

GLPI / OCS

Emetteur(s) : Saviard
Matthieu

Destinataire(s) : Nom(s)

Date : 03/02/2024

Objet : Mise en place d'une solution ticketing Jira

1. Contexte

2. Prérequis

Pour mettre en place ces 3 services, nous allons tous concentrer ces services sur **une machine Debian 11** avec la configuration suivante :

Nous réduisons au maximum la RAM pour réaliser des économies, nous avons également réduit au maximum le CPU.

Nous allons réaliser chronologiquement la réalisation du serveur suivant :

- Installation du Service AD
- Installation du Service DHCP
- Installation du Service DNS

3. Installation et configuration du serveur

a. Installation des services

On commence par mettre a jour la machine

```
root@glpi:~# apt update && upgrade
```

On rajoute une carte, et on va ensuite aller dans → /etc/network/interfaces et la mettre en LAN. On veut une carte en LAN et une en NAT pour télécharger GLPI. Elle sera ensuite supprimée plus tard

```
root@glpi:~# ip ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:0f:77:60 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.32.140/24 brd 192.168.32.255 scope global dynamic ens33
        valid_lft 1727sec preferred_lft 1727sec
    inet6 fe80::20c:29ff:fe0f:7760/64 scope link
        valid_lft forever preferred_lft forever
3: ens36: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:0f:77:6a brd ff:ff:ff:ff:ff:ff
    altname enp2s4
root@glpi:~# nano /etc/net
netconfig network/ networks
root@glpi:~# nano /etc/net
netconfig network/ networks
root@glpi:~# nano /etc/network/interfaces_
```

On met cette configuration

```
GNU nano 5.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp

auto ens36
iface ens36 inet static
address 192.168.100.6/24
gateway 192.168.100.254
```

Et on allume ensuite la carte ens36

```
altname enp2s4
root@glpi:~# ifup ens36
```

On voit ensuite bien que la carte est up

```
valid_lft forever preferred_lft forever
3: ens36: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
link/ether 00:0c:29:0f:77:6a brd ff:ff:ff:ff:ff:ff
altname enp2s4
inet 192.168.100.6/24 brd 192.168.100.255 scope global ens36
    valid_lft forever preferred_lft forever
inet6 fe80::20c:29ff:fe0f:776a/64 scope link
    valid_lft forever preferred_lft forever
root@glpi:~#
```

Nous allons donc pouvoir commencer par installer MariaDB et Apache2. En effet, pour installer GLPI, nous avons besoin d'une base de données. Ici nous allons prendre MariaDB

Nous allons donc effectuer la commande suivante :

```
apt install apache2 php mariadb-server -y
```

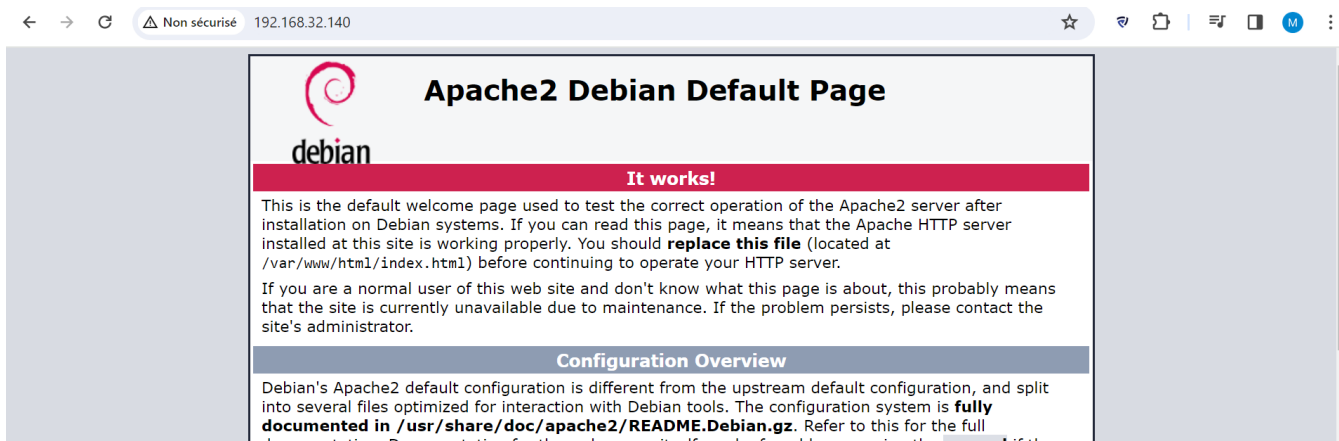
```
root@glpi:~# root@glpi:~# apt install apache2 php mariadb-server -y
```

Une fois le packet installé, on regarde si il fonctionne bien

```
root@glpi:~# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2024-02-04 12:49:43 CET; 27s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Main PID: 9051 (apache2)
    Tasks: 6 (limit: 4615)
   Memory: 11.3M
      CPU: 118ms
   CGroup: /system.slice/apache2.service
           └─9051 /usr/sbin/apache2 -k start
             └─9053 /usr/sbin/apache2 -k start
               └─9054 /usr/sbin/apache2 -k start
                 └─9055 /usr/sbin/apache2 -k start
                   └─9056 /usr/sbin/apache2 -k start
                     └─9057 /usr/sbin/apache2 -k start

févr. 04 12:49:43 glpi systemd[1]: Starting The Apache HTTP Server...
févr. 04 12:49:43 glpi systemd[1]: Started The Apache HTTP Server.
root@glpi:~#
```

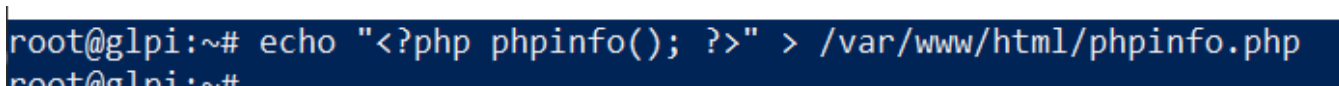
Le service tourne bien, on va voir sur le navigateur si on trouve notre site web



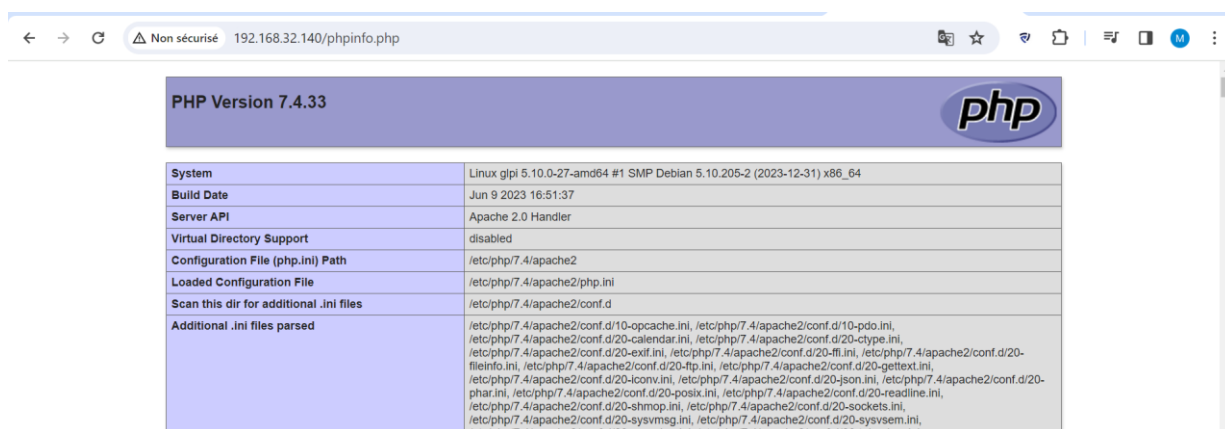
Ca marche bien, on tombe bien sur notre site web.

