GLPI

Índex

GLPI (Gestionnaire Libre de Parc Informatique) és una eina lliure de gestió de serveis TI (ITSM) que permet portar l'inventari d'equips, la gestió d'incidències, els actius de programari i molt més. En aquest document es mostra com instal·lar GLPI en un servidor Ubuntu 26.04 LTS, com connectar-lo amb OCS Inventory per automatitzar l'inventari de màquines, i com configurar l'autenticació i la importació d'usuaris des d'un servidor LDAP.

Figura 1: GLPI Logo

Requisits previs

- Servidor amb Ubuntu Server 26.04 LTS instal·lat i actualitzat.
- Mínim 2 CPU i 2 GB de RAM (recomanat 4 GB en entorns amb diversos usuaris).
- Accés `root` o usuari amb privilegis `sudo`.
- Un nom de domini o, com a mínim, una IP fixa per al servidor.
- Connexió a Internet per descarregar paquets.

1. Prepara el sistema

Actualitza la llista de paquets

```
sudo apt update
```

Actualitza el sistema

```
sudo apt upgrade
```

1.1. Instal·la Apache, PHP i extensions necessàries

GLPI necessita PHP 8.2 o superior. Ubuntu 26.04 LTS ja inclou PHP 8.5 als seus dipòsits oficials, per la qual cosa no cal afegir dipòsits externs.

```
sudo apt install apache2 \
  php php-cli php-common php-curl php-gd php-ldap php-mysql \
  php-xmlrpc php-xml php-mbstring php-bcmath php-intl php-zip \
  php-redis php-bz2 php-apcu php-soap libapache2-mod-php php-cas
```

NOTA

`php-ldap` és imprescindible per a la integració amb LDAP que es configurarà més endavant, i `php-soap`/`php-cas` per a funcionalitats addicionals d'autenticació i API.

1.2. Instal·la MariaDB

```
sudo apt install mariadb-server
```

Un cop instal·lat, assegura'l:

```
sudo mariadb-secure-installation
```

Respon afirmativament a totes les preguntes (establir contrasenya root, eliminar usuaris anònims, desactivar accés remot de root, eliminar la base de dades de test i recarregar privilegis).

```
NOTE: MariaDB is secure by default in Debian. Running this script is
      useless at best, and misleading at worst. This script will be
      removed in a future MariaDB release in Debian. Please read
      /usr/share/doc/mariadb-server/README.Debian.gz for details.

Enter root user password or leave blank:

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer
 ↪  'n'.

Switch to unix_socket authentication [Y/n]
Enabled successfully (or at least no errors was emitted)!
Reloading privilege tables..
 ... Success!


You already have your root account protected, so you can safely answer
 ↪  'n'.

Change the root password? [Y/n]
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]
SQL executed without errors!
The operation might have been successful, or it might have not done
 ↪  anything.

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]
SQL executed without errors!
The operation might have been successful, or it might have not done
 ↪  anything.

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]
 - Dropping test database...
SQL executed without errors!
The operation might have been successful, or it might have not done
 ↪  anything.
 - Removing privileges on test database...
SQL executed without errors!
The operation might have been successful, or it might have not done
 ↪  anything.

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

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

Activa i arrenca els serveis:

```
sudo systemctl enable --now apache2 mariadb
```

Comprova que estiguin actius

```
systemctl is-active apache2 mariadb
```

Ambdós haurien de mostrar `active`.

2. Crea la base de dades de GLPI

Accedeix a MariaDB com a root:

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

I executem dins de la consola SQL:

```
CREATE DATABASE glpi;
GRANT ALL PRIVILEGES ON glpi.* TO usuari@localhost IDENTIFIED BY
 ↪  'una_contrasenya_segura';
GRANT SELECT ON mysql.time_zone_name TO usuari@localhost;
FLUSH PRIVILEGES;
EXIT;
```

IMPORTANT

Substitueix `una_contrasenya_segura` per una contrasenya forta i guarda-la, ja que la necessitaràs al punt 5 durant la instal·lació amb l'assistent. El permís sobre `mysql.time_zone_name` permet que GLPI gestioni correctament les zones horàries, ja que és una eina pensada per a equips distribuïts arreu del món. Si la taula de zones horàries de MySQL/MariaDB no està carregada, es pot carregar amb:

```
sudo mysql_tzinfo_to_sql /usr/share/zoneinfo | sudo mysql -u root
 ↪  -p mysql
```

3. Descarrega i desplega GLPI

Descarrega l'última versió estable des del dipòsit oficial de GitHub (en el moment d'escriure aquest document, la 11.0.8). Pots consultar la versió més recent a https://github.com/glpi-project/glpi/releases

```
wget -c https://github.com/glpi-project/glpi/releases/download/11.0.
 ↪  8/glpi-11.0.8.tgz
```

Descomprimeix al document root per defecte d'Apache.

```
sudo tar -xvzf glpi-11.0.8.tgz -C /var/www/html/
```

Esborra el fitxer descarregat.

```
rm glpi-11.0.8.tgz
```

3.1. Estructura de directoris recomanada

Des de la versió 10, la documentació oficial de GLPI recomana separar la configuració, els fitxers de dades i els registres de fora del directori web públic, per motius de seguretat.

Crea les carpetes:

```
sudo mkdir -p /etc/glpi /var/lib/glpi /var/log/glpi
```

Mou els fitxers de dades.

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

Crea el fitxer `local_define.php` que redirigeix cap a `/etc/glpi` (aquest és l'únic fitxer que GLPI necessita trobar al webroot per saber on és la resta):

```
sudo nano /var/www/html/glpi/config/local_define.php
```

Contingut (stub dins del webroot):

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

Crea ara el fitxer `local_define.php` real a `/etc/glpi/`, amb la resta de rutes (aquest **no** és visible des del web):

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

Contingut:

```
<?php
define('GLPI_VAR_DIR', '/var/lib/glpi');
define('GLPI_DOC_DIR', GLPI_VAR_DIR);
define('GLPI_CACHE_DIR', GLPI_VAR_DIR . '/_cache');
define('GLPI_CONFIG_DIR', '/etc/glpi');
define('GLPI_LOG_DIR', '/var/log/glpi');
```

3.2. Permisos

Modifica el propietari de les carpetes.

