

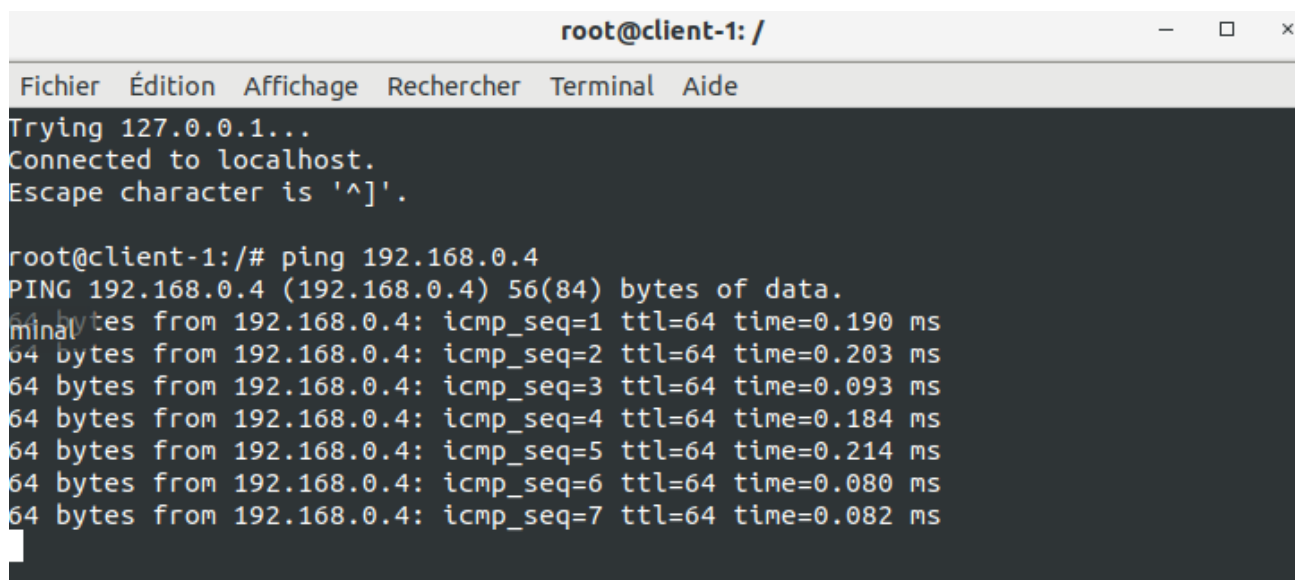
Troubleshooting Web

Situation 1 :

Symptôme : Le site web interne de l'entreprise qui vous consulte a toujours été accessible via www.formation.lab ou bien 192.168.0.4. Malheureusement, ce site n'est plus accessible aujourd'hui. Pourriez-vous jeter un coup d'œil afin de trouver une solution au problème?

Collecte des symptômes :

On commence par vérifier si le serveur www est joignable depuis un client par un ping :



