

Installation & Configuration

Service DNS

Cette procédure guide l'installation et la configuration d'un service DNS primaire utile à la résolution de noms de domaines en adresses IP et inversement.

SOMMAIRE

-

Prérequis à la configuration	p.2
Configuration du service DNS - Résolution Directe	p.3-4
Tests du DNS - Zone Directe	p.5-6
Configuration du service DNS - Résolution Inversé	p.7
Tests du DNS - Zone Inversée	p.8

Prérequis à la configuration

*Il est essentiel de respecter la casse
(Différenciation Minuscule/Majuscule et les espaces/tabulations)*

Bon à savoir : Ce texte signale une commande
Celui-là signale un "path" ou un fichier

Installation Bind9

Avant toute nouvelle installation, on met à jour les paquets déjà présents sur la machine :
`apt update`

Installation paquet apache 2 :

```
apt install bind9
```

```
systemctl status bind9
```

 (Si bind9 fonctionne, un message positif est affiché)

Pour la gestion du service dns bind9 :

```
systemctl status/start/stop/restart/reload bind9
```

Pour vérifier le fonctionnement du fichier de configuration `named.conf.local` et des fichiers de zones : `db.quoniam.local` & `db.172.17.`

```
named-checkconf -z
```

Autres prérequis :

Il est nécessaire d'être équipé de :

- Une machine serveur Debian 12.x, correctement installée et opérationnelle.
- Une machine Windows cliente afin de tester le DNS
- Des privilèges d'administration pour installer des logiciels et modifier les configurations.
- Une connexion réseau fonctionnelle
- Un éditeur de texte tel que *nano* pour ajuster les fichiers de configuration.
- Un navigateur web pour tester le fonctionnement du service

Configuration du service DNS - Résolution Directe

On commence par modifier le nom de la machine avec `nano /etc/hostname`

Il est conseillé d'utiliser un nom de machine familier facilement réutilisable.

`DebianDNS1-INITIALES` par exemple (ne pas inclure de “_”).

```
GNU nano 7.2 /etc/hostname *  
DebianDNS1-RQ
```

Le fichier stocké dans `/etc/resolv.conf` contient les différents serveurs DNS utilisés par le système. Dedans, on écrit uniquement le serveur DNS voulu (IP du serveur Linux ici)

Ce fichier peut se réinitialiser tout seul si une IP statique n’a pas été configurée sur la machine, il ne faut donc pas hésiter à le vérifier régulièrement (cela peut expliquer un dysfonctionnement).

```
GNU nano 7.2 /etc/resolv.conf *  
gameserver 172.17.219.139
```

=> `/etc/bind/named.conf.local`

Dans ce fichier, on ajoute les lignes supplémentaires :

```
GNU nano 7.2 /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 "quoniam.local" IN {  
type master;  
file "db.quoniam.local";  
};
```

Il est nécessaire de personnaliser les noms de domaine :

`nom.local` / `db.nom.local`

Par la suite, on va créer (touch ou nano) le fichier db.nom.local dans le répertoire

=> `/var/cache/bind/db.quoniam.local`

```
GNU nano 7.2 /var/cache/bind/db.quoniam.local *
$TTL 86400

quoniam.local. IN SOA DebianDNS-RQ.quoniam.local. root.quoniam.local. (
    1      ; Serial
    604800 ; Refresh
    86400  ; Retry
    2419200 ; Expire
    86400  ); Negative Cache TTL

quoniam.local. IN NS DebianDNS-RQ.quoniam.local.

DebianDNS-RQ.quoniam.local. IN A 172.17.219.139
poste25.quoniam.local. IN A 172.17.219.139
```

Vérification du bon fonctionnement du service avec cette configuration :

```
root@DebianDNS1-RQ:~# named-checkconf -z
```

