

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.

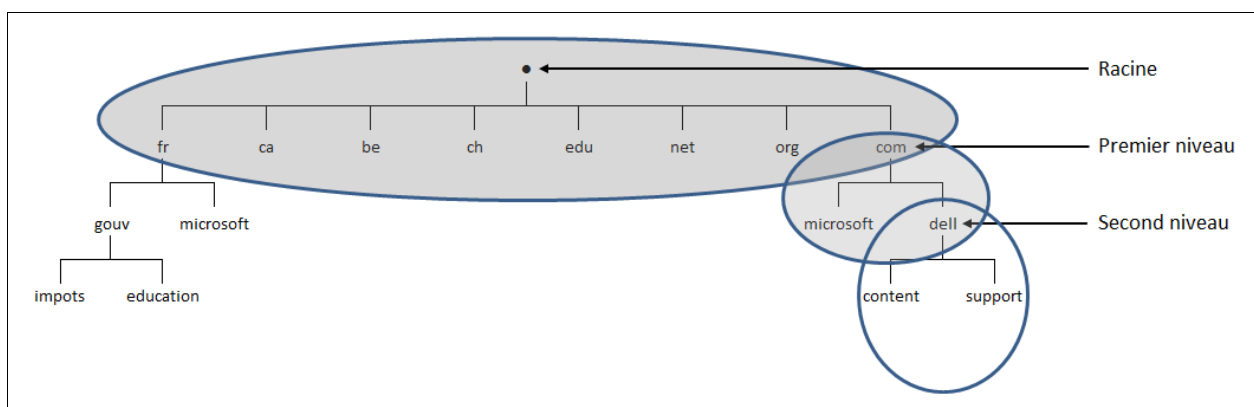
Le système DNS (Domain Name System) utilise un **espace de noms Internet**. Il se compose d'une **arborescence de domaines** dont le niveau le plus bas correspond à un **enregistrement de ressource**.

La **racine** d'un espace de noms Internet est représentée par un **point** sous lequel on trouve les **domaines de premier niveau** : **fr**, **ch**, **com**, **edu** sont quelques exemples de noms de domaine de premier niveau. L'**IANA** (Internet Assigned Numbers Authority) **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.

L'**IANA** n'a autorité que sur les domaines de premier niveau et les organismes se situant au premier niveau ont autorité jusqu'au second niveau. Au-delà, la responsabilité devient celle de l'entreprise ou du particulier.

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) un **nom complet identifiant la ressource** 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 :