On va ensuite créer une page PHP, en effet, on a besoin d'une page PHP pour ce qui sera notre futur GLPI, on va donc exécuter la commande suivante :

```
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```



Et on tombe bien dessus :



b. Configuration de la base de données MariaDB

On va commencer par restreindre l'accès à notre base de données. En effet, c'est très important car on va créer un utilisateur root, et si quelqu'un venait à avoir accès à un tel utilisateur alors il pourrait compromettre notre outil de ticketing

On va donc exécuter la commande suivante :

```
mysql_secure_installation
```

Ensuite cela va lancer la boucle suivante :

Faire entrée

```
root@glpi:~# mysql_secure_installation
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB  
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
```

```
In order to log into MariaDB to secure it, we'll need the current  
password for the root user. If you've just installed MariaDB, and  
haven't set the root password yet, you should just press enter here.
```

```
Enter current password for root (enter for none):
```

```
root@glpi:~# mysql_secure_installation
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB  
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
```

```
In order to log into MariaDB to secure it, we'll need the current  
password for the root user. If you've just installed MariaDB, and  
haven't set the root password yet, you should just press enter here.
```

```
Enter current password for root (enter for none):
```

```
OK, successfully used password, moving on..
```

```
Setting the root password or using the unix_socket ensures that nobody  
can log into the MariaDB root user without the proper authorisation.
```

```
You already have your root account protected, so you can safely answer 'n'.
```

```
Switch to unix_socket authentication [Y/n] n  
... skipping.
```

```
You already have your root account protected, so you can safely answer 'n'.
```

```
Change the root password? [Y/n] y
```

```
New password:
```

```
Re-enter new password:
```

```
Password updated successfully!
```

```
Reloading privilege tables..
```

```
... Success!
```

```
By default, a MariaDB installation has an anonymous user, allowing anyone  
to log into MariaDB without having to have a user account created for  
them. This is intended only for testing, and to make the installation  
go a bit smoother. You should remove them before moving into a  
production environment.
```

```
Remove anonymous users? [Y/n] y
```

```
... Success!
```

```
Normally, root should only be allowed to connect from 'localhost'. This  
ensures that someone cannot guess at the root password from the network.
```

```
Disallow root login remotely? [Y/n]
```

```
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
root@glpi:~#
```

c. Installation des extensions PHP

Pour notre GLPI, on aura besoin d'extensions précises qui faciliteront nos tâches, voici toutes les installations en question :

On a donc des extensions OBLIGATOIRES et des extensions qui sont OPTIONNELLES

Voici donc la liste principale des extensions qui sont obligatoires pour notre serveur GLPI et leur fonctionnalités :

EXTENSION OBLIGATOIRE	
curl	: Pour les requêtes HTTP et l'interaction avec des API.
fileinfo	: Pour obtenir des informations sur les fichiers.
gd	: Pour la manipulation d'images.
json	: Pour la prise en charge du format JSON.
mbstring	: Pour gérer les caractères multi-octets.
mysqli	: Pour se connecter et interroger la base de données MySQL.
session	: Pour le support des sessions utilisateur.
zlib	: Pour les fonctions de sauvegarde et de restauration de la base de données.
simplexml	: Pour manipuler des données XML de manière simple.
xml	: Pour le traitement des données XML.
intl	: Pour les opérations liées aux caractères internationaux et à la localisation.

Voici ensuite les extensions qui sont OPTIONNELLES :

EXTENSION OPTIONNELLES	
cli	: pour utiliser PHP en ligne de commande (scripts, actions automatiques, etc.) ;
domxml	: utilisé pour l'authentification CAS ;
ldap	: utiliser l'annuaire LDAP pour l'authentification ;
openssl	: communications sécurisées ;
xmlrpc	: utilisé pour l'API XMLRPC.
APCu	: peut être utilisé pour le cache.

On va donc toutes les installer avec la commande suivante :

```
apt install php-{ldap,apcu,xmlrpc,mysql,mbstring,curl,gd,xml,intl,bz2,zip} -y
```

Une fois le packet installé, on restart le service apache

```
root@glpi:~# systemctl restart apache2
```

d. Création de la base de données et de notre utilisateur

MariaDB	
Base de données	dbglpi
Utilisateur	userglpi

On va créer la base de données suivante avec son super utilisateur userglpi

On va donc nous connecter au service SQL →

```
root@glpi:~# mysql -u root
```

Et on réalise les commandes suivantes :

```
root@glpi:~# mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 38
Server version: 10.5.21-MariaDB-0+deb11u1 Debian 11

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;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> grant all privileges on dbglpi.* to userglpi@'localhost' identified by 'userglpi';
Query OK, 0 rows affected (0,002 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> select user,host from mysql.user;
+-----+-----+
| User      | Host      |
+-----+-----+
| mariadb.sys | localhost |
| mysql      | localhost |
| root       | localhost |
| userglpi   | localhost |
+-----+-----+
4 rows in set (0,002 sec)

MariaDB [(none)]> SHOW GRANTS FOR userglpi@localhost;
+-----+-----+
| Grants for userglpi@localhost
+-----+-----+
| GRANT USAGE ON *.* TO `userglpi`@`localhost` IDENTIFIED BY PASSWORD '*5245472BAD9DA5F741337D42E2B7455ABE61B401' |
| GRANT ALL PRIVILEGES ON `dbglpi`.* TO `userglpi`@`localhost`
+-----+-----+
2 rows in set (0,000 sec)

MariaDB [(none)]>
```

e. Téléchargement de GLPI

On va ensuite télécharger notre GLPI. Pour cela, on va installer notre GLPI dans un dossier /tmp que nous allons créer nous-mêmes

```
root@glpi:~# cd
root@glpi:~# mkdir tmp
root@glpi:~# cd tmp/
```

Une fois dans le dossier /tmp, on va installer la commande wget et installer notre paquet GLPI qui fonctionnera ensuite sur notre machine

```
root@glpi:~/tmp# apt install wget
```


On installe ensuite le paquet avec la commande suivante :

```
Paramétrage de wget (1.21.14deb1) ...  
root@glpi:~/tmp# wget https://github.com/glpi-project/glpi/releases/download/10.0.5/glpi-10.0.5.tgz
```

Une fois notre package installer on va décompresser le tout dans le fichier /var/www/html

```
root@glpi:~/tmp# tar xzf glpi-10.0.5.tgz -C /var/www/html/
```

```
root@glpi:~/tmp# cd /var/www/html/  
root@glpi:/var/www/html# ls  
glpi index.html phpinfo.php  
root@glpi:/var/www/html#
```

On retrouve donc bien le GLPI

Pour que notre service fonctionne correctement, on va devoir donner des droits au compte de service www-data

```
root@glpi:/var/www/html# chown -R www-data:www-data /var/www/html/glpi/  
root@glpi:/var/www/html# chmod -R 775 /var/www/html/glpi/  
root@glpi:/var/www/html# ls -l  
total 20  
drwxrwxr-x 23 www-data www-data 4096 4 nov. 2022 glpi  
-rw-r--r-- 1 root root 10701 4 févr. 12:49 index.html  
-rw-r--r-- 1 root root 20 4 févr. 12:53 phpinfo.php  
root@glpi:/var/www/html#
```

On va ensuite aller dans notre fichier php.ini et mettre

```
root@glpi:/var/www/html# nano /etc/php/7.4/apache2/php.ini
```

Et on met la ligne suivante :

```
session.cookie_httponly = on
```

On va ensuite sur notre navigateur et on va configurer GLPI :

GLPI

GLPI SETUP

Licence

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <<https://fsf.org/>>
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

[Des traductions non officielles sont également disponibles](#)

Continuer >

On faire ensuite installer

Début de l'installation

i **Installation ou mise à jour de GLPI**

Choisissez 'Installation' pour une nouvelle installation de GLPI.
Choisissez 'Mise à jour' pour lancer la mise à jour de votre version de GLPI à partir d'une version antérieure.

Installer ⬇️

Mettre à jour ↻

Étape 0

Vérification de la compatibilité de votre environnement avec l'exécution de GLPI

TESTS EFFECTUÉS	RÉSULTATS
Requis Parser PHP	✓
Requis Configuration des sessions	✓
Requis Mémoire allouée	✓
Requis mysqli extension	✓
Requis Extensions du noyau de PHP	✓
Requis curl extension <i>Requis pour l'accès à distance aux ressources (requêtes des agents d'inventaire, Marketplace, flux RSS, ...).</i>	✓
Requis gd extension <i>Requis pour le traitement des images.</i>	✓
Requis intl extension <i>Requis pour l'internationalisation.</i>	✓
Requis libxml extension <i>Requis pour la gestion XML.</i>	✓
Requis zlib extension <i>Requis pour la gestion de la communication compressée avec les agents d'inventaire. L'installation de paquets gzin</i>	✓


On fait continuer

Suggéré Configuration de sécurité pour les sessions <i>Permet de s'assurer que la sécurité relative aux cookies de session est renforcée. La directive PHP "session.cookie_httponly" devrait être définie à "on" pour prévenir l'accès aux cookies depuis les scripts côté client.</i>	⚠
Suggéré exif extension <i>Renforcer la sécurité de la validation des images.</i>	✓
Suggéré ldap extension <i>Active l'utilisation de l'authentification à un serveur LDAP distant.</i>	✓
Suggéré openssl extension <i>Active l'envoi de courriel en utilisant SSL/TLS.</i>	✓
Suggéré zip extension <i>Active l'installation de paquets zip à partir du Marketplace.</i>	✓
Suggéré bz2 extension <i>Active l'installation des paquets bz2 à partir du Marketplace.</i>	✓
Suggéré Zend OPcache extension <i>Améliorer les performances du moteur PHP.</i>	✓
Suggéré Extensions émulées de PHP <i>Améliorer légèrement les performances.</i>	✓
Suggéré Permissions pour le répertoire du marketplace <i>Active l'installation des plugins à partir du Marketplace.</i>	✓

Voulez-vous continuer ?

Continuer >
Réessayer ↻

On rentre ensuite nos identifiants de compte SQL précédemment créés



The screenshot shows the 'GLPI SETUP' interface for 'Étape 1: Configuration de la connexion à la base de données'. It features three input fields: 'Serveur SQL (MariaDB ou MySQL)' with the value 'localhost', 'Utilisateur SQL' with the value 'userglpi', and 'Mot de passe SQL' which is masked with dots. A yellow 'Continuer >' button is located at the bottom left.

On sélectionne notre base de données :



The screenshot shows the 'GLPI SETUP' interface for 'Étape 2: Test de connexion à la base de données'. A green success message 'Connexion à la base de données réussie' is displayed in a box at the top. Below it, the text 'Veuillez sélectionner une base de données :' is followed by a radio button for 'Créer une nouvelle base ou utiliser une base existante :'. Underneath, a list of database names is shown, with 'dbgipi' selected and highlighted by a red circle. A yellow 'Continuer >' button is at the bottom left.



GLPI SETUP

Étape 3

Initialisation de la base de données.

OK - La base a bien été initialisée

Continuer >

Faire continuer 2x

Continuer >

Puis « Utiliser GLPI »



GLPI SETUP

Étape 6

L'installation est terminée

Les identifiants et mots de passe par défaut sont :

- glpi/glpi pour le compte administrateur
- tech/tech pour le compte technicien
- normal/normal pour le compte normal
- post-only/postonly pour le compte postonly

Vous pouvez supprimer ou modifier ces comptes ainsi que les données initiales.

👍 Utiliser GLPI

On se connecte ensuite avec les identifiants suivants :

- ID : glpi
- MDP : glpi

Une fois arrivé sur la page, on a 2 messages d'erreurs suivants :



- Pour des raisons de sécurité, veuillez changer le mot de passe par défaut pour le(s) utilisateur(s) : glpi post-only tech normal
- Pour des raisons de sécurité, veuillez supprimer le fichier : install/install.php

- Le premier est dû aux 3 comptes, on a 3 mots de passes par défaut qu'il faut changer
- Le second est dû au fichier install.php qu'il faut supprimer ou déplacer

On clique donc sur tous les comptes en bleu et on met le mot de passe suivant : @Azerty123

Ensuite, on retourne sur notre machine Debian et on fait la commande suivante :

