

# Mise en place du réseau TechNova



## Sommaire

<b>Sommaire.....</b>	<b>1</b>
<b>Partie 1 - Présentation de l'entreprise TechNova.....</b>	<b>2</b>
<b>Partie 2 - Détail sur l'infrastructure du lab.....</b>	<b>3</b>
Sous partie 1 : Description du matériel :.....	3
Sous partie 2 : Schéma.....	3
<b>Partie 3 - Le plan d'adressage.....</b>	<b>4</b>
Sous -partie 1 : VLAN et sous réseau.....	4
Sous -partie 2 : Adresses des machines.....	4
Sous -partie 3 : Adresses (réseau privé hôte).....	5
<b>Partie 4 - Identifiants et mots de passe.....</b>	<b>5</b>
<b>Partie 5 - Version utilisés.....</b>	<b>6</b>
<b>Partie 6 - Mise en place d'un routeur Pfsense.....</b>	<b>7</b>
Sous partie 1 : Création de la machine.....	7
Sous partie 2 : Configuration de Pfsense.....	8
Sous partie 3 : Configuration basique.....	15
Sous partie 4 : Lien Pfsense et PC hôte.....	16
Sous partie 5 : Configuration du DHCP relay.....	18
<b>Partie 7 - Mise en place d'un switch HP Aruba.....</b>	<b>18</b>
Sous partie 1 : Création de la machine.....	18
Sous partie 2 : Connexion du routeur sur une interface.....	18
Sous partie 3 : Lien switch et PC hôte.....	20

<b>Partie 8 - Mise en place du Proxmox virtualisé (SRV-01).....</b>	<b>22</b>
Sous partie 1 : Configuration de la machine.....	22
Sous partie 2 : Installation et configuration de Proxmox.....	25
Sous partie 3 : Routage du Vlan 30.....	26
Sous partie 4 : Configuration du réseau privé hôte pour le lien vm → Pc hôte.....	28
<b>Partie 9 - Mise en place du Proxmox physique (SRV-02).....</b>	<b>28</b>
Sous partie 1 : Configuration de la machine.....	28
Sous partie 2 : Installation et configuration de Proxmox.....	29
Sous partie 3 : Lien serveur → PC hôte.....	30
Sous partie 4 : Connexion sur le switch.....	30
<b>Partie 10 - Mise en place d'un client Linux Debian (graphique) dédié à l'administration.</b>	<b>32</b>
Sous partie 1 : Création de la machine.....	32
Sous partie 2 : Installation et configuration de Debian.....	34
<b>Partie 11 - Mise en place d'un serveur DHCP sous debian.....</b>	<b>36</b>
Sous partie 1 : Création de la machine.....	36
Sous partie 2 : Configuration du DHCP.....	39
Sous partie 3 : Agent relais sur le switch.....	42
Sous partie 4 : Tests sur TNV-01.....	42
<b>Partie 12 - Mise en place d'un serveur DNS avec bind9.....</b>	<b>43</b>
Sous partie 1 : Création de la machine.....	43
Sous partie 2 : Configuration de bind9.....	44
Sous partie 3 : Configuration des DNS forwarders.....	44
<b>Partie 13 - Mise en place d'un Active Directory.....</b>	<b>46</b>
<b>Sous partie 1 : Création de la machine et configuration de Windows.....</b>	<b>46</b>
Sous partie 2 : Création du domaine technova.local.....	47
Sous partie 3 : Mise en place du Dynamic DNS (DDNS).....	49
Sous partie 4 : Ajout du Forwarder pour résoudre le WAN.....	52
<b>Partie 14 - Mise en place des PC client Windows 11.....</b>	<b>53</b>
Sous partie 1 : Création de la machine.....	53
Sous partie 2 : Configuration de Windows.....	55
<b>Partie 15 - Mise en place d'un serveur web intranet via apache2.....</b>	<b>55</b>
Sous partie 1 : Création et configuration de la machine.....	55
Sous partie 2 : Installation et configuration d'apache2.....	56

## Partie 1 - Présentation de l'entreprise TechNova

**Technova** est une PME de 50 collaborateurs spécialisée dans le développement d'IA pour le secteur médical (HealthTech), traitant quotidiennement des données patients sensibles et des algorithmes brevetés. L'entreprise, divisée entre des équipes R&D, administratives et commerciales, souffre actuellement d'une infrastructure obsolète qui expose ces actifs

critiques. Ce projet vise donc à la refonte intégrale de son réseau pour implémenter une segmentation stricte et une politique de sécurité robuste, indispensables pour protéger sa propriété intellectuelle et se conformer aux normes de santé.

C'est dans ce contexte que l'entreprise souhaite **repenser son infrastructure de A à Z** à l'aide d'un "Lab", permettant de simuler des incidents et de valider des politiques de sécurité robustes avant leur déploiement en production.

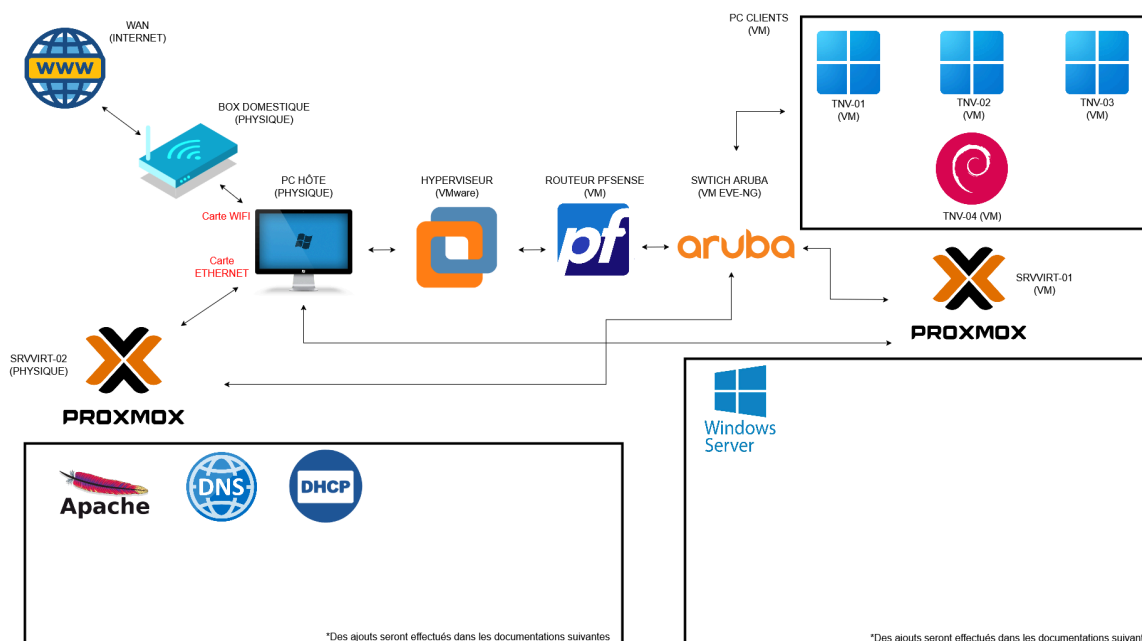
A travers cette procédure le réseau est repensé de manière non sécurisée afin de documenter toute la sécurisation.

## Partie 2 - Détail sur l'infrastructure du lab

### Sous partie 1 : Description du matériel :

- Un PC hôte Windows 11 (32go ram) avec VMware. Les vm sont : srv-01 / Les PC Clients / Un routeur virtualisé (intermédiaire entre le bas et le wan / Un switch virtualisé. D'autres machines y seront intégrés au fil des procédures
- Un serveur Proxmox (8go ram) (srv-02) pour des serveurs services légers. Ce serveur est relié au PC hôte via un câble réseau. Il n'est pas sur le réseau domestique.
- Une box internet domestique (wan du lan)

### Sous partie 2 : Schéma



## Partie 3 - Le plan d'adressage

### Sous -partie 1 : VLAN et sous réseau

Notre réseau sera découpé en plusieurs parties afin d'isoler certains services.

Nom du VLAN	VLAN ID	Adresse
DEFAULT	10	192.168.10.0/24
UTILISATEURS	20	192.168.20.0/24
SERVEURS	30	192.168.30.0/24
INFORMATIQUE	50	192.168.50.0/24
DMZ	60	172.16.60.0/24
BlackHole	999	/

### Sous -partie 2 : Adresses des machines

Nom	@IP	Masque	Passerelle	DNS	Lié au domaine
R1-PFSENSE	192.168.2.254	/24	/	/	/
SW1	192.168.2.1	/24	192.168.2.254	/	/
SRV-01	192.168.30.101	/24	192.168.30.254	8.8.8.8	/
SRV-02	192.168.30.102	/24	192.168.30.254	8.8.8.8	/
TNV-01	DHCP	DHCP	DHCP	DHCP	Oui
SRV-DHCP	192.168.30.5	/24	192.168.30.254	192.168.30.1 (8.8.8.8 avant mise en place de l'AD)	Oui
SRV-DNS	192.168.30.2	/24	192.168.30.254	192.168.30.1 (8.8.8.8 avant mise en place de l'AD)	Oui
SRV-AD	192.168.30.1	/24	192.168.30.254	192.168.30.1	/
TNV-02	DHCP	DHCP	DHCP	DHCP	Oui
TNV-03	DHCP	DHCP	DHCP	DHCP	Oui

TNV-04	DHCP	DHCP	DHCP	DHCP	Oui
SRV-WEB	192.168.30.10	/24	192.168.30.254	192.168.30.1	Oui

### Sous -partie 3 : Adresses (réseau privé hôte)

Nom	Adresse	Masque
R1-PFSENSE	192.168.150.1	/24
SW1	192.168.150.2	/24
SRV-01	192.168.150.101	/24
SRV-02	192.168.150.102	/24
TNV-01	192.168.150.51	/24
SRV-DHCP	192.168.30.5	/24
SRV-DNS	192.168.30.2	/24
SRV-AD	192.168.150.3	/24
TNV-02	192.168.150.52	/24
TNV-03	192.168.150.53	/24
TNV-04	192.168.150.54	/24
SRV-WEB	192.168.30.10	/24

## Partie 4 - Identifiants et mots de passe

Nom	Identifiant	Mot de passe
R1-PFSENSE	admin	pfsense
SW1	admin	/
SRV-01	root	Password1234
SRV-02	root	Password1234
TNV-01	armel	armel

	root	root
SRV-DHCP	armel root	armel root
SRV-DNS	armel root	armel root
SRV-AD	Administrateur	Password1234
TNV-02	admin	Password1234
TNV-03	admin	Password1234
TNV-04	admin	Password1234
SRV-WEB	armel root	armel root

Des mots de passes faibles sont utilisés mais seront changés au fil des procédures afin d'évoquer l'importance d'utilisation de mot de passe fort.

⚠ : Un Keepass sera disponible sur Github :  
<https://github.com/armel-plantier/Portfolio/tree/main/Documents/Keepass>

## Partie 5 - Version utilisés

Nom de la machine	Version	Version du service utilisé
R1-PFSENSE	pfsense : 2.8.1	/
SW1	AOS-CX_10_16_1006	/
SRV-01	Proxmox : proxmox-ve_9.1-1	/
SRV-02	Proxmox : proxmox-ve_9.1-1	/
TNV-01	Debian 13.2	/
SRV-DHCP	Debian 13.2	isc-dhcp-server : 4.4.3
SRV-DNS	Debian 13.2	bind9 : 1:9.20.18-1~deb13u1
SRV-AD	Windows Server 2025 Standard Evaluation : 24h2	/
TNV-02	Windows 11 : 25h2	/
TNV-03	Windows 11 : 25h2	/

TNV-04	Windows 11 : 25h2	/
SRV-WEB	Debian 13.2	apache2 : 2.4.66-1~deb13u1

## Partie 6 - Mise en place d'un routeur Pfsense

Ce routeur va servir d'intermédiaire entre le réseau domestique (considéré comme WAN) et le réseau du lab (LAN).

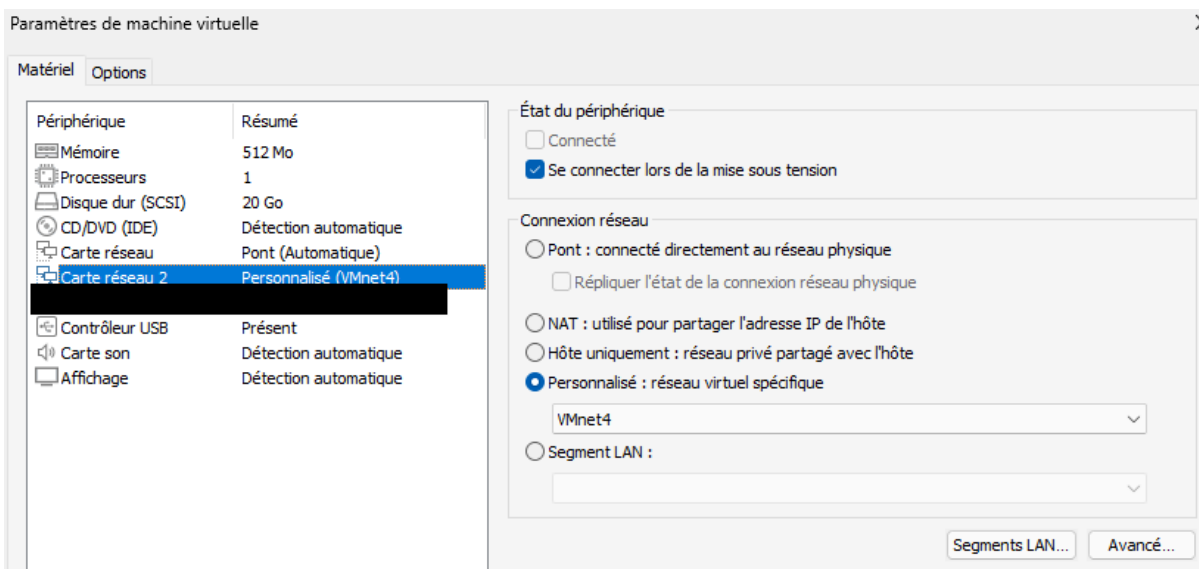
### Sous partie 1 : Création de la machine

Voici la configuration :

Nom :	Routeurpfsense
Emplacement :	C:\Users\Armel\Documents\Virtual Machines\Routeur...
Version :	Workstation 25H2
Système d'explo...	FreeBSD version 10 et antérieures 64 bits
Disque dur :	20 Go, Diviser
Mémoire :	512 Mo
Adaptateur rés...	Pont (Automatique)
Autres périphéri...	CD/DVD, Contrôleur USB, Carte son

Il faudra également récupérer l'iso pfsense :  Iso

Il faudra ensuite ajouter une carte réseau.

