

Chapitre 2 - Serveur Debian DS1: installation du service DNS

Sommaire :

2.1. Serveurs racine.....	1
2.2. Installation du paquetage BIND.....	1
2.3. Zone de recherche directe et zone de recherche inversée.....	4
2.4. Construction des fichiers de zone.....	6
2.5. Démarrage et tests du service.....	7
2.6. Outils de test de résolution de noms.....	10
2.7. S'appuyer sur un DNS externe : la redirection.....	13
2.8. Test à partir du client Ubuntu.....	15

2.1. Serveurs racine.

```
. 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
;
```

2.2. 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
bind9 est déjà la version la plus récente (1:9.18.19-1~deb12u1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 67 non mis à jour.
root@DS1: ~#
```

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 7.2 /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.default-zones";
```

- « **/etc/bind/named.conf.options** » : fichier contenant les options de BIND9 ;
- « **/etc/bind/named.conf.local** » : fichier contenant les 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 60
-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 506 9 févr. 11:22 named.conf.default-zones
-rw-r--r-- 1 root bind 388 6 févr. 17:39 named.conf.local
-rw-r--r-- 1 root bind 165 2 févr. 11:40 named.conf.local.sauv
-rw-r--r-- 1 root bind 887 9 févr. 11:28 named.conf.options
-rw-r--r-- 1 root bind 846 2 févr. 11:40 named.conf.options.sauv
-rw-r--r-- 1 root bind 458 2 févr. 11:40 named.conf.sauv
-rw-r--r-- 1 bind bind 100 2 févr. 11:01 rndc.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 Fri 2024-02-02 11:01:46 CET; 39min ago
     Docs: man:named(8)
    Main PID: 916 (named)
      Status: "running"
       Tasks: 6 (limit: 2307)
      Memory: 45.6M
         CPU: 119ms
    CGroup: /system.slice/named.service
            └─916 /usr/sbin/named -f -u bind

févr. 02 11:01:46 DS1 named[916]: network unreachable resolving './DNSKEY/IN': 2001:500:9f::42#53
févr. 02 11:01:46 DS1 named[916]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
févr. 02 11:01:46 DS1 named[916]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
févr. 02 11:01:46 DS1 named[916]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
févr. 02 11:01:46 DS1 named[916]: managed-keys-zone: Initializing automatic trust anchor management
févr. 02 11:01:46 DS1 named[916]: resolver priming query complete: success
févr. 02 11:01:46 DS1 named[916]: checkhints: b.root-servers.net/A (170.247.170.2) missing from hin
févr. 02 11:01:46 DS1 named[916]: checkhints: b.root-servers.net/A (199.9.14.201) extra record in h
févr. 02 11:01:46 DS1 named[916]: checkhints: b.root-servers.net/AAAA (2801:1b8:10::b) missing from
févr. 02 11:01:46 DS1 named[916]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) extra recor
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 bind** ».

```

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

