PortailSIO

NOUVELLE FORMULE

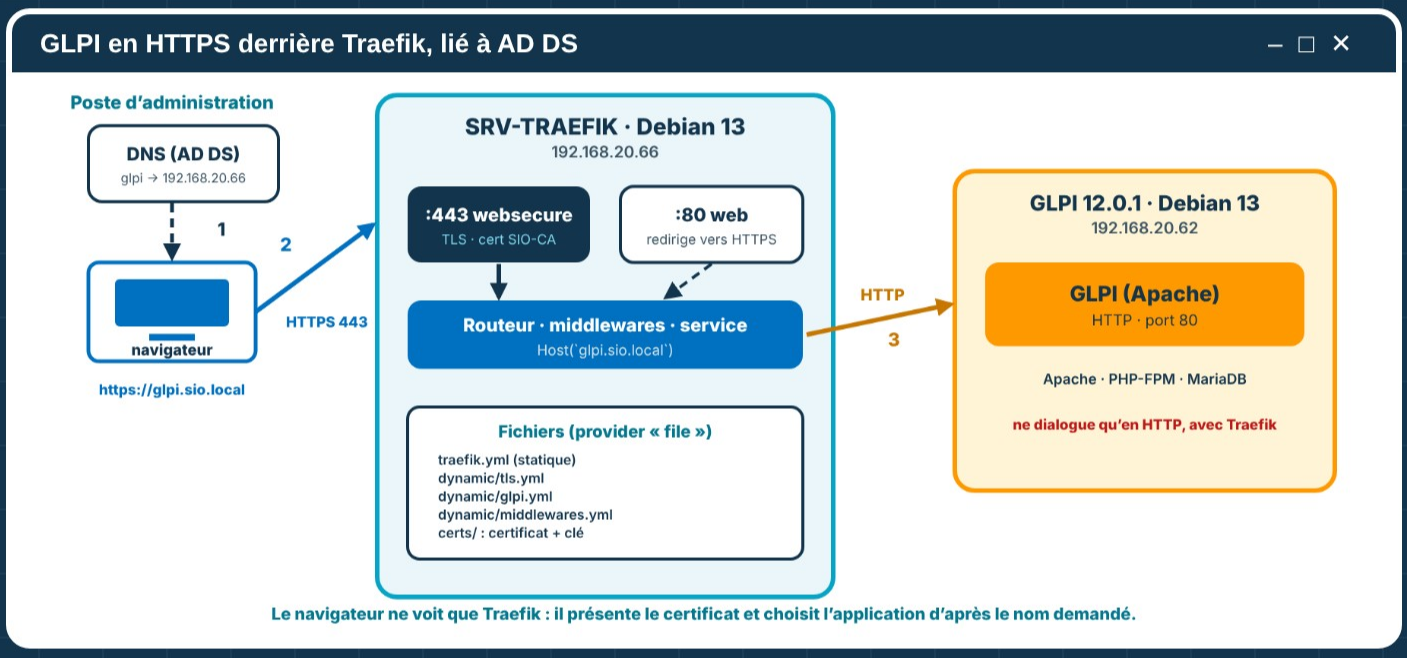
TUTORIEL

DEBIAN 13 · TRAEFIK 3.7 · HTTPS

Installer derrière Traefik

GLPI





1. Préparer les deux serveurs et le DNS
2. Installer GLPI en natif sur Debian 13
3. Installer Traefik et obtenir le certificat
4. Publier GLPI avec les fichiers dynamiques de Traefik
5. Adapter GLPI au proxy et le sécuriser
6. Lier GLPI à l'annuaire AD DS

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

Ce tutoriel en ligne

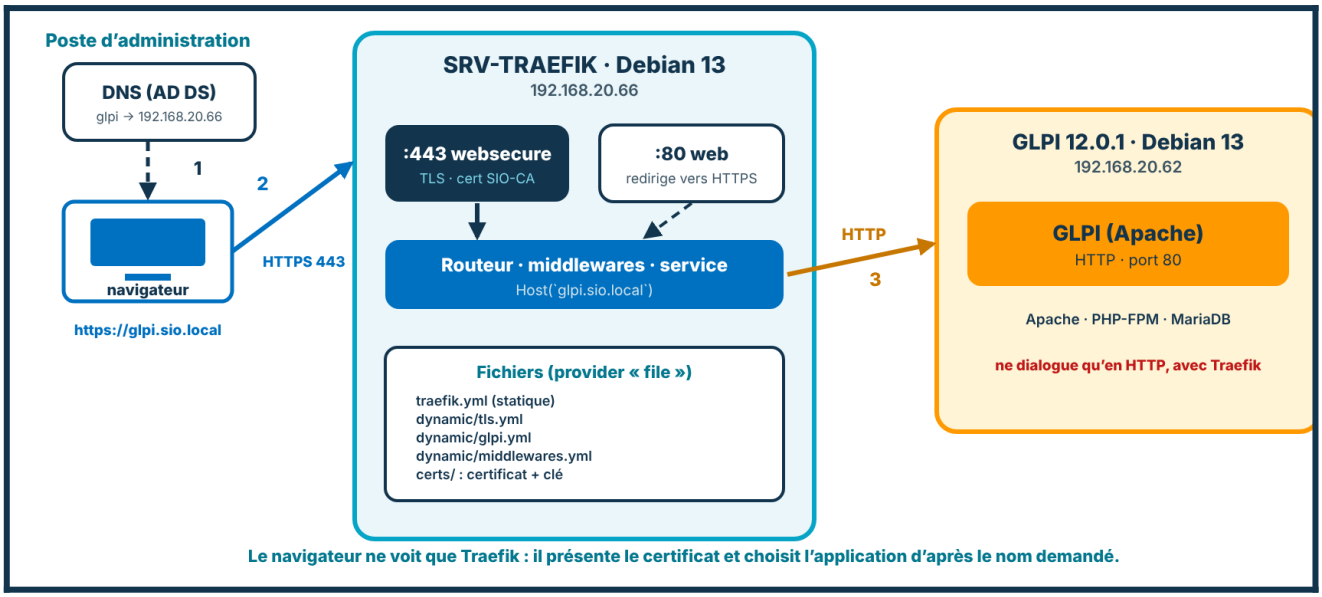
Scannez le QR code. Tous les tutoriels :

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 de deux machines virtuelles 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, avec l'autorité de certification **SIO-CA** et **LDAPS** activé : voir le tutoriel « Activer LDAPS sur AD DS »). Le tutoriel est de niveau **expert** : il demande d'être à l'aise avec Linux, le DNS et les certificats.

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… Ses utilisateurs saisissent leurs identifiants dans le navigateur : le site doit donc être servi en **HTTPS**, et non en HTTP simple.

Traefik est un **proxy inverse** (en anglais *reverse proxy*) : un serveur placé **devant** les applications, qui reçoit toutes les connexions des utilisateurs et les transmet à la bonne application. Il apporte trois choses. Il **chiffre** les échanges (c'est lui qui présente le certificat HTTPS), il **aiguille** chaque requête d'après le nom demandé (`glpi.sio.local`, `zabbix.sio.local`…) et il ajoute des **protections** (en-têtes de sécurité, filtrage par adresse). GLPI n'a plus à gérer le HTTPS ni à être exposé aux utilisateurs.

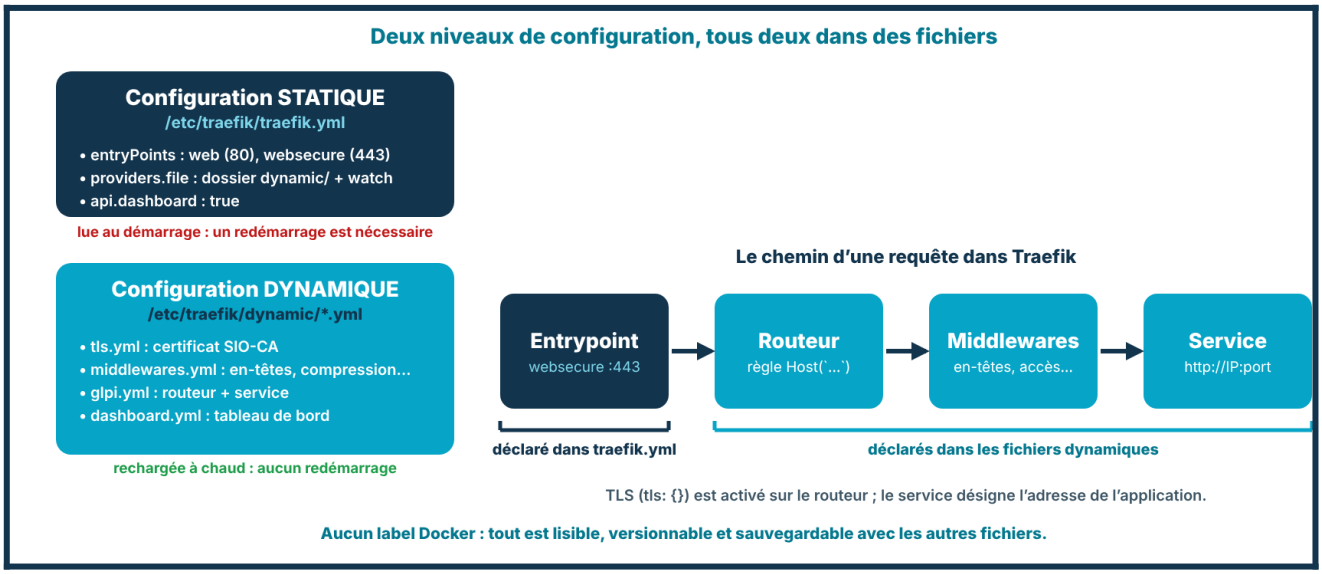


Le trajet d'une requête

- **1 – Le DNS** : le nom `glpi.sio.local` est déclaré dans l'annuaire AD DS et pointe vers l'adresse de **Traefik**, pas vers celle de GLPI
- **2 – HTTPS** : le navigateur se connecte à Traefik sur le port **443**. Traefik présente un certificat délivré par **SIO-CA**, auquel les postes du domaine font déjà confiance. Le port 80 existe aussi, mais il ne fait que renvoyer vers HTTPS
- **3 – HTTP** : Traefik transmet la requête à Apache sur SRV-GLPI, en clair, sur le réseau des serveurs. Seul Traefik peut joindre Apache : nous fermerons l'accès direct à l'étape 5

La liaison avec l'annuaire (étape 6) est **indépendante** de Traefik : c'est SRV-GLPI qui interroge directement les contrôleurs de domaine, par une connexion chiffrée **LDAPS**, pour vérifier le mot de passe de chaque utilisateur.

