Chapitre 2 - Serveur Debian DS1 : installation du service DNS

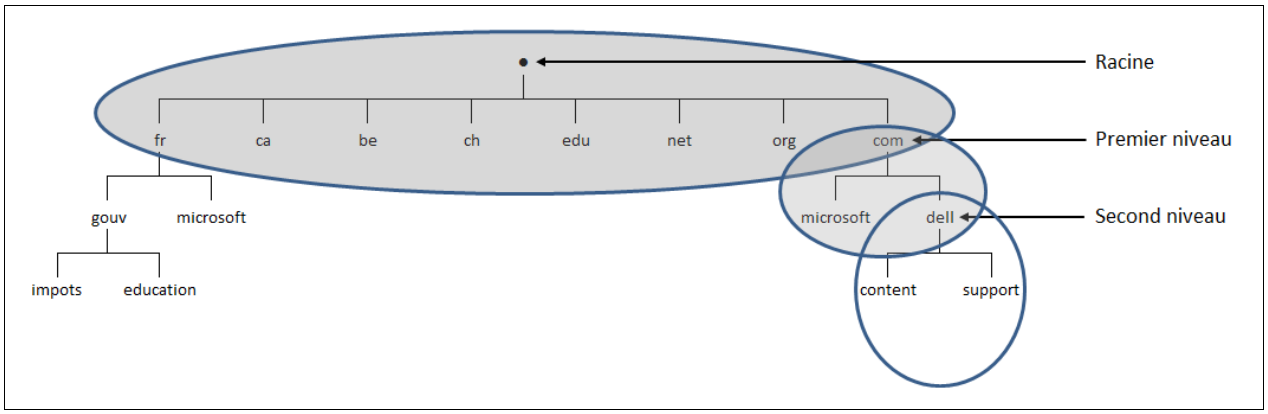
Après avoir installé le paquetage **BIND9** (**Berkeley Internet Name Domain**), vous allez mettre en place un service DNS sur le serveur DS1. Il fournira le service DNS principal d'une **zone** nommée **sio-exupery.local**. L'extension **.local** ne portera pas à confusion vis-à-vis des **serveurs racines**.

2.1. L'espace de noms Internet.

Le système DNS (Domain Name System) utilise un **espace de noms Internet**. Il se compose d'une **arborescence de domaines** dont le niveau le plus bas correspond à un **enregistrement**.

La **racine** de l'espace de noms Internet est représentée par un **point** sous lequel on trouve les **domaines de premier niveau** : **fr** et **com** sont quelques exemples de noms de domaine de premier niveau. L'**IANA** gère la racine et coordonne la délégation des noms de domaine de premier niveau auprès d'organismes. Par exemple, l'**AFNIC** gère le domaine **fr**.
Les entreprises ou les particuliers peuvent acheter un nom de domaine à partir du **second niveau**.
Elles peuvent alors ajouter des **sous-domaines** ou des **enregistrements** en fonction de leurs besoins.

Ce sont des **serveurs DNS différents** qui gèrent les différents niveaux. La figure ci-dessous montre l'organisation hiérarchique de l'espace de noms Internet et la **gestion des zones** à l'aide des **serveurs DNS** :



On appelle **FQDN** (Fully Qualified Domain Name) le nom complet identifiant un enregistrement depuis l'enregistrement jusqu'à la racine. Chaque point étant un séparateur de niveau hiérarchique et la lecture se fait de droite (racine) à gauche (enregistrement). Par exemple, **www.ac-nice.fr.** est un FQDN où :

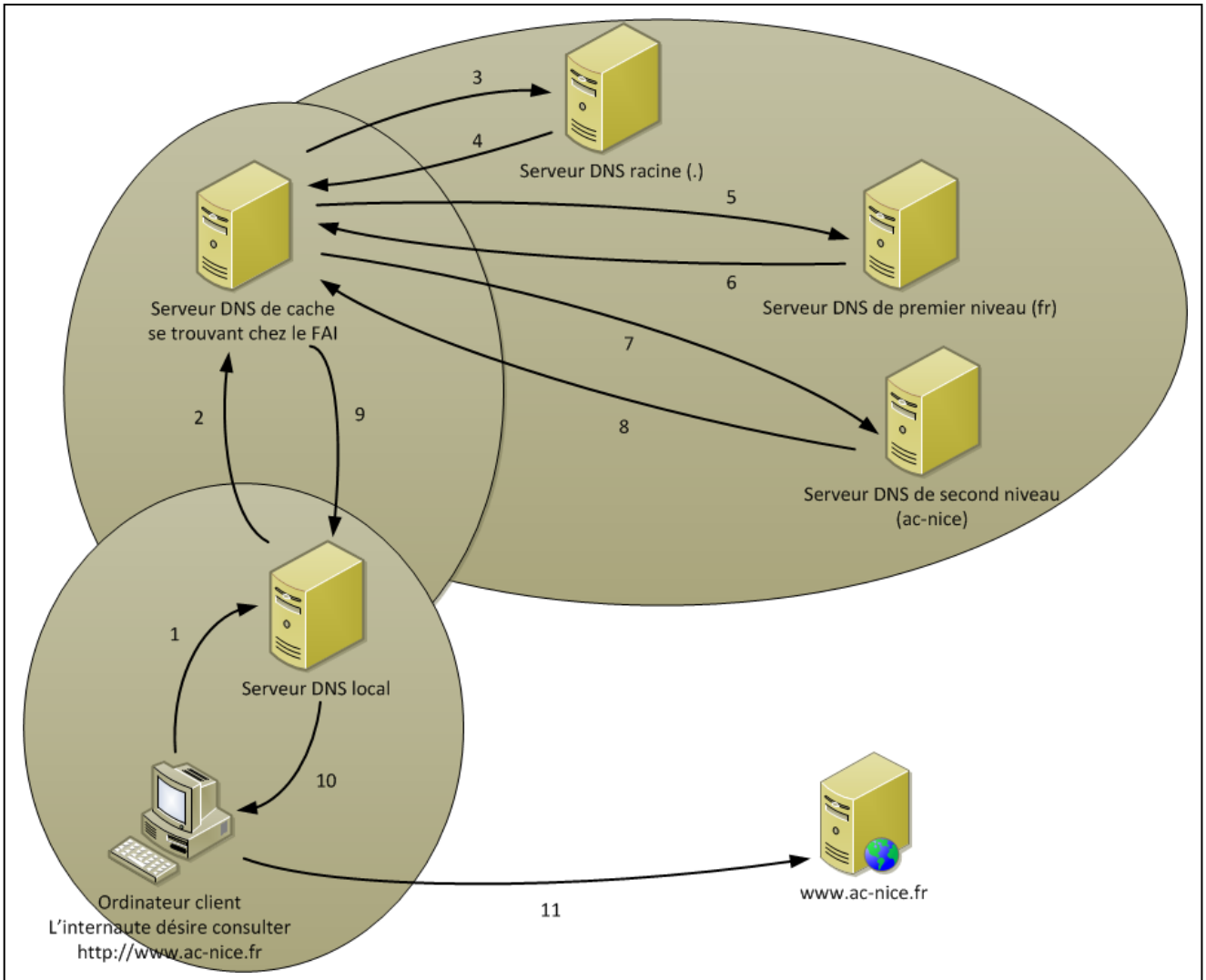
- **.** (point) représente la racine.
- **fr** représente le nom de domaine de premier niveau.
- **ac-nice** représente le nom de domaine de second niveau.
- **www** représente un enregistrement dans la zone, ici un enregistrement de type hôte.

