IJO'S & MONKEYS

1. Introducción al proyecto

La ONG **IJO's & Monkeys** tiene como objetivo fundamental unir compromiso social, cuidado del medio ambiente y educación, alineándose con los Objetivos de Desarrollo Sostenible. Nuestra labor se apoya no solo en acciones directas sobre la comunidad y el entorno, sino también en la manera en que la tecnología puede servir de puente para conectar personas, optimizar procesos y garantizar que cada miembro de la ONG tenga acceso seguro y eficiente a la información que necesita.

Para lograr esto, hemos desarrollado un **ecosistema digital integral** que centraliza y organiza todos los recursos de la ONG, pensado para que cada usuario, desde el equipo IT, la secretaría y los voluntarios hasta los veterinarios, disponga de las herramientas necesarias según sus responsabilidades y necesidades. Este ecosistema se apoya en un **servidor AD** que funciona como columna vertebral, gestionando la estructura de usuarios, sus permisos y directivas, incluyendo personalización de escritorios, instalación automática de aplicaciones y control de horarios según turnos.

En torno a esta base, la infraestructura se despliega dentro de un entorno virtualizado con **Proxmox**, protegido por un **router virtual Pfsense**, que actúa como firewall, DNS y servidor DHCP, garantizando la seguridad y disponibilidad de todos los servicios. En la **zona desmilitarizada (DMZ)** se encuentran los servidores de contenedores, administrados centralmente mediante **Portainer**, lo que permite gestionar, actualizar y monitorizar cada servicio de manera eficiente y ordenada.

Cada contenedor cumple una función específica dentro del ecosistema: **Nextcloud** permite abrir las puertas a compartir y sincronizar documentos entre todos los usuarios, con control de acceso según perfiles y disfrutar de todo lo que el usuario image en un servicio infinito en la nube; **Wiki.js** alberga la documentación interna, desde guías de infraestructura hasta información científica, con permisos diferenciados según el tipo de usuario; **GLPI** organiza el inventario de equipos y la gestión de incidencias, asegurando que los problemas informáticos se resuelvan rápidamente; **Rocket.Chat** conecta al equipo a través de chats generales y privados, incluyendo canales de alertas y comunicación por grupos; **Apache Guacamole** ofrece acceso remoto seguro a los equipos para que el equipo IT pueda asistir a los usuarios a distancia; un **servidor de correo** garantiza la comunicación formal y rápida dentro de la ONG, permitiendo enviar notificaciones, alertas y correos oficiales a cada usuario, integrándose de manera transparente con el resto del ecosistema; un **FTP seguro** permite el intercambio confidencial de archivos, mientras que el **servidor web cifrado** expone la identidad de la ONG y ofrece un chat comunitario en tiempo real para la interacción pública. Finalmente, un **servidor de backups** con **TrueNAS** asegura que toda la información crítica esté protegida y sea recuperable ante cualquier contingencia.

Este ecosistema está diseñado para funcionar de manera integrada y automatizada. Cada usuario recibe un entorno adaptado a su rol, con las aplicaciones necesarias preinstaladas y accesos controlados, lo que permite trabajar de manera eficiente y segura. Al mismo tiempo, toda la infraestructura refuerza la misión de la ONG, demostrando cómo la tecnología puede ser un aliado poderoso para conectar, organizar y potenciar la acción social y medioambiental.

El presente documento tiene como propósito **detallar la planificación, implementación y funcionamiento de este ecosistema digital**, sirviendo

como guía para la gestión interna, referencia técnica y base para futuras mejoras, mostrando cómo la tecnología puede convertirse en un instrumento para amplificar el impacto de IJO's & Monkeys.

2. Sobre la ONG IJO's & Monkeys

IJO's & Monkeys nació de un impulso simple pero poderoso: **unir alegría y propósito**, conectar personas con la naturaleza y con la sociedad, y ofrecer un espacio donde el compromiso social se viviera con entusiasmo, creatividad y positividad. A primera vista, nuestra ONG podría parecer solo un grupo de "monos" jugando y divirtiéndose, pero detrás de esa fachada se encuentra una intención profunda: cada acción, cada proyecto y cada interacción refleja un esfuerzo consciente por generar un impacto real, sustentable y significativo. Somos un organismo que late entre la diversión y la responsabilidad, entre la risa fácil y la reflexión silenciosa, consciente de que la felicidad y la melancolía pueden coexistir.

Nuestra **identidad visual** es un espejo de esta filosofía dual. El logo, aparentemente un plátano, encierra mucho más de lo que se percibe a simple vista. Con un poco de atención se revela una sonrisa, una expresión de positividad y bienvenida que invita a todos a participar y sentir la alegría de la comunidad. Pero la forma ascendente del plátano también es un símbolo de superación: un camino que se eleva hacia metas codiciadas, que no está exento de desafíos ni de momentos oscuros. La base negra representa ese túnel oscuro, esos instantes de incertidumbre, de soledad o de agotamiento emocional, ese vacío silencioso que todos cargamos. Y sin embargo, a medida que el plátano asciende, el degradado de verdes dibuja un sendero lleno de esperanza, de esfuerzo recompensado, un tránsito sutil y alegre hacia la cima que todos buscamos, aunque sepamos que detrás de cada logro hay cicatrices que no siempre se ven.

El color suplementario brilla como un sol tímido sobre esta trayectoria: un destello de energía y optimismo que ilumina los momentos grises, aunque su intensidad recuerde que la luz nunca es absoluta y que incluso en la alegría hay fragilidad. La tipografía **Cocogoose**, con sus curvas desenfadadas y su carácter carismático, aporta ligereza y accesibilidad, y al mismo tiempo nos recuerda que la apariencia alegre puede coexistir con un interior más complejo, más roto, más humano.

Todo esto no es solo estética: **nuestra identidad de marca se aplica en cada interacción**, en cada documento, en cada recurso visual de la ONG. Desde la paleta de colores que guía los diseños de Figma hasta el uso de tipografía y logotipo en nuestros canales, reflejamos la filosofía de IJO's & Monkeys: transmitir alegría, vitalidad y positividad, mientras reconocemos y abrazamos nuestras sombras internas. Las imágenes, los gradientes, los espacios en blanco y los elementos gráficos trabajan juntos para crear una experiencia donde la esperanza y la melancolía conviven, donde cada miembro puede sentirse inspirado y a la vez comprendido en su humanidad compleja.

En este sentido, IJO's & Monkeys es más que una ONG; es un **ecosistema emocional y social**, un lugar donde la alegría y

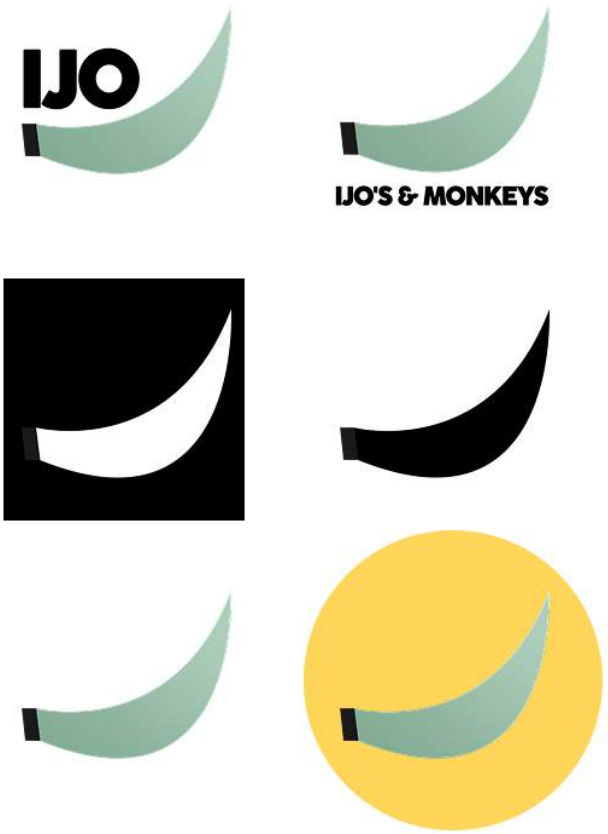
la tristeza no son opuestos, sino capas que se superponen, generando profundidad, significado y conexión. Nuestro trabajo con la comunidad, nuestros proyectos medioambientales y educativos, y nuestro compromiso social, se ven reflejados en cada detalle de nuestra marca, recordándonos que **la belleza verdadera nace de la aceptación de todas las emociones**, de los contrastes y de los matices.

Así, cada vez que alguien observa nuestro logo, percibe más que un plátano sonriente. Ve una historia de esfuerzo y resiliencia, de incertidumbre que se transforma en caminos infinitos de posibilidad. Ve un destello de luz que brilla sobre la oscuridad, una invitación a participar en algo mayor, y al mismo tiempo un guiño íntimo a la fragilidad que nos hace humanos. En IJO's & Monkeys, la alegría es contagiosa, pero también sabemos que detrás de cada sonrisa hay historias que no siempre se cuentan, y que esa profundidad es lo que nos conecta de manera genuina con nuestra comunidad y con el mundo que queremos cuidar.


IJO'S & MONKEYS


IJO
Somos IJO
ONG
especializada
en todo tipo
de monos.
tel: 000 000 000 | mail: info@ijo.org


IJO' s & Monkeys
ESTOY
ROTO
POR
DENTRO
Y ME ESTOY
MURIENDO.



3. Arquitectura general del ecosistema tecnológico

El ecosistema tecnológico de **IJO's & Monkeys** nace de la necesidad de unir orden, eficiencia y corazón. En una organización donde cada minuto puede marcar la diferencia en la vida de un animal, la infraestructura no puede ser un obstáculo: debe ser una aliada silenciosa. Todo el entorno ha sido

concebido bajo una premisa clara: ofrecer estabilidad, seguridad y flexibilidad, con recursos adaptados a cada función dentro de la ONG.

Servidores: el núcleo del sistema

El corazón del ecosistema late en tres servidores cuidadosamente seleccionados y configurados, cada uno con un papel claro en el entramado digital de la organización.

Servidor de Directorio Activo (AD - Windows Server)

Este servidor es la columna vertebral del entorno: gestiona usuarios, políticas, autenticaciones y servicios compartidos. Es el punto de anclaje que mantiene cohesionada la red y define la identidad digital de cada miembro de la ONG.
Se ha optado por **Windows Server 2019** por su estabilidad, integración con entornos mixtos y facilidad de administración.

Componentes recomendados:

- CPU: **Intel Xeon Silver 4310** **(2.1 GHz, 12 cores)**: equilibrio entre rendimiento y eficiencia para manejar múltiples peticiones de autenticación y políticas simultáneas.
- RAM: **32 GB DDR4 ECC**: suficiente para mantener en memoria las estructuras del AD, DNS, GPOs y la carpeta compartida sin cuellos de botella.
- Almacenamiento: **2 SSD NVMe de 1 TB en RAID 1**: velocidad y redundancia, garantizando integridad ante fallos.
- Sistema: **Windows Server 2019 Standard (GUI)**, configurado con roles de **Active Directory**, **DNS** y **File Server**.

En él se aloja también una carpeta de red compartida, que contiene los programas comunes, scripts de despliegue, fondos de pantalla corporativos, imágenes de las GPOs y la intranet interna. Es un punto de encuentro entre orden y funcionalidad.

Servidor de Servicios (SRV-CONTAINERS)

El segundo servidor se encarga de alojar todos los servicios de la ONG, desde las comunicaciones internas hasta el almacenamiento en la nube. Para garantizar su portabilidad, escalabilidad y mantenimiento, todos los servicios se han desplegado en **contenedores Docker** orquestados con **Portainer** haciendo uso de **stacks** para el despliegue y gestión.
Entre los servicios activos destacan:

- **Nextcloud**, para la sincronización de documentos internos, compartir archivos y acceder al correo entre otras muchas cosas.
- **Rocket.Chat**, canal principal de comunicación entre departamentos.
- **GLPI Agent** y **GLPI Server**, para la gestión de inventario y soporte técnico.
- **Mail Server** (basado en Postfix y Dovecot), proporcionando cuentas de correo personalizadas bajo el dominio interno.
- **PortalAD:** portal creado por y para IJO's & Monkeys. Permite crear usuarios y asignarles un departamento mediante una interfaz web.
- **Wikijs:** documentación interna de la empresa con permisos y visibilidad controlada.
- **Apache guacamole:** asistencia telemática y centralizada.

Componentes del servidor:

- **CPU: AMD EPYC 7302P (16 cores)**: sobresaliente rendimiento multihilo ideal para la virtualización ligera y la contenedorización.
- **RAM: 64 GB DDR4 ECC**: margen suficiente para ejecutar múltiples contenedores simultáneamente sin degradación del rendimiento.
- **Almacenamiento: 2 SSD NVMe de 2 TB en RAID 1 + HDD de 4 TB para logs y backups locales**.
- **Sistema: Ubuntu Server con Docker y Docker Compose**, configurado para aislar servicios y facilitar despliegues automatizados.

La elección de un entorno Linux responde tanto a la eficiencia en recursos como a la seguridad y control granular que ofrece en entornos productivos.

Servidor NAS / Backup (SRV-BACKUP)

El tercer servidor cumple el papel de guardián silencioso de los datos. Su función es doble: almacenar información importante y realizar copias de seguridad **incrementales** de los equipos, así como **copias completas** en intervalos definidos.
Usa **rsync** y **BorgBackup** para optimizar el espacio y garantizar integridad en las versiones de archivos.

Componentes del servidor:

- **CPU: Intel Xeon E-2236 (6 cores, 3.4 GHz)**: rendimiento sólido y estable.
- **RAM**: **16 GB DDR4 ECC**.
- **Almacenamiento**: **4 discos HDD de 8 TB en RAID 10**, priorizando fiabilidad y velocidad en lecturas/escrituras.

- **Sistema**: **TrueNAS SCALE**, que aporta interfaz gráfica, snapshots ZFS y compatibilidad nativa con backups automáticos.

Un **SAI (Sistema de Alimentación Ininterrumpida)** complementa esta infraestructura, asegurando que los servidores tengan tiempo suficiente para apagarse de forma controlada ante un corte eléctrico, evitando corrupción de datos y garantizando continuidad operativa.

Puestos de trabajo: tecnología al servicio de cada función

Cada equipo dentro de la ONG dispone de un hardware pensado para que la tecnología no limite su labor, sino que la potencie.

Equipo IT

El departamento técnico necesita máquinas versátiles y potentes, capaces de soportar virtualización, edición multimedia y tareas de soporte remoto.

Configuración ideal:

- **CPU**: **AMD Ryzen 9 7900X** **(12 cores)**.
- **RAM**: **64 GB DDR5**.
- **Almacenamiento**: **SSD NVMe de 2 TB + HDD 4 TB**.
- **GPU**: **NVIDIA RTX 4060 Ti**, para tareas de renderizado, diseño y edición de vídeo.

Esta configuración permite ejecutar máquinas virtuales, levantar entornos de prueba y producir contenido audiovisual para campañas y redes sociales.

Secretaría

Aquí la fiabilidad y la agilidad son clave. No necesitan potencia bruta, sino equipos que respondan rápido a la multitarea administrativa.

Configuración:

- **CPU**: Intel Core i5-13400.
- **RAM**: 16 GB DDR4.
- **Almacenamiento**: SSD NVMe de 1 TB.

Un sistema fluido y silencioso, ideal para tareas de ofimática, gestión documental y comunicación interna.

Veterinarios

Los equipos de veterinaria deben ser capaces de ejecutar software médico y programas de gestión animal sin interrupciones.

Configuración:

- **CPU**: AMD Ryzen 7 7700.
- **RAM**: 32 GB DDR5.
- **Almacenamiento**: SSD NVMe 2 TB.
- **GPU**: NVIDIA GTX 1660 Super, suficiente para renderizar imágenes y análisis visuales.

Voluntarios

Necesitan equipos ligeros, portátiles y resistentes que les permitan moverse entre las instalaciones o trabajar desde campo.

Propuesta:

- Portátil **Dell XPS 13** **o** **Lenovo ThinkPad T14s**, con procesador i7, 16 GB RAM, SSD 1 TB y batería de larga duración.

Virtualización y red

Todo el entorno ha sido **virtualizado en Proxmox VE**, una plataforma que actúa como base sólida sobre la que se despliegan las máquinas virtuales. Su única función es la de **alojar y ejecutar los sistemas virtuales**, delegando el control de red al router virtual **pfSense**, encargado de la gestión avanzada del tráfico.

El router **pfSense** cumple varias funciones críticas:

- Actúa como **firewall** para proteger el entorno interno.
- Hace de **servidor DNS**, resolviendo nombres dentro del dominio.
- Asigna direcciones IP mediante **DHCP**, asegurando control total de las asignaciones.
- Divide el entorno en redes lógicas:

    1. **DMZ (192.168.1.0/24)**: red aislada para servidores, ofreciendo un nivel adicional de seguridad. Esta zona “desmilitarizada” permite exponer ciertos servicios al exterior sin comprometer la red interna.

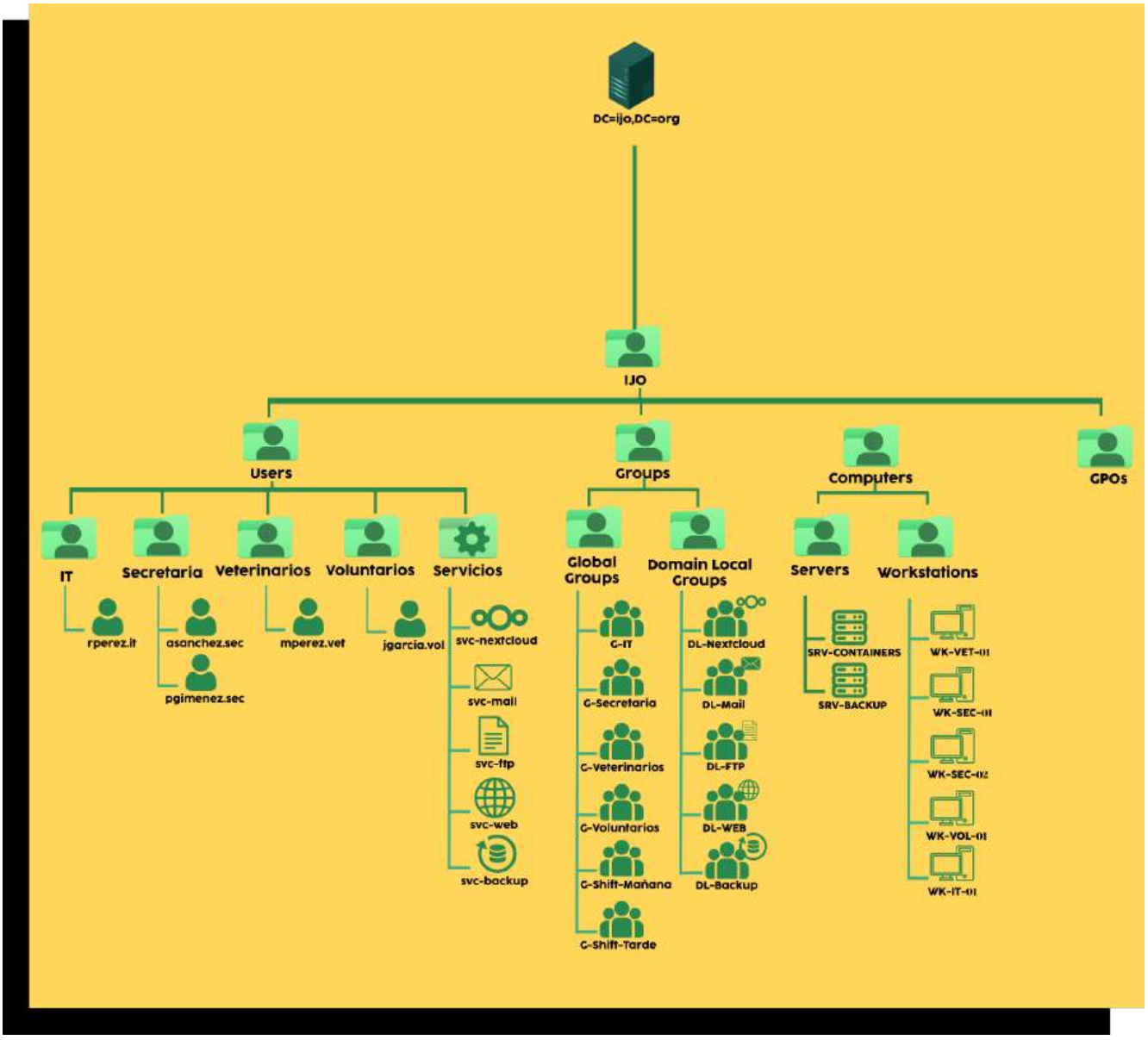
2. **LAN (192.168.2.0/24)**: red interna para los equipos de trabajo.

3. **WAN (10.10.16.x/24)**: interfaz externa con salida a Internet.

Los servidores cuentan con **IP fija dentro de la DMZ**, garantizando que los servicios sean accesibles y estables.

La estructura de Active Directory

El Active Directory es el cerebro lógico de todo el sistema. Bajo el dominio **DC=ijo,DC=org**, se organiza un conjunto de **Unidades Organizativas** (OUs) que permiten segmentar con precisión los distintos elementos de la red.


DC=ijo,DC=org
IJO
Users
Groups
Computers
GPOs
IT
Secretaria
Veterinarios
Voluntarios
Servicios
rperez.it
asanchez.sec
pgimenez.sec
mperez.vet
jgarcia.vol
svc-nextcloud
svc-mail
svc-ftp
svc-web
svc-backup
Global Groups
Domain Local Groups
G-IT
G-Secretaria
G-Veterinarios
G-Voluntarios
G-Shift-Mañana
G-Shift-Tarde
DL-Nextcloud
DL-Mail
DL-FTP
DL-WEB
DL-Backup
Servers
Workstations
SRV-CONTAINERS
SRV-BACKUP
WK-VET-01
WK-SEC-01
WK-SEC-02
WK-VOL-01
WK-IT-01

- En la raíz se encuentra la **OU=IJO**, matriz de toda la estructura. Dentro de ella descansan:

  - **OU=Users**: contiene las subunidades por departamentos: **IT**, **Secretaria**, **Veterinarios**, **Voluntarios** y una **OU=Servicios**, que aloja las **cuentas de servicio** utilizadas por aplicaciones (como Nextcloud, Rocket.Chat, Mail…). Cada usuario de servicio posee los permisos mínimos necesarios para evitar brechas de seguridad.

  - **OU=Groups**: subdividida en:

    - **OU=Global Groups (G-)**, que representan grupos lógicos basados en el personal y turnos. Ejemplo: **G-IT**, **G-Secretaria**, **G-Veterinarios**, **G-Voluntarios**, **G-Shift-Mañana**, **G-Shift-Tarde**. Estos grupos son usados para asignar políticas o permisos comunes a usuarios de un mismo rol o franja horaria.

    - **OU=Domain Local Groups (DL-)**, que agrupan permisos específicos ligados a servicios: **DL-Mail**, **DL-Nextcloud**, **DL-Backup**, **DL-FTP, DL-WEB**. Aunque en entornos Windows suelen servir para dar acceso a recursos locales, en este caso su función es representar los accesos que cada servicio Linux otorga mediante LDAP, reforzando la coherencia de la autenticación centralizada.

  - **OU=Computers**: dividida a su vez en:

- **OU=Servers**, donde se registran las máquinas virtuales **SRV-CONTAINERS** y **SRV-BACKUP**.

- **OU=Workstations**, con los equipos físicos de cada área (**WK-IT-01**, **WK-SEC-01**, **WK-VET-01**, etc.).

- **OU=GPOs**: guarda las políticas de grupo que moldean la experiencia de usuario y las reglas de seguridad. Entre ellas:

  - **Asignación de fondos de pantalla** personalizados por departamento.
  - **Limitaciones horarias** para el personal con turno de mañana o tarde.
  - **Instalación automática** de aplicaciones esenciales (GLPI Agent, Nextcloud Files, Rocket.Chat).

Esta estructura jerárquica mantiene el orden, facilita la administración y reduce el riesgo de errores humanos, al tiempo que deja espacio para crecer sin caos.

4. Servicios y aplicaciones

Todos los servicios principales de **IJO's & Monkeys** se ejecutan en el **SRV-CONTAINERS**, el corazón operativo de la ONG.
Este servidor orquesta los contenedores que dan vida al ecosistema digital: desde la nube interna hasta la wiki, desde el sistema de incidencias hasta el correo institucional.

Cada contenedor se ejecuta de forma **aislada, cifrada y controlada**, utilizando certificados generados desde la **Autoridad Certificadora (CA)** interna, denominada **IJO_CA**.
A partir de ella, se emiten certificados individuales para cada servicio, asegurando que todas las conexiones dentro de la red, ya sean entre servidores o con los clientes, estén **protegidas por TLS/SSL**.
La autenticación se gestiona de manera **centralizada a través del Active Directory**, utilizando el atributo **sAMAccountName** como identificador único. Solo el **cliente de correo** emplea un formato distinto para la autenticación (usuario@ijo.org), por compatibilidad con los protocolos SMTP e IMAP.

El script solo pide el **nombre del servicio** y genera automáticamente todos los certificados necesarios, guardándolos en /srv/certs/.

Así, todos los docker-compose apuntan a esa ruta para usar los certificados sin configuración manual.

```
#!/bin/bash

# ========================

# Variables principales

# ========================

# Ruta base donde se guardarán los certificados

BASE_DIR="/srv/certs"

# Archivos de la CA

CA_DIR="/srv/IJO_CA"
```

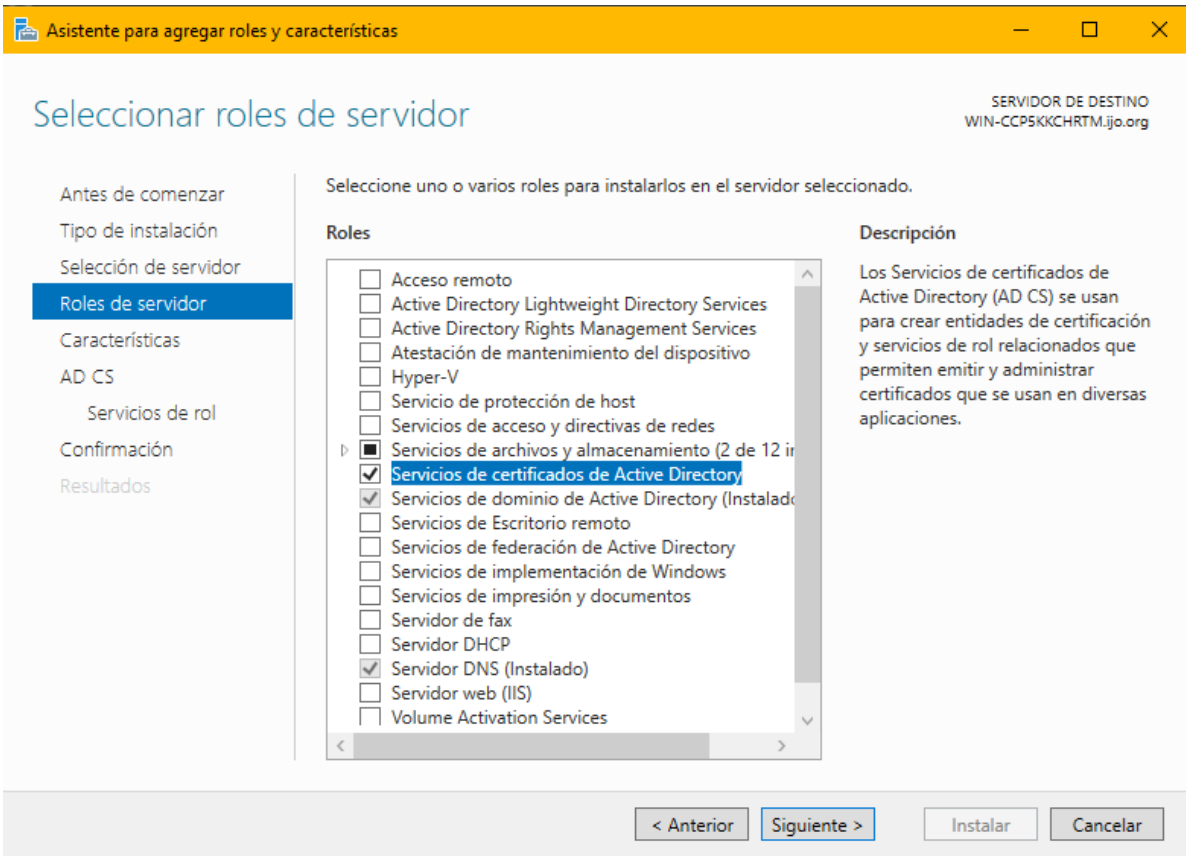
```
CA_KEY="$CA_DIR/rootCA.key"

CA_CRT="$CA_DIR/rootCA.crt"

# Algoritmo y tamaño de clave

KEY_ALGO="rsa"

KEY_SIZE=2048



# ========================

# Pedir nombre del certificado / servicio

# ========================

read -p "Introduce el nombre del servicio para el certificado (ej: servidor1): "
NAME

# Crear carpetas específicas para este servicio

SERVICE_DIR="$BASE_DIR/$NAME"

CSR_DIR="$SERVICE_DIR/csr"

CRT_DIR="$SERVICE_DIR/crt"

COMBINED_DIR="$SERVICE_DIR/combined"

mkdir -p "$CSR_DIR" "$CRT_DIR" "$COMBINED_DIR"
```

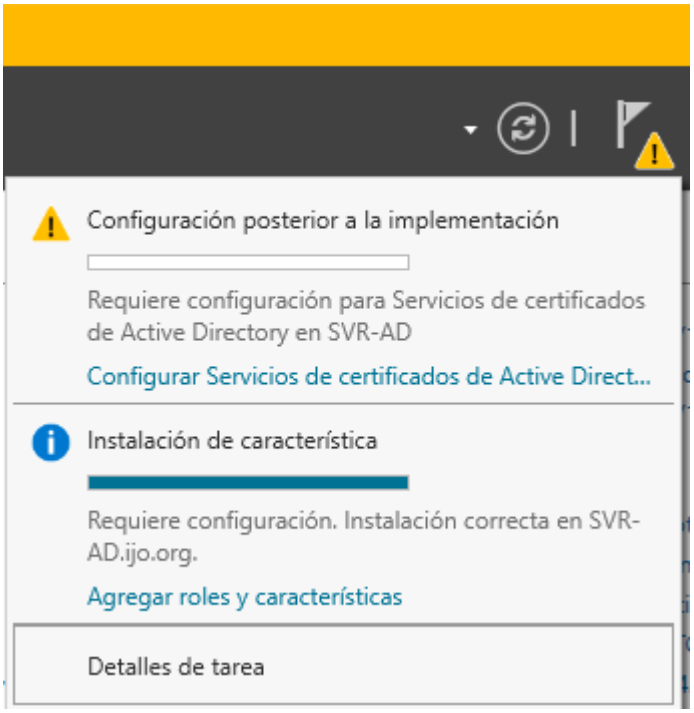
```
# Definir paths de los archivos del nuevo certificado
KEY_FILE="$SERVICE_DIR/$NAME.key"
CSR_FILE="$CSR_DIR/$NAME.csr"
CRT_FILE="$CRT_DIR/$NAME.crt"
COMBINED_FILE="$COMBINED_DIR/$NAME.pem"


# ==========================
# Generar clave privada
# ==========================
echo "Generando clave privada en $KEY_FILE..."
openssl genrsa -out "$KEY_FILE" $KEY_SIZE
# ==========================
# Generar CSR (Certificate Signing Request)
# ==========================
echo "Generando CSR en $CSR_FILE..."
openssl req -new -key "$KEY_FILE" -out "$CSR_FILE" -subj "/CN=$NAME"
# ==========================
```

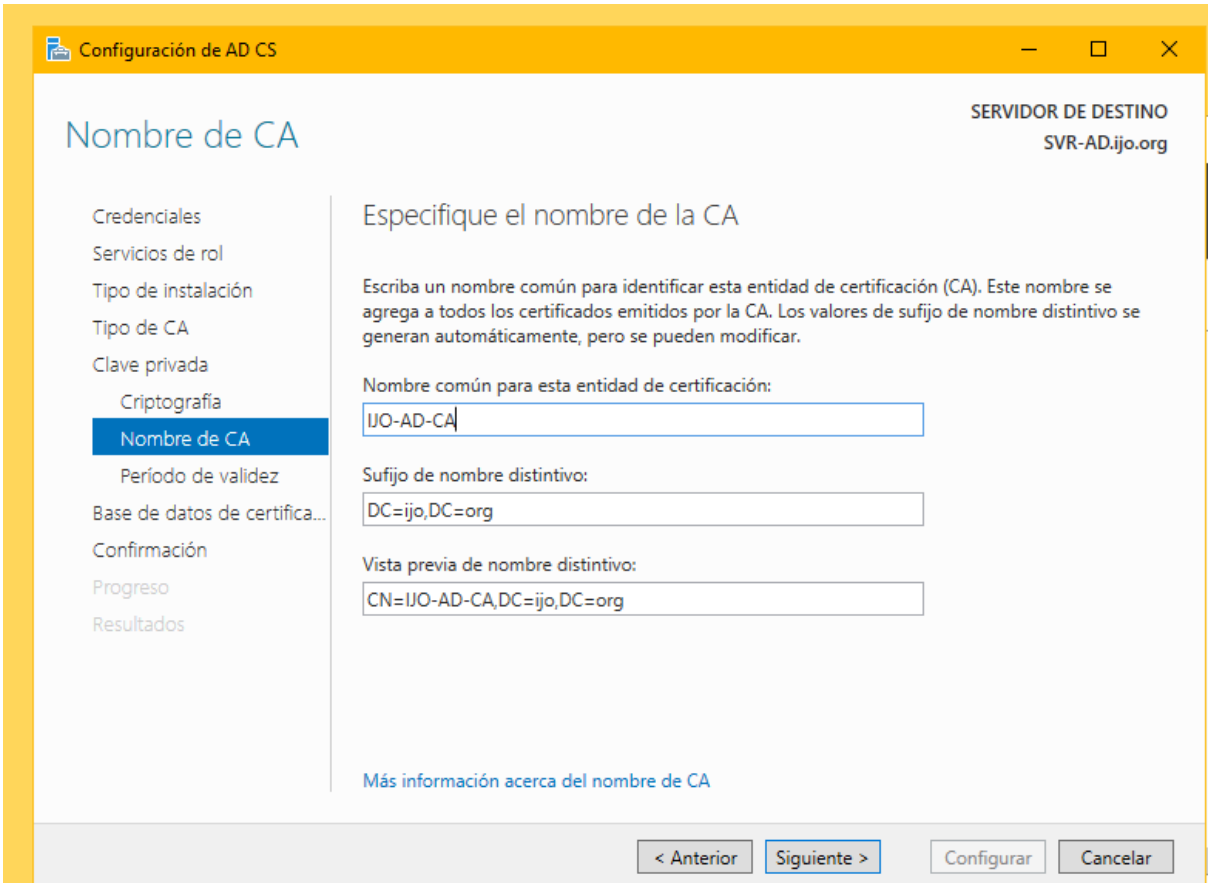
```
# Firmar CSR con CA para generar CRT

# ========================

echo "Generando certificado firmado en $CRT_FILE..."

openssl x509 -req -in "$CSR_FILE" -CA "$CA_CRT" -CAkey "$CA_KEY"
-CAcreateserial -out "$CRT_FILE" -days 365 -sha256

# ========================

# Crear archivo combinado (key + crt + CA crt)

# ========================

echo "Creando archivo combinado en $COMBINED_FILE..."

cat "$KEY_FILE" "$CRT_FILE" "$CA_CRT" > "$COMBINED_FILE"

echo "¡Proceso completado!"

echo "Clave privada: $KEY_FILE"

echo "CSR: $CSR_FILE"

echo "Certificado: $CRT_FILE"

echo "Archivo combinado: $COMBINED_FILE"
```