```

- Installez les deux paquets recommandés lors de l'installation de bind9 (**dnsutils** et **resolvconf**) :

```

root@DS1: ~# apt-get install dnsutils 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 :
  dnsutils resolvconf
0 mis à jour, 2 nouvellement installés, 0 à enlever et 67 non mis à jour.
Il est nécessaire de prendre 315 ko dans les archives.
Après cette opération, 455 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 dnsutils all 1:9.18.19-1~deb12u1 [259 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 resolvconf all 1.91+nmu1 [55,6 kB]
315 ko réceptionnés en 0s (643 ko/s)
Préconfiguration des paquets...
Sélection du paquet dnsutils précédemment désélectionné.
(Lecture de la base de données... 57661 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../dnsutils_1%3a9.18.19-1~deb12u1_all.deb ...
Dépaquetage de dnsutils (1:9.18.19-1~deb12u1) ...
Sélection du paquet resolvconf précédemment désélectionné.
Préparation du dépaquetage de .../resolvconf_1.91+nmu1_all.deb ...
Dépaquetage de resolvconf (1.91+nmu1) ...
Paramétrage de resolvconf (1.91+nmu1) ...
Created symlink /etc/systemd/system/sysinit.target.wants/resolvconf.service → /lib/systemd/system/resolvconf.service.
Created symlink /etc/systemd/system/systemd-resolved.service.wants/resolvconf-pull-resolved.path → /lib/systemd/system/resolvconf-pull-resolved.path.
Unit /lib/systemd/system/resolvconf-pull-resolved.path is added as a dependency to a non-existent unit systemd-resolved.service.
Created symlink /etc/systemd/system/systemd-resolved.service.wants/resolvconf-pull-resolved.service → /lib/systemd/system/resolvconf-pull-resolved.service.
Unit /lib/systemd/system/resolvconf-pull-resolved.service is added as a dependency to a non-existent unit systemd-resolved.service.
Paramétrage de dnsutils (1:9.18.19-1~deb12u1) ...
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
Traitement des actions différées (« triggers ») pour resolvconf (1.91+nmu1) ...
root@DS1: ~#

```

2.3. 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 7.2 /etc/bind/named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
//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 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.

    // 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;

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

```

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

2.4. 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. (
    2024020201
    1w
    1d
    4w
    1w )
@ IN NS DS1.sio-exupery.local.
DS1 IN A 192.168.4.254
UD1 IN A 192.168.4.1
UD2 IN A 192.168.4.2
```

- 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. (
    2024020201
    1w
    1d
    4w
    1w )
@ IN NS DS1.sio-exupery.local.
254 IN PTR DS1.sio-exupery.local.
1 IN PTR UD1.sio-exupery.local.
2 IN PTR UD2.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: ~#ls -l /var/cache/bind
total 16
-rw-rw-r-- 1 root bind 234  2 févr. 13:16 db.sio-exupery.local
-rw-rw-r-- 1 bind bind 821  2 févr. 11:47 managed-keys.bind
-rw-rw-r-- 1 bind bind 1717  2 févr. 11:46 managed-keys.bind.jnl
-rw-rw-r-- 1 root bind 267  2 févr. 13:14 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 2 févr. 13:16 /var/cache/bind
root@DS1: ~#_
```

2.5. 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 7.2 /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** :

Premièrement, on désactive les 2 interfaces :

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

Puis, on modifie le fichier « **/etc/network/interfaces** » :

```

GNU nano 7.2 /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 172.17.101.205
netmask 255.255.0.0
network 172.17.0.0
broadcast 172.17.255.255
gateway 172.17.250.2

#interface enp0s8
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

```

- 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
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "resolvectl status" to see details about the actual nameservers.

nameserver 192.168.4.254
search sio-exupery.local
root@DS1: ~#_

```


- **Premier test** : lancez l'utilitaire de vérification **named-checkconf** qui vérifie le fichier « **/etc/bind/named.conf** ».

```
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 2024020201
OK
root@DS1: /var/cache/bind#
```

- 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: /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 2024020201
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**.

```
root@DS1: ~#journalctl -f
févr. 09 10:23:21 DS1 systemd[1]: session-4.scope: Deactivated successfully.
févr. 09 10:23:21 DS1 systemd-logind[501]: Session 4 logged out. Waiting for processes to exit.
févr. 09 10:23:21 DS1 systemd[1]: getty@tty2.service: Scheduled restart job, restart counter is at 1
févr. 09 10:23:21 DS1 systemd[1]: Stopped getty@tty2.service - Getty on tty2.
févr. 09 10:23:21 DS1 systemd[1]: Started getty@tty2.service - Getty on tty2.
févr. 09 10:23:21 DS1 systemd-logind[501]: Removed session 4.
févr. 09 10:23:29 DS1 login[791]: pam_unix(login:session): session opened for user root(uid=0) by LOGIN(uid=0)
févr. 09 10:23:29 DS1 systemd-logind[501]: New session 5 of user root.
févr. 09 10:23:29 DS1 systemd[1]: Started session-5.scope - Session 5 of User root.
févr. 09 10:23:29 DS1 login[797]: ROOT LOGIN on '/dev/tty2'
```

