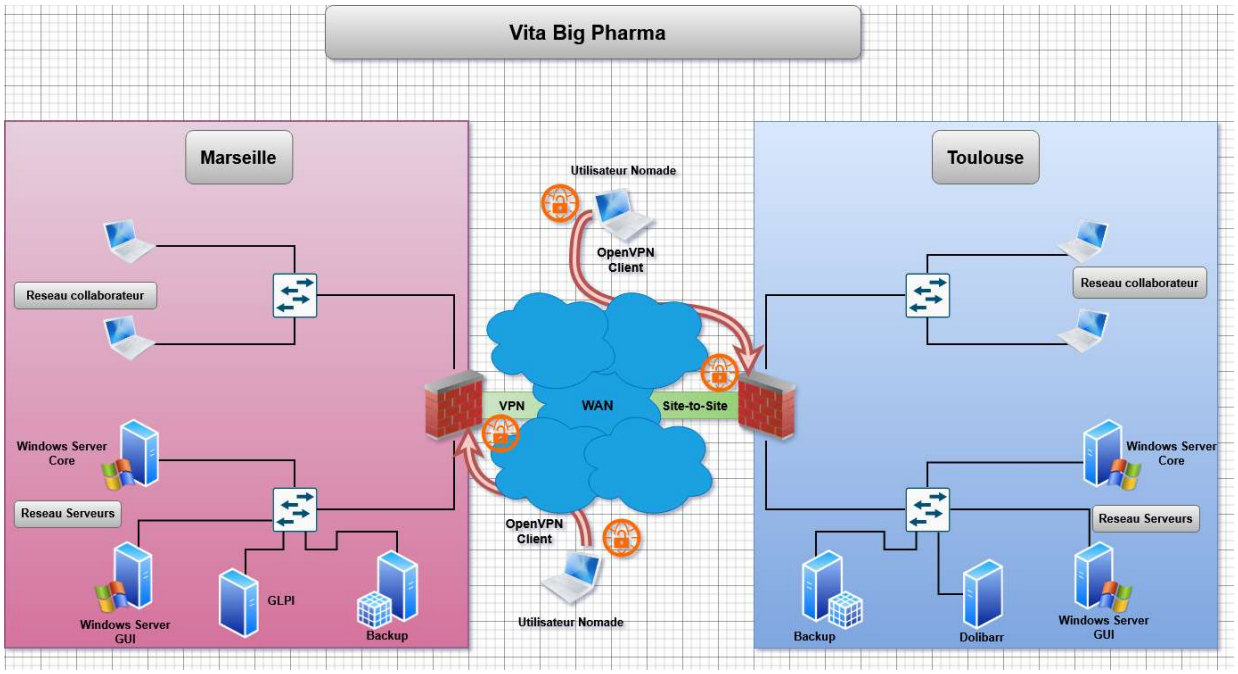
BTS SIO SISR - U6

Projet 2 S - Vita Big Pharma

Conception, déploiement et exploitation d'une infrastructure réseau sécurisée

Documentation technique - Version 1



Élément	Information
Entreprise étudiée	Vita Big Pharma
Site documenté	Marseille
Rôle du site	Site technique : support informatique et service technique
Environnement	VirtualBox, OPNsense, Windows Server, Debian, GLPI, Prometheus
Session	2025/2026

Périmètre de cette V1
Cette documentation suit l'ordre de la feuille de route, mais elle ne détaille que les éléments réellement appuyés par les captures fournies. Elle est centrée sur le site de Marseille et sur les preuves disponibles dans l'archive de captures.

Sommaire

1. Présentation de l’entreprise
2. Analyse du besoin
3. Étude de solutions
4. Solution retenue
5. Architecture technique
6. Mise en œuvre
7. Tests et validation
8. Exploitation et maintenance
9. Sécurité et supervision
10. Conclusion et perspectives
11. Annexes

1. Présentation de l'entreprise

Vita Big Pharma est une entreprise pharmaceutique spécialisée dans la fabrication de compléments alimentaires. Dans le scénario du projet, l'entreprise s'implante en France avec deux sites : Toulouse pour le siège administratif et Marseille pour le site technique.

Site	Services	Rôle
Toulouse	Direction, Ressources Humaines, Finance	Siège administratif
Marseille	Support informatique, Service technique	Site technique documenté dans cette V1

Le dossier présenté ici concerne principalement la partie Marseille, qui doit fournir les services techniques, l'accès aux outils de support, l'authentification locale, la sécurité réseau et les premières fonctions de supervision.

2. Analyse du besoin

2.1 Besoins fonctionnels

- Permettre l'authentification des utilisateurs du site Marseille via un domaine Active Directory.
- Séparer le réseau collaborateurs du réseau serveurs afin de limiter les risques de propagation en cas d'incident.
- Mettre à disposition un outil de ticketing GLPI pour le support informatique.
- Prévoir un accès VPN nomade pour l'administration ou le télétravail.
- Superviser les ressources du serveur Linux hébergeant les services métiers.
- Réaliser un premier niveau d'audit de sécurité sur l'Active Directory et sur le serveur Linux.

2.2 Contraintes techniques et sécurité

- Les LAN sont isolés par site et segmentés selon leur usage.
- Les règles de filtrage sont centralisées sur OPNsense.
- Les accès d'administration doivent rester limités aux comptes autorisés.
- Les comptes utilisateurs sont créés à partir d'un fichier CSV afin d'éviter les erreurs de saisie.
- Les captures intégrées servent de preuves de réalisation et de validation.

3. Étude de solutions

Besoin	Solution retenue	Alternative	Justification
Pare-feu / routage	OPNsense	pfSense	Interface claire, support VPN, filtrage, WireGuard, adapté à une maquette BTS.
Annuaire	Active Directory + DNS	OpenLDAP	Standard en environnement Windows, gestion centralisée des utilisateurs et groupes.
Ticketing	GLPI	OTRS / Zammad	Outil connu en BTS SISR,

			ticketing, parc informatique, groupes support.
Supervision	Prometheus + node_exporter	Zabbix	Déploiement léger, métriques système Linux, compatible Docker.
Audit AD	PingCastle	Scripts PowerShell	Rapport lisible et score de risque synthétique pour Active Directory.
Audit Linux	Lynis	Auditd manuel	Audit local rapide, recommandations de durcissement.

4. Solution retenue

La solution retenue repose sur une architecture multi-réseaux autour d'un pare-feu OPNsense. Le site Marseille dispose d'un LAN collaborateurs, d'un LAN serveurs et d'un accès VPN nomade WireGuard. Les services internes sont portés par Windows Server pour l'Active Directory et par Debian pour GLPI et la supervision.

Composant	Rôle
OPNsense	Pare-feu, routage, règles réseau, WireGuard
Windows Server GUI	Contrôleur de domaine principal, DNS, administration AD
Windows Server Core	Serveur secondaire / serveur technique, configuration légère
Debian 13	GLPI, base de données, Prometheus, node_exporter, Lynis
Windows 11 collaborateur	Poste client de test, jonction au domaine, test VPN
Windows 10 admin	Poste d'administration pour OPNsense, GLPI et les tests

5. Architecture technique

5.1 Schéma logique

Le schéma ci-dessous représente l'architecture cible de la maquette. Il sert de référence de conception. Dans cette V1, la partie réalisée et documentée est la partie Marseille.

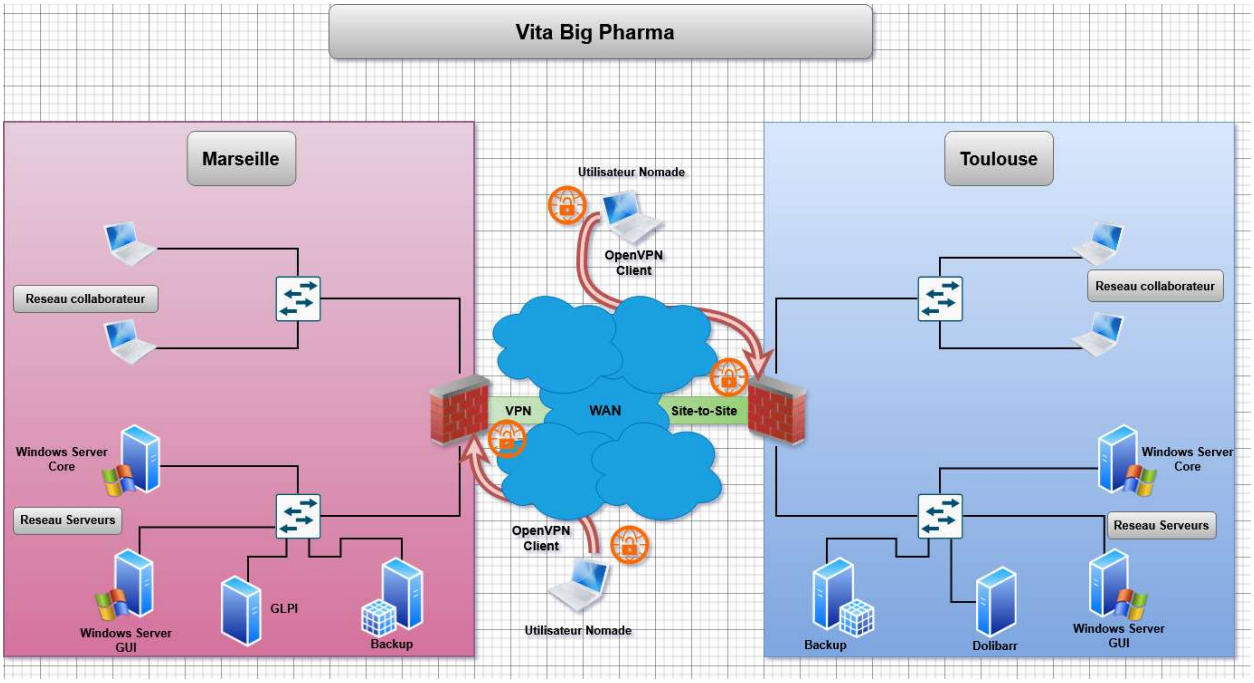


Figure 1 - Schéma logique de conception Vita Big Pharma

5.2 Plan d'adressage de Marseille

Réseau / équipement	Adresse	Usage
WAN OPNsense	10.31.0.2/24	Accès extérieur / réseau hôte
LAN Collaborateurs	172.16.1.0/24	Postes collaborateurs, passerelle 172.16.1.1
LAN Serveurs	172.16.2.0/24	Serveurs internes, passerelle 172.16.2.1
Tunnel WireGuard	10.9.0.0/24	Clients VPN nomades
Serveur GLPI Debian	172.16.2.4	Application GLPI et supervision
Poste collaborateur Win11	172.16.1.15	Client de test
Client VPN	10.9.0.10	Adresse attribuée au client WireGuard

5.3 Nommage et domaine

Élément	Nom retenu dans la maquette
Domaine Active Directory	vitapharmamrs.local
Serveur AD principal	SRV-MRS-01
Serveur secondaire / technique	SRV-BACKUP-01
Serveur Linux	Debian13-GLPI
Poste client	WIN11-COLLABORA

6. Mise en œuvre

6.1 Installation et configuration du pare-feu OPNsense

OPNsense est installé avec trois interfaces principales : WAN, LAN collaborateurs et LAN serveurs. La console locale confirme les adresses IP des interfaces. Les premiers tests de connectivité Internet sont réalisés depuis le pare-fu.

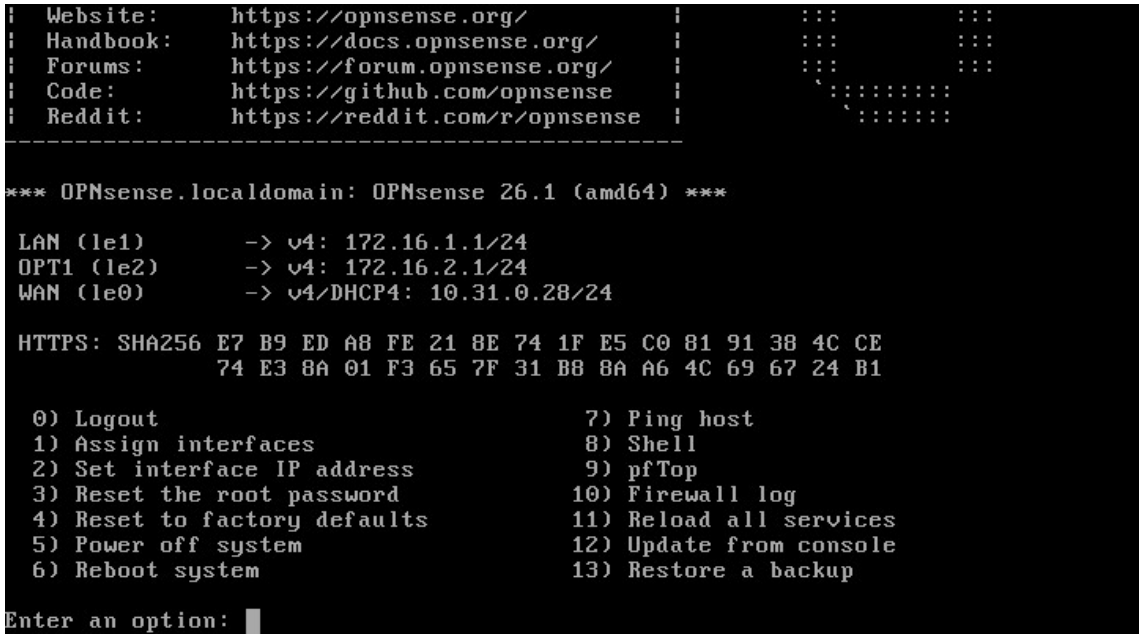


Figure 2 - Console OPNsense : interfaces LAN, OPT1 et WAN configurées

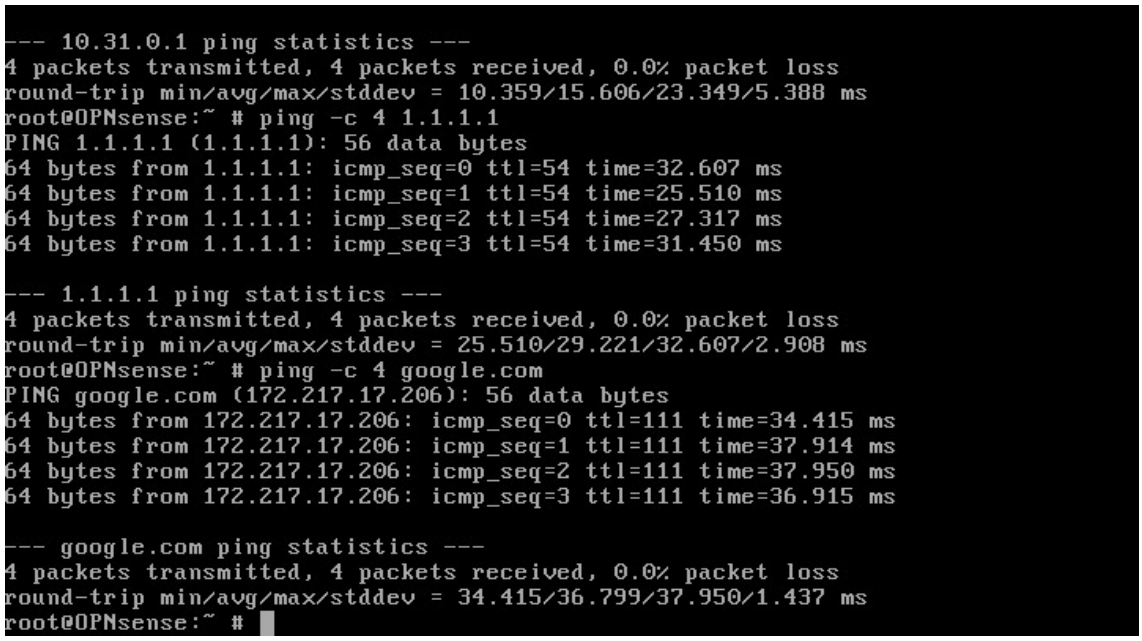


Figure 3 - Test de connectivité Internet depuis OPNsense vers 1.1.1.1 et google.com

