ÉDITION PUBLIQUE - DONNÉES INTERNES MASQUÉES

DOSSIER PROFESSIONNEL TSSR · HOMELAB

Brique GLPI

Gestion de parc et d'assistance intégrée à l'Active Directory

A Installation et paramétrage du serveur GLPI

B Authentification centralisée et gestion des habilitations

C Déploiement de l'agent d'inventaire par stratégie de groupe

Serveur	— VM 108 —
Socle	Debian 13 « Trixie » · Apache 2.4.68 · PHP 8.4-FPM · MariaDB 11.8
Applicatif	GLPI 11.0.8 · GLPI Agent 1.19 (Windows x64)
Interconnexions	(LDAP, DNS, GPO) · (partage de déploiement) · (sauvegarde)
Réalisation	9 et 10 septembre 2026
Auteur	Julien BARBET — Titre professionnel TSSR, CIPECMA Saintes, promotion 2026

Rapport technique — environnement de laboratoire virtualisé sous Proxmox VE 9.2.2

Sommaire

1. Contexte et objectifs 3

2. Architecture et choix techniques 5

Partie A — Installation et paramétrage 7

A.1 Création de la machine virtuelle 7
A.2 Installation de Debian 13 minimale 9
A.3 Réseau, résolution DNS et sauvegarde 11
A.4 Socle Apache, PHP-FPM et MariaDB 13
A.5 Base de données GLPI 15
A.6 Déploiement de GLPI 11 et hôte virtuel Apache 16
A.7 Assistant d'installation 17
A.8 Sécurisation post-installation 20
A.9 Tâches automatiques 21

Partie B — Authentification centralisée et habilitations 22

B.1 Besoin et principe 22
B.2 Compte de service [redacted] 22
B.3 Déclaration de l'annuaire dans GLPI 24
B.4 Import des utilisateurs et première connexion 26
B.5 Groupes AD et règles d'habilitation 28
B.6 Validation des habilitations dynamiques 32
B.7 Cycle de vie des comptes en exploitation 34

Partie C — Déploiement de l'agent d'inventaire 36

C.1 Activation de l'inventaire côté serveur 36
C.2 Choix de la méthode de déploiement 37
C.3 Partage de déploiement sur [redacted] 37
C.4 Script PowerShell et GPO de démarrage 40
C.5 Validation sur les postes clients 41

3. Incidents rencontrés et diagnostics 44

4. Résultat et bilan 49

5. Leçons apprises et axes d'amélioration 50

Annexe A — Index des figures 52

Annexe B — Questions de jury anticipées 55

Annexe C — Ticket d'incident du déploiement de l'agent 56

1. Contexte et objectifs

1.1 Contexte

Le homelab virtualisé sous Proxmox VE héberge l'ensemble des briques de mon Dossier Professionnel : un domaine Active Directory [redacted] un serveur de fichiers organisé selon le modèle AGDLP, une supervision Zabbix, une sauvegarde Proxmox Backup Server et une plateforme de déploiement FOG. Il manquait la brique qui répond à deux questions quotidiennes d'un service informatique : **que contient le parc**, et **qui a demandé quoi**.

GLPI (Gestionnaire Libre de Parc Informatique), édité par Teclib', couvre ces deux besoins : inventaire du matériel et des logiciels d'un côté, centre de services (tickets d'assistance) de l'autre. Son intérêt dans le lab est qu'il se raccorde naturellement aux briques existantes : l'Active Directory pour les identités, les stratégies de groupe pour le déploiement des agents, le serveur de fichiers pour héberger le programme d'installation.

Machine	Adresse	Rôle dans cette brique
[redacted]	[redacted]	Contrôleur de domaine : DNS, annuaire interrogé en LDAP, GPO de déploiement
[redacted]	[redacted]	Partage caché [redacted] contenant le MSI de l'agent
[redacted]	[redacted]	Sauvegarde nocturne de la VM GLPI
[redacted] / 02	[redacted] / . 203	Postes Windows du domaine, cibles de l'inventaire
[redacted]	[redacted]	**Nouveau serveur : application GLPI**

1.2 Objectifs

Partie	Objectif	Critère de validation
A	Installer GLPI sur un socle Linux minimal, maîtrisé et durci	Assistant terminé, installateur supprimé, fichiers sensibles non exposés au web, tâches automatiques exécutées par le cron système
B	Permettre aux utilisateurs du domaine de se connecter avec leurs identifiants AD, et faire dépendre leurs droits de leur appartenance à un groupe	Connexion d'un compte AD, profil attribué automatiquement par une règle sans intervention dans GLPI
C	Inventorier automatiquement les postes du domaine	Agent installé par GPO sans intervention sur le poste, fiche ordinateur créée dans GLPI

1.3 Compétences mobilisées

Code	Domaine	Mise en œuvre dans la brique
CP1	Support et centre de services	Outil de gestion des demandes et du parc, profils Self-Service / Technicien

CP2	Active Directory et GPO	Compte de service, groupes globaux, enregistrements DNS, GPO de démarrage, droits partage/NTFS
CP3	Serveur Linux	Debian 13, réseau NetworkManager, Apache, PHP-FPM, MariaDB, cron
CP6	Automatisation par script	Script PowerShell idempotent d'installation silencieuse de l'agent

2. Architecture et choix techniques

2.1 Vue d'ensemble des flux

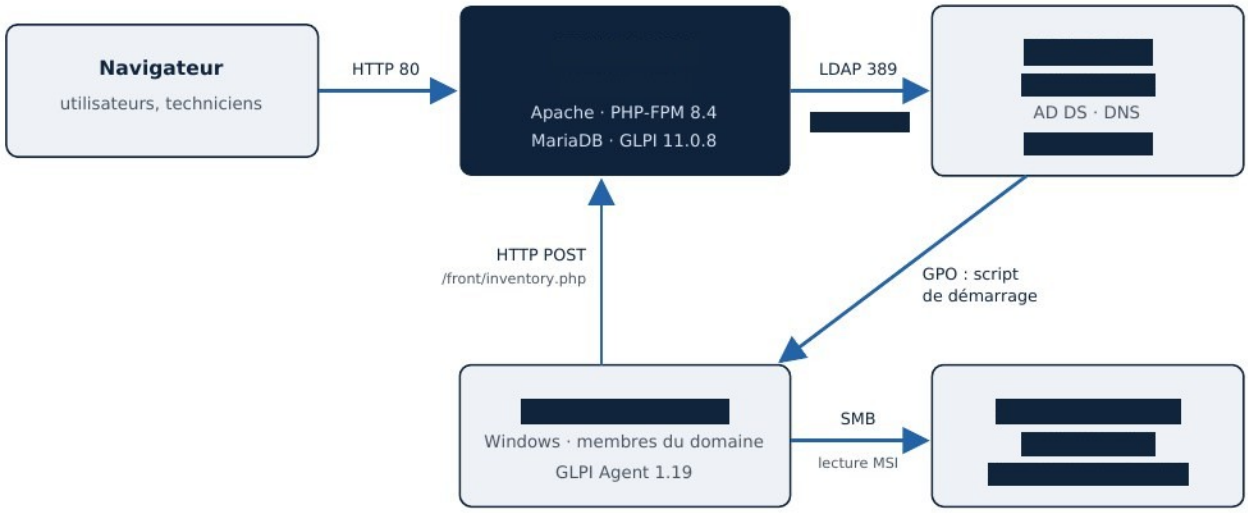


Schéma — Flux entre [redacted] et le reste du lab. Le poste initie toujours la connexion vers le serveur GLPI pour transmettre son inventaire ; GLPI initie la connexion LDAP vers le contrôleur de domaine.

2.2 Fiche technique de la VM

Paramètre	Valeur
VMID / nom	108 — [redacted] — VMID égal au dernier octet de l'IP
Réseau	[redacted] — passerelle [redacted] (Bbox) — DNS [redacted] uniquement
Système	Debian 13.6 « Trixie » netinst, noyau 6.12, installation minimale (SSH + utilitaires)
Processeur / mémoire	2 vCPU type `host` — 4 Go, ballooning minimum 2 Go
Disque	32 Go sur `vmdata`, VirtIO SCSI single, discard et IO thread activés
Micrologiciel	SeaBIOS, machine i440fx
Carte réseau	VirtIO sur `vmbr0`
Intégration Proxmox	Agent QEMU activé, démarrage automatique avec l'hyperviseur, incluse dans le job de sauvegarde PBS

2.3 Choix techniques

Choix retenu	Alternative écartée	Justification
Debian 13	Debian 12 + dépôt PHP tiers	GLPI 11 exige PHP 8.2 minimum ; Debian 13 fournit PHP 8.4 dans ses dépôts officiels. Aucun dépôt tiers, mises à jour de sécurité suivies par Debian.
SeaBIOS / i440fx	OVMF / q35	Aucun besoin d'UEFI, de Secure Boot ou de TPM sur ce serveur ; on évite la complexité NVRAM d'OVMF rencontrée sur la brique FOG.
Installation minimale	Tâche « serveur web » de l'installateur	Contrôler précisément chaque paquet installé plutôt qu'hériter d'une configuration générique.
PHP-FPM	mod_php	PHP tourne dans un pool de processus séparé d'Apache (isolation, limites propres) et Apache reste en MPM event.
MariaDB locale, utilisateur dédié `@localhost`	Compte root, accès réseau	Moindre privilège : l'utilisateur GLPI n'a de droits que sur sa base et ne peut se connecter que localement.
Archive officielle Teclib'	Paquet de distribution	GLPI est distribué directement par l'éditeur. Contrainte d'exploitation assumée : les mises à jour de GLPI ne suivent pas `apt upgrade`.
DocumentRoot sur `public/`	DocumentRoot sur la racine GLPI	Architecture de GLPI 11 : `config/` et `files/` restent hors de la racine web, inaccessibles par une URL.
NetworkManager conservé	`/etc/network/interfaces`	Resté en place après le retrait de GNOME. On ne modifie pas une configuration réseau fonctionnelle en cours de montage ; elle s'administre proprement avec `nmcli`.
Partage dédié sur [redacted]	MSI dans le [redacted]	Le [redacted]se réplique entre tous les contrôleurs de domaine : il est réservé aux scripts et modèles de stratégie, pas au stockage de binaires.

Partie A — Installation et paramétrage

A.1 Création de la machine virtuelle

L'ISO Debian 13.6 netinst a été déposée dans le stockage `local` de l'hyperviseur, puis la VM 108 créée selon la fiche technique ci-dessus. La case « Démarrer à l'amorçage » a été cochée : un serveur d'assistance qui ne redémarre pas seul après une coupure de l'hyperviseur serait indisponible au moment où l'on en a le plus besoin. Le pare-feu Proxmox de la carte réseau a été laissé désactivé pendant l'installation, pour ne pas mêler un filtrage réseau aux éventuels problèmes de téléchargement ; son activation est planifiée en fin de brique (voir section 5).

