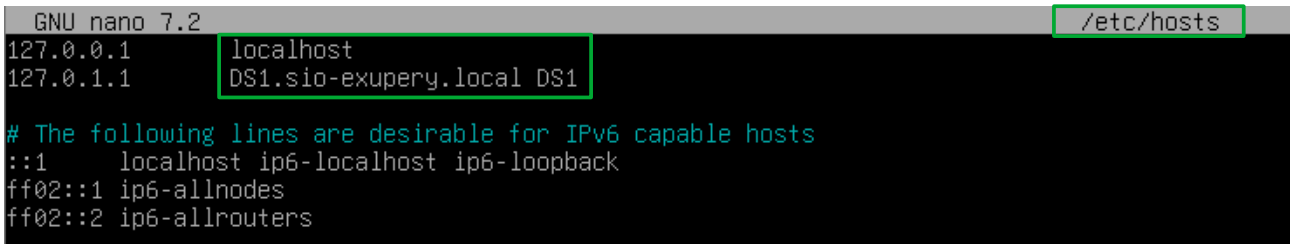
BTS 1 - Services Informatiques aux Organisations

Chap2 Serveur Debian DS1 : installation du service DNS

Table des matières

1. Avant l'installation du service

Modification dans le fichier /etc/hosts grâce à la commande **nano /etc/hosts**



2. Installation du paquetage BIND

Installation du paquetage BIND9 par la commande **apt-get install bind9**

```
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 ufw
Les NOUVEAUX paquets suivants seront installés :
  bind9 bind9-utils dns-root-data
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 917 ko dans les archives.
Après cette opération, 2 080 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 bind9-utils amd64 1:9.18.28-1~deb12u2 [413 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 dns-root-data all 2024041801~deb12u1 [4 356 B]
Réception de :3 http://deb.debian.org/debian bookworm/main amd64 bind9 amd64 1:9.18.28-1~deb12u2 [500 kB]
917 ko réceptionnés en 2s (578 ko/s)
Sélection du paquet bind9-utils précédemment désélectionné.
(Lecture de la base de données... 33870 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../bind9-utils_1%3a9.18.28-1~deb12u2_amd64.deb ...
Dépaquetage de bind9-utils (1:9.18.28-1~deb12u2) ...
Sélection du paquet dns-root-data précédemment désélectionné.
Préparation du dépaquetage de .../dns-root-data_2024041801~deb12u1_all.deb ...
Dépaquetage de dns-root-data (2024041801~deb12u1) ...
Sélection du paquet bind9 précédemment désélectionné.
Préparation du dépaquetage de .../bind9_1%3a9.18.28-1~deb12u2_amd64.deb ...
Dépaquetage de bind9 (1:9.18.28-1~deb12u2) ...
Paramétrage de dns-root-data (2024041801~deb12u1) ...
Paramétrage de bind9-utils (1:9.18.28-1~deb12u2) ...
Paramétrage de bind9 (1:9.18.28-1~deb12u2) ...
Ajout du groupe « bind » (GID 110)...
Fait.
Ajout de l'utilisateur système « bind » (UID 102) ...
Ajout du nouvel utilisateur « bind » (UID 102) avec pour groupe d'appartenance « bind » ...
Pas de création du répertoire personnel « /var/cache/bind ».
wrote key file "/etc/bind/rndc.key"
named-resolvconf.service is a disabled or a static unit, not starting it.
Created symlink /etc/systemd/system/bind9.service → /lib/systemd/system/named.service.
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /lib/systemd/system/named.service.
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
root@DS1: ~#_
```

Démarrage du service DNS BIND avec la commande **systemctl start bind9**

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

Vérification des configurations BIND dans le fichier **/etc/bind/named.conf**

```
  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";
```

Vérification des configurations BIND dans 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 auto;

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

Vérification des configurations BIND dans le fichier **/etc/bind/named.conf.local**

```
  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";
```