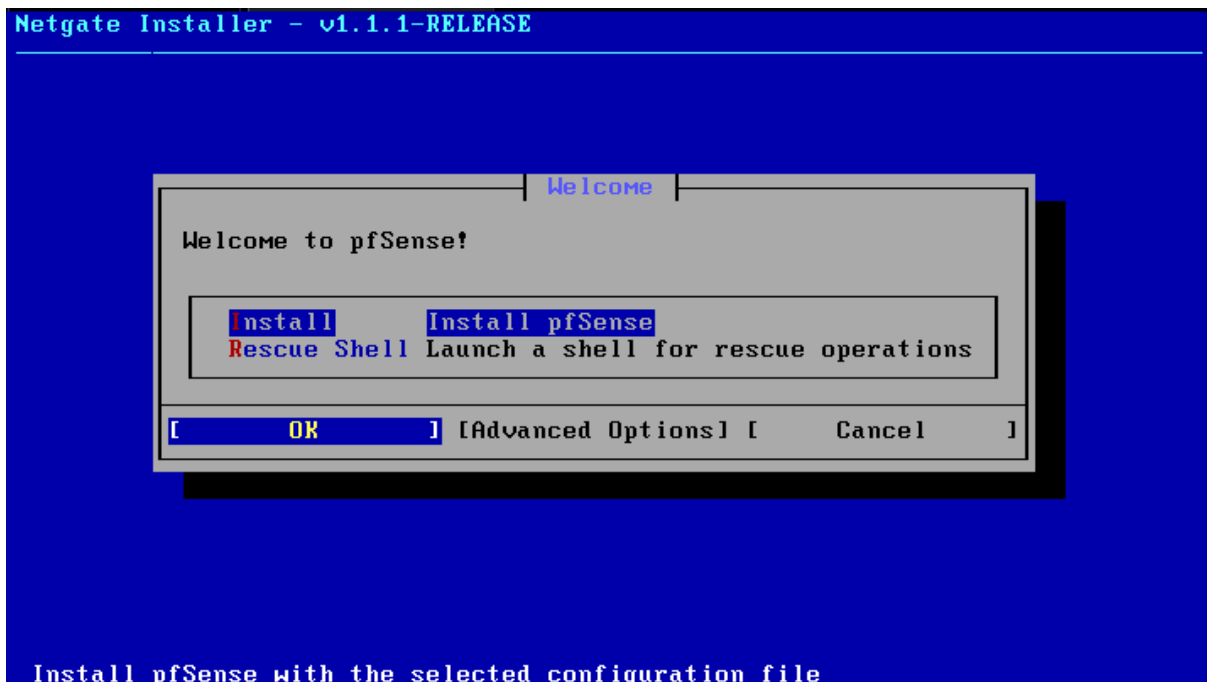
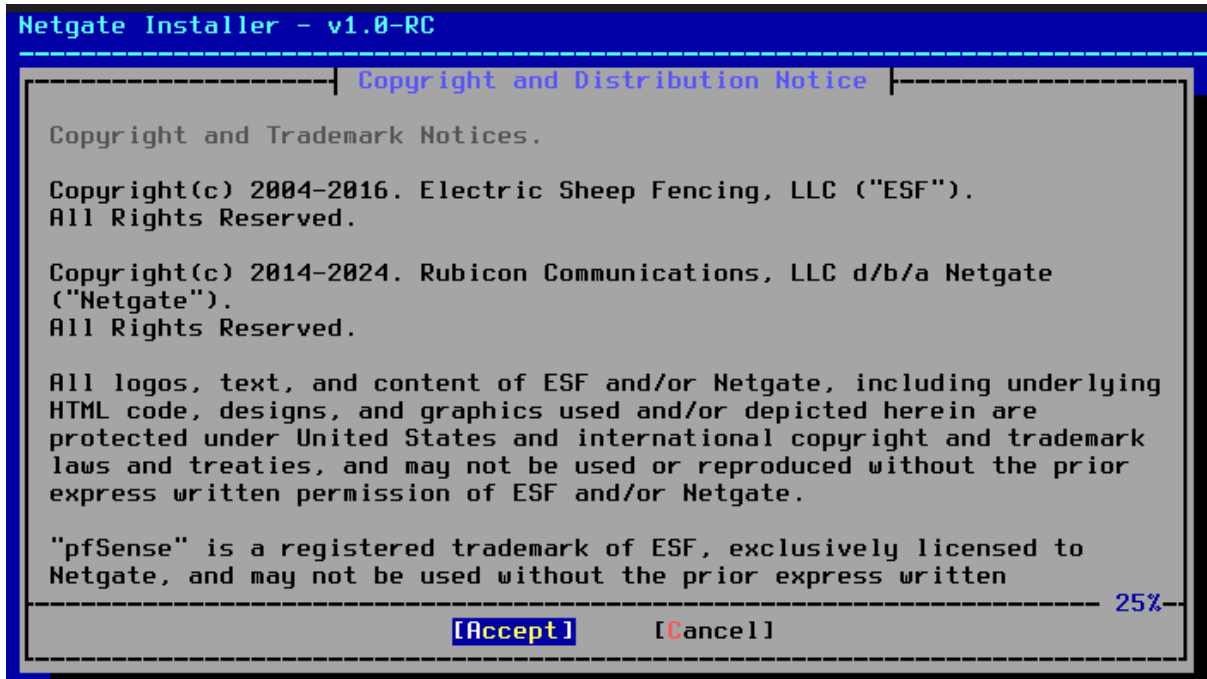




TECHNOVA

Nous allons ensuite pouvoir démarrer la machine et passer à la configuration pfsense.

## Sous partie 2 : Configuration de Pfsense

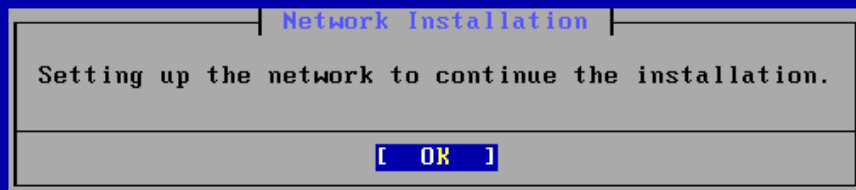




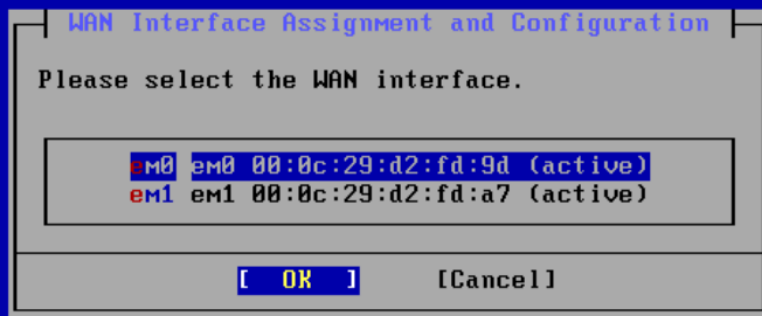


TECHNOVA

Netgate Installer - v1.1.1-RELEASE



Netgate Installer - v1.1.1-RELEASE



On sélectionne em0.



## Netgate Installer - v1.1.1-RELEASE

WAN (em0) Network Mode Setup

Adjust the network operation mode for the WAN (em0) interface if necessary.

>>> Continue	Proceed with the installation
M Interface Mode	DHCP (client)
U VLAN Settings	VLAN Tagging disabled
U Use local resolver	false

[ OK ] [Cancel]

Continue with the displayed settings

Puis on sélectionne em1.

## Netgate Installer - v1.1.1-RELEASE

LAN Interface Assignment and Configuration

Please select the LAN interface.

None	Do not assign the LAN interface
M1	em1 00:0c:29:d2:fd:a7 (active)

[ OK ] [ Skip ] [Cancel]



## Netgate Installer - v1.1.1-RELEASE

**LAN (em1) Network Mode Setup**

Adjust the network operation mode for the LAN (em1) interface if necessary.

>>> Continue	Proceed with the installation
M Interface Mode	STATIC
U VLAN Settings	VLAN Tagging disabled
I IP Address	192.168.1.1/24
D DHCPD Enabled	false

[ OK ] [Cancel]

Continue with the displayed settings

## Netgate Installer - v1.1.1-RELEASE

**Interface Assignment and Configuration**

Detected: VMware Virtual Machine

Please confirm the interface assignment to continue with the installation.

LAN	em1 (active)
WAN	em0 (active)

[ Continue ] [Assign/Configure] [ Cancel ]



## Netgate Installer - v1.1.1-RELEASE

## Active Subscription Validation

This device does not have an active pfSense Plus subscription.

To purchase pfSense Plus:

Software Store: <https://www.netgate.com/purchase-plus>

NDI: 87fd 448f 0b1b afda b388

and select 'Retry Validation' once purchase is complete.

Or select 'Install CE' to install pfSense CE software.

[ **Install CE** ]

[ **Retry Validation** ]

[ **Cancel** ]

## Netgate Installer - v1.1.1-RELEASE

## Installation Options

Please select the File System type and the Partition Scheme.

>> **Continue**

**Proceed with the installation**

**F** File System

ZFS (recommended default)

**P** Partition Scheme

GPT (compatible with MBR)

[ **OK** ]

[ **Cancel** ]

Continue with the displayed settings



Netgate Installer - v1.1.1-RELEASE

**ZFS Virtual Device Type Configuration**

Select the ZFS Virtual Device configuration type.

**stripe Stripe - No Redundancy**

[ **OK** ] [Cancel]

[1+ Disks] Striping provides maximum storage but no redundancy

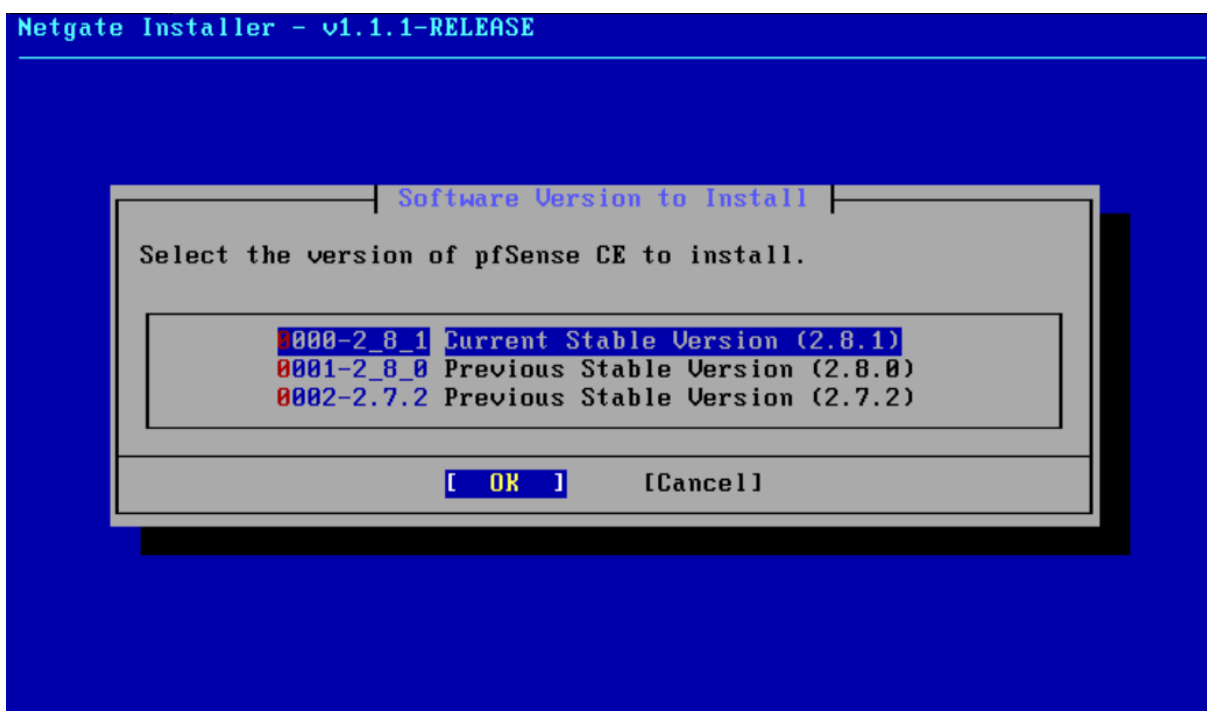
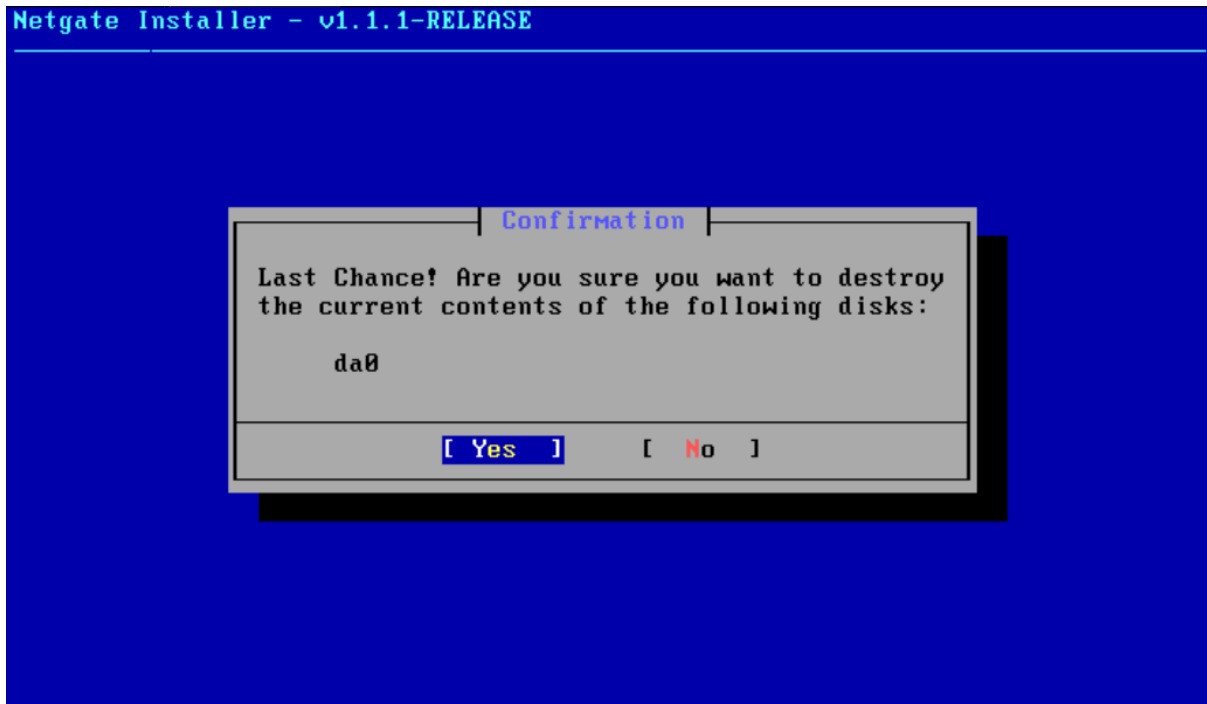
Netgate Installer - v1.1.1-RELEASE

**Disk Selection**

Select the disk(s) for software installation.

[X] **1a0 20G <VMware, VMware Virtual S>**

[ **OK** ] [Advanced Options] [ Cancel ]



L'installation va ensuite se lancer.

```
----- Installation Details -----
GPUs starting with the HD7000 series / Tahiti) or i915kms (for Intel
APUs starting with HD3000 / Sandy Bridge) through kld_list in
/etc/rc.conf. radeonkms for older AMD GPUs can be loaded and there are
some positive reports if EFI boot is NOT enabled.

For amdgpu: kld_list="amdgpu"
For Intel: kld_list="i915kms"
For radeonkms: kld_list="radeonkms"

Please ensure that all users requiring graphics are members of the
"video" group.

Please note that this package was built for FreeBSD 15.0.
If this is not your current running version, please rebuild
it from ports to prevent panics when loading the module.

pfSense Post Installation setup

pfSense Post Installation setup .. done.

-----
< OK >
```

Ce message nous indique que l'installation est terminée.

⚠ : Il ne faut pas faire "Ok". Seulement arrêter la machine et retirer l'iso pour ne pas rebooter dessus.

## Sous partie 3 : Configuration basique

Si tout s'est bien passé, vous devriez avoir ceci :

```
Mon ordinateur x Routeur-Pfsense x
Starting CRON... done.
pfSense 2.8.1-RELEASE amd64 20251215-1731
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 87fd448f0b1bafdab388

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 -> v4/DHCP4: 192.168.1.26/24
v6/DHCP6: 2a01:cb05:46c:da00:20c:29ff:fed2:fd9d/64
LAN (lan) -> em1 -> v4: 192.168.1.1/24

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address      11) Restart GUI
3) Reset admin account and password 12) PHP shell + pfSense tools
4) Reset to factory defaults        13) Update from console
5) Reboot system                    14) Enable Secure Shell (sshd)
6) Halt system                      15) Restore recent configuration
7) Ping host                        16) Restart PHP-FPM
8) Shell
```

Nous allons commencer par désactiver IPV6 sur nos 2 interfaces :

- 1) Sélectionner l'option 2
- 2) Sélectionner l'interface WAN (1)
- 3) Y
- 4) N
- 5) ENTER
- 6) N

Il n'est pas impossible que l'IPV6 revienne automatiquement. Cela dépendra de la box ou du routeur présent côté WAN.

Il faudra faire de même pour l'interface LAN en créant la default gateway :

- 1) Sélectionner l'option 2
- 2) Sélectionner l'option 2 (LAN)
- 3) N
- 4) 192.168.2.254
- 5) /24
- 6) ENTER
- 7) N
- 8) ENTER
- 9) N
- 10) N

Le résultat doit être le suivant :

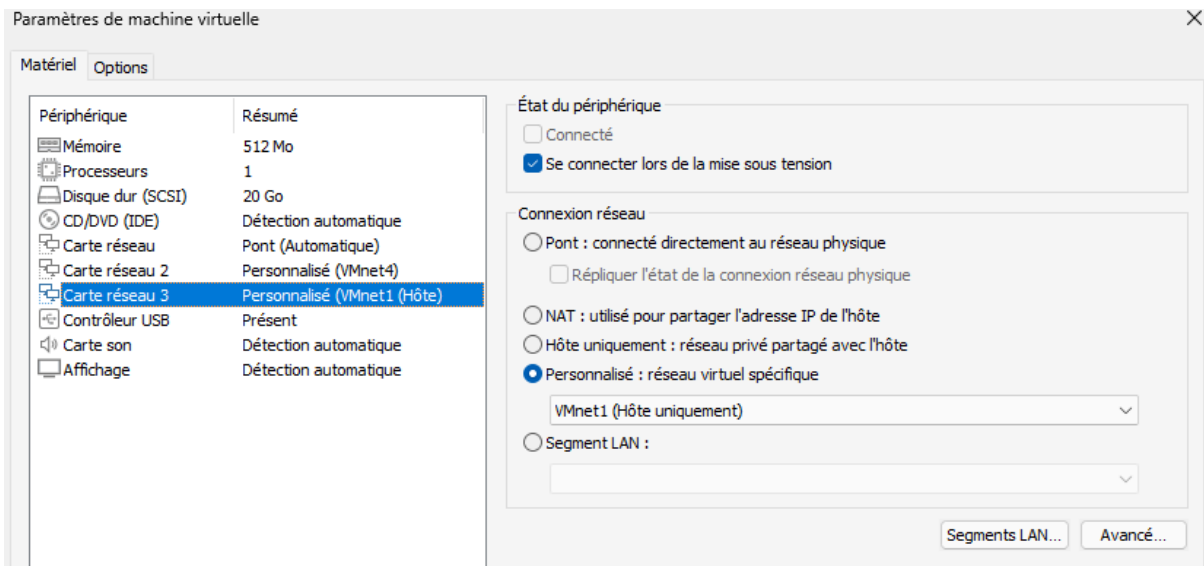
```
The IPv4 LAN address has been set to 192.168.2.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
https://192.168.2.254/
```

Nous avons désormais notre configuration minimale pour un fonctionnement.

