Diana Margarian
16/02/2024

Chapitre 2 – Serveur Debian DS1 : installation du service DNS

Sommaire :

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.

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.

```
  GNU nano 7.2                                /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
ff02::2 ip6-allrouters
```

2.8 Installation du paquetage BIND

➔ On installe le paquetage BIND avec la commande **apt-get install bind9** 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 :
  bind-doc resolvconf ufw
Les NOUVEAUX paquets suivants seront installés :
  bind9 bind9-utils dns-root-data
0 mis à jour, 3 nouvellement installés, 0 à enlever et 67 non mis à jour.
Il est nécessaire de prendre 904 ko dans les archives.
Après cette opération, 2.042 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
```

➔ On démarre 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 :
➔ Avec la commande **/etc/bind/named.conf** : Qui incluent en général deux fichiers :

```
  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";
```

➔ On visualise les fichiers de configuration dans le répertoire **/etc/bind** :

```
root@DS1: ~#ls -l /etc/bind/
total 48
-rw-r--r-- 1 root root 2403 21 sep 19:33 bind.keys
-rw-r--r-- 1 root root  255 21 sep 19:33 db.0
-rw-r--r-- 1 root root  271 21 sep 19:33 db.127
-rw-r--r-- 1 root root  237 21 sep 19:33 db.255
-rw-r--r-- 1 root root  353 21 sep 19:33 db.empty
-rw-r--r-- 1 root root  270 21 sep 19:33 db.local
-rw-r--r-- 1 root bind  458 21 sep 19:33 named.conf
-rw-r--r-- 1 root bind  498 21 sep 19:33 named.conf.default-zones
-rw-r--r-- 1 root bind  165 21 sep 19:33 named.conf.local
-rw-r--r-- 1 root bind  846 21 sep 19:33 named.conf.options
-rw-r----- 1 bind bind  100  9 fév 10:10 rndc.key
-rw-r--r-- 1 root root 1317 21 sep 19:33 zones.rfc1918
root@DS1: ~#_
```

➔ On sauvegarde 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#_
```

➔ On vérifie l'état du service bind avec la commande systemctl status bind9 :

```
root@DS1: /etc/bind#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 10:13:36 CET; 7min ago
       Docs: man:named(8)
   Main PID: 499 (named)
     Status: "running"
      Tasks: 6 (limit: 2307)
     Memory: 41.7M
        CPU: 135ms
     CGroup: /system.slice/named.service
             └─499 /usr/sbin/named -f -u bind

fév 09 10:13:36 DS1 named[499]: network unreachable resolving './DNSKEY/IN': 2001:500:2d::d#53
fév 09 10:13:36 DS1 named[499]: network unreachable resolving './NS/IN': 2001:500:2d::d#53
fév 09 10:13:36 DS1 systemd[1]: Started named.service - BIND Domain Name Server.
fév 09 10:13:36 DS1 named[499]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance >
fév 09 10:13:36 DS1 named[499]: resolver priming query complete: success
fév 09 10:13:36 DS1 named[499]: checkhints: b.root-servers.net/A (170.247.170.2) missing from hints
fév 09 10:13:36 DS1 named[499]: checkhints: b.root-servers.net/A (199.9.14.201) extra record in hin>
fév 09 10:13:36 DS1 named[499]: checkhints: b.root-servers.net/AAAA (2801:1b8:10::b) missing from h>
fév 09 10:13:36 DS1 named[499]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) extra record >
fév 09 10:13:37 DS1 named[499]: listening on IPv6 interface enp0s8, fe80::a00:27ff:fec1:d61c%3#53
lines 1-22/22 (END)_
```

➔ On installe le paquet recommandé lors de l'installation de bin9 :

```
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.
```

2.9 Zone de recherche directe et zone de recherche inversée

➔ On renseigne 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 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";
```

2.10 Construction des fichiers de zone.

➔ On crée le fichier **/var/cache/bind/db.sio.exupery-local** pour la zone de recherche directe dans lequel on fait figurer les enregistrements correspondant à nos 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
UD3 IN 192.168.4.1_
```

➔ On crée le fichier pour la résolution inverse **/var/cache/bind/rev.sio-exupery.local** dans lequel on fait 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 UD3_sio-exupery.local.
```

➔ On attribue ces deux 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  210  9 fév 10:39 db.sio-exupery.local
-rw-rw-r-- 1 bind bind  821  9 fév 10:14 managed-keys.bind
-rw-rw-r-- 1 bind bind 1717  9 fév 10:13 managed-keys.bind.jnl
-rw-rw-r-- 1 root bind  235  9 fév 10:46 rev.sio-exupery.local
root@DS1: ~#_
```

➔ On vérifie la même appartenance du groupe pour le répertoire :

```
root@DS1: ~#ls -ld /var/cache/bind
drwxrwxr-x 2 root bind 4096  9 fév 10:46 /var/cache/bind
root@DS1: ~#_
```

➢ On remarque qu'il y a bien la même appartenance du groupe pour le répertoire.

