TP1 R303 "DNS SERVEUR"

Jean-Marc Pouchoulon

Septembre 2023

1 Objectif du TP

L'objectif de ce TP est d'installer un serveur DNS. Le logiciel utilisé est Bind qui est la solution la plus utilisée dans le domaine. Le TP va nécessiter de travailler avec un container sous DEBIAN. Le domaine à configurer va être in.iutbeziers.fr (le in indiquant qu'il s'agit d'un domaine interne , mais il s'agit d'une convention, on aurait très bien pu prendre un autre sub-domaine) Le livre suivant `http://www.zytrax.com/books/dns/` est une référence accessible en licence CC sur Bind et peut vous être utile.

2 Organisation et Notation du TP

Le TP est à réaliser seul. Vous utiliserez le container registry.iutbeziers.fr/debianiut pour vos installations. Prenez des notes et des copies d'écrans qui vont alimenter votre porte-folio.

L'enseignant validera votre progression. Appelez-le quand:

1. Votre serveur bind fonctionne et résout.
2. La résolution fonctionne sur in.iutbeziers.fr répond avec comme enregistrement le nom de votre container.
3. La zone inverse fonctionne.

3 Installation d'un server DNS Bind

Créez d'abord un réseau net-salle-x (x=numéro de poste) pour votre container (exemple à adapter en fonction de la salle) : On est en salle 213, vous avez le poste (x=2) et c'est votre carte réseau eno1 qui est branchée sur le réseau physique:

```
# creation d'un réseau de type macvlan
docker network create -d macvlan --subnet=10.213.0.0/16 --gateway=10.213.255.254 \
--ip-range=10.213.2.64/26  -o parent=eno1 net-213-2
# listez les réseaux docker sur votre machine
docker network ls
# pour info pour supprimer le réseau net-213-2
# docker network rm  net-213-2
```

Ce réseau macvlan connecte votre container au réseau de la salle sans NAT.

Lancez votre container:

```
# Rafraîchissez votre image
docker pull registry.iutbeziers.fr/debianiut:latest
# lancez le container qui est rattaché rattachez-le au réseau net-213-1
```

```
docker run --network=net-213-1   -v /home/test/bind:/etc/bind --dns=10.255.255.200 \
--name c-213-2-64 --hostname c-213-2-64 -it registry.iutbeziers.fr/debianiut  bash
# vérifiez que vous avez une adresse réseau dans le vlan de la salle depuis le container (.64)
ip a
```

Faire un apt update afin de vérifier que tout fonctionne.

3.1 Installation des packages nécessaires dans chaque container

```
apt-get install bind9 dnsutils
# démarrez le DNS
service named start
```

dnsutils est un paquet qui contient entre autre l'utilitaire dig qui permet d'interroger un DNS et qui est la commande standard de test d'un DNS en milieu professionnel.

3.2 Fichiers de configuration de BIND

Les fichiers de configuration de BIND sont localisés dans l'arborescence /etc/bind/ :

named.conf : fichier de configuration principal du serveur BIND. Il utilise la directive include pour inclure d'autres fichiers de configuration.

```
//This is the primary configuration file for the BIND DNS server named.
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

named.conf.options : fichier dédié aux options du serveur BIND, qui décrit généralement les caractéristiques communes à l'ensemble des zones.

named.conf.local : permet d'ajouter de nouvelles configurations. On utilisera ce fichier par la suite pour la création de notre serveur maître.

named.conf.default-zones : contient la configuration des serveurs root, boucle locale et boucle locale inverse.

Pour bien comprendre l'utilité de ces fichiers, examinons de près leurs contenus :

1. A quoi sert le fichier named.conf.default-zones ? Pour le savoir démarrez le service bind9 et interrogez le serveur via la commande dig sur localhost et 127.0.0.1.

```
//prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/etc/bind/db.root";
};

//be authoritative for the localhost forward and reverse zones, and for
//broadcast zones as per RFC 1912

zone "localhost" {
        type master;
```

```
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};
```

2. A quoi sert le ficher /etc/nsswitch.conf ? Si je fais un ping localhost qui fait la résolution du nom localhost ? quel est le fichier utilisé dans ce cas ?

3.3 Configuration des fichiers de notre zone in.iutbeziers.fr

Modifiez named.conf.local afin d'inclure la zone in.iutbeziers.fr.

