

15/12/2023

PPE GLPI

F

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE		N° réalisation :
Nom, prénom : Alexis PENET		N° candidat :
Épreuve ponctuelle <input type="checkbox"/>	Contrôle en cours de formation <input checked="" type="checkbox"/>	Date : 15/12/2023
Organisation support de la réalisation professionnelle		
Intitulé de la réalisation professionnelle Mise en place de GLPI et sécurisation du serveur.		
Période de réalisation : 15/11/2023 – 15/12/2023 Lieu : Senlis		
Modalité : <input checked="" type="checkbox"/> Seul(e) <input type="checkbox"/> En équipe		
Compétences travaillées <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Concevoir une solution d'infrastructure réseau <input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau <input checked="" type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau 		
Conditions de réalisation ¹ (ressources fournies, résultats attendus)		
Serveur GLPI Serveur AD/CS Client W10/11 Serveur AD Les résultats attendus du PPE sont : Installation de GLPI Attribution de ticket en automatique Inventaire du parc Réservation de salle Gestion de contrat et fournisseurs Base de connaissance Alerte par mail lors de l'attribution du ticket à un technicien. Https (Rôle AD/CS pour faire signer le ticket) Connexion LDAP entre l'AD et GLPI		
Description des ressources documentaires, matérielles et logicielles utilisées ²		
https://tutos-info.fr/wp-content/uploads/2023/02/TUTORIEL-INSTALLER-GLPI-10.0.6-SUR-DEBIAN-11.pdf https://www.it-connect.fr/generer-une-demande-de-certificat-csr-avec-openssl/ VMware Workstation 17 Windows 10 22h2 Windows 11 23h2 Debian 11 Windows server 2022 Word, bloc note		
Modalités d'accès aux productions ³ et à leur documentation ⁴		
[REDACTED]		

Sommaire	
Introduction	3
Contexte	3
Architecture réseau	4
Pourquoi choisir GLPI ?	5
Installation de GLPI	6
Personnalisation de la page d'accueil GLPI	11
Connexion LDAP	13
DNS	15
Mise en place du HTTPS pour GLPI	17
Agent GLPI	25
Réservation	27
Base de connaissances	30
Gestion de contrats et Fournisseurs	31
Attribution de ticket en automatique	33
Alerte par email lors de la création du ticket	36
Erreurs rencontrés	38
Conclusion	39

Introduction

Cette mission consiste à mettre en place un serveur GLPI sous Debian 11 dans un réseau d'entreprise pour gérer au mieux les demandes des utilisateurs, les contrats, la gestion du parc...

Pour ce faire je vais d'abord installer GLPI 10 puis le configurer.

L'entreprise possède déjà un contrôleur de domaine avec le rôle AD/DC et DNS de configurer, tout ceci est indispensable pour l'installation et la configuration de GLPI.

Contexte

L'entreprise TechVolution, à la suite d'un renouvellement de son parc informatique, il l'a été décidé de revoir le serveur GLPI dans son ensemble et d'améliorer l'équipement de ce serveur.

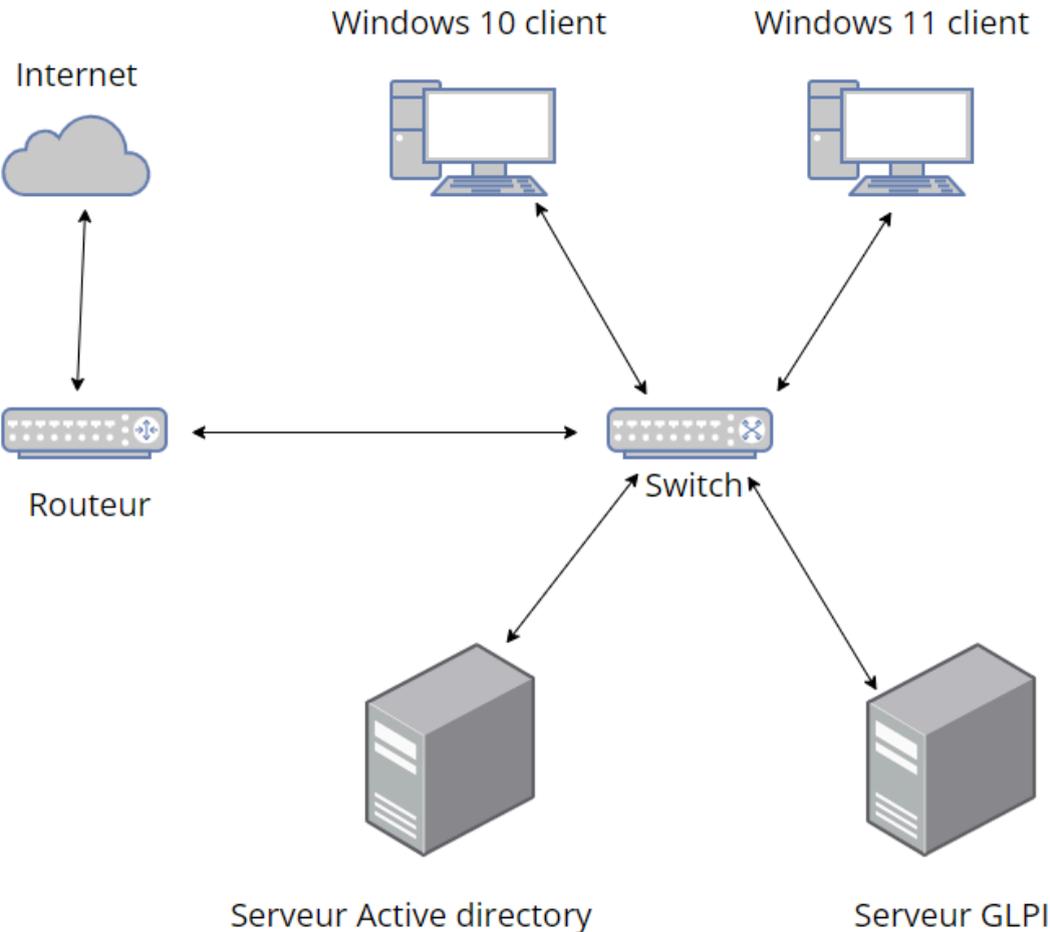
L'intervenant sera un administrateur réseau de l'entreprise TechVolution.

L'entreprise a décidé de mettre en place un serveur GLPI sur une version 10.0.6 afin de pouvoir gérer les demandes des salariés par le biais des tickets, réservations de salle, inventaire du parc, gestion de contrat est fournisseurs.

Les matériels nécessaires avec des modifications qui seront ajoutés pour une utilisation plus optimale :

- Création d'un active directory sous Windows Server 2022 avec un rôle DNS et AD/DC.
- GLPI 10 sous Debian 11.
- GLPI et Active Directory seront reliés par une connexion LDAP.
- Client Windows 10.
- Client Windows 11.
- La connexion au serveur GLPI sera sécurisée grâce au protocole HTTPS.
- La page de connexion de GLPI sera customisé.

Architecture réseau



Pourquoi choisir GLPI ?

GLPI est une application basée sur le web qui nous permet de gérer tout notre système d'information comme de la gestion de licence, inventaire du parc, réservation de salle...

Grâce à toutes ces fonctionnalités GLPI va nous permettre de répondre correctement aux demandes des salariés en fonction de ce qu'ils veulent.

Nous pouvons personnaliser la page d'accueil de GLPI grâce à un plugin que nous allons ajouter.

GLPI nous offre la possibilité de personnaliser les tickets grâce au droit des utilisateurs mais aussi de notifier des administrateurs pour chaque ticket.

GLPI propose la connexion LDAP ce qui nous permettra de mieux gérer les utilisateurs et groupes sur GLPI.

GLPI est une application très complète et gratuite il nous permettra de répondre à toutes nos attentes.

