

Serveur Bind.

Présentation :

Le DNS (Domain Name System) est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.

Il existe plusieurs serveurs DNS gratuit comme OpenDNS ou bien Bind. Nous allons utiliser ce dernier qui est sur un noyau Unix.

Objectif :

Installer un serveur DNS en ligne de commande sur une distribution Linux avec son serveur esclave.

Pré requis :

- ➔ Deux Ordinateurs sur Linux (ici, on utilisera la Debian 8.2).
- ➔ Avoir une connexion internet.
- ➔ Avoir deux IP fixe pour les serveurs Bind.
- ➔ Dans la suite du TP, le linux maître s'appelle serveurbind, son adresse IP est 192.168.1.32/24 et le linux esclave serveurbindslv avec comme adresse IP 192.168.1.33/24. Enfin le nom du réseau est quantin.local

Sommaire :

- I. Installation des paquets sur la machine Linux.
- II. Configuration des fichiers dans /etc/.
- III. Configuration des fichiers dans /etc/bind.
- IV. Test avec Serveur Maître
- V. Configuration d'un Serveur Bind esclave
- VI. Test avec Serveur Esclave
- VII. DNS Dynamique
- VIII. Test sur les Clients

I. Installation des paquets sur la machine Linux.

Avant toute installation, il faut faire une mise à jour de la machine avec la commande *apt-get update*

Pour installer les deux paquets qu'il nous faut, on utilise la commande *apt-get install*

```
root@serveurbind:/# apt-get install bind9 dnsutils
```

Après, nous pouvons mettre la machine en IP fixe car un serveur n'est jamais être en DHCP. On édite alors le fichier */etc/network/interfaces* :

```
iface eth0 inet static
address 192.168.1.32
mask 255.255.255.0
gateway 192.168.1.254
dns-nameservers 192.168.1.32
```

II. Configuration des fichiers dans /etc/.

Avant de modifier les fichiers de Bind, il faut faire quelques modifications dans les fichiers dans */etc/*

Dans */etc/hostname/*, ajouter au nom de votre ordi, le nom FQDN de votre réseau :

```
serveurbind.quantin.local
```

Dans */etc/host/*, ajouter une ligne avec l'adresse IP de votre machine suivi du nom complet de la machine et de son nom :

```
192.168.1.32    serveurbind.quantin.local    serveurbind
```

Dans */etc/host.conf/*, ajouter cette ligne :

```
order hosts, bind
```

Enfin, dans */etc/resolv.conf*, changer votre domaine et la recherche et ajouter l'adresse de votre serveur DNS :

```
domain quantin.local
search quantin.local
nameserver 192.168.1.32
```

III. Configuration des fichiers Bind.

Les fichiers de configurations se situent dans le répertoire `/etc/bind/` donc :

```
root@serveurbind:/# cd /etc/bind/
```

On va commencer par le fichier de la zone de recherche directe mais avant toute modification, il est préférable d'en faire une copie pour toujours avoir un original non-changé.

```
cp db.local db.quantin.local
```

Après avoir édité la copie ici `db.quantin.local`, on doit opérer les changements nécessaires :

```
GNU nano 2.2.6          Fichier : db.quantin.local          Modifié
;
; BIND data file for local loopback interface
;
$TTL      604800
$ORIGIN   quantin.local.
@         IN      SOA      serveurbin.quantin.local. root.serveurbind.quantin.local.$
                2          ; Serial
                604800     ; Refresh
                86400      ; Retry
                2419200    ; Expire
                604800 )   ; Negative Cache TTL
;
                NS       serveurbind
                MX       10 serveurbind
serveurbind  A         192.168.1.32
localhost   A         127.0.0.1
www         IN      CNAME   serveurbind
```

On va s'occuper maintenant de la zone de recherche inversée donc on effectue toujours une copie :

```
cp db.127 db.quantin.local.inv
```

Puis on édite la copie et on applique les changements :

```
GNU nano 2.2.6      Fichier : db.quantin.local.inv
┆
┆ ; BIND reverse data file for local loopback interface
┆ ;
┆ $TTL      604800
┆ $ORIGIN  1.168.192.in-addr.arpa.
┆ @        IN      SOA      serveurbin.quantin.local. root.quantin.local. (
┆                               1          ; Serial
┆                               604800     ; Refresh
┆                               86400     ; Retry
┆                               2419200   ; Expire
┆                               604800 )   ; Negative Cache TTL
┆ ;
┆ 32       IN      NS       serveurbind.quantin.local.
┆          PTR     serveurbind.quantin.local.
```

Dernier fichier à configurer, pas besoin de faire une copie, seulement de l'éditer :

```
nano named.conf.local
```

On crée les zones directe et inversé. Ici, notre réseau est 192.168.1.0 donc on met le net id dans le fichier :

```
GNU nano 2.2.6      Fichier : 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 "quantin.local" {
┆     type master;
┆     file "/etc/bind/db.quantin.local";
┆     forwarders{};
┆ };
┆
┆ zone "1.168.192.in-addr.arpa" {
┆     type master;
┆     file "/etc/bind/db.quantin.local.inv";
┆     forwarders{};
┆ };
┆
```

On peut maintenant redémarrer Bind9 :

```
service bind9 restart
```

IV. Test avec Serveur Maître

On va maintenant faire des tests avec les outils DNS c'est-à-dire nslookup et dig et aussi des tests de vérifications avec named-checkzone.