```
root@glpi:/var/www/html# cd ..
root@glpi:/var/www# cd /var/www/html/glpi/install
root@glpi:/var/www/html/glpi/install# mv install.php .install.php
root@glpi:/var/www/html/glpi/install#
```

Ensuite, le message d'erreur disparaîtra

f. Sécurisation de GLPI

Nous allons donc sécuriser notre accès à GLPI, en effet, nous voulons configurer notre serveur pour qu'on puisse y avoir accès depuis seulement notre VLAN Serveurs et via un URL spécifique grâce au DNS pour que nos machines puissent faire la traduction entre IP et nom de domaine

On va donc commencer par créer un enregistrement de service sur notre DNS principal

Nouvel hôte ×

Nom (utilise le domaine parent si ce champ est vide) :

Nom de domaine pleinement qualifié (FQDN) :

Adresse IP :

Créer un pointeur d'enregistrement PTR associé

Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Une fois l'enregistrement créé, nous allons créer le fichier conf pour notre GLPI

```
root@glpi:/etc/apache2/sites-available# touch glpi.conf  
root@glpi:/etc/apache2/sites-available# nano glpi.conf
```

```

<IfModule mod_ssl.c>
    <VirtualHost _default_:443>

        ServerName glpi.safetech.com
        ServerAlias safetech.com *.safetech.com
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/glpi

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

SSLEngine on
SSLCertificateFile      /etc/ssl/private/safetech.pem

    </VirtualHost>
</IfModule>

```

Puis on déplace le repertoire glpi

En effet, on le déplace car on veut matcher avec le DocumentRoot

```

root@glpi:~# mv /var/www/html/glpi/ /var/www/

```

g. Création du certificat SSL

On regarde si le paquet SSL est bien installé

```

root@glpi:~# dpkg -l ssl-cert

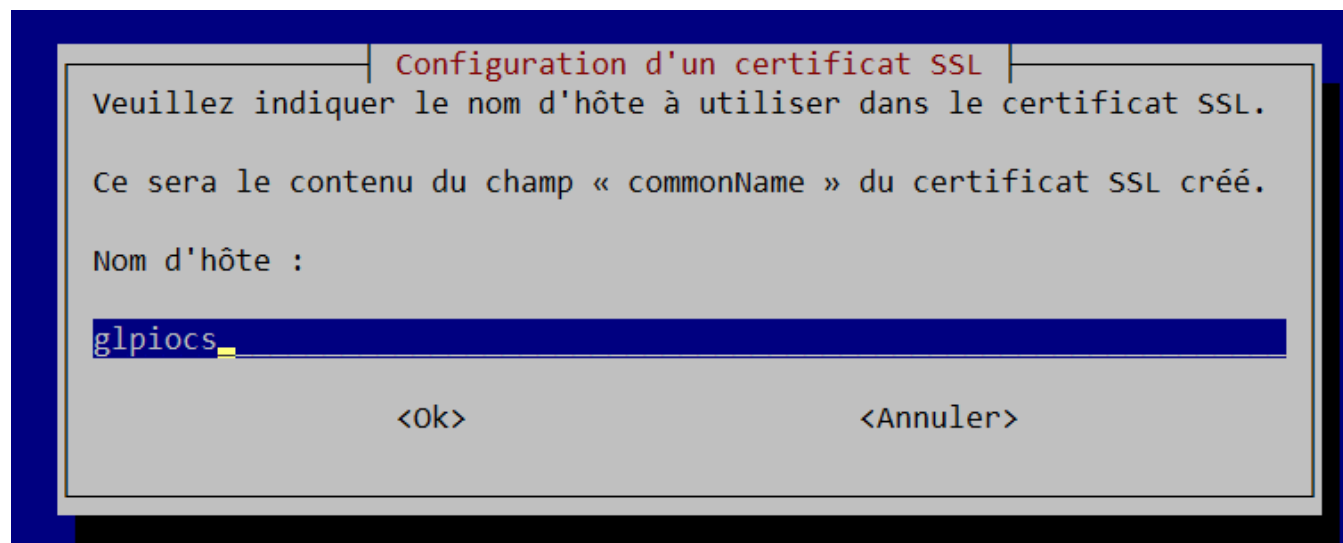
```

```

root@glpi:/etc/apache2/sites-available# root@glpi:/etc/apache2/sites-available# cd
root@glpi:~# dpkg -l ssl-cert
Souhait=inconnU/Installé/suppRimé/Purgé/H=à garder
| État=Non/Installé/fichier-Config/dépaqUeté/échec-conFig/H=semi-installé/W=attend-traitement-déclenchements
|/ Err?=(aucune)/besoin Réinstallation (État,Err: majuscule=mauvais)
||/ Nom                Version             Architecture Description
+++-----+-----+-----+-----+-----+-----+-----+-----+
ii  ssl-cert             1.1.0+nmu1         all          simple debconf wrapper for OpenSSL
root@glpi:~# dpkg -l ssl-cert

```


Il est bien installé, on va donc générer un certificat



On rentre les infos suivantes :



Notre certificat a bien été créé :

```
root@glpi:~# cd /etc/ssl/private/
root@glpi:/etc/ssl/private# ls
0851bc1f.0 safetech.pem ssl-cert-snakeoil.key
root@glpi:/etc/ssl/private#
```

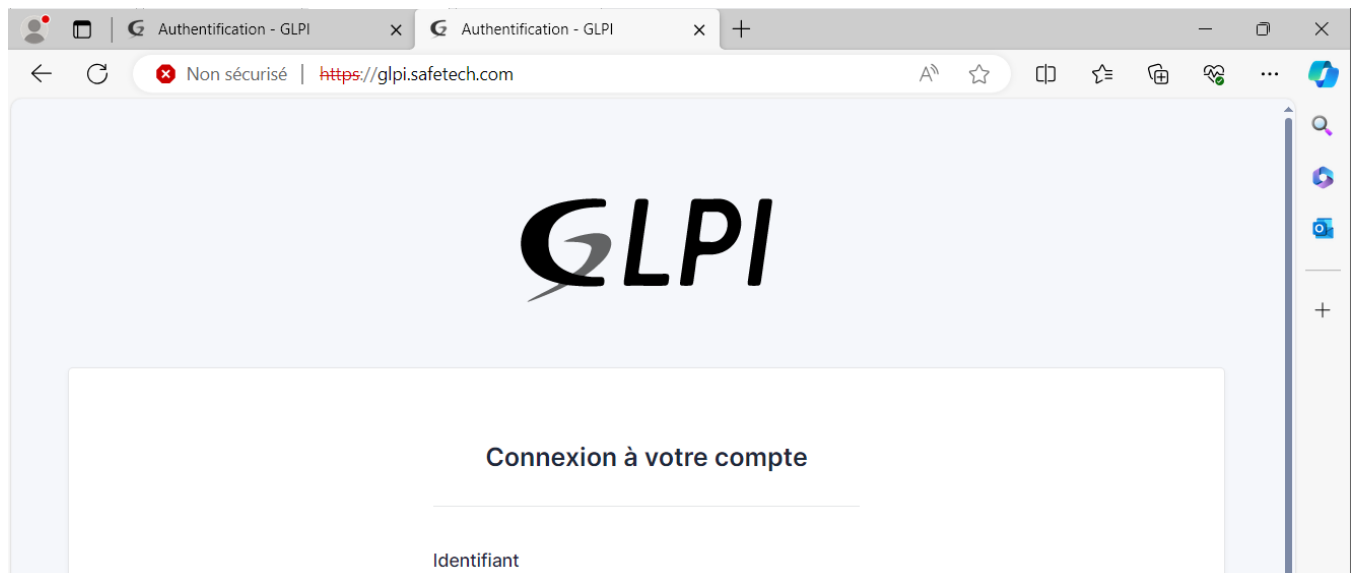
On va donc ensuite activer le mode SSL →