Visualisation des fichiers de configuration dans le répertoire /bind par la commande **ls -l /etc/bind/**

```
root@DS1: ~#ls -l /etc/bind/
total 60
-rw-r--r-- 1 root root 2403 27 juil.  2024 bind.keys
-rw-r--r-- 1 root root  255 27 juil.  2024 db.0
-rw-r--r-- 1 root root  271 27 juil.  2024 db.127
-rw-r--r-- 1 root root  237 27 juil.  2024 db.255
-rw-r--r-- 1 root root  353 27 juil.  2024 db.empty
-rw-r--r-- 1 root root  270 27 juil.  2024 db.local
-rw-r--r-- 1 root bind  458 22 janv. 09:26 named.conf
-rw-r--r-- 1 root bind  506 29 janv. 09:55 named.conf.default-zones
-rw-r--r-- 1 root bind  389 29 janv. 10:17 named.conf.local
-rw-r--r-- 1 root bind  165 22 janv. 09:30 named.conf.local.sauv
-rw-r--r-- 1 root bind  885 29 janv. 13:48 named.conf.options
-rw-r--r-- 1 root bind  846 22 janv. 09:29 named.conf.options.sauv
-rw-r--r-- 1 root bind  458 22 janv. 09:29 named.conf.sauv
-rw-r----- 1 bind bind  100 22 janv. 09:23 rndc.key
-rw-r--r-- 1 root root 1317 27 juil.  2024 zones.rfc1918
root@DS1: ~#
```

Sauvegarde des fichiers de configuration vers des fichiers terminant par .sauv avec la commande **cp**

```
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#_
```

Vérification de 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 Wed 2025-01-22 09:23:16 CET; 7min ago
       Docs: man:named(8)
   Main PID: 808 (named)
     Status: "running"
      Tasks: 8 (limit: 2315)
     Memory: 34.8M
        CPU: 75ms
     CGroup: /system.slice/named.service
             └─808 /usr/sbin/named -f -u bind

janv. 22 09:23:16 DS1 named[808]: network unreachable resolving './NS/IN': 2001:500:1::53#53
janv. 22 09:23:16 DS1 named[808]: network unreachable resolving './DNSKEY/IN': 2001:7fe::53#53
janv. 22 09:23:16 DS1 named[808]: network unreachable resolving './NS/IN': 2001:7fe::53#53
janv. 22 09:23:16 DS1 named[808]: network unreachable resolving './DNSKEY/IN': 2001:dc3::35#53
janv. 22 09:23:16 DS1 named[808]: network unreachable resolving './NS/IN': 2001:dc3::35#53
janv. 22 09:23:16 DS1 named[808]: network unreachable resolving './DNSKEY/IN': 2001:500:2::c#53
janv. 22 09:23:16 DS1 named[808]: network unreachable resolving './NS/IN': 2001:500:2::c#53
janv. 22 09:23:16 DS1 named[808]: managed-keys-zone: Initializing automatic trust anchor management
janv. 22 09:23:16 DS1 named[808]: managed-keys-zone: Initializing automatic trust anchor management
janv. 22 09:23:16 DS1 named[808]: resolver priming query complete: success
lines 1-22/22 (END)_
```

Installation du paquet resolvconf avec la commande **apt-get install resolvconf**

```
root@DS1: ~#apt-get install resolvconf
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
resolvconf est déjà la version la plus récente (1.91+nmu1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@DS1: ~#_
```

3. Zone de recherche directe et zone de recherche inversée

Renseignements des zones dans le fichier **/etc/bind/named.conf.local**

```
 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; };
};_
```

Affichage de l'emplacement des fichiers de zones **db.sio-exupery.local** et **rev.sio-exupery.local** dans le fichier le fichier **named.conf.options**

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

4. Construction des fichiers de zone

Création du fichier **db.sio-exupery.local** pour la zone de recherche directe.

```
  GNU nano 7.2                                  /var/cache/bind/db.sio-exupery.local
; Fichier pour la résolution directe
$TTL 86400
@ IN SOA DS1.sio-exupery.local root.sio-exupery.local. (
        2024020401
        1w
        1d
        4w
        1w )

@ IN NS DS1.sio-exupery.local.
DS1 IN A 192.168.4.254
UD1 IN A 192.168.4.1
```

Création du fichier **rev.sio-exupery.local** pour la zone de recherche inverse.

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

Attribution ces 2 fichiers de zone au groupe **BIND** afin de les rendre accessibles au démon avec la commande **chgrp bind /var/cache/bind/*** et **chmod 664 /var/cache/bind/***

```
root@DS1: ~#chgrp bind /var/cache/bind/*
root@DS1: ~#chmod 664 /var/cache/bind/*
root@DS1: ~#
```

Affichage des droits des fichiers **db.sio-exupery.local** et **rev.sio-exupery.local** par la commande **ls -l /var/cache/bind**

