

TC4 -M2 / DNS

1) Définir le rôle d'un serveur DNS

DNS (Domain Name System) le rôle d'un DNS est de lier un adresse IP a un nom de domaine.

2) Expliciter le fonctionnement d'un serveur DNS. Quelques éléments à considérer.

le DNS comme un annuaire téléphonique, mais au lieu de faire correspondre les noms des personnes avec leur adresse postale, cet annuaire fait correspondre des noms d'ordinateurs avec des adresses IP. Le DNS est plutôt organisé en annuaires plus petits, appelés domaines.

Tout ordinateur voulant connaître un numéro ou un nom peut interroger son serveur DNS.

Lorsque celui-ci a besoin d'un enregistrement, il sait comment interroger d'autres serveurs DNS

(en émettant une requête). Lorsqu'un serveur DNS interroge d'autres serveurs DNS, il émet une requête « en amont ».

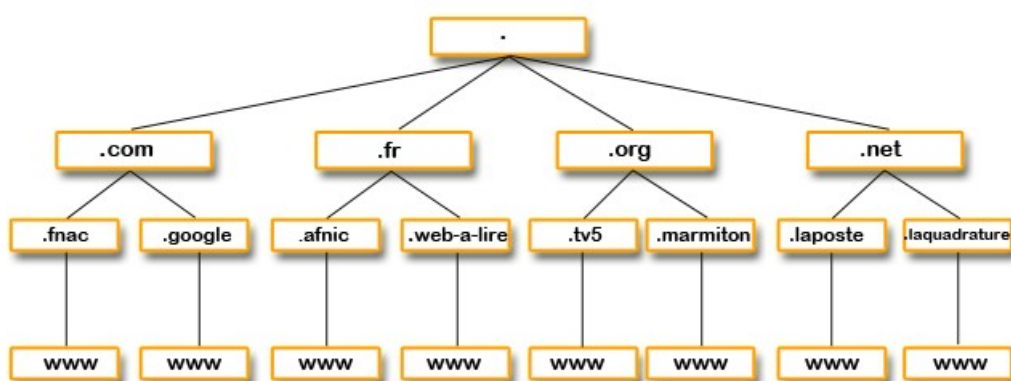
Le DNS utilise un processus particulier. Avant tout l'utilisateur va faire suivre sa requête de résolution à un résolveur distant, qui est souvent par défaut le résolveur du FAI concerné. Par exemple pour `www.wikipedia.fr`, le résolveur va alors entamer la procédure suivante :

Demande l'adresse du TLD « .fr » à l'un des serveurs racine

Demande l'adresse du serveur « wikipedia.fr » au serveur .fr

Demande l'enregistrement « www » au serveur wikipedia.fr

Le résolveur envoie finalement la réponse à l'utilisateur qui peut désormais interroger son serveur web.



Vulnérabilités

DNS n'est pas sur (RFC 3833), les principaux problèmes connus sont :

Le Cache Poisonning

Les attaques de type Denial of Service

Le Name Chaining

L'interception de paquets

Le brute force du champ Identification

Modèle :

Ports utilisés : port 53 protocole UDP

Méthodes d'accès :

Sécurité : Protocole DNSSEC DOH DoT

Nom de domaine (FQDN) : Fully qualified domain name

Reverse : Reverse DNS (rDNS) désigne une requête DNS permettant de retourner le nom de domaine et le nom d'hôte d'une adresse IP.

Cache : stockage d'adresse l'IP sur une machine ou un serveur, ce qui accélère l'accès.

3) Lister les éventuels problèmes de sécurité lié à ce service.

4) Choisir un serveur DNS et justifier ce choix.

5) Quel est l'intérêt de mettre en place un serveur DNS dans un réseau d'entreprise ?

