Projet BTS 2

Vita Big Pharma

Noms: **NDONGO TOVOR**

Prénoms : **Moïse Glory**

Classe BTS 2 SIO / Groupe 1

Année 2026

Table des matières

Présentation de l’entreprise

Vita Big Pharma est une entreprise du secteur Pharmaceutique spécialisée dans la fabrication et la commercialisation de compléments alimentaires. Son activité repose dur des exigences élevées en matière de qualité, et de traçabilité et de conformité réglementaire, propres au domaine de la santé.

Dans le cadre de son implémentation en France, l’entreprise souhaite s’implanter durablement en s’appuyant sur une organisation répartie sur deux sites distants.

Le site de Toulouse, qui constitue le siège administratif, regroupe les fonctions stratégiques et de gestion de l’entreprise, notamment la direction, les ressources humaines et le service financier. Ce site est au cœur des décisions et de la gouvernance de l’entreprise.

Le site de Marseille est dédié aux activités techniques et informatiques. Il accueille le service technique ainsi que les supports informatiques, chargé de l’exploitation, de la maintenance et de l’assistance aux utilisateurs sur l’ensemble des sites.

Afin d’accompagner cette entreprise multi-sites, Vita Big Pharma souhaite mettre en place une infrastructure informatique centralisée, sécurisée et évolutive, pour garantir la continuité de service, de faciliter le télétravail, avoir une assistance inter-sites efficace, et de permettre la supervision ainsi que l’audit de sécurité. Une attention particulière est également portée à la qualité de service réseau, notamment grâce à des mécanismes de Traffic Shaping pour les collaborateurs.

Analyse des besoins

Dans le cadre de son implantation en France, **Vita Big Pharma** adopte une organisation **multi-sites** avec un siège administratif à Toulouse et un site technique à Marseille. Cette répartition géographique impose la mise en place d'une **infrastructure informatique fiable, sécurisée et centralisée**, pour supporter les activités critiques de l'entreprise.

Les enjeux principaux sont :

Assurer la **continuité de service** des applications et des données.

Garantir la **sécurité des informations sensibles** (données RH, financières, techniques).

Permettre la **collaboration et l'assistance à distance** entre les deux sites.

Offrir une infrastructure **évolutive**, adaptée à la croissance future de l'entreprise.

	Sites	
	Marseille	**Toulouse**
Services	Technique	Direction
	Support Informatique	Ressource humaine
	----------	Finance

Besoins fonctionnels

Communication inter-sites

- Interconnexion sécurisée entre les sites de Toulouse et Marseille.
- Accès transparent aux ressources partagées (serveurs, applications, fichiers).
- Mise en place de VPN site à site pour garantir la confidentialité des échanges.

Accès utilisateurs et télétravail

- Accès distant sécurisé pour les collaborateurs en télétravail.
- Authentification centralisée des utilisateurs.
- Gestion des droits d'accès selon les services (Direction, RH, Finance, Technique, Support).

Services informatiques

- Centralisation des services essentiels :
    - Annuaire (ex : Active Directory).
    - Serveur de fichiers.
    - Serveur de sauvegarde.
    - Serveurs applicatifs.
- Disponibilité élevée des services critiques.

Support et assistance technique

- Possibilité pour le support informatique de Marseille d'intervenir à distance sur les postes et serveurs.
- Outils de prise en main et de supervision à distance.

Besoins techniques

Infrastructure réseau

- Segmentation du réseau par **VLAN** (par service).
- Mise en place de mécanismes de **Traffic Shaping** pour prioriser les flux critiques.

Sécurité

- Déploiement de **pare-feu OpnSense** sur chaque site.
- Filtrage des flux réseau.
- Journalisation des accès et des événements (logs).
- Protection contre les intrusions et les accès non autorisés.

Supervision et audit

- Outils de **supervision réseau et système** (disponibilité, performance).
- Suivi des tentatives d'accès et incidents de sécurité.
- Possibilité d'audit pour répondre aux bonnes pratiques et obligations réglementaires.

Outils métiers

- GLPI (ticketing, inventaire).
- Dolibarr (ERP).

Besoins organisationnels

- Centralisation de l'administration du système d'information.
- Documentation claire de l'infrastructure et des procédures.
- Mise en place de procédures de sauvegarde et de restauration.
- Plan de continuité et de reprise d'activité (PCA / PRA, à minima conceptuel).

Contraintes du projet

- Infrastructure conforme aux **bonnes pratiques informatiques**.
- Solution **évolutive** permettant l'ajout de nouveaux utilisateurs ou sites.
- Respect des contraintes de sécurité liées au secteur pharmaceutique.
- Maquette fonctionnelle reproductible dans un environnement pédagogique.

Contraintes juridiques

Le Respect du **RGPD**, est la principale contrainte juridique des organisations et entreprise présent sur le territoire Européen. Parmi ces contraintes, nous retenons :

- La gestion des comptes utilisateurs.
- La Journalisation.
- La limitation des accès.
- La sauvegarde et confidentialité des données.
- La politique de mot de passe renforcée.
- La traçabilité des actions administratives.

Étude de solutions

1. Objectifs de la solution

La solution proposée doit répondre aux besoins identifiés lors de l'analyse, à savoir :

- Interconnecter les deux sites distants de **Toulouse** et **Marseille**.
- Centraliser les services informatiques tout en assurant une haute disponibilité.
- Garantir la **sécurité des échanges et des données**.
- Permettre le **télétravail sécurisé**.
- Faciliter l'**administration, la supervision et l'assistance inter-sites**.
- Mettre en œuvre une **qualité de service réseau** adaptée aux usages métiers.

2. Principe général de la solution

La solution repose sur une **infrastructure informatique centralisée et sécurisée**, organisée autour :

D'un **site principal** (Toulouse) hébergeant les services critiques.

D'un **site secondaire** (Marseille) disposant d'un accès sécurisé aux ressources centrales.

D'une **interconnexion site à site**, garantissant la confidentialité et l'intégrité des flux.

D'une **segmentation réseau par VLAN** afin d'isoler les services et renforcer la sécurité.

Cette architecture permet une administration centralisée tout en assurant une continuité de service entre les deux sites.

3. Architecture réseau

Organisation multi-sites

Site de Toulouse (siège administratif)

- ✓ Hébergement des serveurs centraux (AD, fichiers, sauvegardes).
- ✓ Accès des services Direction, RH et Finance.
- ✓ Point central de l'infrastructure.

Site de Marseille (site technique)

- ✓ Postes du service technique et du support informatique.
- ✓ Accès aux ressources du site de Toulouse via VPN sécurisé.
- ✓ Support et maintenance à distance.

Interconnexion inter-sites

- ✓ Mise en place d'un **VPN site à site chiffré**.
- ✓ Tunnel permanent entre les pares-feux des deux sites.
- ✓ Sécurisation des échanges sur le réseau public (Internet).
- ✓ Transparence pour les utilisateurs (accès identique à un réseau local).

Plan d'adressage IP

- Utilisation d'adresses IP privées (RFC 1918).
- Adresse dynamique avec Protocol DHCP.
- Routage inter-VLAN assuré par un équipement de niveau 3 (pare-feu OpnSens).

5. Services informatiques déployés

Le déploiement des services suivants :

- **Annuaire Active Directory** :
  - Gestion centralisée des utilisateurs et des groupes.
  - Authentification unique sur le réseau.
- **DNS / DHCP** :
  - Résolution de noms interne.

    - Attribution automatique des adresses IP.
- **Serveur de fichiers** :
    - Stockage centralisé.
    - Droits d’accès par service.
- **Serveur de sauvegarde** :
    - Sauvegarde régulière des données critiques.
    - Possibilité de restauration en cas d’incident.
- **Outils de supervision** :
    - Surveillance des équipements et services avec Prometheus.
    - Alertes en cas de panne ou de surcharge.

6. Sécurité de la solution

La sécurité est un élément central de la solution retenue :

- Déploiement de **pare-feu** sur chaque site.
- Mise en place d’un **VPN nomade** pour le télétravail.
- Journalisation des accès et événements.
- Limitation des droits utilisateurs selon le principe du **moindre privilège**.

7. Qualité de service (QoS / Traffic Shaping)

Afin de garantir une bonne qualité de service pour les utilisateurs :

- Priorisation des flux critiques (administration, accès serveurs).
- Limitation de la bande passante pour les usages non prioritaires.
- Amélioration des performances globales du réseau collaborateur.

8. Avantages de la solution proposée

- **Sécurité renforcée** des données et des échanges.
- **Centralisation** de l'administration et des services.
- **Évolutivité** : ajout facile de nouveaux utilisateurs ou sites.
- **Continuité de service** assurée.
- **Facilité d'exploitation** et de supervision.

9. Limites et évolutions possibles

- Ajout de redondance matérielle (haute disponibilité).
- Mise en place d'un PRA / PCA plus avancé.
- Extension à de nouveaux sites ou services cloud.

Solutions techniques retenues

Solutions Retenues	Solutions Alternatives	Avantages	Inconvénient
OPNsense	Ffsense	Sécurisation et filtrage du réseau.	
Active Directory /DNS.		Solution complète	
Dolibarr		Simple à utiliser	
Prometheus	Centreon	Supervision pousser serveur	

- ✓ **OPNSense (pare-feu, VPN, Traffic Shaping).**
- ✓ **Active Directory / DNS.**
- ✓ **GLPI, Dolibarr.**
- ✓ **Prometheus.**

Cahier de charges Techniques

1. Objectifs du projet

Les principaux objectifs du projet sont les suivants :

- Mettre en place une infrastructure réseau reliant les deux sites distants.
- Centraliser les services informatiques de l'entreprise.
- Assurer la sécurité des données et des communications.
- Permettre l'accès distant sécurisé pour le télétravail.
- Faciliter l'administration et la maintenance du système informatique.
- Mettre en place un système de supervision du réseau.
- Garantir la qualité de service grâce à la gestion des flux réseau (Traffic Shaping).
- Concevoir une solution évolutive et conforme aux bonnes pratiques.

2. Périmètre du projet

Le projet concerne les deux sites de l'entreprise :

Site de Toulouse (siège administratif)

Ce site comprend :

- La direction
- Le service des ressources humaines
- Le service financier
- Les serveurs principaux

Site de Marseille (site technique)

Ce site comprend :

- Le service technique
- Le support informatique
- Les postes utilisateurs techniques

3. Contraintes

Contraintes techniques

- Utilisation d'adresses IP privées
- Architecture évolutive
- Compatibilité avec les environnements professionnels

Contraintes de sécurité

- Respect des bonnes pratiques de sécurité informatique
- Protection contre les accès non autorisés

Contraintes pédagogiques

- La solution devra être maquettée dans un environnement de simulation ou virtualisation (ex : Packet Tracer, GNS3, VMware, VirtualBox).

4. Plan d'adressage IP

L'infrastructure devra utiliser des adresses IP privées conformément à la norme RFC 1918.
Chaque site disposera d'un plan d'adressage structuré et segmenté par VLAN.

Site de Toulouse (Siège administratif)

Plage réseau principale : **192.168.1.0/24**

LAB Serveur	**Services**	**Ip adresse**	**Passerelle**
Windows serveur GUI	AD, DNS	192.168.1.0/24	192.168.1.1/24
Windows Core			
Debian (Dolibarr)	Dolibarr, Prometheus		
Backup	Backup		
LAB Collaborateur	**Services**	**Ip adresse**	**Passerelle**
Windows client	Utilisateur	192.168.10.0/24	192.168.10.1/24

Site de Marseille (Site technique)

Plage réseau principale : **172.16.1.0/24**

LAB Serveur	**Services**	**Ip adresse**	**Passerelle**
Windows serveur GUI	AD, DNS	172.16.1.0/24	172.16.1.1/24
Windows Core			
Debian (GLPI)	GLPI, Prometheus		
Backup	Backup		
LAB Collaborateur	**Services**	**Ip adresse**	**Passerelle**
Windows client	Utilisateur	172.16.2.0/24	172.16.2.1/24

Interconnexion inter-sites

Un tunnel VPN site à site sera mis en place entre les deux pares-feux via Internet.

Réseaux autorisés à travers le VPN :

- 192.168.1.0/24
- 172.16.1.0/24

5. Nommage des serveurs

Une convention de nommage normalisée devra être respectée afin de faciliter l'administration et la supervision.

Codes sites :

- TLS = Toulouse
- MRS = Marseille

Types de serveurs :

- DC = Domain Controller
- FS = File Serveur
- DHCP = Serveur DHCP
- DNS = Serveur DNS
- BCK = Backup
- SUP = Supervision

6. Domaine Active Directory

Un domaine Active Directory unique sera mis en place afin de centraliser l'authentification et la gestion des ressources.

Nom de domaine interne :

vbpharma.local

Architecture retenue :

- 1 forêt
- 1 domaine
- Contrôleur de domaine principal à Toulouse
- Contrôleur de domaine secondaire à Marseille (réplication AD)

Organisation des unités d'organisation (OU) :

- OU_Toulouse
- OU_Marseille
- OU_Direction
- OU_RH

- OU_Finance
- OU_Technique
- OU_Support

7. Services par site

Site de Toulouse (Site principal)

Services hébergés :

- Contrôleur de domaine principal (AD DS)
- Serveur DNS principal
- Serveur de fichiers
- Serveur de sauvegarde

Ce site constitue le centre névralgique de l'infrastructure.

Site de Marseille (Site secondaire)

Services hébergés :

- Contrôleur de domaine secondaire
- DNS secondaire
- Outil de supervision réseau
- Outil d'assistance à distance

Le site de Marseille assurera également le support informatique global.

8. Traffic Shaping – Limitation de débit LAN Collaborateurs

Afin de garantir la qualité de service et d'éviter la saturation du réseau, un mécanisme de Traffic Shaping est mis en place sur les pares-feux ou routeurs.

Exigence :

Le débit du LAN Collaborateurs devra être limité à :

5 Mb/s

Objectifs :

- Prioriser les flux critiques (administration, serveurs, VPN).

- Éviter la saturation du lien Internet.
- Garantir des performances stables pour les services métiers.
- Empêcher les usages non professionnels de monopoliser la bande passante.

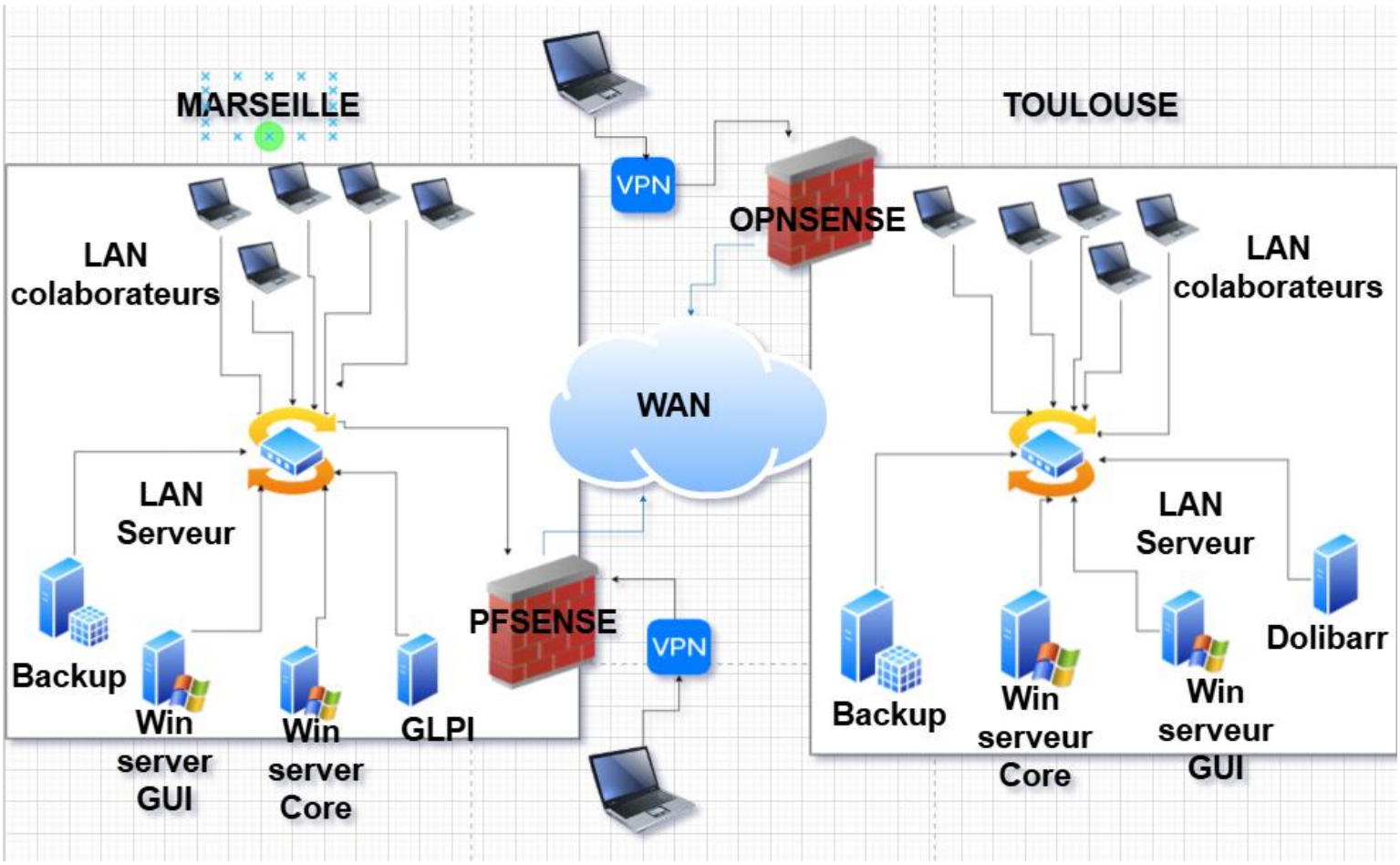
La politique de QoS devra distinguer :

- Flux prioritaires (serveurs, AD, sauvegardes).
- Flux standards (navigation utilisateurs).
- Flux limités (réseau collaborateurs).

Synthèse des exigences techniques

Élément	**Exigence**
Plan IP	Segmentation par VLAN, plages distinctes par site
Domaine AD	1 forêt, 1 domaine, réplication multi-site
Serveurs	Nommage normalisé par site
Services	Centralisation à Toulouse, redondance à Marseille
Traffic Shaping	Limitation LAN Collaborateurs à 5 Mb/s

Architecture technique



LAN SERVER	IP & MASQUE
Opnsense	10.0.250.62
Windows GUI	192.168.1.9/24
Windows core	192.168.1.90/24
Dolibarr	192.168.1.30/24
Backup	192.168.1.20/24
LAN COLABORATEUR	**IP & MASQUE**
Windows client	192.168.10.0/24

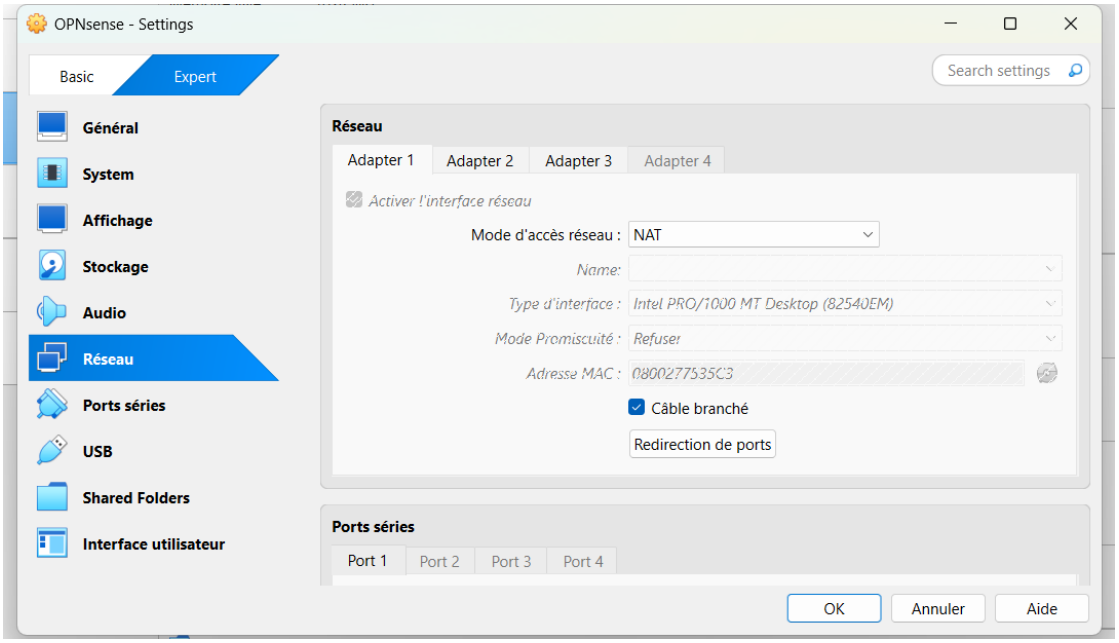
Mise en œuvre

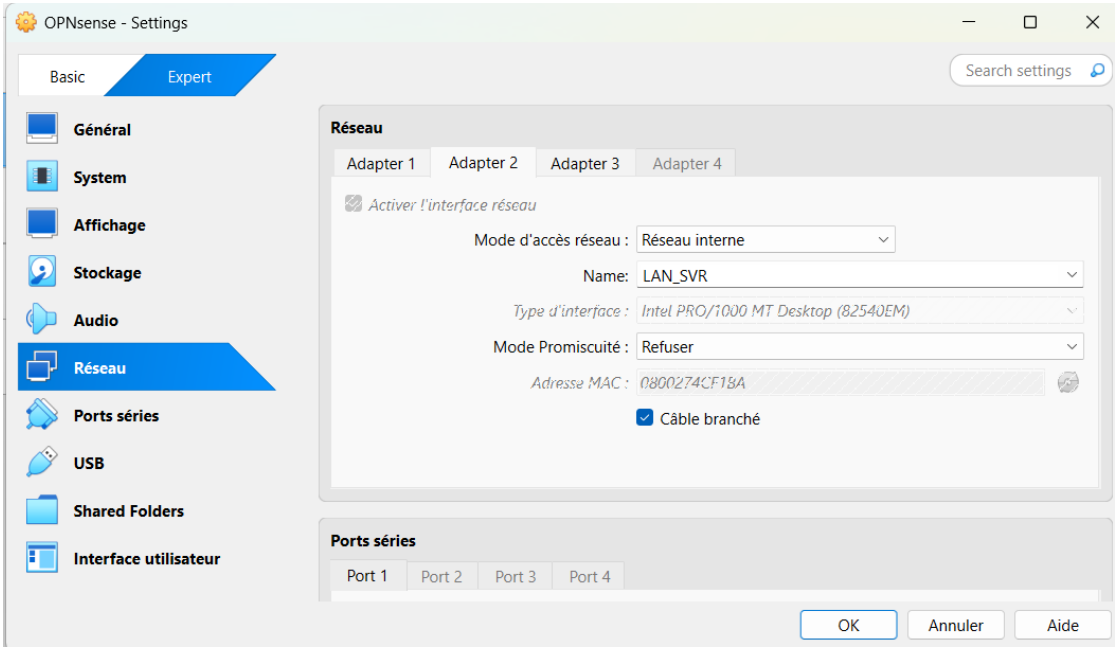
Installation et configuration des Machines Virtuelles, et déploiement des services

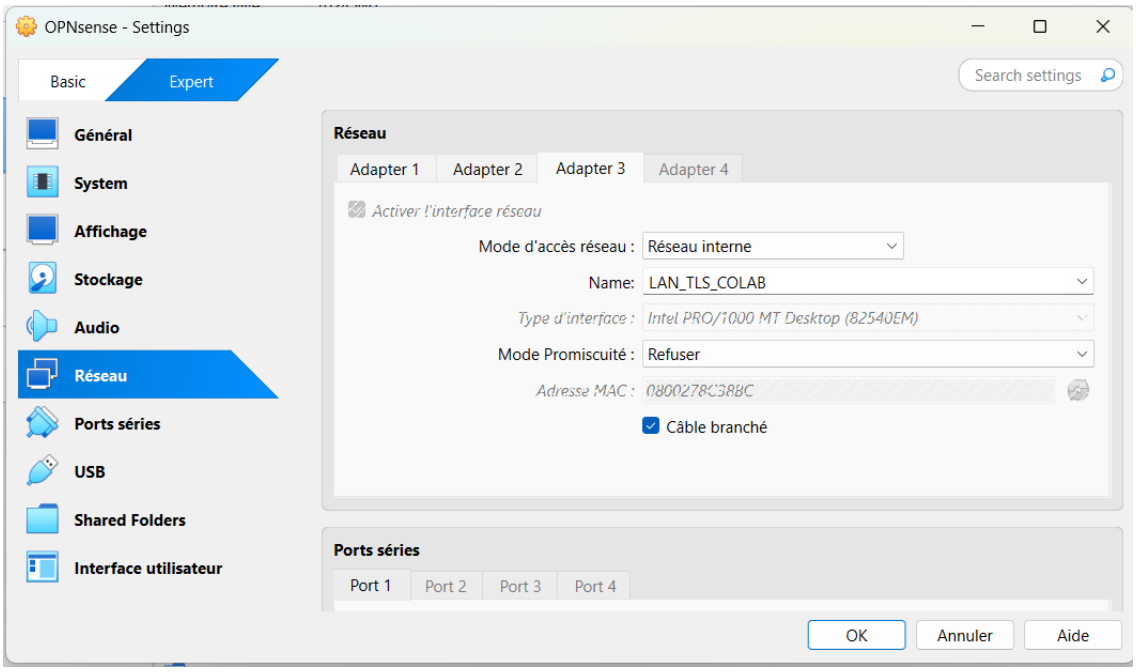
Installation et configuration du Firewall OPNsense :

J'ai téléchargé l'iso Opnsense sur le site officiel. En suite j'ai créé la machine virtuelle dans VirtualBox.

