PortailSIO

NOUVELLE FORMULE

TUTORIEL

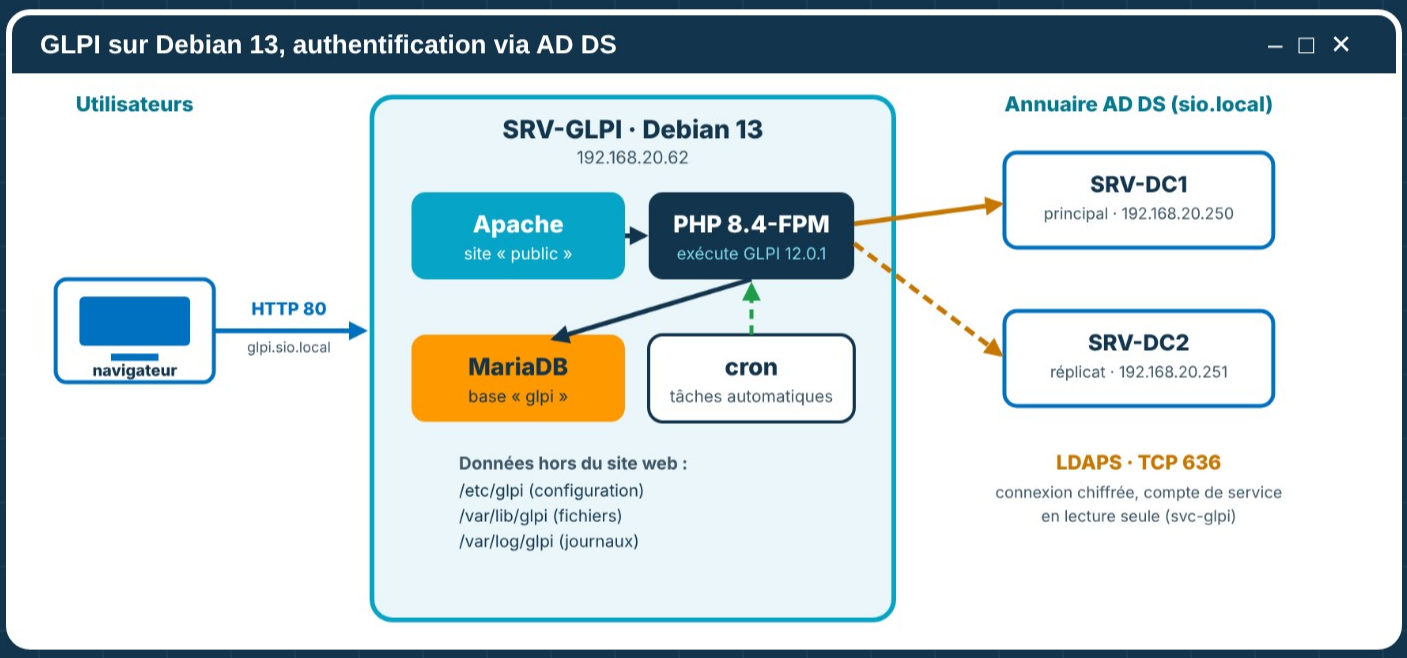
DEBIAN 13 · GLPI 12.0.1

Installer et lier à AD/DS

GLPI



NIVEAU
Intermédiaire



1. Préparer le serveur Debian 13 et le DNS
2. Installer Apache, PHP 8.4 et MariaDB
3. Installer et configurer GLPI 12.0.1
4. Terminer l'installation et sécuriser GLPI
5. Préparer AD DS : compte de service et LDAPS
6. Lier GLPI à l'annuaire et importer les utilisateurs

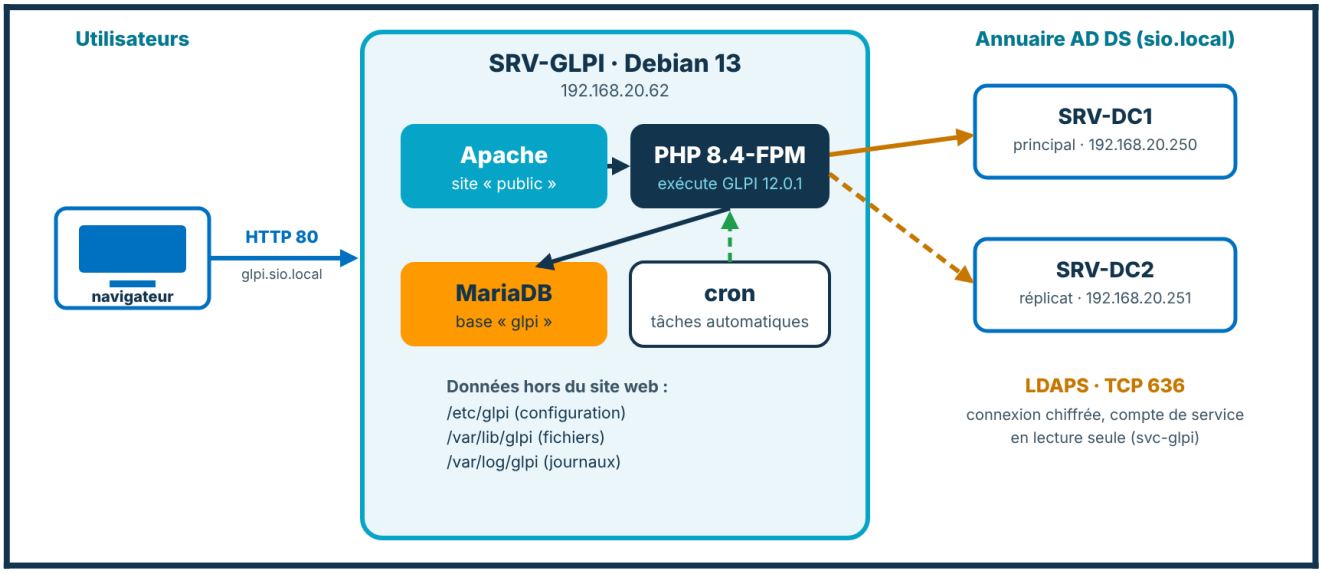
CC BY-NC
Utilisation commerciale interdite
© PortailSIO – 11/2026

Ce tutoriel en ligne
Scannez le QR code. Tous les tutoriels :
portail.sio-ndlp.fr/tutoriels.php

Ce tutoriel a été réalisé avec l'hyperviseur © Proxmox VE. Il peut être réalisé dans un environnement de virtualisation personnel à l'aide des logiciels © VirtualBox ou © VMware Player. Il **suppose que vous disposez d'une machine virtuelle Debian 13** (installation minimale avec serveur SSH) et du domaine **sio.local** construit dans les tutoriels précédents (contrôleurs **SRV-DC1** et **SRV-DC2** sous Windows Server 2025).

GLPI est une solution libre de **gestion de parc informatique** et de **gestion des demandes** (ITSM) : inventaire du matériel et des logiciels, tickets d'assistance, contrats, licences… C'est l'outil de référence des services informatiques et des épreuves du BTS SIO. La version **12.0.1** s'installe sur **PHP 8.3 ou plus** : Debian 13, qui fournit PHP 8.4, convient parfaitement.

Dans ce tutoriel, nous installons GLPI **« en natif »** (Apache, PHP-FPM et MariaDB directement sur Debian 13, sans conteneur), nous le sécurisons, puis nous le **lions à l'annuaire AD DS** pour que les utilisateurs se connectent avec leur compte Windows. Voici les composants et leurs échanges :



Les composants

- **Apache** reçoit les requêtes des navigateurs et ne publie que le sous-dossier `public` de GLPI
- **PHP-FPM** exécute le code de GLPI (une application web écrite en PHP)
- **MariaDB** stocke toutes les données : matériel, tickets, utilisateurs, configuration
- **cron** déclenche chaque minute les tâches automatiques (notifications, nettoyages, inventaire…)
- **AD DS** (SRV-DC1 et son réplicat SRV-DC2) authentifie les utilisateurs par une connexion **chiffrée LDAPS**, à l'aide d'un compte de service en lecture seule

Dans le cadre de ce tutoriel, nous utilisons les machines suivantes (VLAN SERVEURS, réseau 192.168.20.0 /24) :

Machine	Rôle	Système	Adresse IP
SRV-GLPI	Serveur GLPI (nom `srv-glpi`, alias DNS `glpi.sio.local`)	Debian 13	192.168.20.62
SRV-DC1	Contrôleur de domaine, DNS, annuaire principal	Windows Server 2025	192.168.20.250
SRV-DC2	Contrôleur de domaine, DNS, annuaire de secours	Windows Server 2025	192.168.20.251
Poste admin	Navigateur web pour utiliser GLPI (DNS = les deux contrôleurs)	Windows 11	DHCP

Pour **SRV-GLPI**, prévoyez au minimum **2 vCPU, 4 Go de mémoire et 30 Go de disque**. Ces valeurs, comme les adresses et les mots de passe d'exemple, sont à adapter à votre environnement. Les commandes Debian sont exécutées avec un compte autorisé à utiliser `sudo` (ou directement en `root`, sans le préfixe `sudo`) ; les commandes Windows, dans **PowerShell** ouvert **en tant qu'administrateur** sur **SRV-DC1**.