Dans un navigateur Internet, le point symbolisant la racine est ajouté automatiquement à la fin de l'URL.

2.2. La résolution d'un nom Internet en adresse IP.

Pour résoudre un nom en adresse IP, il faut utiliser un résolveur ; celui-ci peut travailler soit de manière récursive, soit de manière itérative. Le **mode récursif** est surtout utilisé par les ordinateurs clients qui font une requête et attendent une réponse de type résolu ou non résolu. Le **mode itératif** est utilisé par les serveurs DNS qui ont la charge de localiser un hébergeur potentiel de la zone recherchée en commençant par la racine.

La figure ci-dessous illustre la procédure suivie pour qu'un ordinateur client reçoive l'adresse IP pour le nom considéré :



L'ordinateur client veut afficher le site www.ac-nice.fr dans son navigateur. Si l'adresse IP correspondante ne se trouve pas déjà dans le cache DNS de l'ordinateur client, ce dernier effectue une **requête récursive** auprès du serveur DNS du réseau local (1).
Le serveur DNS local reçoit la requête du client ; comme il ne fait pas autorité pour la zone, et si l'adresse IP ne figure pas déjà dans son cache, le serveur DNS local effectue une **demande récursive** auprès du serveur DNS de cache de son fournisseur d'accès Internet (2).
Le serveur DNS du fournisseur d'accès Internet ne trouve pas l'adresse dans son cache ; il effectue alors une **requête itérative** auprès des serveurs racine (3).
Un serveur racine répond en disant de contacter le serveur gérant le premier niveau du domaine fr ; il lui fournit l'adresse IP du serveur (4).
Le serveur DNS de cache contacte alors le serveur DNS de premier niveau avec une **requête itérative** (5).
Le serveur DNS de premier niveau répond en disant de contacter le serveur gérant le domaine de second niveau ac-nice ; il lui fournit l'adresse IP du serveur (6).
Le serveur DNS de cache contacte alors le serveur DNS de second niveau avec une **demande itérative** (7) : « possèdes-tu un enregistrement **www** dans ton domaine **ac-nice.fr ?** »
Le serveur DNS de second niveau répond en fournissant l'adresse IP pour le nom www.ac-nice.fr (8). L'adresse est maintenant résolue.
Le serveur DNS de cache du fournisseur Internet renvoie la réponse auprès du serveur de cache du réseau local (9) après l'avoir stockée dans son cache. Elle sera utilisée pour les demandes ultérieures et restera dans le cache pendant la durée de vie (TTL) de l'enregistrement.

Le serveur DNS de cache du réseau local renvoie la réponse auprès du client (10) après l'avoir stockée dans son cache. Elle sera utilisée pour les demandes ultérieures et restera dans le cache pendant la durée de vie (TTL) de l'enregistrement.
Enfin, l'ordinateur client reçoit la réponse et la stocke dans son cache DNS local afin d'être réutilisée ultérieurement tant que le TTL est plus grand que 0. Il peut maintenant contacter le site Web www.ac-nice.fr dont il connaît l'adresse IP.

2.3. DNS et réseau local

Le serveur et les stations ont besoin d'un serveur DNS dans le réseau local. Lorsqu'un ordinateur du réseau veut résoudre le nom du serveur ou d'un autre ordinateur du réseau, il s'adresse au serveur DNS déclaré dans ses propriétés réseau.

Imaginons que nous mettions dans le paramétrage TCP/IP des stations, l'adresse du serveur DNS du FAI. Les stations s'adresseraient au DNS du FAI pour résoudre les noms des ordinateurs du réseau local. Le fournisseur d'accès n'ayant pas ces informations, les stations vont mal fonctionner et des lenteurs seront inévitables.

En mettant, dans le paramétrage TCP/IP des stations, l'adresse IP du serveur DNS local, DS1 en l'occurrence, les stations trouveront rapidement le serveur et les autres stations du réseau. Il reste le problème de la résolution des noms de domaine Internet. Le serveur DNS DS1 s'appuiera sur le serveur DNS « au-dessus de lui » c'est-à-dire Roi (172.17.254.1) - ou votre box à la maison - (cf. instructions **forward** et **forwarders**) qui s'adressera à son tour au serveur DNS du FAI.

