BTS SIO · OPTION SISR · SESSION 2026

BAGARRY Matthias

DOSSIER TECHNIQUE

Mise en œuvre, sécurisation et exploitation d'un centre de services GLPI et d'un pare-feu OPNsense

0 CONTEXTE ET OBJECTIFS

Ce projet a été mené dans le cadre du PPE pour le client GEFOR (Groupe Européen de Formation), organisme de formation présent sur six sites en France. Le site de Paris 1er accueille plusieurs promotions (SIO, GPME, TC) déjà rattachées au domaine Active Directory gefor.lan déployé lors d'un projet précédent.

L'objectif est double : déployer un outil de gestion de tickets et d'inventaire (GLPI 10) accessible aussi bien depuis le LAN interne que depuis l'extérieur via un port non-standard, et restructurer le réseau autour d'un pare-feu OPNsense en architecture trois pattes (LAN / DMZ / WAN) pour isoler le service exposé.

▸ OBJECTIFS PÉDAGOGIQUES

Maîtriser la segmentation réseau via un pare-feu open source (OPNsense) en architecture DMZ. Déployer une pile LAMP complète (Apache, MariaDB, PHP) et une application métier open source (GLPI). Industrialiser l'authentification par interconnexion LDAP avec un Active Directory existant. Mettre en place les bonnes pratiques de durcissement Linux (SSH, Fail2Ban, UFW, TLS) attendues sur un service exposé en DMZ.

▸ POURQUOI CETTE ARCHITECTURE

GLPI doit être accessible depuis l'extérieur (stagiaires en télétravail) tout en étant intégré à l'annuaire interne. Deux contraintes contradictoires : exposition publique et accès aux comptes du domaine. La réponse classique est la DMZ : le serveur exposé est isolé du LAN par le pare-feu, qui n'autorise qu'un flux LDAP unidirectionnel (DMZ → LAN sur TCP/389). En cas de compromission du serveur web, l'attaquant reste confiné dans la DMZ sans accès direct aux postes ni au contrôleur de domaine.

État de l'art : choix des solutions techniques

Avant de retenir GLPI comme outil de gestion de tickets et d'inventaire, plusieurs solutions open source ont été évaluées.

Outil	Points forts	Limites
GLPI	Ticketing + inventaire natif, intégration LDAP/AD, communauté française active, gratuit	Interface vieillissante
osTicket	Léger, simple à déployer	Pas d'inventaire, LDAP limité
Zammad	Interface moderne, multicanal	Pas d'inventaire, plus complexe
OTRS	Très complet	Version libre abandonnée, courbe d'apprentissage élevée

GLPI s'impose comme le choix le plus cohérent pour GEFOR : c'est la seule solution qui couvre à la fois le ticketing et l'inventaire automatisé dans une version entièrement gratuite, avec une intégration Active Directory native et une large base documentaire en français — un avantage concret pour une équipe de stagiaires.

Pour la couche réseau, deux pare-feux open source ont été comparés :

Outil	Points forts	Limites
OPNsense	Interface moderne, mises à jour fréquentes, WireGuard natif	Moins de documentation que pfSense
pfSense	Très documenté, large communauté	Version CE de plus en plus limitée depuis le rachat par Netgate

OPNsense a été retenu pour sa politique de mises à jour plus transparente et l'intégration native de WireGuard, utile pour l'accès VPN envisagé en perspective.

1 ANALYSE ET ARCHITECTURE

L'infrastructure existante repose sur un hyperviseur Hyper-V hébergeant le contrôleur de domaine Windows Server 2019 (gefor.lan). Tout le projet GLPI/OPNsense est déployé sur ce même hyperviseur sous forme de machines virtuelles. La connectivité Internet transite par la box du fournisseur d'accès.

1.1 Architecture cible (segmentation trois pattes)

Le choix s'est porté sur une architecture Three-Homed Firewall : OPNsense possède trois interfaces réseau virtuelles, chacune connectée à un commutateur virtuel Hyper-V dédié. Cette topologie applique le principe de défense en profondeur : aucun flux ne passe d'une zone à l'autre sans transiter explicitement par le pare-feu.

Interface	Réseau IP	Rôle
WAN	192.168.0.0/24	Liaison vers la box GEFOR et l'Internet public
LAN	192.168.120.0/24	Zone interne sécurisée : AD et postes Windows 10
DMZ	192.168.125.0/24	Zone démilitarisée hébergeant le serveur GLPI
VPN	192.168.135.0/24	Réseau dédié au tunnel d'administration distante

▸ POURQUOI UN /24 PAR ZONE

Chaque zone reçoit son propre sous-réseau pour deux raisons. Premièrement, lisibilité opérationnelle : un administrateur identifie immédiatement la zone d'une machine à son IP (.120 → LAN, .125 → DMZ). Deuxièmement, simplicité des règles de filtrage : une règle peut cibler une zone entière par son sous-réseau plutôt que de lister des IP individuelles. Enfin, le /24 offre 254 hôtes utiles, largement suffisant pour chaque segment et avec de la marge pour la croissance.

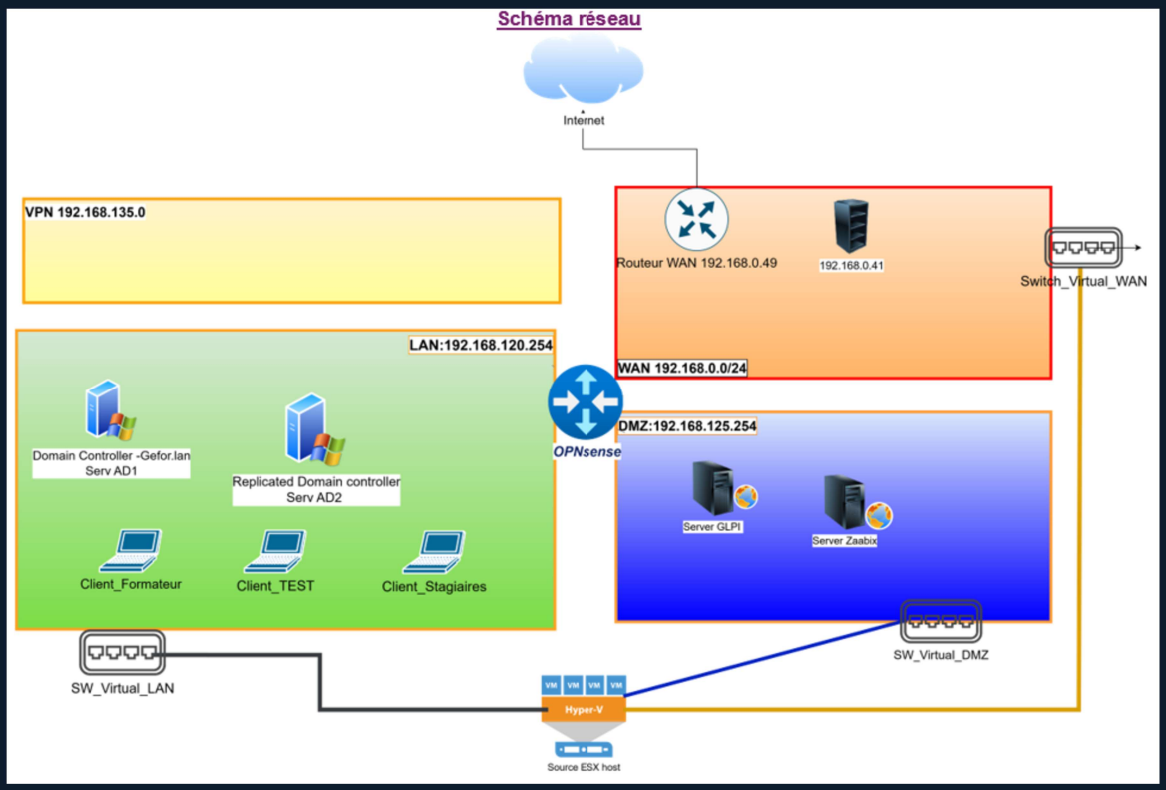

Figure 1 – *Schéma réseau cible — segmentation OPNsense en trois pattes (WAN, LAN, DMZ) avec serveurs GLPI et Zabbix en DMZ et Active Directory en LAN.*

