



BTS — Services Informatiques aux Organisations 1ère année

Ubuntu Server 16.04—GLPI et FusionInventory

1 / Ubuntu Server 16.04 : Mise en place mot de passe sur compte ROOT

Se connecter avec l'utilisateur créé lors de l'installation.
(Identifiant : administrateur, mot de passe : admin)

Entrez ensuite :

sudo su , validez, puis entrez ensuite le mot de passe défini ci-dessus et validez.

Mise à jour du mot de passe du compte ROOT :

Commande : **sudo passwd root** et entrez un mot de passe pour le compte ROOT.

Rebooter le Serveur. (Commande : **reboot**)

2 / Ubuntu Server 16.04 : Paramétrage de l'adressage IP STATIQUE

Se connecter avec le compte ROOT à chaque redémarrage ou reboot du serveur

Une fois que l'on a déterminé quelle adresse IP Statique on voulait donner à notre serveur Linux, il faut faire en sorte que ce serveur prenne cette adresse IP et n'en change plus jamais au redémarrage de votre serveur.

Avec winSCP ou en manuel (sous l'éditeur VIM), éditez le fichier **/etc/network/interfaces**, pour ajouter l'adressage IP souhaité. (ci-dessous, un exemple du fichier interfaces pour un adressage statique)

Exemple de configuration d'adressage au niveau du fichier "interfaces"

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

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens32
iface ens32 inet static
    address 192.168.0.243
    netmask 255.255.255.0
    network 192.168.0.0
    broadcast 192.168.0.255
    gateway 192.168.0.254
    # dns-* options are implemented by the resolvconf package, if installed
    dns-nameservers 192.168.0.1
```

REDEMARREZ ensuite le serveur s'il y a eu création ou modification d'adressage avec la commande **REBOOT**



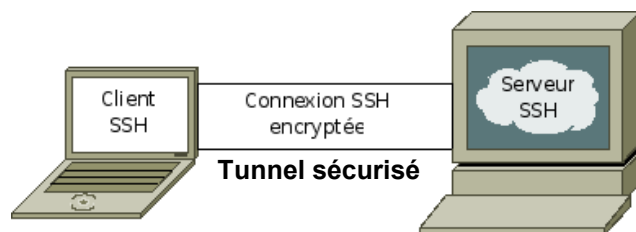
Installation de NETDATA (voir feuille annexe)

3 / Installation du service OPEN SSH

OpenSSH : nécessaire pour le contrôle à distance et le transfert de données entre des ordinateurs en réseau. OpenSSH est une version libre de la famille d'outils du protocole Secure Shell (SSH) pour le contrôle à distance ou le transfert des fichiers entre les ordinateurs.

Le serveur OpenSSH, `sshd`, attend en permanence des connexions depuis des clients. Quand une requête de connexion a lieu, `sshd` établit la connexion correcte en fonction du type de client. Par exemple, si un client se connecte avec le client `ssh`, le serveur OpenSSH va établir une connexion sécurisée après une authentification. Si un client se connecte avec WinSCP (par exemple), le serveur OpenSSH va commencer un transfert de fichier sécurisé entre le serveur et le client après une authentification.

Connexion sécurisée SSH = création d'un tunnel dans lequel circuleront les différentes données encryptées que vous envoyez et recevez



Installation du Service SSH :

Installation du service SSH : `sudo apt-get install openssh-server`

Vérification du status du service SSH: `sudo service ssh status`

Nous pouvons remarquer ici, avec la commande « `sudo service ssh status` », que le service est bien lancé et que son port de communication est 22.

4 / Ubuntu Server 16.04 : Autoriser l'utilisateur ROOT sur l'accès SSH (winSCP)

Nous devons, maintenant, autoriser l'utilisateur ROOT à avoir accès en SSH via WinSCP aux différents répertoires et fichiers de son serveur linux UBUNTU.
Il faut, pour cela, modifier un fichier appartenant à OPENSSH. (le fichier `sshd_config`).

Autoriser ROOT à accéder au SSH :

Commande : VIM (éditeur)

Veillez changer dans le fichier `/etc/ssh/sshd_config` la ligne

PermitRootLogin yes

Enregistrer et quitter sous VIM : `:wq`

Rebooter le Serveur. (Commande : `reboot`)

et

Tester l'accès avec WinSCP en SFTP avec l'utilisateur ROOT

5 / Ubuntu Server 16.04 : Installation de APACHE

Le logiciel libre **Apache HTTP Server (Apache)** est un serveur HTTP créé et maintenu au sein de la fondation Apache. C'est le serveur HTTP le plus populaire du World Wide Web.

Apache fonctionne principalement sur les systèmes d'exploitation UNIX (Linux, Mac OS X, Solaris, BSD et UNIX) et Windows.



Installation et configuration du Service APACHE :

