TP2 : Configurer un serveur DNS

Rabii El Ghorfi

Ce TP a pour but de vous présenter comment installer et configurer un serveur DNS en utilisant l'application *BIND*.
Dans ce TP un cas concret de configuration DNS sera traité, à vous de l'adapter selon vos besoins.

Objectifs :

- Installer un serveur DNS sur un PC serveur GNU/Linux.
- Visiter les principaux fichiers de configuration utiles à DNS.
- Utiliser le service DNS depuis un poste client GNU/Linux, ou Windows.

Introduction

Sur Internet, toutes les machines sont identifiées (et identifiables) par une adresse IP. Cependant, il n'est pas évident de demander à tout-un-chacun de retenir l'adresse IP du serveur web de Google ou plus important encore, du serveur wiki de Ubuntu-fr.

C'est pour cela que l'on a créé les noms de domaines. Les noms de domaine permettent d'identifier un réseau. En ajoutant le nom de la machine, on obtient le nom de l'hôte (hôte se trouvant dans un domaine).

Par exemple, cette page se trouve sur une machine qui est elle-même dans un domaine. Si vous examinez la barre URL de votre navigateur, vous verrez une adresse de ce type :

```
http://doc.ubuntu-fr.org/serveur/bind9
```

La partie qui nous intéresse est **doc.ubuntu-fr.org**. Cette chaîne de caractère signifie que vous vous adressez à la machine **doc** qui se trouve sur le domaine **ubuntu-fr.org**.

Lorsque vous introduisez ce nom d'hôte, il est converti en adresse IP afin de pouvoir demander la page `serveur/bind9` au travers du protocole `http`.

L'acronyme DNS signifie *Domain Name Server*, en français, *serveur de nom de domaine*.

Donc, quand votre machine (à la maison ou au bureau) demande le serveur `doc.ubuntu-fr.org`, il s'adresse tout d'abord aux DNS mondiaux pour savoir quel est la machine qui gère les noms sur le domaine `ubuntu-fr.org`. Imaginons que cette machine se nomme `ns.ubuntu-fr.org`.

Lorsque votre machine sait que `ns.ubuntu-fr.org` gère le nom de domaine `ubuntu-fr.org`, elle interroge le serveur de nom `ns` pour obtenir l'IP de la machine `doc` qui se trouve sur son domaine. A ce moment-là, `ns.ubuntu-fr.org` répond que la machine `doc.ubuntu-fr.org` porte l'adresse IP `212.27.33.233`.

Voilà, comment fonctionne un DNS sans entrer dans les détails. Pour plus d'informations concernant le DNS, je vous renvoie vers Google et Wikipedia.

Pour installer un serveur DNS, nous allons utiliser une application bien connue des administrateurs réseaux : **BIND**.

Installation de BIND

Pour installer *BIND* sur Ubuntu, il n'y a rien de plus simple. Installez les paquets suivants :

- `sudo apt-get install bind9`
- `sudo apt-get install bind9-doc`

Configuration de BIND

Considérons le réseau local suivant :

- Le réseau local est `192.168.251.*` et se nomme `bureau.lan`.
- La machine serveur DNS est aussi le serveur de mail et porte l'IP `192.168.251.202`; elle se nomme `mail2`.
- Il y a 3 autres machines sur le réseau : `192.168.251.200` (nommée `twin1`), `192.168.251.201` (nommée `twin2`) et `192.168.251.205` (nommée `portable`).

Remarque : L'utilisation du TLD (*Top Level Domain*) fictif `.lan` est voulue. En effet, n'utilisez pas un TLD existant comme `.com` ou `.be` sans en être le propriétaire.

Voyons comment configurer le serveur BIND avec ce petit réseau.

Configuration de base du serveur

Le fichier named.conf

La configuration principale de BIND se fait dans le fichier `/etc/bind/named.conf`.