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

root@client-1:/# ping 192.168.0.4
PING 192.168.0.4 (192.168.0.4) 56(84) bytes of data.
64 bytes from 192.168.0.4: icmp_seq=1 ttl=64 time=0.190 ms
64 bytes from 192.168.0.4: icmp_seq=2 ttl=64 time=0.203 ms
64 bytes from 192.168.0.4: icmp_seq=3 ttl=64 time=0.093 ms
64 bytes from 192.168.0.4: icmp_seq=4 ttl=64 time=0.184 ms
64 bytes from 192.168.0.4: icmp_seq=5 ttl=64 time=0.214 ms
64 bytes from 192.168.0.4: icmp_seq=6 ttl=64 time=0.080 ms
64 bytes from 192.168.0.4: icmp_seq=7 ttl=64 time=0.082 ms
```

Il marche, le problème n'est pas là. On essaye ensuite d'accéder au site avec le navigateur links, tout en faisant une capture Wireshark entre le client et le switch :



La connexion est refusée.

No.	Time	Delta	Source	Destination	Protocol	Length	Info
1	2023-12-29 13:34:46,478813	0.000000	192.168.0.17	192.168.0.1	DNS	77	Standard query 0xfecf A www.formation.lab
2	2023-12-29 13:34:46,478858	0.000045	192.168.0.17	192.168.0.1	DNS	77	Standard query 0x85f7 AAAA www.formation.lab
3	2023-12-29 13:34:46,479034	0.000176	192.168.0.1	192.168.0.17	DNS	93	Standard query response 0xfecf A www.formation.lab A 192.168.0.4
4	2023-12-29 13:34:46,479060	0.000026	192.168.0.1	192.168.0.17	DNS	130	Standard query response 0x85f7 AAAA www.formation.lab SOA soa.formation.lab
5	2023-12-29 13:34:46,479238	0.000178	192.168.0.17	192.168.0.4	TCP	74	32944 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=730730652 TSecr=730730653
6	2023-12-29 13:34:46,479301	0.000063	192.168.0.4	192.168.0.17	TCP	54	80 → 32944 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	2023-12-29 13:34:46,479845	0.000544	192.168.0.17	192.168.0.1	DNS	77	Standard query 0xe1fa A www.formation.lab
8	2023-12-29 13:34:46,479871	0.000026	192.168.0.17	192.168.0.1	DNS	77	Standard query 0xc6c2 AAAA www.formation.lab
9	2023-12-29 13:34:46,480040	0.000169	192.168.0.1	192.168.0.17	DNS	93	Standard query response 0xe1fa A www.formation.lab A 192.168.0.4
10	2023-12-29 13:34:46,480061	0.000021	192.168.0.1	192.168.0.17	DNS	130	Standard query response 0xc6c2 AAAA www.formation.lab SOA soa.formation.lab
11	2023-12-29 13:34:46,480187	0.000126	192.168.0.17	192.168.0.4	TCP	74	32946 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=730730653 TSecr=730730654
12	2023-12-29 13:34:46,480264	0.000077	192.168.0.4	192.168.0.17	TCP	54	80 → 32946 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	2023-12-29 13:34:46,480810	0.000546	192.168.0.17	192.168.0.1	DNS	77	Standard query 0xd21d A www.formation.lab
14	2023-12-29 13:34:46,480841	0.000031	192.168.0.17	192.168.0.1	DNS	77	Standard query 0x7816 AAAA www.formation.lab
15	2023-12-29 13:34:46,480933	0.000092	192.168.0.1	192.168.0.17	DNS	93	Standard query response 0xd21d A www.formation.lab A 192.168.0.4
16	2023-12-29 13:34:46,480956	0.000023	192.168.0.1	192.168.0.17	DNS	130	Standard query response 0x7816 AAAA www.formation.lab SOA soa.formation.lab
17	2023-12-29 13:34:46,481061	0.000105	192.168.0.17	192.168.0.4	TCP	74	32956 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=730730654 TSecr=730730655
18	2023-12-29 13:34:46,481131	0.000070	192.168.0.4	192.168.0.17	TCP	54	80 → 32956 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Avec Wireshark on voit que le DNS marche (les trames en bleu) et donne bien l’adresse du serveur web, mais la connexion TCP ne marche pas et le navigateur réessaye plusieurs fois.

No.	Time	Delta	Source	Destination	Protocol	Length	Info
1	2023-12-29 13:34:46,478813	0.000000	192.168.0.17	192.168.0.1	DNS	77	Standard query 0xfecf A www.formation.lab
2	2023-12-29 13:34:46,478858	0.000045	192.168.0.17	192.168.0.1	DNS	77	Standard query 0x85f7 AAAA www.formation.lab
3	2023-12-29 13:34:46,479034	0.000176	192.168.0.1	192.168.0.17	DNS	93	Standard query response 0xfecf A www.formation.lab A 192.168.0.4
4	2023-12-29 13:34:46,479060	0.000026	192.168.0.1	192.168.0.17	DNS	130	Standard query response 0x85f7 AAAA www.formation.lab SOA soa.formation.lab
5	2023-12-29 13:34:46,479238	0.000178	192.168.0.17	192.168.0.4	TCP	74	32944 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=730730652 TSecr=730730653
6	2023-12-29 13:34:46,479301	0.000063	192.168.0.4	192.168.0.17	TCP	54	80 → 32944 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	2023-12-29 13:34:46,479845	0.000544	192.168.0.17	192.168.0.1	DNS	77	Standard query 0xe1fa A www.formation.lab
8	2023-12-29 13:34:46,479871	0.000026	192.168.0.17	192.168.0.1	DNS	77	Standard query 0xc6c2 AAAA www.formation.lab
9	2023-12-29 13:34:46,480040	0.000169	192.168.0.1	192.168.0.17	DNS	93	Standard query response 0xe1fa A www.formation.lab A 192.168.0.4
10	2023-12-29 13:34:46,480061	0.000021	192.168.0.1	192.168.0.17	DNS	130	Standard query response 0xc6c2 AAAA www.formation.lab SOA soa.formation.lab
11	2023-12-29 13:34:46,480187	0.000126	192.168.0.17	192.168.0.4	TCP	74	32946 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=730730653 TSecr=730730654
12	2023-12-29 13:34:46,480264	0.000077	192.168.0.4	192.168.0.17	TCP	54	80 → 32946 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	2023-12-29 13:34:46,480810	0.000546	192.168.0.17	192.168.0.1	DNS	77	Standard query 0xd21d A www.formation.lab
14	2023-12-29 13:34:46,480841	0.000031	192.168.0.17	192.168.0.1	DNS	77	Standard query 0x7816 AAAA www.formation.lab
15	2023-12-29 13:34:46,480933	0.000092	192.168.0.1	192.168.0.17	DNS	93	Standard query response 0xd21d A www.formation.lab A 192.168.0.4
16	2023-12-29 13:34:46,480956	0.000023	192.168.0.1	192.168.0.17	DNS	130	Standard query response 0x7816 AAAA www.formation.lab SOA soa.formation.lab
17	2023-12-29 13:34:46,481061	0.000105	192.168.0.17	192.168.0.4	TCP	74	32956 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=730730654 TSecr=730730655
18	2023-12-29 13:34:46,481131	0.000070	192.168.0.4	192.168.0.17	TCP	54	80 → 32956 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	2023-12-29 13:34:51,656786	5.175655	8a:02:1e:15:f0...	9a:79:bd:94...	ARP	42	Request for 192.168.0.17
20	2023-12-29 13:34:51,656819	0.000033	3e:59:ff:03:a8...	9a:79:bd:94...	ARP	42	Response for 192.168.0.17
21	2023-12-29 13:34:51,656823	0.000004	9a:79:bd:94:2d...	3e:59:ff:03...	ARP	42	Request for 192.168.0.17
22	2023-12-29 13:34:51,656832	0.000009	9a:79:bd:94:2d...	8a:02:1e:15...	ARP	42	Response for 192.168.0.17
23	2023-12-29 13:34:51,656865	0.000033	3e:59:ff:03:a8...	9a:79:bd:94...	ARP	42	Request for 192.168.0.17
24	2023-12-29 13:34:51,656983	0.000118	8a:02:1e:15:f0...	9a:79:bd:94...	ARP	42	Response for 192.168.0.17
25	2023-12-29 13:34:51,657000	0.000017	9a:79:bd:94:2d...	8a:02:1e:15...	ARP	42	Request for 192.168.0.17
26	2023-12-29 13:34:51,657007	0.000007	9a:79:bd:94:2d...	3e:59:ff:03...	ARP	42	Response for 192.168.0.17
27	2023-12-29 13:36:08,942182	77.285175	c2:01:7d:b3:00...	CDP/VTP/DTP...	CDP	371	CDP packet

Les réponses TCP du serveur (ligne 6 par exemple) ont le flag ‘Reset’ activé, ce qui veut dire que le serveur met fin à l’échange sans qu’il soit fini.

On va voir du côté serveur sur la machine www, dans le fichier de configuration d’apache /etc/apache2/apache2.conf :

