⏩ Par le temps ? Utilise mon role ansible bind9😄

```
git clone https://github.com/leghort/role-ansible.git
```

Présentation

Qu'est-ce que le DNS ?

Le DNS à pour but de traduire les noms de domaine en adresses IP. Chaque appareil connecté à un réseau dispose d'une adresse IP unique que les autres appareils utilisent afin de le trouver. Grâce aux serveurs DNS, une adresses IP (par exemple, 172.217.19.238 en IPv4) devient www.google.com c'est tout de même plus simple à mémoriser.

Pour mettre en place un tel service dans un réseau privé je vais créé un serveur DNS sous debian11 avec l'outil Bind9.

Installation de bind9

Prérequis

Je commence par installer les paquets `dnsutils` et `bind9`

```
sudo apt-get install dnsutils bind9 -y
```

Bien maintenant je vais pouvoir crée une zone par exemple **cossu.tech**

ℹ️ Uniquement les machines qui ont pour dns principale notre serveur bind 9 utilliseront notre zone.

Déjà il fait change le nom du serveur par le nom à diffuser dans mon cas `cossu.tech`

```
sudo hostnamectl set-hostname cossu.tech
```

Il faut également changer la résolution de nom local pour cela il va falloir connaitre l'addresse ip du serveur j'utiliser la commande

```
ip a
```

> 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
> link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
> inet 127.0.0.1/8 scope host lo
> valid_lft forever preferred_lft forever
> 2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
> link/ether 08:00:27:6d:df:9d brd ff:ff:ff:ff:ff:ff
> inet 192.168.1.24/24 brd 192.168.1.255 scope global dynamic enp0s3
> valid_lft 84835sec preferred_lft 84835sec

192.168.1.24 est donc l'adresse ip du serveur il ne reste plus qu'a la renseigner dans le fichier.

```
sudo nano /etc/hosts
```

> 127.0.0.1 localhost
> 127.0.1.1 cossu.tech
> 192.168.1.24 cossu.tech

Pour effectuer des tests j'indique au serveur de faire appel à lui même "192.168.1.24".

```
sudo nano /etc/resolv.conf
```

ℹ️ Cette modification disparaitra après le redémarrage du serveur.

> domain cossu.tech
> search cossu.tech
> nameserver 192.168.1.25

Je redémarre le service resolved pour appliquer les modifications.

```
sudo systemctl restart systemd-resolved
sudo systemctl enable systemd-resolved
```

Petite vérification

```
systemd-resolve --status
```

> Global
> Protocols: +LLMNR +mDNS -DNSOverTLS DNSSEC=no/unsupported
> resolv.conf mode: foreign
> Current DNS Server: 192.168.1.24
> DNS Servers: 192.168.1.24
> DNS Domain: cossu.tech

Visiblement tout va bien.

Configuration

Je vais modifier la configuration de bind 9 pour lui indiquer que tous les noms qu'il ne connaît pas seront a transféré à une autre serveur dns par exemple 8.8.8.8 (le dns de google).

```
sudo nano /etc/bind/named.conf.options
```

Ce fichier contient les options de configuration du serveur DNS.

```
options {
        directory "/var/cache/bind";
  forwarders {
            8.8.8.8;
        };
        dnssec-validation auto;
  listen-on-v6 { any; };
};
```

Dans un autre fichier je déclare les noms de domaines et le chemin vers un fichier qui servira de "base de données".

ℹ️ Les infos `in-addr.arpa` sont à modifier en fonction du réseau, je suis dans un réseau `192.168.1.0/24`

```
sudo nano /etc/bind/named.conf.local
```

```
zone "cossu.tech" {
  type master;
  file "/etc/bind/db.cossu.tech";
};

zone "1.168.192.in-addr.arpa" {
  type master;
  file "/etc/bind/db.1.168.192.in-addr.arpa";
};
```

Création des bases

Allez c'est partie pour créer un fichier "base de données" qui référence les associations ip / nom.

```
sudo nano /etc/bind/db.cossu.tech
```

```
$TTL 604800
$ORIGIN cossu.tech.
@     IN     SOA     dns.cossu.tech. admin.cossu.tech (
          20221703    ; Numero de serie AnneMoisJour
          604800      ; Temps de rafraichissement
          86400       ; Temps entre les essais
          2419200     ; Temps expiration
          604800 )    ; Valeur TTL minimum
@     IN NS dns.cossu.tech.

dns               IN A 192.168.1.24
linux             IN A 192.168.1.14
linuxPortable         IN A 192.168.1.18
win10             IN A 192.168.1.45
```

Maintenant il faut s'assurer qu'il n'y a pas d'erreur dans les fichiers *db.cossu.tech*

```
sudo named-checkzone cossu.tech /etc/bind/db.cossu.tech
```

> zone cossu.dev/IN: loaded serial 20221703
> OK

C'est OK donc je passe à la configuration de la zone inverse qui permet d'obtenir un nom à partir d'une adresse ip.

```
sudo nano /etc/bind/db.1.168.192.in-addr.arpa
```

```
$TTL    604800
@       IN      SOA     dns.cossu.tech. admin.cossu.tech (
                        20221703    ; Numero de serie AnneMoisJour
                        604800      ; Temps de rafraichissement
                        86400       ; Temps entre les essais
                        2419200     ; Temps expiration
                        604800 )    ; Valeur TTL minimum

@       IN      NS      dns.cossu.tech.
24      IN      PTR     dns.cossu.tech.
14      IN      PTR     linux.cossu.tech.
18      IN      PTR     linuxPortable.cossu.tech.
45      IN      PTR     win10.cossu.tech.
```

Je vérifie la syntaxe du fichier *db.1.168.192.in-addr.arpa*

```
sudo named-checkzone 1.168.192.in-addr.arpa /etc/bind/db.1.168.192.in-addr.arpa
```

> zone 1.168.192.in-addr.arpa/IN: loaded serial 20221703
> OK

Tout va bien, il est temps de redémarrer le service bind9

```
sudo systemctl restart bind9
```

Le moment fatidique est arrivé, voir si la résolution de nom fonctionne. Pour cela la commande *nslookup* est un allié de choix.

```
nslookup linux.cossu.tech
```

> Server: 192.168.1.24
> Address: 192.168.1.24#53
>
> Name: linux.cossu.tech
> Address: 192.168.1.14

Le serveur dns 192.168.1.24 dit que le nom `linux.cossu.tech` est égale à l'adresse `192.168.1.14`, ça fonctionne ! Aller au tout de la zone inverse

```
nslookup 192.168.1.14
```

> 14.1.168.192.in-addr.arpa name = linux.cossu.tech.

Nslookup dit que 192.168.1.14 c'est le nom `linux.cossu.dev` ! Le serveur change les noms en ip et inversement. 🤩

📝https://www.cloudflare.com/fr-fr/learning/dns/what-is-dns/
📝https://wiki.csnu.org/index.php/Installation_et_configuration_de_bind9
📝https://www.isc.org/bind/
📝https://wiki.debian.org/fr/Bind9