2024

Installer GLPI et Fusion inventory sous ubuntu 20.04



BRIEUC LE_FAUCHEUR Saint-Sauveur 08/02/2024

<mark>1/ : Configurer Ubuntu 20.04</mark>

Pour commencer on vas d'abord paramétrer l'adressage IP en entrant la commande :

« sudo vim /etc/netplan/00-installer-config.yaml »



Il est important de respecter chaques espace, et une fois cela fait on lance la commande « **sudo netplan apply** » et on reboot.

Ensuite on procède a l'installation d'Apache2

Pour se faire il faut taper la commande : « sudo apt-get update » pour mettre a jour les paquet et rentrer la commande « sudo apt-get install apache2 »

root@lefaucheur:~# sudo apt-get install apache2

Et après modifier le fichier « vi /etc/apache2/apache2.conf »



La ligne ajoutée est tout en haut et c'est « ServerName 192.168.0.196 »

Ensuite au lieu de reboot nous pouvons effectuer la commande « sudo systemctl restart apache2 » qui vas restart apache2.



L'opération a bien marché !

On vas aussi installer openssh, pour se faire on lance la commande :

« sudo apt-get install openssh-server » une fois cela fait on rentre ceci :

« vi /etc/ssh/sshd_config » et dans la ligne PermitRootLogin on met yes

Include /etc/ssh/sshd_config.d/*.conf
<pre>#LoginGraceTime 2m PermitRootLogin_yes #StrictModes yes #MaxAuthTries 6 #MaxSessions 10</pre>
<pre># Change to yes to enable challenge-response passwords (beware issues with # some PAM modules and threads) "/etc/ssh/sshd_config" 123L, 3274C</pre>

2/ : Installation de Mariadb

On lance ensuite les commandes suivantes :

« sudo apt install mariadb-server »

« sudo mysql_secure_installation »

Une fois l'installation faite nous allons suivre ces lignes de commandes dans l'ordre :

« sudo mysql -u root –p »

« UPDATE mysql.user SET plugin = 'HOS4mdp' WHERE User = 'root'; »

« FLUSH PRIVILEGES ; »

QUIT;

Ensuite on vas créer le user et la data base pour GLPI :

- « mysql -u root -p »
- « CREATE DATABASE glpi; »
- « CREATE USER 'glpi'@'localhost' IDENTIFIED BY 'HOS4mdp'; »
- « GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@'localhost' ; »
- « FLUSH PRIVILEGES; »
- « EXIT; »

3/ : Installation de GLPI

Ensuite on vas installer glpi, comme installé précédemment, on vas l'installer avec WinSCP on vas donc installer glpi version 9.5.0 disponible sur ce site : <u>https://glpiproject.org/fr/glpi-9-5-version/</u>

Ensuite on le dézip et on le met dans ce dossier : « /var/www/html/ » et on glisse le dossier dedans



Ensuite on vas sur internet avec cette URL : http://192.168.0.196/glpi/

Normalement nous rencontrerons des difficultés pour l'installation, il faudra installer ces packets ci-dessous :

- apt-get install php-mbstring
- apt-get install php-mysqli
- apt-get install php-curl
- apt-get install php-gd
- apt-get install php-simplexml
- apt-get install php-intl

Une fois les paquets installer ils faut donner les droits, pour ce faire il faut lancer cette commande : « chown –R www-data :www-data /var/www/html/glpi »

On « sudo systemctl restart mariadb » et on peut poursuivre l'installation. En se fiant a glpi ensuite on se connecte a GLPI comme logs glpi et glpi (pour le mdp)

Et ensuite on installe Fusion Inventory 9.5+4.2, on l'installera avec ce lien :

« https://github.com/fusioninventory/fusioninventory-for-glpi/releases » et on descendra jusqu'à trouver le version cité précédemment une fois cela fait on le dé zip et on le range dans le dossier « /var/www/html/glpi/plugins/ » Et après on l'installe sur GLPI.

Une fois cela fait on installe L'agent avec ce lien : « https://fusioninventory.org/ » penser a prendre l'agent en 2.6

Une fois cela fait le lance on fait suivant, suivant on met dans le mode serveur :

« hhtp://192.168.0.196/glpi/plugins/fusioninventory » on fais suivant, suivant on l'exécute bien en tant que service Windows,

Pour les options du serveur http on laisse par défaut, Bien penser a cocher les deux premières cases ainsi que la dernière.

Et volla tout est por	Et vo	ılà	tout	est	bor
-----------------------	-------	-----	------	-----	-----

✓ Actions									
Nom	Statut	Fabricant	Numéro de série	Туре	Modèle	Système d'exploitation - Nom	Lieu	Dernière modification	Composants - Processeur
HOS4POSTE09		LENOVO	S4QX7841	Desktop	ThinkStation P340	Windows		2024-02-08 12:55	Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz
Nom	Statut	Fabricant	Numéro de série	Туре	Modèle	Système d'exploitation - Nom	Lieu	Dernière modification	Composants - Processeur
Actions									

4/ : Mise en place de la sécurisation du protocole HTTPS

Pour cette étape on vas créer un certificat auto signer

On lace un cd /, et on fait un « mkdir ~/certificates» et on rentre dedans avec un