```

root@www: /etc/apache2

Fichier  Édition  Affichage  Rechercher  Terminal  Aide

GNU nano 4.8  apache2.conf

Listen 8080
ServerName www.formation.lab

IncludeOptional mods-enabled/*.load
IncludeOptional mods-enabled/*.conf

#
# Dynamic shared object (DSO) support
#
# To be able to use the functionality of a module which was built as a
# DSO you have to place corresponding 'LoadModule' lines at this location so the
# dynamic shared object is loaded at runtime
# Note: The module name should be 'a module name' not just 'module name'
#
# LoadModule modules

#
# Uncomment and use the following line if you want to use the functionality
# of a module which is built as a DSO but that has been temporarily
# disabled for debugging reasons (by using DebugModule to load the module)
#
# LoadModule debugmodule

#
# Worker threads
#
# To be able to use the functionality of a module which was built as a
# DSO you have to place corresponding 'LoadModule' lines at this location so the
# dynamic shared object is loaded at runtime
# Note: The module name should be 'a module name' not just 'module name'
#
# LoadModule modules

#
# Uncomment and use the following line if you want to use the functionality
# of a module which is built as a DSO but that has been temporarily
# disabled for debugging reasons (by using DebugModule to load the module)
#
# LoadModule debugmodule

#
# Error log
#
ErrorLog /var/log/apache2/error.log

#
# Log format
#
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
CustomLog /var/log/apache2/access.log combined

#
# LogLevel
#
LogLevel debug

```

Le problème :

La première ligne du fichier de configuration fait écouter le serveur apache sur le port 8080. Links par défaut envoie les requêtes sur le port 80, et donc la connexion est refusée.

Solution :

Il faut changer la configuration d'apache pour qu'il écoute sur le port 80. La première ligne devient 'Listen 80'. Après redémarrer apache, le site web marche à nouveau depuis les deux clients :

```
root@client-1: /

Fichier  Édition  Affichage  Rechercher  Terminal  Aide

Apache2 Ubuntu Default Page: It works (p1 of 4)
Ubuntu Logo Apache2 Ubuntu Default Page
It works!
reshark

This is the default welcome page used to test the correct operation of the
Apache2 server after installation on Ubuntu systems. It is based on the
equivalent page on Debian, from which the Ubuntu Apache packaging is
derived. If you can read this page, it means that the Apache HTTP server
installed at this site is working properly. You should replace this file
(located at /var/www/html/index.html) before continuing to operate your
HTTP server.

