

Troubleshooting DNS

Situation 1

Collecte des symptômes :

Commande que j'utilise sur le client et l'output sont :

- ping www.google.com

```
root@client-1: /  
Fichier Édition Affichage Rechercher Terminal Aide  
root@client-1:/# ping www.google.com  
ping: www.google.com: Temporary failure in name resolution  
root@client-1:/#
```

- ping 0.0.0.0

```
root@client-1: /  
Fichier Édition Affichage Rechercher Terminal Aide  
root@client-1:/# ping 0.0.0.0  
PING 0.0.0.0 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.026 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.062 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.035 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.042 ms
```

Le client peut accéder à l'internet mais ne peut pas accéder aux liens par noms.

J'ai fait une trace sur wireshark, mais il n'y a pas une trace que je peux voir quand je fais un ping à google.com, alors je regarde si le client a l'adresse IP du résolveur.

- cat etc/resolv.conf

```
root@client-1: /  
Fichier Édition Affichage Rechercher Terminal Aide  
root@client-1:/# cat etc/resolv.conf  
domain formation.lab  
search formation.lab  
root@client-1:/#
```

Je regarde dans le fichier resolve.conf dans le client et je vois que le client n'a pas l'adresse IP du résolveur.

Description du problème :

Le client n'est pas connecté avec le résolveur, alors il n'est pas possible de résoudre le nom du lien.

Proposition de solution :

Une solution est d'ajouter une option dans le fichier `/etc/dhcp/dhcpd.conf` avec l'adresse IP du résolveur et redémarrer les serveurs. La ligne qu'il doit être ajouter est : « option domain-name-servers 192.168.0.1; »

Situation 2

Collecte des symptômes :

Commande que j'utilise sur le client et l'output :

- ping `www.formation.lab`

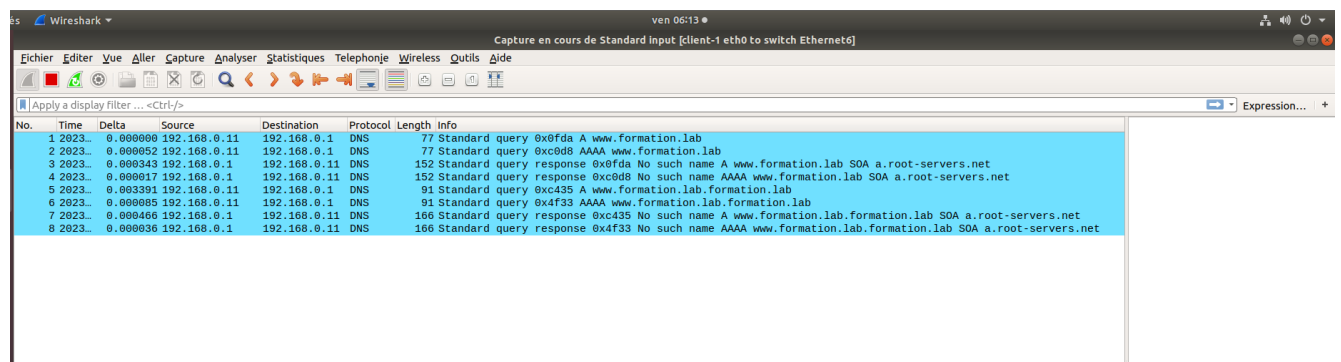
```

root@client-1: /
Fichier Édition Affichage Rechercher Terminal Aide
root@client-1:/# ping www.formation.lab
ping: www.formation.lab: Name or service not known
root@client-1:/#

```

Ici on peut voir que le ping ne s'effectue pas correctement et rend une erreur.

- Trace wireshark du ping `www.formation.lab` sur le client :



Ici on peut voir la trace wireshark du ping `www.formation.lab`.

