Projet BTS SIO SISR

Conception, déploiement et exploitation d’une infrastructure réseau sécurisée

Société	VitaBigPharma
Réalisation professionnelle	Mise en place d’une infrastructure réseau multi-sites sécurisée avec Active Directory et VPN
Nom, prénom	BELAROUSSI Sofiane
Option	SISR
Période	Décembre 2025
Lieu	Iris Montpellier

Sommaire

1. Présentation de l’entreprise

1.1 Contexte

VitaBigPharma est une entreprise pharmaceutique fictive qui souhaite s’installer en France sur deux sites : Toulouse et Marseille. Le site de Toulouse correspond au siège administratif et regroupe la direction, les ressources humaines et la finance. Le site de Marseille correspond au site technique, avec le support informatique et le service technique.

L’entreprise ne dispose pas encore d’une infrastructure informatique existante sur ces deux sites. Le projet consiste donc à concevoir, déployer et documenter une infrastructure complète à partir de zéro. L’objectif est de disposer d’un système d’information sécurisé, centralisé, évolutif et capable de garantir la continuité de service.

1.2 Organisation des sites

Site	Services / départements	Rôle du site
Toulouse	Direction, ressources humaines, finance	Gestion administrative et services centraux
Marseille	Service technique, support informatique	Support, maintenance et assistance utilisateurs

1.3 Objectifs du projet

- Mettre en place une authentification centralisée avec Active Directory et DNS.
- Sécuriser les échanges entre Marseille et Toulouse grâce à un VPN site-à-site IPsec.
- Permettre l’accès distant des utilisateurs nomades avec OpenVPN.
- Séparer les réseaux serveurs et collaborateurs afin de limiter les accès inutiles.
- Mettre en place un partage de fichiers sécurisé avec des droits par groupes.
- Déployer GLPI pour la gestion des incidents et du support informatique sur le site de Marseille.

- Prevoir les sauvegardes, les tests et la documentation d'exploitation.

2. Analyse du besoin

2.1 Besoins fonctionnels

Besoin	Description
Authentification	Centraliser les comptes utilisateurs et l’ouverture de session sur le domaine.
Partage de fichiers	Mettre à disposition des dossiers partagés avec des accès par service.
Télétravail	Permettre un accès distant sécurisé via VPN nomade OpenVPN.
Communication inter-sites	Relier Marseille et Toulouse par un tunnel VPN site-à-site IPsec.
Sauvegarde	Protéger les données et permettre la restauration en cas d’incident.
Support	Centraliser les tickets et demandes utilisateurs avec GLPI.

2.2 Contraintes

Type de contrainte	Contraintes retenues
Techniques	Infrastructure virtualisée, réseaux segmentés, deux sites distants, haute disponibilité Active Directory, VPN IPsec et OpenVPN, pare-feu pfSense.
Sécurité	Gestion des droits, filtrage des flux, séparation des réseaux, journalisation, sauvegardes régulières et VPN chiffré.
Réglementaires	Respect du RGPD, protection des données personnelles, politique d’accès stricte et sauvegardes fiables.
Organisationnelles	Projet réalisé dans un contexte BTS SIO SISR, avec documentation, tests techniques et présentation au jury.

2.3 Étude de l’existant

Aucune infrastructure informatique n’est déjà en place sur les sites de Toulouse et Marseille. Il n’existe pas encore de domaine Active Directory, de serveurs métiers, de pare-feu configurés ni de services réseau. Toute l’infrastructure doit donc être conçue, maquetée et déployée.

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.

Figure 1 - Besoins, contraintes réglementaires et étude de l'existant du projet.

3. Étude des solutions

3.1 Tableau comparatif des solutions techniques

Besoin	Solution retenue	Alternatives étudiées	Justification
Pare-feu / VPN / QoS	pfSense	OPNsense, firewall matériel, UFW	Solution complète, répandue, compatible avec Proxmox, adaptée au VPN et au filtrage.
Authentification centralisée	Active Directory / DNS	LDAP seul	Gestion centralisée des utilisateurs, des groupes, des GPO et intégration Windows native.
VPN site-à-site	IPsec	OpenVPN site-à-site	Standard sécurisé, performant et adapté aux communications inter-sites.
VPN nomade	OpenVPN	WireGuard	Solution fiable et documentée pour l'accès distant des utilisateurs.
Ticketing / support	GLPI	OCS Inventory, Redmine	Outil adapté au support informatique, compatible LDAP/AD.
ERP côté Toulouse	Dolibarr	Odoo	Solution légère et open-source adaptée aux besoins d'une PME.
Sauvegardes	rsync / scripts ou scripts Windows	Bacula	Solution simple, automatisable et suffisante pour le projet.
Audit AD	PingCastle	BloodHound	Outil spécialisé pour l'analyse de la sécurité Active Directory.
Audit Linux	Lynis	OpenSCAP	Audit complet et simple à mettre en œuvre.

Remarque : le modèle fourni mentionne OPNsense comme solution possible, mais la réalisation et les captures de déploiement utilisent pfSense. La documentation finale retient donc pfSense comme pare-feu principal du projet.

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

Figure 2 - Solutions techniques étudiées et retenues.

4. Architecture technique retenue

4.1 Schéma général

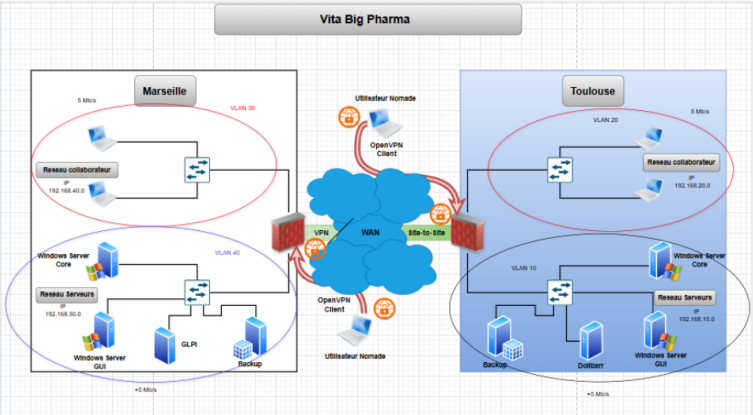
L'architecture retenue est une architecture multi-sites. Chaque site est protégé par un pare-feu pfSense. Les réseaux internes sont séparés en deux zones : un réseau serveurs et un réseau collaborateurs. Les deux sites sont interconnectés par un VPN site-à-site IPsec. Les utilisateurs nomades peuvent se connecter via OpenVPN.

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

Figure 3 - Schéma général et plan d'adressage de l'infrastructure multi-sites.

4.2 Architecture logique

Site	Réseau	Adresse réseau	Passerelle	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 / 192.168.30.1 selon maquette	30
Marseille	LAN collaborateurs	192.168.40.0/24	192.168.40.254 / 192.168.40.1 selon maquette	40

4.3 Périmètre personnel

Dans le cadre de la réalisation professionnelle, le périmètre principal concerne le site de Marseille. Les éléments traités sont la configuration du pare-feu pfSense, la segmentation réseau, les contrôleurs de domaine Active Directory/DNS, le serveur de fichiers, les GPO, GLPI, le VPN IPsec avec Toulouse et l'accès distant OpenVPN.

5. Déploiement de l’infrastructure

5.1 Installation et configuration du pare-feu pfSense

Le déploiement commence par la mise en place de pfSense sur l’infrastructure virtualisée. pfSense joue le rôle de passerelle, de pare-feu, de routeur, de serveur VPN et de point de contrôle des flux réseau.

Élément	Valeur
OS	pfSense CE
Hyperviseur	Proxmox
Interfaces	WAN / LAN / OPT1
Rôle	Routage, filtrage, NAT, VPN IPsec, OpenVPN, QoS
LAN	Réseau collaborateurs
OPT1	Réseau serveurs

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

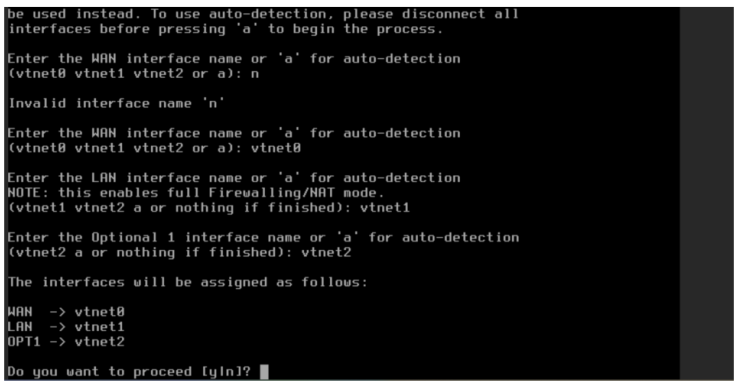


Figure 4 - Déploiement initial de pfSense et assignation des interfaces virtuelles.

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

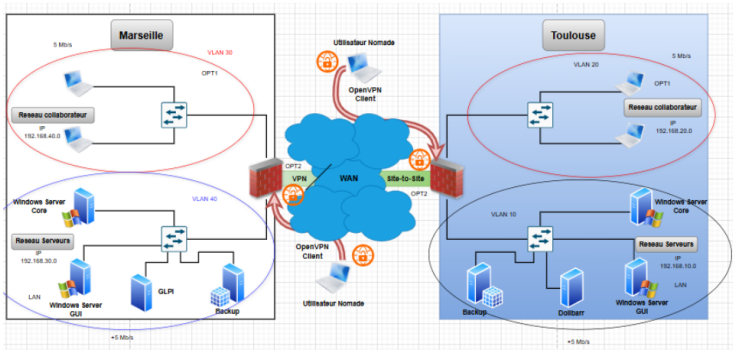


Figure 5 - Récapitulatif des interfaces WAN, LAN et OPT1.

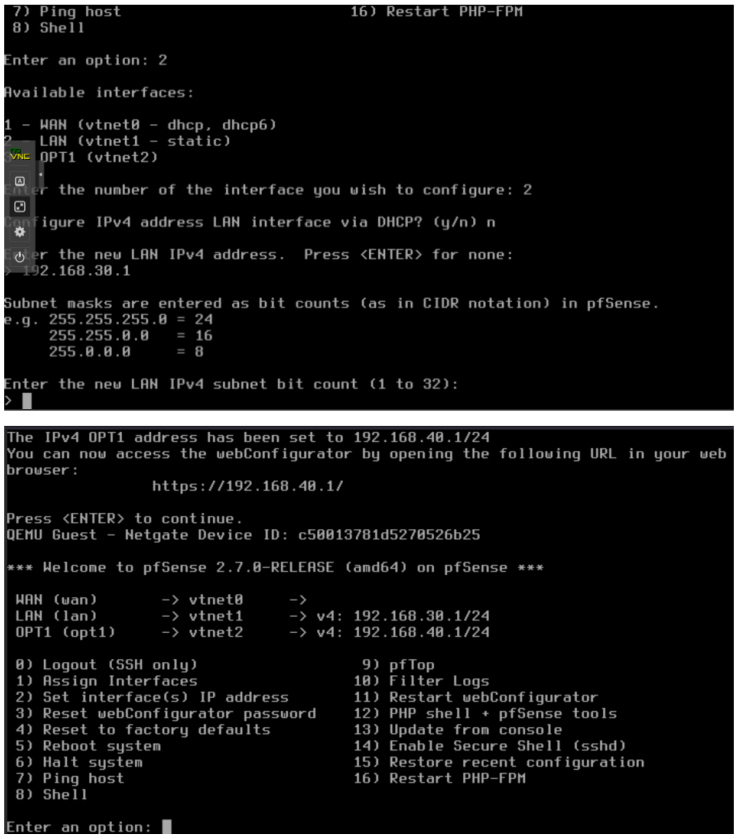


Figure 6 - Configuration des interfaces LAN et OPT1 côté Marseille.

Figure 7 - Configuration WAN et accès à l'interface web pfSense.

