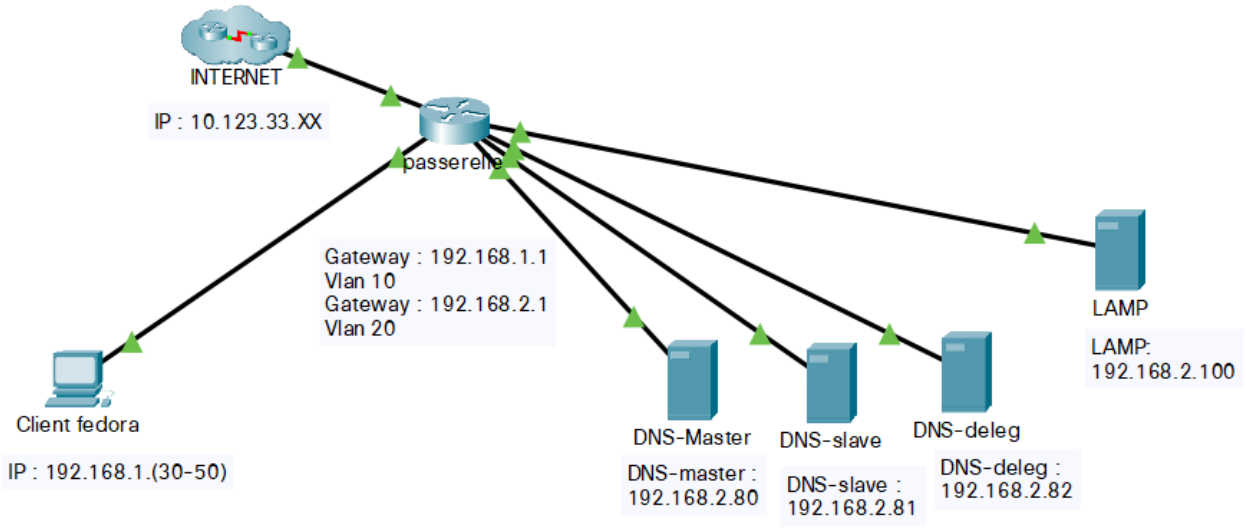
Samson Lucas

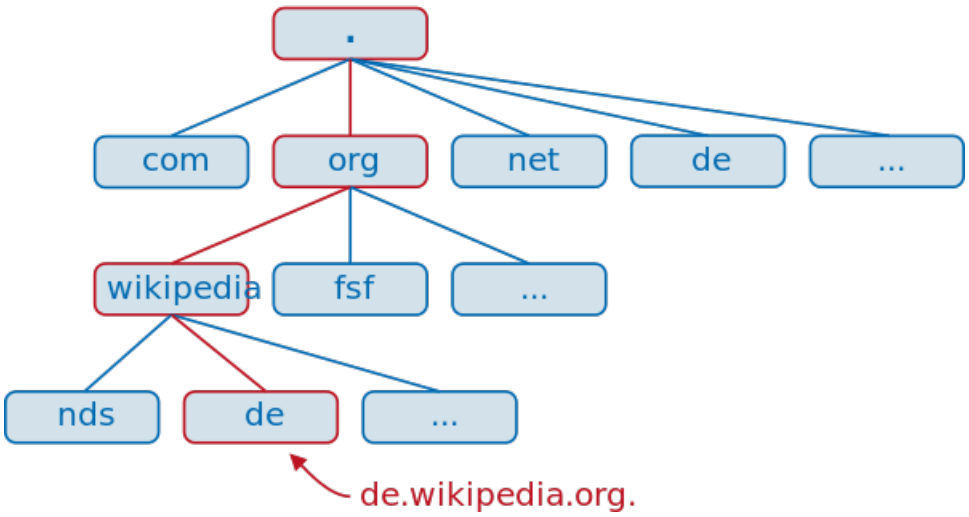
Doc DNS Slave / délégation

Infrastructure réseau :



DNS (Domain Name System)
est un service informatique qui résout les noms de domaine Internet en adresse IP Les équipements connectés à un réseau IP, comme Internet, possèdent une adresse IP qui les identifie sur le réseau. Pour faciliter l'accès aux hôtes sur un réseau IP, un mécanisme a été mis en place pour associer un nom à une adresse IP. Ce nom, plus simple à retenir, est appelé « nom de domaine ». *Résoudre un nom de domaine* consiste à trouver l'adresse IP qui lui est associée.