If you are a normal user of this web site and don't know what this page is
about, this probably means that the site is currently unavailable due to
maintenance. If the problem persists, please contact the site's
administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream
default configuration, and split into several files optimized for
interaction with Ubuntu tools. The configuration system is fully
documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for
Image http://www.formation.lab/icons/ubuntu-logo.png
```

Et l'échange TCP ce passe maintenant bien. On voit la requête GET http du client ligne 8 et que la réponse du serveur ligne 17 a un statut 200 (OK) et un type MIME text/html :

No.	Time	Delta	Source	Destination	Protocol	Length	Info
1	2023-12-29 13:40:43,994177	0.000000	192.168.0.17	192.168.0.1	DNS	77	Standard query 0x21b9 A www.formation.lab
2	2023-12-29 13:40:43,994210	0.000033	192.168.0.17	192.168.0.1	DNS	77	Standard query 0xecb8 AAAA www.formation.lab
3	2023-12-29 13:40:43,994401	0.000191	192.168.0.1	192.168.0.17	DNS	93	Standard query response 0x21b9 A www.formation.lab A 192.168.0.4
4	2023-12-29 13:40:43,994425	0.000024	192.168.0.1	192.168.0.17	DNS	130	Standard query response 0xecb8 AAAA www.formation.lab SOA soa.formation.lab
5	2023-12-29 13:40:43,996750	0.002325	192.168.0.17	192.168.0.4	TCP	74	64904 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=731088167 ...
6	2023-12-29 13:40:43,999025	0.002275	192.168.0.4	192.168.0.17	TCP	74	80 → 64904 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=...
7	2023-12-29 13:40:43,999132	0.000107	192.168.0.17	192.168.0.4	TCP	66	64904 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=731088172 TSecr=3676339931
8	2023-12-29 13:40:43,999143	0.000011	192.168.0.17	192.168.0.4	HTTP	681	GET / HTTP/1.1
9	2023-12-29 13:40:43,999186	0.000043	192.168.0.4	192.168.0.17	TCP	66	80 → 64904 [ACK] Seq=1 Ack=616 Win=64640 Len=0 TSval=3676339933 TSecr=731088...
10	2023-12-29 13:40:43,999434	0.000248	192.168.0.4	192.168.0.17	TCP	1514	80 → 64904 [ACK] Seq=1 Ack=616 Win=64640 Len=1448 TSval=3676339933 TSecr=731...
11	2023-12-29 13:40:43,999443	0.000009	192.168.0.4	192.168.0.17	TCP	1514	80 → 64904 [ACK] Seq=1449 Ack=616 Win=64640 Len=1448 TSval=3676339933 TSecr=...
12	2023-12-29 13:40:43,999457	0.000014	192.168.0.4	192.168.0.17	TCP	1514	80 → 64904 [ACK] Seq=2897 Ack=616 Win=64640 Len=1448 TSval=3676339933 TSecr=...
13	2023-12-29 13:40:43,999462	0.000005	192.168.0.4	192.168.0.17	TCP	1514	80 → 64904 [ACK] Seq=4345 Ack=616 Win=64640 Len=1448 TSval=3676339933 TSecr=...
14	2023-12-29 13:40:43,999467	0.000005	192.168.0.4	192.168.0.17	TCP	1514	80 → 64904 [PSH, ACK] Seq=5793 Ack=616 Win=64640 Len=1448 TSval=3676339933 T...
15	2023-12-29 13:40:43,999473	0.000006	192.168.0.4	192.168.0.17	TCP	1514	80 → 64904 [ACK] Seq=7241 Ack=616 Win=64640 Len=1448 TSval=3676339933 TSecr=...
16	2023-12-29 13:40:43,999478	0.000005	192.168.0.4	192.168.0.17	TCP	1514	80 → 64904 [ACK] Seq=8689 Ack=616 Win=64640 Len=1448 TSval=3676339933 TSecr=...
