

# Rapport TSSR : Projet Lab VMware

Jean-Paul MELISSE

## 1 Introduction

Ce projet s'inscrit dans une démarche d'apprentissage autonome dans le domaine de l'administration des systèmes et des réseaux, suite à une formation TSSR (Technicien Systèmes et Réseaux) partiellement suivie. L'objectif est de concevoir et déployer un laboratoire réseau complet en environnement virtualisé à l'aide de VMware Workstation.

La PME fictive TechNova Solutions, spécialisée dans les services numériques, souhaite moderniser son infrastructure informatique. Ce projet simule la création d'un environnement réseau sécurisé, structuré et adapté aux besoins typiques d'une petite entreprise : gestion centralisée des utilisateurs, partage de ressources, sécurité réseau, et hébergement de services accessibles depuis l'extérieur.

Ce projet permet de mettre en pratique plusieurs compétences clés du métier de technicien systèmes et réseaux : installation de services réseau, sécurisation via un pare-feu (pfSense), configuration d'un domaine Active Directory, mise en place de GPO, et tests de connectivité.

## 2 Cahier des charges

### 2.1 Objectifs techniques

L'infrastructure mise en place devra permettre à l'entreprise de :

- Centraliser la gestion des comptes utilisateurs via un serveur Active Directory (AD).
- Partager des fichiers entre services grâce à un serveur de fichiers avec contrôle d'accès.
- Sécuriser l'infrastructure réseau grâce à un pare-feu (pfSense) avec une séparation logique des zones LAN / DMZ / WAN.
- Héberger un site web consultable depuis l'extérieur dans une zone isolée (DMZ).
- Tester les règles de sécurité réseau (isolation, filtrage, journalisation).

### 2.2 Contraintes

- L'ensemble du projet doit être réalisé en environnement virtualisé, avec VMware Workstation.
- L'infrastructure sera entièrement locale, sans perturber le réseau domestique existant.
- Les IP seront définies en adresses privées selon une topologie personnalisée.
- Aucun accès physique à du matériel réel (switchs, câblage) n'est requis.

## 2.3 Résultats attendus

- Fonctionnement opérationnel de tous les services déployés (AD, DNS, DHCP, partage de fichiers, serveur web).
- Tests concluants sur la connectivité réseau, la sécurité (firewall) et les GPO.
- Rapport complet structurant toutes les étapes du projet et justifiant les choix techniques.

## 3 Conception de l'infrastructure

### 3.1 Architecture réseau logique

L'infrastructure est segmentée en trois zones réseau distinctes simulant des VLANs virtuels via VMware Workstation :

- LAN (Réseau local) : regroupe les serveurs internes (AD, fichiers) et les postes clients.
- DMZ (Zone démilitarisée) : contient le serveur web accessible depuis l'extérieur.
- WAN (réseau externe simulé) : représente Internet et les machines externes.

Chaque zone est isolée sur une interface dédiée du pare-feu pfSense, qui gère le routage interzones et applique les règles de sécurité.

Zone	Nom du réseau VMware	Adresse IP	Rôle
WAN	VMnet1	192.168.10.0/24	Accès externe (Internet simulé)
LAN	VMnet2	192.168.100.0/24	Réseau interne sécurisé
DMZ	VMnet3	192.168.200.0/24	Zone semi-ouverte (serveur web)

Table 1: Architecture réseau logique simulée sous VMware

### 3.2 Plan d'adressage IP

Machine	Système d'exploitation	Adresse IP	Réseau
pfSense (WAN)	pfSense	192.168.10.1	VMnet1
pfSense (LAN)	pfSense	192.168.100.1	VMnet2
pfSense (DMZ)	pfSense	192.168.200.1	VMnet3
Serveur AD/DNS/DHCP	Windows Server 2022	192.168.100.10	LAN
Serveur de fichiers	Windows Server 2022	192.168.100.11	LAN
Client Admin	Windows 10 Pro	192.168.100.100 (DHCP)	LAN
Client Direction	Windows 10 Pro	192.168.100.101 (DHCP)	LAN
Serveur Web	Debian 12 / Ubuntu	192.168.200.10	DMZ
Machine Externe (test)	Windows / Linux	192.168.10.50	WAN

Table 2: Plan d'adressage IP

### 3.3 Schéma réseau et Simulation avec Cisco Packet Tracer

Dans le cadre du projet, une version simulée de l'architecture réseau a été réalisée avec Cisco Packet Tracer. Bien que Packet Tracer ne permette pas de simuler directement des appliances comme pfSense

ou VMware, une modélisation équivalente a été construite pour visualiser les flux réseau, tester les règles de routage et configurer des éléments de base (ex : routeurs, VLAN, serveurs).

La Figure 1 illustre la topologie de l'infrastructure à travers un schéma réseau réalisé dans Cisco Packet Tracer.

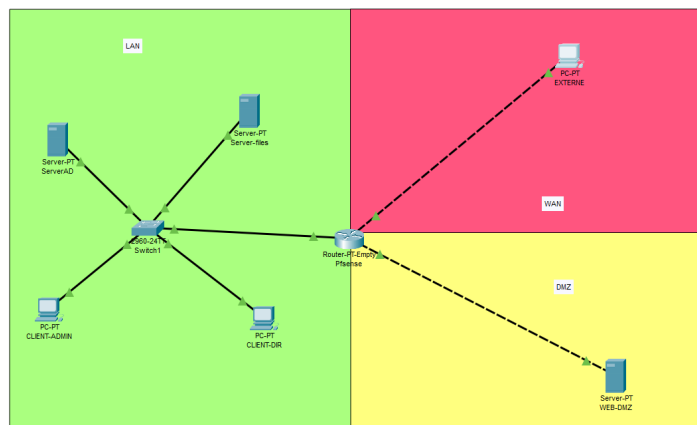


Figure 1: Schéma de l'infrastructure sur Cisco Packet Tracer

**Fichier de simulation :** Le fichier `cisco_lab_tssr.pkt` est disponible dans le dépôt GitHub du projet sous `/configs/`.

**Configuration du routeur simulant pfSense** Sur le "pfSense" simulé avec un routeur Cisco, on configure :

- Les trois interfaces correspondant aux zones LAN, DMZ et WAN.
- Le protocole RIP (ou du routage statique) pour l'interconnexion des zones.
- Des règles ACL pour sécuriser l'accès réseau.

La configuration se fait depuis le terminal CLI :

- "enable" pour passer en mode privilégié
- "configure terminal" pour entrer en mode de configuration

**Mise en place des règles ACL :**

- Pour commencer, on veut que seul le serveur web est accessible depuis l'extérieur ( uniquement l'accès HTTP - port 80). Donc on tape la ligne :

```
access-list 100 permit tcp any host 192.168.200.10 eq 80
```

- Puis, on refuse tout autre accès aux autres services du serveur depuis l'extérieur. On tape la commande :

```
access-list 100 deny ip any 192.168.200.0 0.0.0.255
```

- On fait de même avec le LAN. On coupe tout accès depuis l'extérieur. On tape :

```
access-list 100 deny ip any 192.168.100.0 0.0.0.255
```

- Enfin, on autorise les connexions sortantes. On tape :

```
access-list 100 permit ip any any
```

On va aussi ajouter une redirection vers le serveur web depuis le routeur côté extérieur (WAN) sur le port 80 (accès http). On tape la commande : "ip nat inside source static tcp 192.168.200.10 80 192.168.10.1 80". Pour que cette ligne fonctionne, il faut déclarer les accès inside et outside de la table nat. On modifie l'interface côté DMZ "ici en tapant interface g7/0" et on tape la commande "ip nat inside" pour l'indiquer à la table nat. On tape "exit" pour sortir de l'interface DMZ. On fait de même du côté WAN "ici en tapant interface g9/0" et on tape la commande "ip nat outside" pour l'indiquer à la table nat. Enfin, l'ACL (qui sont des règles ACL étendues) est appliquée sur l'interface WAN en entrée. On tape donc la ligne : "ip access-group 100 in". On peut voir les étapes précédentes sur la Figure 2.

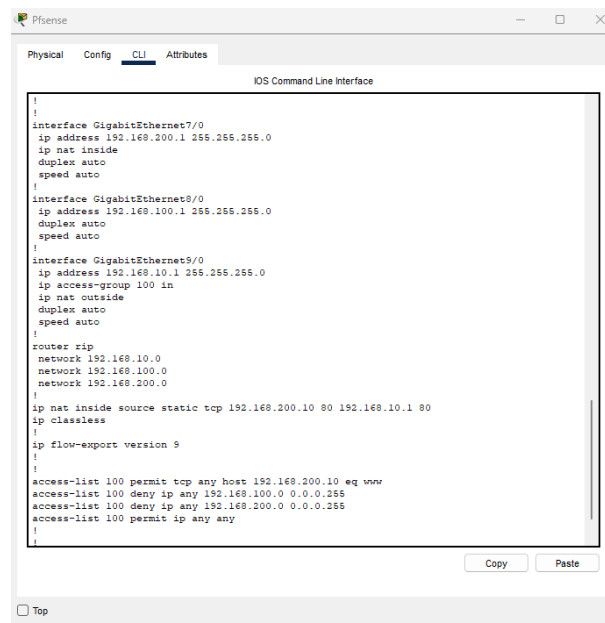


Figure 2: Configuration de PfSense dans Packet Tracer

**Configuration des services internes** On va aussi configurer les autres machines et surtout le serveur Active Directory. Ce dernier est configuré pour jouer également le rôle de serveur DHCP pour les clients du LAN (Voir la Figure 3).

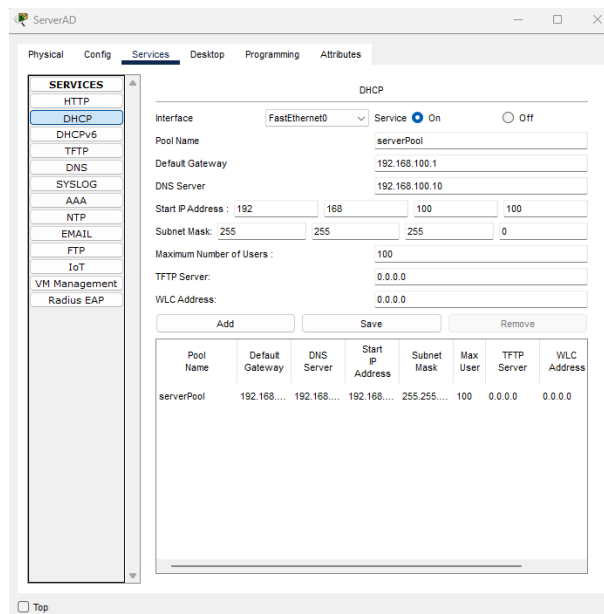


Figure 3: Configuration du service DHCP dans Packet Tracer

## Tests de connectivité entre zones

Sur la machine externe, on essaie de se connecter au DMZ et au LAN avec la commande `ping`. On voit sur la Figure 4 qu'on n'y arrive pas.

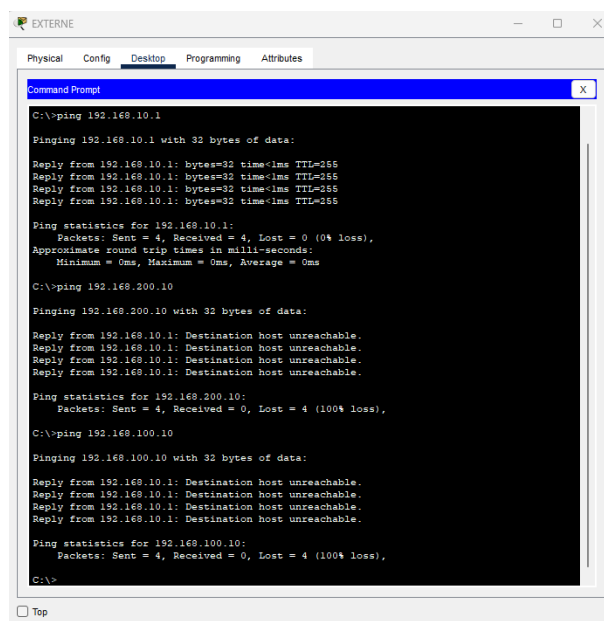


Figure 4: Blocage des pings vers les zones internes

Par contre, sur la machine externe, on voit qu'on arrive à accéder à la page web du serveur sur la DMZ grâce à la redirection (Voir la Figure 5).

