



Rapport de projet

Mise en place d'une infrastructure réseau et de services pour l'entreprise SoCoDevI

NERON DE AZEVEDO Aloïs – SIO 2

Table des matières

- Introduction
- Objectifs du projet
- Planning prévisionnel du projet
- Description des étapes du projet (Architecture réseaux, la mise en place avec les tests et les problèmes rencontrés avec solutions)
 1. Étape 1 : Redondance de l'accès Internet
 2. Étape 2 : Mise en place d'un NAS (TrueNAS)
 3. Étape 3 : Configuration automatique des postes de travail grâce aux GPO
 4. Étape 4 : Gestion du parc informatique avec GLPI
 5. Étape 5 : Clonage des postes de travail (Clonezilla)
 6. Étape 6 : Hébergement des serveurs dans le cloud (ESXi)
 7. Étape 7 : Rédaction du rapport
- Planning réel du projet
- Références

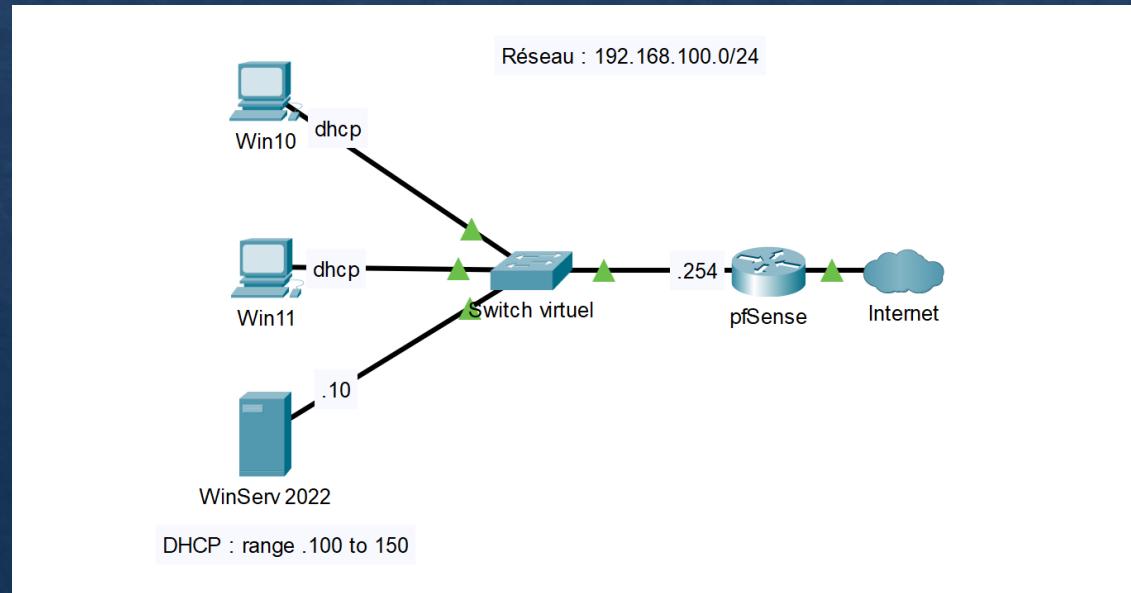
Introduction

Ce projet a pour objectif de moderniser et sécuriser l'infrastructure informatique de SOCODEVI. Il comprend la mise en place d'une redondance pour les accès Internet, la création d'un système de stockage réseau (NAS), l'automatisation de la configuration des postes de travail, ainsi que la gestion centralisée du parc informatique. Le projet inclut également la migration des serveurs vers un prestataire de cloud sécurisé, tout en maintenant une connexion fiable avec les bureaux via un VPN.

Introduction

A savoir :

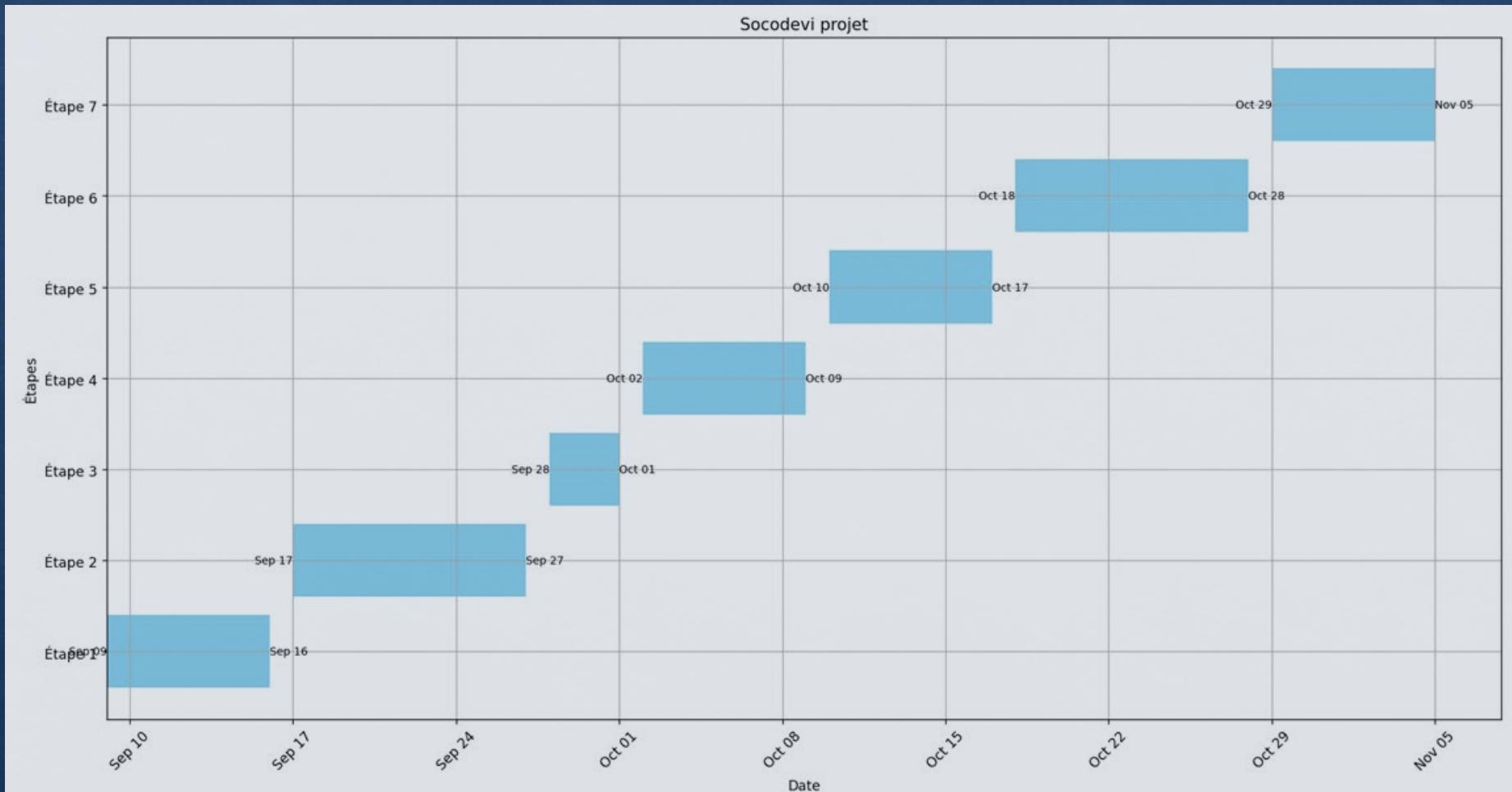
Tout le projet est basé sur une infrastructure dite « base » sur laquelle l'AD est déjà configurer. Sans rentrer dans le détail celui-ci possède le DNS de google en principal et celui du lycée en secondaire pour des raisons de facilité à travailler en dehors du lycée. Le pool DHCP est aussi configuré pour les machines clientes avec l'attribution automatique de la passerelle et du DNS.



Objectifs du projet

- 1. Améliorer la disponibilité** des services réseau en mettant en place une redondance des accès Internet via deux pare-feu pfSense.
- 2. Centraliser et sécuriser les données** en déployant un système de stockage réseau (NAS) avec TrueNAS, synchronisé avec Active Directory.
- 3. Automatiser la gestion des postes de travail** grâce à des stratégies de groupe sur Windows Server, facilitant l'installation de logiciels et la configuration des utilisateurs.
- 4. Gérer efficacement le parc informatique** avec GLPI pour un inventaire automatisé des équipements.
- 5. Déployer rapidement les postes de travail** à l'aide de Clonezilla pour cloner une configuration standardisée.
- 6. Migrer les serveurs vers un prestataire de cloud** tout en assurant une connexion sécurisée par VPN entre les serveurs hébergés et les bureaux de l'entreprise.

Planning prévisionnel



Planning réel

Etape 1 : 9 - 12 septembre – 4j

Etape 2 : 12 - 15 septembre – 4j

Etape 3 : 19 - 22 septembre – 4j

Etape 4 : 10 - 13 Octobre – 4j

Etape 5 : 30 septembre – 1 Octobre 2j

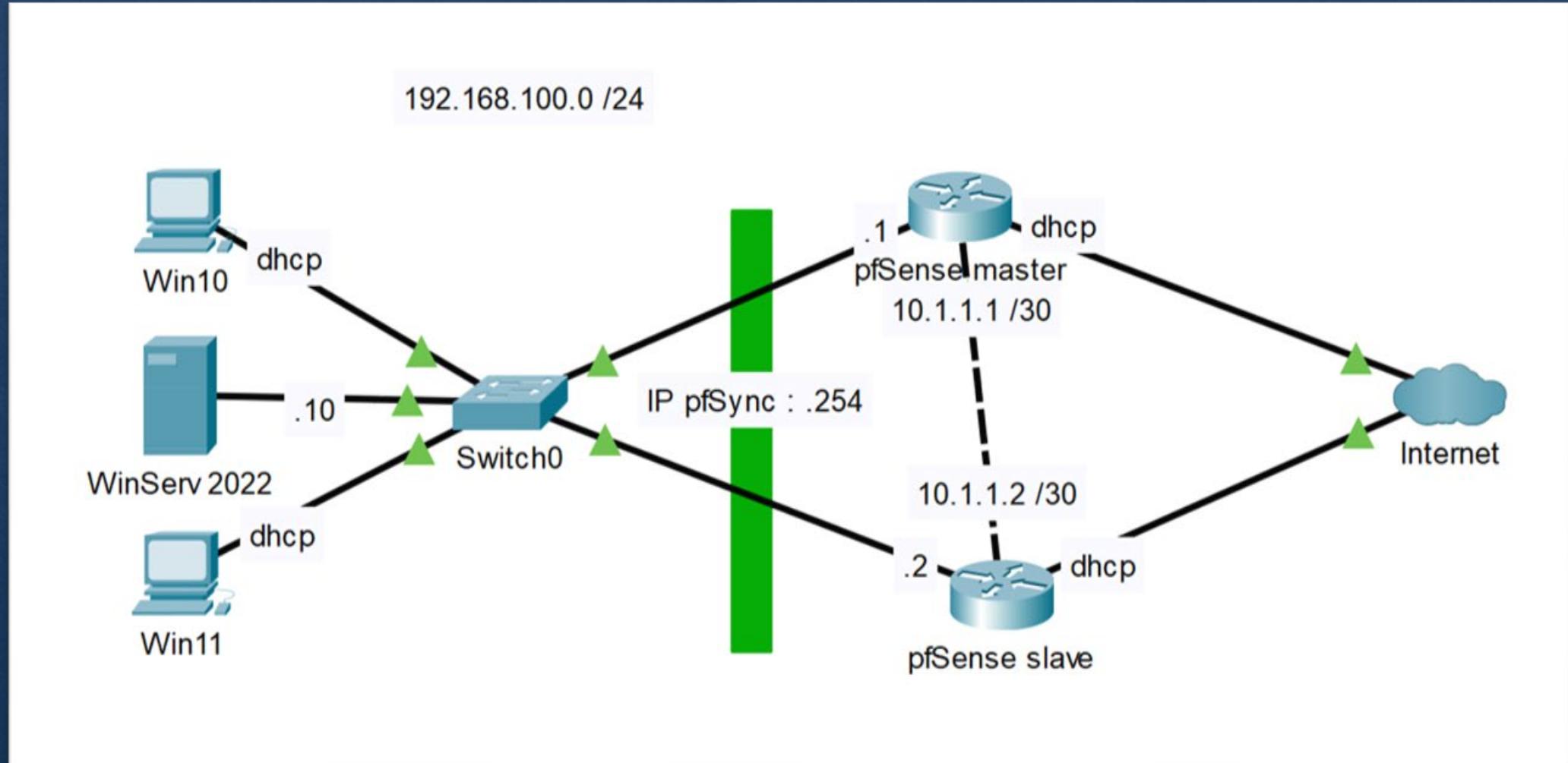
Etape 6 : 7 - 14 Novembre – 8j

Etape 7 : 9 septembre au 29 Novembre

Etape 1 – Redondance pfSense



Etape 1 – Architecture réseau



Etape 1 – Mise en place

Principe de fonctionnement

En cas de défaillance de pfSense principal (.1), pfSense secondaire (.2) prend le relais sans aucune interruption de service. La bascule est totalement transparente.

Afin d'assurer la réplication du routeur principale, 3 éléments doivent être configurés :

- **CARP (Common Address Redundancy Protocol)** est un protocole permettant à plusieurs hôtes présents sur un même réseau de partager une adresse IP.
- **pfsync** est un protocole permettant de synchroniser entre deux serveurs pfSense l'état des connexions en cours
- **XML-RPC** est un protocole permettant la réplication de données d'un serveur vers un autre.

Etape 1 – Mise en place | CARP

Nous allons commencer par configurer les adresses virtuelles dans firewall puis **Virtual IPs**. Ensuite nous cliquerons sur « +add » pour ajouter l'IP virtuel.

The screenshot shows a configuration interface with a sidebar on the left containing the following items:

- Firewall ▾ (highlighted with a red box)
- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs (highlighted with a red box)

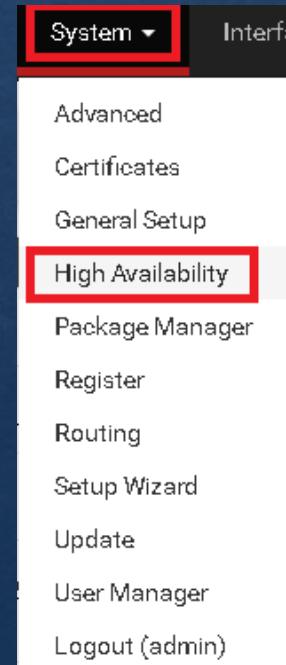
The main area is titled "Edit Virtual IP". It includes the following fields:

- Type: IP Alias CARP Proxy ARP Other
- Interface: LAN
- Address type: Single address
- Address(es): 192.168.100.254 / 24
- Virtual IP Password: Enter the VHID group password. Confirm
- VHID Group: 1
- Advertising frequency: Base (1) Skew (0)
- Description: A description may be entered here for administrative reference (not parsed).

Etape 1 – Mise en place | pfSync

WAN (wan)	-> em0	-> v4/DHCP4: 192.168.15.77/24
LAN (lan)	-> em1	-> v4: 192.168.100.1/24
PFSYNC (opt1)	-> em2	-> v4: 10.1.1.1/30
WAN (wan)	-> em0	-> v4/DHCP4: 192.168.15.75/24
LAN (lan)	-> em1	-> v4: 192.168.100.2/24
PFSYNC (opt1)	-> em2	-> v4: 10.1.1.2/30

Pour configurer pfSync nous allons rajouter une 3ème interface aux deux pfSense pour les relier directement entre eux même si cela n'est pas nécessaire.



Ensuite nous pouvons retourner sur nos configurations web dans **system** puis **High availability**.

Etape 1 – Mise en place

Sur le routeur principal

State Synchronization Settings (pfsync)

Synchronize states	<input checked="" type="checkbox"/> pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
Synchronize Interface	PFSYNC <input type="button" value="▼"/>
	If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.
Filter Host ID	1bf11163 <input type="text"/>
	Custom pf host identifier carried in state data to uniquely identify which host created a firewall state. Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abedef01). Each node participating in state synchronization must have a different ID.
pfsync Synchronize Peer IP	10.1.1.2 <input type="text"/>
	Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Sur le routeur secondaire

pfsync Synchronize Peer IP	10.1.1.1 <input type="text"/>
	Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Etape 1 – Mise en place | XML RPC

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP: 10.1.1.2
Enter the IP address of the firewall to which the selected configuration sections should be synchronized.
XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username: admin
Enter the webConfigurator username of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password: Confirm:
Enter the webConfigurator password of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and password option on backup cluster members!

Synchronize admin: synchronize admin accounts and autoupdate sync password.
By default, the admin account does not synchronize, and each node may have a different admin password.
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Select options to sync:

- User manager users and groups
- Authentication servers (e.g. LDAP, RADIUS)
- Certificate Authorities, Certificates, and Certificate Revocation Lists
- Firewall rules
- Firewall schedules
- Firewall aliases
- NAT configuration
- IPsec configuration
- OpenVPN configuration (Implies CA/Cert/CRL Sync)
- DHCP Server settings
- DHCP Relay settings
- DHCPv6 Relay settings
- WOL Server settings
- Static Route configuration
- Virtual IPs
- Traffic Shaper configuration
- Traffic Shaper Limiters configuration
- DNS Forwarder and DNS Resolver configurations
- Captive Portal

Toggle All

En dessous de la configuration pfSync nous avons la configuration du protocole XML RPC qui est à configurer **uniquement** sur le pfSense principal. Nous n'allons pas synchronisé le compte admin pour une meilleure sécurité.

Etape 1 – Mise en place

Enfin il ne nous reste plus qu'à gérer le firewall pour autorisé la LAN à aller sur le routeur

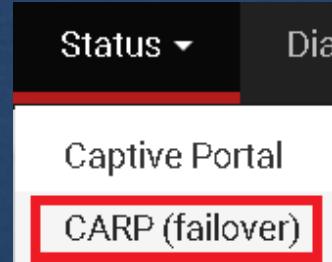
Grâce à la synchronisation des deux pfSense faites précédemment il n'est pas nécessaire de faire la configuration sur le routeur secondaire. La règle est synchronisée automatiquement

Edit Firewall Rule

Action	Pass				
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.					
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.				
Interface	LAN				
Choose the interface from which packets must come to match this rule.					
Address Family	IPv4				
Select the Internet Protocol version this rule applies to.					
Protocol	Any				
Choose which IP protocol this rule should match.					
Source					
Source	<input type="checkbox"/> Invert match	LAN subnets	Source Address	/	
Destination					
Destination	<input type="checkbox"/> Invert match	PFSYNC subnets	Destination Address	Activer Windows Accédez aux paramètres	

Etape 1 – Mise en place

On peut vérifier le statut de chaque pfSense dans l'onglet « status » puis CARP



Principal

CARP Status			
Interface and VHID	Virtual IP Address	Description	Status
LAN@1	192.168.100.254/24		MASTER

Secondaire

CARP Status			
Interface and VHID	Virtual IP Address	Description	Status
LAN@1	192.168.100.254/24		BACKUP

Etape 1 – Tests

pfSense principal : 192.168.100.1

pfSense secondaire : 192.168.100.2

A partir d'une machine cliente, nous lançons un **tracert** pour voir où passe notre client pour sortir du réseau.

Les deux routeurs en fonctionnement

```
C:\Users\win10>tracert youtube.com

Détermination de l'itinéraire vers youtube.com [172.217.19.46]
avec un maximum de 30 sauts :

 1    <1 ms      <1 ms      <1 ms  192.168.100.1
 2      3 ms      2 ms      2 ms  192.168.15.248
 3     27 ms      5 ms      4 ms  192.0.0.1
```

Le routeur principal est éteint

```
C:\Users\win10>tracert youtube.com

Détermination de l'itinéraire vers youtube.com [172.217.19.46]
avec un maximum de 30 sauts :

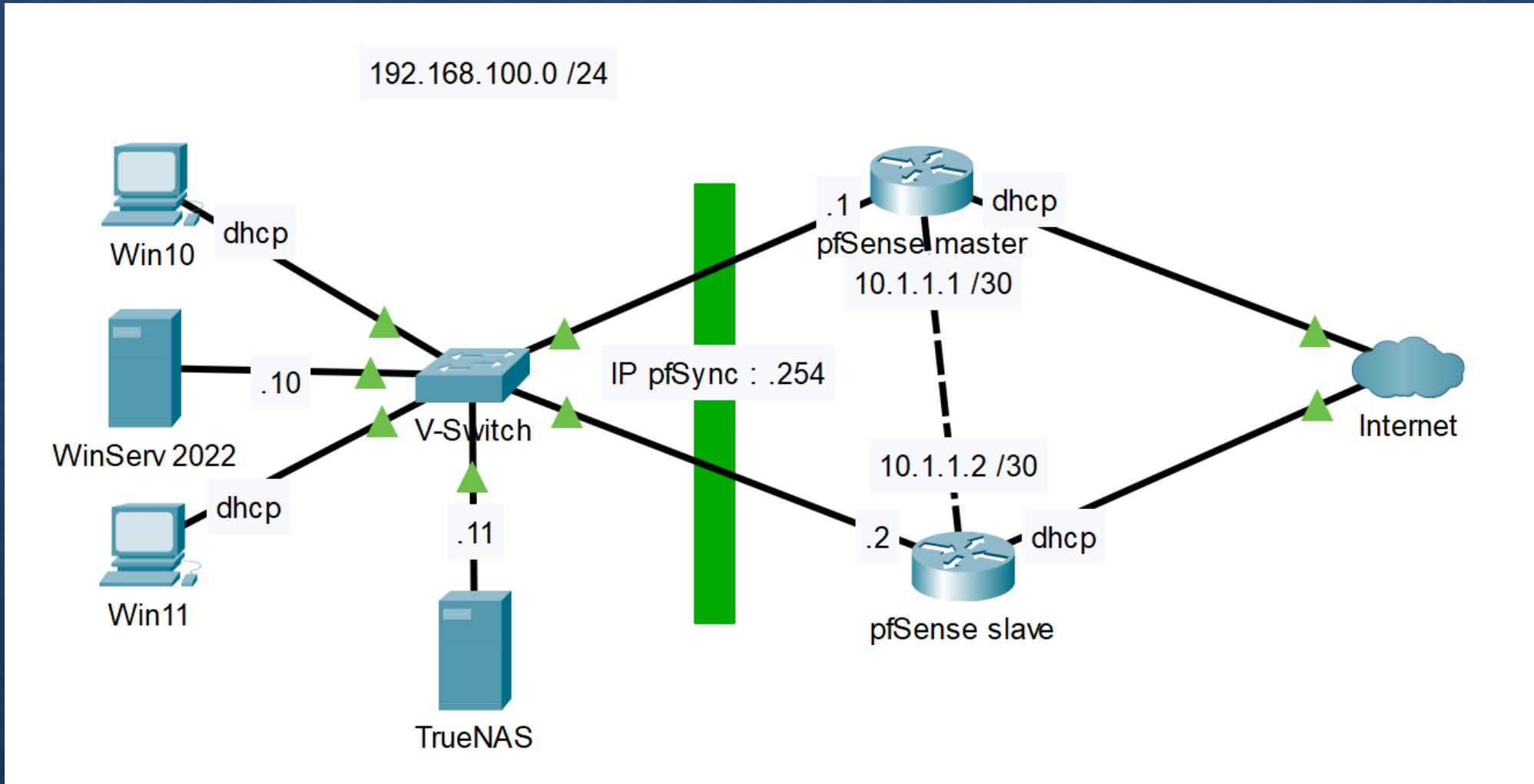
 1      1 ms      <1 ms      <1 ms  192.168.100.2
 2      3 ms      2 ms      2 ms  192.168.15.248
 3     44 ms      4 ms      3 ms  192.0.0.1
```

On constate bien que le routeur secondaire prend le relais instantanément si le principal n'est plus disponible.