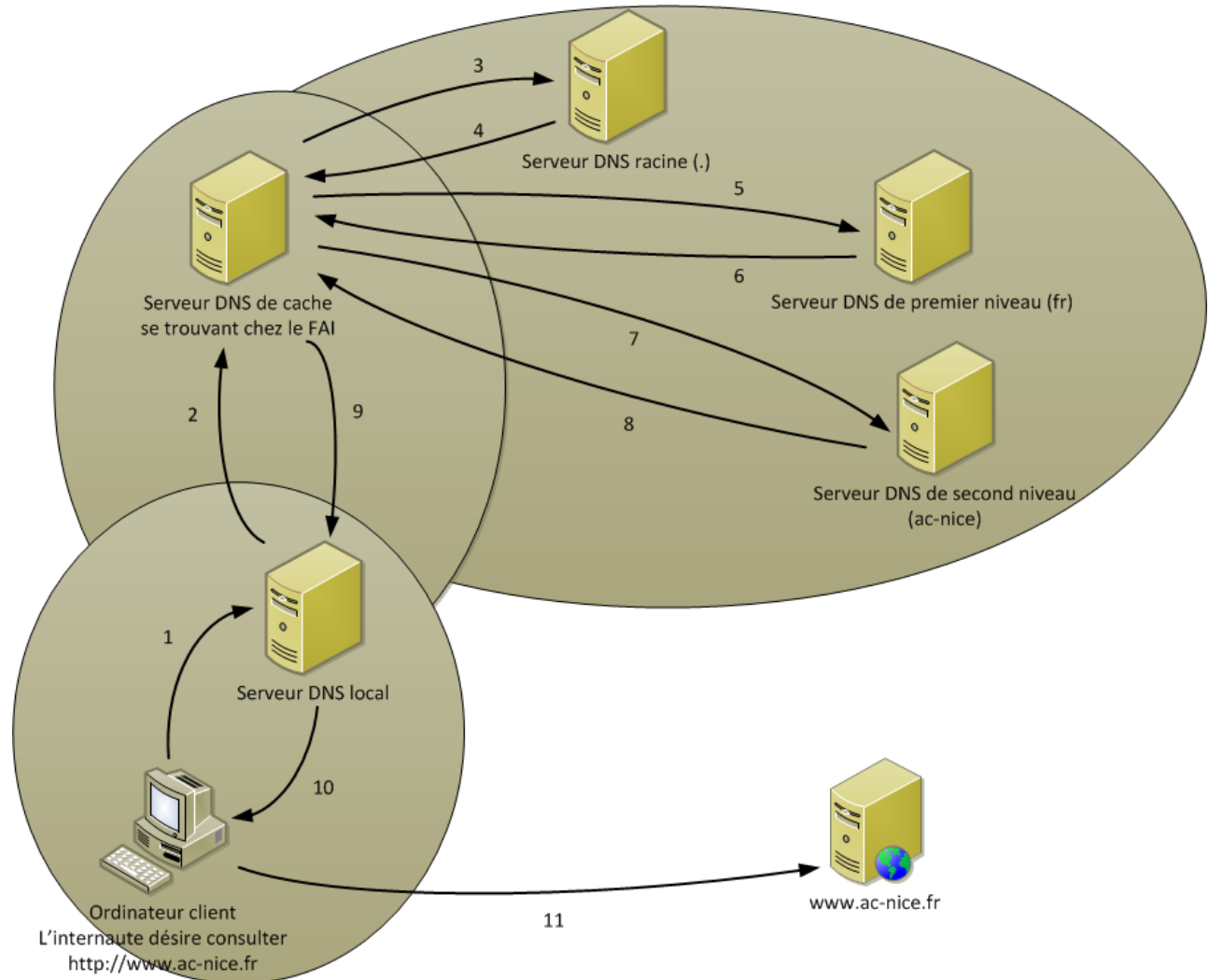
- **.** (point) représente la racine.
- **fr** représente le nom de domaine de premier niveau.
- **ac-nice** représente le nom de domaine de second niveau.
- **www** représente un **enregistrement** dans la zone, ici un enregistrement de type **hôte**.

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. Il faudra empêcher le serveur DS1 de s'adresser directement aux serveurs racines** et donc de les « importuner » avec les demandes de résolution externe. Le serveur DNS DS1 s'appuiera donc 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:base::2:30
;
; FORMERLY NS1.ISI.EDU
;
B.ROOT-SERVERS.NET. 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
;
C.ROOT-SERVERS.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-dnsutils bind9-host bind9-libs bind9-utils dns-root-data
Paquets suggérés :
  bind-doc resolvconf 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 67 non mis à jour.
Il est nécessaire de prendre 3 017 ko dans les archives.
Après cette opération, 3 194 ko d'espace disque seront libérés.
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 ;

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz 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.default-zones";
```

- **/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 48
-rw-r--r-- 1 root root 2403 21 sept. 19:33 bind.keys
-rw-r--r-- 1 root root 255 21 sept. 19:33 db.0
-rw-r--r-- 1 root root 271 21 sept. 19:33 db.127
-rw-r--r-- 1 root root 237 21 sept. 19:33 db.255
-rw-r--r-- 1 root root 353 21 sept. 19:33 db.empty
-rw-r--r-- 1 root root 270 21 sept. 19:33 db.local
-rw-r--r-- 1 root bind 458 21 sept. 19:33 named.conf
-rw-r--r-- 1 root bind 498 21 sept. 19:33 named.conf.default-zones
-rw-r--r-- 1 root bind 165 21 sept. 19:33 named.conf.local
-rw-r--r-- 1 root bind 846 21 sept. 19:33 named.conf.options
-rw-r----- 1 bind bind 100 4 févr. 15:35 rnoc.key
-rw-r--r-- 1 root root 1317 21 sept. 19:33 zones.rfc1918
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 (/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Sun 2024-02-04 15:35:08 CET; 6min ago
     Docs: man:named(8)
   Main PID: 975 (named)
   Status: "running"
    Tasks: 6 (limit: 2307)
   Memory: 37.9M
      CPU: 55ms
   CGroup: /system.slice/named.service
           └─975 /usr/sbin/named -f -u bind
```