```
sudo apt-get update  
sudo apt-get install apache2
```

Editez le fichier apache2.conf (avec winSCP ou VIM)

```
sudo vim /etc/apache2/apache2.conf
```

A l'intérieur du fichier, au tout début, ajoutez la ligne :

```
ServerName adresse_ip_de_votre_serveur
```

Redémarrez Apache pour validez le changement effectué

```
sudo systemctl restart apache2
```

Vous pouvez ensuite tester et vérifier l'accès à APACHE, sur un autre poste de votre réseau, via la commande ci-dessous dans un navigateur : http://adresse_ip_de_votre_serveur. Vous pouvez constater que vous arrivez bien sur la page APACHE. Votre service APACHE est donc démarré et fonctionnel sur votre Serveur LINUX Ubuntu.

6 / Ubuntu Server 16.04 : ACTIVER LE FIREWALL

Un serveur doit, pour des raisons évidentes, être sécurisé...même un serveur LINUX ! . C'est pourquoi, il est important d'activer dès maintenant son FIREWALL (en effet, le FireWall n'est pas activé par défaut à l'installation du serveur LINUX).

Démarrage du Firewall :

```
sudo ufw enable
```

REBOOTER le serveur

Tester et vérifier l'accès à APACHE (http://adresse_ip_de_votre_serveur). Vous pouvez constater que vous n'avez plus accès à APACHE. (Le FireWall de votre serveur Linux bloque maintenant l'accès). Il va maintenant falloir accorder l'accès à APACHE au niveau du Firewall de votre serveur LINUX Ubuntu. Le FireWall doit accepter les requêtes HTTP et HTTPS des machines qui voudraient se connecter au serveur Web sous Ubuntu Server.

Voir la liste des applications disponibles via le Firewall

```
sudo ufw app list
```

Voir l'information des services APACHE au niveau du Firewall

```
sudo ufw app info "Apache Full"
```

Autoriser le service APACHE au niveau du Firewall

```
sudo ufw allow in "Apache Full"
```

Cette dernière commande autorise le trafic entrant (au travers du FireWall) sur le Service APACHE.
Tester et vérifier l'accès à APACHE (http://adresse_ip_de_votre_serveur).

Vous pouvez constater que vous avez à nouveau accès à APACHE !

Vérification de l'accès à WinSCP suite à l'activation du Firewall sur votre serveur Linux

Tester et vérifier l'accès WinSCP vers votre Serveur LINUX

*Vous pouvez constater que vous n'avez plus accès à votre Serveur LINUX via WinSCP !
Il va donc falloir ouvrir le port de communication SSH au niveau de votre FireWall sur votre Serveur LINUX. (Port N° 22).*

Ouverture du port N°22 (pour le service SSH)

```
sudo ufw allow 22/tcp
```

Tester et vérifier à nouveau l'accès

WinSCP vers votre Serveur LINUX

Vous pouvez constater que vous avez accès à nouveau à votre Serveur LINUX via WinSCP !



Vous ferez de même pour le service NETDATA (installé en début de TP)

Visualisation des règles mises en place au niveau du Firewall sur votre serveur Linux

La commande ci-dessous va vous permettre de visualiser les règles que vous avez ouvert au niveau de votre FireWall sur votre serveur LINUX.

