Administration d'un serveur DNS (Domain Name System) TP N° 12

Pascal Sicard

1 Introduction

Nous allons nous intéresser dans ce TP à la configuration d'un serveur DNS. Pour administrer un serveur DNS, il faut créer plusieurs fichiers de configuration contenant les correspondances nom-adresse de la (ou les) zone gérée, les adresses des serveurs de la zone racine et diverses informations permettant à l'application DNS serveur de faire son travail.

2 Déclaration des zones et localisation des fichiers de données

Un fichier particulier indique quelles zones DNS sont traitées et où se trouvent les fichiers de correspondances (nom/adresse) proprement dit. Sous Unix, c'est le fichier */etc/named.conf*. Sous freeBSD, c'est le fichier */etc/namedb/named.conf*.

Exemple de fichier */etc/named.conf* (sous Unix) :

```
// $FreeBSD: src/etc/namedb/named.conf,v 1.15.2.4 2005/09/10 08:28:34 dougb Exp $
//
// Refer to the named.conf(5) and named(8) man pages, and the documentation
// in /usr/share/doc/bind9 for more details.
//
// If you are going to set up an authoritative server, make sure you
// understand the hairy details of how DNS works.  Even with
// simple mistakes, you can break connectivity for affected parties,
// or cause huge amounts of useless Internet traffic.

options {
directory "/etc/namedb";
pid-file "/var/run/named/pid";
dump-file "/var/dump/named_dump.db";
```

```
statistics-file "/var/stats/named.stats";
};

zone "." {
type hint;
file "named.root";
};

zone "0.0.127.IN-ADDR.ARPA" {
type master;
file "master/localhost.rev";
};

/* An example master zone*/
zone "example.net" {
type master;
file "master/example.net";
};

/* Examples of forward and reverse slave zones*/
zone "example.com" {
type slave;
file "slave/example.com";
masters {
192.168.1.1;
};
};
zone "1.168.192.in-addr.arpa" {
type slave;
file "slave/1.168.192.in-addr.arpa";
masters {
192.168.1.1;
};
};
```

La ligne *directory* indique le répertoire où se trouve les fichiers contenant les données DNS. Les lignes *zone* indiquent pour une zone gérée par le serveur :

- Si le serveur est primaire ou secondaire
- Le nom des fichiers de données correspondant à la zone
- Les adresses des serveurs primaires

Dans l'exemple précédent :

- Les informations concernant les machines de la zone *example.com* sont dans le fichier */etc/namedb/slave/example.com*.
- Ce serveur est un serveur esclave (ou secondaire) pour cette zone.
- L'adresse du serveur maître de cette zone est *192.168.1.1*

Ce serveur gère aussi les adresses de type *192.168.1* et l'adresse *127.0.0* (loopback) pour les interrogations inverses (nom à partir de l'adresse). Le fichier contenant les serveurs de la zone racine est */etc/namedb/named.root*

3 Les fichiers de base de données DNS

Voici en exemple le début du fichier pour la zone *ujf-grenoble.fr*

```
$ORIGIN .
$TTL 86400 ; 1 day
ujf-grenoble.fr IN SOA cubango.ujf-grenoble.fr. fr-ujf-subdom-admin.ujf-grenoble.fr. (
                                    2007011113 ; serial
                                    14400      ; refresh (4 hours)
                                    3600       ; retry (1 hour)
                                    3600000    ; expire (5 weeks 6 days 16 hours)
                                    14400      ; minimum (4 hours)
                                    )
                            NS csjf.ujf-grenoble.fr.
                            NS adminpg.inpg.fr.
                            NS cubango.ujf-grenoble.fr.
                            MX 10 ouveze2.ujf-grenoble.fr.
                            MX 10 ouveze4.ujf-grenoble.fr.
                            MX 30 ouveze1.ujf-grenoble.fr.
                            MX 30 ouveze3.ujf-grenoble.fr.
                            TXT "Universite Joseph Fourier - Grenoble 1"
                            TXT "UJF BP 53  F-38041 GRENOBLE Cedex 9 (France)"
$ORIGIN ujf-grenoble.fr.
100parrains-100classes CNAME awash
15g4                    A 152.77.207.218
                            MX 10 ouveze1
                            MX 10 ouveze2
15ia                    A 152.77.207.210
                            MX 10 ouveze1
                            MX 10 ouveze2
15pc                   A 152.77.207.101
                            MX 10 ouveze1
                            MX 10 ouveze2
....
```