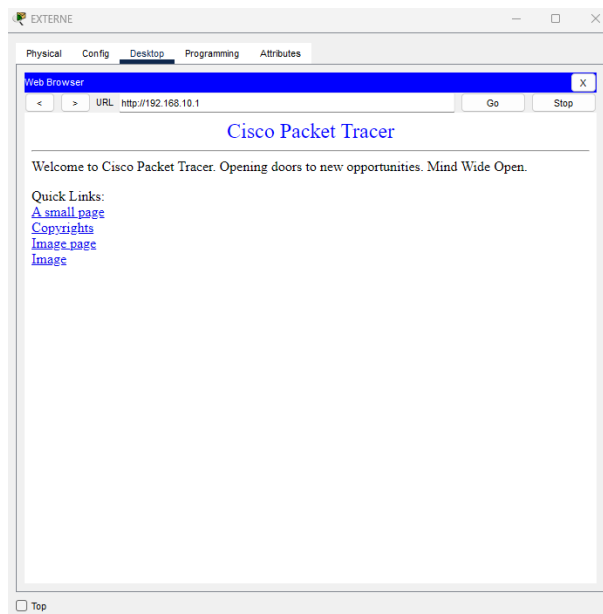


Figure 5: Accès au site Web de la DMZ depuis l'extérieur

Concernant la connexion entre les machines LAN et le serveur en DMZ, on peut voir sur les Figures 6 et 7 que la communication entre les machines se passe sans problème.

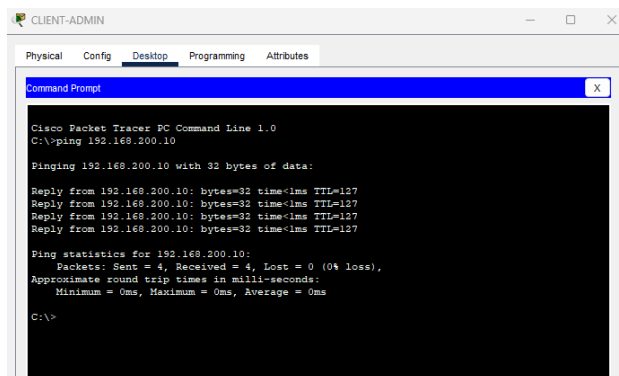


Figure 6: Connexion entre le LAN et le DMZ - coté LAN

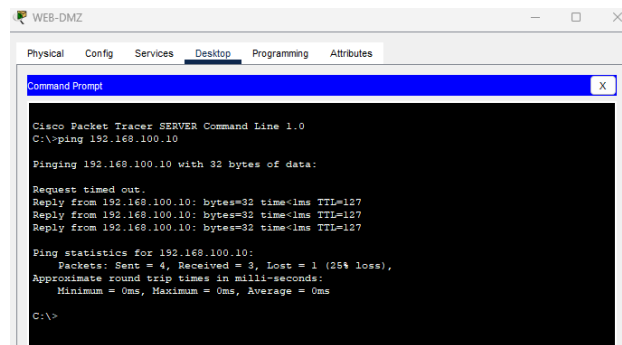


Figure 7: Connexion entre le LAN et le DMZ - coté DMZ

### 3.3.1 Renforcement de la sécurité sur l'interface WAN

Afin de limiter les informations divulguées à l'extérieur, certaines options ont été désactivées sur l'interface WAN du routeur simulant pfSense. Cela permet de réduire la surface d'attaque et de ne pas répondre inutilement à des requêtes réseau potentiellement malveillantes.

Voici les commandes appliquées sur l'interface WAN (g9/0) :

- no ip icmp unreachable ! Ne répond pas aux paquets bloqués (ACL) [non supporté dans Packet Tracer]
- no ip redirects ! Empêche l'envoi de redirections ICMP [non supporté dans Packet Tracer]
- no ip proxy-arp ! Empêche le proxy ARP (évite certaines attaques réseau)

Ces paramètres rendent le comportement du pare-feu plus silencieux :

- Un paquet bloqué par une règle ACL n'est pas suivi d'un message "ICMP unreachable".
- Le routeur n'envoie pas de redirections de route qui pourraient être exploitées.
- Il ne répond pas à des requêtes ARP pour d'autres machines, ce qui réduit les risques d'empoisonnement ARP.

Dans Cisco Packet Tracer, seule la commande "no ip proxy-arp" est fonctionnelle. Les deux autres commandes sont des bonnes pratiques de sécurité qu'on retrouve dans des environnements Cisco réels, mais qui ne sont pas implémentées dans ce simulateur.

## 4 Mise en œuvre

### 4.1 Configuration réseau dans VMware Workstation

Dans ce projet, le réseau virtuel est segmenté de manière isolée en utilisant les fonctionnalités NAT et LAN Segment proposées directement par VMware Workstation, afin de simuler les zones WAN, LAN et DMZ de manière simple et sécurisée.

#### Segmentation retenue :

Zone	Type de réseau	Nom	Usage
WAN	Réseau NAT (VMnet)	VMnet NAT	Simule l'accès Internet (machine externe)
LAN	LAN Segment	LAN_SEG	Réseau interne sécurisé (AD, clients)
DMZ	LAN Segment	DMZ_SEG	Zone démilitarisée (serveur web)

Table 3: Segmentation réseau dans VMware Workstation

#### Attribution des interfaces aux VMs :

Machine	Interface WAN	Interface LAN	Interface DMZ
pfSense	VMnet NAT	LAN_SEG	DMZ_SEG
Serveur AD/DHCP	—	LAN_SEG	—
Serveur de fichiers	—	LAN_SEG	—
Clients Windows 10	—	LAN_SEG	—
Serveur Web	—	—	DMZ_SEG
Machine externe	VMnet NAT	—	—

Table 4: Attribution des interfaces aux VMs

Ce choix permet :

- Une séparation logique simple à mettre en œuvre,
- Une simulation réaliste des flux entre zones,
- Une configuration plus rapide sans passer par l'éditeur VMnet.

Un LAN Segment dans VMware Workstation est un type de réseau virtuel isolé, permettant à plusieurs machines virtuelles de communiquer uniquement entre elles, sans aucun accès à l'extérieur (ni à l'hôte, ni à Internet). C'est un excellent moyen de simuler un réseau privé, comme un LAN interne ou une DMZ, sans interférence ni besoin de configuration réseau avancée.

## **4.2 Création de la machine virtuelle pfSense**

Pour commencer, une machine virtuelle pfSense est créée sous VMware Workstation, en suivant les étapes suivantes :

1. Cliquer sur "Create a New Virtual Machine", puis choisir "Custom (advanced)", et cliquer deux fois sur "Next".
2. Sélectionner "I will install the operating system later", puis cliquer sur "Next".
3. Dans "Guest Operating System", cocher "Other" et choisir "FreeBSD 12 64-bit", puis cliquer sur "Next".
4. Donner le nom "pfSense" à la VM et choisir le dossier de destination, puis cliquer sur "Next".
5. Attribuer 1 cœur (1 processor, 1 core), 512 Mo de RAM, puis cliquer sur "Next".
6. Pour la première carte réseau, choisir le type "NAT" (ce sera l'interface WAN), puis cliquer trois fois sur "Next".
7. Choisir "Create a new virtual disk", cliquer sur "Next".
8. Définir une taille de 10 Go, cocher "Store virtual disk as a single file", puis cliquer deux fois sur "Next", et enfin "Finish".

### **4.2.1 Ajout des interfaces réseau supplémentaires**

Avant d'allumer la VM, il faut ajouter deux interfaces réseau supplémentaires :

1. Cliquer sur "Edit virtual machine settings".
2. Dans "CD/DVD (SATA)", cocher "Use ISO image file" et sélectionner l'image ISO de Pfsense.
3. Cliquer sur "Add...", puis choisir "Network Adapter", et cliquer sur "Finish".
4. Répéter l'opération une seconde fois pour avoir au total trois cartes réseau.
5. Configurer les interfaces :
  - La première carte reste en NAT (WAN)
  - La deuxième est affectée au LAN Segment nommé LAN\_SEG
  - La troisième est affectée au LAN Segment nommé DMZ\_SEG



On peut voir un résumé de la configuration de Pfsense sur la Figure 8.

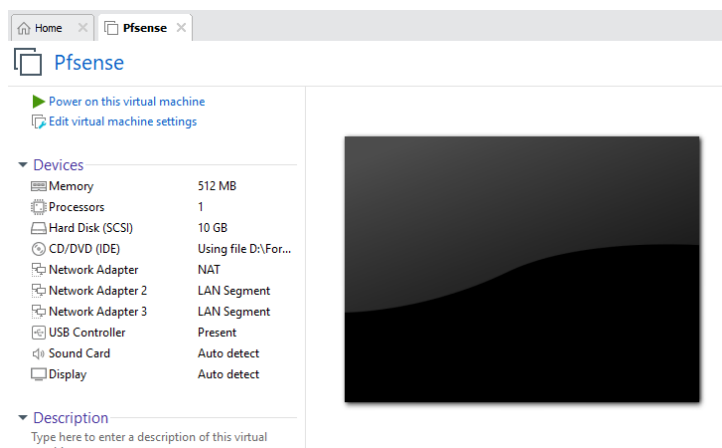


Figure 8: Résumé de la configuration de la machine Pfsense

Remarque : si nécessaire, on peut adapter la configuration du réseau NAT dans Virtual Network Editor, notamment pour définir une plage cohérente avec le sous-réseau WAN prévu (ex : 192.168.10.0/24).

#### 4.2.2 Installation de Pfsense

Après avoir démarré la VM, on clique sur "Accept", puis sur "Install". Pour le clavier, on choisit "French" et on valide en tapant sur "Entrée", puis on choisit "Continue with fr.kbd keymap" et on valide en tapant sur "Entrée". On choisit "Auto (ZFS)" et on appuie sur "Entrée", puis la même chose pour "Install" et "stripe". On appuie sur la barre d'espace pour sélectionner le disque dur et on appuie sur "Entrée" pour continuer. On choisit "Yes" pour effacer le disque dur et installer pfsense. Quand l'installation est finie, on choisit "No" pour ne pas ouvrir un shell et on appuie sur "Entrée". Enfin, on choisit "Reboot" et on appuie sur "Entrée" pour redémarrer la VM.

#### 4.2.3 Configuration des interfaces (WAN/LAN/DMZ)

Après le redémarrage de la VM pfSense, on configure manuellement les adresses IP pour chaque interface à partir de la console.

1. Appuyer sur la touche 2 pour accéder au menu de configuration des interfaces.
2. Une liste des interfaces disponibles apparaît (généralement em0, em1, em2). Leur ordre peut varier, donc il est recommandé d'identifier les interfaces à l'aide de leur adresse MAC si nécessaire.

#### Configuration de l'interface LAN :

- Sélectionner l'interface correspondant au LAN.
- Répondre n pour désactiver le DHCP.
- Saisir l'adresse IP statique suivante : 192.168.100.1/24
- Laisser vide l'adresse IPv6 (appuyer sur Entrée).
- Répondre n pour ne pas activer le serveur DHCP sur cette interface.

