M3105 : Supervision réseau et application DNS

PAILLASSE 8

Yanis PC droit

Maxime PC gauche

Introduction :

A chaque domaine correspond 2 zones : une zone directe pour la traduction nom → IP et une zone "reverse" pour une traduction IP → nom.
On suppose que l'on possède :

- Le domaine rt.fr
- Les adresses 172.15.0.0/22

D'un point de vue DNS, on possède donc 2 zones :

- La zone directe rt.fr.
- La zone inverse 15.172.in-addr.arpa.

Installation :

Pour faire du DNS nous allons utiliser bind9 donc :

```
#sudo apt update
#sudo apt install bind9
```

Le serveur DNS est maintenant installé, il faut le démarrer :

```
#sudo systemctl named start
```

Le service s'appelle named mais il s'agit bien de paquet bind9.

1 Zone directe (Nom => IP)

Maintenant que notre serveur DNS est installé on va pouvoir commencer à le configurer.
Mais avant il faut savoir ce que l'on veut mettre dans notre serveur DNS.

On commence par découper notre /22 en 4 /24 ce qui donne :

172.15.0.0/22

- 172.15.0.0/24
- 172.15.1.0/24
- 172.15.2.0/24
- 172.15.3.0/24

172.15.0.0/24 pour les serveurs a adresse IP fixe :

- Thor : 172.15.0.1/24 Serveur web
- Odin : 172.15.0.2/24 Serveur mail
- Locki : 172.15.0.3/24 Serveur debian (dépôt de paquet)

172.15.3.0/24 pour les équipements réseau :

- Imprimante : 172.15.3.1/24
- Passerelle : 172.15.3.254/24

Maintenant que l'on a ces informations on va monter un tableau avec champ, classe et valeur qui nous servira à construire notre fichier de zone.

Champ	**Classe**	**Valeur**
@	SOA	ns1.rt.fr.
@	NS	ns1.rt.fr.
@	NS	ns2.rt.fr.
@	MX	mail.rt.fr.
ns1	A	10.4.105.115
ns2	A	10.4.105.116
thor	A	172.15.0.1
odin	A	172.15.0.2
locki	A	172.15.0.3
router	A	172.15.3.254
printer	A	172.15.3.1
mail	A	172.15.0.2
debian	CNAME	locki
www	CNAME	thor

Dans un premier temps on crée un fichier rt.zone dans lequel on va mettre la zone directe
Ce fichier sera déclaré dans le fichier named.conf.local.

@ est une variable qui correspond au nom de la zone donc dans notre cas « rt.fr. »
1D veut dire que la valeur est valable 1 jour
IN veut dire internet (aujourd'hui facultatif)
SOA veut dire Start Of Authaurity
ns1.rt.fr. Indique l'adresse du serveur ayant autorité
hostmaster.rt.fr. Est l'adresse électronique de celui qui gère les DNS (On ne peut pas mettre de @ car c'est une variable)

On remplie donc notre fichier rt.zone de la sorte :

```
$TTL 24h ;

@ 1D IN SOA ns1_        hostmaster.rt.fr (
                        3       ;
                        3H      ;
                        15      ;
                        1w      ;
                        3h      ;
                        )

@       IN      MX      10      mail    ;
@       IN      NS      ns1             ;
@       IN      NS      ns2             ;

ns1     IN      A       172.27.6.120    ;
ns2     IN      A       172.27.6.121    ;

mail    IN      A       172.15.0.2      ;
locki   IN      A       172.15.0.3      ;
thor    IN      A       172.15.0.1      ;
router  IN      A       172.15.3.254    ;
printer IN      A       172.15.3.1      ;
odin    IN      A       172.15.0.2      ;

debian  IN      CNAME   locki           ;
www     IN      CNAME   thor            ;
~
~
```

Contenu du fichier rt.zone

NB : les adresse IP des serveurs ns1 et ns2 ne sont pas les mêmes que pendant la séance car je reprends le TP chez moi mais ça ne change strictement rien.

Maintenant on déclare notre zone dans le fichier named.conf.local tel que :

```
//
// 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 "rt.fr." {
        type master;
        file "/etc/bind/rt.zone";
};
~
```

Contenu du fichier named.conf.local

On n'oublie pas de mettre un point à la fin de rt.fr. et on précise le fichier qui reprend cette zone.

On redémarre bind via :

```
#systemctl named restart
```

Pour vérifier si notre DNS marche on utilise la commande dig en spécifiant notre serveur dns et le nom que l'on veut résoudre. On ajout quelque paramètre afin d'avoir un affichage propre :

```
#dig +noall +question + answer @172.27.6.120 printer.rt.fr
```

```
root@Lofi:/etc/bind# dig +noall +question +answer  @172.27.6.120 printer.rt.fr
;printer.rt.fr.                 IN      A
printer.rt.fr.          86400   IN      A       172.15.3.1
root@Lofi:/etc/bind#
```

Résultat de la commande dig sur notre serveur DNS pour www sur le domaine rt.fr

2 Partage de charge

Pour faire du partage de charge on met pour un même champ, www par exemple, plusieurs adresses IP. On doit donc enlever le CNAME pour thor et remplir rt.zone de la sorte.

```
$TTL 24h ;

@ 1D IN SOA ns1         hostmaster.rt.fr (
                        3       ;
                        3H      ;
                        15      ;
                        1w      ;
                        3h      ;
                        )

@       IN      MX      10      mail    ;
@       IN      NS      ns1             ;
@       IN      NS      ns2             ;

ns1     IN      A       172.27.6.120    ;
ns2     IN      A       172.27.6.121    ;

mail    IN      A       172.15.0.2      ;
locki   IN      A       172.15.0.3      ;
www     IN      A       172.15.0.10     ;
www     IN      A       172.15.0.11     ;
www     IN      A       172.15.0.12     ;
router  IN      A       172.15.3.254    ;
printer IN      A       172.15.3.1      ;
odin    IN      A       172.15.0.2      ;

debian  IN      CNAME   locki           ;
~
~
```