Source :

<https://www.ionos.fr/digitalguide/serveur/know-how/reverse-dns/>

<http://igm.univ-mlv.fr/~dr/XPOSE2014/DNSSEC/dns.html>

<https://www.titanhq.fr/blog/comment-dns-aider-nuire-securite-reseau/>

<https://www.varonis.com/fr/blog/dns-kezako>

<https://www.varonis.com/fr/blog/guide-de-securite-dns?hsLang=fr>

https://fr.wikipedia.org/wiki/Domain_Name_System

DOC DNS

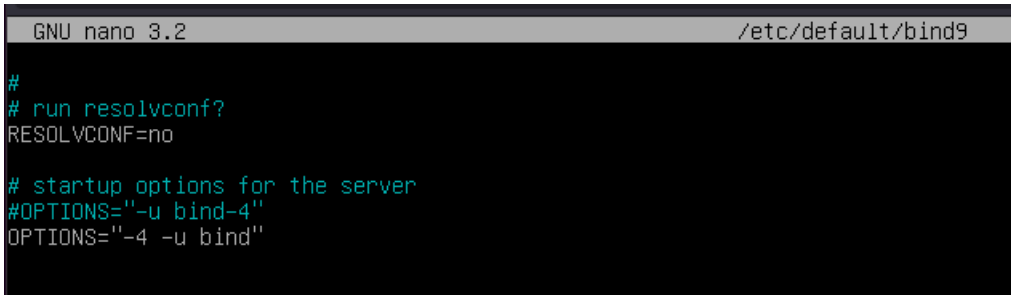
installation de bind9

```
sudo apt install bind9 bind-utils bind-host bind-doc
```

configurer le DNS en IPV4

```
nano / etc / default / bind9
```

```
OPTIONS= "-4 -u bind"
```



```
GNU nano 3.2 /etc/default/bind9
#
# run resolvconf?
RESOLVCONF=no
# startup options for the server
#OPTIONS="-u bind-4"
OPTIONS="-4 -u bind"
```

voir le statue du service

```
systemctl status bind9
```

redémarrer le service DNS bind9

```
systemctl restart bind9
```

activer le service bind9

```
systemctl enable bind9
```

utiliser la commande dig sur un client

```
dig @adress google.fr
```

sur le serveur DNS

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

le forwarders : est un serveur DNS (Domain Name System) sur un réseau qui transfère les requêtes DNS pour les noms DNS externes aux serveurs DNS en dehors de ce réseau.

le recursion : Une recherche DNS récursive est l'endroit où un serveur DNS communique avec plusieurs autres serveurs DNS pour rechercher une adresse IP et la renvoyer au client.

il y a une différence en les deux requêtes avec la commande dig car le serveur DNS à enregistrer le nom de domaine qui a été demandé lors de la première demande ce qui a rendu la demande beaucoup plus rapidement pour le second.

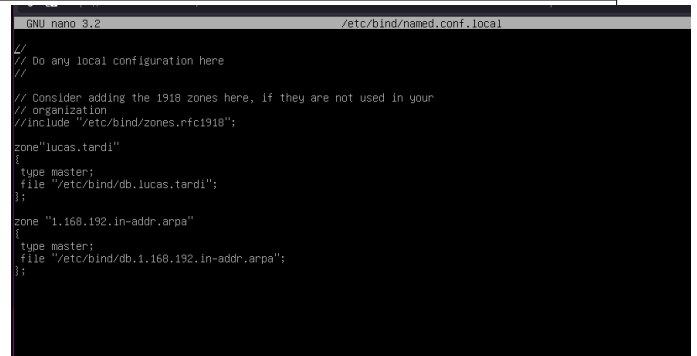
!/ ne pas utiliser une extension existante comme .com .fr .ru .en .org

aller dans le fichier

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

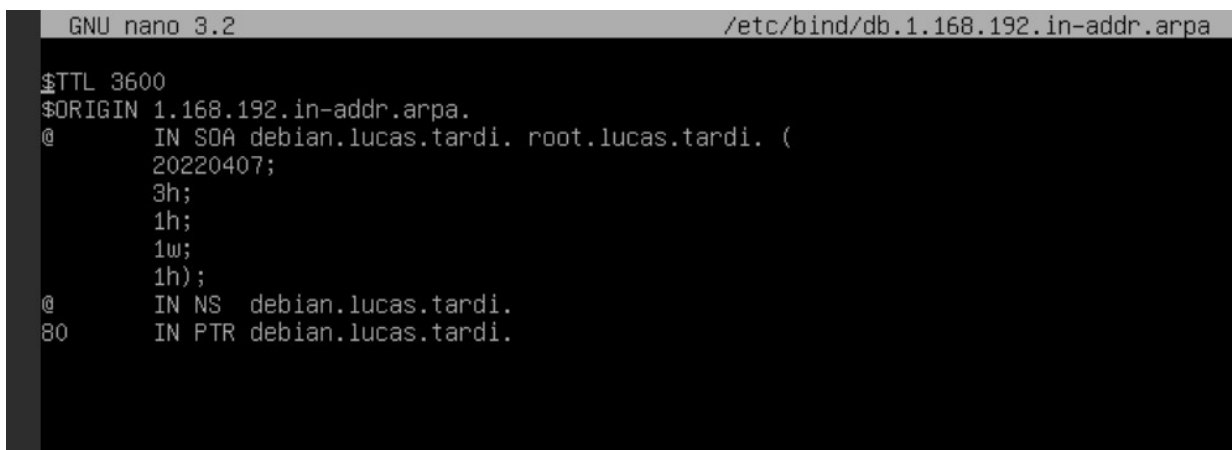
mise en place des zone sur le DNS

```
zone « lucas.tardi » {  
    type master ;  
    file « /etc/bind/db.lucas.tardi » ;  
};  
  
zone « 1.168.192.in-addr.arpa » {  
    type master ;  
    file « /etc/bind/db.1.168.192.in-addr.arpa » ;  
};
```