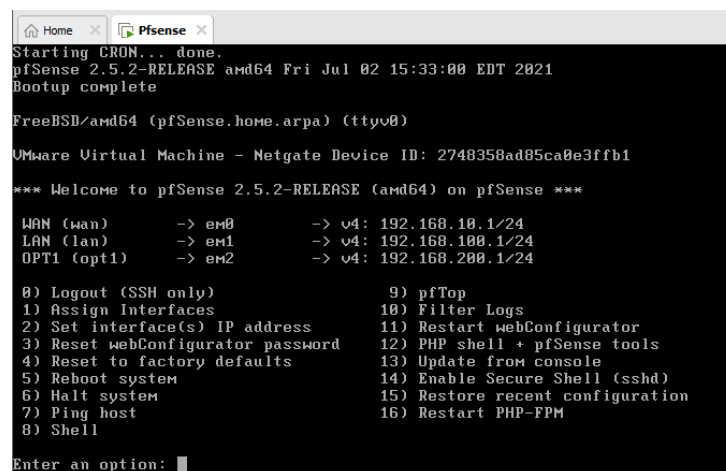
### Configuration de l'interface WAN :

- Sélectionner l'interface correspondant au WAN.
- Répondre n pour désactiver le DHCP (si activé par défaut).
- Saisir l'adresse IP statique suivante : 192.168.10.1/24
- Mettre l'adresse IP de la passerelle : 192.168.10.254
- Laisser vide l'adresse IPv6.
- Ne pas activer de service DHCP sur cette interface.

### Configuration de l'interface DMZ :

- Sélectionner l'interface correspondant à la DMZ.
- Répondre n pour désactiver le DHCP.
- Saisir l'adresse IP statique suivante : 192.168.200.1/24
- Laisser vide l'adresse IPv6.
- Répondre n pour le DHCP.

On peut voir les résultats des étapes précédentes sur la Figure 9.



```
Starting CRON... done.
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 2748358ad85ca0e3ffb1

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.10.1/24
LAN (lan)      -> em1      -> v4: 192.168.100.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.200.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator 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

Enter an option: █
```

Figure 9: Adresses IPs des interfaces sur Pfsense

### Remarques :

- Nom des interfaces dans pfSense : Par défaut, pfSense nomme les interfaces supplémentaires sous forme OPT1, OPT2, etc. Dans ce projet, l'interface correspondant à la DMZ apparaît initialement sous le nom OPT1. Ce nom peut être modifié via l'interface web de pfSense pour une meilleure lisibilité (ex : renommer OPT1 en DMZ).
- Passerelle sur l'interface WAN : Lors de la configuration de l'interface WAN, il est important de spécifier une passerelle par défaut pour permettre à pfSense d'accéder à Internet via NAT. Dans le cas de ce projet, la passerelle NAT a été manuellement définie sur 192.168.10.254 dans le Virtual Network Editor de VMware. Exemple de configuration WAN :

- Adresse IP : 192.168.10.1/24
- Passerelle : 192.168.10.254

À ce stade, pfSense est prêt à être administré via son interface Web (WebGUI), accessible à l'adresse <http://192.168.100.1> depuis une machine du LAN. L'étape suivante consiste donc à créer et installer un serveur dans ce réseau local, afin d'accéder à cette interface et poursuivre la configuration (pare-feu, NAT, DHCP, etc.).

### **4.3 Serveur Active Directory : Windows Server 2022**

Nous retournons sur VMware Workstation pour créer la machine virtuelle qui jouera le rôle de contrôleur de domaine (AD). Voici les étapes à suivre :

1. Cliquer sur "Create a New Virtual Machine", puis choisir "Custom (advanced)", et cliquer deux fois sur "Next".
2. Sélectionner "I will install the operating system later", puis cliquer sur "Next".
3. Dans "Guest Operating System", cocher "Microsoft Windows" et choisir "Windows Server 2022", puis cliquer sur "Next".
4. Donner le nom "ServeurAD" à la VM et choisir le dossier de destination, puis cliquer sur "Next".
5. Attribuer 2 processeurs (1 cœur chacun) et 2 Go de RAM, puis cliquer sur "Next".
6. Pour la carte réseau, sélectionner "Host-only" (nous la changerons en LAN Segment juste après), puis cliquer trois fois sur "Next".
7. Choisir "Create a new virtual disk", cliquer sur "Next".
8. Définir une taille de 60 Go, cocher "Store virtual disk as a single file", puis cliquer deux fois sur "Next", et enfin "Finish".

Avant d'allumer la VM, on va changer son interface réseau :

1. Cliquer sur "Edit virtual machine settings".
2. Dans "CD/DVD (SATA)", cocher "Use ISO image file" et sélectionner l'image ISO de Windows Server 2022.
3. Dans "Network Adapter", changer la connexion en "LAN Segment", et sélectionner le segment correspondant au LAN.

On peut voir un résumé de la configuration du Serveur AD sur la Figure 10.

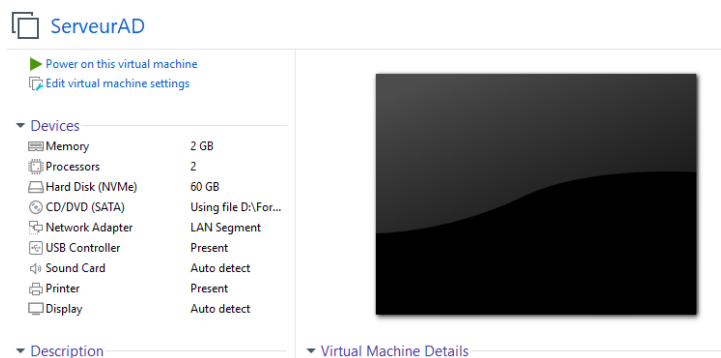


Figure 10: Résumé de la configuration de la machine Serveur AD

#### 4.3.1 Installation du Serveur Windows 2022 - Contrôleur de domaine

Après avoir démarré la VM ServeurAD, appuyer sur n'importe quelle touche pour démarrer sur l'image ISO du CD. Dans les premières options d'installation, sélectionner :

- Langue à installer : Français (France)
- Format horaire et monétaire : Français (France)
- Clavier ou méthode d'entrée : Français

Cliquer ensuite sur Suivant, puis sur Installer maintenant. Dans la liste des éditions, choisir : Windows Server 2022 Standard Evaluation (Expérience de bureau), puis cliquer sur Suivant. Cocher la case "J'accepte les termes du contrat de licence logiciel Microsoft", puis cliquer sur Suivant. Choisir l'option "Personnalisé : Installer uniquement le système d'exploitation Microsoft Server". Dans la liste des disques, sélectionner "Lecteur 0 – Espace non alloué" comme destination de l'installation, puis cliquer sur Suivant pour lancer l'installation.

Une fois l'installation terminée et le système redémarré, une fenêtre vous invite à définir un mot de passe pour le compte Administrateur. Saisir le mot de passe suivant deux fois : Azerty123!, puis cliquer sur Terminer (cf: Figure 11).

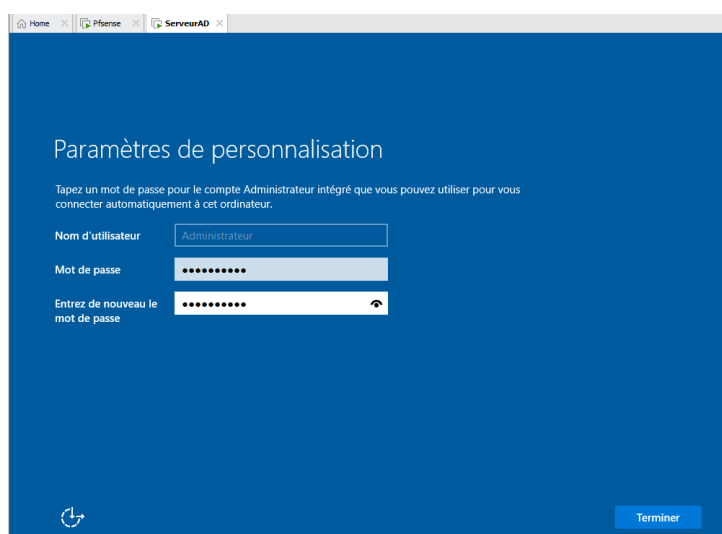


Figure 11: Installation du Serveur AD

### 4.3.2 Configuration classique de Windows Server – Préparation à l'accès web de pfSense

Après le redémarrage, appuyer sur "Ctrl+Alt+Suppr" et saisir le mot de passe pour se connecter en tant qu'Administrateur. La première étape consiste à changer le nom du serveur et à attribuer une adresse IP statique, afin de permettre l'accès à l'interface web de pfSense.

**Remarques :** Avant de continuer, il est recommandé d'installer VMware Tools pour améliorer les performances et la fluidité de la machine virtuelle.

#### Renommer le serveur

1. Ouvrir la fenêtre "Exécuter" en recherchant run dans le menu démarrer.
2. Taper sysdm.cpl puis appuyer sur Entrée.
3. Dans l'onglet Nom de l'ordinateur, cliquer sur Modifier...
4. Entrer le nom : ServeurAD, puis cliquer sur OK deux fois pour valider.
5. Redémarrage requis (à faire après les étapes suivantes).

#### Configuration de l'adresse IP statique

1. Réouvrir Exécuter (run) et taper ncpa.cpl, puis Entrée pour ouvrir les connexions réseau.
2. Clic droit sur Ethernet0, puis Propriétés.
3. Dans la liste, décochez IPv6 pour le désactiver.
4. Double-cliquer sur Protocole Internet version 4 (TCP/IPv4).
5. Cocher "Utiliser l'adresse IP suivante" et remplir :
  - Adresse IP : 192.168.100.10
  - Masque : 255.255.255.0
  - Passerelle par défaut : 192.168.100.1
6. Cocher "Utiliser l'adresse de serveur DNS suivante" :
  - DNS préféré : 192.168.100.10 (c'est l'adresse IP du serveur lui-même, car il jouera le rôle de serveur DNS une fois les rôles installés)
7. Cocher "Valider les paramètres en quittant", puis cliquer sur OK deux fois.

Les étapes ci-dessus sont illustrées dans les Figures 12 et 13.

