PARIS PANTHÉON-ASSAS UNIVERSITÉ

Installation et configuration de GLPI

BTS SIO SISR 2022 – 2024

Contexte :
Dans le cadre de l'entreprise SITKA, une société spécialisée dans la gestion informatique, l'objectif principal est d'améliorer la gestion du parc informatique et du service desk en mettant en place une solution intégrée basée sur GLPI, une application open-source de renom. Cette solution offre une multitude de fonctionnalités, allant de la gestion des ressources informatiques à la création de tickets d'assistance, en passant par la liaison avec des annuaires LDAP et des outils d'inventaire automatisé.

À Propos de SITKA

- **Nom de l'Entreprise : SITKA**
- **Type de Société : Société Anonyme (SA)**
- **Nombre d'Employés : 1560**
- **Le chiffre d'affaires annuel de SITKA s'élève à 19 600 000€**

Objectifs du Projet :

Améliorer la Gestion du Parc Informatique : GLPI permettra une gestion centralisée et efficace des ressources matérielles et logicielles du parc informatique, y compris les ordinateurs, les périphériques, les logiciels et les licences.

Optimiser le Service Desk : GLPI offre des fonctionnalités avancées de gestion des tickets d'assistance, permettant à notre équipe informatique de suivre et de résoudre efficacement les incidents et les demandes des utilisateurs.

Intégration avec des Annuaire LDAP et des Outils d'Inventaire Automatisé : GLPI peut être intégré avec des annuaires LDAP existants, facilitant ainsi l'authentification des utilisateurs et la gestion des droits d'accès. De plus, GLPI peut être associé à des outils d'inventaire automatisé pour maintenir des informations précises sur le parc informatique.

Conclusion :
L'implémentation de GLPI chez SITKA représente une étape significative dans l'amélioration de la gestion informatique. Cette solution intégrée offrira à mon entreprise les outils nécessaires pour optimiser la gestion du parc informatique, améliorer la satisfaction des utilisateurs et soutenir la croissance continue de l'entreprise.

1- Mise en place d'un serveur **LAMP**

a- Mise à jour de la distribution
b- Renommer la machine en glpi c- Configuration des interfaces réseaux d- Installation d'apache2 PHP et Mariadbc e- Restriction de l'accès à la base de données mariadb

2- Installation et configuration de glpi
   a- Installation des extensions PHP
   b- Création de la base de données glpi (dbglpi) et l'utilisateur (userglpi)
   c- Téléchargement et installation de GLPI

3- Configuration et sécurisation de l'accès à glpi a- Accès à glpi avec un nom de domaine b- Sécurisation de glpi en masquant sa version et l'os utilisé. c- Sécurisation par SSL

4- Liaison de glpi avec active directory
   a- Création de l'UO et des utilisateurs sur le contrôleur de domaine
   b- Création de la liaison avec l'annuaire ldap
   c- Importation des utilisateurs à partir de notre base d'annuaire ldap

5- Liaison de glpi avec ocs-inventory

6- Création de tickets
   a- Notification par mail b- Notification par collecteurs
   c- Gestion des tickets

7- Fusion-inventory
   a- Installation du plugin fusion-inventory b- Installation des agents fusion-inventory

Solution open--source de gestion de parc informatique et de service desk, GLPI est une application Full Web pour gérer l'ensemble de vos problématiques de gestion de parc informatique : de la gestion de l'inventaire des composantes matérielles ou logicielles d'un parc informatique à la gestion de l'assistance aux utilisateurs.

Des fonctionnalités à forte valeurs ajoutées

- Gestion et suivi des ressources informatiques
- Gestion et suivi des licences
- Gestion et suivi des consommables
- Base de connaissances
- Gestion des réservations
- Service Desk (helpdesk, SLA.)
- Inventaire automatisé
- Télé déploiement

Avec l'utilisation conjointe de la solution d'inventaire OCS Inventory NG ou de la suite de plugins FusionInventory

Des avantages importants pour votre structure

- Réduction des coûts
- Optimisation des ressources
- Gestion rigoureuse des licences
- Démarche qualité
- Satisfaction utilisateur
- Sécurité

Diffusé sous licence libre GPL, GLPI est disponible gratuitement.

Une solution rapide à déployer et simple à utiliser

- Prérequis techniques minimums
- Mise en production immédiate
- Accessible depuis un simple navigateur Web
- Interface paramétrable
- Utilisation intuitive
- Ajout aisé de fonctionnalité grâce à un système de plugins
- Communication avec des annuaires existants

Ceci revient à mettre en place un serveur **LAMP** (Linux, Apache, PHP et MySQL) GLPI nécessite un serveur Web prenant en charge PHP, comme :

- Apache 2 (ou plus récent) ;

- Nginx ;
- Microsoft IIS .

1- Mise en place d'un serveur **LAMP**

a- Mise à jour de la distribution

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

b- Renommer la machine en glpi

```
root@debian:~# hostnamectl set-hostname glpi
```

c- Configuration des interfaces réseaux

- Ajouter une carte et la mettre sur un Lan segment, l'autre carte doit rester en Nat pour pouvoir aller sur Internet afin de télécharger glpi.

```
root@glpi:~# vim /etc/network/interfaces
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

# The secry network interface
allow-hotplug ens36
iface ens36 inet static
address 172.20.0.30/24
```

```
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:29:74:f6:f7 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.44.131/24 brd 192.168.44.255 scope global dynamic ens33
       valid_lft 1682sec preferred_lft 1682sec
    inet6 fe80::20c:29ff:fe74:f6f7/64 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:29:74:f6:01 brd ff:ff:ff:ff:ff:ff
    altname enp2s4
```

Il ne faut pas oublier d'activer la carte rajoutée

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

d- Installation d'**apache2 PHP et Mariadb**

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

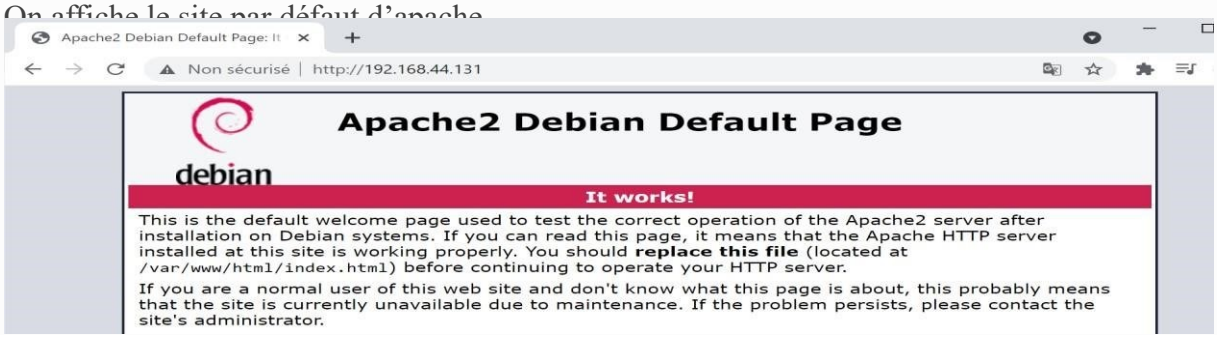
On vérifie le bon fonctionnement d'apache

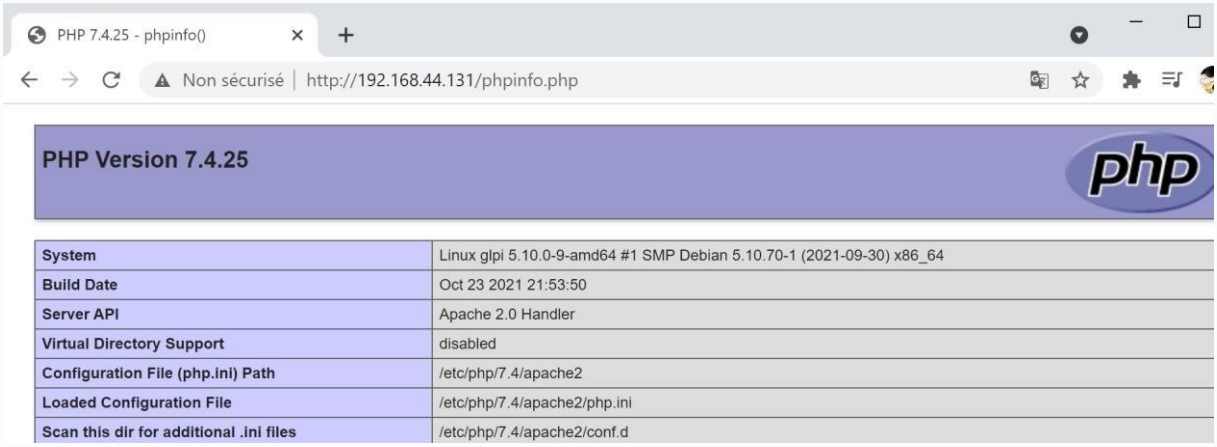
On teste le bon fonctionnement du PHP, en créant une page phpinfo.php dont le contenue est ci-dessous

```
root ocs-glpi:~# echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

```
root@glpi:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2021-11-11 10:04:55 CET; 8min ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2186 (apache2)
      Tasks: 55 (limit: 2303)
     Memory: 8.9M
        CPU: 98ms
     CGroup: /system.slice/apache2.service
             ├─2186 /usr/sbin/apache2 -k start
             ├─2426 /usr/sbin/apache2 -k start
             └─2427 /usr/sbin/apache2 -k start
```

On affiche le site par défaut d'apache





e- Restriction de l'accès à la base de données mariadb

On lance le script de sécurité **mysql_secure_installation** pour restreindre l'accès au serveur

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

On va devoir répondre à la multitude de questions qui vont s'afficher

On définit le mot de passe root :

On tape entrée

Enter current password for root (enter for none: entree

On nous demande si on veut créer un mot de passe pour le compte root de la base de données. Il faut choisir N. Le compte root de MariaDB est lié à la maintenance du système, nous ne devons pas modifier les méthodes d'authentification configurées pour ce compte.

le compte root de la base de données configuré pour s'authentifier à l'aide du plugin **unix_socket**

Switch to unix_socket authentication [Y/n] n

Change the root password? [Y/n] Y
New password:**root**
Re-enter new password:**root** Password updated successfully**!**

On supprime les utilisateurs anonymes, de root, etc...

Remove anonymous **users**? [Y/n] Y

les connexions distantes

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

La base de test

Remove **test** database and access to it? [Y/n] Y

Recharger les tables de privilèges maintenant

Reload privilege tables now? [Y/n] Y

2- Installation et configuration de glpi

a-

Installation des extensions PHP

Les extensions PHP suivantes sont requises pour que l'application glpi fonctionne correctement :

- curl : pour l'authentification CAS, le contrôle de version GLPI, la télémétrie, … ;
- fileinfo : pour obtenir des informations supplémentaires sur les fichiers ;
- gd : générer des images ;
- json : pour obtenir la prise en charge du format de données JSON ;
- mbstring : pour gérer les caractères multi-octets ;
- mysqli : pour se connecter et interroger la base de données ;
- session : pour obtenir le support des sessions utilisateur ;
- zlib : pour obtenir les fonctions de sauvegarde et de restauration de la base de données ;
- simplexml ;
- xml ;
- intl .

Même si ces extensions ne sont pas obligatoires, il est conseillé de les installer.
Les extensions PHP suivantes sont requises pour certaines fonctionnalités supplémentaires de GLPI :

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

Configuration

Le fichier de configuration PHP (php.ini) doit être adapté pour refléter les variables suivantes :

