|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | |  | |
| Documentation technique | | |  | |
|  | | |  | |
|  | | | 27/02/2024**Installation et configuration d'un outil d'inventaire et de ticketing (GLPI)** | |
|  | | |  | |
|  |  |  | |  | |
|  | Définition *GLPI est un logiciel libre de gestion de parc informatique et de helpdesk, conçu pour aider les entreprises à inventorier leurs ressources informatiques (matériels, logiciels) et à gérer les demandes d'assistance de leurs utilisateurs. Facile à utiliser et modulaire, GLPI permet aux administrateurs de suivre l'ensemble de leurs équipements informatiques, de planifier des maintenances et de gérer efficacement les incidents et demandes de support. C'est un outil clé pour optimiser l'utilisation des ressources informatiques et améliorer le support aux utilisateurs.* | | |  | |

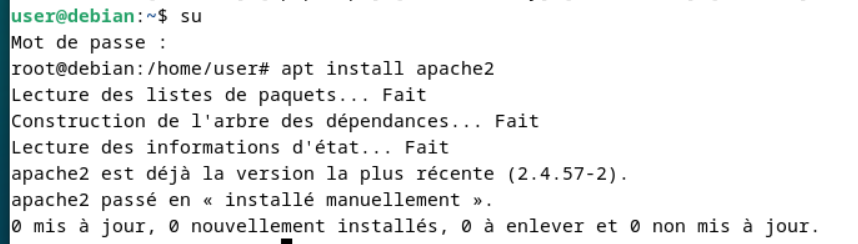
### Prérequis

Pour cette documentation, il y a plusieurs prérequis nécessaires :

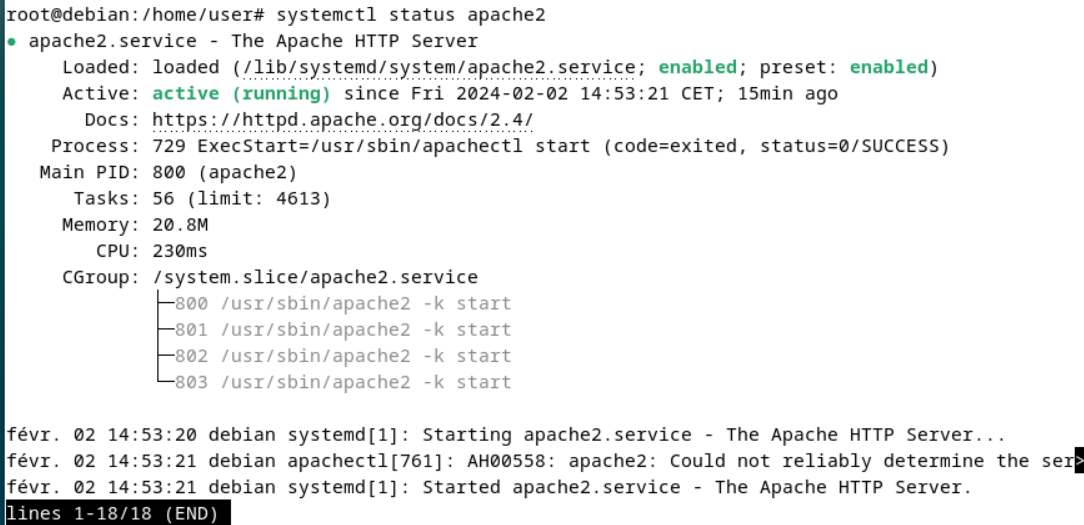
* Une clé USB vide pour booter,
* L’ISO Proxmox Backup Server disponible sur <https://www.proxmox.com/en/downloads>,
* Une tour qui pourra héberger le serveur de backup (minimum 256 Go de stockage),
* Un Serveur Proxmox Virtual Environnement fonctionnel.

### Installation de GLPI

On se connecte avec le root pour se mettre en admin afin de ne pas être obligé de mettre “sudo” à chaque début de commande.  
  
