Conception et déploiement d’une infrastructure réseau sécurisée multi-sites pour l’entreprise Vita Big Pharma

---

Phase 1 : Analyse et conception

1. Contexte général du projet

Dans le cadre de la préparation au **BTS Services Informatiques aux Organisations (SIO)**, ce projet a pour objectif la **conception, le déploiement et l’exploitation d’une infrastructure réseau sécurisée** répondant aux besoins d’une entreprise en phase de développement.

L’étude porte sur la mise en place d’une infrastructure informatique moderne, centralisée et sécurisée, respectant les bonnes pratiques en matière de réseau, de sécurité et d’administration des systèmes.

1.2 Présentation de l’entreprise

Vita Big Pharma est une entreprise du secteur pharmaceutique spécialisée dans la **fabrication de compléments alimentaires**.
Dans le cadre de son développement à l’échelle nationale, l’entreprise souhaite s’implanter en France en s’appuyant sur **deux sites géographiquement distants**, chacun ayant un rôle bien défini.

1.2.1 Site de Toulouse – Siège administratif

Le site de Toulouse constitue le **siège administratif** de l’entreprise. Il regroupe les services suivants :

- Direction générale
- Ressources Humaines
- Service Finance

Ce site concentre les fonctions décisionnelles et administratives de l’entreprise.

1.2.2 Site de Marseille – Site technique

Le site de Marseille est dédié aux activités techniques et informatiques. Il comprend :

- Service technique
- Support informatique

Ce site assure la gestion technique de l'infrastructure ainsi que l'assistance aux utilisateurs, y compris pour le site distant de Toulouse.

1.2.3 Répartition des services par site

Afin de répondre aux besoins organisationnels de l'entreprise, les services sont répartis entre les deux sites en fonction de leurs missions. Cette répartition permet d'optimiser la gestion administrative tout en centralisant les compétences techniques sur un site dédié.

Le tableau ci-dessous présente la répartition des services au sein de l'entreprise **Vita Big Pharma**.

Site	Rôle du site	Services présents
Toulouse	Siège administratif	Direction générale Ressources humaines Finance
Marseille	Site technique	Service technique Support informatique

Le site de Toulouse concentre les fonctions stratégiques et administratives de l'entreprise, tandis que le site de Marseille est orienté vers les activités techniques et l'exploitation de l'infrastructure informatique. Cette organisation justifie la mise en place de mécanismes de communication sécurisés entre les deux sites afin d'assurer la continuité des services et le support inter-sites.

1.3 Enjeux et objectifs de l'infrastructure

L'entreprise souhaite disposer d'une **infrastructure informatique** répondant aux critères suivants :

- **Centralisée**, afin de faciliter l'administration et la gestion des ressources
- **Sécurisée**, pour garantir la protection des données sensibles et la conformité aux bonnes pratiques
- **Évolutive**, afin d'accompagner la croissance de l'entreprise
- **Fiable**, assurant une haute disponibilité des services

Cette infrastructure doit permettre :

- La **continuité de service** entre les deux sites
- Le **télétravail sécurisé** pour les collaborateurs
- L'**assistance technique inter-sites**
- La **supervision** et l'**audit de sécurité** de l'infrastructure
- La **qualité de service réseau** pour les utilisateurs grâce à des mécanismes de *Traffic Shaping*

1.4 Rôle et missions confiées à l’étudiant

Dans le cadre de ce projet, l’étudiant est chargé de :

- **Analyser les besoins** de l’entreprise
- **Concevoir et maquetter** l’infrastructure réseau et système
- **Déployer les serveurs et services nécessaires**
- **Documenter**, exploiter et maintenir la solution mise en place

Cette documentation vise à décrire l’ensemble des choix techniques réalisés, les étapes de déploiement ainsi que les procédures d’exploitation.

---

2. Analyse des besoins fonctionnels et techniques

2.1 Besoins fonctionnels

L’infrastructure à mettre en place doit avant tout permettre une communication fiable et sécurisée entre les deux sites distants de l’entreprise. Les échanges inter-sites doivent être protégés afin de garantir la confidentialité des données sensibles, notamment celles liées aux ressources humaines, à la finance et aux outils métiers.

La gestion des utilisateurs doit être centralisée à l’aide d’un annuaire unique, permettant une authentification homogène sur l’ensemble des services. Cette centralisation doit s’accompagner d’une gestion fine des droits, basée sur des groupes, afin de contrôler précisément les accès aux ressources selon les fonctions occupées par les collaborateurs.

L’entreprise exprime également un besoin fort en matière de partage de fichiers. Les données doivent être accessibles de manière sécurisée, tout en intégrant des mécanismes de quotas afin de maîtriser l’espace de stockage utilisé par chaque utilisateur et chaque service.

Plusieurs outils métiers sont indispensables au fonctionnement quotidien de l’entreprise. Un outil de gestion des incidents et du support informatique est nécessaire pour assurer le suivi des demandes utilisateurs, tandis qu’un progiciel de gestion intégré doit permettre la gestion administrative et financière. Ces services doivent être disponibles, sécurisés et intégrés à l’annuaire d’entreprise.

Le télétravail constitue également un besoin fonctionnel majeur. Les collaborateurs doivent pouvoir accéder aux ressources internes de l’entreprise à distance, via une solution sécurisée, sans compromettre la sécurité du système d’information.

Enfin, l’infrastructure doit permettre la supervision des équipements et des services, ainsi que la mise en place de sauvegardes fiables. Les services critiques, tels que l’annuaire Active

Directory et le service DNS, doivent bénéficier d'une haute disponibilité afin d'assurer la continuité de service.

2.2 Besoins et contraintes techniques

Sur le plan technique, l'infrastructure doit reposer sur une segmentation claire des réseaux afin de limiter les risques et de renforcer la sécurité globale. Les réseaux dédiés aux serveurs doivent être isolés de ceux utilisés par les collaborateurs, tout en restant accessibles de manière contrôlée.

Les accès au système d'information doivent être strictement sécurisés. Cela implique la mise en place de pare-feu, de tunnels VPN pour les communications inter-sites et les accès distants, ainsi que de stratégies de groupe permettant de renforcer la sécurité des postes et des comptes utilisateurs.

L'administration de l'infrastructure doit être facilitée par l'automatisation de certaines tâches récurrentes, notamment la création et la gestion des comptes utilisateurs. Cette automatisation contribue à réduire les erreurs humaines et à améliorer l'efficacité de l'exploitation.

Les données de l'entreprise doivent faire l'objet de sauvegardes régulières, planifiées et vérifiables. Ces sauvegardes doivent pouvoir être restaurées en cas d'incident, garantissant ainsi la résilience du système d'information.

---

3. Contraintes réglementaires et organisationnelles

La conception et le déploiement de l'infrastructure réseau de l'entreprise Vita Big Pharma doivent s'inscrire dans un cadre réglementaire strict, en particulier en raison de la nature sensible des données traitées. En tant qu'entreprise du secteur pharmaceutique, Vita Big Pharma manipule des informations à caractère personnel et potentiellement confidentiel, ce qui impose le respect des réglementations en vigueur.

Sur le plan réglementaire, l'infrastructure doit être conforme au **Règlement Général sur la Protection des Données (RGPD)**. Cela implique que les données personnelles des collaborateurs soient collectées, stockées et traitées de manière sécurisée et limitée à leur strict usage professionnel. La gestion des comptes utilisateurs doit être rigoureuse, avec des droits d'accès attribués uniquement en fonction des besoins métiers. Les accès aux données sensibles doivent être tracés afin de garantir une traçabilité des actions, notamment pour les opérations d'administration du système d'information.

La politique de sécurité doit également intégrer des règles de gestion des mots de passe renforcées, incluant des exigences de complexité, de renouvellement et de protection contre les accès non autorisés. Les mécanismes de sauvegarde mis en place doivent garantir la

confidentialité, l'intégrité et la disponibilité des données, tout en permettant une restauration rapide en cas d'incident ou de sinistre.

D'un point de vue organisationnel, la présence de deux sites géographiquement distants impose une coordination efficace entre les équipes. Le site de Marseille, en charge des services techniques et du support informatique, doit être en mesure d'administrer et d'assister les utilisateurs du site de Toulouse. Cela nécessite une infrastructure centralisée, des outils de supervision accessibles à distance et des procédures d'intervention clairement définies.

L'organisation du support informatique doit permettre une gestion structurée des incidents, avec une répartition des rôles et des niveaux d'intervention. La documentation technique et les procédures d'exploitation jouent un rôle essentiel pour assurer la continuité de service, faciliter la maintenance et garantir la pérennité de l'infrastructure, indépendamment des intervenants.

Enfin, l'évolution future de l'entreprise constitue une contrainte organisationnelle à prendre en compte dès la phase de conception. L'infrastructure doit être suffisamment flexible pour permettre l'ajout de nouveaux utilisateurs, de nouveaux services ou de nouveaux sites, sans remise en cause majeure de l'architecture existante.

---

4. Étude de l'existant et hypothèses retenues

4.1 Constat initial

À l'origine du projet, l'entreprise Vita Big Pharma ne dispose d'aucune infrastructure informatique existante sur le territoire français. L'implantation des deux sites de Toulouse et de Marseille correspond à une phase de création et de structuration du système d'information. Il n'existe donc ni réseau local opérationnel, ni serveurs en production, ni services centralisés tels qu'un annuaire, un système de sauvegarde ou des outils de supervision.

Cette absence d'existant constitue à la fois une contrainte et une opportunité. Elle impose de concevoir une infrastructure complète depuis zéro, tout en offrant la liberté de s'appuyer directement sur des solutions modernes, sécurisées et conformes aux bonnes pratiques actuelles, sans avoir à composer avec des choix techniques antérieurs.

4.2 Hypothèses et choix d'architecture

Compte tenu de l'organisation de l'entreprise et de la répartition géographique de ses services, le choix d'une **architecture multi-sites** s'impose naturellement. Les deux sites doivent fonctionner de manière autonome pour les usages quotidiens, tout en restant étroitement interconnectés afin d'assurer la continuité des services et la cohérence du système d'information.

L’architecture retenue repose sur une interconnexion sécurisée entre les sites, permettant le partage des ressources, l’assistance technique à distance et l’accès aux services métiers hébergés sur l’un ou l’autre site. Cette approche permet également de garantir une meilleure résilience, chaque site disposant de ses propres ressources critiques, tout en bénéficiant d’une centralisation logique de l’administration.

L’hypothèse retenue est celle d’une infrastructure évolutive, capable d’accueillir de nouveaux utilisateurs, de nouveaux services ou de futurs sites, sans remise en cause majeure de l’architecture globale. Ce choix s’inscrit pleinement dans la stratégie de développement national de l’entreprise.

4.3 Hypothèses retenues

Dans le cadre de ce projet, plusieurs hypothèses ont été retenues afin de concevoir une infrastructure cohérente avec les besoins actuels et futurs de l’entreprise Vita Big Pharma. Il est considéré que les deux sites disposent d’une connexion Internet stable et suffisante pour supporter des échanges sécurisés et permanents entre Toulouse et Marseille. Cette connectivité est indispensable pour assurer l’accès aux services centralisés, la supervision à distance et le support inter-sites.

Il est également admis que l’ensemble des collaborateurs utilise des postes de travail récents, compatibles avec les solutions de sécurité déployées, notamment les politiques de groupe et les clients VPN. Cette hypothèse permet de garantir une application homogène des règles de sécurité et une gestion centralisée des postes utilisateurs.

L’infrastructure est pensée comme entièrement virtualisée, afin d’optimiser l’utilisation des ressources matérielles, de faciliter les opérations de maintenance et de simplifier les procédures de sauvegarde et de restauration. Les services critiques sont déployés sur chaque site, notamment l’annuaire et le service DNS, afin de limiter la dépendance à un lien unique et d’améliorer la disponibilité globale.

Enfin, il est supposé que l’entreprise dispose d’une équipe informatique capable d’assurer l’exploitation quotidienne de l’infrastructure, ainsi que la maintenance et l’évolution des services dans le temps, en s’appuyant sur une documentation complète et des procédures formalisées.

4.4 Avantages de l’architecture multi-sites

Le choix d’une architecture multi-sites présente de nombreux avantages pour une entreprise disposant de plusieurs implantations géographiques. Il permet tout d’abord d’assurer une meilleure continuité de service. En cas de défaillance partielle d’un site ou d’une interruption temporaire de la connectivité, chaque site conserve un niveau de fonctionnement autonome grâce à la présence locale des services essentiels.

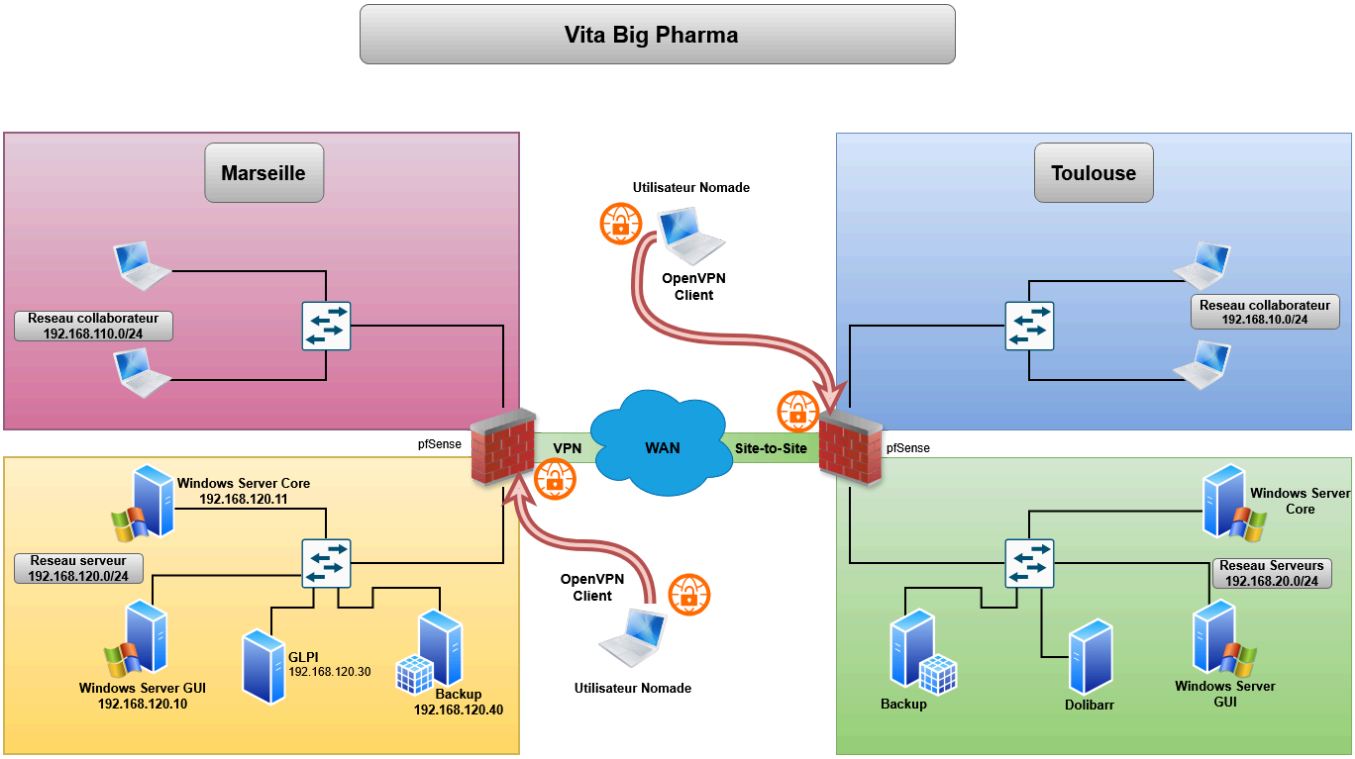
Cette architecture facilite également la centralisation de l'administration tout en conservant une répartition logique des ressources. Les équipes techniques peuvent intervenir à distance sur l'ensemble de l'infrastructure, ce qui réduit les délais d'intervention et améliore la qualité du support fourni aux utilisateurs.

Sur le plan de la sécurité, l'architecture multi-sites permet de segmenter les réseaux et de contrôler finement les flux inter-sites. Les échanges peuvent être chiffrés et filtrés, limitant ainsi les risques liés aux intrusions ou aux fuites de données. Elle offre aussi un cadre adapté à la mise en œuvre de politiques de sauvegarde et de supervision réparties, renforçant la résilience globale du système d'information.

Enfin, cette approche s'inscrit dans une logique d'évolutivité. L'ajout d'un nouveau site ou de nouveaux services peut être envisagé sans refonte complète de l'infrastructure existante, ce qui accompagne efficacement la stratégie de développement de l'entreprise.

---

5. Schéma cible et principes retenus



Le schéma logique retenu repose sur une architecture multi-sites avec, sur chaque site, une séparation stricte entre le réseau des serveurs et celui des collaborateurs. Cette segmentation réduit fortement la surface d'attaque et permet de maîtriser les flux autorisés. Chaque site dispose d'un pare-feu (OPNsense/pfSense) positionné en frontière entre le LAN interne et Internet, jouant à la fois le rôle de passerelle, de filtre, de terminaison VPN et de point de mise en œuvre de la qualité de service.

L’interconnexion entre Toulouse et Marseille est assurée par un **VPN IPsec site-à-site** entre les deux pare-feux. Le télétravail est pris en charge via un **VPN nomade** (OpenVPN ou WireGuard), également terminé sur le pare-feu, afin d’éviter toute exposition directe des services internes.

5.1 Plan d’adressage IP et segmentation

Le plan d’adressage proposé utilise des plages privées distinctes par site pour éviter tout conflit et simplifier le routage inter-sites. Chaque site possède deux réseaux : un réseau « Collaborateurs » et un réseau « Serveurs ». Les passerelles par défaut sont portées par le pare-feu, ce qui garantit que tout trafic entre VLANs (ou vers le VPN/Internet) est filtré.

Site	LAN Collaborateurs	LAN Serveurs	VPN	Passerelle FW
Toulouse	192.168.200.0/24	192.168.100.0/24	192.168.30.0/24	192.168.100.1 192.168.200.1 192.168.30.1
Marseille	192.168.10.0/24	192.168.20.0/24	192.168.30.0/24	192.168.10.1 192.168.20.1 192.168.30.1

Marseille – 192.168.20.0/24**

- TLS-DC1 (GUI) : 192.168.20.10
- TLS-DC2 (Core) : 192.168.20.11
- Dolibarr (ERP) : 192.168.20.30
- Backup : 192.168.20.40

Toulouse – 192.168.120.0/24**

- MRS-DC1 (GUI) : 192.168.120.10
- MRS-DC2 (Core) : 192.168.120.11
- GLPI : 192.168.120.30
- Backup : 192.168.120.40

DHCP et IP statiques

Les postes collaborateurs peuvent être en DHCP sur chaque site (ex. plage .100 à .199) et les serveurs en IP statiques. Ça évite les conflits et facilite la supervision.