```
root@glpi:/etc/ssl/private# root@glpi:/etc/ssl/private# cd
root@glpi:~# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
root@glpi:~# systemctl restart apache2_
```

Et ensuite activer la conf glpi.conf →

```
root@glpi:~# root@glpi:~# a2ensite glpi.conf
Enabling site glpi.
To activate the new configuration, you need to run:
    systemctl reload apache2
root@glpi:~# systemctl restart apache2
root@glpi:~#
```

On va ensuite sur notre contrôleur de domaine et on teste si <https://glpi.safetech.com> ouvre le dashboard de notre outil de ticketing →



Ca marche parfaitement.

h. Sécurisation de l'ESXI

Par défaut, Apache envoie de requêtes HTTP par défaut qui contiennent des informations sensibles telles que l'OS utilisé, la version de l'OS, ce qui peut mettre en péril notre sécurité pour notre ESXI. On va donc masquer ces requêtes.

Voici une liste des requêtes HTTP les plus utilisées :

Requêtes HTTP	
GET	Demande une ressource au serveur Web
POST	Envoie des images / données confidentielles dans le corps
HEAD	Récupère que l'en tête de la page web
PUT	Envoie des données au serveur pour être stockées à l'URL spécifique
DELETE	Supprime la ressource spécifiée

- Pour masquer donc les requêtes http on va donc modifier le dossier de configuration Apache2 suivant : **/etc/apache2/conf-enabled/security.conf**

Les paramètres à modifier sont donc **ServerTokens** et **ServerSignatures**

```
ServerTokens OS
#ServerTokens Full

#
# Optionally add a line containing
# name to server-generated pages
# listings, mod_status and mod_in
# documents or custom error docum
# Set to "EMail" to also include
# Set to one of: On | Off | EMail
#ServerSignature Off
ServerSignature On
```

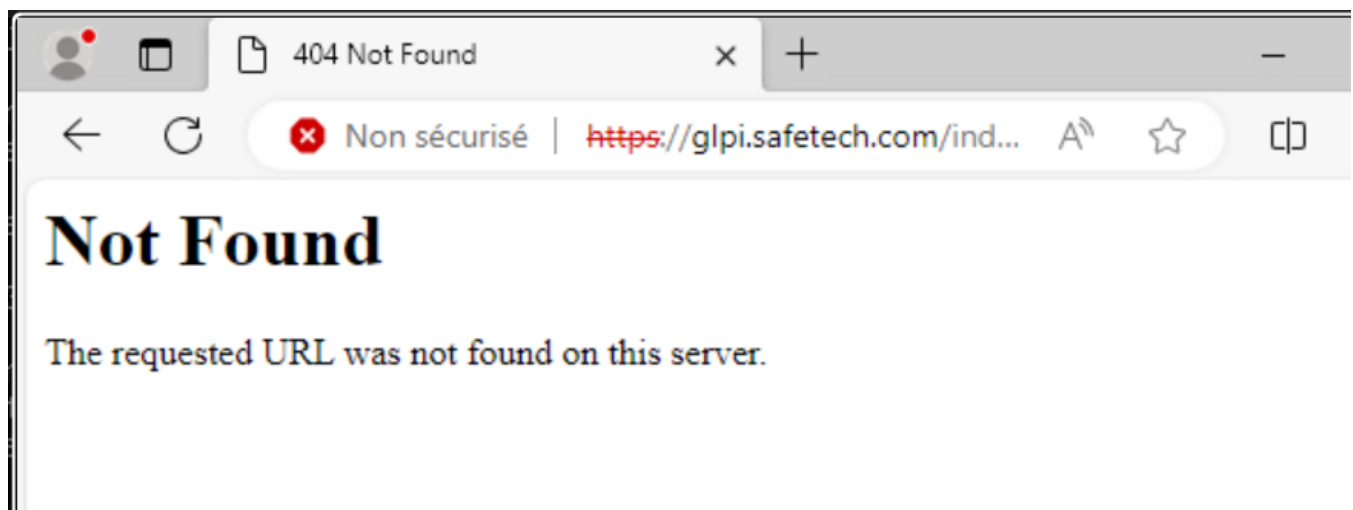
- Par défaut la configuration est comme ça, on va donc mettre #ServerTokens OS et #ServerSignature On en commentaires

```
# where Full conveys the most informatio
#ServerTokens Minimal
#ServerTokens OS
#ServerTokens Full