2.11 Démarrage et tests du service.

➔ On modifie le fichier **/etc/hosts** qui ne doit contenir que la référence à la boucle locale et le nom FQDN du serveur :

```
  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
```

➔ On désactive les deux interfaces enp0s3 et enp0s8 avec la commande ifdown puis on modifie le fichier **/etc/network/interfaces** pour qu'il contienne les directives dns-search, dns-domain et dns-nameservers :

➔ Network : réseau du lycée

➔ Suppression du DNS sur enp0s3.

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

```
  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
auto enp0s3
iface enp0s3 inet static
address 172.17.101.218
netmask 255.255.0.0
network 172.17.0.0
broadcast 172.17.255.255
gateway 172.17.250.2



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_
```

➔ On réactive les deux interfaces avec la commande ifup puis on vérifie 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 enp0s8
root@DS1: ~#_
```

```
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 : on lance l'utilitaire de vérification **named-checkconf** qui vérifie le fichier **/etc/bind/named.conf.**

➔ On lance 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.**

```
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 2024020901
OK
```

```
root@DS1: /var/cache/bind#named-checkzone -d 4.168.192.in-addr.arpa rev.sio-exupery.local
loading "4.168.192.in-addr.arpa" from "rev.sio-exupery.local" class "IN"
zone 4.168.192.in-addr.arpa/IN: loaded serial 2024020401
OK
root@DS1: /var/cache/bind#_
```

➔ Deuxième test : on ouvre une autre console, puis on se connecte en tant que root

➔ On lance la commande **journalctl -f** permettant de voir en temps réel le journal de base de systemd :

```
root@DS1: ~#journalctl -f
fév 09 11:23:06 DS1 named[6258]: network unreachable resolving 'in-addr.arpa/DNSKEY/IN': 2001:67c:e
::1#53
fév 09 11:24:36 DS1 systemd[1]: Starting systemd-tmpfiles-clean.service - Cleanup of Temporary Direc
tories...
fév 09 11:24:36 DS1 systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
fév 09 11:24:36 DS1 systemd[1]: Finished systemd-tmpfiles-clean.service - Cleanup of Temporary Direc
tories.
fév 09 11:24:36 DS1 systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dclean.service.mount: Deactiva
ted successfully.
fév 09 11:29:26 DS1 systemd[1]: Started getty@tty2.service - Getty on tty2.
fév 09 11:29:39 DS1 login[6283]: pam_unix(login:session): session opened for user root(uid=0) by LOG
IN(uid=0)
fév 09 11:29:39 DS1 systemd-logind[347]: New session 4 of user root.
fév 09 11:29:39 DS1 systemd[1]: Started session-4.scope - Session 4 of User root.
fév 09 11:29:39 DS1 login[6288]: ROOT LOGIN  on '/dev/tty2'
```

➔ On revient sur la première console et on relance le service bind9 :

```
root@DS1: /var/cache/bind#systemctl restart bind9
root@DS1: /var/cache/bind#
```

➔ On observe sur la console la sortie des messages de log pour le service bind9.

➔ On doit voir si le service à démarrer ou s'il indique des erreurs :

```
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './DNSKEY/IN': 2001:500:2d::d#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './NS/IN': 2001:500:2d::d#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './DNSKEY/IN': 2001:503:ba3e::2:30#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './DNSKEY/IN': 2001:dc3::35#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './NS/IN': 2001:dc3::35#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './DNSKEY/IN': 2001:500:12::d0d#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './DNSKEY/IN': 2001:7fe::53#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './NS/IN': 2001:7fe::53#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './DNSKEY/IN': 2001:500:2::c#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './NS/IN': 2001:500:2::c#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './DNSKEY/IN': 2001:7fd::1#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './NS/IN': 2001:7fd::1#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './DNSKEY/IN': 2001:500:9f::42#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './DNSKEY/IN': 2001:500:1::53#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './NS/IN': 2001:500:1::53#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './DNSKEY/IN': 2001:500:a8::e#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './DNSKEY/IN': 2001:503:c27::2:30#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './DNSKEY/IN': 2001:500:200::b#53
fév 09 11:32:23 DS1 named[6298]: network unreachable resolving './NS/IN': 2001:500:200::b#53
fév 09 11:32:24 DS1 named[6298]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance
timer complete)
fév 09 11:32:24 DS1 named[6298]: resolver priming query complete: success
fév 09 11:32:24 DS1 named[6298]: checkhints: b.root-servers.net/A (170.247.170.2) missing from hints
fév 09 11:32:24 DS1 named[6298]: checkhints: b.root-servers.net/A (199.9.14.201) extra record in hin
ts
fév 09 11:32:24 DS1 named[6298]: checkhints: b.root-servers.net/AAAA (2801:1b8:10::b) missing from h
ints
fév 09 11:32:24 DS1 named[6298]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) extra record
in hints
```