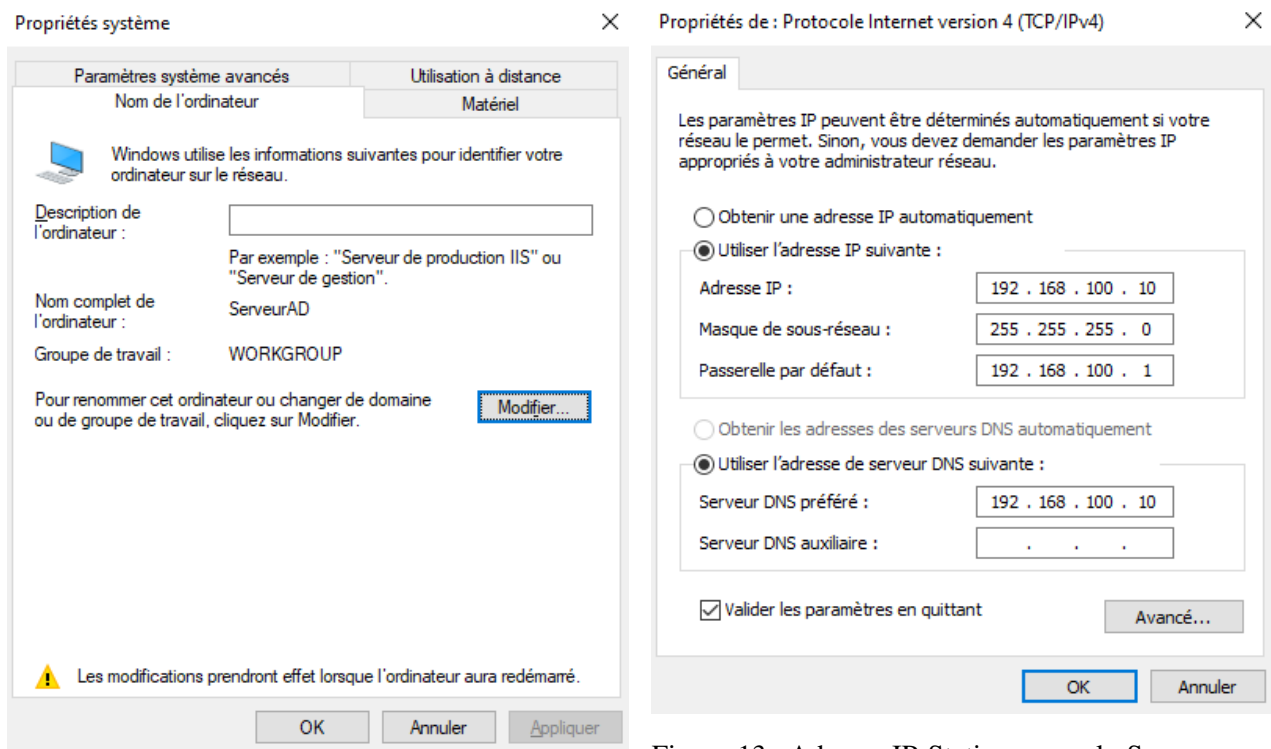


Figure 12: Renommer le serveur AD

Figure 13: Adresse IP Statique pour le Serveur AD

**Vérification :** Ouvrir l'invite de commandes (cmd) et taper ipconfig pour vérifier la nouvelle configuration réseau. Comme le montre la Figure 14, l'adresse IP est bien définie en statique. Enfin, redémarrer le serveur pour appliquer le nouveau nom d'hôte.

```

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. . . . . : 192.168.100.1
  
```

Figure 14: Vérification de l'IP du Serveur AD avec ipconfig

Une fois le serveur configuré avec une IP statique, il est désormais possible d'accéder à l'interface web de pfSense depuis un navigateur à l'adresse suivante : <http://192.168.100.1>

### 4.3.3 Configuration graphique de pfSense

Après avoir redémarré le serveur, on ouvre le navigateur Edge et on tape l'adresse suivante dans la barre : <http://192.168.100.1>. On accède alors à l'interface web de pfSense. On se connecte avec les identifiants par défaut : admin pour le nom d'utilisateur et pfsense pour le mot de passe. (Ces identifiants

seront changés plus tard pour renforcer la sécurité de l'infrastructure.) On suit ensuite l'assistant de configuration initiale :

- Cliquer sur Next deux fois.
- Définir un nom de domaine (par exemple homelab.infra) et modifier si besoin le nom d'hôte (ici on conserve pfSense).
- Indiquer les serveurs DNS primaire et secondaire. Ici :
  - DNS primaire : 8.8.8.8 (Google DNS)
  - DNS secondaire : 1.1.1.1 (Cloudflare DNS)

Cela permet à pfSense de résoudre les noms de domaine externes pour lui-même et pour les clients qui s'appuieraient sur lui comme relais DNS.

- Cliquer sur Next.
- Choisir la timezone Europe/Paris, puis Next.
- Dans la configuration de l'interface WAN, s'assurer que les options suivantes sont cochées :
  - Block private networks from entering via WAN
  - Block bogon networks
- Cliquer sur Next.
- Vérifier la configuration de l'interface LAN, puis cliquer sur Next.
- Définir un nouveau mot de passe pour l'administration WebGUI (ici, par exemple : Admin!123), puis cliquer sur Next, puis sur Reload.

Une fois le rechargement terminé, cliquer sur Finish, puis Accept et enfin Close. Ensuite, pour renommer l'interface OPT1 en DMZ :

- Aller dans le menu Interfaces > OPT1,
- Modifier le nom en DMZ,
- Cliquer sur Save puis Apply Changes.

On peut voir les résultats des étapes précédentes sur la Figure ??.

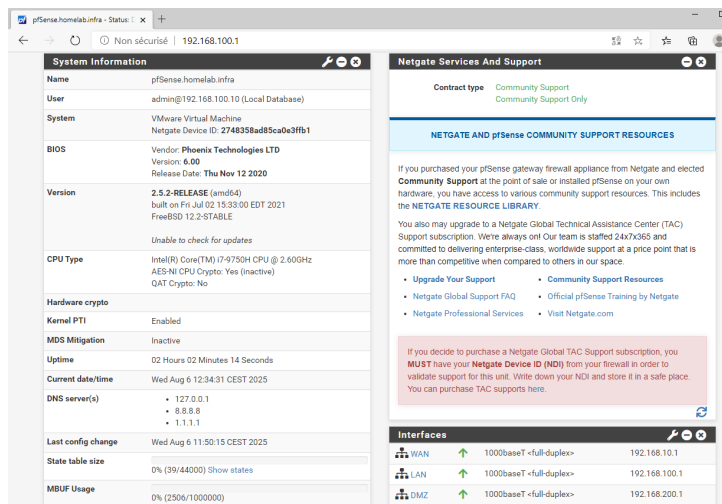


Figure 15: Résumé de la configuration de Pfsense interface graphique

**Remarque concernant le DNS dans le LAB :** Par défaut, les machines du réseau LAN utilisent le serveur ServeurAD comme DNS principal (IP : 192.168.100.10), car celui-ci sera configuré plus tard pour gérer les services DNS et Active Directory.

Cependant, tant que le rôle DNS n'est pas encore installé et configuré sur ServeurAD, celui-ci ne peut pas résoudre les noms de domaine externes. Cela provoque des échecs de navigation Internet depuis les clients qui utilisent ce DNS.

Une solution temporaire consiste à ajouter pfSense (192.168.100.1) comme serveur DNS secondaire sur les machines clientes. Ainsi, si ServeurAD ne parvient pas à résoudre un nom, la requête est transmise à pfSense, qui lui, dispose des DNS publics configurés précédemment (Google, Cloudflare).

Exemple de configuration DNS sur le client :

- DNS préféré : 192.168.100.10 (ServeurAD)
- DNS auxiliaire : 192.168.100.1 (pfSense)

À ce stade, la configuration initiale de pfSense via l'interface graphique est terminée. Nous y reviendrons ultérieurement pour affiner les règles de pare-feu et les paramètres de sécurité, une fois que l'ensemble des serveurs du LAB auront été installés et correctement configurés.

#### 4.3.4 Configuration du serveur – Préparation pour un contrôleur de domaine

On commence par préparer notre serveur afin qu'il puisse recevoir les rôles nécessaires pour les prochaines étapes (AD, DHCP, DNS). Pour cela, on ouvre la fenêtre "Exécuter" (Win + R), on tape "services.msc" puis Entrée. On active et démarre les trois services suivants, liés à la découverte réseau et à Active Directory :

- Découverte SSDP,
- Hôte des périphériques UPnP,



- Publication des ressources de découverte de fonctions (cf. Figure 16).

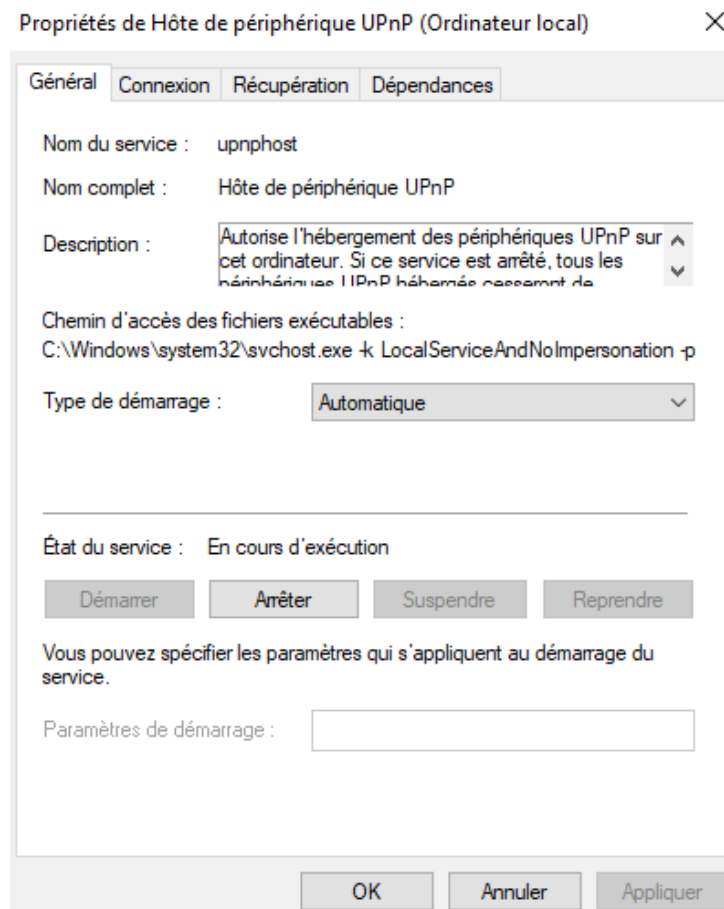


Figure 16: Activation des services nécessaires à ADDS sur le Serveur AD

Ensuite, dans le Gestionnaire de serveur (accessible via la barre de recherche), on clique sur "Ajouter des rôles et des fonctionnalités".

- On clique sur "Suivant",
- On coche "Installation basée sur un rôle ou une fonctionnalité",
- Puis "Sélectionner un serveur du pool" et on choisit notre serveur.

On sélectionne ensuite les rôles suivants :

- Services AD DS,
- Serveur DNS,
- Serveur DHCP.

À chaque ajout, on clique sur "Ajouter des fonctionnalités" quand demandé. Une fois les rôles sélectionnés, on clique sur "Suivant" autant de fois que nécessaire, puis sur "Installer" (cf. Figures 17 et 18).

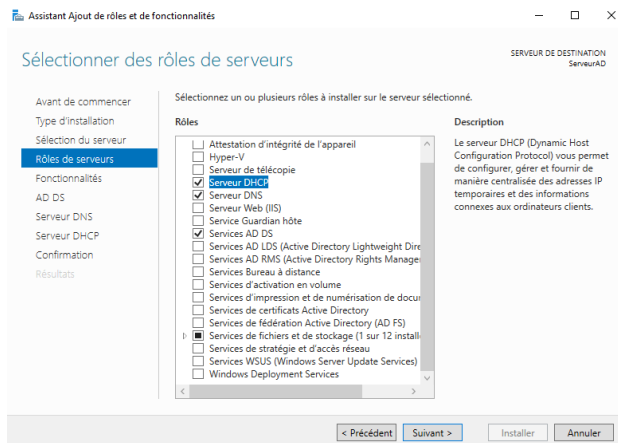


Figure 17: Ajout des rôles sur le Serveur AD

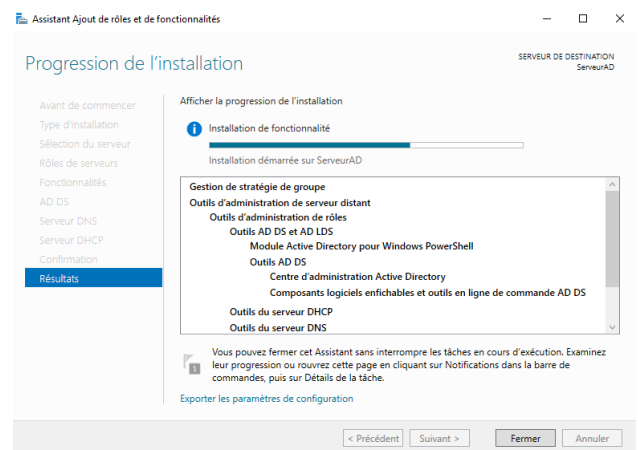


Figure 18: Installation des rôles sur le Serveur AD

Une fois l'installation terminée, on clique sur "Fermer". On passe ensuite à la promotion du serveur en contrôleur de domaine, créant ainsi une nouvelle forêt.