```
root@DS1: ~#ls -l /var/cache/bind
total 16
-rw-rw-r-- 1 root bind  212 29 janv. 09:23 db.sio-exupery.local
-rw-r--r-- 1 bind bind  221 29 janv. 09:07 managed-keys.bind
-rw-r--r-- 1 bind bind 2438 29 janv. 09:06 managed-keys.bind.jnl
-rw-r--r-- 1 root root  233 29 janv. 09:32 rev.sio-exupery.local
root@DS1: ~#_
```

Affichage de l'appartenance du groupe pour le répertoire bind grâce à la commande
ls -ld /var/cache/bind

```
root@DS1: ~#ls -ld /var/cache/bind
drwxrwxr-x 2 root bind 4096 22 janv. 10:09 /var/cache/bind
root@DS1: ~#_
```

5. Démarrage et tests du services

Modification du fichier **/etc/hosts** pour l'adresse 127.0.0.1 et 192.168.4.254

```
  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
```

Désactivation de l'interface enp0s3 et enp0s8 avec la commande **ifdown**

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

Configuration de l'interface ep0s3 et enp0s8 avec la commande **nano /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 172.17.101.214
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_


#This is an autoconfigured IPv6 interface
#iface enp0s3 inet6 auto
```

Activation de l'interface enp0s3 et enp0s8 avec la commande **ifup**

```
root@DS1: ~#ifup enp0s3
root@DS1: ~#ifup enp0s8
root@DS1: ~#
```

Vérification de l'adresse DNS avec la commande **cat /etc/resolv.conf**

```
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: ~#
```

Désactivation de DNSSEC avec l'instruction dnssec-validation sur **no** 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 no;

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

Re-lancement du service BIND avec la commande **systemctl restart bind9**

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

Vérification de la configuration avec l'utilitaire **named-checkconf**

```
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 2024020401
OK
root@DS1: /var/cache/bind#_
```

Vérification de la configuration avec l'utilitaire **named-checkzone**

```
root@DS1: ~#cd /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 2024020401
OK
root@DS1: /var/cache/bind#_
```

Visualisation des journaux avec la commande **journalctl -f** pour voir le journal de base de systemd.

```
root@DS1: ~#journalctl -f
janv. 29 09:17:02 DS1 CRON[591]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
janv. 29 09:17:02 DS1 CRON[592]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)
janv. 29 09:17:02 DS1 CRON[591]: pam_unix(cron:session): session closed for user root
janv. 29 09:28:01 DS1 systemd[1]: Starting apt-daily-upgrade.service - Daily apt upgrade and clean activities...
janv. 29 09:28:03 DS1 systemd[1]: apt-daily-upgrade.service: Deactivated successfully.
janv. 29 09:28:03 DS1 systemd[1]: Finished apt-daily-upgrade.service - Daily apt upgrade and clean activities.
janv. 29 09:29:36 DS1 systemd[1]: Starting systemd-tmpfiles-clean.service - Cleanup of Temporary Directories...
janv. 29 09:29:37 DS1 systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
janv. 29 09:29:37 DS1 systemd[1]: Finished systemd-tmpfiles-clean.service - Cleanup of Temporary Directories.
janv. 29 09:29:37 DS1 systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dclean.service.mount: Deactivated successfully.
```

Vérification du service BIND9 avec la commande **systemctl restart bind9**

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

Sortie des messages de log pour le service BIND9

```
janv. 29 09:37:55 DS1 named[685]: automatic empty zone: RESOLVER.ARPA
janv. 29 09:37:55 DS1 named[685]: configuring command channel from '/etc/bind/rndc.key'
janv. 29 09:37:55 DS1 named[685]: command channel listening on 127.0.0.1#953
janv. 29 09:37:55 DS1 named[685]: configuring command channel from '/etc/bind/rndc.key'
janv. 29 09:37:55 DS1 named[685]: command channel listening on ::1#953
janv. 29 09:37:55 DS1 named[685]: managed-keys-zone: loaded serial 8
janv. 29 09:37:55 DS1 named[685]: zone 0.in-addr.arpa/IN: loaded serial 1
janv. 29 09:37:55 DS1 named[685]: zone 127.in-addr.arpa/IN: loaded serial 1
janv. 29 09:37:55 DS1 named[685]: zone 255.in-addr.arpa/IN: loaded serial 1
janv. 29 09:37:55 DS1 named[685]: zone localhost/IN: loaded serial 2
janv. 29 09:37:55 DS1 named[685]: zone 4.168.192.in-addr.arpa/IN: loaded serial 2024020401
janv. 29 09:37:55 DS1 named[685]: zone sio-exupery.local/IN: loaded serial 2024020401
janv. 29 09:37:55 DS1 named[685]: all zones loaded
janv. 29 09:37:55 DS1 systemd[1]: Started named.service - BIND Domain Name Server.
janv. 29 09:37:55 DS1 named[685]: running
janv. 29 09:37:55 DS1 named[685]: zone sio-exupery.local/IN: sending notifies (serial 2024020401)
```

