GLPI: Installation sur Debian 10

Installation de GLPI

1. Installer les paquets nécessaires

```
apt update
apt dist-upgrade
apt-get install nginx mariadb-server php-fpm php-mysql php-curl php-
intl php-zip php-bz2 \
php-ldap php-gd php-imap php-mbstring php-xml php-xmlrpc php-apcu php-
cas
```

2. Sécuriser mariadb

```
mysql_secure_installation
```

3. Télécharger & décompresser le package

```
wget -qO- https://github.com/glpi-
project/glpi/releases/download/9.5.3/glpi-9.5.3.tgz | tar xvzf -
```

4. Copier les fichiers téléchargés dans /var/www

```
cp -r glpi /var/www
```

5. Editer le fichier /etc/nginx/sites-enabled/default

```
nano /etc/nginx/sites-enabled/default
```

default

```
server {
        listen 80 default_server;
        listen [::]:80 default_server;
        root /var/www/;
        index index.php index.html index.htm index.nginx-
debian.html;

        server_name _;
        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a
404.
                try_files $uri $uri/ =404;
        }

        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
```

```
                fastcgi_pass unix:/run/php/php7.3-fpm.sock;
                fastcgi_param SERVER_NAME $host;
        }

        location /glpi/files/ {
                deny all;
                return 404;
       }

}
```

6. Protéger PHP d'une potentielle faille

```
sed -i 's/;cgi.fix_pathinfo=1/cgi.fix_pathinfo=0/g'
/etc/php/7.3/fpm/php.ini
```

7. Redémarrer Nginx

```
service nginx restart
```

8. Configurer un utilisateur Mysql pour Glpi

```
mysql -u root -p
```

```
CREATE DATABASE glpi;
CREATE USER glpi@localhost IDENTIFIED BY "**motdepasse**";
GRANT ALL PRIVILEGES ON glpi.* TO glpi@localhost;
flush privileges;
quit
```

9. Changer le propriétaire du dossier

```
chown -R www-data:www-data /var/www/glpi/
```

10. Visiter la page de GLPI pour configurer via l'interface Web http://ip/glpi

11. Configurer un cron pour les tâches

```
crontab -e
```

et coller la ligne suivante

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

12. Editer le fichier php.ini dans le répertoire /etc/php/7.3/**cli**

```
nano /etc/php/7.3/cli/php.ini
```

et adapter cette ligne pour y indiquer votre timezone

```
date.timezone = Europe/Brussels
```

Vous pouvez aussi l'adapter pour autoriser l'upload de fichiers volumineux

```
upload_max_filesize = 500M
post_max_size = 500M
memory_limit = 500M
default_socket_timeout = 6000
```

13. Editer le fichier php.ini dans le répertoire /etc/php/7.3/fpm

```
nano /etc/php/7.3/fpm/php.ini
```

et adapter cette ligne pour y indiquer votre timezone

```
date.timezone = Europe/Brussels
```

Vous pouvez aussi l'adapter pour autoriser l'upload de fichiers volumineux

```
upload_max_filesize = 500M
post_max_size = 500M
memory_limit = 500M
default_socket_timeout = 6000
```

Installation de FusionInventory

1. Télécharger le plug-in pour GLPI

```
wget https://github.com/fusioninventory/fusioninventory-for-glpi/releases/download/glpi9.5.0%2B1.0/fusioninventory-9.5.0+1.0.tar.bz2
```

2. Décompresser l'archive

```
tar xvfj fusioninventory-9*
```

3. Copier les fichiers dans le bon répertoire

```
cp -r fusioninventory /var/www/glpi/plugins/
```

4. Changer le propriétaire des fichiers

```
chown -R www-data:www-data /var/www/glpi/
```

5. Dans GLPI, installer puis activer le plugin FusionInventory

Intégration au serveur LDAP/Active Directory

1. Installer les packages nécessaires

```
apt-get install php-ldap ldap-utils
```

2. Copier le certificat du serveur LDAP dans le répertoire /usr/local/share/ca-certificates

```
cp server-ad.crt /usr/local/share/ca-certificates
```

