

Compte-Rendu : Installation du service DNS

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 3.2 /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

- 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
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  bind9utils dns-root-data net-tools python3-ply
Paquets suggérés :
  bind9-doc dnsutils resolvconf ufw python-ply-doc
Les NOUVEAUX paquets suivants seront installés :
  bind9 bind9utils dns-root-data net-tools python3-ply
0 mis à jour, 5 nouvellement installés, 0 à enlever et 27 non mis à jour.
Il est nécessaire de prendre 1 066 ko/1 385 ko dans les archives.
Après cette opération, 5 123 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
```

- 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 :

```
GNU nano 3.2 /etc/bind/named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.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";
```

- 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
cp: impossible d'évaluer 'named.conf.options': Aucun fichier ou dossier de ce type
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
• bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-02-18 09:59:55 CET; 55min left
     Docs: man:named(8)
  Main PID: 526 (named)
    Tasks: 4 (limit: 1150)
   Memory: 16.9M
   CGroup: /system.slice/bind9.service
           └─526 /usr/sbin/named -u bind

févr. 18 09:59:55 DS1 named[526]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
févr. 18 09:59:55 DS1 named[526]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
févr. 18 09:59:55 DS1 named[526]: network unreachable resolving './DNSKEY/IN': 2001:503:c27::2:30#53
févr. 18 09:59:55 DS1 named[526]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
févr. 18 09:59:55 DS1 named[526]: network unreachable resolving './DNSKEY/IN': 2001:7fd::1#53
févr. 18 09:59:55 DS1 named[526]: network unreachable resolving './NS/IN': 2001:7fd::1#53
févr. 18 09:59:55 DS1 named[526]: network unreachable resolving './DNSKEY/IN': 2001:500:12::d0d#53
févr. 18 09:59:55 DS1 named[526]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
févr. 18 09:59:55 DS1 named[526]: managed-keys-zone: Key 20326 for zone . acceptance timer complete:
févr. 18 09:59:55 DS1 named[526]: resolver priming query complete
lines 1-20/20 (END)
```

- 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
Lecture des informations d'état... Fait
resolvconf est déjà la version la plus récente (1.79).
dnsutils est déjà la version la plus récente (1:9.11.5.P4+dfsg-5.1+deb10u2).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 27 non mis à jour.
root@DS1: ~#

```

2.9 Zone de recherche directe et zone de recherche inversée

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

```

GNU nano 3.2 /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
zones "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; };
};_

```

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 3.2 /var/cache/bind/db.sio-exupery.local

; Fichier pour la résolution directe
$TTL 86400
@ IN SOA DS1.sio-exupery.local. root.sio-exupery.local. (
    2019011101
    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 3.2 /var/cache/bind/rev.sio-exupery.local

; Fichier pour la résolution inverse
$TTL 86400
@ IN SOA DS1.sio-exupery.local. root.sio-exupery.local. (
    2019011101
    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 233 févr. 18 09:17 db.sio-exupery.local
-rw-rw-r-- 1 bind bind 821 févr. 18 2021 managed-keys.bind
-rw-rw-r-- 1 bind bind 512 févr. 18 2021 managed-keys.bind.jnl
-rw-rw-r-- 1 root bind 266 févr. 18 09:21 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 févr. 18 09:22 /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 3.2 /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` :

```
GNU nano 3.2 /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 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
```

- 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: ~#_
```

- 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 namedcheckzone sur vos fichiers de zone. 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 2019011101
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 2019011101
OK
root@DS1: /var/cache/bind#_
```

- Ouvrez une autre console (Ctrl+Alt+F2), connectez-vous en tant que root et lancez la commande tail -f /var/log/syslog permettant de voir en temps réel le fichier de logs général.
- 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 logs 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...).

