

## **Procédure service DNS bind9 sous linux debian**

### **SOMMAIRE :**

<b>Prérequis.....</b>	<b>1</b>
<b>La zone directe.....</b>	<b>3</b>
<b>La zone inversée.....</b>	<b>7</b>

Cette procédure détaillée explique étape par étape comment installer et configurer un service DNS primaire basé sur BIND9, permettant de traduire des noms de domaines en adresses IP, ainsi que d'effectuer l'opération inverse, offrant ainsi une gestion complète et efficace de la résolution DNS sur un système Linux Debian.

## Prérequis

Mettre à jour les dépôts et les paquets, exécutez la commande : `apt update`

Installez le service avec la commande : `apt install bind9`

Assurez-vous que le service est actif avec : `systemctl status bind9`

Vérifiez les fichiers de configuration de BIND avec : `named-checkconf -z`



## La zone directe

Modifier le fichier de configuration principal : Éditez le fichier principal avec : [nano /etc/bind/named.conf](#), Configurer le fichier named.conf.local, Modifiez ce fichier avec : [nano /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 "gael.local" IN {
    type master;
    file "db.gael.local";
};
```

Créer un fichier de zone directe : créez un fichier pour votre zone dans /var/cache/bind/, par exemple : [nano /var/cache/bind/db.gael.local](#)

Modifier le nom de la machine en éditant le fichier hostname : [nano /etc/hostname](#)

```
GNU nano 7.2 /etc/hostname
DebianDNS1-gg

```

Ajouter les enregistrements nécessaires dans le fichier de zone en allant dans le named.conf.local avec la commande [nano /etc/bind/named.conf.local](#) et ajouter le texte ci-dessous

```
$TTL 86400

gael.local.      IN      SOA      debianDNS-gg.gael.local.      root.gael.local.      (
    1           ; Serial
    604800      ; Refresh
    86400       ; Retry
    2419200     ; Expire
    86400      ) ; Negative Cache TTL

gael.local.      IN      NS       debianDNS-gg.gael.local.

debianDNS-gg.gael.local.      IN      A          172.17.219.159
poste26.gael.local.      IN      A          172.17.219.159
```

Vérification de la syntaxe du fichier named.conf.local et des fichiers de zones avec la commande [named-checkconf -z](#)

```
root@DebianDNS1-gg:~# named-checkconf -z
zone gael.local/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
```

Gestion du service dns bind9 en vérifiant le statut actuel avec la commande `systemctl status bind9`

```
root@DebianDNS1-gg:~# 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 10:35:24 CET; 9s ago
     Docs: man:named(8)
   Main PID: 645 (named)
    Status: "running"
     Tasks: 6 (limit: 4644)
    Memory: 32.5M
       CPU: 44ms
   CGroup: /system.slice/named.service
           └─645 /usr/sbin/named -f -u bind

déc. 12 10:35:24 DebianDNS1-gg named[645]: network unreachable resolving './DNSKEY/IN': 2001:500:1::53#53
déc. 12 10:35:24 DebianDNS1-gg named[645]: network unreachable resolving './NS/IN': 2001:500:1::53#53
déc. 12 10:35:24 DebianDNS1-gg named[645]: network unreachable resolving './DNSKEY/IN': 2801:1b8:10::b#53
déc. 12 10:35:24 DebianDNS1-gg named[645]: network unreachable resolving './NS/IN': 2801:1b8:10::b#53
déc. 12 10:35:24 DebianDNS1-gg named[645]: network unreachable resolving './DNSKEY/IN': 2001:500:12::d0d#53
déc. 12 10:35:24 DebianDNS1-gg named[645]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
déc. 12 10:35:24 DebianDNS1-gg named[645]: network unreachable resolving './DNSKEY/IN': 2001:500:9f::42#53
déc. 12 10:35:24 DebianDNS1-gg named[645]: network unreachable resolving './DNSKEY/IN': 2001:7fd:1#53
déc. 12 10:35:24 DebianDNS1-gg named[645]: resolver priming query complete: success
déc. 12 10:35:24 DebianDNS1-gg named[645]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance)
```

Test de la zone directe avec la commande `dig www.google.fr` et `dig -x`

