

## Troubleshooting DNS

### Situation 1 :

**Symptôme :** L'employé occupant le poste "Client-1" se plaint de ne plus pouvoir naviguer sur Internet depuis la dernière mise à jour du réseau.

### Collecte des symptômes :

Après avoir démarré les serveurs dhcp et bind, on commence par tester la connectivité depuis client-1 avec une commande ping, par exemple sur 192.168.0.2 :

```
root@client-1: /
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
root@client-1:/# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
sharkytes from 192.168.0.2: icmp_seq=1 ttl=64 time=1.02 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=64 time=0.195 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=64 time=0.232 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=64 time=0.248 ms
64 bytes from 192.168.0.2: icmp_seq=5 ttl=64 time=0.208 ms
^C
--- 192.168.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4074ms
rtt min/avg/max/mdev = 0.195/0.381/1.023/0.321 ms
root@client-1:/#
```

Le ping fonctionne.

On teste ensuite le DNS avec dig, en lui demandant l'adresse de formation.lab :

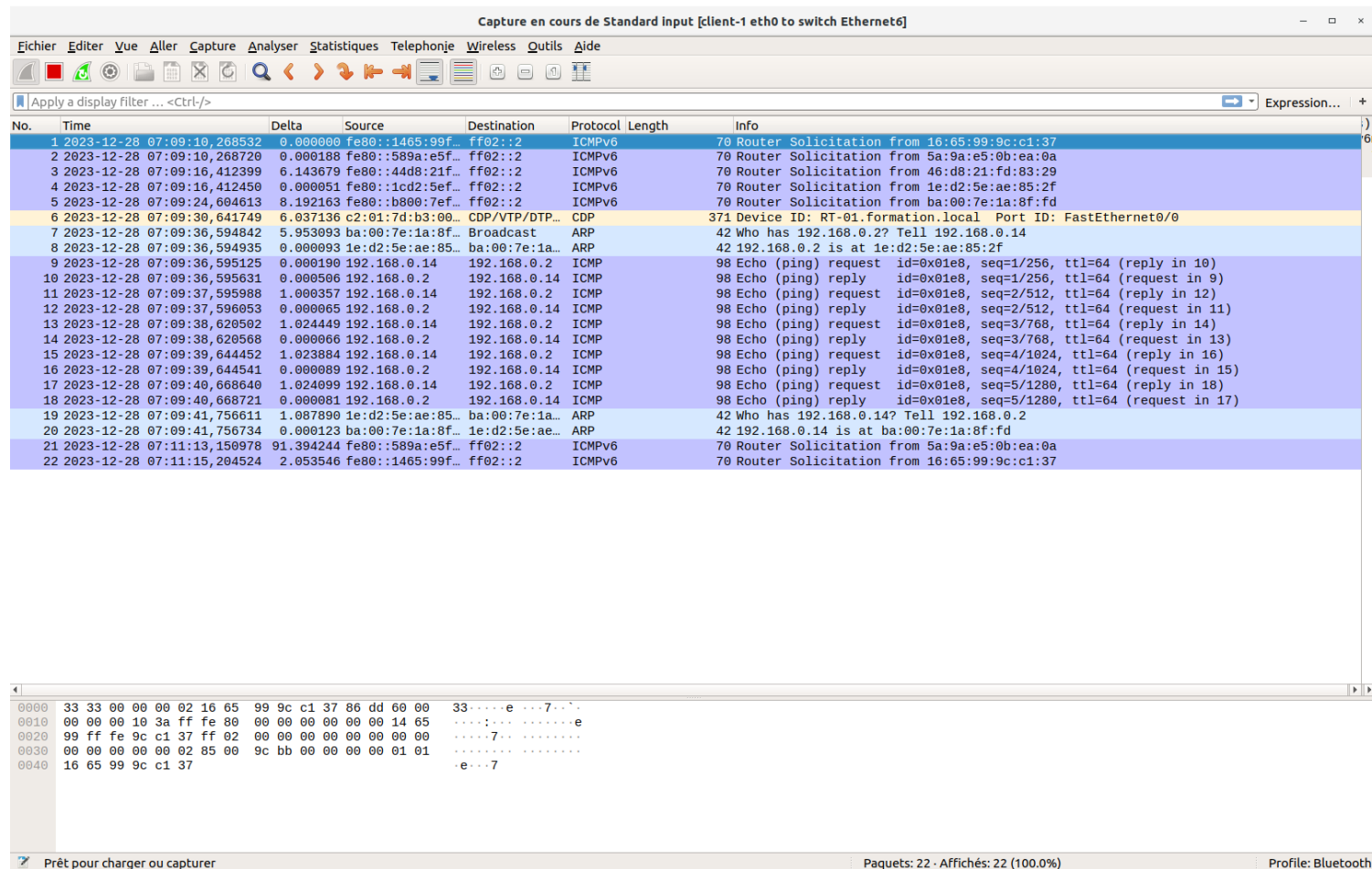
```
root@client-1:/# dig formation.lab

; <<>> DiG 9.16.1-Ubuntu <<>> formation.lab
;; global options: +cmd
;; connection timed out; no servers could be reached

root@client-1:/#
```

