PLOUZENNEC Eliaz

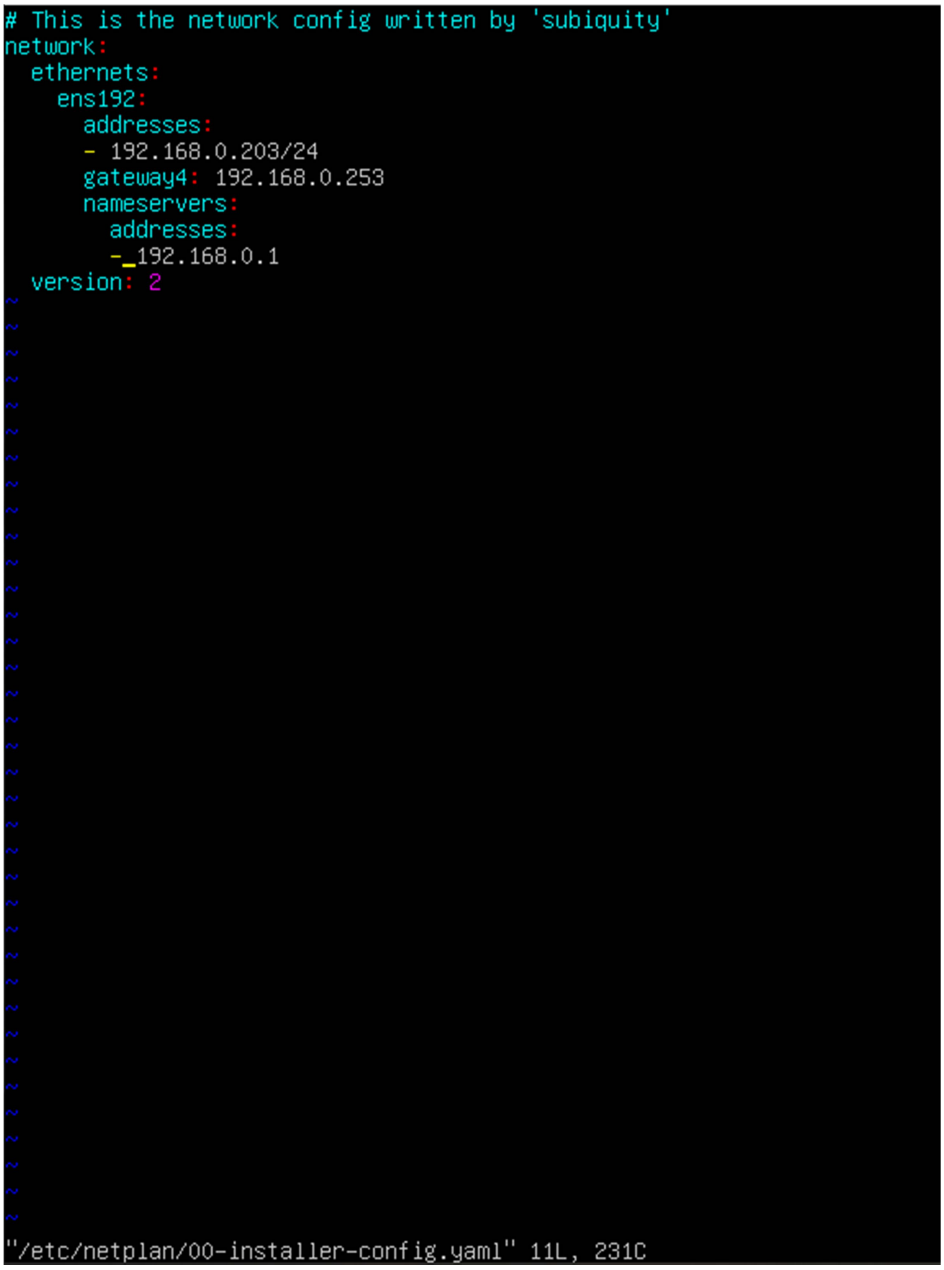
TP : GLPI Ubuntu server 20.04

06/02/24

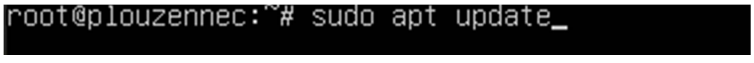
Contenu

Introduction :

Etape 1 : Initialisation de la connexion



On configure l'adresse ip.



