

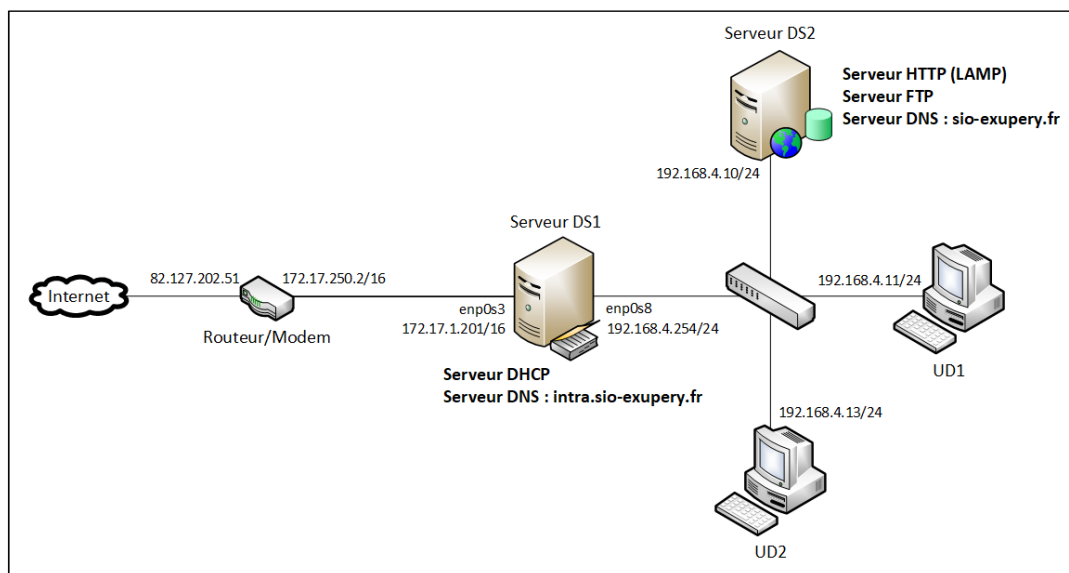
Chapitre 6 – Serveur Debian DS2 et DS1 : délégation DNS

Pour l'instant, le serveur DS1 sert de serveur DNS pour la zone **sio-exupery.local**. L'objectif est maintenant de recourir à un **nom de domaine internet en .fr** soit **sio-exupery.fr** (il n'est pas envisageable d'utiliser un nom de domaine en .fr dans l'arborescence mondiale sans que celui-ci ne soit déposé auprès de l'**AFNIC**).

Deux serveurs DNS vont être mis en œuvre :

- DS2 : serveur DNS pour la zone **sio-exupery.fr** ;
- DS1 : **serveur DNS en délégation** pour la zone **intra.sio-exupery.fr**.

La zone **sio-exupery.local** doit être supprimée au profit d'une **délégation de zone** en Intranet.



1. Installation du nouveau service DNS sur DS2

- Installez BIND9 sur le serveur DS2 (cf. chapitre 2 pages 4 et 5).
- Renseignez le fichier **/etc/bind/named.conf.local** avec cette fois-ci les zones suivantes :

```
GNU nano 2.7.4 Fichier : /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.fr" IN {
    type master;
    file "db.sio-exupery.fr";
    allow-update { none; };
};

zone "4.168.192.in-addr.arpa" IN {
    type master;
    file "rev.sio-exupery.fr";
    allow-update { none; };
};
```

- Créez le fichier **/var/cache/bind/db.sio-exupery.fr** pour la **zone de recherche directe** avec l'inscription d'un **serveur DNS en délégation** pour la zone **intra.sio-exupery.fr** et des **alias (CNAME)** pour le serveur Web et FTP :

```

GNU nano 2.7.4          Fichier : /var/cache/bind/db.sio-exupery.fr
; Fichier pour la résolution directe
$TTL 86400
@      IN SOA  DS2.sio-exupery.fr. root.sio-exupery.fr. (
                2019020701
                1w
                1d
                4w
                1w )
@      IN NS   DS2.sio-exupery.fr.
intra.sio-exupery.fr.      IN NS   DS1.intra.sio-exupery.fr.
DS2.sio-exupery.fr.      IN A    192.168.4.10
DS1.intra.sio-exupery.fr. IN A    192.168.4.254
ftp      IN     CNAME DS2
www      IN     CNAME DS2