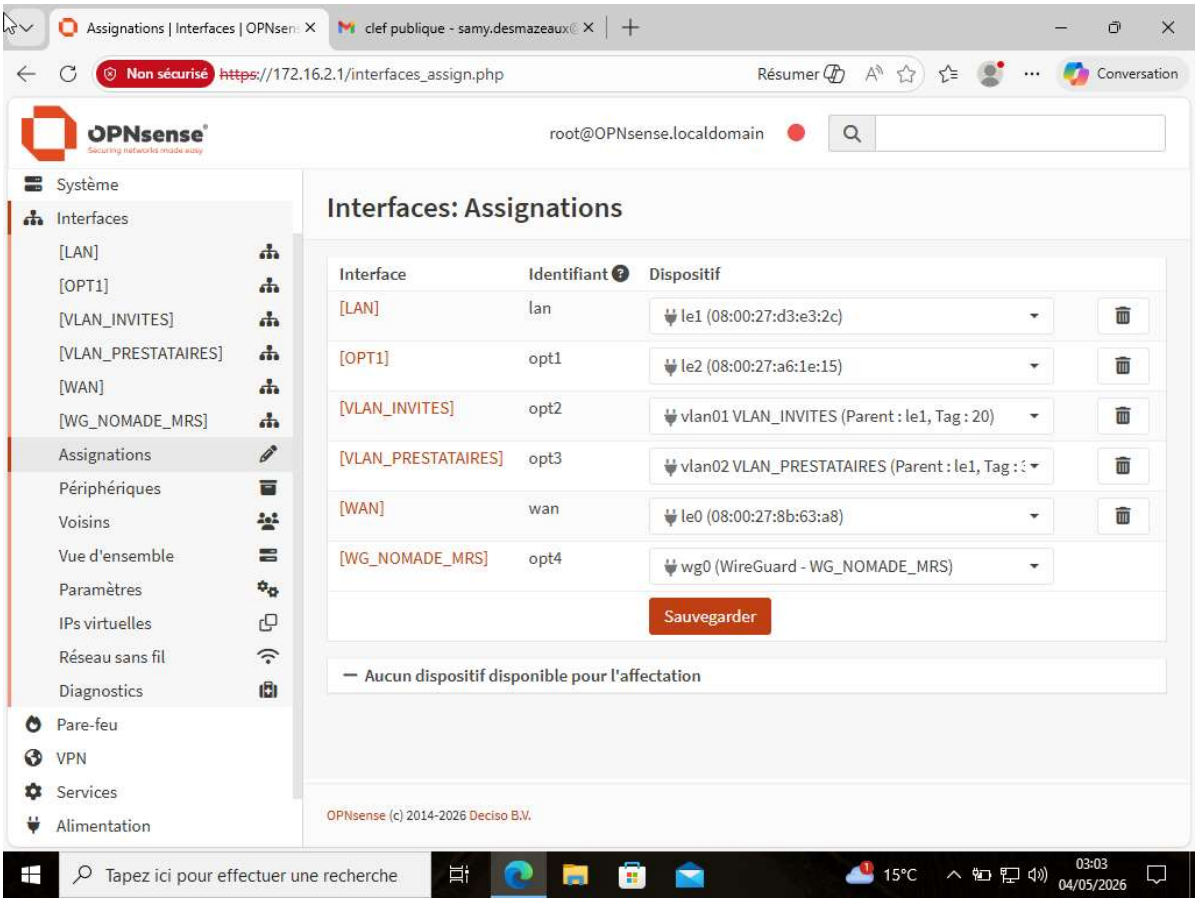


Figure 4 - Assignation des interfaces OPNsense depuis l'interface web

6.2 Configuration du VPN nomade WireGuard

Le VPN nomade est configuré avec une instance WireGuard dédiée au site Marseille. Les clés visibles dans les captures ont été masquées dans la documentation.

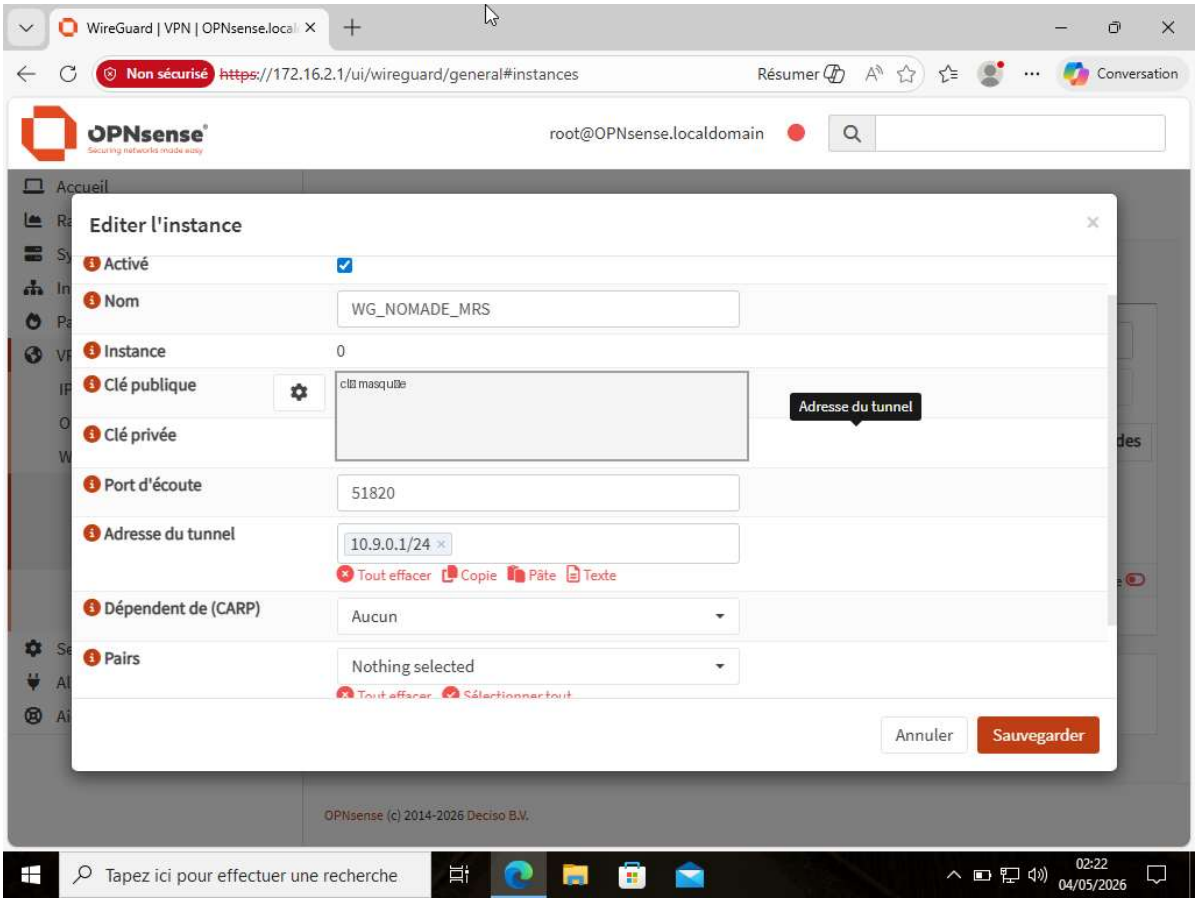


Figure 5 - Instance WireGuard WG_NOMADE_MRS avec adresse de tunnel 10.9.0.1/24

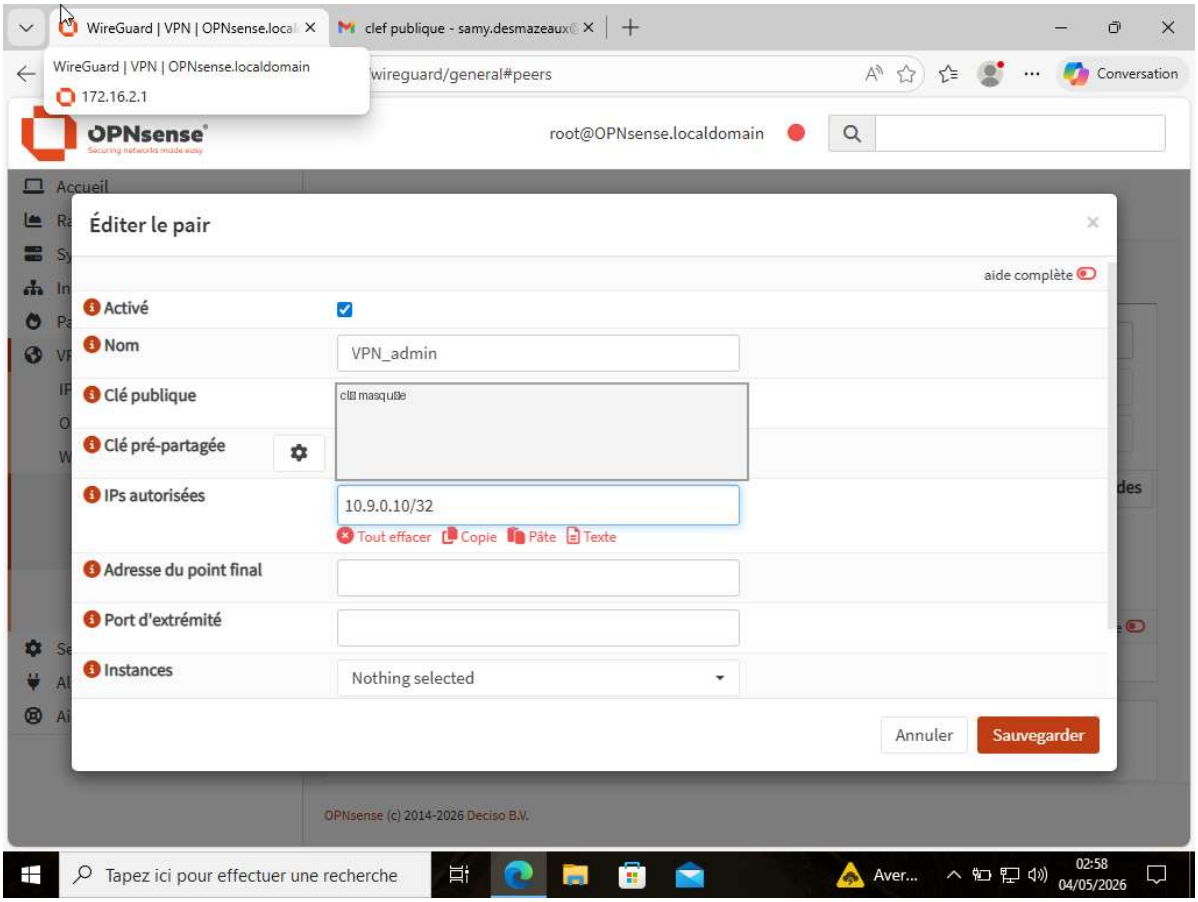


Figure 6 - Pair WireGuard VPN_admin avec IP autorisée 10.9.0.10/32

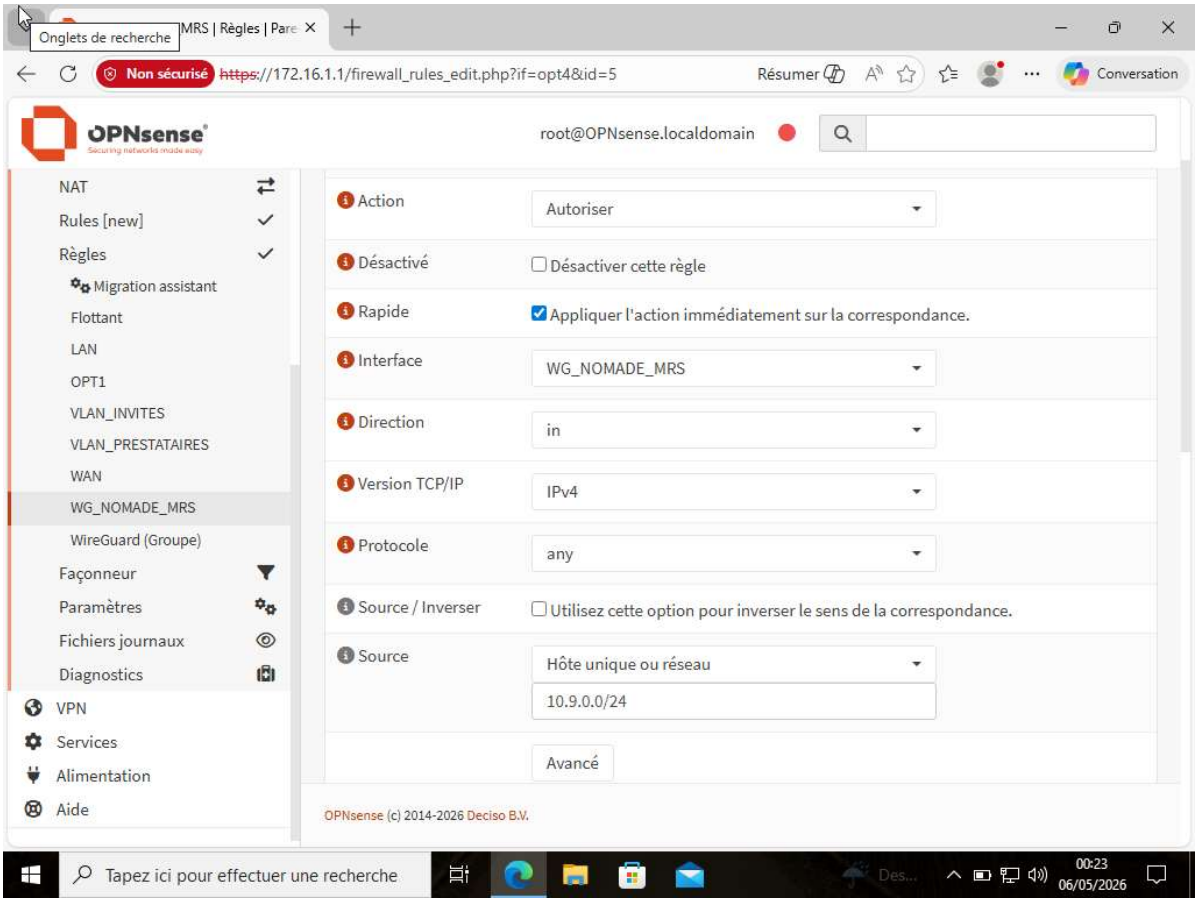


Figure 7 - Règle pare-feu autorisant les flux du réseau VPN nomade

6.3 Déploiement Active Directory et DNS

Le domaine Active Directory utilisé dans la maquette Marseille est vitapharmamrs.local. Le serveur Windows GUI sert d'administration principale. Un serveur Windows Server Core est également configuré pour un rôle serveur secondaire ou technique.