Etape 2 : Installation de la Base de donnée :

On update

Installation de mariadb

```
root@plouzennec:~# sudo mysql_secure_installation
```

Installation de mysql

```
"/etc/netplan/00-installer-config.yaml" 11L, 231C written
root@plouzennec:~# sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 36
Server version: 10.3.39-MariaDB-0ubuntu0.20.04.2 Ubuntu 20.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database glpi
```

On configure dans mariadb, avec sudo 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;
```

Puis

```
sudo apt -y install php php-
{curl,zip,bz2,gd,imagick,intl,apcu,memcache,imap,mysql,cas,ldap,tidy,pear,xmlrpc,ps
pell,mbstring,json,iconv,xml,gd,xsl}
```

On installe apache2 :

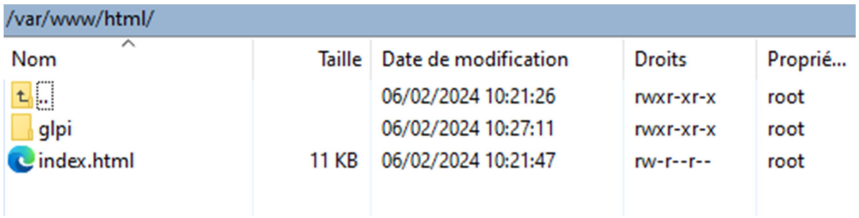
```
sudo apt -y install apache2 libapache2-mod-php
```

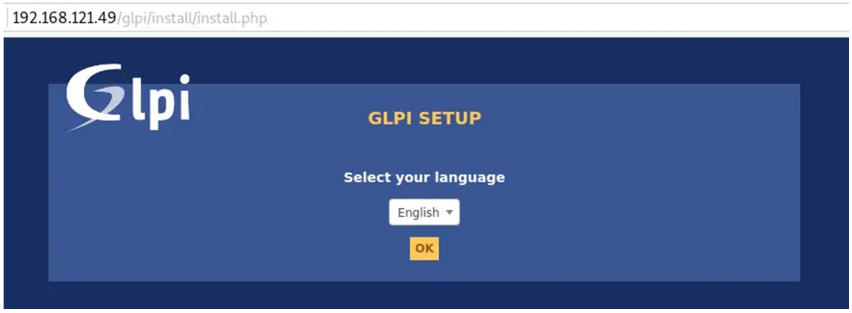
On modifie le fichier de cette facon :

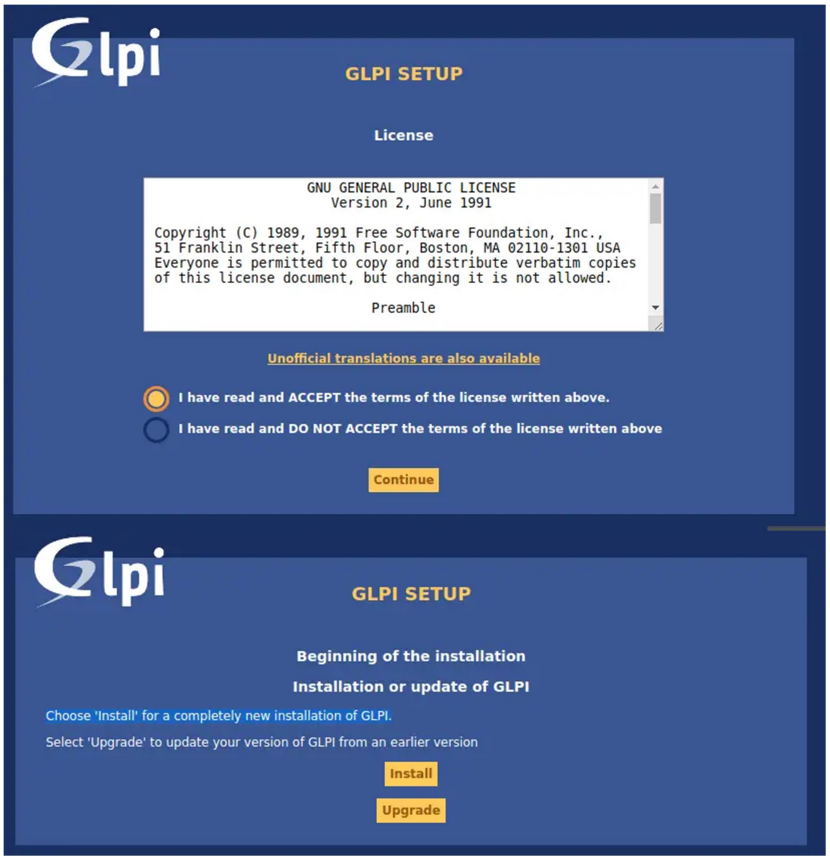
```
sudo vim /etc/php/*/apache2/php.ini