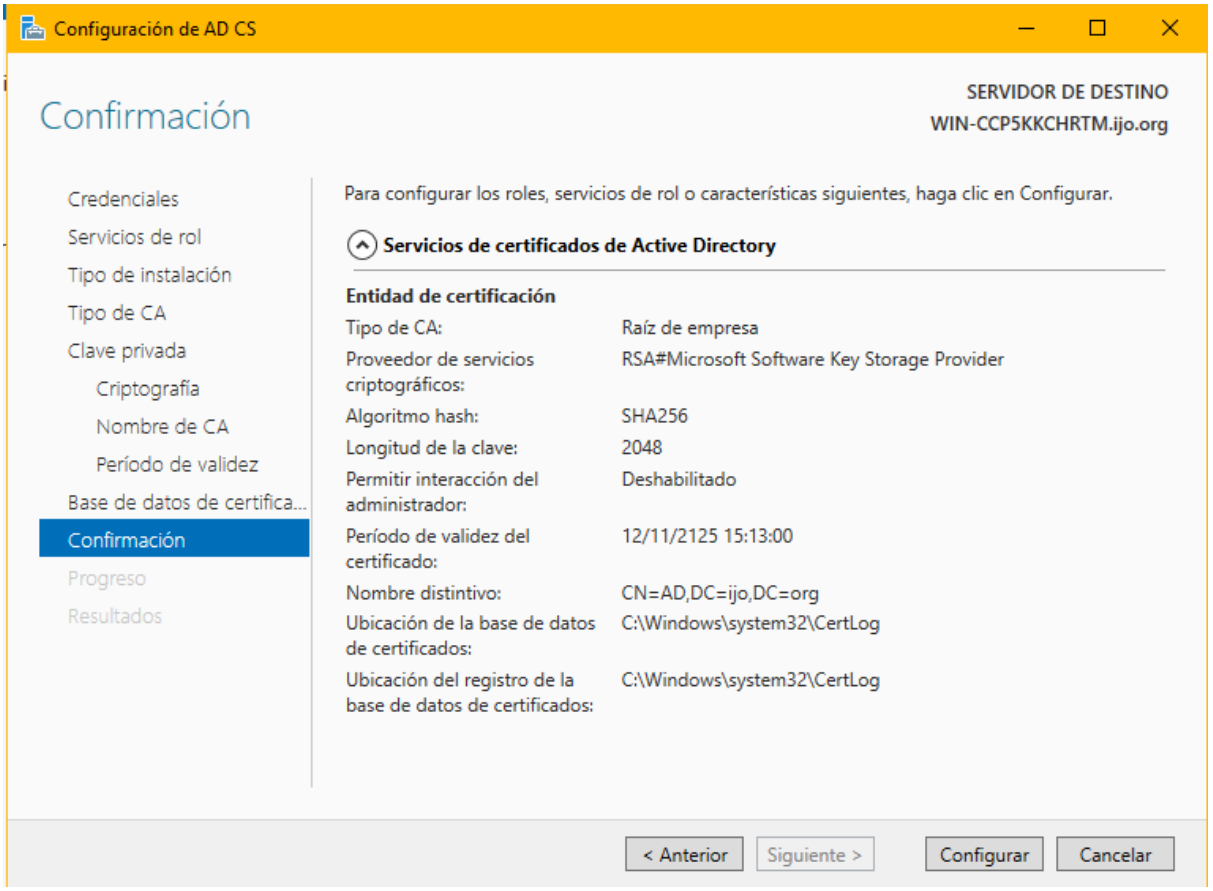
Exceptuando el servicio **PortalAD**, todos los contenedores se comunican con el directorio activo mediante **LDAPS (LDAP sobre TLS)**, un canal cifrado que protege las credenciales y consultas.

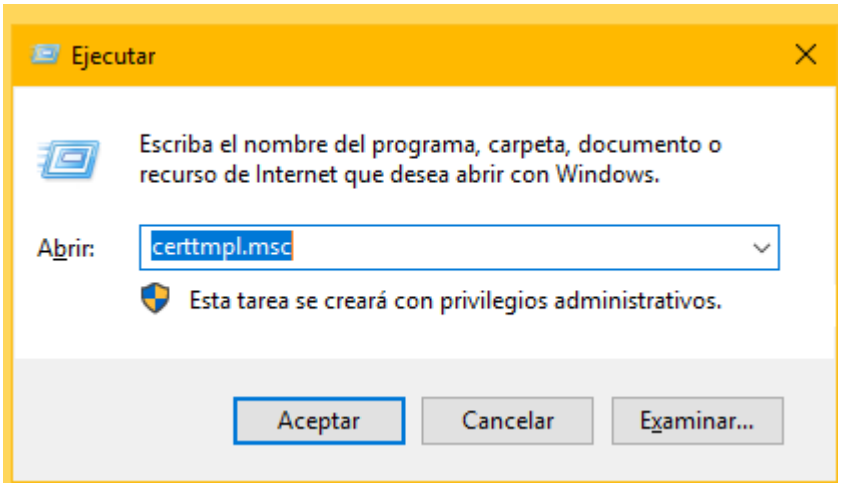
Para habilitarlo en nuestro AD, es necesario seguir estos pasos:

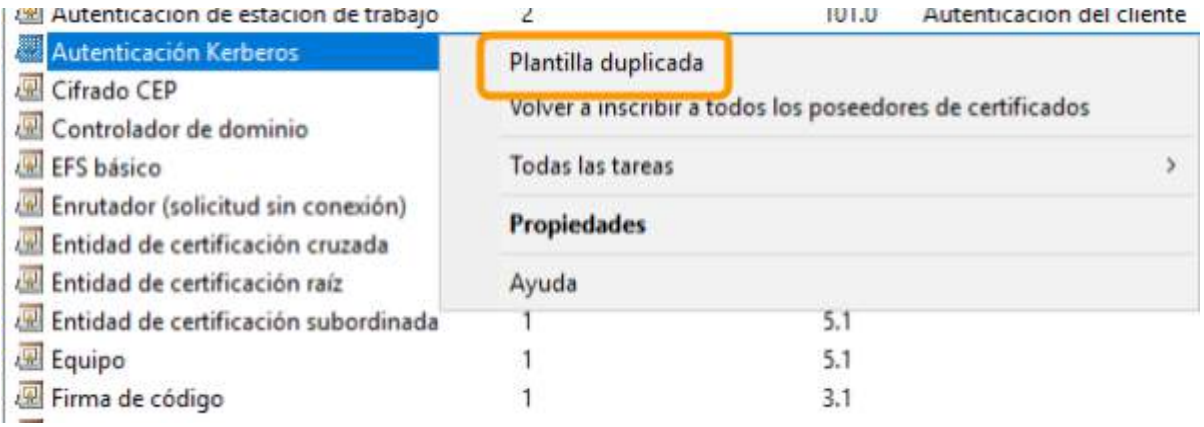


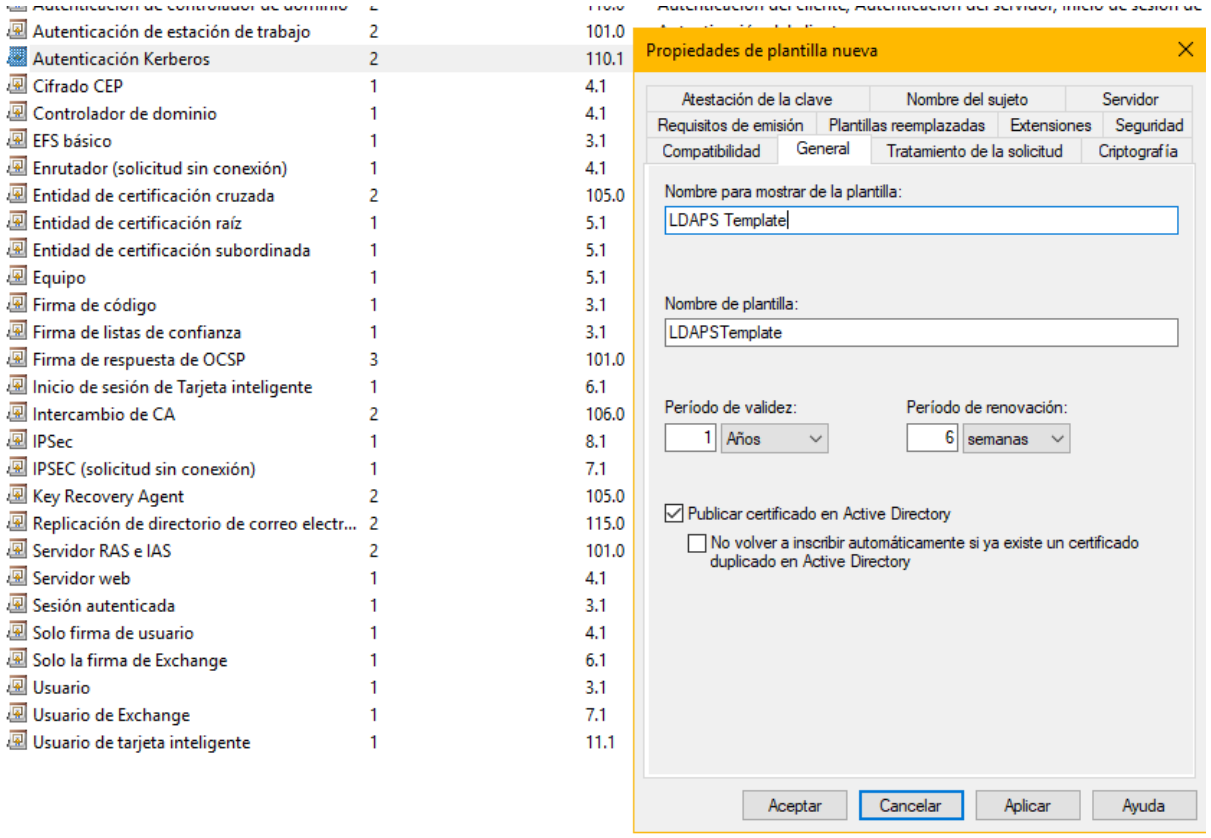

Configuración posterior a la implementación
Requiere configuración para Servicios de certificados de Active Directory en SVR-AD
Configurar Servicios de certificados de Active Direct...
Instalación de característica
Requiere configuración. Instalación correcta en SVR-AD.ijo.org.
Agregar roles y características
Detalles de tarea

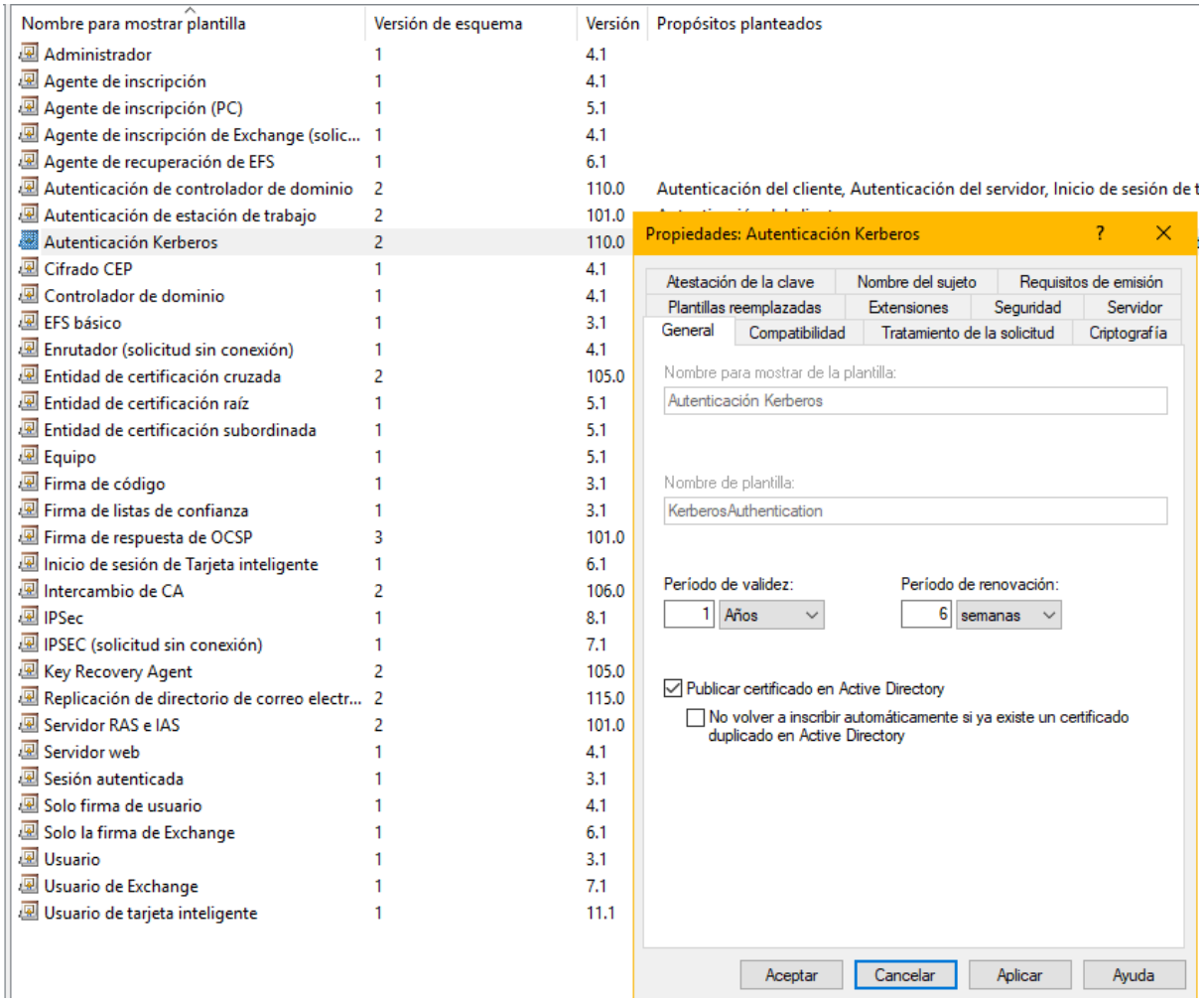

Configuración de AD CS
Nombre de CA
SERVIDOR DE DESTINO
SVR-AD.ijo.org
Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez
Base de datos de certifica...
Confirmación
Progreso
Resultados
Especifique el nombre de la CA
Escriba un nombre común para identificar esta entidad de certificación (CA). Este nombre se agrega a todos los certificados emitidos por la CA. Los valores de sufijo de nombre distintivo se generan automáticamente, pero se pueden modificar.
Nombre común para esta entidad de certificación:
IJO-AD-CA
Sufijo de nombre distintivo:
DC=ijo,DC=org
Vista previa de nombre distintivo:
CN=IJO-AD-CA,DC=ijo,DC=org
Más información acerca del nombre de CA
< Anterior
Siguiente >
Configurar
Cancelar

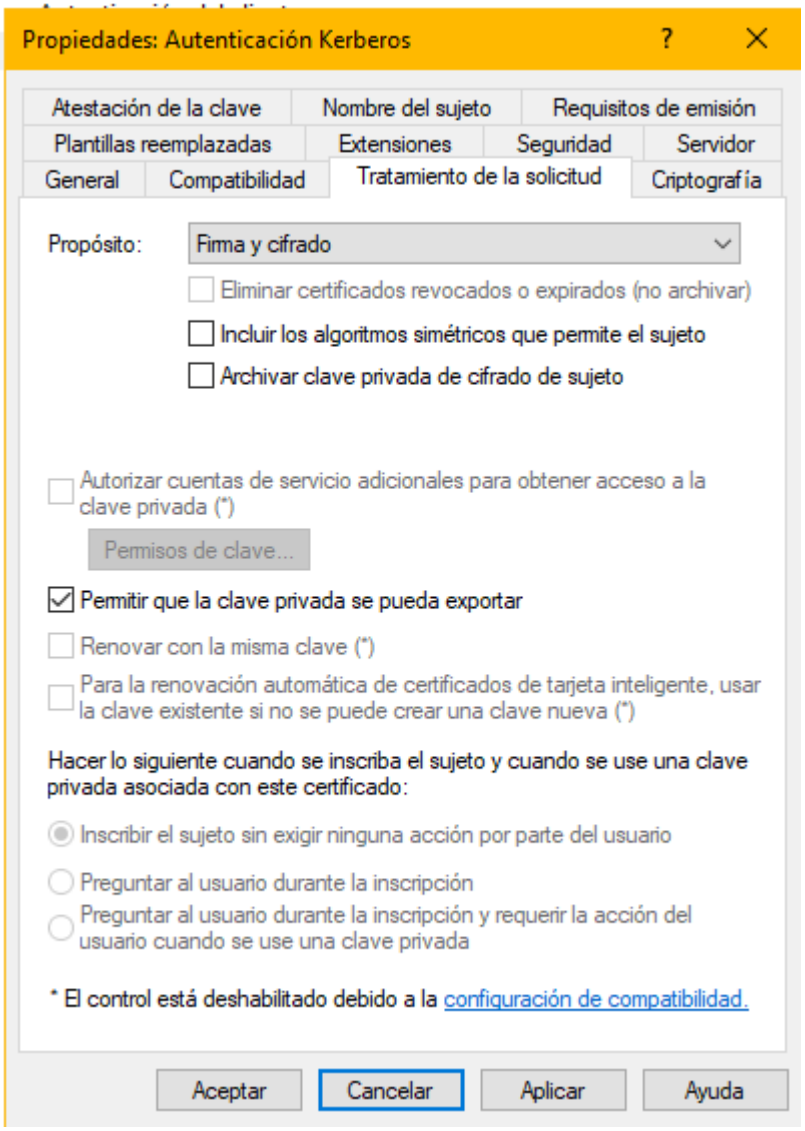

Configuración de AD CS
Confirmación
SERVIDOR DE DESTINO
WIN-CCP5KKCHRTM.ijo.org
Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez
Base de datos de certifica...
Confirmación
Progreso
Resultados
Para configurar los roles, servicios de rol o características siguientes, haga clic en Configurar.
Servicios de certificados de Active Directory
Entidad de certificación
Tipo de CA: Raíz de empresa
Proveedor de servicios criptográficos: RSA#Microsoft Software Key Storage Provider
Algoritmo hash: SHA256
Longitud de la clave: 2048
Permitir interacción del administrador: Deshabilitado
Período de validez del certificado: 12/11/2125 15:13:00
Nombre distintivo: CN=AD,DC=ijo,DC=org
Ubicación de la base de datos de certificados: C:\Windows\system32\CertLog
Ubicación del registro de la base de datos de certificados: C:\Windows\system32\CertLog
< Anterior
Siguiente >
Configurar
Cancelar

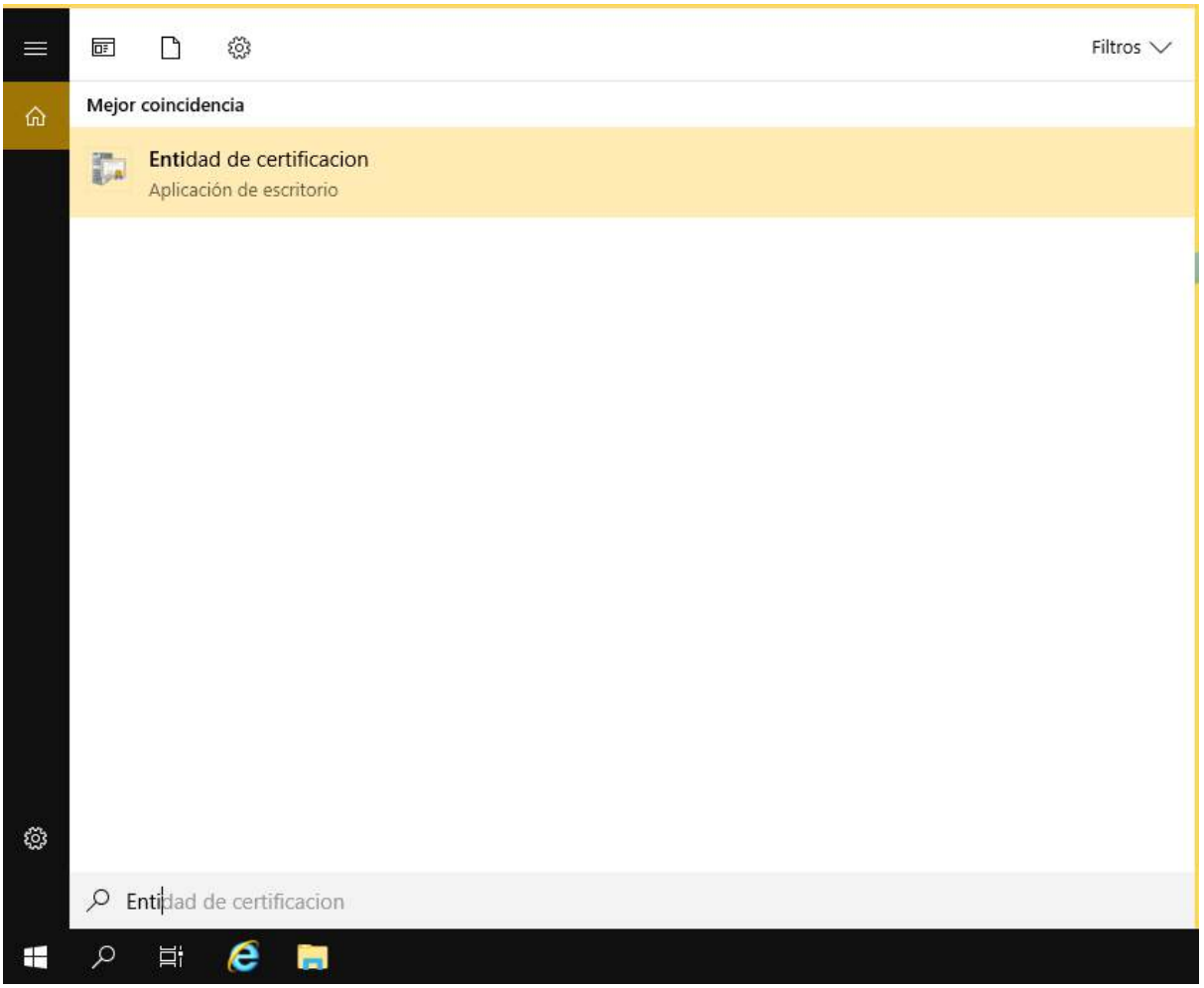

Ejecutar
Escriba el nombre del programa, carpeta, documento o recurso de Internet que desea abrir con Windows.
Abrir:
certtmpl.msc
Esta tarea se creará con privilegios administrativos.
Aceptar
Cancelar
Examinar...

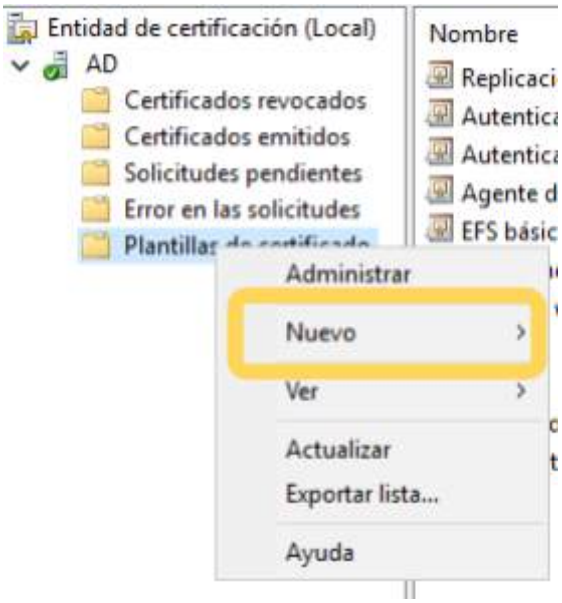

Autenticación de estación de trabajo 2 101.0 Autenticación del cliente
Autenticación Kerberos
Cifrado CEP
Controlador de dominio
EFS básico
Enrutador (solicitud sin conexión)
Entidad de certificación cruzada
Entidad de certificación raíz
Entidad de certificación subordinada 1 5.1
Equipo 1 5.1
Firma de código 1 3.1
Plantilla duplicada
Volver a inscribir a todos los poseedores de certificados
Todas las tareas
Propiedades
Ayuda

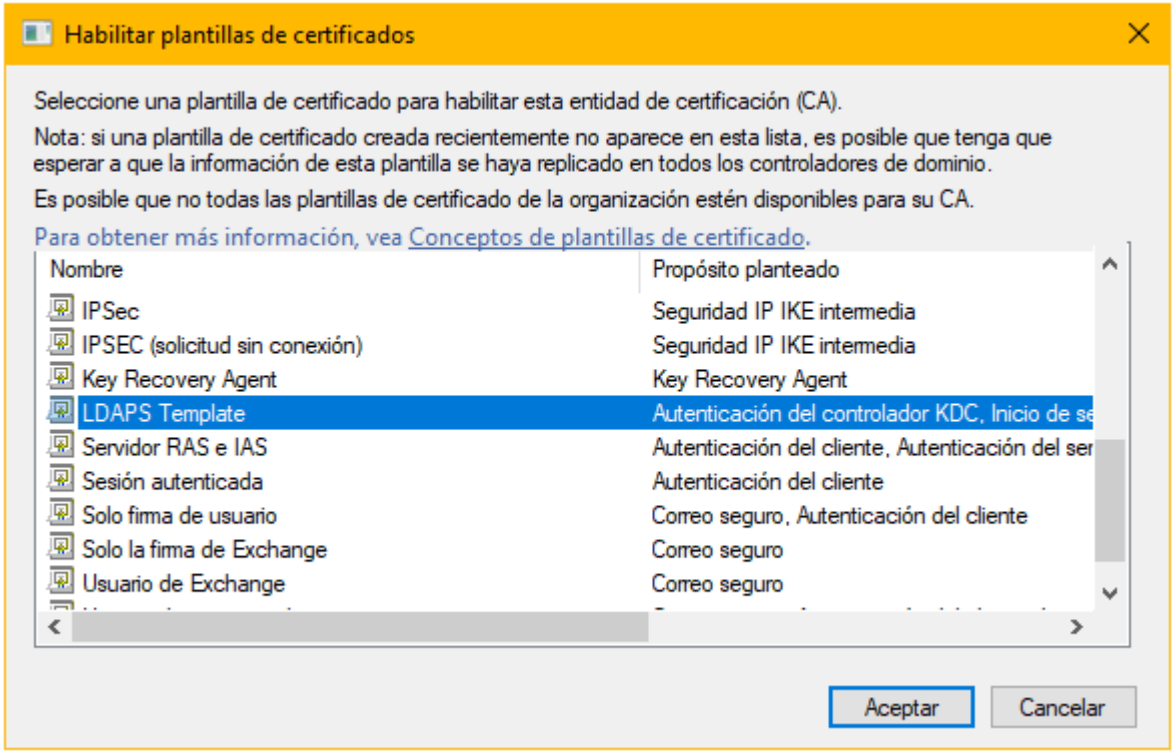

Autenticación de estación de trabajo 2 101.0
Autenticación Kerberos 2 110.1
Cifrado CEP 1 4.1
Controlador de dominio 1 4.1
EFS básico 1 3.1
Enrutador (solicitud sin conexión) 1 4.1
Entidad de certificación cruzada 2 105.0
Entidad de certificación raíz 1 5.1
Entidad de certificación subordinada 1 5.1
Equipo 1 5.1
Firma de código 1 3.1
Firma de listas de confianza 1 3.1
Firma de respuesta de OCSP 3 101.0
Inicio de sesión de Tarjeta inteligente 1 6.1
Intercambio de CA 2 106.0
IPSec 1 8.1
IPSEC (solicitud sin conexión) 1 7.1
Key Recovery Agent 2 105.0
Replicación de directorio de correo electr... 2 115.0
Servidor RAS e IAS 2 101.0
Servidor web 1 4.1
Sesión autenticada 1 3.1
Solo firma de usuario 1 4.1
Solo la firma de Exchange 1 6.1
Usuario 1 3.1
Usuario de Exchange 1 7.1
Usuario de tarjeta inteligente 1 11.1
Propiedades de plantilla nueva
Atestación de la clave
Nombre del sujeto
Servidor
Requisitos de emisión
Plantillas reemplazadas
Extensiones
Seguridad
Compatibilidad
General
Tratamiento de la solicitud
Criptografía
Nombre para mostrar de la plantilla:
LDAPS Template
Nombre de plantilla:
LDAPSTemplate
Período de validez:
1
Años
Período de renovación:
6
semanas
Publicar certificado en Active Directory
No volver a inscribir automáticamente si ya existe un certificado duplicado en Active Directory
Aceptar
Cancelar
Aplicar
Ayuda

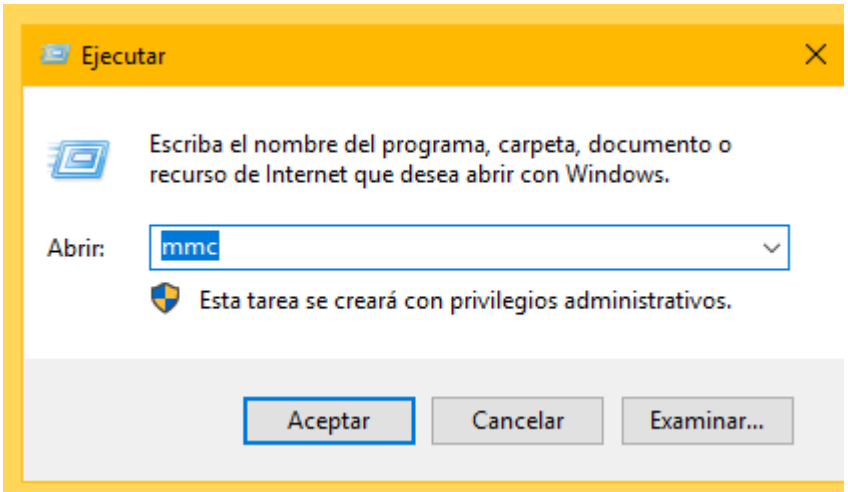

Nombre para mostrar plantilla
Versión de esquema
Versión
Propósitos planteados
Administrador 1 4.1
Agente de inscripción 1 4.1
Agente de inscripción (PC) 1 5.1
Agente de inscripción de Exchange (solic... 1 4.1
Agente de recuperación de EFS 1 6.1
Autenticación de controlador de dominio 2 110.0 Autenticación del cliente, Autenticación del servidor, Inicio de sesión de t
Autenticación de estación de trabajo 2 101.0
Autenticación Kerberos 2 110.0
Cifrado CEP 1 4.1
Controlador de dominio 1 4.1
EFS básico 1 3.1
Enrutador (solicitud sin conexión) 1 4.1
Entidad de certificación cruzada 2 105.0
Entidad de certificación raíz 1 5.1
Entidad de certificación subordinada 1 5.1
Equipo 1 5.1
Firma de código 1 3.1
Firma de listas de confianza 1 3.1
Firma de respuesta de OCSP 3 101.0
Inicio de sesión de Tarjeta inteligente 1 6.1
Intercambio de CA 2 106.0
IPSec 1 8.1
IPSEC (solicitud sin conexión) 1 7.1
Key Recovery Agent 2 105.0
Replicación de directorio de correo electr... 2 115.0
Servidor RAS e IAS 2 101.0
Servidor web 1 4.1
Sesión autenticada 1 3.1
Solo firma de usuario 1 4.1
Solo la firma de Exchange 1 6.1
Usuario 1 3.1
Usuario de Exchange 1 7.1
Usuario de tarjeta inteligente 1 11.1
Propiedades: Autenticación Kerberos
Atestación de la clave
Nombre del sujeto
Requisitos de emisión
Plantillas reemplazadas
Extensiones
Seguridad
Servidor
General
Compatibilidad
Tratamiento de la solicitud
Criptografía
Nombre para mostrar de la plantilla:
Autenticación Kerberos
Nombre de plantilla:
KerberosAuthentication
Período de validez:
1
Años
Período de renovación:
6
semanas
Publicar certificado en Active Directory
No volver a inscribir automáticamente si ya existe un certificado duplicado en Active Directory
Aceptar
Cancelar
Aplicar
Ayuda

