Projet 2 BTS SIO SISR

Conception, déploiement et exploitation d'une infrastructure réseau sécurisée
Entreprise : Vita Big Pharma
Site : Marseille
Étudiant : Zakariyae Outouil
Session 2026

Sommaire

1. Présentation de l’entreprise

Vita Big Pharma est une entreprise pharmaceutique spécialisée dans la fabrication de compléments alimentaires. Dans le cadre de son développement national, l'entreprise dispose de deux sites géographiques :

- Toulouse : siège administratif (Direction, Ressources Humaines, Finance)
- Marseille : site technique (Support informatique, Service technique)

Dans le cadre de ce projet, j'ai été chargé de concevoir et déployer l'infrastructure du site de Marseille. Le site de Toulouse est présent dans le contexte de l'entreprise afin de représenter une architecture multi-sites, mais il n'entre pas dans le périmètre de ma réalisation. Mon travail porte sur la mise en place des services réseau, de l'Active Directory, de la sécurité, de la supervision et de l'administration du site de Marseille.

Direction Générale	Supervision des deux sites
Site Toulouse	Direction / RH / Finance
Direction	Administration
Ressources Humaines	Gestion du personnel
Finance	Comptabilité

Site Marseille	Site technique
Support informatique	Gestion des incidents et assistance
Service technique	Exploitation et maintenance

2. Analyse du besoin

2.1 Besoins

Vita Big Pharma souhaite disposer d'une infrastructure informatique sécurisée et centralisée pour son site de Marseille.

L'entreprise doit permettre :

- L'authentification centralisée des utilisateurs ;
- La gestion des droits par groupes ;
- Le partage sécurisé des fichiers ;
- L'utilisation d'outils métiers comme GLPI ;
- L'administration et la supervision de l'infrastructure ;
- La sécurisation des accès réseau ;
- Le télétravail via VPN ;
- La sauvegarde des données et des services.

2.2 Contraintes

Pour répondre à ces besoins, plusieurs contraintes doivent être respectées :

- Séparation des réseaux serveurs et collaborateurs ;
- Contrôle des accès utilisateurs ;
- Sécurisation des communications réseau ;
- Mise en place d'un pare-feu ;
- Application d'une politique de mot de passe renforcée ;
- Sauvegardes régulières ;
- Respect des bonnes pratiques de sécurité et du RGPD.

2.3 Objectifs du projet

L'objectif est de mettre en place une infrastructure fiable permettant d'assurer la disponibilité des services, la sécurité des données et une administration centralisée du site de Marseille.

3. Étude des solutions

Afin de répondre aux besoins de sécurité, d'administration et de supervision, plusieurs solutions ont été étudiées.

3.1 Pare-feu

Critères	**OPNsense**	**pfSense**
Prix	Gratuit, open-source	Gratuit, open-source
Virtualisation	Compatible (Proxmox, VMware, VirtualBox)	Compatible (Proxmox, VMware, VirtualBox)
Sécurité	Basé sur HardenedBSD, mises à jour fréquentes	Basé sur FreeBSD, solution très mature
Evolutivité	Architecture modulaire via plugins	Extensions via packages
VPN IPsec	Support natif IPsec	Support natif IPsec
VPN OpenVPN	OpenVPN intégré	OpenVPN intégré
Intégration AD	Authentification via LDAP / RADIUS	Authentification via LDAP / RADIUS

Solution retenue : OPNsense

OPNsense a été retenu pour son interface intuitive, sa compatibilité avec les environnements virtualisés et ses fonctionnalités intégrées de sécurité, VPN et gestion de bande passante.

3.2 Annuaire et authentification

Solution	Avantages	Inconvénients
Active Directory	Standard en entreprise, gestion centralisée	Nécessite Windows Server
OpenLDAP	Open source	Administration plus complexe

Solution retenue : Active Directory
Active Directory permet la centralisation des utilisateurs, groupes et stratégies de sécurité.

3.3 Supervision

Solution	Avantages	Inconvénients
Prometheus	Open source, métriques détaillées	Configuration plus technique
Centreon	Interface complète	Plus lourd à deployer

Solution retenue : Prometheus
Prometheus a été retenu afin de superviser les ressources système des serveurs et détecter rapidement les incidents.

3.4 Gestion des incidents

Solution	Avantages	Inconvénients
GLPI	Inventaire, tickets, AD	Configuration initiale
OSTicket	Simple	Moins complet

Solution retenue : GLPI
GLPI permet la gestion des incidents, l'inventaire du parc et l'organisation du support informatique.

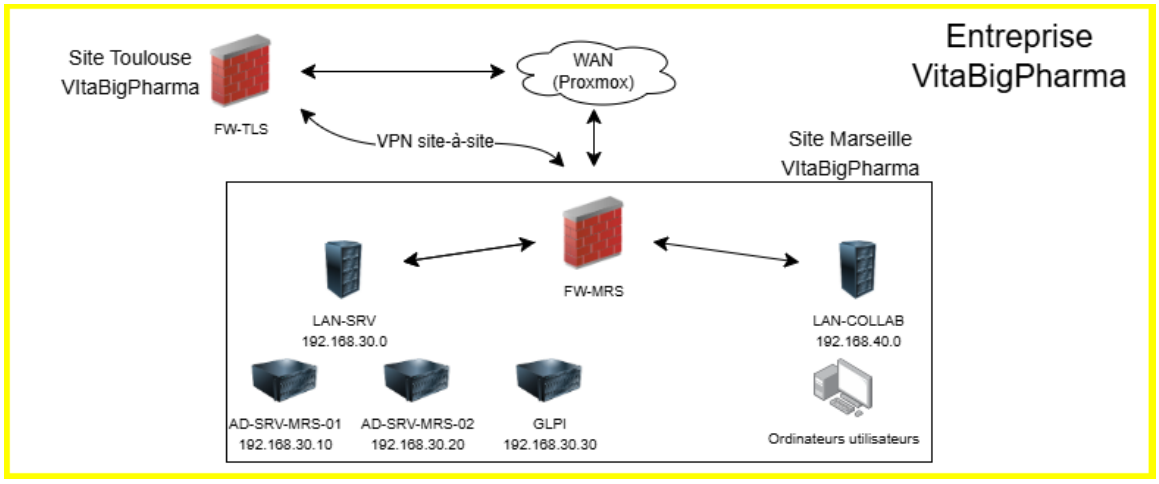
4. Architecture technique retenue

4.1 Présentation de l'architecture

L'infrastructure mise en place repose sur un site principal situé à Marseille. L'ensemble des services est hébergé dans un environnement virtualisé.
L'architecture est composée :

- D'un pare-feu OPNsense ;
- D'un réseau Serveurs ;
- D'un réseau Collaborateurs ;
- D'un contrôleur de domaine Active Directory ;
- D'un serveur de fichiers ;
- D'un serveur GLPI ;
- D'outils de supervision et d'administration.

