

Configuration du service DNS sur CentOS 6

Il y'a beaucoup de chose que j'ignore encore dans ce service mais le peut de chose que je sais est que sont principe de fonctionnement est un peu comme celui du répertoire téléphonique et les numéros associés. Les ordinateurs utilisent les adresses IP qui sont des chiffres et il serait très difficile de mémorisé les chiffres que de mémoriser un nom significatif comme google.com, yahoo.fr ou encore facebook.com. Donc lorsque vous ouvrir votre navigateur et vous tapez www.google.com, c'est le DNS qui fait le reste du travail. Nous allons sans plus faire de discours configurer ce service. Comme nous l'avons détaillé dans les tutoriels sur **l'installation d'un dépôt local** et préciser la création d'un alias dans le tutoriel sur la **configuration du DHCP**, nous allons installer **bind** (qui est le package du DNS) de la manière suivante :

```
[root@serveur aurelien]# yu install bind
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
* c6-media:
Setting up Install Process
Package 32:bind-9.7.0-5.P2.el6.i686 already installed and latest version
```

Bon vous pouvez constater que sur mon système il est déjà installé. Il ne nous reste plus qu'a le configurer.

Il existe un excellent livre sur le système. Il s'agit du manuel de bind9. Doc vous allez le mettre sur votre bureau avec la commande suivante et pouvoir le consulter pour comprendre contrairement ce que cache bind.

```
Cp /usr/share/doc/bind-9.7.0/arm/Bv9ARM.pdf /home/nom_utilisateur/Bureau
```

Le premier fichier que nous allons modifier est **/etc/named.conf**. Utilisez votre éditeur favori pour l'éditer. Vous allez vous rendre compte qu'il y'a déjà pas mal de chose dans ce fichier. Modifier les a votre convenance mais je ne modifie

généralement rien et je me contente juste d'ajouter mes zones. Voilà ce que j'ai ajouté pour le moment :

```
zone "aurelien.lan" {
    type master;
    file "aurelien";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "aurelien.rev";
};
```

Le type master veut dire que mon domaine est le maître. S'il est esclave on met slave à la place. Vous remarquez la zone se terminant par **in-addr.arpa** (doit toujours apparaître à la fin d'une résolution inverse). C'est la résolution inverse de la zone **aurelien.lan**

File indique le nom du fichier de configuration de zone

Vous avez remarqué dans la section options ceci :

```
options {
    directory      "/var/named";
    dump-file      "/var/named/data/cache_dump.db";
```

En fait **directory** spécifie le répertoire qui va contenir les fichiers de configuration

Maintenant que nous avons mis sur pied nos zones, nous allons nous rendre dans le répertoire **/var/named/** et créer les fichiers de zones. Ici il s'agit du fichier **aurelien** et **aurelien.rev**

Voici quelques directives que nous pouvons avoir dans les fichiers de zones :

TTL qui indique le temps de vie de la zone en secondes. Cela signifie que

Chaque enregistrement de la zone sera valable durant le temps indiqué par TTL

SOA (star of authority) : elle permet de décrire la zone

IN: the Internet. Définit une classe d'enregistrement qui correspond aux données Internet (IP)

NS (name Server) : désigne un serveur dns de la zone

A pour adresse IP

Cette liste est vraiment tres longue, alors vous allez consulter les manuels pour faire mieux ce que vous voulez. A la fin, je vais mettre mes fichiers avec un peu de commentaire.

Lorsque vous avez bien renseigne vos zones et que, il existe des commandes pour vérifier le fichier **named.conf** et les fichiers de zone

1- Pour **named.conf**, vous vous rendez dans **/etc** et vous faite :

named-checkconf named.conf

2- Pour les fichiers de zones, vous vous rendez dans le repertoire **/var/named** et vous faite

named-checkzone nom_du_fichier_de_zone

Si tout se passe bien, elles ne renverront rien. Vous pouvez maintenant redémarrer le service comme ceci :

```
[root@serveur etc]# service named restart
Arrêt de named : [ OK ]
Démarrage de named : [ OK ]
[root@serveur etc]# █
```

Avant de continuer, nous devons modifier certains fichiers. Il s'agit du fichier **/etc/hosts** et du fichier **/etc/resolv.conf**. Dans ces deux fichiers, nous allons mettre les renseignements comme ceci :

Fichier **/etc/hosts**.

```
192.168.1.4 serveur
127.0.0.1 localhost.localdomain localhost
::1 serveur localhost6.localdomain6 localhost6
192.168.1.4 aurelien.lan
```