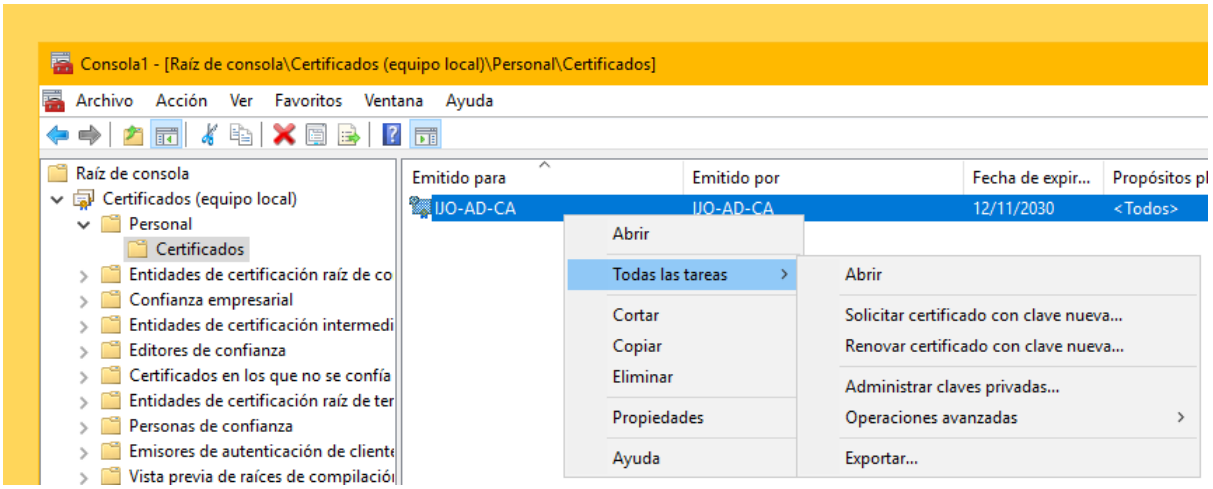

Propiedades: Autenticación Kerberos
Atestación de la clave
Nombre del sujeto
Requisitos de emisión
Plantillas reemplazadas
Extensiones
Seguridad
Servidor
General
Compatibilidad
Tratamiento de la solicitud
Criptografía
Propósito:
Firma y cifrado
Eliminar certificados revocados o expirados (no archivar)
Incluir los algoritmos simétricos que permite el sujeto
Archivar clave privada de cifrado de sujeto
Autorizar cuentas de servicio adicionales para obtener acceso a la clave privada (*)
Permisos de clave...
Permitir que la clave privada se pueda exportar
Renovar con la misma clave (*)
Para la renovación automática de certificados de tarjeta inteligente, usar la clave existente si no se puede crear una clave nueva (*)
Hacer lo siguiente cuando se inscriba el sujeto y cuando se use una clave privada asociada con este certificado:
Inscribir el sujeto sin exigir ninguna acción por parte del usuario
Preguntar al usuario durante la inscripción
Preguntar al usuario durante la inscripción y requerir la acción del usuario cuando se use una clave privada
* El control está deshabilitado debido a la configuración de compatibilidad.
Aceptar
Cancelar
Aplicar
Ayuda

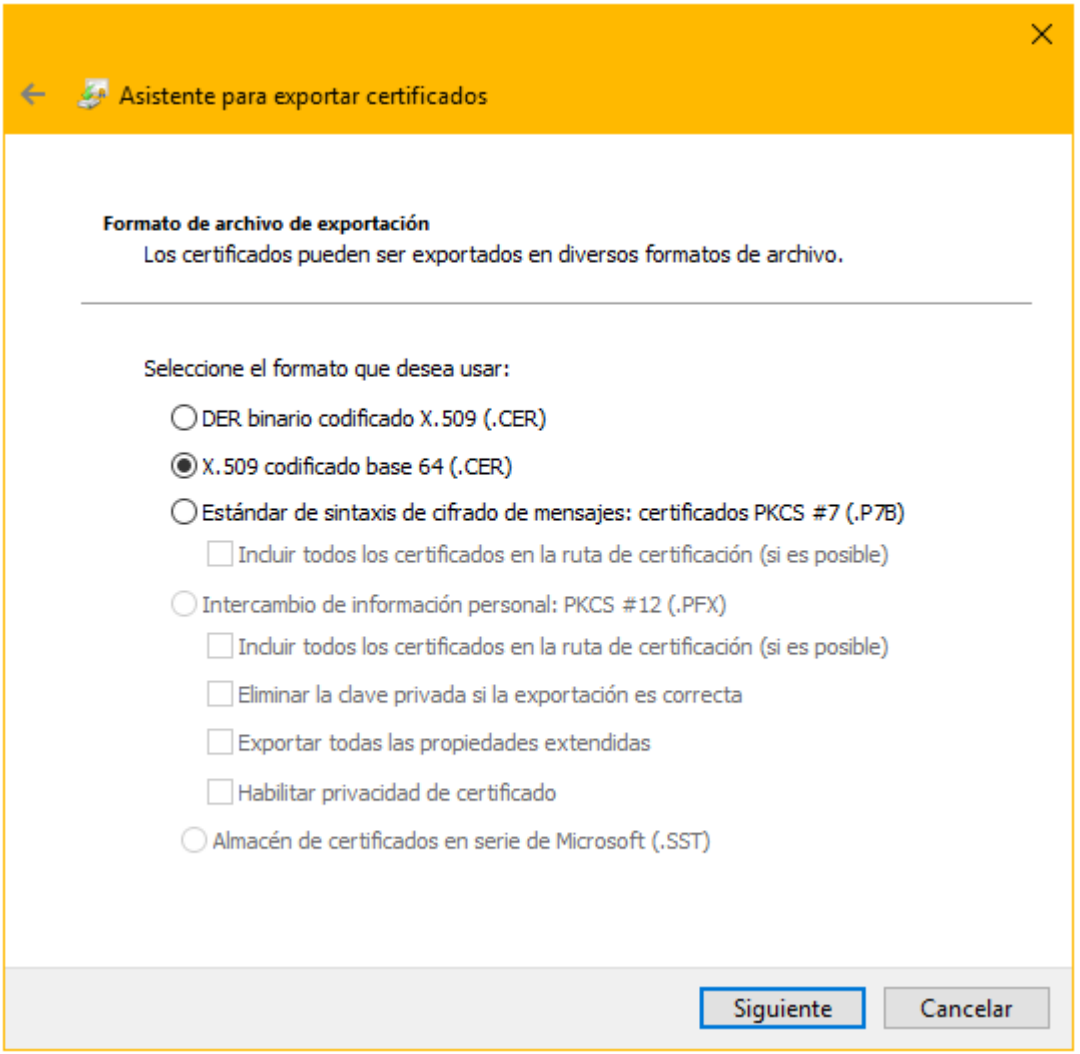

Filtros
Mejor coincidencia
Entidad de certificacion
Aplicación de escritorio
Entidad de certificacion

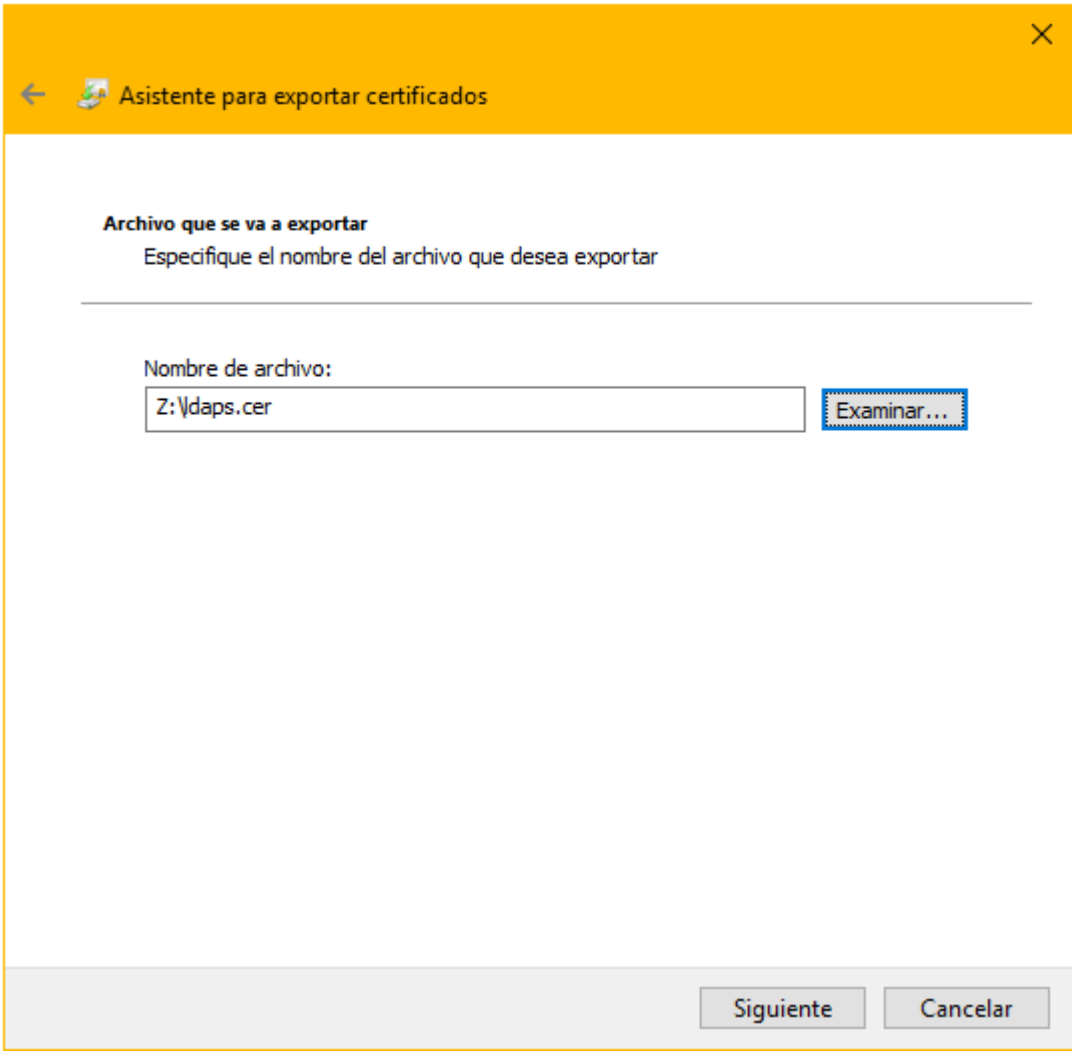

Entidad de certificación (Local)
AD
Certificados revocados
Certificados emitidos
Solicitudes pendientes
Error en las solicitudes
Plantillas de certificado
Nombre
Replicaci
Autentica
Autentica
Agente d
EFS básic
Administrar
Nuevo
Ver
Actualizar
Exportar lista...
Ayuda


Habilitar plantillas de certificados
Seleccione una plantilla de certificado para habilitar esta entidad de certificación (CA).
Nota: si una plantilla de certificado creada recientemente no aparece en esta lista, es posible que tenga que esperar a que la información de esta plantilla se haya replicado en todos los controladores de dominio.
Es posible que no todas las plantillas de certificado de la organización estén disponibles para su CA.
Para obtener más información, vea Conceptos de plantillas de certificado.
Nombre
Propósito planteado
IPSec
Seguridad IP IKE intermedia
IPSEC (solicitud sin conexión)
Seguridad IP IKE intermedia
Key Recovery Agent
Key Recovery Agent
LDAPS Template
Autenticación del controlador KDC, Inicio de se
Servidor RAS e IAS
Autenticación del cliente, Autenticación del ser
Sesión autenticada
Autenticación del cliente
Solo firma de usuario
Correo seguro, Autenticación del cliente
Solo la firma de Exchange
Correo seguro
Usuario de Exchange
Correo seguro
Aceptar
Cancelar


Ejecutar
Escriba el nombre del programa, carpeta, documento o recurso de Internet que desea abrir con Windows.
Abrir:
mmc
Esta tarea se creará con privilegios administrativos.
Aceptar
Cancelar
Examinar...


Consola1 - [Raíz de consola\Certificados (equipo local)\Personal\Certificados]
Archivo Acción Ver Favoritos Ventana Ayuda
Raíz de consola
Certificados (equipo local)
Personal
Certificados
Entidades de certificación raíz de co
Confianza empresarial
Entidades de certificación intermedi
Editores de confianza
Certificados en los que no se confía
Entidades de certificación raíz de ter
Personas de confianza
Emisores de autenticación de cliente
Vista previa de raíces de compilació
Emitido para
Emitido por
Fecha de expir...
Propósitos pl
IJO-AD-CA
IJO-AD-CA
12/11/2030
<Todos>
Abrir
Todas las tareas
Cortar
Copiar
Eliminar
Propiedades
Ayuda
Abrir
Solicitar certificado con clave nueva...
Renovar certificado con clave nueva...
Administrar claves privadas...
Operaciones avanzadas
Exportar...


Asistente para exportar certificados
Formato de archivo de exportación
Los certificados pueden ser exportados en diversos formatos de archivo.
Seleccione el formato que desea usar:
DER binario codificado X.509 (.CER)
X.509 codificado base 64 (.CER)
Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)
Incluir todos los certificados en la ruta de certificación (si es posible)
Intercambio de información personal: PKCS #12 (.PFX)
Incluir todos los certificados en la ruta de certificación (si es posible)
Eliminar la clave privada si la exportación es correcta
Exportar todas las propiedades extendidas
Habilitar privacidad de certificado
Almacén de certificados en serie de Microsoft (.SST)
Siguiente
Cancelar



Y deberemos tener a mano este certificado que usaremos en la mayoría de servicios.

Cada servicio tiene además un **nombre de dominio local** y un puerto asignado, lo que mantiene el acceso ordenado y facilita la gestión.

Servicio	Puerto
www.ijo.org	80, 443
portainer.ijo.org	8080
nextcloud.ijo.org	8081
glpi.ijo.org	8082
wiki.ijo.org	8083
rocket.ijo.org	8084
portalad.ijo.org	8085
guacamole.ijo.org	8086

Portainer

Portainer es el panel de mando de todo el ecosistema.

Ejecutado como contenedor dentro del SRV-CONTAINERS, se inicia automáticamente junto con el sistema operativo, ofreciendo una **interfaz web** intuitiva para supervisar los stacks, redes, imágenes y contenedores Docker.

El acceso está restringido a los **usuarios del grupo G-IT** del dominio **ijo.org**, quienes pueden crear, detener o modificar contenedores según las necesidades de la ONG.

Es, en esencia, el **tablero de control** de la infraestructura: un punto único donde todo cobra sentido.

Instalación y puesta en marcha

Antes de poner en marcha **Portainer**, es imprescindible preparar el terreno. Esto significa tener **Docker** y **Docker Compose** instalados en el servidor que actuará como contenedor maestro. Siguiendo las guías oficiales, esta instalación es rápida y directa, y marca el primer paso hacia un ecosistema de contenedores limpio, organizado y fácilmente escalable.

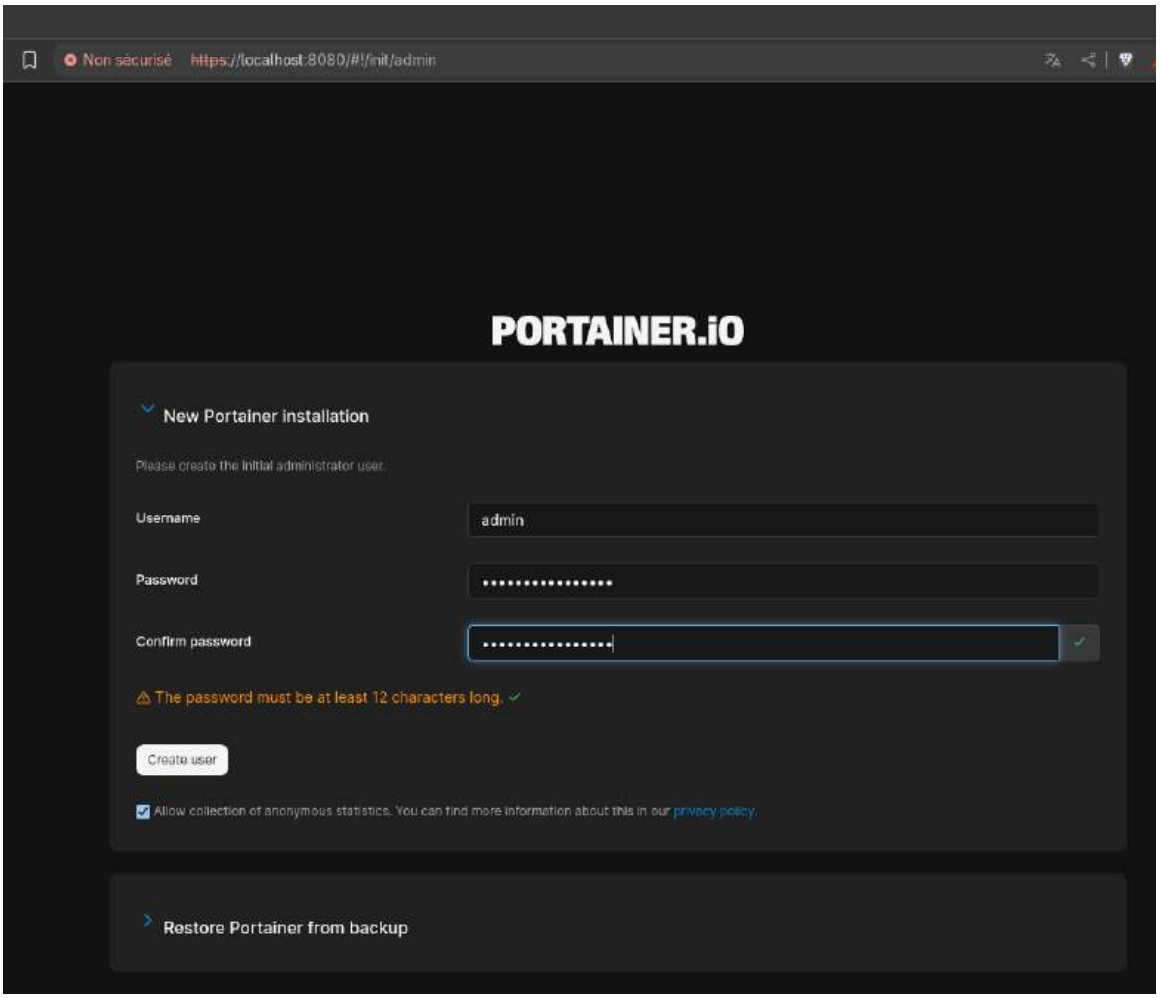
Con Docker y Docker Compose ya listos, el siguiente paso es **definir el stack que levantará Portainer**. Para ello, se crea un archivo docker-compose.yml que describa cómo se ejecutará el contenedor: qué imagen utilizar, cómo se exponen los puertos, qué volúmenes persistentes son necesarios y qué variables de entorno configuran la autenticación y la persistencia de datos. Este archivo es, en cierto modo, el plano del contenedor: un mapa que indica cómo debe nacer y crecer Portainer dentro de nuestro servidor, garantizando que al iniciar el sistema, el servicio se levante de manera automática, estable y segura. Todas las rutas relativas a contenedores, se encotrarán dentro de **/home/contenedores/servidores/** y aqui se crearará una carpeta para cada servicio.

```
services:

 portainer:

   image: portainer/portainer-ce:latest

   container_name: portainer
```

```
restart: unless-stopped

ports:

  - "8080:9443"

volumes:

  - /var/run/docker.sock:/var/run/docker.sock

  - /home/contenedores/servidores/portainer/data:/data
```

Una vez que **Portainer** está en marcha, el siguiente paso es acceder a su **interfaz web**. Esto se puede hacer a través de la **IP del servidor host**, o, si ya hemos configurado el DNS en **pfSense**, mediante su dominio local: https://portainer.ijo.org:8080. En nuestro caso, y para mantener la simplicidad durante la fase de pruebas, accederemos directamente por la IP.

Al entrar, lo primero que nos recibe es la pantalla de inicio (imagen ilustrativa). Aquí debemos **crear un usuario administrador**, que será la base sobre la cual se gestionarán todos los contenedores, stacks y configuraciones de Portainer. Este usuario se convierte en la llave maestra de todo el ecosistema de contenedores: sin él, ninguna acción crítica podría ejecutarse de forma segura.



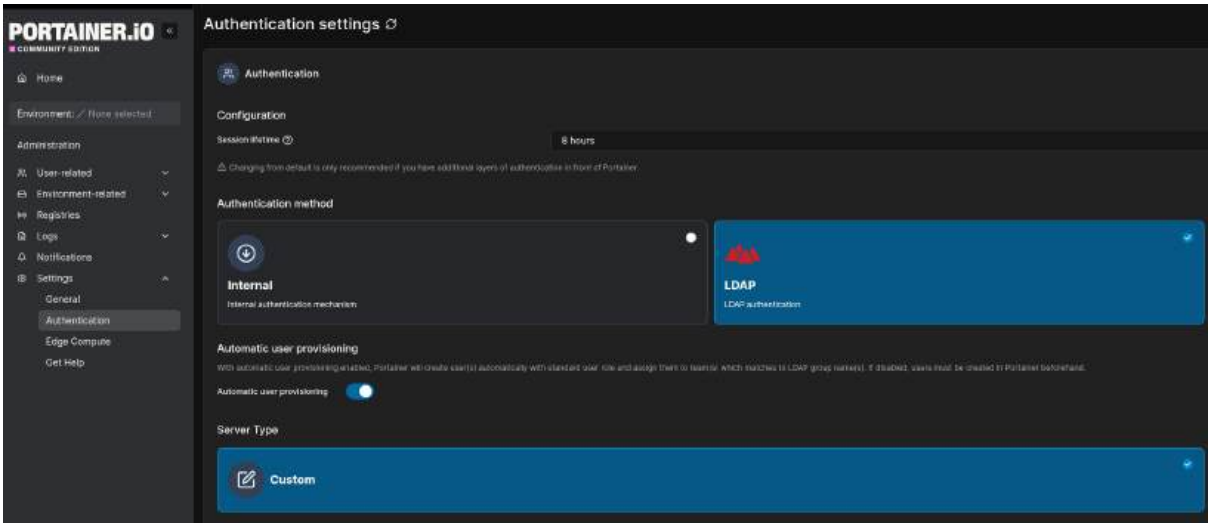
Configuración de LDAP

Con la cuenta de administrador lista, el siguiente paso es integrar Portainer con **Active Directory**, para centralizar la autenticación de usuarios. En este momento, debemos advertir que la **versión Community de Portainer no soporta LDAPS** (LDAP sobre SSL/TLS), por lo que, dado que estamos en un

entorno de pruebas, nos conformamos con conectar mediante **LDAP sin cifrado**.

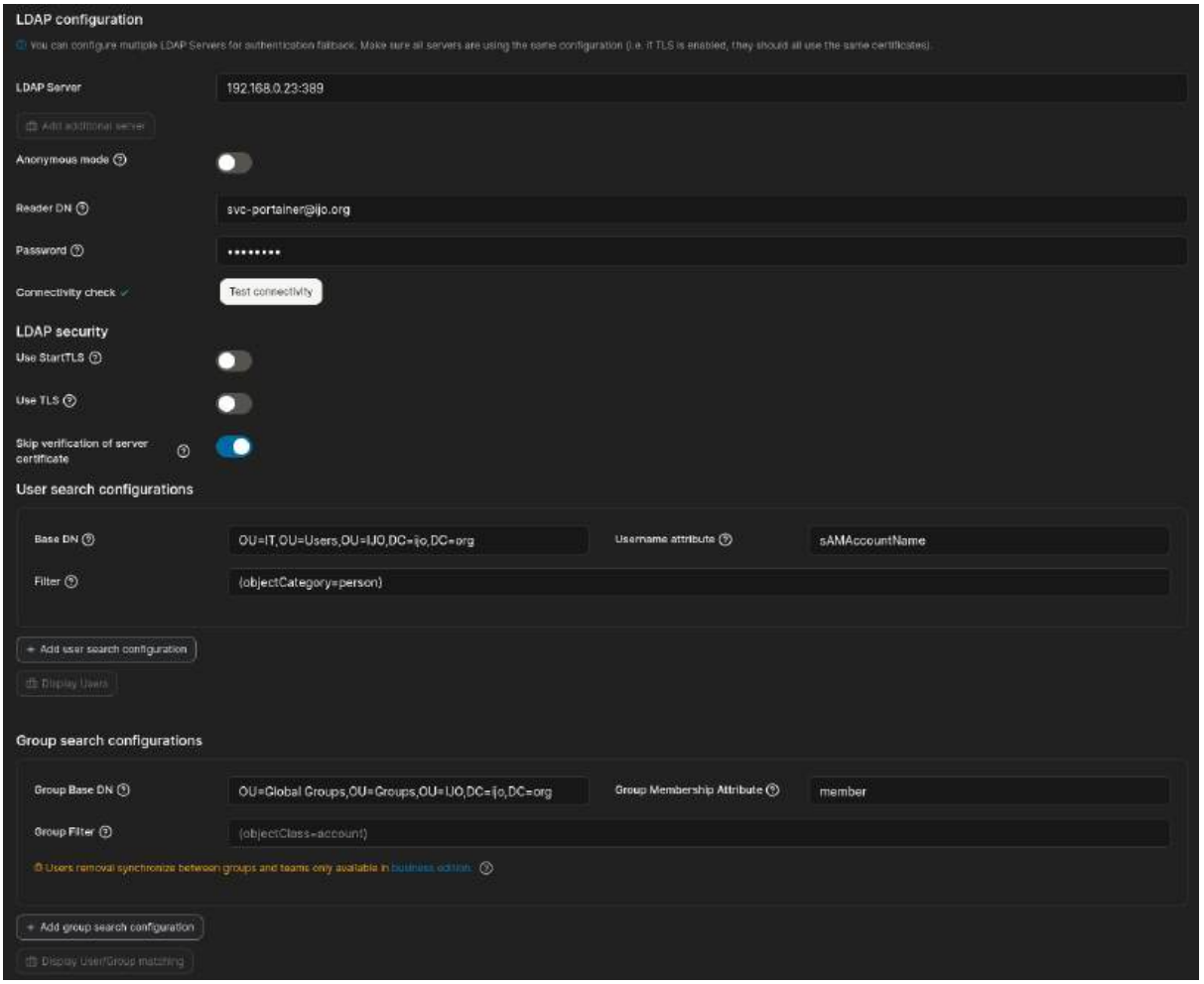
Para configurarlo, accedemos a:

Settings > Authentication > LDAP



Allí introducimos los parámetros de nuestro servidor de AD y **limitamos la base de búsqueda** a:

OU=IT,OU=Users,OU=IJO,DC=ijo,DC=org

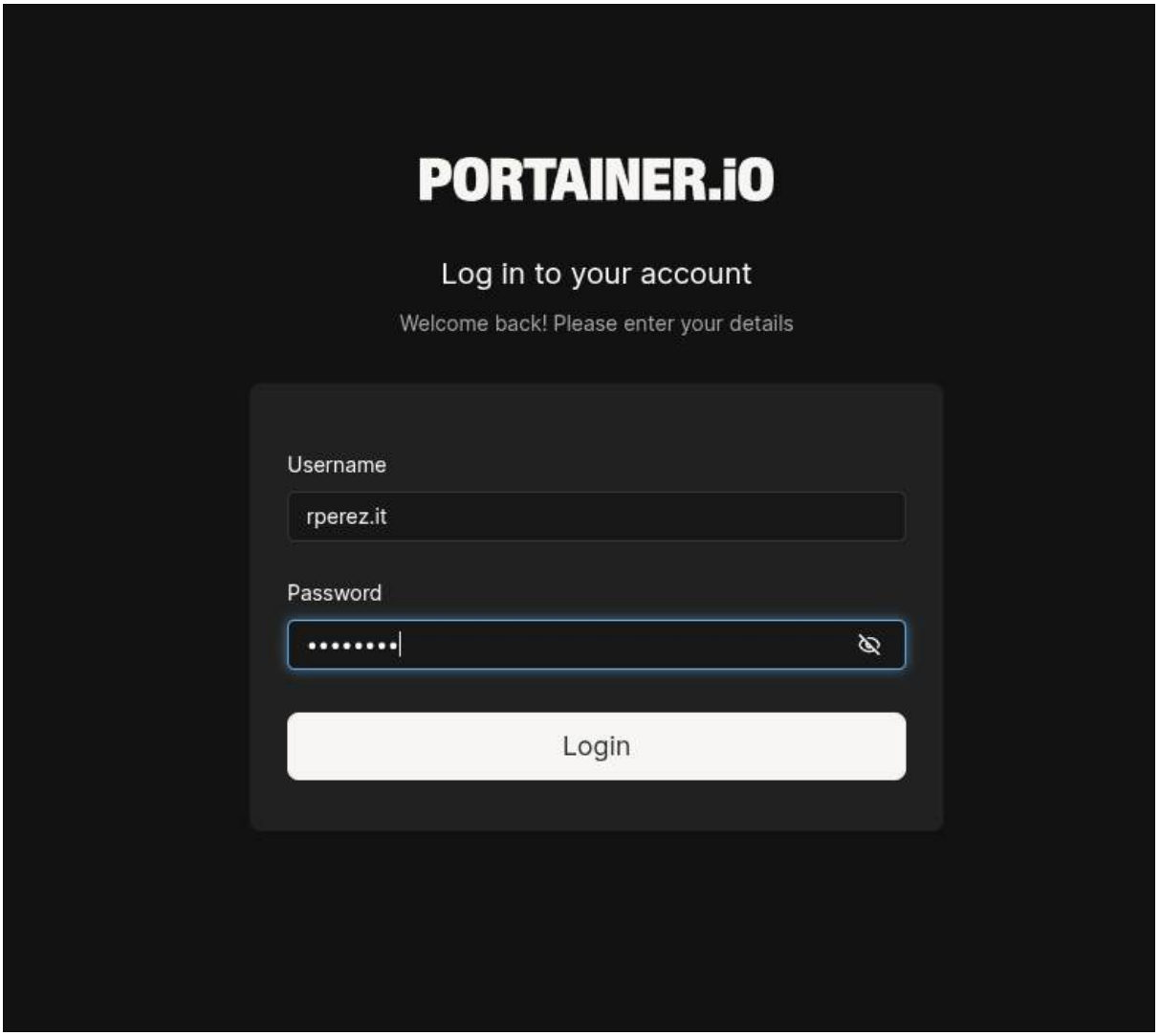


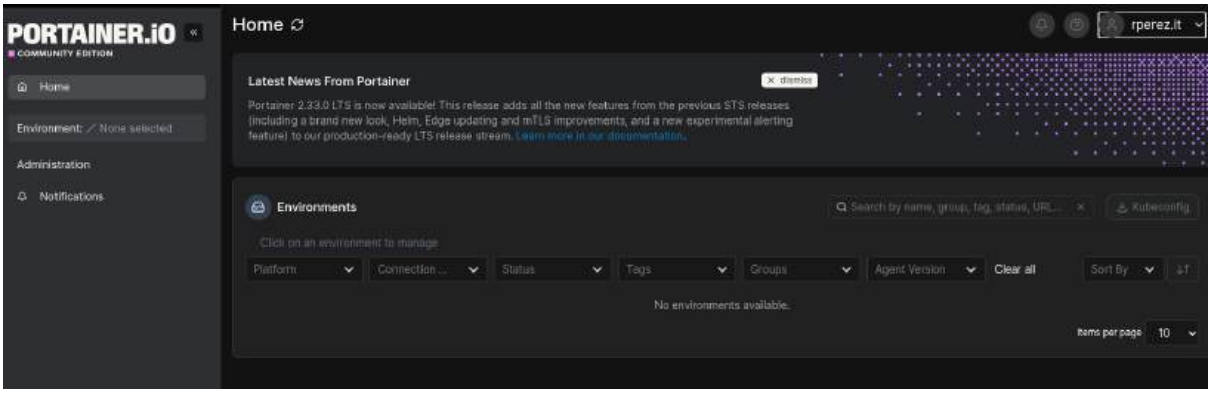
Esto asegura que solo los miembros del grupo IT sean visibles y puedan autentificarse a través de Portainer.

Limitación importante: la versión Community no permite mapear permisos directamente desde AD a los contenedores o stacks. Por ello, cada usuario debe recibir permisos de forma **manual** dentro de Portainer, asignándolos según su rol y responsabilidad. Aunque no es automático, esta gestión manual nos permite tener control total sobre quién puede crear, detener o

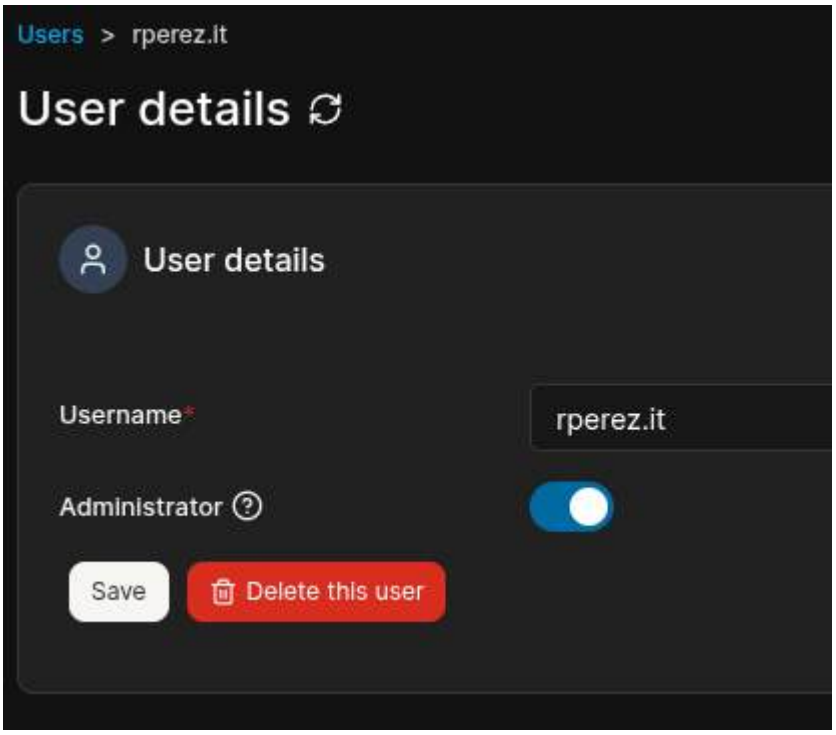
modificar los contenedores, asegurando que la infraestructura se mantenga ordenada y segura.

Probamos la autenticación:





Y le asignamos permisos de administrador:



Ahora ya podemos levantar todos los demás servicios.

Nextcloud

Nextcloud representa la **nube privada de IJO's & Monkeys**, una extensión digital del espíritu colaborativo de la organización.
Permite compartir documentos, sincronizar archivos desde cualquier dispositivo, acceder al correo, crear calendarios comunes y mantener la seguridad de los datos dentro del propio dominio.