ÉTAPE 1 SUR 6

01 Préparer le serveur Debian 13 et le DNS

Avant d'installer GLPI, on prépare le système (mises à jour, nom, adresse fixe, heure) et on déclare le nom **glpi.sio.local** dans le DNS du domaine. Sur **SRV-GLPI** :

1. Mettez le système à jour : `sudo apt update && sudo apt full-upgrade -y`
2. Donnez son nom au serveur et déclarez-le dans le fichier `hosts` (nom complet et nom court) :

TERMINAL

```
sudo hostnamectl set-hostname srv-glpi
echo "192.168.20.62  glpi.sio.local  srv-glpi" | sudo tee -a /etc/hosts
```

3. Réglez le fuseau horaire : `sudo timedatectl set-timezone Europe/Paris`
4. Donnez au serveur une **adresse IP fixe** (adaptez le nom de la carte, ici `ens18`, avec `ip -br address`) : éditez `/etc/network/interfaces` puis redémarrez le réseau avec `sudo systemctl restart networking` :

/etc/network/interfaces

```
auto ens18
iface ens18 inet static
    address 192.168.20.62/24
    gateway 192.168.20.254
```

5. Indiquez les **DNS du domaine** dans `/etc/resolv.conf` (`sudo nano /etc/resolv.conf`) : le serveur doit retrouver `srv-dc1.sio.local` et `srv-dc2.sio.local` :

/etc/resolv.conf

```
search sio.local
nameserver 192.168.20.250
nameserver 192.168.20.251
```

6. Sur **SRV-DC1**, déclarez l'alias DNS de GLPI (l'enregistrement est répliqué sur SRV-DC2 avec la zone) :

POWERSHELL

```
Add-DnsServerResourceRecordA -Name "glpi" -ZoneName "sio.local" `
    -IPv4Address "192.168.20.62"
```

7 Vérifiez le résultat : nom, adresse IP, résolution DNS des contrôleurs et de GLPI, heure :

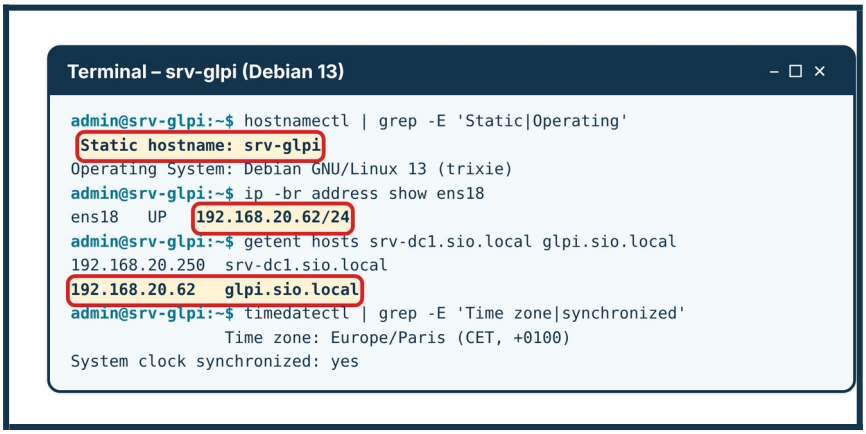


Figure 1 – Contrôle de la préparation du serveur

À SAVOIR

Si « System clock synchronized » indique « no », installez un service de temps (`sudo apt install -y chrony`). L'heure doit être juste : le certificat LDAPS de l'étape 5 a des dates de validité.

✔ POINT DE CONTRÔLE

- `hostnamectl` affiche le nom **srv-glpi** et Debian GNU/Linux **13**
- L'adresse IP **192.168.20.62** est fixe
- `getent hosts srv-dc1.sio.local glpi.sio.local` renvoie les deux adresses
- Le fuseau horaire est **Europe/Paris** et l'horloge est **synchronisée**

02 ÉTAPE 2 SUR 6 — Installer Apache, PHP 8.4 et MariaDB

A – Installer Apache et PHP-FPM avec les extensions de GLPI

GLPI s'appuie sur plusieurs **extensions PHP** (base de données, images, LDAP, chiffrement…). Elles s'installent en une seule commande ; Apache est ici associé à **PHP-FPM**, un service PHP séparé plus rapide et mieux isolé que le module classique :

TERMINAL

```
sudo apt install -y apache2 php8.4-fpm php8.4-cli php8.4-mysql php8.4-curl \
    php8.4-gd php8.4-intl php8.4-mbstring php8.4-xml php8.4-zip php8.4-bz2 \
    php8.4-ldap php8.4-opcache php8.4-bcmath
```

Extension / paquet	Utilité pour GLPI
php8.4-mysql	Connexion à MariaDB (extension `mysqli`)
php8.4-curl, php8.4-xml	Appels web (marketplace, inventaire) et lecture de fichiers XML
php8.4-gd, php8.4-intl, php8.4-mbstring	Images, gestion des langues, caractères accentués
php8.4-ldap	Connexion à l'annuaire AD DS (étape 6)
php8.4-zip, php8.4-bz2, php8.4-opcache, php8.4-bcmath	Archives, accélération du code PHP, calculs

1 Vérifiez la version de PHP, puis que **toutes** les extensions utiles sont chargées. Si une extension manque, la commande l'affiche (aucun message = tout est présent) :

TERMINAL
```
php -v | head -1
EXT="curl fileinfo gd intl mysqli mbstring SimpleXML dom ctype iconv openssl"
EXT="$EXT bz2 exif ldap zip bcmath opcache"
for e in $EXT; do php -m | grep -qiw "$e" || echo "MANQUE : $e"; done
```

B – Régler PHP pour GLPI

GLPI contrôle la configuration de PHP à l'installation. On crée un petit fichier de réglages qui sécurise les cookies de session et fixe des limites confortables (documents joints jusqu'à 20 Mo) :

1 Créez le fichier avec `sudo nano /etc/php/8.4/fpm/conf.d/90-glpi.ini` et saisissez :

/etc/php/8.4/fpm/conf.d/90-glpi.ini
```
session.cookie_httponly = On
session.cookie_samesite = Lax
memory_limit = 256M
upload_max_filesize = 20M
post_max_size = 20M
max_execution_time = 60
```

2 Redémarrez PHP-FPM puis contrôlez la prise en compte et l'état des services :

TERMINAL
```
sudo systemctl restart php8.4-fpm
sudo php-fpm8.4 -i | grep -E 'session.cookie_(httponly|samesite)'
systemctl is-active php8.4-fpm apache2
```

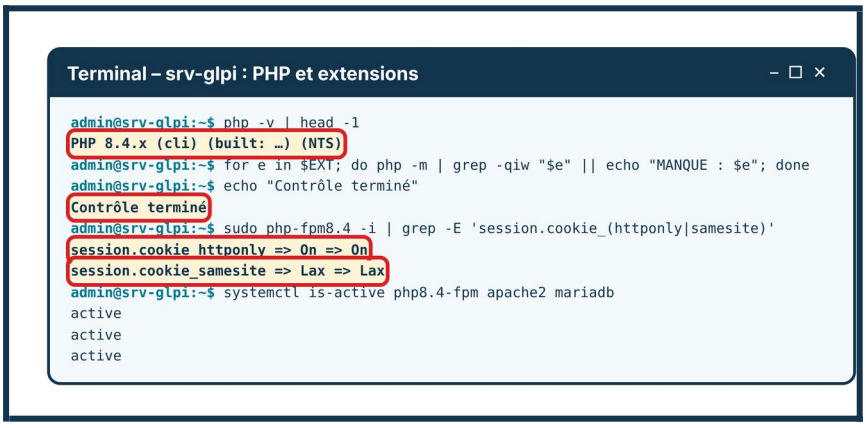


Figure 2 – PHP 8.4, extensions et réglages de session

À SAVOIR

`session.cookie_httponly` interdit aux scripts du navigateur de lire le cookie de session, `samesite` limite son envoi à votre site. Ajoutez `session.cookie_secure = On` uniquement quand GLPI sera servi en HTTPS : avec HTTP simple, la connexion deviendrait impossible.

