Configuration serveur HP HPE proliant ML350 GEN9

Table des matières

Pré-requis :

- ISO : Windows server 2022
- ISO : Windows 10 / 11 (pour la/les machines clientes)

- ISO pfSense
- Clé bootable

Cette documentation présentera l'installation et la configuration d'un serveur HP Proliant avec un Windows Server 2022.

Pour chaque VM crée, il faudra :

a) Renommer la vm

b) Redémarrer la vm

c) Attribuer une IP, un masque, une passerelle, un DNS. Pour la passerelle on mettre 192.168.26.254. Poue le DNS de l'AD : 127.0.0.1, pour les VM : IP_AD

d) Joindre les VMs au domaine. Pour cela dans le menu Windows, taper dans la barre de recherche système > paramètres avancés du système. Dans la fenêtre ouvrante > nom de l'ordinateur > modifier → joindre au domaine.

Un mot de passe et un identifiant seront demandés : taper les id admin de la vm AD

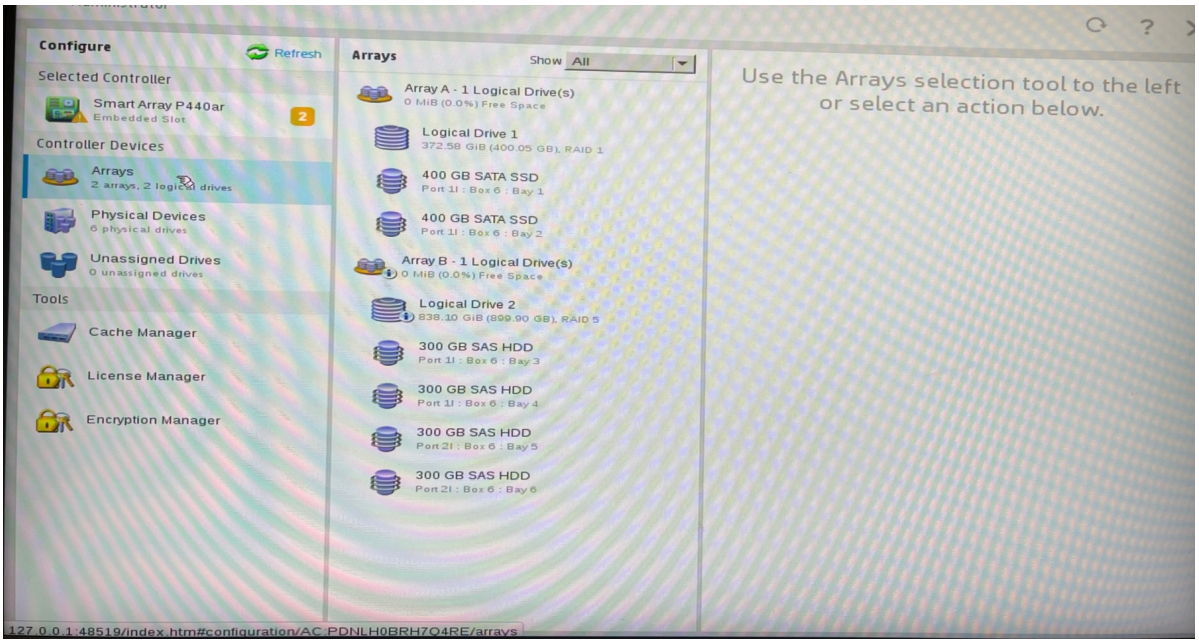
Pour chaque VM, pour chaque rôle installé, se connecter en tant qu'administrateur du domaine

Étape 1 : Configuration RAID

Au démarrage, aller dans intelligent provisionning (F10) > hp storage administrator, dans action > create array> sélectionner SATA SSD > Sélectionner les 2 disques de 400 GB pour le système et les mettre en RAID 1 (mirroring) > create array > finish

Pour le reste, aller dans unsagned drives > sélectionner les disques restants > create array> et les mettre en RAID 5 (mieux pour la restauration)

Il aurait été possible de les mettre en RAID 6, les deux RAID ont de la parité sur chaque disques, le RAID 6 permet de gérer des disques de différentes tailles. Ici, on utilisera le RAID 5 avec nos disques de 300 GB



Redémarrer le serveur

Étape 2 : Installer Windows Server sans clé

Pour booter avec une clé voir Étape 3

Une fois le serveur redémarrer, il faut attribuer une adresse IP au serveur pour pouvoir se connecter à l'ILO et booter sur l'OS (différents supports possibles : Clé USB, image disque …).

Aller dans system utility (F9) > system configuration > setting option : vérifier que ILO 4 Functionnality et ILO 4 Configuration utility soit « enabled ».

> echap > network option > on peut voir l'IP attribuée, le masque ainsi que la passerelle.

IP : 172.16.1.114

Masque : 255.255.255.0

Passerelle : 172.16.1.240

Sur un autre poste se connecter à l'ILO via l'IP attribuée, rentrer les identifiants de connexion, marqués généralement sur une face du serveur.

Étape 2.1 : ILO

Pour booter vers l'image disque, il faut activer la console via l'ILO. Aller dans remote console > launch. Dans les onglets de la console aller dans virtual drives > images files CD/DVD ISO > sélectionner l'ISO souhaitée, ici l'ISO de Windows serveur

> exit and resume normal boot

→ Installation Windows server

Étape 3 : Installer Windows Server avec clé

Au démarrage > boot menu (F11) > sélectionner la bonne clé USB.

Suivre les instructions (intuitives), sélectionner installation standard expérience de bureau car nous voulons une interface graphique. Pour utiliser uniquement du Powershell et avoir les outils d'administration à distance comme Windows Admin Center, sélectionner « standard » Pas besoin de pilote avec la clé.

Pour l'installation, on choisira installation personnalisée

Une fois Windows server installé, enlever la clé pour ne pas rebooter sur la clé au redémarrage.

Une fois le serveur redémarrer, on peut voir qu'à chaque démarrage le serveur check son system, s'il repère des erreurs il proposera soit F1 pour continuer (erreur) soit F2 pour avoir plus d'informations sur les erreurs. Appuyer sur F1 si ce sont des erreurs dites « bénignes »

3.1 : MDP

Il est demandé de créer un mot de passe Admin, pour cela il faut respecter les politiques de sécurités mises en vigueur par l'ANSI , un mot de passe doit contenir 15 caractères pour un service critique contre 9 à 12 pour un service peu critique.

Microsoft en revanche, privilégie des « passkeys »

Étape 4 : Nommer le PC

Il faut nommer le PC avant toute configuration, après ça ne sera plus possible.

Taper dans la barre de recherche Windows : « nom » et cliquer sur « à propos de ce PC » > renommer le PC

Suivre sa convention de nommage pour repérer de quel type de machine il s'agit, pour quel service et son numéro.

Ici on mettra : SRV-LAB-01

Étape 5 : Mises à jour

Effectuer toutes les mises à jour et reboot le serveur

Étape 6 : Partition données

Dans le menu Windows, ouvrir mmc.exe > fichier > snapin (ajout/supp…) > gestionnaire de disque > ajouter > …. > aller dans disques non alloués > clic droit > volume simple (laisser par défaut)

Étape 7 : Connexion à distance

Aller dans paramètres > autoriser la connexion bureau à distance.

Étape 7 : Rôle AD

--SCREEN--

Étape 8 : Installer Rôle Hyper-V

Pré-requis :

- Option de virtualisation activée (ici, dans BIOS > System utilities (F9))

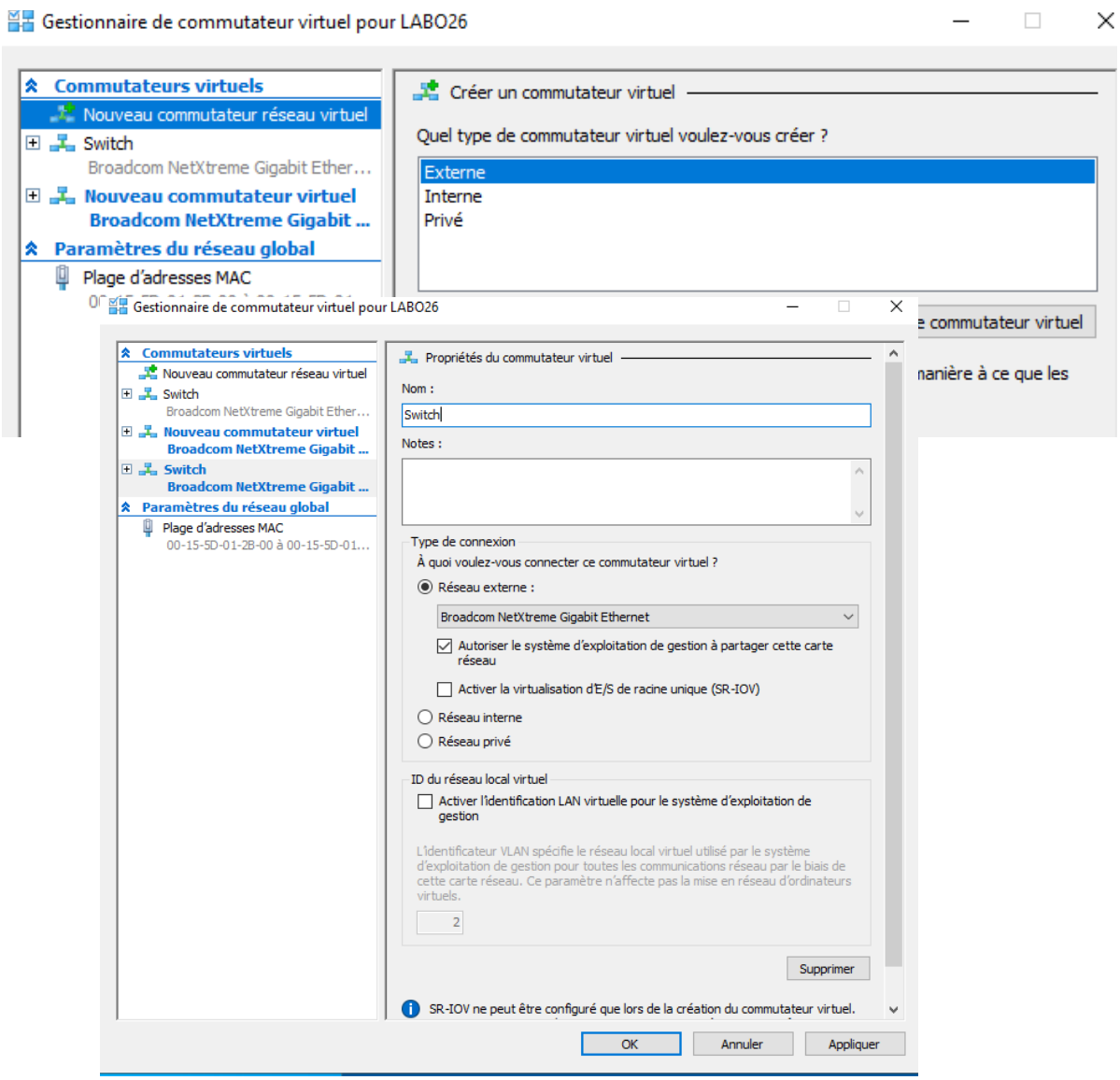
Hyper-V est un hyperviseur de niveau 1 (barre métal) développée par Microsoft. Contrairement à ceux de niveau 2 qui s'exécutent comme des applications sur un système d'exploitation hôte, Hyper-v s'exécute directement sur le matériel physique, plaçant l'OS principal dans une partition parant.

Dans le gestionnaire de serveur, aller dans gérer > ajout des rôles et fonctionnalités > sélectionner le rôle hyper-V , tout laisser par défaut > installer

Étape 9 : Switch virtuel (si besoin connexion directe au réseau)

Si les VMs ont besoin d'une connexion internet sans passer par un routeur > aller dans gestionnaire du rôle hyper-v > aller sur le serveur ici, LABO26 > gestionnaire de commutateur > choisir : externe > créer un commutateur virtuel

Attribuer le nom souhaité



Pour le projet, on mettra le réseau en interne, en mode LABO.

> Le serveur et les Vms peuvent communiquer entre eux.

Avec un réseau privé, seules les Vms auraient pu communiquer entre elles.

Étape 10 : AD

Pour cette vm et les suivantes, se référer à 10.1

Pré-requis :

- ISO Windows Server 2022
- Rôle hyper-v installé
- Disque avec dossier crées spécial pour les VM, on l'appellera DATA et le dossier « Hyper-v »

Toujours dans gestionnaire hyper-v > LABO26 > nouveau > ordinateur virtuel

Suivre les instructions (intuitives) lors de la création de la Vm. Pour la « génération » choisir : 2

Pour la mémoire, lui allouer 6096 Go pour une meilleure performance ainsi que 4 cœurs ou plus. Pour l'emplacement de la Vm, changer l'emplacement public par le chemin du dossier crée

a) Dans le gestionnaire de serveur, aller dans « ajout de rôle et de fonctionnalité » > dans gérer > rôle > cocher Services de domaine Active Directory (AD DS) > clic sur suivant jusqu'à « installer »

b) Une fois le rôle installé, cliquer sur l'alerte en haut à droite « Promouvoir ce serveur en contrôleur de domaine »

c) Sélectionnez « Ajouter une nouvelle forêt » et entrez le nom de domaine souhaité, ici on mettra « mathilde.local »

domaine.

d) Définissez les options pour le niveau fonctionnel de la forêt et du domaine, ainsi que le mot de passe du mode de restauration des services d'annuaire (DSRM).

Pour « spécifier les fonctionnalités de contrôleur de domaine », laissez les deux premières cases cochées

e) Suivre les instructions à l'écran et redémarrez le serveur une fois la promotion terminée.

Étape 11 : Adressage IP

Il est important que le serveur avec le rôle AD ait une IP fixe comme tous les autres serveurs qui vont suivre

Dans les paramètres > Ethernet > centre de réseau et partage > modifier les paramètres de la carte réseau > clic droit > propriété.

Dans la fenêtre ouvrante, clic sur Protocole internet version 4 (TCP/ IPV4) > propriétés

Attribuer l'IP, le masque, la passerelle ainsi que le serveur DNS. Pour le serveur DNS on mettra l'IP du serveur lui-même, il passera ensuite automatiquement en localhost.

Possible de mettre directement le localhost soit 127.0.0.1

IP : 192.168.26.25

MASQUE : 255.255.255.0 (/24)

PASSERELLE : 192.168.26.254

Étape 12 : DHCP

Si pas IP fixe pour les VM clientes : dans le gestionnaire de serveur > gérer > ajout de rôle ou de fonctionnalités > cocher DHCP > suivant jusqu'à installer

Dans outils > gestionnaire DHCP > IPv4 > clic droit > nouvelle étendue

Il faut laisser au minimum 10 IP fixes réservées pour les différents services associés au serveur. On admettra qu'il y a en plus 30 postes. (Pool DHCP = 30)

Pour le renouvellement de bail, il est important de le renouveler régulièrement pour les besoins en adressage IP . Réduire le temps à 1j.