```
sudo chown -R www-data:www-data /var/www/html/glpi /etc/glpi
 ↪  /var/lib/glpi /var/log/glpi
```

Modifica els permisos de la carpeta.

```
sudo chmod -R 755 /var/www/html/glpi
```

Dona permís a Apache per escriure a les carpetes

```
sudo mkdir -p /etc/systemd/system/apache2.service.d
```

```
sudo tee /etc/systemd/system/apache2.service.d/override.conf >
 ↪  /dev/null << 'EOF'
[Service]
ReadWritePaths=/var/log/apache2 /var/cache/apache2/mod_cache_disk
 ↪  /etc/glpi /var/lib/glpi /var/log/glpi
EOF
```

4. Configuració del servidor web Apache

4.1. Certificat SSL autosignat per a `glpi.thos.local`

Atès que GLPI gestiona credencials d'usuari (i, més endavant, l'autenticació contra LDAP), és molt recomanable servir-lo sempre sobre HTTPS, encara que sigui amb un certificat autosignat dins d'una xarxa interna o de centre educatiu sense un nom de domini públic.

Genera el certificat

Genera un certificat autosignat vàlid durant 825 dies (límit habitual acceptat per navegadors moderns) amb el `Common Name` (CN) corresponent al nom del servidor.

```
sudo openssl req -x509 -nodes -days 825 -newkey rsa:4096 \
  -keyout /etc/ssl/private/glpi.thos.local.key \
  -out /etc/ssl/certs/glpi.thos.local.crt \
  -subj "/C=ES/ST=Barcelona/L=Mataro/O=IES Thos i
   ↪  Codina/OU=ASIX/CN=glpi.thos.local" \
  -addext "subjectAltName=DNS:glpi.thos.local"
```

> L'extensió `subjectAltName` (SAN) és necessària perquè els navegadors moderns (Chrome, Firefox) ja no validen certificats que només especifiquin el nom al camp `CN`; cal que el SAN inclogui el mateix nom de domini.

Restringeix els permisos de la clau privada.

```
sudo chmod 600 /etc/ssl/private/glpi.thos.local.key
```

Canvia el propietari de les claus.

```
sudo chown root:root /etc/ssl/private/glpi.thos.local.key
```

```
sudo chown root:root /etc/ssl/certs/glpi.thos.local.crt
```

4.2. Crea la configuració HTTPS

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

```
<VirtualHost *:443>
    ServerAdmin webmaster@localhost

    ServerName glpi.thos.local
    DocumentRoot /var/www/html/glpi/public
    <Directory /var/www/html/glpi/public>
        Require all granted
            RewriteEngine On
            RewriteCond %{HTTP:Authorization} ^(.+)$
            RewriteRule .* -
 ↪  [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
            RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]
    </Directory>

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

    SSLEngine on

    SSLCertificateFile      /etc/ssl/certs/glpi.thos.local.crt
    SSLCertificateKeyFile   /etc/ssl/private/glpi.thos.local.key

    <FilesMatch "\.(?:cgi|shtml|phtml|php)$">
        SSLOptions +StdEnvVars
    </FilesMatch>
    <Directory /usr/lib/cgi-bin>
        SSLOptions +StdEnvVars
    </Directory>
</VirtualHost>
```

4.4. Crea la configuració HTTP (redirecció)

Crea un fitxer de configuració de virtual host específic per a GLPI. El `DocumentRoot` ha d'apuntar al directori `public/`, que és l'arrel pública segura de GLPI 10/11:

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

```
<VirtualHost *:80>
    ServerName glpi.thos.local
    Redirect permanent / https://glpi.thos.local/
</VirtualHost>
```

4.5. Habilita els mòduls i els llocs

Comprova la sintaxi

```
sudo apache2ctl configtest
```

Resposta esperada:

```
Syntax OK
```

Activa els mòduls necessaris:

```
sudo a2enmod rewrite headers ssl
```

Resposta:

```
Enabling module rewrite.
Enabling module headers.
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL
 ↪  and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

Activa els llocs

```
sudo a2ensite glpi.conf glpi-ssl.conf
```

Resposta:

```
Enabling site glpi.
Enabling site glpi-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

Si l'eina de tallafocs `ufw` està activa, obre també el port HTTPS:

```
sudo ufw allow 'Apache Full'
```

Resposta esperada:

```
Rules updated
Rules updated (v6)
```

4.6. Cookies

Cal indicar a PHP que les cookies de sessió només s'enviïn per connexions xifrades:

```
sudo nano /etc/php/8.5/apache2/php.ini
```

Busca la línia (normalment ja hi és, comentada o a 0): `session.cookie_secure = 0`, i canvia-la a:

```
session.cookie_secure = 1
```

4.7. Reinicia Apache

Com que has modificat el fitxer de configuració font d'apache2.service cal que executis `systemctl daemon-reload` per tornar a carregar les unitats.

```
sudo systemctl daemon-reload
```

Reinicia Apache

```
sudo systemctl restart apache2.service
```

CONSELL

Si l'`Apache` permet l'accés directe a `/var/www/html/glpi/` (sense passar per `public/`), l'assistent d'instal·lació mostrarà l'avís *"Web server root directory configuration is not safe"*. Assegura't que el `DocumentRoot` apunta exclusivament a `public/`.

4.8. Avís del navegador per certificat no confiat

En tractar-se d'un certificat autosignat (no emès per una entitat certificadora reconeguda), els navegadors mostraran un avís de seguretat (*"La connexió no és privada"* o similar) la primera vegada que s'accedeixi a `https://glpi.thos.local/`. Això és normal i esperat en aquest escenari; cal acceptar l'excepció de seguretat per continuar.

Per evitar aquest avís a tots els equips de l'organització, es pot distribuir el fitxer `glpi.thos.local.crt` com a certificat de confiança mitjançant una política de grup (Active Directory) o gestió centralitzada de certificats, en lloc de canviar a un certificat emès per una CA pública.

També tens l'alternativa de crear una Autoritat de Certificació privada amb OpenSSL

5. Assistent d'instal·lació web

Obre un navegador i accedeix a:

```
https://glpi.thos.local/
```

Figura 2: Configuració de GLPI

L'assistent guiarà els passos següents:

1 - **Selecció d'idioma**: triar Català o Castellà segons preferència.

Figura 3: Tria l'idioma

2 - **Llicència**: acceptar els termes GPL.

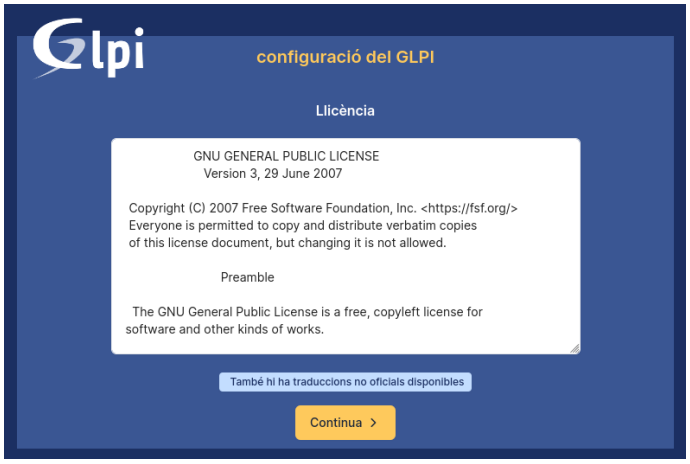

Figura 4: Llicència

3 - **Tipus d'instal·lació**: triar *Instal·lació* (no *Actualització*).

Figura 5: Inici de la instal·lació

4 - **Comprovació de requisits**: verifica que totes les extensions PHP necessàries estan instal·lades (si manqués alguna, l'assistent ho indicarà).

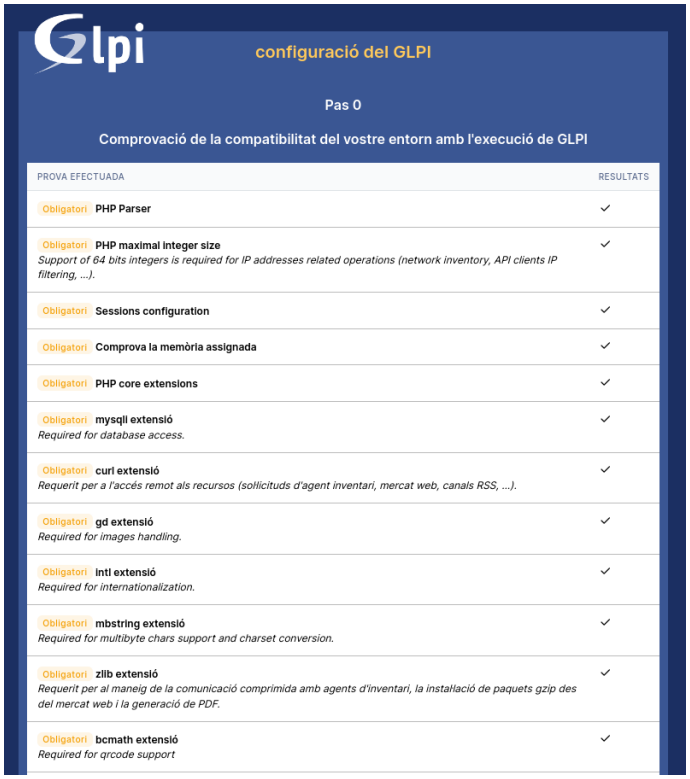

Figura 6: Requisits PHP 1/2

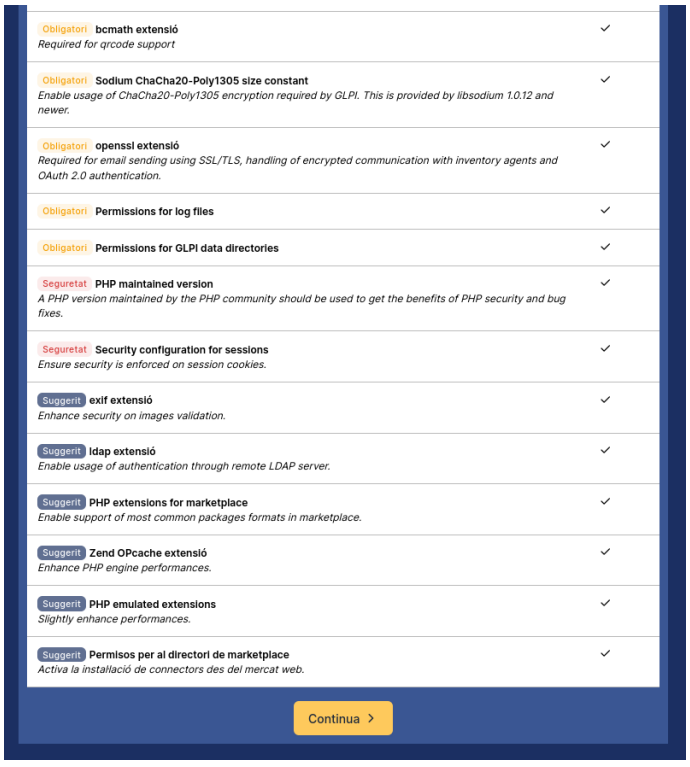

Figura 7: Requisits PHP 2/2

5 - **Configuració de la connexió a la base de dades**:

```
Servidor SQL: localhost
Usuari SQL: usuari
Contrasenya: una_contrasenya_segura  # Definida a l'apartat 2.
```

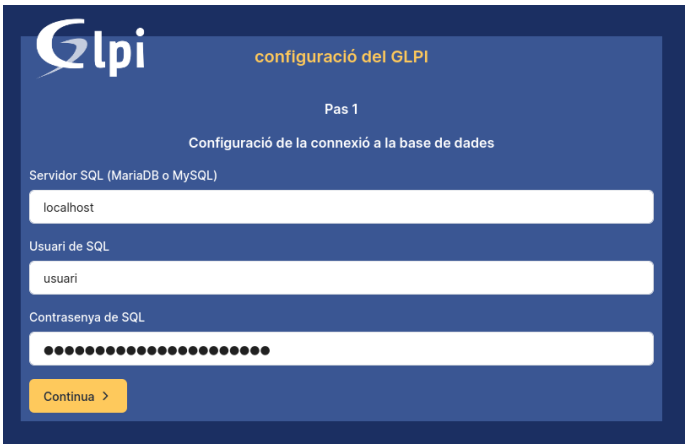

Figura 8: Connexió a la BBDD

Figura 9: Prova de la connexió a la BBDD

6 - **Inicialització de la base de dades**

Figura 10: Inicialització de la base de dades

7 - **Estadístiques**

Figura 11: Estadístiques

8 - **Possibilitat d'acollir-se al servei comercial**

Figura 12: Servei comercial

9 - **Resum i instal·lació**: revisar i prémer *Instal·lar*.

Figura 13: Instal·lació finalitzada

10 - **Accés amb les credencials**: glpi / glpi

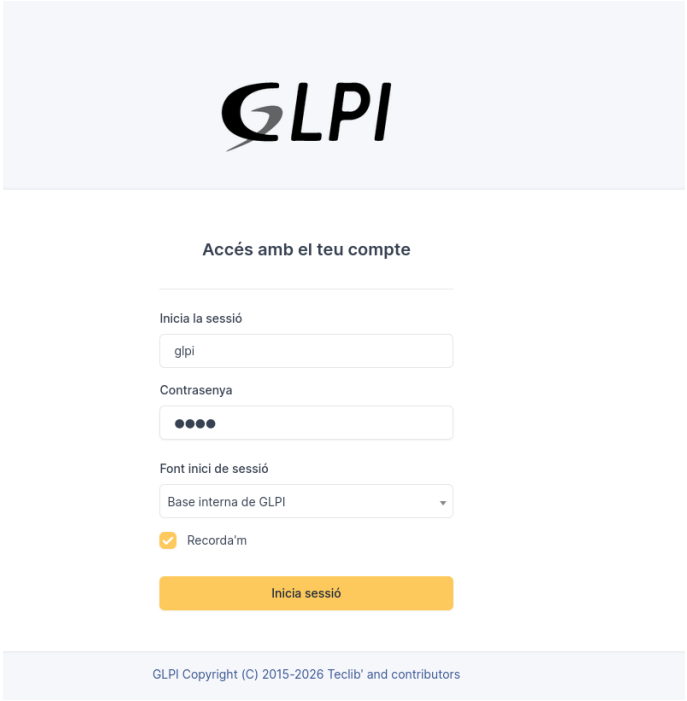

Figura 14: Accés com a Super-Admin

11 - **Tauler de control**

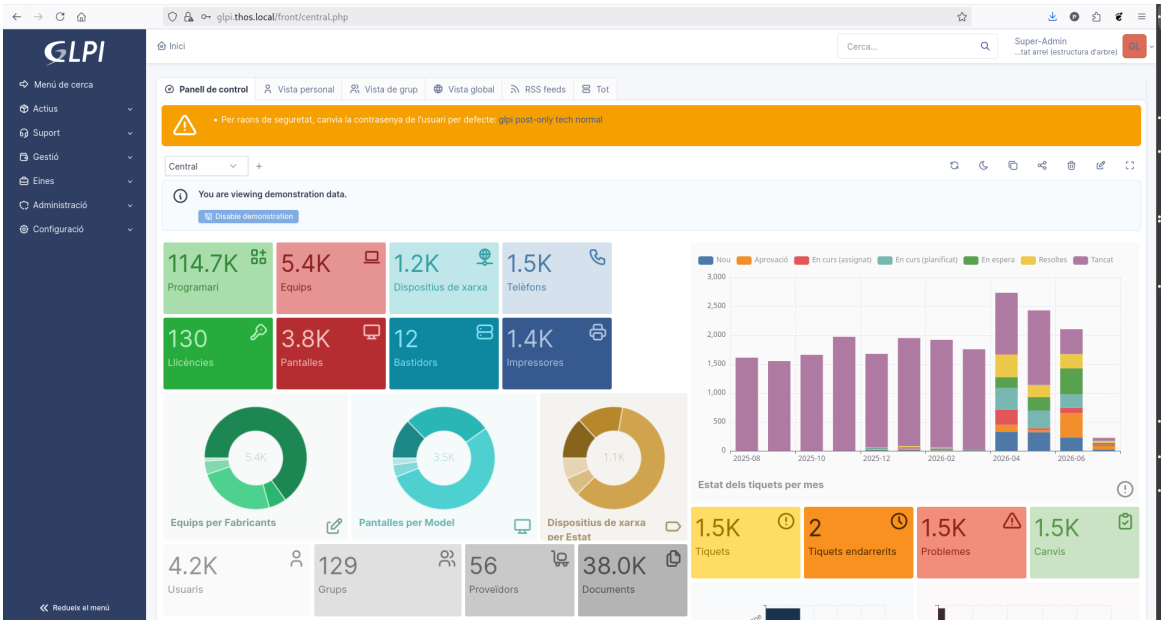

Figura 15: Tauler de control

12 - **Pas de seguretat obligatori després de la instal·lació:**

1. Elimina el fitxer d'instal·lació:

```
sudo rm /var/www/html/glpi/install/install.php
```

2. Canvia les contrasenyes per defecte dels quatre usuaris creats (`glpi`, `tech`, `normal`, `post-only`) des d'*Administració* > *Usuaris*.

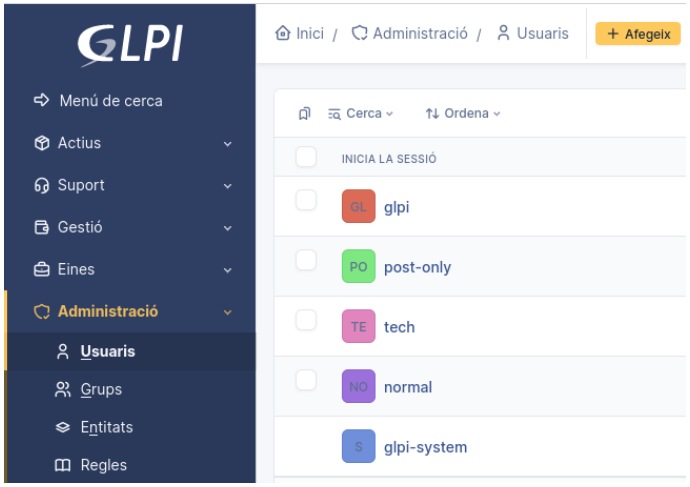

Figura 16: Usuaris

6. Configuració de tasques automàtiques (cron)

GLPI necessita executar tasques automàtiques (notificacions, neteja de la base de dades, sincronitzacions, etc.). Configura un cron que executi l'script `cron.php` cada minut:

```
sudo crontab -u www-data -e
```

Afegeix la línia:

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

7. Connexió amb OCS Inventory

OCS Inventory NG és una eina d'inventari automàtic de maquinari i programari mitjançant agents instal·lats als equips. La integració amb GLPI permet importar i sincronitzar automàticament aquest inventari dins de GLPI, mantenint GLPI com a consola central de gestió.

7.1. Requisits previs

- Un servidor OCS Inventory NG ja instal·lat i funcionant (versió 2.x o superior), amb agents desplegats als equips client.
- El connector oficial `ocsinventoryng` per a GLPI, compatible amb les versions 10.x i 11.x de GLPI.

7.2. Instal·lació del connector OCS Inventory NG

Mou-te a la carpeta temporal

```
cd /tmp
```

Descarrega el connector des del dipòsit oficial:

```
wget -c https://github.com/pluginsGLPI/ocsinventoryng/releases/downl
 ↪  oad/2.1.11/glpi-ocsinventoryng-2.1.11.tar.bz2
```

Descomprimeix

```
sudo tar -xjf glpi-ocsinventoryng-2.1.11.tar.bz2 -C
 ↪  /var/www/html/glpi/plugins/
```

Canvia el propietari de la carpeta

```
sudo chown -R www-data:www-data
 ↪  /var/www/html/glpi/plugins/ocsinventoryng
```

Esborra el fitxer descarregat

```
rm glpi-ocsinventoryng-2.1.11.tar.bz2
```

A GLPI, ves a **Configuració > Connectors** i:

1 - Localitza *OCS Inventory NG* a la llista.

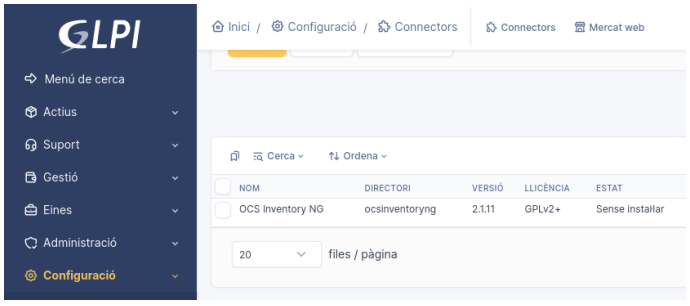

Figura 17: Connector OCS Inventory NG

2 - A la dreta, clica a *Instal·lar*.

3 - Un cop instal·lat, clica a *Activar*.

Figura 18: Connector activat

7.3. Configuració de la connexió amb el servidor OCS

Dins de GLPI, ves a **Eines > OCS Inventory NG** i afegeix un nou servidor OCS amb les dades següents:

Figura 19: Afegeix servidor OCSNG

Camp	Descripció
URL del servidor OCS	p. ex. `http://ocsserver/ocsreports`
Tipus de connexió	Base de dades (per defecte) o API REST
Servidor de la BD OCS	IP o nom del servidor MySQL d'OCS
Nom de la BD OCS	normalment `ocsweb`
Usuari de la BD OCS	usuari amb permisos de lectura sobre `ocsweb`
Contrasenya de la BD OCS	contrasenya de l'usuari anterior

El connector admet dos mètodes de connexió: accés directe a la base de dades d'OCS (mètode tradicional) o connexió a través de l'API REST d'OCS Inventory. El mètode de base de dades segueix sent el més habitual i directe.

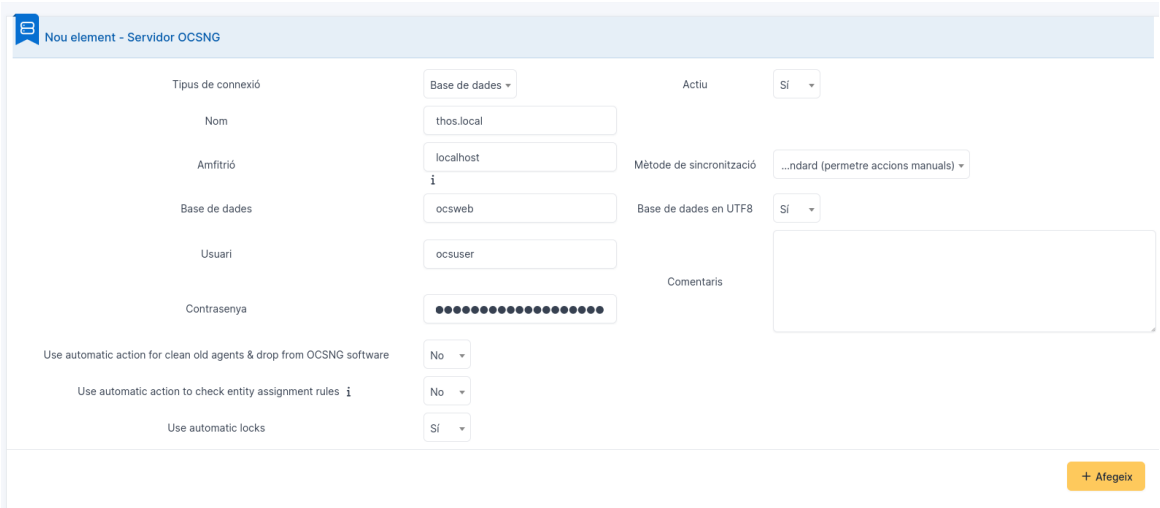

Figura 20: Configuració del servidor

Si s'opta per la connexió directa a la base de dades, cal assegurar-se que el servidor MySQL/MariaDB d'OCS Inventory permet connexions remotes des del servidor GLPI (obrir el port 3306 al tallafocs si els servidors són diferents), i crear un usuari amb permisos de **només lectura** sobre la base `ocsweb`:

```
CREATE USER 'glpi_ocs'@'IP_servidor_GLPI' IDENTIFIED BY
 ↪  'contrasenya_segura';
GRANT SELECT ON ocsweb.* TO 'glpi_ocs'@'IP_servidor_GLPI';
FLUSH PRIVILEGES;
EXIT;
```

Figura 21: Prova de connexió

La prova de connexió fallarà. Edita la base de dades d'OCS Inventory

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

Actualitza el valor a 1