3. Mettre à jour la database des certificats

```
update-ca-certificates
```

4. Vérifiez si vous savez vous connecter sur le serveur LDAP distant

```
#Si je veux vérifier localement un certificat sur base des CA présents dans /etc/ssl/certs
#openssl verify -CApath /etc/ssl/certs sambaCert.pem
openssl s_client -showcerts -connect srv-ad.makeitsimple.lan:636
```

La réponse devrait être : ***Verify return code: 0 (ok)***

5. Editer le fichier ldap.conf

```
nano /etc/ldap/ldap.conf
```

Il devrait ressembler à ceci

ldap.conf

```
BASE    dc=makeitsimple.lan
URI     ldaps://srv-ad.makeitsimple.lan

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
```

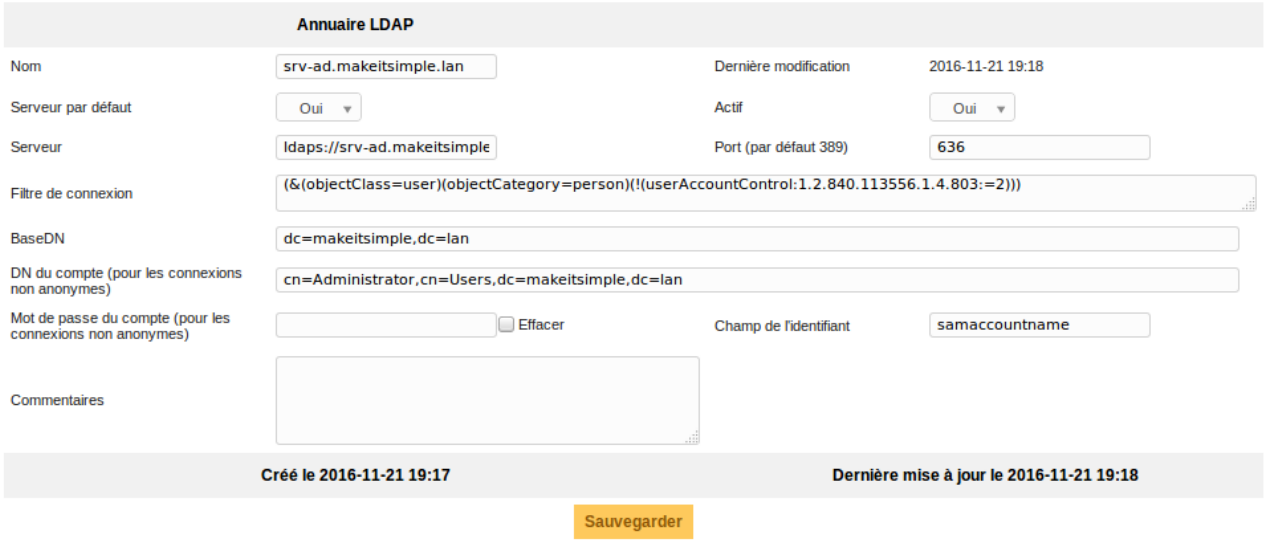
```
TLS_CACERT      /etc/ssl/certs/ca-certificates.crt
```

6. Faire un test de connexion en interrogeant le serveur LDAP

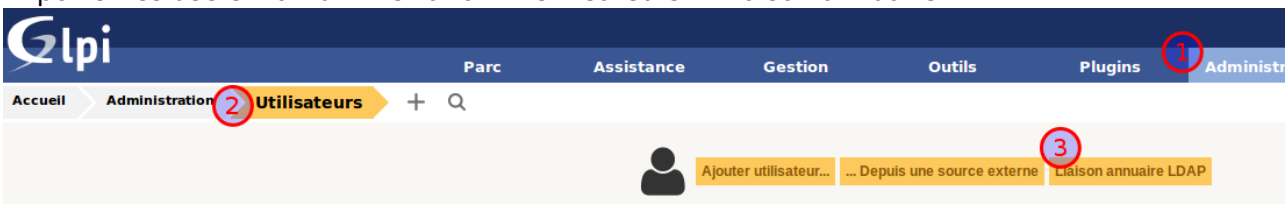
```
ldapsearch -x -d 1 -D
'cn=Administrator,cn=Users,dc=makeitsimple,dc=lan' -W -
b'cn=Users,dc=MAKEITSIMPLE,dc=LAN'
```

