Configuration de GLPI en HTTPS

DELZOR THOMAS

2025

GLPI

Configuration de GLPI en HTTPS avec certificat SSL (auto-signé)

✨ Introduction

Cette procédure vise à mettre en place le protocole HTTPS sur une instance GLPI afin de sécuriser les échanges entre les utilisateurs et le serveur. Elle est particulièrement utile dans un environnement interne ou de test, en utilisant un certificat SSL auto-signé.

> GLPI (Gestionnaire Libre de Parc Informatique) est une application web permettant de gérer un inventaire de parc informatique et de mettre en place une gestion des demandes d'assistance. Elle est très utilisée dans les collectivités, les entreprises, les établissements scolaires, etc.

> Pourquoi passer GLPI en HTTPS ?

> Par défaut, GLPI est accessible en HTTP (port 80), ce qui signifie que les données transitent en clair sur le réseau. Cela représente un risque important pour la confidentialité et l'intégrité des informations.

> L'HTTPS (port 443) permet de :

> 🔐 Chiffrer les communications entre le navigateur et le serveur

> 🛡️ Éviter l'interception de mots de passe ou de données sensibles

> 🔒 Protéger contre les attaques de type "man-in-the-middle"

> Dans cette procédure, nous allons utiliser un **certificat SSL auto-signé**, qui permet de bénéficier du chiffrement même sans autorité de certification officielle (utile pour les tests ou les environnements privés).

📜 Étape 1 : Création du certificat SSL auto-signé

Lancez la commande suivante :

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
-keyout /etc/ssl/private/glpi-selfsigned.key \
-out /etc/ssl/certs/glpi-selfsigned.crt
```

Pendant la création, plusieurs informations vous seront demandées. Pour le champ **"Common Name (e.g. server FQDN or YOUR name)"**, saisissez **l'adresse IP ou le nom de domaine** de votre serveur GLPI.

Cela permettra d'associer le certificat à la bonne adresse.

🛠️ Étape 2 : Configuration du site Apache pour utiliser HTTPS

Éditez le fichier de configuration du site GLPI :

```
sudo nano /etc/apache2/sites-available/glpi.conf
```

Ajoutez les lignes suivantes à l'intérieur du bloc `<VirtualHost *:443>` (ou créez ce bloc si nécessaire)

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

Exemple de configuration complète :

```
<VirtualHost *:443>
    ServerName glpi.mondomaine.local
    DocumentRoot /var/www/glpi

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

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

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

> Remplacez glpi.mondomaine.local par votre nom de domaine ou IP locale si besoin.

⚙️ Étape 3 : Activation du SSL sur Apache

Activez le module SSL et redémarrez Apache :

```
sudo a2enmod ssl
sudo systemctl restart apache2
```

✅ Étape 4 : Vérification

Dans votre navigateur, accédez à l'adresse :

```
https://IP_DU_SERVEUR
```

🎯 Conclusion

Votre instance GLPI est désormais accessible de manière sécurisée via HTTPS (port 443). Cela renforce la confidentialité et la sécurité des échanges avec votre plateforme.