Nous installons également le serveur web apache2 sur notre Debian afin d’héberger l’interface web de GLPI sur ce serveur apache.



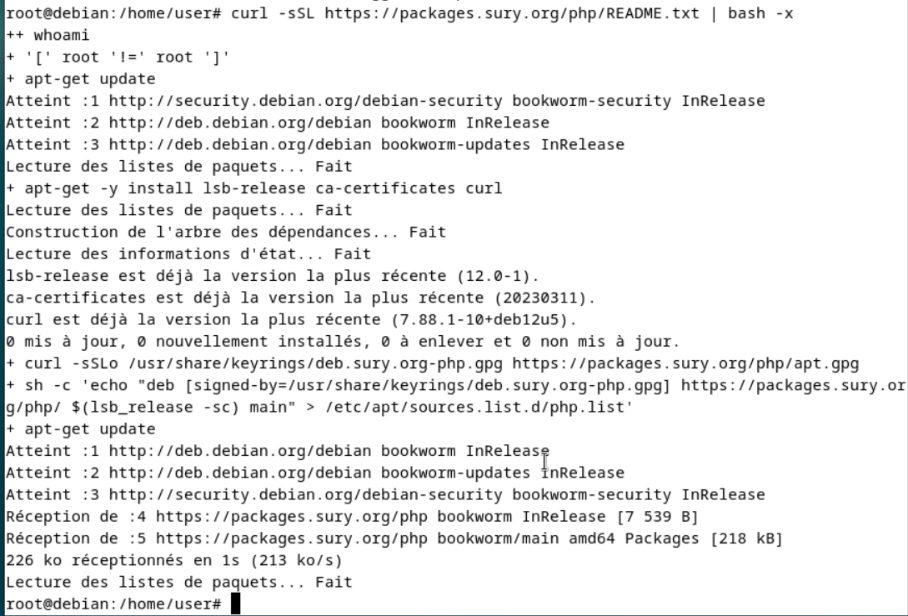
Nous utilisons la commande ‘systemctl status apache2’ pour vérifier que le service Apache est bien actif et en cours d'exécution sur le serveur, ce qui est essentiel pour confirmer que notre serveur web est prêt à héberger l'interface web de GLPI.



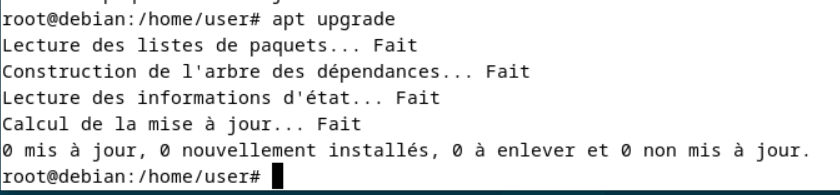
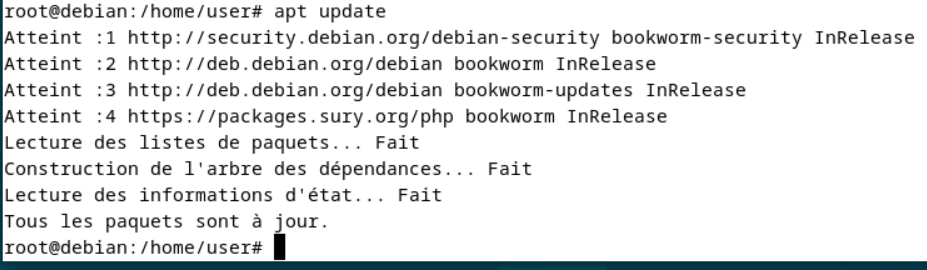
Nous exécutons la commande ‘apt install ca-certificates apt-transport-https software-properties-common’ pour s'assurer que notre système est capable de gérer les sources de paquets sécurisées via HTTPS et de vérifier l'authenticité des paquets téléchargés grâce aux certificats d'autorité, un prérequis pour l'installation et la maintenance sécurisée de GLPI et de ses dépendances sur notre serveur.