Le serveur ne peut pas être joint.

On regarde une trace Wireshark enregistrée entre client-1 et le switch pendant ces commandes :

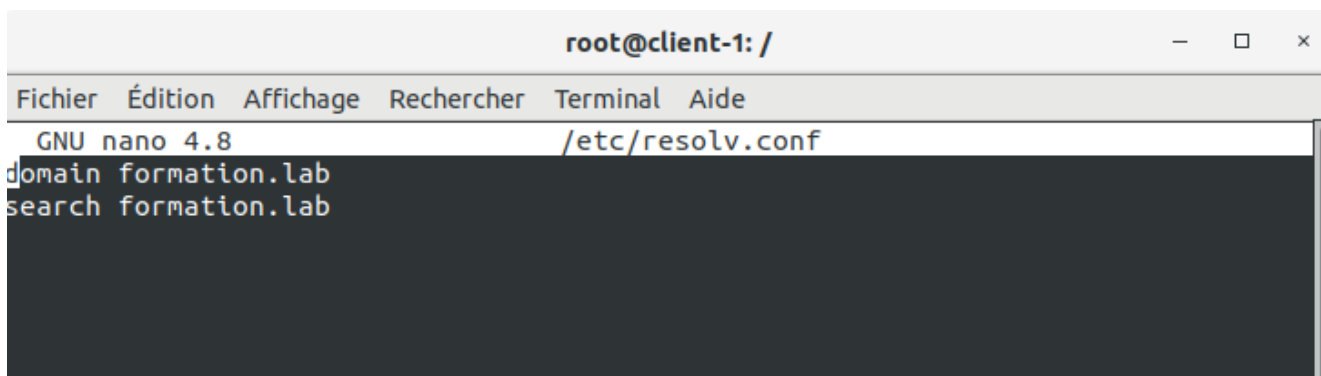


On voit bien les pings, au milieu en mauve, mais la commande dig n'a pas générée de trafic.

## Le problème :

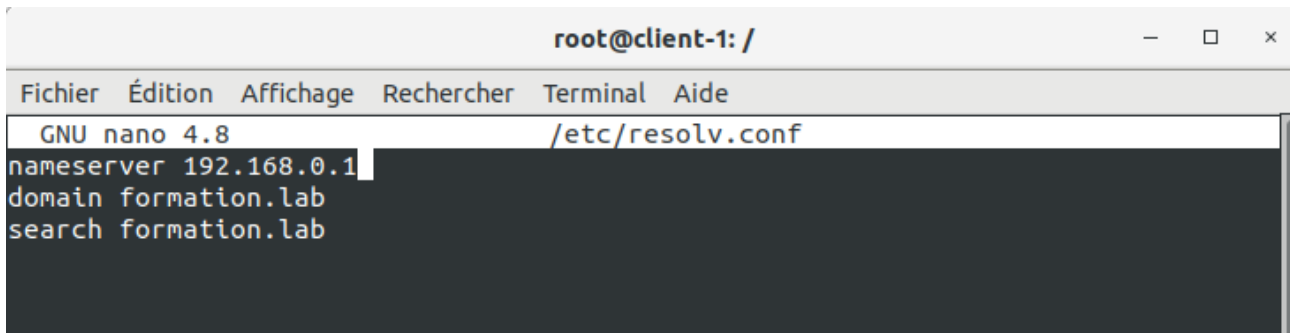
Par déduction la machine client ne connaît probablement pas l'adresse du résolveur, et donc ne peut rien lui envoyer.