17	2023-12-29 13:40:43,999482	0.000004	192.168.0.4	192.168.0.17	HTTP	1136	HTTP/1.1 200 OK (text/html)
18	2023-12-29 13:40:44,000117	0.000635	192.168.0.17	192.168.0.4	TCP	66	64904 → 80 [ACK] Seq=616 Ack=1449 Win=64128 Len=0 TSval=731088172 TSecr=3676...
19	2023-12-29 13:40:44,000139	0.000022	192.168.0.17	192.168.0.4	TCP	66	64904 → 80 [ACK] Seq=616 Ack=2897 Win=64128 Len=0 TSval=731088173 TSecr=3676...
20	2023-12-29 13:40:44,000144	0.000005	192.168.0.17	192.168.0.4	TCP	66	64904 → 80 [ACK] Seq=616 Ack=4345 Win=64128 Len=0 TSval=731088173 TSecr=3676...
21	2023-12-29 13:40:44,000148	0.000004	192.168.0.17	192.168.0.4	TCP	66	64904 → 80 [ACK] Seq=616 Ack=5793 Win=64128 Len=0 TSval=731088173 TSecr=3676...
22	2023-12-29 13:40:44,000152	0.000004	192.168.0.17	192.168.0.4	TCP	66	64904 → 80 [ACK] Seq=616 Ack=7241 Win=64128 Len=0 TSval=731088173 TSecr=3676...
23	2023-12-29 13:40:44,000156	0.000004	192.168.0.17	192.168.0.4	TCP	66	64904 → 80 [ACK] Seq=616 Ack=8689 Win=64128 Len=0 TSval=731088173 TSecr=3676...
24	2023-12-29 13:40:44,000160	0.000004	192.168.0.17	192.168.0.4	TCP	66	64904 → 80 [ACK] Seq=616 Ack=10137 Win=64128 Len=0 TSval=731088173 TSecr=367...
25	2023-12-29 13:40:44,000164	0.000004	192.168.0.17	192.168.0.4	TCP	66	64904 → 80 [ACK] Seq=616 Ack=11207 Win=64128 Len=0 TSval=731088173 TSecr=367...
26	2023-12-29 13:40:49,004686	5.004522	192.168.0.4	192.168.0.17	TCP	66	80 → 64904 [FIN, ACK] Seq=11207 Ack=616 Win=64640 Len=0 TSval=3676344939 TSe...
27	2023-12-29 13:40:49,032740	0.028054	3e:59:ff:03:a8...	9a:79:bd:94...	ARP	42	Who has 192.168.0.17? Tell 192.168.0.1
28	2023-12-29 13:40:49,032781	0.000041	9a:79:bd:94:2d...	3e:59:ff:03...	ARP	42	192.168.0.17 is at 9a:79:bd:94:2d:af
29	2023-12-29 13:40:49,044977	0.012196	192.168.0.17	192.168.0.4	TCP	66	64904 → 80 [ACK] Seq=616 Ack=11208 Win=64128 Len=0 TSval=731093218 TSecr=367...
30	2023-12-29 13:40:51,851153	2.806176	192.168.0.17	192.168.0.4	TCP	66	64904 → 80 [FIN, ACK] Seq=616 Ack=11208 Win=64128 Len=0 TSval=731096024 TSec...
31	2023-12-29 13:40:51,851224	0.000071	192.168.0.4	192.168.0.17	TCP	66	80 → 64904 [ACK] Seq=11208 Ack=617 Win=64640 Len=0 TSval=3676347785 TSecr=73...

No.	Time	Delta	Source	Destination	Protocol	Length	Info
1	2023-12-29 13:40:43,994177	0.000000	192.168.0.17	192.168.0.1	DNS	77	Standard query query 0x...
2	2023-12-29 13:40:43,994210	0.000033	192.168.0.17	192.168.0.1	DNS	77	Standard query response 0x...
3	2023-12-29 13:40:43,994401	0.000191	192.168.0.1	192.168.0.17	DNS	93	Standard query query 0x...
4	2023-12-29 13:40:43,994425	0.000024	192.168.0.1	192.168.0.17	DNS	130	Standard query response 0x...
5	2023-12-29 13:40:43,996756	0.002325	192.168.0.17	192.168.0.4	TCP	74	66 46904 → 80 [RST] Seq=1010 Win=0 Len=0
6	2023-12-29 13:40:43,999025	0.002275	192.168.0.4	192.168.0.17	TCP	74	80 → 66 46904 [RST] Seq=1010 Win=0 Len=0
7	2023-12-29 13:40:43,999132	0.000107	192.168.0.17	192.168.0.4	TCP	66	66 46904 → 80 [RST] Seq=1010 Win=0 Len=0
8	2023-12-29 13:40:43,999143	0.000011	192.168.0.17	192.168.0.4	HTTP	681	GET / HTTP/1.1
