



2024 - 2026

BTS Services Informatique aux Organisations



BENNACEUR Rayan

Introduction

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 Mariadb
- 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- Importation des utilisateurs à partir de notre base d'annuaire ldap

5- Liaison de glpi avec ocs-inventory

6- Crédit 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

Introduction

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 aisément 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:~# 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: ens3: <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 ens3
            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

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
```

Il ne faut pas oublier d'activer la carte rajoutée

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

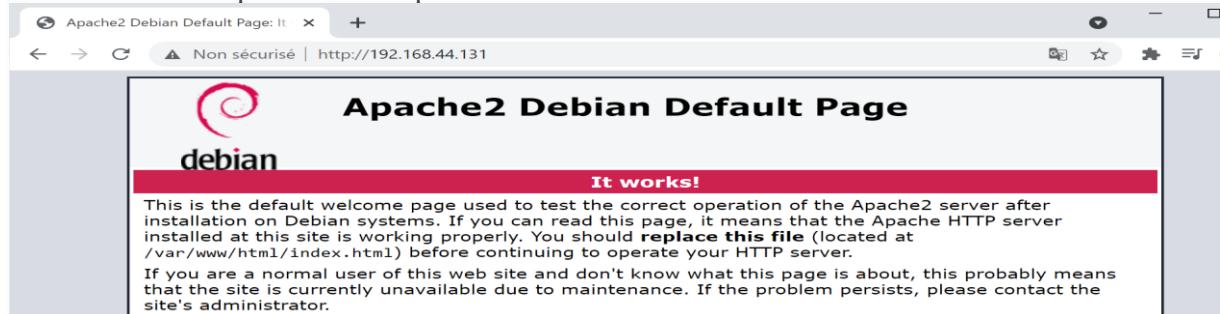
d- Installation d'apache2 PHP et Mariadb

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

On vérifie le bon fonctionnement d'apache

```
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



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

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

System	Linux glpi 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64
Build Date	Oct 23 2021 21:53:50
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d

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 ;
- `ldap` : utiliser l'annuaire LDAP pour l'authentification ;
- `openssl` : communications sécurisées ;
- `xmlrpc` : utilisé pour l'API XMLRPC.
- `APCu` : peut être utilisé pour le cache.

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 **dbgipi**

```
MariaDB [(none)]> create database dbgipi;
```

Query OK, 1 row affected (0.001 sec)

Je crée un utilisateur **userglpi** et je lui donne tous les priviléges sur la bases **dbgipi**

```
MariaDB [(none)]> grant all privileges on dbgipi.* 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
dbgipi
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 `dbgipi`.* 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 : <https://glpi-project.org/downloads> on copie le lien

LA DERNIÈRE VERSION STABLE DE GLPI

GLPI VERSION 10.0.3

13/09/2022 – Archive TGZ – 33.4Mo

[Télécharger >](#)

LA DERNIÈRE DOCUMENTATION GLPI

DOC VERSION 10.0

Administrateurs / Utilisateurs / Développeurs / Agent GLPI

[Obtenir de la documentation >](#)

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