5.2 Mise en place du VPN site-à-site IPsec

Le VPN site-à-site IPsec permet de relier les réseaux internes de Marseille et de Toulouse à travers un tunnel chiffré. Les deux pare-feux pfSense utilisent une configuration cohérente : une phase 1 pour l'authentification des pare-feux et une ou plusieurs phases 2 pour définir les réseaux qui communiquent.

Élément	Configuration attendue
Objectif	Connecter Marseille et Toulouse de manière sécurisée.
Technologie	VPN IPsec site-à-site.
Authentification	Clé prépartagée identique sur les deux pare-feux.
Réseaux Marseille	192.168.30.0/24 et 192.168.40.0/24.
Réseaux Toulouse	192.168.10.0/24 et 192.168.20.0/24.
Validation	Ping inter-sites et statut du tunnel IPsec.

Dans la phase 2, les réseaux sont inversés entre les deux sites : côté Marseille, le réseau local est Marseille et le réseau distant est Toulouse ; côté Toulouse, le réseau local est Toulouse et le réseau distant est Marseille.

5.3 Installation Active Directory et DNS

5.2.1 Configuration réalisée du VPN site-à-site IPsec

La mise en place du tunnel IPsec a été réalisée depuis l'interface d'administration de pfSense du site de Marseille. L'objectif était de permettre la communication sécurisée avec le réseau distant de Toulouse, sans exposer directement les services internes. La configuration s'appuie sur une phase 1 IKEv2 pour l'authentification des passerelles et sur une phase 2 pour définir les réseaux autorisés à traverser le tunnel.

Paramètre	Configuration retenue
Passerelle locale	pfSense Marseille - WAN 10.34.20.1
Passerelle distante	pfSense distant - WAN 10.34.30.1
Mode	IPsec site-à-site, IKEv2, authentification par clé prépartagée
Réseau local	192.168.30.0/24 pour le réseau serveurs de Marseille
Réseau distant	192.168.10.0/24 pour le réseau serveur/administration distant
Validation	Tunnel établi et ping inter-sites réussi vers 192.168.10.20

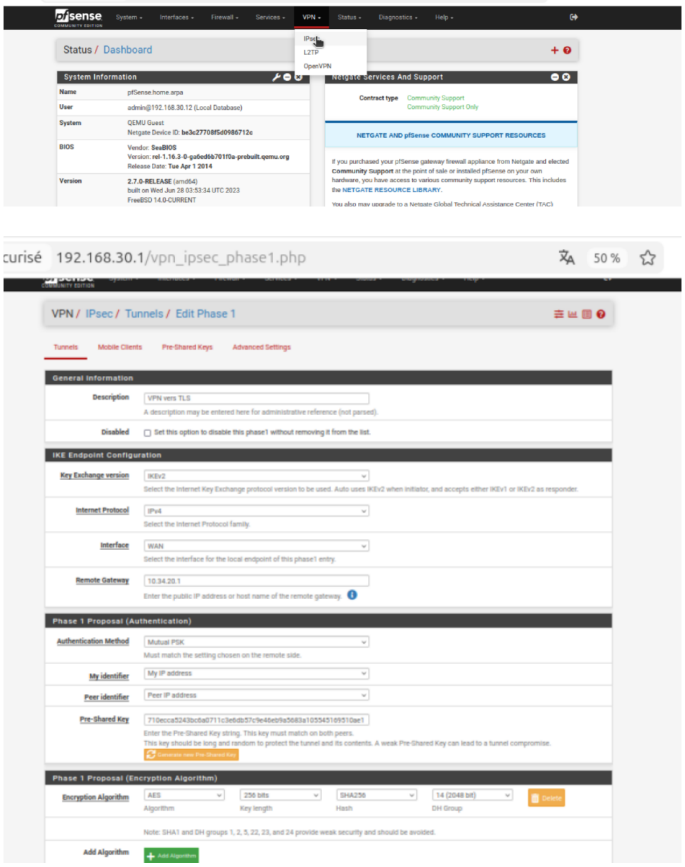
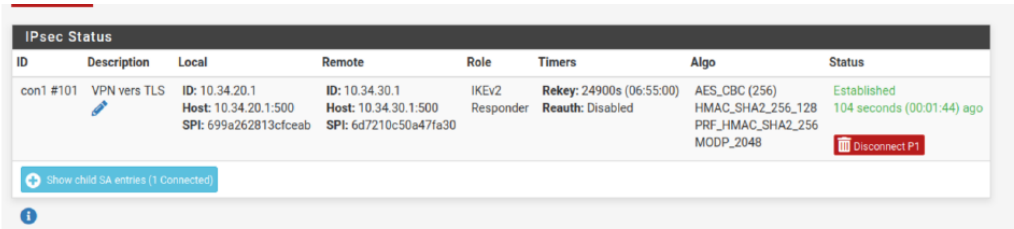


Figure - Configuration de la phase 1 IPsec sur pfSense : protocole IKEv2, interface WAN, passerelle distante et paramètres de chiffrement.

5.2.2 Validation du tunnel IPsec

Après l'enregistrement de la configuration, l'état du tunnel a été contrôlé depuis le menu Status > IPsec. La phase 1 et la phase 2 apparaissent comme établies. Un test de connectivité a ensuite été réalisé vers un poste du site distant afin de vérifier le routage entre les deux réseaux.



Je ping son pc admin via son ip 192.168.10.20

OpenVPN Nomade

Figure - Statut IPsec établi et test de ping réussi vers le poste distant 192.168.10.20.

Le ping vers le poste distant confirme que le trafic inter-sites traverse correctement le tunnel. Cette validation permet de s'assurer que les règles IPsec et le routage sont opérationnels pour les échanges nécessaires entre Marseille et Toulouse.

5.2.3 Accès distant OpenVPN nomade

En complément du VPN site-à-site, un accès nomade OpenVPN a été préparé sur pfSense pour permettre à un utilisateur extérieur de rejoindre les ressources internes de Marseille. Le serveur OpenVPN est publié sur l'interface WAN en UDP 1194 et attribue aux clients une adresse dans le réseau tunnel 192.168.60.0/24.

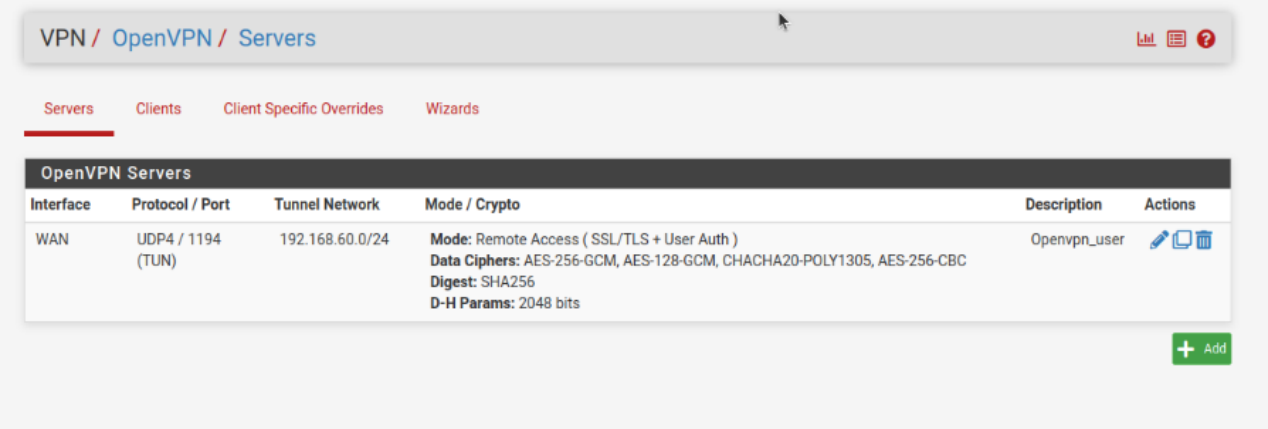


Figure - Serveur OpenVPN configuré sur le WAN en UDP 1194 avec le réseau tunnel 192.168.60.0/24.

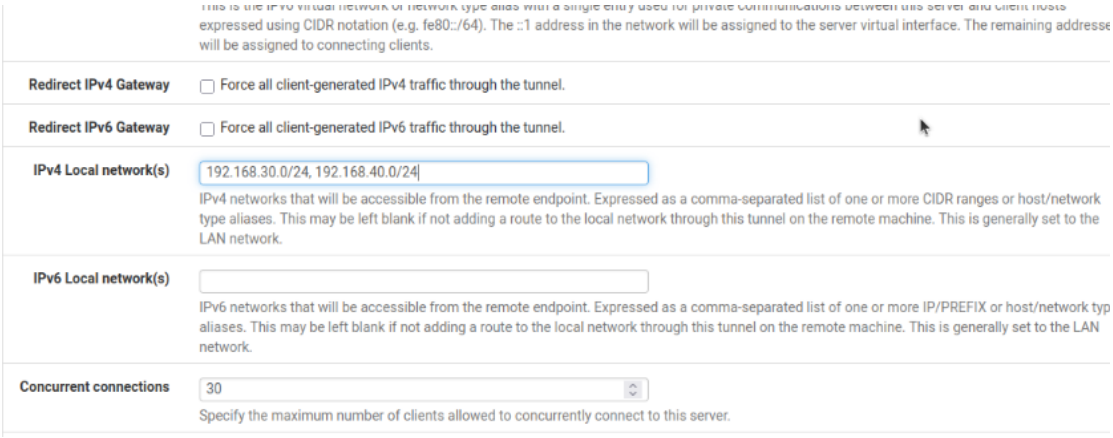
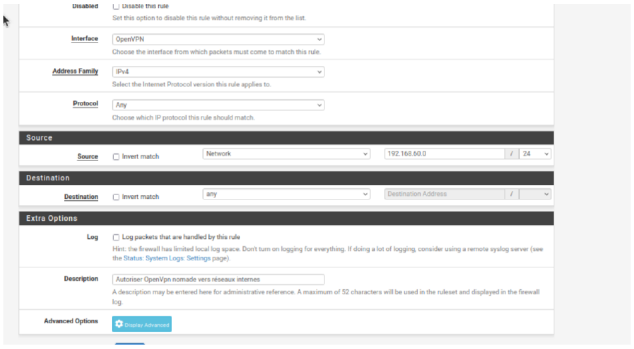


Figure - Réseaux internes publiés au client VPN : 192.168.30.0/24 et 192.168.40.0/24.

Les deux réseaux internes de Marseille sont donc annoncés au client VPN : le réseau serveurs et le réseau collaborateurs. Cette configuration permet d'utiliser le même point d'entrée sécurisé pour les besoins de télétravail et d'administration à distance.

5.2.4 Règles de filtrage et compte VPN

La règle OpenVPN autorise le réseau tunnel 192.168.60.0/24 à accéder aux réseaux internes. L'utilisateur VPN dispose également d'un certificat associé, ce qui complète l'authentification par identifiant et mot de passe.



Les clients VPN qui reçoivent une IP en 192.168.60.x ont le droit d'accéder aux réseaux internes.

Figure - Règle OpenVPN : les clients recevant une adresse en 192.168.60.x peuvent accéder aux réseaux internes autorisés.

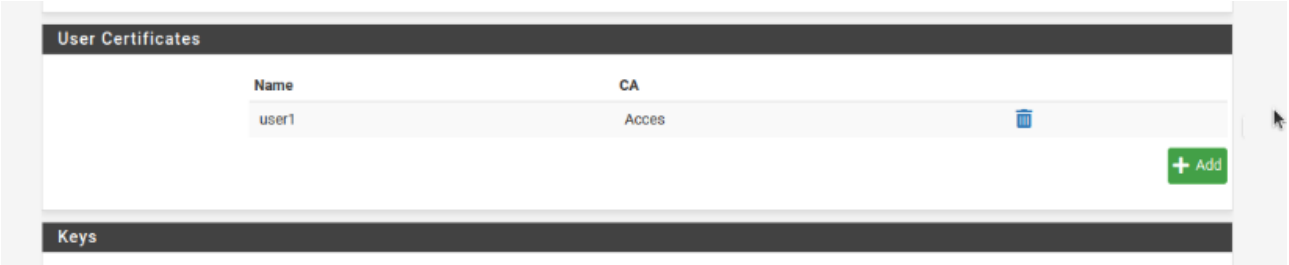


Figure - Certificat utilisateur associé au compte user1 pour l'authentification OpenVPN.