1.2 Ressources allouées aux machines virtuelles

VM	OS	vCPU	RAM	Disque	Rôle
OPNSENSE-FW	OPNsense 24.1	2	2 Go	20 Go	Pare-feu / passerelle
SRV-GLPI	Ubuntu Server 22.04 LTS	2	4 Go	40 Go (LVM)	Pile LAMP + GLPI
SRV-AD	Windows Server 2019	2	4 Go	60 Go	AD DS + DNS (existant)

1.3 Planification (diagramme de Gantt)

Le projet a été planifié sur deux semaines (S49 et S50) avec une décomposition en tâches courtes journalières. Le séquencement respecte les dépendances techniques : création des VM puis installation des OS, puis OPNsense doit être opérationnel avant le déploiement de GLPI (sinon pas de routage WAN/DMZ pour télécharger les paquets).

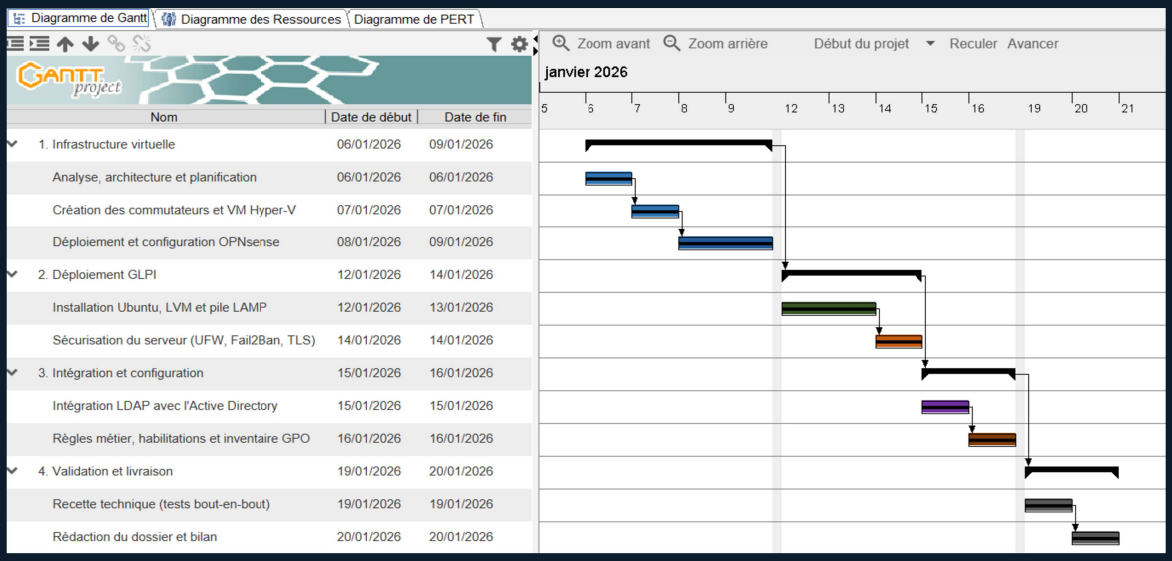

Figure 2 – *Diagramme de Gantt du projet, semaines 2 et 3 (janvier 2026) : infrastructure réseau, déploiement GLPI et intégration AD.*

2 INFRASTRUCTURE VIRTUELLE (HYPER-V)

Toutes les machines virtuelles tournent sur Hyper-V. La création des commutateurs virtuels doit précéder l'installation des VM, car chaque VM est rattachée à un commutateur dès sa création. Trois commutateurs virtuels sont nécessaires : un par zone réseau.

2.1 Création des commutateurs virtuels

La console Hyper-V → Gestionnaire de commutateur virtuel permet de créer trois switches de type différent selon leur rôle. Le switch WAN est configuré en mode externe (lié à la carte physique de l'hyperviseur pour atteindre la box). Les switches LAN et DMZ sont configurés en mode interne : trafic isolé entre VM, sans communication avec l'hôte ni avec l'extérieur — seul OPNsense, qui possède une patte sur chaque switch, fait passer les flux entre zones.

```
# Création des switches virtuels en PowerShell (alternative au GUI)
New-VMSwitch -Name 'SW-WAN' -NetAdapterName 'Ethernet' -AllowManagementOS $true
New-VMSwitch -Name 'SW-LAN' -SwitchType Internal
New-VMSwitch -Name 'SW-DMZ' -SwitchType Internal

# Vérification
Get-VMSwitch | Format-Table Name, SwitchType, NetAdapterInterfaceDescription
```

▸ **DIFFÉRENCE EXTERNE / INTERNE / PRIVÉ**

Externe : la carte virtuelle est bridgée sur une carte physique. Les VM peuvent communiquer avec l'extérieur. Utilisé uniquement pour le WAN. Interne : isolé du physique mais l'hôte Hyper-V possède une carte sur ce switch. Pratique pour administrer les VM depuis l'hôte. Utilisé pour LAN et DMZ ici. Privé : totalement isolé, même l'hôte n'y a pas accès. Utilisé pour des labs très cloisonnés.

2.2 Création des machines virtuelles

Chaque VM est créée en génération 2 (UEFI, démarrage sécurisé désactivable pour les OS Linux), avec rattachement initial au commutateur correspondant à sa zone. L'ISO d'installation est monté sur le contrôleur IDE 1 lors de la première installation.

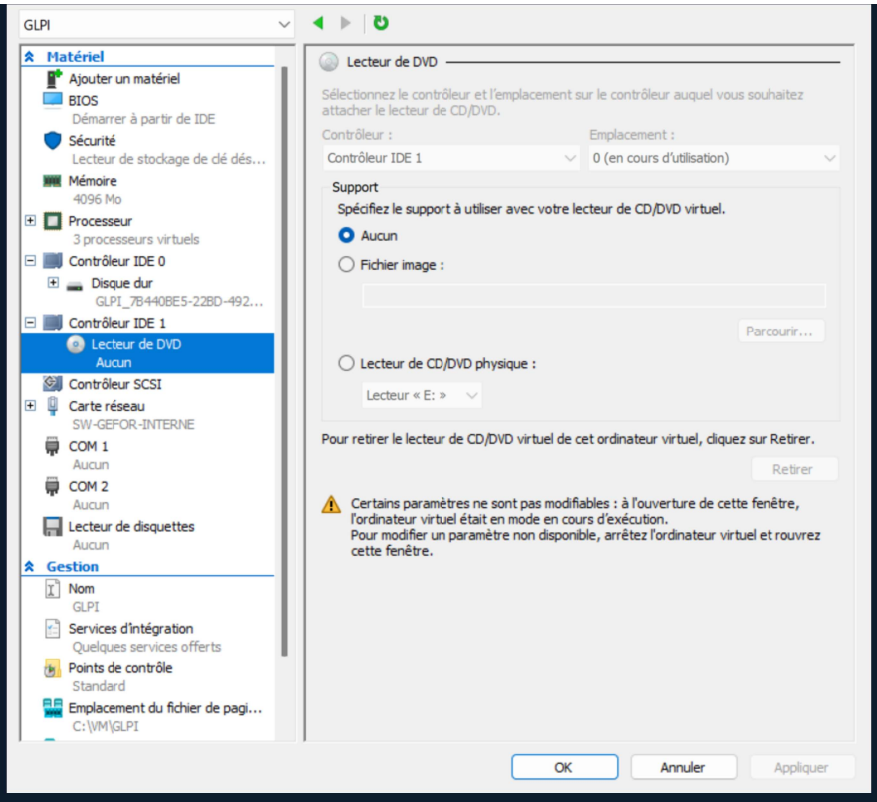

Figure 3 — *Paramètres Hyper-V de la VM SRV-GLPI — retrait de l'ISO d'installation après le premier démarrage pour éviter de relancer l'installateur à chaque boot.*

