

## Sommaire :

2.8. Installation du paquetage BIND .....	1
---	---

## 2.8. Installation du paquetage BIND

Je commence par installer le paquetage BIND et ses dépendances :

```
Les paquets supplémentaires suivants seront installés :
  bind9-dnsutils bind9-host bind9-libs bind9-utils dns-root-data
Paquets suggérés :
  bind9-doc ufw
Les NOUVEAUX paquets suivants seront installés :
  bind9 bind9-utils dns-root-data
Les paquets suivants seront mis à jour :
  bind9-dnsutils bind9-host bind9-libs
3 mis à jour, 3 nouvellement installés, 0 à enlever et 26 non mis à jour.
Il est nécessaire de prendre 1 903 kB dans les archives.
Après cette opération, 1 697 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de : 1 http://deb.debian.org/debian trixie/main amd64 bind9-host amd64 1:9.20.15-1~deb13u1 [55,4 kB]
Réception de : 2 http://deb.debian.org/debian trixie/main amd64 bind9-dnsutils amd64 1:9.20.15-1~deb13u1 [165 kB]
Réception de : 3 http://deb.debian.org/debian trixie/main amd64 bind9-libs amd64 1:9.20.15-1~deb13u1 [1 238 kB]
Réception de : 4 http://deb.debian.org/debian trixie/main amd64 bind9-utils amd64 1:9.20.15-1~deb13u1 [184 kB]
Réception de : 5 http://deb.debian.org/debian trixie/main amd64 dns-root-data all 2025080400~deb13u1 [5 948 B]
Réception de : 6 http://deb.debian.org/debian trixie/main amd64 bind9 amd64 1:9.20.15-1~deb13u1 [254 kB]
1 903 ko réceptionnés en 28s (67,4 ko/s)
Lecture des fichiers de modifications (« changelog »)... Terminé
(Lecture de la base de données... 61426 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../0-bind9-host_1%3a9.20.15-1~deb13u1_amd64.deb ...
Dépaquetage de bind9-host (1:9.20.15-1~deb13u1) sur (1:9.20.11-4) ...
Préparation du dépaquetage de .../1-bind9-dnsutils_1%3a9.20.15-1~deb13u1_amd64.deb ...
Dépaquetage de bind9-dnsutils (1:9.20.15-1~deb13u1) sur (1:9.20.11-4) ...
Préparation du dépaquetage de .../2-bind9-libs_1%3a9.20.15-1~deb13u1_amd64.deb ...
Dépaquetage de bind9-libs:amd64 (1:9.20.15-1~deb13u1) sur (1:9.20.11-4) ...
Sélection du paquet bind9-utils précédemment désélectionné.
Préparation du dépaquetage de .../3-bind9-utils_1%3a9.20.15-1~deb13u1_amd64.deb ...
Dépaquetage de bind9-utils (1:9.20.15-1~deb13u1) ...
Sélection du paquet dns-root-data précédemment désélectionné.
Préparation du dépaquetage de .../4-dns-root-data_2025080400~deb13u1_all.deb ...
Dépaquetage de dns-root-data (2025080400~deb13u1) ...
Sélection du paquet bind9 précédemment désélectionné.
Préparation du dépaquetage de .../5-bind9_1%3a9.20.15-1~deb13u1_amd64.deb ...
Dépaquetage de bind9 (1:9.20.15-1~deb13u1) ...
Paramétrage de bind9-libs:amd64 (1:9.20.15-1~deb13u1) ...
Paramétrage de dns-root-data (2025080400~deb13u1) ...
Paramétrage de bind9-utils (1:9.20.15-1~deb13u1) ...
Paramétrage de bind9 (1:9.20.15-1~deb13u1) ...
wrote key file "/etc/bind/rndc.key"
named-resolvconf.service is a disabled or a static unit, not starting it.
Created symlink '/etc/systemd/system/bind9.service' + '/usr/lib/systemd/system/named.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/named.service' + '/usr/lib/systemd/system/named.service'.
Paramétrage de bind9-host (1:9.20.15-1~deb13u1) ...
Paramétrage de bind9-dnsutils (1:9.20.15-1~deb13u1) ...
Traitement des actions différées (« triggers ») pour man-db (2.13.1-1) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.41-12) ...
root@DS1: ~#
```

Maintenant je démarre le service DNS bind avec la commande “ systemctl start bind9 ” :

```
root@DS1: ~#systemctl start bind9
root@DS1: ~#
```

La configuration DNS de base dans les fichiers /etc/bind/named.conf :

```
GNU nano 8.4 /etc/bind/named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.root-hints";
```