```
Feb 19 16:53:31 DS1 named[1263]: zone 255.in-addr.arpa/IN: loaded serial 1
Feb 19 16:53:31 DS1 named[1263]: zone 127.in-addr.arpa/IN: loaded serial 1
Feb 19 16:53:31 DS1 named[1263]: zone localhost/IN: loaded serial 2
Feb 19 16:53:31 DS1 named[1263]: zone 4.168.192.in-addr.arpa/IN: loaded serial 2019011101
Feb 19 16:53:31 DS1 named[1263]: all zones loaded
Feb 19 16:53:31 DS1 systemd[1]: Started BIND Domain Name Server.
Feb 19 16:53:31 DS1 named[1263]: running
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './DNSKEY/IN': 2001:500:12::d0d#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './DNSKEY/IN': 2001:7fd::1#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './NS/IN': 2001:7fd::1#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './DNSKEY/IN': 2001:7fe::53#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './NS/IN': 2001:7fe::53#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './DNSKEY/IN': 2001:500:a8::e#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './DNSKEY/IN': 2001:dc3::35#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './NS/IN': 2001:dc3::35#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './DNSKEY/IN': 2001:500:2d::d#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './NS/IN': 2001:500:2d::d#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './DNSKEY/IN': 2001:500:200::b#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './NS/IN': 2001:500:200::b#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './DNSKEY/IN': 2001:500:9f::42#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './DNSKEY/IN': 2001:503:c27::2:30#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './DNSKEY/IN': 2001:500:1::53#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './NS/IN': 2001:500:1::53#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './DNSKEY/IN': 2001:503:ba3e::2:30#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './DNSKEY/IN': 2001:500:2::c#53
Feb 19 16:53:31 DS1 named[1263]: network unreachable resolving './NS/IN': 2001:500:2::c#53
Feb 19 16:53:31 DS1 named[1263]: managed-keys-zone: Key 20326 for zone . acceptance timer complete:
key now trusted
Feb 19 16:53:31 DS1 named[1263]: resolver priming query complete
```

- Vérifiez la présence sur votre système du paquetage dnsutils installé à la suite de bind (cf. page 5) :

```
root@DS1: ~#dpkg -l | grep -i dnsutils
ii  dnsutils      1:9.11.5.P4+dfsg-5.1+deb10u2      amd64      Clients provided
with BIND
root@DS1: ~#_
```

- Saisissez la commande host DS1.sio-exupery.local :

```
root@DS1: ~#host DS1.sio-exupery.local
DS1.sio-exupery.local has address 192.168.4.254
root@DS1: ~#
```

- Saisissez la commande host -v DS1.sio-exupery.local ; la sortie écran doit vous montrer les différentes questions au service DNS (QUESTION SECTION) et les réponses conformément aux enregistrements figurant dans les fichiers de configuration :

```

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;DS1.sio-exupery.local.      IN      A

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

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

Received 69 bytes from 192.168.4.254#53 in 6 ms
Trying "DS1.sio-exupery.local"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36723
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;DS1.sio-exupery.local.      IN      AAAA

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

Received 80 bytes from 192.168.4.254#53 in 6 ms
Trying "DS1.sio-exupery.local"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41781
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;DS1.sio-exupery.local.      IN      MX

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

Received 80 bytes from 192.168.4.254#53 in 5 ms
root@DS1: ~#

```

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

```

root@DS1: ~#dig UD1.sio-exupery.local

;<<>> DiG 9.11.5-P4-5.1+deb10u2-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: 49946
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 4096
; COOKIE: 02e00446c44a26fcc18f981f602fe08f47e7779d293e7d93 (good)
;; QUESTION SECTION:
;UD1.sio-exupery.local.          IN      A

;; ANSWER SECTION:
UD1.sio-exupery.local.  86400   IN      A      192.168.4.1

;; 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: ven. févr. 19 17:00:15 CET 2021
;; MSG SIZE rcvd: 128

root@DS1: ~#

```

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

```

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

;<<>> DiG 9.11.5-P4-5.1+deb10u2-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: 36237
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 4096
; COOKIE: 55629ba3d4ec93f528b0eca2602fe0b7933ea09925f7b88d (good)
;; 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: ven. févr. 19 17:00:55 CET 2021
;; MSG SIZE rcvd: 149

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 9.11.5-P4-5.1+deb10u2-Debian <<>> www.dunod.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50303
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;; udp: 4096
; COOKIE: e7d709e7ea454740539a4ee8602fe123699ac12113cbf471 (good)
;; QUESTION SECTION:
;www.dunod.com.                IN      A

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

;; Query time: 2296 msec
;; SERVER: 192.168.4.254#53(192.168.4.254)
;; WHEN: ven. févr. 19 17:02:43 CET 2021
;; MSG SIZE rcvd: 86

root@DS1: ~#

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

root@DS1: ~#

```

- 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=0.045 ms
64 bytes from DS1.sio-exupery.local (192.168.4.254): icmp_seq=2 ttl=64 time=0.024 ms

--- DS1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 4ms
rtt min/avg/max/mdev = 0.024/0.034/0.045/0.012 ms
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=0.328 ms
64 bytes from UD1.sio-exupery.local (192.168.4.1): icmp_seq=2 ttl=64 time=0.310 ms

--- UD1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1ms
rtt min/avg/max/mdev = 0.310/0.319/0.328/0.009 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=57 time=15.3 ms
64 bytes from 93.184.221.161: icmp_seq=2 ttl=57 time=10.1 ms

--- cs234.wpc.alphacdn.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 10.070/12.688/15.306/2.618 ms
root@DS1: ~#

