plus tard	

	Client Windows XP
RAM	512 Mo
Disque dur	10 Go
Nom de l'ordinateur	win-xp-client
Mot de passe administrateur	afpa
Utilisateur	Tunui Franken
Adresse IP	192.168.0.9/24
Passerelle	192.168.0.1
DNS primaire	192.168.0.11
DNS secondaire	192.168.0.12

3 Configuration des serveurs Samba

3.1 Prérequis

Il faut plusieurs choses avant de procéder à l'installation. Les étapes suivantes sont nécessaires sur les deux serveurs :

- **Un nom d'hôte.**
  Nous utilisons `debian-server-1` et `debian-server-2`.
- **Un nom de domaine DNS pour la fôret AD.**
  Nous utilisons `afpa.fr`. Il faut noter que le nom de domaine ne pourra pas être modifié, et que le TLD ne peut pas être `.local`, qui est utilisé par Avahi.
- **Une adresse IP statique.**
  Nous utilisons `192.168.0.11` et `192.168.0.12`.
- **Désactiver les outils qui écrasent le fichier `/etc/resolv.conf`.**
  Par exemple `NetworkManager` ou `resolvconf`.
- **Vérifier qu'aucun processus Samba ne tourne.**
  À priori avec une nouvelle installation d'OS, on ne devrait rien trouver, mais sait-on jamais :

  ```
  # ps ax | egrep "samba|smbd|nmbd|winbindd"
  ```

  ... et arrêter tout processus qui s'affiche.
- **Le contrôleur de domaine doit résoudre le FQDN et le nom d'hôte du contrôleur de domaine.**
  On ajoute les lignes suivantes au fichier `/etc/hosts` :

  ```
  127.0.0.1      localhost
  192.168.0.11   debian-server-1.afpa.fr   debian-server-1
  192.168.0.12   debian-server-2.afpa.fr   debian-server-2
  ```

- **Supprimer le fichier `/etc/krb5.conf` s'il existe.**

3.2 Installation

On commence par installer BIND, même si on fera la configuration plus tard. En effet, samba aura besoin de l'utilsateur `bind` lors de l'installation pour des histoires de droits sur des fichiers. Il faut donc que bind9 soit installé avant samba.

```
# apt install bind9 bind9utils
```

Puis on installe les paquets nécessaires pour Samba :

```
# apt install acl attr samba samba-dsdb-modules samba-vfs-modules winbind libpam
   -winbind libnss-winbind libpam-krb5 krb5-config krb5-user dnsutils
```

- On n'utilise pas de DHCP, donc on répond non à la question demandant de modifier `/etc/samba/smb.conf` pour le DHCP.
- Pour le royaume Kerberos, on indique `AFPA.FR`.

— On indique les serveurs Kerberos `debian-server-1 debian-server-2`.
— Pour le serveur administratif, on va indiquer `debian-server-1`.

3.3 Active Directory sur le serveur principal : créer la forêt

Sur le serveur principal, on doit créer la fôret Active Directory et promouvoir le serveur en contrôleur de domaine. La commande samba va générer un fichier `/etc/samba/smb.conf`, donc on commence par supprimer celui qui a été créé lors de l'installation :

```
# rm /etc/samba/smb.conf
```

Puis on crée la forêt :

```
# samba-tool domain provision --use-rfc2307 --realm=AFPA.FR --domain=AFPA --
   server-role=dc --dns-backend=BIND9_DLZ --adminpass=Afpa123
```

3.4 Configuration du DNS pour Samba

Le DNS est à configurer sur les deux serveurs pour la redondance.

On a installé BIND avec Samba.