```
sudo ufw status verbose
```

7 / Ubuntu Server 16.04 : installation de MYSQL

Maintenant que votre serveur web est accessible, il est temps d'installer Mysql.
Entrez la commande ci-dessous :

```
sudo apt-get install mysql-server
```

Pendant l'installation, il faudra choisir et rentrer un mot de passe pour le compte ROOT de MYSQL (cf ci-dessous) (question de sécurité !).
Vous prendrez le même mot de passe que le compte ROOT. (admin)

Configuration de mysql-server-5.7

Il est très fortement recommandé d'établir un mot de passe pour le compte d'administration de MySQL (« root »).

Si ce champ est laissé vide, le mot de passe ne sera pas changé.

Nouveau mot de passe du superutilisateur de MySQL :

<Ok>

8 / Ubuntu Server 16.04 : installation de PHP

PHP: Hypertext Preprocessor, plus connu sous son sigle PHP (acronyme récursif), est un langage de programmation libre, principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP. PHP est un langage impératif orienté objet.

Installation de PHP :

```
sudo apt-get install php libapache2-mod-php php-mcrypt php-mysql php-curl
```

9 / Ubuntu Server 16.04 : installation de PHPMYADMIN

phpMyAdmin (PMA) est une application Web de gestion pour les systèmes de gestion de base de données MySQL réalisée en PHP et distribuée sous licence GNU GPL.

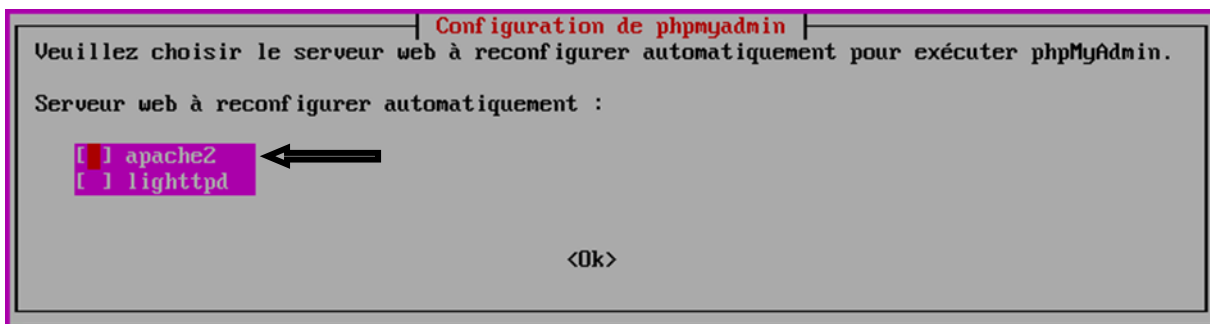
Il s'agit de l'une des plus célèbres interfaces pour gérer une base de données MySQL sur un serveur PHP. De nombreux hébergeurs, gratuits comme payants, le proposent ce qui évite à l'utilisateur d'avoir à l'installer.

Cette interface pratique permet d'exécuter, très facilement et sans grandes connaissances en bases de données, des requêtes comme les créations de table de données, insertions, mises à jour, suppressions et modifications de structure de la base de données, ainsi que l'attribution et la révocation de droits et l'import/export. Ce système permet de sauvegarder commodément une base de données sous forme de fichier .sql et d'y transférer ses données, même sans connaître SQL.

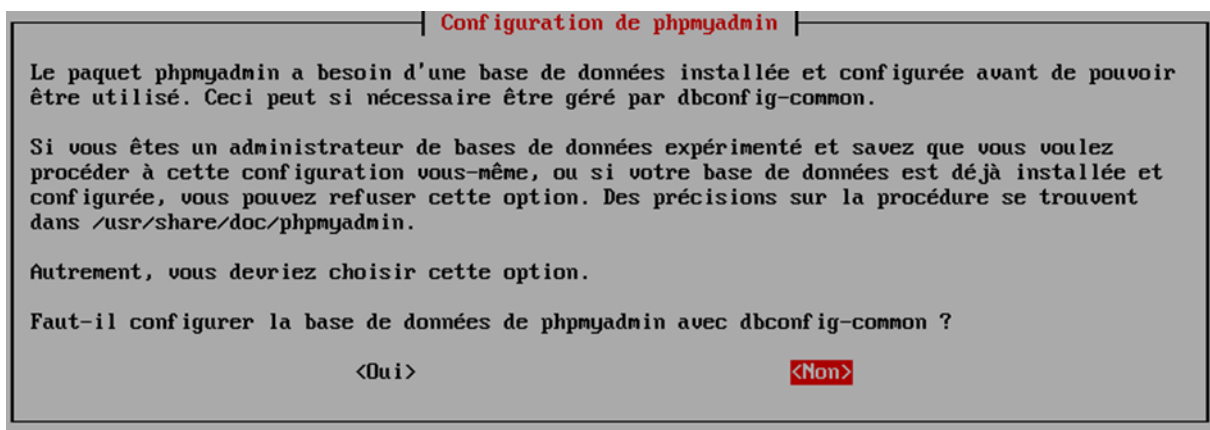


Installation de PHPMYADMIN