```
memory_limit = 64M ;        // max memory limit file_uploads
= on ;
max_execution_time = 600 ;  // not mandatory but recommended session.auto_start
= off ;
session.use_trans_sid = 0 ; // not mandatory but recommended
```

Maintenant on installe toutes les extensions nécessaires au fonctionnement de glpi, on peut lister toutes les extensions avec la commande ci-dessous

```
root@glpi:~# apt search ^php-
```

Donc on installe toutes ces extensions PHP sur notre terminal

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

Redémarrer apache2

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

b- Création de la base de données glpi (dbglpi) et l'utilisateur (userglpi)

Pour fonctionner, GLPI nécessite un serveur de base de données

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

Je crée une base de données qui s'appelle **dbglpi**

```
MariaDB [(none)]> create database dbglpi;
Query OK, 1 row affected (0.001 sec)
```

Je crée un utilisateur userglpi et je lui donne tous les privileges sur la bases dbglpi

```
MariaDB [(none)]> grant all privileges on dbglpi.* to userglpi@'localhost' identified by
'userglpi';
Query OK, 0 rows affected (0.002 sec)
```

Je recharge les droits

```
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)
```

Vérification de mes requêtes

J'affiche ma base de données

```
MariaDB [(none)]> show databases;
```

```
+--------------------+
| Database           |
+--------------------+
| dbglpi             |
| dbocs              |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
5 rows in set (0.005 sec)
```

J'affiche les utilisateurs dans mariadb

MariaDB [dbocs]> **select user,host from mysql.user;**

```
+-------------+-----------+
| User        | Host      |
+-------------+-----------+
| mariadb.sys | localhost |
| mysql       | localhost |
| root        | localhost |
| userglpi    | localhost |
| userocs     | localhost |
+-------------+-----------+
5 rows in set (0.006 sec)
```

J'affiche les droits de l'utilisateur userglpi

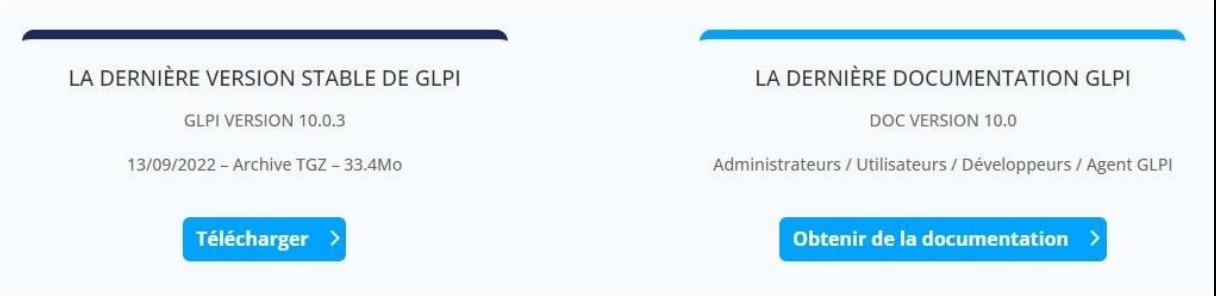
MariaDB [dbocs]> **SHOW GRANTS FOR userglpi@localhost;**

```
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)
```

c- Téléchargement et installation de GLPI

On va sur le site de glpi et on copie le lien de téléchargement

Le lien de téléchargement est : tar x on copie le lien



On crée un répertoire **tmp** dans lequel on va télécharger glpi, avec la commande wget

```
wget https://github.com/glpi-project/glpi/releases/download/10.0.10/glpi-10.0.10.tgz
```

```
root@glpi:~# mkdir tmp

root@glpi:~# cd tmp

root@glpi:~/tmp# wget https://github.com/glpi-project/glpi/releases/download/9.5.6/glpi-9.5.6.tgz
glpi-10.0.3.tgz                     100%[=========================================================>]  56,35M  2,94MB/s    ds 30s
2022-10-10 23:01:54 (1,91 MB/s) – « glpi-10.0.3.tgz » sauvegardé [59087820/59087820]
```

On décompresse notre fichier téléchargé dans /var/www/html.ls

```
root@glpi:~/tmp# tar xzf glpi-9.5.6.tgz -C /var/www/html
```

na

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

On donne les droits sur le dossier et les sous dossiers ainsi que les fichiers GLPI au compte et au groupe **www-data**

```
root@glpi:/var/www/html# ls -l
total 20
drwxr-xr-x 21 user user  4096 15 sept. 10:51 glpi
-rw-r--r--  1 root root 10701 11 nov.  16:36 index.html
-rw-r--r--  1 root root    24 11 nov.  17:28 phpinfo.php
```

```
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 21 www-data www-data  4096 15 sept. 10:51 glpi
-rw-r--r--  1 root     root     10701 11 nov.  16:36 index.html
-rw-r--r--  1 root     root        24 11 nov.  17:28 phpinfo.php
```

Dans le fichier php.ini il faut mettre session.cookie httponly à **on**

```
root@glpi:~# vim /etc/php/7.4/apache2/php.ini
```

```
; Whether or not to add the httpOnly flag to the cookie, which makes it
; inaccessible to browser scripting languages such as JavaScript.
; http://php.net/session.cookie-httponly
session.cookie_httponly = on
```

Allez le navigateur *sur* http://votre_ip/glpi ,à la page pour terminer l'installation va s'afficher.

On sélectionne la langue et on appuie sur ok pour continuer

On tombe sur cette fenêtre expliquant le type de licence utilisée pour GLPI

On commence notre installation ou on met à jours notre GLPI déjà installé

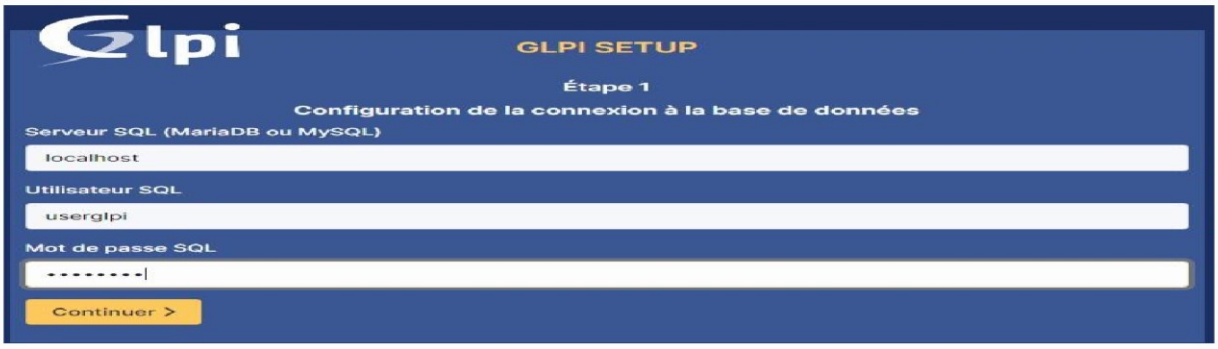
Le programme d'installation vérifie si les prérequis sont réuni pour entamer l'installation de glpi


GLPI SETUP
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
Requis pour l'accès à distance aux ressources (requêtes des agents d'inventaire, Marketplace, flux RSS, ...).
Requis gd extension
Requis pour le traitement des images.
Requis intl extension
Requis pour l'internationalisation.
Requis libxml extension
Requis pour la gestion XML.
Requis zlib extension
Requis pour la gestion de la communication compressée avec les agents d'inventaire, l'installation de paquets gzip à partir du Marketplace et la génération de PDF.
Requis Libsodium ChaCha20-Poly1305 constante de taille
Activer l'utilisation du cryptage ChaCha20-Poly1305 requis par GLPI. Il est fourni par libsodium à partir de la version 1.0.12.
Requis Permissions pour les fichiers de log
Requis Permissions pour le répertoire des données variables
Suggéré Accès protégé au répertoire des fichiers
L'accès Web aux répertoires GLPI var doit être désactivé afin d'empêcher tout accès non autorisé à ceux-ci.
L'accès web au dossier "files" ne devrait pas être autorisé
Vérifier le fichier .htaccess et la configuration du serveur web
Suggéré Configuration de sécurité pour les sessions
Permet de s'assurer que la sécurité relative aux cookies de session est renforcée.
Suggéré exif extension
Renforcer la sécurité de la validation des images.

On se connecte sur la base de donné MariaDB

-Serveur SQL (MariaDB ou MySQL) : **localhost**

-Utilisateur SQL : **userglpi**
-Mot de passe SQL : **userglpi**

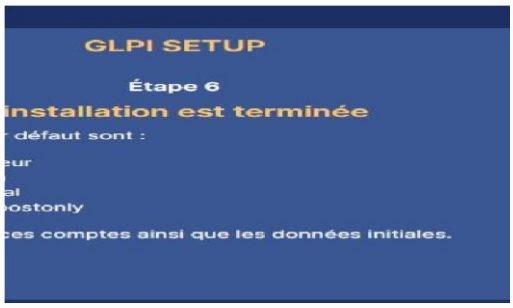


On sélectionne notre base de données crée auparavant

Choisissez d'envoyer ou non vos données de statistiques

Soutenir le projet avec un don

Notre installation a réussi



Il reste plus qu'à vous connecter :

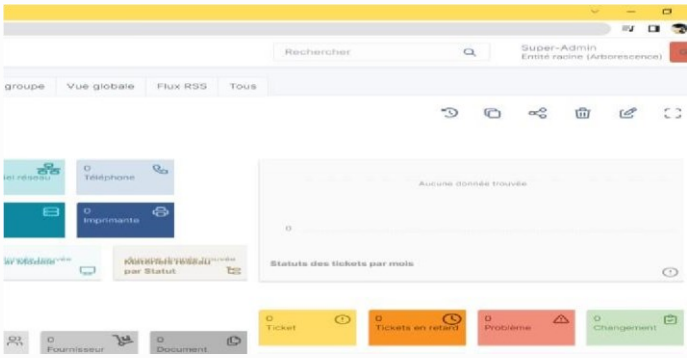
- Identifiant : **glpi**
- Mot de passe : **glpi**

On a deux messages d'erreurs

- Mot de passe par défaut pour certains comptes glpi post-only tech norma qu'on doit changer ; il faut cliqu
- sur chaqu'un des trois utilisateurs et changer son mot de passe. ou
- Le fichier Install qu'on doit supprimer, renommer déplacer

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

En actualisant notre page on a plus d'erreurs

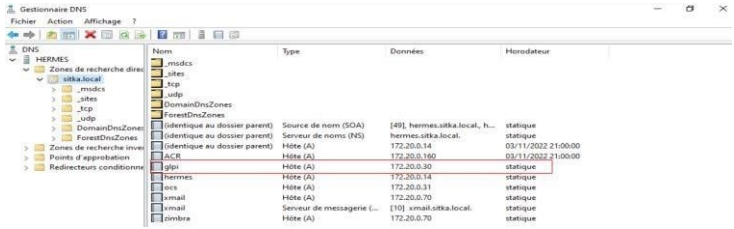


3- Configuration et sécurisation de l'accès à glpi

a. Accès à glpi avec un nom de domaine i-

Création d'un enregistrement DNS

Pour avoir un accès à l'interface web glpi avec le nom de domaine ; on crée un enregistrement de type A sur notre serveur DNS.



j- Configuration du Virtual host

Dans le répertoire **/etc/apache2/sites-available** je cree un fichier **glpi.conf**

