Tutoriel Pour l’installation d’un DNS avec bind9

1 – Installer bind9 pour avoir le service DNS

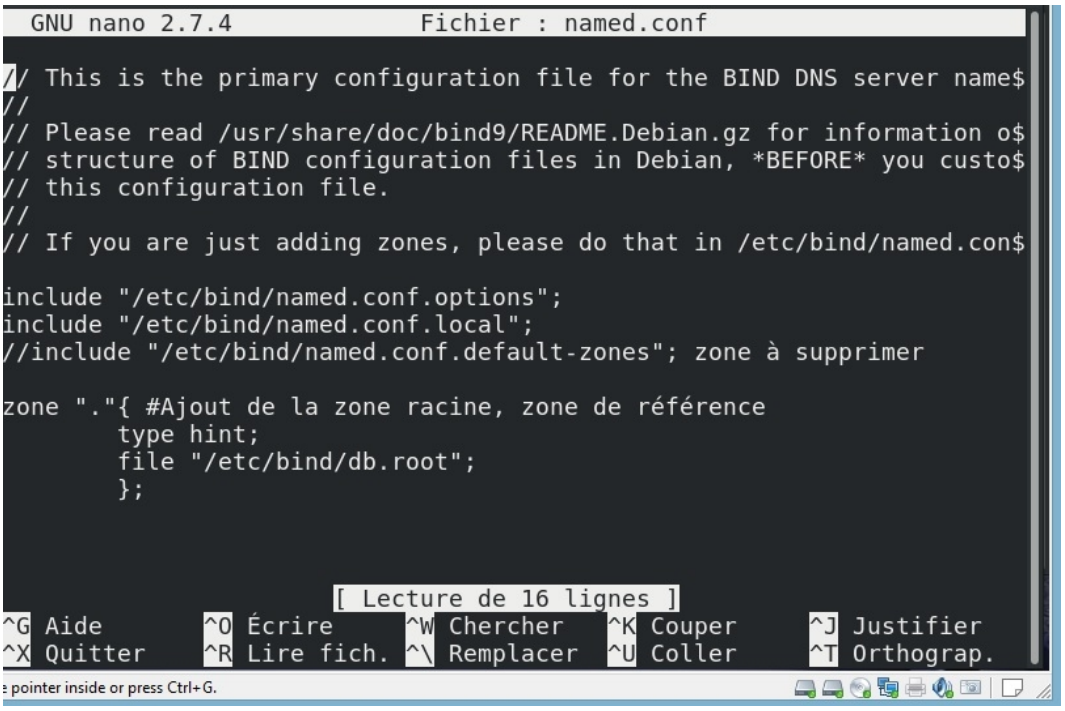
Il vous faudra d’abord passer en root avec la commande su

Puis utiliser apt-get install bind9

2 – Les fichiers de configuration sont dans /etc/bind

Utilisez donc cd /etc/bind/ pour vous y rendre.

3-On commence par named.conf



(Le fichier db.root contient les 13 servs racine)

NB : Il faut bien penser à commenter la ligne qui inclut le fichier named.conf.default-zones. Celui-ci contient les zones par défaut (Racine, broadcast, forward et reverse). Il est désactivé dans le cadre de ce TP, mais d’autres configurations peuvent nécessiter de le conserver actif. Dans debian 9 ce fichier contient la zone racine, mais ça n’as pas toujours été le cas. A vous de vérifier et de voir ce vous voudrez en faire, selon vos besoins, plus tard. En somme la zone racine doit être spécifiée dans l’un des deux fichiers (soit named.conf soit named.conf.default-zones), mais pas dans les deux en même temps.

Le fichier named.conf.options est comme son nom l’indique un fichier d’options modifiable à loisir.