```
sudo apt-get install phpmyadmin apache2-utils
```



Ici, il faut choisir **APACHE2** en sélectionnant avec la touche ESPACE !, puisque c'est apache que nous avons installé précédemment



Ici, il faut répondre **NON**.

Vous pouvez ensuite vérifier le bon fonctionnement de phpmyadmin, sur un autre poste de votre réseau, avec la commande ci-dessous dans un navigateur :

```
http://adresse_IP_de_votre_serveur/phpmyadmin
```

10 / Ubuntu Server 16.04 : installation de GLPI version 9.1

GLPI (acronyme de gestionnaire libre de parc informatique) est un logiciel libre de gestion des services informatiques (ITSM) et de gestion des services d'assistance (issue tracking system et ServiceDesk). Cette solution open source est éditée en PHP et distribuée sous licence GPL.

GLPI est une application web qui aide les entreprises à gérer leur système d'information. Parmi ses caractéristiques, cette solution est capable de construire un inventaire de toutes les ressources de la société et de réaliser la gestion des tâches administratives et financières. Les fonctionnalités de cette solution aident les Administrateurs IT à créer une base de données regroupant des ressources techniques et de gestion, ainsi qu'un historique des actions de maintenance. La fonctionnalité de gestion d'assistance ou helpdesk fournit aux utilisateurs un service leur permettant de signaler des incidents ou de créer des demandes basées sur un actif ou non, ceci par la création d'un ticket d'assistance.



Téléchargement de GLPI 9.1

```
cd /tmp
wget https://github.com/glpi-project/glpi/releases/download/9.1/glpi-9.1.tar.gz
```

Ici, l'archive de glpi est téléchargée directement dans le répertoire TMP de votre serveur LINUX Ubuntu.

Installation de GLPI 9.1

```
cd /opt/
sudo tar -xvzf /tmp/glpi-9.1.tar.gz
```

Ici, le fichier téléchargé glpi est directement décompressé dans son répertoire d'installation OPT sur votre serveur LINUX Ubuntu.

Création d'un fichier glpi.conf

Création du fichier avec l'éditeur VIM ou WinScp.
Le fichier glpi.conf doit se trouver dans le répertoire : **"/etc/apache2/conf-available/glpi.conf"**

Le fichier glpi.conf doit contenir les lignes suivantes :

ATTENTION, il faut absolument respecter les Majuscules et minuscules dans les lignes de commande ci-dessous. (le service APACHE risquerait de ne plus vouloir démarrer !)

```
Alias /glpi /opt/glpi

<Directory /opt/glpi>
DirectoryIndex index.php
Options FollowSymLinks
AllowOverride Limit Options FileInfo
Require all granted
</Directory>
```

Il faut maintenant activer la configuration glpi :

```
cd /etc/apache2/conf-enabled
sudo ln -s ../conf-available/glpi.conf
```

↳ Lettre L minuscule

REDEMARRER le service APACHE :

```
sudo service apache2 restart
```

Appliquer certaines permissions au dossier de GLPI