Effectivement, il n'y a pas de namserveur dans /etc/resolv.conf :



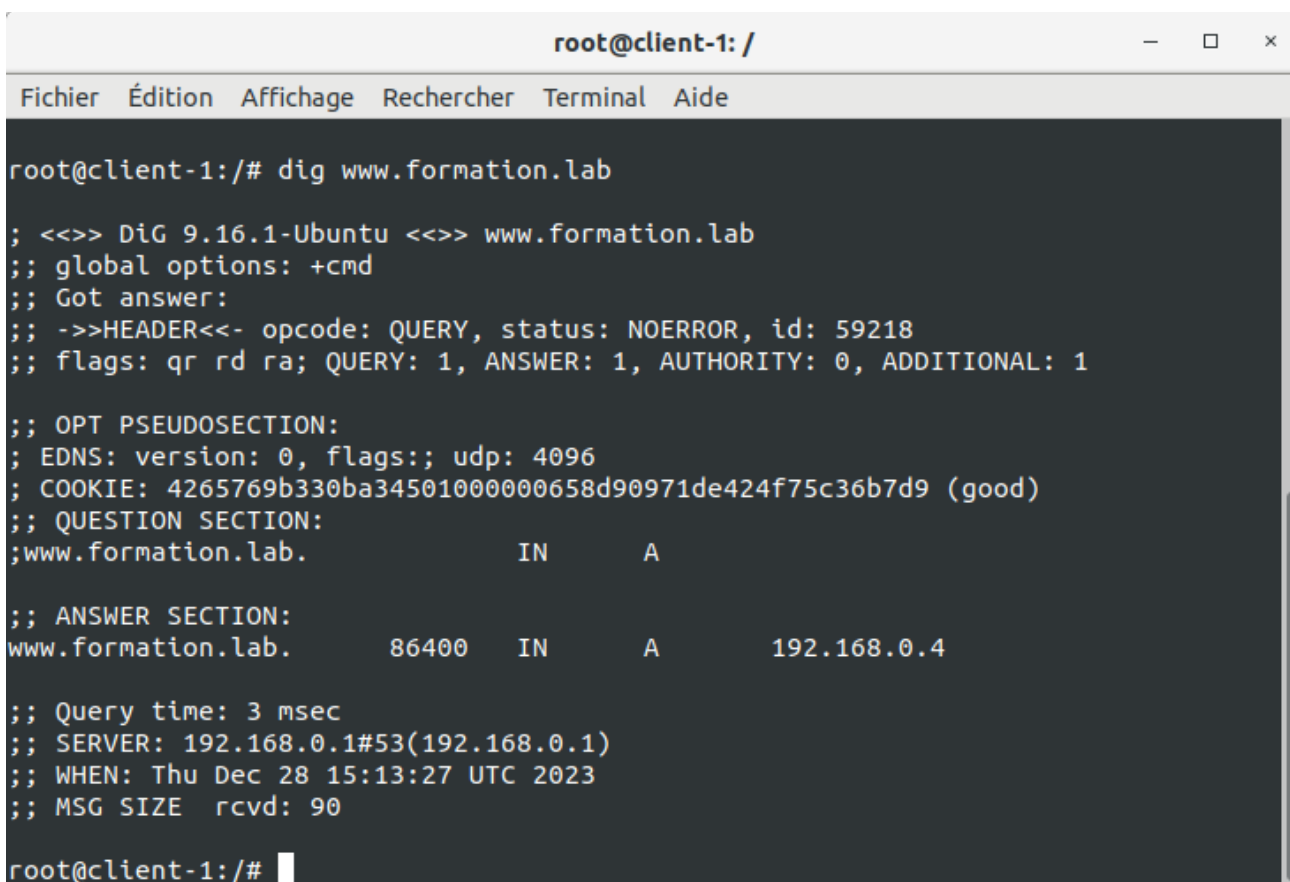
## Solution :