Installation de GLPI

1. Mise à jour des paquets Debian 11

```
apt update  
apt upgrade
```

2. Installation d'Apache2

```
apt install apache2  
apt install ca-certificates apt-transport-https software-properties-common wget curl  
lsb-release -y  
curl -sSL https://packages.sury.org/php/README.txt | bash -x  
apt update  
apt upgrade
```

3. Installation de php 8.2

```
apt install php8.2 libapache2-mod-php8.2  
sudo systemctl restart apache2
```

4. Installation de MariaDB

```
apt install mariadb-server  
mysql_secure_installation ( C'est pour sécuriser mariaDB il vous suffit de suivre les  
étapes )
```

5. Création de la base de données GLPI

```
mysql -u root -p  
(Saisir le mot de passe du root)  
create database glpi ; (création de la base de données)  
create user 'glpi'@'localhost' identified by 'glpi'; (création de l'utilisateur avec mot de  
passe)  
grant all privileges on glpi.* to 'glpi'@'localhost' with grant option; ( on attribue les  
droits utilisateurs)  
flush privileges; (on met à jour les modifications)  
quit
```

6. Téléchargement et décompression de l'archive GLPI

```
wget https://github.com/glpi-project/glpi/releases/download/10.0.6/  
glpi-10.0.6.tgz
```

```
tar xvf glpi-10.0.6.tgz (décompression de l'archive)
mv glpi /var/www/html/glpi (on déplace les fichiers dans un autre dossier)
```

7. Installation de GLPI 10 sur le WEB

Avant de lancer l'installation il faut installer tous les modules PHP :

```
apt install php8.2-curl php8.2-gd php8.2-mbstring php8.2-zip php8.2-xml php8.2-ldap
php8.2-intl php8.2-mysql php8.2-dom php8.2-simplexml php-json php8.2-phdbg
php8.2-cg
```

On donne la propriété à l'administrateur d'apache :

```
chown -R www-data:www-data /var/www/html/glpi/
chmod -R 755 /var/www/html/glpi/
```

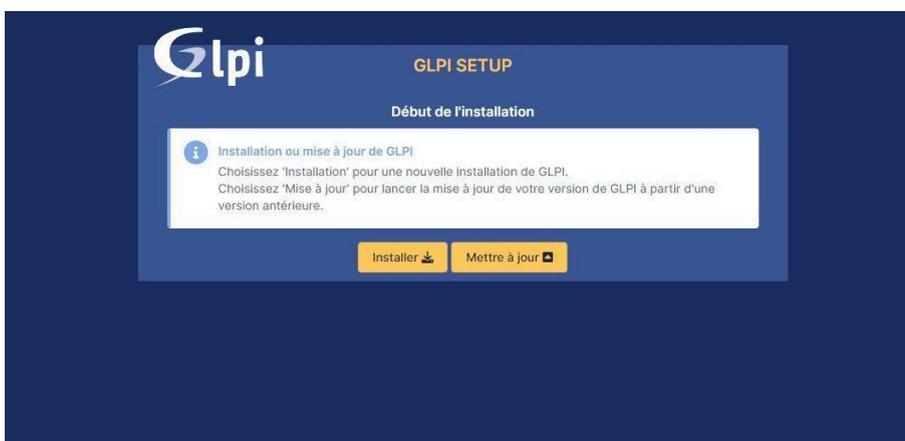
On redémarre le serveur apache :

```
systemctl restart apache2
```

Le serveur sera accessible par <http://ip@server/glpi> ou localhost/glpi.
Nous pouvons sélectionner la langue puis appuyer sur ok.



Il faut accepter les termes du contrat de licence de GLPI.



.On clique sur installer.

On vérifie que tout est en ordre si ce n'est pas le cas au niveau d'un prérequis une erreur sera afficher ce sera à vous de le régler. (Si vous avez suivis toutes les étapes correctement aucune erreur ne s'affichera excepter l'accès protégé l'erreur est normale c'était déjà le cas sous glpi 9)

Puis on clique sur suivant.



GLPI SETUP

Étape 1

Configuration de la connexion à la base de données

Serveur SQL (MariaDB ou MySQL)

localhost

Utilisateur SQL

glpi

Mot de passe SQL

....

Continuer >

On se connecte à la base de données utilisé par GLPI. Le mot de passe est "glpi".



GLPI SETUP

Étape 2

Test de connexion à la base de données

✓ Connexion à la base de données réussie

Veillez sélectionner une base de données :

Créer une nouvelle base ou utiliser une base existante :

glpi

Continuer >

On sélectionne glpi puis on clique sur continuer.



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 "Télémetrie", qui envoie anonymement, avec votre permission, des données à notre site de télémétrie. 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 votre 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](#)

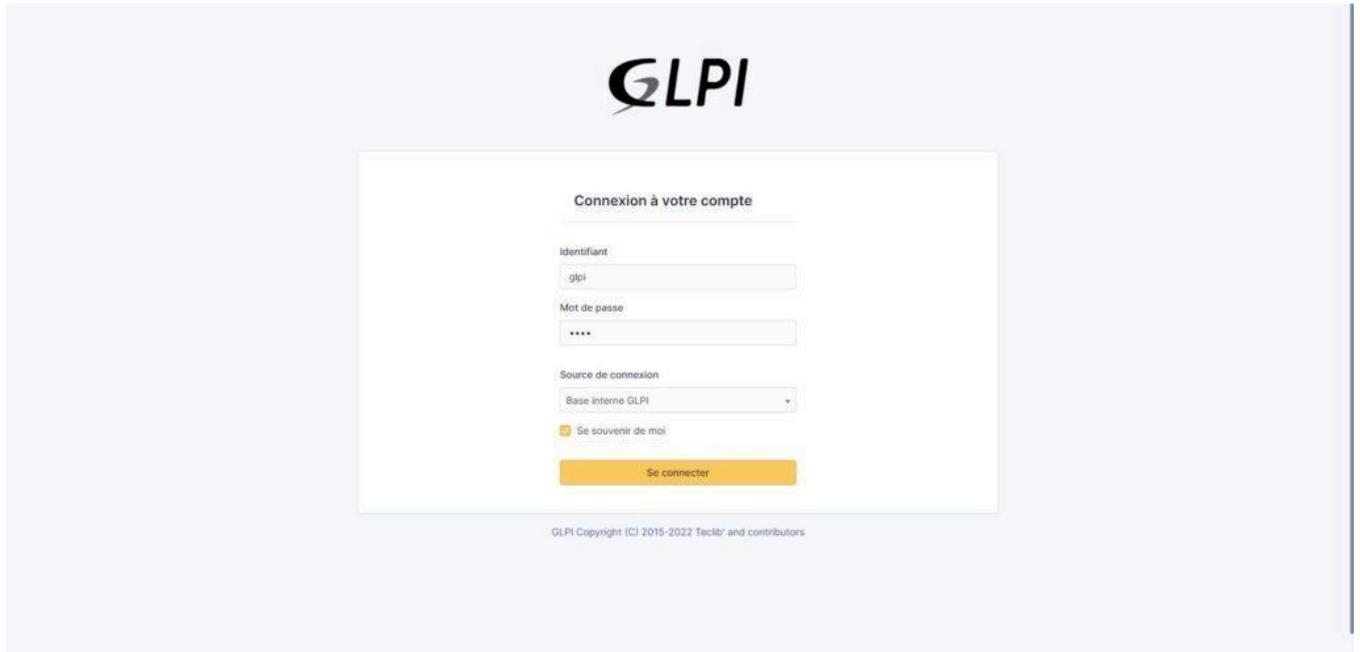
Continuer >

Vous pouvez choisir si oui ou non vous souhaitez envoyer des statiques à GLPI.



L'installation est terminée, il faut cliquer sur continuer pour utiliser GLPI.





La page de connexion de GLPI s'affiche juste en bas il nous suffit de rentrer les informations.

identifiant : glpi

mot de passe : glpi



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

Pour les 2 messages d'erreurs il suffit de changer les mots de passe des différents comptes.
Pour la seconde, il faut aller en ligne de commande en root puis taper cette commande.

su - | rm -f /var/www/html/glpi/install/install.php.

Personnalisation de la page d'accueil GLPI

1 - Nous allons personnaliser la page d'accueil GLPI grâce à un plugin s'appelant custom login. Custom login va nous permettre de pouvoir modifier la couleur, d'ajouter un logo et une image.

Plugin disponible [?](#)

https://github.com/serviceticst/glpi-plugin-custom_login/releases/tag/v1.0.6

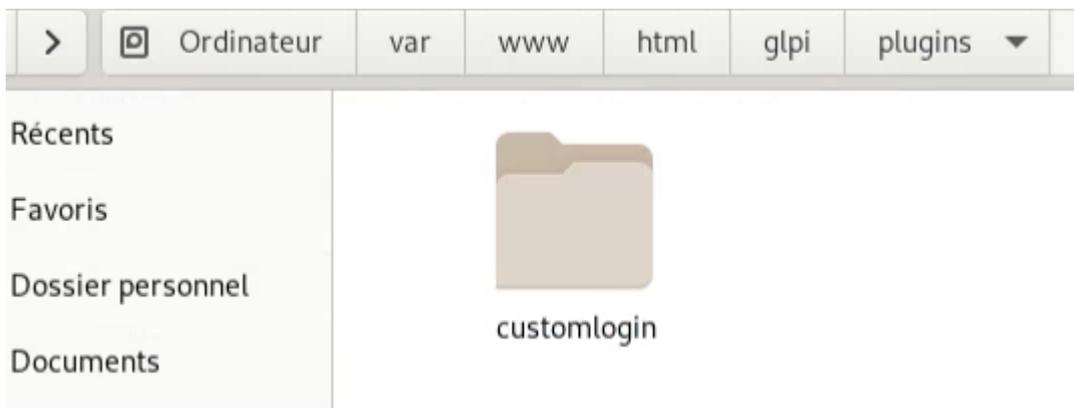
Vous installez le plugin une fois cela fait il apparaîtra dans /home/glpi/
Téléchargements.