- Dans le Gestionnaire de serveur, on clique sur le drapeau Notifications (en haut),
- Puis sur "Promouvoir ce serveur en contrôleur de domaine".
- On coche "Ajouter une nouvelle forêt" et on saisit le nom du domaine : homelab.infra (cf. Figure 19)).

On clique sur "Suivant", on entre deux fois le mot de passe pour le Mode de restauration (DSRM) (ici : Azerty123!) puis Suivant jusqu'à la fin. On clique enfin sur "Installer". Le serveur redémarre automatiquement à la fin de l'installation.

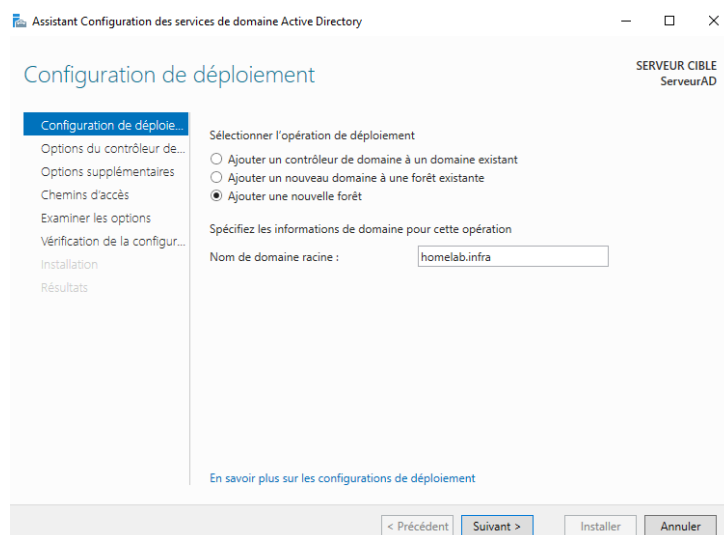


Figure 19: Promotion du Serveur AD en contrôleur de domaine

Après le redémarrage, on se connecte avec le compte Administrateur du domaine HOMELAB.

**Attention :** deux des trois services activés précédemment peuvent s'être désactivés après la promotion. Il faut penser à les réactiver.

**Création de la zone DNS :** On ouvre de nouveau le Gestionnaire de serveur, puis :

- Outils → DNS.
- Dans l'arborescence, on clique-droit sur Zone de recherche inversée → Nouvelle zone.
- On suit l'assistant :
  - Zone principale,
  - IPv4,
  - ID de réseau : 192.168.100,
  - Mises à jour dynamiques sécurisées uniquement,
  - Puis Terminer.

On peut voir la zone créée sur la Figure 20.

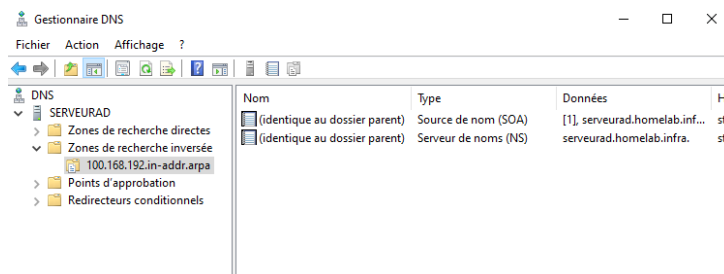


Figure 20: Création de la zone de recherche inversée DNS

Ensuite, on ajoute un pointeur PTR :

- Clic-droit sur la zone inversée → Nouveau pointeur (PTR)....,
- On parcourt pour retrouver ServeurAD dans la zone de recherche directe,
- On coche la case "Autoriser tout utilisateur identifié à mettre à jour...",
- On valide avec OK.

On vérifie ensuite que le DNS fonctionne avec la commande nslookup depuis l'outil graphique DNS (clic-droit sur ServeurAD → Exécuter nslookup). (cf. Figure 21)

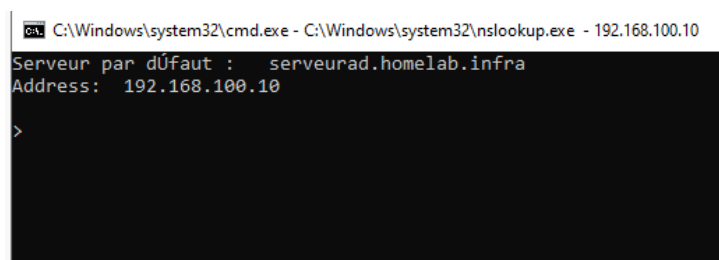


Figure 21: Résolution DNS via nslookup

**Configuration du service DHCP :** La prochaine étape consiste à configurer le service DHCP.

Tout d'abord, dans le Gestionnaire de serveur, on clique sur le drapeau Notifications (en haut), puis sur "Terminer la configuration DHCP". On clique sur "Suivant", puis sur "Valider". Une fois la configuration post-installation réalisée (voir Figure 22), on clique sur "Fermer".

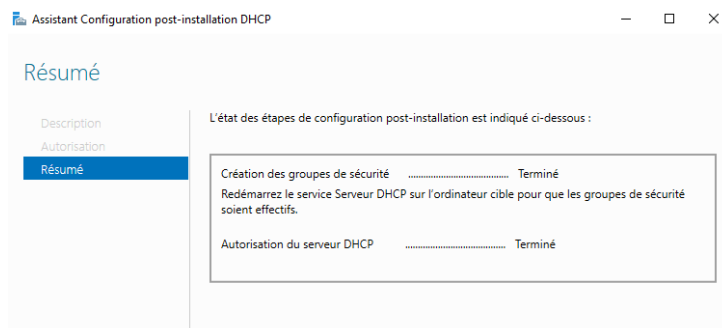


Figure 22: Configuration post-installation du DHCP

Ensuite, il faut créer une nouvelle étendue. Pour cela, on clique sur Outils > DHCP pour ouvrir la console de gestion. Dans le panneau de gauche, on fait un clic droit sur "IPv4" puis sur "Nouvelle étendue...".

Après avoir cliqué sur "Suivant", on donne un nom à l'étendue (ex. : Accès Client LAN) et une description (ex. : Plage réservée aux clients du LAN), puis on clique sur "Suivant". On définit la plage d'adresses IP :

- Adresse de début : 192.168.100.100
- Adresse de fin : 192.168.100.200

On clique ensuite sur "Suivant" à 4 reprises (en gardant les paramètres par défaut sur ces étapes) (voir Figure 23).

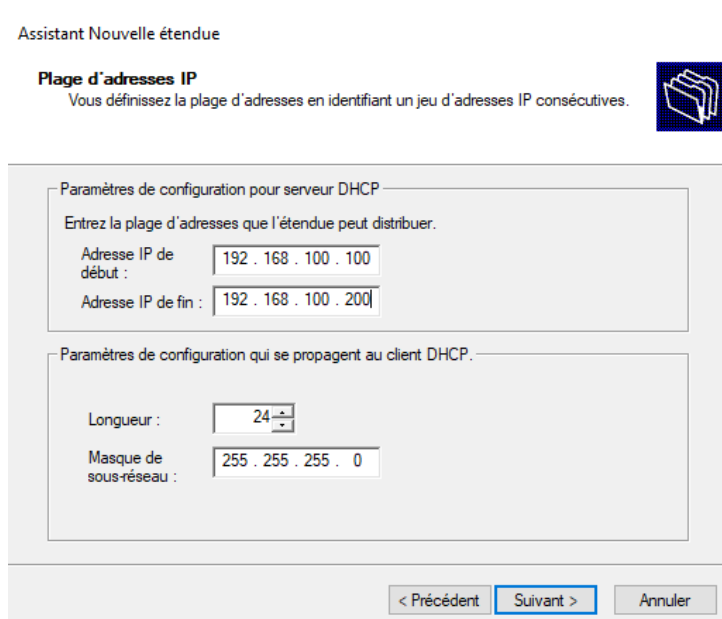


Figure 23: Définition de la plage d'adresses IP sur le serveur AD

À l'étape de configuration de la passerelle, on saisit l'adresse IP du pfSense côté LAN (192.168.100.1) puis on clique sur "Ajouter". On poursuit avec "Suivant" encore 4 fois (en laissant les valeurs par défaut), puis on termine avec "Terminer".

#### 4.3.5 Création des utilisateurs et des groupes

Dans cette étape, nous allons créer les utilisateurs et les répartir dans différentes unités d'organisation (OU) ainsi que dans les groupes correspondants. Deux approches sont possibles pour cette opération :

- **Méthode graphique** : via la console Utilisateurs et ordinateurs Active Directory, accessible depuis le Gestionnaire de serveur > Outils > Utilisateurs et ordinateurs AD.
- **Méthode automatisée** : via un script PowerShell exploitant un fichier CSV et les modules Active Directory.

**Création des unités d'organisation (OU)** Nous avons d'abord créé manuellement l'OU principale TECHNOVA. Pour cela, dans la console Utilisateurs et ordinateurs Active Directory, on clique-droit sur le domaine "homelab.infra", puis on sélectionne Nouveau > Unité d'organisation. On lui donne un nom (ici : TECHNOVA) et on laisse la case Protéger le conteneur contre une suppression accidentelle cochée, puis on valide (cf. Figure 24).

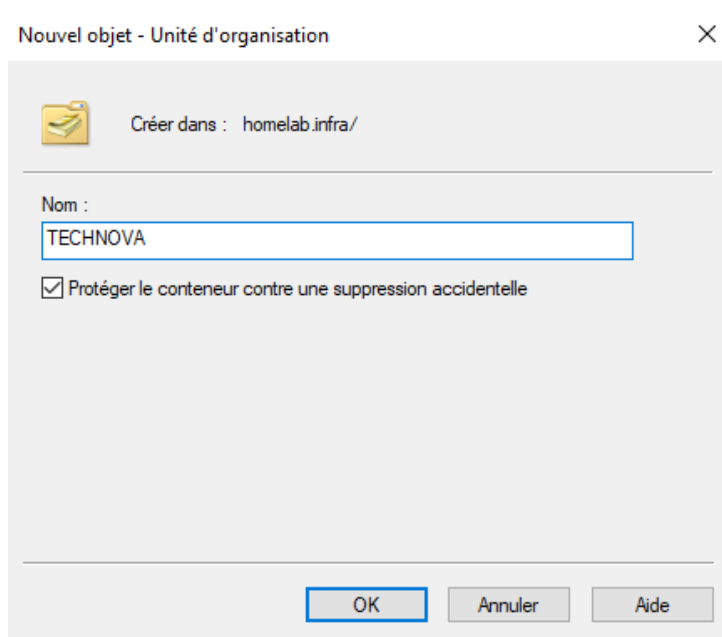


Figure 24: Création d'une unité d'organisation sur le serveur AD

**Création des groupes** De la même manière, la création des groupes nécessaires à la gestion des utilisateurs se fait manuellement via la console AD. On clique-droit sur l'OU souhaitée (par exemple TECHNOVA ou une OU dédiée Groupes), puis on choisit Nouveau > Groupe. On renseigne le nom du groupe (par exemple : Direction, Secrétariat, Comptabilité, Informatique, Tous\_Utilisateurs), on sélectionne le type (Sécurité) et la portée (Global ou Domaine local), puis on valide la création (Voir Figure 25).

