M3105 : Domain Name Service (DNS)

October 18, 2022

Vous devez envoyer votre rapport électronique au format PDF par mail à l'enseignant en fin de séance.

Commandes utiles :

- `systemctl start nom_du_service`
  pour (re-)démarrer un service. A chaque changement du fichier de configuration d'un service, il faut le redémarrer.
- `tail -f /var/log/syslog` pour les logs génériques de la machine. Certains services, comme Apache, demandent à syslog de mettre leur logs dans un fichier/répertoire particulier, par exemple /var/log/apache2.
  Alternativement, vous pouvez utiliser `journalctl -u nom_du_service` qui donne directement le log du service.
- Vérifier les services qui tournent sur la machine et écoutent sur lesquelles :
  `netstat -ltun` (l pour listen → serveur, u/t: UDP+/TCP, n : numérique plutôt que nom, ex: 80 ou HTTP)
- Assigner une adresse IP à une interface d'une machine : `ip address add 192.168.1.1/24 dev eth0`

Créez une machine virtuelle debian et assurez-vous de sa connectivité au réseau. Installez le serveur dns qui s'appelle named et dont le nom de paquet s'appelle bindxx où xx est la version. Pour trouver son nom, faîtes :

```
apt-cache search bind | grep \^bind
```

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, pour ce TP, que vous possédez :

- Le domaine rt.fr
- Les adresses 172.15.0.0/16

D'un point de vue DNS, vous possédez donc 2 zones :

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

1 Zone directe

Créez votre fichier de zone directe. Pour ce faire, modifiez le fichier named.conf.local (inspirez vous de named.conf.default-zones) et indiquez-y les informations pour votre nouvelle zone. Un exemple de fichier de zone est donné en fin de section.
Vous possédez les machines suivantes :

- 3 serveurs ayant les 3 premières adresses : Thor, Odin et Locki
- Thor fait office de serveur web et Locki fait office de serveur debian (dépot local de paquets).
- Odin sera le serveur mail: il devra répondre à **mail.rt.fr** et avoir son enregistrement MX avec la priorité 10.
- Votre machine, qui a une adresse en 10.4.{105,110}.x sera le serveur DNS primaire de cette zone. Il aura pour nom **dns.rt.fr**. Notez que le serveur DNS n'a pas à avoir une adresse dans cette zone.

Quand vous avez écrit votre fichier de zone, redémarrez bind et **regardez les erreurs dans les logs. En effet, bind ne crashe que si aucune zone démarre et comme certaines démarrent toujours, vous ne voyez pas de plantage**.
Pour tester votre serveur vous pouvez utiliser host, dig, nslookup.... Par exemple, avec dig :
`dig @server name type`
où *name* est la question DNS, par exemple www.rt.fr et *type* vaut ANY, A, MX, SOA, etc

```
$TTL    86400 ; 24 hours could have been written as 24h or 1d
; $TTL used for all RRs without explicit TTL value

@  1D IN  SOA ns1.example.com. hostmaster.example.com. (
                                2002022401 ; serial
                                3H ; refresh
                                15 ; retry
                                1w ; expire
                                3h ; nxdomain ttl
                               )
@       IN  NS     ns1.example.com. ; in the domain
@       IN  NS     ns2.smokeyjoe.com. ; second dns external to domain

@       IN  MX  10 mail.example.com. ;  mail serveur with  weight 10

; server host definitions

ns1     IN  A      192.168.0.1  ;name server
www     IN  A      192.168.0.2  ;web server
mail  IN A  192.168.0.3  ;mail  server
ftp     IN  CNAME  www.example.com.  ;ftp server definition

; non server domain hosts
bill    IN  A      192.168.0.4
fred    IN  A      192.168.0.5
```

2 Partage de charge

Testez le « partage de charge » en mettant plusieurs adresses IP à une même machine et en interrogeant ensuite côté client pour voir si cela fonctionne en utilisant watch et dig simultanément. watch permet de répeter une même commande de manière automatique toutes les *x* secondes (2 par défaut).