5.2 Traffic Shaping et priorisation des services

Afin de garantir une bonne expérience utilisateur et éviter qu'un usage "non critique" ne dégrade les services centraux, une politique de **Traffic Shaping** est appliquée sur l'interface du **LAN Collaborateurs** de chaque pare-feu. Le débit est limité à **5 Mb/s**, tandis que les flux essentiels restent prioritaires afin d'assurer la continuité des services et la stabilité de l'authentification.

Le principe est le suivant : le trafic sortant des collaborateurs est encadré, mais les flux critiques (authentification Active Directory, DNS, accès ERP/Dolibarr, accès GLPI et trafic VPN) passent en priorité. Concrètement, on met en place une file/queue haute priorité (ou des règles de priorisation) pour ces flux, et une file par défaut pour le reste.

6. Comparaison des solutions techniques et choix retenu

Cette partie vise à comparer différentes solutions techniques envisageables pour répondre aux besoins de l'entreprise Vita Big Pharma, puis à justifier les choix finaux retenus pour la conception de l'infrastructure.

6.1 Pare-feu, VPN et Traffic Shaping

Solution retenue

OPNSense

Alternatives étudiées

- Sophos XG
- FortiGate
- UFW / iptables (Linux)

Comparaison synthétique

Critère	**OPNsense / pfSense**	**Sophos / FortiGate**	**iptables / UFW**
Coût	Gratuit (open source)	Licence payante	Gratuit
Pare-feu avancé	Oui	Oui	Basique
VPN (IPsec, OpenVPN, WireGuard)	Oui	Oui	Oui (manuel)
Traffic Shaping / QoS	Oui (intégré)	Oui	Complexe
Interface graphique	Oui	Oui	Non
Adapté BTS / maquettage	Oui	Moyen	Peu

Avantages et inconvénients

OPNsense / pfSense offrent une solution complète intégrant pare-feu, VPN site-à-site, VPN nomade et gestion du Traffic Shaping dans une interface web claire. Ils sont largement utilisés dans les environnements professionnels et pédagogiques.

Leur principal inconvénient réside dans la nécessité d'une bonne compréhension réseau pour une configuration optimale, notamment pour la QoS et les règles avancées.

Justification du choix final

Le choix d'OPNsense s'impose par son **excellent rapport fonctionnalités / coût** et ses **richesse fonctionnelle**. Ils permettent de mettre en œuvre l'ensemble des exigences du projet (VPN, segmentation, filtrage, Traffic Shaping) sans dépendre de solutions propriétaires coûteuses.

6.2 Services d'annuaire et de résolution de noms

Solution retenue

Active Directory avec DNS intégré

Alternatives étudiées

- Samba AD
- LDAP + DNS Bind
- Azure Active Directory

Comparaison synthétique

Critère	Active Directory	Samba AD	LDAP + Bind
Centralisation des comptes	Oui	Oui	Oui
Gestion des GPO	Oui	Partielle	Non
Intégration Windows	Native	Bonne	Faible
Administration graphique	Oui	Limitée	Non
Usage en entreprise	Très répandu	Répandu	Technique

Avantages et inconvénients

Active Directory permet une **gestion centralisée des utilisateurs**, des ordinateurs et des droits, tout en offrant des **stratégies de groupe (GPO)** indispensables à la sécurisation des

postes. L’intégration du DNS simplifie l’administration et garantit le bon fonctionnement de l’authentification.

En contrepartie, cette solution nécessite des licences Windows Server et une maintenance rigoureuse.

Justification du choix final

Active Directory est retenu car il constitue une **référence dans les infrastructures professionnelles**, particulièrement dans les environnements Windows. Il répond parfaitement aux besoins d’authentification centralisée, de gestion des droits et de sécurité attendus dans le cadre de ce projet.

6.3 Services métiers : gestion et support

Solution retenue

GLPI (support informatique)
Dolibarr (ERP)

Alternatives étudiées

- GLPI → OTRS, Freshdesk
- Dolibarr → Odoo, ERPNext, Sage

Comparaison synthétique

Outil	Avantages principaux	Inconvénients
GLPI	Open source, AD natif, inventaire	Interface parfois complexe
OTRS	Ticketing puissant	Moins orienté inventaire
Dolibarr	Léger, open source, modulaire	Fonctionnalités avancées limitées
Odoo	Très complet	Plus lourd, plus complexe

Justification du choix final

GLPI est retenu pour sa **gestion du support**, son **système de ticketing** et son **intégration native avec Active Directory**, ce qui facilite l’administration des utilisateurs et des droits. Dolibarr est choisi pour la gestion administrative et financière en raison de sa **simplicité**, de sa **légèreté** et de son **adéquation aux besoins d’une PME**.

Ces deux solutions sont open source, bien documentées et parfaitement adaptées à un contexte pédagogique et professionnel.

6.4 Supervision, sauvegarde et audit de sécurité

Solutions retenues

Prometheus, **rsync**, **PingCastle**, **Lynis**

Alternatives étudiées

- Supervision : Zabbix, Nagios
- Sauvegarde : Bacula, Veeam
- Audit : Nessus, OpenVAS

Comparaison synthétique

Domaine	Solution retenue	Avantages	Inconvénients
Supervision	Prometheus	Léger, moderne, Docker	Nécessite configuration
Sauvegarde	rsync	Simple, fiable, scriptable	Pas d'interface graphique
Audit AD	PingCastle	Spécialisé AD	Limité à AD
Audit Linux	Lynis	Rapide, complet	Lecture des rapports

Justification du choix final

Les outils retenus sont **légers**, **open source** et **adaptés à une infrastructure de taille moyenne**. Prometheus permet un suivi précis des ressources, rsync assure des sauvegardes fiables et automatisables, tandis que PingCastle et Lynis offrent une vision claire du niveau de sécurité des systèmes Windows et Linux.

Ces choix garantissent une **bonne couverture fonctionnelle** tout en restant cohérents avec les objectifs pédagogiques du projet.

6.5 Dimensionnement des machines

Nom	Rôle	CPU	RAM	Stockage	Type stockage	OS	Édition	V
FW-MRS	Pare-feu / VPN	2 vCPU	2 Go	20 Go	SSD	OPNsense	CE	S
MRS-DC1	AD / DNS (principal)	2 vCPU	4 Go	60 Go	SSD	Windows Server	Standard (GUI)	2
MRS-DC2	AD / DNS (secondaire)	2 vCPU	2 Go	40 Go	SSD	Windows Server	Standard (Core)	2

Nom	Rôle	CPU	RAM	Stockage	Type stockage	OS	Édition	V
MRS-GLPI	Ticketing / Inventaire	2 vCPU	4 Go	80 Go	SSD	Debian	Serveur	1
MRS-BACKUP	Sauvegardes	2 vCPU	4 Go	500 Go	HDD	Debian	Serveur	1

7. Plan de tests de l’infrastructure

Le plan de tests a pour objectif de valider le bon fonctionnement, la sécurité et la résilience de l’infrastructure mise en place. Il permet de vérifier que les besoins exprimés dans le cahier des charges sont correctement couverts avant la mise en exploitation.

7.1 Tests fonctionnels

Les tests fonctionnels visent à s’assurer que les services fournis aux utilisateurs sont opérationnels et conformes aux attentes.

ID	Test	Méthode	Résultat attendu
TF-01	Connexion utilisateur AD	Ouverture de session sur poste collaborateur	Authentification réussie
TF-02	Application des GPO	Connexion poste utilisateur	Lecteurs mappés, politiques appliquées
TF-03	Accès partages réseau	Accès aux dossiers par service	Droits respectés
TF-04	Accès GLPI	Connexion via navigateur	Accès autorisé selon groupe
TF-05	Accès Dolibarr	Connexion ERP	Accès restreint par rôle
TF-06	VPN site-à-site	Ping inter-sites	Communication fonctionnelle
TF-07	VPN nomade	Connexion distante	Accès aux ressources internes
TF-08	Sauvegarde	Exécution script rsync	Sauvegarde terminée sans erreur

7.2 Tests de sécurité

Les tests de sécurité permettent de valider la protection du système d'information face aux accès non autorisés et aux mauvaises configurations.

ID	Test	Méthode	Résultat attendu
TS-01	Isolation VLAN	Tentative d'accès direct serveur depuis LAN collaborateur	Accès refusé hors flux autorisés
TS-02	Règles pare-feu	Scan de ports ciblé	Ports non autorisés fermés
TS-03	Politique de mot de passe	Création mot de passe faible	Refus
TS-04	Accès VPN	Tentative sans certificat	Connexion refusée
TS-05	Audit AD	Analyse PingCastle	Niveau de risque maîtrisé
TS-06	Audit Linux	Analyse Lynis	Aucune alerte critique

7.3 Tests de continuité de service

Ces tests permettent de vérifier la disponibilité des services critiques en cas d'incident.

ID	Test	Méthode	Résultat attendu
TC-01	Arrêt DC principal	Arrêt volontaire	Authentification toujours possible
TC-02	Coupure lien inter-sites	Simulation panne WAN	Fonctionnement local maintenu
TC-03	Restauration sauvegarde	Restauration fichier / BDD	Données récupérées
TC-04	Surcharge réseau collaborateur	Test bande passante	Services critiques prioritaires

8. Cahier des charges technique

Cette section constitue le livrable technique de référence. Elle formalise l'architecture, les configurations attendues et les paramètres de sécurité.

8.1 Tableau technique – Plan d'adressage et serveurs

Site	Service	Rôle	Adresse IP
Marseille	TLS-DC1	AD / DNS (GUI)	192.168.20.10
Marseille	TLS-DC2	AD / DNS (Core)	192.168.20.11
Marseille	Dolibarr	ERP	192.168.20.30
Marseille	Backup	Sauvegardes	192.168.20.40
Marseille	OPNsense	Firewall	10.34.50.51
Toulouse	MRS-DC1	AD / DNS (GUI)	192.168.200.10
Toulouse	MRS-DC2	AD / DNS (Core)	192.168.200.11
Toulouse	GLPI	Ticketing	192.168.200.30
Toulouse	Backup	Sauvegardes	192.168.200.40

8.2 Description des configurations attendues

Chaque site dispose d'un pare-feu OPNsense configuré comme passerelle par défaut, assurant le filtrage, le routage inter-VLAN, la terminaison VPN et la mise en œuvre de la QoS. Les réseaux sont segmentés entre LAN Collaborateurs et LAN Serveurs, avec un contrôle strict des flux.

L'authentification est centralisée via Active Directory, avec réplication locale sur chaque site. Les services métiers sont intégrés à l'annuaire afin de garantir une gestion cohérente des droits.

La supervision est assurée par Prometheus, tandis que les sauvegardes sont automatisées à l'aide de scripts basés sur rsync.

8.3 Paramètres de sécurité et de QoS

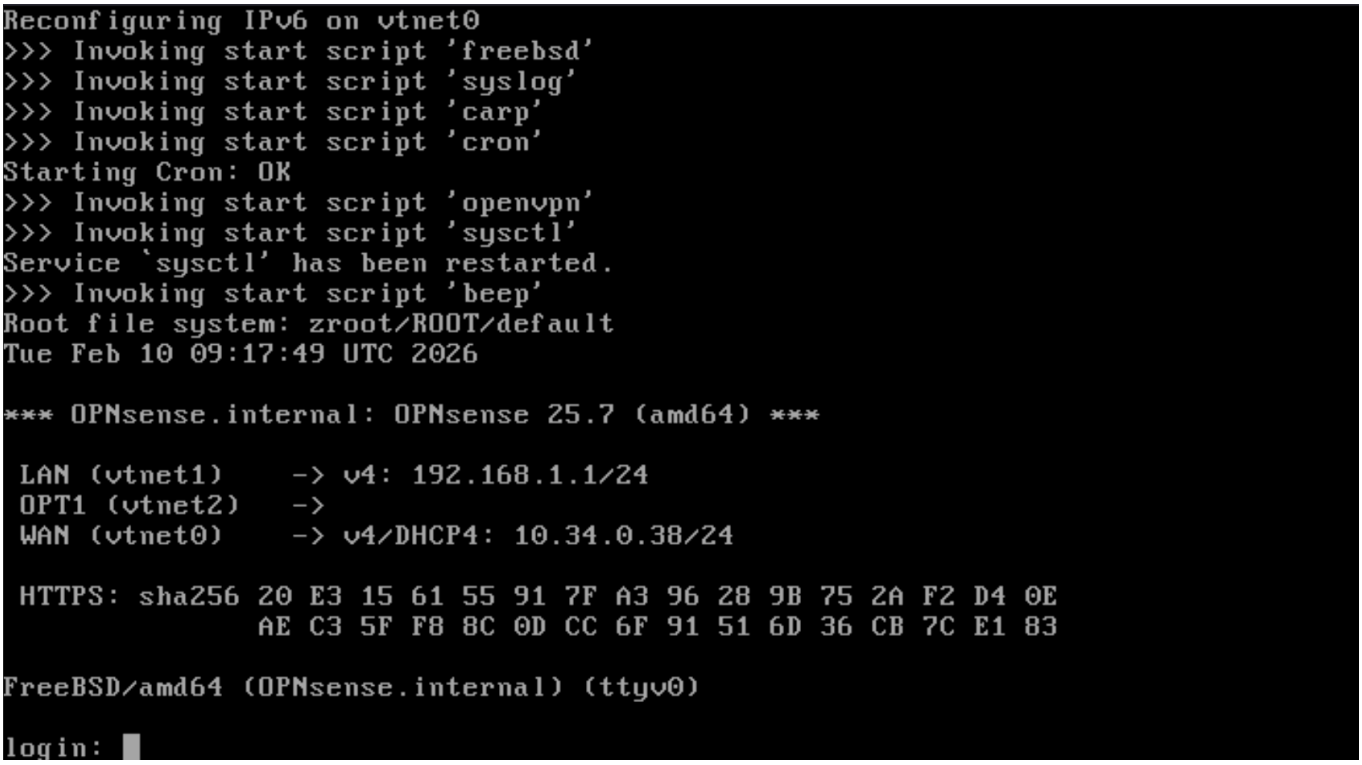
Les paramètres de sécurité reposent sur une politique de filtrage restrictive, n'autorisant que les flux nécessaires au fonctionnement des services. Les accès distants sont exclusivement réalisés via VPN chiffré.

La qualité de service est mise en œuvre sur le LAN Collaborateurs avec une limitation de débit à **5 Mb/s**, afin d'éviter toute saturation et de garantir la priorité aux services critiques tels que l'authentification, l'ERP, le support GLPI et les tunnels VPN.