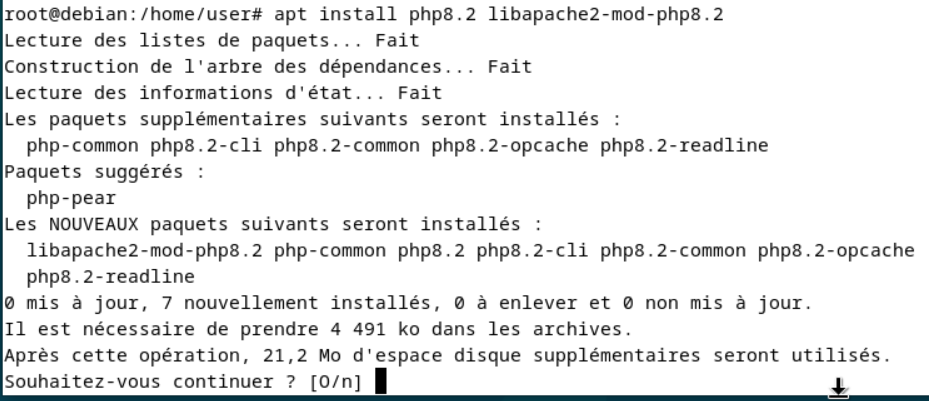
Nous utilisons des commandes comme ‘curl’ et ‘apt-get update’ pour ajouter un nouveau dépôt de PHP et mettre à jour la liste des paquets, afin d'installer la dernière version de PHP nécessaire pour GLPI.



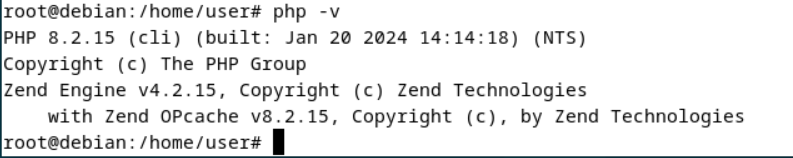
‘apt update’ synchronise les listes de paquets et ‘apt upgrade’ installe les mises à jour, assurant la sécurité et l'actualité du système Debian.



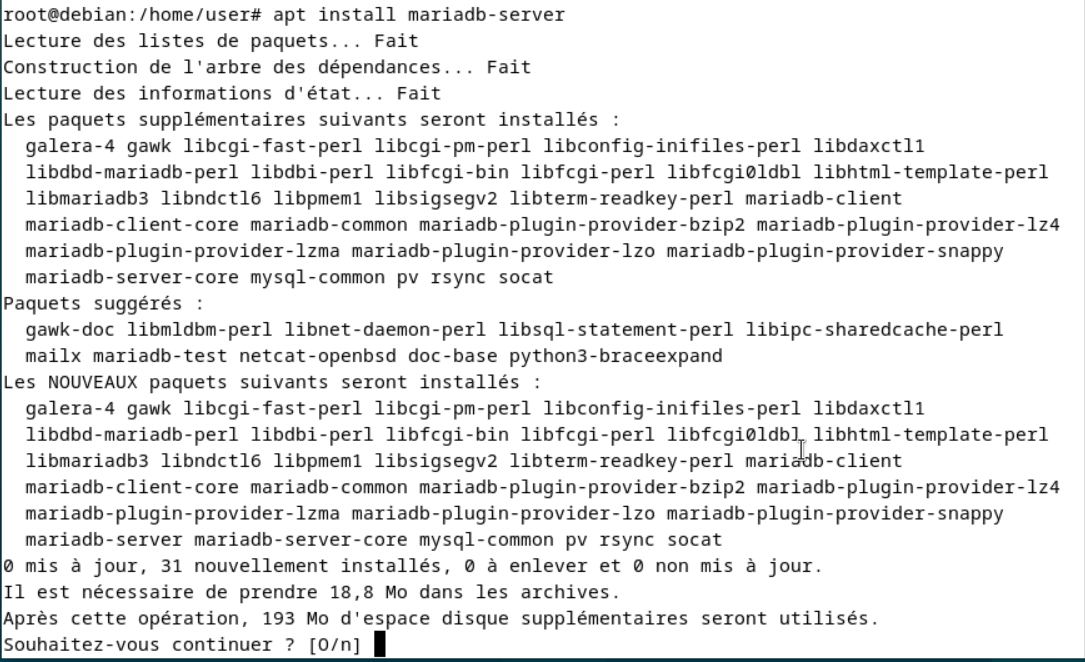
La commande ‘apt install php8.2 libapache2-mod-php8.2’ installe PHP 8.2 et son module Apache pour exécuter des applications PHP comme GLPI sur le serveur web.



