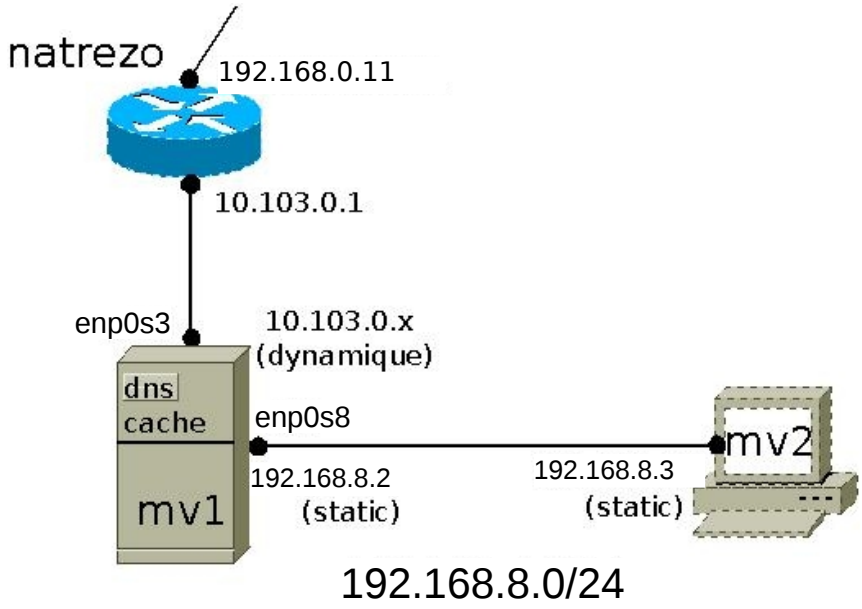
TP – DNS

Exercice 1: Serveur de cache

- Réalisez la maquette suivante:



VirtualBox:

. enp0s3 de mv1 en mode bridge
. enp0s8 de mv1 et enp0s3 de mv2 en mode réseau interne (intnet1)

Maquette:

. Configuration des interfaces de mv1 et mv2 (voir avant)

. Passerelle par défaut sur mv2 --> 192.168.8.2
/etc/sysconfig/network-scripts/route-enp0s3
default via 192.168.0.2 dev enp0s3

. Passerelle par défaut sur mv1 --> 10.103.0.1 (par dhcp)

Particularités:

Sur mv1:
. Activer l'Ip forwarding (voir avant)
En permanent via mise à jour de /etc/sysctl.conf

. Activer le Nating (voir avant)
En permanent via:
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
service iptables save
systemctl enable iptables

- Installez les packages de Bind sur MV1.

```
# rpm -qa bind
# dnf search bind
# dnf install bind bind-libs bind-utils -y

 (Ne pas installer bind-chroot !!!)

Reconstitution du named.conf à partir de /etc/named.conf et de
                                          /etc/named.rfc1912.zones

# mkdir /etc/bind-backup
# mv /etc/named* /etc/bind-backup
```

- Configurez le fichier /etc/named.conf sur MV1.

```
# cat /etc/bind-backup/named.conf /etc/bind-backup/named.rfc1912.zones
                                                              > /etc/named.conf

--- Mise à jour de /etc/named --- (Voir syllabus)

# cat /var/named/named.ca
...
# cat /var/named/named.loopback
...                                   (+ suppression RR concernant IPV6)

# cat /var/named/named.localhost
...                                   (+ suppression RR concernant IPV6)
```

- Configurez les resolvers des 2 machines.

```
MV1# echo nameserver 127.0.0.1 > /etc/resolv.conf
MV2# echo nameserver 192.168.8.2 > /etc/resolv.conf
```

- Vérifiez le fichier /etc/nsswitch.conf des 2 machines.

```
Sur MV1 et MV2:
--- Mise à jour de /etc/nsswitch.conf ---
# cat /etc/nsswitch.conf
...
hosts: files dns
```

- Vérifiez le fichier /etc/hosts des 2 machines.

```
Sur MV1 et MV2:
--- Mise à jour de /etc/hosts (+ suppression ligne concernant IPV6) ---
# cat /etc/hosts
127.0.0.1 localhost ...
```

- Lancez votre dns + vérification des logs dans /var/log/messages + vérification via named-checkconf **et** named-checkzone

```
MV1# named-checkconf /etc/named.conf
MV1# named-checkzone localhost /var/named/named.localhost
zone localhost/IN: loaded serial 0
OK

MV1# systemctl start named

MV1# cat /var/log/messages | more
Starting BIND ...                              → démarrage de bind
...
loading configuration from '/etc/named.conf' → fichier de config. utilisé
...
listening on Ipv4 interface lo, 127.0.0.1#53
listening on Ipv4 interface enp0s8, 192.168.8.2#53 → interfaces à l'écoute+port
...
zone 1.0.0.127.in-addr.arpa/IN: loaded serial 0
zone 1.0.0.127.in-addr.arpa/IN: loaded serial 0 → zones chargées + n° de serie
...

MV1# ps ax | grep named
...                  → le daemon named tourne

MV1# ss -tunl
...                  → named tourne en tcp et udp et écoute sur le port 53
```