C – Installer MariaDB et créer la base

Debian 13 fournit **MariaDB 11.8**, que GLPI 12 prend en charge. Installez-la, sécurisez-la, puis créez la base **glpi** et son utilisateur :

1 Installez MariaDB : `sudo apt install -y mariadb-server` (le service démarre automatiquement)

2. Lancez `sudo mariadb-secure-installation` et répondez : **Entrée** (pas de mot de passe root actuel), `n` (authentification par socket déjà active), `n` (pas de mot de passe root), puis `Y` aux quatre dernières questions (comptes anonymes, root à distance, base de test, rechargement des privilèges)
3. Chargez les **fuseaux horaires** dans MariaDB (GLPI les utilise pour afficher les dates dans le bon fuseau) :

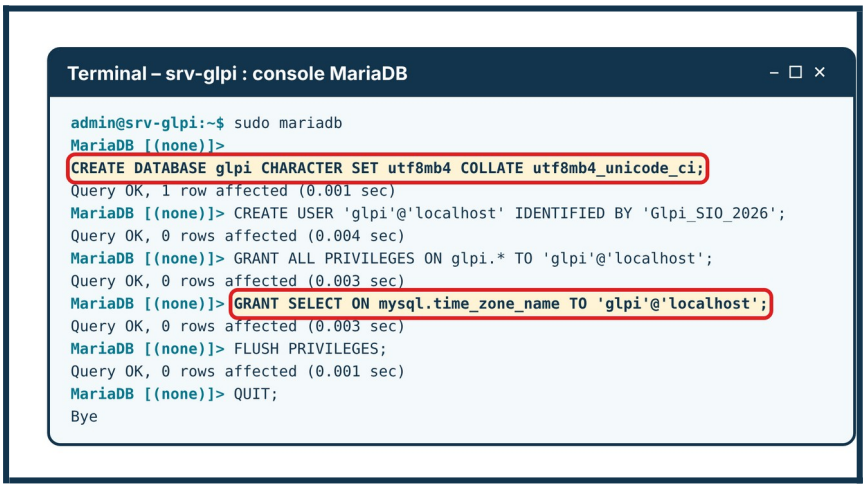
TERMINAL

```
mariadb-tzinfo-to-sql /usr/share/zoneinfo | sudo mariadb mysql
```

4. Ouvrez la console avec `sudo mariadb` puis créez la base, l'utilisateur et ses droits :

CONSOLE MARIADB

```
CREATE DATABASE glpi CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
CREATE USER 'glpi'@'localhost' IDENTIFIED BY 'Glpi_SIO_2026';
GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@'localhost';
GRANT SELECT ON mysql.time_zone_name TO 'glpi'@'localhost';
FLUSH PRIVILEGES;
QUIT;
```



À SAVOIR

Le jeu de caractères utf8mb4 gère tous les caractères (accents, symboles, emoji). Le droit en lecture sur `mysql.time_zone_name` permet à GLPI de vérifier que les fuseaux sont chargés.

Figure 3 – Console MariaDB : création de la base et de l'utilisateur

REMARQUE IMPORTANTE

`Glpi_SIO_2026` n'est qu'un exemple : **choisissez un mot de passe solide** pour l'utilisateur **glpi** de la base. Vous le saisirez une seule fois, dans l'assistant d'installation (étape 4) ; GLPI le range ensuite dans `/etc/glpi/config_db.php`, lisible uniquement par `www-data`.

✔ **POINT DE CONTRÔLE**

- `sudo mariadb -e "SHOW DATABASES;"` liste la base **glpi**
- `php -v` indique **PHP 8.4** et le contrôle des extensions n'affiche aucun « MANQUE »
- `systemctl is-active php8.4-fpm apache2 mariadb` répond **active** trois fois

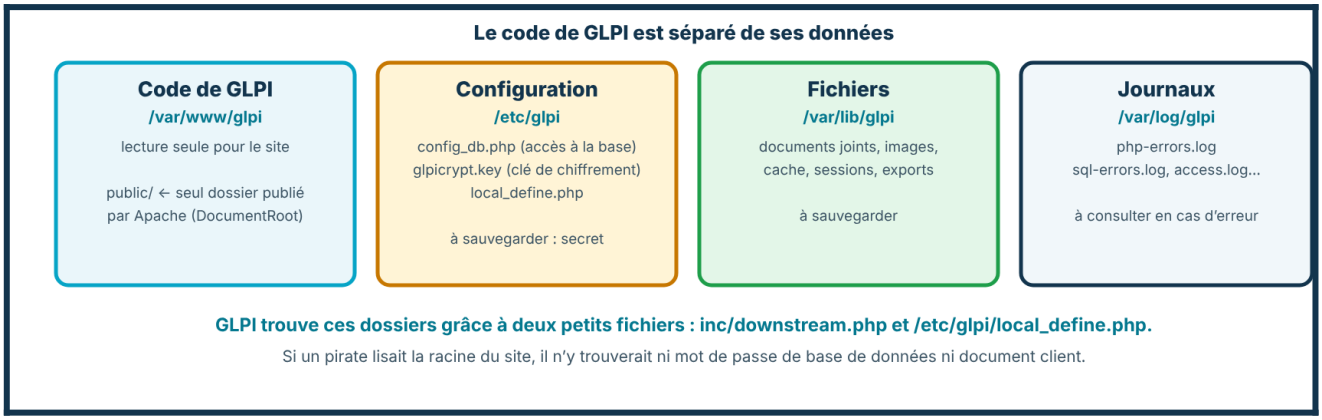
03 ÉTAPE 3 SUR 6
Installer et configurer GLPI 12.0.1

A – Télécharger et décompresser GLPI

1 Téléchargez l'archive officielle de la version **12.0.1** (dépôt GitHub du projet) et décompressez-la dans `/var/www` :

TERMINAL
```
cd /tmp
wget https://github.com/glpi-project/glpi/releases/download/12.0.1/glpi-12.0.1.tgz
sudo tar -xzf glpi-12.0.1.tgz -C /var/www/
```

Le dossier **/var/www/glpi** contient maintenant le programme. Par défaut, ce dossier contient aussi la **configuration**, les **fichiers déposés** par les utilisateurs et les **journaux** : c'est pratique pour un essai, mais déconseillé en production. On sépare donc le code des données :



B – Séparer le code, la configuration et les données

1 Déplacez la configuration et les fichiers hors du site web, et créez le dossier des journaux :

TERMINAL
```
sudo mv /var/www/glpi/config /etc/glpi
sudo mv /var/www/glpi/files /var/lib/glpi
sudo mkdir /var/log/glpi
```

2 Indiquez à GLPI où se trouve sa configuration : créez `sudo nano /var/www/glpi/inc/downstream.php` :

/var/www/glpi/inc/downstream.php
```
<?php
define('GLPI_CONFIG_DIR', '/etc/glpi/');
if (file_exists(GLPI_CONFIG_DIR . '/local_define.php')) {
    require_once GLPI_CONFIG_DIR . '/local_define.php';
}
```

3 Puis, dans `sudo nano /etc/glpi/local_define.php`, indiquez l'emplacement des fichiers et des journaux :

/etc/glpi/local_define.php

```
<?php
define('GLPI_VAR_DIR', '/var/lib/glpi');
define('GLPI_LOG_DIR', '/var/log/glpi');
```

4 Appliquez les droits : le code appartient à **root** (le site ne peut pas se modifier lui-même), les données et la configuration à **www-data**, l'utilisateur d'Apache et de PHP-FPM :

TERMINAL

```
sudo chown -R root:root /var/www/glpi
sudo find /var/www/glpi -type d -exec chmod 755 {} +
sudo find /var/www/glpi -type f -exec chmod 644 {} +
sudo chown -R www-data:www-data /etc/glpi /var/lib/glpi /var/log/glpi
sudo chown -R www-data:www-data /var/www/glpi/marketplace
```

REMARQUE IMPORTANTE

Le dossier `marketplace` reste inscriptible : c'est là que GLPI installe ses **extensions** (plugins). Les sauvegardes doivent désormais couvrir **trois** emplacements : la base de données, `/etc/glpi` (qui contient la clé de chiffrement `glpicrypt.key`, sans elle les mots de passe stockés deviennent illisibles) et `/var/lib/glpi`.