Les réseaux sont séparés afin d'améliorer la sécurité et de limiter les accès aux ressources critiques.



4.2 Plan d'adressage

MRS-FW-01 WAN	10.34.60.51	Interface WAN
MRS-LAN-SRV	192.168.30.0	Réseau LAN-SRV
MRS-LAN-COLLAB	192.168.40.0	Réseau LAN-COLLAB
MRS-LAN-ADMIN	192.168.100.0	Réseau LAN-ADMIN
MRS-SRV-AD-01	192.168.30.10	Domain Controller/AD/DNS
MRS-SRV-AD-02	192.168.30.20	Domain Controller/AD/DNS
MRS-SRV-GLPI	192.168.50.30	Serveur GLPI
MRS-ADMIN-PC-01	192.168.100.10	Poste d'administration

4.3 Plan de nommage

MRS-FW-01	Pare-feu du réseau
MRS-LAN-SRV	Réseau pour les serveurs
MRS-LAN-COLLAB	Réseau pour les collaborateurs
MRS-LAN-ADMIN	Réseau pour l'administration
MRS-SRV-AD-01	Contrôleur de domaine principal
MRS-SRV-AD-02	Contrôleur de domaine secondaire
MRS-SRV-GLPI	Serveur GLPI
MRS-ADMIN-PC-01	Poste d'administration

4.4 Services déployés

OPNsense	Sécurité réseau
Active Directory	Gestion des utilisateurs
DNS	Résolution de noms
Glpi	Gestion des incidents
VPN	Accès sécurisé
Serveur de fichiers	Partage des données
Prometheus	Supervision
Sauvegardes	Protection des données

5. Mise en œuvre

5.1 OPNsense

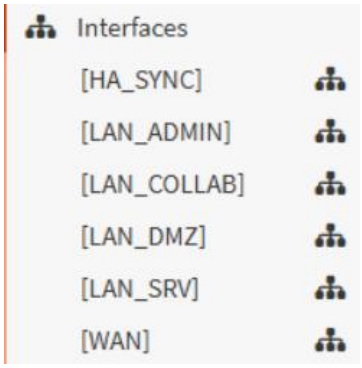
Objectif

Afin de sécuriser l'infrastructure du site de Marseille, un pare-feu OPNsense a été déployé. Celui-ci permet la segmentation des réseaux, le contrôle des flux réseau ainsi que la limitation de bande passante sur le réseau collaborateurs.

Configuration des interfaces

Les interfaces suivantes ont été configurées :

- WAN : accès au réseau externe
- LAN_SRV : réseau serveurs
- LAN_COLLAB : réseau collaborateurs
- LAN_ADMIN : réseau d'administration
- LAN_DMZ : zone démilitarisée
- HA_SYNC : synchronisation



Configuration des règles de filtrage

Des règles de pare-feu ont été mises en place afin d'autoriser uniquement les flux nécessaires au fonctionnement de l'infrastructure. Les réseaux serveurs, collaborateurs et administration disposent chacun de règles adaptées à leur utilisation.

Firewall: Rules: WAN

Select category | Inspect

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules 16
	IPv4 UDP	*	*	WAN address	51820	*	*	Allow WireGuard

pass | block | reject | log | in | first match
pass (disabled) | block (disabled) | reject (disabled) | log (disabled) | out | last match

Firewall: Rules: LAN_ADMIN

Select category | Inspect

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules 14
	IPv4 *	LAN_ADMIN net	*	*	*	*	*	Allow Any
	IPv4+6 TCP	*	*	LAN_ADMIN address	80 (HTTP)	*	*	Anti Lockout
	IPv4+6 TCP	*	*	LAN_ADMIN address	443 (HTTPS)	*	*	Anti Lockout

pass | block | reject | log | in | first match
pass (disabled) | block (disabled) | reject (disabled) | log (disabled) | out | last match

Firewall: Rules: LAN_SRV

Select category | Inspect

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules 16
	IPv4 *	LAN_SRV net	*	*	*	*	*	Default allow LAN to any rule
	IPv6 *	LAN_SRV net	*	*	*	*	*	Default allow LAN IPv6 to any rule

pass | block | reject | log | in | first match
pass (disabled) | block (disabled) | reject (disabled) | log (disabled) | out | last match

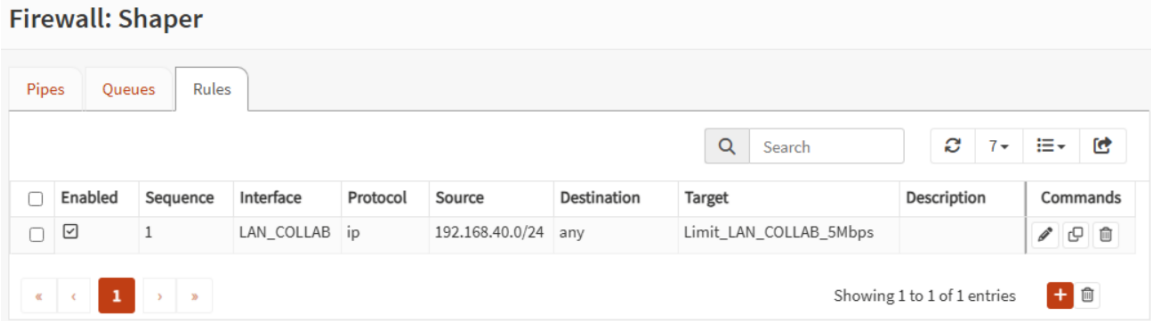
Firewall: Rules: LAN_COLLAB

Select category | Inspect

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules 14
	IPv4 *	LAN_COLLAB net	*	*	*	*	*	Default allow LAN to any rule

pass | block | reject | log | in | first match
pass (disabled) | block (disabled) | reject (disabled) | log (disabled) | out | last match

Mise en place du Traffic Shaping
Une limitation de bande passante à 5 Mbit/s a été appliquée sur le réseau LAN_COLLAB afin d'éviter qu'une saturation du réseau utilisateur n'impacte les services critiques de l'entreprise.



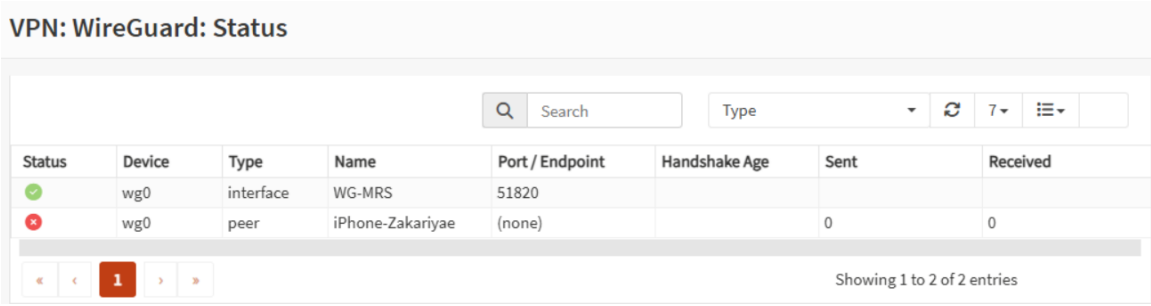
Résultat
Le pare-feu assure la séparation des réseaux, le contrôle des accès et la priorisation des services critiques. L'infrastructure dispose ainsi d'un premier niveau de sécurité avant le déploiement des autres services.