```
root@glpi:~# cd /etc/apache2/sites-available/
root@glpi:/etc/apache2/sites-available# vim glpi.conf
```

Je crée et je configure mon fichier glpi.conf comme indiqué ci-dessous

```
<IfModule mod_ssl.c>
    <VirtualHost *:80>
  ServerName glpi.sitka.local
  DocumentRoot /var/www/html/glpi/public

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

<Directory /var/www/glpi/public>
     Require all granted
     RewriteEngine On

     RewriteCond %{REQUEST_FILENAME} !-f
     RewriteRule ^(.*)$ index.php [QSA,L]
  </Directory>
</VirtualHost>
</ifmodule>
```

```
<IfModule mod_ssl.c>
      <VirtualHost *:443>
    ServerName glpi.sitka.local
    DocumentRoot /var/www/glpi/public

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

<Directory /var/www/glpi/public>
        Require all granted
        RewriteEngine On
        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]
    </Directory>
</VirtualHost>
</ifmodule>
```

Je démarre me mode rewrite Ainsi que apache2

```
root@glpi:~# a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

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

Je déplace le répertoire glpi vers /var/www

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

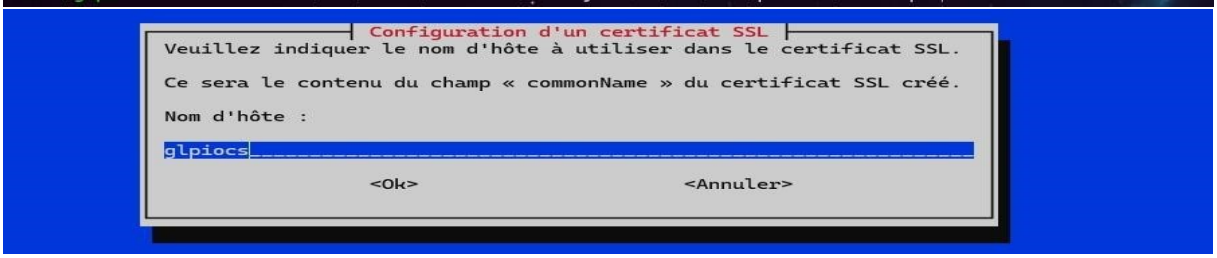
c- Sécurisation de l'accès par l'interface web glpi avec du ssl i- Création du certificat SSL On vérifie la présence du paquet ssl-cert

```
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
```

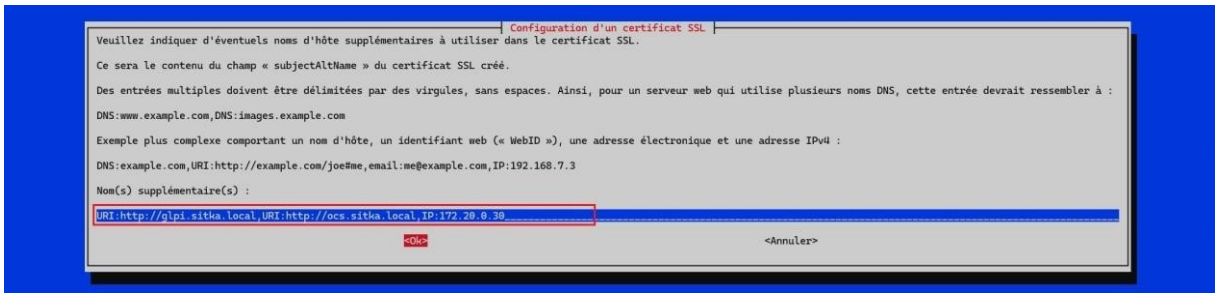
Création d'un fichier pem (Privacy Enhanced Mail (PEM)) contenant un certificat autosigné et une clé privée.

```
root glpi:~# make-ssl-cert /usr/share/ssl-cert/ssleay.cnf  /etc/ssl/private/sitka.pem
```

```
root@glpi:~# make-ssl-cert /usr/share/ssl-cert/ssleay.cnf  /etc/ssl/private/sitka.pem
```



On rentre les adresses suivantes :



On vérifie la création du fichier pem

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

En affichant sitka.pem on se rend compte s'aperçoit qu'il possède un certificat et une clé privé

```
root@glpi:/etc/ssl/private# cat sitka.pem
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCkRFlDEEPOuORl
ondgr/Aq5jVR3Y+G/FM6IAnTE5rUHCEmLtsTKHIkhwUnAad9m8r0NL5S5y17bCXY
2H6TDttP5mOZWD5kNI7a8xDoh1bi0OFOBusBXYlpCENzhVVZS+PmRYKmuF1SoRyU
eBR9Xt7LI6LIVGkNc3d3XniOkuH9jfbFZNpjKS7lsALzNxxU34sjo/+GbCCnCsIY
sk9pVxh76e5RnVvnnNuKXK+kwKus/JrIigytDoTbuP8i5LJdTH9e2xQFfwG8fpc7
g/NxFuEH7V0/gpWqFblwtvmyR/ALaidDFxK+/f0ZU+BpdqU2lYushhN/u35Q8QjN
YVe6XrYLAgMBAAECggEAO7luCuga/0pSIHHVnZ3aYH6a3E0GJjoPuI51g/0Yyg4A
L3XRyUFnXsiIowoC77R5MhkLkfFLpBhKGnF8c9NvAbnudI6VALHrTsgZWbH7cTQo
9smlIDX2A+4xOAs+YN0q20pimmNl6ukRDxopuPuJXapzQQsPtwhIY2pBwvS8ngcu
hSvgQ11gIip0mIDLDG0AP2nAfx4Uz+AHzjKT1wpDDEj2tIrgPzFPI0/7i2Utw2i9
pGUR23VheHxNG+e2JE6X3EBpDdtWQCRBol1DPoiwJajG0N1Cltfuzz3imzlfEwjP
++dwQV0Xa4m8UOED7kszOpgb51rlkeJRNRizrsoowQKBgQDTftdg9eEg70QUL5Iw
G4fv9ZVmFI4pT2zDExrTwQ27Of7OGwbu/Aaf2EhIFLFJPgonbUa5OEVufbJKacxx
pNiWUrjLPmqbBZie9sqTyoErqc2y/0x3uwBC614aNZz+EkMcXGoLlulqUSUw5jKf
5a71jJjsGWu5C5BPYnVzAExxuQKBgQDG1VTnfj0k9X3HzCNm502V+bxCzG4PmhcE
J6UgiKJ4peCbnsi9hLtWl1Dh1RHSVUOpUgmLO0spYo/+Khv4ONpnML7TsLqKQpT8
iarUt0J7EZ5vZqFCNBLz4wZBgBAgNal7L6cug0ITOfeB+XmD+EDcHHPaRBLdlhXf
SN1yE3BX4wKBgC+EG9eI5l+D4gO2/F0aklvzDPG2RIo7cfAR5sEUaoVZ7klYASLI
NKTM7tBi9cHC0n0xK+aJIfBFBT16r5gItTBwvVvMVh8mDrgIMlMp+ANbTv+cJA3y
UYi3YJj62p6qc7F3gcvAyAg+2uA1l8Ic1EYOpHzG6VDVrEJpmIGR25rhAoGBAMRz
ox/WKrOJmmz91Tym7JFx3gBh25yusm74fL5YQa7StckMaWpW6oHzn4aB7snSVLfG
xoc6XljVeU+2a0wlYCT0lJaz1pskje+2VYM2Tgkqr0+CJ3Ix4Uf21weAcG5ilsGP
o67hITe93j4dL2KktfDEa/MLr1ggIhwq8iDz89vhAoGAWVvSPY9EMF5mqiqFRWaM
W/kQUgAe6PrMWLrx+DMLypUm1PGfDfrBsUzHhiVsZ/TU4kj3Nhra5XKEJHloHvXF
RN/zxBGe4TBpR+b0VwmPl3ZhiQWcXSEH/a04vZ1DhDPlQVpCL8DAqrvd3EhI4qiF
BZYBXKXOaPSgiKplGn4EcUY=
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDCjCCAfKgAwIBAgIUThulUij009/GPlfgYBnctoWGoHowDQYJKoZIhvcNAQEL
BQAwEjEQMA4GA1UEAwwHZ2xwaW9jczAeFw0yMjExMDUxNjI5MjhaFw0zMjExMDIx
NjI5MjhaMBIxEDAOBgNVBAMMB2dscGlvY3MwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCkRFlDEEPOuORlondgr/Aq5jVR3Y+G/FM6IAnTE5rUHCEmLtsT
KHIkhwUnAad9m8r0NL5S5y17bCXY2H6TDttP5mOZWD5kNI7a8xDoh1bi0OFOBusB
XYlpCENzhVVZS+PmRYKmuF1SoRyUeBR9Xt7LI6LIVGkNc3d3XniOkuH9jfbFZNpj
KS7lsALzNxxU34sjo/+GbCCnCsIYsk9pVxh76e5RnVvnnNuKXK+kwKus/JrIigyt
DoTbuP8i5LJdTH9e2xQFfwG8fpc7g/NxFuEH7V0/gpWqFblwtvmyR/ALaidDFxK+
/f0ZU+BpdqU2lYushhN/u35Q8QjNYVe6XrYLAgMBAAGjWDBWMAkGA1UdEwQCMAAw
SQYDVR0RBEIwQIIHZ2xwaW9jc4YXaHR0cDovL2dscGkuc2l0a2EubG9jYWyGFmh0
dHA6Ly9vY3Muc2l0a2EubG9jYWyHBKwUAB4wDQYJKoZIhvcNAQELBQADggEBAEjN
mFJiNjAF+ZwKAAAGi54KVrfp7zYuIkW0njai9BPrbbIgr7M2+Z5KBfSURXBYthKI
bl51kRoSxix1oKsjpOfislETQT2G00YS5eCAqFbCnRFzcQLU6hNAfvLzwdd+lUSq
Jvm7YnViJzl0qC0NXxLdV/THNlTr8SdXeamiIauL1X9q+0lErxAlUaiGyCmfPXvm
oIACJu2+/1M7BUil0ptk1mBoPut/h6gOUf2/FdtctBhBzFKtvIJCBQexzEcfd85h
D6jj91trghqEfANnBRDGVH/+NEsnmRwkWw89s3JxcuIXOcx5XKtdzT85Do1tuRrl
PUHqndIhtjdAi9Rk5MY=
-----END CERTIFICATE-----
```