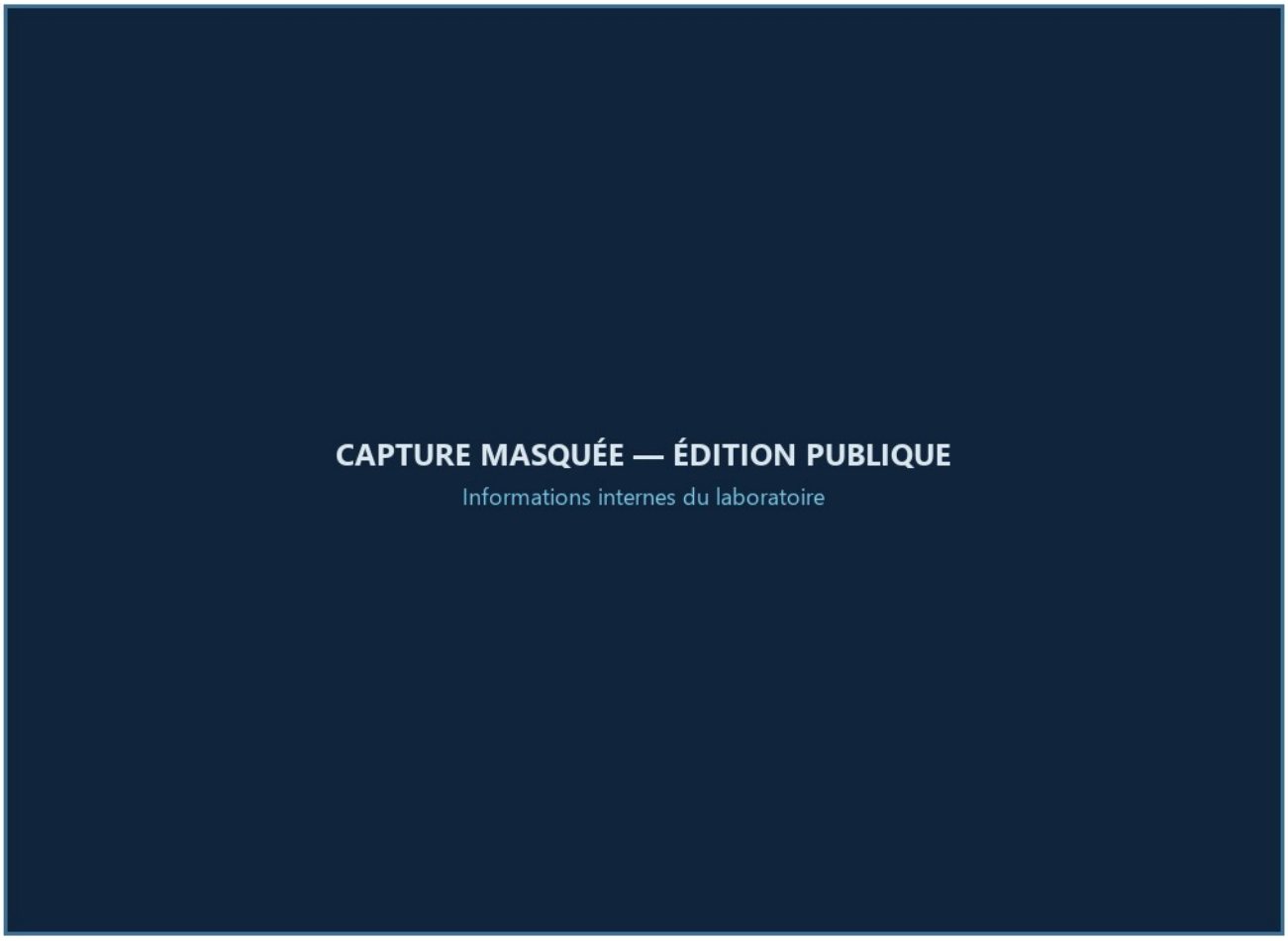


Figure 1 — Sélection de l'image Debian 13.6 netinst lors de la création de la VM



Figure 2 — Récapitulatif de création de la VM 108 [redacted] (onglet Confirmation)



Figure 3 — Vue Matériel de la VM 108 avant le premier démarrage



Figure 4 — Options de la VM : démarrage à l'amorçage et agent QEMU activés



Figure 5 — Premier démarrage sur l'installateur Debian 13, en mode BIOS

A.2 Installation de Debian 13 minimale

L'installation a été réalisée en mode texte depuis la console noVNC. Le réseau a été configuré manuellement (l'autoconfiguration DHCP de la box ayant été annulée) avec un DNS unique pointant sur le contrôleur de domaine : un second résolveur externe (box, 8.8.8.8) ne connaîtrait pas la zone [redacted] et provoquerait des échecs de résolution aléatoires. La machine a été nommée [redacted] dans le domaine DNS [redacted] et un compte `julien` créé en plus de root.

Le partitionnement assisté a produit une partition primaire ext4 de 32,6 Go montée sur `/` et une partition logique de swap de 1,8 Go, sans LVM. Pour un serveur mono-usage, une partition racine unique est cohérente ; en cas de croissance de la base ou des documents joints, l'extension reste possible à chaud : agrandissement du disque dans Proxmox, puis `growpart` et `resize2fs`.

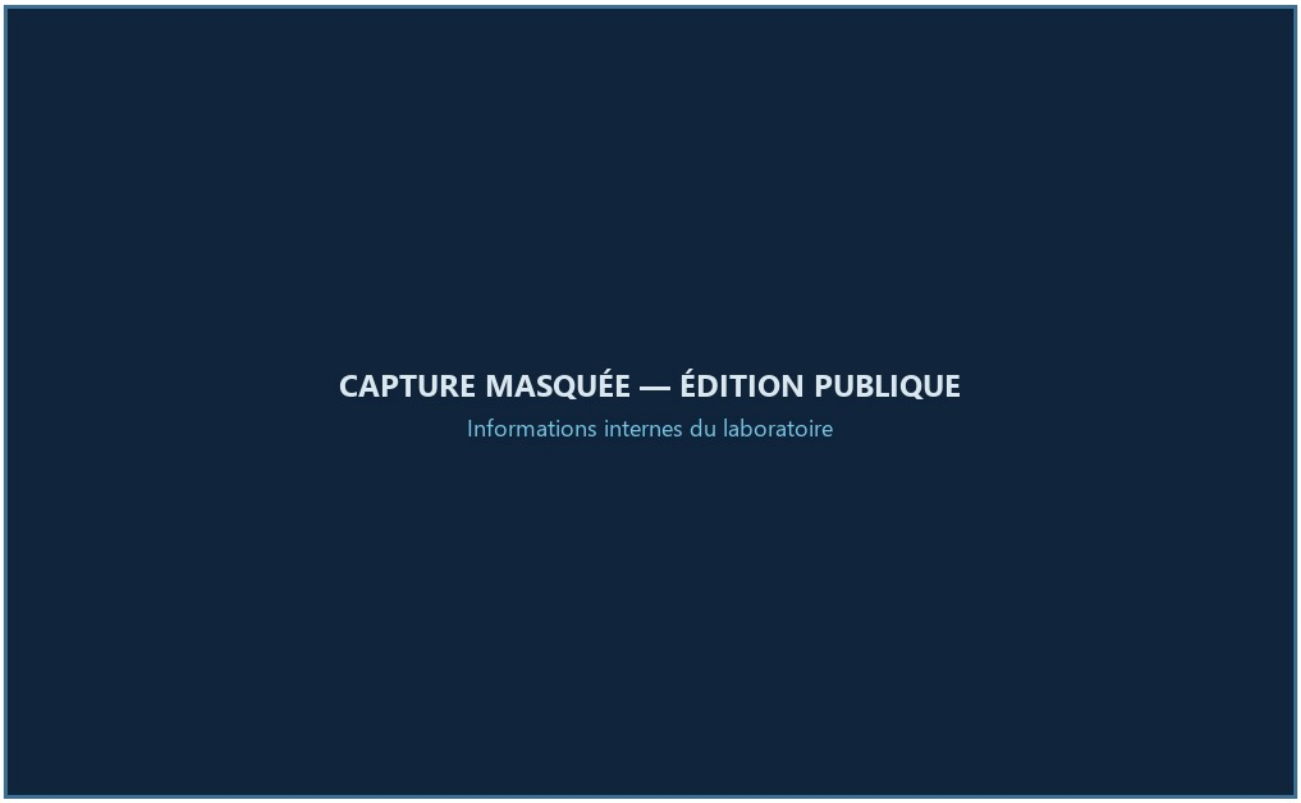


Figure 6 — Table des partitions avant écriture : racine ext4 et swap, sans LVM

À la sélection des logiciels, seuls « serveur SSH » et « utilitaires usuels du système » devaient rester cochés. La capture montre que la tâche « environnement de bureau Debian » est restée cochée : même sans sélectionner GNOME, cette tâche installe le bureau par défaut de Debian, qui est GNOME. Le bureau a donc été retiré après le premier démarrage (incident I1, section 3).



Figure 7 — Sélection des logiciels : « environnement de bureau Debian » resté coché, origine de l'incident I1

```
systemctl set-default multi-user.target
apt purge -y task-gnome-desktop gnome-shell gdm3
apt autoremove --purge -y && apt clean
apt install -y qemu-guest-agent sudo dnsutils
systemctl enable --now qemu-guest-agent
usermod -aG sudo julien
```

A.3 Réseau, résolution DNS et sauvegarde

Correction de la configuration réseau

La configuration héritée du premier passage DHCP laissait deux défauts : le domaine de recherche valait `lan` (celui de la box) et un serveur DNS IPv6 de la box court-circuitait le contrôleur de domaine. IPv6 étant inutile dans ce lab en IPv4, il a été désactivé sur la connexion. La passerelle a ensuite été corrigée en [redacted] (incident I2).

```
nmcli con mod "Wired connection 1" ipv4.dns-search [redacted]
nmcli con mod "Wired connection 1" ipv6.method disabled
nmcli con mod "Wired connection 1" ipv4.gateway [redacted]
nmcli con up "Wired connection 1"
echo 'Acquire::ForceIPv4 "true";' > /etc/apt/apt.conf.d/99force-ipv4
```



Figure 8 — Contrôles post-installation : espace disque, IP fixe, système sain, resolv.conf corrigé, résolution du DC (IPv6 publiques floutées)

> **POINT D'ATTENTION**
>
> La capture montre que `getent hosts` [redacted] renvoyait d'abord une adresse IPv6 publique : le contrôleur de domaine s'est enregistré dans sa propre zone avec l'IPv6 attribuée par la box (enregistrement AAAA en plus du A). Sans conséquence pour GLPI, qui résout bien l'IPv4 (`getent ahostsv4`), mais c'est un résidu à nettoyer côté DC. Les adresses IPv6 publiques ont été floutées sur les captures.

Enregistrement DNS sur le contrôleur de domaine

Contrairement à un poste Windows, un serveur Debian ne s'enregistre pas automatiquement dans le DNS Active Directory. L'enregistrement A et son pointeur PTR ont été créés manuellement dans

le gestionnaire DNS de [redacted] ce qui permet d'atteindre le portail par son nom et facilite la supervision.



Figure 9 — Création de l'hôte [redacted] (A + PTR) dans la zone [redacted] (IPv6 publiques floutées)

```
getent ahostsv4 [redacted]      # résolution directe
dig [redacted] -x [redacted] +short      # résolution inverse (PTR)
```



Figure 10 — Résolutions directe et inverse fonctionnelles depuis le serveur GLPI

Intégration à la sauvegarde

Le job de sauvegarde Proxmox est configuré en mode **exclusion** : toutes les VM sont sauvegardées sauf celles explicitement cochées [redacted] qui ne peut pas se sauvegarder elle-même, et la VM éphémère de test de restauration). La VM 108 a donc été intégrée automatiquement au périmètre, sans modification du job : mode Instantané grâce à l'agent QEMU, compression ZSTD, destination `pbs-lab`, exécution à 02:00.



Figure 11 — Job de sauvegarde en mode exclusion : [redacted] incluse d'office

> **POURQUOI LE MODE EXCLUSION**
>
> En mode sélection, chaque nouvelle VM doit être ajoutée à la main, et c'est l'oubli classique. En mode exclusion, une VM créée plus tard entre d'office dans le périmètre de sauvegarde : le risque est inversé, on ne peut qu'oublier d'exclure, ce qui est sans danger.

A.4 Socle Apache, PHP-FPM et MariaDB

Tous les composants proviennent des dépôts officiels Debian 13. L'extension `php-bcmath` a été ajoutée après la vérification des prérequis de GLPI (incident I4).

```
apt install -y apache2 mariadb-server \
  php php-fpm php-mysql php-mbstring php-curl php-gd php-xml php-intl \
  php-ldap php-zip php-bz2 php-opcache php-cli php-apcu php-bcmath \
  wget unzip curl
```

Extension	Rôle
`php-mysql`	Dialogue avec MariaDB
`php-ldap`	Indispensable à la liaison avec l'Active Directory (partie B)
`php-gd` , `php-intl`	Traitement d'images et internationalisation

`php-apcu`, `php-opcache`	Cache applicatif et cache du code compilé
`php-zip`, `php-bz2`	Gestion des archives
`php-bcmath`	Calcul en précision arbitraire, exigé par GLPI 11 (génération de QR codes)

Au premier essai, l'installation a échoué faute de sortie Internet. La passerelle a été corrigée (incident I2) avant de relancer la commande :

```
[redacted] ip route
default via [redacted] dev ens18 proto static metric 100
[redacted] dev ens18 proto kernel scope link src [redacted] metric 100
[redacted] ping -c2 9.9.9.9
64 bytes from 9.9.9.9: icmp_seq=1 ttl=53 time=10.3 ms
64 bytes from 9.9.9.9: icmp_seq=2 ttl=53 time=8.91 ms
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
```



Figure 12 — Versions installées depuis les dépôts Debian : PHP 8.4.24, Apache 2.4.68, MariaDB 11.8.6

```
a2enmod proxy_fcgi setenvif rewrite
a2enconf php8.4-fpm
systemctl enable --now php8.4-fpm mariadb apache2
systemctl restart apache2
systemctl is-active apache2 php8.4-fpm mariadb
curl -I [redacted]
```



Figure 13 — Modules et configuration PHP-FPM activés, trois services actifs, Apache répondant en HTTP 200

A.5 Base de données GLPI

MariaDB a d'abord été durcie avec `mariadb-secure-installation` : mot de passe root explicite (authentification `unix_socket` non retenue, pour garder une authentification documentée), suppression des utilisateurs anonymes et de la base de test, interdiction de la connexion root à distance. La base et son utilisateur dédié ont ensuite été créés.

```
CREATE DATABASE [redacted] CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
CREATE USER [redacted] IDENTIFIED BY '********';
GRANT ALL PRIVILEGES ON [redacted] TO [redacted]
GRANT SELECT ON mysql.time_zone_name TO [redacted]
FLUSH PRIVILEGES;
```

```
mariadb-tzinfo-to-sql /usr/share/zoneinfo | mariadb -u root -p mysql
```

POURQUOI CES CHOIX

- **utf8mb4** couvre l'intégralité de l'Unicode ; l'ancien jeu `utf8` de MySQL est limité à 3 octets par caractère.
- **Utilisateur dédié limité à localhost** : droits restreints à la seule base [redacted] aucune connexion possible depuis le réseau.
- **Fuseaux horaires chargés** et lisibles par [redacted] : sans eux, GLPI affiche un avertissement permanent et la gestion des dates est approximative.