Cette partie est cohérente avec le principe de moindre exposition : aucun service interne n'est publié directement sur Internet, l'accès s'effectue uniquement après authentification sur le VPN.

L’infrastructure Active Directory a été installée sur Windows Server 2022. Le premier contrôleur de domaine permet de centraliser les utilisateurs, les groupes et les droits. Un second contrôleur de domaine est ajouté afin d’assurer la redondance Active Directory et DNS.

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

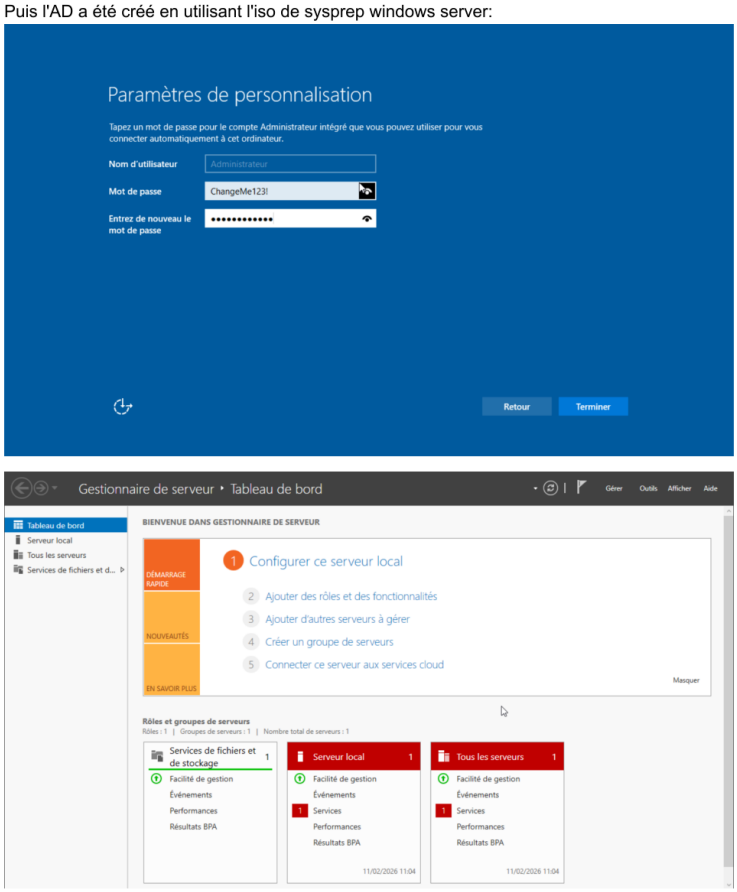


Figure 8 - Installation initiale de Windows Server et accès au gestionnaire de serveur.

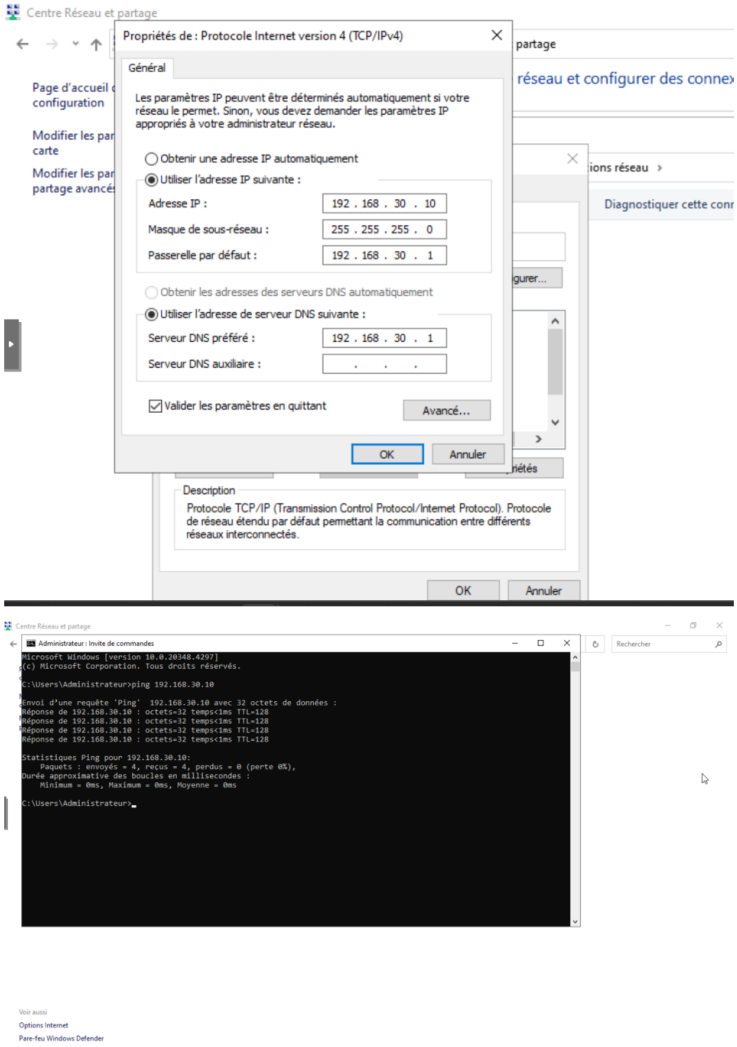


Figure 9 - Configuration IPv4 du serveur AD1.

Le premier controleur de domaine est configure avec une adresse IP fixe afin de garantir sa disponibilite pour les postes et les serveurs. La passerelle pointe vers pfSense et le DNS est configure vers le service interne du domaine. Cette configuration permet ensuite aux machines clientes de localiser correctement le domaine mrs.vitabigpharma.local.

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

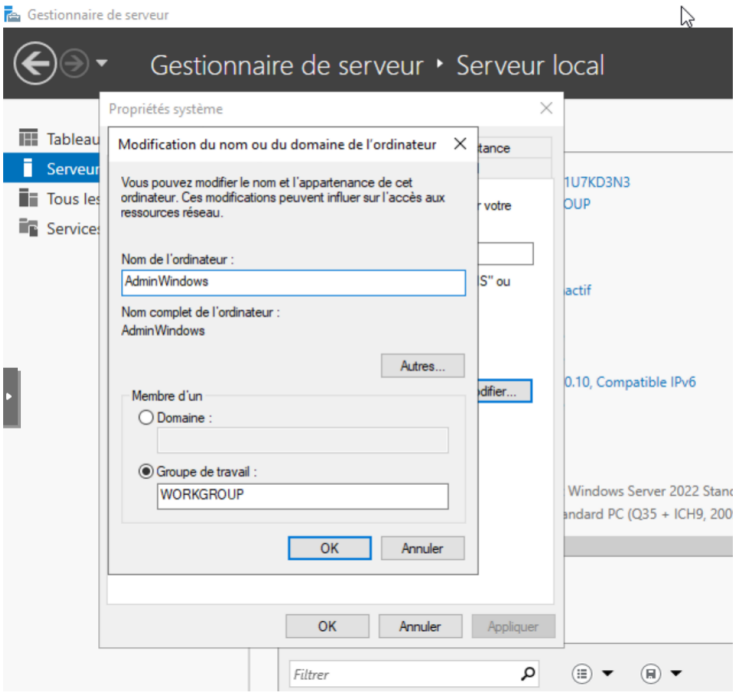
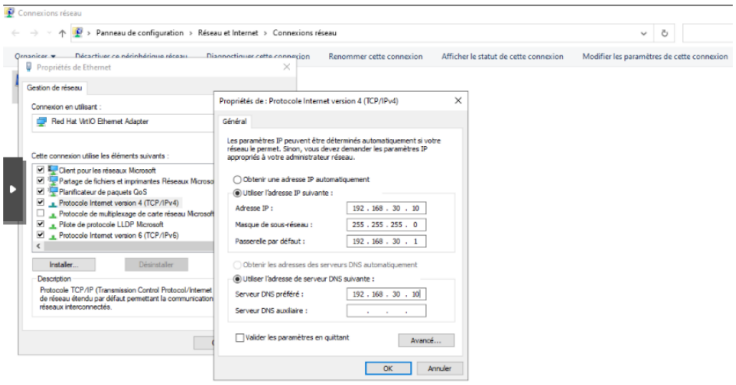
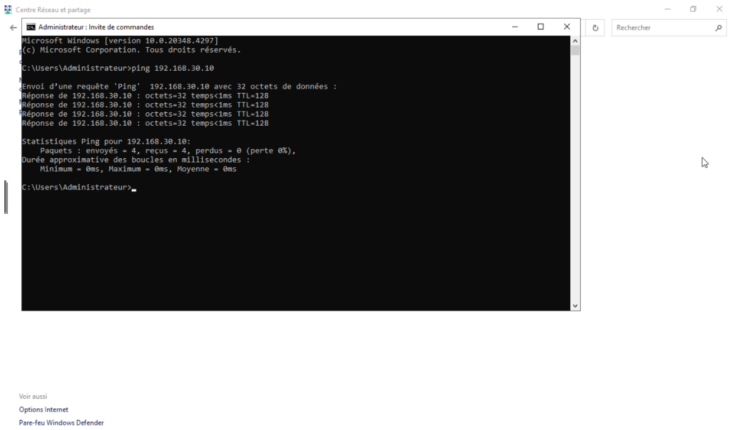


Figure 10 - Renommage du serveur avant promotion en contrôleur de domaine.

Le serveur est renomme avant sa promotion en controleur de domaine. Cette etape permet d'avoir un nom clair et coherent dans l'annuaire Active Directory. Le renommage est realise avant l'installation definitive du role AD DS afin d'eviter les changements complexes une fois le domaine cree.



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`

Figure 11 - Vérification réseau et configuration du DNS préféré.

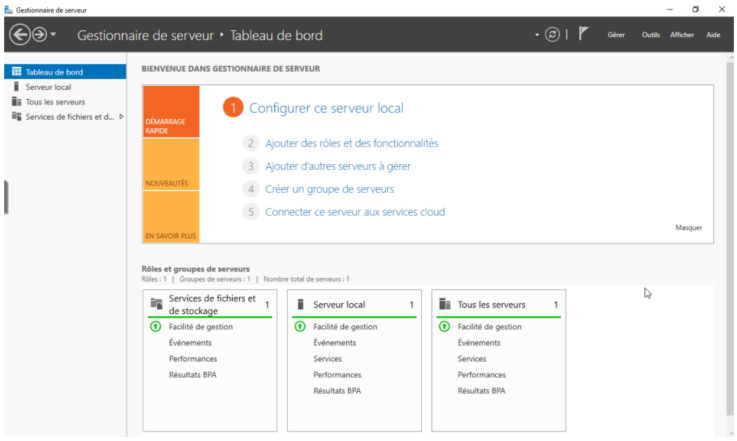
La connectivite reseau est verifiee avant la promotion du serveur. Les tests de ping confirment que le serveur communique avec sa passerelle et les autres elements du reseau. Le DNS prefere est ensuite ajuste pour preparer le fonctionnement du domaine Active Directory.

- **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

Figure 12 - Le DNS préféré du contrôleur de domaine pointe vers lui-même.

Le controleur de domaine utilise son propre service DNS pour resoudre les noms internes du domaine. Cette configuration est indispensable pour l'authentification, la recherche des controleurs de domaine et l'application des strategies de groupe. Le serveur peut ensuite etre utilise comme reference DNS par les postes clients.