6. Outils de test de résolution de noms

Vérification de la présence sur le système du paquetage dnsutils avec la commande
dpkg -l | grep -i dnsutils

```
root@DS1: ~#dpkg -l | grep -i dnsutils
ii  bind9-dnsutils              1:9.18.28-1~deb12u2           amd64        Clients provided with BIND 9
root@DS1: ~#
```

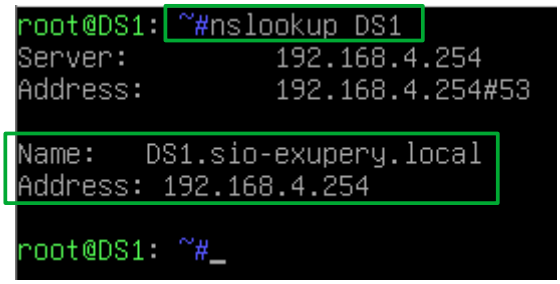
Tests DNS internes et externes :
Commande **dig UD1.sio-exupery.local**

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

; <<>> DiG 9.18.28-1~deb12u2-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: 414
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 043514cc48a2bf5c010000006799e9de4976ff83056a0fbc (good)
;; QUESTION SECTION:
;UD1.sio-exupery.local.         IN      A

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

;; Query time: 4 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Wed Jan 29 09:42:06 CET 2025
;; MSG SIZE  rcvd: 94

root@DS1: ~#_
```

Commande **dig SOA sio-exupery.local**

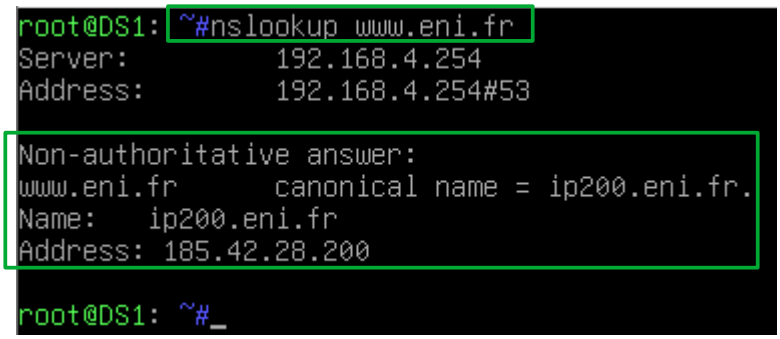
```
root@DS1: ~#dig SOA sio-exupery.local

; <<>> DiG 9.18.28-1~deb12u2-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: 58662
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 4e89f96523a67b4b010000006799ea88563cfe167afed772 (good)
;; QUESTION SECTION:
;sio-exupery.local.             IN      SOA

;; ANSWER SECTION:
sio-exupery.local.      86400   IN      SOA     DS1.sio-exupery.local.sio-exupery.local. root.sio-exupery.local. 202

;; Query time: 0 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Wed Jan 29 09:44:56 CET 2025
;; MSG SIZE  rcvd: 154
```

Commande **nslookup DS1** pour voir l'adresse IP DS1.sio-exupery.local



Commande **dig www.dunod.com**

Commande **nslookup www.eni.fr**



Vérification de la résolution DNS interne et externe sur DS1, US1 et 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=0.035 ms
64 bytes from DS1.sio-exupery.local (192.168.4.254): icmp_seq=2 ttl=64 time=0.059 ms

--- DS1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1137ms
rtt min/avg/max/mdev = 0.035/0.047/0.059/0.012 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=0.583 ms
64 bytes from UD1.sio-exupery.local (192.168.4.1): icmp_seq=2 ttl=64 time=0.757 ms

--- UD1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1026ms
rtt min/avg/max/mdev = 0.583/0.670/0.757/0.087 ms
root@DS1: ~#ping -c 2 www.ac-nice.fr
PING www.ac-nice.fr.cdn.cloudflare.net (141.101.90.106) 56(84) bytes of data.
64 bytes from 141.101.90.106 (141.101.90.106): icmp_seq=1 ttl=56 time=34.9 ms
64 bytes from 141.101.90.106 (141.101.90.106): icmp_seq=2 ttl=56 time=46.2 ms

--- www.ac-nice.fr.cdn.cloudflare.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1193ms
rtt min/avg/max/mdev = 34.868/40.547/46.227/5.679 ms
root@DS1: ~#
```