```
chmod -R 777 /opt/glpi/files  
chmod -R 777 /opt/glpi/config
```

chmod (abréviation de **change mode**) est un appel système d'Unix ainsi que la commande correspondante qui permet de changer les permissions d'accès d'un fichier ou d'un répertoire.

Un utilisateur a le droit de faire un chmod sur un fichier :

- s'il est root ou s'il est le propriétaire du fichier en question.

Récapitulatif des différentes valeurs possibles fréquemment utilisées

644 - Lecture, écriture pour le propriétaire / Lecture pour les autres

666 - Lecture, écriture pour tout le monde

700 - Lecture, écriture, exécution juste pour le propriétaire

705 - Le propriétaire à tous les droits / Le groupe aucun / Les autres lire et exécuter

755 - Le propriétaire à tous les droits / Les autres lire et exécuter

764 - Tous droits pour le propriétaire / Lecture, écriture pour le groupe / Lecture seule pour les autres

774 - Tous les droits pour le propriétaire et le groupe / Lecture seule pour les autres

775 - Tous les droits pour le propriétaire et le groupe / Lecture et exécution pour les autres

777 - Tous les droits pour tous

Installation finale de GLPI 9.1

Vous pouvez ensuite terminer l'installation de GLPI, avec la commande ci-dessous dans un navigateur :

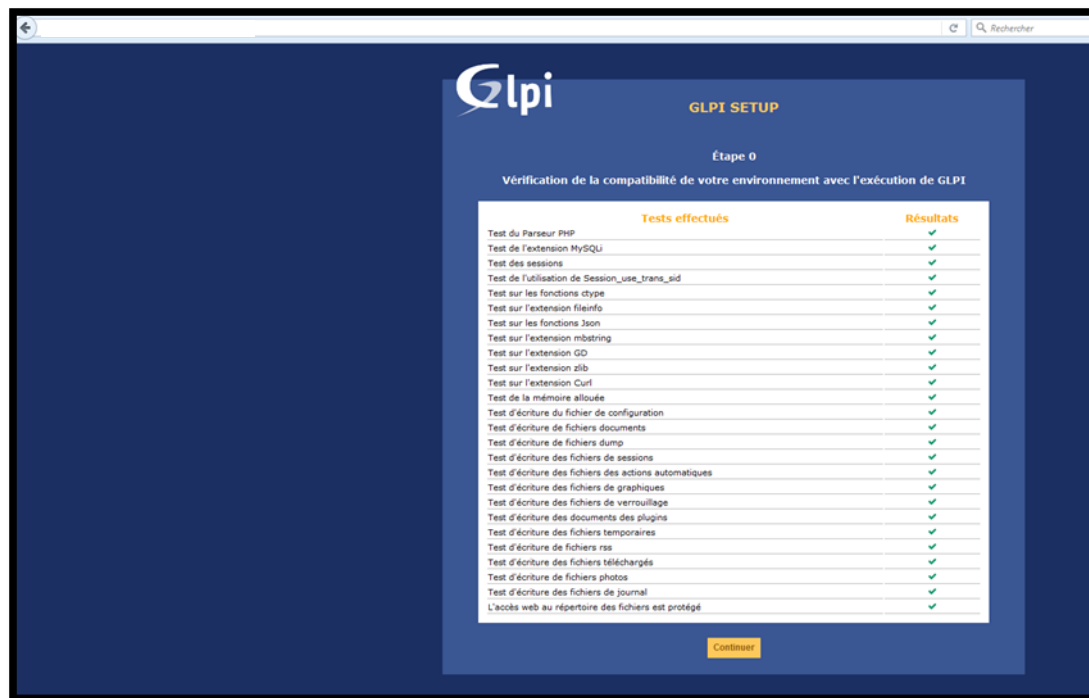
```
http://adresse_IP_de_votre_serveur/glpi
```



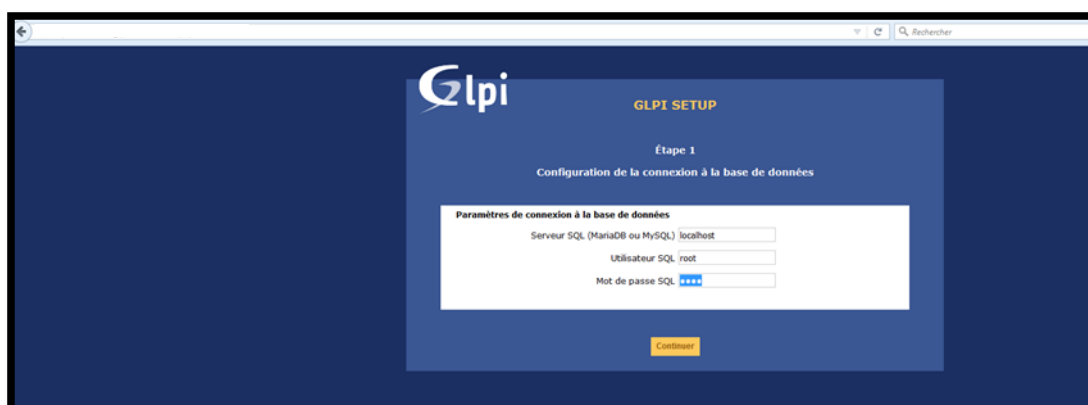
Choisir le langage de GLPI : ici, « Français ».



J'ai lu et ACCEPTE les termes de la licences...



GLPI vérifie si votre environnement est bien compatible. Si les résultats sont corrects alors, cliquer sur « Continuer ».



GLPI a besoin, maintenant, de plusieurs informations afin de créer sa base de données.