Je visualise les fichiers de configuration dans le répertoire /etc/bind/ :

```
root@DS1: ~#ls -l /etc/bind/
total 20
-rw-r--r-- 1 root bind 455 22 oct. 18:00 named.conf
-rw-r--r-- 1 root bind 42 22 oct. 18:00 named.conf.local
-rw-r--r-- 1 root bind 43 22 oct. 18:00 named.conf.options
-rw-r--r-- 1 root bind 116 22 oct. 18:00 named.conf.root-hints
-rw-r----- 1 bind bind 100 22 janv. 15:44 rndc.key
root@DS1: ~#
```

sauvegarde les 3 fichiers afin d'éviter toute mauvaise manipulation

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@DS1: ~#ls -l /etc/bind
total 32
-rw-r--r-- 1 root bind 455 22 oct. 18:00 named.conf
-rw-r--r-- 1 root bind 42 22 oct. 18:00 named.conf.local
-rw-r--r-- 1 root bind 42 22 janv. 15:59 named.conf.local.sauv
-rw-r--r-- 1 root bind 43 22 oct. 18:00 named.conf.options
-rw-r--r-- 1 root bind 43 22 janv. 15:59 named.conf.options.sauv
-rw-r--r-- 1 root bind 116 22 oct. 18:00 named.conf.root-hints
-rw-r--r-- 1 root bind 455 22 janv. 15:58 named.conf.sauv
-rw-r----- 1 bind bind 100 22 janv. 15:44 rndc.key
root@DS1: ~#_
```

- Vérifiez l'état du service bind avec la commande `systemctl status bind9` :

```
-rw-r----- 1 bind bind 100 22 janv. 15:44 rndc.key
root@DS1: ~#systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Thu 2026-01-29 15:15:44 CET; 3min 58s ago
  Invocation: c1edd01cc73542a49b902adc25cd4ba8
     Docs: man:named(8)
    Main PID: 848 (named)
      Status: "running"
        Tasks: 8 (limit: 2317)
       Memory: 33.3M (peak: 35.4M)
          CPU: 75ms
    CGroup: /system.slice/named.service
           └─848 /usr/sbin/named -f -u bind

Janv. 29 15:15:44 DS1 named[848]: network unreachable resolving './DNSKEY/IN': 2001:500:1::53#53
Janv. 29 15:15:44 DS1 named[848]: network unreachable resolving './NS/IN': 2001:500:1::53#53
Janv. 29 15:15:44 DS1 named[848]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
Janv. 29 15:15:44 DS1 named[848]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Janv. 29 15:15:44 DS1 named[848]: network unreachable resolving './DNSKEY/IN': 2001:500:2d::d#53
Janv. 29 15:15:44 DS1 named[848]: network unreachable resolving './NS/IN': 2001:500:2d::d#53
Janv. 29 15:15:44 DS1 named[848]: network unreachable resolving './DNSKEY/IN': 2801:1b8:10::b#53
Janv. 29 15:15:44 DS1 named[848]: network unreachable resolving './NS/IN': 2801:1b8:10::b#53
Janv. 29 15:15:54 DS1 named[848]: managed-keys-zone: Unable to fetch DNSKEY set '.': timed out
Janv. 29 15:15:54 DS1 named[848]: resolver priming query complete: timed out
root@DS1: ~#_
```

## 2.9. Zone de recherche directe et zone de recherche inversée

- Renseignez, dans le fichier `/etc/bind/named.conf.local`, le nom des zones ainsi que les fichiers de zone qui vont contenir les enregistrements :

```
GNU nano 8.4
//
// Do any local configuration here
//
zone "sio-exupery.local" IN {
    type master;
    file "do.sio.exupery.local";
    allow-update { none; };
};

zone "4.168.192.in-addr.arpa" IN {
    type master;
    file "rev.sio-exupery.local";
    allow-update { none; };
};
```

L'emplacement des fichiers de zone `db.sio-exupery.local` et `rev.sio-exupery.local` figure comme option avec la directive `directory` dans le fichier `named.conf.options` :

```
options {
    directory "/var/cache/bind";
};
```

## 2.10. Construction des fichiers de zone

- Créez le fichier `/var/cache/bind/db.sio-exupery.local` pour la zone de recherche directe dans lequel vous faites figurer les enregistrements correspondant à vos machines :

```
; Fichier pour la résolution directe
$TTL 86400
@ IN SOA DS1.sio-exupery.local. root.sio-exupery.local. (
    2026011301
    1w
    1d
    4w
    1W )
@ IN NS DS1.sio-exupery.local.
DS1 IN A 192.168.4.254
DD1 IN A 192.168.4.1
```

- Créez le fichier pour la résolution inverse `/var/cache/bind/rev.sio-exupery.local` dans lequel vous faites figurer les enregistrements de type PTR (pointeur) qui sont le contraire des enregistrements de type A et qui permettent donc de résoudre une adresse IP en nom d'hôte :

