Mise en place d'un serveur LDAP avec OpenLDAP sous Linux

Superviseur : Patrice Krzanik

Tunui Franken

Table des matières

1 But de la manœuvre

Nous allons implémenter une topologie de type Active Directory, mais avec OpenLDAP sous Linux. Nous aurons deux serveurs LDAP pour la redondance et deux clients faisant partie du domaine.

2 Prérequis

Conformément au but de la manœuvre (voir 1), nous allons utiliser plusieurs VM :

— Deux VM pour faire les serveurs LDAP, contenant une installation simple mais fonctionnelle de Debian 10 (Buster).
— Deux VM pour faire les clients. Peu importe leur OS, mais pour s'assurer que tout soit compatible, nous allons utiliser une VM sous Windows XP et une VM sous Xubuntu 20.04 (pour la légèreté).

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	8.8.8.8, que l'on va changer plus tard	

	Client Xubuntu	Client Windows XP
RAM	1 Go	512 Mo
Disque dur	10 Go	10 Go
Nom de l'ordinateur	xubuntu-client	win-xp-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	afpa	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 Schéma LDAP

4 Configuration des serveurs DNS

Nous avons deux machines serveurs qui attendent l'installation des services qui nous intéressent. On va commencer par installer un serveur DNS sur chacune des deux machines.

De manière assez logique, `debian-server-1` servira de serveur DNS principal et `debian-server-2` de DNS secondaire.

Nous allons utiliser BIND.

4.1 Installation de BIND

Tout d'abord, on installe BIND sur chaque machine :

```
# apt install bind9
```

4.2 Configuration du serveur principal

On édite le fichier `/etc/bind/named.conf.local` pour déclarer notre zone :

```
zone "afpa.fr" {
    type master;
    file "/etc/bind/db.afpa.fr";
    allow-transfer { 192.168.0.12; };
};
```

On vérifie la syntaxe avec `named-checkconf /etc/bind/named.conf.local`.

Puis on configure la zone. On commence par créer le fichier nécessaire :

```
# cp /etc/bind/db.local /etc/bind/db.afpa.fr
```

Puis on édite `/etc/bind/db.afpa.fr` :

```
$TTL    604800
$ORIGIN afpa.fr.
@                               IN      SOA     debian-server-1.afpa.fr. admin.
    afpa.fr. (
                                                    2 ; Serial
                                                 3600 ; Refresh
                                                 3000 ; Retry
                                              2419200 ; Expire
                                               604800 ; Negative Cache TTL
                                            )
;
@                               IN      NS      debian-server-1.afpa.fr.
@                               IN      NS      debian-server-2
debian-server-1                 IN      A       192.168.0.11
debian-server-2                 IN      A       192.168.0.12
```

```
_ldap._tcp.afpa.fr.             IN      SRV 10 0 389 debian-server-1.afpa.fr.
_ldap._tcp.dc._msdcs.afpa.fr.   IN      SRV 10 0 389 debian-server-1.afpa.fr.
_ldap._tcp.afpa.fr.             IN      SRV 20 0 389 debian-server-2.afpa.fr.
_ldap._tcp.dc._msdcs.afpa.fr.   IN      SRV 20 0 389 debian-server-2.afpa.fr.
```

On vérifie la syntaxe avec `named-checkzone afpa.fr /etc/bind/bd.afpa.fr`.

On peut maintenant redémarrer BIND :

```
# systemctl restart bind9
```

4.3 Configuration du serveur secondaire

Comme précédemment, on édite le fichier `/etc/bind/named.conf.local` pour déclarer notre zone.

```
zone "afpa.fr" {
    type slave;
    file "/var/cache/bind/db.afpa.fr";
    masters { 192.168.0.11; };
};
```

On vérifie la syntaxe avec `named-checkconf /etc/bind/named.conf.local`.

Ne pas oublier de redémarrer BIND :

```
# systemctl restart bind9
```

C'est tout, puisque c'est le `master` qui met à jour le `slave`.