```

@ = sio-exupery.fr

Notez la présence nécessaire de l'enregistrement de type **NS** pour la zone **intra** et de l'enregistrement de type **A** pour le serveur de nom de la zone déléguée (**DS1**). Ce dernier se trouve dans la même arborescence. La présence des enregistrements de type **CNAME** - **ftp** et **www** - permet la résolution des url **ftp://ftp.sio-exupery.fr** et **http://www.sio-exupery.fr**.

- Créez le fichier pour la zone de recherche inverse **/var/cache/bind/rev.sio-exupery.fr** :

```

GNU nano 2.7.4          Fichier : /var/cache/bind/rev.sio-exupery.fr
; Fichier pour la résolution inverse
$TTL 86400
@      IN SOA  DS2.sio-exupery.fr. root.sio-exupery.fr. (
                2019020701
                1w
                1d
                4w
                1w )
@      IN NS   DS2.sio-exupery.fr.
10     IN PTR  DS2.sio-exupery.fr.

```

- Attribuez ces 2 fichiers de zone au groupe **bind** afin de les rendre accessibles au démon :

```

root@DS2 ~ #chgrp bind /var/cache/bind/*
root@DS2 ~ #chmod 664 /var/cache/bind/*
root@DS2 ~ #

```

- Mettez à jour le fichier **/etc/hosts** qui doit contenir la référence à la boucle locale et le nom de l'hôte positionné cette fois-ci sur la zone **sio-exupery.fr** :

```

GNU nano 2.7.4          Fichier : /etc/hosts
127.0.0.1    localhost
192.168.4.10 DS2.sio-exupery.fr DS2
# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters

```

- Mettez à jour le fichier **/etc/network/interfaces** :

```

GNU nano 2.7.4          Fichier : /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.4.10
netmask 255.255.255.0
network 192.168.4.0
broadcast 192.168.4.255
gateway 192.168.4.254
dns-search sio-exupery.fr
dns-domain sio-exupery.fr
dns-nameservers 192.168.4.10

```

- Faites prendre en compte les modifications (**ifdown enp0s3** et **ifup enp0s3**) et relancez le service DNS :

```

root@DS2 ~ #systemctl restart bind9
root@DS2 ~ #

```

- Suite à la modification du fichier **/etc/network/interfaces**, vérifiez que le fichier **/etc/resolv.conf** contienne les directives **nameserver 192.168.4.10** et **search sio-exupery.fr** :

```

root@DS2 ~ #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 192.168.4.10
search sio-exupery.fr
root@DS2 ~ #_

```

- Comme indiqué Chapitre 2 page 14, commentez les lignes concernant les serveurs racines dans le fichier **/etc/bind/named.conf.default-zones** :

```

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

```

- Modifiez le fichier **/etc/bind/named.conf.options** afin de mettre en place la redirection :
 - décommentez les lignes ayant trait à l'instruction **forwarders** ;
 - les requêtes DNS ne concernant pas la zone sio-exupery.fr seront redirigées vers le serveur DNS du FAI ou vers votre box à la maison ;
 - ne pas mettre la directive **allow-recursion** ;
 - n'oubliez pas de mettre la directive **dnssec-validation** à **no** (dnssec n'est pas encore mis en place).

```

GNU nano 7.2          /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";
    forward only;
    forwarders { 192.168.1.1; };
    dnssec-validation no;
    listen-on-v6 { any; };
};

```

dnssec-validation no ;