2.12 Outils de test de résolution de noms.

➔ On vérifie la présence sur notre 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 provided wit
h BIND 9
root@DS1: ~#_
```

➔ On saisit la commande **dig UD3.sio-exupery.local** :

```
root@DS1: ~#dig UD3.sio-exupery.local

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> UD3.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: 37189
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d5f009a8e1a073cd0100000065c60278d83d12e8dd62bb2 (good)
;; QUESTION SECTION:
;UD3.sio-exupery.local.         IN      A

;; ANSWER SECTION:
UD3.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 11:46:16 CET 2024
;; MSG SIZE  rcvd: 94

root@DS1: ~#_
```

➔ On saisit 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: 39149
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: aaf905b504a7ba870100000065ce0099a7d4013d258efb29 (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
20901 604800 86400 2419200 604800

;; Query time: 4 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Thu Feb 15 13:16:25 CET 2024
;; MSG SIZE  rcvd: 119
```

➔ On saisit 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
```

➔ On saisit 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: 35070
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b86d601310bf75e30100000065ce01f4ef7dd7620e855563 (good)
;; QUESTION SECTION:
;www.dunod.com.                 IN      A

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

;; Query time: 1248 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Thu Feb 15 13:22:12 CET 2024
;; MSG SIZE  rcvd: 86
```

```
root@DS1: ~#nslookup www.eni.fr
;; communications error to 192.168.4.254#53: timed out
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
```

➔ On vérifie enfin la résolution DNS interne et externe avec :

- Un ping sur DS1.sio-exupery.local ;
- Un ping sur UD3.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=0.327 ms
64 bytes from DS1.sio-exupery.local (192.168.4.254): icmp_seq=2 ttl=64 time=0.050 ms

--- DS1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.050/0.188/0.327/0.138 ms
```

```
root@DS1: ~#ping -c 2 UD3
PING UD3.sio-exupery.local (192.168.4.1) 56(84) bytes of data.
64 bytes from UD3.sio-exupery.local (192.168.4.1): icmp_seq=1 ttl=64 time=2.80 ms
64 bytes from UD3.sio-exupery.local (192.168.4.1): icmp_seq=2 ttl=64 time=1.81 ms

--- UD3.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 1.809/2.303/2.798/0.494 ms
```

```
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=34.3 ms
64 bytes from 93.184.221.161: icmp_seq=2 ttl=56 time=35.4 ms

--- cs234.wpc.alphacdn.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 4140ms
rtt min/avg/max/mdev = 34.340/34.877/35.415/0.537 ms
```

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

➔ On commente 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 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, on ouvre avec l'éditeur de texte nano le fichier **/etc/bind/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 no;

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

➔ On décommente la ligne comportant l'instruction forwarders
➔ On modifie 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 { 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; };
};
```


➔ On relance le service DNS
➔ On vérifie 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 2024-02-16 09:25:01 CET; 43s ago
       Docs: man:named(8)
   Main PID: 6317 (named)
     Status: "running"
      Tasks: 4 (limit: 2307)
     Memory: 35.2M
        CPU: 93ms
     CGroup: /system.slice/named.service
             └─6317 /usr/sbin/named -f -u bind