Nous ouvrons le terminal, on se rend dans le dossier téléchargements en faisant.

```
" cd /home/glpi/Téléchargement "
```

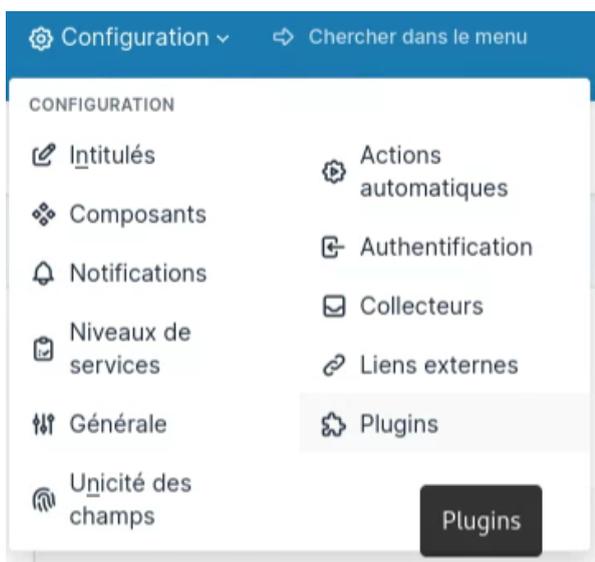
Puis on copie le dossier dans le dossier plugin du glpi.

```
mv customlogin /var/www/html/glpi/plugins.
```



Nous ouvrons le glpi sur le WEB, <http://@ipduserveur/glpi>.

Puis nous allons dans configuration → Plugin.



Filtrer la liste des plugins

CL Custom Login

GLPv3
Service TIC
1.0.4

Configurer

Nous cliquons sur le bouton configurer.

Votre plugin ici ? Contactez-nous. ✉

Nous avons 3 cases ou nous pouvons ajouter des images le premier est pour le logo, le deuxième pour ajouter une image en premier plan est le troisième pour ajouter une couleur.

Personalização

Logo 

Background Front 

Background Bottom 

Fichier(s) (2 Mio maximum) ⓘ
Glissez et déposez votre fichier ici, ou
Parcourir... Aucun fichi...électionné.

Fichier(s) (2 Mio maximum) ⓘ
Glissez et déposez votre fichier ici, ou
Parcourir... Aucun fichi...électionné.

Fichier(s) (2 Mio maximum) ⓘ
Glissez et déposez votre fichier ici, ou
Parcourir... Aucun fichi...électionné.

Salvar



Et voilà le résultat de ma page d'accueil

Connexion LDAP

Le LDAP est un protocole d'authentification pour les services d'annuaire.

Ils stockent des informations telles que :

- Les utilisateurs
- Les caractéristiques de ces utilisateurs
- Le privilège d'appartenance à un groupe
- Et plus encore ...

1. Configuration de la connexion LDAP sur GLPI

Depuis la page d'accueil nous nous rendons sur [Configuration](#) [Authentification](#) [Annuaire LDAP](#) [Ajouter](#)

Nous allons configurer les cases correspondantes :

Nom TECHVOLUTION

Serveur par défaut oui (les deux)

Serveur 192.168.20.10 (@ip du serveur Active directory)

Port 389

Filtre de connexion (&(objectClass=user)(objectCategory=person)(!(userAccountControl :1.2.0840.113556.1.4.803 :=2))) | (dans préconfiguration on clique sur Active directory puis le filtre de connexion s'affiche)

BaseDN DC=tech,DC=lan (pour l'obtenir on va dans les utilisateurs de l'AD et ordinateurs [affichage](#) [fonctionnalité avancer](#) [clic droit](#) sur le nom de domain [propriété](#) [Editeur d'attribut](#) [distinguishedName](#))

Utiliser un compte oui

DN du compte CN=José JM.Monier,CN=Users,DC=tech,DC=LAN (Pour l'obtenir c'est la même manip sauf qu'il faut aller dans le paramètre du compte que l'on veut utiliser et il faut qu'il soit dans le groupe admin du domaine)

Mot de passe du compte on rentre le mdp du compte

Champ de l'identification samaccountname

Champ de synchronisation objectguid

Sauvegarder

TECHVOLUTION	Dernière modification	2023-11-15 15:06
Oui	Actif	Oui
192.168.20.10	Port (par défaut 389)	389
(&(objectClass=user)(objectCategory=person)((userAccountControl:(1.2.840.113556.1.4.803:=2)))		
DC=tech,DC=lan		
Oui		
CN=José JM. Monier,CN=Users,DC=tech,DC=lan		
<input type="text"/>		
<input type="checkbox"/> Effacer	<input type="text"/>	
samaccountname	Commentaires	<input type="text"/>
objectguid	<input type="text"/>	

🗑 Supprimer définitivement
💾 Sauvegarder

On se rend dans tester puis on clique pour tester la connexion entre le GLPI et le serveur AD.

Accueil / Configuration / Authentification / Annuaire LDAP + Ajouter Rechercher

Annuaire LDAP - TECHVOLUTION Actions - 1/1

<ul style="list-style-type: none"> Annuaire LDAP Tester Utilisateurs Groupes Informations avancées Réplicats Historique 2 Tous 	<p>Tester la connexion à l'annuaire LDAP</p> <p style="text-align: center;">Test réussi : Serveur principal TECHVOLUTION</p> <p style="text-align: center;">Tester</p>
---	---

Puis dans utilisateurs → Annuaire LDAP → mode expert, nous pouvons importer tous les utilisateurs de l'AD dans GLPI.

DNS

Le DNS (domain name system) sert à traduire une adresse ip en nom.

Nous allons voir ce qu'est un hôte A et un alias.

Un hôte A va me permettre d'ajouter un nom DNS GLPI.

L'Alias va me permettre d'ajouter un nom DNS que je veux pour la connexion des clients, l'Alias sera utilisé pour les clients.

Au yeux de l'AD l'hôte A va servir un garder un nom logique pour tous les autres hôtes A alors que l'alias va me permettre de mettre un nom comme je le veux pour les utilisateurs de l'entreprise.

Dans mon entreprise TECHVOLUTION la zone direct et indirect est déjà configuré nous allons donc directement voir comment changer l'adresse ip en nom.

Nous ouvrons la barre de recherche pour taper DNS puis dans zone direct ☞ tech.lan on fait un clic droit et on clic sur nouvelle hôte A ou AAA.

Je vais configurer les cases correspondantes :

Nom ☞ supportglpi

Nom de domaine ☞ c'est automatique donc on ne touche pas

Adresse ip ☞ 192.168.20.20 (@ip du serveur glpi)

Nouvel hôte

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

Nom de domaine pleinement qualifié (FQDN) :
supportglpi.tech.lan.

Adresse IP :
192.168.20.20

Créer un pointeur d'enregistrement PTR associé

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

Ajouter un hôte Annuler

A la suite je vais créer un alias pour les clients.

Sur le même chemin je vais faire un clic droit sur ajouter un Alias (CNAME).

Je vais configurer les différentes cases :

Nom [?] glpi

Nom de domaine [?] c'est automatique donc on ne touche pas

Nom de domaine complet [?] Nous cliquons sur parcourir est reliés l'hôte A à l'alias, nous allons donc cliquer sur l'hôte A.

Nouvel hôte

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

supportglpi

Nom de domaine pleinement qualifié (FQDN) :

supportglpi.tech.lan.

Adresse IP :

192.168.20.20

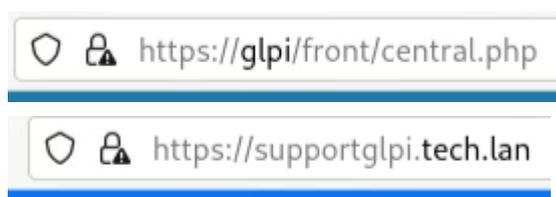
Créer un pointeur d'enregistrement PTR associé

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

Ajouter un hôte Annuler

Nous pouvons voir que l'hôte A et l'alias fonctionne.

En http ce sera <http://glpi/glpi> et <http://supportglpi.tech.lan/glpi> je suis en https donc il s'affiche autrement.



Mon lien est en https car la mise en place du certificat a été fait, c'est ce que nous allons voir dans le prochain sujet.

Mise en place du HTTPS pour GLPI

Le protocole HTTPS (hyper text transfert protocol secure) c'est une extension du protocole http mais grâce a l'https les données entre le navigateur et l'internaute sont chiffrés, ils ne peuvent pas être espionnés par des personnes malveillantes.

Une attaque MitMHTTP permet d'intercepter des communications pour pouvoir le lire le https offrent une option de cryptage ce qui nous permettra de ne pas être lu.

Nous allons voir comment mettre en place un https en interne.

1. Création du certificat sous OpenSSL Debian 11.

Pour commencer, nous allons sur le serveur glpi on ouvre le terminal en root.

```
Su -  
MDP
```

Une fois cela fait on va dans le dossier des certificats GLPI.

```
cd /etc/ssl/certs
```

Cette commande permet de créer la clé et le certificat.

