

Bachelier en informatique et Systèmes

Informatique industrielle

3^{ème} année

HELHa

Haute École Louvain
en Hainaut

Catégorie technique

Laboratoire de réseaux

DNS

2015 – 2016

Haveaux Valentin

Tables des matières

1	Serveur DNS	4
2	Procédure	4
2.1	Cartes réseaux non reconnus	4
2.2	Activer l'IP forwarding et le nating	4
2.3	Installer les packages.....	4
2.4	Mise à jours fichier de configuration.....	4
2.5	Attention aux permissions.....	5
2.6	Configurer les resolvers des machines	5
2.7	Vérifier le fichier /etc/nsswitch.conf des machines	5
2.8	Vérifiez le fichier /etc/hosts des machines	5
2.9	Lancez votre dns + vérification des logs	5
2.10	Tester et debugger votre DNS	5
3	Serveur de cache	6
4	Serveur forward esclave	6
5	Serveur autoritaire récursif	7
6	Service autoritaire itératif	7
7	Fichier de zone	8
8	Fichier de zone reverse	8
9	Délégation et sous domaine.....	9
9.1	Fichier de la zone parente	9
9.2	Fichier de la zone reverse parente	9
9.3	Fichier de la zone fille.....	10
9.4	Fichiez la zone reverse fille.....	10
10	Debug DNS	11

10.1	dig.....	11
10.1.1	Autre cas.....	11
10.1.2	Domaine non trouvées	11
10.2	nslookup	12
10.2.1	Suivre la chaîne de délégations	12
10.2.2	Recherche inverse	12
11	Syntaxe d'un Ressource Record	13
11.1	Les différents types	13
12	Les fichiers de zones.....	14

DNS

1 Serveur DNS

Daemon du serveur DNS:	named
Package:	bind – bind-utils – bind-libs
Fichier de configuration:	/etc/named.conf fichier de configuration principal /var/named dossier par défaut contenant les fichiers de zones
Lancement/arrêt/redémarrage:	service dhcpd start/stop/restart
Vérifier la configuration:	named-checkconf /etc/named.conf
Vérifier la zone:	named-checkzone <nom zone> <fichier de zone>

2 Procédure

2.1 Cartes réseaux non reconnus

```
# rm -rf /etc/udev/rules.d/70-persistent-net.rules  
  
# reboot
```

2.2 Activer l'IP forwarding et le nating

```
# mcedit /etc/sysctl.conf                  ip_forward=1  
  
# echo 'iptables -t nat -A POSTROUTING -j MASQUERADE' >> /etc/rc.local  
  
# /etc/rc.local
```

2.3 Installer les packages

```
yum install bind bind-libs bind-utils -y
```

2.4 Mise à jours fichier de configuration

Mise à jour de /etc/named.conf

Supprimer les RR concernant l'IPv6 dans:

```
/var/named/named.loopback et /var/named/named.localhost
```

```
named-checkconf /etc/named.conf
```

Ajouter vos zones, puis vérifiez les :

```
named-checkconf "nom zone" "fichier de zone"
```

2.5 Attention aux permissions

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

2.6 Configurer les résolveurs des machines

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

```
MV2# echo nameserver 192.168.0.2 > /etc/resolv.conf
```

2.7 Vérifier le fichier /etc/nsswitch.conf des machines

```
grep hosts: /etc/nsswitch.conf
```

...

```
hosts: files dns
```

2.8 Vérifiez le fichier /etc/hosts des machines

--- Mise à jour de /etc/hosts (+ suppression ligne concernant IPV6) ---

```
# cat /etc/hosts
```

```
127.0.0.1 localhost ...
```

2.9 Lancez votre dns + vérification des logs

```
service named start
```

```
tail -50 /var/log/messages | grep named
```

```
ps ax | grep named
```

```
netstat -tunl
```