Pas d'erreur bloquante (les avertissements n'apparaîtront plus à partir des pages 13 et 14)

```
févr. 04 15:35:08 DS1 named[975]: network unreachable resolving './DNSKEY/IN': 2001:500:1::53#53
févr. 04 15:35:08 DS1 named[975]: network unreachable resolving './NS/IN': 2001:500:1::53#53
févr. 04 15:35:08 DS1 named[975]: network unreachable resolving './DNSKEY/IN': 2001:dc3::35#53
févr. 04 15:35:08 DS1 named[975]: network unreachable resolving './NS/IN': 2001:dc3::35#53
févr. 04 15:35:08 DS1 named[975]: managed-keys-zone: Initializing automatic trust anchor management
févr. 04 15:35:08 DS1 named[975]: resolver priming query complete: success
févr. 04 15:35:08 DS1 named[975]: checkhints: b.root-servers.net/A (170.247.170.2) missing from hints
févr. 04 15:35:08 DS1 named[975]: checkhints: b.root-servers.net/A (199.9.14.201) extra record in hints
févr. 04 15:35:08 DS1 named[975]: checkhints: b.root-servers.net/AAAA (2801:1b8:10::b) missing from hints
févr. 04 15:35:08 DS1 named[975]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) extra record in hints
lines 1-22/22 (END)
```

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 bind**.

- Si ce n'est déjà fait, installez le paquet recommandé lors de l'installation de bind9 (**resolvconf**) :

```
root@DS1: ~#apt-get install resolvconf
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  resolvconf
0 mis à jour, 1 nouvellement installés, 0 à enlever et 67 non mis à jour.
Il est nécessaire de prendre 55,6 ko dans les archives.
```

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 2.2.6      Fichier : /etc/bind/named.conf.local      Modifié
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
//les zones
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 2.2.6      Fichier : /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";
```

- L'instruction **allow-update { none; }** n'autorise pas les **mise 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 faites figurer les **enregistrements** correspondant à vos machines :

```
GNU nano 7.2      /var/cache/bind/db.sio-exupery.local
; Fichier pour la résolution directe
$TTL 86400
@ IN SOA DS1.sio-exupery.local. root.sio-exupery.local. (
    2024020401
    1w
    1d
    4w
    1w )
@ IN NS DS1.sio-exupery.local.
DS1 IN A 192.168.4.254
UD1 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 7.2 /var/cache/bind/rev.sio-exupery.local
; Fichier pour la résolution inverse
$TTL 86400
@ IN SOA DS1.sio-exupery.local. root.sio-exupery.local. (
    2024020401
    1w
    1d
    4w
    1w )
@ IN NS DS1.sio-exupery.local.
254 IN PTR DS1.sio-exupery.local.
1 IN PTR UD1.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` :

```

GNU nano 2.7.4 Fichier : /etc/network/interfaces
# 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 192.168.1.101
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1

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

```

Annotations :

- ← Réseau 172.17.0.0/16 au Lycée (pointe vers l'adresse IP 192.168.1.101)
- ← Suppression du DNS Roi (ou du FAI) sur enp0s3 (pointe vers la suppression de la ligne gateway)
- ← Votre serveur DNS gérant la zone sio-exupery.local (pointe vers les directives dns-search, dns-domain, dns-nameservers)

- 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 ~ #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 ~ #

```

- Dans le fichier **named.conf.options**, mettez l'instruction **dnssec-validation auto** sur **no** dans ce chapitre.

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#>

```

GNU nano 2.2.6      Fichier : /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====$
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====$
    dnssec-validation auto;

    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
};

```

Remplacez auto par no

- Relancez le service **bind9** :