Etape 2 – TrueNAS

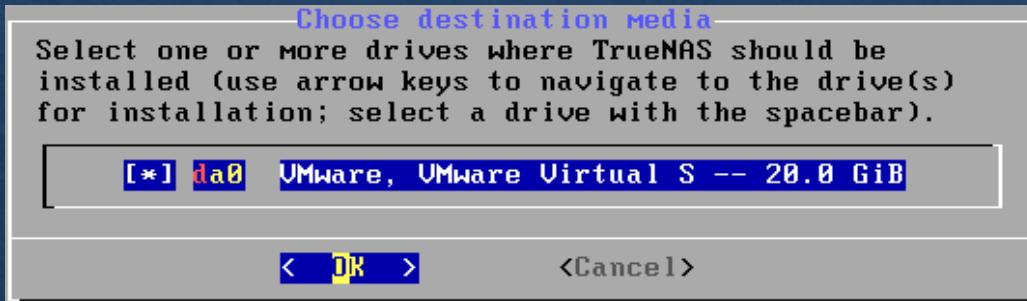
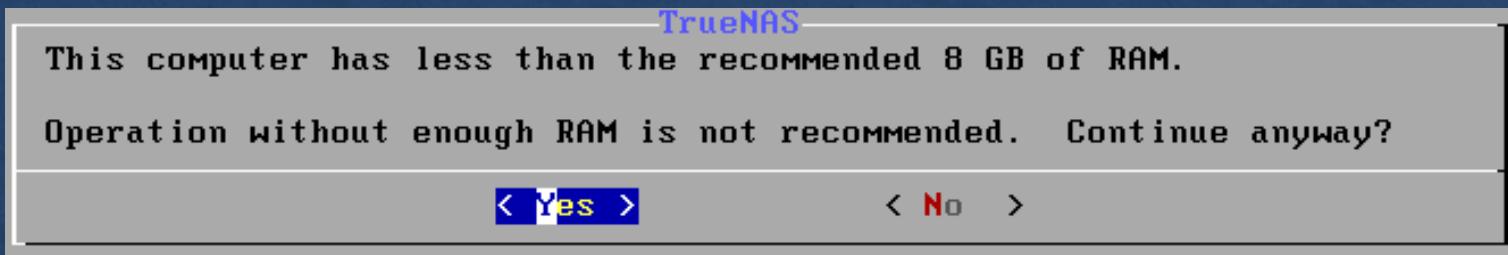


Etape 2 – Architecture réseau

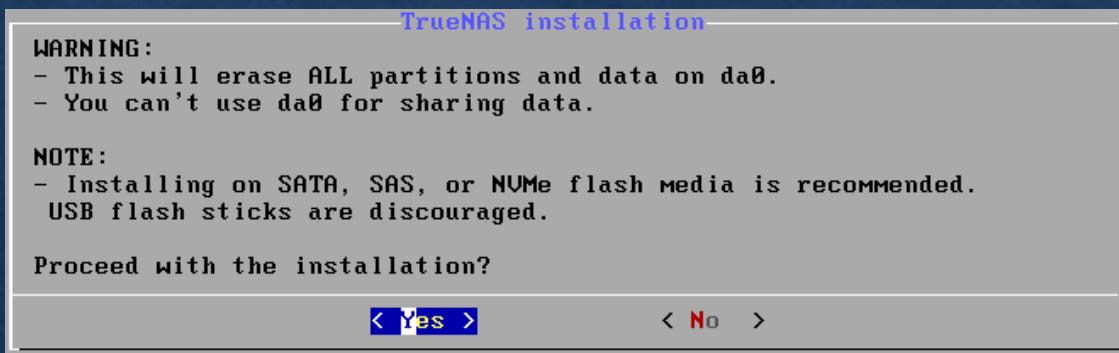


Etape 2 – Mise en place

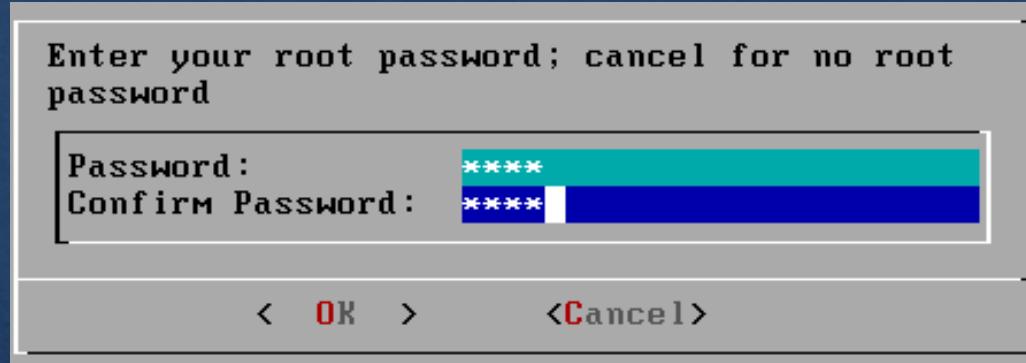
- 1 Install/Upgrade**
- 2 Shell**
- 3 Reboot System**
- 4 Shutdown System**



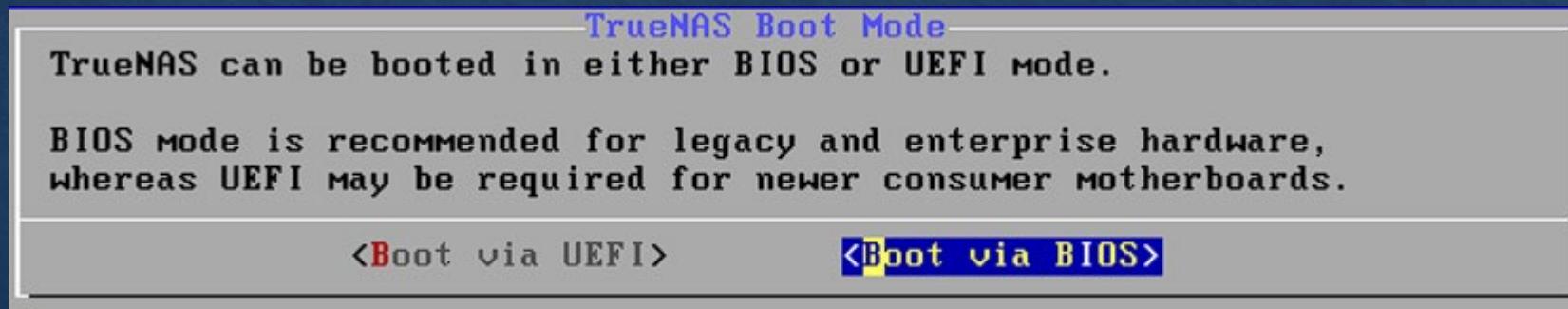
- 1) Install/Upgrade
- 2) Yes
- 3) On appui sur « espace » pour cocher la case puis « ok »
- 4) Yes



Etape 2 – Mise en place



- 5) On met le mot de passe souhaiter
- 6) On boot via le BIOS
- 7) OK



Etape 2 – Mise en place

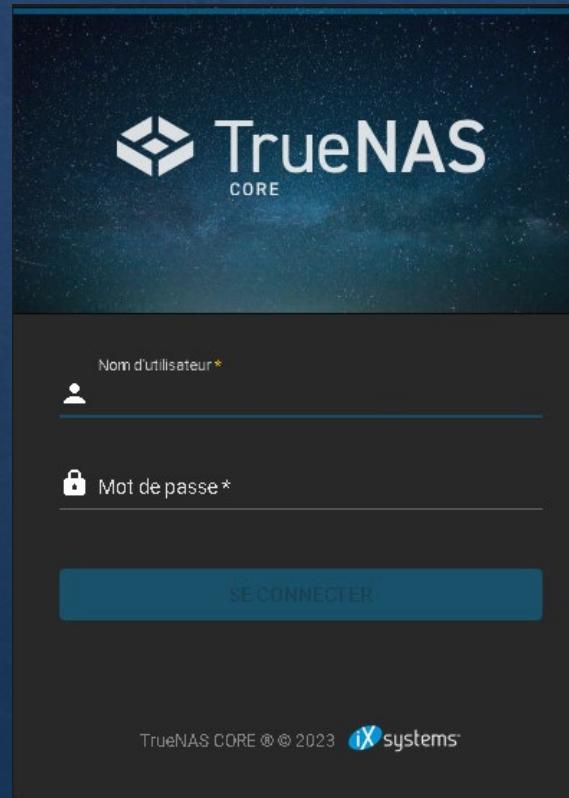
Console setup

-
- 1) Configure Network Interfaces
- 2) Configure Link Aggregation
- 3) Configure VLAN Interface
- 4) Configure Default Route
- 5) Configure Static Routes
- 6) Configure DNS
- 7) Reset Root Password
- 8) Reset Configuration to Defaults
- 9) Shell
- 10) Reboot
- 11) Shut Down

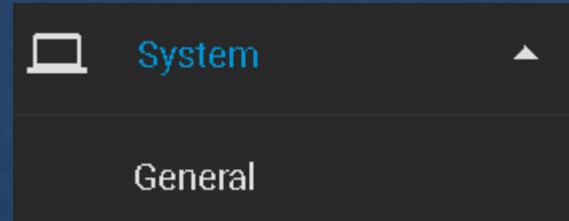
The web user interface is at:

<http://192.168.100.200>
<https://192.168.100.200>

Une fois la machine lancer on y voit différentes options dont l'IP de pour y accéder via l'interface WEB.

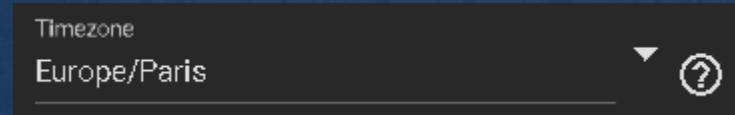


Etape 2 – Mise en place

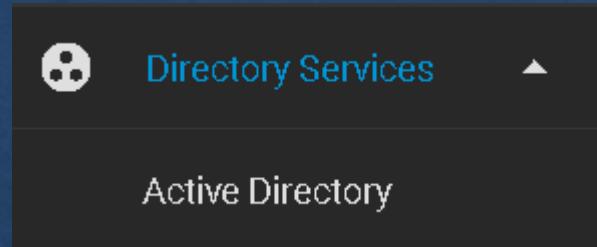


Il est important de changer la time zone car l'entrée de la machine dans le domaine risque de ne pas fonctionner correctement.

Par défaut sur « los angeles »,
nous le mettrons Europe/Paris



Etape 2 – Mise en place



Dans la section « directory services » puis dans active directory nous allons pouvoir mettre notre NAS dans le domaine.

Il suffit de mettre le nom du domaine ainsi que le compte pour se connecter au domaine, dans notre cas celui de l'administrateur.

The screenshot shows a configuration screen for "Domain Credentials". It includes fields for "Domain Name" (SOCODEV1.FR), "Domain Account Name" (administrateur), and "Domain Account Password" (redacted). A checkbox for "Enable (requires password or Kerberos principal)" is checked. At the bottom, there are buttons for "SAVE", "ADVANCED OPTIONS", and "REBUILD DIRECTORY SERVICE CACHE". The "SAVE" button is highlighted with a red border.

Domain Credentials

Domain Name *

SOCODEV1.FR

Domain Account Name *

administrateur

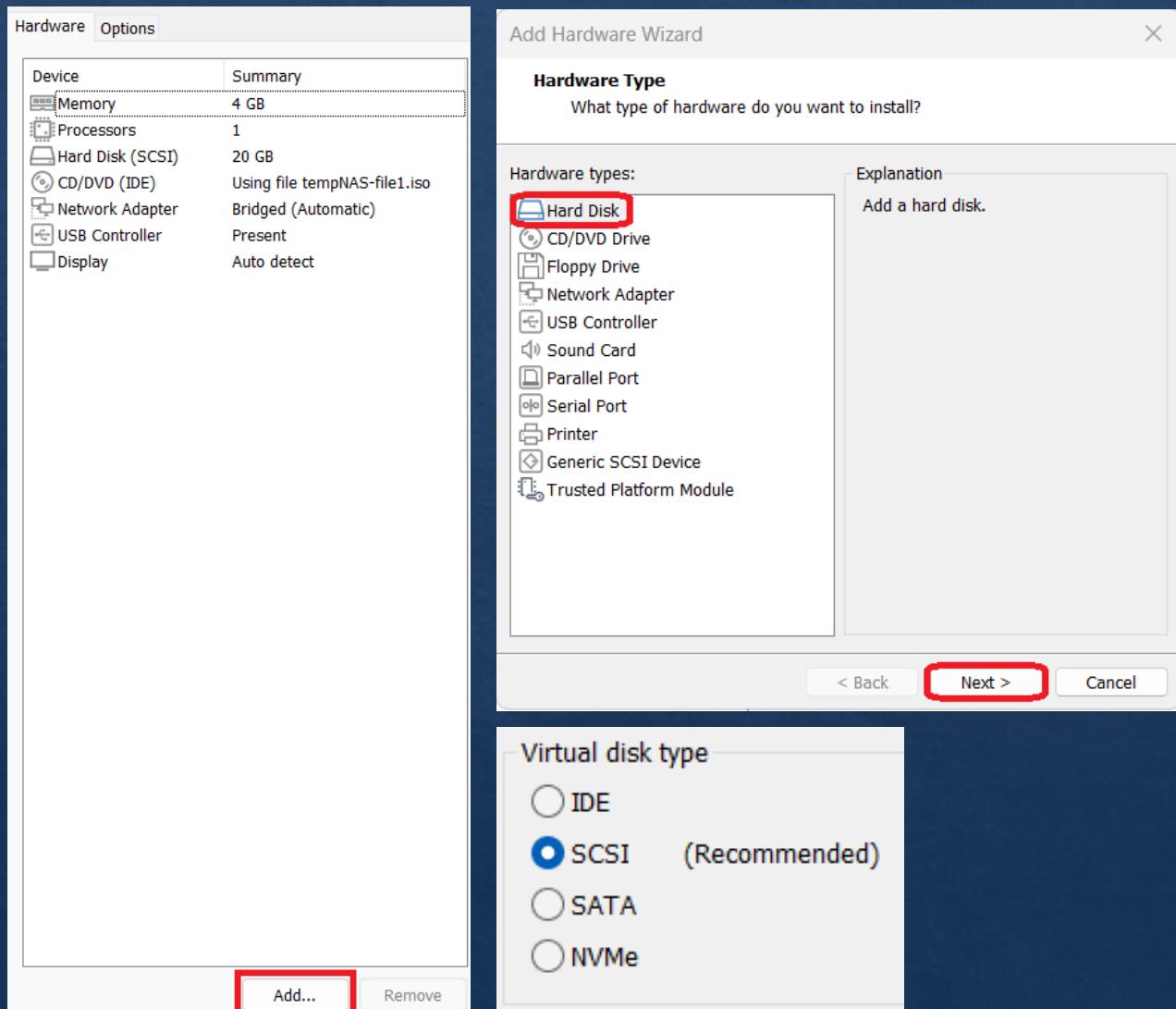
Domain Account Password *

.....

Enable (requires password or Kerberos principal) [?](#)

SAVE **ADVANCED OPTIONS** **REBUILD DIRECTORY SERVICE CACHE**

Etape 2 – Mise en place

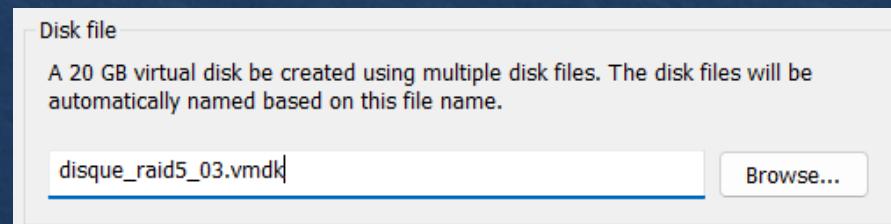
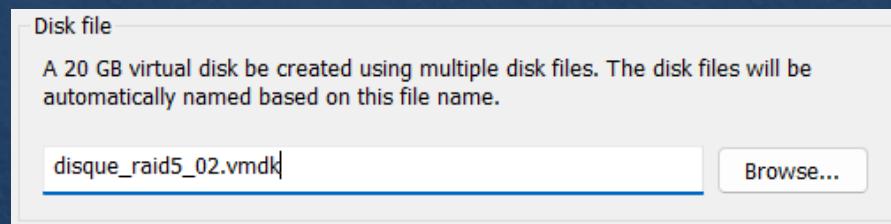
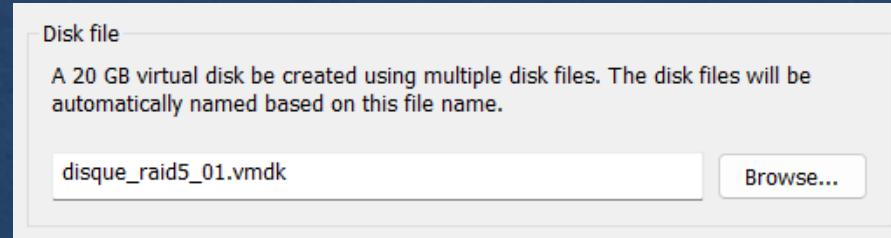
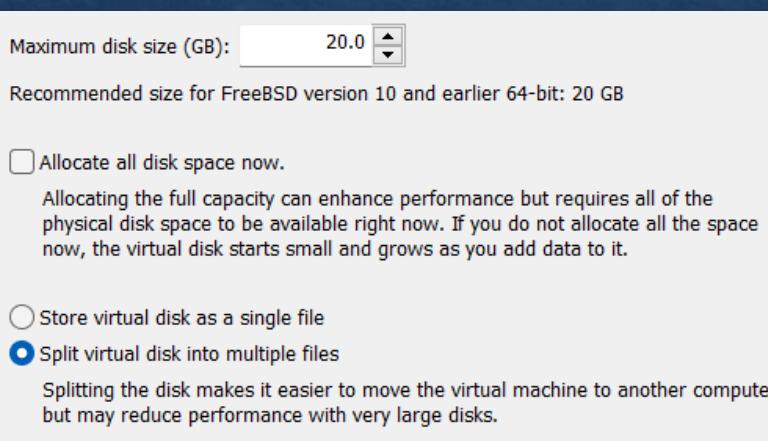
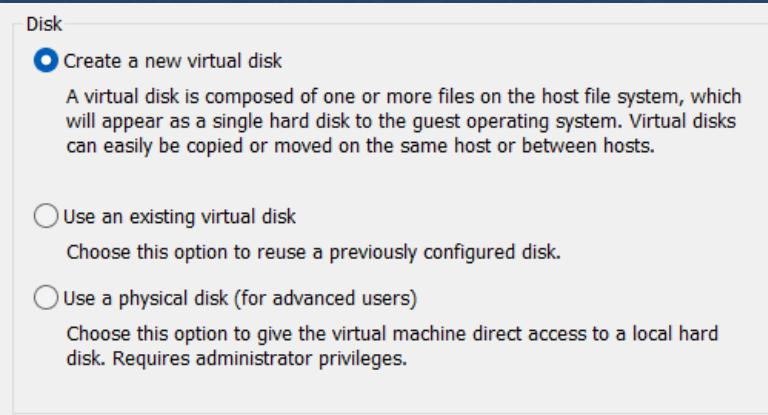


Pour faire un raid, il est nécessaire d'avoir plusieurs disques. Nous allons en rajouter 3 pour notre raid 5.

Dans les paramètres de la VM :

- add
- HARD DISK
- next
- format en SCSI car meilleur dans ce type d'utilisation.

Etape 2 – Mise en place



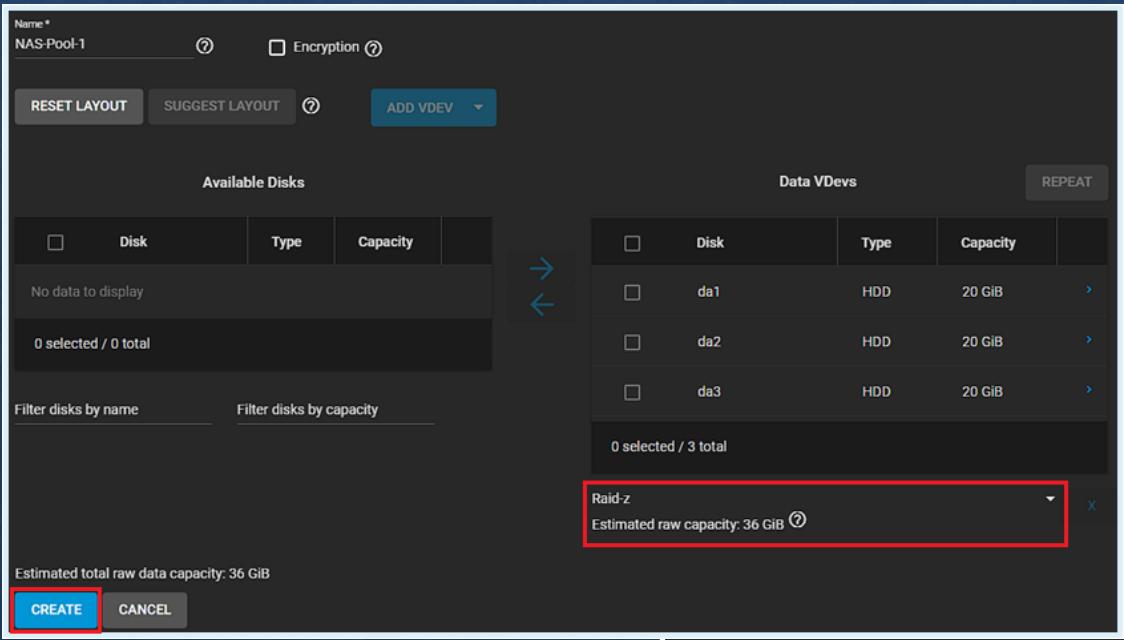
On choisit l'option « create a new virtual disk », on choisit la quantité de stockage souhaiter et on leurs donne un nom.

Etape 2 – Mise en place

The screenshot shows a dark-themed user interface for managing storage pools. At the top, a navigation bar has 'Storage' selected. Below it, a sub-menu titled 'Pools' is shown. In the main content area, the title 'Pools' is at the top, followed by the message 'No pools'. A prominent blue 'ADD' button is located in the top right corner of this section. Below this, a modal window titled 'Create a pool:' is displayed. It contains two options: 'Create new pool' (radio button selected) and 'Import an existing pool' (radio button unselected). At the bottom of the modal are two buttons: 'CANCEL' and a large blue 'CREATE POOL' button, which is highlighted with a red border.

Pour mettre en place un nouveau pool afin de créer des dossiers partagés par la suite il suffit d'aller dans l'onglet « Storage » et de « add » un nouveau pull.

Etape 2 – Mise en place



On crée notre raid (**raid-z**) en sélectionnant tout nos disques créés précédemment.

On va ensuite ajouter nos dossiers partagés.

The screenshot shows the 'Datasets' table with one entry: 'NAS-Pool-1' (FILESYSTEM, 863.05 MiB). A context menu is open for this entry, with the 'Add Dataset' option highlighted with a red box. Other options include Add Zvol, Edit Options, Edit Permissions, User Quotas, Group Quotas, and Create Snapshot.

NAS-Pool-1	FILESYSTEM	863.05 MiB	33.69 GiB	lz4	1.10	false	OFF	Comments
ONLINE	✓	863.05 MiB (2%) Used	33.69 GiB Free					

Etape 2 – Mise en place

Name and Options

Name * utilisateurs ?

Comments Dossiers personnel ?

Sync Inherit (standard) ▼ ?

Compression level Inherit (lz4) ▼ ?

Enable Atime Inherit (off) ▼ ?

Encryption Options

Inherit (non-encrypted) ?

Other Options

ZFS Deduplication Inherit (off) ▼ ?

Case Sensitivity Sensitive ▼ ?

Share Type Generic ▼ ?

Buttons

SUBMIT CANCEL ADVANCED OPTIONS

On donne un nom au nouveau dataset et on l'envoi

Etape 2 – Mise en place

Sharing
Apple Shares (AFP)
Block Shares (iSCSI)
Unix Shares (NFS)
WebDAV Shares
Windows Shares (SMB)

Samba

No data to display

COLUMNS ADD

On va maintenant partager les Dataset crée sur notre domaine.

Dans l'onglet sharing puis Windows Shares

Nous allons « add » les dossiers voulu

Public

/mnt/Pool 1/Public

Utilisateurs

/mnt/Pool 1/Utilisateurs

Etape 2 – Mise en place

Basic

Path *
 /mnt/NAS-Pool-1/utilisateurs ?

Name
utilisateurs ?

Purpose
Private SMB Datasets and Shares ▼ (?) Description

Enabled ?

Access

<input checked="" type="checkbox"/> Enable ACL ?	<input checked="" type="checkbox"/> Use as Home Share ?
<input type="checkbox"/> Export Read Only ?	<input type="checkbox"/> Time Machine ?
<input checked="" type="checkbox"/> Browsable to Network Clients ?	<input checked="" type="checkbox"/> Enable Shadow Copies ?
<input type="checkbox"/> Allow Guest Access ?	<input type="checkbox"/> Export Recycle Bin ?
<input type="checkbox"/> Access Based Share Enumeration ?	<input type="checkbox"/> Use Apple-style Character Encoding ?

Hosts Allow ?

Hosts Deny ?

Other Options

<input checked="" type="checkbox"/> Enable Alternate Data Streams ?
<input checked="" type="checkbox"/> Enable SMB2/3 Durable Handles ?
<input type="checkbox"/> Enable FSRVP ?

Paramètres pour le dossier utilisateurs

Etape 2 – Mise en place

Paramètres pour le dossier Public

Basic

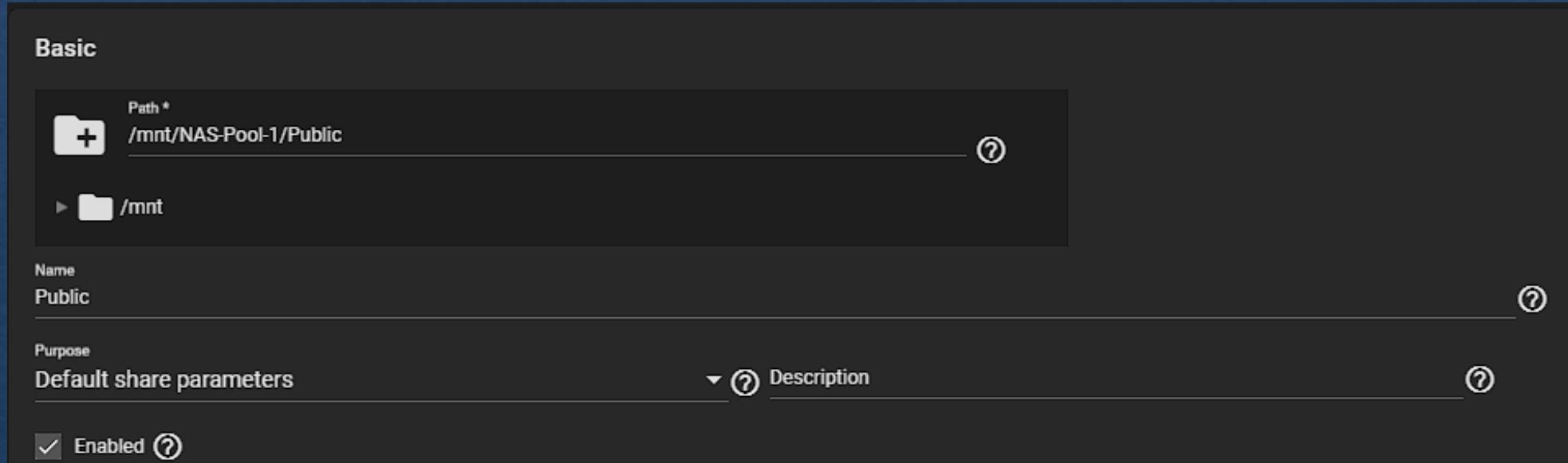
Path *
 /mnt/NAS-Pool-1/Public 

▶  /mnt

Name
Public 

Purpose
Default share parameters  Description 

Enabled 

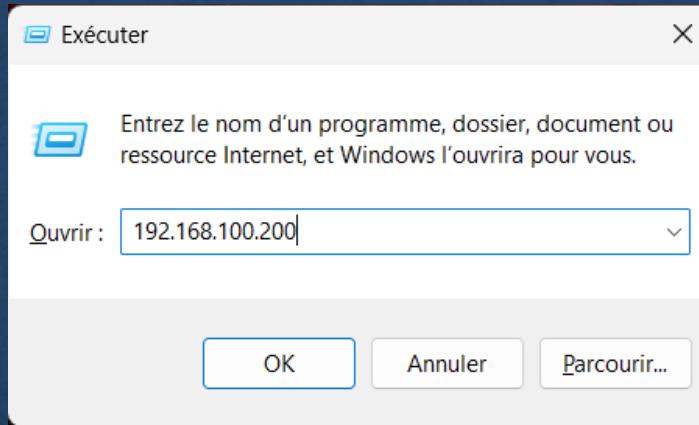


Etape 2 – Mise en place

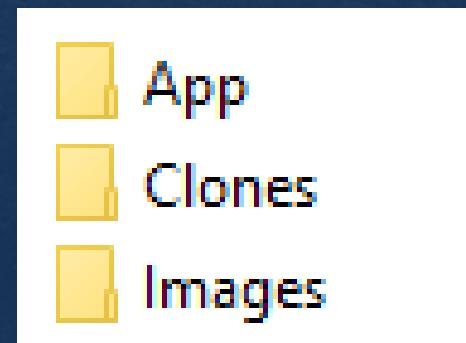
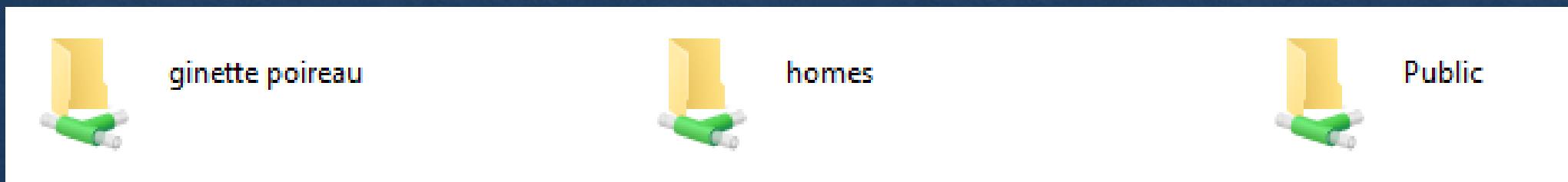
Pool 1 (System Dataset Pool)		ONLINE ✓ 98.95 MiB (0%) Used 34.43 GiB Free						
Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments
Pool 1	FILESYSTEM	98.95 MiB	34.43 GiB	lz4	2.04	false	OFF	
Public	FILESYSTEM	83.54 MiB	34.43 GiB	Inherits (lz4)	1.01	false	OFF	Partage commun de l'entreprise
Utilisateurs	FILESYSTEM	841.84 KiB	34.43 GiB	Inherits (lz4)	1.00	false	OFF	dossiers personnel
SOCODEVI	FILESYSTEM	713.97 KiB	34.43 GiB	Inherits (lz4)	1.01	false	OFF	
administrateur	FILESYSTEM	127.88 KiB	34.43 GiB	Inherits (lz4)	1.00	false	OFF	
win10	FILESYSTEM	127.88 KiB	34.43 GiB	Inherits (lz4)	1.00	false	OFF	
win11	FILESYSTEM	127.88 KiB	34.43 GiB	Inherits (lz4)	1.00	false	OFF	

Voici l'architecture une fois les dossiers partagés et une fois que les utilisateurs se sont connectés la première fois, ils apparaissent dans la liste.