```
#wget https://github.com/glpi-project/glpi/releases/download/10.0.3/glpi-10.0.3.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   0s
2022-10-10 23:01:54 (1,93 MB/s) - « glpi-10.0.3.tgz » sauvegardé [59087826/59087828]
```

On décomprime notre fichier téléchargé dans /var/www/html.

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

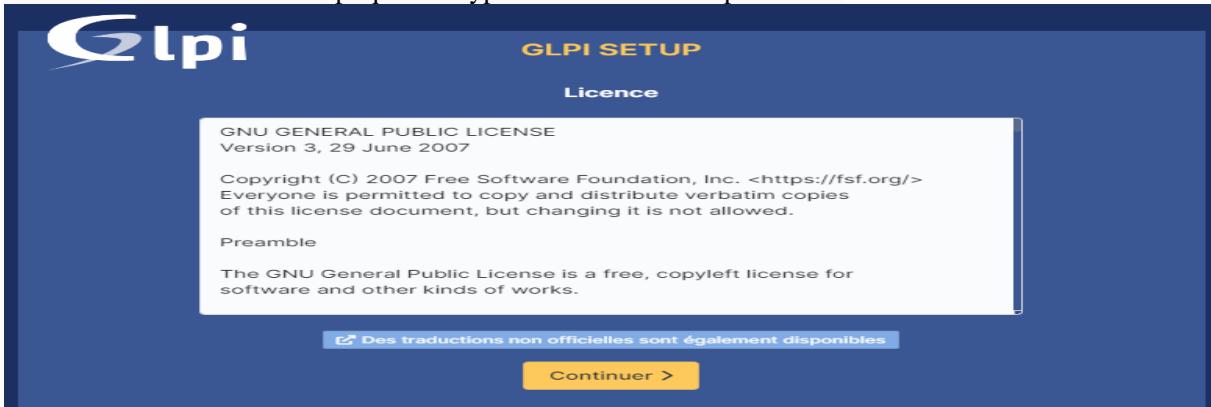
```
; Whether or not to add the httpOnly flag to the cookie, which makes it
; inaccessible to browser scripting languages such as JavaScript.
; http://php.net/session.cookie-httponly
session.cookie_httponly = on
```

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 jour notre GLPI déjà installé



Le programme d'installation vérifie si les prérequis sont réunis 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.	✓
Suggéré ldap extension Active l'utilisation de l'authentification à un serveur LDAP distant.	✓
Suggéré openssl extension Active l'envoi de courriel en utilisant SSL/TLS.	✓
Suggéré zip extension Active l'installation de paquets zip à partir du Marketplace.	✓
Suggéré bz2 extension Active l'installation des paquets bz2 à partir du Marketplace.	✓
Suggéré Zend OPcache extension Améliorer les performances du moteur PHP.	✓
Suggéré Extensions émulées de PHP Améliorer légèrement les performances.	✓
Suggéré Permissions pour le répertoire du marketplace Active l'installation des plugins à partir du Marketplace.	✓

Voulez-vous continuer ?

Continuer >

Réessayer C

On se connecte sur la base de donné MariaDB

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

-Utilisateur SQL : **userglpi**

-Mot de passe SQL : **userglpi**



GLPI SETUP
Étape 1
Configuration de la connexion à la base de données

Serveur SQL (MariaDB ou MySQL)
localhost

Utilisateur SQL
userglpi

Mot de passe SQL
.....|

Continuer >

On sélectionne notre base de données créée auparavant



GLPI SETUP
Étape 2
Test de connexion à la base de données

Connexion à la base de données réussie

Veuillez sélectionner une base de données :

Créer une nouvelle base ou utiliser une base existante :

dbgipi

Continuer >



GLPI SETUP
Étape 3
Initialisation de la base de données.

OK - La base a bien été initialisée

Continuer >

Choisissez d'envoyer ou non vos données de statistiques



GLPI SETUP
Étape 4
Récolter des données

Envoyer "statistiques d'usage"
Nous avons besoin de vous pour améliorer GLPI et son écosystème de plugins !

Depuis GLPI 9.2, nous avons introduit une nouvelle fonctionnalité de statistiques appelée "Télématrice", qui envoie anonymement, avec votre permission, des données à notre site de télématrice.