▸ POURQUOI RETIRER L'ISO APRÈS INSTALLATION

Tant que l'ISO reste monté et que le BIOS de la VM démarre sur le DVD avant le disque dur, chaque redémarrage relance l'installateur au lieu de booter sur le système installé. Le réflexe correct est d'éjecter l'ISO (option « Aucun » dans le lecteur DVD) puis de vérifier dans l'onglet Microprogramme/BIOS que le disque dur est bien en première position dans l'ordre de démarrage.

3 DÉPLOIEMENT DU PARE-FEU OPNSENSE

OPNsense est une distribution dérivée de FreeBSD spécialisée dans le pare-feu et le routage. L'installation se fait depuis l'ISO officiel (opnsense-24.1-dvd-amd64.iso) et démarre sur un live-system avec un assistant texte. Le compte par défaut pendant l'installation est installer / opnsense.

3.1 Configuration des interfaces

Après le premier démarrage, OPNsense présente un menu console permettant d'assigner les interfaces aux zones logiques. Chaque carte virtuelle Hyper-V apparaît sous un nom hn0, hn1, hn2 (driver Hyper-V). L'assignation suit l'ordre de rattachement aux switches.

Interface OPNsense	Carte Hyper-V	Adresse IP	Mode

WAN	SW-WAN	192.168.0.49/24	DHCP (box)
LAN	SW-LAN	192.168.120.254/24	Statique
DMZ (OPT1)	SW-DMZ	192.168.125.254/24	Statique

▸ CONVENTION D'ADRESSAGE DE LA PASSERELLE

L'adresse .254 est attribuée par convention à la passerelle de chaque sous-réseau. Cela laisse la plage .1 à .253 pour les hôtes et fournit une adresse mémorisable pour les configurations DHCP et les routes par défaut. Toutes les VM du LAN auront 192.168.120.254 comme passerelle, toutes celles de la DMZ auront 192.168.125.254.

3.2 Politique de filtrage (Default Deny)

OPNsense applique par défaut une politique « tout interdire » sur le WAN entrant. Sur les interfaces LAN et DMZ, une règle « LAN to any » est créée par défaut pour ne pas casser le fonctionnement initial — il faut la remplacer par des règles explicites. Les règles implémentées suivent le principe du moindre privilège : seuls les flux nécessaires au fonctionnement métier sont autorisés.

Source	Destination	Port / Protocole	Rôle
LAN net	DMZ (SRV-GLPI)	TCP/443 (HTTPS)	Accès helpdesk interne
DMZ (SRV-GLPI)	LAN (SRV-AD)	TCP/389 (LDAP)	Synchronisation utilisateurs
WAN any	DMZ (SRV-GLPI)	TCP/8443 (PAT)	Accès distant stagiaires
LAN net	WAN	TCP/80, 443, 53	Navigation internet postes
DMZ	WAN	TCP/80, 443	Mises à jour APT serveur GLPI

▸ POURQUOI BLOQUER DMZ → LAN PAR DÉFAUT

C'est l'essence même de la DMZ. Si un attaquant compromet le serveur web exposé en DMZ (via une faille PHP, par exemple), il ne doit pas pouvoir rebondir vers le LAN où se trouvent l'AD et les données sensibles. La seule exception autorisée est le flux LDAP vers l'IP fixe du contrôleur de domaine, sur le port 389 uniquement. Tout le reste (SMB, RDP, ICMP) est bloqué. C'est l'inverse du flux LAN → DMZ qui, lui, est large puisque les utilisateurs internes doivent consulter le helpdesk.

3.3 NAT/PAT pour l'accès externe (port non-standard)

Le cahier des charges impose que GLPI soit accessible depuis Internet sur un port non-standard pour limiter le bruit des scans automatisés. Une règle de redirection de port (Port Forward) est créée sur l'interface WAN : tout trafic entrant sur le port 8443 est redirigé vers 192.168.125.207:443 (l'IP du serveur GLPI en DMZ). Cette règle se configure dans Pare-feu → NAT → Redirection de port.

Paramètre	Valeur
Interface	WAN
Protocole	TCP
Port destination externe	8443
IP destination interne	192.168.125.207 (SRV-GLPI)
Port destination interne	443 (HTTPS standard côté serveur)
Filter rule association	Pass (création automatique de la règle de filtrage associée)

▸ POURQUOI DISSIMULER LE PORT

Les scanners automatisés (Shodan, Censys, scripts de bruteforce) ciblent en priorité les ports standard (22, 80, 443, 3389). Exposer GLPI sur 8443 ne supprime pas la possibilité d'être trouvé — un scan exhaustif de tous les ports finit par tomber dessus — mais réduit drastiquement le bruit de fond et donc le risque d'attaque opportuniste. C'est de la sécurité par l'obscurité, qui n'a de valeur qu'en complément des autres couches : Fail2Ban, TLS et authentification LDAP forte.

[SCREENSHOT À INSÉRER]

Interface OPNsense — règle de redirection de port WAN:8443 → DMZ:443.

Commande : `OPNsense → Pare-feu → NAT → Redirection de port`

→ Capturer la liste des règles NAT avec la règle 8443→443 visible, puis cliquer dessus pour afficher le détail (interface WAN, protocole TCP, IP destination 192.168.125.207, port 443) et faire une seconde capture du formulaire.

4 DÉPLOIEMENT DE LA VM SRV-GLPI

La VM hébergeant GLPI tourne sous Ubuntu Server 22.04 LTS. Le choix d'Ubuntu LTS plutôt que Debian s'explique par le support cinq ans (jusqu'en 2027) et la disponibilité native des paquets PHP 8.1 requis par GLPI 10. L'installation se fait sans interface graphique pour limiter la surface d'attaque et la consommation de ressources.

4.1 Partitionnement LVM

Le partitionnement utilise LVM (Logical Volume Manager) pour pouvoir étendre les volumes sans redémarrer en cas de saturation. Les répertoires critiques sont isolés sur des volumes logiques séparés.

Volume logique	Point de montage	Taille	Justification

lv-root	/	10 Go	Système Ubuntu et binaires
lv-www	/var/www	10 Go	Application GLPI et documents joints (uploads)
lv-mysql	/var/lib/mysql	10 Go	Base de données MariaDB
lv-log	/var/log	5 Go	Isolation logs (anti-DoS par saturation)
lv-swap	swap	2 Go	Swap (pour 4 Go RAM)

▸ POURQUOI ISOLER /VAR/LOG ET /VAR/LIB/MYSQL

Si les logs explosent (attaque DDoS, boucle d'erreur), seul le volume /var/log se remplit ; le système et la base GLPI continuent de tourner. Si la base MariaDB grossit anormalement (table de tickets non purgée, fuite mémoire), elle ne peut pas remplir le système. C'est le même principe que l'isolation /var/spool/postfix dans le projet relais SMTP : confiner les pannes à leur volume d'origine.