Figure 14 — Connexion avec [redacted] : base [redacted] accessible, 486 fuseaux horaires chargés

La capture démontre le moindre privilège : [redacted] ne voit que sa base, `information_schema`, et la base `mysql` uniquement parce qu'il dispose d'un droit de lecture sur la table des fuseaux. La visibilité d'une base ne donne pas accès à ses autres tables.

A.6 Déploiement de GLPI 11 et hôte virtuel Apache

```
cd /tmp
wget https://github.com/glpi-project/glpi/releases/download/11.0.8/glpi-11.0.8.tgz
tar -xzf glpi-11.0.8.tgz -C /var/www/
chown -R www-data:www-data /var/www/glpi
find /var/www/glpi -type d -exec chmod 755 {} \;
find /var/www/glpi -type f -exec chmod 644 {} \;
```

Apache s'exécute sous l'identité `www-data`, propriétaire de l'arborescence : répertoires en 755 (traversables), fichiers en 644 (lisibles, non exécutables). Aucun droit 777.



Figure 15 — Version 11.0.8 confirmée par le répertoire version et par la constante GLPI_VERSION du code source

```
<VirtualHost *:80>
    ServerName [redacted]
    DocumentRoot /var/www/glpi/public

    <Directory /var/www/glpi/public>
        Require all granted
        RewriteEngine On
        RewriteCond %{HTTP:Authorization} ^(.+)$
        RewriteRule .* - [E=HTTP_AUTHORIZATION:%1]
        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/glpi_error.log
    CustomLog ${APACHE_LOG_DIR}/glpi_access.log combined
</VirtualHost>
```

```
a2dissite 000-default.conf
a2ensite glpi.conf
apache2ctl configtest
systemctl reload apache2
curl -I [redacted]
```

POURQUOI LE DOCUMENTROOT SUR PUBLIC/

C'est le changement de sécurité majeur de GLPI 11. Seul `public/` est exposé au web ; `config/` (identifiants de la base) et `files/` (documents joints) sont hors de la racine web et physiquement inaccessibles par une URL, quelle que soit la configuration du reste d'Apache. Les versions antérieures exposaient toute l'arborescence et la protégeaient par des règles `.htaccess` . Les règles de réécriture renvoient toute requête vers le contrôleur frontal `index.php` .



Figure 16 — Syntaxe Apache validée et réponse HTTP 200 avec cookie de session HttpOnly

Le cookie de session porte l'attribut `HttpOnly` : il ne peut pas être lu par du JavaScript dans le navigateur, ce qui limite le vol de session en cas de faille XSS.

A.7 Assistant d'installation

L'assistant web a été lancé depuis un navigateur du réseau local sur `http://srv-` [redacted] L'accès au site ne demande pas que le poste soit membre du domaine : seules la résolution DNS et la connectivité sur le port 80 sont nécessaires. L'appartenance au domaine n'interviendra que pour l'authentification (partie B), et c'est alors GLPI qui interrogera le contrôleur de domaine.

La vérification des prérequis a signalé une seule extension bloquante, `bcmath` , installée puis prise en compte après redémarrage de PHP-FPM (incident I4).



Figure 17 — Vérification des prérequis : tests requis validés



Figure 18 — Fin de la vérification : tests de sécurité et extensions suggérées (LDAP, OPcache) validés

La connexion à la base utilise `localhost` et non l'adresse IP : l'utilisateur étant déclaré [redacted] une connexion via 127.0.0.1 ou [redacted] serait vue par MariaDB comme provenant d'un autre hôte et refusée. La connexion passe en outre par la socket Unix locale, sans aller-retour réseau.

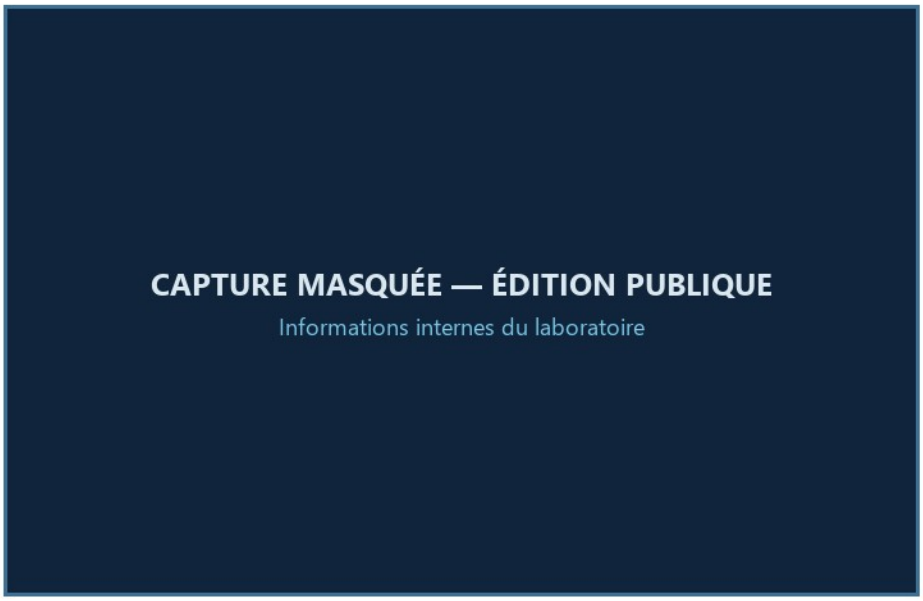


Figure 19 — Connexion de l'assistant à la base de données (mot de passe masqué)



Figure 20 — Initialisation de la base réussie

L'envoi de statistiques d'usage a été décoché : un serveur interne ne transmet pas de données vers l'extérieur sans décision explicite de la DSI.

L'assistant rappelle en fin d'installation les quatre comptes créés par défaut, `glpi`, `tech`, `normal` et `post-only`, dont les mots de passe par défaut sont documentés publiquement. La première connexion se fait sur la base interne de GLPI, seule source d'authentification disponible à ce stade.

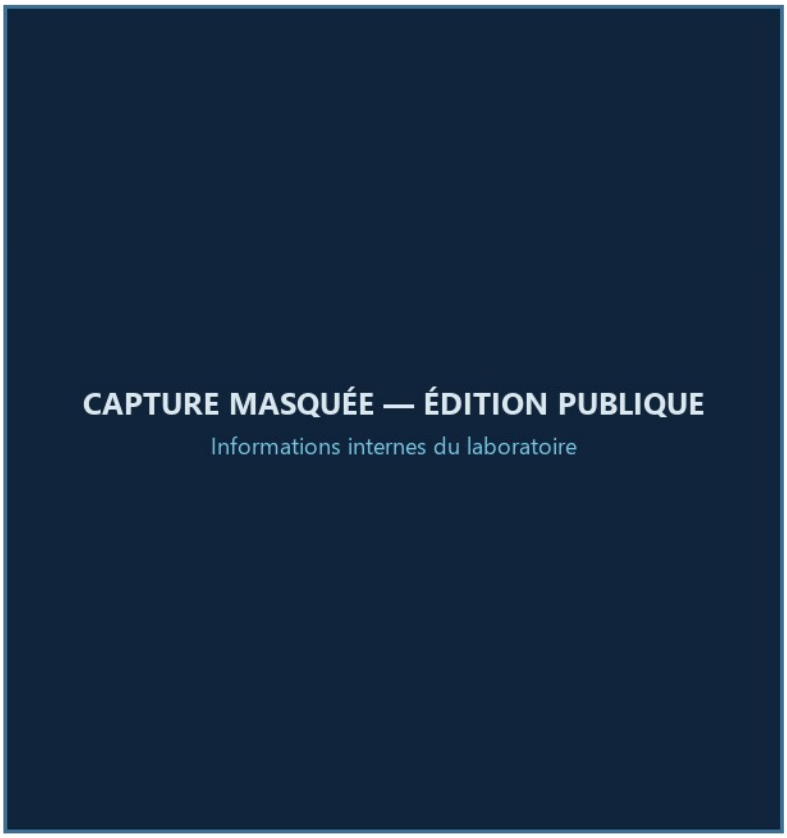


Figure 21 — Page de connexion de GLPI après installation : source « Base interne GLPI »

A.8 Sécurisation post-installation

Les quatre comptes créés par défaut (`glpi`, `tech`, `normal`, `post-only`) ont des identifiants publiquement connus : c'est la première faille des installations GLPI. Ils ont été **renommés** (par exemple `glpi` devenu `glpi-system`, `tech` devenu `technicien`) et leurs mots de passe changés, et un compte nominatif `julien` a été créé pour l'administration courante. Renommer plutôt que seulement changer le mot de passe prive un attaquant de la moitié de l'information.



Figure 22 — Liste des utilisateurs après renommage des comptes par défaut

```
rm -f /var/www/glpi/install/install.php
curl -I [redacted]      # 404 attendu
curl -I [redacted]      # 404 attendu
```

```
[redacted] curl -I [redacted]
HTTP/1.1 404 Not Found
Server: Apache/2.4.68 (Debian)
x-frame-options: SAMEORIGIN
Set-Cookie: glpi_…; path=/; HttpOnly
```

Les deux requêtes renvoient 404. La première empêche de relancer l'assistant par-dessus l'installation existante. La seconde prouve que le fichier contenant les identifiants MariaDB n'est pas atteignable depuis le web, grâce au DocumentRoot sur `public/`. On relève aussi l'en-tête `x-frame-options: SAMEORIGIN` posé par GLPI, qui protège contre le détournement de clic (clickjacking).

A.9 Tâches automatiques

GLPI s'appuie sur des actions automatiques (envoi des notifications, purge des journaux, traitements d'inventaire). En mode « GLPI », elles ne se déclenchent qu'au chargement d'une page par un utilisateur, donc jamais la nuit ni le week-end. Elles ont été confiées au cron système.

```
echo "* * * * * www-data /usr/bin/php /var/www/glpi/front/cron.php" > /etc/cron.d/glpi
chmod 644 /etc/cron.d/glpi
systemctl restart cron
```

La tâche s'exécute sous `www-data` et non sous root : le processus n'a que les droits nécessaires sur l'arborescence GLPI, et les fichiers de cache qu'il crée restent modifiables par le serveur web. Dans **Configuration → Actions automatiques**, les 48 actions ont été basculées en mode **CLI** par une action de masse. Certaines restent désactivées par défaut (vérification de réplication SQL, recherche de mises à jour) : elles ne servent que dans des contextes précis et n'ont pas été activées sans raison.



Figure 23 — Actions automatiques : 48 actions en mode CLI, dernières exécutions le jour même

Partie B — Authentification centralisée et habilitations

B.1 Besoin et principe

Le besoin : permettre aux utilisateurs du domaine d'accéder à GLPI avec leurs identifiants habituels, et faire dépendre leurs droits dans l'outil de leur appartenance à un groupe de l'annuaire, sans double gestion des comptes.

Le principe : GLPI ne stocke aucun mot de passe pour ces utilisateurs. À la connexion, il transmet la demande d'authentification au contrôleur de domaine en LDAP, qui valide les identifiants. Une seule politique de mots de passe s'applique, et la désactivation d'un compte dans l'AD ferme immédiatement l'accès à GLPI. Les droits sont ensuite calculés par des règles qui lisent les groupes AD de l'utilisateur.

B.2 Compte de service [redacted]

GLPI a besoin d'un compte pour interroger l'annuaire (opération de « bind »). Un compte de service dédié a été créé dans une unité d'organisation `Comptes de service`, qui sépare les comptes techniques des comptes utilisateurs et permet de leur appliquer des stratégies spécifiques.



Figure 24 — Création de l'OU Comptes de service à la racine du domaine

Option du compte	Justification
Changement du mot de passe à la prochaine ouverture : **non**	Un compte de service ne se connecte jamais de façon interactive
L'utilisateur ne peut pas changer de mot de passe : **oui**	Le mot de passe est géré par l'administrateur, pas par le service
Le mot de passe n'expire jamais : **oui**	Une expiration arrêterait la liaison sans prévenir, panne difficile à diagnostiquer

Groupes : **Utilisateurs du domaine uniquement**	Tout utilisateur authentifié peut lire l'annuaire : c'est le besoin exact, ni plus ni moins



Figure 25 — Création du compte [redacted] dans l'OU Comptes de service



Figure 26 — Le compte [redacted] dans son OU dédiée



Figure 27 — Nom distinctif (distinguishedName) de [redacted] dans l'OU Comptes de service

> **POURQUOI LE MOINDRE PRIVILÈGE ICI**
>
> Le mot de passe de ce compte est enregistré dans la configuration d'une application web. Si ce compte était administrateur du domaine, la compromission du serveur GLPI donnerait les clés de tout le domaine. En lecture seule, une fuite expose au pire le contenu de l'annuaire.