80.10.246.2 (DNS
FAI Orange)
ou serveur DNS ROI
ou votre box
ou 8.8.8.8

- Relancez le service DNS et testez la résolution DNS depuis DS2 :

```
root@DS2 ~ #dig SOA sio-exupery.fr

;<<>> DiG 9.10.3-P4-Debian <<>> SOA sio-exupery.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 558
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sio-exupery.fr.                IN      SOA

;; ANSWER SECTION:
sio-exupery.fr.                86400  IN      SOA      DS2.sio-exupery.fr.  root.sio-exupery.fr. 2019020701
604800 86400 2419200 604800

;; AUTHORITY SECTION:
sio-exupery.fr.                86400  IN      NS       DS2.sio-exupery.fr.

;; ADDITIONAL SECTION:
DS2.sio-exupery.fr.            86400  IN      A        192.168.4.10

;; Query time: 0 msec
;; SERVER: 192.168.4.10#53(192.168.4.10)
;; WHEN: Sat Feb 09 10:27:38 CET 2019
;; MSG SIZE rcvd: 118

root@DS2 ~ #_
```

```
root@DS2 ~ #dig DS2.sio-exupery.fr

;<<>> DiG 9.10.3-P4-Debian <<>> DS2.sio-exupery.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41089
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;DS2.sio-exupery.fr.           IN      A

;; ANSWER SECTION:
DS2.sio-exupery.fr.            86400  IN      A        192.168.4.10

;; AUTHORITY SECTION:
sio-exupery.fr.                86400  IN      NS       DS2.sio-exupery.fr.

;; Query time: 0 msec
;; SERVER: 192.168.4.10#53(192.168.4.10)
;; WHEN: Sat Feb 09 10:29:12 CET 2019
;; MSG SIZE rcvd: 77

root@DS2 ~ #_
```

```

root@DS2 ~ #dig DS1.intra.sio-exupery.fr

;<>> DiG 9.10.3-P4-Debian <>> DS1.intra.sio-exupery.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40272
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;DS1.intra.sio-exupery.fr.      IN      A

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

;; AUTHORITY SECTION:
sio-exupery.fr.          86400 IN      NS      DS2.sio-exupery.fr.

;; ADDITIONAL SECTION:
DS2.sio-exupery.fr.     86400 IN      A      192.168.4.10

;; Query time: 0 msec
;; SERVER: 192.168.4.10#53(192.168.4.10)
;; WHEN: Sat Feb 09 10:30:04 CET 2019
;; MSG SIZE rcvd: 103

root@DS2 ~ #_

```

```

root@DS2 ~ #dig www.ac-nice.fr

;<>> DiG 9.10.3-P4-Debian <>> www.ac-nice.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63950
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.ac-nice.fr.              IN      A

;; ANSWER SECTION:
www.ac-nice.fr.             18      IN      CNAME   mars.ac-nice.fr.
mars.ac-nice.fr.           16189   IN      A      194.167.84.155

;; Query time: 43 msec
;; SERVER: 192.168.4.10#53(192.168.4.10)
;; WHEN: Sat Feb 09 10:53:37 CET 2019
;; MSG SIZE rcvd: 78

root@DS2 ~ #

```

2. Transformation du DNS sur le serveur DS1

- Depuis le serveur **DS1**, **modifiez** les zones dans le fichier **/etc/bind/named.conf.local** :

```
GNU nano 2.7.4      Fichier : /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";

zone "intra.sio-exupery.fr" IN {
    type master;
    file "db.intra.sio-exupery.fr";
    allow-update { key "rndc-key"; };
};

zone "4.168.192.in-addr.arpa" IN {
    type master;
    file "rev.intra.sio-exupery.fr";
    allow-update { key "rndc-key"; };
};
```

- Il s'agit de **créer** le fichier pour la zone directe **/var/cache/bind/db.intra.sio-exupery.fr** adapté à la délégation de la zone. Pour ce faire :
 - **Vérifiez préalablement que DS1 soit serveur SSH** (vérifiez pour cela la présence du paquetage **openssh-server** à l'aide de la commande **dpkg -l | grep -i ssh** ; si ce n'est pas le cas, installez **openssh-server** avec la commande **apt-get install openssh-server**).

```
root@DS1 ~ #dpkg -l | grep -i ssh
ii keychain                2.8.2-0.1                all          key manager for OpenSSH
ii libssh2-1:amd64        1.7.0-1                  amd64       SSH2 client-side library
ii openssh-client         1:7.4p1-10+deb9u4       amd64       secure shell (SSH) client, for secure access to remote machines
ii openssh-server        1:7.4p1-10+deb9u4       amd64       secure shell (SSH) server, for secure access from remote machines
ii openssh-sftp-server   1:7.4p1-10+deb9u4       amd64       secure shell (SSH) sftp server module, for SFTP access from remote machines
ii task-ssh-server       3.39                     all         SSH server
root@DS1 ~ #
```

