

# DOSSIER DE PROJET SEAHAWKS

Nadia  
**BENBOUALI**

AIS 2024-2025



**SEAHAWKS**  
MONITORING



**SIMPLON**  
.CO

# SWINGWARE

- **Présentation de l'entreprise**
- **Cahier des charges & objectifs du projet**
- **La gestion de projet**
- **Les solutions retenues**
- **Les spécifications techniques**
- **La mise en œuvre**

# PRESENTATION DE L'ENTREPRISE

## Création

Fondée au début des années 2020  
Par deux développeurs français experts  
du secteur

## Implantation

Siège à Kansas City (USA)  
Datacenter à Roubaix (France)

## Spécialisation

Services IT pour les équipes de football  
américain professionnel (NFL)

## Activité

Infogérance, audit, conseil, intégration  
d'infrastructures

# Qui est NFL IT ?

## Effectif

100+ employés  
30 techniciens itinérants  
30 support  
40 administratifs

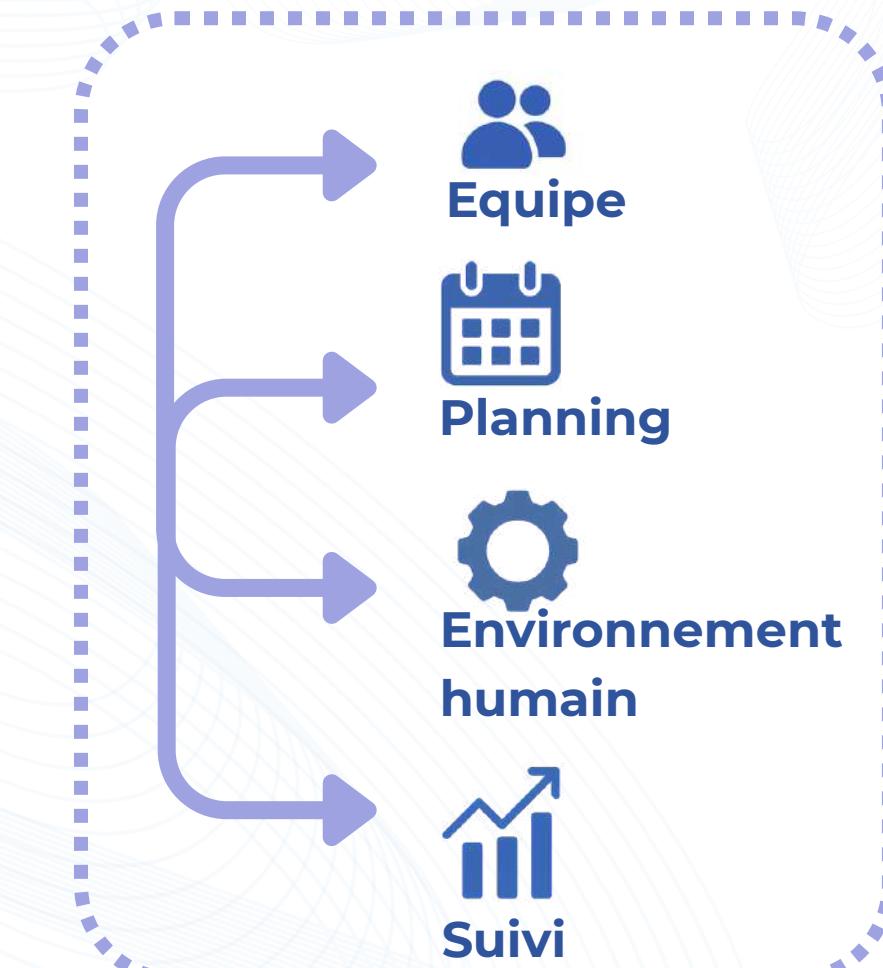
## Client principal

Contrat exclusif avec la National Football  
League  
32 franchises clientes

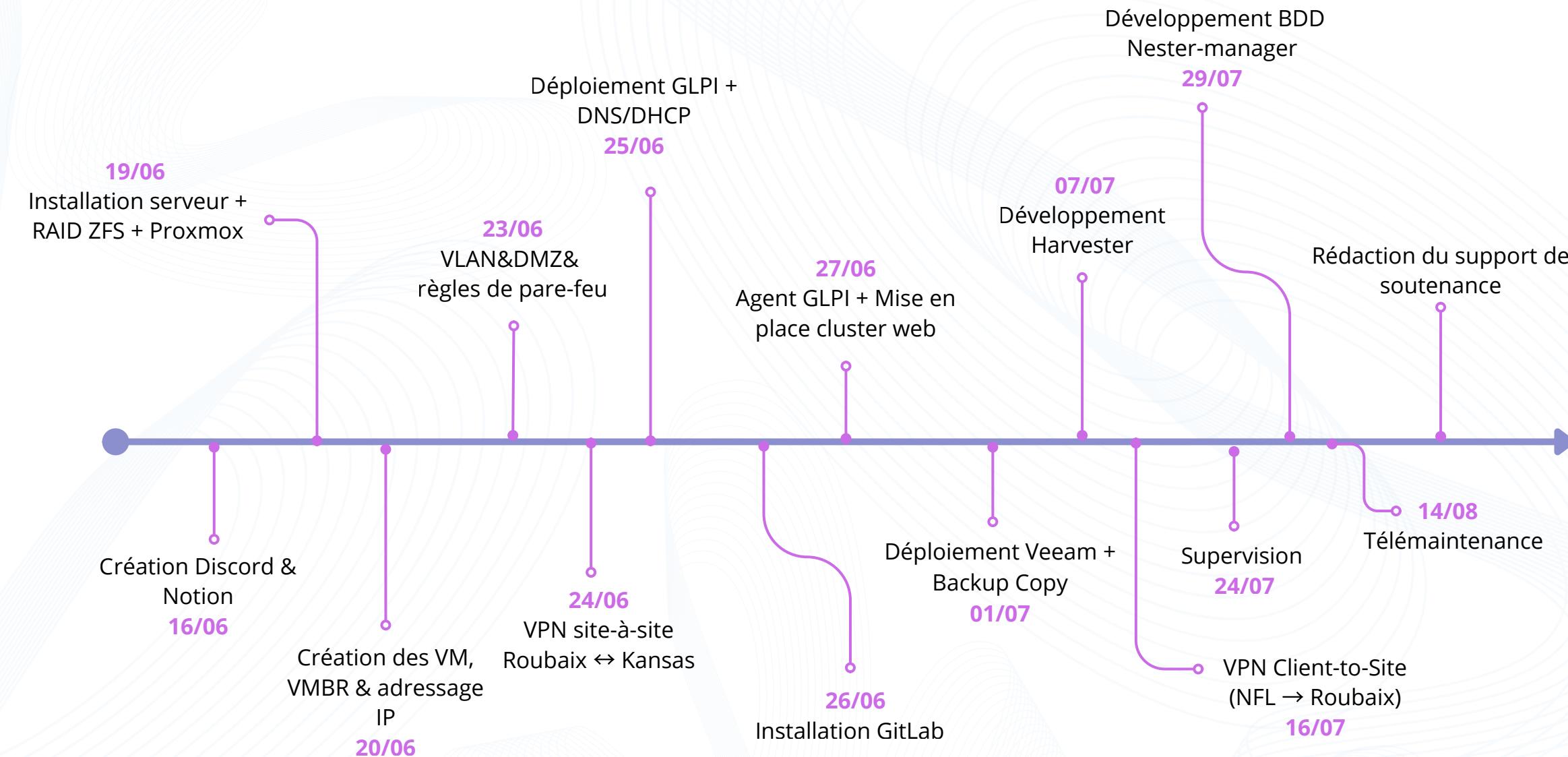
# Cahier des charges & objectifs du projet

Besoins identifiés	Objectifs à atteindre	Services/solutions prévus
-Interventions trop fréquentes sur site	Permettre un support à distance sécurisé	VPN IPsec site-à-site entre Roubaix et Kansas (pfSense)
-Manque de visibilité sur le parc machine	Avoir un inventaire automatique et à jour	GLPI Inventory + agent sur chaque VM
-Suivi non centralisé des incidents	Traiter et suivre les demandes utilisateurs efficacement	GLPI avec gestion des tickets
-Risque de perte de données critiques	Sauvegarder régulièrement les machines	Veeam Backup & Replication + Backup Copy
-Aucun outil pour superviser les ressources	Obtenir des indicateurs techniques en temps réel	Grafana + Prometheus
-Pas de visualisation des données techniques collectées	Offrir une interface lisible au support technique	Développement de l'application web Nester
-Besoin de récolter automatiquement les données locales	Automatiser les scans et les diagnostics réseau	Développement du Harvester (scripts + JSON)
-Besoin de garantir la haute disponibilité de l'interface web	Assurer l'accès continu au Nester même en cas de panne serveur	Cluster web (HAProxy + NGINX)
-Simplifier la maintenance des applications internes.	Faciliter les évolutions du Harvester	Plateforme GitLab

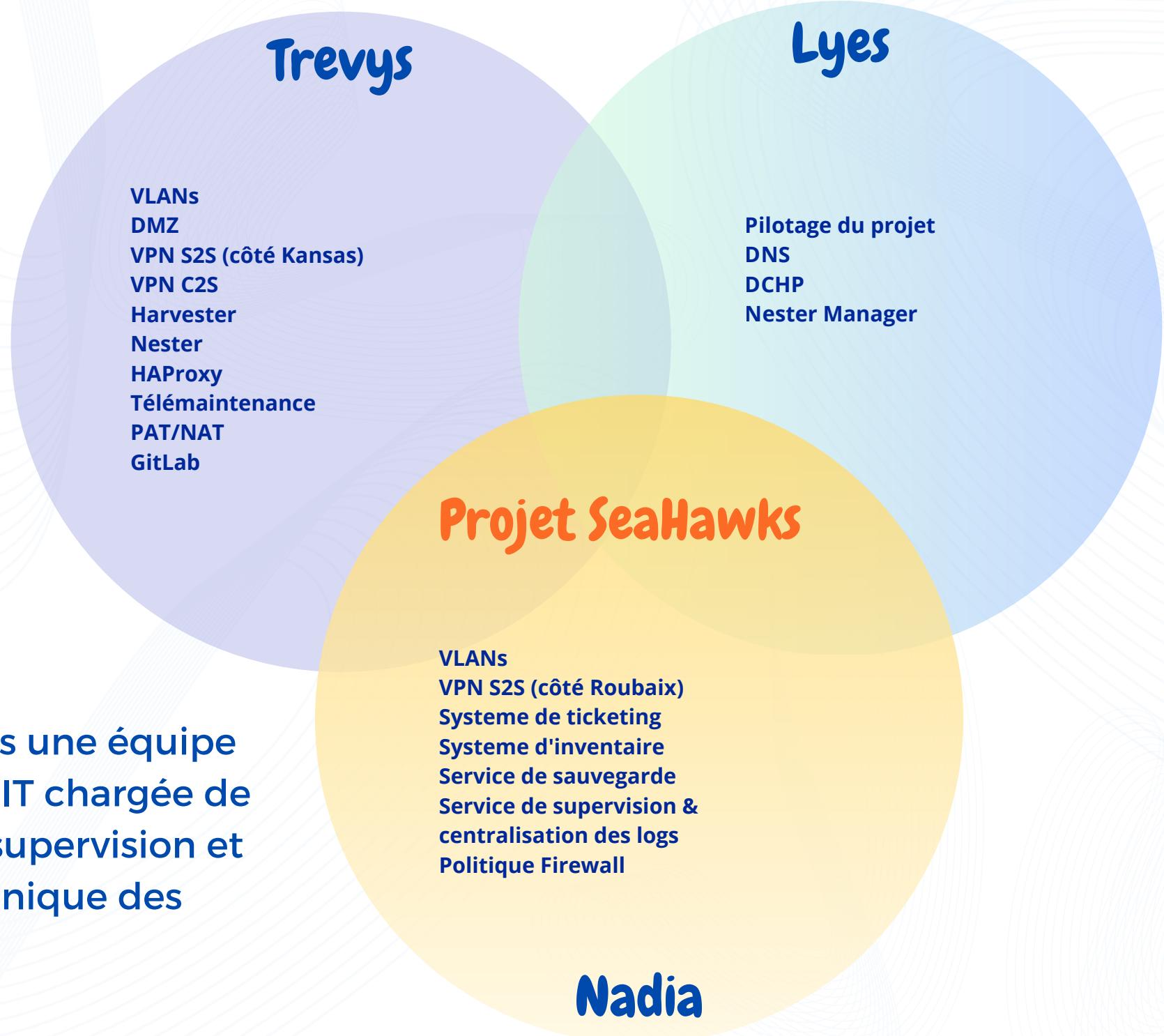
# LA GESTION DE PROJET



# PLANNING DU PROJET



# ÉQUIPE SEAHAWKS MONITORING



Nous incarnons une équipe interne de NFL IT chargée de moderniser la supervision et le support technique des franchises NFL.

**Mission :** Concevoir, développer et déployer le service SeaHawks Monitoring

**Objectifs :**

- Répondre au manque d'outils de maintenance à distance
- Proposer une solution innovante pour les 32 franchises NFL
- Garantir la viabilité et le support technique

# OUTILS COLLABORATIFS

**Projet SeaHawks**

Par état Tous les projets Gantt Mes projets

	Personne assignée	Priorité	État	Date de début	Date de fin	Budget
Prise de connaissance des documents	Lyes Daci Trevys nad	Elevée	Terminé	16/06/2025	16/06/2025	
Planification et schématisation de l'infra	Lyes Daci Trevys nad	Elevée	Terminé	16/06/2025	16/06/2025	
Mise en place de Proxmox	Lyes Daci Trevys nad	Elevée	Terminé	17/06/2025	17/06/2025	
Sécurité : - Sécurisation accès HTTP/SSH (fail2ban ?)	Trevys nad Lyes Daci	Pas commencé				
Télémaintenance : - Reverse SSH ou VNC fonctionnent	Lyes Daci N nad Trevys	Elevée	En cours			
Supervision (Prometheus/Graphana) : - Prometheus	Lyes Daci N nad Trevys		Terminé			
Configuration des agents VB	Lyes Daci Trevys nad		Terminé			
Système de Gestion de Bases de Données (Phase 4)	Lyes Daci N nad Trevys		En cours	21/07/2025	25/07/2025	
Développement du HARVESTER (Phase 3 - EA1)	Lyes Daci Trevys nad		Terminé	01/07/2025	03/07/2025	
Cluster web	Lyes Daci Trevys nad	Moyenne	Terminé	26/06/2025	30/06/2025	
Veeam backup server	N nad Lyes Daci Trevys		Terminé			
Gitlab	Lyes Daci N nad Trevys	Moyenne	Terminé	24/06/2025	26/06/2025	
Serveurs GLPI / DNS,DHCP	Lyes Daci N nad Trevys		Terminé			
Configuration PFsense	Lyes Daci N nad Trevys		En cours	20/06/2025		
Adressage IP	Lyes Daci N nad Trevys	Elevée	Terminé			
Compte rendu / Powerpoint	Lyes Daci Trevys nad	Elevée	En cours	18/06/2025		
Création du discord	Lyes Daci Trevys nad	Elevée	Terminé	16/06/2025	16/06/2025	



AIS - Projet SeaHawks - Suivi de Stage Salsabil

# 🔍 | règlement

Nadia Trevys

zz | afk-room

| Bienvenue & Infos +

# 🔍 | règlement

# 🔊 | bienvenue

# 🎙️ | présentation-projet

# 🎯 | objectifs

# 📅 | planning-projet

# 🌟 | équipe

# 📣 | annonces

| Communication +

# 💬 | discussion-générale

# 🤔 | questions

/voix connectée

local / AIS - Projet SeaHawks - Suivi ...

**Bienvenue sur AIS - Projet SeaHawks**

**Suivi de Stage Salsab**

Ceci est le début de la vie de ce serveur.

16 juin 2025

Lyes 16/06/2025 11:53

Règlement du Serveur SeaHawks

✓ Respect et bienveillance dans les échanges.  
✓ Utilisation des bons salons selon le sujet.  
✓ Tenue à jour du journal de bord (#journal-de-bord) et des tâches (#tâche).  
✓ Partage uniquement de contenu lié au projet.

🚫 Ce serveur est à usage strictement professionnel dans le cadre du projet.

Toute utilisation détournée entraînera une exclusion.