B.3 Déclaration de l'annuaire dans GLPI

Dans **Configuration → Authentification → Annuaires LDAP**, un annuaire a été ajouté à partir du préréglage Active Directory, puis complété.

Champ	Valeur
Nom	AD [redacted] — serveur par défaut, actif
Serveur / port	[redacted] / 389
BaseDN	[redacted]
DN du compte (bind)	[redacted] de [redacted]
Filtre de connexion	`(&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))`
Champ de l'identifiant	`samaccountname`
Champ de synchronisation	`objectguid`

POURQUOI CES VALEURS

- **Filtre** : ne retient que les objets utilisateurs de type personne et exclut les comptes désactivés. La dernière condition teste le bit 2 (compte désactivé) de l'attribut `userAccountControl` au moyen de la règle de comparaison binaire de l'AD. Sans ce filtre, GLPI verrait aussi les comptes d'ordinateurs et les comptes désactivés.
- **samaccountname** : c'est l'identifiant court que les utilisateurs saisissent déjà pour ouvrir leur session Windows.
- **objectguid** : identifiant unique généré par l'AD à la création de l'objet et jamais modifié. Si l'on se basait sur le DN, un simple déplacement d'utilisateur entre deux OU changerait son identité aux yeux de GLPI et créerait un doublon.

Une espace parasite après la virgule dans le DN du compte a été retirée avant validation, et le filtre de connexion, laissé vide par le préréglage, a été renseigné.



Figure 28 — Paramètres de l'annuaire Active Directory dans GLPI (mot de passe masqué)

Le test de connexion déroule les cinq étapes d'une liaison LDAP : ouverture du flux TCP sur le port 389, prise en compte du BaseDN, validation de l'URI, authentification du compte de service, puis exécution d'une recherche. Il trouve 8 utilisateurs dans l'annuaire.



Figure 29 — Test de la liaison LDAP réussi : cinq étapes validées, 8 utilisateurs trouvés

B.4 Import des utilisateurs et première connexion

Sous GLPI 11, l'import n'est plus proposé dans la barre d'outils de la liste des utilisateurs ; il a été atteint par sa page dédiée `/front/ldap.import.php`. Les comptes proposés portent leur `objectguid` comme identifiant de synchronisation, preuve directe du paramétrage précédent.



Figure 30 — Les 8 comptes de l'annuaire proposés à l'import, identifiés par leur objectguid

L'import a été **sélectif** : les comptes utilisateurs [redacted] [redacted] `lbernard`, `jb`, `ab`) ont été importés, tandis que [redacted] et les comptes d'administration `adm-srvad` et `adm-julien` ont été écartés. Ces comptes techniques n'ont pas vocation à apparaître comme usagers du parc ni à ouvrir des tickets.



Figure 31 — Utilisateurs GLPI après import : comptes AD aux côtés des comptes locaux

[redacted] s'est ensuite connecté avec son identifiant et son mot de passe de domaine. Il reçoit le profil par défaut **Self-Service** : il peut créer et suivre ses propres tickets, sans voir le parc ni les demandes des autres.

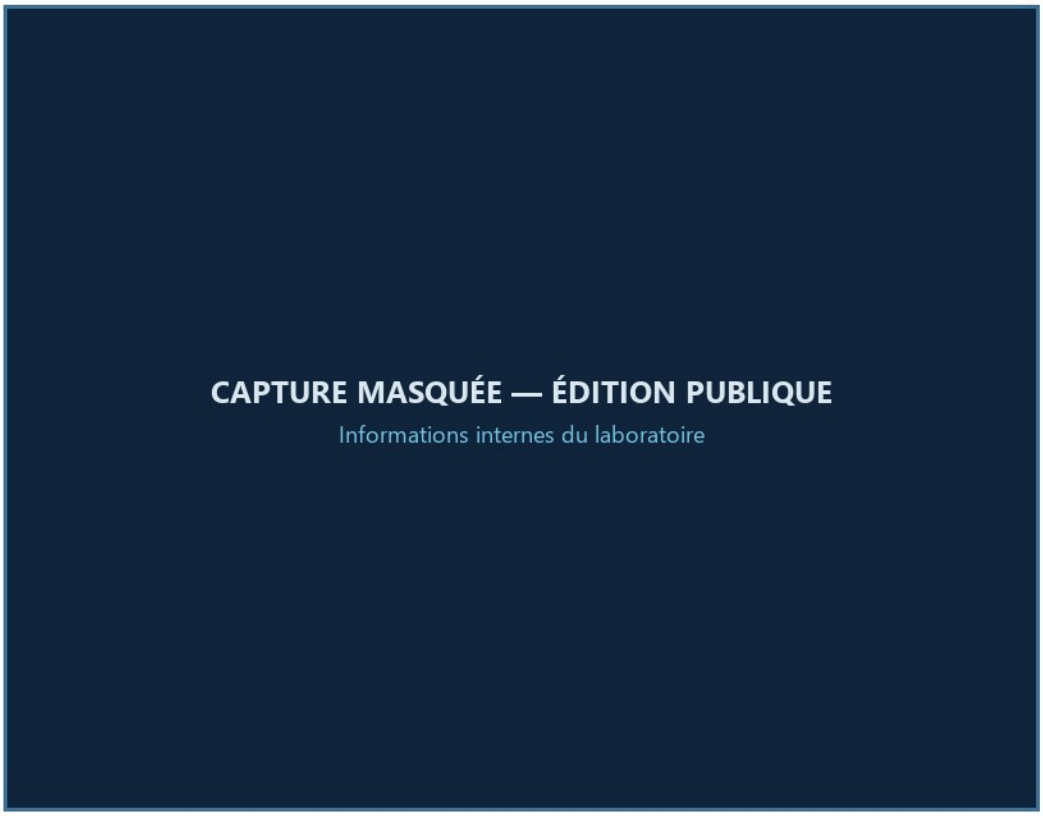


Figure 32 — Connexion de [redacted] avec ses identifiants de domaine, source « AD [redacted] »

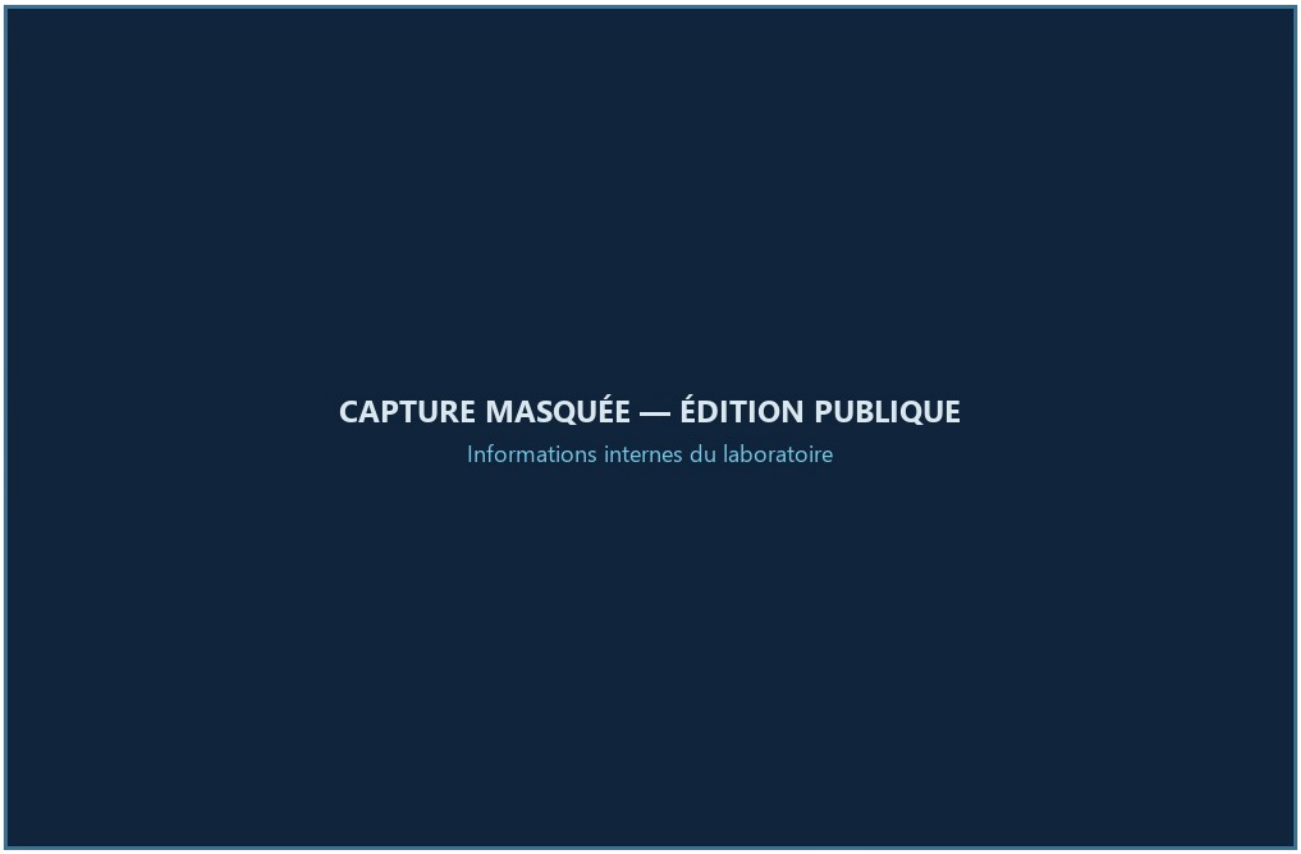


Figure 33 — Portail Self-Service ouvert pour [redacted]

B.5 Groupes AD et règles d'habilitation

Groupes de l'annuaire

L'arborescence existante (OU Utilisateurs, Ordinateurs, Groupes, Comptes de service) a été conservée : les règles d'habilitation de GLPI s'appuient sur l'appartenance à un groupe, pas sur l'emplacement dans l'annuaire. Deux groupes globaux de sécurité ont été créés dans l'OU `Groupes`, dans la convention de nommage des groupes AGDLP déjà en place.

Groupe	Membre de test	Profil GLPI visé
[redacted]	[redacted]	Technician
[redacted]	[redacted]	Super-Admin

Un troisième groupe [redacted] a été étudié puis écarté : le profil Self-Service étant déjà attribué par défaut à tout utilisateur importé, ce groupe n'aurait d'intérêt que pour restreindre l'accès à GLPI à un périmètre défini, ce qui demanderait en plus un filtre de connexion dédié (voir axes d'amélioration).