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

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

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

```

févr. 09 10:41:49 DS1 named[841]: configuring command channel from '/etc/bind/rndc.key'
févr. 09 10:41:49 DS1 named[841]: command channel listening on 127.0.0.1#953
févr. 09 10:41:49 DS1 named[841]: configuring command channel from '/etc/bind/rndc.key'
févr. 09 10:41:49 DS1 named[841]: command channel listening on ::1#953
févr. 09 10:41:49 DS1 named[841]: managed-keys-zone: loaded serial 6
févr. 09 10:41:49 DS1 named[841]: zone sio-exupery.local/IN: loaded serial 2024020201
févr. 09 10:41:49 DS1 named[841]: zone 0.in-addr.arpa/IN: loaded serial 1
févr. 09 10:41:49 DS1 named[841]: zone 127.in-addr.arpa/IN: loaded serial 1
févr. 09 10:41:49 DS1 named[841]: zone 4.168.192.in-addr.arpa/IN: loaded serial 2024020201
févr. 09 10:41:49 DS1 named[841]: zone localhost/IN: loaded serial 2
févr. 09 10:41:49 DS1 named[841]: zone 255.in-addr.arpa/IN: loaded serial 1
févr. 09 10:41:49 DS1 named[841]: all zones loaded
févr. 09 10:41:49 DS1 named[841]: running
févr. 09 10:41:49 DS1 systemd[1]: Started named.service - BIND Domain Name Server.

```

2.6. Outils de test de résolution de noms

- Vérifiez la présence sur votre système du paquetage **dnsutils** installé à la suite de **bind**

```

root@DS1: ~#dpkg -l | grep -i dnsutils
ii bind9-dnsutils      1:9.18.19-1~deb12u1      amd64      Clients' protocols and utilities provided with BIND 9
ii dnsutils           1:9.18.19-1~deb12u1      all        Transitional package for bind9-dnsutils
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: 35822
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 9d8357641f7921030100000065c5f6636a33c4ac3dbc86de (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: Fri Feb 09 10:54:43 CET 2024
;; MSG SIZE rcvd: 94

root@DS1: ~#

```

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

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

; <>> DiG 9.18.19-1~deb12u1-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: 28529
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 1232
; COOKIE: 787d3beae50556380100000065c5f6c94ade136a28b1aa6b (good)
;; QUESTION SECTION:
;sio-exupery.local.                IN      SOA

;; ANSWER SECTION:
sio-exupery.local.                86400   IN      SOA      DS1.sio-exupery.local. root.sio-exupery.local. 20240
20201 604800 86400 2419200 604800

;; Query time: 0 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Fri Feb 09 10:56:25 CET 2024
;; MSG SIZE rcvd: 119

root@DS1: ~#
```

- 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

root@DS1: ~#
```

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

```
root@DS1: ~#dig www.dunod.com

; <>> DiG 9.18.19-1~deb12u1-Debian <>> www.dunod.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15579
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 1232
; COOKIE: 4634f04bb8afa6ba0100000065c5f8d7daf7cccb77ae1dd4 (good)
;; QUESTION SECTION:
;www.dunod.com.                IN      A

;; ANSWER SECTION:
www.dunod.com.                10800   IN      A          51.144.190.143

;; Query time: 240 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Fri Feb 09 11:05:11 CET 2024
;; MSG SIZE rcvd: 86
```

```

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

Non-authoritative answer:
www.eni.fr   canonical name = ip200.eni.fr.
Name:   ip200.eni.fr
Address: 185.42.28.200

root@DS1: ~#