C – Publier GLPI avec Apache

Apache doit publier **uniquement** le dossier `public` de GLPI et confier les pages PHP à PHP-FPM. Créez `sudo nano /etc/apache2/sites-available/glpi.conf` :

/etc/apache2/sites-available/glpi.conf

```
<VirtualHost *:80>
    ServerName glpi.sio.local
    DocumentRoot /var/www/glpi/public
    <Directory /var/www/glpi/public>
        Require all granted
        RewriteEngine On
        RewriteCond %{HTTP:Authorization} ^(.+)$
        RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]
    </Directory>
    <FilesMatch \.php$>
        SetHandler "proxy:unix:/run/php/php8.4-fpm.sock|fcgi://localhost/"
    </FilesMatch>
    ErrorLog ${APACHE_LOG_DIR}/glpi-error.log
</VirtualHost>
```

1 Activez les modules nécessaires, remplacez le site par défaut par celui de GLPI, vérifiez la syntaxe et rechargez Apache :

TERMINAL

```
sudo a2enmod rewrite proxy_fcgi setenvif
sudo a2dissite 000-default
sudo a2ensite glpi
sudo apachectl configtest
sudo systemctl reload apache2
```

D – Programmer les tâches automatiques

GLPI a besoin d'exécuter régulièrement des tâches (envoi des notifications, nettoyage, collecte des e-mails…). On les confie au planificateur du système plutôt qu'aux visites des utilisateurs. Créez `sudo nano /etc/cron.d/glpi` :

/etc/cron.d/glpi

```
* * * * * www-data /usr/bin/php /var/www/glpi/front/cron.php >/dev/null 2>&1
```

1 Contrôlez le tout (dossiers, syntaxe Apache, fichier cron) :

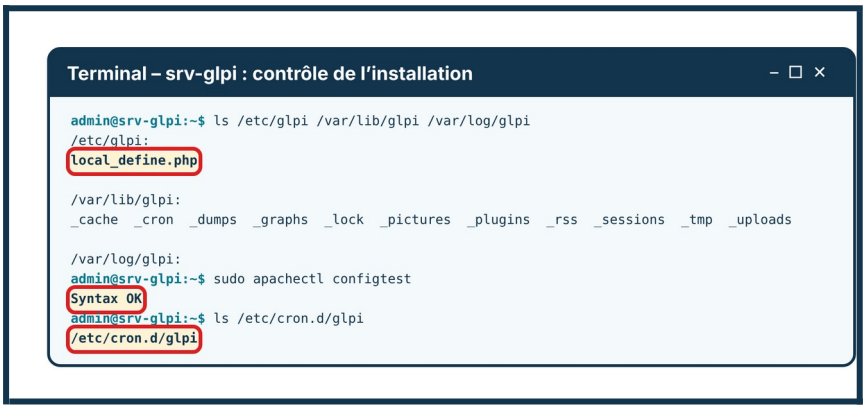


Figure 4 – Contrôle des dossiers déplacés, d'Apache et du cron

À SAVOIR

Le dossier `/var/log/glpi` est vide pour l'instant : GLPI y écrira ses journaux. La liste de `/var/lib/glpi` peut différer légèrement selon la version.

✔ **POINT DE CONTRÔLE**

- `/etc/glpi/local_define.php` existe et `/var/lib/glpi` contient les dossiers `_cache`, `_sessions`…
- `sudo apachectl configtest` affiche **Syntax OK**
- Le site par défaut d'Apache est désactivé et **glpi** est activé (`ls /etc/apache2/sites-enabled`)
- Le fichier `/etc/cron.d/glpi` existe

04 ÉTAPE 4 SUR 6 Terminer l'installation et sécuriser GLPI

A – Dérouler l'assistant d'installation

Depuis le **poste d'administration**, ouvrez un navigateur et saisissez `http://glpi.sio.local`. L'assistant d'installation se lance :

1 Choisissez la langue « **Français** » puis cliquez « **OK** » ; acceptez la licence en cliquant « **Continuer** » :



Figure 5 – Assistant GLPI : choix de la langue

À SAVOIR

Si vous voyez la page « Apache2 Debian Default Page », le site par défaut est resté actif : relisez l'étape 3-C.

2 Cliquez « **Installer** » (et non « Mettre à jour », réservé aux montées de version) :



Figure 6 – Assistant GLPI : début de l'installation

3 L'assistant vérifie l'environnement. Toutes les lignes « **Requis** » doivent être vertes ; les lignes « Suggéré » le sont aussi si vous avez suivi l'étape 2. Cliquez « **Continuer** » :



À SAVOIR

Une ligne rouge indique l'élément à corriger (extension PHP manquante, droit d'écriture refusé sur un dossier). Corrigez-le puis rechargez la page.

Figure 7 – Assistant GLPI : vérification de la compatibilité

4 Étape 1 : saisissez le serveur SQL **localhost**, l'utilisateur **glpi** et le mot de passe choisi à l'étape 2, puis cliquez « **Continuer** » :



Figure 8 – Assistant GLPI : connexion à la base

5 Étape 2 : sélectionnez la base existante **glpi** puis cliquez « **Continuer** ». L'étape 3 crée alors les tables (une minute environ) ; cliquez « **Continuer** » à chaque fin d'étape, y compris à l'écran « Une dernière chose avant de démarrer » (collecte de statistiques facultative, à votre convenance) :



Figure 9 – Assistant GLPI : choix de la base de données

6 L'installation est terminée. L'écran rappelle les **quatre comptes par défaut** (mot de passe identique à l'identifiant). Cliquez « **Utiliser GLPI** » puis connectez-vous avec **glpi** / **glpi** :

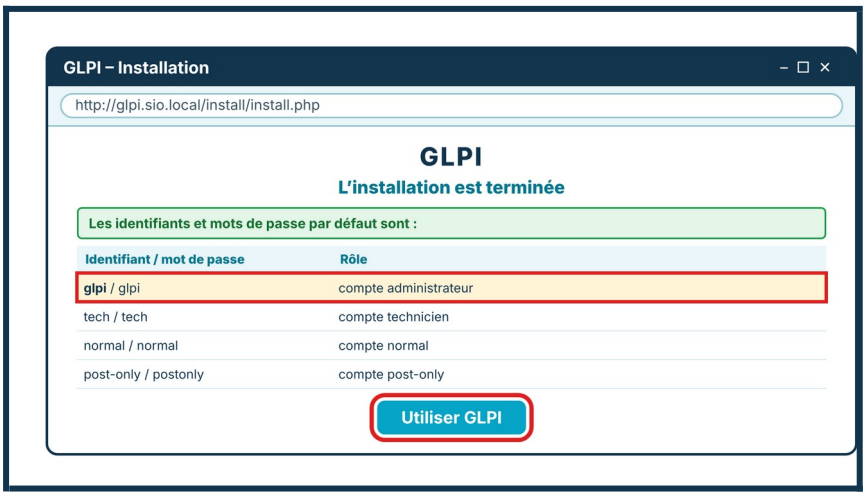


Figure 10 – Assistant GLPI : installation terminée

À SAVOIR

Ces comptes et mots de passe sont publics : le prochain point les neutralise.

B – Sécuriser immédiatement

Dès la connexion, GLPI affiche des **alertes de sécurité** en rouge. Ce sont deux vraies failles à corriger tout de suite :

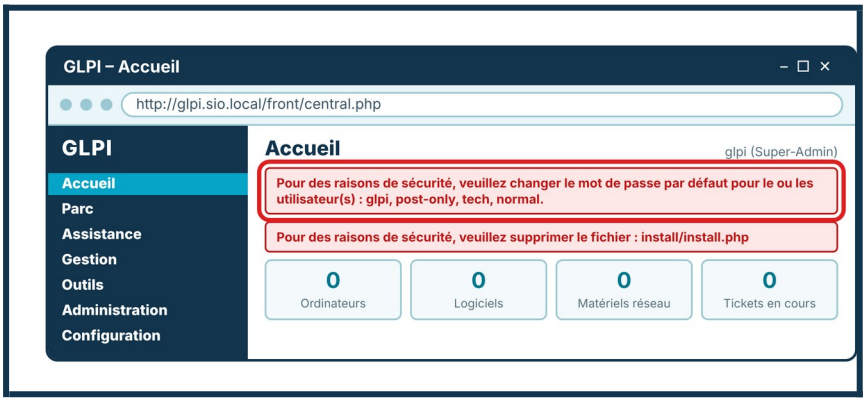


Figure 11 – Page d'accueil : alertes de sécurité

À SAVOIR

Les alertes disparaissent d'elles-mêmes une fois les deux corrections effectuées (rechargez la page).