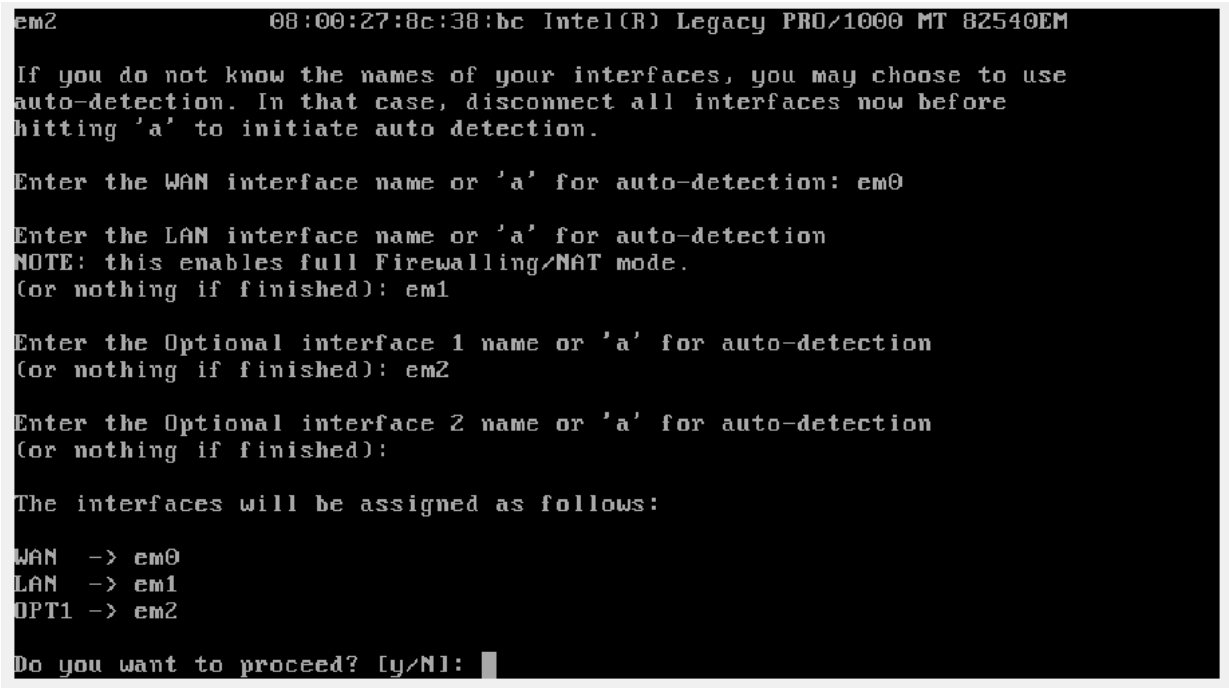
J'ai faire les configurations de base, comme la configuration des interfaces réseaux de la VM

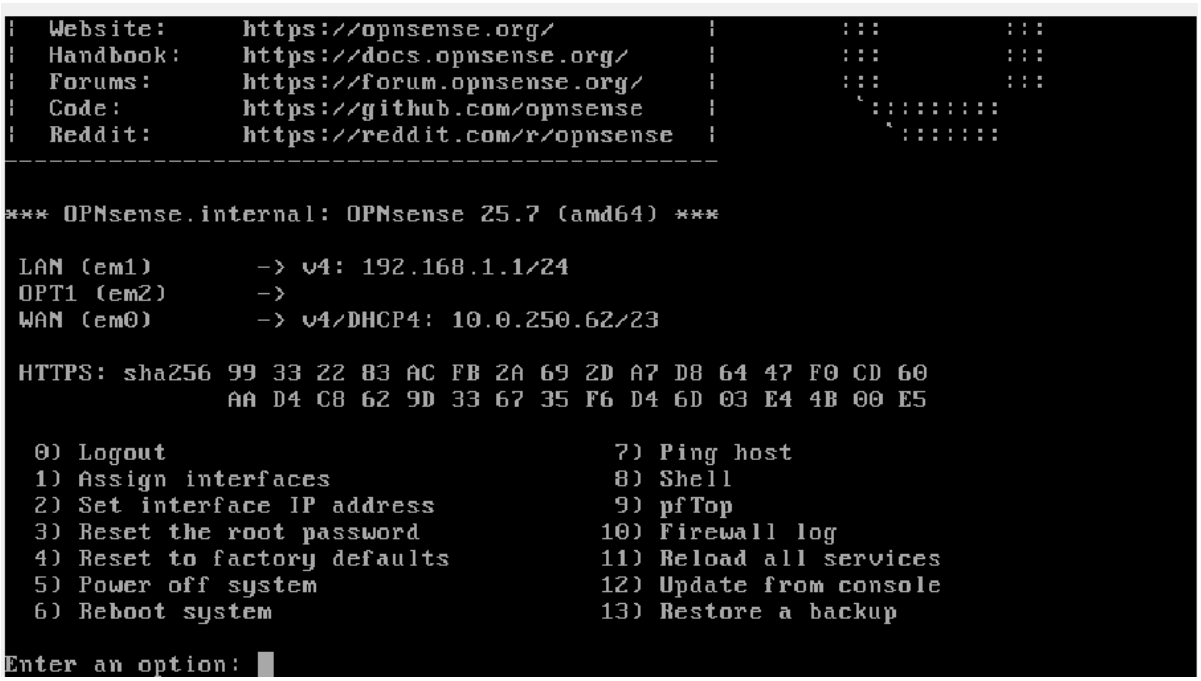



OPNsense - Settings
Basic
Expert
Search settings
Général
System
Affichage
Stockage
Audio
Réseau
Ports séries
USB
Shared Folders
Interface utilisateur
Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Mode d'accès réseau :
Réseau interne
Name:
LAN_SVR
Type d'interface :
Intel PRO/1000 MT Desktop (82540EM)
Mode Promiscuité :
Refuser
Adresse MAC :
0800274CF18A
Câble branché
Ports séries
Port 1
Port 2
Port 3
Port 4
OK
Annuler
Aide


OPNsense - Settings
Basic
Expert
Search settings
Général
System
Affichage
Stockage
Audio
Réseau
Ports séries
USB
Shared Folders
Interface utilisateur
Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Mode d'accès réseau :
Réseau interne
Name:
LAN_TLS_COLAB
Type d'interface :
Intel PRO/1000 MT Desktop (82540EM)
Mode Promiscuité :
Refuser
Adresse MAC :
Câble branché
Ports séries
Port 1
Port 2
Port 3
Port 4
OK
Annuler
Aide

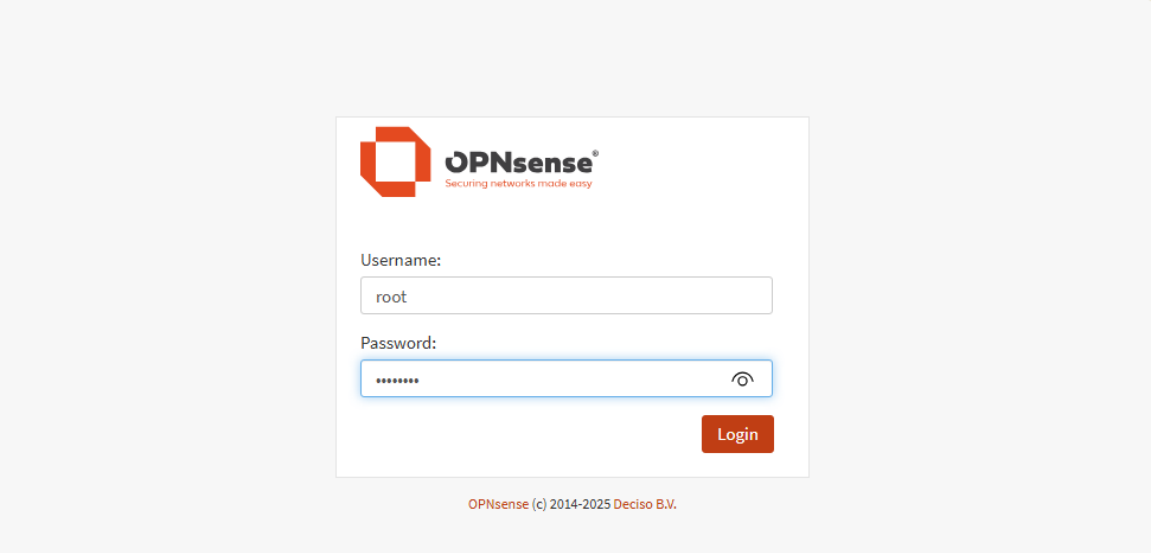
1. Assigner les interfaces en ligne de commande opnsense

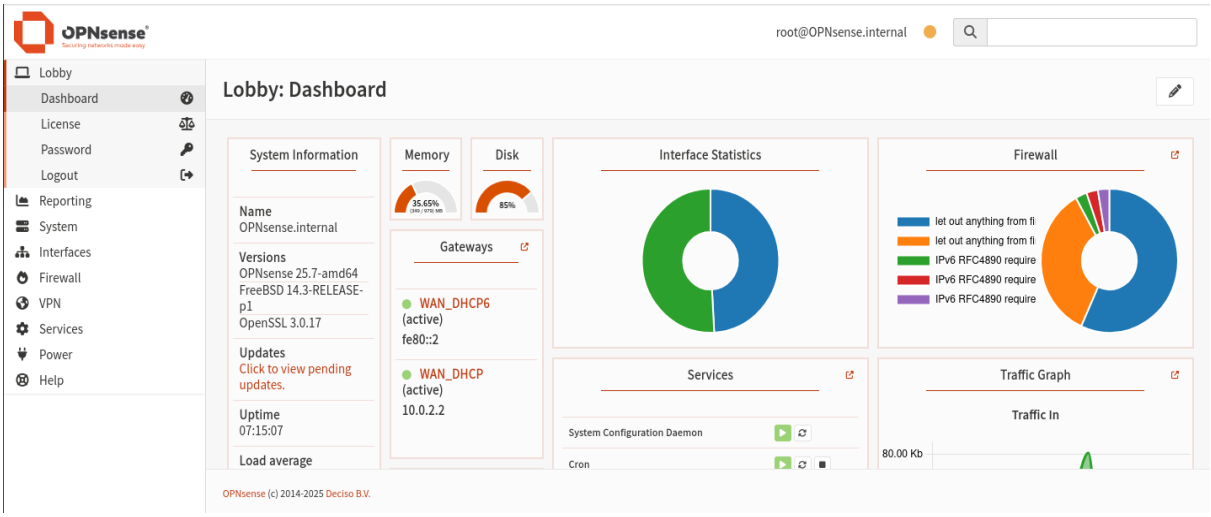




2. Accéder à l'interface web de l'opnsense dans le navigateur via :

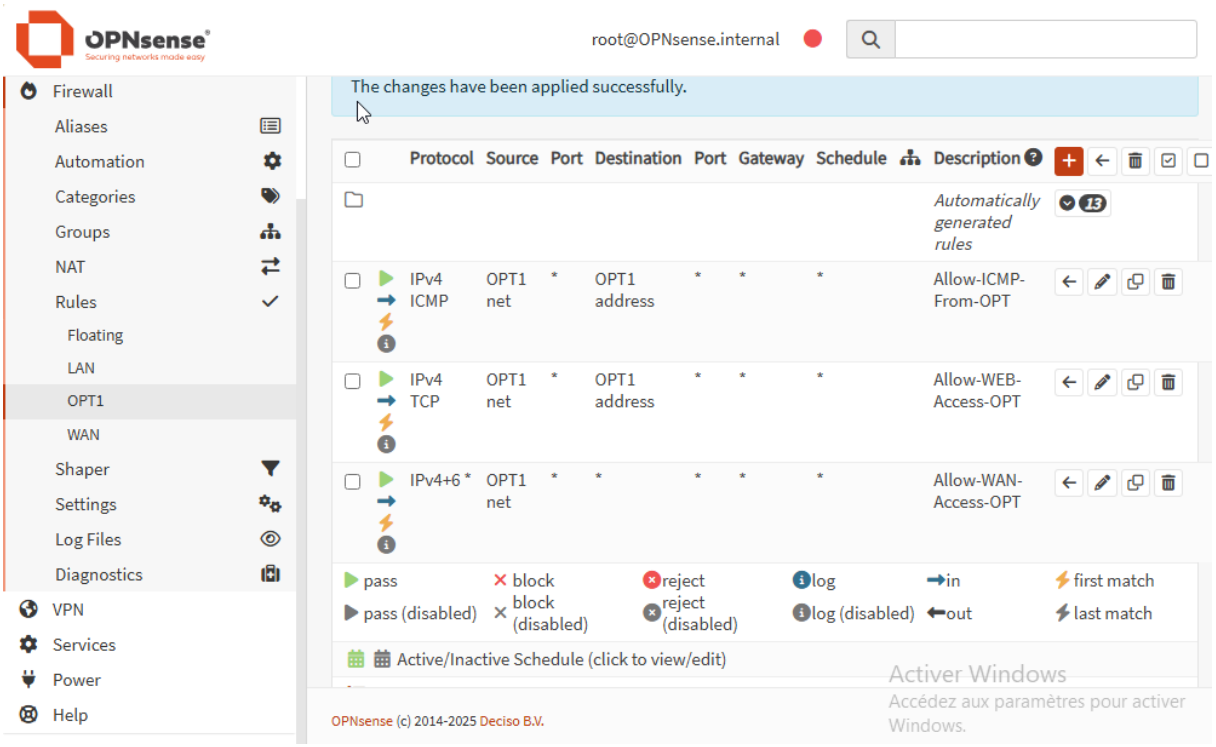
https:// l'adresse_de_la_machine_opnsense





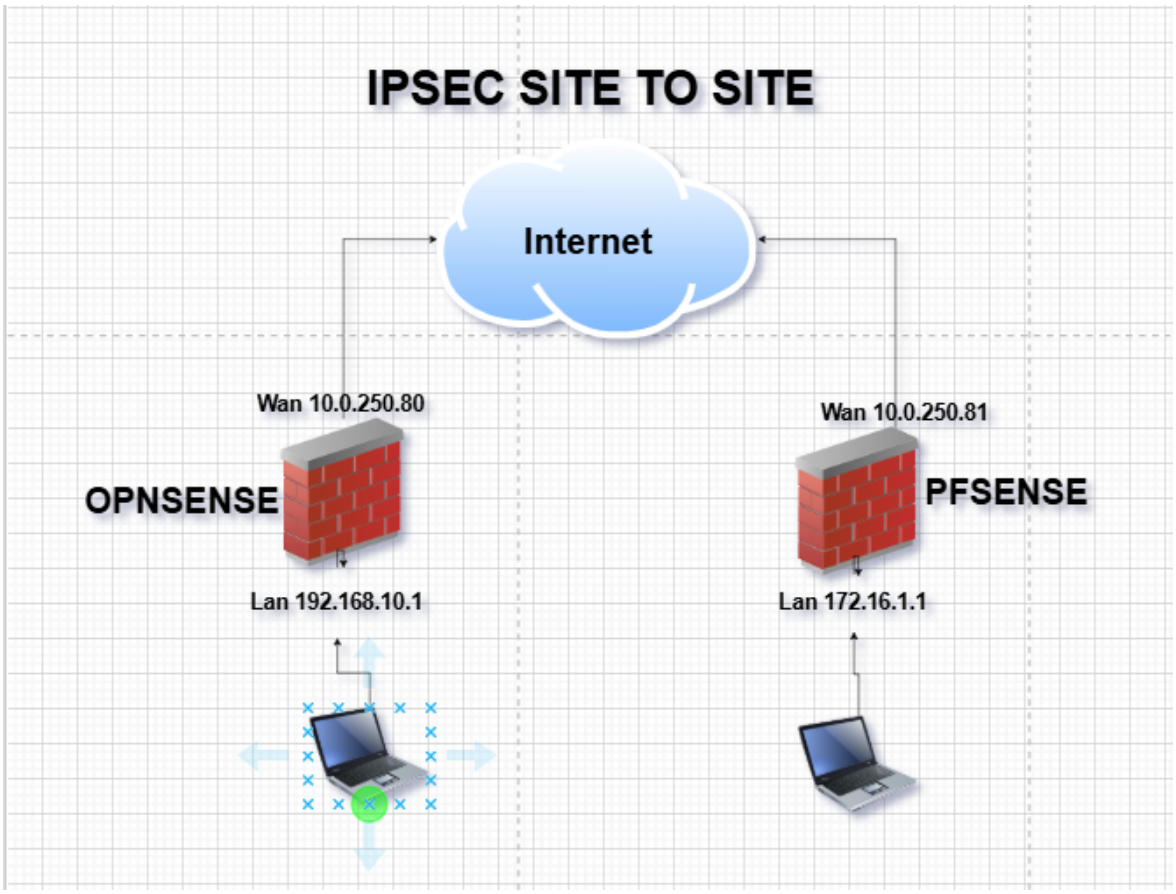
3. Configurer les règles Internet Control Message Protocol (ICMP)

Règle réseau de l'interface OP1 (LAN Collaborateur)



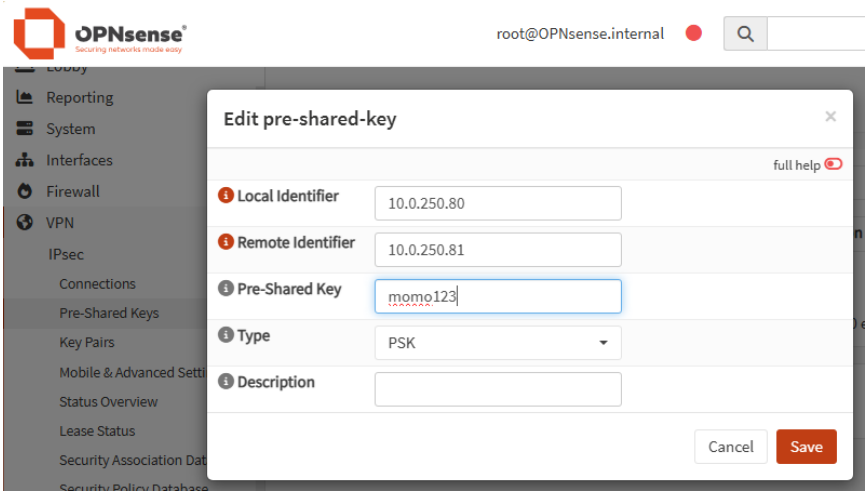
Configuration IPSEC site to site

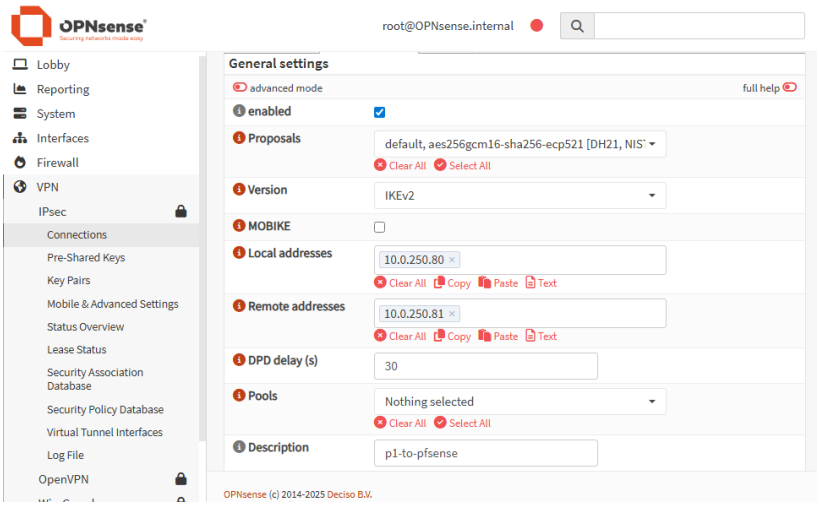
Schema IPSEC



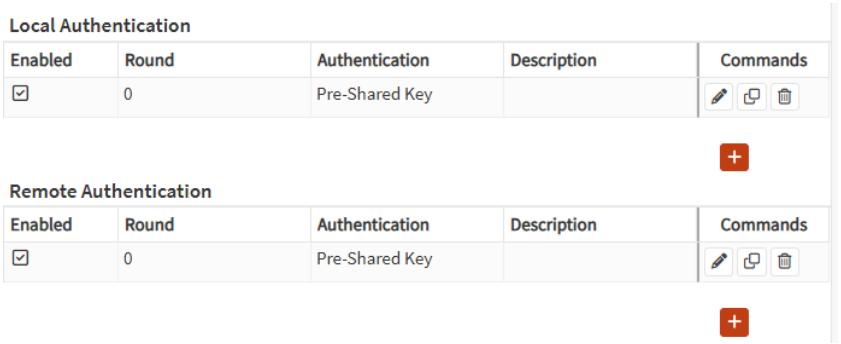
Activation et configuration du service IPSEC sur l'OPNSENSE