Dans le fichier `/etc/default/bind9`, on change la ligne `OPTIONS="-u bind"` qu'on remplace par `OPTIONS="-u bind -4"` :

```
# sed -i 's/-u bind/-u bind -4/' /etc/default/bind9
```

Maintenant on modifie le fichier `/etc/bind/named.conf.options` pour qu'il contienne :

```
// Managing acls
acl internals { 127.0.0.0/8; 192.168.0.0/24; };

options {
    directory "/var/cache/bind";
    version "Go Away 0.0.7";
    notify no;
    empty-zones-enable no;
    auth-nxdomain yes;
    forwarders { 89.2.0.1; 89.2.0.2; };
    allow-transfer { none; };

    dnssec-validation no;
    dnssec-enable no;
    dnssec-lookaside no;

    // If you only use IPv4.
    listen-on-v6 { none; };
    // listen on these ipnumbers.
```

```
    listen-on port 53 { 192.168.0.11; 127.0.0.1; };

    // Added Per Debian buster Bind9.
    // Due to : resolver: info: resolver priming query complete messages in the
        logs.
    // See: https://gitlab.isc.org/isc-projects/bind9/commit/4
        a827494618e776a78b413d863bc23badd14ea42
    minimal-responses yes;

    // Add any subnets or hosts you want to allow to use this DNS server
    allow-query { "internals"; };
    allow-query-cache { "internals"; };

    // Add any subnets or hosts you want to allow to use recursive queries
    recursion yes;
    allow-recursion { "internals"; };

    // https://wiki.samba.org/index.php/Dns-backend_bind
    // DNS dynamic updates via Kerberos (optional, but recommended)
    // ONE of the following lines should be enabled AFTER you provision or join
        a DC with bind9_dlz
    // or AFTER upgrading your dns from internal to bind9_dlz
    // Before Samba 4.9.0
    // tkey-gssapi-keytab "/var/lib/samba/private/dns.keytab";
    // From Samba 4.9.0 ( You will need to run samba_dnsupgrade if upgrading
        your Samba version. )
    tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";
};
```

Sur chaque serveur, les adresses IP sont à adapter (`192.168.0.11` sur `debian-server-1` et `192.168.0.12` sur `debian-server-2`)

Dans le fichier `/etc/bind/named.conf.local`, on ajoute la ligne suivante :

```
include "/var/lib/samba/bind-dns/named.conf";
```

Le dossier `/var/lib/samba/bind-dns/` de cette ligne est créé lors de la promotion en contrôleur de domaine. À ce stade, sur `debian-server-1` cela a été fait, mais sur `debian-server-2` ce sera fait quand le serveur rejoindra la forêt créée précédemment.

Il faut dans les deux cas s'assurer que la dernière ligne de ce fichier inclus (`/var/lib/samba/bind-dns/named.conf`), correspondant à la version 9.11.x de BIND, soit décommentée.

Sur `debian-server-2`, les vérifications suivantes ne pourront être faites qu'après avoir rejoint la forêt.

On vérifie la configuration :

```
# named-checkconf
```

Il faut vérifier certaines permissions de fichiers :

```
# chmod 640 /var/lib/samba/bind-dns/dns.keytab
# chown root:bind /var/lib/samba/bind-dns/dns.keytab

# chmod 770 /var/lib/samba/bind-dns
# chown root:bind /var/lib/samba/bind-dns
```

L'utilisateur `bind` devrait pouvoir lire le fichier `dns.keytab` :

```
# sudo -u bind cat /var/lib/samba/bind-dns/dns.keytab
```

On vérifie que la commande `nsupdate` existe :

```
# which nsupdate
```

Maintenant que le DNS est configuré, il faut que le fichier `/etc/resolv.conf` contienne la bonne entrée pour interroger le bon serveur DNS, en l'occurrence soi-même.