Etape 2 – Tests

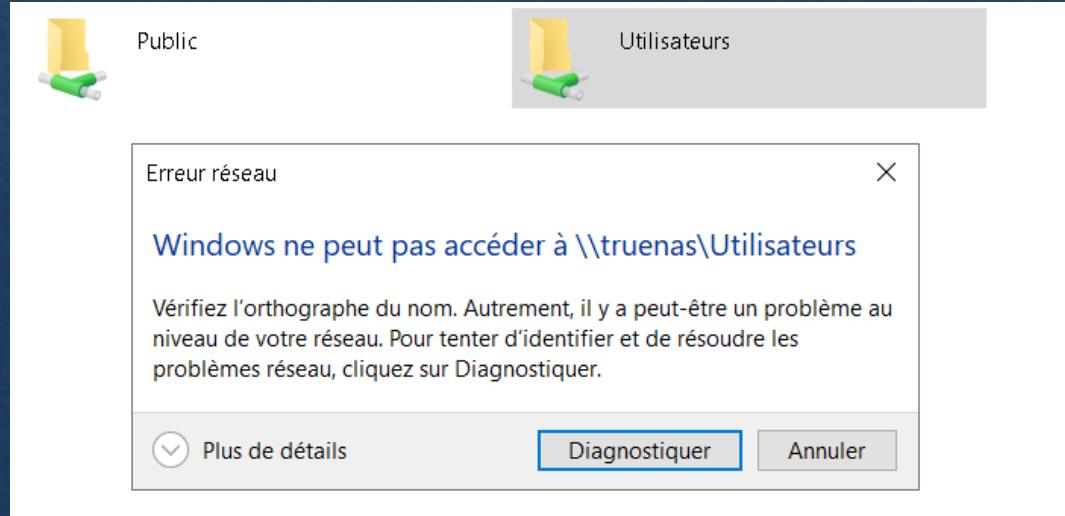


Windows + R puis on y met l'IP du serveur



Etape 2 – Problèmes rencontrés

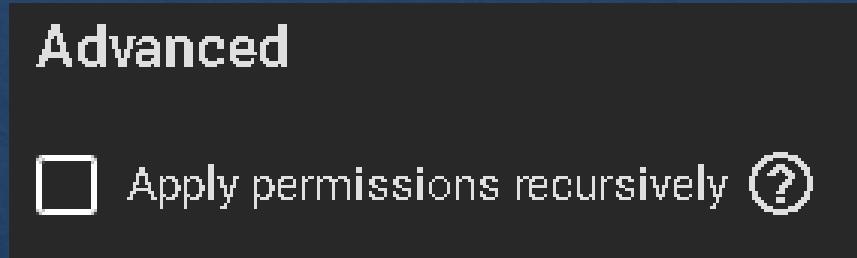
Droits et automatisation sur les dossiers personnels



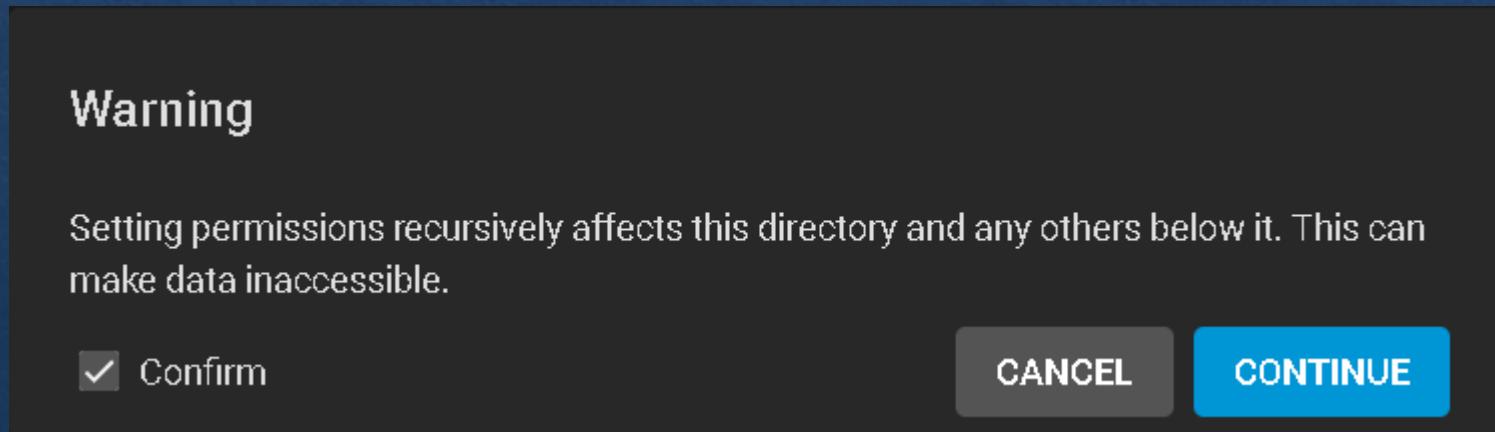
Le problème est le suivant :

Les droits d'accès sont bloqués, de plus, les dossiers personnels n'apparaissent pas.

Etape 2 – Solutions trouvées



Pour régler le soucis de droits il faut aller dans les autorisations du dossier utilisateur il est impératifs de cocher cette case tout en bas de la page.



Etape 2 – Solutions trouvées

The screenshot shows two parts of the TrueNAS web interface. The top part is a table titled 'Samba' listing two shares: 'Public' and 'Utilisateurs'. The 'Utilisateurs' share is selected, and a context menu is open with options: 'Edit' (circled in red), 'Edit Share ACL', 'Edit Filesystem ACL', and 'Delete'. The bottom part is a 'Basic' configuration page for the 'Utilisateurs' share. It shows the path '/mnt/Pool 1/Utilisateurs', a 'Name' field for 'Utilisateurs', and a 'Purpose' dropdown set to 'Private SMB Datasets and Shares' (also circled in red). Under 'Advanced Options', there is a checkbox 'Use as Home Share' which is checked and highlighted with a red box. At the bottom are 'SAVE', 'CANCEL', and 'ADVANCED OPTIONS' buttons.

Pour résoudre le souci de dossier personnel j'ai cherché dans les paramètres du dossier partagé « utilisateurs » pour leurs crée à chacun un dossier personnel automatiquement.

Pour cela il suffit de cocher dans les paramètres avancés « use as home share » et de mettre ce dossier en partage privé avec l'option « private SMB Datasets and shares »

Un redémarrage du NAS s'impose et voici le fameux dossier personnel qui apparait ainsi qu'un dossier « homes » qui est une copie automatique du dossier personnel, je n'ai pas trouvé de solution pour le retirer, TrueNAS le crée automatiquement.

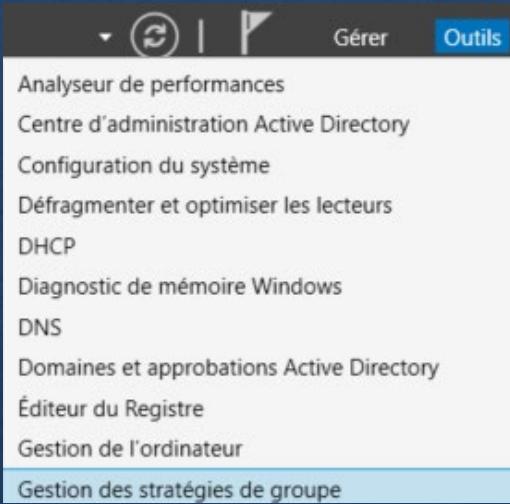


Etape 3 – GPO



Etape 3 – Mise en place

Mise en place de la GPO « papier peint » autrement dit le fond d'écran du bureau des utilisateurs.

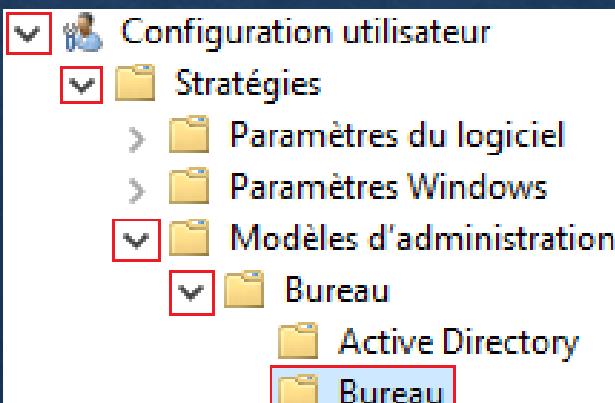


Pour commencer, nous nous rendrons dans l'onglet des GPO en allant dans outils puis « gestion des stratégies de groupe » ou avec le raccourci « gpmc.msc » avec Win + R.

On fait clic droit sur notre domaine puis « Crée un objet de GPO dans ce domaine »



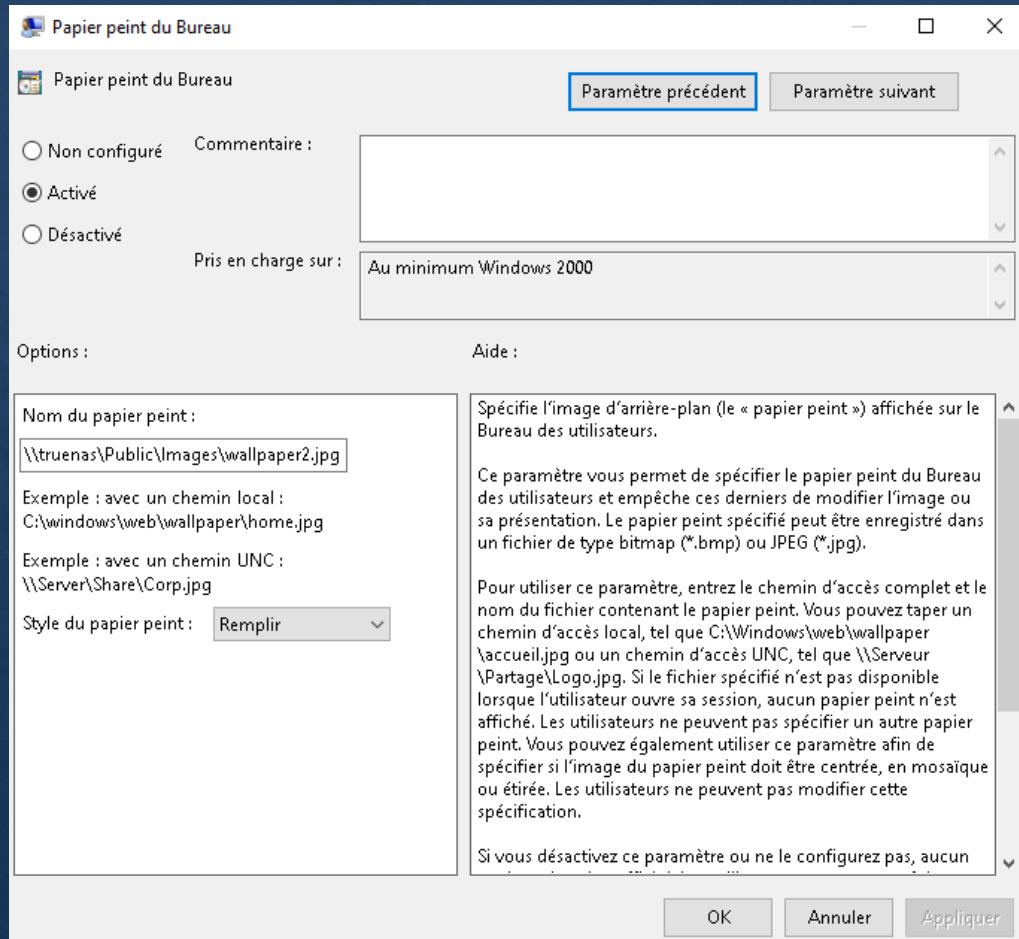
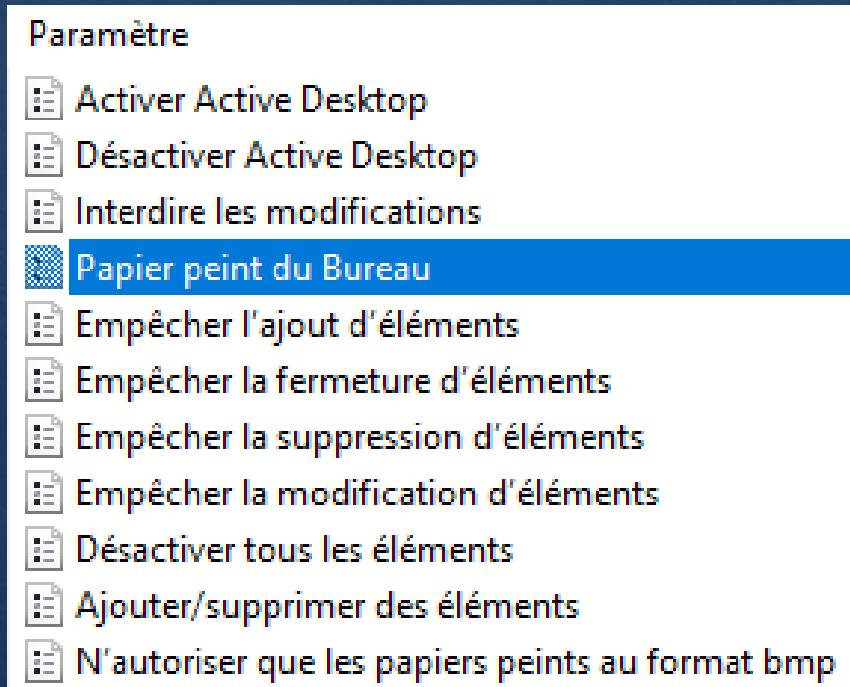
On suit le chemin indiquer et on sélectionne « papier peint du bureau » et on y met la configuration suivante (diapo suivante).



NOTE : L'image doit se trouver dans un dossier disponible à tous les utilisateurs, c'est pourquoi mon image se trouve sur mon NAS dans un dossier public disponible de tous.

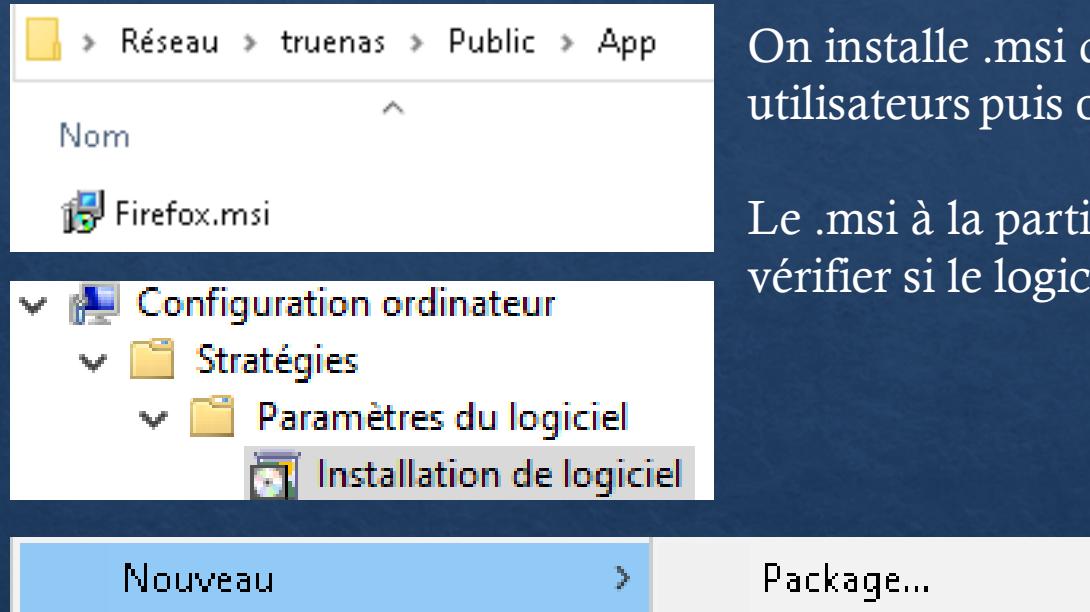
Etape 3 – Mise en place

Mise en place de la GPO « papier peint » autrement dit le fond d'écran du bureau des utilisateurs.



Etape 3 – Mise en place

Mise en place de la GPO pour l'installation automatique de Firefox sur les post client.

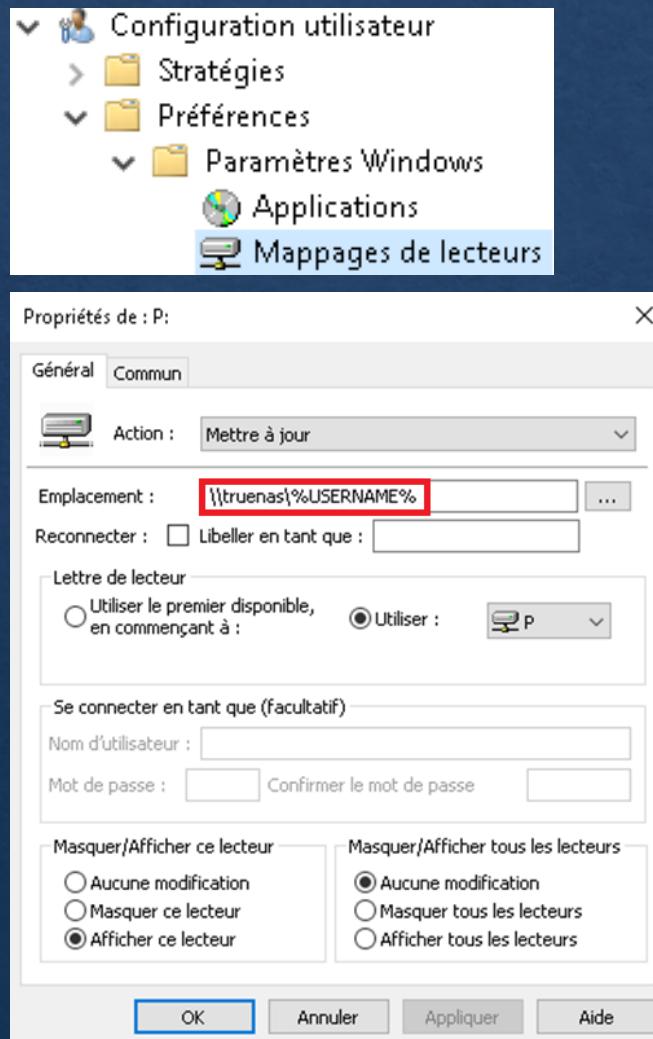


On installe .msi de Firefox que l'on met dans le NAS disponible à tous les utilisateurs puis on crée la GPO.

Le .msi à la particularité de ne pas avoir besoin d'un script pour installer et vérifier si le logiciel est déjà installé sur le système, c'est déjà intégré.

Etape 3 – Mise en place

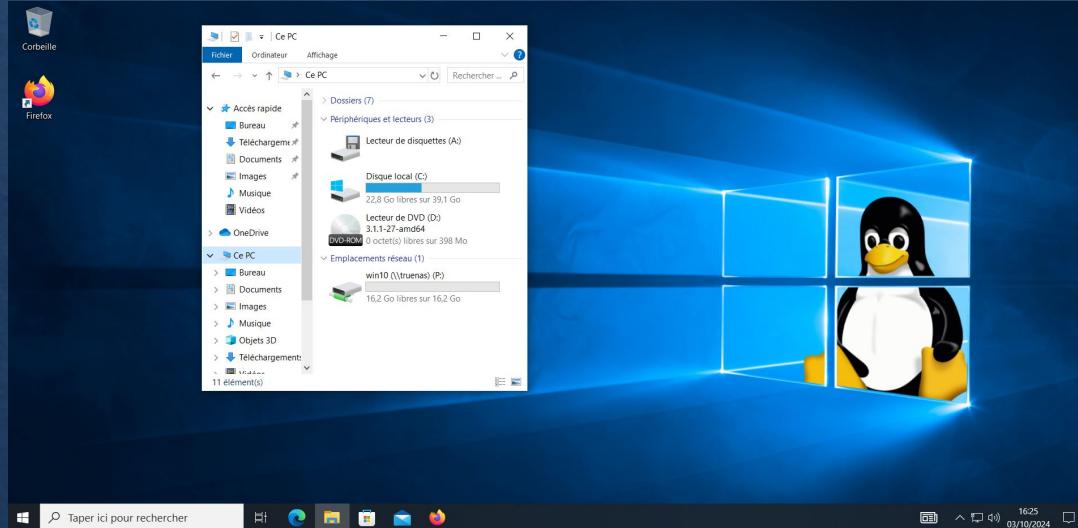
Mise en place de la GPO pour le mappage auto des dossiers personnel sur les post client.



Direction le mappage de lecteurs, clic droit nouveau mappage et on y met la configuration suivante : \\\\truenas\\%USERNAME% pour que ce soit automatique dès le user connecter.

Etape 3 – Tests

Sur une machine cliente nous ouvrons le cmd et nous tapons « gpupdate/force » pour forcer la mise à jour des gpo puis nous nous reconnectons.

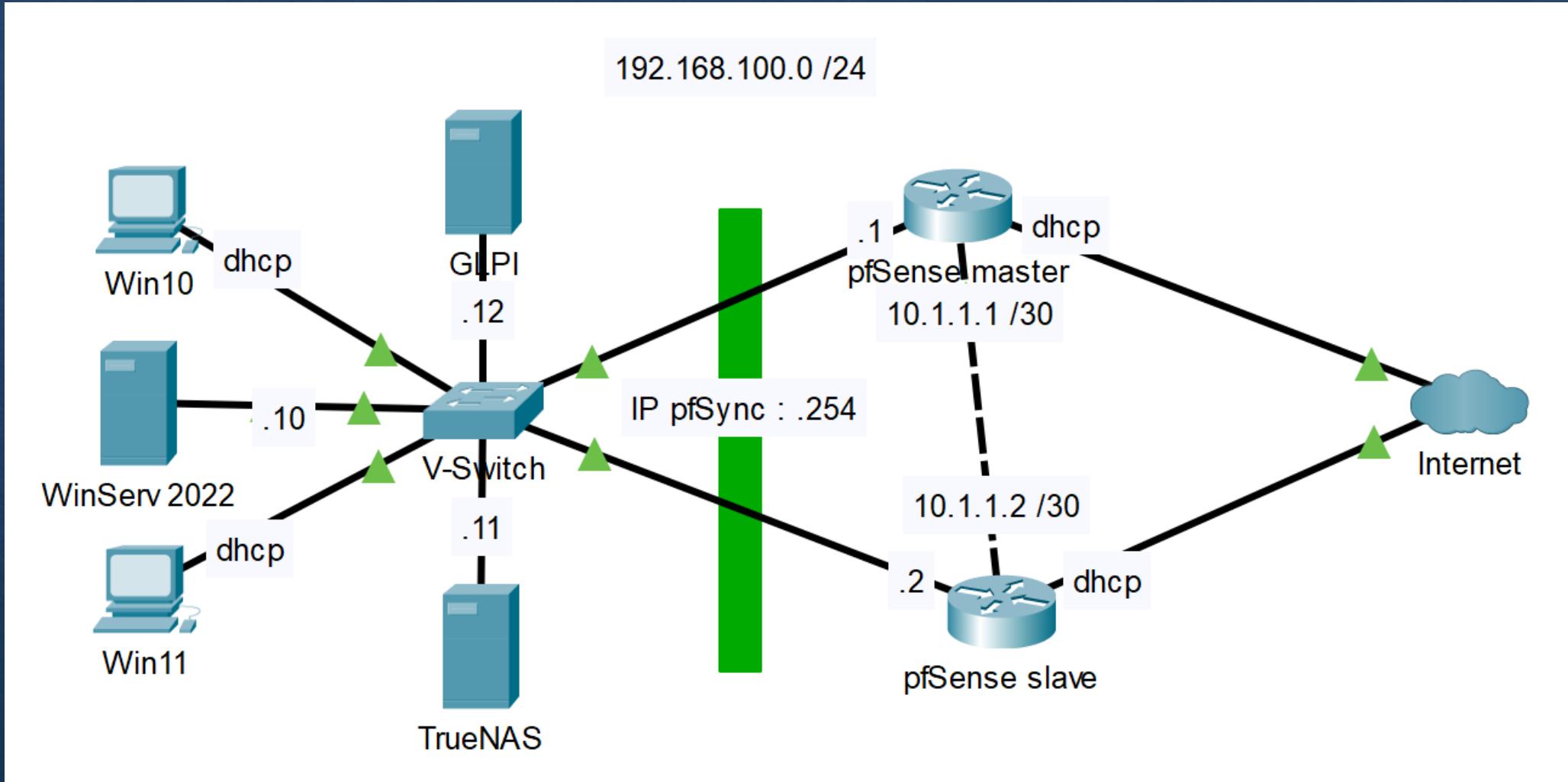


Nous pouvons constater que le fond d'écran à pris effet ainsi que l'installation de Firefox et la mappage auto du disque personnel sur le NAS

Etape 4 – GLPI



Etape 4 – Architecture réseau



Etape 4 – Mise en place

Pour mettre en place le serveur GLPI nous allons devoir installer glpi et crée une base de donnée pour y stocker les informations.