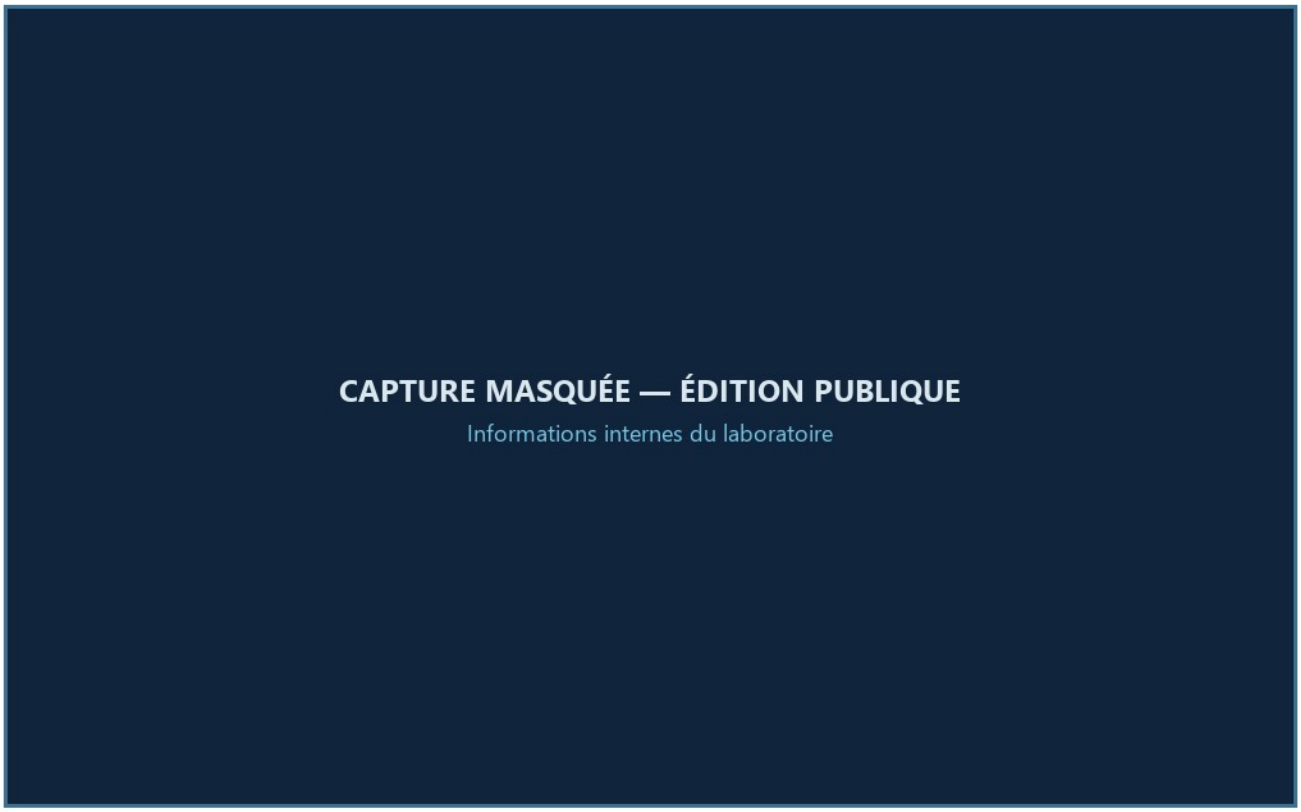


Figure 34 — Création d'un groupe global de sécurité dans l'OU Groupes, à côté des groupes AGDLP existants



Figure 35 — Groupes [redacted] et [redacted] dans l'OU Groupes

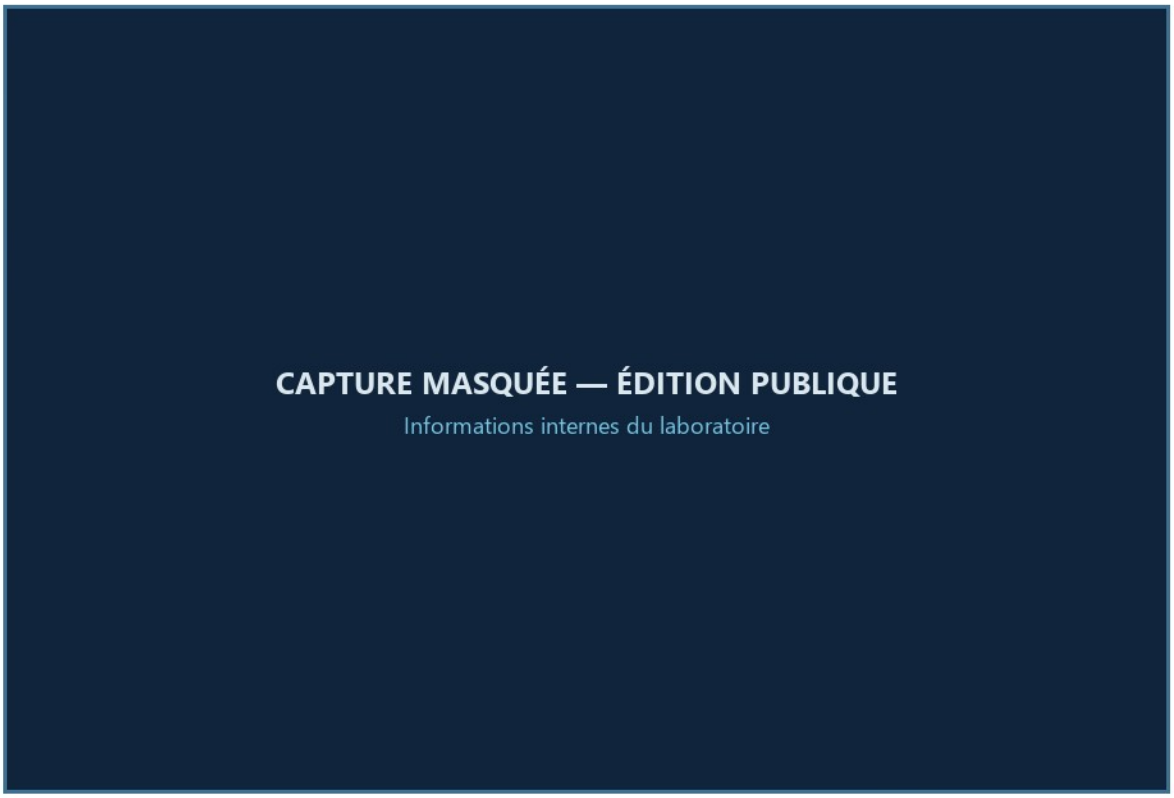


Figure 36 — Ajout de [redacted] au groupe [redacted]

L'onglet **Groupes** de l'annuaire, déjà renseigné par le préréglage, indique à GLPI comment lire l'appartenance : recherche **dans les utilisateurs**, via l'attribut `memberof`. GLPI lit directement sur la fiche de l'utilisateur la liste de ses groupes, au lieu de parcourir chaque groupe à la recherche de ses membres, ce qui est nettement plus efficace sur un annuaire volumineux.



Figure 37 — Paramètres de lecture des groupes : recherche dans les utilisateurs, attribut memberof

Règles d'affectation d'habilitations

Dans **Administration → Règles → Règles d'affectation d'habilitations à un utilisateur**, une règle a été créée par groupe.

Règle	Critère	Actions
AD - Techniciens GLPI	(LDAP) MemberOf **contient** [redacted]	Profil → Technician ; Entité → Entité racine
AD - Admins GLPI	(LDAP) MemberOf **contient** [redacted]	Profil → Super-Admin ; Entité → Entité racine



Figure 38 — Création de la règle AD - Techniciens GLPI, activée



Figure 39 — Critère de la règle : (LDAP) MemberOf contient [redacted]



Figure 40 — Actions de la règle : profil Technician et entité racine

POURQUOI CES RÉGLAGES

- « **contient** » **plutôt que** « **est** » : `memberof` renvoie le DN complet du groupe [redacted] ; on recherche donc le nom du groupe comme sous-chaîne.
- **Action Entité obligatoire** : une habilitation GLPI est un couple profil + entité. Sans entité, GLPI ne sait pas sur quel périmètre attribuer le profil et la règle reste sans effet. Dans une organisation multi-sites, c'est ce champ qui distingue un technicien de tout le parc d'un technicien d'agence.
- **Règle activée** : le formulaire de création propose « Activé : Non » par défaut ; une règle non activée est ignorée.

POINT D'ATTENTION — LE CHOIX DU CRITÈRE

Le critère « Critères globaux - Annuaire LDAP » a d'abord été sélectionné par erreur. Il teste *quel annuaire* a authentifié l'utilisateur, pas son appartenance à un groupe : la règle aurait donné le profil Technician à tous les utilisateurs du domaine. Il a été remplacé par **(LDAP) MemberOf** avant validation (incident I6).

La liste finale contient les deux règles créées, en positions 1 et 2, puis la règle native `Root`, qui affecte l'entité racine aux utilisateurs authentifiés par annuaire LDAP ou par serveur de messagerie, sans toucher aux profils. Une règle vide, créée avant l'abandon du troisième groupe, a été supprimée. L'écran le précise : le moteur traite toutes les règles. Il n'y a pas d'arrêt à la première correspondance : un utilisateur membre des deux groupes cumulerait les deux habilitations, et choisirait son profil actif dans le sélecteur de l'interface.



Figure 41 — Règles d'affectation d'habilitations : les deux règles AD puis la règle native Root

B.6 Validation des habilitations dynamiques

Les règles s'évaluent à la connexion et lors d'une synchronisation, pas rétroactivement sur un compte déjà importé. La synchronisation manuelle d'un compte se fait depuis l'onglet **Synchronisation** de sa fiche utilisateur (et non depuis la barre d'outils de la liste, comme dans les versions précédentes).

[redacted] — groupe Techniciens

Après synchronisation, l'onglet Habilitations de [redacted] affiche Technician sur l'entité racine, suivi du marqueur **(D)** pour « dynamique » : l'habilitation a été attribuée par une règle et sera recalculée à chaque synchronisation. Retirer [redacted] du groupe dans l'AD lui retirera ce profil, sans intervention dans GLPI. Le profil Self-Service attribué à l'import coexiste avec le profil Technician, et la connexion de [redacted] donne bien accès à l'interface technicien (parc, assistance).

[redacted] — groupe Admins

La même démonstration a été conduite pour [redacted] en cinq étapes : état initial avec le seul profil Self-Service (D), synchronisation forcée, apparition du profil Super-Admin dynamique, connexion avec la source d'authentification « AD [redacted] », puis sélecteur de profils montrant les deux habilitations. Elle arrive sur le profil Self-Service et bascule vers Super-Admin lorsqu'elle en a besoin : on ne travaille pas en permanence avec les droits maximaux, sur le même principe que l'UAC sous Windows ou `sudo` sous Linux.



Figure 42 — [redacted] avant synchronisation : profil Self-Service (D) uniquement



Figure 43 — Onglet Synchronisation de la fiche utilisateur : « Forcer la synchronisation »



Figure 44 — Après synchronisation : Super-Admin attribué dynamiquement (D), en plus de Self-Service



Figure 45 — Connexion de [redacted] avec la source d'authentification AD [redacted]



Figure 46 — Sélecteur de profils de [redacted] : Self-Service et Super-Admin

POINT D'ATTENTION — DÉLÉGATION SILENCIEUSE

Ajouter un compte au groupe [redacted] dans l'AD lui donne les pleins pouvoirs sur GLPI sans que personne n'ouvre l'application. C'est tout l'intérêt du mécanisme, et son risque : l'appartenance à ce groupe doit être réservée à des comptes qui le justifient et contrôlée comme celle de tout groupe à privilèges.

B.7 Cycle de vie des comptes en exploitation

La synchronisation compte par compte ne sert qu'aux tests. En exploitation, trois niveaux se complètent :

Mécanisme	Effet	État dans le lab
Synchronisation à la connexion	Réévaluation des règles à chaque ouverture de session : un changement de groupe est pris en compte à la connexion suivante	**En place** (natif)
Synchronisation planifiée des comptes existants	Mise à jour des comptes qui ne se connectent pas (nom, service, désactivation)	**À planifier**
Import planifié des nouveaux comptes	Un arrivant existe dans GLPI avant sa première connexion, ce qui permet de lui affecter du matériel à l'avance	**À planifier**

Les deux derniers niveaux s'automatisent avec la console GLPI, lancée sous `www-data` depuis le cron système (les options exactes sont à valider avec `--help` sur la version installée) :

```
cd /var/www/glpi
sudo -u www-data php bin/console list | grep -i ldap
sudo -u www-data php bin/console ldap:synchronize_users --help
```

Partie C — Déploiement de l'agent d'inventaire

C.1 Activation de l'inventaire côté serveur

GLPI intègre nativement la réception des inventaires, mais elle est désactivée par défaut. Elle a été activée dans **Administration → Inventaire** ; les options d'import (traitement des machines déjà connues, doublons) ont été laissées par défaut.



Figure 47 — Configuration de l'inventaire : activation, options d'import, composants inventoriés

L'écran fixe aussi la fréquence d'inventaire (24 heures), l'entité par défaut (racine) et la liste des composants importés. L'authentification des agents est laissée sur « Aucun » : tout poste capable de joindre le serveur peut lui soumettre un inventaire. C'est acceptable en laboratoire, mais à durcir en production (section 5).

```
curl -I [redacted]
```

Le point d'entrée répond **405 Method Not Allowed**, le résultat attendu : il existe et fonctionne, mais n'accepte que la méthode POST utilisée par les agents pour transmettre leur inventaire, et refuse la requête HEAD du test.



Figure 48 — Point d'entrée inventory.php : réponse 405, le service attend des requêtes POST

C.2 Choix de la méthode de déploiement

L'agent doit connaître l'adresse du serveur GLPI, ce qui impose de passer des paramètres au programme d'installation.

Méthode	Analyse
GPO « Installation de logiciel »	Écartée : ne permet pas de passer de paramètres au MSI. L'agent s'installerait sans savoir où envoyer son inventaire.
Transformation MST	Méthode officielle pour paramétrer un MSI déployé par GPO, mais demande un éditeur de transformations (Orca) et reste peu lisible.
Script de démarrage par GPO	**Retenue** : commande `msiexec` explicite, lisible, documentable, et même méthode que l'agent Zabbix déjà déployé (GPO-Zabbix-Agent).

Le script de démarrage s'exécute au boot sous le compte **ordinateur** (par exemple `PC-CLIENT-01$`) avec les droits SYSTEM, ce qui conditionne les permissions du partage. Le MSI est hébergé sur [redacted] et le script dans le [redacted] chacun à l'emplacement correspondant à sa vocation.