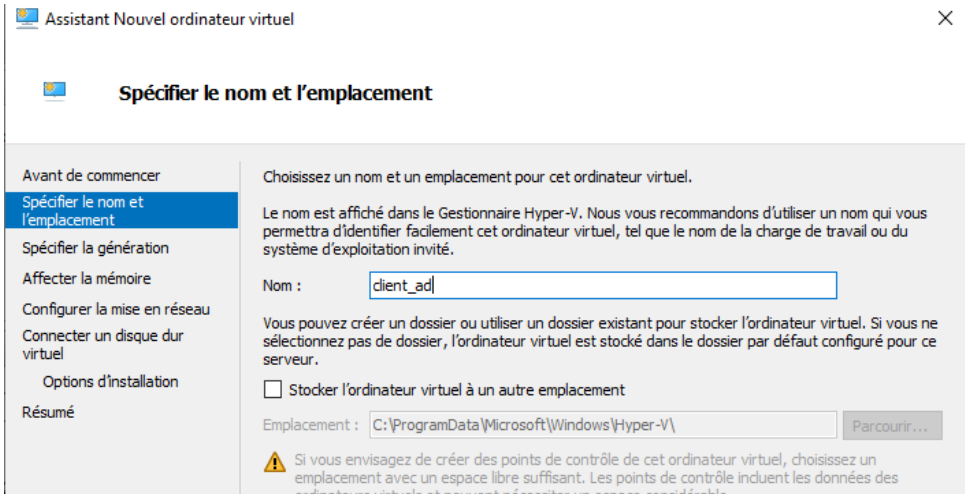
12.1 : DNS

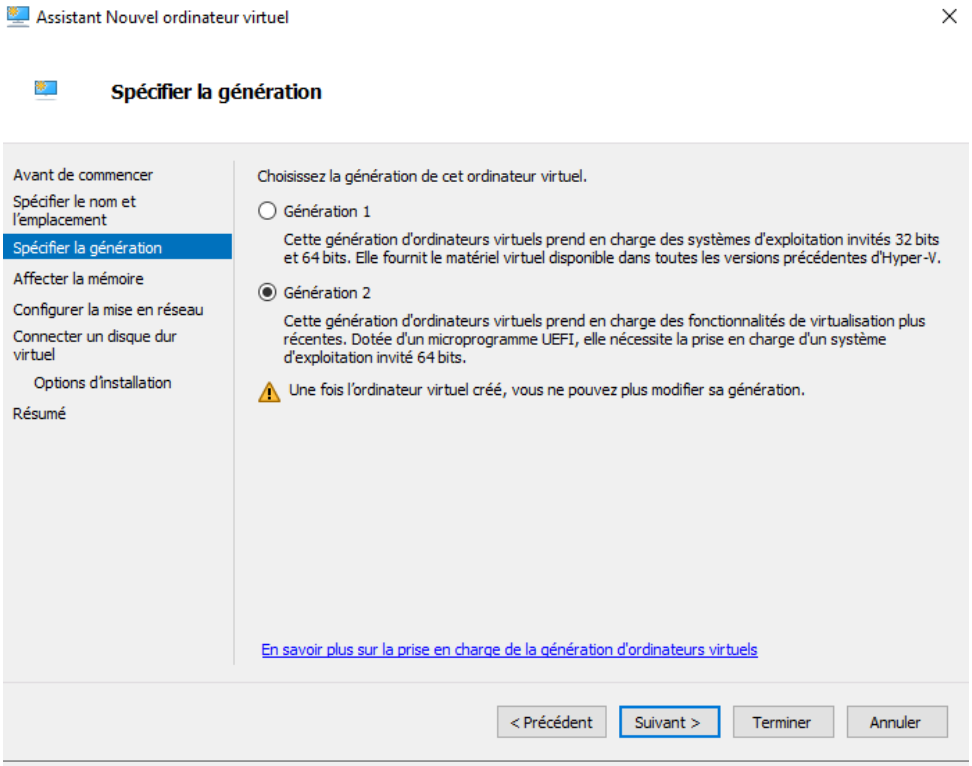
Dans une nouvelle requête, toujours dans « ajout de rôle et de fonctionnalités », ajouter le rôle DNS > suivant jusqu'à installer

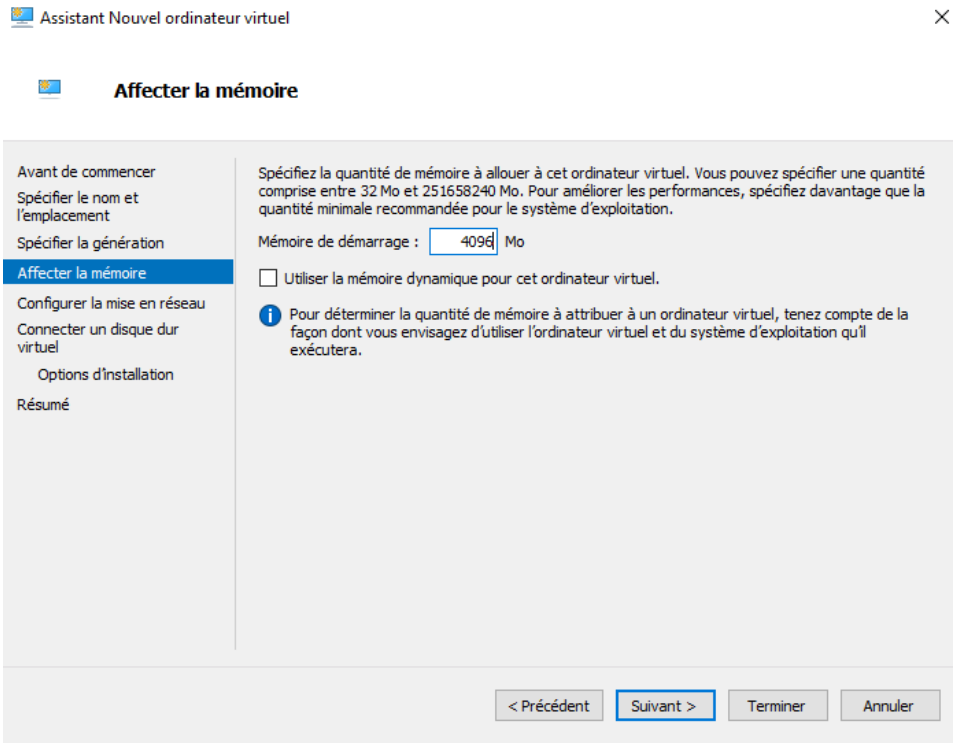
Dans outils > gestionnaire DNS > serveur DNS > clic droit > propriétés

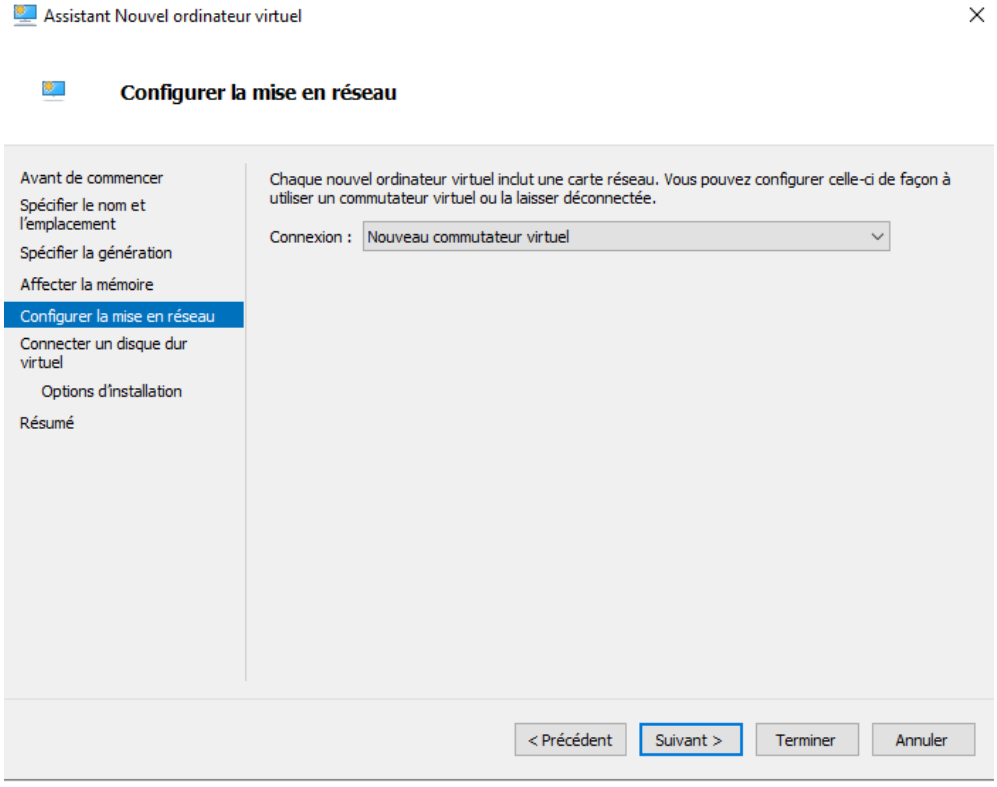
Dans l'onglet redirecteurs > modifier. Ajouter d'autres serveurs DNS comme Google 8.8.8.8

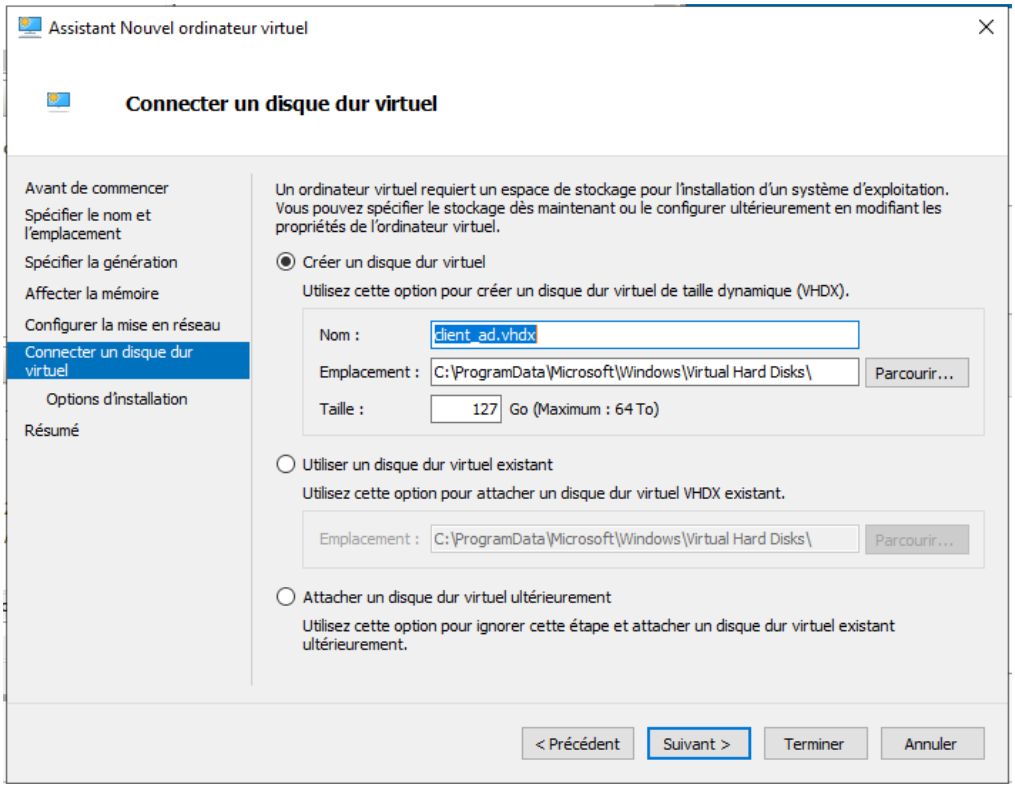
Étape 13 : Cliente - AD

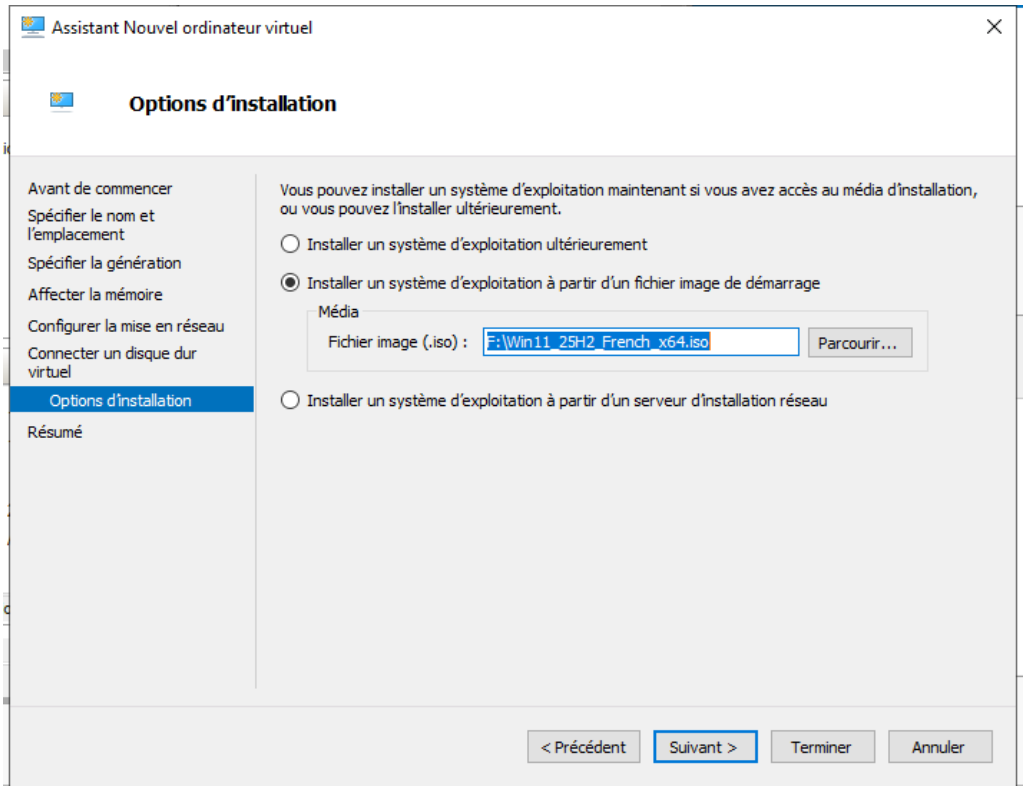





Assistant Nouvel ordinateur virtuel
Affecter la mémoire
Avant de commencer
Spécifier le nom et l'emplacement
Spécifier la génération
Affecter la mémoire
Configurer la mise en réseau
Connecter un disque dur virtuel
Options d'installation
Résumé
Spécifiez la quantité de mémoire à allouer à cet ordinateur virtuel. Vous pouvez spécifier une quantité comprise entre 32 Mo et 251658240 Mo. Pour améliorer les performances, spécifiez davantage que la quantité minimale recommandée pour le système d'exploitation.
Mémoire de démarrage : 4096 Mo
Utiliser la mémoire dynamique pour cet ordinateur virtuel.
Pour déterminer la quantité de mémoire à attribuer à un ordinateur virtuel, tenez compte de la façon dont vous envisagez d'utiliser l'ordinateur virtuel et du système d'exploitation qu'il exécutera.
< Précédent
Suivant >
Terminer
Annuler


Assistant Nouvel ordinateur virtuel
Configurer la mise en réseau
Avant de commencer
Spécifier le nom et l'emplacement
Spécifier la génération
Affecter la mémoire
Configurer la mise en réseau
Connecter un disque dur virtuel
Options d'installation
Résumé
Chaque nouvel ordinateur virtuel inclut une carte réseau. Vous pouvez configurer celle-ci de façon à utiliser un commutateur virtuel ou la laisser déconnectée.
Connexion : Nouveau commutateur virtuel
< Précédent
Suivant >
Terminer
Annuler


Assistant Nouvel ordinateur virtuel
Connecter un disque dur virtuel
Avant de commencer
Spécifier le nom et l'emplacement
Spécifier la génération
Affecter la mémoire
Configurer la mise en réseau
Connecter un disque dur virtuel
Options d'installation
Résumé
Un ordinateur virtuel requiert un espace de stockage pour l'installation d'un système d'exploitation. Vous pouvez spécifier le stockage dès maintenant ou le configurer ultérieurement en modifiant les propriétés de l'ordinateur virtuel.
Créer un disque dur virtuel
Utilisez cette option pour créer un disque dur virtuel de taille dynamique (VHDX).
Nom :
dient_ad.vhdx
Emplacement :
C:\ProgramData\Microsoft\Windows\Virtual Hard Disks\
Parcourir...
Taille :
127
Go (Maximum : 64 To)
Utiliser un disque dur virtuel existant
Utilisez cette option pour attacher un disque dur virtuel VHDX existant.
Emplacement :
C:\ProgramData\Microsoft\Windows\Virtual Hard Disks\
Parcourir...
Attacher un disque dur virtuel ultérieurement
Utilisez cette option pour ignorer cette étape et attacher un disque dur virtuel existant ultérieurement.
< Précédent
Suivant >
Terminer
Annuler


Assistant Nouvel ordinateur virtuel
Options d'installation
Avant de commencer
Spécifier le nom et l'emplacement
Spécifier la génération
Affecter la mémoire
Configurer la mise en réseau
Connecter un disque dur virtuel
Options d'installation
Résumé
Vous pouvez installer un système d'exploitation maintenant si vous avez accès au média d'installation, ou vous pouvez l'installer ultérieurement.
Installer un système d'exploitation ultérieurement
Installer un système d'exploitation à partir d'un fichier image de démarrage
Média
Fichier image (.iso) :
F:\Win11_25H2_French_x64.iso
Parcourir...
Installer un système d'exploitation à partir d'un serveur d'installation réseau
< Précédent
Suivant >
Terminer
Annuler

13.1 : Adressage IP client_ad

Si pas d'IP fixe, une fois le rôle DHCP activé sur la VM AD, aller dans les paramètres > carte réseau > activé le rôle

Étape 14 : Arborescence AD

14.1 : Créer une unité organisation

Dans le gestionnaire de serveur, aller dans outils > utilisateurs et ordinateurs d'active directory

> clic droit sur le domaine > nouveau > unité organisation

14.2 : Créer groupe de sécurité (pour pouvoir ensuite appliquer des GPO)

Créer des utilisateurs sur l'UO dédiée. Il est important de créer les groupes de sécurité et les utilisateurs dans l'UO souhaitée pour pouvoir appliquer des GPO par la suite.

> clic droit sur l'UO > nouveau > groupe

Suivre les instructions (intuitives). On laissera les paramètres par défaut.

14.3 : Créer des utilisateurs

> clic droit sur l'UO > nouveau > utilisateur

On mettra ici : Pauline, Jérémy, Rachel

Suivre les instructions (intuitives)

14.4 : Ajouter des utilisateurs aux groupes

Ajouter des utilisateurs aux différents groupes crées

ici :

Pauline → COMPTABLES

Jérémy → IT

Rachel > RH

Étape 15 : Serveur RDS (nouvelle VM)

Pour cette Vm, allouer au minimum 300Go pour la suite

En premier lieu, renommer la VM (comme toute nouvelle vm ou PC).

