

# Troubleshooting Web

## Première situation

### Contexte :

Le site web interne de l'entreprise qui vous consulte a toujours été accessible via [www.formation.lab](http://www.formation.lab) ou bien 192.168.0.4. Malheureusement, ce site n'est plus accessible aujourd'hui.

### Collecte des symptômes :

J'essaie de démarrer le service apache2 sur le serveur web et il me rend une erreur :

- `apache2ctl start`

```
root@www: /etc/apache2
Fichier Édition Affichage Rechercher Terminal Aide
root@www:/etc/apache2# apache2ctl start
AH00534: apache2: Configuration error: No MPM loaded.
Action 'start' failed.
The Apache error log may have more information.
root@www:/etc/apache2#
```

Je dois encore créer le directory `/etc/apache2/mods-enabled` et vérifier que les modules apache2 sont activés. Les commandes que j'utilise sont :

- `mkdir /etc/apache2/mods-enabled`
- `a2enmod mpm_prefork`
- `a2enmod authz_core`
- `a2enmod dir`
- `a2enmod mime`

Après ça je démarre le service apache2 encore une fois et il ne pose plus un problème. Je le confirme avec la commande `netstat` :

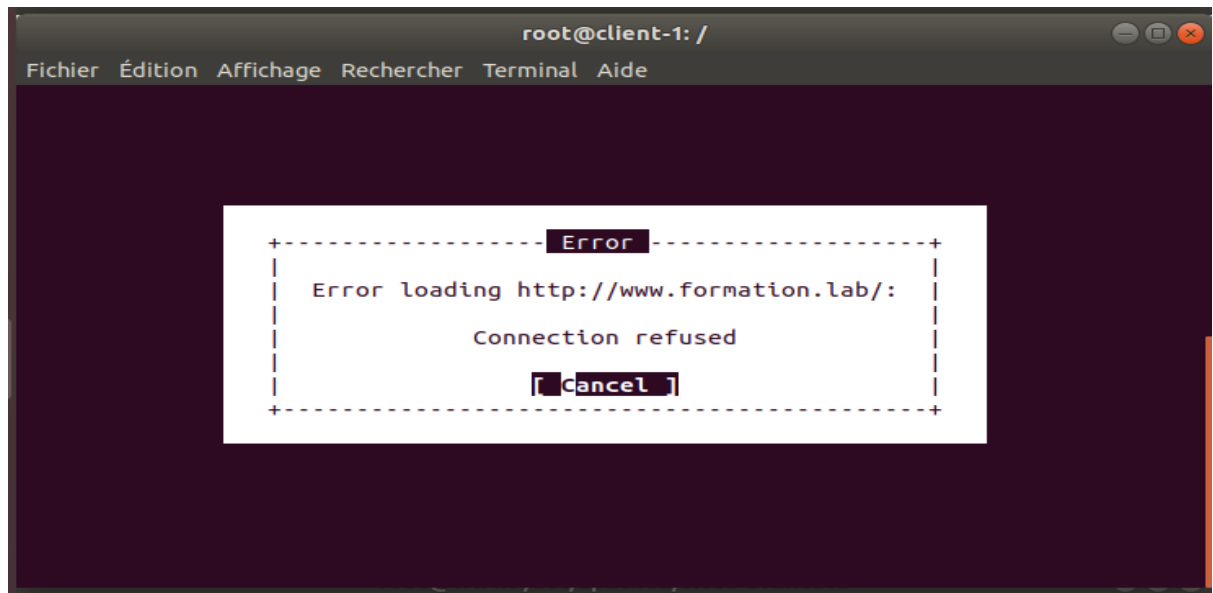
- `netstat -nltp`

```
root@www: /
Fichier Édition Affichage Rechercher Terminal Aide
root@www:/# netstat -nltp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp6      0      0 :::8080                 :::*                    LISTEN
825/apache2
root@www:/#
```

Ici on peut voir que le service apache2 est bien lancé et est placé sur le port 8080.

Sur le client j'utilise la commande pour accéder sur la page [formation.lab](http://www.formation.lab) :

- `links http://www.formation.lab`



La connexion a été refusée. Je lance une trace wireshark sur le client :