Il faut ajouter l'ip du résolveur dans le /etc/resolv.conf du client :



```
root@client-1: /
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 4.8 /etc/resolv.conf
nameserver 192.168.0.1
domain formation.lab
search formation.lab
```

On vérifie que le problème est résolu avec dig :



```
root@client-1: /
Fichier  Édition  Affichage  Rechercher  Terminal  Aide

root@client-1:/# dig www.formation.lab

; <<>> DiG 9.16.1-Ubuntu <<>> www.formation.lab
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59218
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 4265769b330ba34501000000658d90971de424f75c36b7d9 (good)
;; QUESTION SECTION:
;www.formation.lab.                IN      A

;; ANSWER SECTION:
www.formation.lab.                86400   IN      A      192.168.0.4

;; Query time: 3 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Thu Dec 28 15:13:27 UTC 2023
;; MSG SIZE rcvd: 90

root@client-1:/#
```

Cette fois on a une réponse correcte avec l'IP de la machine demandée.

## Situation 2 :

**Symptôme :** L'employé occupant le poste "Client-1" a bien accès à Internet, mais ne peut plus travailler sur le site intranet de l'entreprise.

## Collecte de Symptômes :

Depuis le post client, on peut ping les autres machines :

```
root@client-1: /
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

root@client-1:/# ping 192.168.0.3
PING 192.168.0.3 (192.168.0.3) 56(84) bytes of data.
64 bytes from 192.168.0.3: icmp_seq=1 ttl=64 time=2.14 ms
64 bytes from 192.168.0.3: icmp_seq=2 ttl=64 time=0.298 ms
64 bytes from 192.168.0.3: icmp_seq=3 ttl=64 time=0.171 ms
64 bytes from 192.168.0.3: icmp_seq=4 ttl=64 time=0.274 ms
^C
--- 192.168.0.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3054ms
rtt min/avg/max/mdev = 0.171/0.721/2.141/0.821 ms
root@client-1:/#
```

En faisant une demande DNS avec dig de formation.lab, le résolveur répond mais ne donne pas l'adresse demandée :

```
root@client-1:/# dig formation.lab

; <<>> DiG 9.16.1-Ubuntu <<>> formation.lab
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 33454
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: bcb2646fed52c5301000000658d9939578b001305d8ee7e (good)
;; QUESTION SECTION:
;formation.lab.                IN      A

;; Query time: 0 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Thu Dec 28 15:50:17 UTC 2023
;; MSG SIZE rcvd: 70

root@client-1:/#
```

## Le problème :

On va voir dans la machine resolver. Dans son fichier /etc/bind/named.conf, il manque la zone formation.lab. et la zone reverse :