#
# Optionally add a line containing the s
# name to server-generated pages (intern
# listings, mod_status and mod_info outp
# documents or custom error documents).
# Set to "Email" to also include a mailt
# Set to one of: On | Off | Email
#ServerSignature Off
#ServerSignature On
```

→ Ensuite on fait `systemctl restart apache2`

On va ensuite dans <https://glpi.safetech.com/index.df>



4. Utilisation et configuration de GLPI

i. Synchronisation entre l'AD et GLPI

Notre GLPI est prêt à être utilisation, nous allons donc commencer par importer nos utilisateurs AD et synchroniser notre GLPI avec notre AD.

Pour ceci nous allons aller sur GLPI dans → Authentification-->Annuaire LDAP → Je clique sur le signe + pour rajouter un annuaire ldap → Rechercher → Cocher la ou les cases des utilisateurs à importer

389

389

Filtre de connexion

(&(objectClass=user)(objectCategory=person)((userAccountContro

BaseDN

OU=Professionnels,DC=safetech,DC=com

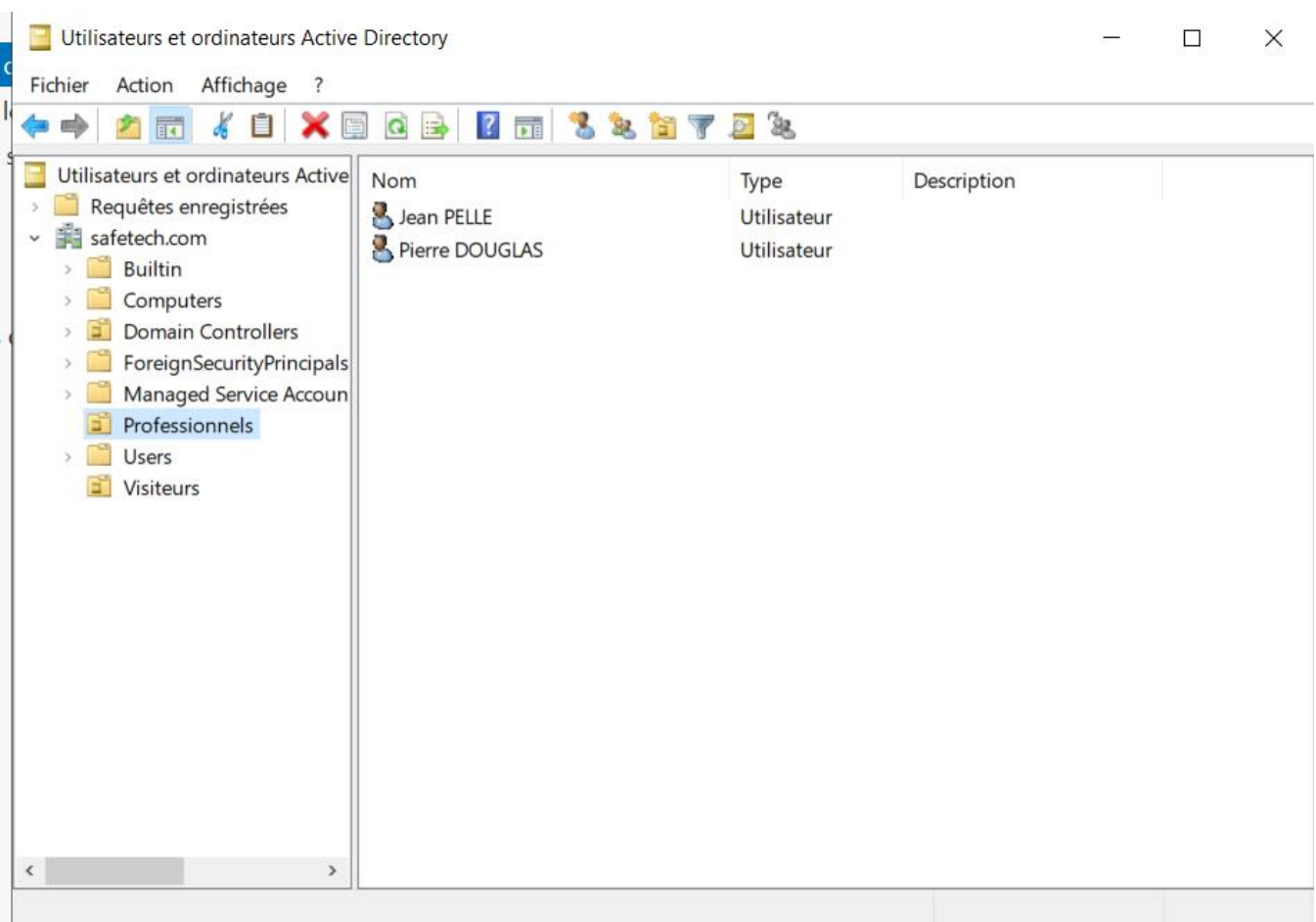
Utilisez un compte (pour les connexions non anonymes) **i**

Oui ▾

DN du compte (pour les connexions non anonymes)

CN=Administrateur,CN=Users,DC=safetech,DC=com

Mot de passe du compte (pour les connexions non anonymes)



On a déjà 2 OU « Professionnels » et « Visiteurs ». On va donc synchroniser tout ça sur notre GLPI

On va sur GLPI dans → Configuration → Authentification → Annuaire LDAP → + → Rechercher → et on coche les utilisateurs à importer

Nom
safetechdc.safetech.com

Dernière modification
2024-02-12 10:58

Serveur par défaut
Oui ▾

Actif
Oui ▾

Serveur
192.168.100.2

Port (par défaut 389)

Port (par défaut 389)
389

Filtre de connexion
(&(objectClass=user)(objectCategory=person)((userAccountContro

BaseDN
OU=Professionnels,DC=safetech,DC=com

Utilisez un compte (pour les connexions non anonymes) i
Oui ▾

DN du compte (pour les connexions non anonymes)
CN=Administrateur,CN=Users,DC=safetech,DC=com

Mot de passe du compte (pour les connexions non anonymes)

CN=Administrateur,CN=Users,DC=safetech,DC=com

Mot de passe du compte (pour les connexions non anonymes)

Effacer

Commentaires

Champ de l'identifiant
samaccountname

Champ de synchronisation i
objectguid

On va ensuite tester la connexion entre notre AD et GLPI en allant dans :

Configuration → Authentification → Annuaire LDAP → Tester la connexion

+ 🔍



1/1

Annuaire LDAP - safetechdc.safetech.com

Annuaire LDAP ▾

Tester la connexion à l'annuaire LDAP

Tester



1/1



Annuaire LDAP -
safetechdc.safetech.com

Tester



Tester la connexion à l'annuaire LDAP

Test réussi : Serveur principal safetechdc.safetech.com

Tester

Le test est réussi



j. Importation des utilisateurs de mon AD

Pour importer nos utilisateurs on va dans **Administration**→**Utilisateurs**→**Annuaire LDAP** et on fait « **Importation de nouveaux utilisateurs** »



On va ensuite cliquer sur « Rechercher »

Importation de nouveaux utilisateurs

Mode expert

Activer le filtrage par date

Critère de recherche pour les utilisateurs

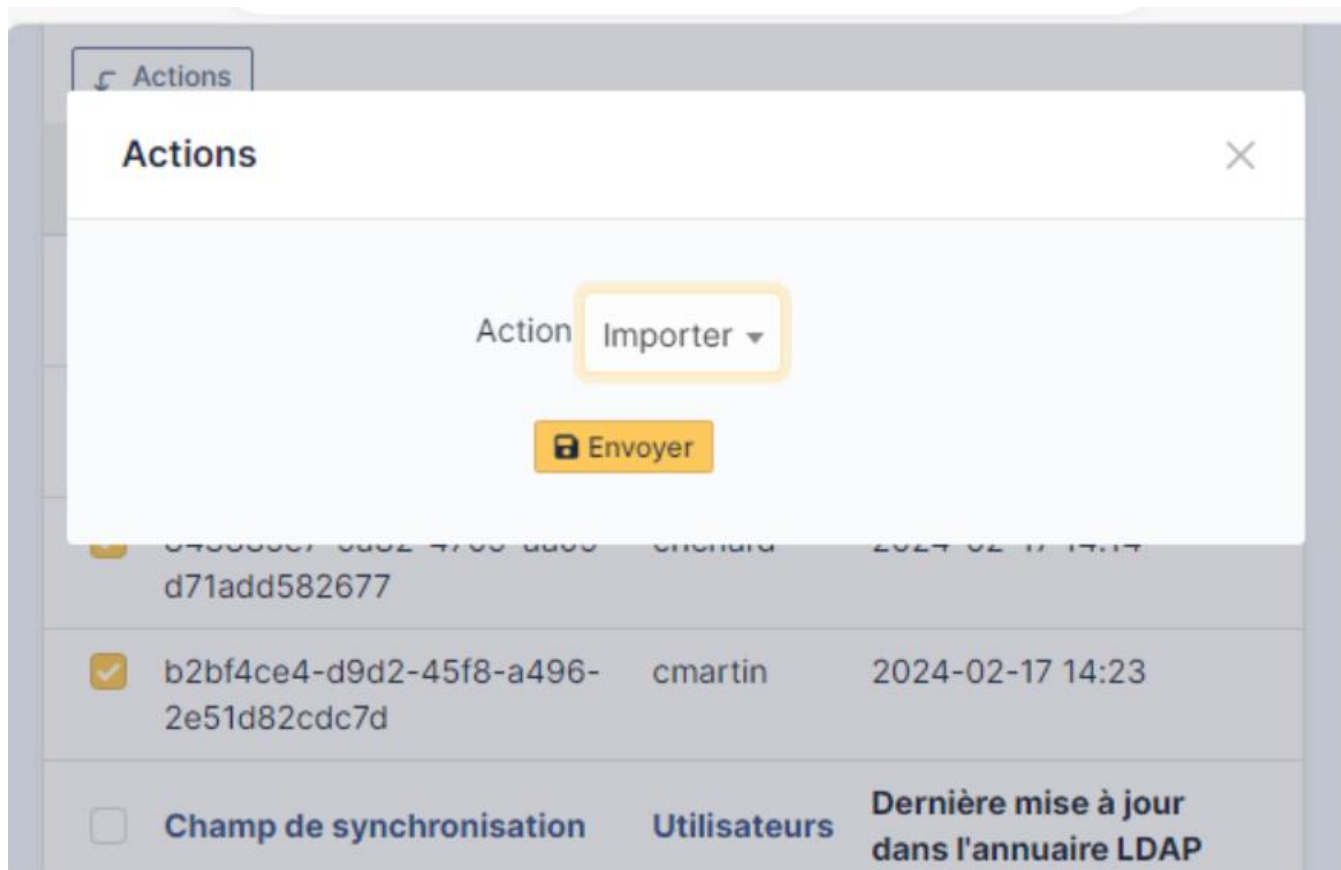
Identifiant	<input type="text"/>	Champ de synchronisation (objectguid)	<input type="text"/>
Courriel	<input type="text"/>	Nom de famille	<input type="text"/>
Prénom	<input type="text"/>	Téléphone	<input type="text"/>

Rechercher

Ensuite on voit tous nos utilisateurs

<input type="checkbox"/>	df152be4-ede8-43ef-b1b3-a3b2b6ac6cc9	pdouglas	2024-02-17 14:23
<input checked="" type="checkbox"/>	b1253e63-19c6-4037-9910-e3e307794121	jpelle	2024-02-17 14:23
<input checked="" type="checkbox"/>	843885e7-9a82-4709-aa09-d71add582677	crichard	2024-02-17 14:14
<input checked="" type="checkbox"/>	b2bf4ce4-d9d2-45f8-a496-2e51d82cdc7d	cmartin	2024-02-17 14:23
<input type="checkbox"/>	Champ de synchronisation	Utilisateurs	Dernière mise à jour dans l'annuaire LDAP

On sélectionne tout, et on fait « Actions » → « Importer » → « Envoyer »



5. Synchronisation avec Zimbra

On va synchroniser notre Zimbra avec GLPI. L'objectif est le suivant :

- Dès qu'on crée un ticket, on veut recevoir un mail sur notre boîte mail via notre serveur de messagerie Zimbra

Ainsi, nos administrateurs pourront mieux administrer et gérer les tickets de l'entreprise SAFETECH.

On va tout d'abord créer notre compte support@zimbra.safetech.com qui va créer nos tickets automatiquement →

	admin@zimbra.safetech.com	
	cmartin@zimbra.safetech.com	Clément M/
	jpelle@zimbra.safetech.com	Jean PELLI
	pdouglas@zimbra.safetech.com	Pierre Douç
	support@zimbra.safetech.com	support

On va donc envoyer un mail depuis GLPI → Zimbra