session.cookie_httponly = on
```

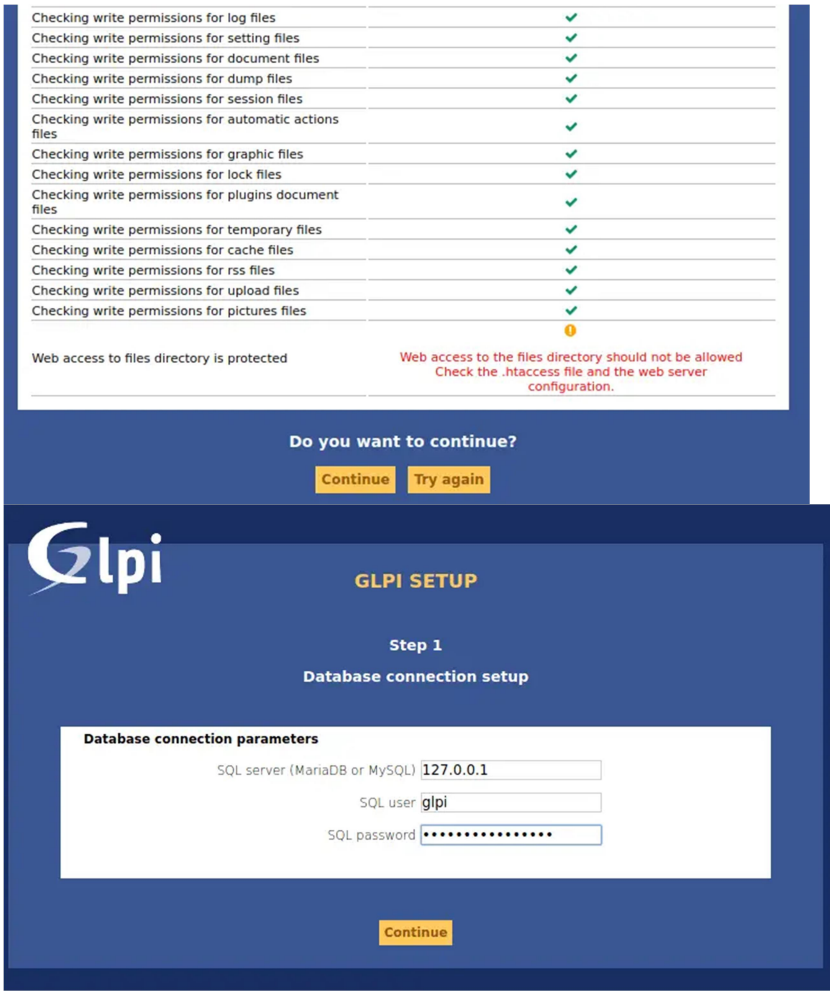
Etape 3 : Installation de GLPI

J'ai telechargé puis decompressé le fichier glpi, pour ensuite le transferer dans var/www/html/



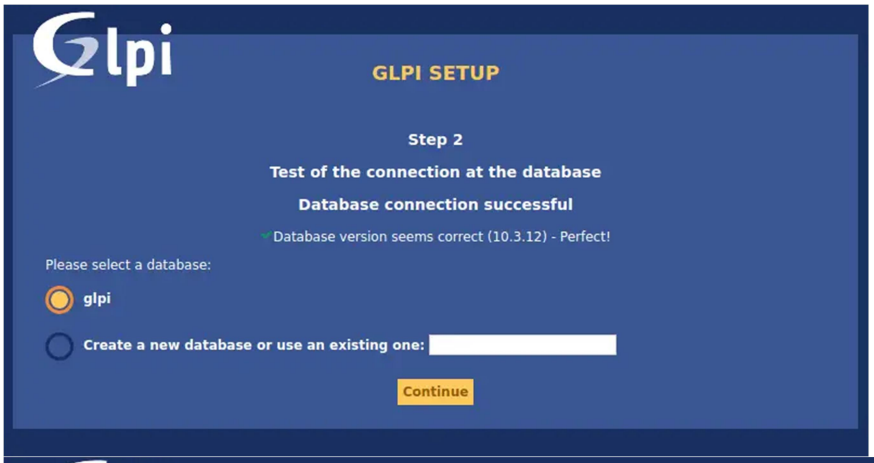


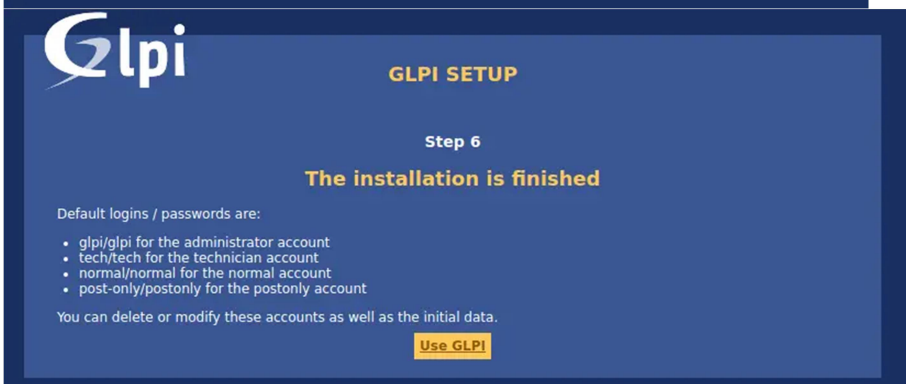



Checking write permissions for log files
Checking write permissions for setting files
Checking write permissions for document files
Checking write permissions for dump files
Checking write permissions for session files
Checking write permissions for automatic actions files
Checking write permissions for graphic files
Checking write permissions for lock files
Checking write permissions for plugins document files
Checking write permissions for temporary files
Checking write permissions for cache files
Checking write permissions for rss files
Checking write permissions for upload files
Checking write permissions for pictures files
Web access to files directory is protected
Web access to the files directory should not be allowed