La magia reside en su integración con **Active Directory**:

- Los usuarios se autentican con su cuenta de dominio.
- Los grupos de AD se mapean automáticamente: G-IT, G-Secretaría, G-Voluntarios y G-Veterinarios.
- Los miembros del grupo **G-IT** reciben privilegios administrativos automáticamente, garantizando que cualquier nuevo integrante del área técnica herede las capacidades necesarias.

Esta sincronización otorga **escalabilidad y control centralizado**, evitando la creación manual de permisos y garantizando que los archivos estén siempre bajo el mismo paraguas de seguridad.

Instalación y puesta en marcha

El proyecto ya está preparado para desplegar **Nextcloud**, con todos los archivos necesarios organizados y listos para ser usados en Google Drive.
Próximamente, todo el contenido estará disponible en **GitHub**, junto con un

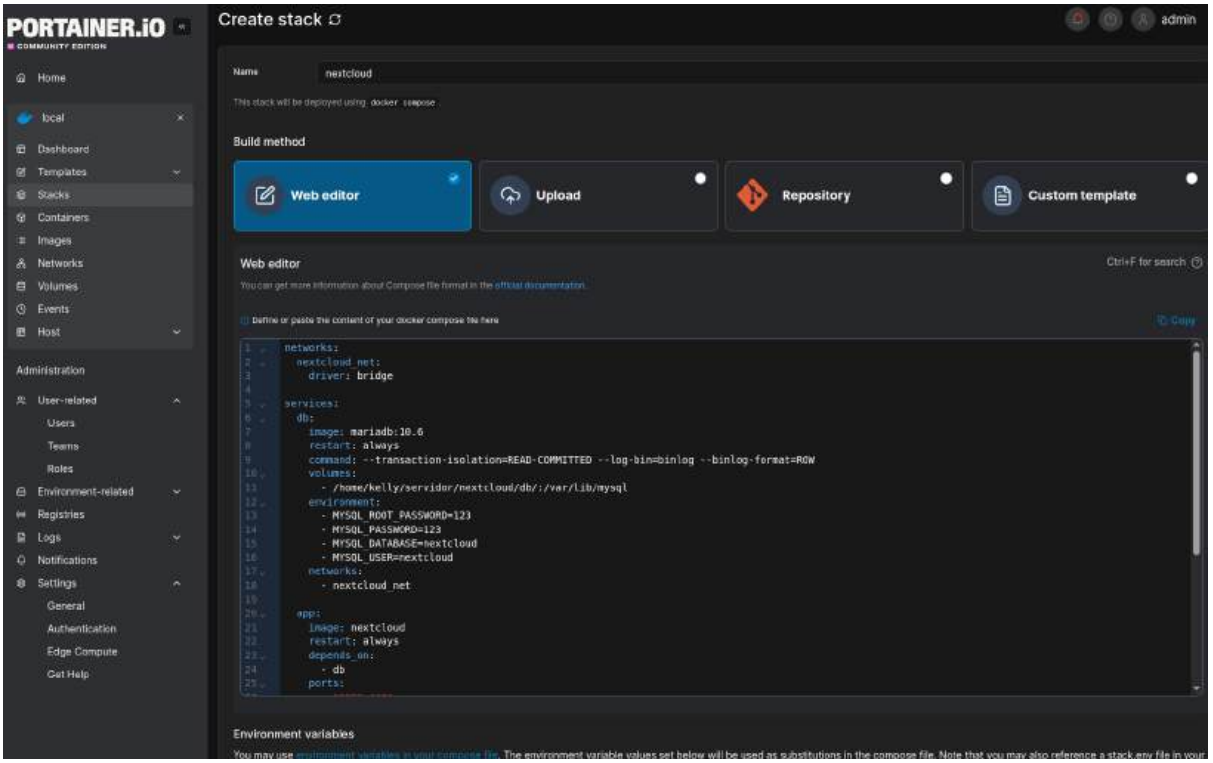
instalador automático que permitirá levantar el servicio de manera ágil y reproducible.

Preparación del entorno

Antes de iniciar, debemos asegurarnos de que **todos los archivos del proyecto se encuentran en las rutas correctas**. Posteriormente, se crea el **Stack en Portainer**, asignándole el puerto correspondiente (8081) y comenzamos la configuración a través del navegador, ya sea por la **IP del servidor** o mediante el dominio local:

https://nextcloud.ijo.org:8081

El docker-compose.yml que despliega Nextcloud incluye un script que **valida e importa certificados**, asegurando que la comunicación con el servicio esté cifrada. Es importante destacar que, en este entorno de pruebas, las variables sensibles están visibles en el archivo, pero en producción **jamás se deben dejar expuestas**; existen métodos seguros para ocultarlas, como archivos .env o gestores de secretos.



Configuración del usuario administrador y aplicaciones

Al acceder por primera vez al panel web, se debe **crear un usuario administrador** por defecto, quien tendrá control total sobre el servidor. A continuación, se pueden habilitar las aplicaciones necesarias para la ONG, adaptando Nextcloud a los requerimientos específicos de cada departamento.


Non sécurisé
https://localhost:8081
Fichier de configuration automatique détecté
Le formulaire de configuration ci-dessous est pré-rempli avec les valeurs du fichier de configuration.
Créer un compte administrateur
Nom du compte administrateur
inaki
Mot de passe du compte administrateur
Mot de passe faible
Stockage & base de données
Installer
Besoin d'aide ? Lire la documentation

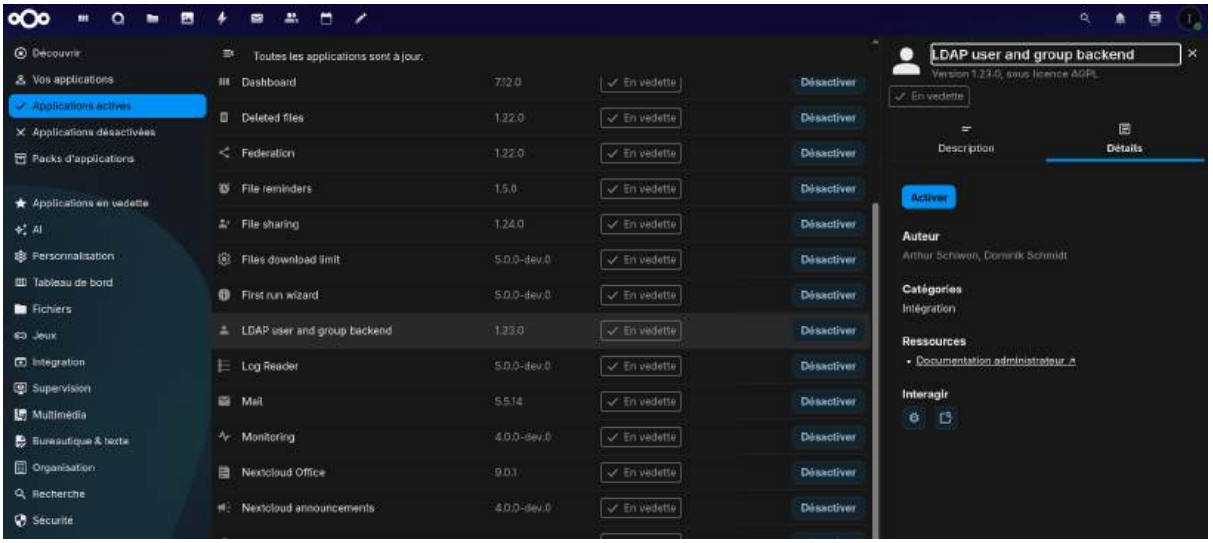
Habilitación de la autenticación LDAP

Para integrar Nextcloud con **Active Directory**, realizamos los siguientes pasos:

Accedemos a:

Aplicaciones > Aplicaciones deshabilitadas > LDAP user and group backend

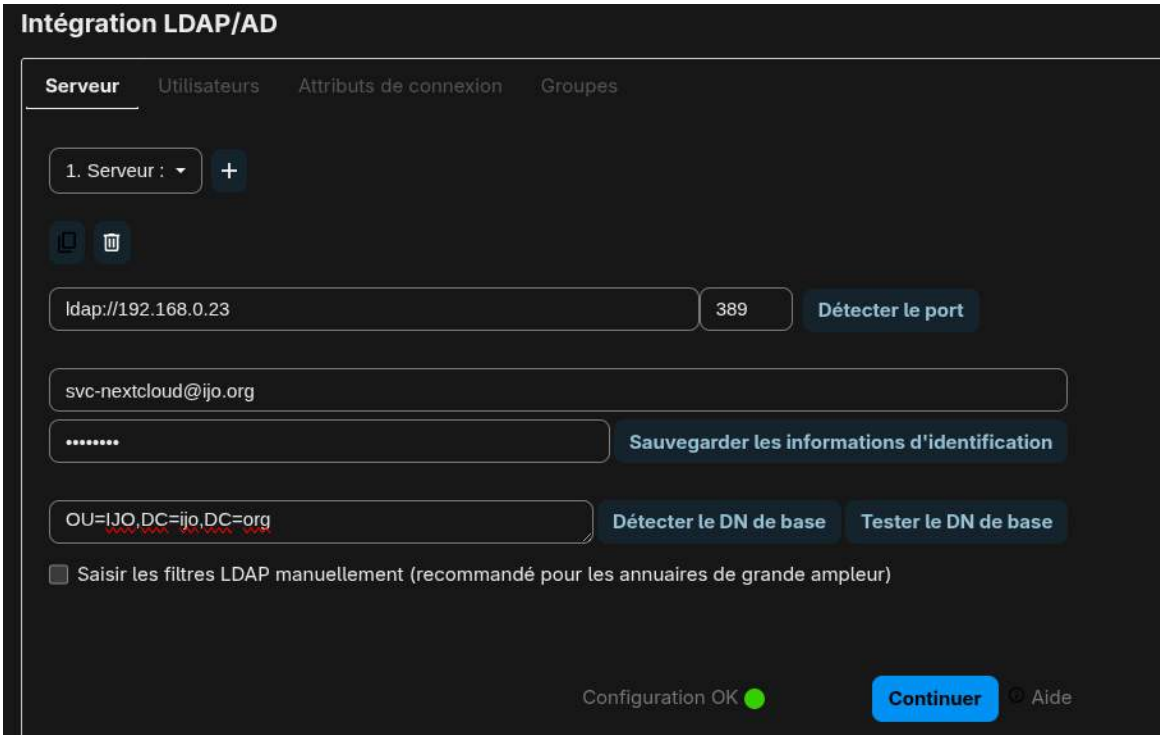
y habilitamos la aplicación. Luego, en el **panel de administración**, aparecerá la sección LDAP en la barra lateral.



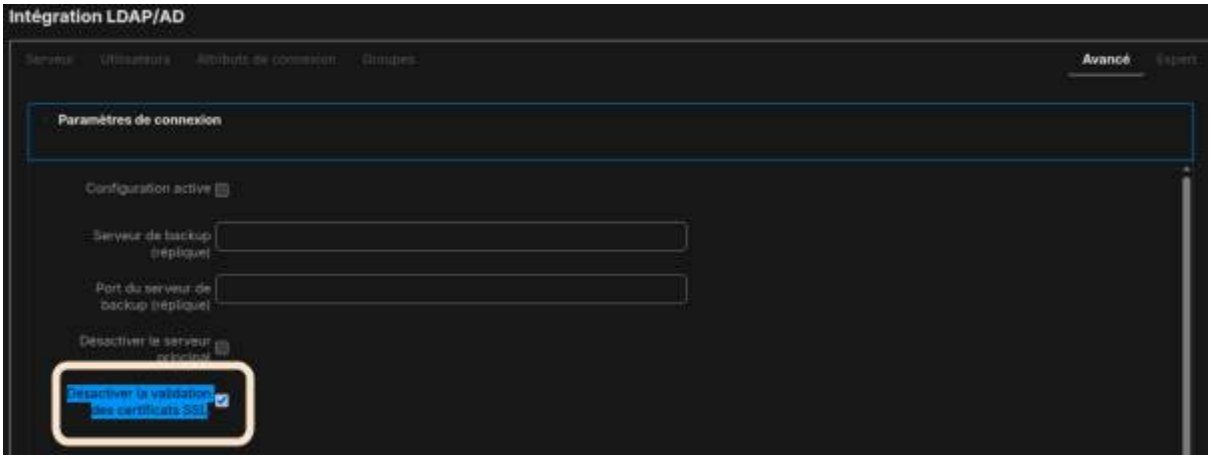
En esta fase inicial, la conexión se realiza mediante **LDAP estándar** (puerto 389), dado que el contenedor no confía en el certificado de AD. El usuario del servicio Nextcloud, **svc-nextcloud**, con permisos de lectura sobre el dominio, se utiliza para establecer la conexión. La **base de búsqueda** se limita a:

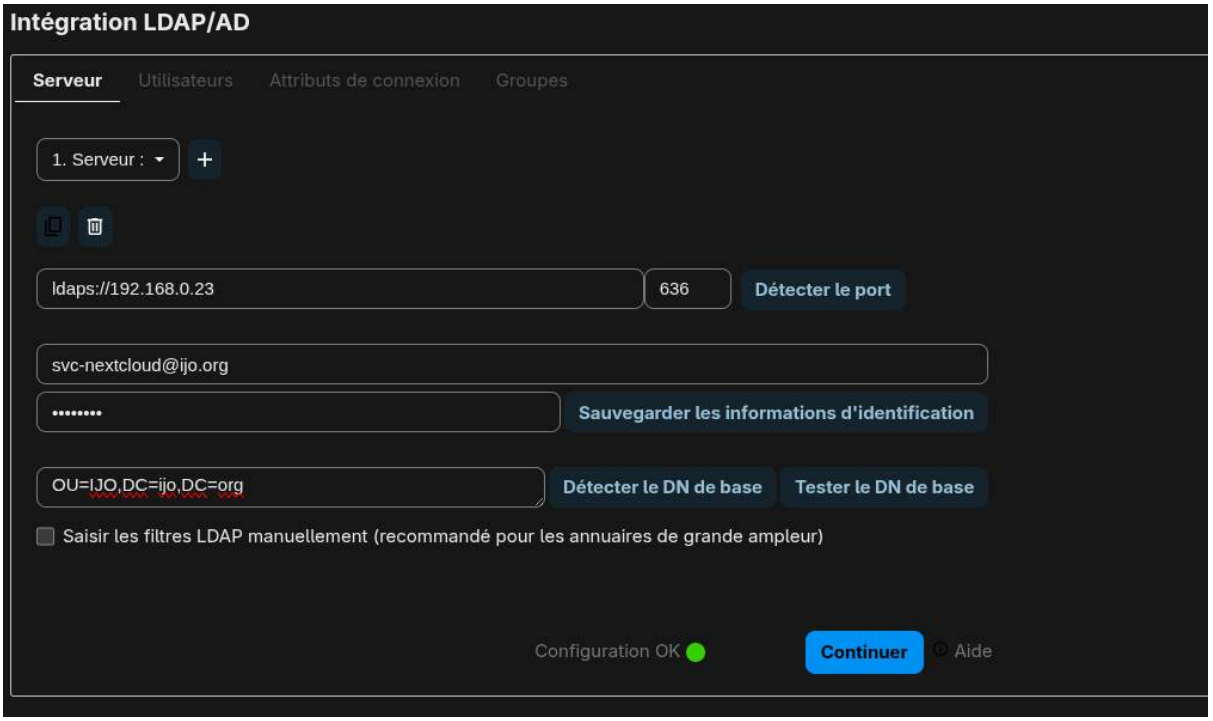
OU=IJO,DC=ijo,DC=org

Comprobamos la conexión y, si es correcta, Nextcloud nos indica OK.

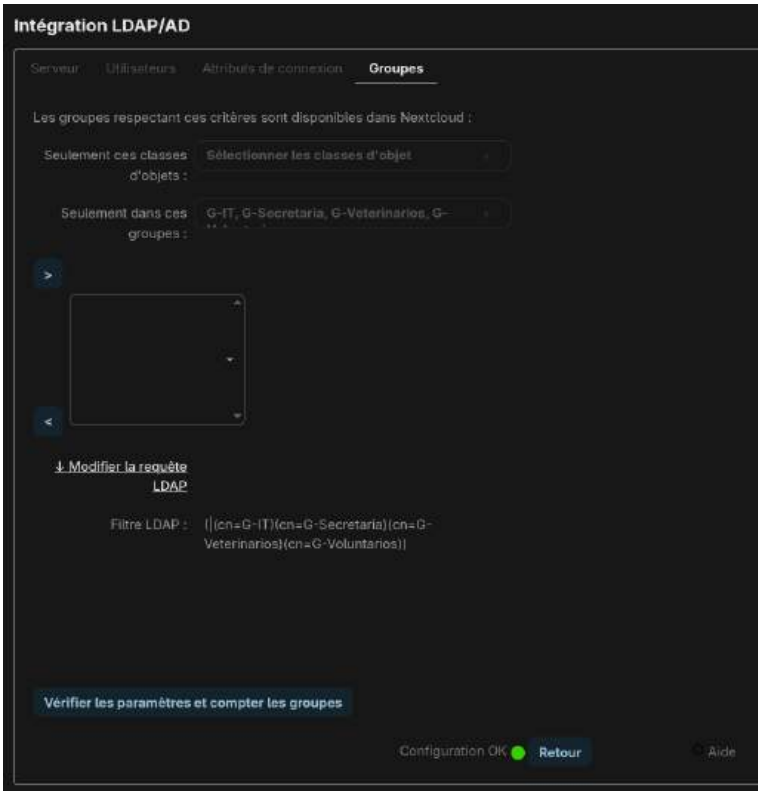


En la pestaña **Avanzado**, deshabilitamos la validación de certificados SSL (temporalmente, por ser entorno de pruebas), y volvemos a la pestaña **Servidor** para completar la configuración, ahora sí, configurando LDAPS con el puerto 636.

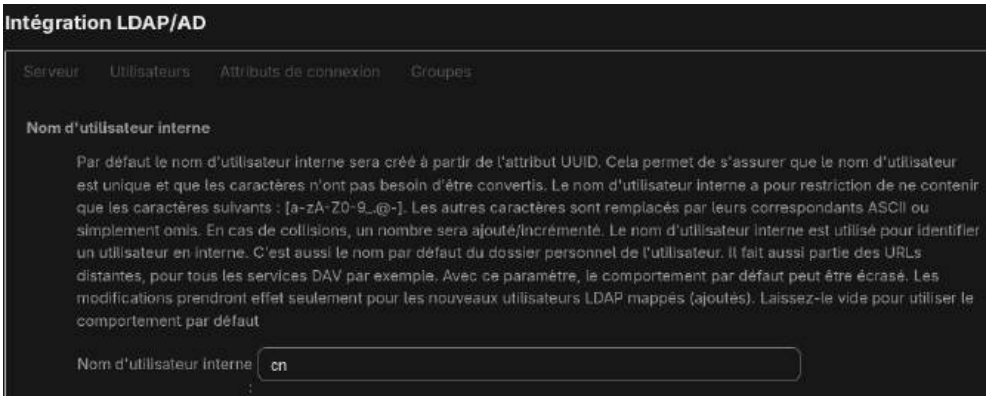

Intégration LDAP/AD
Avancé
Paramètres de connexion
Configuration active
Désactiver la validation des certificats SSL


Intégration LDAP/AD
Serveur
Utilisateurs
Attributs de connexion
Groupes
1. Serveur :
ldaps://192.168.0.23
636
Détecter le port
svc-nextcloud@ijo.org
Sauvegarder les informations d'identification
OU=IJO,DC=ijo,DC=org
Détecter le DN de base
Tester le DN de base
Saisir les filtres LDAP manuellement (recommandé pour les annuaires de grande ampleur)
Configuration OK
Continuer
Aide

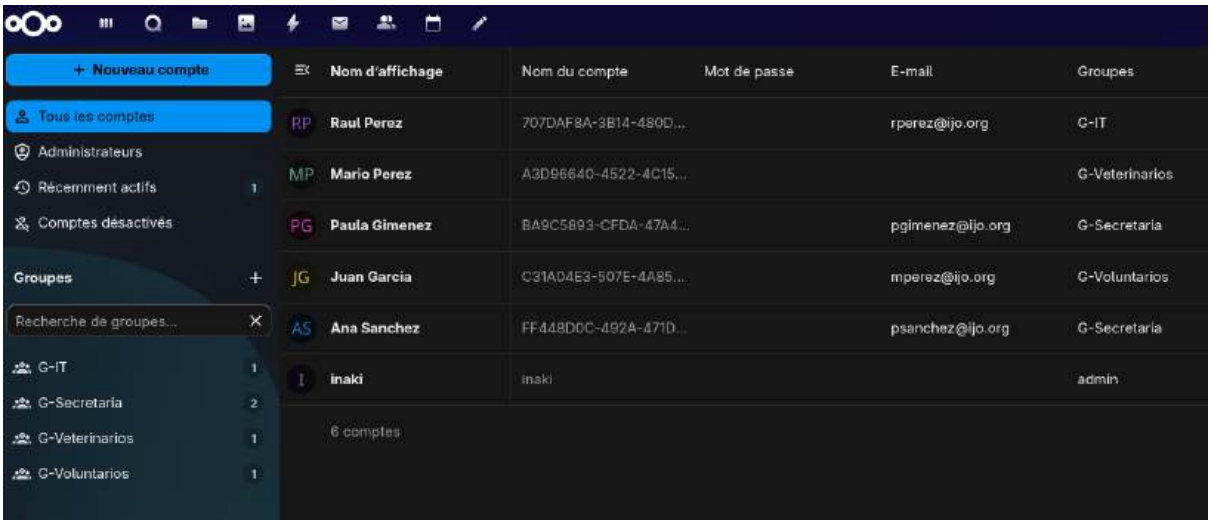
Configuramos los usuarios para que solo se busquen dentro de los **Global Groups**, y en los **atributos de conexión** indicamos que se autentifiquen con su sAMAccountName y correo electrónico.



En la pestaña **Experto**, establecemos **cn** como **Nombre de usuario interno** para evitar que aparezcan nombres extraños o no deseados en la interfaz.

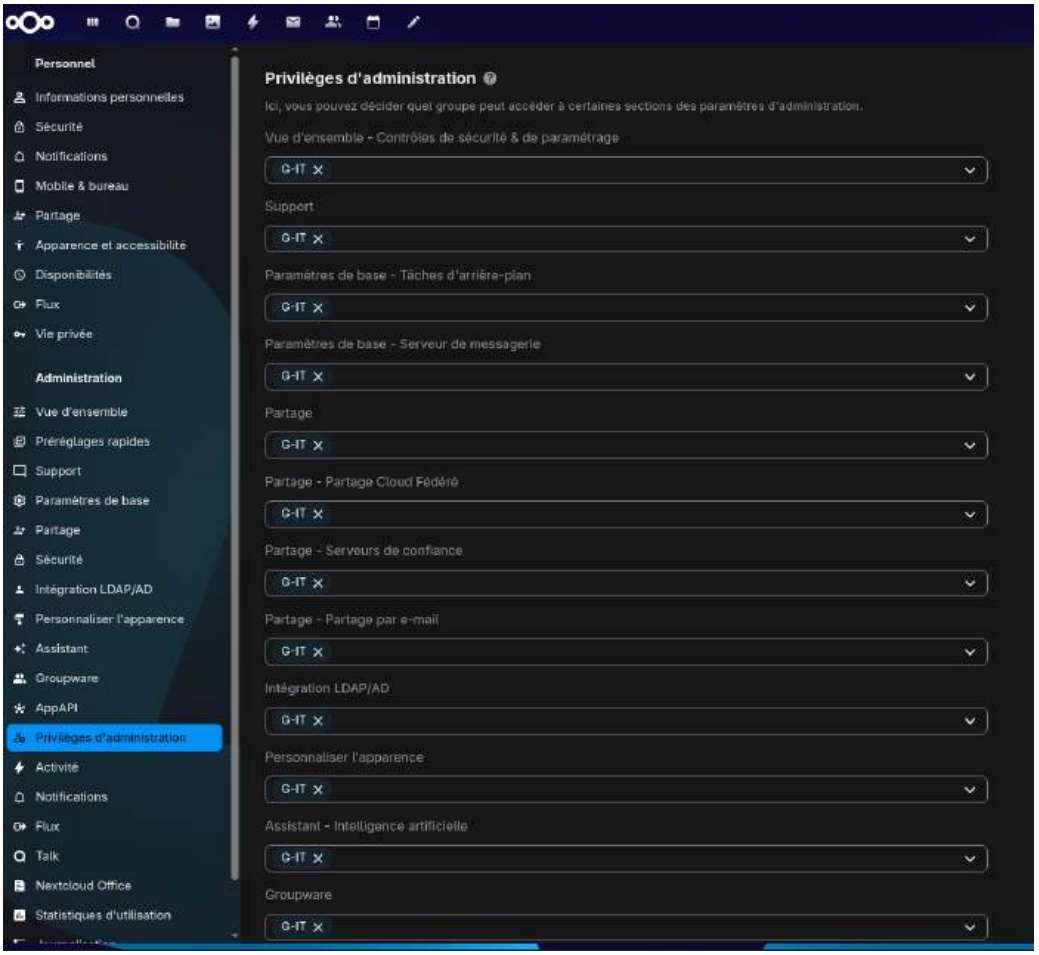


Con esto, los usuarios y grupos de Active Directory quedan **sincronizados automáticamente**, y podemos asignarles permisos y cuotas según corresponda.



Asignación de privilegios

Para garantizar la administración eficiente del sistema, asignamos **todos los permisos de administrador al grupo G-IT**, permitiendo que los miembros del equipo IT gestionen usuarios, aplicaciones, cuotas y configuraciones de Nextcloud sin restricciones.

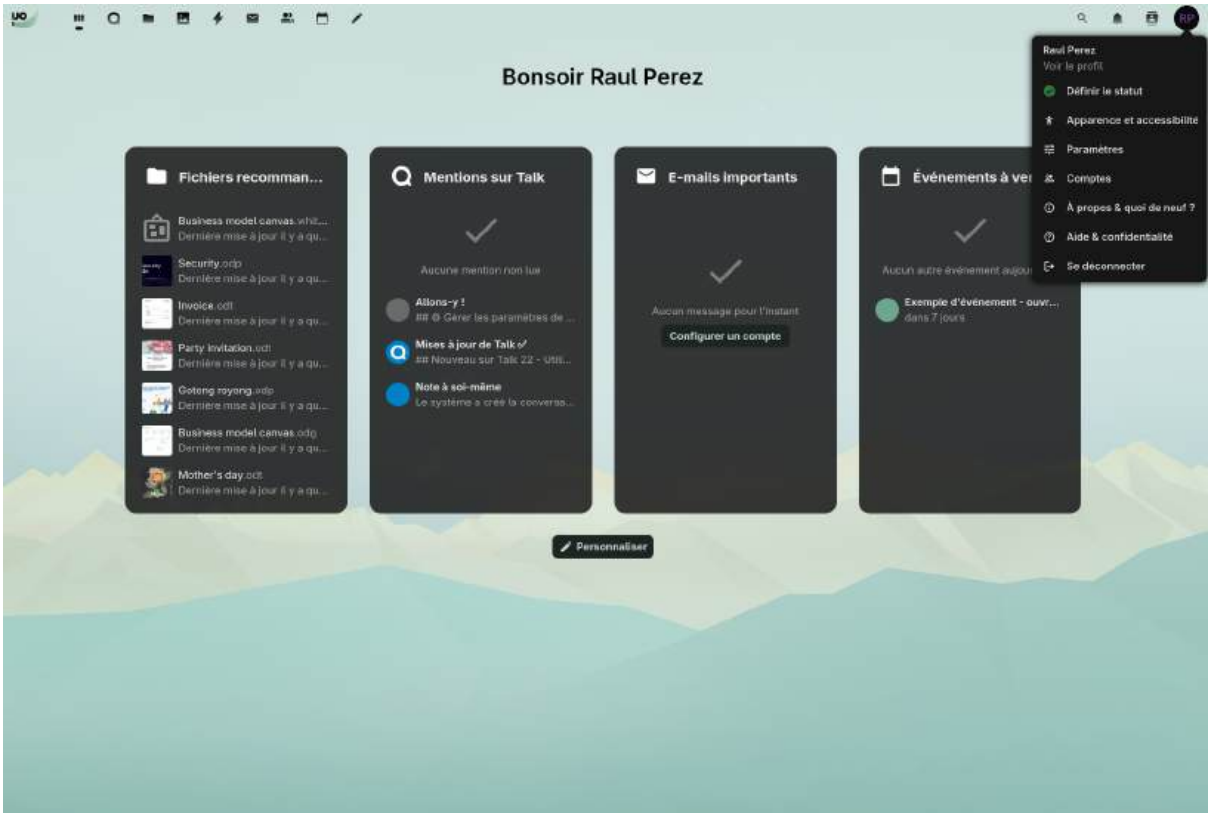


Personalización visual

Nextcloud se adapta al **entorno visual de IJO's & Monkeys**, aplicando colores, logos y elementos de identidad corporativa para reforzar la coherencia con la marca y la experiencia del usuario.

Prueba de conexión

Se realiza una **prueba con un usuario de LDAP**, confirmando que puede autenticarse correctamente y acceder a los recursos asignados. Esto garantiza que la sincronización y los permisos están funcionando según lo esperado.



Configuración adicional

Desde dentro del contenedor, se ejecuta un comando que permitirá que **Nextcloud funcione como cliente de correo**, integrando las cuentas de correo de ijo.org. Este paso asegura que los usuarios puedan enviar y recibir correos desde Nextcloud, consolidando así la plataforma como un **centro de productividad integral** para la ONG.

Dado que estamos trabajando con un **entorno de pruebas** y certificados autofirmados generados por nuestra autoridad interna (IJO_CA), es imprescindible que Nextcloud acepte estos certificados. Para ello, desde dentro del contenedor ejecutamos el siguiente comando:

```
php occ config:system:set mail_smtpstreamoptions --value
'{"ssl":{"verify_peer":false,"verify_peer_name":false,"allow_self_signed":true
}}'
```

Con esta configuración, **cada usuario del dominio `ijo.org` puede usar Nextcloud como su cliente de correo**, integrando de manera fluida mensajería y archivos dentro del mismo ecosistema. Este paso es fundamental para mantener la **coherencia operativa**: los servicios no funcionan de forma aislada, sino que se interconectan, ofreciendo una experiencia integrada y segura para todos los miembros de la ONG.

GLPI

El sistema **GLPI** (Gestionnaire Libre de Parc Informatique) es el **centro de gestión e inventario de la ONG**.
Su propósito: mantener el orden, la trazabilidad y la comunicación fluida entre los equipos.

Cada equipo cliente tiene instalado automáticamente el **GLPI Agent**, distribuido mediante una **GPO**. Este agente recopila información de hardware, software y estado del sistema, y la sincroniza con la base de datos de GLPI.
De este modo, cada equipo, impresora o servidor tiene una **identidad digital** dentro del inventario.

Los usuarios se autentican a través del AD, lo que permite:

- Asociar tickets e incidencias a cada usuario y equipo.
- Sincronizar automáticamente los grupos y roles desde el directorio.

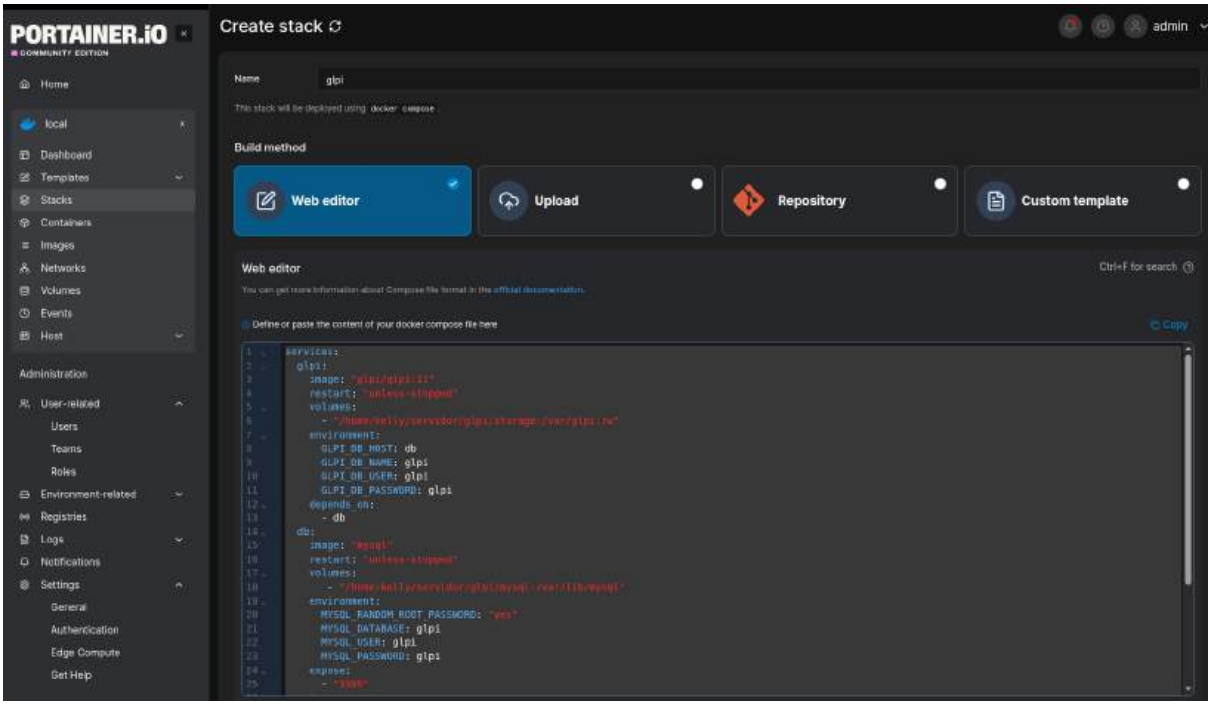
- Permitir que los usuarios del grupo **G-IT** posean permisos de **Super-Admin** (solo en este entorno, por simplicidad).

GLPI se convierte así en el **puente humano y técnico**: los usuarios crean tickets para reportar incidencias, y el equipo IT puede responder, priorizar, documentar y programar intervenciones o accesos remotos desde el mismo entorno.

