

Installation GLPI - Brunin Maxime

Contexte:

I. Installation de GLPI

1. Installation des packages nécessaires
2. Configuration base de données
3. Téléchargement de GLPI
4. Configurer le service web
5. Interface Web GLPI

II. Gestion des habilitations

1. Définition des rôles par grade
2. Mise en place des groupes et des rôles

III. Mise en place d'un collecteur de mail

IV. Continuité de service

1. Mise en place d'un HAProxy
2. Modification sur les deux serveurs GLPI
3. Test du HAProxy et des serveurs
4. Mise en place des statistiques
5. Test de continuité de service

V. Conclusion

Contexte:

Dans le cadre du développement du projet **Marieteam**, une solution de gestion des incidents et des demandes d'assistance a été nécessaire afin de centraliser et de structurer le support utilisateur. Après analyse, la solution **GLPI (Gestionnaire libre de parc informatique)** a été retenue pour ses nombreuses fonctionnalités adaptées à ce besoin, notamment la gestion des tickets, l'inventaire matériel et logiciel, ainsi que la personnalisation des droits utilisateurs.

Ce document a pour objectif de détailler les différentes étapes de la mise en place de cette solution au sein de l'infrastructure. Il couvre notamment :

- L'installation de GLPI sur une machine **Debian 12** ;
- La configuration des **droits et habilitations** pour différents profils utilisateurs ;
- La mise en place d'un **collecteur de mails**, permettant la création automatique de tickets à partir d'e-mails entrants ;
- L'intégration d'un **HAProxy** afin de garantir la **haute disponibilité** et la continuité du service.

Cette documentation a été rédigée dans une optique de traçabilité technique et pourra servir de référence pour toute maintenance ou évolution future du système.

I. Installation de GLPI

GLPI (Gestionnaire Libre de Parc Informatique) est une application web open-source dédiée à la gestion des services informatiques (ITSM) et à l'inventaire du matériel et des logiciels. Utilisé par de nombreuses entreprises et administrations, il permet de centraliser la gestion des ressources informatiques, de suivre les incidents, de planifier les interventions et d'optimiser le support aux utilisateurs.

1. Installation des packages nécessaires

On met à jour la machine avec:

```
apt update && apt upgrade -y
```

On va installer les packages pour transformer la machine en serveur LAMP:

```
apt install apache2 php mariadb-server -y
```

Ensuite installer les dépendances pour GLPI:

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

2. Configuration base de données

Pour sécuriser l'accès à la base de données:

```
mysql_secure_installation
```

Ensuite répondre oui aux questions posées et renseignez les informations souhaitées, le mot de passe souhaité pour la base de données:

```

Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!

```

Maintenant faire:

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

Et entrer le mot de passe de l'étape précédente pour se connecter:

```
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 41
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> _
```

Maintenant il faut créer la base de données et ajouter les droits à l'utilisateur admin :

```
create database db_glpi
grant all privileges on db_glpi.* to admindb_glpi@localhost identified by "vo
tre-MDP";
```

Par exemple ci-dessous:

```
MariaDB [(none)]> create database db_glpi;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> grant all privileges on db_glpi .* to admindb_glpi@localhost identified by "toto";
Query OK, 0 rows affected (0,005 sec)

MariaDB [(none)]> exit
Bye
```

Maintenant on peut quitter mariadb:

```
exit
```

3. Téléchargement de GLPI

Il faut exécuter ces lignes de code pour installer la dernière version de GLPI:

```
cd /tmp
wget https://github.com/glpi-project/glpi/releases/download/10.0.14/glpi-1
0.0.14.tgz
```

```

Résolution de github.com (github.com)... 20.26.156.215
Connexion à github.com (github.com)[20.26.156.215]:443... connecté.
requête HTTP transmise, en attente de la réponse... 302 Found
Emplacement : https://objects.githubusercontent.com/github-production-release-asset-2e65be/39182755/2842594b-8b6c-4b62-871d-1c723d61334c?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20240911%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240911T074929Z&X-Amz-Expires=300&X-Amz-Signature=f693755f2d92a570215ff80767a967c859bbd3a193302bddd5eb608c46ae2d848X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=39182755&response-content-disposition=attachment%3B%20filename%3Dglpi-10.0.14.tgz&response-content-type=application%2Foctet-stream [suivant]
--2024-09-11 09:49:29-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/39182755/2842594b-8b6c-4b62-871d-1c723d61334c?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20240911%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240911T074929Z&X-Amz-Expires=300&X-Amz-Signature=f693755f2d92a570215ff80767a967c859bbd3a193302bddd5eb608c46ae2d848X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=39182755&response-content-disposition=attachment%3B%20filename%3Dglpi-10.0.14.tgz&response-content-type=application%2Foctet-stream
Résolution de objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 185.199.111.133, 185.199.109.133, ...
Connexion à objects.githubusercontent.com (objects.githubusercontent.com)[185.199.108.133]:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 59541870 (57M) [application/octet-stream]
Sauvegarde en : « glpi-10.0.14.tgz »

glpi-10.0.14.tgz          100%[=====] 56,78M  44,9MB/s   ds 1,3s
2024-09-11 09:49:30 (44,9 MB/s) - « glpi-10.0.14.tgz » sauvegardé [59541870/59541870]

```

Créer un dossier glpi dans /etc:

```
mkdir /etc/glpi
```

Ensuite créer un fichier local_define.php

```
nano /etc/glpi/local_define.php
```

Ajouter les lignes suivantes dans le document puis sauvegarder le fichier:

```
<?php
define('GLPI_VAR_DIR', '/var/lib/glpi');
define('GLPI_LOG_DIR', '/var/log/glpi');
```

Il faut déplacer le dossier config dans le dossier glpi et gérer l'accès à ce dernier:

```
mv /var/www/html/glpi/config /etc/glpi
chown -R www-data /etc/glpi/
```

Vérifier le contenu du dossier et le propriétaire avec :

```
ls -l /etc/glpi
```

Ceci devrait s'afficher:

```
root@srvlamp:/tmp# ls -l /etc/glpi/
total 8
drwxr-xr-x 2 www-data utilsio 4096 14 mars 13:03 config
-rw-r--r-- 1 www-data root      88 11 sept. 09:57 local_define.php
```

Déplacer le dossier files de glpi:

```
mv /var/www/html/glpi/files /var/lib/glpi
```

Et créer des dossiers de logs pour GLPI:

```
mkdir /var/log/glpi
chown www-data /var/log/glpi
```

Créer un fichier downstream.php:

```
nano /var/www/html/glpi/inc/downstream.php
```

Et ajouter les lignes suivantes puis sauvegarder le fichier:

```
<?php
define('GLPI_CONFIG_DIR', '/etc/glpi/');
if (file_exists(GLPI_CONFIG_DIR . '/local_define.php')) {
    require_once GLPI_CONFIG_DIR . '/local_define.php';
}
```