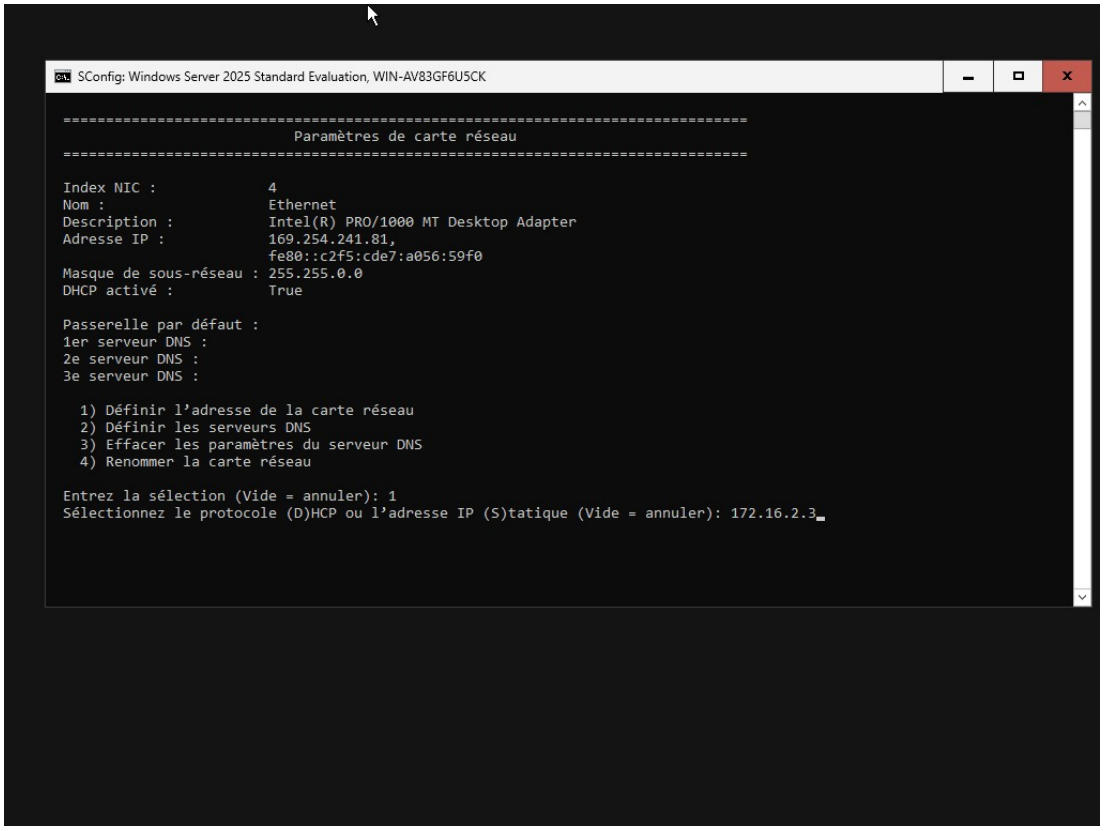


Figure 8 - Début de configuration IP statique du serveur Windows Server Core

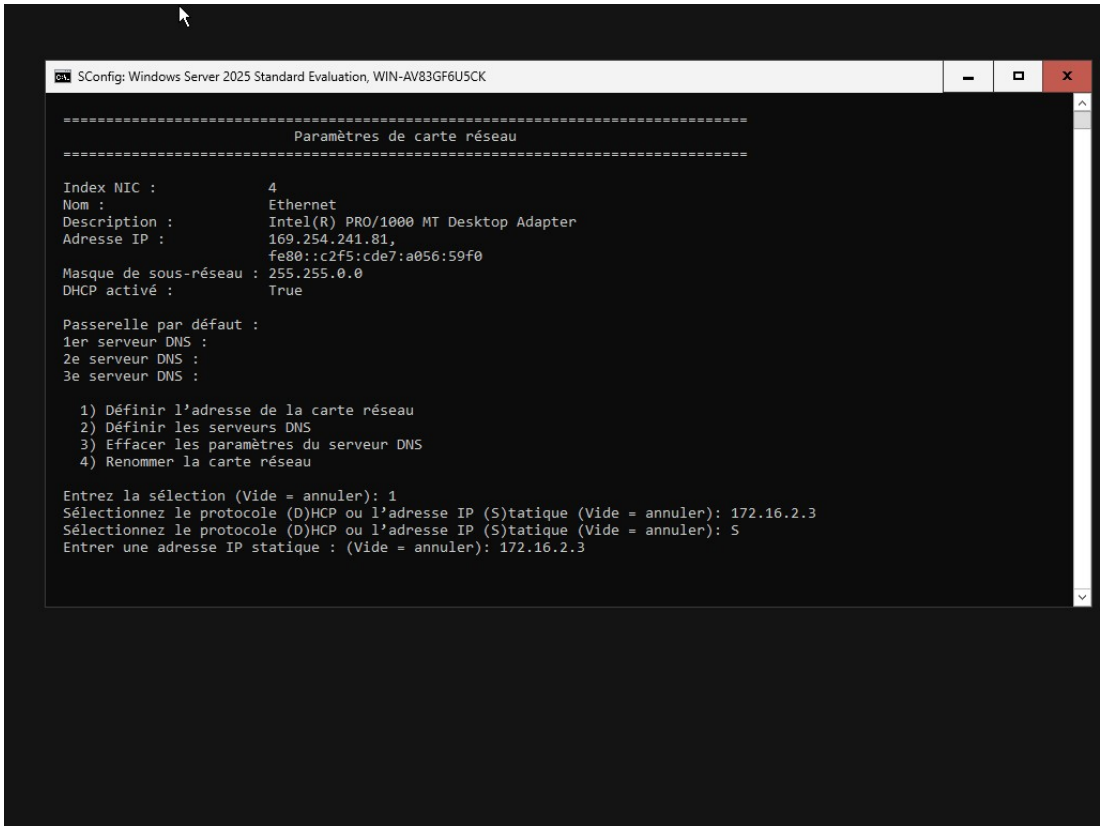


Figure 9 - Saisie de l'adresse 172.16.2.3 sur le serveur Core

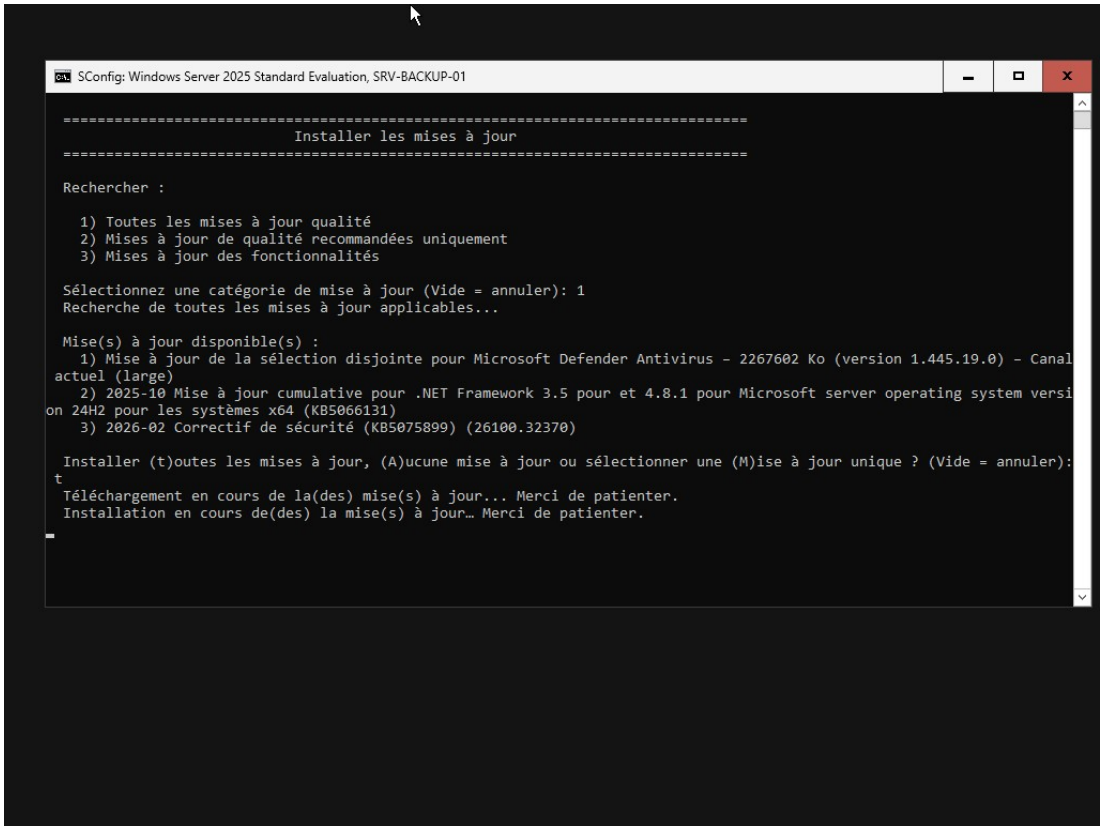


Figure 10 - Mise à jour du serveur Windows Server Core

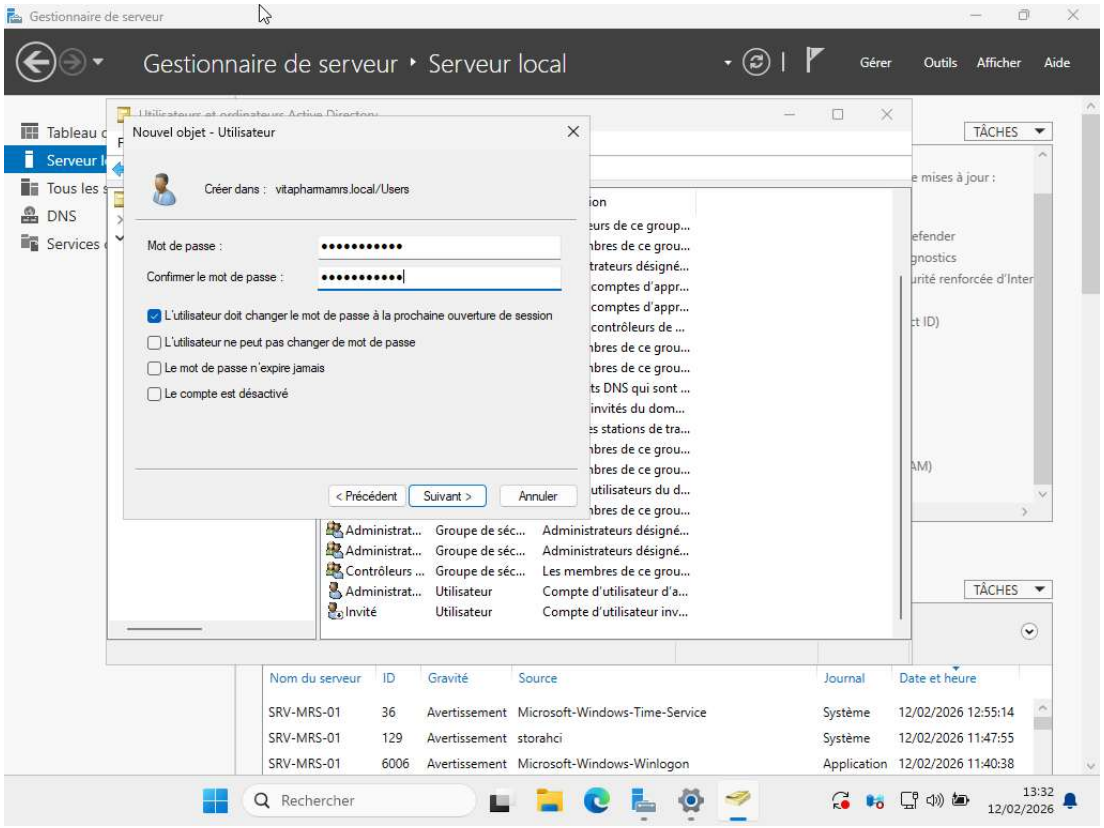


Figure 11 - Création manuelle d'un utilisateur dans Active Directory

6.4 Automatisation des comptes utilisateurs

Les comptes utilisateurs du site Marseille sont importés depuis un fichier CSV. Le fichier contient 30 utilisateurs répartis entre les groupes support SUP_N1, SUP_N2 et SUP_N3.

OU	Groupe	Nombre d'utilisateurs
Support	SUP_N1	10
Support	SUP_N2	10
Technique	SUP_N3	10