2.10 Tester et debugger votre DNS

Vérifier le fonctionnement: nslookup www.helha.be

Vider le cache: rndc flush

Lire les trames: `tshark -V -i eth0 port 53 > sniffdns.txt`

3 Serveur de cache

```
options {
    listen-on port 53 {127.0.0.1 ; 192.1.0.0/24 ; } ; // Port d'écoute, ip admises
    directory "/var/named"; // répertoire des fichiers de zones
};

zone "." in {
    type hint;
    file "named.ca"; // cache des serveurs racines
};

zone "1.0.0.127.in-addr.arpa" {
    type master;
    file "named.loopback"; // zone primaire du reverse loopback
};

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

Ces 3 fichiers de zones seront automatiquement créés lors de l'installation du package 'bind'...

// Zone primaire du loopback.
// Facultative sauf si on veut faire résoudre le nom 'localhost' par le serveur.

4 Serveur forward esclave

```
options {
    listen-on port 53 {127.0.0.1 ; 192.1.0.0/24 ; } ;
    directory "/var/named";
    forwarders {192.2.0.3 ; 192.3.0.3 ;}; // on fait tout suivre
    forward only;
};
```

5 Serveur autoritaire récursif

named.conf

```
options {  
    listen-on port 53 {127.0.0.1 ; 192.168.8.0/24 ; } ; // Port d'écoute, ip admises  
    directory "/var/named";  
    recursion yes;           //récursif (yes par défaut)  
};  
  
zone "." in {                                     (Suite)  
    type hint;  
    file "named.ca";  
};  
  
zone "1.0.0.127.in-addr.arpa" {  
    type master;  
    file "named.loopback";  
};  
  
zone "localhost" {  
    type master;  
    file "named.localhost";  
};  
  
zone "isat.net" {  
    type master;  
    file "db.isat.net";  
}; // zone primaire isat.net  
  
zone "8.168.192.in-addr.arpa" {  
    type master;  
    file "db.isat.net-rev";  
}; // zone primaire du reverse isat.net
```

6 Service autoritaire itératif

```
options {  
    listen-on port 53 {127.0.0.1 ; 192.168.8.0/24 ; } ; // Port d'écoute, ip admises  
    directory "/var/named";  
    recursion no;           // le serveur n'accepte aucune requête récursive  
};  
  
...  
idem ci-avant  
...
```

7 Fichier de zone

```
$ORIGIN isat.net.
$TTL 2D
isat.net. IN SOA ns.isat.net. root.isat.net. (
    2012110700 ; 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
```

8 Fichier de zone reverse

```
$ORIGIN 8.168.192.in-addr.arpa.
$TTL 2D
8.168.192.in-addr.arpa. IN SOA ns.isat.net. root.isat.net. (
    2012110700 ; 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.
```



RR de type 'Pointeur'

Indique le nom associé à un numéro IP dans l'arborescence in-addr.arpa (ip6.arpa)

```
2.8.168.192.in-addr.arpa. IN PTR mail.isat.net.
```


9 Délégation et sous domaine

9.1 Fichier de la zone parente

```
$ORIGIN isat.net.
$TTL 2D
isat.net. IN SOA ns.isat.net. root.isat.net. (
    2012110700 ; 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
```

La délégation de zone est déclarée dans le fichier de zone du domaine parent par un RR de type NS.

Et un RR de type A est ensuite nécessaire pour la correspondance entre l'adresse IP et le nom.

9.2 Fichier de la zone reverse parente

```
$ORIGIN 8.168.192.in-addr.arpa.
$TTL 2D
8.168.192.in-addr.arpa. IN SOA ns.isat.net. root.isat.net. (
    2012110700 ; 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...

9.3 Fichier de la zone fille

```
$ORIGIN ex.isat.net.
$TTL 2D
ex.isat.net. IN SOA ns.ex.isat.net. root.ex.isat.net. (
                                2012110700 ; 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
```



Le fichier de zone du sous-domaine est un fichier de zone classique.

9.4 Fichiez la zone reverse fille

```
$ORIGIN 8.168.192.in-addr.arpa.
$TTL 2D
8.168.192.in-addr.arpa. IN SOA ns.ex.isat.net. root.isat.net. (
                                2012110700 ; 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.
```

10 Debug DNS

10.1 dig

dig → donne la liste des serveurs racines

dig **@server name type** → donne les informations concernant une ressource (name) d'un certain type (type) d'un certain serveur Dns (@server). Suivre ensuite de serveur en serveur jusqu'à trouver l'IP.