Instalación y puesta en marcha

Para desplegar **GLPI**, contamos con todos los archivos necesarios previamente subidos a Google Drive.

Tal como ocurre en otros servicios, los datos sensibles del sistema quedan expuestos en texto plano dentro del stack, por lo que es recomendable protegerlos mediante variables de entorno o volúmenes seguros una vez la infraestructura pase a producción.

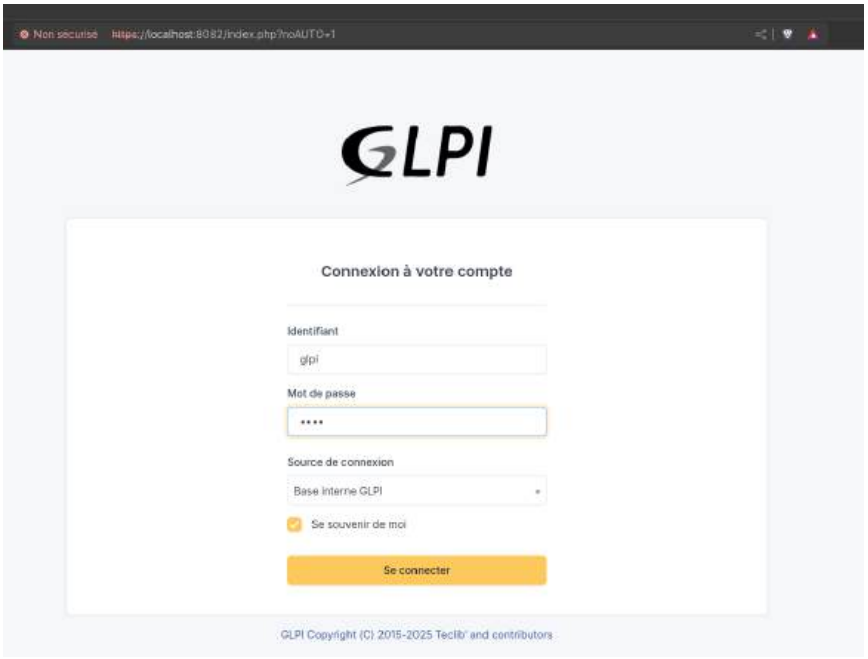


Una vez desplegado el *stack* de Docker, podremos acceder a **GLPI** desde el navegador introduciendo la IP del servidor seguida del puerto 8082, o bien directamente desde la dirección:

https://glpi.ijo.org:8082

Para el primer acceso utilizaremos las credenciales por defecto:

- **Usuario:** glpi
- **Contraseña:** glpi

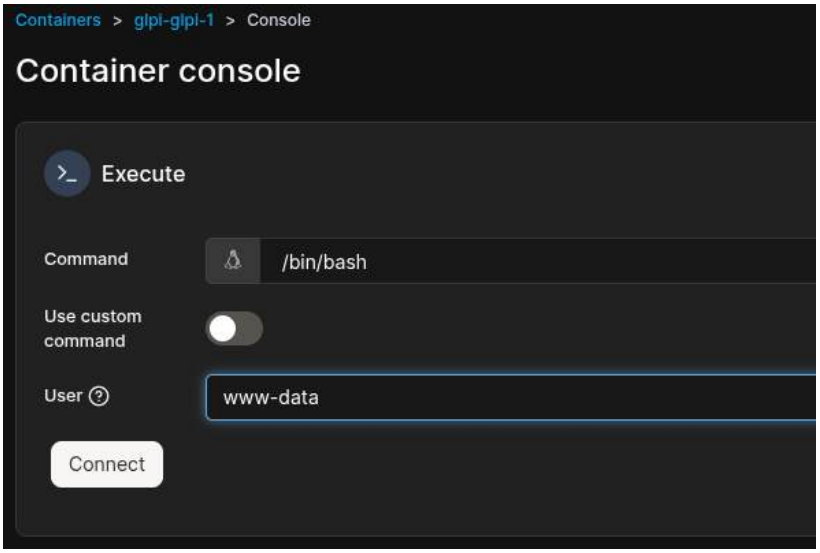


Instalación del plugin GLPI Inventory

El siguiente paso será instalar el **plugin GLPI Inventory**, necesario para la gestión automatizada del inventario de equipos de la organización.

Dentro del panel, iremos a **Setup > Plugins**. Veremos que todavía no aparece ningún complemento activo.

A continuación, accederemos al contenedor de GLPI con el usuario **www-data** y navegaremos hasta la ruta (accederé desde Portainer):



/var/www/glpi/plugins

Comprobamos que el plugin se encuentra en el directorio con:

```
ls
```

Si aparece como glpi-inventory/, debemos renombrarlo con:

```
mv glpi-inventory/ glpiinventory/
```

Finalmente, instalamos el plugin ejecutando:

```
php /var/www/glpi/bin/console --username=glpi glpi:plugin:install glpiinventory
```

Una vez completado este proceso, recargamos la interfaz web de GLPI. Ahora, el plugin **GLPI Inventory** debería aparecer en la lista de complementos. Solo queda habilitarlo clicando en el interruptor (toggle).

Con esto, el sistema ya estará preparado para la gestión automatizada de inventario que utilizaremos más adelante.

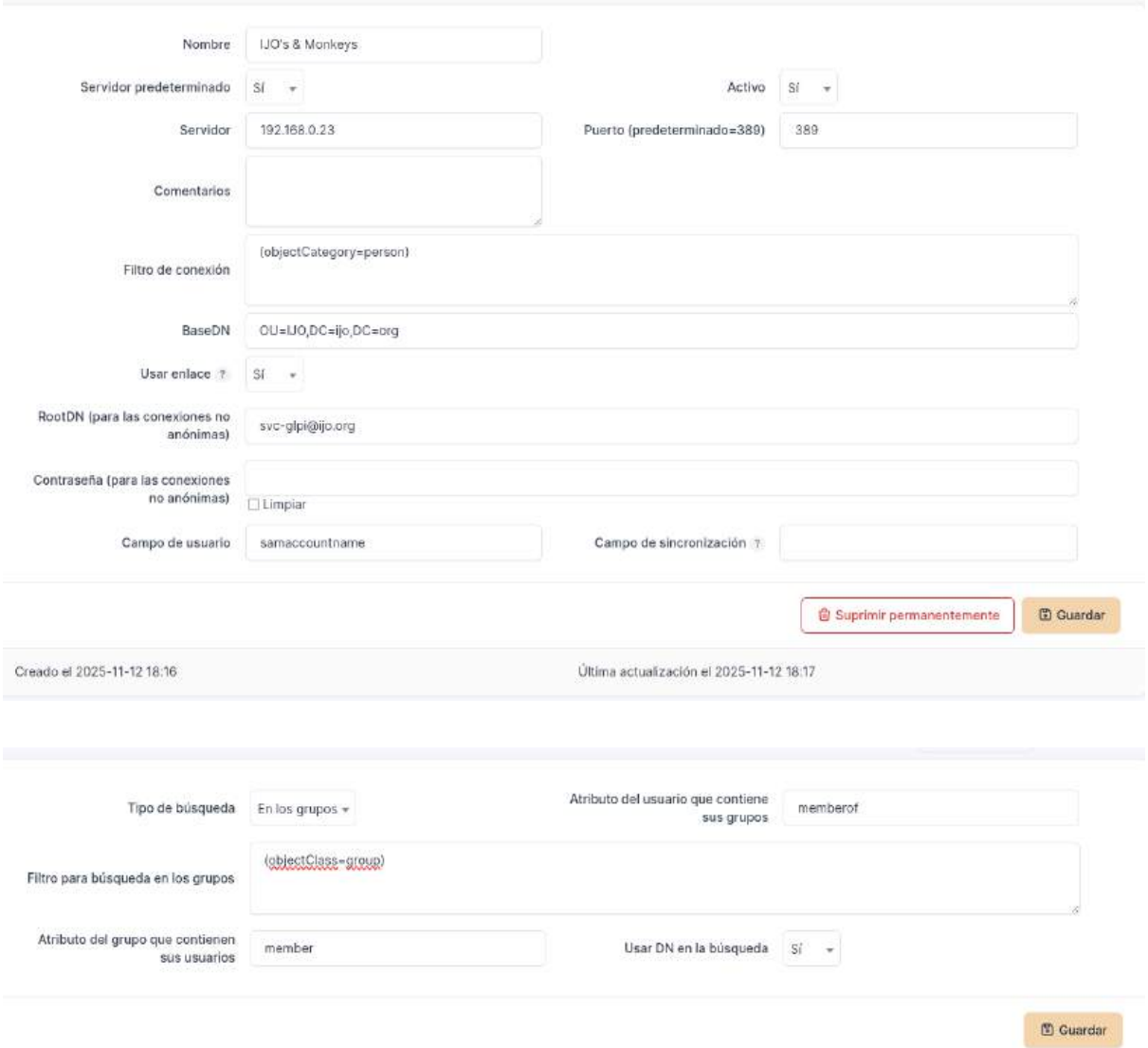
Integración con Active Directory (LDAP)

El siguiente paso consiste en integrar GLPI con el **Active Directory (AD)** de la organización, de modo que los usuarios del dominio puedan autenticarse con sus credenciales y pertenecer a sus grupos de forma automática.

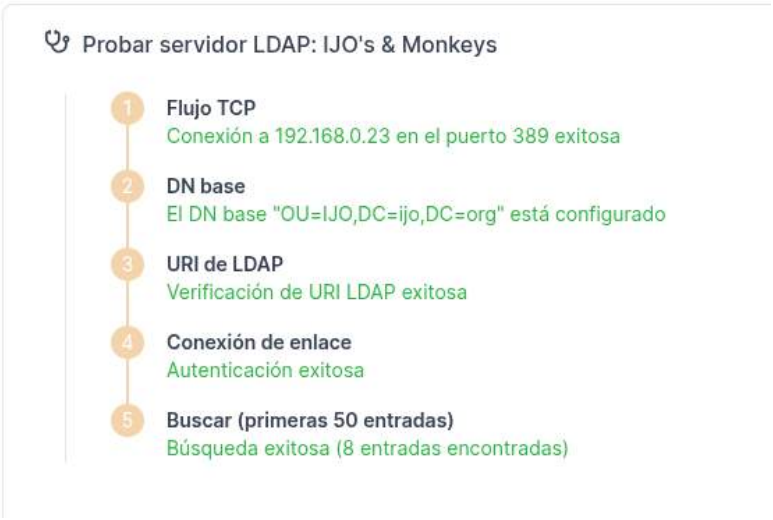
Desde **Setup > Authentication > LDAP directory**, añadiremos una nueva conexión al directorio LDAP, especificando los parámetros del servidor de AD.

Aquí surge una particularidad: GLPI presenta ciertas limitaciones con los **certificados autofirmados**, rechazando por defecto las conexiones SSL sin validación completa. Por ese motivo, y dado que el entorno de la ONG no

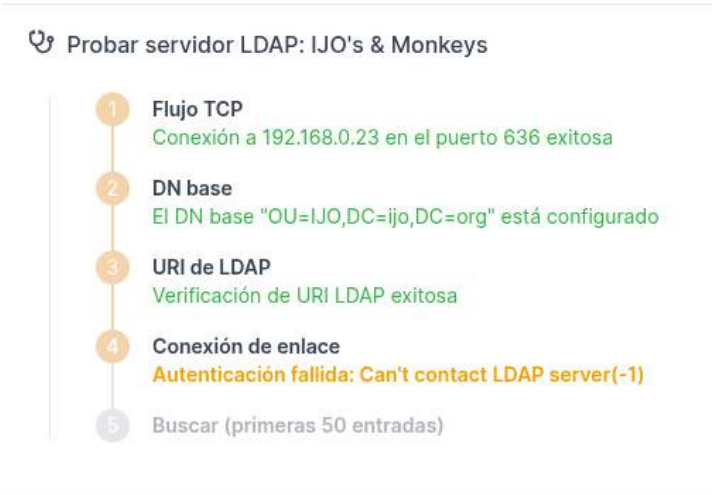
cuenta aún con una autoridad certificadora interna, la conexión se establecerá **sin cifrado** (modo *plain LDAP*) para evitar errores de verificación.



Con **ldap** y el puerto 389:



Con **ldaps** y el puerto 636:



Sincronización de grupos y usuarios

Con la conexión LDAP configurada, debemos sincronizar primero los **grupos**, y después los **usuarios**.

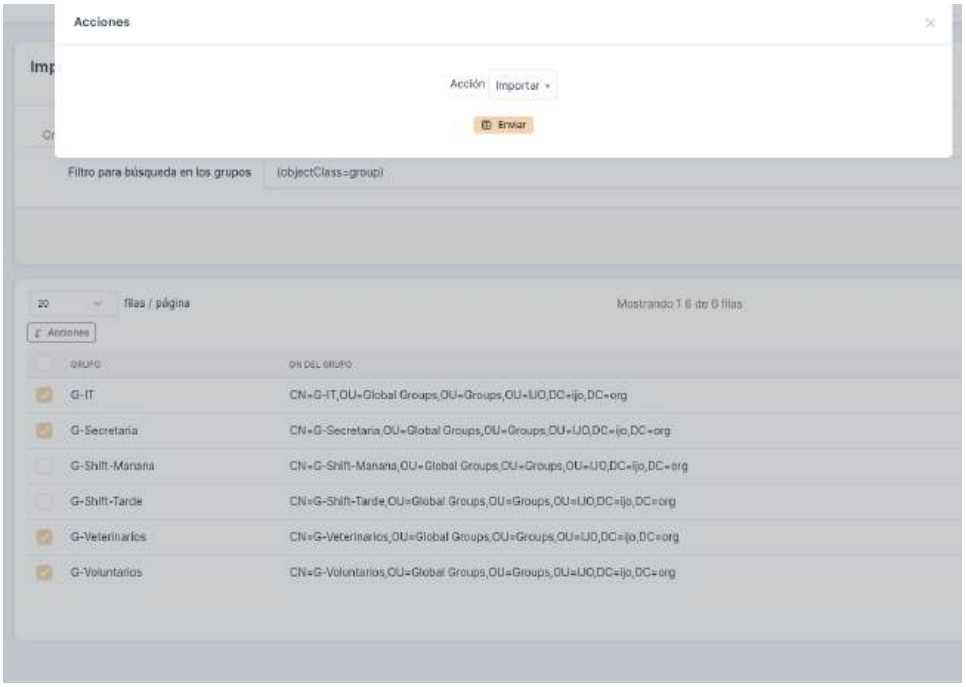
Esto es fundamental, ya que si los grupos no se importan antes, los usuarios no se vincularán correctamente a los suyos.

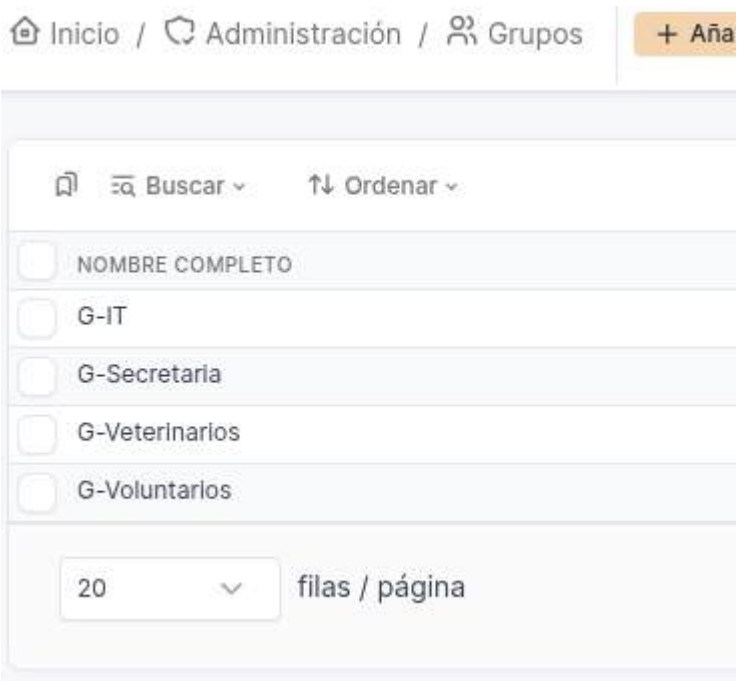
Para ello, cerramos la sesión actual y volvemos a iniciar sesión como `glpi` para aplicar los cambios.

Vamos a **Administration > Groups** y seleccionamos *Enlace a directorio LDAP*.

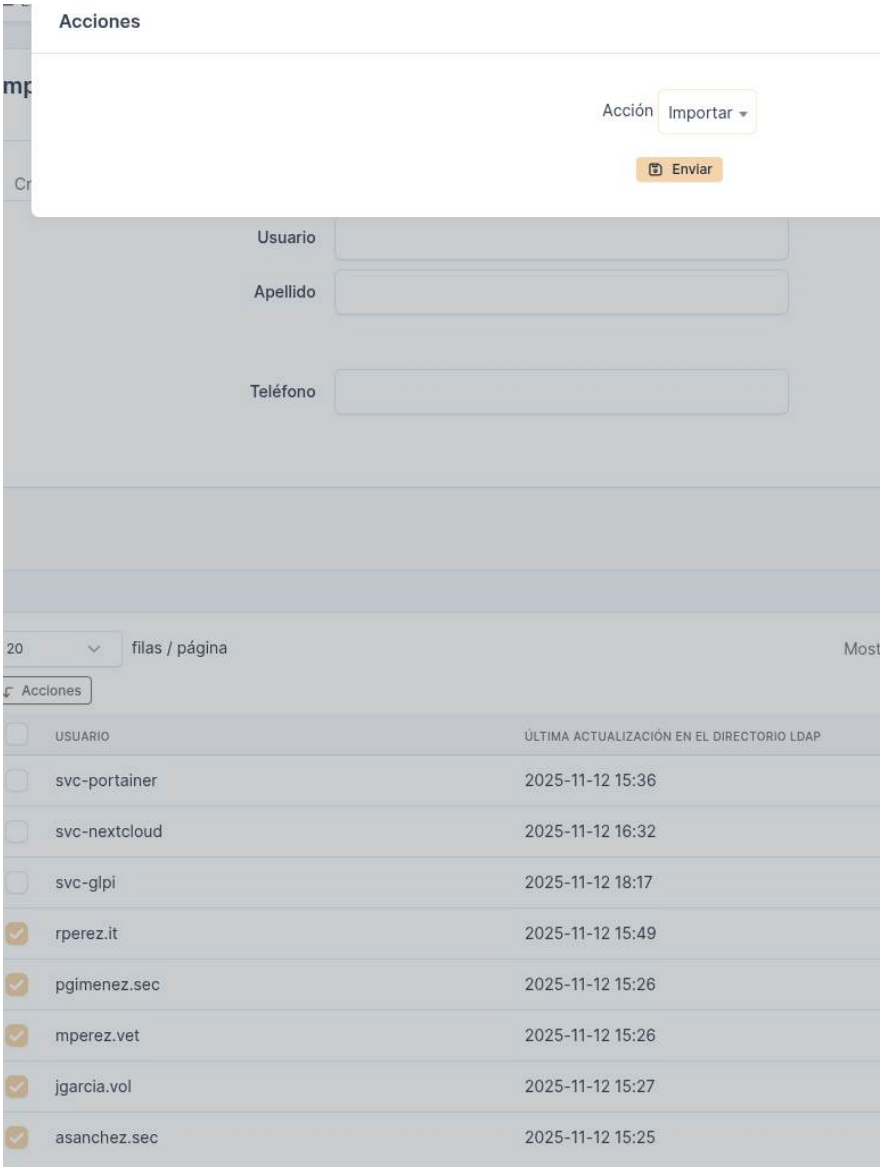
Dentro, clicamos en **Importación de nuevos grupos**, y aparecerán los grupos detectados mediante el filtro (objectClass=group).

Seleccionamos los grupos deseados y los importamos.

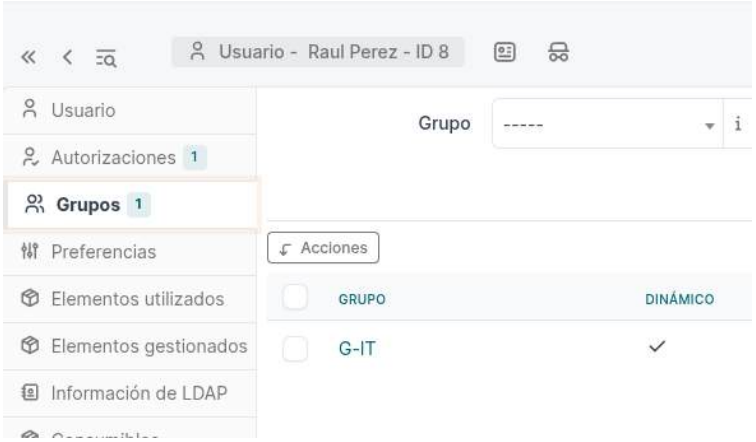

Acciones
Acción
Importar
Enviar
Filtro para búsqueda en los grupos
(objectClass=group)
20
filas / página
Mostrando 1 6 de 6 filas
Acciones
GRUPO
DN DEL GRUPO
G-IT
CN=G-IT,OU=Global Groups,OU=Groups,OU=IJO,DC=ijo,DC=org
G-Secretaria
CN=G-Secretaria,OU=Global Groups,OU=Groups,OU=IJO,DC=ijo,DC=org
G-Shift-Manana
CN=G-Shift-Manana,OU=Global Groups,OU=Groups,OU=IJO,DC=ijo,DC=org
G-Shift-Tarde
CN=G-Shift-Tarde,OU=Global Groups,OU=Groups,OU=IJO,DC=ijo,DC=org
G-Veterinarios
CN=G-Veterinarios,OU=Global Groups,OU=Groups,OU=IJO,DC=ijo,DC=org
G-Voluntarios
CN=G-Voluntarios,OU=Global Groups,OU=Groups,OU=IJO,DC=ijo,DC=org



Repetimos el proceso en **Administration > Users**, para importar los usuarios del dominio.



Si se han seguido los pasos correctamente, los usuarios importados quedarán automáticamente asociados a sus grupos de AD.

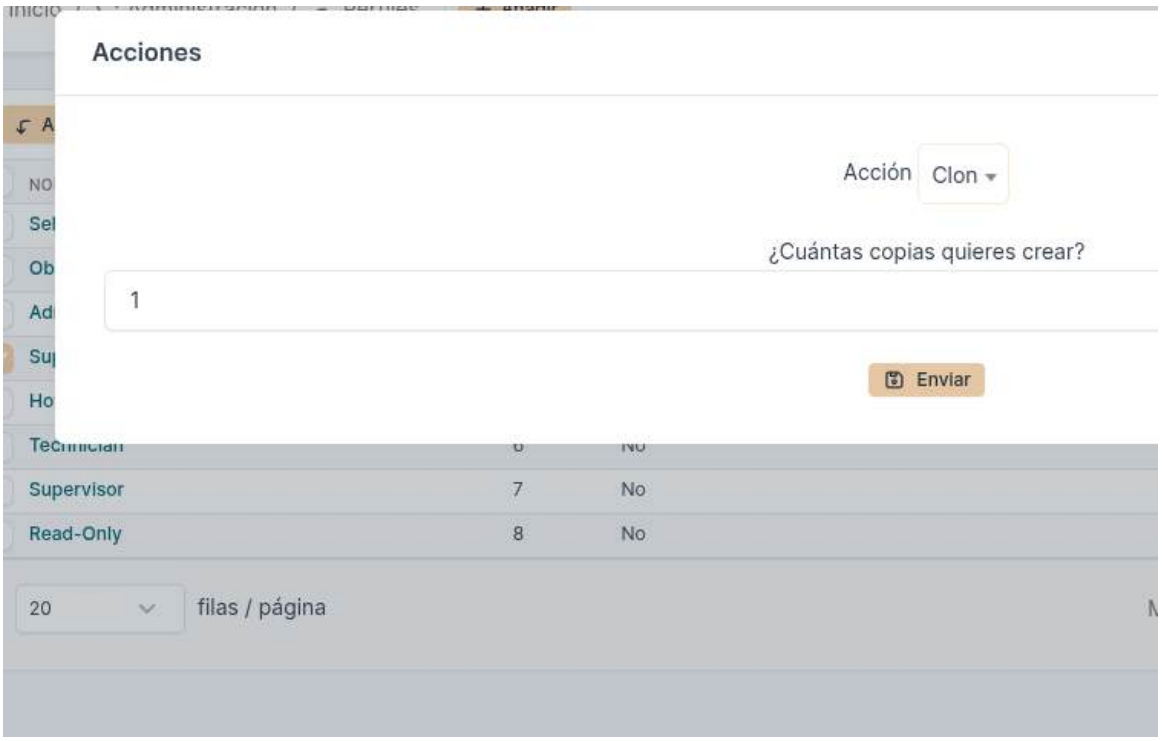


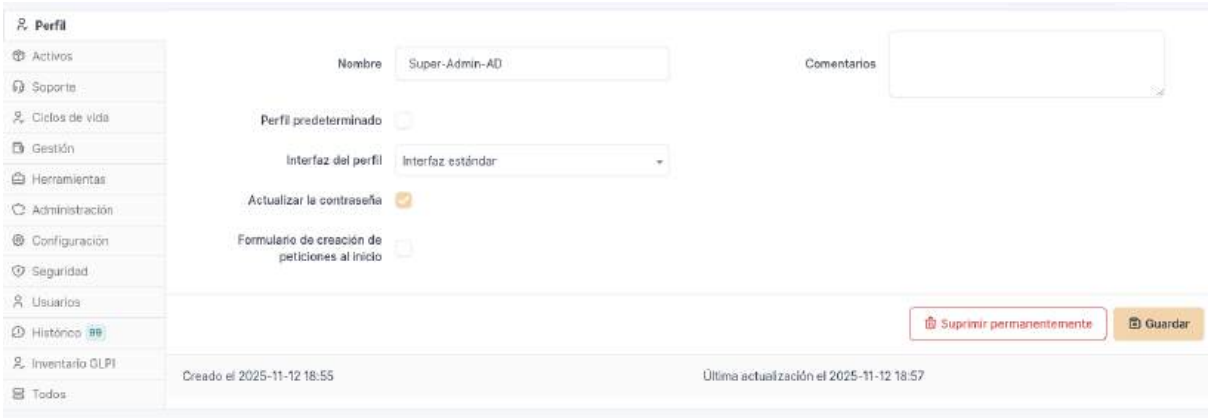
Asignación de permisos al grupo G-IT

A continuación, configuraremos los permisos avanzados del grupo **G-IT**.

En un entorno productivo, otorgar permisos de *Super-Admin* a un grupo completo **no es recomendable**, ya que implica acceso total al sistema. No obstante, para efectos de administración inicial, lo aplicaremos de forma temporal.

Desde **Administration > Profiles**, clonamos el perfil *Super-Admin* y lo renombramos a **Super-Admin-AD**.

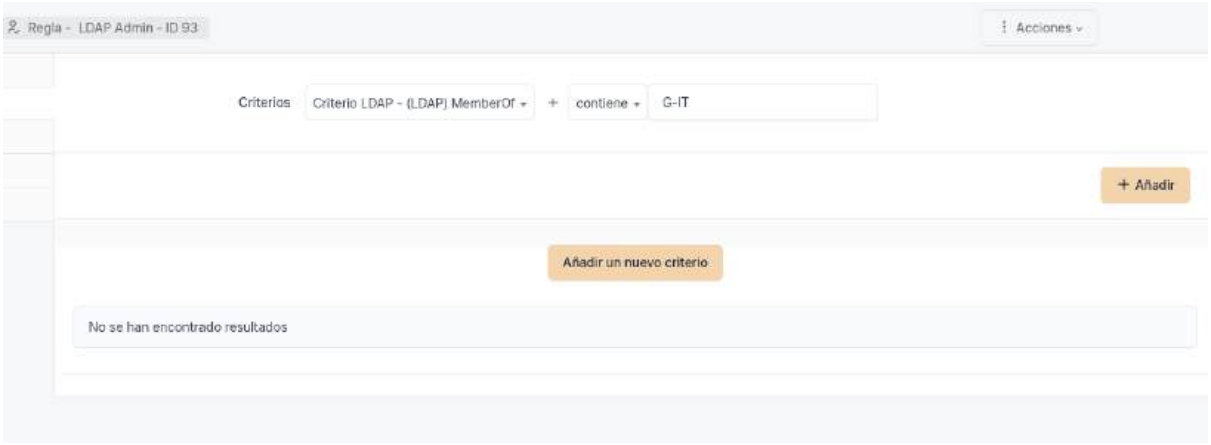




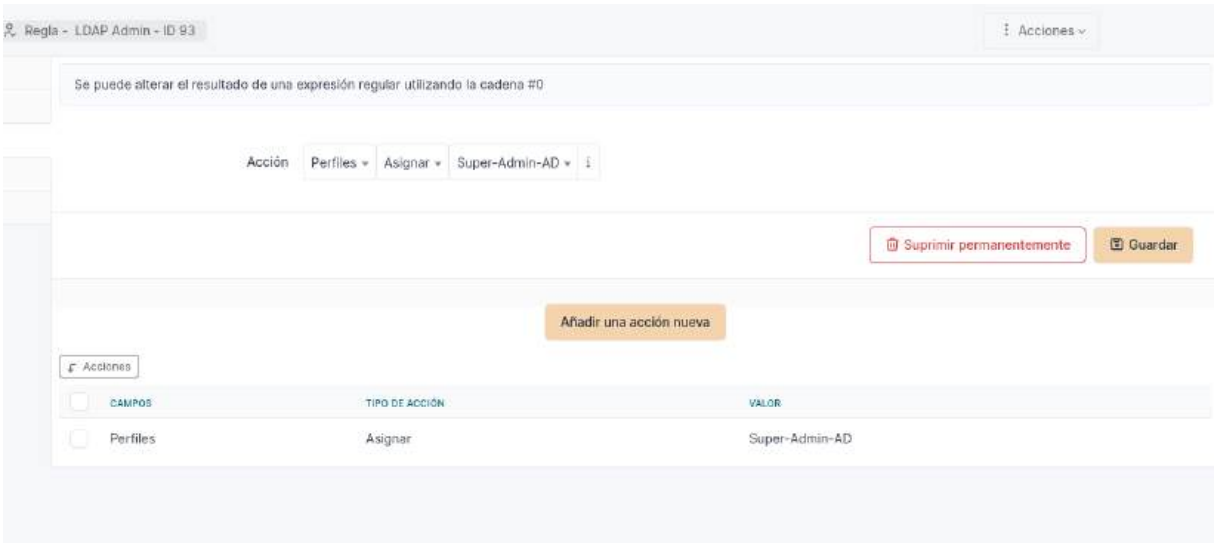
Luego, accedemos a **Administration > Rules > Rules for assigning authorizations** y añadimos una nueva regla.

Le damos un nombre y una descripción orientativos.

En la pestaña *Criteria*, agregamos un nuevo criterio que relacione el grupo LDAP G-IT.

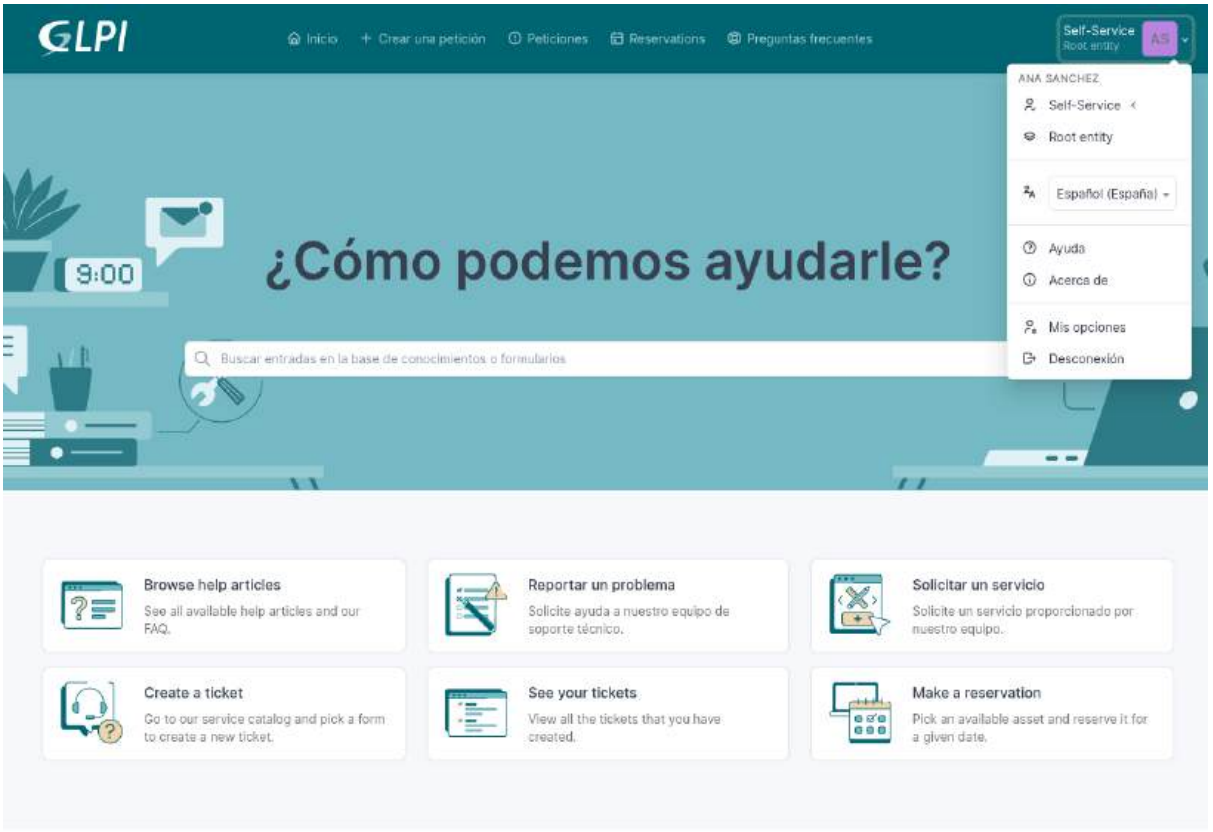


En *Actions*, establecemos que el perfil asignado sea **Super-Admin-AD**, y guardamos los cambios.