Contenu de rt.zone pour faire du partage de charge

Quand on fait plusieurs dig on voit que les adresses ip ne nous sont pas envoyées dans le même ordre, le partage de charge est donc bien effectif, pour www.rt.fr, le navigateur choisira le premier serveur reçu par le DNS (s'il marche). Comme les IP ne sont pas envoyés dans le même ordre, la charge sera répartie sur les 3 serveurs.

```
Every 2.0s: dig +noall +question +answer @172.27.6.120 www.rt.fr

;www.rt.fr.                     IN      A
www.rt.fr.              86400   IN      A       172.15.0.12
www.rt.fr.              86400   IN      A       172.15.0.10
www.rt.fr.              86400   IN      A       172.15.0.11
```

Exemple d'un dig sur www.rt.fr en utilisant watch (IP dans un certain ordre)

```
Every 2.0s: dig +noall +question +answer @172.27.6.120 www.rt.fr

;www.rt.fr.                     IN      A
www.rt.fr.              86400   IN      A       172.15.0.11
www.rt.fr.              86400   IN      A       172.15.0.12
www.rt.fr.              86400   IN      A       172.15.0.10
```

Autre exemple d'un dig sur www.rt.fr en utilisant watch (IP dans un ordre différent)

3 Zone inverse (IP => Nom)

Pour créer un votre zone inverse on peut s'inspirer de db.127. Elle doit contenir un SOA (le même que la zone directe), un serveur DNS au minimum et un enregistrement PTR pour tous les A de la zone directe. Il faut bien faire attention à mettre les nom absolu car ici le @ est 15.127.in-addr.arpa.

```
;
;       Zone inverse pour 172.15.0.0/22
;
$TTL    604800
@ 1D    IN      SOA     ns1.rt.fr.              hostmaster.rt.fr (
                                1         ; Serial
                           604800         ; Refresh
                            86400         ; Retry
                          2419200         ; Expire
                           604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.rt.fr.      ;
@       IN      NS      ns2.rt.fr.      ;

2.0     IN      PTR     mail.rt.fr.     ;
3.0     IN      PTR     locki.rt.fr.    ;
1.0     IN      PTR     thor.rt.fr.     ;
10.0    IN      PTR     www.rt.fr.      ;
11.0    IN      PTR     www.rt.fr.      ;
12.0    IN      PTR     www.rt.fr.      ;
3.254   IN      PTR     router.rt.fr.   ;
3.1     IN      PTR     printer.rt.fr.  ;
2.0     IN      PTR     odin.rt.fr.     ;
```

Contenu de rtinv.zone

Il ne reste plus qu'à ajouter la zone inverse au fichier named.conf.local

```
zone "rt.fr." {
        type master;
        file "/etc/bind/rt.zone";
};


zone "15.172.in-addr.arpa" {
        type master;
        file "/etc/bind/rtinv.zone";
};
~
```

Les deux zones dans named.conf.local

En haut la zone directe et en bas la zone inverse.

On vérifie que tout marche bien grâce à un dig, en précisant -x pour dire qu'il s'agit d'une adresse IP.

```
root@Lofi:/etc/bind# dig +noall +question +answer  @172.27.6.120 -x 172.15.0.1
;1.0.15.172.in-addr.arpa.       IN      PTR
1.0.15.172.in-addr.arpa. 604800 IN      PTR     thor.rt.fr.
root@Lofi:/etc/bind#
```

Résultat d'un dig vers notre serveur DNS avec une adresse IP

Ça marche.

4 Forwader

Notre serveur DNS ne gère que le domaine rt.fr. Pour les autres domaines, il y a 2 options :

- Soit il est resolver, mais cela demande à ce qu'il ait les droits de faire des requêtes DNS vers les serveurs roots (ou tout autre serveur) ce qui est interdit à l'IUT.
- Soit il est forwarder, c'est à dire qu'il renvoie les requêtes pour les domaines qu'il ne connait pas à un serveur qui agit comme un resolver pour lui.

On va choisir la 2ème option, en mettant comme forwarder un serveur DNS du fichier resolv.conf de votre machine dans named.conf.options.

Donc je trouve l'IP d'un resolveur dans /etc/resolv.conf

```
root@Lofi:/etc# cat resolv.conf
# This file was automatically generated by WSL.
# [network]
# generateResolvConf = false
nameserver 172.27.0.1
```

Contenu de resolv.conf

Je rentre cette IP dans named.conf.options en décommentant les lignes concernées.

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
                172.27.0.1;
        };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        listen-on-v6 { any; };
};
```

Contenu de named.conf.options avec l'IP du resolveur DNS

Je redémarre bind et je teste avec un nom qui n'est pas dans mon domaine.

```
root@Lofi:/etc/bind# dig +noall +question +answer  @172.27.6.120 www.google.com
;www.google.com.                        IN      A
www.google.com.         300     IN      A       142.251.37.164
root@Lofi:/etc/bind# vi named.conf.options
root@Lofi:/etc/bind# dig +noall +question +answer  @172.27.6.120 www.google.com
;www.google.com.                        IN      A
www.google.com.         93      IN      A       142.251.37.164
root@Lofi:/etc/bind#
```

Deux commandes dig d'un nom qui n'est pas dans mon domaine à la suite

Je remarque que la première requête prend du temps car notre serveur demande à un autre qui va demander à d'autres tandis que la second est quasi instantanée car le résultat est stocké dans le cache de notre serveur DNS.