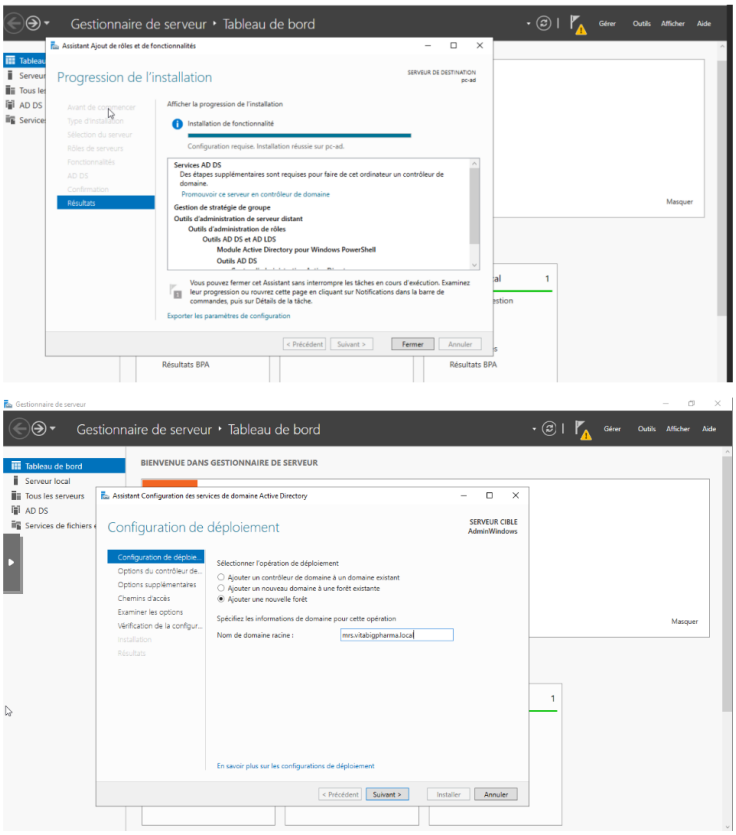


Figure 13 - Ajout du rôle Active Directory Domain Services.

Le role Services de domaine Active Directory est ajoute depuis le Gestionnaire de serveur. Cette installation prepare le serveur a heberger l'annuaire, les comptes utilisateurs, les groupes et les ordinateurs. Le role DNS est installe en complement afin d'assurer la resolution du domaine.

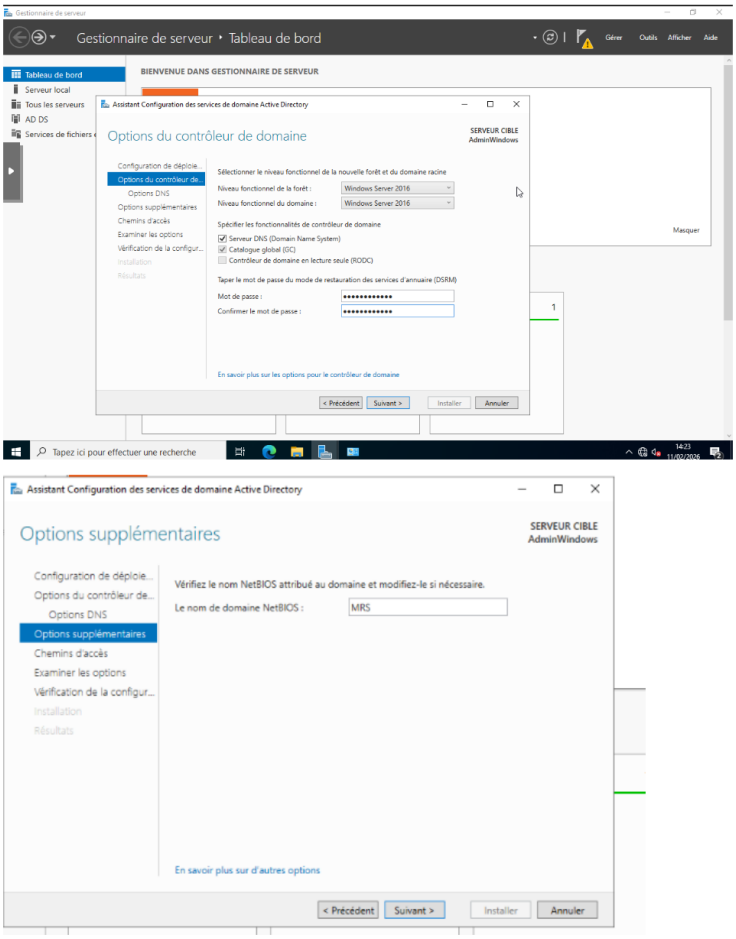
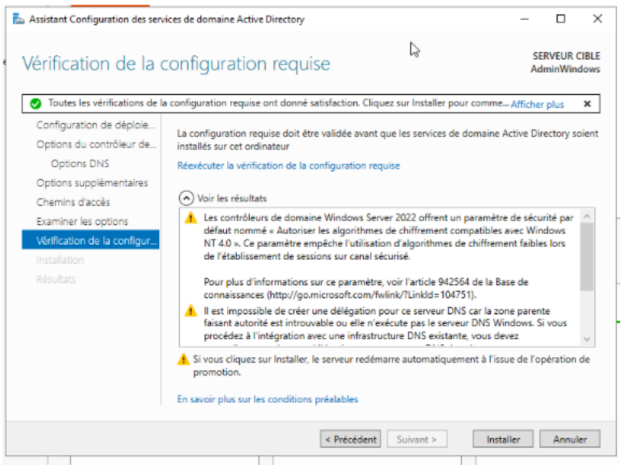


Figure 14 - Promotion du serveur en contrôleur de domaine.

Le serveur est promu en premier controleur de domaine de la foret mrs.vitabigpharma.local. Cette operation cree l'annuaire Active Directory et initialise la structure du domaine. A partir de cette etape, les utilisateurs et les ordinateurs peuvent etre centralises dans l'infrastructure.



(petit changement avec ajout de dns sur AD1):

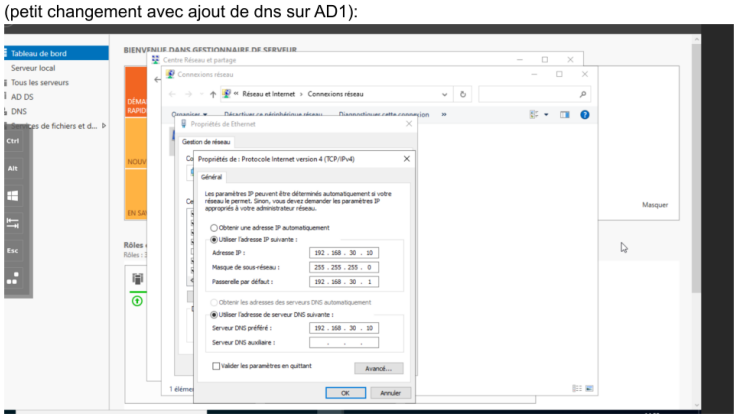


Figure 15 - Vérification de la configuration AD DS et ajustement DNS.

Les prerequis de la promotion AD DS sont verifies avant la finalisation. Les avertissements affiches sont controles et la configuration DNS est ajustee si necessaire. Apres redemarrage, le serveur fonctionne comme controleur de domaine principal.

puis cloner pour ad 2:

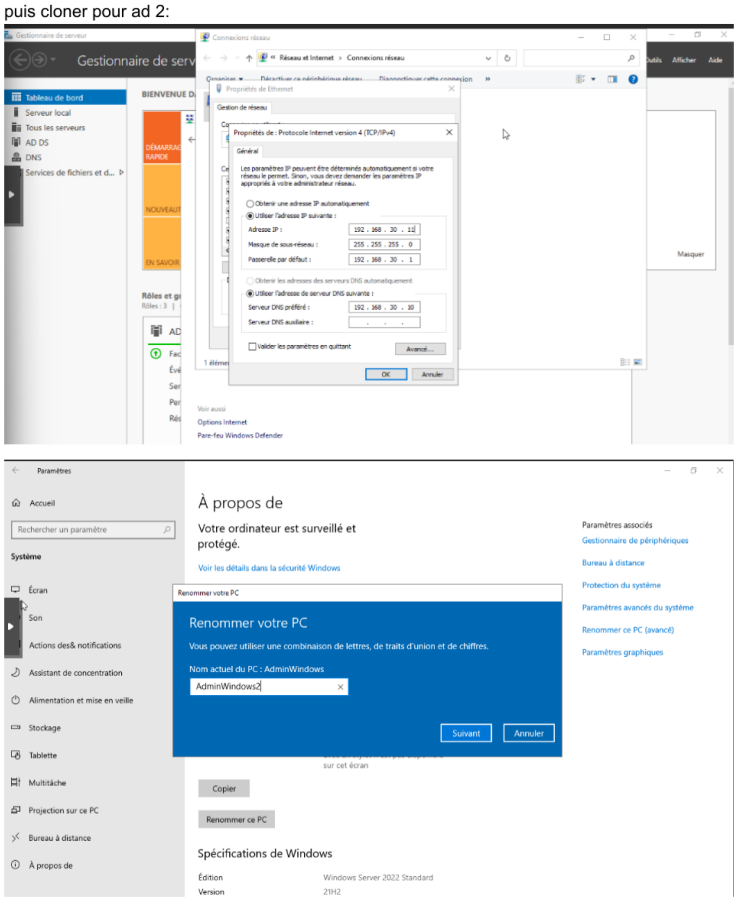


Figure 16 - Préparation du second contrôleur de domaine.

Le second serveur est prepare pour assurer la redondance du domaine. Il recoit une adresse IP fixe et utilise le premier controleur de domaine comme serveur DNS. Cette configuration permet de l'integrer correctement a l'annuaire existant.

AD 2 :

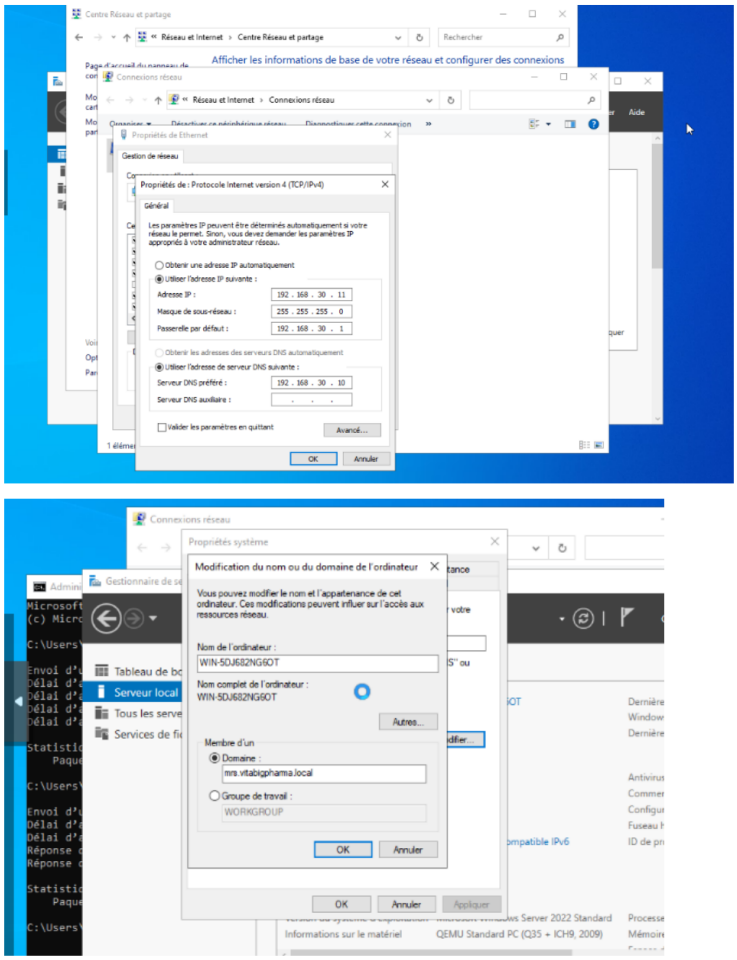
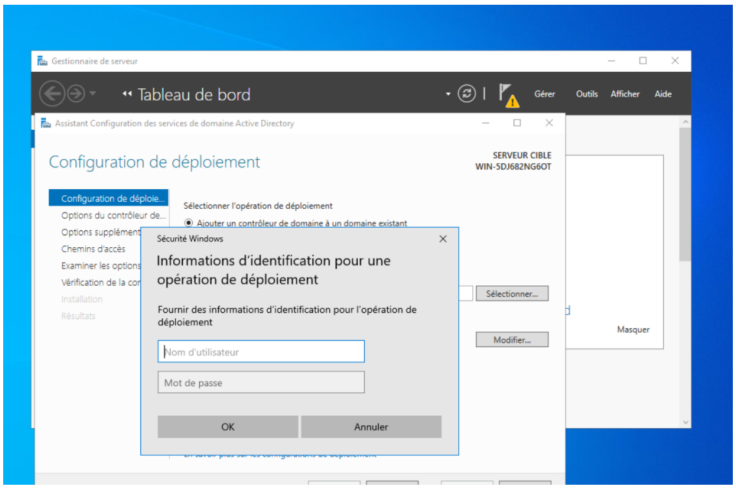


Figure 17 - Configuration réseau et intégration du second serveur au domaine.