Check the .htaccess file and the web server configuration.
Do you want to continue?
Continue
Try again

GLPI SETUP
Step 1
Database connection setup
Database connection parameters
SQL server (MariaDB or MySQL) 127.0.0.1
SQL user glpi
SQL password
Continue

Ici le mot de passe qu'on a rentré prealablement : HOS4mdp

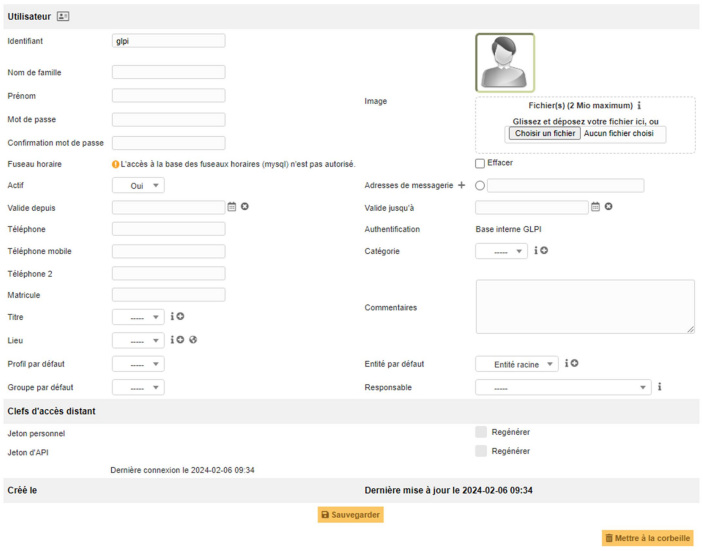




Suivre toutes ces etapes.

Puis changer mdp de glpi pour HOS4mdp

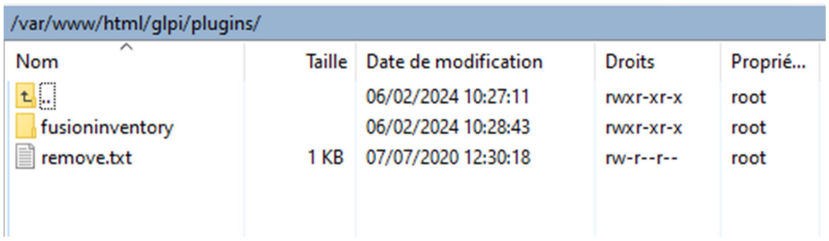
Changer les parametres de securité pour le mdp fort.

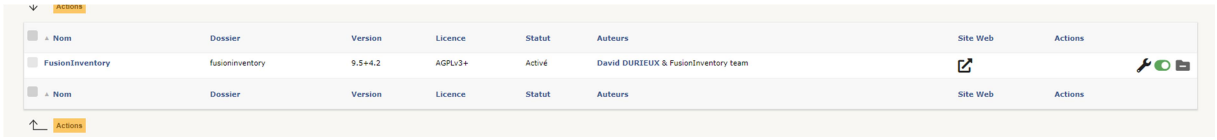


Changer mdp ici.

Etape 4 : Installation du plugin Fusion Inventory

Prendre le plugin sur l'ordinateur physique, le decompresser, puis le transferer ici via winscp.

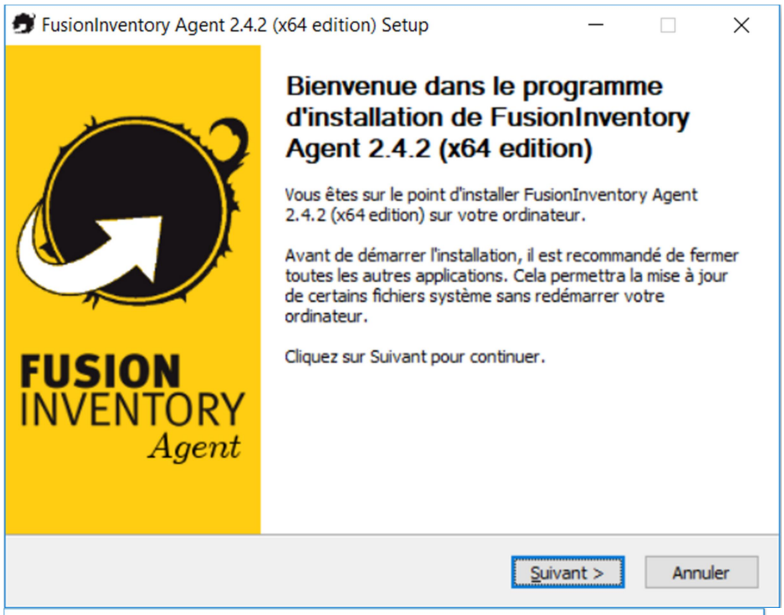


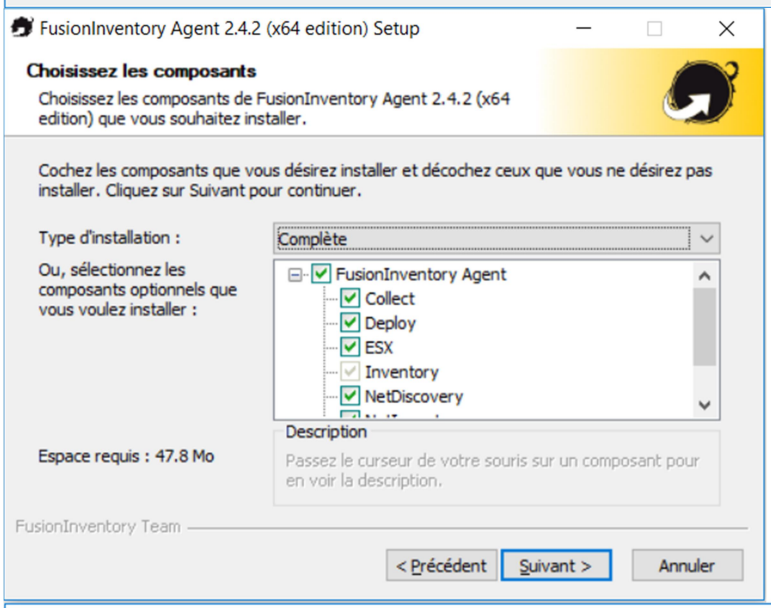


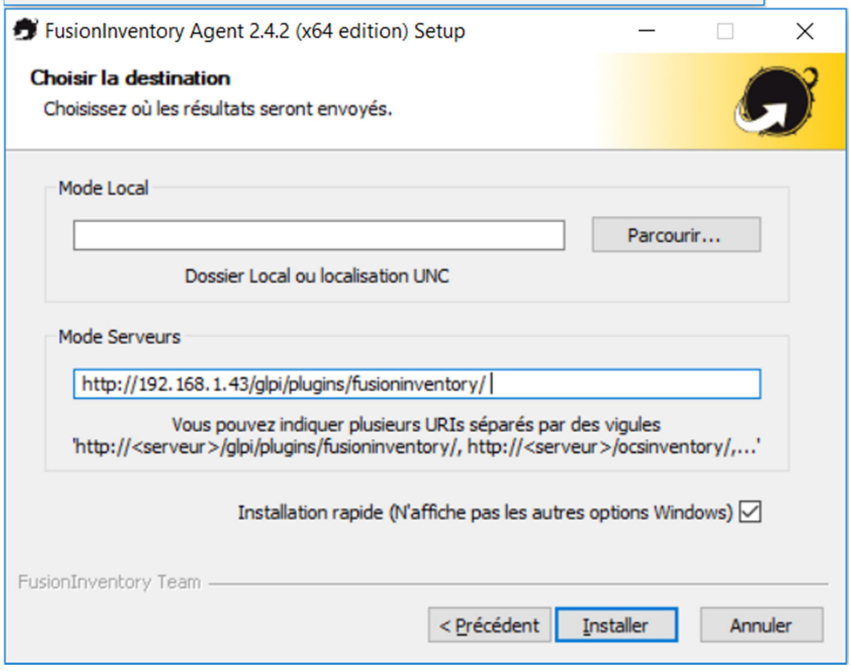
Puis dans glpi, acceder aux plugins, ajouter le plugins, puis l'activer.

Etape 5 : Installation de l'agent fusion inventory