1 **Mot de passe de glpi** : menu « **Administration** » puis « **Utilisateurs** », cliquez **glpi**, saisissez un mot de passe solide (deux fois) et enregistrez

2 **Autres comptes par défaut** (`tech`, `normal`, `post-only`) : cochez-les dans la liste des utilisateurs puis, dans le menu « **Actions** », supprimez-les ; à défaut, changez leur mot de passe

3 **Fichier d'installation** : supprimez-le, il permettrait de relancer l'assistant :

TERMINAL

```
sudo rm /var/www/glpi/install/install.php
```

C – Passer les tâches automatiques en mode CLI

Par défaut, GLPI exécute ses tâches lorsque quelqu'un navigue sur le site. Comme le planificateur du système (étape 3-D) s'en charge, on le déclare à GLPI : menu « **Configuration** » puis « **Actions automatiques** » :

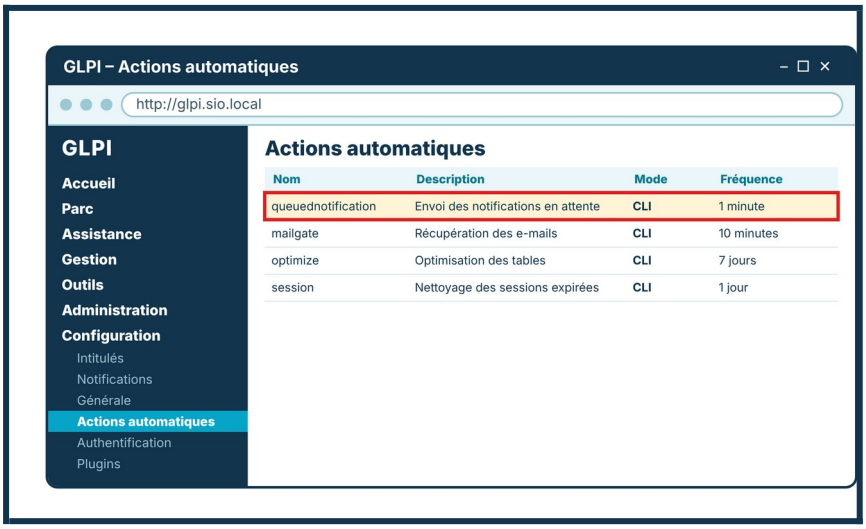


Figure 12 – Configuration > Actions automatiques

À SAVOIR

Ouvrez chaque action concernée (au minimum `queuednotification` et `mailgate`) et réglez son **mode d'exécution** sur « CLI » avant d'enregistrer. Vous pouvez aussi cocher toutes les lignes et utiliser le menu « Actions » de la liste, s'il propose cette modification en masse.

1 Après une minute, contrôlez que les tâches s'exécutent : la colonne « Dernière exécution » de la liste se renseigne, ou lancez la tâche à la main :

TERMINAL

```
sudo -u www-data php /var/www/glpi/front/cron.php
```

À SAVOIR

En production, publiez GLPI en **HTTPS** (certificat délivré par l'autorité de certification de l'entreprise) : les identifiants des utilisateurs ne doivent pas circuler en clair sur le réseau. Dans ce tutoriel, le site reste en HTTP pour se concentrer sur l'installation et sur l'annuaire.

✔ POINT DE CONTRÔLE

- L'assistant s'est terminé sur « **Utiliser GLPI** » et la connexion fonctionne
- Le mot de passe de **glpi** est changé et les comptes `tech`, `normal` et `post-only` sont supprimés
- Le fichier `install/install.php` est supprimé et les alertes rouges ont disparu
- Le mode d'exécution des **actions automatiques** est **CLI**

05 ÉTAPE 5 SUR 6
Préparer AD DS : compte de service et LDAPS

Pour authentifier les utilisateurs, GLPI interroge l'annuaire avec un **compte de service** (lecture seule), puis vérifie le mot de passe de chaque utilisateur. Cette étape se déroule sur les **contrôleurs de domaine** et sur **SRV-GLPI**.

REMARQUE IMPORTANTE

Windows Server 2025 impose la signature LDAP : les connexions LDAP simples (port 389, sans chiffrement) avec identifiant et mot de passe sont **refusées par défaut** sur un domaine neuf. GLPI doit donc utiliser **LDAPS** (LDAP chiffré, port **636**). Il faut pour cela un **certificat** sur chaque contrôleur et la **confiance** de Debian envers ce certificat.

A – Créer l'unité d'organisation, le compte de service et deux utilisateurs de test

Sur **SRV-DC1**, dans PowerShell (**administrateur**), créez les unités d'organisation (OU), le compte **svc-glpi** et deux utilisateurs pour les tests. Si votre domaine possède déjà une OU pour vos utilisateurs, utilisez-la à la place de « Utilisateurs » (ce sera la **BaseDN** de GLPI) :

POWERSHELL
```
$base = "DC=sio,DC=local"
New-ADOrganizationalUnit -Name "Comptes de service" -Path $base
New-ADOrganizationalUnit -Name "Utilisateurs" -Path $base
$mdp = Read-Host -AsSecureString "Mot de passe de svc-glpi"
New-ADUser -Name "svc-glpi" -SamAccountName "svc-glpi" `
    -UserPrincipalName "svc-glpi@sio.local" `
    -Path "OU=Comptes de service,$base" -AccountPassword $mdp `
    -Enabled $true -PasswordNeverExpires $true -CannotChangePassword $true
```

POWERSHELL
```
$mdp = Read-Host -AsSecureString "Mot de passe des utilisateurs de test"
New-ADUser -Name "Alice Martin" -GivenName Alice -Surname Martin `
    -SamAccountName amartin -UserPrincipalName amartin@sio.local `
    -EmailAddress amartin@sio.local -Path "OU=Utilisateurs,$base" `
    -AccountPassword $mdp -Enabled $true
New-ADUser -Name "Bruno Durand" -GivenName Bruno -Surname Durand `
    -SamAccountName bdurand -UserPrincipalName bdurand@sio.local `
    -EmailAddress bdurand@sio.local -Path "OU=Utilisateurs,$base" `
    -AccountPassword $mdp -Enabled $true
```

1 Contrôlez la création :

POWERSHELL
```
Get-ADUser svc-glpi | Select Name, Enabled, DistinguishedName
$ou = "OU=Utilisateurs,$base"
Get-ADUser -Filter * -SearchBase $ou | Select Name, SamAccountName
```

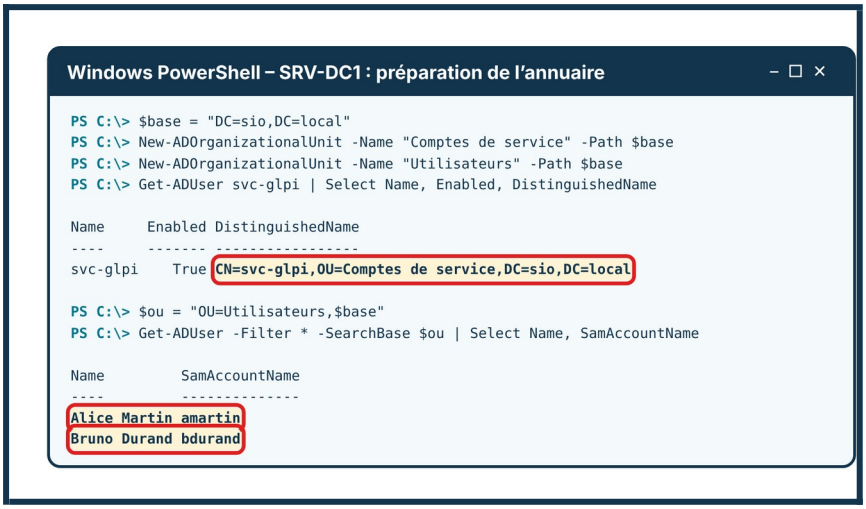


Figure 13 – PowerShell : OU, compte de service et utilisateurs

À SAVOIR

Le compte **svc-glpi** est un compte de domaine ordinaire : il peut lire l'annuaire, rien d'autre. Ne l'ajoutez à aucun groupe d'administration. Son mot de passe n'expire pas, sinon GLPI cesserait de fonctionner le jour de l'expiration.