Ces informations viennent du serveur primaire de la zone *ujf-grenoble.fr*

- *SOA* donne des informations sur l'administrateur ; le nom du serveur primaire (ici *cubango*) et l'adresse mail de la personne concernée : *fr-ujf-subdom-admin@ujf-grenoble.fr.*
- Les informations qui suivent le *SOA* (entre parenthèse) indiquent respectivement :
  - *Serial* : Numéro de version : (aammjjVV)
  - *Refresh* : Pour les serveurs secondaires, période de rafraîchissement (entre deux interrogations), en seconde.
  - *Retry* : Pour les serveurs secondaires, en cas d'échec après un transfert de zone, durée minimale avant l'interrogation suivante
  - *Expire* : durée de vie maximale dans un serveur secondaire si un contrôle de serial number n'a pu être fait (au-delà non garantie)
  - *minimum* : durée de conservation d'un enregistrement dans un cache name server

- NS indique les serveurs de la zone. Ici les serveurs *csjf.ujf-grenoble.fr.*, *adminpg.inpg.fr.*, *cubango.ujf-grenoble.fr.* sont des serveurs de la zone *ujf-grenoble.fr.* Le serveur répondra avec ces informations à une requête *ns*.
- *TXT* donne des indications textuelles comme l'adresse postale.
- *$ORIGIN ujf-grenoble.fr.* indique que tout ce qui suit devra être suffixé par *ujf-grenoble.fr.*
- *A* indique pour un nom, l'adresse correspondante. Par exemple la machine de nom *15g4.ujf-grenoble.fr* a comme adresse *152.77.207.218*
- *MX* indique les serveurs de courriers.
- *CNAME* indique le nom canonique. Permet de créer un alias.
- @ indique un nom égal au nom de la zone (auquel est ajouté le point final).
- Les noms sans '.' à la fin sont relatifs au nom de zone de la directive primary/secondary

4 Expérimentations

4.1 Mise en place de la plateforme

Configurez la plateforme suivant la figure 1. Le routeur de sortie est accessible via une prise murale. Utilisez un ***hub*** (et non un switch) pour pouvoir capturer facilement tous les paquets circulant sur le réseau.

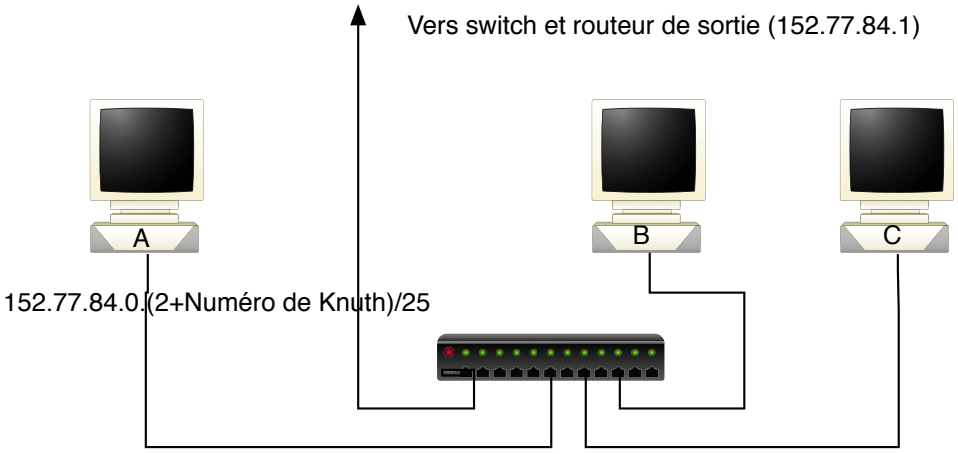

FIGURE 1 – Plateforme

- Pour configurez les machines pour qu'elles puissent accéder à l'extérieur, le plus simple est d'utiliser le script */var/backups/BackToNormal* qui fait le nécessaire. Attention dans ce cas c'est l'interface *em0* qui est configurée.
  Vérifiez que le DNS fonctionne. Si nécessaire modifiez le fichier */etc/resolv.conf*.