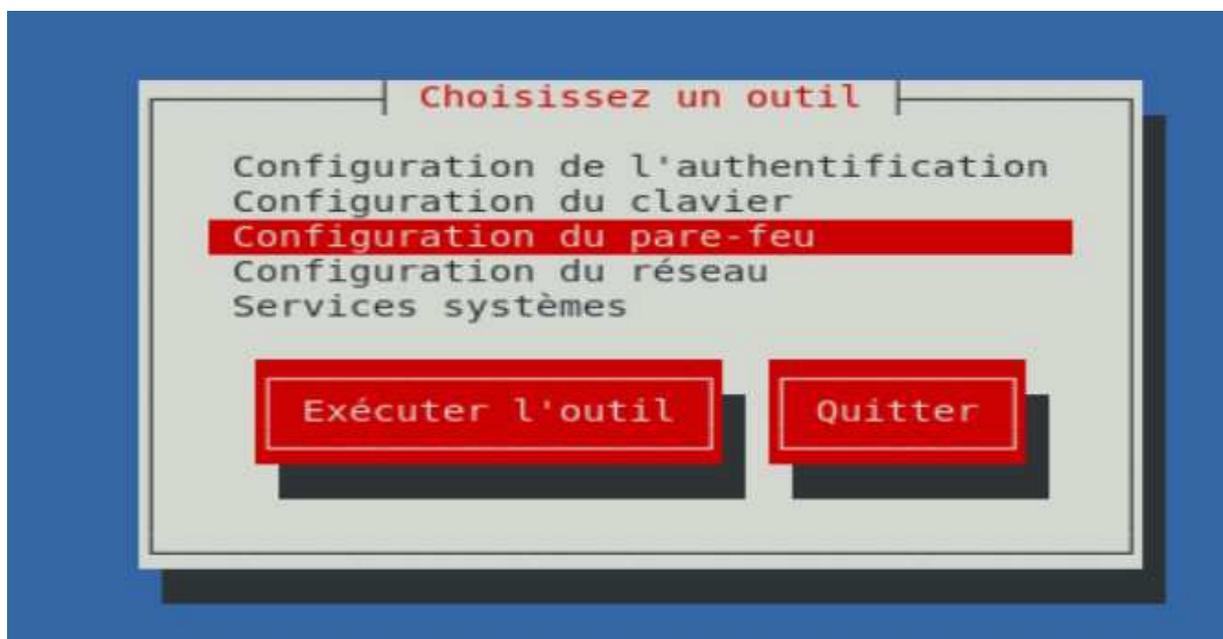
Certaines lignes sont déjà présentes dans le fichier. Vous vous contenterez d'ajouter l'adresse du serveur et le nom **NetBIOS** (nom visible par la commande **hostname**) et le nom du domaine que nous venons de configurer)

Fichier /etc/resolv.conf

```
nameserver 192.168.1.4  
domain aurelien.lan  
search aurelien.lan
```

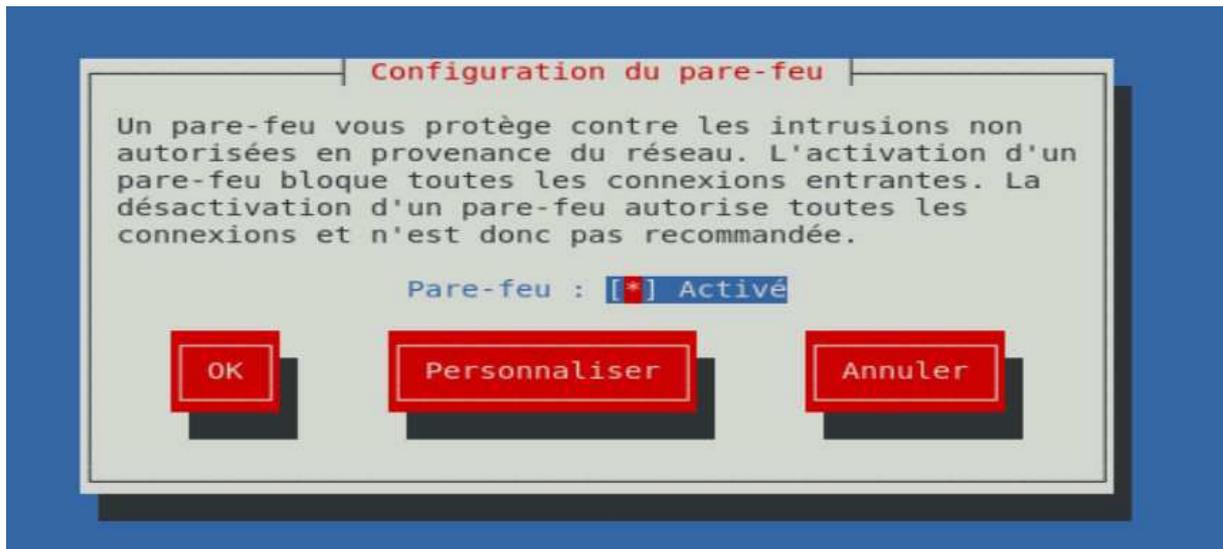
Il reste une chose très importante à faire sur CentOS 6 avant d'utiliser le DNS. Il faut configurer le pare-feu et autoriser le passage pour le DNS. Il existe plusieurs façons de le faire. Je vais vous expliquer la manière avec la commande **setup** :

