[Debian] Serveur DNS

Introduction

Un serveur DNS permet la résolution de noms de domaine en adresse IP et inversement sur un réseau.

Dans ce tutoriel nous utiliserons la solution **Bind9** sur une Debian 11 ayant comme adresse IP 10.100.0.86.

Le domaine configuré sera **elie.local**.



Installation

- Installez le paquet bind :

```
apt update && apt install -y bind9
```

- Au cas où un fichier vous souhaiteriez restaurer les fichiers de configuration par défaut, je vous recommande de faire une sauvegarde de ces différents fichiers :

```
cp /etc/bind/named.conf /etc/bind/named.conf.bak
```

```
cp /etc/bind/named.conf.options /etc/bind/named.conf.options.bak
```

```
cp /etc/bind/named.conf.local /etc/bind/named.conf.local.bak
```

Configuration de forwarding

- Éditez le fichier **/etc/bind/named.conf.options** de sorte à obtenir cette configuration (à adapter) :

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

    recursion yes;

    allow-query { 10.100.0.0/24; 127.0.0.1; };

    forwarders {
        1.1.1.1;
        8.8.8.8;
    };

    forward only;

    dnssec-validation auto;
    auth-nxdomain no;
    listen-on-v6 { any; };
};
```

> Vous pouvez choisir les DNS primaires et secondaires vers lesquels la redirection va se produire dans les **forwarders**, ici j'utilise celui de Cloudflare en primaire et celui de Google en secondaire.

Vérifier les configurations

Vous pouvez vérifier la configuration à l'aide de la commande suivante :

```
named-checkconf
```

Redémarrer le service DNS

Une fois que vous avez vérifié que votre configuration DNS est bonne, vous pouvez redémarrer le service named pour prendre en compte les changements :

```
systemctl restart named
```

Configuration de zone (classique)

- Éditez le fichier **/etc/bind/named.conf.local** pour configurer la zone DNS et ajoutez-y ce contenu (à adapter) :

```
// Configuration DNS
zone "elie.local" IN {
type master;
file "db.elie.local";
allow-update { none; };
};

// Configuration Reverse DNS sur un réseau 10.100.0.X
zone "0.100.10.in-addr.arpa" IN {
type master;
file "rev.elie.local";
allow-update { none; };
};
```

Ajout des entrées DNS

À chaque fois que vous voudrez ajouter une entrée DNS, il faudra écrire l'entrée le fichier de configuration DNS et dans le fichier de configuration du reverse DNS.

- Pour commencer, déplacez-vous dans le répertoire **/var/cache/bind/** et créez votre fichier de configuration des enrtées DNS, ici c'est le fichier **db.elie.local** et ajoutez le contenu suivant (à adapter) :

```
$TTL 86400
@ IN SOA debian-dns.elie.local. root.elie.local. (
2022111401
```

```
1w
1d
4w
1w )
@ IN NS debian-dns.elie.local.
debian-dns IN A 10.100.0.86

; SET DNS RECORDS
mail IN A 10.100.0.200
debian-client-1 IN A 10.100.0.201
```

Ici, le serveur DNS ayant pour adresse IP **10.100.0.86** aura le nom **debian-dns.elie.local** qui est enregistré comme entrée de type A.

On peut voir en dessous qu'un serveur de messagerie et un poste client sont aussi enregistrés dans la base sous leurs noms respectifs (à vous de mettre vos propres entrées).

- Ensuite, toujours dans le répertoire **/var/cache/bind/** il faut créer le fichier de configuration du reverse DNS, ici **rev.elie.local** :

```
$TTL 86400
@ IN SOA debian-dns.elie.local. root.elie.local. (
2022111401
1w
1d
4w
1w )
@ IN NS debian-dns.elie.local.
86 IN PTR debian-dns.elie.local

; SET DNS RECORDS
200 IN PTR mail.elie.local
201 IN PTR debian-client-1.elie.local
```

On s'aperçoit que le contenu est similaire à la configuration du DNS avec un différence majeure au niveau des entrées DNS qui sont de type PTR et où on indique la valeur du dernier octet de l'adresse IP pointant vers le nom correspondant.

Par exemple on reconnait l'entrée du serveur de messagerie "***200 IN PTR mail.elie.local***" où **200** correspond au dernier octet de son adresse c'est à dire 10.100.0.**200**.

Modification des droits des fichiers

Afin que Bind puisse exploiter vos fichiers de configuration, les bons droits doivent être mis dessus :

```
chgrp bind /var/cache/bind/*
```

```
chmod 664 /var/cache/bind/*
```

Modification de /etc/resolv.conf

Il faut indiquer au serveur que le serveur DNS correspond désormais à lui-même dans le fichier **/etc/resolv.conf** :

```
echo "nameserver 10.100.0.86" > /etc/resolv.conf
```

Vérifier les configurations

Voici les deux commandes "magiques" qui permettent de vérifier que les configurations sont correctes :

```
named-checkconf
```

L'option -z permet d'être beaucoup plus verbeux quant aux erreurs que vous pouvez rencontrer :

```
named-checkconf -z
```

Redémarrer le service DNS

Une fois que vous avez vérifié que votre configuration DNS est bonne, vous pouvez redémarrer le service named pour prendre en compte les changements :