2.4. Serveur DNS de cache

Un serveur DNS de cache assure une résolution de noms mais ne dispose pas localement de zones DNS. Il se contente de relayer les demandes vers d'autres serveurs. Ce serveur mettra en cache pour une durée déterminée toutes les résolutions enregistrées.

2.5. Serveurs racine.

Chaque serveur DNS dispose d'une liste des serveurs racine. L'organisme IANA (Internet Assigned Numbers Authority) gère la liste de ces serveurs. Actuellement, ils sont au nombre de 13, disséminés un peu partout dans le monde. Leur nom est de type **lettre.root-servers.net** où « lettre » peut avoir une valeur allant de « a » à « m ».
La liste des serveurs racines figure dans le fichier **/usr/share/dns/root.hints** (il n'est pas conseillé de modifier ou de supprimer ces serveurs).

```
.                       3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.     3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     199.9.14.201
B.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:200::b
;
; FORMERLY C.PSI.NET
;
.                       3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000      A     192.33.4.12
C.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:2::c
```

2.6. Avant l'installation du service

En l'absence de DNS, le fichier **/etc/hosts** de chaque machine permet de renseigner manuellement la correspondance entre l'adresse IP et le nom de la machine. C'est le fichier de configuration du service de nom local. Les adresses indiquées ne sont connues que du poste :

```
 GNU nano 2.7.4                          Fichier : /etc/hosts

127.0.0.1       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
```

2.7. Les fichiers

Vous utiliserez les fichiers suivants :

- Le fichier **/etc/hosts** : comporte l'association IP-nom FQDN du serveur ;
- Le fichier **/etc/resolv.conf** : indique le domaine à rechercher et le **serveur DNS** associé ;
- Le fichier **/etc/hostname** : contient le nom de la machine ;
- Le répertoire **/etc/bind/** : contient la configuration générale du serveur DNS avec les fichiers associés ;
- Les **fichiers de zones** contenant les **enregistrements** : figurent dans **/var/cache/bind/**.

2.8. Installation du paquetage BIND

- Installez le paquetage **BIND** et ses dépendances :

```
root@DS1: ~#apt-get install bind9
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  bind9-utils dns-root-data
Paquets suggérés :
  bind9-doc ufw
Les NOUVEAUX paquets suivants seront installés :
  bind9 bind9-utils dns-root-data
0 mis à jour, 3 nouvellement installés, 0 à enlever et 21 non mis à jour.
Il est nécessaire de prendre 444 kB dans les archives.
Après cette opération, 1 672 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
```

Le paquet dnsutils est installé avec bind9 (cf. page 10)

L'utilisateur bind ainsi que le groupe bind sont créés.

- Démarrez le service DNS bind avec la commande **systemctl start bind9** :

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

- Le service DNS démarre suivant une configuration de base située dans les fichiers :
  - **/etc/bind/named.conf** : fichier général incluant les deux fichiers ci-après ;

```
 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";
```

  - **/etc/bind/named.conf.options** : fichier contenant les options de BIND9 ;
  - **/etc/bind/named.conf.local** : fichier contenant les noms des zones de recherche directe et inversée ainsi que l'indication des fichiers de zone correspondants (vides pour l'instant).
- Visualisez ces 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 12 janv. 14:27 rndc.key
root@DS1: ~#_
```

- Sauvegardez ces trois fichiers afin de pallier toute mauvaise manipulation :

```
root@DS1 ~ #cd /etc/bind
root@DS1 /etc/bind #cp named.conf named.conf.sauv
root@DS1 /etc/bind #cp named.conf.options named.conf.options.sauv
root@DS1 /etc/bind #cp named.conf.local named.conf.local.sauv
root@DS1 /etc/bind #_
```

- Vérifiez l'état du service bind avec la commande **systemctl status 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 Mon 2026-01-12 14:27:29 CET; 7min ago
 Invocation: 4b457449519cc41a095a37ab5b6414875
       Docs: man:named(8)
   Main PID: 1233 (named)
     Status: "running"
      Tasks: 8 (limit: 2303)
     Memory: 29.4M (peak: 31.8M)
        CPU: 156ms
     CGroup: /system.slice/named.service
             └─1233 /usr/sbin/named -f -u bind

janv. 12 14:27:29 DS1 named[1233]: command channel listening on 127.0.0.1#953
janv. 12 14:27:29 DS1 named[1233]: configuring command channel from '/etc/bind/rndc.key'
janv. 12 14:27:29 DS1 named[1233]: command channel listening on ::1#953
janv. 12 14:27:29 DS1 named[1233]: managed-keys-zone: loaded serial 0
janv. 12 14:27:29 DS1 named[1233]: all zones loaded
janv. 12 14:27:29 DS1 named[1233]: FIPS mode is disabled
janv. 12 14:27:29 DS1 systemd[1]: Started named.service - BIND Domain Name Server.
janv. 12 14:27:29 DS1 named[1233]: running
janv. 12 14:27:39 DS1 named[1233]: resolver priming query complete: timed out
janv. 12 14:27:39 DS1 named[1233]: managed-keys-zone: Unable to fetch DNSKEY set '.': timed out
root@DS1: ~#_
```

Après chaque modification des fichiers de configuration, il sera nécessaire pour sa prise en compte de relancer le service bind avec la commande habituelle **systemctl restart bind9**.

2.9. Zone de recherche directe et zone de recherche inversée

Une **zone de recherche directe** permet de résoudre des noms de domaine en adresses IP (résolution directe) tandis qu'une **zone de recherche inversée** permet de résoudre des adresses IP en noms DNS (résolution inverse).

- 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                                  /etc/bind/named.conf.local
//
// Do any local configuration here
//
zone "sio-exupery.local" IN {
        type master;
        file "db.sio-exupery.local";
        allow-update { none; };
};

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

→ Le nom de la zone de recherche inversée s'établit à partir de l'ID réseau (ordre inversé) auquel est accolé le nom d'un domaine spécial **in-addr.arpa** soit **4.168.192.in-addr.arpa** dans le cas présent.