Une fois envoyées, les statistiques d'usage sont agrégées et rendues disponibles à une large audience de développeurs GLPI.

Dites-nous comment vous utilisez GLPI pour que nous améliorons GLPI et ses plugins !
[Voir ce qui sera envoyé...](#)

Référez-vous à GLPI
Par ailleurs, si vous appréciez GLPI et sa communauté, prenez une minute pour référencer votre organisation en remplissant le formulaire suivant Le formulaire d'inscription

Continuer >

Soutenir le projet avec un don



Notre installation a réussi



Il reste plus qu'à vous connecter :

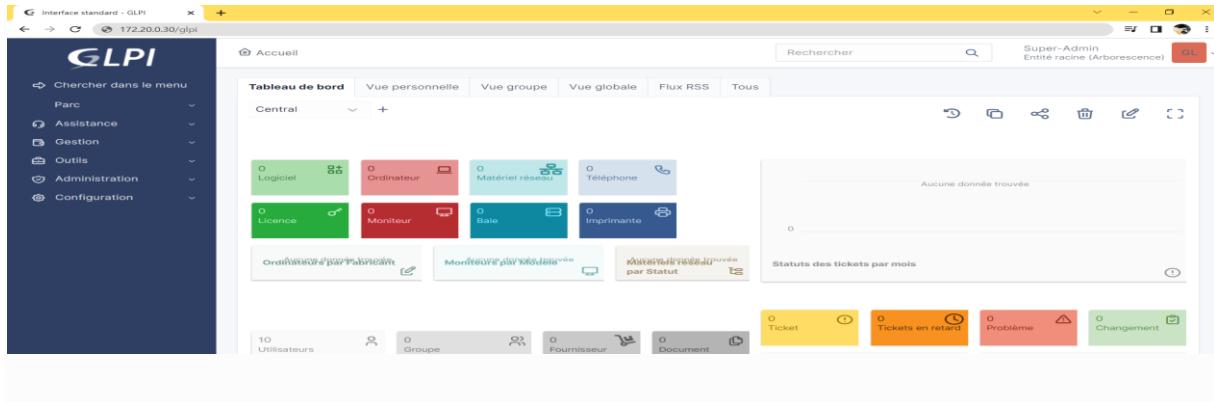
- Identifiant : **glpi**
- Mot de passe : **glpi**

On a deux messages d'erreurs

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

Gestionnaire DNS			
	Nom	Type	Données
DNS	modis	Source de nom (SOA)	[49] hermes.sitka.local., hermes.sitka.local.
HERMES	sites	Source de noms (NS)	hermes.sitka.local.
sitka.local	tcp	Hôte (A)	172.20.0.14 03/11/2022 21:00:00
sites	udp	Hôte (A)	172.20.0.160 03/11/2022 21:00:00
sites	DomainDnsZones	Hôte (A)	172.20.0.30 statique
ForestDnsZones	(identique au dossier parent)	Hôte (A)	172.20.0.30 statique
ForestDnsZones	(identique au dossier parent)	Hôte (A)	172.20.0.31 statique
ForestDnsZones	(identique au dossier parent)	Hôte (A)	172.20.0.70 statique
ForestDnsZones	ACR	Hôte (A)	172.20.0.30 statique
ForestDnsZones	glpi	Hôte (A)	172.20.0.30 statique
hermes	hermes	Hôte (A)	172.20.0.14 statique
hermes	xmail	Hôte (A)	172.20.0.31 statique
hermes	xmail	Hôte (A)	172.20.0.70 statique
hermes	zimbra	Hôte (A)	172.20.0.70 statique

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 _default_:443>

    ServerName glpi.sitka.local
    Serveralias sitka.local *.sitka.local
    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/sitka.pem

</VirtualHost>
</IfModule>
```

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

    ServerName glpi.sitka.local
    Serveralias sitka.local *.sitka.local
    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/sitka.pem

</VirtualHost>
</IfModule>
```

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- Crédration du certificat SSL

On vérifie la présence du paquet ssl-cert

```
root@glpi:~# dpkg -l ssl-cert
Soushant=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+nmul  all  simple debconf wrapper for OpenSSL
```

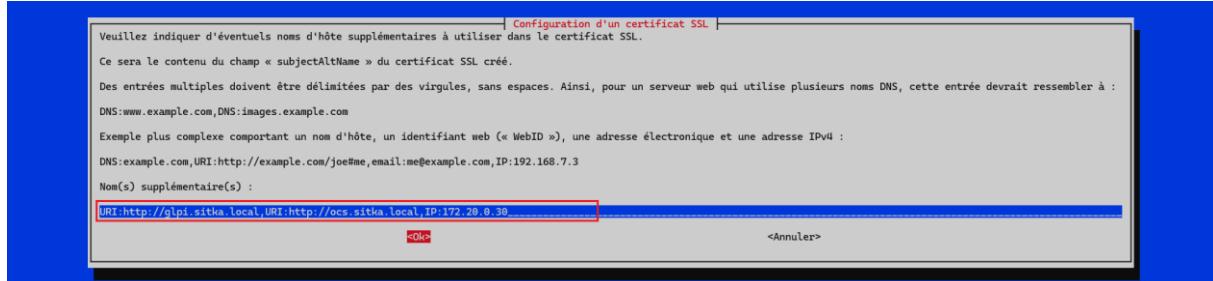
Création d'un fichier pem (Privacy Enhanced Mail (PEM)) contenant un certificat autosigné et une clé privée.