4.2 Configuration réseau statique

La VM SRV-GLPI reçoit une IP statique en DMZ. Sur Ubuntu 22.04, la configuration réseau passe par Netplan (fichier YAML dans /etc/netplan/). L'IP est fixée à 192.168.125.207 avec la passerelle pointant vers OPNsense (192.168.125.254). Le DNS interrogé est celui du contrôleur de domaine (192.168.120.10) pour pouvoir résoudre srv-ad.gefor.lan lors de la requête LDAP.

```
# /etc/netplan/00-installer-config.yaml
network:
  version: 2
  ethernets:
    eth0:
      dhcp4: false
      addresses: [192.168.125.207/24]
      routes:
        - to: default
          via: 192.168.125.254
      nameservers:
        addresses: [192.168.120.10, 1.1.1.1]
        search: [gefor.lan]

# Application de la configuration
sudo netplan apply
ip -br a              # Vérification de l'IP
ip route              # Vérification de la route par défaut
ping -c 3 192.168.125.254   # Test passerelle OPNsense
```

5 INSTALLATION DE LA PILE LAMP ET DE GLPI

GLPI repose sur le triplet Apache (serveur HTTP), MariaDB (base de données) et PHP (langage applicatif). L'ensemble est désigné par l'acronyme LAMP. L'installation suit l'ordre logique : mise à jour système, installation des paquets, sécurisation MariaDB, création de la base, déploiement des sources GLPI, configuration du Virtual Host Apache.

5.1 Installation des paquets

```
# Mise à jour du système
sudo apt update && sudo apt full-upgrade -y

# Installation Apache, MariaDB, PHP 8.1 et toutes les extensions requises par GLPI
sudo apt install -y apache2 mariadb-server \
    php php-mysql php-curl php-gd php-intl php-ldap \
    php-mbstring php-xml php-zip php-bz2 php-imap \
    php-apcu libapache2-mod-php

# Vérification des versions installées
apache2 -v && mariadb --version && php -v
```

▸ POURQUOI PHP-LDAP EST CRITIQUE

L'extension php-ldap est la brique qui permet à GLPI de dialoguer avec l'Active Directory lors de la synchronisation et de l'authentification des utilisateurs. Sans elle, l'onglet « Annuaires LDAP » de GLPI affichera des erreurs et la connexion d'un utilisateur du domaine échouera silencieusement. L'oubli de ce paquet est l'une des erreurs les plus fréquentes lors d'un déploiement GLPI.

5.2 Sécurisation de MariaDB

MariaDB s'installe avec une configuration permissive (compte root sans mot de passe, base de test accessible). Le script mysql_secure_installation guide l'administrateur pour fixer le mot de passe root, supprimer les utilisateurs anonymes, désactiver l'accès root distant et supprimer la base de test.

```
# Lancement de l'assistant de durcissement
sudo mysql_secure_installation

# Réponses recommandées :
# - Switch to unix_socket authentication ? n
# - Change the root password ? Y → saisir un mot de passe fort
# - Remove anonymous users ? Y
# - Disallow root login remotely ? Y
# - Remove test database ? Y
# - Reload privilege tables now ? Y
```

5.3 Création de la base et de l'utilisateur GLPI

GLPI ne doit jamais utiliser le compte root MariaDB. Un utilisateur dédié est créé avec des droits limités à la seule base de l'application, en respect du principe du moindre privilège.

```
# Connexion en tant que root MariaDB
sudo mariadb -u root -p

-- Création de la base et de l'utilisateur dédiés
CREATE DATABASE glpidb CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
CREATE USER 'glpiuser'@'localhost' IDENTIFIED BY 'MotDePasseFort2026!';
GRANT ALL PRIVILEGES ON glpidb.* TO 'glpiuser'@'localhost';
FLUSH PRIVILEGES;
EXIT;

# Initialisation des fuseaux horaires (requis par GLPI 10)
sudo mysql_tzinfo_to_sql /usr/share/zoneinfo | sudo mariadb mysql
sudo mariadb -e "GRANT SELECT ON mysql.time_zone_name TO 'glpiuser'@'localhost'; FLUSH
PRIVILEGES;"
```

5.4 Téléchargement et déploiement de GLPI 10

```
# Récupération de l'archive officielle GLPI 10.0.21
cd /tmp
wget https://github.com/glpi-project/glpi/releases/download/10.0.21/glpi-10.0.21.tgz

# Extraction dans /var/www/html (DocumentRoot Apache par défaut)
sudo tar -xzf glpi-10.0.21.tgz -C /var/www/html/

# Attribution des droits au compte d'exécution Apache (www-data)
sudo chown -R www-data:www-data /var/www/html/glpi
sudo find /var/www/html/glpi -type d -exec chmod 755 {} \;
sudo find /var/www/html/glpi -type f -exec chmod 644 {} \;
```

▸ POURQUOI WWW-DATA

www-data est le compte système sous lequel tourne le processus Apache sur Debian/Ubuntu. Tous les fichiers de l'application doivent appartenir à ce compte pour qu'Apache puisse les lire (et écrire dans les répertoires de cache et d'upload). Donner les droits à root casserait l'application. À l'inverse, donner chmod 777 partout ouvrirait une faille : tout processus pourrait modifier les fichiers PHP et injecter du code.

5.5 Configuration du Virtual Host Apache

Plutôt que de servir GLPI depuis le DocumentRoot par défaut, un Virtual Host dédié est configuré. Cela permet d'avoir une URL propre (myglpi au lieu de /glpi) et de définir des logs séparés pour faciliter le diagnostic.

```
# Création du fichier de configuration
sudo nano /etc/apache2/sites-available/glpi.conf
```

```
<VirtualHost *:80>
    ServerAdmin admin@gefor.lan
    DocumentRoot /var/www/html/glpi
    ServerName myglpi

    <Directory /var/www/html/glpi>
        Options FollowSymlinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/glpi-error.log
    CustomLog ${APACHE_LOG_DIR}/glpi-access.log combined
</VirtualHost>
```

```
# Activation du site et désactivation du site par défaut
sudo a2ensite glpi.conf
sudo a2dissite 000-default.conf

# Activation du module rewrite (requis par GLPI)
sudo a2enmod rewrite

# Vérification de la syntaxe puis redémarrage
sudo apache2ctl configtest
sudo systemctl restart apache2
sudo systemctl status apache2
```

Figure 4 – *Édition du fichier /etc/apache2/sites-available/glpi.conf dans nano — configuration du Virtual Host pointant vers /var/www/html/glpi.*

5.6 Assistant d'installation web

Une fois le Virtual Host actif, l'installation se termine via le navigateur : la première connexion à http://192.168.125.207/glpi/install/install.php déclenche l'assistant de configuration GLPI. Six étapes guidées : choix de la langue, acceptation de la licence, vérification des prérequis, paramètres de connexion à la base de données (glpiuser / glpidb), initialisation des tables, finalisation.