Traefik se configure avec **deux niveaux de fichiers**. La configuration **statique** (ports d'écoute, emplacement des autres fichiers) n'est lue qu'au démarrage. La configuration **dynamique** (certificats, routes, middlewares) est répartie en un **fichier par sujet** et rechargée à chaud. **Dans ce tutoriel, toute la configuration passe par ces fichiers : aucun label Docker n'est utilisé**, et Docker n'est d'ailleurs pas installé :



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-TRAEFIK	Proxy inverse Traefik (nom `srv-traefik`) : seul point d'entrée des utilisateurs	Debian 13	192.168.20.66
SRV-GLPI	Serveur GLPI : Apache, PHP-FPM et MariaDB (nom `srv-glpi`)	Debian 13	192.168.20.62
SRV-DC1	Contrôleur de domaine, DNS, annuaire principal, autorité de certification SIO-CA	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 (DNS = les deux contrôleurs, poste membre du domaine, réseau 192.168.10.0 /24)	Windows 11	DHCP

Prévoyez **2 vCPU, 4 Go de mémoire et 30 Go de disque** pour SRV-GLPI, et **1 vCPU, 1 Go de mémoire et 10 Go de disque** pour SRV-TRAEFIK. 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 les deux serveurs et le DNS

Les utilisateurs ne connaîtront que **SRV-TRAEFIK** : les deux noms `glpi.sio.local` et `traefik.sio.local` désigneront son adresse. Chaque serveur reçoit un nom, une adresse fixe, le bon fuseau horaire et les DNS du domaine.

A – Préparer 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 (SRV-GLPI)

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

3. Donnez au serveur une **adresse IP fixe** (adaptez le nom de la carte, ici `ens18`, avec `ip -br address`) : éditez `/etc/network/interfaces`, indiquez les DNS du domaine dans `/etc/resolv.conf`, 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
```

/etc/resolv.conf

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

4. Vérifiez le résultat : nom, adresse IP, résolution DNS des contrôleurs, heure :

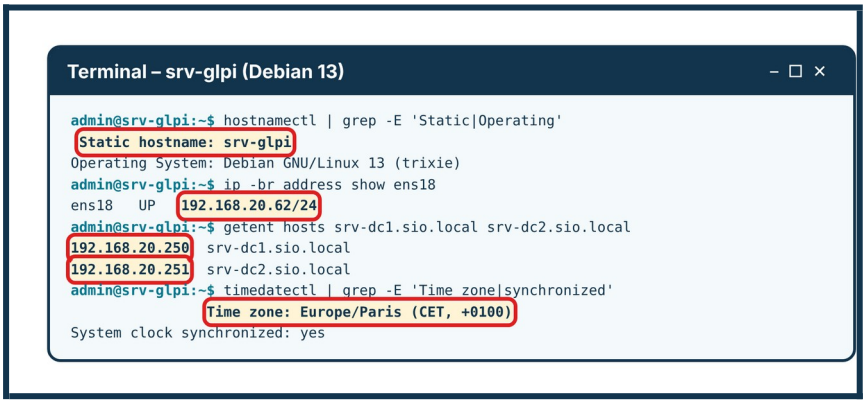


Figure 1 – Contrôle de la préparation de SRV-GLPI

À SAVOIR

Si « System clock synchronized » indique « no », installez un service de temps (`sudo apt install -y chrony`). L'heure doit être juste : les certificats ont des dates de validité.

B – Déclarer les noms dans le DNS

Sur **SRV-DC1**, dans PowerShell (**administrateur**), créez les deux enregistrements. Ils pointent tous deux vers l'adresse de **Traefik** (192.168.20.66) ; l'enregistrement est répliqué sur SRV-DC2 avec la zone :

POWERSHELL (SRV-DC1)

```
Add-DnsServerResourceRecordA -ZoneName sio.local -Name glpi `
    -IPv4Address 192.168.20.66
Add-DnsServerResourceRecordA -ZoneName sio.local -Name traefik `
    -IPv4Address 192.168.20.66
Resolve-DnsName glpi.sio.local, traefik.sio.local -Type A | Select Name, Type, TTL,
IPAddress
```

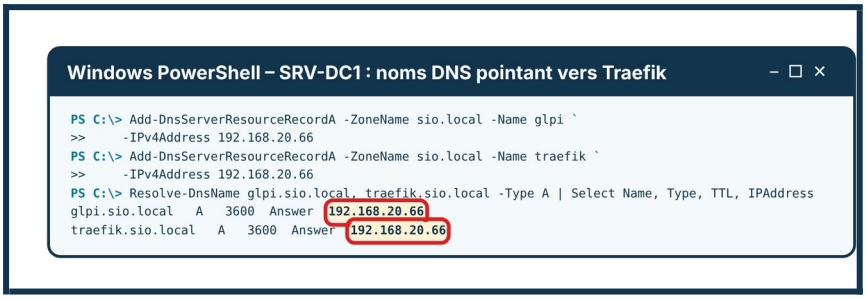


Figure 2 – PowerShell : noms DNS pointant vers Traefik

À SAVOIR

Le nom `glpi` désigne le **service** rendu aux utilisateurs, pas la machine qui l'héberge : si GLPI change de serveur un jour, seule la configuration de Traefik change, pas l'adresse que connaissent les utilisateurs.

À SAVOIR

Si un enregistrement `glpi` pointant vers **192.168.20.62** existe déjà (tutoriel « Installer GLPI et le lier à AD DS »), la commande `Add-` échoue ou crée un doublon. Supprimez d'abord l'ancien : `Remove-DnsServerResourceRecord -ZoneName sio.local -RRType A -Name glpi -Force`, puis recréez-le vers 192.168.20.66.

C – Préparer SRV-TRAEFIK

1 Sur **SRV-TRAEFIK**, mettez le système à jour (`sudo apt update && sudo apt full-upgrade -y`), nommez le serveur, réglez le fuseau et installez `curl` et `tree`, utiles pour les contrôles :

TERMINAL (SRV-TRAEFIK)

```
sudo hostnamectl set-hostname srv-traefik
echo "192.168.20.66  srv-traefik.sio.local  srv-traefik" | sudo tee -a /etc/hosts
sudo timedatectl set-timezone Europe/Paris
sudo apt install -y curl tree wget ca-certificates
```

2 Donnez-lui l'adresse **192.168.20.66** et les mêmes DNS que SRV-GLPI, dans `/etc/network/interfaces` et `/etc/resolv.conf` (même méthode qu'au point A), puis redémarrez le réseau. Contrôlez le résultat, en particulier la résolution des deux noms :

/etc/network/interfaces

```
auto ens18
iface ens18 inet static
    address 192.168.20.66/24
    gateway 192.168.20.254
```



Figure 3 – Contrôle de la préparation de SRV-TRAEFIK

À SAVOIR

`getent hosts` interroge le DNS du domaine comme le ferait une application. Si les noms ne sont pas résolus, vérifiez `/etc/resolv.conf` et que les enregistrements existent sur SRV-DC1 (`Get-DnsServerResourceRecord -ZoneName sio.local -Name glpi`).

✔ POINT DE CONTRÔLE

- SRV-GLPI répond au nom **srv-glpi** et à l'adresse **192.168.20.62**, SRV-TRAEFIK au nom **srv-traefik** et à **192.168.20.66**
- `glpi.sio.local` et `traefik.sio.local` sont résolus en **192.168.20.66** depuis SRV-TRAEFIK
- Le fuseau horaire est **Europe/Paris** et l'horloge est **synchronisée** sur les deux serveurs

02 ÉTAPE 2 SUR 6 Installer GLPI en natif sur Debian 13

Cette étape installe GLPI **12.0.1** sur **SRV-GLPI**, comme dans le tutoriel « Installer GLPI et le lier à AD DS » ; seul l'essentiel est repris ici. À la fin, le site répond en HTTP sur SRV-GLPI mais n'est pas encore installé : l'assistant sera lancé à l'étape 5, **à travers Traefik**. Toutes les commandes de cette étape s'exécutent sur **SRV-GLPI**.

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 associé à **PHP-FPM**, un service PHP séparé plus rapide et mieux isolé que le module classique. Le serveur ne publiera que du HTTP : le HTTPS est l'affaire de Traefik.

TERMINAL (SRV-GLPI)

```
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
```

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 (SRV-GLPI)

```
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

1 GLPI contrôle la configuration de PHP à l'installation. Créez `sudo nano /etc/php/8.4/fpm/conf.d/90-glpi.ini` : cookies de session protégés, et des limites confortables (documents joints jusqu'à 20 Mo) :

/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 (SRV-GLPI)

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

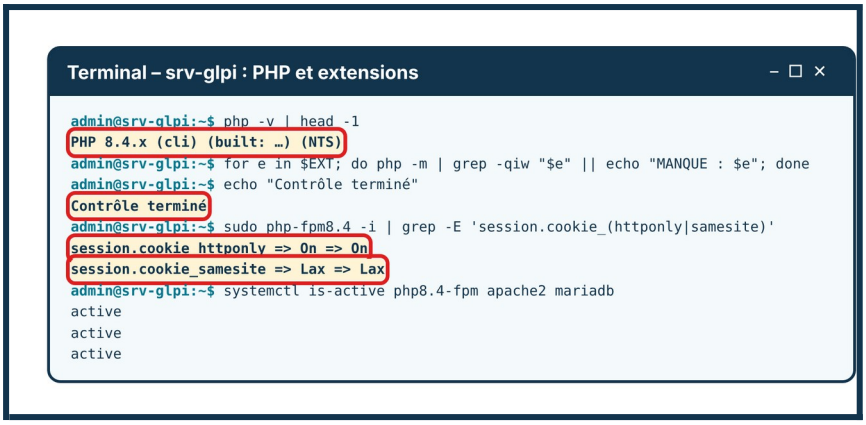


Figure 4 – PHP 8.4, extensions et réglages de session

À SAVOIR

`session.cookie_httponly` interdit aux scripts du navigateur de lire le cookie de session, `samesite` limite son envoi à votre site. La ligne `session.cookie_secure = On` (cookie envoyé uniquement en HTTPS) sera ajoutée à l'étape 5, quand le HTTPS sera en place.

