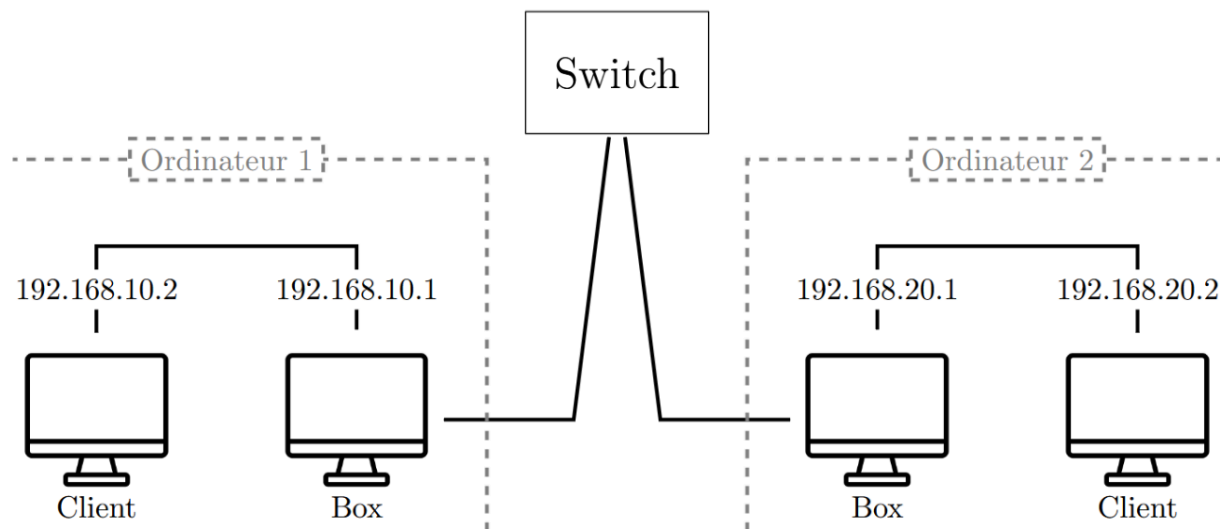


Rapport Landes Lignière - 4A STI FISA

Nous souhaitons mettre en place le réseau suivant,



Les clients doivent avoir les services suivants :

- bind9
- apache2
- nginx
- nfs
- openssh-server

Nous avons malheureusement rencontrés un problème, la salle du TP ne laisse pas les connexions en http, nous modifions donc les /etc/apt/sources.list pour utiliser les connexions https pour installer les services nécessaires.

```
GNU nano 8.4 /etc/apt/sources.list
deb cdrom:[Debian GNU/Linux 13.1.0 _Trixie_ - Official amd64 NETINST with firm
deb https://deb.debian.org/debian/ trixie main non-free-firmware
deb-src https://deb.debian.org/debian/ trixie main non-free-firmware
deb https://security.debian.org/debian-security trixie-security main non-free-f
deb-src https://security.debian.org/debian-security trixie-security main non-fr
# trixie-updates, to get updates before a point release is made;
# see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#_updates
deb https://deb.debian.org/debian/ trixie-updates main non-free-firmware
deb-src https://deb.debian.org/debian/ trixie-updates main non-free-firmware
# This system was installed using small removable media
# (e.g. netinst, live or single CD). The matching "deb cdrom"
# entries were disabled at the end of the installation process.
# For information about how to configure apt package sources,
# see the sources.list(5) manual.
```

Après cette modification et un apt update, la connexion aux miroirs de paquets est rétabli,
nous pouvons donc installer les services nécessaires.