- Vérifiez le bon fonctionnement de votre dns à l'aide de nslookup et dig.

```
MV1# nslookup localhost
Server:  127.0.0.1          → utilisation du dns local pour résoudre la requête
Address: 127.0.0.1#53

Name: localhost
Address: 127.0.0.1          → sait résoudre localhost


MV1# nslookup 127.0.0.1
Server:  127.0.0.1          → utilisation du dns local pour résoudre la requête
Address: 127.0.0.1#53

1.0.0.127.in-addr.arpa  name = localhost. --> sait résoudre localhost en reverse


MV1# nslookup www.helha.be → sait lancer une requête externe récursive
Server:  127.0.0.1          → utilisation du dns local pour résoudre la requête
Address: 127.0.0.1#53

Non-authoritative answer  → la réponse est extraite du cache
Name: www.helha.be
Address: 193.190.66.12    →     sait résoudre www.helha.be par un appel récursif
                                sur un serveur racine (cette résolution se
                                trouve maintenant en cache)

MV1# rndc flush      → on vide le cache

Même chose avec dig:
MV1# dig localhost
...
MV1# dig -x 127.0.0.1
...
MV1# dig www.helha.be
...
```

- Tentez de résoudre une requête dns à partir de MV2.

```
MV2# ping www.helha.be
...

MV2# lynx www.kernel.org
...
```

- Lancez tshark sur MV2 et espionnez une requête dns.

tshark

```
# tshark -i enp0s3 udp port 53
```

Sur MV2

```
MV2# lynx www.helha.be
...
```

Dans tshark, on constate bien que les paquets sont échangés entre 192.168.8.2 et 192.168.8.3 → OK

- Lancez tshark sur MV1 et espionnez une requête dns.

a) qui ne se trouve pas encore en cache

Sur MV1

```
MV1# rndc flush   → on vide le cache
...
```

tshark

```
# tshark -i enp0s3 udp port 53
```

Sur MV1

```
MV1# lynx www.helha.be
...
  + sortir de lynx
```

Dans tshark, on constate bien que la requête est récursive.
Le premier serveur interrogé est un serveur racine.
Le deuxième est un des TLD.
...

b) qui se trouve déjà en cache

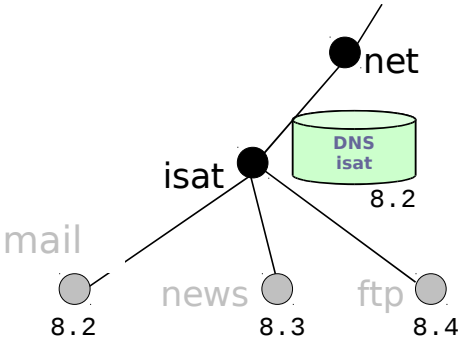
Sur MV1

```
MV1# lynx www.helha.be
...
  + sortir de lynx
```

On constate ici que tshark reste muet sur enp0s3.
Cela signifie que c'est la réponse a été résolue par le cache.

Exercice 2: Serveur autoritaire de cache

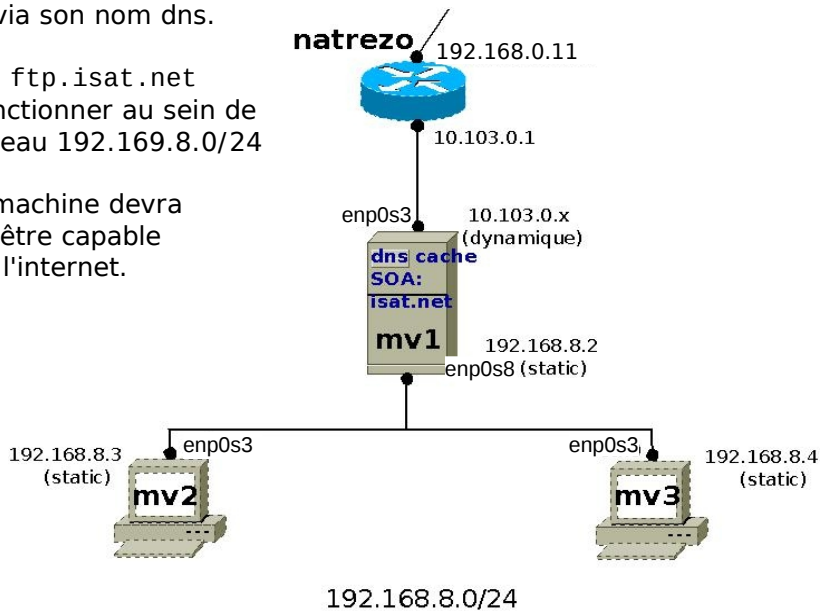
- Construire le serveur dns gérant le domaine isat.net. exposé ci-avant.
Rappel de l'architecture:



Chaque machine devra être capable de répondre à une requête via son nom dns.

ex. `ping ftp.isat.net` devra fonctionner au sein de votre réseau 192.169.8.0/24

Chaque machine devra toujours être capable d'utiliser l'internet.



Les services
mail.isat.net sur 192.168.8.2
news.isat.net sur 192.168.8.3
ftp.isat.net sur 192.168.8.4

Alias sur les noms canoniques
r2d2.isat.net sur 192.168.8.2
yoda.isat.net sur 192.168.8.3
lea.isat.net sur 192.168.8.4

Le DNS
De la zone "isat.net" sur 192.168.8.2

VirtualBox:

. enp0s3 de mv1 en mode bridge
. enp0s8 de mv1 en mode réseau interne (intnet1)
. enp0s3 de mv2 en mode réseau interne (intnet1)
. enp0s3 de mv3 en mode réseau interne (intnet1)

Maquette:

. Configuration des interfaces de mv1, mv2 et mv3 (voir avant)
. Passerelle par défaut sur mv2 et mv3 → 192.168.8.2
. Passerelle par défaut sur mv1 → 10.103.0.1

Particularités:

Sur mv1:

. Activer l'Ip forwarding (voir avant)
En permanent via mise à jour de /etc/sysctl.conf