4. Configurer le service web

Il faut modifier le fichier php.ini:

```
nano /etc/php/8.2/apache2/php.ini
```

Dans le document recherchez la ligne “session.cookie_httponly =” et ajouter “on” à la fin, puis enregistrer les modifications:

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

Créer un fichier glpi.conf, dans le dossier apache2:

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

Dans ce fichier insérer le contenu suivant (en adaptant par rapport au serveur) ici avec ma config par exemple:

```
<VirtualHost *:80>
    # ServerName vm-glpi
    ServerAlias 192.168.192.130
    DocumentRoot /var/www/html
    Alias "/glpi" "/var/www/html/glpi/public"
    <Directory /var/www/html/glpi>
        Require all granted
        RewriteEngine On
        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]
    </Directory>
</VirtualHost>
```

Ensuite il faut reconfigurer Apache et le relancer avec les commandes suivantes:

```
a2enmod rewrite  
a2dissite 000-default.conf  
a2ensite glpi.conf  
systemctl restart apache2
```

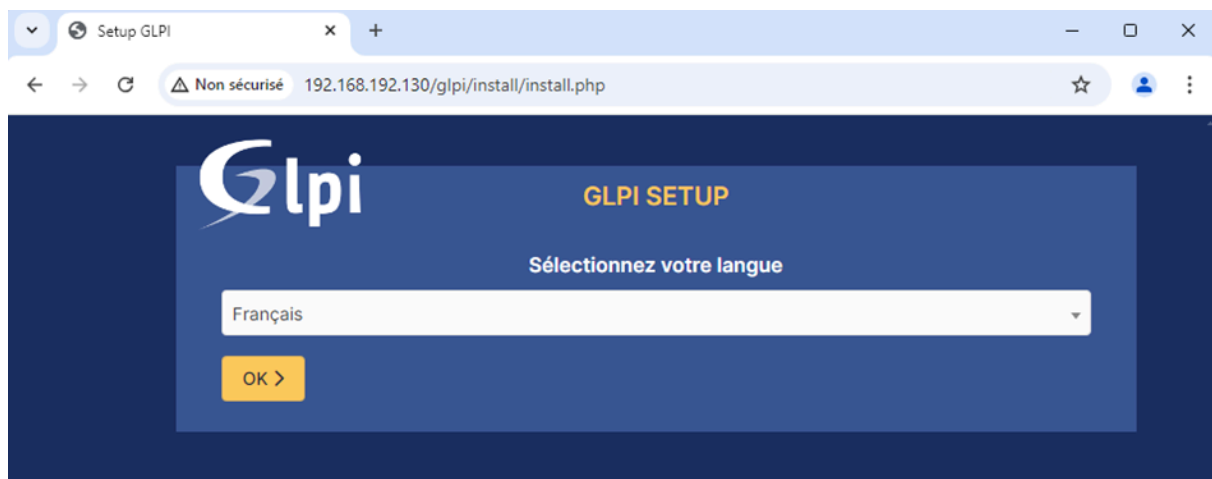
Le serveur GLPI est prêt, on passe à la configuration sur l'interface Web.

5. Interface Web GLPI

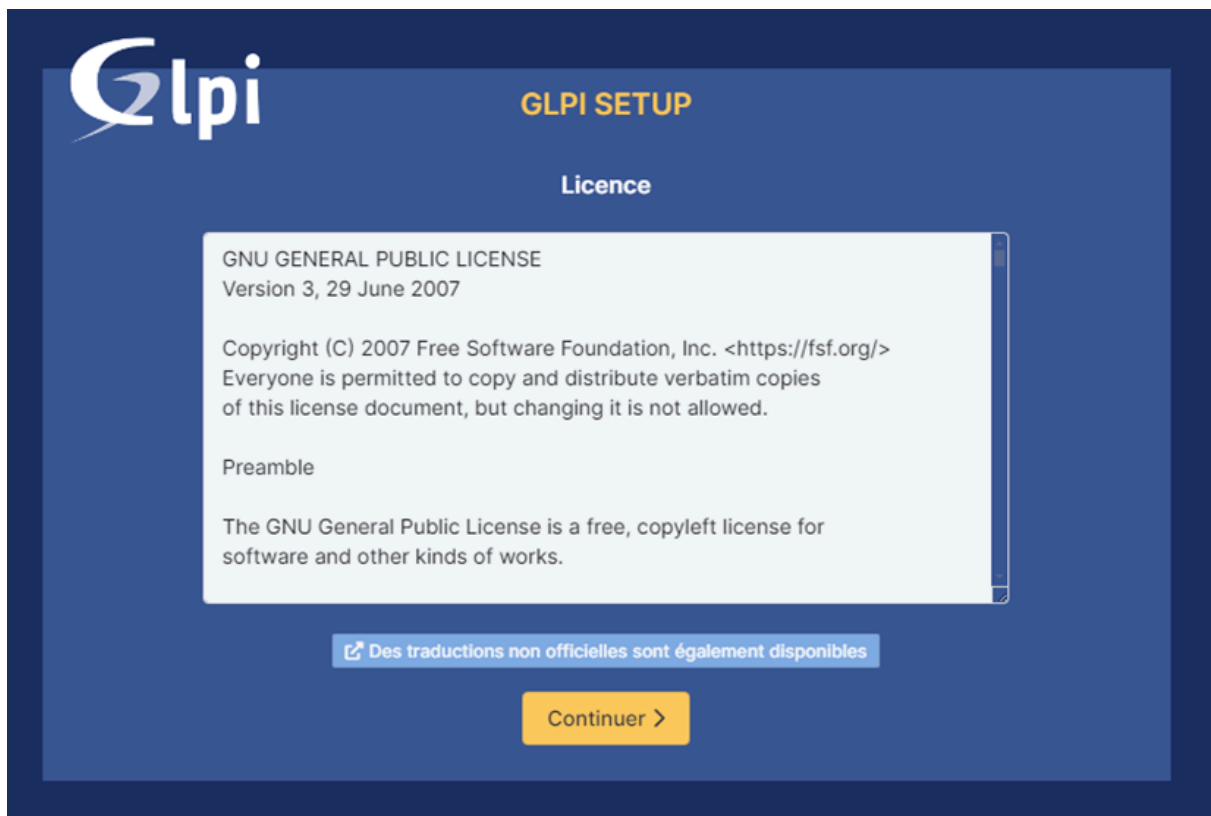
Accéder au service GLPI en tapant cette adresse dans le navigateur (remplacer l'adresse ip par celle du serveur) ici dans mon cas:

<http://192.168.192.130/glpi>

Cette page devrait apparaître:



Cliquer sur Ok et sur continuer sur la page suivante:



Ensuite cliquer sur “Installer”:



Les champs devraient tous être validés, sinon il y a une erreur:



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 <i>Requis pour l'accès à distance aux ressources (requêtes des agents d'inventaire, Marketplace, flux RSS, ...).</i>	✓
Requis gd extension <i>Requis pour le traitement des images.</i>	✓
Requis intl extension <i>Requis pour l'internationalisation.</i>	✓
Requis zlib extension <i>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.</i>	✓
Requis Libsodium ChaCha20-Poly1305 constante de taille <i>Activer l'utilisation du cryptage ChaCha20-Poly1305 requis par GLPI. Il est fourni par libsodium à partir de la version 1.0.12.</i>	✓
Requis Permissions pour les fichiers de log	✓
Requis Permissions pour les dossiers de données	✓
Sécurité Version de PHP maintenue <i>Une version de PHP maintenue par la communauté PHP devrait être utilisée pour bénéficier des correctifs de sécurité et de bogues de PHP.</i>	✓
Sécurité Configuration sécurisée du dossier racine du serveur web <i>La configuration du dossier racine du serveur web devrait être <code>/var/www/html/glpi/public</code> pour s'assurer que les fichiers non publics ne peuvent être accessibles.</i>	✓
Sécurité Configuration de sécurité pour les sessions <i>Permet de s'assurer que la sécurité relative aux cookies de session est renforcée.</i>	✓
Suggéré Taille d'entier maximal de PHP <i>Le support des entiers 64 bits est nécessaire pour les opérations relatives aux adresses IP (inventaire réseau, filtrage des clients API, ...).</i>	✓
Suggéré exif extension <i>Renforcer la sécurité de la validation des images.</i>	✓
Suggéré ldap extension <i>Active l'utilisation de l'authentification à un serveur LDAP distant.</i>	✓
Suggéré openssl extension <i>Active l'envoi de courriel en utilisant SSL/TLS.</i>	✓
Suggéré Extensions PHP pour le marketplace <i>Permet le support des formats de paquets les plus communs dans le marketplace.</i>	✓
Suggéré Zend OPcache extension <i>Améliorer les performances du moteur PHP.</i>	✓
Suggéré Extensions émulées de PHP <i>Améliorer légèrement les performances.</i>	✓
Suggéré Permissions pour le répertoire du marketplace <i>Active l'installation des plugins à partir du Marketplace.</i>	✓

Continuer >

Ensuite saisir les identifiants de l'utilisateur qui a les droits sur la base de données:



GLPI **GLPI SETUP**

Étape 1

Configuration de la connexion à la base de données

Serveur SQL (MariaDB ou MySQL)

localhost

Utilisateur SQL

admindb_glpi

Mot de passe SQL

....

Continuer >

Sélectionner la base de données que l'on a crée précédemment:



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 :

☐

☒ db_glpi

Continuer >

Appuyer sur “Continuer” lors des prochaines étapes:



GLPI SETUP

Étape 3

Initialisation de la base de données.

OK - La base a bien été initialisée

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 "Télémétrie", 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 améliorions GLPI et ses plugins !

[Voir ce qui serait 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 >](#)



Ici, il faut bien noter les identifiants qui nous sont donnés pour les accès à GLPI :



Se connecter en utilisant ces derniers ici:



Connexion à votre compte

Identifiant

glpi

Mot de passe

....

Source de connexion

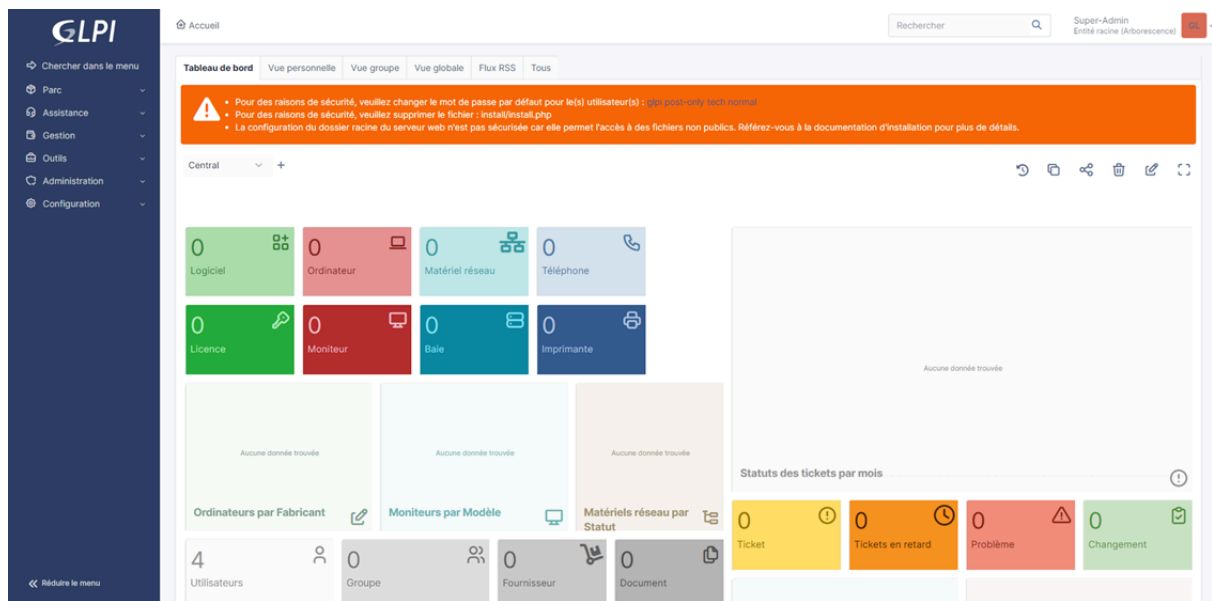
Base interne GLPI ▼

☒ Se souvenir de moi

Se connecter

GLPI Copyright (C) 2015-2024 Teclib' and contributors

En se connectant, l'interface GLPI devrait s'afficher:



Pour faire partir le message d’avertissement il suffit de changer le mot de passe par défaut des 4 utilisateurs, par exemple ici je modifie le mot de passe de l’utilisateur “tech”:

GLPI

Accueil / Administration / Utilisateurs

Utilisateur

Habilitations 1

Groupes

Préférences

Éléments utilisés

Éléments gérés

Tickets créés

Problèmes

Changements

Documents

Réservations

Synchronisation

Liens

Certificats

Historique

Tous

Utilisateur - tech

Identifiant

tech

Image

TE

Fichier(s) (2 Mio maximum) i

Glissez et déposez votre fichier ici, ou

Choisir un fichier

Aucun fichier choisi

☐ Effacer

Nom de famille

Prénom

Mot de passe

....

Confirmation mot de passe

....

Fuseau horaire

GLPI est installé et prêt à être configuré ! Il faut maintenant mettre en place les habilitations et la gestion des tickets. Sans oublier la continuité du service.

II. Gestion des habilitations

La gestion des habilitations dans **GLPI** permet de définir précisément les droits et les rôles des utilisateurs en fonction de leur profil ou de leur service. Grâce à un système de **profils** (administrateur, technicien, demandeur, etc.) associés à des **entités**, il est possible de restreindre ou d'élargir l'accès à certaines fonctionnalités (création de tickets, gestion de l'inventaire, administration du système, etc.). Cette granularité dans les permissions assure une **sécurité renforcée**, une **meilleure organisation** du support, et permet d'adapter l'outil aux besoins spécifiques de chaque service ou utilisateur.