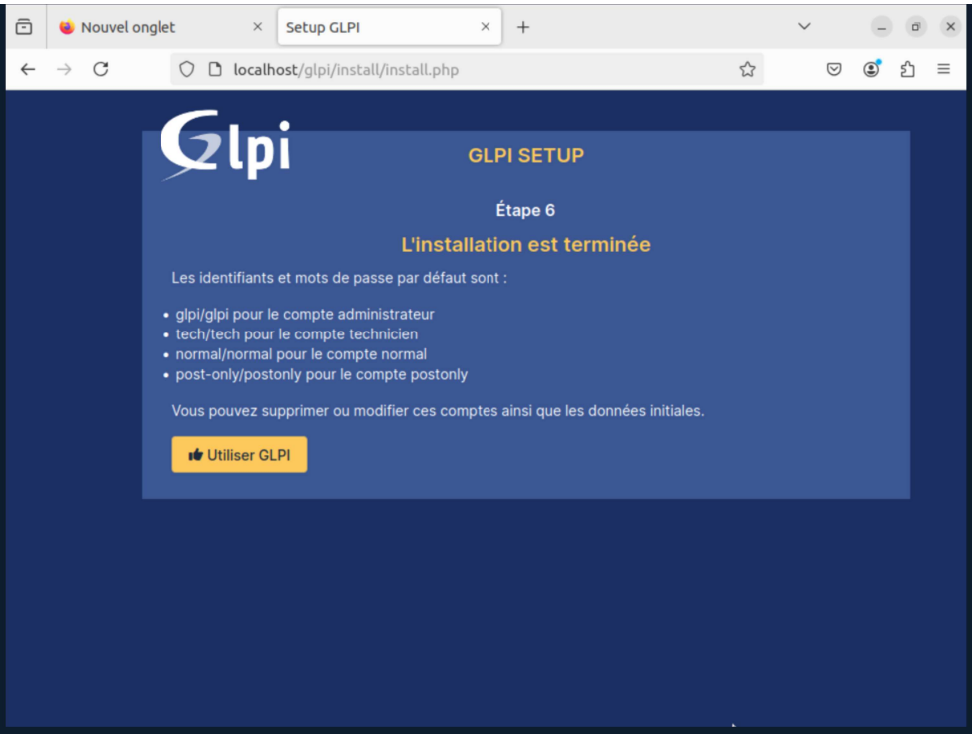

Figure 5 — *Étape 6 de l'assistant GLPI — l'installation est terminée. Affichage des comptes par défaut (glpi/glpi, tech/tech, normal/normal, post-only/postonly).*

▸ ACTION IMMÉDIATE APRÈS INSTALLATION

Les quatre comptes par défaut (glpi, tech, normal, post-only) ont des identifiants triviaux (login = mot de passe). C'est une faille de sécurité critique sur un serveur exposé. La première action est de changer les mots de passe des quatre comptes — voire de désactiver les comptes inutiles (tech, normal, post-only) puisque l'authentification se fera ensuite via LDAP. Il faut aussi supprimer manuellement le fichier /var/www/html/glpi/install/install.php pour empêcher quiconque de relancer l'assistant.

```
# Sécurisation post-installation
sudo rm /var/www/html/glpi/install/install.php

# Vérification que GLPI ne génère plus l'avertissement de sécurité
curl -s http://localhost/glpi/ | grep -i 'install.php' || echo 'OK : install.php
supprimé'
```

6 SÉCURISATION ET DURCISSEMENT

Le serveur SRV-GLPI étant exposé en DMZ et accessible depuis Internet via le PAT 8443, plusieurs couches de durcissement sont appliquées. La défense en profondeur impose de ne pas se reposer sur une seule mesure : pare-feu local en plus du pare-feu OPNsense, Fail2Ban en plus de la complexité des mots de passe, TLS en plus du port non-standard.

6.1 Pare-feu local UFW

Même protégé par OPNsense en amont, le serveur active son propre pare-feu local UFW (Uncomplicated Firewall, frontal de iptables). C'est le principe de défense en profondeur : si une règle OPNsense est mal configurée ou contournée, UFW bloque encore. Politique par défaut : tout interdire en entrée, tout autoriser en sortie.

```
# Politique par défaut
sudo ufw default deny incoming
sudo ufw default allow outgoing

# Ouverture des ports nécessaires
sudo ufw allow 22/tcp    # SSH (administration)
sudo ufw allow 80/tcp    # HTTP (avant migration HTTPS)
sudo ufw allow 443/tcp   # HTTPS (production)

# Activation
sudo ufw enable
sudo ufw status verbose
```

[SCREENSHOT À INSÉRER]

Sortie de ufw status verbose montrant la stratégie Default Deny et les règles actives.

Commande : `sudo ufw status verbose`

→ Capturer la sortie complète avec Status: active, Default: deny (incoming), allow (outgoing), et les règles 22/tcp, 80/tcp, 443/tcp visibles. Cette capture prouve que seuls les ports nécessaires sont ouverts au niveau du serveur.

6.2 Protection SSH par Fail2Ban

Fail2Ban analyse en continu les journaux système et bannit automatiquement les IP qui génèrent trop de tentatives d'authentification échouées. Sur un serveur exposé, c'est la défense la plus efficace contre les attaques par force brute SSH, qui représentent la majorité du bruit de fond Internet.

```
# Installation
sudo apt install fail2ban -y

# Création d'un override (jamais éditer /etc/fail2ban/jail.conf directement)
sudo nano /etc/fail2ban/jail.local
```

```
[DEFAULT]
bantime = 1h          # Durée de bannissement après détection
findtime = 10m        # Fenêtre d'observation
maxretry = 3          # Nombre de tentatives autorisées avant ban

[sshd]
enabled = true
port = 22
filter = sshd
logpath = /var/log/auth.log
backend = systemd
```

```
# Démarrage du service
sudo systemctl enable --now fail2ban

# Vérification de l'état de la jail SSH
sudo fail2ban-client status sshd

# Sortie attendue :
# Status for the jail: sshd
# |- Filter
# |  |- Currently failed: 0
# |  |- Total failed:     12
# |  `- File list:        /var/log/auth.log
# `- Actions
#    |- Currently banned: 1
#    |- Total banned:     3
#    `- Banned IP list:   45.227.255.X
```

▸ **POURQUOI BANTIME 1H ET PAS PERMANENT**

Un bannissement permanent semble plus sûr mais finit par remplir la table iptables avec des dizaines de milliers d'IP, ce qui dégrade les performances. Une heure suffit à décourager les attaques automatisées qui cherchent du résultat rapide ; les attaquants ciblés réessaieront depuis d'autres IP de toute façon. Le combo 3 tentatives / 10 minutes / 1 heure de ban est un compromis éprouvé qui limite les faux positifs (admin qui se trompe deux fois) sans laisser passer le bruteforce.

6.3 Chiffrement TLS (HTTPS)

Sans TLS, les identifiants des utilisateurs (et le mot de passe technique du compte de service LDAP) circulent en clair dans le réseau et sont lisibles par toute machine sur le chemin. Un certificat auto-signé est généré pour le lab — en production il serait remplacé par un certificat Let's Encrypt ou un certificat de la PKI interne.

```
# Génération d'un certificat auto-signé (clé RSA 2048 bits, validité 365 jours)
sudo openssl req -new -x509 -nodes -days 365 -newkey rsa:2048 \
    -keyout /etc/ssl/private/glpi.key \
    -out    /etc/ssl/certs/glpi.crt

# Activation du module SSL d'Apache
sudo a2enmod ssl

# Création du Virtual Host HTTPS
sudo nano /etc/apache2/sites-available/glpi-ssl.conf
```

```
<VirtualHost *:443>
    ServerAdmin admin@gefor.lan
    DocumentRoot /var/www/html/glpi
    ServerName myglpi

    SSLEngine on
    SSLCertificateFile    /etc/ssl/certs/glpi.crt
    SSLCertificateKeyFile /etc/ssl/private/glpi.key

    <Directory /var/www/html/glpi>
        Options FollowSymlinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/glpi-ssl-error.log
    CustomLog ${APACHE_LOG_DIR}/glpi-ssl-access.log combined
</VirtualHost>
```

```
# Activation du site SSL et redémarrage
sudo a2ensite glpi-ssl.conf
sudo systemctl reload apache2

# Test du chiffrement depuis le serveur lui-même
openssl s_client -connect localhost:443 -showcerts < /dev/null 2>&1 | head -20
```

7 INTÉGRATION LDAP AVEC L'ACTIVE DIRECTORY

GLPI s'interconnecte avec le contrôleur de domaine gefor.lan pour récupérer automatiquement les comptes utilisateurs. Cela évite la création manuelle des comptes (plusieurs dizaines de stagiaires) et centralise l'authentification : un mot de passe unique géré dans l'AD pour toutes les applications.