Démarrage du service si fonctionnel

```
root@DebianDNS1-RQ:~# systemctl restart bind9
root@DebianDNS1-RQ:~# systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Thu 2024-12-12 10:35:17 CET; 8s ago
     Docs: man:named(8)
  Main PID: 591 (named)
    Status: "running"
     Tasks: 4 (limit: 2306)
  Memory: 11.2M
     CPU: 40ms
  CGroup: /system.slice/named.service
          └─591 /usr/sbin/named -f -u bind

déc. 12 10:35:17 DebianDNS1-RQ named[591]: network unreachable resolving './DNSKEY/IN': 2001:500:2::c#5
déc. 12 10:35:17 DebianDNS1-RQ named[591]: network unreachable resolving './NS/IN': 2001:500:2::c#5
déc. 12 10:35:17 DebianDNS1-RQ named[591]: network unreachable resolving './DNSKEY/IN': 2001:503:ba3e::c#5
déc. 12 10:35:17 DebianDNS1-RQ named[591]: network unreachable resolving './NS/IN': 2001:503:ba3e::c#5
déc. 12 10:35:17 DebianDNS1-RQ named[591]: network unreachable resolving './DNSKEY/IN': 2001:500:a8::c#5
déc. 12 10:35:17 DebianDNS1-RQ named[591]: network unreachable resolving './NS/IN': 2001:500:a8::c#5
déc. 12 10:35:17 DebianDNS1-RQ named[591]: network unreachable resolving './DNSKEY/IN': 2001:7fe::53#53
déc. 12 10:35:17 DebianDNS1-RQ named[591]: network unreachable resolving './NS/IN': 2001:7fe::53#53
déc. 12 10:35:17 DebianDNS1-RQ named[591]: managed-keys-zone: Key 20326 for zone . is now trusted (
déc. 12 10:35:17 DebianDNS1-RQ named[591]: resolver priming query complete: success
lines 1-22/22 (END)
```

Test du DNS - Zone Directe

Sur le serveur linux DNS :

```
dig poste25.quoniam.local
```

```
root@DebianDNS1-RQ:~# dig poste25.quoniam.local

; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> poste25.quoniam.local
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63122
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c3bd2accfeda065d01000000675aaff65436b6666589cf78 (good)
;; QUESTION SECTION:
;poste25.quoniam.local.      IN      A

;; ANSWER SECTION:
poste25.quoniam.local.  86400   IN      A      172.17.219.139

;; Query time: 0 msec
;; SERVER: 172.17.219.139#53(172.17.219.139) (UDP)
;; WHEN: Thu Dec 12 10:42:14 CET 2024
;; MSG SIZE rcvd: 94
```

```
nslookup www.google.fr
```

```
root@DebianDNS1-RQ:~# nslookup www.google.fr
Server:      172.17.30.1
Address:     172.17.30.1#53

Non-authoritative answer:
Name:   www.google.fr
Address: 142.251.37.163
Name:   www.google.fr
Address: 2a00:1450:4006:811::2003
```

Test client Windows :

(après modification de son serveur DNS dans le panneau de configuration)

Ouverture du cmd et test des commandes suivantes :

```
C:\Users\rquoniam>nslookup pc-prof.quoniam.local
Serveur :    UnKnown
Address:  172.17.219.139

Nom :      pc-prof.quoniam.local
Address:  172.17.17.17
```

```
C:\Users\rquoniam>nslookup www.google.fr
Serveur :    UnKnown
Address:  172.17.219.139

Réponse ne faisant pas autorité :
Nom :      www.google.fr
Addresses:  2a00:1450:4006:811::2003
           142.251.37.163
```

```
C:\Users\rquoniam>nslookup poste25.quoniam.local
Serveur :    UnKnown
Address:  172.17.219.139

Nom :      poste25.quoniam.local
Address:  172.17.219.139
```

Mise en place de la résolution DNS inversé :

On retourne tout d'abord dans le fichier suivant =>

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

Ajout des lignes de configuration comme ci-dessous.

La "zone" correspond au `Net ID inversé` + `partie HostID` => `17.172.in-addr.arpa`

Le "file" est le nom du fichier de configuration utilisé.