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 (SRV-GLPI)

```
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;
```

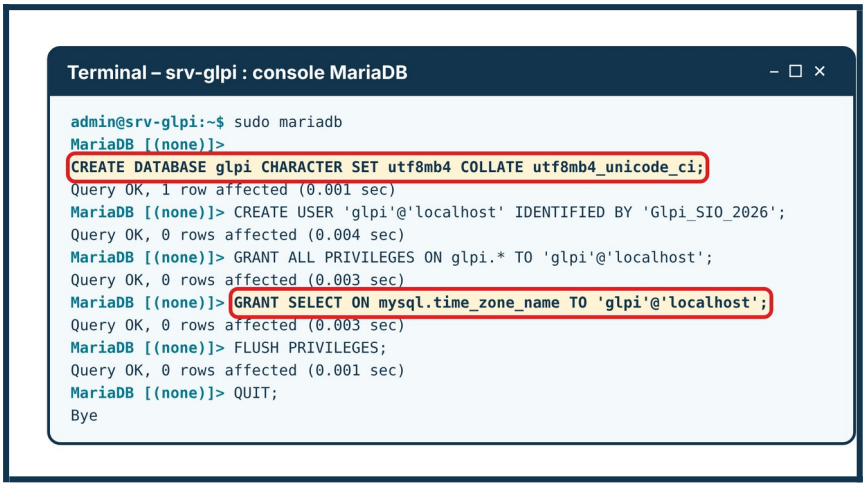


Figure 5 – Console MariaDB : création de la base et de l'utilisateur

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.

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 5) ; GLPI le range ensuite dans `/etc/glpi/config_db.php`, lisible uniquement par `www-data`.

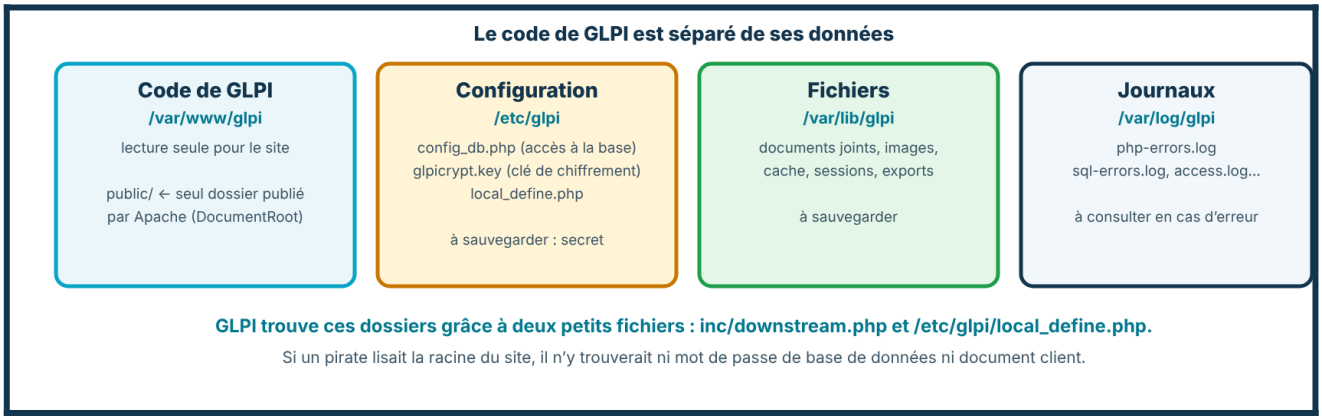
D – Télécharger GLPI et séparer le code des données

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

TERMINAL (SRV-GLPI)

```
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/
```

Par défaut, le dossier **/var/www/glpi** 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 :



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

TERMINAL (SRV-GLPI)

```
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 (SRV-GLPI)

```
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 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`.

E – Publier GLPI avec Apache

Apache doit publier **uniquement** le dossier `public` de GLPI et confier les pages PHP à PHP-FPM. Le `ServerName` reste `glpi.sio.local` : Traefik transmet à Apache le nom demandé par l'utilisateur. Une ligne `CustomLog` crée un journal d'accès propre au site, utile au point 5-B. 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
    CustomLog ${APACHE_LOG_DIR}/glpi-access.log combined
</VirtualHost>
```

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

TERMINAL (SRV-GLPI)

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

F – 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) :

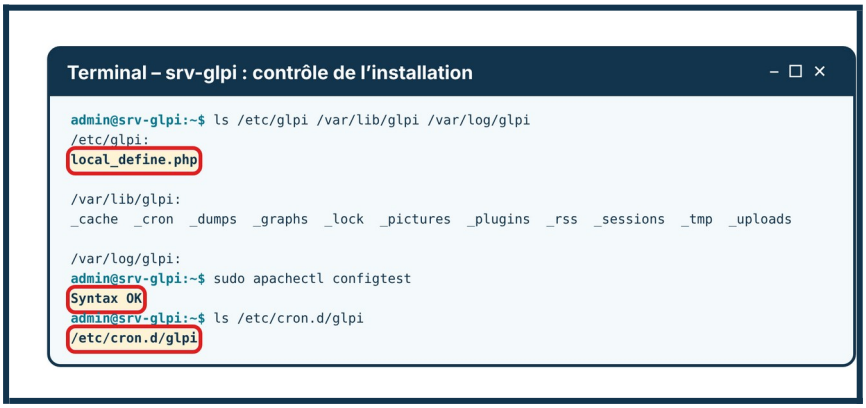


Figure 6 – Contrôle des dossiers déplacés, d'Apache et du cron

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`)
- `sudo mariadb -e "SHOW DATABASES;"` liste la base **glpi** et le fichier `/etc/cron.d/glpi` existe

03 ÉTAPE 3 SUR 6 Installer Traefik et obtenir le certificat

Traefik s'installe sur **SRV-TRAEFIK** : tout ce qui suit, jusqu'à l'étape 4 incluse, est exécuté sur cette machine (sauf indication contraire). L'installation se fait **en natif**, sans conteneur : un exécutable, un compte système et un service.

A – Télécharger et installer l'exécutable

Traefik est distribué sous la forme d'**un seul exécutable**, sans dépendance. On le télécharge depuis la page des versions du projet (GitHub), on vérifie son **empreinte** (somme de contrôle) puis on l'installe dans `/usr/local/bin`. Sur **SRV-TRAEFIK** :

TERMINAL

```
cd /tmp
V=3.7.16
URL=https://github.com/traefik/traefik/releases/download/v$V
wget -q $URL/traefik_v${V}_linux_amd64.tar.gz $URL/traefik_v${V}_checksums.txt
sha256sum -c --ignore-missing traefik_v${V}_checksums.txt
tar -xzf traefik_v${V}_linux_amd64.tar.gz traefik
sudo install -m 0755 traefik /usr/local/bin/traefik
traefik version | head -1
```



Figure 7 – Téléchargement, vérification et installation de Traefik 3.7.16

À SAVOIR

La ligne « OK » prouve que le fichier téléchargé n'a pas été altéré. Si la commande répond « No such file » ou « FAILED », vérifiez le numéro de version dans la page des versions du projet : les noms de fichiers en dépendent.

B – Créer l'utilisateur et les dossiers

1 Traefik ne doit pas tourner en `root` : on crée un compte système dédié, sans mot de passe ni interpréteur de commandes, et les trois dossiers de configuration (statique, dynamique, certificats) :

TERMINAL

```
sudo useradd --system --no-create-home --shell /usr/sbin/nologin traefik
sudo install -d -o traefik -g traefik /etc/traefik /etc/traefik/dynamic
sudo install -d -o traefik -g traefik /etc/traefik/certs /var/log/traefik
```

C – Écrire la configuration statique

La configuration de Traefik se compose de **deux parties**. La **statique** décrit les bases (ports d'écoute, d'où viennent les routes) et n'est lue qu'au démarrage. La **dynamique** décrit les routes, les certificats et les middlewares ; elle est lue dans des **fichiers** et rechargée **à chaud**. Créez `sudo nano /etc/traefik/traefik.yml` :

/etc/traefik/traefik.yml

```
entryPoints:
  web:
    address: ":80"
    http:
      redirections:
        entryPoint:
          to: websecure
          scheme: https
          permanent: true
  websecure:
    address: ":443"

providers:
  file:
    directory: /etc/traefik/dynamic
    watch: true

api:
  dashboard: true

log:
  level: INFO

accessLog:
  filePath: /var/log/traefik/access.log
```

Bloc	Rôle
`entryPoints`	Les ports d'écoute : **web** (80) redirige tout vers **websecure** (443, HTTPS)
`providers.file`	La source des routes : les fichiers du dossier `dynamic`, surveillés (`watch`) pour un rechargement à chaud
`api.dashboard`	Active le tableau de bord ; il sera publié par un routeur protégé (étape 5), pas sur un port ouvert
`accessLog`	Journal des requêtes, utile pour diagnostiquer une route

REMARQUE IMPORTANTE

Traefik offre aussi d'autres sources de configuration (notamment les **labels Docker**). Ici, **toute la configuration passe par des fichiers** : un fichier par application, lisible, comparable et sauvegardable comme n'importe quel autre fichier du serveur. Aucun accès au moteur Docker n'est donc nécessaire.

D – Créer le service systemd et le démarrer

1 Créez `sudo nano /etc/systemd/system/traefik.service` :

/etc/systemd/system/traefik.service

```
[Unit]
Description=Traefik (proxy inverse)
After=network-online.target
Wants=network-online.target

[Service]
User=traefik
Group=traefik
ExecStart=/usr/local/bin/traefik --configFile=/etc/traefik/traefik.yml
AmbientCapabilities=CAP_NET_BIND_SERVICE
NoNewPrivileges=true
Restart=on-failure
LimitNOFILE=65536

[Install]
WantedBy=multi-user.target
```

La ligne `AmbientCapabilities` autorise le compte `traefik` à ouvrir les ports **80 et 443** (ports réservés) sans être `root`. Activez et démarrez le service, puis contrôlez-le :

TERMINAL