1- Configuration de la Key avec les IP WAN

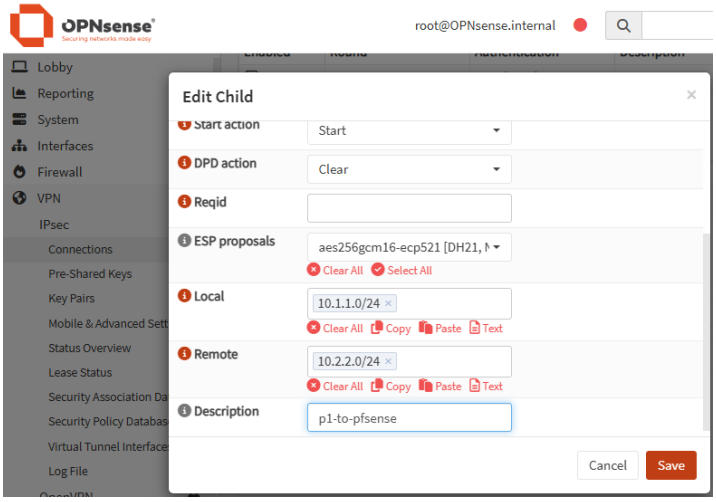


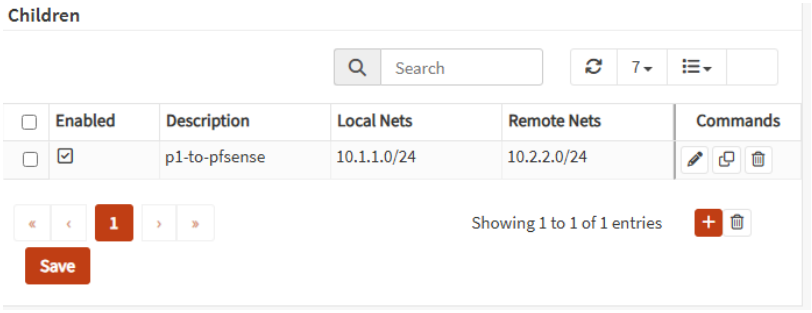


2- Configuration du local Authentication, et du Remote Authentication



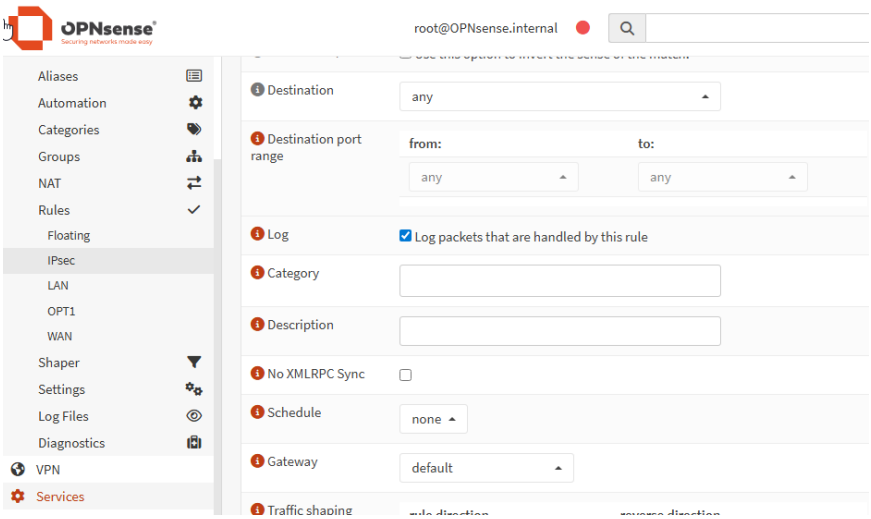
3- Configuration du Child



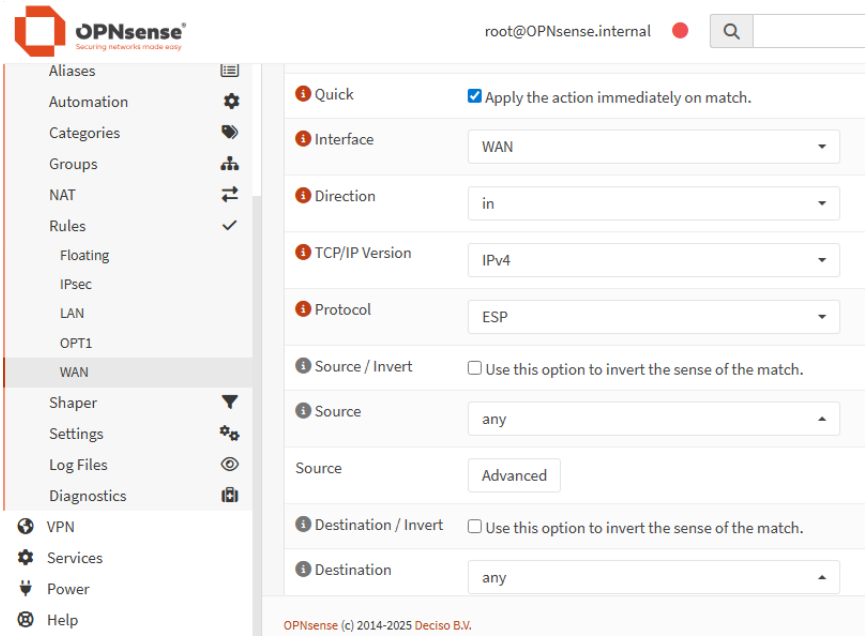


4- Règle Firewall, pour autoriser la communication entre les sites

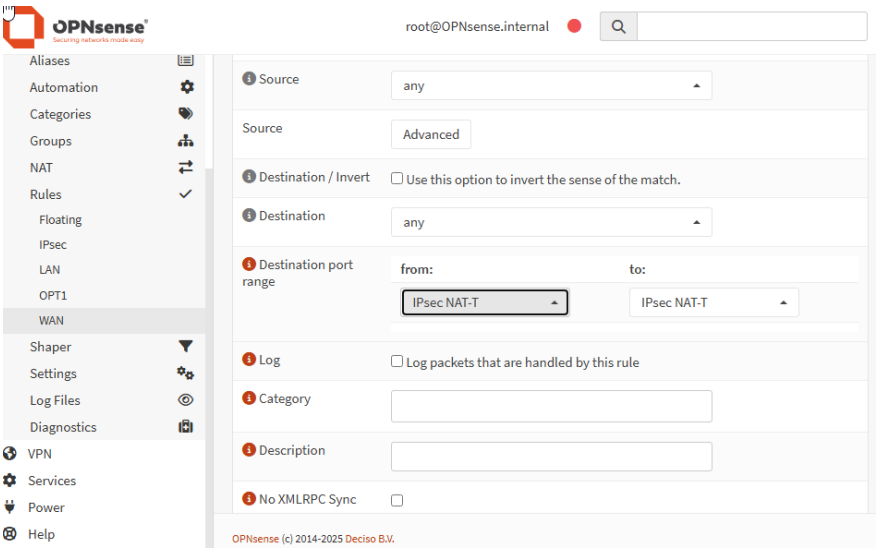
a) règle IPSEC



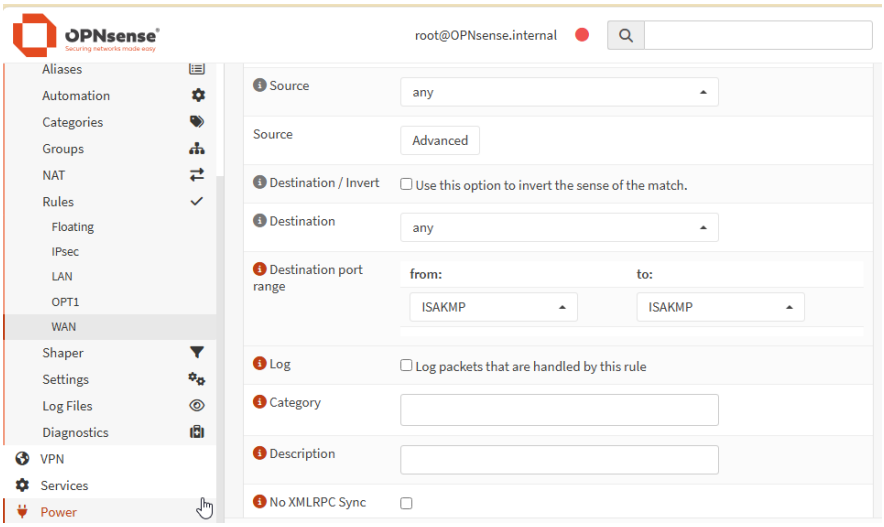
b) règle WAN ESP

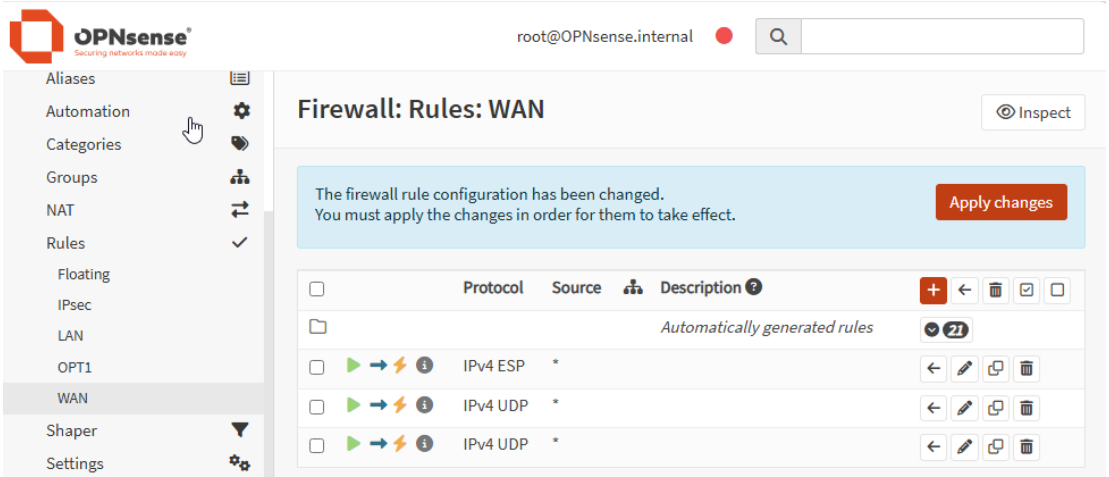


c) règle UDP IPsec NAT-T



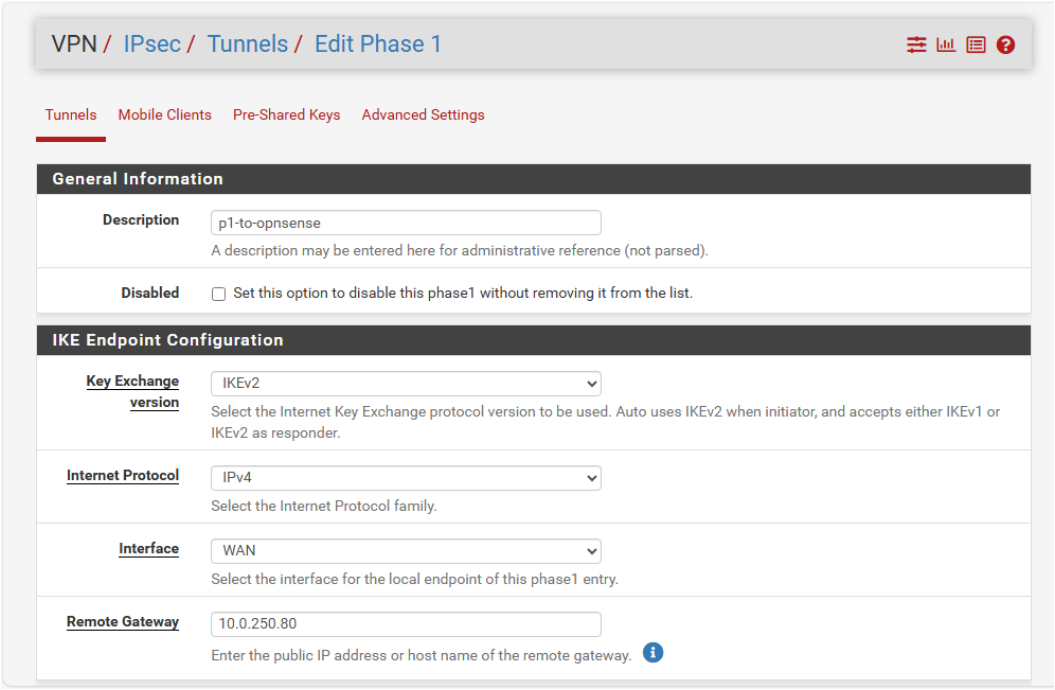
d) règle WAN ISAKMP



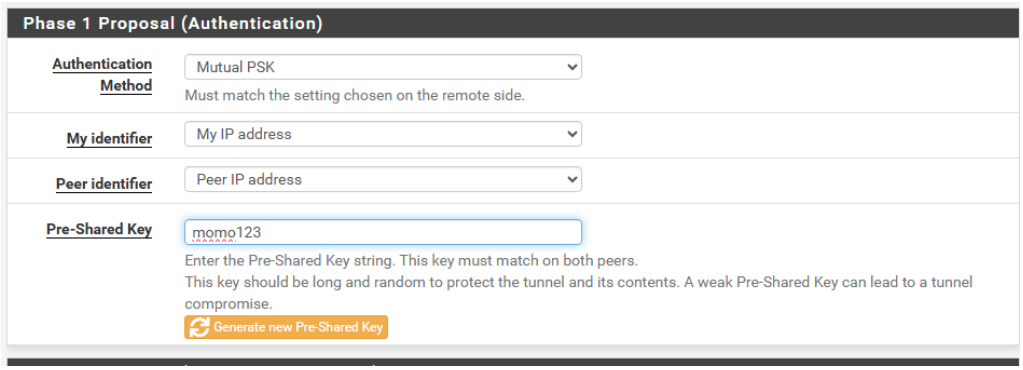


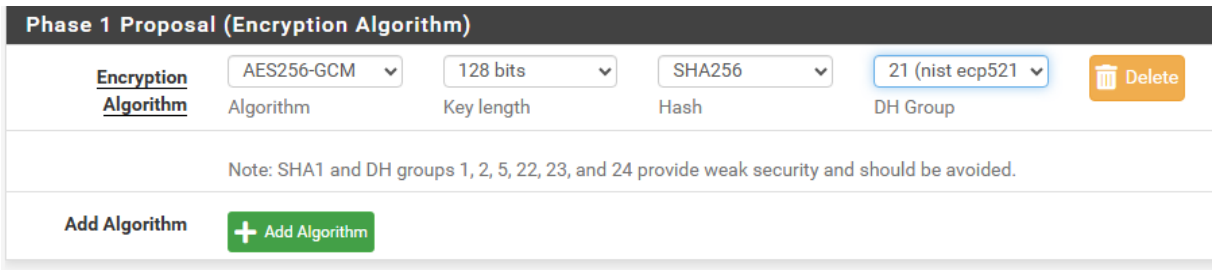
Sur le PFSENSE

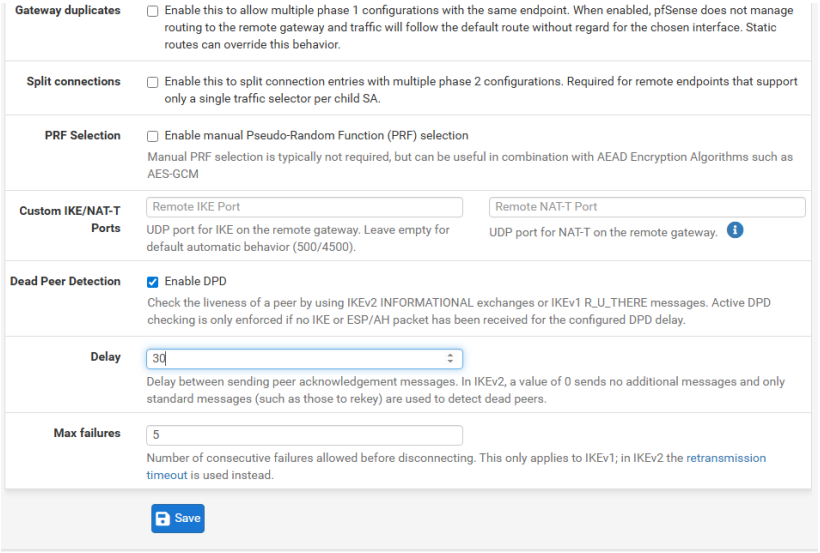
Configuration IPSEC



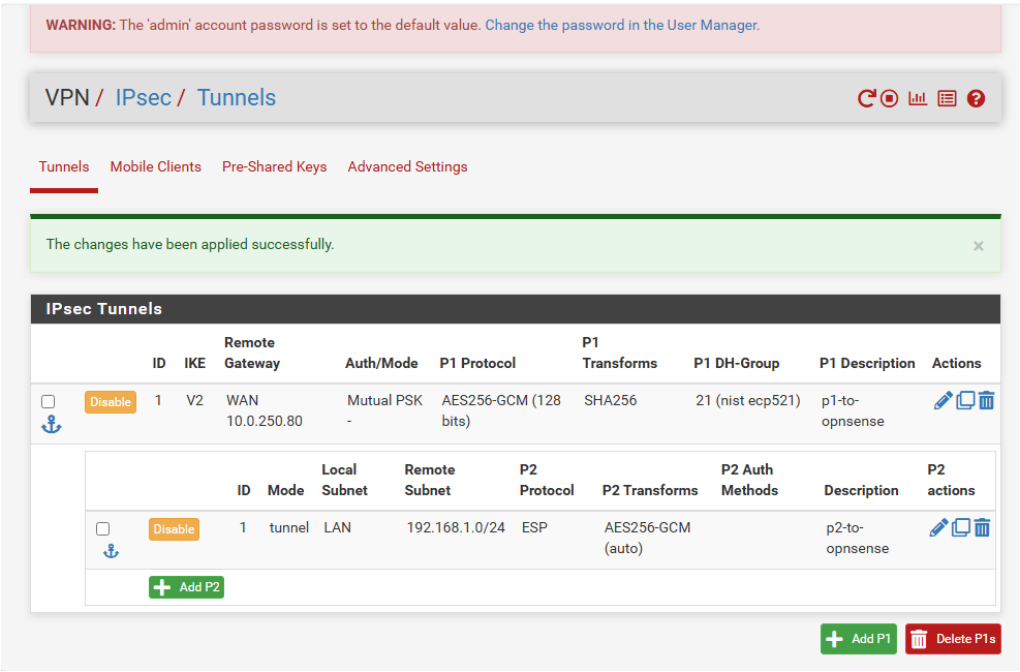
Configuration Key



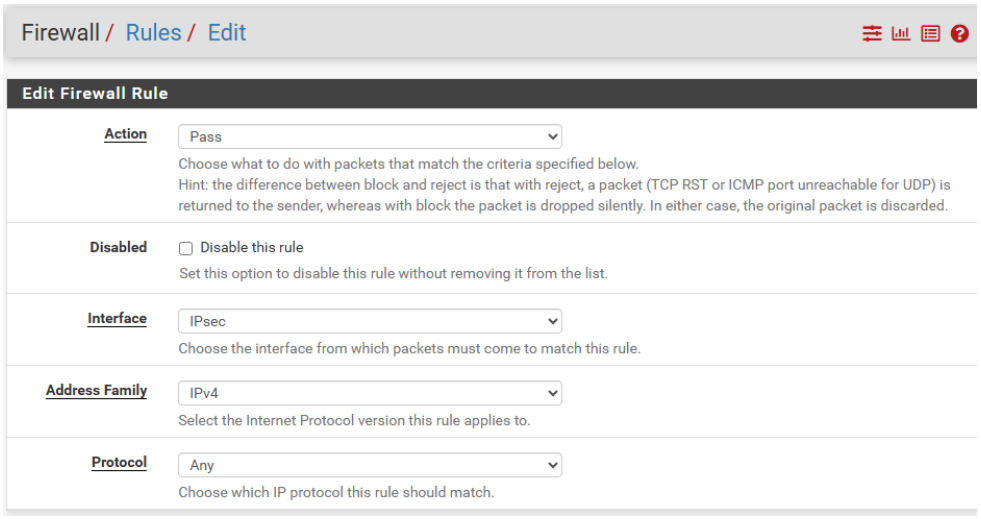


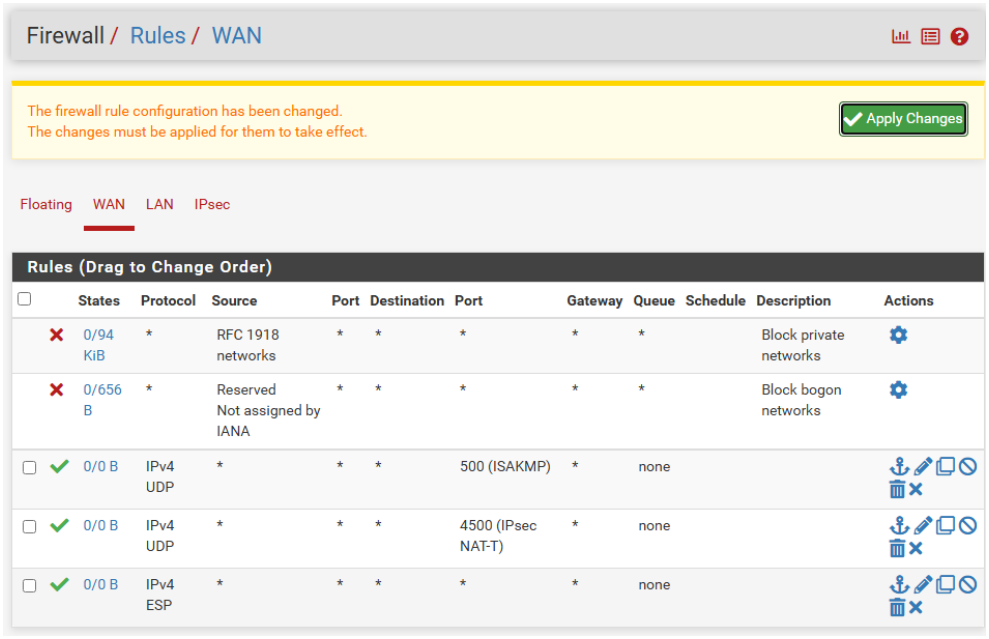


Configuration des tunnels

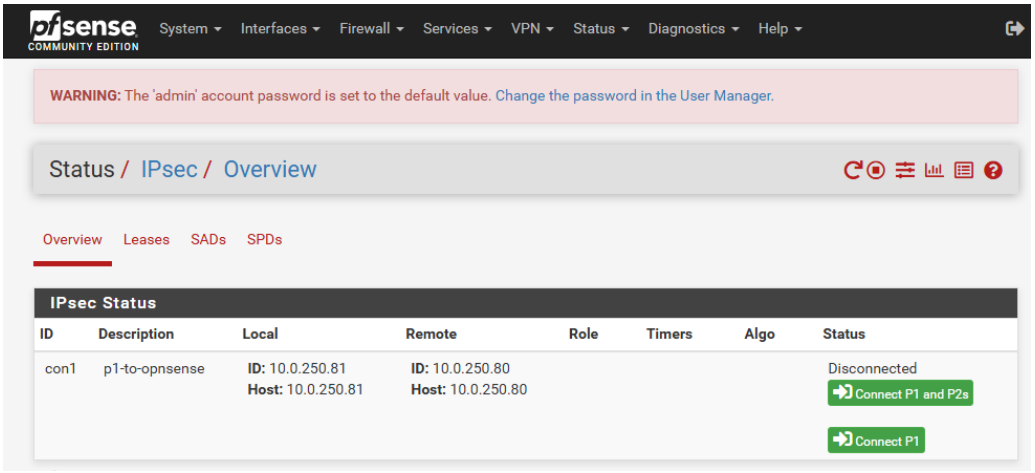


Règle PFSENSE





Teste de connexion



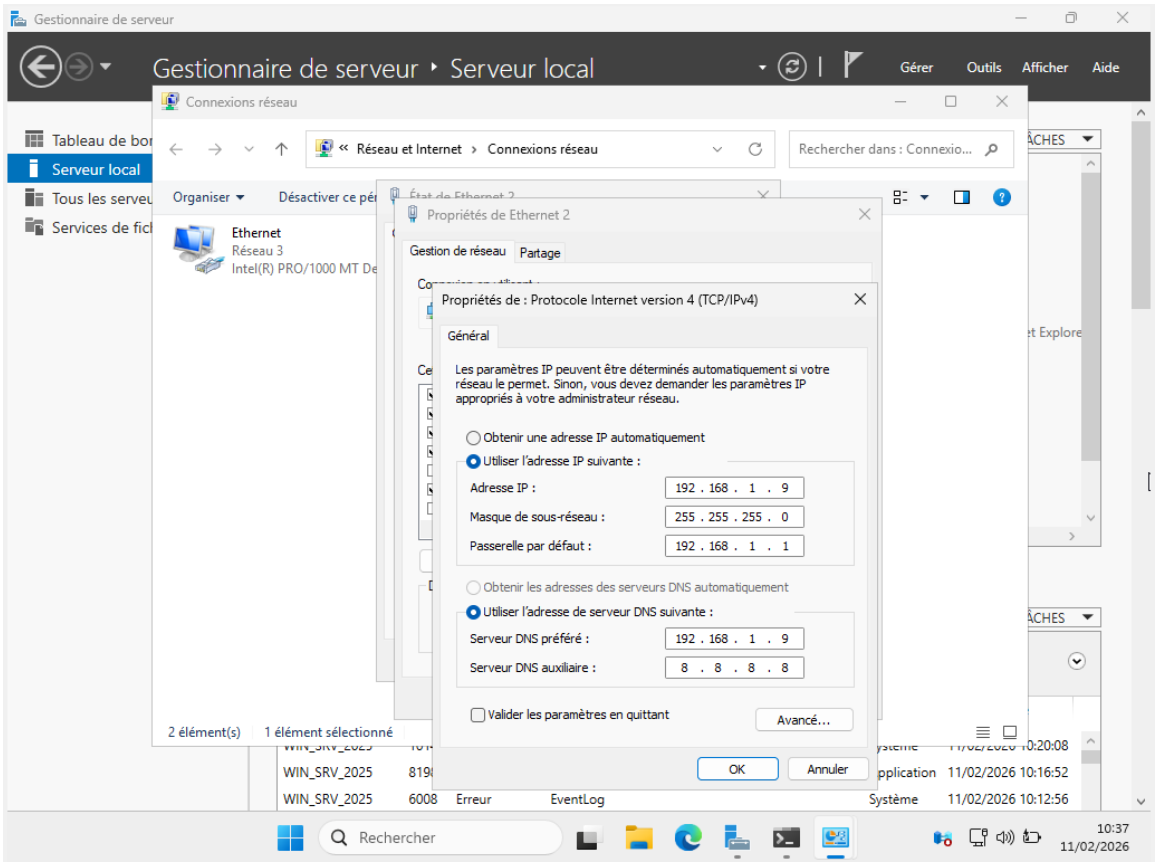
IPsec Status

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #3	p1-to-opnsense	**ID:** Any identifier **Host:** 10.0.250.81:500 **SPI:** 686fbefec0a8d0a2	**ID:** Any identifier **Host:** 10.0.250.80:500 **SPI:** 0000000000000000	IKEv2 Initiator	**Rekey:** Disabled **Reauth:** Disabled		Connecting Disconnect P1

ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats	
con1	p2-to-opnsense	172.16.1.0/24		192.168.1.0/24				Disconnected Connect P2

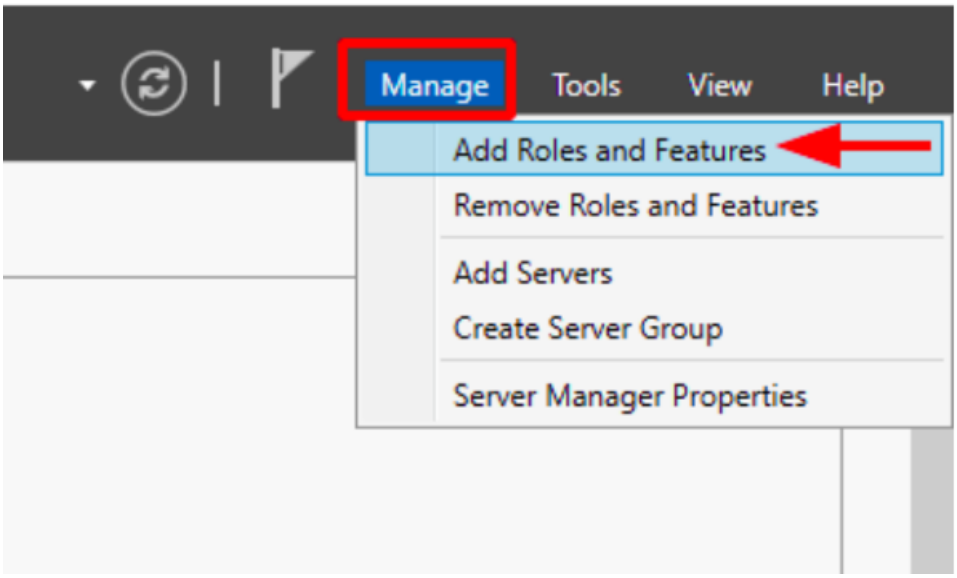
Installation et configuration du Windows serveur 2025

Configuration de la carte réseau

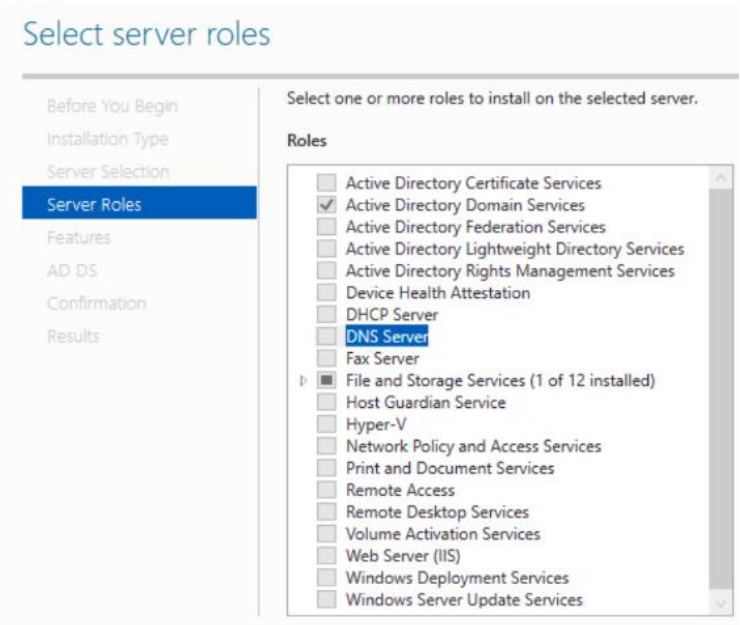


Activation et configuration du service Active Directory et DNS

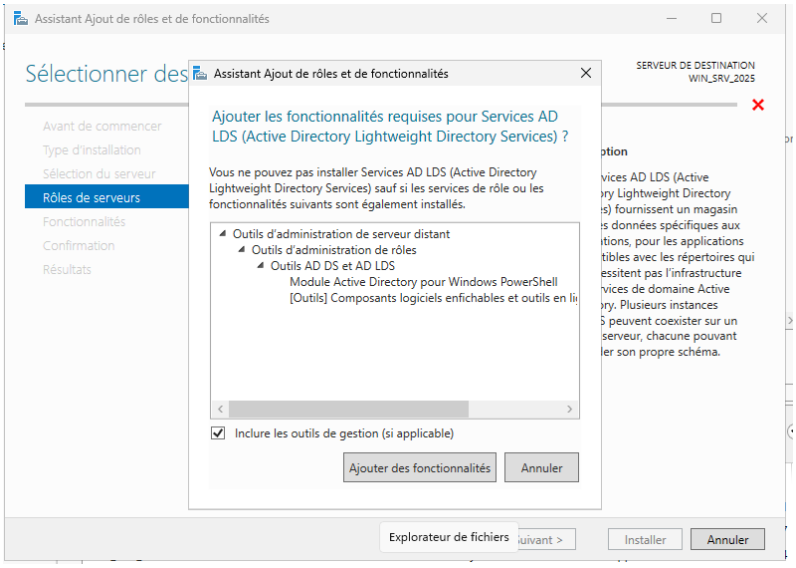
Dans le serveur, sélectionner dans l'onglet manage et dans Add Roles and Features.

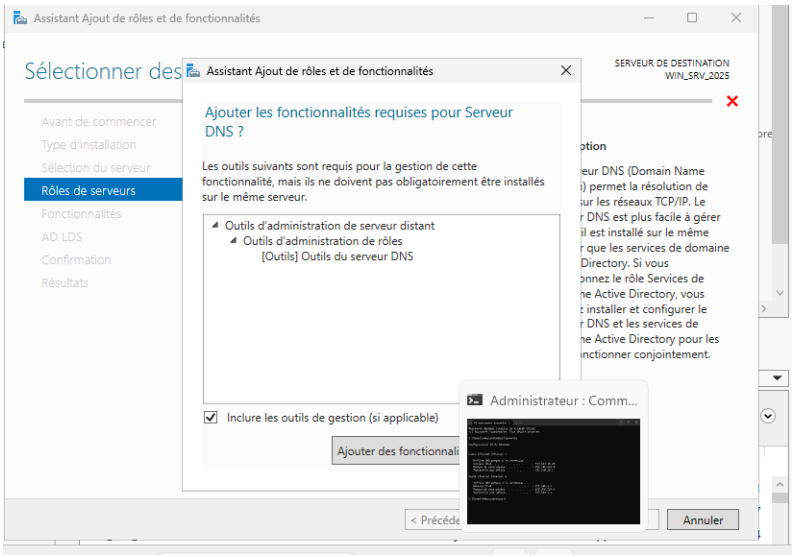


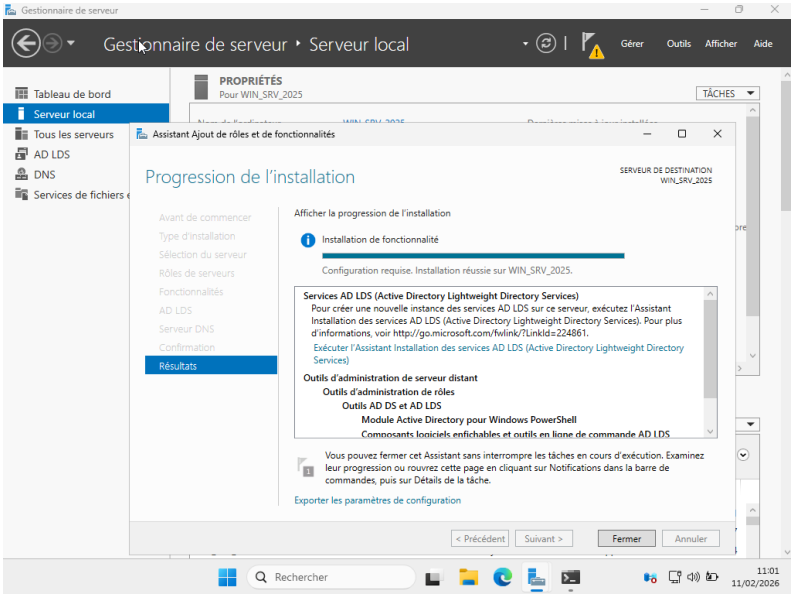
Sélectionner les services Active Directory Domain Services, DNS Server