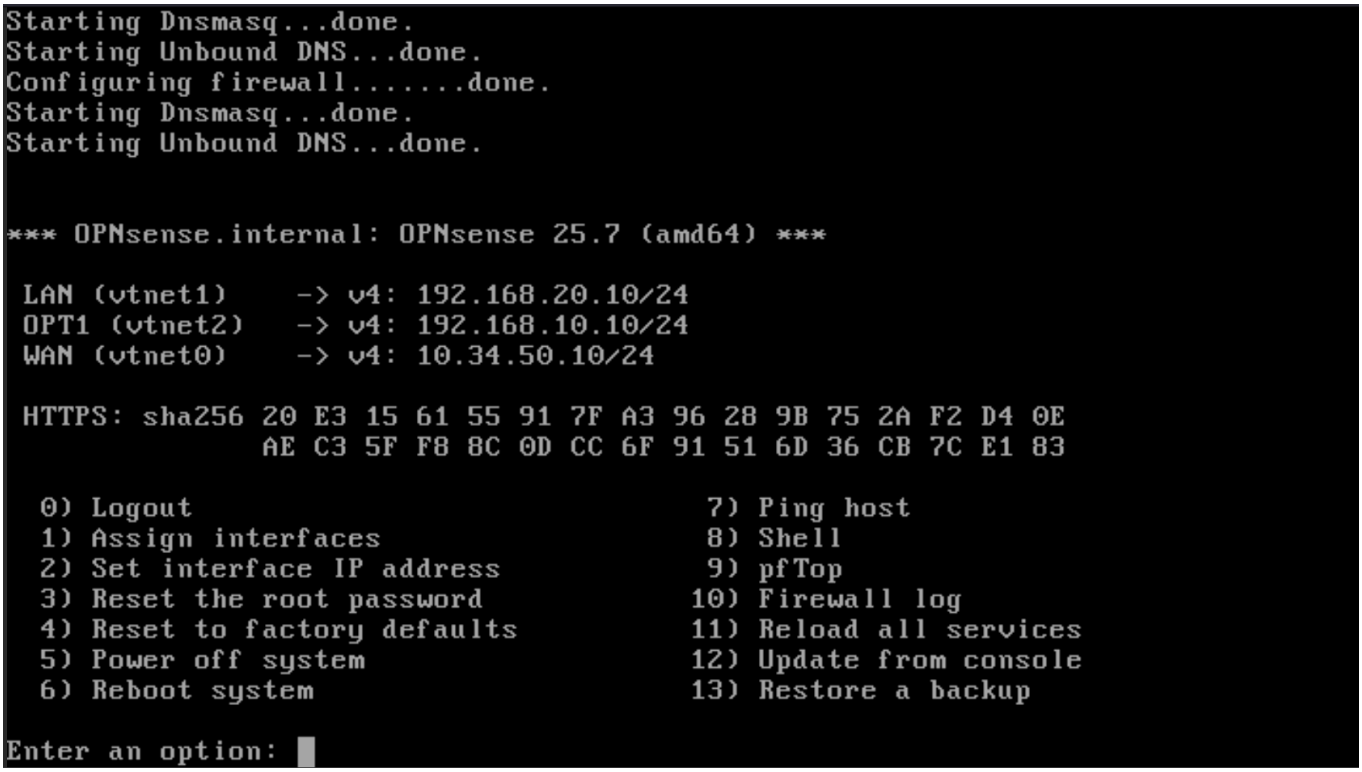
Phase 2 : Déploiement et mise en œuvre

1. Installation des pare-feux OPNSense

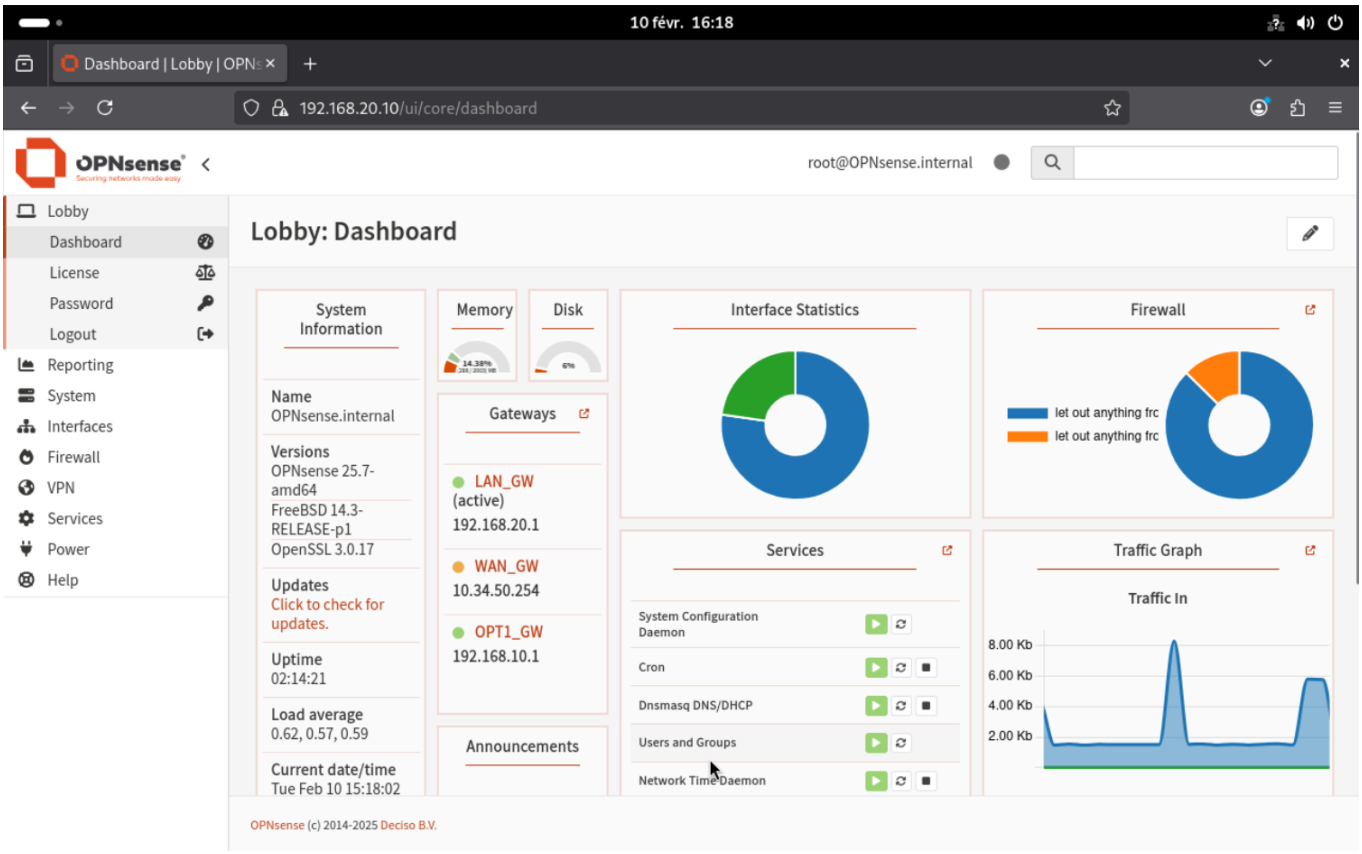
Installation de la VM OPNSense :



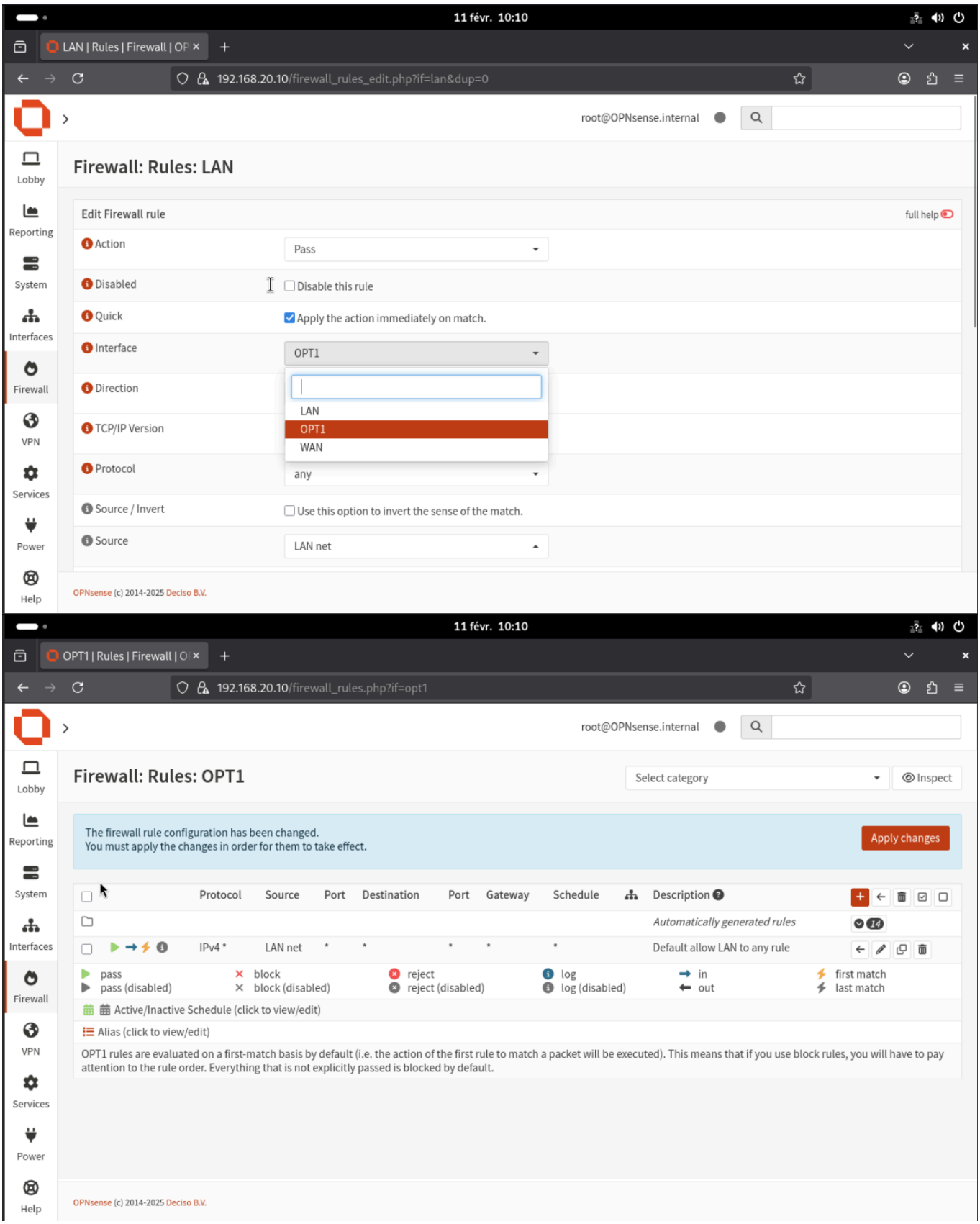
Je configure comme sur mon plan d'adressage mes cartes réseaux :



Je créer une VM Admin (Debian 13) relier à ma carte réseaux net1 me permettant d'accéder à mon interface OPNSense :



Maintenant je configure les règles de filtrages, je décide en premier temps de dupliquer la règles autorisant tout depuis mon interface LAN vers mon interface OPT1 :



2. VPN client-to-site

https://docs.opnsense.org/manual/how-tos/wireguard-client.html

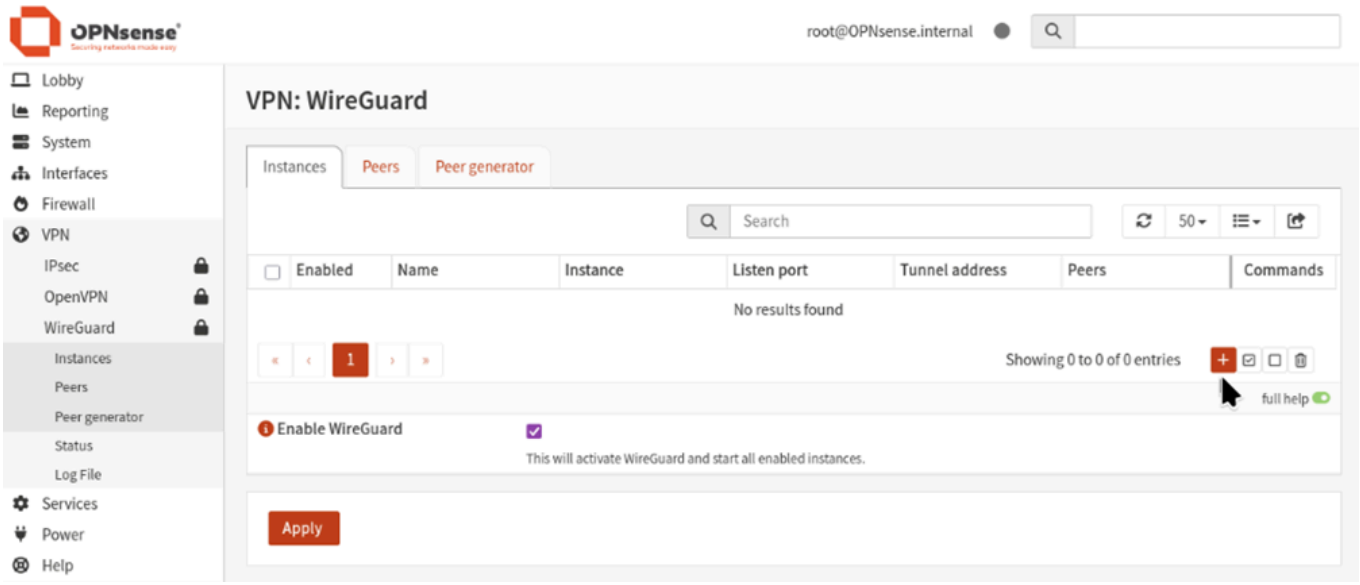
Choix protocole

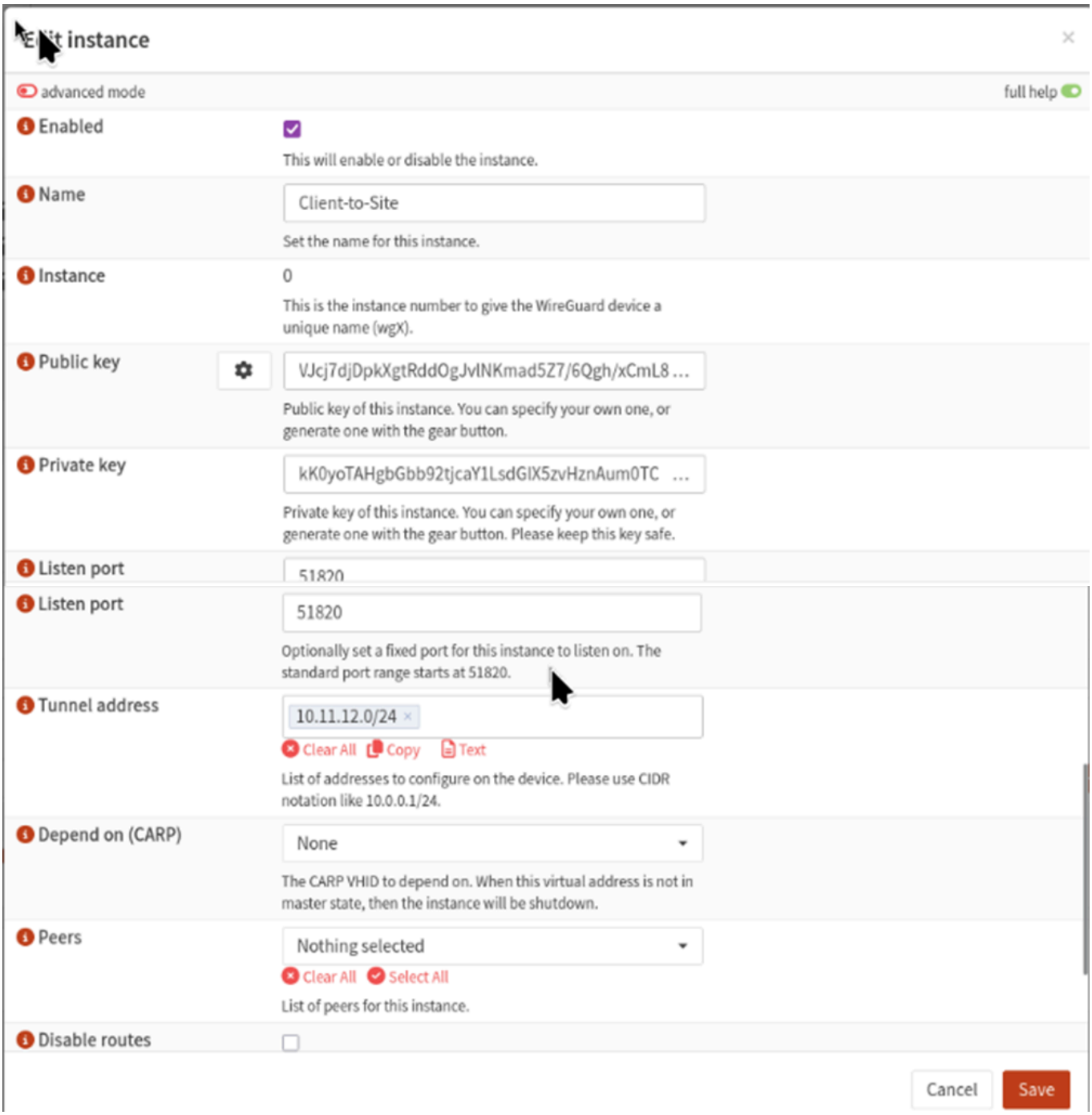
Trois choix s’offrent à nous dans OPNsense :

- OPNvpn : reference depuis des années, c’est un protocole éprouvé mais qui nécessite des manipulations et est un peu lourd en ressources CPU selon le chiffrement demandé

- Ipsec : robuste, il nécessite une configuration assez lourde. Plus adapté à du site to site qu’à un VPN roadwarrior

- Wireguard : protocole moderne, relativement peu de manipulations, et plus léger qu’OPNvpn coté CPU. Ce sera notre protocole de choix ici





note : on expose pas sa clé privée normalement.

On reviendra sur la config plus tard.

Creer client

Peer generator pour gagner du temps :

Instances | Peers | Peer generator

Instance
Client-to-Site
Choose an instance to create a new peer for.

Endpoint
10.34.40.1:51820
Specify how to reach the instance, usually the public address of this firewall. (e.g. my.endpoint.local:51820)

Name
Windows-Client-1
Set the name for this peer.

Public key
bLTnQ/ELWrD6U5jwpqXGkHFG/4hLCsDKdfC/zpU …
Public key of this peer. You can generate the key using the private key piped to "wg pubkey".

Private key
WJjNdoiAusvLSR8t3R4t5PAFnpkYshox2vjCsSHKx …
Private key of this peer, not stored on this host, only used for the configuration below.

Address
10.11.12.1/32

Pre-shared key
/fr+QXQNadqLy2yGZD9PZH1gbGQ8FXP1y63Os8G…
Optional shared secret (PSK) for this peer.

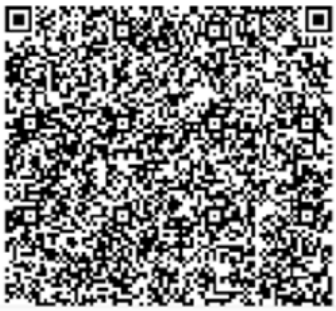
Allowed IPs
0.0.0.0/0,::/0
List of networks allowed to pass through the tunnel adapter. Use CIDR notation like 10.0.0.0/24.

Keepalive interval
Set persistent keepalive interval in seconds.

DNS Servers
1.1.1.1
Comma-separated list of DNS servers to use on the peer.

Config

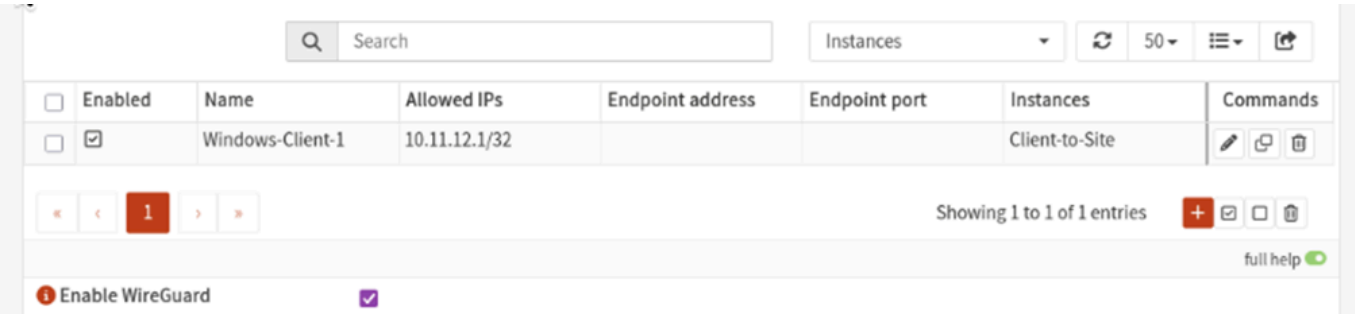
```
[Interface]
PrivateKey =
WJjNdoiAusvLSR8t3R4t5PAFnpkYshox2vjCsSHKxk8=
Address = 10.11.12.1/32

[Peer]
PublicKey = VJcj7djDpkXgtRddOgJvlNKmad5Z7/6Qgh/
xCmL8jjg=
PresharedKey = /
fr+QXQNadqLy2yGZD9PZH1gbGQ8FXP1y63Os8GKaqM=
Endpoint = 10.34.40.1:51820
AllowedIPs = 0.0.0.0/0,::/0
```



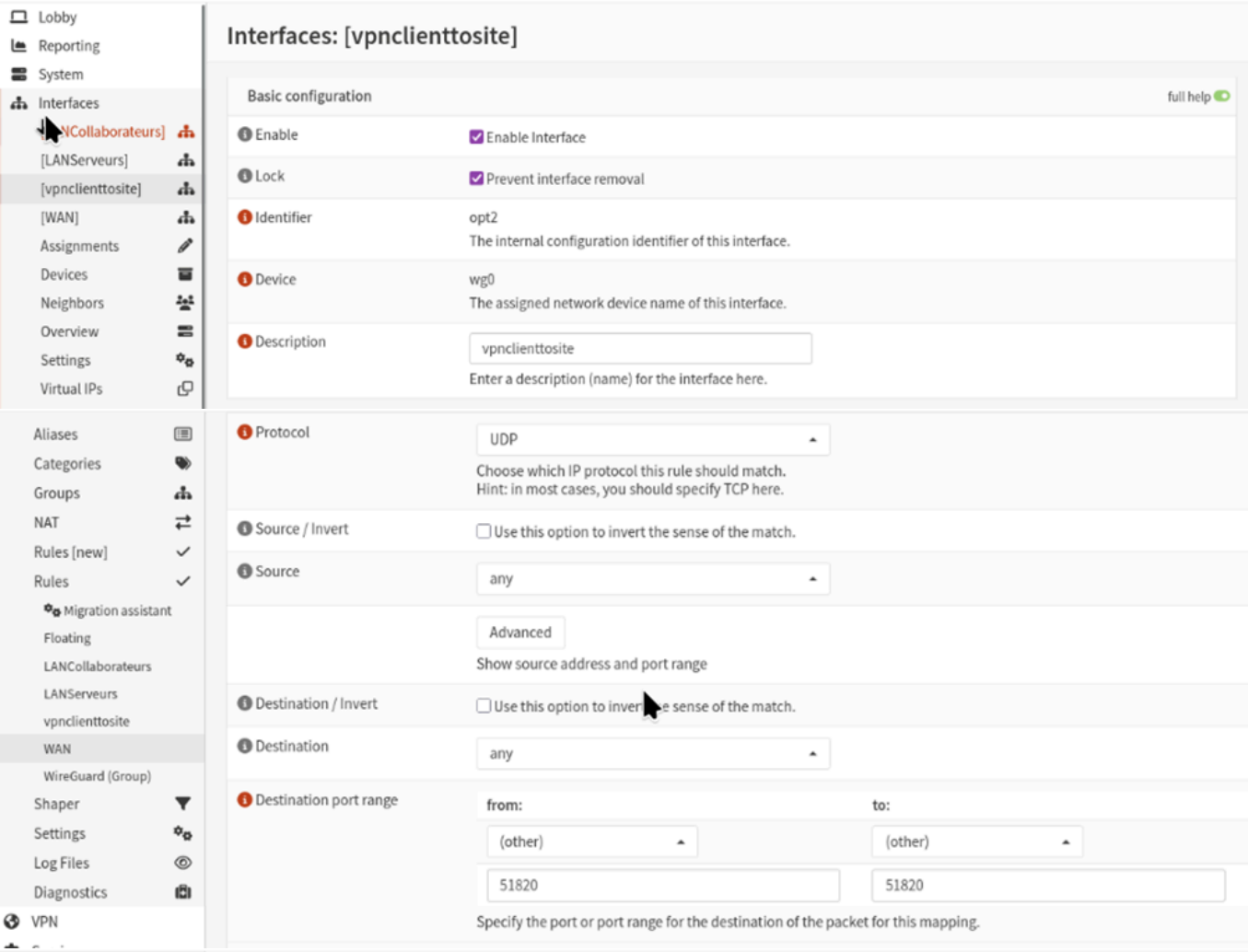
Store and generate next
Store the public parts of this peer and generate a keypair for the next.