## Sous partie 4 : Lien Pfsense et PC hôte

Actuellement la machine est hors du réseau domestique ou est situé le PC hôte. Pour simplifier l'administration, nous allons ajouter une carte réseau à la machine en mode "Hôte uniquement" afin d'accéder à l'interface web sur le PC hôte directement.

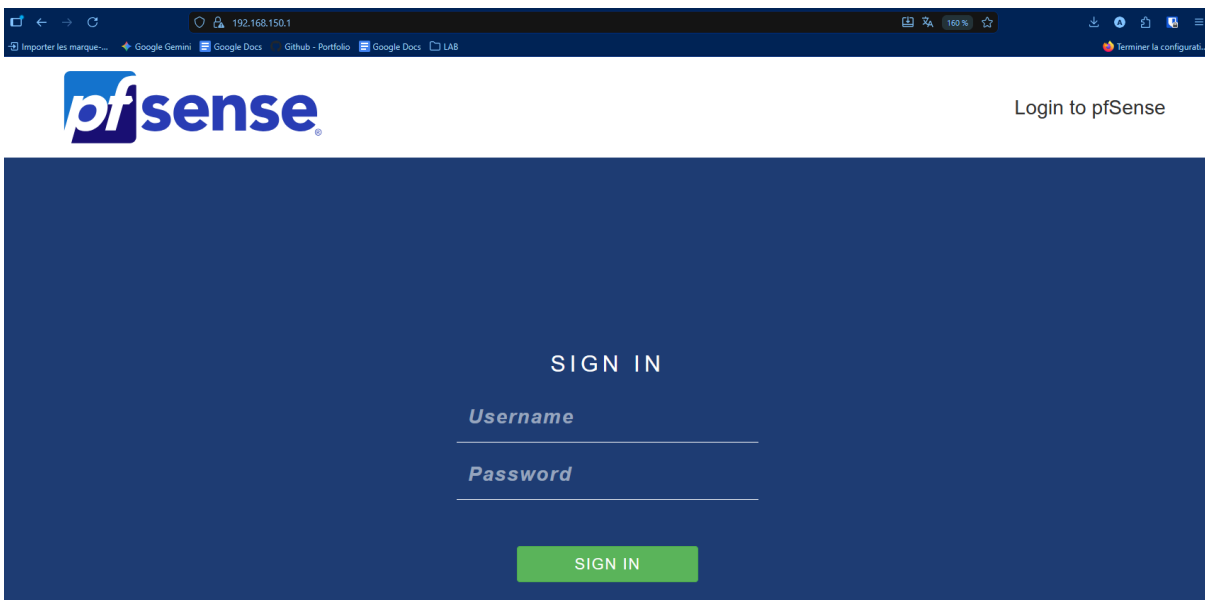




Il faudra ensuite attribuer l'adresse suivante : 192.168.150.1/24 (pensez à assigner l'interface avant)

Pour finir il faudra couper temporairement le pare-feu afin d'accéder à l'interface web :

- 1) Option 8 (Shell)
- 2) pfctl -d
- 3) https://192.168.150.1



Dès que nous allons réactiver le pare-feu (ou redémarrer), ça va rebloquer. Il faut créer une autorisation spécifique :

- 1) Firewall
- 2) Rules
- 3) OPT1
- 4) Add

- 5) Action : Pass
- 6) Protocol : Any
- 7) Source : Any
- 8) Destination : Any

Vous pouvez redémarrer, normalement l'interface doit être accessible.

## Sous partie 5 : Configuration du DHCP relay

Cela nous servira plus tard mais ce qui est fait n'est plus à faire !

Nous allons en avoir besoin pour notre serveur DHCP :

→ Services → DHCP Relay → Enable DHCP Relay

Sélectionnez "LAN" avec CTRL et CLIC

Il faudra ensuite définir le serveur DHCP (Upstream Servers) : 192.168.30.5

Ensuite "Save"

---

## Partie 7 - Mise en place d'un switch HP Aruba

### Sous partie 1 : Création de la machine

Pour cette partie nous avons juste à récupérer le fichier ova de l'os virtuel aruba 10.16 :

 Os Aruba

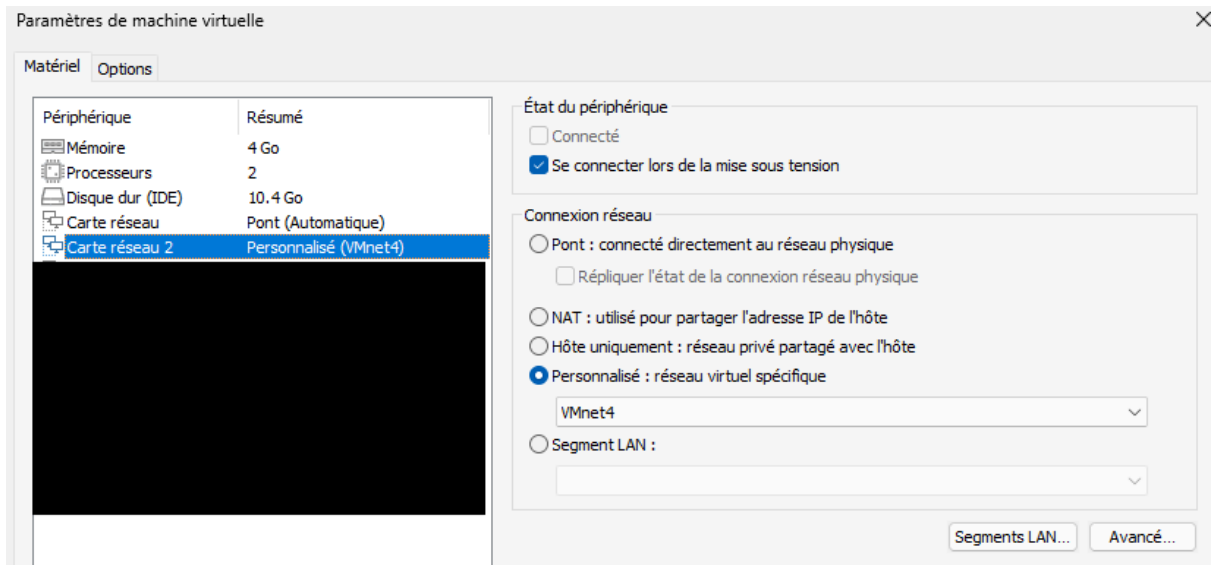
Il faudra ensuite l'importer dans VMware.

Par défaut, toutes les cartes réseau sont en accès par pont.

La première correspond à l'interface mgmt, nous n'y touchons pas pour le moment.

### Sous partie 2 : Connexion du routeur sur une interface

Nous allons donc commencer par éditer la seconde de cette façon :



Vous pourrez ensuite lancer la machine.

Le login par défaut est admin et pour le password il est vierge. Nous le changerons plus tard.

⚠ : Attention le clavier est en qwerty.

Voici la configuration de base :

```
# 1. Passer en mode admin
conf t

# 2. Configurer le VLAN par défaut (VLAN 1)
# C'est ici qu'on met l'IP du switch
interface vlan 1
    ip address 192.168.2.1/24
    no shutdown
    exit

# 3. Associer le port physique 1/1/1 au VLAN 1
# (Par défaut il l'est déjà, mais on s'assure qu'il est allumé)
interface 1/1/1
    no shutdown
    no routing
    vlan access 1
    exit

# 4. Ajouter la route par défaut (La passerelle)
# Cela dit au switch : "Pour sortir, va voir le pfSense"
ip route 0.0.0.0/0 192.168.2.254
```

Pour vérifier on peut faire :

```
sh arp
```

```
switch# sh arp

IPv4 Address      MAC              Port      Physical Port
      State
-----
192.168.2.254     00:0c:29:d2:fd:a7  vlan1     1/1/1
      reachable

Total Number Of ARP Entries Listed: 1.
```

Puis :

```
ping 192.168.2.254
```

```
switch# ping 192.168.2.254
PING 192.168.2.254 (192.168.2.254) 100(128) bytes of data.
108 bytes from 192.168.2.254: icmp_seq=1 ttl=64 time=1.59 ms
108 bytes from 192.168.2.254: icmp_seq=2 ttl=64 time=1.21 ms
108 bytes from 192.168.2.254: icmp_seq=3 ttl=64 time=1.17 ms
108 bytes from 192.168.2.254: icmp_seq=4 ttl=64 time=1.15 ms
108 bytes from 192.168.2.254: icmp_seq=5 ttl=64 time=1.48 ms

--- 192.168.2.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 1.151/1.319/1.591/0.180 ms
```

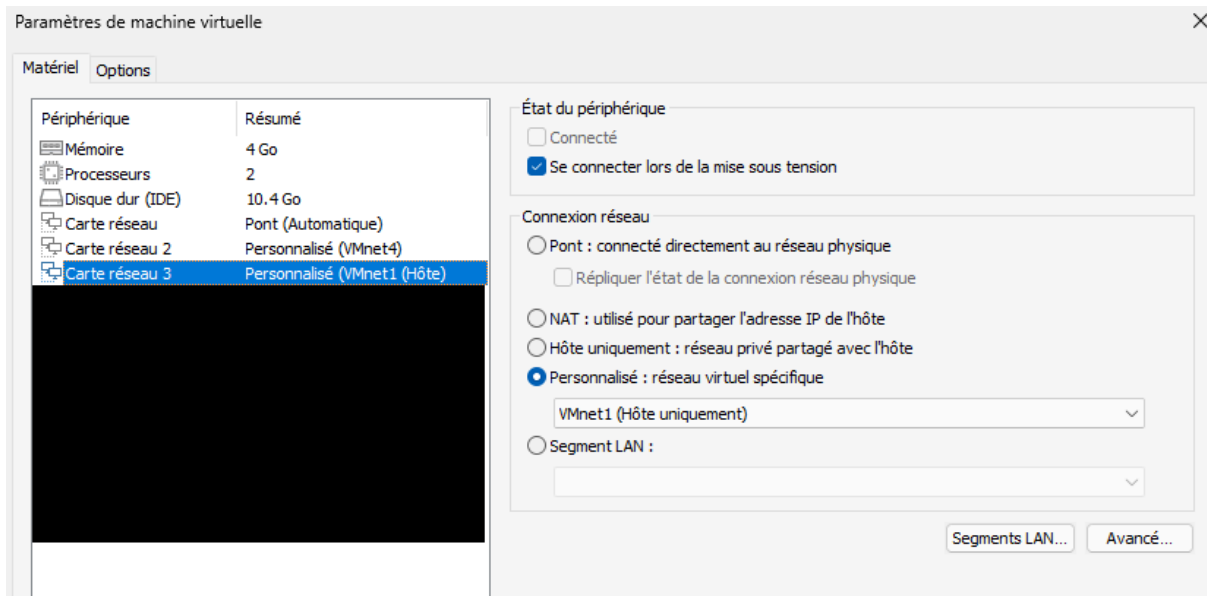
On peut même vérifier qu'on sorte bien :

```
ping 8.8.8.8
```

```
switch# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 100(128) bytes of data.
108 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=12.4 ms
108 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=13.2 ms
108 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=11.5 ms
108 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=14.3 ms
```

### Sous partie 3 : Lien switch et PC hôte

Afin de faciliter l'administration, nous allons ajouter une carte en "réseau privé hôte" pour que le PC hôte puisse se connecter en ssh au switch ou à son interface web. Cela nous permettra notamment de pouvoir utiliser un clavier AZERTY



Nous devons également lui attribuer une IP.

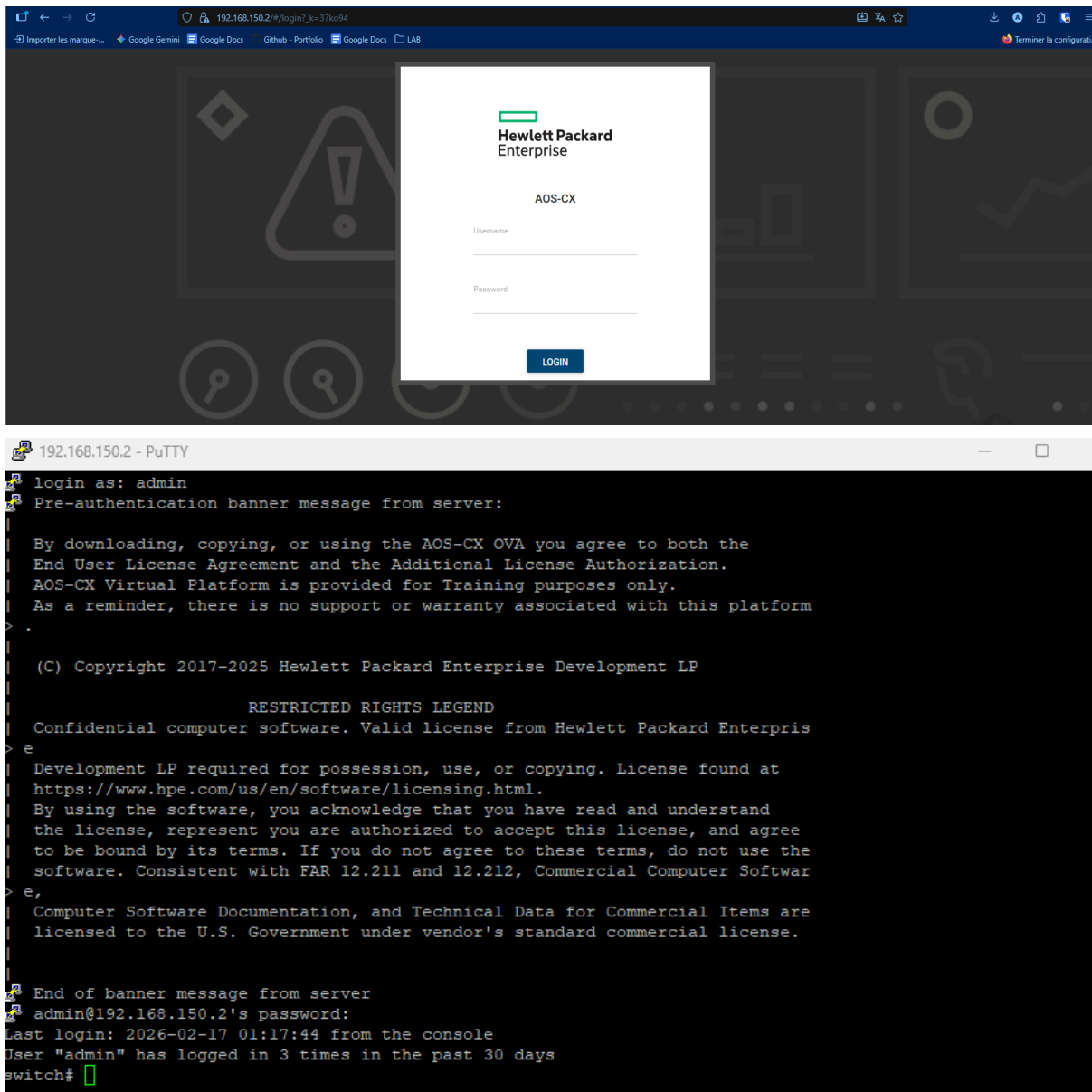
```
conf t

interface 1/1/2
    no shutdown
    routing
    ip address 192.168.150.2/24
    exit
```

Nous allons également activer HTTPS et SSH

```
# Activer le serveur HTTPS sur les ports de données
conf t
https-server vrf default


# Activer le SSH sur les ports de données
conf t
ssh server vrf default
```



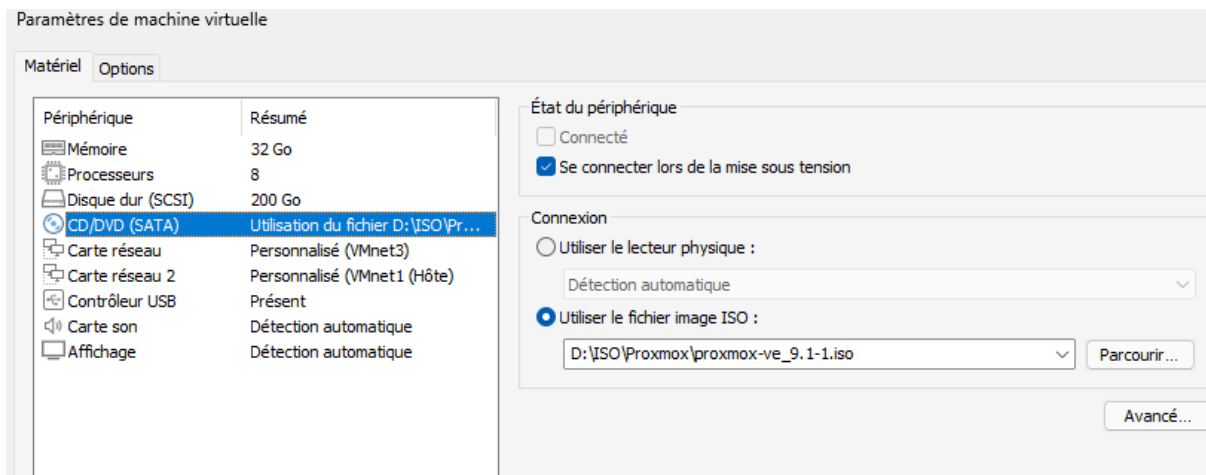
Nous avons donc la connexion la plus basique sur notre switch.