On rentre les informations nécessaires

```
sudo openssl req -sha256 -nodes -newkey rsa:2048 -keyout supportglpi.tech.lan.key -out  
glpi.csr
```

```
root@GLPI:~# sudo openssl req -sha256 -nodes -newkey rsa:2048 -keyout supportglpi.tech.lan.key -out glpi.csr  
Generating a RSA private key  
.....+++++  
...+++++  
writing new private key to 'supportglpi.tech.lan.key'  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [AU]:FR  
State or Province Name (full name) [Some-State]:OISE  
Locality Name (eg, city) []:Senlis  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Tech-Volution  
Organizational Unit Name (eg, section) []:  
Common Name (e.g. server FQDN or YOUR name) []:supportglpi.tech.lan  
Email Address []:
```

Pour le common name il faut rentrer l'hôte A (DNS), quand on clique sur la propriété de l'hôte A on marquera dans common name le nom de domaine pleinement qualifiés.

Après le common name nous ne sommes pas obligé de marquer quelque chose.



Une fois cela fait le Certificat en.CSR et la clé seront télécharger dans le /etc/ssl/certs.
CSR ☒ c'est une demande de signature.

Icon	Filename	Size
	glpi.crt	1,9 ko
	supportglpi.tech.lan.key	1,7 ko

2. Installation du certificat sous Windows Server 2022 avec le rôle ADCS

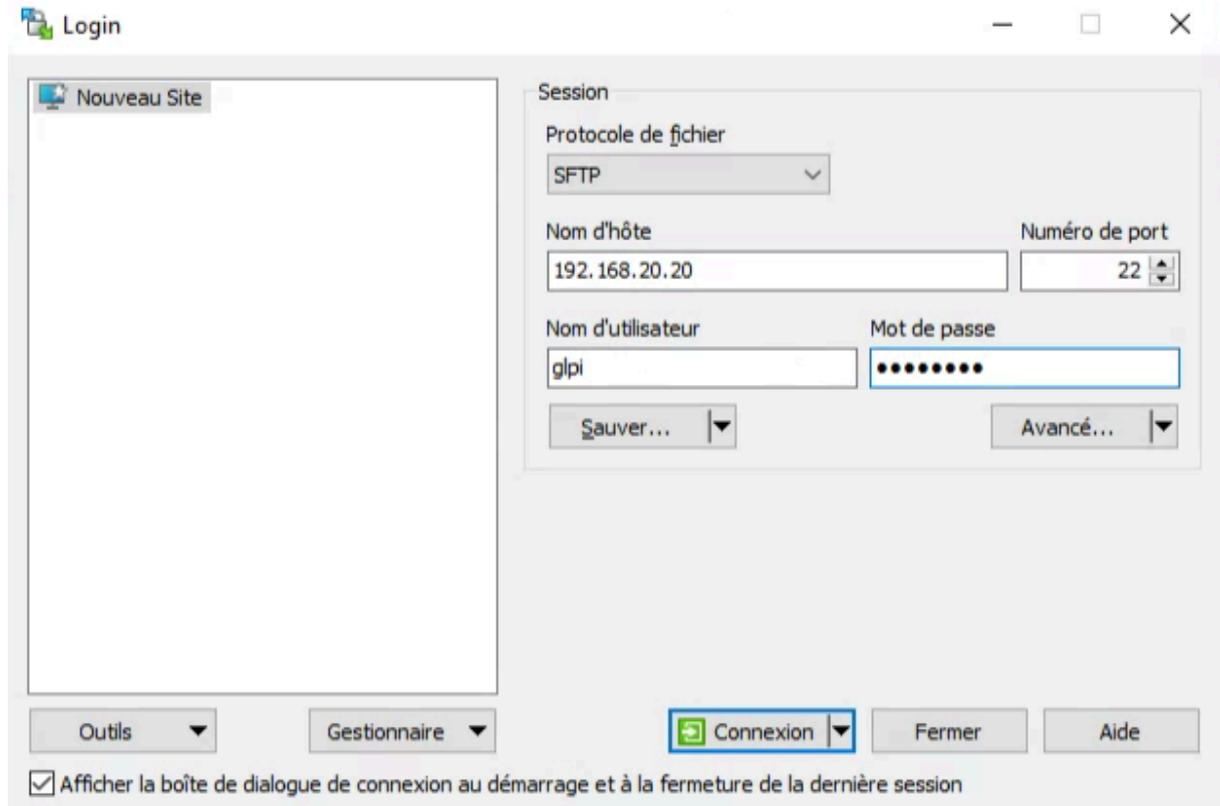
Le rôle ADCS (Active Directory Certificates Services) permet de gérer et de crée des clés et des certificats sur Windows Server dans notre cas l'ADCS nous servira à signer ce certificat et le déployer.

Sur Windows Server il faut aller sur internet et installer WinSCP.

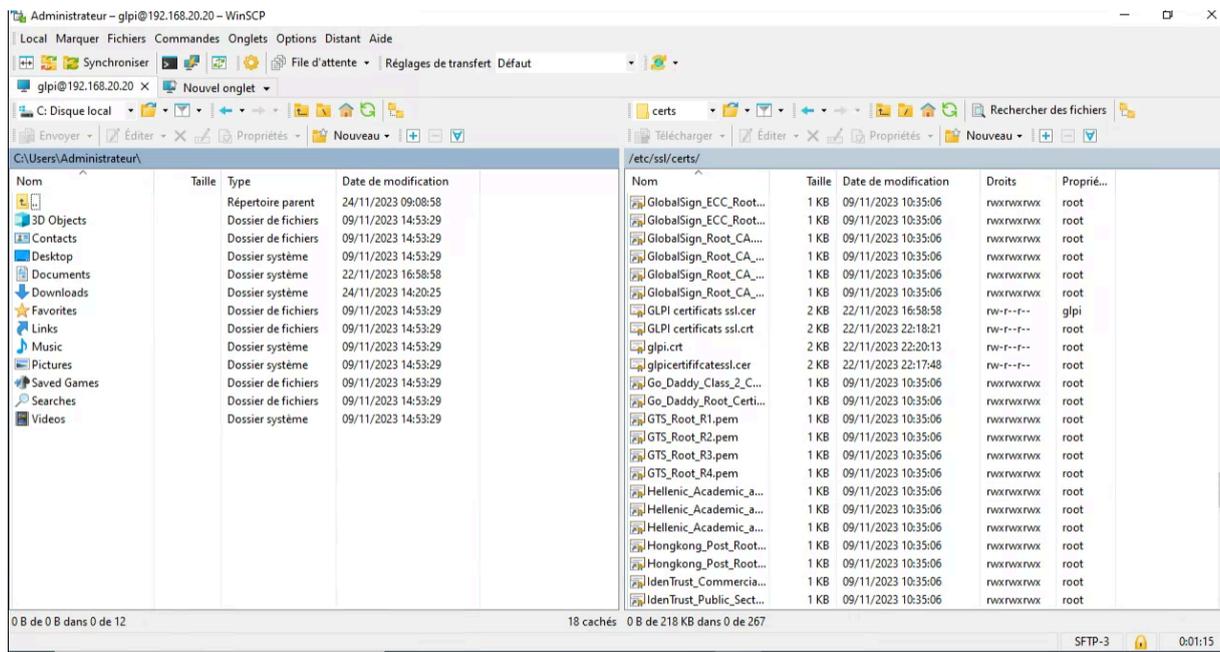
WinSCP va nous servir à transférer le CSR vers le Windows Server.

SFTP offre une connexion sécurisée mais il y'a d'autres possibilités que j'aurais pu prendre comme le FTP qui permet de chiffrer les données de transfert et bien d'autres ...

On rentre l'adresse ip du serveur GLPI le user et le mot de passe.



Une fois faits-nous arrivons sur cette page.



Avec les barres bleues il nous suffit de parcourir les fichiers et de glisser le CSR sur le Windows Server.

Je l'enregistre dans documents.

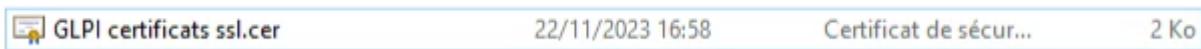
A partir de là je peux fermer WinSCP et ouvrir le cmd en administrateur.