**Notion :** Planification des tâches, suivi de l'avancement, centralisation des documents du projet.



**Discord :** Communication instantanée (textes, voix, partages d'écran) et coordination en temps réel.



# LES SOLUTIONS REtenues

Service / Solution choisie	Justification du choix
-VPN IPsec site-à-site (pfSense)	Assure une communication sécurisée entre les sites Roubaix et Kansas. Facile à déployer via pfSense, open source et robuste.
-VPN Client-to-Site (WireGuard)	Garantit un tunnel sécurisé entre les franchises NFL (Harvester) et le serveur central (Nester). Léger, rapide et automatisable avec systemd.
-GLPI Inventory	Permet l'inventaire automatique des machines via agents. Solution libre, très utilisée, facile à intégrer.
-GLPI (gestion des tickets)	Assure le suivi des incidents, des demandes de support et permet un historique clair. Interface simple et adaptée à un usage en entreprise.
-Veeam Backup & Replication	Outil de sauvegarde fiable et complet. Compatible Linux/Windows. Possibilité de planifier des Backup Copy, restauration souple.
-Grafana + Prometheus	Couple open source performant pour superviser l'état des machines, métriques réseau et services critiques. Tableaux de bord personnalisés.
-Développement de l'application web Nester	Interface interne de visualisation des données envoyées par les Harvesters. Codée en Python, légère, personnalisable, centralisée.
-Développement du Harvester	Agent distant développé en Python permettant d'effectuer des scans réseau, mesurer la latence, remonter les rapports en JSON. Adapté aux franchises clientes.
-Cluster Web (HAProxy + NGINX)	3 serveurs web reliés à un load balancer HAProxy en round-robin. NGINX en frontal. Assure la haute disponibilité, la répartition de charge et la sécurité de l'interface web.
-Plateforme GitLab	Déployée pour centraliser le code source (Harvester/Nester), gérer les dépôts et les utilisateurs. Assure traçabilité et collaboration.

# LES SPÉCIFICATIONS TECHNIQUES

# Architecture réseau et plan IP

## Site de Roubaix

Équipement	Adresse IP	VLAN/OS	Notes
-pfsens-roubaix (WAN)	10.25.3.47	FreeBSD	Connexion vers l'extérieur (Internet/cloud VPN)
-pfsens-roubaix (LAN)	10.10.10.1	-	Réseau interne du site de Roubaix (Datacenter)
-vm-lb-nester	10.10.12.2	DMZ/Debian12	Répartiteur de charge (Load Balancer) pour le cluster web
-vm-nester1	10.10.12.7	DMZ/Ubuntu	Serveur Seahawks Nester 1 (Cluster web)
-vm-nester2	10.10.12.8	DMZ/Ubuntu	Serveur Seahawks Nester 2 (Cluster web)
-vm-nester3	10.10.12.9	DMZ/Ubuntu	Serveur Seahawks Nester 3 (Cluster web)
-vm-gitlab	10.10.10.3	VLAN10-RockyLinux	Mise à jour Harvester

Équipement	Adresse IP	VLAN/OS	Notes
-vm-db-nester	10.10.10.4	VLAN10-AlmaLinux	SGBD pour Nester Seahawks
-vm-graf-prom-loki	10.10.10.5	VLAN10-ArchLinux	Supervision (Grafana/Prometheus/Loki)
-vm-backupSrv	10.10.10.12	VLAN10-WinSrv2019	Serveur Veeam Backup et RéPLICATION
-WinRoubaix	10.10.30.13	VLAN30-Win10	Poste Technicien LAN Roubaix
-vm-depot linux	10.10.10.11	VLAN10-Debian12	Serveur stockage sauvegardes
-vmBackupCopy	10.10.10.20	VLAN10-Debian12	Serveur copie sauvegardes
-pfSense VPNwireGuard	10.10.20.1		VPN Client nomade- côté routeur

# Architecture réseau et plan IP

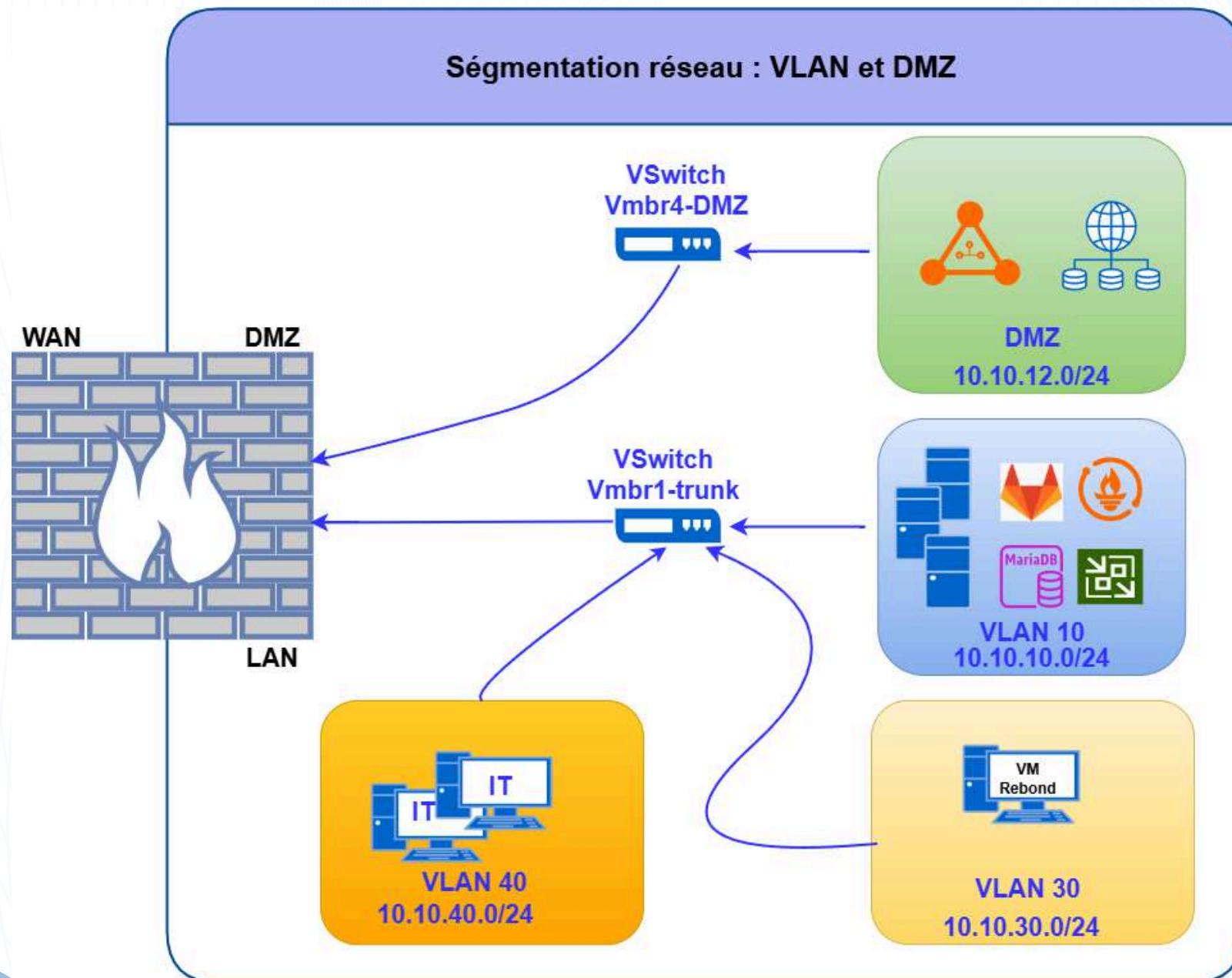
## Site de Kansas

Équipement	Adresse IP	OS	Notes
-pfsens-kansas (WAN)	10.25.3.27	FreeBSD	Connexion vers l'extérieur (Internet/cloud VPN)
-pfsens-kansas (LAN)	192.168.60.1	-	Réseau interne Kansas City (Siège social)
-vm-dns-dhcp	192.168.60.2	AlpineLinux	Serveur DNS + DHCP siège
-vm-glpi	192.168.60.20	Debian12	Ticketing/Inventaire GLPI
-vm-wintech	192.168.60.13	Win10	VM rebond support

## Franchise NFL

Équipement	Adresse IP	OS	Notes
-pfsens-NFL (WAN)	10.25.3.28	FreeBSD	Connexion vers l'extérieur (Internet)
-pfsens-NFL (LAN)	172.16.30.1	-	Réseau interne NFL
-vm-harvester-x	172.16.30.10	Debian 12	Client de supervision (franchise)
-Client Harvester	10.10.20.2		VPN Client nomade côté client

# Cloisonnement réseau VLAN et DMZ



- Mise en place de VLANs pour cloisonner les environnements :
- VLAN 10 – Services : supervision, sauvegarde, base de données, GitLab, GLPI.
- VLAN 30 – Bastion : VM rebond dédiée à la téléaintenance.
- VLAN 40 – IT : postes techniques des administrateurs.
- Création d'une DMZ (10.10.12.0/24) isolant les services exposés (HAProxy, Nester).
- Application de règles pfSense pour contrôler strictement les flux entre VLANs, DMZ et WAN.

# TECHNOLOGIES MOBILISÉES

## Virtualisation



## Réseau



## Supervision



## Sauvegarde



## Ticketing/Inventaire

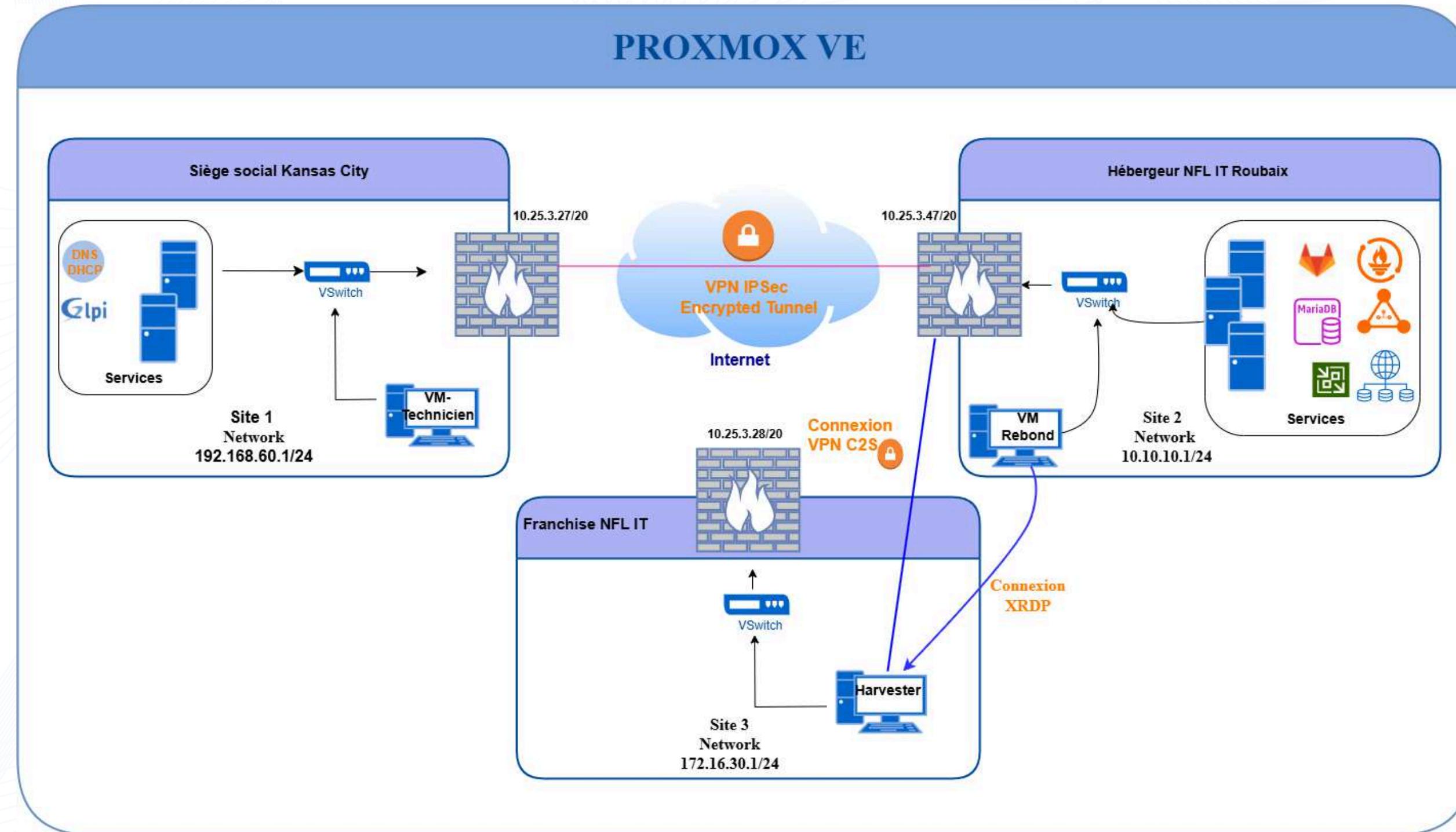


## Développement

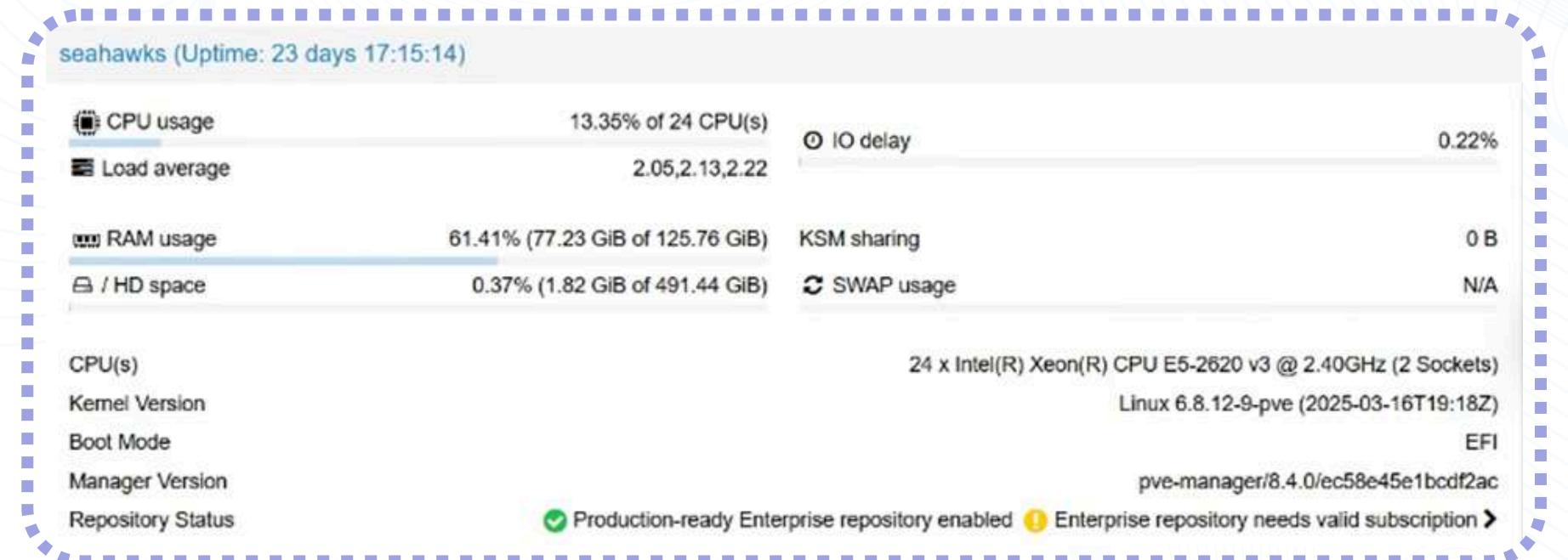


# LA MISE EN ŒUVRE

# SCHÉMA DE L'INFRASTRUCTURE



# ENVIRONNEMENT TECHNIQUE MIS EN PLACE



**Stockage :** RAID-Z3 – 2,39 To utiles

**Mémoire vive :** 128 Go DDR4 ECC

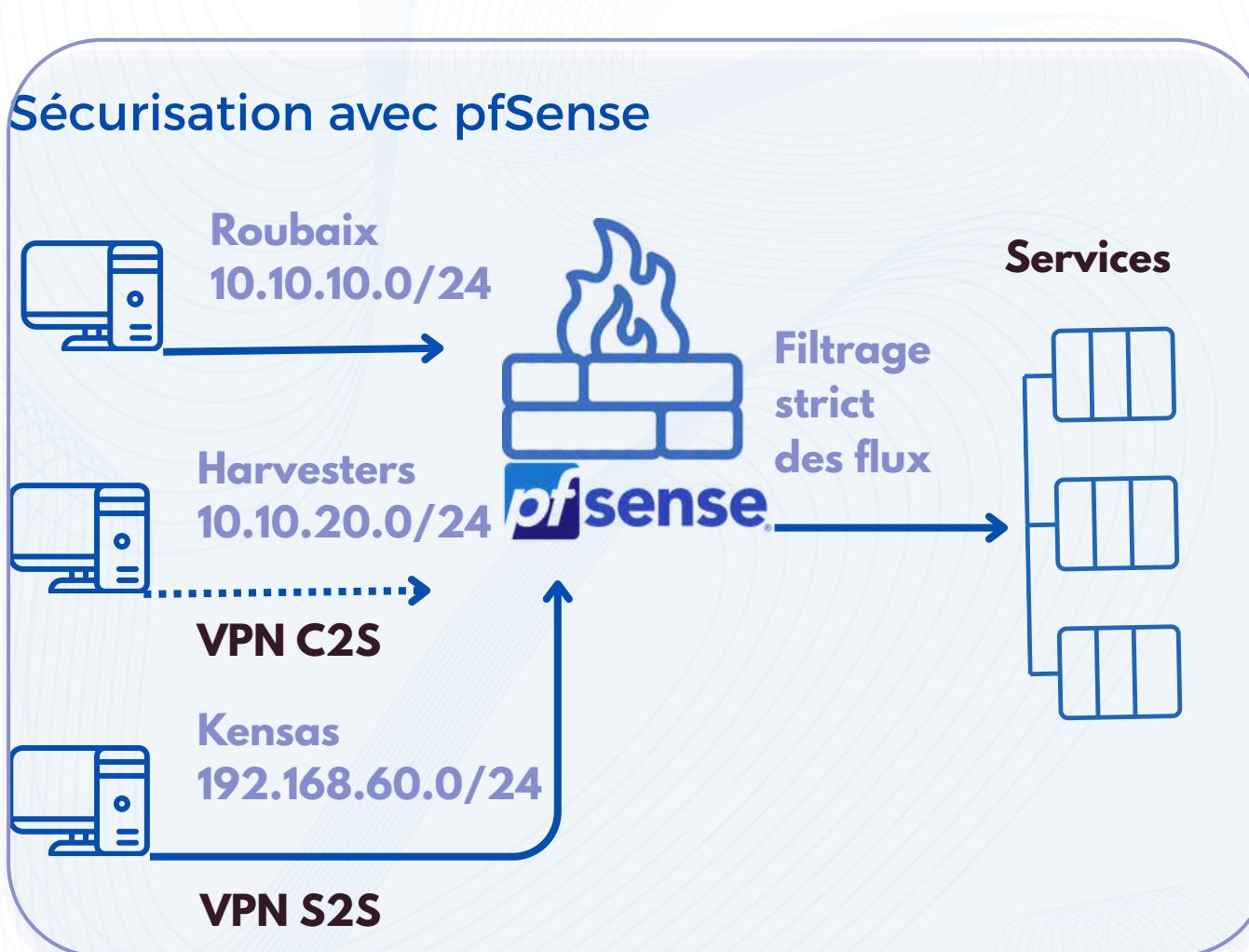
**Processeur :** 2× Xeon E5-2620 v3 – 24 threads