```
; Fichier pour la résolution inverse
$TTL 86400
@ IN SOA DS1.sio-exupery.local. root.sio-exupery.local. (
    2026011301
    1w
    1d
    4w
    1w )
@ IN NS DS1.sio-exupery.local.
254 IN PTR DS1.sio-exupery.local.
1 IN PTR DD1.sio-exupery.local.
```

Attribuez ces 2 fichiers de zone au groupe bind afin de les rendre accessibles au démon :

```
root@DS1: ~#chgrp bind /var/cache/bind/*
root@DS1: ~#chmod 664 /var/cache/bind/*
root@DS1: ~#
```

```
root@DS1: ~#chmod 664 /var/cache/bind/*
root@DS1: ~#ls -l /var/cache/bind
total 16
-rw-rw-r-- 1 root bind 212 29 janv. 15:36 db.sio-exupery.local
-rw-rw-r-- 1 bind bind 287 29 janv. 15:21 managed-keys.bind
-rw-rw-r-- 1 bind bind 1849 29 janv. 15:20 managed-keys.bind.jnl
-rw-rw-r-- 1 root bind 235 29 janv. 15:41 rev.sio-exupery.local
root@DS1: ~#
```

Vérifiez la même appartenance du groupe pour le répertoire :

```
root@DS1: ~#ls -ld /var/cache/bind
drwxrwxr-x 2 root bind 4096 29 janv. 15:41 /var/cache/bind
root@DS1: ~#
```

## 2.11.

### Démarrage et tests du service

▪ Modifiez le fichier /etc/hosts qui ne doit contenir que la référence à la boucle locale et le nom FQDN du serveur (laissez les lignes pour IPv6) :

```
127.0.0.1 localhost.localdomain localhost
127.0.1.1 DS1.sio-exupery.local DS1_

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Désactivez les deux interfaces enp0s3 et enp0s8 avec la commande ifdown puis modifiez le fichier /etc/network/interfaces pour qu'il contienne les directives dns-search, dns-domain et dns-nameservers :

```
root@DS1: ~#ifdown enp0s3
root@DS1: ~#ifdown enp0s8
root@DS1: ~#
```

```

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
address 172.17.101.213
netmask 255.255.0.0
network 172.17.0.0
broadcast 172.17.101.255
gateway 172.17.250.3

allow-hotplug enp0s8
iface enp0s8 inet static
address 192.168.4.254
netmask 255.255.255.0
network 192.168.4.0
broadcast 192.168.4.255
dns-search sio-exupery.local
dns-domain sio-exupery.local
dns-nameservers 192.168.4.254_

# This is an autoconfigured IPv6 interface
#iface enp0s3 inet6 auto

```

- Réactivez les deux interfaces avec la commande ifup puis vérifiez que le fichier /etc/resolv.conf indique bien l'adresse IP du serveur DNS ainsi que la zone de recherche DNS :

```

root@DS1: ~#ifup enp0s3
root@DS1: ~#ifup enp0s8
root@DS1: ~#cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.4.254
search sio-exupery.local
root@DS1: ~#

```

- Relancez le service bind9 et vérifiez l'état du service :

```

search sio-exupery.local
root@DS1: ~#systemctl restart bind9
root@DS1: ~#systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Thu 2026-01-29 15:55:55 CET; 28s ago
 Invocation: f2ad90d5429946168a3d14f0670a1d
    Docs: man:named(8)
   Main PID: 1250 (named)
    Status: "running"
     Tasks: 6 (limit: 2317)
    Memory: 24.3M (peak: 26.4M)
       CPU: 42ms
    CGroup: /system.slice/named.service
           └─1250 /usr/sbin/named -f -u bind

Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './DNSKEY/IN': 2001:503:ba3e::2:30#53
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './DNSKEY/IN': 2801:1b8:10::b#53
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './NS/IN': 2801:1b8:10::b#53
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './DNSKEY/IN': 2001:500:12::d0d#53
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
Janv. 29 15:56:05 DS1 named[1250]: managed-keys-zone: Unable to fetch DNSKEY set '.': timed out
Janv. 29 15:56:05 DS1 named[1250]: resolver priming query complete: timed out
root@DS1: ~#

```

- Deuxième test : lancez l'utilitaire de vérification named-checkconf qui vérifie le fichier /etc/bind/named.conf (si c'est bon, il ne retourne rien). Lancez ensuite le deuxième utilitaire de vérification named-checkzone sur vos fichiers de zone /var/cache/bind/db.sio-exupery.local et /var/cache/bind/rev.sio-exupery.local. Il renvoie normalement le message figurant ci-dessous :

```

root@DS1: /etc/bind#named-checkconf /var/cache/bind
root@DS1: /var/cache/bind#named-checkzone -d sio-exupery.local db.sio-exupery.local
loading "sio-exupery.local" from "db.sio-exupery.local" class "IN"
zone sio-exupery.local/IN: loaded serial 2026011301
OK
root@DS1: /var/cache/bind#named-checkzone -d 4.168.192.in-addr.arpa rev.sio-exupery.local
loading "4.168.192.in-addr.arpa" from "rev.sio-exupery.local" class "IN"
zone 4.168.192.in-addr.arpa/IN: loaded serial 2026011301
OK
root@DS1: /var/cache/bind#

```

- Troisième test : ouvrez une autre console (Ctrl+Alt+F2), connectez-vous en tant que root et lancez la commande journalctl -f permettant de voir en temps réel le journal de base de systemd.