→ 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** :

```
 GNU nano 8.4                                    /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";
};
```

→ L'instruction **allow-update { none ; }** n'autorise pas les mises à jour dynamiques, dans les fichiers **db** et **rev**, des enregistrements DNS des stations clientes via le serveur DHCP. Vous devez donc mettre à jour ces enregistrements manuellement dans un premier temps.

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 faîtes figurer les enregistrements correspondant à vos machines :

```
 GNU nano 8.4                                    /var/cache/bind/db.sio-exupery.local
; 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
```

DS1 est le serveur Start Of Authority ayant la responsabilité de la zone sio-exupery.local

@ correspond au nom de la zone « sio-exupery.local » figurant dans le fichier /etc/bind/named.conf.local

Ce fichier a un format très strict comme indiqué ci-dessous. Veillez donc à bien renseigner le fichier de zone.

```
$TTL ttl
nomzone   IN   SOA   serveur mailadmin (
                serial
                refresh
                retry
                expire
                negative )
nomzone   IN   NS   serveur
```

→ **TTL** : durée de conservation en secondes des données en mémoire cache.

→ **Nomzone** : FQDN de la zone gérée par ce fichier (le nom de la zone doit se terminer par un point). Il est souvent remplacé par un arobase (@) pour alléger le fichier.

→ **Mailadmin** : adresse e-mail de l'administrateur du serveur. L'arobase étant un caractère réservé dans les fichiers de zone, il est conventionnellement remplacé par un point.

→ **Serial**, **refresh**, **retry** et **expire** : valeurs numériques utilisées quand la zone est répliquée lorsqu'il y a plusieurs serveurs DNS.

Notez que le numéro de série mentionné dans l'exemple ci-dessus se compose de la date du jour lors de la création du fichier ainsi que d'un numéro d'index qui sert pour les échanges avec un serveur secondaire (10 caractères).

→ **Negative** : indique combien de temps le serveur doit conserver en cache une réponse négative.

→ Un **enregistrement** représente un **hôte** se situant dans la zone. Les ordinateurs peuvent s'inscrire **dynamiquement**, par l'intermédiaire d'un serveur DHCP, ou **manuellement** grâce à un administrateur.

- Les enregistrements pour résoudre un nom d'hôte en adresse IPv4 sont de type **A**.
- Un enregistrement de type **AAAA** fait correspondre à un nom une adresse IPv6.

- L'enregistrement de type **SOA** (**Start Of Authority** ou début d'autorité) indique le serveur ayant la responsabilité de la zone. Toute zone fonctionnelle a un enregistrement SOA.
- Les enregistrements de type **NS** (**Name Server** ou serveur de noms) indiquent les serveurs de noms pour la zone. Toute zone fonctionnelle a au moins un enregistrement NS.

- 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 :

```
  GNU nano 8.4                                    /var/cache/bind/rev.sio-exupery.local
; 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.
```

La zone de recherche inversée « 4.168.192.in-addr.arpa », figurant dans le fichier /etc/bind/named.conf.local, contient le Net-ID dans son nom

- 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 ~ #ls -l /var/cache/bind
total 16
-rw-rw-r-- 1 root bind  233 janv. 10 20:57 db.sio-exupery.local
-rw-rw-r-- 1 bind bind 1421 janv. 10 19:32 managed-keys.bind
-rw-rw-r-- 1 bind bind  512 janv. 10 19:32 managed-keys.bind.jnl
-rw-rw-r-- 1 root bind  266 janv. 10 21:19 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 janv. 10 21:19 /var/cache/bind
root@DS1 ~ #_
```

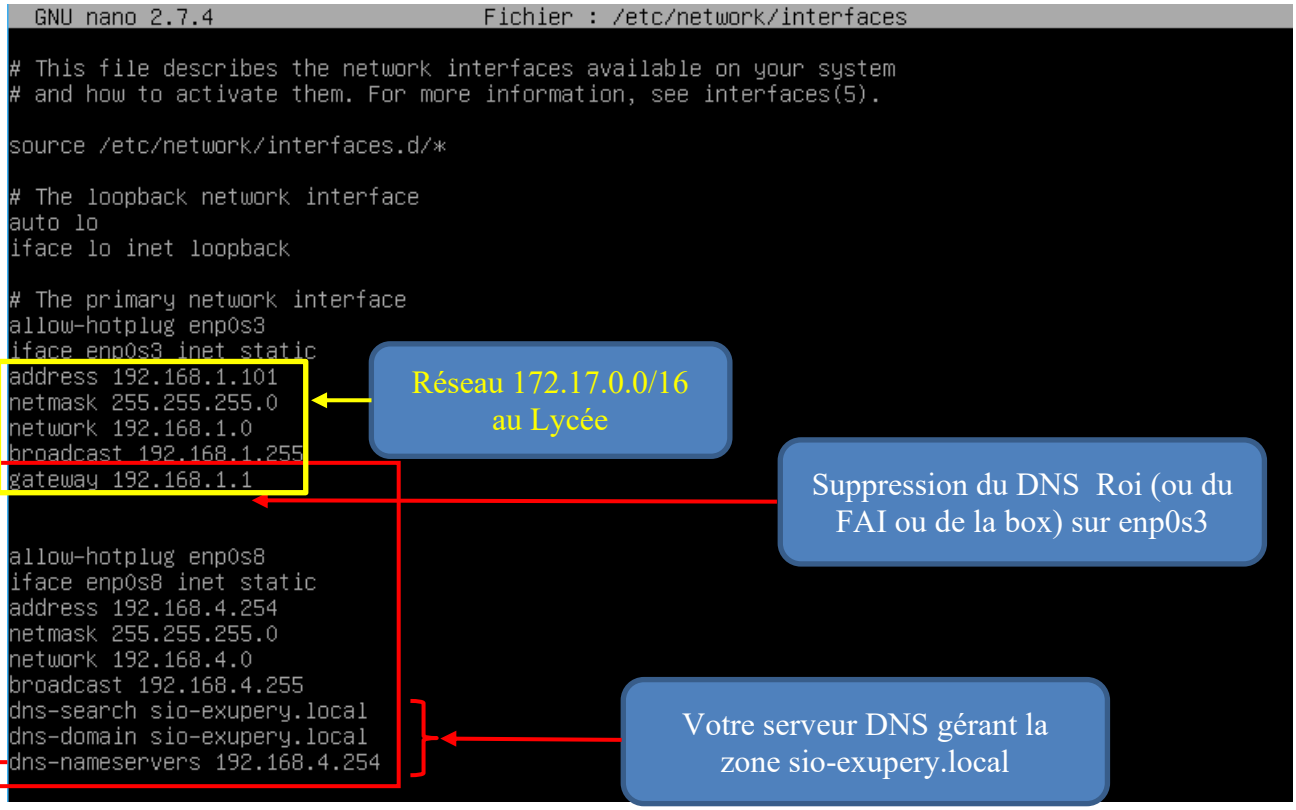
2.11. Démarrage et tests du service

- 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) :