**Réseau :** Proxmox VE 8.4.0, SDN activé

# ENVIRONNEMENT TECHNIQUE MIS EN PLACE

Bridge	Interface	Réseau IP	Usage
vmbr0	eno1	10.25.3.0/20	Réseau WAN (connexion Internet)
vmbr1	-	10.10.10.0/24	Réseau interne principal (site Roubaix)
vmbr2	-	192.168.60.0/24	Réseau du siège social (Kansas City)
vmbr3	-	172.16.30.0/24	Réseau isolé des franchises NFL
Vmbr4	-	10.10.12.0/24	Réseau DMZ (serveurs exposés : HAProxy, Nester)

# SÉCURISATION DE L'INFRASTRUCTURE AVEC pfSense



- **Objectif du service :** Sécuriser et cloisonner les flux réseau entre Roubaix, Kansas et les franchises.
- **Rôle dans le projet :** Filtrage « moindre privilège », mise en place des tunnels VPN (site-à-site IPsec, client-à-site WireGuard), contrôle d'accès aux services critiques (pfSense, GLPI, Grafana, Veeam).
- **Particularité technique :** Pare-feu centralisé avec règles restrictives ; SSH par comptes/clefs (pas de root) ; interfaces web accessibles uniquement depuis le LAN ; VPN chiffrés (AES-256 pour IPsec, WireGuard pour les Harvesters).
- **Mise en place du NAT/PAT pour le serveur Nester (redirection HTTP depuis l'extérieur vers le LAN interne).**

# Annexes – Sécurisation de l'infrastructure avec pfSense

The screenshot shows the pfSense IPsec Status page. At the top, a warning message reads: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title "Status / IPsec / Overview" is displayed, along with navigation links for Overview, Leases, SADs, and SPDs. The main section is titled "IPsec Status" and contains two tables.

**IPsec Status Table:**

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #311	VpnKansas-Roubaix	ID: 10.25.3.47 Host: 10.25.3.47:500 SPI: d842fd4e4fa615bd	ID: 10.25.3.27 Host: 10.25.3.27:500 SPI: 50af2b0e86c2d617	IKEv2 Initiator	Rekey: 25305s (07:01:45) Reauth: Disabled	AES_CBC (128) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established 30 seconds (00:00:30) ago

**SPD Status Table:**

ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats
con1: #1132	Multiple	10.10.10.0/24 10.10.12.0/24 10.10.30.0/24 10.10.40.0/24	Local: cd23b55a Remote: c8ee59fc	192.168.60.0/24	Rekey: 2906s (00:48:26) Life: 3570s (00:59:30) Install: 30s (00:00:30)	AES_GCM_16 (128) IPComp: None	Bytes-In: 45,671 (45 KiB) Packets-In: 34 Bytes-Out: 11,964 (12 KiB) Packets-Out: 87

État du VPN site-to-site IPsec sur le pfSense de Roubaix (connexion avec Kansas)

# Annexes – Sécurisation de l'infrastructure avec pfSense

The screenshot shows the pfSense web interface under the 'Firewall / NAT / Outbound' tab. The 'Outbound' tab is selected. In the 'Mode' section, the first option ('Automatic outbound NAT rule generation. (IPsec passthrough included)') is selected. Below this, there is a 'Save' button. The 'Mappings' section contains a table with one row: a WAN interface mapping to port 80 (HTTP) on the WAN address.

Interface	Source Port	Destination Port	NAT Address	Static Port	Description	Actions
WAN	10.10.10.0/24 *	*	WAN address	*	NAT Nester HTTP	

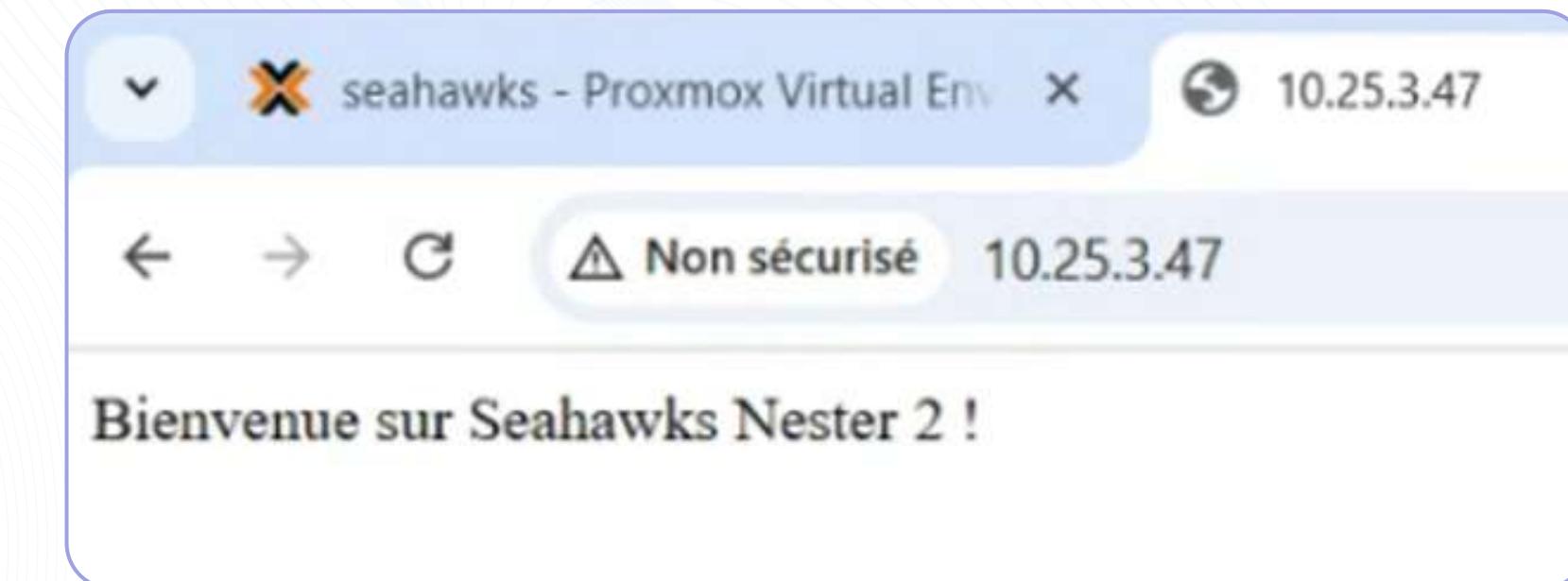
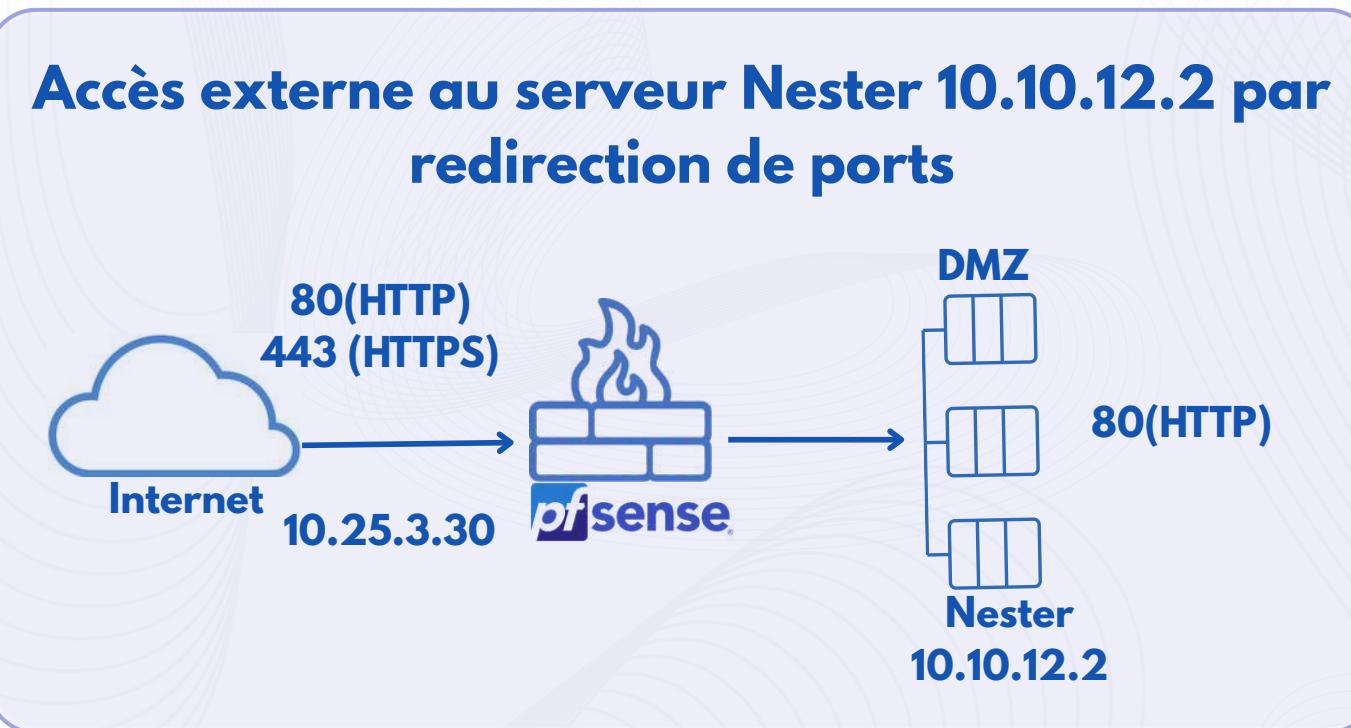
Outbound NAT pfSense — NAT sortant vers l'IP WAN pour accéder à Nester (HTTP)

The screenshot shows the pfSense web interface under the 'Firewall / NAT / Port Forward' tab. The 'Port Forward' tab is selected. In the 'Rules' section, there is a single rule listed: a PAT rule for port 80 (HTTP) on the WAN interface, mapped to port 80 (HTTP) on the internal IP 10.10.12.2. The rule uses TCP protocol and has source ports \* and destination ports \*.

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
WAN	TCP	*	*	WAN address	80 (HTTP)	10.10.12.2	80 (HTTP)	PAT Nester HTTP	

Configuration de la règle NAT/PAT sur pfSense : redirection du port HTTP du WAN vers le serveur interne Nester

# Annexes – Sécurisation de l'infrastructure avec pfSense



Résultat de la redirection : accès externe au serveur Nester via pfSense

# Annexes – Sécurisation de l'infrastructure avec pfSense

WireGuard Tunnels						
Name	Description	Public Key	Address / Assignment	Listen Port	Peers	Actions
▼ tun_wg0	VPNRoubaix-Harvester client to site	6N1mxyaeE+120R8iS1mRcfUPwksB+wY4...	WG_VPN (opt1)	51820	1	
Peers						
Peers	Description	Public Key	Tunnel	Allowed IPs	Endpoint	
	Harvester to Rou...	pPOuiZJQ1zKU55KkY7kZ6pl3kxWNzsjR...	tun_wg0	10.10.20.0/24	10.10.20.2:51820	

Configuration du tunnel WireGuard sur le pfSense de Roubaix

WireGuard Peers					
Description	Public key	Tunnel	Allowed IPs	Endpoint : Port	Actions
Harvester to Rou...	pPOuiZJQ1zKU55Kk...	tun_wg0	10.10.20.0/24	10.10.20.2:51820	

Association du peer Harvester au tunnel WireGuard : clé publique, sous-réseau VPN 10.10.20.0/24 et endpoint configuré

# Annexes – Sécurisation de l'infrastructure avec pfSense



The screenshot shows a terminal window titled "GNU nano 7.2" with the file path "/etc/wireguard/wg0.conf". The configuration file contains the following sections:

```
admin12@debHARVESTER: ~
GNU nano 7.2
/etc/wireguard/wg0.conf

[Interface]
PrivateKey=aEejyNzW7ClpA3uXppQ3NMEnB4caHl7sM/V9AC00d3E=
Address=10.10.20.2/24
DNS=8.8.8.8

[Peer]
PublicKey=6N1mxyaeE+12OR8iS1mRcfUPwksB+wY4VBWwhz2hmA4=
Endpoint=10.25.3.47:51820
AllowedIPs=10.10.20.0/24, 10.10.10.0/24, 10.10.12.0/24, 10.10.30.0/24
PersistentKeepalive=25
```

Extrait de la configuration WireGuard du Harvester (wg0.conf) – IP VPN 10.10.20.2/24

# Annexes – Sécurisation de l'infrastructure avec pfSense

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 ICMP any	KANSAS_NET	*	RBX_NETS	*	*	none		Kansas to Roubaix ICMP [Tests]	
0/0 B	IPv4 TCP/UDP	KANSAS_NET	*	RBX_LAN	PROM_PORTS	*	none		Kansas to Roubaix LAN Prometheus	
0/0 B	IPv4 TCP	KANSAS_NET	*	RBX_LAN	VEEAM_PORTS	*	none		Kansas to Roubaix LAN Veeam	
0/0 B	IPv4 TCP	KANSAS_NET	*	RBX_BASTION	ADMIN_PORTS	*	none		Kansas to Bastion Admin	
0/0 B	IPv4 TCP	KANSAS_NET	*	RBX_DMZ	WEB_PORTS	*	none		Kansas to DMZ	
0/0 B	IPv4 TCP	KANSAS_NET	*	RBX_IT	ADMIN_PORTS	*	none		Kansas to IT admin	