7. Dans GLPI Configuration → Authentification → Annuaire Ldap → Cliquer sur le +

8. Voici un exemple de configuration, adapter selon les besoins et tester



9. Importer les users via Administration → Utilisateurs → Liaison annuaire LDAP



Configuration SSL

1. Activer et ssl & désactiver l'accès par défaut

```
a2dissite 000-default.conf
a2enmod ssl
```

2. Créer les certicats nécessaires
3. Editer le fichier /etc/apache2/sites-available/glpi.conf

```
nano /etc/apache2/sites-available/glpi.conf
```

Voici à quoi devrait ressembler le fichier

```
#les 4 premières lignes sont des tests pour intercepter tout ce qui
```

```
n'est pas nommé par DNS
<VirtualHost 10.0.0.214:80>
        ServerName 10.0.0.214/
    DocumentRoot /var/www/glpi
</VirtualHost>

<VirtualHost srv-glpi.makeitsimple.lan:80>
    ServerName srv-glpi.makeitsimple.lan/
    Redirect / https://srv-glpi.makeitsimple.lan/
</VirtualHost>

<VirtualHost srv-glpi.makeitsimple.lan:443>
    ServerName srv-glpi.makeitsimple.lan
    DocumentRoot /var/www/glpi

    SSLEngine on
    SSLCertificateFile /etc/apache2/srv-glpi.crt
    SSLCertificateKeyFile /etc/apache2/srv-glpi.key
</VirtualHost>
```

4. Dans les paramètres généraux de GLPI, changer l'url du serveur pour refléter son FQDN. Sinon le déploiement de paquet ne fonctionnera pas. Dans les paramètres Administration → Entités → Root entity → Fusioninventory

Single Sign On (SSO)

1. Installer les paquets kerberos nécessaire

```
apt-get -y install krb5-user libapache2-mod-auth-kerb
```

2. Editer le fichier krb5.conf

```
nano /etc/krb5.conf
```

Coller une configuration +/- similaire

krb5.conf

```
[libdefaults]
        default_realm = MAKEITSIMPLE.LAN

# The following krb5.conf variables are only for MIT Kerberos.
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true

        fcc-mit-ticketflags = true
```

```
[realms]
MAKEITSIMPLE.LAN = {
        kdc = srv-ad.makeitsimple.lan
        admin_server = srv-ad.makeitsimple.lan
        default_domain = srv-ad.makeitsimple.lan
}

.makeitsimple.lan = MAKEITSIMPLE.LAN
makeitsimple.lan = MAKEITSIMPLE.LAN
```

3. Faire un test de session

```
kinit Administrator
```

4. Se connecter sur le serveur Samba-AD et faire les 3 commandes suivantes en modifiant le nom du serveur

```
samba-tool user create --random-password http-glpi.makeitsimple.lan
samba-tool spn add HTTP/glpi.makeitsimple.lan http-
glpi.makeitsimple.lan
samba-tool domain exportkeytab /root/httpd.keytab --
principal=HTTP/glpi.makeitsimple.lan@MAKEITSIMPLE.LAN
```

5. Vérifier avec la commande kvno

```
kvno HTTP/glpi.makeitsimple.lan@MAKEITSIMPLE.LAN
```

6. De retour sur le serveur GLPI, déplacer le fichier dans le dossier apache et lui donner les bons droits

```
mv httpd.keytab /etc/apache2/
chown www-data:root /etc/apache2/httpd.keytab
chmod 640 /etc/apache2/httpd.keytab
```