4 –Ensuite je modifie named.conf.local

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "ju.lab" { //Ici je crée ma zone
        type master;
        file "/var/cache/bind/ju.dns";
        };
```

Le type master signifie que c'est ma première zone, et non pas un sous-domaine. Le fichier « /var/cache/bind/ju.dns » est mon choix ; il faudra par la suite le créer à l'endroit spécifié ici.

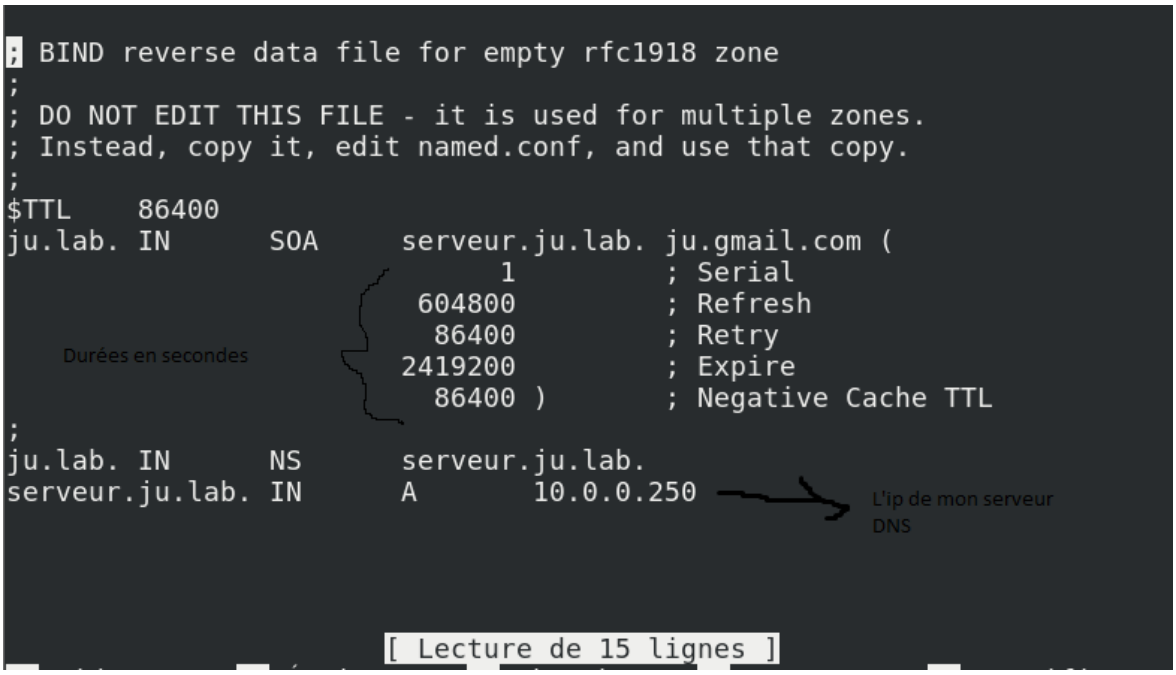
Ju.lab est mon choix, je mets ce que je veux.

5 – Je crée le fichier en question

Cp /etc/bind/db.empty /var/cache/bind/ju.dns ➔ Me permet de prendre db.empty qui est un template (c'est-à-dire un fichier de configuration vierge) afin de le copier dans le dossier choisi var/cache/bind/ et d'aller le modifier par la suite

Je le mets ici dans le dossier /var/ car c'est un fichier amené à changer par la suite, mais si c'est trop compliqué, vous pouvez le mettre ou bon vous semble. Il faut juste préciser le bon chemin dans votre named.conf.local

6 – Modification de mon fichier de dns



Editer le nouveau fichier.

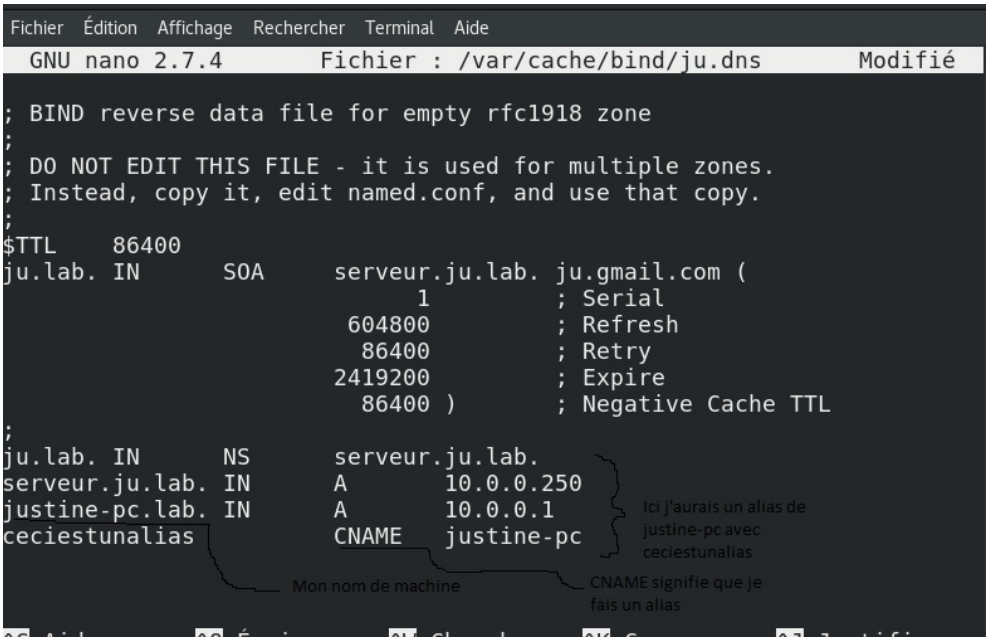
Changer localhost par le Full Qualified Domain Name de votre serveur, en laissant le point "." supplémentaire à la fin. Changer le @ par le nom de votre domaine.

Changer 127.0.0.1 par l'adresse IP du serveur de nom et root.localhost par une adresse mail valide, mais avec un point "." à la place de l'arobase "@". Laisser également le point à la fin.