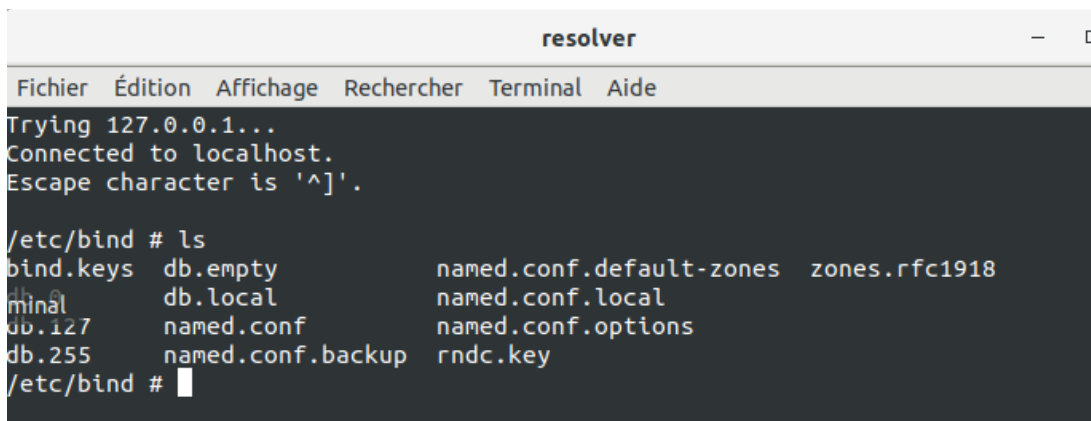
```
resolver
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 4.8                                named.conf

zone "localhost" IN {
    type master;
    file "db.local";
    allow-update { none; };
    notify no;
};

zone "127.in-addr.arpa" IN {
    type master;
    file "db.127";
    allow-update { none; };
    notify no;
};

logging {
    channel "misc" {
        file "/var/log/named/misc.log" versions 4 size 4m;
        print-time YES;
        print-severity YES;
    };
};
```

De plus le fichier /etc/bind/reverse.lab n'est pas présent :

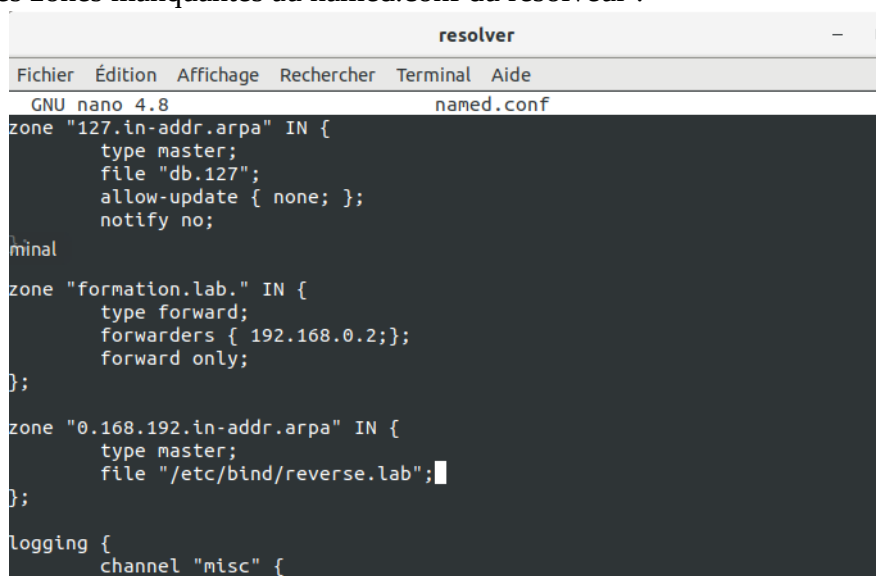


```
resolver
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

/etc/bind # ls
bind.keys      db.empty      named.conf.default-zones  zones.rfc1918
db.127         db.local      named.conf.local          named.conf.options
db.255         named.conf    named.conf.backup         rndc.key
/etc/bind #
```

## Solution :

On ajoute les zones manquantes au named.conf du résolveur :



```
resolver
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 4.8                                named.conf

zone "127.in-addr.arpa" IN {
    type master;
    file "db.127";
    allow-update { none; };
    notify no;
};

zone "formation.lab." IN {
    type forward;
    forwarders { 192.168.0.2; };
    forward only;
};

zone "0.168.192.in-addr.arpa" IN {
    type master;
    file "/etc/bind/reverse.lab";
};

logging {
    channel "misc" {
        file "/var/log/named/misc.log" versions 4 size 4m;
        print-time YES;
        print-severity YES;
    };
};
```