Client - Réseau 192.168.20.0

Connexion à la boxe distante (10.10.4.1) en traversant sa boxe locale (192.168.20.1) et a bien
les services nécessaires d'installer

```
64 bytes from 10.10.4.1: icmp_seq=3 ttl=63 time=2.03 ms
64 bytes from 10.10.4.1: icmp_seq=4 ttl=63 time=2.03 ms
^C
--- 10.10.4.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 2.026/2.123/2.408/0.164 ms
root@Debian13:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:2c:1a:14 brd ff:ff:ff:ff:ff:ff
    altname enx0800272c1a14
    inet 192.168.20.2/24 brd 192.168.20.255 scope global enp0s8
        valid_lft forever preferred_lft forever
root@Debian13:~# traceroute 10.10.4.1
traceroute to 10.10.4.1 (10.10.4.1), 30 hops max, 60 byte packets
 1 192.168.20.1 (192.168.20.1)  4.371 ms  4.045 ms  3.775 ms
 2 10.10.4.1 (10.10.4.1)  3.411 ms  3.073 ms  2.862 ms
root@Debian13:~# apt policy nginx apache2 nfs-server bind9
nginx:
  Installed: 1.26.3-3+deb13u1
  Candidate: 1.26.3-3+deb13u1
  Version table:
*** 1.26.3-3+deb13u1 500
     500 http://deb.debian.org/debian trixie/main arm64 Packages
     100 /var/lib/dpkg/status
apache2:
  Installed: 2.4.65-2
  Candidate: 2.4.65-2
  Version table:
*** 2.4.65-2 500
     500 http://deb.debian.org/debian trixie/main arm64 Packages
     100 /var/lib/dpkg/status
nfs-server:
  Installed: (none)
  Candidate: (none)
  Version table:
bind9:
  Installed: 1:9.20.15-1~deb13u1
  Candidate: 1:9.20.15-1~deb13u1
  Version table:
*** 1:9.20.15-1~deb13u1 500
     500 http://deb.debian.org/debian trixie/main arm64 Packages
     500 http://security.debian.org/debian-security trixie-security/main arm64 Packages
     100 /var/lib/dpkg/status
root@Debian13:~#
```

Client - Réseau 192.168.10.0

Configuration Client 192.168.20.2

Bind9

```
//  
// Do any local configuration here  
//  
zone "Ligniere-tp.org" {  
    type master;  
    file "/etc/bind/db.ligniere-tp.local";  
    allow-update {none;};  
};
```

```
// This is the primary configuration file for the BIND DNS server named.  
//  
// Please read /usr/share/doc/bind9/README.Debian for information on the  
// structure of BIND configuration files in Debian, *BEFORE* you customize  
// this configuration file.  
//  
// If you are just adding zones, please do that in /etc/bind/named.conf.local  
  
include "/etc/bind/named.conf.options";  
include "/etc/bind/named.conf.local";  
include "/etc/bind/named.conf.root-hints";  
  
acl internal-acl {  
    192.168.20.0/24;  
};  
  
view "internal-view" {  
    match-clients { internal-acl; };  
    include "/etc/bind/named.conf.local";  
    #include "/etc/bind/named.conf.default-zones";  
};  
  
view "external-view" {  
    match-clients { any; };  
    include "/etc/bind/named.conf.external";  
    #include "/etc/bind/named.conf.default-zones";  
};
```

```
GNU nano 8.4 /etc/bind/named.conf.external
//
// Do any local configuration here
//
zone "Ligniere-tp.org" {
    type master;
    file "/etc/bind/db.ligniere-tp-external.local";
    allow-update {none;};
};

GNU nano 8.4 /etc/bind/db.ligniere-tp-external.local
; BIND data file for ligniere-tp.local
$TTL      604800
@         IN      SOA      srv-dns.ligniere-tp.local. admin.ligniere-tp.local. (
                                1          ; Serial
                                604800      ; Refresh
                                86400       ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@         IN      NS       srv-dns.ligniere-tp.local.
www       IN      A        10.10.4.2
ns        IN      A        10.10.4.2
box       IN      A        10.10.4.2
```

Le service named ne peut pas démarré suite l'erreur suivante:

```
Feb 05 11:18:01 LignLanClient named[3705]: loading configuration from '/etc/bind/named.conf'
Feb 05 11:18:01 LignLanClient named[3705]: the working directory is now '/var/cache/bind'
Feb 05 11:18:01 LignLanClient named[3705]: /etc/bind/named.conf.local:4: when using 'view' statements, all zones must be in views
Feb 05 11:18:01 LignLanClient named[3705]: loading configuration: failure
Feb 05 11:18:01 LignLanClient named[3705]: exiting (due to fatal error)
Feb 05 11:18:01 LignLanClient systemd[1]: named.service: Main process exited, code=exited, status=1/FAILURE
```