On commence par mettre à jours la vm puis on installe le zip de glpi qu'on extrait directement dans le dossier prévu à cet effet. On y met les droits requis et on peux passer à la suite.

```
root@Serveur-debian:~# apt update && apt upgrade_
```

```
cd /var/www/html  
wget https://github.com/glpi-project/glpi/releases/download/10.0.10/glpi-10.0.10.tgz  
tar -xvzf glpi-10.0.10.tgz
```

```
chown -R www-data:www-data /var/www/html/glpi  
chmod -R 755 /var/www/html/glpi
```

Etape 4 – Mise en place

Maintenant nous pouvons crée la base de données avec le user.

```
mysql -u root -p
```

```
CREATE DATABASE glpi;  
CREATE USER 'glpiuser'@'localhost' IDENTIFIED BY 'glpiuser';  
GRANT ALL PRIVILEGES ON glpi.* TO glpiuser'@'localhost';  
FLUSH PRIVILEGES;
```

Etape 4 – Mise en place

On fait « installer » puis on regarde que toutes les extensions requises soit installées.



TESTS EFFECTUÉS	RÉSULTATS
Requis Parser PHP	✓
Requis Configuration des sessions	✓
Requis Mémoire allouée	✓
Requis mysqli extension	✓
Requis Extensions du noyau de PHP	✓
Requis curl extension <small>Requis pour l'accès à distance aux ressources (requêtes des agents d'inventaire, Marketplace, flux RSS, ...).</small>	✓
Requis gd extension <small>Requis pour le traitement des images.</small>	✓
Requis intl extension <small>Requis pour l'internationalisation.</small>	✓
Requis zlib extension <small>Requis pour la gestion de la communication compressée avec les agents d'inventaire, l'installation de paquets gzip à partir du Marketplace et la génération de PDF.</small>	✓
Requis Libsodium ChaCha20-Poly1305 constante de taille <small>Activer l'utilisation du cryptage ChaCha20-Poly1305 requis par GLPI. Il est fourni par libsodium à partir de la version 1.0.12.</small>	✓
Requis Permissions pour les fichiers de log	✓
Requis Permissions pour les dossiers de données	✓

Etape 4 – Mise en place

On se connecte avec l'utilisateur créé précédemment et on sélectionne la base de donnée créée au début.

The image displays two screenshots of the GLPI SETUP configuration interface, showing the process of connecting to a database and selecting a database.

Screenshot 1 (Left): Configuration de la connexion à la base de données

- GLPI SETUP**
- Étape 1**
- Configuration de la connexion à la base de données**
- Serveur SQL (MariaDB ou MySQL)**: localhost
- Utilisateur SQL**: glpiuser
- Mot de passe SQL**: ****
- Continuer >**

Screenshot 2 (Right): Test de connexion à la base de données

- GLPI SETUP**
- Étape 2**
- Test de connexion à la base de données**
- Connexion à la base de données réussie**
- Veuillez sélectionner une base de données :**
- Créer une nouvelle base ou utiliser une base existante :**
- glpi** (selected)
- Continuer >**

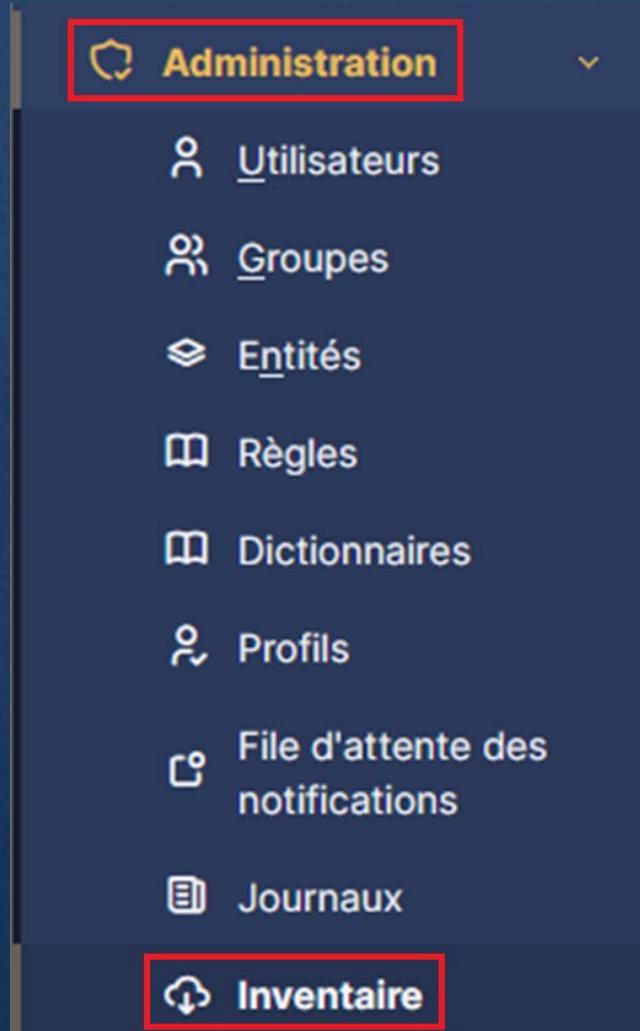
Etape 4 – Mise en place

La configuration de base est finie, nous pouvons accéder à l'interface web de GLPI.



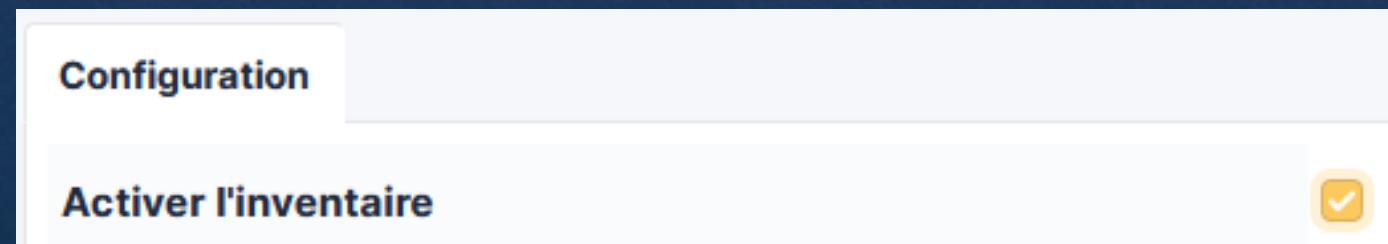
The screenshot shows the GLPI login page. The title 'GLPI' is at the top. Below it, the heading 'Connexion à votre compte' is followed by a form. The 'Identifiant' field contains 'glpi'. The 'Mot de passe' field is filled with '****'. The 'Source de connexion' dropdown is set to 'Base interne GLPI'. A checked checkbox 'Se souvenir de moi' is present. A yellow 'Se connecter' button is at the bottom right.

Etape 4 – Mise en place



Une option à activer sur le serveur est requise au bon fonctionnement de l'inventaire automatique.

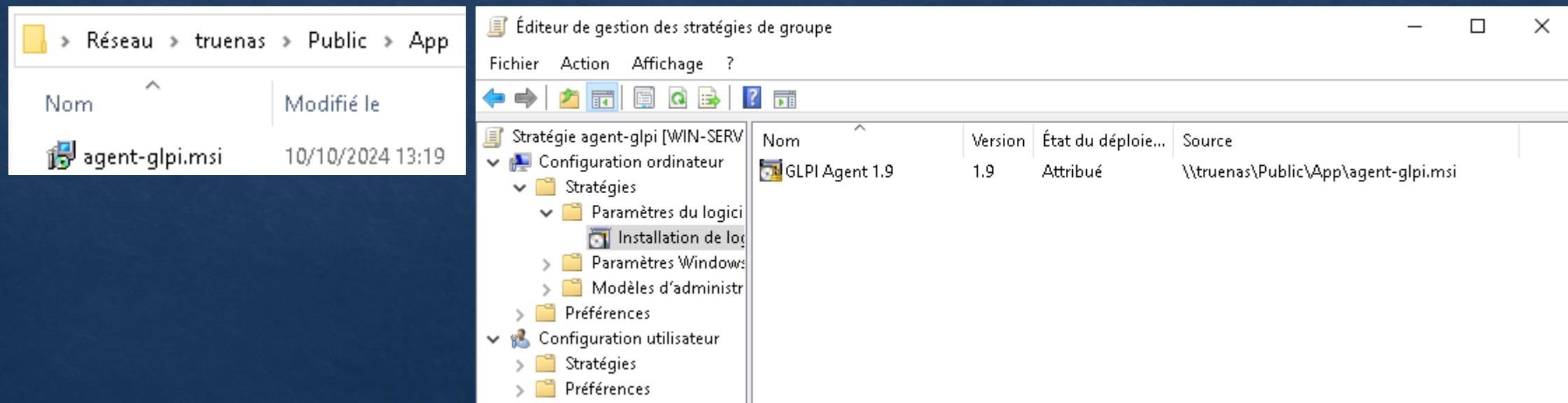
Dans « administration » puis « inventaire », nous devons cocher la case « activer l'inventaire »



Etape 4 – Mise en place

Le serveur GLPI est en place. Maintenant il nous faut installer et configurer l'agent glpi sur tout les postes pour qu'ils envoient leurs informations automatiquement au serveur.

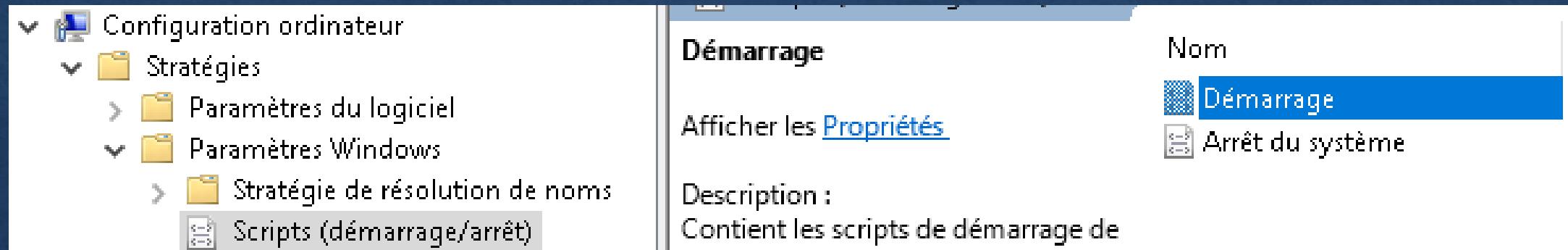
Rien de compliqué, on installe le .msi de glpi et on fait une GPO ordinateur car nous voulons recevoir les informations au démarrage de l'ordinateur et non pas une fois l'utilisateur authentifié.



Etape 4 – Mise en place

L'installation de l'agent est maintenant automatisée, il faut ensuite le configurer pour qu'il sache à qui transmettre les informations.

Pour ce faire, nous allons lui rajouter un script dans la même GPO.



The screenshot shows the Windows Group Policy Management console. On the left, the navigation pane displays the following structure:

- Configuration ordinateur
- Stratégies
 - Paramètres du logiciel
 - Paramètres Windows
 - Stratégie de résolution de noms
 - Scripts (démarrage/arrêt)

The right pane shows the properties of the 'Démarrage' (Startup) GPO. The 'Description' field contains the following text:

Description :
Contient les scripts de démarrage de

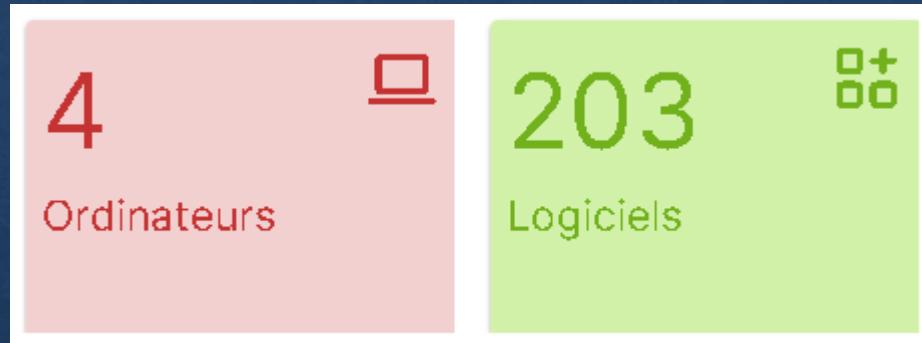
Nom
Démarrage
Arrêt du système

```
@echo off
msiexec /i "\\\Truenas\\Public\\App\\agent-glpi.msi" /quiet RUNNOW=1 ADD_FIREWALL_EXCEPTION=1
EXEMODE=1 SERVER="http://192.168.100.11/glpi/front/inventory.php"
```

Etape 4 – Tests

Pour vérifié que tout fonctionne, on se connecte sur l'interface web et dans l'onglet « ordinateurs » nous retrouverons la liste des machines qui se sont synchronisé.

En cliquant sur une machine, on y retrouve les informations détailler de la machine.



<input type="checkbox"/>	WIN-SERV-2022	VMware, Inc.	VMware-56 4d 6c 47 0e af 34 a9-05 e3 c7 24 34 15 0d 41	VMware	VMware20,1	Microsoft Windows Server 2022 Standard	2024-11-17 12:17	AMD Ryzen 7 5800H with Radeon Graphics
<input type="checkbox"/>	win-serv-2022-B	VMware, Inc.	VMware-56 4d 8a c4 aa cf bd d4-b9 17 48 a7 ae 1f c7 e3	VMware	VMware20,1	Microsoft Windows Server 2022 Standard	2024-11-17 12:38	AMD Ryzen 7 5800H with Radeon Graphics
<input type="checkbox"/>	win10-client	VMware, Inc.	VMware-56 4d e3 f3 8d 7f 27 d2-37 47 b6 aa cc fb fc 15	VMware	VMware20,1	Microsoft Windows 10 Professionnel	2024-11-17 11:33	AMD Ryzen 7 5800H with Radeon Graphics
<input type="checkbox"/>	win11-client	VMware, Inc.	VMware-56 4d 87 78 3f bf 92 68-08 c1 93 a8 9c d1 1d a6	VMware	VMware20,1	Microsoft Windows 11 Professionnel	2024-11-17 11:41	AMD Ryzen 7 5800H with Radeon Graphics

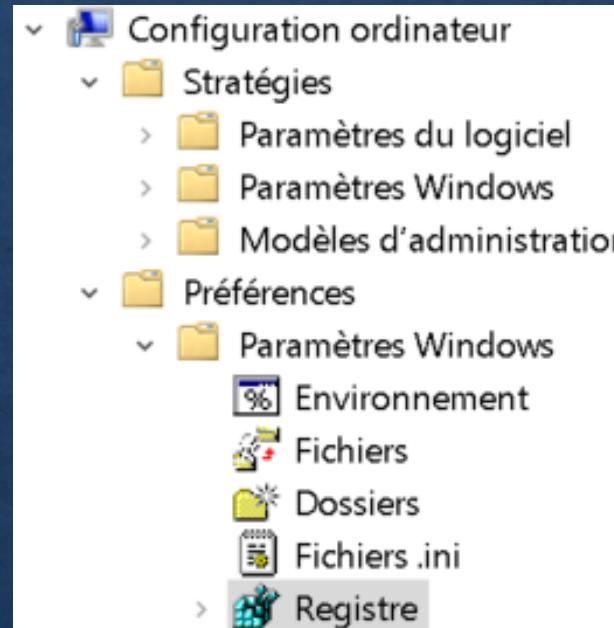
Etape 4 – Problème rencontré

En regardant les logs dans le dossier de l'agent glpi : **C:\Program Files\GLPI-Agent\logs** je me suis rendu compte que je ne parvenais pas à contacter le serveur, j'ai compris que cela pouvait uniquement provenir de la configuration alors je suis aller voir le script.

```
[Fri Oct 11 20:26:55 2024][error] No target defined, aborting
[Fri Oct 11 20:54:16 2024][error] No target defined, aborting
[Fri Oct 11 21:04:52 2024][error] No target defined, aborting
[Fri Oct 11 21:06:43 2024][error] No target defined, aborting
[Fri Oct 11 21:12:24 2024][error] No target defined, aborting
```

Etape 4 – Solution trouvé

Le script ne fonctionnait pas tout le temps et pouvais poser soucis en fonction de windows10 et 11 alors pour résoudre ce souci j'ai modifié la GPO pour passer d'un script à directement une modification de l'éditeur de registre Windows pour y mettre la configuration en dur dans la machine.

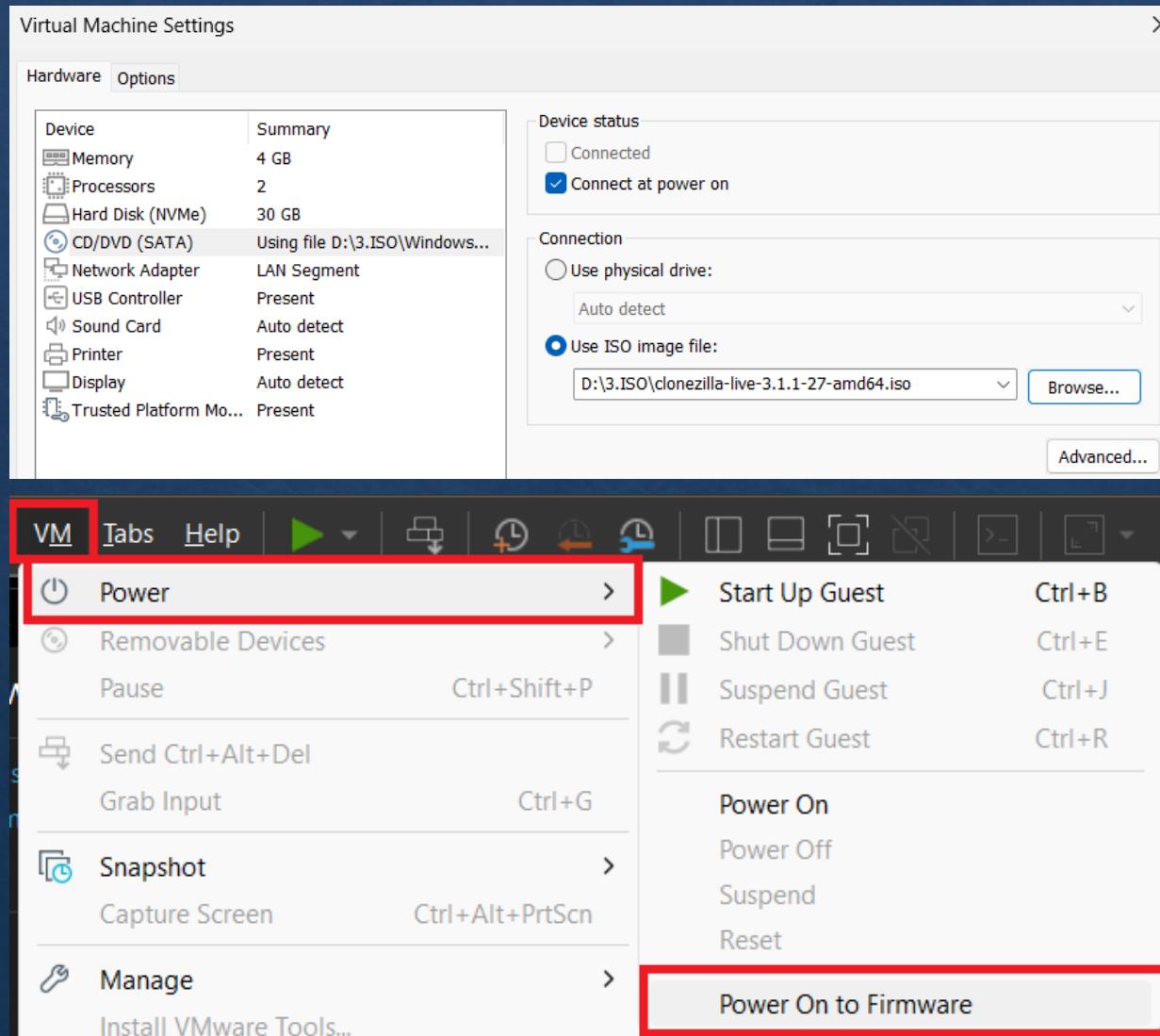


Nom	Ordre	Action	Ruche	Cle	Nom de valeur	Type	Données de valeur	
ah server				HKEY_LOCAL_MACHINE	SOFTWARE\GLPI-Agent	server	REG_SZ	http://192.168.100.11/glpi/front/inventory.php
ah tag				HKEY_LOCAL_MACHINE	SOFTWARE\GLPI-Agent	tag	REG_SZ	socodevi-client-glpi

Etape 5 – Clonezilla



Etape 5 – Mise en place

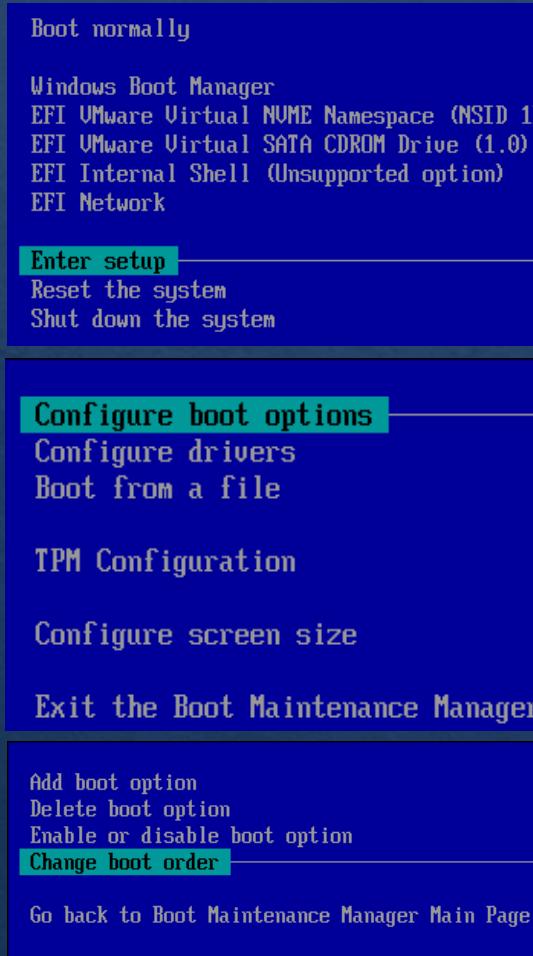


Pour commencer le clonage d'une machine déjà configuré nous allons booter dessus avec clonezilla, pour ce faire nous mettons l'OVA de clonezilla et on ouvre la VM dans le bios.

VM -> Power -> Power On to Firmware

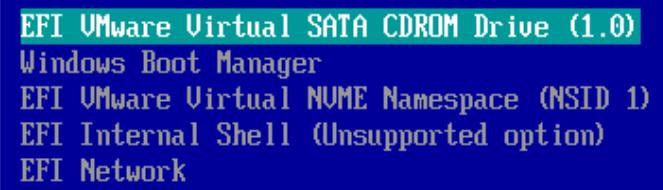
Cet à dire lancer la VM dans le micrologiciel, autrement dit le bios.

Etape 5 – Mise en place



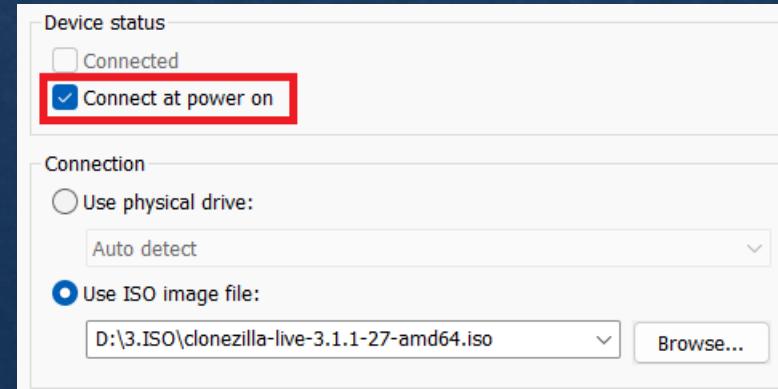
Une fois dans le BIOS :

- Enter setup
- Configure boot options
- Change boot order
- Mettre le SATA en première place



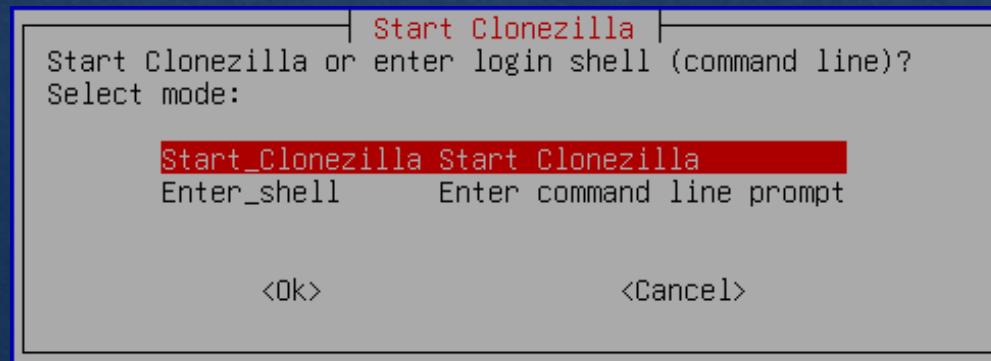
Une fois fait redémarré le VM

Note : bien vérifier l'option dans
VmWare « Connect at power on »



Etape 5 – Mise en place

```
*Clonezilla live (VGA 800x600)
Clonezilla live (VGA 800x600 & To RAM)
Clonezilla live (VGA with large font & To RAM)
Clonezilla live (Speech synthesis)
Other modes of Clonezilla live
Local operating system (if available)
Memtester (VGA 800x600 & To RAM)
Memtest using Memtest86+
Network boot via iPXE
uEFI firmware setup
Clonezilla live 3.1.1-27-amd64 info
```



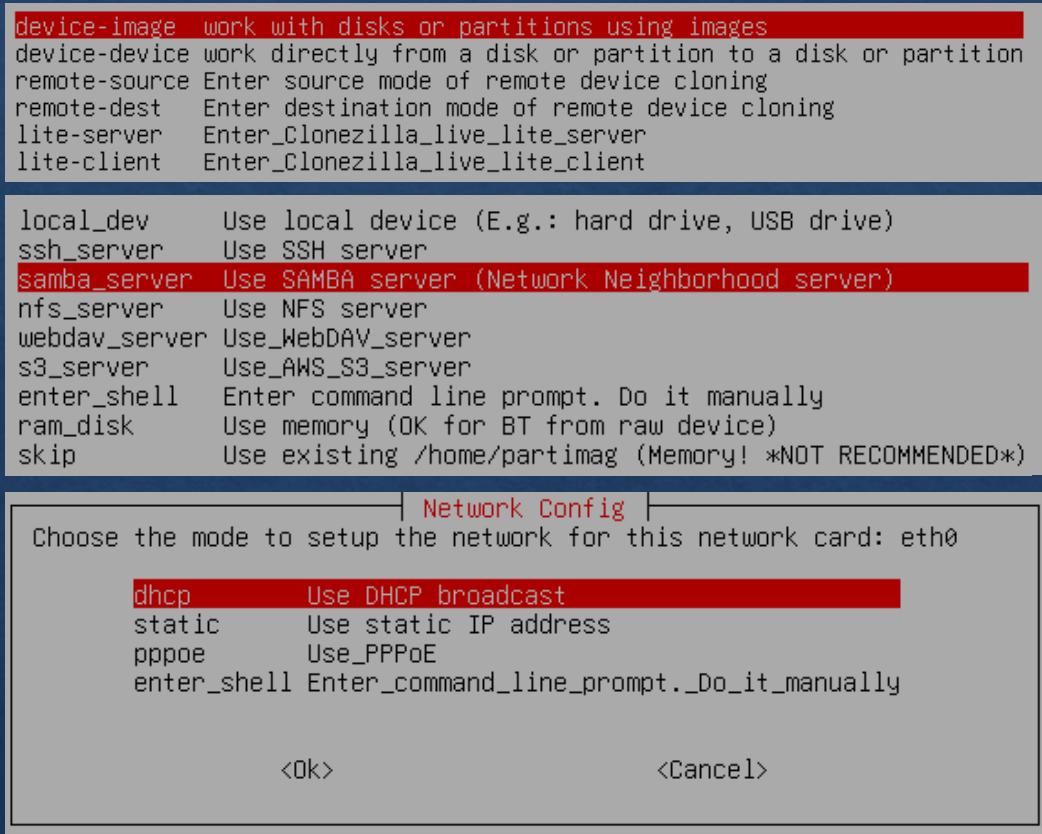
Une fois la configuration sur VmWare fini et la machine lancer vous devriez tomber sur clonezilla.

