Présentation du cas Vita Big Pharma (contexte)

Vita Big Pharma c’est une entreprise pharmaceutique qui veut s’installer en France avec deux sites : Toulouse (le siège avec la direction, RH et finance) et Marseille (le site technique avec support et service technique). Du coup, une infrastructure réseau centralisée, sécurisée et évolutive doit être mise en place pour que l’entreprise puisse travailler correctement, assurer la continuité de service, permettre le télétravail, et sécuriser les échanges entre les deux sites.

Travail à faire

Dans ce projet, les besoins doivent d’abord être analysés en prenant en compte les contraintes techniques et aussi le côté légal (RGPD). Une communication sécurisée entre Toulouse et Marseille doit être assurée, une authentification centralisée doit être mise en place avec Active Directory, et les droits doivent être gérés avec des groupes. Un partage de fichiers sécurisé doit être proposé avec des quotas, et des services métiers doivent être intégrés pour répondre aux besoins de l’entreprise.

Ensuite, l’infrastructure doit être conçue et maquetée avec une séparation claire entre le réseau serveurs et le réseau collaborateurs. Des pare-feu doivent être installés sur chaque site, un VPN site-à-site doit être configuré pour relier Toulouse et Marseille, et un VPN nomade doit être mis en place pour le télétravail. En plus, du Traffic Shaping doit être appliqué sur le réseau collaborateurs afin de limiter le débit et garder la priorité aux services importants.

Enfin, tout doit être déployé, testé et exploité avec des sauvegardes, de la supervision, des audits de sécurité, et une documentation complète (schéma réseau, procédures, scripts, guides, etc.).

Contexte technique (synthèse)

L’infrastructure est répartie sur deux sites reliés par un VPN site-à-site sécurisé. Sur chaque site, un pare-feu protège les réseaux, et une segmentation est mise en place entre un LAN serveurs et un LAN collaborateurs. Un Active Directory avec DNS est déployé pour centraliser la gestion des utilisateurs, des groupes et des stratégies de sécurité (GPO). Les services métiers sont installés selon les besoins des sites, et l’ensemble est complété par un serveur de fichiers avec quotas, des sauvegardes régulières et une solution de supervision.

Tableau récapitulatif des services par site

Site	Services / Départements	Rôle du site
Toulouse (siège administratif)	Direction, Ressources Humaines, Finance	Gestion administrative et services centraux
Marseille (site technique)	Service technique, Support informatique	Support, maintenance, assistance utilisateurs

---

Liste des besoins fonctionnels et techniques

Les besoins fonctionnels sont d'assurer une communication sécurisée entre Toulouse et Marseille, de centraliser l'authentification via Active Directory, de gérer les droits par groupes, et de mettre en place un partage de fichiers sécurisé avec quotas. Le télétravail doit être possible via un accès distant sécurisé, et des services métiers doivent être disponibles pour répondre aux besoins de l'entreprise. La supervision, les sauvegardes et la disponibilité des services critiques doivent aussi être garanties.

Les besoins techniques incluent une segmentation du réseau (serveurs / collaborateurs), l'installation de pare-feu sur chaque site, la mise en place d'un VPN site-à-site et d'un VPN nomade, ainsi que des règles de filtrage. Des GPO doivent être configurées pour sécuriser les postes, automatiser des tâches et déployer des logiciels. Enfin, un Traffic Shaping doit être appliqué sur le réseau collaborateurs afin de limiter le débit et prioriser les services importants.

Contraintes réglementaires et organisationnelles

Le projet doit respecter le RGPD, ce qui impose une gestion stricte des accès, la journalisation, une politique de mot de passe renforcée, ainsi que des sauvegardes régulières et fiables.

L'entreprise étant organisée sur deux sites distants, la solution doit être stable, sécurisée, évolutive et garantir la continuité de service.

Étude de l'existant

Vita Big Pharma étant en cours d'implantation en France, aucune infrastructure informatique existante n'est disponible sur les sites de Toulouse et Marseille. Il n'y a donc pas de serveurs déjà en place, pas de domaine Active Directory, ni de services réseau configurés. Toute l'infrastructure doit être conçue et déployée à partir de zéro.

Hypothèses retenues

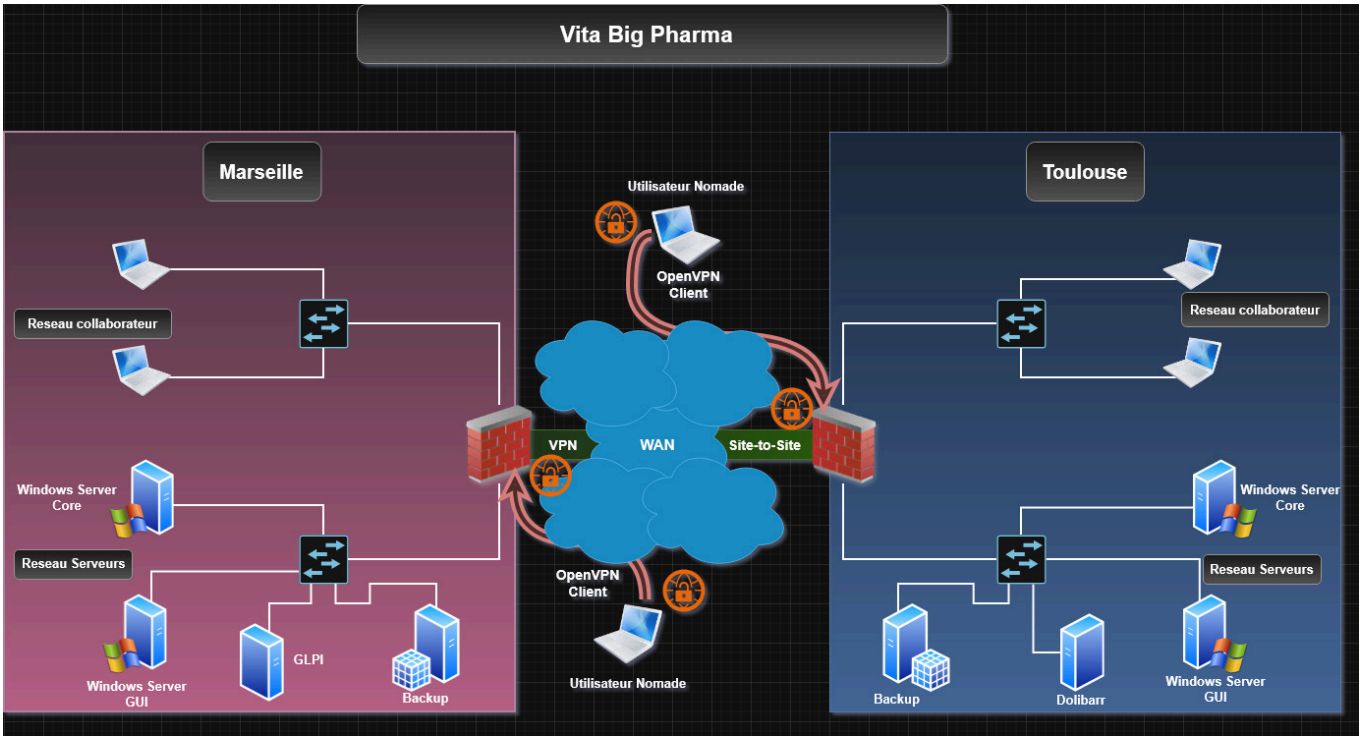
Une architecture multi-sites est retenue, avec un site à Toulouse et un site à Marseille, interconnectés via un VPN site-à-site sécurisé. Chaque site dispose de ses propres services locaux afin d'assurer de bonnes performances et une meilleure continuité de service.

Une segmentation du réseau est également retenue, avec une séparation entre le LAN serveurs et le LAN collaborateurs, protégés par un pare-feu sur chaque site. L'authentification des utilisateurs est centralisée grâce à Active Directory, et le télétravail est rendu possible via un VPN nomade sécurisé.

Justification des choix

Le choix d'une architecture multi-sites permet d'assurer la continuité de service, d'améliorer les performances et de sécuriser les échanges entre les deux sites. La segmentation réseau et l'utilisation de pare-feu renforcent la sécurité, tandis que le VPN permet de garantir la confidentialité des communications. Enfin, cette solution reste évolutive et adaptée au développement de l'entreprise.

Le réseau mis en place



Ce schéma représente une architecture réseau multi-sites pour l'entreprise Vita Big Pharma, avec deux sites distincts à Toulouse et Marseille. Sur chaque site, l'infrastructure est

segmentée en deux LAN séparés : un LAN serveurs et un LAN collaborateurs, chacun connecté à un commutateur et protégé par un pare-feu.

Les pare-feux assurent le filtrage des flux, la sécurisation des accès et la mise en place des tunnels VPN. Un VPN site-à-site permet l'interconnexion sécurisée entre les deux sites, tandis qu'un VPN nomade (OpenVPN) permet l'accès distant des utilisateurs. Les services critiques, tels que les contrôleurs de domaine Active Directory, les serveurs métiers (GLPI à Marseille, Dolibarr à Toulouse) et les serveurs de sauvegarde, sont hébergés sur les LAN serveurs afin de garantir la sécurité, la disponibilité et la cohérence de l'infrastructure.

1/ Les solutions techniques mises en place

Tableau comparatif des solutions techniques

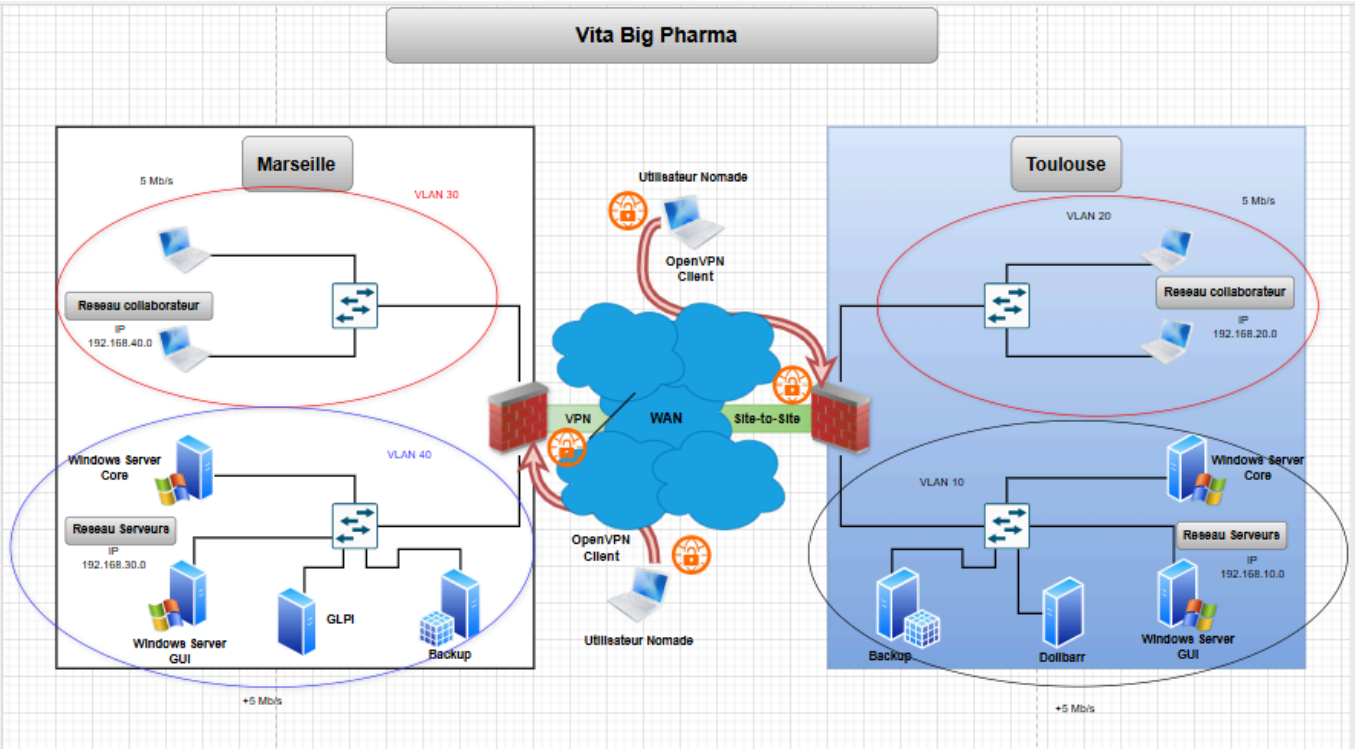
Besoin	**Solution retenue**	**Alternatives étudiées**	**Justification du choix**
Pare-feu / VPN / QoS	**OPNSense / pfSense**	Firewall matériel, UFW	Solution open-source complète, stable, adaptée au VPN et au Traffic Shaping
Authentification centralisée	**Active Directory / DNS**	LDAP seul	Gestion centralisée des utilisateurs, intégration native avec Windows et GPO
VPN site-à-site	**IPsec**	OpenVPN site-à-site	Standard sécurisé, performant et largement utilisé
VPN nomade	**OpenVPN**	WireGuard	Solution fiable, bien documentée et simple à déployer
Ticketing / Inventaire	**GLPI**	OCS Inventory, Redmine	Outil complet, compatible AD, adapté au support informatique
ERP	**Dolibarr**	Odoo	Léger, open-source et adapté aux besoins d'une PME
Supervision	**Prometheus**	Zabbix, Nagios	Collecte efficace des métriques, intégration Docker
Sauvegardes	**rsync + scripts**	Bacula	Solution simple, automatisable et suffisante pour le projet
Audit sécurité AD	**PingCastle**	BloodHound	Outil spécialisé pour l'analyse de la sécurité Active Directory
Audit sécurité Linux	**Lynis**	OpenSCAP	Audit complet et simple à mettre en œuvre

Les solutions retenues sont majoritairement open-source, reconnues et adaptées à une infrastructure multi-sites. Elles permettent de répondre aux besoins fonctionnels et techniques de l’entreprise tout en assurant un bon niveau de sécurité, de supervision et de maintenabilité.

Spécifications techniques

Plan d'adressage

Site	Réseau	Adresse réseau	Masque	Passerelle (pare-feu)	Vlan
Toulouse	LAN Serveurs	192.168.10.0	/24	192.168.10.254	10
Toulouse	LAN Collaborateurs	192.168.20.0	/24	192.168.20.254	20
Marseille	LAN Serveurs	192.168.30.0	/24	192.168.30.254	30
Marseille	LAN Collaborateurs	192.168.40.0	/24	192.168.40.254	40



Tests fonctionnels

Test	Élément testé	Action	Résultat attendu
Accès VLAN 20	Réseau collaborateurs Toulouse	Ping poste → passerelle VLAN 20	Réponse OK
Accès VLAN 30	Réseau collaborateurs Marseille	Ping poste → passerelle VLAN 30	Réponse OK
Accès VLAN 10	Réseau serveurs Toulouse	Ping poste → serveurs AD/Dolibarr	Accès autorisé
Accès VLAN 40	Réseau serveurs Marseille	Ping poste → serveurs AD/GLPI	Accès autorisé
VPN site-à-site	IPsec Toulouse ↔ Marseille	Ping inter-sites	Communication OK
VPN nomade	OpenVPN	Connexion utilisateur distant	Accès aux ressources internes
Services métiers	GLPI / Dolibarr	Connexion Web	Service accessible

Tests de sécurité

Test	Élément testé	Action	Résultat attendu
Filtrage VLAN	VLAN 20/30 vers serveurs	Test accès non autorisé	Accès bloqué
Séparation VLAN	VLAN Collaborateurs ↔ Serveurs	Scan ou tentative hors règles	Accès refusé
Pare-feu WAN	Accès depuis Internet	Tentative accès direct	Accès bloqué
VPN sécurisé	Tunnel IPsec	Vérification chiffrement	Tunnel actif
Traffic Shaping	VLAN 20 / 30	Test débit Internet	Débit limité à 5 Mb/s

Tests de continuité

Test	Élément testé	Action	Résultat attendu
Redondance AD	Contrôleur principal	Arrêt DC principal	Authentification maintenue
Reprise VPN	VPN site-à-site	Coupure / reconnexion	Tunnel rétabli
Sauvegarde	Serveurs	Test restauration fichier	Restauration réussie

Test	Élément testé	Action	Résultat attendu
Continuité télétravail	OpenVPN	Connexion après incident	Accès fonctionnel

Préparation du déploiement

1.1 – Firewall (pfSense)

Élément	Contenu attendu
Solution	**pfSense CE 2.7**
Rôle	Pare-feu, NAT, VPN, QoS
Emplacement	Toulouse / Marseille
Interfaces	WAN / LAN / OPT1
VPN	IPsec (site-to-site), OpenVPN (nomades)
Sécurité	Règles firewall + logs

1.1.1 – Besoins fonctionnels

Besoin	Mise en œuvre
Séparer les réseaux	1 LAN Serveurs + 1 LAN Collaborateurs
Relier les sites	VPN **IPsec**
Accès distant	VPN **OpenVPN**
Sécurité	Filtrage inter-LAN
Débit limité	QoS **5 Mb/s** sur collaborateurs

1.1.2 – Étude de solutions

Critère	pfSense	OPNsense
Pare-feu	Oui	Oui
VPN	IPsec / OpenVPN	IPsec / OpenVPN
QoS	Oui	Oui
Choix	✅ Retenu	Non

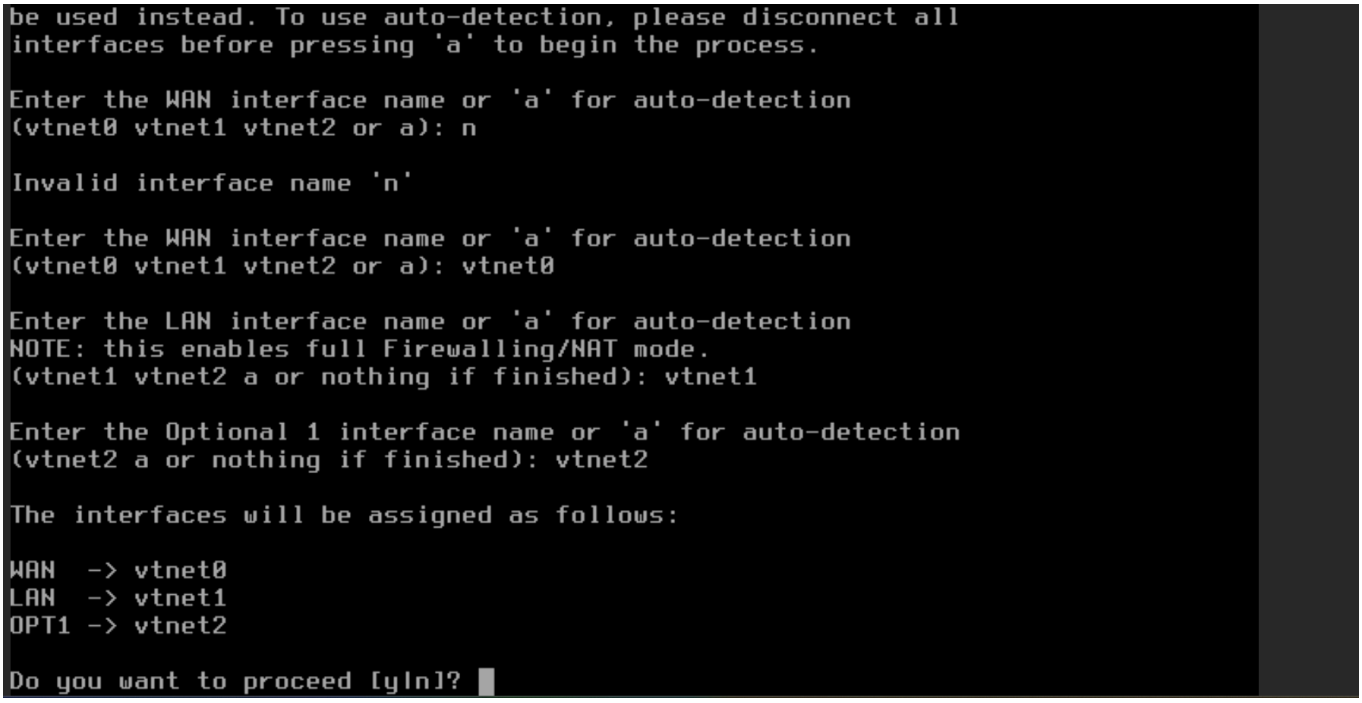
1.1.3 – Solution retenue

Justification
Compatible avec Proxmox
Répond à tous les besoins
Déjà installé et fonctionnel
Adapté à un contexte BTS SIO

2.1 – Architecture technique (pare-feu)

Élément	Valeur
OS	pfSense CE
Hyperviseur	Proxmox
Interfaces	vtnet0 (WAN) / vtnet1 (LAN) / vtnet2 (OPT1)
LAN	Collaborateurs
OPT1	Serveurs
VPN	IPsec + OpenVPN
QoS	5 Mb/s collaborateurs

Déploiement et mise en œuvre

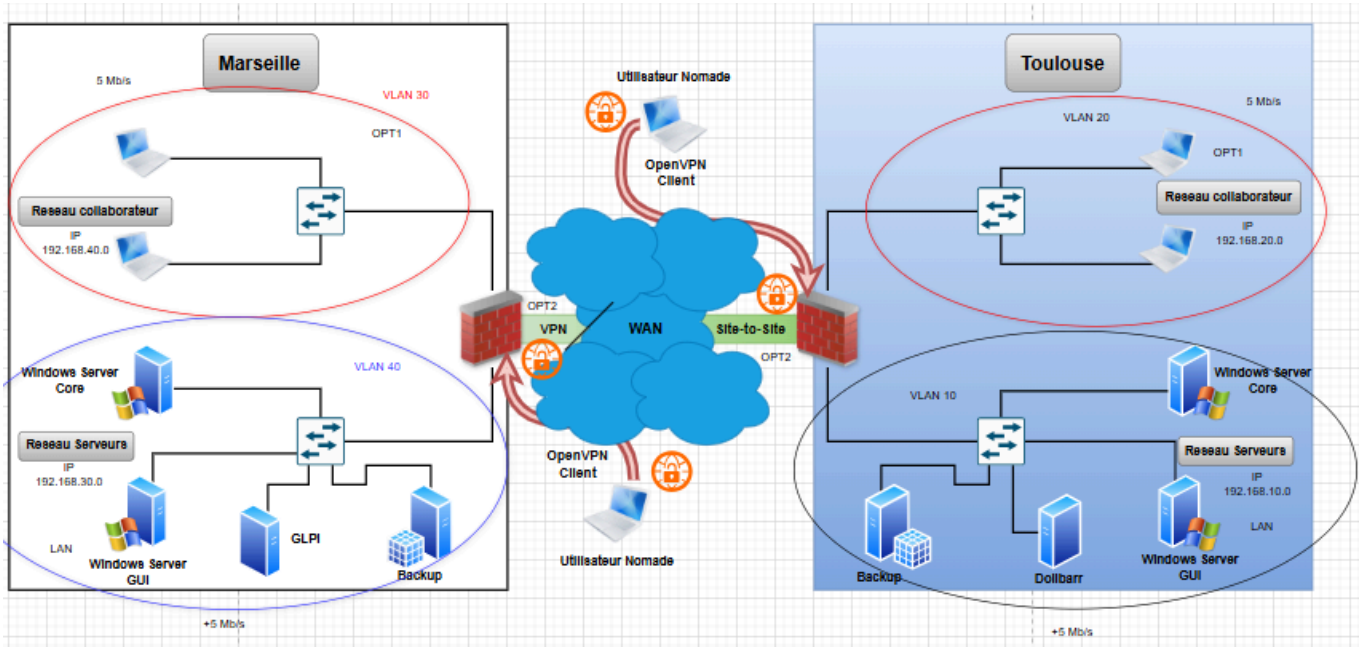


Cette image montre l'étape où **pfSense associe les cartes réseau virtuelles** à leurs rôles.

- Les interfaces ont été assignées correctement :
  - **WAN = vtnet0**
  - **LAN = vtnet1**
  - **OPT1 = vtnet2**

Rôle	Interface	Signification
WAN	vtnet0	Internet
LAN	vtnet1	Réseau interne
OPT1	vtnet2	Réseau optionnel

Mise en place sur le réseau



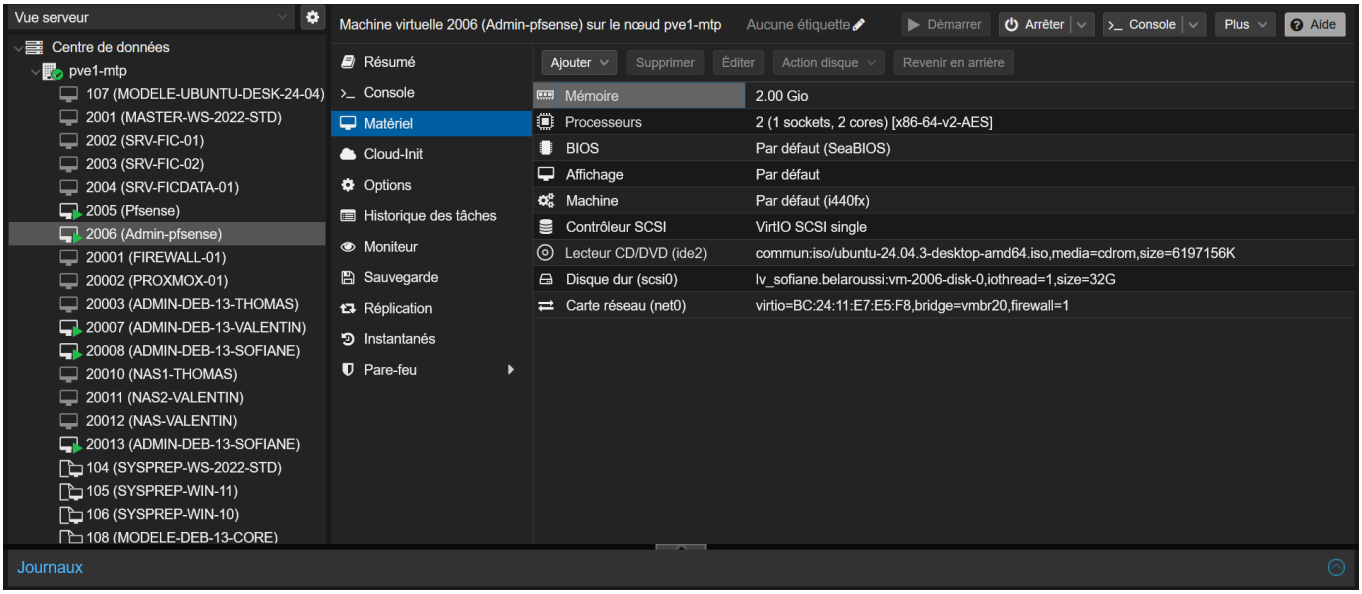
```
 7) Ping host                             16) Restart PHP-FPM
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - static)
3 - OPT1 (vtnet2)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.30.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
>
```

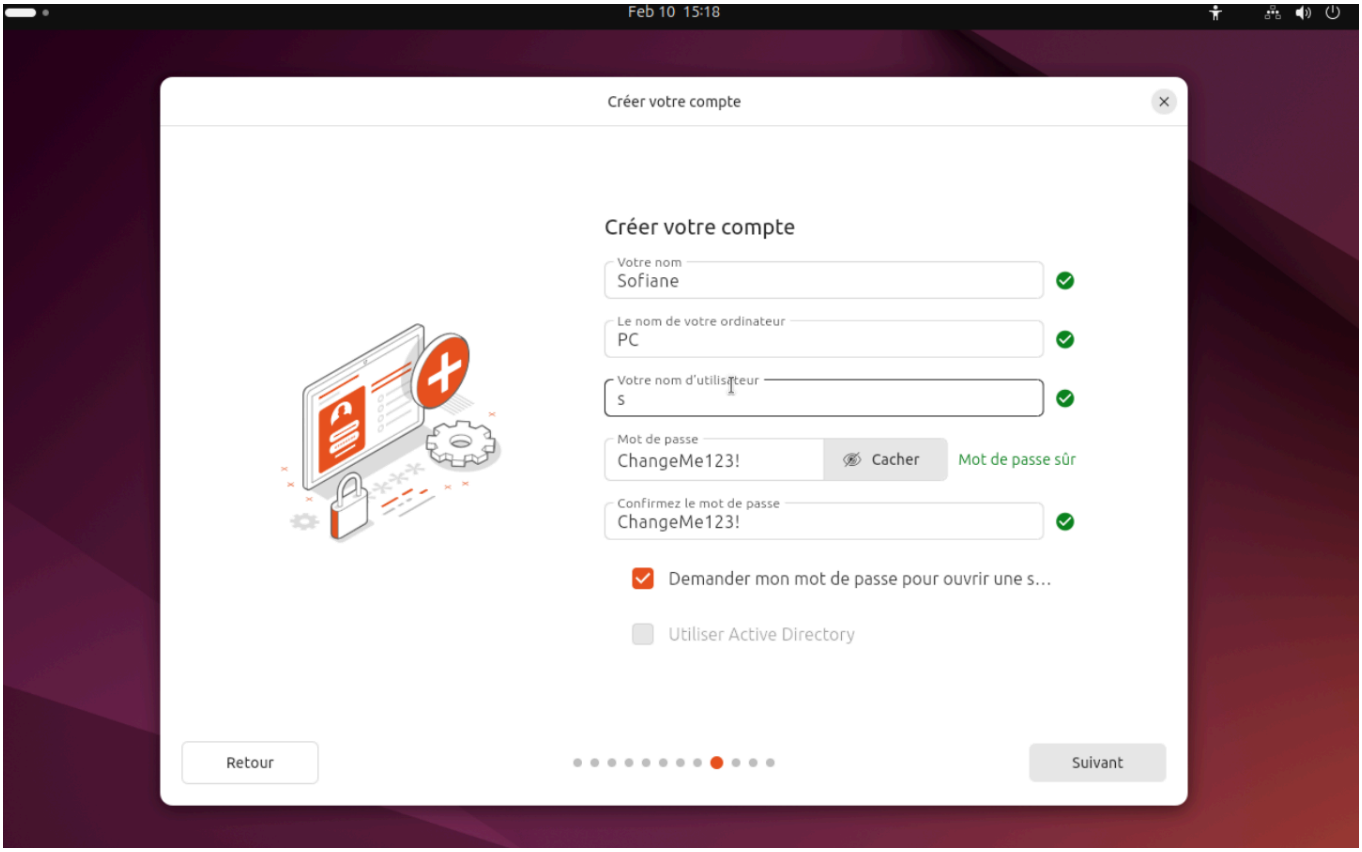
```
The IPv4 OPT1 address has been set to 192.168.40.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.40.1/

Press <ENTER> to continue.
QEMU Guest - Netgate Device ID: c50013781d5270526b25

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet0     ->
 LAN (lan)       -> vtnet1     -> v4: 192.168.30.1/24
 OPT1 (opt1)     -> vtnet2     -> v4: 192.168.40.1/24

 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:
```