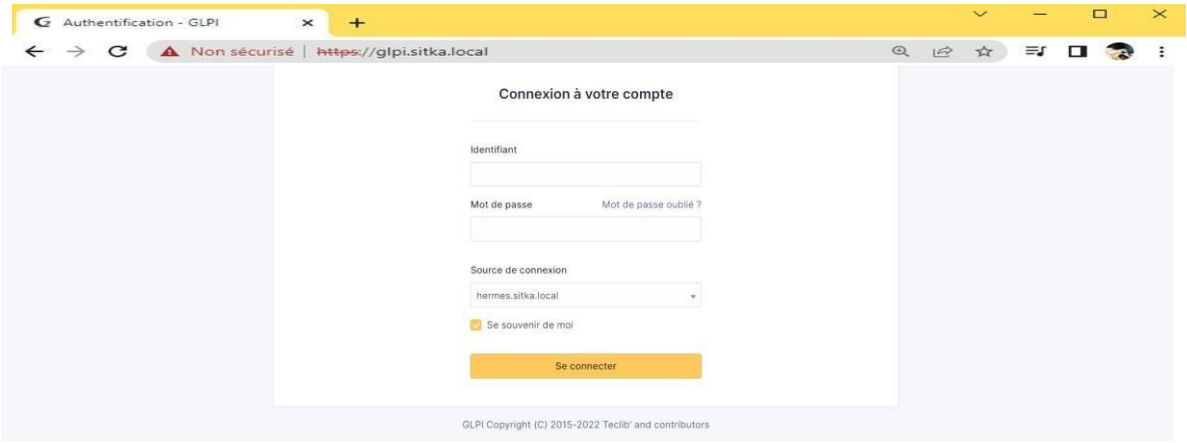
j- Activation du mode ssl et du site glpi.conf

```
root@glpi:/etc/ssl/private# 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:
Module socache_shmcb already enabled
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:/etc/ssl/private# systemctl restart apache2
```

On active la conf glpi.conf

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

root@glpi:~# systemctl reload apache2.
```

On test notre accès sécurisé à glpi



k- Sécuri

sation de glpi en masquant sa version et l'os utilisé.

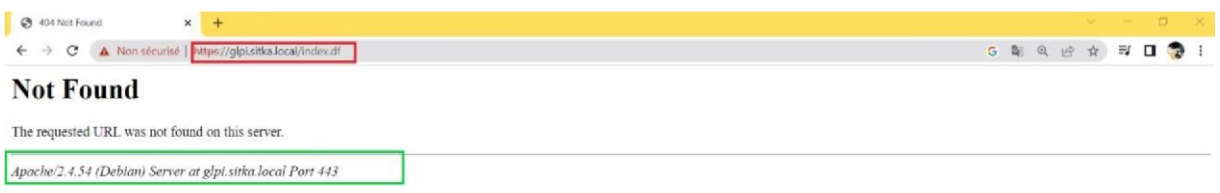
Apache envoie par défaut des entêtes HTTP contenant le nom et la version du serveur web ainsi que le système d'exploitation qui héberge apache, ceci peut être problématique car on peut faciliter l'attaque de notre serveur en divulguant ces informations.

En local on peut afficher ces informations avec la commande apt policy apache2

```
root@glpi:~# apt-cache policy apache2
apache2:
  Installé : 2:4.54-1~deb11u1
  Candidat : 2.4.54-1~deb11u1
 Table de version :
 *** 2.4.54-1~deb11u1 500
        500 http://deb.debian.org/debian bullseye/main amd64 Packages
        100 /var/lib/dpkg/status
     2.4.52-1~deb11u2 500
        500 http://security.debian.org/debian-security bullseye-security/main amd64 Packages
```

A distance sur une machine linux on peut afficher ces informations avec la commande curl en me connectant de n'importe machine

```
┌──(user@etanium)-[~]
└─$ curl -I 172.20.0.30
HTTP/1.1 200 OK
Date: Sat, 05 Nov 2022 18:29:53 GMT
Server: Apache/2.4.54 (Debian)
Last-Modified: Mon, 10 Oct 2022 20:34:27 GMT
ETag: "29cd-5eab415f9ce37"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Content-Type: text/html
```



Pour cacher la version d'Apache, il faut changer des paramètres dans le fichier */etc/apache2/conf-*

*enabled/**security.conf***. **Les paramètres à modifier sont ServerTokens et ServerSignature**, on peut atteindre le même but en rajoutant ces paramètres directement dans le fichier *apache2.conf* à la fin du fichier.

```
root@glpi:~# cd /etc/apache2/conf-enabled/

root@glpi:/etc/apache2/conf-enabled# vim security.conf
```

On désactive la ligne **ServerToken OS** en rajoutant au début de la ligne un #

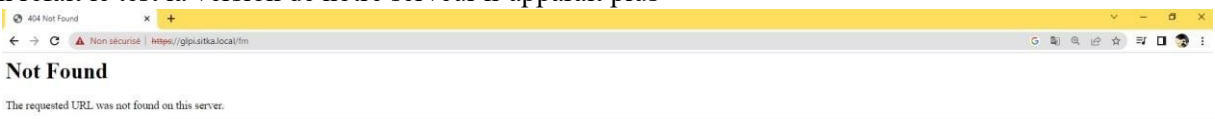
```
ServerTokens OS
```

On désactive la ligne **Server Signature On** en rajoutant au début de la ligne un #