Règles de firewall configurées sur le pfSense du site Kansas

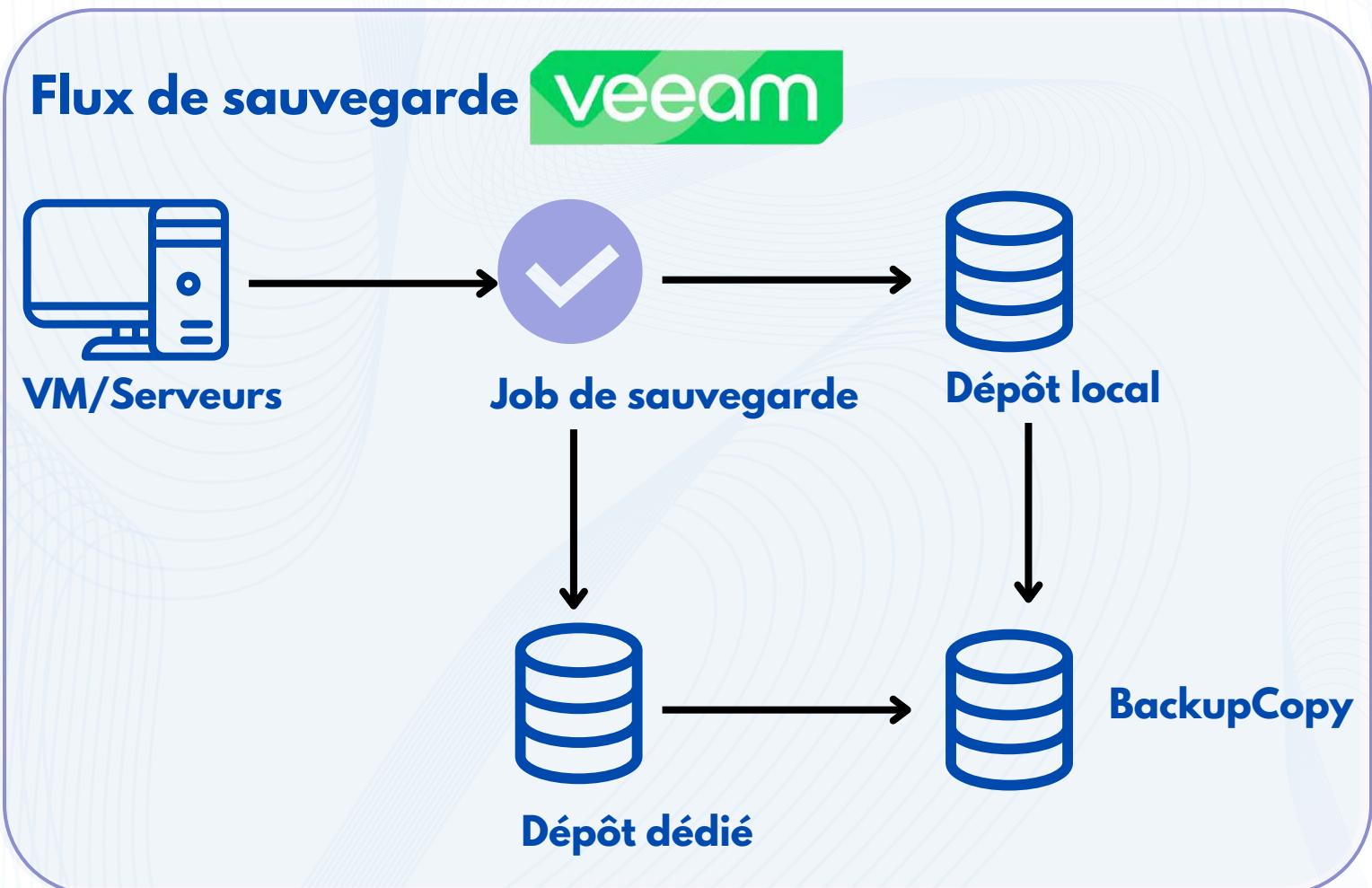
Name	Type	Values	Description	Actions
KANSAS_NET	Network(s)	192.168.60.0/24		
RBX_BASTION	Network(s)	10.10.30.0/24		
RBX_DMZ	Network(s)	10.10.12.0/24		
RBX_IT	Network(s)	10.10.40.0/24		
RBX_LAN	Network(s)	10.10.10.0/24		
RBX_NETS	Network(s)	10.10.10.0/24, 10.10.12.0/24, 10.10.30.0/24, 10.10.40.0/24	All of network in Roubaix	

Définition des alias IP sur pfSense

Name	Type	Values	Description	Actions
ADMIN_PORTS	Port(s)	22, 3389		
PROM_PORTS	Port(s)	9100, 9184		
VEEAM_PORTS	Port(s)	2500, 6160-6200, 10001-10099, 10006, 111-2049		
WEB_PORTS	Port(s)	80, 443		

Définition des alias de ports applicatifs

# SAUVEGARDE AVEC VEEAM BACKUP & RÉPLICATION



- **Objectif du service** (ex : Garantir la sauvegarde fiable et redondante des VMs critiques)
- **Technologie utilisée** (Veeam Backup & Replication Community Edition)
- **Rôle dans le projet** (Sauvegarde quotidienne et Backup Copy)
- **Particularité technique** (Mode agentless et gestion spécifique pour OS non supportés)

# Annexes – Sauvegardes Veeam

The screenshot displays two main windows from the Veeam Backup & Replication interface.

**Left Window (Main View):**

- URL:** https://10.25.3.30:8006/?console=kvm&novnc=1&vmid=115&vmname=vm-win-veeambackupsrv&node=seahawks&resize=off&cmd=
- Panel:** Home
- Search Bar:** Type in an object name to search for
- Table:** All jobs
 

Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target
Backup Copy Alpine	Backup Copy	1	Stopped	9 hours ago	Success	<As new restore poi...	Depot-BackupduBackup
Backup Copy Gitlab	Backup Copy	1	Stopped	2 days ago	Success	<As new restore poi...	Depot-BackupduBackup
Backup Copy Nester2	Backup Copy	1	Stopped	9 minutes ago	Success	<As new restore poi...	Depot-BackupduBackup
Backup Copy Nester3	Backup Copy	1	Stopped	7 minutes ago	Success	<As new restore poi...	Depot-BackupduBackup
Backup Copy vm-glpi	Backup Copy	1	Stopped	2 days ago	Success	<As new restore poi...	Depot-BackupduBackup
Backup Copy/Nester1...	Backup Copy	2	Stopped	19 hours ago	Success	<As new restore poi...	Depot-BackupduBackup
backup Arch via nest...	Linux Agent Backup	1	Stopped	2 days ago	Success	<Not scheduled>	depot linux
Backup gitlab	Linux Agent Backup	1	Stopped	2 days ago	Success	<Not scheduled>	depot linux
Backup nester 1	Linux Agent Backup	1	Stopped	19 hours ago	Success	18/07/2025 22:00	depot linux
Backup Nester3	Linux Agent Backup	1	Stopped	2 days ago	Success	<Not scheduled>	depot linux
Backup NFS Alpine vi...	Linux Agent Backup	1	Stopped	2 days ago	Success	<Not scheduled>	depot linux
BackupNester2	Linux Agent Backup	1	Stopped	3 days ago	Success	<Not scheduled>	depot linux
BackupVm/glpi	Linux Agent Backup	1	Stopped	2 days ago	Success	<Not scheduled>	Default Backup
- Bottom Text:** Vue globale des jobs de Backup & Backup Copy Veeam

**Right Window (Job Details):**

- Panel:** Job details for "Agent Backup Job 1D..."
- Search Bar:** Type in an object name to search for
- Table:** Agent Backup Job 1D...
 

Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target
Agent Backup Job 1D...	Linux Agent Backup	1	Stopped	16 hours ago	Success	<Not scheduled>	Default Backup Repository
backup job (vm-back...	Linux Agent Backup	1	Stopped	4 minutes ago	Success	<Not scheduled>	Depot-Linux-Veeam
- Summary:**

SUMMARY	DATA	STATUS	THROUGHPUT (ALL TIME)
Duration: 03:26	Processed: 5,7 GB (100%)	Success: 1 ✓	Speed: 201
Processing rate: 40 MB/s	Read: 5,7 GB	Warnings: 0	
Bottleneck: Source	Transferred: 2,3 GB (2,5x)	Errors: 0	
- Log:**

Name	Status	Action	Duration
debian	Success	✓ Job started at 04/07/2025 10:12:14 ✓ Building the list of objects to process ✓ Processing debian ✓ Load: Source 85% > Proxy 82% > Network 9% > Target 25% ✓ Primary bottleneck: Source ✓ Job finished at 04/07/2025 10:15:40	00:08 02:33

Sauvegardes vers dépôt isolé Linux et dépôt par défaut

# Annexes – Sauvegardes pfSens

The screenshot displays two windows illustrating the automated backup process for pfSense configurations.

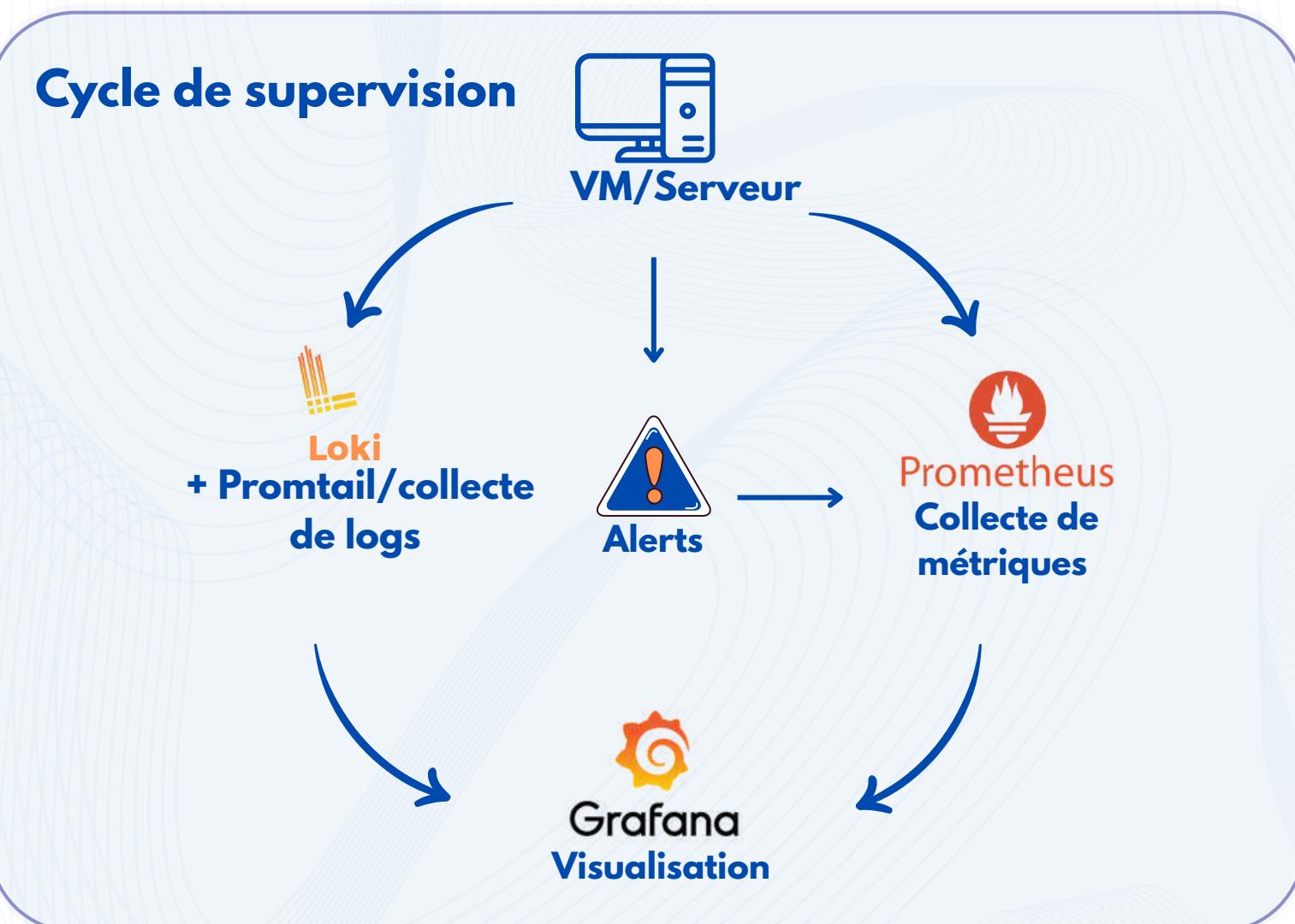
**Windows Task Scheduler:** Shows a list of scheduled tasks. One task, named "Sauvegarde pfSense", is highlighted and shows a successful execution history. The most recent execution at 17/07/2025 13:00:00 is marked with a red box around the status message "L'opération a réussi. (0x0)".

**File Explorer:** Shows the directory structure for the backup configuration files. The path is Ce PC > Disque local (C:) > Backup\_config > Pfsens. Inside this folder, there are three XML files: config-pfSense\_Kansas.xml, config-pfSense\_Roubaix.xml, and config-Pfsense-NFL.xml. These files are also highlighted with a red box.

*Tâche planifiée exécutée avec succès dans le planificateur Windows.*

*Fichier de sauvegarde généré automatiquement par le script programmé*

# SUPERVISION AVEC PROMETHEUS, GRAFANA ET LOKI

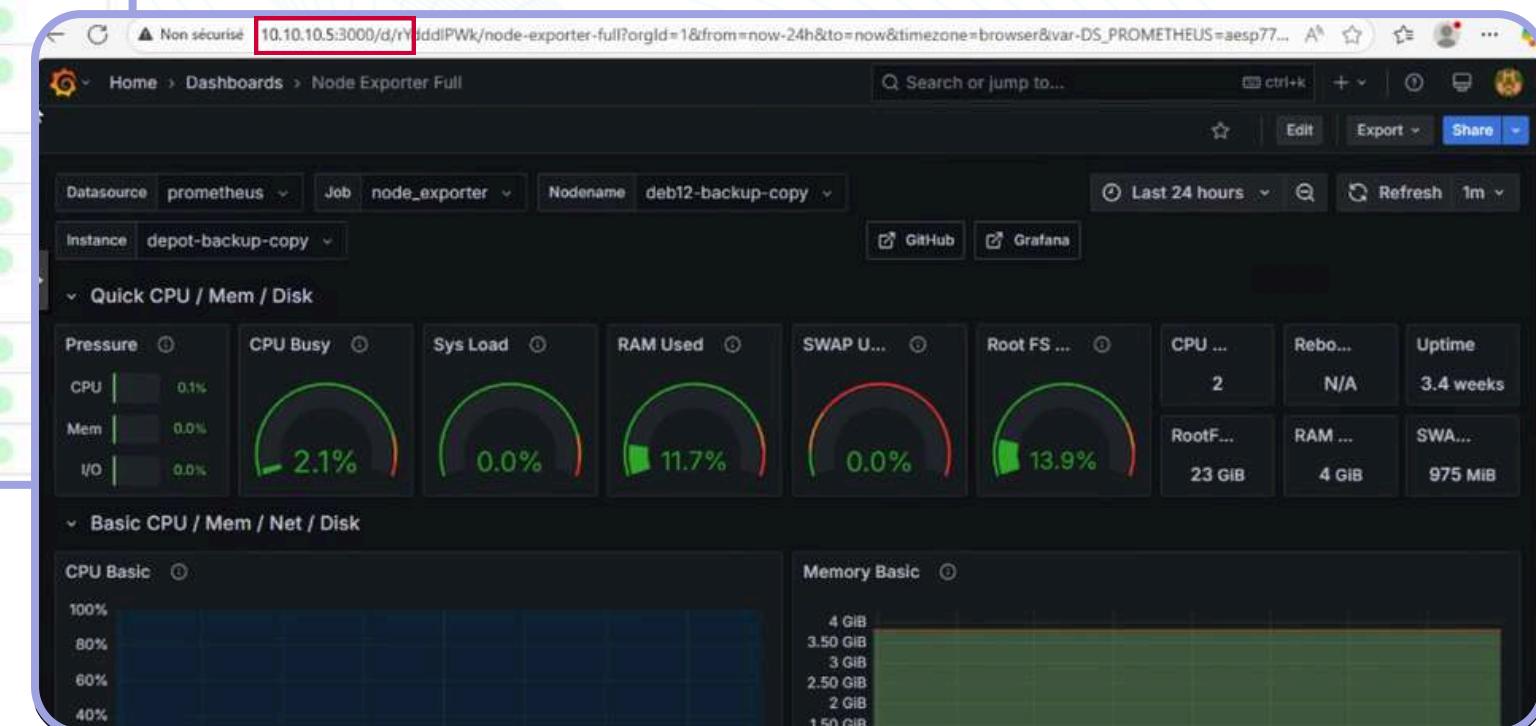


- **Objectif du service :** Assurer le suivi en temps réel des performances et de l'état des systèmes.
- **Technologies utilisées :** Prometheus, Grafana, Loki, Promtail.
- **Rôle dans le projet :** Centraliser la supervision des serveurs, collecter les métriques et les logs, et générer des alertes.
- **Particularité technique :** Architecture combinant supervision des métriques et des logs avec visualisation unifiée dans Grafana.
- **Cas particulier pfSense :** métriques SNMP collectées par Telegraf, exposées à Prometheus puis visualisées dans Grafana

# Annexes - Supervision Prometheus&Grafana

The screenshot shows the Prometheus interface at [10.10.10.5:9090/targets](http://10.10.10.5:9090/targets). The top navigation bar has a red box around the 'Status > Target health' button. Below it, there are filters for 'Select scrape pool', 'Filter by target health', and 'Filter by endpoint or labels'. The main table lists targets under the 'node\_exporter' job, with columns for 'Endpoint', 'Labels', 'Last scrape', and 'State'. All targets are marked as 'UP' with green status indicators. A 'Last target scrape' button is visible at the bottom.

Liste des métriques supervisées par Prometheus



Vue des métriques systèmes collectées depuis les VM

# Annexes - Supervision Prometheus&Grafana

The image displays two screenshots illustrating the integration of Grafana and Prometheus for system monitoring.

**Grafana Interface (Left):** Shows a log volume visualization for the "loki" data source. The chart displays a single data series named "logs" with a value of 2. Below the chart, a log viewer shows two entries from July 28, 2025, at 14:54:11.516:

```
> 2025-07-28 14:54:11.516 log test graf-prom lun. 28 juillet. 2025 14:54:11 CEST
> 2025-07-28 14:54:11.516 log test graf-prom lun. 28 juillet. 2025 14:54:11 CEST
```

**Prometheus Interface (Right):** Shows the configuration for an alert rule named "alert\_cpu". The rule triggers when CPU usage exceeds 80% for more than one minute. The alert is currently firing, as indicated by the red border around the "FIRING (1)" button.