- Votre serveur SQL est hébergé en local sur votre serveur Linux Ubuntu alors entrer : « **localhost** »
 - L'utilisateur de votre base de données SQL, par défaut, est : « **root** »
 - Le mot de passe SQL est celui que vous avez rentré à l'installation du service MYSQL : (cf page 4)
- Une fois ces informations rentrées, cliquer sur **Continuer**



Entrer maintenant le nom de la base de données que GLPI doit créer : « **glpi** », puis cliquer sur Continuer. (Si l'installation bloque ou s'arrête à ce niveau, il faut recommencer la procédure.)

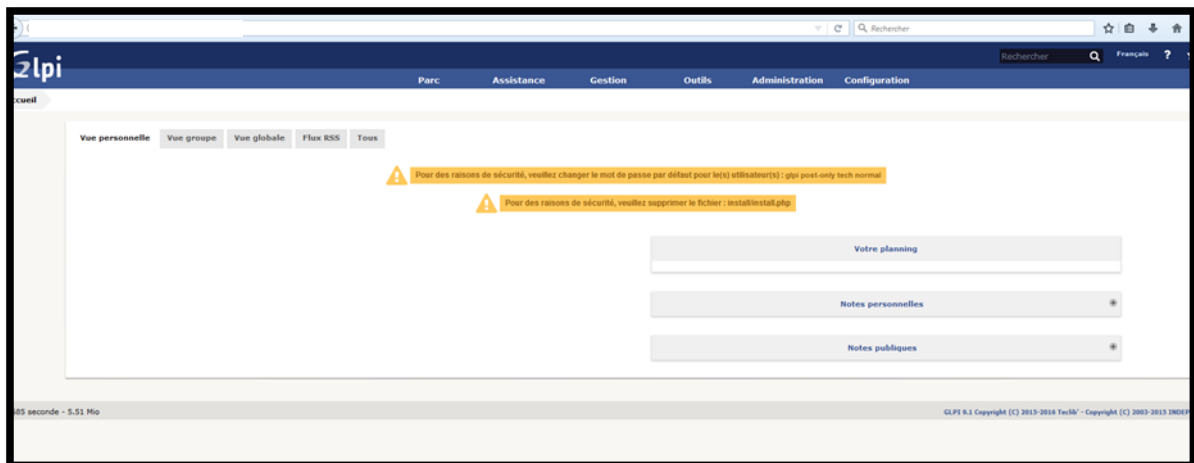
A la fin de l'installation, GLPI vous donne les identifiants et mot de passe des différents utilisateurs créés par défaut.

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

Pour des raisons de sécurité évidente, le mot de passe administrateur sera à changer.



Cliquer sur « **Utiliser GLPI** » afin de vérifier le bon fonctionnement de l'accès à GLPI (interface ci-dessous).



11 / Ubuntu Server 16.04 : installation du plugin FUSIONINVENTORY (version 9.1+1.0)

FusionInventory est un logiciel servant à l'inventaire et la maintenance d'un parc informatique à l'aide d'autres logiciels de ce type telles que GLPI ou OCS Inventory.

Il permet notamment d'effectuer :

- l'inventaire matériel & logiciel (avec agents ou sans agent en utilisant le SNMP) ;
- le Wake-on-lan ;
- le déploiement de logiciels ;
- la découverte du matériel réseau connecté (utilisant Netbios, Nmap et SNMP).



Télécharger la version 9.1+1.0 du plugin FusionInventory sur le site de l'éditeur du logiciel

Placer le fichier téléchargé dans le répertoire PLUGINS sous GLPI : (/opt/glpi/plugins)