Et le fichier reverse.lab (on aurait aussi pu forward les requêtes reverse au SOA) :

```
resolver
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 4.8                                reverse.lab
$TTL      86400 ; 24 hours, could have been written as 24h or 1d
$ORIGIN 0.168.192.in-addr.arpa.
@ 1D IN      SOA soa.formation.lab. admin.formation.lab. (
                                2002022401 ; serial
                                3H ; refresh
                                15 ; retry
                                1w ; expire
                                3h ; minimum
                                )
; Name servers for the zone
IN NS soa.formation.lab.
; server host definitions
1 IN PTR resolver.formation.lab.
2 IN PTR soa.formation.lab.
3 IN PTR dhcp.formation.lab.
4 IN PTR www.formation.lab.
5 IN PTR mail.formation.lab.
```

On redémarre la machine resolver, et on vérifie que le problème est réglé du côté du client, toujours avec dig :

```
root@client-1: /
Fichier  Édition  Affichage  Rechercher  Terminal  Aide

root@client-1: /# dig www.formation.lab

;; <<>> DiG 9.16.1-Ubuntu <<>> www.formation.lab
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11351
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:: udp: 4096
;; COOKIE: 424641b415f8481301000000658d9d892213e558492b5969 (good)
;; QUESTION SECTION:
;www.formation.lab.                IN      A

;; ANSWER SECTION:
www.formation.lab.                86400   IN      A      192.168.0.4

;; Query time: 0 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Thu Dec 28 16:08:41 UTC 2023
;; MSG SIZE rcvd: 90
```

On a bien une section réponse avec l'IP du serveur pour www.formation.lab

### Situation 3 :

**Symptôme :** Comme pour la situation 2, l'employé occupant le poste "Client-1" a bien accès à Internet, mais ne peut plus travailler sur le site intranet de l'entreprise.

### Collecte des symptômes :

Immédiatement en démarrant le serveur bind sur la machine SOA, on voit que la zone formation.lab n'est pas chargée à cause d'une erreur : « NS 'soa.formation.lab.formation.lab' has no address records »

```
root@soa: /
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
28-Dec-2023 16:33:01.541 listening on IPv4 interface lo, 127.0.0.1#53
28-Dec-2023 16:33:01.545 listening on IPv4 interface eth0, 192.168.0.2#53
28-Dec-2023 16:33:01.545 generating session key for dynamic DNS
28-Dec-2023 16:33:01.545 sizing zone task pool based on 2 zones
28-Dec-2023 16:33:01.545 none:100: 'max-cache-size 90%' - setting to 7161MB (out of 7957MB)
28-Dec-2023 16:33:01.545 set up managed keys zone for view _default, file 'managed-keys.bind'
28-Dec-2023 16:33:01.549 none:100: 'max-cache-size 90%' - setting to 7161MB (out of 7957MB)
28-Dec-2023 16:33:01.549 configuring command channel from '/etc/bind/rndc.key'
28-Dec-2023 16:33:01.549 command channel listening on 127.0.0.1#953
28-Dec-2023 16:33:01.549 configuring command channel from '/etc/bind/rndc.key'
28-Dec-2023 16:33:01.549 command channel listening on ::1#953
28-Dec-2023 16:33:01.549 not using config file logging statement for logging due to -g option
28-Dec-2023 16:33:01.561 managed-keys-zone: loaded serial 0
28-Dec-2023 16:33:01.561 zone 0.168.192.in-addr.arpa/IN: loaded serial 2002022401
28-Dec-2023 16:33:01.561 zone formation.lab/IN: NS 'soa.formation.lab.formation.lab' has no address records (A or AAAA)
28-Dec-2023 16:33:01.561 zone formation.lab/IN: not loaded due to errors.
28-Dec-2023 16:33:01.561 all zones loaded
28-Dec-2023 16:33:01.561 running
```