```
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-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwgSjAgEAAoIBAQCKrF1DEEP0uOrL
ondgr/Aq5jVR3Y+G/FM6IAntESrUHCmLstKHikhwlNaAd9m3r0NL5S5y17bCY
2H6TdtPSm0ZWD5kNtA8zDoh1b10FOBu8XYlpCENzVHZs+PmRYkmw15oRyU
eBR9Xc7L16LIVgkNc3d3Xn10kuHjfBZNPjK57lsALzNxu34sjo/+GbCnCs1Y
sk9pxh7ee5rnvnNuKKK+kwKus/JrIigytDoTbuP8i5LJdT9he2xQfwG8fpC7
g/NxFuH7V0/gpwFb1wtvmyR/AlaidDFx+k+/f0ZU+BpdqU2lYushh/u3508QjN
Yve6Xr/yLagMBAAECggEA07uLcuG/0pSIHvNz3aHba3E0GjjoPuI51g/0yg9A
L3XRyUfnxs1lowoC77R5MhLkfFLpBhKGNF8C9NVAbnu16VAlHrTsgZwbH7TQo
9smLI0X2A+4xQAs+YhD0RdxopuPxJaxpQOsPtwhIV2pBvwS8ngu
hSvqQ11gIp0mIDLG0AP2nafx4Uz+AhzjKT1wpDDEj2tIrgPrFPi0/7i2UtW2i9
pGU23VheHxNg+e2jE6X3EBpDtQCRB01DpoinwajG8N1Cltfuz3imzLewjp
++dwQV0xa4m8u0ED7kszOpgb51r1keJRNRIrzsoowQkBgQDTftdg9eEg7Q8UL51w
GUf9ZVmT4pT2zDExrTwQ270f70Gbnu/Aaf2EhIFLFJGponbua50EVufbKacxx
pNiUw;JLPmqbB7ie9sqTyoeRqc2y/0x3uwBC614uAnZz+EkMcXGoLLuqUSu5j9f
5a71jJjsGW5C5BPYnVAExuuKBgQDG1VTnfj0k9X3HzCNm502V+bxzG4Pmhce
J6UgiKJ4peCbsnsihtL10h1RHsvUopUgml08spv0/+Krv0NpnML7tsLqJqpt8
iarUt0J7EZ5vZqFCNBLz4wZbgBaGNa17L6cu9gITOfefB+xM0+EDCHHPaRBldlhxf
SN1yE3BX4wLBg+EG9eISl+d4g02/F8alLvtDPG2Ri7cFAR5sEuaov/77kLYASLI
NKTm7tBi9cHC0n0xk+AIf8FBT16r5gtTbwvVvMvh8mDrgiM1Mp+ANbTv+cJA3y
UY13Yj62pbq7cF3gcvAyAg+2uAl181c1EYophzG6VDbVeJpmIGR25rhAoGBAMR
ox/WKc0Jmmz91Y7Jx3Bh25yusm74fL5Yqa7StckMaLpw60Hzn4Ba7s5nVL-FG
xoc6X1jVeU+2abwLYCT0Jazlpskj+2VM2Tgkqr0+C3jIx4Uf21weAcG51sGP
o67h1Te93j1dL2KktfDea/MUrIggIhwq8id289vhAoGAwVvSPYEMF5mqiqFRwam
W/kQUGaePpMWLrx+DMlypUm1PGFdfrBsUzHh1Vs7/TU4kj3Nhra5XKEJHlOhVxF
RN+zxBge4TBpR+b0VwmPl3ZhiQwCESEH/a04vZ1DhDplQvpCL8DAqrwd3EhI4qf
BZYBXKKOaPSgiokLgn4EcUy-
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDCjCAFKgAwIBAgLUThuLiJ009/GPLfgYBnctoWGoHowDQYJKoZIhvvcNAQEL
BQAwEjQMAIGA1UEAwH2Zxwv9jcaefw0MjExMDUxNjIsMjaRaWzMjExMDIx
NjIsMjaRaB1xEADAOBgNVBAMMB2dsGlv3MwggEiAAGC5qGS1b3DQEBAQAA4tB
DwAwwgEKaoIBAQCKrF1DEEP0uOrLondgs/Aq5jVR3Y+G/FM6IAntESrUHCmLsT
KHIkhwlNaAd9m3r0NL5S5y17bCY2H6TdtP5m0ZwD5kNt7a8xDoh1b10FOBuB
XYlPCENzhVVZS+PmRYmuF1s0ryUeBR9x7tL16LIVgkNc3d3Xnix0kuHjfbrZnpj
K57lsALzNxu34sjo/+GbCCnCs1Yskp/xh76e5RnVnnMuKK+kwKus/JrIigyt
DoTbuP8i5LJdTH9e2xQFfwG8fpC7g/NxuEH7V0/gpwFblwtvmyR/AlaidDFx+k
/f0ZU+BpdqU2lYushh/u3508QjNvYe6XrYLAgMBAGjWDwMAkGa1dEwQCMAAw
SQYDV0RBEIwQ1IH2x2waW9jyc4YxaHR0cDvL2dscGkuc2leaa2ebG9jYwlyGfmh0
dHAGL9yvV3Muc2l0a2FubG9jYwlyHBkwUAB4wDQYJkotIhvcNAQELBQAQdgFBAEjN
mFJinjAF+ZwKAAAGi50KVrfp7zY1kw0nja19PBrbbIgr7M2+Z5KbfSURXBYthKI
bL5ikRoSxi1oKsjpOfis1ETQ12G00ySSeCaqbCnRFzqCLU6HNAfvlzwdd+lUSq
Jvn7yvNijzLqQCONXxldv/THNTx85dxeamiIaul1X9q+0LeTxAla1GyCmFPXvm
oIACJu24/1M7BU110ptk1mBoPut/h6gOUf2/FdtctBhBzfkTvIJCBQexzcfcfd8sh
D6jj91trghqEFANnBRDGvH/+NEsnmRwkW89s3JxcuIXOcx5XKtdzT85D01tuRrl
PUHndihjtda9Rh5MY=
-----END CERTIFICATE-----

```

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

```

root@glpi:/etc/ssl/private# a2enmod ssl
Considering dependency setenif for ssl:
Module setenif 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