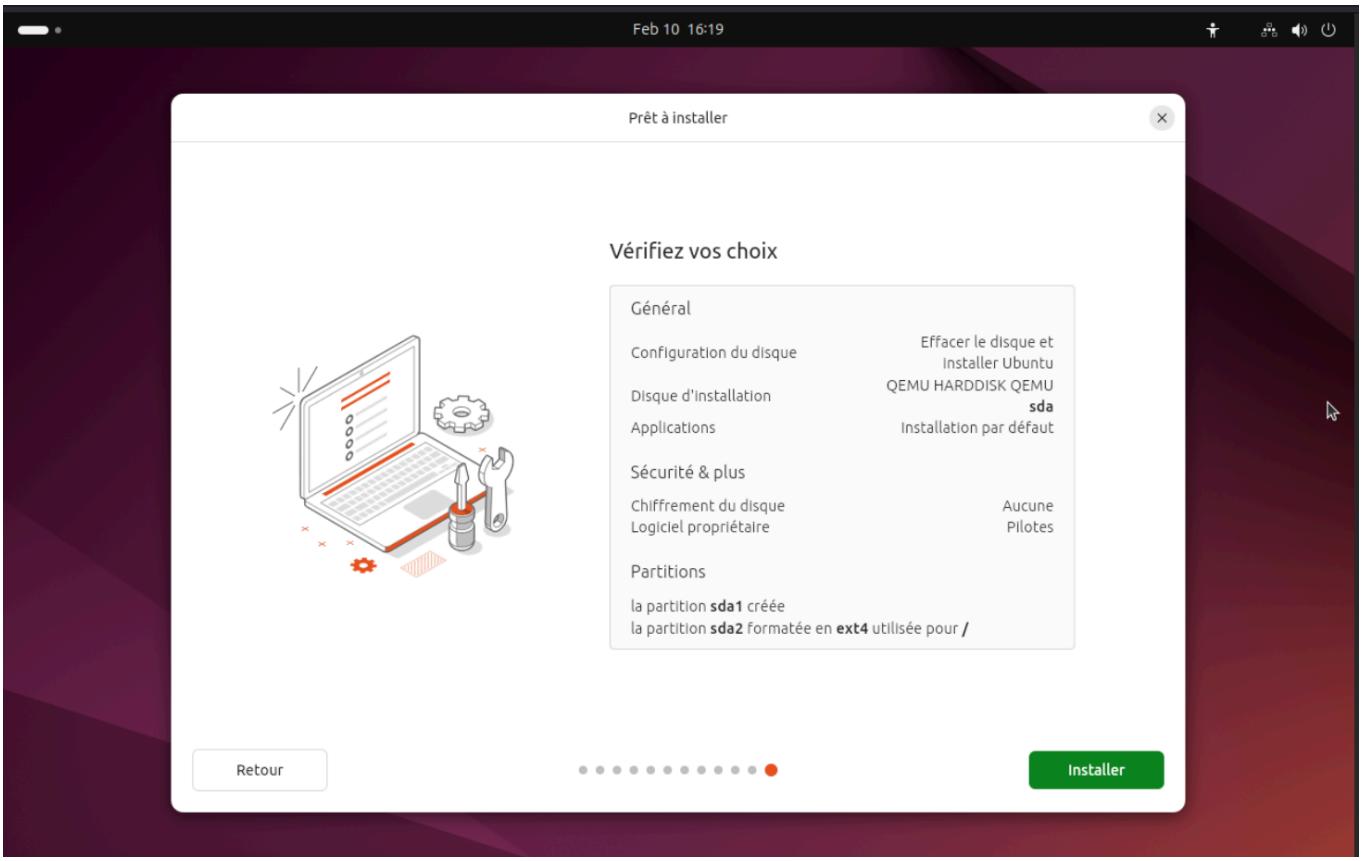
```
>

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on WAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.34.20.2
Enter the end address of the IPv4 client address range: 10.34.20.100
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to WAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 WAN address has been set to 10.34.20.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://10.34.20.254/

Press <ENTER> to continue.
```

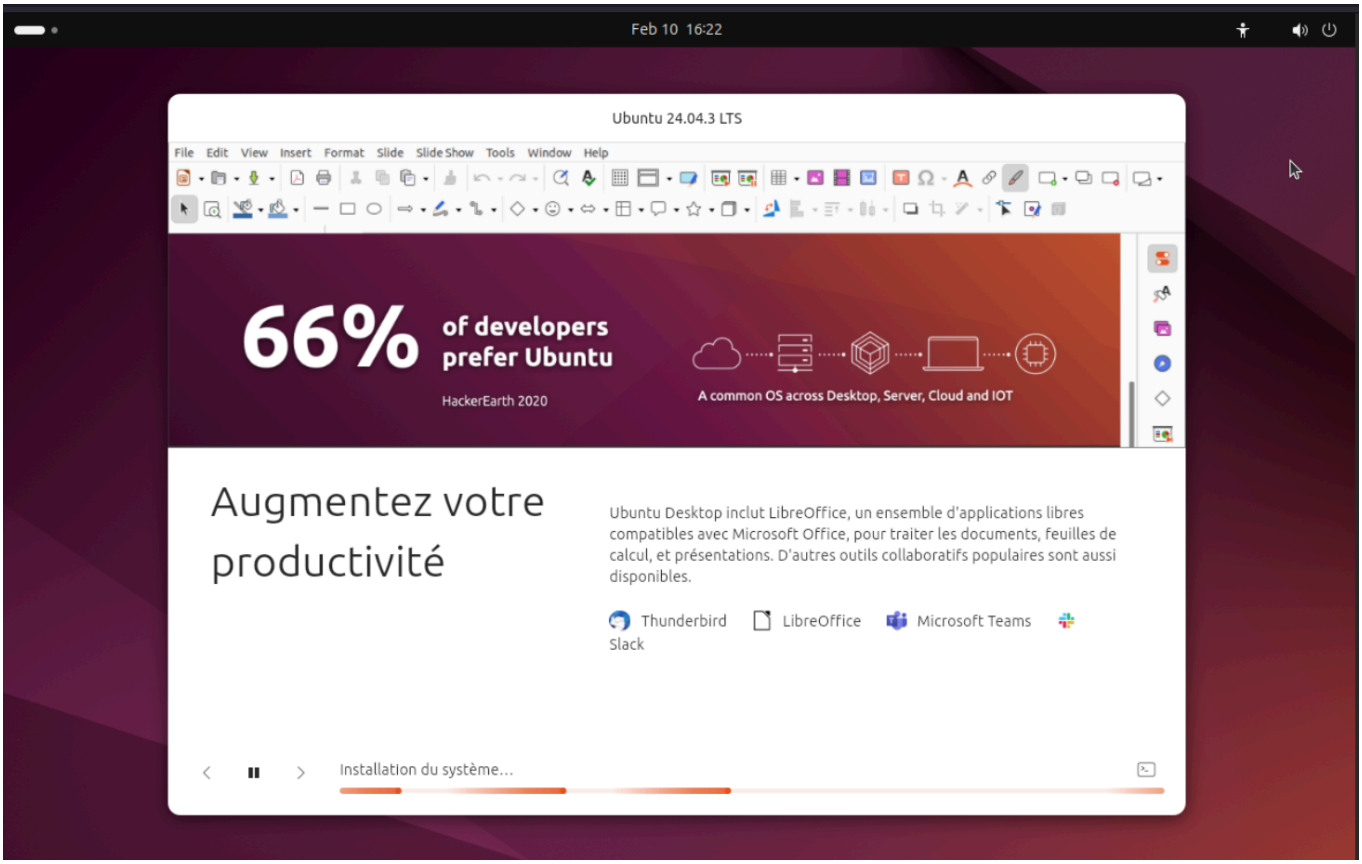
```
The IPv4 WAN address has been set to 10.34.20.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://10.34.20.254/

Press <ENTER> to continue.
QEMU Guest - Netgate Device ID: c50013781d5270526b25

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet0     -> v4: 10.34.20.254/24
 LAN (lan)       -> vtnet1     -> v4: 192.168.30.1/24
 OPT1 (opt1)     -> vtnet2     -> v4: 192.168.40.1/24

 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:
```

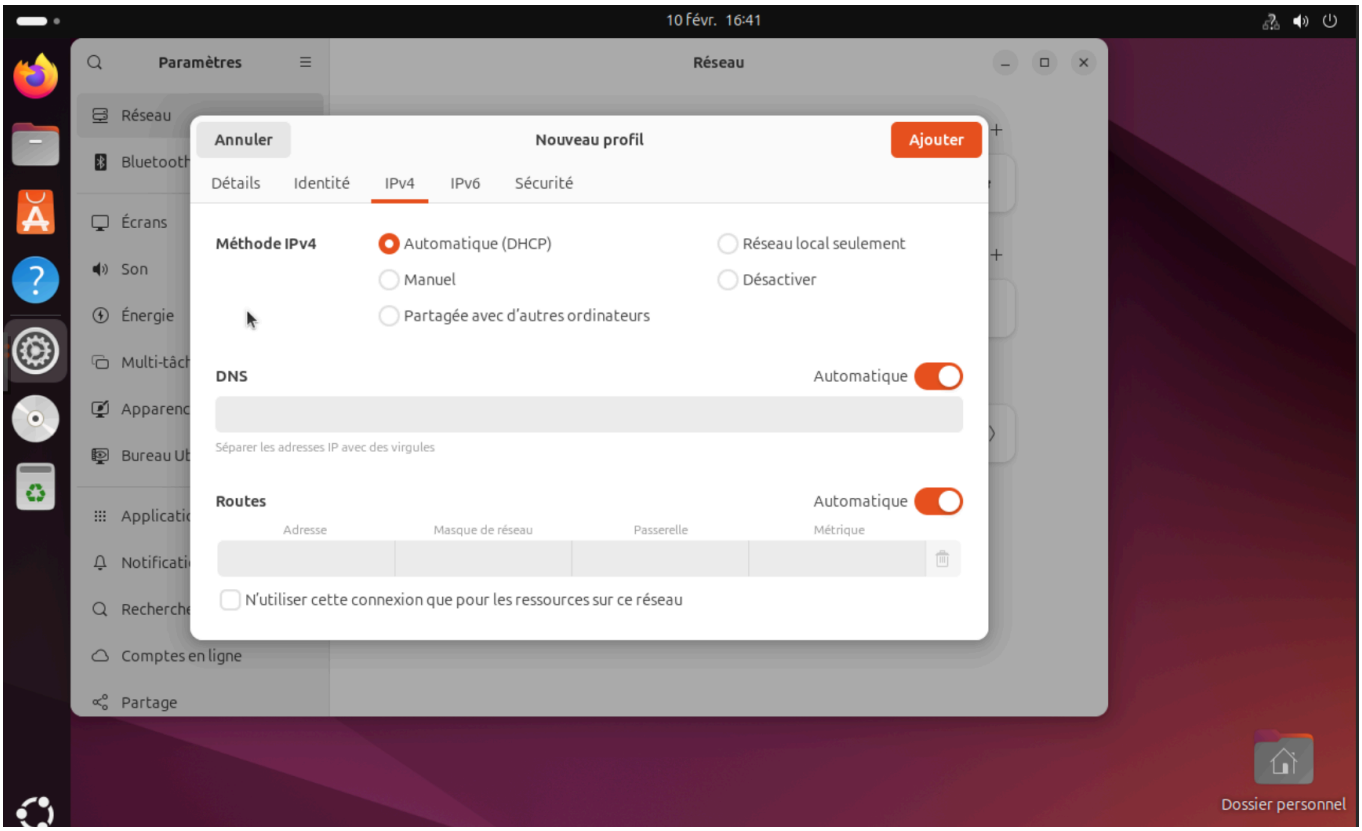
Création de la vm admin:

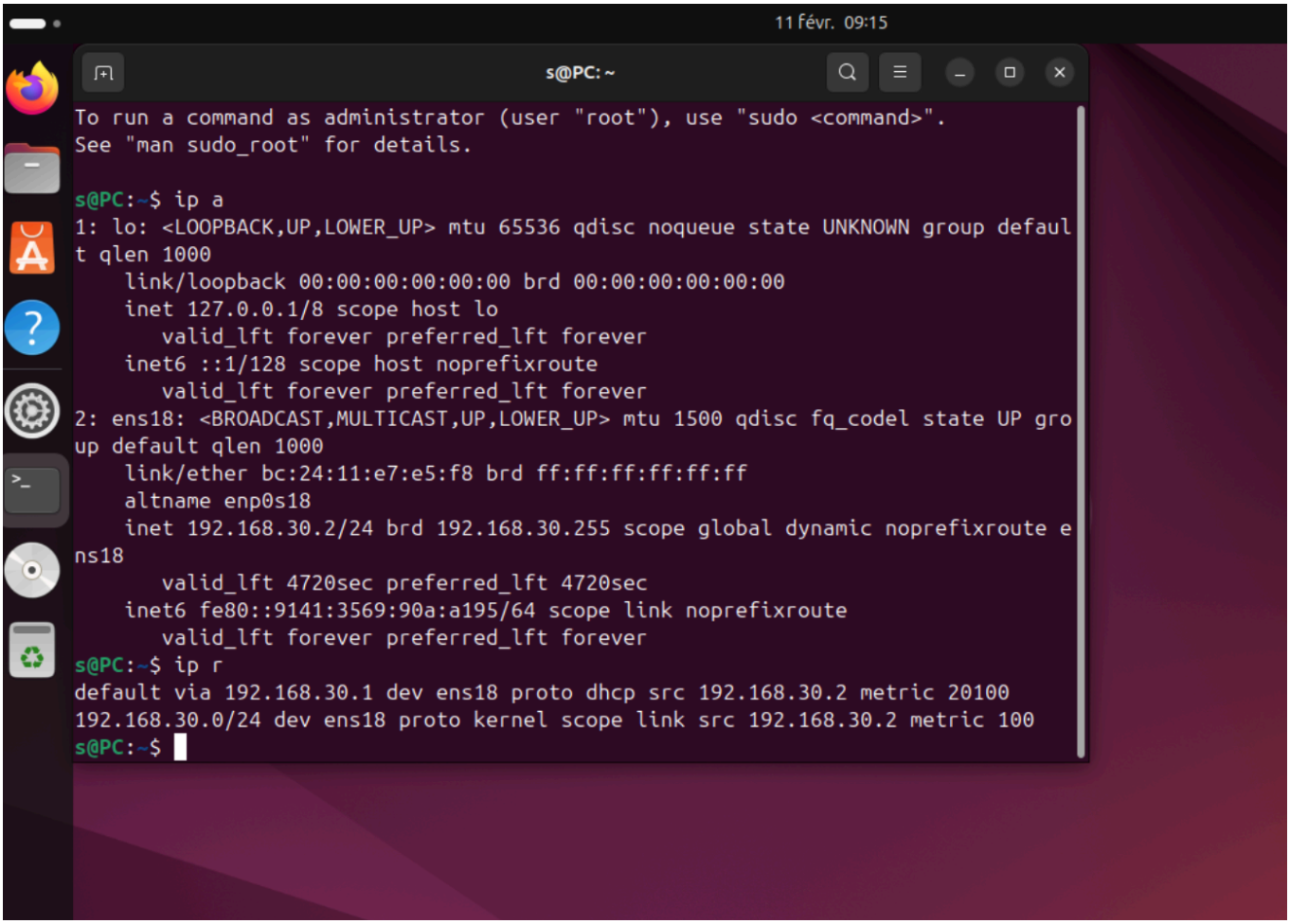


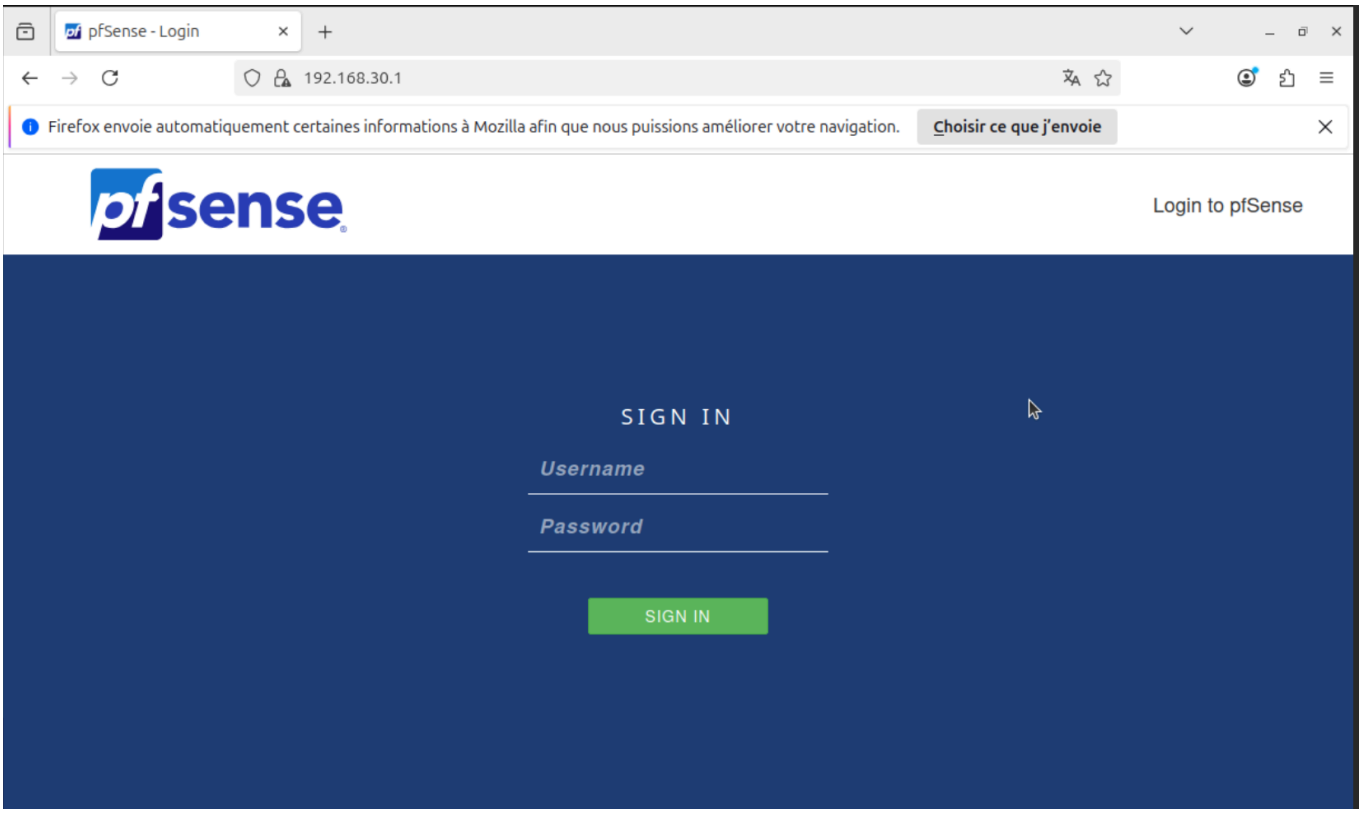



Feb 10 16:19
Prêt à installer
Vérifiez vos choix
Général
Configuration du disque
Effacer le disque et installer Ubuntu
Disque d'installation
QEMU HARDDISK QEMU sda
Applications
Installation par défaut
Sécurité & plus
Chiffrement du disque
Aucune
Logiciel propriétaire
Pilotes
Partitions
la partition sda1 créée
la partition sda2 formatée en ext4 utilisée pour /
Retour
Installer


Feb 10 16:22
Ubuntu 24.04.3 LTS
File Edit View Insert Format Slide Slide Show Tools Window Help
66% of developers prefer Ubuntu
HackerEarth 2020
A common OS across Desktop, Server, Cloud and IOT
Augmentez votre productivité
Ubuntu Desktop inclut LibreOffice, un ensemble d'applications libres compatibles avec Microsoft Office, pour traiter les documents, feuilles de calcul, et présentations. D'autres outils collaboratifs populaires sont aussi disponibles.
Thunderbird
LibreOffice
Microsoft Teams
Slack
Installation du système…

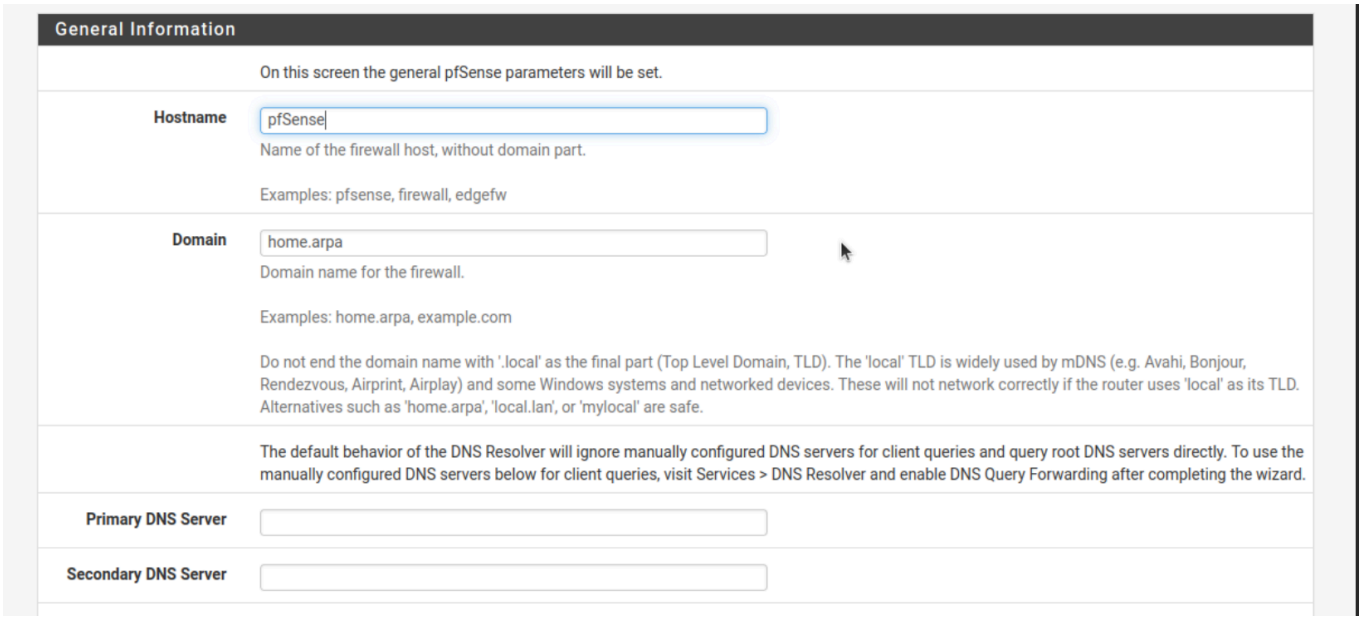

10 févr. 16:41
Paramètres
Réseau
Réseau
Annuler
Nouveau profil
Ajouter
Détails
Identité
IPv4
IPv6
Sécurité
Méthode IPv4
Automatique (DHCP)
Manuel
Partagée avec d'autres ordinateurs
Réseau local seulement
Désactiver
DNS
Automatique
Séparer les adresses IP avec des virgules
Routes
Automatique
Adresse
Masque de réseau
Passerelle
Métrique
N'utiliser cette connexion que pour les ressources sur ce réseau
Écrans
Son
Énergie
Partage
Dossier personnel

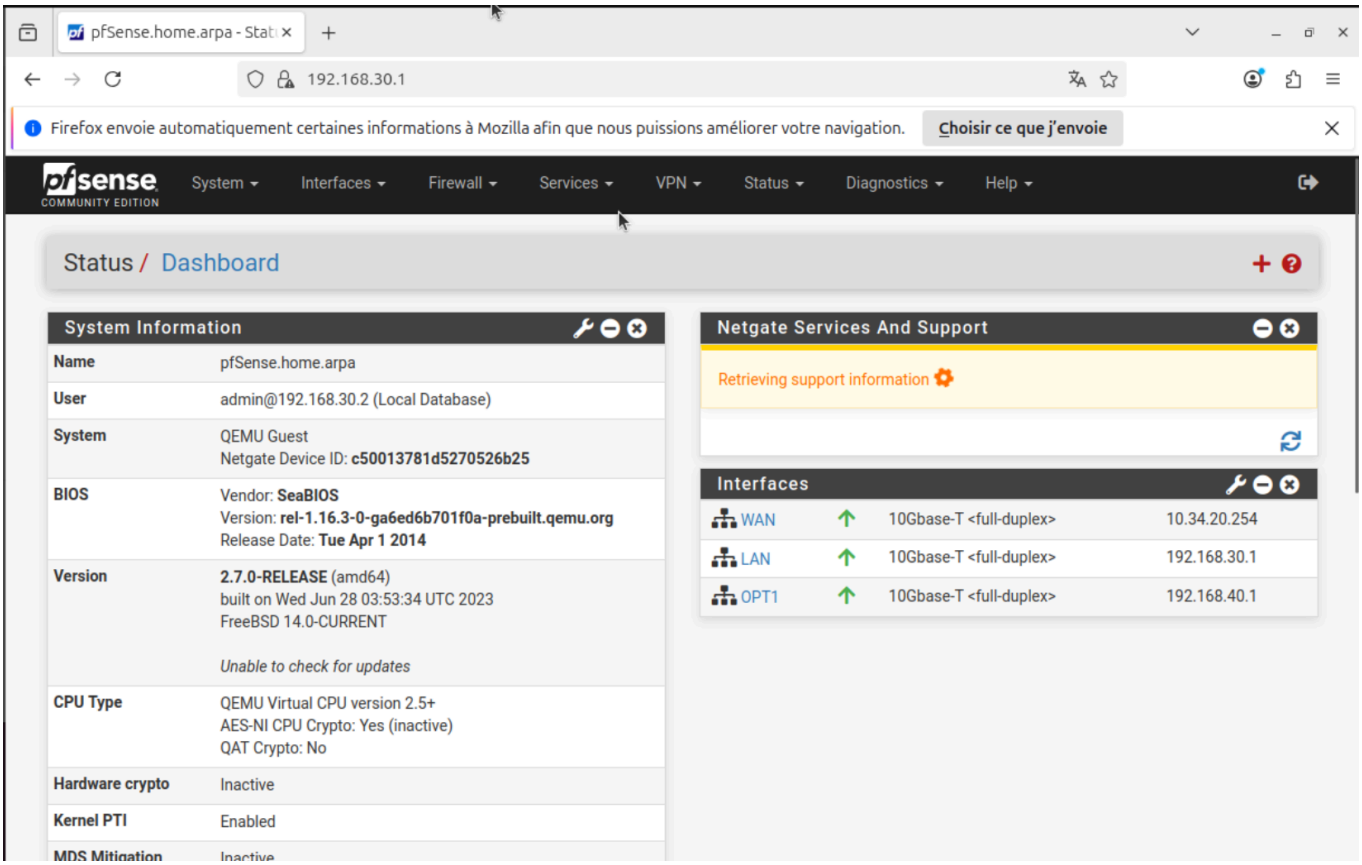

11 févr. 09:15
s@PC: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
s@PC:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether bc:24:11:e7:e5:f8 brd ff:ff:ff:ff:ff:ff
altname enp0s18
inet 192.168.30.2/24 brd 192.168.30.255 scope global dynamic noprefixroute ens18
valid_lft 4720sec preferred_lft 4720sec
inet6 fe80::9141:3569:90a:a195/64 scope link noprefixroute
valid_lft forever preferred_lft forever
s@PC:~$ ip r
default via 192.168.30.1 dev ens18 proto dhcp src 192.168.30.2 metric 20100
192.168.30.0/24 dev ens18 proto kernel scope link src 192.168.30.2 metric 100
s@PC:~$



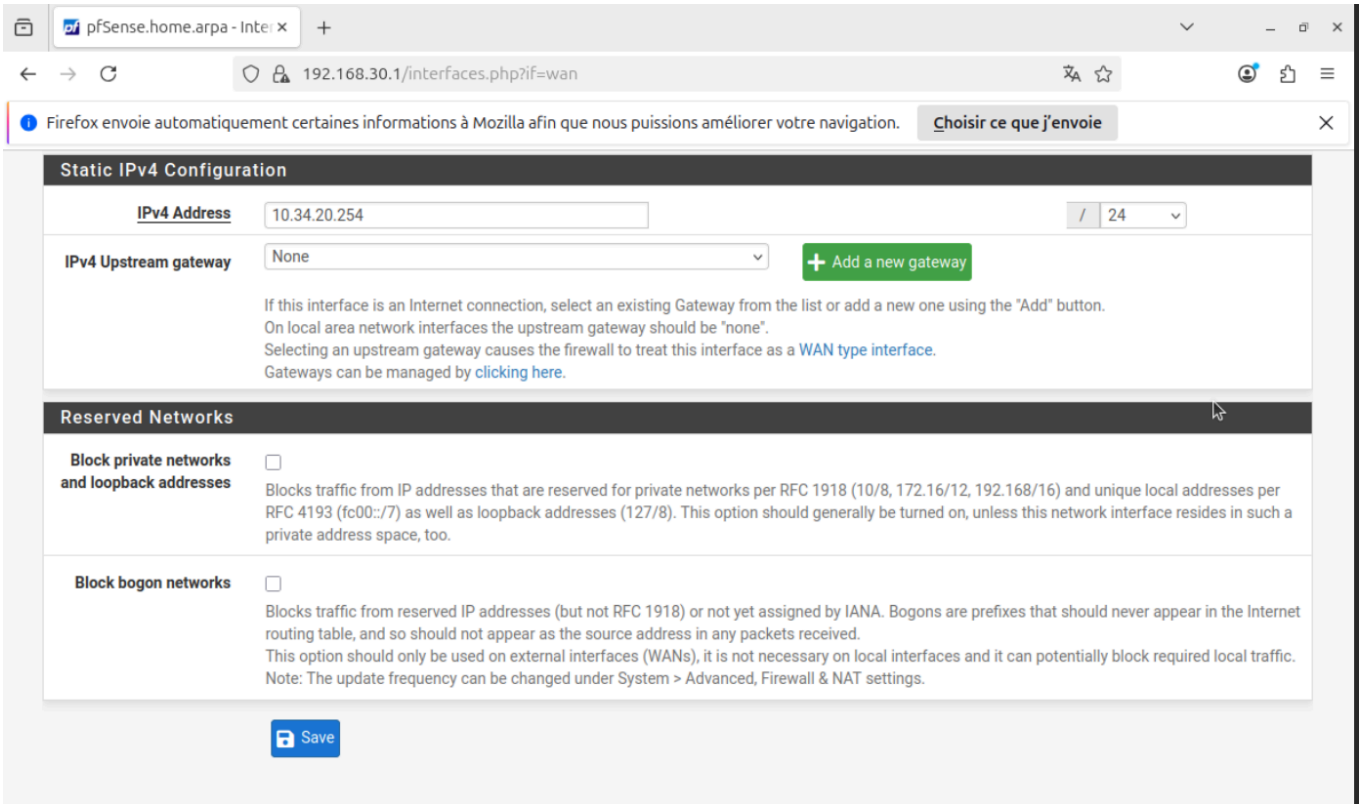
id: admin

mdp: pfsense (puis ChangeMe123!)