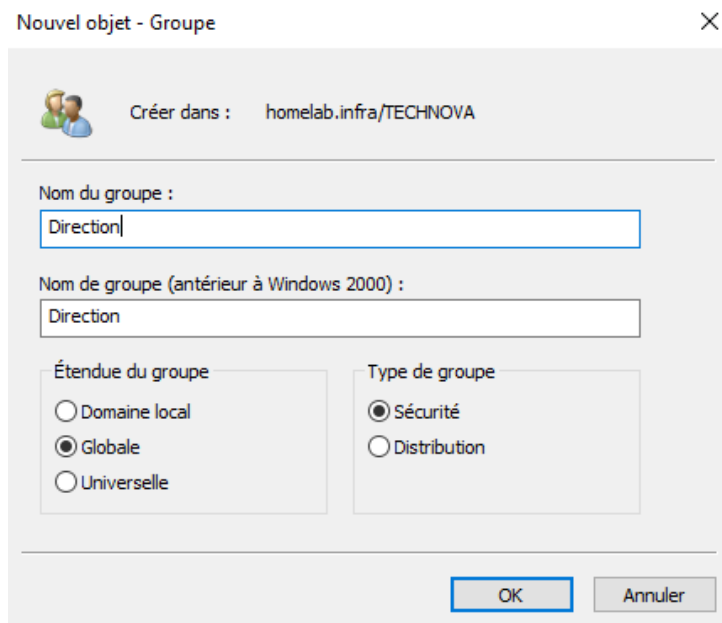


Figure 25: Création d'un groupe sur le serveur AD

Cette organisation permet de gérer efficacement les droits d'accès aux ressources du réseau (partages de fichiers, stratégies GPO, imprimantes, etc.). Chaque groupe correspond à une fonction et regroupe les utilisateurs qui doivent bénéficier d'autorisations spécifiques.

**Remarque :** Ces groupes ont pour but d'organiser les utilisateurs par service dans l'AD. Les groupes spécifiques aux droits d'accès (comme ceux utilisés pour les partages de fichiers) seront créés plus tard, avec une convention de nommage dédiée (ex : G\_Direction, G\_Comptabilité, etc.)

**Import des utilisateurs via PowerShell** Une fois les OU et groupes en place, nous avons automatisé la création des utilisateurs à l'aide d'un script PowerShell personnalisé, basé sur un fichier CSV. Ce fichier contient les informations de six employés : une directrice, deux secrétaires, deux comptables et un technicien informatique, avec des colonnes telles que prénom, nom, fonction, et mot de passe (optionnel). Le script permet de :

- Générer un identifiant unique pour chaque utilisateur (initiale du prénom + nom, en minuscules),
- Créer chaque compte utilisateur dans une OU sélectionnée,
- Définir une adresse e-mail de type prenom.nom@tssr.corp,
- Assigner un mot de passe par défaut ou personnalisé,
- Forcer le changement du mot de passe à la première connexion,
- Ajouter l'utilisateur à un ou plusieurs groupes AD existants.

L'exécution du script est interactive : l'administrateur peut choisir dynamiquement l'OU de destination ainsi que les groupes pour chaque utilisateur via des interfaces graphiques (Out-GridView), ce qui garantit souplesse et praticité. Cette méthode réduit les erreurs de saisie et assure une uniformité dans la création des comptes.

Une fois le script Ajout\_user.ps1 et le fichier Liste\_utilisateurs.csv préparés, on ouvre PowerShell et on se place dans le répertoire où ils sont stockés. L'exécution du script se fait à l'aide de la commande : ".\Ajout\_user.ps1". Dès le lancement, le script demande à l'administrateur de sélectionner le fichier .csv à importer (cf. Figure 26).

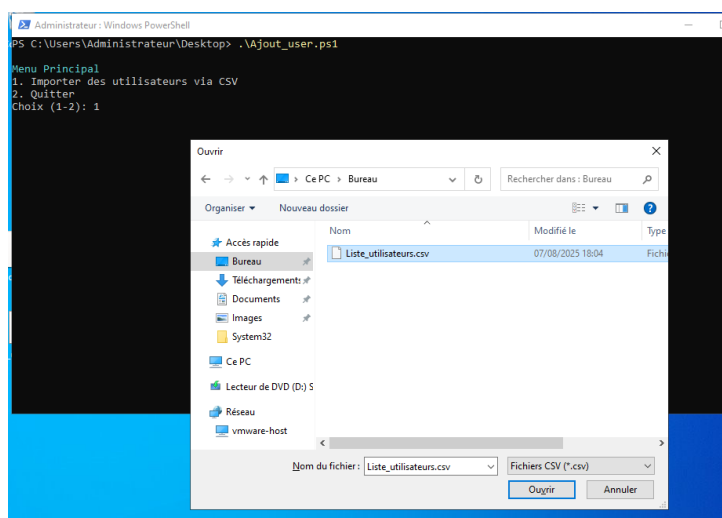


Figure 26: Sélection du fichier Liste\_utilisateurs.csv lors de l'exécution du script

Une fois le fichier chargé, il guide l'utilisateur à travers le processus d'ajout : sélection de l'unité d'organisation (OU), choix des groupes AD, affectation des mots de passe, etc. À la fin de l'exécution, les comptes sont automatiquement créés et ajoutés aux groupes sélectionnés. Les résultats sont visibles à la fois dans la console Active Directory et directement dans PowerShell, comme illustré en Figure 27.

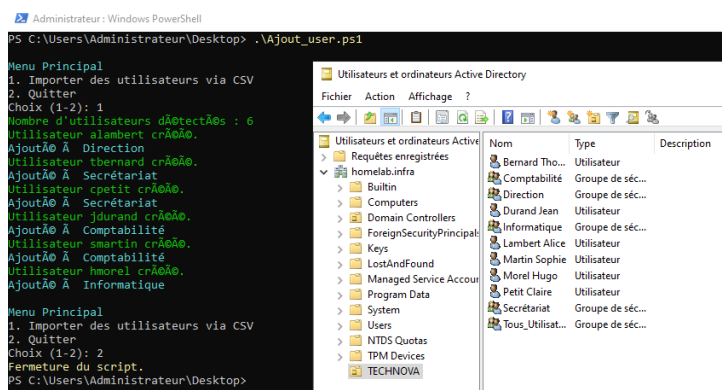


Figure 27: Utilisateurs ajoutés dans Active Directory et confirmation dans PowerShell

Le script se trouve dans le dossier /scripts du dépôt, tandis que le fichier .csv contenant les utilisateurs est placé dans /docs.

#### 4.4 Serveur de fichiers : Windows Server 2022

Nous retournons sur VMware Workstation pour créer la machine virtuelle qui jouera le rôle de serveur de fichiers pour le LAN. Voici les étapes à suivre :

1. Cliquer sur "Create a New Virtual Machine", puis choisir "Custom (advanced)", et cliquer deux fois sur "Next".

2. Sélectionner "I will install the operating system later", puis cliquer sur "Next".
3. Dans "Guest Operating System", cocher "Microsoft Windows" et choisir "Windows Server 2022", puis cliquer sur "Next".
4. Donner le nom "ServeurFichiers" à la VM et choisir le dossier de destination, puis cliquer sur "Next".
5. Attribuer 2 processeurs (1 cœur chacun) et 2 Go de RAM, puis cliquer sur "Next".
6. Pour la carte réseau, sélectionner "Host-only" (nous la changerons en LAN Segment juste après), puis cliquer trois fois sur "Next".
7. Choisir "Create a new virtual disk", cliquer sur "Next".
8. Définir une taille de 60 Go, cocher "Store virtual disk as a single file", puis cliquer deux fois sur "Next", et enfin "Finish".

Avant d'allumer la VM, on va changer son interface réseau :

1. Cliquer sur "Edit virtual machine settings".
2. Dans "CD/DVD (SATA)", cocher "Use ISO image file" et sélectionner l'image ISO de Windows Server 2022.
3. Dans "Network Adapter", changer la connexion en "LAN Segment", et sélectionner le segment correspondant au LAN.

On peut voir un résumé de la configuration du Serveur des Fichiers sur la Figure 28.

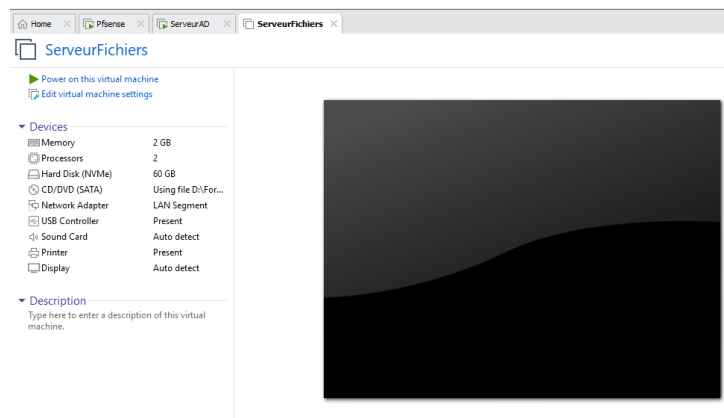


Figure 28: Résumé de la configuration de la machine ServeurFichiers

#### 4.4.1 Installation du Serveur Windows 2022 - Serveur de Fichiers

Après avoir démarré la VM ServeurFichiers, appuyer sur n'importe quelle touche pour démarrer sur l'image ISO du CD. Dans les premières options d'installation, sélectionner :

- Langue à installer : Français (France)
- Format horaire et monétaire : Français (France)



- Clavier ou méthode d'entrée : Français

Cliquer ensuite sur Suivant, puis sur Installer maintenant. Dans la liste des éditions, choisir : Windows Server 2022 Standard Evaluation (Expérience de bureau), puis cliquer sur Suivant. Cocher la case "J'accepte les termes du contrat de licence logiciel Microsoft", puis cliquer sur Suivant. Choisir l'option "Personnalisé : Installer uniquement le système d'exploitation Microsoft Server". Dans la liste des disques, sélectionner "Lecteur 0 – Espace non alloué" comme destination de l'installation, puis cliquer sur Suivant pour lancer l'installation.

Une fois l'installation terminée et le système redémarré, une fenêtre vous invite à définir un mot de passe pour le compte Administrateur. Saisir le mot de passe suivant deux fois : Azerty123!, puis cliquer sur Terminer.

#### **4.4.2 Configuration classique de Windows Serveur – L'intégration dans le domaine**

Après le redémarrage, appuyer sur "Ctrl+Alt+Suppr" et saisir le mot de passe pour se connecter en tant qu'Administrateur. La première étape consiste à changer le nom du serveur et à attribuer une adresse IP statique, afin qu'il puisse rejoindre le domaine.

**Remarques :** Avant de continuer, il est recommandé d'installer VMware Tools pour améliorer les performances et la fluidité de la machine virtuelle.

##### **Renommer le serveur**

1. Ouvrir la fenêtre "Exécuter" en recherchant run dans le menu démarrer.
2. Taper sysdm.cpl puis appuyer sur Entrée.
3. Dans l'onglet Nom de l'ordinateur, cliquer sur Modifier...
4. Entrer le nom : ServeurFichiers, puis cliquer sur OK deux fois pour valider.
5. Redémarrage requis (à faire après les étapes suivantes).

##### **Configuration de l'adresse IP statique**

1. Réouvrir Exécuter (run) et taper ncpa.cpl, puis Entrée pour ouvrir les connexions réseau.
2. Clic droit sur Ethernet0, puis Propriétés.
3. Dans la liste, décochez IPv6 pour le désactiver.
4. Double-cliquer sur Protocole Internet version 4 (TCP/IPv4).
5. Cocher "Utiliser l'adresse IP suivante" et remplir :
  - Adresse IP : 192.168.100.11
  - Masque : 255.255.255.0

- Passerelle par défaut : 192.168.100.1

6. Cocher "Utiliser l'adresse de serveur DNS suivante" :

- DNS préféré : 192.168.100.10

7. Cocher "Valider les paramètres en quittant", puis cliquer sur OK deux fois.

Les étapes ci-dessus sont illustrées dans les Figures 29 et 30.