No.	Time	Delta	Source	Destination	Protocol	Length	Info
1	2023...	0.000000	192.168.0.11	192.168.0.1	DNS	77	Standard query 0x0fda A www.formation.lab
2	2023...	0.000052	192.168.0.11	192.168.0.1	DNS	77	Standard query response 0xc0d8 AAAA www.formation.lab
3	2023...	0.000343	192.168.0.1	192.168.0.11	DNS	152	Standard query response 0x0fda No such name A www.formation.lab SOA a.root-servers.net
4	2023...	0.000017	192.168.0.1	192.168.0.11	DNS	152	Standard query response 0xc0d8 No such name AAAA www.formation.lab SOA a.root-servers.net
5	2023...	0.003391	192.168.0.11	192.168.0.1	DNS	91	Standard query 0xc435 A www.formation.lab.formation.lab
6	2023...	0.000085	192.168.0.11	192.168.0.1	DNS	91	Standard query 0x4f33 AAAA www.formation.lab.formation.lab
7	2023...	0.000466	192.168.0.1	192.168.0.11	DNS	166	Standard query response 0xc435 No such name A www.formation.lab.formation.lab SOA a.root-servers.net
8	2023...	0.000036	192.168.0.1	192.168.0.11	DNS	166	Standard query response 0x4f33 No such name AAAA www.formation.lab.formation.lab SOA a.root-servers.net
9	2023...	5.008533	f6:0b:78:48:9...	5a:42:08:5f...	ARP		
10	2023...	0.000078	5a:42:08:5f:a...	f6:0b:78:48...	ARP		
11	2023...	0.000174	f6:0b:78:48:9...	5a:42:08:5f...	ARP		
12	2023...	0.000026	5a:42:08:5f:a...	f6:0b:78:48...	ARP		
13	2023...	3.283550	c2:01:7d:b3:0...	CDP/VTP/DTP...	CDP		
14	2023...	74.961300	c2:01:7d:b3:0...	DEC-MOP-Rem...	0x6002		
15	2023...	41.307302	c2:01:7d:b3:0...	CDP/VTP/DTP...	CDP		
16	2023...	116.815...	c2:01:7d:b3:0...	CDP/VTP/DTP...	CDP		
17	2023...	116.627...	c2:01:7d:b3:0...	CDP/VTP/DTP...	CDP		

Frame 1: 77 bytes on wire (616 bits), 77 B captured (0.000000 sec on interface)

Ethernet II, Src: 5a:42:08:5f:a5:70 (5a:42:08:5f:a5:70), Dst: 02:00:00:00:00:00 (02:00:00:00:00:00)

Internet Protocol Version 4, Src: 192.168.0.11, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 60246, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x0fda

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

www.formation.lab: type A, class IN

Name: www.formation.lab

[Name Length: 17]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

[Response In: 3]

Sur la trace numéro 1 le client envoie une demande DNS au résolveur. La demande est une demande de trouver l'adresse IP du lien `www.formation.lab`.

Wireshark packet capture showing a DNS query and response. The packet list on the left shows packets 1 through 18. Packet 3 is selected, showing the details pane on the right. The details pane shows the following information:

- Frame 3: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface f6:0b:78:48:9c:91 (f6:0b:78:48:9c:91), Dst: 5a:f6:0b:78:48:9c:91, Src: 192.168.0.1, Dst Port: 60246
- Domain Name System (response)
- Transaction ID: 0x0fda
- Flags: 0x8183 Standard query response, No such name
- Questions: 1
- Answer RRs: 0
- Authority RRs: 1
- Additional RRs: 0
- Queries:
 - www.formation.lab: type A, class IN
 - Name: www.formation.lab
 - [Name Length: 17]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
- Authoritative nameservers:
 - <Root>: type SOA, class IN, mname a.root-servers.net
 - Name: <Root>
 - Type: SOA (Start Of a zone of Authority) (6)
 - Class: IN (0x0001)
 - Time to live: 10524
 - Data length: 64
 - Primary name server: a.root-servers.net
 - Responsible authority's mailbox: nstld.verisign-grs.com
 - Serial Number: 2023122900
 - Refresh Interval: 1800 (30 minutes)
 - Retry Interval: 900 (15 minutes)
 - Expire limit: 604800 (7 days)
 - Minimum TTL: 86400 (1 day)

Sur la trace numéro 3, qui est la réponse du résolveur au client, on peut voir qu'il cherche au root de trouver l'adresse IP pour ce lien mais ne trouve rien et envoie une erreur.