**Log Volume Visualization:**

**Alert Rule Configuration:**

```
100 - (avg by (instance) (rate(node_cpu_seconds_total{mode="idle"}[2m])) * 100) > 80
```

**Alert Details:**

- HighCPUUsage**: The alert is triggered by the metric `node_cpu_seconds_total{mode="idle"}`.
- severity**: warning
- description**: L'utilisation du CPU est supérieure à 80% depuis plus d'une minute.
- summary**: CPU (élevé sur [[ \$labels.instance ]])
- Alert labels**: alertname="HighCPUUsage", instance="grafip", severity="warning"
- State**: FIRING
- Active Since**: 1m 32.774s
- Value**: 100

Consultation des logs systèmes grâce à Grafana + Loki

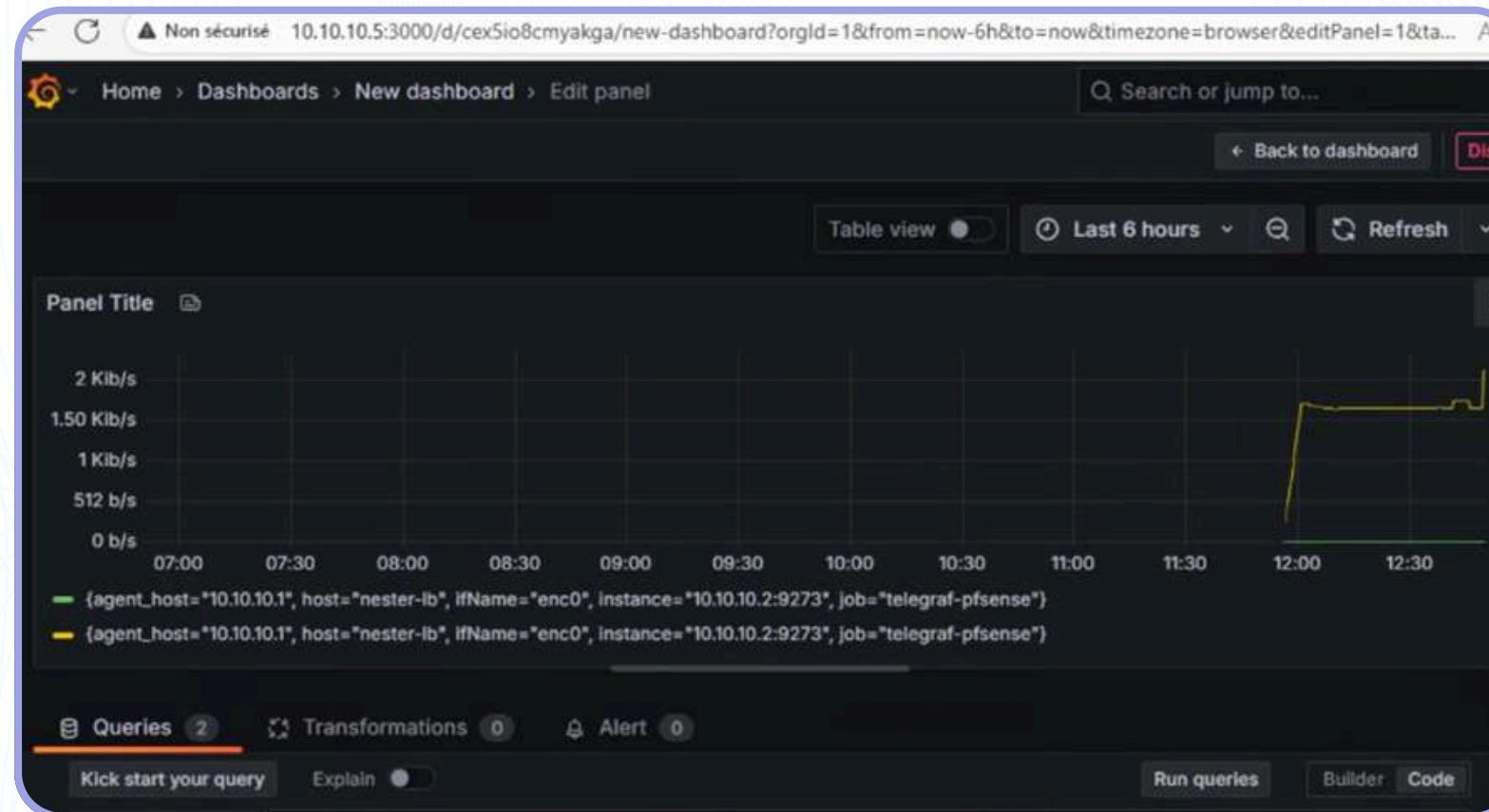
# Annexes - Supervision Prometheus&Grafana



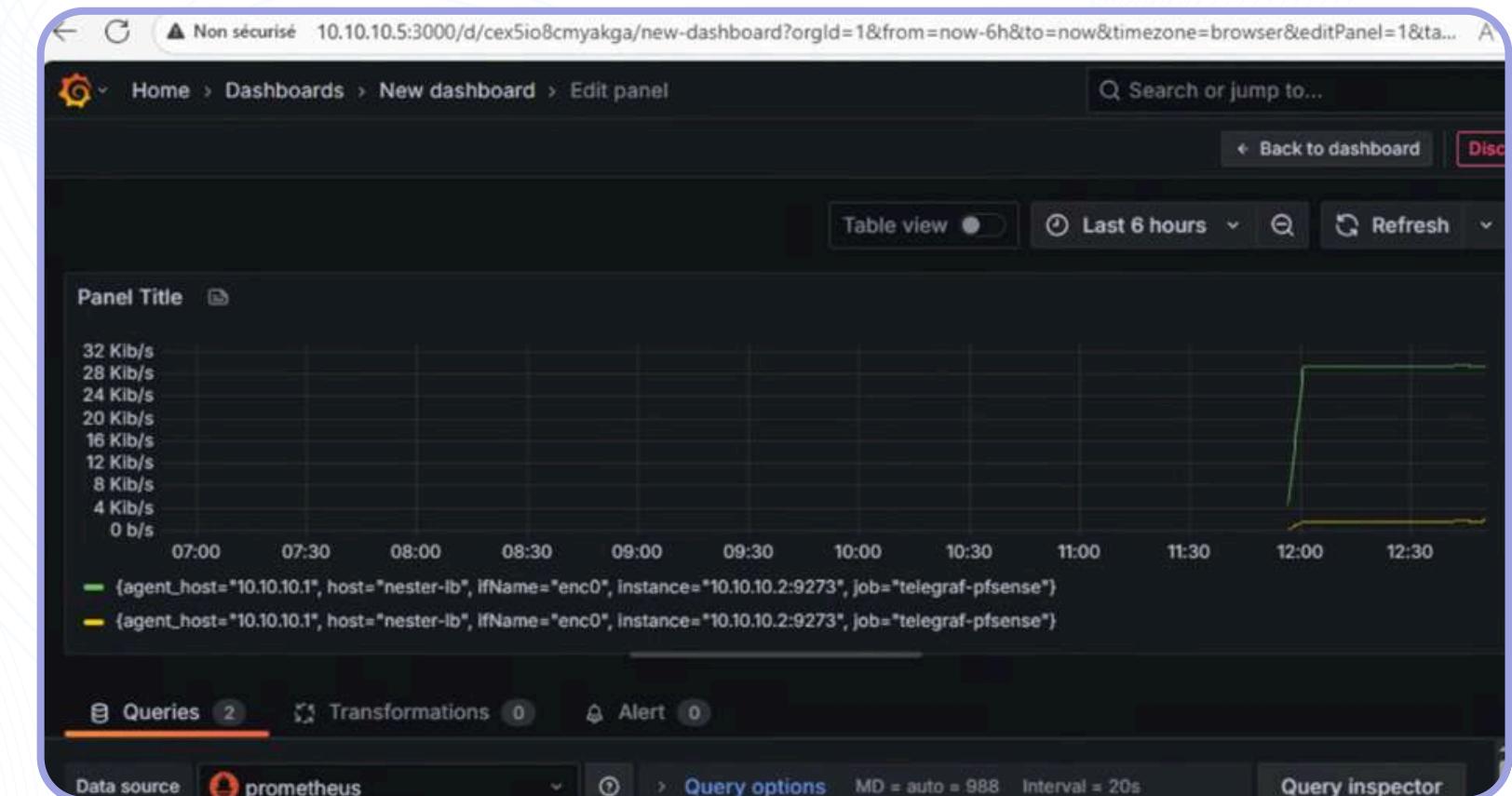
telegraf-pfsense				1 / 1 up	↻
Endpoint	Labels	Last scrape	State		
<a href="http://10.10.10.2:9273/metrics">http://10.10.10.2:9273/metrics</a>	instance="10.10.10.2:9273"; job="telegraf-pfsense"	30.293s ago	UP	Activer Windows	ACCEDEZ aux paramètres pour activer Windows.

Vérification que le job telegraf-pfsense est bien actif et que Prometheus récupère les métriques

# Annexes - Supervision Prometheus&Grafana



Supervision du statut de l'interface WAN (enc0) de pfSense



Traffic réseau entrant/sortant sur l'interface WAN (enc0) de pfSense

# TICKETING AVEC Glpi



- **Objectif du service :** Centraliser et suivre la gestion des incidents et demandes.
- **Technologie utilisée :** GLPI (module Ticketing).
- **Rôle dans le projet :** Assurer la traçabilité, la priorisation et le suivi des tickets.
- **Particularité technique :** Accès différencié par profil (utilisateur, technicien, admin) avec notifications automatiques.

# Annexes - GLPI Ticketing

The screenshot shows the GLPI ticketing interface. On the left, a sidebar menu is visible with categories like Assets, Assistance (selected), Tickets, Problems, Changes, Planning, Statistics, Management, Tools, Administration, and Setup. The main area displays a ticket titled "Unable to access the Seahawks monitoring portal (1)". The ticket details are as follows:

**Title:** Unable to access the Seahawks monitoring portal (1)  
**Opened:** 2025-07-30 14:36  
**Resolved:** 2025-07-31 06:54  
**Closed:** 2025-07-31 07:07  
**Type:** Incident  
**Category:** -----  
**Status:** Closed  
**Last Update:** 2025-07-31 07:07  
**Requester:** normal i  
**Technician:** tech i  
**Time To Resolve:** 00:00:00

The ticket content is divided into three sections:

- Initial Message (TE):** "Seahawks web interface via the address 10.10.10.5. The browser shows a connection error. I've already restarted my PC and checked the network cable. Please verify if the service is online."
- Response (TE):** "Ticket received. First verification : the Seahawks portal at 10.10.10.5 is unreachable from internal network as well. I will check the HAProxy and NGINX services on the web cluster"
- Solution (TE):** "The NGINX service on the web server was down. I restarted the service using systemctl restart nginx, and confirmed that the Seahawks portal is accessible again from 10.10.10.5."

*Ticket GLPI côté technicien : message initial, réponse, et solution*

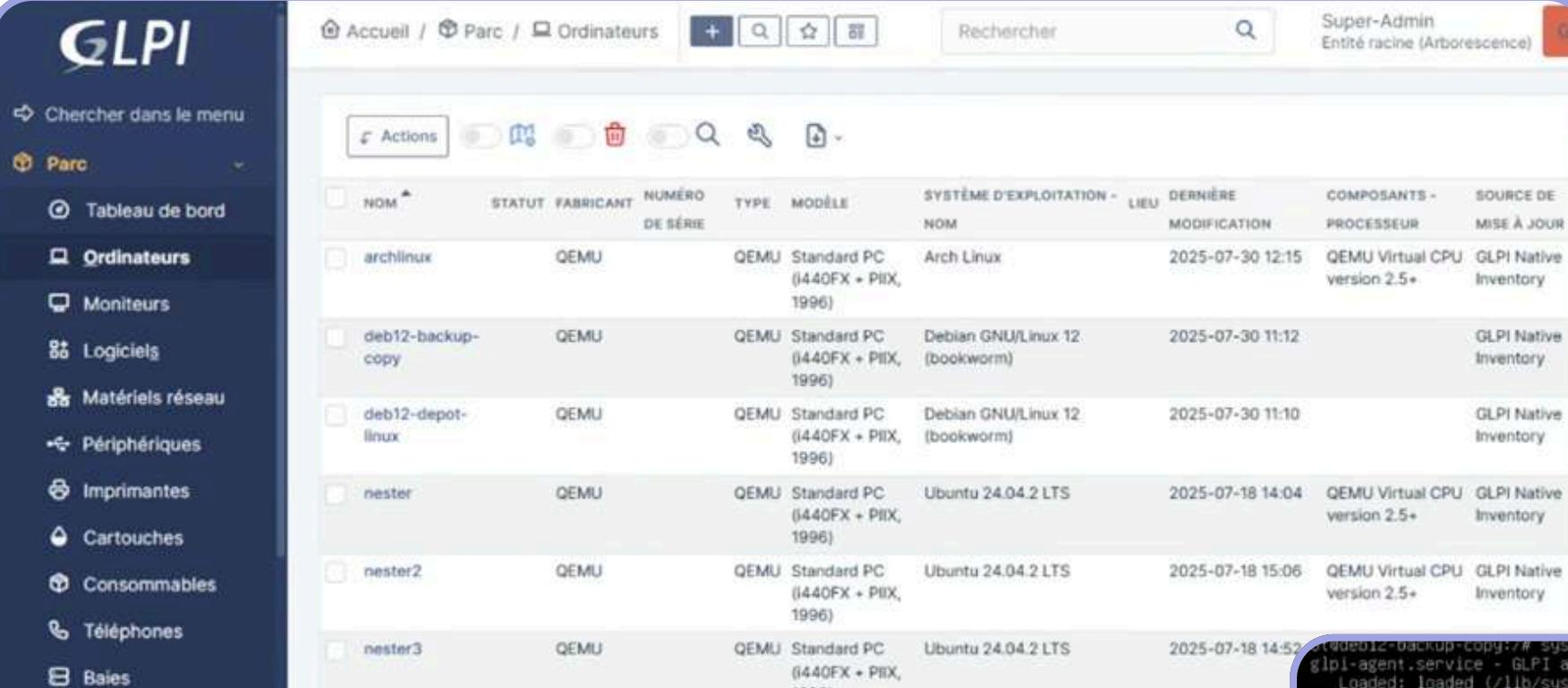
*Ticket GLPI clôturé*

# INVENTAIRE AVEC



- **Objectif du service :** Maintenir un inventaire automatisé et à jour des machines et équipements.
- **Technologie utilisée :** GLPI Inventory + agents GLPI.
- **Rôle dans le projet :** Collecter et centraliser les informations matérielles et logicielles des serveurs et postes clients.
- **Particularité technique :** Inventaire automatique par agent GLPI, avec méthodes alternatives pour les équipements non compatibles (ex. pfSense).

# Annexes - GLPI Inventoring



The screenshot shows the GLPI web interface for managing a fleet of computers. The left sidebar lists categories like 'Tableau de bord', 'Ordinateurs' (selected), 'Moniteurs', etc. The main area displays a table of 10 inventory entries:

NOM	STATUT	FABRICANT	NUMÉRO DE SÉRIE	TYPE	MODELE	SYSTÈME D'EXPLOITATION	LIEU	DERNIÈRE MODIFICATION	COMPOSANTS	SOURCE DE MISE À JOUR
archlinux	QEMU	QEMU		Standard PC (i440FX + PII, 1996)		Arch Linux		2025-07-30 12:15	QEMU Virtual CPU	GLPI Native Inventory
deb12-backup-copy	QEMU	QEMU		Standard PC (i440FX + PII, 1996)		Debian GNU/Linux 12 (bookworm)		2025-07-30 11:12		GLPI Native Inventory
deb12-depot-linux	QEMU	QEMU		Standard PC (i440FX + PII, 1996)		Debian GNU/Linux 12 (bookworm)		2025-07-30 11:10		GLPI Native Inventory
nester	QEMU	QEMU		Standard PC (i440FX + PII, 1996)		Ubuntu 24.04.2 LTS		2025-07-18 14:04	QEMU Virtual CPU	GLPI Native Inventory
nester2	QEMU	QEMU		Standard PC (i440FX + PII, 1996)		Ubuntu 24.04.2 LTS		2025-07-18 15:06	QEMU Virtual CPU	GLPI Native Inventory
nester3	QEMU	QEMU		Standard PC (i440FX + PII, 1996)		Ubuntu 24.04.2 LTS		2025-07-18 14:52		
SrvVeeamBR	QEMU	QEMU		Standard PC	Microsoft Windows			2025-07-30 12:44		

A tooltip on the right side of the table provides a detailed status report for one of the entries:

```

root@deb12-backup-copy:/# systemctl status glpi-agent
glpi-agent.service - GLPI agent
   Loaded: loaded (/lib/systemd/system/glpi-agent.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-07-20 12:14:46 CEST; 1 week 3 days ago
       Docs: man:glpi-agent
     Main PID: 480 (glpi-agent: wai)
        Tasks: 1 (limit: 4637)
      Memory: 76.4M
         CPU: 5min 48.686s
        CGroupl: /system.slice/glpi-agent.service
           └─480 "glpi-agent: waiting"

```

*Liste des machines inventoriées automatiquement dans GLPI*

*Installation de l'agent GLPI sur une machine cliente*



# Annexes - GLPI Inventoring

Fiche GLPI de pfSense du site Kensas avec rapport d'inventaire HTML intégré

The screenshot displays two windows side-by-side. The left window is a browser showing a pfSense inventory report titled "Inventaire automatique pfSense - Kensas". It includes sections for Date (2025-07-20 16:16:16), Adresse IP (10.10.10.1), Nom d'hôte (pfSense.home.arp), Version pfSENse (2.7.2-RELEASE), OS & noyau (FreeBSD pfSense.home.arp 14.0-CURRENT FreeBSD 14.0-CURRENT amd64 1400094 #1 RELENG\_2\_7\_2-n255948-8d2b56da39c: Wed Dec 6 20:45:47 UTC 2023 root@freebsd:/var/jenkins/wd), and Interfaces réseau (ifconfig) with output for em0. The right window is the GLPI software's "Documents" module, specifically the "Ordinateurs" section. It shows a list of documents, with one item highlighted: "Rapport inventaire - Juillet 2025" by "Entité racine" (Type: text/html, Date: 2025-07-18 12:57). A red box highlights the "Documents" tab in the GLPI interface.