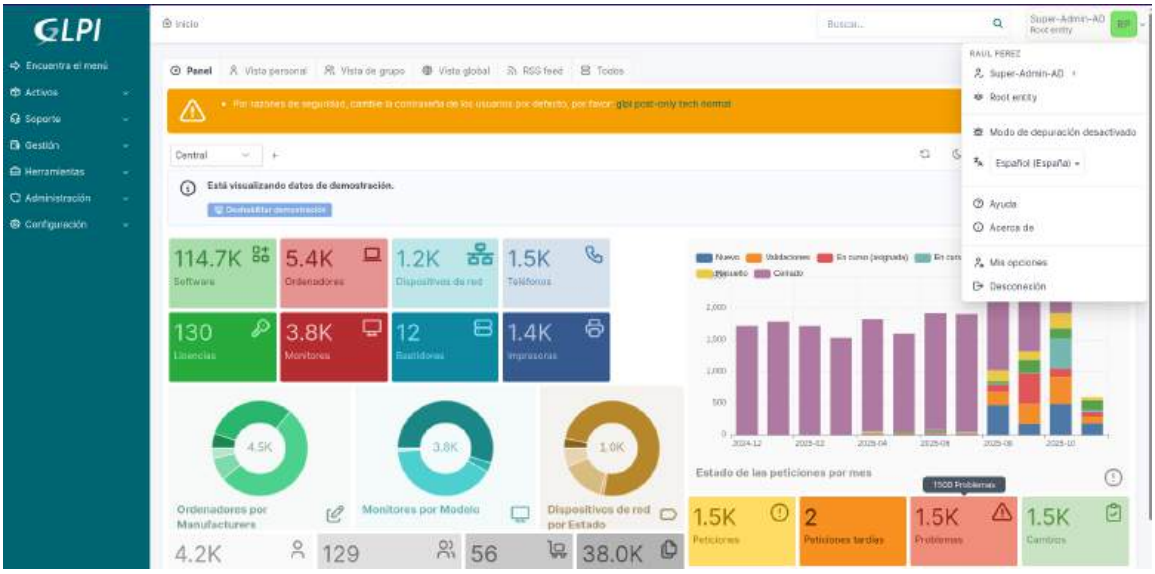


Con esta configuración, cualquier usuario perteneciente al grupo **G-IT** obtendrá permisos administrativos dentro de GLPI, mientras que el resto de usuarios conservará sus permisos limitados.

Esto es la página de inicio de GLPI del usuario **asanchez.sec**:



Esto es la página del usuario **rperez.it**:



Habilitación del inventario automático

Más adelante, una vez creadas las políticas y configurado el entorno de clientes, activaremos la opción que permitirá a los usuarios **reportar incidencias de equipos directamente desde sus estaciones de trabajo**.

Esto será posible gracias al **inventario automático** proporcionado por *GLPI Inventory*, que se desplegará en los equipos del dominio mediante un script remoto.

De este modo, cada equipo del dominio reportará su estado, hardware, software y posibles alertas de forma centralizada, permitiendo al equipo de soporte técnico gestionar la infraestructura con una visión completa y actualizada del parque informático de la ONG.

Guacamole

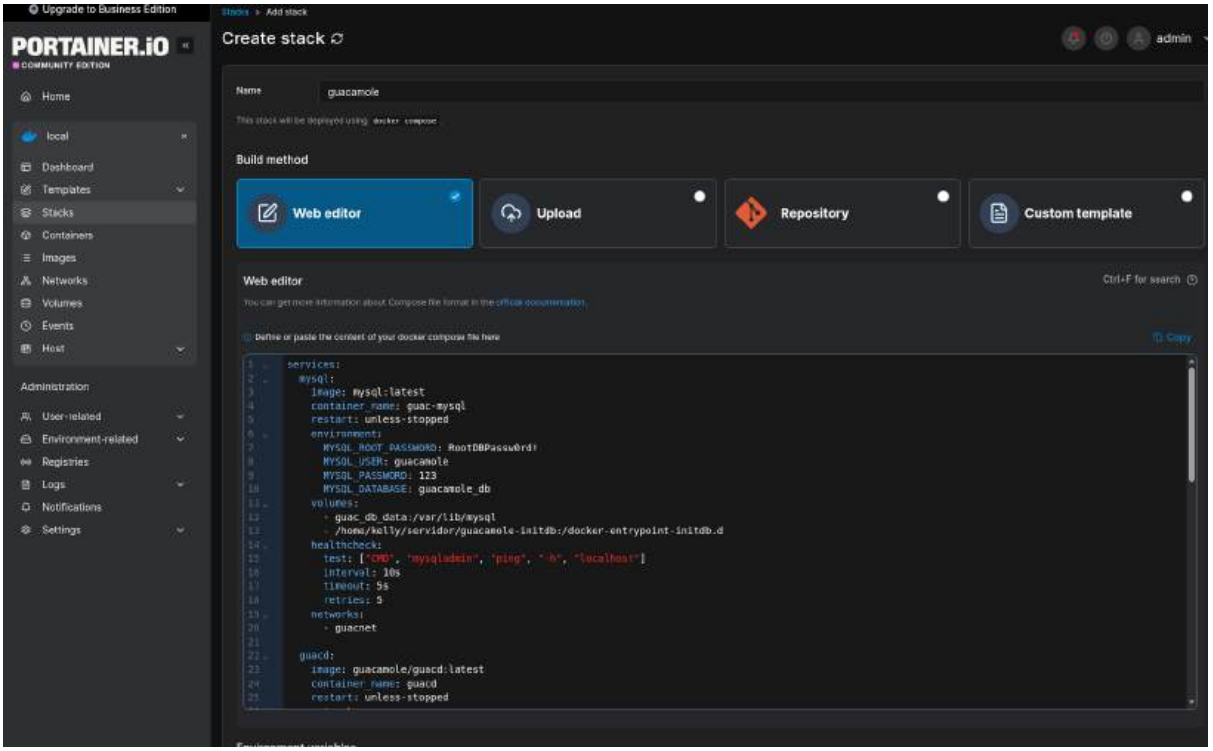
Apache Guacamole ofrece un **acceso remoto seguro y sin cliente** a los equipos y servidores de la ONG.
Totalmente web, permite que un técnico del grupo **G-IT** acceda al escritorio de un equipo o a un servidor por **RDP o SSH**, sin instalar nada en su ordenador.

Está estrechamente vinculado con **GLPI**: cuando un usuario abre un ticket, el técnico puede, previa coordinación, acceder al equipo afectado para diagnosticar y resolver el problema.
Para funcionar, los equipos deben tener el puerto **RDP (3389)** habilitado y permitido en el firewall, lo cual se gestiona mediante una **GPO** específica.

Solo los usuarios del grupo **G-IT** tienen acceso a este servicio, reforzando la confidencialidad y la seguridad interna.

Instalación y puesta en marcha

Apache Guacamole se despliega de manera sencilla siempre que tengamos los archivos necesarios en las rutas correctas dentro del servidor de contenedores. El despliegue se realiza mediante **Portainer**, ejecutando el *stack* correspondiente.



Una vez levantado el stack, el acceso al panel de administración puede realizarse de dos formas:

- Mediante la **IP del servidor** seguida del puerto 8086 y la ruta /guacamole.
- Mediante el dominio configurado en Pfsense: https://guacamole.ijo.org:8086/guacamole

Al ingresar por primera vez, utilizamos las credenciales por defecto:

- **Usuario:** guacadmin
- **Contraseña:** guacadmin

Configuración inicial y permisos

El primer paso es **crear el grupo G-IT**, que corresponde al nombre del grupo de Active Directory de los administradores del sistema.
A este grupo se le otorgarán **todos los permisos administrativos** dentro de Guacamole, asegurando que únicamente los miembros de G-IT puedan acceder al panel y gestionar las conexiones remotas.

PARAMÈTRES

Sessions Actives | Historique | Utilisateurs | Groupes | Con

Cliquez ou appuyez sur un groupe ci-dessous pour gérer ce groupe. En

Nouveau Groupe | Filtre

G-IT

MODIFIER GROUPE

Nom Groupe: G-IT

Désactivé: ☐

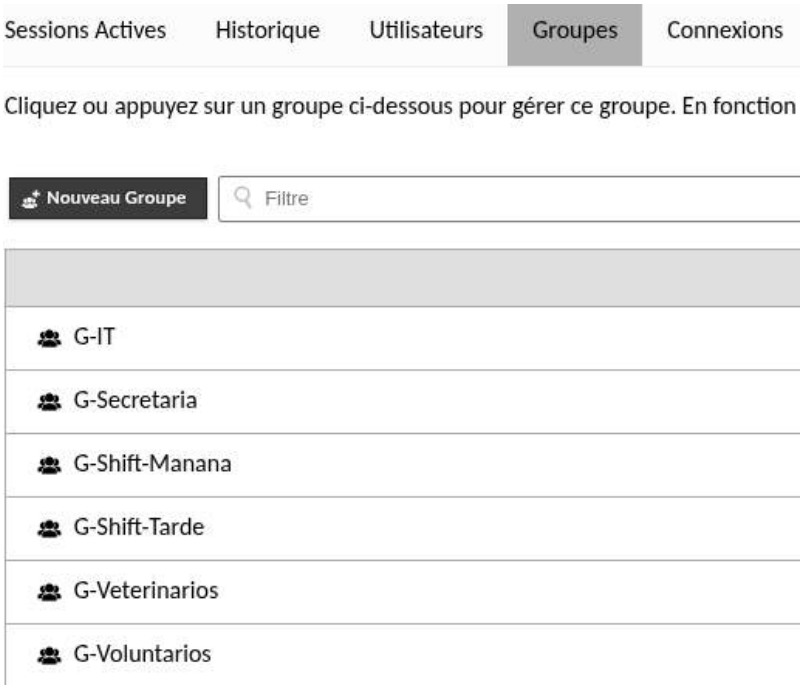
PERMISSIONS

Administration du système:	☑
Audit system:	☑
Créer de nouveaux utilisateurs:	☑
Créer de nouveaux groupes d'utilisateurs:	☑
Créer de nouvelles connexions:	☑
Créer de nouveaux groupes de connexion:	☑
Créer de nouveaux profils de partage:	☑

La integración con **LDAP** se define directamente en el archivo docker-compose.yml, especificando los parámetros necesarios para que Guacamole se configure automáticamente y permita autenticación directa contra Active Directory. Esto asegura que cualquier cambio en AD (usuarios y grupos) se refleje inmediatamente en Guacamole sin necesidad de gestión manual de credenciales.

Ya podríamos acceder con un usuario de la **OU=IT**, los demás usuarios no podrán iniciar sesión.

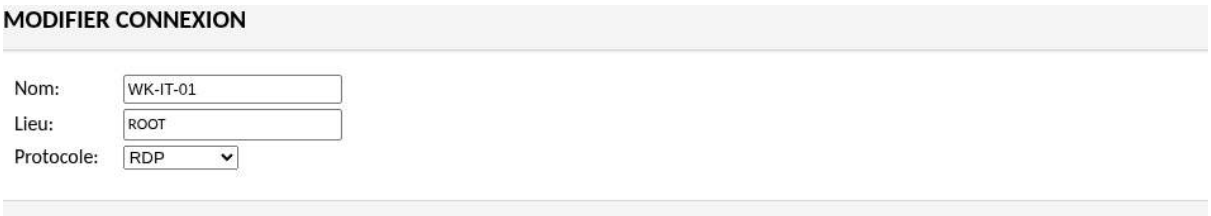

Sessions Actives
Historique
Utilisateurs
Groupes
Connexions
Cliquez ou appuyez sur un utilisateur en dessous pour le gérer. Selon vos permi
Nouvel Utilisateur
Filtre
Identifiant
guacadmin
rperez.it


Sessions Actives
Historique
Utilisateurs
Groupes
Connexions
Cliquez ou appuyez sur un groupe ci-dessous pour gérer ce groupe. En fonction
Nouveau Groupe
Filtre
G-IT
G-Secretaria
G-Shift-Manana
G-Shift-Tarde
G-Veterinarios
G-Voluntarios

Creación de conexiones remotas

Para permitir la asistencia remota a los usuarios de la ONG, crearemos conexiones de tipo **RDP** que simulen escenarios reales. Por ejemplo, para un cliente Windows:

Se crea una **nueva conexión RDP** en Guacamole.



Se especifica la **IP del equipo cliente** y el **puerto 3389**.

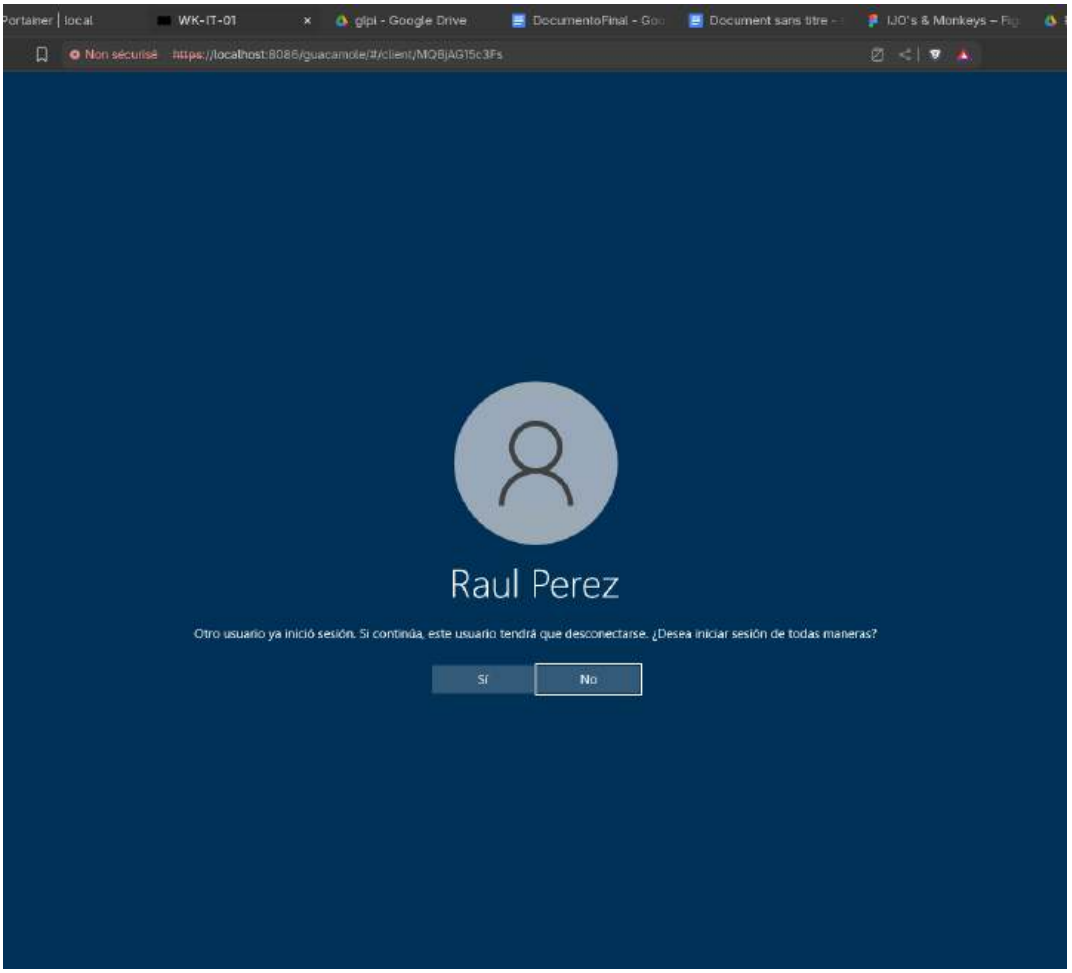
Se configura la conexión para utilizar una cuenta **administrador** del equipo destino. Y deberemos habilitar la casilla de **ignorar certificado del servidor**.

Nota: más adelante, los usuarios del grupo G-IT estarán incluidos automáticamente en el grupo **Administradores del dominio**, permitiendo acceso total a los equipos de los miembros de la ONG. Además, para garantizar que los clientes permitan conexiones remotas, aplicaremos una GPO específica que habilite el acceso remoto y configure los permisos necesarios en los equipos del dominio.

Prueba de la conexión

Una vez creada la conexión, esta aparecerá en el panel de inicio de Guacamole. Para probarla:

Seleccionamos la conexión creada y comprobamos que se puede acceder al escritorio del cliente Windows de forma remota, segura y estable.



Wiki.js

La **documentación** es el alma de cualquier organización bien gestionada. **Wiki.js** da forma a ese conocimiento: una wiki moderna, estructurada y segura, donde cada área de la ONG puede compartir su saber.

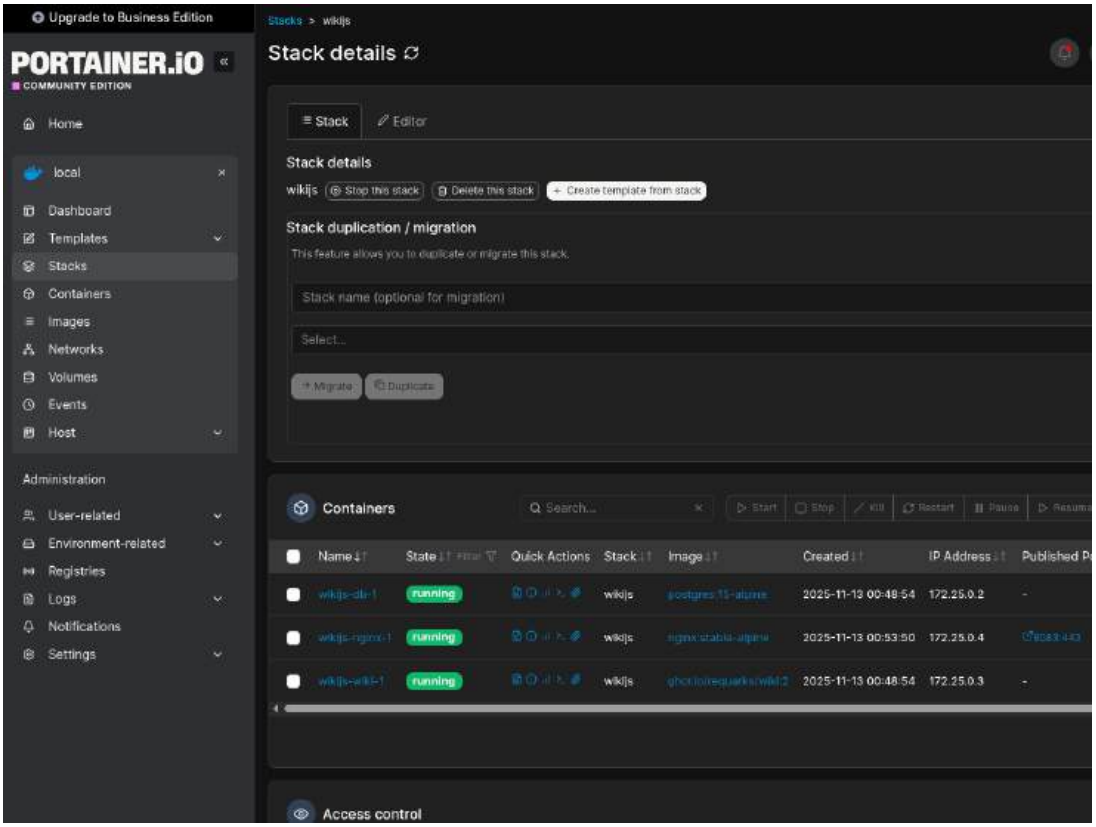
A diferencia de un sistema de carpetas tradicional, Wiki.js utiliza una **estructura lógica o virtual**, dividida en cuatro grandes secciones:

- **Informática:** acceso exclusivo a los usuarios registrados del AD, con manuales, guías y configuraciones internas, útiles para los usuarios de la ONG.
- **Medicina:** administrada por G-Veterinarios, visible para todos, pero editable solo por el grupo G-Veterinarios, el grupo G-IT solo puede ver el historial de modificaciones y eliminar documentos si es necesario.
  Infraestructura: oculta para todos excepto G-IT, donde se documenta la arquitectura técnica y los procedimientos críticos.
- **Actualidad:** abierta a todos los usuarios de AD y usuarios sin autenticar; un espacio libre para compartir noticias, proyectos o reflexiones.

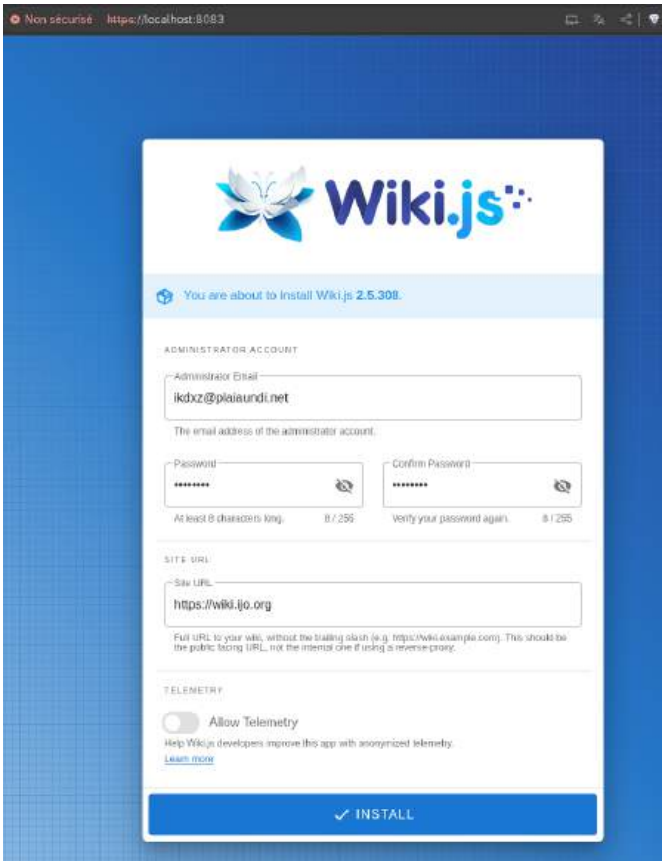
Antes de vincular el AD, se crean los grupos internos con nombres idénticos a los de Active Directory para mapear los permisos correctamente.
El acceso se realiza mediante **LDAPS**, asegurando que la documentación sea un espacio **vivo, colaborativo y seguro**.

Instalación y puesta en marcha

Para iniciar con la instalación de Wiki.js, el primer paso consiste en **levantar el Stack** correspondiente en nuestro servidor de contenedores. Una vez que el Stack esté activo, accedemos a la plataforma a través de la **IP del servidor** y el puerto 8083 o, si ya se encuentra configurado en Pfsense, mediante el dominio https://wiki.ijo.org:8083.

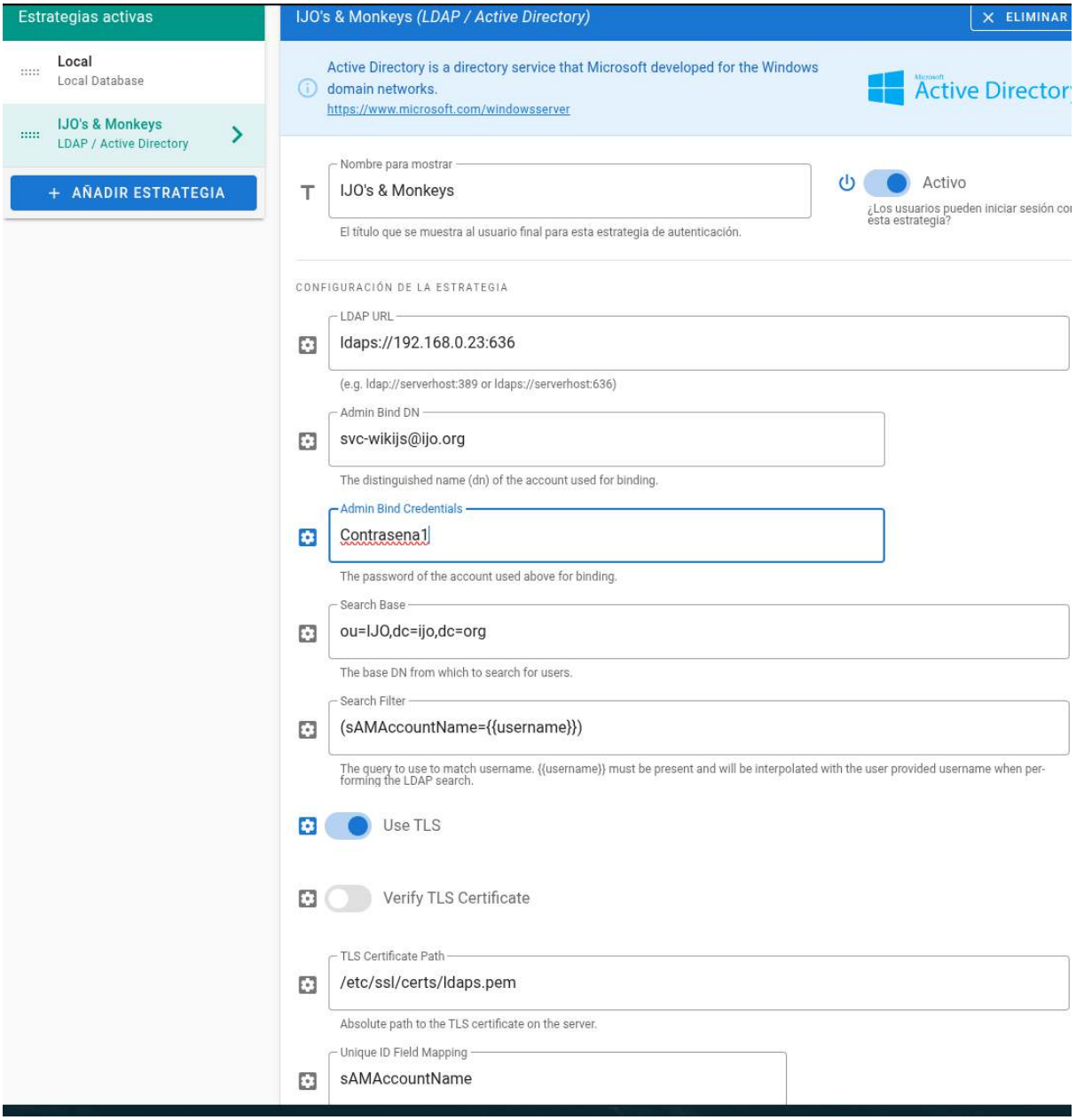


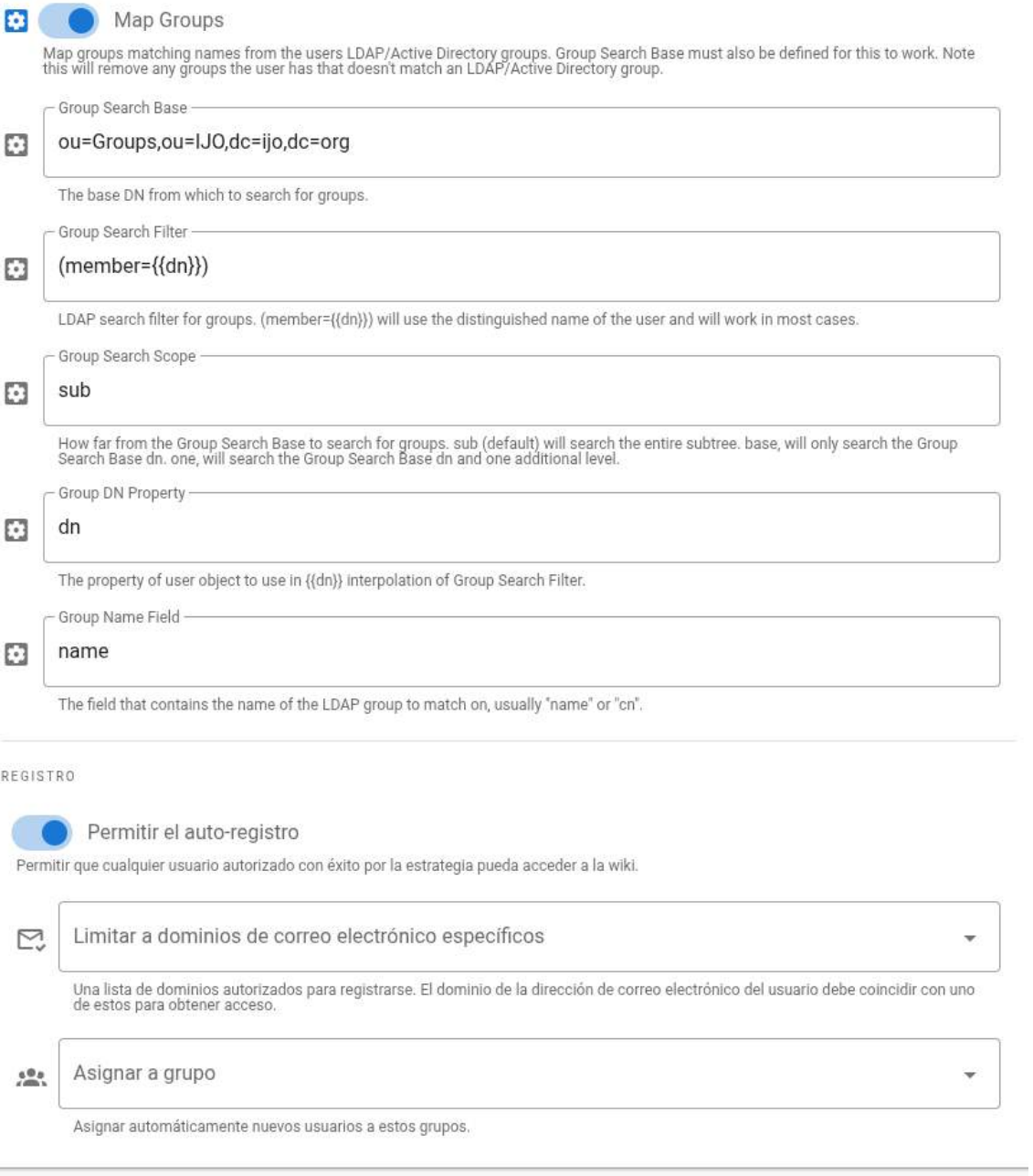
Al abrir la página, introducimos una **cuenta de administrador**, que servirá como usuario principal para la configuración inicial. Tras completar el proceso de instalación, iniciamos sesión con esta cuenta para continuar con la configuración detallada de la plataforma.



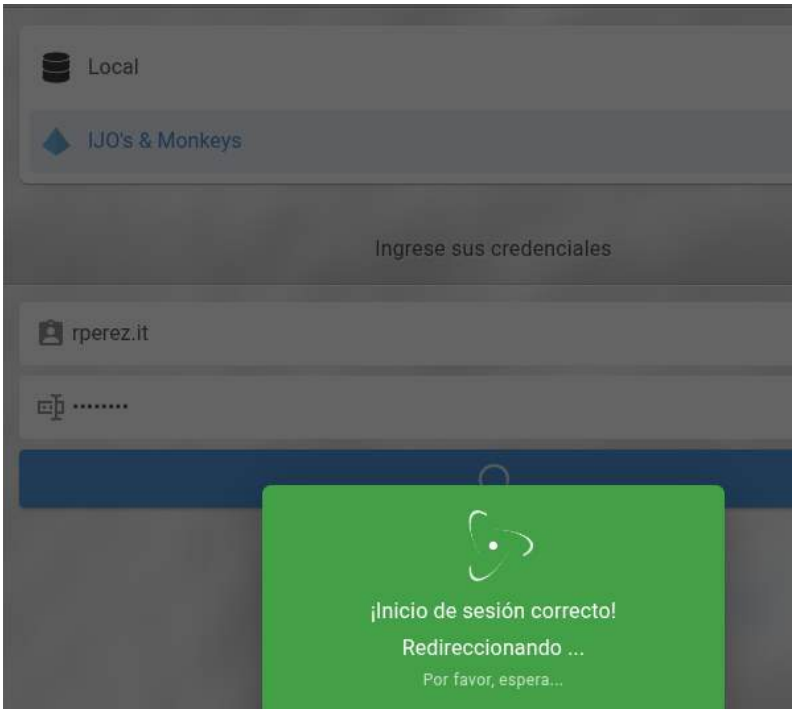
Configuración de LDAP/Active Directory

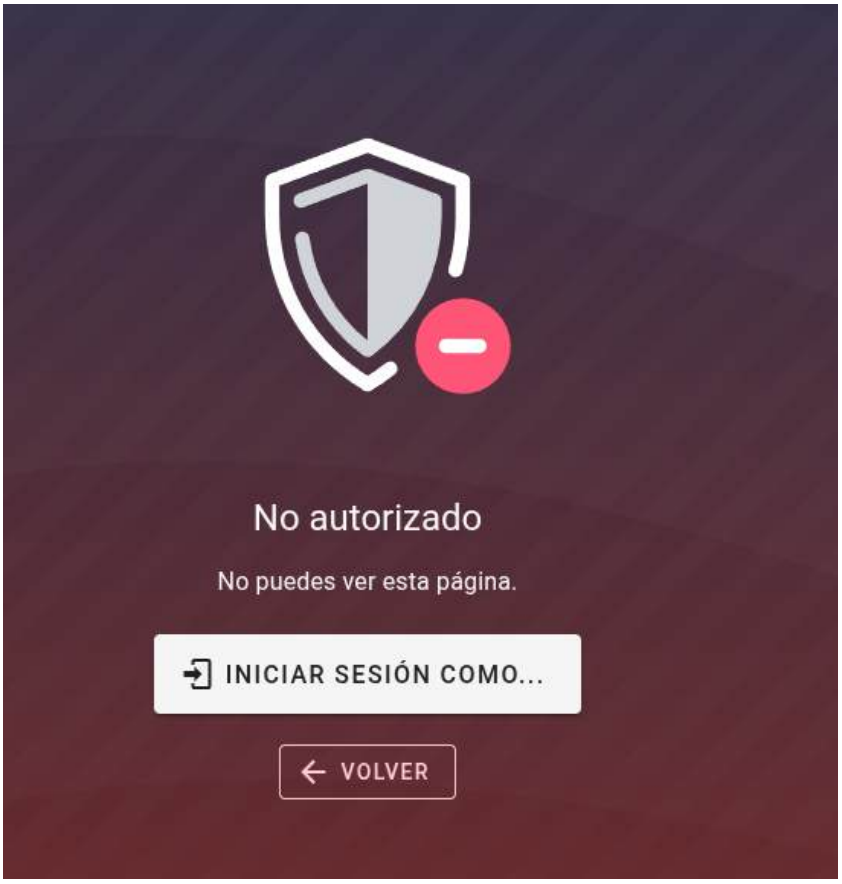
Dentro de la sección de **Administración**, nos dirigimos a la opción de **Autenticación** y añadimos una **nueva estrategia de LDAP/Active Directory**. Configuramos la conexión al servidor AD de acuerdo con la estructura de la organización, asegurándonos de que los usuarios puedan autenticarse correctamente contra nuestro directorio activo.