Hiérarchisation du DNS
Le système des noms de domaine consiste en une hiérarchie dont le sommet est appelé la *racine*. On représente cette dernière par un point. Dans un domaine, on peut créer un ou plusieurs sous-domaines ainsi qu'une *délégation* pour ceux-ci, c'est-à-dire une indication que les informations relatives à ce sous-domaine sont enregistrées sur un autre serveur. Ces sous-domaines peuvent à leur tour déléguer des sous-domaines vers d'autres serveurs.



Un serveur DNS master est un serveur DNS autorise les zones gérées par lui-même dans son propre domaine.

DNS Slave :

Un serveur DNS Slave est un serveur DNS qui réplique les zones gérées par le serveur maître.
Il peut assurer la disponibilité du service en cas de panne du serveur maître.

Mise en place d'un serveur Slave
Pour mettre en place un serveur slave il faut posséder un serveur DNS Master se trouvant dans le même réseau.

Avant de mettre en place le serveur DNS slave il faut modifier le serveur DNS Master dans le but d'autorise le transfert de zone du DNS Master au Slave

Pour autoriser les transferts de zone du DNS Master il faut aller dans le fichier */etc/bind/named.conf.local* en ajoutant dans les zones :

```
 GNU nano 3.2                                    named.conf.local

//
// 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 "lucas.tardi" {
        type master;
        file "/etc/bind/db.lucas.tardi";
        notify yes;
        allow-transfer {192.168.2.81; };
        forwarders {};

};

zone "2.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.2.168.192.in-addr.arpa";
        notify yes;
        allow-transfer {192.168.2.81; };
        forwarders {};
};
```

allow-transfer { x.x.x.x;} ;

notify yes ;

allow-transfer permet d'autoriser le transfert de zone sur une autre DNS via sont adresse IP (x.x.x.x) adresse IP du serveur slave.

Notify Permets d'indiquer dans les logs du serveur DNS Master a quel serveur DNS A-t-il fait un transfert.

Ensuite il faut ajouter le nom de domaine du serveur Slave dans la zone du DNS Master.
Dans le fichier /*etc*/bind/[fichier_de_la_zone]

```
 GNU nano 3.2                                    db.lucas.tardi

$TTL 3600
$ORIGIN lucas.tardi.

@       IN SOA debian.lucas.tardi. root.lucas.tardi. (
        2022111801;
        3h;
        1h;
        1w;
        1h);

@       IN NS  debian.lucas.tardi.
@       IN NS DNSlave.lucas.tardi.


debian                  IN A 192.168.2.80
DNSlave                 IN A 192.168.2.81
pigeon                  IN A 192.168.2.100

enclume         IN CNAME pigeon
glpi            IN CNAME pigeon

deleg                   IN NS debiandeleg.deleg.lucas.tardi.
debiandeleg.deleg       IN A 192.168.2.82
```

@ IN NS
nom_du_serveur_DNS_slave.domaine.
Domaine_de_deuxieme_niveau.

nonmduserveur IN A x.x.x.x
(Adresse IP du serveur DNS slave)

Installation d’un serveur DNS Slave

L’installation d’un serveur DNS slave ce fait de la même façon qu’un serveur DNS master via la solution Bind9 sur Linux.

Récapitulatif :

installation de bind9 sur Debian 10.4

```
sudo apt installer bind9 bind-utils bins-host bind-doc
```

configurer le DNS en ipv4 dans /*etc*/default/bind9 en ajoutant

```
OPTIONS= «  -4 -u bind »
```