## Partie 8 - Mise en place du Proxmox virtualisé (SRV-01)

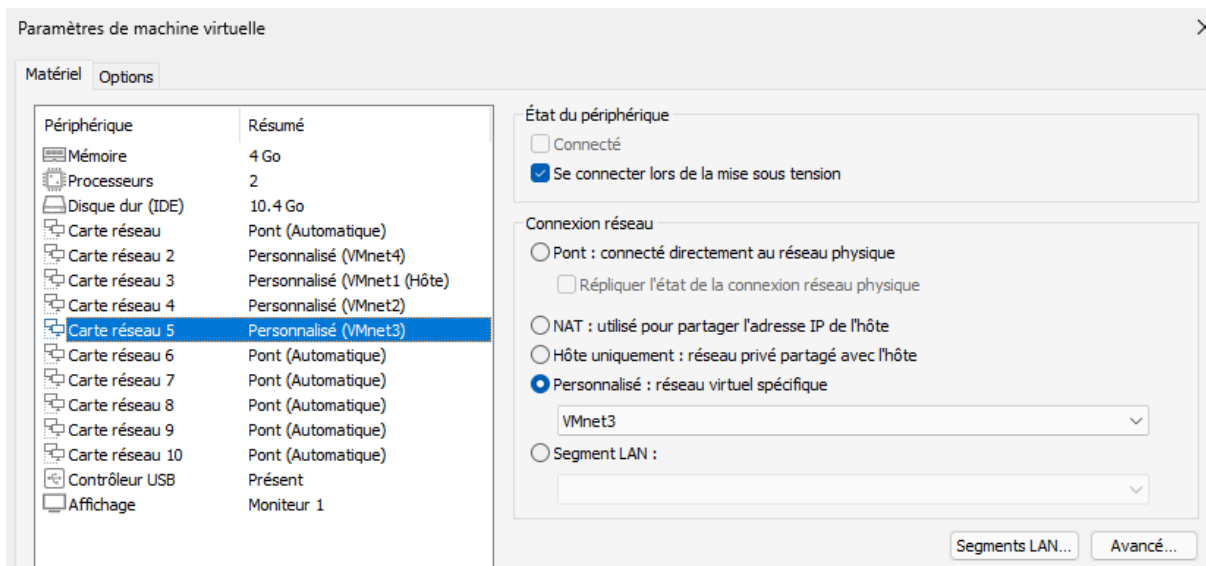
### Sous partie 1 : Configuration de la machine

Il faudra commencer par récupérer l'iso :  Iso

Voici la configuration de la machine :



Il faudra ajouter une carte réseau sur le switch :



Il faudra également apporter cette modification sur le switch :

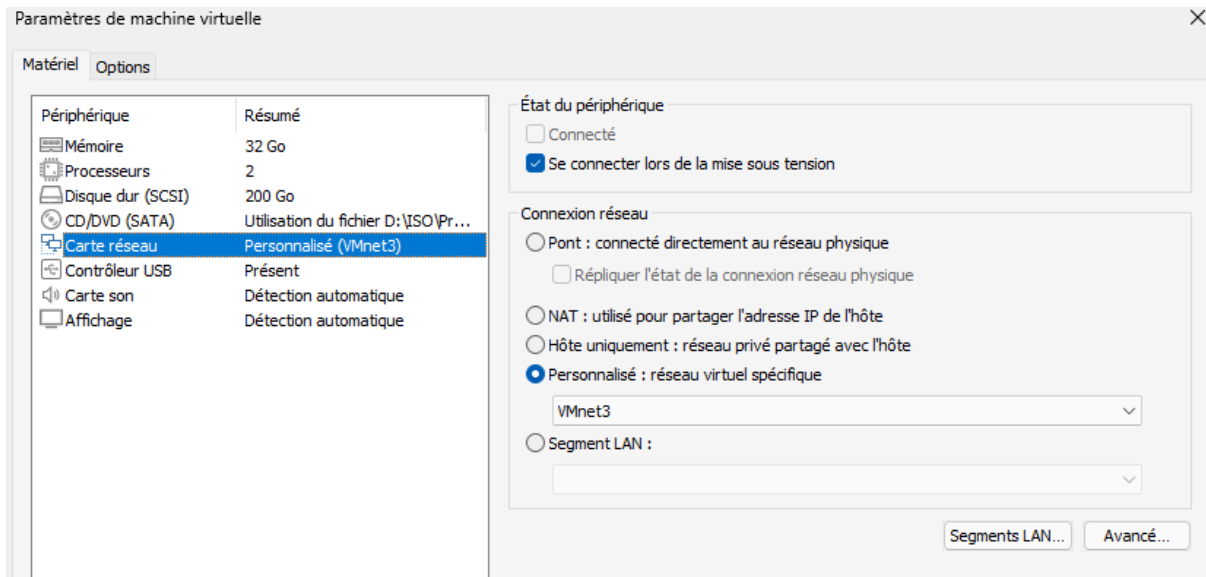
```
conf t
vlan 30
    name SERVEURS
exit

conf t
interface vlan 30
    ip address 192.168.30.254/24
exit

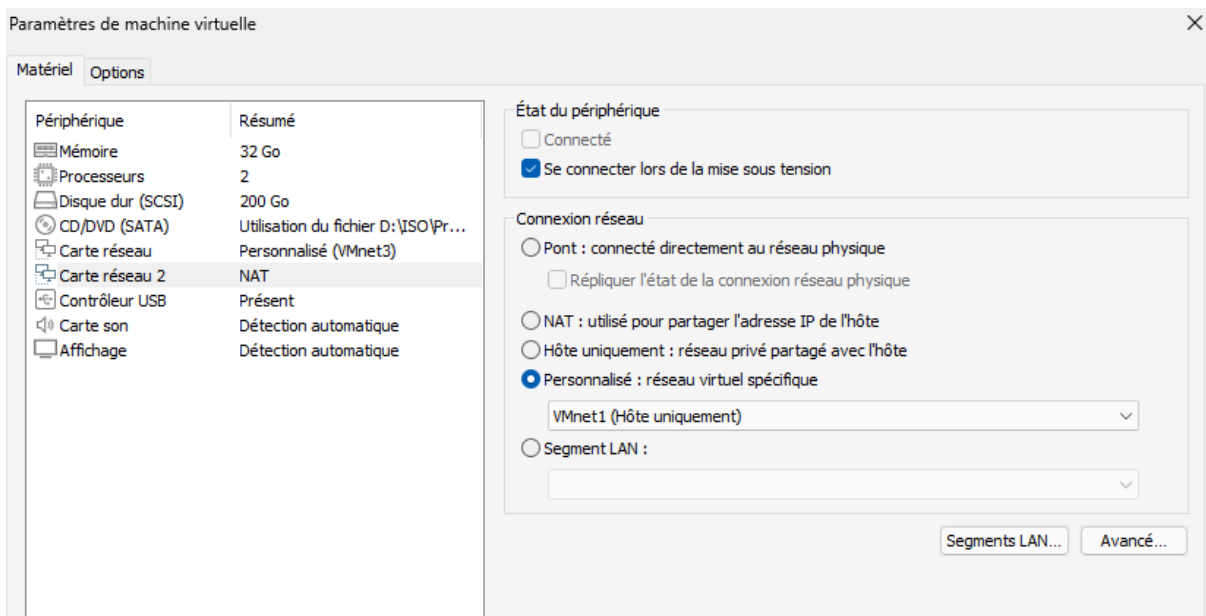
conf t
interface 1/1/4
```

```
no shutdown
no routing
vlan access 30
exit
```

Puis sur notre serveur :

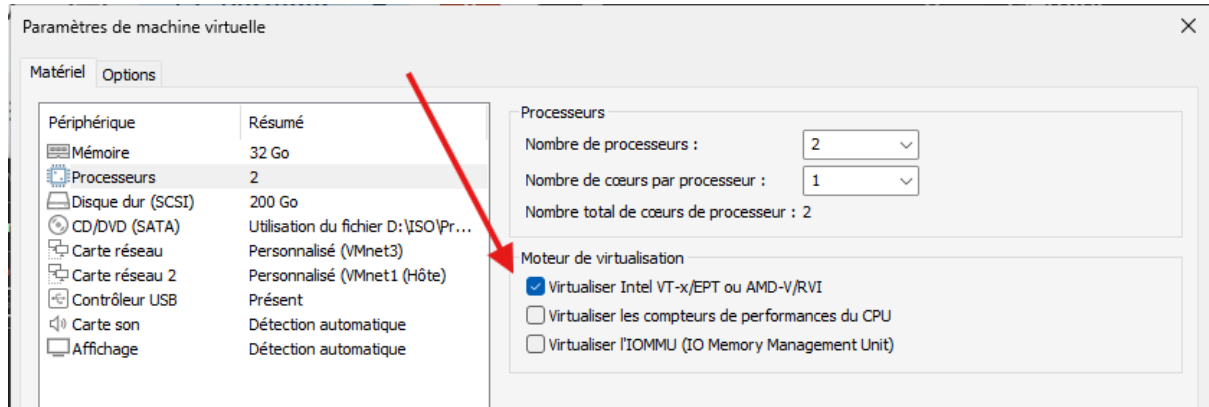


Profitons-en pour ajouter la carte réseau "réseau privé hôte" pour simplifier l'administration.



Il faudra également activer la virtualisation imbriquée :





## Sous partie 2 : Installation et configuration de Proxmox

Nous pouvons désormais lancer la machine.

Voici les étapes d'installation :

- 1) Install Proxmox VE (Graphical)
- 2) I agree
- 3) Sélectionnez le disque → Next
- 4) Country : France / Time zone : Europe/Paris / Keyboard Layout : French
- 5) Password : Password1234! / Email : [aplantier@technova.local](mailto:aplantier@technova.local)
- 6) nic0 / SRV-01.technova.local / 192.168.30.101/24 / 192.168.30.254 / 8.8.8.8
- 7) Install

Une fois l'installation terminée, vous pouvez vous connecter et paramétrer cette connexion réseau.

```
auto lo
iface lo inet loopback

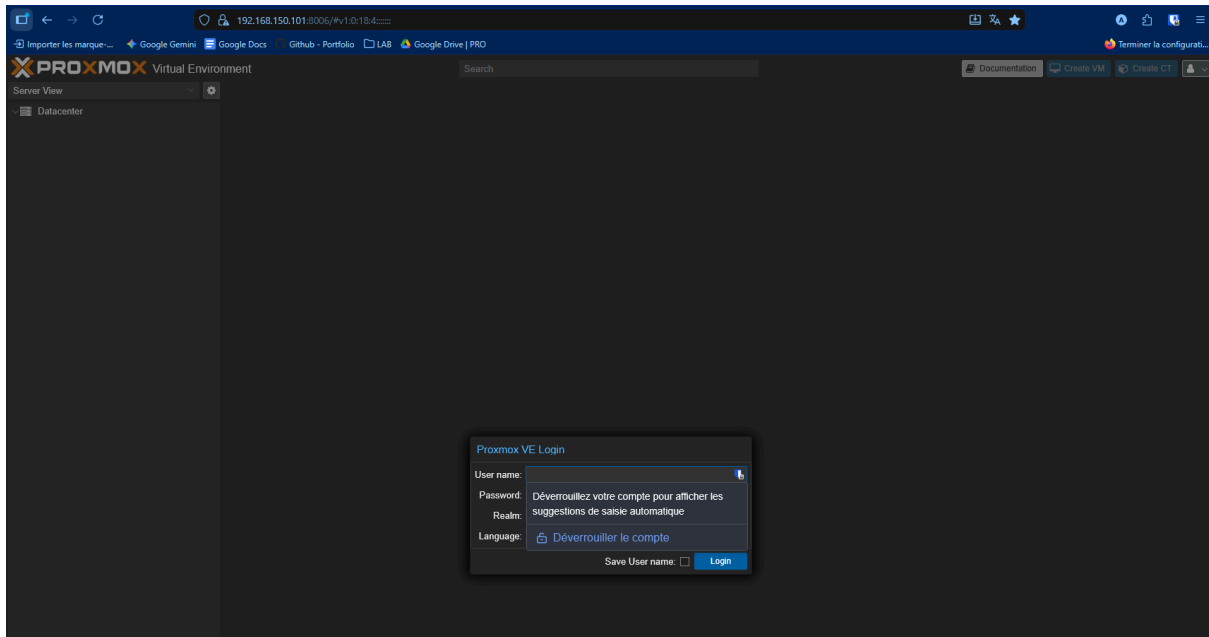
iface nic0 inet manual

auto vbr0
iface vbr0 inet static
    address 192.168.30.101/24
    gateway 192.168.30.254
    bridge-ports nic0
    bridge-stp off
    bridge-fd 0

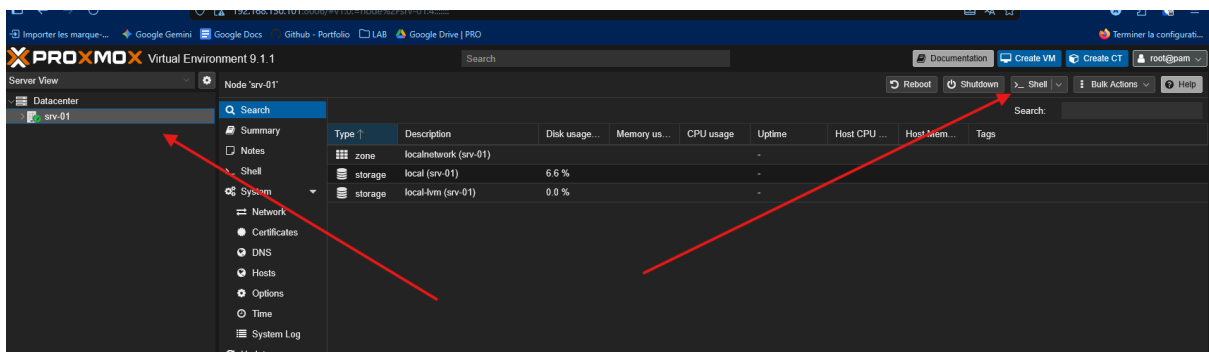
iface nic1 inet static
address 192.168.150.101/24

source /etc/network/interfaces.d/*
```

La connexion en réseau privé hôte est désormais configurée. L'interface web est accessible.



On peut alors se connecter puis ouvrir un "shell"



## Sous partie 3 : Routage du Vlan 30

Il nous reste une dernière partie avant que tout fonctionne correctement.

Le switch envoie le paquet au pfSense, mais pfSense, lui, reçoit un paquet venant de "30.x" et se dit : "Je connais pas ce réseau, je n'ai pas de route pour lui répondre, poubelle."

### 1) Créer la "Porte de retour" (Gateway)

Le pfSense doit savoir par où renvoyer les réponses du VLAN 30.

1. Dans pfSense → System → Routing → Gateways.
2. Add.
  - Interface : LAN (C'est par là que le switch est connecté).

- Name : GW\_SWITCH\_ARUBA.
  - Gateway : 192.168.2.1 (C'est l'IP du switch dans le VLAN de transit).
3. Sauvegarde et Apply Changes.

## 2) Créez la Route Statique

Maintenant on dit à pfSense : "Tout ce qui est pour 30.x, envoie-le à la Gateway qu'on vient de créer".

1. System → Routing → Static Routes.
2. Add.
  - Destination network : 192.168.30.0/24.
  - Gateway : GW\_SWITCH\_ARUBA.
3. Sauvegarde.