Le second serveur est integre au domaine mrs.vitabigpharma.local avant sa promotion. Les parametres reseau sont verifies afin de s'assurer qu'il communique avec le controleur principal. Cette etape valide la resolution DNS et l'authentification avec un compte administrateur du domaine.



AD2:

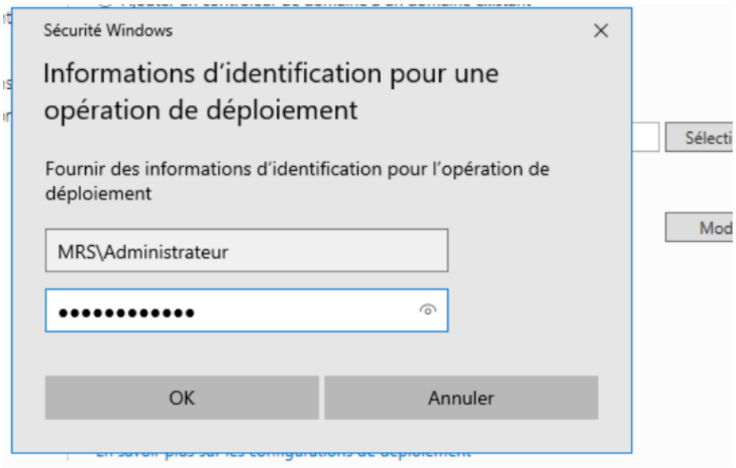
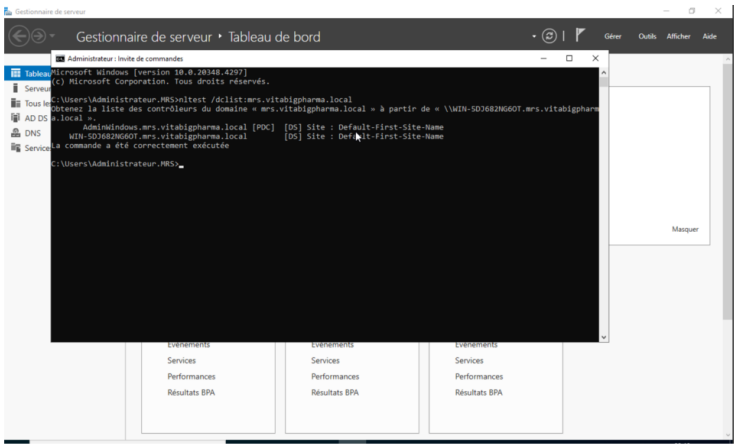


Figure 18 - Ajout d'AD2 comme contrôleur de domaine supplémentaire.

Le serveur AD2 est ajoute comme controleur de domaine supplementaire. Il replique les informations Active Directory et DNS depuis le controleur principal. Cette redondance permet de maintenir l'authentification et la resolution de noms en cas d'indisponibilite d'AD1.

Ca fonctionne:



Déploiement des utilisateurs

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

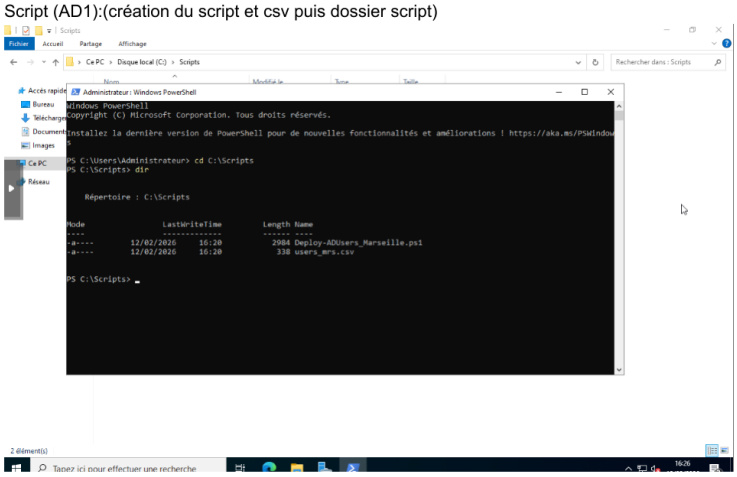
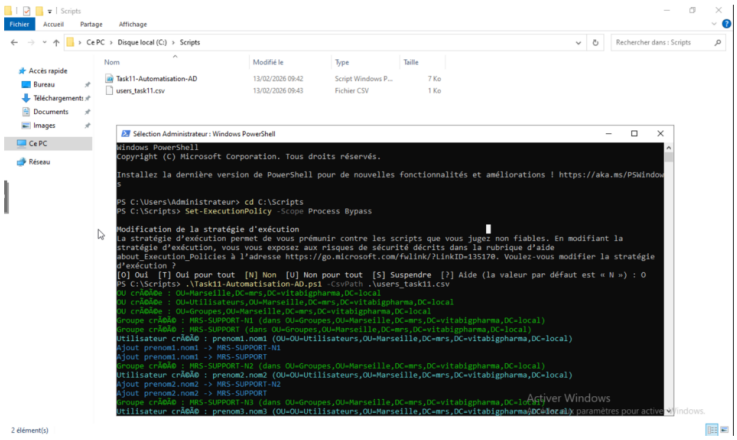


Figure 19 - Vérification du fonctionnement de l’infrastructure Active Directory.

5.4 Automatisation PowerShell

La création des utilisateurs, groupes et unités d’organisation est automatisée à l’aide d’un script PowerShell basé sur un fichier CSV. Cette méthode évite la création manuelle des comptes et limite les erreurs de saisie.

Fichier	Rôle
users_task11.csv	Liste des utilisateurs et informations de service.
Task11-Automatisation-AD.ps1	Script PowerShell de création des objets Active Directory.



déposer les 2 scripts:

users_task11.csv

Task11-Automatisation-AD.ps1

Figure 20 - Dépôt et exécution du script PowerShell et du fichier CSV.

5.4.1 Création d'un compte utilisateur et affectation au groupe

En complément de l'automatisation PowerShell, un compte utilisateur de test a été créé manuellement dans l'annuaire afin de valider le fonctionnement des OU et des groupes de sécurité. Le compte Test Support est placé dans l'OU Marseille > Utilisateurs et rattaché au groupe MRS-SUPPORT.

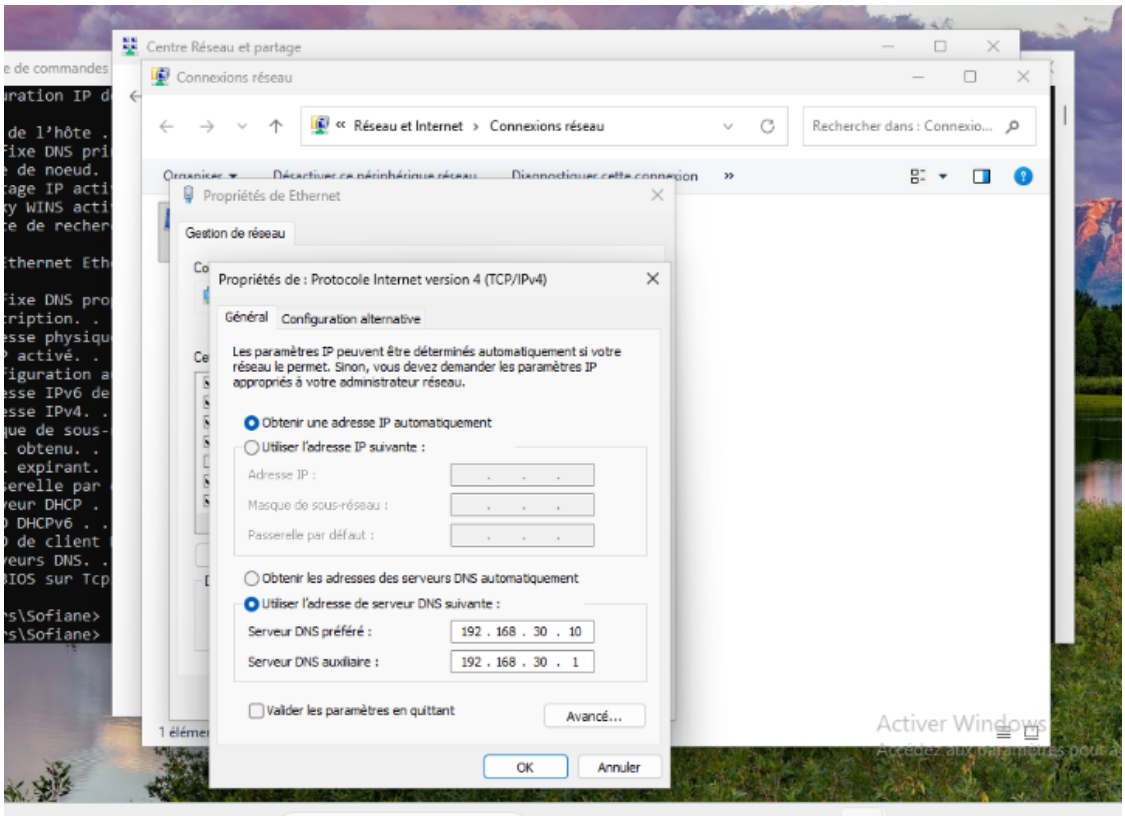


Figure - Le compte Test Support est membre du groupe MRS-SUPPORT et du groupe Utilisateurs du domaine.

L'appartenance au groupe MRS-SUPPORT permet ensuite d'appliquer les droits prévus sur les ressources du service support, notamment les partages réseau et les éventuelles règles applicatives liées à GLPI.

5.4.2 Intégration d'un poste client au domaine

Une VM Windows cliente a été utilisée pour valider l'authentification avec un compte du domaine. Le poste est placé sur le réseau collaborateurs 192.168.40.0/24. La passerelle par défaut est celle de pfSense sur ce segment, tandis que le DNS pointe vers le contrôleur de domaine afin de résoudre mrs.vitabigpharma.local.