Redémarrage du serveur

Joindre ensuite le serveur au domaine et lui attribuer une IP fixe comme la VM AD, ici IP= 192.168.26.3

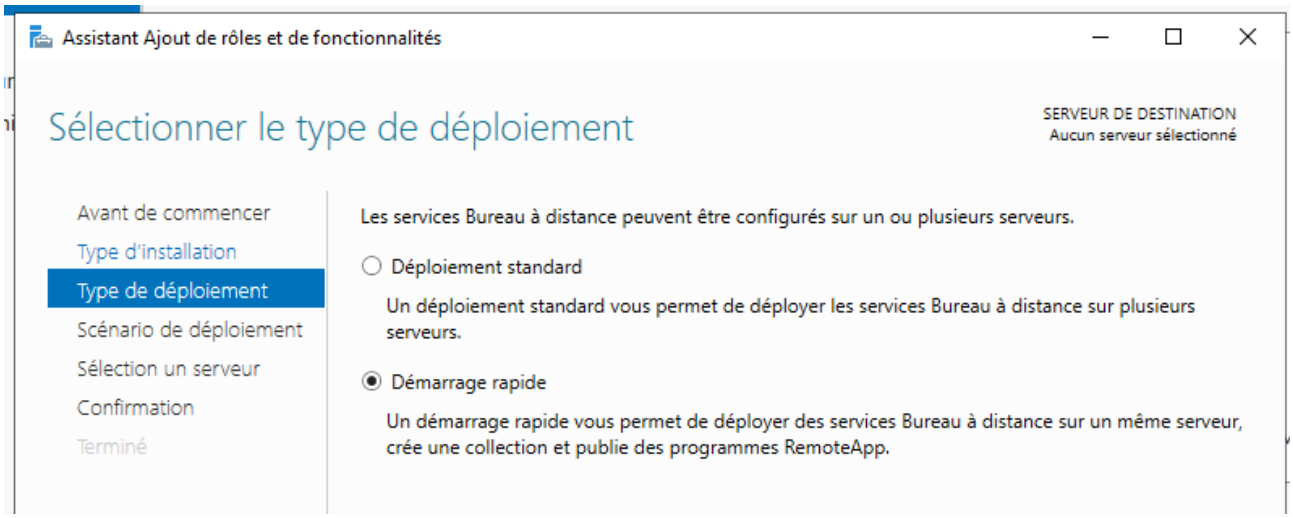
Pour le serveur DNS, on lui attribuera l'IP de la VM AD, soit 192.168.26.2

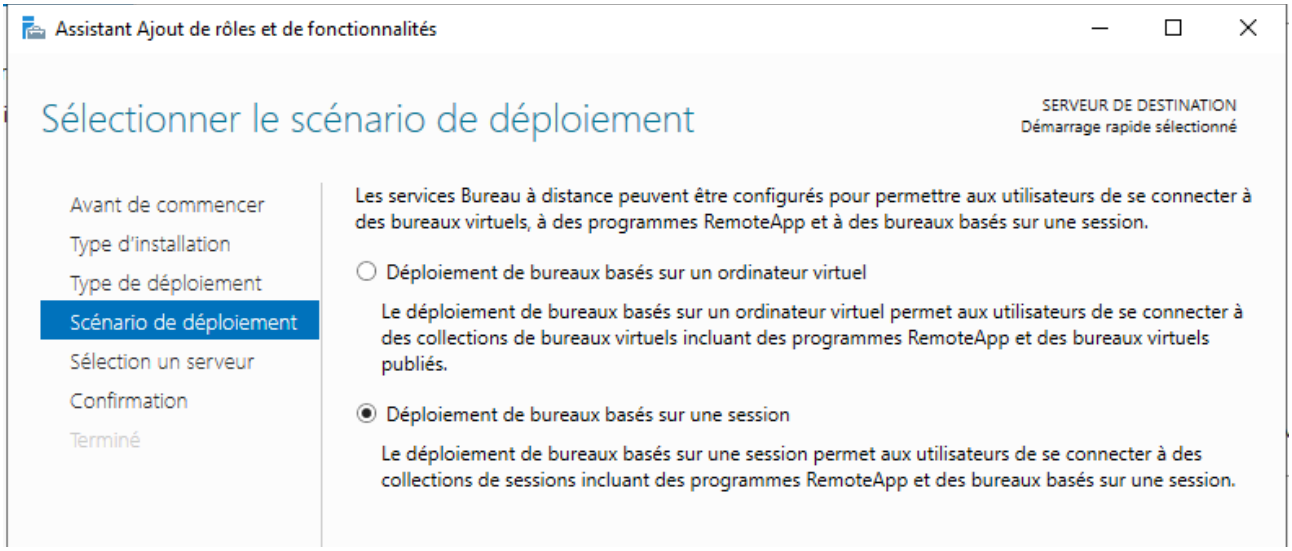
Redémarrer le serveur

Afin d'installer le rôle de bureau à distance, il faut se connecter en admin du domaine, pour cela se déconnecter de la session (de la VM RDP) > ajouter un utilisateur > entrer les identifiants de l'administrateur domaine (ad)

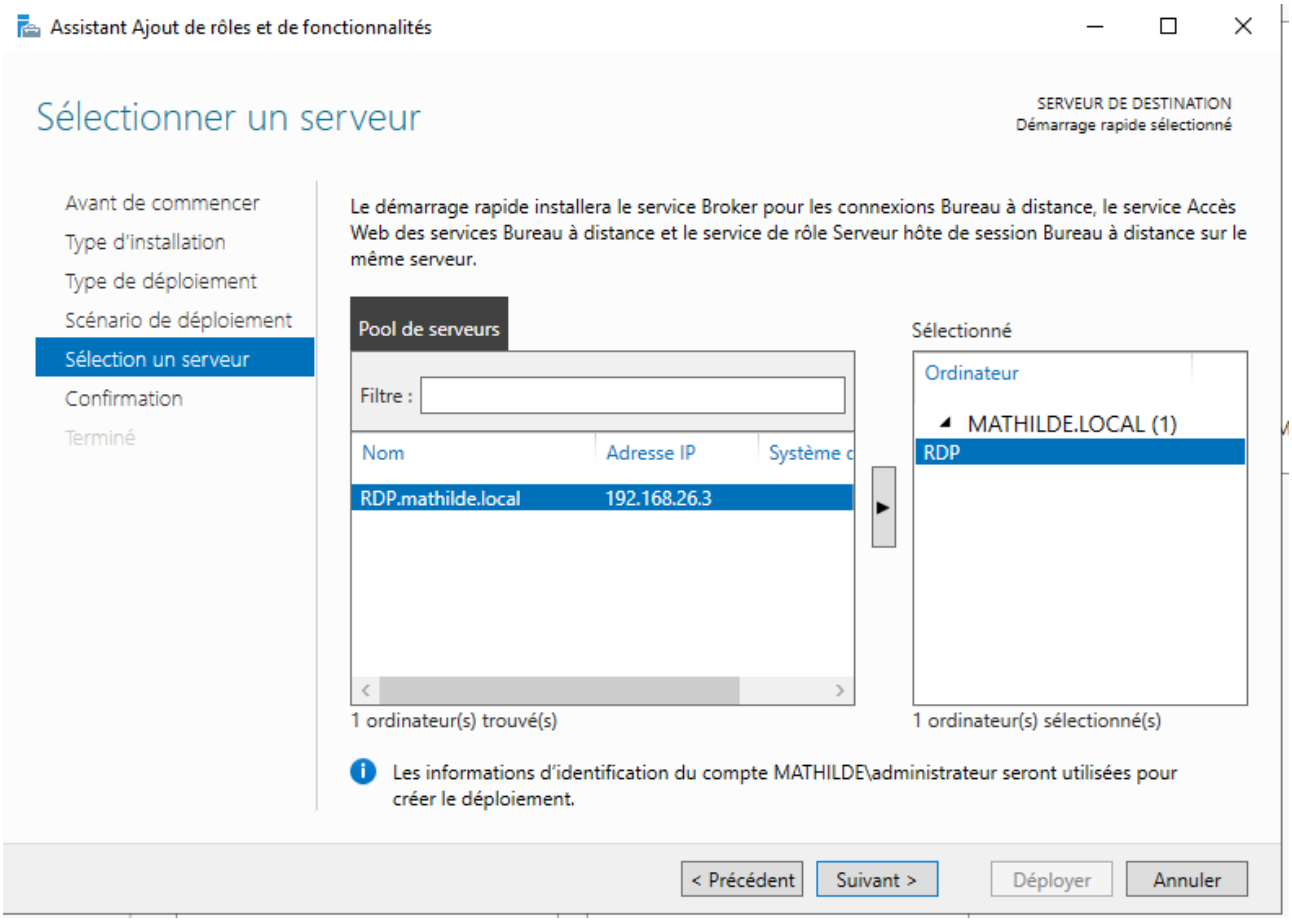
MATHILDE\Administrateur + mdp

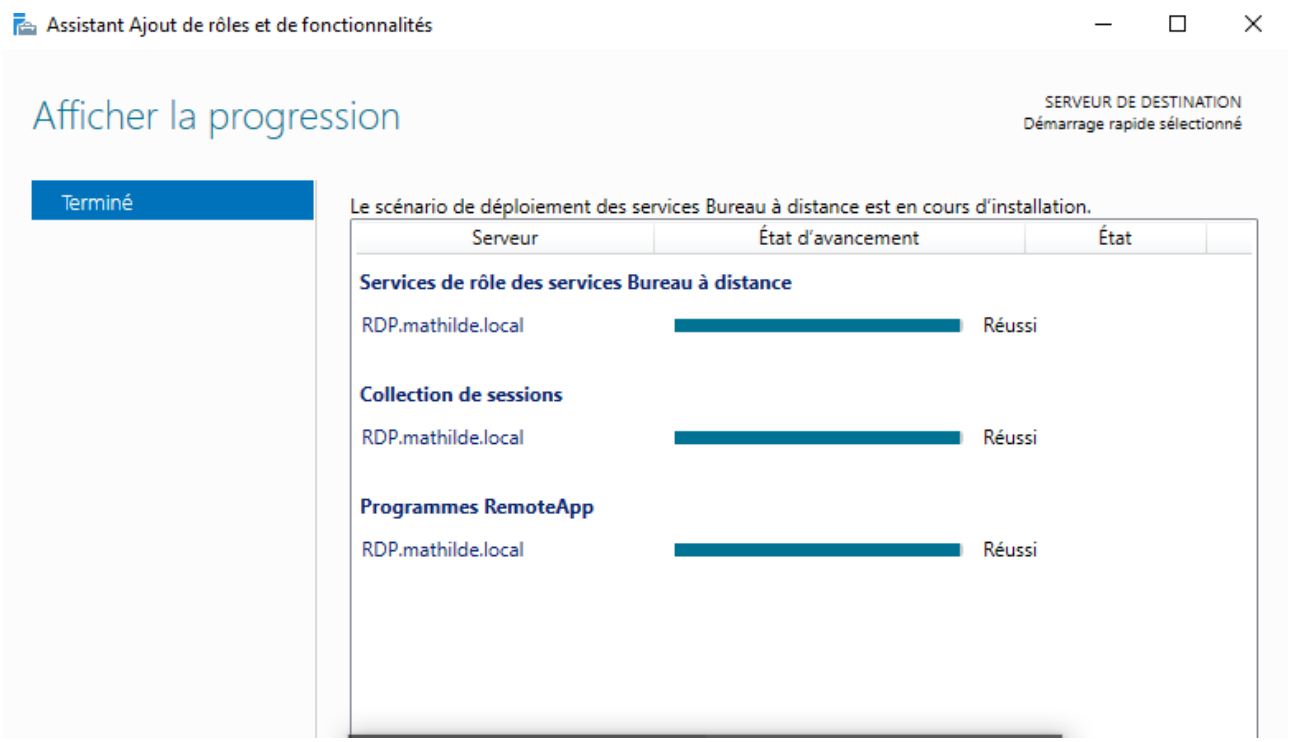
Dans le gestionnaire de serveur > gérer > ajout de rôles et fonctionnalités > installation des services de bureau à distance > démarrage rapide > déploiement de bureau basés sur une session.



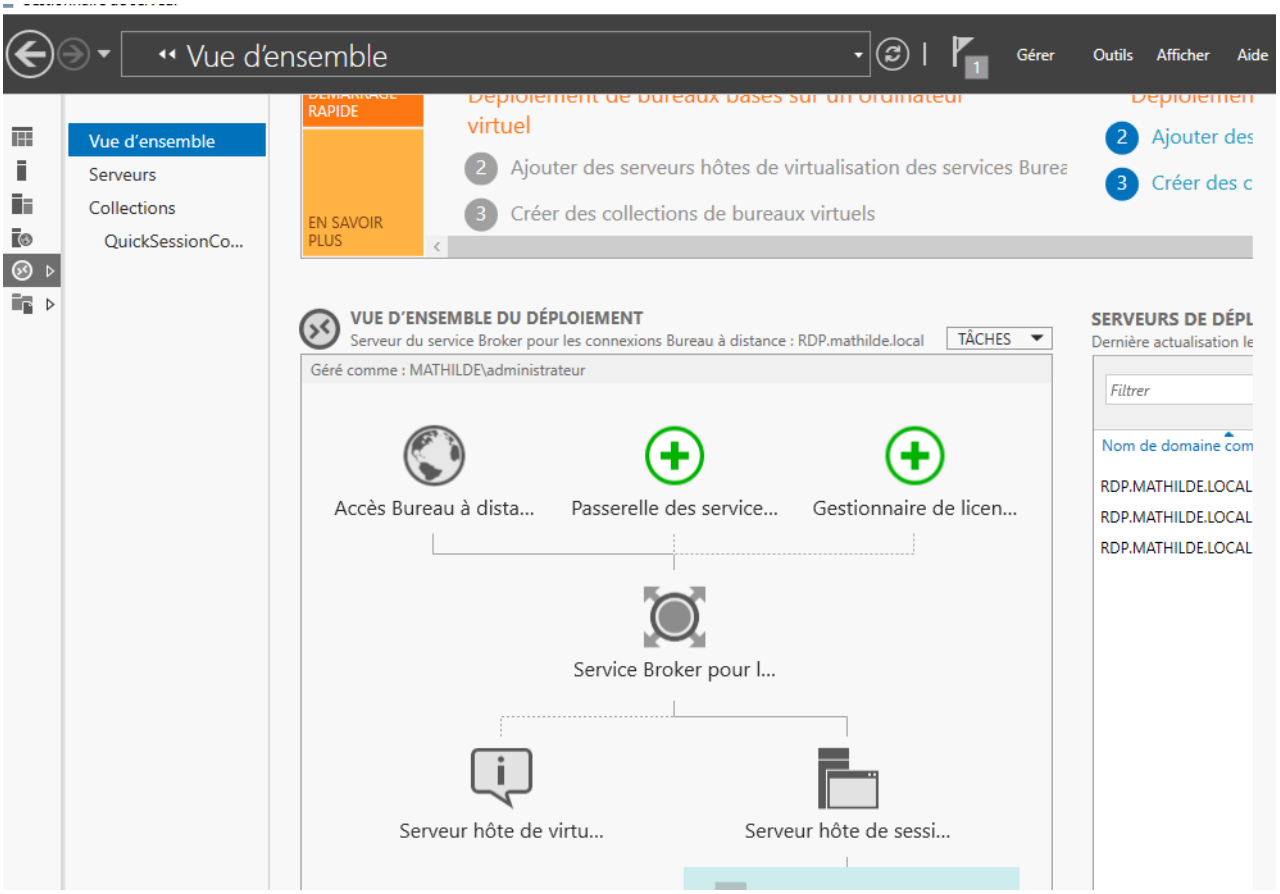

Assistant Ajout de rôles et de fonctionnalités
Sélectionner le scénario de déploiement
SERVEUR DE DESTINATION
Démarrage rapide sélectionné
Avant de commencer
Type d'installation
Type de déploiement
Scénario de déploiement
Sélection un serveur
Confirmation
Terminé
Les services Bureau à distance peuvent être configurés pour permettre aux utilisateurs de se connecter à des bureaux virtuels, à des programmes RemoteApp et à des bureaux basés sur une session.
Déploiement de bureaux basés sur un ordinateur virtuel
Le déploiement de bureaux basés sur un ordinateur virtuel permet aux utilisateurs de se connecter à des collections de bureaux virtuels incluant des programmes RemoteApp et des bureaux virtuels publiés.
Déploiement de bureaux basés sur une session
Le déploiement de bureaux basés sur une session permet aux utilisateurs de se connecter à des collections de sessions incluant des programmes RemoteApp et des bureaux basés sur une session.