B – Créer un certificat LDAPS sur chaque contrôleur

Un contrôleur de domaine active LDAPS dès qu'il trouve, dans le magasin « Ordinateur local > Personnel », un certificat pour son **nom complet** et utilisable pour l'authentification de serveur. En **production**, on le fait délivrer par l'autorité de certification de l'entreprise (AD CS). Pour le **laboratoire**, un certificat auto-signé suffit. Sur **SRV-DC1**, puis sur **SRV-DC2** (en changeant le nom) :

```powershell
# SRV-DC2 : remplacer par srv-dc2.sio.local
$fqdn = "srv-dc1.sio.local"
$cert = New-SelfSignedCertificate -Subject "CN=$fqdn" -DnsName $fqdn `
    -CertStoreLocation Cert:\LocalMachine\My -KeyAlgorithm RSA `
    -KeyLength 2048 -HashAlgorithm SHA256 -NotAfter (Get-Date).AddYears(2)
New-Item -ItemType Directory -Path C:\Temp -Force | Out-Null
# SRV-DC2 : srv-dc2.cer
Export-Certificate -Cert $cert -FilePath C:\Temp\srv-dc1.cer
```

1. Patientez quelques minutes (le contrôleur détecte le certificat tout seul ; au besoin, redémarrez-le), puis contrôlez que le port **636** répond :

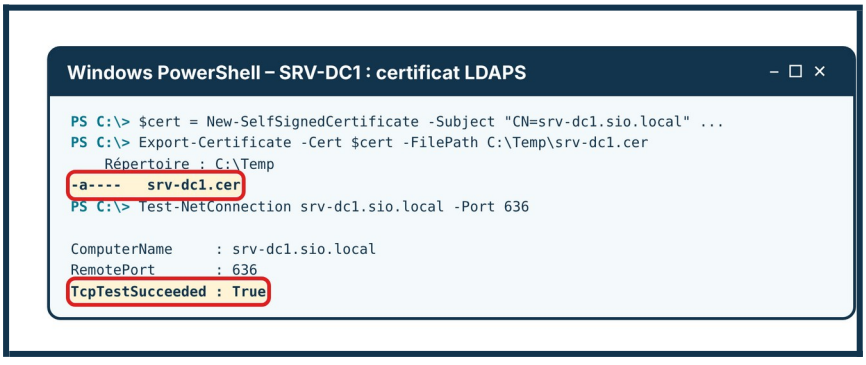


Figure 14 – PowerShell : certificat exporté et port LDAPS

À SAVOIR

Ce test prouve seulement que le port est ouvert. La vérification du certificat lui-même se fait depuis Debian (point suivant).

REMARQUE IMPORTANTE

Un certificat auto-signé de **deux ans** expire un jour : notez la date et renouvelez-le avant, sinon GLPI ne pourra plus joindre l'annuaire (message « Can't contact LDAP server »). Avec AD CS, le renouvellement est automatique.

C – Faire confiance au certificat sur SRV-GLPI

Debian ne connaît pas votre certificat auto-signé et refuserait la connexion. On l'ajoute à ses **autorités de confiance**. Depuis PowerShell, copiez les deux fichiers vers **SRV-GLPI** (ou utilisez WinSCP, ou un partage) :

POWERSHELL (SRV-DC1 ET SRV-DC2)

```
scp C:\Temp\srv-dc1.cer admin@192.168.20.62:/tmp/
scp C:\Temp\srv-dc2.cer admin@192.168.20.62:/tmp/
```

Sur **SRV-GLPI**, convertissez les certificats au format attendu (PEM), déclarez-les comme autorités de confiance et redémarrez PHP-FPM pour qu'il en tienne compte :

TERMINAL

```
cd /tmp
openssl x509 -inform der -in srv-dc1.cer -out srv-dc1.crt
openssl x509 -inform der -in srv-dc2.cer -out srv-dc2.crt
sudo cp srv-dc1.crt srv-dc2.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates
sudo systemctl restart php8.4-fpm
```

1. Installez l'outil de test LDAP et vérifiez la chaîne complète : certificat accepté, puis recherche de l'utilisateur **amartin** avec le compte de service (le mot de passe de **svc-glpi** est demandé) :

TERMINAL

```
sudo apt install -y ldap-utils
openssl s_client -connect srv-dc1.sio.local:636 -verify_return_error \
    </dev/null 2>&1 | grep -E 'subject=|Verify return code'
ldapsearch -H ldaps://srv-dc1.sio.local -D "svc-glpi@sio.local" -W \
    -b "OU=Utilisateurs,DC=sio,DC=local" "(sAMAccountName=amartin)" dn mail
```

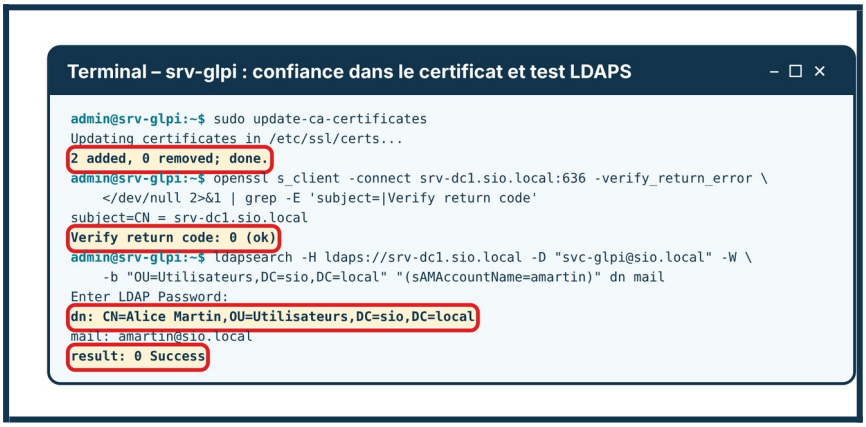


Figure 15 – Debian : confiance dans le certificat et recherche LDAPS

À SAVOIR

« Verify return code: 0 (ok) » prouve que Debian fait confiance au certificat. « result: 0 Success » et la ligne `dn:` prouvent que le compte de service, la BaseDN et LDAPS fonctionnent. Répétez les deux commandes avec `srv-dc2.sio.local`.

✔ **POINT DE CONTRÔLE**

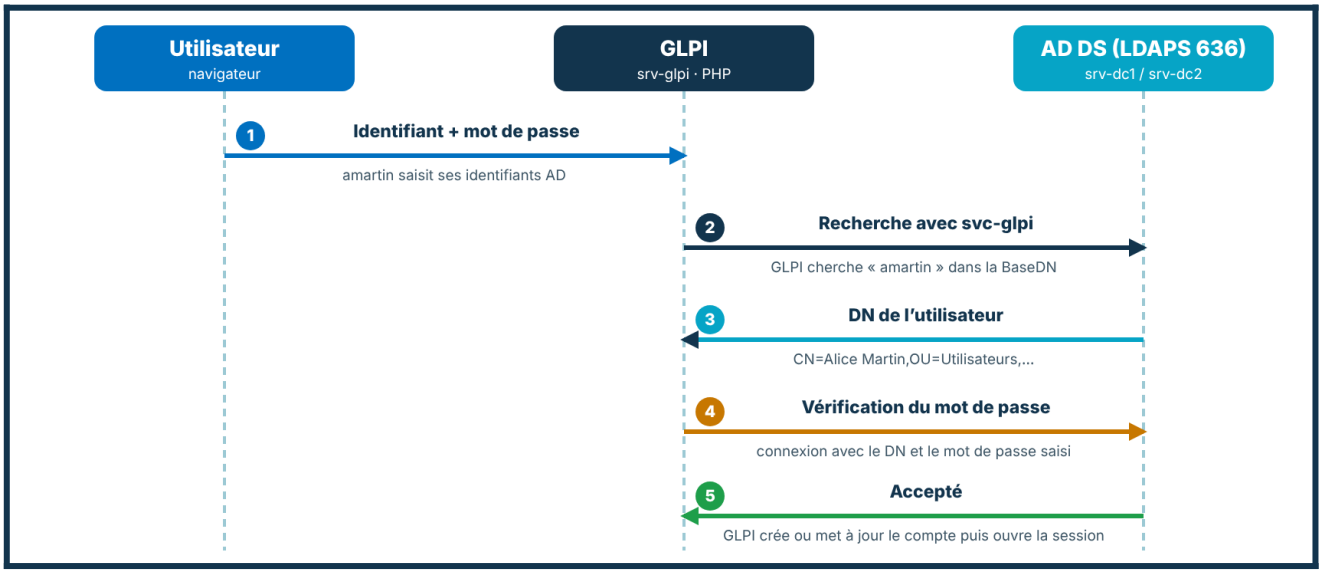
- Les OU **Utilisateurs** et **Comptes de service**, le compte **svc-glpi** et les utilisateurs **amartin** et **bdurand** existent
- Chaque contrôleur présente un certificat à son nom : « Verify return code: **0 (ok)** » pour `srv-dc1` et `srv-dc2`
- `ldapsearch` en **ldaps://** renvoie l'entrée de **Alice Martin** (« result: 0 Success »)

06

ÉTAPE 6 SUR 6

Lier GLPI à l'annuaire et importer les utilisateurs

Tout est prêt : on déclare l'annuaire dans GLPI, on teste, puis on importe les utilisateurs. Voici ce qui se passe quand un utilisateur de l'annuaire se connecte :