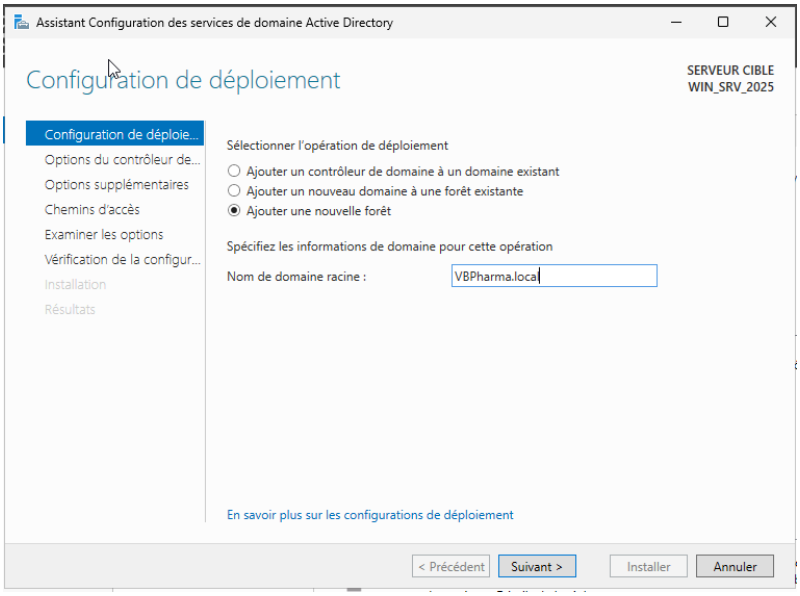
Ajouter les fonctionnalités AD et DNS



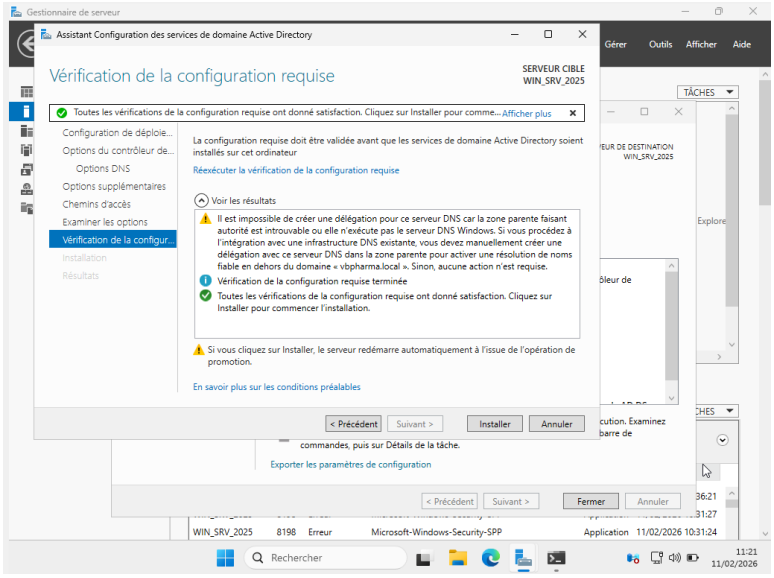




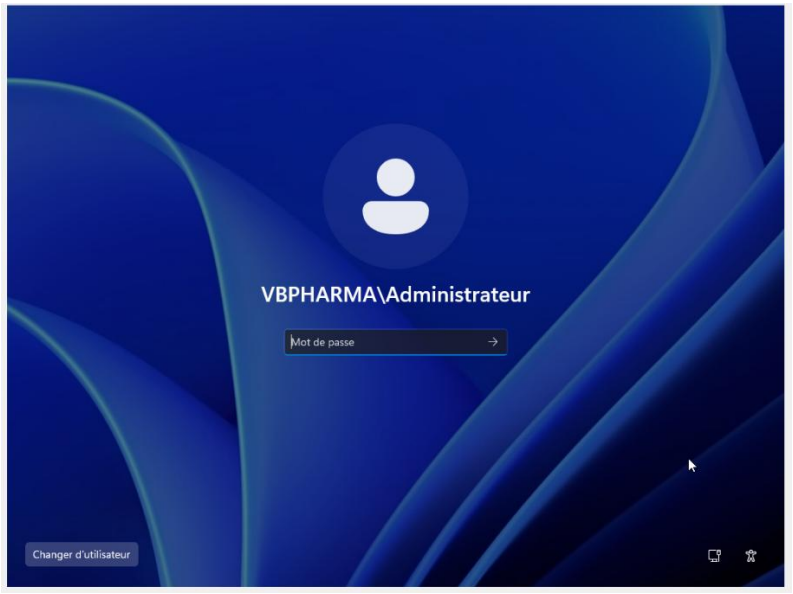
Indication du nom de domaine



Procéder à l’installation

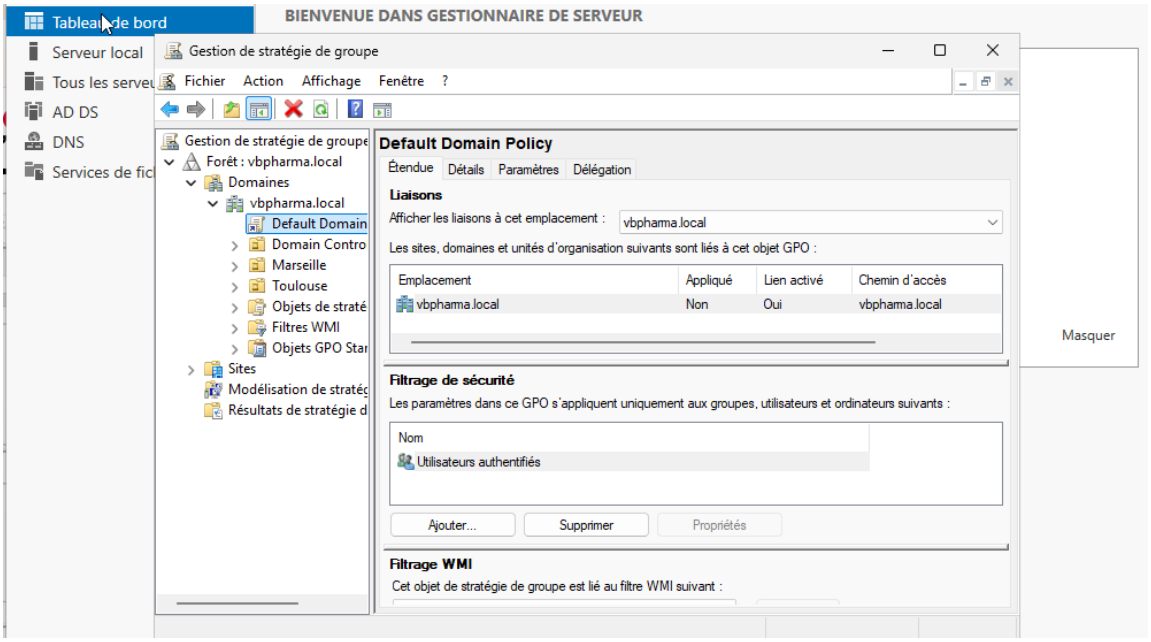


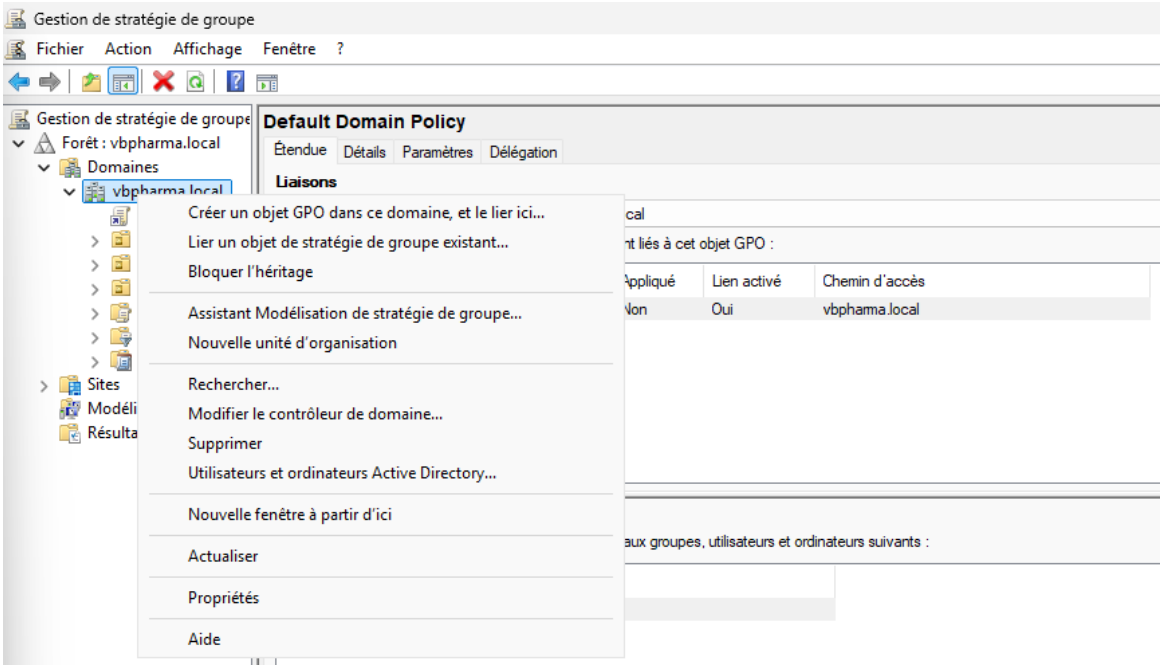
Apres l’installation des services la machine redémarre et se présente ainsi

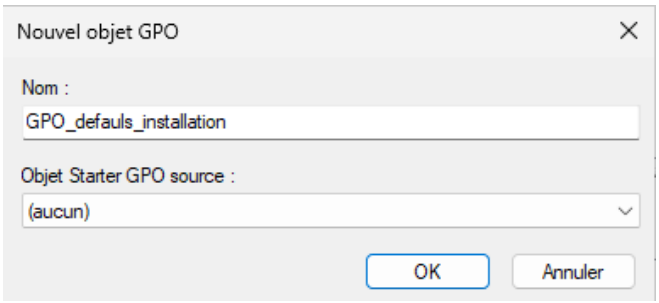


Création de GPO

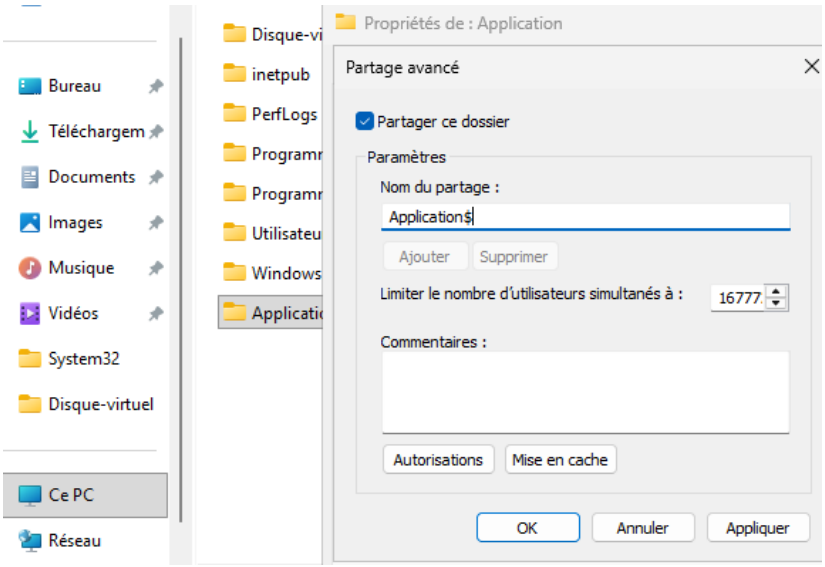
J’ai choisi de faire un déploiement d’application avec une GPO. Pour ce faire, je me suis rendu dans l’option Gestion de stratégie de groupe



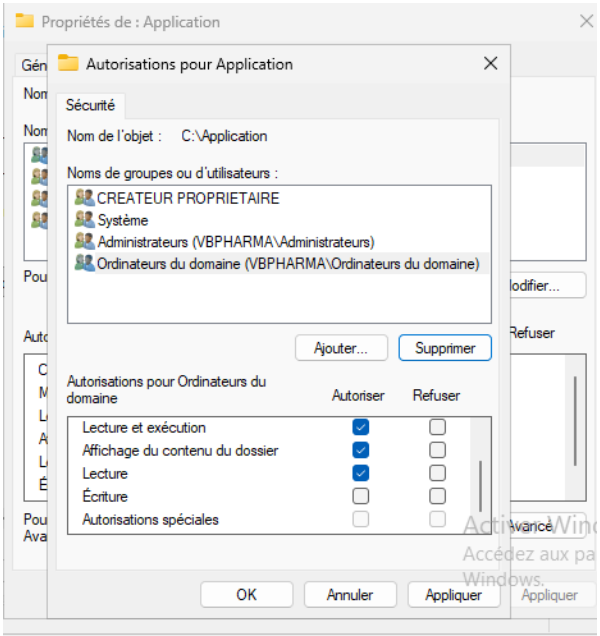




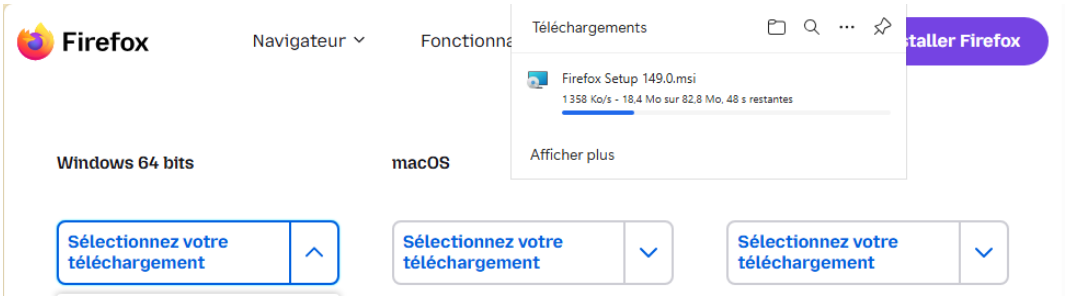
J’ai ensuite créé un dossier partage



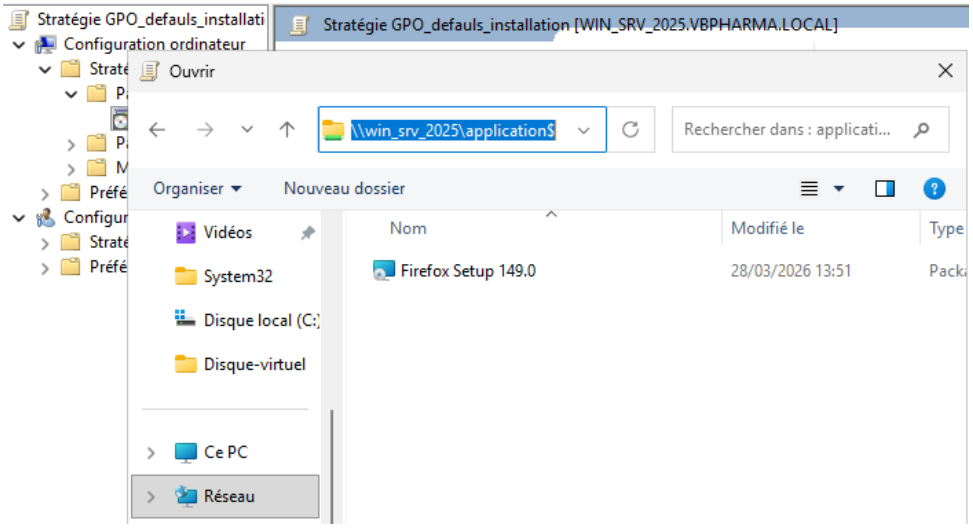
J’ajoute le groupe **Ordinateur du domaine** et défini **les droits NTFS.**

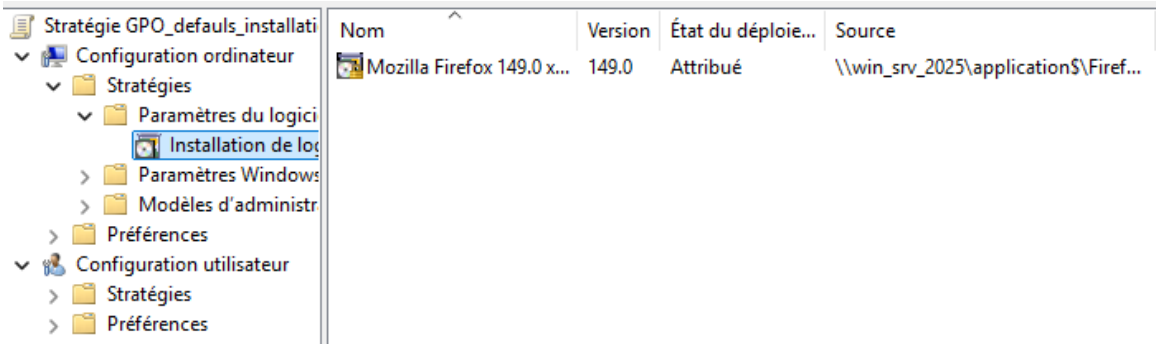


Puis j'ai téléchargé et déposer le fichier msi de Firefox dans le partage

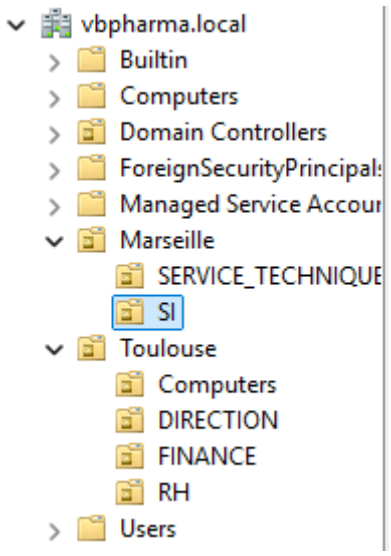


Je me suis assuré de bien choisir le chemin réseau lors de la création.

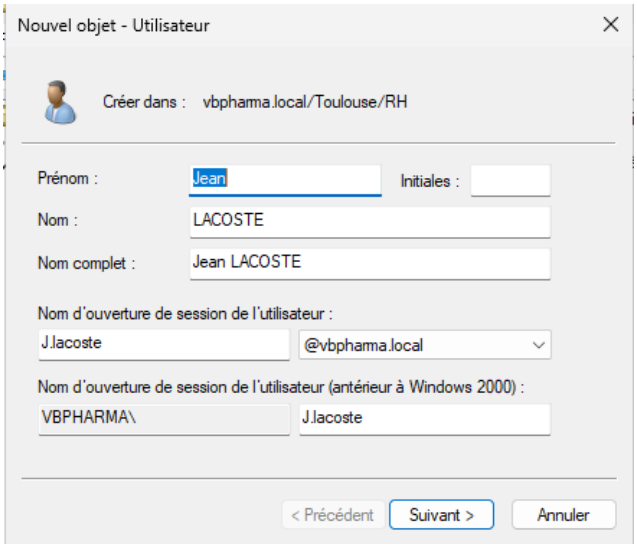


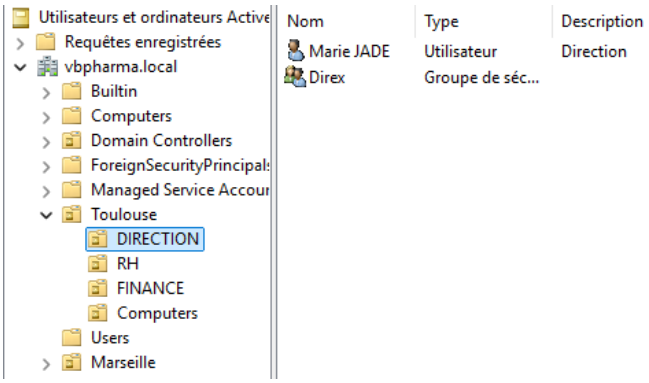


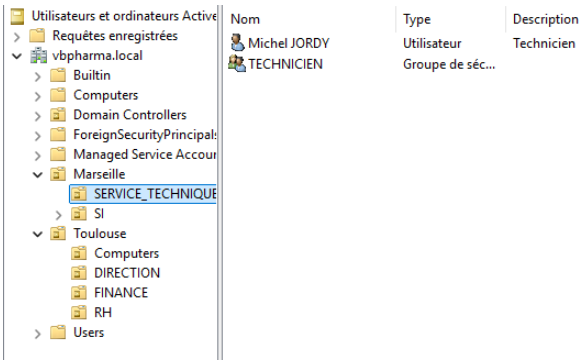
Création d'Unité d'organisation, Site & Service



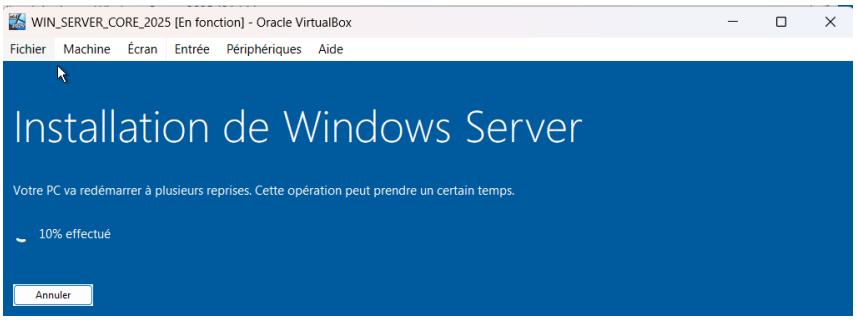
Création d'utilisateur

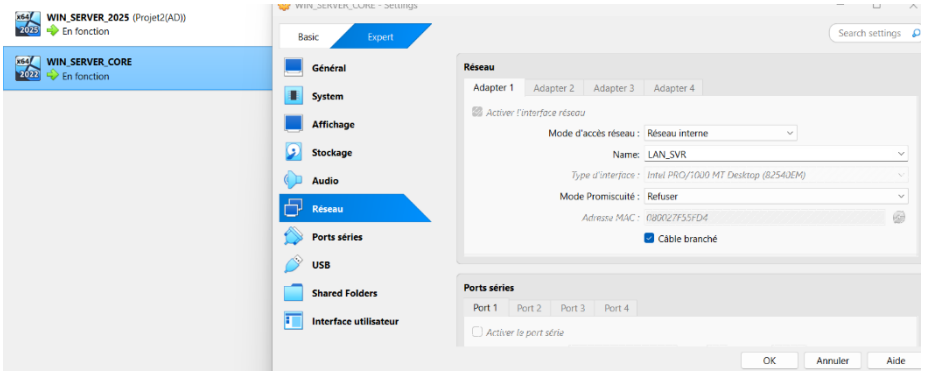




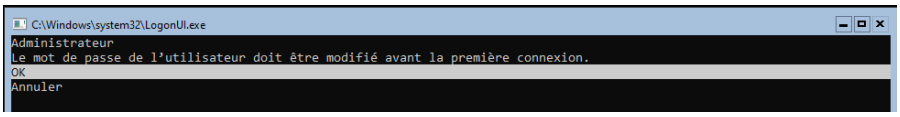


Installation et configuration de la Windows Serveur core 2025





Configuration mot de passe : ******



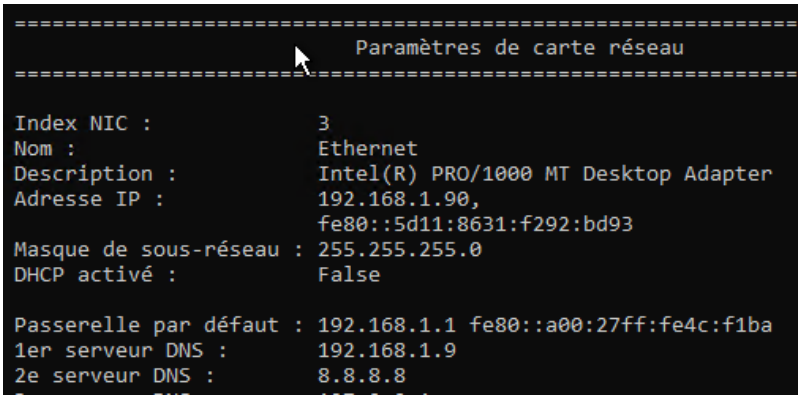
Configuration adresse ip et DNS

IP static : 192.168.1.90 ;

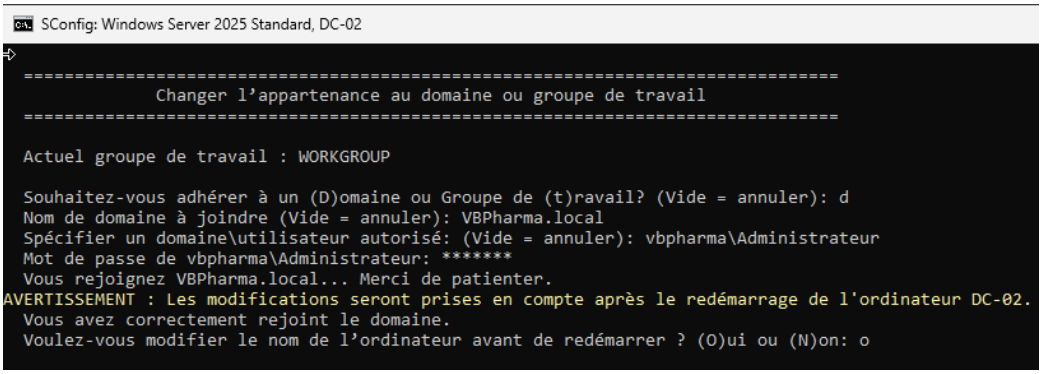
Max de sous réseau : 255.255.255.0 ;

DNS 1 : 192.168.1.9

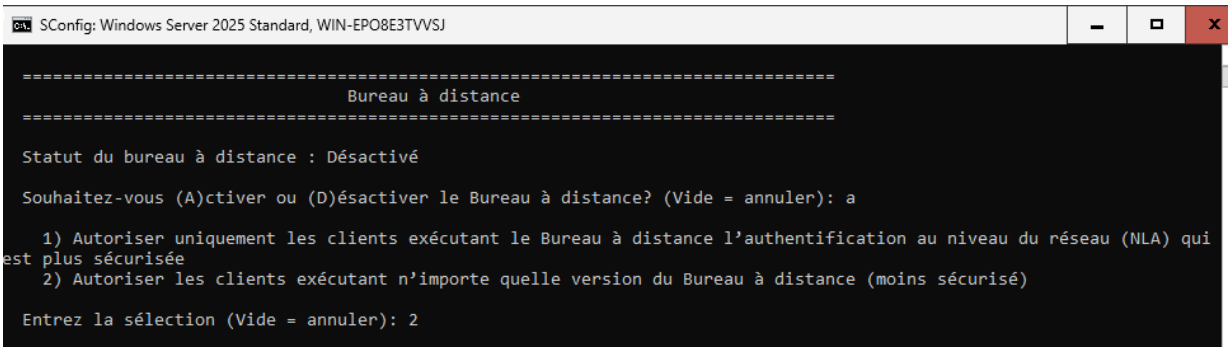
DNS 2 : 8.8.8.8



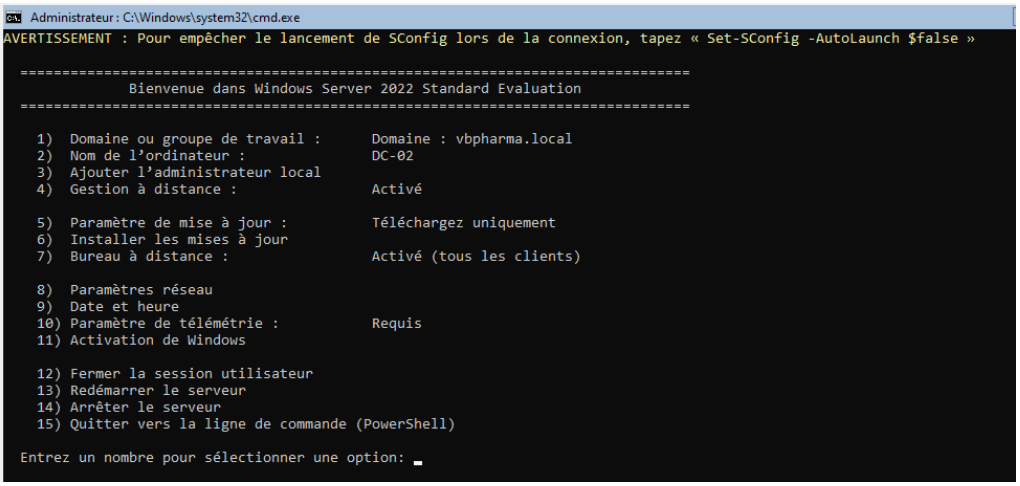
Entrer au domaine **VBPharma.local, et activation de la gestion à distance.**



Activation du bureau à distance

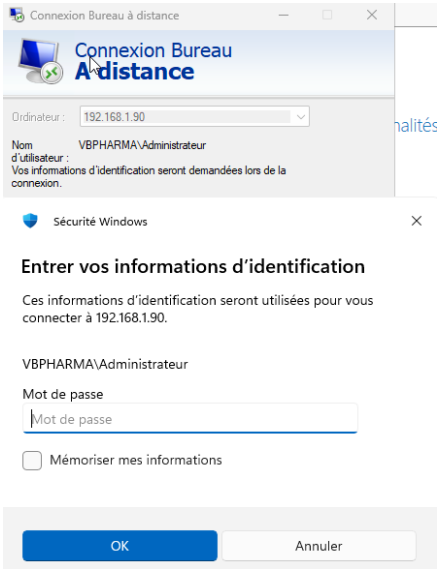


Configuration finale



Installation du service Active Directory sur le core

Se connecter au core grâce à la gestion distance (Bureau à distance) depuis le Windows GUI.