- Récupérez les fichiers nécessaires à la configuration du serveur DNS depuis le Moodle de l'UFR sur A :

- *named.conf*
- *named.root*

  On peut aussi utiliser les fichiers se trouvant déjà dans */etc/namedb* si ils n'ont pas été trop endommagé.
- On peut aussi récupérer le fichier *named.root* sur le site *www.internic.net*.

4.2 Serveur DNS sans gestion de zone

- Modifiez le fichier *named.conf* afin que A ne soit serveur d'aucune zone hormis bien sûr celle de la racine (*"."*) (type particulier (*hint*).
  ATTENTION : Vérifiez que les options *listen-on*{*127.0.0.1 ;* } ; et *forwarders* soient désactivées (en commentaire).

- Placer dans le répertoire prévu le fichier *named.root*.

- Placer le fichier précédemment modifié *named.conf* dans le répertoire */etc/namedb/*.

- Configurez A pour qu'il soit lui-même son serveur DNS (fichier */etc/resolv.conf : 127.0.0.1*).

- Lancez une capture de paquets sur le réseau.

- Lancez sur A le démon serveur DNS : *named -g*

- Configurez la machine B en client DNS de telle manière qu'elle interroge A lors de requêtes DNS (fichier */etc/resolv.conf*).

- Observez le réseau lors des commandes suivantes effectuées sur B :
  - *host -t a ns1.nic.fr*
  - *host -t a microsoft.com* deux fois de suite
  - *host 192.134.4.1*

  Rappelez le principe de l'interrogation (descente dans l'arbre DNS depuis la raine) en analysant les paquets que vous avez capturés. On pourra ajouter un filtre dans *wireshark* sur le protocole *udp* et/ou *dns* On pourra sauvegarder les traces de *wireshark* pour pouvoir analyser les paquets à "tête reposée".

- Configurez votre serveur DNS afin qu'il envoie les requêtes de manière récursive à un autre serveur DNS (option *forwarders* {*adresse-serveurDNS*}).
  Vérifiez par des interrogations et des captures que cela se passe bien comme prévu. Votre serveur DNS a-t-il toujours un cache ? Dans quel cas pratique cette option peut elle être utilisée ?

- Tirez des conclusions sur le mode de fonctionnement (récursif / itératif) et sur les caches dans les serveurs et clients DNS. Refaites quelques requêtes DNS bien choisies sur B si nécessaire.

- Analysez le contenu du fichier de statistiques contenu dans le répertoire spécifié par l'option *statistics-file "/var/stats/named.stats"* dans le fichier *named.conf*. Attention, pour que l'enregistrement de ces statistiques soit effectif, il faut au préalable lancez la commande *rndc stats*.

4.3 Serveur DNS primaire

- Nommez l'ensemble des machines A, B et C par des noms de votre choix.
- Modifiez le fichier de configuration du serveur DNS *named.conf* sur A afin qu'il gère les machines de la zone *monentreprise.fr* en tant que maître. Ne pas oublier d'enlever l'option *forwarders* {*adresse-serveurDNS*}).

- Créez un fichier *monentreprise.fr* par recopie d'un fichier d'exemple (*e.ujf-grenoble.fr* récupéré sur le Moodle ou dans un des fichiers d'exemples donnés dans */etc/namedb*). Modifiez-le afin de donner un nom à chacune des machines de *monentreprise.fr* (attention le démon est sensible aux tabulations et autres délicatesses !). On pourra essayer des alias, nom canonique, serveur de mail...

- Arrêtez si nécessaire puis relancez le démon *named* sur A.