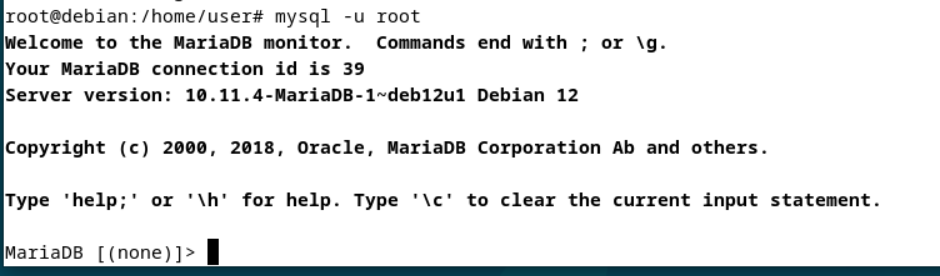
La commande ‘php -v’ est utilisée pour afficher la version actuelle de PHP installée sur le système, permettant de confirmer que nous disposons de la bonne version pour la compatibilité avec GLPI.



Nous lançons ‘apt install mariadb-server’ pour installer le serveur de base de données MariaDB, qui est nécessaire pour stocker et gérer les données de l'application GLPI de manière sécurisée et efficace.



Nous utilisons ‘mysql -u root’ pour accéder à MariaDB et effectuer des tâches administratives telles que créer des utilisateurs, attribuer des privilèges et établir des bases de données pour GLPI. Cela nous permet de sécuriser l'accès à GLPI et d'optimiser la gestion des données.



Dans ces commandes, nous allons d'abord créer une base de données ‘glpi’, puis un utilisateur ‘glpi’ avec des privilèges complets sur cette base, et enfin, nous actualisons les privilèges pour que les modifications prennent effet immédiatement. Cela établit l'environnement nécessaire pour que l'application GLPI fonctionne avec les bonnes permissions.



La commande ‘wget’ suivie de l'URL indiquée télécharge la dernière version de l'application GLPI à partir de GitHub, ce qui nous permet de récupérer l'archive contenant les fichiers nécessaires à l'installation de GLPI sur notre serveur.



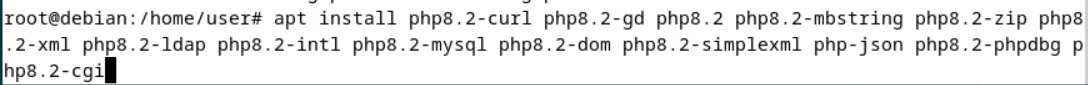
La commande ‘tar xvf glpi-10.0.6.tgz’ extrait les fichiers de GLPI depuis l'archive.



Cette commande déplace le dossier GLPI extrait vers le répertoire racine du serveur web pour finaliser son installation.



Ces extensions PHP sont installées pour garantir la compatibilité et la fonctionnalité complète de GLPI, car elles permettent le traitement d'images, la gestion de chaînes de caractères et la connexion à des bases de données.



Cette commande est utilisée pour attribuer la propriété du répertoire GLPI au serveur web, ce qui assure que le serveur a les permissions appropriées pour lire et écrire dans le dossier de GLPI.