Prenez la première option.

Il vous demandera en premier lieu si vous souhaitez changer la langue ainsi que la disposition du clavier, dans mon cas j'ai laisser par défaut donc anglais en qwerty.

Ensuite vous lancer clonezilla en normal et non en shell sinon vous n'avez pas les aides etc...

Etape 5 – Mise en place

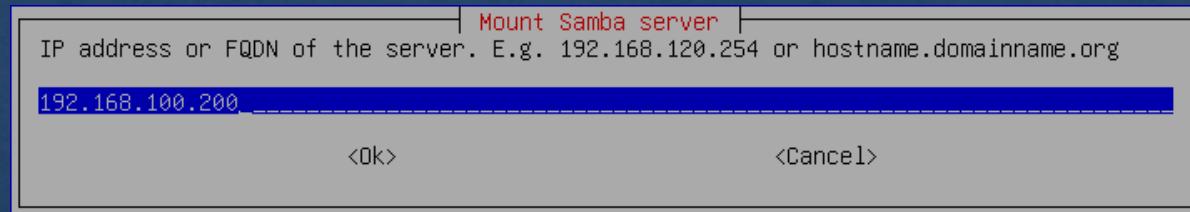


Notre objectif est de faire une image à partir d'un disque alors nous prendrons la première option « device to image »

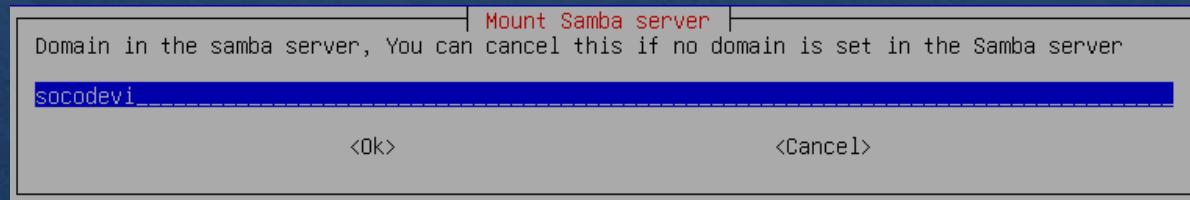
Nous allons déposer notre image sur notre TrueNAS qui utilise un partage de fichier SMB donc samba.

Si le réseau est correctement configuré alors la fonction dhcp est la plus simple mais static fonctionne aussi.

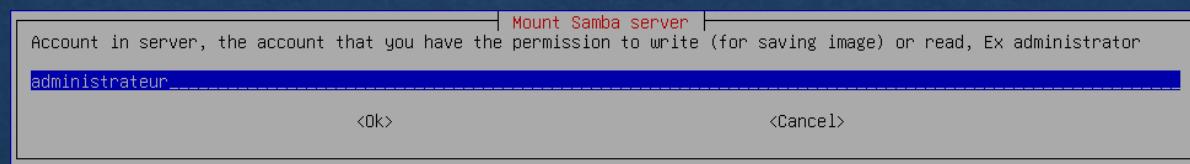
Etape 5 – Mise en place



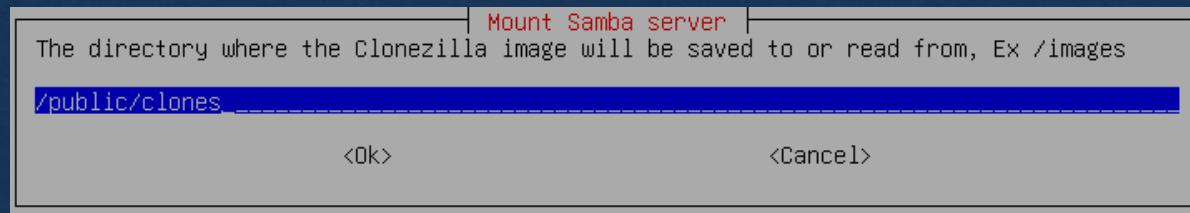
On renseigne l'ip de notre NAS



On renseigne le domaine sans le TDL



On renseigne le compte qui vas permettre la connexion au NAS, il faut donc un compte avec les droits nécessaire, dans notre cas c'est le partage public donc n'importe quel user devrait en théorie fonctionner



On renseigne le chemin du répertoire ou l'on souhaite se connecter

Etape 5 – Mise en place

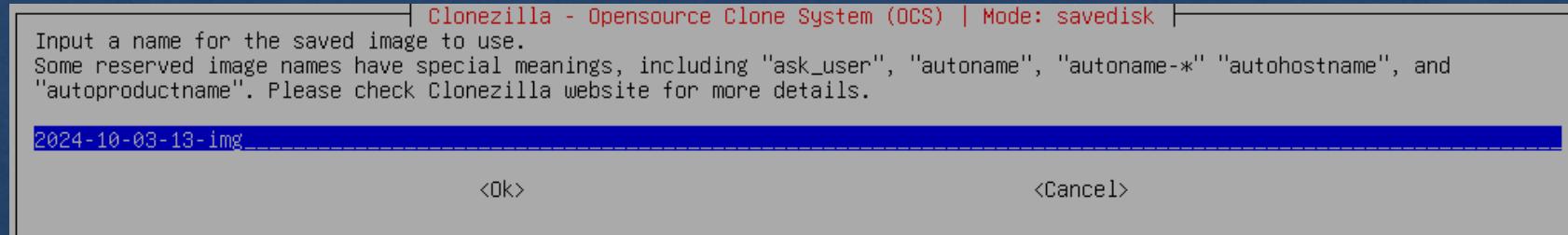
```
Mounting Samba server by:  
LC_ALL=C mount -t cifs "//192.168.100.200/Public/Clones" /home/partimag -o user="administrateur, domain=socodevi"  
Password for administrateur@//192.168.100.200/Public/Clones: _
```

Une fois toutes les informations renseigner, il vous demandera le mdp de l'utilisateur renseigner plus-tôt.

savedisk	Save_local_disk_as_an_image
saveparts	Save_local_partitions_as_an_image
restoredisk	Restore_an_image_to_local_disk
restoreparts	Restore_an_image_to_local_partitions
1-2-mdisks	Restore_an_image_to_multiple_local_disks
recovery-iso-zip	Create_recovery_Clonezilla_live
chk-img-restorable	Check_the_image_restorable_or_not
cvt-img-compression	Convert_image_compression_format_as_another_image
encrypt-img	Encrypt_an_existing_unencrypted_image
decrypt-img	Decrypt_an_existing_encrypted_image
exit	Exit. Enter command line prompt

Vous allez en mode expert et vous prenez l'option « savedisk »

Etape 5 – Mise en place



Vous nommez le fichier



Le disque qu'il vas cloner

Which clone program(s) and what priority do you prefer? Program priority means that if the file system is not supported by the first program, the next program will be used. E.g. If you choose "Priority: ntfsclone > partimage > dd", then if the file system is xfs, Clonezilla will try to use ntfsclone first, and of course, xfs is not supported by ntfsclone, so Clonezilla will try to use partimage with dd being the last program to try if that does not work.
The default settings are optimized. **If you have no idea, keep the default value and do NOT change anything and continue.**

```
-q2 Priority: partclone > partimage > dd  
-q1 Priority: Only dd (supports all filesystem, but inefficient)  
-q Priority: ntfsclone > partimage > dd  
Priority: partimage > dd (no ntfsclone)
```

Si vous n'en savez rien comme moi, laissez par défaut.

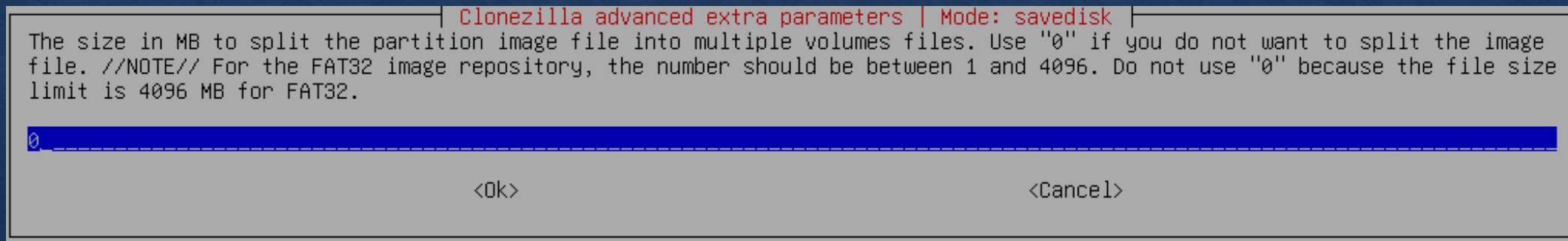
Etape 5 – Mise en place

```
[*] -c Client waits for confirmation before cloning  
[*] -j2 Clone the hidden data between MBR and 1st partition  
[ ] -nogui Use text output only, no TUI/GUI output  
[ ] -a Do NOT force to turn on HD DMA  
[ ] -batch Run clone in batch mode (DANGEROUS!)  
[ ] -rm-win-swap-hib Remove page and hibernation files in Win if exists  
[ ] -ntfs-ok Skip checking NTFS integrity, even bad sectors (ntfsclone only)  
[ ] -rescue Continue reading next one when disk blocks read errors  
[ ] -gm Generate image MD5 checksums  
[ ] -gs Generate image SHA1 checksums  
[ ] -gb Generate image BLAKE2 checksums  
[ ] -gmf Generate checksum for files in device after saving  
[ ] -noabo Image not only accessible by owner  
[ ] -ps Play sound when the job is done  
[ ] -scpt Skip checking the partition table of the source disk is MBR or GPT format  
[ ] -sfs Skip partition file system saving  
[ ] -edio Enable the direct IO mode of Partclone for NVMe SSD
```

Même chose que précédemment

```
-zip Use parallel gzip compression, for multicore/CPU  
-z1 gzip compression (fast with a smaller image)  
-z2p Use parallel bzip2 compression, for multicore/CPU  
-z2 bzip2 compression (slowest but smallest image)  
-z3 lzo compression (faster with image size approx. to that of gzip)  
-z4 lzma_compression_(slowest_but_also_small_image,_faster_decompression_than_bzip2)  
-z5p Use_parallel_xz_compression,_for_multicore/CPU  
-z5 xz_compression_(slowest_but_also_small_image,_faster_decompression_than_bzip2)  
-z6p Use_parallel_lzip_compression,_for_multicore/CPU  
-z6 lzip_compression_(slowest_but_also_small_image,_faster_decompression_than_bzip2)  
-z7 lrzip_compression_(Slow_but_also_small_image)  
-z8 lz4_compression_(Fast_but_also_larger_image)  
-z8p lz4mt_compression_(Fast_but_also_larger_image)  
-z9 zstd_compression_(Very_fast_and_small_image_like_gzip)  
-z9p zstdm_compression_(Very_fast_and_small_image_like_gzip,_for_multicore/CPU)  
-z0 No compression (fastest but largest image size)
```

Laissez par défaut sinon mettez z9p



Laissez 0 pour ne pas segmenter l'image.

Etape 5 – Mise en place

```
-fsck  Skip checking/repairing source file system  
-fsck  Interactively check and repair source file system before saving  
-fsck-y Auto (Caution!) check and repair source file system before saving
```

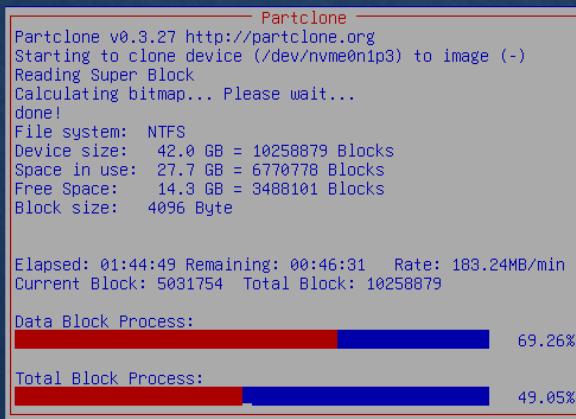
Choix 1 ou 2, aux choix mais nous partirons sur le 2^{ème} par précaution.

```
-senc  Not to encrypt the image  
-enc   Encrypt the image
```

Choix 1 ou 2, aux choix mais dans notre cas se sont des machines vierges sans données sensible, je ne vais pas encrypter l'image.

```
-p choose  Choose reboot/shutdown/etc when everything is finished  
-p true    Enter command line prompt  
-p reboot  Reboot  
-p poweroff Shutdown
```

Je choisis de redémarrer la machine une fois cloner.

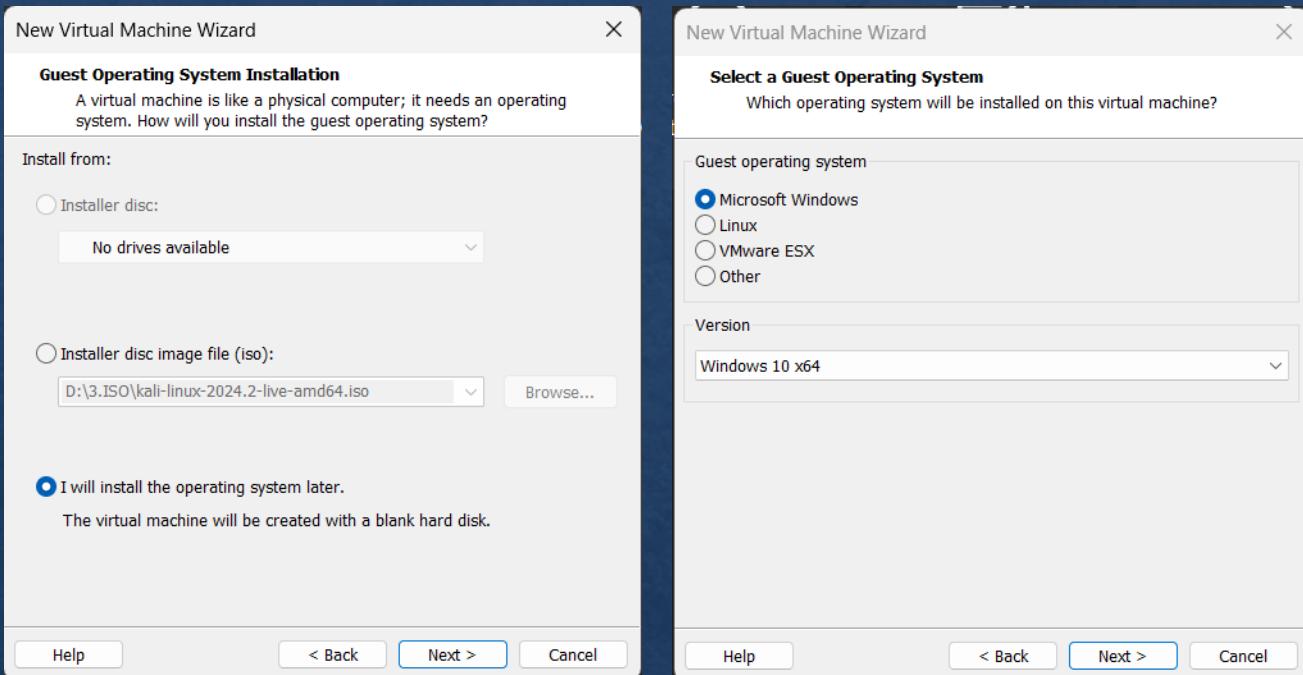


Clonage en cours, plus ou moins long en fonction de la taille du disque à cloner.

Réseau > truenas > Public > Clones >		
Nom	Modifié le	Type
2024-09-30-19-img-windows10-client	30/09/2024 19:27	Dossier de fichiers

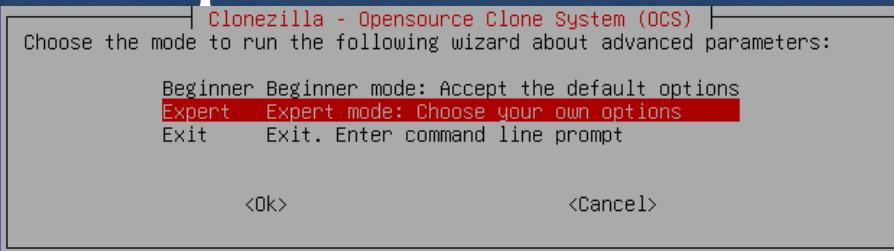
Une fois fini, nous pouvons aller voir à l'endroit indiquer au début que l'image est présente. Dans notre cas c'est dans le NAS. 66

Etape 5 – Tests

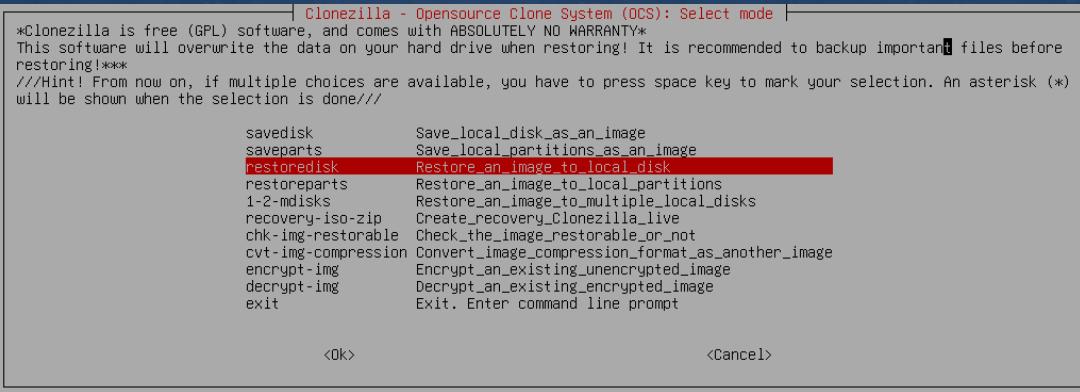


Pour tester si notre image fonctionne nous allons crée une machine vierge sans OS. Nous mettons juste la machine dans notre LAN segment et l'iso de clonezilla pour booter dessus.

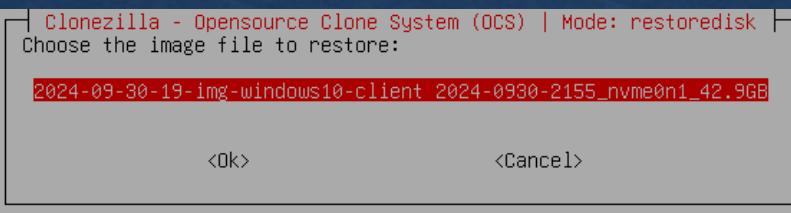
Etape 5 – Tests



Pour déployer une image à partir de notre NAS il faut procéder de la même manière que pour créer une image.



On passe en expert comme avant et nous choisissons l'option « restoredisk » au lieu de « savedisk »



On choisit notre image créée précédemment



On choisit le disque sur lequel importer l'image

Etape 5 – Tests

```
[*] -g auto Reinstall grub in client disk MBR (only if grub config exists)
[*] -e1 auto Automatically adjust filesystem geometry for a NTFS boot partition if exists
[*] -e2 sfdisk uses CHS from EDD(for non-grub boot loader)
[*] -nogui Use text output only, no TUI/GUI output
[*] -hn0 PC Change MS Win hostname (based on IP address) after clone
[*] -hn1 PC Change MS Win hostname (based on MAC address) after clone
[*] -v Prints verbose messages (especially for udpcast)
[*] -batch Run clone in batch mode (DANGEROUS!)
[*] -c Client waits for confirmation before cloning
[*] -t Client skip restoring the MBR (Master Boot Record)
[*] -t1 Client restores the prebuilt bootloader from syslinux (For Windows only)
[*] -t2 Client skip restoring the EBR (Extended Boot Record)
[*] -r Try to resize the filesystem to fit partition size
[*] -rescue Continue reading next one when disk blocks read errors
[*] -e sfdisk uses the CHS value of hard drive from the saved image
[*] -icrc Ignore CRC checking of partclone
[*] -irhr Do not remove Linux udev hardware record after restoring.
[*] -irvd Do not remove NTFS volume dirty flag after it is restored
[*] -ius Do not update syslinux-related files after restoring.
[*] -lui Do not update Initramfs file(s) on the restored GNU/Linux.
[*] -lcids Skip checking destination disk size before creating partition table
[*] -lefi Skip updating boot entries in EFI NVRAM after restoring
[*] -j1 Write MBR (512 B) again after image is restored. Not OK for partition table differs from that of the image
[*] -j2 Clone_the_hidden_data_between_MBR_and_1st_partition
[*] -cm Check image by MD5 checksums
[*] -cs Check image by SHA1 checksums
[*] -cb Check image by BLAKE2 checksums
[*] -cmf Inspect checksum for files in device after restoring
[*] -a Do NOT force to turn on HD DMA
[*] -o0 Run script in $OCS_PRERUN_DIR before clone starts
[*] -o1 Run script in $OCS_POSTRUN_DIR as clone finishes
[*] -srel Save restoring error log in image dir
[*] -ps Play sound when the job is done
[*] -edio Enable the direct IO mode of Partclone for NVMe SSD
```

Clonezilla advanced extra parameters | Mode: restoredisk |

Choose the mode to create the partition table on the target disk: ***ATTENTION***
(1) TO CREATE A NEW PARTITION TABLE ON THE TARGET DISK. ALL THE DATA ON THE TARGET DEVICE WILL BE ERASED!!! (2) Clonezilla will not restore an image from a large disk (partition) to a smaller disk (partition). However, it can restore an image from a small disk (partition) to a larger disk (partition). (3) If you do NOT want Clonezilla to create a partition table, check -k
Set advanced parameters. If you have no idea, keep the default values and do NOT change anything. Just press Enter.

-k0 Use the partition table from the image
-k Do NOT create a partition table on the target disk
-k1 Create partition table proportionally
-k2 Enter command line prompt to create partition manually later
-j0 Use dd to create partition (NOT OK if logical drives exist)
exit Exit

<Ok> <Cancel>

Encore des choix ou nous allons laisser par défaut

| Mode: restoredisk |

The action to perform when everything is finished:

-p choose Choose reboot/shutdown/etc when everything is finished
-p true Enter command line prompt
-p reboot Reboot
-p poweroff Shutdown

<Ok> <Cancel>

Comme avant on choisit ce que l'on souhaite faire une fois l'opération fini.

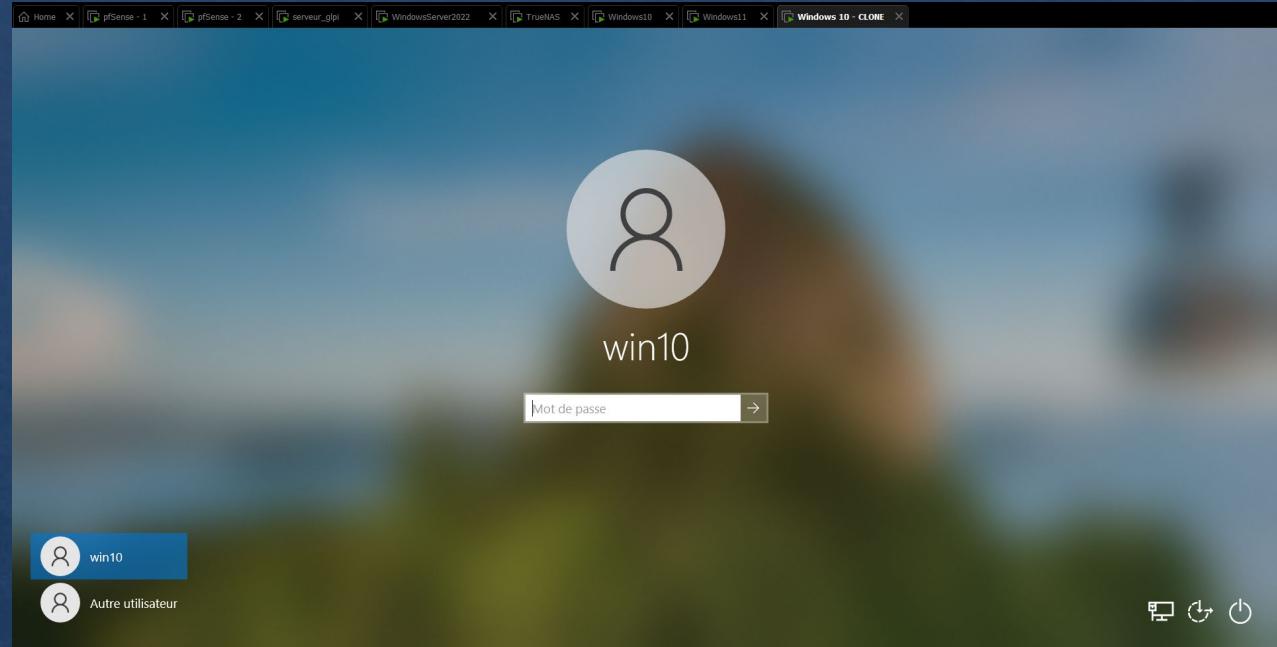
Etape 5 – Tests

```
Partclone v0.3.27 http://partclone.org
Starting to check image (-)
Calculating bitmap... Please wait...
done!
File system: NTFS
Device size: 42.0 GB = 10258879 Blocks
Space in use: 27.7 GB = 6770778 Blocks
Free Space: 14.3 GB = 3488101 Blocks
Block size: 4096 Byte

Elapsed: 00:03:30 Remaining: 00:06:15 Rate: 2.84GB/min
Current Block: 2717295 Total Block: 10258879

Data Block Process:
[██████████] 35.89%

Total Block Process:
[██████████] 26.49%
```



Le clone s'installe et une fois la machine redémarrer nous arrivons sur Windows.
Le clone est donc bien fonctionnel.