7.1 Création d'un compte de service LDAP côté AD

Un compte dédié glpi-ldap est créé dans l'Active Directory. Il sert uniquement à GLPI pour effectuer les requêtes de lecture sur l'annuaire. Ce compte n'a aucun privilège administratif — uniquement le droit de lecture, qui est accordé par défaut à tout compte authentifié dans un domaine AD. Le mot de passe est complexe et n'expire pas (sinon GLPI perdrait l'accès à l'annuaire à chaque renouvellement).

```
# Sur le DC (PowerShell admin)
New-ADUser -Name 'glpi-ldap' -SamAccountName 'glpi-ldap' \
    -UserPrincipalName 'glpi-ldap@gefor.lan' \
    -AccountPassword (ConvertTo-SecureString 'MotDePasseFort2026!' -AsPlainText -Force)
\
    -PasswordNeverExpires $true \
    -Enabled $true \
    -Path 'CN=Users,DC=gefor,DC=lan'
```

7.2 Configuration du connecteur LDAP dans GLPI

Configuration → Authentification → Annuaires LDAP → Ajouter. Les paramètres suivants ciblent le contrôleur de domaine et restreignent la requête aux objets utilisateur (filtre objectClass=user) en excluant les objets désactivés ou techniques.

Paramètre	Valeur
Nom	AD GEFOR
Serveur par défaut	Oui
Actif	Oui
Serveur	192.168.120.10
Port	389
BaseDN	DC=gefor,DC=lan
DN du compte (rootdn)	CN=glpi-ldap,CN=Users,DC=gefor,DC=lan
Mot de passe (rootdn)	MotDePasseFort2026!
Champ de l'identifiant	samaccountname
Filtre de connexion	(&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

▸ DÉCRYPTAGE DU FILTRE LDAP

(objectClass=user) cible la classe user de l'AD. (objectCategory=person) exclut les comptes machine (les ordinateurs sont aussi de classe user dans l'AD). (!(userAccountControl:1.2.840.113556.1.4.803:=2)) est l'expression magique qui exclut les comptes désactivés : 0x2 est le flag ACCOUNTDISABLE de l'attribut userAccountControl, et l'opérateur :1.2.840.113556.1.4.803: est le bitwise-AND LDAP. Au total : on récupère uniquement les comptes utilisateurs réels et activés.

7.3 Synchronisation initiale et import en masse

Une fois le connecteur configuré, Administration → Utilisateurs → Liaison annuaire LDAP → Importation en masse permet de récupérer tous les comptes correspondant au filtre. GLPI les importe avec leurs attributs (nom, prénom, email, groupes d'appartenance).

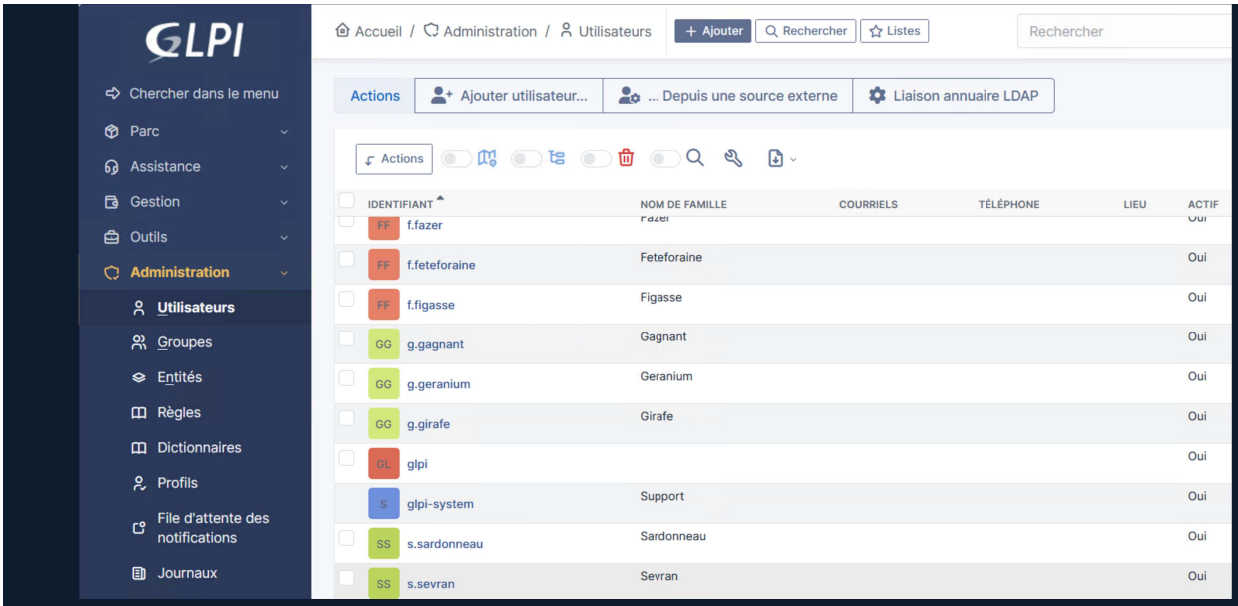

Figure 6 — *Liste des utilisateurs importés depuis l'AD GEFOR — visible dans Administration → Utilisateurs. Les comptes f.fazer, g.gagnant, s.sevran et autres viennent de la synchronisation LDAP.*

8 RÈGLES MÉTIER : HABILITATIONS ET AFFECTATIONS

Importer les utilisateurs ne suffit pas. GLPI doit savoir quel rôle attribuer à chaque personne en fonction de son groupe AD. Le moteur de règles de GLPI permet d'automatiser cette attribution : à chaque connexion, le profil de l'utilisateur est recalculé selon ses groupes d'appartenance LDAP.

8.1 Cartographie rôle métier ↔ profil GLPI

Population	Groupe AD	Profil GLPI	Permissions
Stagiaires SIO	GG_SIO	Technician	Prendre en charge et résoudre les tickets
Formateurs	GG_Formateurs	Supervisor	Voir tous les tickets, KPI, statistiques
Stagiaires GPME/TC	GG_GPME, GG_TC	Self-Service	Créer et suivre leurs propres tickets
Comptes LDAP non groupés	(défaut)	Self-Service (Root entity)	Accès minimal

▸ **POURQUOI LES SIO SONT TECHNICIENS**

Les stagiaires SIO (Services Informatiques aux Organisations) sont en formation informatique. Le PPE prévoit qu'ils traitent les tickets remontés par les autres promotions (GPME en gestion, TC en commerce). C'est pédagogiquement cohérent : ils découvrent le métier de support tout en rendant un service réel à GEFOR. Les formateurs ont le rôle Supervisor pour pouvoir piloter l'activité, voir les indicateurs (temps de résolution, satisfaction) sans pouvoir intervenir directement.

8.2 Création des règles d'affectation d'habilitations

Administration → Règles → Règles d'affectation d'habilitations à un utilisateur. Chaque règle se compose d'un critère (le groupe AD memberOf) et d'une action (assigner tel profil et telle entité). L'ordre des règles est important : GLPI applique la première règle qui correspond, sauf si plusieurs sont marquées « toujours ».