On rentre la commande :

```
C:\Users\Administrateur>certreq -submit -attrib CertificateTemplate:Webserver
```

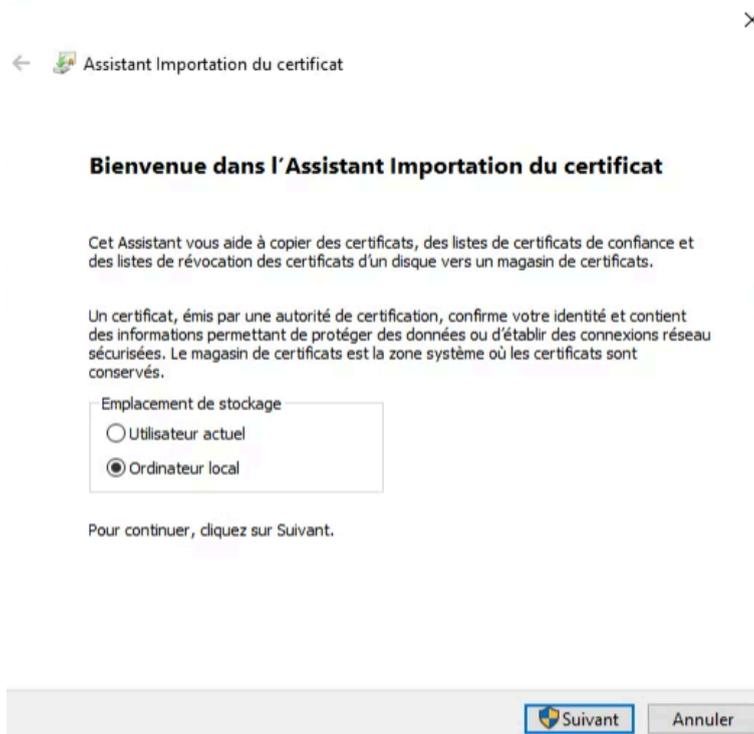
Cette commande va nous permettre d'enregistrer le certificat sous une autre forme dans Windows Server.

Ça ouvre une fenêtre explorateur de fichiers on clique sur le fichier CSR puis on l'enregistre sous un autre nom ce qui donne :

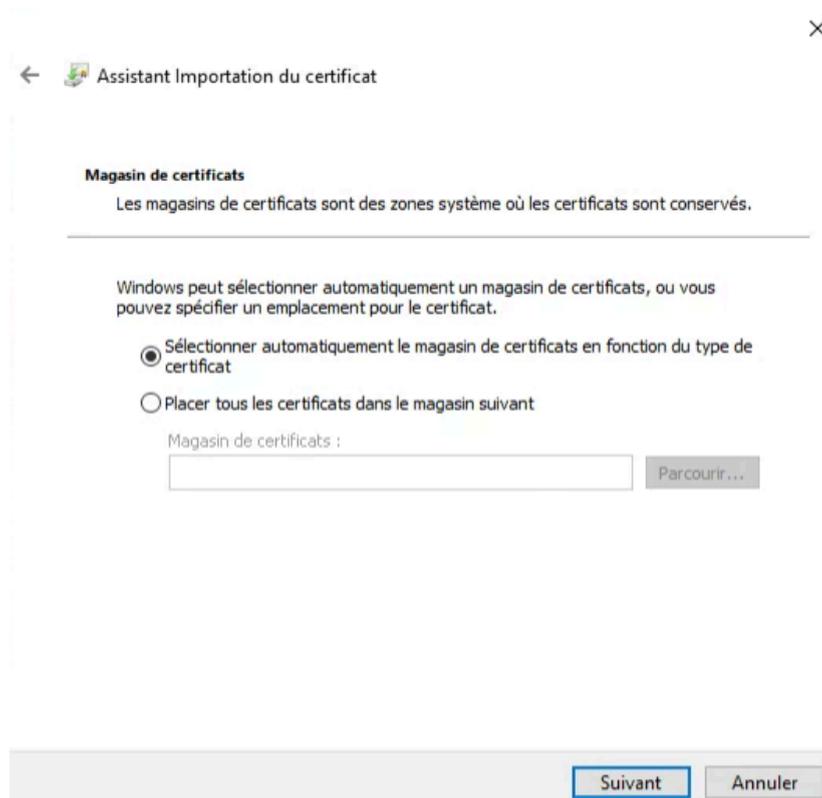


Nous pouvons double cliquer sur le certificat pour l'installer.

Puis on sélectionne ordinateur local.



On sélectionne la première case.



Une fois fait on clique sur terminer puis on fait un `w + r` puis on écrit `mmc`, on sélectionne autorité de certificat et certificat qu'on ajoute en ordinateur local.

Nous pouvons voir que le certificat a bien été ajouté dans autorité de certification de racine de confiance et dans modèle de certificat.

Ensuite on utilise WinSCP pour transférer le CER dans les documents de Debian.

Cer est un fichier de sécurité généré par une autorité de certifications (ADCS)

Puis on copie le fichier vers le dossier `/etc/ssl/certs`.

```
cd /home/gipi/Documents
```

```
mv le nom du certificat /etc/ssl/certs
```

Il faut changer l'extension du CER en CRT car l'extension (CER) n'est pas pris en charge par Debian.

Pour taper la commande on reste dans le dossier où se trouve le CER.

Cette commande sert à changer l'extension du certificat.

```
openssl x509 -inform DER -in chemin/vers/votre_certificat.cer -out  
chemin/vers/votre_certificat.crt
```

La commande va servir a vérifier que le certificat est bien fonctionnel.

```
openssl x509 -in chemin/vers/votre_certificat.crt -text -noout
```

On active le module SSL et activer le rewrite pour apache2.

```
a2enmod ssl
```

```
a2enmod rewrite
```

```
systemctl restart apache2
```

On va ajouter un servername dans le apache2.conf.

```
cd /etc/apache2
```

```
nano apache2.conf
```

```
supportglpi.tech.lan = Hôte A ( DNS)
```

Le fichier est la configuration principale du serveur web apache, il contient des paramètres globaux qui affectent le fonctionnement général du serveur sur le système comme :

- Réglage de sécurité
- Directive principale de configuration ...

```
GNU nano 5.4 apache2.conf
# This is the main Apache server configuration file. It contains the
# configuration directives that give the server its instructions.
# See http://httpd.apache.org/docs/2.4/ for detailed information about
# the directives and /usr/share/doc/apache2/README.Debian about Debian specific
# hints.
ServerName supportglpi.tech.lan
#
#
# Summary of how the Apache 2 configuration works in Debian:
# The Apache 2 web server configuration in Debian is quite different to
```

Puis nous allons configurer 2 fichiers pour faire fonctionner le https pour GLPI.

```
cd /etc/apache2/sites-available
```

```
nano default-ssl.conf
```

On efface toutes lignes par défaut pour rentrer ces lignes une fois fait on enregistre le document en faisant `ctrl + X` `O`.

```

GNU nano 5.4                                default-ssl.conf
<VirtualHost *:443>
SSLEngine on
SSLCertificateFile /etc/ssl/certs/glpi.crt
SSLCertificateKeyFile /etc/ssl/certs/supportglpi.tech.lan.key
servername supportglpi.tech.lan
DocumentRoot /var/www/html/glpi

<Directory /var/www/html/glpi>

    Options FollowSymLinks
    AllowOverride All

    Require all granted
    RewriteEngine On

    # Redirect all requests to GLPI router, unless file exists.
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteRule ^(.*)$ index.php [QSA,L]
</Directory>
</VirtualHost>

```

On reste dans le dossier puis on tape nano 000-default.conf
Puis on rentre ces lignes.

```

GNU nano 5.4                                000-default.conf
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

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

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

```

On vérifie si les 2 fichiers sont bien activés dans le /etc/apache2/sites-enabled

```

root@GLPI:/etc/apache2# cd sites-enabled/
root@GLPI:/etc/apache2/sites-enabled# ls -l
total 0
lrwxrwxrwx 1 root root 35 23 nov. 11:46 000-default.conf -> ../sites-available/000-default.conf
lrwxrwxrwx 1 root root 35 22 nov. 22:26 default-ssl.conf -> ../sites-available/default-ssl.conf
root@GLPI:/etc/apache2/sites-enabled#

```

Si c'est affiché comme cela c'est que les 2 fichiers sont bien activés.
On redémarre apache2.

systemctl restart apache2

Le HTTPS est fonctionnelle avec l'hôte A et L'alias.