A – Déclarer l'annuaire AD DS

1 Connectez-vous à GLPI en **glpi**. Menu « **Configuration** » puis « **Authentification** » puis « **Annuaires LDAP** » ; cliquez « **+** » pour ajouter un annuaire et choisissez la préconfiguration « **Active Directory** » (elle renseigne le filtre et les champs d'AD)

2 Renseignez les champs suivants (les autres valeurs préconfigurées restent inchangées) puis cliquez « **Ajouter** » :

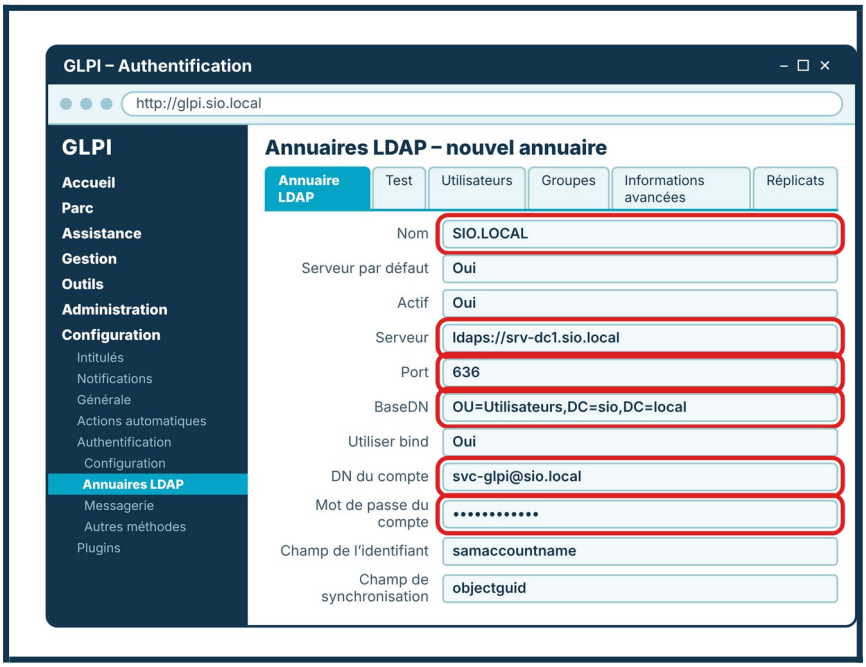


Figure 16 – Annuaires LDAP : formulaire de l'annuaire SIO.LOCAL

À SAVOIR

Le filtre de connexion préconfiguré pour Active Directory ne retient que les comptes utilisateurs **actifs**. Le champ de synchronisation `objectguid` identifie un compte de façon unique : renommer un utilisateur dans l'annuaire ne crée pas de doublon.

Champ	Valeur à saisir	Remarque
Nom	`SIO.LOCAL`	Nom affiché dans GLPI et sur la page de connexion
Serveur par défaut / Actif	Oui / Oui	Source d'authentification utilisée par défaut
Serveur	`ldaps://srv-dc1.sio.local`	Le préfixe **ldaps://** active le chiffrement
Port	`636`	Port LDAPS (389 = LDAP non chiffré)
BaseDN	`OU=Utilisateurs,DC=sio,DC=local`	Où chercher : seuls les comptes de cette OU sont visibles
Utiliser bind	Oui	Connexion authentifiée (le compte de service)
DN du compte	`svc-glpi@sio.local`	Format « identifiant@domaine » accepté par AD
Mot de passe du compte	mot de passe de **svc-glpi**	Stocké chiffré dans la base de GLPI
Champ de l'identifiant	`samaccountname`	Valeur préconfigurée : l'identifiant de connexion
Champ de synchronisation	`objectguid`	Valeur préconfigurée : identifiant unique du compte

B – Tester la connexion et ajouter le second contrôleur

1 Ouvrez l'annuaire créé, onglet « **Test** », puis cliquez « **Tester** » : le message de succès confirme la connexion et l'authentification du compte de service :

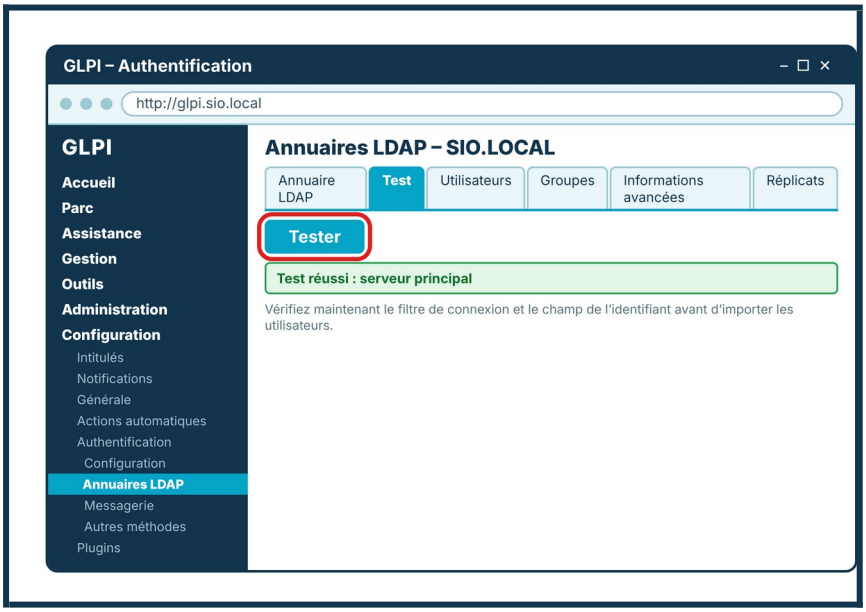


Figure 17 – Annuaire SIO.LOCAL : onglet Test

À SAVOIR

En cas d'échec, le message indique la cause. Reportez-vous au tableau de dépannage en fin de tutoriel : certificat non reconnu, nom du serveur incorrect ou mot de passe erroné.

2 Pour la **tolérance de panne**, ouvrez l'onglet « **Réplicats** », saisissez le nom **SRV-DC2**, le serveur `ldaps://srv-dc2.sio.local` et le port **636**, puis cliquez « **Ajouter** » : si SRV-DC1 est arrêté, GLPI interroge SRV-DC2 :

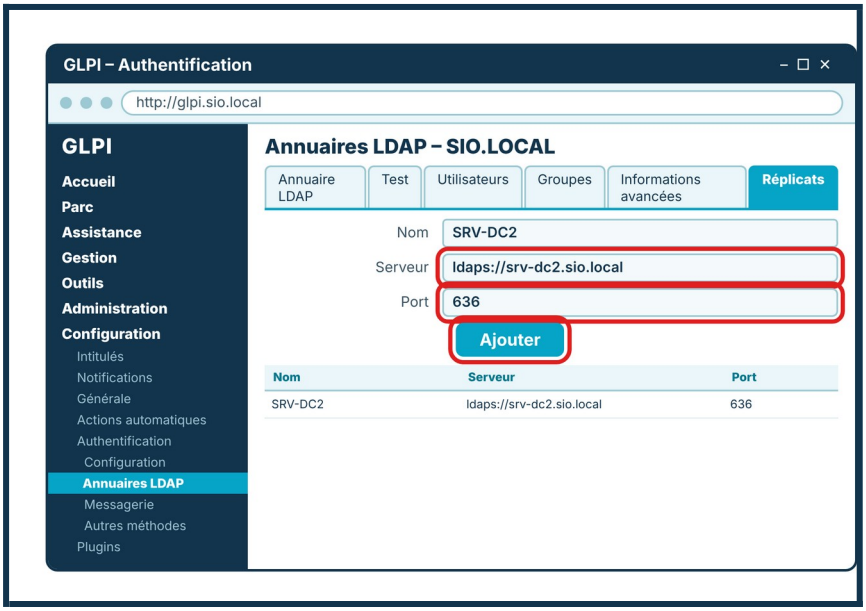


Figure 18 – Annuaire SIO.LOCAL : onglet Réplicats

À SAVOIR

Relancez ensuite le test : il vérifie le serveur principal et chaque réplicat.

C – Importer les utilisateurs

Un utilisateur de l'annuaire peut se connecter **sans import préalable** (GLPI le crée à sa première connexion), mais l'import permet de **préparer les comptes** : leur attribuer des droits ou les ajouter à un ticket avant leur première visite.