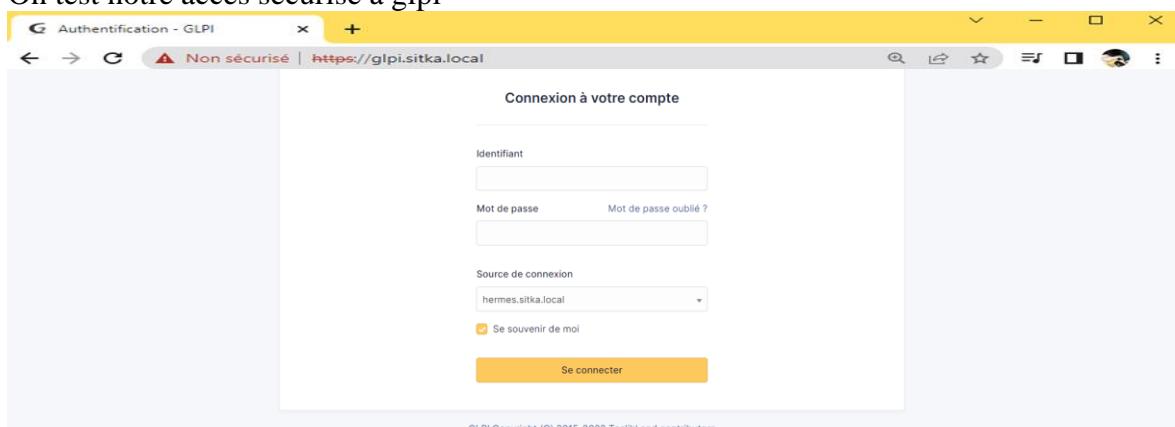
```

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

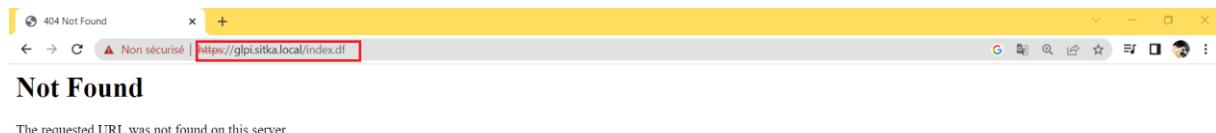
Apache envoie par défaut des entêtes HTTP contenant le nom et la version du serveur web ainsi que le système d'exploitation qui héberge apache, ceci peut être problématique car on peut faciliter l'attaque de notre serveur en divulguant ces informations.

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.

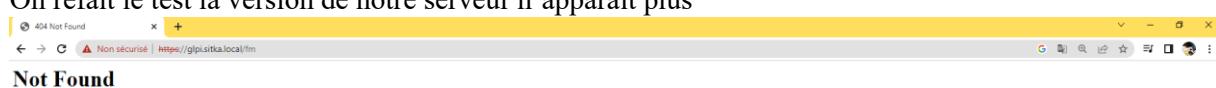
```
root@glpi:~# cd /etc/apache2/conf-enabled/
root@glpi:/etc/apache2/conf-enabled# vim security.conf |
```

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
```

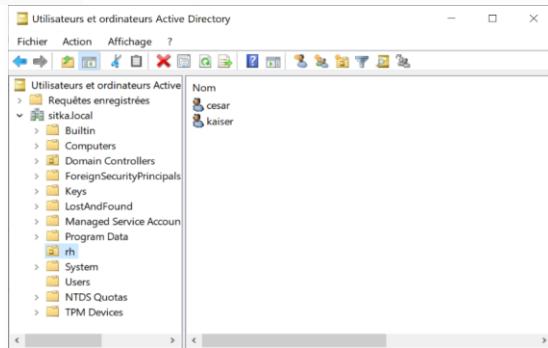
On refait le test la version de notre serveur n'apparait plus



I- 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- Importation des utilisateurs à partir de notre base d'annuaire ldap

Sur GLPI :

- Configuration
- Authentification
- Annuaire LDAP
- Je clique sur le signe + pour rajouter un **annuaire ldap**
- Rechercher
- Cocher la ou les cases des utilisateurs à importer

Je sélectionne configuration + authentification puis je selectionne **Annuaire LDAP**

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

On remplit 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 contrôleur de domaine

On clique sur ajouter après avoir rempli le formulaire

Nouvel élément - Annuaire LDAP

Préconfiguration

Active Directory / Valeurs par défaut

Nom : hermes.sitka.local

Serveur par défaut : Oui

Actif : Oui

Serveur : 172.20.0.14

Port (par défaut 389) : 389

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

BaseDN : OU=rh,DC=sitka,DC=local

Utilisez un compte (pour les connexions non anonymes) : Oui

DN du compte (pour les connexions non anonymes) : CN=Administrateur,CN=Users,DC=sitka,DC=local

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

Champ de l'identifiant : samaccountname

Commentaires :

Champ de synchronisation : objectguid

+ Ajouter

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

Actions	nom*	SERVEUR	DERNIÈRE MODIFICATION	ACTIF
	hermes.sitka.local	172.20.0.14	2022-11-06 09:23	Oui

Éléments visualisés : contenu

Actions

Rechercher

20 lignes / page

Annuaire LDAP - hermes.sitka.local

Tester

Utilisateurs

Groupes

Informations avancées

Réplicats

Historique

Tous

Annuaire LDAP

Nom : hermes.sitka.local

Dernière modification : 2022-10-23 20:38

Serveur par défaut : Oui

Actif : Oui

Serveur : 172.20.0.14

Port (par défaut 389) : 389

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

BaseDN : OU=rh,DC=sitka,DC=local

Utilisez un compte (pour les connexions non anonymes) : Oui

DN du compte (pour les connexions non anonymes) : CN=Administrateur,CN=Users,DC=sitka,DC=local

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

Champ de l'identifiant : samaccountname

Commentaires :

Champ de synchronisation : objectguid

Supprimer définitivement

Sauvegarder

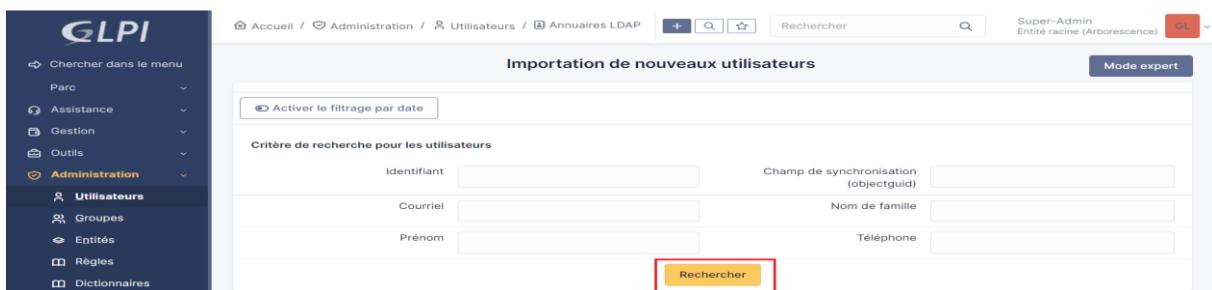
On fait le test de connexion avec active directory



a. 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 plus on clique sur action et on selectionne importer

The screenshot shows a list of users 'kaiser' and 'cesar' with checkboxes checked. The 'Actions' button is highlighted in yellow. Below the list, two sections show 'Dernière mise à jour dans l'annuaire LDAP' for each user, with dates and times listed.