Dans ce fichier, on définit un certain nombre de *zone*. Une *zone* correspond soit à une plage IP d'un réseau ou à un nom de domaine. Les deux zones qui nous intéressent ici sont `192.168.251.*` et `bureau.lan`.

On définit deux zones pour avoir la résolution de nom dans les deux sens. C'est-à-dire que l'on peut obtenir une adresse IP à partir d'un nom d'hôte mais également, que l'on peut obtenir un nom d'hôte à partir d'une adresse IP.

Une zone avec un nom de domaine se définit comme ceci :

```
zone "bureau.lan" {
        type master;
        file "/etc/bind/db.bureau.lan";
};
```

On indique tout d'abord le nom de la zone que l'on connaît avec le mot clé `zone` suivi du nom de domaine (dans notre cas, `"bureau.lan"`. On indique que c'est le DNS maître (en effet, on peut avoir un ou des DNS de backups qui sont aussi appelés des DNS secondaires) en indiquant `type master`. Et enfin, on indique dans quel fichier se trouve les informations de résolution concernant cette zone. En général, on place ces fichiers dans `/etc/bind/` et on préfixe le nom de la zone par `db.`.

Nous définissons également la zone de plage IP pour la résolution inverse. Pour se faire, nous utilisons les mêmes paramètres. Cependant, le nom de la zone s'écrit avec la plage réseau **inversée** suivi de `.in-addr.arpa`. L'entrée de zone pour notre réseau `192.168.251.*` s'écrit comme ceci :

```
zone "251.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192.168.251";
};
```

Nous en avons fini avec le fichier de configuration générale. Voyons maintenant comment définir les noms des machines présentes dans une zone.

Le fichiers zone db.bureau.lan

Comme vous vous en doutez, nous avons un fichier par zone. Les fichiers zones contiennent toutes les entrées comme une table de traduction pour les noms des machines d'une même zone.

Un fichier zone commence toujours par un champ `SOA`, ce champ SOA se compose comme suit :

```
$TTL 3h
@       IN      SOA     ns.bureau.lan. hostmaster.bureau.lan. (
                                2005090201
                                8H
                                2H
                                1W
                                1D )
```

Le symbole `@` désigne la zone décrite par le fichier de configuration (ici, `bureau.lan`). A la place de `@`, vous auriez très bien pu indiquez `bureau.lan.` (*n'oubliez pas le "." à la fin !!!*).

Ensuite, on indique `IN` qui signifie que l'on a affaire à une zone Internet; c'est pour ainsi dire toujours le cas (sauf quelques très rares exceptions). Enfin, toujours sur la première ligne, on indique le serveur DNS qui dispose du fichier zone de référence (important lorsque que l'on a des DNS secondaires) et l'adresse email de la personne responsable de la zone (le premier "." dans le champ d'email est considéré comme un "@").

Dans notre cas, le serveur DNS primaire de la zone est `ns.bureau.lan` et l'adresse email de la personne responsable est `hostmaster@bureau.lan`.

Remarque : Vous avez sans doute noté que le serveur DNS et l'adresse email sont ponctuées par un point ("."). Ce point est **indispensable**. Si vous l'omettez, par défaut, BIND rajoute le nom de la zone et dès lors `ns.bureau.lan.` renvoie `ns.bureau.lan` alors que `ns.bureau.lan` (sans point) renvoie `ns.bureau.lan.bureau.lan`. Il s'agit d'une erreur très fréquente.

Les valeurs qui suivent sont respectivement :

- le numéro de série (souvent on met la date courante suivie d'un numéro d'ordre); `AAAAMMJJxx`.
- le temps de rafraichissement (`refresh`; ici, 8 heures); la valeur recommandée est de 24 heures.
- le temps entre deux essais (`retry`; ici, 2 heures); la valeur recommandée est de 2 heures.
- le temps d'expiration (`expire`; ici, 1 semaine); la valeur recommandée est de 1000 heures.
- la valeur TTL minimum (`minimum`; ici, 1 jour); la valeur recommandée est de 2 jours.