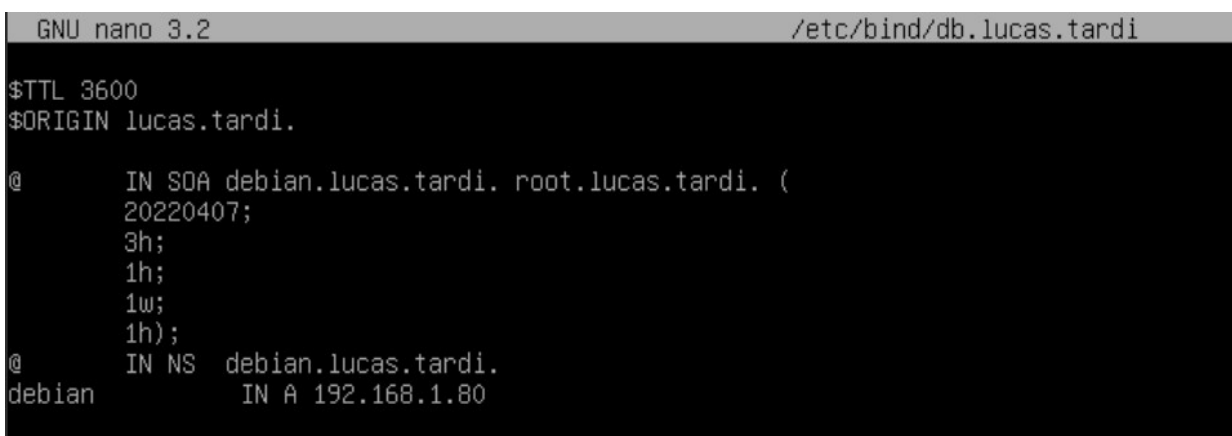


```
GNU nano 3.2 /etc/bind/named.conf.local  
//  
// Do any local configuration here  
//  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
  
zone "lucas.tardi"  
{  
    type master;  
    file "/etc/bind/db.lucas.tardi";  
};  
  
zone "1.168.192.in-addr.arpa"  
{  
    type master;  
    file "/etc/bind/db.1.168.192.in-addr.arpa";  
};
```

il faut créer deux fichier avec le même nom que les zone définis dans le fichier named.conf.local pour configurer les zones.



```
GNU nano 3.2 /etc/bind/db.1.168.192.in-addr.arpa  
$TTL 3600  
$ORIGIN 1.168.192.in-addr.arpa.  
@      IN SOA  debian.lucas.tardi. root.lucas.tardi. (  
        20220407;  
        3h;  
        1h;  
        1w;  
        1h);  
@      IN NS   debian.lucas.tardi.  
80     IN PTR  debian.lucas.tardi.
```



```
GNU nano 3.2 /etc/bind/db.lucas.tardi  
$TTL 3600  
$ORIGIN lucas.tardi.  
@      IN SOA  debian.lucas.tardi. root.lucas.tardi. (  
        20220407;  
        3h;  
        1h;  
        1w;  
        1h);  
@      IN NS   debian.lucas.tardi.  
debian IN A    192.168.1.80
```

relancer le service bind9

permet de recharger le service bind9

```
service bind9 reload
```

puis vous aller vérifier si les deux fichier de configuration de zones sont bien pris.

la commande "named-checkconf -z" permet de voir les erreur des fichier des zone s'il y sont bien écrit est qu'il peut être charger

```
named-checkconf -z
```

```
root@debian:~# named-checkconf -z
zone lucas.tardi/IN: loaded serial 20220407
zone 1.168.192.in-addr.arpa/IN: loaded serial 20220407
zone localhost/IN: loaded serial 2
zone 127.in-addr.arpa/IN: loaded serial 1
zone 0.in-addr.arpa/IN: loaded serial 1
zone 255.in-addr.arpa/IN: loaded serial 1
root@debian:~# _
```

si la commande vous afficher pas d'erreur alors les zones sont bien configurer.