9	2023-12-29 13:40:43,999186	0.000043	192.168.0.4	192.168.0.17	TCP	66	80 → 66 46904 [RST] Seq=1010 Win=0 Len=0
10	2023-12-29 13:40:43,999434	0.000248	192.168.0.4	192.168.0.17	TCP	1514	80 → 66 46904 [RST] Seq=1010 Win=0 Len=0
11	2023-12-29 13:40:43,999443	0.000009	192.168.0.4	192.168.0.17	TCP	1514	80 → 66 46904 [RST] Seq=1010 Win=0 Len=0
12	2023-12-29 13:40:43,999457	0.000014	192.168.0.4	192.168.0.17	TCP	1514	80 → 66 46904 [RST] Seq=1010 Win=0 Len=0
13	2023-12-29 13:40:43,999462	0.000005	192.168.0.4	192.168.0.17	TCP	1514	80 → 66 46904 [RST] Seq=1010 Win=0 Len=0
14	2023-12-29 13:40:43,999467	0.000005	192.168.0.4	192.168.0.17	TCP	1514	80 → 66 46904 [RST] Seq=1010 Win=0 Len=0
15	2023-12-29 13:40:43,999473	0.000006	192.168.0.4	192.168.0.17	TCP	1514	80 → 66 46904 [RST] Seq=1010 Win=0 Len=0
16	2023-12-29 13:40:43,999478	0.000005	192.168.0.4	192.168.0.17	TCP	1514	80 → 66 46904 [RST] Seq=1010 Win=0 Len=0
17	2023-12-29 13:40:43,999482	0.000004	192.168.0.4	192.168.0.17	HTTP	1136	HTTP/1.1 200 OK
18	2023-12-29 13:40:44,000117	0.000635	192.168.0.17	192.168.0.4	TCP	66	66 46904 → 80 [RST] Seq=1010 Win=0 Len=0
19	2023-12-29 13:40:44,000139	0.000022	192.168.0.17	192.168.0.4	TCP	66	66 46904 → 80 [RST] Seq=1010 Win=0 Len=0
20	2023-12-29 13:40:44,000144	0.000005	192.168.0.17	192.168.0.4	TCP	66	66 46904 → 80 [RST] Seq=1010 Win=0 Len=0
21	2023-12-29 13:40:44,000148	0.000004	192.168.0.17	192.168.0.4	TCP	66	66 46904 → 80 [RST] Seq=1010 Win=0 Len=0
22	2023-12-29 13:40:44,000152	0.000004	192.168.0.17	192.168.0.4	TCP	66	66 46904 → 80 [RST] Seq=1010 Win=0 Len=0
23	2023-12-29 13:40:44,000156	0.000004	192.168.0.17	192.168.0.4	TCP	66	66 46904 → 80 [RST] Seq=1010 Win=0 Len=0
24	2023-12-29 13:40:44,000160	0.000004	192.168.0.17	192.168.0.4	TCP	66	66 46904 → 80 [RST] Seq=1010 Win=0 Len=0
25	2023-12-29 13:40:44,000164	0.000004	192.168.0.17	192.168.0.4	TCP	66	66 46904 → 80 [RST] Seq=1010 Win=0 Len=0
26	2023-12-29 13:40:49,004686	5.004522	192.168.0.4	192.168.0.17	TCP	66	80 → 66 46904 [RST] Seq=1010 Win=0 Len=0
27	2023-12-29 13:40:49,032740	0.028054	3e:59:ff:03:a8...	9a:79:bd:94...	ARP	42	Who has 192.168.0.1?
28	2023-12-29 13:40:49,032781	0.000041	9a:79:bd:94:2d...	3e:59:ff:03:a8...	ARP	42	192.168.0.1
29	2023-12-29 13:40:49,044977	0.012196	192.168.0.17	192.168.0.4	TCP	66	66 46904 → 80 [RST] Seq=1010 Win=0 Len=0
30	2023-12-29 13:40:51,851153	2.806176	192.168.0.17	192.168.0.4	TCP	66	66 46904 → 80 [RST] Seq=1010 Win=0 Len=0
31	2023-12-29 13:40:51,851224	0.000071	192.168.0.4	192.168.0.17	TCP	66	80 → 66 46904 [RST] Seq=1010 Win=0 Len=0

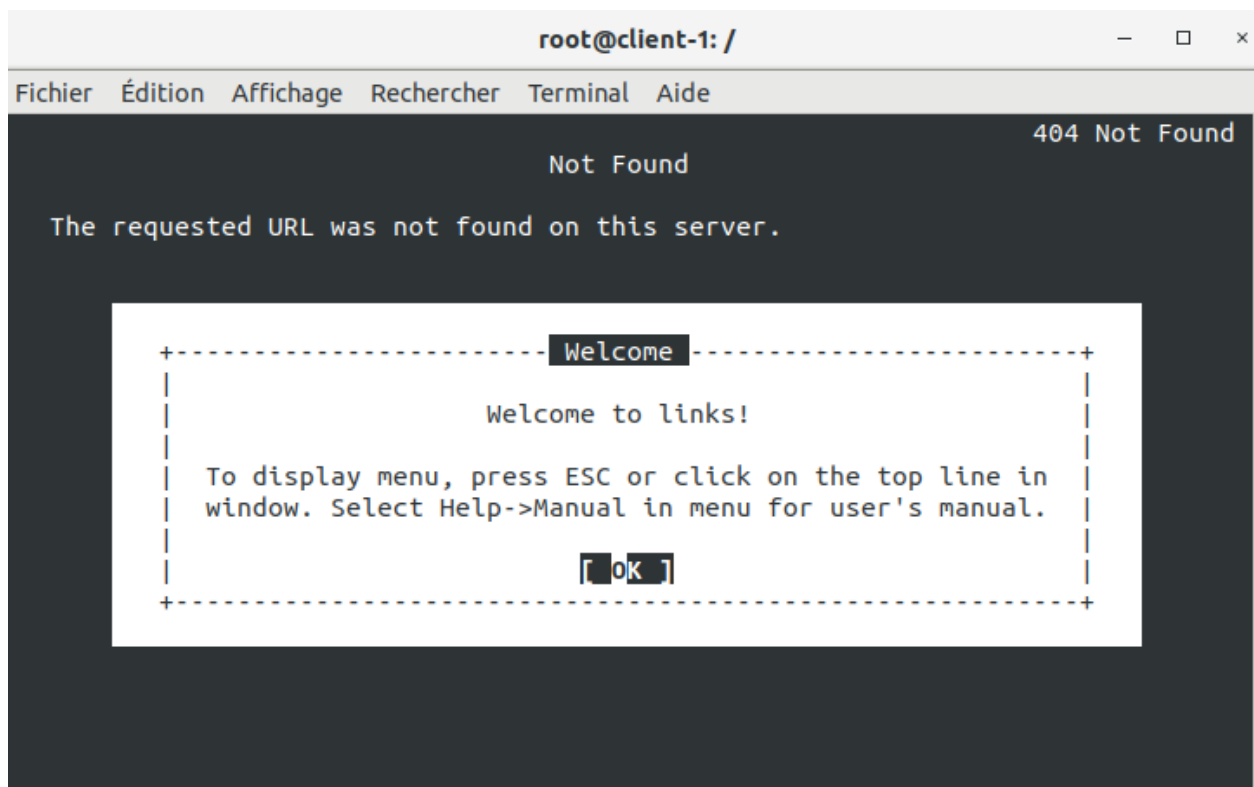
Les réponses TCP du serveur n'ont plus le flag 'Reset'.

Situation 2 :

Symptôme : La page d'accueil du site web interne de l'entreprise qui vous consulte a toujours été accessible depuis 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. Qu'a-t-il pu se passer ?

Collecte de Symptômes :

On essaye d'accéder au site depuis client-1 avec links <http://www.formation.lab> :



Le serveur renvoie un code d'erreur 404 (Not found). Cela veut dire que le serveur apache ne trouve pas la page à afficher.