. Activer le Nating (voir avant)
En permanent via:

```
# iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
# service iptables save
# systemctl enable iptables
```

Après avoir configuré les machines de votre maquette testez:
- *Si elles savent se toucher (ping) les unes et les autres*
- *Si elles savent toucher (ping) une machine externe par son Ip*

- Configurez votre dns:

Installez les packages de Bind sur MV1.

```
MV1# rpm -qa bind
MV1# dnf search bind
MV1# dnf install bind bind-libs bind-utils -y

 (Ne pas installer bind-chroot !!!)

Reconstitution du named.conf à partir de /etc/named et de
                                        /etc/named.rfc1912.zones

MV1# mkdir /etc/bind-backup
MV1# mv /etc/named* /etc/bind-backup
```

Configurez le fichier /etc/named.conf sur MV1.

```
MV1# cat /etc/bind-backup/named.conf /etc/bind-backup/named.rfc1912.zones
                                                              > /etc/named.conf

--- Mise à jour de /etc/named ---

MV1# cat /etc/named.conf
options {
   listen-on port 53 {127.0.0.1 ; 192.168.8.2 ;} ;
   directory "/var/named";
};

zone "." IN {
   type hint;
   file "named.ca";
};

zone "1.0.0.127.in-addr.arpa" IN {
   type master;
   file "named.loopback";
};

zone "localhost" IN {
   type master;
   file "named.localhost";
};

zone "isat.net" IN {
   type master;
   file "db.isat.net";
};

zone "8.168.192.in-addr.arpa" IN {
   type master;
   file "db.isat.net-rev";
};

MV1# cat /var/named/named.ca
...
MV1# cat /var/named/named.loopback
...                                    (+ suppression RR concernant IPV6)

MV1# cat /var/named/named.localhost
...                                    (+ suppression RR concernant IPV6)
```

Configurez les fichiers de la zone du domaine "isat.net" sur MV1

```
MV1# cat /var/named/db.isat.net
$ORIGIN isat.net.
$TTL          2D
isat.net.     IN    SOA     ns.isat.net.   root.isat.net.  (
                                    2017110700 ; Serial
                                    28800      ; Refresh
                                    14400      ; Retry
                                    3600000    ; Expire
                                    7200 )    ; Minimum
              IN    NS    ns.isat.net.

ns            IN    A     192.168.8.2
mail          IN    A     192.168.8.2
news          IN    A     192.168.8.3
ftp           IN    A     192.168.8.4

r2d2          IN    CNAME mail
lea           IN    CNAME ftp
yoda          IN    CNAME news

isat.net.     IN    MX    10    mail

MV1# cat /var/named/ db.isat.net-rev
$ORIGIN       8.168.192.in-addr.arpa.
$TTL          2D
8.168.192.in-addr.arpa.  IN   SOA  ns.isat.net. root.isat.net.  (
                                    2017110700 ; Serial
                                    28800      ; Refresh
                                    14400      ; Retry
                                    3600000    ; Expire
                                    7200  )    ; Minimum
              IN   NS     ns.isat.net.

2             IN   PTR    mail.isat.net.
3             IN   PTR    news.isat.net.
4             IN   PTR    ftp.isat.net.
```

!! Attention aux permissions !!

```
MV1# chgrp named db.isat.net*
```

Configurez les resolvers des 3 machines.

```
MV1# echo nameserver 127.0.0.1 > /etc/resolv.conf
MV2# echo nameserver 192.168.8.2 > /etc/resolv.conf
MV3# echo nameserver 192.168.8.2 > /etc/resolv.conf
```

Vérifiez le fichier /etc/nsswitch.conf des 3 machines.

```
Sur MV1, MV2 et MV3:
--- Mise à jour de /etc/nsswitch.conf ---
# cat /etc/nsswitch.conf
...
hosts: files dns
```

Vérifiez le fichier /etc/hosts des 3 machines.

```
Sur MV1, MV2 et MV3:
--- Mise à jour de /etc/hosts (+ suppression ligne concernant IPV6) ---
# cat /etc/hosts
127.0.0.1 localhost ...
```

Lancez votre dns + vérification des logs dans /var/log/messages + vérification du fichier de configuration et des nouveaux fichiers de zone.

```
MV1# systemctl start named

MV1# named-checkconf /etc/named.conf
MV1# named-checkzone isat.net /var/named/db.isat.net
MV1# named-checkzone 8.168.192.in-addr.arpa /var/named/db.isat.net-rev

MV1# cat /var/log/messages | more
Starting BIND ...                              → démarrage de bind
...
loading configuration from '/etc/named.conf' → fichier de config. utilisé
...
listening on Ipv4 interface lo, 127.0.0.1#53
listening on Ipv4 interface enp0s8, 192.168.8.2#53 → interfaces à l'écoute+port
...
zone 1.0.0.127.in-addr.arpa/IN: loaded serial 0
zone 8.168.192.in-addr.arpa/IN: loaded serial 2017110700
zone localhost/IN: loaded serial 0
zone isat.net/IN: loaded serial 2017110700
...

MV1# ps ax | grep named
...                  --> le daemon named tourne

MV1# ss -tunl
...                  --> named tourne en tcp et udp et écoute sur le port 53
```