C.3 Partage de déploiement sur [redacted]

Un dossier [redacted] a été créé et partagé sous le nom caché [redacted] (le `$` appartient au nom du partage, pas au nom du dossier). Le MSI `GLPI-Agent-1.19-x64.msi`, téléchargé depuis les publications officielles du projet sur GitHub, y a été déposé avec son numéro de version, pour savoir quelle version tourne sur le parc.

Couche	Groupe	Droit
Partage	Tout le monde	Supprimé
Partage	Utilisateurs du domaine	Lecture
Partage	Ordinateurs du domaine	Lecture
NTFS	Ordinateurs du domaine	Lecture et exécution



Figure 49 — Dossier [redacted] créé dans [redacted] sur [redacted]

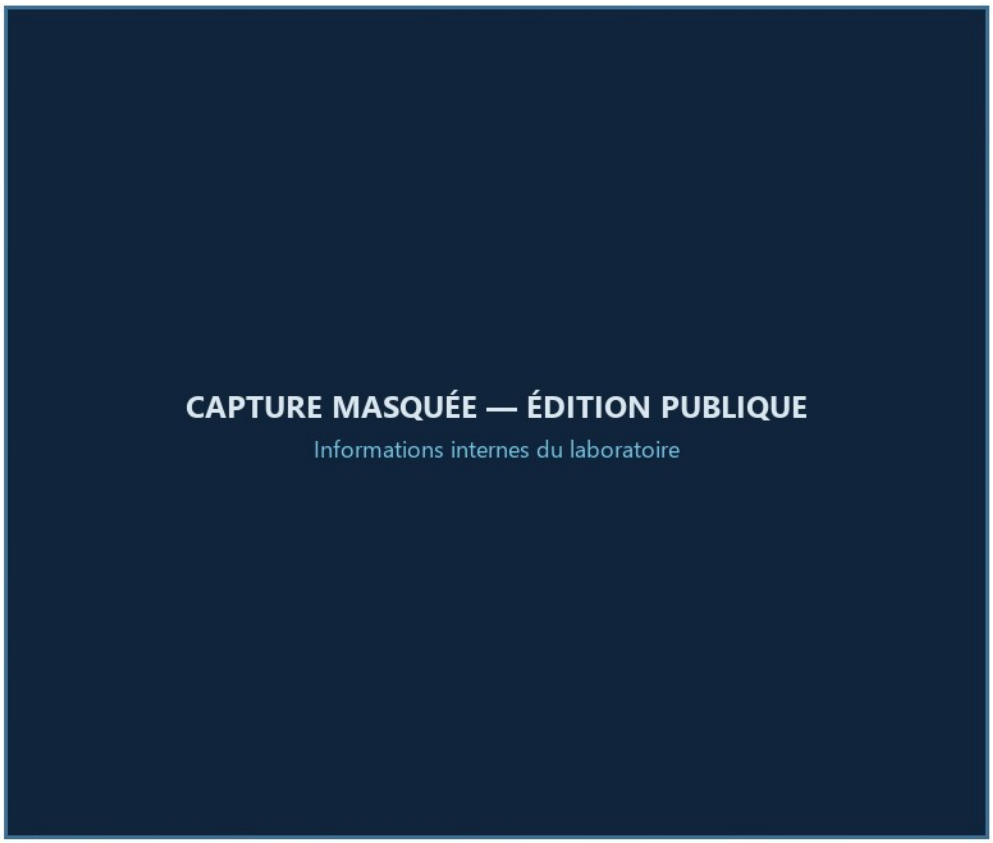


Figure 50 — Partage avancé [redacted] : Ordinateurs et Utilisateurs du domaine en lecture

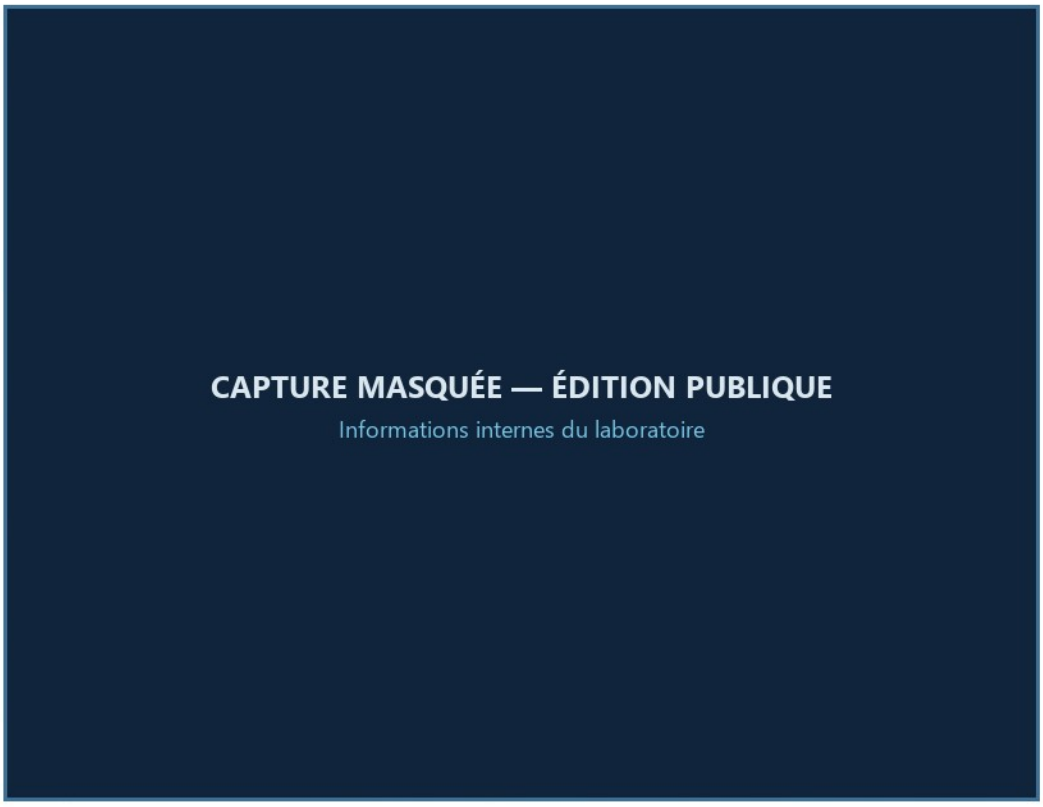


Figure 51 — Permissions NTFS : Ordinateurs du domaine en Lecture et exécution

L'accès a été contrôlé depuis une autre machine du domaine : le MSI (22 720 Ko) est bien visible par le chemin UNC du partage caché.



Figure 52 — Le MSI GLPI-Agent-1.19-x64.msi visible via [redacted] depuis [redacted]

POINT D'ATTENTION — CONTRÔLE TOTAL RETIRÉ

Le groupe `Ordinateurs du domaine` a d'abord été ajouté au partage avec le contrôle total. Or un poste compromis pouvant écrire dans ce partage pourrait remplacer le MSI par un binaire malveillant, ensuite installé sur tout le parc avec les droits SYSTEM. Le droit a été ramené à la seule lecture.

> **POURQUOI DEUX COUCHES DE DROITS**
>
> Les autorisations de partage ne s'appliquent qu'aux accès réseau ; les permissions NTFS s'appliquent toujours. Pour un accès par le réseau, c'est la plus restrictive des deux qui l'emporte. Le groupe `Ordinateurs du domaine` est indispensable : sans lui, le script, qui tourne sous le compte ordinateur, échouerait silencieusement faute d'accès au MSI. Dans la boîte de sélection NTFS, il faut cocher le type d'objet « Ordinateurs » pour que ce groupe soit trouvé.

C.4 Script PowerShell et GPO de démarrage

Le script

Version corrigée, en service. La version initiale et ses défauts sont analysés dans l'incident I7.

```
# [redacted] de l'agent GLPI - Julien Barbet
# Verifie la presence de l'agent avant installation (idempotence)

$Msi      = [redacted]
$Serveur  = [redacted]
$Marqueur = "$env:ProgramFiles\GLPI-Agent\glpi-agent.bat"

if (Test-Path $Marqueur) { exit 0 }

$Arguments = @(
    "/i", "`"$Msi`""
    "/quiet", "/norestart"
    "RUNNOW=1"
    "SERVER=`"$Serveur`""
    "ADD_FIREWALL_EXCEPTION=1"
)

Start-Process msiexec.exe -ArgumentList $Arguments -Wait -NoNewWindow
exit 0
```

Élément	Rôle
`Test-Path $Marqueur`	Idempotence : si l'agent est déjà installé, le script sort immédiatement au lieu de réinstaller à chaque démarrage
Guillemets simples sur `$Msi`	Le `$` de [redacted] est pris littéralement ; entre guillemets doubles, PowerShell tenterait de l'interpréter comme une variable
`/quiet /norestart`	Installation silencieuse, sans redémarrage imposé
`SERVER`	Adresse du point d'entrée d'inventaire de GLPI
`RUNNOW=1`	Premier inventaire transmis immédiatement après l'installation
`ADD_FIREWALL_EXCEPTION=1`	Exception dans le pare-feu Windows pour le petit serveur HTTP local de l'agent, qui permet de déclencher un inventaire à distance
`Start-Process … -Wait`	Le script attend la fin de `msiexec` avant de se terminer

La GPO

Une GPO `GPO - [redacted] Agent GLPI` a été créée et liée à l'OU `Ordinateur`, en troisième position après GPO-RDP-AutoAcces et GPO-Zabbix-Agent (aucun conflit de paramètres entre elles).

Le script, nommé [redacted] (sans espace, source classique d'échec silencieux en ligne de commande), a été déposé via le bouton « Afficher les fichiers » dans le dossier `Machine\Scripts\Startup` de la GPO, puis déclaré dans l'onglet **Scripts PowerShell** de **Configuration ordinateur → Stratégies → Paramètres Windows → Scripts (démarrage/arrêt)**.



Figure 53 — GPO liée à l'OU Ordinateur et script [redacted] déclaré dans l'onglet Scripts PowerShell

> **POURQUOI PASSER PAR « AFFICHER LES FICHIERS »**
>
> Le dossier ouvert porte le GUID de la GPO : le script est stocké avec la stratégie, se réplique avec elle et disparaît avec elle. Un script déposé ailleurs dans le [redacted] fonctionnerait, mais resterait orphelin le jour où la GPO serait supprimée. Déposer le fichier ne suffit pas : seul ce qui est déclaré dans la liste est exécuté, et un `.ps1` placé dans l'onglet « Scripts » classique ne serait pas lancé par PowerShell.

C.5 Validation sur les postes clients

[redacted] — validation de la commande

Le premier essai par GPO n'a rien installé (incident I7). Pour isoler la cause, la commande d'installation a été exécutée à la main en PowerShell administrateur sur [redacted] : elle a abouti, prouvant que la commande et les droits d'accès au MSI étaient corrects. Lors des démarrages suivants, le script de la GPO sort immédiatement grâce au test de présence : l'idempotence est vérifiée sur ce poste.

```
Get-Service glpi-agent
Test-Path "$env:ProgramFiles\GLPI-Agent"
```



Figure 54 — Service glpi-agent en cours d'exécution sur [redacted]



Figure 55 — [redacted] inventorié : Windows 11 Professionnel, fiche créée à 12 h 30

La fiche remontée détaille 27 composants, 144 logiciels, 143 processus et 5 volumes, ainsi que le système d'exploitation, le BIOS et les contrôleurs, sans aucune saisie manuelle. Le fabricant apparaît en `QEMU` et le modèle en `Standard PC (Q35 + ICH9, 2009)`, ce qui est cohérent avec une VM Proxmox ; sur un poste physique, on obtiendrait la marque, le modèle et le numéro de série, précieux pour rapprocher un poste de son contrat de garantie.



Figure 56 — Fiche détaillée de [redacted] : matériel et logiciels inventoriés automatiquement

Côté Windows, l'agent collecte les informations du système (notamment via WMI), construit un inventaire et le transmet en POST au point d'entrée `inventory.php`. C'est le poste qui initie la connexion vers le serveur : aucun flux entrant n'est nécessaire vers les postes pour l'inventaire lui-même.

[redacted] — validation du déploiement par GPO

[redacted] sans agent, a servi à prouver le déploiement automatisé. Le premier `gpupdate /force` a échoué faute de pouvoir joindre le contrôleur de domaine : le poste interrogeait en priorité le DNS IPv6 annoncé par la box (incident I8). Après correction de la carte réseau (IPv6 désactivé, DNS [redacted] seul, passerelle [redacted] la stratégie s'est appliquée et, au redémarrage suivant, l'agent s'est installé seul. [redacted] a remonté son inventaire à 12 h 43, sans aucune intervention sur le poste.