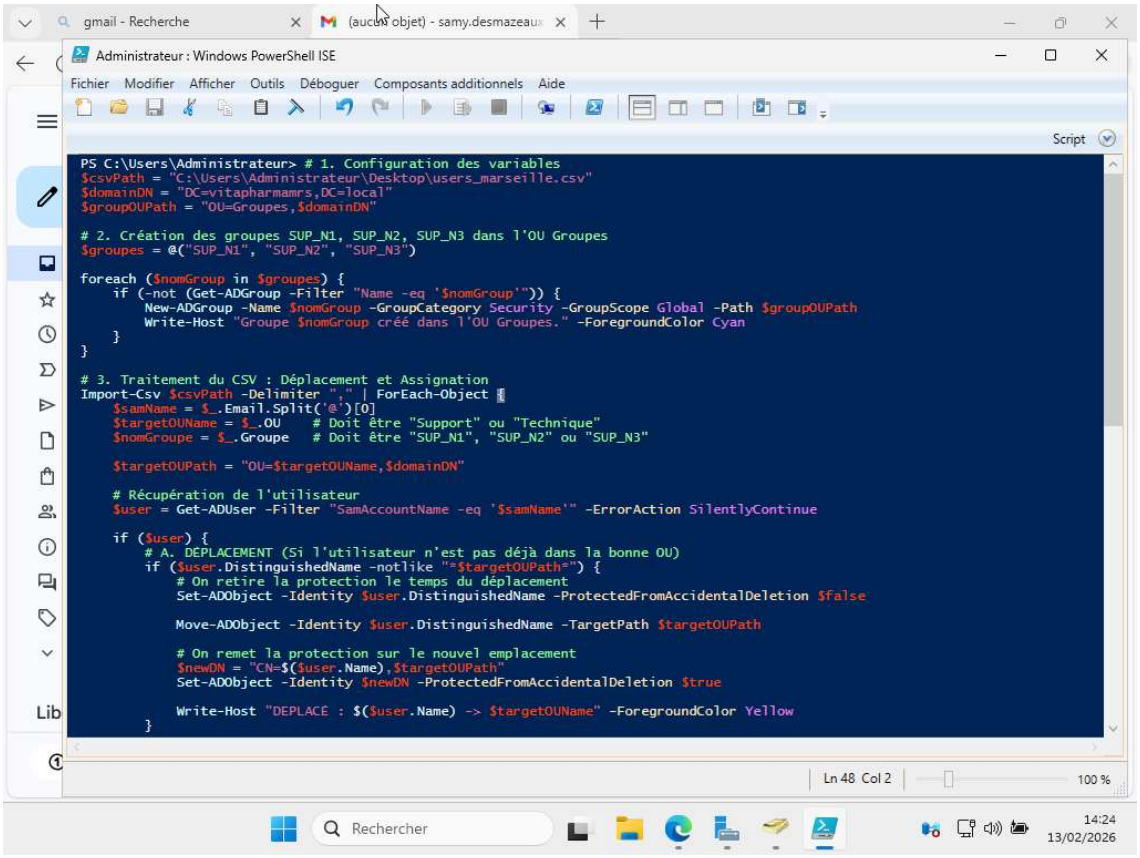


Figure 12 - Script PowerShell : variables, chemin CSV et création des groupes

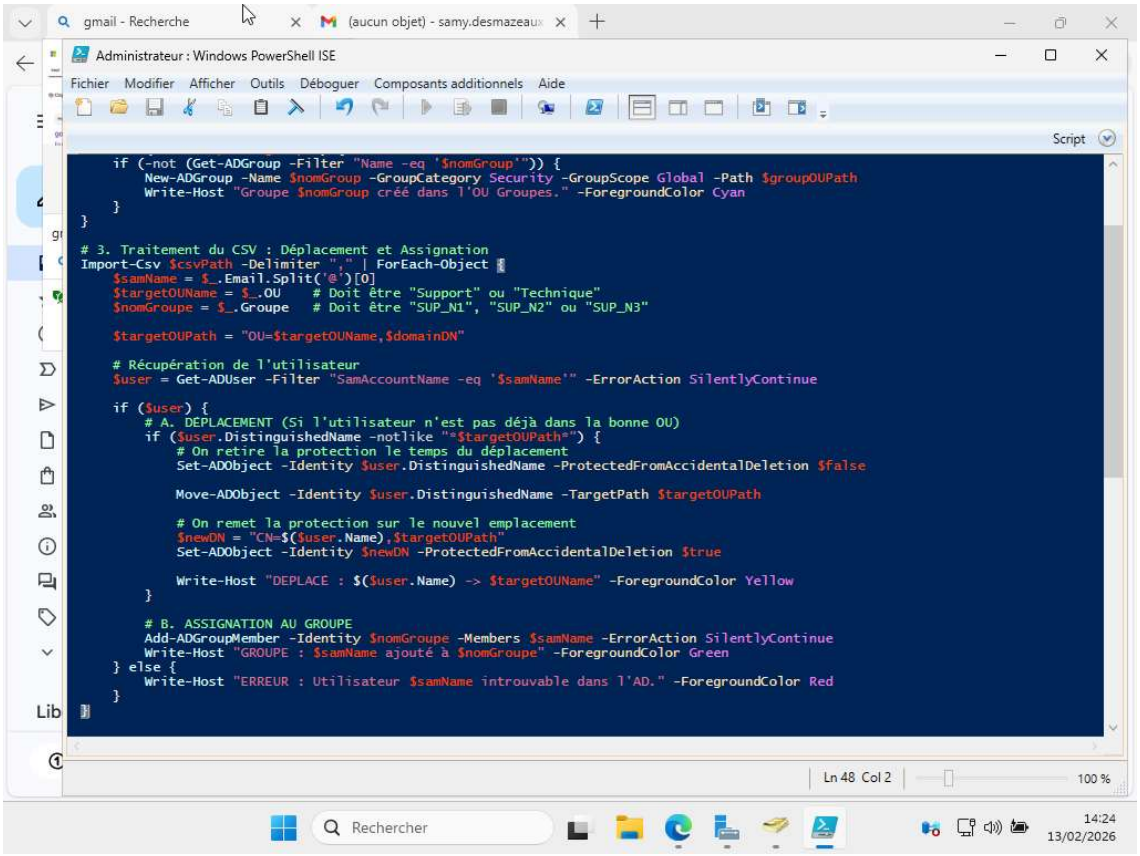


Figure 13 - Script PowerShell : traitement du CSV et déplacement dans les OU

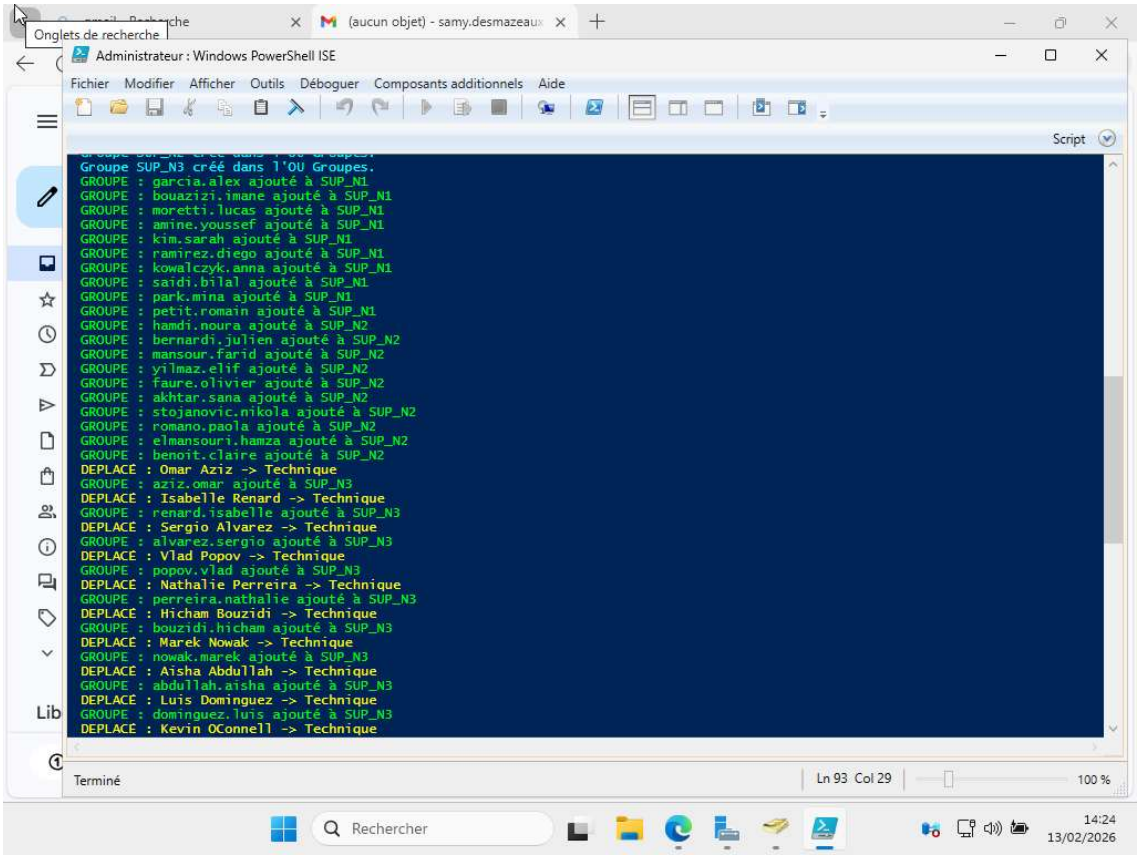


Figure 14 - Sortie du script : utilisateurs déplacés et ajoutés aux groupes

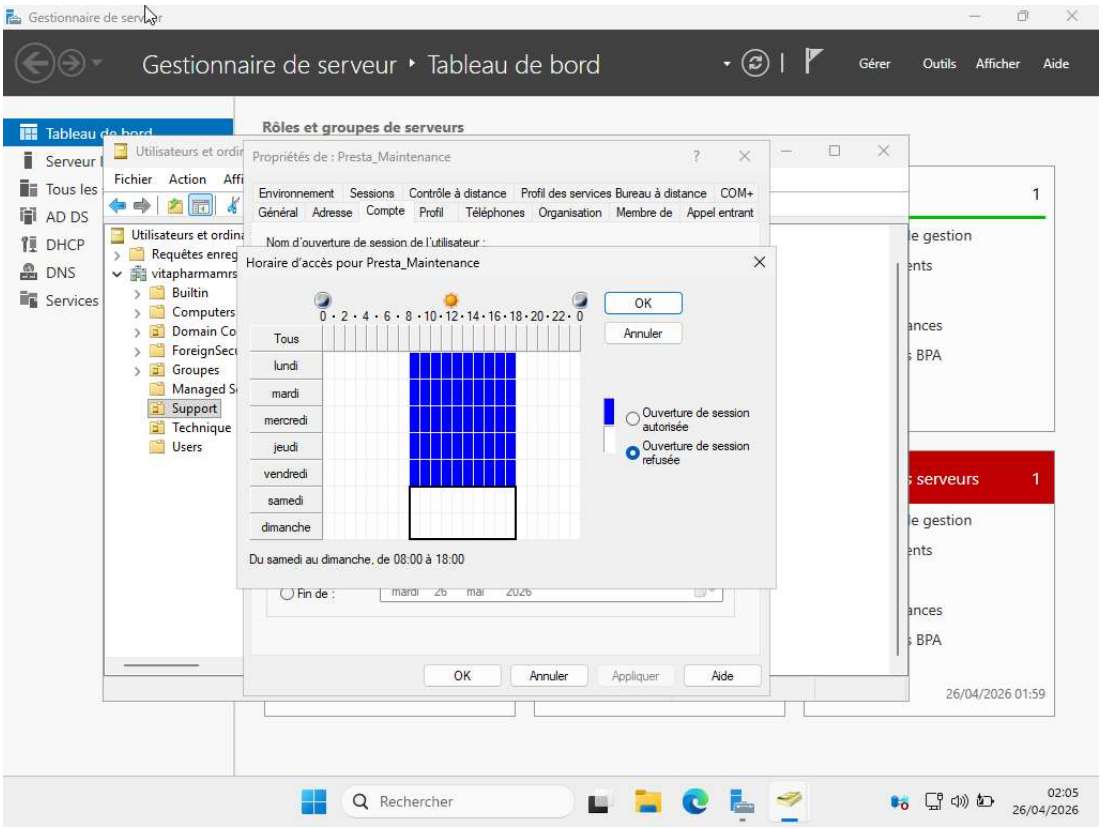


Figure 15 - Exemple de restriction horaire appliquée à un utilisateur AD

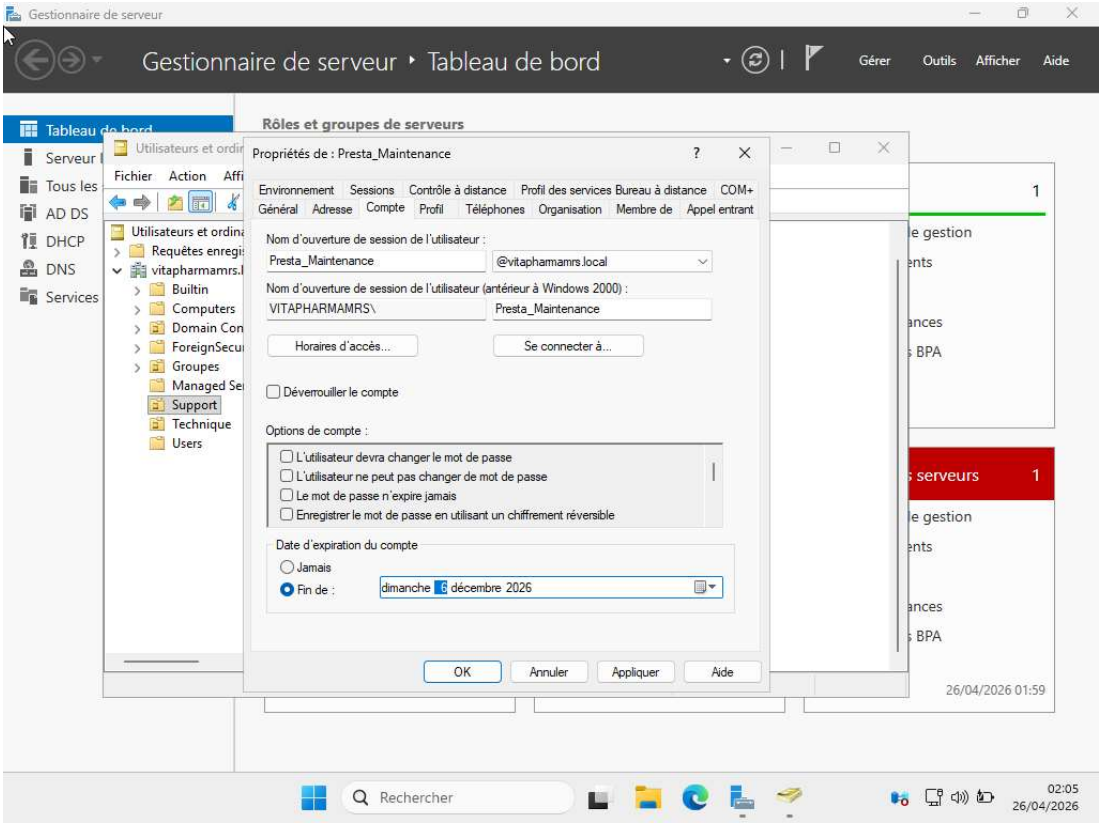


Figure 16 - Exemple d'expiration de compte configurée dans Active Directory

6.5 Intégration du poste collaborateur au domaine

Un poste Windows 11 collaborateur est intégré au domaine Active Directory pour vérifier l'authentification et l'accès aux ressources internes.

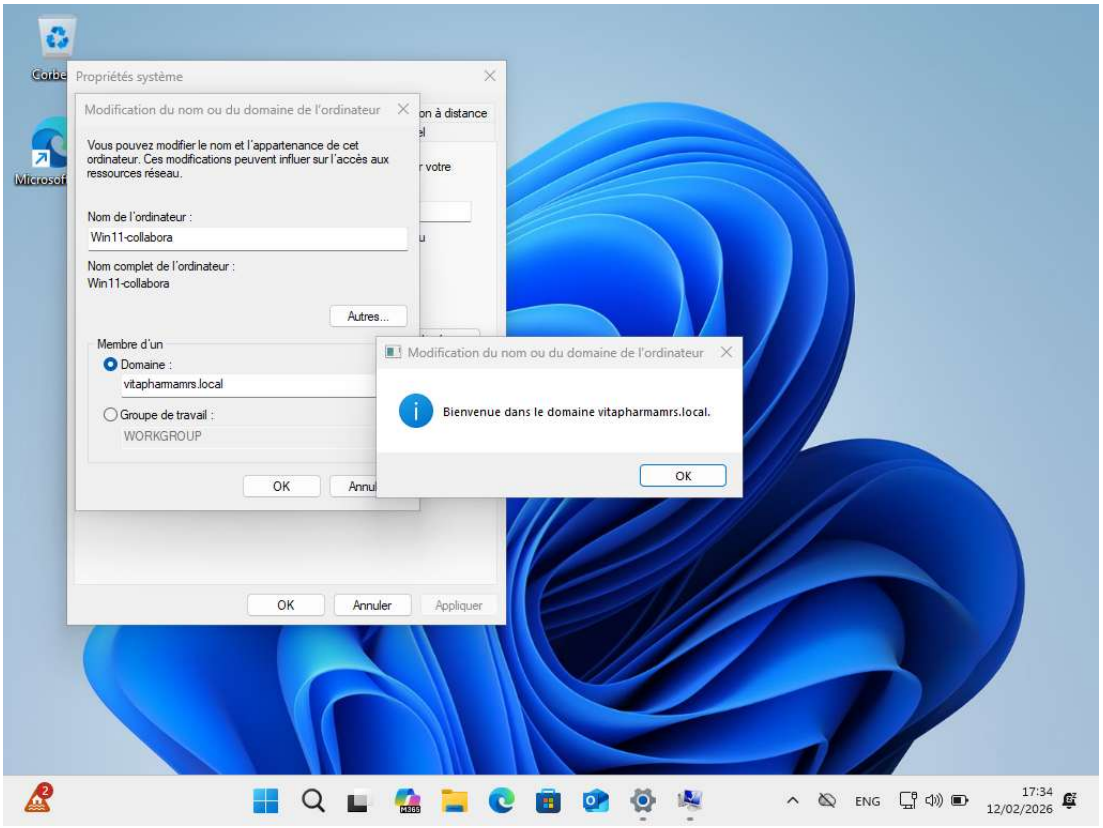


Figure 17 - Jonction du poste Windows 11 au domaine vitapharmamrs.local

6.6 Déploiement du serveur Linux GLPI

Le serveur Debian 13 héberge GLPI. Les captures montrent la configuration réseau, l'installation des paquets nécessaires et la préparation PHP/Apache.