- Fonctionnement (ping + outils de debugage):
. chaque mv doit pouvoir se toucher par son nom ou son alias.

```
MV1# ping yoda.isat.net
MV1# ping news.isat.net
MV1# ping lea.isat.net
MV1# ping ftp.isat.net

MV2# ping r2d2.isat.net
MV2# ping mail.isat.net
MV2# ping lea.isat.net
MV2# ping ftp.isat.net
…

MV1# nslookup -sil
> news.isat.net
Server:       127.0.0.1
Address:      127.0.0.1#53

Name:         news.isat.net
Address:      192.168.8.3               (Faire idem pour ftp et mail …)

> 192.168.8.2
Server:       127.0.0.1
Address:      127.0.0.1#53 (Faire idem pour 192.168.8.3 et 4 …)

2.8.168.192.in-addr.arpa     name = mail.isat.net.

> r2d2.isat.net
Server:       127.0.0.1
Address:      127.0.0.1#53   (Faire idem pour ns, ftp et news …)

r2d2.isat.net canonical name = mail.isat.net.
Name:         mail.isat.net
Address:      192.168.8.2
```

. chaque mv a toujours l'accès à l'internet.

```
MV1# rndc flush   --> on vide le cache

MV1# lynx www.kernel.org
MV2# lynx www.tf1.fr
MV3# lynx www.rtbf.be
```

- Quelques essais

a) Enlevez `192.168.8.2;` de la directive `listen-on` et relancez `named`. Que constatez-vous ?

MV2 et MV3 n'ont plus accès à l'Internet car le réseau sur lequel se trouvent ces machines n'est plus accepté par le dns.
Par contre MV1 a toujours accès car la résolution via le dns de cache.

b) Rajoutez à nouveau ce réseau et ajoutez la directive `recursion no` et relancez `named`. Que constatez-vous ?

MV1,MV2 et MV3 n'ont plus accès à l'Internet car le dns n'accepte plus de résoudre aucune requête récursive. Il n'est plus dns relais (ou ouvert).

c) Remplacez la directive recursion no par:

```
recursion yes ;
allow-recursion {127.0.0.1 ; 192.168.8.0/24;} ;
allow-query-cache {127.0.0.1 ; 192.168.8.0/24;} ;
```

et relancez `named`. Que constatez-vous ?

MV1,MV2 et MV3 ont à nouveau accès à l'Internet car le dns accepte des requêtes récursives venant de lui-même et de l'intranet.

Explications:

*La configuration de Bind par défaut comporte une "faille" de sécurité, en effet la configuration autorise des tierces personnes (celles de l'internet) à utiliser le serveur DNS (sans demander la permission ^^). Cela fait de notre cher Bind un **serveur** DNS **relais** !!*

Pour corriger cette faille:

```
allow-recursion { 127.0.0.1; 192.168.8.0/24; };
```

*Ce qui a pour incidence que l'utilisation de Bind **ne sera autorisée que sur le serveur même et à partir de l'intranet**.*

Avec allow-recursion nous avons déjà comblé une partie de la faille, il reste encore à interdire l'utilisation du cache de notre serveur via:

```
allow-query-cache { 127.0.0.1; 192.168.8.0/24; };
```

d) Rajoutez la directive `version "DNS ISAT"` **et relancez** `named`**. Quelle pourrait-être son utilité ?**

L'option “version” permet de dissimuler la version de Bind, en effet une personne malveillante peut vouloir récupérer la version de votre Bind afin de mener une petite attaque contre ce dernier s'il n'est pas à jour.

Il utilisera l'une des commandes suivantes :

$ dig @r2d2.isat.net version.bind txt chaos
La réponse à cette commande sera :
;; ANSWER SECTION:
VERSION.BIND. 0 CH TXT "9.9.4-RedHat-9.9.4…"

ou

$ nslookup -type=txt -class=chaos version.bind r2d2.isat.net
La réponse à cette commande sera :
VERSION.BIND text = "9.9.4-RedHat-9.9.4…"

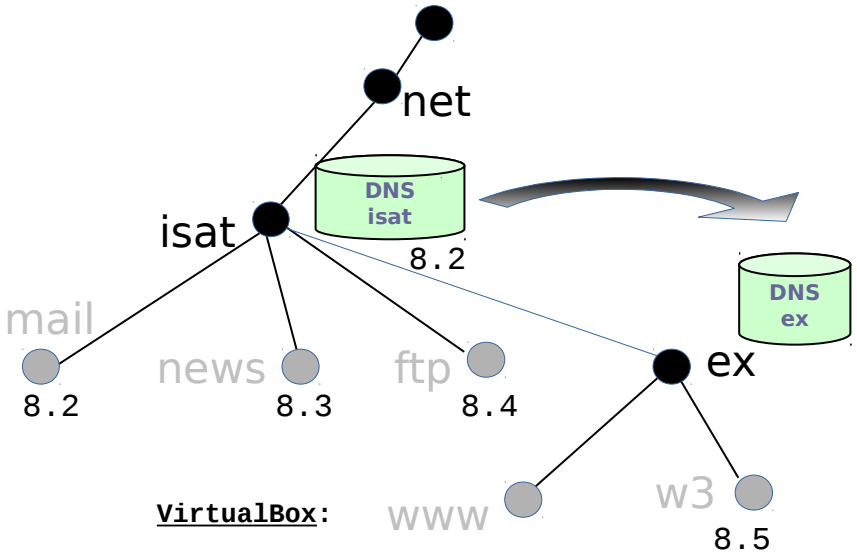
Cette option est donc à ajouter dans le fichier “/etc/named.conf”.