Figure 57 — [redacted] : gpupdate /force terminé sans erreur après correction du réseau



Figure 58 — Les deux postes inventoriés : [redacted] (12 h 30) et [redacted] (12 h 43)

Ces deux captures bouclent la démonstration : un poste installé par la commande validée manuellement, un poste installé par stratégie de groupe, tous deux inventoriés automatiquement.

3. Incidents rencontrés et diagnostics

N°	Incident	Cause identifiée	Correction
I1	Environnement graphique GNOME installé sur le serveur	Tâche « environnement de bureau Debian » restée cochée	`set-default multi-user.target`, purge et `autoremove --purge`
I2	Plus de sortie Internet après désactivation d'IPv6	Passerelle IPv4 erronée (.1 au lieu de .254), masquée tant qu'IPv6 fonctionnait	Passerelle corrigée avec `nmcli`
I3	Téléchargement GLPI en erreur 404	Nom d'archive versionné (`glpi-11.0.8.tgz`) ; `inc/define.php` absent de GLPI 11	URL exacte de l'asset ; version lue autrement
I4	Prérequis bloquant dans l'assistant	Extension `bcmath` exigée par GLPI 11	`apt install php-bcmath`, redémarrage de PHP-FPM
I5	Accès refusé pour [redacted]	Mot de passe saisi incertain (commandes interactives collées en bloc)	`ALTER USER` depuis root MariaDB
I6	Règle d'habilitation trop large	Critère « Annuaire LDAP » au lieu de « (LDAP) MemberOf »	Critère remplacé avant validation
I7	Agent non installé par la GPO	Script dans le mauvais onglet de la GPO, version du MSI erronée, `$` interprété, journal vers un dossier absent	Script corrigé, test direct de la commande
I8	`gpupdate` en échec sur PC-CLIENT-02	DNS IPv6 de la box interrogé avant le DC ; passerelle vide	IPv6 désactivé, DNS .201 seul, passerelle .254
I9	Nom non résolu depuis un poste hors lab	Poste utilisant le DNS de la box (et un VPN actif)	Accès par IP ou entrée dans le fichier `hosts`

I2 — Sortie Internet perdue : la passerelle masquée par IPv6

Symptôme	Juste après la désactivation d'IPv6, l'installation des paquets échoue : aucune connexion vers les dépôts Debian.
Première hypothèse	Résolution renvoyant des adresses IPv6 injoignables : apt forcé en IPv4 (`99force-ipv4`). Le problème persiste : ce n'était pas la cause.
Diagnostic	La résolution IPv4 fonctionne et la route par défaut existe. Le ping vers Internet renvoie `Destination Host Unreachable` émis par **le serveur lui-même** : il ne parvient pas à joindre sa passerelle au niveau 2. La table ARP (`ip neigh show`) montre [redacted] `FAILED` , alors que [redacted] répond avec l'adresse MAC de la box et que le DC, sur le même sous-réseau, répond normalement.
Cause	Passerelle saisie en [redacted] lors de la configuration manuelle, alors que la Bbox est en .254. Tant qu'IPv6 était actif, la sortie Internet passait en IPv6 par la box et masquait l'erreur ; le reste du lab, sur le même sous-réseau, n'a jamais besoin de passerelle.
Correction	`nmcli con mod "Wired connection 1" ipv4.gateway` [redacted] puis vérification : route via .254, ping de la box et de 9.9.9.9. Les autres serveurs Linux du lab ont été contrôlés : leur passerelle était correcte.
Leçon	Un « Host Unreachable » émis par sa propre adresse désigne un problème de voisinage (ARP), pas de routage lointain. Et désactiver une pile réseau peut révéler un défaut que l'autre pile masquait.

I4 — Extension bcmath : quand la documentation est en retard sur la version

Symptôme	L'assistant affiche une ligne rouge et remplace « Continuer » par « Réessayer ».
Cause	GLPI 11 exige l'extension PHP `bcmath` (génération de QR codes), absente de la liste d'extensions reprise des procédures écrites pour GLPI 10.
Correction	`apt install -y php-bcmath` , puis `systemctl restart php8.4-fpm apache2` : l'extension est chargée au démarrage du pool FPM, pas à la volée. Contrôle par `php -m | grep bcmath` .
Leçon	L'écran des prérequis de l'éditeur fait foi sur n'importe quel tutoriel ; un avertissement orange se discute, une ligne rouge se corrige.

I6 — Un critère de règle qui aurait promu tout le domaine

Symptôme	Aucun : l'erreur a été repérée à la relecture de la règle, avant validation.
Cause	Le critère « Critères globaux - Annuaire LDAP » vérifie quel annuaire a authentifié l'utilisateur. Associé à l'action Technician, il aurait promu technicien chaque utilisateur du domaine.
Correction	Remplacement par **(LDAP) MemberOf** contient [redacted]
Leçon	Une règle d'habilitation se relit comme une règle de pare-feu : l'erreur ne produit aucun message, seulement des droits en trop.

I7 — L'agent ne s'installe pas par la GPO

Symptôme	Après `gpupdate /force` et redémarrage de [redacted] `Get-Service glpi-agent` ne trouve aucun service de ce nom.
Diagnostic	Démarche en entonnoir, tracée dans un ticket (annexe C) : `gpresult /r /scope:computer` montre la GPO appliquée, la stratégie n'est donc pas en cause ; `LastBootUpTime` (13 h 38) est postérieur au dépôt du script (13 h 23), le script a donc eu l'occasion de s'exécuter. La vérification de la GPO sur le DC révèle que le script n'est pas déclaré dans l'onglet Scripts PowerShell. Enfin, `Test-Path` sur le chemin du MSI renvoie `False`.
Causes	Quatre défauts cumulés : le script déposé dans le dossier Startup n'était pas déclaré dans l'onglet **Scripts PowerShell** (un `.ps1` placé dans l'onglet Scripts classique n'est pas lancé par PowerShell) ; le nom du MSI codé en dur en 1.16 alors que le fichier déposé est en 1.19 ; les chemins entre guillemets doubles, où PowerShell interprète le `$` de [redacted] ; un journal d'installation dirigé vers un sous-dossier `logs` inexistant.
Correction	Script déclaré dans le bon onglet, version corrigée en 1.19, guillemets simples, journalisation retirée. La commande a été validée seule sur [redacted] avant de retester la GPO sur [redacted]
Leçon	Un script de démarrage échoue sans message : on valide la commande à la main avant de la confier à une GPO, on vérifie ce que la GPO déclare réellement, et on évite de coder une version en dur dans un script de déploiement.



Figure 59 — Version initiale du script : MSI en version 1.16, chemins entre guillemets doubles, journal vers un dossier absent



Figure 60 — Script déposé dans le dossier Startup de la GPO, mais liste des Scripts PowerShell encore vide

I8 — Le DNS IPv6 de la box court-circuite le contrôleur de domaine

Symptôme	Sur [redacted] `gpupdate /force` échoue : Windows ne parvient pas à joindre le contrôleur de domaine.
Diagnostic	`ipconfig /all` liste en premier un serveur DNS IPv6 (la box), puis [redacted]; le suffixe DNS de connexion vaut `lan`. Le poste interroge d'abord un résolveur qui ignore la zone [redacted]
Correction	`Disable-NetAdapterBinding -ComponentID ms_tcpip6`, DNS [redacted] seul, `ipconfig /flushdns`, contrôle par `nltest` [redacted] La passerelle, restée vide, a été renseignée en [redacted] pour rétablir Internet.
Leçon	Même famille que l'incident du serveur GLPI et que le problème NLA déjà documenté : la box annonce IPv6 à tout le réseau. La cause racine est globale et appelle une correction globale (voir section 5), pas un réglage poste par poste.

4. Résultat et bilan

Élément	État	Preuve
VM 108 démarrant avec l'hyperviseur, sauvegardée chaque nuit	**Validé**	A.1, A.3
Debian 13 minimale, IP fixe, résolution directe et inverse	**Validé**	A.2, A.3
Socle LAMP en PHP-FPM, base dédiée en moindre privilège	**Validé**	A.4, A.5
GLPI 11.0.8, DocumentRoot restreint à `public/`	**Validé**	A.6, A.8
Comptes par défaut renommés, installateur supprimé	**Validé**	A.8
Actions automatiques exécutées par le cron système	**Validé**	A.9
Authentification des comptes AD via compte de service	**Validé**	B.3, B.4
Habilitations dynamiques pilotées par groupes AD	**Validé**	B.5, B.6
Agent d'inventaire déployé par GPO, inventaire remonté	**Validé**	C.5
Synchronisation et import LDAP planifiés	**À faire**	Section B.7
HTTPS, pare-feu de la VM, liaison LDAP chiffrée	**À faire**	Section 5

La brique GLPI est opérationnelle de bout en bout : un utilisateur du domaine se connecte avec son mot de passe habituel, ses droits dans l'outil découlent de ses groupes AD, et les postes du domaine s'inventorient seuls dès leur démarrage. Elle relie quatre briques du lab (AD, serveur de fichiers, sauvegarde, virtualisation) et ne demande aucune double saisie : l'annuaire reste l'unique référence pour les identités, et les agents l'unique source pour l'inventaire.

5. Leçons apprises et axes d'amélioration

5.1 Leçons apprises

- **Vérifier chaque valeur saisie à la main** : une passerelle erronée est restée invisible jusqu'à ce qu'une autre pile réseau cesse de la masquer.
- **Les prérequis de l'éditeur priment sur les tutoriels** : GLPI 11 a changé son arborescence, le nom de son archive et ses extensions requises.
- **Tester une commande seule avant de l'automatiser** : la validation manuelle de `msiexec` a isolé en quelques minutes ce que la GPO masquait.
- **Ne pas coller de blocs contenant des saisies interactives** : les invites de mot de passe se superposent et l'on perd la trace de ce qui a été exécuté.
- **Raisonner en cause racine** : l'IPv6 annoncé par la box a touché le serveur GLPI, un poste client et, auparavant, la classification réseau NLA des serveurs Windows.

5.2 Axes d'amélioration

Amélioration	Détail
HTTPS	Certificat issu d'une autorité interne ou auto-signé, redirection du port 80 vers 443. Les identifiants AD transitent aujourd'hui en clair entre le navigateur et GLPI.
Liaison LDAP chiffrée	La liaison utilise LDAP sur le port 389 : le mot de passe du compte de service et ceux des utilisateurs transitent en clair entre GLPI et le DC. Passage en LDAPS (636) avec un certificat sur le contrôleur de domaine.
Pare-feu	Activer le pare-feu Proxmox de la VM 108 avec le groupe de sécurité `admin-lab`, et UFW sur le serveur (HTTP depuis le LAN, SSH depuis l'administration), dans la logique du pare-feu multicouches du lab.
IPv6 de la box	GPO désactivant IPv6 sur les postes du domaine, ou arrêt des annonces de routeur IPv6 sur la box ; suppression de l'enregistrement AAAA du DC dans sa zone.
Synchronisation LDAP	Synchronisation quotidienne des comptes existants et import nocturne des nouveaux comptes via la console GLPI en cron (section B.7) ; fuseau horaire de l'annuaire à aligner sur Europe/Paris.
Accès restreint à GLPI	Groupe [redacted] associé à un filtre de connexion LDAP, pour que seuls ses membres puissent se connecter et que l'accès soit visible dans l'annuaire.
Script de déploiement	Recherche dynamique du MSI (`Get-ChildItem` filtré sur `GLPI-Agent-*-x64.msi`) au lieu d'une version codée en dur ; journal d'installation dans un sous-dossier accessible en écriture aux ordinateurs uniquement ; mise à jour de l'agent quand une nouvelle version est déposée.
Authentification des agents	Activer l'authentification des agents dans la configuration de l'inventaire, pour que seuls des agents légitimes puissent soumettre un inventaire au serveur.

Supervision et sauvegarde	Ajouter [redacted] à Zabbix (services Apache, PHP-FPM, MariaDB, espace disque) et contrôler la présence de la VM 108 dans l'historique du job PBS.
Mises à jour de GLPI	Procédure de mise à jour manuelle à formaliser (sauvegarde de la base et de `files/`, remplacement du code, migration par la console), puisque GLPI ne suit pas `apt`.

Annexe A — Index des figures

Correspondance entre les figures du rapport et les fichiers de captures d'origine. Quatre fichiers n'ont pas été retenus : un doublon exact de l'écran des prérequis (Install_GLPI_VErsion_07), un doublon des autorisations de partage (05_droit_du_dossier…), la liste vide des annuaires LDAP avant création (Annuaire_LDAP_05, écran intermédiaire) et un tableau des comptes par défaut recopié de la session de travail (Install_GLPI_VErsion_11), qui n'est pas un écran de GLPI.

