La résolution des noms

Arnaud Goulut et Ludovic Terrier

Avril 2010

1 Partie 1 : Le DNS côté client

1.1 Le fichier `/etc/resolv.conf`

Pour utiliser le DNS de l'UTT (ie. 193.50.230.240), il faut dans le fichier `/etc/resolv.conf` mettre :

```
nameserver 193.50.230.240
search utt.fr
```

Contenu du fichier resolv.conf

On peut utiliser deux directives dans ce fichier :
- search : ajoute automatiquement ce suffixe lors des résolutions
- domain : définit le domaine auquel appartient la machine

1.2 L'outils dig

Dig peut être utiliser pour effectuer différents types de requêtes.

1.2.1 Directe

Une requête directe avec dig s'obtient avec la commande : `dig flickr.com in A`

```
;; QUESTION SECTION:
;flickr.com.                    IN      A

;; ANSWER SECTION:
flickr.com.             335     IN      A       68.142.214.24

;; AUTHORITY SECTION:
flickr.com.             76681   IN      NS      ns2.yahoo.com.
flickr.com.             76681   IN      NS      ns5.yahoo.com.
flickr.com.             76681   IN      NS      ns3.yahoo.com.
flickr.com.             76681   IN      NS      ns1.yahoo.com.

;; Query time: 60 msec
;; SERVER: 212.27.40.241#53(212.27.40.241)
;; WHEN: Sat May  1 14:43:58 2010
;; MSG SIZE  rcvd: 140
```

Résultat d'une requête directe

1.2.2 Inverse

Une requête inverse avec dig s'obtient avec la commande : `dig -x 193.50.230.240`

```
;; QUESTION SECTION:
;240.230.50.193.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
240.230.50.193.in-addr.arpa. 86400 IN   PTR     pluton.utt.fr.

;; AUTHORITY SECTION:
230.50.193.in-addr.arpa. 86400  IN      NS      pluton.utt.fr.
230.50.193.in-addr.arpa. 86400  IN      NS      orion.utc.fr.

;; Query time: 68 msec
;; SERVER: 212.27.40.241#53(212.27.40.241)
;; WHEN: Sat May  1 14:52:08 2010
;; MSG SIZE  rcvd: 110
```

Contenu d'une requête inverse

1.2.3 Mail exchange

Une requête mail exchange avec dig s'obtient avec la commande : `dig utbm.fr in MX`

```
;; QUESTION SECTION:
;utbm.fr.                       IN      MX

;; ANSWER SECTION:
utbm.fr.                259200  IN      MX      1 serveur2314.utbm.fr.

;; AUTHORITY SECTION:
utbm.fr.                259200  IN      NS      pluton.utt.fr.
utbm.fr.                259200  IN      NS      portail1.utbm.fr.
utbm.fr.                259200  IN      NS      portail2.utbm.fr.
utbm.fr.                259200  IN      NS      portail5.utbm.fr.

;; ADDITIONAL SECTION:
serveur2314.utbm.fr.    259200  IN      A       193.48.231.4
portail1.utbm.fr.       600     IN      A       193.48.246.2
portail2.utbm.fr.       259200  IN      A       193.48.246.11
portail5.utbm.fr.       259200  IN      A       193.48.246.16

;; Query time: 84 msec
;; SERVER: 212.27.40.241#53(212.27.40.241)
;; WHEN: Sat May  1 15:03:15 2010
;; MSG SIZE  rcvd: 211
```

Contenu d'une requête de type Exchange Mail

1.3 L'outil whois

La commande whois permet de récupérer l'ensemble des informations concernant un nom de domaine telles que le propriétaire, qui le gère, les numéros à joindre ou la date d'expiration par exemple. Ci-dessous un exemple avec le domaine `fedoraproject.org` :

```
Domain ID:D101496757-LROR
Domain Name:FEDORAPROJECT.ORG
Created On:24-Sep-2003 10:32:11 UTC
Last Updated On:23-Jul-2009 17:52:39 UTC
Expiration Date:24-Sep-2010 10:32:11 UTC
Sponsoring Registrar:Network Solutions LLC (R63-LROR)
Status:CLIENT TRANSFER PROHIBITED
Registrant ID:41295926-NSI
Registrant Name:Red Hat, Inc.
Registrant Organization:Red Hat, Inc.
Registrant Street1:1801 Varsity Drive
Registrant City:Raleigh
Registrant State/Province:NC
Registrant Postal Code:27606
Registrant Country:US
Registrant Phone:+1.919754370
Registrant FAX:+1.919754370
Registrant Email:domainadmin@redhat.com
Admin ID:41295926-NSI
Admin Name:Red Hat, Inc.
Admin Organization:Red Hat, Inc.
Admin Street1:1801 Varsity Drive
Admin City:Raleigh
Admin State/Province:NC
Admin Postal Code:27606
Admin Country:US
Admin Phone:+1.919754370
Admin FAX:+1.919754370
Admin Email:domainadmin@redhat.com
Tech ID:41434783-NSI
Tech Name:Fedora Project
Tech Street1:Red Hat
Tech Street2:1801 Varsity Drive
Tech City:Raleigh
Tech State/Province:NC
Tech Postal Code:27606
Tech Country:US
Tech Phone:+1.919754370
Tech Email:admin@fedora.redhat.com
Name Server:NS1.FEDORAPROJECT.ORG
Name Server:NS2.FEDORAPROJECT.ORG
DNSSEC:Unsigned
```