Vérifier la présence des utilisateurs importés dans le menu :

- Administration
- Utilisateur.

Identifiant	Nom de famille	Adresses de messagerie	Téléphone	Lieu	Actif
cesar	cesar			Oui	
glpi				Oui	
kaiser				Oui	
normal				Oui	
post-only				Oui	
tech				Oui	

On test une connexion ldap avec glpi

Connexion à votre compte

Identifiant	<input type="text" value="kaiser"/>
Mot de passe	<input type="password" value="*****"/>
Source de connexion	<input type="text" value="hermes.sitka.local"/>
<input checked="" type="checkbox"/> Se souvenir de moi	
<input type="button" value="Se connecter"/>	

1- Crédation 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

```
root@glpi:~# telnet xmail.sitka.local 25
Trying 172.20.0.70...
Connected to xmail.sitka.local.
Escape character is '^]'.
220 xmail.sitka.local ESMTP Postfix
hello 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><LF>
subject:test d'envoi de mail à partir de glpi
ceci est un test vers zimbra

250 2.0.0 Ok: queued as 484981201C4
quit
221 2.0.0 Bye
Connection closed by foreign 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

The screenshot shows the Zimbra web interface. In the top navigation bar, the URL is https://zimbra.sitka.local:8443/. The main area displays a list of emails under the 'Réception' folder. One email is selected, showing the subject: 'test de mail - ceci est un test d'envoi de mail entre support et admin'. The email was received at 20:28. A note below the list says 'Pour afficher une conversation, cliquez dessus.'

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

The screenshot shows the GLPI administration interface. The left sidebar is open with 'Administration' selected, then 'Utilisateurs'. A new user account is being created with the identifier 'glpi'. The 'Email' field is filled with 'support@xmail.sitka.local'. Other fields like 'Nom de famille', 'Prénom', 'Mot de passe', and 'Confirmer mot de passe' are also visible. On the right side, there are tabs for 'Courriels', 'Authentification', and 'Catégorie'. At the bottom right, there are buttons for 'Mettre à jour le cache' and 'Sauvegarder'.

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

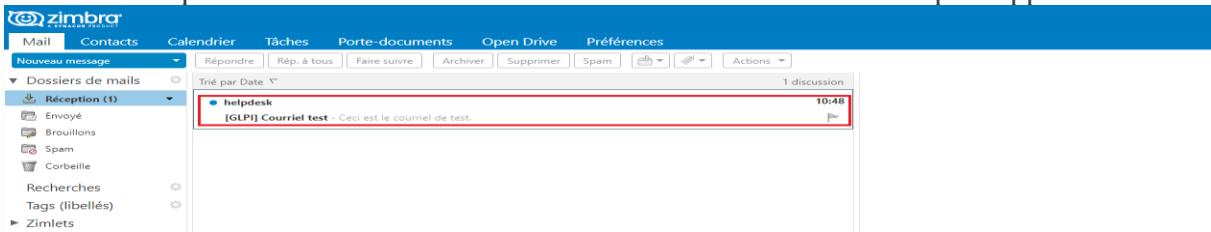
The screenshot shows the GLPI configuration interface. The left sidebar has 'Notifications' selected. In the main area, there are two sections: 'Configuration des notifications' and 'Notifications'. The 'Configuration des notifications' section contains three checkboxes: 'Activer le suivi', 'Activer les notifications par courriel', and 'Activer les notifications navigateur'. The 'Activer les notifications par courriel' checkbox is highlighted with a red box and a red arrow labeled '2'. The 'Notifications' section contains a single checkbox 'Modèles de notifications', which is also highlighted with a red box and a red arrow labeled '3'.

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.support.local on sauvegarde en suite notre formulaire

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

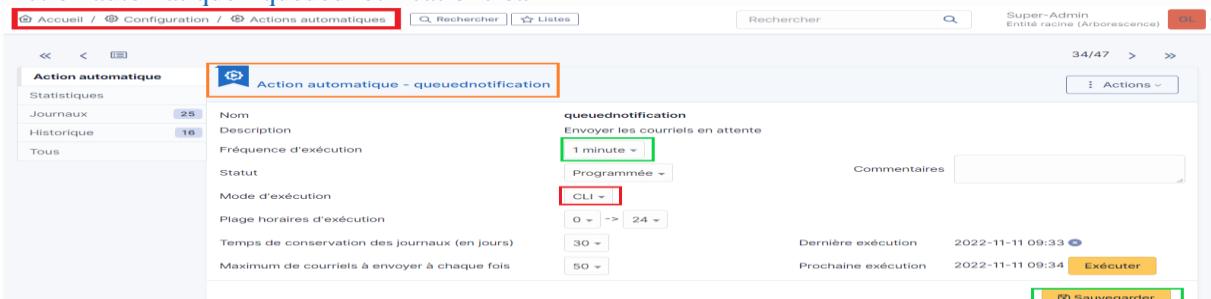


Et on vérifie que le mail du test est bien arrivé dans la boîte mail du compte support



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

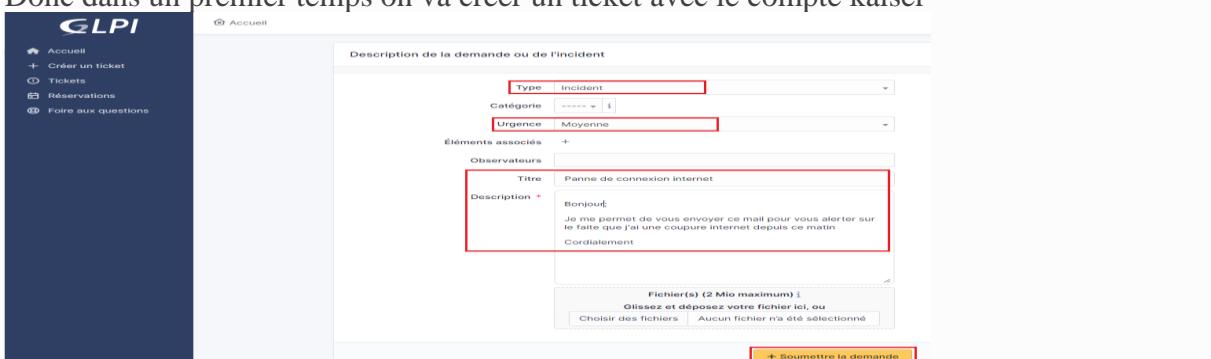
Action automatique - queuednotificationclean



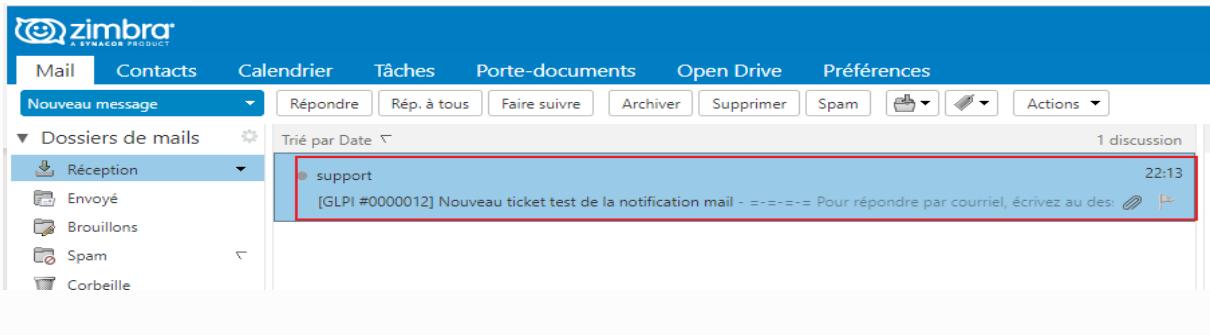
Maintenant on va vérifier le fonctionnement de l'alerte configurée en se connectant avec un utilisateur et en créant un ticket ; le compte glpi devrait être

Alerter de la création du ticket à travers la réception d'un mail dans sa boîte 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 boîte mail support



The screenshot shows the Zimbra webmail interface. The top navigation bar includes Mail, Contacts, Calendrier, Tâches, Porte-documents, Open Drive, and Préférences. Below the navigation is a toolbar with buttons for Répondre, Rép. à tous, Faire suivre, Archiver, Supprimer, Spam, and Actions. A sidebar on the left titled 'Dossiers de mails' shows 'Réception' selected, with sub-options Envoyé, Brouillons, Spam, and Corbeille. The main pane displays an email from 'support' with the subject '[GLPI #0000012] Nouveau ticket test de la notification mail'. The message is framed by a red border.

b- Notification par collecteurs

Les collecteurs nous permettent la création des tickets automatiquement par envois de mail
Glpi grâce aux tâches automatiques va récupérer le mail puis va créer un ticket

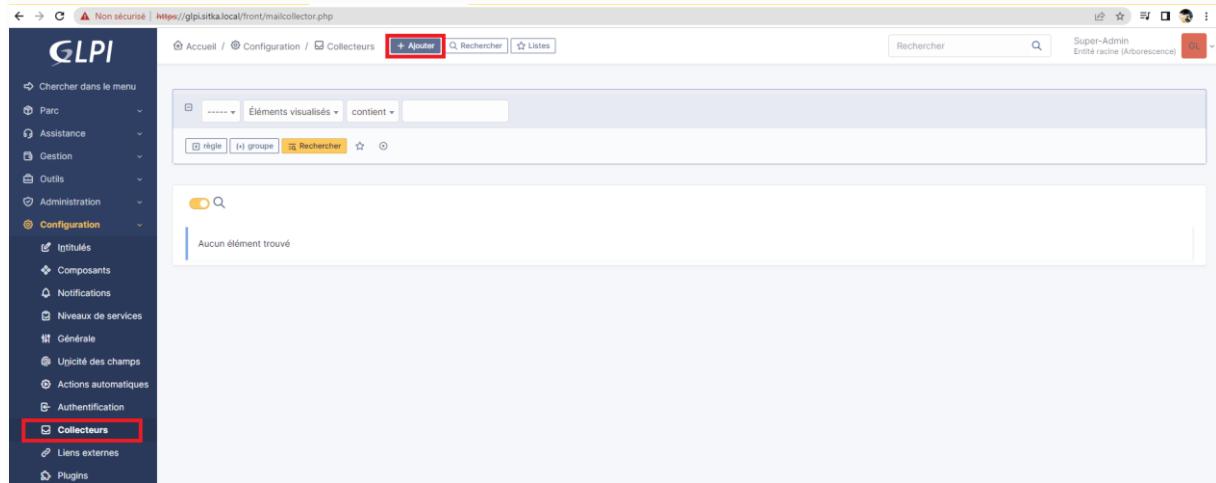
Attention pour cette procédure fonctionne il faut que l'utilisateur ainsi que son mail existe
dans la base glpi si non il y'aura un refus de glpi

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