10.1.1 Autre cas

dig www.helha.be

dig +trace www.helha.be → *Recherche à partir de la racine*

dig lesoir.be MX

dig -x 204.13.162.123 → *Recherche inverse*

10.1.2 Domaine non trouvées

;; -> HEADER ... status : NXDOMAIN → *Non eXistant DOMAIN*

10.2 nslookup

Cette commande peut être utilisée en mode interactif

10.2.1 Suivre la chaîne de délégations

```
# nslookup
> server e.root-servers.net      → on choisit un serveur racine
> set type=NS                   → on s'intéresse aux records de type NS
> org.                          → quels sont les dns qui gèrent org. ?
...
> server d0.org...              → on passe sur un de ces serveurs
> reseaucerta.org.             → quels sont les dns qui gèrent reseaucerta.org. ?
...
> server a.dns.gandi.net        → on passe sur un de ces serveurs
> set type=A                    → on s'intéresse aux records de type A
> www.reseaucerta.org          → quelle est l'Ip de www.reseaucerta.org ?
...

> set type=MX                   → on s'intéresse aux records de type MX
> reseaucerta.org.             → quels sont les serveurs de mail de reseaucerta.org ?
...
> set type=A                    → on s'intéresse aux records de type A
> smtp.reseaucerta.org.        → quelle est l'ip du serveur smtp de reseaucerta.org ?
...
> set type=ANY                  → on s'intéresse à tout
> reseaucerta.org.
...
```

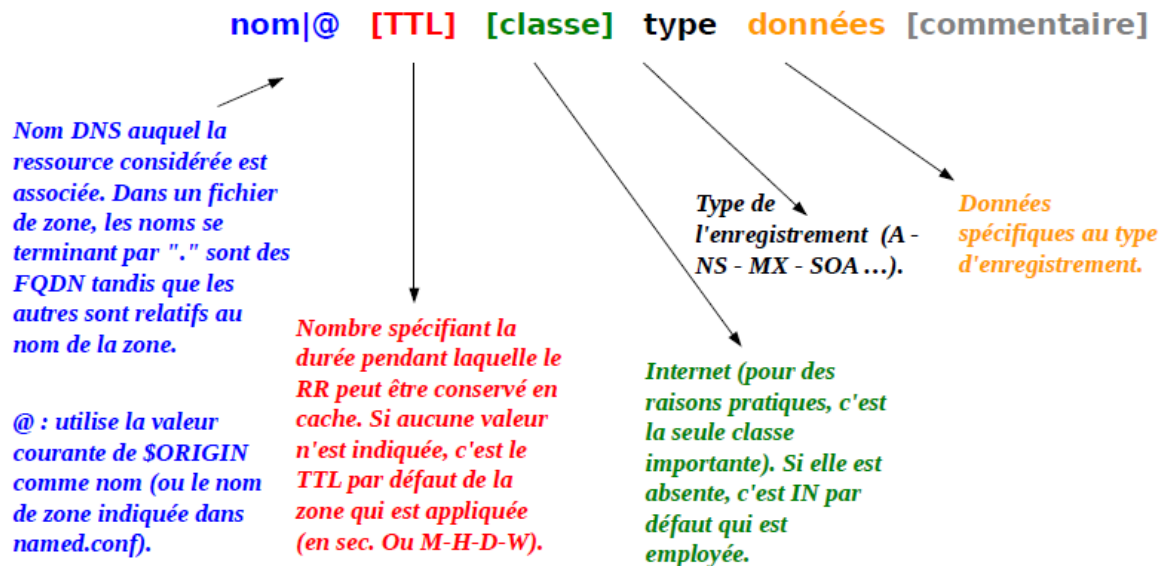
Autres cas

```
# nslookup www.lelibre.be → C'est le Dns par défaut qui est choisi pour résoudre le nom.
# nslookup www.lelibre.be 109.88.203.3 → C'est un autre Dns qui est choisi.
# nslookup 91.121.208.164 → Recherche inverse résolue avec le Dns par défaut.
```