Redirection de port 80 et 53 sur Box 10.10.4.1

```
root@LignLanBox:~# iptables -A PREROUTING -t nat -i enp0s8 -p tcp --dport 80 -j DNAT --t
o-destination 192.168.20.2:80
root@LignLanBox:~# iptables -A PREROUTING -t nat -i enp0s8 -p tcp --dport 53 -j DNAT --t
o-destination 192.168.20.2:53
root@LignLanBox:~# iptables -A FORWARD -p tcp -d 192.168.20.2 --dport 80 -j ACCEPT
root@LignLanBox:~# iptables -A FORWARD -p tcp -d 192.168.20.2 --dport 53 -j ACCEPT
root@LignLanBox:~# iptables -A POSTROUTING -t nat -s 192.168.20.2 -o enp0s8 -j MASQUERAD
E
root@LignLanBox:~#
```

Apache2 - NGINX

Fichier Machine Écran Entrée Périphériques Aide

GNU nano 8.4

/etc/apache2/sites-available/clangless.conf

<VirtualHost *:7171>

ServerName backup.lign-tp.org

DocumentRoot /var/www/clangless

ErrorLog \${APACHE_LOG_DIR}/clangless_error.log

CustomLog \${APACHE_LOG_DIR}/clangless_access.log combined

<VirtualHost>

root@LignLanClient:~# a2ensite reseau.conf

perl: warning: Setting locale failed.

perl: warning: Please check that your locale settings:

LANGUAGE = (unset),

LC_ALL = (unset),

LC_CTYPE = (unset),

LC_NUMERIC = (unset),

LC_COLLATE = (unset),

LC_TIME = (unset),

LC_MESSAGES = (unset),

LC_MONETARY = (unset),

LC_ADDRESS = (unset),

LC_IDENTIFICATION = (unset),

LC_MEASUREMENT = (unset),

LC_PAPER = (unset),

LC_TELEPHONE = (unset),

LC_NAME = (unset),

LANG = "fr_FR.UTF-8"

are supported and installed on your system.

perl: warning: Falling back to the standard locale ("C").

Enabling site reseau.

To activate the new configuration, you need to run:

systemctl reload apache2

root@LignLanClient:~# a2ensite clangless.conf

perl: warning: Setting locale failed.

perl: warning: Please check that your locale settings:

LANGUAGE = (unset),

LC_ALL = (unset),

LC_CTYPE = (unset),

LC_NUMERIC = (unset),

LC_COLLATE = (unset),

LC_TIME = (unset),

LC_MESSAGES = (unset),

LC_MONETARY = (unset),

LC_ADDRESS = (unset),

LC_IDENTIFICATION = (unset),

LC_MEASUREMENT = (unset),

LC_PAPER = (unset),

LC_TELEPHONE = (unset),

LC_NAME = (unset),

LANG = "fr_FR.UTF-8"

are supported and installed on your system.

perl: warning: Falling back to the standard locale ("C").

Enabling site clangless.

```

root@LignLanClient:~# apachectl configtest
AH00557: apache2: apr_sockaddr_info_get() failed for LignLanClient
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1
Syntax OK
root@LignLanClient:~# systemctl reload apache2
root@LignLanClient:~# curl http://localhost:7070
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
  <head>
    <title>Index of /</title>
  </head>
  <body>
<h1>Index of /</h1>
    <table>
      <tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
      <tr><th colspan="5"><hr></th></tr>
      <tr><th colspan="5"><hr></th></tr>
    </table>
<address>Apache/2.4.65 (Debian) Server at localhost Port 7070</address>
</body></html>
root@LignLanClient:~# curl http://localhost:7171
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
  <head>
    <title>Index of /</title>
  </head>
  <body>
<h1>Index of /</h1>
    <table>
      <tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
      <tr><th colspan="5"><hr></th></tr>
      <tr><th colspan="5"><hr></th></tr>
    </table>
<address>Apache/2.4.65 (Debian) Server at localhost Port 7171</address>
</body></html>