```
  GNU nano 2.7.4                          Fichier : /etc/hosts

127.0.0.1       localhost.localdomain   localhost
192.168.4.254   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: ~#
```



- 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 :

```
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 Mon 2026-01-12 16:28:49 CET; 16s ago
 Invocation: 029b77af47cc46d0ab35d55ab00378f8
       Docs: man:named(8)
   Main PID: 1499 (named)
     Status: "running"
      Tasks: 6 (limit: 2303)
     Memory: 24.4M (peak: 26.6M)
        CPU: 52ms
     CGroup: /system.slice/named.service
             └─1499 /usr/sbin/named -f -u bind

janv. 12 16:28:49 DS1 named[1499]: command channel listening on ::1#953
janv. 12 16:28:49 DS1 named[1499]: managed-keys-zone: loaded serial 7
janv. 12 16:28:49 DS1 named[1499]: zone 4.168.192.in-addr.arpa/IN: loaded serial 2026011301
janv. 12 16:28:49 DS1 named[1499]: zone sio-exupery.local/IN: loaded serial 2026011301
janv. 12 16:28:49 DS1 named[1499]: all zones loaded
janv. 12 16:28:49 DS1 named[1499]: FIPS mode is disabled
janv. 12 16:28:49 DS1 named[1499]: running
janv. 12 16:28:49 DS1 systemd[1]: Started named.service - BIND Domain Name Server.
janv. 12 16:28:59 DS1 named[1499]: managed-keys-zone: Unable to fetch DNSKEY set '.': timed out
janv. 12 16:28:59 DS1 named[1499]: 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: ~#cd /etc/bind
root@DS1: /etc/bind#named-checkconf
root@DS1: /etc/bind#cd /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#
```

```
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 évènements 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. 12 16:30:01 DS1 CRON[1510]: pam_unix(cron:session): session closed for user root
janv. 12 16:30:37 DS1 systemd[1]: Started anacron.service - Run anacron jobs.
janv. 12 16:30:37 DS1 anacron[1514]: Anacron 2.3 started on 2026-01-12
janv. 12 16:30:37 DS1 anacron[1514]: Normal exit (0 jobs run)
janv. 12 16:30:37 DS1 systemd[1]: anacron.service: Deactivated successfully.
janv. 12 16:40:58 DS1 systemd[1]: Started getty@tty2.service - Getty on tty2.
janv. 12 16:41:04 DS1 login[1528]: pam_unix(login:session): session opened for user root(uid=0) by root(uid=0)
janv. 12 16:41:04 DS1 systemd-logind[685]: New session 9 of user root.
janv. 12 16:41:04 DS1 systemd[1]: Started session-9.scope - Session 9 of User root.
janv. 12 16:41:04 DS1 login[1528]: ROOT LOGIN ON tty2
_
```

- 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. 12 16:42:19 DS1 named[1552]: configuring command channel from '/etc/bind/rndc.key'
janv. 12 16:42:19 DS1 named[1552]: command channel listening on 127.0.0.1#953
janv. 12 16:42:19 DS1 named[1552]: configuring command channel from '/etc/bind/rndc.key'
janv. 12 16:42:19 DS1 named[1552]: command channel listening on ::1#953
janv. 12 16:42:19 DS1 named[1552]: managed-keys-zone: loaded serial 8
janv. 12 16:42:19 DS1 named[1552]: zone 4.168.192.in-addr.arpa/IN: loaded serial 2026011301
janv. 12 16:42:19 DS1 named[1552]: zone sio-exupery.local/IN: loaded serial 2026011301
janv. 12 16:42:19 DS1 named[1552]: all zones loaded
janv. 12 16:42:19 DS1 named[1552]: FIPS mode is disabled
janv. 12 16:42:19 DS1 named[1552]: running
janv. 12 16:42:19 DS1 systemd[1]: Started named.service - BIND Domain Name Server.
janv. 12 16:42:29 DS1 named[1552]: managed-keys-zone: Unable to fetch DNSKEY set '.': timed out
janv. 12 16:42:29 DS1 named[1552]: resolver priming query complete: timed out
```

Il est rare de réussir une configuration DNS du premier coup. En cas de dysfonctionnement, reprenez l'activité depuis le début de la configuration du service DNS en contrôlant soigneusement la présence, la syntaxe (point, point-virgule ou accolade manquants par exemple) ainsi que les droits des fichiers de configuration.

2.12. Outils de test de résolution de noms

- **ping**

Même si ce n'est pas sa fonction première, **ping** peut tout à fait servir de test rudimentaire pour tester une résolution de noms. Quand on utilise ping pour tester une résolution de noms, c'est la traduction de l'adresse qui importe et non la réponse ICMP de la machine distante.