1. Définition des rôles par grade

Ici, j'ai mis en place une hiérarchie et **adapté en conséquence** les droits de chacun. Voici une liste des personnes et des rôles associés, accompagnée d'une explication des choix effectués :

- Durand Alexandre :
 - o Président Directeur Général :
 - Observateur, il peut tout observer mais il ne doit rien modifier
- Lefebvre Marc :
 - o Directeur du Support Logiciel :
 - Observateur, il gère les équipes et un rôle Directeur Support Logiciel pour gérer les tickets et les changements, valider les demandes de changement et la consultation des éléments matériels liés aux tickets
 - Groupe logiciel et responsable du groupe
- Morel Isabelle :
 - o Responsable Adjointe du Support Logiciel :
 - Technician, car elle gère les équipes en soutiens, avec un rôle Responsable Adjoint pour gérer les plannings
 - Groupe logiciel
- Simon David :
 - o Directeur du Support Réseau :
 - Observateur, il gère les équipes et un rôle Directeur Support Réseau pour gérer les tickets et les changements, valider les demandes de changement et la consultation des éléments matériels liés aux tickets
 - Groupe réseau et responsable du groupe
- Fontaine Camille :
 - o Responsable Adjointe du Support Réseau :
 - Technician, car elle gère les équipes en soutiens, avec un rôle Responsable Adjoint pour gérer les plannings
 - Groupe réseau
- Blanc Laurent :
 - o Directeur de la Sécurité Informatique :
 - Observateur, il gère les équipes et un rôle Directeur Support Sécurité Informatique pour gérer les tickets et les changements, valider les demandes de changement et la consultation des éléments matériels liés aux tickets
 - Groupe sécurité et responsable du groupe

- Guerin Sarah :
 - o Responsable Adjointe de la Sécurité Informatique :
 - Technician, car elle gère les équipes en soutiens, avec un rôle Responsable Adjoint pour gérer les plannings
 - Groupe sécurité
- Martin Pierre :
 - o Responsable du HelpDesk :
 - Super-Admin, car il gère l'intégralité du système
- Dubois Sophie :
 - o Technicien Niveau 1 Logiciel :
 - Technician, car elle s'occupe seulement de résoudre des tickets
 - Groupe logiciel
- Leroy Julien :
 - o Technicien Niveau 1 Réseau :
 - Technician, car il s'occupe seulement de résoudre des tickets
 - Groupe réseau
- Moreau Clara :
 - o Technicien Niveau 2 Logiciel :
 - Gestion Habilitations GLPI – Brunin Maxime 2SLAM
 - Technician, car elle s'occupe seulement de résoudre des tickets
 - Groupe logiciel
- Bernard Thomas :
 - o Technicien Niveau 2 Sécurité :
 - Technician, car il s'occupe seulement de résoudre des tickets
 - Groupe sécurité
- Fournier Nicolas :
 - o Technicien Niveau 3 Réseau :
 - Technician, car il s'occupe seulement de résoudre des tickets avec un rôle Niveau 3 pour valider les actions pour les incidents critiques et l'accès aux matériels nécessaires pour résoudre les incidents
 - Groupe réseau
- Rousseau Laura :
 - o Technicien Niveau 3 Systèmes :
 - Technician, car elle s'occupe seulement de résoudre des tickets avec un rôle Niveau 3

pour valider les actions pour les incidents critiques et l'accès aux matériels nécessaires pour résoudre les incidents

- Groupe réseau

- Petit Antoine :

- o Analyste de Sécurité :

- Observer, car il se concentre sur la surveillance des incidents de sécurité et effectue des audits pour renforcer les politiques de sécurité

- Groupe sécurité

- Girard Emma :

- o Coordinatrice du Support :

- Supervisor, car elle coordonne les résolutions des tickets

2. Mise en place des groupes et des rôles

III. Mise en place d'un collecteur de mail

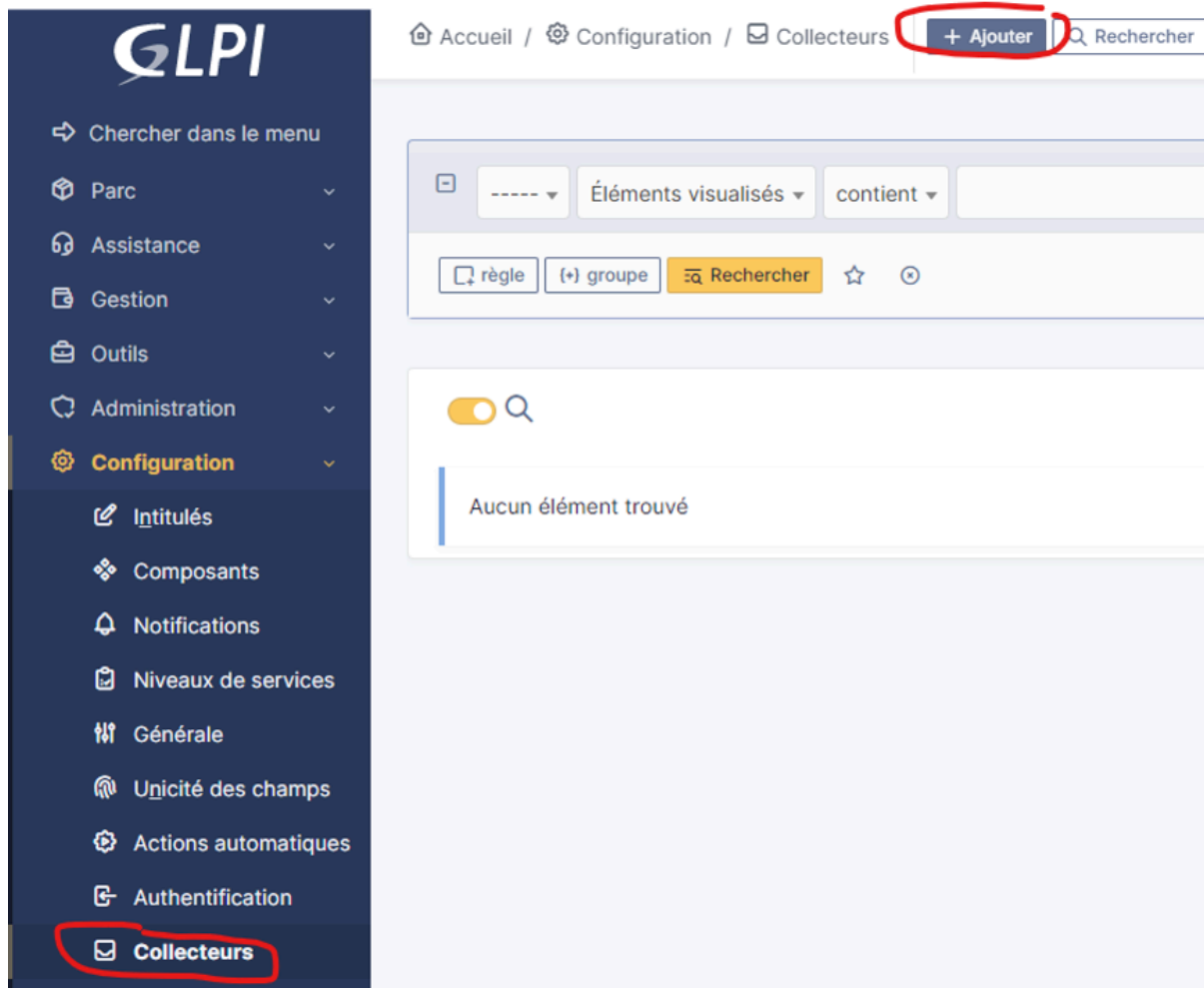
Ici nous allons mettre en place un collecteur de mail qui permet de récupérer automatiquement les e-mails envoyés à une adresse spécifique (ex : support@entreprise.com) pour les **convertir en tickets** dans le système. Cela facilite la création de demandes d'assistance sans passer par l'interface GLPI, tout en centralisant les requêtes des utilisateurs.