On voit le même code d'erreur 404 dans la capture Wireshark, dans la réponse du serveur ligne 10 :

No.	Time	Delta	Source	Destination	Protocol	Length	Info
1	2023-12-29 14:17:19,133475	0.000000	192.168.0.16	192.168.0.1	DNS	77	Standard query 0xae20 A www.formation.lab
2	2023-12-29 14:17:19,133659	0.000184	192.168.0.1	192.168.0.16	DNS	93	Standard query response 0xae20 A www.formation.lab
3	2023-12-29 14:17:19,133669	0.000010	192.168.0.16	192.168.0.1	DNS	77	Standard query 0x6724 AAAA www.formation.lab
4	2023-12-29 14:17:19,134125	0.000456	192.168.0.1	192.168.0.16	DNS	130	Standard query response 0x6724 AAAA www.formation.lab
5	2023-12-29 14:17:19,134233	0.000108	192.168.0.16	192.168.0.4	TCP	74	57460 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
6	2023-12-29 14:17:19,134311	0.000078	192.168.0.4	192.168.0.16	TCP	74	80 → 57460 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
7	2023-12-29 14:17:19,134341	0.000030	192.168.0.16	192.168.0.4	TCP	66	57460 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
8	2023-12-29 14:17:19,134461	0.000120	192.168.0.16	192.168.0.4	HTTP	681	GET / HTTP/1.1
9	2023-12-29 14:17:19,134523	0.000062	192.168.0.4	192.168.0.16	TCP	66	80 → 57460 [ACK] Seq=1 Ack=616 Win=64640 Len=0 TS
10	2023-12-29 14:17:19,134725	0.000202	192.168.0.4	192.168.0.16	HTTP	479	HTTP/1.1 404 Not Found (text/html)
11	2023-12-29 14:17:19,134768	0.000043	192.168.0.16	192.168.0.4	TCP	66	57460 → 80 [ACK] Seq=616 Ack=414 Win=64128 Len=0
12	2023-12-29 14:17:24,135481	5.000713	192.168.0.4	192.168.0.16	TCP	66	80 → 57460 [FIN, ACK] Seq=414 Ack=616 Win=64640 L
13	2023-12-29 14:17:24,176741	0.041260	192.168.0.16	192.168.0.4	TCP	66	57460 → 80 [ACK] Seq=616 Ack=415 Win=64128 Len=0
14	2023-12-29 14:17:24,232821	0.056080	fa:59:84:e5:3a...	e2:14:2a:8d...	ARP	42	Who has 192.168.0.16? Tell 192.168.0.1
15	2023-12-29 14:17:24,232849	0.000028	e2:14:2a:8d:86...	fa:59:84:e5...	ARP	42	Who has 192.168.0.1? Tell 192.168.0.16
16	2023-12-29 14:17:24,232897	0.000048	e2:14:2a:8d:86...	02:6a:74:0f...	ARP	42	Who has 192.168.0.4? Tell 192.168.0.16
17	2023-12-29 14:17:24,232906	0.000009	e2:14:2a:8d:86...	fa:59:84:e5...	ARP	42	192.168.0.16 is at e2:14:2a:8d:86:3e
18	2023-12-29 14:17:24,232911	0.000005	fa:59:84:e5:3a...	e2:14:2a:8d...	ARP	42	192.168.0.1 is at fa:59:84:e5:3a:71
19	2023-12-29 14:17:24,232948	0.000037	02:6a:74:0f:6c...	e2:14:2a:8d...	ARP	42	192.168.0.4 is at 02:6a:74:0f:6c:fb
20	2023-12-29 14:17:39,136428	14.903480	192.168.0.16	192.168.0.4	TCP	66	57460 → 80 [FIN, ACK] Seq=616 Ack=415 Win=64128 L
21	2023-12-29 14:17:39,136522	0.000094	192.168.0.4	192.168.0.16	TCP	66	80 → 57460 [ACK] Seq=415 Ack=617 Win=64640 Len=0

Comme dit dans l'énoncé, le site marche si on utilise l'url <http://192.168.0.4/index.html>. C'est aussi le cas avec <http://www.formation.lab/index.html>. Le problème vient bien du serveur apache.

Dans le fichier /var/log/apache2/error.log du serveur, on ne voit que le chemin vers le dossier html est correct, mais on ne trouve pas la source de l'erreur :

