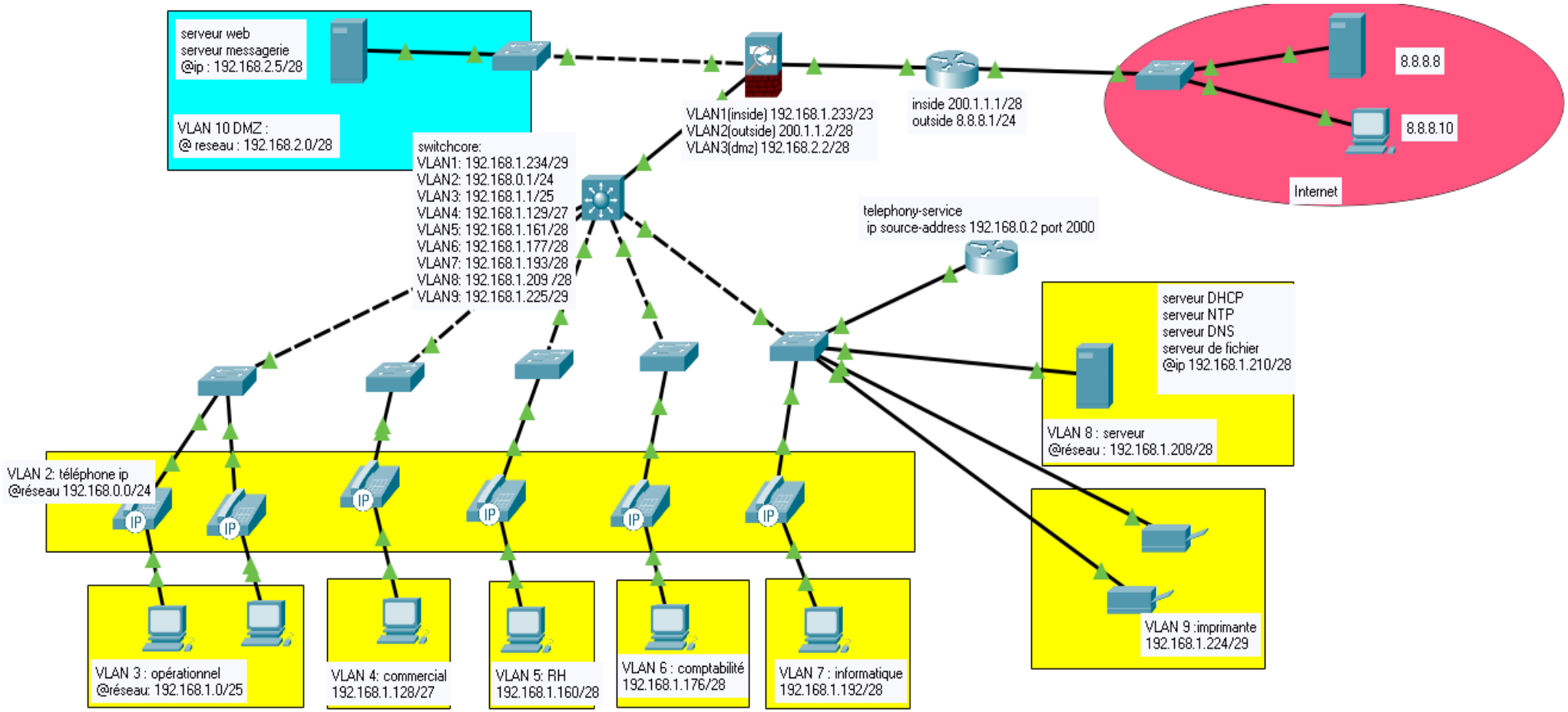
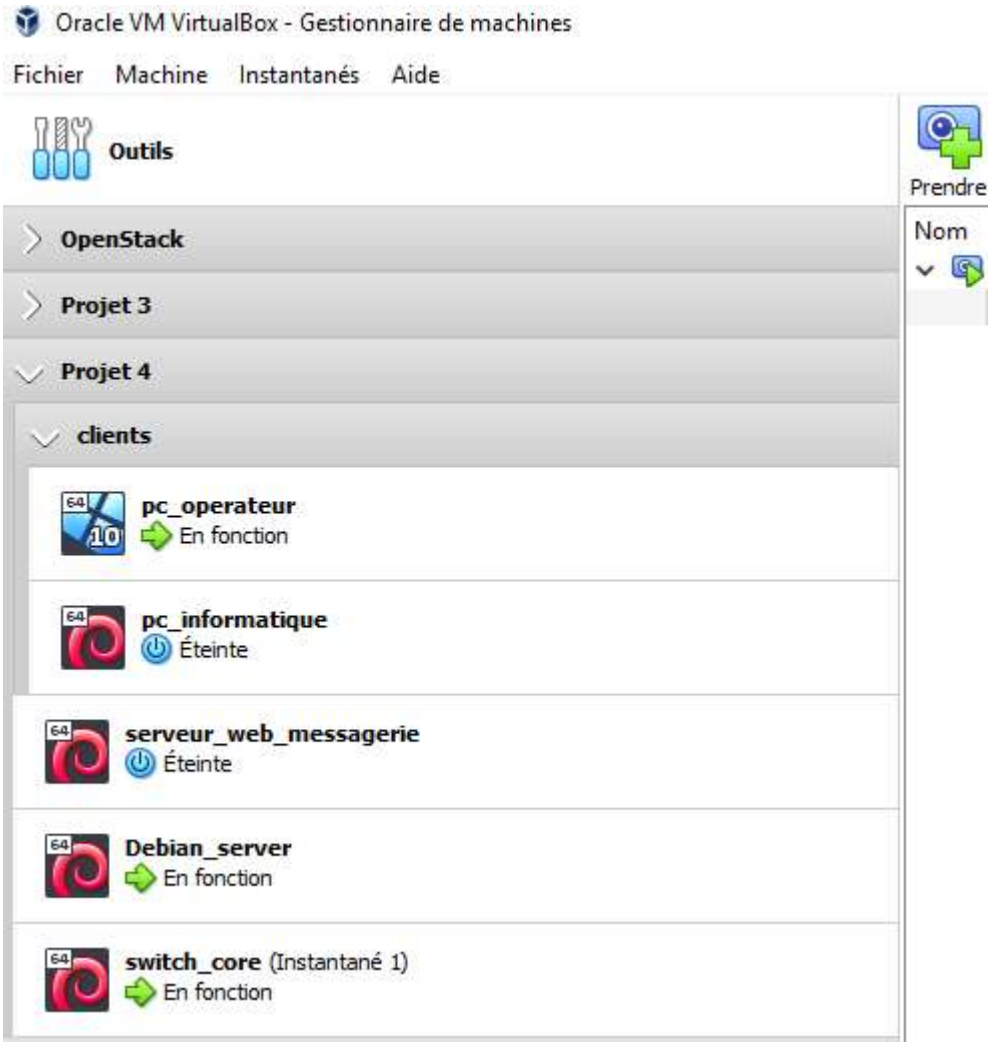
Perfectionner l'infrastructure systèmes et réseaux d'une entreprise


serveur web
serveur messagerie
@ip : 192.168.2.5/28
VLAN 10 DMZ :
@ reseau : 192.168.2.0/28
VLAN1(inside) 192.168.1.233/23
VLAN2(outside) 200.1.1.2/28
VLAN3(dmz) 192.168.2.2/28
inside 200.1.1.1/28
outside 8.8.8.1/24
8.8.8.8
8.8.8.10
Internet
switchcore:
VLAN1: 192.168.1.234/29
VLAN2: 192.168.0.1/24
VLAN3: 192.168.1.1/25
VLAN4: 192.168.1.129/27
VLAN5: 192.168.1.161/28
VLAN6: 192.168.1.177/28
VLAN7: 192.168.1.193/28
VLAN8: 192.168.1.209 /28
VLAN9: 192.168.1.225/29
telephony-service
ip source-address 192.168.0.2 port 2000
serveur DHCP
serveur NTP
serveur DNS
serveur de fichier
@ip 192.168.1.210/28
VLAN 8 : serveur
@réseau : 192.168.1.208/28
VLAN 2: téléphone ip
@réseau 192.168.0.0/24
IP
VLAN 9 :imprimante
192.168.1.224/29
VLAN 3 : opérationnel
@réseau: 192.168.1.0/25
VLAN 4: commercial
192.168.1.128/27
VLAN 5: RH
192.168.1.160/28
VLAN 6 : comptabilité
192.168.1.176/28
VLAN 7 : informatique
192.168.1.192/28

Mettre en pratique cette infrastructure :



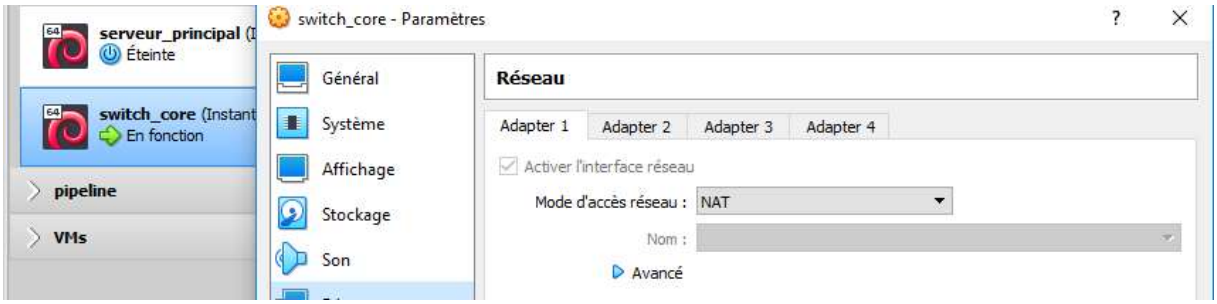
Configuration de switch_core :