Décompresser le fichier téléchargé (à l'aide de WinScp par exemple, en cliquant droit sur le fichier / Commandes manuelles / untar/GZIP)

Attention : les fichiers décompressés du plugin fusioninventory doivent se trouver dans un répertoire fusioninventory (exemple ci-dessous)

/opt/glpi/plugins/fusioninventory/

Modification du fichier SETUP.PHP du Plugin Fusioninventory

Il est nécessaire, pour des raisons de compatibilités avec GLPI, de modifier le fichier SETUP.PHP du plugin FusionInventory.

Cette modification peut se faire directement avec l'éditeur VIM ou via WinSCP

Nom	Taille	Date de modification	Droits
..		03/03/2017 15:09:38	rw-rw-r--x
scripts		03/03/2017 15:09:42	rw-rw-r--x
report		03/03/2017 15:09:42	rw-rw-r--x
pics		03/03/2017 15:09:42	rw-rw-r--x
locales		03/03/2017 15:09:42	rw-rw-r--x
lib		03/03/2017 15:09:41	rw-rw-r--x
js		03/03/2017 15:09:38	rw-rw-r--x
install		03/03/2017 15:09:38	rw-rw-r--x
inc		03/03/2017 15:09:38	rw-rw-r--x
front		03/03/2017 15:09:38	rw-rw-r--x
docs		03/03/2017 15:09:38	rw-rw-r--x
css		03/03/2017 15:09:38	rw-rw-r--x
b		03/03/2017 15:09:38	rw-rw-r--x
ajax		03/03/2017 15:09:38	rw-rw-r--x
setup.php	25 KB	19/12/2016 16:20:10	rw-rw-r--
README.asciidoc	2 KB	19/12/2016 16:19:08	rw-rw-r--
prototype.js	160 KB	19/12/2016 16:19:10	rw-rw-r--
PICTURES	1 KB	19/12/2016 16:19:08	rw-rw-r--
LICENSE	34 KB	19/12/2016 16:19:08	rw-rw-r--
index.php	3 KB	19/12/2016 16:19:08	rw-rw-r--
hook.php	101 KB	19/12/2016 16:19:08	rw-rw-r--
effects.js	38 KB	19/12/2016 16:19:08	rw-rw-r--

Il faut, pour effectuer la modification de compatibilité, rechercher la chaîne de caractères **GLPI_VERSION** et **modifier sa valeur**

Valeur de modification : 0.85 (cf ci-dessous)

Une fois la modification effectuée, **enregistrer le fichier SETUP.PHP**