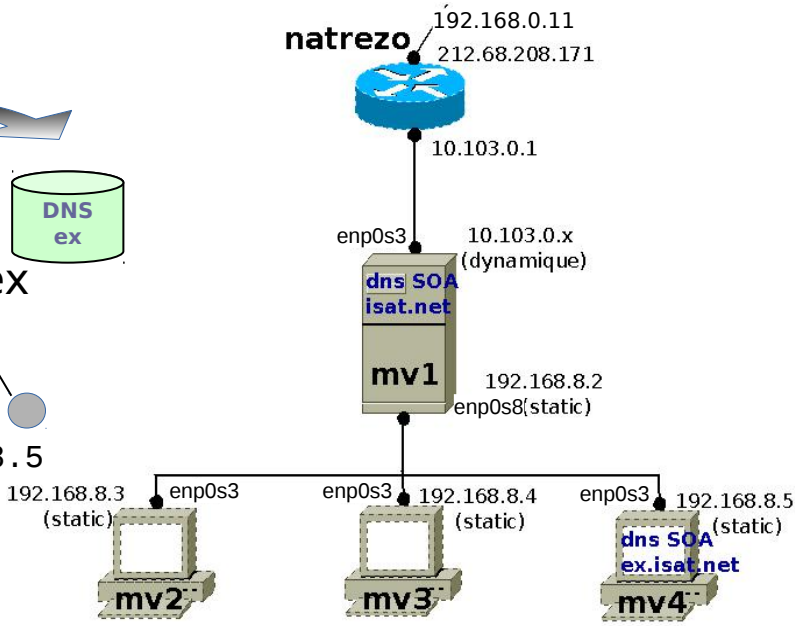
version "DNS ISAT";

Désormais lorsqu'une personne voudra afficher la version de votre Bind, il verra “DNS ISAT” et non plus la version de bind embarquée sur le système…

Exercice 3: Délégation et sous domaine

- **Construire les serveurs dns gérant les domaines isat.net et ex.isat.net**





VirtualBox:

```
. enp0s3 de mv1 en mode bridge
. enp0s8 de mv1 en mode réseau interne (intnet1)
. enp0s3 de mv2 en mode réseau interne (intnet1)
. enp0s3 de mv3 en mode réseau interne (intnet1)
. enp0s3 de mv4 en mode réseau interne (intnet1)
```

Maquette:

```
. Configuration des interfaces de mv1, mv2, mv3 et mv4 (voir avant)
. Passerelle par défaut sur mv2, mv3 et mv4 →  192.168.8.2
. Passerelle par défaut sur mv1 →  10.103.0.1
```

Particularités:

```
SSur mv1:
              . Activer l'Ip forwarding (voir avant)
                   En permanent via mise à jour de /etc/sysctl.conf

              . Activer le Nating (voir avant)
                   En permanent via:
                       # iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
                       # service iptables save
                       # systemctl enable iptables
```

Après avoir configuré les machines de votre maquette testez:

- *Si elles savent se toucher (ping) les unes et les autres*
- *Si elles savent toucher (ping) une machine externe par son Ip*
-

- Configurez vos dns:

Installez les packages de Bind sur MV1 et MV4 (voir avant)

Voir avant

Configurez le fichier /etc/named.conf sur MV1.

```
MV1# cat /etc/named.conf
options {
   listen-on port 53 {127.0.0.1 ; 192.168.8.2 ;} ;
   directory "/var/named";
};

zone "." IN {
   type hint;
   file "named.ca";
};

zone "1.0.0.127.in-addr.arpa" IN {
   type master;
   file "named.loopback";
};

zone "localhost" IN {
   type master;
   file "named.localhost";
};

zone "isat.net" IN {
   type master;
   file "db.isat.net";
};

zone "8.168.192.in-addr.arpa" IN {
   type master;
   file "db.isat.net-rev";
};

MV1# cat /var/named/named.ca
...
MV1# cat /var/named/named.loopback
...                                    (+ suppression RR concernant IPV6)

MV1# cat /var/named/named.localhost
...                                    (+ suppression RR concernant IPV6)
```

Configurez les fichiers de la zone du domaine "isat.net" sur MV1

```
MV1# cat /var/named/db.isat.net
$ORIGIN isat.net.
$TTL          2D
isat.net.     IN    SOA   ns.isat.net.   root.isat.net.  (
                                        2017110700 ; Serial
                                        28800      ; Refresh
                                        14400      ; Retry
                                        3600000    ; Expire
                                        7200 )    ; Minimum
              IN    NS    ns.isat.net.
ex            IN    NS    ns.ex.isat.net.

ns            IN    A     192.168.8.2
mail          IN    A     192.168.8.2
news          IN    A     192.168.8.3
ftp           IN    A     192.168.8.4
ns.ex         IN    A     192.168.8.5

isat.net.     IN    MX    10    mail

MV1# cat /var/named/ db.isat.net-rev
$ORIGIN       8.168.192.in-addr.arpa.
$TTL          2D
8.168.192.in-addr.arpa.  IN   SOA  ns.isat.net. root.isat.net.  (
                                        2017110700 ; Serial
                                        28800      ; Refresh
                                        14400      ; Retry
                                        3600000    ; Expire
                                        7200  )    ; Minimum
              IN   NS     ns.isat.net.
5             IN    NS    ns.ex.isat.net.

2             IN   PTR    mail.isat.net.
3             IN   PTR    news.isat.net.
4             IN   PTR    ftp.isat.net.
```

Pour signaler que la résolution inverse de cette adresse doit se faire via la zone reverse du serveur ns.ex.isat.net…