```

2.13 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 3.2 /etc/bind/named.conf.default-zones

// prime the server with knowledge of the root servers
//zone "." {
//    type hint;
//    file "/usr/share/dns/root.hints";
//};

```

- Ouvrez avec l'éditeur de texte nano (ou vim) le fichier /etc/bind/named.conf.options. Décommentez la ligne comportant l'instruction forwarders et modifiez le fichier de la manière suivante :

```

GNU nano 3.2 /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; };
    listen-on-v6 { any; };
};

```

- Relancez le service DNS et testez à nouveau une résolution externe à partir du serveur DS1 ; la résolution devrait être plus rapide :

```

root@DS1: ~#systemctl restart bind9
root@DS1: ~#
root@DS1: ~#dig www.ac-nice.fr

; <<>> DiG 9.11.5-P4-5.1+deb10u2-Debian <<>> www.ac-nice.fr
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24669
; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::; udp: 4096
; COOKIE: 7c107482181d864a1377c8db602fefce575a873ab553b1e1 (good)
; QUESTION SECTION:
;www.ac-nice.fr.                                IN      A

; ANSWER SECTION:
www.ac-nice.fr.                21546   IN      CNAME   cs234.wpc.alphacdn.net.
cs234.wpc.alphacdn.net.       3546    IN      A       93.184.221.161

; Query time: 25 msec
; SERVER: 192.168.4.254#53(192.168.4.254)
; WHEN: ven. févr. 19 18:05:18 CET 2021
; 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 :

```

GNU nano 4.8 /etc/hostname
sio-virtualbox

```

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

```

GNU nano 4.8 /etc/hosts
127.0.0.1    localhost
192.168.4.1  UD1.sio-exupery.local  UD1

```

- 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).

```

GNU nano 4.8                                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]

```

- 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@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 08:00:27:03:fe:54 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::3ab1:38a8:c96b:427b/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 metric 100
sio@ud1:~$

```

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

```
sio@ud1:~$ 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 "resolvectl 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
options edns0
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 févr.  4 10:08 /etc/resolv.conf -> ../run/systemd/res
olve/stub-resolv.conf
sio@ud1:~$

sio@ud1:~$ cd /run/systemd/resolve
sio@ud1:/run/systemd/resolve$ ls -l
total 8
drwx----- 2 systemd-resolve systemd-resolve 60 févr. 19 17:34 netif
-rw-r--r-- 1 systemd-resolve systemd-resolve 615 févr. 19 17:40 resolv.conf
-rw-r--r-- 1 systemd-resolve systemd-resolve 733 févr. 19 17:40 stub-resolv.con
f
sio@ud1:/run/systemd/resolve$
```

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

```
sio@ud1:/run/systemd/resolve$ 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@ud1:/run/systemd/resolve$
```

- 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 9.16.1-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: 44666
;; 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: ven. févr. 19 18:09:04 CET 2021
;; MSG SIZE rcvd: 91

sio@ud1:~$
```

```

sio@ud1:~$ dig DS1.sio-exupery.local

; <<>> DiG 9.16.1-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: 31364
;; 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)
;; WHEN: ven. févr. 19 18:08:03 CET 2021
;; MSG SIZE rcvd: 66

sio@ud1:~$
sio@ud1:~$ dig www.eni.fr

; <<>> DiG 9.16.1-Ubuntu <<>> www.eni.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52240
;; 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.              600     IN      A      185.42.28.200

;; Query time: 56 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: ven. févr. 19 18:07:01 CET 2021
;; MSG SIZE rcvd: 55

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:
Name:   www.editions-eyrolles.com
Address: 213.244.11.249

sio@ud1:~$
```

- 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=0.326 ms
64 bytes from DS1.sio-exupery.local (192.168.4.254): icmp_seq=2 ttl=64 time=0.325 ms

--- DS1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1031ms
rtt min/avg/max/mdev = 0.325/0.325/0.326/0.000 ms
sio@ud1:~$
```

- Lancez Firefox et vérifiez l'accès à Internet.