```
root@DebianDNS1-gg:~# dig www.google.fr

; <<>> DiG 9.18.28-1~debl2u2-Debian <<>> www.google.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 55776
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0dceb547d627fc0501000000675aafdd07d7d81a2c120ce0 (good)
;; QUESTION SECTION:
;www.google.fr.                IN      A

;; Query time: 132 msec
;; SERVER: 172.17.219.159#53(172.17.219.159) (UDP)
;; WHEN: Thu Dec 12 10:41:49 CET 2024
;; MSG SIZE rcvd: 70
```

```
root@DebianDNS1-gg:~# dig -x 172.17.219.159

; <<>> DiG 9.18.28-1~debl2u2-Debian <<>> -x 172.17.219.159
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 29582
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a7be395edeb8334401000000675aaf982042554f442d8e88 (good)
;; QUESTION SECTION:
;159.219.17.172.in-addr.arpa.  IN      PTR

;; AUTHORITY SECTION:
17.172.IN-ADDR.ARPA.      86400  IN      SOA      17.172.IN-ADDR.ARPA. . 0 28800 7200 604800 86400

;; Query time: 0 msec
;; SERVER: 172.17.219.159#53(172.17.219.159) (UDP)
;; WHEN: Thu Dec 12 10:40:40 CET 2024
;; MSG SIZE rcvd: 138
```

Ajouter les enregistrements nécessaires dans le fichier de zone : [pc-prof.gael.local](#).  
[172.17.17.17](#)

```
$TTL 86400
gael.local.      IN      SOA      debianDNS-gg.gael.local.      root.gael.local.      (
    1          ;      Serial
    604800     ;      Refresh
    86400      ;      Retry
    2419200    ;      Expire
    86400      );     Negative Cache TTL
;
gael.local.      IN      NS       debianDNS-gg.gael.local.
;
debianDNS-gg.gael.local.      IN      A          172.17.219.159
poste26.gael.local.      IN      A          172.17.219.159
pc-prof.gael.local.      IN      A          172.17.17.17
```

Vérifier la syntaxe avec la commande [named-checkconf -z](#)

```
root@DebianDNS1-gg:~# named-checkconf -z
zone gael.local/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
```

Tester la zone directe avec la commande `dig -x 172.17.17.17`

```
root@DebianDNS1-gg:~# dig -x 172.17.17.17

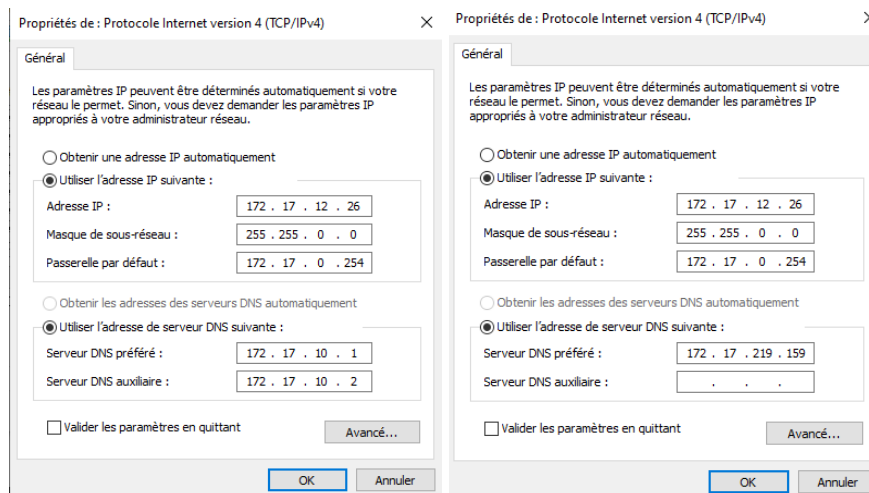
; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> -x 172.17.17.17
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 11895
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: fc481452d2921b9501000000675ab3deb2d63d2430f77e8e (good)
;; QUESTION SECTION:
;17.17.17.172.in-addr.arpa.      IN      PTR

;; AUTHORITY SECTION:
17.172.IN-ADDR.ARPA.      86400   IN      SOA      17.172.IN-ADDR.ARPA. . 0 28800 7200 604800 86400

