INSTALLATION ET CONFIGURATION SERVEUR DNS SOUS LINUX

- 1. Quand il est configuré en serveur de noms en mode cache, BIND9 effectuera les résolutions de noms et se souviendra de la réponse lorsque qu'un domaine sera demandé une nouvelle fois.
- 2. En tant que serveur maitre primaire, BIND9 lit les données d'une zone dans un fichier sur son serveur hôte et il fait autorité pour cette zone.
- 3. En tant que maitre secondaire, BIND9 obtient les données de la zone depuis le serveur de noms faisant autorité pour la zone.

Aperçu

Les fichiers de configuration DNS sont situés dans le répertoire /etc/bind. Le fichier de configuration de base est /etc/bind/named.conf.

La ligne include spécifie le nom du fichier contenant les options DNS. La ligne directory dans le fichier /etc/bind/named.conf.options indique au DNS où chercher les fichiers. Tous les fichiers utilisés par BIND seront relatifs à ce répertoire.

Le fichier /etc/bind/db.root décrit les serveurs DNS racines mondiaux. Les serveurs changeant de temps à autre, il est nécessaire de mettre à jour ce fichier de temps en temps. Ceci est généralement effectué par des mises à jour du paquet bind9. La section zone définit le serveur maitre, et est stockée dans le fichier spécifié par l'option file.

Il est possible de configurer un unique serveur comme serveur de noms en mode cache, maitre primaire et maitre secondaire. Un serveur peut faire autorité sur une zone (**Start of Authority, SOA**), tout en fournissant un service secondaire pour une autre zone, et en fournissant des services de cache pour les hôtes sur le LAN local.

Serveur de noms de cache

La configuration par défaut alloue un rôle de serveur cache. Il vous suffit d'ajouter les adresses IP des DNS de votre FAI. Dé-commentez simplement et modifiez ce qui suit dans /etc/bind/named.conf.options :

Remplacez 1.2.3.4 et 5.6.7.8 par les adresses IP des véritables serveurs de noms.

Redémarrez à présent le serveur DNS pour appliquer les changements. Saisissez dans un terminal :

```
sudo systemctl restart bind9.service
```

Maitre primaire

Dans cette section, *BIND9* sera configuré comme serveur primaire du domaine *example.com*. Remplacez *example.com* par votre FQDN (Fully Qualified Domain Name).

Fichier zone de recherche directe (Forward zone)

Pour ajouter une zone DNS à BIND9 afin de le transformer en serveur maitre primaire, il faut tout d'abord modifier /etc/bind/named.conf.local :

```
zone "example.com" {
    type master;
    file "/etc/bind/db.example.com";
};
```

Nous utiliserons un fichier zone existant comme modèle pour la création du fichier /etc/bind/db.example.com :

```
sudo cp /etc/bind/db.local /etc/bind/db.example.com
```

Créer un *enregistrement A* pour le domaine de base, *exemple.com*. Également, créer un *enregistrement A* pour *ns.exemple.com*, le serveur de noms dans cet exemple :

```
;
; BIND data file for example.com
$TTL
        604800
        IN
                 SOA
                         example.com. root.example.com. (
                                           ; Serial
                          604800
                                           ; Refresh
                           86400
                                          ; Retry
                         2419200
                                           ; Expire
                          604800 )
                                           ; Negative Cache TTL
        IN
                         192.168.1.10
                Α
;
@
                         ns.example.com.
        IN
                NS
                         192.168.1.10
@
        IN
                A
```

```
0 IN AAAA ::1
ns IN A 192.168.1.10
```

Vous devez incrémenter le *numéro de série (Serial Number)* à chaque fois que vous modifiez le fichier de zone. Si vous faites de multiples modifications en seule fois, n'incrémentez le numéro qu'une seule fois.

Vous pouvez ajouter maintenant les enregistrements DNS à la fin du fichier de zone.

Une fois les modifications apportées au fichier de zone, *BIND9* doit être redémarré pour que les changements soient pris en compte :

```
sudo systemctl restart bind9.service
```

Fichier zone de recherche inverse

Maintenant que la zone est configurée pour résoudre les noms en adresses IP, il est nécessaire de paramétrer la **zone de recherche inverse** (Reverse zone). Celle-ci permet de résoudre les adresses IP en noms.

Modifiez /etc/bind/named.conf.local et ajoutez ce qui suit :

Modifiez /etc/bind/named.conf.local et ajoutez ce qui suit :

```
zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};
```

Remplacez 1.168.192 par les trois premiers octets du réseau que vous utilisez. Nommez également le fichier de zone /etc/bind/db.192 en conséquence. Il devrait correspondre au premier octet de votre réseau.

Créez maintenant le fichier /etc/bind/db.192 :

```
sudo cp /etc/bind/db.127 /etc/bind/db.192
```

Modifiez ensuite /etc/bind/db.192 en changeant les mêmes options que dans /etc/bind/db.example.com :

```
;
; BIND reverse data file for local 192.168.1.XXX net
;
$TTL 604800
@ IN SOA ns.example.com. root.example.com. (
2 ; Serial
```

```
604800
                                           ; Refresh
                            86400
                                           ; Retry
                          2419200
                                           ; Expire
                           604800)
                                           ; Negative Cache TTL
;
(a
        IN
                 NS
                          ns.
10
        IN
                 PTR
                          ns.example.com.
```

Après avoir créé le fichier de zone de recherche inverse, redémarrez BIND9 :

```
sudo systemctl restart bind9.service
```

Maitre secondaire

Une fois que le *maitre primaire* est paramétré il faut configurer un *maitre secondaire* afin de maintenir la disponibilité du domaine en cas d'indisponibilité du serveur primaire.

Nous devons tout d'abord autoriser le transfert de zone sur le serveur maitre primaire. Ajoutez l'option *allow-transfer* dans les exemples de définitions de zone de recherche directe et inverse du fichier /etc/bind/named.conf.local :

```
zone "example.com" {
          type master;
          file "/etc/bind/db.example.com";
          allow-transfer { 192.168.1.11; };
};

zone "1.168.192.in-addr.arpa" {
          type master;
          file "/etc/bind/db.192";
          allow-transfer { 192.168.1.11; };
};
```

Remplacez 192.168.1.11 par l'adresse IP de votre serveur de noms secondaire.

Redémarrer Bind9 sur le serveur primaire

```
sudo systemctl restart bind9.service
```

Installez ensuite le paquet *bind9* sur votre serveur maitre secondaire de la même manière que pour le serveur primaire. Puis modifiez le fichier /etc/bind/named.conf.local et ajoutez les déclarations suivantes pour les zones de recherche directe et inverse :

```
zone "example.com" {
    type slave;
    file "db.example.com";
    masters { 192.168.1.10; };
};

zone "1.168.192.in-addr.arpa" {
    type slave;
    file "db.192";
    masters { 192.168.1.10; };
};
```

Remplacez 192.168.1.10 par l'adresse IP de votre serveur de noms primaire.

Redémarrez BIND9 sur votre serveur maître secondaire :

```
sudo systemctl restart bind9.service
```