```
UPDATE config SET IVALUE='1' WHERE NAME='TRACE_DELETED';
EXIT;
```

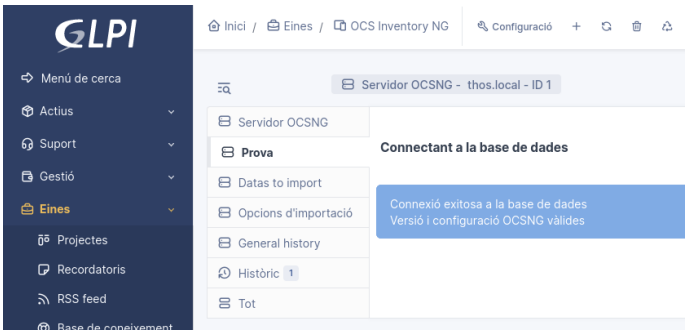

Figura 22: Connexió exitosa

7.4. Regles d'importació

Abans d'importar, és recomanable definir les regles d'assignació a **Configuració > Regles > Regles per a la importació i vinculació d'ordinadors**. Aquestes regles determinen, per exemple:

- A quina entitat de GLPI s'assigna cada equip importat (segons l'etiqueta TAG, el domini, el rang d'IP, etc.).
- Com es vinculen els equips ja existents a GLPI per evitar duplicats (normalment pel número de sèrie o l'adreça MAC).

7.5. Procés d'importació

A **Connectors > OCSNG > Importar nous equips de l'ordinador**:

1. Selecciona el servidor OCS configurat.
2. Tria els equips a importar (es pot filtrar per nom, IP, TAG, etc.).
3. Selecciona les dades a sincronitzar: maquinari, programari, xarxa, etc.
4. Clica a *Importar*.

El connector mostra una interfície amb l'estat dels processos d'importació en curs o finalitzats.

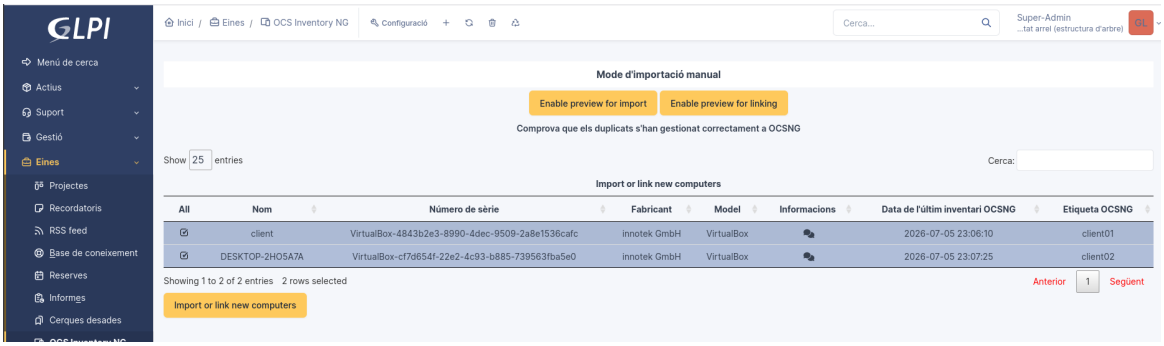

Figura 23: Importació d'equips

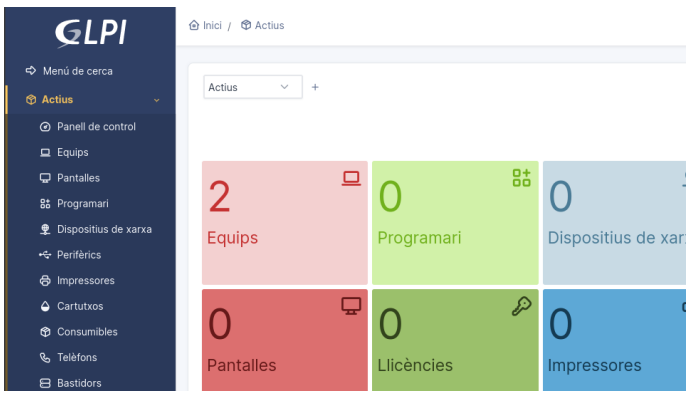

Figura 24: Equips afegits

7.6. Sincronització automàtica

Per mantenir l'inventari sempre actualitzat, es pot configurar una tasca automàtica (a través del cron de GLPI ja configurat al punt 6) que sincronitzi periòdicament els equips ja vinculats. Això es configura a **Connectors > OCSNG > Tasques automàtiques**, on es pot triar la freqüència (horària, diària, setmanal).

> **Nota sobre l'evolució del connector:** GLPI incorpora des de fa diverses versions el seu propi agent natiu (*GLPI Agent*, antic FusionInventory), que pot substituir OCS Inventory si es vol simplificar l'arquitectura a llarg termini. No obstant això, si ja es disposa d'una infraestructura OCS desplegada, el connector `ocsinventoryng` segueix sent la via recomanada per mantenir-la integrada amb GLPI.

8. Configuració dels usuaris des d'LDAP

GLPI permet autenticar i importar usuaris des d'un directori LDAP (Active Directory, OpenLDAP, etc.), evitant haver de crear comptes manualment.

8.1. Comprovació prèvia

Cal assegurar-se que l'extensió `php-ldap` està instal·lada (ja s'ha inclòs al punt 1.1). Es pot verificar amb:

```
php -m | grep ldap
```

Resposta esperada:

```
ldap
```

8.2. Configuració del directori LDAP a GLPI

A GLPI, ves a **Configuració > Autenticació > Directoris LDAP** i clica el botó *Afegeix*.

Figura 25: Afegeix directori LDAP

Els camps principals a omplir són:

Camp	Descripció	Exemple
Nom	Nom descriptiu del directori	`LDAP Institut`
Servidor	IP o nom DNS del servidor LDAP	`ldap.thos.local`
Port LDAP	Port del servei (389 sense xifrar, 636 per a LDAPS)	`389`

Filtre de connexió	Filtre per limitar quins objectes es consideren usuaris	`(objectClass=inetOrgPerson)` o `(objectClass=user)` per a AD
BaseDN	Base de cerca dins l'arbre LDAP	`dc=thos,dc=local`
Compte per a connexió (RootDN)	Compte tècnic amb permís de lectura	`cn=admin,dc=thos,dc=local`
Contrasenya	Contrasenya del compte anterior	---
Camp de login	Login de l'usuari	`uid`

Per a **Active Directory**, normalment el RootDN té la forma `cn=svc_glpi,ou=ServiceAccounts,dc=thos,dc=local` i el filtre de connexió sol ser `(&(objectClass=user)(objectCategory=person))`.

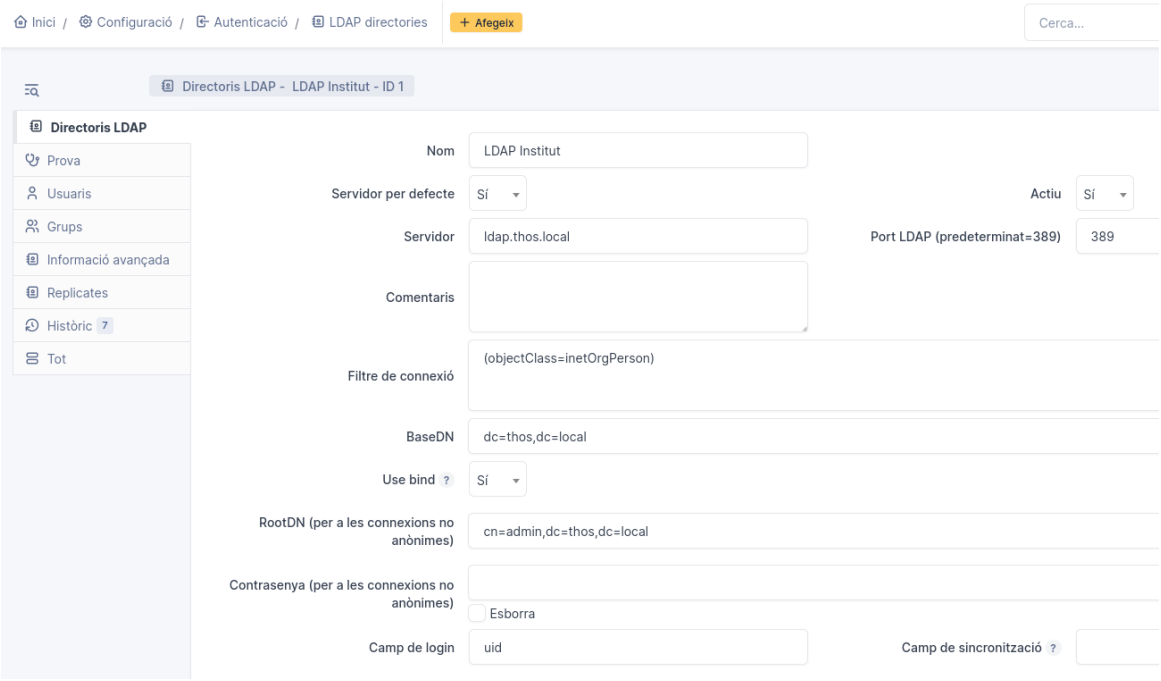

Figura 26: Configuració directori LDAP

8.3. Test de connexió

Un cop desats els paràmetres, GLPI ofereix un botó *Prova* a la mateixa pantalla de configuració, que verifica la connectivitat i les credencials abans de continuar.

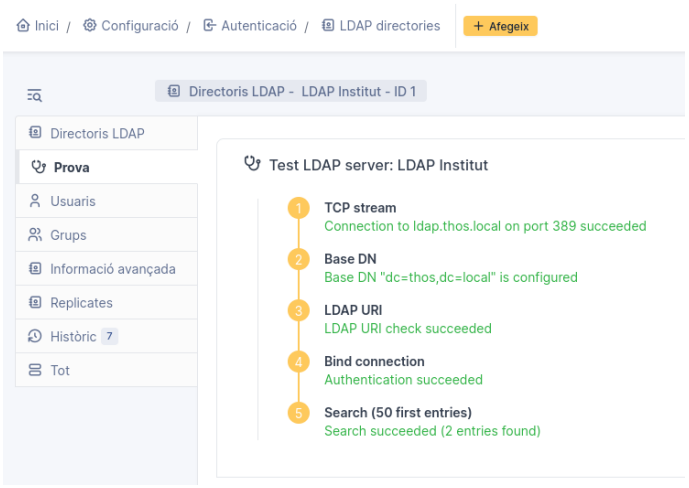

Figura 27: Prova la connexió LDAP

8.4. Mapatge d'atributs

A la pestanya **Usuaris** del directori LDAP configurat, es defineix la correspondència entre els atributs de LDAP i els camps d'usuari de GLPI. Els més habituals són:

Camp de GLPI	Atribut LDAP típic (OpenLDAP)	Atribut LDAP típic (Active Directory)
Login	`uid`	`sAMAccountName`
Nom	`givenName`	`givenName`
Cognom	`sn`	`sn`
Correu electrònic	`mail`	`mail`
Telèfon	`telephoneNumber`	`telephoneNumber`

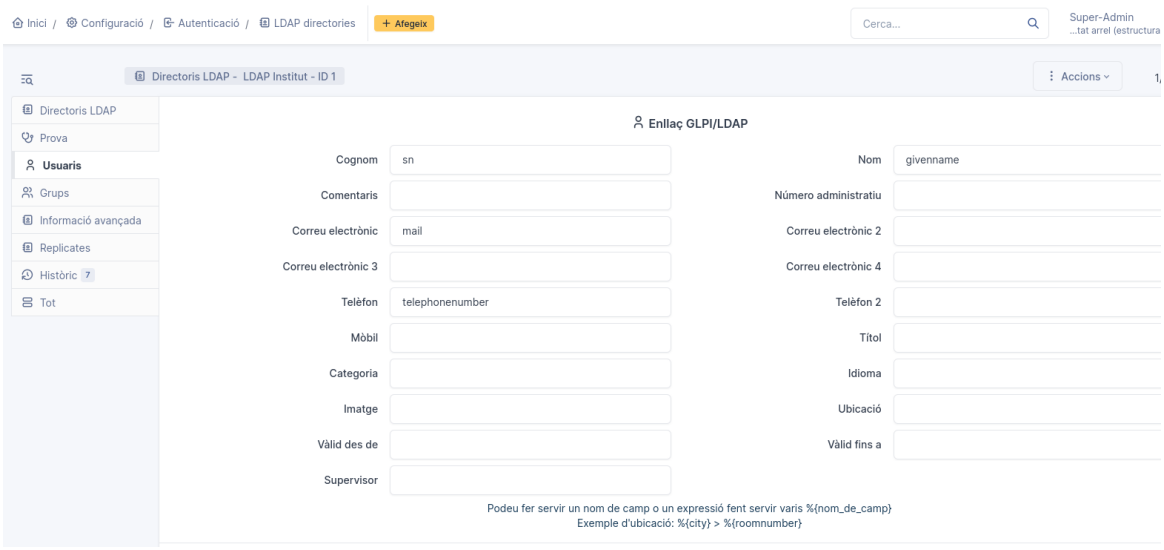

Figura 28: Mapatge d'atributs LDAP

8.5. Importació d'usuaris

Clica a Administració > Usuaris > Enllaç LDAP

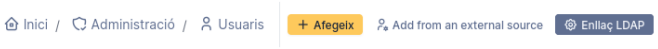

Figura 29: Importa usuaris LDAP

Figura 30: Importa o sincronitza usuaris LDAP

Els usuaris importats podran autenticar-se a GLPI fent servir directament les seves credencials d'LDAP, ja que GLPI delega l'autenticació al directori en lloc de desar contrasenyes pròpies.

Figura 31: Login d'usuari LDAP

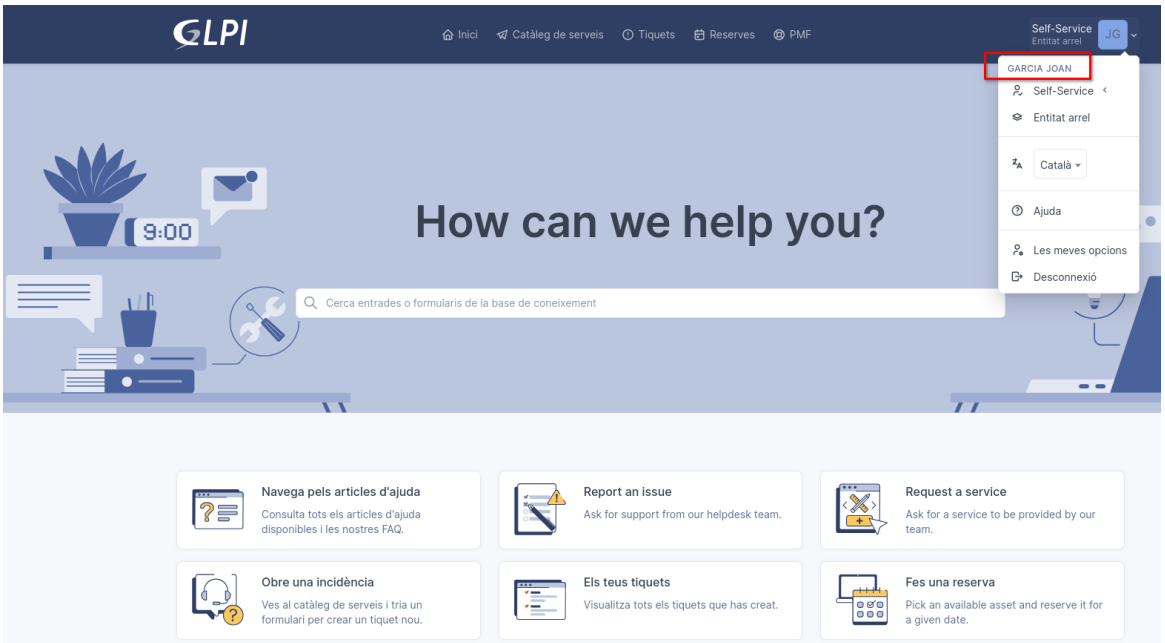

Figura 32: Interfície de l'usuari

8.6. Sincronització automàtica i grups

Per mantenir els usuaris sincronitzats (altes, baixes i canvis d'atributs), es recomana:

- Activar l'opció **Sincronització automàtica** dins la configuració del directori, que utilitzarà el cron de GLPI (ja configurat al punt 6) per actualitzar periòdicament els comptes.
- Si es vol importar també l'estructura de grups de LDAP (per exemple, per assignar perfils o entitats automàticament segons el grup), configurar-ho a **Configuració > Autenticació > Directoris LDAP > Grups LDAP**, indicant el BaseDN de grups i el filtre corresponent (p. ex. `(objectClass=groupOfNames)`).
- Es poden definir **regles d'autenticació** a **Configuració > Regles > Regles per a l'autenticació LDAP** per assignar automàticament perfils, entitats o ubicacions als usuaris importats segons atributs LDAP (per exemple, l'OU a la qual pertanyen).

8.7. Resolució de problemes habituals

- **Error de connexió**: comprovar que el port LDAP (389/636) no està bloquejat pel tallafocs entre el servidor GLPI i el controlador de domini.
- **No es troben usuaris**: revisar el BaseDN i el filtre de cerca; provar primer amb una eina externa com `ldapsearch` per confirmar que la consulta retorna resultats:

```
ldapsearch -x -H ldap://ldap.thos.local -D
↪  "cn=admin,dc=thos,dc=local" -W -b "dc=thos,dc=local"
↪  "(objectClass=inetOrgPerson)"
```

- **Usuaris importats sense correu o dades**: revisar el mapatge d'atributs, ja que pot variar segons l'esquema LDAP del directori d'origen.

9. Resum final

Amb aquesta configuració, el servidor Ubuntu queda amb:

- Un **GLPI** funcional sobre Apache, PHP i MariaDB, amb l'estructura de directoris segura recomanada (configuració, dades i registres fora de l'arrel web pública).
- La **importació automàtica d'inventari** des d'OCS Inventory NG mitjançant el connector oficial, amb regles d'assignació i sincronització periòdica.
- L'**autenticació i importació d'usuaris des de LDAP**, amb mapatge d'atributs i sincronització automàtica per mantenir els comptes actualitzats.

Si en el futur el servidor passa a tenir un nom de domini públic accessible des d'Internet, es pot substituir el certificat autosignat per un certificat emès per una entitat de confiança (per exemple, mitjançant Certbot/Let's Encrypt), reutilitzant el mateix `VirtualHost` de port 443 i només canviant les directives `SSLCertificateFile` i `SSLCertificateKeyFile`.

Versions d'aquest document

- HTML - glpi.html
- PDF - glpi.pdf
- ODT - glpi.odt
- MD - glpi.md