> suivant


Assistant Ajout de rôles et de fonctionnalités
Sélectionner un serveur
SERVEUR DE DESTINATION
Démarrage rapide sélectionné
Avant de commencer
Type d'installation
Type de déploiement
Scénario de déploiement
Sélection un serveur
Confirmation
Terminé
Le démarrage rapide installera le service Broker pour les connexions Bureau à distance, le service Accès Web des services Bureau à distance et le service de rôle Serveur hôte de session Bureau à distance sur le même serveur.
Pool de serveurs
Filtre :
Nom
Adresse IP
Système d
RDP.mathilde.local
192.168.26.3
1 ordinateur(s) trouvé(s)
Sélectionné
Ordinateur
MATHILDE.LOCAL (1)
RDP
1 ordinateur(s) sélectionné(s)
Les informations d'identification du compte MATHILDE\administrateur seront utilisées pour créer le déploiement.
< Précédent
Suivant >
Déployer
Annuler



Dans le gestionnaire de serveur, dans services Bureau à distance, la fenêtre ci-dessous doit apparaître.



Une fois tous les « services » (brocker, web ...) installées pour le rdp, hors mode labo pour les licences, se rendre dans outil d'administration > gestionnaire de licence > se connecter au serveur

Ici en mode labo donc pas besoin

15.1 : Collection

Pour pouvoir faire une collection, il faut d'abord créer un dossier de partage.

Si pas d'espace disque suffisant dans la vm :

> aller sur le serveur > gestionnaire hyper-v > clic droit sur la vm > propriété > étendre le disque. Cela permettra d'avoir un espace non-alloué qui sera utilisé par la suite.

Ou directement

→ Retour sur la vm avec le serveur RDS , aller dans gestionnaire de disque, sur la partie non-allouée > clic droit > nouveau volume.

Dans ce volume , créer un dossier , ici il s'appellera « RDSprofiles ».

Droit de partage

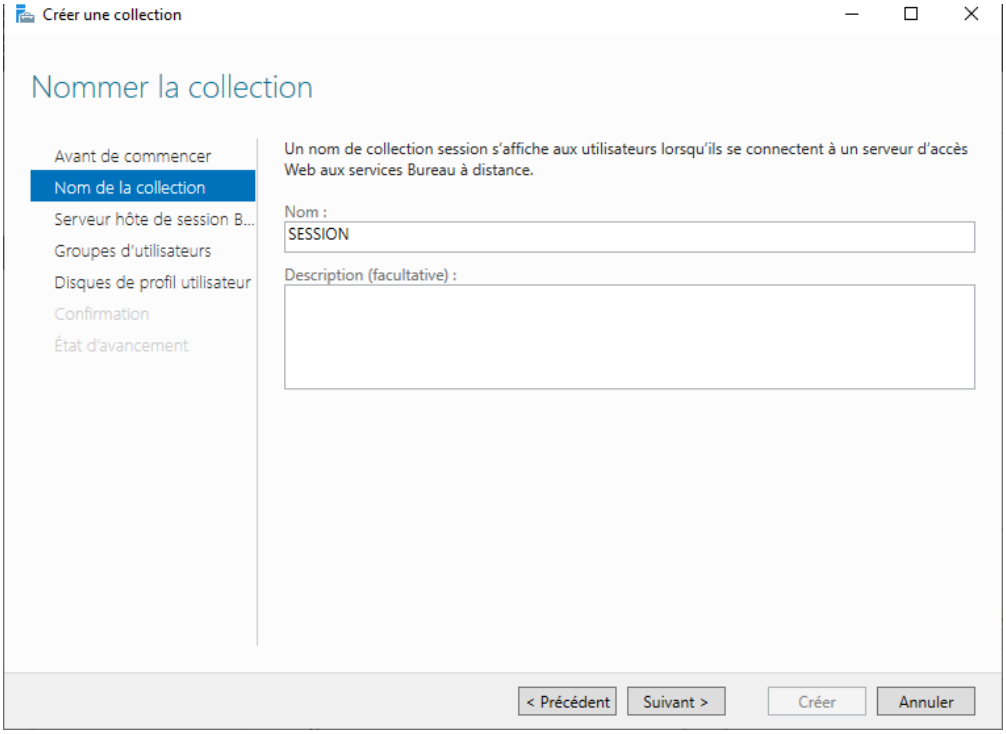
> clic droit sur RDSprofiles > propriétés

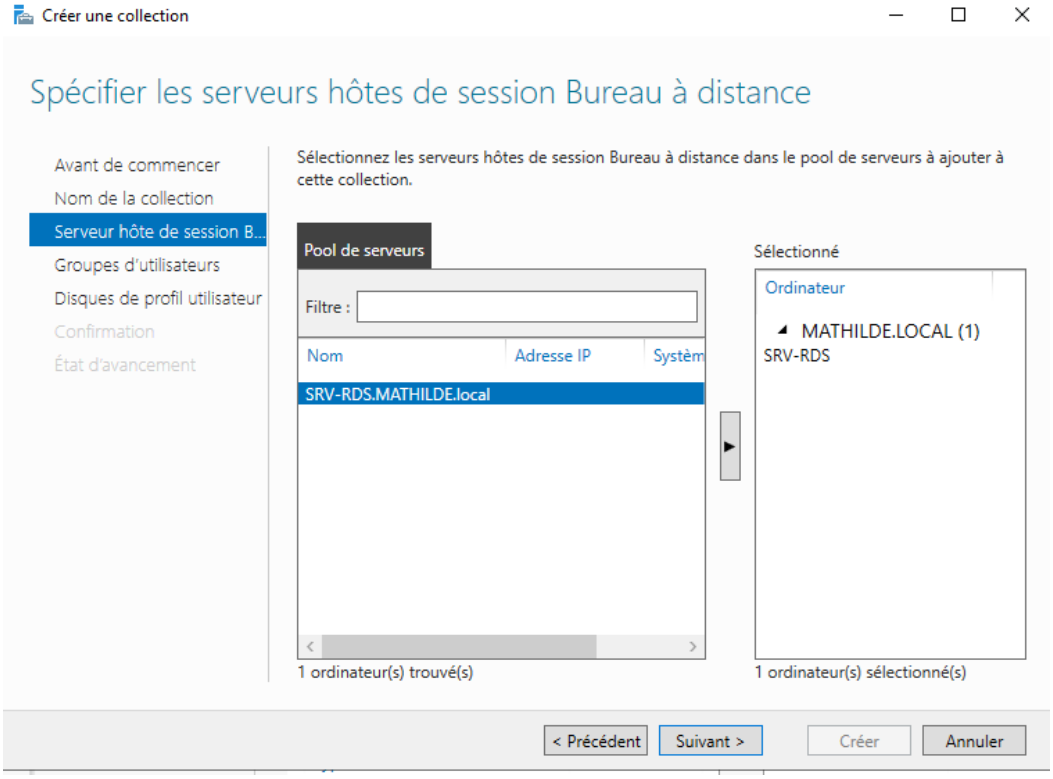
Dans l'onglet « partage », clic sur partage > partager le dossier (choisir les utilisateurs)

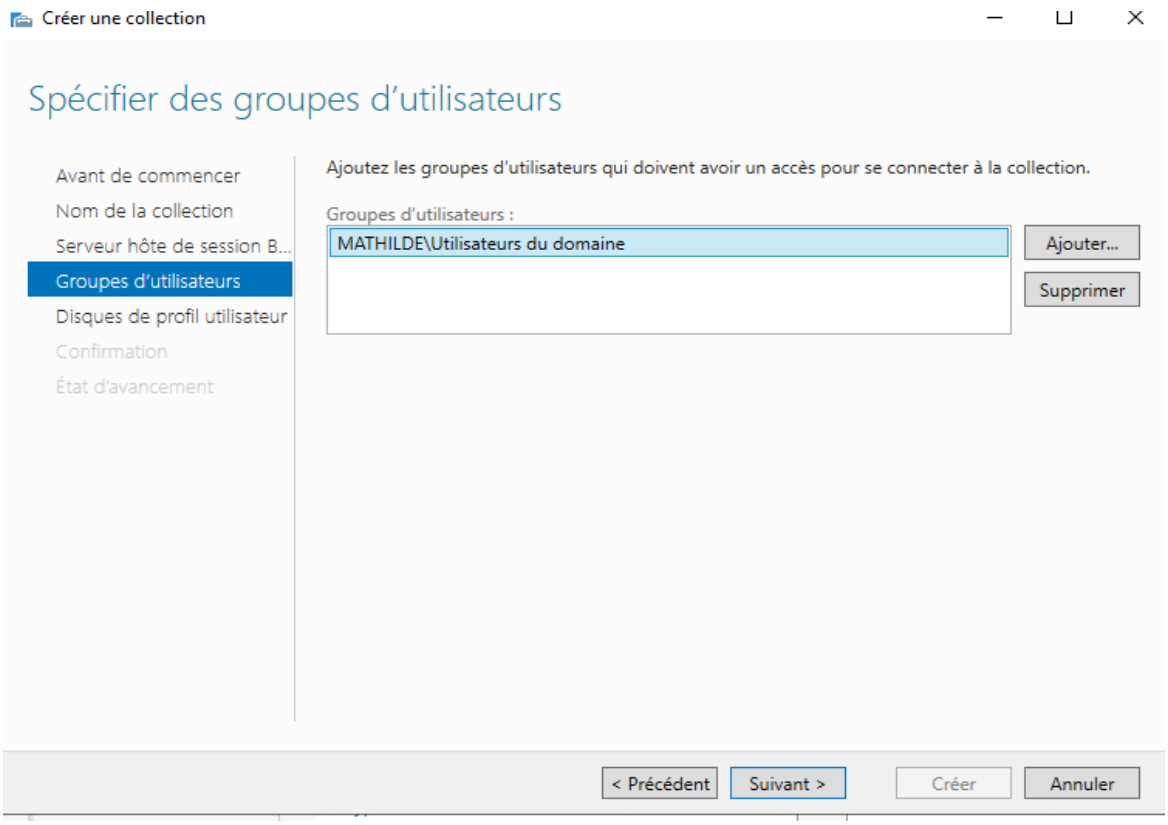
En bas dans « partage avancé » > autorisation > mettre admin + les groupes qui pourront accéder au serveur

Pour la collection, on supprimera celle existante.

Dans Collections > tâches > créer une collection de session


Créer une collection
Nommer la collection
Avant de commencer
Nom de la collection
Serveur hôte de session B...
Groupes d'utilisateurs
Disques de profil utilisateur
Confirmation
État d'avancement
Un nom de collection session s'affiche aux utilisateurs lorsqu'ils se connectent à un serveur d'accès Web aux services Bureau à distance.
Nom :
SESSION
Description (facultative) :
< Précédent
Suivant >
Créer
Annuler


Créer une collection
Spécifier les serveurs hôtes de session Bureau à distance
Avant de commencer
Nom de la collection
Serveur hôte de session B...
Groupes d'utilisateurs
Disques de profil utilisateur
Confirmation
État d'avancement
Sélectionnez les serveurs hôtes de session Bureau à distance dans le pool de serveurs à ajouter à cette collection.
Pool de serveurs
Filtre :
Nom
Adresse IP
Systèm
SRV-RDS.MATHILDE.local
1 ordinateur(s) trouvé(s)
Sélectionné
Ordinateur
MATHILDE.LOCAL (1)
SRV-RDS
1 ordinateur(s) sélectionné(s)
< Précédent
Suivant >
Créer
Annuler



Pour la partie suivante « disques de profil utilisateur », renseigner le chemin du dossier **RDSprofiles** et indiquer la taille de disque de sessions souhaités. Ici on laissera par défaut : 20

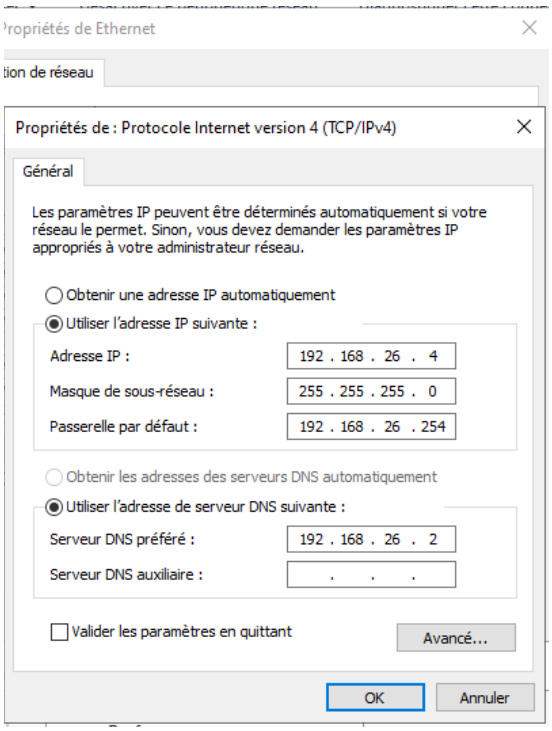
Aller sur la collection créée > tâches > modifier les propriétés > appliquer

Pour vérifier si la connexion à distance fonctionne, se connecter via un autre utilisateur du domaine

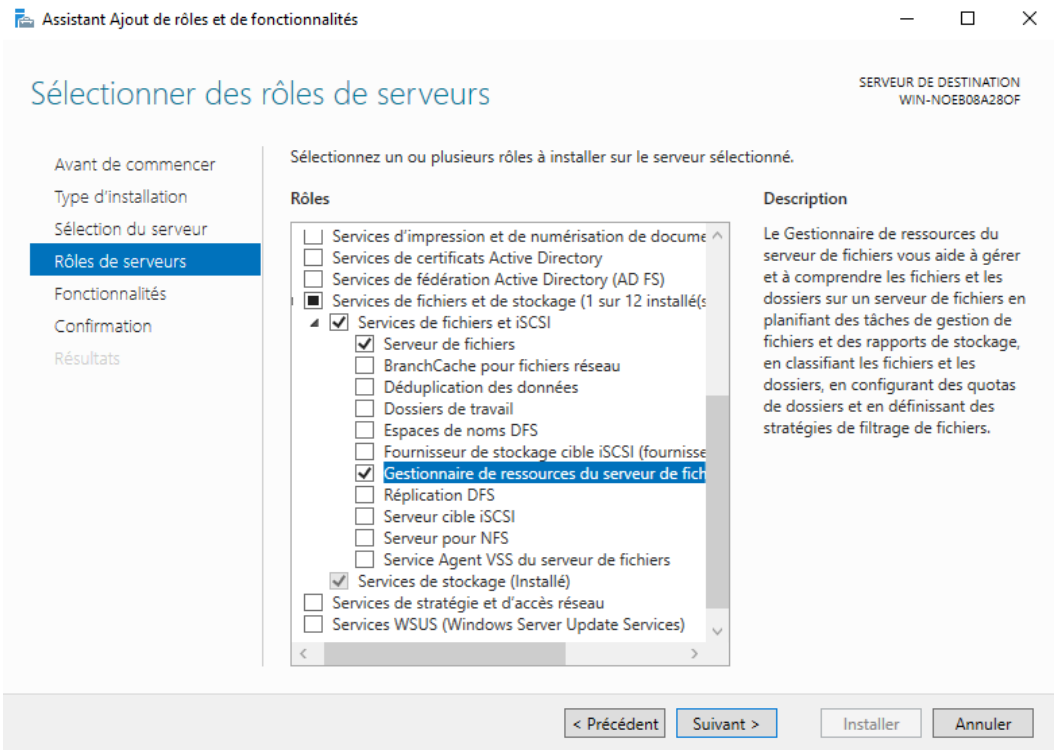
Étape 16 : Système de fichiers

> Créer une nouvelle vm pour le rôle

- renommer la vm
- joindre la vm au domaine
- attribuer une ip fixe à la vm (192.168.26.4) ; DNS = IP AD (192.168.26.2)



Dans « gérer », aller dans « ajouts de rôles et de fonctionnalités » > ajouter « gestionnaire de ressources du serveur de fichier »



17.1 : Dossier partagé

Pour créer un dossier partagé, il faut un espace disque dédié avec un dossier et ses sous dossiers correspondants aux différences services.

Toujours sur le serveur de fichier, dans le menu Winodws, taper gestionnaire de disques. Une fois dans le gestionnaire pour allouer un disque pour les données, sur la partie non-allouée > clic droit > nouveau volume.

Ensuite, avec les groupes de sécurités crées dans l'AD, la gestion des droits de partages et droits NTFS est possible.

Droit de Partage

Sur le nouveau disque (datas) > créer un dossier principal qui regroupera les groupes de sécurité (correspondant / en relation) avec l'AD.

Dossier principal (**PARTAGE**) : droit de partage = tout le monde. Clic droit sur le dossier > propriétés. Dans l'onglet « partage », aller dans « partage avancé » et cocher la case « partager ce dossier »

Dans « autorisations » en bas à gauche, laisser « tout le monde » en écriture/lecture. On ne met pas contrôle total pour des raisons de sécurité.