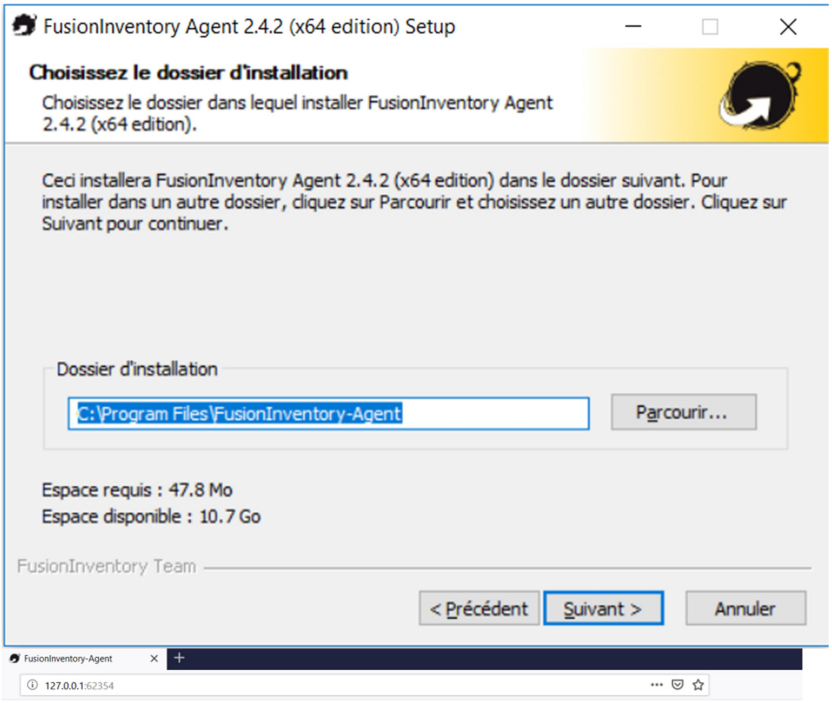
Sur le pc physique installer l'agent fusion inventory qui est compatible avec la version de glpi.


FusionInventory Agent 2.4.2 (x64 edition) Setup
FUSION
INVENTORY
Agent
Bienvenue dans le programme d'installation de FusionInventory Agent 2.4.2 (x64 edition)
Vous êtes sur le point d'installer FusionInventory Agent 2.4.2 (x64 edition) sur votre ordinateur.
Avant de démarrer l'installation, il est recommandé de fermer toutes les autres applications. Cela permettra la mise à jour de certains fichiers système sans redémarrer votre ordinateur.
Cliquez sur Suivant pour continuer.
Suivant >
Annuler

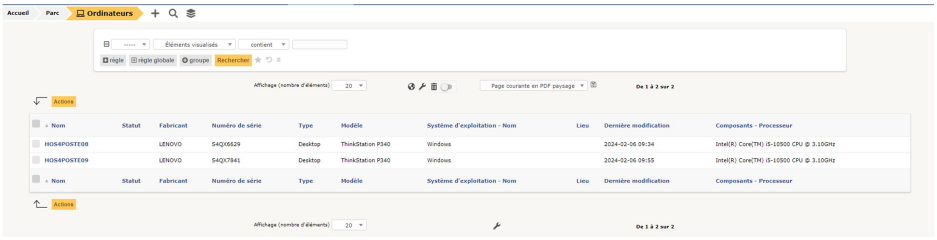

FusionInventory Agent 2.4.2 (x64 edition) Setup
Choisissez les composants
Choisissez les composants de FusionInventory Agent 2.4.2 (x64 edition) que vous souhaitez installer.
Cochez les composants que vous désirez installer et décochez ceux que vous ne désirez pas installer. Cliquez sur Suivant pour continuer.
Type d'installation :
Complète
Ou, sélectionnez les composants optionnels que vous voulez installer :
FusionInventory Agent
Collect
Deploy
ESX
Inventory
NetDiscovery
Description
Passez le curseur de votre souris sur un composant pour en voir la description.
Espace requis : 47.8 Mo
FusionInventory Team
< Précédent
Suivant >
Annuler


FusionInventory Agent 2.4.2 (x64 edition) Setup
Choisir la destination
Choisissez où les résultats seront envoyés.
Mode Local
Parcourir...
Dossier Local ou localisation UNC
Mode Serveurs
http://192.168.1.43/glpi/plugins/fusioninventory/
Vous pouvez indiquer plusieurs URIs séparés par des vigules
'http://<serveur>/glpi/plugins/fusioninventory/, http://<serveur>/ocsinventory/,...'
Installation rapide (N'affiche pas les autres options Windows)
FusionInventory Team
< Précédent
Installer
Annuler

Mettre son adresse IP à la place.



Suivre ces etapes puis forcer l'inventaire.



On retrouve ici l'inventaire de notre machine.

Etape 6 : Sécurisation HTTPS

On créé le certificat :