Etape 5 – Problème rencontré

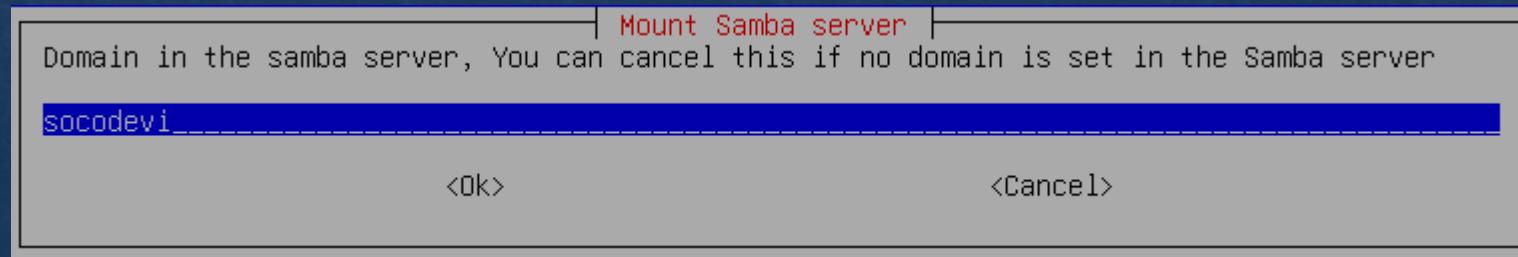
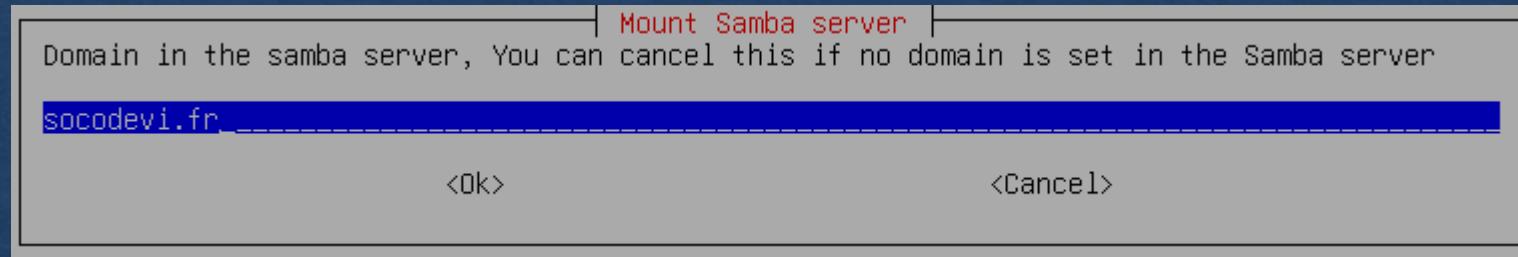
```
Mounting Samba server by:  
LC_ALL=C mount -t cifs "//192.168.100.200/Public/Clones" /home/partimag -o user="administrateur, domain=socodevi.fr"  
Password for administrateur@//192.168.100.200/Public/Clones:  
mount error(13): Permission denied  
Refer to the mount.cifs(8) manual page (e.g. man mount.cifs) and kernel log messages (dmesg)
```

L'un des problèmes rencontrés est au moment du clonage, un message d'erreur m'indique que je n'ai pas les permissions requises.

Etape 5 – Solution trouvée

Après avoir chercher le souci de droit et permissions du dossier public sur TrueNAS, je suis tomber sur un forum qui a annoncer avoir eu un souci similaire et s'être rendu compte que c'était une erreur de nom de domaine.

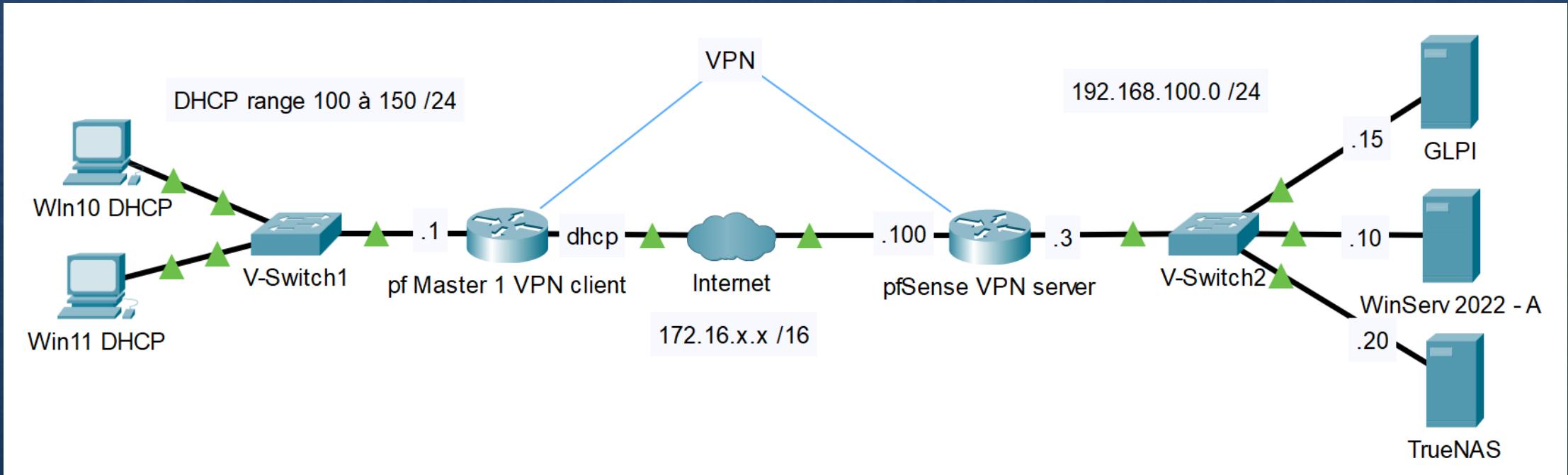
J'ai alors refait la manipulation en modifiant le nom de domaine sans mettre le TDL et le souci était réglé.



Etape 6 – ESXi



Etape 6 – Architecture réseau

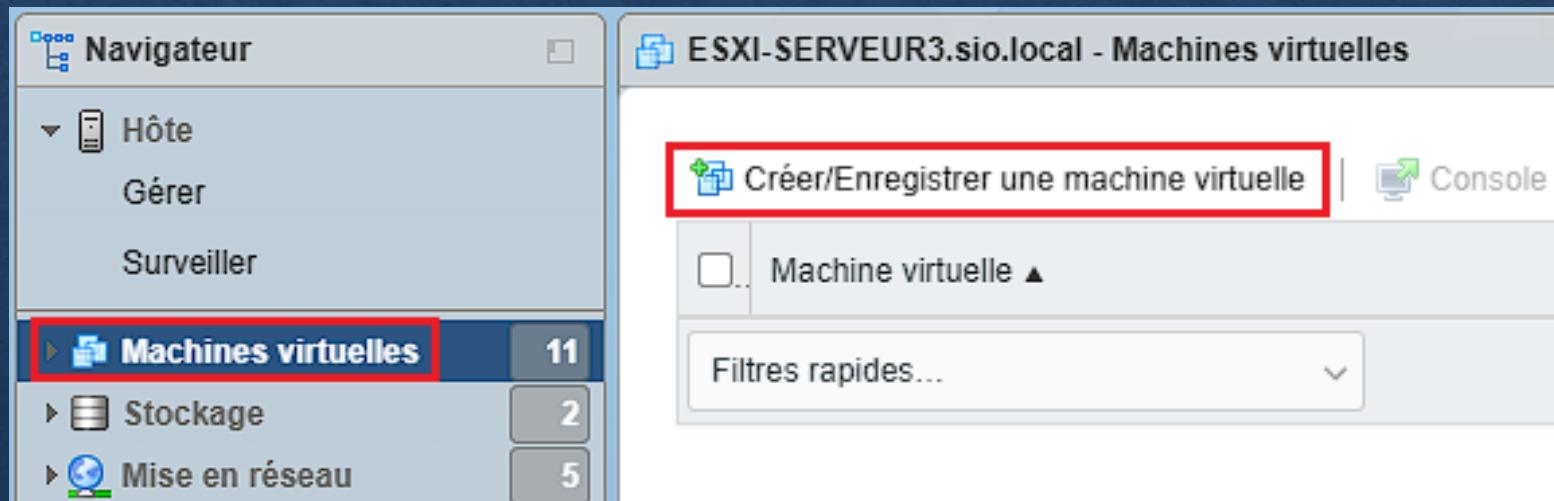


Etape 6 – Mise en place

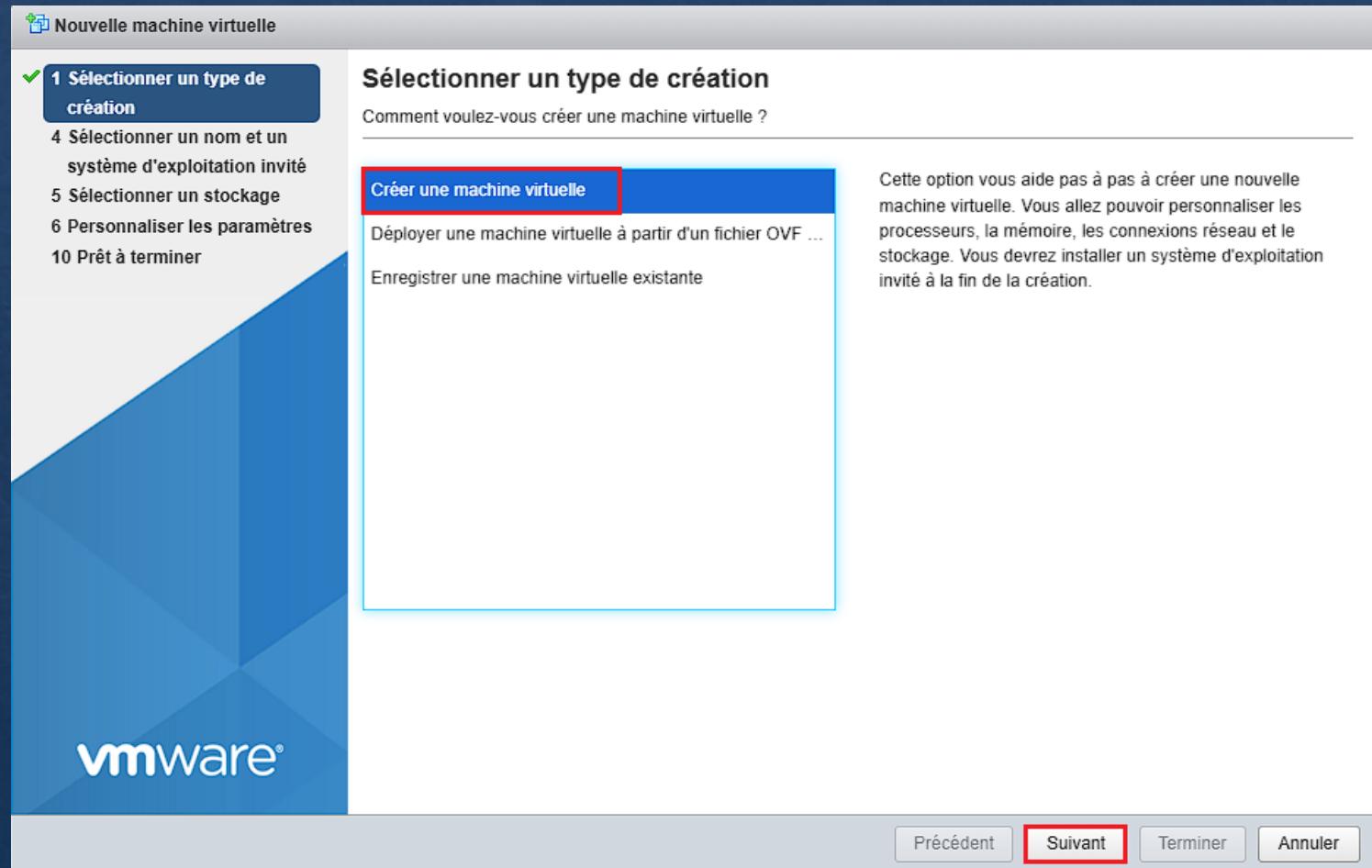
Nous allons commencer par mettre en place le pfSense distant qui sera notre serveur VPN.

Sur le serveur ESXi nous allons créer notre pfSense.

Pour se faire nous allons dans l'onglet « **Machines virtuelles** » puis « **créer une machine virtuelle** ».

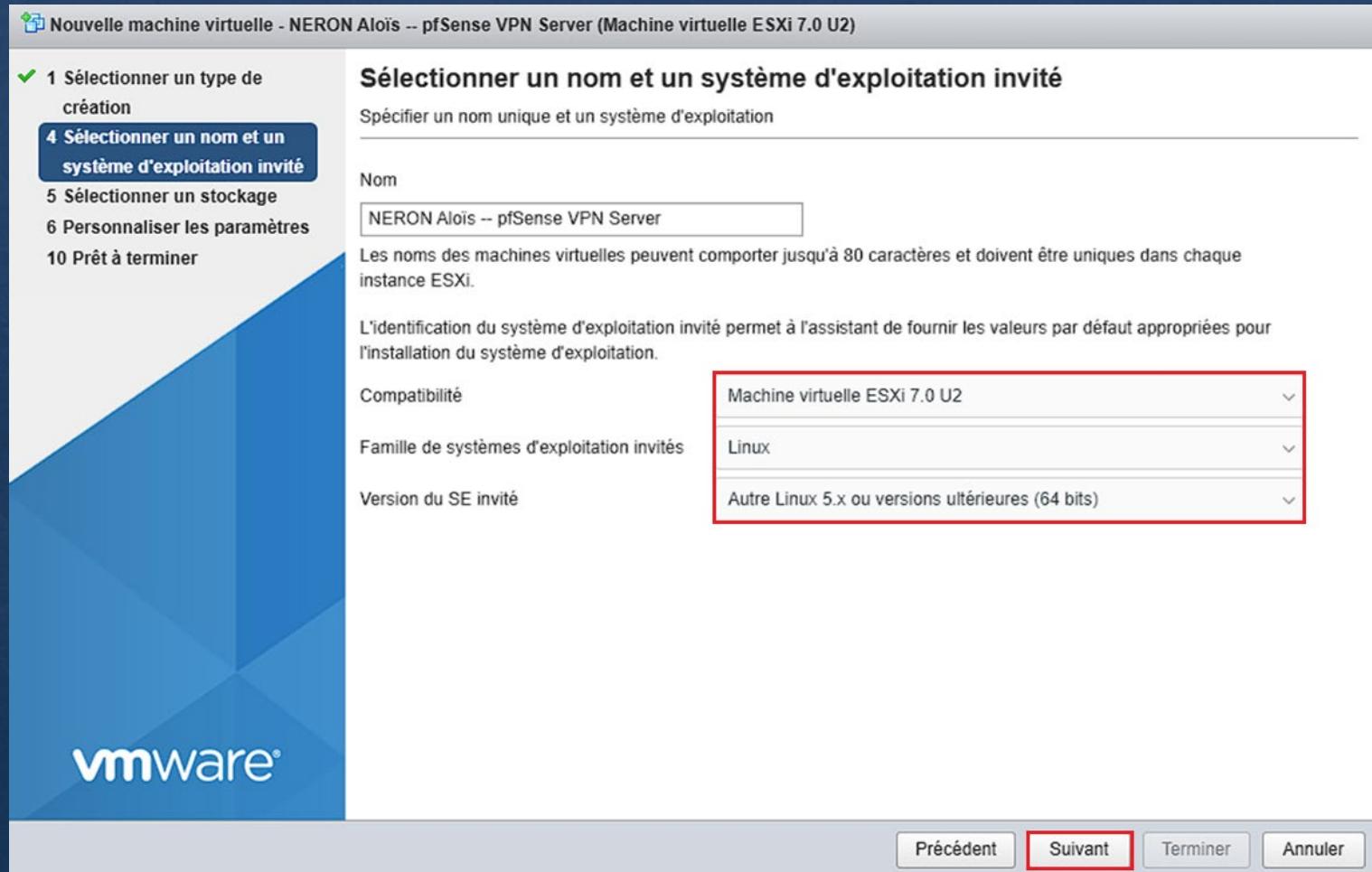


Etape 6 – Mise en place



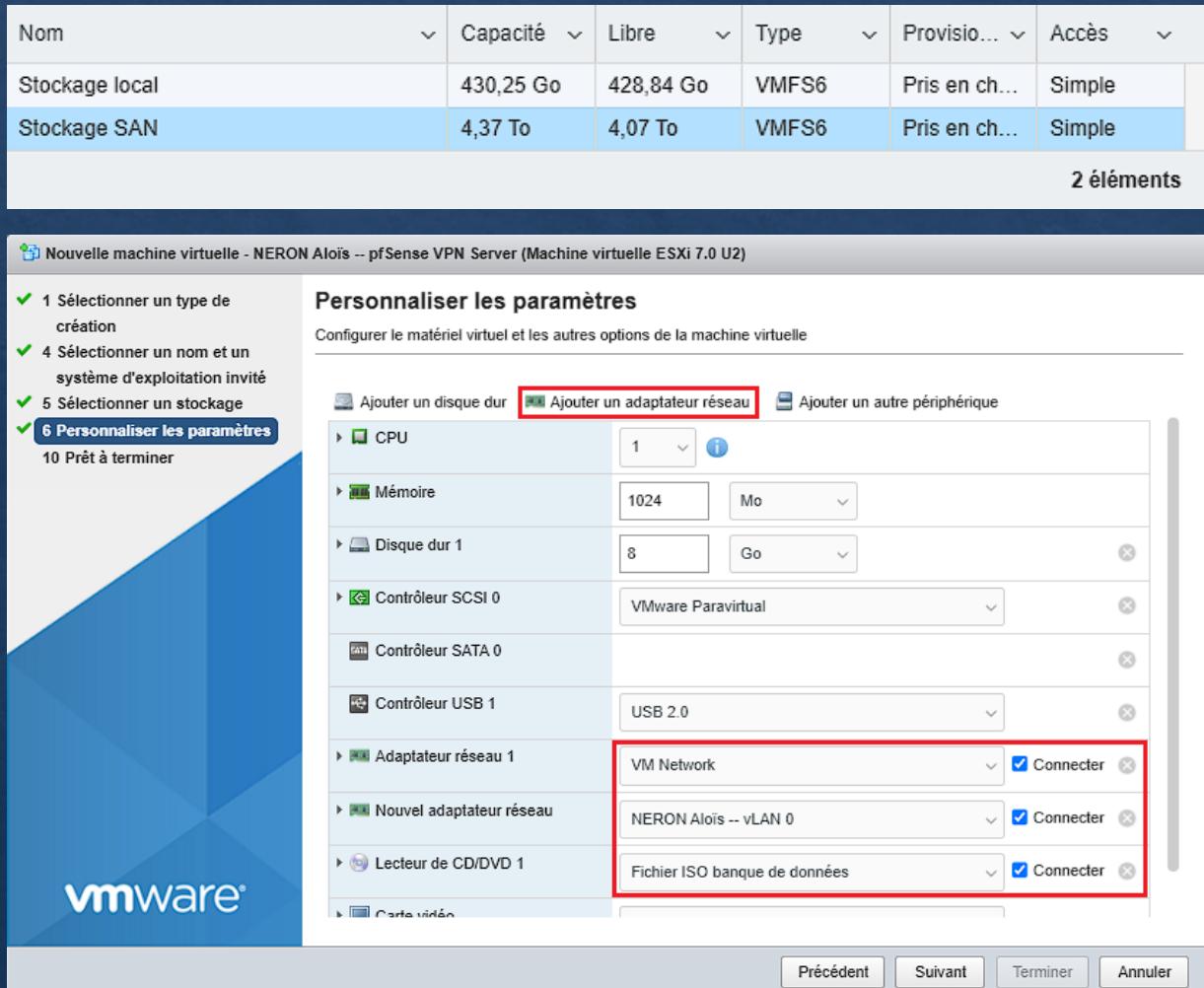
Sélectionner
« créer une machine virtuelle »
puis « Suivant »

Etape 6 – Mise en place



On lui met les paramètres ci-dessous puis « suivant ».

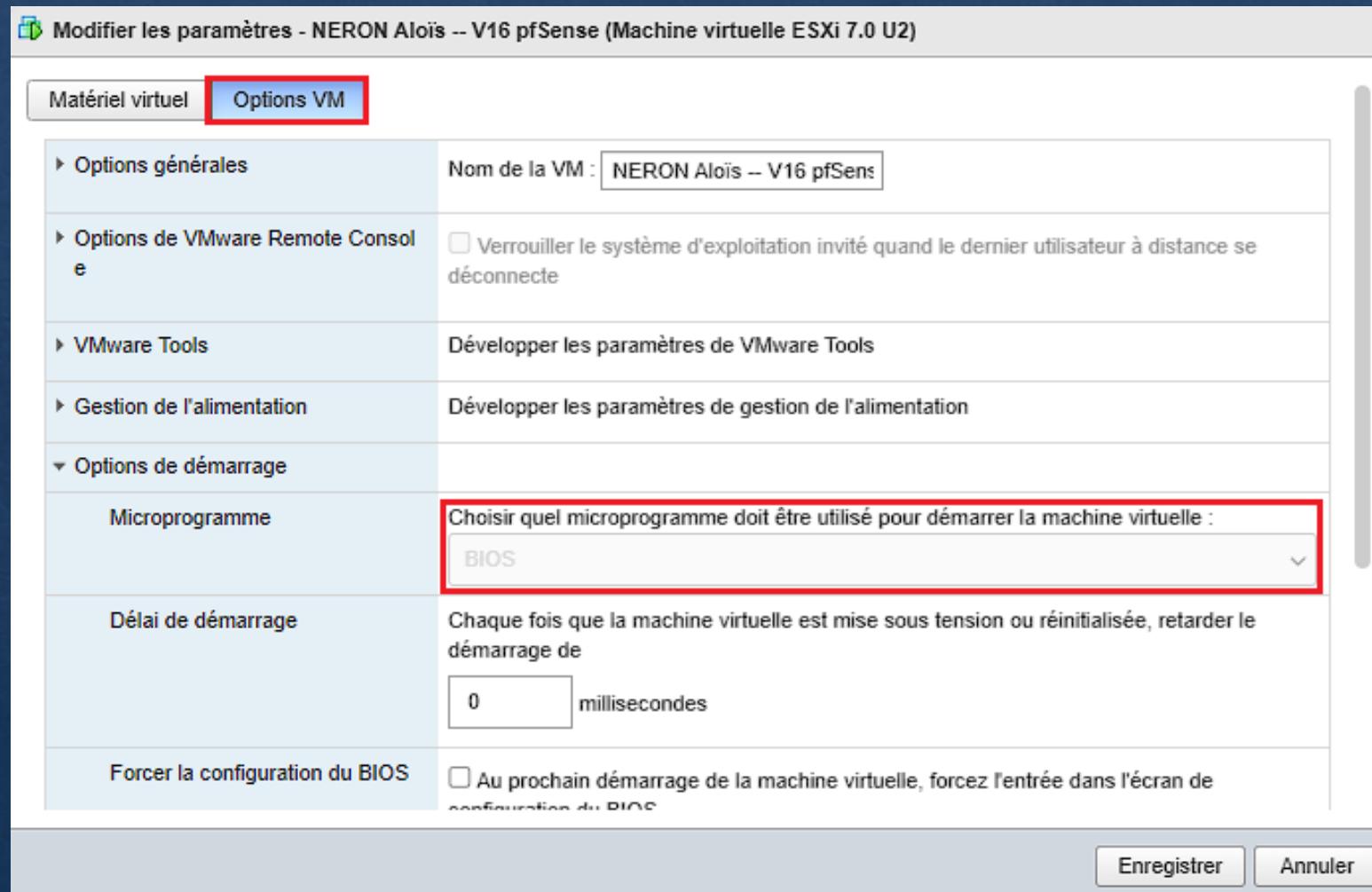
Etape 6 – Mise en place



On sélectionne le SAN pour stocker notre VM.

Au niveau des composants il faudra rajouter une carte réseaux et mettre l'ISO de pfSense dans le lecteur CD/DVD.

Etape 6 – Mise en place



Pour pouvoir lancer la VM et la configuration de pfSense il faut d'abord choisir le bon firmware qui est en UEFI par défaut et le mettre en BIOS.

Etape 6 – Mise en place

The screenshot shows the pfSense web interface under the 'VPN' menu. The 'OpenVPN' section is selected, and the 'Servers' tab is active. A sub-section titled 'OpenVPN Servers' is displayed with columns for Interface, Protocol / Port, Tunnel Network, Mode / Crypto, Description, and Actions. In the 'Actions' column, there is a green button with a white plus sign labeled 'Add', which is highlighted with a red box.

Pour le pfSense serveur nous restons sur la page par défaut qui est déjà sur « Servers » et on clic sur ‘Add’

Etape 6 – Mise en place

General Information	
Description	VPN serveur
A description of this VPN for administrative reference.	
Disabled	<input type="checkbox"/> Disable this server
Set this option to disable this server without removing it from the list.	
Unique VPN ID	Server 1 (ovpns1)
Mode Configuration	
Server mode	Peer to Peer (Shared Key)
WARNING: OpenVPN has deprecated shared key mode as it does not meet current security standards. Shared key mode will be removed from future versions. Convert any existing shared key VPNs to TLS and do not configure any new shared key OpenVPN instances.	
Device mode	tap - Layer 2 Tap Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)	

On décoche la case pour activer le vpn serveur, on y met le mode de clé partagé et « device mode » en couche 2.

Etape 6 – Mise en place

Endpoint Configuration

<u>Protocol</u>	UDP on IPv4 only
<u>Interface</u>	WAN
The interface or Virtual IP address where OpenVPN will receive client connections.	
<u>Local port</u>	1194
The port used by OpenVPN to receive client connections.	

Nous utiliserons l'ipv4 avec l'interface WAN pour le VPN et on y laisse le port par défaut.