Estrategias activas
Local
Local Database
IJO's & Monkeys
LDAP / Active Directory
+ AÑADIR ESTRATEGIA
IJO's & Monkeys (LDAP / Active Directory)
ELIMINAR
Active Directory is a directory service that Microsoft developed for the Windows domain networks.
https://www.microsoft.com/windowsserver
Active Director
Nombre para mostrar
IJO's & Monkeys
El título que se muestra al usuario final para esta estrategia de autenticación.
Activo
¿Los usuarios pueden iniciar sesión co esta estrategia?
CONFIGURACIÓN DE LA ESTRATEGIA
LDAP URL
ldaps://192.168.0.23:636
(e.g. ldap://serverhost:389 or ldaps://serverhost:636)
Admin Bind DN
svc-wikijs@ijo.org
The distinguished name (dn) of the account used for binding.
Admin Bind Credentials
Contrasena1
The password of the account used above for binding.
Search Base
ou=IJO,dc=ijo,dc=org
The base DN from which to search for users.
Search Filter
(sAMAccountName={{username}})
The query to use to match username. {{username}} must be present and will be interpolated with the user provided username when performing the LDAP search.
Use TLS
Verify TLS Certificate
TLS Certificate Path
/etc/ssl/certs/ldaps.pem
Absolute path to the TLS certificate on the server.
Unique ID Field Mapping
sAMAccountName


Map Groups
Map groups matching names from the users LDAP/Active Directory groups. Group Search Base must also be defined for this to work. Note this will remove any groups the user has that doesn't match an LDAP/Active Directory group.
Group Search Base
ou=Groups,ou=IJO,dc=ijo,dc=org
The base DN from which to search for groups.
Group Search Filter
(member={{dn}})
LDAP search filter for groups. (member={{dn}}) will use the distinguished name of the user and will work in most cases.
Group Search Scope
sub
How far from the Group Search Base to search for groups. sub (default) will search the entire subtree. base, will only search the Group Search Base dn. one, will search the Group Search Base dn and one additional level.
Group DN Property
dn
The property of user object to use in {{dn}} interpolation of Group Search Filter.
Group Name Field
name
The field that contains the name of the LDAP group to match on, usually "name" or "cn".
REGISTRO
Permitir el auto-registro
Permitir que cualquier usuario autorizado con éxito por la estrategia pueda acceder a la wiki.
Limitar a dominios de correo electrónico específicos
Una lista de dominios autorizados para registrarse. El dominio de la dirección de correo electrónico del usuario debe coincidir con uno de estos para obtener acceso.
Asignar a grupo
Asignar automáticamente nuevos usuarios a estos grupos.

Una vez completada la configuración, es momento de probar el acceso con un usuario de AD. Inicialmente, el usuario podrá iniciar sesión, pero no tendrá permisos administrativos ni de edición. Para asignar estos permisos, debemos crear los grupos de LDAP dentro de Wiki.js.





Creación de grupos y asignación de permisos

1. **Grupo G-IT:** Este grupo tendrá **permisos de administración**, lo que permite gestionar la configuración completa de Wiki.js.
2. **Resto de grupos**: Posteriormente se crean los grupos restantes: G-Veterinarios, G-Secretaría, G-Voluntarios. Cada grupo tendrá permisos específicos según su función y responsabilidad dentro de la ONG.

ID	Name	Users
1	**Administrators**	1
2	**Guests**	1
3	**G-IT**	1
4	**G-Veterinarios**	0
5	**G-Secretaria**	0
6	**G-Voluntarios**	0

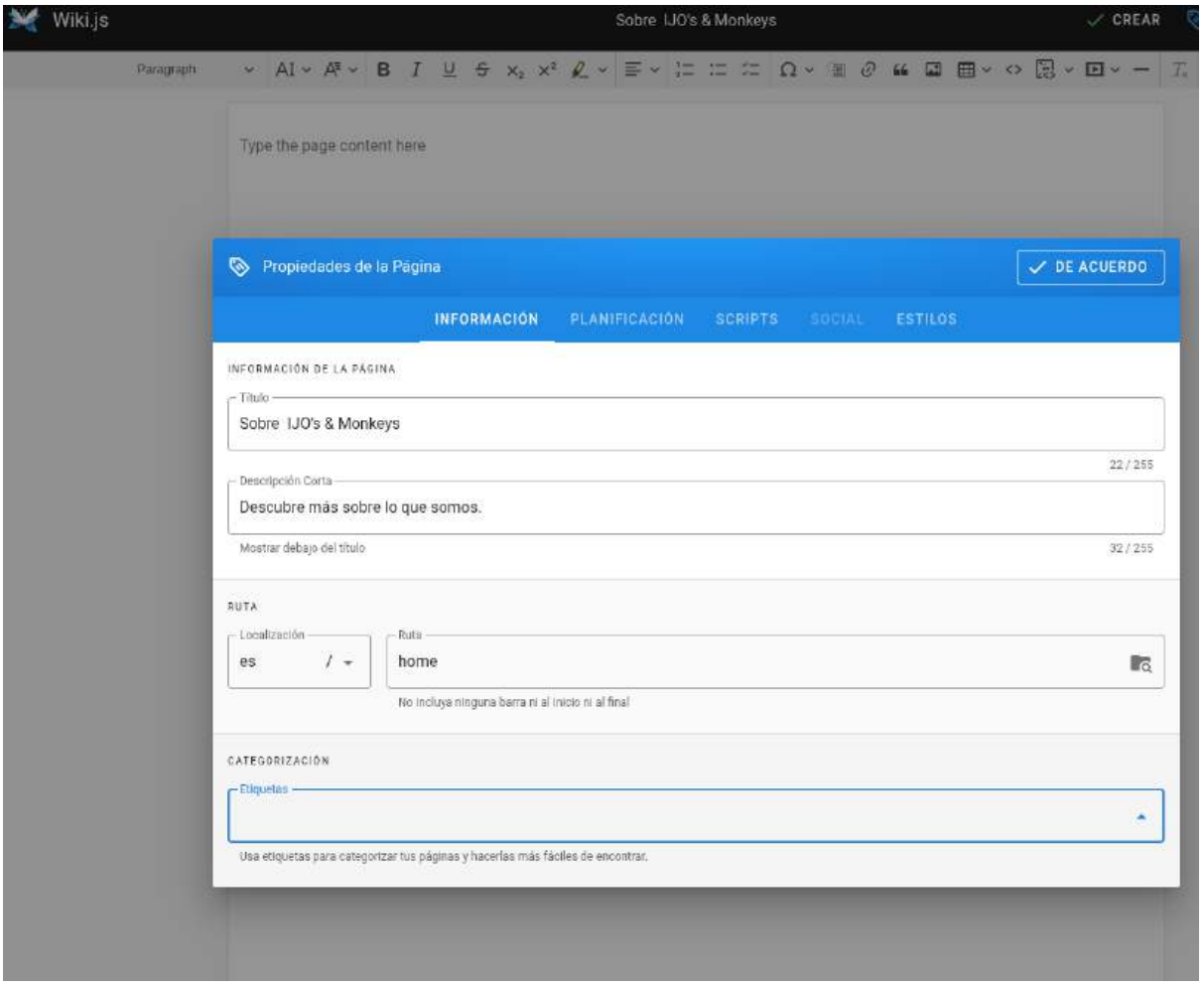
Después de crear el grupo G-IT, la pantalla de inicio será distinta para el usuario perteneciente a este grupo.

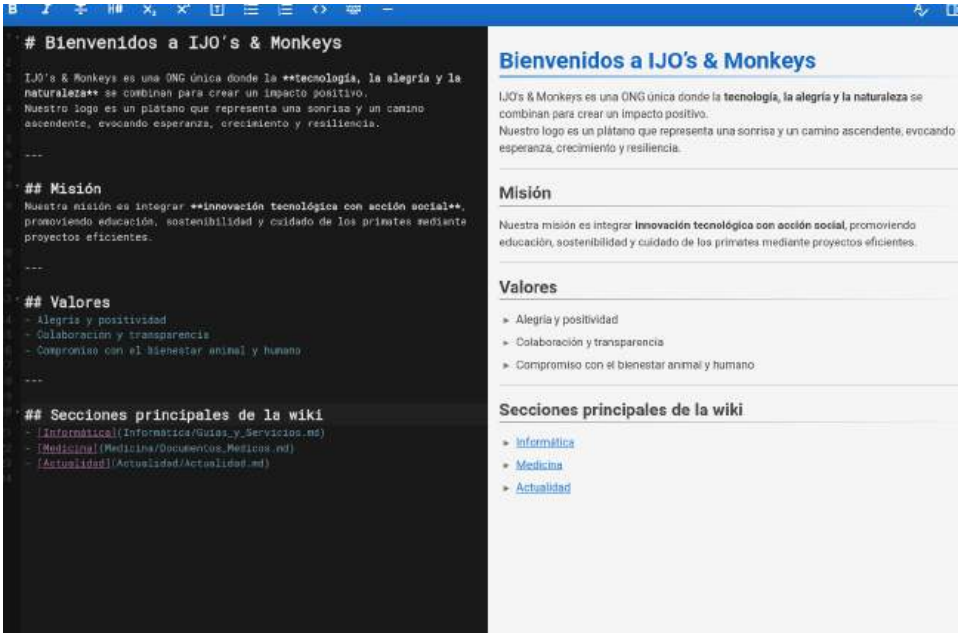
Con los grupos configurados, podemos proceder a crear páginas de prueba y establecer la **estructura de la wiki**. Es importante entender que Wiki.js utiliza **carpetas virtuales**: estas carpetas no se configuran directamente, sino que se generan automáticamente al crear páginas dentro de ellas.

Creación de páginas y reglas de acceso

Página de inicio: Servirá como punto de entrada principal a la wiki.

Secciones principales: Se crean páginas dentro de las carpetas virtuales **Infraestructura**, **Medicina**, **Informática**, **IJO** y **Actualidad**, cada una con contenido y permisos específicos.


Wiki.js
Sobre IJO's & Monkeys
CREAR
Paragraph
Type the page content here
Propiedades de la Página
DE ACUERDO
INFORMACIÓN
PLANIFICACIÓN
SCRIPTS
SOCIAL
ESTILOS
INFORMACIÓN DE LA PÁGINA
Título
Sobre IJO's & Monkeys
22 / 255
Descripción Corta
Descubre más sobre lo que somos.
Mostrar debajo del título
32 / 255
RUTA
Localización
es
/
Ruta
home
No incluya ninguna barra ni al inicio ni al final
CATEGORIZACIÓN
Etiquetas
Usa etiquetas para categorizar tus páginas y hacerlas más fáciles de encontrar.



```
# Bienvenidos a IJO's & Monkeys

IJO's & Monkeys es una ONG única donde la **tecnología, la alegría y la naturaleza** se combinan para crear un impacto positivo.
Nuestro logo es un plátano que representa una sonrisa y un camino ascendente, evocando esperanza, crecimiento y resiliencia.

---

## Misión
Nuestra misión es integrar **innovación tecnológica con acción social**, promoviendo educación, sostenibilidad y cuidado de los primates mediante proyectos eficientes.

---

## Valores
- Alegría y positividad
- Colaboración y transparencia
- Compromiso con el bienestar animal y humano

---

## Secciones principales de la wiki
- [Informática](Informática/Guías_y_Servicios.md)
- [Medicina](Medicina/Documentos_Médicos.md)
- [Actualidad](Actualidad/Actualidad.md)
```

Bienvenidos a IJO's & Monkeys

IJO's & Monkeys es una ONG única donde la **tecnología, la alegría y la naturaleza** se combinan para crear un impacto positivo.
Nuestro logo es un plátano que representa una sonrisa y un camino ascendente, evocando esperanza, crecimiento y resiliencia.

Misión

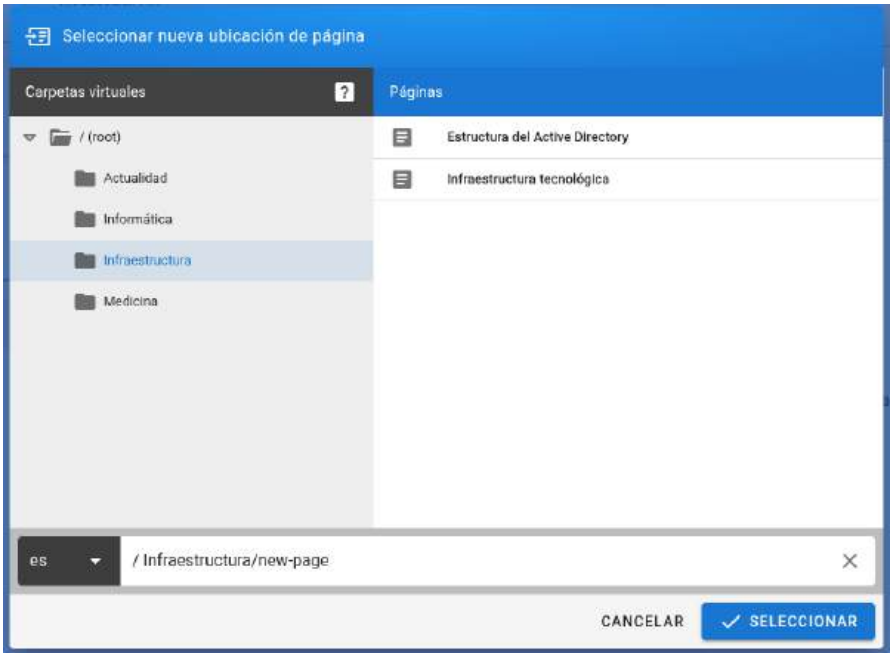
Nuestra misión es integrar **innovación tecnológica con acción social**, promoviendo educación, sostenibilidad y cuidado de los primates mediante proyectos eficientes.

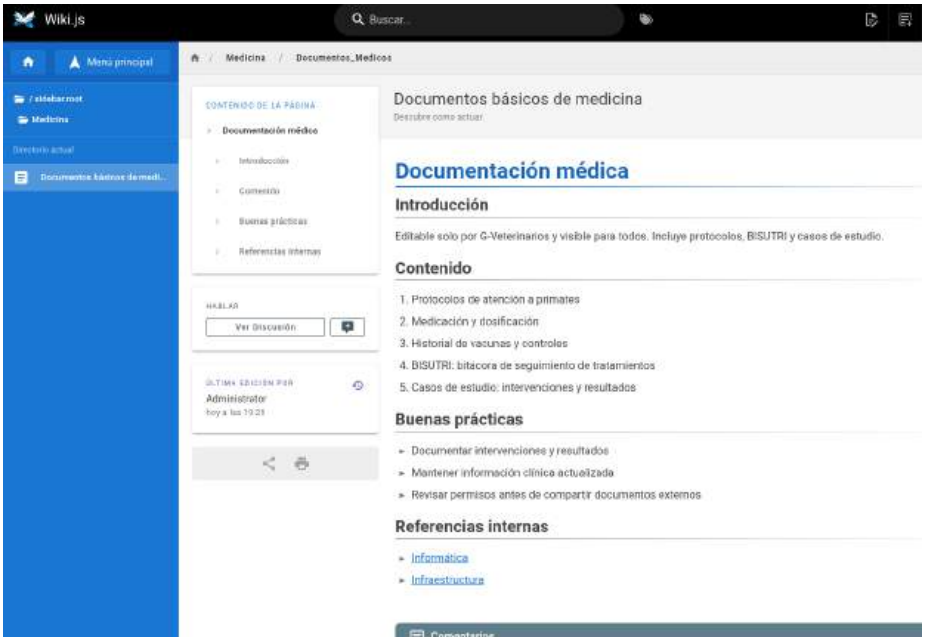
Valores

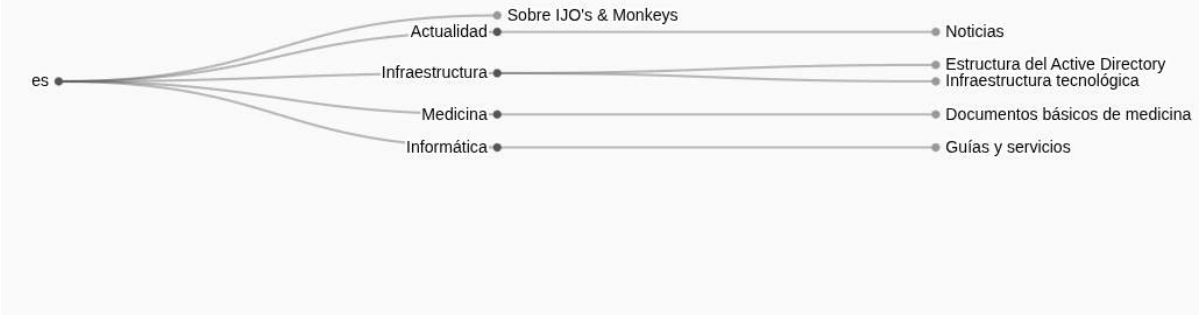
- Alegría y positividad
- Colaboración y transparencia
- Compromiso con el bienestar animal y humano

Secciones principales de la wiki

- Informática
- Medicina
- Actualidad


Seleccionar nueva ubicación de página
Carpetas virtuales
Páginas
/ (root)
Actualidad
Informática
Infraestructura
Medicina
Estructura del Active Directory
Infraestructura tecnológica
es
/ Infraestructura/new-page
CANCELAR
SELECCIONAR


Wiki.js
Buscar...
Menú principal
Medicina
Documentos_Medicos
Documentos básicos de medicina
Documentación médica
Introducción
Editable solo por G-Veterinarios y visible para todos. Incluye protocolos, BISUTRI y casos de estudio.
Contenido
1. Protocolos de atención a primates
2. Medicación y dosificación
3. Historial de vacunas y controles
4. BISUTRI: bitácora de seguimiento de tratamientos
5. Casos de estudio: intervenciones y resultados
Buenas prácticas
Documentar intervenciones y resultados
Mantener información clínica actualizada
Revisar permisos antes de compartir documentos externos
Referencias internas
Informática
Infraestructura



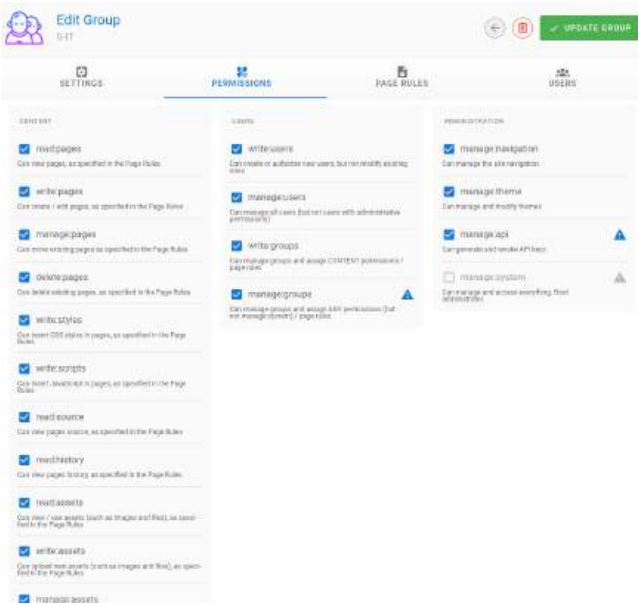
Reglas de permisos por sección:

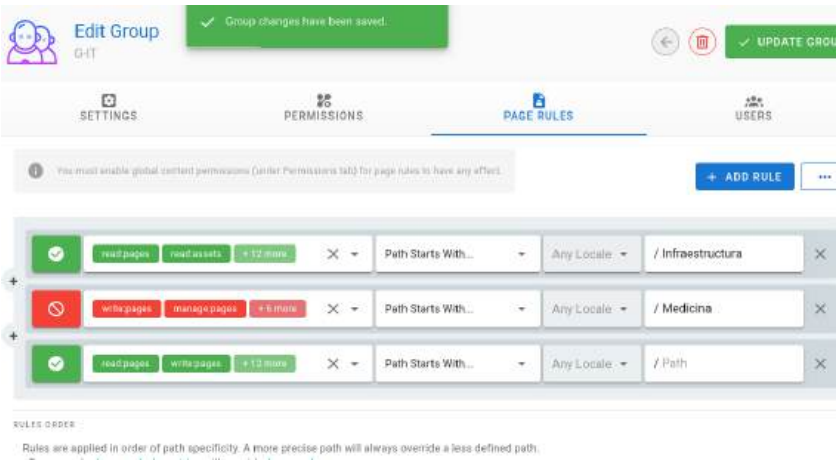
- **Infraestructura**: Solo el **equipo de informática** puede acceder y editar. Los demás grupos no tendrán acceso a esta sección.
- **Medicina**: El grupo de **veterinarios** tiene control completo. El grupo **IT** puede ver las versiones de los documentos y eliminarlos si es necesario, pero solo los veterinarios pueden escribir y comentar.
- **Actualidad**: Todos los usuarios dentro del dominio pueden crear, modificar y comentar contenido. Los usuarios invitados únicamente pueden **visualizar**.
- **Informática**: Todo el dominio tiene acceso para **visualizar documentación informativa**, manuales o protocolos. No se permite editar, y los usuarios invitados **no pueden acceder** a esta sección.

Con estas reglas aplicadas, se asegura que cada sección de la wiki tenga el **nivel de acceso adecuado según las responsabilidades de cada grupo**, protegiendo la información sensible y permitiendo colaboración eficiente.

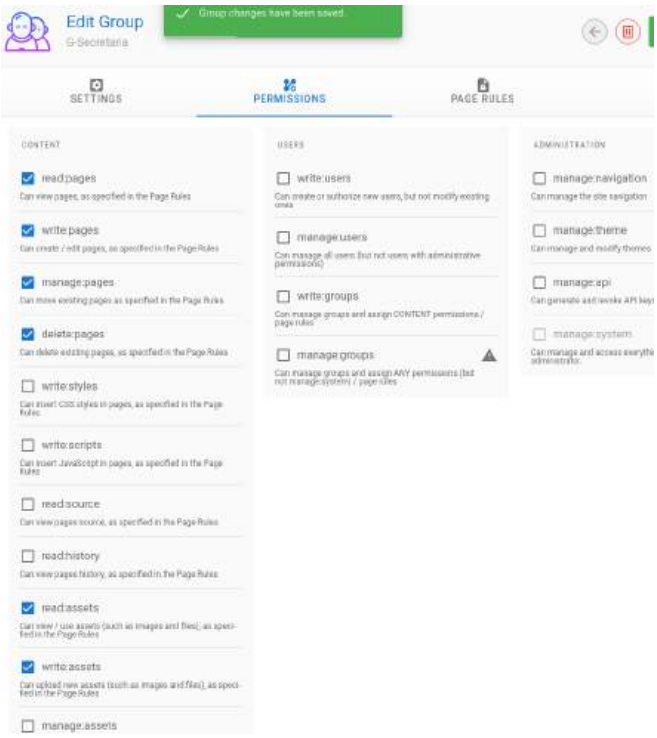
Ahora aplicamos las reglas:

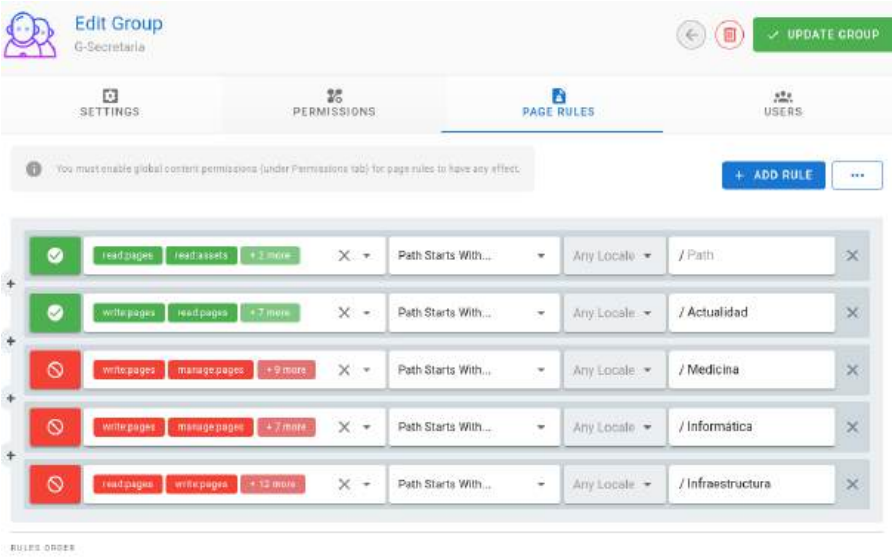
G-IT



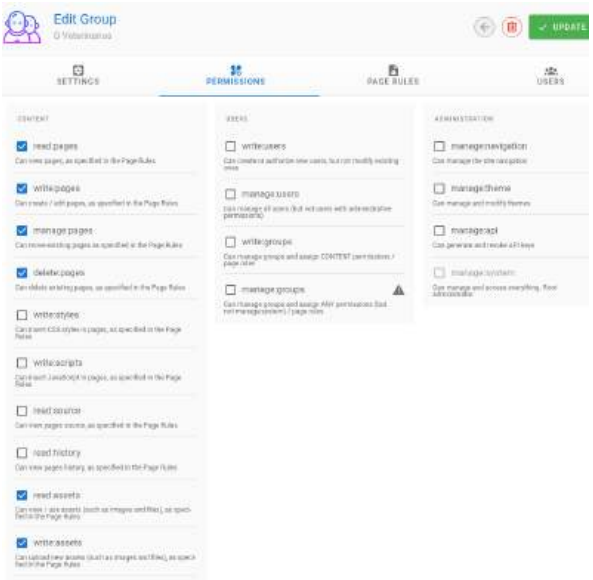


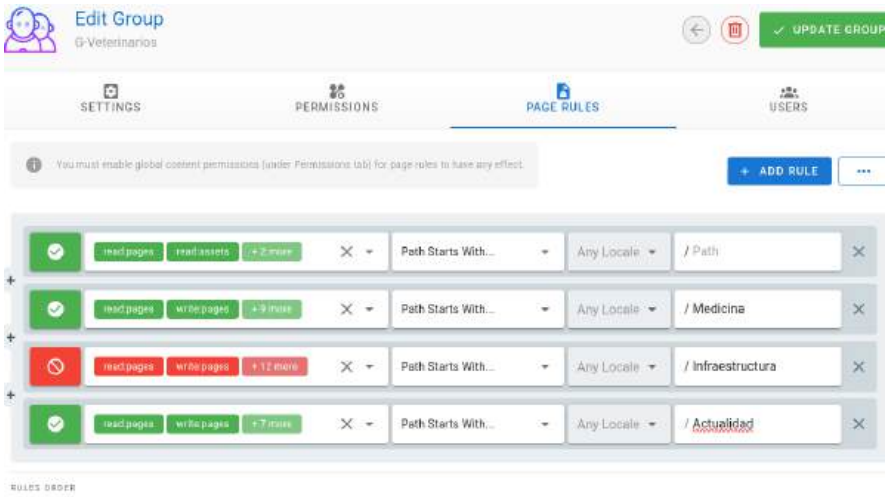
G-Secretaría



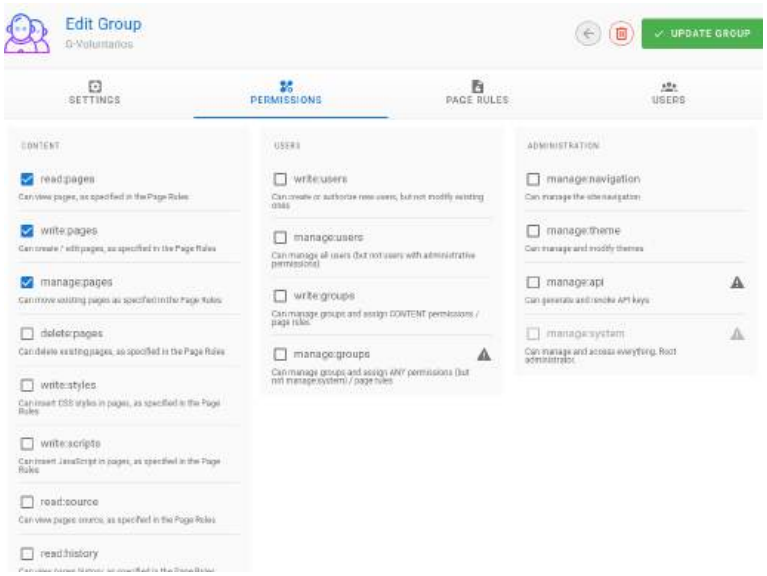


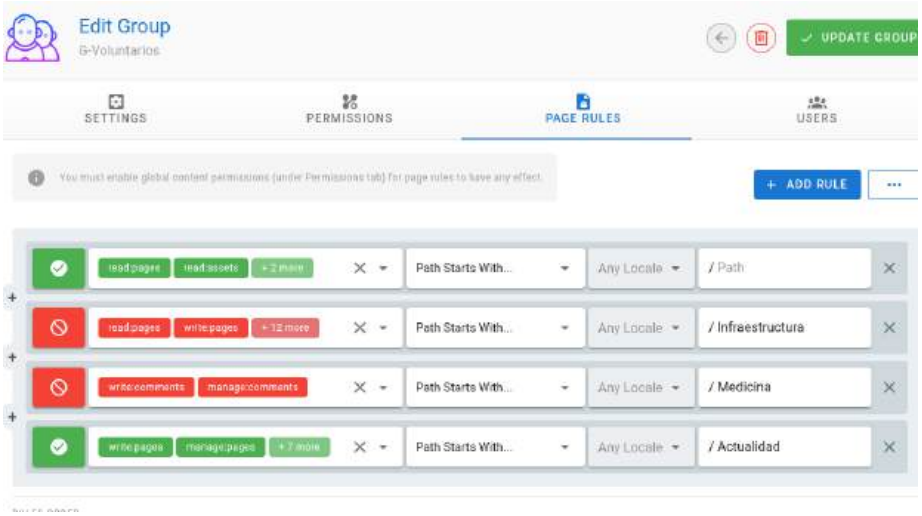
G-Veterinarios



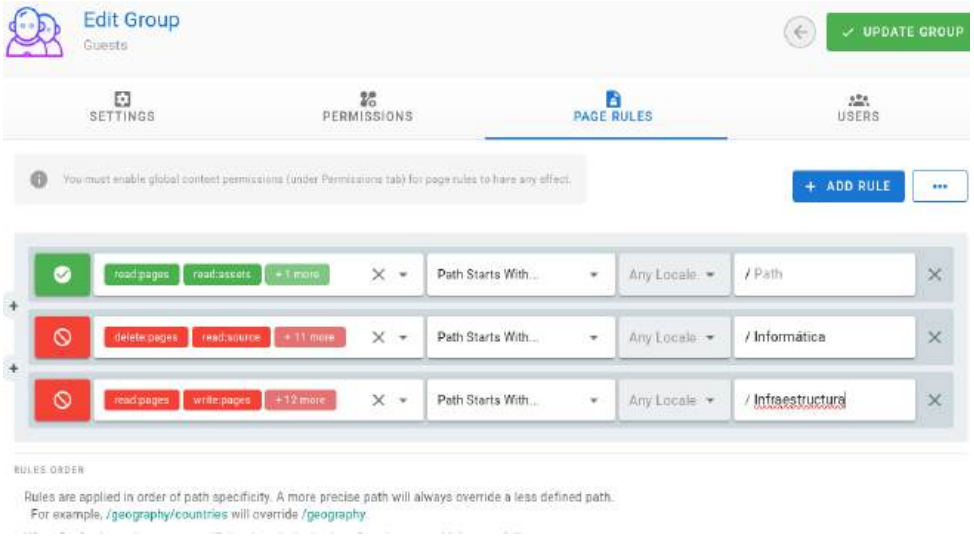


G-Voluntarios




Edit Group
G-Voluntarios
UPDATE GROUP
SETTINGS
PERMISSIONS
PAGE RULES
USERS
ADD RULE
Path Starts With...
Any Locale
/ Path
/ Infraestructura
/ Medicina
/ Actualidad

Invitados


Edit Group
Guests
UPDATE GROUP
SETTINGS
PERMISSIONS
PAGE RULES
USERS
ADD RULE
Path Starts With...
Any Locale
/ Path
/ Informática
/ Infraestructura
RULES ORDER
Rules are applied in order of path specificity. A more precise path will always override a less defined path.
For example, /geography/countries will override /geography

Consideraciones finales

Aunque existen múltiples configuraciones avanzadas disponibles en Wiki.js (permisos más granulados, plantillas, integraciones externas, auditorías, etc.), por el momento la plataforma se dejará configurada con esta estructura básica, que garantiza seguridad, organización y un flujo de trabajo funcional para todos los miembros de IJO's & Monkeys.