```
sudo systemctl daemon-reload
sudo systemctl enable --now traefik
systemctl is-active traefik
sudo ss -tlnp | grep traefik
```

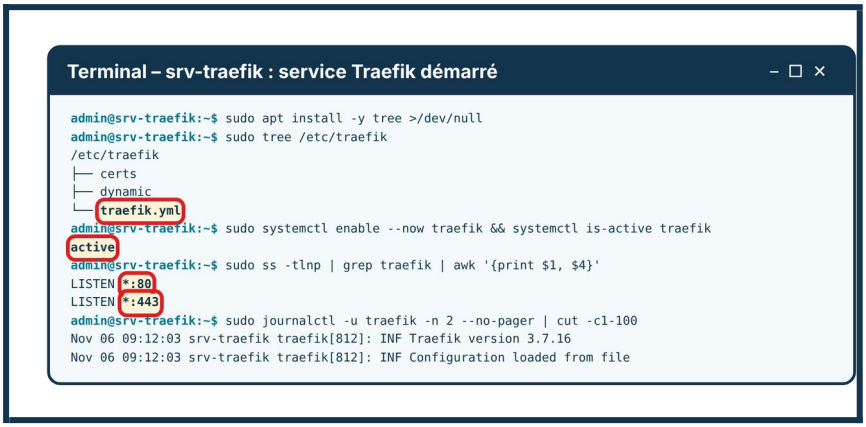


Figure 8 – Traefik démarré : arborescence et ports en écoute

À SAVOIR

À ce stade, le dossier `dynamic` est vide : Traefik répond « 404 page not found » à toute requête, ce qui est normal. En cas d'échec, `sudo journalctl -u traefik -n 20` indique la ligne du fichier YAML en cause (indentation, guillemets).

✔ POINT DE CONTRÔLE

- `sha256sum` affiche **OK** et `traefik version` indique **3.7.16**
- Le service **traefik** est « active » et écoute sur les ports **80** et **443**
- Les dossiers `/etc/traefik/dynamic` et `/etc/traefik/certs` existent et appartiennent à `traefik`

Les navigateurs n'acceptent un site HTTPS que si son certificat est délivré par une autorité **qu'ils connaissent**. Dans le domaine **sio.local**, c'est l'autorité interne **SIO-CA** (construite dans le tutoriel « Activer LDAPS sur AD DS ») : les postes Windows du domaine lui font déjà confiance. Nous allons lui demander un certificat pour **glpi.sio.local et traefik.sio.local**. La clé privée est créée sur **SRV-TRAEFIK** et ne le quitte jamais : seule la demande (CSR) voyage.

E – Créer la clé privée et la demande de certificat

1 Créez le fichier de description `sudo nano /tmp/glpi.cnf` : le certificat doit porter **tous les noms** utilisés (champ « Subject Alternative Name »), les navigateurs ignorant le nom principal seul :

/tmp/glpi.cnf

```
[req]
distinguished_name = dn
req_extensions = ext
prompt = no

[dn]
CN = glpi.sio.local

[ext]
subjectAltName = DNS:glpi.sio.local, DNS:traefik.sio.local
```

2 Générez la clé privée (RSA 2048) et la demande de certificat, puis contrôlez le contenu de la demande :

TERMINAL

```
sudo openssl req -new -newkey rsa:2048 -nodes -config /tmp/glpi.cnf \
    -keyout /etc/traefik/certs/glpi.key -out /tmp/glpi.csr
openssl req -in /tmp/glpi.csr -noout -subject -verify
openssl req -in /tmp/glpi.csr -noout -text | grep -A1 Alternative
```



Figure 9 – Clé privée et demande de certificat avec ses deux noms

À SAVOIR

Le fichier `.key` est la clé privée : elle reste sur SRV-TRAEFIK, avec des droits restreints (voir plus bas). Le fichier `.csr` ne contient que la clé **publique** et les noms : il peut circuler librement.

F – Faire signer la demande par SIO-CA

Sur **SRV-DC1** (qui héberge l'autorité de certification), dans PowerShell ouvert **en tant qu'administrateur**, récupérez la demande, soumettez-la avec le modèle « **Serveur Web** » (nom interne `WebServer`) puis renvoyez le certificat obtenu vers SRV-TRAEFIK :

POWERSHELL

```
scp admin@192.168.20.66:/tmp/glpi.csr C:\Temp\
certreq -submit -config "SRV-DC1.sio.local\SIO-CA" `
    -attrib "CertificateTemplate:WebServer" `
    C:\Temp\glpi.csr C:\Temp\glpi.cer
scp C:\Temp\glpi.cer admin@192.168.20.66:/tmp/
```



Figure 10 – Signature de la demande par l'autorité SIO-CA

À SAVOIR

Si `certreq` répond « Refusé » ou « En attente », le modèle « Serveur Web » n'est pas activé sur l'autorité (console certsrv > Modèles de certificats > Nouveau > Modèle de certificat à délivrer) ou le compte n'a pas le droit « Inscrire » dessus.

G – Installer le certificat sur SRV-TRAEFIK

1. Convertissez le certificat reçu au format PEM, donnez la clé au compte `traefik` seul, puis vérifiez que le certificat correspond bien à la clé :

TERMINAL

```
sudo openssl x509 -in /tmp/glpi.cer -out /etc/traefik/certs/glpi.crt
sudo chown -R traefik:traefik /etc/traefik/certs
sudo chmod 600 /etc/traefik/certs/glpi.key
sudo openssl x509 -in /etc/traefik/certs/glpi.crt -noout -subject -issuer -enddate
sudo openssl x509 -in /etc/traefik/certs/glpi.crt -noout -ext subjectAltName
cmp <(sudo openssl x509 -in /etc/traefik/certs/glpi.crt -noout -pubkey) \
    <(sudo openssl pkey -in /etc/traefik/certs/glpi.key -pubout) \
    && echo "Clé et certificat correspondent"
```

À SAVOIR

Si OpenSSL répond « Could not read certificate » (ou « unable to load »), le fichier reçu est au format binaire : ajoutez l'option `-inform der` à la première commande.



Figure 11 – Certificat installé : émetteur, noms et correspondance avec la clé

À SAVOIR

Le certificat vaut deux ans environ (durée du modèle). Notez sa date de fin : **un certificat expiré rend le site inaccessible** (alerte du navigateur). Pour un renouvellement, répétez ces trois points puis remplacez les deux fichiers : Traefik les relit à chaud.

✔ POINT DE CONTRÔLE

- La demande `glpi.csr` contient les noms **glpi.sio.local** et **traefik.sio.local**
- SIO-CA a émis le certificat (« **Émis** ») et il est copié dans `/etc/traefik/certs`
- L'émetteur affiché est **SIO-CA** et la clé privée est lisible uniquement par `traefik`

ÉTAPE 4 SUR 6

04 Publier GLPI avec les fichiers dynamiques de Traefik

Nous créons maintenant les fichiers du dossier `/etc/traefik/dynamic`. Traefik les **surveille** : il charge chaque fichier dès qu'il est enregistré, sans redémarrage. Un fichier invalide est ignoré (et signalé dans le journal) : le reste de la configuration continue de fonctionner. Les trois premiers fichiers sont **communs** à toutes les applications que Traefik publiera un jour ; le dernier est propre à GLPI.

A – Déclarer le certificat et les options TLS

1. Créez `sudo nano /etc/traefik/dynamic/tls.yml` : il indique à Traefik le certificat à présenter (il choisit le bon d'après le nom demandé par le navigateur) et impose TLS 1.2 au minimum :

/etc/traefik/dynamic/tls.yml

```
tls:
  certificates:
    - certFile: /etc/traefik/certs/glpi.crt
      keyFile: /etc/traefik/certs/glpi.key
  options:
    default:
      minVersion: VersionTLS12
```

B – Créer les middlewares réutilisables

Un **middleware** modifie la requête ou la réponse au passage dans Traefik. On en déclare trois dans un fichier, que tous les routeurs pourront réutiliser. Créez `sudo nano /etc/traefik/dynamic/middlewares.yml` :

/etc/traefik/dynamic/middlewares.yml

```
http:
  middlewares:
    secure-headers:
      headers:
        stsSeconds: 31536000
        contentTypeNosniff: true
        referrerPolicy: same-origin
        customFrameOptionsValue: SAMEORIGIN
    compression:
      compress: {}
    admin-seulement:
      ipAllowList:
        sourceRange:
          - 192.168.20.0/24
          - 192.168.10.0/24
```

Middleware	Effet
`secure-headers`	Ajoute des en-têtes de sécurité : HSTS (le navigateur n'utilisera plus que HTTPS pendant un an), interdiction de deviner le type des fichiers, cadres limités au même site
`compression`	Compresse les réponses (pages plus légères sur le réseau)
`admin-seulement`	Autorise uniquement les adresses listées (`ipAllowList`) : à utiliser pour les interfaces d'administration

REMARQUE IMPORTANTE

Adaptez les réseaux de `sourceRange` : ils doivent contenir l'adresse du **poste d'administration** (ici 192.168.10.0/24, à remplacer par votre réseau), sinon vous ne pourrez plus ouvrir le tableau de bord. **Le HSTS est mémorisé un an par le navigateur** : ne l'activez pas sur un nom de domaine que vous pourriez devoir exposer un jour en HTTP.

C – Publier le tableau de bord de Traefik

1. Créez `sudo nano /etc/traefik/dynamic/dashboard.yml` : un routeur, réservé aux administrateurs, vers le service interne `api@internal` :

/etc/traefik/dynamic/dashboard.yml

```
http:
  routers:
    dashboard:
      rule: "Host(`traefik.sio.local`)"
      entryPoints:
        - websecure
      middlewares:
        - admin-seulement
        - secure-headers
      service: api@internal
      tls: {}
```

Un routeur associe trois éléments : une **règle** (`rule` : ici, le nom de site demandé), des **middlewares** (appliqués dans l'ordre) et un **service** (la destination). `tls: {}` active HTTPS sur ce routeur avec le certificat déclaré à l'étape A.

D – Publier GLPI

Un fichier par application : celui-ci décrit le **routeur** (quel nom, quels middlewares) et le **service** (où se trouve GLPI). GLPI étant servi à la racine du site, aucun middleware particulier n'est nécessaire. Créez `sudo nano /etc/traefik/dynamic/glpi.yml` :

/etc/traefik/dynamic/glpi.yml