Named-checkzone :

```
root@serveurbind:/etc/bind# named-checkzone quantin.local /etc/bind/db.quantin.local
zone quantin.local/IN: loaded serial 2
OK
```

```
root@serveurbind:/etc/bind# named-checkzone quantin.local /etc/bind/db.quantin.local.inv
/etc/bind/db.quantin.local.inv:7: ignoring out-of-zone data (1.168.192.in-addr.arpa)
/etc/bind/db.quantin.local.inv:15: ignoring out-of-zone data (32.1.168.192.in-addr.arpa)
zone quantin.local/IN: has 0 SOA records
zone quantin.local/IN: has no NS records
zone quantin.local/IN: not loaded due to errors.
```

Nslookup :

```
root@serveurbind:/etc/bind# nslookup
> 192.168.1.32
Server:          192.168.1.32
Address:         192.168.1.32#53

32.1.168.192.in-addr.arpa      name = serveurbind.quantin.local.
```

```
root@serveurbind:/etc/bind# nslookup
> serveurbind
Server:          192.168.1.32
Address:         192.168.1.32#53

Name:   serveurbind.quantin.local
Address: 192.168.1.32
```

Dig :

```
root@serveurbind:/etc/bind# dig serveurbind

;<<>> DiG 9.9.5-9+deb8u3-Debian <<>> serveurbind
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 10828
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;serveurbind.                IN      A

;; AUTHORITY SECTION:
.                10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2015091800 1800 900 604800 86400

;; Query time: 1010 msec
;; SERVER: 192.168.1.32#53(192.168.1.32)
;; WHEN: Fri Sep 18 14:53:35 CEST 2015
;; MSG SIZE rcvd: 115
```

V. Configuration d'un Serveur Bind9 Esclave

Sur une autre machine linux, nous allons installer aussi Bind9 et nous allons le configurer en tant qu'esclave.

On va éditer seulement un fichier, le named.conf.local :

```
root@serveurbindsrv:/# nano /etc/bind/named.conf.local
```

Puis le configurer comme ceci :

```
zone "quantin.local" IN {
    type slave;
    masters { 192.168.1.32 ; } ;
    file "/etc/bind/db.quantin.local"
};

zone "1.168.192.in-addr.arpa" IN {
    type slave;
    masters { 192.168.1.33 ; } ;
    file "/etc/bind/db.quantin.local.inv"
};
```

Sur le Serveur Maître, on édite le named.conf.local et on rajoute les deux lignes jaunes :

```
zone "quantin.local" IN {
    type master;
    file "/etc/bind/db.quantin.local";
    forwarders{};
    notify yes ;
    allow-transfer { 192.168.1.33 ; } ;
};

zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "/etc/bind/db.quantin.local.inv";
    forwarders{};
    notify yes ;
    allow-transfer { 192.168.1.33 ; } ;
};
```


VI. Tests avec Serveur Esclave.

@Ip du Serveur Maître :

```
root@serveurbindsrv:/# nslookup 192.168.1.32
Server:          192.168.1.32
Address:         192.168.1.32#53

32.1.168.192.in-addr.arpa      name = serveurbind.quantin.local.
```

@IP du Serveur Esclave :

```
root@serveurbindsrv:/# nslookup 192.168.1.33
Server:          192.168.1.32
Address:         192.168.1.32#53

33.1.168.192.in-addr.arpa      name = serveurbindsrv.quantin.local.
```

Résolution de nom du Serveur Maître :

```
root@serveurbindsrv:/# nslookup serveurbind
Server:          192.168.1.32
Address:         192.168.1.32#53

Name:   serveurbind.quantin.local
Address: 192.168.1.32
```

Résolution de nom du Serveur Esclave :

```
root@serveurbindsrv:/# nslookup serveurbindsrv
Server:          192.168.1.32
Address:         192.168.1.32#53

Name:   serveurbindsrv.quantin.local
Address: 192.168.1.33
```

Puis dans les logs, nous vérifions si tout c'est bien passé :

```
serveurbind named[987]: zone quantin.local/IN: sending notifies (serial 3)
serveurbind named[987]: zone 1.168.192.in-addr.arpa/IN: sending notifies (serial 3)
```

VII. DNS Dynamique

Pour Windows :

On va modifier un fichier sur le serveur bind :

```
root@serveurbind:/etc/bind# nano named.conf.local
```