## 3. Autoriser le trafic (Firewall & NAT)

C'est souvent là que ça bloque encore.

A. Le Pare-feu (Firewall Rules) Les paquets du VLAN 30 arrivent physiquement sur l'interface LAN de pfSense.

1. Firewall → Rules → LAN.
2. Regardez les règles. Souvent, la règle par défaut autorise "LAN Net". Or, 192.168.30.x N'EST PAS dans "LAN Net" (qui est 2.x).
3. Ajoutez une règle en haut de la liste :
  - Action : Pass.
  - Source : Any (ou Network -> 192.168.30.0/24).
  - Destination : Any.

B. Le NAT (Outbound NAT) - CRUCIAL Pour aller sur Internet, ton serveur doit "emprunter" l'IP publique du pfSense.

1. Firewall → NAT → Outbound.
2. Cochez le mode Hybrid Outbound NAT et cliquez sur Save.
3. Créez une nouvelle règle (Mapping) en cliquant sur la flèche vers le haut (Add) :
  - Interface : WAN.
  - Protocole : Any.
  - Source : Network -> 192.168.30.0/24.
  - Translation : WAN address.
  - Sauvegardez et Apply Changes

Vous pouvez normalement pinguer :

- 1) La passerelle : 192.168.30.254
- 2) Le switch : 192.168.2.1
- 3) Le routeur 192.168.2.254
- 4) WAN (dns google) : 8.8.8.8

## Sous partie 4 : Configuration du réseau privé hôte pour le lien vm → Pc hôte

SRV-01 → System → Network :

### 1. Enlever l'IP de la carte brute (nic1)

1. Sélectionnez nic1 et cliquez sur le bouton Edit en haut.
2. Efface complètement l'adresse 192.168.150.101/24 du champ IPv4/CIDR.
3. La case "Autostart" doit être décochée ou grisée (si l'option est là) et → OK.

### 2. Création du Switch Virtuel (vmbr1)

1. Cliquez sur Create → Linux Bridge.
2. Remplir les champs comme ceci :
  - Name : vmbr1 (par défaut)
  - IPv4/CIDR : 192.168.150.101/24 (On redonne l'IP à Proxmox, mais cette fois sur le bridge)
  - Bridge ports : nic1 (C'est ici qu'on branche le switch virtuel à la vraie carte réseau)
  - Gateway (IPv4) : (Laissez complètement vide)
3. Cliquez sur Create.

### 3. Appliquer les modifications

1. En haut de l'écran → Apply Configuration. Proxmox va redémarrer ses cartes réseau en quelques secondes.

Il suffira d'aller dans la configuration d'une VM, de mettre sa carte réseau sur vmbr1, et de lui donner une IP disponible dans ce réseau (par exemple 192.168.150.1/24).

La configuration classique est désormais réalisée.

---

## Partie 9 - Mise en place du Proxmox physique (SRV-02)

### Sous partie 1 : Configuration de la machine

En premier lieu nous allons relier le serveur physique sur la carte ethernet du pc hôte avec un câble réseau.

Ensuite il faudra une clé usb de 4go et l'iso Proxmox. A partir de cela, il faudra rendre "bootable" la clé à l'aide de l'outil rufus.

## Sous partie 2 : Installation et configuration de Proxmox

Une fois cela fait il faudra “booter” sur la clé et ainsi réaliser l’installation Proxmox avec les paramètres suivants :

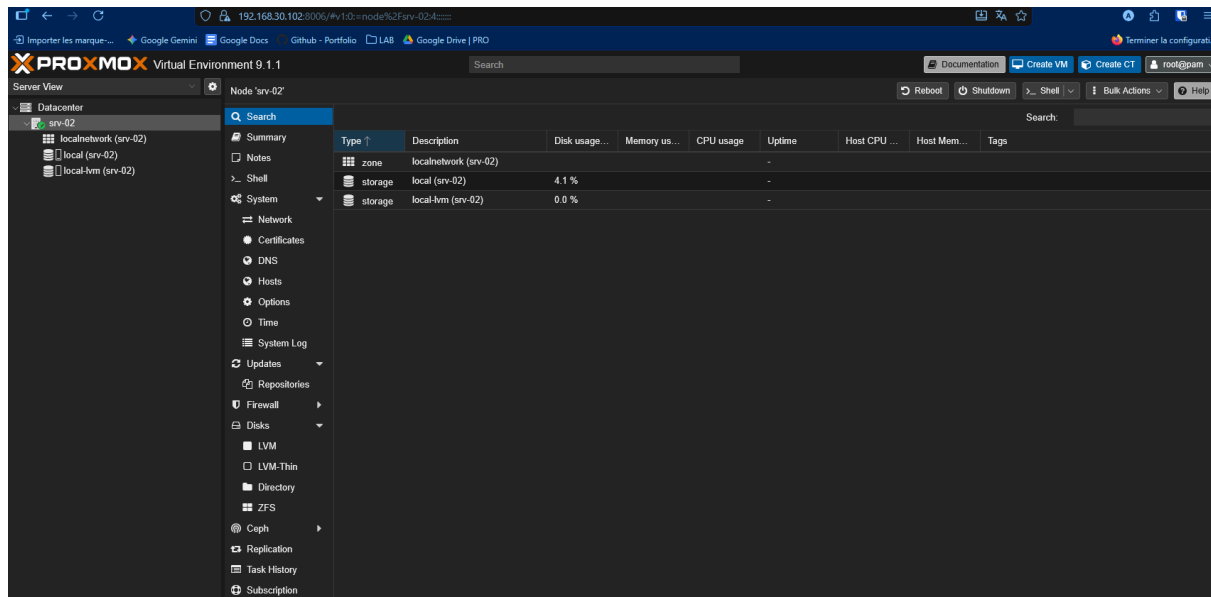
- 1) Install Proxmox VE (Graphical)
- 2) I agree
- 3) Sélectionnez le disque → Next
- 4) Country : France / Time zone : Europe/Paris / Keyboard Layout : French
- 5) Password : Password1234! / Email : [aplantier@technova.local](mailto:aplantier@technova.local)
- 6) nic0 / SRV-02.technova.local / 192.168.30.102/24 / 192.168.30.254 / 8.8.8.8
- 7) Install

## Sous partie 3 : Lien serveur → PC hôte

Pour simplifier l'administration, il nous faut afficher l'interface sur notre PC hôte.

Windows R → ncpa.cpl → Ethernet → IPV4 → Adresse 192.168.30.200 → Masque 255.255.255.0

L'interface doit être disponible.



## Sous partie 4 : Connexion sur le switch

Actuellement, notre serveur est uniquement relié à notre PC. Nous devons donc créer le lien entre le PC et VMware. Pour ce faire, il faudra ouvrir l'éditeur de réseau virtuel et "ponter" VMnet2 sur la carte ethernet.

Éditeur de réseau virtuel

Nom	Type	Connexion externe	Connexion d'hôte	DHCP	Adresse de sou...
VMnet0	Ponté	Killer(R) Wireless-AC 1550 ...	-	-	-
VMnet1	Hôte u...	-	Connecté	-	192.168.150.0
VMnet2	Ponté	Killer E2500 Gigabit Ethernet...	-	-	-
VMnet8	NAT	NAT	Connecté	Activé	192.168.146.0

Ajouter un réseau... Supprimer le réseau Renommer le réseau...

Informations sur VMnet

☒ Pont (connecter les machines virtuelles directement au réseau externe)

Ponté sur : Killer E2500 Gigabit Ethernet Controller Paramètres automatiques...

☐ NAT (adresse IP de l'hôte partagée avec les VM) Paramètres du NAT...

☐ Hôte uniquement (connecter les machines virtuelles en interne dans un réseau privé)

☐ Connecter un hôte et un adaptateur virtuel à ce réseau  
Nom de l'adaptateur virtuel de l'hôte : Adaptateur réseau VMware VMnet 2

☐ Utiliser le service DHCP local pour distribuer les adresses IP aux machines virtuelles Paramètres DHCP...

Adresse IP de sous-réseau : . . . Masque de sous-réseau : . . .

Rétablir les valeurs par défaut Importer... Export... OK Annuler Appliquer Aide

Il faudra ensuite appliquer VMNet2 sur notre switch :

Paramètres de machine virtuelle

Matériel Options

Périphérique	Résumé
Mémoire	4 Go
Processeurs	2
Disque dur (IDE)	10.4 Go
Carte réseau	Pont (Automatique)
Carte réseau 2	Personnalisé (VMnet4)
Carte réseau 3	Personnalisé (VMnet1 (Hôte))
Carte réseau 4	Personnalisé (VMnet2)
Carte réseau 5	Personnalisé (VMnet3)
Carte réseau 6	Pont (Automatique)
Carte réseau 7	Pont (Automatique)
Carte réseau 8	Pont (Automatique)
Carte réseau 9	Pont (Automatique)
Carte réseau 10	Pont (Automatique)
Contrôleur USB	Présent
Affichage	Moniteur 1

État du périphérique

☐ Connecté

☒ Se connecter lors de la mise sous tension

Connexion réseau

☐ Pont : connecté directement au réseau physique

☐ Répliquer l'état de la connexion réseau physique

☐ NAT : utilisé pour partager l'adresse IP de l'hôte

☐ Hôte uniquement : réseau privé partagé avec l'hôte

☒ Personnalisé : réseau virtuel spécifique

VMnet2

☐ Segment LAN :

Segments LAN... Avancé...

Voici la configuration à ajouter :

```
conf t

# On sélectionne le nouveau port
interface 1/1/3
    no shutdown

    # Très important : on désactive le routage sur ce port physique
    # car c'est l'interface VLAN 30 qui gère l'IP, pas le port lui-même.
    no routing

    # On met le port dans le VLAN 30
    vlan access 30
exit
```

Vous pouvez normalement pinguer :

- 5) La passerelle : 192.168.30.254
- 6) Le switch : 192.168.2.1
- 7) Le routeur 192.168.2.254
- 8) WAN (dns google) : 8.8.8.8

---

## Partie 10 - Mise en place d'un client Linux Debian (graphique) dédié à l'administration

### Sous partie 1 : Création de la machine

Il faudra commencer par récupérer l'iso Debian 13 :  Iso

Voici la configuration de la machine :



Assistant Nouvelle machine virtuelle

**Prêt à créer une machine virtuelle**  
Cliquez sur Terminer pour créer la machine virtuelle et commencer l'installation de Debian 13.x 64 bits.

La machine virtuelle sera créée avec les paramètres suivants :

Nom :	TNV-01
Emplacement :	C:\Users\Armel\Documents\Virtual Machines\TNV-01
Version :	Workstation 25H2
Système d'explo...	Debian 13.x 64 bits
Disque dur :	20 Go, Diviser
Mémoire :	2048 Mo
Adaptateur rés...	Aucun
Autres périphéri...	Cœurs de CPU 2, CD/DVD, Contrôleur USB, Carte son

Personnaliser le matériel...

☐ Mettre sous tension cette machine virtuelle après sa création

< Précédent Terminer Annuler

Il faudra ajouter une carte réseau :

Paramètres de machine virtuelle

Matériel Options

Périphérique	Résumé
Mémoire	2 Go
Processeurs	2
Disque dur (SCSI)	20 Go
CD/DVD (SATA)	Utilisation du fichier D:\ISO\De...
Carte réseau	Personnalisé (VMnet5)
Contrôleur USB	Présent
Carte son	Détection automatique
Affichage	Détection automatique

État du périphérique

☐ Connecté  
☒ Se connecter lors de la mise sous tension

Connexion réseau

☐ Pont : connecté directement au réseau physique  
☐ Répliquer l'état de la connexion réseau physique

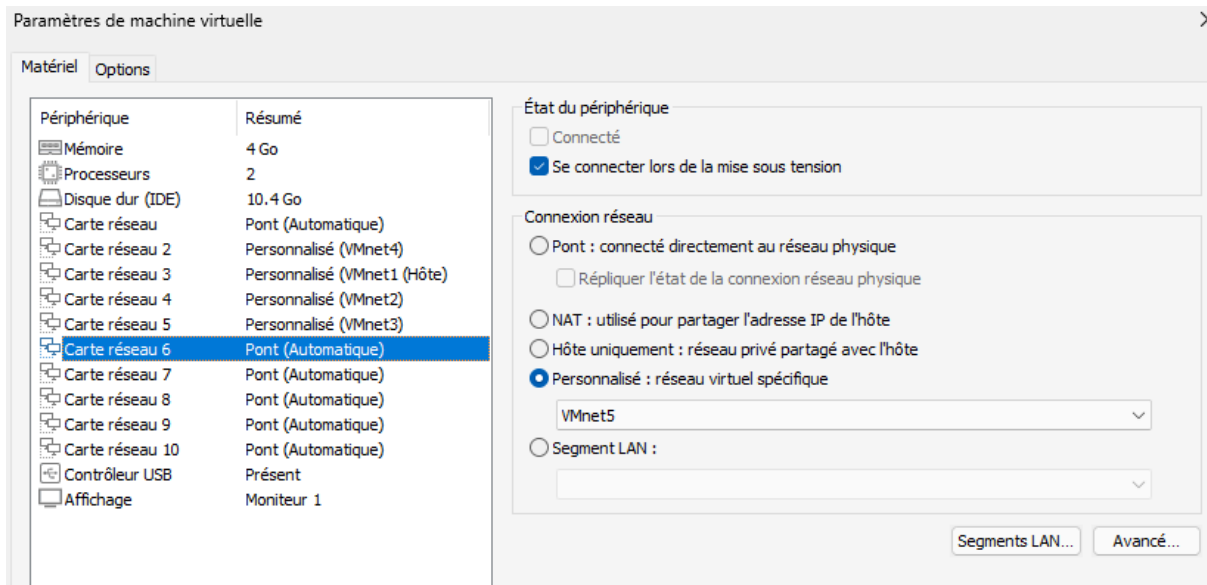
☐ NAT : utilisé pour partager l'adresse IP de l'hôte  
☐ Hôte uniquement : réseau privé partagé avec l'hôte  
☒ Personnalisé : réseau virtuel spécifique

VMnet5

☐ Segment LAN :

Segments LAN... Avancé...

Puis sur le switch :



Ce poste est destiné à l'informatique alors il va également falloir créer le vlan et l'administrer :

```
conf t
vlan 50
name INFORMATIQUE
exit

ip interface vlan 50
ip address 192.168.50.254 255.255.255.0
exit

int 1/1/5
no sh
no routing
vlan access 50
exit

write memory
```

⚠ : Il faut penser à déclarer ce vlan sur le routeur, sinon il refusera le transit car réseau inconnu.

→ Voir [Mise en place du réseau TechNova](#)

## Sous partie 2 : Installation et configuration de Debian

⚠ : Avec la configuration réseau actuelle l'installation ne sera pas complète. Pour qu'elle le soit je bascule la machine sur le réseau domestique temporairement.

Nous pouvons désormais lancer la machine et configurer Debian.

Une fois installé, nous allons stopper la machine, puis appliquer les paramètres réseau classique de façon à être connecté sur le switch.