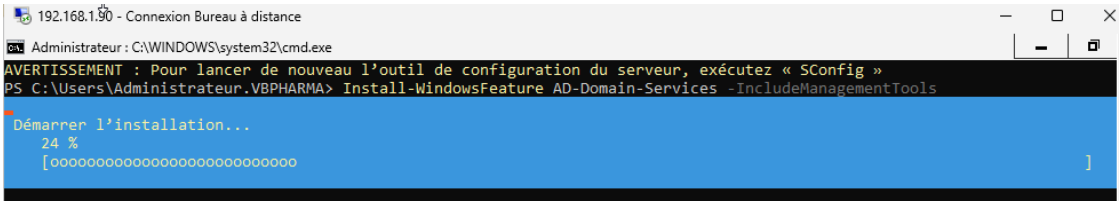


Installation du service AD

Installation Du rôle AD DS sur le Server Core 2025

Commande:

Install-WindowsFeature AD-Domain-Services -IncludeManagementTools



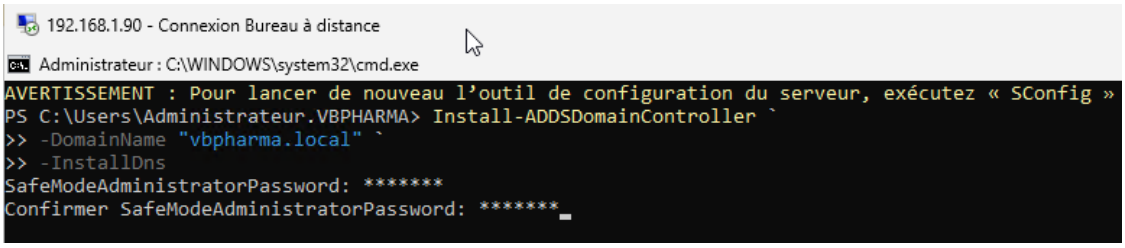
Installation de ADDSDomain Controller et replication de l'Active directory sur le serveur core

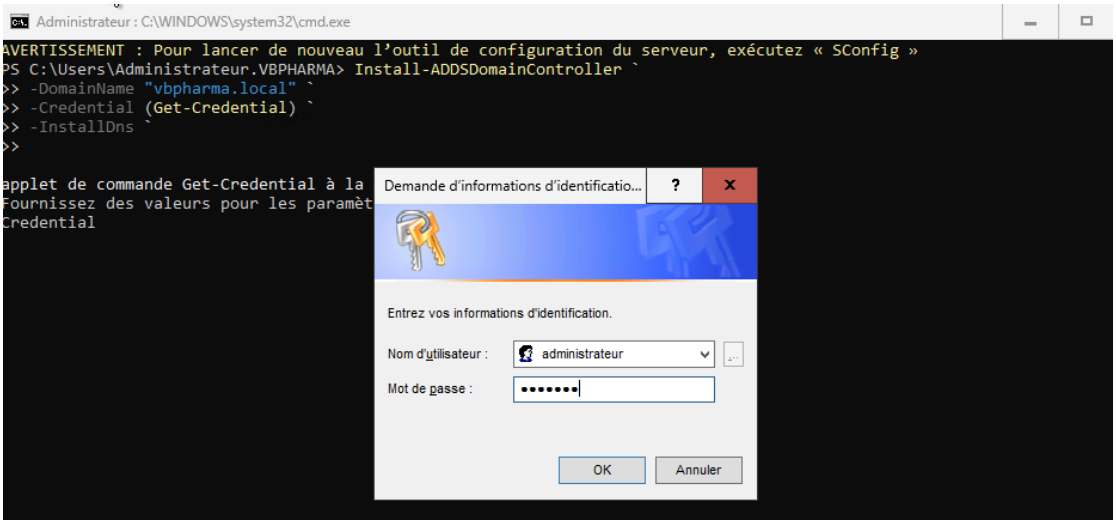
Commande :

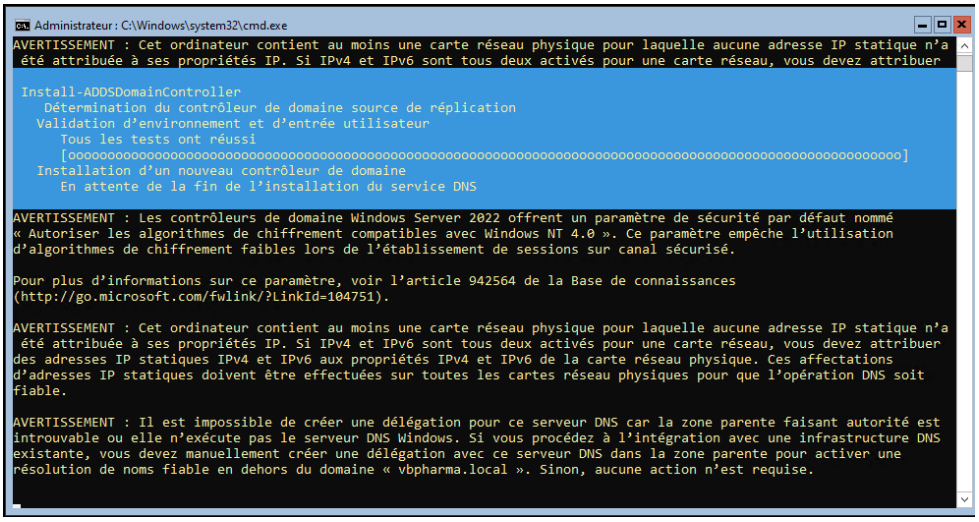
Install-ADDSDomaininController`

-Domainname "vbpharma.local" `

-InstallDns



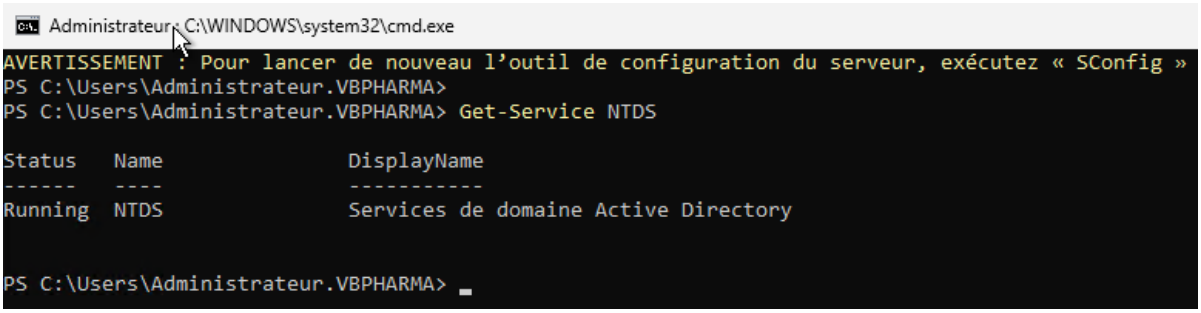




Vérification de la replication

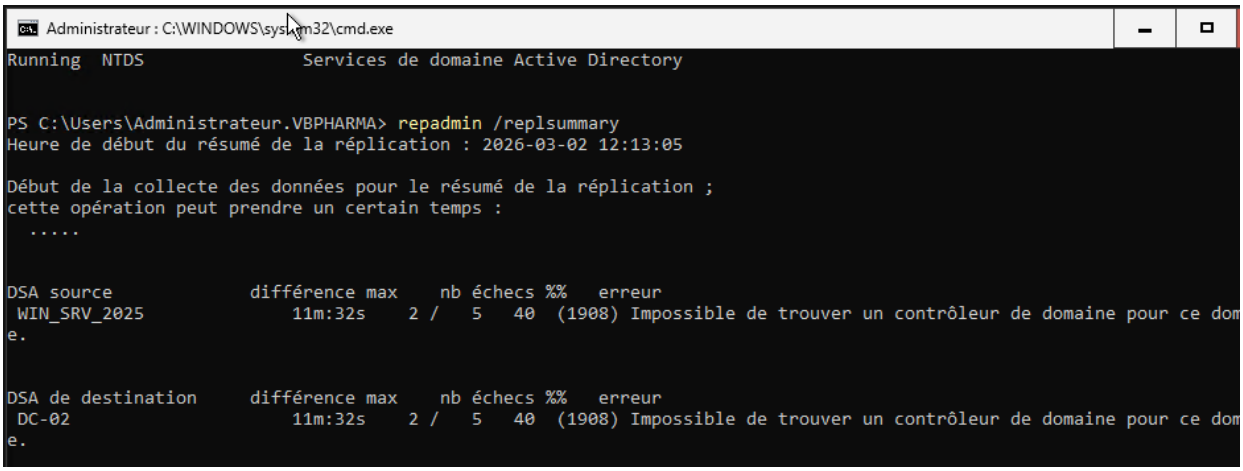
Commande :

Get-Service NTDS

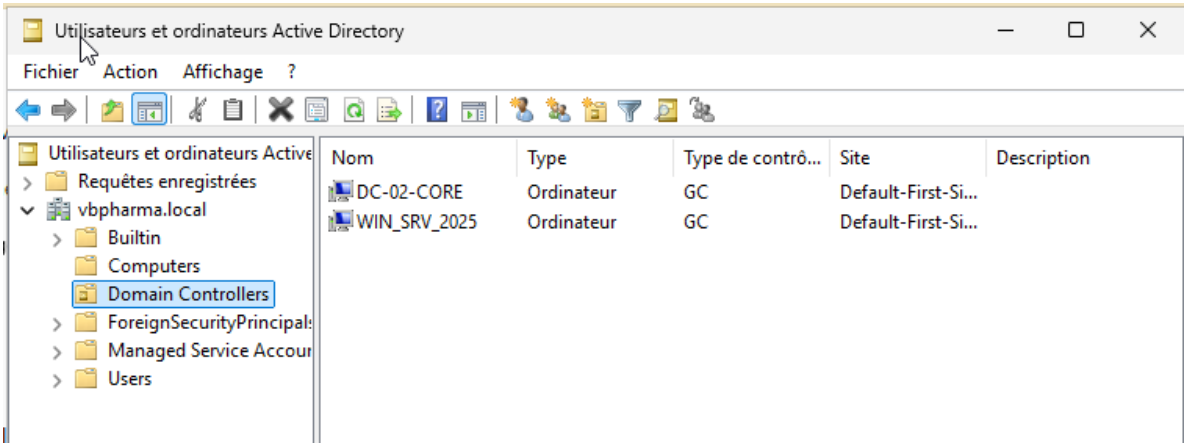


Commande :

Repadmin /replsummary



Dans l'Active Directory



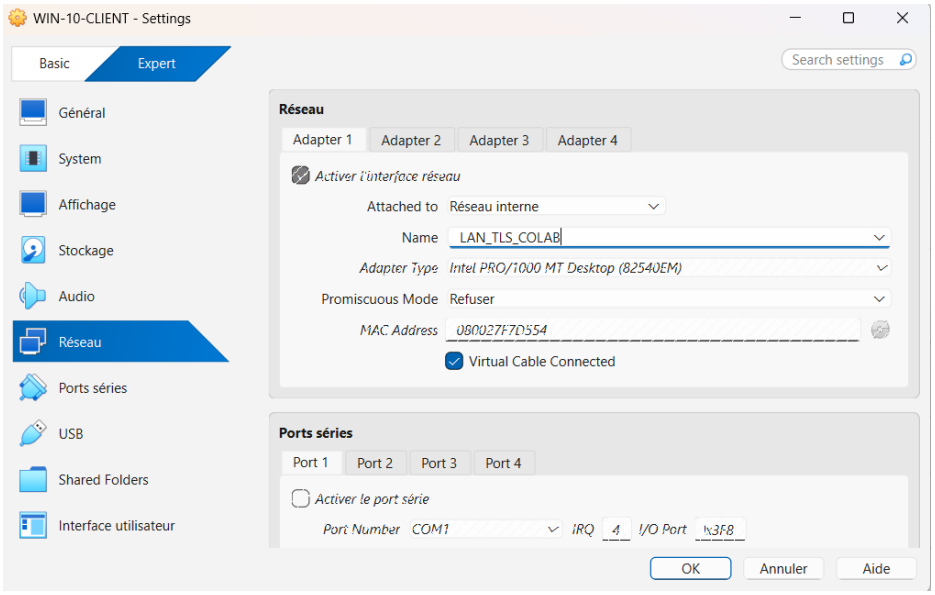
Installation et configuration des VM Windows Clients

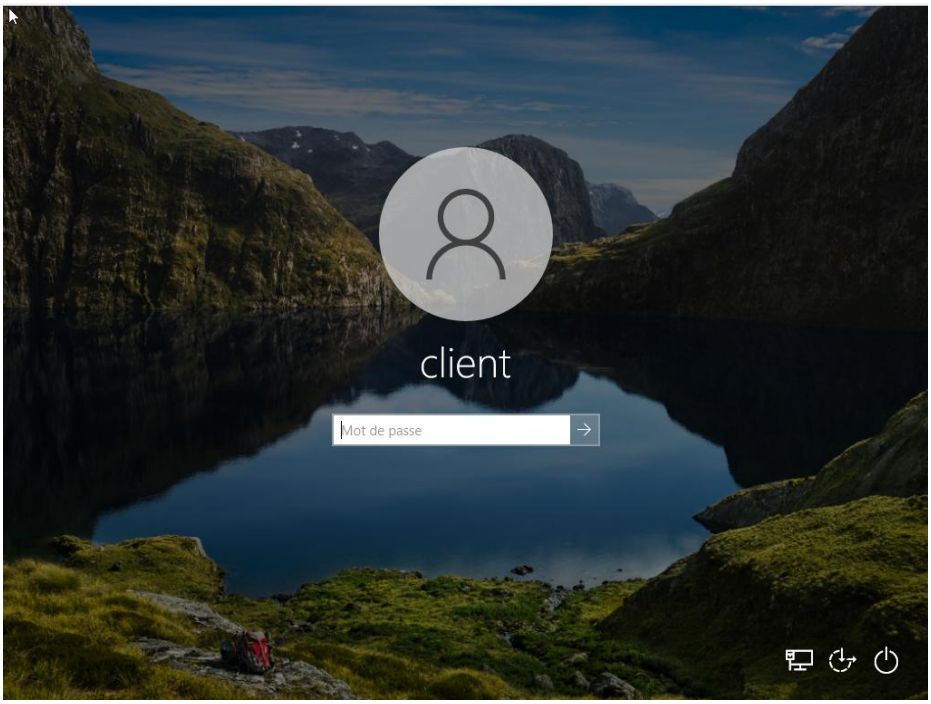
J'ai choisi d'installer des Windows 10 comme client, car elles sont légères et répondent parfaitement aux attentes de ce projet.

L’une d’entre elle jouera le rôle de poste de travail à distance & l’autre le rôle de poste de travail bureau.

Configuration du client à distance

Sur le client 1, j’ai configuré et installer un VPN nomade. La machine sera donc sur le LAN collaborateur.



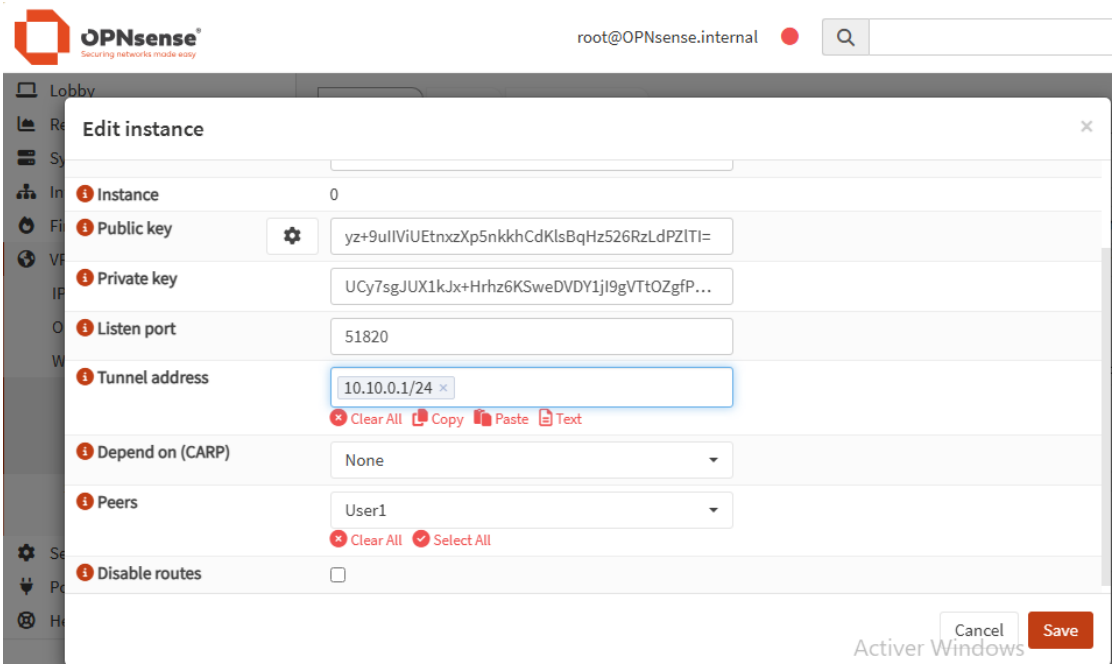


Configuration VPN nomade : WireGuard

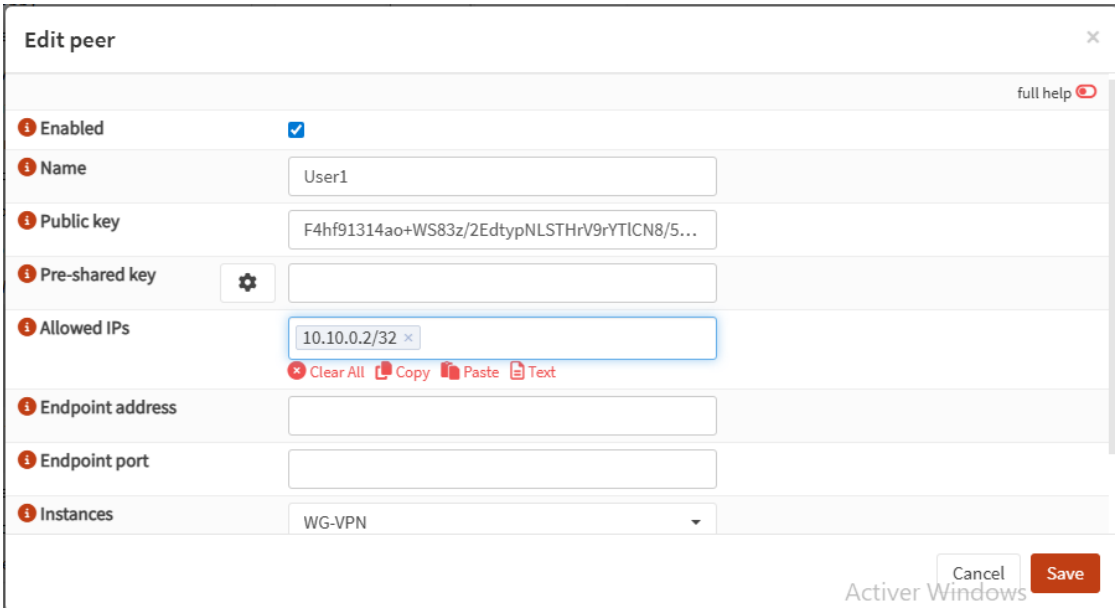
Sur l’OPNSENSE, j’ai activé et configurer le VPN wireGuard

Dans VPN, WireGuard, j’ajoute et configure une nouvelle instance.

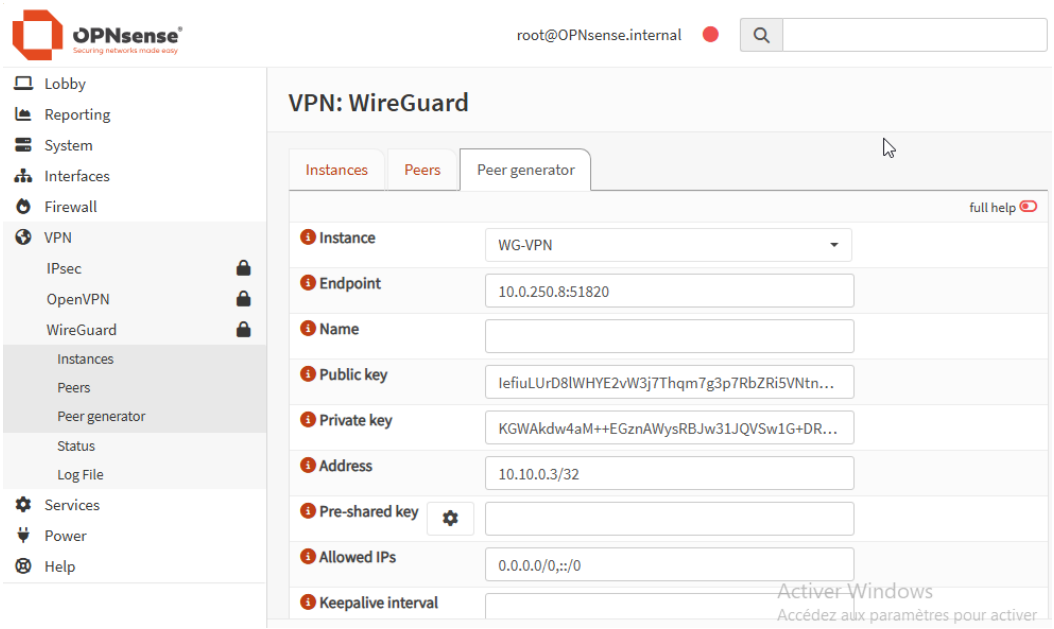
Je choisir une adresse IP pour le Tunnel address côté OPNSENSE.

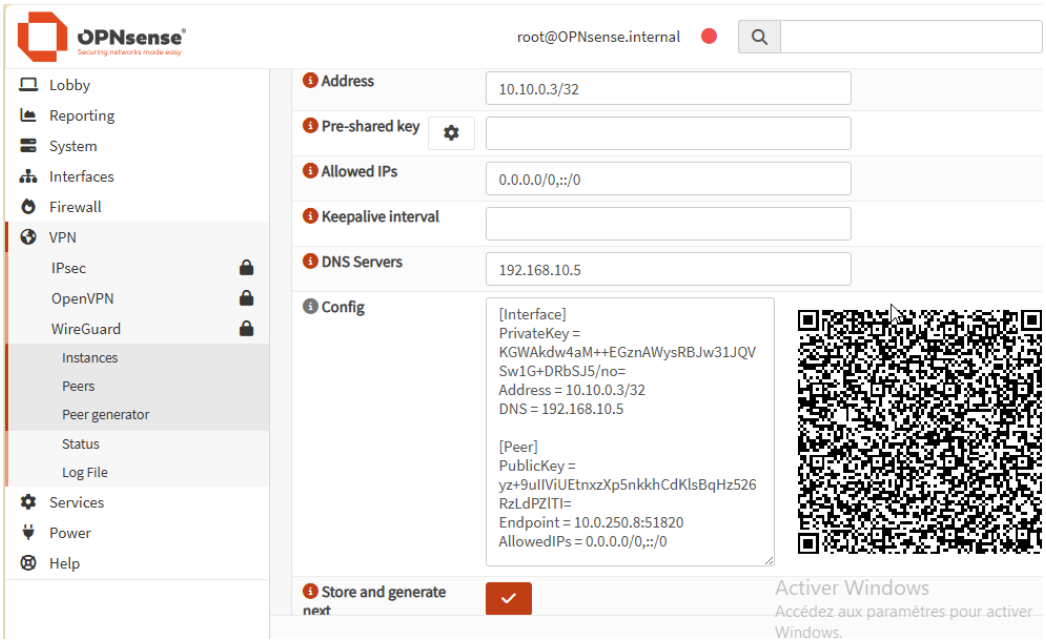


Puis configurer le PEER, choisir une IP de connexion au client

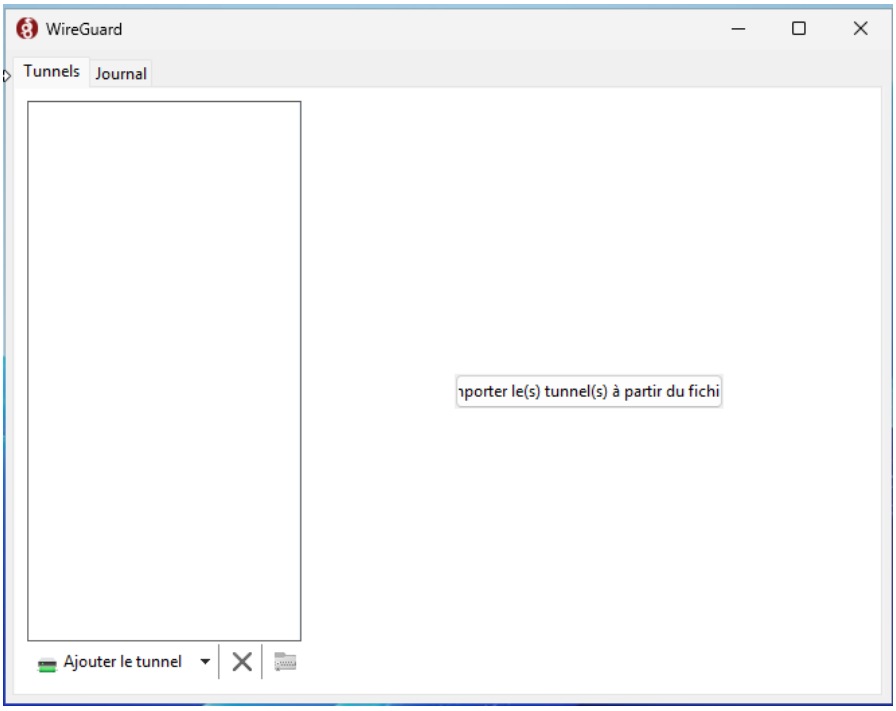


Puis je génère le Peer dans l'option Peer generator.