Description du problème :

Le résolveur envoie une requête au root server et ne fait pas un forward au SOA, qui contient l'adresse IP de l'intranet.

Proposition de solution :

Il faut ajouter une zone forward de l'intranet dans le fichier /etc/bind/named.conf dans le résolveur pour résoudre ce problème.

Dans ce cas ça doit être :

```
zone "formation.lab." IN {
    type forward;

    forwarders { 192.168.0.2; };

    forward only;
};
```

```
root@client-1:/# ping www.formation.lab
PING www.formation.lab (192.168.0.4) 56(84) bytes of data:
64 bytes from 192.168.0.4 (192.168.0.4): icmp_seq=1 ttl=64 time=0.390 ms
64 bytes from 192.168.0.4 (192.168.0.4): icmp_seq=2 ttl=64 time=0.709 ms
64 bytes from 192.168.0.4 (192.168.0.4): icmp_seq=3 ttl=64 time=0.366 ms
64 bytes from 192.168.0.4 (192.168.0.4): icmp_seq=4 ttl=64 time=0.237 ms
64 bytes from 192.168.0.4 (192.168.0.4): icmp_seq=5 ttl=64 time=0.191 ms
```

Situation 3

Collecte des symptômes :

Commande que j'utilise cette commande sur le client et l'output est :

- dig www.formation.lab

```

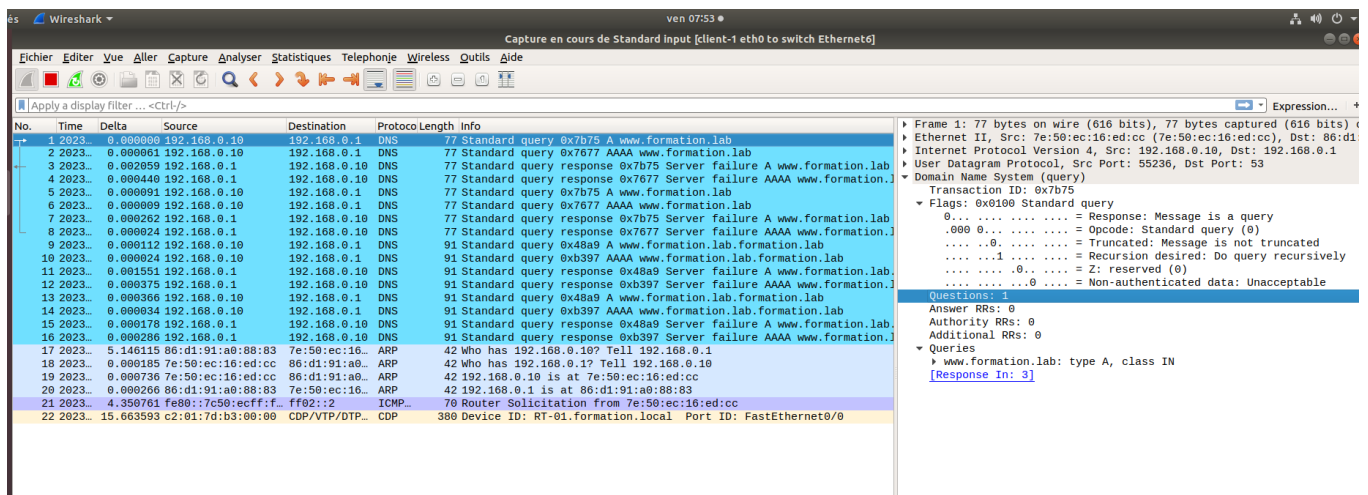
root@client-1: /

Fichier  Édition  Affichage  Recherche  Terminal  Aide

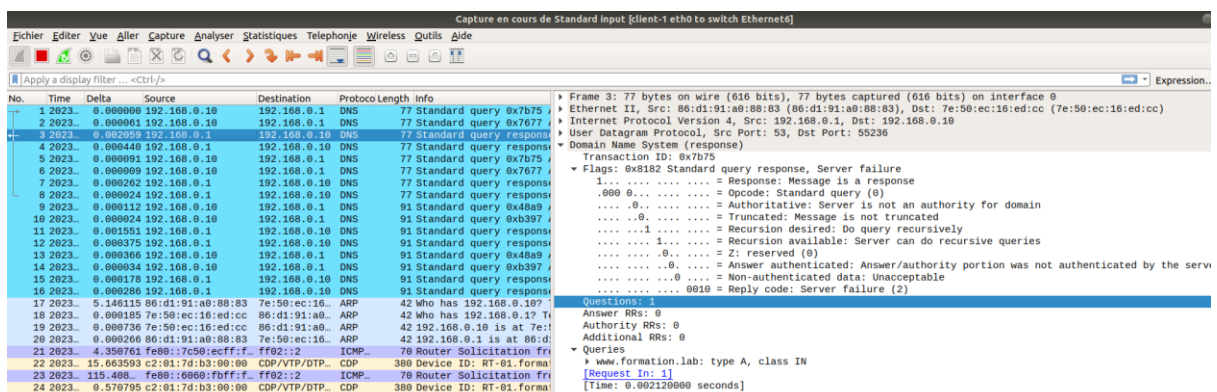
root@client-1:/# ping www.formation.lab
ping: www.formation.lab: Temporary failure in name resolution
root@client-1:/#