!! Attention aux permissions !!

```
MV1# chgrp named db.isat.net*
```

Configurez le fichier /etc/named.conf sur MV4.

```
MV4# cat /etc/named.conf
options {
   listen-on port 53 {127.0.0.1 ; 192.168.8.5 ;};
   directory "/var/named";
};

zone "." IN {
   type hint;
   file "named.ca";
};

zone "1.0.0.127.in-addr.arpa" IN {
   type master;
   file "named.loopback";
};

zone "localhost" IN {
   type master;
   file "named.localhost";
};

zone "ex.isat.net" {
   type master;
   file "db.ex.isat.net";
};

zone "8.168.192.in-addr.arpa" {
   type master;
   file "db.ex.isat.net-rev";
};
```

```
MV4# cat /var/named/named.ca
...
MV4# cat /var/named/named.loopback
...                                    (+ suppression RR concernant IPV6)

MV4# cat /var/named/named.localhost
...                                    (+ suppression RR concernant IPV6)
```

Configurez les fichiers de la zone du domaine "ex.isat.net" sur MV4

```
MV4# cat /var/named/db.ex.isat.net
$ORIGIN ex.isat.net.
$TTL    2D
ex.isat.net.  IN    SOA     ns.ex.isat.net.   root.ex.isat.net.  (
                                        2017110700 ; Serial
                                        28800      ; Refresh
                                        14400      ; Retry
                                        3600000    ; Expire
                                        7200 )    ; Minimum
          IN  NS    ns.ex.isat.net.

ns        IN  A     192.168.8.5
www       IN  A     192.168.8.5
w3        IN  A     192.168.8.5


MV4# cat /var/named/db.ex.isat.net-rev
$ORIGIN      8.168.192.in-addr.arpa.
$TTL         2D
8.168.192.in-addr.arpa.  IN   SOA  ns.ex.isat.net. root.isat.net.  (
                                        2017110700 ; Serial
                                        28800      ; Refresh
                                        14400      ; Retry
                                        3600000    ; Expire
                                        7200  )    ; Minimum
             IN   NS     ns.ex.isat.net.

5            IN   PTR    www.ex.isat.net.
5            IN   PTR    www3.ex.isat.net.
```

!! Attention aux permissions !!

```
MV4# chgrp named db.ex.isat.net*
```

Configurez les resolvers des 4 machines.

```
MV1# echo nameserver 127.0.0.1 > /etc/resolv.conf
MV2# echo nameserver 192.168.8.2 > /etc/resolv.conf
MV3# echo nameserver 192.168.8.2 > /etc/resolv.conf
MV4# echo nameserver 192.168.8.2 > /etc/resolv.conf
```

Vérifiez le fichier /etc/nsswitch.conf des 4 machines.

```
Sur MV1, MV2, MV3 et MV4:
--- Mise à jour de /etc/nsswitch.conf ---
# cat /etc/nsswitch.conf
...
hosts: files dns
```

Vérifiez le fichier /etc/hosts des 4 machines.

```
Sur MV1, MV2, MV3 et MV4:
--- Mise à jour de /etc/hosts (+ suppression ligne concernant IPV6) ---
# cat /etc/hosts
127.0.0.1 localhost ...
```

Lancez vos 2 dns + vérification des logs dans /var/log/messages

```
MV1# systemctl start named
MV1# tail -50 /var/log/messages | grep named

MV4# systemctl start named
MV4# tail -50 /var/log/messages | grep named
```

- Fonctionnement (ping + outils de debugage):

. chaque mv doit pouvoir se toucher par son nom.

```
MV4# ping mail.isat.net      → pour la zone parente
MV4# ping news.isat.net
MV4# ping ftp.isat.net
MV4# ping www.ex.isat.net    → pour la zone fille
MV4# ping w3.ex.isat.net

MV2# ping mail.isat.net      → pour la zone parente
MV2# ping news.isat.net
MV2# ping ftp.isat.net
MV4# ping www.ex.isat.net    → pour la zone fille
MV4# ping w3.ex.isat.net

…

MV1# nslookup -sil
> news.isat.net
Server:     127.0.0.1
Address:    127.0.0.1#53

Name:       news.isat.net
Address:    192.168.8.3            (Faire idem pour ftp et mail …)

> 192.168.8.2
Server:     127.0.0.1
Address:    127.0.0.1#53           (Faire idem pour 192.168.8.3 et 4)

2.8.168.192.in-addr.arpa  name = mail.isat.net.
```

> 192.168.8.5 → *la requête est envoyée au dns local … (suite)*

```
Server:     127.0.0.1
Address:    127.0.0.1#53

Non-authoritative answer
5.8.168.192.in-addr.arpa            name = www.8.168.192.in-addr.arpa.
5.8.168.192.in-addr.arpa            name = w3.8.168.192.in-addr.arpa.

Authoritative answers can be found from:
5.8.168.192.in-addr.arpa            nameserver = ns.ex.isat.net.
```

(suite) … et est résolue par ns.ex.isat.net

```
> www.ex.isat.net
Server:     127.0.0.1
Address:    127.0.0.1#53

Non-authoritative answer
Name:       www.ex.isat.net
Address:    192.168.8.5             (Faire idem pour w3 …)

MV4# nslookup -sil
> news.isat.net
Server:     192.168.8.2
Address:    192.168.8.2#53

Name:       news.isat.net
Address:    192.168.8.3             (Faire idem pour ftp et mail …)

> 192.168.8.2
Server:     192.168.8.2
Address:    192.168.8.2#53          (Faire idem pour 192.168.8.3 et 4…)

2.8.168.192.in-addr.arpa  name = mail.isat.net.
```

> 192.168.8.5 → *la requête est envoyée au dns 192.168.8.2 … (suite)*

```
Server:     192.168.8.2
Address:    192.168.8.2#53

Non-authoritative answer
5.8.168.192.in-addr.arpa            name = www.8.168.192.in-addr.arpa.
5.8.168.192.in-addr.arpa            name = w3.8.168.192.in-addr.arpa.

Authoritative answers can be found from:
5.8.168.192.in-addr.arpa            nameserver = ns.ex.isat.net.
```