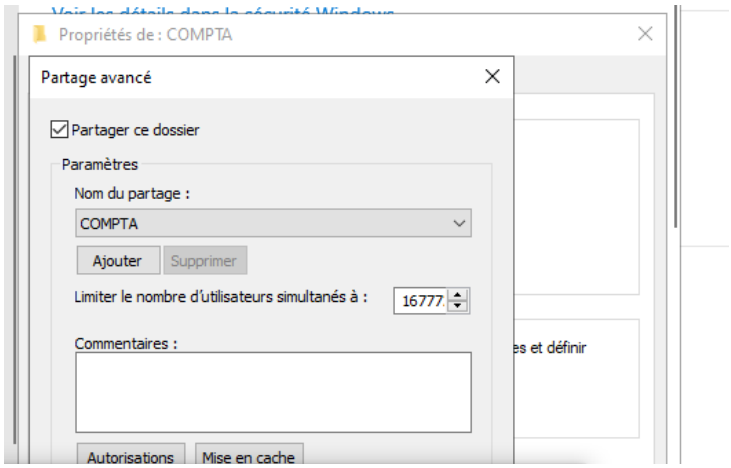
> cliquer sur « appliquer » puis ok

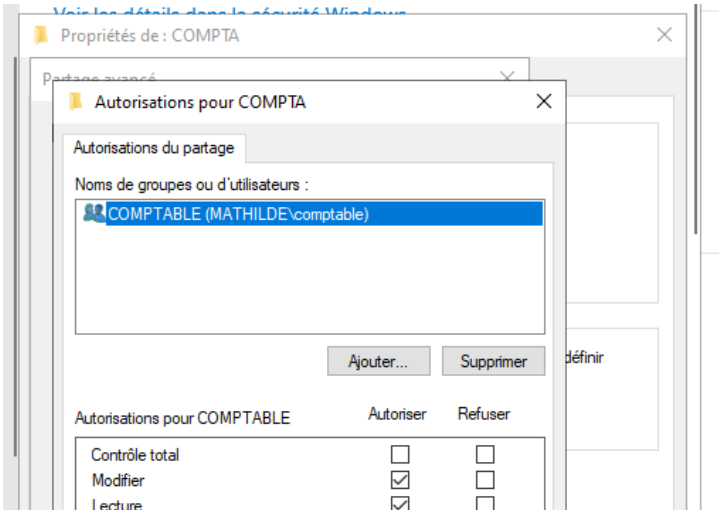
> cliquer une nouvelle fois sur « appliquer » puis ok

Sous dossier

Répéter la même procédure pour chaque sous dossier en remplaçant « tout le monde » par le groupe de sécurité correspondant au sous dossier. On laissera en écriture/lecture

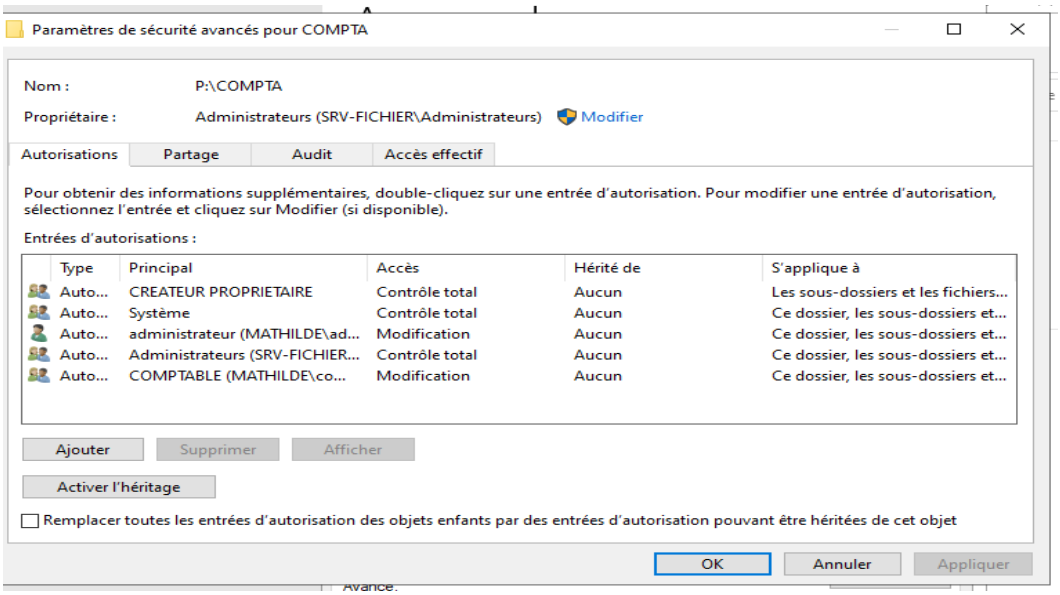
EX : sous dossier COMPTA





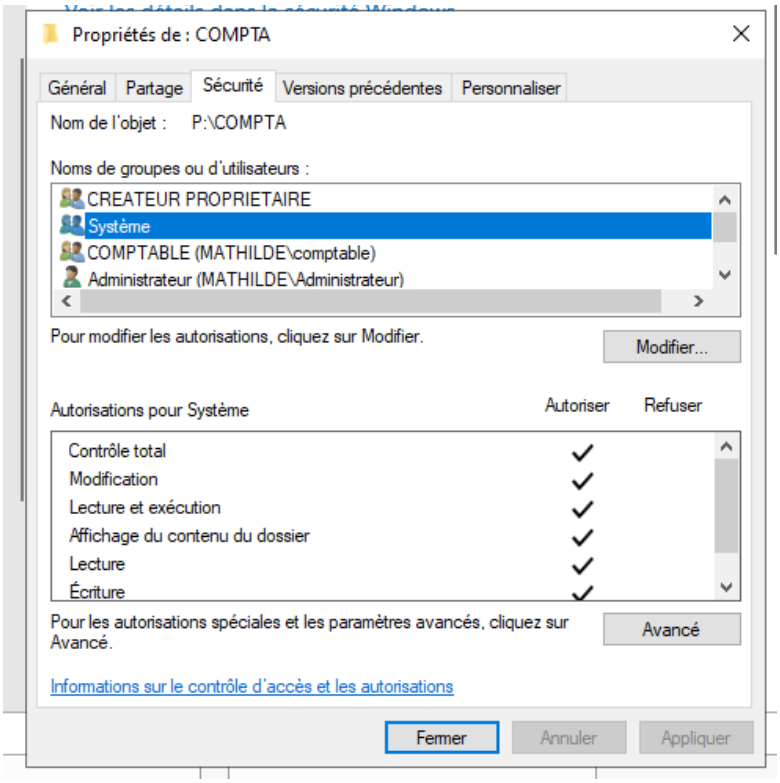
Droit NTFS

Afin d'appliquer des droits NTFS, il faut désactiver l'héritage. Pour cela, toujours dans les propriétés, aller dans l'onglet « sécurité » > avancé > désactiver l'héritage > convertir les autorisations héritées en autorisations explicites sur cet objet



Sous dossiers

Toujours dans les propriétés, dans l'onglet sécurité > supprimer tous les comptes « utilisateurs » même admin, rajouter le groupe de sécurité correspondant + administrateur utilisateur



Pour le système, CREATEUR PROPRIETAIRE et l'administrateur SRV = contrôle total

Pour le groupe de sécurité et l'administrateur utilisateur = tout sauf contrôle total

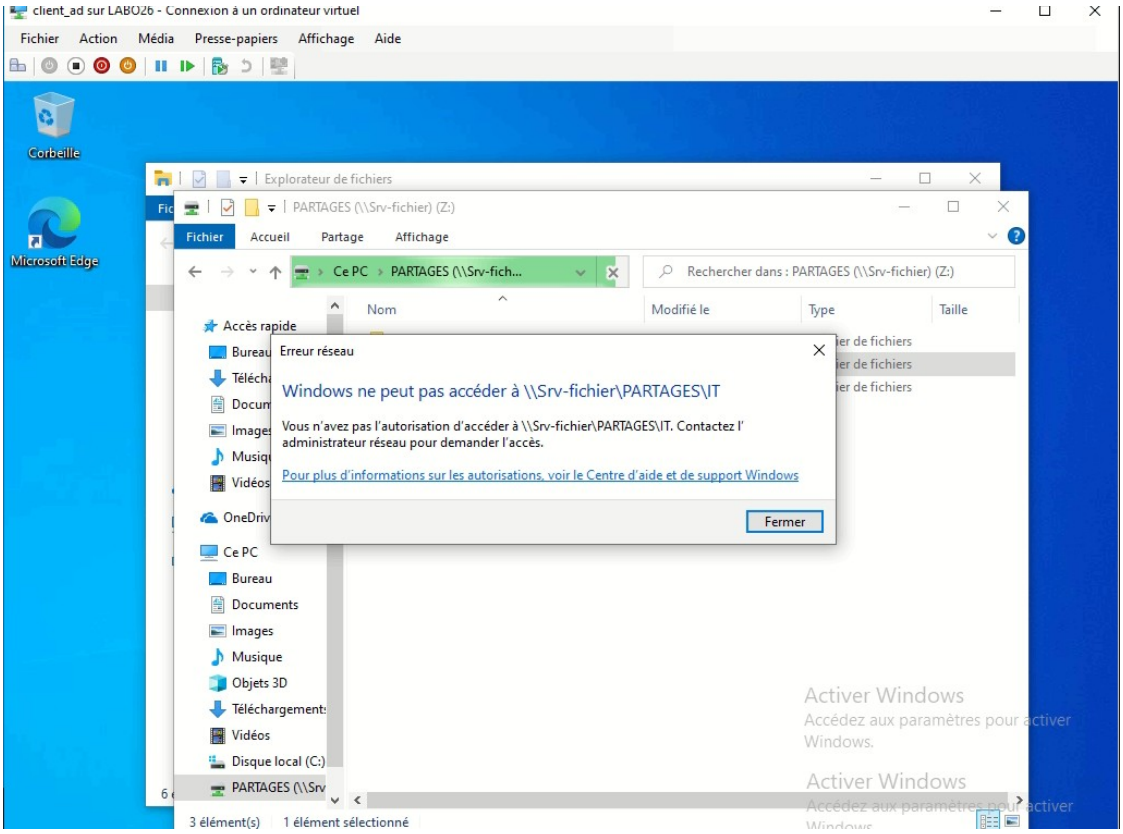
TEST :

sur la VM cliente > se connecter à un utilisateur du domaine.

Dans l'explorateur de fichier > clic droit sur ce PC > connecter un lecteur réseau > mettre le chemin du dossier de partages. Ici : \\SRV-FICHIER\PARTAGES

Le dossier de partages apparaît. Ici, l'utilisateur fait parti du groupe de sécurité COMPTA et ne peux accéder au dossier IT.

Les droits et autorisations sont appliqués.



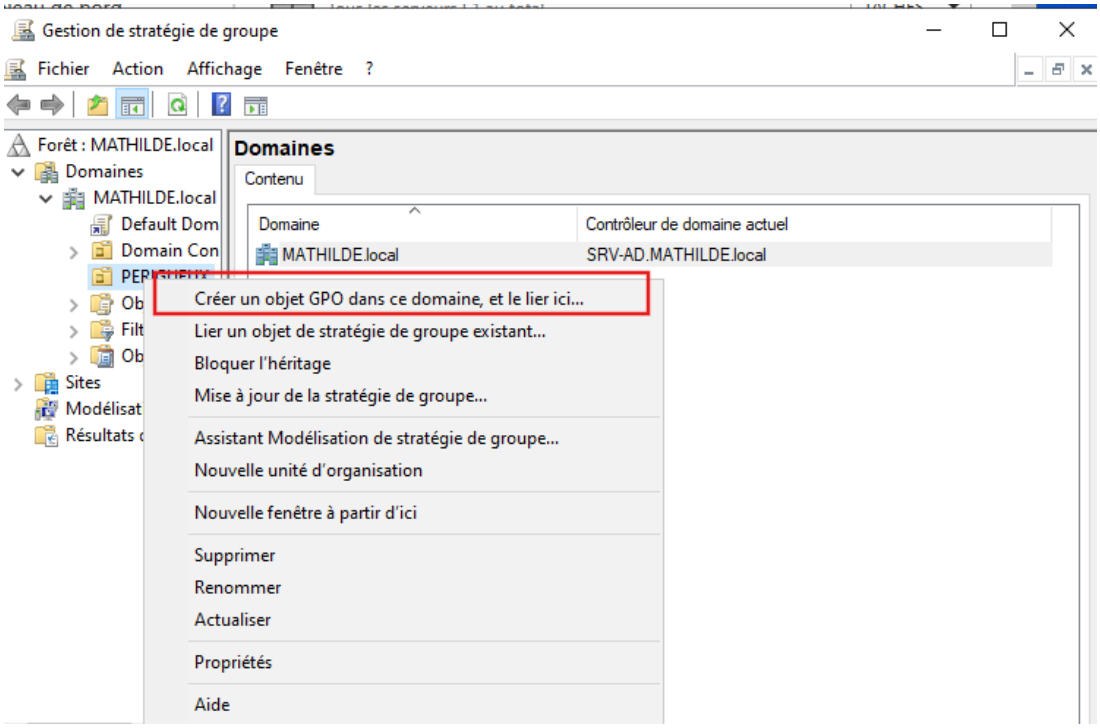
Étape 18 : GPO / Mappage du dossier partagé

Pour monter le dossier partagé sur les autres utilisateurs du domaine, on va faire une GPO. Aller dans outils > gestion de stratégie locale.

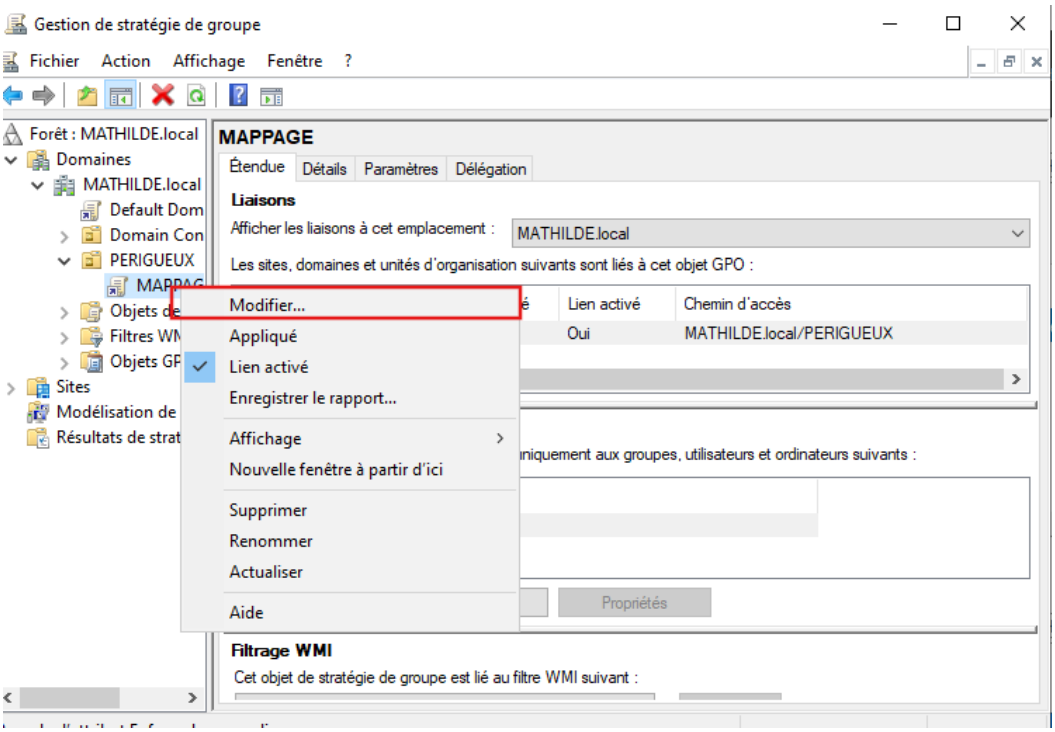
Se placer sur le domaine (à droite) puis sur l'UO souhaitée.