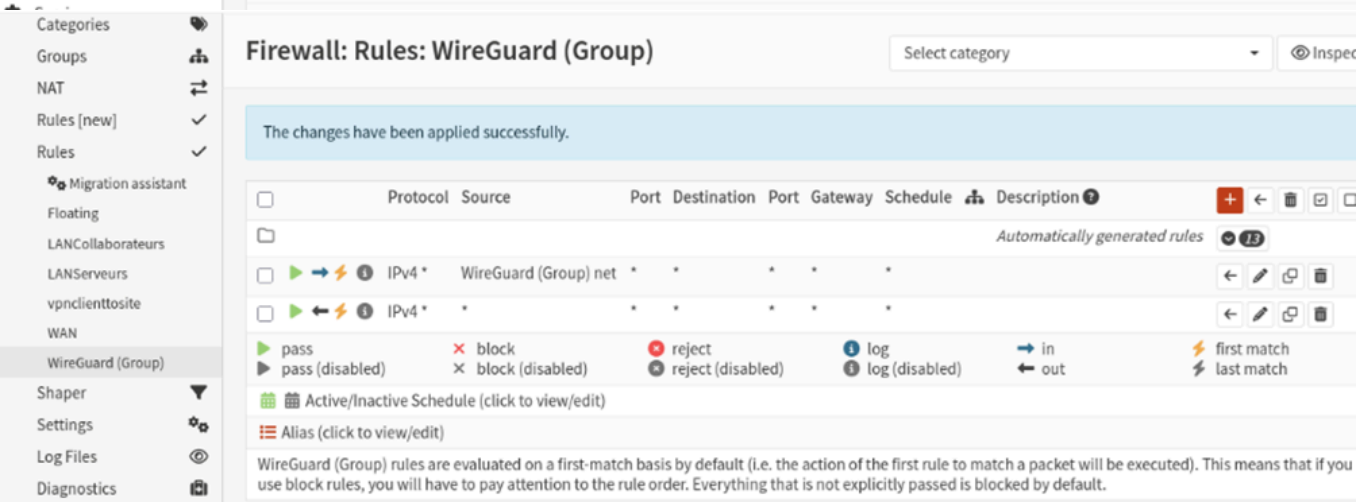
Enable WireGuard
This will activate WireGuard and start all enabled instances.

Apply

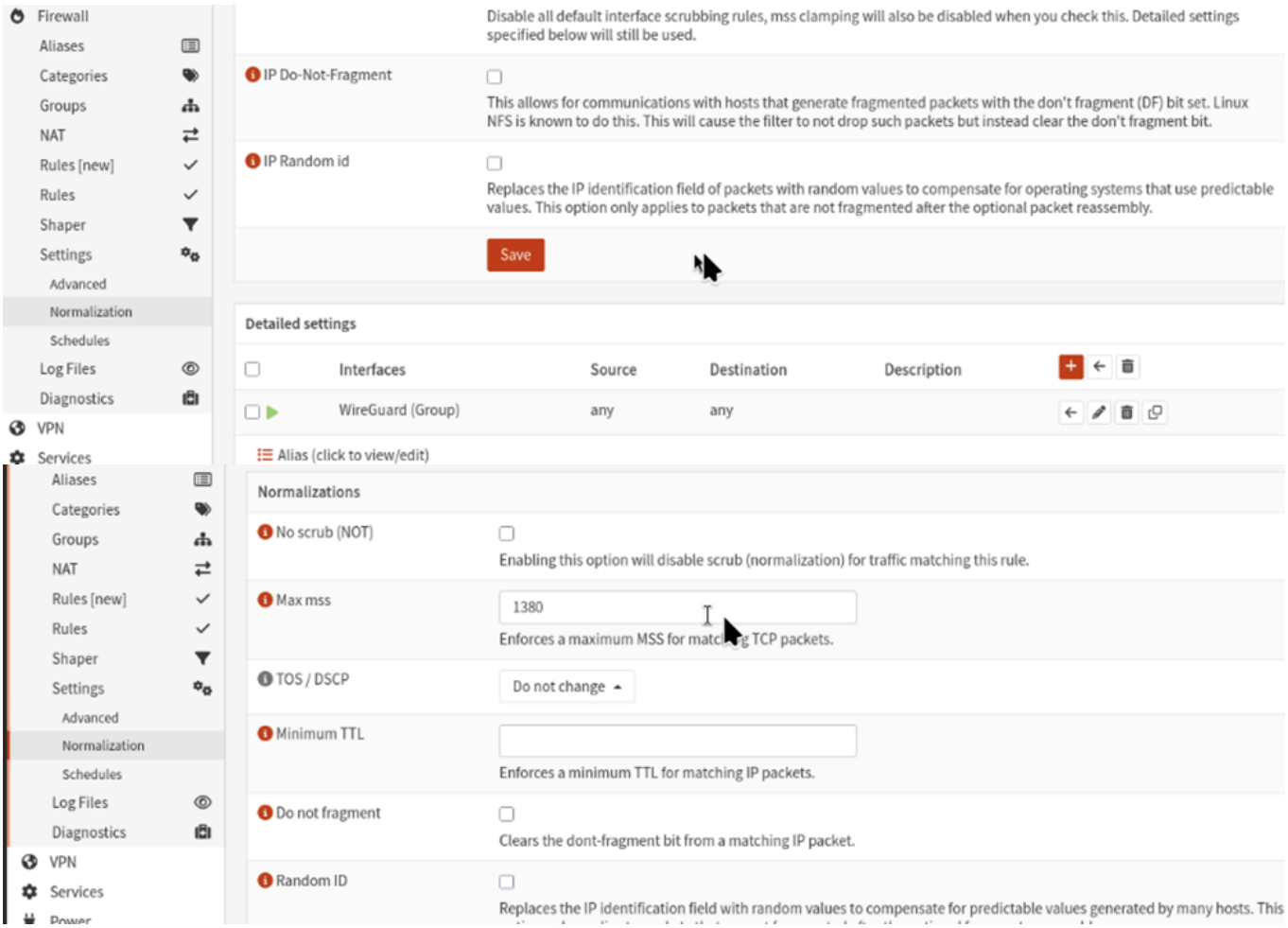


Configurer interface et pare feu





Normalisation :



Configurer client (windows)

Installer le client

copier la configuration

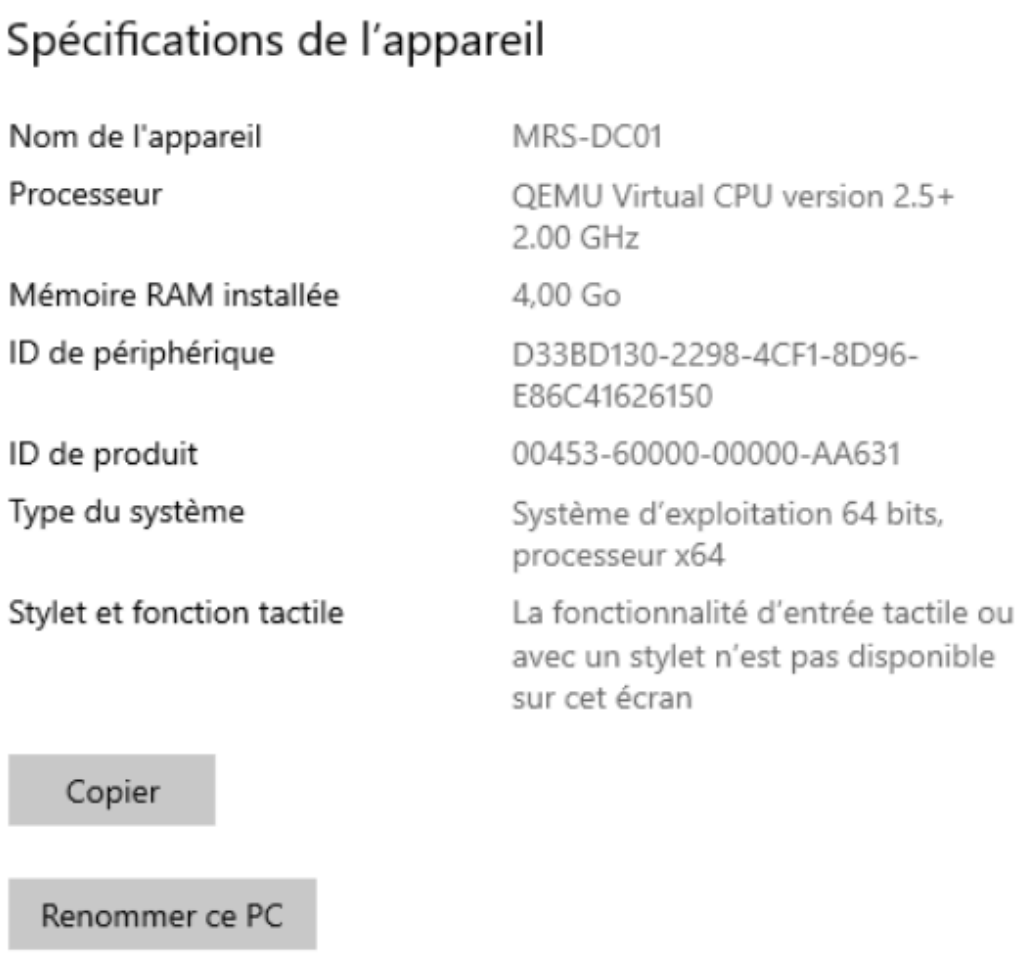
connecter

3. Installation Active Directory et DNS

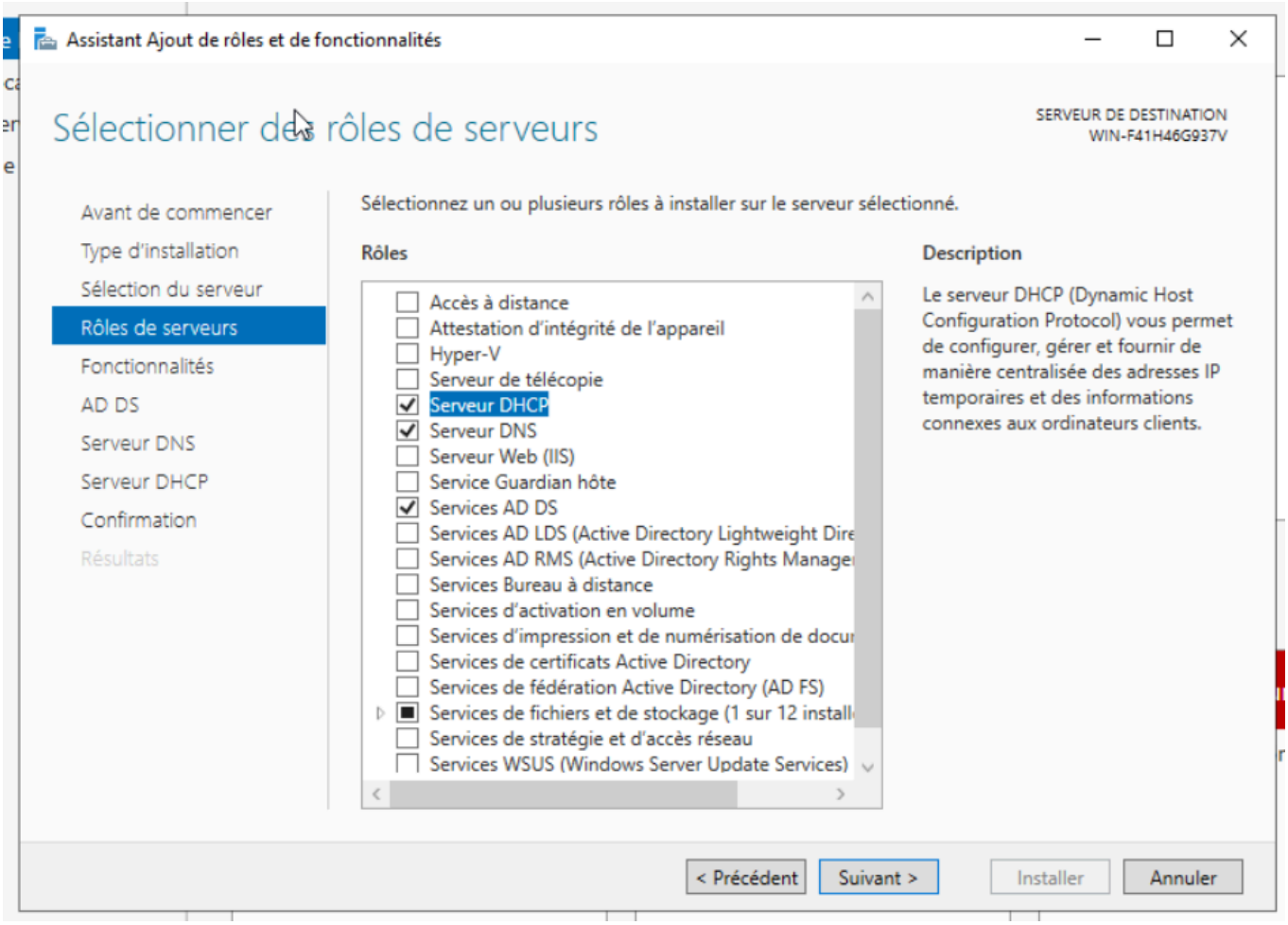
3.1 Configuration du DC

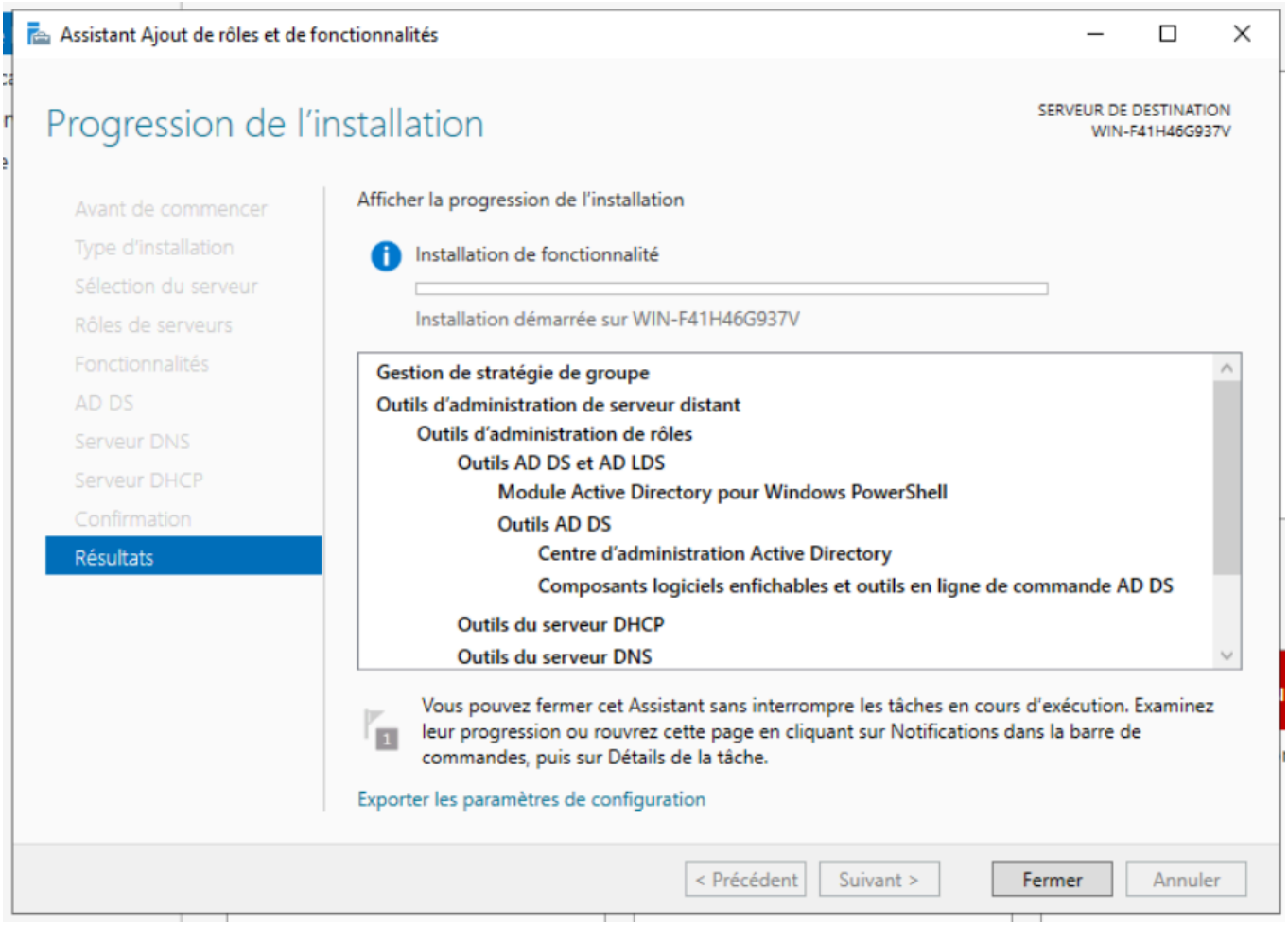
Configuration de l'IP fixe pour le serveur :