10.2.2 Recherche inverse

```
# nslookup
> server e.root-servers.net      → on choisit un serveur racine
> set type=PTR                   → on s'intéresse aux records de type PTR
> 91.121.208.164                 → y a-t-il un RR de ce type dans sa zone in-addr.arpa ?
...                               → Et le serveur ne me répond pas directement, mais
...                               m'envoie une liste de serveurs ont autorité sur les
...                               adresses qui commencent par 91
> server dns12.ovh.net           → on en choisit un au hasard ...
> 91.121.208.164                → ... et on lui repose la même question
...
...                               → Ici, on a déjà la réponse. Cela signifie que dns12.ovh.net
...                               a autorité sur toutes les Ips du domaine 91.in-addr.arpa
...                               car il s'agit d'un réseau de classe A
```

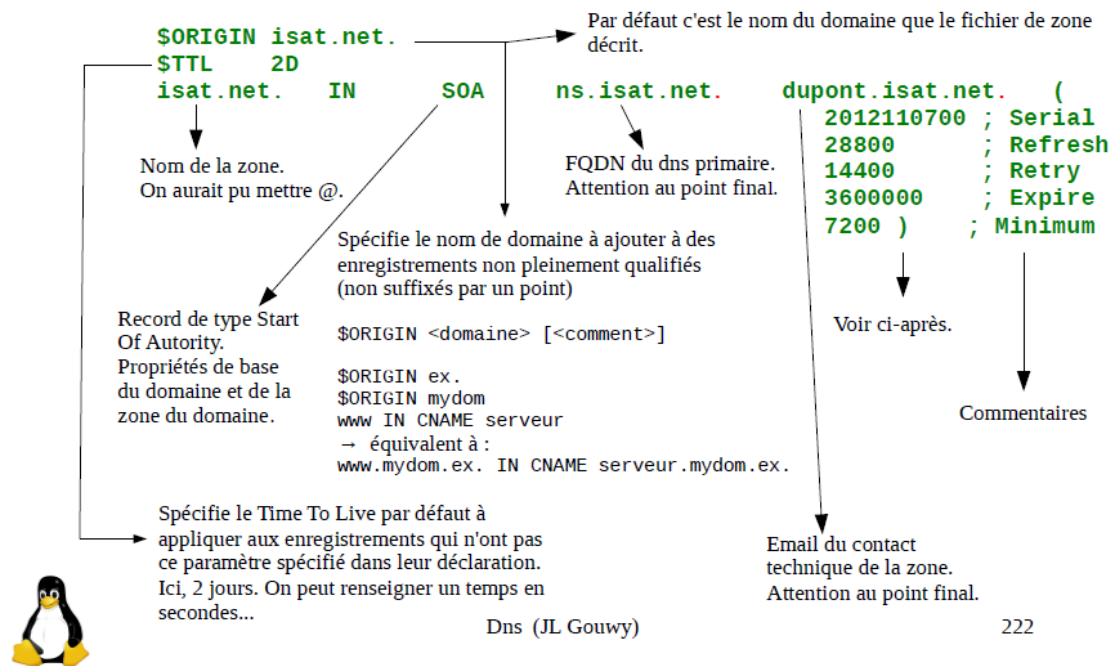
11 Syntaxe d'un Ressource Record



11.1 Les différents types

- A:** RR de type IPv4 Address, pour identifier une machine par un nom.
- AAAA:** RR de type IPv6 Address, pour identifier une machine par un nom.
- SOA:** RR de type Start Of Authority: propriétés de base du domaine et de la zone du domaine
- MX:** RR de type Mail Exchanger, pour indiquer l'adresse mail du domaine.
- NS:** RR de type Name Server. Serveur qui reçoit la délégation et la gestion des données de la zone.
- PTR:** RR de type Pointeur. Indique le nom associé à l'IP.

