Compte Rendu: Installation de GLPI

1. Objectif du projet

L'objectif est d'installer et de configurer la solution open-source **GLPI (Gestionnaire Libre de Parc Informatique)** pour répondre aux besoins de gestion de tickets d'une organisation. L'installation repose sur une architecture de serveur web standard (LAMP).

2. Procédure Technique

Étape 1 : Préparation du système

Mise à jour des dépôts et des paquets installés pour garantir la stabilité du serveur.

```
sudo apt-get update && sudo apt-get upgrade
```

Étape 2 : Installation de la pile LAMP

Installation du serveur Web Apache, du moteur PHP et du gestionnaire de base de données MariaDB.

```
sudo apt-get install apache2 php mariadb-server
```

Étape 3 : Installation des dépendances PHP spécifiques

GLPI nécessite des extensions PHP particulières pour le traitement des données (XML, JSON, base de données, graphismes).

```
sudo apt-get install php-xml php-common php-json php-mysql php-mbstring php-curl php-gd php-intl php-zip php-bz2 php-imap php-apc
```

Ajout de l'extension pour la future liaison avec un annuaire (LDAP) :

```
sudo apt-get install php-ldap
```

Étape 4 : Configuration de la base de données

1. Sécurisation du service SQL :
   Exécution du script de sécurisation (définition du mot de passe root, suppression des utilisateurs anonymes).

```
sudo mysql_secure_installation
```

2. Création de la base et de l'utilisateur dédié :
   Configuration d'un utilisateur spécifique pour GLPI afin d'appliquer le principe du moindre privilège.

```
sudo mysql -u root -p
```

```
-- Commandes SQL exécutées :
CREATE DATABASE db23_glpi;
GRANT ALL PRIVILEGES ON db23_glpi.* TO glpi_adm@localhost IDENTIFIED BY
"MotDePasseRobuste";
FLUSH PRIVILEGES;
EXIT;
```

Étape 5 : Déploiement des sources de GLPI

Téléchargement de l'archive officielle (version 10.0.20) et extraction dans le répertoire de publication du serveur Apache.

```
cd /tmp
wget https://github.com/glpi-project/glpi/releases/download/10.0.20/glpi-10.0.20.tgz
sudo tar -xzvf glpi-10.0.20.tgz -C /var/www/html/
```

Étape 6 : Gestion des permissions

Attribution de la propriété du dossier GLPI à l'utilisateur www-data (utilisateur exécutant Apache) pour permettre au serveur d'écrire dans les fichiers de configuration et les logs.

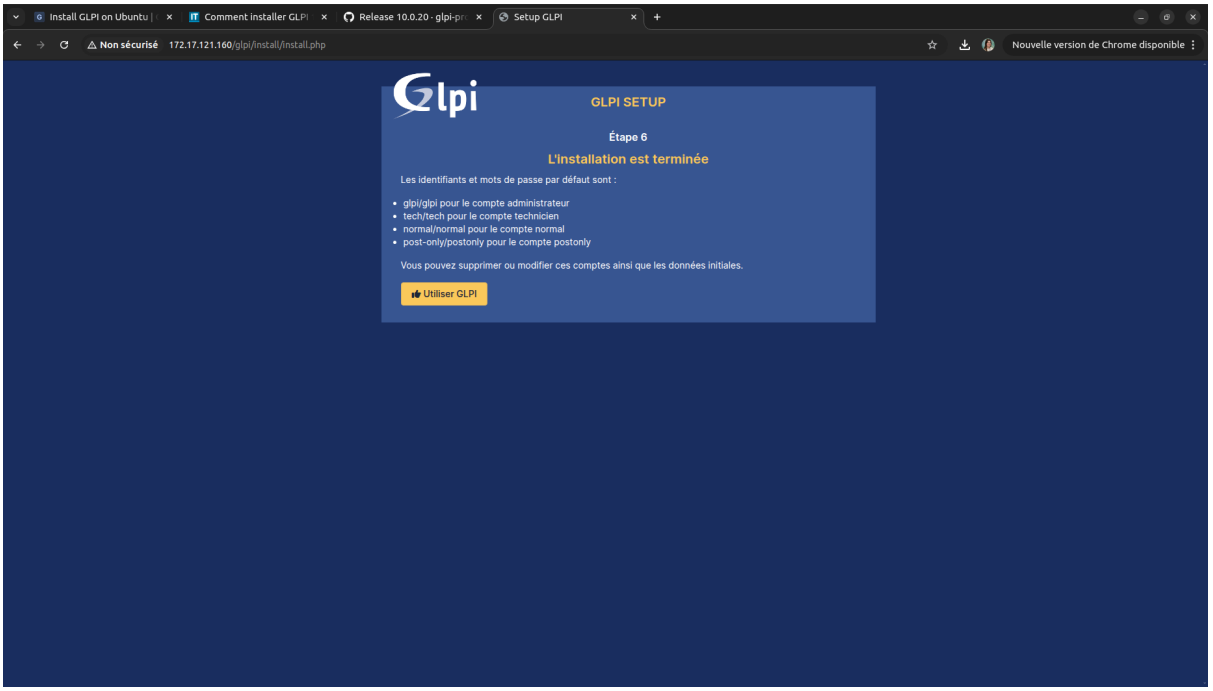
```
sudo chown www-data /var/www/html/glpi/ -R
```