Fig.	Légende	Fichier d'origine
1	Sélection de l'image Debian 13.6 netinst lors de la création de la VM	GLPI__Montage_VM_01.png
2	Récapitulatif de création de la VM 108 [redacted] (onglet Confirmation)	GLPI__Montage_VM_02.png
3	Vue Matériel de la VM 108 avant le premier démarrage	GLPI__Montage_VM_03.png
4	Options de la VM : démarrage à l'amorçage et agent QEMU activés	GLPI__Montage_VM_04.png
5	Premier démarrage sur l'installateur Debian 13, en mode BIOS	GLPI__Montage_VM_05.png
6	Table des partitions avant écriture : racine ext4 et swap, sans LVM	GLPI__Montage_VM_06.png
7	Sélection des logiciels : « environnement de bureau Debian » resté coché, origine de l'incident I1	GLPI__Montage_VM_07.png
8	Contrôles post-installation : espace disque, IP fixe, système sain, resolv.conf corrigé, résolution du DC (IPv6 publiques floutées)	GLPI_Parametrage_VM_01.png (flouté)
9	Création de l'hôte [redacted] (A + PTR) dans la zone [redacted] (IPv6 publiques floutées)	Integration_au_DNS_du_SRV_AD_…_VM_02.png (flouté)
10	Résolutions directe et inverse fonctionnelles depuis le serveur GLPI	Integration_au_DNS_du_SRV_AD_GLPI_Parametrage-Integration_au_DNS_du_SRV_AD_VM_03.png
11	Job de sauvegarde en mode exclusion : [redacted] incluse d'office	GLPI_Integration_de_la_save_du_SRV.png
12	Versions installées depuis les dépôts Debian : PHP 8.4.24, Apache 2.4.68, MariaDB 11.8.6	Install_GLPI_VErsion_01.png
13	Modules et configuration PHP-FPM activés, trois services actifs, Apache répondant en HTTP 200	Install_GLPI_VErsion_02.png
14	Connexion avec [redacted] : base [redacted] accessible, 486 fuseaux horaires chargés	Install_GLPI_VErsion_03.png
15	Version 11.0.8 confirmée par le répertoire version et par la constante GLPI_VERSION du code source	Install_GLPI_VErsion_04.png
16	Syntaxe Apache validée et réponse HTTP 200 avec cookie de session HttpOnly	Install_GLPI_VErsion_05.png
17	Vérification des prérequis : tests requis validés	Install_GLPI_VErsion_06.png
18	Fin de la vérification : tests de sécurité et extensions suggérées (LDAP, OPcache) validés	Install_GLPI_VErsion_08.png
19	Connexion de l'assistant à la base de données (mot de passe masqué)	Install_GLPI_VErsion_09.png
20	Initialisation de la base réussie	Install_GLPI_VErsion_10.png
21	Page de connexion de GLPI après installation : source « Base interne GLPI »	Install_GLPI_VErsion_12.png
22	Liste des utilisateurs après renommage des comptes par défaut	Parametrage_Interface_01_.png
23	Actions automatiques : 48 actions en mode CLI, dernières exécutions le jour même	Parametrage_Interface_02_.png

24	Création de l'OU Comptes de service à la racine du domaine	Annuaire_LDAP_01_-_Creation_OU_Comptes_de_service.png
25	Création du compte [redacted] dans l'OU Comptes de service	Annuaire_LDAP_02_-_Creation_du_Compte_de_service_GLPI.png
26	Le compte [redacted] dans son OU dédiée	Annuaire_LDAP_03_-_Creation_du_Compte_de_service_GLPI.png
27	Nom distinctif (distinguishedName) de [redacted] dans l'OU Comptes de service	Annuaire_LDAP_04_-_distinguishedName_du_compte_de_service.png
28	Paramètres de l'annuaire Active Directory dans GLPI (mot de passe masqué)	Annuaire_LDAP_06_-_liaison_AD_a_GLPI.png
29	Test de la liaison LDAP réussi : cinq étapes validées, 8 utilisateurs trouvés	Annuaire_LDAP_07_-_liaison_LDAP_reussi_.png
30	Les 8 comptes de l'annuaire proposés à l'import, identifiés par leur objectguid	Annuaire_LDAP_08_-_import_utilisateur_de_l_AD.png
31	Utilisateurs GLPI après import : comptes AD aux côtés des comptes locaux	Annuaire_LDAP_09_-_import_utilisateur_de_l_AD.png
32	Connexion de [redacted] avec ses identifiants de domaine, source « AD [redacted] »	Annuaire_LDAP_10-_connexion_a_un_compte_tout_fraichement_importé.png
33	Portail Self-Service ouvert pour [redacted]	Annuaire_LDAP_11-_connexion_a_un_compte_tout_fraichement_importé.png
34	Création d'un groupe global de sécurité dans l'OU Groupes, à côté des groupes AGDLP existants	[redacted]dmin.png
35	Groupes [redacted] et [redacted] dans l'OU Groupes	[redacted]dmin.png
36	Ajout de [redacted] au groupe [redacted]	[redacted]hnciens_pour_tester.png
37	Paramètres de lecture des groupes : recherche dans les utilisateurs, attribut memberof	04_Parametrage_des_groupe_dans_GLPI.png
38	Création de la règle AD - Techniciens GLPI, activée	05_Creation_des_regles_d_attribution_au_groupe.png
39	Critère de la règle : (LDAP) MemberOf contient [redacted]	06_Creation_des_regles_d_attribution_au_groupe.png
40	Actions de la règle : profil Technician et entité racine	07_Creation_des_regles_d_attribution_au_groupe.png
41	Règles d'affectation d'habilitations : les deux règles AD puis la règle native Root	08_Creation_des_regles_d_attribution_au_groupe.png
42	[redacted] avant synchronisation : profil Self-Service (D) uniquement	09_habilitation_d_un_utilisateur_avant_syncro.png
43	Onglet Synchronisation de la fiche utilisateur : « Forcer la synchronisation »	10_habilitation_d_un_utilisateur_forcer_la_syncro.png
44	Après synchronisation : Super-Admin attribué dynamiquement (D), en plus de Self-Service	11_habilitation_d_un_utilisateur_apres_syncro.png
45	Connexion de [redacted] avec la source d'authentification AD [redacted]	[redacted]
46	Sélecteur de profils de [redacted] : Self-Service et Super-Admin	[redacted]en_le_profil_admin.png
47	Configuration de l'inventaire : activation, options d'import, composants inventoriés	01_Activer_l_inventaire_dans_GLPI.png
48	Point d'entrée inventory.php : réponse 405, le service attend des requêtes POST	02_.png

49	Dossier [redacted] créé dans [redacted] sur [redacted]	[redacted] ICHIER_pour_y_deposer_l_agent_MSI_.png
50	Partage avancé [redacted] : Ordinateurs et Utilisateurs du domaine en lecture	[redacted] ER_pour_y_deposer_l_agent_MSI_.png
51	Permissions NTFS : Ordinateurs du domaine en Lecture et exécution	05_onglet_securité_droit_du_dossier_deploiement_sur_SRV_FICHIER_pour_y_deposer_l_agent_MSI_.png
52	Le MSI GLPI-Agent-1.19-x64.msi visible via \\srv-[redacted] depuis [redacted]	06_Test_qu_on_voit_bien_le_glpi_agent_depuis_un_autre_poste_du_domaine.png
53	GPO liée à l'OU Ordinateur et script [redacted] déclaré dans l'onglet Scripts PowerShell	09_Creation_du_script_Agent_GLPI_.png
54	Service glpi-agent en cours d'exécution sur [redacted]	10_GPo_appliqué__.png
55	[redacted] inventorié : Windows 11 Professionnel, fiche créée à 12 h 30	11_PC_bien_remonté_dans_GLPI_.png
56	Fiche détaillée de [redacted] : matériel et logiciels inventoriés automatiquement	12_Composants_du_PC_remonté.png
57	[redacted] : gpupdate /force terminé sans erreur après correction du réseau	13_Gpupdate_sur_un_2eme_poste___redemarrage.png
58	Les deux postes inventoriés : [redacted] (12 h 30) et PC-CLIENT-02 (12 h 43)	13_pc_client_02_bien_remonter_sur_glpi_.png
59	Version initiale du script : MSI en version 1.16, chemins entre guillemets doubles, journal vers un dossier absent	07_Creation_du_script_Agent_GLPI_.png
60	Script déposé dans le dossier Startup de la GPO, mais liste des Scripts PowerShell encore vide	08_Creation_du_script_Agent_GLPI_.png

Annexe B — Questions de jury anticipées

Pourquoi avoir pointé le DocumentRoot sur public/ ?

Parce que c'est l'architecture de GLPI 11 : seul ce répertoire doit être exposé. Les identifiants de la base (`config/`) et les documents joints (`files/`) sont hors de la racine web ; je l'ai prouvé avec un 404 sur `config_db.php` .

Votre compte de service a quels droits ?

Uniquement ceux d'un utilisateur du domaine, qui suffisent pour lire l'annuaire. Son mot de passe est stocké dans une application web : s'il était administrateur, compromettre GLPI reviendrait à compromettre le domaine.

Pourquoi objectguid comme champ de synchronisation ?

C'est un identifiant immuable attribué par l'AD. Le DN change dès qu'on déplace un utilisateur d'OU, ce qui créerait un doublon dans GLPI.

Que se passe-t-il si l'on retire [redacted] du groupe [redacted] ?

Son habilitation Technician est dynamique (marqueur D) : elle disparaît à sa prochaine connexion ou synchronisation, sans aucune action dans GLPI.

Pourquoi une action « Entité » dans vos règles ?

Une habilitation GLPI associe un profil à une entité. Sans entité, la règle n'attribue rien. En multi-sites, c'est ce qui limiterait un technicien à son agence.

Votre liaison LDAP est-elle chiffrée ?

Non, elle utilise le port 389 : c'est une limite assumée du lab, que je traiterais en production par LDAPS avec un certificat sur le contrôleur de domaine. C'est dans mes axes d'amélioration.

Pourquoi un script de démarrage plutôt qu'une GPO d'installation de logiciel ?

La GPO d'installation ne permet pas de passer de paramètres au MSI, et l'agent doit connaître l'adresse du serveur. Le script rend la commande explicite et vérifie la présence de l'agent pour ne pas réinstaller à chaque démarrage.

Pourquoi donner des droits à « Ordinateurs du domaine » sur le partage ?

Le script de démarrage s'exécute sous le compte ordinateur, pas sous celui d'un utilisateur. En lecture seule : un poste qui pourrait écrire dans le partage pourrait y remplacer le MSI.

Pourquoi localhost et pas l'IP du serveur dans la connexion à la base ?

L'utilisateur MariaDB est déclaré pour `localhost` ; une connexion par l'IP serait vue comme venant d'un autre hôte et refusée. La connexion passe aussi par la socket locale.

Comment avez-vous trouvé la panne de passerelle ?

Le « Host Unreachable » venait de ma propre machine : problème de niveau 2. La table ARP montrait .1 en FAILED et .254 joignable avec la MAC de la box. La passerelle était mal saisie, et l'IPv6 masquait l'erreur jusqu'à sa désactivation.

Pourquoi le mode CLI pour les actions automatiques ?

En mode GLPI, les tâches ne tournent que si quelqu'un charge une page ; la nuit et le week-end, rien ne s'exécute. En CLI, c'est le cron système qui les lance chaque minute, sous `www-data` .

Annexe C — Ticket d'incident du déploiement de l'agent

Le dépannage de l'incident I7 a été conduit et consigné comme un ticket d'assistance, sur le modèle de ceux que GLPI permet désormais de gérer dans le lab.

Champ	Contenu
Titre	Agent GLPI non installé après déploiement par GPO
Type / catégorie	Incident — Déploiement logiciel / stratégies de groupe
Élément concerné	[redacted] — GPO « GPO - [redacted] Agent GLPI »
Contexte	Nouvelle GPO créée sur [redacted] pour installer l'agent GLPI au démarrage des postes. `gpupdate /force` puis redémarrage du poste.
Constat	`Get-Service glpi-agent` : aucun service trouvé ; le dossier `GLPI-Agent` est absent de `Program Files`.
Vérification 1	La GPO est-elle appliquée au poste ? `gpresult /r /scope:computer` → **oui**.
Vérification 2	Le poste a-t-il redémarré après l'ajout du script ? `(Get-CimInstance Win32_OperatingSystem).LastBootUpTime` → **oui** (13 h 38, script déposé à 13 h 23).
Vérification 3	Le script référence-t-il le bon MSI ? Premier contrôle visuel jugé correct, mais `Test-Path` sur le chemin exact renvoie `False` : le script cible la version 1.16, le partage contient la 1.19.
Vérification 4	Contrôle de la GPO sur le DC : le script est rattaché à l'onglet **Scripts** et non **Scripts PowerShell**.
Résolution	Script déclaré dans l'onglet Scripts PowerShell ; nom du MSI corrigé ; chemin UNC entre guillemets simples ; journalisation retirée. Commande validée manuellement sur [redacted] puis déploiement automatique confirmé sur [redacted] (inventaire reçu à 12 h 43).
Statut	**Résolu**