Clic droit > créer une GPO dans ce domaine et le lier ici > Nommer la GPO

Ici : **MAPPAGE**

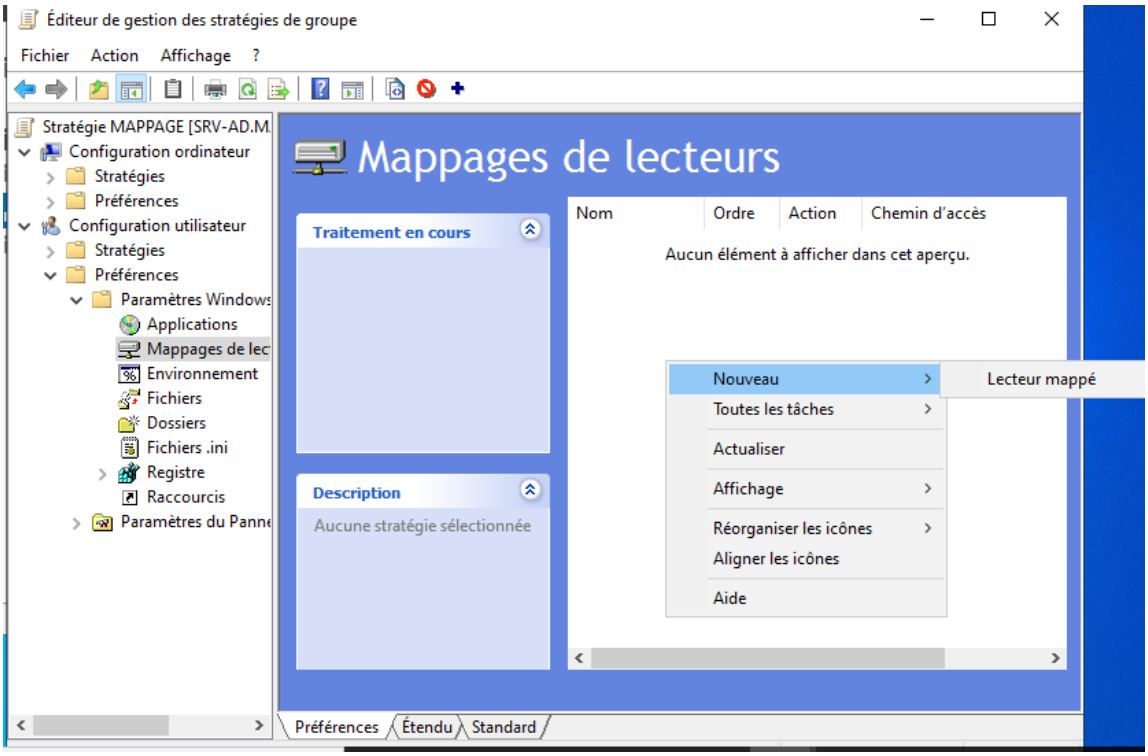


Une fois la GPO créée > clic droit dessus > modifier

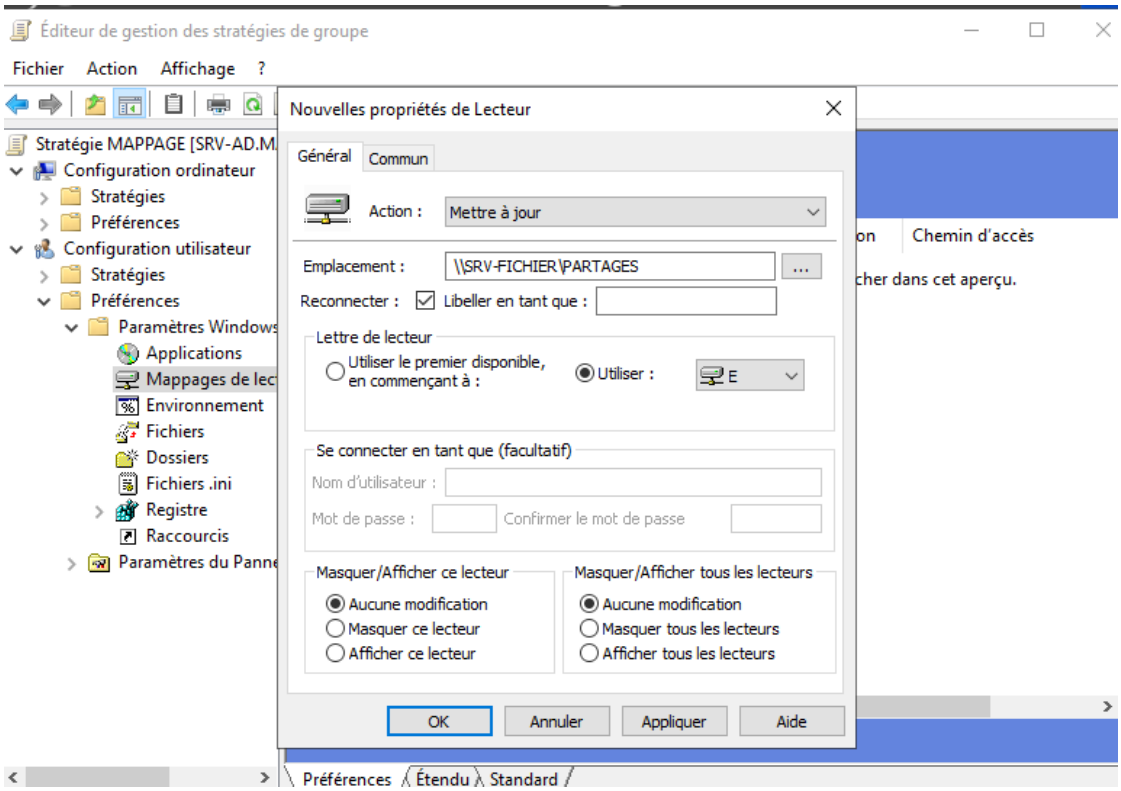


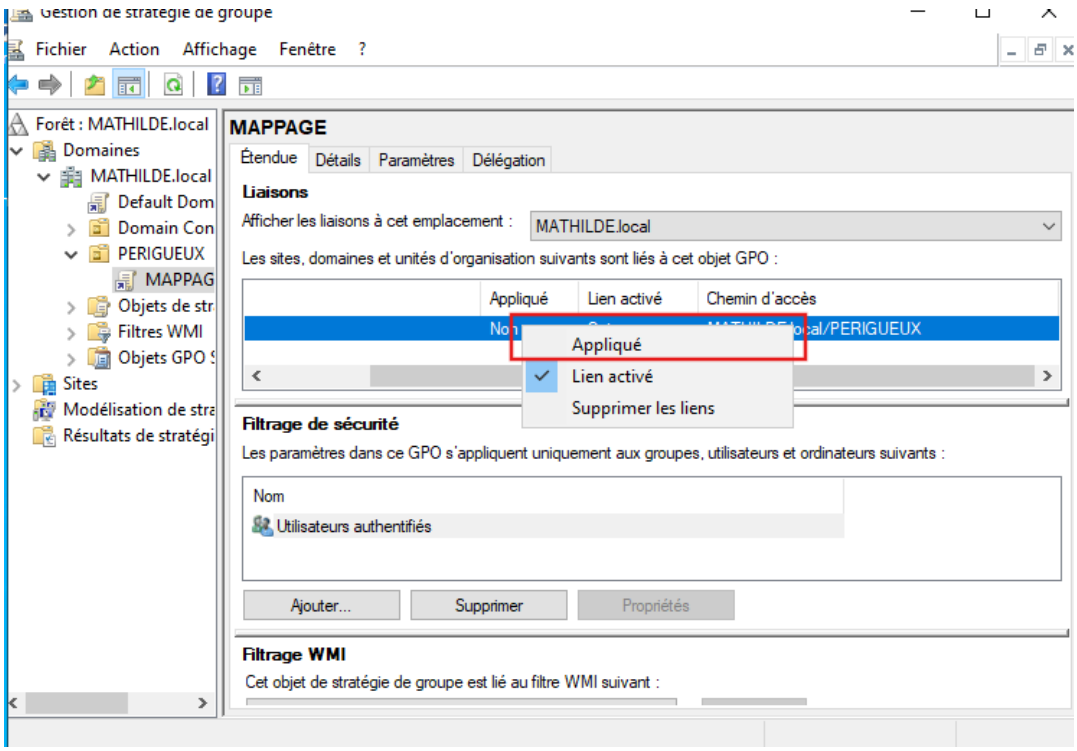
Aller ensuite dans configurations utilisateurs > préférences > paramètres Windows > Mappage de lecteurs.

Clic droit sur la zone vide > nouveau > lecteur mappé



Dans la fenêtre ouvrante, cocher reconnecter si le lecteur doit être permanent. Ici on cochera la case. Dans l'onglet « commun », vérifier que tout soit décocher.





> aller dans la console et forcer la GPO. Taper : **gpupdate /force**

Connecter le pc à un utilisateur du domaine, le dossier partagé sera présent.

Étape 19 : Routeur pfSense

Pré-requis :

- 2 cartes réseaux (WAN, LAN)
- ISO pfSense
- vm pour pfSence

Pour une meilleure sécurité, il faut cloisonner le réseau. Pour cela, connecter une autre carte réseau qui sera spéciale pour le routeur.

a) Carte réseau pfSence

Dans le gestionnaire hyper-v > gestionnaire de commutateur virtuel

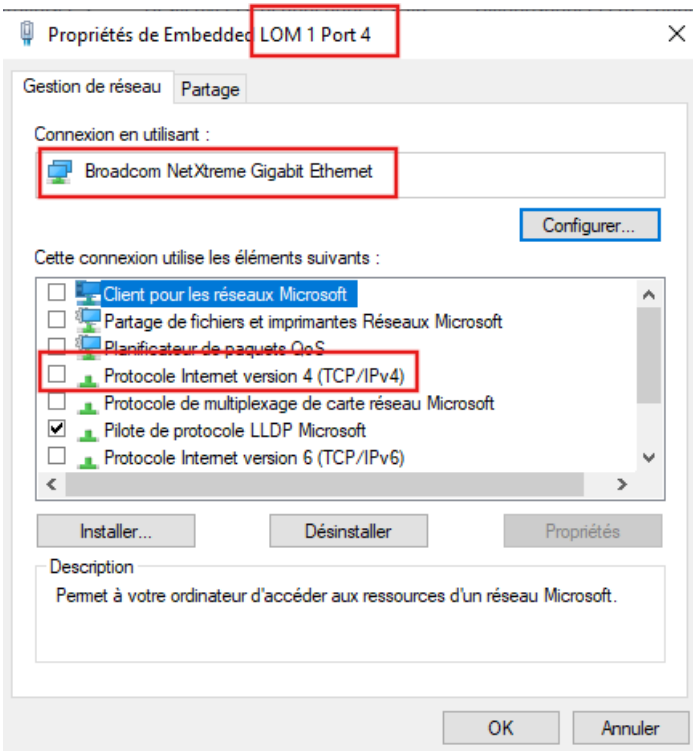
Choisir le type : externe > créer un nouveau commutateur virtuel. Lui associer la nouvelle carte réseau. (pour savoir la bonne, se rendre dans centre de réseau et partage et regarder au port correspondant).

Cocher « autoriser l'OS a partagé cette carte »

Ici, on l'appellera WANpfSense.

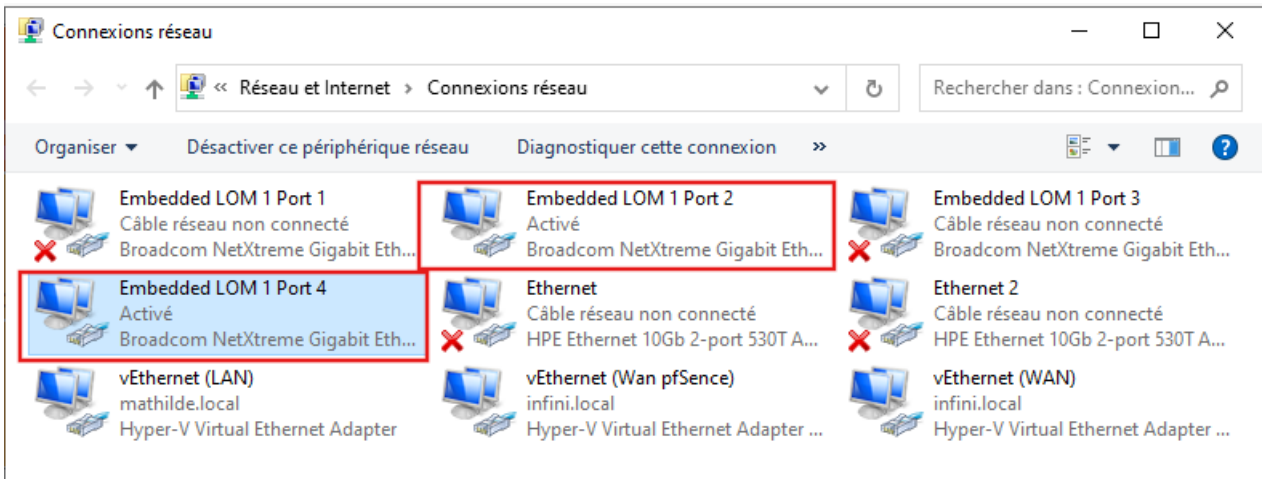
b) IP

Dans le centre de réseau et de partage du serveur physique, s'assurer dans les propriétés de la carte réseau correspondante (la deuxième qui n'a pas de croix rouge pour le routeur) ait le DHCP IPV4 **désactivé**. Il ne faut pas laisser le PC lui attribuer une IP, c'est pfSense qui va s'en occuper.

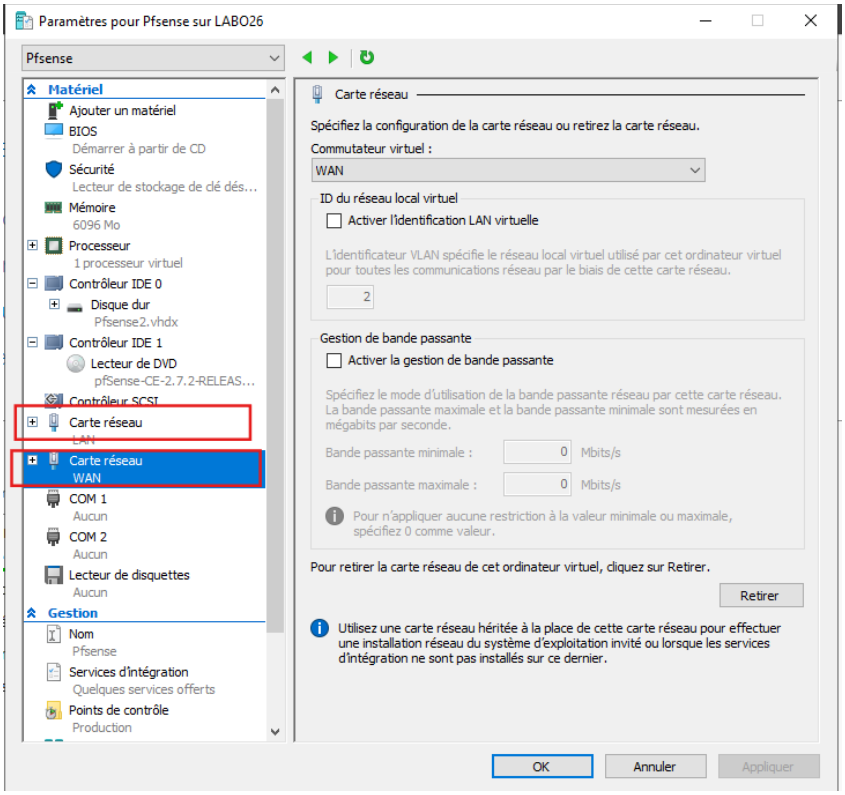


Le statut de la carte doit passer en « activé »

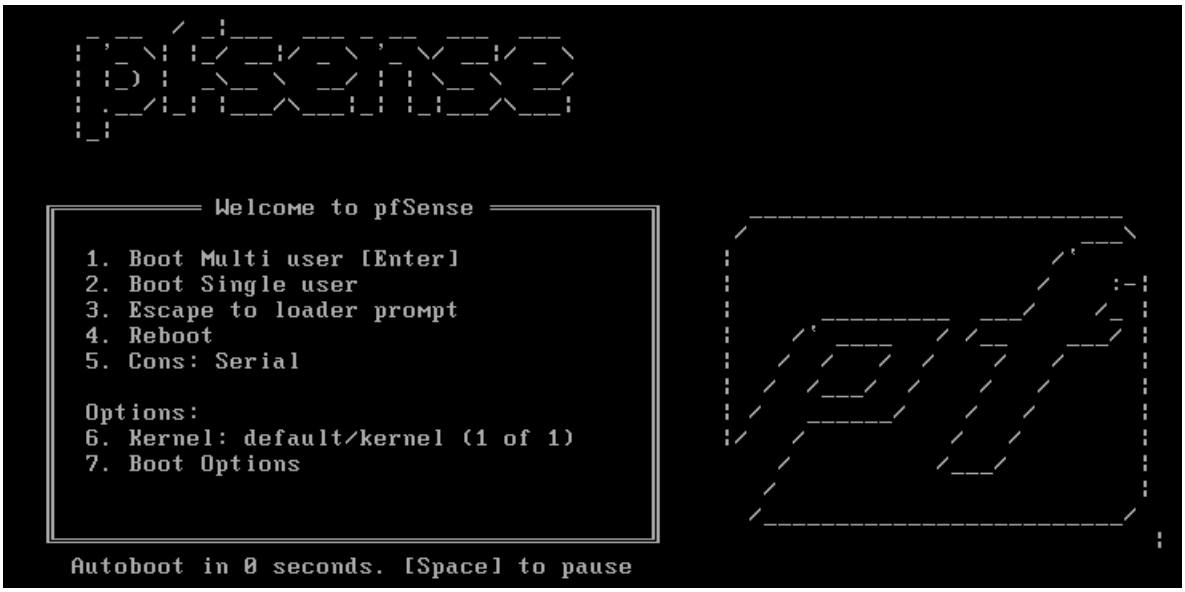
Ici, la carte WANpfSence correspond au LOM 1 port 4