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

Mise en place des lignes en commentaires du fichier **named.conf.defoult-zones** qui ont des traits au serveurs racines.

```
  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";
//};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};
```

Mise en place de la redirection avec la ligne dnssec-validation sur **no** 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 no;

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

Décommentation de la ligne comportant l'instruction **forwarders** 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.

        forward only;
        forwarders { 172.17.254.1 };
        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; };
};
```

Relancement du service DNS et vérification du service BIND9 avec la commande **systemctl restart bind9** et **systemctl status bind9**

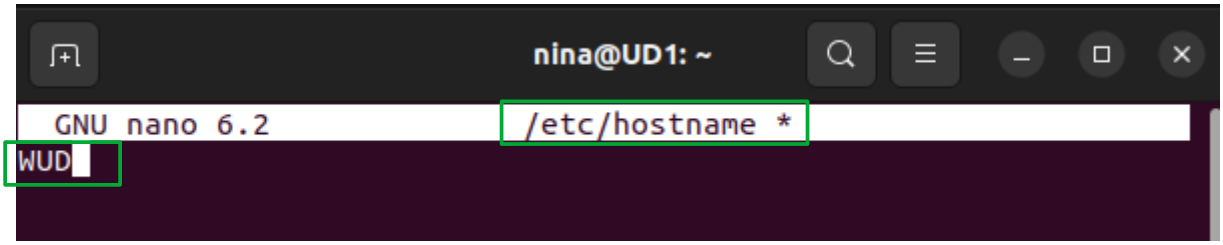
```
root@DS1: ~#systemctl restart bind9
root@DS1: ~#systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-01-29 13:49:01 CET; 7s ago
       Docs: man:named(8)
   Main PID: 619 (named)
     Status: "running"
      Tasks: 6 (limit: 2315)
     Memory: 30.6M
        CPU: 27ms
     CGroup: /system.slice/named.service
             └─619 /usr/sbin/named -f -u bind

janv. 29 13:49:01 DS1 named[619]: zone 4.168.192.in-addr.arpa/IN: loaded serial 2024020401
janv. 29 13:49:01 DS1 named[619]: zone 0.in-addr.arpa/IN: loaded serial 1
janv. 29 13:49:01 DS1 named[619]: zone sio-exupery.local/IN: loaded serial 2024020401
janv. 29 13:49:01 DS1 named[619]: zone sio-exupery.local/IN: sending notifies (serial 2024020401)
janv. 29 13:49:01 DS1 named[619]: zone 127.in-addr.arpa/IN: loaded serial 1
janv. 29 13:49:01 DS1 named[619]: zone 255.in-addr.arpa/IN: loaded serial 1
janv. 29 13:49:01 DS1 named[619]: zone localhost/IN: loaded serial 2
janv. 29 13:49:01 DS1 named[619]: all zones loaded
janv. 29 13:49:01 DS1 systemd[1]: Started named.service - BIND Domain Name Server.
janv. 29 13:49:01 DS1 named[619]: running
root@DS1: ~#
```

Test de la résolution externe à partir du serveur DS1 avec la commande **dig www.ac-nice.fr**

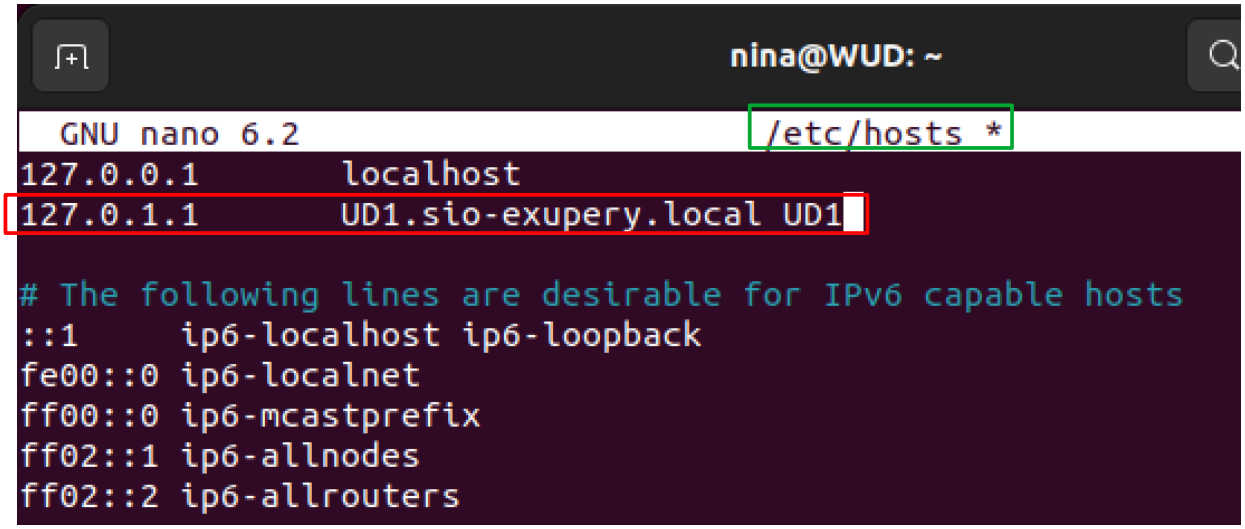
```
root@DS1: ~#dig www.ac-nice.fr

; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> www.ac-nice.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53079
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c025dbcc6ad576e801000000679a2426b6bbd4cdca10d284 (good)
;; QUESTION SECTION:
;www.ac-nice.fr.                        IN      A

;; ANSWER SECTION:
www.ac-nice.fr.         1039    IN      CNAME   www.ac-nice.fr.cdn.cloudflare.net.
www.ac-nice.fr.cdn.cloudflare.net. 300 IN A     141.101.90.106
www.ac-nice.fr.cdn.cloudflare.net. 300 IN A     141.101.90.105
www.ac-nice.fr.cdn.cloudflare.net. 300 IN A     141.101.90.104
www.ac-nice.fr.cdn.cloudflare.net. 300 IN A     141.101.90.107

;; Query time: 92 msec
;; SERVER: 192.168.4.254#53(192.168.4.254) (UDP)
;; WHEN: Wed Jan 29 13:50:46 CET 2025
;; MSG SIZE  rcvd: 182

root@DS1: ~#
```

8. Test à partir du client Ubuntu

Démarrage du client Ubuntu UD1 et vérification du nom de l'ordinateur dans le fichier **/etc/hostname**

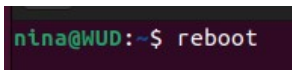


Modification du nom de l'ordinateur dans le fichier **/etc/hosts**

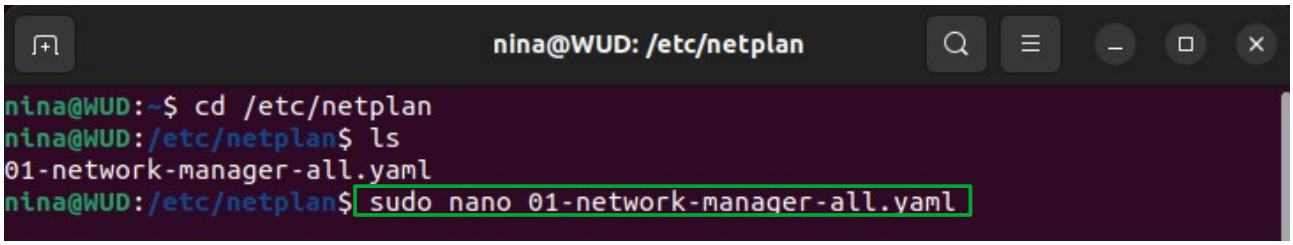


→ Les modifications n'ayant pas été correctement enregistrées pour renommer UD1, la machine sera nommée WUD pour la suite du TP.

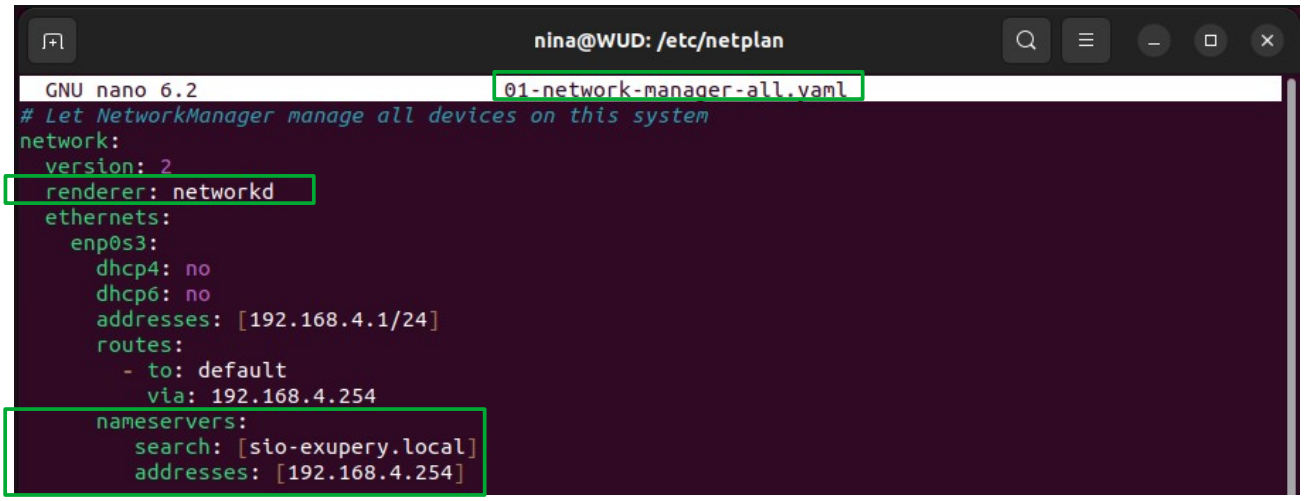
Redémarrage de la machine Ubuntu par la commande **reboot**



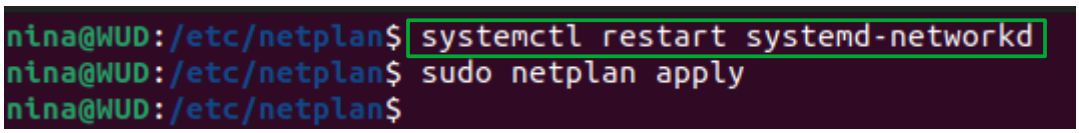
Configuration des paramètres IP et de l'adresse du serveur DNS.



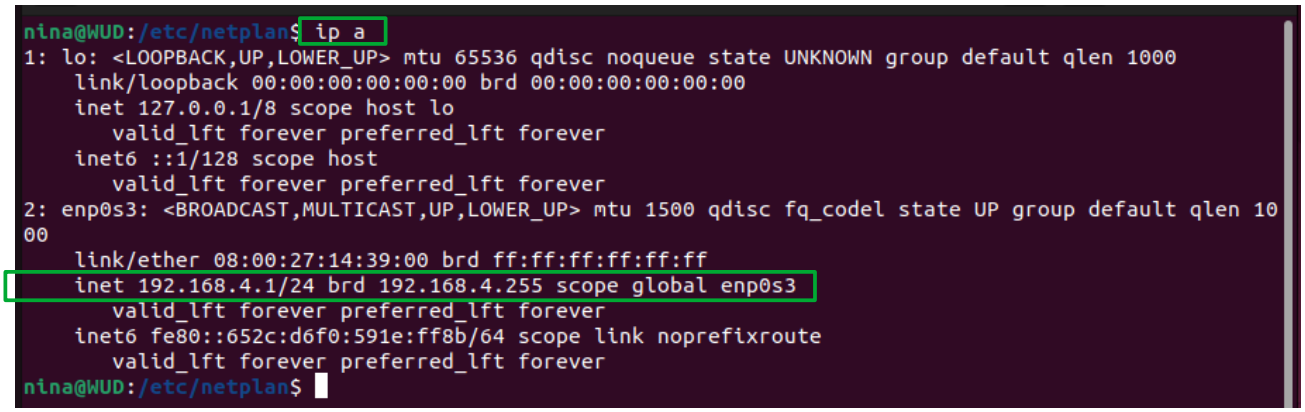
Configuration des paramètres IP et de l'adresse du serveur DNS.



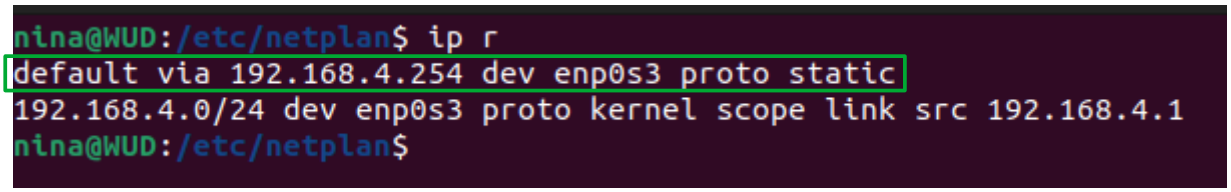
Pour redémarrer la service systemd-networkd et appliquer la configuration réseau avec la commande **systemctl restart systemd-networkd** et **sudo netplan appy**



Vérification de la configuration réseau avec la commande **ip a**



Vérification de la configuration réseau avec la commande **ip r**



Vérification de la configuration réseau avec la commande **cat /etc/resolv.conf**