Inventaire automatique pfSense - Kensas

Date : 2025-07-20 16:16:16

Adresse IP : 10.10.10.1

**Nom d'hôte**

pfSense.home.arp

**Version pfSENse**

2.7.2-RELEASE

**OS & noyau**

FreeBSD pfSense.home.arp 14.0-CURRENT FreeBSD 14.0-CURRENT amd64 1400094 #1 RELENG\_2\_7\_2-n255948-8d2b56da39c: Wed Dec 6 20:45:47 UTC 2023 root@freebsd:/var/jenkins/wd

**Interfaces réseau (ifconfig)**

```
em0: flags=1008843 metric 0 mtu 1500
description: WAN
options=48120bb
ether bc:24:11:b8:4a:e1
inet 10.25.3.47 netmask 0xffffffff broadcast 10.25.15.255
inet fe80::be24:11ff:feb8:4a1%em0 prefixlen 64 scopeid 0x1
media: Ethernet autoselect (1000baseT )
```

Fiche GLPI de pfSense du site Kensas avec rapport d'inventaire HTML intégré

Non sécurisé 192.168.60.20/glpi/front/computer.form.php?id=3

Accueil / Parc / Ordinateurs + Rechercher Super-Admin Entité racine (Arborescence) GLPI

Ajouter un document

Analyse d'impact

Systèmes d'exploitation

Composants

Volumes

Logiciels

Connexions

Ports réseau

Connecteurs

Contrôle à distance

Gestion

Contrats

Actions

Documents 1

Rapport inventaire - Juillet 2025

Entité racine

pfsense-kensas-report...

text/html

#75ceaf14-e509fb39-687a44a3142404.87060471#

2025-07-18 12:57

Associer un document existant

Actions

Documents

Nom Entité Fichier Lien web Rubrique Type MIME Balise Date

Rapport inventaire - Juillet 2025 Entité racine pfsense-kensas-report... text/html #75ceaf14-e509fb39-687a44a3142404.87060471# 2025-07-18 12:57

Nom Entité Fichier Lien web Rubrique Type MIME Balise Date

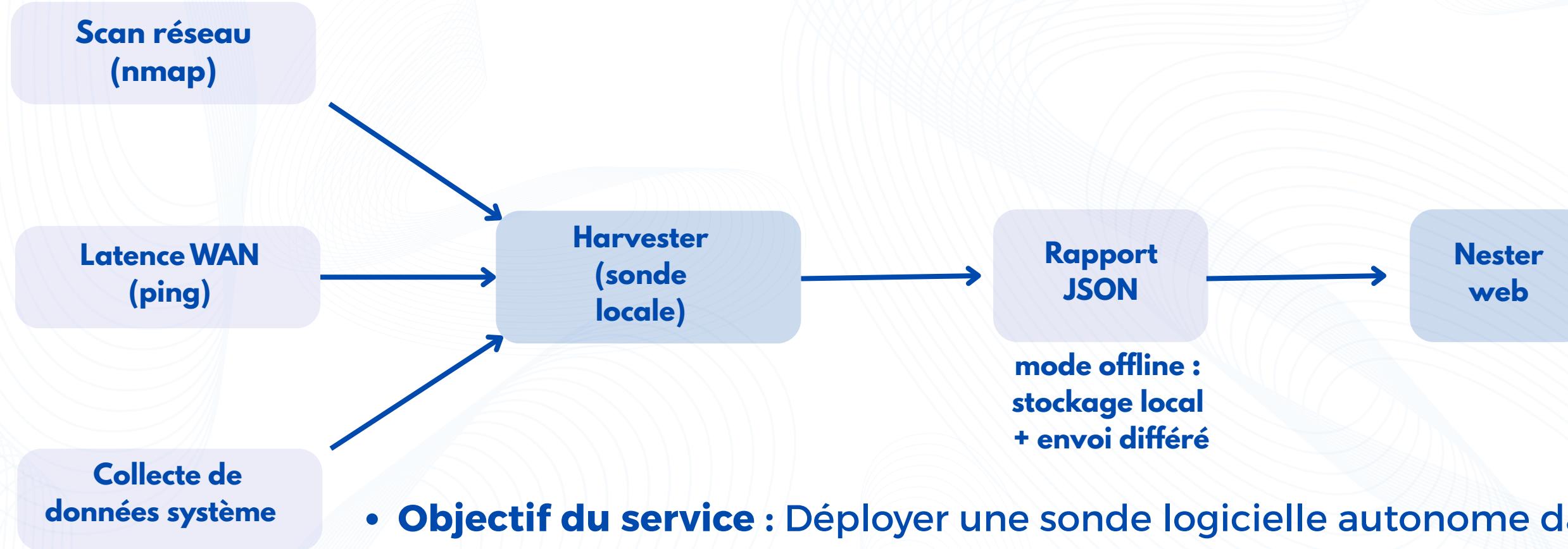
Virtualisation

Extrait du rapport HTML généré par script depuis pfSense, joint à la fiche GLPI

# DE LA COLLECTE À LA CENTRALISATION

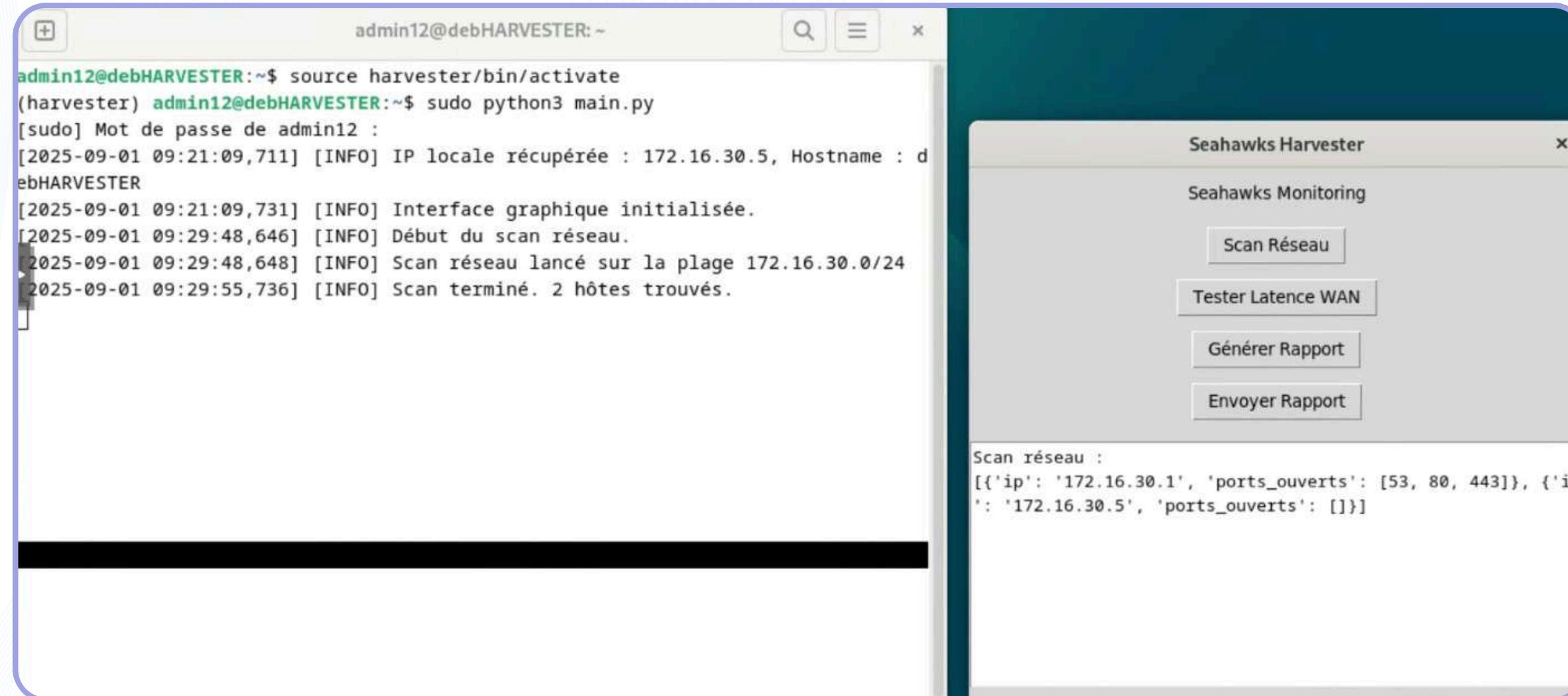


# L'APPLICATION HARVESTER



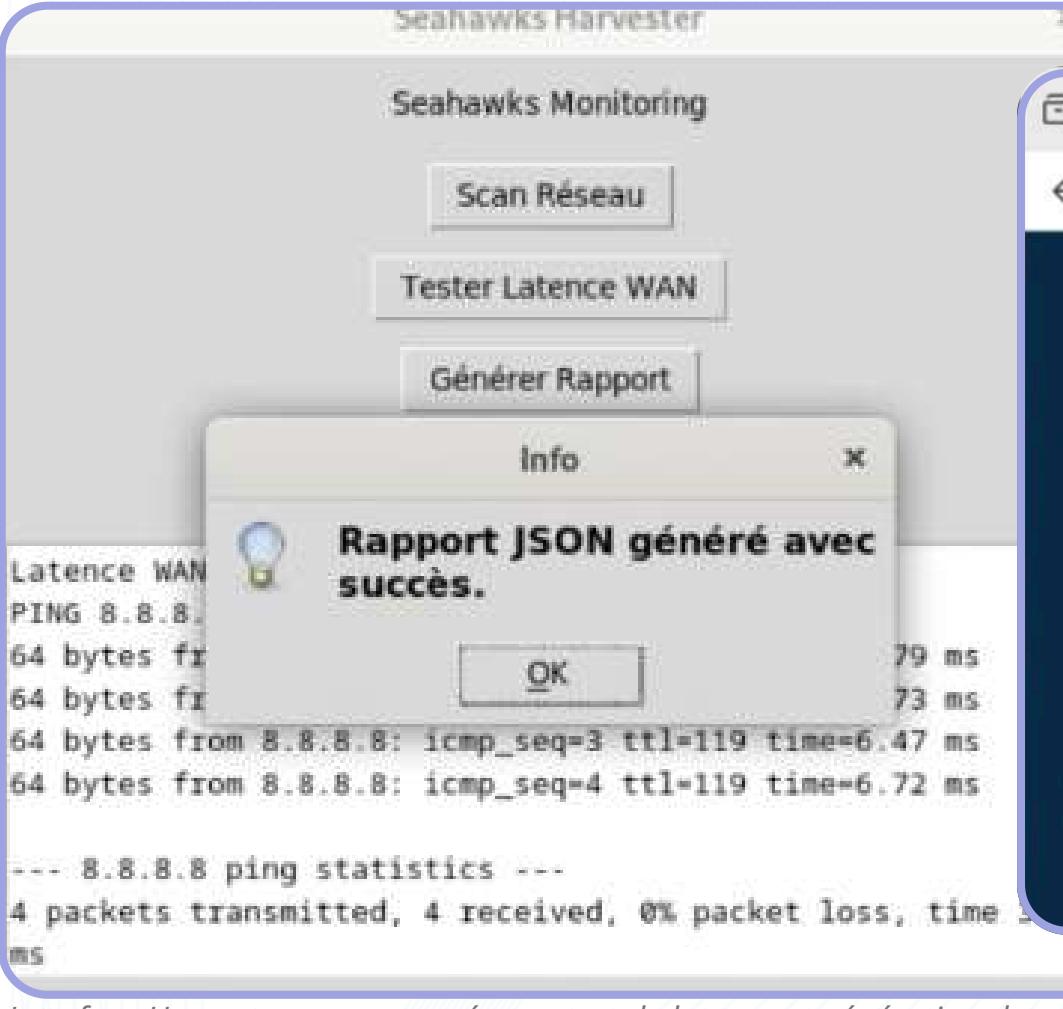
- **Objectif du service :** Déployer une sonde logicielle autonome dans chaque franchise NFL pour collecter les informations réseau et système.
- **Technologies utilisées :** Python (interface Tkinter), nmap (scan réseau), scripts internes (latence, rapports JSON).
- **Rôle dans le projet :** Fournir un diagnostic local et transmettre les données collectées vers Nester (application web centralisée).
- **Particularité technique :** Fonctionne même sans connexion avec le datacenter, stockage local des rapports et envoi différé.

# Annexes - Application Harvester



Harvester – Interface locale. Exécution d'un scan réseau via l'interface graphique Python.

# Annexes - Application Harvester



The screenshot shows the Seahawks Harvester application interface. On the left, there's a sidebar with "Seahawks Harvester" at the top, followed by "Seahawks Monitoring" and three buttons: "Scan Réseau", "Tester Latence WAN", and "Générer Rapport". A modal window titled "Info" is open, displaying a green icon and the message "Rapport JSON généré avec succès." (JSON report generated successfully). Below the modal, there's some terminal-like output related to network traffic analysis.

Dashboard Nester – Vue des Harvesters. Tableau de bord central affichant les données collectées (IP, latence WAN, horodatage).

Dashboard - Seahawks Neste x +

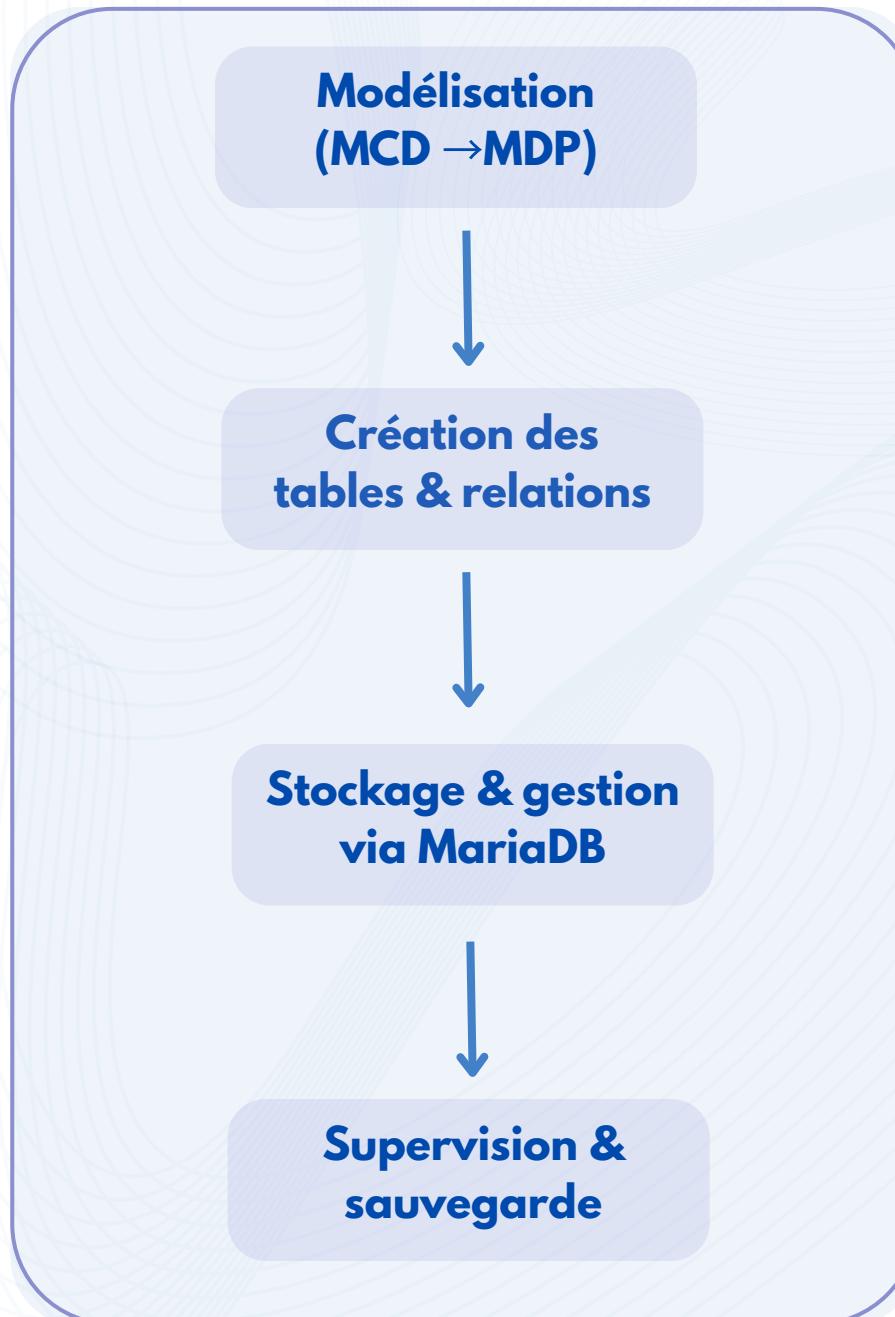
Non sécurisé http://10.10.12.2/dashboard

Tableau de bord - Données des Harvesters

ID	Nom de machine	Adresse IP	Latence WAN	Horodatage	Version	Détails
17	debHARVESTER	172.16.30.5	PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data. 64 by	2025-09-09 13:37:59	1.0.0	<a href="#">Voir</a>
16	debHARVESTER	172.16.30.5	PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data. 64 by	2025-09-08 16:24:57	1.0.0	<a href="#">Voir</a>
15	debHARVESTER	172.16.30.5	PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data. 64 by	2025-08-29 15:16:27	1.0.0	<a href="#">Voir</a>
13	debHARVESTER	172.16.30.5	PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data. 64 by	2025-08-28 14:54:33	1.0.0	<a href="#">Voir</a>
11	debHARVESTER	172.16.30.5	PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data. 64 by	2025-08-27 22:52:56	1.0.0	<a href="#">Voir</a>
1	debHARVESTER	172.16.30.5	PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data. 64 by	2025-08-27 20:25:45	1.0.0	<a href="#">Voir</a>

Interface Harvester avec scan réseau, test de latence et génération de rapport JSON

# LA BASE DE DONNÉES NESTER\_MANAGER



- **Objectif du service :** Centraliser la gestion et les données des Harvesters.
- **Technologie utilisée :** MariaDB (SGBD open source, fiable et performant).
- **Rôle dans le projet :** Stockage structuré des données techniques et opérationnelles.
- **Particularité technique :** Sauvegarde planifiée via script bash et supervision par Grafana.