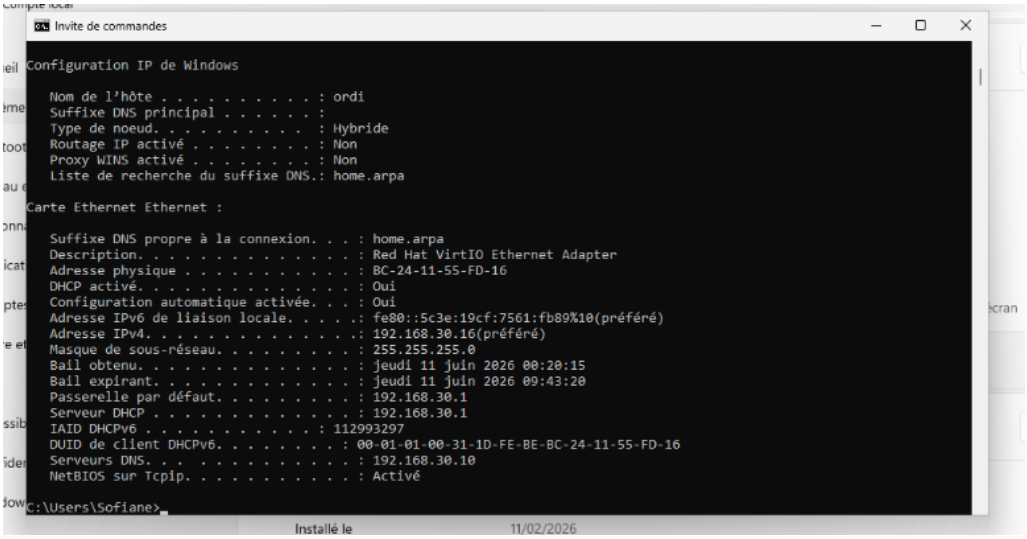


Figure - Configuration réseau du poste client : adresse en 192.168.40.0/24 et DNS pointant vers le contrôleur de domaine.

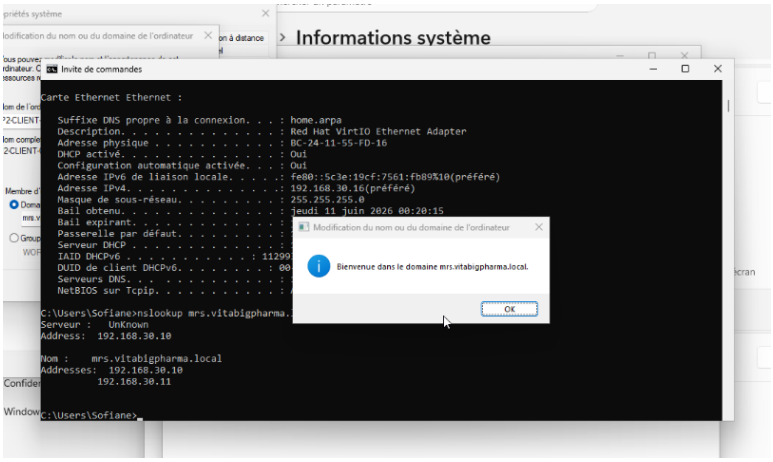
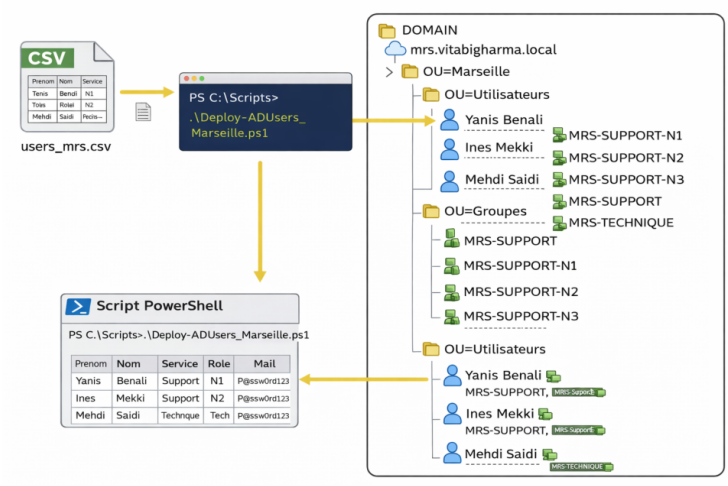


Figure - Résolution DNS du domaine et intégration réussie du poste au domaine mrs.vitabigpharma.local.

Le message de bienvenue dans le domaine confirme que le poste peut contacter le contrôleur de domaine et que les identifiants administrateur utilisés pour l'ajout sont valides. Après redémarrage, l'ouverture de session peut être testée avec le compte MRS\tsupport ou tsupport@mrs.vitabigpharma.local.

le script a été fait grâce à ce plan:



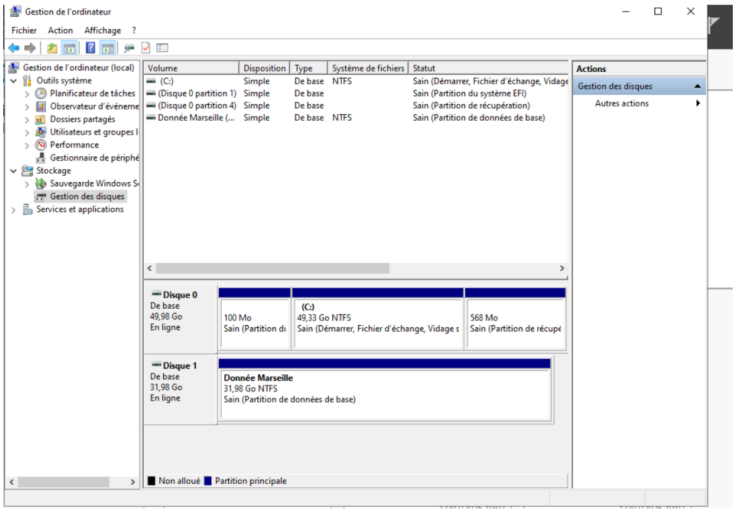
serveur de fichier:
Création de vm pour serveur de fichier.

Création d'un nouveau disque "Donnée Marseille"

Figure 21 - Logique du script : création des OU, utilisateurs et groupes AD.

5.5 Serveur de fichiers

Un serveur de fichiers est déployé sur le site de Marseille afin de centraliser les données des services. Un disque dédié “Donnée Marseille” est ajouté, puis des dossiers partagés sont créés : Commun, Support et Technique. Les permissions sont gérées à l’aide des groupes Active Directory afin que chaque service accède uniquement aux ressources nécessaires.



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

Figure 22 - Ajout d’un disque dédié aux données de Marseille.

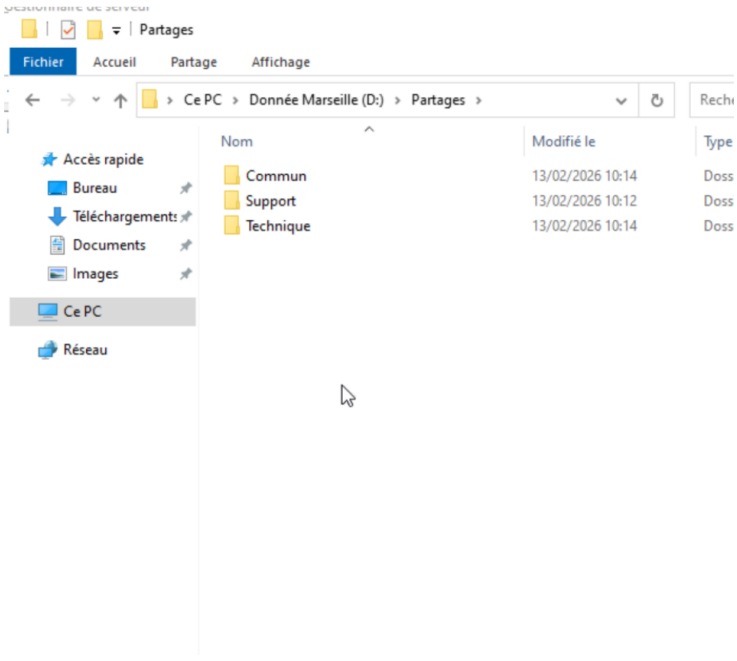


Figure 23 - Création des dossiers partagés Commun, Support et Technique.

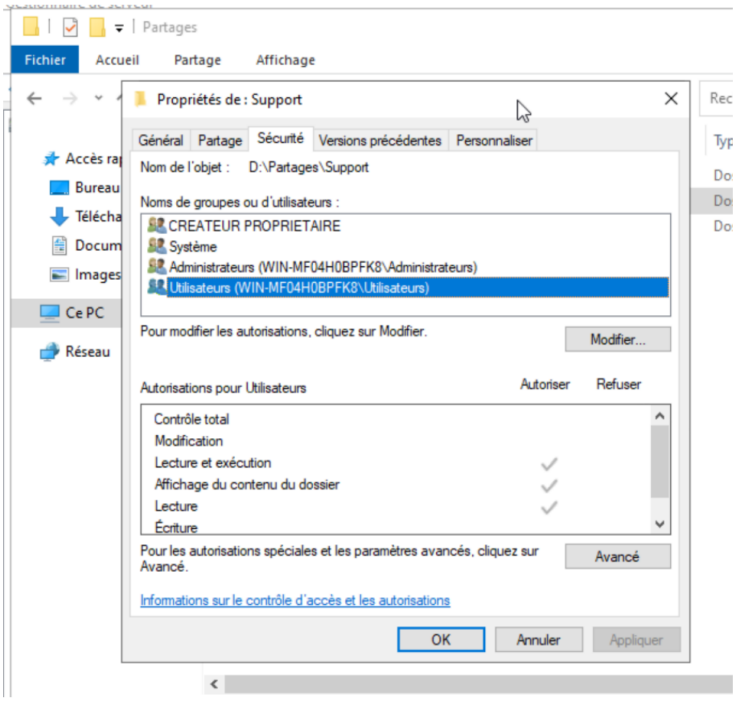
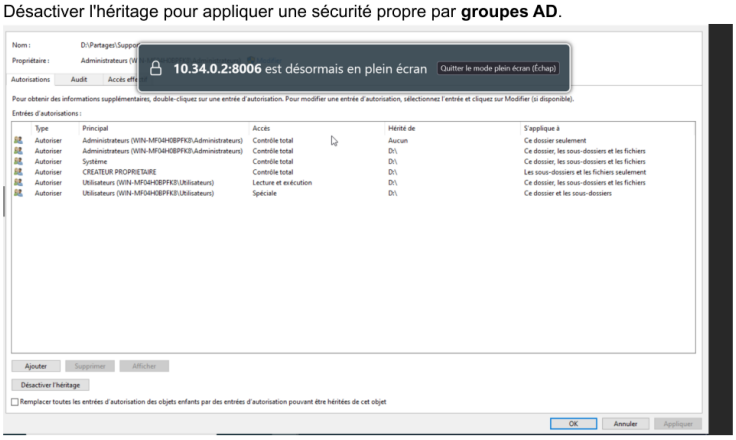


Figure 24 - Vérification des permissions NTFS sur le dossier Support.

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



Ip serveur:

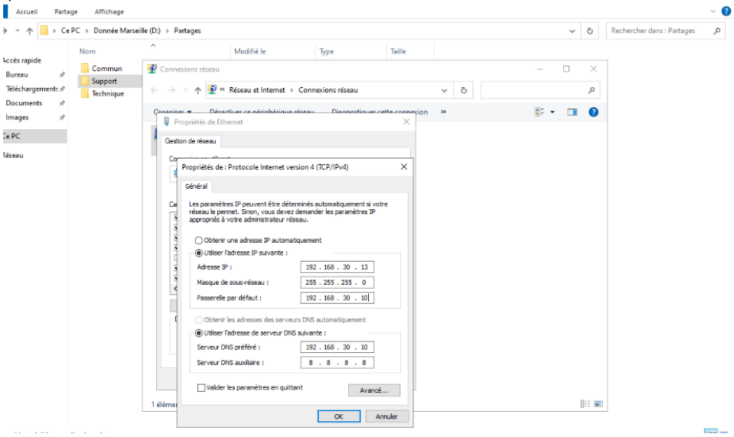


Figure 25 - Désactivation de l’héritage et configuration IP du serveur de fichiers.

