



Installation
Configuration

Serveur DNS

Debian 7.2

Bind9

Objectif : mettre en place un serveur DNS afin de pouvoir effectuer des résolutions de noms FQDN en adresse IP et d'adresse IP en noms FQDN.

Tout d'abord nous allons installer le paquet avec la commande **apt-get install bind9**. Les fichiers qui sont en **named** sont des fichiers de configurations qui définissent le type de zone. Les fichiers **db** sont des fichiers de zones directes pour un domaine.

Dans le fichier **named.conf.local** est le fichier dans lequel on définit nos zones directes ou inversées de notre domaine.

Exemple de configuration :

```
zone « lycée.fr » IN{
    type master ; #slave (secondaire)
file « /var/cache/bind/db.lycée.fr » ; #db pour la zone directes
};
zone « 1.168.192.in-addr.arpa » IN{
    type master ;
    file « var/cache/bind/rev.lycée.fr » ; #rev pour la zone inversée
};
```

Pour tester notre fichier de configuration on utilise la commande **named-checkconf /chemincomplet (/etc/bind/named.conf.local)**.

Une fois ceci fait on crée notre zone directe dans **/var/cache/bind/xxxxxxxxx (db.lycee.fr)**.

Structure du fichier :

```
$TTL ttl
@ IN SOA serveur. Mailadmin. ( #nom zone : @ #mail : admin.lycee.fr
    20140925 ; SERIAL
    172800 ; REFRESH
    600 ; RETRY
    1209600 ; EXPIRE
    600 ) ; Negative Cache TTL
@ IN NS serveur.domaine.local. (debian.lycee.fr)
debian IN A 192.168.1.93 (serveur IN A adresse ip serveur)
ENZO-PC IN A 192.168.1.94 (machine)
```

Ensuite on crée la zone inversée dans **/var/cache/bind/xxxxxxxxx (rev.lycee.fr)**.

Structure du fichier :

```
$TTL 3600
@ IN SOA serveur. Mailadmin. (
    20140925 ; SERIAL
    172800 ; REFRESH
    600 ; RETRY
    1209600 ; EXPIRE
    600 ) ; Negative Cache TTL
@ IN NS serveur.
93 IN PTR serveur.domaine.local. (93 = 4e octet de l'ip)
94 IN PTR machine.domaine.local. (machine)
```

Ensuite redémarrez le service avec la commande **service bind9 restart** ou recharger les fichiers de configuration sans redémarrer le service avec la commande : **rndc reload**.

Tolérance de panne de serveur DNS :

Il suffira d'installer **bind9** sur une machine secondaire et de rajouter dans le fichier `named.conf.local` de la machine maître les lignes suivantes dans chaque zone :

```
notify yes ;
allow-transfer {192.168.1.x;} ; #@ip du serveur secondaire
```

Ensuite n'oubliez pas de changer le nom de votre machine si votre machine secondaire a le même nom que votre machine principale avec la commande **nano /etc/hostname** et **nano /etc/hosts**.

Une fois ceci fait il faut configurer le fichier `named.conf.local` de votre machine secondaire :

```
zone « lycée.fr » IN{
    type slave ;
    masters {192.168.1.x;} ; #@ip serveur principal
    file « /var/cache/bind/db.lycée.fr » ; #db pour la zone directes
};
```

```
zone « 1.168.192.in-addr.arpa » IN{
    type slave ;
    masters {192.168.1.x;} ; #@ip serveur principal
    file « var/cache/bind/rev.lycée.fr » ; #rev pour la zone inversée
};
```

Vous devrez ensuite ajoutez plusieurs lignes dans votre zone directe de votre machine principale :

```
@ IN NS hostname (de la machine secondaire).lycee.fr.
hostname (de la machine secondaire).lycee.fr. IN A 192.168.1.x #@ip serveur secondaire
```

Ensuite ajoutez plusieurs lignes dans votre zone inversée de votre machine principale :

```
@ IN NS hostname (de la machine secondaire).lycee.fr.
95 IN PTR hostname(de la machine secondaire).lycee.fr.
```

Pour vérifier le bon fonctionnement, modifiez les zones sur le DNS principal en changeant les valeurs de la ligne `SERIAL` en incrémentant et tapez la commande **rndc reload**. Si vous avez les nouveaux fichiers de zones dans votre serveur secondaire alors votre serveur DNS marche !