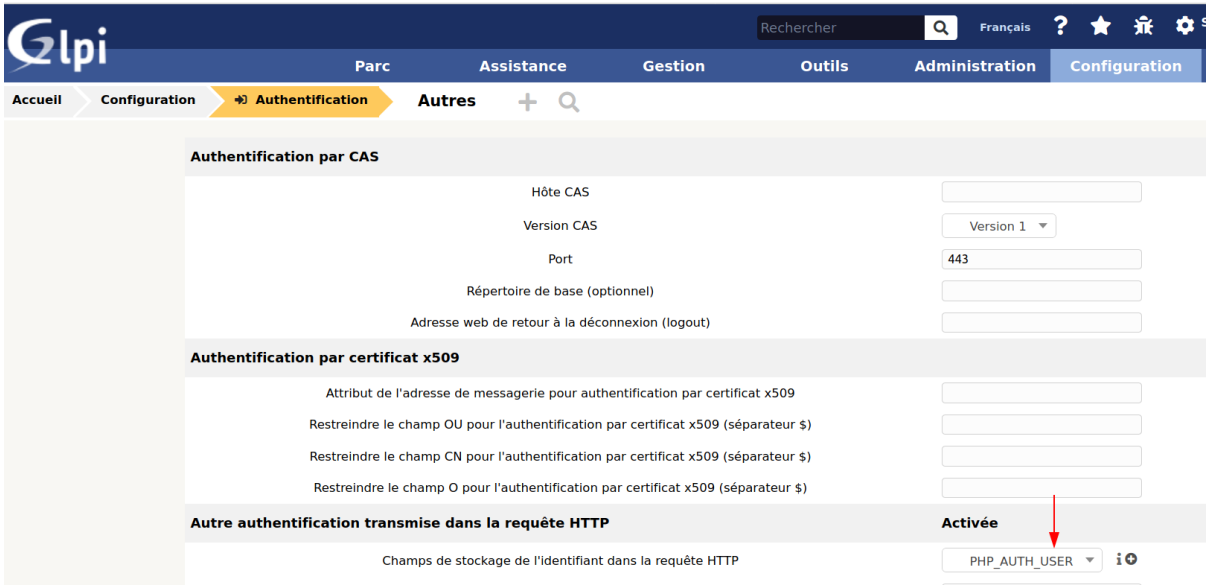
7. Editer le fichier apache

```
nano /etc/apache2/sites-enabled/000-default.conf
```

000-default.conf

```
DocumentRoot /var/www
 Servername glpi.makeitsimple.lan
 <Location />
                AuthType Kerberos
                AuthName "Demande d'identification SSO"
                KrbAuthRealms MAKEITSIMPLE.LAN
                KrbServiceName HTTP/glpi.makeitsimple.lan
                Krb5Keytab /etc/apache2/httpd.keytab
                KrbMethodNegotiate On
                KrbMethodK5Passwd On
                require valid-user
```

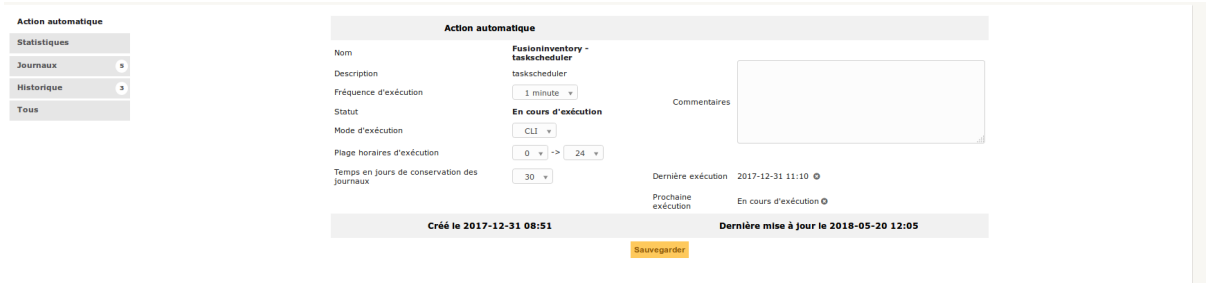
```
        </Location>
```

8. Dans GLPI → Configuration → Authentification → Autre méthode d'authentification
    1. Champs de stockage de l'identifiant : PHP_AUTH_USER
    2. Supprimer le domaine des identifiants : NON
    3. 

9. Le navigateur doit être en mesure d'envoyer les infos Kerberos. Pour IE/edge Chromium, il faut que le site soit reconnu comme Sécurité=intranet et l'intranet renseigné par exemple "*.makeitsimple.lan".

Cron ne veut pas fonctionner

1. Liste numérotéeVérifier que le timezone est bien configuré dans les deux fichiers PHP
2. Voir dans Configuration → Action automatique → Tasksheduler si
    1. Mode éxécution = CLI
    2. Prochaine exécution n'est pas bloqué



Sources

- https://blog.untoldvoyage.com/2012/10/08/sharepoint-sso-ntlm-from-apache-ubuntu/