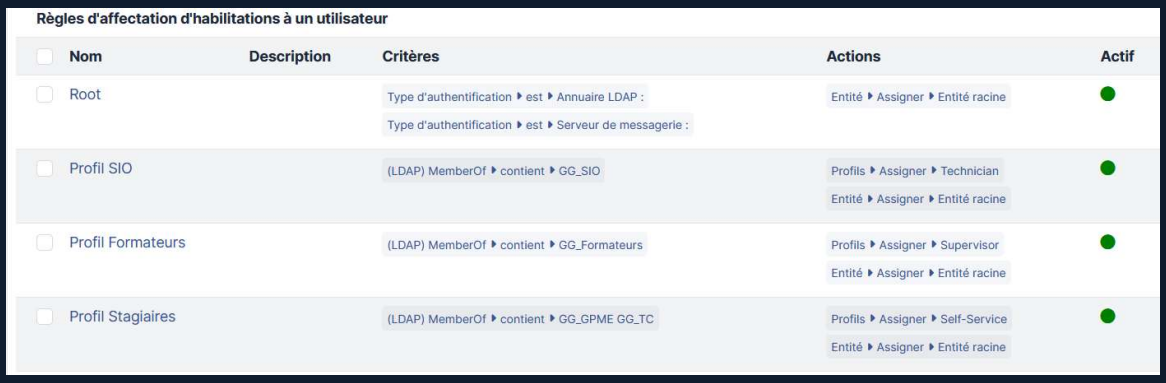

Figure 7 – *Règles d'affectation d'habilitations — Profil SIO assigné comme Technician, Profil Formateurs comme Supervisor, Profil Stagiaires (GPME, TC) comme Self-Service. Toutes les règles sont actives (point vert).*

8.3 Règle d'affectation automatique des tickets

En complément de l'habilitation, une règle d'affectation des tickets entrants est créée. Tout nouveau ticket créé dans la catégorie « Support utilisateur » est automatiquement assigné au groupe technique GG_SIO. Configuration → Règles → Règles métier pour les tickets → Ajouter.

Élément	Valeur
Nom de la règle	Affectation auto support → SIO
Condition d'évaluation	À l'ajout
Critère	Catégorie ITIL est « Support utilisateur »
Action 1	Affecter au groupe technique : GG_SIO
Action 2	Statut : Nouveau (laissé tel quel)
Action 3	Notification email au groupe (oui)

8.4 Extension des habilitations aux stagiaires Titre Professionnel TSSR

En complément des stagiaires SIO, les stagiaires du Titre Professionnel Technicien Supérieur Systèmes et Réseaux (TS&R) sont également habilités au profil Technician. Un groupe GG_TSR est créé dans l'Active Directory sur le même modèle que GG_SIO, et une règle d'habilitation identique est configurée dans GLPI : tout utilisateur membre de GG_TSR se voit attribuer le profil Technician sur l'entité Paris 1er.

La règle d'affectation automatique des tickets définie en 8.3 cible les deux groupes techniques : GG_SIO et GG_TSR sont tous deux définis comme destinataires. Ainsi, un ticket entrant dans la catégorie "Support utilisateur" est automatiquement assigné aux deux groupes, et le premier technicien disponible — SIO ou TSSR — peut le prendre en charge.

8.5 Configuration des entités et des lieux plus statuts

GLPI structure ses objets (tickets, équipements, utilisateurs) selon une arborescence d'entités. Pour être conforme à l'organisation de GEFOR, une entité racine GEFOR a été créée, sous laquelle sont rattachés les différents sites : Paris 1er, Misy-sur-Yonne, Lille, Strasbourg, Marseille et Nantes. Le site Paris 1er, qui accueille les promotions BTS et Bac Pro, constitue l'entité principale du périmètre de ce projet.

À l'intérieur de chaque entité, des lieux ont été définis pour permettre de localiser précisément les équipements de l'inventaire et d'orienter les tickets selon leur origine géographique. Les promotions (SIO, GPME, TC) ont été rattachées à leur entité respective, ce qui permet aux règles d'habilitation de s'appliquer correctement selon le périmètre de chaque utilisateur.

Cette organisation garantit qu'un formateur ne voit que les tickets et équipements de son entité, et qu'un technicien SIO intervient dans le périmètre qui lui est assigné.

9 AUTOMATISATION DE L'INVENTAIRE

Le second usage de GLPI est l'inventaire matériel et logiciel. Plutôt que de saisir manuellement chaque poste, l'agent GLPI est déployé sur tous les clients Windows 10 et remonte quotidiennement les informations. L'agent est un service Windows léger qui interroge WMI puis envoie les données au serveur GLPI via HTTPS.

9.1 Préparation côté serveur GLPI

Le module d'inventaire natif de GLPI 10 doit être activé : Administration → Inventaire → « Activer l'inventaire » coché. Il génère une URL de réception au format https://srv-glpi/glpi/front/inventory.php que les agents utilisent pour pousser leurs données. Aucun composant tiers (FusionInventory) n'est nécessaire avec GLPI 10.

9.2 Déploiement de l'agent par GPO

Le déploiement manuel sur chaque poste serait fastidieux. La méthode professionnelle passe par une GPO Active Directory qui pousse l'installation MSI au démarrage des machines. L'installation est silencieuse (paramètre /quiet) et préconfigure l'URL du serveur GLPI directement dans la commande.

```
REM Commande MSI exécutée par la GPO au démarrage des postes

msiexec /i \\srv-ad\Deploiement$\GLPI-Agent-1.7.3-x64.msi /quiet \
    ADD_FIREWALL_EXCEPTION=1 \
    EXECMODE=Service \
    SERVER=https://srv-glpi.gefor.lan/glpi/front/inventory.php


REM Vérification que le service tourne (sur un poste cible)
sc query GLPI-Agent
```

▸ POURQUOI EN GPO ET NON EN SCRIPT DE LOGON

Une GPO d'installation logicielle s'exécute dans le contexte SYSTEM avec les privilèges nécessaires pour installer un MSI, contrairement à un script de logon qui tourne avec les droits limités de l'utilisateur connecté. La GPO est aussi idempotente : si le MSI est déjà installé à la version cible, elle n'agit pas. Pour les mises à jour ultérieures, il suffit de remplacer le MSI dans le partage de déploiement et d'incrémenter la version.

9.3 Vérification de la remontée

Quelques minutes après le déploiement, les postes apparaissent dans Parc → Ordinateurs. Chaque fiche contient la configuration matérielle (CPU, RAM, disques, cartes réseau) et l'inventaire logiciel (programmes installés avec versions). La fréquence de remontée par défaut est de 24 heures, paramétrable via PROLOG_FREQ.

[SCREENSHOT À INSÉRER]

Interface GLPI — Parc → Ordinateurs montrant la liste des postes Windows 10 remontés par les agents.

Commande : `GLPI → Parc → Ordinateurs`

→ Capturer la liste des ordinateurs avec au moins 3 postes Windows 10 visibles, leurs noms NetBIOS, leur dernière date de mise à jour (preuve que l'agent tourne) et leur OS détecté.

10 VALIDATION TECHNIQUE (RECETTE)

La phase de recette valide la conformité aux quatre axes du cahier des charges : accès externe sécurisé, synchronisation LDAP, inventaire automatique, segmentation réseau effective. Chaque test est documenté avec sa procédure et son critère d'acceptation.