5.2 VPN nomade (Wireguard)

Objectif
Afin de permettre un accès sécurisé à l'infrastructure depuis l'extérieur, un VPN nomade WireGuard a été mis en place.

Configuration
Un tunnel WireGuard a été configuré sur le pare-feu OPNsense. Un client mobile a été ajouté en tant que pair VPN afin de permettre une connexion sécurisée depuis Internet.

Le port UDP 51820 a été autorisé sur l'interface WAN afin d'accepter les connexions entrantes.

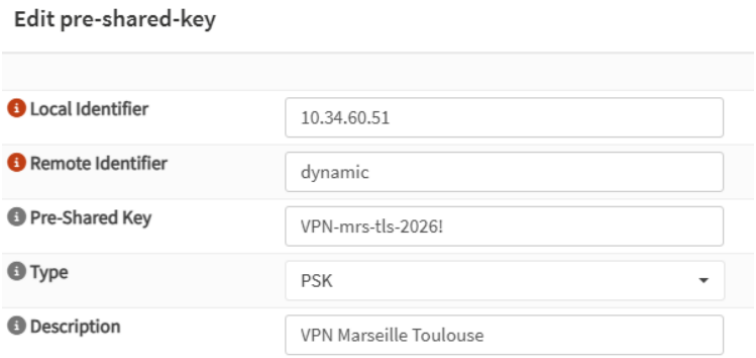


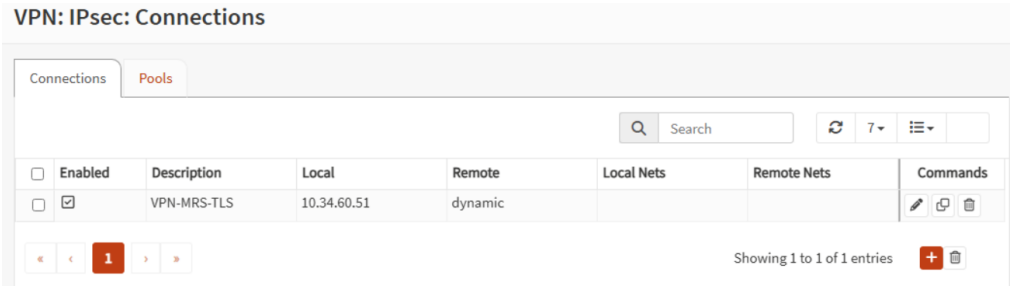
Résultat
Les utilisateurs autorisés peuvent accéder à distance aux ressources du réseau de manière chiffrée et sécurisée grâce au protocole WireGuard.

5.3 VPN site-à-site

Objectif
Afin de permettre la communication sécurisée entre les différents sites de l'entreprise, un tunnel VPN IPsec site-à-site a été mis en place entre Marseille et Toulouse.

Configuration
Une connexion IPsec a été créée sur OPNsense à l'aide d'une clé pré-partagée (PSK). Le tunnel permet d'établir une liaison chiffrée entre les deux sites tout en garantissant la confidentialité des échanges.



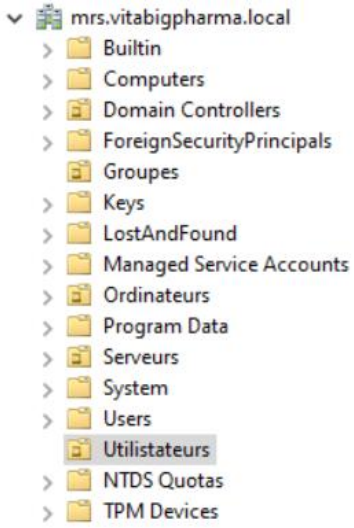


Résultat
Le VPN IPsec permet l'interconnexion sécurisée des réseaux de l'entreprise et prépare la communication entre les infrastructures distantes.

5.4 Active Directory / DNS

Objectif
Afin de centraliser l'administration des utilisateurs et des ressources, un contrôleur de domaine Active Directory a été déployé avec le service DNS intégré.

Création de l'annuaire Active Directory
Le domaine **mrs.vitabigpharma.local** a été créé. Plusieurs unités d'organisation (OU) ont été mises en place afin de structurer l'environnement et faciliter l'administration.



Création des utilisateurs
Les utilisateurs de l'entreprise ont été créés dans l'annuaire afin de permettre leur authentification sur le domaine.

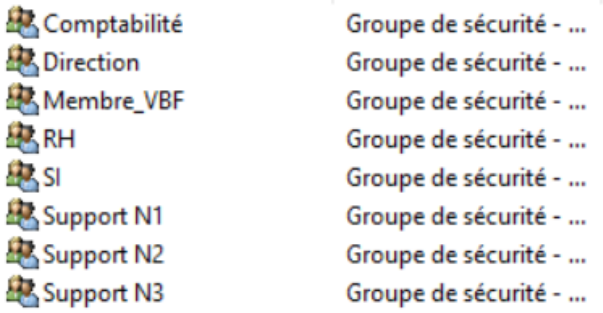
Exemples :

- Compta
- Direction
- RH
- SI1
- SI2
- SI3

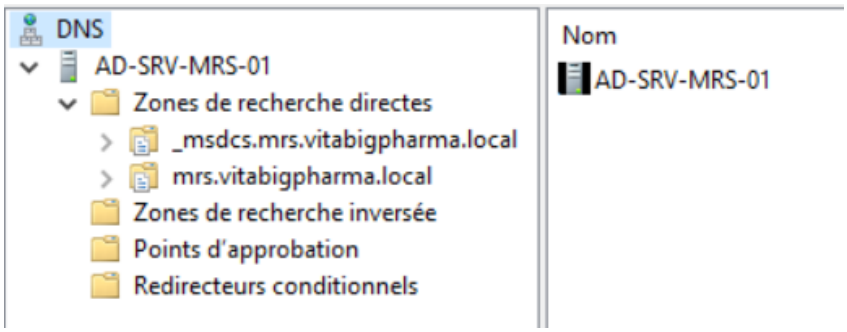
Gestion des groupes
Des groupes de sécurité ont été créés afin de simplifier l'attribution des droits et la gestion des accès.