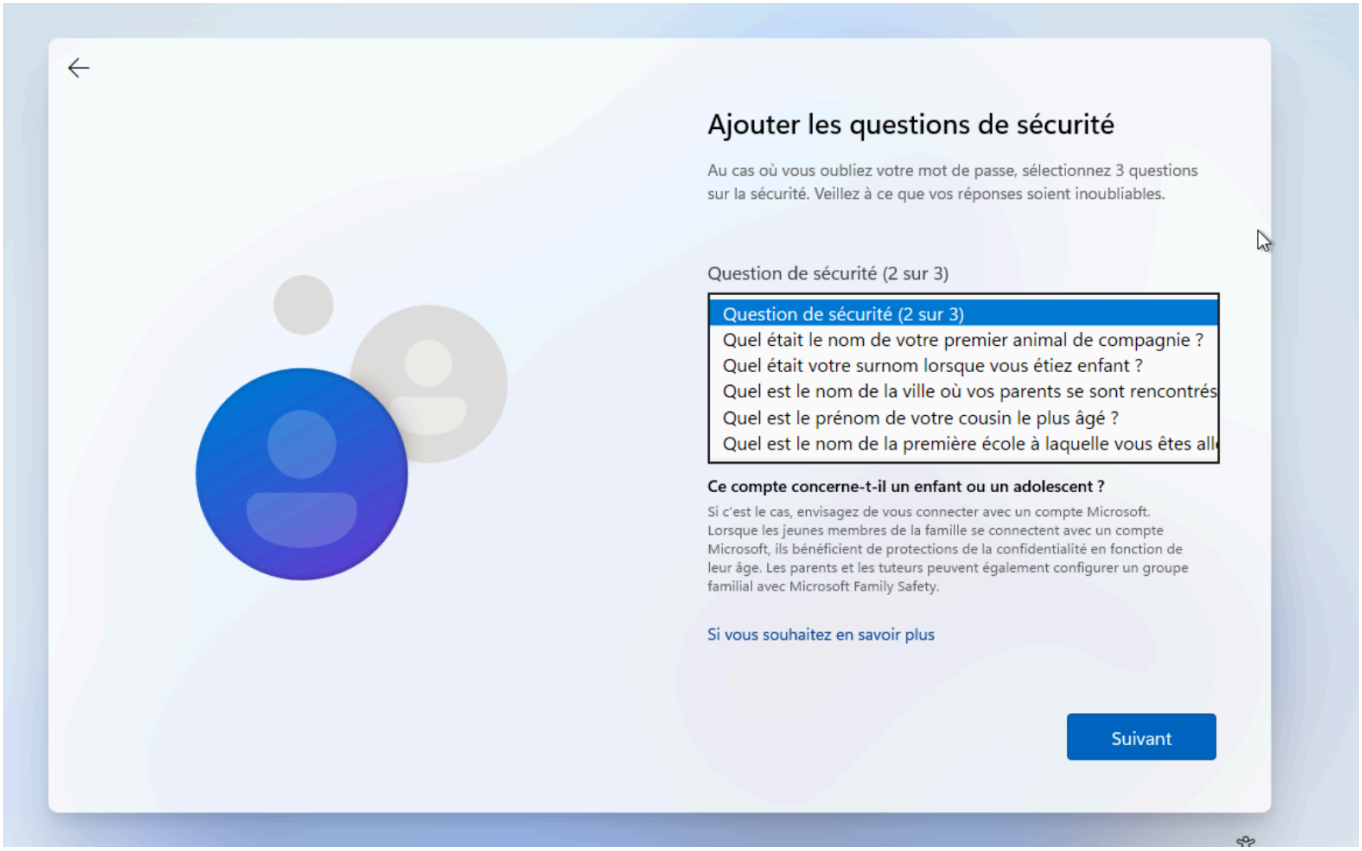


Décocher les 2 de Reserved Networks

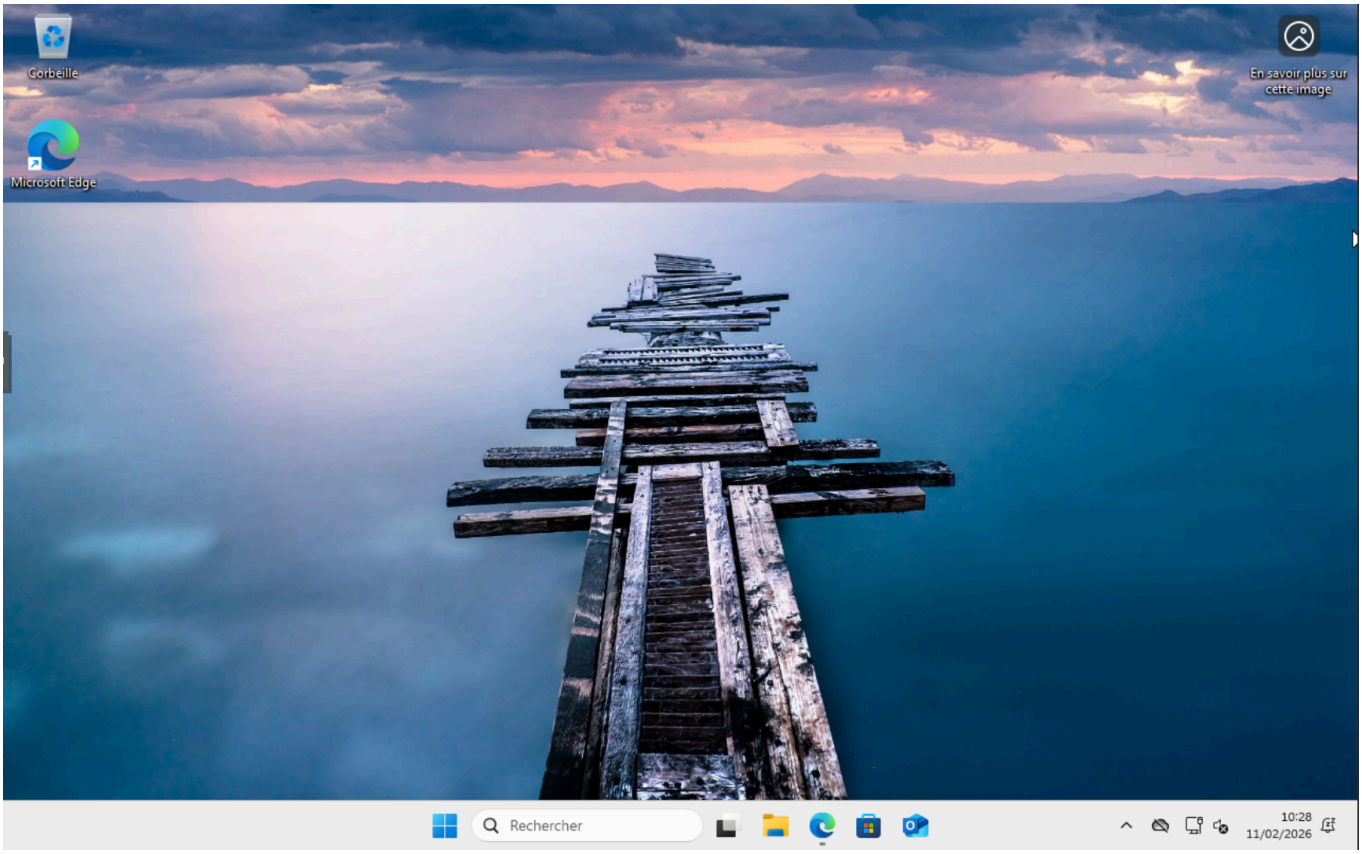


Puis créer la vm utilisateur sous windows 11

J'ai créé en me connectant à un domaine (domaine scolaire ou pro)

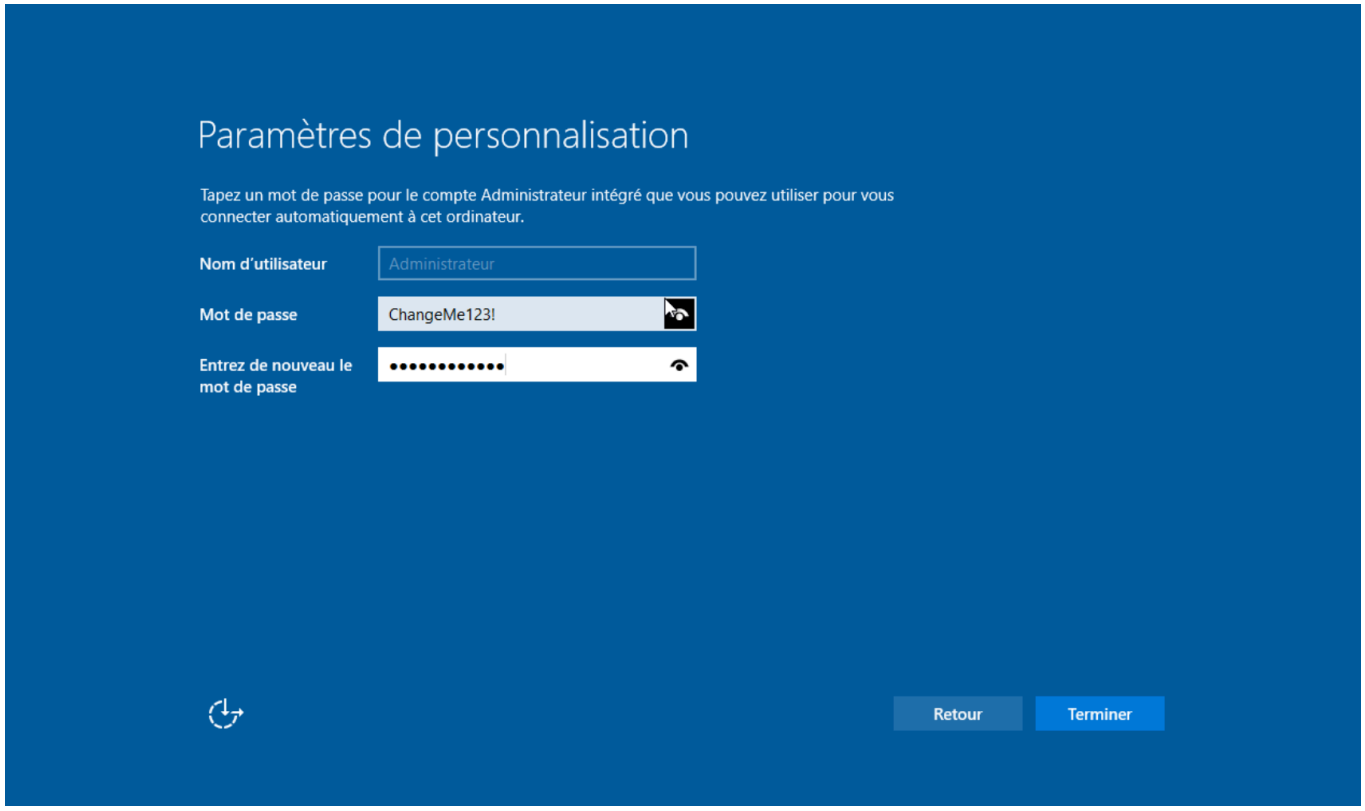


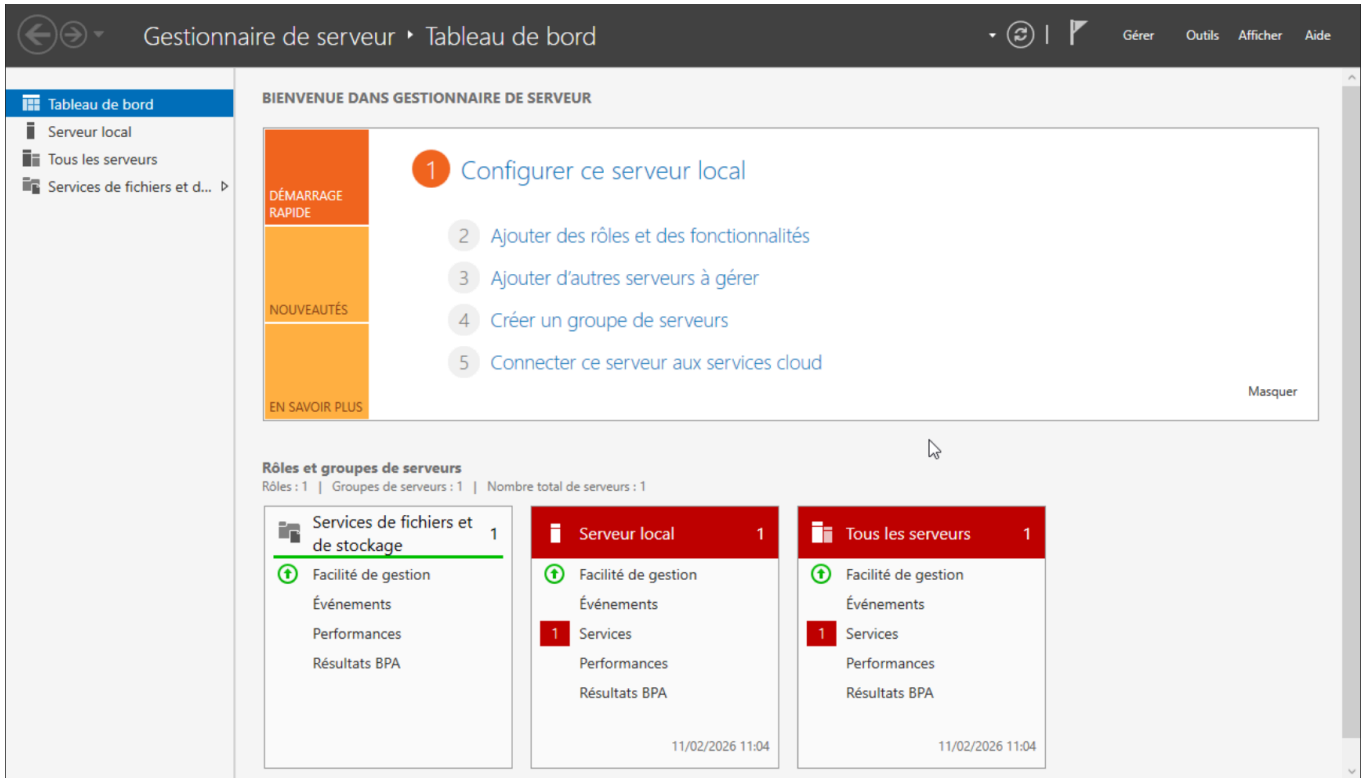
id: Sofiane
mdp: ChangeMe123!

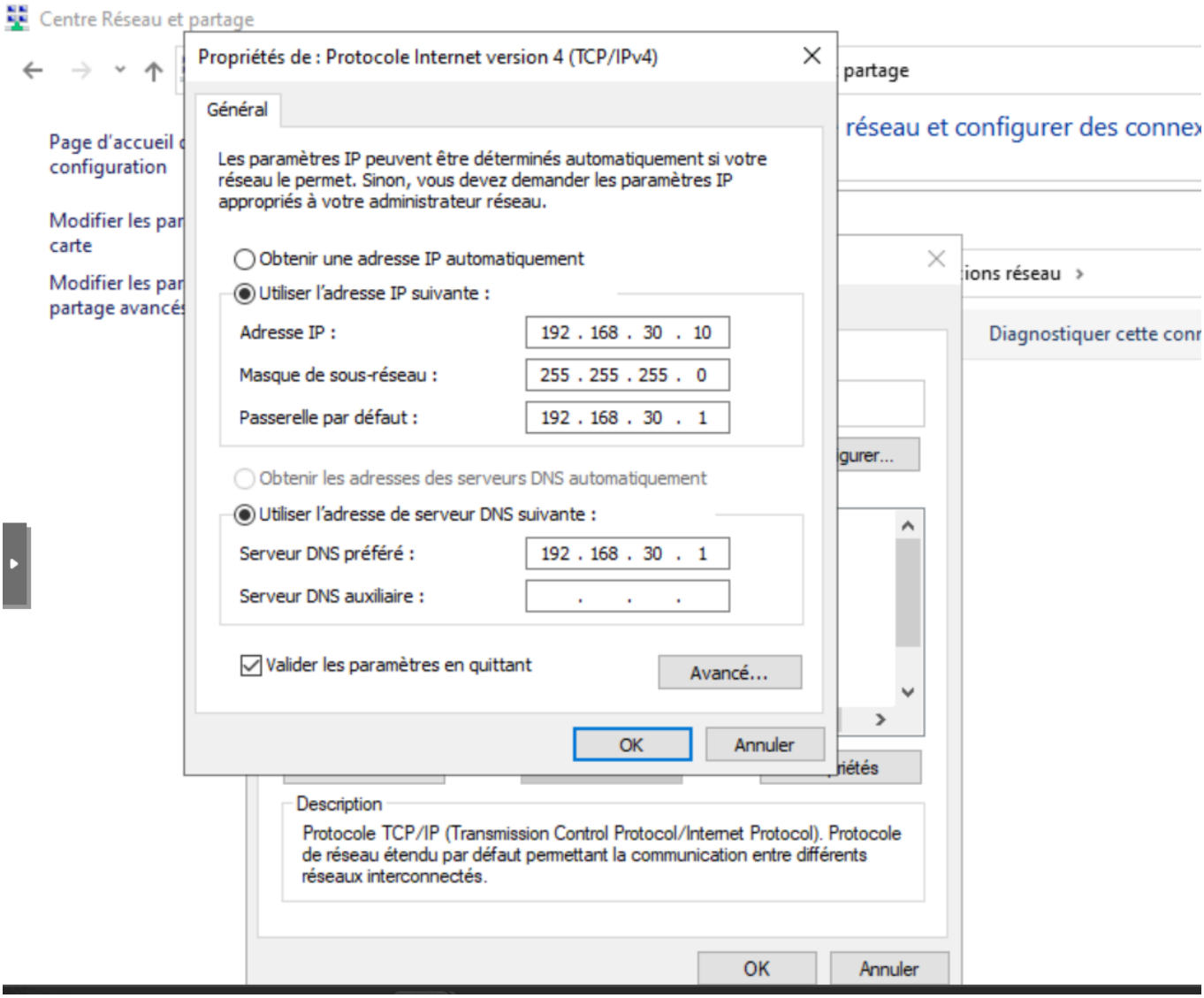


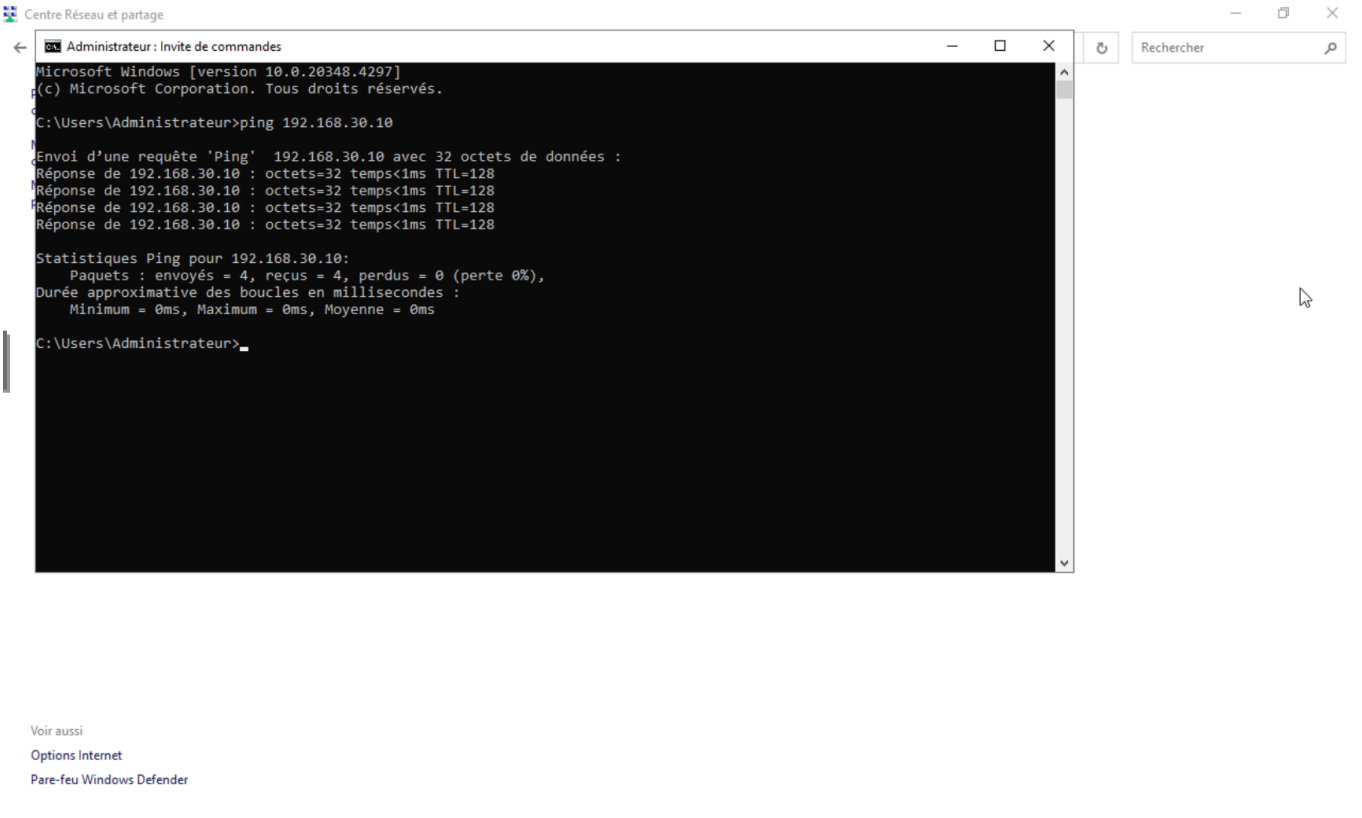
nom du pc: ordi

Puis l'AD a été créé en utilisant l'iso de sysprep windows server:

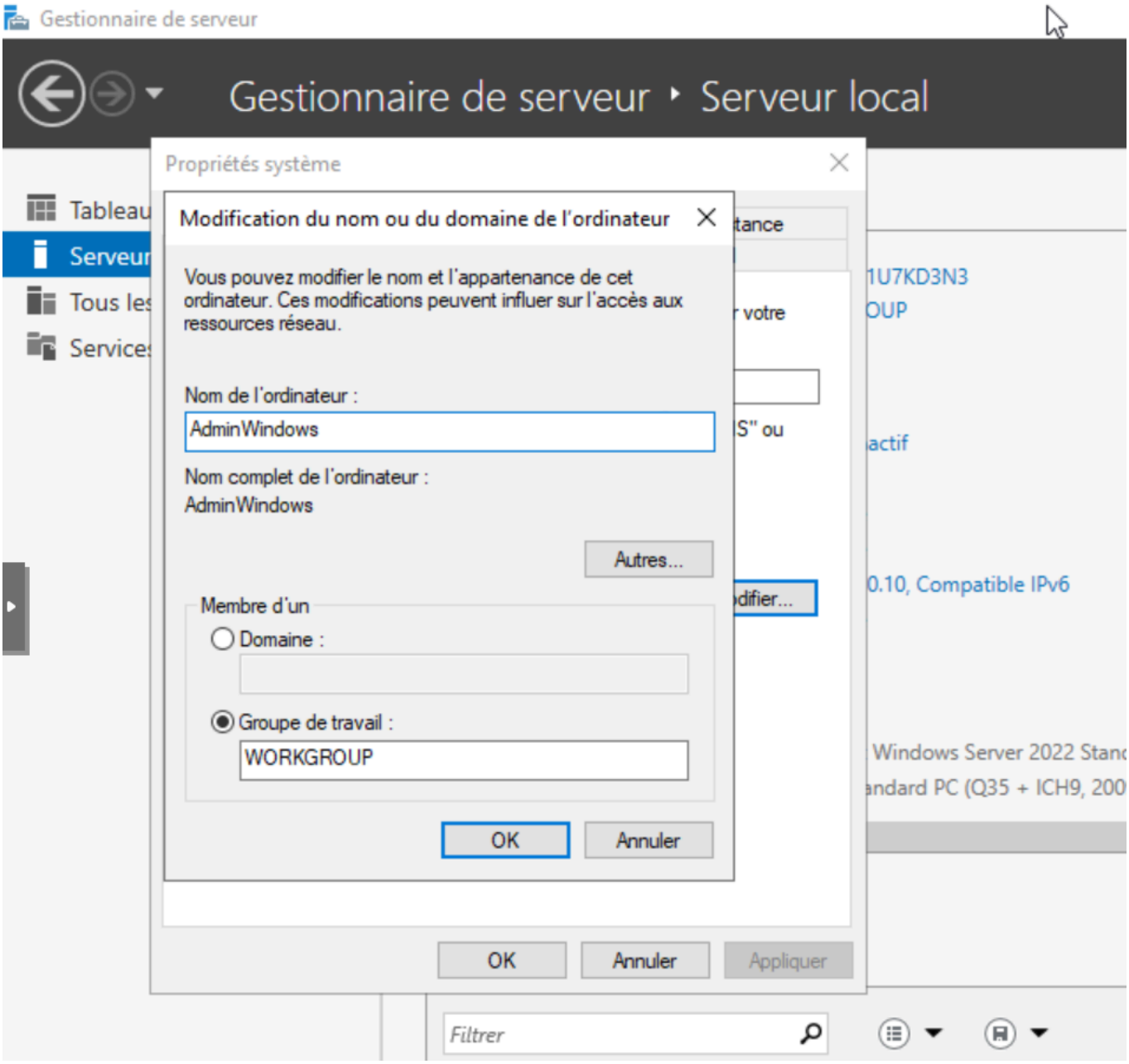


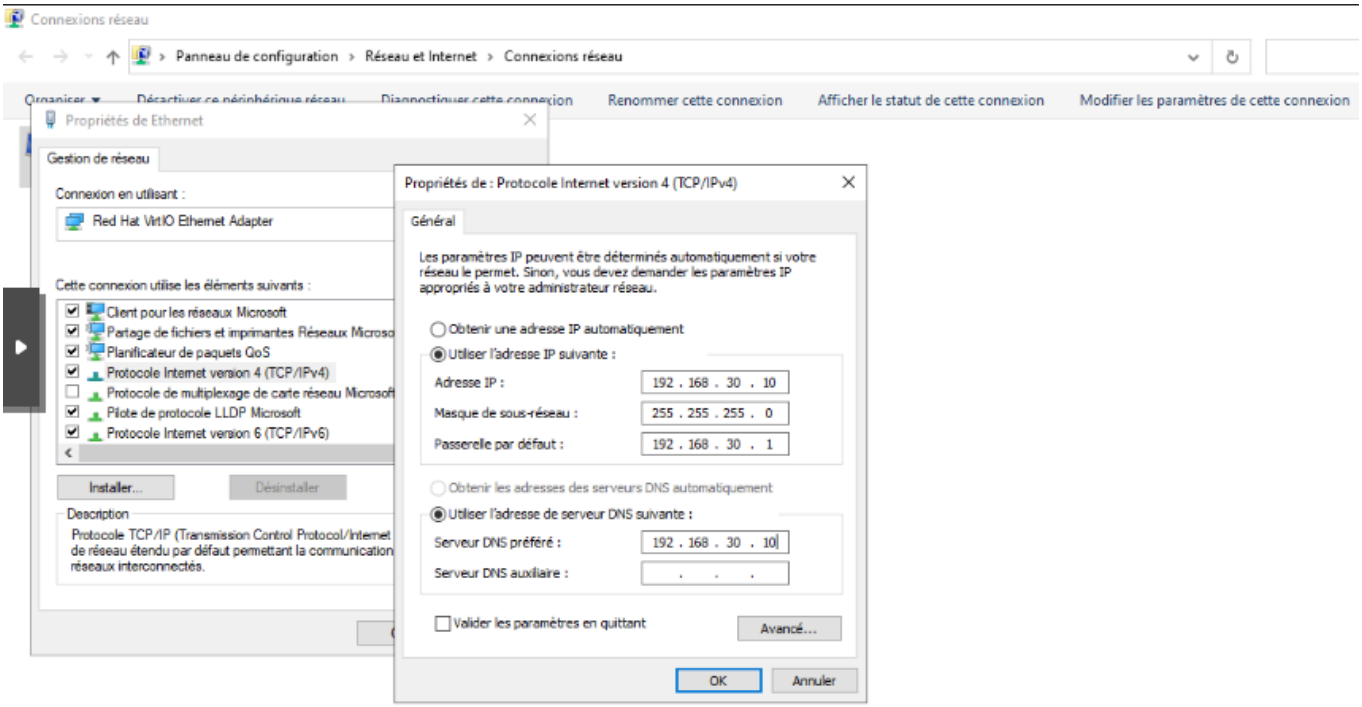



Centre Réseau et partage
Propriétés de : Protocole Internet version 4 (TCP/IPv4)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP : 192 . 168 . 30 . 10
Masque de sous-réseau : 255 . 255 . 255 . 0
Passerelle par défaut : 192 . 168 . 30 . 1
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré : 192 . 168 . 30 . 1
Serveur DNS auxiliaire :
Valider les paramètres en quittant
Avancé...
OK
Annuler
Description
Protocole TCP/IP (Transmission Control Protocol/Internet Protocol). Protocole de réseau étendu par défaut permettant la communication entre différents réseaux interconnectés.
OK
Annuler

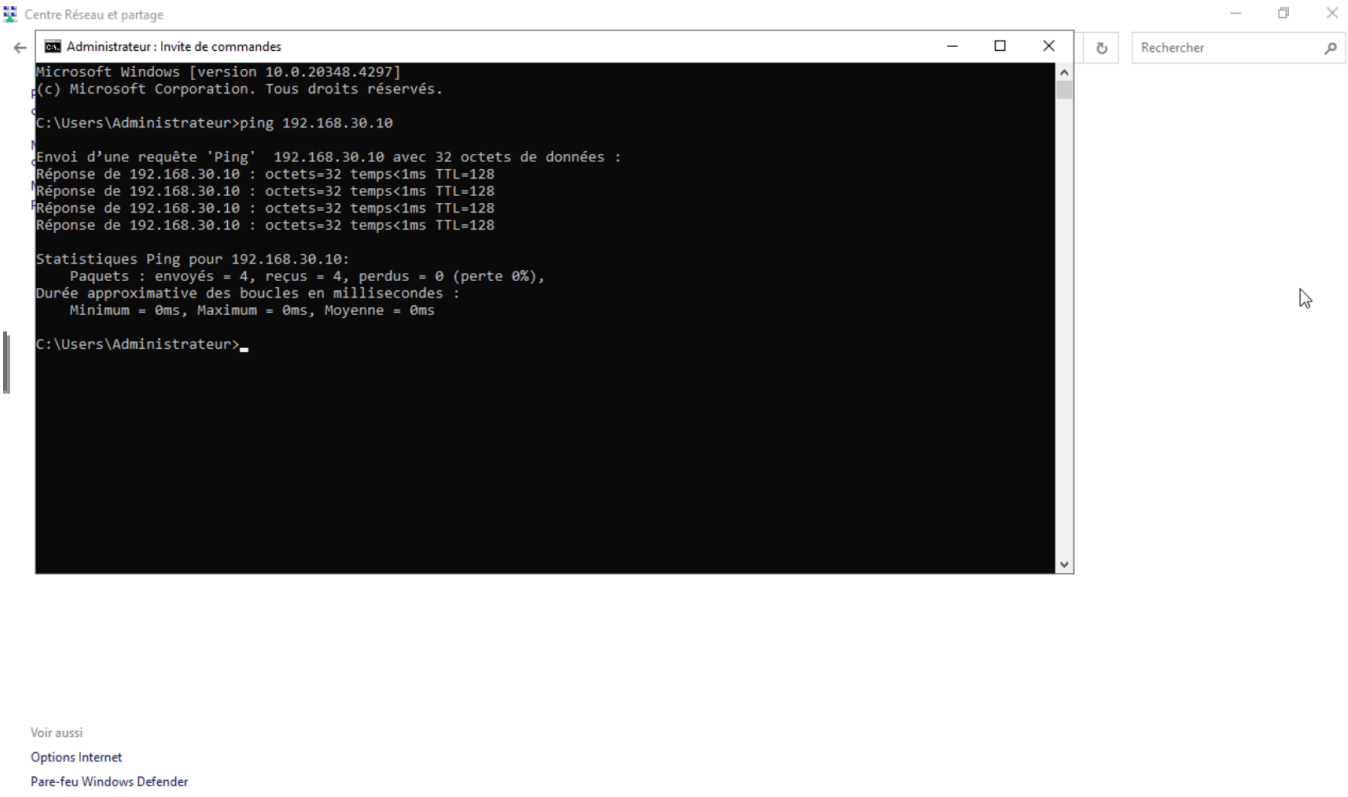

Centre Réseau et partage
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.20348.4297]
(c) Microsoft Corporation. Tous droits réservés.
C:\Users\Administrateur>ping 192.168.30.10
Envoi d'une requête 'Ping' 192.168.30.10 avec 32 octets de données :
Réponse de 192.168.30.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.30.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.30.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.30.10 : octets=32 temps<1ms TTL=128
Statistiques Ping pour 192.168.30.10:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
C:\Users\Administrateur>
Rechercher
Voir aussi
Options Internet
Pare-feu Windows Defender

J'ai renommé la machine puis redémarré la machine afin que les modifications soient prises en compte





Après vérification en ping on peut voir que ça fonctionne:



Sur **le serveur AD**, le **DNS préféré doit être la même IP que lui**, donc :

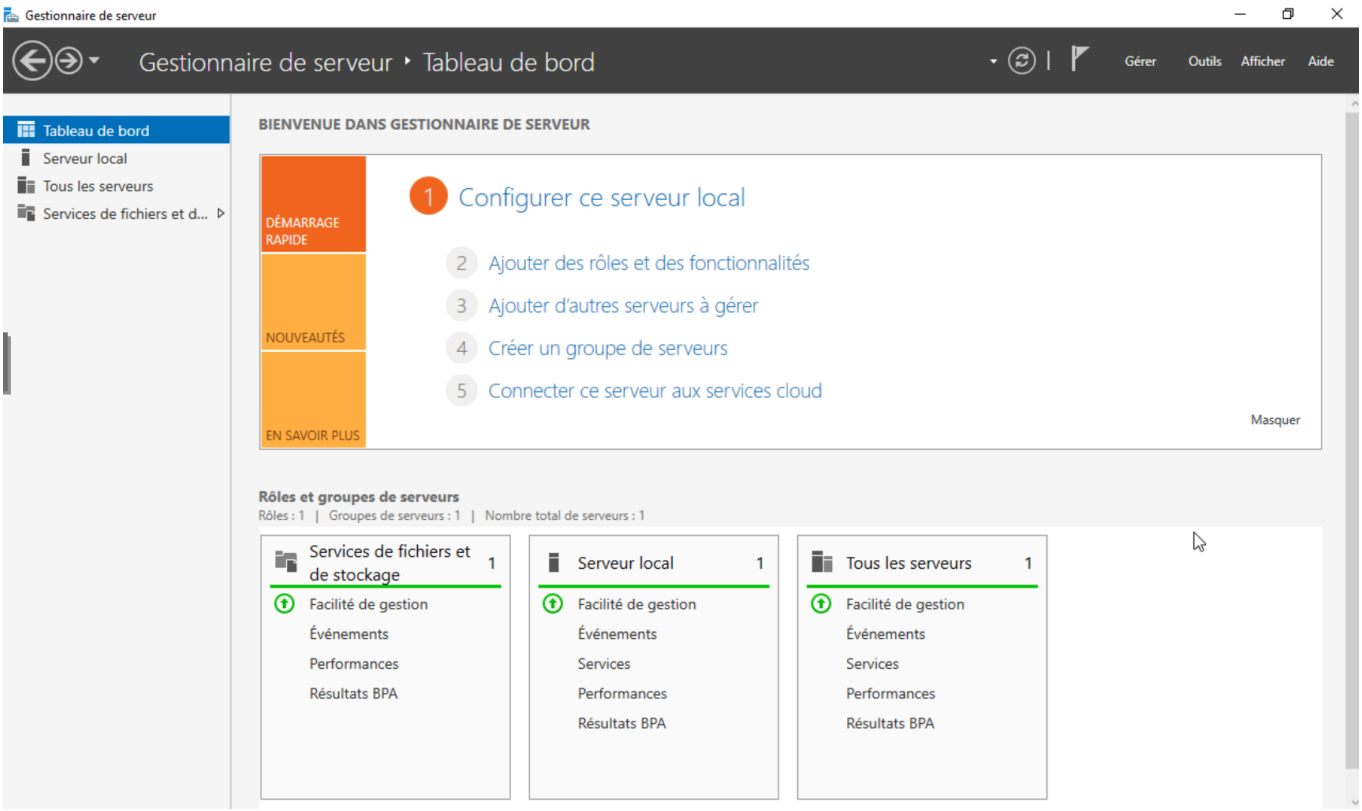
- **IP serveur AD** : `192.168.30.10`

- **DNS préféré** : `192.168.30.10`

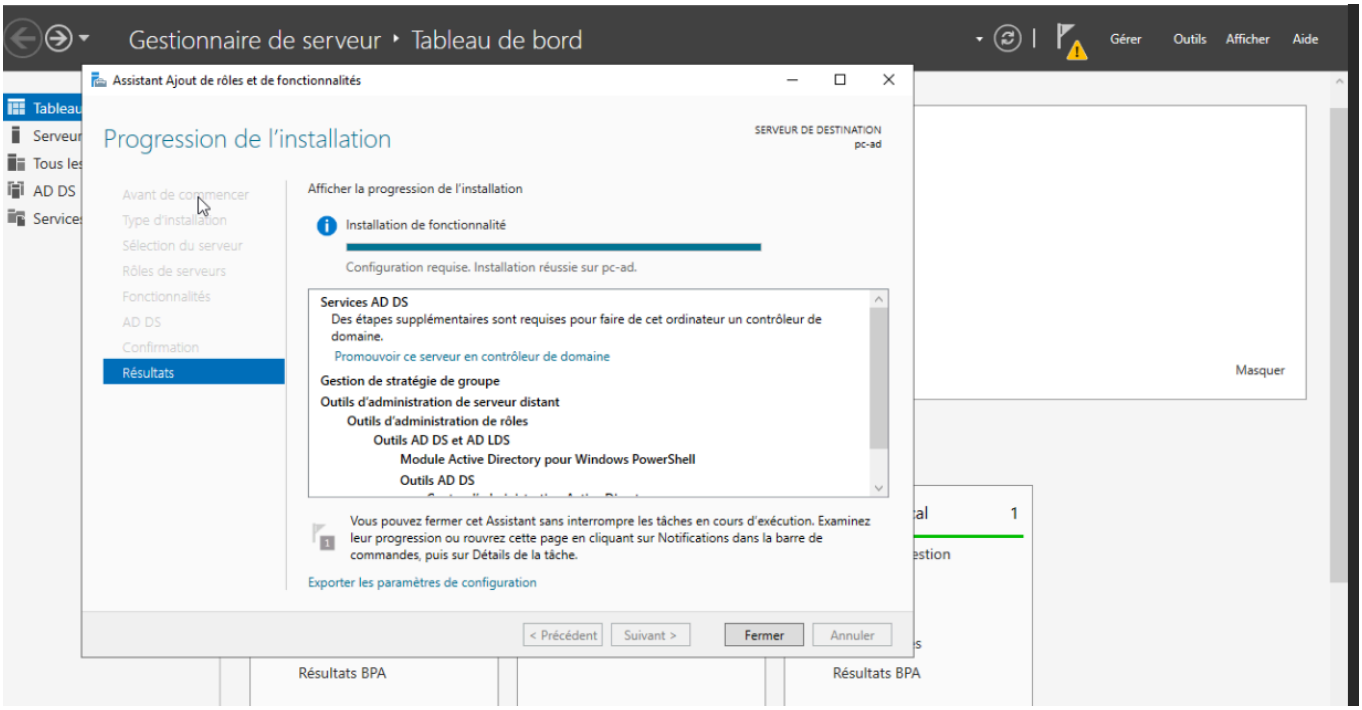
Pourquoi ?
Parce que quand il sera contrôleur de domaine, **c'est lui qui va fournir le DNS du domaine**.

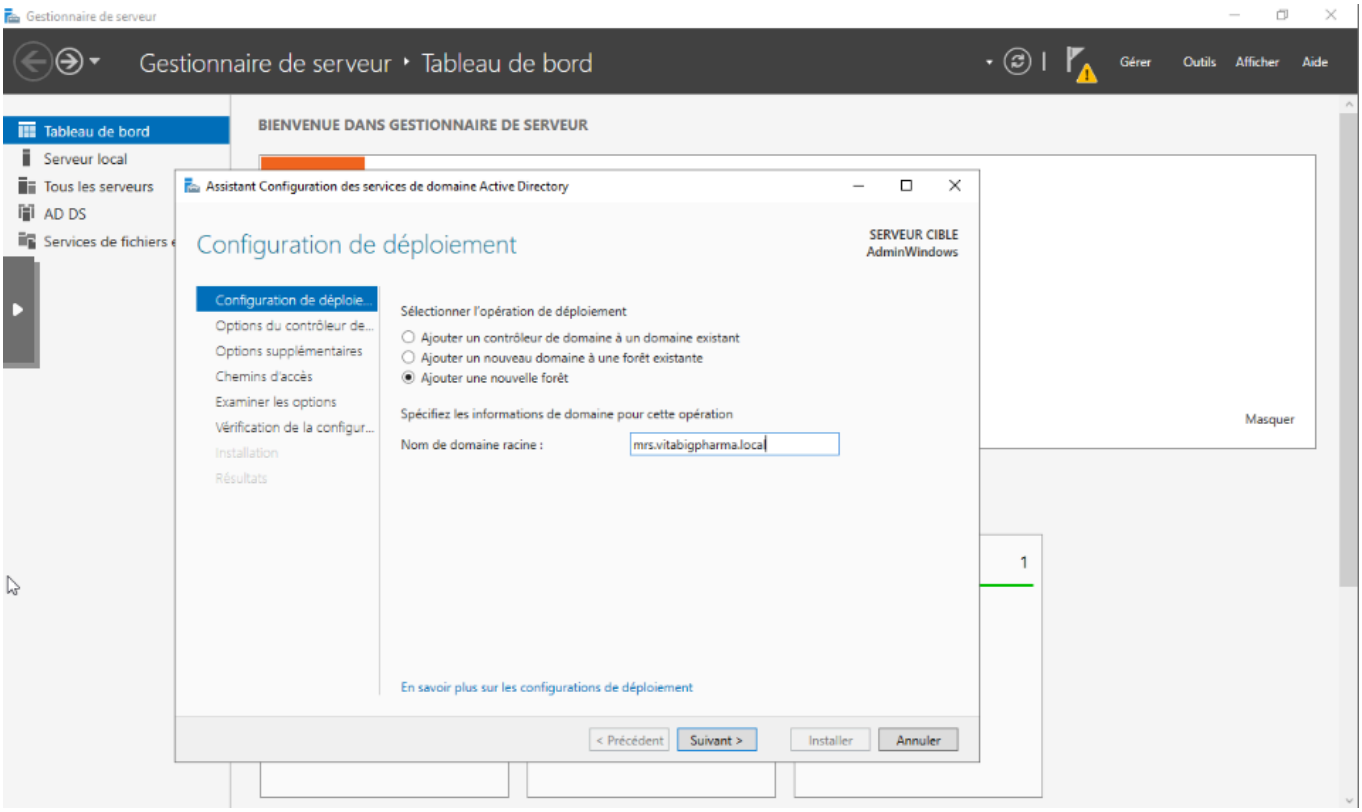
La passerelle reste bien :

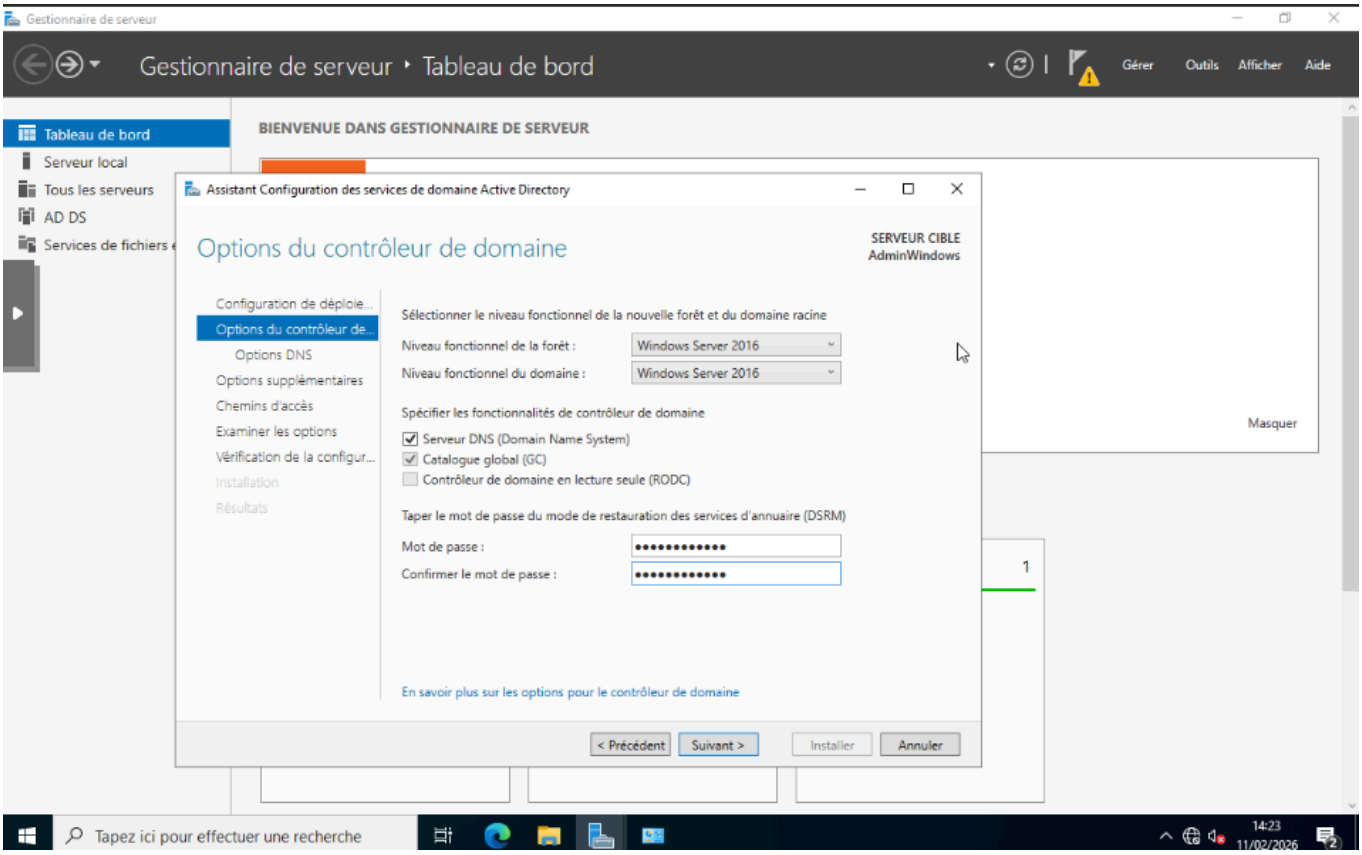
- **Passerelle** : `192.168.30.1` (pfSense LAN Marseille)

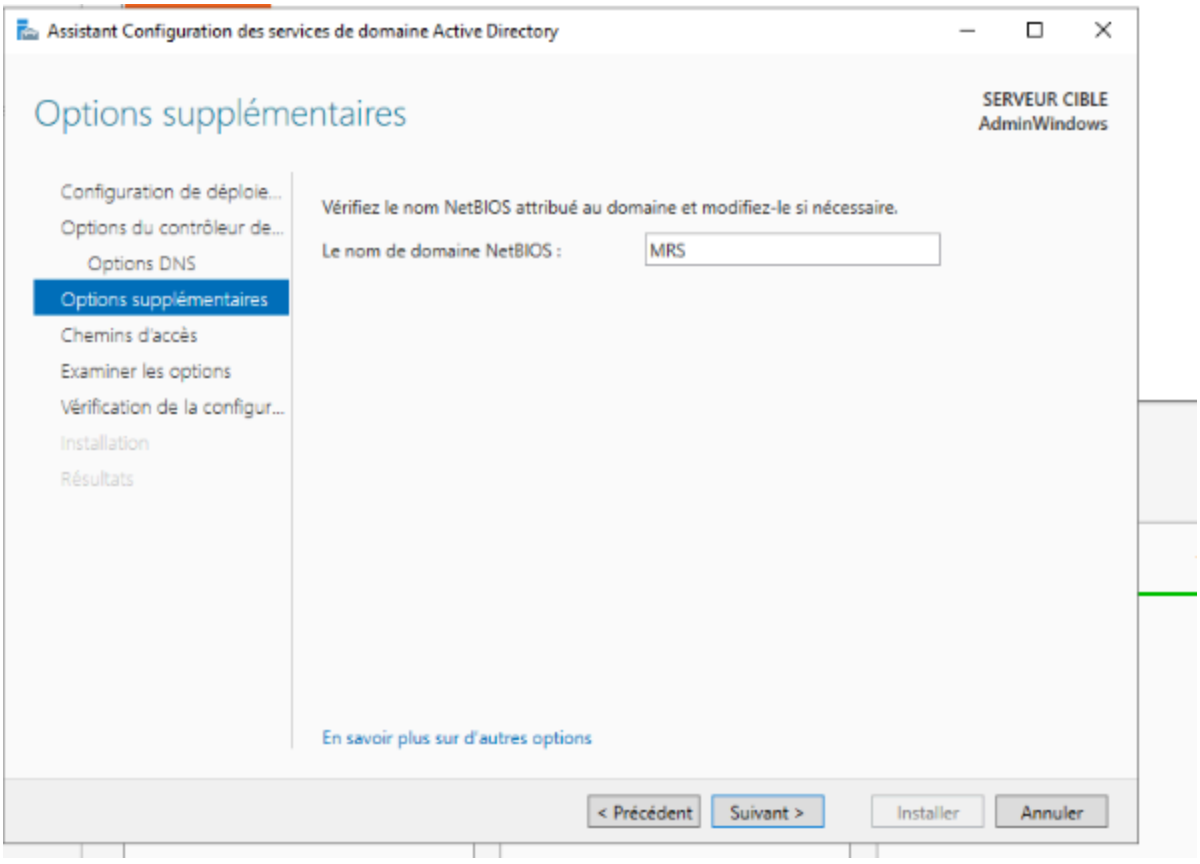


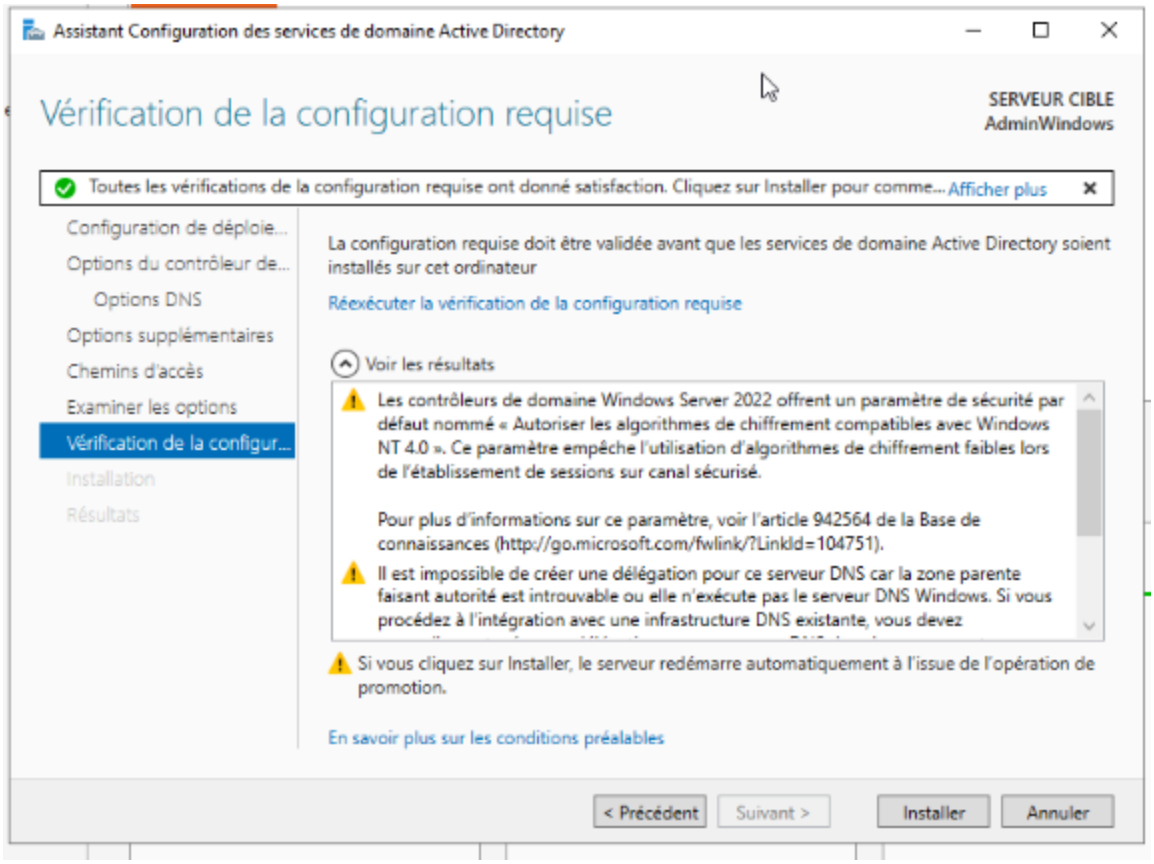
Progression AD


Gestionnaire de serveur ‣ Tableau de bord
Gérer
Outils
Afficher
Aide
Assistant Ajout de rôles et de fonctionnalités
Progression de l'installation
SERVEUR DE DESTINATION
pc-ad
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD DS
Confirmation
Résultats
Afficher la progression de l'installation
Installation de fonctionnalité
Configuration requise. Installation réussie sur pc-ad.
Services AD DS
Des étapes supplémentaires sont requises pour faire de cet ordinateur un contrôleur de domaine.
Promouvoir ce serveur en contrôleur de domaine
Gestion de stratégie de groupe
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils AD DS et AD LDS
Module Active Directory pour Windows PowerShell
Outils AD DS
Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.
Exporter les paramètres de configuration
< Précédent
Suivant >
Fermer
Annuler
Masquer
Résultats BPA
Résultats BPA