```
root@plouzennec:~# cd /
root@plouzennec:/# mkdir /etc/apache2/ssl
```

On créé le fichier ssl dans apache2.

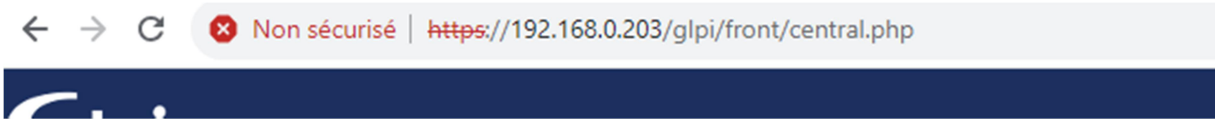
```
root@plouzennec:/# mv ~/certificates/* /etc/apache2/ssl
```

On le deplace le certificat.

```
root@plouzennec:/# sudo a2enmod ssl_
```

```
root@plouzennec:/# sudo a2ensite default-ssl.conf_
root@plouzennec:/# sudo service apache2 restart_
```

On restart Apache2.



Puis le site est bien sécurisé avec https:// devant.

Etape 7 : Redirection automatique sur https://

Dans /etc/apache2/site-available/000-default.conf, on modifie le document de cette manière :

```
        ServerName 192.168.0.203
        Redirect permanent / https://192.168.0.203/
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Puis sudo service apache2 reload, et le site va directement en https quand on rentre l'adresse ip.

Etape 8 : Sauvegarde automatique quotidienne

Pour commencer, il faut créer un fichier pour le script de sauvegarde, et aussi où vont se stocker les sauvegardes. On créé le fichier dans root :

Mkdir ~/scripts

On rentre dans scripts pour configurer le fichier de sauvgarde .sh :

Nano ~/scripts/glpi_backup.sh

Pour ecrire dedans :

```
#!/bin/bash

# Paramètres de connexion à la base de données
DB_USER="votre_utilisateur"          # Remplacez par le nom d'utilisateur
DB_PASSWORD="votre_mot_de_passe"      # Remplacez par le mot de passe de la
DB_NAME="nom_de_votre_base_de_donnees" # Remplacez par le nom de la base de

# Chemin de sauvegarde
BACKUP_DIR=~/backup
TIMESTAMP=$(date +"%Y%m%d%H%M%S")
BACKUP_FILE="$BACKUP_DIR/glpi_backup_$TIMESTAMP.sql"

# Commande de sauvegarde
mysqldump -u $DB_USER -p$DB_PASSWORD --databases $DB_NAME > $BACKUP_FILE
```

Où il faut remplacer les 3 premiers par root, HOS4mdp, et glpi.

Ensuite donner les permissions d'exécution au script :

chmod +x ~/scripts/glpi_backup.sh

Et pour la sauvegarde automatique on rentre dans :

crontab –e

Pour rentrer :

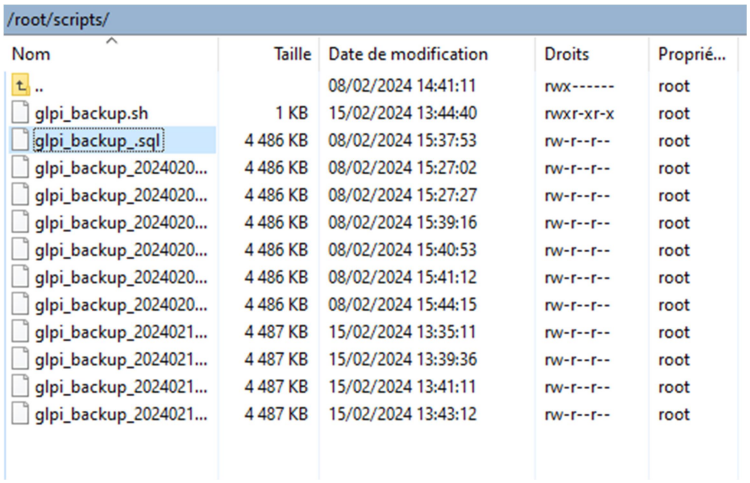
0 2 * * * ~/scripts/glpi_backup.sh

La commande crontab -e est utilisée pour éditer le fichier de table des tâches cron pour un utilisateur spécifique.

Et ici 0 2 * * * ~/scripts/glpi_backup.sh

Ca signifie que ca se fait tous les jours à 2h00 du matin. Le 0 signifie 0 minutes, le 2 signifie 2h, et les 3 autres etoiles signifient jourdumois, mois, jourdelasemaine, ici qui sont inutiles vu que la sauvegarde doit etre quotidienne.