Capture en cours de Standard Input [client-1 eth0 to switch Ethernet6]						
No.	Time	Delta	Source	Destination	Protocol	Length
1	2023...	0.000000	192.168.0.16	192.168.0.1	DNS	77
2	2023...	0.000084	192.168.0.16	192.168.0.1	DNS	77
3	2023...	0.001180	192.168.0.1	192.168.0.16	DNS	93
4	2023...	0.000056	192.168.0.1	192.168.0.16	DNS	130
5	2023...	0.001469	192.168.0.16	192.168.0.4	TCP	74
6	2023...	0.000183	192.168.0.4	192.168.0.16	TCP	54
7	2023...	0.001706	192.168.0.16	192.168.0.1	DNS	77
8	2023...	0.000220	192.168.0.16	192.168.0.1	DNS	77
9	2023...	0.000696	192.168.0.1	192.168.0.16	DNS	93
10	2023...	0.000042	192.168.0.1	192.168.0.16	DNS	130
11	2023...	0.001524	192.168.0.16	192.168.0.4	TCP	74
12	2023...	0.000162	192.168.0.4	192.168.0.16	TCP	54
13	2023...	0.001698	192.168.0.16	192.168.0.1	DNS	77
14	2023...	0.000070	192.168.0.16	192.168.0.1	DNS	77
15	2023...	0.001416	192.168.0.1	192.168.0.16	DNS	93
16	2023...	0.000127	192.168.0.1	192.168.0.16	DNS	130
17	2023...	0.001862	192.168.0.16	192.168.0.4	TCP	74
18	2023...	0.000193	192.168.0.4	192.168.0.16	TCP	54

Sur la trace wireshark on peut voir que l'échange DNS fonctionne bien et le client fait une demande au serveur web, mais sur la trace numéro 6 on peut voir que la connexion est refusée. Nous allons regarder la trace numéro 6 :

Capture en cours de Standard Input [client-1 eth0 to switch Ethernet6]						
No.	Time	Delta	Source	Destination	Protocol	Length
1	2023...	0.000000	192.168.0.16	192.168.0.1	DNS	77
2	2023...	0.000084	192.168.0.16	192.168.0.1	DNS	77
3	2023...	0.001180	192.168.0.1	192.168.0.16	DNS	93
4	2023...	0.000056	192.168.0.1	192.168.0.16	DNS	130
5	2023...	0.001469	192.168.0.16	192.168.0.4	TCP	74
6	2023...	0.000183	192.168.0.4	192.168.0.16	TCP	54
7	2023...	0.001706	192.168.0.16	192.168.0.1	DNS	77
8	2023...	0.000220	192.168.0.16	192.168.0.1	DNS	77
9	2023...	0.000696	192.168.0.1	192.168.0.16	DNS	93
10	2023...	0.000042	192.168.0.1	192.168.0.16	DNS	130
11	2023...	0.001524	192.168.0.16	192.168.0.4	TCP	74
12	2023...	0.000162	192.168.0.4	192.168.0.16	TCP	54
13	2023...	0.001698	192.168.0.16	192.168.0.1	DNS	77
14	2023...	0.000070	192.168.0.16	192.168.0.1	DNS	77
15	2023...	0.001416	192.168.0.1	192.168.0.16	DNS	93
16	2023...	0.000127	192.168.0.1	192.168.0.16	DNS	130
17	2023...	0.001862	192.168.0.16	192.168.0.4	TCP	74
18	2023...	0.000193	192.168.0.4	192.168.0.16	TCP	54

Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface  
Ethernet II, Src: 86:e0:58:0f:aa:21 (86:e0:58:0f:aa:21), Dst: b6:e5:28:4f:a0:16  
Internet Protocol Version 4, Src: 192.168.0.4, Dst: 192.168.0.16  
Transmission Control Protocol, Src Port: 80, Dst Port: 57034, Seq: 1, Ack: 1, Win: 0, Len: 0  
Destination Port: 57034  
[Stream index: 0]  
[TCP Segment Len: 0]  
Sequence number: 1 (relative sequence number)  
[Next sequence number: 1 (relative sequence number)]  
Acknowledgment number: 1 (relative ack number)  
0101 ... = Header Length: 20 bytes (5)  
Flags: 0x014 (RST, ACK)  
000. .... = Reserved: Not set  
...0. .... = Nonce: Not set  
...0. .... = Congestion Window Reduced (CWR): Not set  
...0. .... = ECN-Echo: Not set  
...0. .... = Urgent: Not set  
...1. .... = Acknowledgment: Set  
...0. .... = Push: Not set  
[Expert Info (Warning/Sequence): Connection reset (RST)]  
[Connection reset (RST)]  
[Severity Level: Warning]  
[Group: Sequence]  
...0. .... = Syn: Not set  
...0. .... = Fin: Not set  
[TCP Flags: .....A.R..]  
Window size value: 0  
[Calculated window size: 0]  
[Window size scaling factor: -1 (unknown)]  
Checksum: 0x6ffdf [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0  
[SEQ/ACK analysis]  
[Timestamps]

Ici on peut voir que la demande utilise le protocole TCP, car c'est pour un lien d'une site web. Le port par défaut que le TCP utilise est le port 80. Le flag RST a été utilisé pour terminer la connexion immédiatement.

### Description du problème :

La connexion est refusée car le port que le service apache utilise est le port 8080, ce ça qu'on a vu avec la commande netstat. Le port utilise par défaut pour les liens est le port 80, alors la connection est refusée. Dans le fichier /etc/apache2/apache2.conf on peut voir que le Listen est sur 8080.

### Proposition de solution :

Changer le port du listen dans le fichier etc/apache2/apache2.conf de 8080 à 80. Maintenant c'est possible d'accéder au liens <http://www.formation.lab>.