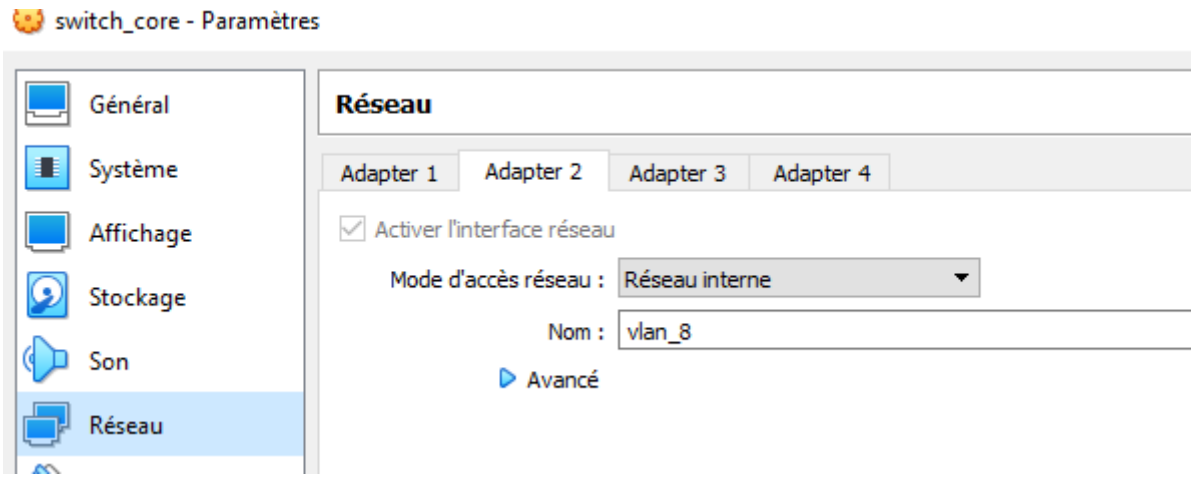
Vm debian de 1go de ram

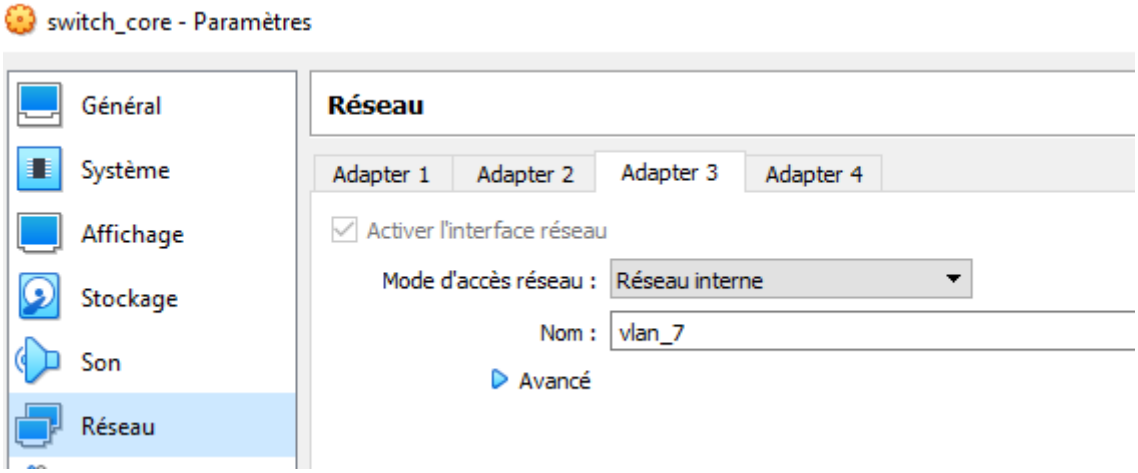
Création de 4 interfaces :

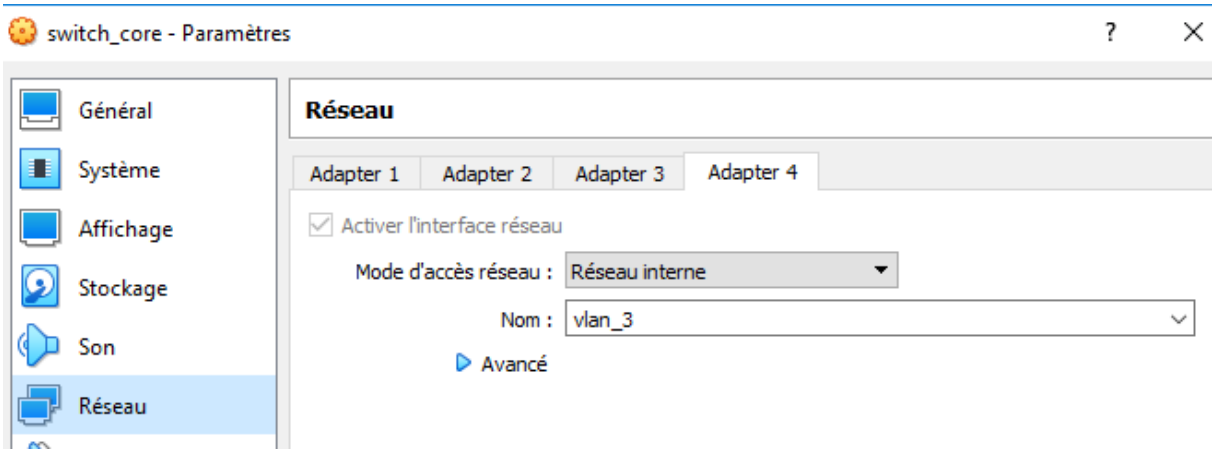
Nat pour accéder à Internet

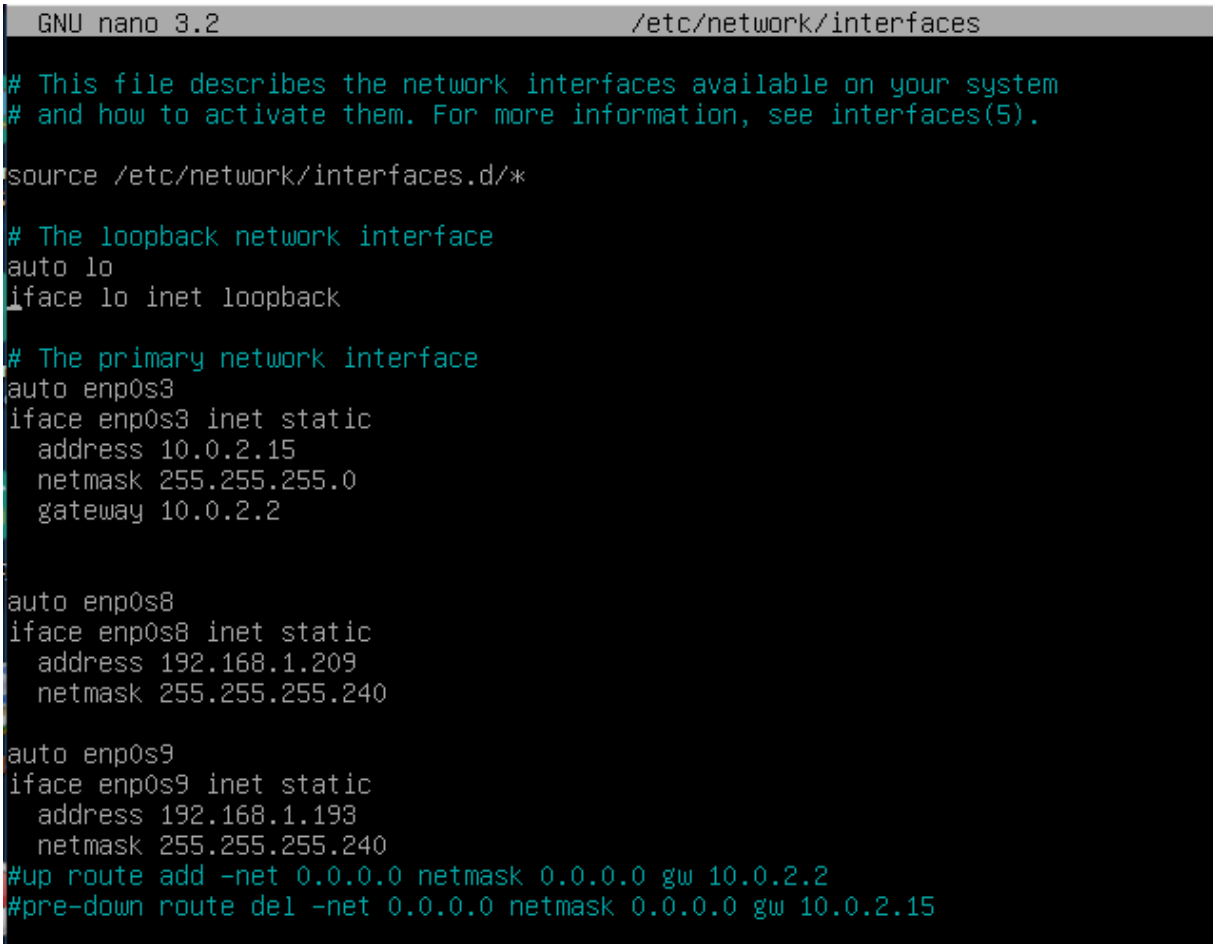
Et 3 segments internes (VLAN)

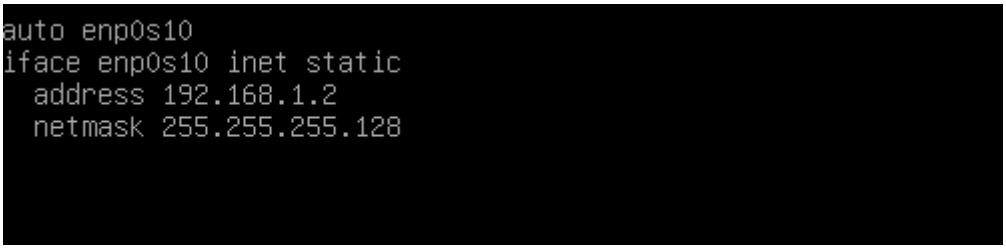



switch_core - Paramètres
Général
Système
Affichage
Stockage
Son
Réseau
Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Mode d'accès réseau :
Réseau interne
Nom :
vlan_8
Avancé


switch_core - Paramètres
Général
Système
Affichage
Stockage
Son
Réseau
Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Mode d'accès réseau :
Réseau interne
Nom :
vlan_7
Avancé


switch_core - Paramètres
Général
Système
Affichage
Stockage
Son
Réseau
Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Mode d'accès réseau :
Réseau interne
Nom :
vlan_3
Avancé