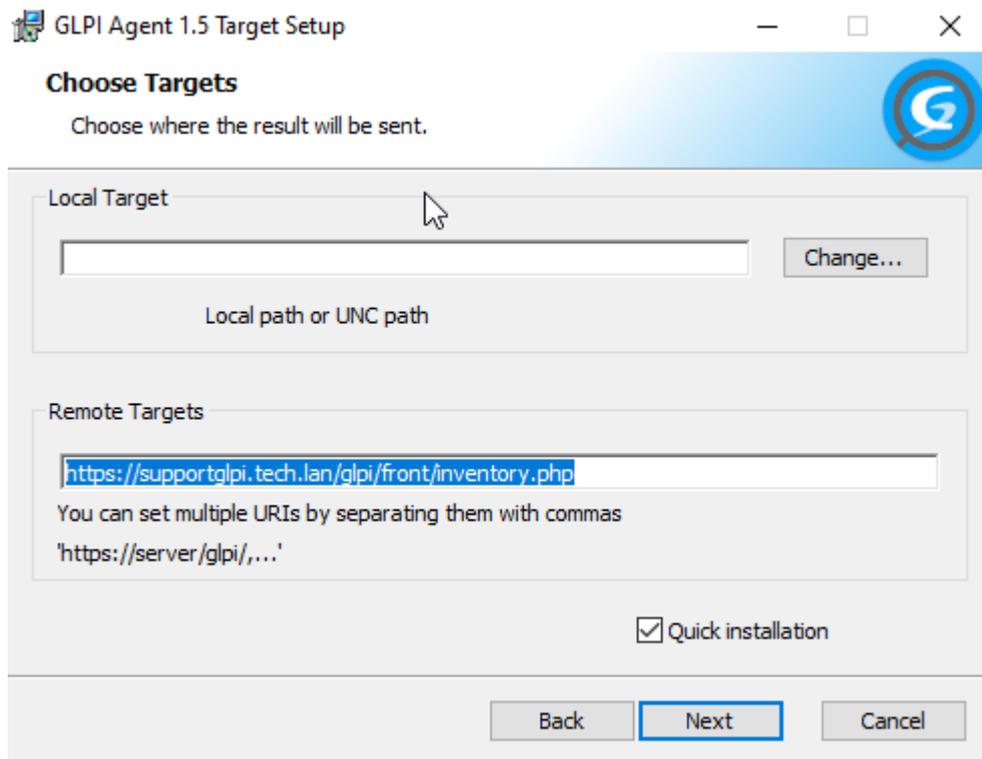
Agent GLPI

L'agent GLPI est un programme utilisé pour exécuter l'inventaire automatique des machines. Il prend en charge l'exécution d'autres tâches telles que le déploiement de packages, la collecte d'information, la découverte et l'inventaire distant ESX et les périphériques réseaux.

Nous allons déployer l'agent sur l'active Directory et les 2 clients Windows.

 GLPI-Agent-1.5-x64 07/11/2023 13:52 Package Windows... 16 233 Ko

On lance l'installation du .exe sur l'ad et les clients.



On rentre le lien GLPI accessible avec l'hôte A.

Après il faut attendre 1h avant que le machines remonte vers le GLPI.

(Mais si on ne veut pas attendre on peut forcer l'agent à remonter les informations.)

Une fois fait les ordinateurs apparaîtront dans le tableau de bord.

Tableau de bord

Vue personnelle

Vue groupe

Vue globale

Flux RSS

Tous

Central ▼ +

187 
Logiciels

3 
Ordinateurs

0 
Matériel réseau

0 
Téléphone

0 
Licence

0 
Moniteur

0 
Baie

0 
Imprimante

Réservation

Nous allons mettre en place des réservations de salle dans GLPI.
Je vais montrer toutes les étapes pour le faire.

Premièrement, nous allons installer un plugin s'appelant gestion d'objet.
La manipulation pour déplacer le plugin dans le dossier et l'activé a été vu précédemment.

On clique sur configuration puis on clique sur ajouter pour créer une catégorie.
Dans identifiant internes je mets le nom << salle >>



Nouvel élément - Types d'objets

Identifiant interne: salle

Libellé: []

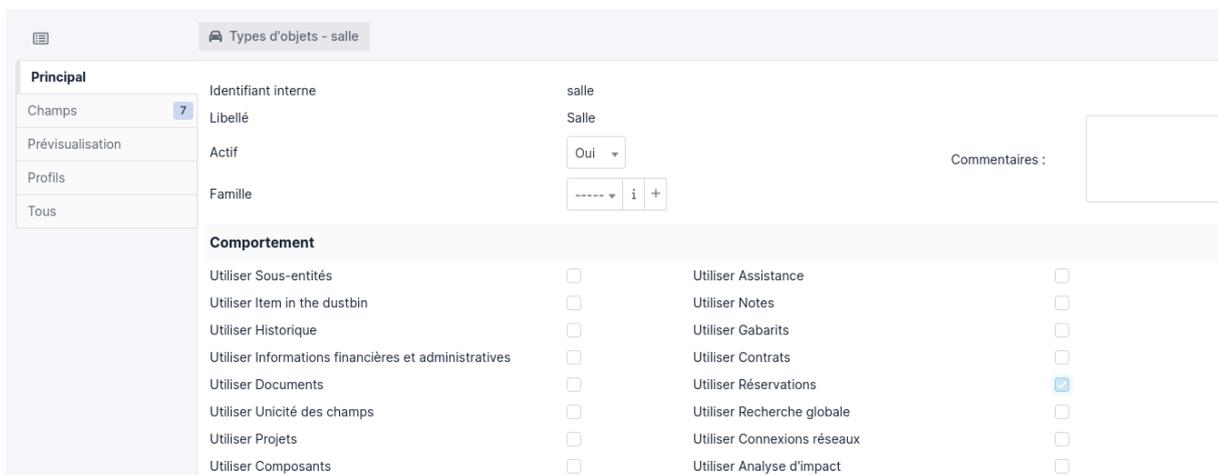
Actif: Non

Famille: [] i +

Commentaires: []

+ Ajouter

On met oui pour le rendre actif et on coche utiliser Réservations.



Types d'objets - salle

Principal

Identifiant interne: salle

Libellé: Salle

Actif: Oui

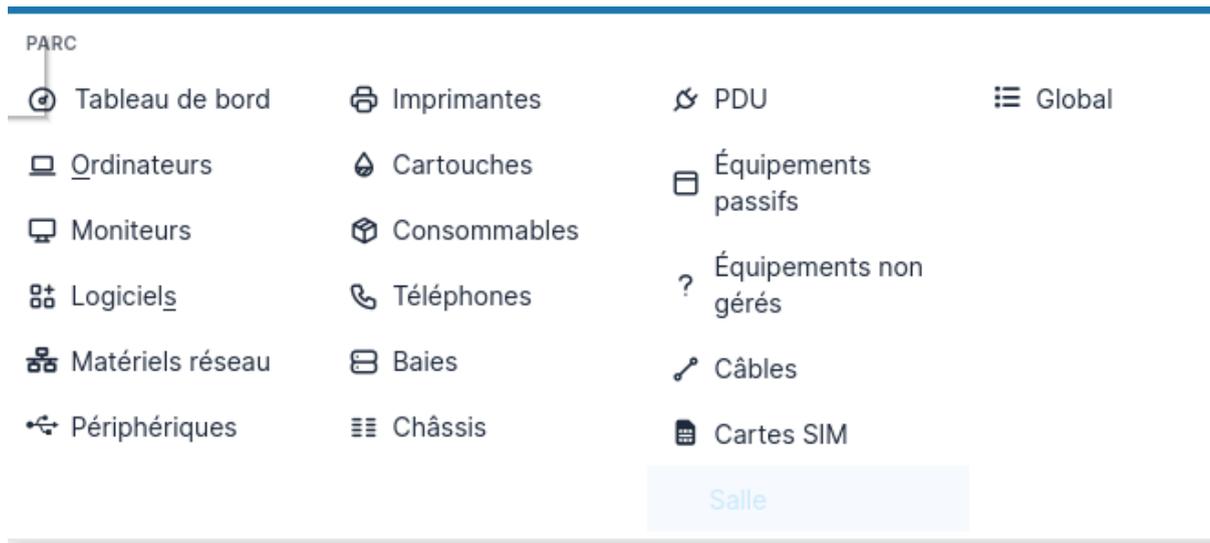
Famille: [] i +

Commentaires: []

Comportement

Utiliser Sous-entités	<input type="checkbox"/>	Utiliser Assistance	<input type="checkbox"/>
Utiliser Item in the dustbin	<input type="checkbox"/>	Utiliser Notes	<input type="checkbox"/>
Utiliser Historique	<input type="checkbox"/>	Utiliser Gabarits	<input type="checkbox"/>
Utiliser Informations financières et administratives	<input type="checkbox"/>	Utiliser Contrats	<input type="checkbox"/>
Utiliser Documents	<input type="checkbox"/>	Utiliser Réservations	<input checked="" type="checkbox"/>
Utiliser Unicité des champs	<input type="checkbox"/>	Utiliser Recherche globale	<input type="checkbox"/>
Utiliser Projets	<input type="checkbox"/>	Utiliser Connexions réseaux	<input type="checkbox"/>
Utiliser Composants	<input type="checkbox"/>	Utiliser Analyse d'impact	<input type="checkbox"/>

Une catégorie a été ajoutés dans l'onglet parc de GLPI on clique sur salle.