Exemples :

- Comptabilité
- Direction
- RH
- SI
- Support N1
- Support N2
- Support N3



Configuration du DNS
Le service DNS a été installé sur le contrôleur de domaine AD-SRV-MRS-01. Une zone de recherche directe mrs.vitabigpharma.local a été créée afin de permettre la résolution de noms nécessaire au fonctionnement de l'Active Directory.



Résultat
L'infrastructure dispose d'un annuaire centralisé permettant la gestion des utilisateurs, des groupes et des ressources de l'entreprise.

5.5 Script PowerShell

Objectif
Afin d'automatiser l'administration de l'Active Directory, un script PowerShell a été développé pour gérer les utilisateurs à partir d'un fichier CSV.

Réalisation
Un fichier CSV contenant les informations des utilisateurs (nom, prénom, identifiant et mot de passe) a été créé.

Le script PowerShell importe les données du fichier CSV puis compare les utilisateurs présents dans l'Active Directory avec ceux du fichier source. Les comptes absents du fichier peuvent être supprimés et les nouveaux utilisateurs sont automatiquement créés dans l'unité d'organisation **Utilisateurs**.

Nouvel utilisateur

nv_utilisateur.csv - Bloc-notes

Fichier Edition Format Affichage Aide

```
Nom,Prenom,Login,Password
Outouil,Zakariyae,z.outouil,ChangeMe123!
,SI1,test_si1,ChangeMe123!
,SI2,test_si2,ChangeMe123!
,SI3,test_si3,ChangeMe123!
,RH,test_rh,ChangeMe123!
,Directeur,test_direction,ChangeMe123!
,Comptable,test_compta,ChangeMe123!
test,test,test,ChangeMe123!
```

Exécution du script

```
PS C:\Users\Administrateur> $users = Import-Csv "C:\Users\Administrateur\Desktop\nv_utilisateur.csv.txt"
>>
>> # Récupérer les logins du CSV
>> $csvLogins = $users.Login
>>
>> # Récupérer les utilisateurs AD dans ton OU
>> $adUsers = Get-ADUser -Filter * -SearchBase "OU=Utilistateurs,DC=mrs,DC=vitabigpharma,DC=local"
>>
>> # 🗑 SUPPRESSION
>> foreach ($adUser in $adUsers) {
>>     if ($csvLogins -notcontains $adUser.SamAccountName) {
>>         Remove-ADUser -Identity $adUser -Confirm:$false
>>     }
>> }
>>
>> # 🆕 CREATION
>> foreach ($u in $users) {
>>     if (-not (Get-ADUser -Filter "SamAccountName -eq '$($u.Login)'" -ErrorAction SilentlyContinue)) {
>>         New-ADUser -Name "$($u.Prenom) $($u.Nom)" `
>>         -SamAccountName $u.Login `
>>         -UserPrincipalName "$($u.Login)@mrs.vitabigpharma.local" `
>>         -AccountPassword (ConvertTo-SecureString $u.Password -AsPlainText -Force) `
>>         -Enabled $true `
>>         -Path "OU=Utilistateurs,DC=mrs,DC=vitabigpharma,DC=local"
>>     }
>> }
PS C:\Users\Administrateur>
```

Création réussie du profil

Nom	Type
Compta	Utilisateur
Direction	Utilisateur
RH	Utilisateur
SI1	Utilisateur
SI2	Utilisateur
SI3	Utilisateur
test test	Utilisateur
Zakariyae Outouil	Utilisateur

Résultat
L'automatisation de la création des comptes utilisateurs permet de réduire le temps d'administration et de limiter les erreurs de saisie. Les utilisateurs sont créés directement dans l'Active Directory à partir du fichier CSV.

5.6 Serveur de fichiers

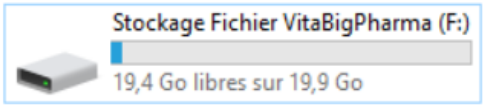
Objectif

Mettre à disposition un espace de stockage centralisé accessible par les utilisateurs de l'entreprise.

Réalisation

Un volume de stockage dédié a été créé afin d'accueillir les données de l'entreprise. Les permissions NTFS ont été configurées et un lecteur réseau a été déployé par GPO sur les postes du domaine.

Emplacement stockage des fichiers

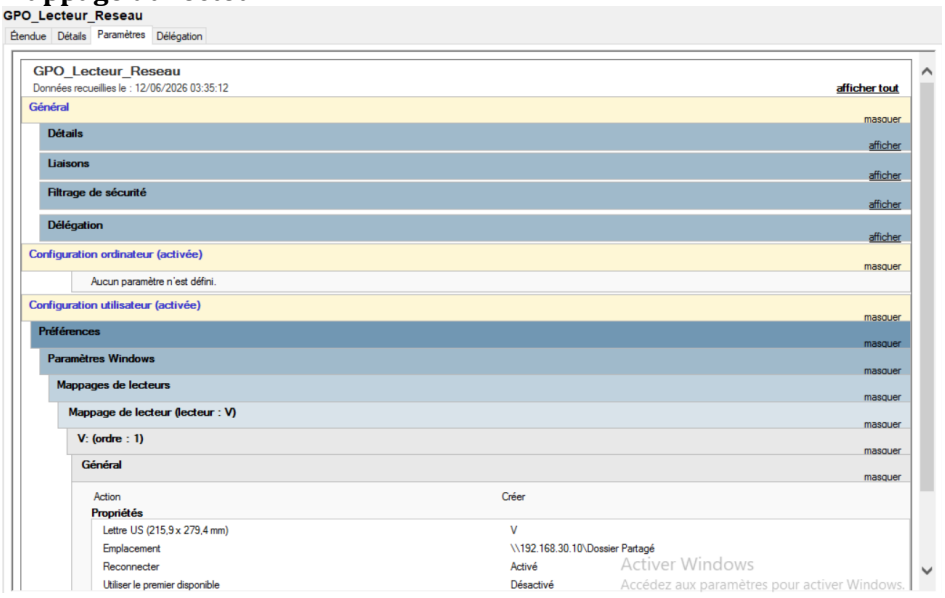


Droit NTFS

Entrées d'autorisations :

Type	Principal	Accès	Hérité de	S'applique à
Auto...	Administrateurs (MRS\Admin...	Contrôle total	Aucun	Ce dossier, les sous-dossiers et...
Auto...	Système	Contrôle total	Aucun	Ce dossier, les sous-dossiers et...
Auto...	CREATEUR PROPRIETAIRE	Contrôle total	Aucun	Les sous-dossiers et les fichiers...
Auto...	Utilisateurs (MRS\Utilisateurs)	Lecture et exécution	Aucun	Ce dossier, les sous-dossiers et...
Auto...	Utilisateurs (MRS\Utilisateurs)	Création de dossier/ajo...	Aucun	Ce dossier et les sous-dossiers
Auto...	Utilisateurs (MRS\Utilisateurs)	Création de fichier/écri...	Aucun	Les sous-dossiers seulement
Auto...	Tout le monde	Lecture et exécution	Aucun	Ce dossier seulement

Mappage du lecteur



Résultat

Les utilisateurs disposent d'un espace de stockage partagé accessible via un lecteur réseau. Les accès sont contrôlés grâce aux permissions définies sur le serveur.