```
nina@WUD:/etc/netplan$ 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
nina@WUD:/etc/netplan$
```

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

```
nina@WUD:~$ ls -l /etc/resolv.conf
lrwxrwxrwx 1 root root 39 janv. 10 14:32 /etc/resolv.conf -> ../run/systemd/resolve/stub-resolv.conf
nina@WUD:~$
```

Vérification des fichiers s'appelant resolv avec la commande **cd /run/systemd/resolv**

```
nina@WUD:~$ cd /run/systemd/resolve
nina@WUD:/run/systemd/resolve$ ls -l
total 8
srw-rw-rw- 1 systemd-resolve systemd-resolve   0 janv. 29 14:07 io.systemd.Resolve
drwx------ 2 systemd-resolve systemd-resolve  60 janv. 29 14:07 netif
-rw-r--r-- 1 systemd-resolve systemd-resolve 804 janv. 29 14:27 resolv.conf
-rw-r--r-- 1 systemd-resolve systemd-resolve 936 janv. 29 14:27 stub-resolv.conf
nina@WUD:/run/systemd/resolve$
```

Affichage du fichier **resolv.conf** pour vérifier l'adresse du serveur DNS

```
nina@WUD:/run/systemd/resolve$ 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
nina@WUD:/run/systemd/resolve$
```

La commande **dig SOA sio-exupery.local**

```
nina@WUD:~$ 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: 24639
;; 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.sio-exupery.local. root.sio-exupery.
local. 2024020401 604800 86400 2419200 604800

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Jan 29 14:36:53 CET 2025
;; MSG SIZE  rcvd: 109

nina@WUD:~$
```

La commande **dig DS1.sio-exupery.local**

```
nina@WUD:~$ 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: 27379
;; 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: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Jan 29 14:38:53 CET 2025
;; MSG SIZE  rcvd: 66

nina@WUD:~$
```

La commande **dig www.eni.fr**

```
nina@WUD:~$ 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: 63357
;; 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: 63 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Jan 29 14:39:54 CET 2025
;; MSG SIZE  rcvd: 75

nina@WUD:~$
```

La commande **nslookup www.editions-eyrolles.com**

```
nina@WUD:~$ 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 = app943253.prod.cudawaas.com.
app943253.prod.cudawaas.com     canonical name = waas-prod-app-a978c6906656d1f69447ac81ef5f2
9ee.trafficmanager.net.
waas-prod-app-a978c6906656d1f69447ac81ef5f29ee.trafficmanager.net       canonical name = waa
sprod-app-53c57dcd5270778795e5d53a512d0297.francecentral.cloudapp.azure.com.
Name:   waasprod-app-53c57dcd5270778795e5d53a512d0297.francecentral.cloudapp.azure.com
Address: 4.176.6.76

nina@WUD:~$
```

La commande **ping -c 2 DS1**

```
nina@WUD:~$ ping -c 2 DS1
PING DS1.sio-exupery.local (192.168.4.254) 56(84) bytes of data.
64 bytes from DS1.sio-exupery.local (192.168.4.254): icmp_seq=1 ttl=64 time=0.394 ms
64 bytes from DS1.sio-exupery.local (192.168.4.254): icmp_seq=2 ttl=64 time=0.922 ms

--- DS1.sio-exupery.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.394/0.658/0.922/0.264 ms
nina@WUD:~$
```

Vérification de l'accès à Internet en affichant le site web de l'Académie de Nice.