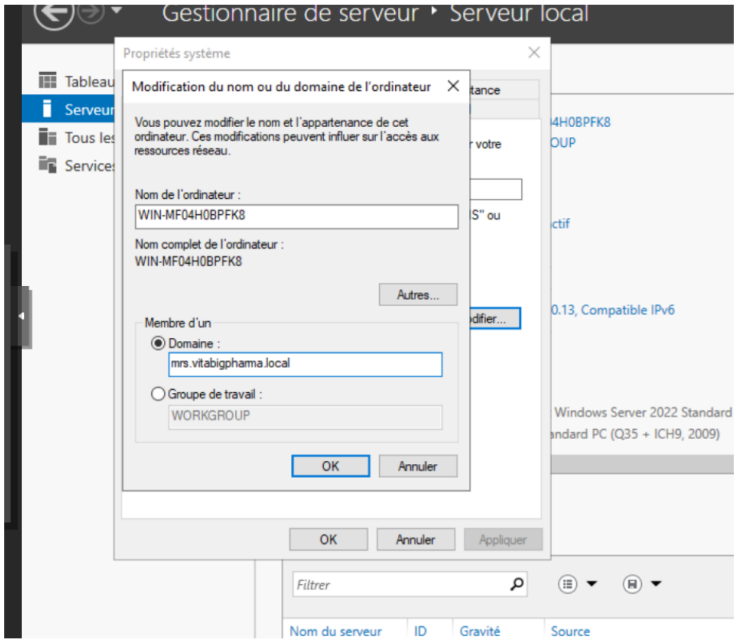


Figure 26 - Intégration du serveur de fichiers au domaine.

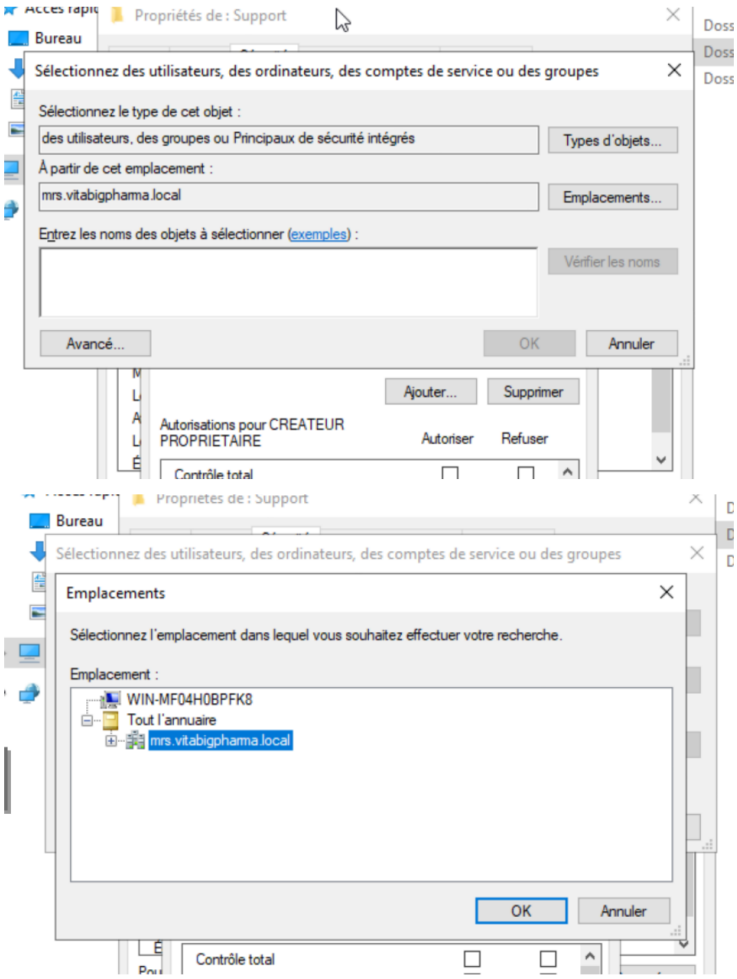


Figure 27 - Sélection des groupes Active Directory pour les permissions.

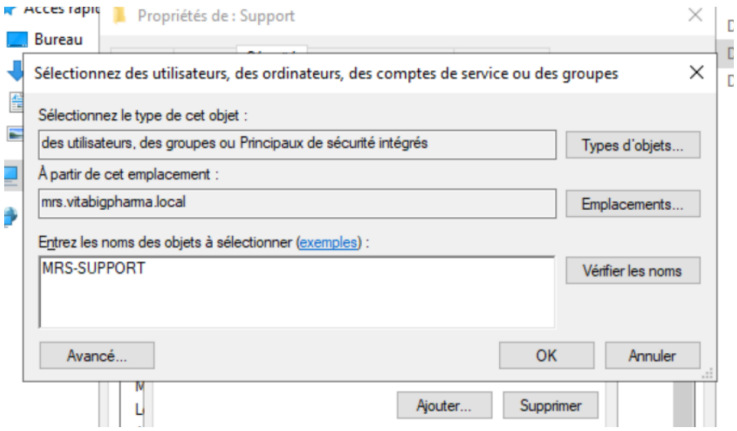


Figure 28 - Ajout du groupe MRS-SUPPORT sur le dossier Support.

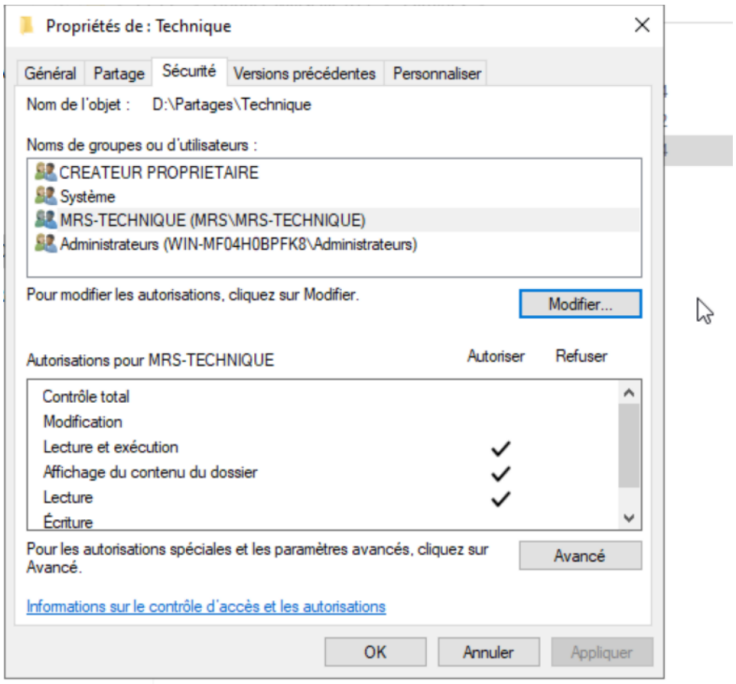


Figure 29 - Permissions du groupe MRS-TECHNIQUE sur le dossier Technique.

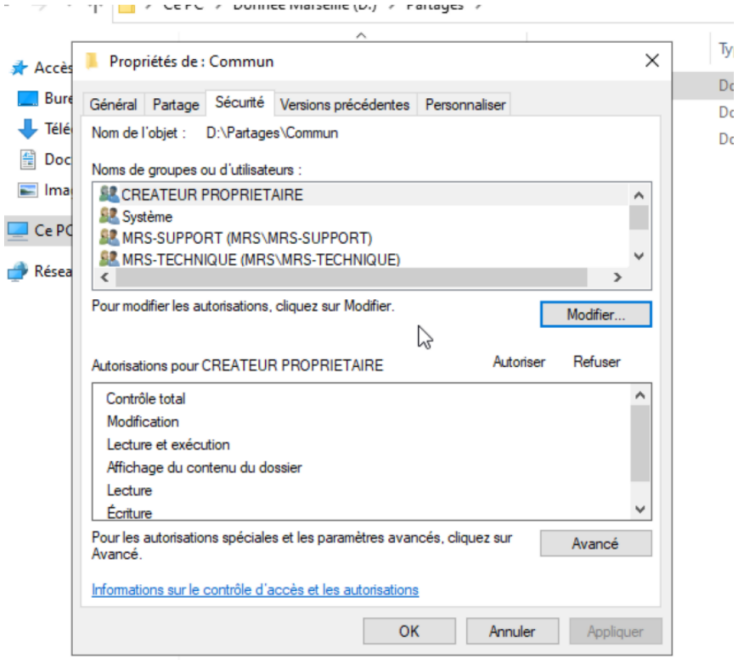
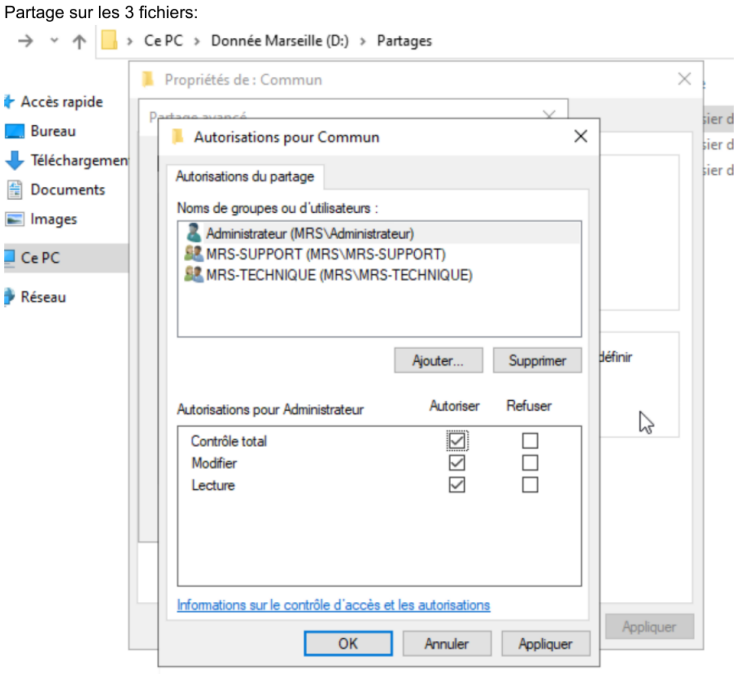


Figure 30 - Permissions sur le dossier Commun.

Partage sur les 3 fichiers:



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

Figure 31 - Partage des trois dossiers et finalisation du serveur de fichiers.

5.6 GPO

Les GPO permettent d'appliquer automatiquement des paramètres aux utilisateurs et aux postes du domaine. Dans ce projet, elles sont utilisées notamment pour le mappage automatique des lecteurs réseau selon les services.

GPO via AD1:

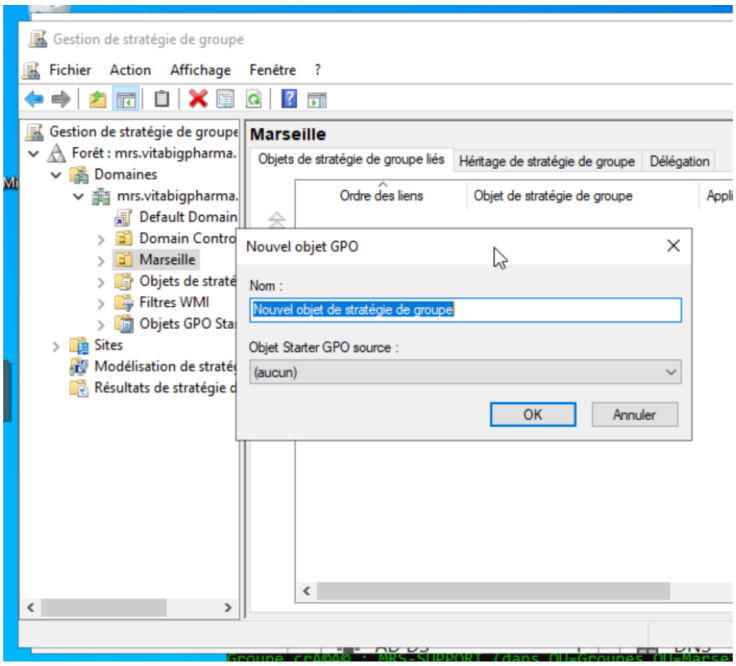


Figure 32 - Création d'une GPO liée à l'OU Marseille.