3 Zone inverse

Créez votre zone inverse en vous inspirant 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 votre zone directe.
Pour tester votre serveur sur la zone inverse :

```
dig @server -x IP
Example
dig @10.1.102.101 -x 172.15.0.1
```

4 Forwader

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

- soit il est *resolver* comme vu en TD, 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 des serveurs DNS de l'université dans le fichier named.conf.options, que vous trouvez dans le fichier resolv.conf de votre machine.
Test:

```
dig @10.1.102.101 www.google.fr
```

5 Section Bonus : Serveur esclave

- Utilisez la seconde machine de la paillasse, installez bind.
- Sur la second machine, mettez vos zones directe et inverse dans named.conf.local, mais en mode *slave*, en mettant l'adresse IP de la machine principale comme maître - voir Figure 1.
- Sur la machine maître, modifiez named.conf.options pour que :
  - le maître accepte le transfert de zone lorsqu'il sera demandé. Il faut ajouter une commande du type **allow-transfer { 203.0.113.1; };**
  - le maître avertisse l'esclave si il y a changement dans la base. Il faut ajouter une commande du type **notify yes;**
- Sur la seconde machine, changez les droits du répertoire /etc/bind de manière à ce que bind puisse créer des fichiers: **chown bind /etc/bind**

Montrez que cela fonctionne en interrogeant l'esclave sur les 2 zones gérées par le maître.

5.1 Transfert de zone

L'enregistrement SOA contient des paramètres (*serial, refresh, expire,....*) qui sont des indications pour le serveur esclave. Trouvez leur signification dans la RFC 1537 `https://www.ietf.org/rfc/rfc1537.txt`. Nous allons comprendre ici quel protocole niveau transport et application est utilisé lors du transfert de zone.

- Démarrez wireshark sur une des machines en mettant un filtre sur les 2 adresses IP des 2 machines
- Modifiez le fichier de zone directe sur le serveur primaire en ajoutant un nouveau serveur IP, Balder.
- Quel protocole niveau couche application est utilisé (facile)?
- Quel protocole niveau couche transport a été utilisé? Justifiez.

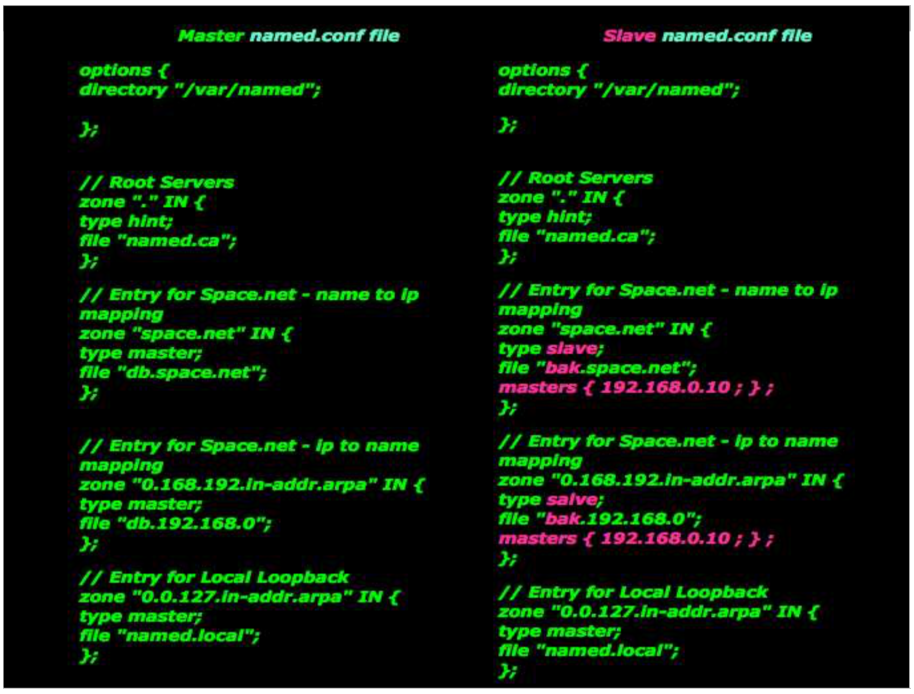

Figure 1: Configuration maître/esclave