5.7 Stratégies de groupe (GPO)

Objectif

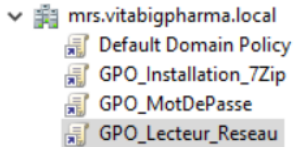
Automatiser la configuration des postes utilisateurs et renforcer la sécurité du domaine.

Réalisation

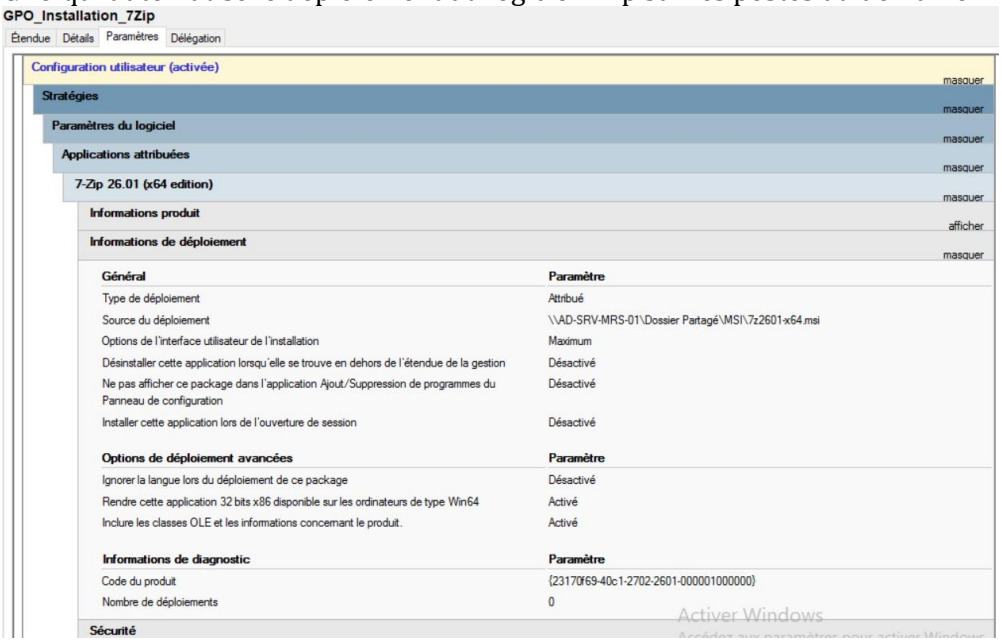
Plusieurs stratégies de groupe ont été déployées sur le domaine Active Directory :

- GPO_MotDePasse : application de règles de sécurité pour les mots de passe.
- GPO_Installation_7Zip : déploiement automatisé du logiciel 7-Zip.
- Lecteur_Reseau : montage automatique du lecteur réseau sur les postes utilisateurs.

Liste des GPO



GPO qui automatise le déploiement du logiciel 7zip sur les postes du domaine.



GPO qui renforce la sécurité des comptes utilisateurs.

GPO qui fournit un accès simple et centralisé aux fichiers de l'entreprise.

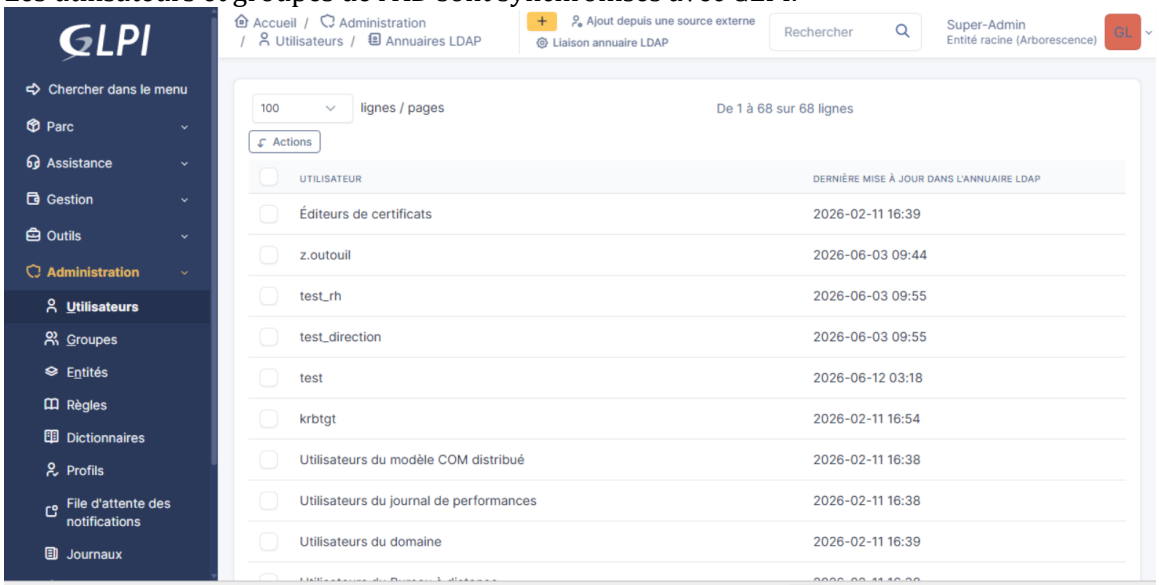
Résultat
Les postes du domaine sont configurés automatiquement lors de leur intégration au domaine, ce qui simplifie l'administration et garantit l'application homogène des paramètres de sécurité.

5.8 GLPI

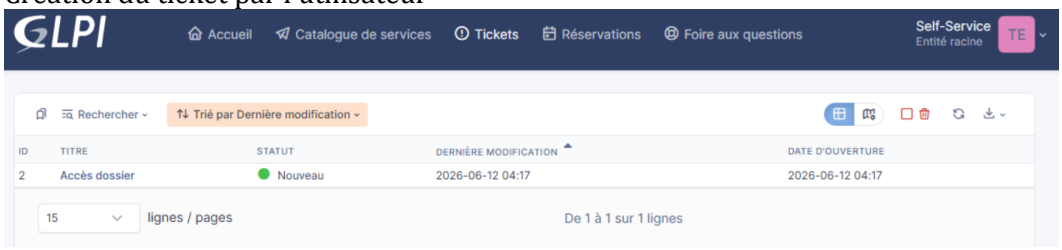
Objectif
Mettre en place une solution de gestion des incidents afin de centraliser les demandes des utilisateurs et améliorer le suivi du support informatique.