```

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

```

- **Premier 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 2019012601
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 2019012601
OK
root@DS1: /var/cache/bind#_

```

- **Deuxième 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**, avec la version Debian 12 donc inutile de chercher à l'afficher avec la commande **tail -f /var/log/syslog**.

```
root@DS1: ~#journalctl -f
févr. 04 18:03:57 DS1 named[720]: checkhints: b.root-servers.net/A (170.247.170.2) missing from hints
févr. 04 18:03:57 DS1 named[720]: checkhints: b.root-servers.net/A (199.9.14.201) extra record in hints
févr. 04 18:03:57 DS1 named[720]: checkhints: b.root-servers.net/AAAA (2801:1b8:10::b) missing from hints
févr. 04 18:03:57 DS1 named[720]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) extra record in hints
févr. 04 18:03:59 DS1 named[720]: listening on IPv6 interface enp0s3, 2a01:cb1d:490:1500:a00:27ff:fe8d:1c99#53
févr. 04 18:09:25 DS1 systemd[1]: Started getty@tty2.service - Getty on tty2.
févr. 04 18:09:34 DS1 login[896]: pam_unix(login:session): session opened for user root(uid=0) by LOGIN(uid=0)
févr. 04 18:09:34 DS1 systemd-logind[456]: New session 3 of user root.
févr. 04 18:09:34 DS1 systemd[1]: Started session-3.scope - Session 3 of User root.
févr. 04 18:09:34 DS1 login[902]: ROOT LOGIN on '/dev/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 (il est fréquent d'oublier les points...).

```
févr. 04 18:15:40 DS1 named[913]: configuring command channel from '/etc/bind/rndc.key'
févr. 04 18:15:40 DS1 named[913]: command channel listening on 127.0.0.1#953
févr. 04 18:15:40 DS1 named[913]: configuring command channel from '/etc/bind/rndc.key'
févr. 04 18:15:40 DS1 named[913]: command channel listening on ::1#953
févr. 04 18:15:40 DS1 named[913]: managed-keys-zone: loaded serial 11
févr. 04 18:15:40 DS1 named[913]: zone sio-exupery.local/IN: loaded serial 2024020401
févr. 04 18:15:40 DS1 named[913]: zone 0.in-addr.arpa/IN: loaded serial 1
févr. 04 18:15:40 DS1 named[913]: zone 4.168.192.in-addr.arpa/IN: loaded serial 2024020401
févr. 04 18:15:40 DS1 named[913]: zone 255.in-addr.arpa/IN: loaded serial 1
févr. 04 18:15:40 DS1 systemd[1]: Started named.service - BIND Domain Name Server.
févr. 04 18:15:40 DS1 named[913]: zone 127.in-addr.arpa/IN: loaded serial 1
févr. 04 18:15:40 DS1 named[913]: zone localhost/IN: loaded serial 2
févr. 04 18:15:40 DS1 named[913]: all zones loaded
févr. 04 18:15:40 DS1 named[913]: running
févr. 04 18:15:40 DS1 named[913]: zone sio-exupery.local/IN: sending notifies (serial 2024020401)
févr. 04 18:15:50 DS1 named[913]: resolver priming query complete: timed out
févr. 04 18:15:50 DS1 named[913]: managed-keys-zone: Unable to fetch DNSKEY set '.': 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  dnsutils      1:9.10.3.dfsg.P4-12.3+deb9u4  amd64      Clients provided with BIND
root@DS1 ~ #
```

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

- Saisissez la commande **dig UD1.sio-exupery.local** :

```
root@DS1: ~#dig UD1.sio-exupery.local
;<><> DiG 9.18.19-1~deb12u1-Debian <>> UD1.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: 5051
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1 AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: d74239a0f29d04210100000065bfce5b51b829675a34f116 (good)
;; QUESTION SECTION:
;UD1.sio-exupery.local.      IN      A
;; ANSWER SECTION:
UD1.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: Sun Feb 04 18:50:19 CET 2024
;; 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

```

- Saisissez les commandes **dig www.dunod.com** et **nslookup www.eni.fr** :