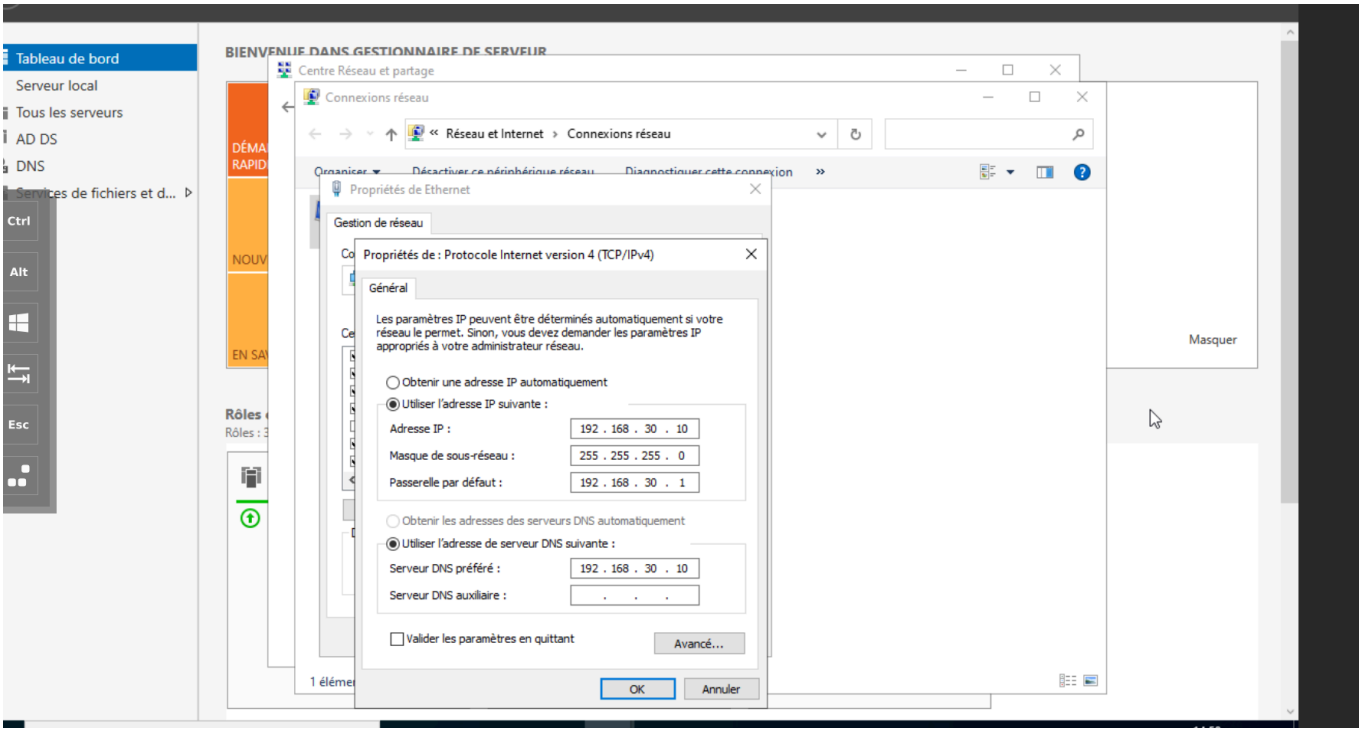

Gestionnaire de serveur
Gestionnaire de serveur ‣ Tableau de bord
Gérer
Outils
Afficher
Aide
Tableau de bord
Serveur local
Tous les serveurs
AD DS
Services de fichiers
BIENVENUE DANS GESTIONNAIRE DE SERVEUR
Assistant Configuration des services de domaine Active Directory
Configuration de déploiement
SERVEUR CIBLE
AdminWindows
Configuration de déploie...
Options du contrôleur de...
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Sélectionner l'opération de déploiement
Ajouter un contrôleur de domaine à un domaine existant
Ajouter un nouveau domaine à une forêt existante
Ajouter une nouvelle forêt
Spécifiez les informations de domaine pour cette opération
Nom de domaine racine :
mrs.vitabigpharma.local
En savoir plus sur les configurations de déploiement
< Précédent
Suivant >
Installer
Annuler
Masquer


Gestionnaire de serveur
Gestionnaire de serveur ‣ Tableau de bord
Gérer
Outils
Afficher
Aide
Tableau de bord
Serveur local
Tous les serveurs
AD DS
Services de fichiers
BIENVENUE DANS GESTIONNAIRE DE SERVEUR
Masquer
Assistant Configuration des services de domaine Active Directory
Options du contrôleur de domaine
SERVEUR CIBLE
AdminWindows
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine
Niveau fonctionnel de la forêt :
Windows Server 2016
Niveau fonctionnel du domaine :
Windows Server 2016
Spécifier les fonctionnalités de contrôleur de domaine
Serveur DNS (Domain Name System)
Catalogue global (GC)
Contrôleur de domaine en lecture seule (RODC)
Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)
Mot de passe :
Confirmer le mot de passe :
En savoir plus sur les options pour le contrôleur de domaine
< Précédent
Suivant >
Installer
Annuler
Tapez ici pour effectuer une recherche
14:23
11/02/2026

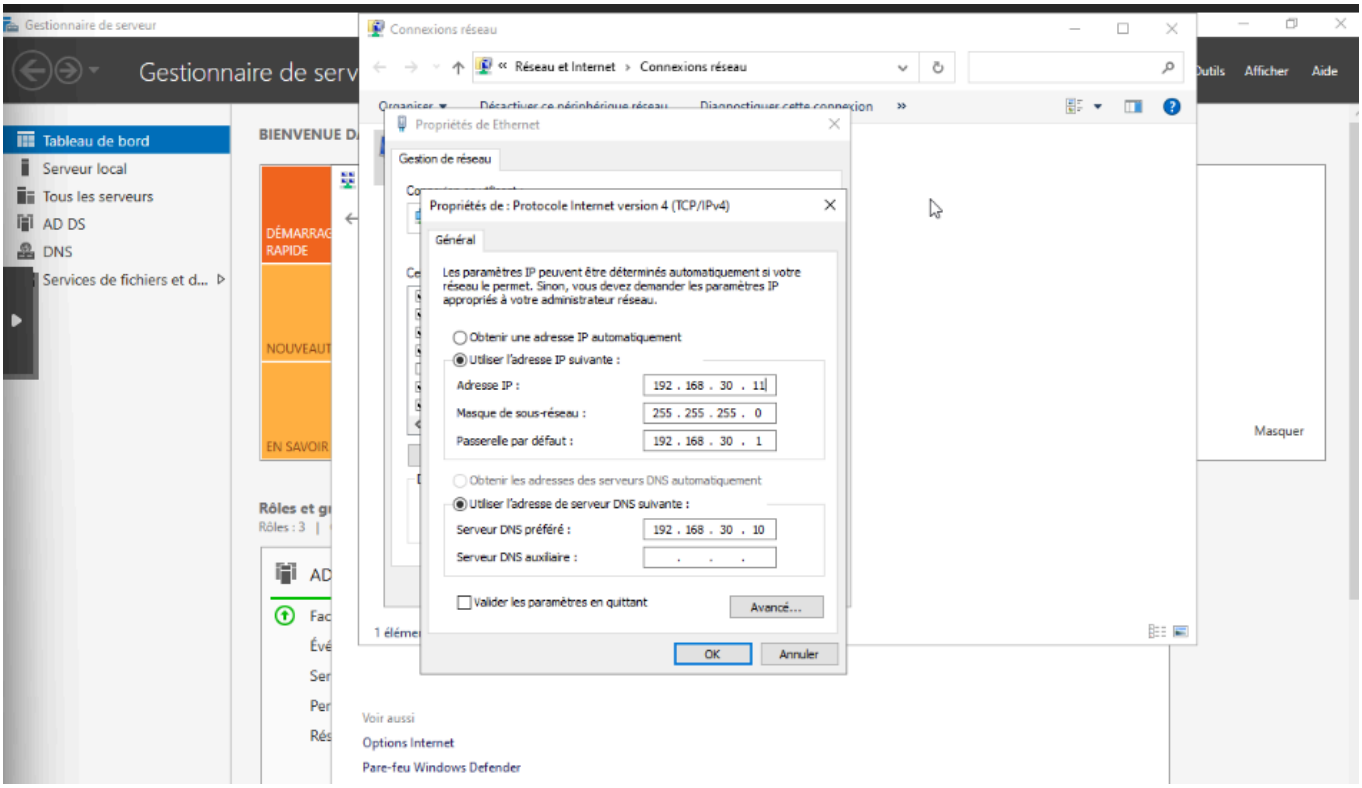

Assistant Configuration des services de domaine Active Directory
Options supplémentaires
SERVEUR CIBLE
AdminWindows
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.
Le nom de domaine NetBIOS :
MRS
En savoir plus sur d'autres options
< Précédent
Suivant >
Installer
Annuler

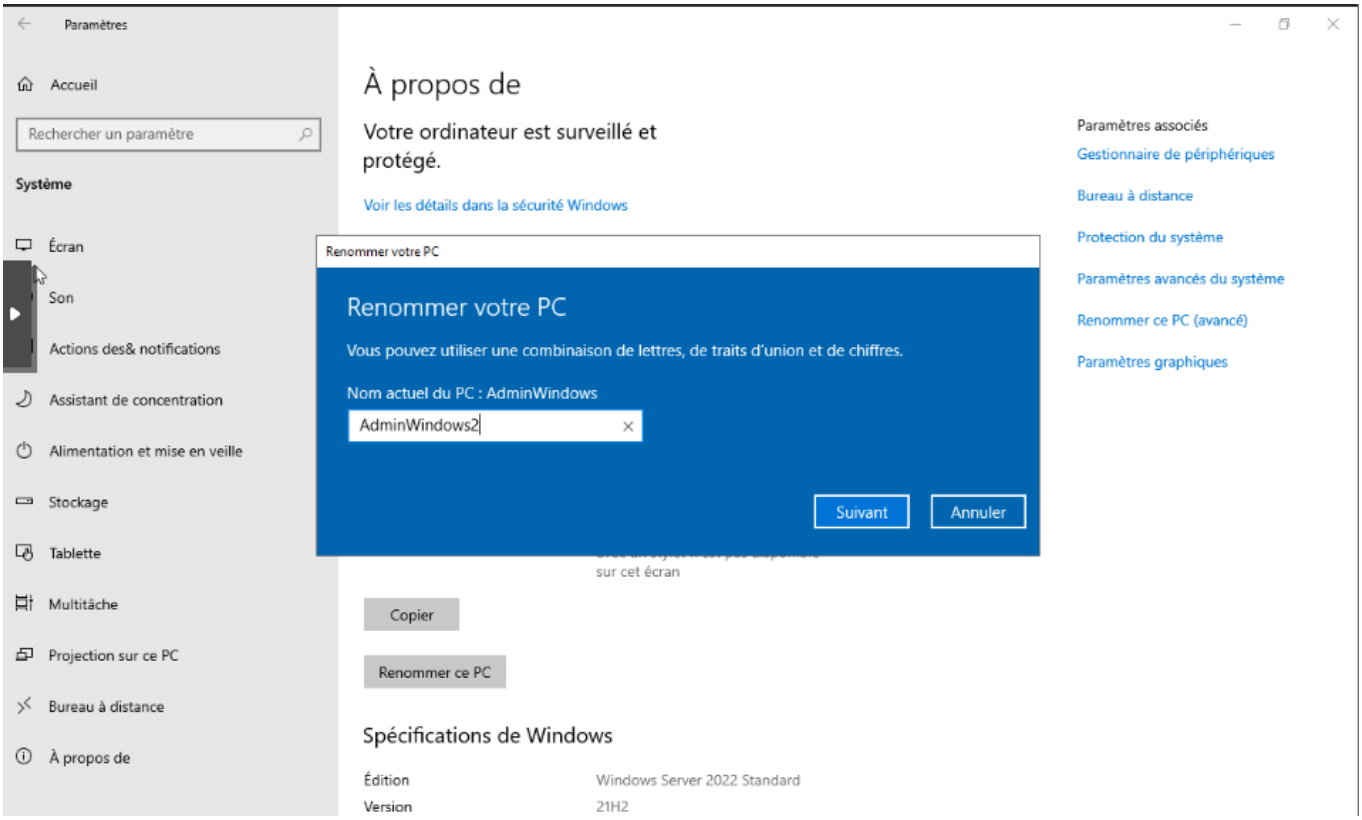


(petit changement avec ajout de dns sur AD1):

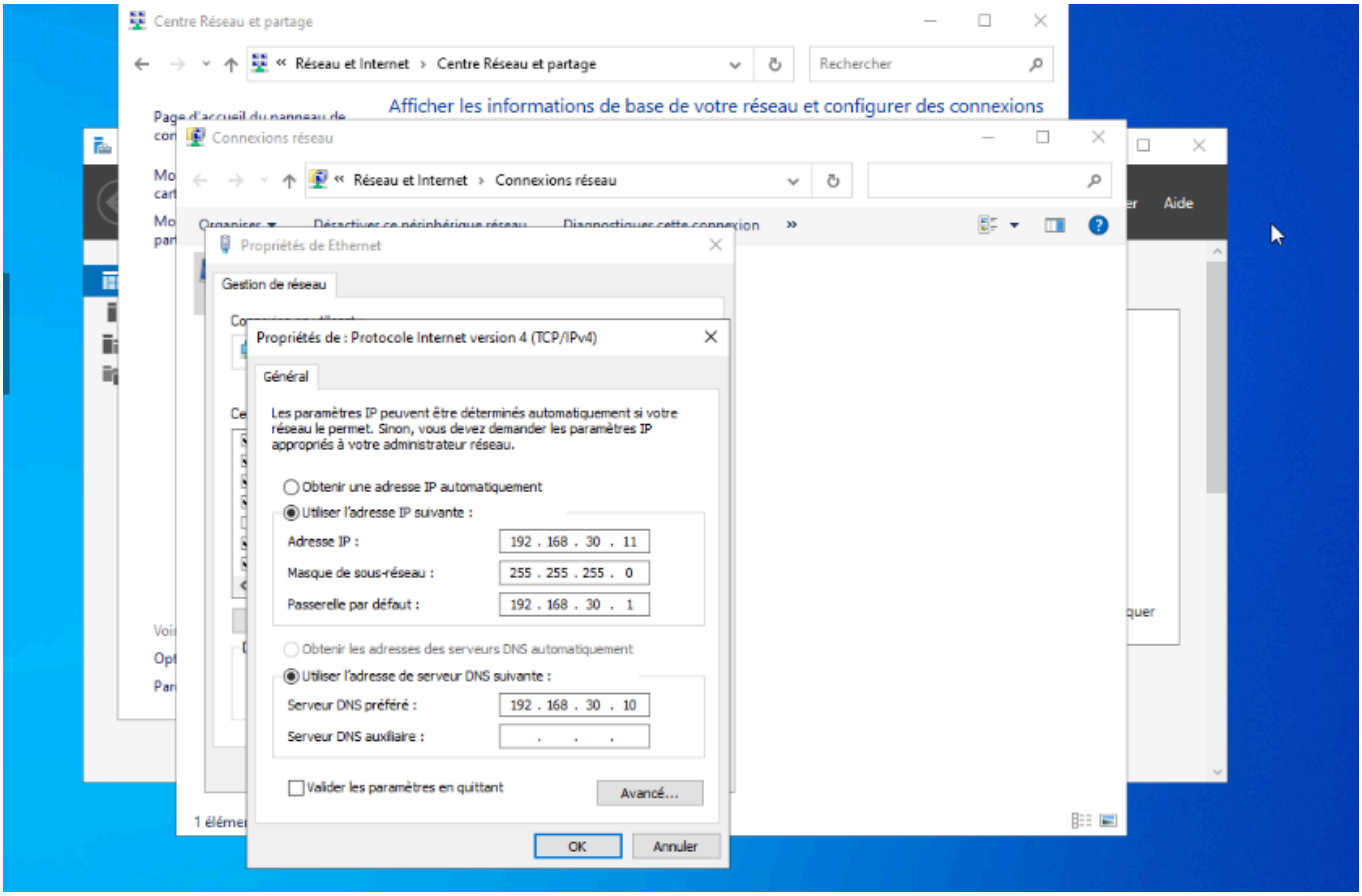


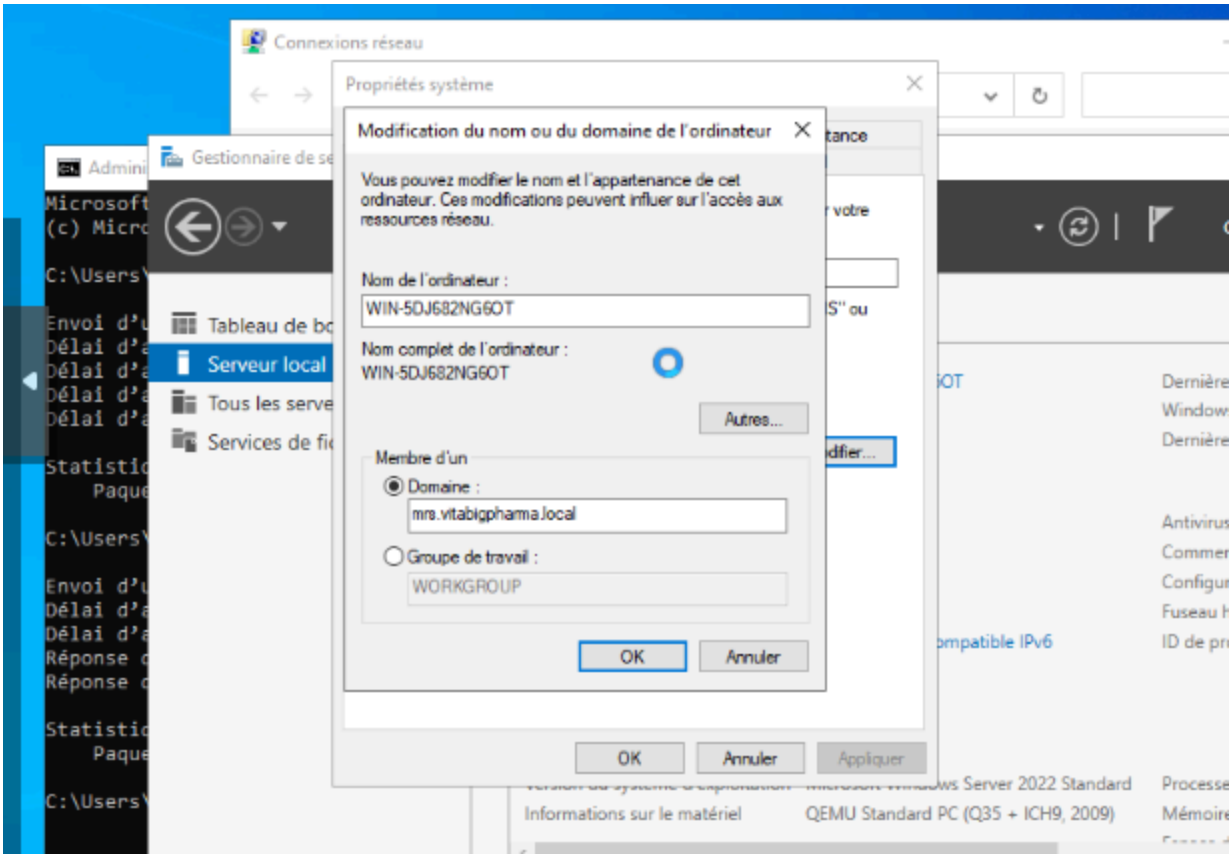
puis cloner pour ad 2:

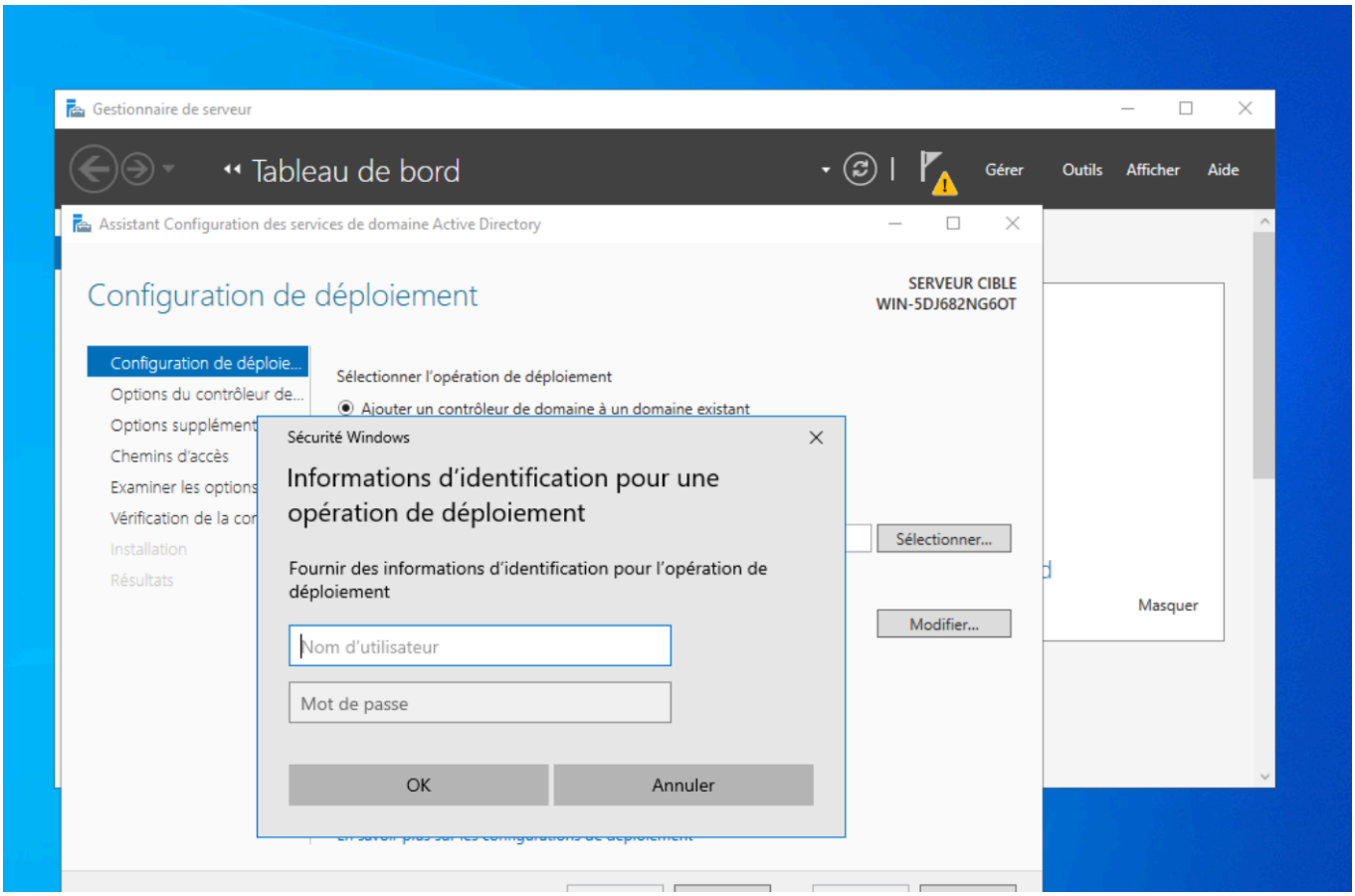




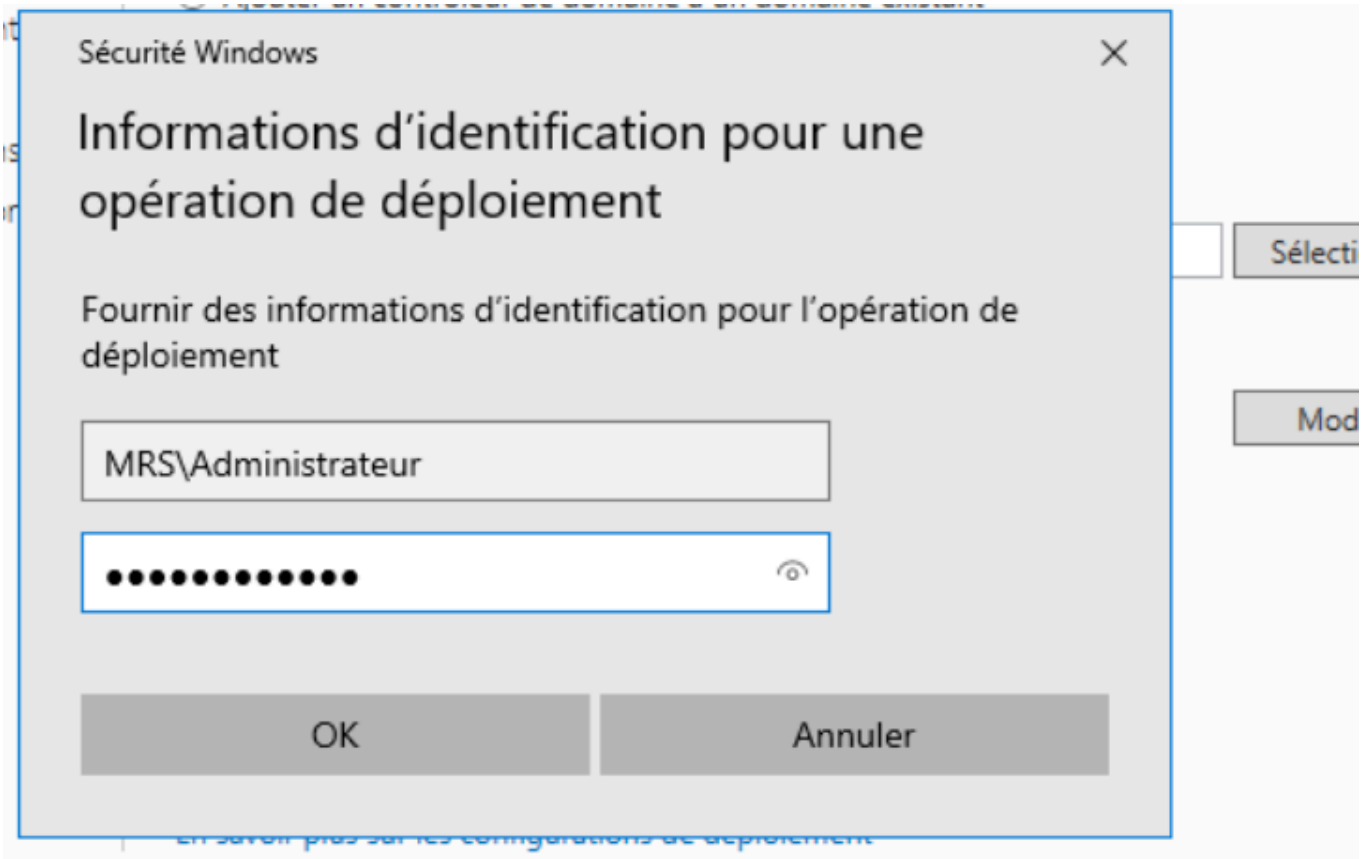
AD 2 :


Centre Réseau et partage
Réseau et Internet › Centre Réseau et partage
Rechercher
Afficher les informations de base de votre réseau et configurer des connexions
Connexions réseau
Réseau et Internet › Connexions réseau
Propriétés de Ethernet
Gestion de réseau
Propriétés de : Protocole Internet version 4 (TCP/IPv4)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP : 192 . 168 . 30 . 11
Masque de sous-réseau : 255 . 255 . 255 . 0
Passerelle par défaut : 192 . 168 . 30 . 1
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré : 192 . 168 . 30 . 10
Serveur DNS auxiliaire :
Valider les paramètres en quittant
Avancé...
OK
Annuler