voir le statue du service

```
systemclt status bind9
```

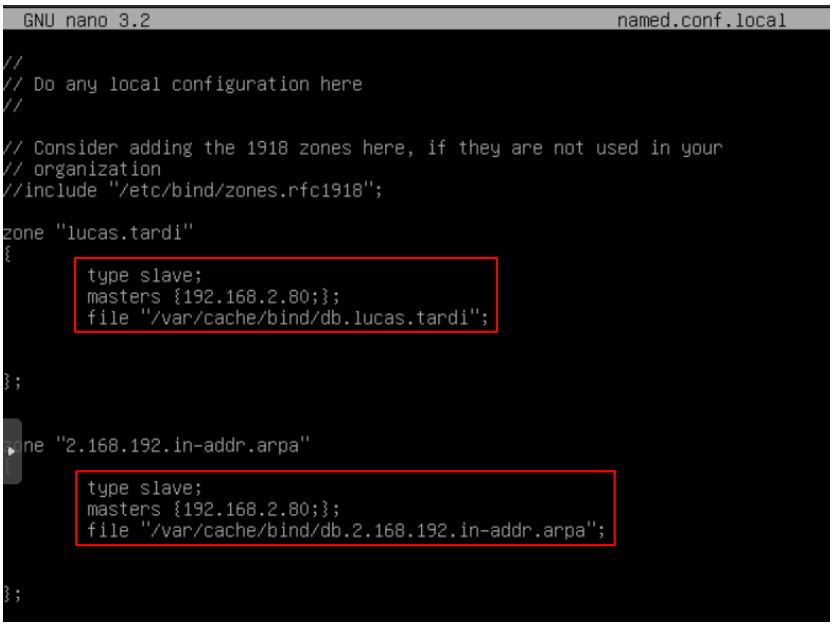
redémarrer le service DNS bind9

```
systemctl restart bind9
```

activer le service bind9

```
systemctl enable bind9
```

après avoir installé le serveur DNS via bind9 il faut configurer les zones dans le fichier. */etc/bind/named.conf.local* dans le but qu’il récupére les fichier de zone du DNS master.



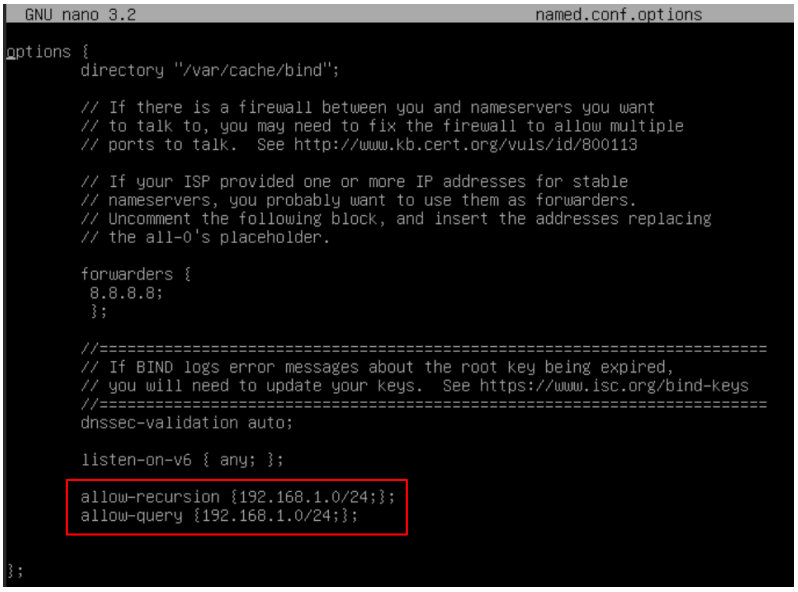

```
Type slave ;
masters { x.x.x.x ;} ;
file
« /var/cache/bind/[nomdufichier
delazone] » ;
```

type slave ; permet de configurer le serveur en DNS slave.
Master {x.x.x.x ;} ;
indique le serveur master de la zone via sont adresse IP.
File « permet d’indiquer l’emplacement du ficher de cache du serveur DNS.

après avoir configurer le ficher **named.conf.local.**
il faut autoriser le serveur DNS slave à interagir avec le réseau 192.168.1.0 (réseau client) via les ACL puis indiquer dans la direction l'emplacement du ficher de cache du serveur DNS.

ACL :
allow-recusion {xxx.xxx.xxx.xxx;} ;
allow-query {xxx.xxx.xxx.xxx;} ;

direction :
directory «/var/cache/bind » ;



après avoir configuré le serveur DNS slave

Il faut retourner sur le serveur DNS master pour qu'il ne réponde plus aucun client.