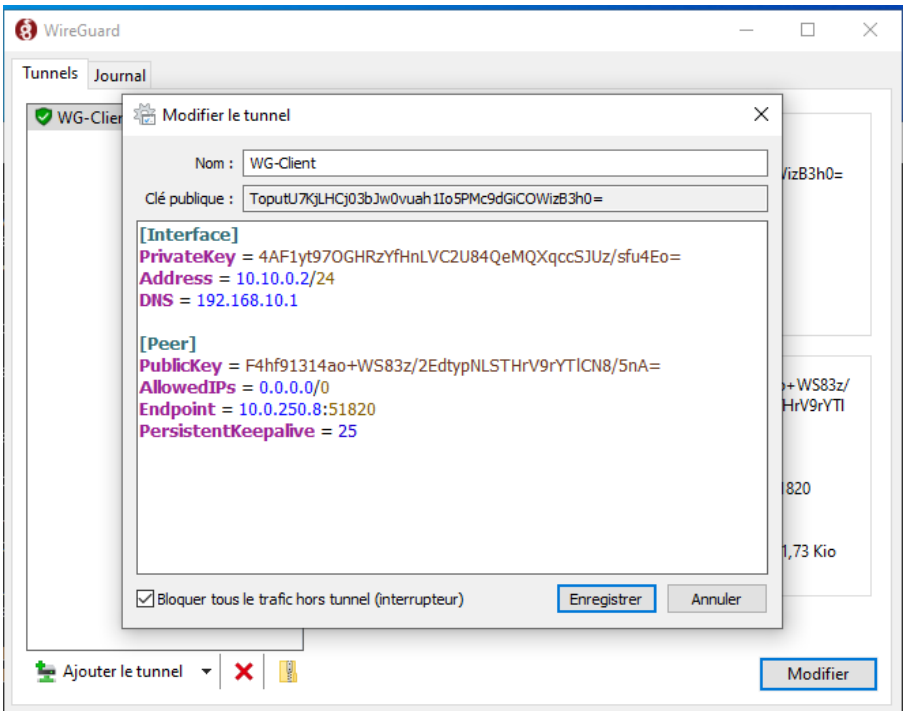

OPNsense
root@OPNsense.internal
Lobby
Reporting
System
Interfaces
Firewall
VPN
IPsec
OpenVPN
WireGuard
Instances
Peers
Peer generator
Status
Log File
Services
Power
Help
VPN: WireGuard
Instances
Peers
Peer generator
full help
Instance
WG-VPN
Endpoint
10.0.250.8:51820
Name
Public key
lefiuLUrD8lWHYE2vW3j7Thqm7g3p7RbZRi5VNtn...
Private key
KGWAkdw4aM++EGznAWysRBJw31JQVSw1G+DR...
Address
10.10.0.3/32
Pre-shared key
Allowed IPs
0.0.0.0/0,::/0
Keepalive interval
Activer Windows
Accédez aux paramètres pour activer


OPNsense
root@OPNsense.internal
Lobby
Reporting
System
Interfaces
Firewall
VPN
IPsec
OpenVPN
WireGuard
Instances
Peers
Peer generator
Status
Log File
Services
Power
Help
Address
10.10.0.3/32
Pre-shared key
Allowed IPs
0.0.0.0/0,::/0
Keepalive interval
DNS Servers
192.168.10.5
Config
[Interface]
PrivateKey =
KGWAkdw4aM++EGznAWysRBJw31JQV
Sw1G+DRbSJ5/no=
Address = 10.10.0.3/32
DNS = 192.168.10.5
[Peer]
PublicKey =
yz+9uIlViUEtnxzXp5nkkhCdKlsBqHz526
RzLdPZlTI=
Endpoint = 10.0.250.8:51820
AllowedIPs = 0.0.0.0/0,::/0
Store and generate next
Activer Windows
Accédez aux paramètres pour activer Windows.

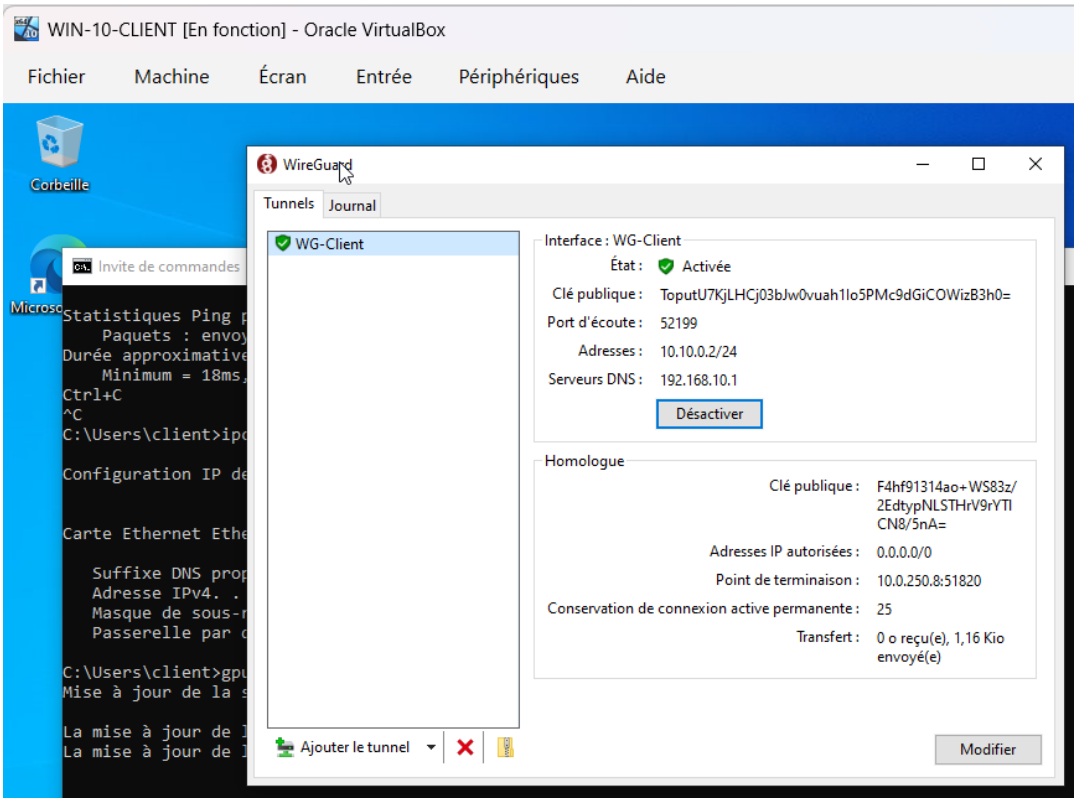
Sur le client, j'installe WireGuard, et configure le tunnels client.



Je renseigner les parametttres critique dont l'addresse de l'interface client (choisie lors de la configurartion opnsense) et le Peer

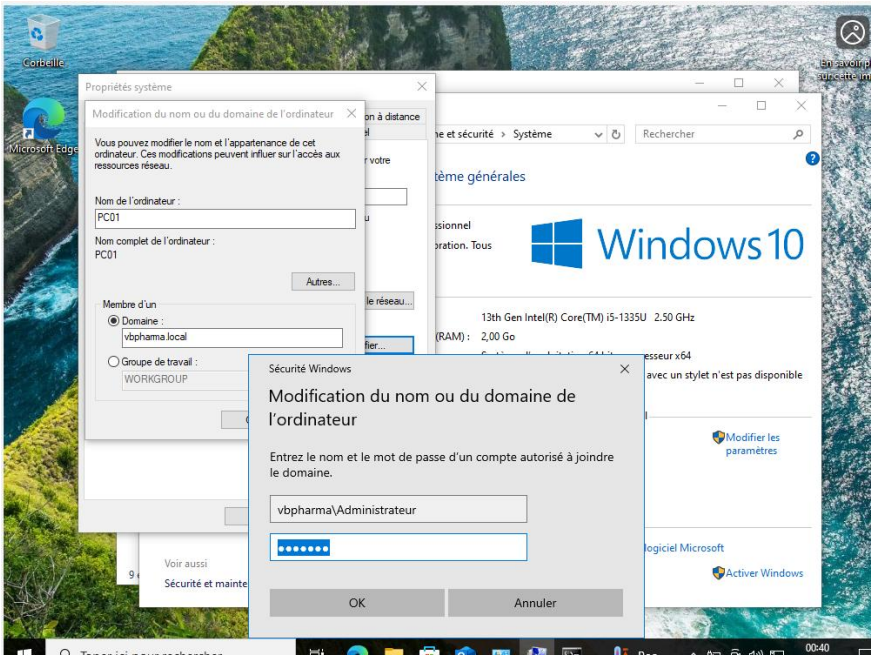


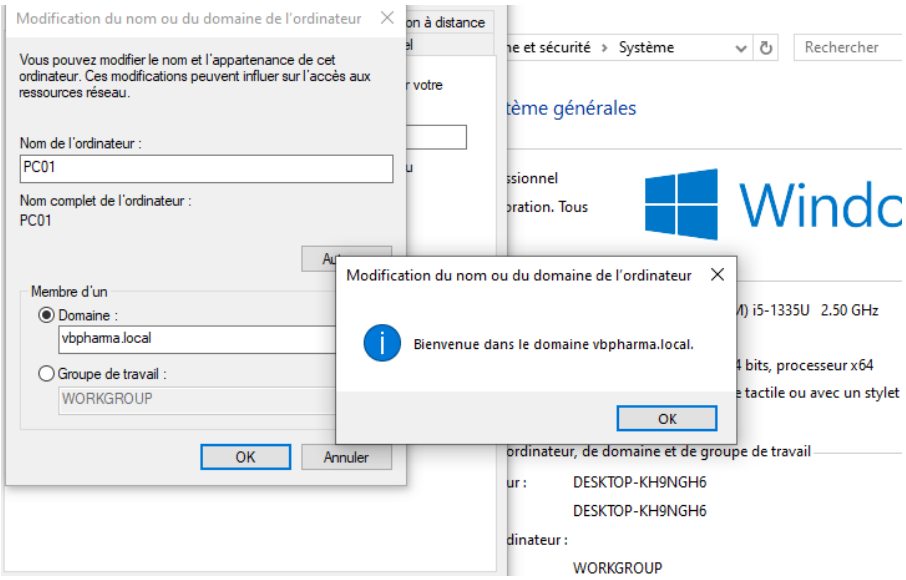
J’effectue le tester de connexion avec le VPN.



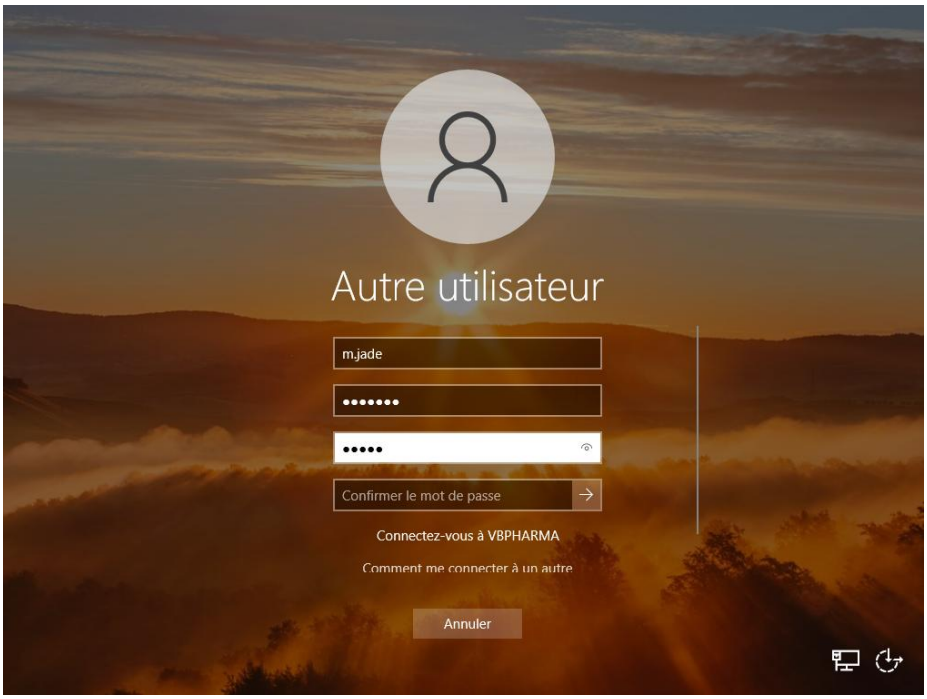
Configuration du poste de travail de bureau, intégration au domaine

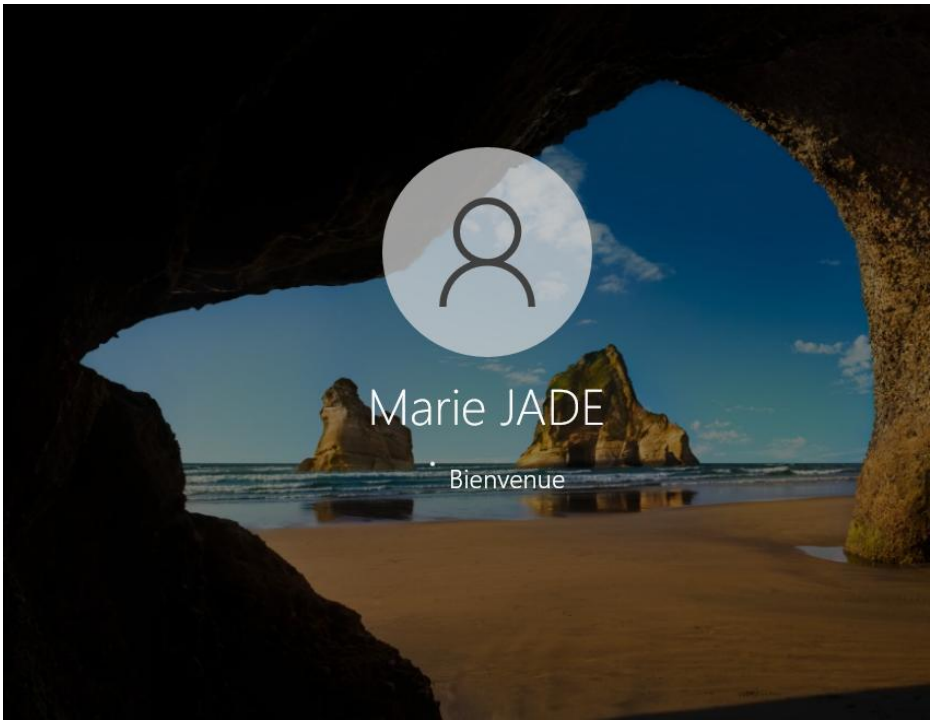
Pour sa configuration, je choisi de l'intégrer au domaine vbpharma.





Ensuite je me suis connecté avec L'utilisateur du domaine, Marie JADE. Comme configurer dans mon Active Directory, le mot de passe doit être changer lors de la première connexion, et doit respecter les spécificités des bonnes pratiques en termes de choix de mots (8 caractères, majuscules, chiffres, et caractères spéciaux au minimum)





Installation de Dolibarr sur ma Debian 13

Commande :

4- Installation de docker compose

- Sudo apt update
- Sudo apt install docker.io docker-compose -y

Vérification

- docker --version
- docker compose version

5- Création des dossiers et fichiers

Création du dossier dolibarr

- mkdir ~/dolibarr
- cd ~/dolibarr

Création du fichier docker-compose.yml

- nano docker-compose.yml

Coller ceci

```
version: '3.8'


services:
 mariadb:
  image: mariadb:10.6
  container_name: dolibarr_db
  restart: always
  environment:
   MYSQL_ROOT_PASSWORD: rootpassword
   MYSQL_DATABASE: dolibarr
   MYSQL_USER: dolibarr
   MYSQL_PASSWORD: dolibarrpassword
```

```
  volumes:
    - db_data:/var/lib/mysql
  dolibarr:
   image: dolibarr/dolibarr:latest
   container_name: dolibarr_app
   restart: always
   depends_on:
    - mariadb
   environment:
    DOLI_DB_HOST: mariadb
    DOLI_DB_NAME: dolibarr
    DOLI_DB_USER: admin
    DOLI_DB_PASSWORD: *********
   ports:
    - "8080:80"
   volumes:
    - dolibarr_documents:/var/www/documents
    - dolibarr_custom:/var/www/html/custom
volumes:
  db_data:
  dolibarr_documents:
  dolibarr_custom:
```

6- Lancer dolibarr

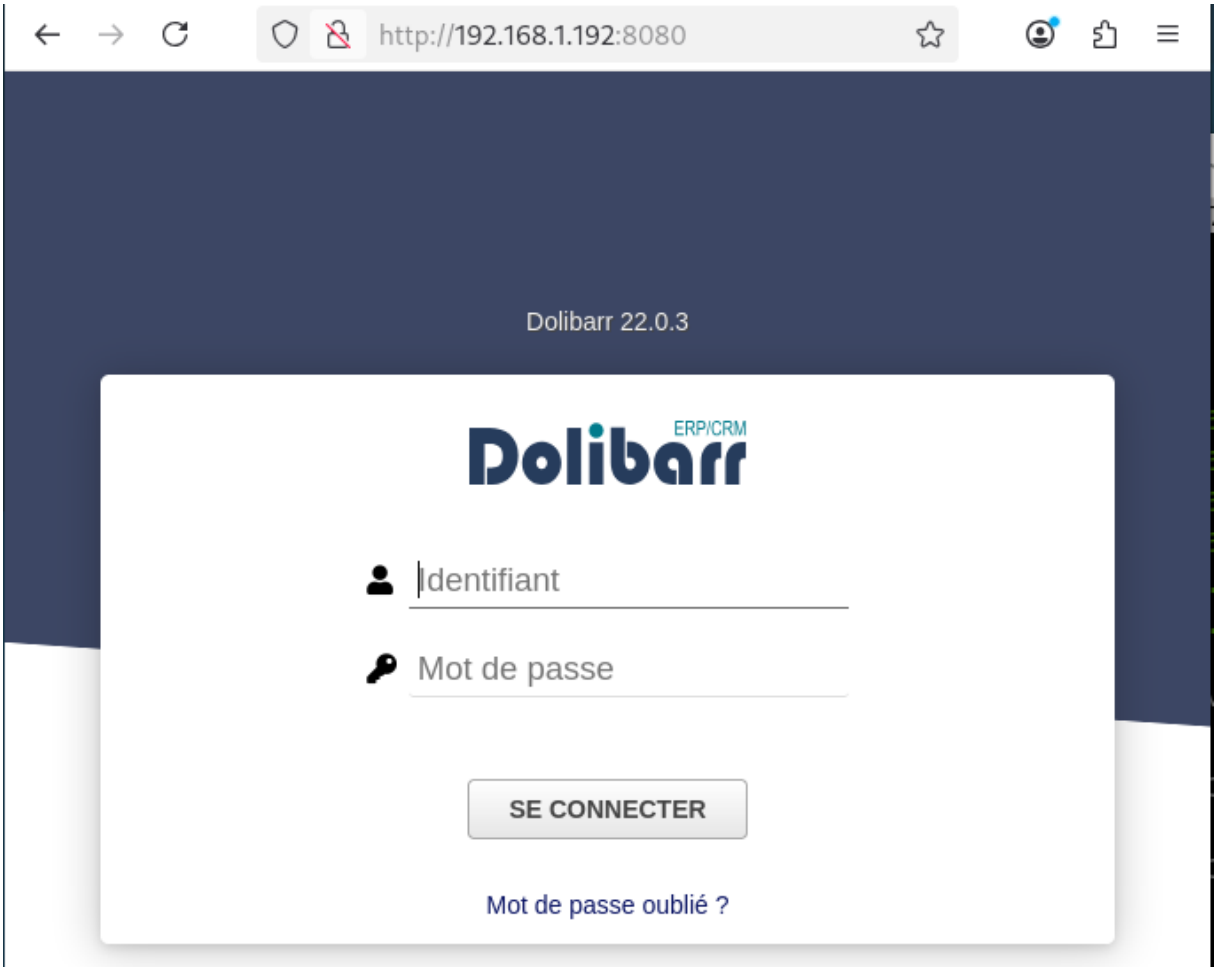
- docker compose up -d

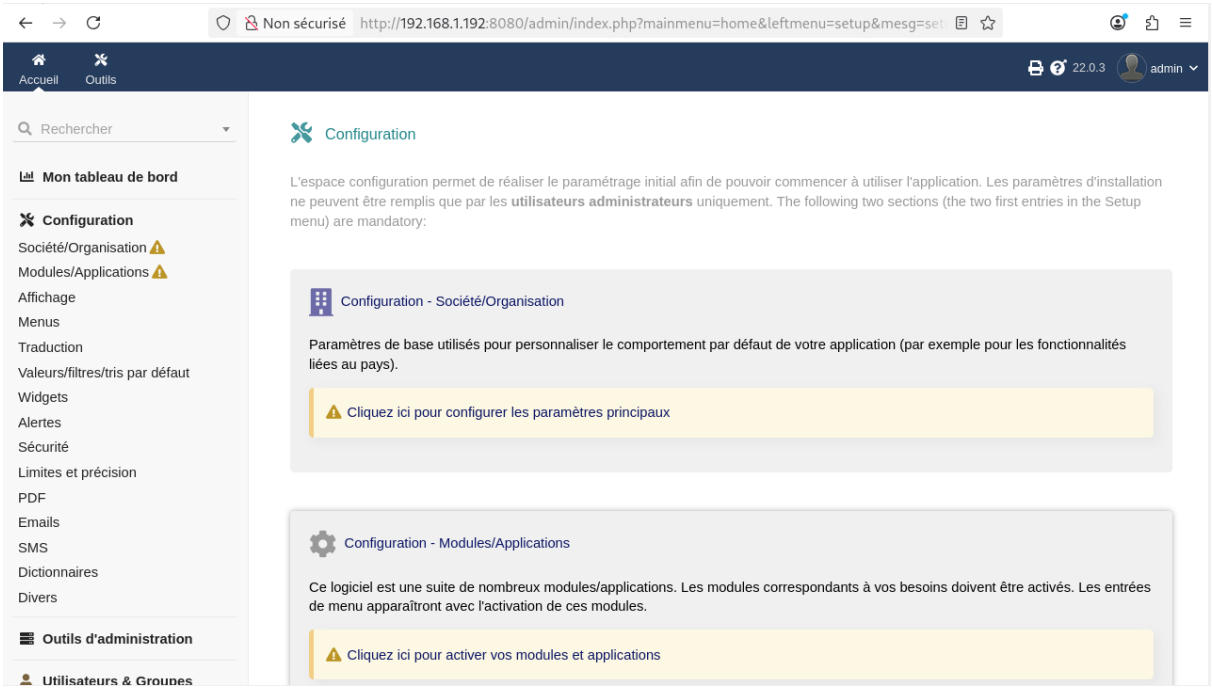
verification

- docker ps

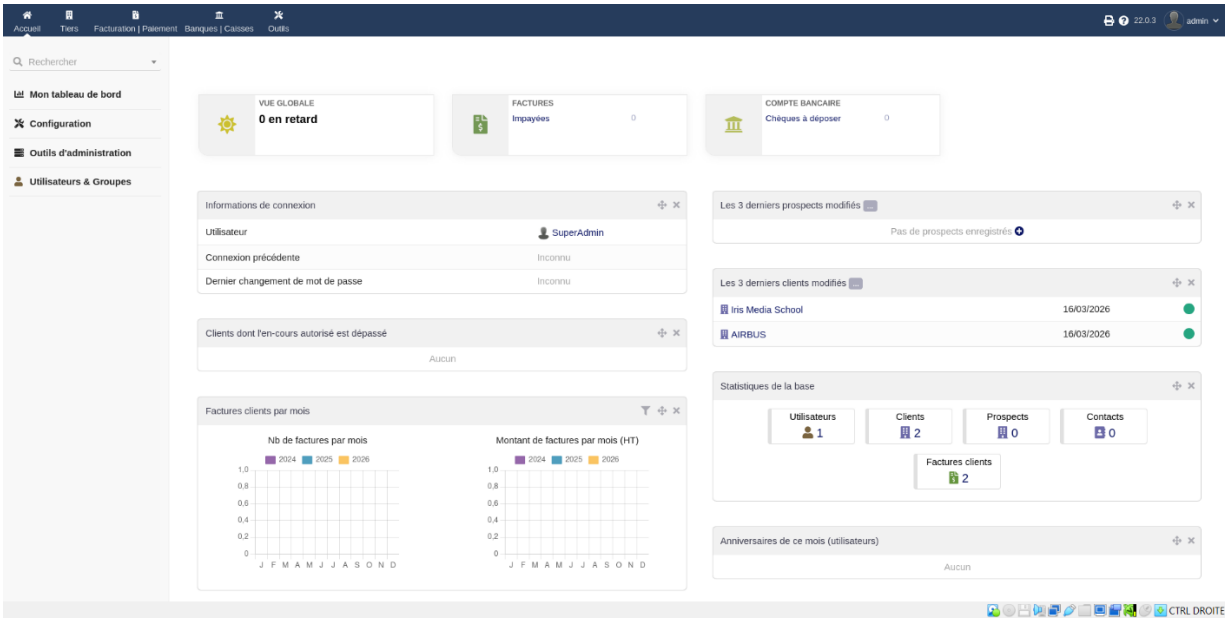
7- Accéder à l'interface

Accéder à l'interface web via le navigateur en : **http://192.168.1.30:8080**

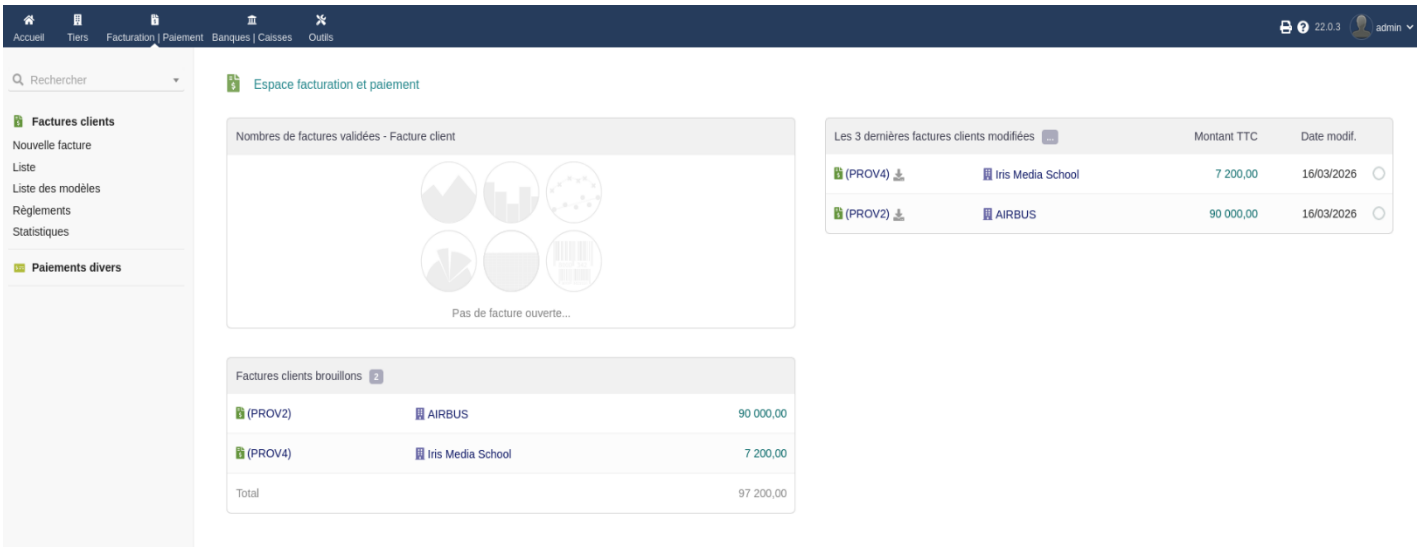




Configuration de société/Organisation & Modules/Applications



Création de tiers et de factures


Accueil
Tiers
Facturation | Paiement
Banques | Caisses
Outils
22.0.3
admin
Rechercher
Factures clients
Nouvelle facture
Liste
Liste des modèles
Règlements
Statistiques
Paiements divers
Espace facturation et paiement
Nombres de factures validées - Facture client
Pas de facture ouverte...
Factures clients brouillons 2
(PROV2) AIRBUS 90 000,00
(PROV4) Iris Media School 7 200,00
Total 97 200,00
Les 3 dernières factures clients modifiées ...
Montant TTC
Date modif.
(PROV4) Iris Media School 7 200,00 16/03/2026
(PROV2) AIRBUS 90 000,00 16/03/2026

VBPHARMA

Facture (PROV2) - Non validé

Date facturation : 16/03/2026
Date échéance : 15/04/2026
Code client : CU2603-00001

Émetteur

VBPHARMA
31000 Toulouse

Adressé à

AIRBUS
31000 Toulouse

Catégorie d'opérations : Mixte - Livraison de biens & prestation de services

Montants exprimés en Euros

Désignation	TVA	P.U. HT	Qté	Total HT
Licence logiciel	20%	70 000,00	1	70 000,00
Service client premium	20%	5 000,00	1	5 000,00

Conditions de règlement: Règlement à 30 jours

Total HT	75 000,00
Total TVA 20%	15 000,00
Total TTC	90 000,00

Un mode de paiement a été défini de type VIR mais la configuration du module Facture n'a pas été complétée pour définir les informations affichées pour ce mode de paiement.