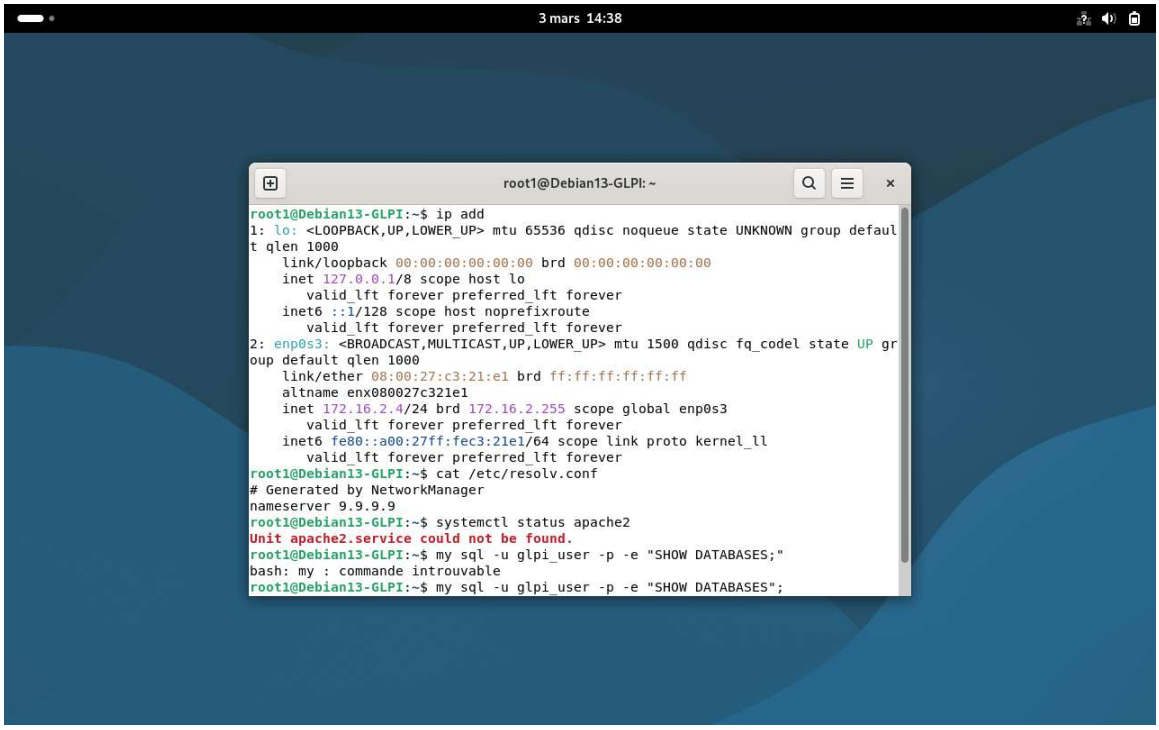


Figure 18 - Vérification réseau du serveur Debian GLPI et adresse 172.16.2.4/24

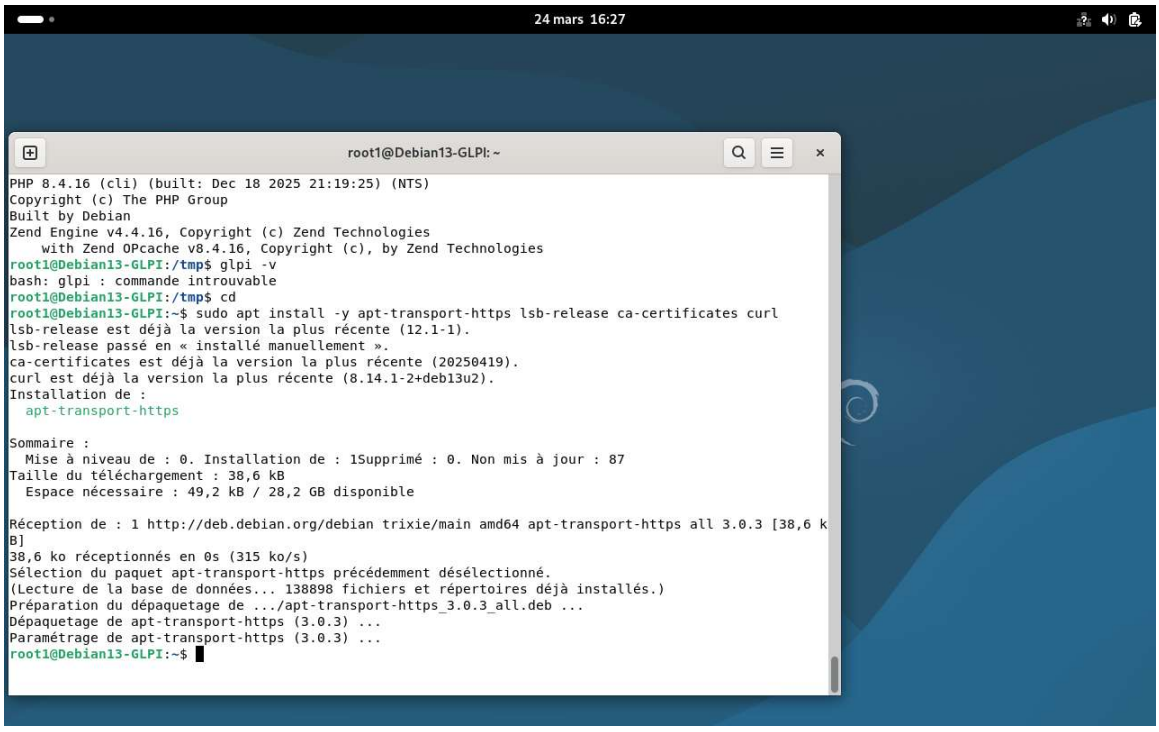


Figure 19 - Vérification PHP et installation de paquets nécessaires

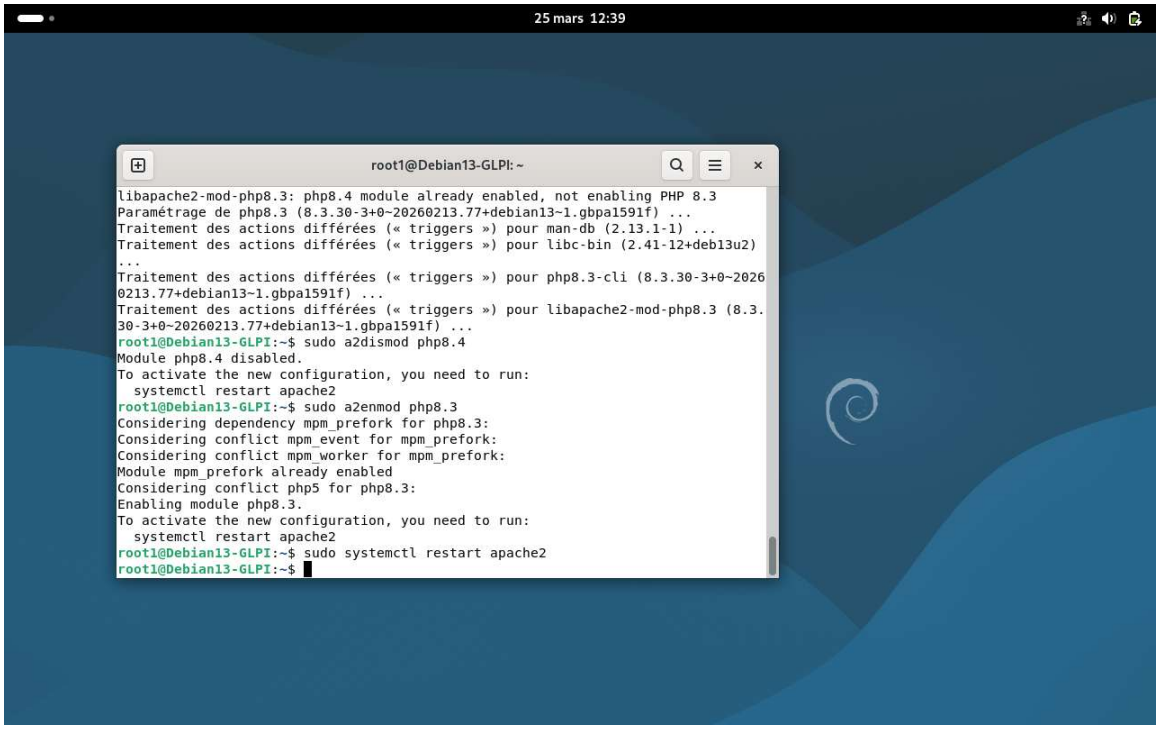


Figure 20 - Activation du module PHP et redémarrage d'Apache

6.7 Mise en service de GLPI

GLPI est utilisé pour gérer les incidents et référencer un premier inventaire de parc. Les captures prouvent la création d'un ticket, son traitement et l'enregistrement d'un ordinateur dans le parc.

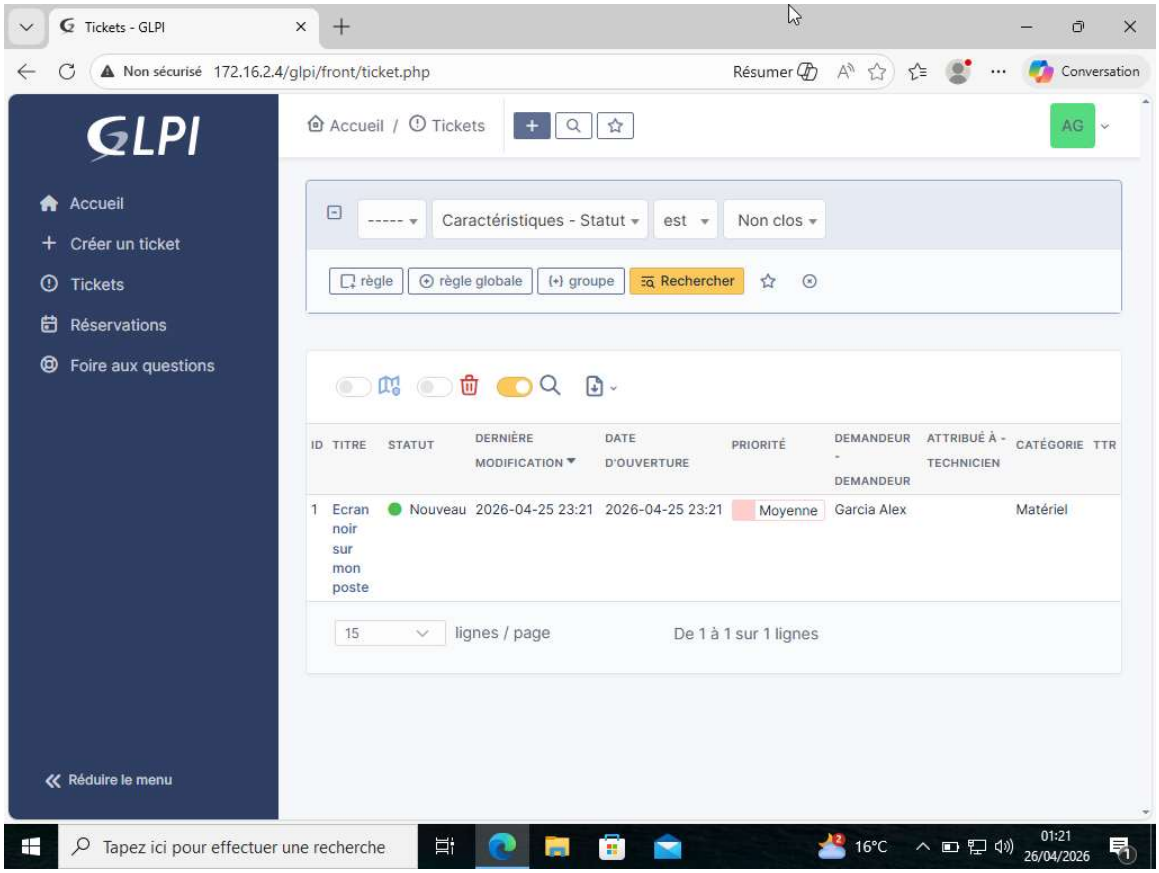


Figure 21 - Liste des tickets GLPI : incident “Écran noir sur mon poste”

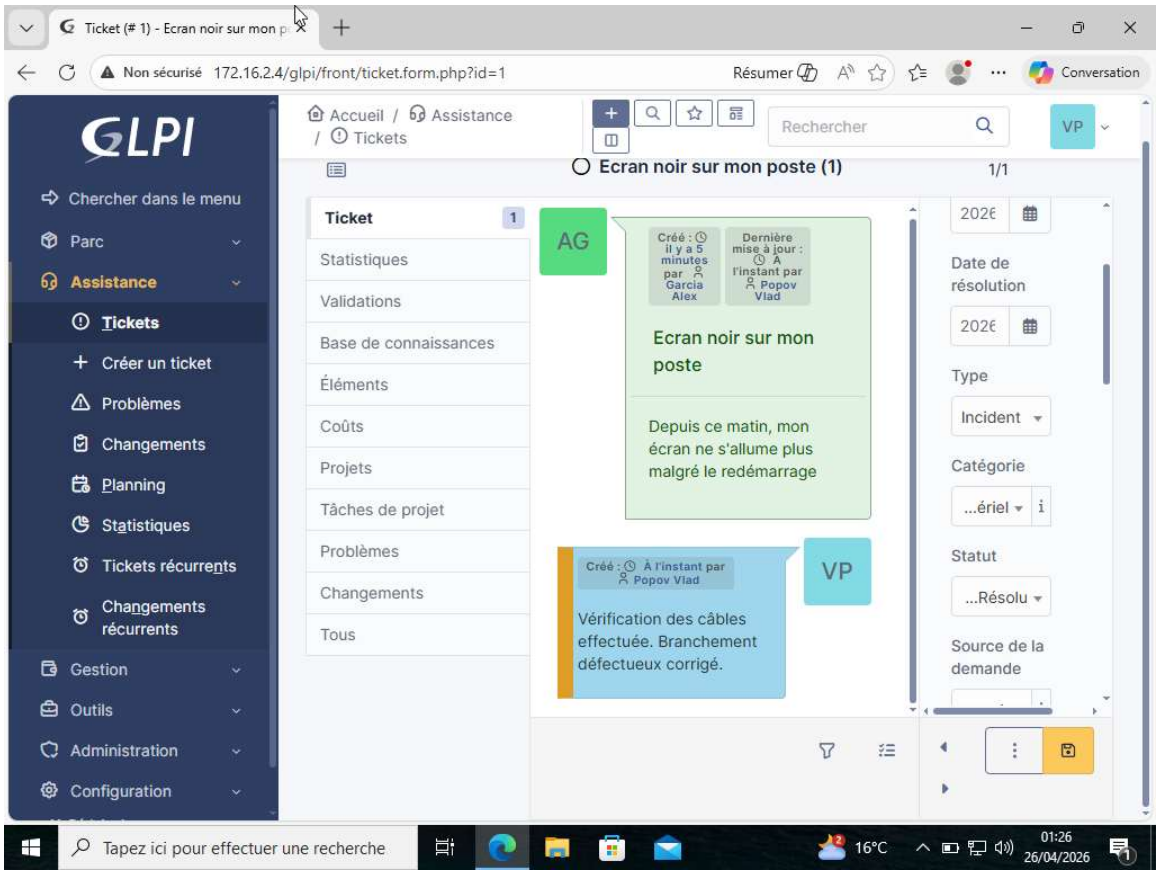


Figure 22 - Suivi du ticket GLPI et résolution indiquée

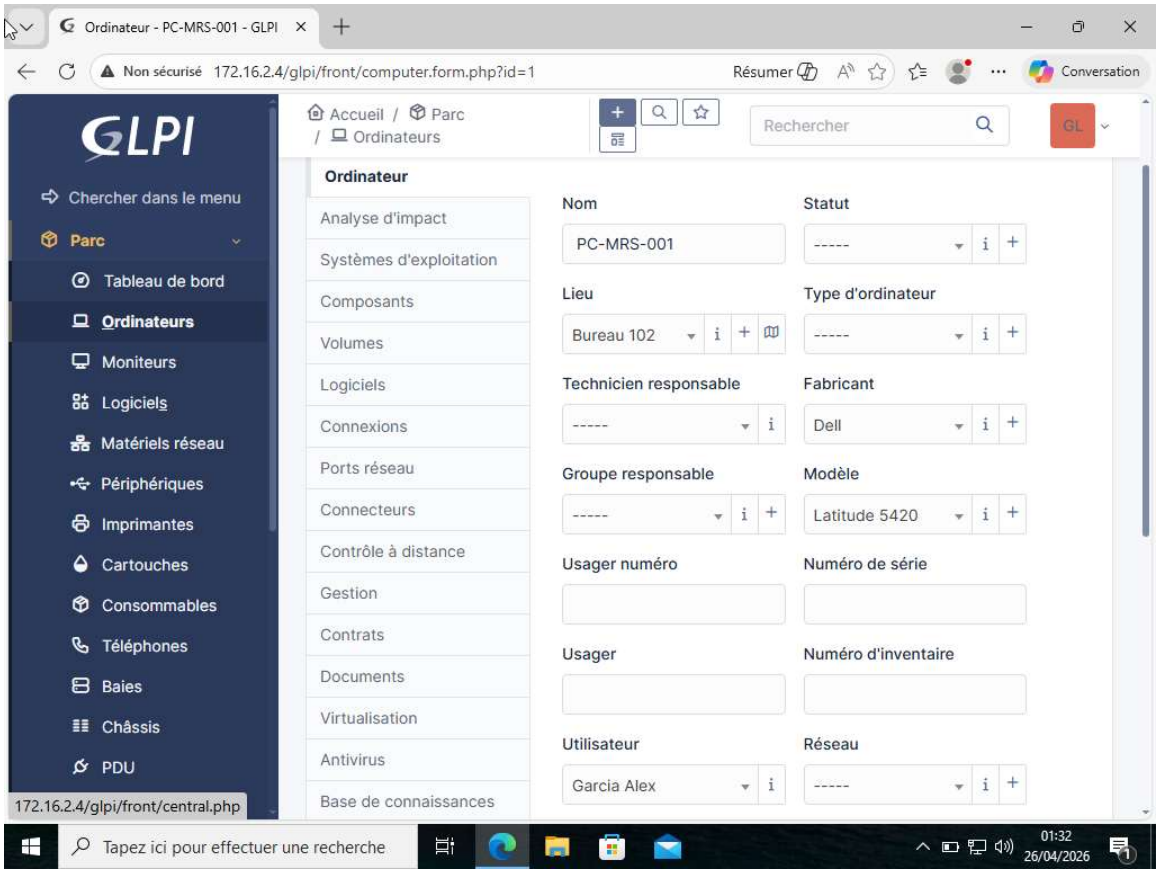


Figure 23 - Fiche ordinateur PC-MRS-001 dans le parc GLPI

7. Tests et validation

Les tests ci-dessous valident les principaux éléments de la maquette Marseille : connectivité, VPN, accès inter-réseaux, domaine et services métiers.