Résultat de la commande whois

2 Partie 2 : Mise en œuvre d'un serveur relai

Le serveur

2.1 Installation de Bind9

```
options {
        listen-on port 53 { 192.168.3.129; };
        listen-on-v6 port 53 { ::1; };
        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";
        allow-query     { localhost; 192.168.3.0/24; };
        recursion yes;
        forward first;
        forwarders {
        193.50.230.240 port 53;
        };
};

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

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

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

Contenu du fichier named.conf

2.2 Configuration du resolver

Il suffit de remplacer l'adresse IP de l'ancien DNS présent dans le fichier `/etc/resolv.conf` par celle du serveur faisant office de relai.

2.3 Fonctionnement du relai

No.	Time	Source	Destination	Protocol	Info
2	0.786661	192.168.3.1	192.168.3.129	DNS	Standard query A utbm.fr
3	0.787142	192.168.3.129	193.50.230.240	DNS	Standard query A utbm.fr
4	0.789477	193.50.230.240	192.168.3.129	DNS	Standard query response A 193.48.246.91
5	0.789686	192.168.3.129	192.168.3.1	DNS	Standard query response A 193.48.246.91

FIGURE 1 – Requête DNS via un relai.

3 Partie 3 : Résolution du domaine b3.re12.fr

3.1 Configuration

Pour pouvoir gérer la zone b3.re12.fr il faut effectuer deux opérations :
- ajouter dans le fichier `/etc/named.conf` la gestion de cette zone
- créer le fichier contenant l'ensemble des paramètres de la zone

3.1.1 Modification du fichier `/etc/named.conf`

```
zone "b3.re12.fr" IN {
        type master;
        file "db.b3.re12.fr";
};
```

Lignes à ajouter

3.1.2 Création du fichier `/var/named/b3.re12.fr`

```
$TTL 3h
@       IN      SOA     ns.b3.re12.fr. hostmaster.b3.re12.fr. (
                                2005090202
                                8H
                                2H
                                1W
                                1D )

@       IN      NS      ns.b3.re12.fr.

@       IN      MX   10   mail.b3.re12.fr.

pc-arnaud       IN A 192.168.3.1
pc-ludo         IN A 192.168.3.129
router-ludo     IN A 192.168.3.254
router-arnaud   IN A 192.168.3.126
ns              IN NS 192.168.3.129
mail            IN A 192.168.3.129
```

Ensemble des paramètres de la zone

3.2 La résolution inverse

3.2.1 Modification du fichier `/etc/named.conf`

```
zone "3.168.192.in-addr.arpa" IN {
        type master;
        file "db.3.168.192.in-addr.arpa";
};
```

Ajout de la zone inverse à gérer

3.2.2 Création du fichier `/var/named/db3.inv`

```
$TTL    604800
@       IN      SOA     ns.b3.re12.fr. root.b3.re12.fr.     (
                2010042701 ; Serial (date + incrementation)
                7200       ; Refresh
                3600       ; Retry
                1209600    ; Expire
                604800     ; Negative Cache TTL
                )

A 192.168.3.1
A 192.168.3.129
A 192.168.3.254
A 192.168.3.126
NS 192.168.3.129
A 192.168.3.129

1                   PTR     pc-arnaud
129                 PTR     pc-ludo
254                 PTR     router-ludo
126                 PTR     router-arnaud
```

Paramètres de la zone inverse

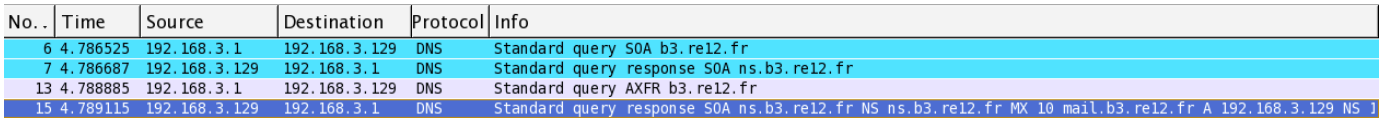
4 Partie 4 : Mise en place d'un serveur secondaire

Dans cette partie, nous avons configurés un second serveur afin qu'il agisse comme un DNS secondaire. Au niveau de la configuration, il suffit d'indiquer dans le fichier `/etc/named.conf` que le contenu de la zone est à récupérer sur le serveur primaire (`ie. master`).