Etape 6 – Mise en place

Cryptographic Settings

Shared Key

```
#  
# 2048 bit OpenVPN static key  
#  
-----BEGIN OpenVPN Static key V1-----  
0ad9f6c520f71e013000d2c7fed230a7
```

Paste the shared key here

Data Encryption Algorithms

AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)

Available Data Encryption Algorithms
Click to add or remove an algorithm from the list

AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. i

Fallback Data Encryption Algorithm

AES-256-CBC (256 bit key, 128 bit block)

The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.

Auth digest algorithm

SHA256 (256-bit)

The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto

No Hardware Crypto Acceleration

Pour la partie chiffrement on met de côté la clé de partage que nous devrons copier dans la configuration cliente par la suite.

Nous laisserons les algorithmes par défaut.

Etape 6 – Mise en place

Tunnel Settings

IPv4 Tunnel Network

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

Petite subtilité pour le serveur uniquement, il faut lui mettre une IP pour pouvoir finaliser la configuration.

Etape 6 – Mise en place

The screenshot shows the pfSense web interface under the 'Clients' tab. The 'Clients' tab is highlighted with a red underline. Below it, there's a table titled 'OpenVPN Clients' with columns: Interface, Protocol, Server, Mode / Crypto, Description, and Actions. In the 'Actions' column, there's a green button with a white plus sign and the word 'Add'.

OpenVPN Clients					
Interface	Protocol	Server	Mode / Crypto	Description	Actions
					+ Add

Pour le pfSense client, nous devons aller sur l'onglet ‘Clients’ et on clic sur ‘Add’

Etape 6 – Mise en place

Endpoint Configuration

Protocol	UDP on IPv4 only
Interface	WAN
The interface used by the firewall to originate this OpenVPN client connection	
Local port	
Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.	
Server host or address	172.16.100.100
The IP address or hostname of the OpenVPN server.	
Server port	1194
The port used by the server to receive client connections.	
Proxy host or address	
The address for an HTTP Proxy this client can use to connect to a remote server. TCP must be used for the client and server protocol.	
Proxy port	
Proxy Authentication	none
The type of authentication used by the proxy server.	

La configuration est similaire à la différence où nous devrons y informer l'IP distante du serveur VPN.

Etape 6 – Mise en place

Shared Key

```
#  
# 2048 bit OpenVPN static key  
#  
-----BEGIN OpenVPN Static key V1-----  
0ad9f6c520f71e013000d2c7fed230a7  
4243d657bf04bbf708da986128dd7036  
da0a9ada4d0797a4088e51b6617226bb  
45a09db3311b58786d43f460c82c121c  
cbc504321903c74d813bf3c4608f0bab  
0b2df820920f1dbe53f6160265ddee6f  
50a46e68767d519bf3bbfe180a6763ea  
d6bbccc0664145da322ae2f227af7580  
fad01609ac30cd0b2d98050ec67bbb41  
51717b9496371133b5bb5d13ed425c1a  
042ae3a9f5008f2f6f4356be89afbd9  
a20a338acab32390714fe27c7d273109  
2bb92adb78fc424641e5e0d15d21ee4d  
9fd119e237f3be939817a4cbc6ee2f68  
c54437393226ba4d9c1255812ecef059  
fa0c158922afc00f5929deb9c4758cf2  
-----END OpenVPN Static key V1-----
```

On y copie-colle la clé de partage générée par le serveur au début et ce sera tout pour la config cliente.

Etape 6 – Mise en place

Avant de passer à la configuration du FW il faut activer toutes les nouvelles interfaces qui se sont créée avec le VPN.

The screenshot shows the pfSense web interface for managing network ports. At the top, there is a dropdown menu labeled "Available network ports:" containing the option "ovpnc1 (vpn client - pfSense master)". To the right of the dropdown is a green button with a plus sign and the text "Add". Below this, the main interface title is "Interfaces / OPT1 (ovpnc1)". Underneath the title, a dark bar contains the text "General Configuration". At the bottom of this bar are two buttons: "Enable" and "Enable interface". The "Enable interface" button has a checked checkbox next to it.

Etape 6 – Mise en place

Il faut aussi désactiver le blocage des réseaux privés sur toutes les interfaces.

Reserved Networks	
Block private networks and loopback addresses	<input type="checkbox"/> Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	<input type="checkbox"/> Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Etape 6 – Mise en place

Il faut rajouter un bridge entre notre nouvelle interface VPN et notre LAN.

Interfaces / Bridges

Bridge Interfaces			
Interface	Members	Description	Actions
BRIDGE0	LAN, OPT2	pont entre LAN et WAN VPN	 

Cela crée encore une nouvelle interface qu'il faut aussi activer et configurer comme les autres.

Etape 6 – Mise en place

The screenshot shows four panels of the pfSense firewall configuration interface, each displaying a list of rules:

- WAN Panel:** Shows one rule for port 1194 (OpenVPN) from WAN address to *.
- OPT1 Panel:** Shows one rule for port 0/482 KiB from * to *.
- OPT2 Panel:** Shows one rule for port 0/0 B from * to *.
- OpenVPN Panel:** Shows one rule for port 0/720 B from * to *.

Each panel includes a header with interface names (Floating, WAN, LAN, OPT1, OPT2, OpenVPN) and a "Rules (Drag to Change Order)" section with columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions (edit, copy, delete).

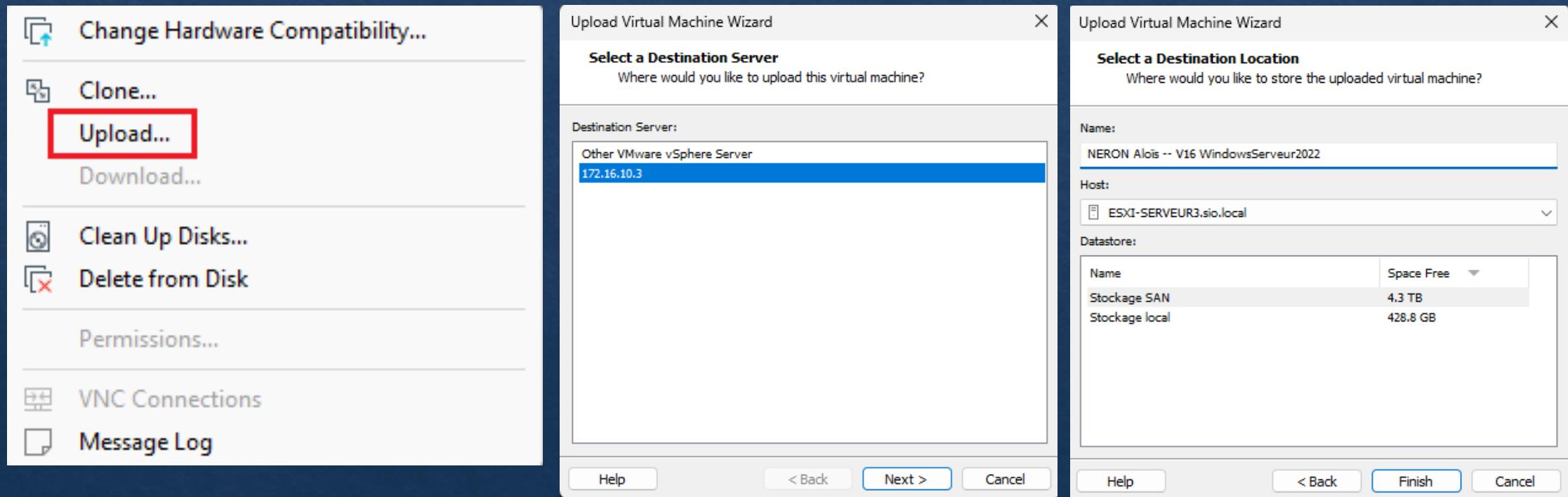
Configuration du FW
dans les deux pfSense

Etape 6 – Mise en place

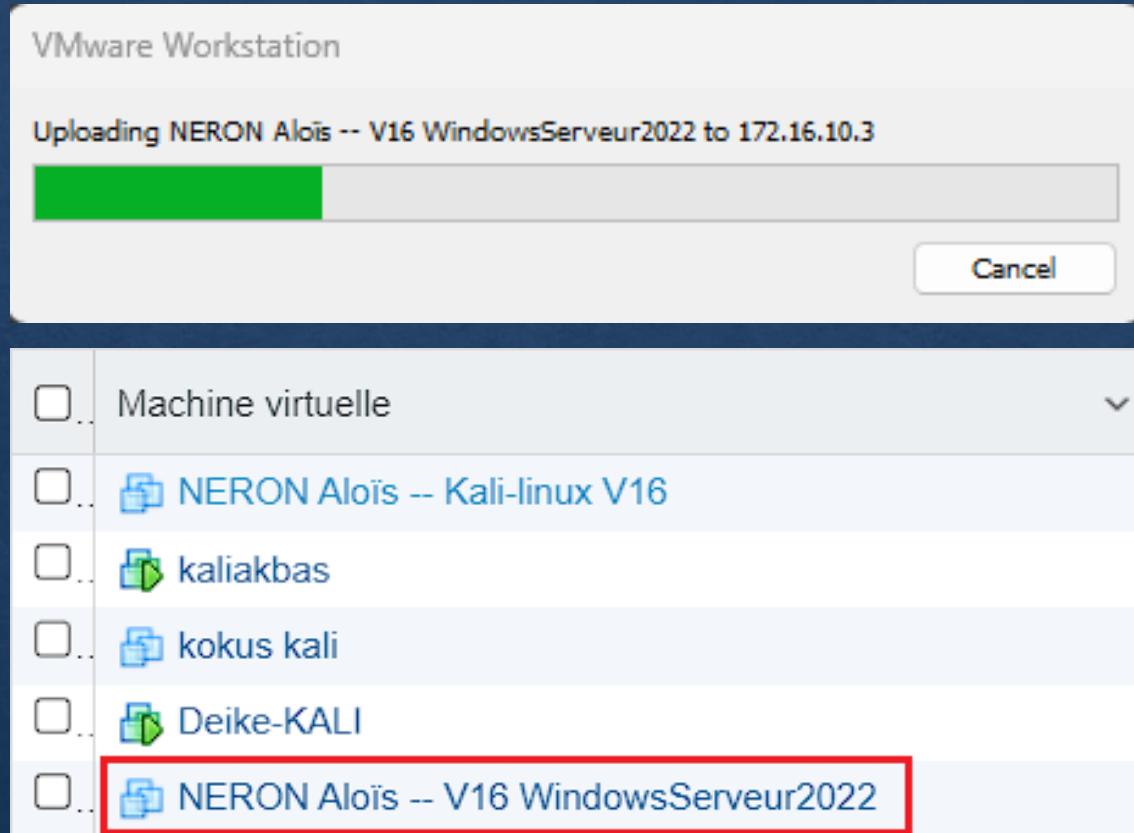
Il est possible d'exporter les VM sur l'ESXi depuis Workstation directement.

Pour ce faire : clic droit sur la VM puis « manage » et « upload »

On rentre les infos du serveur distant si nécessaire, pour ma part c'était déjà fait. On lui donne un nom et on choisit l'endroit sur le serveur, dans notre cas le SAN.

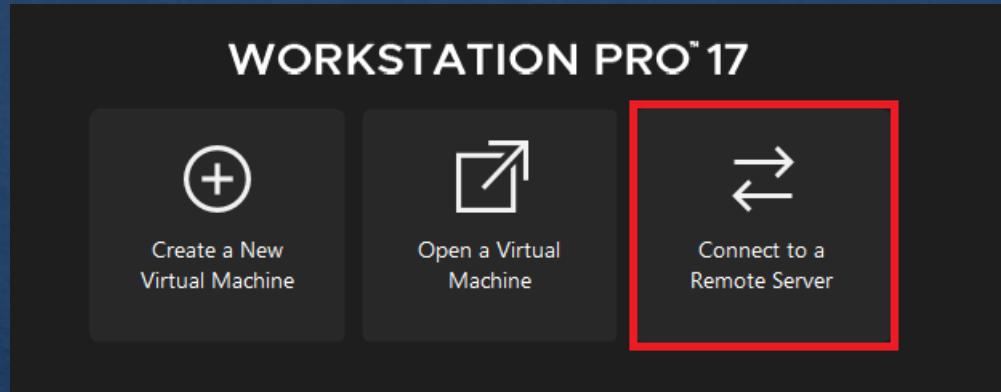


Etape 6 – Mise en place



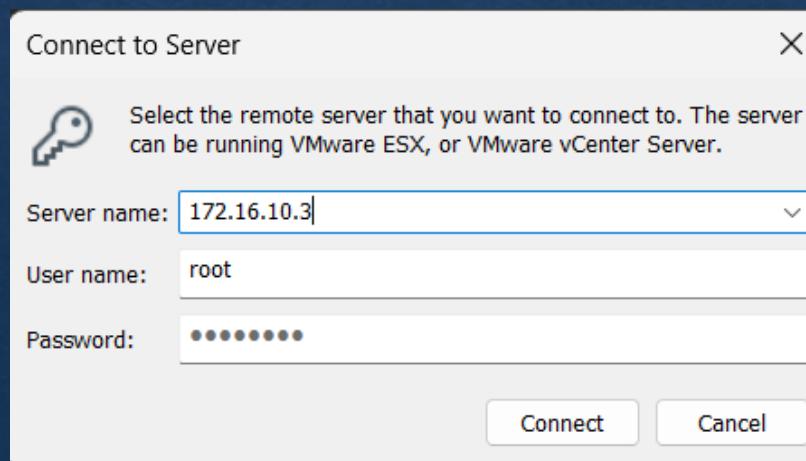
Un fois l'exportation terminé, on retrouvera notre VM dans l'onglet « machines virtuelles »

Etape 6 – Mise en place



Nous avons la possibilité de lancer les serveurs directement sur l'interface web de l'ESXI mais je vais le faire directement à travers l'hyperviseur Workstation sur mon pc.

Comme pour exporter les VM nous rentrons les infos du serveur distant afin d'y voir nos VM.

A screenshot of the VMware ESXi host interface. At the top, it shows the IP address 172.16.10.3. Below are buttons for "Create a new virtual machine", "Restart host", "Shut down host", and "Enter maintenance mode". On the right, it shows "CPU Usage: 351 MHz" and "Memory Usage: 18.7 GB". A section titled "Virtual Machines" lists the following VMs and their status:

Name	Status
NERON Aloïs -- V16 WindowsServer2022	Powered on
NERON Aloïs -- V16 TrueNAS	Powered on
NERON Aloïs -- V16 pfSense	Powered on
NERON Aloïs -- V16 GLPI	Powered on
Matéo-Pêche-Pfsense-VPN	Powered on

Etape 6 – Tests

Client Instance Statistics								
Name	Status	Last Change	Local Address	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service
ovpnc1 client vpn UDP4	Connected (Success)	Thu Nov 7 15:24:44 2024	172.16.5.71:54801		172.16.100.100:1194	608 B	80 B	  
Peer to Peer Server Instance Statistics								
Name	Status	Last Change	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service	
ovpns1 VPN@SOCODEVI UDP4:1194	Connected (Success)	Thu Nov 7 15:23:58 2024	10.0.8.1	172.16.5.71	960 B	1 KiB	  	

Etape 6 – Tests

```
└─(toto㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:00:7b:1d brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.66/24 brd 192.168.100.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe00:7b1d/64 scope link proto kernel ll
        valid_lft forever preferred_lft forever
```

```
C:\Users\win10>ping 192.168.100.66
```

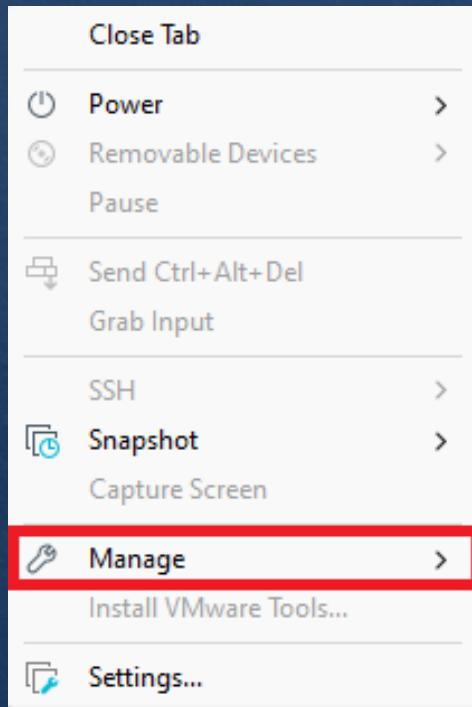
```
Envoi d'une requête 'Ping' à 192.168.100.66 avec 32 octets de données :
Réponse de 192.168.100.66 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.100.66 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.100.66 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.100.66 : octets=32 temps=2 ms TTL=64
```

La machine Windows ping la machine linux de qui se trouve de l'autre côté du VPN.

Etape 6 – Problèmes rencontrés

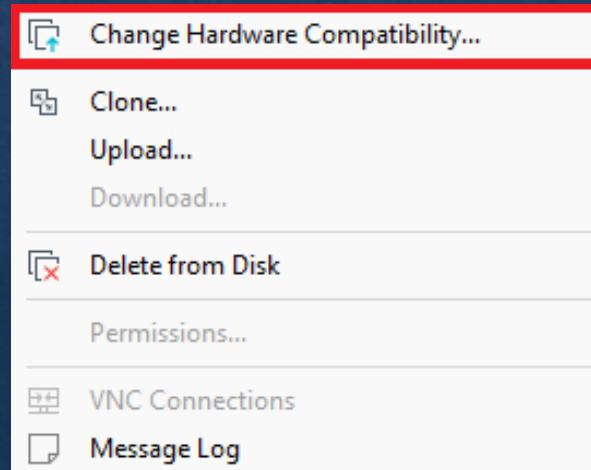
Le projet a été fait avec des VM créées sur des versions de Workstation récente (V.17), cependant celles-ci ne sont pas compatibles avec les dernières versions de ESXi. Il nous était alors impossible d'importer les VM sur le serveur.

Etape 6 – Solutions trouvées

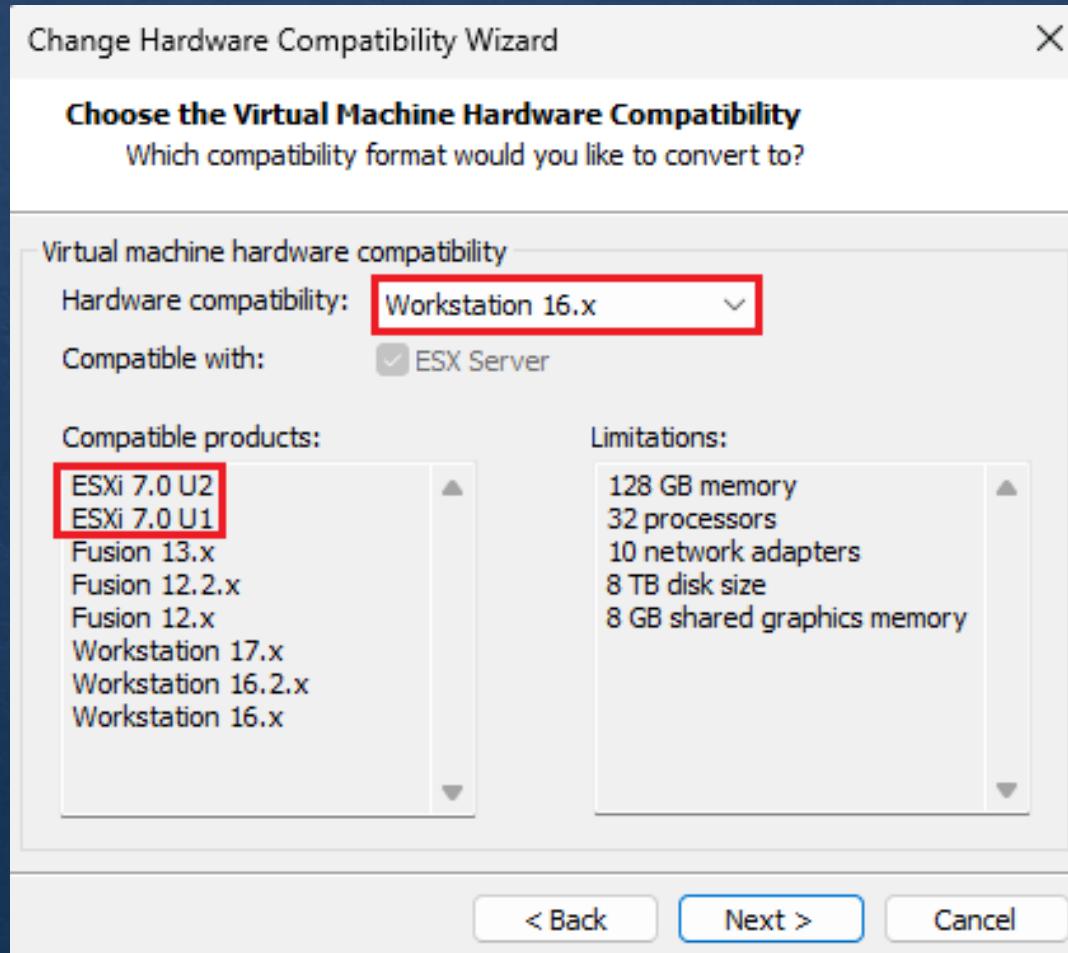


Pour changer la version d'une VM :

On choisit la VM souhaiter puis dans l'onglet « VM », « manage » et enfin « Change Hardware Compatibility »



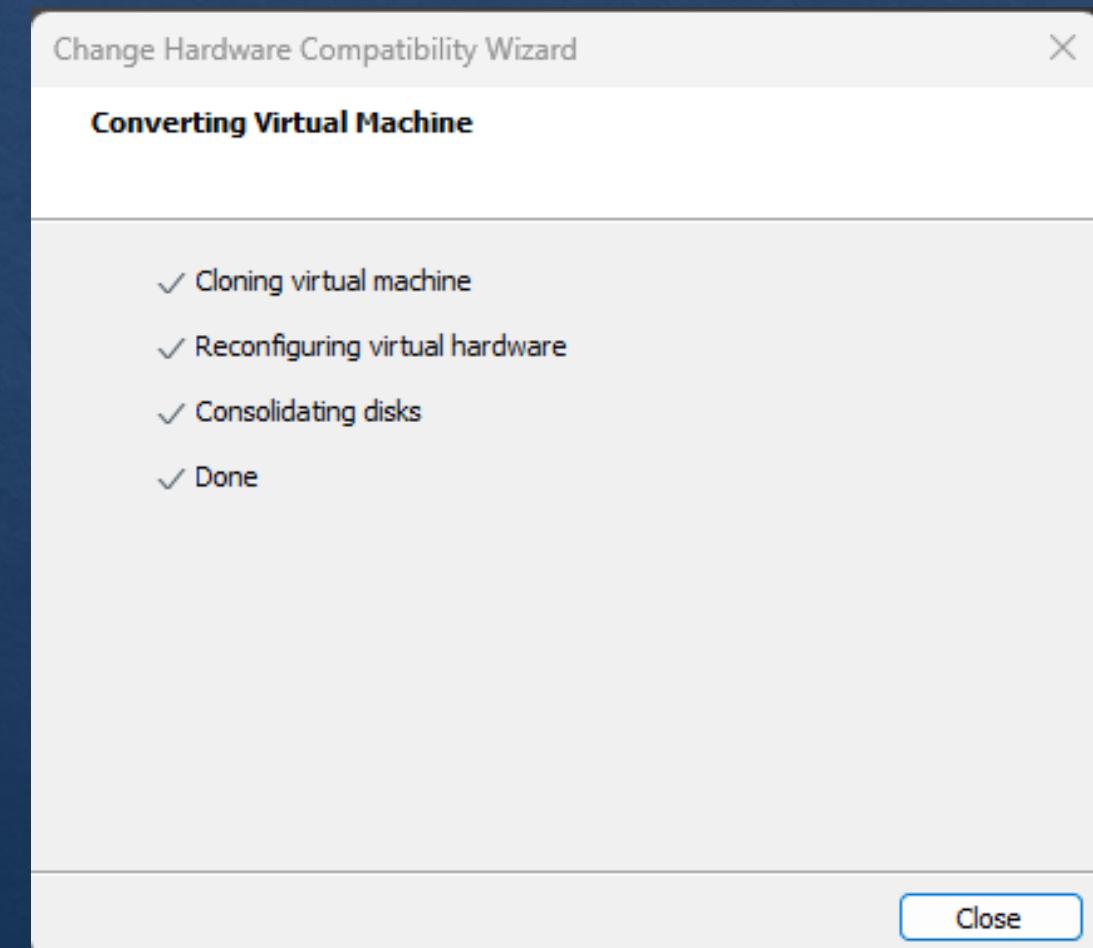
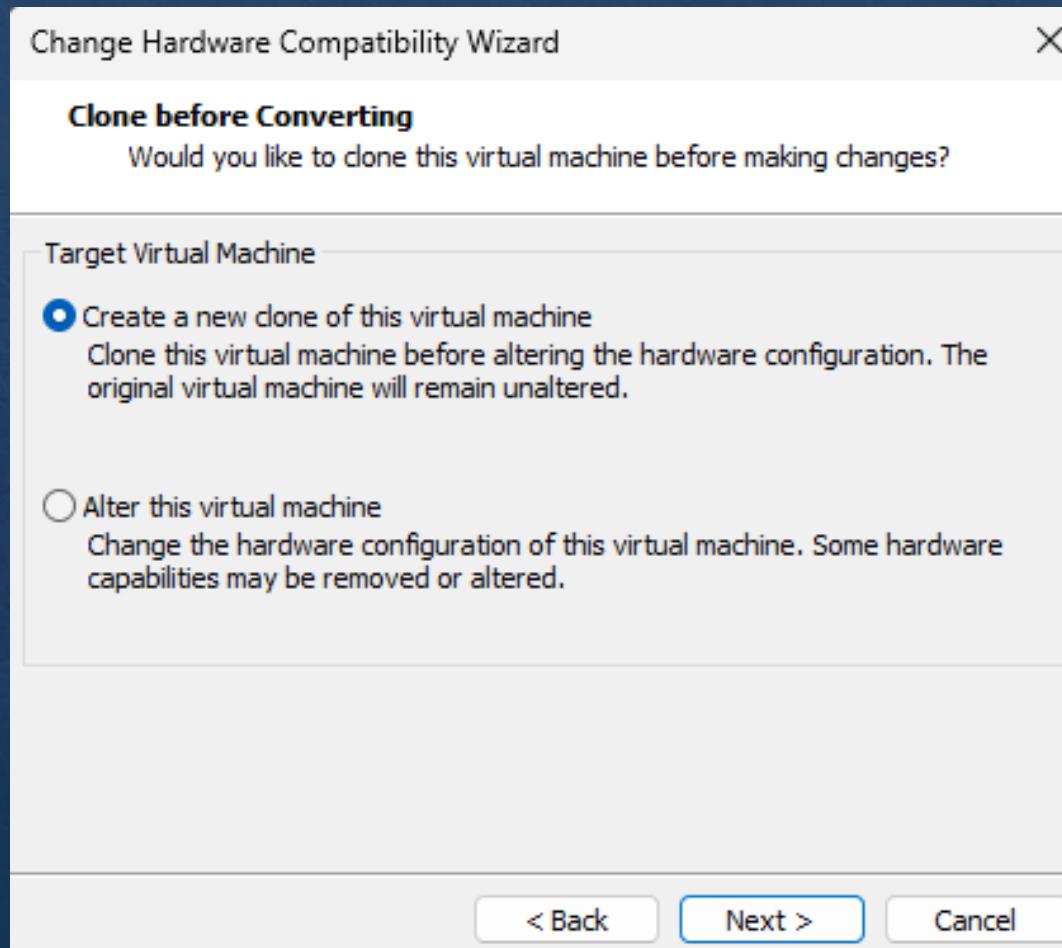
Etape 6 – Solutions trouvées



La version la plus récente qui reste compatible avec l'ESXI est la 16.