En utilisant les valeurs que j'ai stipulées ci-dessus, tout devrait fonctionner. Pour plus d'informations, je vous renvoie à Google.

Après le champ SOA, on indique le serveur de nom à consulter pour résoudre un nom d'hôte dans le domaine `bureau.lan`. Nous faisons ça avec un champ `NS` de la manière suivante :

```
@       IN      NS      ns.bureau.lan.
```

Ensuite (ceci est facultatif), si vous avez un serveur de mail, vous pouvez indiquer au serveur DNS que les adresses de la forme `*@bureau.lan` sont gérées par un serveur de mail prédéfini; nous le faisons comme ceci :

```
@       IN      MX      10      mail2.bureau.lan.
```

Remarque : La valeur `10` indique la priorité du serveur concerné. En indiquant plusieurs champs `MX` avec des valeurs différentes, vous pouvez indiquer des serveurs de mail secondaires.

Enfin, nous terminons ce fichier zone avec *la table de traduction* des hôtes en adresse IP :

```
ns              IN      A       192.168.251.202
mail2           IN      A       192.168.251.202
twin1           IN      A       192.168.251.200
twin2           IN      A       192.168.251.201
portable        IN      A       192.168.251.205
```

Le fichier zone complet pour `bureau.lan` ressemble à ceci :

```
$TTL 3h
@       IN      SOA     ns.bureau.lan. hostmaster.bureau.lan. (
                                2005090201
                                8H
                                2H
                                1W
                                1D )

@       IN      NS      ns.bureau.lan.

@       IN      MX      10      mail2.bureau.lan.

ns              IN      A       192.168.251.202
mail2           IN      A       192.168.251.202
twin1           IN      A       192.168.251.200
twin2           IN      A       192.168.251.201
portable        IN      A       192.168.251.205
```

Avant de pouvoir utiliser notre serveur DNS, nous allons renseigner la zone pour la plage IP de notre réseau. La zone se décrit vaguement comme la précédente, à la différence près que l'on utilise le mot clé `PTR` au lieu de `A` dans la table de traduction.

Voici le fichier zone pour notre réseau 192.168.251.* d'exemple:

```
$TTL 3h
@       IN      SOA     ns.bureau.lan. hostmaster.bureau.lan. (
                                2005090201
                                8H
                                2H
                                1W
                                1D )

@       IN      NS      ns.bureau.lan.

@       IN      MX      10      mail2.bureau.lan.

202             IN      PTR     ns.bureau.lan.
202             IN      PTR     mail2.bureau.lan.
200             IN      PTR     twin1.bureau.lan.
201             IN      PTR     twin2.bureau.lan.
205             IN      PTR     portable.bureau.lan.
```

Nous pouvons maintenant demander à notre serveur de prendre en compte nos modifications via la commande suivante :

```
sudo /etc/init.d/bind9 reload
```

Nous pouvons maintenant passer à la phase de vérification.

Vérification de la configuration

Pour vérifier la configuration de notre serveur DNS, nous allons lui adresser des requêtes directement via l'utilitaire `nslookup`

```
ols@mail2:/$ nslookup
> server 127.0.0.1
Default server: 127.0.0.1
Address: 127.0.0.1#53
> mail2.bureau.lan
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   mail2.bureau.lan
Address: 192.168.251.202
> 192.168.251.201
Server:         127.0.0.1
Address:        127.0.0.1#53

201.251.168.192.in-addr.arpa    name = twin2.bureau.lan.
> set q=mx
> bureau.lan
Server:         127.0.0.1
Address:        127.0.0.1#53
bureau.lan    mail exchanger = 10 mail2.bureau.lan.
> exit
```

Si tout se déroule normalement, vous pouvez configurer vos clients et utiliser votre serveur DNS.

Configuration avancée

Configuration d'un serveur DNS secondaire

Dans cette section, nous allons envisager la configuration d'un serveur DNS secondaire qui se synchronise avec le serveur DNS principal que nous avons défini ci-dessus.