On peut ne pas rendre static pour l'interface nat (d'acces à internet) , on peut la laisser en dhcp→

auto enp0s3

Iface enp0s3 inet dhcp

systemctl restart networking

Activer le routage et le rendre permanant:

nano /etc/sysctl.conf

Eliminer # dans cette ligne :

net.ipv4.ip_forward=1

restart le service:

sudo systemctl restart procps

Lorsque je fais un ping vers internet à partir d'un pc client la trame se perd dans le réseau sans retour pour résoudre à ce problème :

Voici le lien pour cette procédure :

https://www.thomaslaurenson.com/blog/2018-07-05/building-an-ubuntu-linux-gateway/

Add a NAT forwarding rule using `iptables`:

```
sudo iptables -t nat -A POSTROUTING -o ens160 -j MASQUERADE
```

Save the `iptables` configuration:

```
sudo apt install iptables-persistent
sudo su
sudo iptables-save > /etc/iptables/rules.v4
exit
```

Installez le **Relais DHCP** :

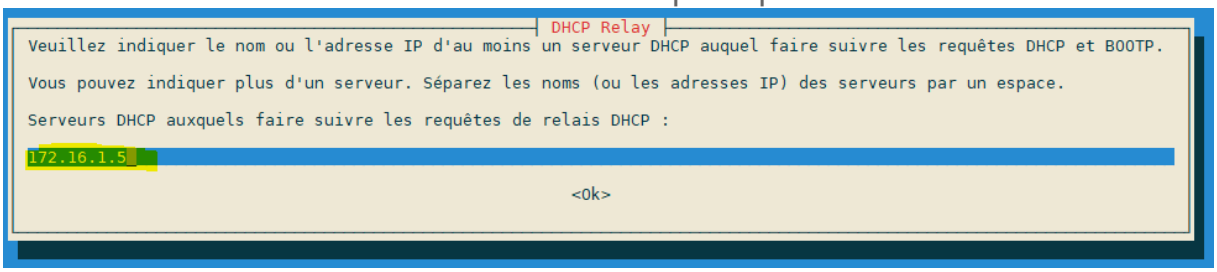
https://pixelabs.fr/dhcp-et-dhcp-relais-sous-debian-9/#Installation_DHCP_Debian-1

root@pixelabs:~# **apt install isc-dhcp-relay**

Lecture des listes de paquets... Fait

Construction de l'arbre des dépendances

- Mettez l'adresse du serveur DHCP principal. Ici c'est **Debian-1**



Serveurs DHCP auxquels faire suivre les requêtes de relais DHCP :
192.168.1.210

- Cliquez sur **Entrée**
- **Interface où le relais DHCP sera à l'écoute : Ne rien mettre**
- Cliquez sur **Entrée**

- **Option supplémentaires :** **Ne rien mettre**
- Cliquez sur **Entrée.**

I-\ Installation et Configuration du serveur DHCP

1-\ Installation du serveur DHCP sur un serveur DEBIAN 10

Installer le service :

```
apt install isc-dhcp-server
```

Sur Debian, il y a une petite spécificité, il faut indiquer dans **/etc/default/isc-dhcp-server** sur quelles interfaces va écouter le service DHCP.

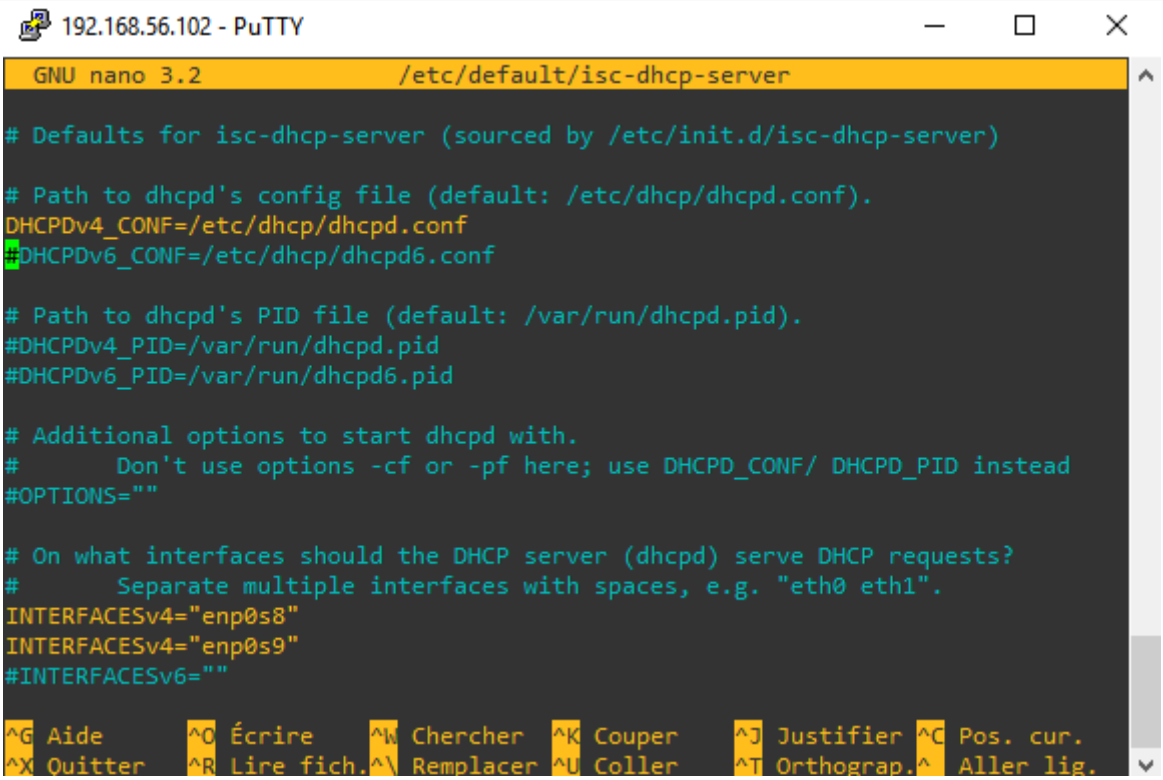
```
nano /etc/default/isc-dhcp-server
```

On décommente :

```
DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
```

Et un peu plus bas, on spécifie les interfaces d'écoute.

```
INTERFACESv4="enp23s0"
INTERFACESv6="enp23s0"
```



on lance notre DHCP:

```
systemctl start isc-dhcp-server
```

Et on ajoute le service au démarrage :

```
systemctl enable isc-dhcp-server
```

2-\ Configuration du serveur DHCP sur un serveur DEBIAN 10

Configurer le fichier /etc/dhcp/dhcpd.conf

```
option domain-name-servers 192.168.1.210, 8.8.8.8;
default-lease-time 600;
max-lease-time 7200;
ddns-update-style none;
subnet 192.168.0.0 netmask 255.255.255.0 {
        option subnet-mask 255.255.255.0;
        option routers 192.168.0.2;
        range 192.168.0.3 192.168.100.153;
}
subnet 192.168.1.128 netmask 255.255.255.224 {
        option subnet-mask 255.255.255.224;
        option routers 192.168.1.129;
        range 192.168.1.130 192.168.1.158;
}
subnet 192.168.1.160 netmask 255.255.255.240 {
        option subnet-mask 255.255.255.240;
        option routers 192.168.1.161;
        range 192.168.1.162 192.168.1.174;
}
subnet 192.168.1.176 netmask 255.255.255.240 {
        option subnet-mask 255.255.255.240;
        option routers 192.168.1.177;
        range 192.168.1.178 192.168.1.190;
}
subnet 192.168.1.192 netmask 255.255.255.240 {
        option subnet-mask 255.255.255.240;
        option routers 192.168.1.193;
        range 192.168.1.194 192.168.1.206;
}
subnet 192.168.1.208 netmask 255.255.255.240 {
        option subnet-mask 255.255.255.240;
        option routers 192.168.1.209;
        range 192.168.1.210 192.168.1.222;
}
subnet 192.168.1.224 netmask 255.255.255.248 {
        option subnet-mask 255.255.255.248;
        option routers 192.168.1.225;
        range 192.168.1.194 192.168.1.230;
}
```