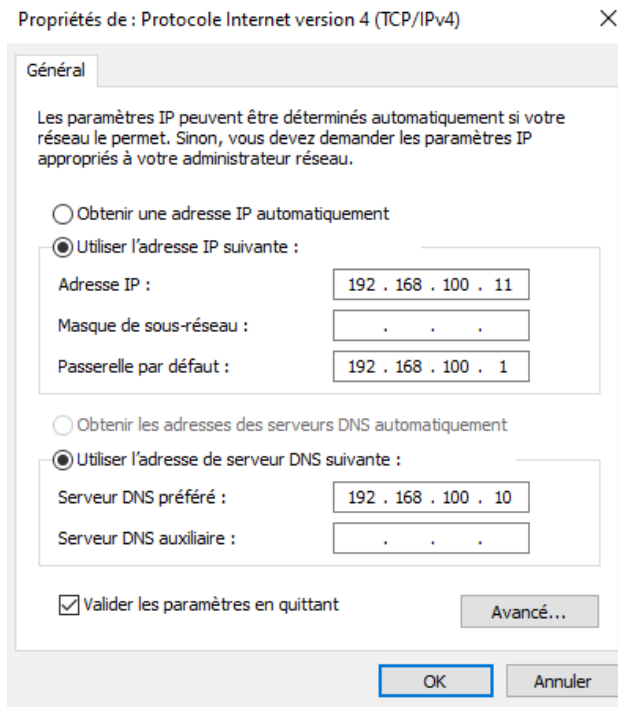


Figure 29: Renommer le serveur des Fichiers

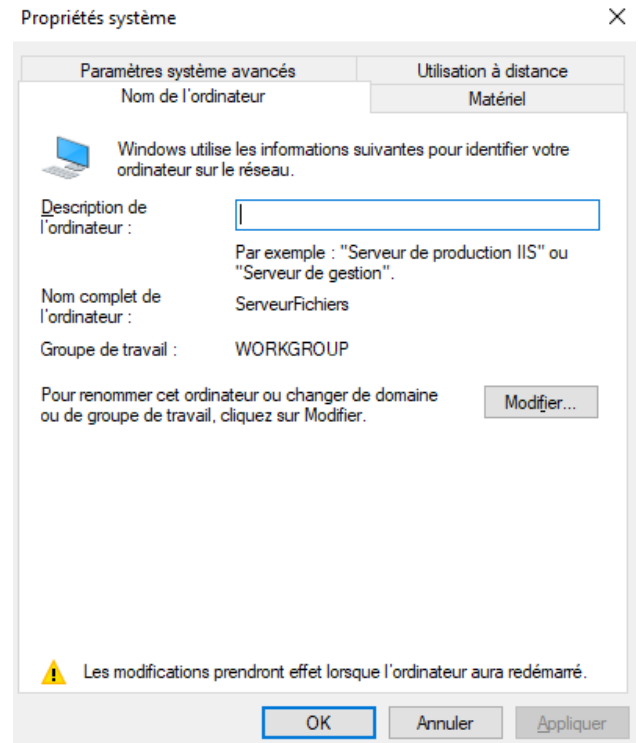


Figure 30: Adresse IP Statique pour le Serveur des Fichiers

**Vérification :** Ouvrir l'invite de commandes (cmd) et taper ipconfig pour vérifier la nouvelle configuration réseau. Comme le montre la Figure 31, l'adresse IP est bien définie en statique. Enfin, redémarrer le serveur pour appliquer le nouveau nom d'hôte.

```

C:\Users\Administrateur>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. . . . . : 192.168.100.1

C:\Users\Administrateur>_

```

Figure 31: Vérification de l'IP du Serveur des Fichiers avec ipconfig

**Ajouter dans le domaine** Après le redémarrage du serveur, on va le faire rejoindre le domaine.

1. Réouvrir la fenêtre "Exécuter" en recherchant run dans le menu démarrer.
2. Taper sysdm.cpl puis appuyer sur Entrée.
3. Dans l'onglet Nom de l'ordinateur, cliquer sur Modifier...
4. Cocher la case membre d'un domaine et mettre le domaine "homelab.infra"
5. Mettre les identifiants de l'admin du serveur AD
6. Redémarrage requis (à faire après les étapes suivantes).

Après le redémarrage du serveur des Fichiers (suite à l'intégration dans le domaine), on se connecte à présent avec un compte du domaine, ici : homelab\Administrateur. Le serveur étant désormais membre du domaine homelab.infra, il est prêt à recevoir des stratégies de groupe (GPO) et à gérer les droits d'accès en fonction des groupes définis.

Les étapes ci-dessus sont illustrées dans les Figures 32

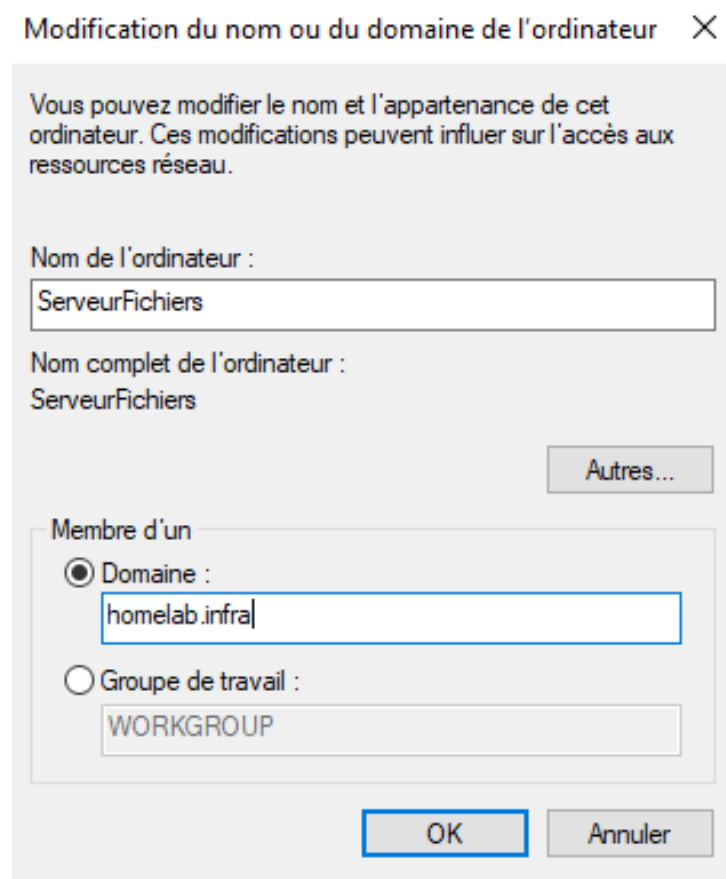


Figure 32: Intégration du Serveur des Fichiers dans le domaine homelab.infra

#### 4.4.3 Configuration du serveur de fichiers (NTFS, partages)

Pour la prochaine étape, on va configurer le serveur de fichiers. Pour commencer, on va d'abord ajouter un nouveau disque sur la machine "serveurFichiers" depuis VMware Workstation (cf : Figure 33).

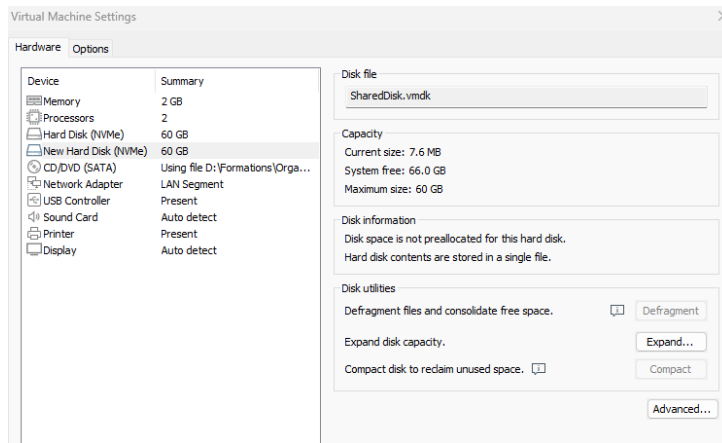


Figure 33: Ajouter un nouveau disque sur le serveur de Fichiers

Sur la machine "serveurFichier", on ouvre Gestion de l'ordinateur et on clique sur "gestion des disques". On initialise le Disque 1 (Voir la Figure 34)

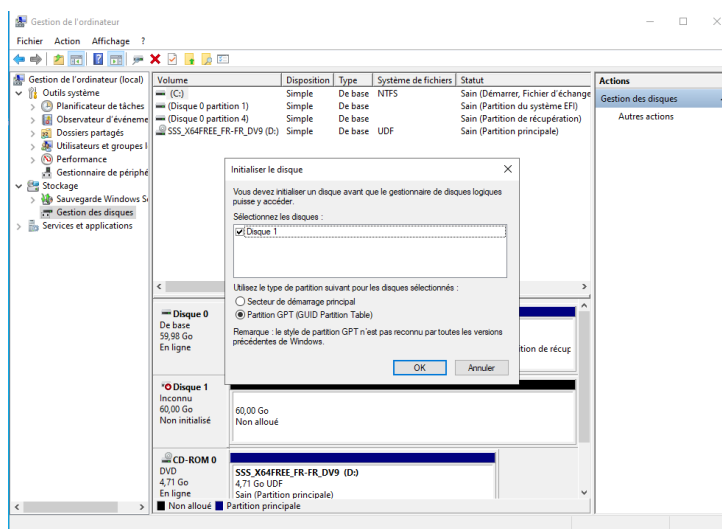


Figure 34: Initialiser le nouveau disque sur le serveur de Fichiers

On clique-droit sur "Disque 1" et sur "Nouveau volume simple...". On clique sur "Suivant" autant que nécessaire. On change le nom le volume (ici : Partages et la lettre E), on coche la case "Effectuer un formatage rapide" et on clique sur "Suivant" puis sur "Terminer".

Une fois le disque formaté et disponible dans l'explorateur de fichiers sous la lettre "E:\", on crée un nouveau dossier nommé "Partages". Dans ce dossier, on crée ensuite les sous-dossiers suivants, chacun correspondant à un service de l'entreprise (cf : Figure 35):

- Direction
- Secrétariat
- Comptabilité
- Informatique

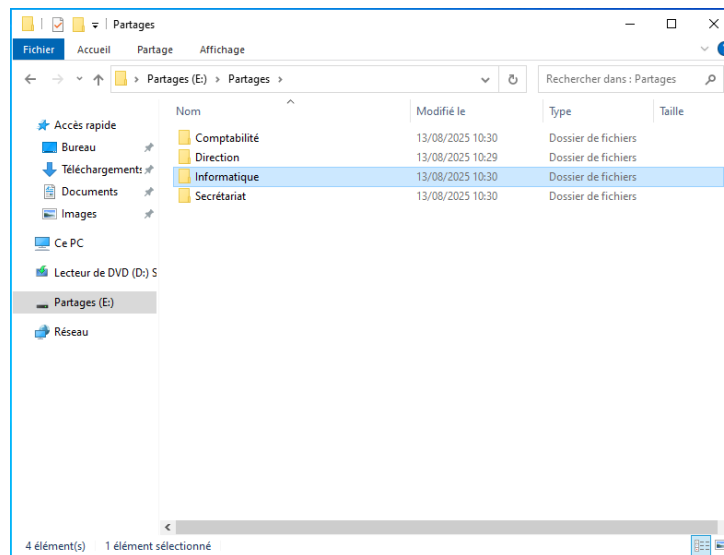


Figure 35: Arborescence des dossiers dans E:\Partages

**Création des groupes de sécurité dans l'Active Directory** Pour gérer les accès aux dossiers partagés du serveur de fichiers, nous avons créé des **groupes de sécurité dédiés**, distincts de ceux utilisés pour l'organisation des utilisateurs dans l'AD. Les groupes créés sont les suivants :

- G\_Direction
- G\_Secrétariat
- G\_Comptabilité
- G\_Informatique

On clique-droit sur l'OU souhaitée (par exemple TECHNOVA ou une OU dédiée Groupes), puis on choisit Nouveau > Groupe. On renseigne le nom du groupe (par exemple : G\_Direction, G\_Secrétariat, G\_Comptabilité, G\_Informatique), on sélectionne le type (Sécurité) et la portée (Global), puis on valide la création (Voir Figure 36).