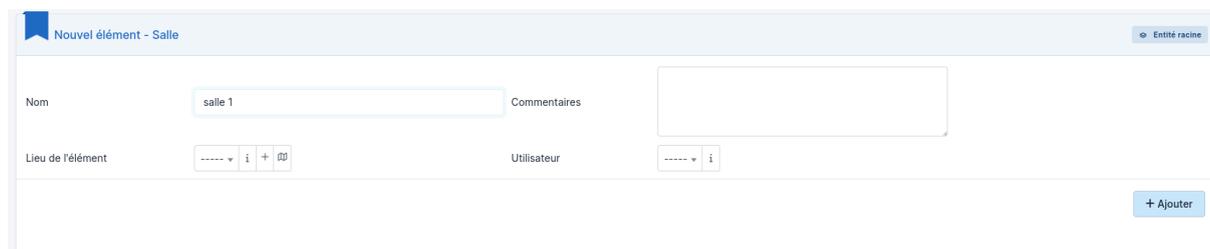


Une fois dedans nous pouvons ajouter des éléments et leurs donnés un nom je vais créer 3 salle.

Salle 1

Salle 2

Salle 3



Puis nous allons dans outils est réservation, nous pouvons voir que c'est 3 éléments sont réservables.

ça fonctionne également sur le planning de la semaine.



Ajouter une réservation ×

Réserver un matériel

Élément Salle ▾
salle 2 ▾

Par glpi ▾ i

Date de début 2023-12-05 00:00:00 📅

Durée 1 jour ▾

Répétition Aucune ▾

Commentaires

réunion comptabilité |

Ajouter

 **Tous les matériels réservables**

décembre 2023

< > Aujourd'hui

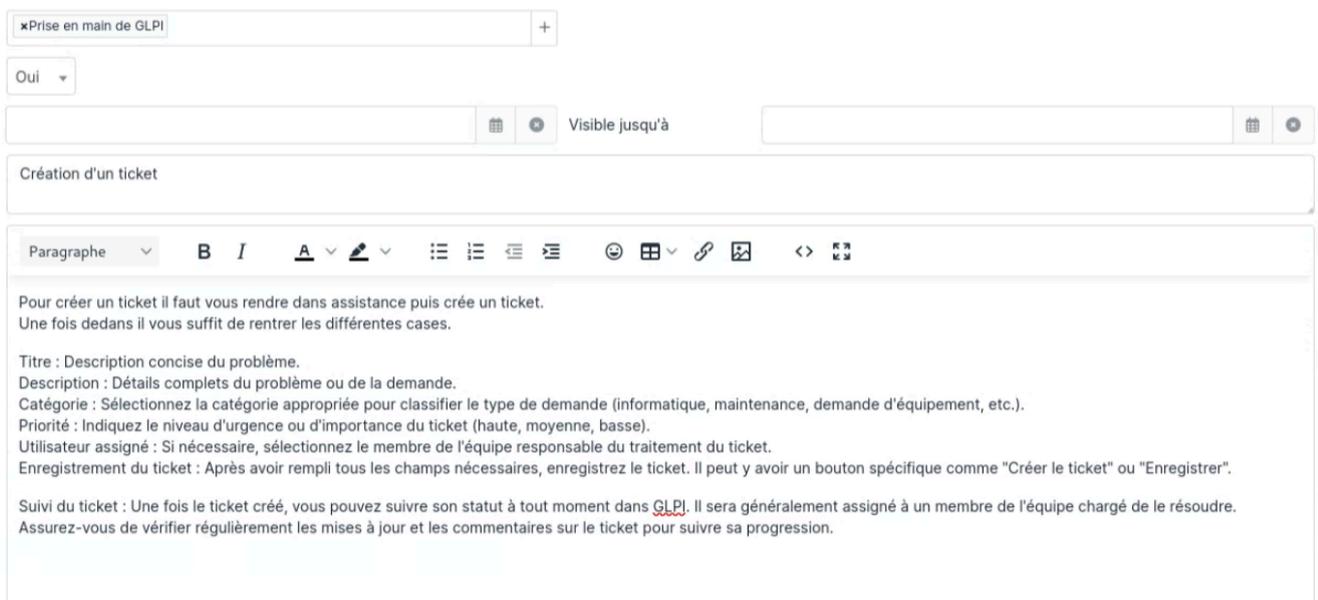
Sem.	lun.	mar.	mer.	jeu.
48	27	28	29	
49	4	5	6	
	16:07 salle 2			
50	11	12	13	

Base de connaissances

Le principe de la base de connaissances est de répertorier les informations dans un même endroit sur plusieurs sujets différents.

Nous allons mettre en place une aide dans la base de connaissances.

Pour commencer nous allons aller dans outils  base de connaissances puis on ajoute un élément a la base de connaissances.



Prise en main de GLPI

Oui

Visible jusqu'à

Création d'un ticket

Paragraphe

B *I* A           

Pour créer un ticket il faut vous rendre dans assistance puis crée un ticket.
Une fois dedans il vous suffit de rentrer les différentes cases.

Titre : Description concise du problème.
Description : Détails complets du problème ou de la demande.
Catégorie : Sélectionnez la catégorie appropriée pour classifier le type de demande (informatique, maintenance, demande d'équipement, etc.).
Priorité : Indiquez le niveau d'urgence ou d'importance du ticket (haute, moyenne, basse).
Utilisateur assigné : Si nécessaire, sélectionnez le membre de l'équipe responsable du traitement du ticket.
Enregistrement du ticket : Après avoir rempli tous les champs nécessaires, enregistrez le ticket. Il peut y avoir un bouton spécifique comme "Créer le ticket" ou "Enregistrer".

Suivi du ticket : Une fois le ticket créé, vous pouvez suivre son statut à tout moment dans [GLPI](#). Il sera généralement assigné à un membre de l'équipe chargé de le résoudre. Assurez-vous de vérifier régulièrement les mises à jour et les commentaires sur le ticket pour suivre sa progression.

Nous pouvons ajouter une catégorie qu'on appellera Prise en main de GLPI.

On donne un titre est une explication puis on clique sur ajouter.

Nous devons mettre oui sur la FAQ pour que les utilisateurs puissent le voir dans la partie FAQ.



La base de connaissance a été créé.

La création d'une cible est d'un élément associé n'est pas obligatoire pour que les utilisateurs puissent voir l'aide.

Gestion de contrats et Fournisseurs

La gestion de contrats et fournisseurs va nous permettre de pouvoir stocker tous les contrats et de pouvoir les gérer grâce aux différentes fonctionnalités qui nous est offert par GLPI 10. Nous allons voir comment mettre tous cela en place.

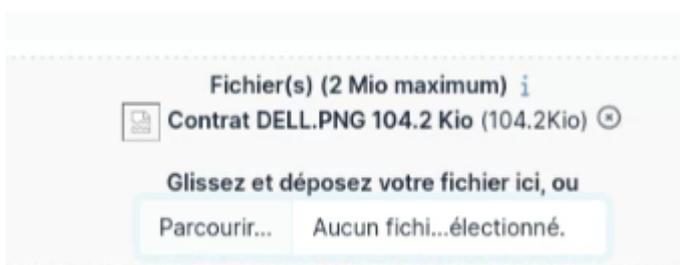
1. Contrat

On va d'abord s'occuper de remplir la partie contrat.

Pour ce faire on se rend dans gestion  contrat puis on clique sur ajouter.

Nous pouvons remplir les cases correspondantes aux nécessités du contrat.

Une fois cela fait on clique sur ajoutés.



Nous avons un menu à gauche de l'écran.

Dans documents on ajoute le contrat correspondant.

Le menu nous offre énormément de possibilités pour la gestion du contrat notamment dans éléments ou nous pouvons ajoutés les ordinateurs concernés par le contrat. (Les ordinateurs que l'agent a remontés).

2. Fournisseurs

Pour configurer la partie fournisseurs on va dans gestion Fournisseurs.

On clique sur ajouter pour rajouter des informations sur les différentes cases.

The image shows a form for adding a supplier. The form is divided into several sections:

- General Information:** Nom (Ordinateur), Matricule, Fax, Courriel (j.dubois@dell.com), Ville (Texas), État (Etats-Unis), Commentaires.
- Contact Information:** Type de tiers, Téléphone (09 25 67 89 02), Site Web (https://www.dell.com/fr-fr), Adresse, Code postal (77573), Pays (Etats-Unis).
- Images:** A section for uploading files, labeled 'Fichier(s) (2 Mio maximum)'. It includes a 'Parcourir...' button and a note 'Aucun fichier déposé'.
- Activation:** A dropdown menu for 'Actif' set to 'Oui'.

To the right of the form is a preview of a contract document titled 'Contrat d'achat de matériel informatique DELL'. The document contains detailed terms and conditions in French, including sections for 'Description', 'Spécifications techniques', 'Marque', 'Modèle', 'Configuration', 'Conditions de paiement', 'Livraison', 'Garantie', and 'Responsabilités'.

Fournisseur
Contacts
Contrats 1
Éléments
Documents
Tickets
Problèmes
Changements
Liens
Notes
Base de connaissances
Historique 2
Tous

Une fois qu'on n'a remplis les cases nous pouvons voir que nous avons accès a tout un panel de gestion sachant que dans contrat nous pouvons ajoutés le contrat que nous avons remplis précédemment.