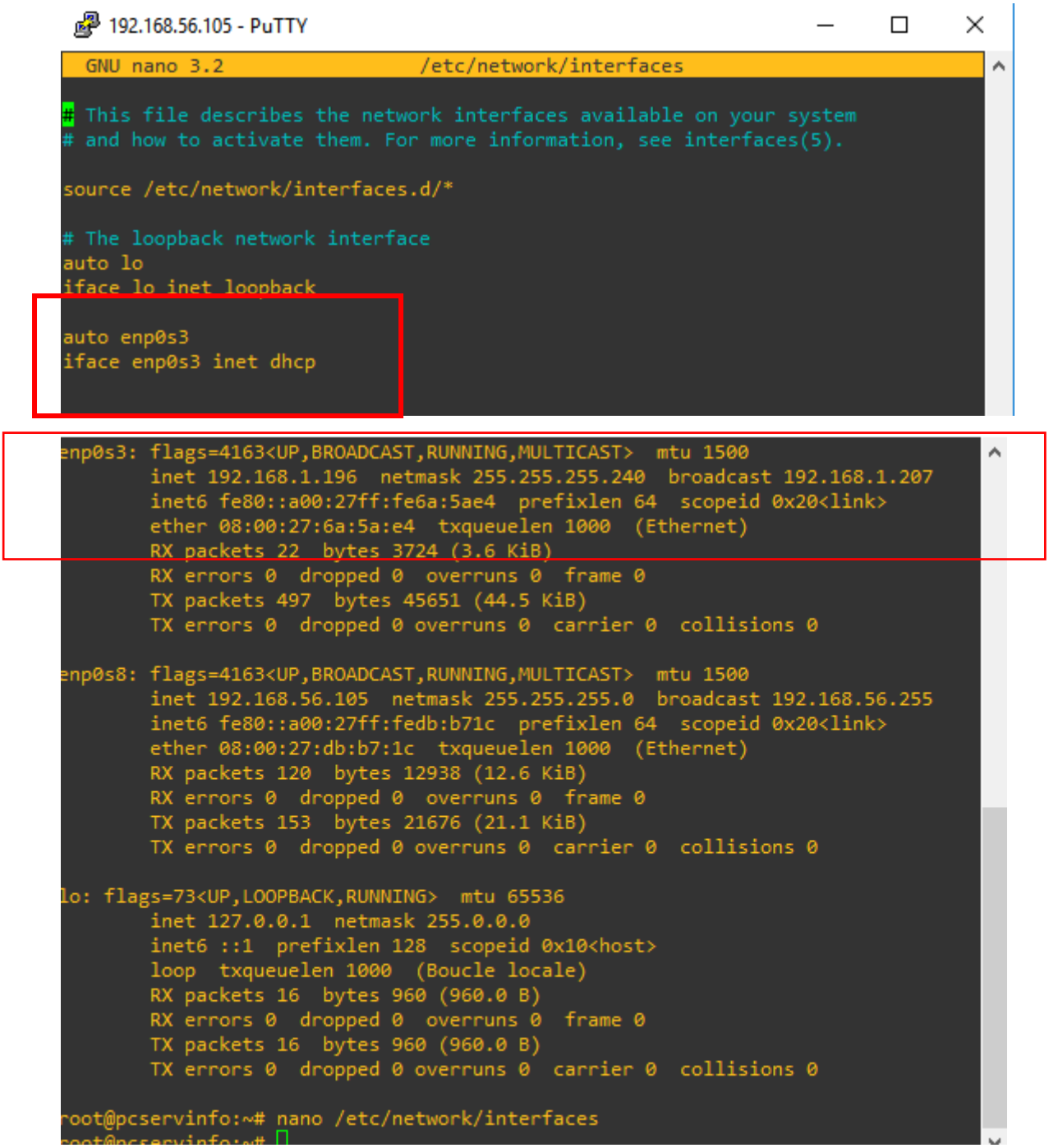
Après la modification, il faut toujours restart (dans les 2 sens serveur et client)

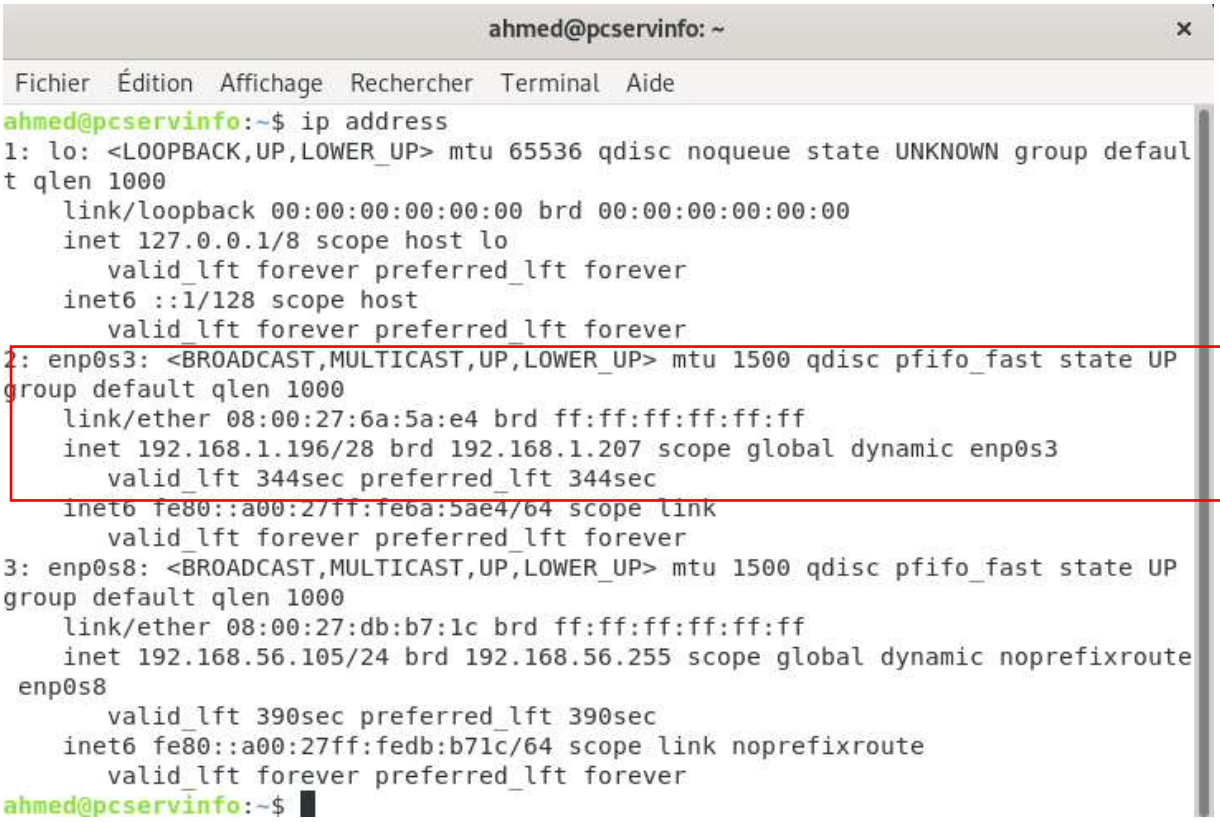
systemctl restart isc-dhcp-server

systemctl restart networking

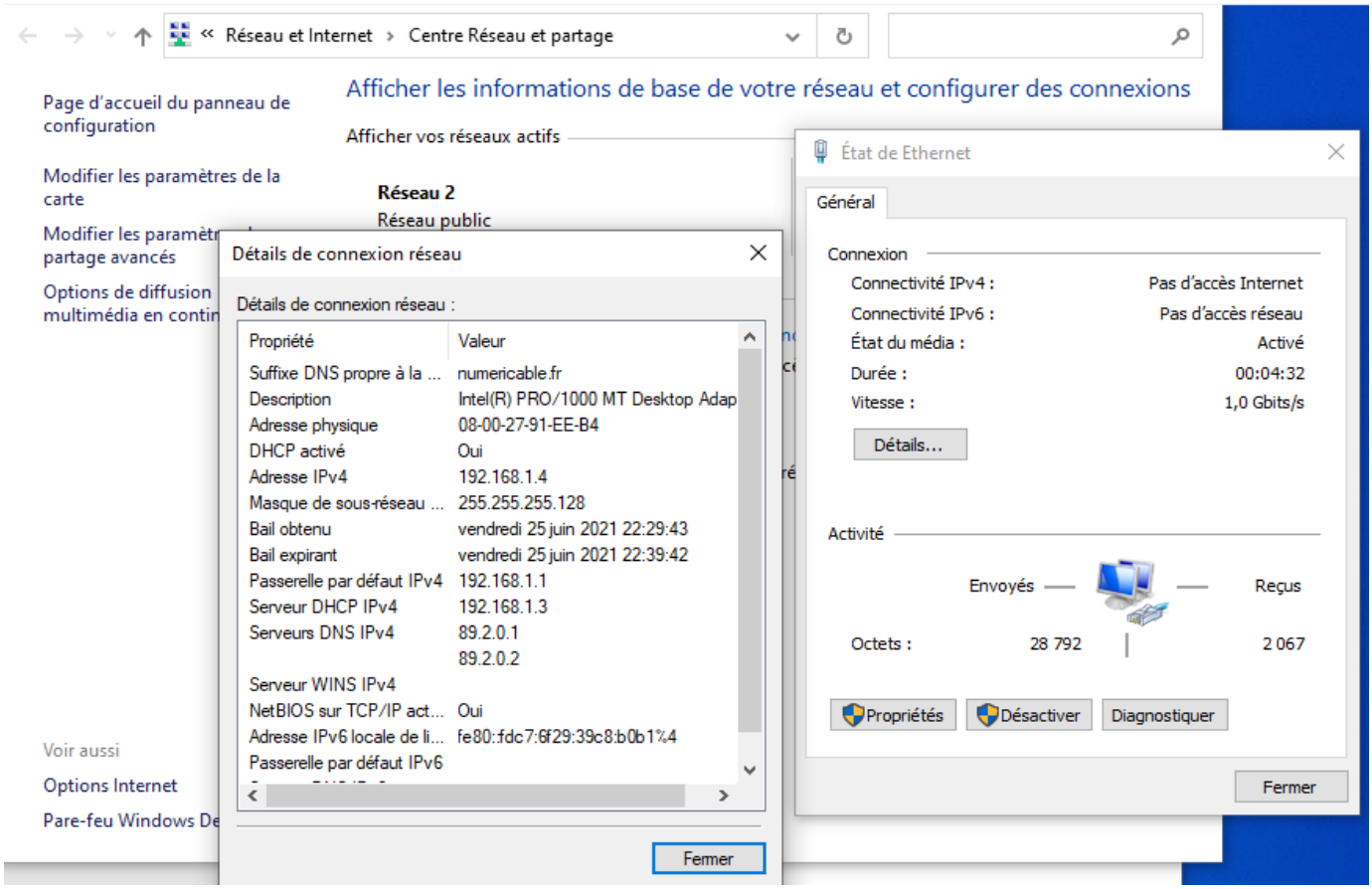
3-\ Test du service DHCP sur un poste client :

Poste Debian :




ahmed@pcservinfo: ~
Fichier Édition Affichage Rechercher Terminal Aide
ahmed@pcservinfo:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
link/ether 08:00:27:6a:5a:e4 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.196/28 brd 192.168.1.207 scope global dynamic enp0s3
valid_lft 344sec preferred_lft 344sec
inet6 fe80::a00:27ff:fe6a:5ae4/64 scope link
valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
link/ether 08:00:27:db:b7:1c brd ff:ff:ff:ff:ff:ff
inet 192.168.56.105/24 brd 192.168.56.255 scope global dynamic noprefixroute
enp0s8
valid_lft 390sec preferred_lft 390sec
inet6 fe80::a00:27ff:fedb:b71c/64 scope link noprefixroute
valid_lft forever preferred_lft forever
ahmed@pcservinfo:~$

Poste Windows :



II-\ Installation et Configuration du serv eur DNS

https://www.linuxbabe.com/debian/authoritative-dns-server-debian-10-buster-bind9

1-\ Installation du serveur DNS sur un serveur DEBIAN 10

```
sudo apt update
sudo apt install bind9 bind9utils bind9-doc
```

Check version number.

```
named -v
```

To check the version number and build options, run

```
named -V
```

By default, BIND automatically starts after installation.You check its status with:

```
systemctl status bind9
```

If it's not running, then start it with:

```
sudo systemctl start bind9
```

And enable auto start at boot time:

```
sudo systemctl enable bind9
```

2-\ Configuration du serveur DNS sur un serveur DEBIAN 10

The main BIND configuration file `/etc/bind/named.conf` sources the settings from 3 other files.