fév 16 09:25:01 DS1 named[6317]: managed-keys-zone: loaded serial 16
fév 16 09:25:01 DS1 named[6317]: zone 127.in-addr.arpa/IN: loaded serial 1
fév 16 09:25:01 DS1 named[6317]: zone 0.in-addr.arpa/IN: loaded serial 1
fév 16 09:25:01 DS1 named[6317]: zone localhost/IN: loaded serial 2
fév 16 09:25:01 DS1 named[6317]: zone 255.in-addr.arpa/IN: loaded serial 1
fév 16 09:25:01 DS1 named[6317]: zone 4.168.192.in-addr.arpa/IN: loaded serial 2024020401
fév 16 09:25:01 DS1 named[6317]: zone sio-exupery.local/IN: loaded serial 2024020901
fév 16 09:25:01 DS1 named[6317]: all zones loaded
fév 16 09:25:01 DS1 systemd[1]: Started named.service - BIND Domain Name Server.
fév 16 09:25:01 DS1 named[6317]: running
root@DS1: ~#
```

➔ On teste 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: 60790
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 631120b00cdd2bb20100000065cf1c3d59cc420654d623ad (good)
;; QUESTION SECTION:
;www.ac-nice.fr.                        IN      A

;; ANSWER SECTION:
www.ac-nice.fr.         20514   IN      CNAME   cs234.wpc.alphacdn.net.
cs234.wpc.alphacdn.net. 3600    IN      A       93.184.221.161

;; Query time: 176 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Fri Feb 16 09:26:37 CET 2024
;; MSG SIZE  rcvd: 123

root@DS1: ~#
```

2.14 Test à partir du client Ubuntu.

➔ On démarre le client Ubuntun UD3 et on vérifie le nom de l'ordinateur dans le fichier **/etc/hostname** :

```
  GNU nano 6.2                          /etc/hostname
UD3
```

➔ On modifie l'association IP-nom FQDN dans le fichier **/etc/hosts** puis on redémarre ensuite la machine Ubuntu :

```
  GNU nano 6.2                           /etc/hosts *
127.0.0.1       localhost
192.168.4.1     UD3.sio-exupery.local   UD3

# 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
```

➔ On configure 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.yam1** (on remplace **NetworkManager** par **networkd dans renderer**).

```
sio@UD3:~$ cd /etc/netplan
sio@UD3:/etc/netplan$ ls
01-network-manager-all.yaml
sio@UD3:/etc/netplan$ sudo nano 01-network-manager-all.yaml
```

➔ On doit 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.

```
  GNU nano 6.2          /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]
```

➔ En une seule commande, netplan apply, on génère le fichier et on redémarre le service :

```
sio@UD3:/etc/netplan$ sudo netplan apply
/etc/netplan/01-network-manager-all.yaml:10:1: Invalid YAML: inconsistent indent
ation:
gateway4: 192.168.4.254
^
```

➔ On vérifie la configuration réseau :

```
sio@UD3:/etc/netplan$ 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
       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 08:00:27:23:66:2c brd ff:ff:ff:ff:ff:ff
    inet 192.168.4.1/24 brd 192.168.4.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::6ff6:2b11:5b32:7bc4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
sio@UD3:/etc/netplan$
```

```
sio@UD3:~$ 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@UD3:~$
```

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

```
sio@UD3:~$ 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@UD3:~$
```

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

```
sio@UD3:~$ ls -l /etc/resolv.conf
lrwxrwxrwx 1 root root 39 févr.  1 16:17 /etc/resolv.conf -> ../run/systemd/reso
lve/stub-resolv.conf
```

```
sio@UD3:~$ cd /run/systemd/resolve
sio@UD3:/run/systemd/resolve$ ls -l
total 8
srw-rw-rw- 1 systemd-resolve systemd-resolve   0 févr. 16 10:05 io.systemd.Resol
ve
-rw-r--r-- 1 systemd-resolve systemd-resolve 804 févr. 16 10:05 resolv.conf
-rw-r--r-- 1 systemd-resolve systemd-resolve 936 févr. 16 10:05 stub-resolv.conf
sio@UD3:/run/systemd/resolve$
```

➔ On affiche le fichier **/run/systemd/resolve/resolv.conf** pour verifier l'adresse du serveur DNS :

```
sio@UD3:~$ 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@UD3:~$
```

➔ On saisit successivement les commandes **dig SOA sio-exupery.local**, **dig DS1.sio-exupery.local** puis **dig www.eni.fr** :

```
sio@UD3:~$ dig SOA sio-exupery.local

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-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: 2181
;; 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. 2024020901 604800 86400 2419200 604800

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Feb 16 10:30:12 CET 2024
;; MSG SIZE  rcvd: 91

sio@UD3:~$
```

```
sio@UD3:~$ dig DS1.sio-exupery.local

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-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: 47372
;; 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: 7 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Feb 16 10:31:04 CET 2024
;; MSG SIZE  rcvd: 66

sio@UD3:~$
```

```
sio@UD3:~$ dig www.eni.fr

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> www.eni.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17515
;; 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.             600     IN      CNAME   ip200.eni.fr.
ip200.eni.fr.           600     IN      A       185.42.28.200

;; Query time: 183 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Feb 16 10:31:37 CET 2024
;; MSG SIZE  rcvd: 75

sio@UD3:~$
```