12 Les fichiers de zones



```

$ORIGIN isat.net.
$TTL 2D
isat.net. IN SOA ns.isat.net.

```

Serial: Spécifie la version des données de la zone.
A incrémenter à chaque modification (nécessaire pour à synchronisation des serveurs secondaires)
Conseil : YYYYMMDDxx → max. 99 modif./jour

Refresh: Intervalle, ici en sec., entre 2 vérifications du serial number par les secondaires.

Retry: Intervalle, ici en sec., entre 2 vérifications du serial number par les secondaires si la 1ere vérification a échoué.

Expire: Temps, ici en sec., après lequel le secondaire détruit les données de la zone qu'il possède et arrête de répondre aux requêtes pour cette zone s'il ne parvient pas à contacter le serveur primaire.

retry<<refresh<<expire

```

dupont.isat.net. (
    2012110700 ; Serial
    28800      ; Refresh
    14400      ; Retry
    3600000    ; Expire
    7200       ; Minimum
)

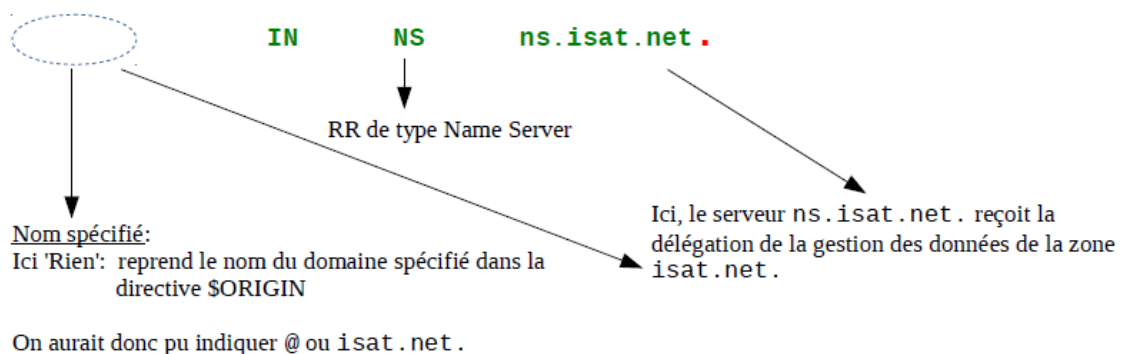
```

Minimum:

Temps que doit rester dans le cache une réponse négative suite à une question sur ce domaine.

Deux types de réponses négatives :

- NXDOMAIN : aucun RR ayant le nom demandé dans la classe (IN) n'existe dans cette zone.
- NODATA : aucune donnée pour le triplet (nom, type, classe) demandé n'existe ; il existe d'autres records possédant ce nom, mais de type différent.



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

RR de type IPv4 Address

Indique l'adresse IPv4 associée à un nom.
mail.isat.net. IN A 192.168.8.2

AAAA: Adresse IPv6

Les noms non pleinement qualifiés (ne se terminant pas par un point) sont relatifs au nom du domaine spécifié dans la directive \$ORIGIN
Donc, ici, les écritures :

mail.isat.net.	IN	A	192.168.8.2
et			
mail	IN	A	192.168.8.2

sont équivalentes.

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

RR de type 'Canonical name'

Indique que le nom est un alias
vers un autre nom (le nom canonique)

alias IN CNAME nom.canonique.

isat.net.	IN	MX	10	mail
-----------	----	----	----	------

RR de type 'Mail Exchanger'

Spécifie un serveur de messagerie pour la zone : email à quelqu-un@nom

On cherche dans le DNS un MX indiquant la machine sur laquelle il faut envoyer le courrier pour nom.

Un paramètre précise le poids relatif de l'enregistrement MX:
Si plusieurs MX existent, le courrier est envoyé en 1er à la machine ayant le poids le plus bas, puis dans l'ordre croissant des poids en cas d'échec

nom	IN	MX	10	nom.relais1.
	IN	MX	20	nom.relais2.
	IN	MX	30	nom.relais3.