Élément testé	Méthode / preuve	Résultat
Connectivité WAN OPNsense	Ping vers 1.1.1.1 et google.com	Validé
Interfaces OPNsense	LAN 172.16.1.1, OPT1 172.16.2.1, WAN 10.31.0.2	Validé
VPN nomade	Interface VPN_admin en 10.9.0.10	Validé
Accès LAN collaborateurs	Ping 172.16.1.1 depuis le client	Validé
Accès LAN serveurs	Ping 172.16.2.1 depuis le client	Validé
Domaine Windows	Jonction au domaine vitapharmamrs.local	Validé
GLPI	Création et résolution d'un ticket test	Validé

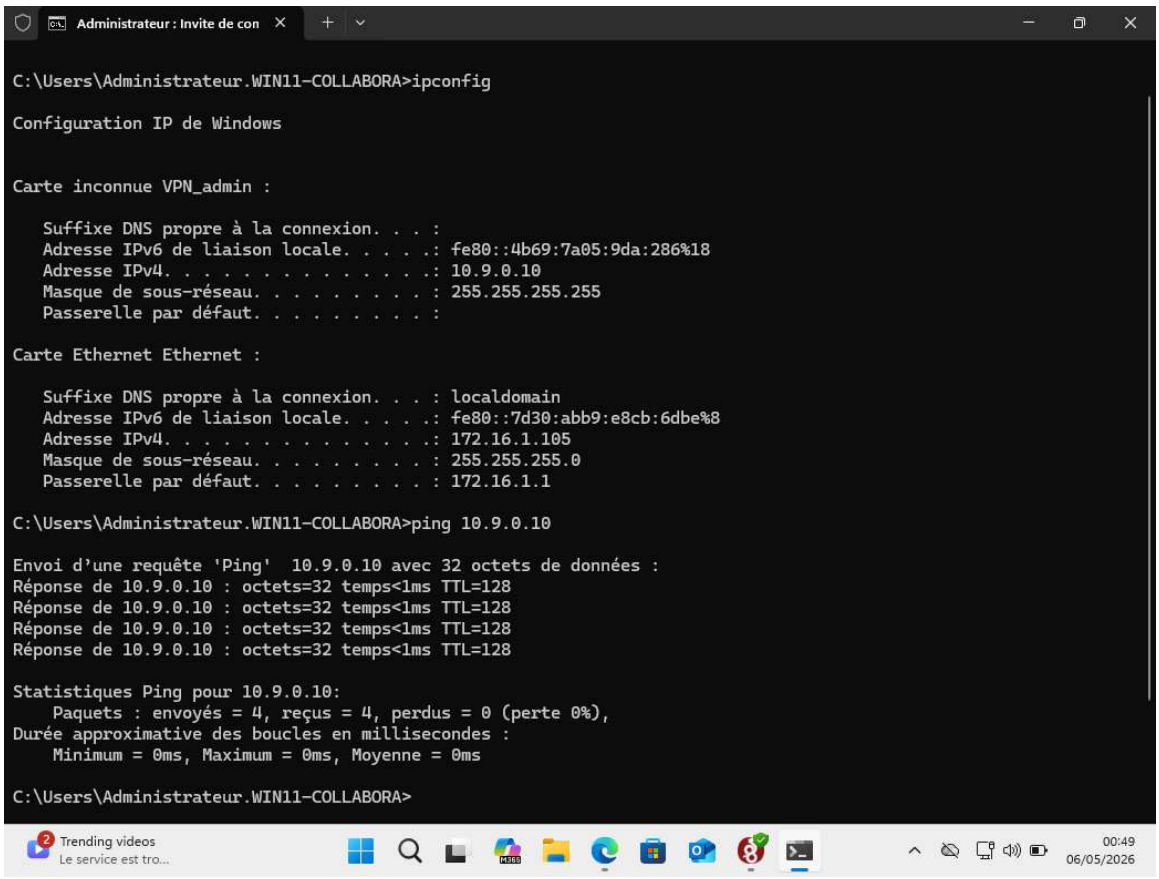


Figure 24 - Client Windows 11 : IP VPN 10.9.0.10 et ping local du tunnel

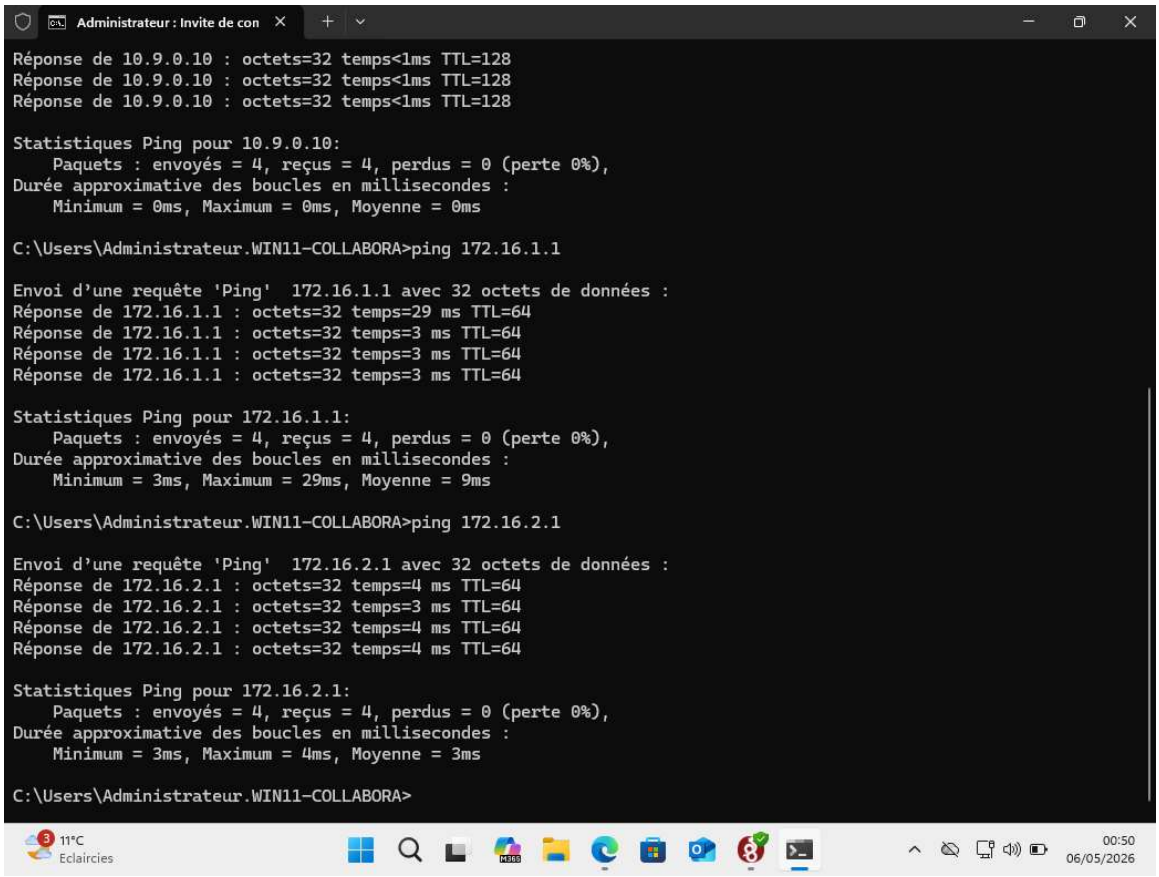


Figure 25 - Test de ping vers les passerelles 172.16.1.1 et 172.16.2.1

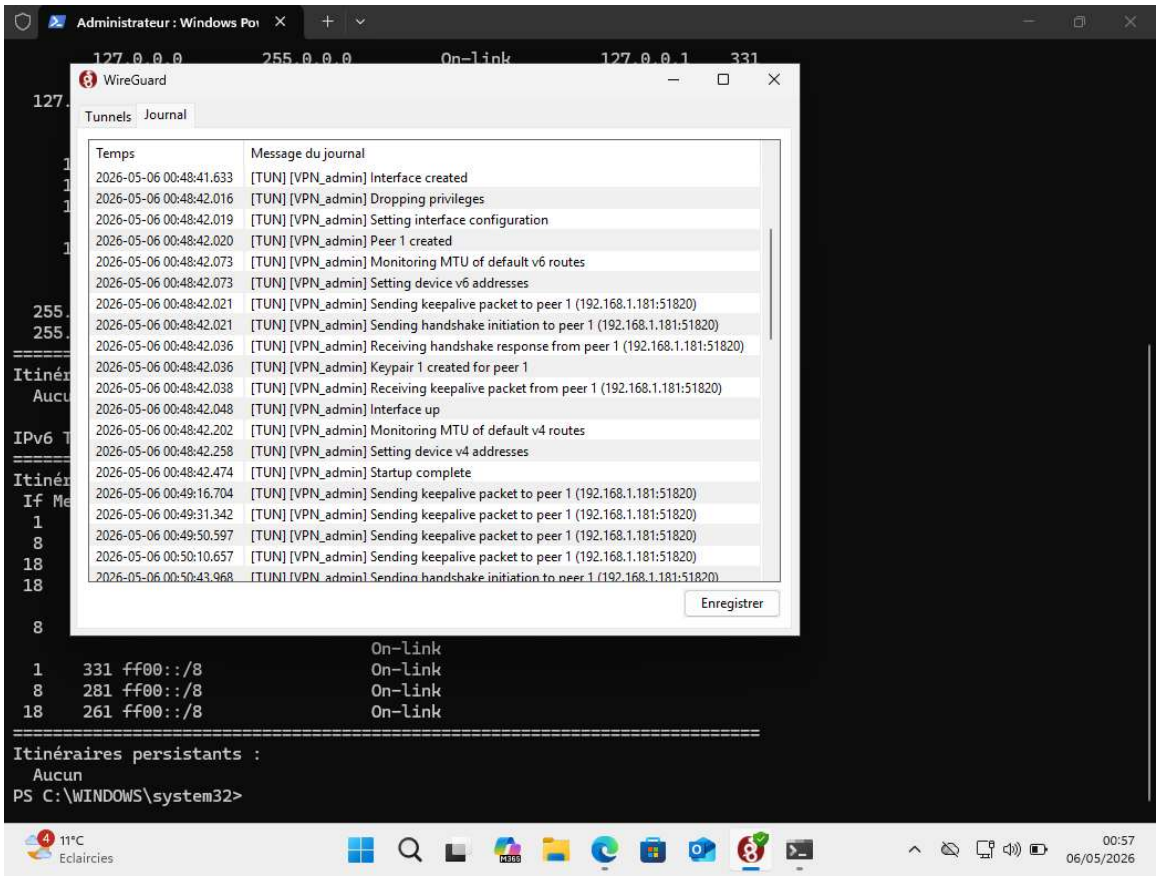


Figure 26 - Journal WireGuard : interface montée et handshake avec le pair

8. Exploitation et maintenance

8.1 Sauvegarde GLPI

Une sauvegarde de la base GLPI est déclenchée via un script Bash. La capture montre la présence de la base glpi et l'exécution du script backup_glpi.sh.

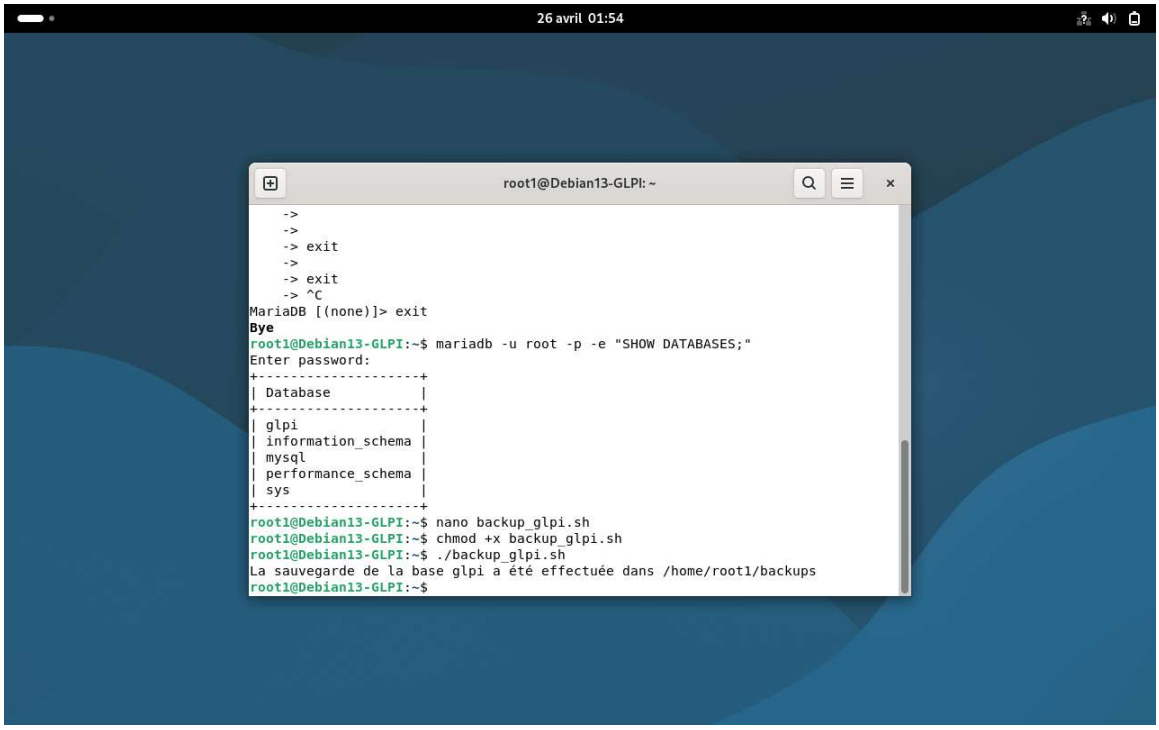


Figure 27 - Exécution du script de sauvegarde GLPI et confirmation de sauvegarde

8.2 Procédure d'exploitation GLPI

- Un utilisateur crée un ticket depuis GLPI.
- Le support qualifie l'incident et renseigne les informations utiles.
- Le technicien ajoute une réponse de résolution.
- Le ticket passe au statut résolu après traitement.

9. Sécurité et supervision

9.1 Supervision Prometheus

Prometheus est déployé sur Debian avec node_exporter. Les cibles sont visibles dans l'interface Prometheus et plusieurs requêtes permettent de suivre CPU, RAM et disque.