- **nslookup**

nslookup est l'outil le plus commun lors de l'interrogation des serveurs DNS pour une résolution de noms. Il est présent sur la plupart des plates-formes Unix et Windows.

- **dig**

dig est un outil plus récent que nslookup pour l'interrogation et le diagnostic des serveurs DNS. Il est le plus précis et le plus abouti des outils de test.

dig *@IP* ***nom*** *TYPE*

→ **nom** : le nom complet (**FQDN**) dont on veut assurer la résolution.
→ @IP (facultatif) : l'adresse IP du serveur DNS à interroger. En cas d'omission, les serveurs de noms interrogés sont ceux référencés dans /etc/resolv.conf.
→ TYPE (facultatif) : par défaut, dig fait des requêtes de type A (résolution ordinaire de nom en adresse IPv4). Le paramètre type s'il est précisé permet d'adresser des requêtes d'un autre type.

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

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

Vous allez utiliser la commande **dig** disponible avec l'installation du paquetage **dnsutils**.

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

```
root@DS1: ~#dig DD1.sio-exupery.local

; <<>> DiG 9.20.15-1~deb13u1-Debian <<>> DD1.sio-exupery.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: 9681
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 4db64accb50c370e0100000069656b2b3ec5b4cf05f50656 (good)
;; QUESTION SECTION:
;DD1.sio-exupery.local.         IN      A

;; ANSWER SECTION:
DD1.sio-exupery.local.  86400   IN      A       192.168.4.1

;; Query time: 0 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Mon Jan 12 22:44:11 CET 2026
;; MSG SIZE  rcvd: 94

root@DS1: ~#
```

- Saisissez la commande **dig SOA sio-exupery.local** :

```
root@DS1 ~ #dig SOA sio-exupery.local

; <<>> DiG 9.10.3-P4-Debian <<>> SOA sio-exupery.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38610
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sio-exupery.local.             IN      SOA

;; ANSWER SECTION:
sio-exupery.local.      86400   IN      SOA     DS1.sio-exupery.local. root.sio-exupery.local. 20190
11101 604800 86400 2419200 604800

;; AUTHORITY SECTION:
sio-exupery.local.      86400   IN      NS      DS1.sio-exupery.local.

;; ADDITIONAL SECTION:
DS1.sio-exupery.local.  86400   IN      A       192.168.4.254

;; Query time: 0 msec
;; SERVER: 192.168.4.254#53(192.168.4.254)
;; WHEN: Sun Jan 13 21:42:00 CET 2019
;; MSG SIZE  rcvd: 121
```

- Saisissez la commande **nslookup DS1** :

```
root@DS1 ~ #nslookup DS1
Server:         192.168.4.254
Address:        192.168.4.254#53

Name:   DS1.sio-exupery.local
Address: 192.168.4.254
```

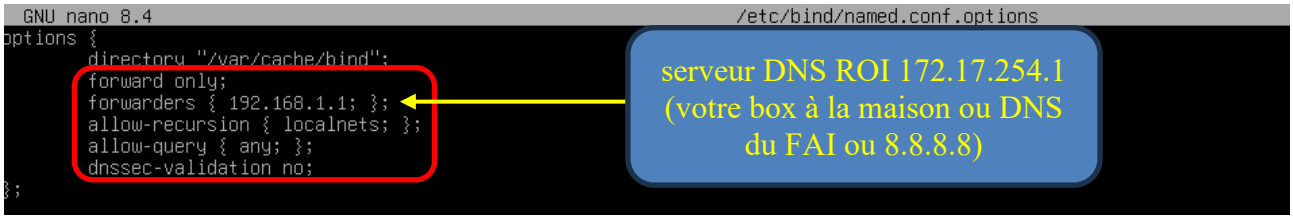
- Vérifiez enfin la résolution DNS interne avec :
  - un ping sur DS1.sio-exupery.local ;
  - un ping sur DD1.sio-exupery.local.

```
root@DS1: ~#ping -c 2 DS1
PING DS1.sio-exupery.local (192.168.4.254) 56(84) bytes of data.
64 bytes from DS1.sio-exupery.local (192.168.4.254): icmp_seq=1 ttl=64 time=0.072 ms
64 bytes from DS1.sio-exupery.local (192.168.4.254): icmp_seq=2 ttl=64 time=0.097 ms

--- DS1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1048ms
rtt min/avg/max/mdev = 0.072/0.084/0.097/0.012 ms
root@DS1: ~#ping -c 2 DD1
PING DD1.sio-exupery.local (192.168.4.1) 56(84) bytes of data.
64 bytes from DD1.sio-exupery.local (192.168.4.1): icmp_seq=1 ttl=64 time=2.51 ms
64 bytes from DD1.sio-exupery.local (192.168.4.1): icmp_seq=2 ttl=64 time=1.18 ms

--- DD1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1325ms
rtt min/avg/max/mdev = 1.181/1.845/2.509/0.664 ms
root@DS1: ~#
```

2.13. S'appuyer sur un DNS externe : la redirection

Pour l'instant, DS1 s'occupe des résolutions **internes** de la **zone sio-exupery.local**. La résolution **externe** sera dévolue au serveur DNS **« au-dessus de lui »**. Il faut, pour cela, que le serveur DS1 redirige ses requêtes vers le **serveur Roi** (la **box** ou le **serveur DNS du FAI** à la maison).

- Afin de mettre en place la redirection, modifiez avec l'éditeur de texte nano le fichier **/etc/bind/named.conf.options** :



Avec l'instruction **forward only**, toutes les requêtes ne concernant pas la zone **sio-exupery.local** seront redirigées obligatoirement vers le serveur DNS ROI (votre box à la maison) désigné par l'instruction **forwarders**.