- Vérifiez également que le fichier de configuration **/etc/ssh/sshd_config** autorise l'**accès SSH à l'utilisateur root** :

```

GNU nano 2.7.4          Fichier : /etc/ssh/sshd_config
#      $OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.
# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
# Ciphers and keying
#RekeyLimit default none
# Logging
#SyslogFacility AUTH
#LogLevel INFO
# Authentication:
#LoginGraceTime 2m
PermitRootLogin yes

```

→ Relancez le service **sshd** si le fichier de configuration **sshd_config** a été modifié :

```

root@DS1 ~ #systemctl restart sshd
root@DS1 ~ #

```

→ Enfin, copiez le fichier **db.sio-exupery.fr** depuis **DS2** vers **DS1** avec la commande **scp** :

```

root@DS2 ~ #scp /var/cache/bind/db.sio-exupery.fr root@192.168.4.254:/var/cache/bind/
The authenticity of host '192.168.4.254 (192.168.4.254)' can't be established.
ECDSA key fingerprint is SHA256:fI6Qb78DrezJFYjTFMJWtvfOEDushP/DEU14uju1SrQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.4.254' (ECDSA) to the list of known hosts.
root@192.168.4.254's password:
db.sio-exupery.fr                               100% 345   391.8KB/s   00:00
root@DS2 ~ #_

```

- Depuis **DS1**, modifiez le fichier copié **db.sio-exupery.fr** et renommez-le au moment de l'enregistrer en **db.intra.sio-exupery.fr** :

```

GNU nano 7.2          /var/cache/bind/db.intra.sio-exupery.fr
; Fichier pour la résolution directe
$TTL 86400
@      IN SOA  DS1.intra.sio-exupery.fr. root.intra.sio-exupery.fr. (
        2024032101
        1w
        1d
        4w
        1w )
@      IN NS  DS1.intra.sio-exupery.fr.
DS1.intra.sio-exupery.fr.  IN A  192.168.4.254

```

Intra.sio-exupery.fr
Cf. page 6

- Créez de manière similaire le fichier **/var/cache/bind/rev.intra.sio-exupery.fr** pour la zone inverse : copiez dans un premier temps depuis **DS2** le fichier **rev.sio-exupery.fr** vers **DS1** avec la commande **scp** :

```

root@DS2 ~ #scp /var/cache/bind/rev.sio-exupery.fr root@192.168.4.254:/var/cache/bind/
root@192.168.4.254's password:
rev.sio-exupery.fr                               100% 198   455.6KB/s   00:00
root@DS2 ~ #

```

- Depuis DS1, modifiez le fichier copié et renommez-le au moment de l'enregistrer en **rev.intra.sio-exupery.fr** :

```

GNU nano 7.2 /var/cache/bind/rev.intra.sio-exupery.fr
; Fichier pour la résolution inverse
$TTL 86400
@      IN SOA  DS1.intra.sio-exupery.fr. root.intra.sio-exupery.fr. (
        2024032101
        1w
        1d
        4w
        1w )
@      IN NS  DS1.intra.sio-exupery.fr.
254   IN PTR DS1.intra.sio-exupery.fr.

```

- 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 ~ #

```

- Modifiez le fichier **/etc/hosts** en spécifiant **DS1.intra.sio-exupery.fr** :

```

GNU nano 2.7.4 Fichier : /etc/hosts
127.0.0.1 localhost.localdomain localhost
192.168.4.254 DS1.intra.sio-exupery.fr DS1

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

```

- Modifiez le fichier **/etc/network/interfaces** puis faites prendre en compte les modifications concernant l'interface **enp0s8** avec les commandes **ifdown** et **ifup** :

```

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 intra.sio-exupery.fr
dns-domain intra.sio-exupery.fr
dns-nameservers 192.168.4.254

```

- Vérifiez que le fichier **/etc/resolv.conf** contienne les directives **nameserver 192.168.4.254** et **search intra.sio-exupery.fr** :