Je renomme le serveur :



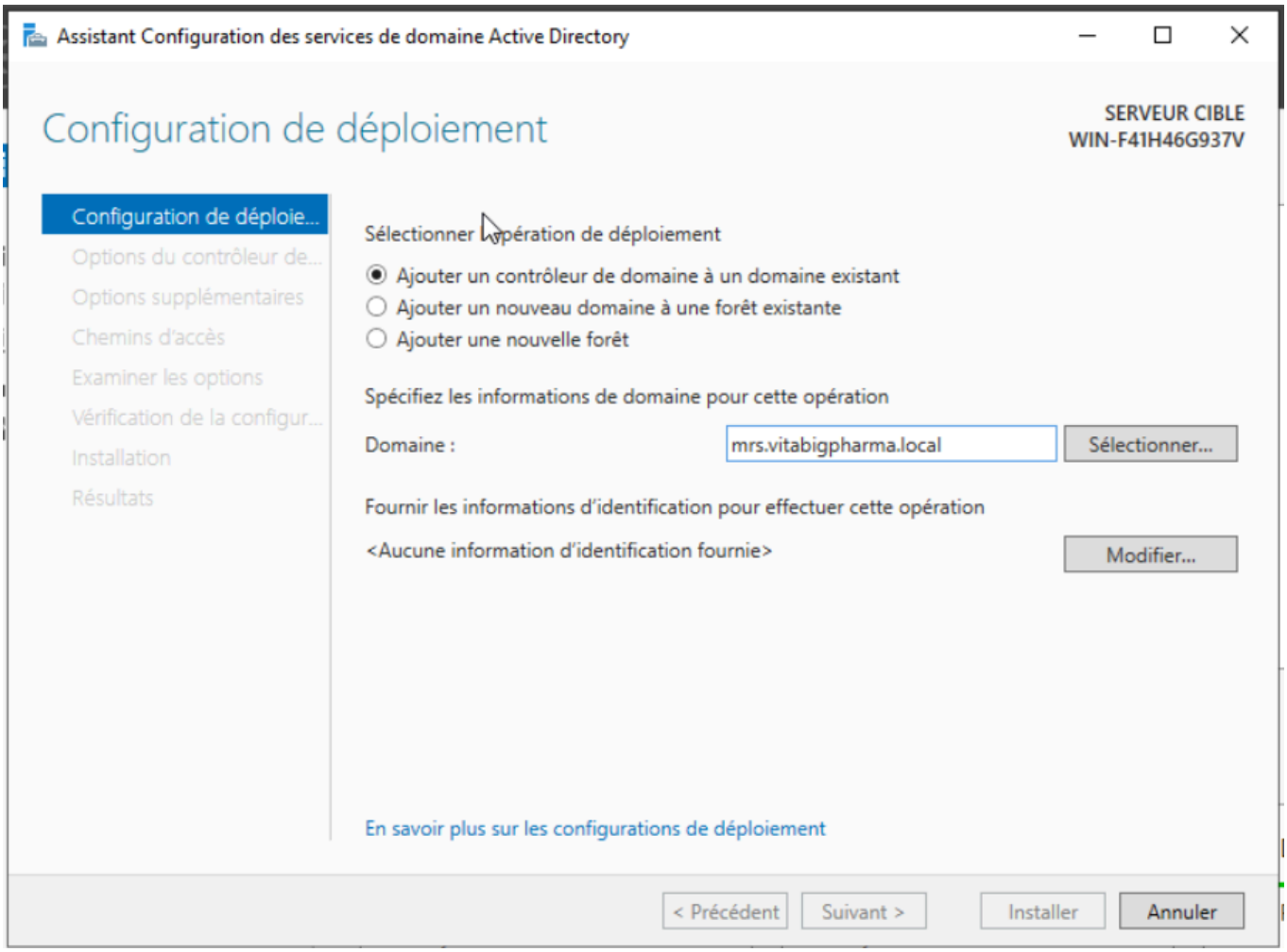
Je configure mon serveur Windows 10 pour en faire un serveur AD, DNS et DHCP :

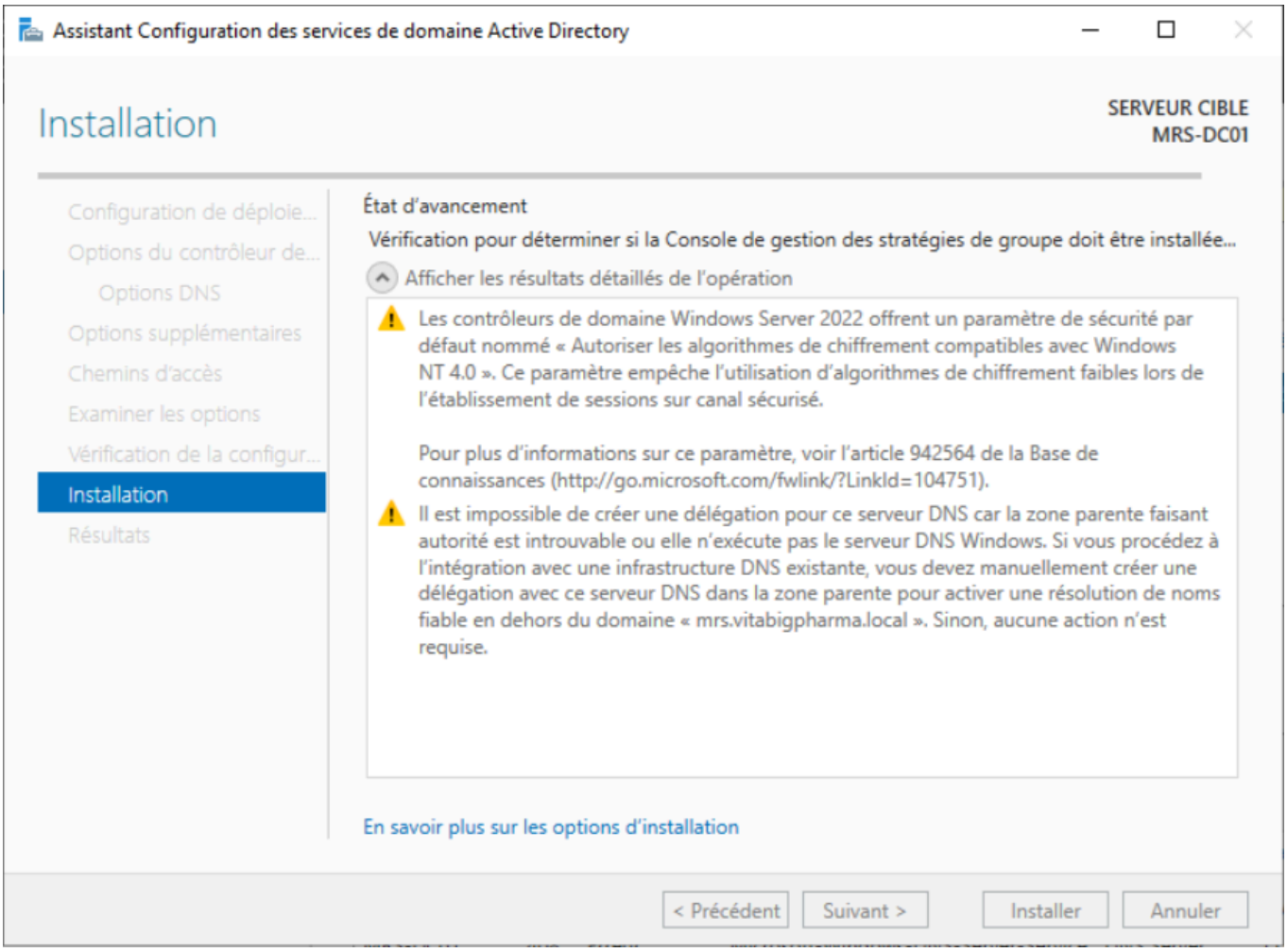




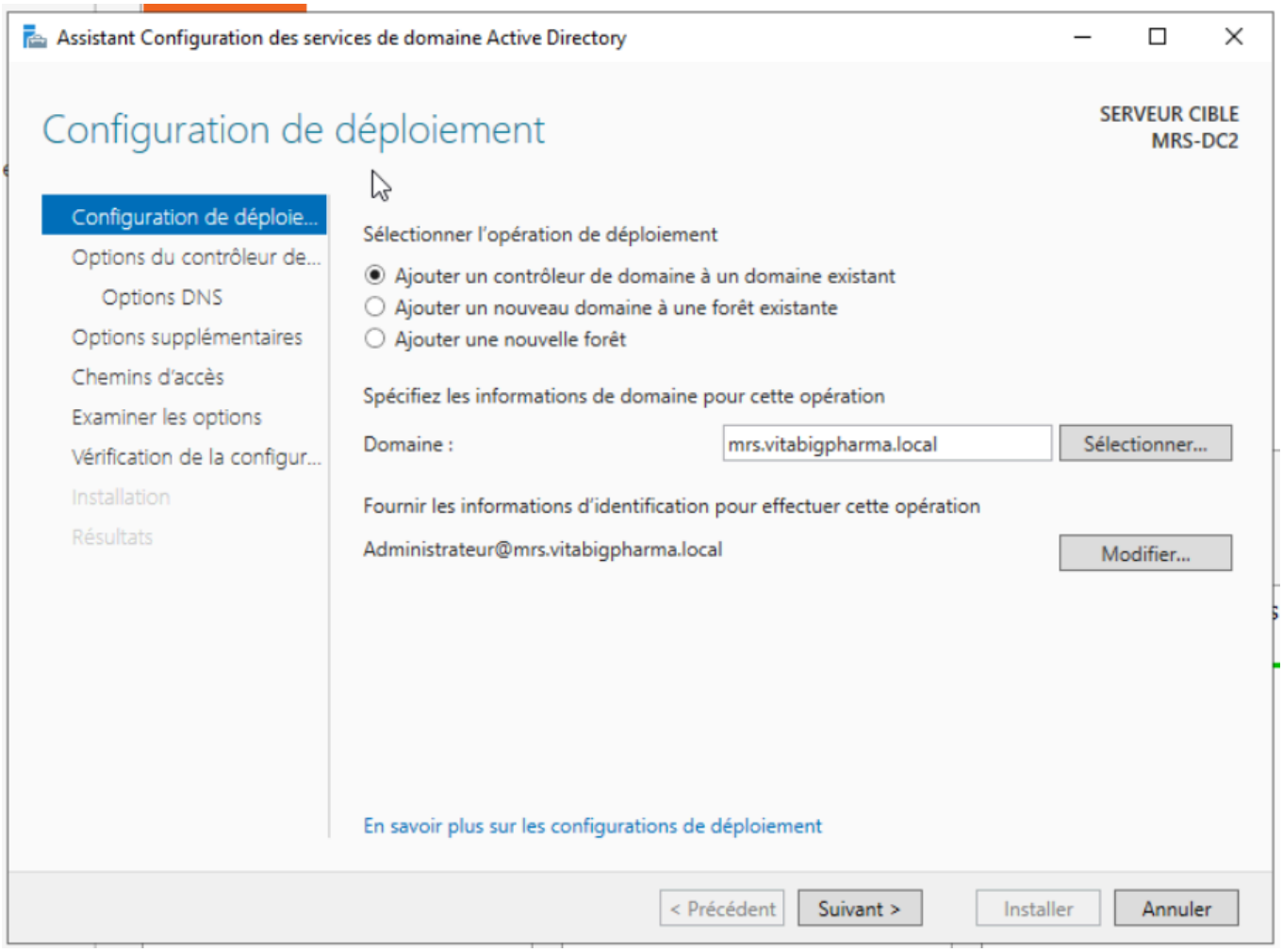
3.2 Configuration de l'AD

Configuration du nom de domaine :



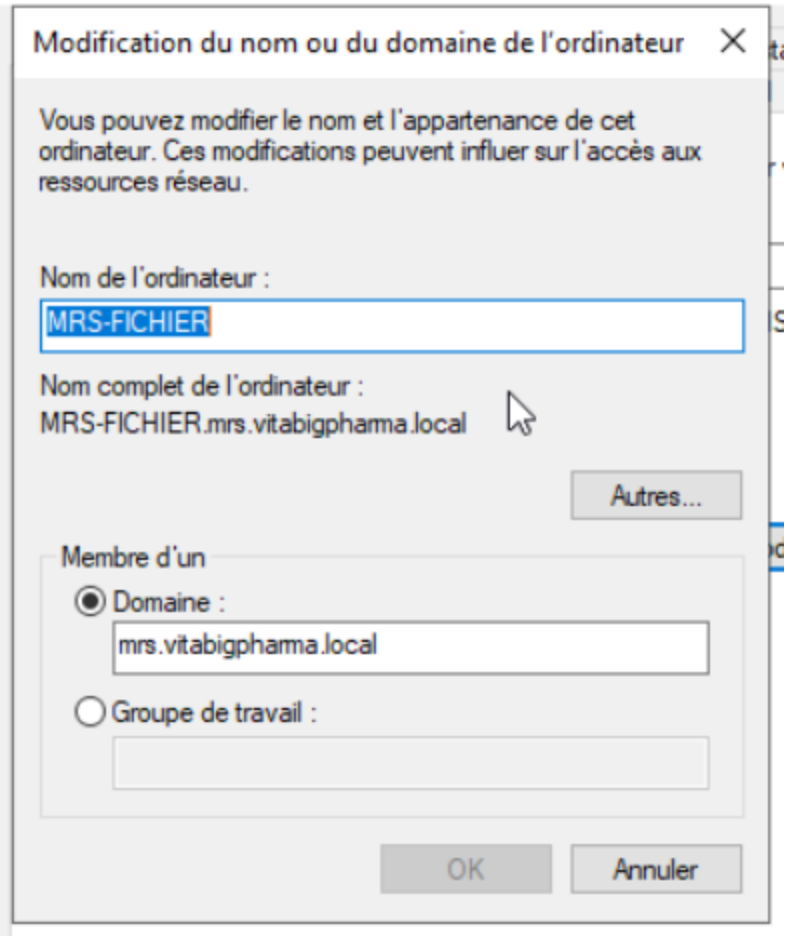


AD mis en place, maintenant je créer un second pour qu'il puisse prendre le relais en cas de panne :