Réalisation
GLPI a été installé sur un serveur dédié. Une liaison LDAP a été configurée afin d'importer automatiquement les utilisateurs de l'Active Directory dans l'application.

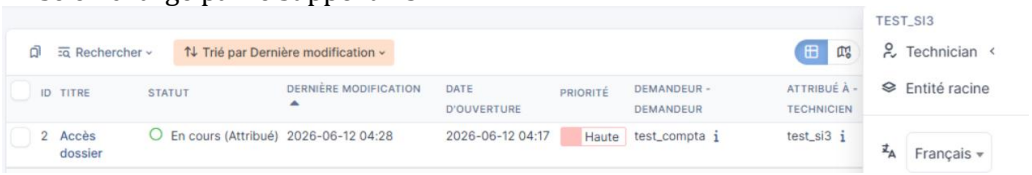
Les utilisateurs et groupes de l'AD sont synchronisés avec GLPI.



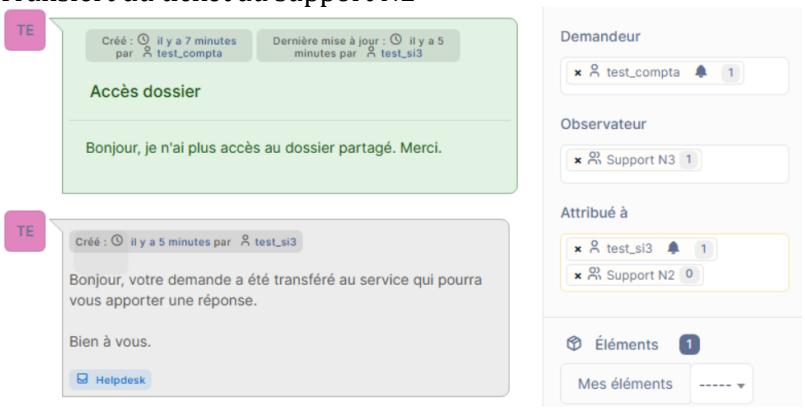
Création du ticket par l'utilisateur



Prise en charge par le support N3



Transfert du ticket au support N2



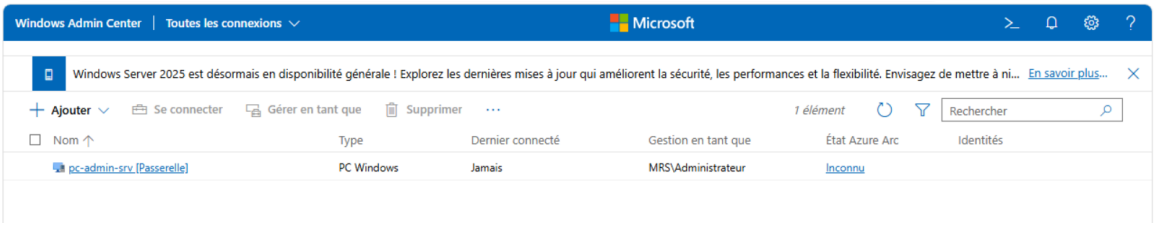
Résolution de l'incident et clôture du ticket

Un utilisateur du service comptabilité a signalé un problème d'accès au dossier partagé. Le ticket a été pris en charge par le support N3 puis transféré au support N2 pour traitement. Après analyse, l'accès a été rétabli et le ticket clôturé.

5.9 Windows Admin Center

Objectif
Centraliser l'administration des serveurs et postes Windows depuis une interface web unique.

Réalisation
Windows Admin Center a été installé sur le poste d'administration afin de faciliter la gestion de l'infrastructure. La solution permet d'accéder à distance aux équipements Windows et d'effectuer des tâches d'administration depuis une interface web sécurisée.

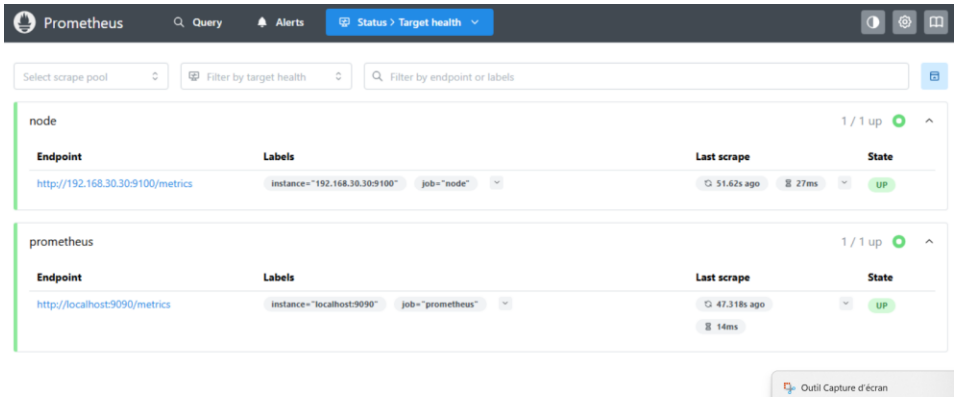


Résultat
L'administration des équipements Windows est simplifiée grâce à une interface centralisée accessible depuis le poste d'administration.

5.10 Prometheus

Objectif
Mettre en place une solution de supervision afin de surveiller l'état et la disponibilité des services de l'infrastructure.

Réalisation
Prometheus a été installé et configuré afin de collecter les métriques des équipements supervisés. Les cibles configurées sont interrogées régulièrement afin de vérifier leur disponibilité.



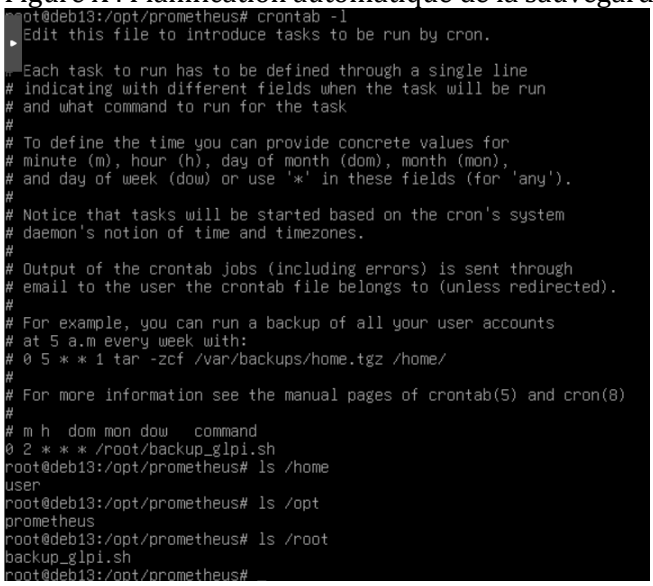
Résultat
La supervision permet de vérifier le bon fonctionnement des services et d'être alerté en cas d'indisponibilité d'un équipement ou d'un service.