```

root@DS1 ~ #dig www.dunod.com

;<<>> DiG 9.10.3-P4-Debian <<>> www.dunod.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61281
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.dunod.com.                  IN      A
;; ANSWER SECTION:
www.dunod.com.                  172800 IN      A        195.81.225.57
;; AUTHORITY SECTION:
dunod.com.                       172795 IN      NS       ns1.hachette-livre.com.
dunod.com.                       172795 IN      NS       ns3.hachette-livre.com.
dunod.com.                       172795 IN      NS       ns2.hachette-livre.com.
;; ADDITIONAL SECTION:
ns1.hachette-livre.com.          172795 IN      A        195.81.225.19
ns2.hachette-livre.com.          172795 IN      A        195.81.224.19
ns3.hachette-livre.com.          172795 IN      A        80.11.178.47

;; Query time: 1959 msec
;; SERVER: 192.168.4.254#53(192.168.4.254)
;; WHEN: Sun Jan 13 21:48:42 CET 2019
;; MSG SIZE rcvd: 175

```

```

root@DS1 ~ #nslookup www.eni.fr
Server:      192.168.4.254
Address:    192.168.4.254#53

Non-authoritative answer:
Name:      www.eni.fr
Address: 185.42.28.200

```

- Vérifiez enfin la résolution DNS interne et externe avec :
 - un ping sur DS1.sio-exupery.local ;
 - un ping sur UD1.sio-exupery.local ;
 - un ping sur www.ac-nice.fr.

```

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=0.022 ms
64 bytes from DS1.sio-exupery.local (192.168.4.254): icmp_seq=2 ttl=64 time=0.026 ms

--- DS1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1028ms
rtt min/avg/max/mdev = 0.022/0.024/0.026/0.002 ms
root@DS1 ~ #ping -c 2 WUD
PING WUD.sio-exupery.local (192.168.4.1) 56(84) bytes of data.
64 bytes from WUD.sio-exupery.local (192.168.4.1): icmp_seq=1 ttl=64 time=0.239 ms
64 bytes from WUD.sio-exupery.local (192.168.4.1): icmp_seq=2 ttl=64 time=0.307 ms

--- WUD.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1025ms
rtt min/avg/max/mdev = 0.239/0.273/0.307/0.034 ms

```

```

root@DS1 ~ #ping -c 2 www.ac-nice.fr
PING mars.ac-nice.fr (194.167.84.155) 56(84) bytes of data.
64 bytes from 194.167.84.155: icmp_seq=1 ttl=49 time=50.0 ms
64 bytes from 194.167.84.155: icmp_seq=2 ttl=49 time=50.6 ms

--- mars.ac-nice.fr ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 9468ms
rtt min/avg/max/mdev = 50.077/50.374/50.671/0.297 ms
root@DS1 ~ #_

```

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

Votre serveur DNS fonctionne mais vous allez le rendre plus performant. Actuellement, DS1 s'occupe des résolutions de la zone sio-exupery.local mais aussi des résolutions externes pour les machines du réseau local et construit donc son cache. **Pour l'instant**, le serveur DS1, s'il doit faire une **résolution externe**, va s'adresser aux seuls serveurs qu'il connaisse, à savoir les **serveurs racine**. Cette méthode de résolution n'est pas forcément la plus rapide. De façon à réduire la charge de travail du serveur DNS DS1 et surtout des serveurs racines, il serait souhaitable que la résolution externe soit dévolue au serveur DNS **« au-dessus de lui »**. Il faut, pour cela, que le serveur DS1 redirige ses requêtes vers le **serveur Roi** (ou le **serveur DNS du FAI**).

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

```

GNU nano 3.2 /etc/bind/named.conf.default-zones Modifié
// prime the server with knowledge of the root servers
//zone "." {
//     type hint;
//     file "/usr/share/dns/root.hints";
//};

```

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

```

GNU nano 2.2.6      Fichier : /etc/bind/named.conf.options
options {
  directory "/var/cache/bind";

  // If there is a firewall between you and nameservers you want
  // to talk to, you may need to fix the firewall to allow multiple
  // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

  // If your ISP provided one or more IP addresses for stable
  // nameservers, you probably want to use them as forwarders.
  // Uncomment the following block, and insert the addresses replacing
  // the all-0's placeholder.