```

LigLanBox [En fonction] - Oracle VirtualBox

Fichier	Machine	Écran	Entrée	Périphériques	Aide
GNU nano 8.4					/etc/hosts *
127.0.0.1		localhost			
127.0.1.1		Debian13.myguest.virtualbox.org	Debian13		
127.0.0.1		www.lign-tp.org			
127.0.0.1		backup.clandess-tp.org			
127.0.0.1		backup.lign-tp.org			
# The following lines are desirable for IPv6 capable hosts					
::1		localhost	ip6-localhost	ip6-loopback	
ff02::1		ip6-allnodes			
ff02::2		ip6-allrouters			
root@LignLanClient:~# ln -s /etc/nginx/sites-available/proxy-tp /etc/nginx/sites-enabled/					
root@LignLanClient:~# nginx -t					
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok					
nginx: configuration file /etc/nginx/nginx.conf test is successful					
root@LignLanClient:~# systemctl reload nginx					

```

Fichier  Machine  Écran  Entrée  Périphériques  Aide
GNU nano 8.4 /etc/nginx/sites-available/proxy-tp
upstream lign_backend {
    server 127.0.0.1:7070;
    server backup.clandess-tp.org backup;
}

server {
    listen 80;
    server_name www.lign-tp.org;

    location / {
        proxy_pass http://lign_backend;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
    }
}

server {
    listen 80;
    server_name backup.lign-tp.org;

    location / {
        proxy_pass http://127.0.0.1:7171;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
    }
}

root@LignLanClient:~# curl www.lign-tp.org
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of </title>
</head>
<body>
<h1>Index of </h1>
<table>
<tr><th valign="top"></th><th><a href="?C=N;0=D">Name</a></th><th><a href="?C=M;0=A">Last modified</a></th><th><a href="?C=S;0=A">Size</a></th><th><a href="?C=0;0=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.65 (Debian) Server at www.lign-tp.org Port 80</address>
</body></html>

root@LignLanClient:~# systemctl restart apache2
root@LignLanClient:~# systemctl start nginx
root@LignLanClient:~#

```

NFS

Notre chemin vers le site web est situé à /var/www/reseau, nous indiquons donc au serveur nfs de donner accès à la box, et par effet de cascade, au client distant, le droit de lecture et écriture ainsi que la synchronisation continue.

```

GNU nano 8.4 /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
/var/www/reseau 10.10.4.1(rw,sync,no_subtree_check)

```

SSH

Génération d'une clé asymétrique ssh

```
root@LignLanClient:~# ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519): networktp
Enter passphrase for "networktp" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in networktp
Your public key has been saved in networktp.pub
The key fingerprint is:
SHA256:gWIF/23ZXwkVLPXi8ly/jQVAK2+TEMd9r5Z0GG2km9A root@LignLanClient
The key's randomart image is:
+--[ED25519 256]--+
|      ...      +++Bo|
|      o .      .o=+o*|
|      o o .      o+E=+|
|      . . . o o +0++|
|      S + oo=*o|
|      .      =++.|
|      .+ o|
|      oo|
|      ...|
+-----[SHA256]-----+
root@LignLanClient:~# █
```

Création de l'utilisateur binome sur le client


```
root@LignLanClient:~# adduser binome
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
    LANGUAGE = (unset),
    LC_ALL = (unset),
    LC_CTYPE = (unset),
    LC_NUMERIC = (unset),
    LC_COLLATE = (unset),
    LC_TIME = (unset),
    LC_MESSAGES = (unset),
    LC_MONETARY = (unset),
    LC_ADDRESS = (unset),
    LC_IDENTIFICATION = (unset),
    LC_MEASUREMENT = (unset),
    LC_PAPER = (unset),
    LC_TELEPHONE = (unset),
    LC_NAME = (unset),
    LANG = "fr_FR.UTF-8"
are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for binome
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n]
root@LignLanClient:~#
```