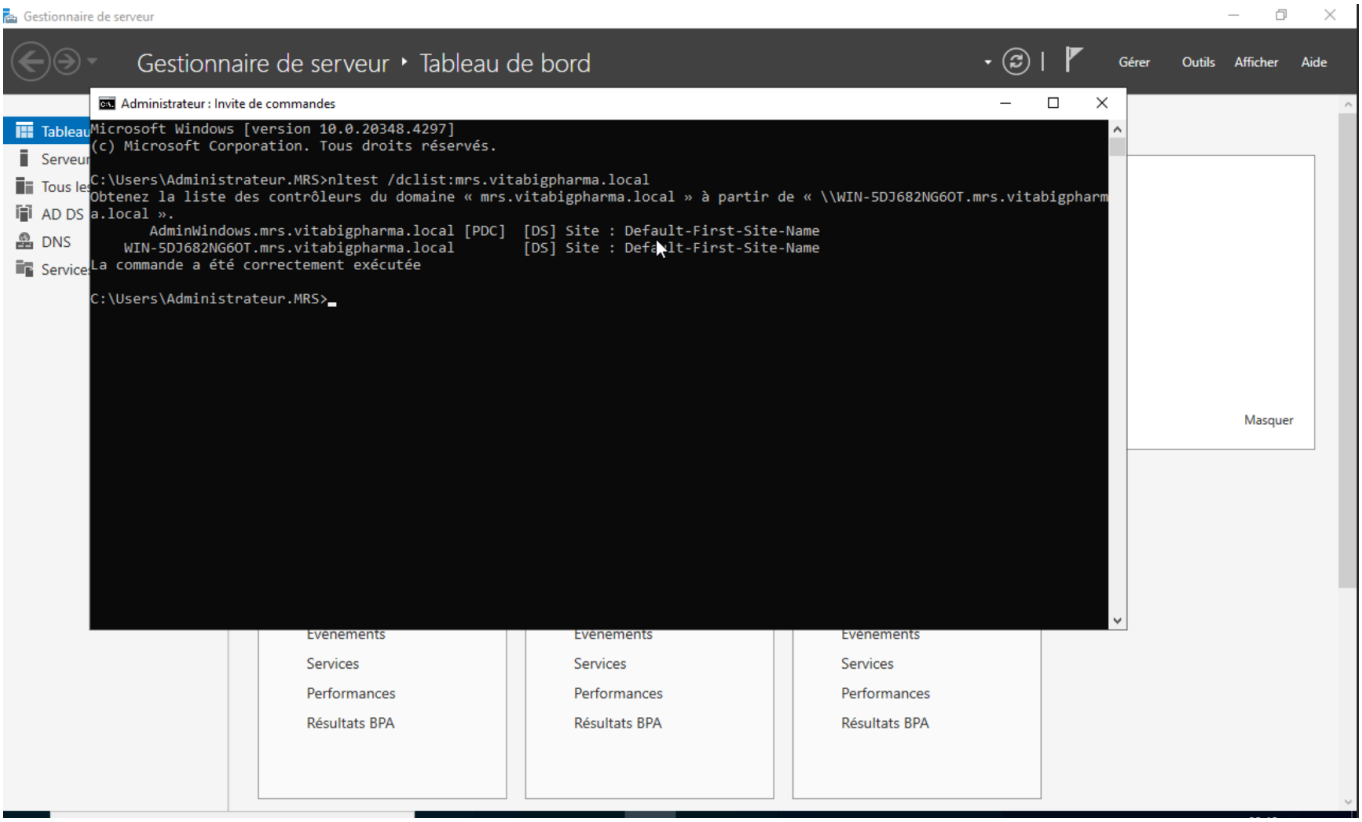

Connexions réseau
Propriétés système
Modification du nom ou du domaine de l'ordinateur
Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influer sur l'accès aux ressources réseau.
Nom de l'ordinateur :
WIN-5DJ682NG6OT
Nom complet de l'ordinateur :
WIN-5DJ682NG6OT
Autres...
Membre d'un
Domaine :
mrs.vitabigpharma.local
Groupe de travail :
WORKGROUP
OK
Annuler
Appliquer
Gestionnaire de serveur
Tableau de bord
Serveur local
Tous les serveurs
Services de fichiers
Informations sur le matériel
QEMU Standard PC (Q35 + ICH9, 2009)


Gestionnaire de serveur
Tableau de bord
Gérer
Outils
Afficher
Aide
Assistant Configuration des services de domaine Active Directory
Configuration de déploiement
SERVEUR CIBLE
WIN-5DJ682NG6OT
Configuration de déploie...
Options du contrôleur de...
Options supplément
Chemins d'accès
Examiner les options
Vérification de la cor
Installation
Résultats
Sélectionner l'opération de déploiement
Ajouter un contrôleur de domaine à un domaine existant
Sélectionner...
Modifier...
Masquer
Sécurité Windows
Informations d'identification pour une opération de déploiement
Fournir des informations d'identification pour l'opération de déploiement
Nom d'utilisateur
Mot de passe
OK
Annuler

AD2:

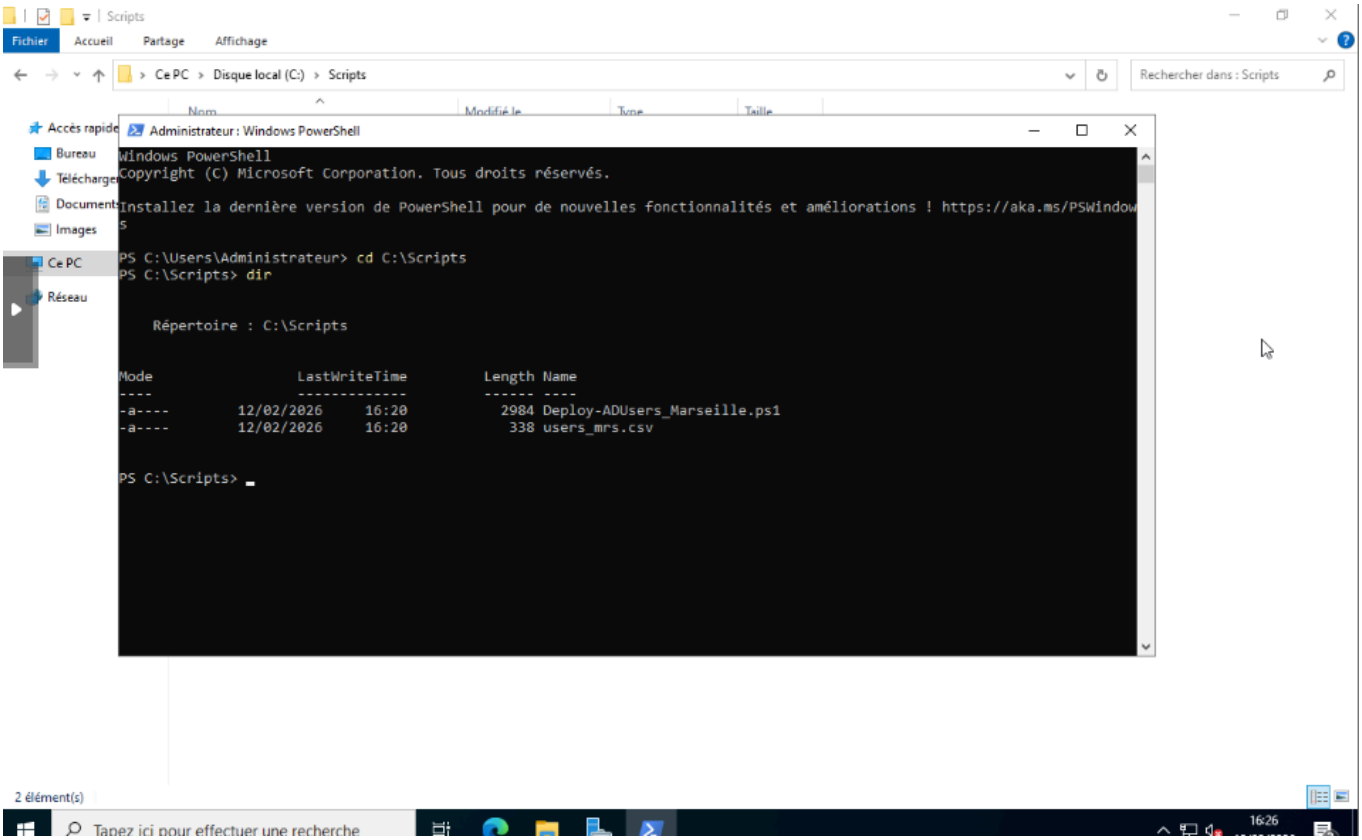

Sécurité Windows
Informations d'identification pour une opération de déploiement
Fournir des informations d'identification pour l'opération de déploiement
MRS\Administrateur
OK
Annuler

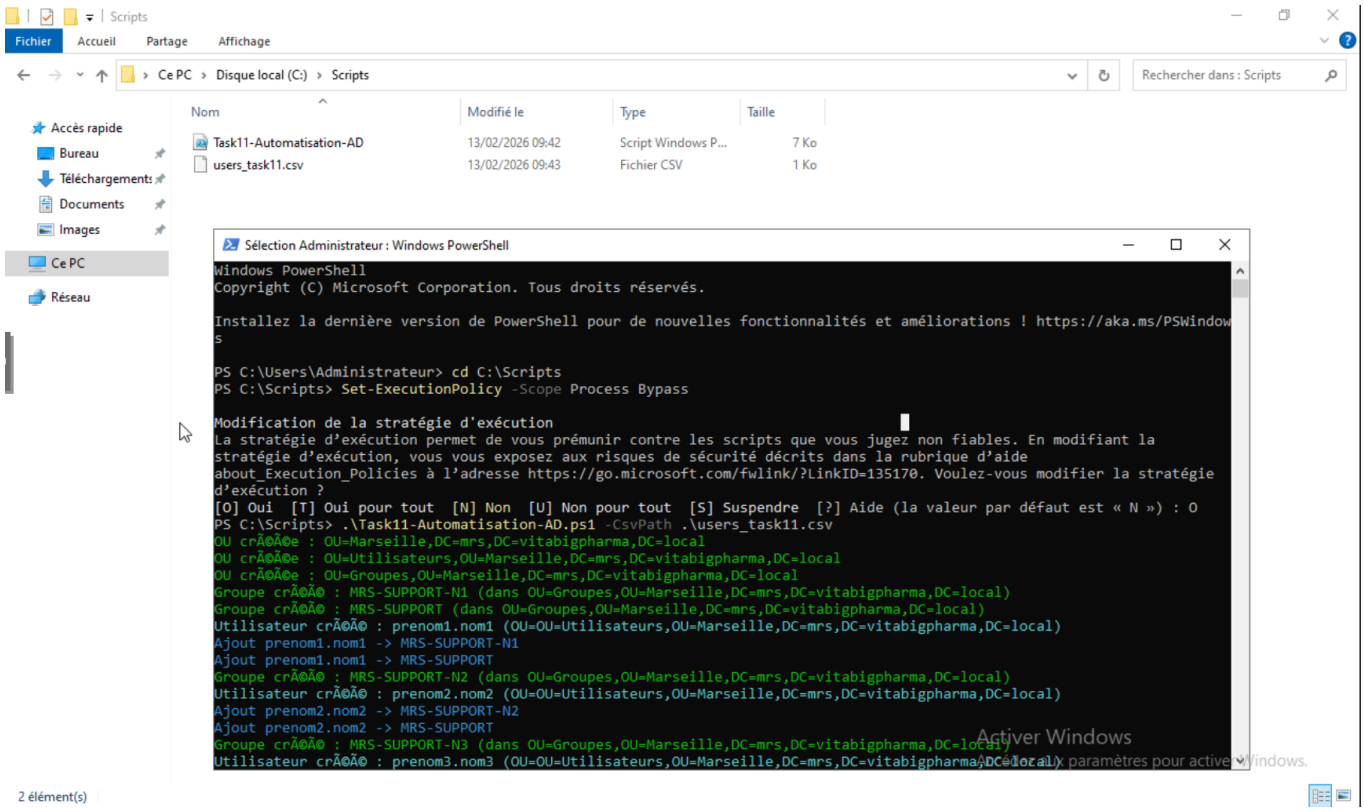
Ca fonctionne:



Déploiement des utilisateurs

Script (AD1):(création du script et csv puis dossier script)



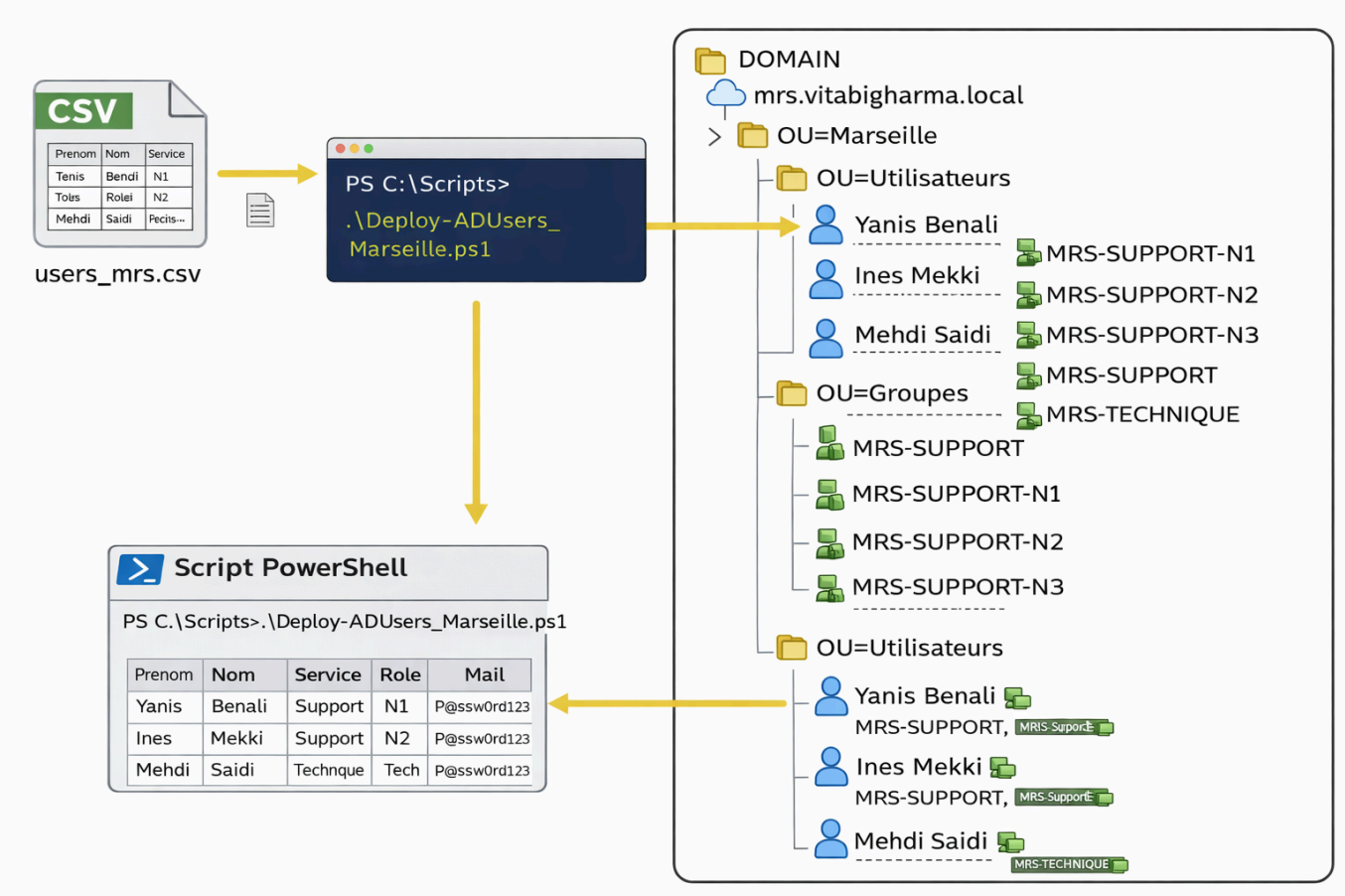


déposer les 2 scripts:

users_task11.csv

Task11-Automatisation-AD.ps1

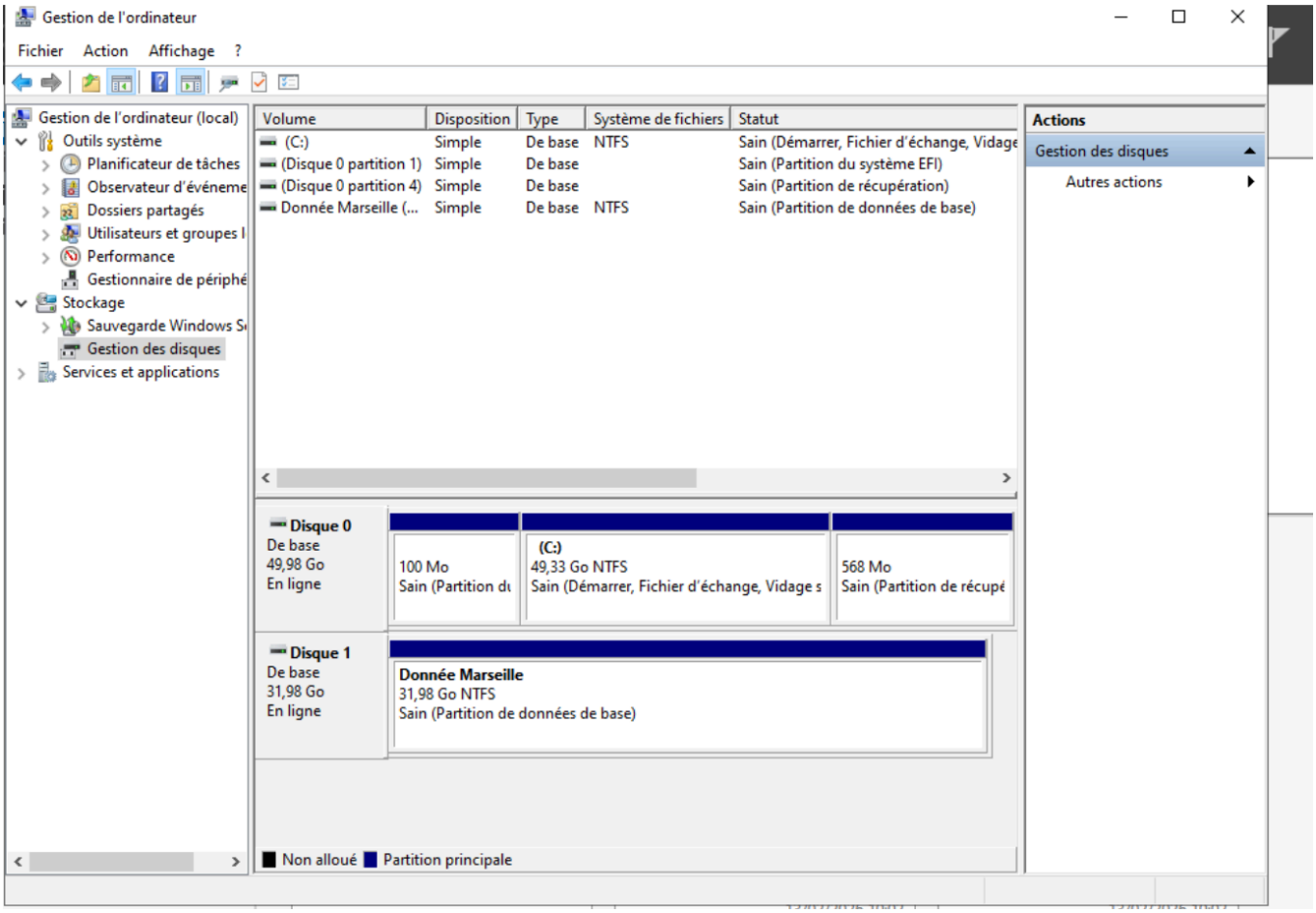
le script a été fait grâce à ce plan:



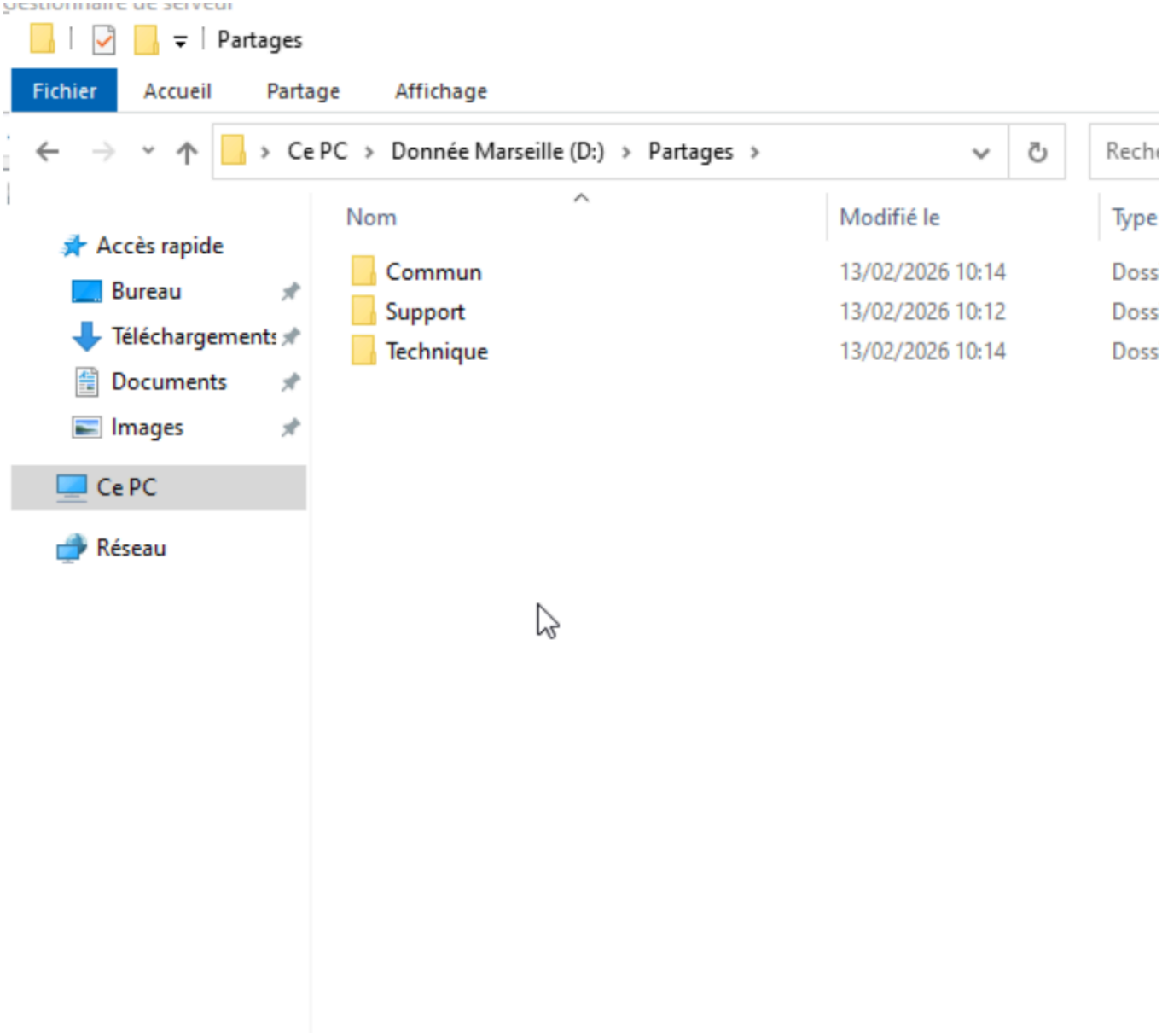
serveur de fichier:

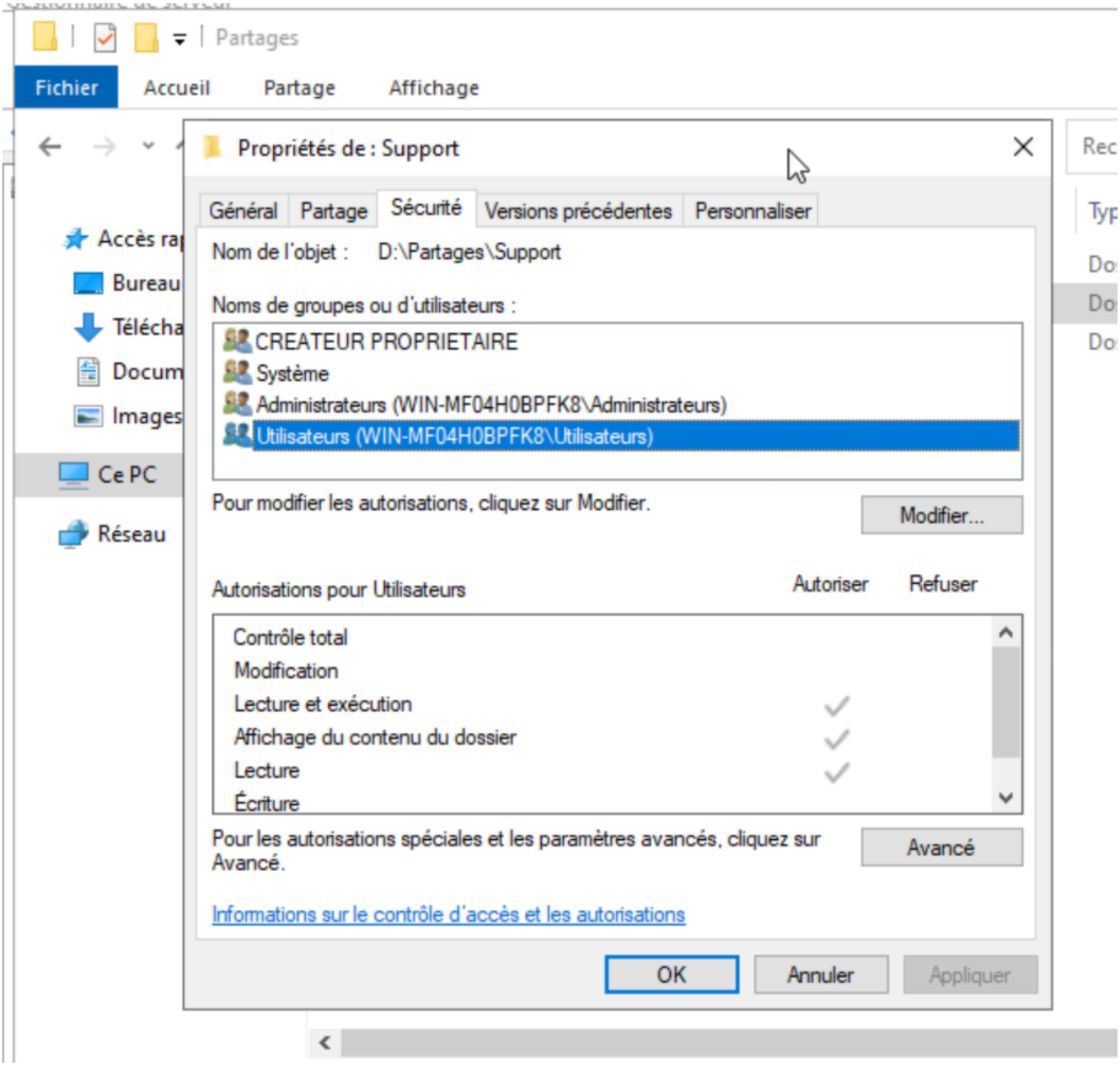
Création de vm pour serveur de fichier.