- /etc/bind/named.conf.options
- /etc/bind/named.conf.local
- /etc/bind/named.conf.default-zones

```
sudo nano /etc/bind/named.conf.options
```

Add the following lines in the options {...} clause.

```
// hide version number from clients for security reasons.
version "not currently available";

// disable recursion on authoritative DNS server.
recursion no;

// enable the query log
querylog yes;

// disallow zone transfer
allow-transfer { none; };
```

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        listen-on-v6 { any; };

        // hide version number from clients for security reasons
        version "not currently available";

        // disable recursion on authoritative DNS server
        recursion no;

        // enable the query log
        querylog yes;

        // disallow zone transfer
        allow-transfer {none; };

};
```

```
sudo systemctl restart bind9
```

I.1 - Master DNS Server Configuration

```
sudo nano /etc/bind/named.conf.local
```

Add the following lines to this file. Replace example.com with your own domain name. Replace 12.34.56.78 with the IP address of slave DNS server.

```
zone "example.com" {
        type master;
        file "/etc/bind/db.example.com";
        allow-query { any; };
        allow-transfer { 12.34.56.78; };
};
```

Debian_server [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

```
 GNU nano 3.2                          /etc/bind/named.conf.local

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization

//include "/etc/bind/zones.rfc1918";

zone "stecherif.fr" {
        type master;
        file "/etc/bind/db.stecherif.fr";
        allow-query { any; };
};
```

Instead of creating a zone file from scratch, we can use a zone template file. Copy the content of `db.empty` to a new file.

```
sudo cp /etc/bind/db.empty /etc/bind/db.example.com
```

cp /etc/bind/db.empty /etc/bind/db.steabc.fr

By default, it looks like this:

```
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    86400
@       IN      SOA     localhost. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
```

You can change it to this instead.

nano /etc/bind/db.steabc.fr

Debian_server [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

```
 GNU nano 3.2                              /etc/bind/db.stecherif.fr

; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    86400
$ORIGIN stecherif.fr.

@       IN      SOA     server1.stecherif.fr. root.stecherif.fr. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;

@       IN      NS      server1.stecherif.fr.
server1 IN      A       192.168.1.210
```

Editer ou remplacer le nom de la machine

nano /etc/hostname

192.168.56.102 - PuTTY

```
 GNU nano 3.2                              /etc/hostname

server1
```

Affecter l'addresse ip au nom du host

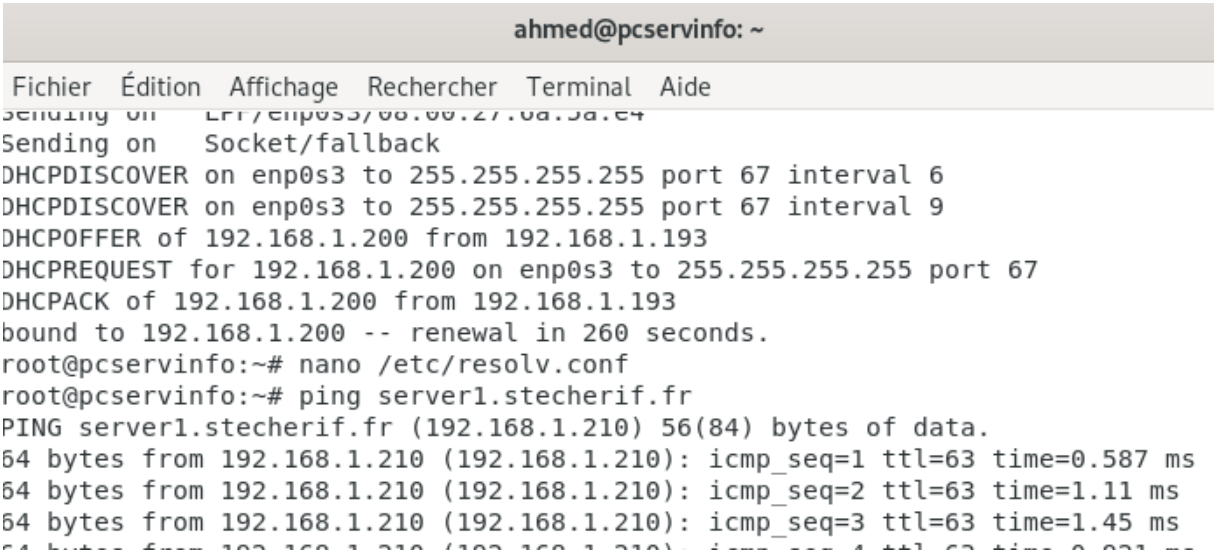
Debian_server [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

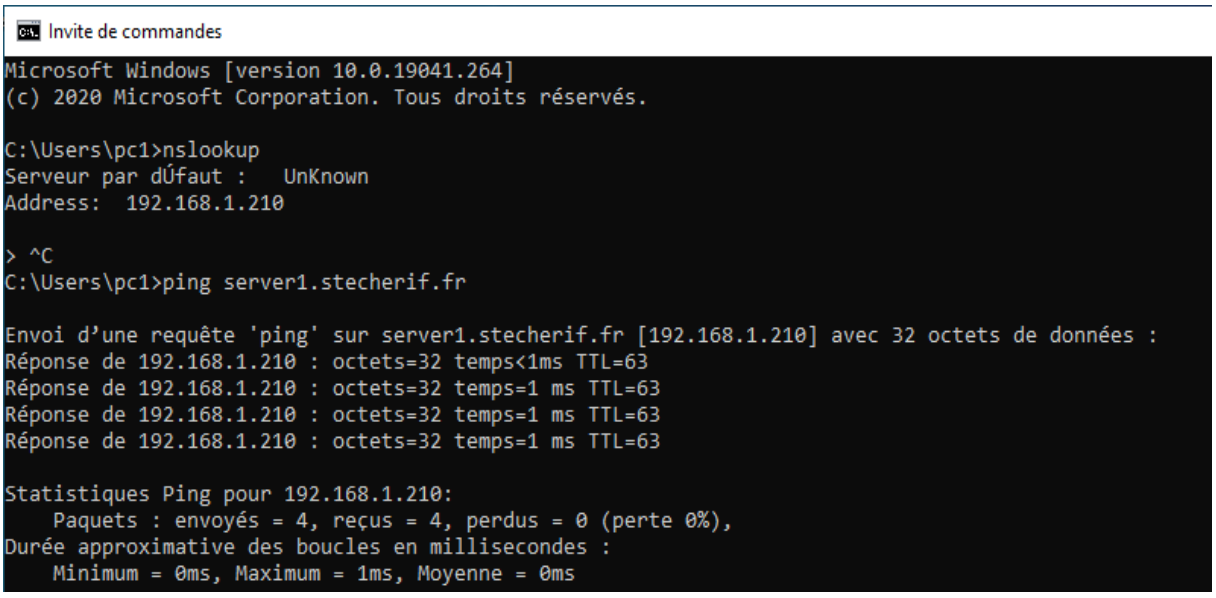
```
 GNU nano 3.2                                        /etc/hosts

127.0.0.1       localhost
127.0.1.1       server1

192.168.1.210   server1.stecherif.fr

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

3-\ Test du service DNS sur un poste client :

Poste linux (Debian)



Poste Windows 10



III-\ Installation et Configuration du serveur NTP

1-\ Installation du serveur NTP sur un serveur DEBIAN 10

https://openclassrooms.com/fr/courses/1733551-gerez-votre-serveur-linux-et-ses-services/5236031-configurez-un-serveur-de-temps-pour-etre-toujours-a-l-heure

```
$ sudo apt-get install chrony
```

```
Nano /etc/chrony/chrony.conf
```

Add the following lines :

Allow 192.168.0.0/23

```
$ sudo systemctl enable chrony
$ sudo systemctl start chrony
```

```
$ sudo timedatectl set-ntp false
```

2-\ Configuration du service NTP sur un client DEBIAN 10

http://perso.univ-lemans.fr/~emicoul/Documentations/Linux/outils_syst/Timesyncd.html

1 - Retirer les services ntp (et ntpdate)

```
systemctl stop ntp.service
systemctl disable ntp.service
systemctl status ntp.service
```

2 - Configurer timesyncd pour utiliser un serveur de temps :

```
vi /etc/systemd/timesyncd.conf
```

[Time]
NTP= 192.168.1.210

3 - Activer la synchro ntp :

```
timedatectl set-ntp true
```

4- Activer le service timesyncd :

```
systemctl enable systemd-timesyncd.service
systemctl start systemd-timesyncd.service
systemctl status systemd-timesyncd.service
```

Si les erreurs suivantes apparaissent :

ConditionFileIsExecutable=!/usr/sbin/ntpd was not met
Condition check resulted in Network Time Synchronization being skipped.