```
//
// 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 "in.iutbeziers.fr" {
        type master;
        file "/etc/bind/db.in.iutbeziers.fr";
};
// Reverse Zone de in.iutbeziers.fr
// Adaptez la zone a l'adressage ip de la salle
zone "2.213.10.in-addr.arpa" {
        type master;
        file "/etc/bind/db.10.213.2";
};
```

Autorisez aussi l'accès au cache et au dns via les lignes suivantes dans /etc/bind/named.conf.options:

```
allow-query-cache { any; };
allow-query { any; };
```

Pensez à redémarrer Bind afin que vos modifications soient prises en compte.

3.4 Configuration des adresses de la zone

1. Vous devez maintenant renseigner db.in.iutbeziers.fr et db.X.X.X ou X.X.X est votre réseau Voilà un exemple réel d'une zone existante. Inspirez vous en pour créer votre fichier de zone:

```
;------------ in.ac-montpellier.master -------------
$TTL 1h;
$ORIGIN in.ac-montpellier.fr.
@               IN      SOA     dnsin-01 mail (
```

```
                                2022090901      ; Serial
                                3600          ; Refresh(6h)
                                3600          ; Retry(6h)
                                3600000         ; Expire(41j)
                                86400 )       ; Minimum(24h)
                IN      NS      dnsin-01
                IN      MX 0    smtp

dnsin-01        IN      A       172.29.170.152
smtp            IN      A       172.29.170.153


; ---------- Reverse de la zone 172.29.170 ----------
$TTL 1d;
$ORIGIN 170.29.172.in-addr.arpa.

@               IN      SOA     dnsin-01.in.ac-montpellier.fr. mail.in.ac-montpellier.fr. (
                                2022090901      ;  Serial
                                43200         ; Refresh
                                21600         ; Retry
                                3600000         ; Expire
                                86400 )       ; Minimum
;
; ================  Serveurs du Domaine  ====================
;
                IN      NS      dnsin-01.in.ac-montpellier.fr.
                IN      MX 0    smtp.in.ac-montpellier.fr.

; -------------------------  Machines ------------------------------
152             IN      PTR     dnsin-01.in.ac-montpellier.fr.
153             IN      PTR     smtp.in.ac-montpellier.fr.
```

SOA donne des informations sur l'administrateur ; le nom du serveur primaire (ici dnsin-01.in.ac-montpellier.fr) et l'adresse mail de la personne concernée : admin@ac-montpellier.fr Les informations qui suivent le SOA (entre parenthèses) indiquent respectivement :

- Serial : Numéro de version : (aaaammjjVV)
- Refresh : Pour les serveurs secondaires, c'est la période de rafraîchissement (entre deux interrogations), en seconde.
- Retry : Pour les serveurs secondaires, en cas d'échec après un transfert de zone, c'est la durée minimale avant l'interrogation suivante.
- Expire : Indique dans combien de temps les enregistrements non répliqués perdent leurs validités. (Utilisé par le secondaire)
- minimum : durée de conservation d'un enregistrement dans un cache name server
- NS indique les NAMEs SERVERS de la zone. C'est ce qui sert à résoudre des requêtes de type NS.
- $ORIGIN in.ac-montpellier.fr indique que tout ce qui suit est suffixé par in.ac-montpellier.fr. (sauf les enregistrements qui se terminent par un point)
- MX indique les Mail Exchanger qui sont les serveurs points d'entrée au domaine .
- • A indique pour un nom, l'adresse correspondante. Par exemple la machine de nom.
- CNAME indique le nom canonique. C'est ce qu'on appelle communément un alias.
- @ indique un nom égal au nom de la zone dans le fichier de configuration vu au dessus. Si $ORIGIN est défini alors @ prend le contenu de $ORIGIN

3.5 "Tips and tricks" et vérification

Bind est extrêmement sensible à la syntaxe et peu bavard lors du chargement de ses fichiers de zone.

La commande **named-checkconf -z** permet de vérifier la syntaxe de vos saisies.

Il est souvent judicieux après avoir killé le daemon named ou via **service bind9 stop** de le relancer en interactif via la commande **named -g -c /etc/bind/named.conf** ou dans une version très verbeuse

named -u bind -d9 -g -c /etc/bind/named.conf

N'oubliez pas **dig** qui vous permettra de vérifier que le DNS répond:

```
dig   @127.0.0.1 dnsin-01.in.iutbeziers.fr
dig   @127.0.0.1 -x 10.213.2.2
```

Pensez aussi à reloader votre daemon bind une fois la configuration modifiée.