Le serveur DNS secondaire proprement dit

Pour configurer le serveur secondaire, nous devons simplement indiquer à BIND les zones qu'il doit traiter en mode esclave. Sur base de la configuration ci-dessus, nous configurons le fichier `/etc/bind/named.conf` de serveur DNS secondaire de la manière suivante :

```
zone "bureau.lan" {
        type slave;
        masters {192.168.251.202;} ;
        file "/etc/bind/db.bureau.lan";
};

zone "251.168.192.in-addr.arpa" {
        type slave;
        masters {192.168.251.202;} ;
        file "/etc/bind/db.192.168.251";
};
```

En faisant cela, il est inutile d'indiquer les fichiers zones (fichier `db.`) sur le serveur DNS secondaire. Les fichiers proviendront d'une synchronisation avec le DNS primaire.

Remarque : L'utilisateur faisant fonctionner le serveur DNS doit avoir les droits d'écriture sur les fichiers zones renseignés dans la configuration ci-dessus.

Modification de la configuration du serveur DNS primaire

Nous devons renseigner dans les fichiers zones le deuxième serveur DNS, et pour se faire, on ajoute la ligne suivante au fichier `/etc/bind/db.bureau.lan` :

```
@       IN      NS      ns2.bureau.lan.
```

et nous devons également renseigner l'adresse IP de `ns2.bureau.lan` (n'oubliez pas de mettre à jour le fichier de zone pour le sous-réseau IP également avec le mot clé `PTR` !) :

```
ns2             IN      A       192.168.251.250

250             IN      PTR     ns2.bureau.lan.
```

Après avoir modifié les zones et de ce fait, dévoilé `ns2`, nous pouvons maintenant indiquer au serveur DNS maître que le serveur DNS secondaire peut accéder aux données de zones.

Pour ce faire, les informations concernant les zones qui nous intéressent (dans le fichier `/etc/bind/named.conf` du serveur maître) deviennent ceci :

```
zone "bureau.lan" {
        type master;
        notify yes;
        allow-transfer {192.168.251.250;} ;
        file "/etc/bind/db.bureau.lan";
};

zone "251.168.192.in-addr.arpa" {
        type master;
        notify yes;
        allow-transfer {192.168.251.250;} ;
        file "/etc/bind/db.192.168.251";
};
```

Après toutes ces modifications, demandez au service BIND de recharger la configuration :

```
sudo /etc/init.d/bind9 reload
```

Et surtout, n'hésitez pas à re-tester votre configuration (sur les deux serveurs).

Configuration des clients

La configuration de la résolution de nom pour les machines Linux se fait dans le fichier `/etc/resolv.conf`. Dans ce fichier, vous pouvez ajouter le domaine de recherche via la ligne suivante (en premier dans le fichier) :

```
search bureau.lan
```

Et ensuite, les adresses de vos serveurs de noms (primaire interne, autres internes, puis ceux de votre fournisseur d'accès par exemple) de la manière suivante :

```
nameserver 192.168.251.202
```

L'ordre dans lequel vous indiquez les lignes est important. Si tout se passe bien vous devriez avoir le résultat suivant:

```
search bureau.lan
nameserver 192.168.251.202
nameserver 192.168.251.212
nameserver 193.121.171.135
nameserver 193.74.208.65
```

Linux va essayer de résoudre un nom de la manière suivante (si une étape ne fonctionne pas, il essaye la suivante) :

- recherche du serveur de nom de `bureau.lan` et interrogation de ce serveur.
- interrogation du serveur DNS `192.168.251.202` qui est mon serveur DNS primaire (interne)
- interrogation du serveur DNS `192.168.251.212` qui est mon serveur DNS secondaire (interne)
- interrogation du serveur DNS `193.121.171.135` qui est le serveur DNS primaire de mon provider
- interrogation du serveur DNS `193.74.208.65` qui est le serveur DNS secondaire de mon provider