Supprimer ntp :

```
apt remove ntp ntpdate
```

3-\ Test du service NTP sur le client debian :

```
systemctl status systemd-timesyncd.service
```

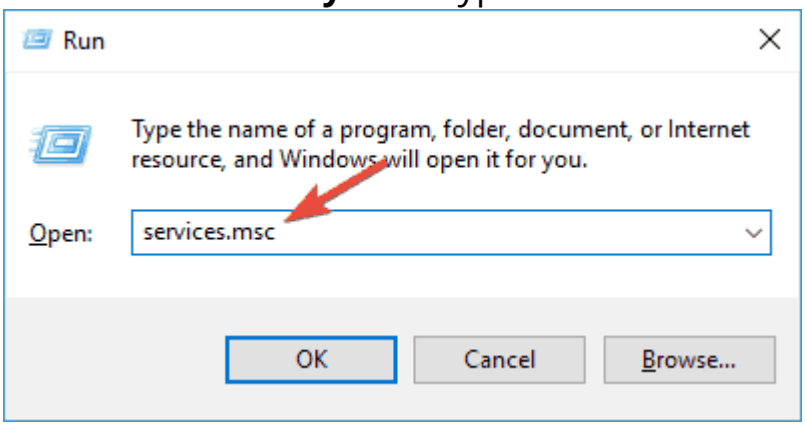
```
root@pcservinfo:~# systemctl restart systemd-timesyncd.service
root@pcservinfo:~# systemctl status systemd-timesyncd.service
● systemd-timesyncd.service - Network Time Synchronization
   Loaded: loaded (/lib/systemd/system/systemd-timesyncd.service; enabled; vendo
  Drop-In: /usr/lib/systemd/system/systemd-timesyncd.service.d
           └─disable-with-time-daemon.conf
   Active: active (running) since Mon 2021-07-12 16:51:23 CEST; 2s ago
     Docs: man:systemd-timesyncd.service(8)
 Main PID: 2919 (systemd-timesyn)
   Status: "Synchronized to time server for the first time 192.168.1.210:123 (19
    Tasks: 2 (limit: 2347)
   Memory: 1.2M
   CGroup: /system.slice/systemd-timesyncd.service
           └─2919 /lib/systemd/systemd-timesyncd
```

4-\ Configuration du service NTP sur un client windows 10

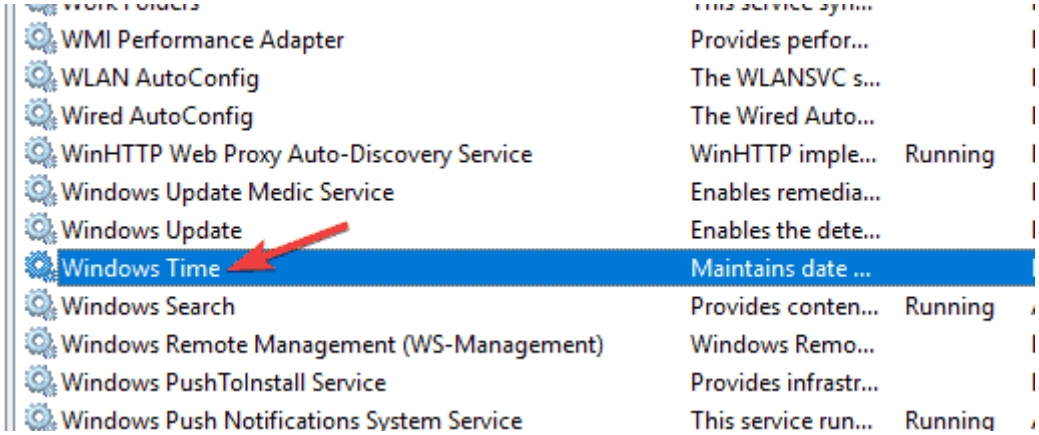
Démarrer le service

https://windowsreport.com/wrong-time-on-windows-clock-fix/

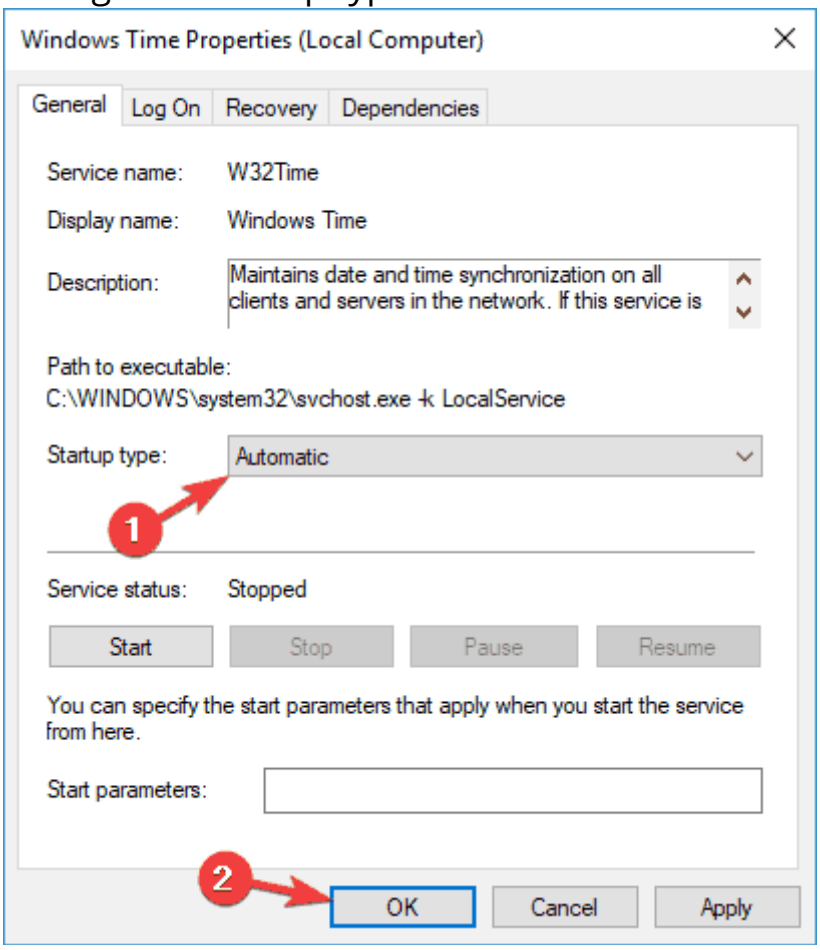
1. Press **Windows Key + R** > type **services.msc** > hit **Enter**.



2. Scroll down to **Windows Time** > double-click it.



3. Change the startup type to **Automatic** > click on **Apply** >**OK**.



Exécuter cmd en tant que administrateur et saisir les commandes suivants

w32tm /config /syncfromflags:manual /manualpeerlist:192.168.1.210

w32tm /config /update

w32tm /resync

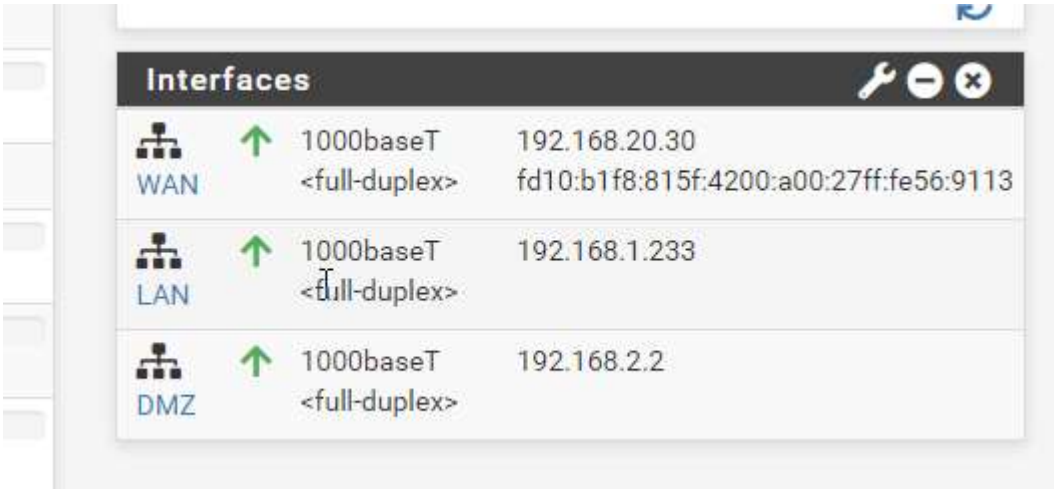
```
C:\Windows\system32>W32TM /config /syncfromflags:manual /manualpeerlist:192.168.1.210
La commande s'est terminée correctement.

C:\Windows\system32>w32TM /config /update
La commande s'est terminée correctement.

C:\Windows\system32>w32tm /resync
Envoi de la commande de resynchronisation à l'ordinateur local
La commande s'est terminée correctement.
```

5-\ Test du service NTP sur le client windows :

```
C:\Windows\system32>w32tm /query /peers
Nb d'homologues : 1

Homologue : 192.168.1.210
État : Actif
Temps restant : 549.2541343s
Mode : 3 (Client)
Couche : 3 (Référence secondaire, synchronisée par (S)NTP)
HomologueIntervalle d'interrogation : 10 (1024s)
HôteIntervalle d'interrogation : 10 (1024s)
```

w32tm /query /peers

configuration pfsense



Enable	☑ Enable interface
Description	WAN Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	DHCP6
MAC Address	xx:xx:xx:xx:xx:xx This field can be used to modify ("spoof") the MAC address of this interface Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blan
MTU	If this field is blank, the adapter's default MTU will be used. This is typically
MSS	If a value is entered in this field, then MSS clamping for TCP connections to header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unle

Static IPv4 Configuration

IPv4 Address	192.168.20.30	/ 24
IPv4 Upstream gateway	default - 192.168.20.1	+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the '
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicki

DHCP6 Client Configuration

Options	☐ Advanced Configuration Use advanced DHCPv6 configuration options.	☐ Configuration Override Override the configuration from this file.
Use IPv4 connectivity as parent interface	☐ Request a IPv6 prefix/information through the IPv4 connectivity link	
Request only an IPv6 prefix	☐ Only request an IPv6 prefix, do not request an IPv6 address	
DHCPv6 Prefix Delegation size	64 The value in this field is the delegated prefix length provided by the DHCPv6 server. Normally specified by the I	
Send IPv6 prefix hint	☐ Send an IPv6 prefix hint to indicate the desired prefix size for delegation	