D'abord se rendre dans le menu de configuration de la GLPI, cliquer sur "Générale" et autoriser les suivis anonymes et les ouvertures de tickets anonymes.

The screenshot shows the GLPI configuration interface. The sidebar on the left has the 'Configuration' menu highlighted. The main content area shows the 'Assistance' section with various settings. The 'Autoriser les suivis anonymes (collecteur)' and 'Autoriser les ouvertures de tickets anonymes (helpdesk, collecteur)' options are both set to 'Oui' (Yes) and are circled in red. The 'Matrice de calcul de la priorité' (Priority calculation matrix) is also visible at the bottom.

	Très haut	Haut	Moyen	Bas	Très bas
Impact	Oui	Oui		Oui	Oui
Urgence					
Très haute	Oui				
Haute	Oui				
Moyenne					
Basse	Oui				

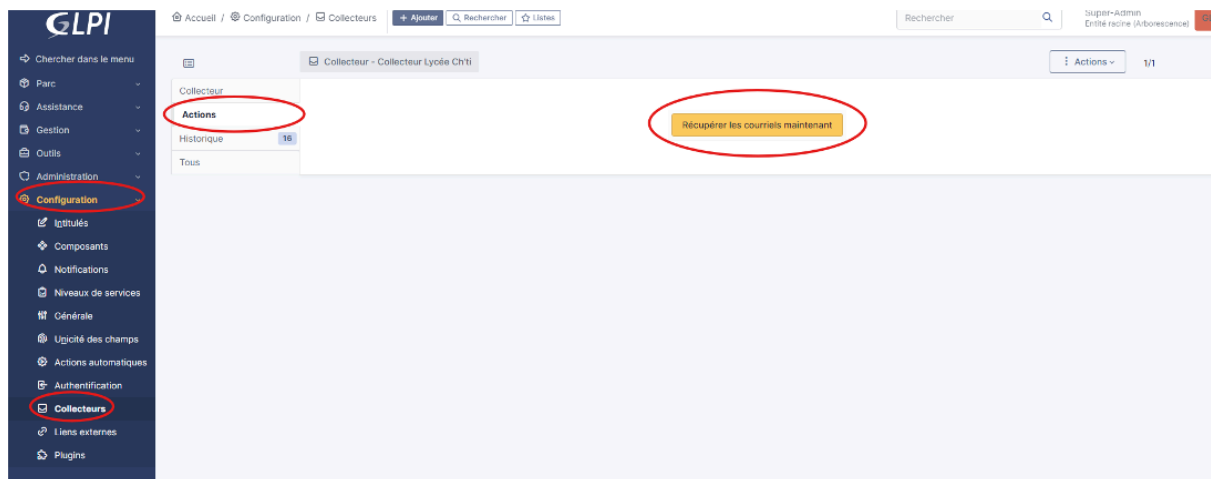
Toujours dans le menu “Configuration”, sélectionner “Collecteurs” et cliquer sur le bouton “Ajouter” en haut:



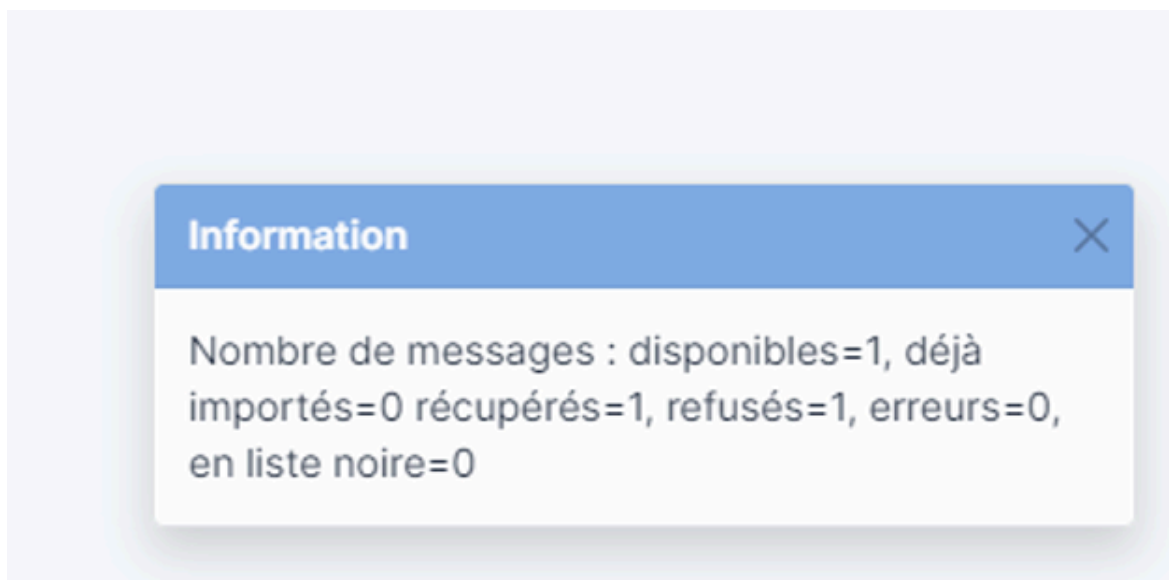
Entrer les informations du collecteur, ici j'utilise une adresse free:

Nom	Collecteur
Actif	Oui
Serveur	imap.free.fr
Options de connexion	IMAP TLS DEBUG
Dossier des messages entrants (optionnel, souvent INBOX)	
Port (optionnel)	993
Chaîne de connexion	{imap.free.fr:993/imap/tls/debug}
Identifiant	maxime2@indriamihaja.free
Mot de passe	<input type="password"/> <input type="checkbox"/> Effacer
Dossier d'archivage des courriels acceptés (optionnel)	
Dossier d'archivage des courriels refusés (optionnel)	
Taille maximale des fichiers importés par le collecteur	2 Mio
Utiliser la date du courriel au lieu de celle de la collecte	Non
Utiliser "Répondre à" en tant que demandeur (si disponible)	Non
Ajouter les utilisateurs CC comme observateurs	Non
Collecter uniquement les emails non lus	Oui