```

- trace wireshark du client après le ping sur www.formation.lab :



La trace numéro 1 on peut voir que le client envoie une demande DNS au resolveur et demande l'adresse IP de www.formation.lab.



La trace numéro 3 on peut voir que il y a un serveur failure, le résolveur dit que le nom n'est pas dans la liste qu'il contient.

- Trace wireshark sur le résolveur après un ping sur www.formation.lab :

Capture en cours de Standard Input [switch Ethernet1 to resolver eth0]									
No.	Time	Delta	Source	Destination	Protocol	Length	Info		
1	2023..	0.000000	192.168.0.10	192.168.0.1	DNS	77	Standard query 0x80f...		
2	2023..	0.000079	192.168.0.10	192.168.0.1	DNS	77	Standard query 0xa5f...		
3	2023..	0.000514	192.168.0.1	192.168.0.2	DNS	116	Standard query 0x342...		
4	2023..	0.000418	192.168.0.2	192.168.0.1	DNS	116	Standard query response		
5	2023..	0.000046	192.168.0.1	192.168.0.2	DNS	116	Standard query 0xa37...		
6	2023..	0.000575	192.168.0.2	192.168.0.1	DNS	116	Standard query response		
7	2023..	0.000028	192.168.0.1	192.168.0.10	DNS	77	Standard query response		
8	2023..	0.000271	192.168.0.1	192.168.0.10	DNS	77	Standard query response		
9	2023..	0.000210	192.168.0.10	192.168.0.1	DNS	77	Standard query 0x80f...		
10	2023..	0.000025	192.168.0.10	192.168.0.1	DNS	77	Standard query 0xa5f...		
11	2023..	0.000271	192.168.0.1	192.168.0.10	DNS	77	Standard query response		
12	2023..	0.000046	192.168.0.1	192.168.0.10	DNS	77	Standard query response		
13	2023..	0.000130	192.168.0.10	192.168.0.1	DNS	91	Standard query 0xe3b...		
14	2023..	0.000022	192.168.0.10	192.168.0.1	DNS	91	Standard query 0x12b...		
15	2023..	0.000468	192.168.0.1	192.168.0.2	DNS	130	Standard query 0xb0f...		
16	2023..	0.000039	192.168.0.1	192.168.0.2	DNS	130	Standard query 0x368...		
17	2023..	0.000589	192.168.0.2	192.168.0.1	DNS	130	Standard query response		
18	2023..	0.000134	192.168.0.2	192.168.0.1	DNS	130	Standard query response		
19	2023..	0.000516	192.168.0.1	192.168.0.10	DNS	91	Standard query response		
20	2023..	0.000047	192.168.0.1	192.168.0.10	DNS	91	Standard query response		
21	2023..	0.000120	192.168.0.10	192.168.0.1	DNS	91	Standard query 0xe3b...		
22	2023..	0.000013	192.168.0.10	192.168.0.1	DNS	91	Standard query 0x12b...		