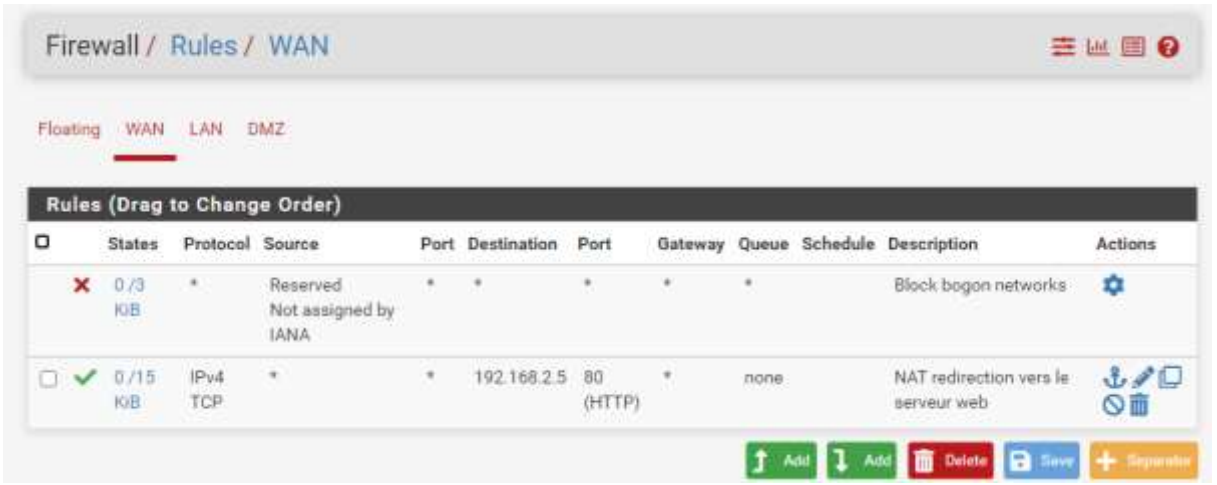
Firewall / NAT / Port Forward

Port Forward | 1:1 | Outbound | NPt

Rules

		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐	✓ ⇄	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.2.5	80 (HTTP)	redirection vers le serveur web	

Add | Add | Delete | Save | + Separator



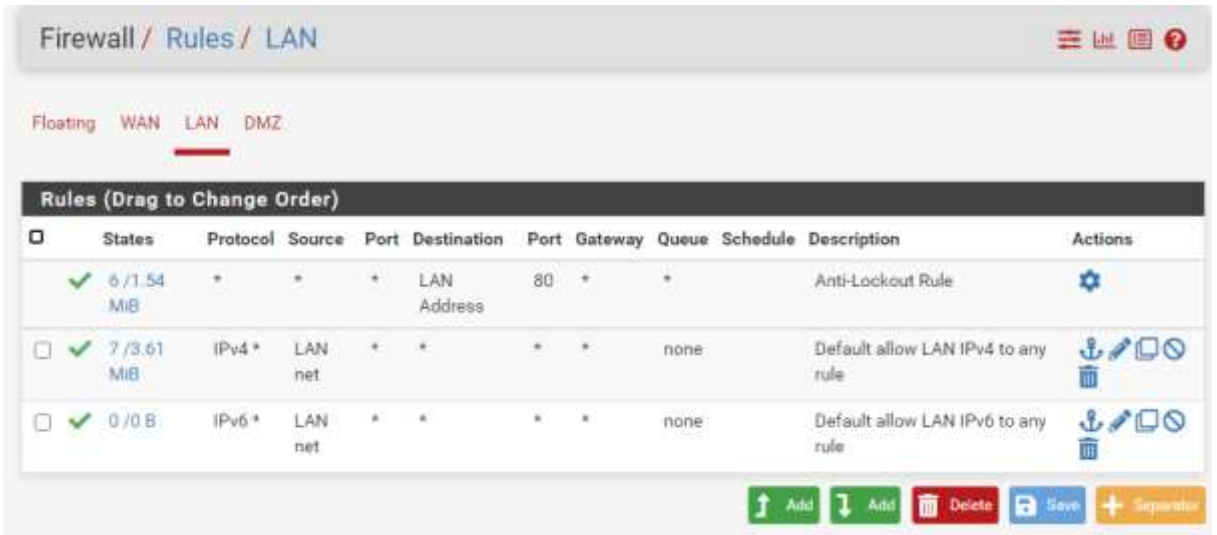
Firewall / Rules / WAN

Floating WAN LAN DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0 /3 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
✓	0 /15 KiB	IPv4 TCP	*	*	192.168.2.5	80 (HTTP)	*	none		NAT redirection vers le serveur web	

Add Add Delete Save Separator



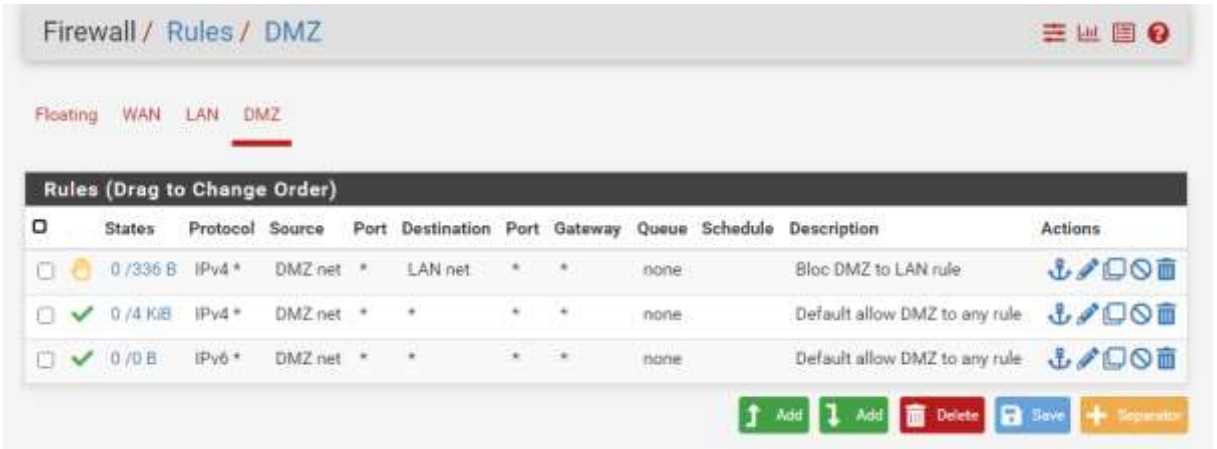
Firewall / Rules / LAN

Floating WAN LAN DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	6 /1.54 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✓	7 /3.61 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN IPv4 to any rule	
✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator



Firewall / Rules / DMZ

Floating WAN LAN DMZ

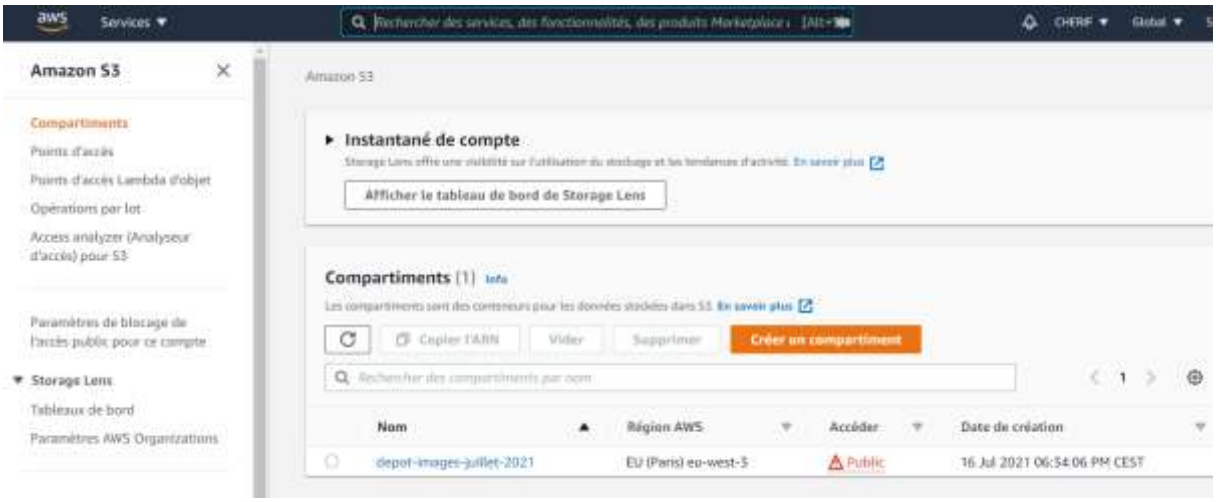
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0 /336 B	IPv4 *	DMZ net	*	LAN net	*	*	none		Bloc DMZ to LAN rule	
✓	0 /4 KiB	IPv4 *	DMZ net	*	*	*	*	none		Default allow DMZ to any rule	
✓	0 /0 B	IPv6 *	DMZ net	*	*	*	*	none		Default allow DMZ to any rule	

Add Add Delete Save Separator

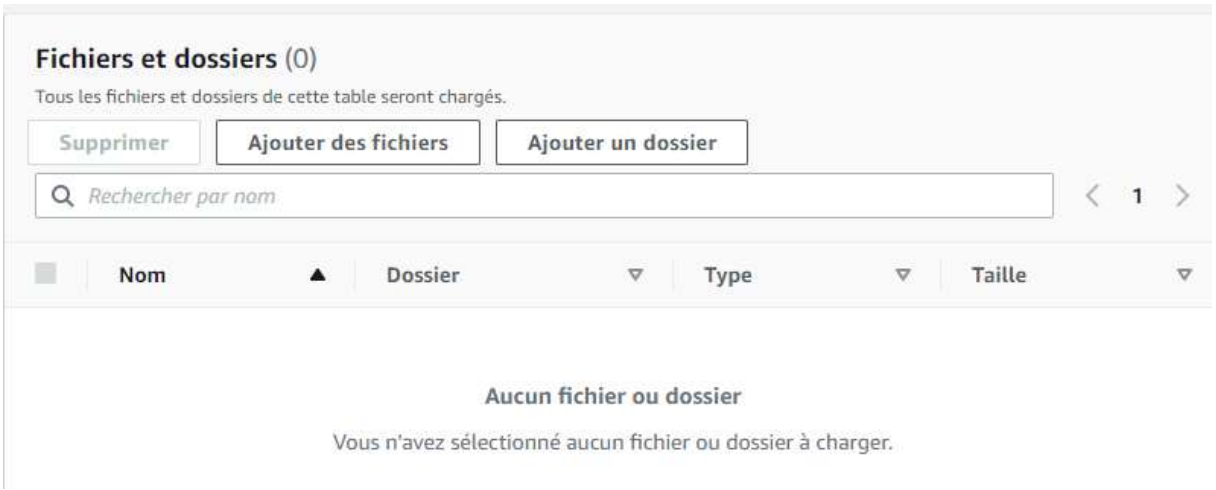
Amazon S3

Stocker des fichiers statiques sur Amazon S3



Cliquer sur créer un compartiment (bucket)→ donner un nom unique → choisir les options par defaut