```
root@www: /var/log/apache2
Fichier Édition Affichage Rechercher Terminal Aide
GNU nano 4.8 error.log
[Fri Dec 29 22:15:15.907896 2023] [watchdog:debug] [pid 875] mod_watchdog.c(452): AH010033: Watchdog: Running with WatchdogInterval 1000ms
[Fri Dec 29 22:15:15.907919 2023] [watchdog:debug] [pid 875] mod_watchdog.c(461): AH02974: Watchdog: found parent providers.
[Fri Dec 29 22:15:15.907922 2023] [watchdog:debug] [pid 875] mod_watchdog.c(507): AH02977: Watchdog: found child providers.
[Fri Dec 29 22:15:15.907923 2023] [watchdog:debug] [pid 875] mod_watchdog.c(515): AH02978: Watchdog: Looking for child (_singleton_).
[Fri Dec 29 22:15:15.907925 2023] [watchdog:debug] [pid 875] mod_watchdog.c(515): AH02978: Watchdog: Looking for child (_default_).
[Fri Dec 29 22:15:15.908279 2023] [unixd:alert] [pid 876] AH02155: getpuid: couldn't determine user name from uid 4294967295, you probably need to modify the User directive
[Fri Dec 29 22:15:15.908295 2023] [watchdog:debug] [pid 876] mod_watchdog.c(566): AH02980: Watchdog: nothing configured?
[Fri Dec 29 22:15:15.908302 2023] [mpm_prefork:notice] [pid 875] AH00163: Apache/2.4.41 (Ubuntu) configured -- resuming normal operations
[Fri Dec 29 22:15:15.908307 2023] [mpm_prefork:info] [pid 875] AH00164: Server built: 2021-09-28T22:28:10
[Fri Dec 29 22:15:15.908310 2023] [core:notice] [pid 875] AH00094: Command line: '/usr/sbin/apache2'
[Fri Dec 29 22:15:15.908312 2023] [core:debug] [pid 875] log.c(1568): AH02639: Using SO_REUSEPORT: yes (1)
[Fri Dec 29 22:15:15.908314 2023] [mpm_prefork:debug] [pid 875] prefork.c(914): AH00165: Accept mutex: none (default: sysvsem)
[Fri Dec 29 22:15:15.908317 2023] [unixd:alert] [pid 877] AH02155: getpuid: couldn't determine user name from uid 4294967295, you probably need to modify the User directive
[Fri Dec 29 22:15:15.908333 2023] [watchdog:debug] [pid 877] mod_watchdog.c(566): AH02980: Watchdog: nothing configured?
[Fri Dec 29 22:15:15.908453 2023] [unixd:alert] [pid 878] AH02155: getpuid: couldn't determine user name from uid 4294967295, you probably need to modify the User directive
[Fri Dec 29 22:15:15.908463 2023] [unixd:alert] [pid 879] AH02155: getpuid: couldn't determine user name from uid 4294967295, you probably need to modify the User directive
[Fri Dec 29 22:15:15.908474 2023] [watchdog:debug] [pid 879] mod_watchdog.c(566): AH02980: Watchdog: nothing configured?
[Fri Dec 29 22:15:15.908474 2023] [watchdog:debug] [pid 878] mod_watchdog.c(566): AH02980: Watchdog: nothing configured?
[Fri Dec 29 22:15:15.908496 2023] [unixd:alert] [pid 880] AH02155: getpuid: couldn't determine user name from uid 4294967295, you probably need to modify the User directive
[Fri Dec 29 22:15:15.908507 2023] [watchdog:debug] [pid 880] mod_watchdog.c(566): AH02980: Watchdog: nothing configured?
[Fri Dec 29 22:17:19.134635 2023] [authz_core:debug] [pid 876] mod_authz_core.c(845): [client 192.168.0.16:57460] AH01628: authorization result: granted (no directives)
[Fri Dec 29 22:17:19.134680 2023] [core:info] [pid 876] [client 192.168.0.16:57460] AH00129: Attempt to serve directory: /var/www/html/
[Fri Dec 29 22:17:19.167079 2023] [unixd:alert] [pid 882] AH02155: getpuid: couldn't determine user name from uid 4294967295, you probably need to modify the User directive
[Fri Dec 29 22:17:19.167112 2023] [watchdog:debug] [pid 882] mod_watchdog.c(566): AH02980: Watchdog: nothing configured?
[Fri Dec 29 22:22:10.900272 2023] [authz_core:debug] [pid 877] mod_authz_core.c(845): [client 192.168.0.16:38358] AH01628: authorization result: granted (no directives)
[Fri Dec 29 22:22:10.900310 2023] [core:info] [pid 877] [client 192.168.0.16:38358] AH00129: Attempt to serve directory: /var/www/html/
[Fri Dec 29 22:22:25.324218 2023] [authz_core:debug] [pid 879] mod_authz_core.c(845): [client 192.168.0.16:40906] AH01628: authorization result: granted (no directives)
[Fri Dec 29 22:22:33.218108 2023] [authz_core:debug] [pid 878] mod_authz_core.c(845): [client 192.168.0.16:54844] AH01628: authorization result: granted (no directives)
[Fri Dec 29 22:22:47.479081 2023] [authz_core:debug] [pid 880] mod_authz_core.c(845): [client 192.168.0.16:50122] AH01628: authorization result: granted (no directives)
[Fri Dec 29 22:22:55.673003 2023] [authz_core:debug] [pid 882] mod_authz_core.c(845): [client 192.168.0.16:46250] AH01628: authorization result: granted (no directives)
[Fri Dec 29 22:23:00.881617 2023] [authz_core:debug] [pid 876] mod_authz_core.c(845): [client 192.168.0.16:46258] AH01628: authorization result: granted (no directives)
[Fri Dec 29 22:23:04.302361 2023] [authz_core:debug] [pid 877] mod_authz_core.c(845): [client 192.168.0.16:43726] AH01628: authorization result: granted (no directives)
[Fri Dec 29 22:23:09.172546 2023] [authz_core:debug] [pid 879] mod_authz_core.c(845): [client 192.168.0.16:43728] AH01628: authorization result: granted (no directives)
```

Le problème :

Le serveur apache ne semble pas connaître le nom du fichier html à afficher.

En fait le problème se trouve dans le fichier de configuration du module dir, /etc/apache2/mods-available/dir.conf :

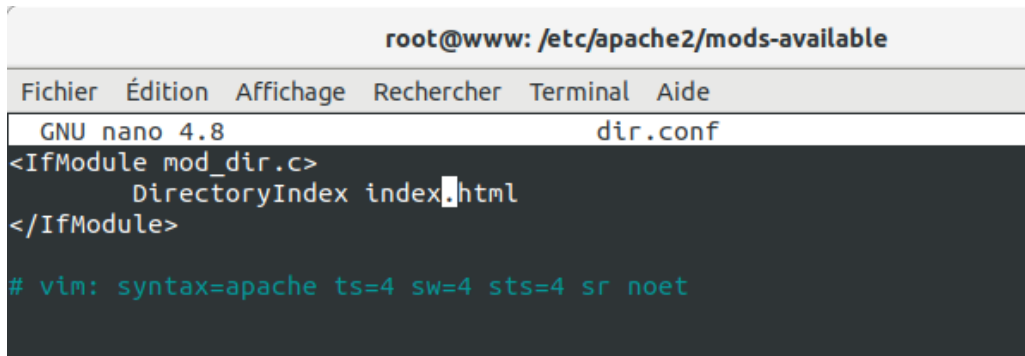
```
root@www: /etc/apache2/mods-available
Fichier Édition Affichage Rechercher Terminal Aide
GNU nano 4.8 dir.conf
<IfModule mod_dir.c>
    DirectoryIndex home.html
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Le nom de fichier par défaut configuré est home.html, mais notre page web est dans un fichier appelé index.html.

Solution :

Pour résoudre le problème on peut par exemple modifier le nom de fichier dans /var/www/html, indiquer explicitement le nom de fichier dans la configuration du site, ou changer /etc/apache2/mods-available/dir.conf pour que le nom de fichier par défaut soit index.html :



```
root@www: /etc/apache2/mods-available
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 4.8                                dir.conf
<IfModule mod_dir.c>
    DirectoryIndex index.html
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Après cette modification, le site web est accessible des deux postes clients avec links <http://www.formation.lab>.