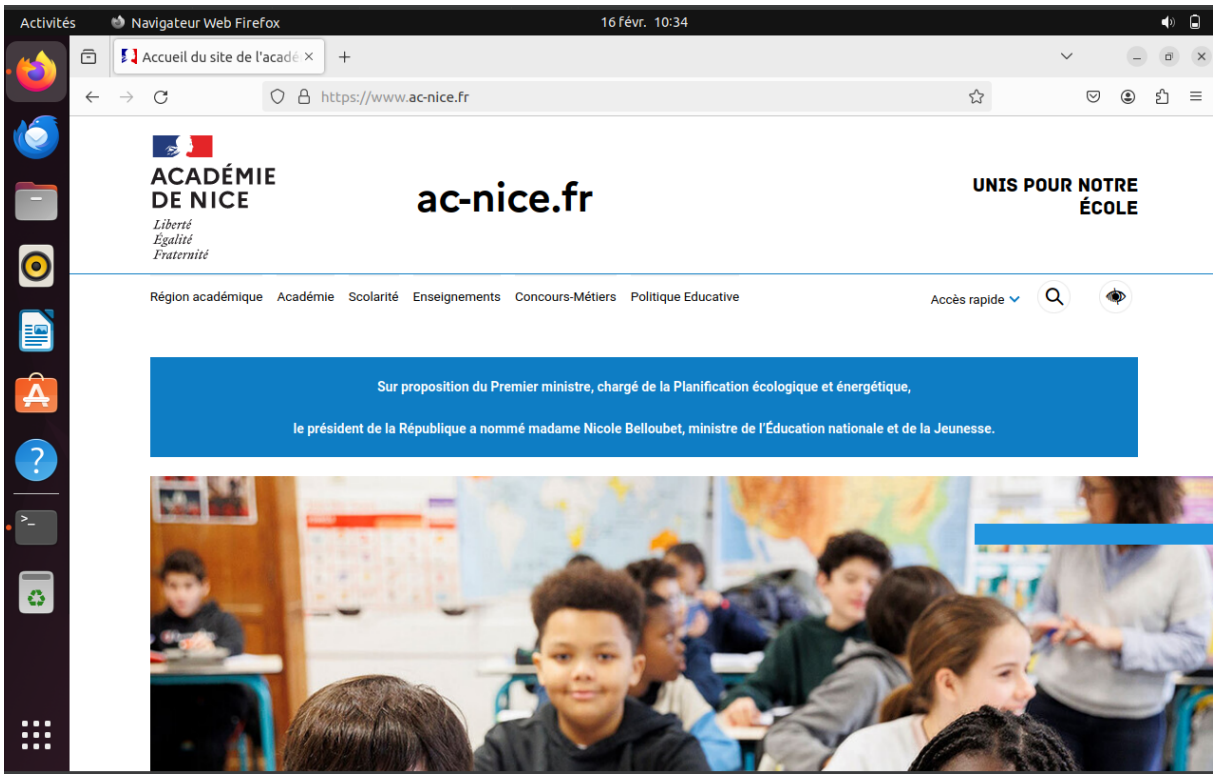
➔ On saisit la commande **nslookup** www.editions-eyrolles.com

```
sio@UD3:~$ 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

sio@UD3:~$
```

➔ On fait un ping sur DS1.

```
sio@UD3:~$ 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=4.33
 ms
64 bytes from DS1.sio-exupery.local (192.168.4.254): icmp_seq=2 ttl=64 time=3.15
 ms

--- DS1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 3.149/3.738/4.327/0.589 ms
sio@UD3:~$
```

➔ On lance le Firefox et on vérifie l'accès à Internet en affichant le site web de l'Académie de Nice.


Activités
Navigateur Web Firefox
16 févr. 10:34
Accueil du site de l'acadé
https://www.ac-nice.fr
ACADÉMIE
DE NICE
Liberté
Égalité
Fraternité
ac-nice.fr
UNIS POUR NOTRE
ÉCOLE
Région académique
Académie
Scolarité
Enseignements
Concours-Métiers
Politique Educative
Accès rapide
Sur proposition du Premier ministre, chargé de la Planification écologique et énergétique,
le président de la République a nommé madame Nicole Belloubet, ministre de l'Éducation nationale et de la Jeunesse.