(suite) … et est résolue par ns.ex.isat.net

```
> www.ex.isat.net
Server:     192.168.8.2
Address:    192.168.8.2#53

Non-authoritative answer
Name:       www.ex.isat.net
Address:    192.168.8.5             (Faire idem pour w3 …)
```

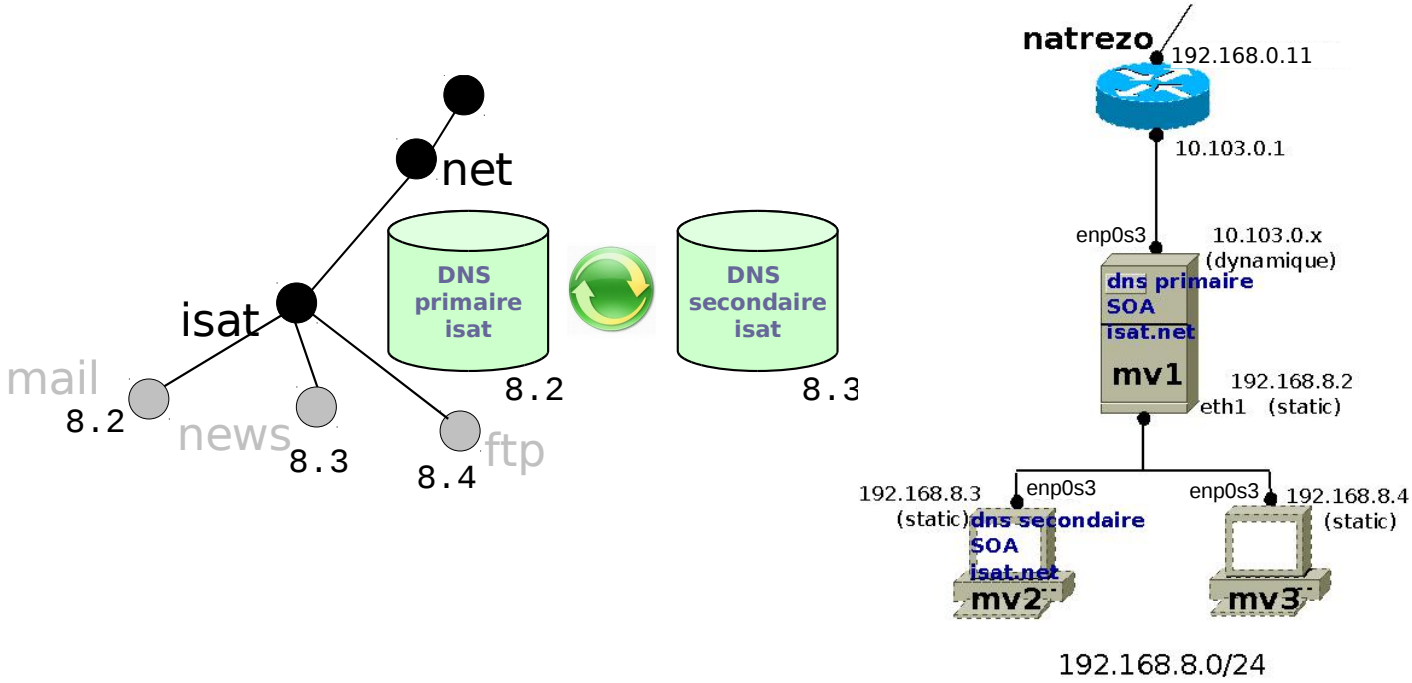
. chaque mv a toujours l'accès à l'internet.

```
MV1# rndc flush   --> on vide le cache

MV1# lynx www.kernel.org
MV2# lynx www.tf1.fr
MV3# lynx www.rtbf.be
MV4# lynx www.ovh.com
```

Exercice 4: Redondance

- Construire les serveurs dns primaires et secondaires de 'isat.net.':



VirtualBox: Voir exercice 3

Maquette: Voir exercice 3

Particularités: Voir exercice 3

- Configurez vos dns:

Installez les packages de Bind sur MV1 et MV2 (voir avant)

Configurez le fichier /etc/named.conf sur MV1.

```
MV1# cat /etc/named.conf
options {
   listen-on port 53 {127.0.0.1 ; 192.168.8.2 ; };
   directory "/var/named";
};

zone "." IN {
   type hint;
   file "named.ca";
};

zone "1.0.0.127.in-addr.arpa" IN {
   type master;
   file "named.loopback";
};

zone "localhost" IN {
   type master;
   file "named.localhost";
};
```

```
zone "isat.net" IN {
   type master;
   notify yes;
   also-notify {192.168.8.3;} ;
   allow-transfer {192.168.8.3;};
   file "db.isat.net";
};

zone "8.168.192.in-addr.arpa" In {
   type master;
   notify yes;
   also-notify {192.168.8.3;} ;
   allow-transfer {192.168.8.3;};
   file "db.isat.net-rev";
};

MV1# cat /var/named/named.ca
...
MV1# cat /var/named/named.loopback
...                                    (+ suppression RR concernant IPV6)

MV1# cat /var/named/named.localhost
...                                    (+ suppression RR concernant IPV6)
```