Installation de la Backup server

Installer rsync sur la vm dolibarr

Sudo apt update

Sudo apt install rsync openssh-client -y

Installer rsync sur la vm backup server

Sudo apt update

Sudo apt install rsync openssh-server -y

Se connecter à la vm backup server via ssh :

Ssh user-backup@192.168.1.20

Créer le dossier de backup

Mkdir -p /home/user-backup/backups/dolibarr

Chown user-backup:user-backup /home/user-backup/backups/dolibarr

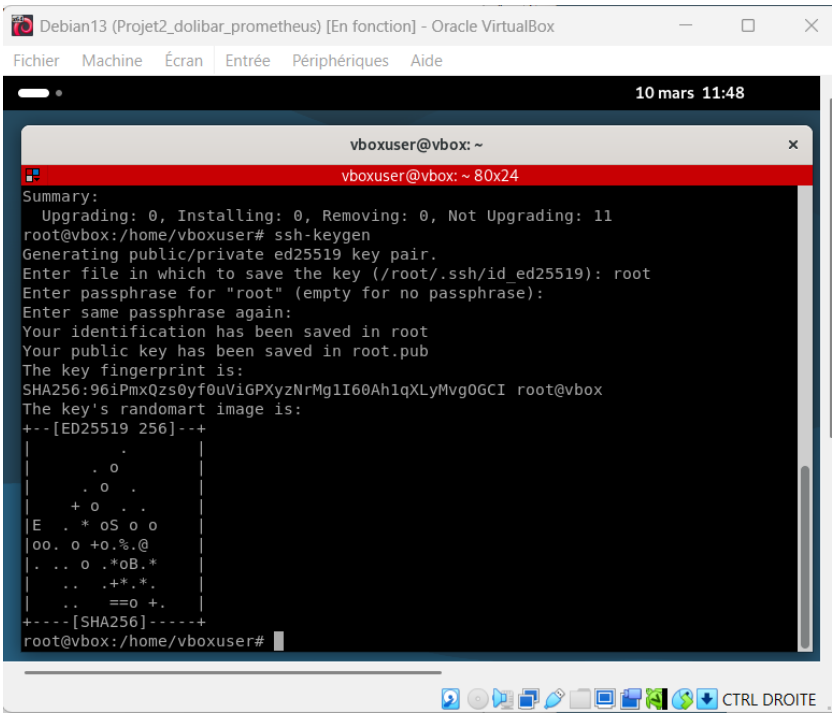
Chmod 700 /home/user-backup/backups/dolibarr

exit

Sur la vm dolibarr

Copier la clef ssh

Ssh-keygen -f "/root/.known_hosts" -R "192.168.1.20"



Puis tester pour accepter la nouvelle clef

Ssh user-backup@192.168.1.20

Exit

Etape clef sauvegarde backup

Docker ps

Si les conteneurs son arrêter

Docker start dolibarr-db

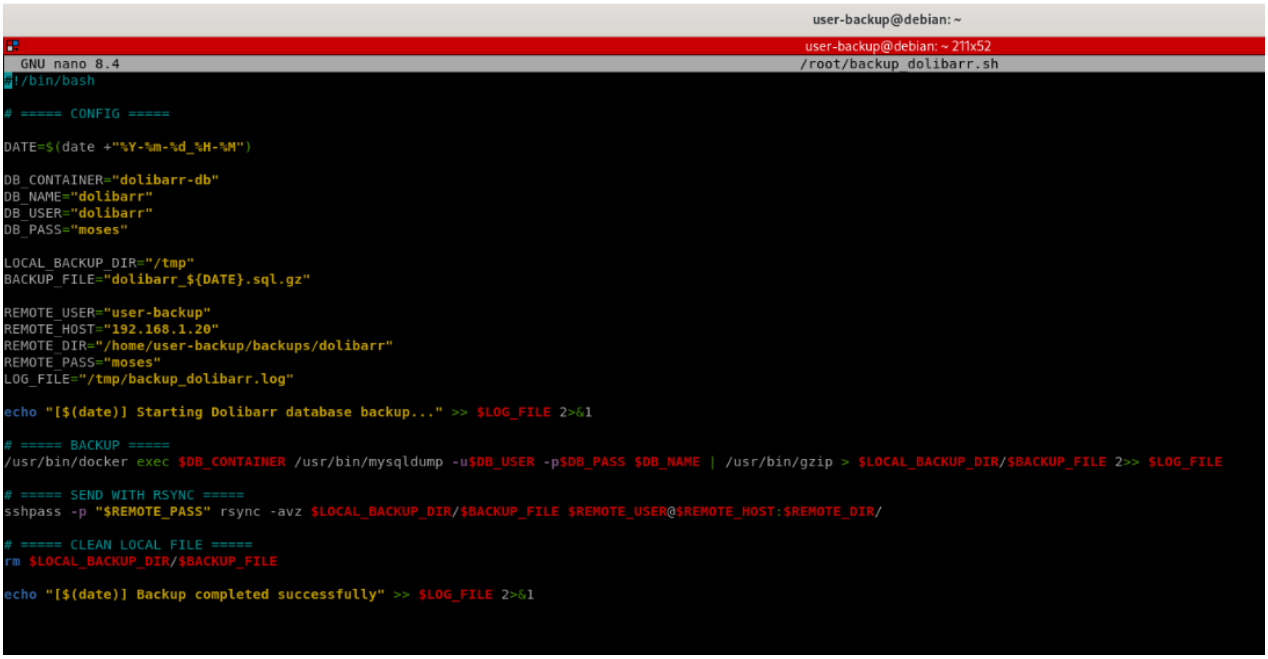
Docker start dolibarr

Docker ps

Creer le dossier script

Nano /home/vboxuser/backup_dolibarr.shh

Coller le script dans le fichier



Rendre le script exécutable

Chmod +x /home/vboxuser/backup_dolibarr.sh

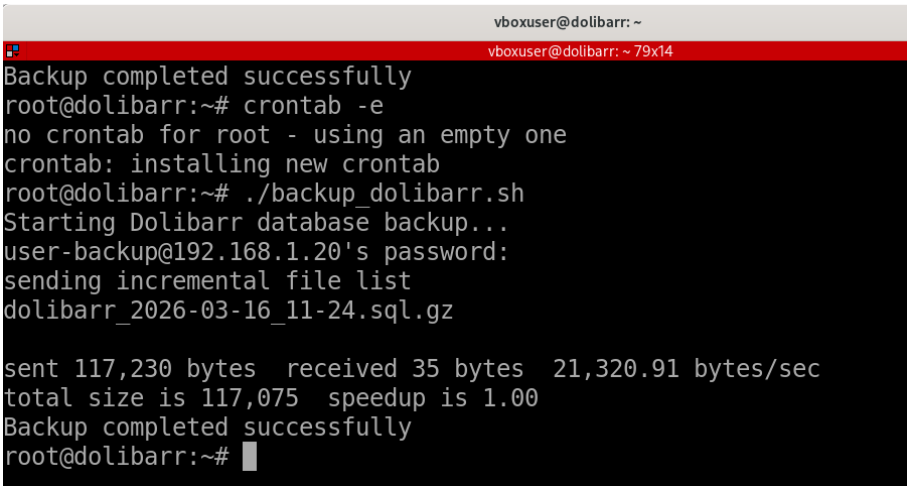
Tester le script

Se connecter en root dolibarr

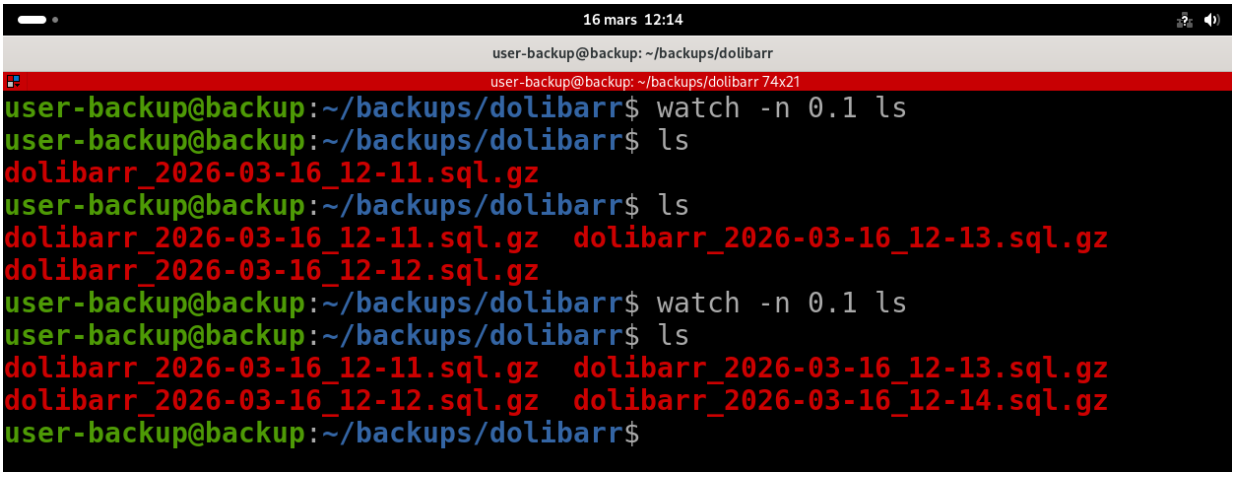
Su –

Commande pour exécuter le script

./backup_dolibarr.sh

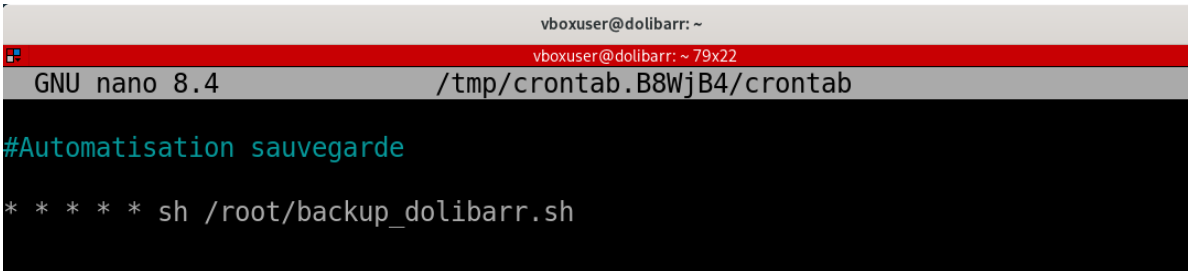


Vérifier sur la vm backup dans le dossier dolibarr



Automatiser avec Cron et tester la sauvegarde chaque minute

Crontab -e

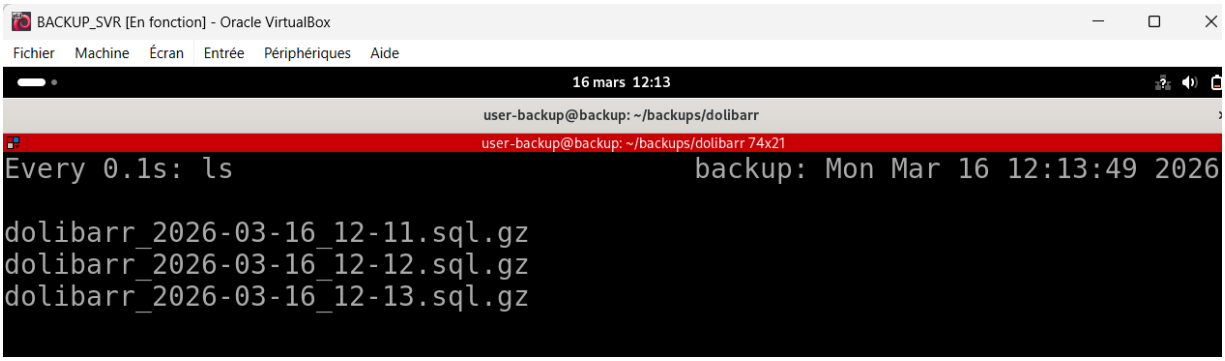


Vérifier sur le backup server

Commande

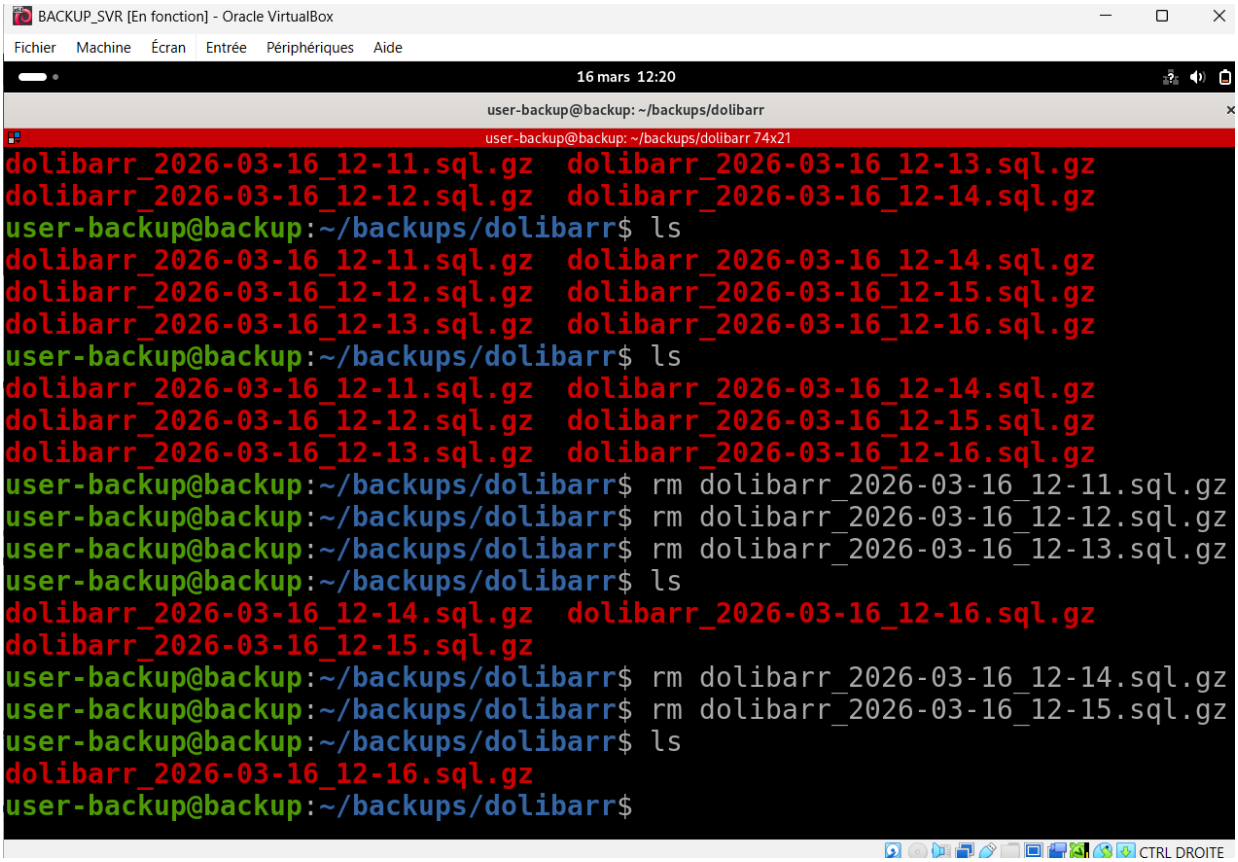
Watch -n 0.1 ls

Elle permet de surveiller en temps réel les changements dans un dossier (création, suppression, modification de fichiers) avec une mise à jour 10 fois par seconde

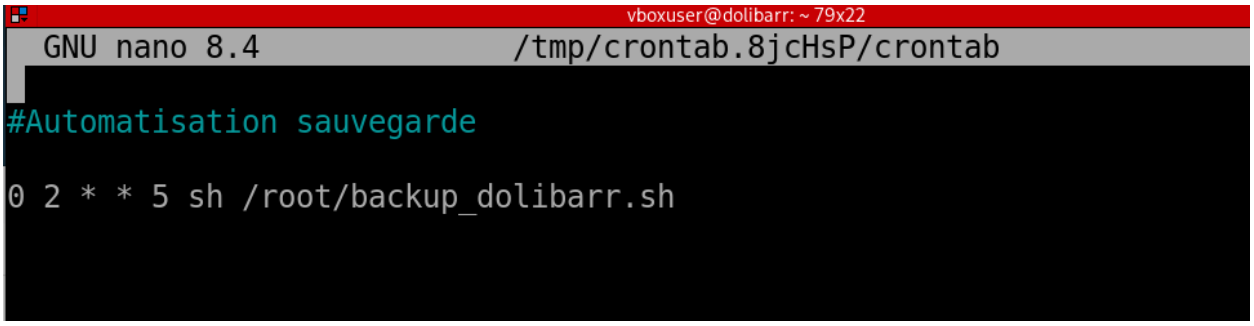


Commande

Ls



Modifier le crontab et programmer une sauvegarde tous les vendredis à 2h



Installation de Prometheus sur ma Debian 13

Commande :

1- **Création du dossier Prometheus**

- mkdir -p /opt/prometheus
- cd /opt/prometheus

2- **Création du fichier de configuration Prometheus**

nano prometheus.yml

Coller ceci

global :

scrape_interval :15s

scrape_configs :

-job_name : ‘prometheus’

static-configs :

-targets : [‘localhost :9090’]

3- **Lancer prometheus**

Docker run -d \

--name=prometheus \

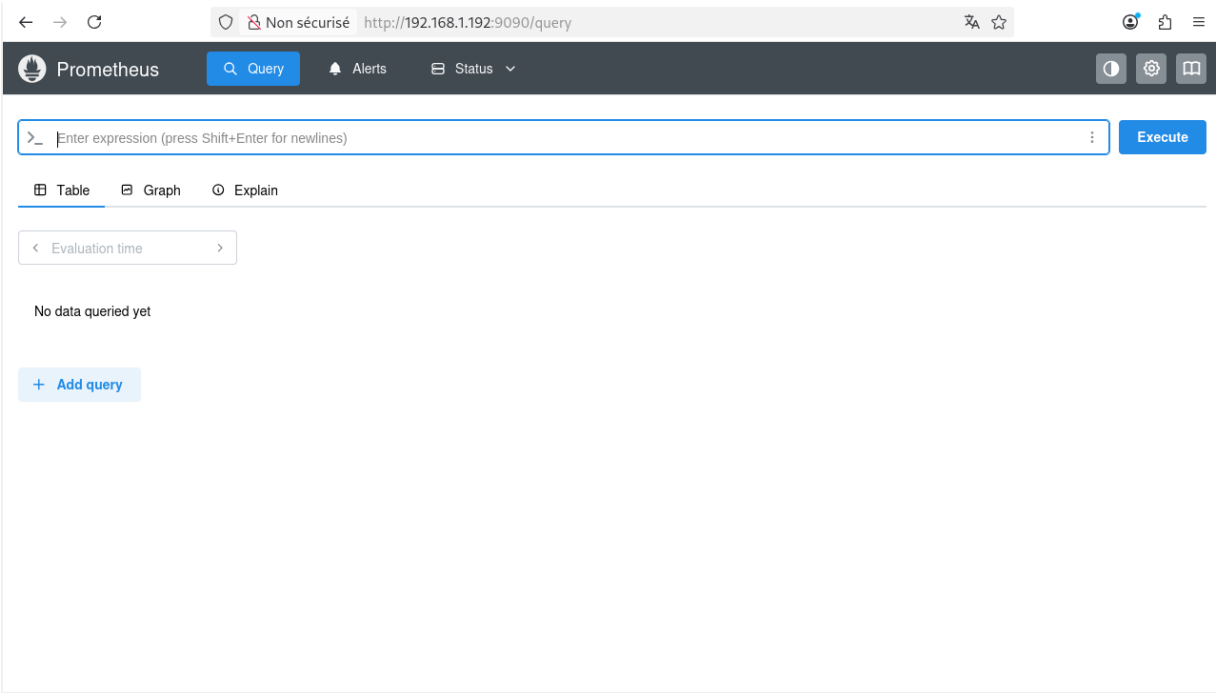
-p 9090 :9090

-v /opt/prometheus/prometheus.yml:/etc/prometheus/prometheus.yml \

Prom/prometheus

4- **Accéder à l’interface web**

Accéder à l’interface web via le navigateur en : **http://192.168.1.30:9090**



5- Remonter des servers

A- Outil de type linux

Installation de **Node Exporter** (binaire officiel).

Le service expose les métriques sur **port 9100**.

Sudo apt install prometheus-node-exporter

```
root@debian:/home/backup-server# systemctl status prometheus-node-exporter
● prometheus-node-exporter.service - Prometheus exporter for machine metrics
     Loaded: loaded (/usr/lib/systemd/system/prometheus-node-exporter.service; enabled; preset:
     Active: active (running) since Sun 2026-03-29 00:37:20 CET; 2min 6s ago
 Invocation: 27db46ccee2343609e397df848c016cf
       Docs: https://github.com/prometheus/node_exporter
   Main PID: 4732 (prometheus-node)
      Tasks: 6 (limit: 2280)
     Memory: 10.6M (peak: 11.1M)
        CPU: 2.616s
     CGroup: /system.slice/prometheus-node-exporter.service
             └─4732 /usr/bin/prometheus-node-exporter
```

B- Outil de type Windows

Prometheus ne peut pas interroger Windows directement, il faut un exporter.

Installation de **Windows Exporter** (MSI).

Choisir les collectors (CPU, RAM, disque, réseau...).

Le service expose les métriques sur **port 9182**.

Le Windows serveur core, n'est pas d'interface graphique, je vais procéder par un partage depuis l'Active directory de mon Windows server GUI.

Création du partage sur la Windows GUI

```
PS C:\WINDOWS\system32> Test-Path "\\192.168.1.90\C$\Temp"
False
PS C:\WINDOWS\system32> Copy-Item "C:\Users\Administrateur\Downloads\windows_exporter-0.31.3-amd64.msi" \\192.
168.1.90\C$\Temp
PS C:\WINDOWS\system32>
```

Sur la Windows core

```
PS C:\Users\Administrateur.VBPHARMA> New-Item -ItemType Directory -Path C:\Temp


    Répertoire : C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        29/03/2026     00:29                Temp


PS C:\Users\Administrateur.VBPHARMA> cd C:\Temp
>> msiexec /i windows_exporter-0.31.3-amd64.msi ENABLED_COLLECTORS="cpu,logical_disk,net,os" /quiet
PS C:\Temp>
PS C:\Temp> Get-Service windows_exporter
>> Start-Service windows_exporter
>> Get-Service windows_exporter

Status   Name               DisplayName
------   ----               -----------
Running  windows_exporter   windows_exporter
Running  windows_exporter   windows_exporter
```

C- Autre outil

Pour Opnsense, on va se connecter à son interface web, et installer l'Exporter dédier (**opnsense-exporter**)

OPNsense ne fournit pas nativement de métriques Prometheus.
Il faut utiliser un exporter externe comme **os-node-exporter** (Go), qui interroge l'API d'OPNsense.

Installation de **os-node-exporter** sur une machine (Linux ou Docker).

L'exporter expose les métriques sur **port 9101**.

D- Sur prometheus

Dans le terminal de l'hôte de prométhéums, on va éditer le fichier prometheus.yml.

Toute d'abord, se connecter en super utilisateur (root), et inspecter le conteneur prométhéums dans docker avec la commande :

Docker inspect prometheus

Il faut ensuite éteindre le conteneur prometheus avec la commande :

Docker stop prometheus

Il est impossible de modifier directement le fichier yml présent dans le conteneur prometheus, il faut alors copier le fichier

Ensuite, éditer le fichier

Nano /opt/prometheus/prometheus.yml

```
  GNU nano 8.4        /opt/prometheus/prometheus.yml *
global:
  scrape_interval: 15s

scrape_configs:
  - job_name: 'prometheus'
    static_configs:
      - targets: ['localhost:9090']

  - job_name: 'backup-server'
    static_configs:
      - targets: ['192.168.1.20:9100']

  - job_name: 'windows-server'
    static_configs:
      - targets: ['192.168.1.9:9182']

  - job_name: 'windows-server-core'
    static_configs:
      - targets: ['192.168.1.90:9182']
```

Puis remplacer le fichier dans le conteneur

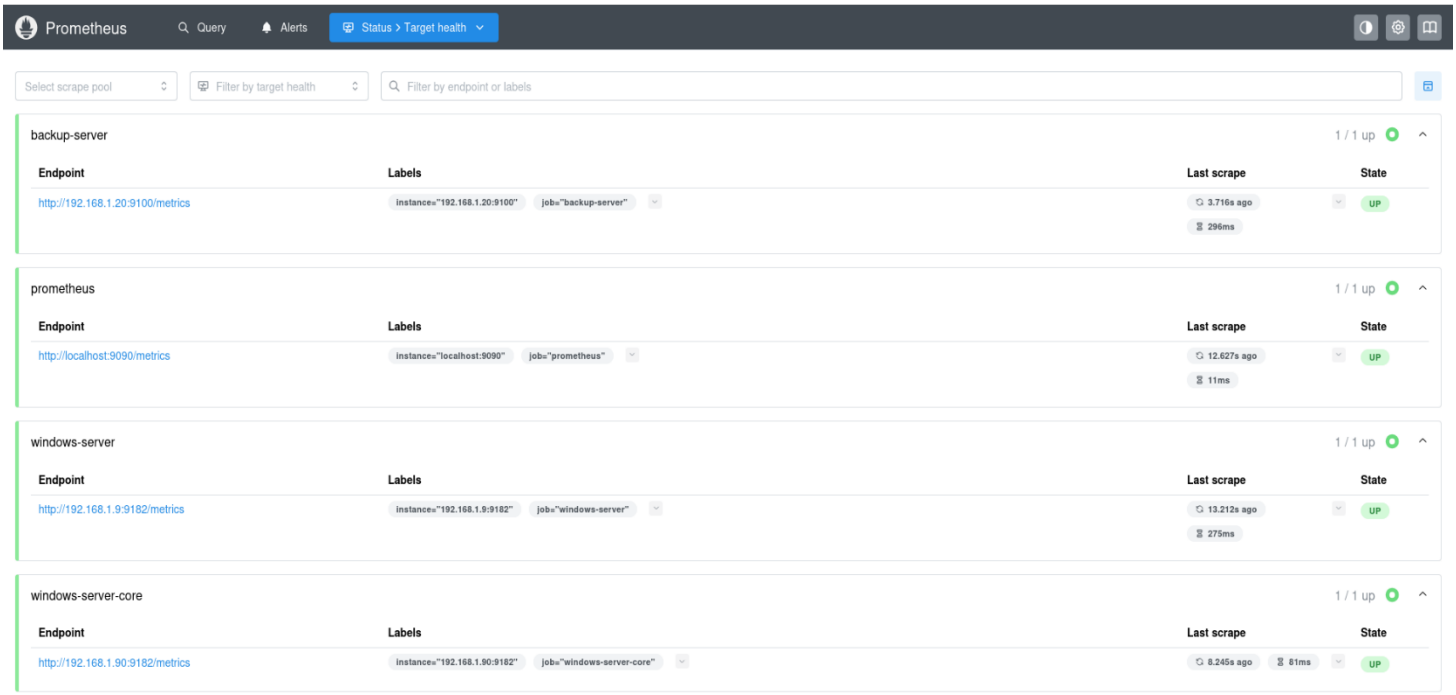
Enfin, relancer le conteneur avec la commande :

docker start prometheus

Ou

docker restart prometheus

En se reconnectant à l'interface web de prometheus, dans Status > Target health, on peut voir les servers remonter.