1 Menu « **Administration** » puis « **Utilisateurs** », bouton « **Lier un annuaire externe** » puis « **Importation de nouveaux utilisateurs** » ; cliquez « **Rechercher** », cochez les utilisateurs (ou la case d'en-tête pour tous) puis « **Actions** » et « **Importer** » :

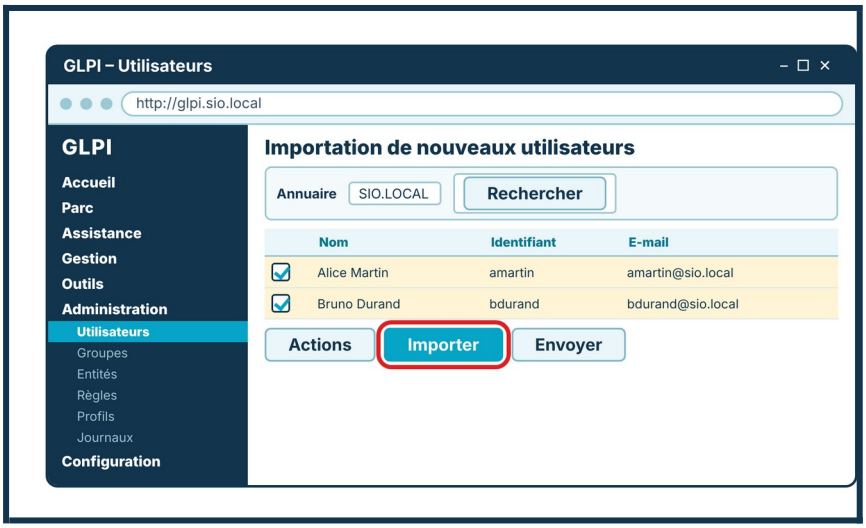


Figure 19 – Importation de nouveaux utilisateurs

À SAVOIR

Seuls les comptes de la BaseDN qui répondent au filtre apparaissent. Un compte désactivé dans l'annuaire n'est pas proposé.

2 La liste des utilisateurs contient désormais **amartin** et **bdurand**, dont la source d'authentification est l'annuaire :

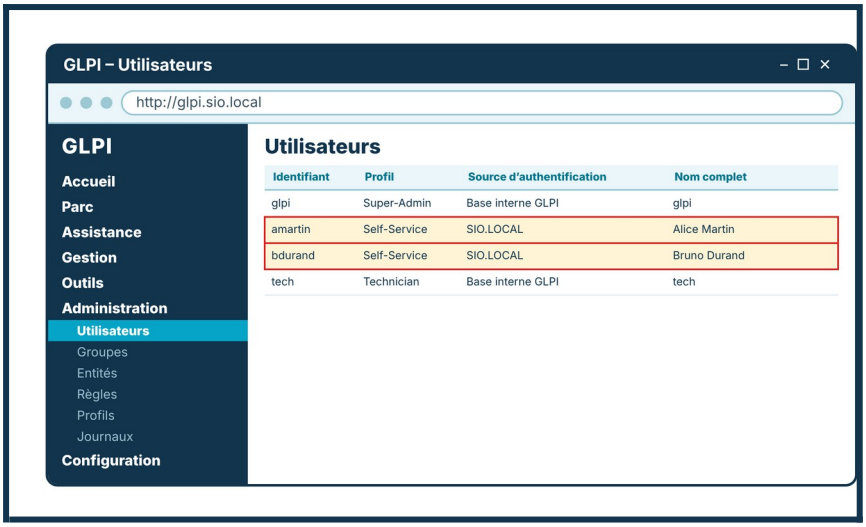


Figure 20 – Administration > Utilisateurs : comptes importés

À SAVOIR

Les utilisateurs importés reçoivent le profil par défaut du paramétrage de GLPI (en général « Self-Service » : créer des tickets et suivre les siens). Pour confier un autre rôle, ouvrez le compte, onglet « Habilitations », et ajoutez un profil (par exemple « Technician »).

D – Se connecter avec un compte Windows

1 Déconnectez-vous de GLPI, puis ouvrez la page de connexion dans une **fenêtre de navigation privée** : saisissez **amartin**, son mot de passe de domaine, et sélectionnez **SIO.LOCAL** dans « Connexion à » :



Figure 21 – Page de connexion de GLPI avec l'annuaire

À SAVOIR

Le mot de passe n'est jamais copié dans GLPI : à chaque connexion, GLPI le fait vérifier par l'annuaire. Changer ou réinitialiser le mot de passe dans Active Directory suffit donc.

2 **Pour aller plus loin** : la commande `sudo -u www-data php /var/www/glpi/bin/console glpi:ldap:synchronize_users --help` décrit la synchronisation en masse des utilisateurs (créations, mises à jour, désactivations), qui peut être planifiée

✔ POINT DE CONTRÔLE

- Le **test** de l'annuaire SIO.LOCAL réussit, serveur principal et réplicat
- **amartin** et **bdurand** sont importés avec l'annuaire comme source d'authentification
- **amartin** ouvre une session GLPI avec son **mot de passe Windows**
- Si SRV-DC1 est arrêté, la connexion fonctionne encore grâce à **SRV-DC2**

Notre GLPI est **opérationnel** : installé en natif sur Debian 13, séparé de ses données, sécurisé, et relié à AD DS en LDAPS avec un second contrôleur en secours. Il reste à le remplir (inventaire, entités, profils, plugin d'inventaire) et à le publier en HTTPS.

Dépannage : les symptômes les plus fréquents

Symptôme	Cause probable	Solution
Page « Apache2 Debian Default Page »	Le site par défaut est resté actif	`sudo a2dissite 000-default && sudo a2ensite glpi && sudo systemctl reload apache2`
Pages GLPI en erreur 404 (sauf la première)	Le module de réécriture n'est pas activé	`sudo a2enmod rewrite && sudo systemctl restart apache2`
Le navigateur télécharge ou affiche le code PHP	PHP-FPM n'est pas relié à Apache	Vérifier `proxy_fcgi` activé et le `SetHandler` du site ; `systemctl status php8.4-fpm`
Assistant : ligne « Requis » en rouge	Extension PHP manquante ou droit d'écriture refusé	Relancer le contrôle des extensions (étape 2-A) ; refaire les `chown` de l'étape 3-B
Erreur 500 ou page blanche	Erreur PHP ou de configuration	`sudo tail -n 30 /var/log/glpi/php-errors.log` et `/var/log/apache2/glpi-error.log`
Test LDAP : « Can't contact LDAP server »	Certificat non reconnu, nom différent du certificat ou port 636 bloqué	Refaire l'étape 5-C ; utiliser le **nom complet** du contrôleur, pas son adresse IP ; `sudo systemctl restart php8.4-fpm`
`ldapsearch` **: « Strong(er) authentication required »**	Connexion LDAP non chiffrée refusée par Windows Server 2025	Utiliser `ldaps://` et le port **636**, jamais `ldap://` avec mot de passe
« Invalid credentials » (code 49)	DN du compte ou mot de passe incorrect, compte désactivé	Saisir `svc-glpi@sio.local` ; tester `ldapsearch -W` ; vérifier `Get-ADUser svc-glpi`
Test réussi mais aucun utilisateur à importer	BaseDN incorrecte ou OU vide	Comparer avec `Get-ADUser -SearchBase` ; vérifier la casse et les virgules de la BaseDN
Un utilisateur de l'annuaire ne peut pas se connecter	Compte en dehors de la BaseDN, désactivé, ou mauvaise source choisie	Contrôler son OU, son état, et sélectionner **SIO.LOCAL** dans « Connexion à »
Les actions automatiques ne s'exécutent pas	Fichier cron mal formé ou droits incorrects	Fichier `/etc/cron.d/glpi` en 644, propriétaire root, terminé par un saut de ligne ; tester à la main

Pense-bête : où regarder

Où / commande	Utilité
Configuration > Authentification > Annuaires LDAP	Déclarer, tester et dupliquer les annuaires (réplicats)
Administration > Utilisateurs	Liste des comptes, import, profils et habilitations
Configuration > Actions automatiques	Tâches planifiées, mode d'exécution et dernière exécution
`/var/log/glpi/`	Journaux de GLPI : `php-errors.log`, `sql-errors.log`, `access.log`
`/var/log/apache2/glpi-error.log`	Erreurs du serveur web pour le site GLPI
`/etc/glpi/`	Configuration (`config_db.php`) et clé de chiffrement (`glpicrypt.key`) : à sauvegarder
`/var/lib/glpi/`	Documents joints, images, cache, sessions : à sauvegarder
`sudo -u www-data php /var/www/glpi/bin/console`	Console GLPI : maintenance, synchronisation LDAP, mises à jour
`openssl s_client -connect <contrôleur>:636`	Vérifier le certificat LDAPS présenté par un contrôleur
`ldapsearch -H ldaps://… -D … -W`	Tester l'annuaire sans passer par GLPI