# Annexes - Base de données nester-manager

```
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 371
Server version: 10.5.27-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| nester_manager |
| performance_schema |
| seahawks_db |
+-----+
5 rows in set (0,001 sec)

MariaDB [(none)]>
```

Figure 48 Affichage des bases disponibles dans MariaDB, dont nester\_manager et seahawks\_db

```
root@vm-db-nester html]# mariadb
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 6
Server version: 10.5.27-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SELECT user, host FROM mysql.user;
+-----+-----+
| User      | Host    |
+-----+-----+
| mariadb.sys | localhost |
| mysql       | localhost |
| root        | localhost |
+-----+-----+
3 rows in set (0,038 sec)

MariaDB [(none)]> ALTER USER 'root'@'localhost' IDENTIFIED BY 'root';
Query OK, 0 rows affected (0,049 sec)

MariaDB [(none)]> FLUSH PRIVILEGES
    ->;
Query OK, 0 rows affected (0,004 sec)
```

Figure 47 Liste des utilisateurs et hôtes autorisés à se connecter à MariaDB

# Annexes - Base de données nester-manager

The screenshot shows the phpMyAdmin interface for a MySQL server at localhost. The left sidebar lists databases: Nouvelle base de données, information\_schema, mysql, nester\_manager (selected), performance\_schema, and seahawks\_db. The main area is titled 'Aperçu des comptes utilisateurs' (User Accounts Preview) and displays a table of users:

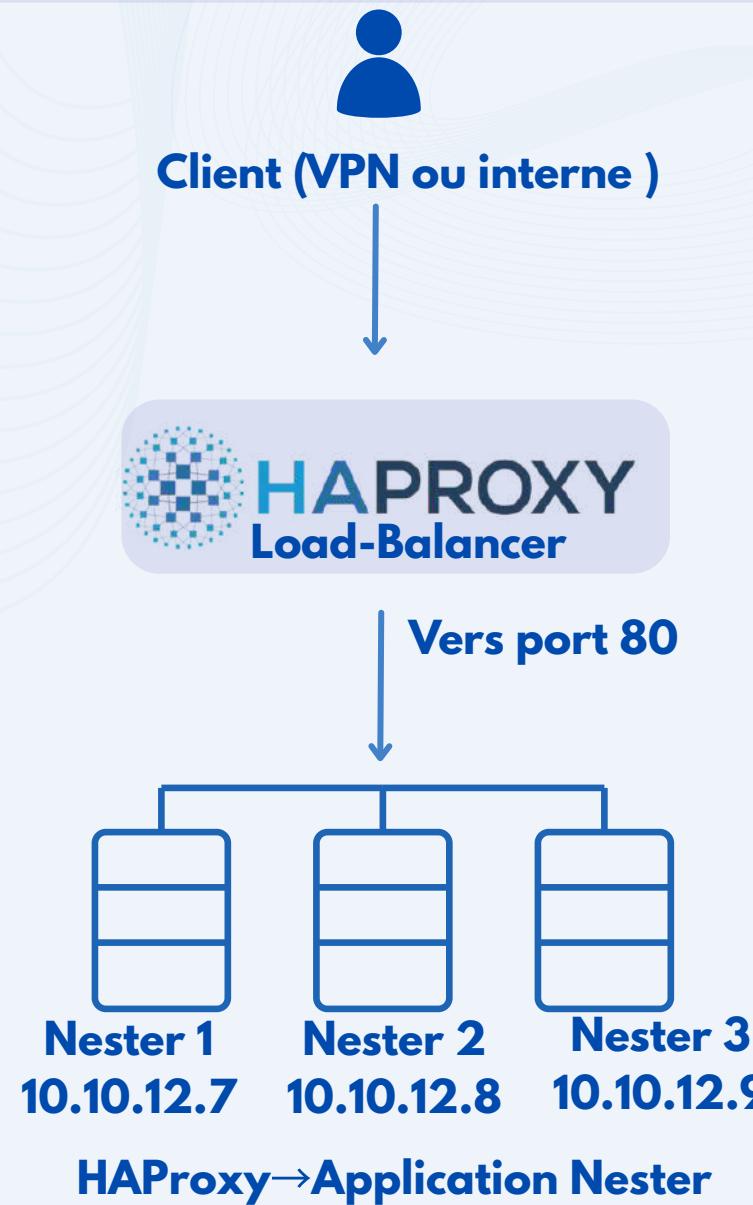
Nom d'utilisateur	Nom d'hôte	Mot de passe	Priviléges globaux	Grant	Action
admin_nester	%	Oui	ALL PRIVILEGES	Oui	<a href="#">Editer les priviléges</a> <a href="#">Exporter</a> <a href="#">Verrouiller</a>
mariadb.sys	localhost	Non	USAGE	Non	<a href="#">Editer les priviléges</a> <a href="#">Exporter</a> <a href="#">Déverrouiller</a>
mysql	localhost	Oui	ALL PRIVILEGES	Oui	<a href="#">Editer les priviléges</a> <a href="#">Exporter</a> <a href="#">Verrouiller</a>
nester_app	10.10.12.%	Oui	USAGE	Non	<a href="#">Editer les priviléges</a> <a href="#">Exporter</a> <a href="#">Verrouiller</a>
root	localhost	Oui	ALL PRIVILEGES	Oui	<a href="#">Editer les priviléges</a> <a href="#">Exporter</a> <a href="#">Verrouiller</a>

Below the table are buttons for 'Tout cocher' (Select All), 'Avec la sélection : [Exporter](#)', 'Nouvel utilisateur' (New User), and 'Ajouter un compte d'utilisateur' (Add User Account).

Figure 50 Interface phpMyadmin : aperçu de la gestion des utilisateurs et droits d'accès à la base MariaDB (Nester Manager)

# LE CLUSTER WEB AVEC HAProxy

## Fonctionnement de cluster Web SewHawks



- **Objectif du service :** Garantir la haute disponibilité et la répartition de charge de l'application Seahawks Nester pour assurer un accès continu et performant.
- **Technologies utilisées :** HAProxy, Debian 12, WireGuard pour l'équilibrage, l'hébergement et la sécurisation des échanges.
- **Rôle dans le projet :** Centraliser l'affichage des données des Harvester et fournir un point d'entrée unique pour les utilisateurs autorisés.
- **Particularités techniques :** Trois nœuds Nester redondants, équilibrage round-robin, chiffrement des communications par VPN.

# Annexes - Le Cluster Web

```
GNU nano 7.2
global
  log /dev/log    local0
  log /dev/log    local1 notice
  chroot /var/lib/haproxy
  stats socket /run/haproxy/admin.sock mode 660 level admin
  stats timeout 30s
  user haproxy
  group haproxy
  daemon

  # Default SSL material locations
  ca-base /etc/ssl/certs
  crt-base /etc/ssl/private

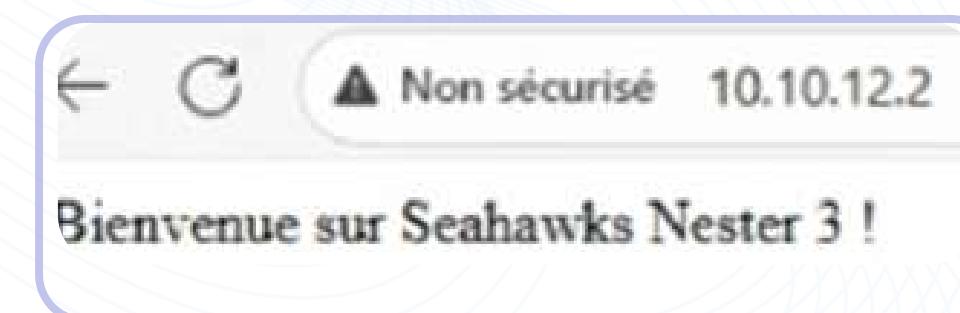
  # See: https://ssl-config.mozilla.org/#server=haproxy&server=ss
  ssl-default-bind-ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-
  ssl-default-bind-ciphersuites TLS_AES_128_GCM_SHA256:TLS_AES_
  ssl-default-bind-options ssl-min-ver TLSv1.2 no-tls-tickets

defaults
  log    global
  mode   http
  option httplog
  option dontlognull
  timeout connect 5000
  timeout client  50000
  timeout server  50000
  errorfile 400 /etc/haproxy/errors/400.http
  errorfile 403 /etc/haproxy/errors/403.http
  errorfile 408 /etc/haproxy/errors/408.http
  errorfile 500 /etc/haproxy/errors/500.http
  errorfile 502 /etc/haproxy/errors/502.http
  errorfile 503 /etc/haproxy/errors/503.http
  errorfile 504 /etc/haproxy/errors/504.http

frontend http_front
  bind *:80
  default_backend nester_servers

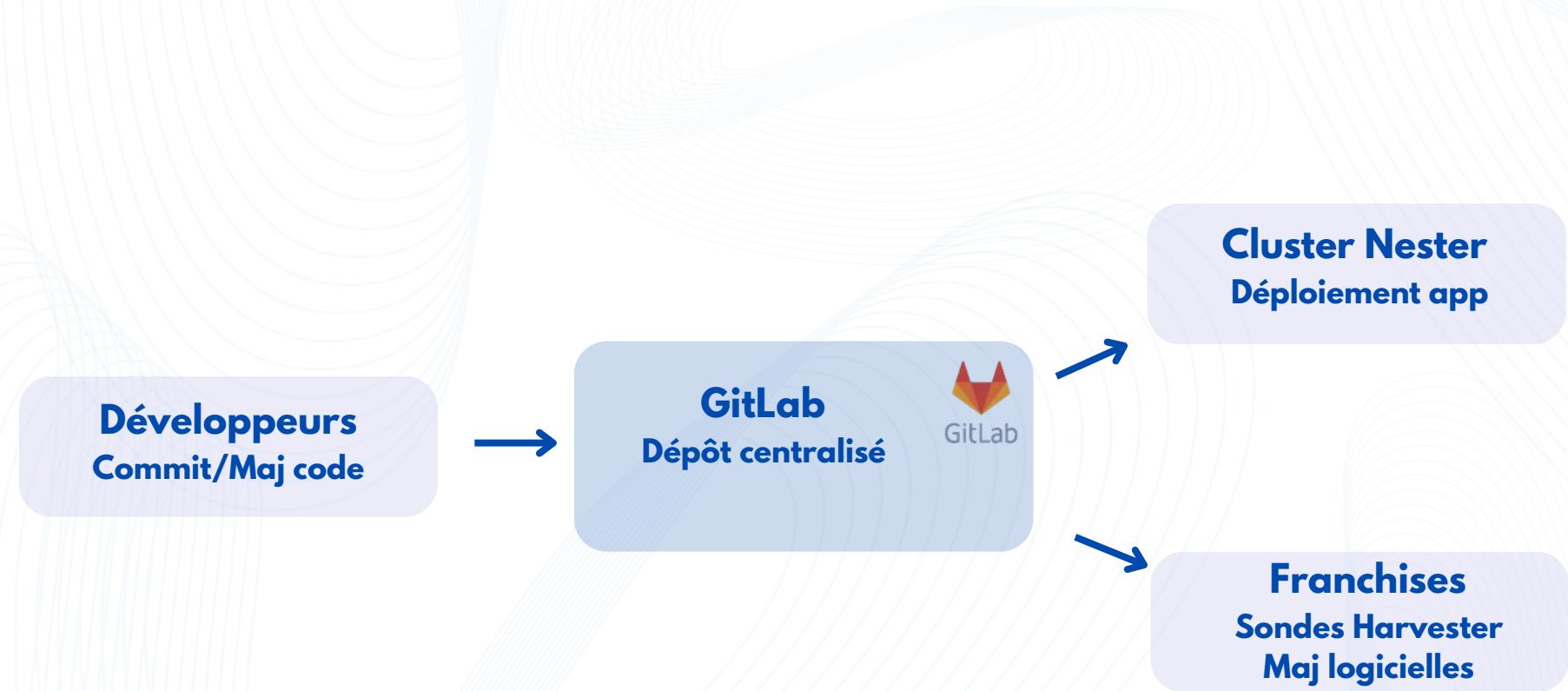
backend nester_servers
  balance roundrobin
  option httpchk
  server nester1 10.10.12.7:8000 check
  server nester2 10.10.12.8:8000 check
  server nester3 10.10.12.9:8000 check
```

Configuration HAProxy du cluster web, avec stratégie round-robin vers les serveurs Nester.



Le Load Balancing HAProxy : balance round-robin.

# GESTION DU CODE SOURCE AVEC



## Objectif du service :

- Centraliser le développement.
- Technologie utilisée :
- GitLab (dépôts de code, gestion collaborative).

## Rôle dans le projet :

- Héberge le code source du Harvester et du Nester.
- Permet le suivi du code source et la gestion des versions des applications Harvester et Nester

## Particularité technique :

- Accès sécurisé via VPN, gestion des versions

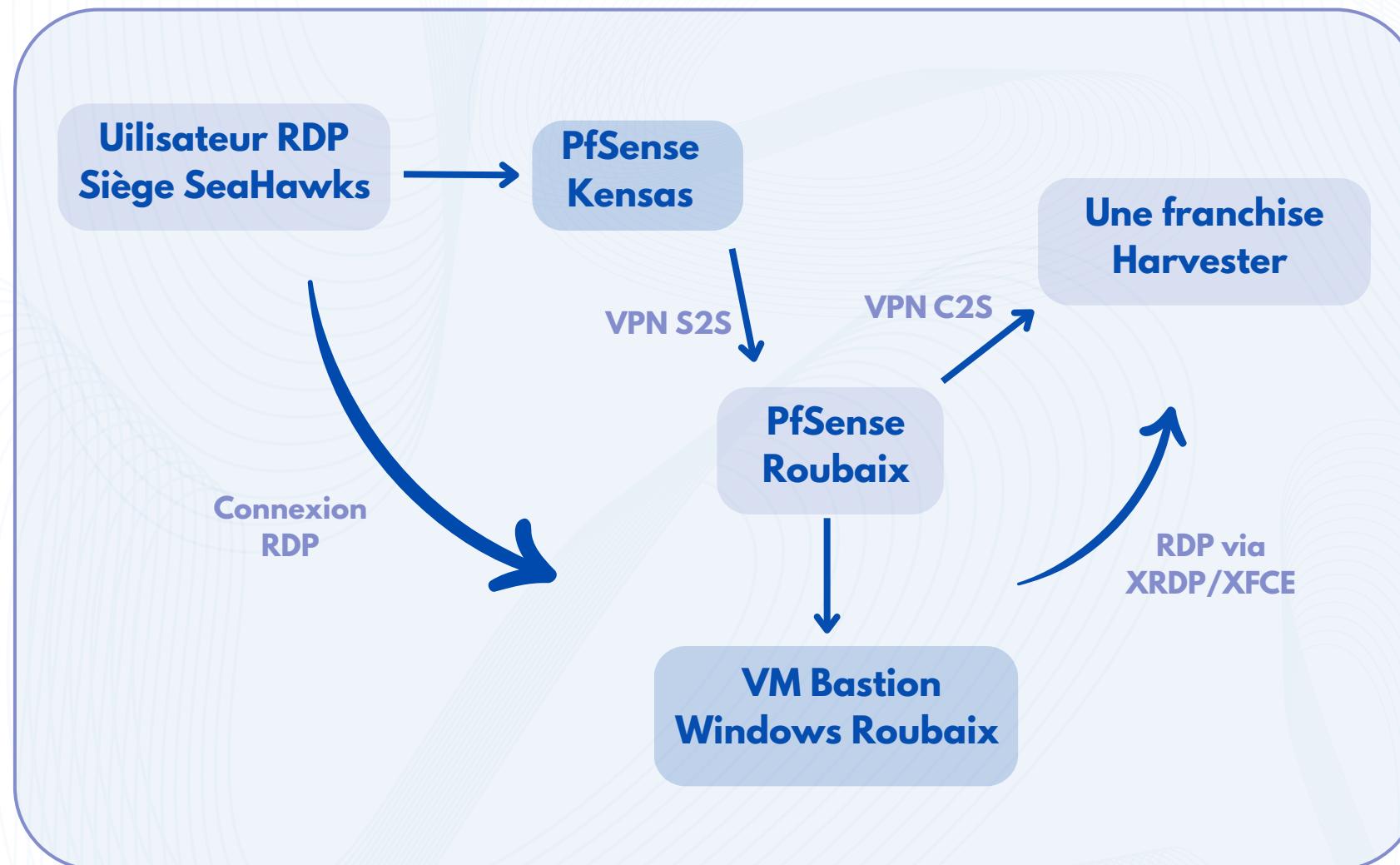
## Annexe - Plateforme GitLab

The screenshot shows the GitLab interface for the 'NFL IT' group. The left sidebar displays the group navigation with 'NFL IT' selected. The main area shows two projects: 'Seahawks Harvester' and 'Seahawks Nester'. Both projects were created 1 month ago and have 0 stars.