Sur `debian-server-1` :

```
nameserver 127.0.0.1
```

Sur `debian-server-2` :

```
nameserver 192.168.0.11
nameserver 127.0.0.1
```

On peut maintenant relancer le service `bind9` :

```
# systemctl restart bind9
```

Et on fait des requêtes DNS de vérification :

```
$ host -t NS afpa.fr
$ host -t A localhost 127.0.0.1
$ host -t PTR 127.0.0.1 127.0.0.1
```

On vérifie également que notre DNS sait sortir sur Internet :

```
$ host debian.org
```

3.5 Configuration de Kerberos

Sur `debian-server-1`, il faut copier le ficher de configuration Kerberos créé par Samba dans `/etc/` (et écraser si le fichier était déjà présent) :

```
# cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

Sur `debian-server-2`, on va écrire ce fichier `/etc/krb5.conf` à la main :

```
[libdefaults]
    default_realm = AFPA.FR
    dns_lookup_realm = false
    dns_lookup_kdc = true
```

Puis on vérifie :

```
# kinit administrator
# klist
```

On vérifie que `bind` pourra accéder à `/etc/krb5.conf` :

```
# chmod 644 /etc/krb5.conf
# chown root:bind /etc/krb5.conf
# sudo -u bind cat /etc/krb5.conf
```

3.6 Démarrage de Samba

Sur `debian-server-1`, on démarre le service samba. Sur `debian-server-2`, passer cette partie, on y reviendra plus tard.

Les services `smbd` et `winbindd` doivent être démarrés en tant que processus fils du service `samba`. Il faut donc tout d'abord masquer et désactiver ces services :

```
# systemctl mask smbd nmbd winbind
# systemctl disable smbd nmbd winbind
```

Pour créer le fichier de service pour `samba`, on doit supprimer le lien symbolique `/etc/systemd/system/samba-ad-dc.service` :

```
# systemctl unmask samba-ad-dc.service
```

... et créer un fichier à la place, avec le contenu suivant :

```
[Unit]
Description=Samba Active Directory Domain Controller
After=network.target remote-fs.target nss-lookup.target

[Service]
Type=forking
ExecStart=/sbin/samba -D
PIDFile=/run/samba/samba.pid
ExecReload=/bin/kill -HUP $MAINPID

[Install]
WantedBy=multi-user.target
```

On relance la configuration `systemd` :

```
# systemctl daemon-reload
```

Puis on active le service en question pour qu'il se lance au démarrage :

```
# systemctl enable samba-ad-dc
```

On peut enfin le démarrer :

```
# systemctl start samba-ad-dc
```

3.7 Active Directory sur le serveur secondaire : rejoindre la forêt

Sur le serveur secondaire, on ne doit pas créer de fôret Active Directory mais rejoindre la fôret créée par le serveur principal :

```
# rm /etc/samba/smb.conf
# samba-tool domain join afpa.fr DC -U"AFPA\administrator" --dns-backend=
   BIND9_DLZ --option='idmap_ldb:userfc2307 = yes'
```

Ne pas oublier de retourner dans la section DNS (3.4) pour faire les vérifications qui n'étaient pas possibles avant.

3.8 Configuration de la synchronisation des horloges

Il faut que les horloges de nos deux serveurs soient synchronisées. Pour cela on va installer et configurer `ntpd` sur chaque contrôleur de domaine de la forêt.

On installe le paquet `ntp` :

```
# apt install ntp
```

Puis on change les permissions du dossier `/var/lib/samba/ntp_signd` :

```
# chown root:ntp /var/lib/samba/ntp_signd
# chmod 750 /var/lib/samba/ntp_signd
```

Enfin on crée le fichier `/etc/ntpd.conf` et on y ajoute les lignes suivantes :

```
# Local clock. Note that is not the "localhost" address!
server 127.127.1.0
fudge  127.127.1.0 stratum 10

# Where to retrieve the time from
server 0.pool.ntp.org    iburst prefer
server 1.pool.ntp.org    iburst prefer
server 2.pool.ntp.org    iburst prefer

driftfile     /var/lib/ntp/ntp.drift
logfile       /var/log/ntp
```

```
ntpsigndsocket /var/lib/samba/ntp_signd/

# Access control
# Default restriction: Allow clients only to query the time
restrict default kod nomodify notrap nopeer mssntp