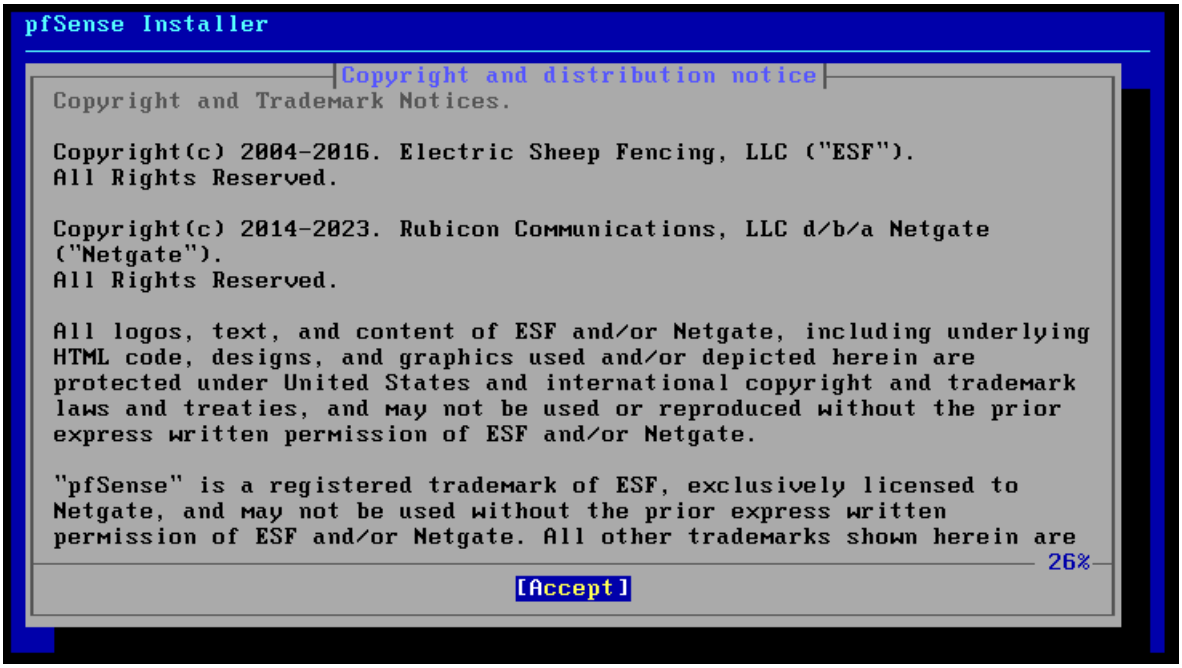


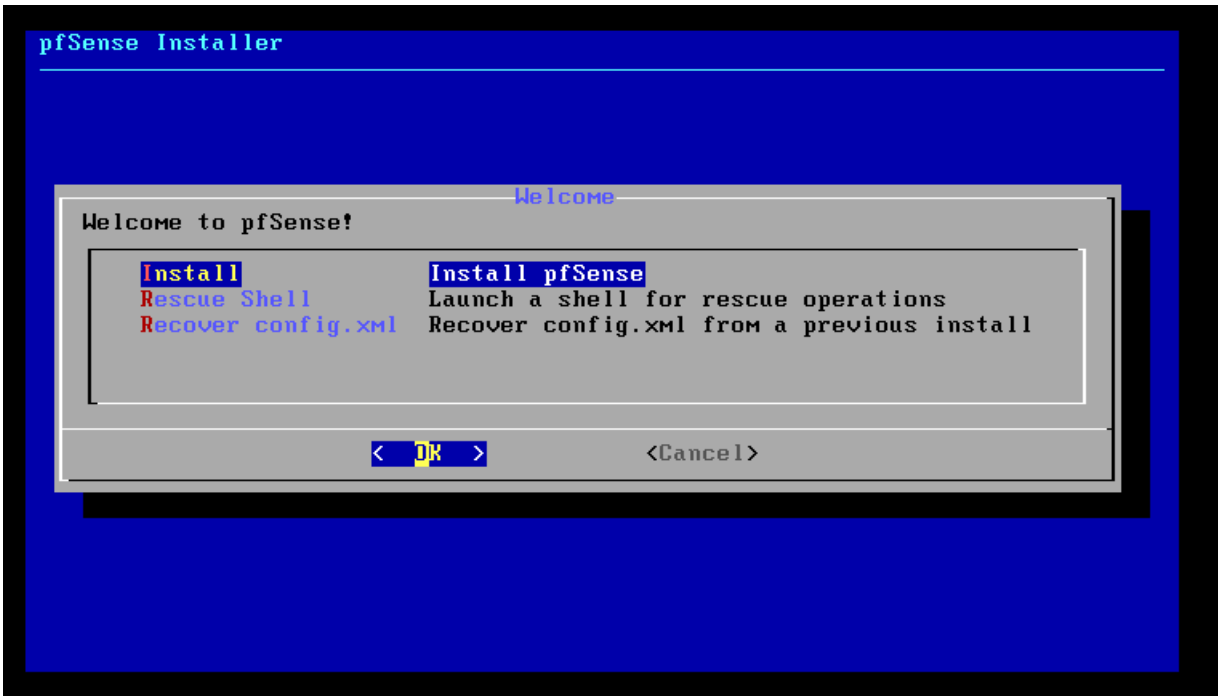
Une fois la carte réseau spéciale pfSense ajoutée dans le gestionnaire des commutateurs et ajoutée sur la vm pfSence (vm éteinte)ainsi que la carte LAN (commutateur en interne)

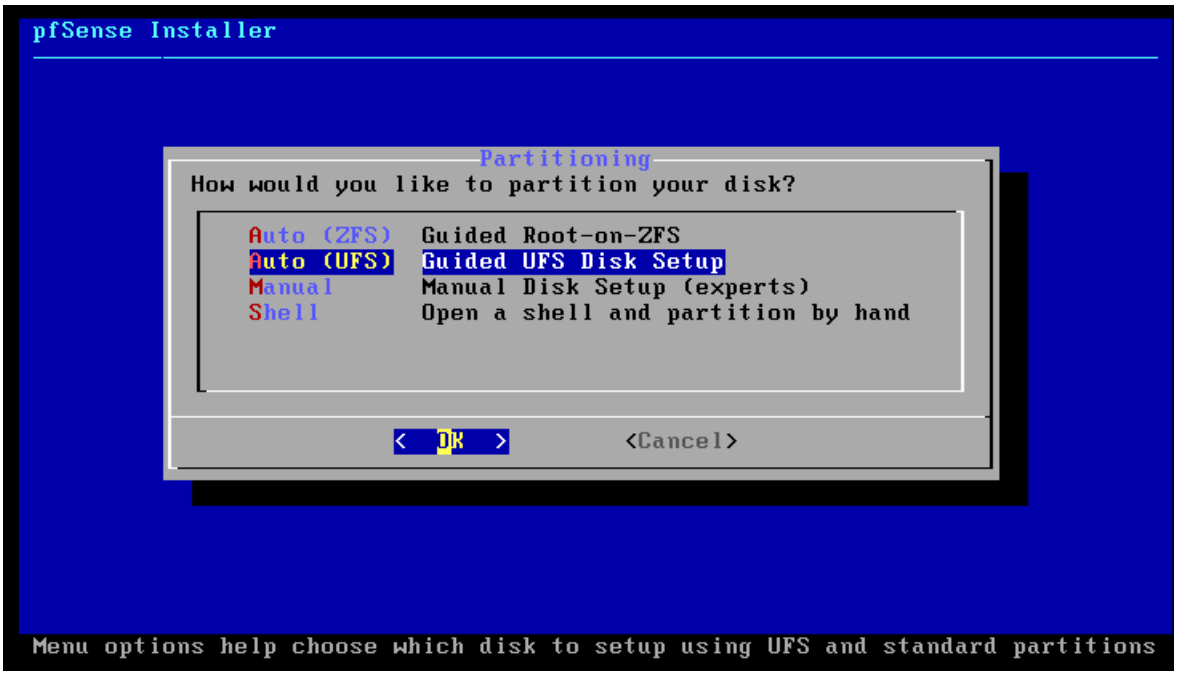


> lancer le démarrage de la VM

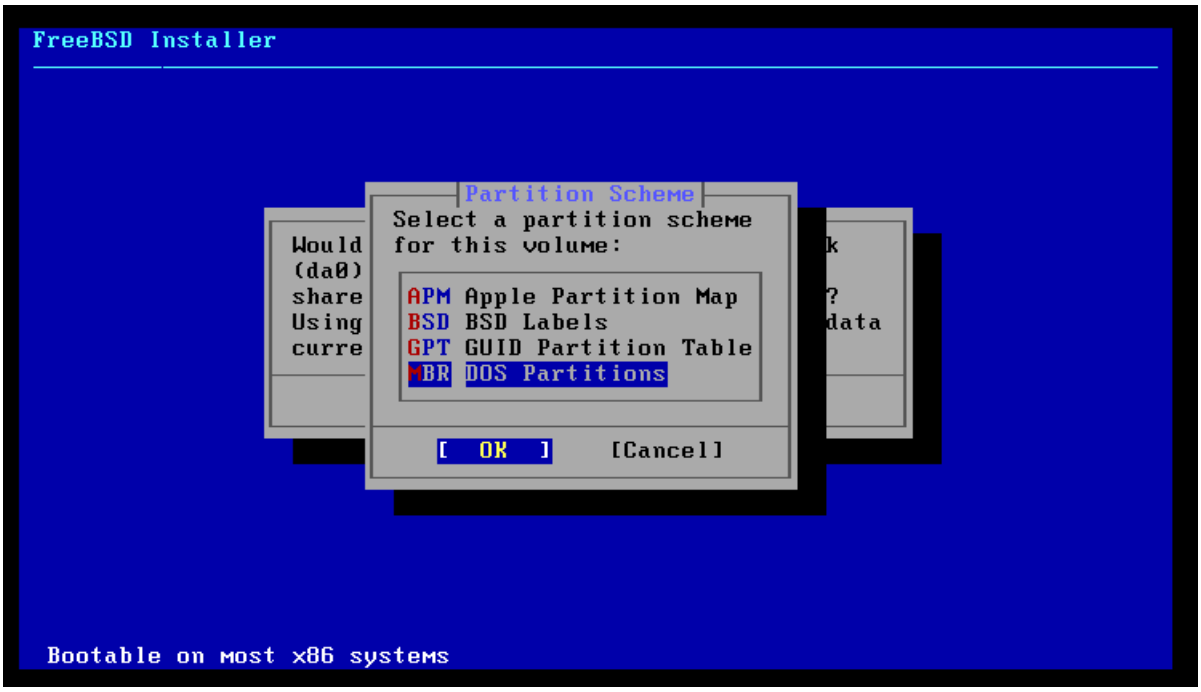


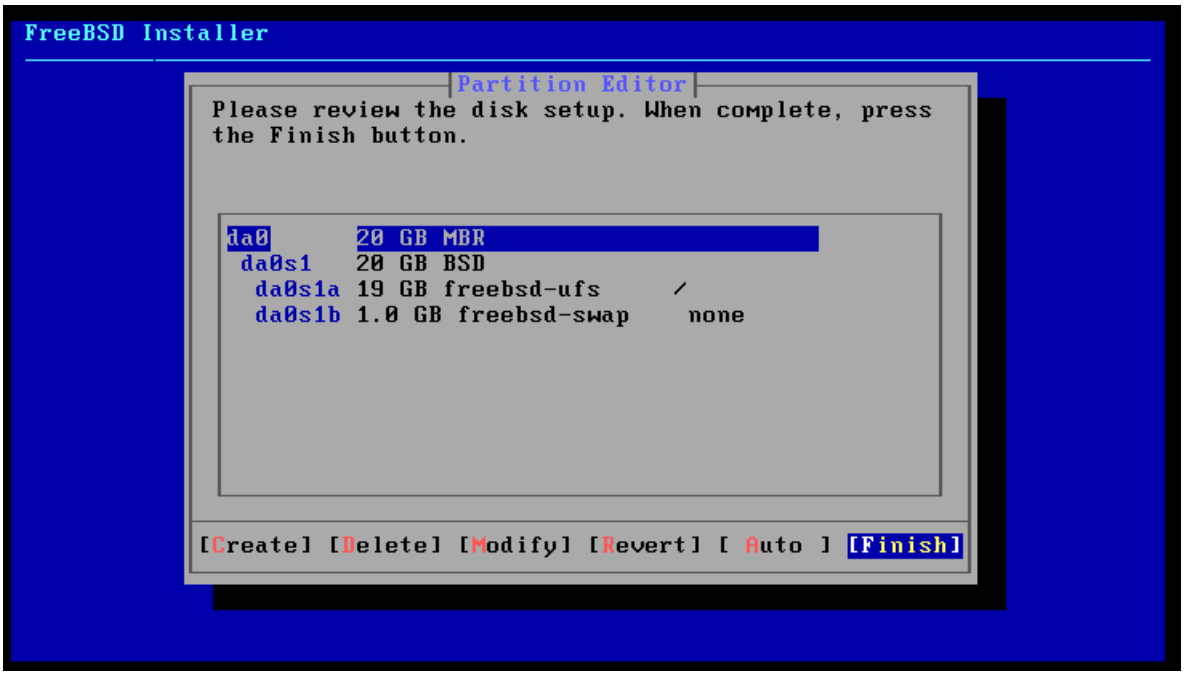

pfSense Installer
Copyright and distribution notice
Copyright and Trademark Notices.
Copyright(c) 2004-2016. Electric Sheep Fencing, LLC ("ESF").
All Rights Reserved.
Copyright(c) 2014-2023. Rubicon Communications, LLC d/b/a Netgate ("Netgate").
All Rights Reserved.
All logos, text, and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate.
"pfSense" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are
26%
[Accept]


pfSense Installer
Welcome
Welcome to pfSense!
Install
Install pfSense
Rescue Shell
Launch a shell for rescue operations
Recover config.xml
Recover config.xml from a previous install
< OK >
<Cancel>


pfSense Installer
Partitioning
How would you like to partition your disk?
Auto (ZFS) Guided Root-on-ZFS
Auto (UFS) Guided UFS Disk Setup
Manual Manual Disk Setup (experts)
Shell Open a shell and partition by hand
< OK >
<Cancel>
Menu options help choose which disk to setup using UFS and standard partitions

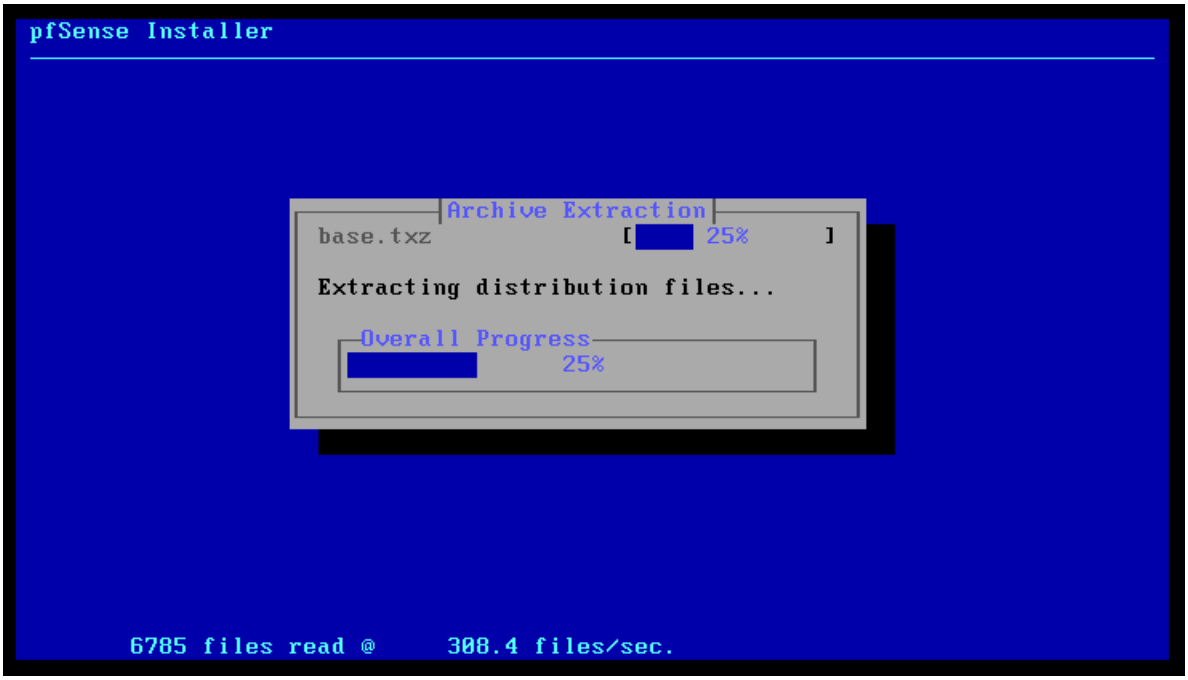

FreeBSD Installer
Partition
Would you like to use this entire disk (da0) for pfSense or partition it to share it with other operating systems? Using the entire disk will erase any data currently stored there.
[Entire Disk]
[Partition]