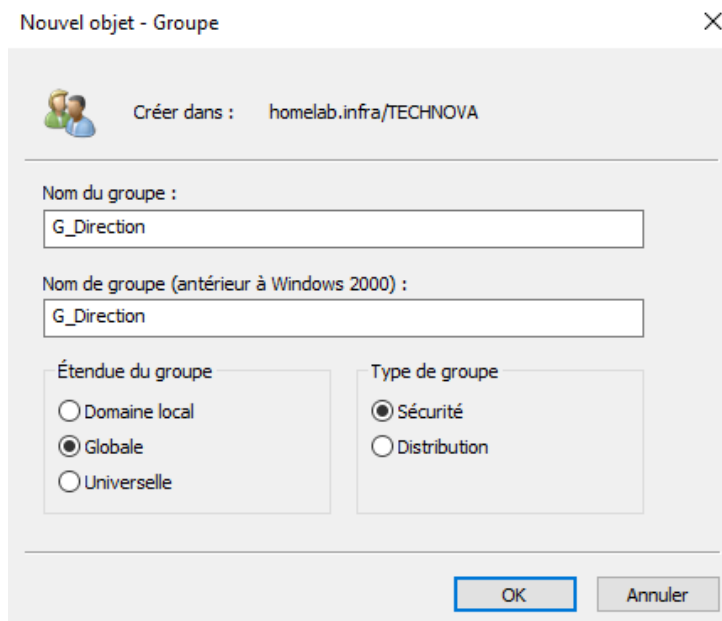


Figure 36: Création d'un groupe de sécurité dans l'AD

Chaque utilisateur est ensuite ajouté au groupe correspondant à son service. Aucun droit n'est attribué directement à un utilisateur (Voir la Figure 37).

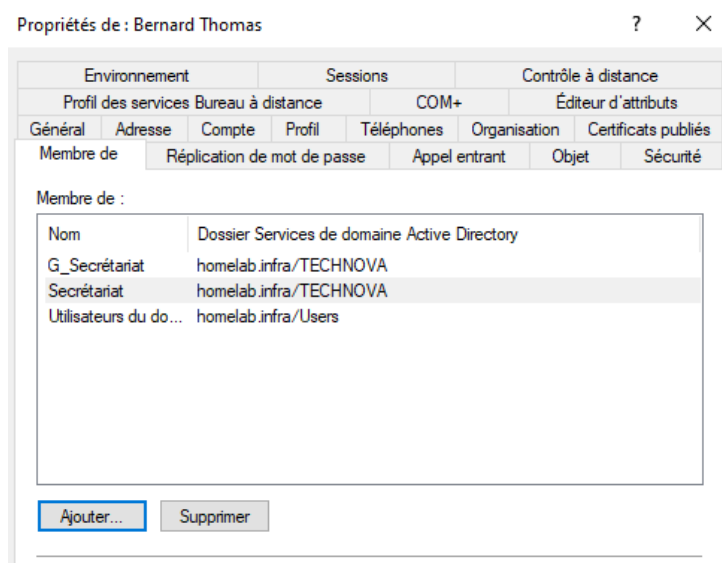


Figure 37: Ajout d'un utilisateur dans un groupe de sécurité sur l'AD

**Application des droits NTFS** Sur la machine "serveurFichiers", on clique-droit sur chacun des dossiers ("E:\Partages\Direction", "Secrétariat", etc.) puis sur "Propriétés > Sécurité > Modifier... > Ajouter..." pour attribuer les droits au "groupe AD" correspondant.

Table 5: Droits NTFS par groupe de sécurité

Dossier	Groupe AD	Droits NTFS
Direction	G_Direction	Contrôle total
Secrétariat	G_Secrétariat	Lecture / écriture
Comptabilité	G_Comptabilité	Lecture / écriture
Informatique	G_Informatique	Contrôle total

### Remarques importantes :

- On supprime les droits par défaut de "Utilisateurs", "Tout le monde", etc.
- On désactive l'héritage si nécessaire pour appliquer des règles spécifiques à chaque dossier.
- L'accès au dossier 'Partages' peut être limité en lecture seule à tous les groupes si besoin, ou simplement masqué.

On peut voir un exemple sur la Figure 38.

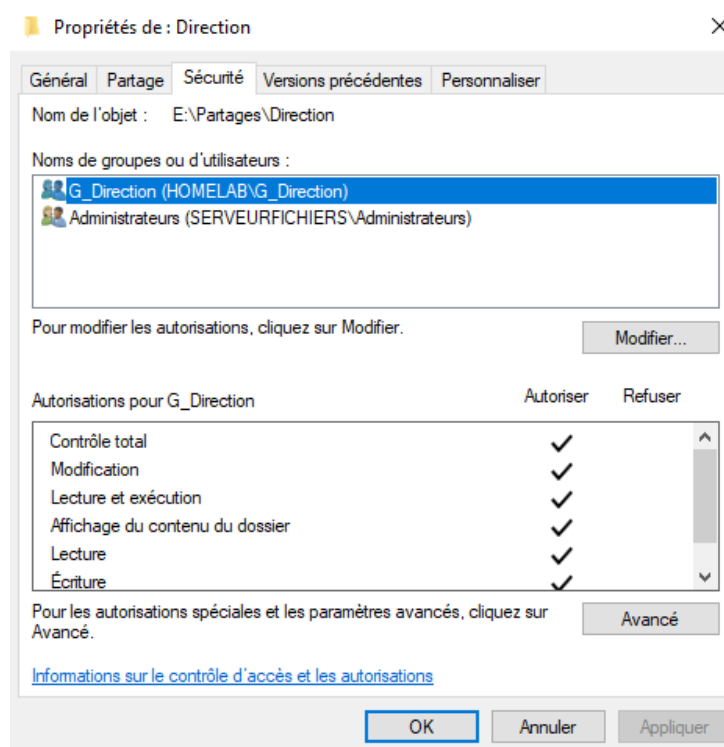


Figure 38: Appliquer les droits NTFS sur les sous-dossiers sur le serveur des Fichiers

**Partage des dossiers sur le réseau** On partage ensuite chaque dossier individuellement (clic droit > Partager avec > Partage avancé), en utilisant le même nom que le dossier pour éviter toute confusion (cf : Figure 39). Pour chaque partage :

- On coche "Partager ce dossier"
- On donne un nom simple, ex : "Direction", "Secrétariat", etc.
- Dans "Autorisations", on supprime "Tout le monde" et on ajoute le groupe AD correspondant avec les droits nécessaires

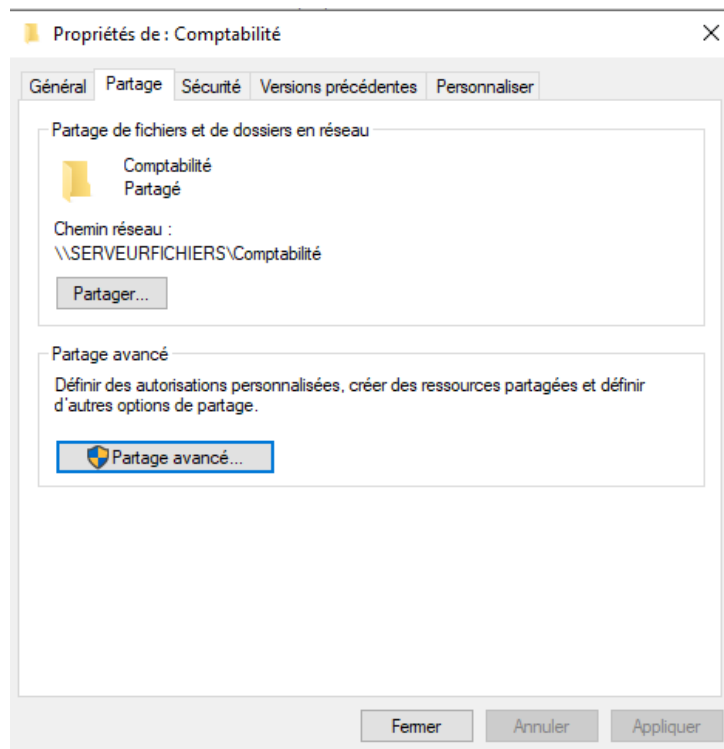


Figure 39: Partage avancé d'un dossier sur le réseau

**Masquage des dossiers non autorisés** Pour éviter que les utilisateurs voient les dossiers partagés auxquels ils n'ont pas accès, nous avons activé la fonctionnalité "Access-Based Enumeration" (ABE) sur le dossier partagé principal (Partages). Cette fonctionnalité masque dynamiquement les sous-dossiers visibles en fonction des droits NTFS attribués à chaque utilisateur.

Activation :

- Ouvrir le Gestionnaire de serveur sur le serveur de fichiers
- Aller dans Services de fichiers et de stockage > Partages
- Clic droit sur le partage concerné (Partages) > Propriétés
- Dans l'onglet Paramètres, cocher l'option : "Activer l'énumération basée sur les accès" (cf : Figure)

Ainsi, un utilisateur du groupe "G\_Secrétariat" ne verra pas les dossiers "Direction" ou "Informatique", sauf s'il a les autorisations nécessaires.



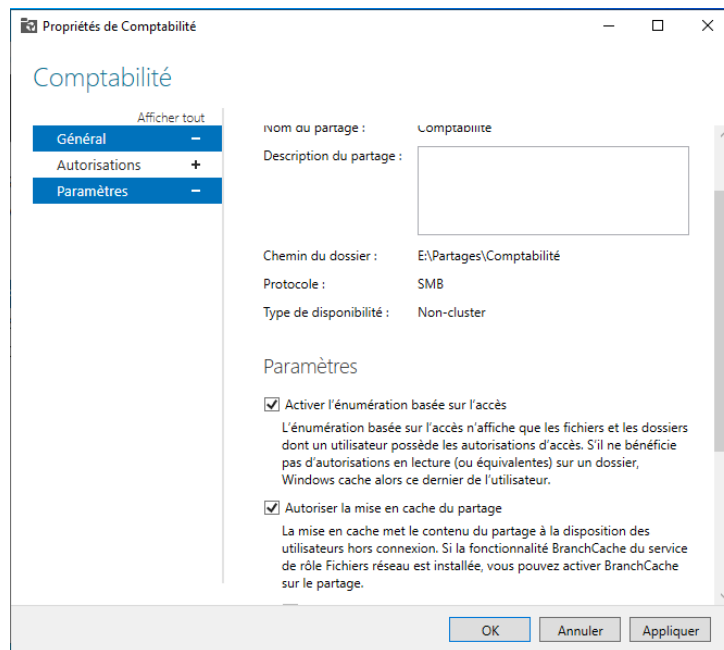


Figure 40: Masque un dossier non autorisé via ABE sur le serveur des Fichiers

Le serveur de fichiers est désormais configuré avec une structure de dossiers organisée, des permissions NTFS adaptées, et des partages sécurisés activés. La prochaine étape consistera à configurer les machines clientes, afin de vérifier leur intégration au domaine et leur accès contrôlé aux ressources partagées selon les droits définis.