```
root@gipi: # telnet 192.168.100.4 25
Trying 192.168.100.4...
Connected to 192.168.100.4.
Escape character is '^]'.
220 zimbra.safetech.com ESMTP Postfix
helo 192.168.100.4
250 zimbra.safetech.com
mail from:<support@safetech.com>
250 2.1.0 Ok
rcpt to:<admin@safetech.com>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject: test d'envoi depuis GLPI

^R

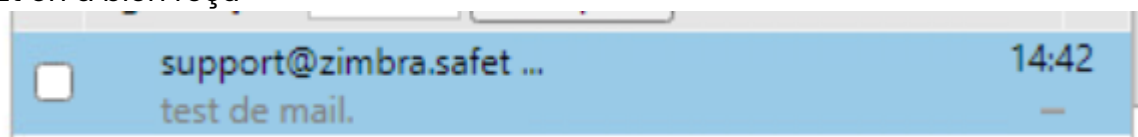
<CR><LF>

;

.
```

Ensuite on va voir si on a bien reçu le mail sur le dashboard zimbra

Et on a bien reçu



On va donc ensuite renseigner sur GLPI le mail du compte support@zimbra.safetech.com

→ On va sur GLPI dans « Administration » → « Utilisateurs »

Identifiant

Nom de famille

Prénom

Mot de passe

Confirmation mot de passe

Fuseau horaire L'utilisation des fuseaux horaires n'a pas été activé.
Exécutez la commande "php bin/console
glpi:database:enable_timezones" pour l'activer.

Actif Courriels

On remplit le courriel → support@zimbra.safetech.com et on met pour ID : GLPI et MDP : @Azerty123

On va ensuite dans → Configuration → Configuration des notifications et on coche tout

Accueil / Configuration / Notifications

Rechercher

Configuration des notifications

Activer le suivi

Activer les notifications par courriel

Activer les notifications navigateur

On remarque qu'on a déjà un autre compte GLPi → on renome le compte précédemment créé en support

Utilisateur

Habilitations 1

Identifiant

Nom de

On retourne sur la page et on coche tout → puis faire « Enregistrer »

⚠ Vous devez activer au moins un mode de notification.

Activer le suivi

Activer les notifications par courriel

Activer les notifications navigateur

 Enregistrer

On va ensuite dans configuration des mails par courrier et on remplit les infos suivantes →

Accueil / Configuration / Notifications

Rechercher

Super-Admin
Entité racine (Arborescence) GL

Notifications courriel

Courriel de l'administrateur	<input type="text" value="support@zimbra.safete"/>	Nom de l'administrateur	<input type="text" value="support@zimbra.safetech.cor"/>
Courriel de l'expéditeur <i>i</i>	<input type="text" value="support@zimbra.safete"/>	Nom de l'expéditeur du message <i>i</i>	<input type="text" value="support@zimbra.safetech.cor"/>
Adresse de réponse <i>i</i>	<input type="text" value="support@zimbra.safete"/>	Nom de réponse <i>i</i>	<input type="text"/>
Adresse de non réponse <i>i</i>	<input type="text"/>	Nom de non réponse <i>i</i>	<input type="text"/>
Ajouter des documents dans les notifications de ticket	<input type="button" value="Oui"/> ▼		
Signature des courriels	<input type="text" value="Centre d'administration de <u>ticketing</u> de l'entreprise <u>Safetech</u>."/>		
Mode d'envoi des courriels	<input type="text" value="SMTP"/>	Testateur d'envoi par	<input type="text" value="F"/>

Accueil / Configuration / Notifications

Rechercher

Super-Admin
Entité racine (Arborescence) GL

Tenter d'envoyer de nouveau dans (minutes) 5

Serveur de messagerie

Vérifier le certificat Oui

Hôte SMTP 192.168.100.4 Port 25

Identifiant SMTP (optionnel) Mot de passe SMTP (optionnel)

Effacer

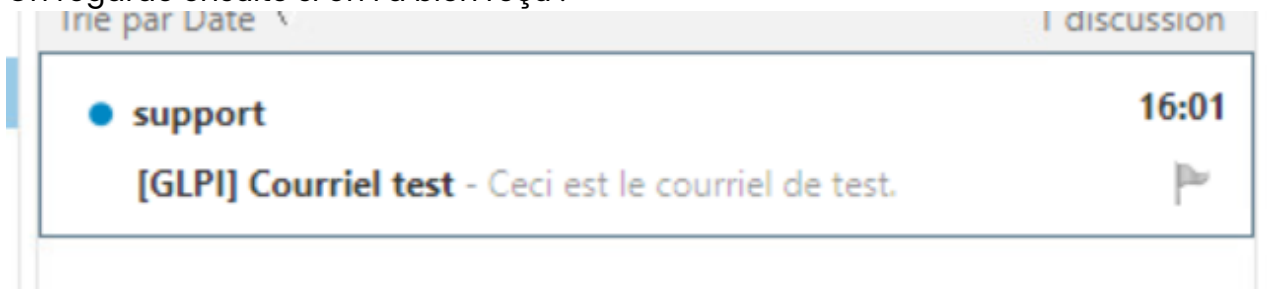
Expéditeur du message i support@zimbra.safetech.com

On teste ensuite d'envoyer un courrier →



Et on fait sauvegarder

On regarde ensuite si on l'a bien reçu :



Il est bien dans la boîte mail

Maintenant, on va configurer les actions automatiques pour que tout soit automatisé, on va donc dans Accueil → Configuration → Actions automatiques

On va dans « queued notification » et on met en CLI →

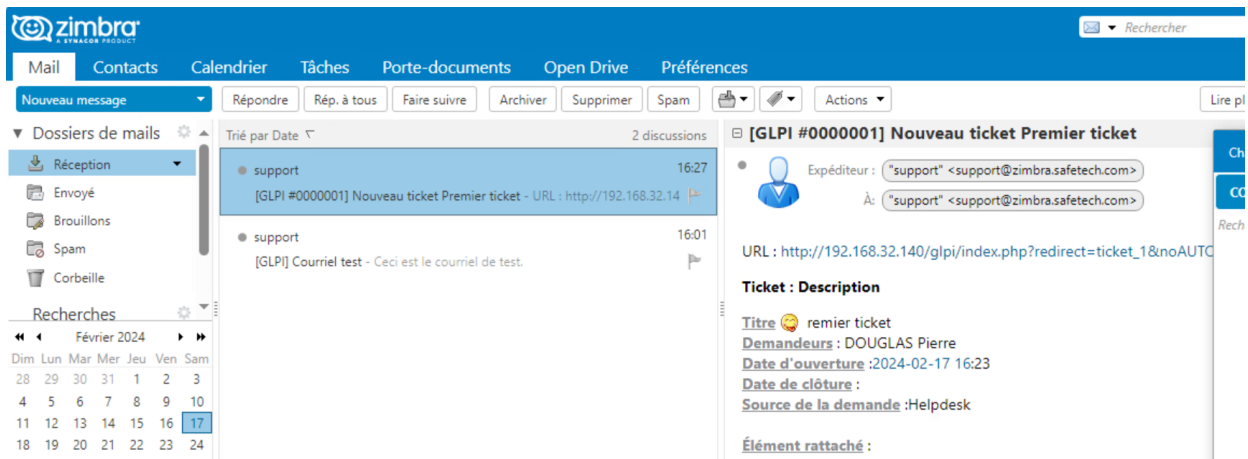
The screenshot shows the configuration page for an automatic action named 'queuednotification'. The 'Mode d'exécution' (Execution mode) is set to 'CLI'. Other settings include: 'Fréquence d'exécution' (Execution frequency) at 1 minute, 'Statut' (Status) as 'Programmée' (Scheduled), 'Plage horaires d'exécution' (Execution time range) from 0 to 24, and 'Temps de conservation des journaux (en jours)' (Log retention time in days) at 30. The last execution was on 2024-02-17 at 15:55. The description is 'Envoyer les courriels en attente' (Send emails on hold).

On enregistre, et ensuite on va tester si ça marche. On va se connecter sur un compte GLPI utilisateur et créer un ticket et voir si on reçoit un mail dans la boîte mail support

On va donc sur le compte pdouglas sur GLPi et on créé le ticket →

The screenshot shows the ticket creation form in GLPI. The 'Urgence' (Priority) is set to 'Très basse' (Very low). The 'Titre' (Title) is 'Premier ticket'. The 'Description' (Description) contains the text 'Bonjour, Premier ticket pour test la boîte support GLP|'. The user is identified as 'Self-Service Entité racine (Arborescence) PD'.

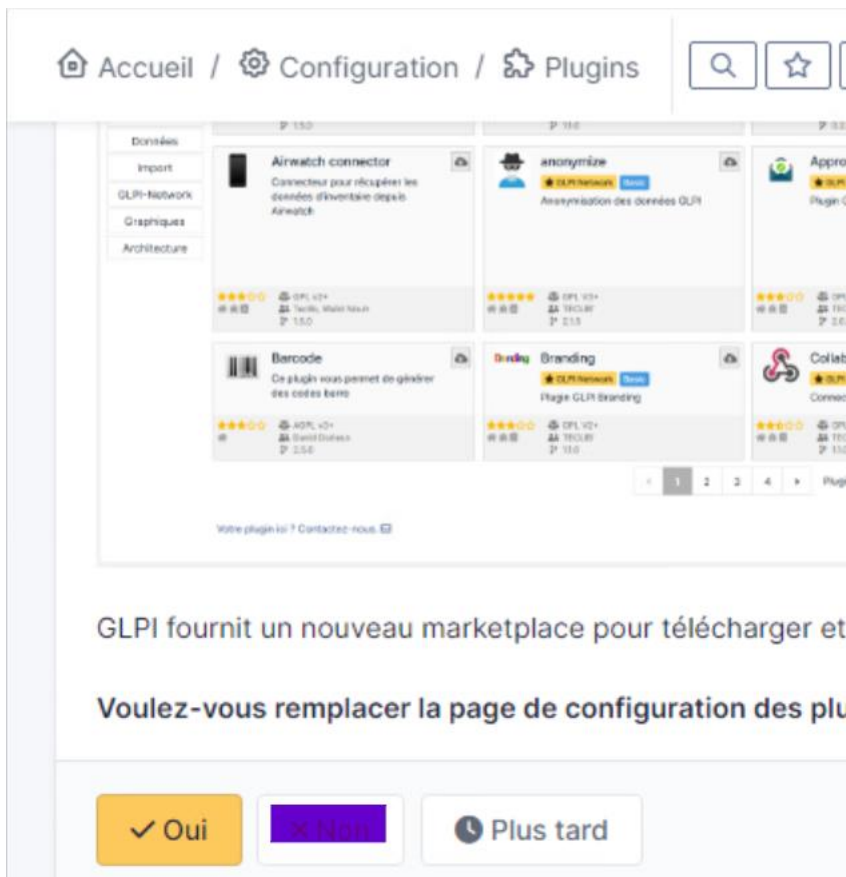
On a bien reçu le ticket :



6. Inventorisation avec OCS

Nous allons intégrer avec notre outil de ticketing, un outil permettant d'inventoriser notre parc informatique. Cet outil est appelé Fusion Inventory, qui va remonter les machines de notre parc informatique.

On va donc aller dans le marketplace et installer le plug-in FusionInventory



On met non, ensuite on va sur notre machine GLPI et on va installer le paquet github de OCS →

<https://github.com/pluginsGLPI/ocsinventoryng/releases/download/2.0.4/glpi-ocsinventoryng-2.0.4.tar.bz2>