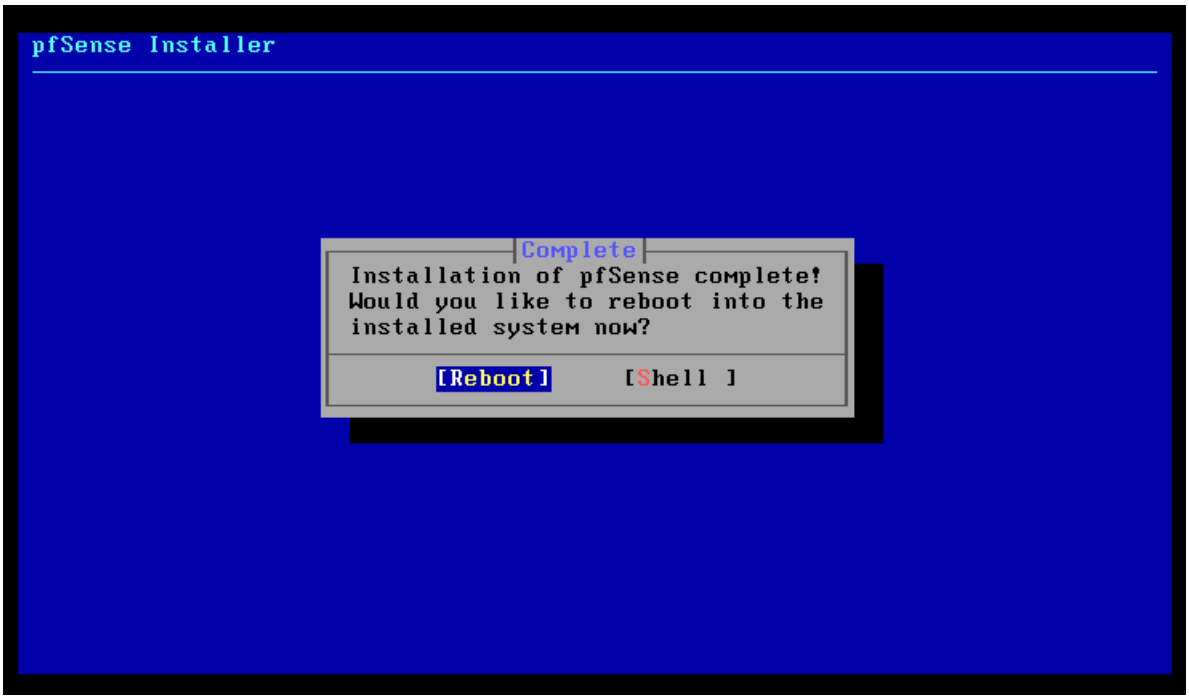

FreeBSD Installer
Partition Scheme
Select a partition scheme
for this volume:
APM Apple Partition Map
BSD BSD Labels
GPT GUID Partition Table
MBR DOS Partitions
[OK]
[Cancel]
Would
(da0)
share
Using
curre
k
?
data
Bootable on most x86 systems


FreeBSD Installer
Partition Editor
Please review the disk setup. When complete, press
the Finish button.
da0 20 GB MBR
da0s1 20 GB BSD
da0s1a 19 GB freebsd-ufs /
da0s1b 1.0 GB freebsd-swap none
[Create] [Delete] [Modify] [Revert] [Auto] [Finish]


FreeBSD Installer
Partition Editor
Please review the disk setup. When complete, press the Finish button.
Confirmation
Your changes will now be written to disk. If you have chosen to overwrite existing data, it will be PERMANENTLY ERASED. Are you sure you want to commit your changes?
[Commit] [Revert & Exit] [Back]
[Create] [Delete] [Modify] [Revert] [Auto] [Finish]

>


pfSense Installer
Archive Extraction
base.txz [25%]
Extracting distribution files...
Overall Progress
25%
6785 files read @ 308.4 files/sec.



Enlever l'iso si problème de reeboot

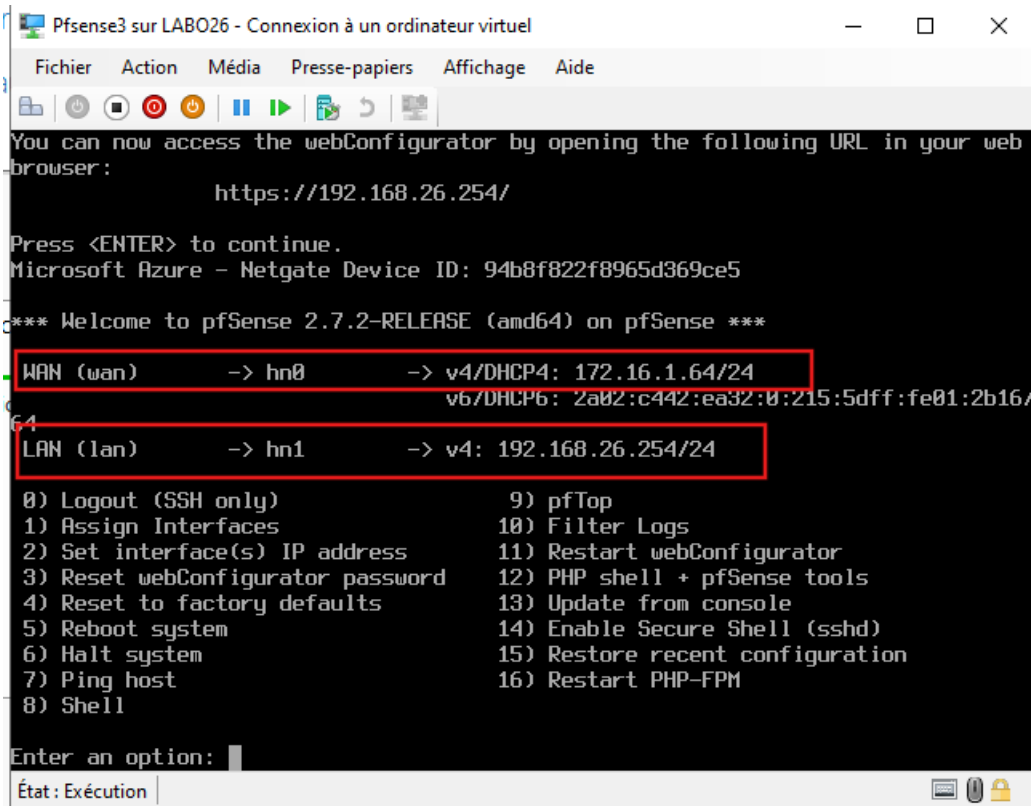
> une fois la vm redémarrée, d'autres paramètres sont à faire :

Attribuer la WAN à hn0 et la LAN à hn1.

On peut voir que la WAN a une adresse IP attribuée par DHCP, mais la LAN en a une par défaut. Il faut mettre la passerelle des VMs.

Pour cela dans le menu > 2 > 2 (pour changer la LAN sinon WAN = 1) > à la question si on veut du DHCP = non > on lui attribue comme IP la passerelle des VMs, Ici 192.168.26.254

On doit obtenir la configuration suivante



Test connexion internet sur les VMs du domaine = OK

Étape 20 : Configuration pfSense

Pour configurer pfSense, il faut se rendre sur l'interface graphique via internet. Depuis une machine (connectée à internet et au domaine) > navigateur web > taper l'IP de carte LAN (l'IP des passerelles Vms) soit 192.168.26.254

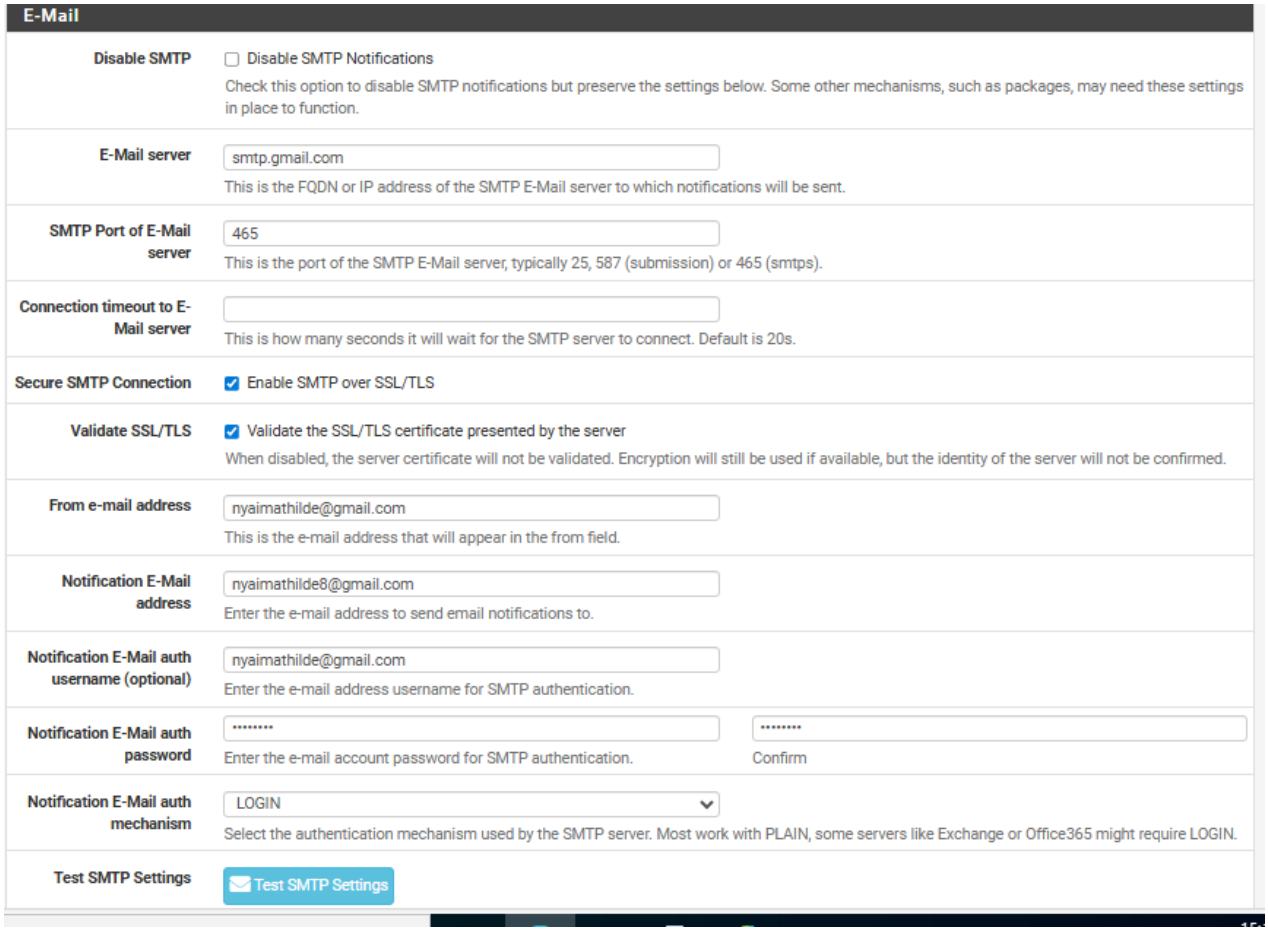
Pour se connecter entrer l'ID et mdp par défaut :

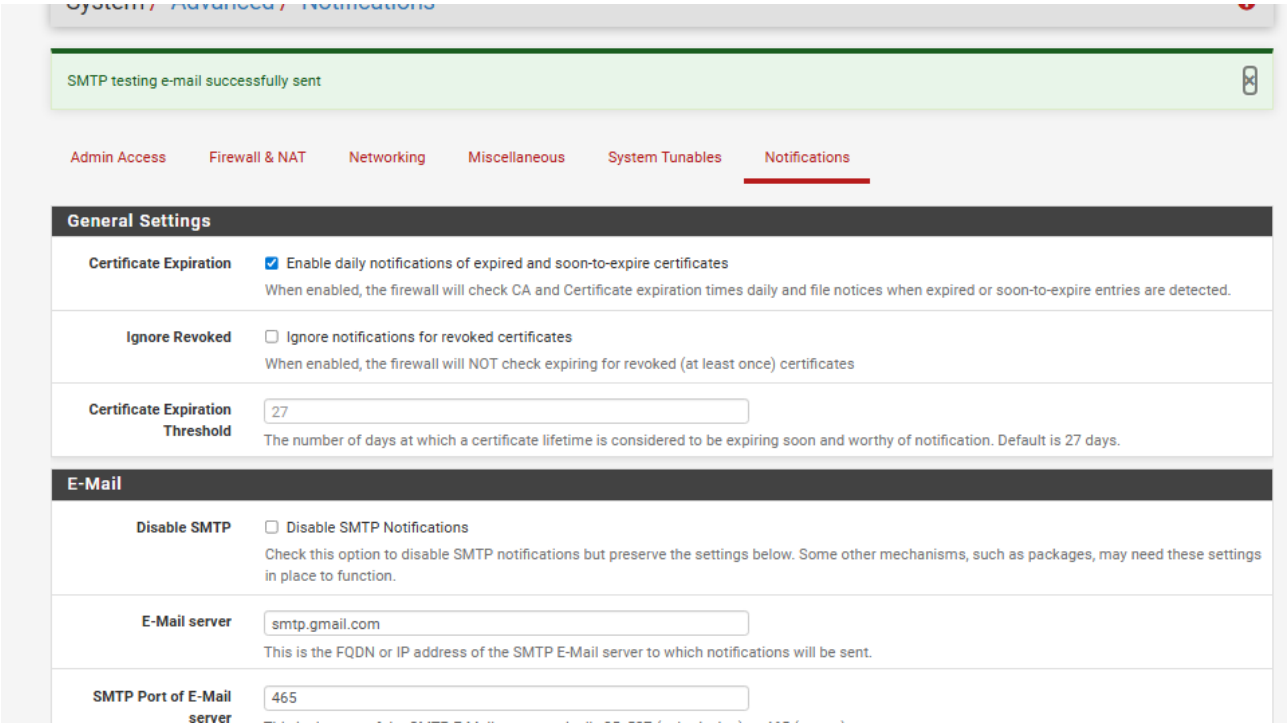
id : admin

mdp : pfsense

Suivre les instructions (intuitives)

20.1 : Configuration serveur SMTP





20.2 : IPv6

Désactiver l'IPv6 permet de réduire les surfaces d'attaque en supprimant un protocole supplémentaire qui pourrait être mal configuré ou peu maîtrisé. Cela permet aussi la simplification de la gestion et du diagnostic réseau notamment dans des environnements où IPv6 n'est pas utilisé ou nécessaire. Cette désactivation peut aussi éviter certains problèmes de connectivité, comme des comportements imprévus liés à la priorité d'IPv6 sur IPv4, ainsi que des conflits potentiels avec des équipements, applications ou systèmes plus anciens qui ne supportent pas l'IPv6.

- Désactiver l'IPv6 au niveau du LAN et du WAN.

Sur l'interface web du routeur, aller dans Interfaces > LAN > au niveau de « DHCPv6 » passer sur « NONE ». Faire de même sur l'interface WAN

Étape 21 : Access-list

Une Access Control List est une liste de règles simples qui sert à autoriser ou refuser du trafic.

Les ACL sont utilisées pour déterminer qui ou quoi peut accéder à une ressource, tandis que les règles de pare-feu sont utilisées pour filtrer le trafic réseau selon principalement les mêmes critères que les ACL mais sont généralement plus strictes et peuvent inclure des fonctionnalités avancées comme l'inspection des paquets.

Les ACL peuvent être standard. Elle filtrent selon uniquement l'adresse IP source et sont numérotées de 1 à 99 et de 1300 à 1999.

Exemple : autoriser un réseau à accéder au routeur

access-list 23 permit 192.168.26.0 0.0.0.255

Les Access-list peuvent aussi être étendues. Elles filtrent selon :

- l'adresse IP source / destination
- le réseau
- le protocole (IP, TCP, UDP, ICMP…)
- le port (si ACL étendue)

Elles sont numérotées de 100 à 199 et de 2000 à 2699.

Exemple : autoriser le protocole TCP en provenance de n'importe quel poste dont le n° de port est supérieur à 1023 à destination de n'importe quel poste dont le n° de port est égal à 443

access-list 101 permit tcp any gt 1023 any eq 443 ou **access-list 101 permit tcp any any eq 443**

Dans pfSense, l'onglet ACL est utilisé pour le contrôle d'accès aux services du pare-feu lui-même, pas au trafic qui traverse le réseau.

Il sert à définir qui a le droit d'accéder à :

- l'interface Web (GUI)
- le SSH
- les services internes (VPN, captive portal, etc.)

Étape 22 : règles pare-feu

Les règles de pare-feu peuvent filtrer le trafic selon les mêmes principes que les ACL. Avant de configurer des règles de pare-feu il est préférable de configurer en amont les règles NAT.

Les règles inutilisées doivent être supprimées régulièrement afin de maintenir une configuration claire et sécurisée.

Les règles d'un pare-feu se lisent se haut en bas. La première règle correspondante est appliquée. Les règles qui autorisent au début, et une qui bloque tout à la fin.