5.11 Sauvegardes

Objectif
Mettre en place une solution de sauvegarde automatisée afin de sécuriser les données de l'application GLPI et de permettre leur restauration en cas d'incident.

Réalisation
Un script de sauvegarde nommé **backup_glpi.sh** a été créé sur le serveur Linux. Son exécution est automatisée à l'aide du service **Cron**, avec une sauvegarde programmée quotidiennement à **02h00**.

Figure X : Planification automatique de la sauvegarde GLPI via Cron.



Le script backup_glpi.sh est exécuté automatiquement tous les jours à 02h00 afin d'assurer la sauvegarde régulière des données de l'application GLPI.

Résultat
Les sauvegardes sont exécutées automatiquement chaque jour sans intervention manuelle, garantissant la protection des données de l'application GLPI.

5.12 Audit de sécurité Linux

Objectif
Évaluer le niveau de sécurité du serveur Linux et identifier les points d'amélioration afin de renforcer sa protection.

Réalisation
Un audit de sécurité a été réalisé à l'aide de l'outil **Lynis**. Cet outil analyse la configuration du système et vérifie différents éléments de sécurité tels que les services, les permissions, le pare-feu et les paramètres de durcissement.

L'analyse Lynis a effectué 274 tests de sécurité et a attribué un indice de durcissement (Hardening Index) de 67 au serveur Linux.

```
Lynis security scan details:

Hardening index : 67 [#############       ]
Tests performed : 274
Plugins enabled : 1

Components:
- Firewall               [V]
- Malware scanner        [X]

Scan mode:
Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

Lynis modules:
- Compliance status      [?]
- Security audit         [V]
- Vulnerability scan     [V]

Files:
- Test and debug information      : /var/log/lynis.log
- Report data                     : /var/log/lynis-report.dat
```

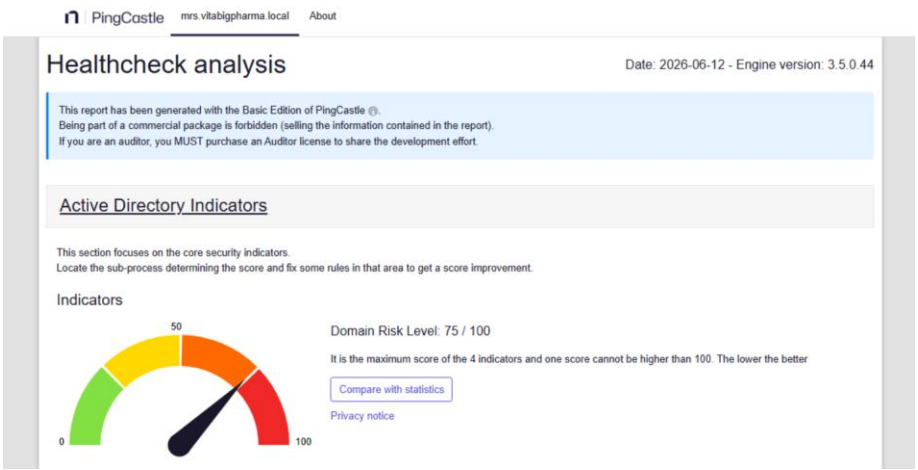
Résultat
L'audit a permis de vérifier le niveau de sécurité du serveur et d'identifier les éventuelles recommandations d'amélioration afin de renforcer sa sécurité globale.

5.13 Audit de sécurité Active Directory

Objectif
Évaluer le niveau de sécurité de l'Active Directory afin d'identifier les vulnérabilités et les mauvaises pratiques de configuration.

Réalisation
L'outil **PingCastle** a été utilisé pour réaliser un audit de sécurité de l'environnement Active Directory. Cet audit permet d'analyser la configuration du domaine et de détecter les risques de sécurité.

Rapport d'audit Active Directory généré par PingCastle



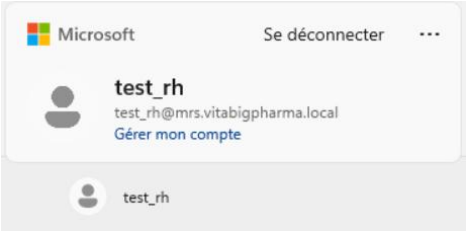
Le rapport PingCastle attribue au domaine un **niveau de risque de 75/100** et fournit des recommandations permettant d'améliorer la sécurité de l'Active Directory.

Résultat
L'audit a permis d'obtenir une vision globale du niveau de sécurité du domaine et d'identifier les points nécessitant un renforcement de la sécurité.

6. Tests et validation

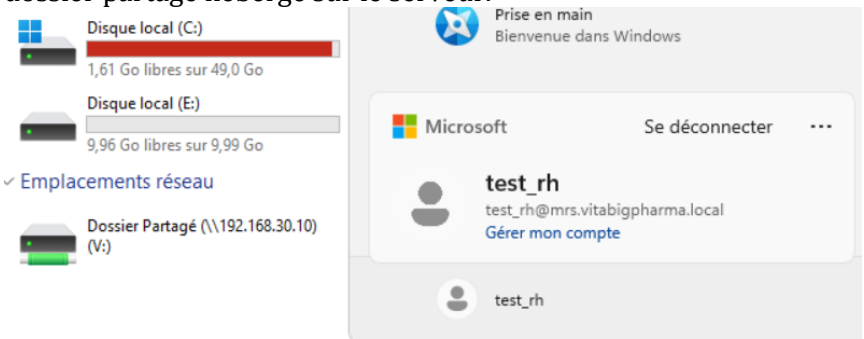
6.1 Active Directory

Connexion avec un utilisateur du domaine :



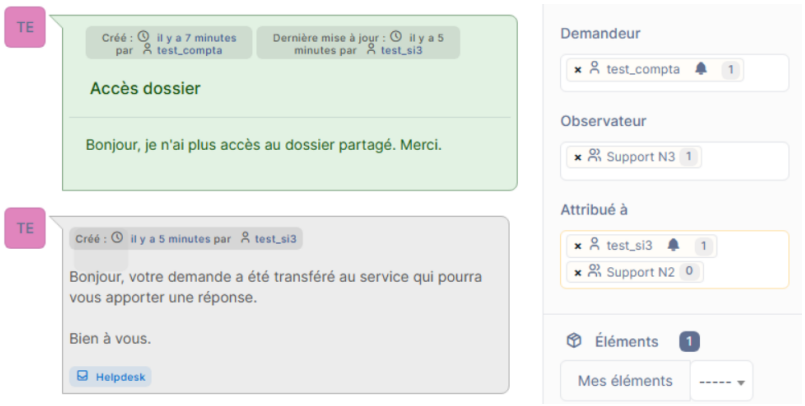
6.2 Partage réseau + GPO

Le lecteur réseau V: est automatiquement monté grâce à la GPO et permet d'accéder au dossier partagé hébergé sur le serveur.