### Le problème :

Dans le fichier de zone /etc/bind/formation.lab il est écrit 'soa.formation.lab' à la place de 'soa' dans la ligne du nameserver pour le SOA. Ce qui est interprété comme le sous-domaine soa.formation.lab du domaine formation.lab, donc soa.formation.lab.formation.lab.

```
soa
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 4.8 formation.lab
$ORIGIN formation.lab.
$TTL 1d

@      IN      SOA      soa.formation.lab      vvds.ephec.be. (
                2001062501 ; serial
                21600    ; refresh after 6 hours
                3600     ; retry after 1 hour
                604800   ; expire after 1 week
                86400    ) ; minimum TTL of 1 day

;

@      IN      NS      soa.formation.lab
@      IN      MX      10      mail

soa    IN      A        192.168.0.2
resolver    IN      A        192.168.0.1
dhcpd     IN      A        192.168.0.3
www       IN      A        192.168.0.4
mail      IN      A        192.168.0.5
```



Cela produit aussi une erreur parce qu'il n'y a pas d'adresse indiquée pour 'soa.formation.lab' en dessous.

Après corriger cette ligne :

```
soa
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 4.8                                formation.lab
$ORIGIN formation.lab.
$TTL 1d

@      IN      SOA      soa.formation.lab      vvds.ephec.be. (
                2001062501 ; serial
                21600      ; refresh after 6 hours
                3600      ; retry after 1 hour
                604800     ; expire after 1 week
                86400 )    ; minimum TTL of 1 day
;

@      IN      NS       soa
@      IN      MX       10      mail

soa                IN      A      192.168.0.2
resolver          IN      A      192.168.0.1
dhcpd             IN      A      192.168.0.3
www               IN      A      192.168.0.4
mail              IN      A      192.168.0.5
```

Et ajouter un point après soa.formation.lab à la ligne 4, en redémarrant le serveur bind l'erreur n'est plus là :

```
root@soa: /
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
28-Dec-2023 16:40:10.313 using default UDP/IPv6 port range: [32768, 60999]
28-Dec-2023 16:40:10.313 listening on IPv4 interface lo, 127.0.0.1#53
28-Dec-2023 16:40:10.313 listening on IPv4 interface eth0, 192.168.0.2#53
28-Dec-2023 16:40:10.313 generating session key for dynamic DNS
28-Dec-2023 16:40:10.313 sizing zone task pool based on 2 zones
28-Dec-2023 16:40:10.313 none:100: 'max-cache-size 90%' - setting to 7161MB (out
of 7957MB)
28-Dec-2023 16:40:10.313 set up managed keys zone for view _default, file 'manag
ed-keys.bind'
28-Dec-2023 16:40:10.313 none:100: 'max-cache-size 90%' - setting to 7161MB (out
of 7957MB)
28-Dec-2023 16:40:10.317 configuring command channel from '/etc/bind/rndc.key'
28-Dec-2023 16:40:10.317 command channel listening on 127.0.0.1#953
28-Dec-2023 16:40:10.317 configuring command channel from '/etc/bind/rndc.key'
28-Dec-2023 16:40:10.317 command channel listening on ::1#953
28-Dec-2023 16:40:10.317 not using config file logging statement for logging due
to -g option
28-Dec-2023 16:40:10.333 managed-keys-zone: loaded serial 0
28-Dec-2023 16:40:10.333 zone 0.168.192.in-addr.arpa/IN: loaded serial 200202240
1
28-Dec-2023 16:40:10.333 zone formation.lab/IN: loaded serial 2001062501
28-Dec-2023 16:40:10.333 all zones loaded
28-Dec-2023 16:40:10.333 running
```



Et depuis le poste client, avec un commande dig on peut voir que le SOA répond correctement avec l'adresse IP du site web :

```
root@client-1: /
Fichier  Édition  Affichage  Rechercher  Terminal  Aide

root@client-1:/# dig www.formation.lab

; <<>> DiG 9.16.1-Ubuntu <<>> www.formation.lab
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 758
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 245baee728cf841001000000658da51275825163c4722b9f (good)
;; QUESTION SECTION:
;www.formation.lab.                IN      A

;; ANSWER SECTION:
www.formation.lab.                86400   IN      A      192.168.0.4

;; Query time: 0 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Thu Dec 28 16:40:50 UTC 2023
;; MSG SIZE rcvd: 90
```