Création d'un nouveau disque "Donnée Marseille"

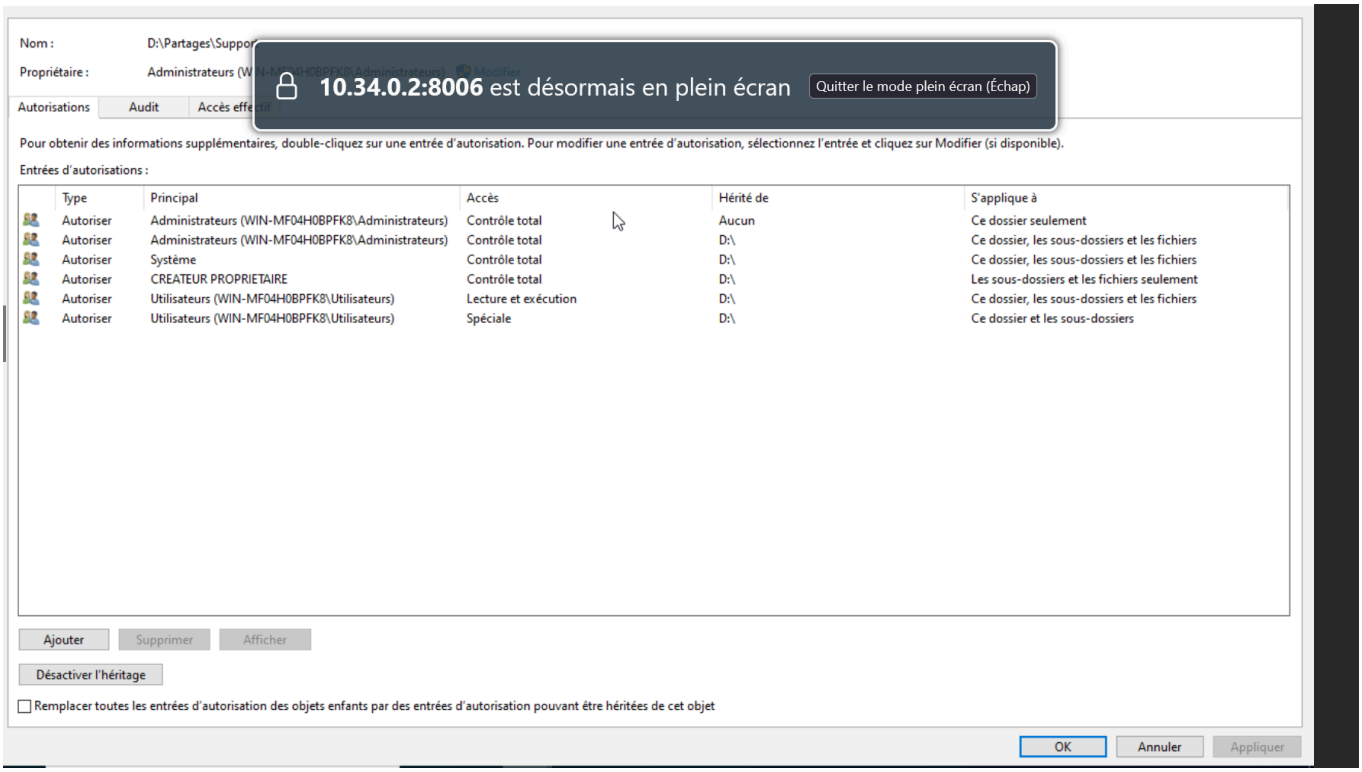


Créer les dossier liés via D:/ qui représente les données de Marseille

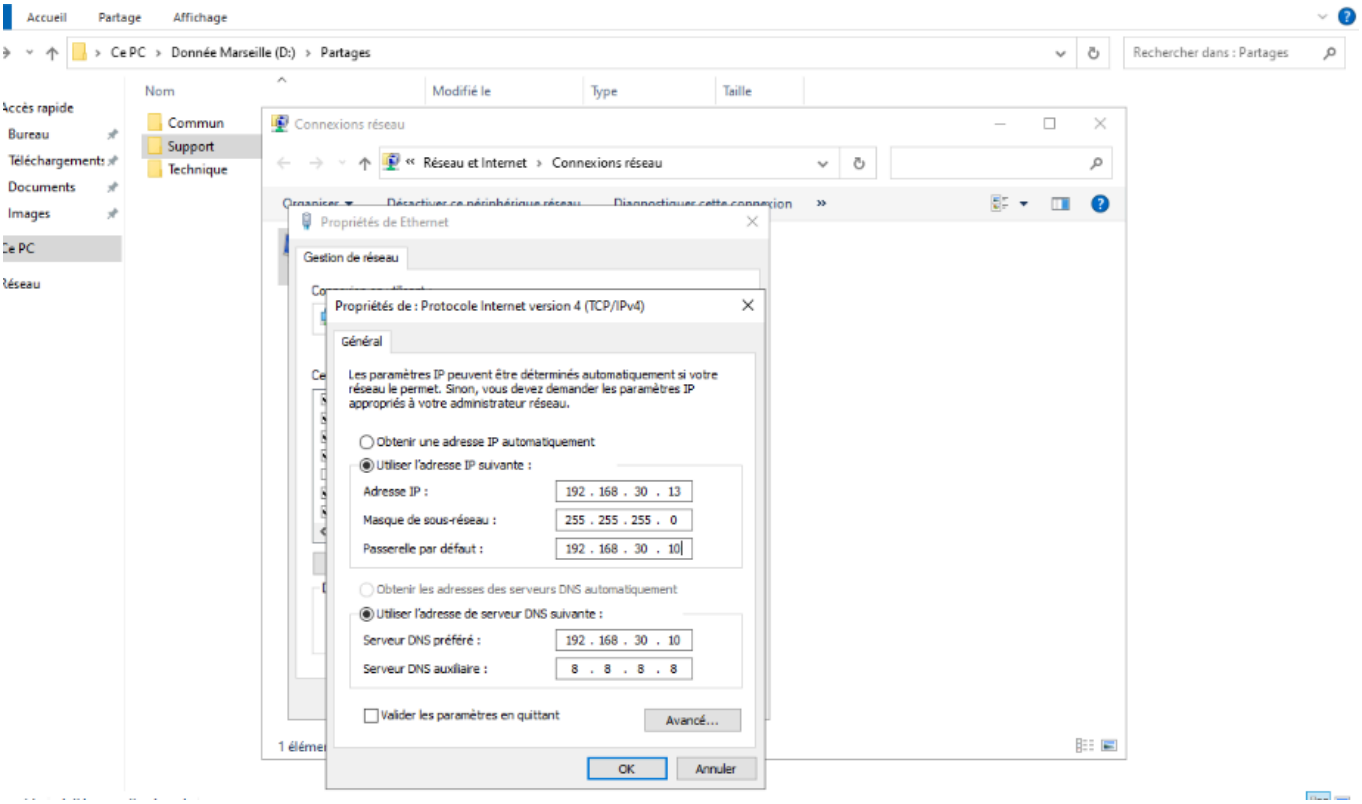

Partages
Fichier
Accueil
Partage
Affichage
Ce PC
Donnée Marseille (D:)
Partages
Accès rapide
Bureau
Téléchargements
Documents
Images
Ce PC
Réseau
Nom
Modifié le
Type
Commun
13/02/2026 10:14
Doss
Support
13/02/2026 10:12
Doss
Technique
13/02/2026 10:14
Doss

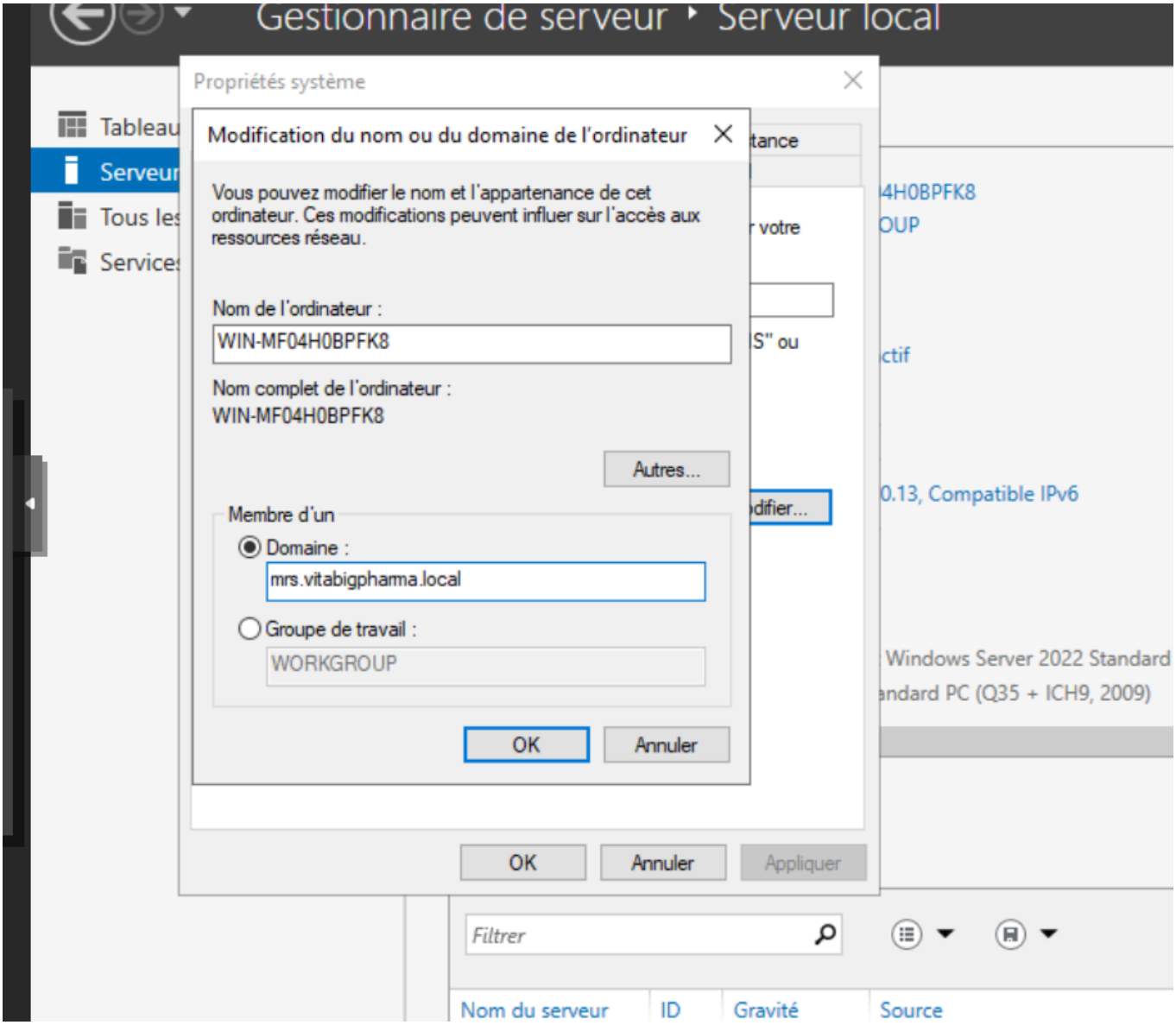

Partages
Fichier
Accueil
Partage
Affichage
Propriétés de : Support
Général
Partage
Sécurité
Versions précédentes
Personnaliser
Nom de l'objet : D:\Partages\Support
Noms de groupes ou d'utilisateurs :
CREATEUR PROPRIETAIRE
Système
Administrateurs (WIN-MF04H0BPFK8\Administrateurs)
Utilisateurs (WIN-MF04H0BPFK8\Utilisateurs)
Pour modifier les autorisations, cliquez sur Modifier.
Modifier...
Autorisations pour Utilisateurs
Autoriser
Refuser
Contrôle total
Modification
Lecture et exécution
Affichage du contenu du dossier
Lecture
Écriture
Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé.
Avancé
Informations sur le contrôle d'accès et les autorisations
OK
Annuler
Appliquer
Accès ra
Bureau
Télécha
Docum
Images
Ce PC
Réseau

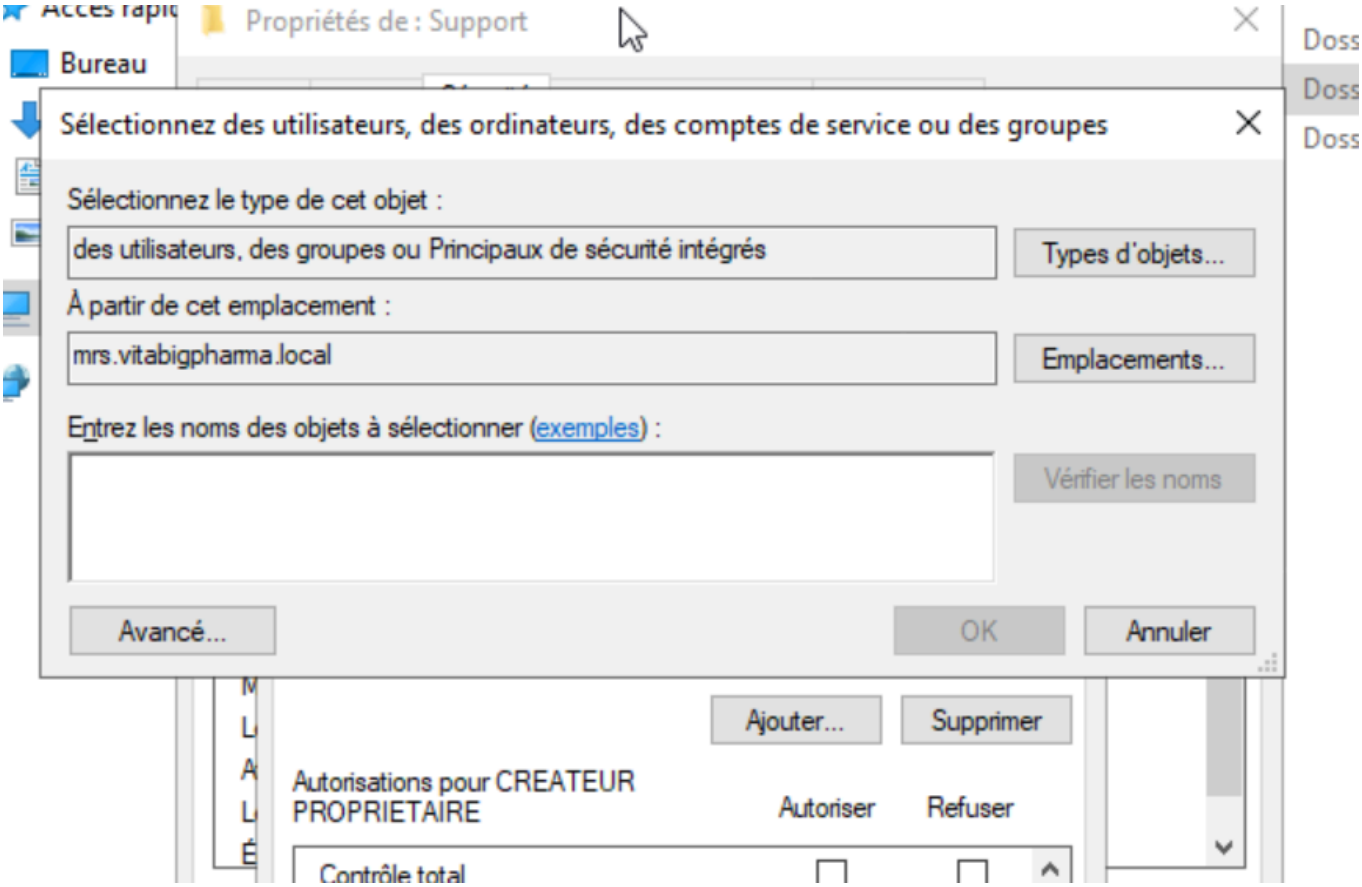
Désactiver l'héritage pour appliquer une sécurité propre par **groupes AD**.

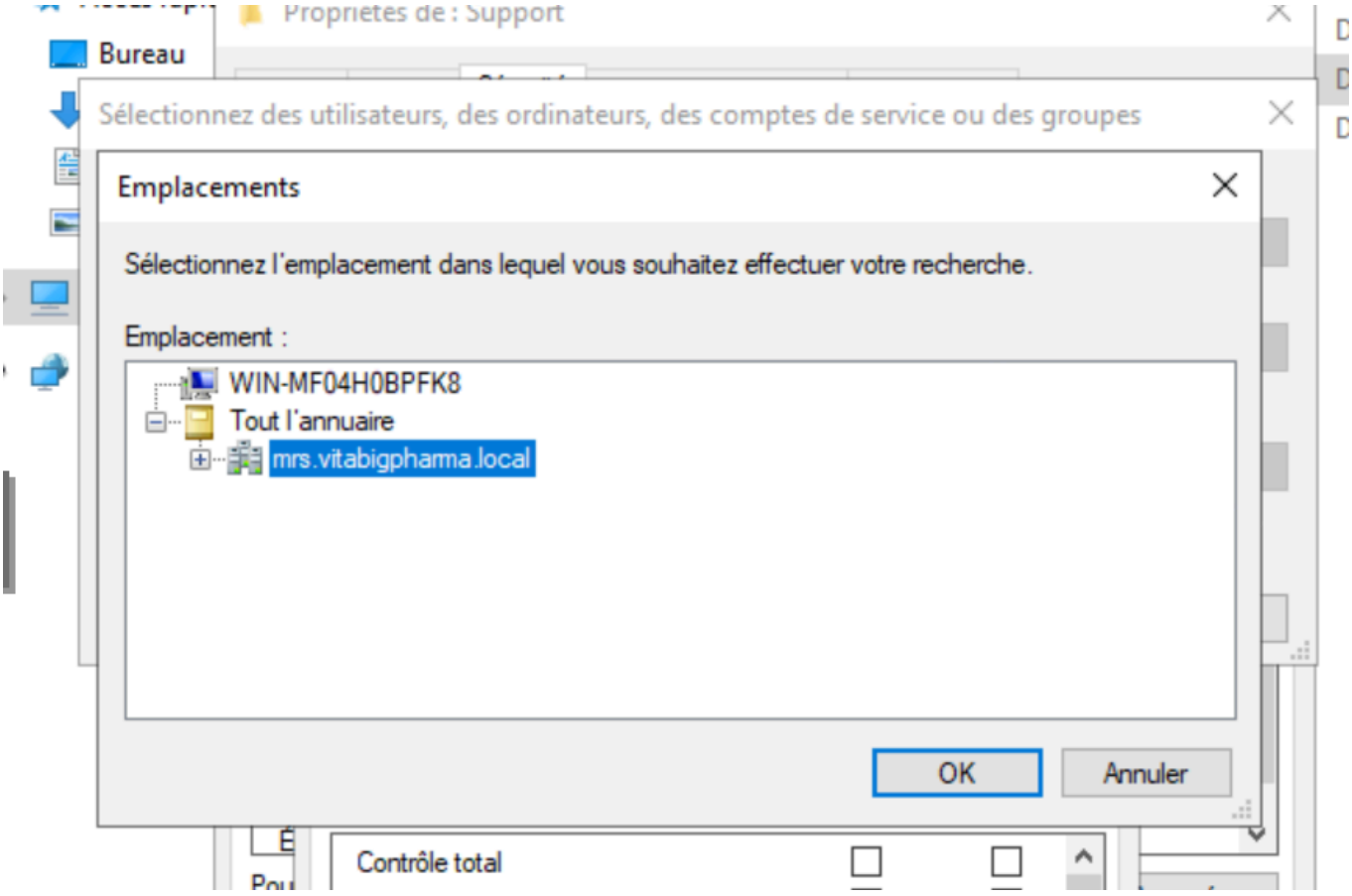


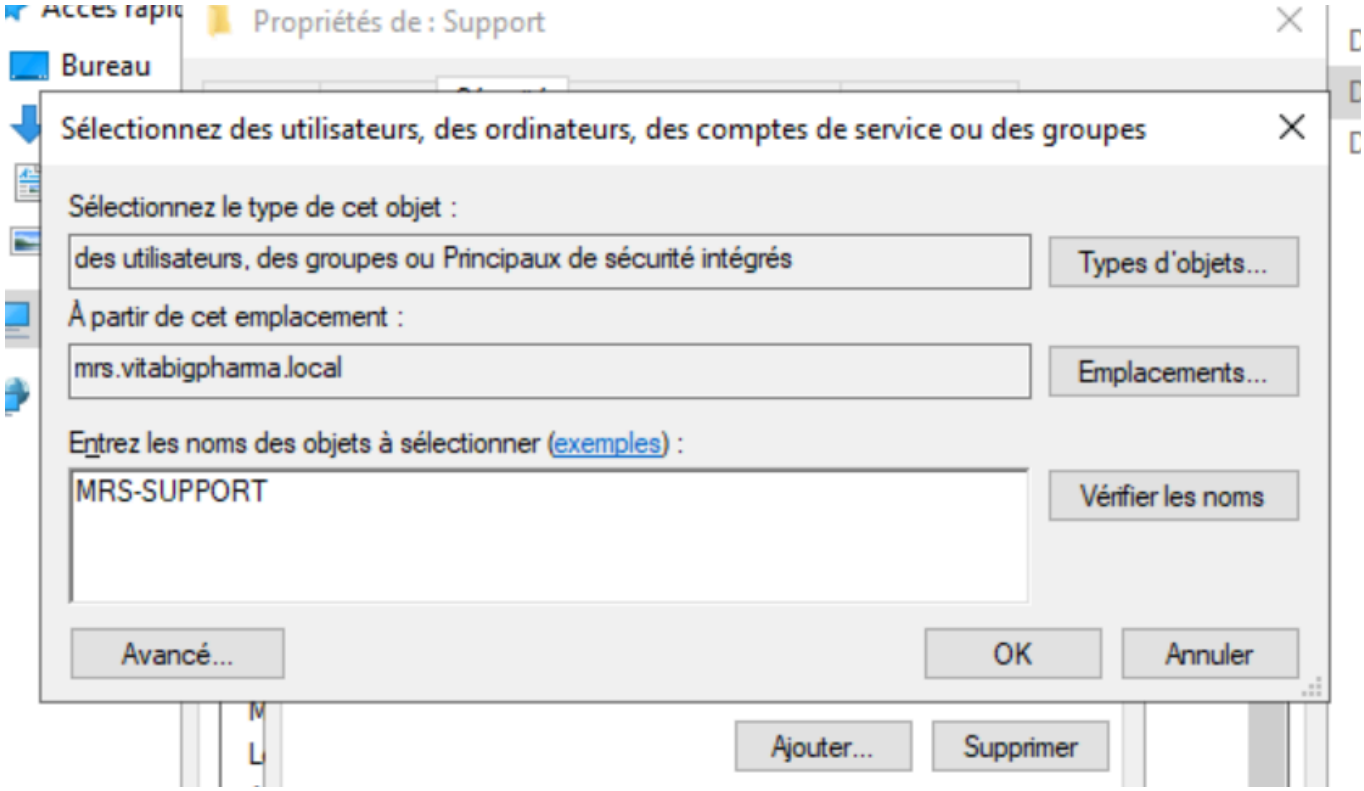
Ip serveur:

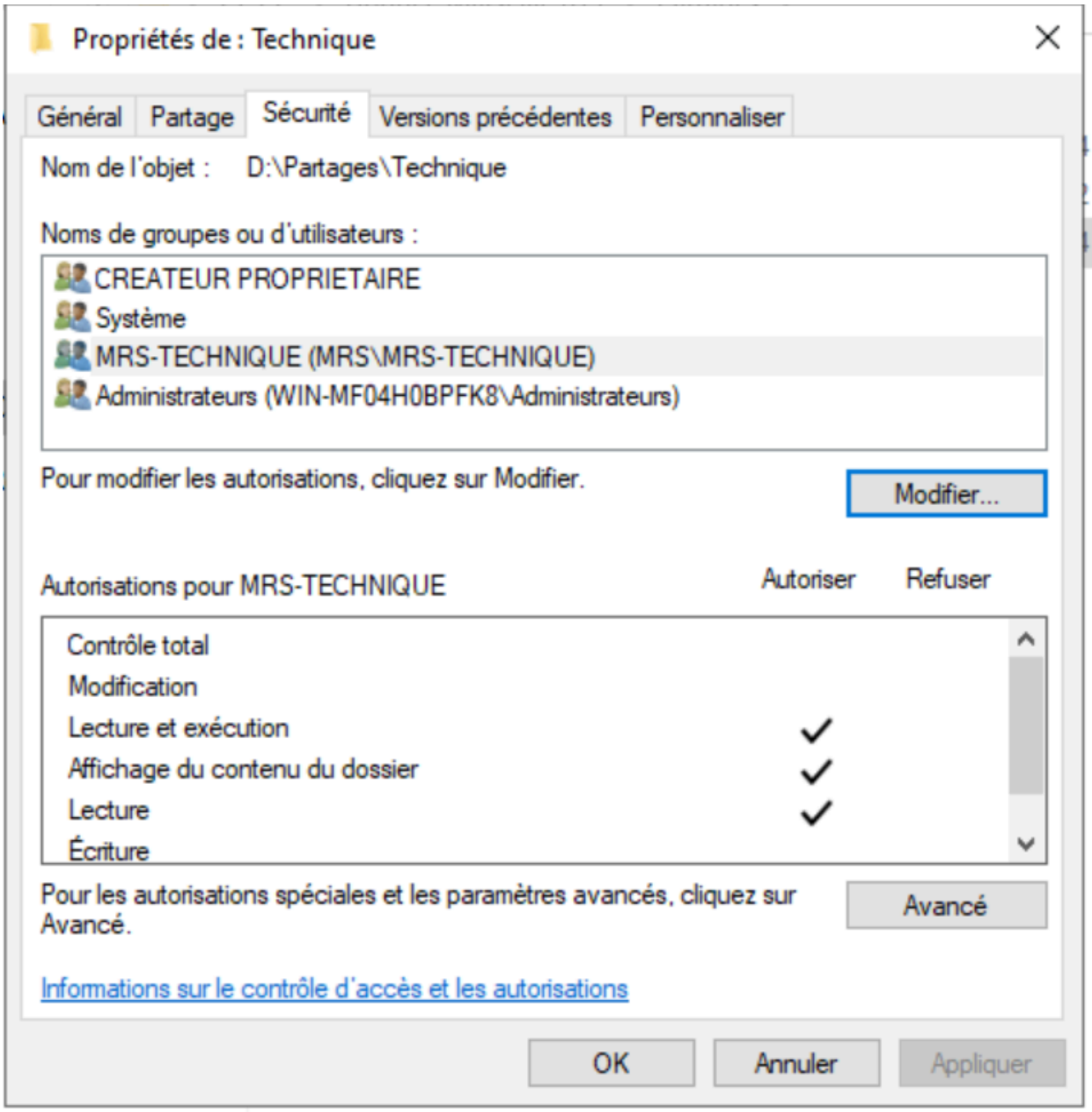


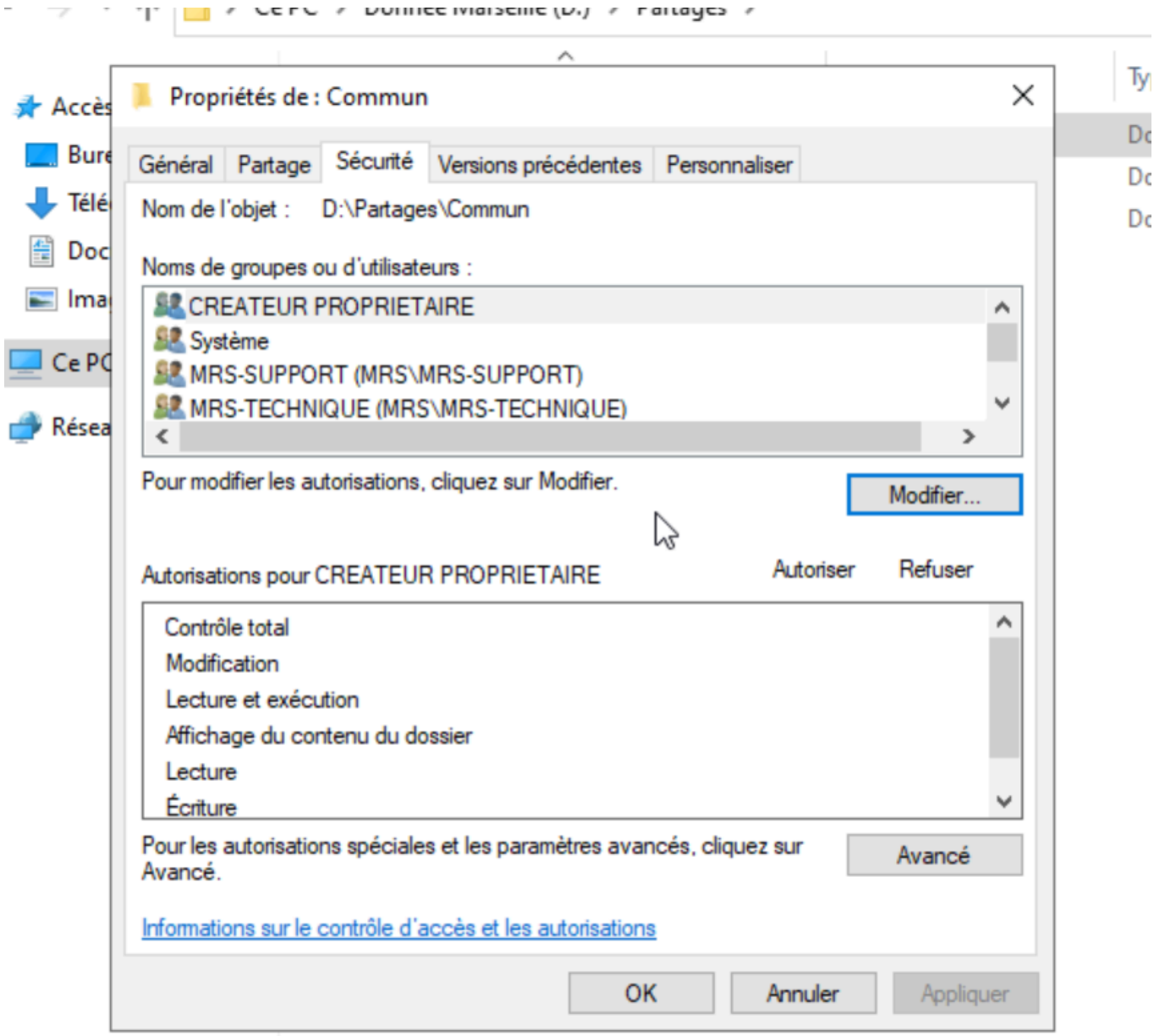

Gestionnaire de serveur ‣ Serveur local
Propriétés système
Modification du nom ou du domaine de l'ordinateur
Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influer sur l'accès aux ressources réseau.
Nom de l'ordinateur :
WIN-MF04H0BPFK8
Nom complet de l'ordinateur :
WIN-MF04H0BPFK8
Autres...
Membre d'un
Domaine :
mrs.vitabigpharma.local
Groupe de travail :
WORKGROUP
OK
Annuler
OK
Annuler
Appliquer
Tableau
Serveur
Tous les
Services
Filtrer
Nom du serveur
ID
Gravité
Source


Propriétés de : Support
Bureau
Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes
Sélectionnez le type de cet objet :
des utilisateurs, des groupes ou Principaux de sécurité intégrés
Types d'objets...
À partir de cet emplacement :
mrs.vitabigpharma.local
Emplacements...
Entrez les noms des objets à sélectionner (exemples) :
Vérifier les noms
Avancé...
OK
Annuler
Ajouter...
Supprimer
Autorisations pour CREATEUR PROPRIETAIRE
Autoriser
Refuser
Contrôle total