  // forwarders {
  //     0.0.0.0;
  // };

  //=====
  // If BIND logs error messages about the root key being expired,
  // you will need to update your keys.  See https://www.isc.org/bind-keys
  //=====
  dnssec-validation auto;

  auth-nxdomain no;    # conform to RFC 2135
  listen-on-v6 { any; };
};

```

auto a été remplacé par no à la page 9

- Décommentez la ligne comportant l’instruction **forwarders** et modifiez le fichier de la manière suivante :

```

GNU nano 7.2      /etc/bind/named.conf.options
options {
  directory "/var/cache/bind";

  // If there is a firewall between you and nameservers you want
  // to talk to, you may need to fix the firewall to allow multiple
  // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

  // If your ISP provided one or more IP addresses for stable
  // nameservers, you probably want to use them as forwarders.
  // Uncomment the following block, and insert the addresses replacing
  // the all-0's placeholder.

  forward only;
  forwarders { 192.168.1.1; };
  allow-recursion { localnets; };

  //=====
  // If BIND logs error messages about the root key
  // you will need to update your keys.  See https://www.isc.org/bind-keys
  //=====

  dnssec-validation no;

  listen-on-v6 { any; };
};

```

80.10.246.2 (DNS FAI Orange)
ou serveur DNS ROI
ou 8.8.8.8 ou les trois
/ Votre box à la maison

Avec l’instruction **forward only**, toutes les requêtes ne concernant pas la zone **sio-exupery.local** seront redirigées obligatoirement vers le serveur DNS du FAI Orange ou 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**.

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

```

root@DS1: ~#systemctl restart bind9
root@DS1: ~#systemctl status bind9
• named.service - BIND Domain Name Server
  Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
  Active: active (running) since Sun 2024-02-04 19:02:54 CET; 10s ago
    Docs: man:named(8)
  Main PID: 972 (named)
  Status: "running"
  Tasks: 4 (limit: 2307)
  Memory: 33.0M
    CPU: 32ms
  CGroup: /system.slice/named.service
          └─972 /usr/sbin/named -f -u bind

févr. 04 19:02:54 DS1 named[972]: zone 0.in-addr.arpa/IN: loaded serial 1
févr. 04 19:02:54 DS1 named[972]: zone sio-exupery.local/IN: loaded serial 2024020401
févr. 04 19:02:54 DS1 named[972]: zone localhost/IN: loaded serial 2
févr. 04 19:02:54 DS1 named[972]: zone 4.168.192.in-addr.arpa/IN: loaded serial 2024020401
févr. 04 19:02:54 DS1 named[972]: zone 127.in-addr.arpa/IN: loaded serial 1
févr. 04 19:02:54 DS1 named[972]: zone 255.in-addr.arpa/IN: loaded serial 1
févr. 04 19:02:54 DS1 named[972]: all zones loaded
févr. 04 19:02:54 DS1 systemd[1]: Started named.service - BIND Domain Name Server.
févr. 04 19:02:54 DS1 named[972]: running
févr. 04 19:02:54 DS1 named[972]: zone sio-exupery.local/IN: sending notifies (serial 2024020401)
root@DS1: ~#_

```

- Testez à nouveau une résolution externe à partir du serveur DS1 ; la résolution devrait être plus rapide :

```

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

;<<>> DiG 9.18.19-1~deb12u1-Debian <<>> www.ac-nice.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46393
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 5962ed72ba087aaf0100000065bfd1e4ec377ad307bebfe9 (good)
;; QUESTION SECTION:
;www.ac-nice.fr.                IN      A

;; ANSWER SECTION:
www.ac-nice.fr.                6768   IN      CNAME   cs234.wpc.alphacdn.net.
cs234.wpc.alphacdn.net.       1354   IN      A       93.184.221.161