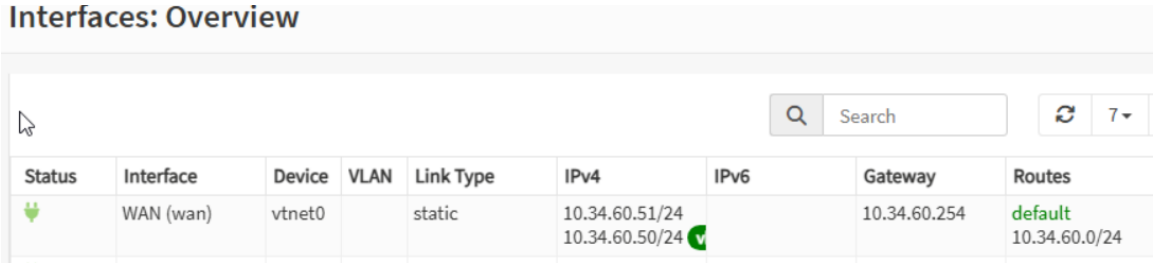
6.3 GLPI

Ticket créé par un utilisateur et traité par un technicien.



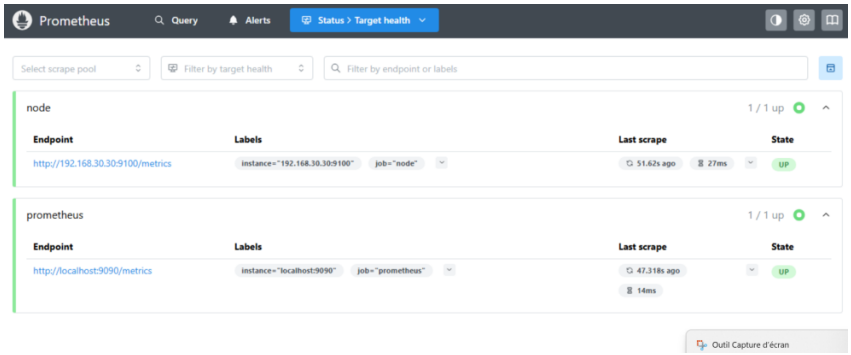
6.4 VPN Wireguard

La solution WireGuard a été déployée et configurée. La connexion VPN a été validée en environnement de test interne. L'ouverture vers Internet nécessite une redirection du port UDP 51820 sur l'équipement amont.



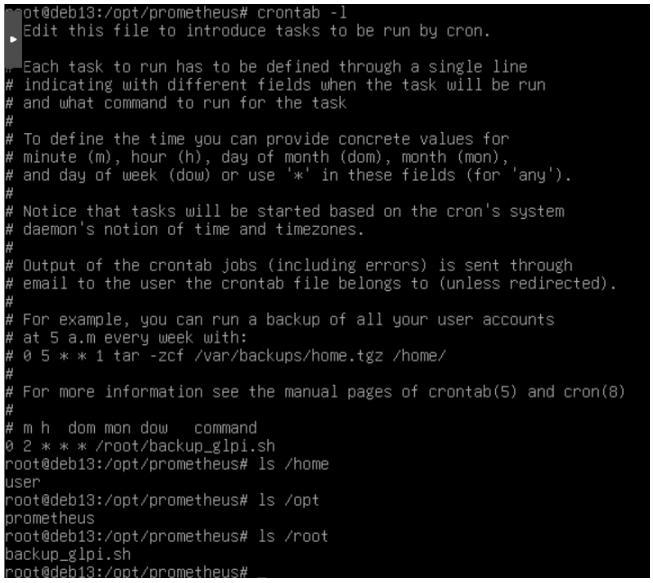
6.5 Prometheus

Vérification si les cibles supervisées sont joignables et remontent leurs métriques.



6.6 Sauvegarde

Vérification si la sauvegarde automatique est programmée.



7. Exploitation et maintenance

Supervision
La supervision de l'infrastructure est assurée par Prometheus, permettant de surveiller la disponibilité des services et la remontée des métriques système.

Sauvegardes
Les sauvegardes sont automatisées grâce à un script exécuté quotidiennement via Cron afin de protéger les données de l'application GLPI.

Administration
L'administration des serveurs Windows est réalisée via Windows Admin Center. L'Active Directory permet la gestion centralisée des utilisateurs, groupes et postes du domaine.

Gestion des incidents
Les incidents sont traités via GLPI selon un processus de création, affectation, traitement et clôture des tickets.

8. Sécurité

Sécurité réseau
La sécurité du réseau est assurée par le pare-feu OPNsense. Des règles de filtrage ont été mises en place afin de contrôler les flux entre les différents réseaux de l'infrastructure. Un VPN IPsec inter-sites et un VPN WireGuard pour les accès distants ont également été configurés.

Sécurité Active Directory
L'authentification est centralisée via Active Directory. Une politique de mot de passe renforcée a été déployée à l'aide des stratégies de groupe (GPO).

Gestion des droits
Les utilisateurs sont organisés dans des groupes de sécurité afin de simplifier l'attribution des permissions et limiter les accès aux ressources.

Audits de sécurité
Des audits de sécurité ont été réalisés à l'aide des outils PingCastle et Lynis afin d'identifier les éventuelles vulnérabilités et recommandations d'amélioration.

9. Gestion des incidents

Procédure

La gestion des incidents est assurée à l'aide de GLPI. Chaque incident suit un cycle de traitement défini :

1. Création du ticket par l'utilisateur.
2. Qualification de l'incident.
3. Affectation à un technicien ou à un groupe de support.
4. Traitement de l'incident.
5. Résolution.
6. Clôture du ticket.

Exemple
Un utilisateur du service comptabilité a signalé un problème d'accès à un dossier partagé. Le ticket a été pris en charge par le support N3 puis transféré au support N2 pour traitement. Après intervention, l'accès a été rétabli et le ticket clôturé.

10. Conclusion

Ce projet m'a permis de concevoir et déployer une infrastructure réseau sécurisée pour le site de Marseille de l'entreprise VitaBigPharma. Les objectifs fixés ont été atteints grâce à la mise en place d'un pare-feu OPNsense, d'un Active Directory, d'une solution de gestion des incidents GLPI, d'un système de supervision Prometheus ainsi que de mécanismes de sauvegarde et d'audit de sécurité. Ce projet m'a permis de développer mes compétences en administration systèmes, réseaux et cybersécurité.

11. Perspectives d'amélioration

- Mise en place d'une haute disponibilité des pare-feux.
- Déploiement d'une authentification multifacteur (MFA).
- Ajout de nouveaux serveurs supervisés dans Prometheus.
- Renforcement de la stratégie de sauvegarde.
- Mise en place d'une supervision graphique avec Grafana.