```

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 intra.sio-exupery.fr
root@DS1 ~ #_

```

- Modifiez, dans le fichier **/etc/bind/named.conf.options**, l'instruction **forwarders** qui redirige dorénavant les requêtes DNS ne concernant pas la zone **intra.sio-exupery.fr** vers le serveur DNS DS2 ayant pour adresse IP 192.168.4.10 :

```

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

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

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

    forward only;
    forwarders { 192.168.4.10; };
    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; };
};

```

- **SISR** : remplacez **sio-exupery.local** par **intra.sio-exupery.fr** dans le **fichier de configuration du DHCP /etc/dhcp/dhcpd.conf** :

```

GNU nano 2.7.4 Fichier : /etc/dhcp/dhcpd.conf Modifié
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# option definitions common to all supported networks...
option domain-name "intra.sio-exupery.fr";
option domain-name-servers 192.168.4.254;

default-lease-time 86400;
max-lease-time 604800;

subnet 192.168.4.0 netmask 255.255.255.0 {
# étendue de la plage DHCP
    range 192.168.4.11 192.168.4.100;
# passerelle
    option routers 192.168.4.254;
# masque de sous-réseau
    option subnet-mask 255.255.255.0;
#
    ddns-domainname "intra.sio-exupery.fr";
    ddns-rev-domainname in-addr.arpa;
}

include "/etc/dhcp/rndc.key";
# Zones DNS à mettre à jour
zone intra.sio-exupery.fr. {
    primary 127.0.0.1;
    key rndc-key;
}
zone 4.168.192.in-addr.arpa. {
    primary 127.0.0.1;
    key rndc-key;
}

```

- Redémarrez DS1 et DS2 afin de redémarrez les services concernés par les modifications.
- Testez la résolution DNS pour la zone **intra.sio-exupery.fr** en demandant le SOA :

```

root@DS1 ~ #dig SOA intra.sio-exupery.fr

;<>> DiG 9.10.3-P4-Debian <>> SOA intra.sio-exupery.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54122
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
intra.sio-exupery.fr.      IN      SOA

;; ANSWER SECTION:
intra.sio-exupery.fr.    86400  IN      SOA      DS1.intra.sio-exupery.fr.  root.intra.sio-exupery.fr.
2019020702 604800 86400 2419200 604800

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

;; ADDITIONAL SECTION:
DS1.intra.sio-exupery.fr. 86400  IN      A       192.168.4.254

;; Query time: 0 msec
;; SERVER: 192.168.4.254#53(192.168.4.254)
;; WHEN: Sun Feb 10 11:35:14 CET 2019
;; MSG SIZE rcvd: 124

root@DS1 ~ #_

```

- **SISR** : depuis le serveur DHCP DS1, lancez la commande **journalctl -f** puis démarrez UD1. Vérifiez l'existence de l'enregistrement DNS du client UD1 au travers des lignes comportant les mentions **added new forward map** et **added reverse map** :