The screenshot shows the GLPI configuration interface. The left sidebar has sections like Parc, Assistance, Gestion, Outils, Administration, Configuration, Intitulés, Composants, Notifications, Niveaux de services, Générale, Urgicité des champs, Actions automatiques, Authentification, and Collecteurs. The 'Collecteurs' section is highlighted with a red box. The main pane shows a search bar and a message stating 'Aucun élément trouvé'. At the top, there is a navigation bar with Accueil, Configuration, Collecteurs, and an 'Ajouter' button, which is also highlighted with a red box.

Après on remplit le formulaire comme indiqué ci-dessous ; si on choisit pop au lieu d'IMAP
il faut mettre le port **995** 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

NOM	TYPE D'ÉLÉMENT	DESCRIPTION
contract	Contrat	Envoi des alertes sur les contrats
countAll	Recherche sauvegardée	Mettre à jour le temps d'exécution de tous les marque pages
createInquest	Ticket	Génération des enquêtes de satisfaction
DomainsAlert	Domaine	Domaines expirés ou à explorer
graph	Action automatique	Nettoyage des graphiques générés
infocom	Informations financières et administratives	Envoyer des alertes sur les informations financières et administratives
logs	Action automatique	Nettoyage des anciens journaux
mailgate	Collecteur	Récupération des messages (collecteurs)
mailgateerror	Collecteur	Envoyer des alertes sur les erreurs de collecteur
olaticket	Niveau de OLA pour le Ticket	Action automatique pour les OLAs
passwordexpiration	Utilisateur	Gérer les politiques d'expiration des mots de passe des utilisateurs
pendingreason_autobump_autosolve	Suivi / Résolutions automatiques	Suivi et résolutions automatiques pour les tickets en attente
planningrecall	Rappel du planning	Envoyer les rappels pour le planning

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

The screenshot shows the GLPI interface with the 'Actions automatiques' menu selected. The main panel displays a configuration form for an automatic action named 'mailgate'. The 'Fréquence d'exécution' is set to '10 minutes'. The 'Prochaine exécution' button is highlighted with a red box. At the bottom right, there is a large red box around the 'Exécuter' button.

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.

The screenshot shows the 'Collecteurs' configuration page. The 'Actions' tab is selected in the sidebar. In the main panel, a red box highlights the 'Récupérer les courriels maintenant' button.

c- Gestion des tickets

2- Fusion-inventory

a- Installation du plugin fusion-inventory

The screenshot shows the 'Plugins' configuration page. The 'Plugins' menu item is selected in the sidebar. A red box highlights the 'Oui' button in a confirmation dialog at the bottom.

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>

Assets	4	3.82 MB	20 days ago
fusioninventory-10.0.3+1.0.tar.bz2		3.82 MB	20 days ago
fusioninventory-10.0.3+1.0.zip		5.56 MB	20 days ago
Source code (zip)			20 days ago
Source code (tar.gz)			20 days ago

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 décomprime le plugin téléchargé

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

On déplace le plugin vers /var/www/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'icône avec le signe plus en bas à droite

The screenshot shows the GLPI interface with the 'Configuration' menu selected. In the 'Plugins' section, there is a table listing the FusionInventory plugin. The table has columns for Nom, Dossier, Version, Licence, Statut, Auteurs, Site Web, and Actions. A red box highlights the 'Actions' button and the '+' icon in the top right corner of the table header.

L'installation démarre

The screenshot shows the GLPI interface with the 'Actions' button highlighted. Below it, a message box displays the progress of the plugin installation: "Installation of plugin FusionInventory (0 seconde)", "Clean data from old installation of the plugin (0 seconde)", "Clean rules from old installation of the plugin (0 seconde)", and "Creation tables in database (0 seconde)".

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

The screenshot shows the GLPI interface with the 'Actions' button highlighted. The FusionInventory plugin is listed in the table with a status icon showing it is not activated. A red box highlights the status icon.

Une fois activé l'icône devient verte

The screenshot shows the GLPI interface with the 'Actions' button highlighted. The FusionInventory plugin is listed in the table with a status icon showing it is activated. A red box highlights the status icon.

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

The screenshot shows the GLPI interface with a warning message: "Le cron de GLPI ne fonctionne pas, voir documentation". A red box highlights this message.

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

