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 deux clients faisant partie du domaine.

2 Prérequis

— Deux VM pour faire les contrôleurs de domaine, contenant une installation simple mais fonctionnelle de Debian 10 (Buster).
— Deux VM pour faire les clients. Pour s'assurer que tout soit compatible, nous allons utiliser une VM sous Windows XP et une VM sous Windows 10.

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	Client Windows 10
RAM	512 Mo	2 Go
Disque dur	10 Go	50 Go
Nom de l'ordinateur	win-xp-client	win-10-client
Domaine	afpa.fr	afpa.fr
Mot de passe root	afpa	afpa
Utilisateur	Tunui Franken	Tunui Franken
Identifiant	Tunui Franken	Tunui Franken
Mot de passe utilisateur	N/A	N/A
Adresse IP	192.168.0.9/24	192.168.0.10/24
Passerelle	192.168.0.1	192.168.0.1
DNS primaire	192.168.0.11	192.168.0.11
DNS secondaire	192.168.0.12	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

Sur les deux serveurs, on installe les paquets nécessaires :

```
# 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 Samba sur le serveur principal

On va maintenant faire des configurations sur `debian-server-1`.

3.3.1 Mise en place de l'Active Directory Samba

Sur le serveur principal, on doit créer la fôret Active Directory. 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
```

3.3.2 Configuration du DNS pour Samba

On installe BIND :

```
# apt install bind9 bind9utils
```

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 { 8.8.8.8; 8.8.8.4; };
    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; ::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";
};
```

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

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

On vérifie la configuration et on relance le service `bind9` :

```
# named-checkconf && systemctl restart bind9
```

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 :

```
nameserver 127.0.0.1
```

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 interroger les serveurs racines :

```
$ host debian.org
```

3.3.3 Configuration de Kerberos

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
```

3.3.4 Démarrage de Samba

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
```

On doit maintenant créer le fichier de service pour `samba` dans `/etc/systemd/system/samba-ad-dc.service` 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=/var/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
```

3.4 Configuration de la synchronisation des horloges

Il faut que les horloges de nos deux serveurs soient synchronisées. Pour cela on va utiliser `ntpd`.

À finir...

3.5 Samba sur le serveur secondaire

On peut maintenant passer sur `debian-server-2`.

3.5.1 Configuration de Kerberos

On ajoute les paramètres suivants dans le fichier `/etc/krb5.conf` :

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

Puis on vérifie :

```
# kinit administrator
# klist
```

3.5.2 Mise en place de l'Active Directory Samba

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

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

3.6 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`.

3.7 Vérifications

```
$ 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'
```

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
```

On vérifie Kerberos :

```
# kinit administrator
# klist
```

4 Ajout des clients au domaine LDAP

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

— Pour Windows XP :
— Pour Windows 10 :

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