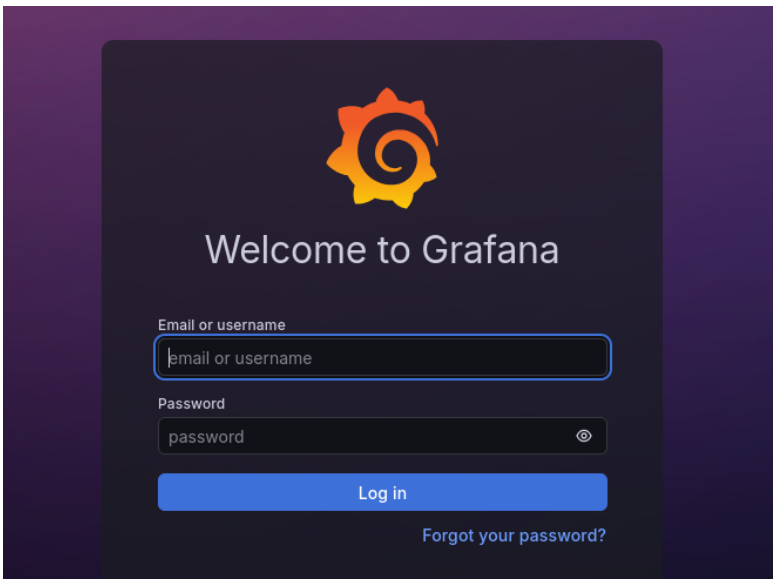

Prometheus
Query
Alerts
Status > Target health
Select scrape pool
Filter by target health
Filter by endpoint or labels
backup-server
1 / 1 up
Endpoint
Labels
Last scrape
State
http://192.168.1.20:9100/metrics
instance="192.168.1.20:9100"
job="backup-server"
3.716s ago
296ms
UP
prometheus
1 / 1 up
Endpoint
Labels
Last scrape
State
http://localhost:9090/metrics
instance="localhost:9090"
job="prometheus"
12.627s ago
11ms
UP
windows-server
1 / 1 up
Endpoint
Labels
Last scrape
State
http://192.168.1.9:9182/metrics
instance="192.168.1.9:9182"
job="windows-server"
13.212s ago
275ms
UP
windows-server-core
1 / 1 up
Endpoint
Labels
Last scrape
State
http://192.168.1.90:9182/metrics
instance="192.168.1.90:9182"
job="windows-server-core"
8.245s ago
61ms
UP

Installation de Grafana pour le Dashboard

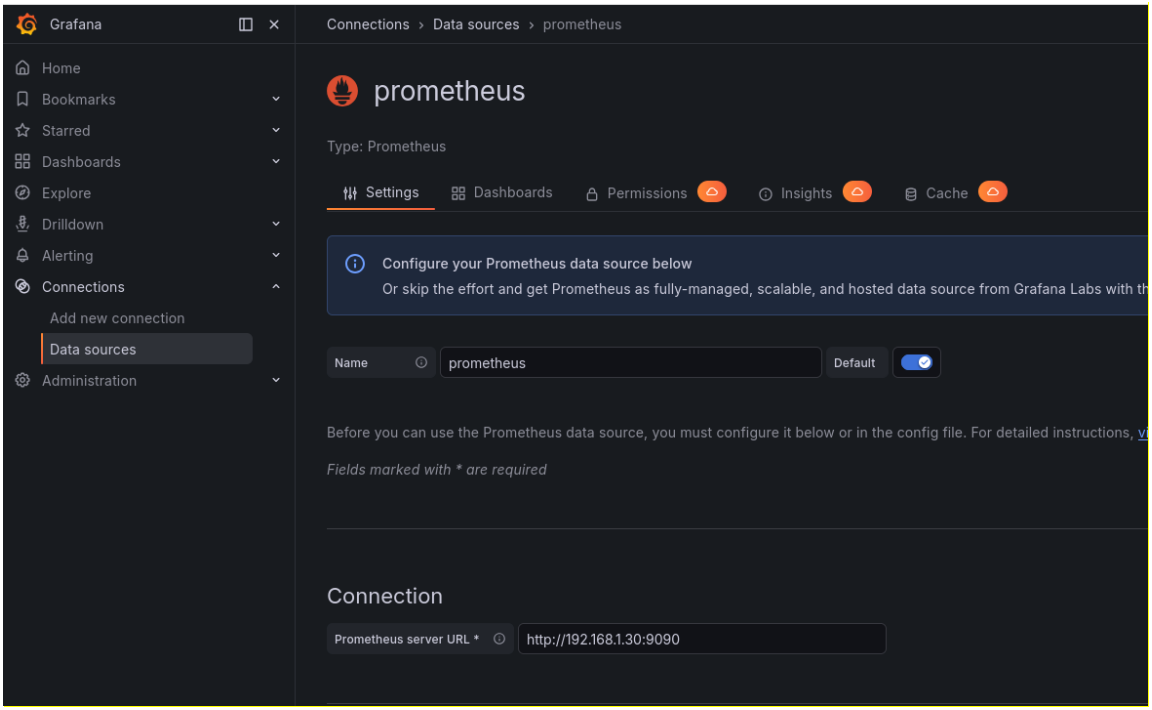
Commande

Docker run -d -p 3000 :3000 –name=grafana grafana/grafana

Connection à Grafana: **http://192.168.1.30:3000**

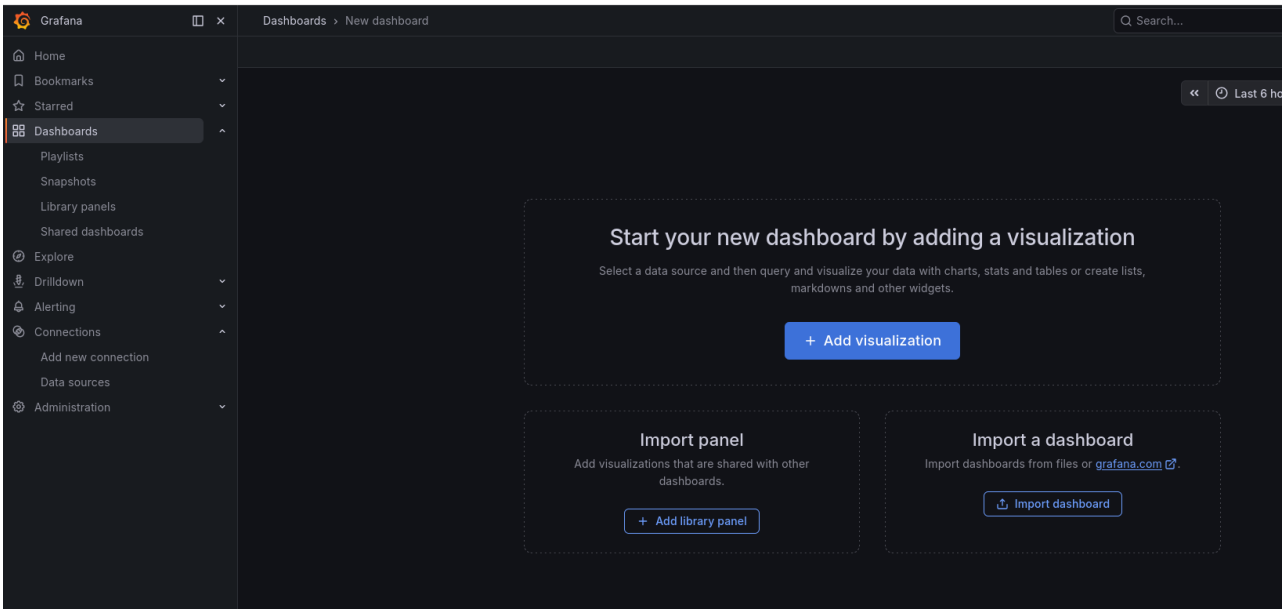


J’ai renseigné ma data sources avec l’url de connexion à Prometheus.

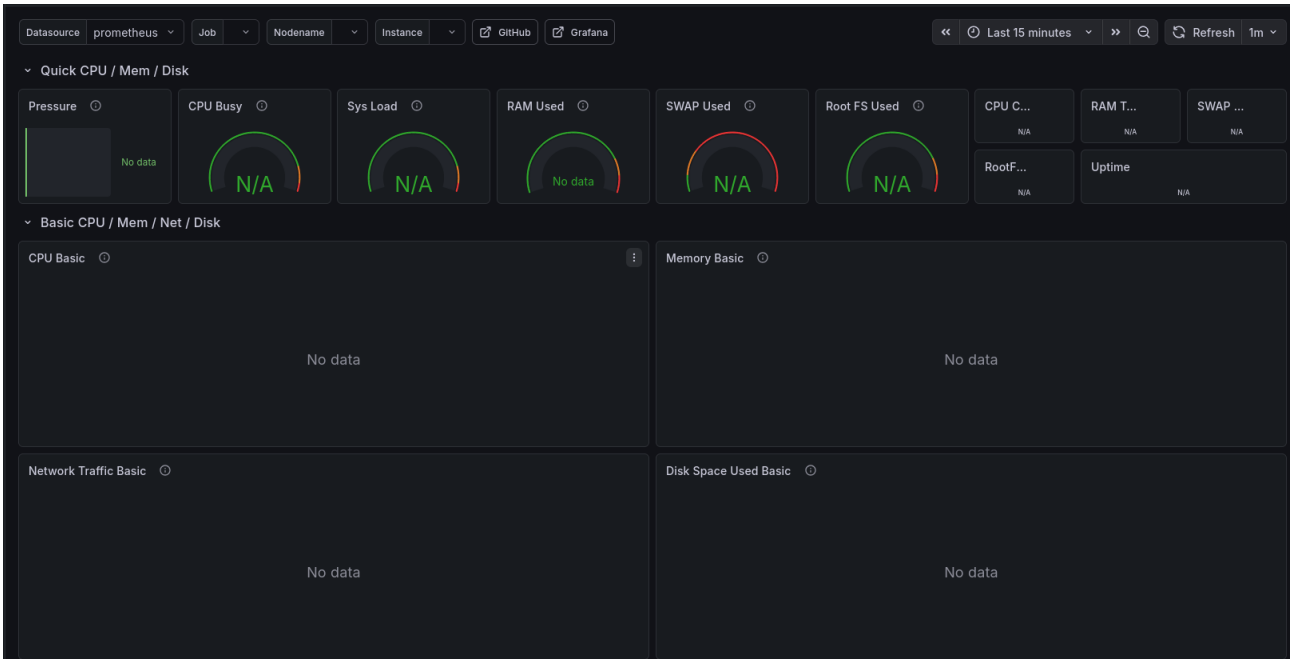


Sur le Dashboard, j’ai besoin de vois des données comme, l’utilisation **CPU**, **RAM**,

J’ai trouvé un Dashboard qui pouvais répondre à mes attentes, j’ai choisi d’importer ce Dashboard.



Sur ce dernier, je pourrais voir l’utilisation CPU, RAM, SWAP, ou encore Sys Load.



! Pourquoi être passer par Docker pour Dolibarr et prometheus ?

Passer par Docker pour installer Prometheus et Dolibarr sur une VM Debian a été la solution la plus propre, la plus rapide et la plus maintenable.

Docker apporte plusieurs avantages dont :

1. Isolation propre des services

Sans Docker, chaque service installe des dépendances, des versions spécifiques de bibliothèques, puis des fichiers de configuration un peu partout dans /etc, /var, /usr.

- Alors les services se marchent dessus
- Les mises à jour cassent des choses
- La VM devient difficile à maintenir.

Avec Docker :

- Chaque service tourne dans son propre environnement,
- Aucune dépendance n'est installée sur l'hôte,
- Aucune pollution du système.

2. Mises à jour plus simples et plus sûres

Prometheus et Dolibarr évoluent vite.
Sans Docker : mise à jour manuelle, risques de conflits, sauvegardes compliquées.

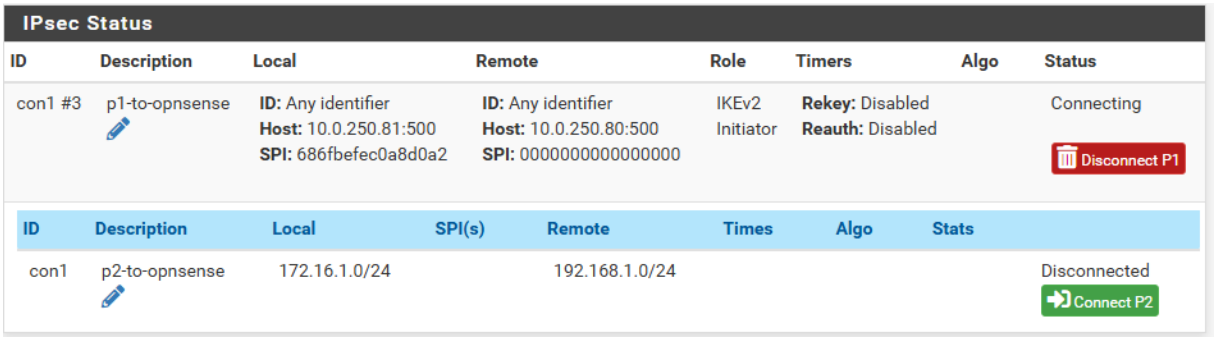
Avec Docker :

- Tu mets à jour en changeant une image (docker pull),
- Tu redémarres le conteneur,
- Si ça casse, tu reviens instantanément à l'ancienne version.

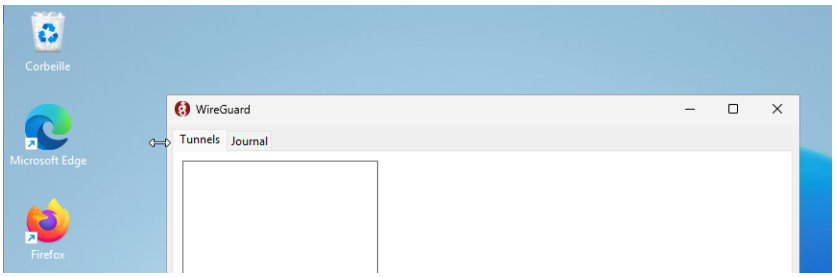
Pour résumer C'est beaucoup plus fiable, pour un technicien d'exploitation, c'est un énorme gain de temps.

Tests et validation

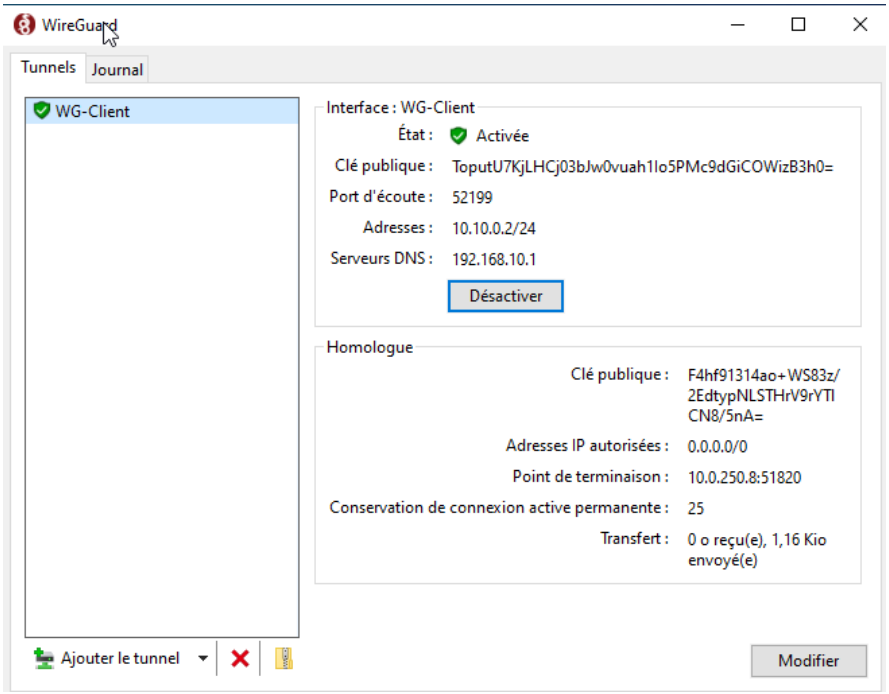
Teste VPN IP SEC :



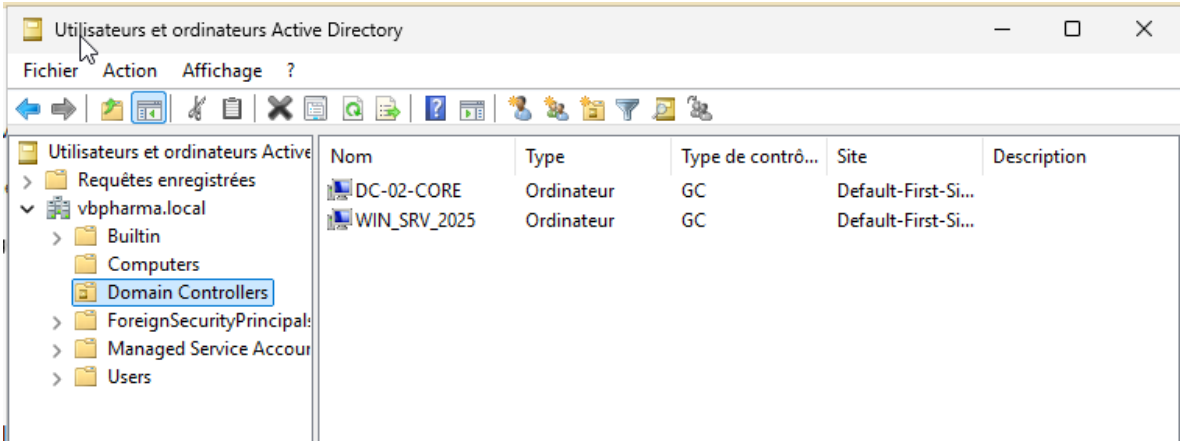
Teste GPO :



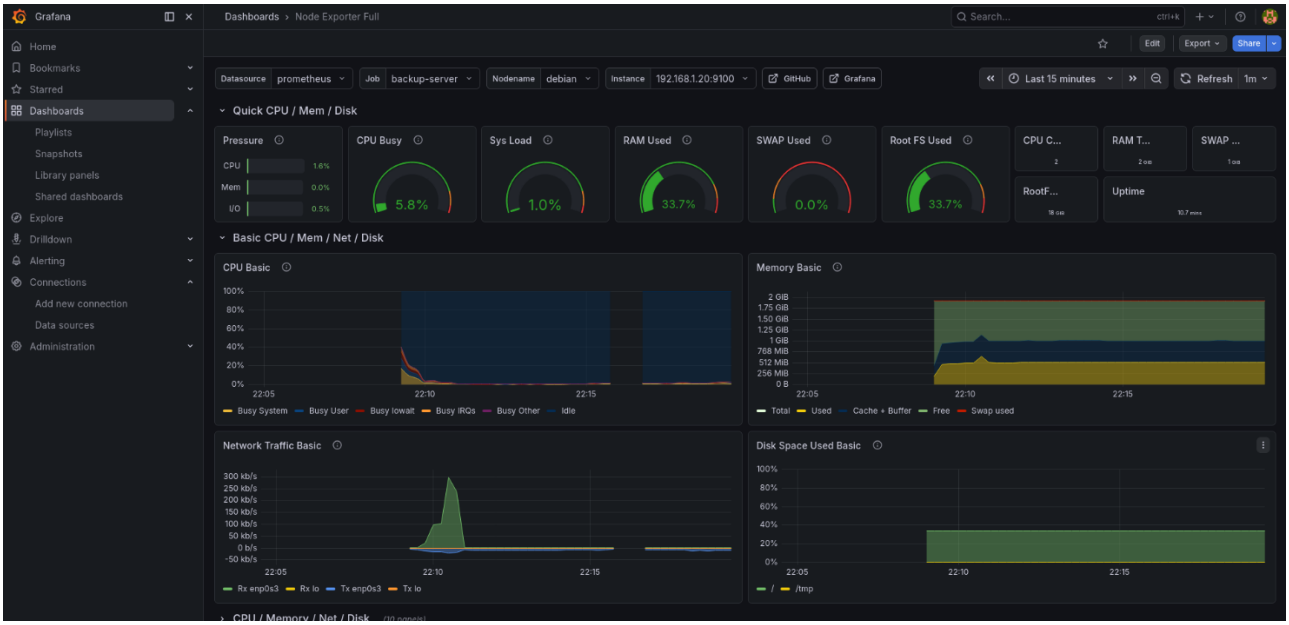
Teste VPN nomade :



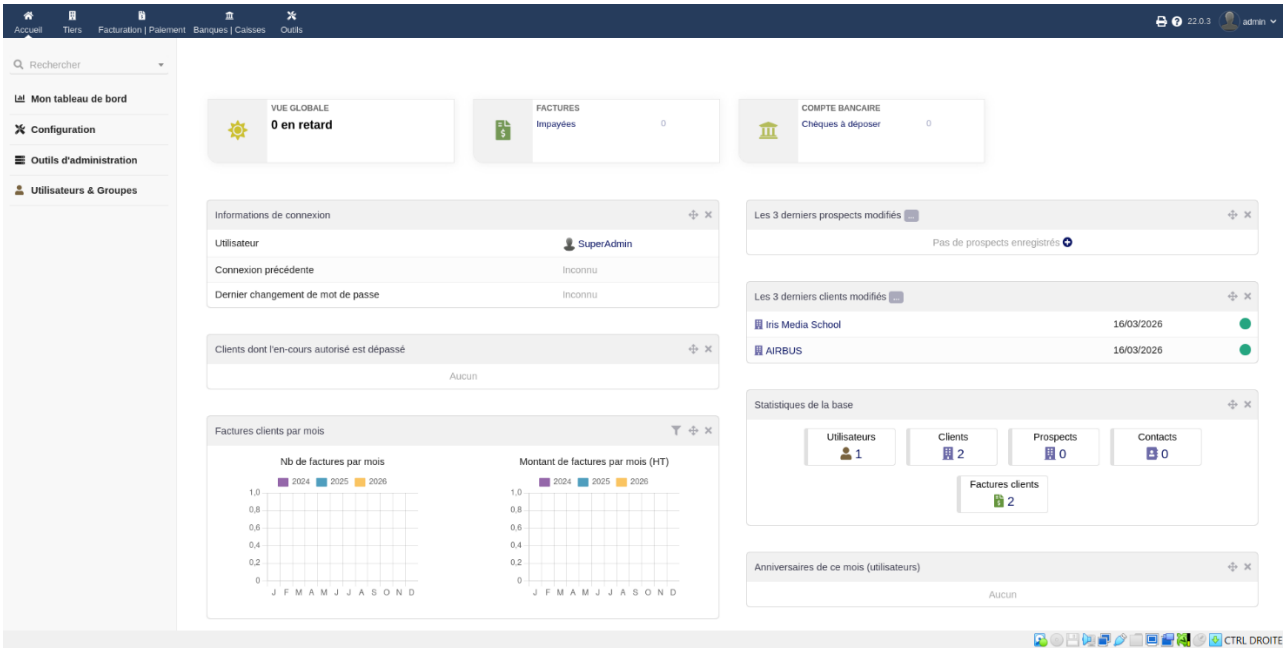
Teste réplication Active Directory :



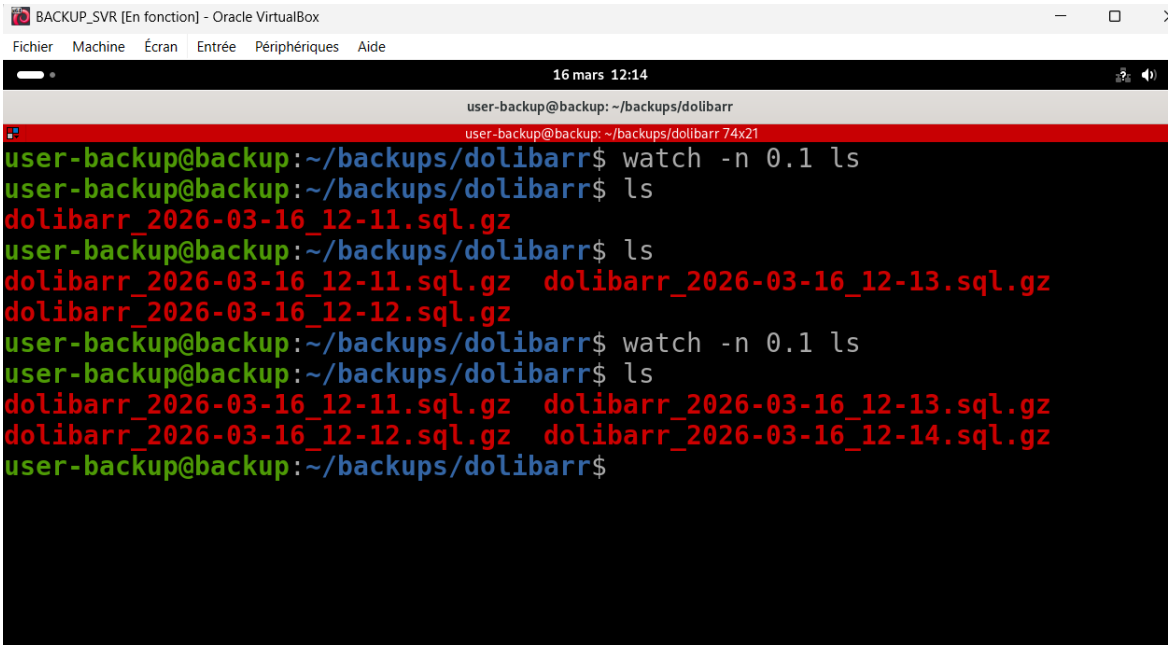
Teste Dashboard Prometheus avec Grafana :



Teste Dolibarr :



Teste Serveur Backup :



Exploitation et maintenance

Axes d’améliorations

Ce projet comporte néanmoins des axes d'amélioration. L'absence de redondance matérielle sur les équipements critiques constitue une limite de la solution actuelle. La mise en place d'un Plan de Reprise d'Activité formalisé, d'une solution SIEM pour la corrélation des logs de sécurité, ou encore l'intégration complète de GLPI pour la gestion du parc et du ticketing représentent des évolutions naturelles qui rendraient l'infrastructure encore plus robuste et conforme aux exigences d'un environnement de production réel.

Conclusion et perspectives.

Ce projet de mise en place d'une infrastructure informatique pour Vita Big Pharma m'a permis de concevoir et déployer une solution réseau complète, sécurisée et fonctionnelle dans un contexte multi-sites, en réponse à des besoins métiers concrets issus du secteur pharmaceutique.

D'un point de vue technique, j'ai pu mettre en œuvre un large éventail de compétences propres au bloc SISR. La configuration du pare-feu OPNsense, la mise en place du VPN IPsec site à site entre Toulouse et Marseille, ainsi que le VPN nomade WireGuard pour le télétravail, m'ont permis d'appréhender concrètement les enjeux de la sécurisation des communications sur un réseau étendu. Le déploiement de l'Active Directory sur Windows Server 2025, avec réplication vers un contrôleur de domaine secondaire sous Windows Server Core, m'a confronté aux problématiques réelles d'administration centralisée et de haute disponibilité des services d'annuaire. La mise en place de Dolibarr comme ERP d'entreprise, couplée à une solution de sauvegarde automatisée via rsync et crontab, a renforcé ma compréhension des enjeux de continuité de service et de protection des données, en lien direct avec les exigences du RGPD. Enfin, le déploiement de Prometheus et Grafana m'a initié aux pratiques de supervision moderne, permettant une visibilité en temps réel sur l'état des serveurs et des ressources systèmes.

Sur le plan organisationnel, ce projet m'a appris à structurer mon travail selon une démarche de projet rigoureuse : analyse des besoins, étude de solutions, rédaction d'un cahier des charges, mise en œuvre, puis phase de tests et de validation. J'ai également dû faire face à plusieurs incidents techniques, notamment lors de la configuration du tunnel IPsec ou de la réplication Active Directory, ce qui m'a permis de développer une méthodologie de diagnostic et de résolution de problèmes que je considère essentielle dans le métier de technicien informatique.

Au-delà des aspects techniques, ce projet m'a appris à ne pas me décourager face aux obstacles : certaines configurations ont nécessité de nombreuses heures de recherche et de tests avant de fonctionner, et c'est précisément dans ces moments-là que j'ai le plus progressé.

En conclusion, ce projet m'a donné l'opportunité de mobiliser et d'approfondir l'ensemble des compétences techniques et organisationnelles attendues dans le cadre du BTS SIO option SISR, tout en me préparant aux réalités du terrain que je rencontrerai dans ma vie professionnelle.