ID	Fonctionnalité testée	Procédure	Résultat attendu	Statut
T01	Accès externe (PAT 8443)	curl -k https://IP_PUBLIQUE:8443/glpi/ depuis WAN	Page de login GLPI servie en HTTP 200	Validé
T02	Synchronisation LDAP	Importation en masse depuis Annuaires LDAP	Comptes SIO, GPME, formateurs importés	Validé
T03	Inventaire dynamique	Vérifier Parc → Ordinateurs après GPO	Postes Windows 10 visibles avec config matérielle	Validé
T04	Pare-feu DMZ → LAN bloqué	ping 192.168.120.10 depuis SRV-GLPI	100% packet loss (ICMP bloqué)	Validé
T05	Pare-feu LAN → DMZ HTTPS OK	curl -k https://192.168.125.207 depuis LAN	Page GLPI servie	Validé
T06	Fail2Ban actif	fail2ban-client status sshd	Jail sshd active, IP bannies après 3 essais	Validé

10.1 Procédures détaillées de test

Test T01 — Accès externe via le PAT 8443 :

```
# Depuis une machine en WAN (192.168.0.0/24)
curl -k -I https://192.168.0.49:8443/glpi/

# Sortie attendue :
# HTTP/1.1 200 OK
# Server: Apache/2.4.52 (Ubuntu)
# Set-Cookie: glpi_xxx=...

# Test depuis le navigateur : https://192.168.0.49:8443/glpi/
# → Page de login GLPI affichée (avertissement de certificat auto-signé : normal)
```

Test T04 — Vérification du blocage DMZ → LAN :

```
# Depuis SRV-GLPI (DMZ : 192.168.125.201)
ping -c 4 192.168.120.10        # Vers le DC en LAN

# Sortie attendue :
# PING 192.168.120.10 (192.168.120.10) 56(84) bytes of data.
# --- 192.168.120.10 ping statistics ---
# 4 packets transmitted, 0 received, 100% packet loss

# Mais le LDAP doit passer (règle explicite) :
telnet 192.168.120.10 389
# Connected to 192.168.120.10. → OK
```

▸ INTERPRÉTATION DU TEST T04

Le résultat « 100% packet loss » sur l'ICMP combiné au « Connected » sur le port 389 valide précisément la politique de filtrage : la DMZ ne peut joindre le LAN que sur le port LDAP, rien d'autre. C'est exactement le comportement attendu d'une DMZ. Si le ping passait, cela signifierait que la règle « DMZ to any » a été laissée par défaut, ce qui constituerait une faille majeure.

10.2 Commandes de diagnostic et exploitation

Commande	Usage
sudo tail -f /var/log/apache2/glpi-access.log	Suivi en temps réel des accès web
sudo tail -f /var/log/apache2/glpi-error.log	Diagnostic des erreurs PHP/Apache
sudo fail2ban-client status sshd	État des bannissements en cours
sudo ufw status numbered	Liste des règles UFW avec numéros pour suppression
sudo systemctl status apache2 mariadb fail2ban	État groupé des trois services critiques
mysql -u glpiuser -p glpidb -e 'SHOW TABLES;'	Vérification des tables GLPI

11 INCIDENTS RENCONTRÉS ET RÉSOLUTIONS

11.1 Boot loop sur l'ISO d'installation

Symptôme : après l'installation d'Ubuntu, la VM relance systématiquement l'installateur au démarrage au lieu de booter sur le système. Diagnostic : l'ISO est restée montée et le BIOS de la VM démarre en priorité sur le DVD. Résolution : Paramètres VM → Contrôleur IDE 1 → Lecteur DVD → cocher « Aucun », puis vérifier dans l'onglet Microprogramme que le disque dur est en première position dans l'ordre de démarrage.

11.2 Échec apt update (résolution DNS)

Symptôme : sudo apt update retourne « Temporary failure resolving fr.archive.ubuntu.com ». Diagnostic : la VM SRV-GLPI était initialement rattachée à un switch interne sans accès Internet, et OPNsense n'était pas encore opérationnel pour router. Résolution temporaire : changement du switch virtuel pour Default Switch (NAT Hyper-V) le temps des installations APT. Résolution définitive après mise en production OPNsense : remise sur SW-DMZ avec OPNsense en passerelle.

11.3 GLPI ne synchronise pas l'AD (binding LDAP)

Symptôme : Annuaires LDAP → Tester → « Erreur de connexion au serveur LDAP ». Diagnostic en deux temps : (1) tcpdump sur SRV-GLPI montre que les paquets partent vers 192.168.120.10:389 mais ne reçoivent aucune réponse → la requête est bloquée. (2) Vérification dans OPNsense : la règle DMZ → LAN sur TCP/389 n'avait pas été créée. Résolution : ajout de la règle explicite Pare-feu → Règles → DMZ → « DMZ net to LAN net (SRV-AD) on TCP/389 → Pass ».

> ▸ LEÇON OPÉRATIONNELLE
>
> Cet incident illustre l'importance de tester les flux dans les deux sens lors d'une mise en production. La règle DMZ → LAN avait été oubliée car nous avions raisonné « qui consomme GLPI ? » (sens LAN → DMZ) sans penser « de quoi GLPI a-t-il besoin ? » (sens DMZ → LAN). La méthode systématique consiste à dresser une matrice de flux (source × destination × port) avant de configurer les règles, et de cocher chaque case lors des tests.

11.4 Confusion shell Linux ⇔ shell MariaDB

Symptôme : copier-coller de commandes SQL dans le terminal Linux génère des erreurs « command not found ». Diagnostic : les commandes SQL doivent être saisies dans le shell MariaDB (prompt mariadb> ou mysql>), pas dans le shell système (prompt $). Résolution : vigilance sur le prompt actif et systématisation de l'usage de mariadb -u glpiuser -p glpidb -e "..." pour exécuter du SQL en une ligne depuis le shell système.

12 BILAN ET PERSPECTIVES

Le projet a permis de déployer une infrastructure de ticketing fonctionnelle et conforme au cahier des charges sur les quatre axes : accès externe sécurisé via PAT 8443, intégration LDAP avec l'AD existant, inventaire automatisé par GPO, et segmentation réseau via OPNsense en architecture trois pattes.

Les compétences SISR mobilisées couvrent les blocs B1 (administration des postes et serveurs), B2 (réseau d'entreprise) et B3 (sécurité). La défense en profondeur est concrètement appliquée à plusieurs niveaux : pare-feu périmétrique OPNsense + pare-feu local UFW, port non-standard 8443 + Fail2Ban + TLS, isolation DMZ + restrictions explicites des flux DMZ → LAN.

12.1 Pistes d’amélioration

Axe	Amélioration envisagée	Bénéfice
TLS	Remplacer le certificat auto-signé par Let’s Encrypt	Suppression des avertissements navigateur
Supervision	Déploiement de Zabbix sur SRV-ZABBIX (DMZ)	Détection proactive des pannes
Sauvegardes	Backup quotidien de glpidb + dossier /var/www/html/glpi	RPO 24h en cas de sinistre
Authentification	Activation de l’authentification à double facteur GLPI	Renforcement vs vol de mot de passe
VPN	Configuration WireGuard sur OPNsense	Accès admin distant sans exposer SSH
Logs	Centralisation syslog vers un serveur dédié	Conservation des traces post-incident

12.2 Bibliographie

Documentation officielle GLPI : https://glpi-project.org/documentation/. Documentation OPNsense (chapitres NAT et Firewall) : https://docs.opnsense.org/. Documentation Fail2Ban : https://github.com/fail2ban/fail2ban/wiki. Microsoft Learn — Hyper-V Virtual Switch : https://learn.microsoft.com/. RFC 4511 (LDAP) et RFC 5246 (TLS 1.2).