Créer un enregistrement de type hôte A pour le serveur de nom serveur.ju.lab :

Je peux également y ajouter mon pc par exemple avec son nom (je ne le ferais pas pour la suite du tuto). De plus il faut absolument incrémenter le numéro de série à chaque fois que ce fichier est modifié (l’option serial). On peut ensuite

ajouter des alias comme suit :



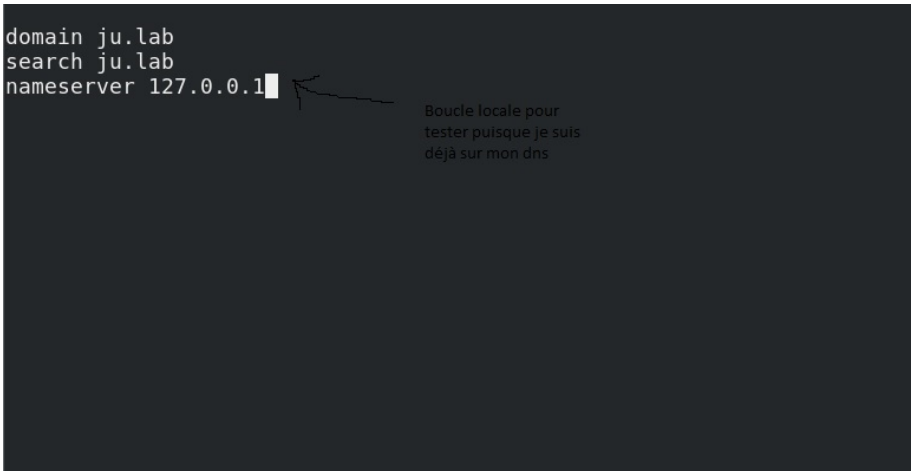
7 – Redémarrage du service

On peut ensuite redémarrer le service avec un systemctl bind9 restart

Il faut ensuite vérifier que la zone est bien chargée avec un journalctl –u bind9 –e

Voir « All Zones Loaded » ne suffit pas, il faut bien vérifier la zone en particulier (ici ju.lab)

8 – test



Nano /etc/resolv.conf pour modifier le fichier resolv.conf

Il s’agit du fichier qui donne l’adresse du serveur dns que j’utilise sur linux.

JE peux ensuite tester par un ping serveur.ju.lab sur la même machine.

SI problème je peux vérifier /etc/nsswitch.conf, qui détermine les sources à partir desquelles obtenir les informations de nom.

9-Zone Inverse

Par la suite je vais ajouter une zone inverse (qui donne une ip à partir d'un nom) dans named.conf.local, sur le même modèle que la zone crée auparavant.

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "ju.lab" {
        type master;
        file "/var/cache/bind/ju.dns";
        };

zone "10.IN-ADDR.ARPA"{
        type master;
        file "/var/cache/bind/reverse.dns";
        };
```