Cd ~/certificates et après on rentre cette commande :

« openssl req -x509 -newkey rsa :4096 -keyout apache.key -out apache.crt -days 365 -nodes »



Pour plus de sécurité on vas le déplacer dans un sous répertoire, on fais

« mkdir /etc/apache2/ssl »

Et on le déplace : « mv ~/certificates/* /etc/apache2/ssl » (l'étoile signifie qu'on prend tout)

Si il y a des complications, on peut les changer de place manuellement avec WinSCP dans le sous répertoire qu'ont veux

Ensuite on fait un « sudo vi /etc/apache2/sites-available/default-ssl.conf »



Dedans on vas mettre notre adresse mail dans « ServerAdmin » et on vas rajouter la ligne « ServerName 192.168.0.196 »

Ensuite dans SSLCertificateFile on vas changer les lignes pour mettre celles comme dans l'image. Et pareil pour celle en dessous

On redémarre apache2. Après on rentre « sudo a2enmod ssl » et on rentre « sudo a2ensite default-ssl.conf » on relance apache2 encore une fois

On fais un "cd /" et "vi /etc/apache2/sites-available/000-default.conf"



On met les informations comme le screen ci-dessus,

Le server Name avec notre IP et en dessous le redirect <u>« / https://192.168.0.196 »</u> Bien penser à respecter l'espace après le / .



Et voilà tout est bon ! 🙂

4/ : Sauvegarde quotienne de la base de données

Pour commencer on va créer un dossier sauvegarde dans le /root/ Et ensuite on va créer un fichier que l'on va nommer « glpi_backup.sh »

Dans ce fichier on vas mettre ce code ci-dessous :

#!/bin/bash

Configuration
DB_USER="root"
DB_PASS="HOS4mdp"
DB_NAME="glpi"
BACKUP_DIR="/root/sauvegarde"
DATETIME=\$(date +"%Y-%m-%d %H-%M-%S")

Vérifier si le répertoire de sauvegarde existe, sinon le créer

if [! -d "\$BACKUP_DIR"]; then

mkdir -p \$BACKUP_DIR

fi

Sauvegarde de la base de données GLPI

mysqldump -u \$DB_USER -p\$DB_PASS \$DB_NAME > \$BACKUP_DIR/glpi_backup_\$DATETIME.sql

Vérifier si la sauvegarde de la base de données a réussi

if [\$? -eq 0]; then

echo "Sauvegarde de la base de données GLPI réussie."

else

echo "Erreur lors de la sauvegarde de la base de données GLPI."

exit 1

Compression de la sauvegarde

tar -czvf \$BACKUP_DIR/glpi_files_backup_\$DATETIME.tar.gz /var/www/html/glpi

Vérifier si la compression a réussi

if [\$? -eq 0]; then

echo "Compression des fichiers GLPI réussie."

else

echo "Erreur lors de la compression des fichiers GLPI."

exit 1

fi

echo "Sauvegarde quotidienne de GLPI terminée avec succès."

Une fois fais on lance la commande « chmod +x /root/sauvegarde/glpi_backup.sh »

Ensuite on vas planifier la sauvegarde du script.sh avec la commande "crontab –e"

On fais 1 et une fois dans le fichier on met cette ligne de commande :

« 0 2 * * * /root/sauvegarde/glpi_backup.sh » on enregistre et on quitte.

fi

<u> 4/ : Sauvegarde quotidienne dans un serveur NAS</u>

On modifie le fichier.sh de cette manière :

```
#!/bin/bash
# Paramètres de connexion à la base de données
DB_USER="root"
DB PASSWORD="HOS4mdp"
DB NAME="glpi"
# Chemin de sauvegarde local
BACKUP DIR LOCAL=/home/
TIMESTAMP=$(date +"%Y%m%d%H%M%S")
BACKUP_FILE="$BACKUP_DIR_LOCAL/glpi_backup_$TIMESTAMP.sql"
# Chemin de sauvegarde sur le NAS
NAS USER="LE FAUCHEUR"
NAS IP="192.168.0.241"
NAS_SHARE="//192.168.0.241/LE_FAUCHEUR"
NAS PASSWORD="MTYHS6B"
NAS_MOUNT_POINT="/mnt/nas_backup"
# Création du répertoire local si nécessaire
sudo mkdir -p $BACKUP_DIR_LOCAL
# Création du point de montage pour le NAS
sudo mkdir -p $NAS_MOUNT_POINT
# Montage du partage SMB avec nom d'utilisateur et mot de passe
sudo mount.cifs $NAS_SHARE $NAS_MOUNT_POINT -o
username=$NAS USER,password=$NAS PASSWORD,vers=2.0
# Vérifie si le montage a réussi
if [ $? -ne 0 ]; then
  echo "Échec du montage du NAS."
  exit 1
fi
# Commande de sauvegarde
mysqldump -u $DB USER -p$DB PASSWORD --databases $DB NAME > $BACKUP FILE
# Copie du fichier de sauvegarde vers le NAS
cp $BACKUP_FILE $NAS_MOUNT_POINT/
# Démontage du partage SMB
sudo umount $NAS MOUNT POINT
```