Puis dans les deux zones, rajouter les lignes surlignées en jaunes (on met l'adresse IP du serveur DHCP ou 127.0.0.1 si on a le dns et le dhcp sur la même machine) :

```
zone "quantin.local" IN {
    type master;
    file "/etc/bind/db.quantin.local";
    forwarders{};
    notify yes ;
    allow-transfer { 192.168.1.33 ; } ;
    allow-update { 192.168.1.134; };
};

zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "/etc/bind/db.quantin.local.inv";
    forwarders{};
    notify yes ;
    allow-transfer { 192.168.1.33 ; } ;
    allow-update { 192.168.1.134; };
};
```

Enfin, sur le serveur dhcp, dans le fichier dhcp.conf, on rajoute ses lignes (dans primary, mettre l'adresse IP du DNS ou 127.0.0.1 si on a le dns et le dhcp sur la même machine) :

```
zone quantin.local. { primary 192.168.1.32; }
zone 1.168.192.in-addr.arpa. { primary 192.168.1.32; }
```

```
ddns-update-style interim;
ddns-updates on;
ignore client-updates;
update-static-leases on;
allow-unknown-clients;
```

Pour Linux :

Il suffit de changer la ligne dans le fichier :

```
nano /etc/dhcp/dhclient.conf
```

Puis remplacer cette ligne par :

```
send host-name = "debian8.quantin.local";
```

Après toutes les modifications, il faut redémarrer le service Bind et Dhcp.

VIII. Test sur les Clients :

Windows :

Après avoir demandé un bail dhcp (*ipconfig /release* puis *ipconfig /renew*) on regarde notre adresse IP avec *ipconfig* :

```
Carte Ethernet Connexion au réseau local :
    Suffixe DNS propre à la connexion. . . : quantin.local
    Adresse IPv4. . . . . : 192.168.1.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.1.254
```

On remarque l'ajout automatique dans la zone directe :

```
$TTL 300 ; 5 minutes
WIN7      A      192.168.1.1
          TXT   "310a9f1056428dcb2d35316553d1b6998a"
```

Linux :

Après avoir demandé un bail dhcp (*ifdown eth0* puis *ifup eth0*) on regarde notre adresse IP avec *ifconfig* :

```
root@debian8:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:bf:a6:54
          inet adr:192.168.1.3  Bcast:192.168.1.255  Masque:255.255.255.0
```

On remarque aussi comme pour le windows , l'ajout automatique dans la zone directe :

```
$TTL 300 ; 5 minutes
debian8.quantin.local  A      192.168.1.3
                      TXT   "000f4745b04ed9d4c4e2b2b36badbd93f7"
```

En recherche inversé, l'ajout des deux clients s'est aussi fait:

```
$ORIGIN 1.168.192.in-addr.arpa.
$TTL 300      ; 5 minutes
1             PTR      WIN7.quantin.local.
3             PTR      debian8.quantin.local.quantin.local.
```

Dans le `/var/log/syslog`, on voit bien la mise à jour et l'ajout du client Windows :

```
updating zone 'quantin.local/IN': adding an RR at 'WIN7.quantin.local' A
updating zone 'quantin.local/IN': adding an RR at 'WIN7.quantin.local' TXT
serveurbind named[1065]: zone quantin.local/IN: sending notifies (serial 4)
updating zone '1.168.192.in-addr.arpa/IN': deleting rrsset at '1.1.168.192.in-addr.arpa'
updating zone '1.168.192.in-addr.arpa/IN': adding an RR at '1.1.168.192.in-addr.arpa'
serveurbind named[1065]: zone 1.168.192.in-addr.arpa/IN: sending notifies (serial 4)
```

Mais aussi la mise à jour et l'ajout du client linux :

```
zone quantin.local/IN: sending notifies (serial 4)
zone 1.168.192.in-addr.arpa/IN: sending notifies (serial 4)
updating zone 'quantin.local/IN': adding an RR at 'debian8.quantin.local' A
updating zone 'quantin.local/IN': adding an RR at 'debian8.quantin.local' TXT
updating zone '1.168.192.in-addr.arpa/IN': deleting rrsset at '3.1.168.192.in-addr.arpa'
updating zone '1.168.192.in-addr.arpa/IN': adding an RR at '3.1.168.192.in-addr.arpa'
zone quantin.local/IN: sending notifies (serial 5)
```

Remarque, deux fichiers ont été créé avec l'extension `.jnl` . Ce sont des fichiers divers principalement associés avec Journal Macro Data File :

```
-rw-r--r-- 1 bind bind 771 oct. 1 11:58 db.quantin.local
-rw-r--r-- 1 bind bind 602 oct. 1 12:00 db.quantin.local.inv
-rw-r--r-- 1 bind bind 2227 oct. 1 11:47 db.quantin.local.inv.jnl
-rw-r--r-- 1 bind bind 3024 oct. 1 11:47 db.quantin.local.jnl
```