```
systemctl restart named
```

Configuration de vues (avancé)

Cette approche est particulière puisque contrairement à la configuration en mode zone, nous pourrons définir des entrées et des traitements différents selon **l'interface** par laquelle la requête DNS va entrer.

Le domaine sera toujours **elie.local** .

Pour cet exemple nous aurons un lab avec 2 réseaux :

Réseaux	Adresse réseau
LAN	192.168.0.0/24
DMZ	10.0.0.0/24

Ainsi que 3 machines :

Machine	Adresse interface LAN	Adresse interface DMZ	Rôle
vm-deb01	192.168.0.253	10.0.0.253	Serveur DNS
vm-deb02	192.168.0.1	/	Client LAN
vm-deb03	/	10.0.0.1	Serveur web

- L'ensemble des configurations se fera dans le dossier **/etc/bind** cette fois :

```
cd /etc/bind/
```

- Voici à quoi doit ressembler le fichier **named.conf.options** :

```
acl myclients { 127.0.0.0/8; 192.168.0.0/24; 10.0.0.0/24; };

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

        forwarders { 1.1.1.1; };

        dnssec-validation auto;

        forward only;

        listen-on { 127.0.0.1; 192.168.0.253; 10.0.0.253; };

        allow-transfer { none; };

        allow-query { myclients; };
};
```

- Le fichier **named.conf.zones** :

```
zone "elie.local" {
        type master;
        file "/etc/bind/localzones/db.elie.local";
```

```
};

zone "elie.local" {
        type master;
        file "/etc/bind/localzones/db.elie.local.external";
};
```

- Le fichier **common-zones.conf** :

```
zone "elie.local" {
        type master;
        file "/etc/bind/localzones/db.elie.local";
};

zone "elie.local" {
        type master;
        file "/etc/bind/localzones/db.elie.local.external";
};
```

- Le fichier **named.conf** :

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian 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";

view "local" {
        match-clients { 192.168.0.0/24; };
        allow-query { any; };
        recursion no;
        zone "elie.local" {
                type master;
                file "/etc/bind/localzones/db.elie.local";
```

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

view "external" {
        match-clients { 10.0.0.0/24; };
        allow-query { any; };
        recursion no;
        zone "elie.local" {
                type master;
                file "/etc/bind/localzones/db.elie.local.external";
        };
        include "/etc/bind/named.conf.default-zones";
};
```

- Le fichier **named.conf.internal-zones** :

```
view "internal" {
        # match all except targets defined on [match-clients] on internal section
        match-clients { 127.0.0.0/8; 192.168.0.0/24 };
        # allow all queries
        allow-query { any; };
        # not allow recursive queries
        recursion no;
        zone "elie.local" {
                type master;
                file "/etc/bind/localzones/db.elie.local";
        };
        include "/etc/bind/named.conf.default-zones";
};
```

- Le fichier **named.conf.external-zones** :

```
view "external" {
        # match all except targets defined on [match-clients] on internal section
        match-clients { 10.0.0.0/24; };
        # allow all queries
        allow-query { any; };
        # not allow recursive queries
        recursion no;
```

```
        zone "elie.local" {
                type master;
                file "/etc/bind/localzones/db.elie.local.external";
        };
        include "/etc/bind/named.conf.default-zones";
};
```

- Créer un dossier **localzones** et se déplacer dedans :

```
mkdir localzone && cd localzone
```

- Créer le fichier de la zone interne soit **db.elie.local** :

```
$TTL 86400
@ IN SOA vm-deb01.elie.local. root.elie.local. (
        2022111401
        1w
        1d
        4w
        1w
)
@ IN NS vm-deb01.elie.local.
vm-deb01 IN A 192.168.0.253

; SET DNS RECORDS
vm-deb02 IN A 192.168.0.1
```

- Créer le fichier de la vue externe soit **db.elie.local.externa**l :

```
$TTL 86400
@ IN SOA vm-deb01.elie.local. root.elie.local. (
        2022111402
        1w
        1d
        4w
        1w
)
@ IN NS vm-deb01.elie.local.
vm-deb01 IN A 10.0.0.253

; SET DNS RECORDS
```

```
web-srv IN A 10.0.0.1
```

- Créer le fichier du reverse DNS de la vue interne **rev.elie.local** :

```
$TTL 86400
@ IN SOA vm-deb01.elie.local. root.elie.local. (
        2022111401
        1w
        1d
        4w
        1w
)
@ IN NS vm-deb01.elie.local.
253 IN PTR vm-deb01.elie.local

; SET DNS RECORDS
1 IN PTR vm-deb02.elie.local
```

- Créer le fichier du reverse DNS de la vue externe **rev.elie.local** :

```
$TTL 86400
@ IN SOA vm-deb01.elie.local. root.elie.local. (
        2022111401
        1w
        1d
        4w
        1w
)
@ IN NS vm-deb01.elie.local.
253 IN PTR vm-deb01.elie.local

; SET DNS RECORDS
1 IN PTR web-srv.elie.local
```

Revision #9
Created 2023-09-25 20:24:14 UTC by Elieroc
Updated 2023-11-12 11:41:09 UTC by Elieroc