```
http:
  routers:
    glpi:
      rule: "Host(`glpi.sio.local`)"
      entryPoints:
        - websecure
      middlewares:
        - secure-headers
        - compression
      service: glpi
      tls: {}

  services:
    glpi:
      loadBalancer:
        servers:
          - url: "http://192.168.20.62"
```

Élément	Signification
`rule`	Condition d'aiguillage : la requête est destinée à ce routeur si le nom de site demandé est `glpi.sio.local`
`entryPoints: websecure`	Le routeur n'écoute que sur le port 443 ; le port 80 ne fait que rediriger (configuration statique)
`middlewares`	Appliqués dans l'ordre : en-têtes de sécurité, puis compression. Ils sont définis dans `middlewares.yml` et réutilisés tels quels
`service: glpi`	Renvoie au service du même nom, déclaré en bas du fichier
`loadBalancer.servers`	L'adresse d'Apache sur SRV-GLPI. Une seule adresse ici ; en ajouter une deuxième répartirait la charge entre deux serveurs
`tls: {}`	Active HTTPS sur ce routeur avec le certificat déclaré dans `tls.yml`

REMARQUE IMPORTANTE

Dans un fichier YAML, une **erreur d'indentation** change le sens du fichier ou l'invalide. La règle `rule` est entre guillemets, car elle contient des parenthèses et des accents graves. En cas de doute, `sudo journalctl -u traefik -n 20` indique le fichier et la ligne en cause.

E – Contrôler les fichiers et le démarrage

1 Sur **SRV-TRAEFIK**, affichez l'arborescence de la configuration, les ports en écoute et le nombre d'erreurs du journal des cinq dernières minutes :

TERMINAL (SRV-TRAEFIK)

```
sudo tree /etc/traefik
sudo ss -tlnp | grep traefik | awk '{print $1, $4}'
sudo journalctl -u traefik --since "5 min ago" --no-pager | grep -ci error
```

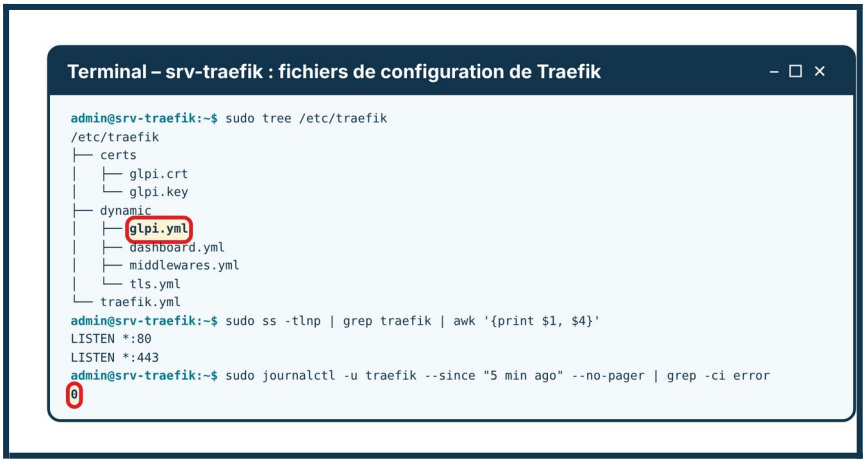


Figure 12 – Fichiers de configuration de Traefik

À SAVOIR

Un compteur différent de `0` indique un fichier mal formé : `sudo journalctl -u traefik -n 20` donne le nom du fichier et la ligne. Traefik n'a pas besoin d'être redémarré : les fichiers dynamiques sont rechargés à chaud.

F – Tester la chaîne en ligne de commande

Pour tester depuis SRV-TRAEFIK lui-même, ce serveur doit faire confiance à **SIO-CA** (les postes Windows du domaine lui font déjà confiance, pas Debian). Sur **SRV-DC1**, exportez le certificat de l'autorité et copiez-le :

POWERSHELL (SRV-DC1)

```
New-Item -ItemType Directory -Path C:\Temp -Force | Out-Null
certutil -ca.cert C:\Temp\sio-ca.cer
scp C:\Temp\sio-ca.cer admin@192.168.20.66:/tmp/
```

Sur **SRV-TRAEFIK**, convertissez-le au format PEM, ajoutez-le aux autorités de confiance du système et vérifiez le certificat de Traefik par rapport à ce magasin :

TERMINAL (SRV-TRAEFIK)

```
sudo openssl x509 -inform der -in /tmp/sio-ca.cer \
    -out /usr/local/share/ca-certificates/sio-ca.crt
sudo update-ca-certificates
openssl verify /etc/traefik/certs/glpi.crt
```



Figure 13 – Confiance dans SIO-CA et vérification du certificat

À SAVOIR

« OK » prouve que le certificat de Traefik est signé par SIO-CA. Si OpenSSL répond « Could not read certificate », le fichier exporté est déjà au format PEM : copiez-le simplement dans `/usr/local/share/ca-certificates/sio-ca.crt`.

1 Testez la redirection HTTP vers HTTPS et le certificat présenté :

TERMINAL (SRV-TRAEFIK)

```
curl -sI http://glpi.sio.local | grep -iE '^(HTTP|location)'
curl -sv https://glpi.sio.local/ -o /dev/null 2>&1 \
    | grep -E 'subject:|issuer:|verify'
```



Figure 14 – Redirection et certificat vus par curl

À SAVOIR

Le premier test montre le port 80 qui renvoie vers HTTPS ; le deuxième, l'émetteur du certificat. « 404 page not found » signale qu'aucun routeur ne correspond au nom demandé ; « 502 Bad Gateway », que Traefik n'atteint pas Apache.

G – Ouvrir le tableau de bord de Traefik

Depuis le **poste d'administration** (membre du domaine), ouvrez `https://traefik.sio.local`. Le navigateur affiche le cadenas **sans avertissement** : il fait confiance à SIO-CA. Le tableau de bord liste les routeurs lus dans les fichiers :

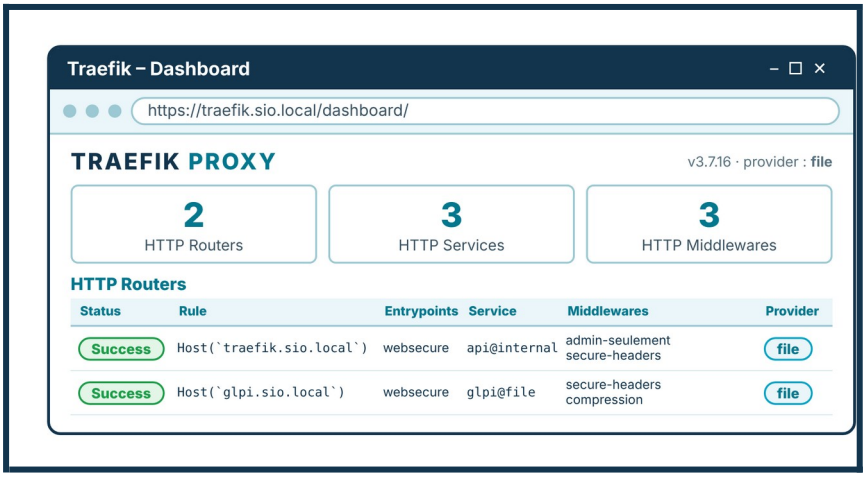


Figure 15 – Tableau de bord de Traefik : routeurs, services et middlewares

À SAVOIR

Un routeur « Success » est actif ; une erreur s'affiche en rouge avec sa cause. Le provider « file » rappelle que la configuration vient des fichiers. Un message « 403 Forbidden » signale que l'adresse du poste n'est pas dans `sourceRange` (middleware `admin-seulement`).

À SAVOIR

Un poste **hors domaine** n'a pas SIO-CA dans ses autorités de confiance : le navigateur affiche un avertissement. Importez le fichier `sio-ca.cer` dans les « Autorités de certification racines de confiance » du poste, ou déployez-le par GPO pour tous les postes du domaine.

✔ **POINT DE CONTRÔLE**

- Le dossier `/etc/traefik/dynamic` contient **tls.yml**, **middlewares.yml**, **dashboard.yml** et **glpi.yml**
- `openssl verify` répond **OK** et `curl` affiche **308** vers `https://glpi.sio.local/`
- Les réseaux de `sourceRange` incluent l'adresse du **poste d'administration**
- Le tableau de bord de Traefik affiche les routeurs **dashboard** et **glpi** en « Success »

05 ÉTAPE 5 SUR 6 Adapter GLPI au proxy et le sécuriser

Traefik est en place : il reste à installer GLPI à travers lui, à corriger deux détails que le proxy introduit (HTTPS et adresse des clients) et à fermer l'accès direct à Apache. Sauf indication contraire, les commandes s'exécutent sur **SRV-GLPI**.

A – Indiquer à PHP que les cookies sont servis en HTTPS

Les utilisateurs se connectent en HTTPS : le cookie de session peut donc être marqué « sécurisé », ce qui interdit au navigateur de l'envoyer en HTTP clair. Ajoutez la ligne au fichier de réglages de PHP et redémarrez PHP-FPM :

TERMINAL (SRV-GLPI)

```
echo 'session.cookie_secure = On' | sudo tee -a /etc/php/8.4/fpm/conf.d/90-glpi.ini
sudo systemctl restart php8.4-fpm
```

B – Voir l'adresse réelle des utilisateurs dans Apache

Pour Apache, toutes les connexions viennent désormais de **Traefik** : le journal d'accès (et le journal de GLPI, qui reprend l'adresse vue par le serveur web) affichent donc 192.168.20.66 au lieu de l'adresse de l'utilisateur. Traefik transmet l'adresse d'origine dans l'en-tête `X-Forwarded-For` ; le module **remoteip** d'Apache peut la lire, à condition de **ne faire confiance qu'à Traefik**. Le même fichier indique à PHP que la connexion d'origine était en HTTPS (en-tête `X-Forwarded-Proto`). Créez `sudo nano /etc/apache2/conf-available/proxy-traefik.conf` :

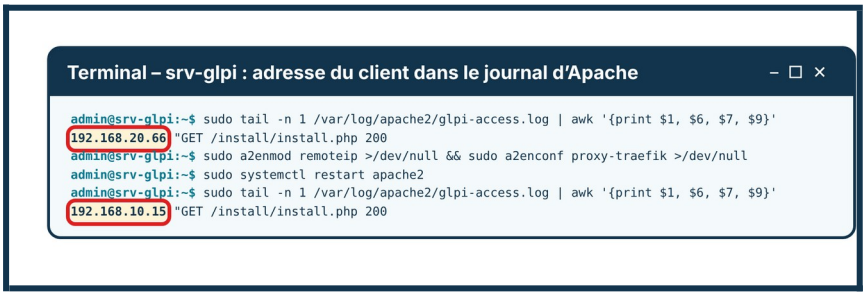
/etc/apache2/conf-available/proxy-traefik.conf