N'ayant pas de connexion au client distant, nous ferons la manipulation de ssh-copy-id et de connexion sur l'utilisateur binome avec la machine Box1. L'utilisateur Binome a été créé au préalable.

```

root@LignLanClient:~# ssh-copy-id -i networktp binome@10.10.4.1
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "networktp.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any
that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now i
t is to install the new keys
binome@10.10.4.1's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -i ./networktp 'binome@10.10.4.1'"
and check to make sure that only the key(s) you wanted were added.

root@LignLanClient:~# ssh -i ./networktp 'binome@10.10.4.1'
Linux debian 6.12.63+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.63-1 (2025-12-30) x8
6_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
binome@debian:~$ █

```

La clé a bien été transféré et nous avons bien une connexion ssh sans utilisation de mot de passe.

Fondamentalement, nous pourrions imaginer de partager les clés à l'aide d'un fichier `authorized_keys` dans le `/home/<username>/.ssh` de tous les utilisateurs.

Ce fichier se présentant de la manière suivante pour la clé envoyé pour binome sur la box:

```

binome@debian:~$ cat .ssh/authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBEqKpkmPMGQ8N6QCu/zsfFpY5pxLGjpuwf02eqf2+ck root@LignLanClient

```

key-format key-value username@hostname

On peut facilement imaginer de la partager pour tous, avec un script pour préparer un `authorized_keys` utilisant une unique clé pour tous les utilisateurs., mais cela viendrait avec d'énormes capacités d'attaques possibles car une clé pourrait permettre d'accéder à l'intégralité des comptes en simultanée. C'est un risque bien trop important pour le mettre en place.

Configuration Client 192.168.10.2

Le deuxième client n'a pas réussi à obtenir une connexion sur la box distante malgré une masquerade et un ip forwarding actif.

Box1 -> Box2 - Fonctionnel

Box2 -> Box1 - Fonctionnel

Client2 -> Box1 - Fonctionnel

Client1 -> Box2 - Non fonctionnel

```

root@debian:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_c
    link/ether 08:00:27:dc:73:c1 brd ff:ff:ff:ff:ff:ff
    altname enx080027dc73c1
    inet 10.10.4.1/24 brd 10.10.4.255 scope global enp0s3
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc fq_codel state DOWN
    link/ether 08:00:27:49:b3:ca brd ff:ff:ff:ff:ff:ff
    altname enx08002749b3ca
root@debian:~# ping 10.10.4.2
PING 10.10.4.2 (10.10.4.2) 56(84) bytes of data.
64 bytes from 10.10.4.2: icmp_seq=1 ttl=64 time=2.78 ms
64 bytes from 10.10.4.2: icmp_seq=2 ttl=64 time=1.23 ms
^C
--- 10.10.4.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.229/2.004/2.780/0.775 ms
root@debian:~#
root@debian:~# sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
root@debian:~# iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

```

Bind9

GNU nano 8.4 /etc/bind/named.conf.local

```
//  
// Do any local configuration here  
//  
zone "liglan-tp.org" {  
    type master;  
    file "/etc/bind/db.liglan-tp.org";  
    allow-update { none };  
};  
  
acl internal-acl {  
    192.168.10.0/24;  
};  
  
view "internal-view" {  
    match-clients { internal-acl; };  
    include "/etc/bind/named.conf.local";  
    include "/etc/bind/named.conf.default-zones";  
};
```

LigLanHost1 (Lien de base pour debian et LigLanClient2) [En fon

Fichier Machine Écran Entrée Périphériques Aide

GNU nano 8.4 /etc/bind/named.conf.local

```
//  
// Do any local configuration here  
//  
zone "clandess-tp.org" {  
    type master;  
    file "etc/bind/db.clandess-tp.local";  
    allow-update { none; };  
};  
  
acl internal-acl {  
    192.168.10.0/24;  
};  
  
view "internal-view" {  
    match-clients { internal-acl; };  
    include "/etc/bind/named.conf.local";  
    include "/etc/bind/named.conf.default-zones";  
};  
  
view "external-view" {  
    match-clients { any; };  
    include "/etc/bind/named.conf.external";  
    include "/etc/bind/named.conf.default-zones";  
};_
```