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.

Revision #1
Created 2026-07-27 03:45:50 CEST by Admin
Updated 2026-07-27 03:45:50 CEST by Admin