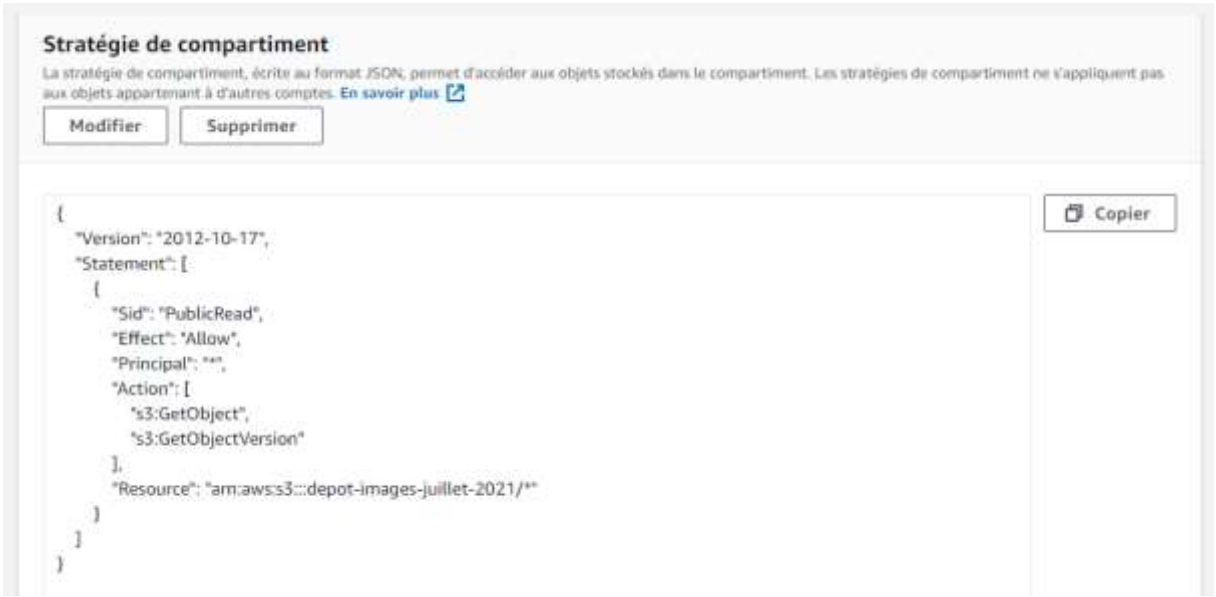
Accéder a ce compartiment dans mon cas (depot-images-juillet-2021) → Ajouter un objet (charger un fichier (upload file))



Pour rendre le projet accessible par tous le monde → il faut le rendre public

1-\ désactiver Bloquer l'accès public (paramètres de compartiment)

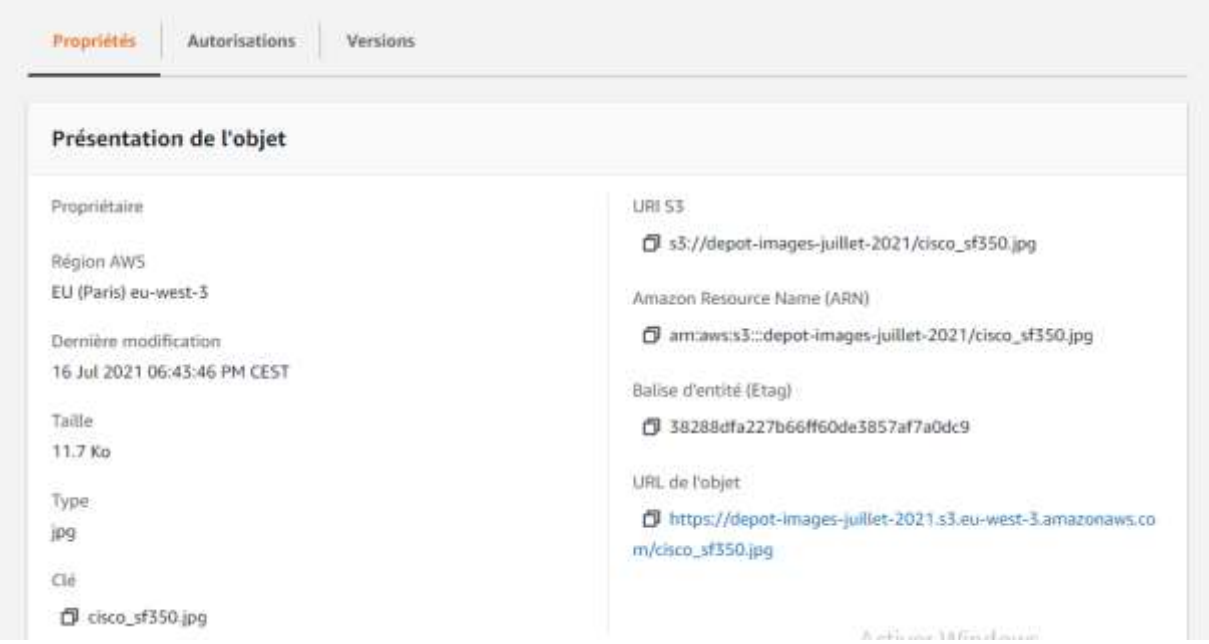
2-\ Ajouter une règle (stratégie de compartiment)




```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::depot-images-juillet-2021/*"
    }
```

]
}

Accéder aux objets publiés



Cliquer sur l'url de l'objet

Liens sur S3 :

https://medium.com/@kyle.galbraith/how-to-host-a-website-on-s3-without-getting-lost-in-the-sea-e2b82aa6cd38

https://openclassrooms.com/fr/courses/4810836-decouvrez-le-cloud-avec-amazon-web-services/5047911-stocker-et-acceder-a-des-fichiers-sur-s3

https://www.youtube.com/watch?v=s1Tu0yKmDKU

IV-\ Installation et Configuration du serveur NFS

1-\ Installation du serveur NTP sur un serveur DEBIAN 10

```
apt-get update

apt-get install ntp

sntp --version

systemctl restart ntp
```

```
systemctl status ntp
```

Installing an NTP client

```
apt-get install ntpdate

apt-get install ntp
```

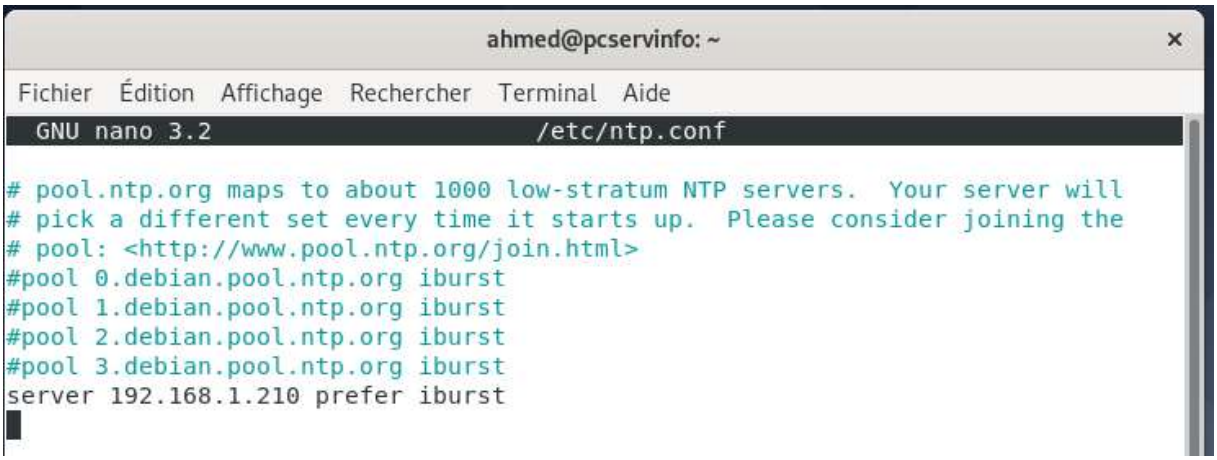
2-\ Configuration du serveur NTP sur pc client DEBIAN 10

Run the following command to open a configuration file in the nano editor.

```
nano /etc/ntp.conf
```

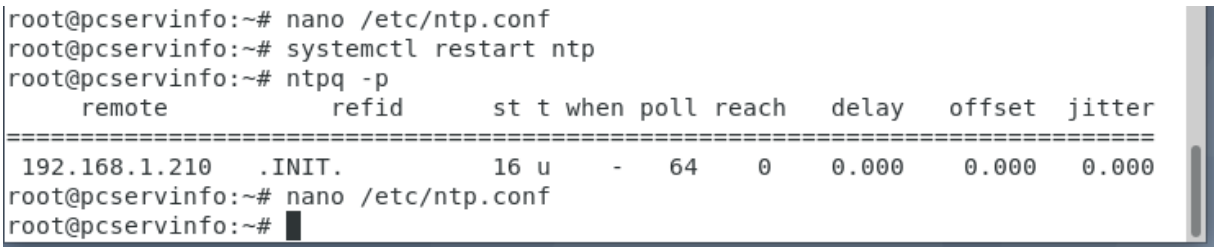
Add the following lines,

```
server 10.1.1.1 prefer iburst
```



Systemctl restart ntp

Ntpq -p



3-\ Test du service NTP sur un poste client :