## Deuxième situation

### Contexte :

La page d'accueil du site web interne de l'entreprise qui vous consulte a toujours été accessible depuis [www.formation.lab](http://www.formation.lab) ou encore 192.168.0.4. Aujourd'hui, ce lien ne donne plus de résultats.... Étrange car le site reste pourtant accessible via 192.168.0.4/index.html.

### Collecte des symptômes :

Ici j'avais les mêmes problèmes pour démarrer le service apache2 et je prends les mêmes étapes comme dans la première situation. Après les étapes je démarre le service apache2 et un netstat :

- `apache2ctl start`
- `netstat -ntlp`

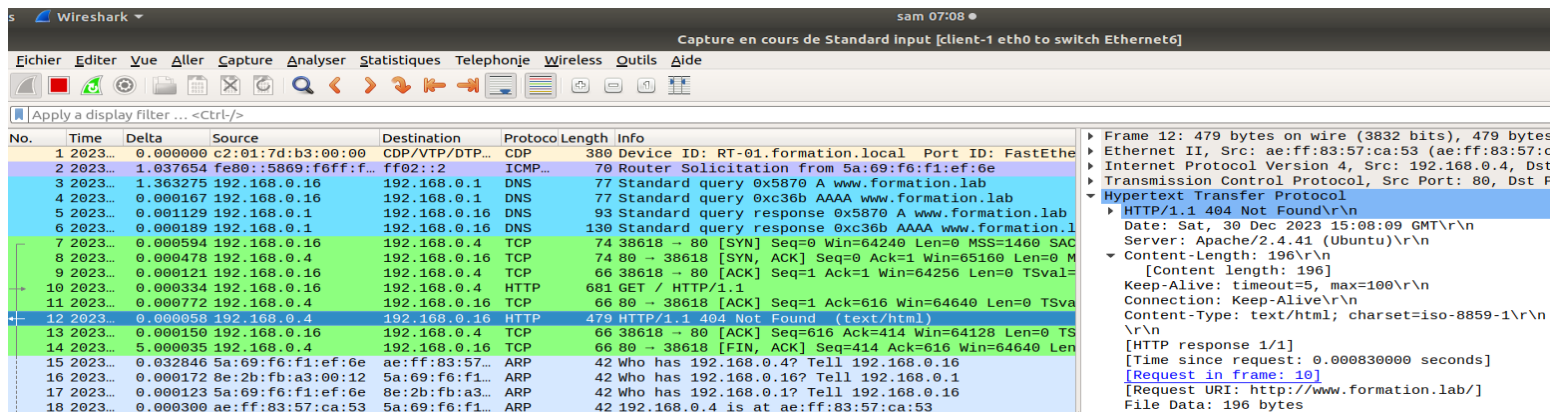
```
root@www:/# apache2ctl start
root@www:/# netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp6      0      0 :::80                  :::*                    LISTEN
819/apache2
root@www:/#
```

J'utilise la commande sur le client et il me donne cet output :

- `links http://www.formation.lab`

```
root@client-1: /
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
404 Not Found
Not Found
The requested URL was not found on this server.
```

Ici il me rend une erreur 404, qu'il dit que le lien demandé ne se trouve pas sur ce serveur. Je lance aussi une trace wireshark sur le client :



Dans la trace numéro 10 on voit bien que le client fait une demande GET au serveur web, mais la trace numéro 12 dit bien que le lien demandé n'existe pas. Je regarde dans les error logs et la dernière erreur est :

```
[Sat Dec 30 15:16:52.374727 2023] [authz_core:debug] [pid 822] mod_authz_core.c(845): [client 192.168.0.16:34850] AH01628
: authorization result: granted (no directives)
[Sat Dec 30 15:16:52.374819 2023] [core:info] [pid 822] [client 192.168.0.16:34850] AH00129: Attempt to serve directory:
/var/www/html/
root@www:/var/log/apache2#
```

Il semble qu'il y a une erreur avec la directive, alors je regarde dans le fichier de configuration de la directive dans /etc/apache2/mods-available/dir.conf :

```
root@www:/etc/apache2/mods-available
Fichier Édition Affichage Recherche Terminal Aide
GNU nano 4.8 dir.conf
<IfModule mod_dir.c>
    DirectoryIndex home.html
</IfModule>
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Ici on peut voir que le fichier attendu est bien un fichier home.html. Maintenant je regarde quel fichier se trouve dans la directive /var/www/html/ qu'on a vu dans le error log :

```
root@www:/var/www/html# ls
index.html
```

On va bien que ce soit un fichier avec le nom index.html

### Description du problème :

L'erreur se forme parce que le nom du DirectoryIndex est « home.html », mais le fichier, que le serveur a, est nommé index.html, ça fait que le service apache peut montrer le page web <http://www.formation.lab/index.html>, mais pas <http://www.formation.lab>.

### Proposition de solution :

Une solution est de changer dans /etc/apache2/mods-available/dir.conf le home.html à index.html.