```
ServerSignature On
```

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

On refait le test la version de notre serveur n'apparait plus



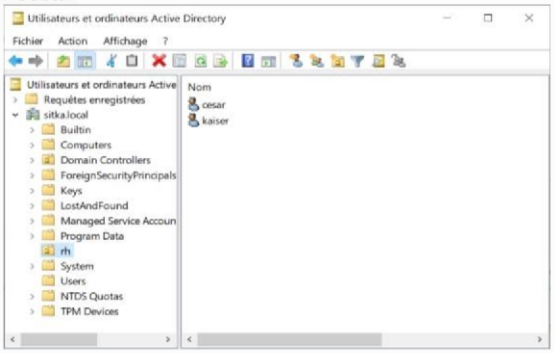
l

- **Liaison de Glpi avec Active directory**

a-

Création de l'UO et des utilisateurs sur le contrôleur de domaine

Sur mon contrôleur de domaine je crée une unité d'organisation **rh** dans laquelle je crée deux utilisateur **kaiser** et **cesar**



b- Création de la liaison avec l'annuaire ldap

Sur GLPI :

- Configuration
- Authentification
- Annuaire LDAP
- Je clique sur le signe + pour rajouter un **annuaire ldap**

Je clique sur le signe + pour rajouter un **annuaire ldap**

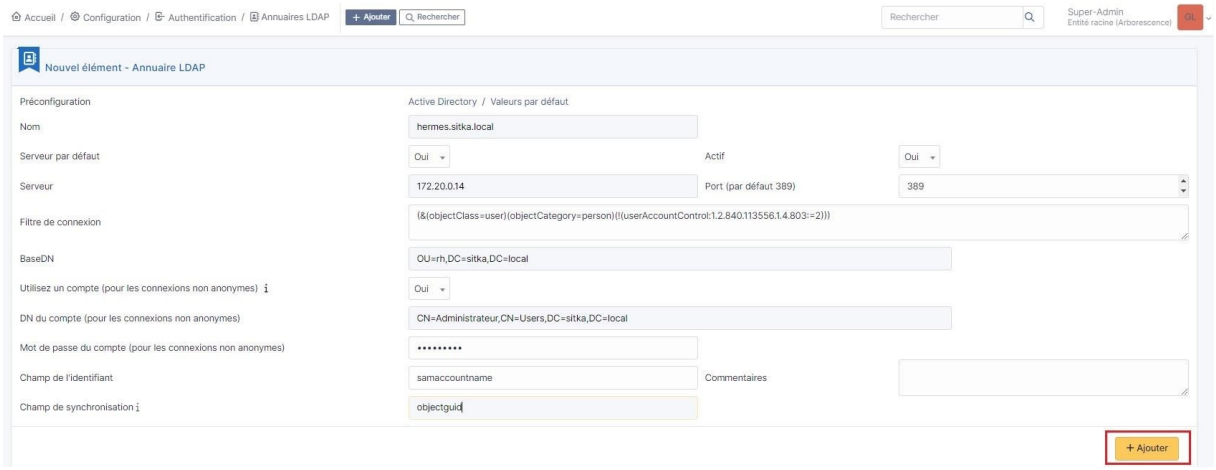
On remplie notre formulaire avec les informations ci-dessous :

Dans filtre de connexion on applique le filtre suivant :

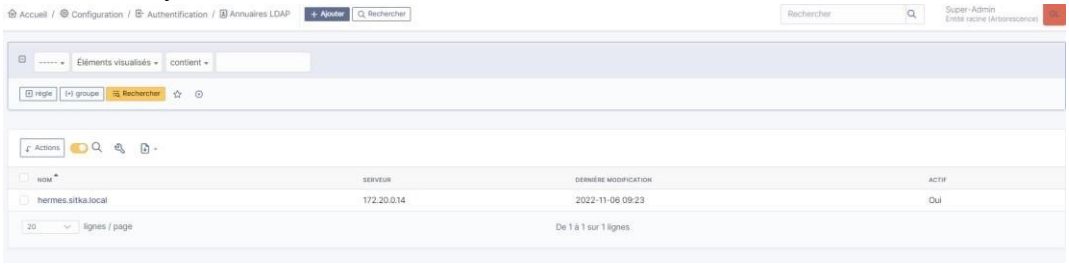
(&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

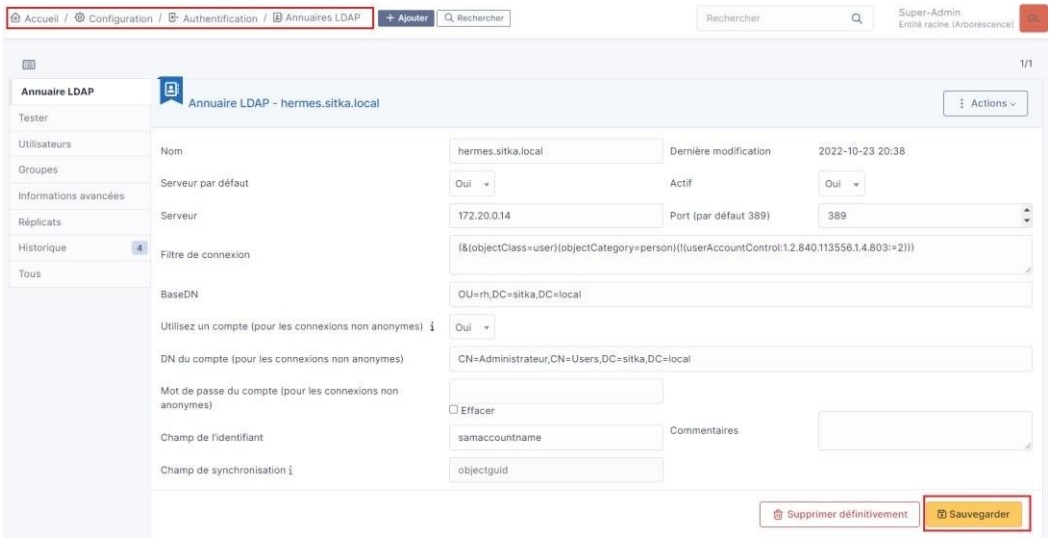
Dans Mot de passe du compte : Il faut mettre le mot de passe de l'administrateur de notre controleur de domaine

On clique sur ajouter aprés avoir remplie le formulaire



On tombe apés sur cette page on clique sur le lien hermes.sitka.local pour tester la liaison avec active directory





On fait le test de connexion avec active directory

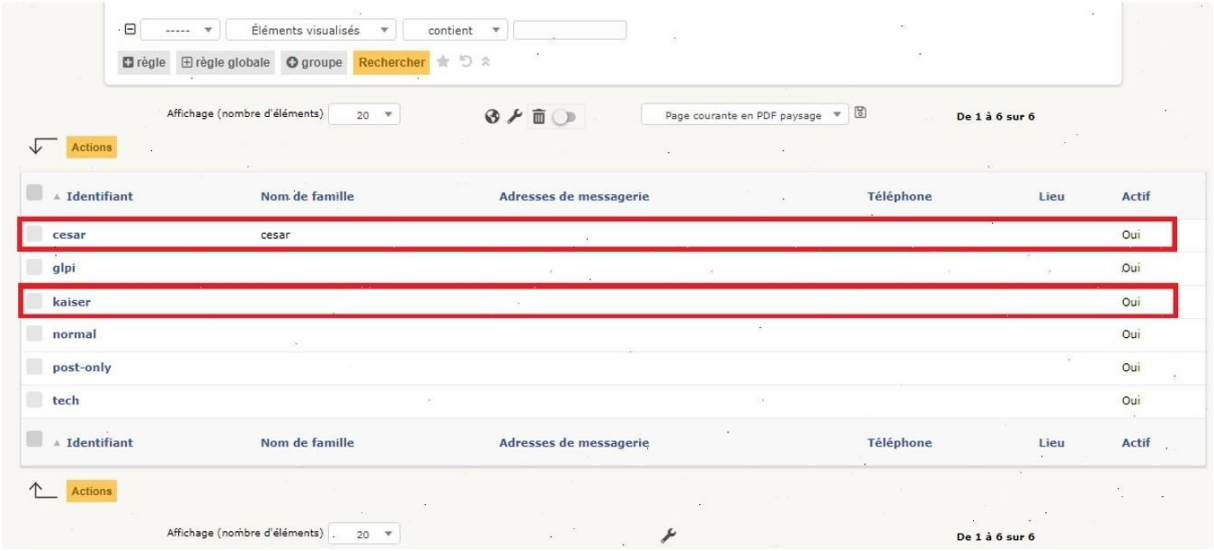
c- Importation des utilisateurs à partir de notre base d'annuaire ldap Sur GLPI :

- Administration
- Utilisateur
- Liaison annuaire LDAP
- Importation de nouveaux utilisateurs
- Rechercher
- Cocher la ou les cases des utilisateurs à importer
- Action
- Importer • Envoyer.

On coche les utilisateur qu'on veut telecharger pius on clique sur action et on selectionne importer

Vérifier la présence des utilisateurs importés dans le menu :

- Administration
- Utilisateur.



On test une connexion ldap avec glpi

1- Création de tickets

a- Configuration de la notification par mail

Maintenant sur glpi on va activer une fonctionnalité d'alerte en configurant les notifications sur notre serveur glpi.

Dès qu'il y'a création d'un ticket, l'administrateur sera informé par mail de la création de ce ticket et ainsi il pourra le traiter.

Tout d'abord on va tester l'envoi de mail par **telnet** de notre serveur glpi vers la messagerie Zimbra

└─# **telnet xmail.sitka.local 25** Trying 172.20.1.70...

Connected to xmail.sitka.local.s

Escape character is '^]'.

220 xmail.sitka.local ESMTP Postfix

helo xmail.sitka.local

250 xmail.sitka.local

mail from:<support@xmail.sitka.local>

250 2.1.0 Ok

rcpt to:<admin@xmail.sitka.local>

250 2.1.5 Ok data

354 End data with <CR><LF>.<CR><L

subject:test d'envoie glpi

ceci est un test >

.

0972

250 2.0.0 Ok:

quit queued

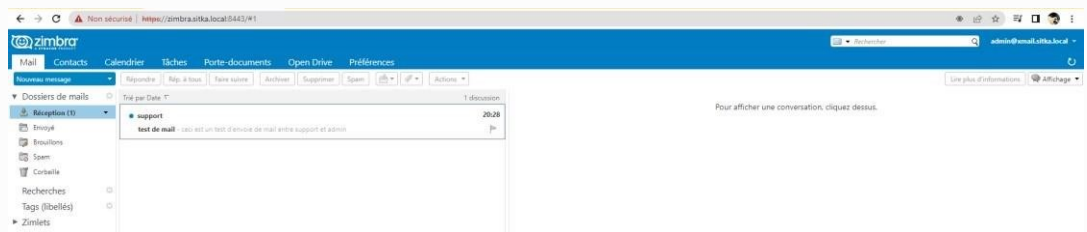
C1FCBE

2.0.0 Bye

closed by

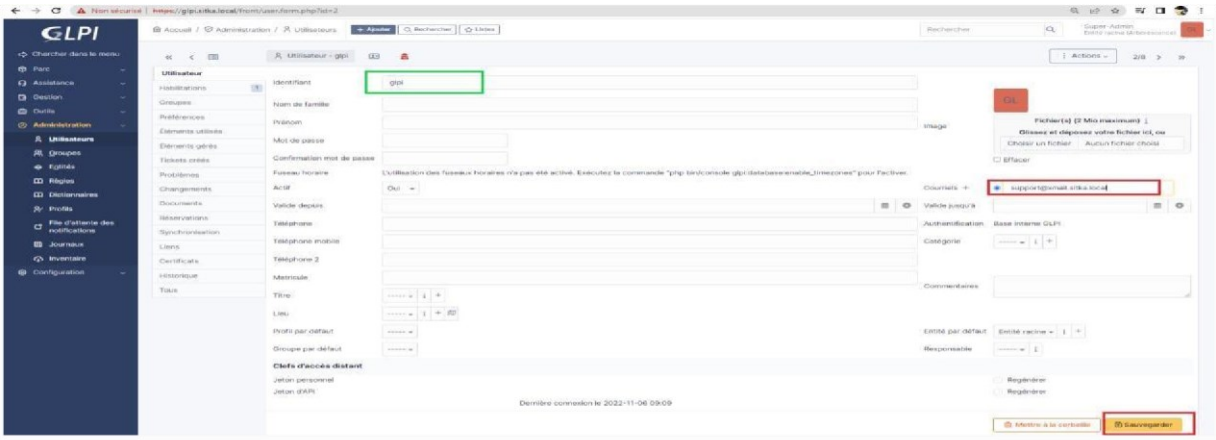
fo host.

On vérifie sur Zimbra la réception du mail de la part de support, pour s'assurer du bon fonctionnement de la notification glpi par mail

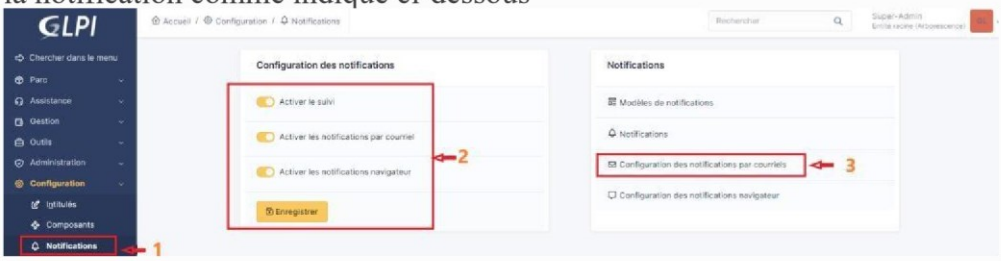


Il faut renseigner le mail du compte glpi donc on va sur

-administration + utilisateurs ; on sélectionne le compte glpi, on peut créer un autre utilisateur et lui affecter le profil admin

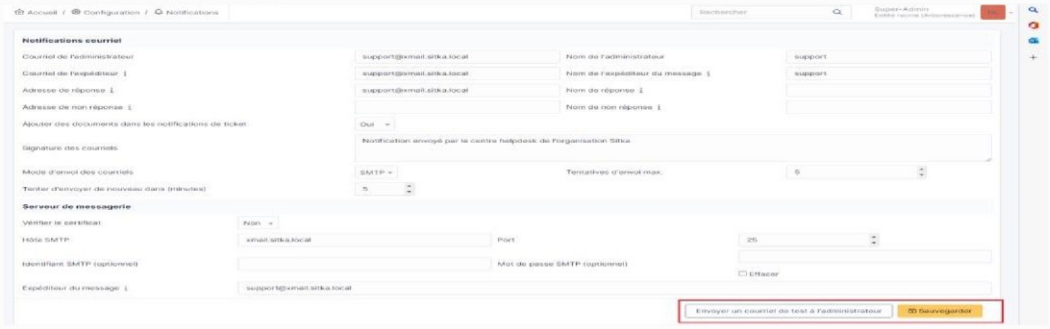


Une fois le test d'envois de mail est fait et que le mail du compte glpi est renseigné on active la notification comme indiqué ci-dessous



On configure la notification par mail en remplissant le formulaire comme indiqué ci-dessous

Le courriel de l'administrateur donc le compte glpi est support@xmail.sitka.local on sauvegarde en suite notre formulaire

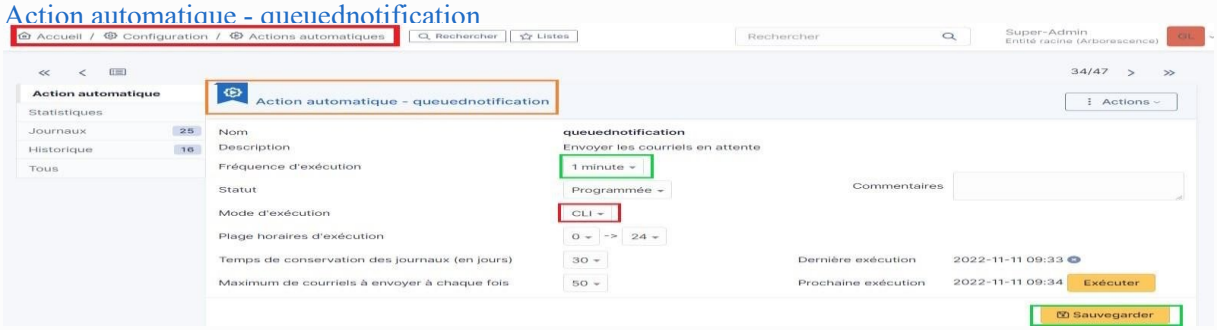


On fait un test d'envoi de notification au compte support

Et on vérifie que le mail du test est bien arrivé dans la boite mail du compte support

Attention il faut vérifier la fréquence d'envoi d'alerte dans le menu ;

Action automatique - queuednotification



On se rend sur cette page du site officiel en cliquant le bouton documentation pour déterminer la procédure à suivre selon le système d'exploitation utilisé

https://documentation.fusioninventory.org/FusionInventory_for_GLPI/cron/

On ouvre le fichier de configuration de cron avec la commande ci-dessous on nous demande de choisir l'éditeur pour ouvrir cron

1

A la fin du fichier on rajoute la ligne encadrée ci-dessous

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

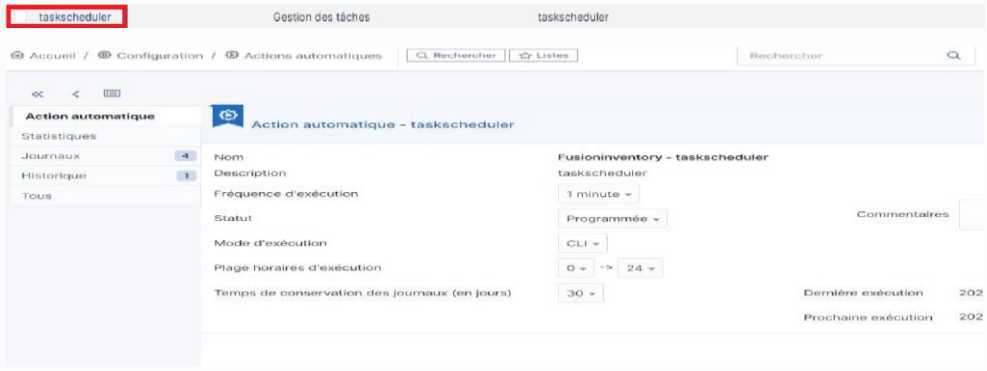
```
# m h .dom mon dow   command
* * * * * cd /var/www/glpi/front/ && /usr/bin/php cron.php &>/dev/null
```

Enfin en redémarre le service cron