```

mars 22 07:45:02 DS1 dhcpd[940]: DHCPDISCOVER from 08:00:27:a5:00:f9 via enp0s8
mars 22 07:45:03 DS1 dhcpd[940]: DHCPOFFER on 192.168.4.11 to 08:00:27:a5:00:f9 (UD1) via enp0s8
mars 22 07:45:03 DS1 dhcpd[940]: DHCPREQUEST for 192.168.4.11 (192.168.4.254) from 08:00:27:a5:00:f9
(UD1) via enp0s8
mars 22 07:45:03 DS1 dhcpd[940]: DHCPACK on 192.168.4.11 to 08:00:27:a5:00:f9 (UD1) via enp0s8
mars 22 07:45:03 DS1 named[741]: client @0x7ff403d97b68 127.0.0.1#64579/key rndc-key: signer "rndc-k
ey" approved
mars 22 07:45:03 DS1 named[741]: client @0x7ff403d97b68 127.0.0.1#64579/key rndc-key: updating zone
'intra.sio-exupery.fr/IN': adding an RR at 'UD1.intra.sio-exupery.fr' A 192.168.4.11
mars 22 07:45:03 DS1 named [741]: client @0x7ff403d97b68 127.0.0.1#64579/key rndc-key: updating zone
'intra.sio-exupery.fr/IN': adding an RR at 'UD1.intra.sio-exupery.fr' TXT "31d3b949b6e8f2969ffdbf05d
98bbfc85e"
mars 22 07:45:04 DS1 dhcpd [940]: Added new forward map from UD1.intra.sio-exupery.fr to 192.168.4.11
mars 22 07:45:04 DS1 named[741]: client @0x7ff403d97b68 127.0.0.1#64579/key rndc-key: signer "rndc-k
ey" approved
mars 22 07:45:04 DS1 named[741]: client @0x7ff403d97b68 127.0.0.1#64579/key rndc-key: updating zone
'4.168.192.in-addr.arpa/IN': deleting rrsset at '11.4.168.192.in-addr.arpa' PTR
mars 22 07:45:04 DS1 named[741]: client @0x7ff403d97b68 127.0.0.1#64579/key rndc-key: updating zone
'4.168.192.in-addr.arpa/IN': adding an RR at '11.4.168.192.in-addr.arpa' PTR UD1.intra.sio-exupery.f
r.
mars 22 07:45:04 DS1 dhcpd[940]: Added reverse map from 11.4.168.192.in-addr.arpa to UD1.intra.sio-e
xupery.fr

```

- **SLAM** : ajoutez manuellement l'enregistrement **UD1** de **type A** (192.168.4.11) à la fin du fichier **db.intra.sio-exupery.fr** ainsi que celui de **type PTR** (11) dans le fichier **rev.intra.sio-exupery.fr** (cf. Chapitre 2 pages 6 et 7).
- Pinguez **UD1** depuis DS1 pour constater la résolution DNS :

```

root@DS1: ~#ping -c 2 UD1
PING UD1.intra.sio-exupery.fr (192.168.4.11) 56(84) bytes of data:
64 bytes from UD1.intra.sio-exupery.fr (192.168.4.11): icmp_seq=1 ttl=64 time=0.603 ms
64 bytes from UD1.intra.sio-exupery.fr (192.168.4.11): icmp_seq=2 ttl=64 time=1.10 ms

--- UD1.intra.sio-exupery.fr ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1032ms
rtt min/avg/max/mdev = 0.603/0.853/1.104/0.250 ms
root@DS1: ~#

```

- **SISR** : Constatez les inscriptions DNS par la création des deux nouveaux fichiers de zone avec l'extension **.jnl** dans le répertoire **/var/cache/bind** :

```
root@DS1 ~ #ls -l /var/cache/bind/
total 48
-rw-rw-r-- 1 root bind 269 févr. 9 13:03 db.intra.sio-exupery.fr
-rw-r--r-- 1 bind bind 861 févr. 9 14:15 db.intra.sio-exupery.fr.jnl
-rw-rw-r-- 1 root bind 345 févr. 9 12:33 db.sio-exupery.fr
-rw-rw-r-- 1 bind bind 365 févr. 5 17:56 db.sio-exupery.local
-rw-rw-r-- 1 bind bind 4822 févr. 5 17:44 db.sio-exupery.local.jnl
-rw-rw-r-- 1 bind bind 221 janv. 13 22:27 managed-keys.bind
-rw-rw-r-- 1 root bind 223 févr. 9 13:09 rev.intra.sio-exupery.fr
-rw-r--r-- 1 bind bind 813 févr. 9 14:15 rev.intra.sio-exupery.fr.jnl
-rw-rw-r-- 1 root bind 198 févr. 9 12:35 rev.sio-exupery.fr
-rw-rw-r-- 1 bind bind 397 févr. 5 17:55 rev.sio-exupery.local
-rw-rw-r-- 1 bind bind 3372 févr. 5 17:44 rev.sio-exupery.local.jnl
root@DS1 ~ #_
```

- **SISR** : constatez, à l'aide de la commande **cat**, l'inscription du client DNS **UD1** dans les fichiers de zone **/var/cache/bind/db.intra.sio-exupery.fr** et **/var/cache/bind/rev.intra.sio-exupery.fr** :