Project	Created	Stars
Seahawks Harvester	1 month ago	0
Seahawks Nester	1 month ago	0

Interface Gitlab - Vue des dépôts de code SeaHawks Harvester et SeaHawks Nester centralisés dans Gitlab

# LA TÉLÉMAINTENANCE



## Objectif du service :

- Assurer un accès à distance centralisé et sécurisé aux Harvesters déployés dans les franchises.
- Technologie utilisée :
- VM Windows Bastion (RDP), pfSense (VPN site-à-site et WireGuard), XRDP + XFCE sur Debian.

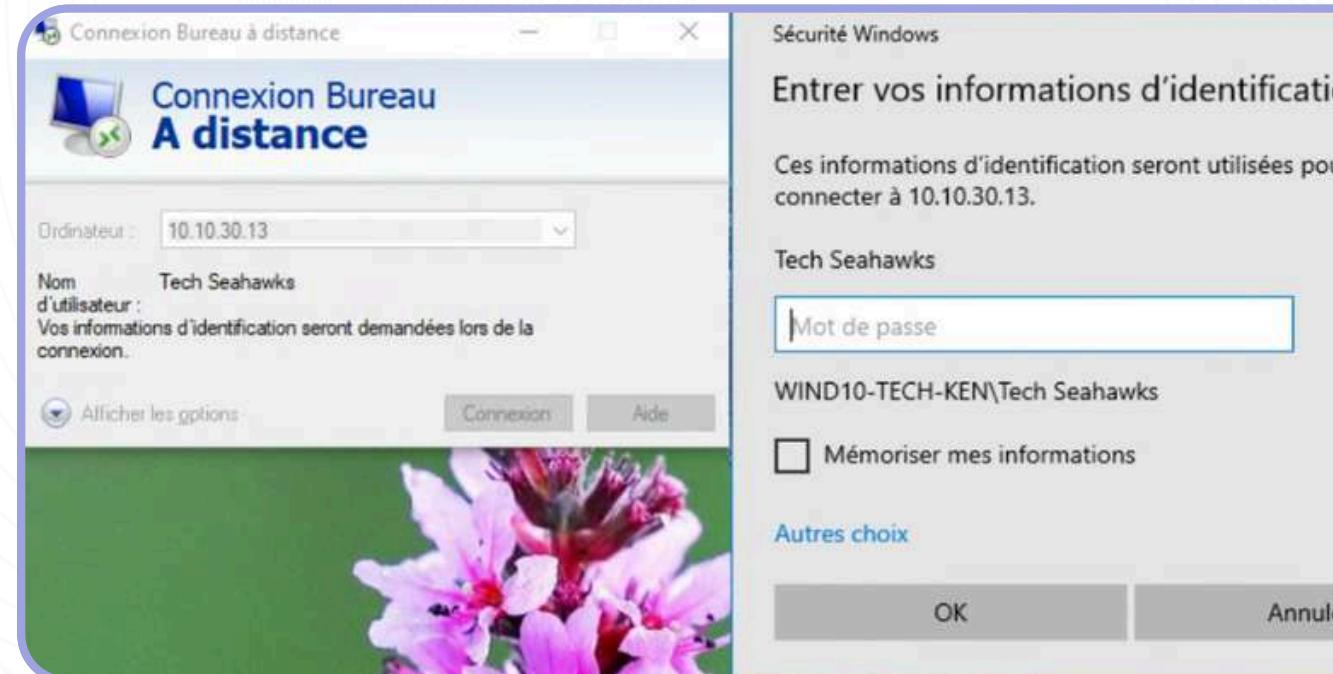
## Rôle dans le projet :

- Centralise la télémaintenance via un point de rebond unique et fournit une interface graphique légère pour l'administration des Harvesters.

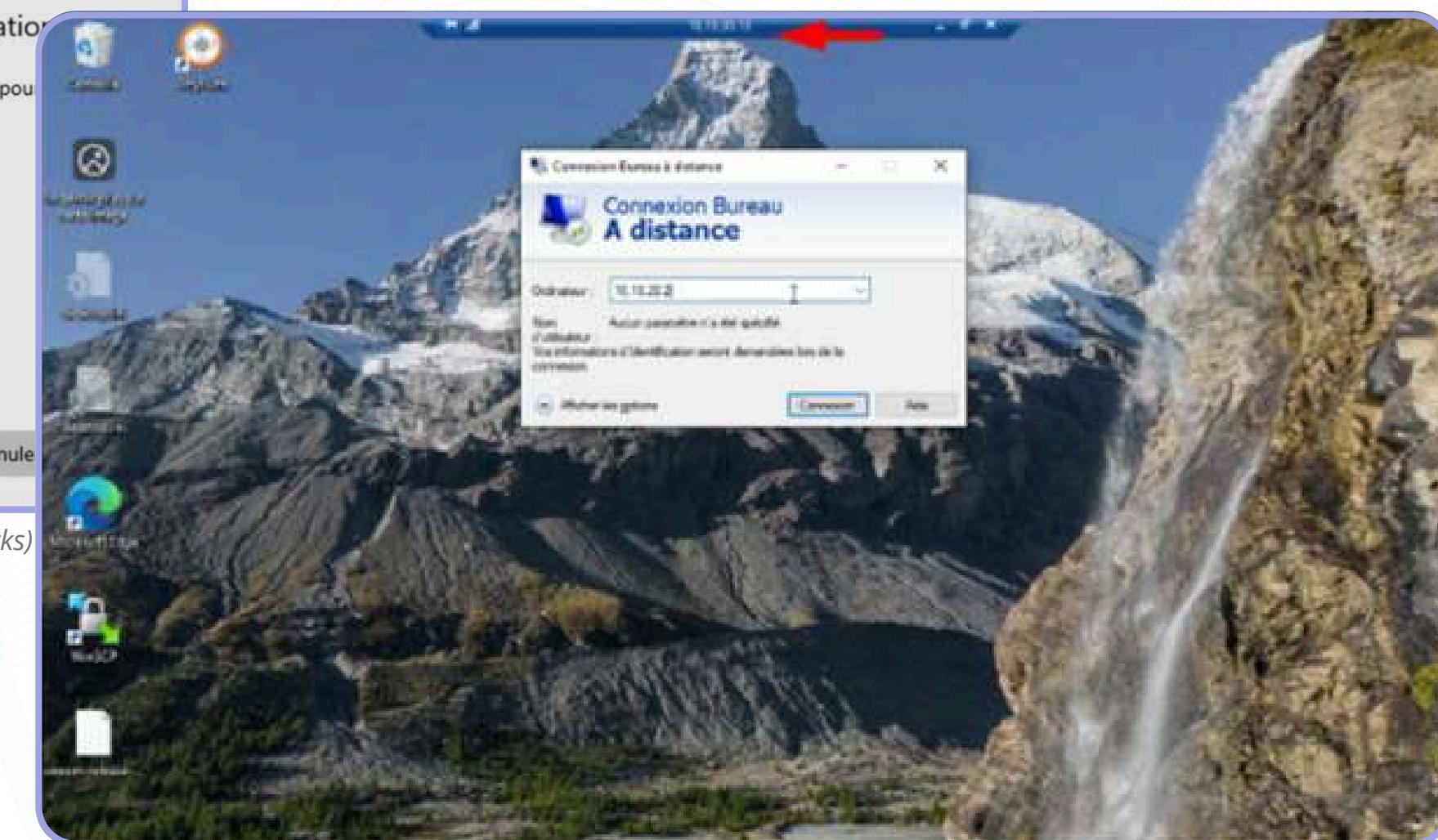
## Particularité technique :

- Accès limité aux IP du siège via VPN, avec compte dédié et logs de connexion pour la traçabilité.

# Annexe - La Télémaintenance

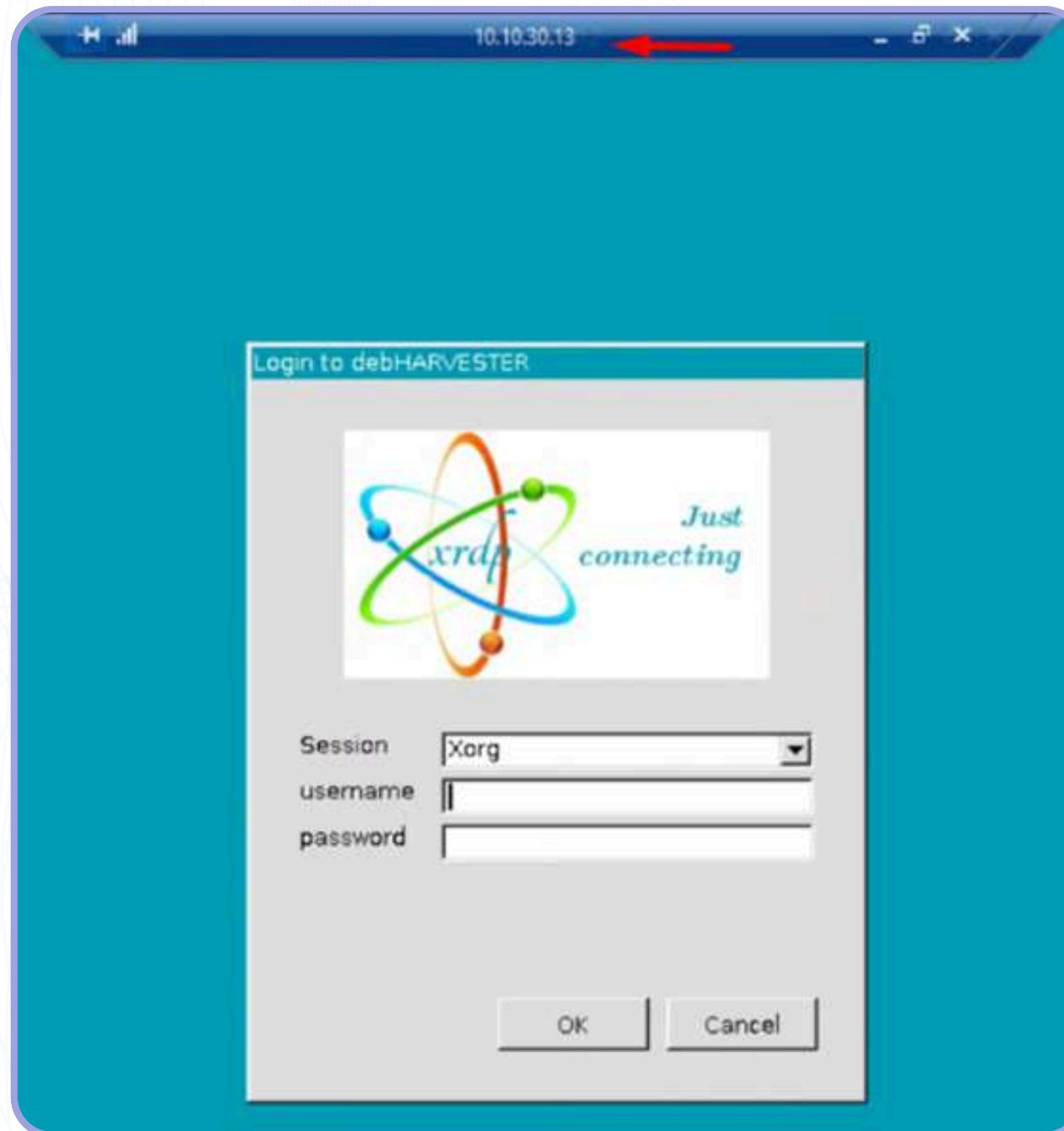


Accès distant sécurisé via le bastion (connexion RDP avec authentification Tech SeaHawks)

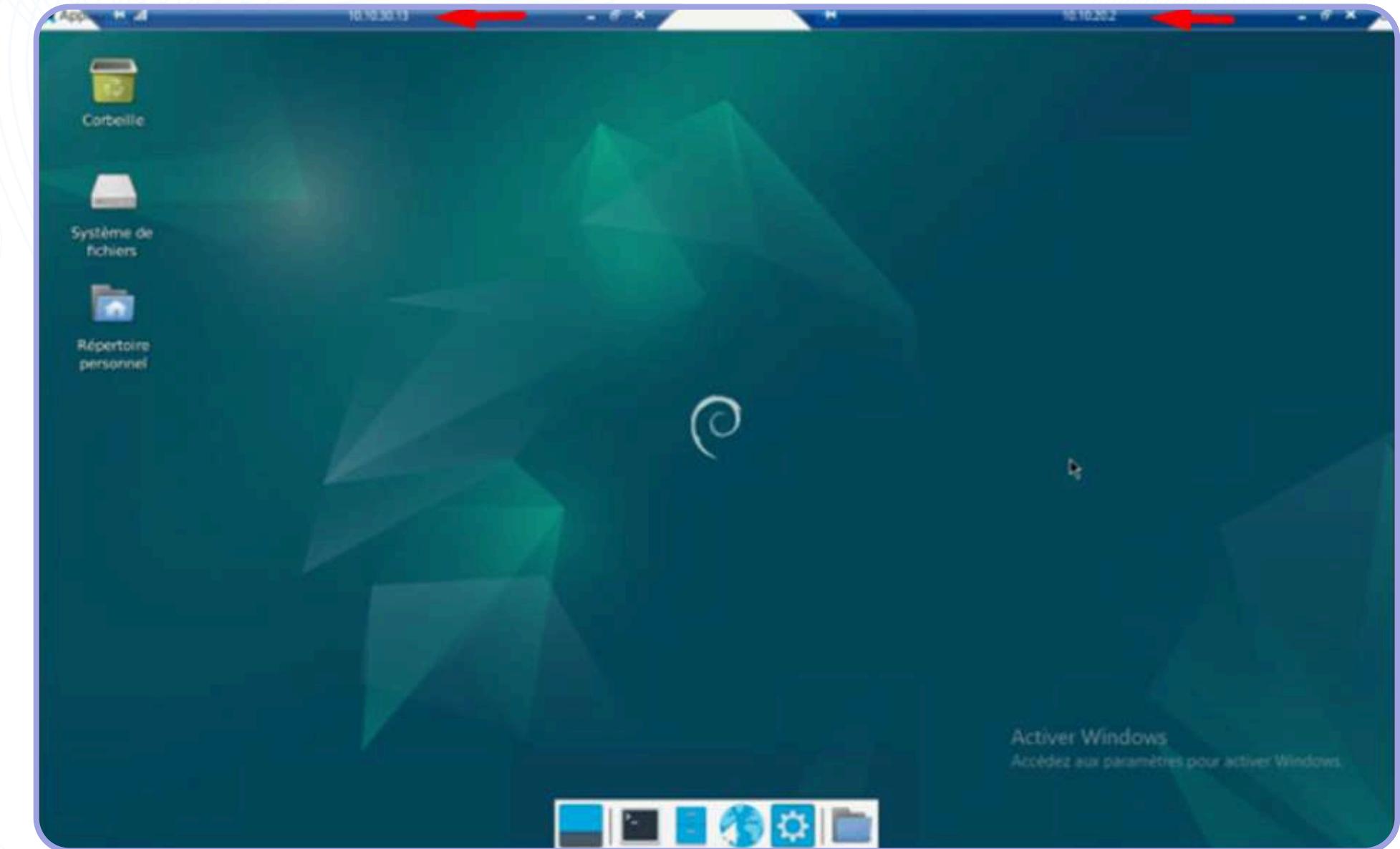


Connexion Bastion – RDP  
Accès distant au bastion Windows, depuis le siège, via protocole RDP (10.10.20.2).

## Annexe - La Télémaintenance



Connexion Harvester – XRDP  
Connexion graphique distante sur un Harvester Debian via XRDP.



Téléaintenance – Rebonds Bastion → Harvester  
Session distante active entre le bastion (10.10.10.13) et un Harvester (10.10.20.2).

# MERCI !