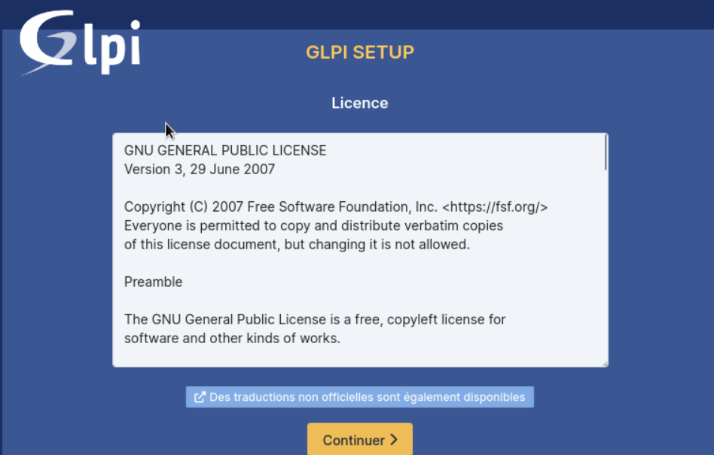
Nous ajustons les droits d'accès du dossier GLPI pour le propriétaire, le groupe et les autres utilisateurs, garantissant le bon fonctionnement de l'application sur le serveur web.



Nous accédons à l'interface web de GLPI pour sélectionner la langue et commencer le processus d'installation et de configuration du système.



Sur cette page de l'interface web de GLPI, nous devons cliquer sur ‘Continuer’ après avoir lu les termes de la licence GNU General Public License pour procéder à l'installation.



Nous choisissons l'option ‘Installer’ pour démarrer une nouvelle installation de GLPI, étant donné que nous n'effectuons pas une mise à jour d'une version précédente.



Nous sommes à l'étape de vérification des prérequis où le système confirme que toutes les extensions PHP nécessaires pour GLPI sont bien installées et actives.

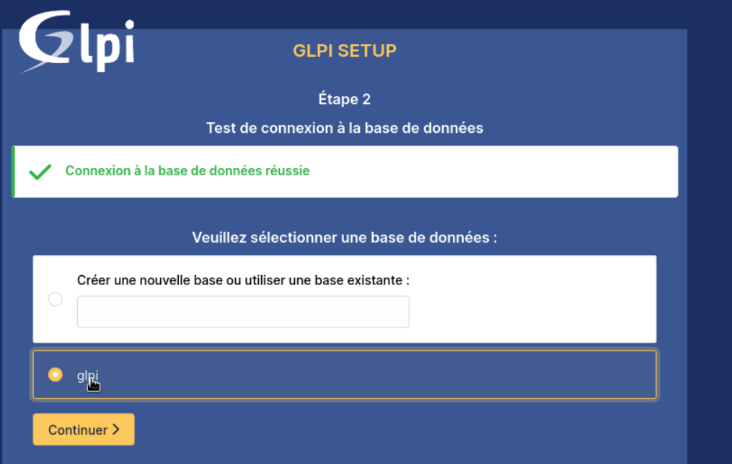
Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Sur l'interface de configuration de GLPI, nous utilisons l'utilisateur 'glpi' précédemment créé dans MariaDB pour établir la connexion à la base de données dédiée à GLPI.



On sélectionne notre base de données ici pour continuer la configuration de GLPI.



On vient d’initialiser la base de données et il ne reste plus qu'à cliquer sur ‘Continuer’ pour aller à l’étape suivante du setup de GLPI.



L'installation de GLPI est terminée, et on peut voir les identifiants par défaut pour les différents comptes. Maintenant, on peut cliquer sur "Utiliser GLPI" pour démarrer.



On se connecte à notre compte GLPI en utilisant les identifiants par défaut, puisque c’est la première fois qu’on y accède.



### Résolution Message d’avertissement

On est sur le tableau de bord de GLPI en tant que Super-Admin, et on va commencer par changer les mots de passe par défaut des utilisateurs pour des raisons de sécurité, comme indiqué par le premier message d'erreur.