```
RemoteIPHeader X-Forwarded-For
RemoteIPInternalProxy 192.168.20.66
SetEnvIf X-Forwarded-Proto "^https$" HTTPS=on
```

1 Ouvrez `https://glpi.sio.local` dans le navigateur du poste d'administration : la première page de l'assistant s'affiche (ne continuez pas encore). Lisez la dernière ligne du journal (colonnes : adresse, requête, code), activez le module et la configuration, redémarrez Apache, rechargez la page et relisez le journal :

TERMINAL (SRV-GLPI)

```
sudo tail -n 1 /var/log/apache2/glpi-access.log | awk '{print $1, $6, $7, $9}'
sudo a2enmod remoteip > /dev/null && sudo a2enconf proxy-traefik > /dev/null
sudo systemctl restart apache2
sudo tail -n 1 /var/log/apache2/glpi-access.log | awk '{print $1, $6, $7, $9}'
```



À SAVOIR

Avant : l'adresse de Traefik. Après : l'adresse du poste d'administration. La directive `RemoteIPInternalProxy` limite la confiance à Traefik ; sans elle, n'importe quel client pourrait falsifier l'en-tête `X-Forwarded-For`.

Figure 16 – Adresse du client dans le journal d'Apache

C – Dérouler l'assistant d'installation

Depuis le **poste d'administration**, rechargez `https://glpi.sio.local` : l'assistant d'installation se lance, **à travers Traefik**.

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



À SAVOIR

L'adresse affichée est bien `https://glpi.sio.local` : la page a traversé Traefik. Si vous voyez la page « Apache2 Debian Default Page », le site par défaut est resté actif : relisez l'étape 2-E.

Figure 17 – Assistant GLPI : choix de la langue

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



Figure 18 – 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-la puis rechargez la page.

Figure 19 – 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** » :



À SAVOIR

La base se trouve sur SRV-GLPI, le même serveur que GLPI : l'adresse est `localhost`, pas celle de Traefik.

Figure 20 – 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) :

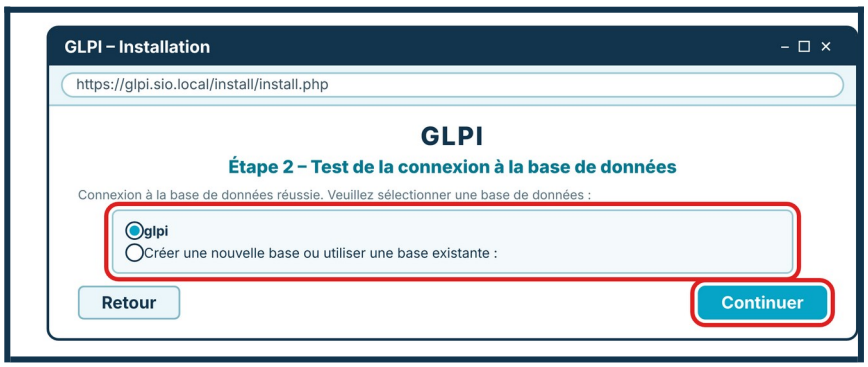


Figure 21 – Assistant GLPI : choix de la base de données

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** :

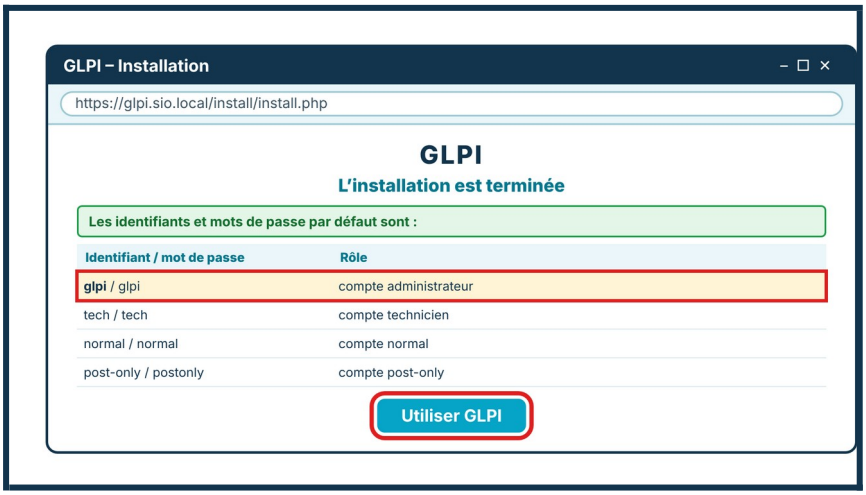


Figure 22 – Assistant GLPI : installation terminée

À SAVOIR

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

D – Sécuriser immédiatement

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



Figure 23 – 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 (SRV-GLPI)

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

E – 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 2-F) s'en charge, on le déclare à GLPI : menu « **Configuration** » puis « **Actions automatiques** » :

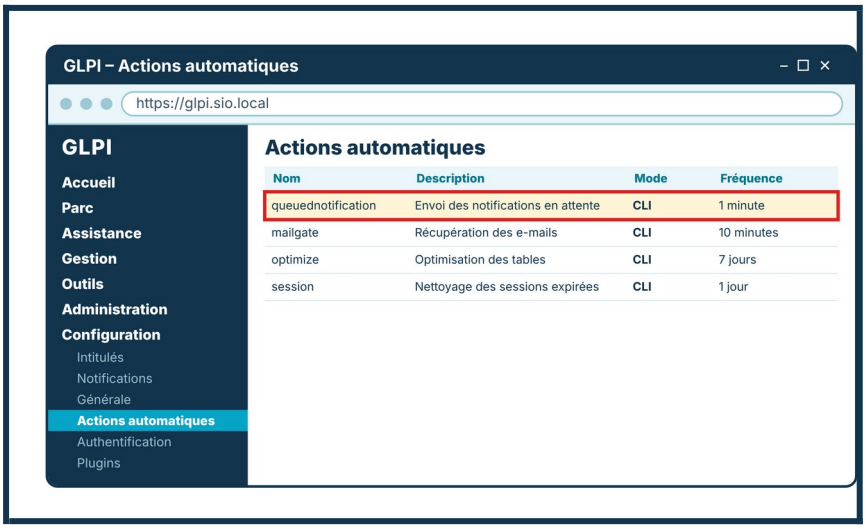


Figure 24 – Configuration > Actions automatiques

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 (SRV-GLPI)

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

F – Déclarer l'adresse publique de GLPI

GLPI construit certains liens à partir de son **URL de l'application** : ceux des notifications envoyées par e-mail, par exemple. Elle doit contenir l'adresse que connaissent les utilisateurs, et non celle du serveur. Menu « **Configuration** » puis « **Générale** », champ « **URL de l'application** » : saisissez `https://glpi.sio.local` (sans barre oblique finale), puis enregistrez.

G – Fermer l'accès direct à GLPI

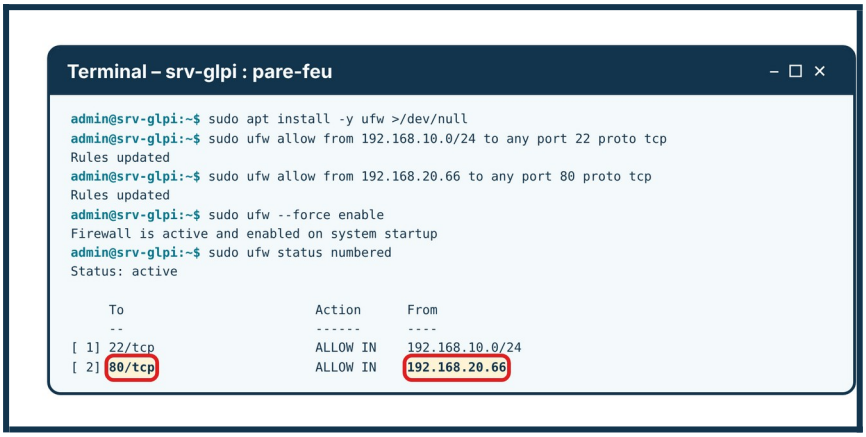
Tant qu'Apache répond à tout le monde, un utilisateur peut contourner Traefik (et donc le HTTPS) en saisissant `http://192.168.20.62`. On installe un pare-feu sur SRV-GLPI qui n'autorise que l'indispensable : le **SSH** depuis le réseau d'administration et le **port 80 depuis Traefik seulement**.

TERMINAL (SRV-GLPI)