```
estart
```

Dernière étape on va dans **configuration Actions automatique** on vérifie la configuration puis on clique

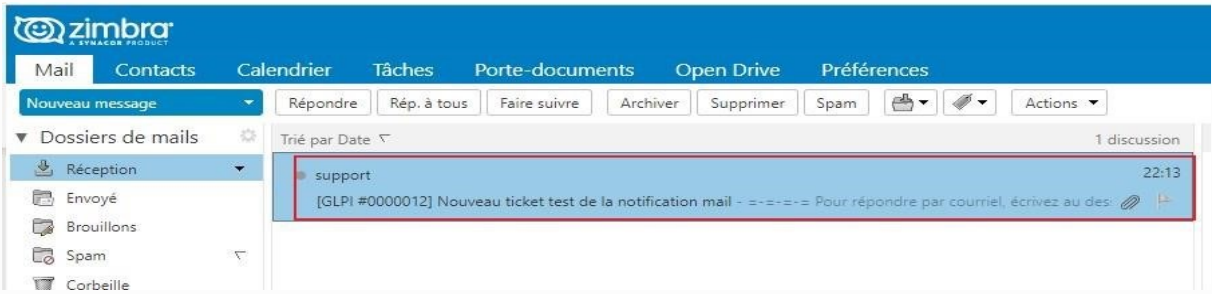
sur exécuter pour activer cron de glpi le gestionnaire des taches de cron



Maintenant on va vérifier le fonctionnement de l'alerte configurée en se connectant avec un utilisateur et en créant un ticket ; le compte glpi devrait être

Alerter de la création du ticket à travers la réception d'un mail dans sa boite mail support. Donc dans un premier temps on va créer un ticket avec le compte kaiser

On vérifie ensuite la réception du mail de l'alerte dans la boite mail support

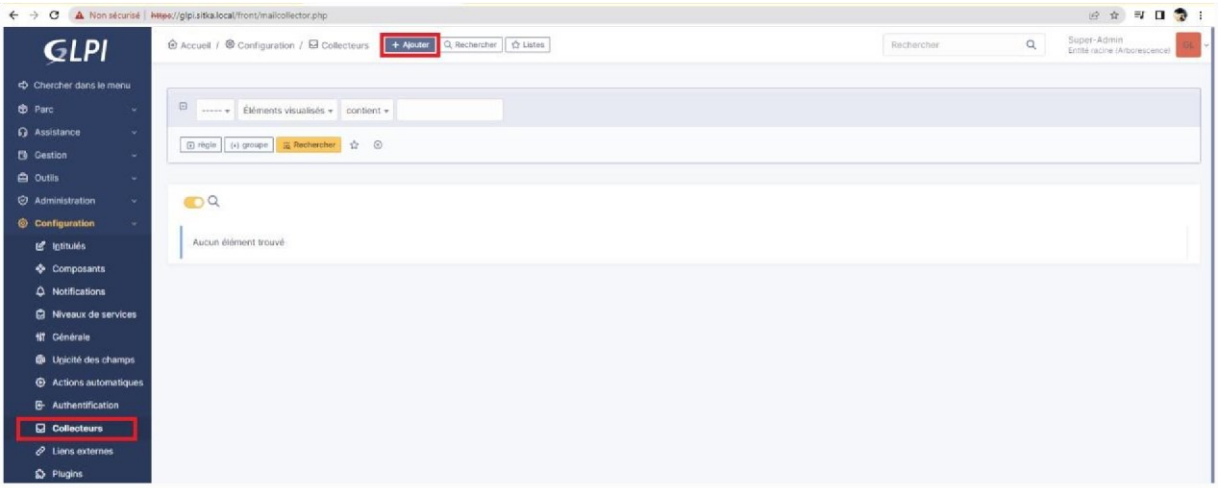


b- Notification par collecteurs

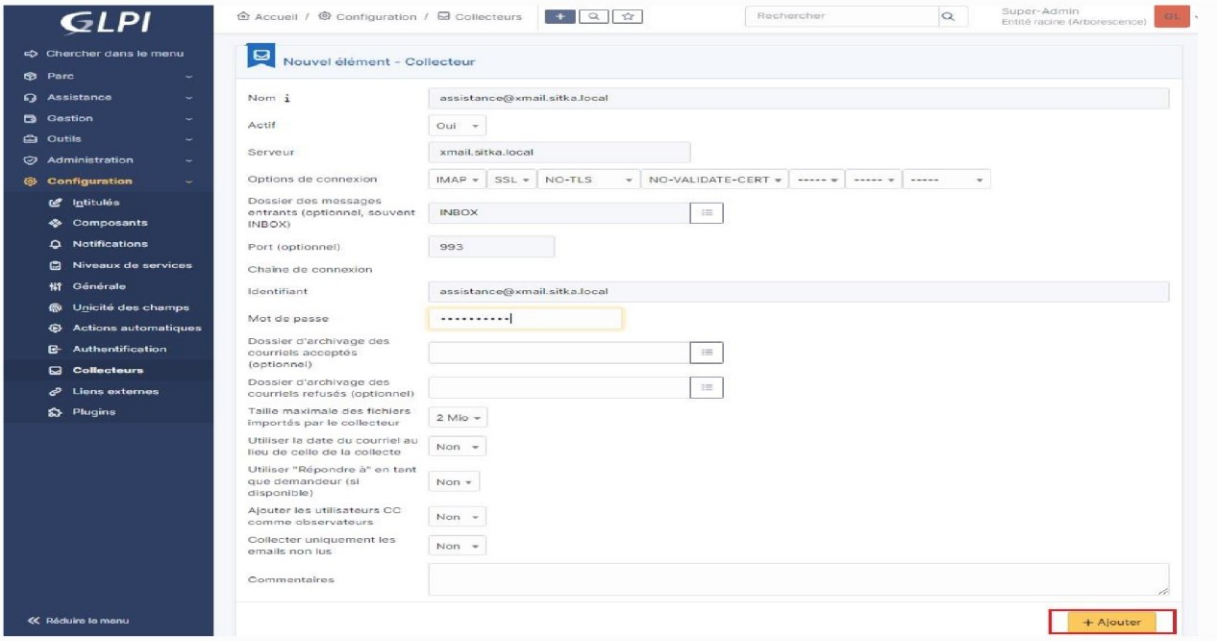
Les collecteurs nous permettent la création des tickets automatiquement par envois de mail
Glpi grâce aux taches automatiques va récupérer le mail puis va créer un ticket
Attention pour cette procédure fonctionne il faut que l'utilisateur ainsi que son mail existe dans la base glpi si non il y'aura un refus de glpi

Pour notre procédure on va utiliser le comptes assistance avec son courriel
Assistance@xmail.sitka.local

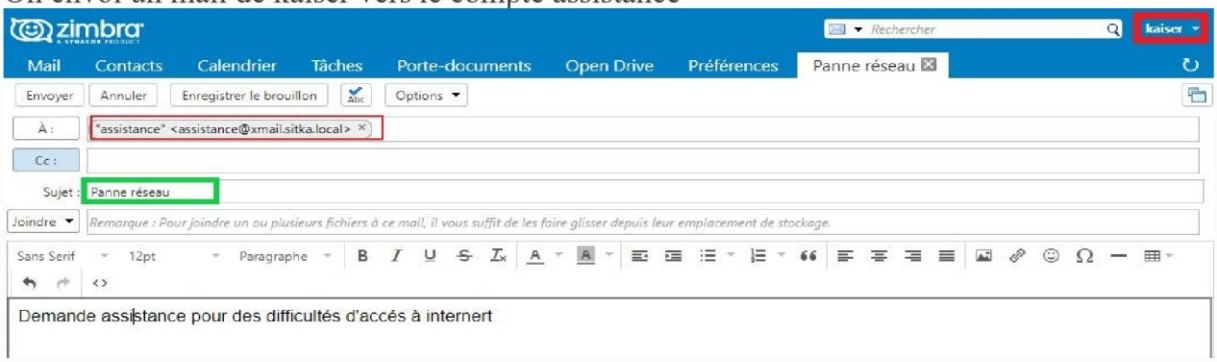
On va dans **Configuration + Collecteurs+ Ajouter** Pour
créer un CollecteurCréation d'un collecteur



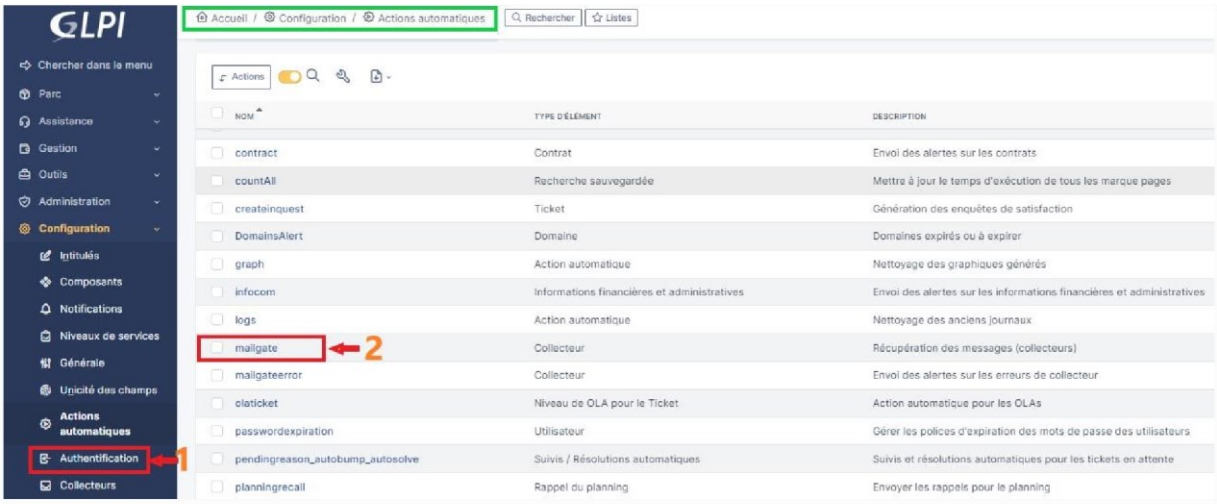
Après on remplit le formulaire comme indiqué ci-dessous : si on choisit pop au lieu d'IMAP il faut mettre le port **993** une fois le formulaire remplie on clique sur **ajouter**



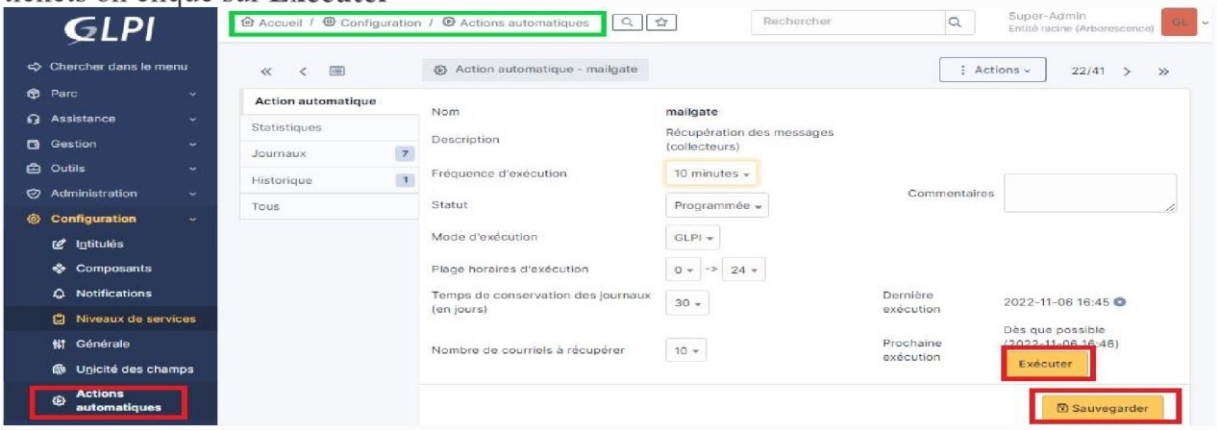
On envoi un mail de kaiser vers le compte assistance



Pour collecter le mail on va sur Configuration + Actions automatiques +mailgate

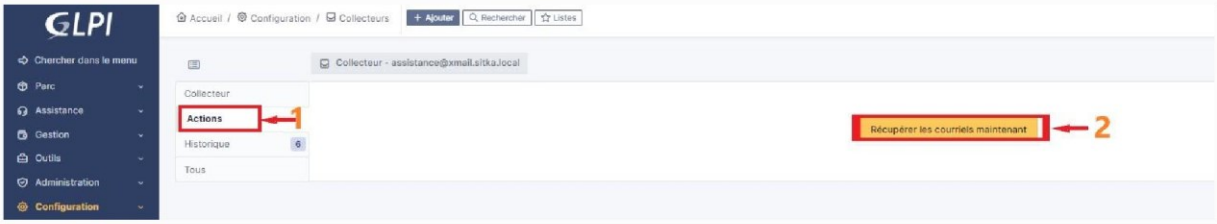


On peut changer les paramètres après on sauvegarde pour collecter les mails pour générer les tickets on clique sur **Exécuter**



Une autre méthode pour collecter les mails pour générer les tickets on va sur **Configuration** + **Collecteurs puis** on sélectionne l'onglet Actions et en fin on clique sur **Récupérer les courriels maintenant** comme indiqué ci-dessous.

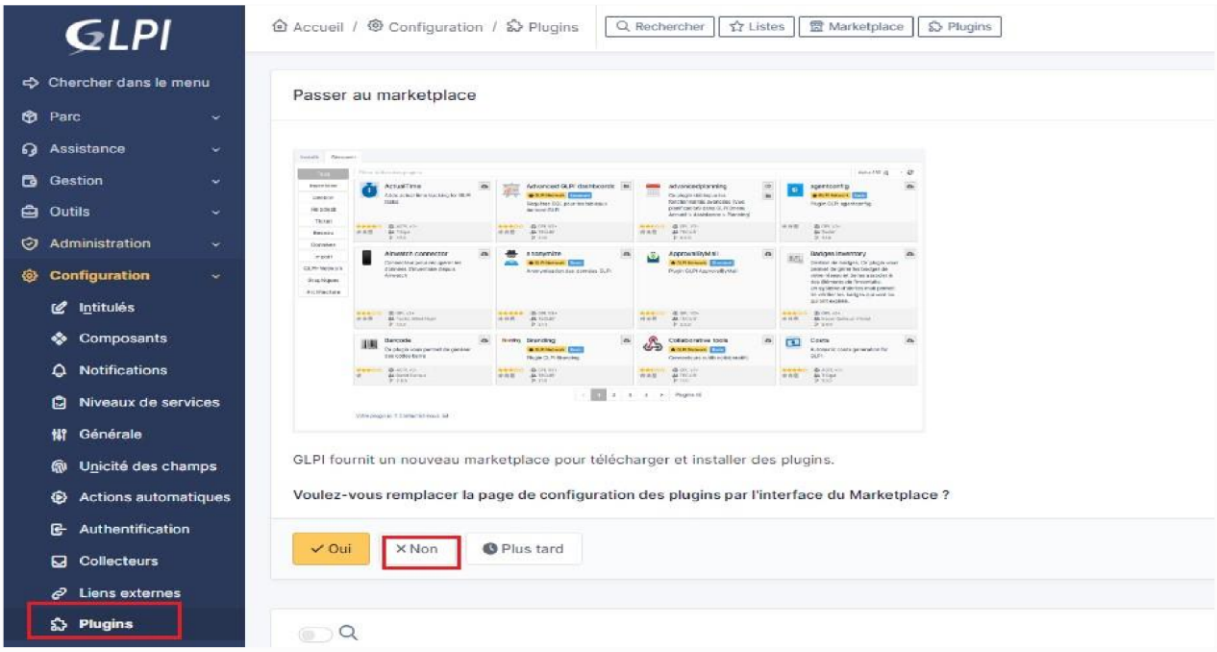
Après il faut vérifier si le ticket a été générer.



c- Gestion des tickets

2- Fusion-inventory

a- Installation du plugin fusion-inventory



Tout d'abord il faut se rendre au site suivant pour télécharger la version adéquate de fusion inventory

https://github.com/fusioninventory/fusioninventory-for-glpi/releases/tag/glpi10.0.3%2B1.0

On copie le lien de la version fusion inventory pour linux puis on télécharge le plugin