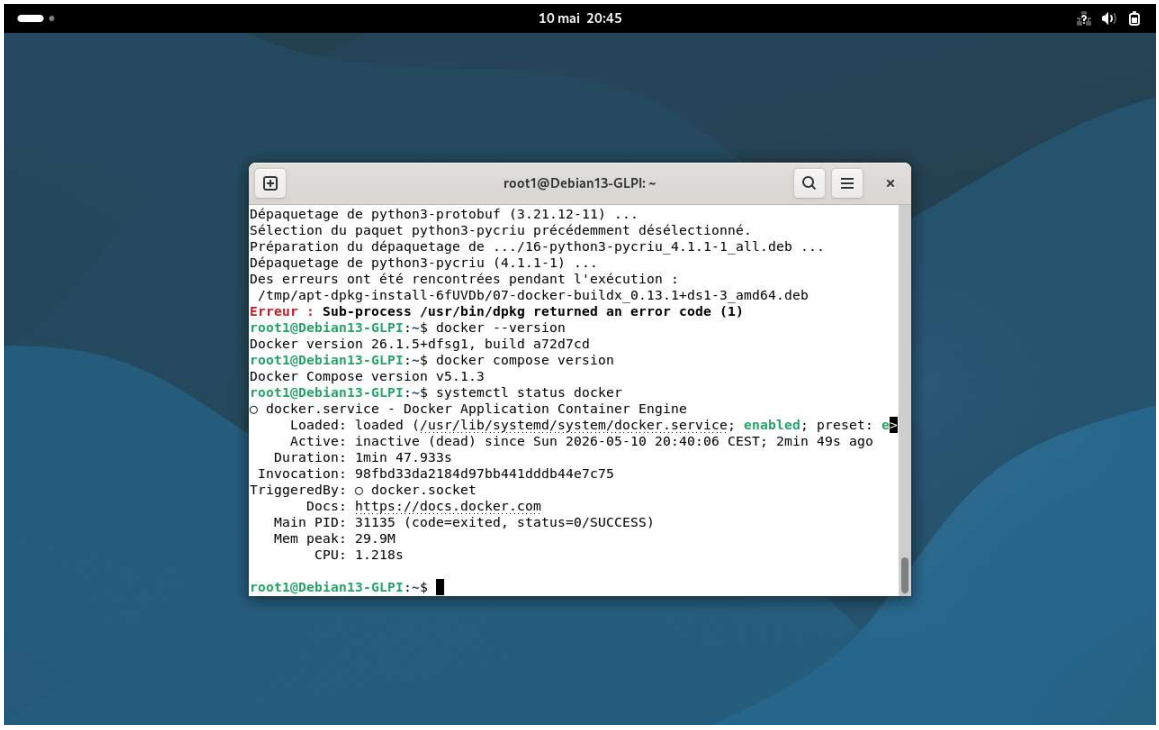


Figure 28 - Vérification Docker sur le serveur Debian

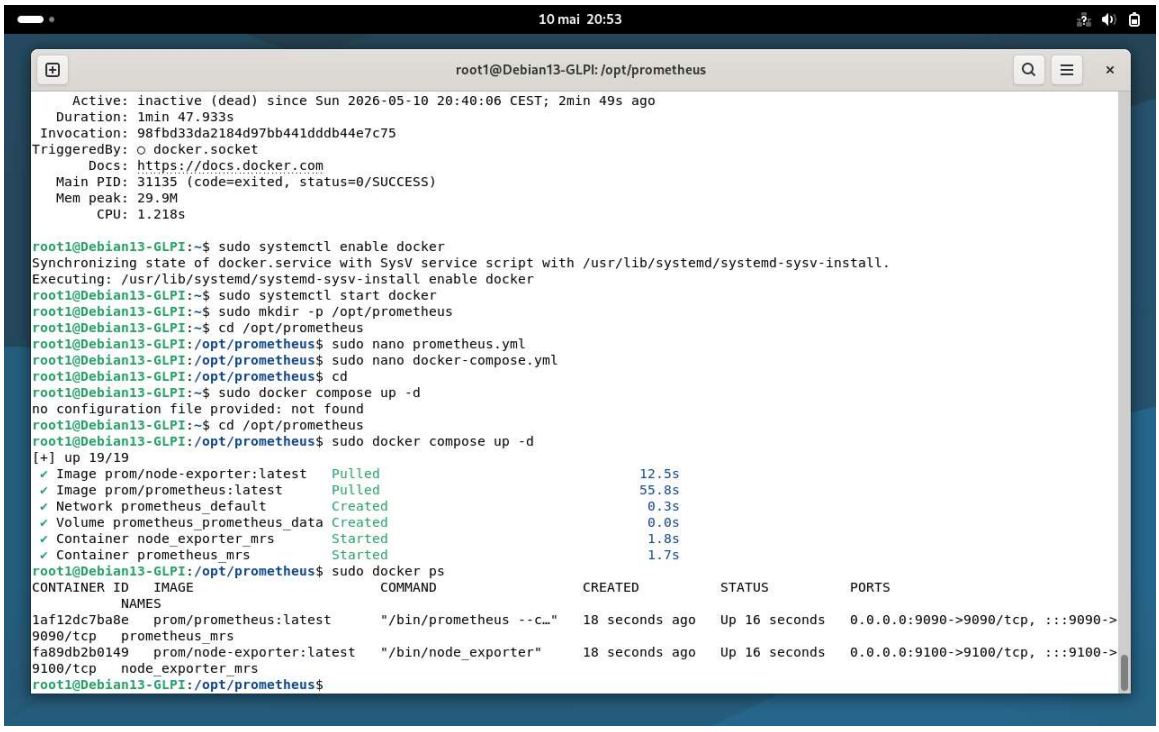


Figure 29 - Déploiement Prometheus et node_exporter avec Docker Compose

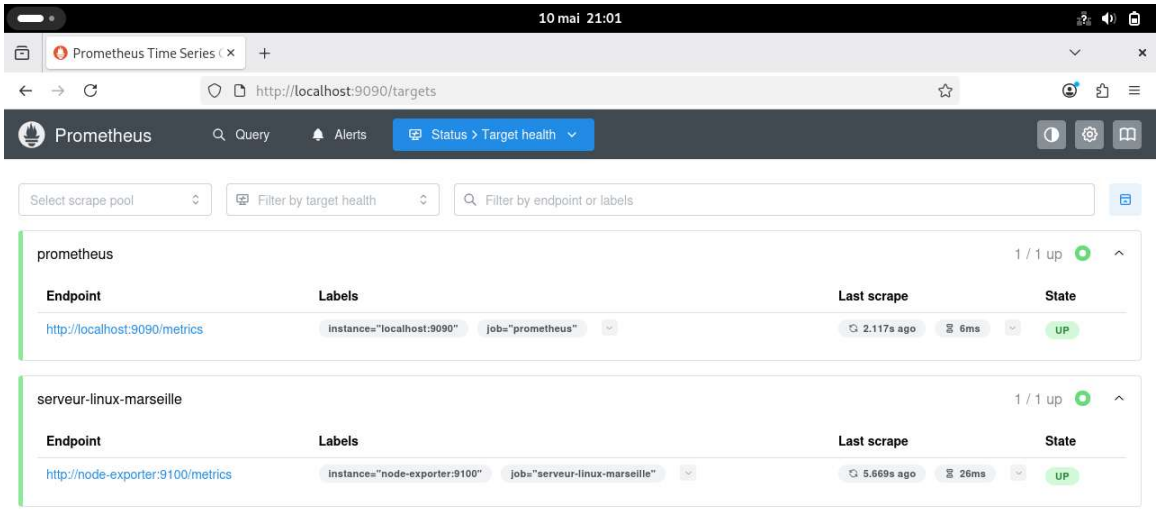


Figure 30 - Prometheus : cibles prometheus et serveur-linux-marseille à l'état UP

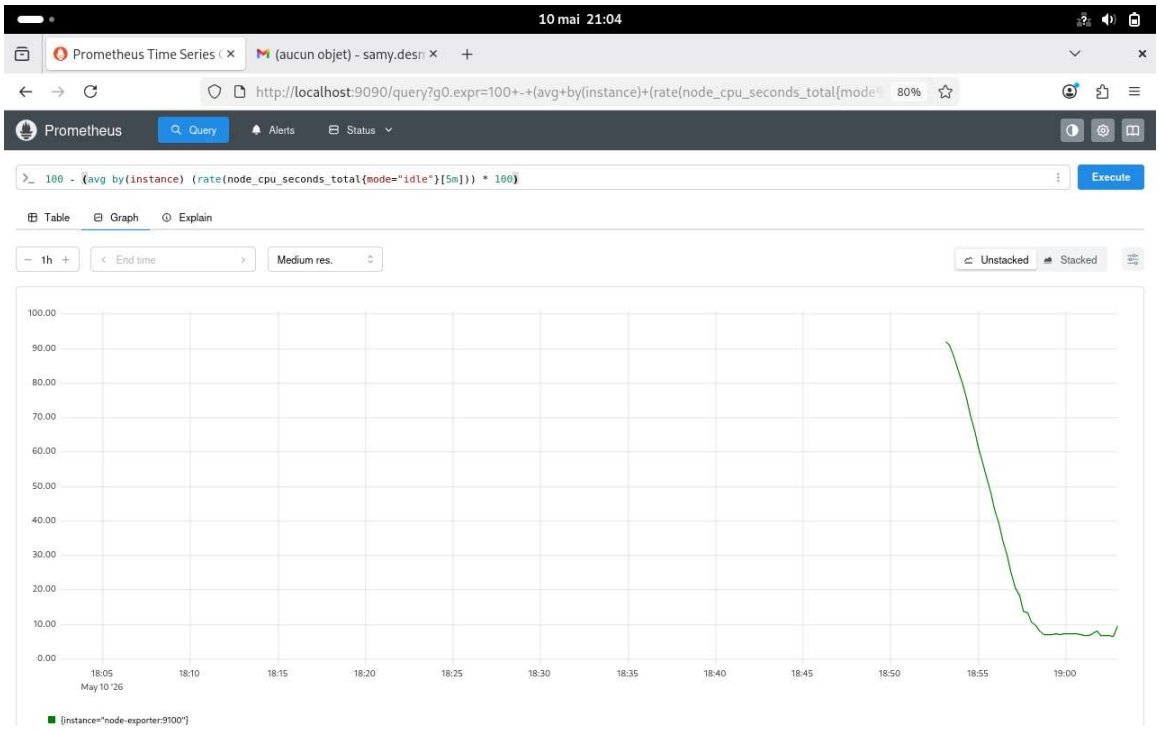


Figure 31 - Prometheus : suivi de l'usage CPU

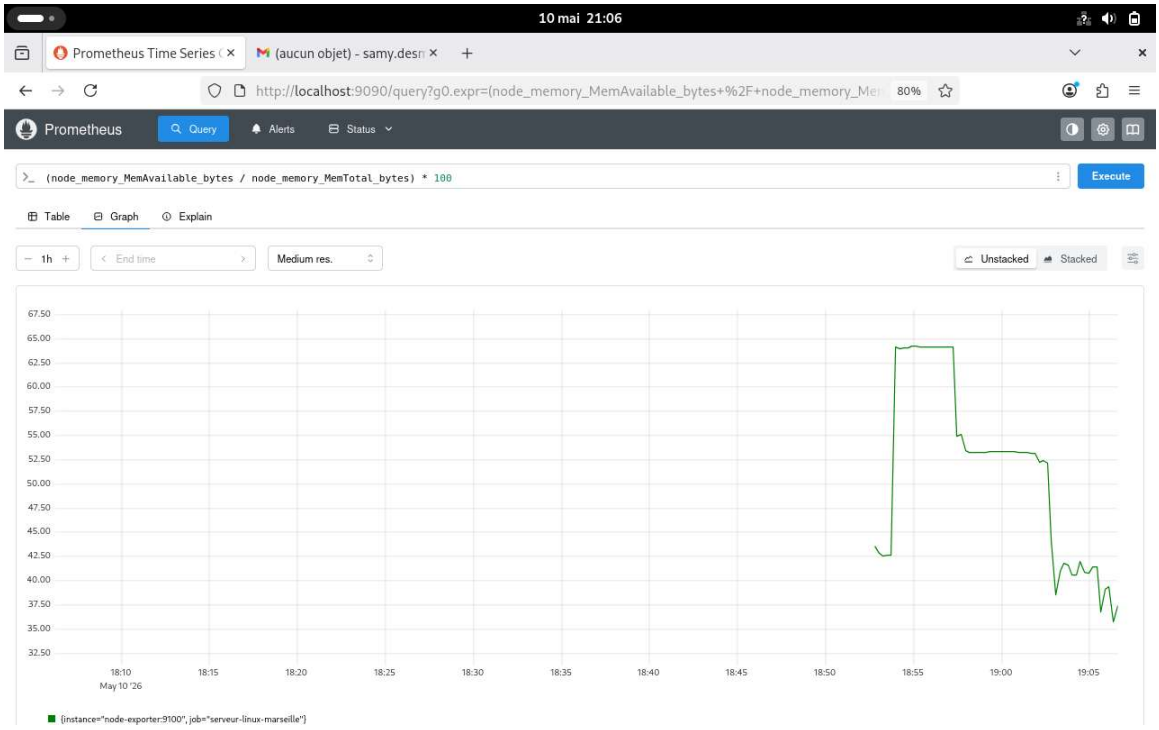


Figure 32 - Prometheus : suivi de l'usage mémoire

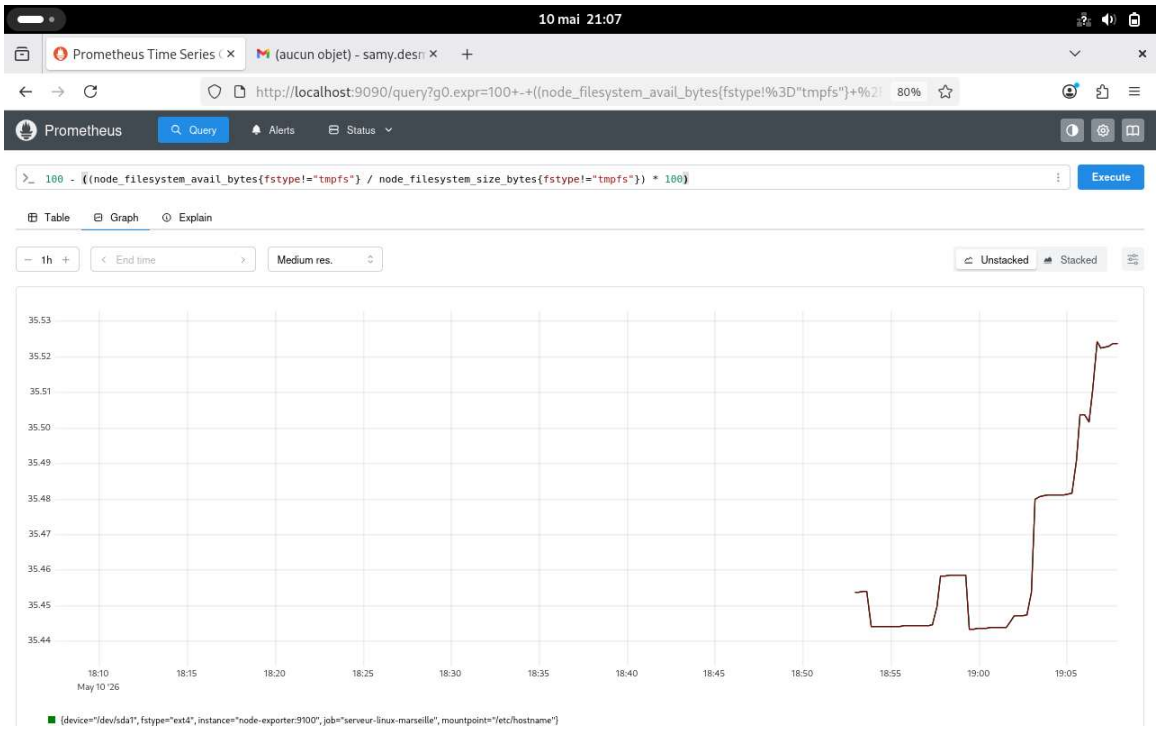


Figure 33 - Prometheus : suivi de l'espace disque disponible

9.2 Audit Active Directory avec PingCastle

PingCastle est utilisé pour obtenir une première lecture du risque Active Directory. Le score affiché sert de base à des recommandations de durcissement.