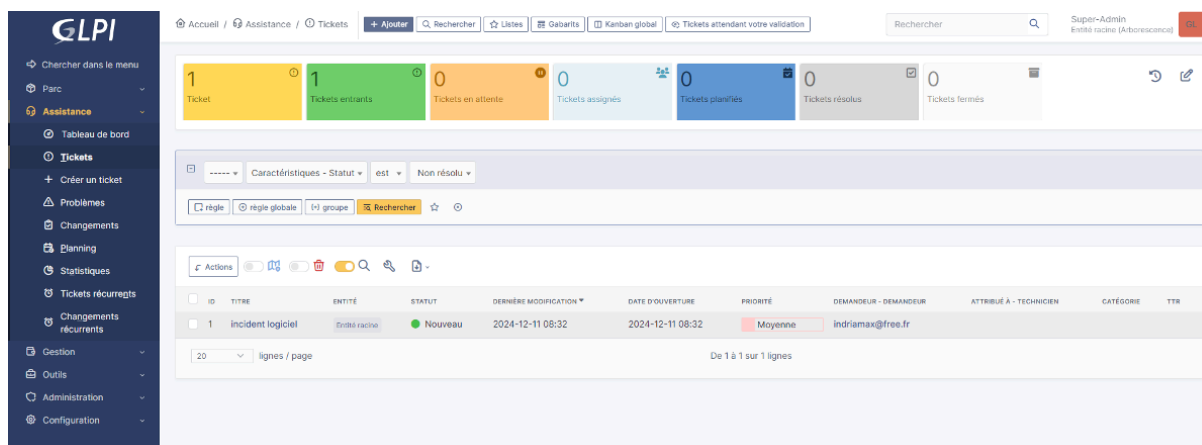
Ensuite, on envoie par mail au collecteur, le problème que l'on rencontre et avec GLPI on va récupérer les mails et en faire un ticket. Pour se faire on reste dans le menu "Configuration" et dans "Collecteurs". Mais cette fois-ci on va aller dans le menu "Actions" et cliquer sur le bouton "Récupérer les courriels maintenant". Cela aura pour effet de récupérer les mails et les transformer en ticket et ainsi assurer leur prise en charge par les personnes habilitées.



Un pop-up devrait s'afficher pour confirmer la récupération:



On peut ensuite se rendre dans le menu “Assistance” de GLPI et le ticket devrait apparaitre dans le menu:



Désormais la création de ticket est automatisé, mettons maintenant en place la continuité du service avec le HAProxy.

IV. Continuité de service

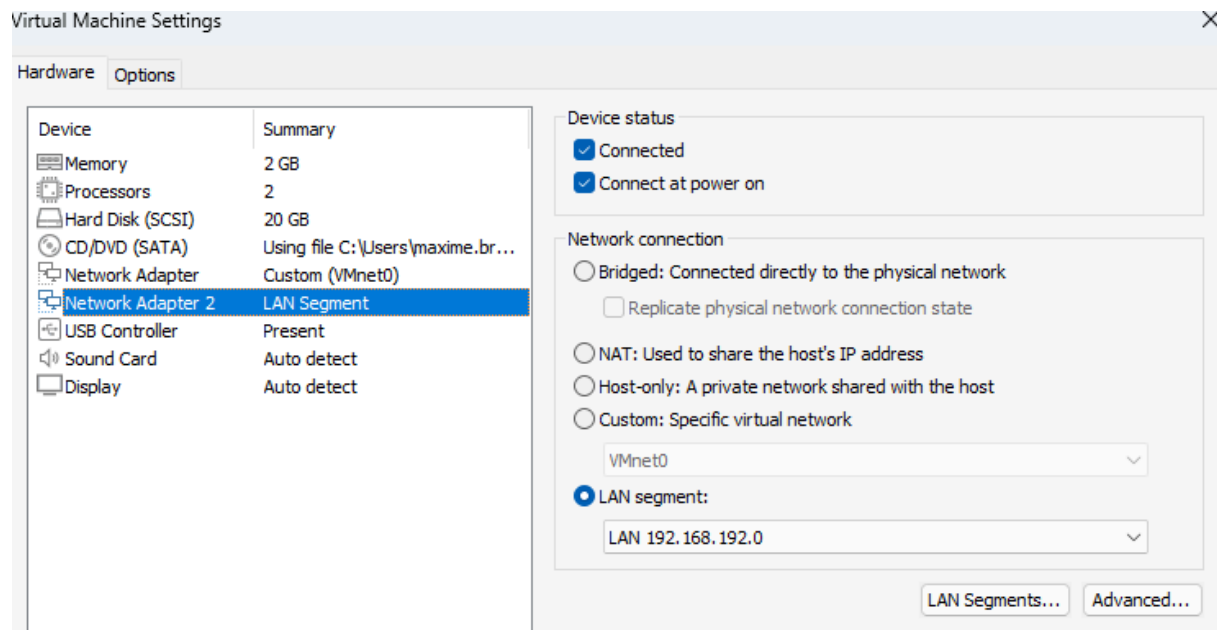
HAProxy (High Availability Proxy) est un répartiteur de charge (load balancer) open-source reconnu pour sa performance, sa fiabilité et sa flexibilité. Il est couramment utilisé pour distribuer le trafic réseau entre plusieurs serveurs, assurant ainsi une meilleure disponibilité, une montée en charge efficace et une tolérance aux pannes.

Grâce à ses nombreuses fonctionnalités, HAProxy est un composant clé dans les architectures orientées haute disponibilité et dans la gestion du trafic HTTP(s) et TCP à grande échelle.

Ici, je vais utiliser la VM qui contient le GLPI de Marieteam et la cloner pour mettre en place un HAProxy entre les deux serveurs. Ceci permettra de garantir l'accès à au moins un serveur en cas de panne.