```
zone "b3.re12.fr" IN {
  type slave;
  masters {192.168.3.129;} ;
};
```

Configuration du serveur secondaire

On peut ensuite vérifier le bon fonctionnement avec Wireshark :

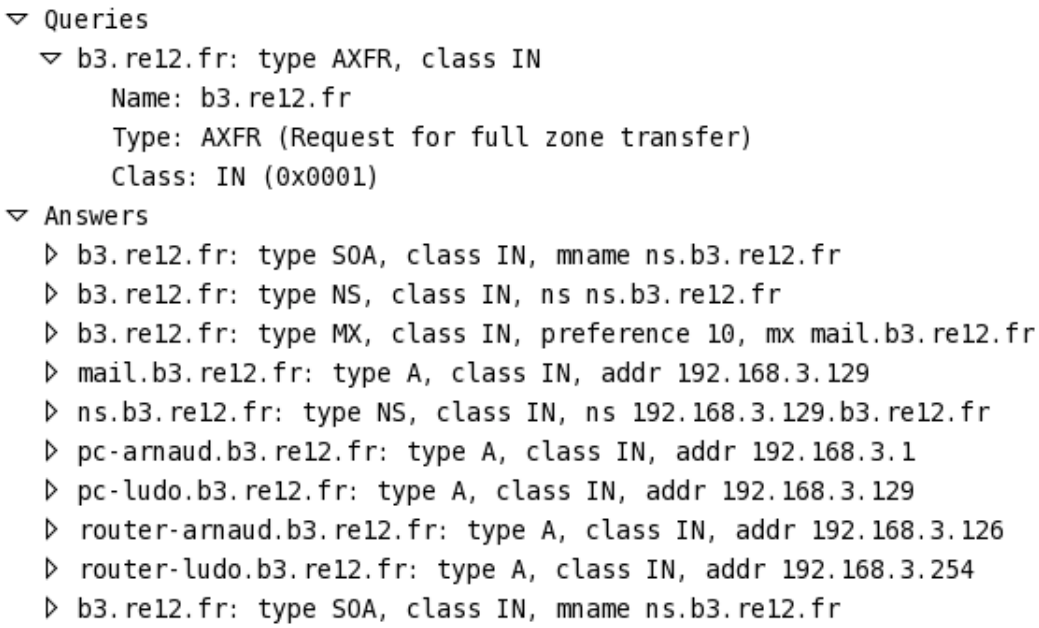


No.	Time	Source	Destination	Protocol	Info
6	4.786525	192.168.3.1	192.168.3.129	DNS	Standard query SOA b3.re12.fr
7	4.786687	192.168.3.129	192.168.3.1	DNS	Standard query response SOA ns.b3.re12.fr
13	4.788885	192.168.3.1	192.168.3.129	DNS	Standard query AXFR b3.re12.fr
15	4.789115	192.168.3.129	192.168.3.1	DNS	Standard query response SOA ns.b3.re12.fr NS ns.b3.re12.fr MX 10 mail.b3.re12.fr A 192.168.3.129 NS 1

FIGURE 2 – Requête de transfert de zone via le serveur primaire.

Dans cette capture, on voit que le serveur secondaire (`192.168.3.1`) effectue une requête de type AXFR pour récupérer les informations de la zone b3.re12.fr.

En regardant plus précisément le contenu de la réponse donnée par le serveur maître (`192.168.3.129`) on voit l'ensemble des enregistrements de la zone b3.re12.fr.



```
▽ Queries
  ▽ b3.re12.fr: type AXFR, class IN
      Name: b3.re12.fr
      Type: AXFR (Request for full zone transfer)
      Class: IN (0x0001)
▽ Answers
  ▷ b3.re12.fr: type SOA, class IN, mname ns.b3.re12.fr
  ▷ b3.re12.fr: type NS, class IN, ns ns.b3.re12.fr
  ▷ b3.re12.fr: type MX, class IN, preference 10, mx mail.b3.re12.fr
  ▷ mail.b3.re12.fr: type A, class IN, addr 192.168.3.129
  ▷ ns.b3.re12.fr: type NS, class IN, ns 192.168.3.129.b3.re12.fr
  ▷ pc-arnaud.b3.re12.fr: type A, class IN, addr 192.168.3.1
  ▷ pc-ludo.b3.re12.fr: type A, class IN, addr 192.168.3.129
  ▷ router-arnaud.b3.re12.fr: type A, class IN, addr 192.168.3.126
  ▷ router-ludo.b3.re12.fr: type A, class IN, addr 192.168.3.254
  ▷ b3.re12.fr: type SOA, class IN, mname ns.b3.re12.fr
```

FIGURE 3 – Qestion et réponse de la requête AXFR.