



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

Superviseur : Patrice Krzanik

Tunui Franken



Table des matières

1	But de la manœuvre	3
2	Prérequis	3
3	Schéma LDAP	4
4	Configuration des serveurs DNS	5
4.1	Installation de BIND	5
4.2	Configuration du serveur principal	5
4.3	Configuration du serveur secondaire	6
4.4	Ajout de la résolution inverse	6
4.5	Changement de l'adresse du resolver	7
5	Configuration des serveurs LDAP	8
5.1	Installation	8
5.2	Ajout de premières entrées dans l'annuaire	9
5.3	Vérification de la communication entre les deux servers	10
6	Configuration des serveurs Samba	12
6.1	Prérequis	12
6.2	Installation	12
6.3	Configuration du module BIND9_DLZ	12
6.4	Configuration de la synchronisation des horloges	13
6.5	Samba sur le serveur principal	13
6.6	Samba sur le serveur secondaire	13
6.7	Configuration de la réplication entre les contrôleurs de domaine	14
6.8	Vérifications	14
7	Ajout des clients au domaine LDAP	15
8	Sources	16

1 But de la manœuvre

Nous allons implémenter une topologie de type Active Directory, mais avec OpenLDAP sous Linux. Le but est que les clients ne sachent pas s'ils sont dans un domaine géré avec OpenLDAP ou avec Active Directory.

Nous aurons deux serveurs LDAP pour la redondance et deux clients faisant partie du domaine.

Quand on ajoute un client Windows à un domaine, il va chercher un contrôleur de domaine Active Directory. Nos serveurs LDAP ne sont pas contrôleurs de domaine Active Directory.

Nous pourrions utiliser un logiciel tiers pour gérer l'authentification du client Windows en utilisant LDAP, par exemple *pGina* (<http://pgina.org/>). Mais cela ne mettrait pas le client Windows dans un domaine Active Directory à proprement parler. De plus, cela rajouterait une contrainte dans un contexte de déploiement.

Il faut avoir un serveur qui prenne le rôle du contrôleur de domaine et qui s'authentifie avec le serveur LDAP. Nous allons utiliser pour cela un serveur Samba.

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 désactiver les outils comme NetworkManager ou resolvconf.

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 serveurs

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
```

6 Configuration des serveurs Samba

Nous utilisons deux serveurs LDAP pour la redondance. Il est logique d'utiliser deux serveurs Samba pour la même raison. Chaque machine serveur (`debian-server-1` et `debian-server-2`) aura un serveur Samba en plus du serveur LDAP.

6.1 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 forêt 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`. Nous avons bien édité le fichier `/etc/resolv.conf` à la main (voir 4.5).
- **Vérifier qu'aucun processus Samba ne tourne.**
`# 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.**

6.2 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
```

6.3 Configuration du module BIND9_DLZ

À faire...

6.4 Configuration de la synchronisation des horloges

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

6.5 Samba sur le serveur principal

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

6.5.1 Mise en place de l'Active Directory Samba

Sur le serveur principal, on doit créer la forêt Active Directory :

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

6.5.2 Configuration de Kerberos

Il faut copier le fichier de configuration Kerberos créé par Samba dans `/etc/` :

```
# cp /usr/local/samba/private/krb5.conf /etc/krb5.conf
```

6.5.3 Démarrage de Samba

On démarre le service `samba` en l'activant pour qu'il démarre automatiquement :

```
# systemctl enable samba && systemctl start samba
```

6.6 Samba sur le serveur secondaire

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

6.6.1 Configuration de Kerberos

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

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

Puis on vérifie :

```
# kinit administrator  
# klist
```

6.6.2 Mise en place de l'Active Directory Samba

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

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

6.7 Configuration de la réplication entre les contrôleurs de domaine

6.8 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
```

On vérifie Kerberos :

```
# kinit administrator
# klist
```

7 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 :

Quand on ajoute un client Windows à un domaine, il cherche à joindre un contrôleur de domaine Active Directory.

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