Une image contenant texte, Police, capture d’écran

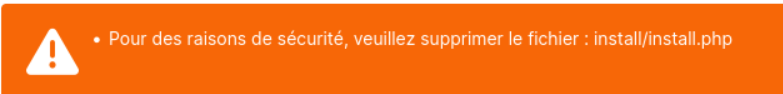
Description générée automatiquement

Une image contenant texte, capture d’écran

Description générée automatiquementNous devons modifier le mot de passe pour les différents comptes GLPI, y compris les comptes ‘glpi’, ‘post-only’, ‘tech’ et ‘normal’ afin de résoudre le premier message d’avertissement.  
Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Pour éliminer ce risque de sécurité ci-dessous, nous allons supprimer le fichier ‘install/install.php’, empêchant ainsi un accès non autorisé à l'outil d'installation de GLPI.



- La commande ‘cd /var/www/html/glpi’ est utilisée pour naviguer vers le dossier racine de l'installation GLPI sur le serveur.

- Ensuite, ‘ls’ est exécutée pour afficher le contenu de ce dossier, permettant de vérifier que le dossier ‘install’ est bien présent.

- La commande ‘cd install’ permet de se déplacer dans le dossier ‘install’, qui contient le script d'installation.

- Un second ‘ls’ est utilisé pour lister les fichiers dans le dossier ‘install’, ce qui confirme la présence du fichier ‘install.php’ à supprimer.

La raison derrière ces commandes est de naviguer dans le système de fichiers pour localiser puis supprimer le fichier ‘install.php’ pour des raisons de sécurité, comme recommandé par GLPI.

Une image contenant texte, Police, capture d’écran, blanc

Description générée automatiquement

La commande ‘rm -rf install.php’ a été exécutée pour supprimer définitivement le fichier ‘install.php’ du dossier d'installation de GLPI. Cela permet donc de résoudre le message d’incident.



Le message d’avertissement indique que la configuration actuelle du dossier racine du serveur web n'est pas sécurisée car elle permet l'accès à des fichiers non publics. Il faut donc ajuster les permissions ou la configuration du serveur pour restreindre cet accès et assurer la sécurité des données.



Pour résoudre le problème, on exécute la commande ‘nano glpi/src/System/Requirement/SafeDocumentRoot.php’ pour ouvrir le fichier en question dans l'éditeur de texte Nano, afin de modifier les configurations pour sécuriser le dossier racine du serveur web.

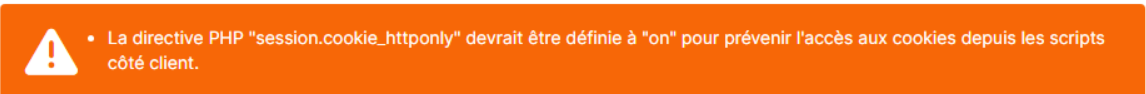


Il suffit d'ajouter la ligne ‘return;’ dans le fichier ‘SafeDocumentRoot.php’ pour répondre à ce message d'avertissement et sécuriser la configuration.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

L’avertissement indique qu’il faut activer la directive `session.cookie\_httponly` dans la configuration PHP. En mettant cette option à "on", on augmente la sécurité en empêchant les scripts côté client d’accéder aux cookies de session.



On utilise cette commande pour ouvrir le fichier de configuration PHP avec l'éditeur Nano, afin de modifier la directive concernant les cookies de session pour renforcer la sécurité.



Une fois dans le document, nous modifions la ligne ‘session.cookie\_httponly’ en y ajoutant ‘on’, pour renforcer la sécurité des cookies de session. Selon les versions de PHP, on pourrait aussi mettre ‘true’ à la place de ‘on’.

Une image contenant capture d’écran, Police, texte

Description générée automatiquement

Après avoir modifié le fichier, on le quitte en s’assurant de sauvegarder les modifications, puis on exécute la commande ‘systemctl restart apache2’. Cela permet de redémarrer le serveur web Apache pour que les modifications de configuration PHP prennent effet.

