Chapitre 5 - Sécurité et sauvegardes

HTTPS, reverse proxy, permissions, sauvegarde et restauration.

HTTPS et reverse proxy Caddy

HTTPS et reverse proxy Caddy

10.1 Exemple avec Caddy

Sur le serveur Caddy :

```
glpi.dreamsaphir.fr {
    reverse_proxy 192.168.1.100:80
}
```

Puis :

```
sudo caddy validate --config /etc/caddy/Caddyfile
sudo systemctl reload caddy
```

Le DNS public doit pointer vers Caddy et les ports 80/443 doivent arriver sur Caddy, pas directement sur le serveur GLPI.

10.2 Conserver l’adresse IP du client

Si Apache n’est accessible que depuis Caddy, activer `mod_remoteip` :

```
sudo a2enmod remoteip
```

Ajouter dans le VirtualHost, en remplaçant l’adresse de Caddy :

```
RemoteIPHeader X-Forwarded-For
RemoteIPTrustedProxy 192.168.1.10
```

Puis :

```
sudo apache2ctl configtest
sudo systemctl reload apache2
```

Ne jamais faire confiance à `X-Forwarded-For` provenant de n’importe quelle adresse.

> Documentation GLPI 11 — Debian 12, Apache, PHP 8.2 et MariaDB.

Sécurité, pare-feu et clés de chiffrement

Sécurité, pare-feu et clés de chiffrement

10.3 Pare-feu

Si Caddy est sur une autre machine, autoriser le port 80 uniquement depuis son adresse :

```
sudo apt install -y nftables
```

La politique exacte dépend du pare-feu déjà présent. Ne pas activer une nouvelle politique restrictive à distance avant d’avoir explicitement autorisé SSH et vérifié la console de secours.

10.4 Mesures indispensables

- utiliser HTTPS uniquement ;
- pointer Apache vers `/var/www/glpi/public` ;
- changer ou désactiver les comptes par défaut ;
- activer la MFA pour les administrateurs ;
- appliquer rapidement les versions de sécurité ;
- sauvegarder la base, les documents, la configuration et les clés ;
- limiter les droits MariaDB à la seule base `glpi` ;
- utiliser LDAPS plutôt que LDAP simple ;
- limiter l’accès SSH aux administrateurs ;
- ne pas exposer MariaDB sur Internet ;
- maintenir Debian, Apache, PHP et les plugins ;
- vérifier régulièrement les journaux ;

- tester les restaurations ;
- limiter les données personnelles collectées au strict besoin.

10.5 Clés de chiffrement

GLPI utilise des clés pour chiffrer certaines informations sensibles. Les fichiers présents dans `/etc/glpi`, notamment `glpi.key`, `glpicrypt.key`, `oauth.pem` et `oauth.pub` selon la configuration, doivent faire partie de chaque sauvegarde.

La perte de la base seule est grave. La perte de la base accompagnée des clés peut rendre certaines données chiffrées définitivement inutilisables.

> Documentation GLPI 11 — Debian 12, Apache, PHP 8.2 et MariaDB.

Sauvegarde complète de GLPI

Sauvegarde complète de GLPI

Une sauvegarde GLPI complète contient au minimum :

1. la base MariaDB ;
2. `/etc/glpi` ;
3. `/var/lib/glpi/files` ;
4. `/var/lib/glpi/marketplace` ;
5. `/var/www/glpi/inc/downstream.php` ;
6. la configuration Apache et, si utilisé, Caddy.

Un snapshot de VM est pratique avant une opération, mais ne remplace pas une sauvegarde exportée et testée.

11.1 Sauvegarde manuelle

Créer un dossier daté :

```
sudo install -d -m 0700 /var/backups/glpi
BACKUP_DATE="$(date +%F_%H-%M-%S)"
sudo install -d -m 0700 "/var/backups/glpi/${BACKUP_DATE}"
```

Sauvegarder la base :

```
sudo mariadb-dump \
  --single-transaction \
  --quick \
```

```
  --routines \
  --triggers \
  glpi \
  | sudo gzip \
  > "/var/backups/glpi/${BACKUP_DATE}/glpi-database.sql.gz"
```

Sauvegarder les fichiers :

```
sudo tar -czf \
  "/var/backups/glpi/${BACKUP_DATE}/glpi-files.tar.gz" \
  /etc/glpi \
  /var/lib/glpi/files \
  /var/lib/glpi/marketplace \
  /var/www/glpi/inc/downstream.php \
  /etc/apache2/sites-available/glpi.conf
```

Contrôler :

```
sudo ls -lh "/var/backups/glpi/${BACKUP_DATE}"
sudo gzip -t \
  "/var/backups/glpi/${BACKUP_DATE}/glpi-database.sql.gz"
sudo tar -tzf \
  "/var/backups/glpi/${BACKUP_DATE}/glpi-files.tar.gz" \
  | head
```

Copier ensuite cette sauvegarde vers un autre serveur ou support. Une sauvegarde conservée uniquement sur la VM GLPI ne protège pas contre la perte de cette VM.

> Documentation GLPI 11 — Debian 12, Apache, PHP 8.2 et MariaDB.

Restauration de GLPI

Restauration de GLPI

11.2 Restauration de la base

Activer la maintenance :

```
cd /var/www/glpi
sudo -u www-data php bin/console glpi:maintenance:enable
```

Recréer une base vide :

```
sudo mariadb
```

```
DROP DATABASE glpi;
CREATE DATABASE glpi
  CHARACTER SET utf8mb4
  COLLATE utf8mb4_unicode_ci;
GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

Restaurer :

```
sudo gzip -dc \
  /var/backups/glpi/DATE/glpi-database.sql.gz \
  | sudo mariadb glpi
```

Restaurer les fichiers :

```
sudo tar -xzf \
  /var/backups/glpi/DATE/glpi-files.tar.gz \
  -C /
```

Rétablir les permissions :

```
sudo chown -R www-data:www-data \
  /etc/glpi \
  /var/lib/glpi \
  /var/log/glpi
```

Contrôler puis désactiver la maintenance :

```
cd /var/www/glpi
sudo -u www-data php bin/console glpi:system:check_requirements
sudo -u www-data php bin/console db:check_schema_integrity
sudo -u www-data php bin/console glpi:maintenance:disable
```

Ne jamais restaurer une sauvegarde sur une base ayant déjà subi une migration partielle. Recréer une base vide avant une nouvelle tentative.

> Documentation GLPI 11 — Debian 12, Apache, PHP 8.2 et MariaDB.