# No restriction for "localhost"
restrict 127.0.0.1

# Enable the time sources to only provide time to this host
restrict 0.pool.ntp.org  mask 255.255.255.255  nomodify notrap nopeer noquery
restrict 1.pool.ntp.org  mask 255.255.255.255  nomodify notrap nopeer noquery
restrict 2.pool.ntp.org  mask 255.255.255.255  nomodify notrap nopeer noquery

tinker panic 0
```

La dernière ligne n'est utile que dans le cas d'une installation sur VM, où le système n'a pas accès à une horloge physique.

On finit par relancer le service :

```
# systemctl restart ntp
```

3.9 Configuration de la réplication entre les contrôleurs de domaine

La réplication entre contrôleurs de domaine d'une fôret AD est automatique, mais le répertoire `sysvol` n'est pas répliqué. Pour ça, on va utiliser `rsync`.

`rsync` étant unidirectionnel, on doit choisir un contrôleur de domaine sur lequel faire toutes nos modifications. L'autre contrôleur de domaine récupèrera les modifications, donc toute modification faite sur ce contrôleur de domaine sera écrasé par la réplication.

Avant de commencer, il faut que les ID User et Group soient les mêmes chez les deux contrôleurs de domaines. Pour cela, on crée d'abord une sauvegarde du fichier `/var/lib/samba/private/idmap.ldb` sur `debian-server-1` : |

```
# tdbbackup -s .bak /var/lib/samba/private/idmap.ldb
```

On transfère ensuite le fichier de sauvegarde résultant `/var/lib/samba/private/idmap.ldb.bk` sur `debian-server-2` :

```
# scp /var/lib/samba/private/idmap.ldb.bak debian-server-2:/var/lib/samba/
   private/
```

Sur `debian-server-2`, on retire le suffixe `.bak` pour remplacer le fichier existant :

```
# mv /var/lib/samba/private/idmap.ldb.bak /var/lib/samba/private/idmap.ldb
```

Attention à ne pas faire cette commande sur `debian-server-1` !

Ensuite, toujours sur `debian-server-2`, on lance la commande suivante :

```
# net cache flush
```

On peut maintenant mettre en place `rsync`.

3.9.1 Sur le contrôleur de domaine principal

On commence par le contrôleur de domaine principal, `debian-server-1`.

On installe `rsync` :

```
# apt install rsync
```

On crée le fichier `/etc/rsyncd.conf` avec le contenu suivant :

```
[SysVol]
path = /var/lib/samba/sysvol/
comment = Samba Sysvol Share
uid = root
gid = root
read only = yes
auth users = sysvol-replication
secrets file = /var/lib/samba/etc/rsyncd.secret
```

Puis on crée le fichier `/var/lib/samba/etc/rsyncd.secret` avec le contenu suivant :

`sysvol-replication:Afpa123`

Le mot de passe n'est pas obligatoirement le même que celui de Samba !

Il faut bien-sûr adapter les permissions de ce fichier pour qu'il ne soit pas lisible :

```
# chmod 640 /var/lib/samba/etc/rsyncd.secret
```

On peut maintenant redémarrer le service.

```
# systemctl restart rsync
```

3.9.2 Sur le contrôleur de domaine secondaire

On installe `rsync` :

```
# apt install rsync
```

On crée un fichier de mot de passe `/var/lib/samba/etc/rsync-sysvol.secret` avec le mot de passe défini sur `debian-server-1` :

```
# mkdir /var/lib/samba/etc && echo "Afpa123" > /var/lib/samba/etc/rsync-sysvol.
   secret
```

Il faut encore une fois adapter les permissions de ce fichier pour qu'il ne soit pas lisible :

```
# chmod 640 /var/lib/samba/etc/rsync-sysvol.secret
```

Et on est prêt à lancer la réplication !

On commence par un `--dry-run` pour un faire un test :