Systemd gère le lancement des processus au démarrage, leur arrêt ou leur redémarrage (cf. la commande systemctl), les logs système, la planification des tâches...

Journald est le daemon qui centralise l'historique des événements dans un journal (log) notamment les messages concernant l'activité des services du système. La commande journalctl permet d'afficher tous les logs ou uniquement celui spécifique à un service.

Le journal syslog n'est plus disponible, par défaut, depuis la version Debian 12 donc inutile de chercher à l'afficher avec la commande tail -f /var/log/syslog.

```

root@DS1: ~#journalctl -f
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './DNSKEY/IN': 2001:503:ba3e::2:30#53
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './DNSKEY/IN': 2801:1b8:10::b#53
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './NS/IN': 2801:1b8:10::b#53
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './DNSKEY/IN': 2001:500:12::d0d#53
Janv. 29 15:55:55 DS1 named[1250]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
Janv. 29 15:56:05 DS1 named[1250]: managed-keys-zone: Unable to fetch DNSKEY set '.': timed out
Janv. 29 15:56:05 DS1 named[1250]: resolver priming query complete: timed out

```

- Revenez sur la première console (Ctrl+Alt+F1) et relancez le service bind9 :

```

root@DS1: ~#systemctl restart bind9
root@DS1: ~#

```

- Observez sur la seconde console la sortie des messages de log pour le service bind9. Vous devez voir si le service a démarré ou s'il indique des erreurs.

```

Janv. 29 16:24:37 DS1 named[1377]: automatic empty zone: HOME.ARPA
Janv. 29 16:24:37 DS1 named[1377]: automatic empty zone: RESOLVER.ARPA
Janv. 29 16:24:37 DS1 named[1377]: configuring command channel from '/etc/bind/rndc.key'
Janv. 29 16:24:37 DS1 named[1377]: command channel listening on 127.0.0.1#953
Janv. 29 16:24:37 DS1 named[1377]: configuring command channel from '/etc/bind/rndc.key'
Janv. 29 16:24:37 DS1 named[1377]: command channel listening on ::1#953
Janv. 29 16:24:37 DS1 named[1377]: managed-keys-zone: loaded serial 17
Janv. 29 16:24:37 DS1 named[1377]: zone 4.168.192.in-addr.arpa/IN: loaded serial 2026011301
Janv. 29 16:24:37 DS1 named[1377]: zone sio-exupery.local/IN: loading from master file db.sio.exupery.local failed: fi
Janv. 29 16:24:37 DS1 named[1377]: zone sio-exupery.local/IN: not loaded due to errors.
Janv. 29 16:24:37 DS1 named[1377]: all zones loaded
Janv. 29 16:24:37 DS1 named[1377]: FIPS mode is disabled
Janv. 29 16:24:37 DS1 named[1377]: running
Janv. 29 16:24:37 DS1 systemd[1]: Started named.service - BIND Domain Name Server.
Janv. 29 16:24:37 DS1 named[1377]: network unreachable resolving './DNSKEY/IN': 2801:1b8:10::b#53
Janv. 29 16:24:37 DS1 named[1377]: network unreachable resolving './DNSKEY/IN': 2001:7fd::1#53
Janv. 29 16:24:37 DS1 named[1377]: network unreachable resolving './NS/IN': 2001:7fd::1#53
Janv. 29 16:24:37 DS1 named[1377]: network unreachable resolving './DNSKEY/IN': 2001:500:9f::42#53
Janv. 29 16:24:37 DS1 named[1377]: network unreachable resolving './NS/IN': 2001:500:9f::42#53

```

## 2.12. Outils de test de résolution de noms

- Vérifiez la présence sur votre système du paquetage dnsutils installé à la suite de bind (cf. page 4) :

```

root@DS1: ~#systemctl restart bind9
root@DS1: ~#dpkg -l | grep -i dnsutils
ii bind9-dnsutils      1:9.20.15-1~deb13u1      amd64      Clients provided with BIND 9
root@DS1: ~#

```

- Saisissez la commande dig DD1.sio-exupery.local :