;; Query time: 0 msec
;; SERVER: 172.17.219.159#53(172.17.219.159) (UDP)
;; WHEN: Thu Dec 12 10:58:54 CET 2024
;; MSG SIZE rcvd: 136
```

## Test windows, commencer par changer le DNS par défaut



## Test windows à partir du FQDN avec la commande `nslookup pc-prof.gael.local`

```
C:\Users\ggautier>nslookup pc-prof.gael.local
Serveur : UnKnown
Address: 172.17.219.159

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

## Test windows à partir du FQDN avec la commande `nslookup www.google.fr`

```
C:\Users\ggautier>nslookup www.google.fr
Serveur : UnKnown
Address: 172.17.219.159

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

## La zone inversée

Modifier le fichier named.conf.local en ajoutant la zone inversée

```
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 "gael.local" IN {
type master;
file "db.gael.local";
};

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

Créer un nouveau fichier pour la zone inversée appelée db.172.17 dans [/var/cache/bind](#)

```
GNU nano 7.2 /var/cache/bind/db.172.17 *
$TTL 86400
17.172.in-addr.arpa.    IN      SOA      debianDNS-gg.gael.local.    root.gael.local.
                        1      ;      Serial
                        604800 ;      Refresh
                        86400  ;      Retry
                        2419200;      Expire
                        86400  ) ;      Negative Cache TTL
;

17.172.in-addr.arpa.    IN      NS       debianDNS-gg.gael.local.
;
159.219.17.172.in-addr.arpa.    IN      PTR      debianDNS-gg.gael.local.
159.219.17.172.in-addr.arpa.    IN      PTR      poste26.gael.local.
17.17.17.172.in-addr.arpa.    IN      PTR      pc-prof.gael.local.
;
```

faire une vérification [named-checkconf -z](#)

```
root@DebianDNS1-gg:~# named-checkconf -z
zone gael.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
```



Redémarrer le service avec `systemctl restart bind9` puis le vérifier le status avec `systemctl status bind9`

```
root@DebianDNS1-gg:~# systemctl restart bind9
root@DebianDNS1-gg:~# 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 13:52:39 CET; 7s ago
     Docs: man:named(8)
  Main PID: 854 (named)
    Status: "running"
     Tasks: 6 (limit: 4644)
  Memory: 32.5M
     CPU: 56ms
  CGroup: /system.slice/named.service
          └─854 /usr/sbin/named -f -u bind
```

Tester sur le serveur client avec la commande `dig -x "ip"`

```
root@DebianDNS1-gg:~# dig -x 172.17.17.17

; <<>> DiG 9.18.28-1~debl2u2-Debian <<>> -x 172.17.17.17
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21772
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: acb26af79ea4927601000000675add754dacc62f580c5ef (good)
;; QUESTION SECTION:
;17.17.17.172.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
17.17.17.172.in-addr.arpa. 86400 IN      PTR      pc-prof.gael.local.

;; Query time: 0 msec
;; SERVER: 172.17.219.159#53(172.17.219.159) (UDP)
;; WHEN: Thu Dec 12 13:56:21 CET 2024
;; MSG SIZE rcvd: 114
```

```
root@DebianDNS1-gg:~# dig -x 172.17.219.159

; <<>> DiG 9.18.28-1~debl2u2-Debian <<>> -x 172.17.219.159
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 3567
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 69929aa5d5003e6601000000675adde8ac39640db2b31050 (good)
;; QUESTION SECTION:
;159.219.17.172.in-addr.arpa.    IN      PTR

;; AUTHORITY SECTION:
17.172.in-addr.arpa.      86400   IN      SOA      debianDNS-gg.gael.local. root.gael.local. 1 604800 86400 241920 0 86400

;; Query time: 0 msec
;; SERVER: 172.17.219.159#53(172.17.219.159) (UDP)
;; WHEN: Thu Dec 12 13:58:16 CET 2024
;; MSG SIZE rcvd: 167
```

Sur la machine cliente, utilisez la commande `nslookup "ip"` pour effectuer le test.

```
C:\Users\ggautier>nslookup 172.17.17.17
Serveur : UnKnown
Address: 172.17.219.159

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

```
C:\Users\ggautier>nslookup 172.17.219.159
Serveur : poste26.gael.local
Address: 172.17.219.159

Nom : debianDNS-gg.gael.local
Address: 172.17.219.159
```