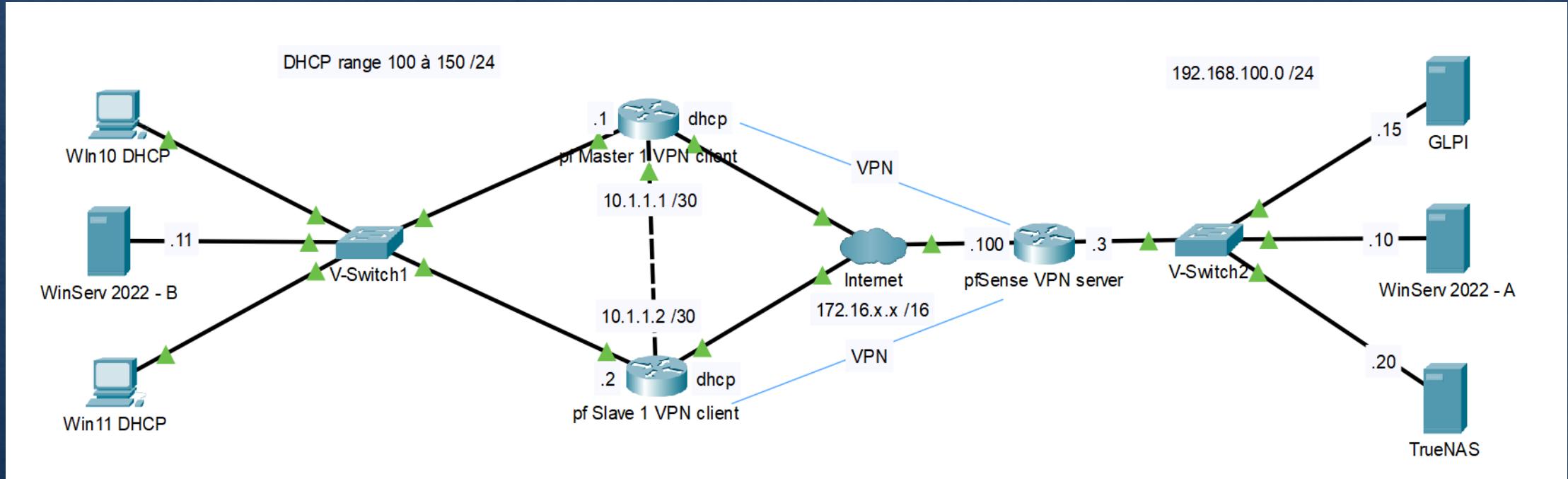
On la sélectionne puis « next ».

Etape 6 – Solutions trouvées



Etape 6 – Redondance

Etape 6 – Architecture réseau



Etape 6 – Présentation

Pour mettre en lien toutes les étapes du projet et les TP faits en classe, j'aimerais rajouter au projet les différentes redondances pour garder cette disponibilité au sein de l'entreprise en cas de soucis technique inattendu.

Pour ce faire, je vais y rajouter la redondance pfSense de l'étape 1 au VPN mais surtout la redondance du Windows Serveur.

Etape 6 – Mise en place - VPN

Etant donné que la redondance est déjà en place mais pas le VPN, il suffira simplement de mettre en place un second client de la même manière que le pfSense master, activer les nouvelles interfaces. Le FW n'a même pas besoins d'être configurer car la synchronisation duplique déjà les règles de filtrage ce qui est très pratique.

Etape 6 – Mise en place - VPN

On vérifie les interfaces après la création du second client VPN

Interfaces / Interface Assignments									
Interface Assignments	Interface Groups	Wireless	VLANs	QinQs	PPPs	GREs	GIFs	Bridges	LAGGs
Interface	Network port								
WAN	em0 (00:0c:29:91:91:21)								
LAN	em1 (00:0c:29:91:91:2b)								 Delete
pfSync	em2 (00:0c:29:91:91:35)								 Delete
OPT2	ovpncl1 (vpn client - pfSense master)								 Delete
OPT3	BRIDGE0 (SLAVE – pont LAN & WAN VPN)								 Delete

Etape 6 – Mise en place - VPN

On vérifie que la synchronisation a bien dupliquée les règles de filtrage.

Floating	WAN	LAN	PFSYNC	OPT2	OPT3	OpenVPN					
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	*	*	*	*	*	none			
Floating	WAN	LAN	PFSYNC	OPT2	OPT3	OpenVPN					
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	*	*	*	*	*	none			
Floating	WAN	LAN	PFSYNC	OPT2	OPT3	OpenVPN					
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1/3 KiB	IPv4 *	*	*	*	*	*	none			

Etape 6 – Mise en place - VPN

Enfin on regarde l'état du tunnel

Client Instance Statistics									
Name	Status	Last Change	Local Address	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service	
ovpnclient1 vpn client - pfSense master	Connected (Success)	Fri Nov 29 8:14:40 2024	172.16.5.94:43844		172.16.100.100:1194	3.34 MiB	24 KiB		

On constate que le VPN créé sur le pfSense slave a finalement été écraser par celui du pfSense master du à la synchronisation. Cependant je ne sais pas s'il le fait aussi pour les interfaces étant donné qu'il faut les activer manuellement.

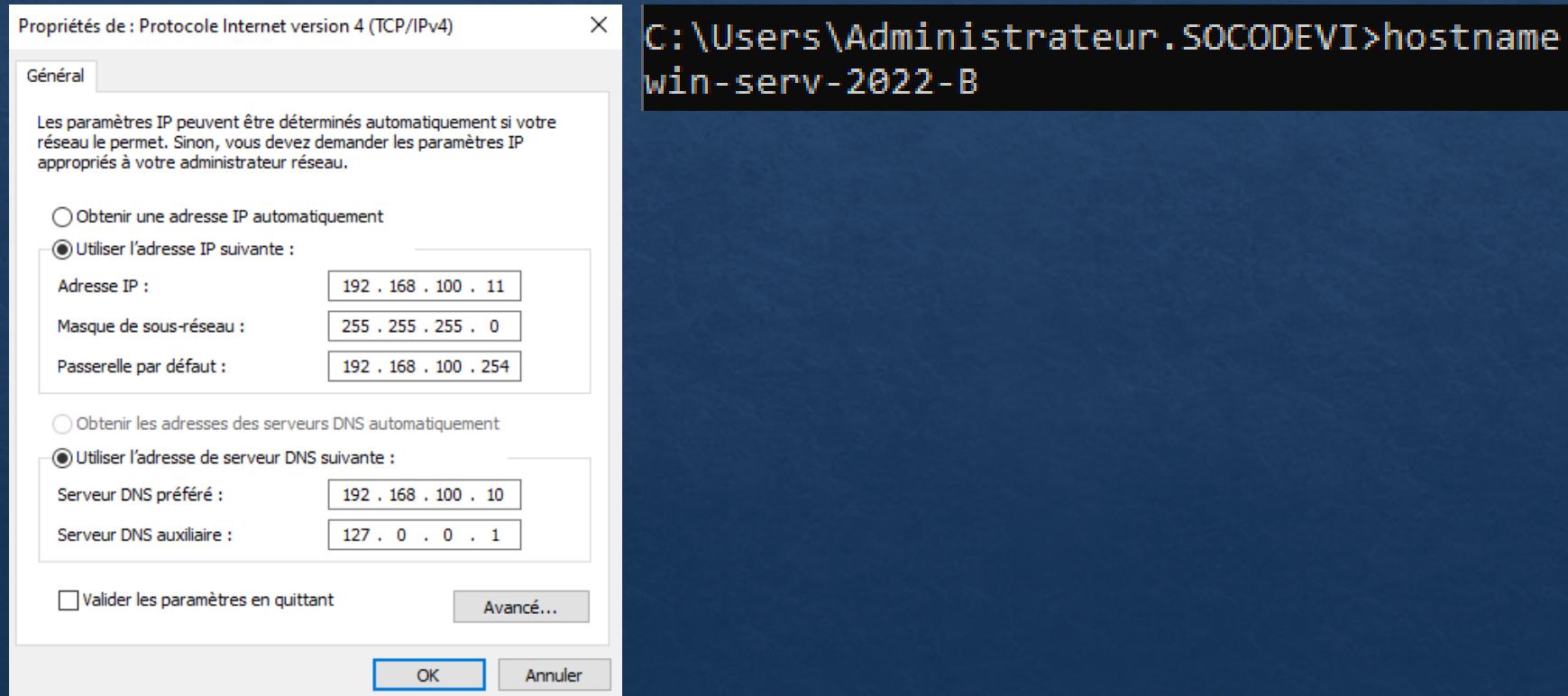
Etape 6 – Mise en place – WinServ2022 B

J'ai fait le choix de positionner la redondance de l'AD dans le LAN en partant du principe qu'il serait plus judicieux de l'avoir dans une infrastructure physique différente en cas de problèmes dans le LAN distant afin d'éviter que la redondance soit endommagée en même temps que l'AD principal.

Même si la redondance n'est pas complète (pas de redondance des GPO par exemple) cela permettra au minimum d'avoir un accès internet provisoire le temps de résoudre le souci.

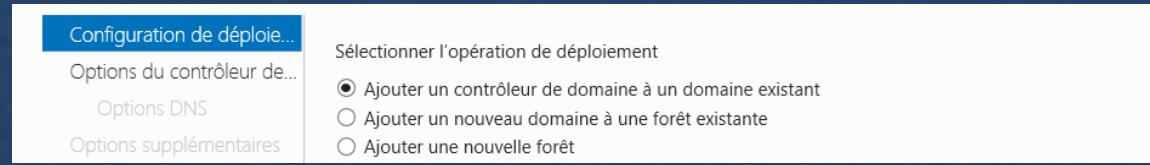
Etape 6 – Mise en place – WinServ2022 B

Pour mettre en place un contrôleur de domaine secondaire, on commence par créer une nouvelle machine vierge qu'il faudra renommée d'entrée et installer le service ADDS. On lui mettra une configuration IP du domaine sans oublier de mettre l'AD principal en DNS.



Etape 6 – Mise en place – WinServ2022 B

Au moment de l'installation de l'AD il faudra choisir l'option
« Ajouter un contrôleur de domaine à un domaine existant »

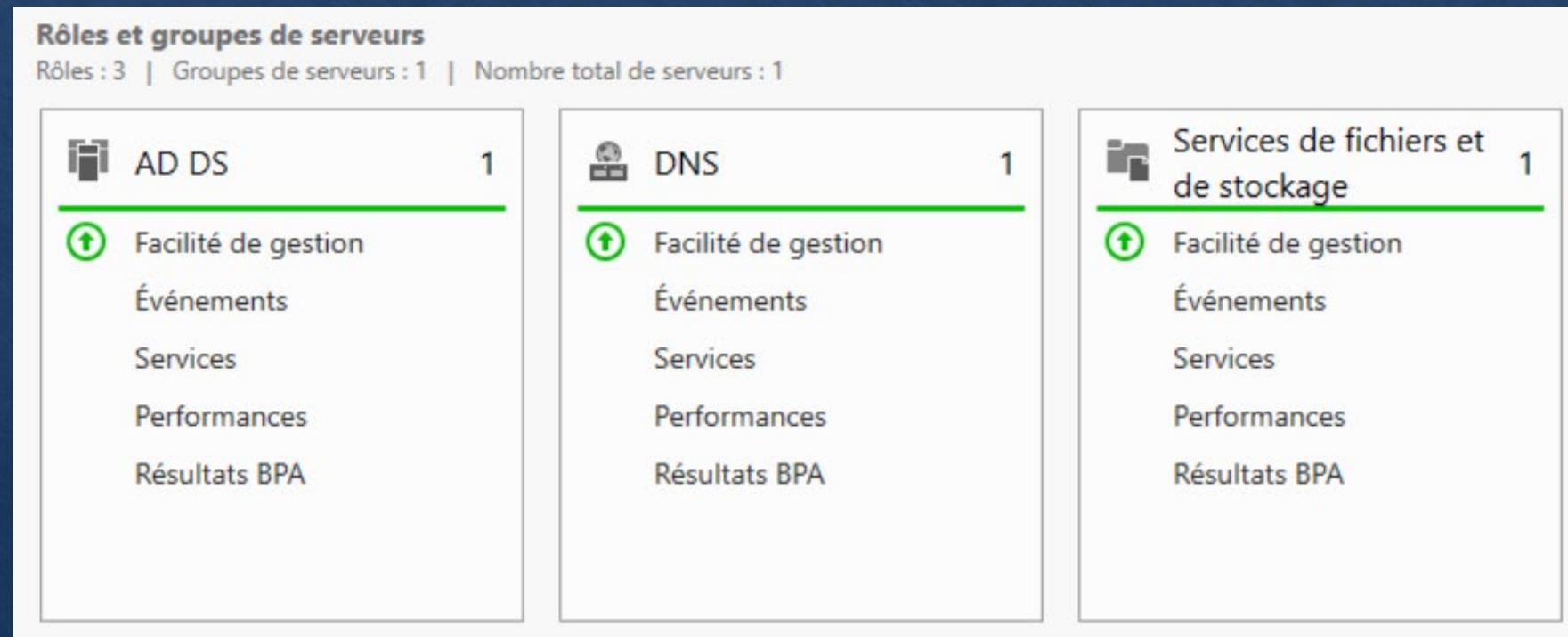


Dans « options supplémentaires » on y indique notre AD principal.



Etape 6 – Mise en place – WinServ2022 B

Une fois l'installation fini on doit apercevoir les serveurs installés sur le principal apparaître sur le nouveau serveur.



Etape 6 – Mise en place – WinServ2022 B

Le DHCP est configuré mais il n'est pas répliqué. Il nous faut alors créer un basculement automatique depuis le serveur principal.

Pour ce faire on sélectionne notre serveur secondaire et on y met les paramètres souhaités.

Configurer un basculement

Spécifier le serveur partenaire à utiliser pour le basculement

Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire : Ajouter un serveur

Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

Configurer un basculement

Créer une relation de basculement

Créer une relation de basculement avec le partenaire win-serv-2022-b

Nom de la relation : failover DHCP

Délai de transition maximal du client (MCLT) : 1 heures 0 minutes

Mode : Serveur de secours

Configuration du serveur de secours

Rôle du serveur partenaire : Veille

Adresses réservées pour le serveur de secours : 10 %

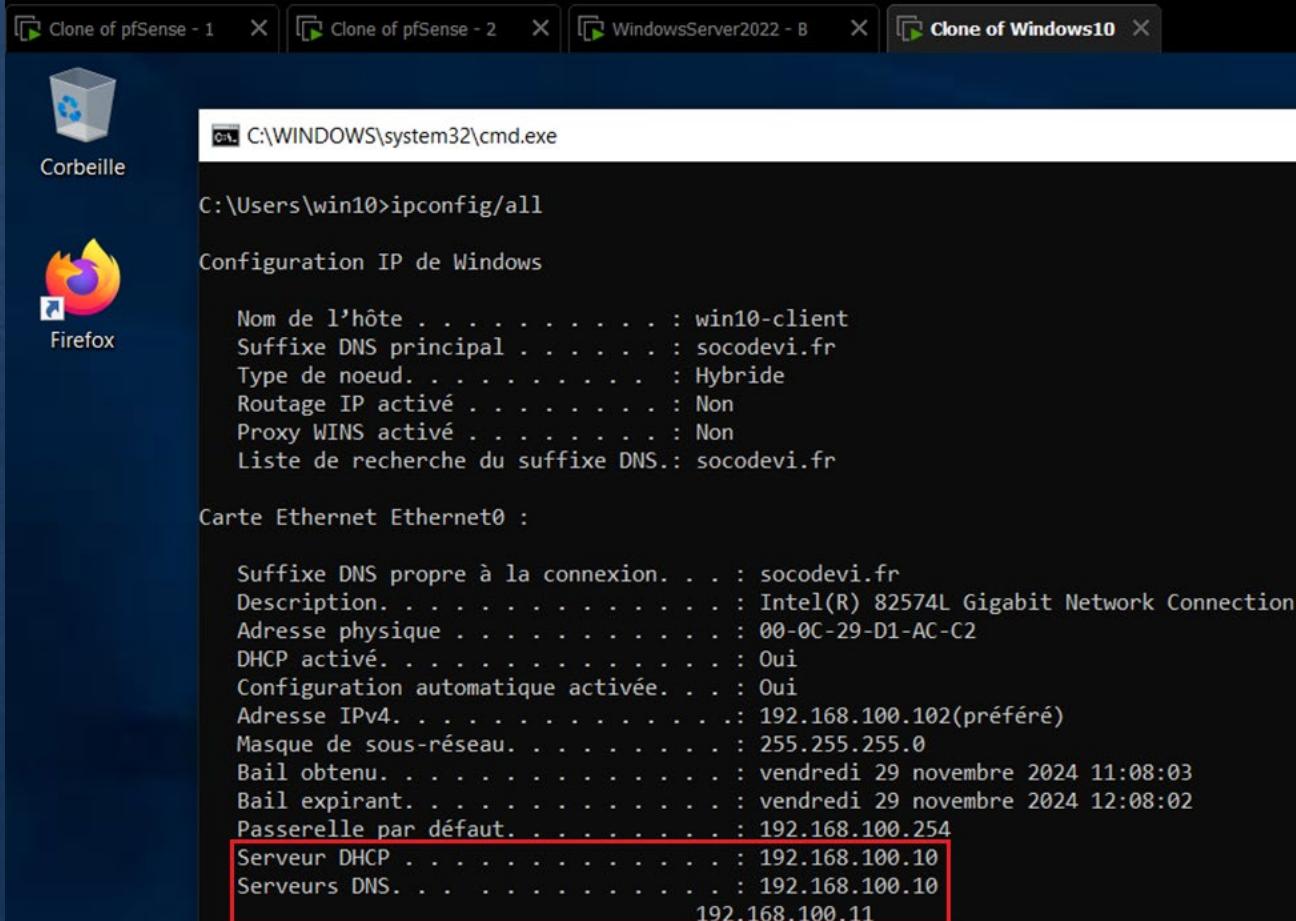
Intervalle de basculement d'état : 60 minutes

Activer l'authentification du message

Secret partagé : *****

< Précédent Suivant > Annuler

Etape 6 – Mise en place – Tests



Ma machine cliente sur la LAN ainsi que les deux pfSense VPN client actifs et le serveur redondant actifs aussi.

Etape 6 – Mise en place – Tests

La config IP de l'AD principal

```
C:\Users\Administrateur>hostname  
WIN-SERV-2022  
  
C:\Users\Administrateur>ipconfig  
  
Configuration IP de Windows  
  
Carte Ethernet Ethernet0 :  
  
    Suffixe DNS propre à la connexion. . . . .  
    Adresse IPv4. . . . . : 192.168.100.10  
    Masque de sous-réseau. . . . . : 255.255.255.0  
    Passerelle par défaut. . . . . : 192.168.100.254
```

La config IP de l'AD secondaire

```
C:\Users\Administrateur.SOCODEVI>hostname  
win-serv-2022-B  
  
C:\Users\Administrateur.SOCODEVI>ipconfig  
  
Configuration IP de Windows  
  
Carte Ethernet Ethernet0 :  
  
    Suffixe DNS propre à la connexion. . . . .  
    Adresse IPv4. . . . . : 192.168.100.11  
    Masque de sous-réseau. . . . . : 255.255.255.0  
    Passerelle par défaut. . . . . : 192.168.100.254
```

Etape 6 – Mise en place – Tests

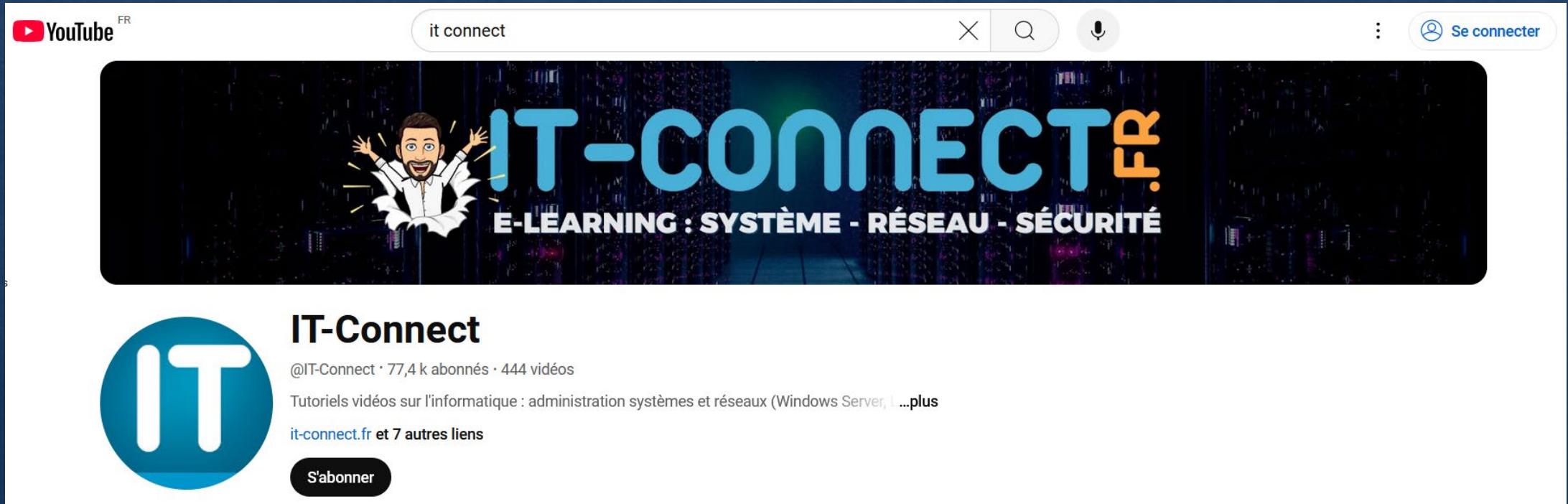
Pour tester les deux redondances je vais éteindre le serveur distant et le pfSense master

Suffixe DNS propre à la connexion	: socodevi.fr
Description	: Intel(R) 82574L Gigabit Network Connection
Adresse physique	: 00-0C-29-D1-AC-C2
DHCP activé	: Oui
Configuration automatique activée	: Oui
Adresse IPv4	: 192.168.100.102(préféré)
Masque de sous-réseau	: 255.255.255.0
Bail obtenu	: vendredi 29 novembre 2024 11:30:31
Bail expirant	: vendredi 29 novembre 2024 13:35:38
Passerelle par défaut	: 192.168.100.254
Serveur DHCP	: 192.168.100.11
Serveurs DNS	: 192.168.100.10 192.168.100.11

Etape 6 – Mise en place – Tests

J'accède toujours à internet , le NAS est accessible mais uniquement depuis l'AD secondaire.

Les clients le ping mais n'y ont pas accès. Je n'ai pas eu le temps de me pencher sur le sujet donc pas de solution trouvée.



Etape 6 – Erreurs rencontrés

Au moment de l'arrêt du DC principal, le second ne prend pas le relais.

Etape 6 – Solutions trouvée

En affichant la liste des serveurs enregistrés, j'ai remarqué qu'il avait garder la première configuration de l'AD secondaire que j'ai modifier par la suite.

```
PS C:\Users\Administrateur> Get-DhcpServerInDC

IPAddress          DnsName
-----            -----
192.168.100.9      win-n5m7pbih08.socodevi.fr
192.168.100.10     win-serv-2022.socodevi.fr

PS C:\Users\Administrateur> Remove-DhcpServerInDC -DnsName "win-n5m7pbih08.socodevi.fr" -IPAddress "192.168.100.9"
AVERTISSEMENT : L'autorisation du serveur DHCP win-n5m7pbih08.socodevi.fr avec l'adresse IP 192.168.100.9, a été
correctement annulée dans Active Directory. L'initialisation de la vérification d'autorisation a échoué sur le serveur
DHCP. Erreur : Le serveur RPC n'est pas disponible. (1722).
PS C:\Users\Administrateur> Get-DhcpServerInDC

IPAddress          DnsName
-----            -----
192.168.100.10     win-serv-2022.socodevi.fr

PS C:\Users\Administrateur> Add-DhcpServerInDC -DnsName "win-serv-2022-b.socodevi.fr" -IPAddress "192.168.100.11"
PS C:\Users\Administrateur> Get-DhcpServerInDC

IPAddress          DnsName
-----            -----
192.168.100.11      win-serv-2022-b.socodevi.fr
192.168.100.10     win-serv-2022.socodevi.fr
```

Etape 6 – Solutions trouvée

Commande :
Repadmin /replsummary

DSA source	différence max	nb échecs	%	erreur
WIN-SERV-2022	38m:58s	0 / 5	0	
WIN-SERV-2022-B	30m:55s	0 / 5	0	
DSA de destination	différence max	nb échecs	%	erreur
WIN-SERV-2022	30m:56s	0 / 5	0	
WIN-SERV-2022-B	38m:59s	0 / 5	0	

Références

Etape 1 : redondance pfSense

<https://www.it-connect.fr/fail-over-pfsense-via-carp-et-pfsync/>

<https://duckduckgo.com/?q=pfsync+tuto&iax=videos&ia=videos&iai=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3D5wQgDNSXLLs>

<https://www.provya.net/?d=2016/10/02/07/48/16-pfsense-configurer-un-cluster-de-2-pfsense-redondants-failover>

Etape 2 : Stockage NAS

<https://www.youtube.com/watch?v=PwoS4owNsPY>

Etape 3 : GPO

Etape 4 : GLPI

<https://www.youtube.com/watch?v=VPoD7dkwpMU>

https://www.youtube.com/watch?v=8ZGSSdonl_Q

<https://www.it-connect.fr/tuto-installer-configurer-gpo-agent-glpi-windows/>

Etape 5 : Clonage

<https://www.youtube.com/watch?v=Z7cNZGgu66E>

Etape 6 : VPN & Redondance

Le cours + Etape 1