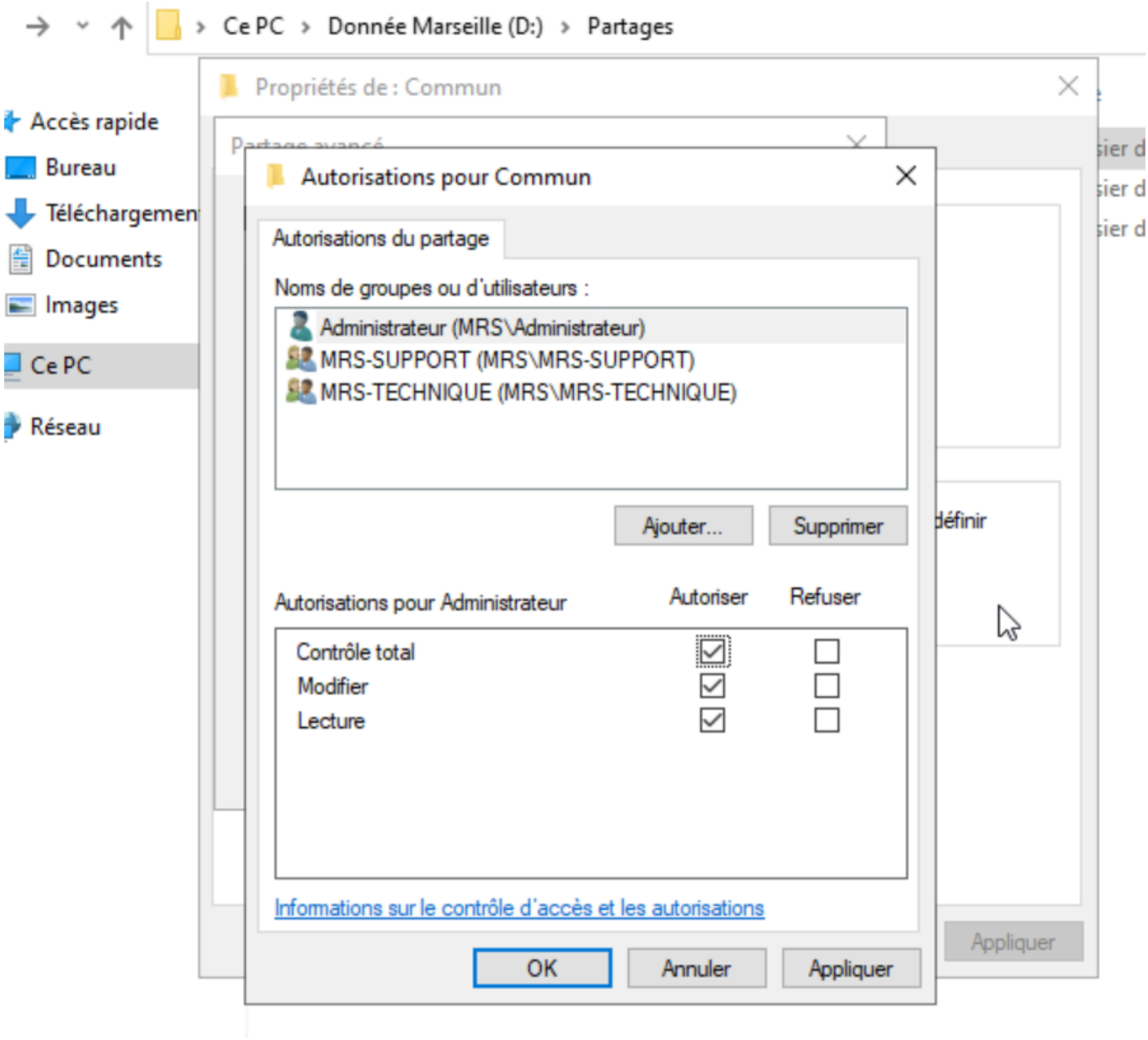

Propriétés de : Support
Bureau
Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes
Emplacements
Sélectionnez l'emplacement dans lequel vous souhaitez effectuer votre recherche.
Emplacement :
WIN-MF04H0BPFK8
Tout l'annuaire
mrs.vitabigpharma.local
OK
Annuler
Contrôle total


Accès rapide
Bureau
Propriétés de : Support
Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes
Sélectionnez le type de cet objet :
des utilisateurs, des groupes ou Principaux de sécurité intégrés
Types d'objets...
À partir de cet emplacement :
mrs.vitabigpharma.local
Emplacements...
Entrez les noms des objets à sélectionner (exemples) :
MRS-SUPPORT
Vérifier les noms
Avancé...
OK
Annuler
Ajouter...
Supprimer


Propriétés de : Technique
Général
Partage
Sécurité
Versions précédentes
Personnaliser
Nom de l'objet : D:\Partages\Technique
Noms de groupes ou d'utilisateurs :
CREATEUR PROPRIETAIRE
Système
MRS-TECHNIQUE (MRS\MRS-TECHNIQUE)
Administrateurs (WIN-MF04H0BPFK8\Administrateurs)
Pour modifier les autorisations, cliquez sur Modifier.
Modifier...
Autorisations pour MRS-TECHNIQUE
Autoriser
Refuser
Contrôle total
Modification
Lecture et exécution
Affichage du contenu du dossier
Lecture
Écriture
Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé.
Avancé
Informations sur le contrôle d'accès et les autorisations
OK
Annuler
Appliquer

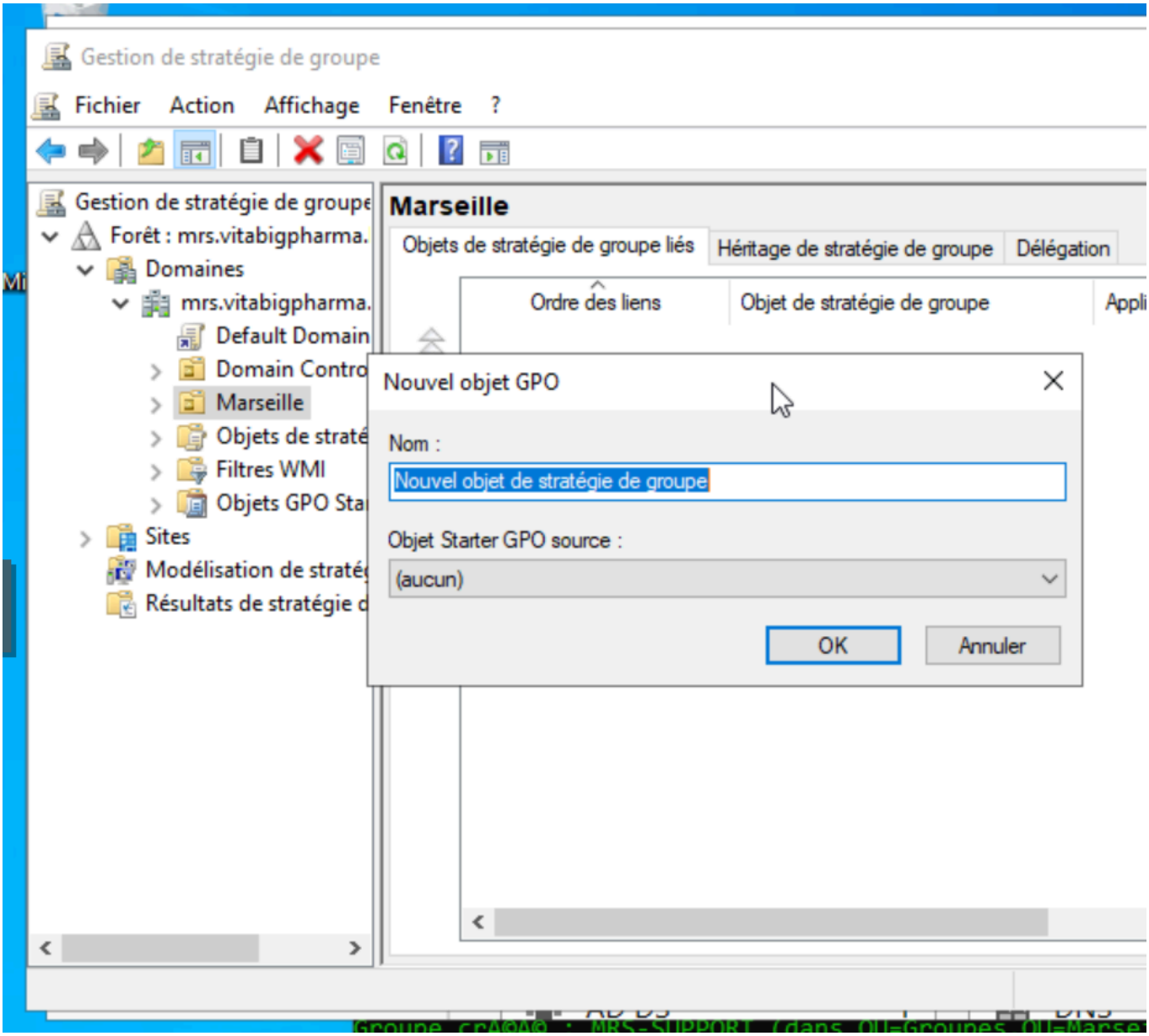

Propriétés de : Commun
Général
Partage
Sécurité
Versions précédentes
Personnaliser
Nom de l'objet : D:\Partages\Commun
Noms de groupes ou d'utilisateurs :
CREATEUR PROPRIETAIRE
Système
MRS-SUPPORT (MRS\MRS-SUPPORT)
MRS-TECHNIQUE (MRS\MRS-TECHNIQUE)
Pour modifier les autorisations, cliquez sur Modifier.
Modifier...
Autorisations pour CREATEUR PROPRIETAIRE
Autoriser
Refuser
Contrôle total
Modification
Lecture et exécution
Affichage du contenu du dossier
Lecture
Écriture
Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé.
Avancé
Informations sur le contrôle d'accès et les autorisations
OK
Annuler
Appliquer

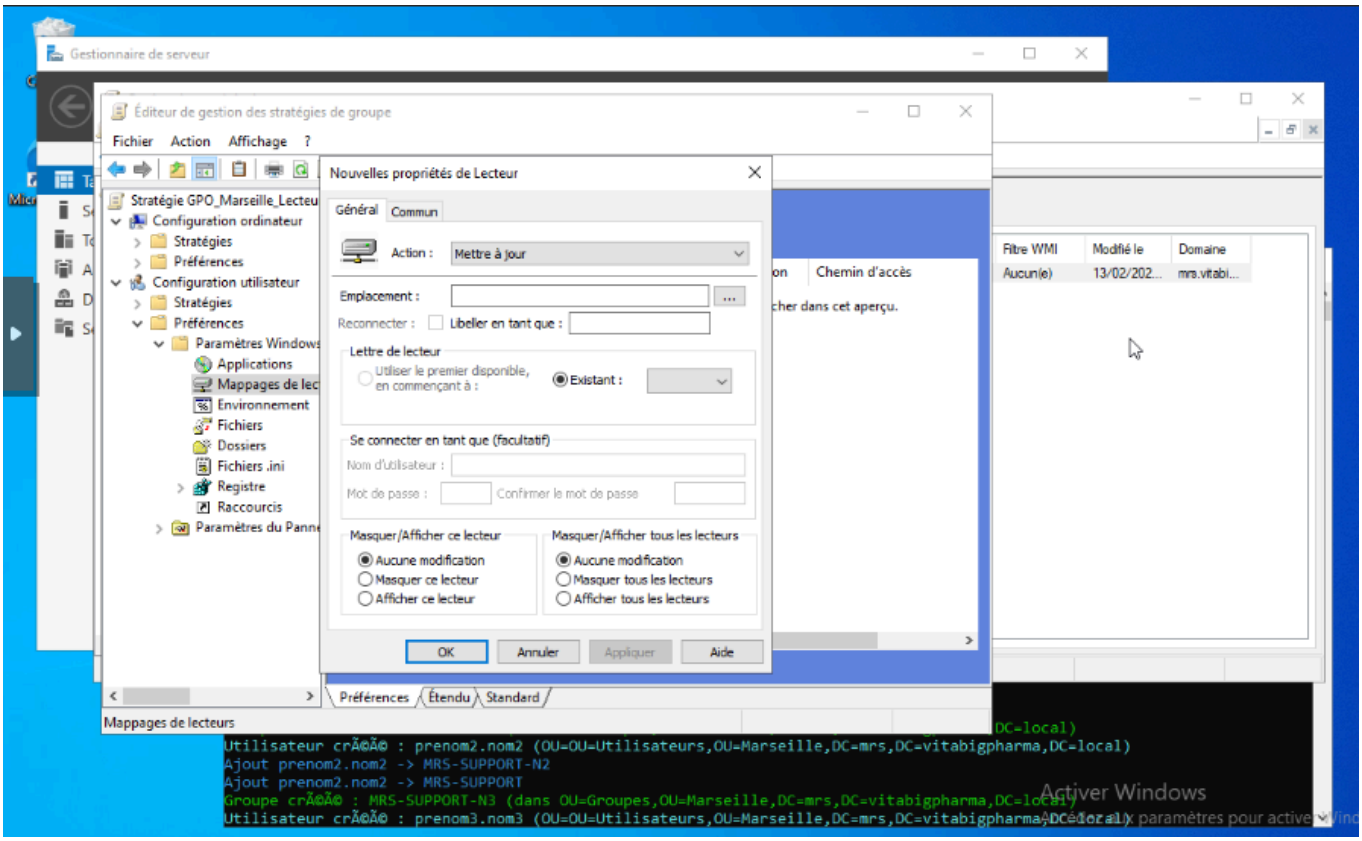
Partage sur les 3 fichiers:

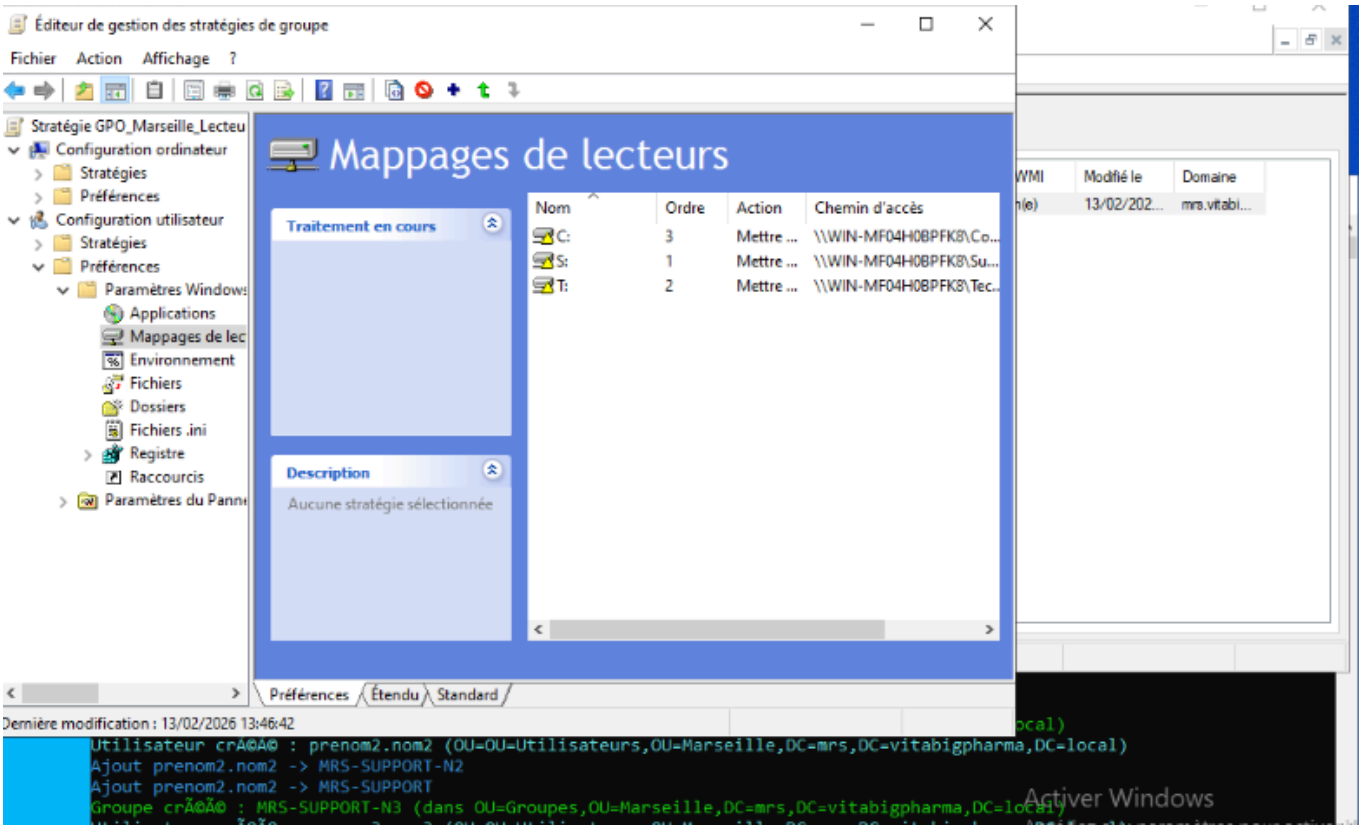


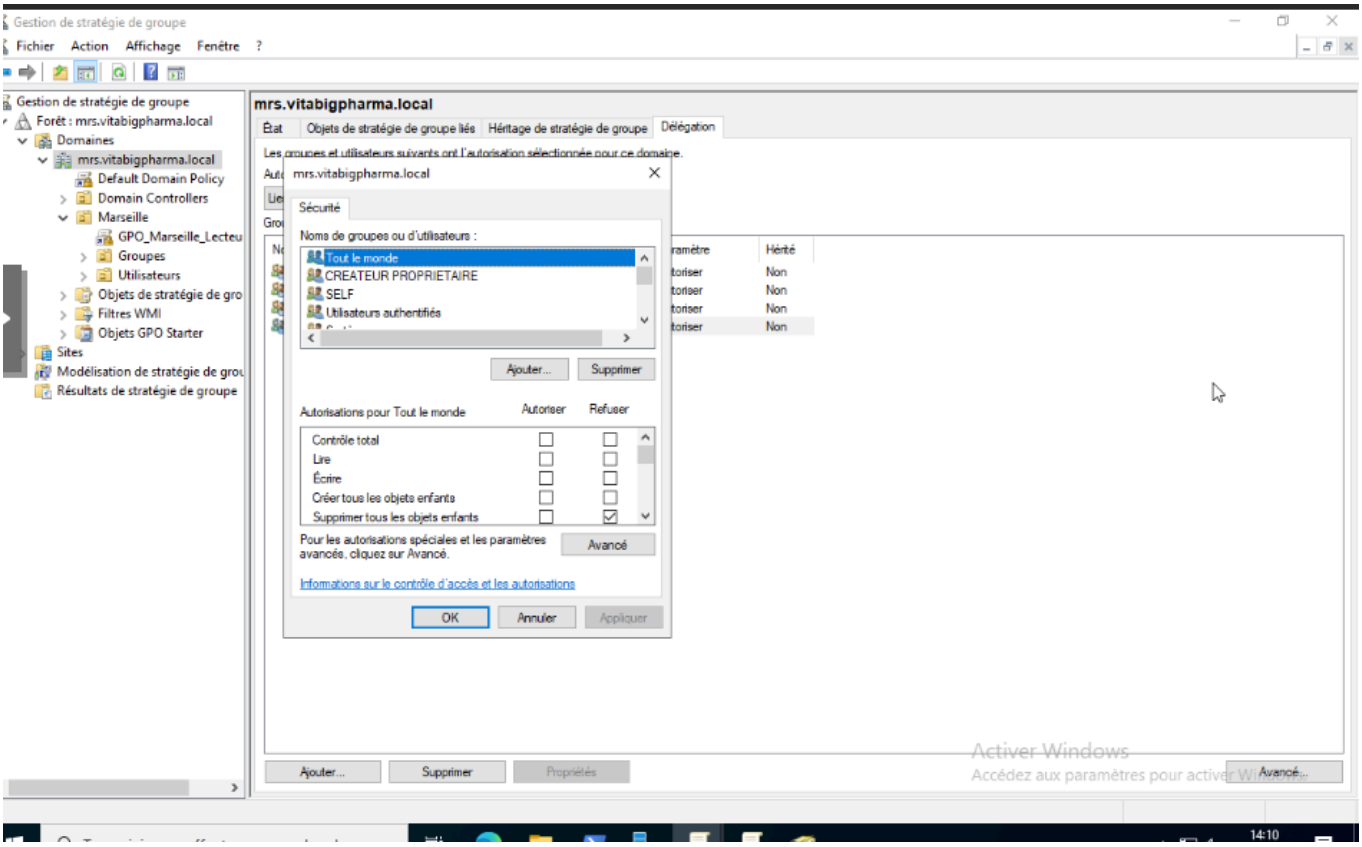
Le serveur fichier est fini(2nd disque + partage)

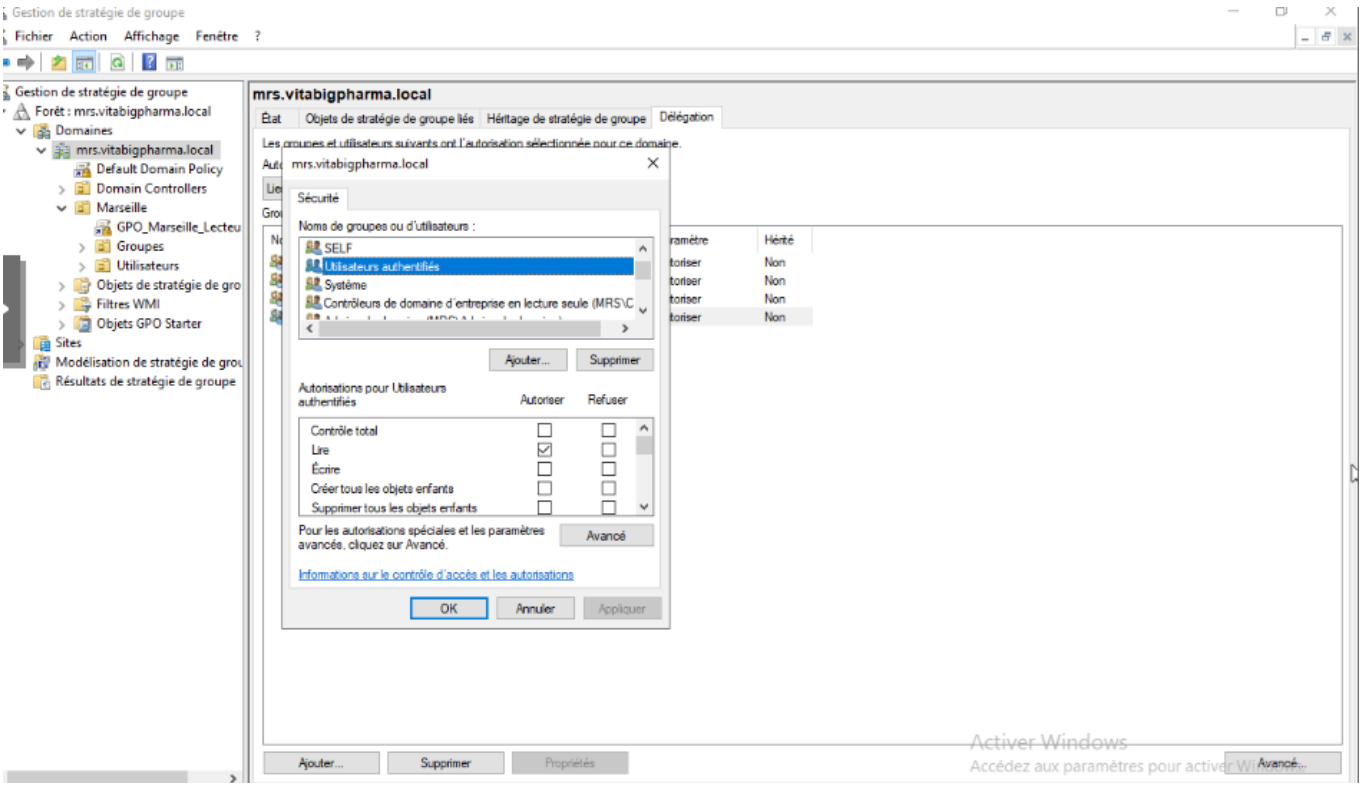
GPO via AD1:


Gestion de stratégie de groupe
Fichier Action Affichage Fenêtre ?
Gestion de stratégie de groupe
Forêt : mrs.vitabigpharma.
Domaines
mrs.vitabigpharma.
Default Domain
Domain Contro
Marseille
Objets de straté
Filtres WMI
Objets GPO Sta
Sites
Modélisation de stratég
Résultats de stratégie d
Marseille
Objets de stratégie de groupe liés
Héritage de stratégie de groupe
Délégation
Ordre des liens
Objet de stratégie de groupe
Appli
Nouvel objet GPO
Nom :
Nouvel objet de stratégie de groupe
Objet Starter GPO source :
(aucun)
OK
Annuler


Gestionnaire de serveur
Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Nouvelles propriétés de Lecteur
Général Commun
Action : Mettre à jour
Emplacement :
Reconnecter : Libeller en tant que :
Lettre de lecteur
Utiliser le premier disponible, en commençant à :
Existant :
Se connecter en tant que (facultatif)
Nom d'utilisateur :
Mot de passe : Confirmer le mot de passe
Masquer/Afficher ce lecteur
Aucune modification
Masquer ce lecteur
Afficher ce lecteur
Masquer/Afficher tous les lecteurs
Aucune modification
Masquer tous les lecteurs
Afficher tous les lecteurs
OK Annuler Appliquer Aide
Stratégie GPO_Marseille_Lecteu
Configuration ordinateur
Stratégies
Préférences
Configuration utilisateur
Stratégies
Préférences
Paramètres Windows
Applications
Mappages de lec
Environnement
Fichiers
Dossiers
Fichiers .ini
Registre
Raccourcis
Paramètres du Panne
Préférences Étendu Standard
Mappages de lecteurs
Filtre WMI Modifié le Domaine
Aucun(e) 13/02/202... mrs.vitabi...
Chemin d'accès
cher dans cet aperçu.
DC=local)
Utilisateur crÃ©Ã© : prenom2.nom2 (OU=OU=Utilisateurs,OU=Marseille,DC=mrs,DC=vitabigpharma,DC=local)
Ajout prenom2.nom2 -> MRS-SUPPORT-N2
Ajout prenom2.nom2 -> MRS-SUPPORT
Groupe crÃ©Ã© : MRS-SUPPORT-N3 (dans OU=Groupes,OU=Marseille,DC=mrs,DC=vitabigpharma,DC=local)
Utilisateur crÃ©Ã© : prenom3.nom3 (OU=OU=Utilisateurs,OU=Marseille,DC=mrs,DC=vitabigpharma,DC=local)
Activer Windows


Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie GPO_Marseille_Lecteu
Configuration ordinateur
Stratégies
Préférences
Configuration utilisateur
Stratégies
Préférences
Paramètres Windows
Applications
Mappages de lec
Environnement
Fichiers
Dossiers
Fichiers .ini
Registre
Raccourcis
Paramètres du Panne
Mappages de lecteurs
Traitement en cours
Description
Aucune stratégie sélectionnée
Nom Ordre Action Chemin d'accès
C: 3 Mettre ... \\WIN-MF04H0BPFK8\Co...
S: 1 Mettre ... \\WIN-MF04H0BPFK8\Su...
T: 2 Mettre ... \\WIN-MF04H0BPFK8\Tec...
Préférences Étendu Standard
Dernière modification : 13/02/2026 13:46:42
Modifié le Domaine
13/02/202... mrs.vitabi...
Utilisateur crÃ©Ã© : prenom2.nom2 (OU=OU=Utilisateurs,OU=Marseille,DC=mrs,DC=vitabigpharma,DC=local)
Ajout prenom2.nom2 -> MRS-SUPPORT-N2
Ajout prenom2.nom2 -> MRS-SUPPORT
Groupe crÃ©Ã© : MRS-SUPPORT-N3 (dans OU=Groupes,OU=Marseille,DC=mrs,DC=vitabigpharma,DC=local)
Activer Windows





Mise en place de GLPI via VM Debian 13 en graphique :

stting second disque

Aller dans windows r+ diskmcrg.msc ça ouvre le disque.

Clique droit nouveau volume créeer un volume.

Serveur de fichier -) disque (il y est)

Cliquer dessus , tache nouveau volume / assistant , suivant...
nom du volume :data/ Il y aitdans ce pc
clique droit pull de stockage/ tache / nouveau pull de stockage suivant . Nomer daya

Intégrer la machine dans le domaine.Win+r: Ncpa.cpl System.ctl
Mettre dans ipv4
sysdl.cpl. Nomer data.nrs
nomer domaine: nrs.vitabigpharma.local
Nouveau dossier dans pc (repertoir parrage) Aller dans propriété