4.4 Ajout de la résolution inverse

Dans le fichier `/etc/bind/named.conf.local` modifié plus tôt, il faut ajouter la zone inverse :

```
zone "0.168.192.in-addr.arpa." {
    type master;
    file "/etc/bind/db.192.168.0";
};
```

On crée le fichier de zone correspondant (`db.192.168.0`) :

```
$TTL 604800
$ORIGIN 0.168.192.in-addr.arpa.
@       IN      SOA     debian-server-1.afpa.fr. admin.afpa.fr. (
                                  2 ; Serial
                               3600 ; Refresh
                               3000 ; Retry
                            2419200 ; Expire
```

```
                            604800 ; Negative Cache TTL
                           )
;
@       IN      NS      debian-server-1.afpa.fr.
@       IN      NS      debian-server-2.afpa.fr.
11      IN      PTR     debian-server-1.afpa.fr.
12      IN      PTR     debian-server-2.afpa.fr.
```

Et on redémarre le serveur :

```
# systemctl restart bind9
```

4.5 Changement de l'adresse du resolver

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

```
nameserver 127.0.0.1
```

Pour vérifier le bon fonctionnement, sur chaque machine on utilise la commande suivante :

```
$ host -t NS afpa.fr
```

On vérifie également que notre DNS sait interroger les serveurs racines :

```
$ host debian.org
```

Il est à noter que nous éditons le fichier `/etc/resolv.conf` à la main parce que notre installation Debian n'utilise pas de gestionnaire de connexion. Si on utilise NetworkManager par exemple, le fichier `/etc/resolv.conf` sera écrasé, il faut donc dans ce cas utiliser NetworkManager.

5 Configuration des serveurs LDAP

5.1 Installation

Il faut tout d'abord installer le serveur LDAP. Sur Debian il s'agit du paquet `slapd`. On va lui ajouter `ldap-utils`, un paquet utilisé pour configurer `slapd` et les dossiers.

```
# apt install slapd ldap-utils
```

Pendant l'installation on nous demande un mot de passe pour l'administrateur de l'annuaire LDAP. On va utiliser `afpa`.

On peut d'ores et déjà interagir avec l'annuaire LDAP. Par défaut, il a été préconfiguré avec le nom de domaine de notre DNS (qu'on a défini sur `afpa.fr`).

```
# ldapsearch -x -b "dc=afpa,dc=fr"
```

On peut se connecter en tant qu'administrateur en utilisant le mot de passe défini pendant l'installation :

```
# ldapsearch -x -D "cn=admin,dc=afpa,dc=fr" -W -b "dc=afpa,dc=fr"
```

- `-x` utilise l'authentification simple.
- `-D` utilise le Distinguished Name (DN) pour établir une connexion.
- `-W` permet de ne pas fournir le mot de passe dans la commande.
- `-b` utilise une base différente de celle par défaut pour la recherche.

On va maintenant finir la configuration :

```
# dpkg-reconfigure slapd
```

Et on répond aux questions :

- `Voulez-vous omettre la configuration d'OpenLDAP ?`
  → Non
- `Nom de domaine :`
  → `afpa.fr`
- `Nom d'entité (« organization ») :`
  → `afpa`
- `Mot de passe de l'administrateur :`
  → `afpa`
- `Module de base de données à utiliser :`
  → `MDB`
- `Faut-il supprimer la base de données lors de la purge du paquet ?`
  → Non
- `Faut-il déplacer l'ancienne base de données ?`
  → Oui

Pour éviter de devoir spécifier la base à chaque fois, on va modifier le fichier `/etc/ldap/ldap.conf`. On décommente les lignes commençant par `BASE` et `URI` et on

ajuste leur valeur :

```
BASE    dc=apfa,dc=fr
URI     ldap://localhost:389
```

On teste si ça marche :

```
# systemctl restart slapd
# ldapsearch -x
```

Ne pas oublier de faire les mêmes étapes sur `debian-server-2`.

5.2 Ajout de premières entrées dans l'annuaire

Nous allons plus tard configurer la réplication entre les deux serveurs. Il ne faut donc faire ces étapes que sur la machine principale, `debian-server-1`.

Pour ajouter une entrée dans l'annuaire, deux étapes :