```
sudo apt install -y ufw
sudo ufw allow from 192.168.10.0/24 to any port 22 proto tcp
sudo ufw allow from 192.168.20.66 to any port 80 proto tcp
sudo ufw --force enable
sudo ufw status numbered
```

REMARQUE IMPORTANTE

Autorisez le SSH avant d'activer le pare-feu : une règle d'accès SSH erronée vous enferme dehors (adaptez le réseau d'administration 192.168.10.0/24 au vôtre). En cas de blocage, reprenez la main depuis la **console Proxmox** et saisissez `sudo ufw disable`. Gardez cette console ouverte pendant l'opération.



À SAVOIR

Le pare-feu refuse tout ce qui n'est pas listé (politique par défaut d'ufw : entrant refusé, sortant autorisé). Les connexions de GLPI vers l'annuaire (LDAPS, port 636) sont des connexions **sortantes** : elles ne sont pas concernées.

Figure 25 – Pare-feu de SRV-GLPI : seul Traefik joint le port 80

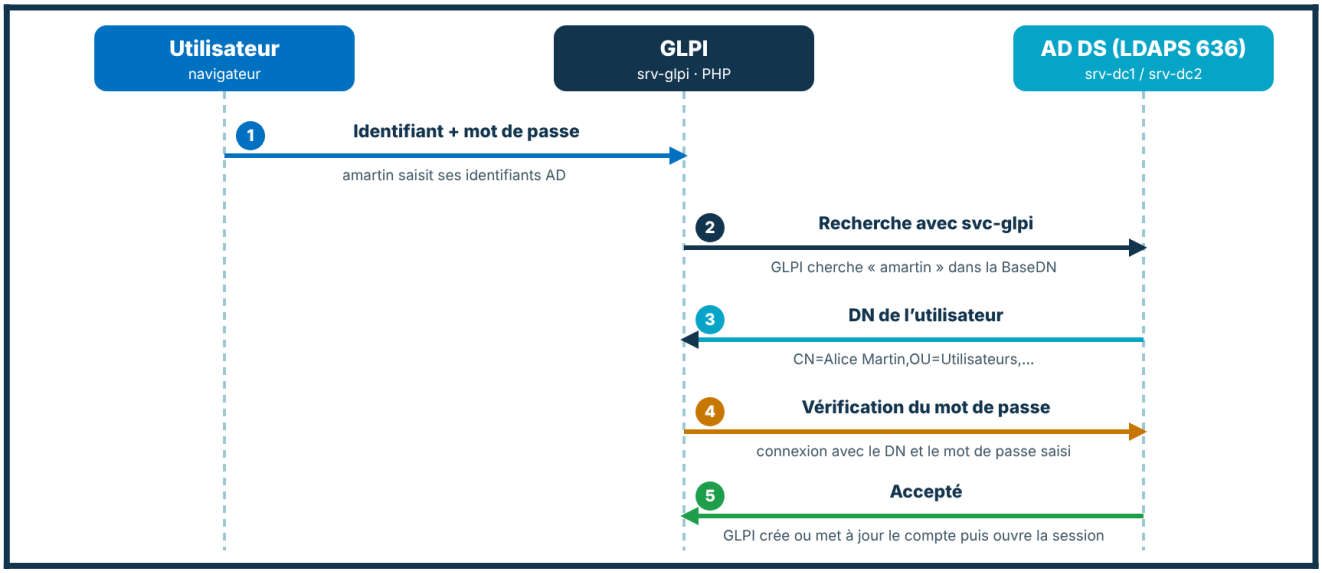
Contrôlez depuis le **poste d'administration** : `http://192.168.20.62` ne répond plus (le navigateur attend puis abandonne), alors que `https://glpi.sio.local` fonctionne toujours.

✔ POINT DE CONTRÔLE

- L'assistant s'est déroulé en **HTTPS** à l'adresse `https://glpi.sio.local` et la connexion fonctionne
- Le mot de passe de **glpi** est changé, les comptes `tech`, `normal` et `post-only` sont supprimés et `install/install.php` n'existe plus
- Le mode d'exécution des **actions automatiques** est **CLI**
- Le journal d'Apache affiche l'adresse du **poste d'administration**, pas celle de Traefik
- `http://192.168.20.62` est **inaccessible** depuis le poste d'administration

06 ÉTAPE 6 SUR 6 — Lier GLPI à l'annuaire AD DS

Pour authentifier les utilisateurs, GLPI interroge l'annuaire avec un **compte de service** (lecture seule), puis vérifie le mot de passe de chaque utilisateur. Voici ce qui se passe quand un utilisateur de l'annuaire se connecte :



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**). Chaque contrôleur présente un certificat délivré par **SIO-CA** ; il suffit que **SRV-GLPI fasse confiance à cette autorité**.

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 (SRV-DC1)

```
$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 (SRV-DC1)

```
$mdp = Read-Host -AsSecureString "Mot de passe des utilisateurs de test"
New-ADUser -Name "Alice Martin" -GivenName Alice -Surname Martin `
    -SamAccountName amartin -UserPrincipalName amartin@sio.local `
    -EmailAddress amartin@sio.local -Path "OU=Utilisateurs,$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 (SRV-DC1)

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

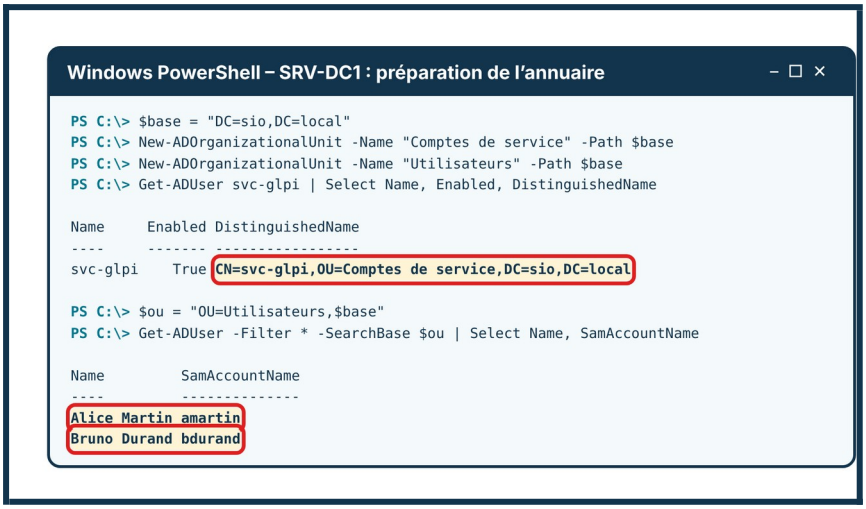


Figure 26 – PowerShell : OU, compte de service et utilisateurs

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 – Faire confiance à SIO-CA sur SRV-GLPI et tester LDAPS

Pour vérifier le certificat d'un contrôleur, un client n'a besoin que du **certificat de l'autorité**, pas de ceux des contrôleurs : un seul fichier couvre SRV-DC1, SRV-DC2 et tout futur contrôleur. C'est le fichier `sio-ca.cer` exporté à l'étape 4-F (refaites l'export si besoin). Depuis **SRV-DC1**, copiez-le vers **SRV-GLPI** :

POWERSHELL (SRV-DC1)

```
scp C:\Temp\sio-ca.cer admin@192.168.20.62:/tmp/
```

Sur **SRV-GLPI**, convertissez-le au format PEM, déclarez-le comme autorité de confiance et redémarrez PHP-FPM pour qu'il en tienne compte (PHP utilise le magasin de confiance du système). Installez ensuite l'outil de test LDAP :

TERMINAL (SRV-GLPI)

```
sudo openssl x509 -inform der -in /tmp/sio-ca.cer \
    -out /usr/local/share/ca-certificates/sio-ca.crt
sudo update-ca-certificates && sudo systemctl restart php8.4-fpm
sudo apt install -y ldap-utils
```

1. 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 (SRV-GLPI)