- Vérifiez par des interrogations DNS sur B (à l'aide la commande *host* ou par des *ping*) qu'il peut déterminer les noms des machines de la zone *monentreprise.fr*. Observez le réseau lors de ces interrogations.
- Modifiez le fichier de configuration du serveur DNS *named.conf* sur A afin qu'il gère les interrogations inverses de vos machines en tant que maître. (voir en exemple le fichier *236.54.193.in-addr.arpa)*

- Modifiez le fichier de configuration du serveur DNS afin d'ajouter un nom canonique à une de vos machines. Testez.
- Pour que cette nouvelle zone soit visible depuis des machines extérieures à ce réseau que faudrait-il faire ?
  En d'autres termes ; expliquez la procédure à suivre pour créer « pour de vrai » une nouvelle zone dans *fr*. (voir `http://www.afnic.fr/`). Quelles sont les modalités et le prix d'un tel enregistrement ?

4.4 Serveur DNS secondaire

- Modifiez le fichier *named.conf* de telle manière que B puisse devenir serveur DNS secondaire des zones précédemment créées sur A (*monentreprise.fr* et *xx.yy.zz.in-addr.arpa)*).
- Notez le répertoire où les fichiers de base de données DNS seront stockés. Créez ce répertoire si nécessaire.

- Configurez B pour qu'il soit lui-même son serveur DNS (fichier */etc/resolv.conf :*

127.0.0.1).

- Lancez une capture de paquets sur le réseau.
- Lancez sur B le démon serveur DNS : *named -g*

- Résumez ce qu'il s'est passé sur le réseau et à quoi cela a-t-il servi ? Pour comprendre plus facilement, lire les messages donnés à l'écran par le serveur DNS.

- Pourquoi les paquets DNS sont-ils parfois encapsulés par TCP ?

- Vérifiez que les fichiers de base de donnée DNS sont apparus sur B pour les deux zones spécifiées.

- A quoi servent les numéro de série des bases de données ?

- Vérifiez que votre serveur DNS fonctionne sur B et répond à des requêtes concernant les zones *monentreprise.fr* et *xx.yy.zz.in-addr.arpa).*

4.5 Serveur DNS secondaire de zones existantes

- Modifiez le fichier *named.conf* de telle manière que B puisse devenir serveur DNS secondaire des zones : *u-ga.fr*, *ujf-grenoble.fr* et *84.77.152.in-addr.arpa* avec comme serveur primaire : *ns1.u-ga.fr* qui a comme adresse **195.83.24.30**.

- Lancez une capture de paquets sur le réseau.

- Arrêtez et relancez sur B le démon serveur DNS : *named -g* .

- Vérifiez que les fichiers contenant les bases de données ont été récupérés.

- Ces bases de données ne sont pas forcément lisibles. Il est possible de les convertir dans un format texte par la commande *named-compilezone*
  Par exemple *named-compilezone -f raw -F text -o example.text example.net example.raw* convertit en format texte dans le fichier *example.text* la base de donnée concernant la zone *example.net* se trouvant dans le fichier *example.raw*.

- Combien de noms DNS apparaissent dans les bases de données de chaque zone importées ?

- Vérifiez que les noms des machines des salles réseaux (*knuth...*) apparaissent dans la base de donnée de *84.77.152.in-addr.arpa*.

- Vérifiez que votre serveur DNS fonctionne sur B et répond à des requêtes concernant ces nouvelles zones. Essayez *host -l u-ga.fr*

5 Sécurité DNS à l'aide de *DNSSEC*

- Expliquez la méthode de signature des réponses aux requêtes DNS permettant de s'assurer que la réponse vient bien d'un serveur "authentique".
- Donnez un exemple d'enregistrement de zone (fichier named.conf) utilisant ce type de mécanisme.
- Expliquez à l'aide d'une capture d'un échange DNS signée que vous aurez capturé (paquet DNSKEY).
- Un site pour tester l'utilisation de DNSSEC dans une zone donnée :
  `https://dnssec-analyzer.verisignlabs.com/imag.fr`