Aller sur un client qui est connecter aux même réseau que le DNS puis vérifier si le client peut faire un requête ICMP (ping) avec le nom de domaine sur serveur DNS.

Ping (client) au serveur DNS

```
ping debian.lucas.tardi
ou
dig debian.lucas.tardi
```


```
[pigeon@localhost ~]$ ping debian.lucas.tardi
PING debian.lucas.tardi (192.168.1.80) 56(84) octets de données.
64 octets de debian.lucas.tardi (192.168.1.80) : icmp_seq=1 ttl=64 temps=0.913 ms
64 octets de debian.lucas.tardi (192.168.1.80) : icmp_seq=2 ttl=64 temps=0.269 ms
64 octets de debian.lucas.tardi (192.168.1.80) : icmp_seq=3 ttl=64 temps=0.257 ms
64 octets de debian.lucas.tardi (192.168.1.80) : icmp_seq=4 ttl=64 temps=0.247 ms
^C
--- statistiques ping debian.lucas.tardi ---
4 paquets transmis, 4 reçus, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.247/0.421/0.913/0.283 ms
[pigeon@localhost ~]$
```

PARTIE 3 Sécurisation du DNS ACL :

un ACL nom complet (Access Control List) a pour but de gérer les droit d'accès aux fichiers est au service peut gérer aussi un liste d'adresse et de port à autoriser ou à interdire sur un machine pour la sécurité du réseaux.

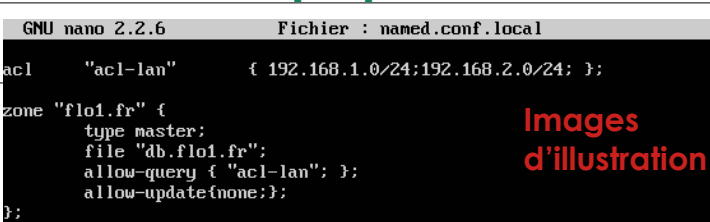
Pour mettre en place un ACL sur le serveur DNS il faut se rendre dans le fichier il faut se rendre dans le fichier **named.conf.options** se sera ici qu'on autorisera les réseaux de confiance est les hôtes pour interroger le serveur DNS.

autorisera les réseaux de confiance est les hôtes

Allow-recursion{192.168.1.0/24;}; Allow-query {192.168.1.0/24 ;};	 <p>GNU nano 2.2.6 Fichier : named.conf.options</p> <pre>options { directory "/var/cache/bind"; allow-query{192.168.1.0/24;192.168.2.254;}; dnssec-validation auto; auth-nxdomain no; # conform to RFC1035 listen-on-v6 { any; }; };</pre> <p>Images d'illustration</p>
--	--

ou peut appliquer différent paramètre pour chaque zone sur le serveur DNS

autorisera les réseaux de confiance est les hôtes [ACL]

acl "acl-lan" { 192.168.1.0/24; }; allow-query { "acl-lan"; }; zone "flo1.fr" { type master; file "db.flo1.fr"; allow-query { "acl-lan"; }; allow-update{none;}; };	 <p>GNU nano 2.2.6 Fichier : named.conf.local</p> <pre>acl "acl-lan" { 192.168.1.0/24;192.168.2.0/24; }; zone "flo1.fr" { type master; file "db.flo1.fr"; allow-query { "acl-lan"; }; allow-update{none;}; };</pre> <p>Images d'illustration</p>
--	--

!/ \ le transfert de zone peut avoir un impacte sur la sécurité du DNS car si un serveur DNS distant essayer de faire un demande de recherche d'un nom de domaine a un serveur DNS priver il peut alors récupérer des informations du réseau qu'il a demander c'est pour cela qu'on doit interdire le transfert de zone.