```

- Vérifiez enfin la résolution DNS interne et externe avec :

- un ping sur **DS1.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=0.041 ms
64 bytes from DS1.sio-exupery.local (192.168.4.254): icmp_seq=2 ttl=64 time=0.040 ms

--- DS1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1026ms
rtt min/avg/max/mdev = 0.040/0.040/0.041/0.000 ms

```

- un ping sur **UD1.sio-exupery.local** ;

```

root@DS1: ~#ping -c 2 UD1
PING UD1.sio-exupery.local (192.168.4.1) 56(84) bytes of data.
64 bytes from UD1.sio-exupery.local (192.168.4.1): icmp_seq=1 ttl=64 time=0.724 ms
64 bytes from UD1.sio-exupery.local (192.168.4.1): icmp_seq=2 ttl=64 time=1.14 ms

--- UD1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.724/0.932/1.141/0.208 ms

```

- un ping sur **www.ac-nice.fr**.

```

root@DS1: ~#ping -c 2 www.ac-nice.fr
PING cs234.wpc.alphacdn.net (93.184.221.161) 56(84) bytes of data.
64 bytes from 93.184.221.161: icmp_seq=1 ttl=56 time=32.9 ms
64 bytes from 93.184.221.161: icmp_seq=2 ttl=56 time=32.8 ms

--- cs234.wpc.alphacdn.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 32.783/32.821/32.872/0.044 ms
root@DS1: ~#

```


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

- 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 importer :

```
GNU nano 7.2 /etc/bind/named.conf.default-zones *
// 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** » et décommentez la ligne comportant l'instruction « **forwarders** » et modifiez le fichier :

```
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 { 80.10.246.2; };
    allow-recursion { localnets; };

    //=====
    // 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 no;

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

Remarque :

- 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 désigné par l'instruction « **forwarders** ».
- On autorise la possibilité de récursivité uniquement pour les réseaux locaux (interfaces du serveur) par l'instruction « **allow-recursion** ».
- L'instruction « **dnssec-validation auto** » est mise dans ce chapitre sur no.

- **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 Fri 2024-02-09 11:33:09 CET; 12s ago
    Docs: man:named(8)
  Main PID: 936 (named)
  Status: "running"
   Tasks: 4 (limit: 2307)
  Memory: 33.0M
    CPU: 23ms
  CGroup: /system.slice/named.service
          └─936 /usr/sbin/named -f -u bind

févr. 09 11:33:09 DS1 named[936]: managed-keys-zone: loaded serial 7
févr. 09 11:33:09 DS1 named[936]: zone 0.in-addr.arpa/IN: loaded serial 1
févr. 09 11:33:09 DS1 named[936]: zone 4.168.192.in-addr.arpa/IN: loaded serial 2024020201
févr. 09 11:33:09 DS1 named[936]: zone sio-exupery.local/IN: loaded serial 2024020201
févr. 09 11:33:09 DS1 named[936]: zone 127.in-addr.arpa/IN: loaded serial 1
févr. 09 11:33:09 DS1 named[936]: zone localhost/IN: loaded serial 2
févr. 09 11:33:09 DS1 named[936]: zone 255.in-addr.arpa/IN: loaded serial 1
févr. 09 11:33:09 DS1 named[936]: all zones loaded
févr. 09 11:33:09 DS1 systemd[1]: Started named.service - BIND Domain Name Server.
févr. 09 11:33:09 DS1 named[936]: running
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: 855
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ac07979a157827b40100000065c6000d1dd910a7d3fe4ef0 (good)
;; QUESTION SECTION:
;www.ac-nice.fr.                IN      A
;; ANSWER SECTION:
www.ac-nice.fr.                15147   IN      CNAME   cs234.wpc.alphacdn.net.
cs234.wpc.alphacdn.net.       3600    IN      A        93.184.221.161

;; Query time: 372 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Fri Feb 09 11:35:57 CET 2024
;; MSG SIZE rcvd: 123