1. Mise en place d'un HAProxy

Voici les paramètres à appliquer à la machine HAProxy:



On installe apache et haproxy:

```
apt -y install apache2
apt -y install haproxy
```

On va ajouter les deux adresses IP des serveurs:

```
nano /etc/hosts
```

```
GNU nano 7.2
127.0.0.1      localhost
127.0.1.1      haproxy
192.168.192.130 srv1
192.168.192.131 srv2_
```

On va paramétrer l'IP de la machine HAProxy pour communiquer avec les serveurs

```
nano /etc/network/interfaces
```

```
# This file describes the network interfaces
# and how to activate them. For more information, see
# the man page of the /etc/network/interfaces file.

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

allow-hotplug ens37
iface ens37 inet static
address 192.168.192.132/24
```

On ajoute le frontend et le backend au HAProxy:

```
nano /etc/haproxy/haproxy.cfg
```

```

GNU nano 7.2 /etc/haproxy/haproxy.cfg *
global
    log /dev/log      local0
    log /dev/log      local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon

    # Default SSL material locations
    ca-base /etc/ssl/certs
    crt-base /etc/ssl/private

    # See: https://ssl-config.mozilla.org/#server=haproxy&server-version=2.0.3&config=intermediate
    ssl-default-bind-ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:
    ssl-default-bind-ciphersuites TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
    ssl-default-bind-options ssl-min-ver TLSv1.2 no-tls-tickets

defaults
    log          global
    mode         http
    option        httplog
    option        dontlognull
    timeout      connect 5000
    timeout      client  50000
    timeout      server  50000
    errorfile    400 /etc/haproxy/errors/400.http
    errorfile    403 /etc/haproxy/errors/403.http
    errorfile    408 /etc/haproxy/errors/408.http
    errorfile    500 /etc/haproxy/errors/500.http
    errorfile    502 /etc/haproxy/errors/502.http
    errorfile    503 /etc/haproxy/errors/503.http
    errorfile    504 /etc/haproxy/errors/504.http

frontend frontend-base
    bind *:80
    default_backend backend-base
    option forwardfor

backend backend-base
    balance roundrobin
    server web1 192.168.192.130:80 check
    server web2 192.168.192.131:80 check

```

2. Modification sur les deux serveurs GLPI

On va s'assurer que les hostname et les IP des machines correspondent à celles du HAProxy:

```
hostnamectl set-hostname nomDuServeur
```

```
nano /etc/network/interfaces
```

```
# This file describes the network in
# and how to activate them. For more

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 static
address 192.168.192.130/24
```

```
GNU nano 7.2
# This file describes the network inte

source /etc/network/interfaces.d/*

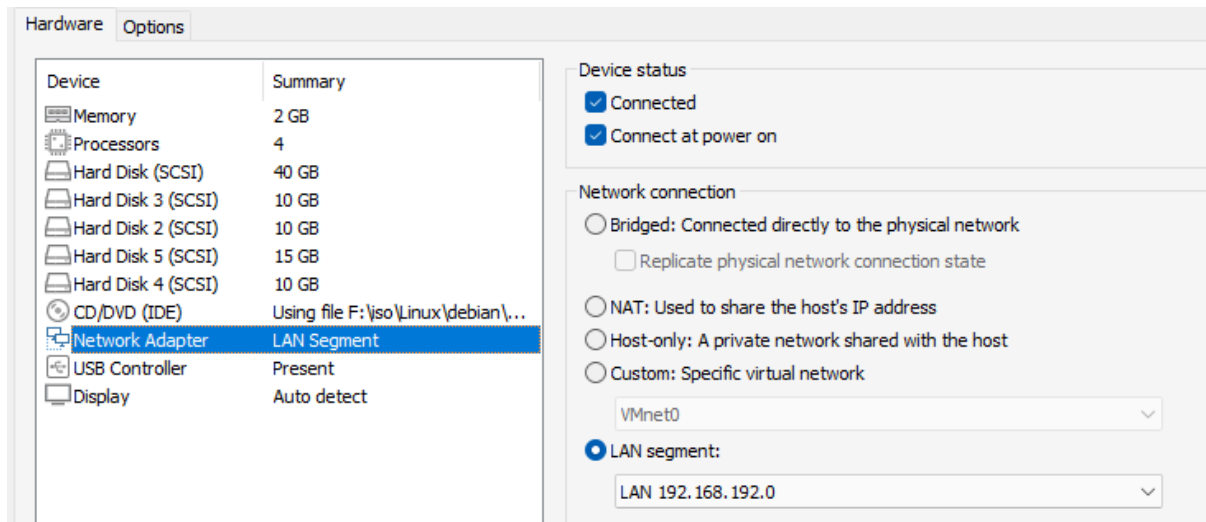
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
allow-hotplug ens33
iface ens33 inet static
address 192.168.192.131
netmask 255.255.255.0
```

On va modifier la page sur laquelle on sera redirigé pour voir quel serveur est utilisé

```
nano /var/www/html/index.html
```

```
div.validator {
}
</style>
</head>
<body>
  <div class="main_page">
    <div class="page_header floating_element">
      
      <span class="floating_element">
        SRV2
      </span>
    </div>
    <!-- <div class="table_of_contents floating_element">
      <div class="section header section header grey">
```

On s'assure que les serveurs GLPI soient bien sur le même LAN Segment que le HAProxy



Redémarrer les deux machines

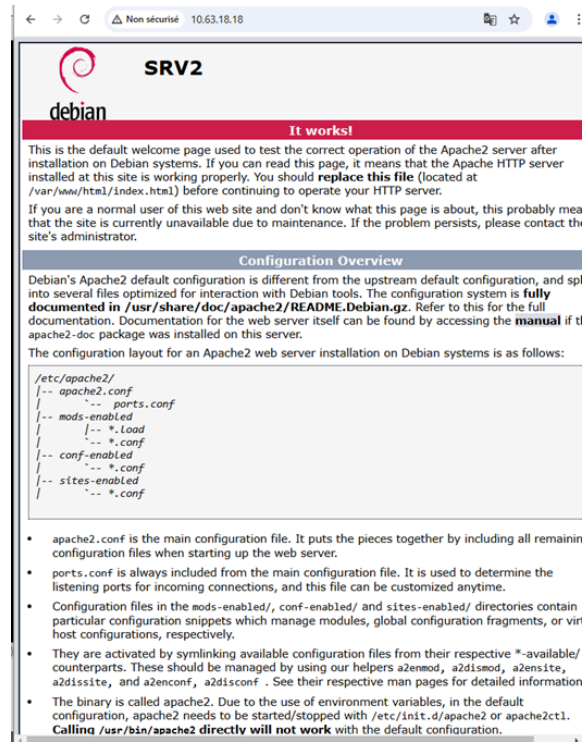
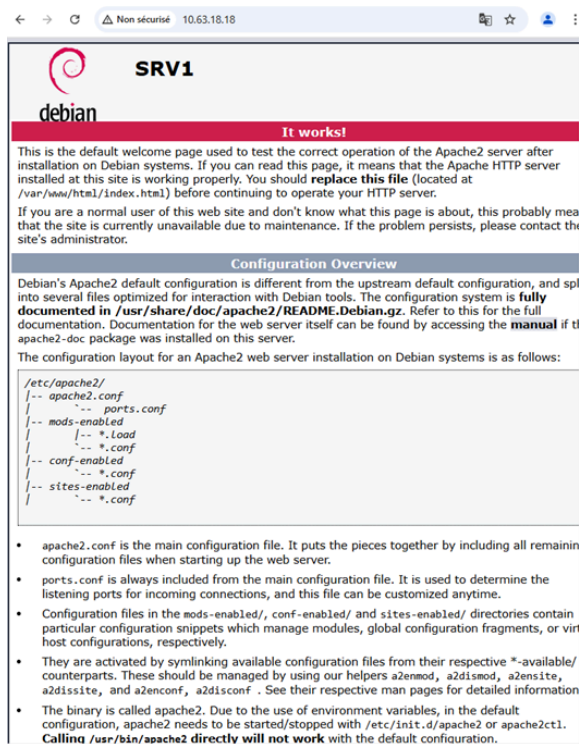
```
reboot
```