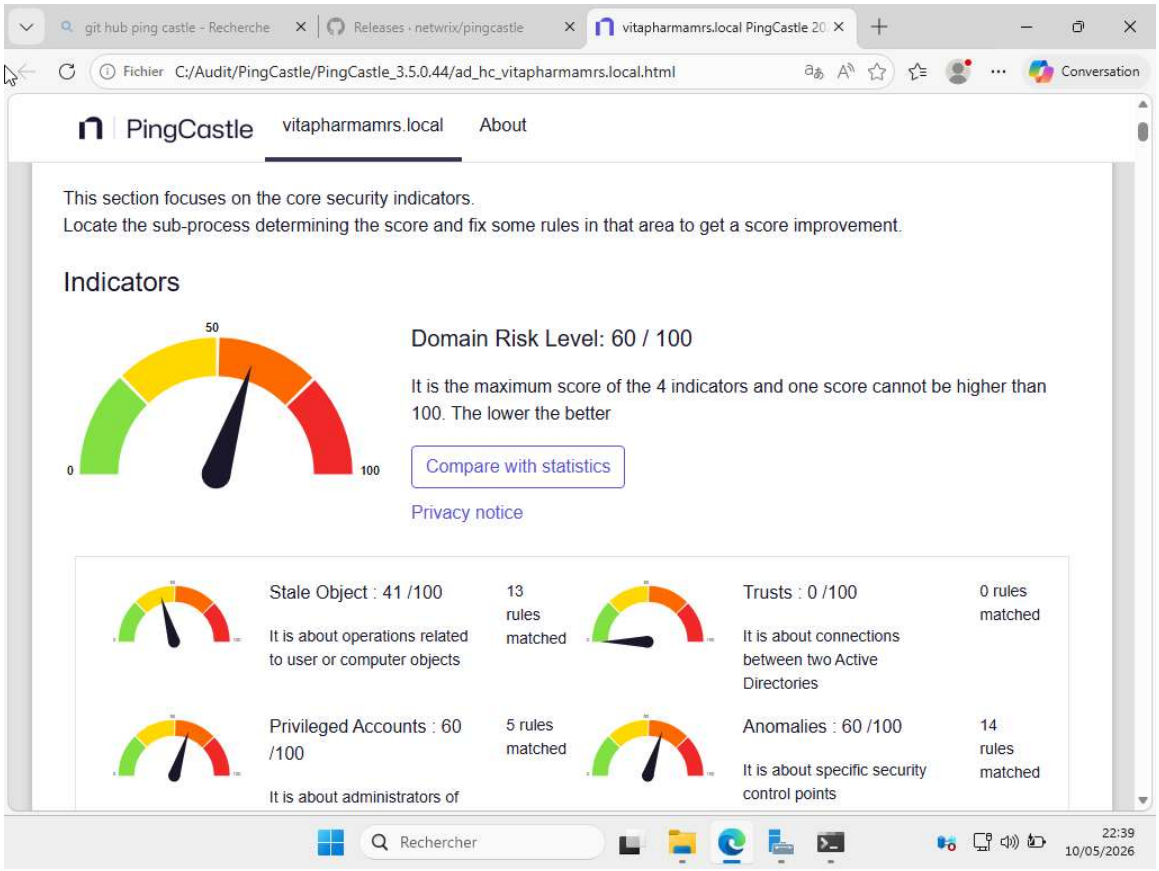


Figure 34 - PingCastle : niveau de risque du domaine vitapharmamrs.local

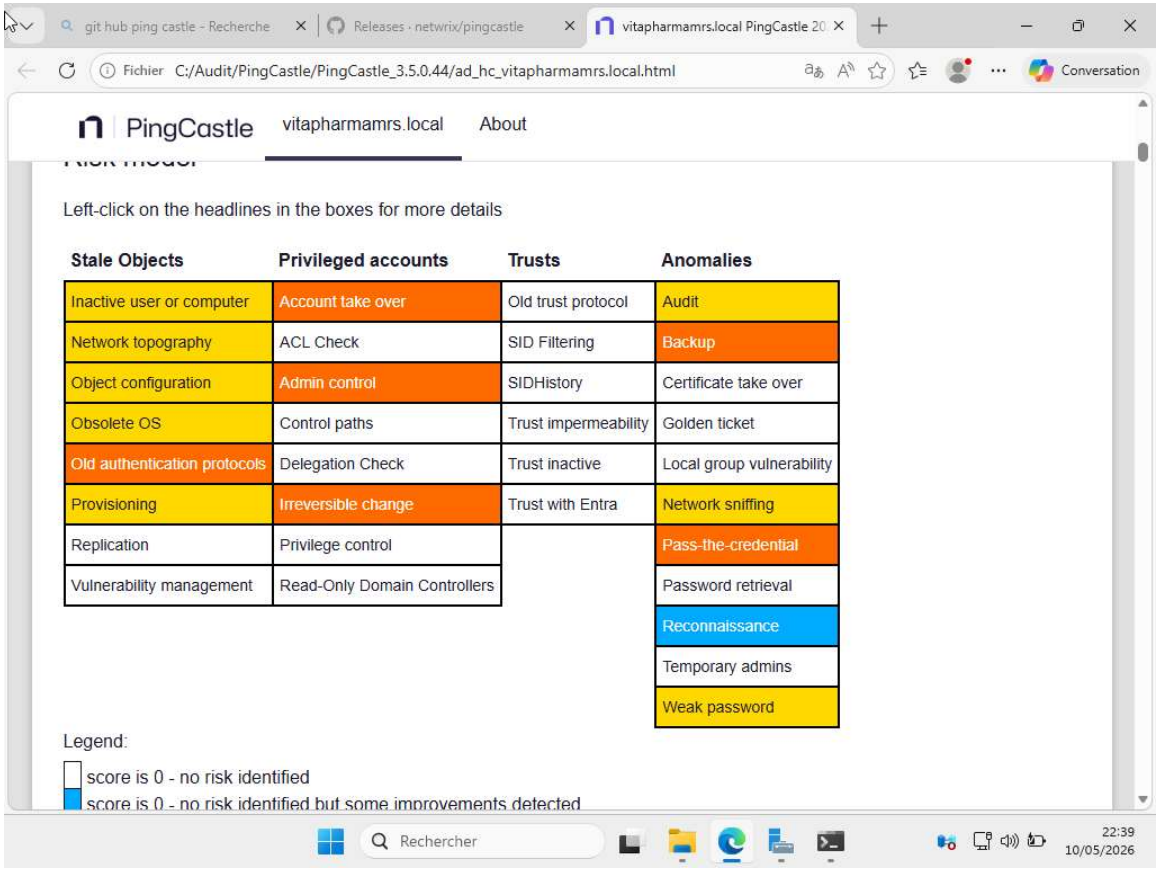


Figure 35 - PingCastle : catégories de risques identifiées

9.3 Audit Linux avec Lynis

Lynis est installé sur le serveur Debian afin d'obtenir des recommandations de durcissement Linux. Le rapport donne un hardening index et une liste d'actions correctives.

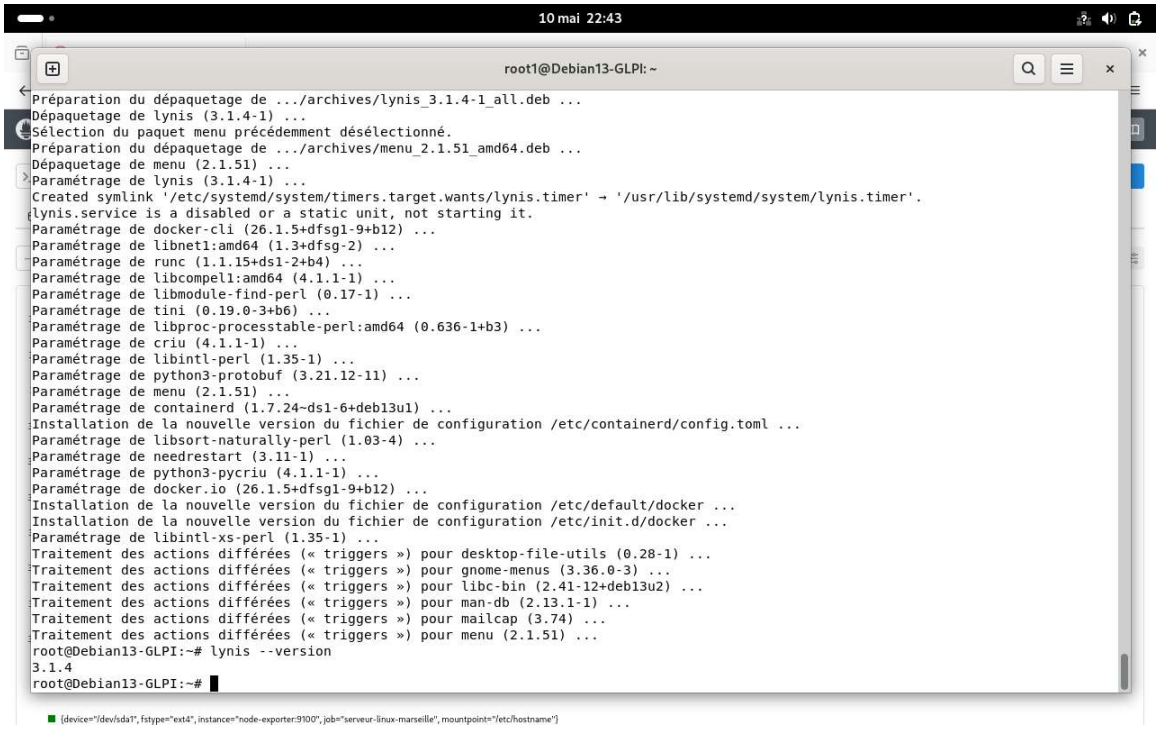


Figure 36 - Installation de Lynis et vérification de la version

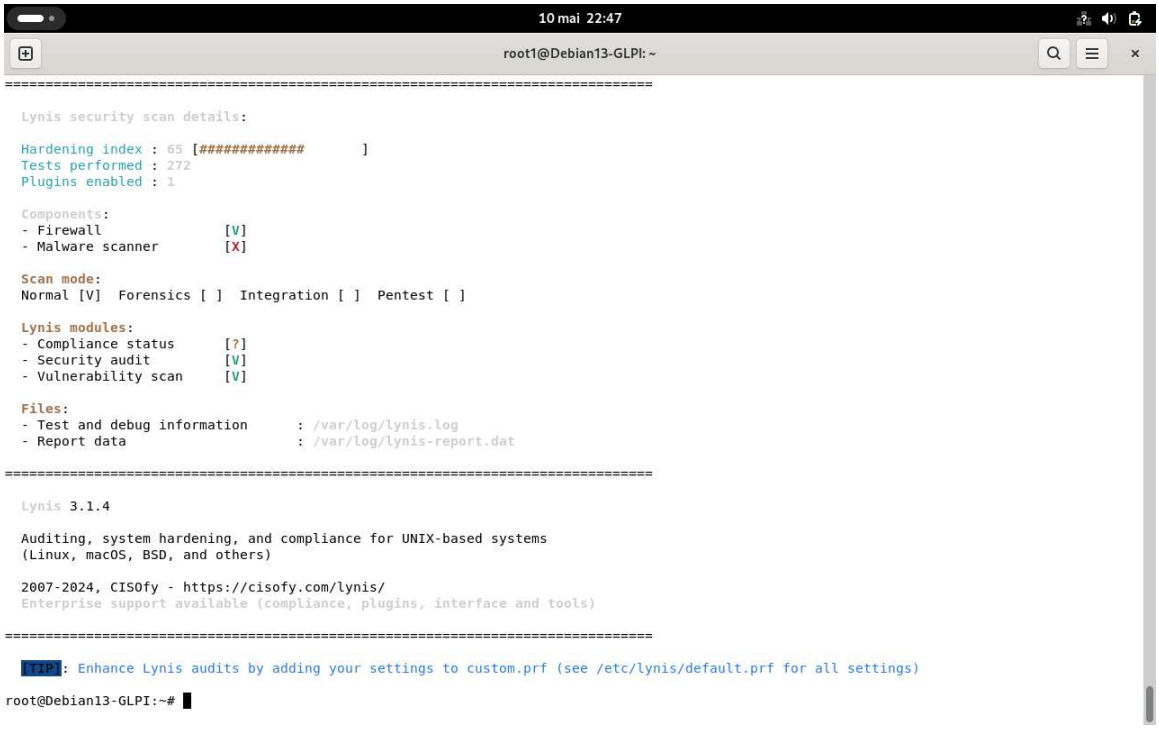


Figure 37 - Lynis : détails de l'audit et hardening index

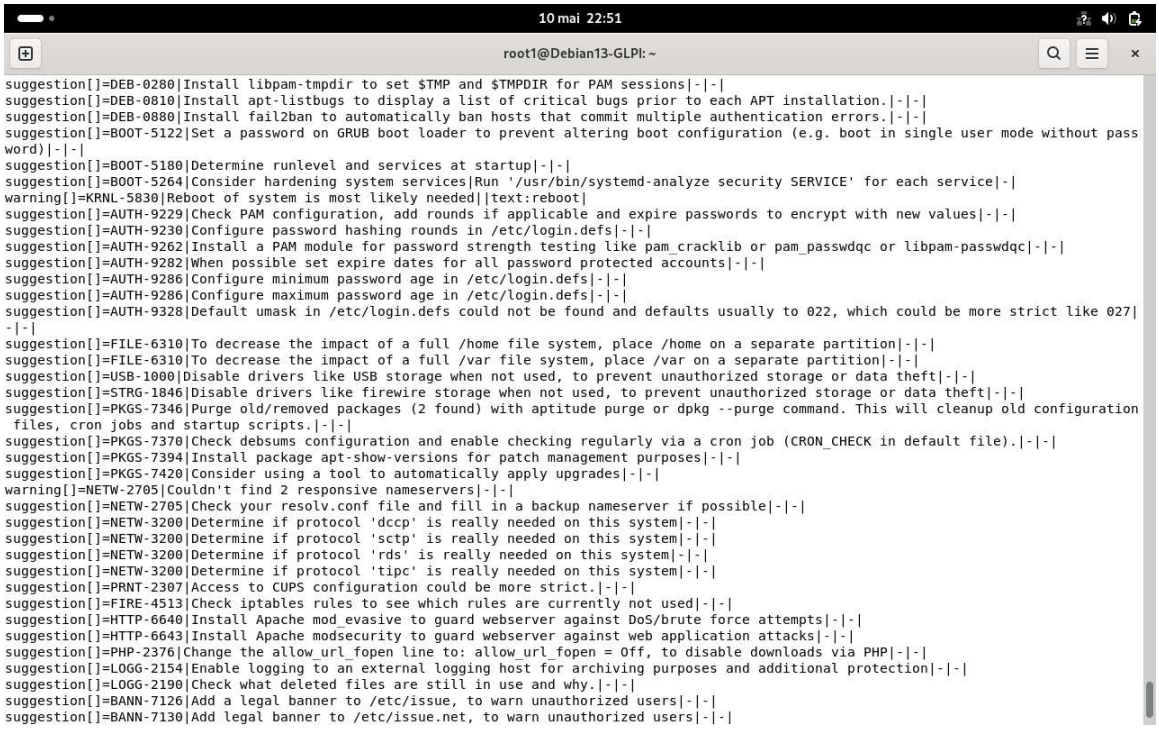


Figure 38 - Lynis : suggestions de durcissement système

Outil	Constat principal	Actions recommandées
PingCastle	Risque AD : stale objects, privileged accounts, anomalies	Nettoyer comptes inactifs, renforcer comptes admin, corriger les anomalies critiques
Lynis	Hardening index 65, nombreuses suggestions	Durcir SSH, journaux, mots de passe, permissions et services inutiles
Prometheus	Cibles UP, métriques CPU/RAM/disque visibles	Ajouter des seuils d'alerte et exporter les tableaux de bord

10. Conclusion et perspectives

Cette V1 documente la réalisation du site Marseille de Vita Big Pharma. La maquette couvre le socle réseau avec OPNsense, l'annuaire Active Directory, l'automatisation des comptes, l'accès VPN nomade, GLPI, une sauvegarde de la base GLPI, la supervision Prometheus et un premier audit de sécurité avec PingCastle et Lynis.

La documentation est volontairement centrée sur les éléments vérifiables par capture. Elle peut être complétée ensuite avec les captures manquantes si d'autres tâches sont finalisées dans la suite du projet.

Synthèse des éléments documentés

Domaine	Résultat documenté
Réseau	OPNsense installé, interfaces configurées, règles VPN ajoutées
Système Windows	Domaine AD fonctionnel, utilisateur et poste client intégrés
Automatisation	Création et classement des utilisateurs via CSV et script PowerShell
Services Linux	GLPI installé et utilisé pour un ticket test
Exploitation	Sauvegarde GLPI exécutée par script
Supervision / sécurité	Prometheus, PingCastle et Lynis utilisés comme preuves d'exploitation

Annexes

Annexe A - Extrait du fichier CSV Marseille

Prénom	Nom	Email	OU	Groupe
Alex	Garcia	garcia.alex@vitabigpharma.local	Support	SUP_N1
Imane	Bouazizi	bouazizi.imane@vitabigpharma.local	Support	SUP_N1
Lucas	Moretti	moretti.lucas@vitabigpharma.local	Support	SUP_N1
Youssef	Amine	amine.youssef@vitabigpharma.local	Support	SUP_N1
Sarah	Kim	kim.sarah@vitabigpharma.local	Support	SUP_N1
Diego	Ramirez	ramirez.diego@vitabigpharma.local	Support	SUP_N1
Anna	Kowalczyk	kowalczyk.anna@vitabigpharma.local	Support	SUP_N1
Bilal	Saidi	saidi.bilal@vitabigpharma.local	Support	SUP_N1
Mina	Park	park.mina@vitabigpharma.local	Support	SUP_N1
Romain	Petit	petit.romain@vitabigpharma.local	Support	SUP_N1
Noura	Hamdi	hamdi.noura@vitabigpharma.local	Support	SUP_N2
Julien	Bernardi	bernardi.julien@vitabigpharma.local	Support	SUP_N2

Annexe B - Exemple de script PowerShell utilisé

```
# Exemple de logique utilisée pour l'import CSV Marseille
$csvPath = "C:\Users\Administrateur\Desktop\users_marseille.csv"
$domainDN = "DC=vitapharmamrs,DC=local"
$groupPath = "OU=Groupes,$domainDN"
$groupes = @("SUP_N1", "SUP_N2", "SUP_N3")

foreach ($nomGroupe in $groupes) {
    if (-not (Get-ADGroup -Filter "Name -eq '$nomGroupe'")) {
        New-ADGroup -Name $nomGroupe -GroupScope Global -Path $groupPath
    }
}

Import-Csv $csvPath -Delimiter ',' | ForEach-Object {
    $samName = $_.Email.Split('@')[0]
    $targetOUName = $_.OU
    $nomGroupe = $_.Groupe
    $targetOUPath = "OU=$targetOUName,$domainDN"

    $user = Get-ADUser -Filter "SamAccountName -eq '$samName'" -ErrorAction SilentlyContinue
    if ($user) {
        Move-ADObject -Identity $user.DistinguishedName -TargetPath $targetOUPath
        Add-ADGroupMember -Identity $nomGroupe -Members $samName -ErrorAction SilentlyContinue
    }
}
```

Annexe C - Sources utilisées pour la V1

- Projet-2-IRIS2.docx : contexte, besoins et cahier des charges initial.

- Feuille de route.docx : ordre de structuration du dossier et tâches attendues.
- Capture_projet2.7z : captures utilisées comme preuves de réalisation.
- users_marseille.csv : jeu d'utilisateurs du site Marseille utilisé pour l'automatisation AD.
- vitaBigPharma-Claire.jpg : schéma logique de conception.