```
root@glpi:~# wget https://github.com/pluginsGLPI/ocsinventoryng/releases/download/2.0.4/glpi-ocsinventoryng-2.0.4.tar.bz2
```

On va ensuite extraire le fichier téléchargé →

```
root@glpi:~# tar xvf fusioninventory-10.0.6+1.1.tar.bz2
```

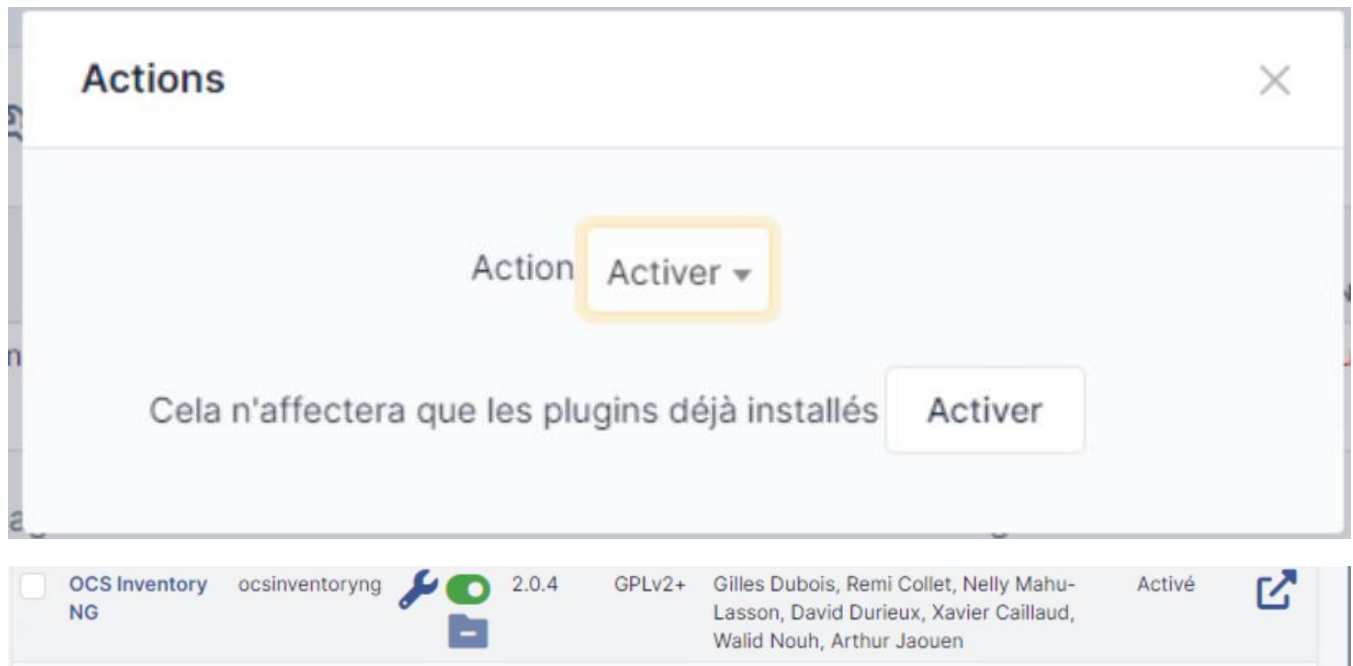
On déplace ensuite le plug-in dans le dossier plugins de GLPI :

```
root@glpi:~# mv fusioninventory /var/www/glpi/plugins/
```

Une fois le dossier Plugins avec notre OCS , on retourne sur le dashboard GLPI et on voit que notre plug in est installé

```
root@glpi:~# wget https://github.com/pluginsGLPI/ocsinventoryng/releases/download/2.0.4/glpi-ocsinventoryng-2.0.4.tar.bz2
```

On installe ensuite le plug-in dans « Actions » et on l'active ensuite



The screenshot shows a modal window titled "Actions" with a close button (X) in the top right corner. In the center, there is a button labeled "Action" with a dropdown arrow, and the word "Activer" is highlighted with a yellow box. Below this, there is a message: "Cela n'affectera que les plugins déjà installés" followed by another "Activer" button. At the bottom, there is a table listing installed plugins. The first row is for "OCS Inventory NG" (plugin name: ocsinventoryng, version: 2.0.4, license: GPLv2+), with a status of "Activé". The authors listed are Gilles Dubois, Remi Collet, Nelly Mahu-Lasson, David Durieux, Xavier Caillaud, Walid Nouh, and Arthur Jaouen.

Plugin	Version	Licence	Statut
OCS Inventory NG	2.0.4	GPLv2+	Activé

On va ensuite configurer le CRON pour faire tourner les plug-ins →



On va ensuite sur la machine GPLPI et on active le crontab

```
root@glpi:~# crontab -u www-data -e_
```

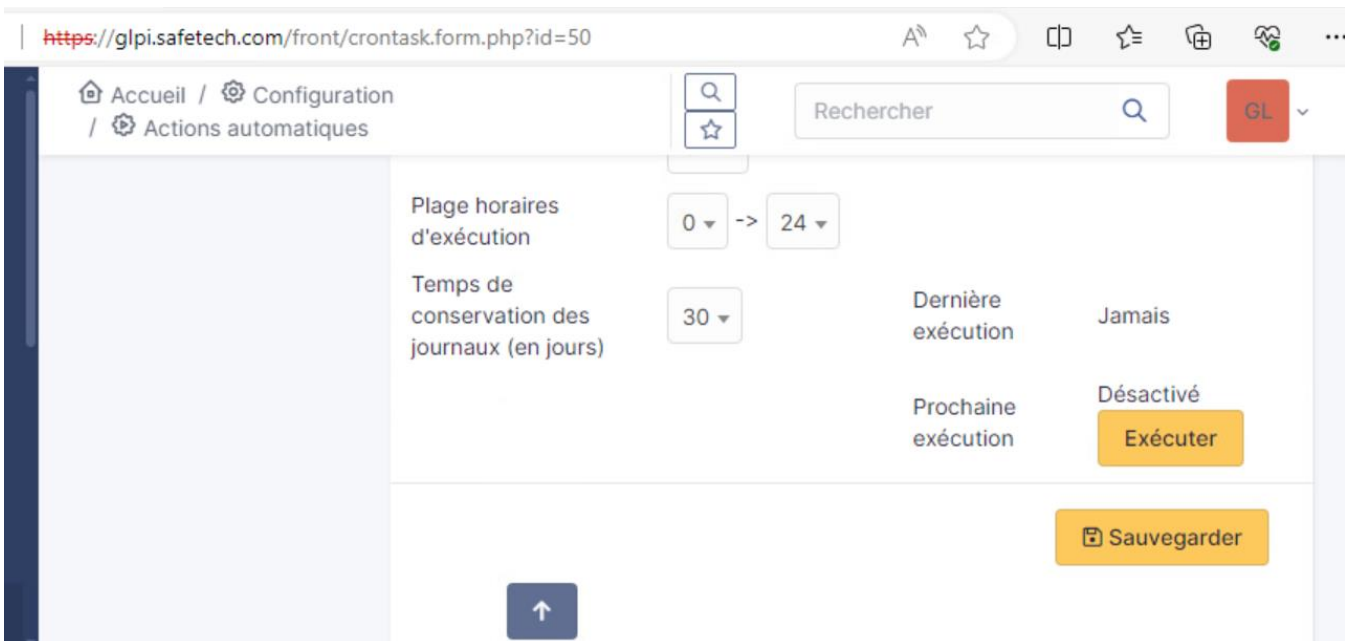
Et on remplit ca :