```

root@glpi-ocs:~# crontab -u www-data -e
no crontab for www-data - using an empty one

Select an editor. To change later, run 'select-editor'.
 1. /bin/nano   <---- easiest
 2. /usr/bin/vim.basic
 3. /usr/bin/vim.tiny

Choose 1-3 [1]: 

```

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

```

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

```

Enfin en redémarre le service cron

```

root@glpi-ocs:~# /etc/init.d/cron restart

```

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 tâches de cron

b- Installation des agents fusion-inventory

On va sur la page GitHub pour télécharger l'agent 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

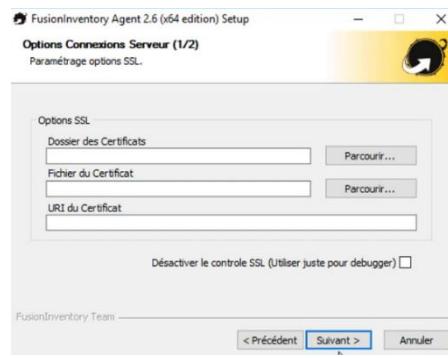
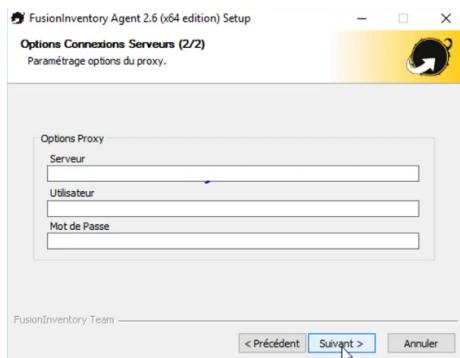
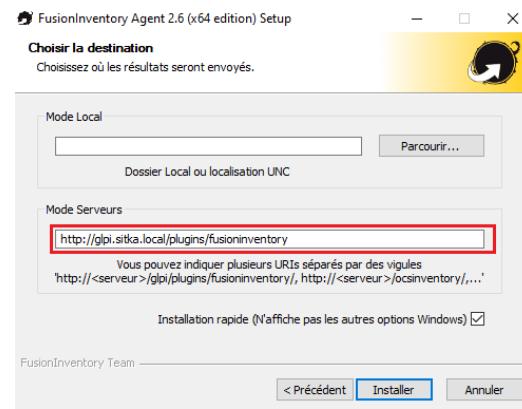
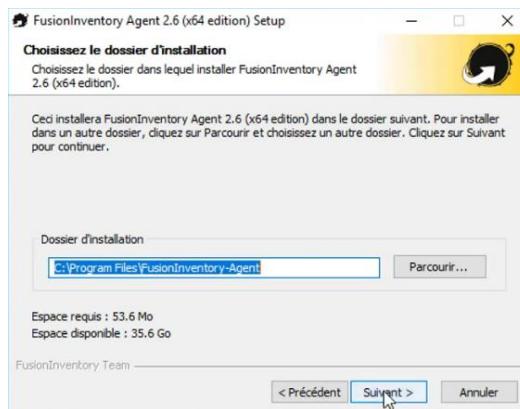
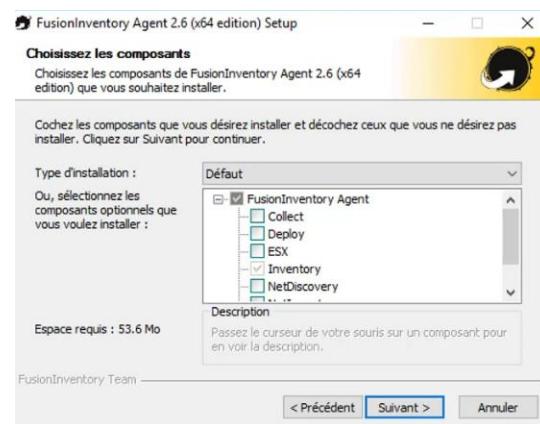
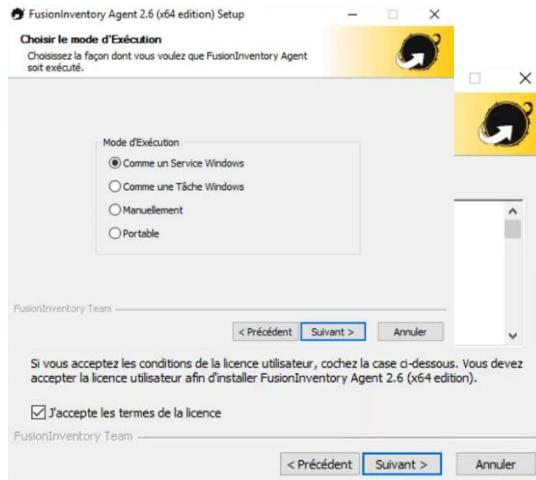
- o Windows installer
 - Windows 64-bit OS: [fusioninventory-agent_windows-x64_2.6.exe](#)
 - Windows 32-bit OS: [fusioninventory-agent_windows-x86_2.6.exe](#)
- o Portable package
 - Windows 64-bit OS: [fusioninventory-agent_windows-x64_2.6-portable.exe](#)
 - Windows 32-bit OS: [fusioninventory-agent_windows-x86_2.6-portable.exe](#)

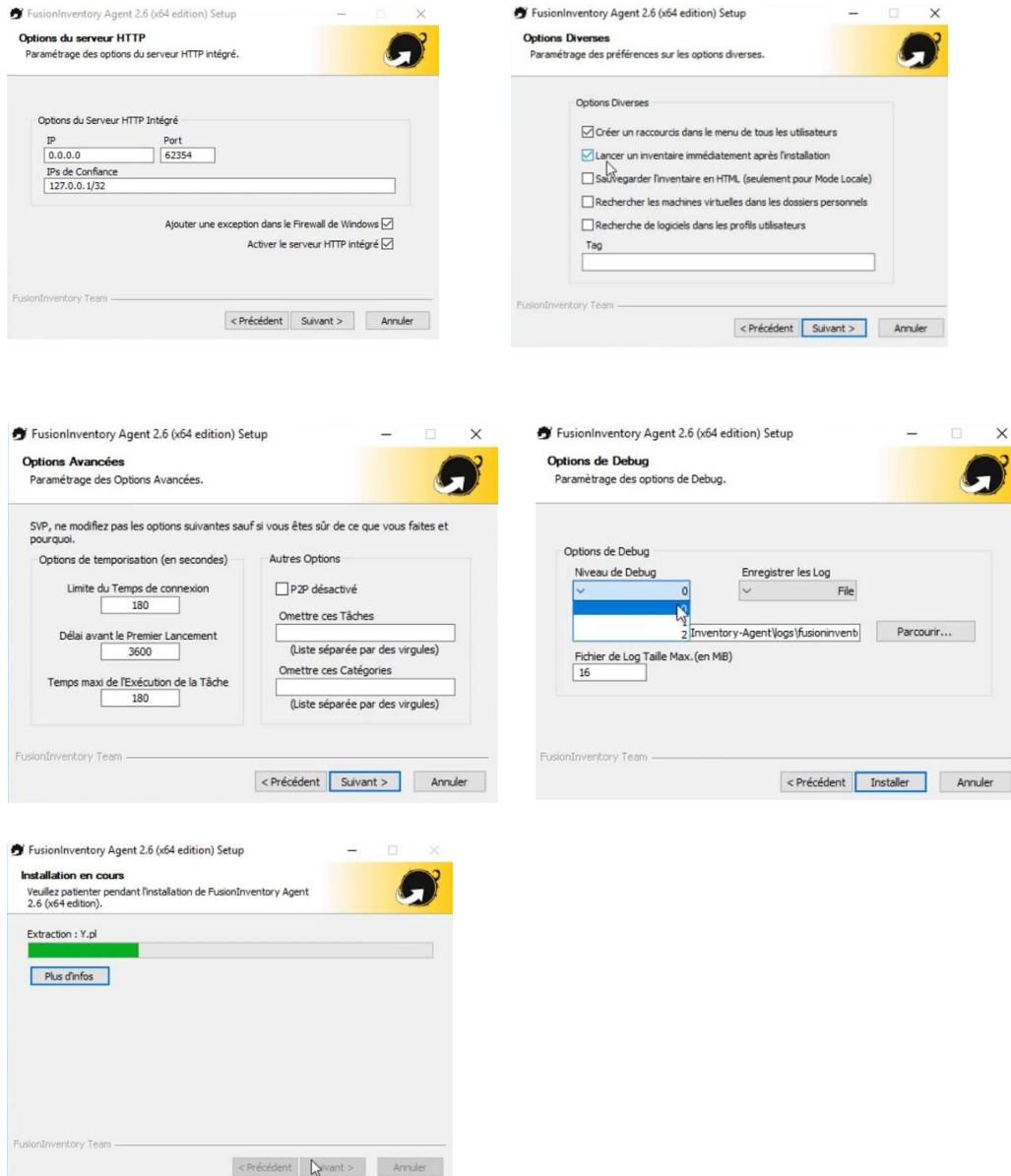
On télécharge la dernière version



Une fois téléchargé on lance l'installation







ii- Installation de l'agent fusion inventory pour linux

On installe le paquet fusioninventory-agent

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

On vérifie l'installation ainsi que la version

```
root@glpi-ocs:~# dpkg -l fusioninventory-agent
Soushaut=inconnU/Installe/suppRime/Purge/H=à garder
| État=Non/Installé/Fichier-Config/dépaqUté/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
```