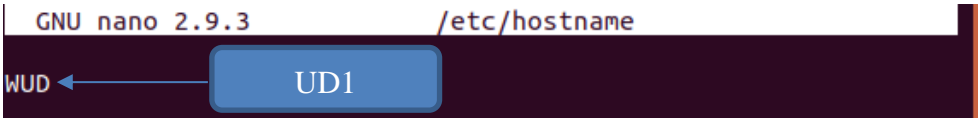
;; Query time: 64 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Sun Feb 04 19:05:24 CET 2024
;; MSG SIZE rcvd: 123

root@DS1: ~#_

```

2.14. Test à partir du client Ubuntu

- Démarrez le client Ubuntu UD1 et vérifiez le nom de l'ordinateur dans le fichier **/etc/hostname** :



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

```

GNU nano 2.9.3 /etc/hosts Modifié
127.0.0.1 localhost
192.168.4.1 WUD.sio-exupery.local WUD
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback

```

- Depuis la version 17.10, Ubuntu utilise **netplan** pour paramétrer les carte réseau. La configuration de ces dernières est gérée non plus depuis le fichier `/etc/network/interfaces` mais à partir d'un fichier `*.yaml` situé dans `/etc/netplan`. Ce fichier est utilisé pour configurer l'interface réseau, que ce soit dans la version Desktop ou Server, à ceci près que dans la version Desktop, il renvoie à l'interface graphique **Network Manager**.

Configurez les paramètres IP ainsi que l'adresse du serveur DNS (DS1 au lieu de ROI), sans passer par l'interface graphique de Network Manager, en modifiant le fichier `/etc/netplan/01-network-manager-all.yaml` (remplacez **NetworkManager** par **networkd** dans **renderer**).

```

sio@WUD: /etc/netplan
Fichier Édition Affichage Rechercher Terminal Aide
sio@WUD:~$ cd /etc/netplan
sio@WUD:/etc/netplan$ ls
01-network-manager-all.yaml
sio@WUD:/etc/netplan$ sudo nano 01-network-manager-all.yaml

```

L'indentation est importante dans les fichiers .yaml (pas de tabulation).

```

GNU nano 2.9.3 /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.4.1/24]
      gateway4: 192.168.4.254
      nameservers:
        search: [sio-exupery.local]
        addresses: [192.168.4.254]

```

« gateway4 has been deprecated »
 routes :
 - to: default
 via: 192.168.4.254

- Vous devez ensuite saisir la commande **netplan generate** pour générer un fichier `.network` dans `/run/systemd/network` puis redémarrer le service **systemd-networkd** avec la commande **systemctl restart systemd-networkd**. Vous pouvez aussi, en une seule commande, **netplan apply**, générer le fichier et redémarrer le service :

```

sio@WUD: /etc/netplan
Fichier Édition Affichage Rechercher Terminal Aide
sio@WUD:/etc/netplan$ sudo netplan apply
[sudo] Mot de passe de sio :
sio@WUD:/etc/netplan$

```

- Vérifiez la configuration réseau :

```
sio@WUD: ~
Fichier Édition Affichage Rechercher Terminal Aide
sio@WUD:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d4:d3:5b brd ff:ff:ff:ff:ff:ff
    inet 192.168.4.1/24 brd 192.168.4.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed4:d35b/64 scope link
        valid_lft forever preferred_lft forever
sio@WUD:~$
```

```
sio@WUD: ~
Fichier Édition Affichage Rechercher Terminal Aide
sio@WUD:~$ ip r
default via 192.168.4.254 dev enp0s3 proto static
192.168.4.0/24 dev enp0s3 proto kernel scope link src 192.168.4.1
sio@WUD:~$
```

- Le fichier **/etc/resolv.conf** ne mentionne pas l'adresse du serveur DNS DS1 :

```
sio@WUD: ~
Fichier Édition Affichage Rechercher Terminal Aide
sio@WUD:~$ cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "systemd-resolve --status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.
nameserver 127.0.0.53
search sio-exupery.local
sio@WUD:~$
```

- Le fichier **/etc/resolv.conf** est un lien symbolique pointant sur le fichier **/run/systemd/resolve/stub-resolv.conf** :

```
sio@WUD: ~
Fichier Édition Affichage Rechercher Terminal Aide
sio@WUD:~$ ls -l /etc/resolv.conf
lrwxrwxrwx 1 root root 39 déc. 2 01:00 /etc/resolv.conf -> ../run/systemd/resolve
lve/stub-resolv.conf
sio@WUD:~$
```