- 1- Mettez vous en super utilisateur et exécutez la commande **setup**
- 2- Vous obtenez ceci :



- 3- Vous appuyez sur enter lorsque vous avez sélectionné avec les touches directionnelles le directive « Configuration du pare-feu » comme sur la figure précédente

4- Lorsque vous avez validez, vous avez l'écran suivant :



A ce niveau monsieur et madame, nos route se sépare pour la commande **Setup** car vous pouvez choisir de désactivez complètement le pare-feu ou de le personnaliser. A vous de voir

Lorsque vous avez autorisé le passage du DNS, vous pouvez mettre votre serveur en réseau et verifier. Voici les captures de mes tests. Comme je vous avez prévenu, j'utilise trois machines virtuelles. Le serveur sur CentOS, deux clients (Windows xp et Débian).

Client Windows

```
C:\Documents and Settings\ aurelien>ping aurelien.lan
Envoi d'une requête 'ping' sur aurelien.lan [192.168.1.4] avec 32 octets de données :
Réponse de 192.168.1.4 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.4 : octets=32 temps=4 ms TTL=64
Réponse de 192.168.1.4 : octets=32 temps=17 ms TTL=64
Réponse de 192.168.1.4 : octets=32 temps=3 ms TTL=64

Statistiques Ping pour 192.168.1.4:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 17ms, Moyenne = 6ms
```

Client Débian

```
debian:/home/aurelien# ping aurelien.lan
PING aurelien.lan (192.168.1.4) 56(84) bytes of data.
64 bytes from serveur.aurelien.lan (192.168.1.4): icmp_seq=1 ttl=64 time=6.52 ms
64 bytes from serveur.aurelien.lan (192.168.1.4): icmp_seq=2 ttl=64 time=3.68 ms
64 bytes from serveur.aurelien.lan (192.168.1.4): icmp_seq=3 ttl=64 time=2.24 ms
64 bytes from serveur.aurelien.lan (192.168.1.4): icmp_seq=4 ttl=64 time=4.59 ms
^C
--- aurelien.lan ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3016ms
rtt min/avg/max/mdev = 2.245/4.262/6.527/1.552 ms
debian:/home/aurelien#
```

Fichier named.conf

```
options {
    directory           "/var/named";
    dump-file           "/var/named/data/cache_dump.db";
    statistics-file     "/var/named/data/named_stats.txt";
    memstatistics-file  "/var/named/data/named_mem_stats.txt";

    recursion yes;

    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside auto;

    /* Path to ISC DLV key */
    bindkeys-file "/etc/named.iscdlv.key";
};

logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};

zone "." IN {
    type hint;
    file "named.ca";
};

zone "aurelien.lan" {
    type master;
    file "aurelien";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "aurelien.rev";
};

include "/etc/named.rfc1912.zones";
```

Fichier aurelien

```
$ORIGIN aurelien.lan.

$TTL 86400
@      IN      SOA      aurelien.lan.  root.aurelien.lan. (
      3; numero serie
      21600; rafraichissement apres 6 heures
      3600; tenter toutes les 1 heures
      604800; tentative expirant apres une semaine
      86400 ) ; TTL mini d'un jour

@      IN      NS      aurelien.lan.

aurelien.lan.  IN      A      192.168.1.4

www          IN      A      192.168.1.4
ftp          IN      A      192.168.1.4
```

Fichier aurelien.lan

```
$ORIGIN 1.168.192.in-addr.arpa.

$TTL 86400
@      IN      SOA      serveur.aurelien.lan.  root.aurelien.lan. (
      3; numero serie
      21600; rafraichissement apres 6 heures
      3600; tenter toutes les 1 heures
      604800; tentative expirant apres une semaine
      86400 ) ; TTL mini d'un jour

@      IN      NS      aurelien.lan.

4      IN      PTR     serveur.aurelien.lan.
```

Je dois m'arrêter la pour le DNS. Si vous avez des questions ou des suggestions, je vous remercie de les faire aux adresses suivantes :

aurelien-lemen.overblog.com

aurelien_lemen@yahoo.fr

<http://www.lopensource.org>

Je vous conseille aussi de regarder Préparation à la certification LPIC-1(LPI 101 LPI 102) [3 édition] de

Sébastien ROHAUT

Il y'a aussi le guide qui se trouve dans votre système que je vous ai fait mettre au bureau. Il s'agit BIND 9 Administrator Reference Manual