```
/**
 * Manage / check the prerequisites of the plugin
 *
 * @global object $DB
 * @return boolean
 */
function plugin_fusioninventory_check_prerequisites() {
    global $DB;

    if (!isset($_SESSION['glpi_plugins'])) {
        $_SESSION['glpi_plugins'] = array();
    }

    if (version_compare(GLPI_VERSION, '0.85', 'lt') || version_compare(GLPI_VERSION, '9.2', 'ge')) {
        echo __('Your GLPI version not compatible, require >= 9.1.1 and < 9.2', 'fusioninventory');
        return FALSE;
    }

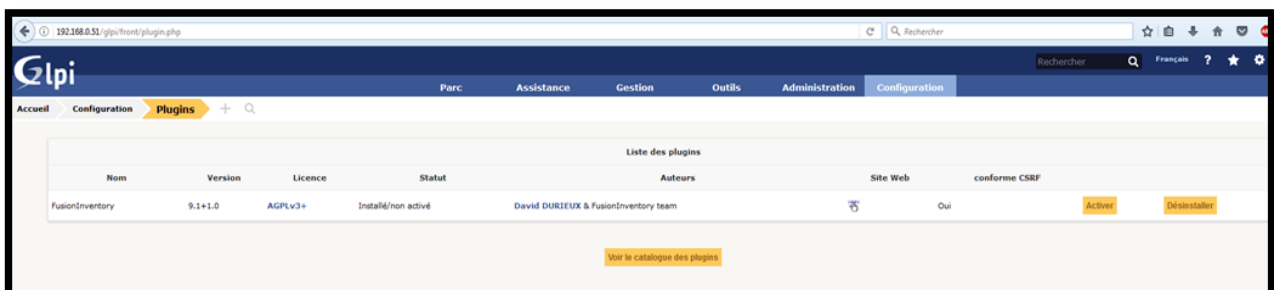
    if (!function_exists('finfo_open')) {
        echo __('fileinfo extension (PHP) is required...', 'fusioninventory');
        return FALSE;
    }

    $plugin = new Plugin();
    if ($plugin->isActivated("fusioninventory")
        && !TableExists("glpi_plugin_fusioninventory_configs")) {
        return FALSE;
    }
}
```

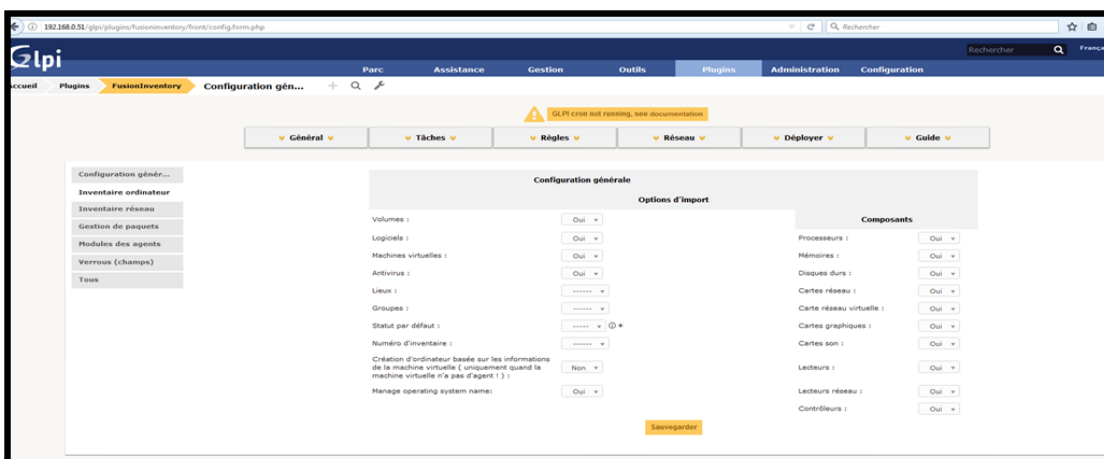
Etape d'activation du plugin FusionInventory

Se rendre sous le menu **Plugins**. Il faut :

- Installer le plugin en cliquant sur **INSTALLER**
- Activer le plugin en cliquant ensuite sur **ACTIVER**



Cliquer sur le plugin et vérifier si les paramètres sont bien sur « oui » comme ci :



Puis dans l'onglet « **Administration** » puis « **Entités** » et « **root entity** »

Ajouter le lien d'url d'accès : «**http://adresse_ip_de_votre_serveur/gipi** »

The screenshot shows the GLPI administration interface. The top navigation bar includes 'Accueil', 'Administration', and 'Entités'. The 'Entités' tab is selected. The main content area is titled 'Entité - Root entity' and shows a form for configuring the root entity. The form includes a dropdown menu for 'Modèle pour le transfert automatique d'ordinateurs dans une autre entité' (currently set to 'Pas de transfert automatique') and a text input field for 'URL d'accès au service (U)' containing the value 'http://192.168.0.51/gipi'. The 'URL d'accès au service (U)' field is highlighted with a red circle. There are 'Sauvegarder' and 'Supprimer définitivement' buttons at the bottom right of the form. A sidebar on the left lists various administration options: Entité, Entités, Adresse, Informations avancées, Notifications, Assistance, Parc, Utilisateurs (5), Règles (1), and Documents.