Pour cela il faut aller dans le fichier named.conf.options
dans */etc/bind/named.conf.options*

puis de retirer l'adresse (IP du réseau client) dans allow-recursion et dans allow-query ;

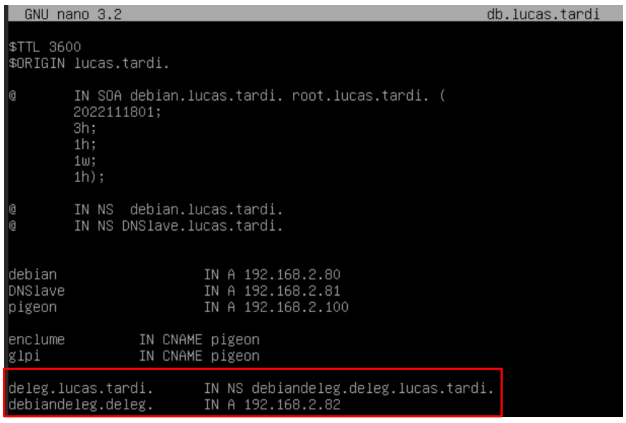
DNS de Délégation :

un serveur de délégation est un serveur DNS qui gérer la gestion d'un sous-domaine l'avantage est la répartition des charges.

Mise en place d'un serveur de délégation
pour mettre en place un serveur de délégation il faut de nouveau installer bind9 sur un nouveau serveur.

Avant de configurer le serveur **DNS deleg** il faut aller sur le **DNS master** dans le but d'attribuer le sous-domaine.

pour attribuer le sous-domaine sur le **DNS master** il faut aller dans le fichier de la zone
dans */etc/bind/[fichier_de_la_zone]* :



Nom_sous_domaine.domaine.Domaine_2éme_niveau. IN NS nom_machine.sous_domaine.domaine.Domaine_2éme_niveau.

nom_de_la_machine.Nom_sous_domaine.
IN A x.x.x.x (adresses du DNS deleg)

Ensuite il faut se rendre sur le fichier named.conf.local (/etc/bind/named.conf.options)
sur le DNS master pour ajouter une ligne dans la configuration des zones

```
 GNU nano 3.2                                    named.conf.local

//
// 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 "lucas.tardi" {
        type master;
        file "/etc/bind/db.lucas.tardi";
        notify yes;
        allow-transfer {192.168.2.81; };
        forwarders {};

};

zone "2.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.2.168.192.in-addr.arpa";
        notify yes;
        allow-transfer {192.168.2.81; };
        forwarders {};
};
```

Forwarders {};

mettre « fowarders {}; » dans la zone permet de forcer le serveur DNS master a regarder dans sont fichier de zone le sous-domaine.

Configuration du serveur DNS deleg

la configuration du serveur DNS deleg ce fait de la même façon que le DNS Master en ajoutant le sous-domaine dans les fichiers de zone.

Dans :

- */etc/bind/*[fichier*_de_la_zone]*
- */etc/bind/*[fichier*_de_la_zone] (reverse)*
- */etc/bind/*named.conf.local

```
 GNU nano 3.2                                    db.deleg.lucas.tardi

$TTL 3600
$ORIGIN deleg.lucas.tardi.

@       IN SOA debiandeleg.deleg.lucas.tardi. root.deleg.lucas.tardi. (
        20221801;
        3h;
        1h;
        1w;
        1h);

@       IN NS  debiandeleg.deleg.lucas.tardi.
@       IN A   192.168.2.82

debiandeleg             IN A 192.168.2.82
test                    IN A 192.168.2.90
```

```
 GNU nano 3.2                                    db.deleg.2.168.192.in-addr.arpa

$TTL 3600
$ORIGIN deleg.2.168.192.in-addr.arpa.
@       IN SOA debiandeleg.deleg.lucas.tardi. root.deleg.lucas.tardi. (
        20221801;
        3h;
        1h;
        1w;
        1h);

@       IN NS   debiandeleg.deleg.lucas.tardi.

82      IN PTR  debiandeleg.deleg.lucas.tardi.
90      IN PTR  test.deleg.lucas.tardi.
```

```
 GNU nano 3.2                                    named.conf.local

//
// 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"deleg.lucas.tardi"
{
        type master;
        file "/etc/bind/db.deleg.lucas.tardi";
};

zone "deleg.2.168.192.in-addr.arpa"
{
        type master;
        file "/etc/bind/db.deleg.2.168.192.in-addr.arpa";
};
```

pour finir il faut autoriser via les ACL dans /*etc*/bind/named.conf.options
le réseau client est le réseau DNS dans le but que le serveur deleg communique avec les autres DNS.

```
        dnssec-validation auto;

        listen-on-v6 { any; };

        version "not currently available";

        recursion yes;

        allow-recursion {192.168.1.0/24; 192.168.2.0/24;};
        allow-query {192.168.1.0/24; 192.168.2.0/24;};
};
```