Nous allons ensuite appliquer cette configuration :

```
GNU nano 8.4 /etc/net
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet static
address 192.168.50.1/24
gateway 192.168.50.254
_
```

```
systemctl restart networking
```

Vous pouvez normalement pinguer :

- 9) La passerelle : 192.168.50.254
- 10) Le switch : 192.168.2.1
- 11) Le routeur 192.168.2.254
- 12) WAN (dns google) : 8.8.8.8

Il faudra ensuite configurer le DNS :

```
nano /etc/resolv.conf
```

```
nameserver 8.8.8.8
```

Nous allons donc pouvoir installer notre interface graphique GNOME :

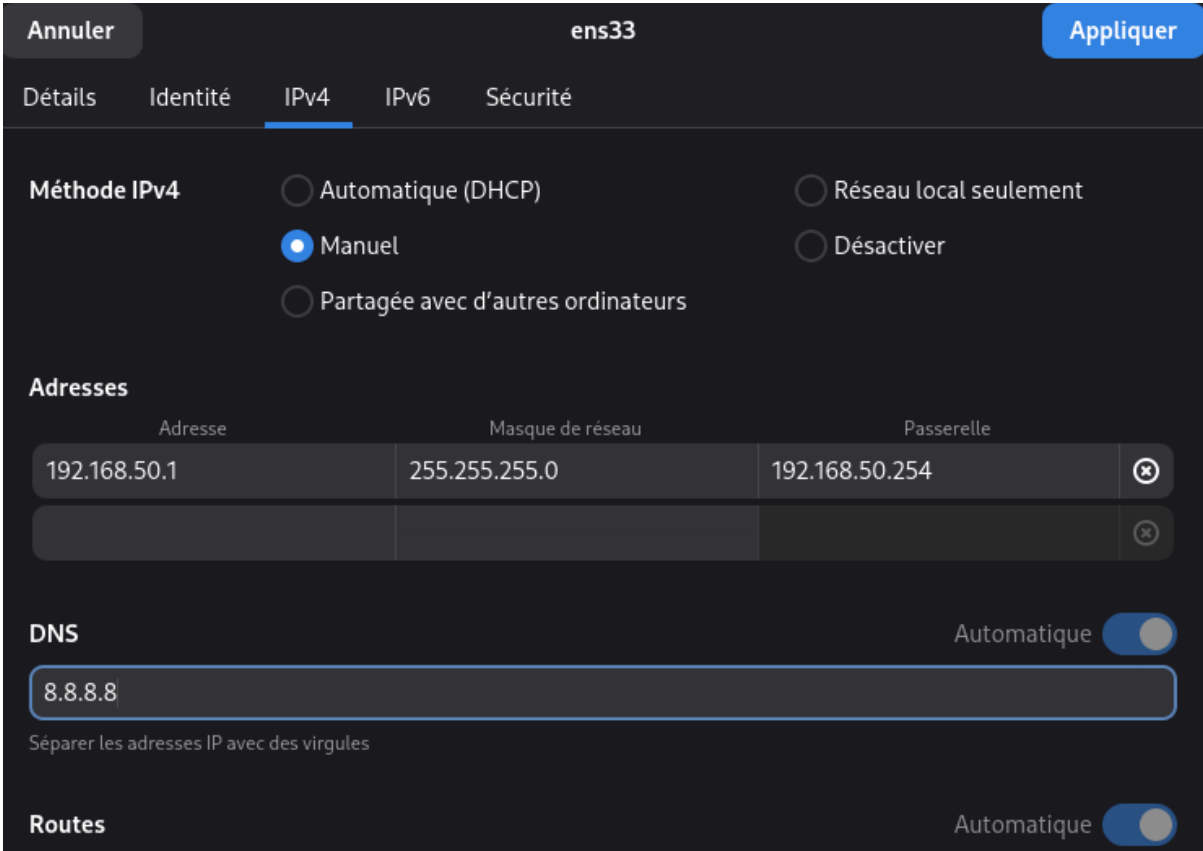
```
apt update
apt install gnome -y
```

L'installation peut prendre entre 5 et 10 minutes. Une fois terminé il faudra redémarrer la machine (avec reboot) et se connecter avec l'utilisateur "armel"

Nous allons ajouter la possibilité de gérer la configuration réseau graphiquement :

- 1) Ouvrir un terminal
- 2) Passer en superutilisateur avec “su”
- 3) nano /etc/NetworkManager/NetworkManager.conf
- 4) Ajouter ceci :  
[ifupdown]  
managed=true
- 5) Redémarrer la machine (graphiquement)

Voici donc la configuration réseau temporaire :



Annuler ens33 Appliquer

Détails Identité IPv4 IPv6 Sécurité

**Méthode IPv4**

☐ Automatique (DHCP) ☐ Réseau local seulement

☒ Manuel ☐ Désactiver

☐ Partagée avec d'autres ordinateurs

**Adresses**

Adresse	Masque de réseau	Passerelle
192.168.50.1	255.255.255.0	192.168.50.254

**DNS** Automatique ☒

8.8.8.8

Séparer les adresses IP avec des virgules

**Routes** Automatique ☒

## Partie 11 - Mise en place d'un serveur DHCP sous debian

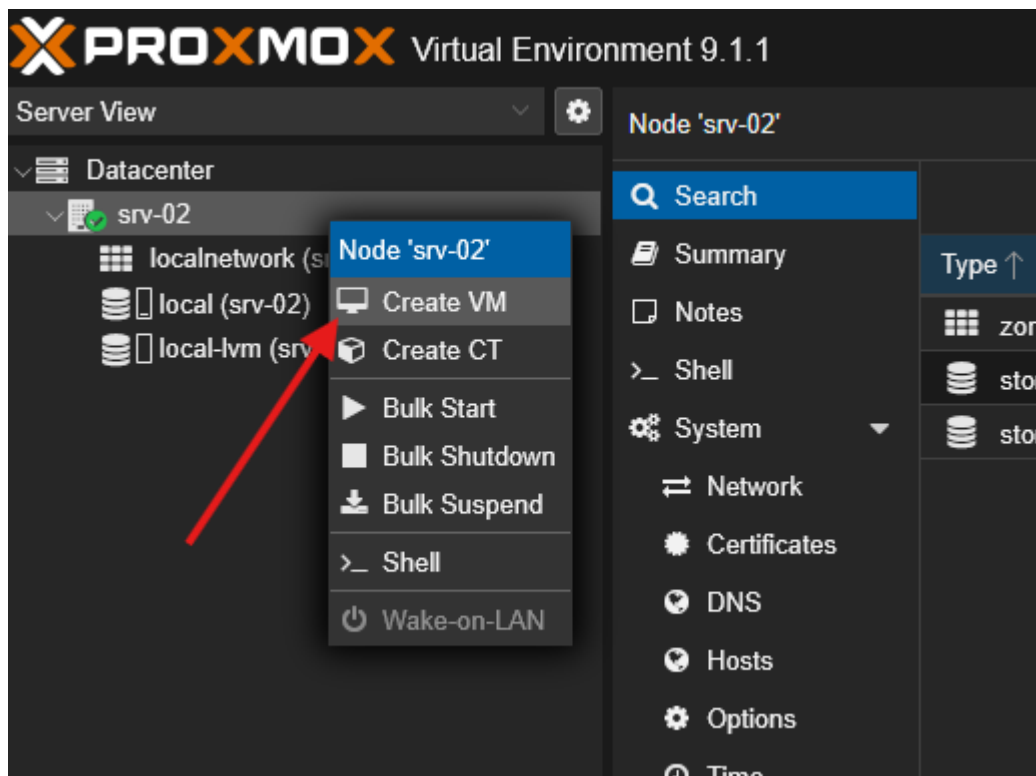
Sous partie 1 : Création de la machine

Nous allons donc mettre en place un serveur DHCP. Pour cela nous allons donc le mettre en place sur le SRV-02.

Il faut commencer par importer l'iso :

Datacenter → srv-02 → local (srv-02) → ISO Images → Upload → Select Files →  
[Sélectionnez l'iso]

On va ensuite pouvoir créer la VM :



Create: Virtual Machine

General
OS
System
Disks
CPU
Memory
Network
Confirm

Key ↑	Value
cores	1
cpu	x86-64-v2-AES
ide2	local:iso/debian-13.3.0-amd64-netinst.iso,media=cdrom
memory	2048
name	SRV-DHCP
net0	virtio,bridge=vibr0,firewall=1
nodename	srv-02
numa	0
ostype	l26
scsi0	local-lvm:32,iotread=on
scsihw	virtio-scsi-single
sockets	1
vmid	100

☐ Start after created

Advanced ☐
Back
Finish

Il faudra ensuite lancer la machine et configurer Debian. Il peut être judicieux de créer une template pour cet iso afin de gagner du temps car nous pouvons cloner des machines.

Modifions le nom de la machine :

```
nano /etc/hostname
```

```
SRV-DHCP.technova.local
```

```
nano /etc/hosts
```

```
127.0.0.1    localhost
192.168.30.5 SRV-DHCP.technova.local SRV-DHCP
```

⚠ : Veuillez bien respecter le plan d'adressage.

## Sous partie 2 : Configuration du DHCP

Nous allons commencer par installer le service. Si besoin il faudra ajouter 8.8.8.8 comme DNS dans resolv.conf

```
apt update
apt install isc-dhcp-server -y
```

Il peut y avoir une ou plusieurs erreurs mais cela n'est pas important.

Nous allons ensuite éditer le fichier de configuration :

```
nano /etc/dhcp/dhcpd.conf
```

- 1) Dans "option domain-name" nous allons devoir mettre le nom de notre domaine. Notre domaine est "technova.local"
- 2) Dans "option domain-name-servers" nous devons ajouter l'adresse ip de la machine serveur DNS. Nous rentrons alors "192.168.30.1"
- 3) Le "default-lease-time" correspond à la durée du bail DHCP par défaut. Il s'agit de la durée pendant laquelle le client peut utiliser l'adresse IP qui lui a été affectée.
- 4) Le "max-lease-time" correspond à la valeur pour le temps maximal du bail DHCP.
- 5) Il faudra décommenter le "authoritative" ligne 21. Cela indique si le serveur DHCP est le serveur officiel du réseau. C'est ce que nous voulons.
- 6) Nous allons maintenant passer aux déclarations des adresses IP. Rendons nous ligne 40. Nous avons un exemple de déclaration en mode commenté, nous allons nous en servir de modèle.

Le fichier devra être configuré comme ceci :

```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# option definitions common to all supported networks...
option domain-name "192.168.30.1";
option domain-name-servers technova.local;

default-lease-time 600;
max-lease-time 7200;
```

```
# The ddns-updates-style parameter controls whether or not the server
will
# attempt to do a DNS update when a lease is confirmed. We default to
the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.

#subnet 10.254.239.0 netmask 255.255.255.224 {
#  range 10.254.239.10 10.254.239.20;
#  option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
#}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#  range dynamic-bootp 10.254.239.40 10.254.239.60;
#  option broadcast-address 10.254.239.31;
#  option routers rtr-239-32-1.example.org;
#}

subnet 192.168.10.0 netmask 255.255.255.0 {
    range 192.168.10.50 192.168.10.200;
    option routers 192.168.10.254;
}

subnet 192.168.20.0 netmask 255.255.255.0 {
```



```
range 192.168.20.50 192.168.20.200;
option routers 192.168.20.254;
option domain-name-servers 192.168.30.1;
}

subnet 192.168.30.0 netmask 255.255.255.0 {
range 192.168.30.150 192.168.30.200;
option routers 192.168.30.254;
option domain-name-servers 192.168.30.1;
}

subnet 192.168.50.0 netmask 255.255.255.0 {
range 192.168.50.100 192.168.50.200;
option routers 192.168.50.254;
option domain-name-servers 192.168.30.1;
}
```

Nous devons également définir le type d'ip que nous voulons utiliser.

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

Ici nous voulons utiliser l'ipv4 donc nous allons ajouter le nom de la carte réseau qui est "ens18". Il faudra également commenter IPV6.

```
GNU nano 8.4 /etc/default/isc-dhcp-server *
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens18"
#INTERFACESv6=""
```

On pourra ensuite redémarrer le service :

```
systemctl restart isc-dhcp-server
```

Notre DHCP est désormais effectif. Nous avons une modification à effectuer sur notre switch.

## Sous partie 3 : Agent relais sur le switch

Nous l'avons déjà fait pour le routeur mais notre switch requiert également cette option.

```
conf t



# 1. Activer le service global de relais
dhcp-relay

# Activation sur le VLAN 10
interface vlan 10
    # L'adresse de ton serveur DHCP physique
    ip helper-address 192.168.30.5
    exit

# Activation sur le VLAN 20
interface vlan 20
    # L'adresse de ton serveur DHCP physique
    ip helper-address 192.168.30.5
    exit

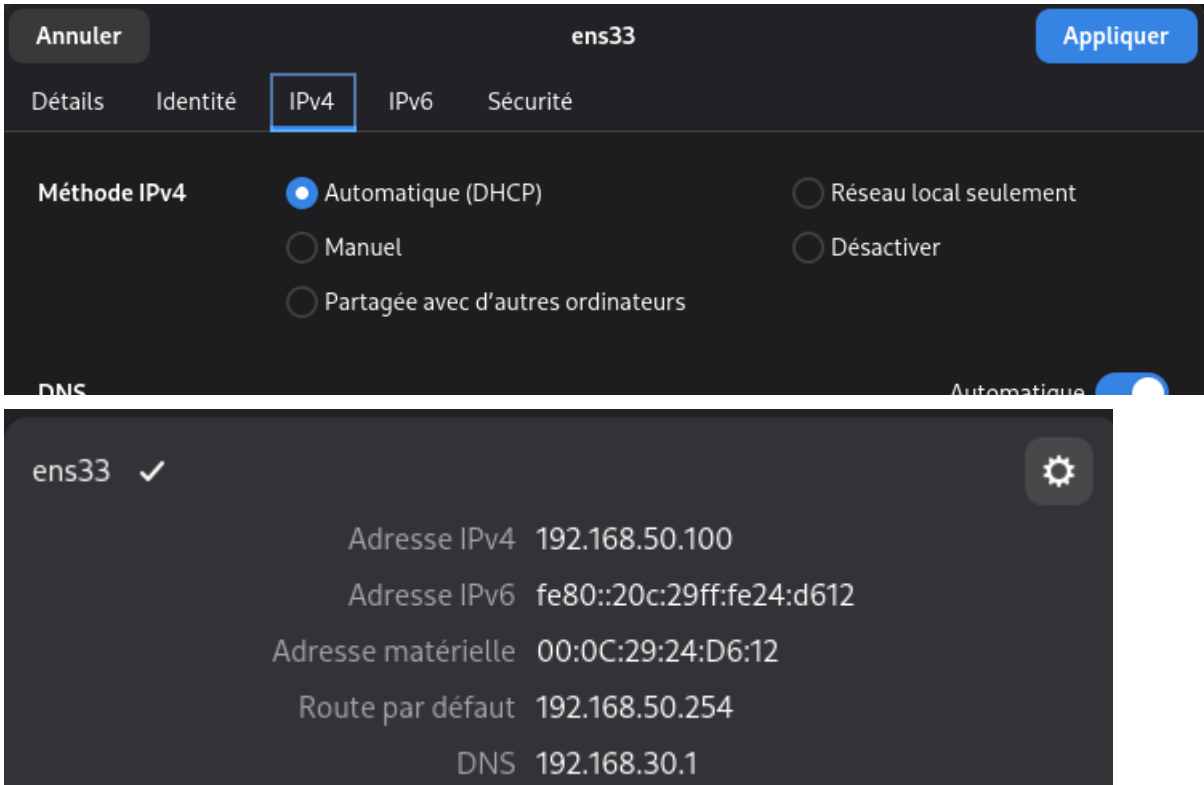
# Activation sur le VLAN 30
interface vlan 20
    # L'adresse de ton serveur DHCP physique
    ip helper-address 192.168.30.5
    exit

# Activation sur le VLAN 50
interface vlan 50
    # L'adresse de ton serveur DHCP physique
    ip helper-address 192.168.30.5
    exit
```

⚠ : Profitez en pour créer tous les vlan :  Mise en place du réseau TechNova et  Mise en place du réseau TechNova . Il faut également leur attribuer une ip en .254. N'oubliez pas de faire un write memory.

## Sous partie 4 : Tests sur TNV-01

Nous pouvons désormais tester notre DHCP sur TNV-01 mais cela doit marcher pour les autres vlans.



The image shows a network configuration window for the interface 'ens33'. At the top, there are buttons for 'Annuler' and 'Appliquer'. Below them are tabs for 'Détails', 'Identité', 'IPv4', 'IPv6', and 'Sécurité', with 'IPv4' currently selected. The 'Méthode IPv4' section has four radio buttons: 'Automatique (DHCP)' (selected), 'Réseau local seulement', 'Manuel', and 'Désactiver'. Below this, there is a 'DNS' section with a dropdown menu set to 'Automatique'. A summary box at the bottom shows the following configuration for 'ens33':  
Adresse IPv4: 192.168.50.100  
Adresse IPv6: fe80::20c:29ff:fe24:d612  
Adresse matérielle: 00:0C:29:24:D6:12  
Route par défaut: 192.168.50.254  
DNS: 192.168.30.1

## Partie 12 - Mise en place d'un serveur DNS avec bind9

Nous allons avoir besoin d'un serveur DNS qui servira à résoudre uniquement l'extérieur du réseau (WAN). Nous aurons également un DNS local par la suite mais nous allons les séparer. Le local sera le primaire qui aura une redirection vers le second, celui que nous allons configurer.

### Sous partie 1 : Création de la machine

Nous allons créer cette machine sur le SRV-02. Nous pouvons cloner le template créé récemment (Debian 13).