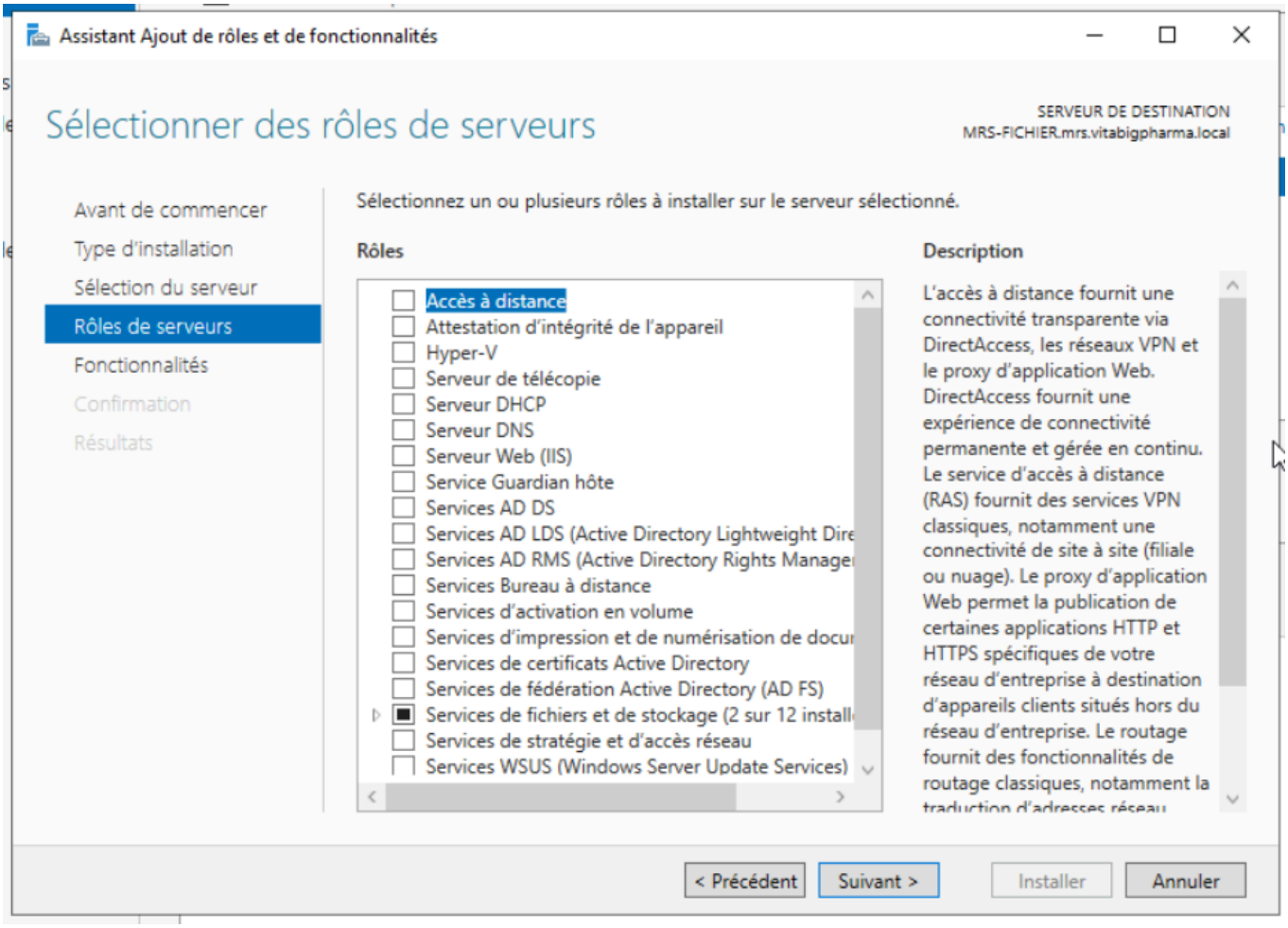


3.3 Déploiement d'un serveur de fichier

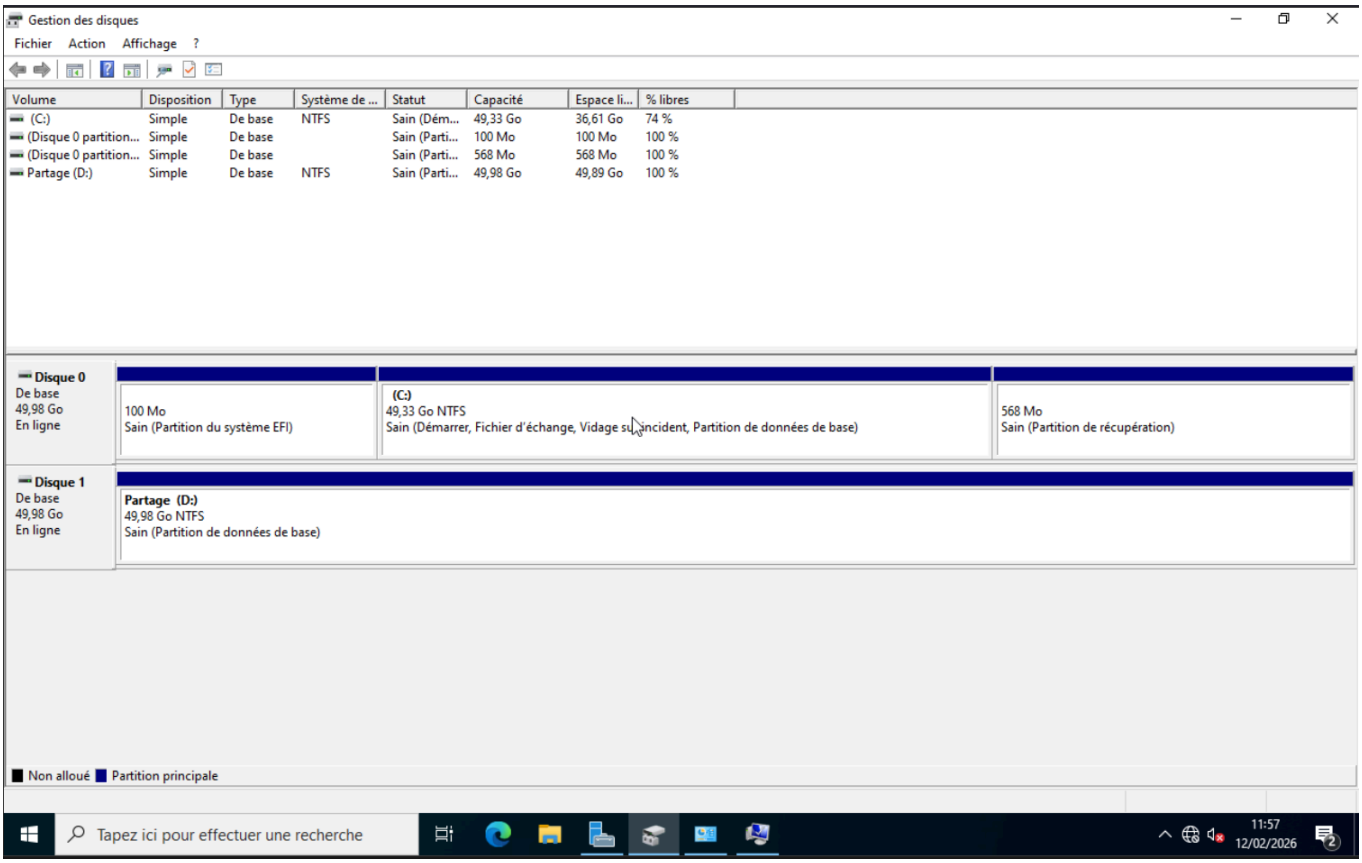
Ajout du serveur au domaine



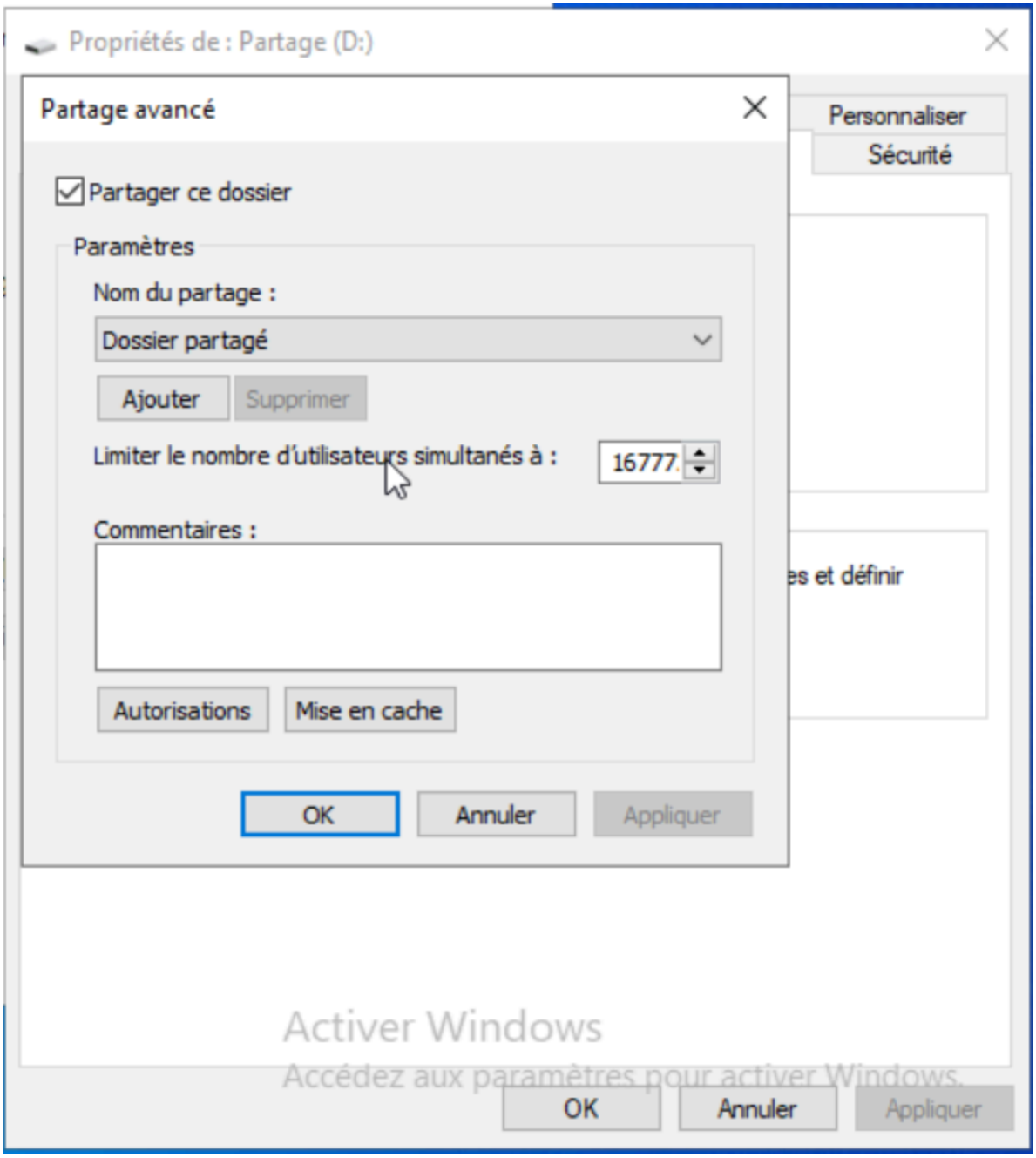
Déclaration du serveur en tant que serveur de fichier



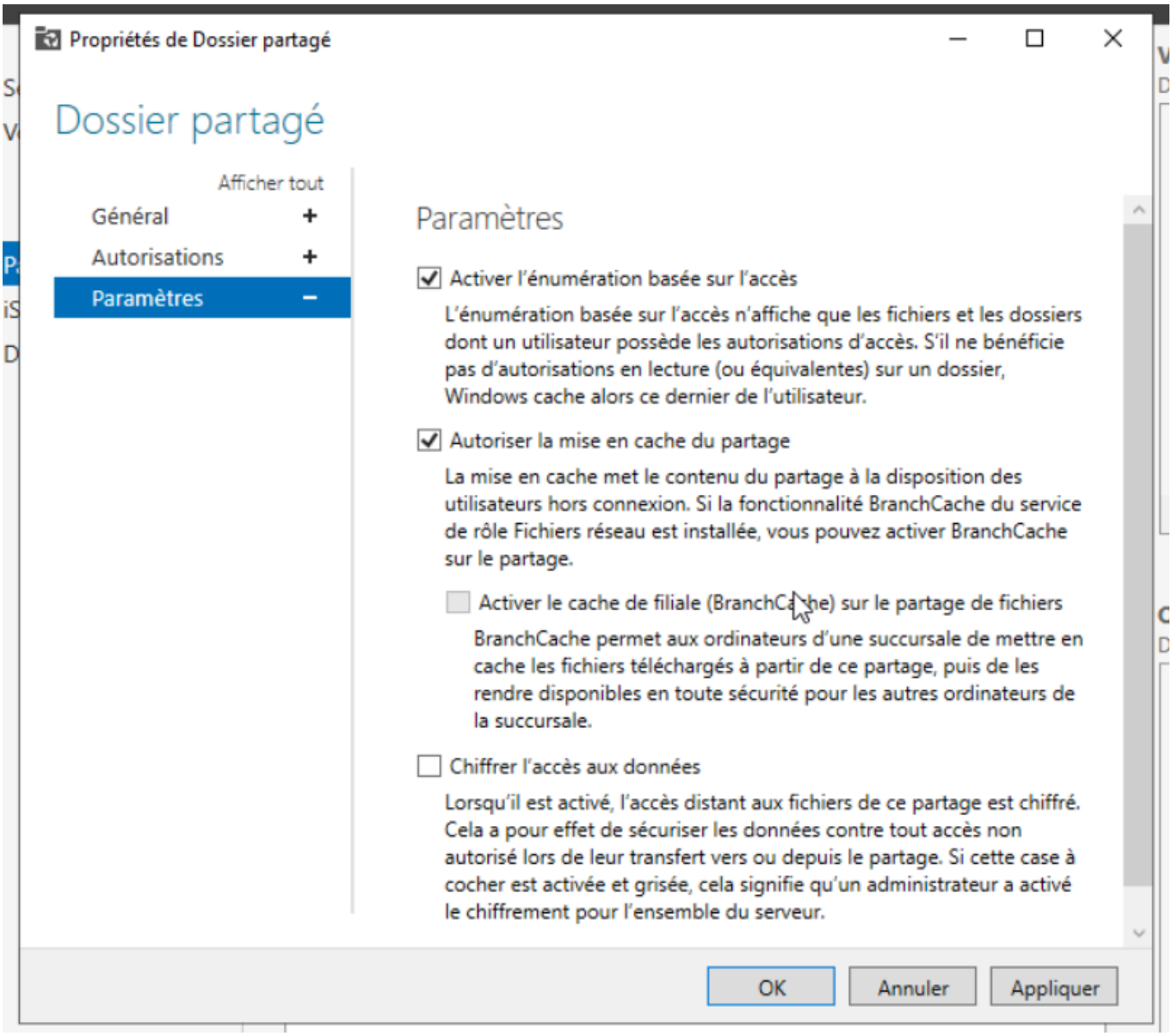
Ajout d'un disque de partage sur le serveur



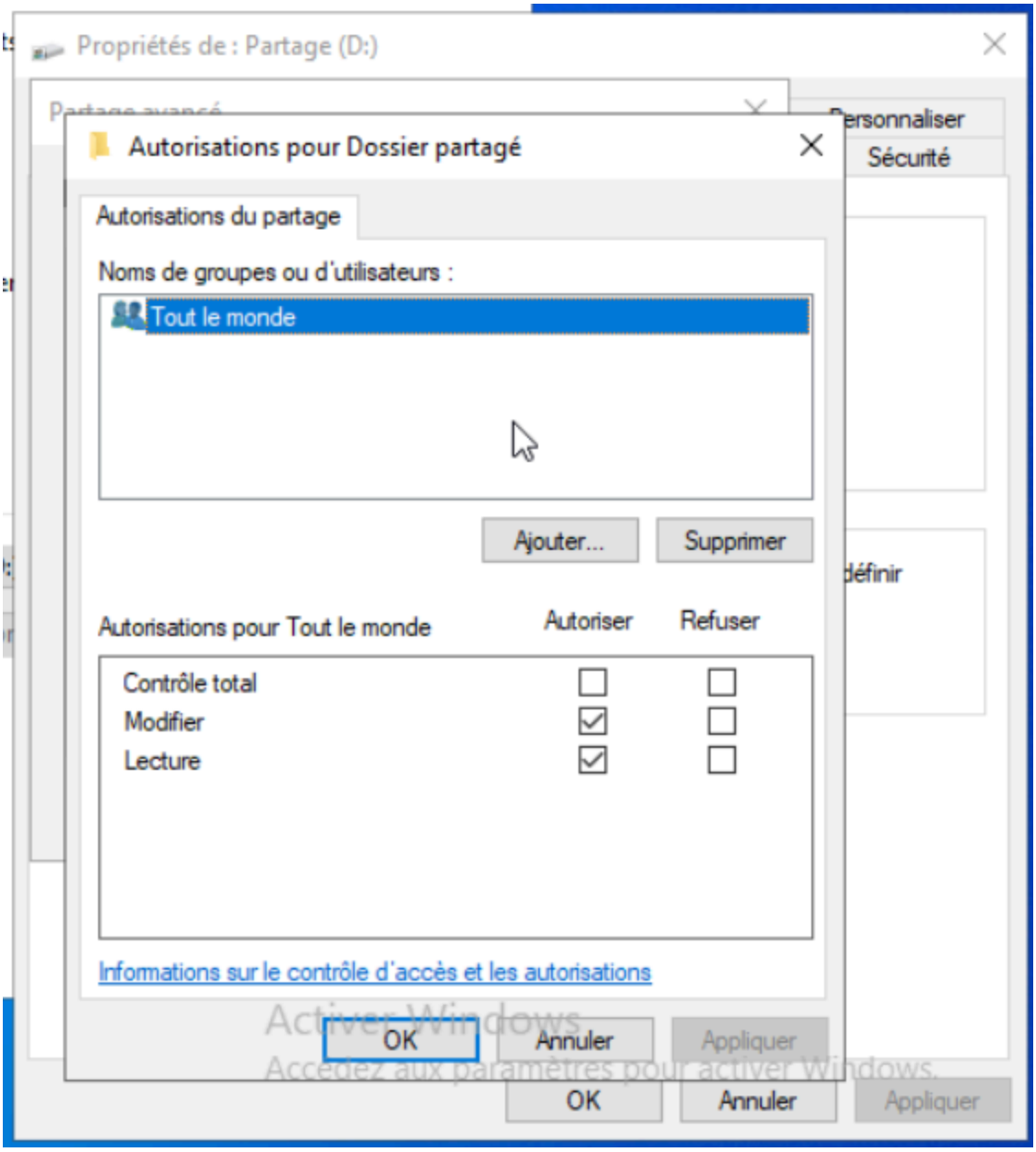
Partage du disque de partage sur le réseau



J'active l'ABE



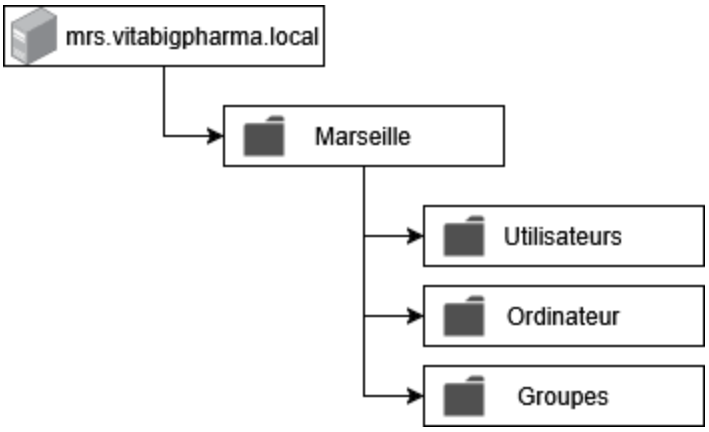
Je gère les droits d'accès



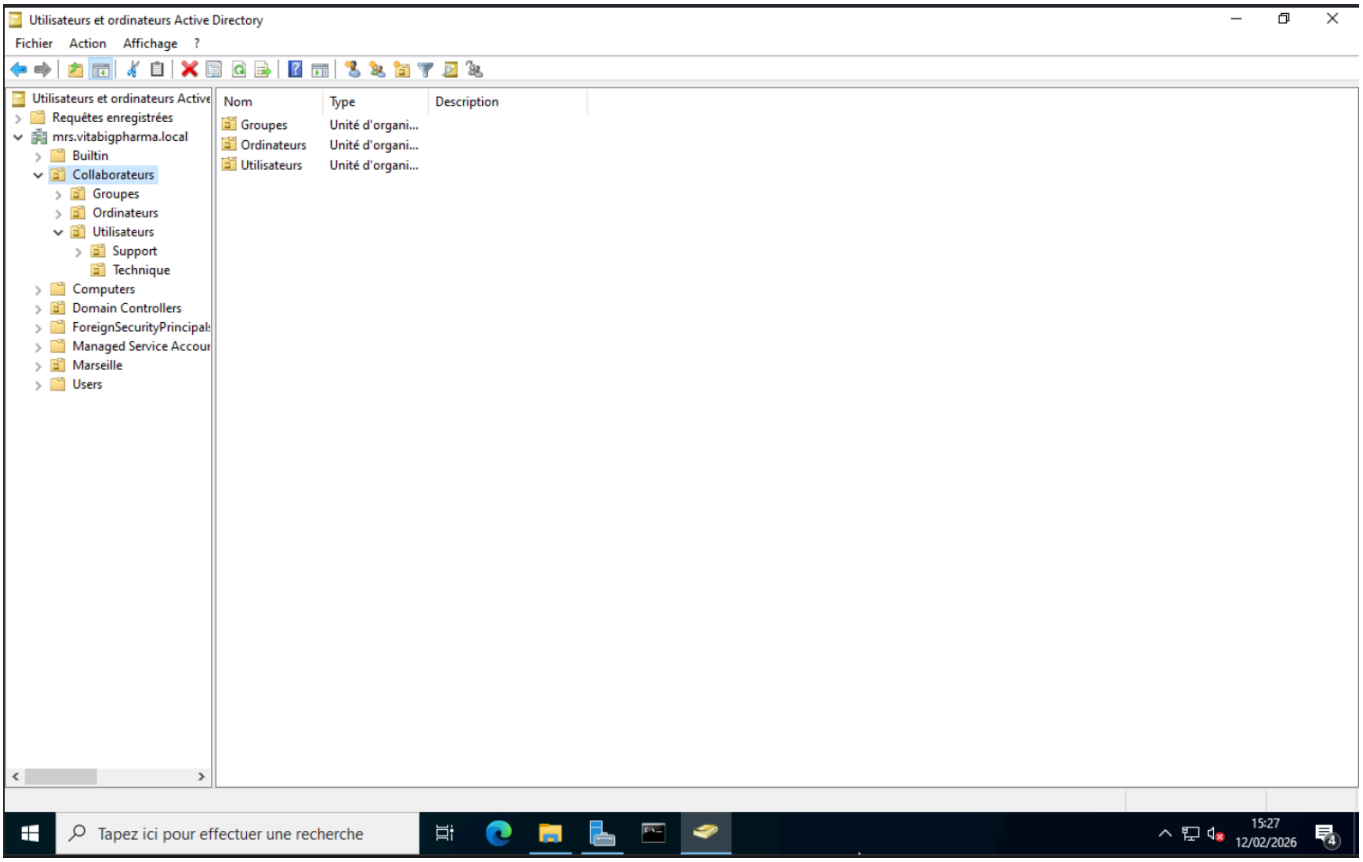
3.4 Déploiement des utilisateurs

Un fichiers csv nous est fourni, il recense tout les utilisateur et leurs fonction, l'objectif est de créer un script de déploiement en PowerShell :