Ainsi maintenant les sauvegardes arrivent automatiquement :

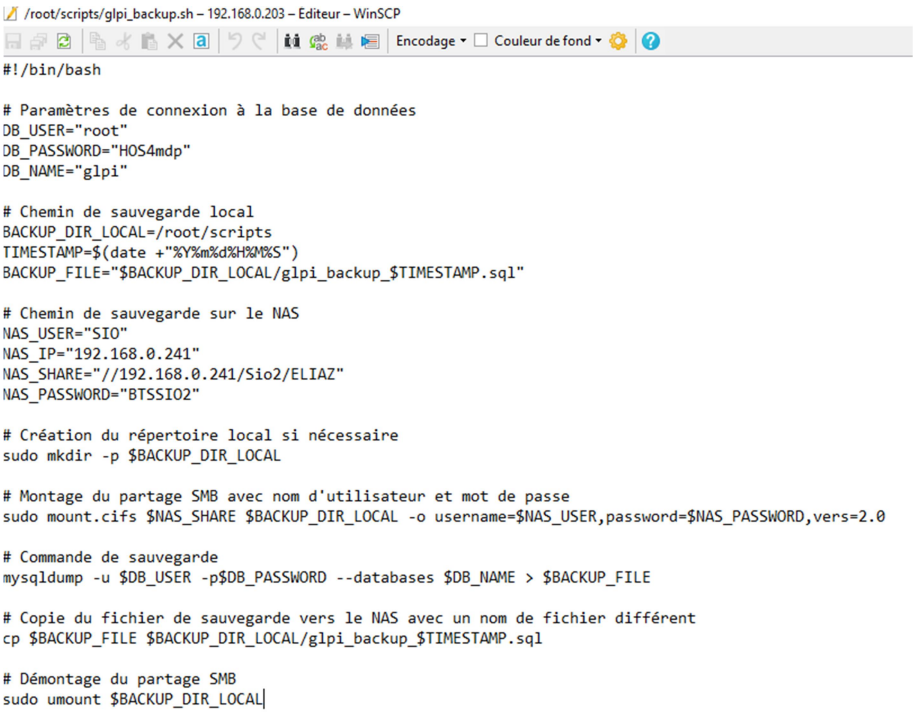


/root/scripts/

Nom	Taille	Date de modification	Droits	Proprié...
..		08/02/2024 14:41:11	rwx------	root
glpi_backup.sh	1 KB	15/02/2024 13:44:40	rwxr-xr-x	root
glpi_backup_.sql	4 486 KB	08/02/2024 15:37:53	rw-r--r--	root
glpi_backup_2024020...	4 486 KB	08/02/2024 15:27:02	rw-r--r--	root
glpi_backup_2024020...	4 486 KB	08/02/2024 15:27:27	rw-r--r--	root
glpi_backup_2024020...	4 486 KB	08/02/2024 15:39:16	rw-r--r--	root
glpi_backup_2024020...	4 486 KB	08/02/2024 15:40:53	rw-r--r--	root
glpi_backup_2024020...	4 486 KB	08/02/2024 15:41:12	rw-r--r--	root
glpi_backup_2024020...	4 486 KB	08/02/2024 15:44:15	rw-r--r--	root
glpi_backup_2024021...	4 487 KB	15/02/2024 13:35:11	rw-r--r--	root
glpi_backup_2024021...	4 487 KB	15/02/2024 13:39:36	rw-r--r--	root
glpi_backup_2024021...	4 487 KB	15/02/2024 13:41:11	rw-r--r--	root
glpi_backup_2024021...	4 487 KB	15/02/2024 13:43:12	rw-r--r--	root

Etape 9 : Sauvegarde quotidienne sur un NAS

On modifie le fichier .sh de cette manière :



/root/scripts/glpi_backup.sh – 192.168.0.203 – Editeur – WinSCP

Encodage ▾ Couleur de fond ▾

```
#!/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=/root/scripts
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="SIO"
NAS_IP="192.168.0.241"
NAS_SHARE="//192.168.0.241/Sio2/ELIAZ"
NAS_PASSWORD="BTSSIO2"

# Création du répertoire local si nécessaire
sudo mkdir -p $BACKUP_DIR_LOCAL

# Montage du partage SMB avec nom d'utilisateur et mot de passe
sudo mount.cifs $NAS_SHARE $BACKUP_DIR_LOCAL -o username=$NAS_USER,password=$NAS_PASSWORD,vers=2.0

# Commande de sauvegarde
mysqldump -u $DB_USER -p$DB_PASSWORD --databases $DB_NAME > $BACKUP_FILE

# Copie du fichier de sauvegarde vers le NAS avec un nom de fichier différent
cp $BACKUP_FILE $BACKUP_DIR_LOCAL/glpi_backup_$TIMESTAMP.sql

# Démontage du partage SMB
sudo umount $BACKUP_DIR_LOCAL
```

On rajoute un chemin de sauveggarde sur le nas, avec le mot de passe, le chemin, l’utilisateur, l’ip. Et une copie du fichier avec un nom de fichier diffrent.