Pour l'adresse de zone c'est l'ip à l'envers suivi de IN-ADDR.ARPA

SI j'avais 192.168.222.0, ca serait 222.168.192.IN-ADDR.ARPA

Je vais créer mon fichier de zone inverse au même endroit que mon fichier de zone (ici dans /var/cache/bind/), pour cela je vais recopier mon fichier de zone normale pour m'en servir de base.

cd /var/cache/bind

cp ju.dns reverse.dns

```
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    86400
10.IN-ADDR.ARPA.        IN      SOA     serveur.ju.lab. ju.gmail.com (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
        IN      NS      serveur.ju.lab.
250.0.0         PTR     serveur.ju.lab.
```

10 parce que je suis sur le réseau 10.0.0.0

Ip à l'envers de mon serv

PTR = pointer

Une fois tout cela fait, je peux relancer le service dns avec systemctl restart bind9. Je peux ensuite lancer un client windows sur le même réseau et tester que ma configuration est bonne avec la commande nslookup

Addendum : Avoir 2 sites, c’est-à-dire des hôtes virtuels

Il faut pour cela que le serveur web (Apache2) et le serveur DNS (bind9) fonctionnent de concert.

Pour ce qui est du serveur apache, voici simplement la configuration utilisée :

```
<VirtualHost *:80>
        ServerName site1.ju.lab
        ServerAdmin aurelienpelletreau@gmail.com
        DocumentRoot /var/www/site1


        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access-site1.log combined

        SSLEngine on

        SSLCertificateFile      /etc/ssl/private/site1.perm


</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet:r default-ssl.conf
```

Ceci est le fichier /etc/apache2/sites-available/001-site1.conf

Il faut que chacun de vos sites ait une adresse (dans servername) qui soit en lien avec votre domaine DNS. Ici Mon domaine DNS s'appelle ju.lab, donc mon site est site1.ju.lab ; c'est tout.

Pour ce qui est du DNS :

```
$TTL    86400
ju.lab. IN      SOA     serveur.ju.lab. aurelienpelletreau@gmail.com. (
                         231020171              ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
ju.lab. IN      NS      serveur.ju.lab.
serveur.ju.lab. IN      A       10.0.0.1
site1.ju.lab.   IN      CNAME   serveur.ju.lab.
site2.ju.lab.   IN      CNAME   serveur.ju.lab.
```

Il s'agit de mon fichier de zone, qui s'appelle ici /var/cache/bind/ju.dns

On peut voir que j’ai ajouté mes 2 sites web (j’ai mis ici leur nom complet pour éviter les erreurs, mais en théorie je pourrais me contenter de site1 et site2), et qu’ils sont tous deux un alias (ce que m’indique le IN CNAME vers mon serveur.ju.lab.

Il faut bien qu’ils redirigent vers le serveur et pas simplement vers le domaine.

*** Plus tôt dans le TP, nous avons utilisé www.site1.fr. Cela ne fonctionnait que grâce à la modification du fichier hosts de mon client windows. Ici le fait d’utiliser un nom logique pour mon site me permet de ne pas avoir à gérer cela et à laisser mon DNS faire tout le boulot. (cela dit si le www vous manque, vous pouvez le mettre, mais alors n’oubliez pas de modifier les fichiers de configuration en accord avec ce nom !).