On distingue les fichiers de résolution directe et indirecte par leur noms.

```
GNU nano 7.2 /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 "quoniam.local" IN {
type master;
file "db.quoniam.local";
};

zone "17.172.in-addr.arpa" IN {
type master;
file "db.172.17";
};
```

Copie du fichier `db.quoniam.local` en `db.172.17` dans le même répertoire.

On le configure ainsi (Adresses IP inversées, échanges domaines/@ et A modifié en PTR) :

```
GNU nano 7.2 db.172.17
$TTL 86400
17.172.in-addr.arpa. IN SOA DebianDNS-RQ.quoniam.local. root.quoniam.local. (
    1      ; Serial
    604800 ; Refresh
    86400  ; Retry
    2419200 ; Expire
    86400  ) ; Negative Cache TTL

17.172.in-addr.arpa. IN NS DebianDNS-RQ.quoniam.local.

139.219.17.172.in-addr.arpa. IN PTR DebianDNS-RQ.quoniam.local
139.219.17.172.in-addr.arpa. IN PTR poste25.quoniam.local
17.17.17.172.in-addr.arpa. IN PTR pc-prof.quoniam.local
```

Vérification du bon fonctionnement des fichiers => `root@DebianDNS1-RQ:~# named-checkconf -z`

Redémarrage du service bind9 si fonctionnel => `systemctl restart bind9`

Tests en Résolution Inversé :

Le paramètre spécifique “-x” impliqué dans la commande “dig” spécifie la résolution inversée.

```
root@DebianDNS1-RQ:/var/cache/bind# named-checkconf -z
zone quoniam.local/IN: loaded serial 1
zone 17.172.in-addr.arpa/IN: loaded serial 1
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
```

Toutes les “séries” sont “chargées” ? Donc le service est fonctionnel ainsi.

Sur le serveur linux DNS :

```
dig -x 172.17.17.17
```

```
GNU nano 7.2 db.172.17
TTL 86400

17.172.in-addr.arpa. IN SOA DebianDNS-RQ.quoniam.local. root.quoniam.local. (
    1 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    86400 ); Negative Cache TTL

17.172.in-addr.arpa. IN NS DebianDNS-RQ.quoniam.local.

139.219.17.172.in-addr.arpa. IN PTR DebianDNS-RQ.quoniam.local
139.219.17.172.in-addr.arpa. IN PTR poste25.quoniam.local
17.17.17.172.in-addr.arpa. IN PTR pc-prof.quoniam.local
```

```
dig -x 172.17.219.139
```

```
root@DebianDNS1-RQ:/var/cache/bind# dig -x 172.17.219.139
; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> -x 172.17.219.139
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48009
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 71a3a6948e1a97f701000000675ade2abb8a4308228f3c7d (good)
;; QUESTION SECTION:
;139.219.17.172.in-addr.arpa. IN PTR

;; ANSWER SECTION:
139.219.17.172.in-addr.arpa. 86400 IN PTR poste25.quoniam.local.17.172.in-addr.arpa.
139.219.17.172.in-addr.arpa. 86400 IN PTR DebianDNS-RQ.quoniam.local.17.172.in-addr.arpa.

;; Query time: 0 msec
;; SERVER: 172.17.219.139#53(172.17.219.139) (UDP)
;; WHEN: Thu Dec 12 13:59:22 CET 2024
;; MSG SIZE rcvd: 166
```


Sur le client windows :

- Ouvrir l'invite de commande (cmd) et entrer :

```
nslookup 172.17.219.139
```

```
C:\Users\rquoniam>nslookup 172.17.219.139
Serveur :   DebianDNS-RQ.quoniam.local.17.172.in-addr.arpa
Address:    172.17.219.139

Nom :       poste25.quoniam.local.17.172.in-addr.arpa
Address:    172.17.219.139
```

```
nslookup 172.17.17.17
```

```
C:\Users\rquoniam>nslookup 172.17.17.17
Serveur :   poste25.quoniam.local.17.172.in-addr.arpa
Address:    172.17.219.139

Nom :       pc-prof.quoniam.local.17.172.in-addr.arpa
Address:    172.17.17.17
```