23	2023..	0.000373	192.168.0.1	192.168.0.10	DNS	91	Standard query response		
24	2023..	0.000031	192.168.0.1	192.168.0.10	DNS	91	Standard query response		
25	2023..	5.215474	ca:5e:24:c5:b2:ad	86:d1:91:a0:	ARP	42	Who has 192.168.0.1?		
26	2023..	0.001071	86:d1:91:a0:88:83	ca:5e:24:c5:	ARP	42	Who has 192.168.0.2?		
27	2023..	0.000231	7e:50:ec:16:ed:cc	86:d1:91:a0:	ARP	42	Who has 192.168.0.1?		
28	2023..	0.000047	86:d1:91:a0:88:83	7e:50:ec:16:	ARP	42	Who has 192.168.0.10?		
29	2023..	0.000076	86:d1:91:a0:88:83	ca:5e:24:c5:	ARP	42	192.168.0.1 is at 86		
30	2023..	0.000048	7e:50:ec:16:ed:cc	86:d1:91:a0:	ARP	42	192.168.0.10 is at 7		

Sur la trace 3 et 4 on peut voir que le résolveur envoie une requête au SOA, mais le SOA dit qu'il ne contient pas ce nom au résolveur.

- nano /etc/bind/formation.lab sur le SOA

```

GNU nano 4.8 formation.lab
$ORIGIN formation.lab.
$TTL 1d

@      IN      SOA      soa.formation.lab      vlds.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

```

Ici on peut voir que la syntaxe du fichier formation.lab n'est pas correcte. Sur la ligne 4 il manque un point pour faire référence au root. Sur la ligne 12 le nameserver c'est seulement « soa » et pas « soa.formation.lab », car il fait référence de la ligne 15.

Description du problème :

Le SOA ne contient pas le nom correct ou syntaxe correct dans les fichiers. Le client peut accéder au internet et envoyer une requête au résolveur. Le résolveur peut aussi envoyer une requête au SOA, mais le SOA n'arrive pas à donner une solution au résolveur. Alors on doit regarder dans les fichiers du SOA. Dans le fichier /etc/etc/formation.lab on peut voir qu'il y a des problèmes syntaxe.

Proposition de solution :

Simplement appliquer les changements dans les lignes 12 et 15 dans le fichier /etc/bind/formation.lab sur le serveur SOA, que j'ai indiqué avant.

```

root@client-1:/# ping www.formation.lab
PING www.formation.lab (192.168.0.4) 56(84) bytes of data.
64 bytes from www.formation.lab (192.168.0.4): icmp_seq=1 ttl=64 time=1.22 ms
64 bytes from www.formation.lab (192.168.0.4): icmp_seq=2 ttl=64 time=0.687 ms
64 bytes from www.formation.lab (192.168.0.4): icmp_seq=3 ttl=64 time=0.483 ms
64 bytes from www.formation.lab (192.168.0.4): icmp_seq=4 ttl=64 time=0.275 ms

```