```
root@glpi:~# wget https://github.com/fusioninventory/fusioninventory-for-glpi/releases/download/glpi10.0.3%2B1.0/fusioninventory-10.0.3+1.0.tar.bz2
```

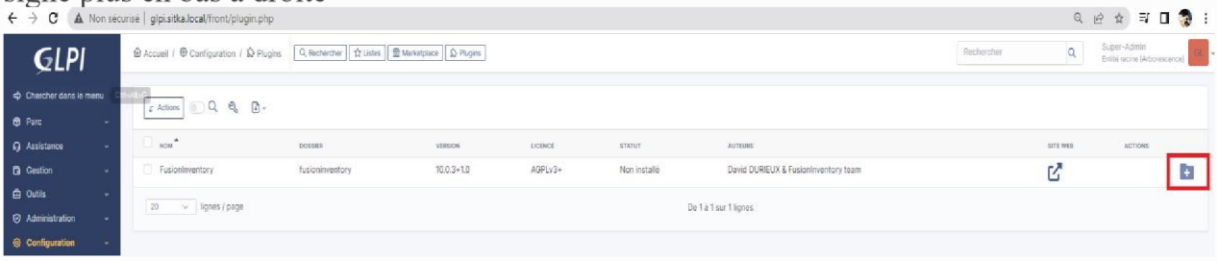
On décompresse le plugin téléchargé