```

2.8. Test à partir du client Ubuntu

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

```
GNU nano 6.2 /etc/hostname
UD1
```

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

```
GNU nano 6.2 /etc/hosts *
127.0.0.1 localhost
192.168.4.1 UD1.sio-exupery.local UD1

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

- 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@UD1:~$ cd /etc/netplan
sio@UD1:/etc/netplan$ ls
01-network-manager-all.yaml
sio@UD1:/etc/netplan$ sudo nano 01-network-manager-all.yaml
sio@UD1:/etc/netplan$
```

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

```

GNU nano 6.2                                01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: networkd
  ethernet:
    enp0s3:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.4.1/24]
      routes:
        - to: default
          via: 192.168.4.254
      nameservers:
        search: [sio-exupery.local]
        addresses: [192.168.4.254]

```

- Utiliser la commande « **netplan apply** », générer le fichier et redémarrer le service :

```

sio@UD1:/etc/netplan$ sudo netplan apply
sio@UD1:/etc/netplan$

```

- Vérifiez la configuration réseau :

```

sio@UD1:~$ 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 08:00:27:9a:8c:e1 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::46d4:c97d:838c:bf57/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
sio@UD1:~$

```

```

sio@UD1:~$ 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@UD1:~$

```


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

```
sio@UD1:~$ cat /etc/resolv.conf
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(
8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# 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 "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically 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
options edns0 trust-ad
search sio-exupery.local
sio@UD1:~$
```

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

```
sio@UD1:~$ ls -l /etc/resolv.conf
lrwxrwxrwx 1 root root 39 janv. 30 12:21 /etc/resolv.conf -> ../run/systemd/reso
lve/stub-resolv.conf

sio@UD1:~$ cd /run/systemd/resolve
sio@UD1:/run/systemd/resolve$ ls -l
total 8
srw-rw-rw- 1 systemd-resolve systemd-resolve 0 févr. 9 13:10 io.systemd.Resol
ve
-rw-r--r-- 1 systemd-resolve systemd-resolve 804 févr. 9 13:10 resolv.conf
-rw-r--r-- 1 systemd-resolve systemd-resolve 936 févr. 9 13:10 stub-resolv.conf
sio@UD1:/run/systemd/resolve$
```

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


```
sio@UD1:~$ cat /run/systemd/resolve/resolv.conf
# This is /run/systemd/resolve/resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# 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 should typically 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@UD1:~$
```

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

```
sio@UD1:~$ dig SOA sio-exupery.local

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-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: 45404
;; 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. 2024020201 604800 86400 2419200 604800

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Feb 09 13:29:31 CET 2024
;; MSG SIZE rcvd: 91

sio@UD1:~$
```

```
sio@UD1:~$ dig DS1.sio-exupery.local

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-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: 62865
;; 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.  86400   IN      A      192.168.4.254

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Feb 09 13:30:21 CET 2024
;; MSG SIZE rcvd: 66

sio@UD1:~$
```

```
sio@UD1:~$ dig www.eni.fr

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> www.eni.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41371
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.eni.fr.                595     IN      CNAME   ip200.eni.fr.
ip200.eni.fr.              595     IN      A       185.42.28.200

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Feb 09 13:31:15 CET 2024
;; MSG SIZE rcvd: 75

sio@UD1:~$
```


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

```
sio@UD1:~$ nslookup www.editions-eyrolles.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.editions-eyrolles.com      canonical name = editions-eyrolles.com.
Name:   editions-eyrolles.com
Address: 89.225.129.16
```

- Faites un ping sur DS1.

```
sio@UD1:~$ 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=0.59
8 ms
64 bytes from DS1.sio-exupery.local (192.168.4.254): icmp_seq=2 ttl=64 time=0.84
7 ms

--- DS1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.598/0.722/0.847/0.124 ms
sio@UD1:~$
```

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