```
sio@WUD: /run/systemd/resolve
Fichier Édition Affichage Rechercher Terminal Aide
sio@WUD:~$ cd /run/systemd/resolve
sio@WUD:/run/systemd/resolve$ ls -l
total 8
-rw-r--r-- 1 systemd-resolve systemd-resolve 618 févr. 10 12:01 resolv.conf
-rw-r--r-- 1 systemd-resolve systemd-resolve 729 févr. 10 12:01 stub-resolv.conf
sio@WUD:/run/systemd/resolve$
```

- Affichez le fichier **/run/systemd/resolve/resolv.conf** pour vérifier l'adresse du serveur DNS.

```
sio@WUD: ~
Fichier Édition Affichage Rechercher Terminal Aide
sio@WUD:~$ cat /run/systemd/resolve/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients directly to
# all known uplink DNS servers. This file lists all configured search domains.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.
nameserver 192.168.4.254
search sio-exupery.local
sio@WUD:~$
```

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

```
sio@WUD: ~  
Fichier Édition Affichage Rechercher Terminal Aide  
sio@WUD:~$ dig SOA sio-exupery.local  
  
;<<>> DiG 9.11.3-1ubuntu1.2-Ubuntu <<>> 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: 23099  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags;; udp: 65494  
;; QUESTION SECTION:  
;sio-exupery.local.          IN      SOA  
  
;; ANSWER SECTION:  
sio-exupery.local.      86400  IN      SOA      DS1.sio-exupery.local. root.sio-  
exupery.local. 2019011101 604800 86400 2419200 604800  
  
;; Query time: 0 msec  
;; SERVER: 127.0.0.53#53(127.0.0.53)  
;; WHEN: Mon Jan 14 15:20:12 CET 2019  
;; MSG SIZE rcvd: 91  
  
sio@WUD:~$
```

```
sio@WUD: ~  
Fichier Édition Affichage Rechercher Terminal Aide  
sio@WUD:~$ dig DS1.sio-exupery.local  
  
;<<>> DiG 9.11.3-1ubuntu1.2-Ubuntu <<>> 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: 38098  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags;; udp: 65494  
;; QUESTION SECTION:  
;DS1.sio-exupery.local.    IN      A  
  
;; ANSWER SECTION:  
DS1.sio-exupery.local.  7152   IN      A        192.168.4.254  
  
;; Query time: 0 msec  
;; SERVER: 127.0.0.53#53(127.0.0.53)  
;; WHEN: Mon Jan 14 15:22:35 CET 2019  
;; MSG SIZE rcvd: 66  
  
sio@WUD:~$
```

```
sio@WUD: ~
Fichier Édition Affichage Rechercher Terminal Aide
sio@WUD:~$ dig www.eni.fr

;<<>> DiG 9.11.3-1ubuntu1.2-Ubuntu <<>> www.eni.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30123
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.eni.fr.                IN      A

;; ANSWER SECTION:
www.eni.fr.                 3600   IN      A      185.42.28.200

;; Query time: 58 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Jan 14 15:23:50 CET 2019
;; MSG SIZE rcvd: 55

sio@WUD:~$
```

- Saisissez la commande **nslookup www.editions-eyrolles.com**.

```
sio@WUD: ~
Fichier Édition Affichage Rechercher Terminal Aide
sio@WUD:~$ nslookup www.editions-eyrolles.com
Server:                127.0.0.53
Address:               127.0.0.53#53

Non-authoritative answer:
Name:   www.editions-eyrolles.com
Address: 213.244.11.249

sio@WUD:~$
```

- Faites un **ping** sur DS1.

```
sio@WUD: ~
Fichier Édition Affichage Rechercher Terminal Aide
sio@WUD:~$ 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=0.26
0 ms
64 bytes from DS1.sio-exupery.local (192.168.4.254): icmp_seq=2 ttl=64 time=0.34
0 ms

--- DS1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1058ms
rtt min/avg/max/mdev = 0.260/0.300/0.340/0.040 ms
sio@WUD:~$
```

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