```
root@glpi:~# tar xfv fusioninventory-10.0.3+1.0.tar.bz2
```

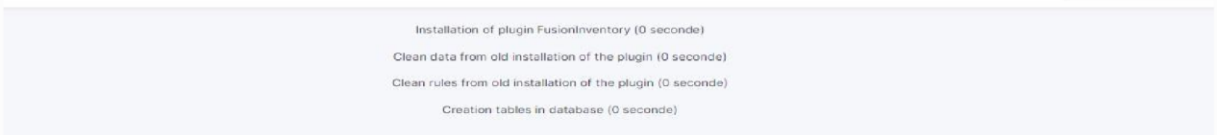
On déplace le plugin vers /var/www/glpi/plugins

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

On revient vers l'interface glpi en allant dans **Configuration + Plugins** on remarque l'apparition de fusion inventory : pour finaliser l'installation on clique sur l'icone avec le signe plus en bas à droite



L'installation démarre



On va sur la page GitHub pour télécharger l'agent fusion inventory

Maintenant il faut activer le plugin en cliquant sur l'icône en bas à droite

Une fois activé l'icône devient verte

Dernier problème à régler on va configurer et activer cron le planificateur de tache de linux

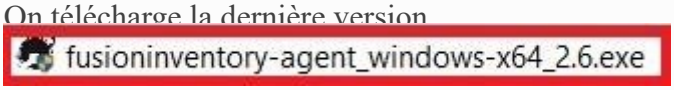
b- Installation des agents fusion-inventory

GitHub - fusioninventory/fusioninventory-agent: FusionInventory Agent

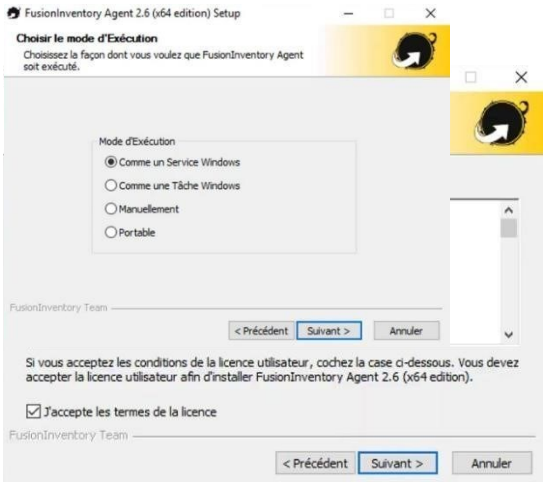
On clique à droite de la page pour afficher les dernières versions de l'agent fusioninventory

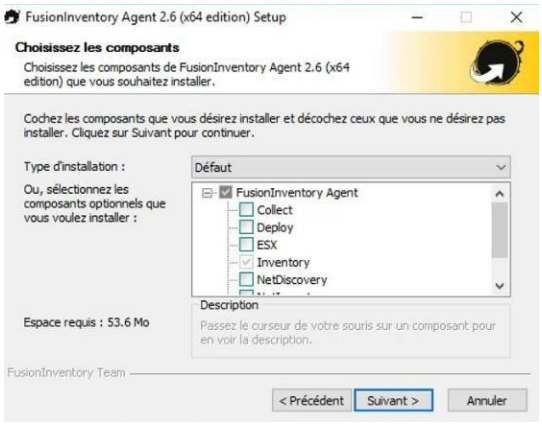
i- Agent fusion inventory pour Windows

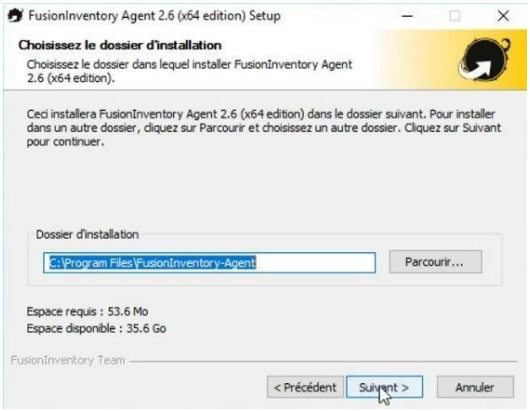
On télécharge la dernière version

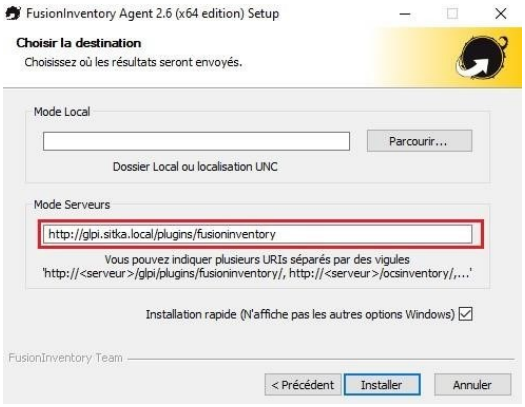


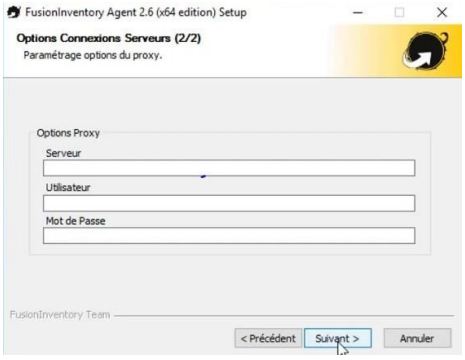
Une fois téléchargé en lance l'installation

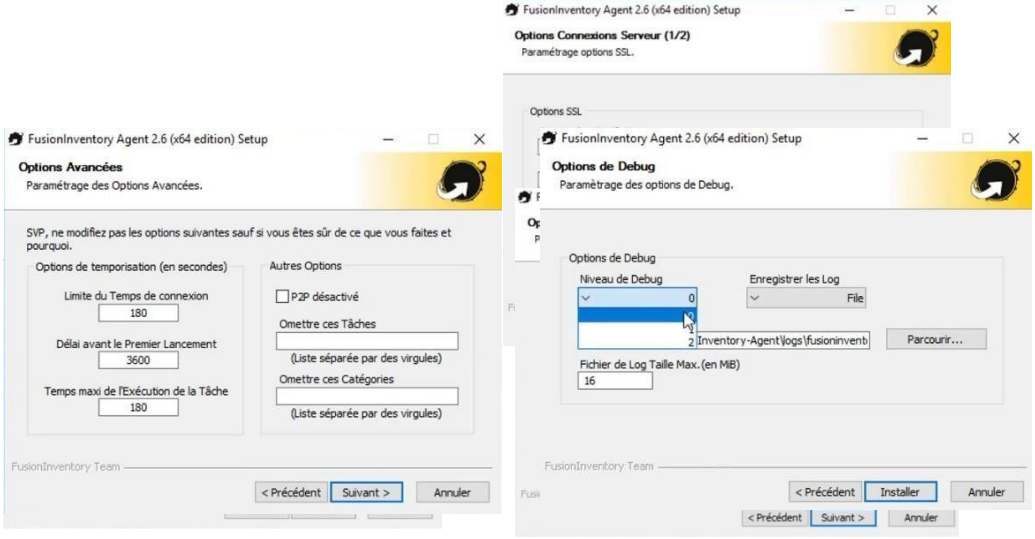

FusionInventory Agent 2.6 (x64 edition) Setup
Choisir le mode d'Exécution
Choisissez la façon dont vous voulez que FusionInventory Agent soit exécuté.
Mode d'Exécution
Comme un Service Windows
Comme une Tâche Windows
Manuellement
Portable
FusionInventory Team
< Précédent
Suivant >
Annuler
Si vous acceptez les conditions de la licence utilisateur, cochez la case ci-dessous. Vous devez accepter la licence utilisateur afin d'installer FusionInventory Agent 2.6 (x64 edition).
J'accepte les termes de la licence
FusionInventory Team
< Précédent
Suivant >
Annuler

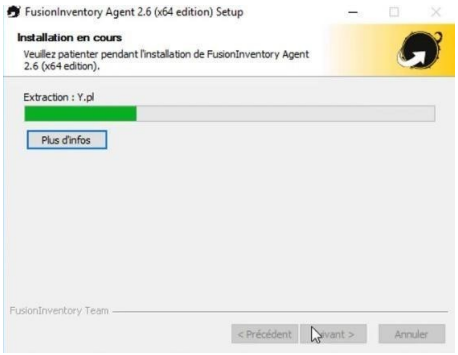

FusionInventory Agent 2.6 (x64 edition) Setup
Choisissez les composants
Choisissez les composants de FusionInventory Agent 2.6 (x64 edition) que vous souhaitez installer.
Cochez les composants que vous désirez installer et décochez ceux que vous ne désirez pas installer. Cliquez sur Suivant pour continuer.
Type d'installation :
Défaut
Ou, sélectionnez les composants optionnels que vous voulez installer :
FusionInventory Agent
Collect
Deploy
ESX
Inventory
NetDiscovery
Description
Espace requis : 53.6 Mo
Passez le curseur de votre souris sur un composant pour en voir la description.
FusionInventory Team
< Précédent
Suivant >
Annuler


FusionInventory Agent 2.6 (x64 edition) Setup
Choisissez le dossier d'installation
Choisissez le dossier dans lequel installer FusionInventory Agent 2.6 (x64 edition).
Ceci installera FusionInventory Agent 2.6 (x64 edition) dans le dossier suivant. Pour installer dans un autre dossier, cliquez sur Parcourir et choisissez un autre dossier. Cliquez sur Suivant pour continuer.
Dossier d'installation
C:\Program Files\FusionInventory-Agent
Parcourir...
Espace requis : 53.6 Mo
Espace disponible : 35.6 Go
FusionInventory Team
< Précédent
Suivant >
Annuler


FusionInventory Agent 2.6 (x64 edition) Setup
Choisir la destination
Choisissez où les résultats seront envoyés.
Mode Local
Parcourir...
Dossier Local ou localisation UNC
Mode Serveurs
http://glpi.sitka.local/plugins/fusioninventory
Vous pouvez indiquer plusieurs URIs séparés par des virgules
'http://<serveur>/glpi/plugins/fusioninventory/, http://<serveur>/ocsinventory/,...'
Installation rapide (N'affiche pas les autres options Windows)
FusionInventory Team
< Précédent
Installer
Annuler


FusionInventory Agent 2.6 (x64 edition) Setup
Options Connexions Serveurs (2/2)
Paramétrage options du proxy.
Options Proxy
Serveur
Utilisateur
Mot de Passe
FusionInventory Team
< Précédent
Suivant >
Annuler





d- Installation de l'agent fusion inventory pour linux

On installe le paquet fusioninventory-agent

```
root@glpi-ocs:~# apt install fusioninventory-agent -y
```

On verifie l'installation ainsi que la version

```
root@glpi-ocs:~# dpkg -l fusioninventory-agent
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  fusioninventory-agent 1:2.6-2      all          hardware and software inventory tool (client)
```

```
root@glpi-ocs:~# vim /etc/fusioninventory/agent.cfg
```

```
# send tasks results to an OCS server
#server = http://server.domain.com/ocsinventory
# send tasks results to a FusionInventory for GLPI server
server = https//glpi.sitka.local/plugins/fusioninventory/
# write tasks results in a directory
#local = /tmp
```