Voici le schéma de la forêt que je souhaite mettre en place



Je créer les OU dans l'Active Directory, pour que mon script range les utilisateurs



Puis je passe les script réaliser et les utilisateurs et groupe remonte

```
<#
Deploy-ADUsersFromCsv.ps1
Domaine: mrs.vitabigpharma.local
Arborescence OU: OU=Collaborateurs -> OU=Utilisateurs | OU=Ordinateurs |
OU=Groupes
CSV attendu: Prenom, Nom, Email, OU (service), Groupe
#>

# ==========================
# ========== VARS =========
# ==========================
```

```
$CsvPath = ".\users_marseille.csv"     # <-- adapte si besoin

$DomainDN   = "DC=mrs,DC=vitabigpharma,DC=local"
$DomainFqdn = "mrs.vitabigpharma.local"

$RootOUName      = "Collaborateurs"
$UsersOUName     = "Utilisateurs"
$ComputersOUName = "Ordinateurs"
$GroupsOUName    = "Groupes"

$GenerateRandomPassword = $true
$DefaultPassword = "P@ssw0rd-Temp-2026!"   # utilisé si
$GenerateRandomPassword = $false
$PasswordLength  = 16
$ForceChangePasswordAtLogon = $true

$ExportPasswords   = $true
$PasswordsOutCsv   = ".\out_passwords.csv"

$WhatIf = $false    # true = simulation

# =========================
# ====== FUNCTIONS ========
# =========================

function Ensure-ADModule {
    if (-not (Get-Module -ListAvailable -Name ActiveDirectory)) {
        Write-Host "Module ActiveDirectory non trouvé. Tentative
d'installation (RSAT-AD-PowerShell)..."
        try {
            Import-Module ServerManager -ErrorAction Stop
            Add-WindowsFeature RSAT-AD-PowerShell | Out-Null
        } catch {
            throw "Impossible d'installer RSAT-AD-PowerShell automatiquement.
Installe-le puis relance."
        }
    }
    Import-Module ActiveDirectory -ErrorAction Stop
}

function Get-Trim([object]$v) { return ("" + $v).Trim() }

function Remove-Diacritics([string]$Text) {
    $normalized = $Text.Normalize([Text.NormalizationForm]::FormD)
    $sb = New-Object System.Text.StringBuilder
```

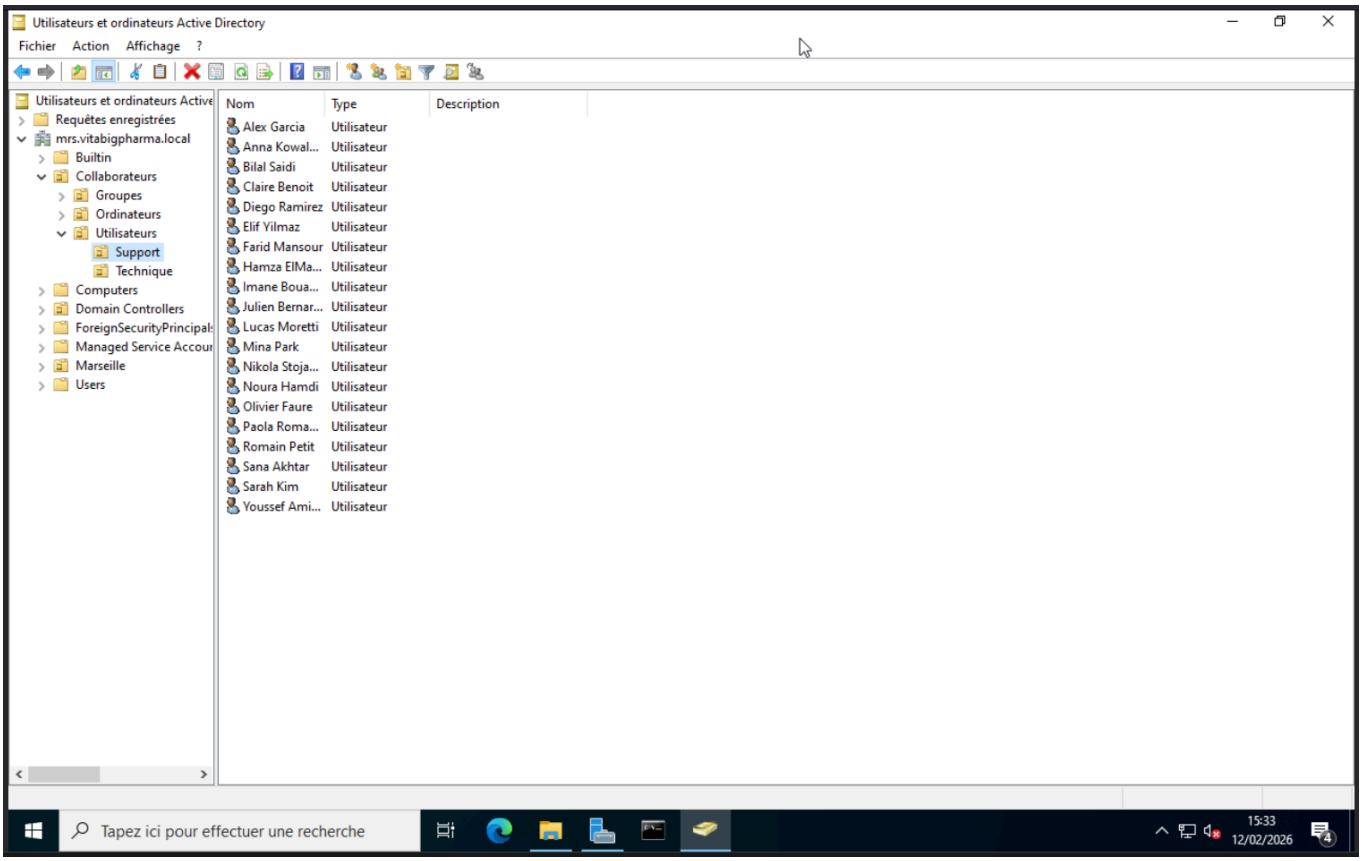
```
    foreach ($ch in $normalized.ToCharArray()) {
        $uc = [Globalization.CharUnicodeInfo]::GetUnicodeCategory($ch)
        if ($uc -ne [Globalization.UnicodeCategory]::NonSpacingMark) {
[void]$sb.Append($ch) }
    }
    return $sb.ToString().Normalize([Text.NormalizationForm]::FormC)
}

function New-RandomPassword([int]$Length = 16) {
    $upper="ABCDEFGHJKLMNPQRSTUVWXYZ"
    $lower="abcdefghijkmnpqrstuvwxyz"
    $digits="23456789"
    $special="!@#$%&*?-_+"
    $all = ($upper+$lower+$digits+$special).ToCharArray()
    $rand = New-Object System.Random
    $chars = @(
        $upper[$rand.Next($upper.Length)]
        $lower[$rand.Next($lower.Length)]
        $digits[$rand.Next($digits.Length)]
        $special[$rand.Next($special.Length)]
    )
    for ($i=$chars.Count; $i -lt $Length; $i++) { $chars +=
$all[$rand.Next($all.Length)] }
    $chars = $chars | Sort-Object { Get-Random }
    -join $chars
}

function Get-UniqueSam([string]$EmailPrefix, [string]$Server) {
    $samBase = Remove-Diacritics ($EmailPrefix.ToLower())
    $samBase = ($samBase -replace "[^a-z0-9._-]", "") -replace "\.",""
    if ($samBase.Length -gt 20) { $samBase = $samBase.Substring(0,20) }

    $sam = $samBase
    $i=1
    while (Get-ADUser -Server $Server -Filter "SamAccountName -eq '$sam'" -
ErrorAction SilentlyContinue) {
        $suffix="$i"
        $baseLen=[Math]::Min(20-$suffix.Length,$samBase.Length)
        $sam=$samBase.Substring(0,$baseLen)+$suffix
        $i++
    }
    $sam
}

function Ensure-OU([string]$OuDn, [string]$OuName, [string]$ParentDn,
[string]$Server) {
```

```
    $exists = $false
    try {
        Get-ADOrganizationalUnit -Server $Server -Identity $OuDn -ErrorAction
Stop | Out-Null
        $exists = $true
    } catch { $exists = $false }

    if (-not $exists) {
        if ($WhatIf) { Write-Host "WhatIf: Création OU $OuDn"; return }
        New-ADOrganizationalUnit -Server $Server -Name $OuName -Path $ParentDn
-ProtectedFromAccidentalDeletion $true | Out-Null
        Write-Host "OU créée: $OuDn"
    }
}

function Ensure-Group([string]$GroupName, [string]$GroupsOuDn,
[string]$Server) {
    $g = Get-ADGroup -Server $Server -Filter "SamAccountName -eq '$GroupName'
-or Name -eq '$GroupName'" -SearchBase $GroupsOuDn -ErrorAction
SilentlyContinue
    if (-not $g) {
        if ($WhatIf) { Write-Host "WhatIf: Création groupe $GroupName dans
$GroupsOuDn"; return $null }
        New-ADGroup -Server $Server -Name $GroupName -SamAccountName
$GroupName -GroupScope Global -GroupCategory Security -Path $GroupsOuDn | Out-
Null
        Write-Host "Groupe créé: $GroupName"
        $g = Get-ADGroup -Server $Server -Filter "SamAccountName -eq
'$GroupName' -or Name -eq '$GroupName'" -SearchBase $GroupsOuDn -ErrorAction
SilentlyContinue
    }
    $g
}

# =========================
# ========== MAIN =========
# =========================

Ensure-ADModule

if (-not (Test-Path $CsvPath)) { throw "CSV introuvable: $CsvPath" }

# DC forcé (pas de découverte)
$DC = "$($env:COMPUTERNAME).$DomainFqdn"
Write-Host "DC utilisé: $DC"
```

```
# OUs racines
$RootOUdn       = "OU=$RootOUName,$DomainDN"
$UsersOUdn      = "OU=$UsersOUName,$RootOUdn"
$ComputersOUdn  = "OU=$ComputersOUName,$RootOUdn"
$GroupsOUdn     = "OU=$GroupsOUName,$RootOUdn"

# Crée arborescence OU
Ensure-OU -OuDn $RootOUdn      -OuName $RootOUName      -ParentDn $DomainDN  -
Server $DC
Ensure-OU -OuDn $UsersOUdn     -OuName $UsersOUName     -ParentDn $RootOUdn  -
Server $DC
Ensure-OU -OuDn $ComputersOUdn -OuName $ComputersOUName -ParentDn $RootOUdn  -
Server $DC
Ensure-OU -OuDn $GroupsOUdn    -OuName $GroupsOUName    -ParentDn $RootOUdn  -
Server $DC

$rows = Import-Csv -Path $CsvPath

$export = New-Object System.Collections.Generic.List[object]
$created=0; $skipped=0; $errors=0

foreach ($r in $rows) {
    try {
        $prenom = Get-Trim $r.Prenom
        $nom    = Get-Trim $r.Nom
        $email  = Get-Trim $r.Email
        $svc    = Get-Trim $r.OU
        $group  = Get-Trim $r.Groupe

        if ([string]::IsNullOrWhiteSpace($prenom) -or
            [string]::IsNullOrWhiteSpace($nom) -or
            [string]::IsNullOrWhiteSpace($email) -or
            [string]::IsNullOrWhiteSpace($svc)) {
            Write-Warning "Ligne invalide. Email='$email'"
            $skipped++
            continue
        }

        # OU de service sous Utilisateurs
        $svcName = (Remove-Diacritics $svc).Trim()
        $svcOuDn = "OU=$svcName,$UsersOUdn"
        Ensure-OU -OuDn $svcOuDn -OuName $svcName -ParentDn $UsersOUdn -Server
$DC

        # Identité
        $sam = Get-UniqueSam -EmailPrefix ($email.Split("@")[0]) -Server $DC
```

```
        $upn = ("{0}@{1}" -f $sam, $DomainFqdn)

        # Déjà existant ?
        $existing = Get-ADUser -Server $DC -Filter "UserPrincipalName -eq
'$upn' -or Mail -eq '$email'" -ErrorAction SilentlyContinue
        if ($existing) {
            Write-Host "SKIP (existe): $email"
            $skipped++
            continue
        }

        # Password
        $plainPwd = if ($GenerateRandomPassword) { New-RandomPassword -Length
$PasswordLength } else { $DefaultPassword }
        $securePwd = ConvertTo-SecureString $plainPwd -AsPlainText -Force

        # Création utilisateur
        if ($WhatIf) {
            Write-Host "WhatIf: New-ADUser $email dans $svcOuDn (sam=$sam)"
        } else {
            New-ADUser -Server $DC `
                -Name (Remove-Diacritics "$prenom $nom") `
                -GivenName $prenom `
                -Surname $nom `
                -DisplayName "$prenom $nom" `
                -SamAccountName $sam `
                -UserPrincipalName $upn `
                -EmailAddress $email `
                -Path $svcOuDn `
                -AccountPassword $securePwd `
                -Enabled $true `
                -ChangePasswordAtLogon $ForceChangePasswordAtLogon | Out-Null

            Write-Host "CREATED: $email (UPN=$upn, OU=$svcOuDn)"
            $created++
        }

        # Groupe : création + ajout
        if (-not [string]::IsNullOrWhiteSpace($group)) {
            $gObj = Ensure-Group -GroupName $group -GroupsOuDn $GroupsOUdn -
Server $DC

            if ($WhatIf) {
                Write-Host "WhatIf: Add-ADGroupMember $sam -> $group"
            } elseif ($gObj) {
                Add-ADGroupMember -Server $DC -Identity
```

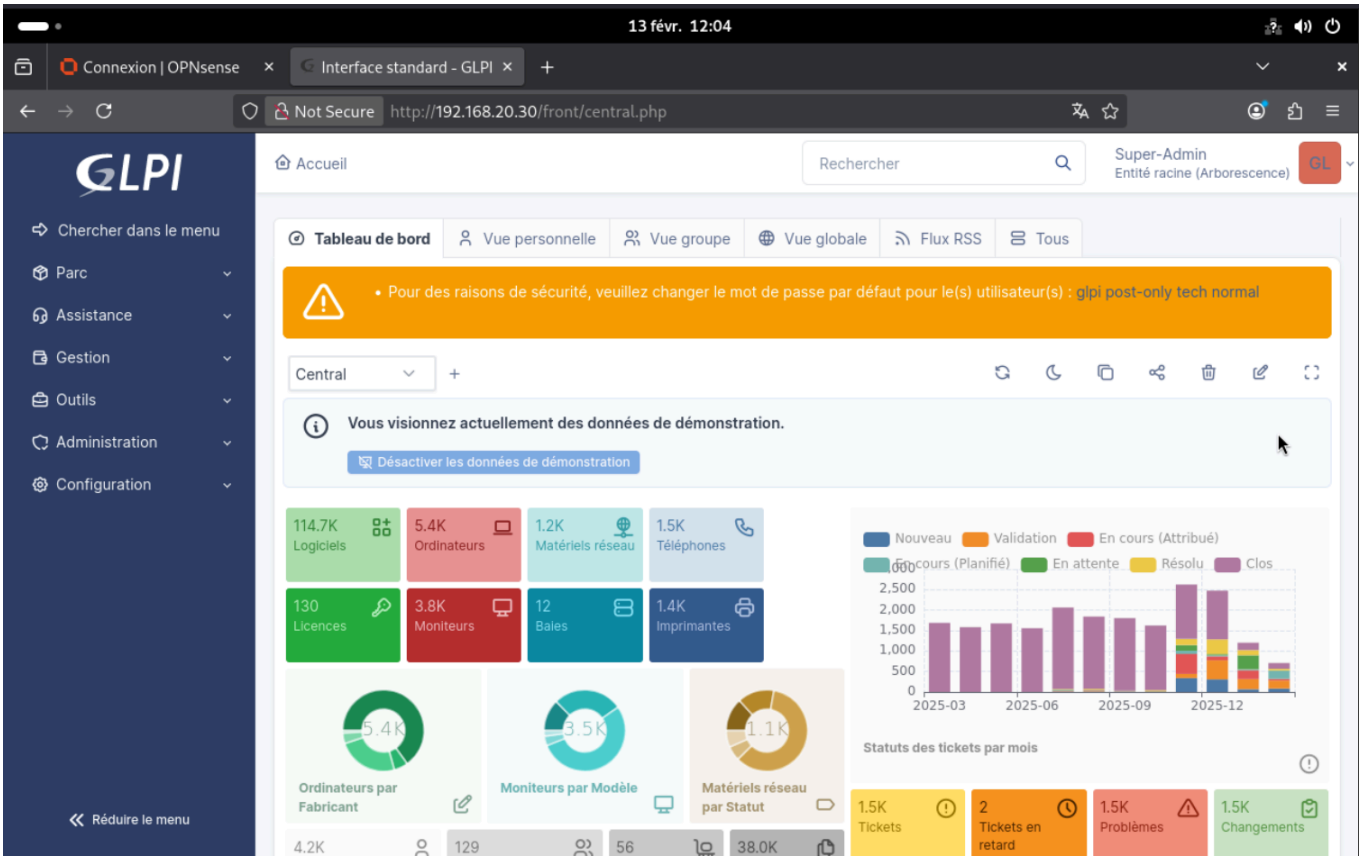
```
$gObj.DistinguishedName -Members $sam -ErrorAction Stop
                Write-Host "GROUP: $sam -> $group"
            }
        }

        if ($ExportPasswords) {
            $export.Add([pscustomobject]@{
                Prenom=$prenom; Nom=$nom; Email=$email; Service=$svc;
Groupe=$group
                SamAccountName=$sam; UPN=$upn; Password=$plainPwd
            })
        }

    } catch {
        $errors++
        Write-Error "Erreur Email='$($r.Email)': $($_.Exception.Message)"
    }
}

if ($ExportPasswords -and $export.Count -gt 0) {
    if ($WhatIf) {
        Write-Host "WhatIf: Export mots de passe vers $PasswordsOutCsv"
    } else {
        $export | Export-Csv -Path $PasswordsOutCsv -NoTypeInformation -
Encoding UTF8
        Write-Host "Export mots de passe: $PasswordsOutCsv"
    }
}

Write-Host ""
Write-Host "Terminé. Créés=$created / Skipped=$skipped / Erreurs=$errors"
```