```
root@DS1 ~ #cat /var/cache/bind/db.intra.sio-exupery.fr
$ORIGIN .
$TTL 86400      ; 1 day
intra.sio-exupery.fr  IN SOA  DS1.intra.sio-exupery.fr. root.intra.sio-exupery.fr. (
        2019020702 ; serial
        604800    ; refresh (1 week)
        86400    ; retry (1 day)
        2419200  ; expire (4 weeks)
        604800  ; minimum (1 week)
)
                NS   DS1.intra.sio-exupery.fr.
$ORIGIN intra.sio-exupery.fr.
DS1             A    192.168.4.254
$TTL 3600      ; 1 hour
UD2             A    192.168.4.13
                TXT  "3128fa7ad4e10dda22ab1986456b7e3e74"
```

UD1

```
root@DS1 ~ #cat /var/cache/bind/rev.intra.sio-exupery.fr
$ORIGIN .
$TTL 86400      ; 1 day
4.168.192.in-addr.arpa IN SOA  DS1.intra.sio-exupery.fr. root.intra.sio-exupery.fr. (
        2019020702 ; serial
        604800    ; refresh (1 week)
        86400    ; retry (1 day)
        2419200  ; expire (4 weeks)
        604800  ; minimum (1 week)
)
                NS   DS1.intra.sio-exupery.fr.
$ORIGIN 4.168.192.in-addr.arpa.
$TTL 3600      ; 1 hour
13             PTR  UD2.intra.sio-exupery.fr.
$TTL 86400    ; 1 day
254           PTR  DS1.intra.sio-exupery.fr.
root@DS1 ~ #
```

- Testez la résolution DNS **hors zone intra.sio-exupery.fr** depuis DS1 :

```

root@DS1 ~ #dig SOA sio-exupery.fr

; <<>> DiG 9.10.3-P4-Debian <<>> SOA sio-exupery.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY status: NOERROR, id: 32967
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sio-exupery.fr.                IN      SOA

;; ANSWER SECTION:
sio-exupery.fr.                86243  IN      SOA      DS2.sio-exupery.fr. root.sio-exupery.fr. 2019020701
604800 86400 2419200 604800

;; AUTHORITY SECTION:
sio-exupery.fr.                86243  IN      NS       DS2.sio-exupery.fr.

;; ADDITIONAL SECTION:
DS2.sio-exupery.fr.            86243  IN      A        192.168.4.10

;; Query time: 0 msec
;; SERVER: 192.168.4.254#53(192.168.4.254)
;; WHEN: Sun Feb 10 11:37:37 CET 2019
;; MSG SIZE rcvd: 118

root@DS1 ~ #_

```

```

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

; <<>> DiG 9.10.3-P4-Debian <<>> www.ac-nice.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY status: NOERROR, id: 42376
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.ac-nice.fr.                IN      A

;; ANSWER SECTION:
www.ac-nice.fr.                459    IN      CNAME    mars.ac-nice.fr.
mars.ac-nice.fr.                457    IN      A        194.167.84.155

;; Query time: 47 msec
;; SERVER: 192.168.4.254#53(192.168.4.254)
;; WHEN: Sun Feb 10 11:49:21 CET 2019
;; MSG SIZE rcvd: 78

root@DS1 ~ #

```

3. Vérifications depuis le client Ubuntu UD1

3.1. Demande de résolution interne

Le principe de résolution est le suivant :

- Une requête sur **intra.sio-exupery.fr** sera traitée par DS1, tout le reste étant dévié sur DS2 ;
- Une requête sur **sio-exupery.fr** sera traitée par DS2, tout le reste étant dévié sur le DNS externe (serveur DNS du FAI ou de Google ou serveur DNS ROI ou box de la maison).

▪ Vérifiez à partir du client Ubuntu UD1 que :

- La commande **dig SOA intra.sio-exupery.fr** retourne le serveur **DS1.intra.sio-exupery.fr** :

```
sio@UD2: ~
Fichier Édition Affichage Rechercher Terminal Aide
sio@UD2:~$ dig SOA intra.sio-exupery.fr