Également si nous retournons dans contrat nous pouvons ajoutés le fournisseur dans le panel fournisseurs.

D'autres fonctionnalités des différents panels contrat et fournisseurs sont disponibles.

Etant donné leurs facilités d'utilisations et de compréhension je ne m'attarderais pas dessus.

Attribution de ticket en automatique

Le but de l'attribution des tickets en automatique est qu'un technicien soit affecté automatiquement au ticket qu'une personne crée pour cela nous allons voir toutes les étapes pour le mettre en place.

Vous aurez besoin d'un utilisateur sans droit admin et technicien et d'un utilisateur avec des droits de technicien.

Pour ce faire on se rend dans administration [Utilisateurs](#) nous sélectionnons l'utilisateur concerné puis nous pouvons modifier les droits dans habilitations pour les droits technicien ça sera technicien et pour les droits basiques ce sera self-services.

The screenshot shows the 'Ajouter une habilitation à un utilisateur' interface. On the left is a sidebar with navigation items: Utilisateur, Habilitations (1), Groupes (1), Préférences, Éléments utilisés, Éléments gérés, Tickets créés, Problèmes, and Changements. The main area has a title 'Ajouter une habilitation à un utilisateur' and a search bar 'Entité racine'. Below are two rows of configuration options, each with an 'Actions' button. The first row has a checkbox for 'Entités' and a 'Profils (D=Dynamique)' dropdown. The second row has a checkbox for 'Entité racine' and a 'Self-Service (R)' dropdown. A third row has a checkbox for 'Entités' and a 'Profils (D=Dynamique)' dropdown. A dropdown menu is open for the 'Profils (D=Dynamique)' dropdown in the second row, showing options: Self-Service, Observer, Read-Only, Self-Service, Super-Admin, Supervisor, and Technician. The 'Self-Service' option is highlighted.

1. Création d'une règle

Premièrement nous allons dans administrations [règles métiers pour les tickets](#) [ajouter](#).

*

The screenshot shows the 'Ajouter / Mettre à jour' rule configuration page. It has a form with the following fields: 'Support ticket' (text input), 'Description' (text input), 'et' (dropdown menu), 'Actif' (checkbox), and 'Oui' (dropdown menu). Below the form is a 'Ajouter / Mettre à jour' button. At the bottom, there is a 'Dernière mise à jour le 2023-12-05 19:31' timestamp and a 'Tester' button.

Nous configurons cette page comme ceci, les différents ajouts vont nous permettre de pouvoir ajouter du contenu/mettre à jour la règle et de la rendre actif.

Règle	
Critères	1
Actions	1
Historique	21
Tous	

Une fois la règle ajoutée le panel de gauche nous offre la possibilité de configurer la partie critères et action.

La partie critères va centraliser tous les utilisateurs basiques.

La partie action va centraliser les techniciens.

Dans critères nous faisons ajouter un nouveau critère et on clique sur demandeur est on ajoute l'utilisateur avec des droits d'utilisation basique. (Pas de droit technicien et admin)

<input type="checkbox"/> Demandeur	est	nathan
------------------------------------	-----	--------

Dans action nous faisons ajouter une nouvelle action et on clique sur technicien et on ajoute l'utilisateur avec des droits de technicien.

<input type="checkbox"/> Technicien	Assigner	Léo
-------------------------------------	----------	-----

Dans action nous faisons ajouter une nouvelle action et on clique sur technicien et on ajoute l'utilisateur avec des droits de technicien.

2. Création du ticket

Identifiant

Mot de passe [Mot de passe oublié ?](#)

Source de connexion

Se souvenir de moi

Se connecter

On se connecte à l'utilisateur que nous avons placé dans demandeur pour ma part c'est Nathan.

Puis nous allons créer un ticket pour voir si notre réglé.

Si la réglé fonctionne le technicien devrait être attribué sans qu'on coche la case correspondante.

Nous allons dans create a ticket puis nous remplissons les cases comme ceci. Attention la case Watchers ne doit pas être remplis, cette case sert à attribuer manuellement un technicien.

Type Incident

Category ----- i

Urgency Medium

Associated elements +

Watchers

Title test

Description * Paragraph B I ...

test

File(s) (2 Mio max) i

Drag and drop your file here, or

Parcourir... Aucun fichi...électionné.

+ Submit message

REQUESTER - REQUESTER	ASSIGNED TO - TECHNICIAN
nathan	Léo

Nous pouvons voir que les techniciens a bien été attribué automatiquement sur le tickets que je viens de créer.

Pour que l'attribution du ticket automatique fonctionne sur tous les utilisateurs il faut que l'utilisateur apparaissent dans demandeur sinon le ticket ne sera pas attribué par le ou les techniciens.

Alerte par email lors de la création du ticket

Le but de l'alerte par mail est d'envoyer une notification de création pour l'utilisateur qui crée le ticket et pour que le technicien reçoive la notification qu'un nouveau ticket a été créé.

Pour cela nous allons voir comment mettre en place l'alerte par email.

Dans configuration puis notification on active le suivi et les notifications par courriels puis nous allons configurer les notifications par courriels.

Courriel de l'administrateur	alexis.penet@proméo-alternaute.fr
Courriel de l'expéditeur <i>i</i>	alexis.penet@proméo-alternaute.fr
Adresse de réponse <i>i</i>	alexis.penet@proméo-alternaute.fr
Adresse de non réponse <i>i</i>	alexis.penet@proméo-alternaute.fr
Ajouter des documents dans les notifications de ticket	Oui <i>v</i>
Signature des courriels	SIGNATURE
Mode d'envoi des courriels	SMTP+TLS <i>v</i>
Tenter d'envoyer de nouveau dans (minutes)	5 <i>v</i>
Serveur de messagerie	
Vérifier le certificat	Oui <i>v</i>
Hôte SMTP	smtp.office365.com Port
Identifiant SMTP (optionnel)	alexis.penet@proméo-alternaute.fr Mot

Il faudra rentrer le mot de passe de l'adresse mail.

Une fois fait dans configuration Action automatique nous pouvons modifier le temps d'exécution des alertes concernant les notifications mail j'en n'ai modifié 2 s'appelant queuenotification et queuenotificationclean.

Ensuite nous devons configurer un mail au utilisateurs concernés pour qu'il puisse recevoir le mail.

Léo = Technicien

Nathan = demandeur

Nous allons dans administration Utilisateurs, on n'a une liste des utilisateurs je clique sur mon utilisateur léo puis dans le menu de gauche nous avons utilisateurs, nous pouvons configurer un mail sur la partie courriel a droit.

Effacer

Courriels +

Valable jusqu'à

Authentification Base interne GLPI

Catégorie

Nous mettons une adresse mail et une date de validité pour l'adresse. Pour ma part j'ai mis la même adresse pour ne pas créer plusieurs mails.

Maintenant nous allons créer un ticket sur notre demandeur comme vu sur le sujet précédant ensuite nous allons voir si l'alerte fonctionne.



Nous pouvons voir que j'ai reçu un mail pour l'utilisateur Nathan et un mail pour le technicien Léo.

Erreurs rencontrés

Pendant la mise en place du HTTPS une erreur a été rencontrée lors de la configuration du fichier conf default-ssl.conf.

Quand j'ai fait un `apache2ctl configtest` qui signifie un test des configurations d'apache2 il mets une erreur d'alignement.

J'ai changé le placement puis le test a été validé par conséquent j'ai pu avoir accès au glpi en HTTPS.

```
root@GLPI:~# apache2ctl configtest
Syntax OK
root@GLPI:~# █
```

```
GNU nano 5.4 default-ssl.conf
<VirtualHost *:443>
SSLEngine on
SSLCertificateFile /etc/ssl/certs/glpi.crt
SSLCertificateKeyFile /etc/ssl/certs/supportglpi.tech.lan.key
servername supportglpi.tech.lan
DocumentRoot /var/www/html/glpi

<Directory /var/www/html/glpi>

    Options FollowSymlinks
    AllowOverride All

    Require all granted
    RewriteEngine On

    # Redirect all requests to GLPI router, unless file exists.
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteRule ^(.*)$ index.php [QSA,L]
</Directory>
</VirtualHost>
█
```

Conclusion

Pour conclure, j'ai réalisé cette mission sur un Debian 11 contenant GLPI version 10. Ce serveur répondra au mieux aux besoins des employés de l'entreprise TechVolution.

L'entreprise bénéficie d'un service de gestion opérationnel avec une connexion sécurisée en HTTPS.

Des attributions de tickets en automatique avec des alertes par email, un inventaire du parc informatique ainsi que des réservations de salle sont également disponibles sur GLPI.

Ajoutés à cela, une base de connaissance, gestion de contrats et fournisseurs et une page de d'accueil de GLPI ont été configurés.

Pour finir une connexion LDAP entre le GLPI et l'active directory a été mise en place.

Cette infrastructure pourra être améliorée grâce aux autres fonctionnalités que nous offre GLPI.