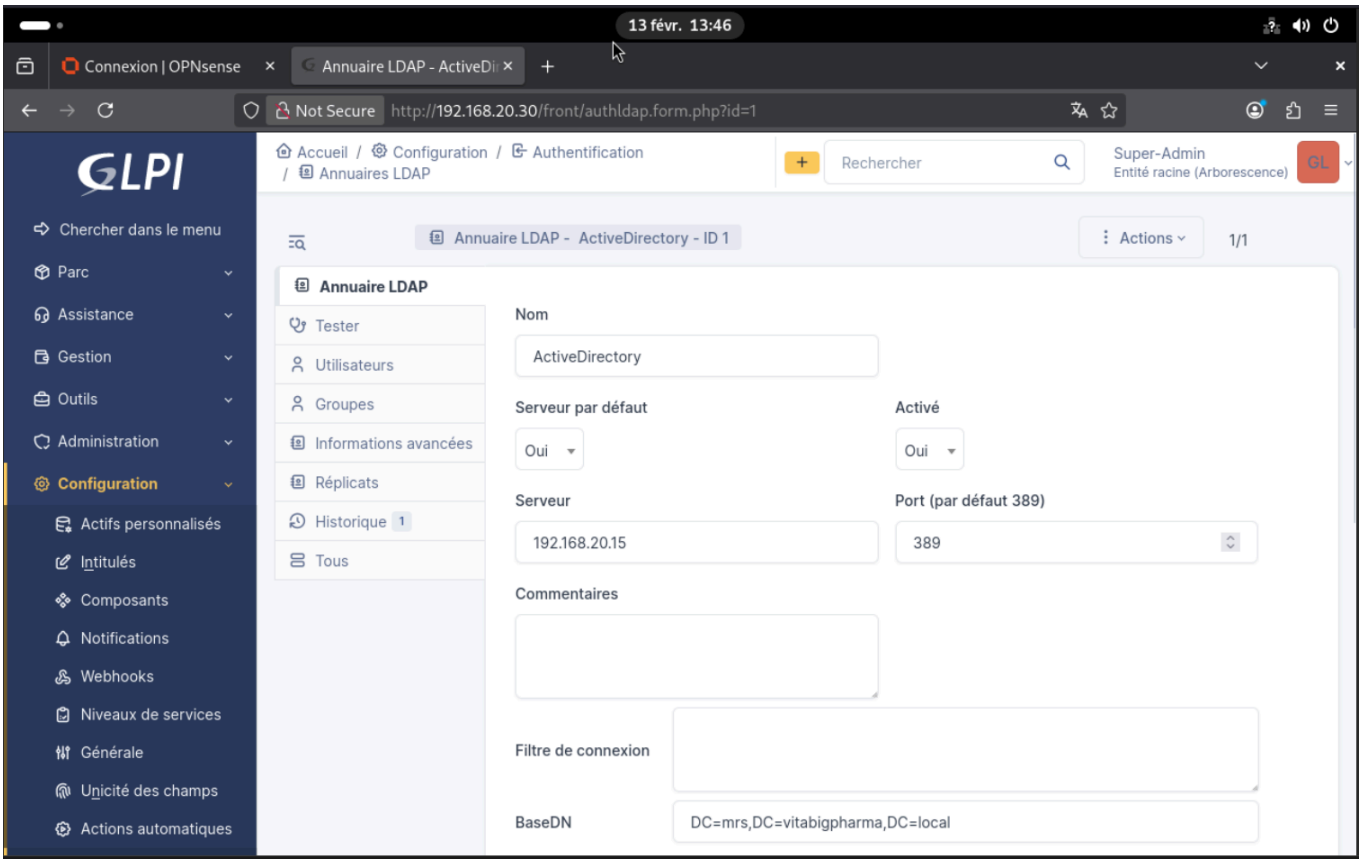
3.5 Déploiement GLPI

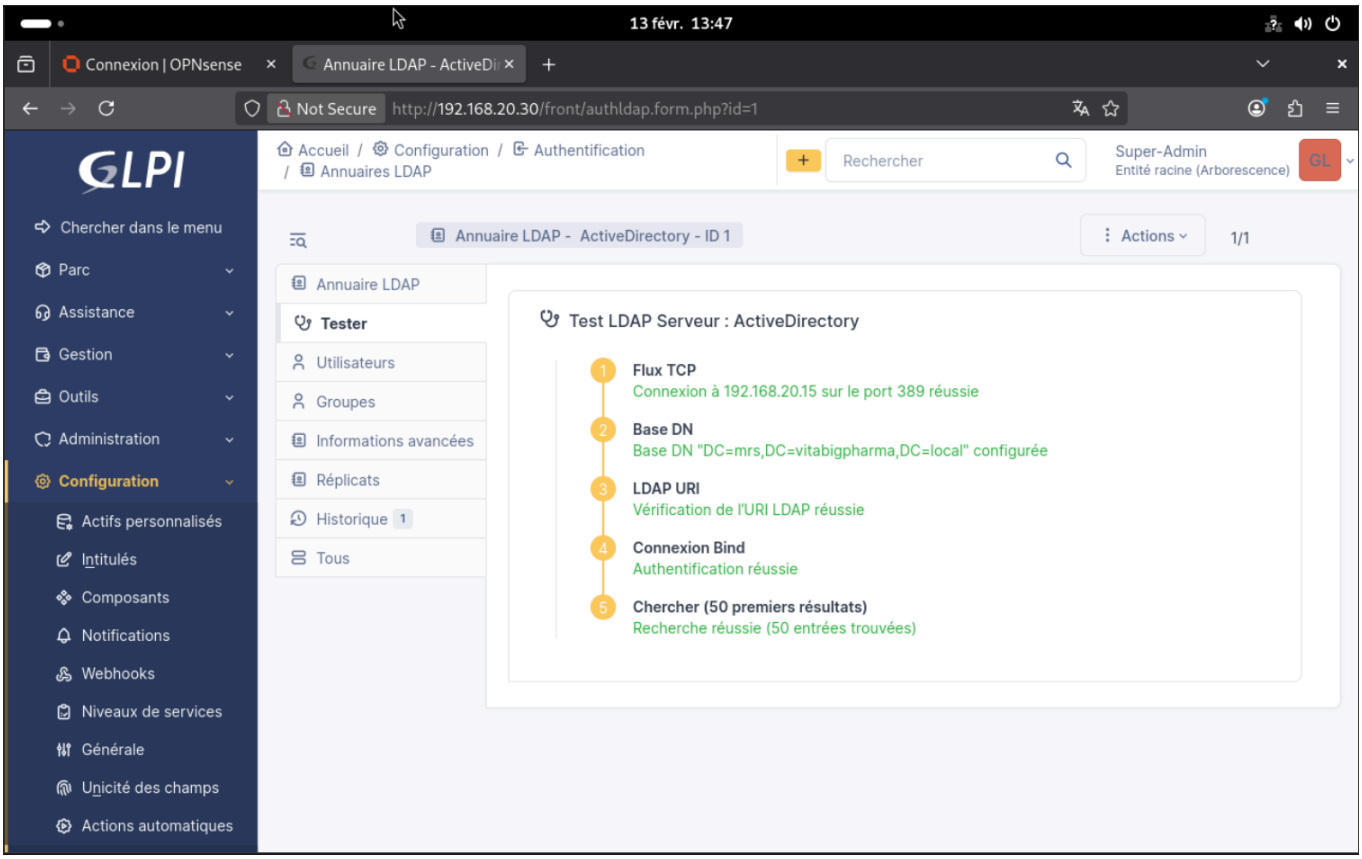
Pour le déploiement de GLPI j'ai suivi le tutoriel suivant : https://www.it-connect.fr/installation-pas-a-pas-de-glpi-10-sur-debian-12/

Et je me connecte depuis ma VM Admin :

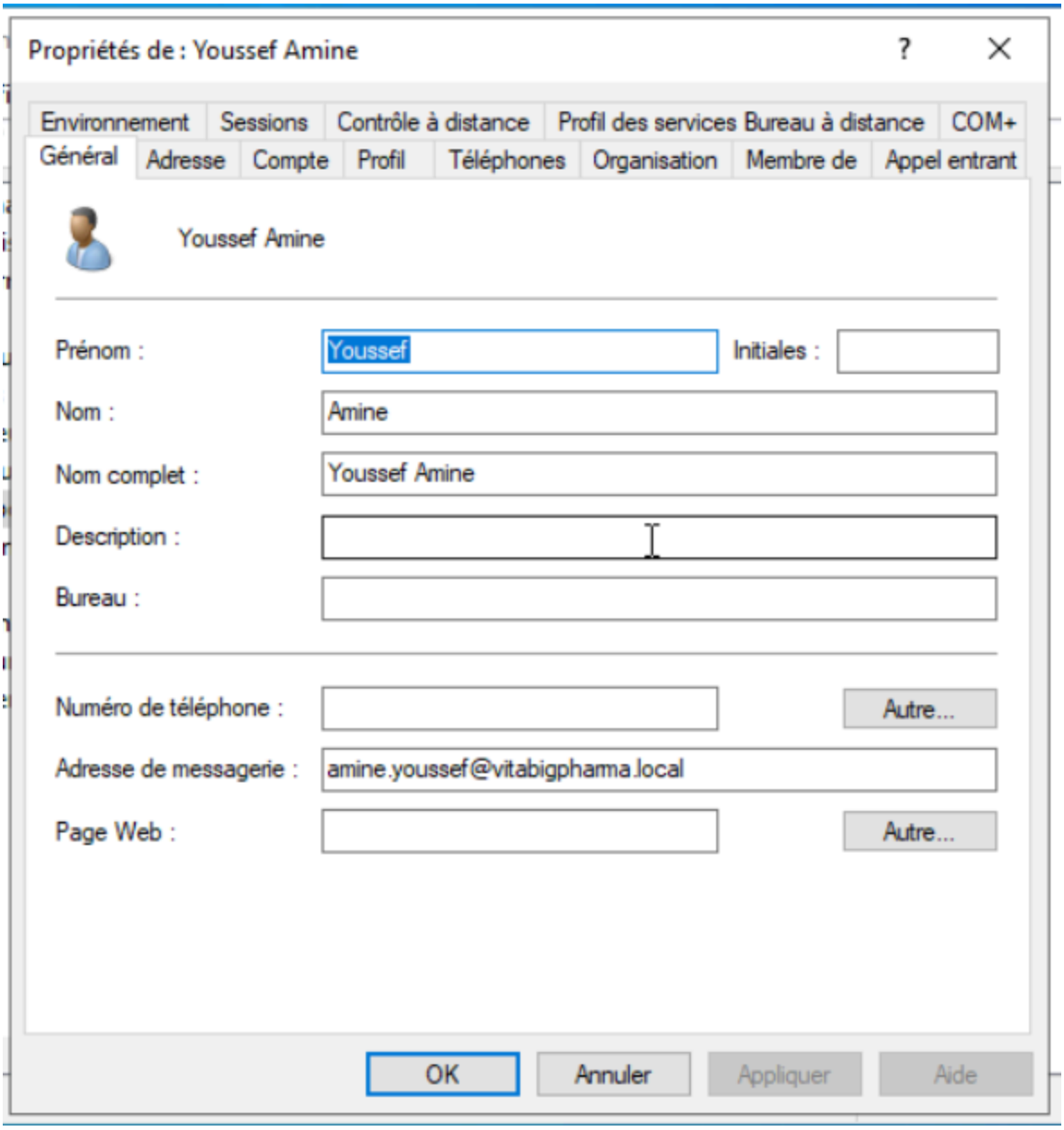


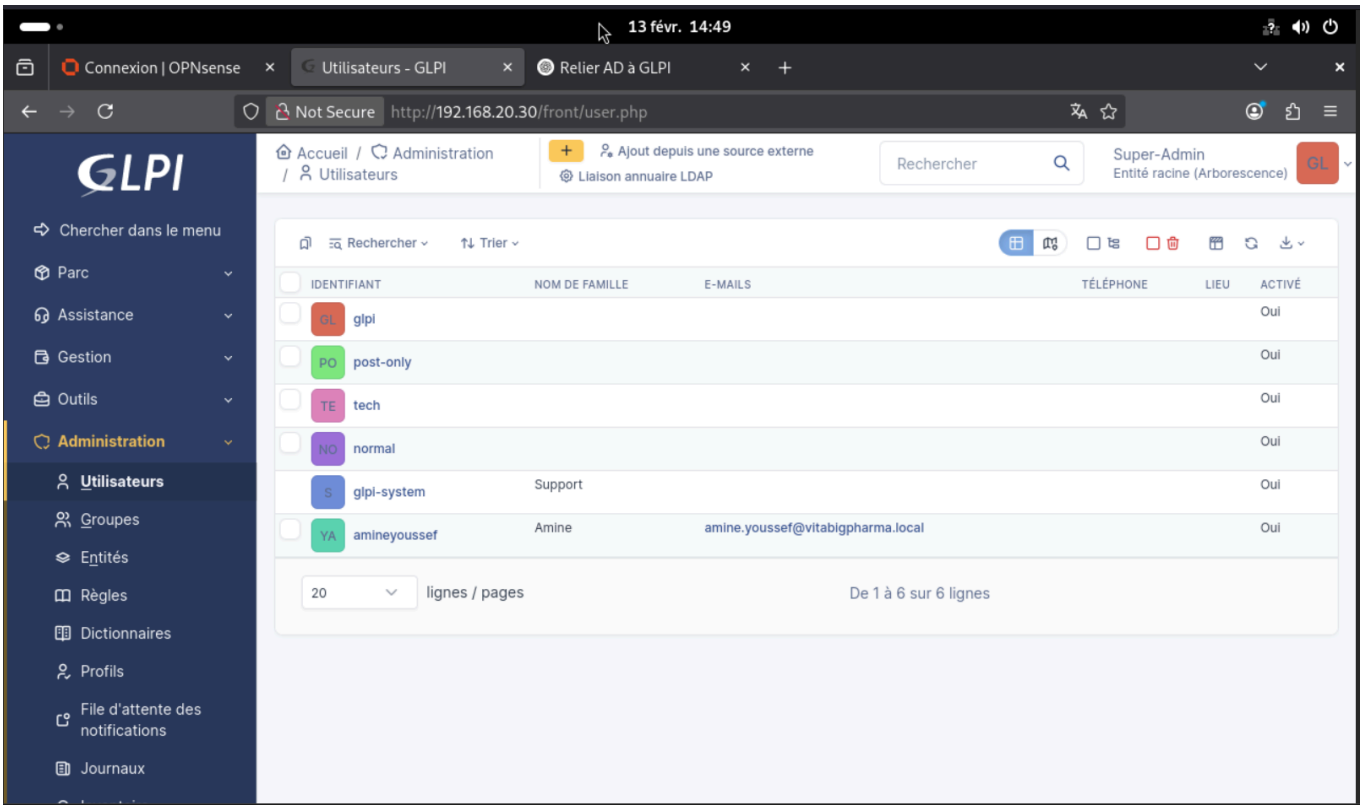
Ensuite je fais la liaison GLPI/AD




13 févr. 13:47
Connexion | OPNsense
Annuaire LDAP - ActiveDi
Not Secure
http://192.168.20.30/front/authldap.form.php?id=1
GLPI
Accueil / Configuration / Authentification / Annuaires LDAP
Rechercher
Super-Admin
Entité racine (Arborescence)
GL
Chercher dans le menu
Parc
Assistance
Gestion
Outils
Administration
Configuration
Actifs personnalisés
Intitulés
Composants
Notifications
Webhooks
Niveaux de services
Générale
Unicité des champs
Actions automatiques
Annuaire LDAP - ActiveDirectory - ID 1
Actions
1/1
Annuaire LDAP
Tester
Utilisateurs
Groupes
Informations avancées
Réplicats
Historique 1
Tous
Test LDAP Serveur : ActiveDirectory
1 Flux TCP
Connexion à 192.168.20.15 sur le port 389 réussie
2 Base DN
Base DN "DC=mrs,DC=vitabigpharma,DC=local" configurée
3 LDAP URI
Vérification de l'URI LDAP réussie
4 Connexion Bind
Authentification réussie
5 Chercher (50 premiers résultats)
Recherche réussie (50 entrées trouvées)

Puis je fais l'importation des utilisateurs, je me connecte un utilisateur de l'AD





Conclusion

Ce projet m'a permis de concevoir et de mettre en œuvre une infrastructure informatique complète, adaptée aux besoins d'une entreprise en phase de développement et répartie sur deux sites géographiquement distincts. J'ai retenu une architecture multi-sites répondant aux exigences de centralisation, de sécurité, de disponibilité et d'évolutivité, tout en assurant la continuité de service entre Toulouse et Marseille.

J'ai fait le choix de solutions techniques cohérentes avec les contraintes du projet, notamment OPNsense pour la gestion réseau, Active Directory pour la centralisation des identités, ainsi que des outils open source comme GLPI. Ces choix m'ont permis d'obtenir une infrastructure fonctionnelle, performante et économiquement viable. La mise en place de mécanismes de sécurité tels que les VPN, la segmentation réseau et les politiques de filtrage m'a également permis de renforcer la protection du système d'information.

J'ai également pu mettre en œuvre des automatisations, en particulier pour le déploiement des utilisateurs via script, ce qui améliore la gestion et limite les erreurs humaines. L'intégration de solutions de supervision et de sauvegarde contribue à garantir la fiabilité et la résilience de l'ensemble.

Enfin, ce projet m'a permis de comprendre l'importance d'une démarche structurée, allant de l'analyse des besoins jusqu'à la validation par des tests. L'infrastructure que j'ai mise en place

constitue une base solide, capable d’évoluer avec l’entreprise et de répondre à de futurs besoins tout en respectant les contraintes réglementaires et organisationnelles.