Modifions ensuite le nom de la machine

```
nano /etc/hostname
```

```
SRV-DNS.technova.local
```

```
nano /etc/hosts
```

```
127.0.0.1    localhost
192.168.30.2 SRV-DNS.technova.local SRV-DNS
```

## Sous partie 2 : Configuration de bind9

Ensuite il faudra installer le service "bind9"

⚠ : Nous n'avons pas encore de DNS, on pourra donc mettre 8.8.8.8 dans le resolv.conf

```
GNU nano 8.4
# Generated by dhcpd
# /etc/resolv.conf.head can replace this line
# /etc/resolv.conf.tail can replace this line
nameserver 8.8.8.8
```

```
apt update
apt install bind9 -y
```

On peut vérifier que le service soit bien lancé

```
systemctl status bind9
```

```
root@debian:~# systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-12-22 00:14:17 CET; 54s ago
     Invocation: 6efc0a68144be8a7aff3e48a4561de
       Docs: man:named(8)
    Main PID: 1065 (named)
      Status: "running"
        Tasks: 5 (limit: 2303)
       Memory: 9.6M (peak: 11.6M)
          CPU: 65ms
      CGroup: /system.slice/named.service
              └─1065 /usr/sbin/named -f -u bind

déc. 22 00:14:17 debian named[1065]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
déc. 22 00:14:17 debian named[1065]: network unreachable resolving './DNSKEY/IN': 2001:7fd::1#53
déc. 22 00:14:17 debian named[1065]: network unreachable resolving './NS/IN': 2001:7fd::1#53
déc. 22 00:14:17 debian named[1065]: network unreachable resolving './DNSKEY/IN': 2001:500:2::c#53
déc. 22 00:14:17 debian named[1065]: network unreachable resolving './NS/IN': 2001:500:2::c#53
déc. 22 00:14:17 debian named[1065]: network unreachable resolving './DNSKEY/IN': 2001:500:9f::42#53
déc. 22 00:14:17 debian named[1065]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
déc. 22 00:14:17 debian named[1065]: network unreachable resolving './DNSKEY/IN': 2001:500:a8::e#53
déc. 22 00:14:17 debian named[1065]: managed-keys-zone: Initializing automatic trust anchor management for
déc. 22 00:14:17 debian named[1065]: managed-keys-zone: Initializing automatic trust anchor management for
lines 1-23/23 (END)
```

## Sous partie 3 : Configuration des DNS forwarders

Configurons donc ce DNS pour qu'il redirige vers l'extérieur

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

Il faudra ajouter ceci :

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

    dnssec-validation auto;

    listen-on-v6 { any; };

    // --- AJOUT DES FORWARDERS ---
    forwarders {
        8.8.8.8;          // DNS Google
        8.8.4.4;          // DNS Google Secondaire
        1.1.1.1;         // DNS Cloudflare

    };
    // -----

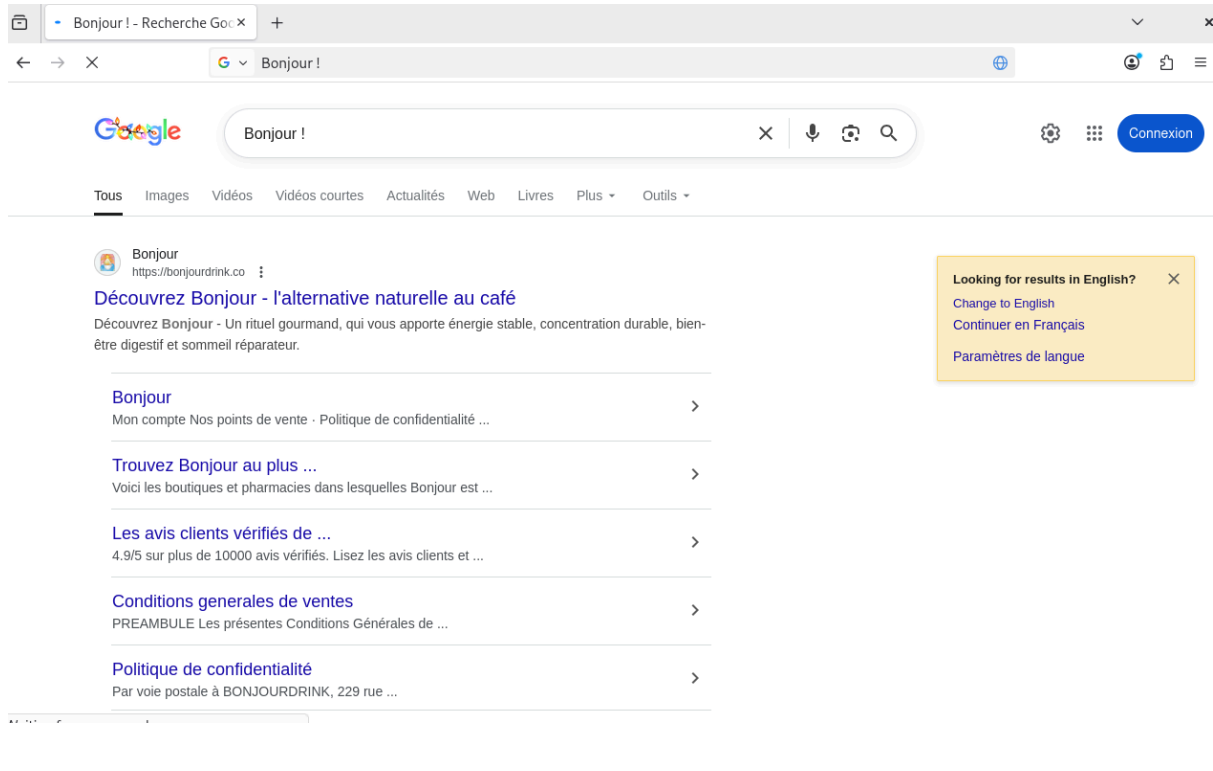
    allow-query { any; };
    recursion yes;
};
```

Il faudra ensuite redémarrer le service :


```
systemctl restart bind9
```

Les clients doivent désormais pouvoir surfer en utilisant le serveur DNS.

⚠ : Il faudra repasser en IP fixe pour le test car celui-ci n'est pas distribué via le DHCP.



## Partie 13 - Mise en place d'un Active Directory

Pour ce serveur plus gourmand, nous allons passer par le SRV-01. N'oubliez pas d'importer l'iso Windows Server :  Iso

### Sous partie 1 : Création de la machine et configuration de Windows

Voici les paramètres de la machine :

Create: Virtual Machine

General OS System Disks CPU Memory Network **Confirm**

Key ↑	Value
bios	ovmf
cores	1
cpu	x86-64-v2-AES
efidisk0	local-lvm:1,efitype=4m,pre-enrolled-keys=1
ide0	local-lvm:80
ide2	local:iso/26100.32230.260111-0550.It_release_svc_refresh_SERVER_EVAL_x64FRE_fr...
machine	q35
memory	4096
name	SRV-AD
net0	e1000,bridge=vmb0,firewall=1
nodename	SRV-01
numa	0
ostype	win11
scsihw	virtio-scsi-single


☐ Start after created

Advanced ☒ **Back** **Finish**

Il faudra configurer Windows avec les options suivantes :

- 1) Système d'exploitation : Windows server 2025 Standard Evaluation (expérience utilisateur)
- 2) Mot de passe : Password1234\*

Vous devrez ensuite arriver sur le bureau Windows.

 : Pensez à renommer la machine et attribuer les adresses correctement. Vous pouvez également ajouter la carte réseau privé hôte.

## Sous partie 2 : Création du domaine technova.local

Commençons: par installer Active Directory

Nous allons ouvrir le "Gestionnaire de serveur" installé nativement sur Windows Server.

Gérer → Ajouter des Rôles et fonctionnalités

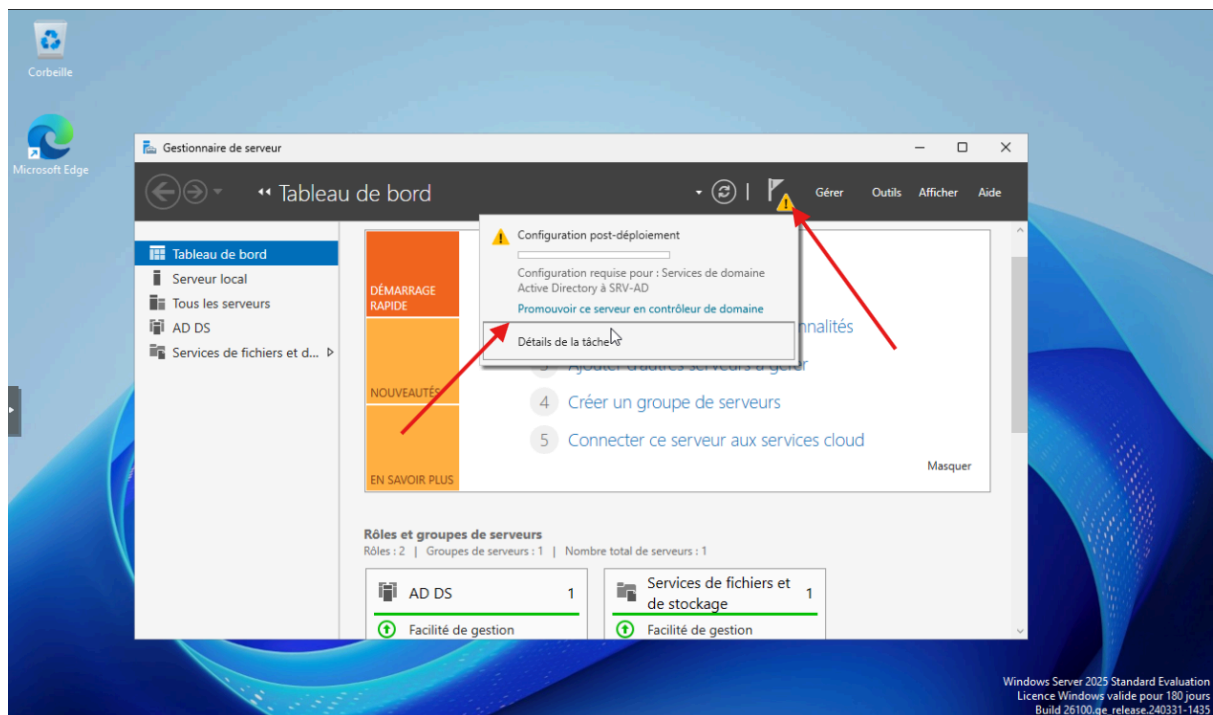
Il faudra respecter les étapes suivantes :

- 1) Suivant
- 2) Suivant

- 3) Suivant
- 4) Sélectionnez "Service de domaine Active Directory"
- 5) Ajouter des fonctionnalités
- 6) Suivants
- 7) Suivants
- 8) Suivants
- 9) Installer

Il faudra ensuite patienter lors de l'installation.

Une fois terminé il faudra promouvoir le serveur en tant que contrôleur de domaine :



Puis :

- 1) Ajouter une nouvelle forêt (nom de racine : technova.local)
- 2) Suivant
- 3) Mot de passe : Password1234
- 4) Suivant
- 5) Suivant
- 6) Suivant
- 7) Suivant
- 8) Suivant
- 9) Installer

Le serveur redémarrera ensuite.

Nous allons ensuite en profiter pour activer le bureau à distance afin de s'y connecter avec "Connexion Bureau à Distance" sur notre PC hôte.



- 1) Ouvrir le "Gestionnaire de serveur"
- 2) Serveur local
- 3) Bureau à distance → Autoriser

## Sous partie 3 : Mise en place du Dynamic DNS (DDNS)

Si nous laissons notre DNS configuré par défaut, il ne pourra résoudre uniquement les machines windows du domaine. Nous devons donc aussi prendre en compte nos autres machines afin qu'elles soient également ajoutées dans les fichiers de zones. Il faudra donc mettre en place un DDNS.


Dans cette architecture, nous allons utiliser les Mises à jour sécurisées (Secure Updates).

1. Windows : Le client le fait nativement via le service "Client DNS".
2. Linux : Nous utiliserons SSSD (System Security Services Daemon). Une fois la machine jointe au domaine, SSSD utilisera son ticket Kerberos pour s'authentifier auprès du DNS et mettre à jour son IP, même si elle est fixe.

Avant de commencer il faut vérifier si le DNS autorise les machines à se mettre à jour.

- 1) Gestionnaire DNS
- 2) Zones de recherche directes
- 3) technova.local
- 4) Clique droit
- 5) Propriété
- 6) Générale
- 7) Mise à jour dynamiques : Sécurisé uniquement

Il va falloir faire pareil pour la résolution inversée après l'avoir créée.

 : Il faut 1 zone inversée par sous réseau. Ceci est donc un exemple pour 192.168.10.0 mais il faudra le faire pour les autres sous réseaux.

- 1) Zones de recherche inversée
- 2) Clique droit
- 3) Nouvelle zone
- 4) Suivant
- 5) Zone principale et cocher la case "enregistrer la zone dans Active Directory" → Suivant
- 6) Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : technova.local → Suivant
- 7) IPV4 → Suivant
- 8) 192.168.10 → Suivant
- 9) N'autoriser que les mises à jour dynamiques sécurisées → Suivant
- 10) Terminer

Nous allons ensuite configurer les machines Debian. C'est la partie la plus technique. Nous allons utiliser realmd et sssd pour joindre le domaine et gérer le DNS.

Nous allons réaliser ceci sur TNV-01 mais il faudra le faire sur chacune des machines Debian.

```
apt update
apt install realmd sssd sssd-tools libnss-sss libpam-sss adcli
packagekit polkitd -y
```

Il faudra ensuite joindre la machine au domaine à l'aide du compte administrateur (Administrateur)

```
/usr/sbin/realmd join -v technova.local -U Administrateur
```

Il faudra ensuite entrer son mot de passe.

Cette ligne nous confirme que ça marche bien

```
* Successfully enrolled machine in realm
```

Nous allons ensuite modifier le fichier de configuration sssd

```
nano /etc/sss/sss.conf
```

Certains éléments sont déjà présents. Le fichier doit ressembler à ceci :

```
[sss]
domains = technova.local
config_file_version = 2
services = nss, pam

[domain/technova.local]
default_shell = /bin/bash
krb5_store_password_if_offline = True
cache_credentials = True
krb5_realm = TECHNOVA.LOCAL
realmd_tags = manages-system joined-with-adcli
id_provider = ad
fallback_homedir = /home/%u@%d
ad_domain = technova.local
use_fully_qualified_names = True
ldap_id_mapping = True
```

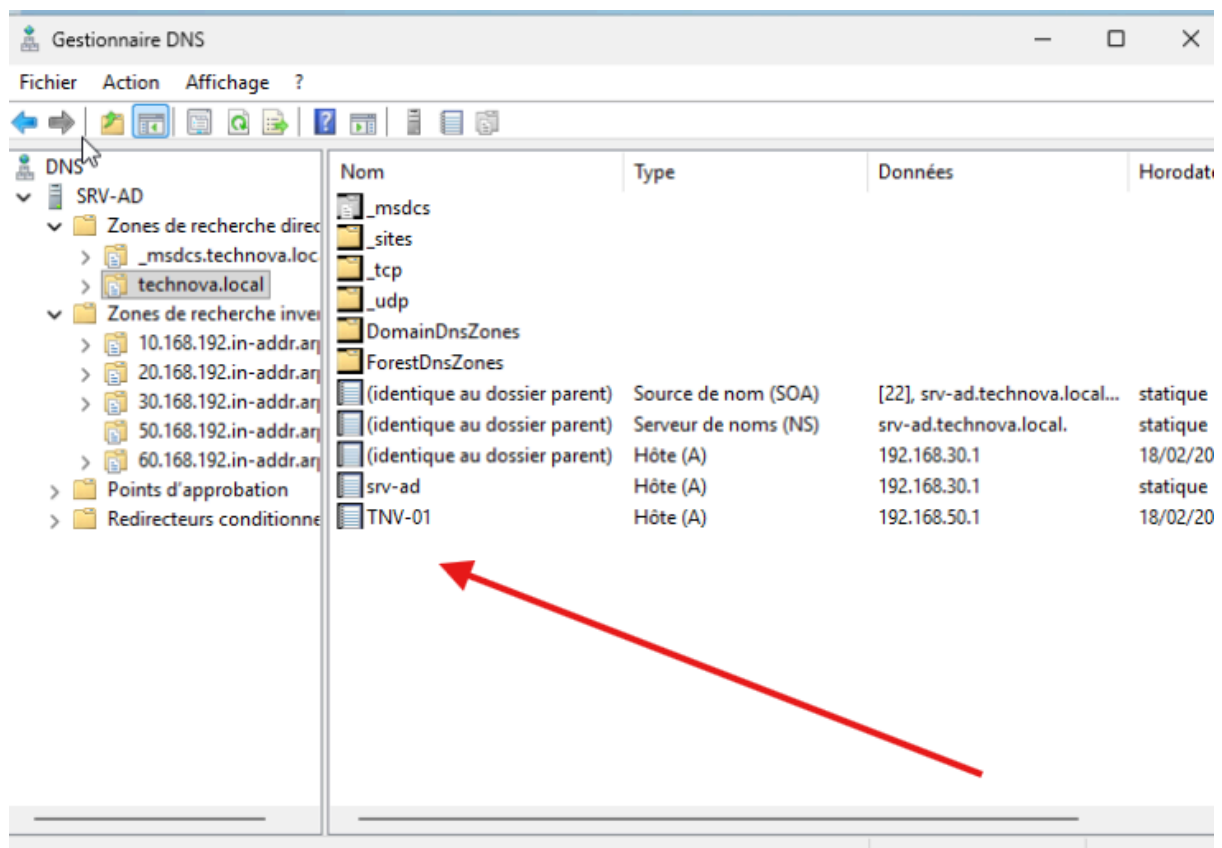
```
# --- CONFIGURATION DDNS ---
access_provider = ad
dyndns_update = true
dyndns_refresh_interval = 43200
dyndns_update_ptr = true
dyndns_ttl = 3600
auth_provider = ad
```

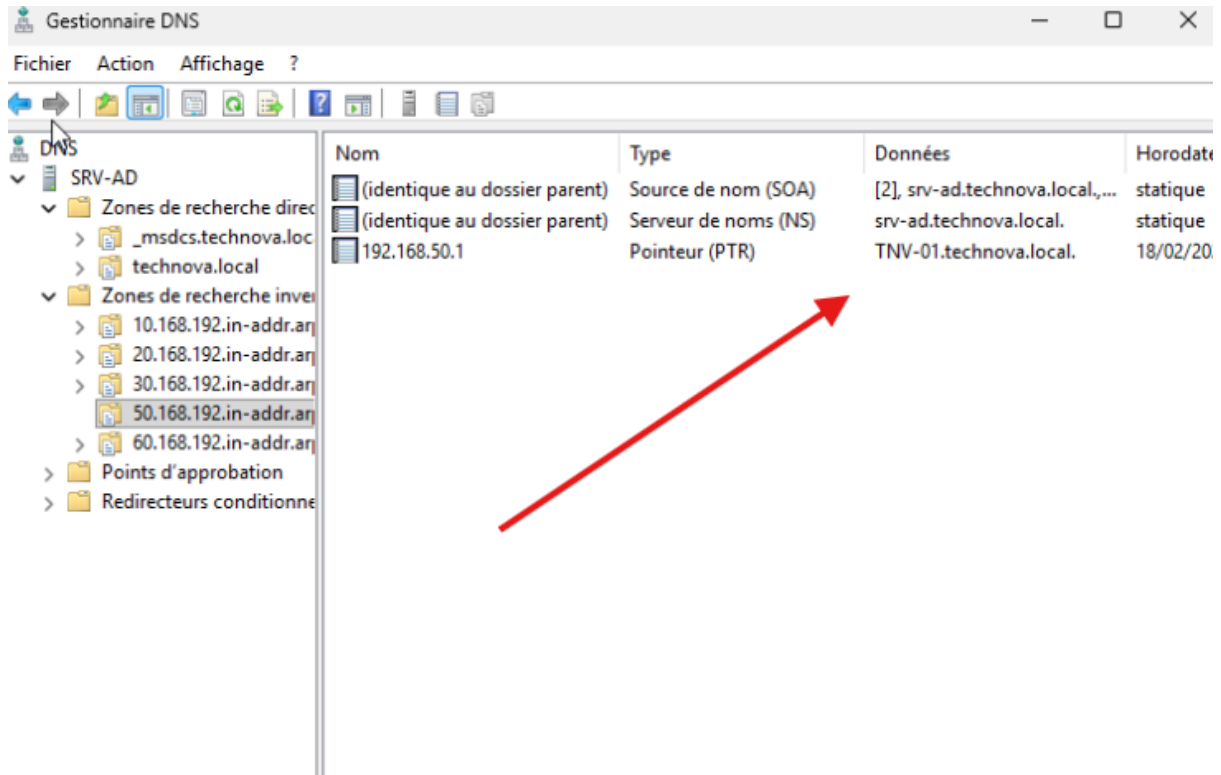
Il faut ensuite appliquer les droits et redémarrer le service