3. Validation de l'installation

L'accès à l'interface de finalisation se fait via un navigateur web à l'adresse suivante :

http://[IP_DU_SERVEUR]/glpi/

L'installation a été confirmée par l'étape finale de l'assistant graphique, permettant l'accès aux comptes par défaut (glpi, tech, normal, post-only).



4. Conclusion

Le service GLPI est désormais opérationnel sur le serveur. La prochaine phase consistera à supprimer le fichier d'installation (install.php) par mesure de sécurité et à paramétrer les entités pour la gestion des tickets.

5. Maintenance curative : Récupération d'un compte administrateur

Contexte : Suite à une modification du mot de passe administrateur rendant l'accès impossible, une intervention directe en base de données a été nécessaire pour réinitialiser les identifiants.

Diagnostic et approche

Le compte `glpi` étant verrouillé, la solution retenue a été de modifier manuellement le hash du mot de passe dans la table des utilisateurs via MariaDB. Bien que GLPI 10 utilise des algorithmes de hachage modernes, l'injection d'un hash SHA1 (obsolète mais compatible pour la récupération) permet de forcer une connexion temporaire.

Procédure d'intervention

Connexion à l'instance MariaDB :

sudo mysql -u root -p

Sélection de la base de données GLPI :
USE db23_glpi;

Mise à jour du mot de passe du compte 'glpi' : L'utilisateur a été mis à jour avec un mot de passe connu (ici, le hash SHA1 correspondant au mot de passe souhaité).

UPDATE glpi_users SET password = 'ton_hash_sha1_ici' WHERE name = 'glpi';

FLUSH PRIVILEGES;

EXIT;

Vérification et durcissement :

- Connexion réussie à l'interface Web avec le nouveau mot de passe.
- **Action de sécurité :** Une fois connecté, le mot de passe a été immédiatement modifié via l'interface utilisateur de GLPI pour générer un hash sécurisé (bcrypt) aux normes actuelles de l'application.

6. Maintenance curative : Récupération du compte administrateur

Contexte : Suite à la perte du mot de passe du compte administrateur (glpi), l'accès à l'interface de gestion est devenu impossible. Une intervention technique directement dans la base de données a été nécessaire pour restaurer cet accès.

Diagnostic et approche technique

Le mot de passe initialement stocké en base de données utilise un hachage moderne de type **bcrypt**. Pour reprendre la main, la stratégie a consisté à remplacer ce hash par un hash **SHA-1**. Bien que le format SHA-1 soit techniquement obsolète, GLPI le reconnaît pour assurer la compatibilité, ce qui permet de forcer une connexion temporaire.

Procédure d'intervention

Les étapes suivantes ont été réalisées en ligne de commande sur le serveur de base de données :

1. **Connexion à MariaDB :** Accès au moteur de base de données avec les privilèges root. sudo mysql -u root -p
2. **Sélection de la base :** Utilisation de la base de données dédiée à l'application. USE db23_glpi;
3. **Modification du mot de passe :** Injection du hash SHA-1 (par exemple, celui correspondant au mot de passe par défaut admin) pour l'utilisateur concerné: UPDATE glpi_users SET password = 'd033e22ae348aeb5660fc2140aec35850c4da997' WHERE name = 'glpi'; *(Note : Le hash ci-dessus correspond au mot de passe "admin" en SHA-1)*.

4. **Application des changements :** Rechargement des privilèges et déconnexion.
   FLUSH PRIVILEGES; EXIT;

Vérification et sécurisation (Durcissement)

- **Validation :** La connexion à l'interface Web a été validée avec le nouveau mot de passe temporaire.
- **Restauration de la sécurité :** Une fois connecté, le mot de passe a été immédiatement rechangé dans les paramètres de l'utilisateur sur GLPI. Cette manipulation permet à l'application de générer à nouveau un hash sécurisé en **bcrypt**, conformément aux normes de sécurité actuelles.