1. créer un fichier LDIF
2. utiliser la commande `ldapadd`

On crée donc un fichier qu'on va appeler `tunuifranken.ldif` avec le contenu suivant :

```
dn: ou=groups,dc=afpa,dc=fr
objectclass: top
objectclass: organizationalUnit
ou: groups
description: OU pour les groupes

dn: ou=users,dc=afpa,dc=fr
objectclass: top
objectclass: organizationalUnit
ou: users
description: OU pour les utilisateurs de l'Afpa

dn: cn=admin,ou=groups,dc=afpa,dc=fr
objectclass: top
objectclass: posixGroup
gidNumber: 500
cn: admin

dn: cn=guest,ou=groups,dc=afpa,dc=fr
objectclass: top
objectclass: posixGroup
gidNumber: 501
cn: guest
```

```
dn: cn=Tunui Franken Admin,ou=users,dc=afpa,dc=fr
objectclass: top
objectclass: posixAccount
objectclass: inetOrgPerson
userPassword: afpaadmin
gidNumber: 500
uidNumber: 1000
userID: tfadmin
homeDirectory: /home/users/tfadmin
loginShell: /bin/sh
givenName: TF Admin
sn: Franken
cn: Tunui Franken Admin

dn: cn=Tunui Franken User,ou=users,dc=afpa,dc=fr
objectclass: top
objectclass: posixAccount
objectclass: inetOrgPerson
userPassword: afpauser
gidNumber: 501
uidNumber: 1001
userID: tfuser
homeDirectory: /home/users/tfuser
loginShell: /bin/sh
givenName: TF User
sn: Franken
cn: Tunui Franken User
```

Ce fichier déclare d'abord deux nouvelles OU à créer, puis deux groupes `admin` et `guest` dans l'OU `groups`, et enfin les utilisateurs `Tunui Franken Admin` et `Tunui Franken User` faisant partie chacun d'un groupe.

On ajoute maintenant les entrées de ce fichier dans l'annuaire :

```
# ldapadd -x -D "cn=admin,dc=afpa,dc=fr" -W -f tunuifranken.ldif
```

Pour vérifier que les entrées ont bien été ajoutées :

```
# ldapsearch -x
```

5.3 Vérification de la communication entre les deux servers

Nous avons maintenant configuré `slapd` sur nos deux serveurs et nous avons ajouté deux entrées à notre serveur `debian-server-1`.

Nous allons maintenant nous assurer que la communication entre les serveurs sous LDAP marche correctement :

Depuis `debian-server-1` :

```
# ldapsearch -x -H ldap://debian-server-2.afpa.fr -D cn=admin,dc=afpa,dc=fr -W
```

Depuis `debian-server-2` :

```
# ldapsearch -x -H ldap://debian-server-1.afpa.fr -D cn=admin,dc=afpa,dc=fr -W
```

5.4 Configuration de la réplication LDAP

5.4.1 Choix du type de réplication

D'après la documentation OpenLDAP, il y a plusieurs possibilités pour la réplication :

- **Syncrepl** (LDAP Sync Replication) — La solution la plus simple mais gourmande en bande passante et en charge.
- **Delta-syncrepl** — Ne synchronise que les changements des attributs des objets, permettant une réplication incrémentale, économisant la bande passante et la charge.
- **N-Way Multi-Provider** — Réplique sur plusieurs contrôleurs de domaines actifs. C'est surtout utile pour la redondance.
- **MirrorMode** — Les contrôleurs de domaine se répliquent mutuellement. Des mises à jour de l'annuaire peuvent être envoyées à l'un ou à l'autre. Nécessite un équilibreur de charge.
- **Syncrepl Proxy Mode** — Utile dans des cas précis de topologie de réseau avec par exemple des pares-feu.

Comme nous n'avons pas d'équilibrage de charge ni de proxy, nous allons utiliser le `Delta-syncrepl`.

5.4.2 Delta-syncrepl pour le contrôleur principal (Provider)

5.4.3 Delta-syncrepl pour le contrôleur secondaire (Consumer)

6 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 LDAP.

— Pour Xubuntu :
— Pour Windows XP :
On entre dans le menu `Démarrer`, puis un clic droit sur `Mon Ordinateur`, clic sur `Propriétés`. Dans l'onglet `Nom de l'ordinateur`, on clique sur `Modifier` pour rejoindre un domaine. Puis on coche `Membre d'un domaine` et on entre `afpa.fr`.

7 Sources

https://openclassrooms.com/fr/courses/857447-apprenez-le-fonctionnement-des-reseaux-tcp-ip/857163-le-service-dns

https://ldap.com/dns-srv-records-for-ldap/

https://wiki.archlinux.org/index.php/OpenLDAP

https://wiki.debian.org/LDAP/OpenLDAPSetup

https://www.openldap.org/doc/admin24/quickstart.html

https://www.openldap.org/doc/admin24/config.html

https://www.openldap.org/doc/admin24/replication.html

https://www.howtoforge.com/set-up-openldap-client-on-debian-10/