;<<> DiG 9.11.3-1ubuntu1.2-Ubuntu <<> SOA intra.sio-exupery.fr
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 64697
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;intra.sio-exupery.fr.          IN      SOA

;; ANSWER SECTION:
intra.sio-exupery.fr.  86400  IN     SOA     DS1.intra.sio-exupery.fr. root.intra.
sio-exupery.fr. 2019020702 604800 86400 2419200 604800

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Feb 10 11:07:33 CET 2019
;; MSG SIZE rcvd: 94
```

- La commande **dig SOA sio-exupery.fr** retourne le serveur **DS2.sio-exupery.fr** :

```
sio@UD2: ~
Fichier Édition Affichage Rechercher Terminal Aide
sio@UD2:~$ dig SOA sio-exupery.fr

;<<> DiG 9.11.3-1ubuntu1.2-Ubuntu <<> SOA sio-exupery.fr
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 36375
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;sio-exupery.fr.              IN      SOA

;; ANSWER SECTION:
sio-exupery.fr.  85328  IN     SOA     DS2.sio-exupery.fr. root.sio-exupery.fr. 201902
0701 604800 86400 2419200 604800

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Feb 10 11:52:52 CET 2019
;; MSG SIZE rcvd: 88
```

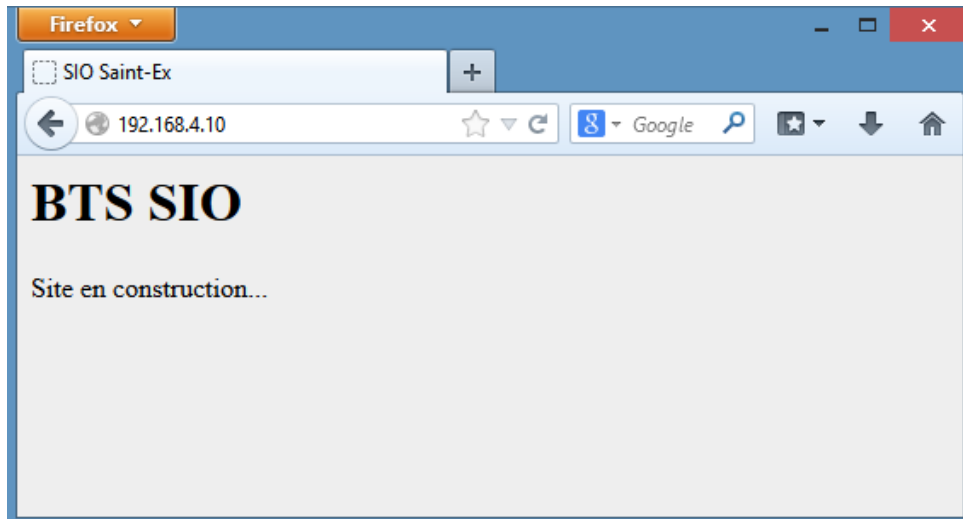
- La commande **dig www.ac-nice.fr** renvoie l'adresse du serveur web de l'Académie de Nice :


```
Microsoft Windows [version 6.3.9600]
(c) 2013 Microsoft Corporation. Tous droits réservés.

C:\WINDOWS\system32>route add 192.168.4.0 mask 255.255.255.0 192.168.1.101
OK!

C:\WINDOWS\system32>
```

- Affichez de nouveau la table de routage de la machine hôte et constatez la présence de la route vers votre réseau 192.168.4.0/24 (capture d'écran à effectuer)
- Dans le navigateur de votre système hôte, inscrivez l'adresse IP 192.168.4.10 comme URL : la page de votre serveur Web sur DS2 doit apparaître :



- Afin d'utiliser l'adresse **http://www.sio-exupery.fr** à la place de l'adresse IP, mettez comme serveur DNS principal, toujours sur le **système hôte**, 192.168.4.10 dans les propriétés de votre connexion au réseau local.

Attention : les modifications de la table de routage s'effacent après le redémarrage du système. Pour les rendre permanentes, il faudrait utiliser un fichier batch (.bat) exécuté à l'initialisation du système.