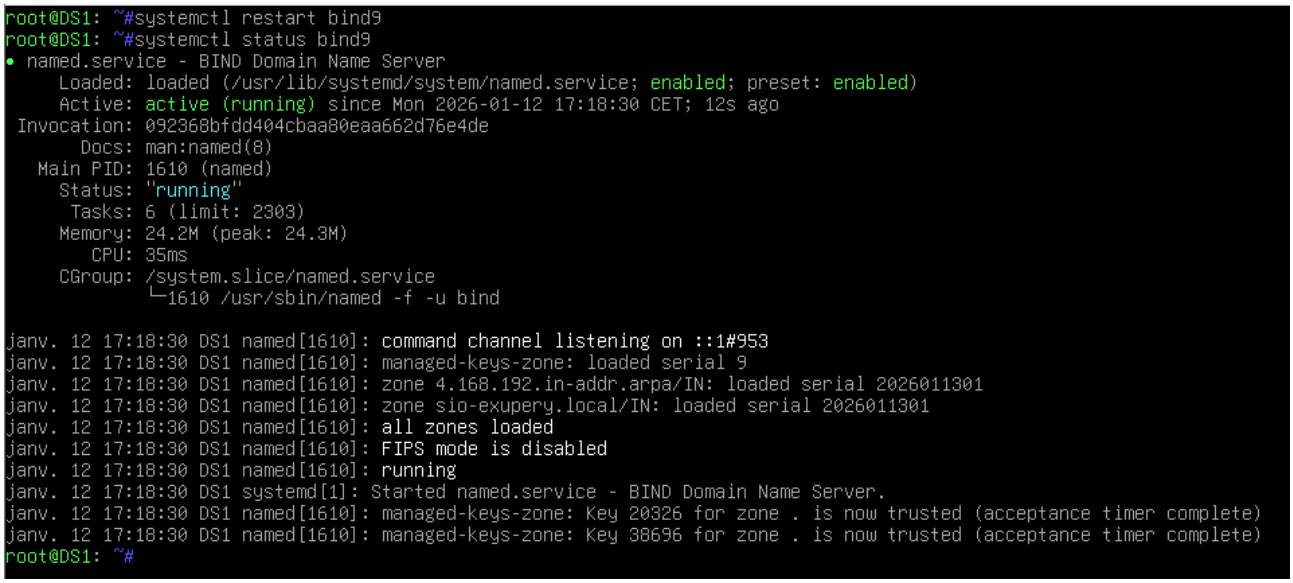
On autorise la possibilité de récursivité uniquement pour les réseaux locaux (interfaces du serveur) par l'instruction **allow-recursion**.

On ajoute également dans ce chapitre l'instruction **dnssec-validation no**.

> Pour plus d'explications concernant les extensions de sécurité du DNS, cf. la page de l'ICANN « DNSSEC – Qu'est-ce que c'est et pourquoi est-ce important ? » notamment la partie « Le DNS en soi n'est pas sécurisé » :
> https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-20-fr#

- Commentez les lignes ayant trait aux serveurs racines dans le fichier **/etc/bind/named.conf.root-hints** de façon à ce que le serveur DS1 ne puisse pas les importuner :

- Relancez le service DNS et vérifiez l'état du service Bind9 :



- Testez une résolution externe à partir du serveur DS1 avec la commande dig puis avec un ping :

```
root@DS1: ~#dig www.ac-nice.fr

; <<>> DiG 9.20.15-1~deb13u1-Debian <<>> www.ac-nice.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14874
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c385a3350c595d590100000069651f26677aa3337987d851 (good)
;; QUESTION SECTION:
;www.ac-nice.fr.                        IN      A

;; ANSWER SECTION:
www.ac-nice.fr.         3600    IN      CNAME   www.ac-nice.fr.cdn.cloudflare.net.
www.ac-nice.fr.cdn.cloudflare.net. 299 IN A     141.101.90.104
www.ac-nice.fr.cdn.cloudflare.net. 299 IN A     141.101.90.107
www.ac-nice.fr.cdn.cloudflare.net. 299 IN A     141.101.90.106
www.ac-nice.fr.cdn.cloudflare.net. 299 IN A     141.101.90.105

;; Query time: 431 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Mon Jan 12 17:19:50 CET 2026
;; MSG SIZE  rcvd: 182

root@DS1: ~#
```

```
root@DS1: ~#ping www.dunod.com
PING www.dunod.com (51.144.190.143) 56(84) bytes of data.
64 bytes from 51.144.190.143: icmp_seq=1 ttl=112 time=36.9 ms
64 bytes from 51.144.190.143: icmp_seq=2 ttl=112 time=36.7 ms
64 bytes from 51.144.190.143: icmp_seq=3 ttl=112 time=36.5 ms
^C
--- www.dunod.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2338ms
rtt min/avg/max/mdev = 36.521/36.701/36.924/0.167 ms
root@DS1: ~#_
```

2.14. Test à partir du client Debian Desktop

- Démarrez le client Debian DD1 et connectez-vous en root depuis le terminal :

```
sio@DEB13: ~
sio@DEB13:~$ su -
Mot de passe :
root@DEB13:~#
```