```
systemctl restart sssd
```

⚠ : Veuillez lier toutes les machines au domaine.

Le résultat doit apparaître dans le gestionnaire DNS du contrôleur de domaine.





## Sous partie 4 : Ajout du Forwarder pour résoudre le WAN

Comme évoqué précédemment, il nous faut un DNS pour résoudre le WAN.

- 1) Ouvrir le "Gestionnaire DNS"
- 2) Cliquez droit sur "SRV-AD"
- 3) Propriétés
- 4) Redirecteurs
- 5) Modifier
- 6) 192.168.30.2
- 7) Ok

Pour vérifier on peut faire la commande suivante :

```
nslookup google.fr 192.168.30.1
```

```
C:\Users\Administrateur>nslookup google.fr 192.168.30.1
Serveur : SRV-AD.technova.local
Address: 192.168.30.1

Réponse ne faisant pas autorité :
Nom : google.fr
Addresses: 2a00:1450:4007:81c::2003
142.250.75.227
```

"Réponse ne faisant pas autorité" signifie que l'AD ne gère pas google.fr (ce qui est normal) et qu'il est allé chercher la réponse ailleurs (via le redirecteur).

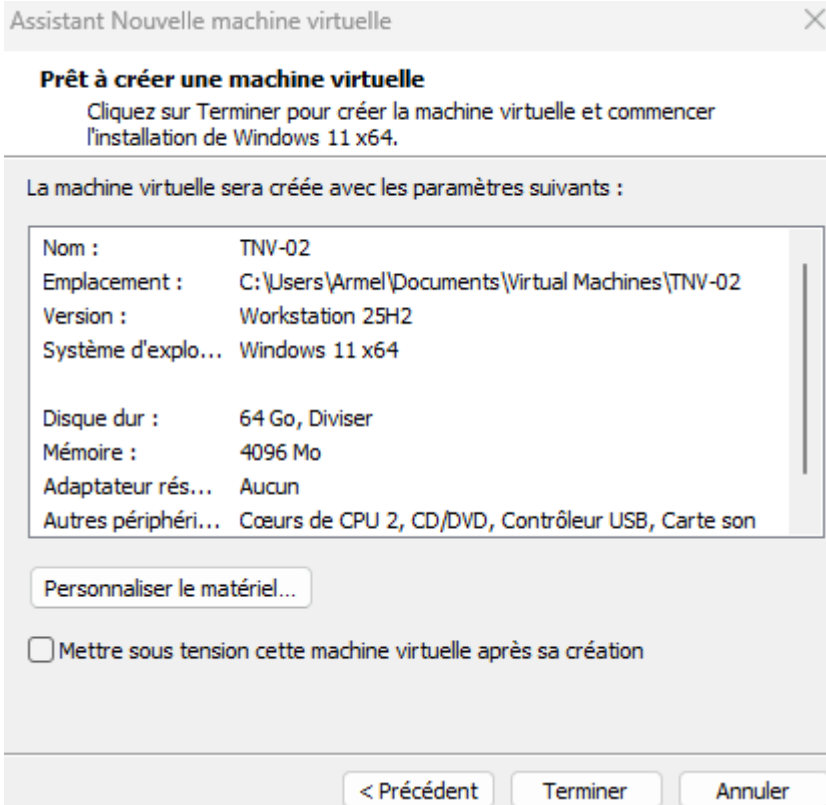
---

## Partie 14 - Mise en place des PC client Windows 11

### Sous partie 1 : Création de la machine

Commencez par récupérer l'iso :  Iso

Ensuite voici la configuration de la machine :



Assistant Nouvelle machine virtuelle

**Prêt à créer une machine virtuelle**

Cliquez sur Terminer pour créer la machine virtuelle et commencer l'installation de Windows 11 x64.

La machine virtuelle sera créée avec les paramètres suivants :

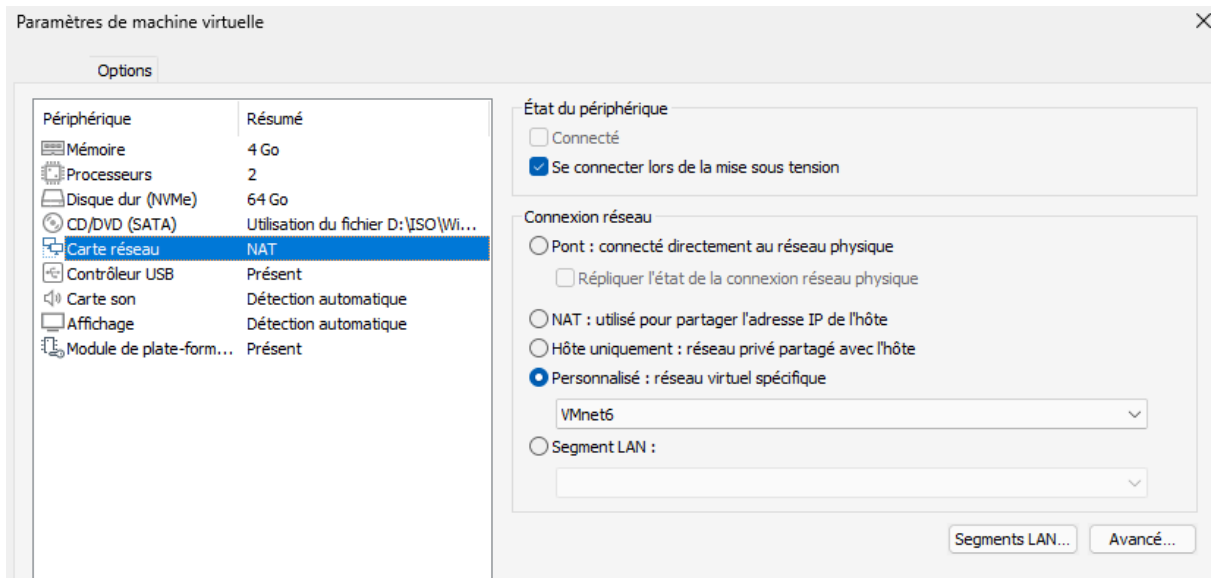
Nom :	TNV-02
Emplacement :	C:\Users\Armel\Documents\Virtual Machines\TNV-02
Version :	Workstation 25H2
Système d'explo...	Windows 11 x64
Disque dur :	64 Go, Diviser
Mémoire :	4096 Mo
Adaptateur rés...	Aucun
Autres périphéri...	Cœurs de CPU 2, CD/DVD, Contrôleur USB, Carte son

Personnaliser le matériel...

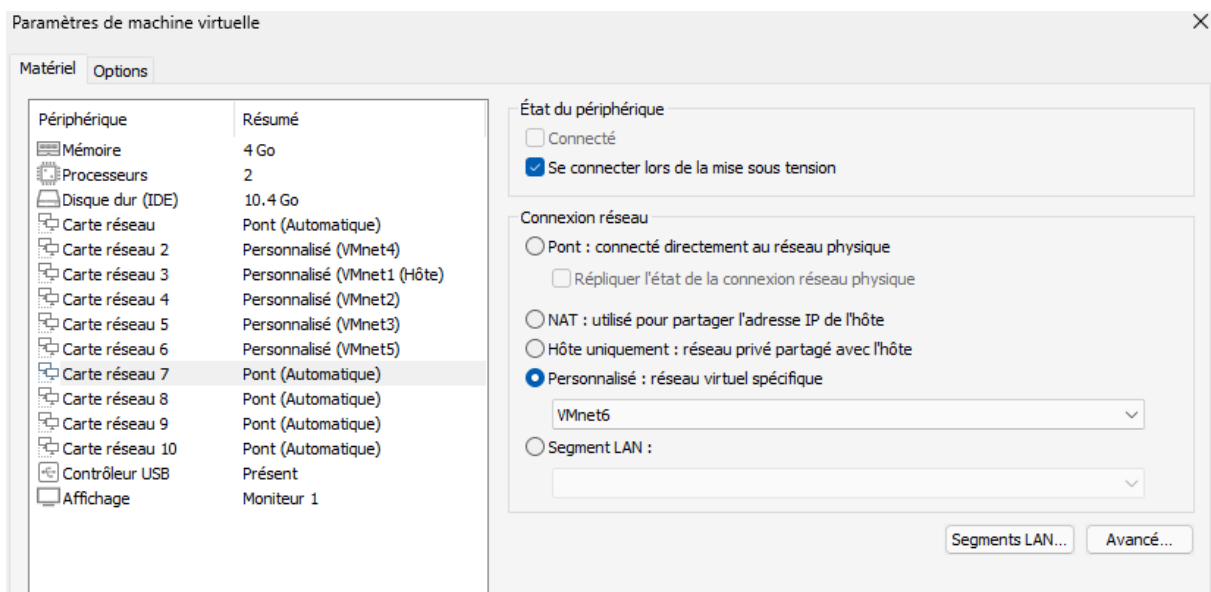
☐ Mettre sous tension cette machine virtuelle après sa création

< Précédent Terminer Annuler

Voici les paramètres réseau de la machine :



Voici la modification à apporter sur le switch



```
int 1/1/6
no sh
no routing
vlan access 20
exit

write memory
```

Vous pourrez désormais démarrer le machine

## Sous partie 2 : Configuration de Windows

Voici les étapes à respecter :

- 1) Image à installer : Windows 11 Professionnel
- 2) Pour réaliser l'installation sans connexion : Shift F10 / start ms-cxh:localonly
- 3) Nom d'utilisateur : admin
- 4) Mot de passe : Password1234
- 5) Une fois sur le bureau il faudra renommer la machine avec : TNV-02
- 6) Il faudra également joindre le domaine technova.local puis redémarrer le poste.

⚠ : Il faudra réaliser l'ensemble des étapes précédentes pour les 3 PC Clients (TNV-02, TNV-03, TNV-04). Attention à bien prendre en compte les changements sur le switch.

---

## Partie 15 - Mise en place d'un serveur web intranet via apache2

### Sous partie 1 : Création et configuration de la machine

Nous allons créer la machine sur SRV-02. Vous pouvez cloner la template Debian 13.



TECHNOVA

Clone VM Template 100

Target node: SRV-02

VM ID: 103

Name: SRV-WEB

Resource Pool:

Mode: Full Clone

Target Storage: Same as source

Format: QEMU image format (qcow2)

Help

Clone

- 1) Renommez correctement la machine
- 2) Définissez les bonnes adresses.
- 3) Joindre la machine au domaine.

## Sous partie 2 : Installation et configuration d'apache2

```
apt update
apt install apache2 -y
```

Nous allons ensuite éditer le fichier html de base, le supprimer et ensuite insérer le code de notre site :

```
nano /var/www/html/index.html
```

## Puis

```
<!DOCTYPE html>
<html lang="fr">
<head>
  <meta charset="UTF-8">
  <title>Intranet Technova</title>
  <style>
    /* --- STYLE GENERAL --- */
    body {
      font-family: 'Segoe UI', sans-serif;
      margin: 0;
      padding: 0;
      background-color: #f4f4f9;
    }
  </style>
</head>
<body>
```



```
/* --- HEADER --- */
header {
  background-color: #005f73; /* Bleu Technova */
  color: white;
  padding: 0 20px;
  display: flex;
  justify-content: space-between;
  align-items: center;
  height: 60px;
}

.logo {
  font-size: 20px;
  font-weight: bold;
}

/* --- MENU NAVIGATION --- */
nav ul {
  list-style: none;
  display: flex;
  gap: 20px;
  margin: 0;
  padding: 0;
}

nav a {
  color: white;
  text-decoration: none;
  font-size: 14px;
  text-transform: uppercase;
  padding: 8px 12px;
  border-radius: 4px;
  transition: background 0.3s;
}

nav a:hover {
  background-color: #0a9396;
}

/* --- CONTENU PRINCIPAL --- */
main {
  padding: 40px;
  max-width: 800px;
  margin: 0 auto;
}
```

```
}

/* --- BOITE OUTIL --- */
.tool-box {
    background: white;
    padding: 30px;
    border-radius: 8px;
    box-shadow: 0 4px 6px rgba(0,0,0,0.1);
    border-top: 5px solid #0a9396; /* Vert Technova */
}

h2 { margin-top: 0; color: #333; }
p { color: #666; }

/* Le bouton */
button {
    background-color: #005f73;
    color: white;
    border: none;
    padding: 10px 20px;
    font-size: 16px;
    cursor: pointer;
    border-radius: 4px;
    margin-top: 10px;
    width: 100%; /* Bouton large */
}

button:hover { background-color: #0a9396; }

/* La zone de résultat */
#password-display {
    margin-top: 20px;
    padding: 15px;
    background-color: #e9ecef;
    border: 1px solid #ccc;
    font-family: 'Courier New', monospace;
    font-size: 20px;
    font-weight: bold;
    color: #333;
    text-align: center;
    letter-spacing: 2px;
}

</style>
</head>
```

```
<body>

  <header>
    <div class="logo">TECHNOVA</div>

    <nav>
      <ul>
        <li><a href="#">Générateur MDP</a></li>
      </ul>
    </nav>
  </header>

  <main>

    <div class="tool-box">
      <h2>🔒 Création de mot de passe</h2>
      <p>Générez un mot de passe sécurisé pour les nouveaux collaborateurs.</p>

      <button onclick="genererMdp()">Générer maintenant</button>

      <div id="password-display">...</div>
    </div>

  </main>

  <script>
    function genererMdp() {
      const chars =
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*";
      ;

      let password = "";
      const length = 12;

      for (let i = 0; i < length; i++) {
        const randomNumber = Math.floor(Math.random() *
chars.length);
        password += chars.substring(randomNumber, randomNumber +
1);
      }

      document.getElementById("password-display").innerText =
password;
    }
  </script>
```

```
</body>  
</html>
```

Le site est désormais opérationnel !