Configurez les fichiers de la zone du domaine "isat.net" sur MV1

```
MV1# cat /var/named/db.isat.net
$ORIGIN isat.net.
$TTL    2D
isat.net.   IN    SOA     ns.isat.net.    root.isat.net.  (
                                          2017110701 ; Serial
                                          28800      ; Refresh
                                          14400      ; Retry
                                          3600000    ; Expire
                                          7200 )     ; Minimum

           IN        NS    ns.isat.net.
           IN        NS    ns2.isat.net.

ns         IN  A     192.168.8.2
ns2        IN  A     192.168.8.3
mail       IN  A     192.168.8.2
news       IN  A     192.168.8.3
ftp        IN  A     192.168.8.4

r2d2       IN  CNAME mail
lea        IN  CNAME ftp
yoda       IN  CNAME news

isat.net.  IN MX    10    mail
```

```
MV1# cat /var/named/db.isat.net-rev
$ORIGIN 8.168.192.in-addr.arpa.
$TTL   2D
8.168.192.in-addr.arpa.  IN   SOA  ns.isat.net. root.isat.net.  (
                                    2017110701 ; Serial
                                    28800      ; Refresh
                                    14400      ; Retry
                                    3600000    ; Expire
                                    7200  )    ; Minimum

             IN    NS    ns.isat.net.
3            IN    NS    ns2.isat.net.

2            IN    PTR   mail.isat.net.
3            IN    PTR   news.isat.net.
4            IN    PTR   ftp.isat.net.
```

Attention aux permissions

```
MV1# chgrp named db.isat.net*
```

Configurez le fichier /etc/named.conf sur MV2.

```
MV2# cat /etc/named.conf
options {
   listen-on port 53 {127.0.0.1 ; 192.168.8.3;} ;
   directory "/var/named";
};

zone "." IN  {
   type hint;
   file "named.ca";
};

zone "1.0.0.127.in-addr.arpa" IN {
   type master;
   file "named.loopback";
};

zone "localhost" IN {
   type master;
   file "named.localhost";
};

zone "isat.net" IN {
   type slave;
   masters { 192.168.8.2; };
   file "slaves/db.isat.net";
};

zone "8.168.192.in-addr.arpa" IN {
   type slave;
   masters { 192.168.8.2; };
  file "slaves/db.isat.net-rev";
};


MV2# cat /var/named/named.ca
...
MV2# cat /var/named/named.loopback
...                                  (+ suppression RR concernant IPV6)

MV2# cat /var/named/named.localhost
...                                  (+ suppression RR concernant IPV6)
```

Configurez les resolvers des 4 machines.

```
MV1# echo nameserver 127.0.0.1 > /etc/resolv.conf
MV2# echo nameserver 127.0.0.1 > /etc/resolv.conf
MV3# echo nameserver 192.168.8.2 > /etc/resolv.conf
MV3# echo nameserver 192.168.8.3 >> /etc/resolv.conf
```

Vérifiez le fichier /etc/nsswitch.conf des 4 machines.

```
Sur MV1, MV2, MV3 et MV4:
--- Mise à jour de /etc/nsswitch.conf ---
# cat /etc/nsswitch.conf
...
hosts: files dns
```

Vérifiez le fichier /etc/hosts des 4 machines.

```
Sur MV1, MV2, MV3 et MV4:
--- Mise à jour de /etc/hosts (+ suppression ligne concernant IPV6) ---
# cat /etc/hosts
127.0.0.1 localhost ...
```

Lancez vos 2 dns + vérification des logs dans /var/log/messages

```
MV1# systemctl start named
MV1# tail -50 /var/log/messages | grep named

MV4# systemctl start named
MV4# tail -50 /var/log/messages | grep named
```

- Lancez un shell sur MV1 et MV2 pour surveiller l'évolution des logs.

```
MV1# tail -f /var/log/messages
MV2# tail -f /var/log/messages
```

Démarrez bind sur le primaire puis sur le secondaire.

```
MV1# systemctl start named
MV2# systemct start named
```

Que constatez-vous ?

Les 2 fichiers db.isat.net et db.isat.net-rev sont bien recopiés dans le dossier /var/named/slaves de MV2. (Attention: named doit avoir la permission d'écrire dans ce dossier !!!)

On constate bien aussi la notification du transfert des zones aussi bien dans les logs du primaire que dans ceux du secondaire. Le transfert est de type AXFR → ***Full zone transfer*** *car les zones recopiées n'existaient pas déjà.*

- Incrémentez le numéro de série et ajoutez un RR factice dans les 2 zones du primaire.

db.isat.net

```
    2017110702 ; Serial
…
bidon  A    192.168.8.5
```

db.isat.net-rev

```
     2017110702 ; Serial
…
5    PTR   bidon.isat.net.
```

Rechargez les zones du primaire.

```
MV1# rndc reload
```

Que constatez-vous ?

Les 2 fichiers db.isat.net et db.isat.net-rev sont bien recopiés dans le dossier /var/named/slaves de MV2. (Attention: named doit avoir la permission d'écrire dans ce dossier !!!)

*On constate bien aussi la notification du transfert des zones aussi bien dans les logs du primaire que dans ceux du secondaire. Le transfert est de type IXFR → **Incremental zone transfer** car les zones recopiées existaient déjà.*

- Sur MV3, déclarez MV1 et MV2 comme dns à contacter pour résoudre des noms et tentez une résolution de noms.

/etc/resolv.conf

```
nameserver 192.168.8.2
nameserver 192.168.8.3
```

```
MV3# ping ftp.isat.net     → ok
```

Stoppez bind sur MV1.

```
MV1# systemctl stop named
```

Retentez une résolution de noms à partir de MV3.
Que constatez-vous ?

```
MV3# ping ftp.isat.net     → ok
```

Cela fonctionne toujours car, bien que le dns primaire (192.168.8.2) soit hors circuit, le secondaire tourne toujours, a autorité sur isat.net et répond donc correctement aux requêtes.