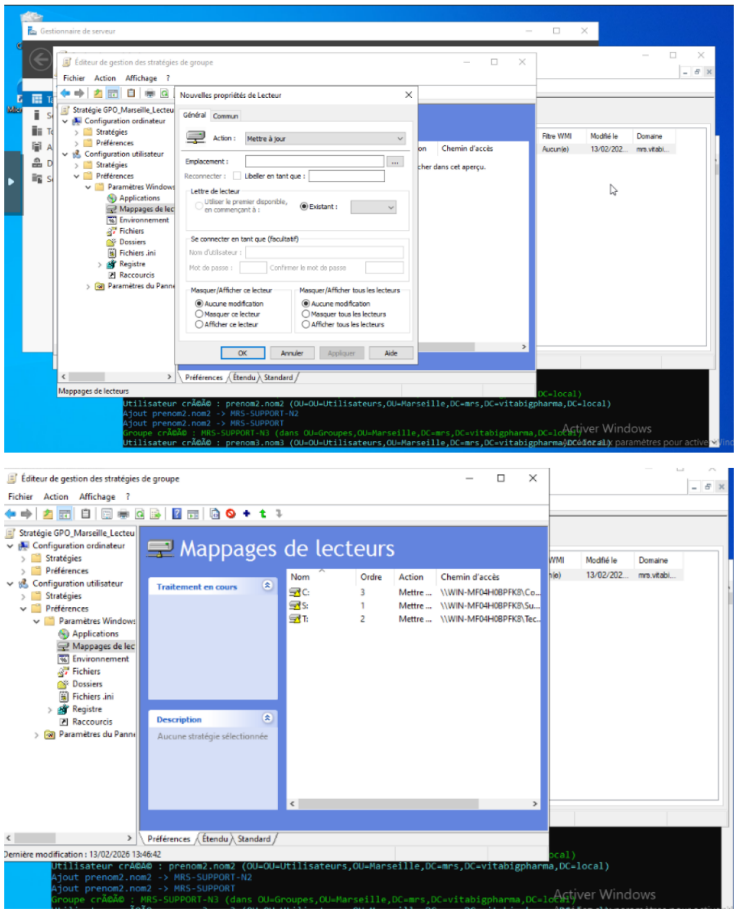
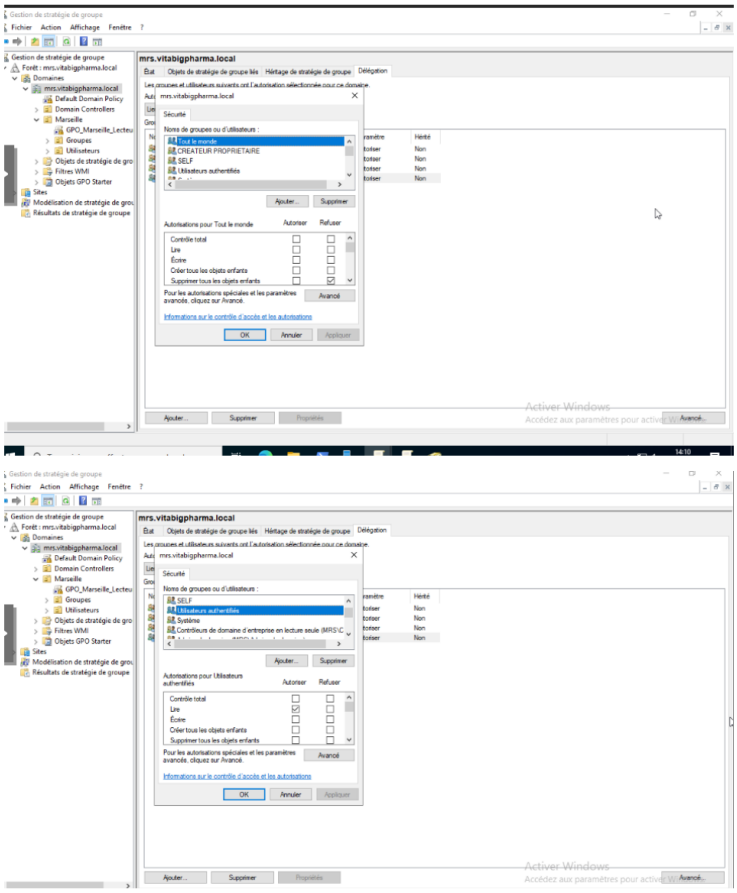


Figure 33 - Configuration du mappage des lecteurs réseau par GPO.

5.7 GLPI

GLPI est déployé sur le site de Marseille pour centraliser les tickets et les demandes de support informatique. Il permet de suivre les incidents, d'affecter les demandes à un technicien et de conserver l'historique des interventions. L'authentification peut être reliée à Active Directory via LDAP afin que les utilisateurs se connectent avec leur compte de domaine.



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)

Figure 34 - Éléments liés à la configuration des droits et début de la mise en place de GLPI.

5.8 Dolibarr

Dolibarr est prévu côté Toulouse pour répondre aux besoins de gestion administrative. Dans cette réalisation, le périmètre personnel porte principalement sur Marseille ; Dolibarr est donc mentionné comme service métier du site de Toulouse, mais il n’est pas le cœur du déploiement présenté.

6. Tests et validation

6.1 Méthodologie

Les tests ont pour objectif de vérifier que chaque composant de l'infrastructure fonctionne correctement : accès réseau, communication inter-sites, sécurité, VPN, authentification, services métiers, sauvegardes et continuité de service.

6.2 Tableau de tests

Test	Élément testé	Action	Résultat attendu
Accès VLAN Marseille	Réseau collaborateurs / serveurs	Ping vers passerelle ou serveur	Réponse OK
VPN site-à-site	IPsec Marseille - Toulouse	Ping inter-sites	Communication OK
VPN nomade	OpenVPN	Connexion utilisateur distant	Accès aux ressources internes
Authentification	Active Directory	Ouverture de session	Connexion réussie
Serveur de fichiers	Partages réseau	Accès aux dossiers selon groupe	Accès autorisé ou refusé selon droits
GLPI	Service web	Connexion à l'interface	Service accessible
Sauvegarde	Serveur de fichiers	Test de restauration fichier	Restauration réussie

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

Figure 35 - Tests fonctionnels, tests de sécurité et tests de continuité.

6.3 Résultats des validations complémentaires

Les vérifications suivantes complètent le tableau de tests présenté précédemment. Elles portent sur les éléments réellement validés pendant la maquette : tunnel IPsec, accès OpenVPN côté pare-feu, création de compte AD et intégration d'un poste client au domaine.

Contrôle réalisé	Résultat obtenu
Tunnel IPsec Marseille - Toulouse	Statut IPsec Established et ping réussi vers 192.168.10.20.
OpenVPN nomade	Serveur OpenVPN configuré en UDP 1194, réseau tunnel 192.168.60.0/24, règles OpenVPN créées.
Compte utilisateur AD	Compte Test Support créé et rattaché au groupe MRS-SUPPORT.
Poste client Windows	Poste client en 192.168.40.16, DNS AD configuré et jonction au domaine réussie.
Résolution DNS interne	Le domaine mrs.vitabigpharma.local est résolu par le contrôleur de domaine 192.168.30.10.

Ces tests confirment le fonctionnement des briques principales du projet : segmentation réseau, résolution DNS AD, authentification centralisée, accès VPN et communication inter-sites. Les règles permissives utilisées pendant la phase de test pourront ensuite être resserrées pour n'autoriser que les flux strictement nécessaires.

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

Figure 36 - Tests de continuité du télétravail et préparation du déploiement pfSense.

7. Exploitation et maintenance

7.1 Sauvegardes

Les sauvegardes concernent en priorite le serveur de fichiers, Active Directory/DNS, GLPI et les configurations pfSense. Le serveur de fichiers est prioritaire car il contient les donnees partagees des services. Une methode simple consiste a utiliser un script planifie qui copie les donnees vers un emplacement de sauvegarde, puis a realiser un test de restauration.

Élément sauvegardé	Objectif
Serveur de fichiers	Restaurer les documents des utilisateurs et services en cas de perte.
Active Directory / DNS	Retrouver l’annuaire, les utilisateurs, les groupes et la configuration du domaine.

Élément sauvegardé	Objectif
GLPI	Conserver les tickets, l’historique et la configuration du support.
pfSense	Restaurer rapidement les règles firewall, le VPN IPsec, OpenVPN et les interfaces.

7.3 Procédure de restauration

- Identifier l’incident et les données ou services impactés.
- Vérifier la disponibilité de la sauvegarde la plus récente.
- Restaurer le fichier, la configuration ou le service concerné.
- Tester le bon fonctionnement après restauration.
- Documenter l’incident et la restauration effectuée.

8. Sécurité

8.1 Mesures de sécurité mises en place

- Segmentation réseau entre serveurs et collaborateurs.
- Filtrage des flux avec pfSense.
- Droits d'accès appliqués par groupes Active Directory.
- Désactivation de l'héritage NTFS sur les dossiers sensibles.
- VPN IPsec chiffré entre Marseille et Toulouse.
- VPN nomade OpenVPN pour l'accès distant.
- Redondance Active Directory / DNS avec deux contrôleurs de domaine.
- Sauvegardes et tests de restauration.

8.2 Audit Active Directory

Le modèle prévoit l'utilisation de PingCastle afin d'analyser la sécurité Active Directory. Cet audit permet d'identifier les faiblesses de configuration et de proposer des recommandations correctives.

8.3 Audit Linux

Le modèle prévoit l'utilisation de Lynis pour réaliser un audit de sécurité des serveurs Linux, notamment pour les services applicatifs comme GLPI. Les résultats peuvent être utilisés pour durcir le système.

8.4 Points d'amélioration sécurité

- Mettre en place une authentification multifacteur pour les accès distants.
- Ajouter un SIEM pour centraliser les journaux et détecter les incidents.
- Durcir les règles firewall après les tests en remplaçant les règles "any" par des règles précises.
- Formaliser une politique de mots de passe et de sauvegarde.

9. Gestion des incidents

La gestion des incidents est assurée par GLPI. Les utilisateurs peuvent créer des tickets pour signaler une panne, une demande ou un besoin d'assistance. Le support informatique peut ensuite qualifier, affecter et suivre les tickets jusqu'à leur résolution.

9.1 Procédure type

Étape	Description
1. Détection	Un utilisateur signale un problème ou une anomalie.
2. Qualification	Le support analyse le type d'incident, son urgence et son impact.
3. Affectation	Le ticket est attribué à un technicien ou à une équipe.
4. Résolution	Le technicien corrige le problème ou applique une solution de contournement.
5. Clôture	Le ticket est fermé après validation de la résolution.

9.2 Exemple d'utilisation

Un utilisateur du service technique ne parvient pas à accéder au dossier partagé Technique. Il ouvre un ticket GLPI. Le support vérifie son appartenance au groupe Active Directory MRS-TECHNIQUE, contrôle les permissions NTFS et partage, puis corrige l'accès si nécessaire.

10. Conclusion

Le projet a permis de concevoir et de déployer une infrastructure multi-sites sécurisée pour VitaBigPharma. La solution répond aux besoins principaux : authentification centralisée, segmentation réseau, communication sécurisée entre Marseille et Toulouse, accès distant, partage de fichiers sécurisé, support avec GLPI, sauvegarde et documentation.

Sur le site de Marseille, les éléments principaux ont été mis en place : pare-feu pfSense, Active Directory/DNS avec redondance, automatisation PowerShell, serveur de fichiers avec droits par groupes, GPO, GLPI et interconnexion avec le site de Toulouse via IPsec. Les tests permettent de valider le fonctionnement général de l'infrastructure.

L'ensemble de la documentation, des schémas, des captures et des procédures doit permettre l'exploitation, la maintenance et la présentation de la solution dans le cadre de l'épreuve E6 du BTS SIO SISR.

11. Perspectives d'amélioration

- Mettre en place une haute disponibilite des pare-feux pour eviter un point unique de panne.

- Activer la MFA pour les acces distants VPN et les comptes sensibles.

- Formaliser un PRA/PCA pour assurer la reprise et la continuite d'activite.