```
* * * * * cd /var/www/glpi/front/ && /usr/bin/php cron.php &>dev/null
```

Et on restart les tâches cron :

```
root@glpi:~# /etc/init.d/cron restart _
```

On va ensuite dans « taskcheduler » dans la configuration automatique GLPI et on exécute le CRON
→



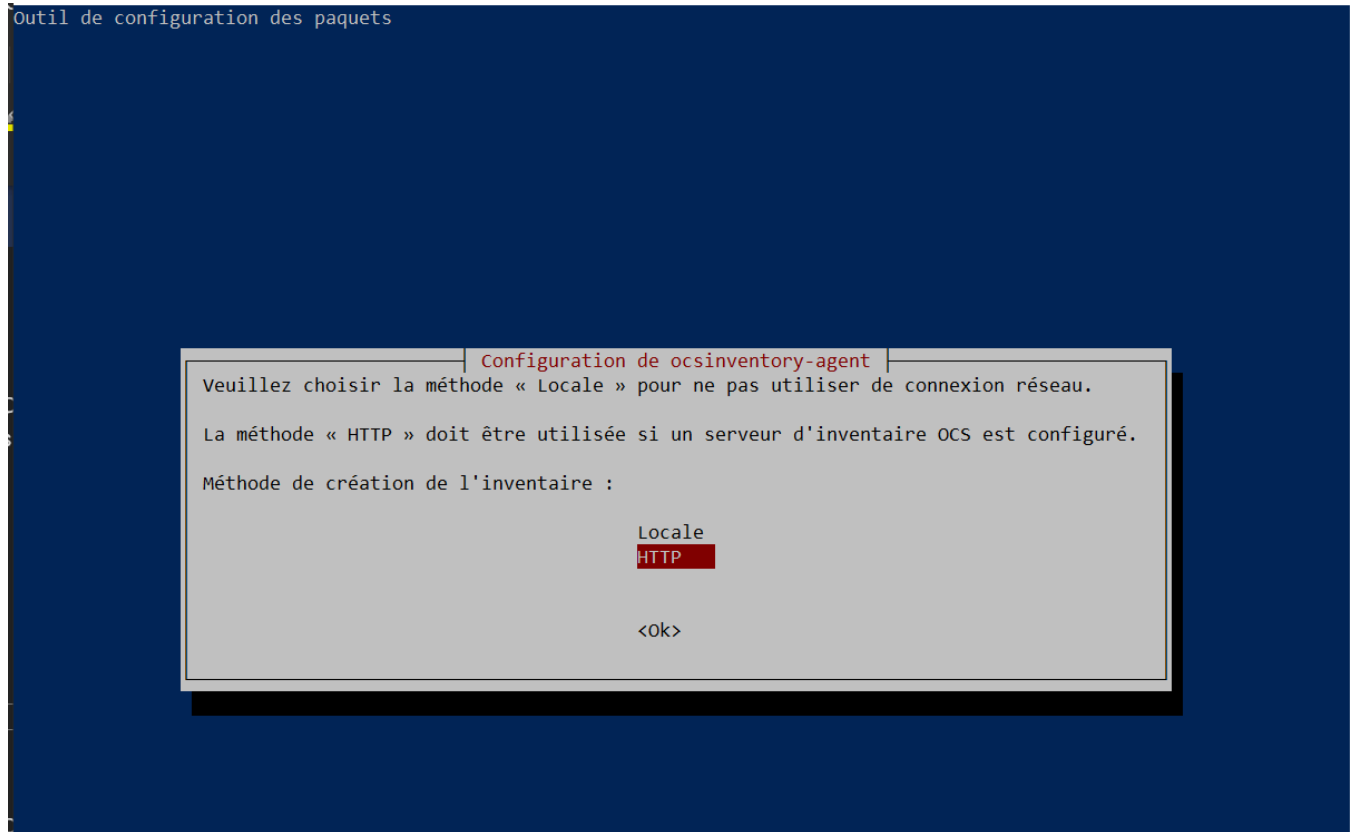
k. Installation d'un agent sur une machine Linux

On va donc installer un agent sur une machine Linux, pour vérifier si ça marche. On va donc l'installer sur notre serveur Zimbra

On commence par installer le paquet agent-ocs

```
root@zimbra:~# apt install ocsinventory-agent
```

Ensuite on met http :



```
wget https://github.com/OCSInventory-NG/UnixAgent/releases/download/v2.10.0/Ocsinventory-Unix-Agent-2.10.0.tar.gz
```

```
root@zimbra:~# os
os: command not found
root@zimbra:~# ls
Ocsinventory-Unix-Agent-2.10.0          zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954
Ocsinventory-Unix-Agent-2.10.0.tar.gz zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz
snap
root@zimbra:~# cd Ocsinventory-Unix-Agent-2.10.0/
root@zimbra:~/Ocsinventory-Unix-Agent-2.10.0# sudo perl Makefile.PL
```

```
# sudo make
```

```
root@zimbra:~/Ocsinventory-Unix-Agent-2.10.0# root@zimbra:~/Ocsinventory-Unix-Agent-2.10.0# sudo make install
```

```
Installing /usr/local/bin/ipdiscover
Appending installation info to /usr/local/lib/x86_64-linux-gnu/perl/5.30.0/perllocal.pod
[ ! -f run-postinst ] || /usr/bin/perl postinst.pl
Do you want to configure the agent?
Please enter 'y' or 'n'?> [y] █
```

/var/log/ocs-inventory-agent.log

```
Installing /usr/local/man/man3/Ocsinventory::Agent::Common.3pm
Installing /usr/local/bin/ocsinventory-agent
Installing /usr/local/bin/ipdiscover
Appending installation info to /usr/local/lib/x86_64-linux-gnu/perl/5.30.0/perllocal.pod
[ ! -f run-postinst ] || /usr/bin/perl postinst.pl
Do you want to configure the agent?
Please enter 'y' or 'n'?> [y] y
Where do you want to write the configuration file?
0 -> /etc/ocsinventory
1 -> /usr/local/etc/ocsinventory
2 -> /etc/ocsinventory-agent
?> 2
Value must be between 0 and 2
?> é
Value must be between 0 and 2
?> 2
Value must be between 0 and 2
?> 1
Do you want to create the directory /usr/local/etc/ocsinventory?
Please enter 'y' or 'n'?> [y]
Should the old unix_agent settings be imported?
Please enter 'y' or 'n'?> [y]
[info] The config file will be written in /usr/local/etc/ocsinventory/ocsinventory-agent.cfg,
What is the address of your ocs server?> https://glpi.safetech.com
Do you need credential for the server? (You probably don't)
Please enter 'y' or 'n'?> [n]
Do you want to apply an administrative tag on this machine?
Please enter 'y' or 'n'?> [y] server - zimbra
Do you want to apply an administrative tag on this machine?
Please enter 'y' or 'n'?> [y] y
tag?> server - zimbra
Do you want to install the cron task in /etc/cron.d?
Please enter 'y' or 'n'?> [y]
Where do you want the agent to store its files? (You probably don't need to change it)?> [/var/lib/ocsinventory-agent]
Do you want to create the /var/lib/ocsinventory-agent directory?

Please enter 'y' or 'n'?> [y]
Should I remove the old unix_agent?
Please enter 'y' or 'n'?> [n]
Do you want to activate debug configuration option?
Please enter 'y' or 'n'?> [y]
Do you want to use OCS Inventory NG Unix Unified agent log file?
Please enter 'y' or 'n'?> [y] /var/log/ocs-inventory-agent.log█
```

7. Identifiants

ID : GLPI

Mdp : @Azerty123