```
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
```

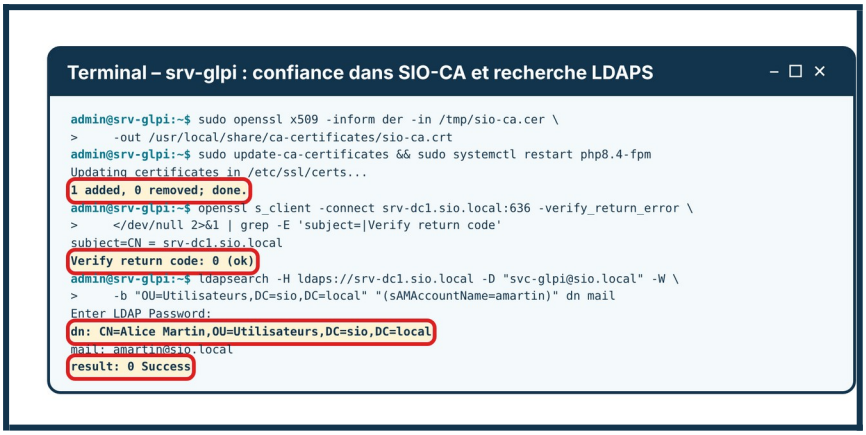


Figure 27 – Debian : confiance dans SIO-CA et recherche LDAPS

À SAVOIR

« Verify return code: 0 (ok) » prouve que SRV-GLPI fait confiance au certificat. « result: 0 Success » et la ligne `dn:` prouvent que le compte de service, la BaseDN et LDAPS fonctionnent. Répétez avec `srv-dc2.sio.local` : le même fichier suffit. Si `-inform der` échoue, le fichier est déjà au format PEM : copiez-le simplement.

À SAVOIR

Si vos contrôleurs utilisent des certificats **auto-signés** (tutoriel « natif » sans autorité), il n'y a pas de SIO-CA : exportez les certificats de SRV-DC1 et de SRV-DC2, convertissez-les en PEM et copiez-les tous deux dans `/usr/local/share/ca-certificates/`. Le reste du tutoriel est identique.

C – Déclarer l'annuaire AD DS dans GLPI

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** » :

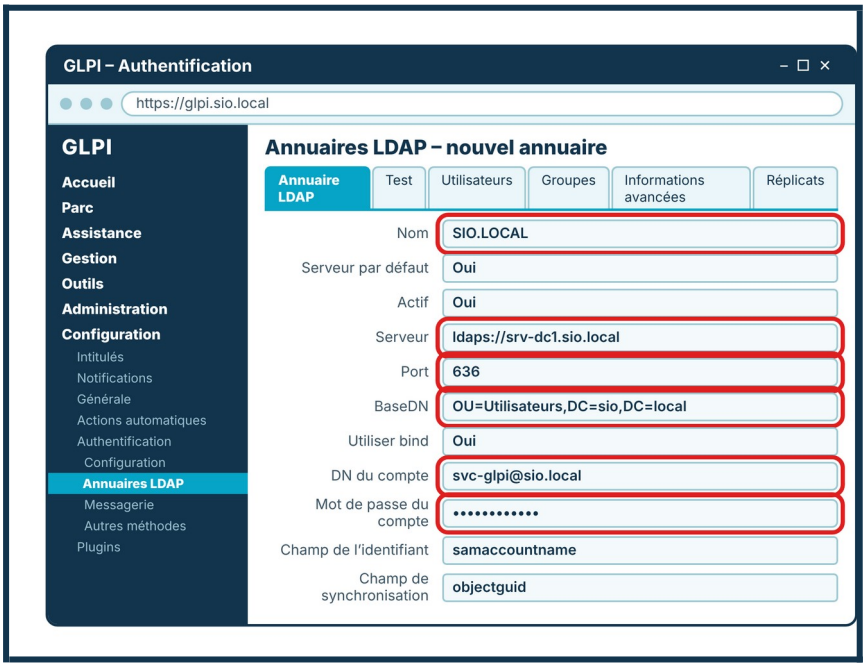


Figure 28 – Annuaires LDAP : formulaire de l'annuaire SIO.LOCAL

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

D – 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 :

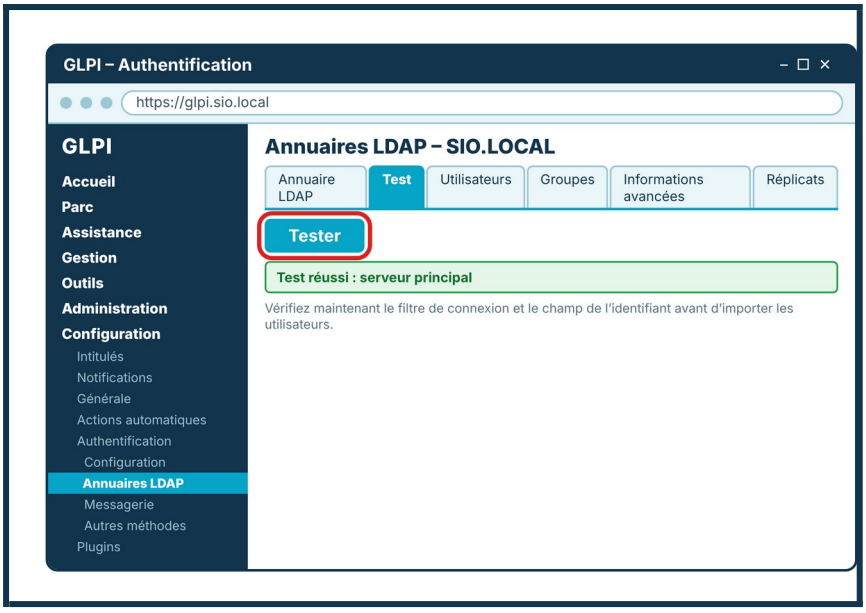


Figure 29 – Annuaire SIO.LOCAL : onglet Test

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 :

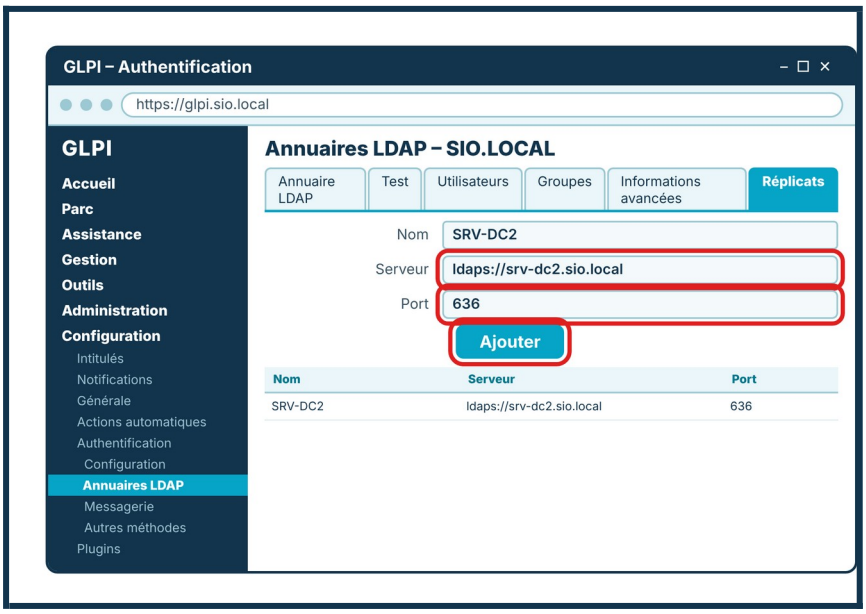


Figure 30 – Annuaire SIO.LOCAL : onglet Réplicats

À SAVOIR

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

E – 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** » :

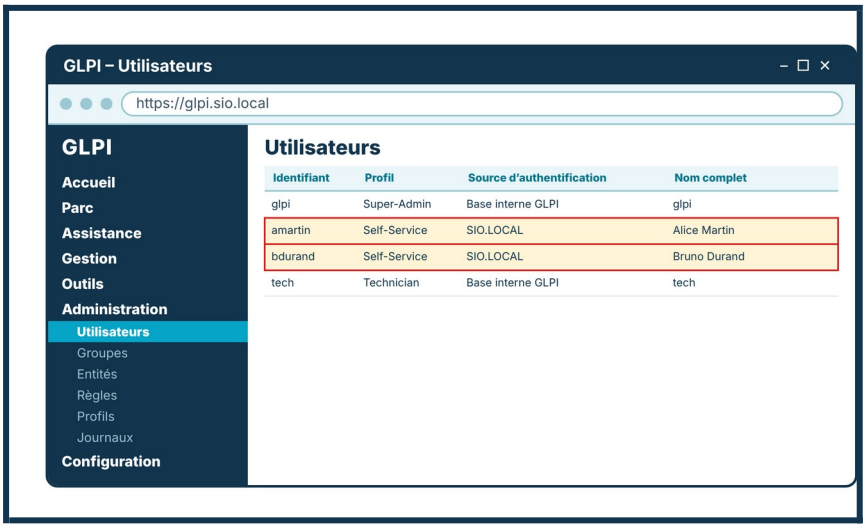


Figure 31 – Importation de nouveaux utilisateurs

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 :



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 »).

Figure 32 – Administration > Utilisateurs : comptes importés

F – Se connecter avec un compte Windows

1 Déconnectez-vous de GLPI, puis ouvrez `https://glpi.sio.local` dans une **fenêtre de navigation privée** : saisissez **amartin**, son mot de passe de domaine, et sélectionnez **SIO.LOCAL** dans « Connexion à » :



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. Le mot de passe circule chiffré de bout en bout : HTTPS entre le navigateur et Traefik, puis LDAPS entre GLPI et le contrôleur.

Figure 33 – Page de connexion de GLPI avec l'annuaire

2 **Pour aller plus loin** : la commande `glpi:ldap:synchronize_users` de `bin/console` synchronise les utilisateurs en masse (planifiable)

✔ 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**, à l'adresse `https://glpi.sio.local`
- Si SRV-DC1 est arrêté, la connexion fonctionne encore grâce à **SRV-DC2**

Notre GLPI est **opérationnel et publié en HTTPS** : les utilisateurs ne connaissent que `https://glpi.sio.local`, Apache n'est joignable que par Traefik, et les comptes Windows servent de comptes GLPI. Une autre application publiée derrière Traefik, c'est un nouveau fichier dans `/etc/traefik/dynamic`.

Dépannage : les symptômes les plus fréquents

Symptôme	Cause probable	Solution
Le service traefik ne démarre pas	Erreur dans `traefik.yml`, ou droits insuffisants sur `/etc/traefik` ou `/var/log/traefik`	`sudo journalctl -u traefik -n 20` ; contrôler l'indentation ; `sudo chown -R traefik:traefik /etc/traefik /var/log/traefik`
`certreq` **: « Refusé » ou « En attente »**	Le modèle « Serveur Web » n'est pas publié sur SIO-CA ou le compte n'a pas le droit « Inscrire »	Console `certsrv` > Modèles de certificats > Nouveau > Modèle à délivrer ; vérifier les droits du modèle
Avertissement de certificat dans le navigateur	Poste hors domaine (SIO-CA inconnue), nom absent des noms alternatifs ou certificat expiré	Importer SIO-CA ; vérifier `openssl x509 -noout -ext subjectAltName` ; contrôler `-enddate`
« 404 page not found » (réponse de Traefik)	Aucun routeur ne correspond : nom absent du DNS ou de la règle `Host`, fichier invalide ou non chargé	`getent hosts glpi.sio.local` ; relire `glpi.yml` ; consulter le journal et le tableau de bord
« 502 Bad Gateway »	Traefik ne joint pas Apache : service arrêté, mauvaise adresse, pare-feu	Depuis SRV-TRAEFIK : `curl -sI http://192.168.20.62` ; vérifier `systemctl status apache2` et `sudo ufw status`
« 403 Forbidden » sur `traefik.sio.local`	L'adresse du poste n'est pas dans `sourceRange`	Ajouter le réseau du poste dans `middlewares.yml` (rechargement automatique)
Page « Apache2 Debian Default Page »	Le site par défaut est resté actif	`sudo a2dissite 000-default && sudo a2ensite glpi && sudo systemctl reload apache2`
Impossible de rester connecté à GLPI, ou retour à la page de connexion	Cookie « sécurisé » envoyé alors que la page est vue en HTTP, ou `session.cookie_secure` sans HTTPS	Toujours passer par `https://glpi.sio.local` ; relire l'étape 5-A et redémarrer `php8.4-fpm`
Le journal d'Apache affiche l'adresse de Traefik	Module remoteip non activé ou adresse de `RemoteIPInternalProxy` incorrecte	`apache2ctl -M | grep remoteip` ; relire `proxy-traefik.conf` ; `sudo systemctl restart apache2`
Accès SSH perdu après activation du pare-feu	Règle du port 22 absente ou réseau d'administration incorrect	Console Proxmox : `sudo ufw disable`, corriger la règle, réactiver
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 »	SIO-CA non reconnue par SRV-GLPI, nom différent du certificat ou port 636 bloqué	Refaire l'étape 6-B ; 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

Pense-bête : commandes et emplacements

Commande / emplacement	Utilité
`sudo systemctl status traefik`	État de Traefik (`restart` après une modification de `traefik.yml`)
`sudo journalctl -u traefik -f`	Journal de Traefik en direct (erreurs de fichiers, de certificat)
`/var/log/traefik/access.log`	Journal des requêtes : routeur et service utilisés pour chacune
`/etc/traefik/dynamic/*.yml`	Configuration dynamique : rechargée à chaud, un fichier par sujet (dont `glpi.yml`)
`/etc/traefik/certs/`	Certificat et clé privée (clé lisible uniquement par `traefik`)
`openssl x509 -in /etc/traefik/certs/glpi.crt -noout -enddate`	Date d'expiration du certificat : à surveiller, renouvellement en suivant l'étape 3 (E à G)
`https://traefik.sio.local`	Tableau de bord de Traefik : routeurs, services, middlewares, erreurs
`sudo ufw status numbered`	Règles du pare-feu de SRV-GLPI
`systemctl status apache2 php8.4-fpm mariadb`	État des trois services de SRV-GLPI
`sudo -u www-data php /var/www/glpi/bin/console`	Console GLPI : maintenance, synchronisation LDAP, mises à jour
`/var/log/glpi/` **et** `/var/log/apache2/glpi-*.log`	Journaux de GLPI (`php-errors.log`, `sql-errors.log`) et d'Apache (accès et erreurs)
`/etc/glpi/` **et** `/var/lib/glpi/`	Configuration, clé de chiffrement (`glpicrypt.key`) et documents joints : à sauvegarder avec la base
Configuration > Authentification > Annuaires LDAP	Déclarer, tester et dupliquer les annuaires (réplicats)
`ldapsearch -H ldaps://… -D … -W`	Tester l'annuaire sans passer par GLPI