```
rsync --dry-run -XAavz --delete-after --password-file=/var/lib/samba/etc/rsync-
    sysvol.secret rsync://sysvol-replication@192.168.0.11/SysVol/ /var/lib/samba
    /sysvol/
```

On peut faire un `# find / -name sysvol` pour voir si on a bien identifié le répertoire `sysvol`. Si on est bien sûr que la destination est bien le répertoire `sysvol` de `debian-server-2`, on peut relancer la commande sans le `--dry-run`.

On va maintenant lancer cette commande toutes les 5 minutes via `cron` :

```
# crontab -e
```

```
*/5 * * * * rsync -XAavz --delete-after --password-file=/var/lib/samba/etc/rsync
    -sysvol.secret rsync://sysvol-replication@192.168.0.11/SysVol/ /var/lib/
    samba/sysvol/
```

Toujours sur `debian-server-2`, on remet les ACL du dossier `sysvol` :

```
# samba-tool ntacl sysvolreset
```

Une fois la réplication mise en place, on peut démarrer le service samba sur `debian-server-2` (voir 3.6).

Maintenant que les deux contrôleurs de domaines sont en marche, la réplication de contrôleurs de domaine s'initialise, ce qui peut prendre jusqu'à 15 minutes.

3.10 Vérifications

Vérifions tout d'abord l'état de la réplication entre contrôleurs de domaine :

```
# samba-tool drs showrepl
```

Cette commande retourne l'état de la réplication du point de vue du contrôleur de domaine sur lequel la commande a été exécutée.

On peut installer le paquet `smbclient` pour faire quelques requêtes de vérification.

```
$ smbclient -L localhost -N
```

Cette commande doit afficher les partages `netlogon` et `sysvol`, qui sont obligatoires dans un contrôleur de domaine.

On peut ensuite vérifier l'authentification sur `netlogon` :

```
$ smbclient //localhost/netlogon -UAdministrator -c 'ls'
$ smbclient //debian-server-1/netlogon -UAdministrator -c 'ls'
$ smbclient //debian-server-2/netlogon -UAdministrator -c 'ls'
```

On peut faire quelques requêtes DNS pour vérifier la configuration DNS de l'AD :

```
$ host -t SRV _ldap._tcp.afpa.fr
$ host -t SRV _kerberos._udp.afpa.fr
$ host -t A debian-server-1.afpa.fr
$ host -t A debian-server-2.afpa.fr
```

4 Ajout du client au domaine Active Directory

La première chose à faire est de s'assurer que le client a comme configuration DNS les adresses IP de nos deux serveurs. Une fois cette vérification faite, on peut l'ajouter au domaine Active Directory.

Dans le menu Démarrer, on fait un clic droit sur *Poste de travail*, puis on clique sur *Propriétés*. Dans l'onglet *Nom de l'ordinateur*, on clique sur *Modifier*. Dans ce menu on coche *Domaine* dans la section *Membre de*. Dans le champ qu'on vient d'activer, on ajoute `afpa.fr`.

On peut ensuite se connecter avec le compte créé avec Samba : `Administrator` avec le mot de passe `Afpa123`.

On redémarre et le client fait partie du domaine !

5 Sources

https://wiki.samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller

https://wiki.samba.org/index.php/Setting_up_a_BIND_DNS_Server

https://wiki.samba.org/index.php/BIND9_DLZ_DNS_Back_End

https://wiki.samba.org/index.php/Managing_the_Samba_AD_DC_Service_Using_Systemd

https://wiki.samba.org/index.php/Time_Synchronisation

https://wiki.samba.org/index.php/Joining_a_Samba_DC_to_an_Existing_Active_Directory

https://wiki.samba.org/index.php/Samba_&_LDAP

https://wiki.samba.org/index.php/Rsync_based_SysVol_replication_workaround

https://wiki.samba.org/index.php/Verifying_the_Directory_Replication_Statuses

https://wiki.samba.org/index.php/Joining_a_Windows_Client_or_Server_to_a_Domain