Redémarrer le HAProxy

```
systemctl restart haproxy
```

3. Test du HAProxy et des serveurs

On navigue vers l'ip associé au serveur HAProxy, ici 10.63.18.18. On obtient donc en affichage une page avec le nom du serveur utilisé. En appuyant sur F5 on voit le balancement entre les serveurs:



4. Mise en place des statistiques

On va retourner dans le fichier de config du HAProxy pour ajouter la page de statistiques et mieux visualiser:

```
nano /etc/haproxy/haproxy.cfg
```

```
listen httpProxy
  bind 10.63.18.18:80
  balance roundrobin
  server srv1 192.168.192.130:80 check
  server srv2 192.168.192.131:80 check
listen stats
  bind *:8080
  stats enable
  stats uri /statsHaproxy
  stats auth admin:password
  stats refresh 30s
```

On redémarre le HAProxy pour les modifications:

systemctl restart haproxy

On navigue vers l'adresse 10.63.18.18:8080/statsHaproxy et on obtient l'affichage suivant:

← → ↻ Non sécurisé 10.63.18.18:8080/statsHaproxy

HAProxy version 2.6.12-1+deb12u1, released 2023/12/16

Statistics Report for pid 1052

> General process information

pid = 1052 (process #1, nbproc = 1, nbthread = 2)
uptime = 0s 0h02m08s
system limits: memmax = unlimited; ulimit-n = 624288
maxsock = 524288; maxconn = 262121; maxpipes = 0
current conns = 2; current pipes = 0/0; conn rate = 0/sec; bit rate = 0.000 kbps
Running tasks: 0/22; idle = 100 %

active UP backup UP
active UP, going down backup UP, going down
active DOWN, going up backup DOWN, going up
active or backup DOWN not checked
active or backup DOWN for maintenance (MAINT)
active or backup SOFT STOPPED for maintenance
Note: "NOLB"/"DRAIN" = UP with load-balancing disabled.

Display option: Scope:
• Hide 'DOWN' servers
• Disable refresh
• Refresh now
• CSV export
• JSON export (schema)

External resources:
• Primary site
• Updates (v2.6)
• Online manual

frontend-base																															
	Queue			Session rate			Sessions				Bytes		Denied	Errors		Warnings		Server													
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle	
Frontend	0	0	-	0	0	0	0	0	0	262121	0	0	0	0	0	0	0	0	0	0	0	0	OPEN								

backend-base																														
	Queue			Session rate			Sessions				Bytes		Denied	Errors		Warnings		Server												
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
srv1	0	0	-	0	0	0	0	0	0	0	0	?	0	0	0	0	0	0	0	0	0	2m8s UP	L4OK in 1ms	1/1	Y	-	0	0	0s	-
srv2	0	0	-	0	0	0	0	0	0	0	0	?	0	0	0	0	0	0	0	0	0	2m8s UP	L4OK in 1ms	1/1	Y	-	0	0	0s	-
Backend	0	0	-	0	0	0	0	0	0	26213	0	0	?	0	0	0	0	0	0	0	0	2m8s UP		2/2	2	0		0	0s	

httpProxy																														
	Queue			Session rate			Sessions				Bytes		Denied	Errors		Warnings		Server												
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
Frontend	0	2	-	0	2	0	0	2	0	262121	2	0	631	3293	0	0	1	0	0	0	0	OPEN								
srv1	0	0	-	0	1	0	0	1	-	1	1	2m1s	631	3293	0	0	0	0	0	0	0	2m8s UP	L4OK in 0ms	1/1	Y	-	0	0	0s	-
srv2	0	0	-	0	0	0	0	0	-	0	0	?	0	0	0	0	0	0	0	0	0	2m8s UP	L4OK in 1ms	1/1	Y	-	0	0	0s	-
Backend	0	0	-	0	1	0	0	1	0	26213	1	1	631	3293	0	0	0	0	0	0	0	2m8s UP		2/2	2	0		0	0s	

stats																														
	Queue			Session rate			Sessions				Bytes		Denied	Errors		Warnings		Server												
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
Frontend	0	5	-	2	2	0	0	2	0	262121	10	0	5496	100597	0	0	1	0	0	0	0	OPEN								
Backend	0	0	-	0	4	0	0	1	0	26213	6	0	0s	5496	100597	0	0	6	0	0	0	2m8s UP		0/0	0	0		0	0s	

5. Test de continuité de service

Pour tester si la continuité de service est assurée, on va effectuer un test. On va shutdown l'un des deux serveurs, vérifier avec les statistiques si le serveur est bien down et ensuite on devrait voir uniquement le serveur 1 utilisé avec l'aide de la page.

shutdown now


Ici les statistiques montrent bien que le serveur 2 est down et que seul le 1 est up:

backend-base																			
Queue			Session rate			Sessions			Bytes			Denied		Errors		Warnings		Status	
Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr
srv1	0	0	-	0	0	0	0	-	0	0	?	0	0	0	0	0	0	0	0
srv2	0	0	-	0	0	0	0	-	0	0	?	0	0	0	0	0	0	0	0
Backend	0	0	-	0	0	0	0	-	26 213	0	?	0	0	0	0	0	0	0	0

httpProxy																			
Queue			Session rate			Sessions			Bytes			Denied		Errors		Warnings		Status	
Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr
Frontend	0	0	-	0	1	0	1	-	1	1	3m53s	631	3 293	0	0	0	0	0	0
srv1	0	0	-	0	1	0	1	-	1	1	3m53s	631	3 293	0	0	0	0	0	0
srv2	0	0	-	0	0	0	0	-	0	0	?	0	0	0	0	0	0	0	0
Backend	0	0	-	0	1	0	1	-	26 213	1	1	3m53s	631	3 293	0	0	0	0	0

On navigue vers la page du serveur HAProxy et on refresh en boucle:

Non sécurisé
10.63.18.18



SRV1

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
```

Donc seul la page du serveur 1 s’affiche, la continuité du service est donc assurée. Le HAProxy est fonctionnel.

V. Conclusion

L'intégration de GLPI au sein du projet Marieteam a permis de structurer et centraliser efficacement la gestion des incidents et des demandes d’assistance. L'installation sur un serveur Debian 12, combinée à la configuration des droits utilisateurs, a permis d’adapter la solution aux besoins spécifiques de l'entreprise. La mise en place d’un collecteur de mails automatisant la création de tickets a amélioré l'efficacité du support. Enfin, l'ajout d’un HAProxy a assuré la haute disponibilité du service, garantissant ainsi la continuité du support informatique. Cette mise en œuvre complète de GLPI permet de répondre de manière optimisée aux besoins du support technique, tout en offrant une flexibilité pour les évolutions futures du système.