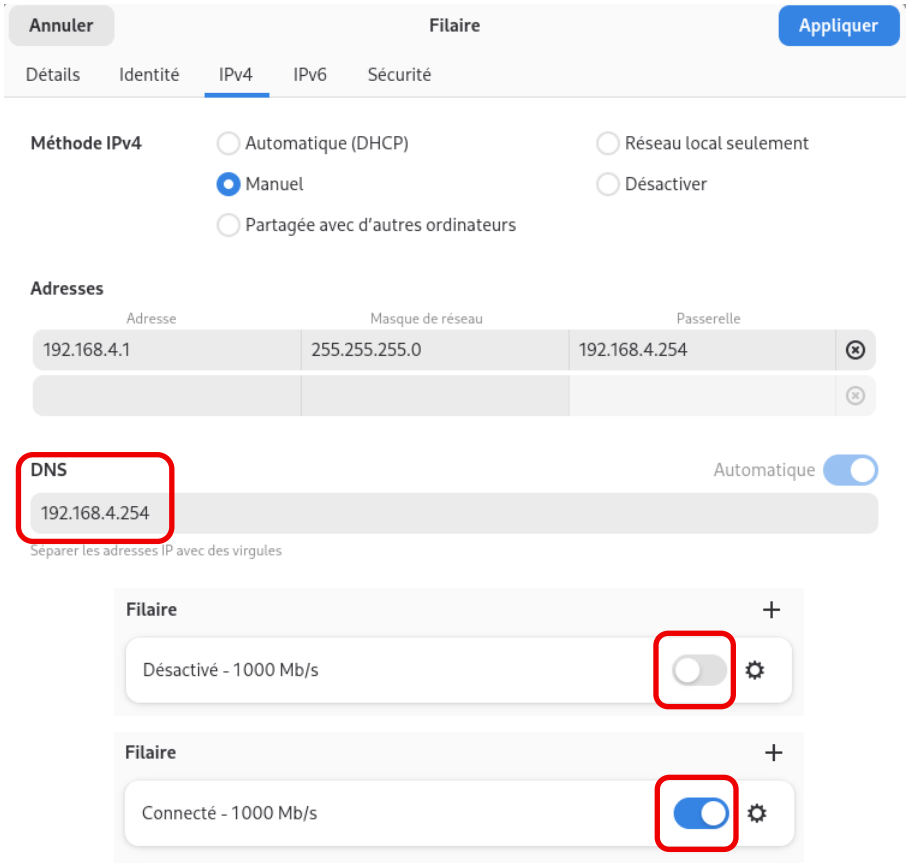
- Modifiez le nom de l'ordinateur dans le fichier **/etc/hostname** :

```
sio@DEB13: ~
 GNU nano 8.4                    /etc/hostname
DD1
```

- Modifiez l'association IP-nom FQDN dans le fichier **/etc/hosts** puis redémarrez ensuite la machine DD1 :

```
sio@DEB13: ~
 GNU nano 8.4                     /etc/hosts *
127.0.0.1       localhost
127.0.1.1       DD1.sio-exupery.local   DD1

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

- Via l'interface Network Manager, modifiez l'adresse du serveur DNS qui n'est plus ROI (ou la box à la maison) mais le serveur DS1 :



- Vérifiez la configuration réseau :

```
sio@DD1:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:a2:36:44 brd ff:ff:ff:ff:ff:ff
    altname enx080027a23644
    inet 192.168.4.1/24 brd 192.168.4.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fea2:3644/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
sio@DD1:~$
```

```
sio@DD1:~$ ip r
default via 192.168.4.254 dev enp0s3 proto static metric 100
192.168.4.0/24 dev enp0s3 proto kernel scope link src 192.168.4.1 metric 100
sio@DD1:~$
```

- Le fichier **/etc/resolv.conf** doit mentionner l'adresse du serveur DNS DS1 :

```
sio@DD1:~$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 192.168.4.254
sio@DD1:~$
```

- Saisissez successivement les commandes **dig SOA sio-exupery.local**, **dig DS1.sio-exupery.local** puis **dig www.dunod.com**.

```
sio@DD1:~$ dig SOA sio-exupery.local

; <<>> DiG 9.20.11-4-Debian <<>> SOA sio-exupery.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: 5005
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 9f56229ae26986230100000006965635997b822d79faab1e6 (good)
;; QUESTION SECTION:
;sio-exupery.local.             IN      SOA

;; ANSWER SECTION:
sio-exupery.local.      86400   IN      SOA     DS1.sio-exupery.local. root.sio-exuper
y.local. 2026011301 604800 86400 2419200 604800

;; Query time: 0 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Mon Jan 12 22:10:50 CET 2026
;; MSG SIZE  rcvd: 119
```

```
sio@DD1:~$ dig DS1.sio-exupery.local

; <<>> DiG 9.20.11-4-Debian <<>> DS1.sio-exupery.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: 54910
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 6a9aa4f31ed5badf010000006965640daa672350a92362f0 (good)
;; QUESTION SECTION:
;DS1.sio-exupery.local.         IN      A

;; ANSWER SECTION:
DS1.sio-exupery.local.  86400   IN      A       192.168.4.254

;; Query time: 4 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Mon Jan 12 22:13:50 CET 2026
;; MSG SIZE  rcvd: 94
```

```
sio@DD1:~$ dig www.dunod.com

; <<>> DiG 9.20.11-4-Debian <<>> www.dunod.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38411
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0a7f9cdc6cabb80c01000000696566bc61a7fe0562c14888 (good)
;; QUESTION SECTION:
;www.dunod.com.                 IN      A

;; ANSWER SECTION:
www.dunod.com.          5202    IN      A       51.144.190.143

;; Query time: 200 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Mon Jan 12 22:25:15 CET 2026
;; MSG SIZE  rcvd: 86
```

- Saisissez la commande **nslookup www.google.com**

```
sio@DD1:~$ nslookup www.google.com
Server:         192.168.4.254
Address:        192.168.4.254#53

Non-authoritative answer:
Name:   www.google.com
Address: 216.58.214.164
Name:   www.google.com
Address: 2a00:1450:4007:80e::2004

sio@DD1:~$
```

- Faites un **ping** sur DS1.

```
root@DD1:~# ping -c 2 DS1.sio-exupery.local
PING DS1.sio-exupery.local (192.168.4.254) 56(84) bytes of data.
64 bytes from _gateway (192.168.4.254): icmp_seq=1 ttl=64 time=0.435 ms
64 bytes from _gateway (192.168.4.254): icmp_seq=2 ttl=64 time=0.718 ms

--- DS1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.435/0.576/0.718/0.141 ms
root@DD1:~#
```

- Lancez Firefox et vérifiez l'accès à Internet en affichant le site web de l'Académie de Nice.