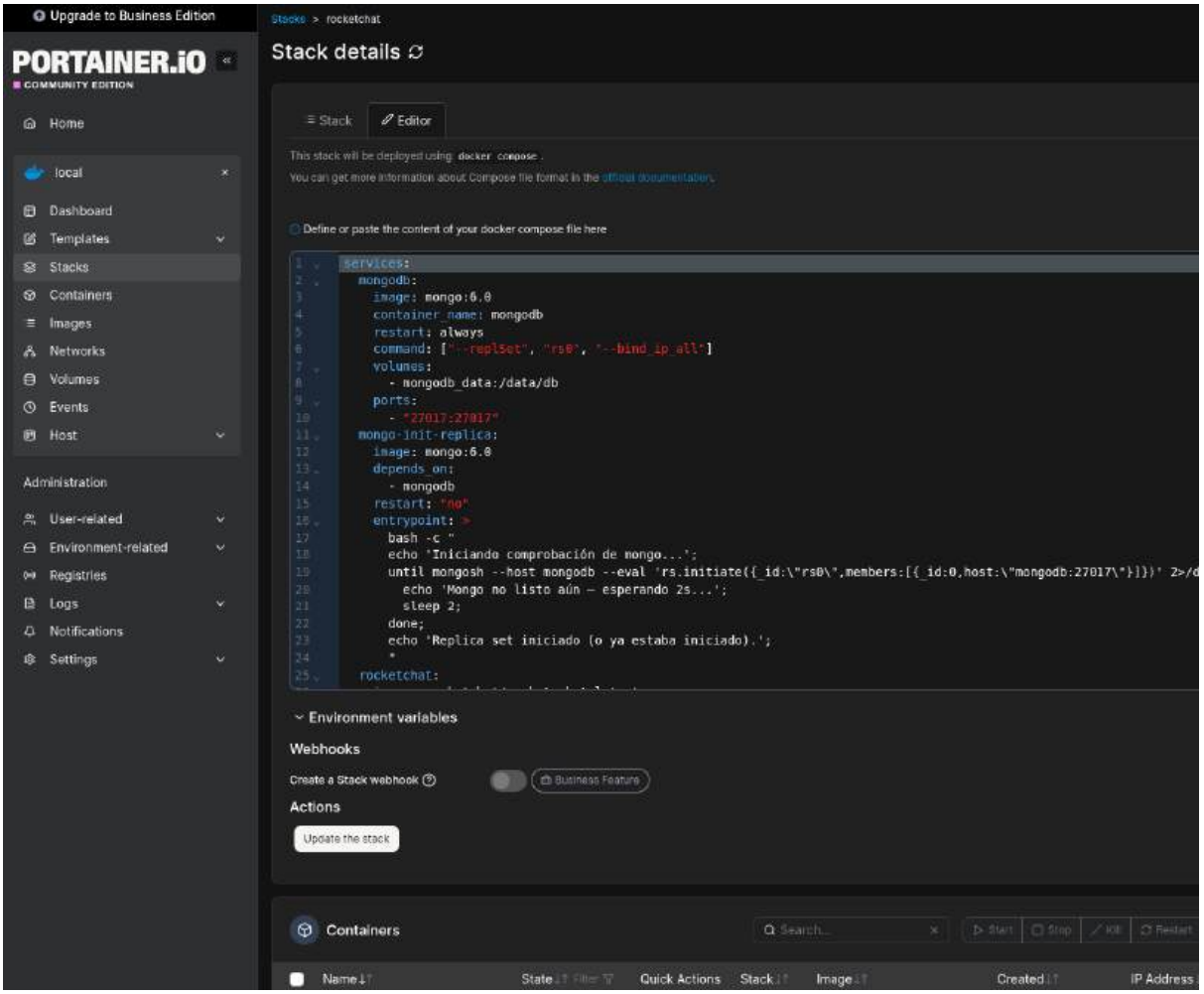
Rocket.chat

Rocket.Chat es el sistema de **mensajería interna** de la ONG.
Permite crear canales por departamento, un canal general, y conversaciones privadas entre usuarios.
Cada miembro del AD tiene su usuario sincronizado automáticamente, con su grupo correspondiente (G-IT, G-Secretaría, etc.), aunque los canales deben crearse manualmente, dado que la versión Community no soporta el mapeo automático de permisos por grupo.

Es la **plaza central digital** de la ONG: el lugar donde se conversa, se comparte, se improvisa y, a veces, se ríe (muy pocas veces) y llora (siempre).

Instalación y puesta en marcha

Para desplegar el servicio de **Rocket.Chat**, comenzaremos levantando el *stack* correspondiente. Este archivo docker-compose.yml contiene todos los servicios necesarios para ejecutar la aplicación, incluyendo el contenedor de Rocket.Chat y su base de datos MongoDB.

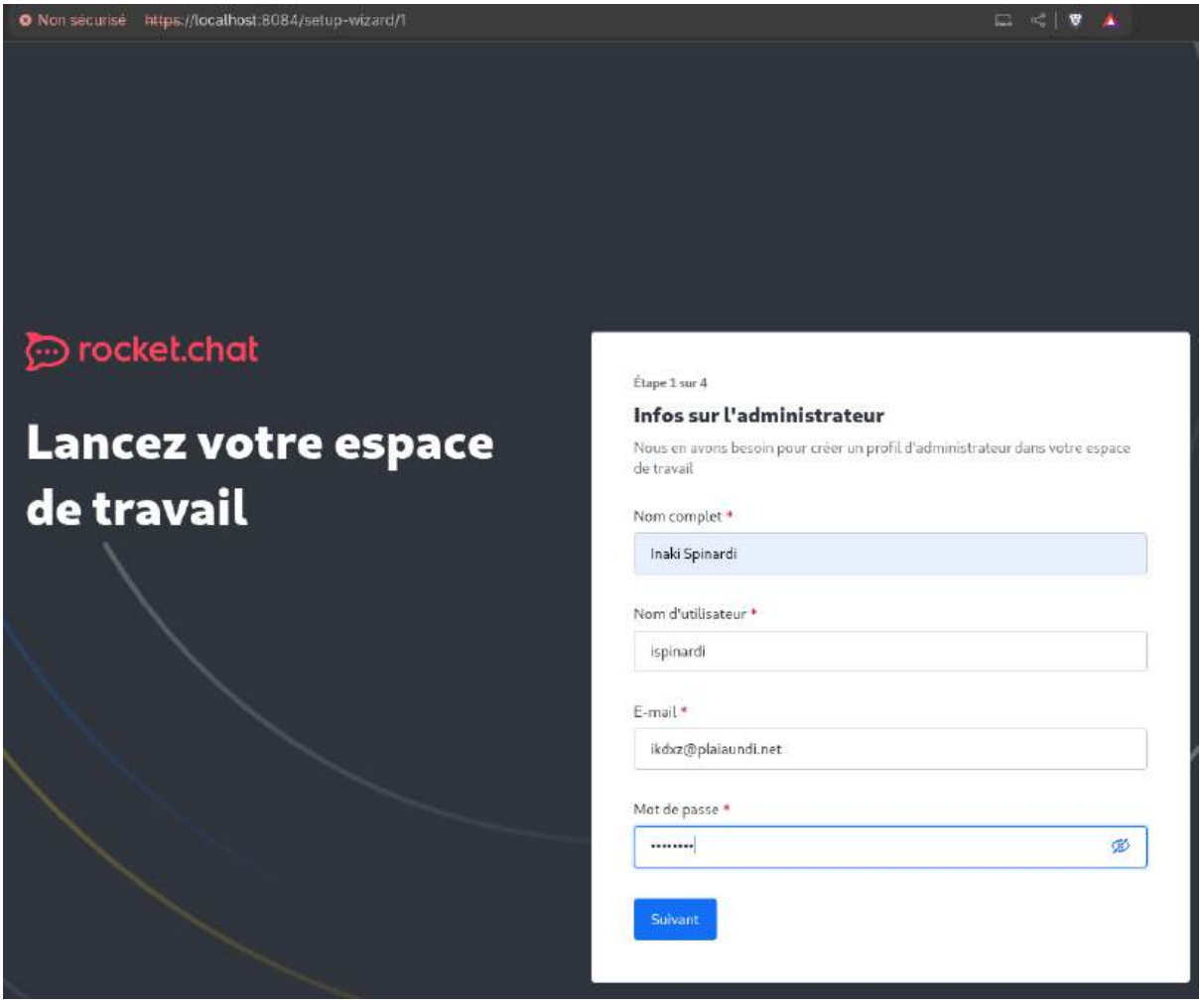


Una vez el *stack* esté en ejecución, podremos acceder al panel web desde:

- **IP local y puerto:** https://<IP_DEL_SERVIDOR>:8084
- **Dominio:** https://rocket.ijo.org:8084

Creación del administrador

La primera vez que accedamos, el sistema solicitará la creación de una **cuenta de administrador**.
Introduce un nombre de usuario, una contraseña segura y un **correo electrónico real**, ya que se enviará un código de verificación a esa dirección.
Este usuario será el encargado de realizar la configuración inicial del entorno.



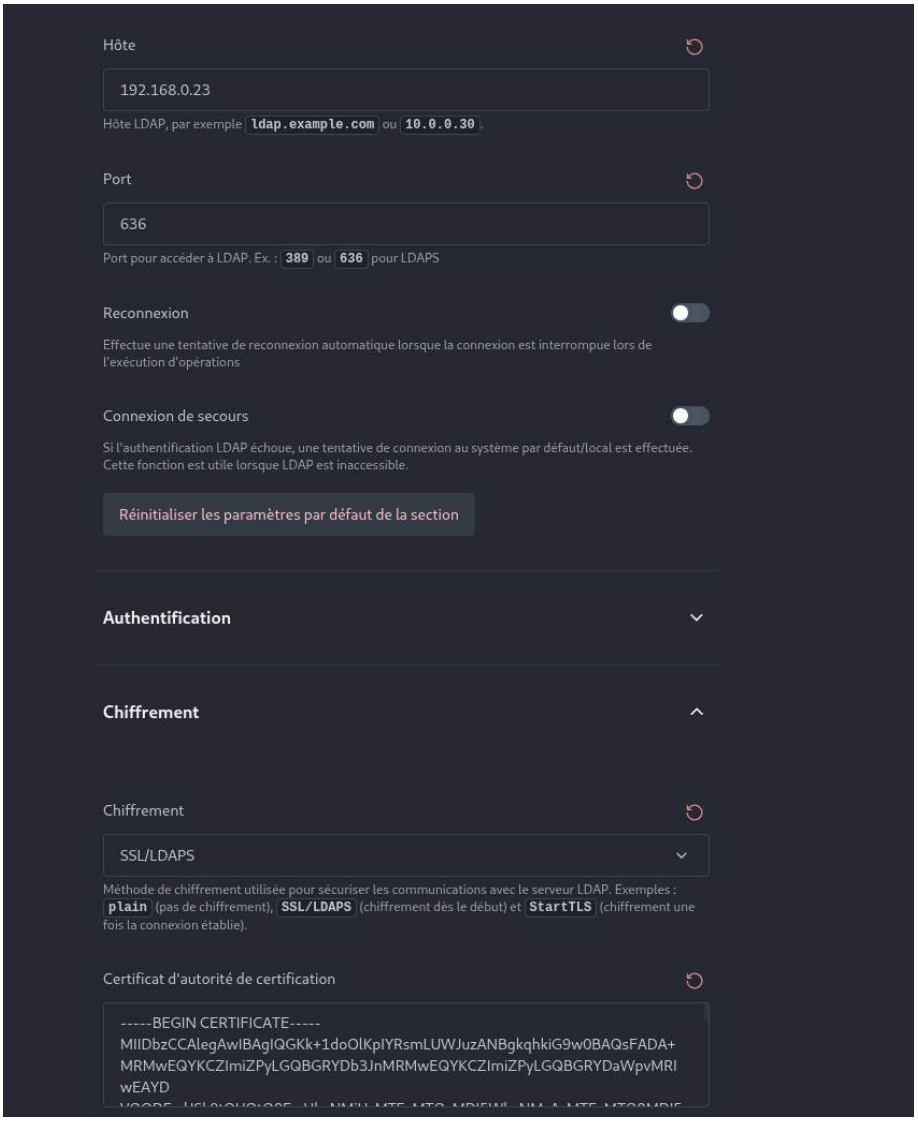
Configuración del servicio LDAP/Active Directory

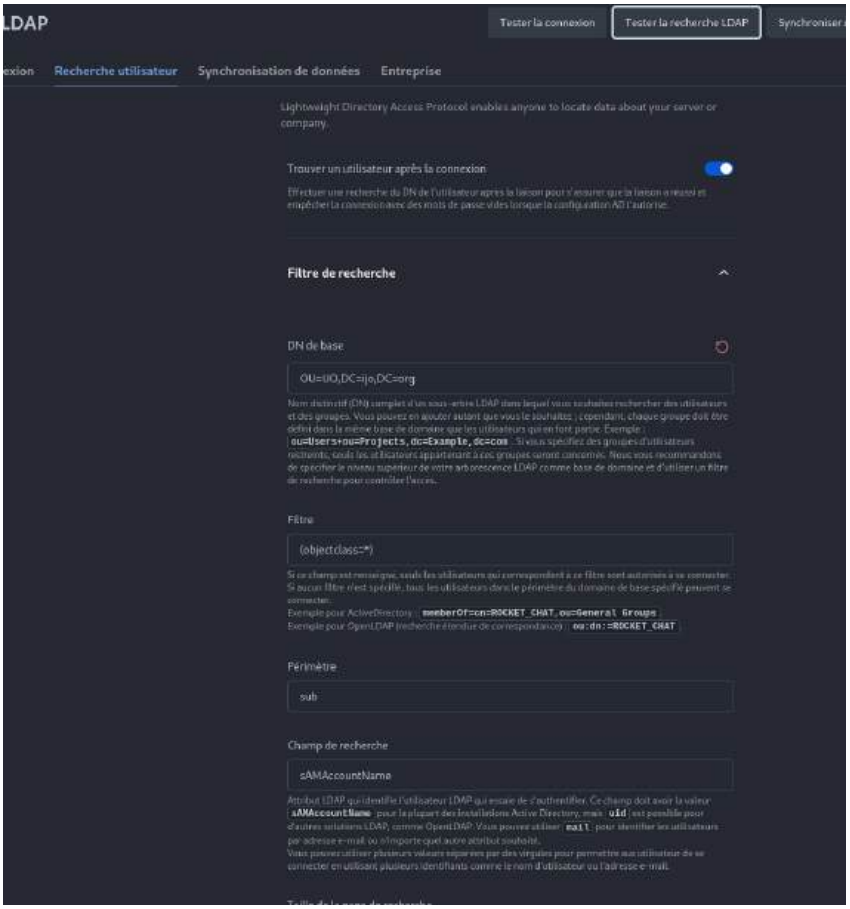
Con la sesión del administrador iniciada, navegamos hasta:

Administración > Workspace > Configuración > LDAP

Allí activaremos el módulo **LDAP**, que permitirá vincular los usuarios del **Active Directory (AD)** con Rocket.Chat.

En este punto, deberemos rellenar los parámetros de conexión, incluyendo:


Hôte
192.168.0.23
Hôte LDAP, par exemple ldap.example.com ou 10.0.0.30.
Port
636
Port pour accéder à LDAP. Ex. : 389 ou 636 pour LDAPS
Reconnexion
Effectue une tentative de reconnexion automatique lorsque la connexion est interrompue lors de l'exécution d'opérations
Connexion de secours
Si l'authentification LDAP échoue, une tentative de connexion au système par défaut/local est effectuée. Cette fonction est utile lorsque LDAP est inaccessible.
Réinitialiser les paramètres par défaut de la section
Authentification
Chiffrement
Chiffrement
SSL/LDAPS
Méthode de chiffrement utilisée pour sécuriser les communications avec le serveur LDAP. Exemples : plain (pas de chiffrement), SSL/LDAPS (chiffrement dès le début) et StartTLS (chiffrement une fois la connexion établie).
Certificat d'autorité de certification
-----BEGIN CERTIFICATE-----
MIIDbzCCAlegAwIBAgIQGKk+1doOlKpIYRsmLUWJuzANBgkqhkiG9w0BAQsFADA+
MRMwEQYKCZImiZPyLGQBGRYDb3JnMRMwEQYKCZImiZPyLGQBGRYDaWpvMRIwEAYD

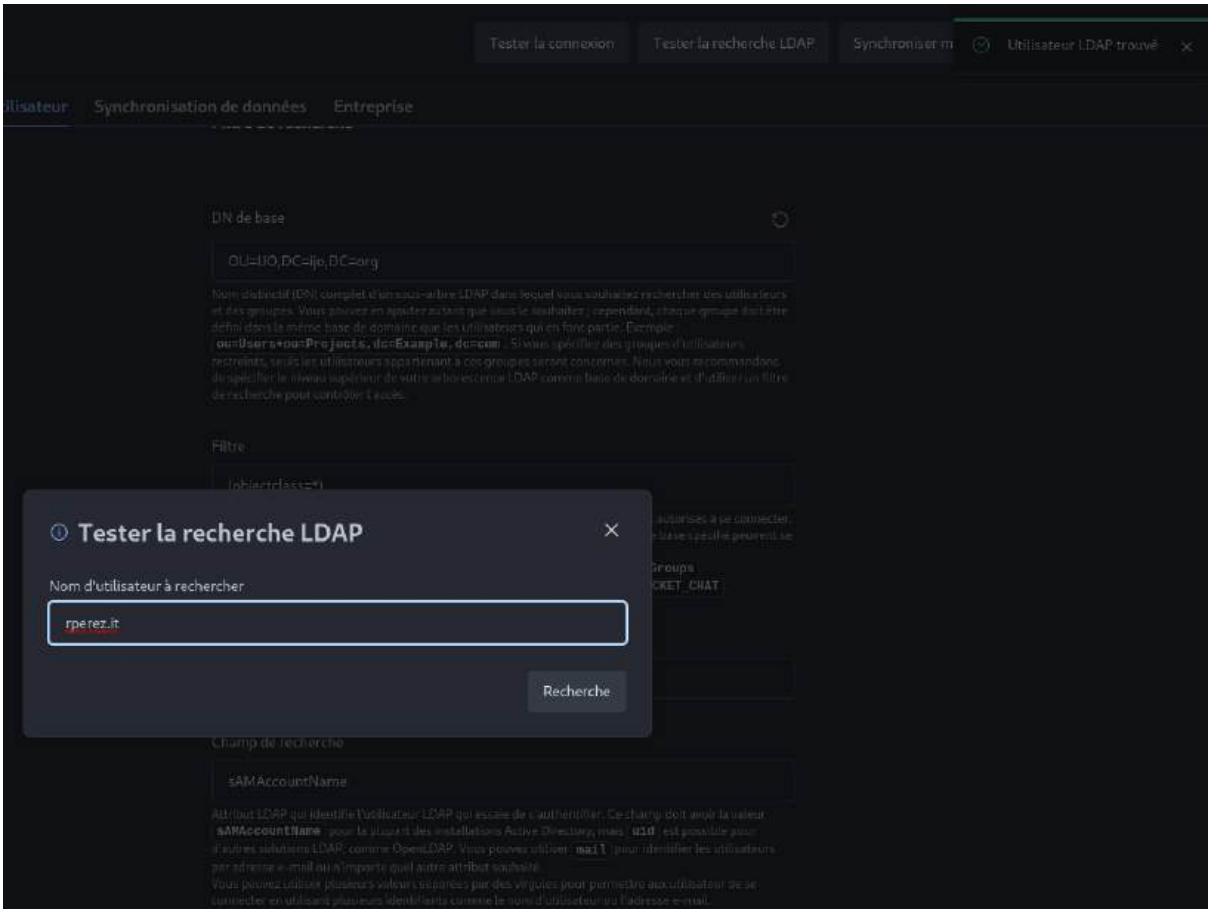


Una peculiaridad importante es que **Rocket.Chat requiere el certificado LDAPS** en formato PEM.

Podremos copiarlo y pegarlo directamente en el campo correspondiente dentro de la configuración LDAP, o bien indicar su ruta si se utiliza un volumen persistente.

Esto es esencial para que la comunicación cifrada con el AD funcione correctamente.

Una vez completada la configuración, seleccionamos "**Probar conexión**" para verificar que Rocket.Chat puede comunicarse con el directorio.



Si todo está correcto, pulsamos "**Sincronizar ahora**" para importar los usuarios del dominio.

Nota: La sincronización de grupos LDAP es una función de pago. Por ello, los canales y grupos deberán configurarse manualmente.

Desactivar autenticación en dos pasos

Antes de permitir el acceso a los usuarios, es necesario desactivar la **autenticación en dos pasos (2FA)**, que viene habilitada por defecto.

Para hacerlo, dirigirse a:

Administración > Configuración > Cuentas > Activar autenticación en dos pasos y **deshabilitarla**.

Con todo listo, probamos a iniciar sesión con un usuario del AD.

Si el acceso es exitoso, el sistema mostrará los canales disponibles y el usuario quedará completamente integrado en la red de comunicación de la ONG.

PortalAD

El **PortalAD** es una pequeña joya desarrollada en **Node.js**, diseñada para aliviar la carga administrativa del equipo técnico.
Solo los usuarios de los grupos **G-IT** y **G-Secretaría** pueden acceder, al resto de usuarios se les deniega el acceso.
Desde un formulario web, se introducen los datos básicos de un nuevo usuario para su creación en el **Active Directory**.

Por seguridad, el portal no utiliza LDAPS y, por tanto, **no puede activar cuentas ni definir contraseñas directamente**; esas acciones se completan

manualmente desde el servidor AD.
Aun así, es una herramienta ligera y elegante que ahorra tiempo y reduce errores en el alta de personal.

Instalación y puesta en marcha

```
docker build -t inaki/portal-ad:latest .
```

Y posteriormente levantamos el Stack.

Servidor Mail

El **servidor de correo** combina **Postfix** y **Dovecot**, ofreciendo a todos los usuarios cuentas bajo el dominio **@ijo.org**.
La autenticación se realiza contra el AD mediante LDAPS, y toda la comunicación está cifrada, **SSL/TLS para envío (SMTP) y STARTTLS para recepción (IMAP/POP3)**.

Esto garantiza privacidad y coherencia: un único usuario, una única identidad.
El sistema maneja la entrega local y el reenvío hacia Internet (solo en local), asegurando que tanto los mensajes internos como externos fluyan con la misma seguridad.

Servidor Web

La **página web pública** de la ONG, alojada en el mismo SRV-CONTAINERS, presenta las labores y proyectos de **IJO's & Monkeys** al mundo.

Planteamiento del proyecto

Lo primero es plantear cómo vamos a diseñar la página web. En nuestro caso al ser una ONG de monos ya tenemos la temática pensada para la página web, pero es importante seguir estos pasos:

.Que sea agradable a la vista
.Que sea explicativa(como funciona y de que se encarga nuestra organización)
.Que sea responsive para mayor accesibilidad desde otros dispositivos

esto por la parte más visual de la página, por otro lado, los apartados técnicos de la pagina deben ser los siguientes:

.Debe ser HTTPS
.Debe tener un apartado administrativo protegido por una contraseña

A parte de esto hemos decidido añadir ciertas características como:

.La página web será levantada en contenedores docker
.Se aplicará una redirección de puertos para que todo el tráfico se dirija a HTTPS
.Se utilizará nginx funcionando con apache para una mejor administración
.La página web tendrá un balanceador para evitar el tráfico excesivo

Todos esto se montara en contenedores sobre un ubuntu server junto al resto de servicios

Instalación y puesta en marcha

Creación del código de la página web

Para crear la página web tendremos que crear un html en el cual este nuestra pagina, ademas del html también tendremos que hacer un css y javascript para hacer más profesional nuestra página, en nuestro caso todo el html,css,javascript van a ir dentro del archivo index.html para evitar problemas para crear la página administrativa se ha seguido el mismo proceso

Nuestra página tiene este código:
Página index
Y este es el código de nuestra pagina administrativa:
Pagina administrativa

Creación de certificados para la página

Para que nuestra página utilice el protocolo HTTPS tenemos que crear una serie de certificados, como en nuestro caso no usaremos una entidad certificadora para firmar los certificados los crearemos autofirmados, Para ello tendremos que instalar openssl con este comando:

```
sudo apt install openssl
```

Una vez instalado openssl crearemos los certificados con este comando:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
```

```
  -keyout ssl/nginx-selfsigned.key \
  -out ssl/nginx-selfsigned.crt \
```

Archivos necesarios para crear nuestro docker compose

Para poder crear los contenedores de nuestra página web tendremos que crear una serie de archivos, estos son: archivo .yaml y archivo de configuración .conf .Sin estos no se podría crear el docker compose además de que en estos configuraremos las características de nuestra página

YAML

Archivo .yaml

En este archivo le diremos a docker compose cuantos contenedores levantar, qué contenido debe tener cada uno, que imagen usar, donde están los certificados para usar HTTPS, que puertos abrir y las características de nginx en este caso.

Para crearlo tenemos que indicar cada contenedor que vamos a crear así:

```
services:
  # Servidor Apache 1 CON PHP
  apache1:
    image: php:8.1-apache
    container_name: apache1
```

```
    volumes:
      -
/home/contenedores/servidores/pagina_web/apache1:/var/www/html
    networks:
      - backend
    restart: unless-stopped
```

En el especificaremos: la imagen que vamos a usar en este caso la de apache con php, el nombre del contenedor, el volumen es decir donde estan los archivos que usará el apache por ejemplo el index.html y donde los montaremos en el contenedor es decir la ruta de montaje.

A la hora de configurar cosas como los puertos, el HTTPS y el balanceador se hace en la parte de creación del contenedor de nginx

```
nginx:
    image: nginx:latest
    container_name: nginx-balancer
    ports:
      - "80:80"
      - "443:443"
    volumes:
      -
/home/contenedores/servidores/pagina_web/nginx/conf.d:/etc/nginx/co
nf.d:ro
```

```
    -
/home/contenedores/servidores/pagina_web/nginx/auth:/etc/nginx/auth:
ro
    - /home/contenedores/servidores/pagina_web/ssl:/etc/nginx/ssl:ro
  depends_on:
    - apache1
    - apache2
    - apache3
  networks:
    - backend
  restart: unless-stopped
```

En el código aparte de especificar la imagen el nombre del contenedor podemos ver los puertos que vamos a usar donde montaremos los certificados en el contenedor además del archivo conf y que depende de los 3 apaches de esta manera podremos hacer de balanceador

CONF

En este archivo es donde configuraremos el contenedor de nginx en el pondremos toda la configuración que queremos como por ejemplo:

```
upstream apache_backend {
    server apache1:80;
    server apache2:80;
    server apache3:80;
}
```

Aquí especificaremos que queremos que ponga los 3 apaches en el puerto 80 para hacer el balanceador

También configuraremos el redireccionamiento a HTTPS

```
# Redirección HTTP a HTTPS
server {
    listen 80;
    server_name _;
    return 301 https://$host$request_uri;
}
```

El uso de certificados

```
 # Certificados SSL
    ssl_certificate /etc/nginx/ssl/nginx-selfsigned.crt;
    ssl_certificate_key /etc/nginx/ssl/nginx-selfsigned.key;
```

Y también la implementación de un área administrativa en la que se necesita poner usuario y contraseña

```
# Configuración con autenticación SOLO para admin.html
    location /admin.html {
        auth_basic "Área de Administración - Acceso Restringido";
        auth_basic_user_file /etc/nginx/auth/.htpasswd;

        proxy_pass http://apache_backend;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_set_header X-Forwarded-Host $host;
```

Para crear el usuario y contraseña lo añadiremos en el archivo /etc/nginx/auth/.htpasswd

Montaje de la página

Una vez tengamos todos los archivo necesarios para crear la página tendremos que colocarlos en el servidor en mi caso todo los archivos de la página se encuentran en
/home/contenedores/servidores/pagina_web
para crear una buena estructura de los archivos y que sea fácilmente comprensible los he montado siguiendo esta estructura

```
/home/contenedores/servidores/pagina_web/
├── apache1/
├── apache2/
├── apache3/
├── nginx/
│   ├── auth/
│   └── conf.d/
├── ssl/
├── docker-compose.yaml
├── Dockerfile-apache.php
└── inicio.sh
```

en ella se separan los archivos de una manera clara para evitar desorden y confusión, una vez montada la estructura de archivos solo queda una cosa

Crear el stack

Nosotros para crear los contenedores hemos utilizado Portainer que es una interfaz gráfica para gestionar contenedores Docker de forma fácil, sin tener que usar todo el rato la línea de comandos

Primero crearemos el Stack que es el nombre que usa para crear un docker compose

Entraremos en el apartado Stack y clicaremos en la opción de Add stack

Una vez ahí nos saldrán varias opciones, la que usaremos en este caso es la de web editor en la que es tan fácil de usar como pegar el contenido de nuestro archivo yaml y darle a deploy the stack
Una vez hecho esto deberían crearse automáticamente todos los contenedores y desplegarse con éxito la página web

Servidor REST

Planteamiento del proyecto

Se nos pide crear un servidor REST para que gestione la información entre la página web y la base de datos, para ello tendremos que hacer una página php que se encargue de hacerlo, en nuestro caso hemos creado una página de mensajes para usar este servidor REST, la función de esa pagina sera gestionar los mensajes para poder guardarlos en nuestra base de datos y viceversa poder mostrar esos mensajes guardados a los clientes de la página, para hacer esto tendremos que crear: la página html, el php y una base de datos

Instalación y puesta en marcha

Página HTML

La página web es la parte que va a ver el ciente por lo tanto tiene que ser tematizada con la temática de nuestra ONG además de ser agradable a la vista y sencilla de usar, el código será principalmente en html y css además de estos también usa javascript para más funcionalidades además de ayudar al php

Página HTML

Base de Datos

La base de datos será una muy sencilla ya que solo almacena mensajes asi que solo consistirá en una tabla la cual tendrá estos campos: un id que será la clave primaria en la que se guardará principalmente el orden en el que se mandaron los mensajes, username para poder saber quién envió el mensaje, message que es donde se almacena el mensaje y timestamp que es para guardar la fecha exacta en la que se mandó el mensaje. En esta base de datos se guardaran todos los mensaje y gracias a su diseño podremos facilitar su uso en el php

Base de datos

PHP

El php es el encargado de gestionar los datos que mostramos y guardamos dentro de la base de datos por lo que es la parte más importante del servidor REST, tiene varias funciones las cuales son:

conectar con la base de datos

```php
<?php
$host = '10.10.16.200';
$port = 3306;
$db   = 'users';
$user = 'manolito';
$pass = 'manolito';

$conn = new mysqli($host, $user, $pass, $db, $port);
```

Este hará que podamos conectarme a la base de datos users con el usuario manolito en el puerto 3306 que es el de mysql

Borrar mensajes

```
// BORRAR MENSAJE si llega id_borrar
if (isset($_GET["id_borrar"])) {
    $id_borrar = intval($_GET["id_borrar"]);
    $conn->query("DELETE FROM mens WHERE id = $id_borrar");
    header("Location: chat.html");
    exit();
}
```

Lo que hace esto es que si llega a recibir el id de un mensaje cuando nosotros usemos el botón de borrar en la página hará un delete del mensaje con el id que nosotros hayamos seleccionado

Almacenar mensajes

```
// INSERTAR si hay mensaje
if (isset($_GET["message"]) && !empty(trim($_GET["message"])) &&
isset($_GET["username"])) {
    $mensaje = $conn->real_escape_string($_GET["message"]);
    $usuario = $conn->real_escape_string($_GET["username"]);

    $insrt = "INSERT INTO mens (username, message) VALUES ('$usuario',
'$mensaje')";
    $conn->query($insrt);
```

```
    // REDIRIGIR A chat.html después de insertar
    header("Location: chat.html");
    exit();
}
```

Lo que hace este código es hacer guardar el el nombre de usuario y mensaje para despues hacer un insert del mensaje enviado además del nombre de usuario siempre y cuando el mensaje no esté vacío

Mostrar mensajes

```
// SIEMPRE devolver JSON CON ID
$sql = "SELECT id, username, message, timestamp FROM mens ORDER BY timestamp ASC";
$result = $conn->query($sql);

$messages = [];
while($row = $result->fetch_assoc()) {
    $messages[] = $row;
}
header('Content-Type: application/json');
echo json_encode($messages);
```

lo que hace este código es primero hacer una consulta de todos los mensajes en orden de envío para después guardar los datos consultados en un array en formato json y después mandarlos al código html y que el javascript se encargue de mostrarlos de una manera bonita

Instalación en servidor

Para que todo esto funcione es muy importante instalar mysql en los contenedores de apache para que puedan hacer conexión a la base de datos, además de esto en la base de datos tendremos que permitir las conexiones externas, una vez hecho todo esto tendremos que meter el php y html en la carpeta de apache

NAS

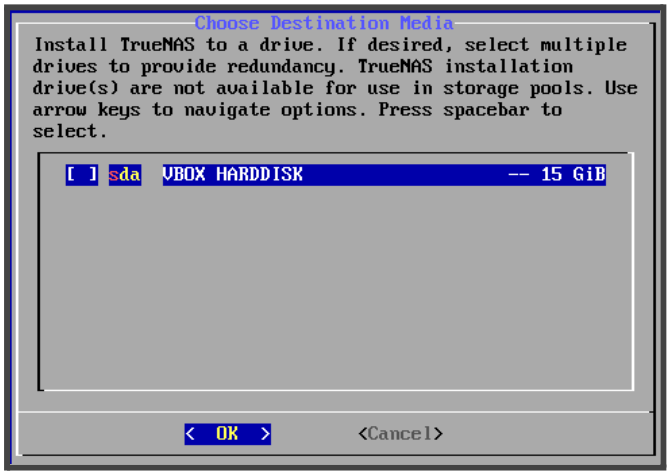
Planteamiento del proyecto

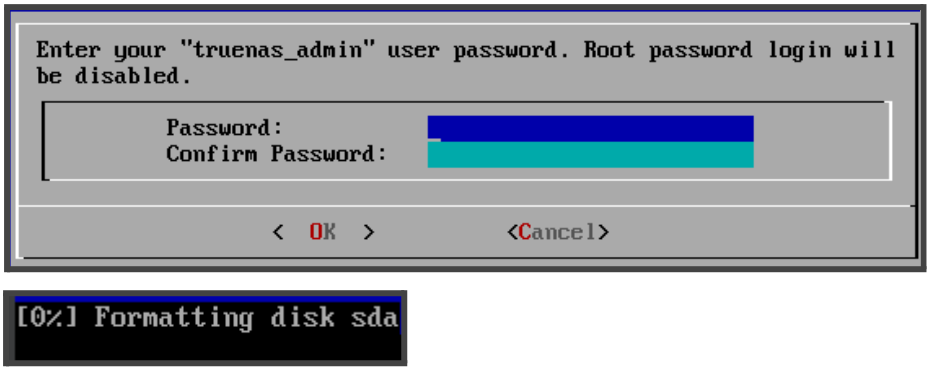
Tenemos que crear un NAS (Network Attached Storage) es un sistema de almacenamiento conectado a la red que permite a varios usuarios y dispositivos guardar, acceder y compartir archivos de forma centralizada para ello necesitaremos una iso para crear el NAS hay varias opciones pero la que hemos usado es Truenas 25.10.0 que es de las más fáciles de usar además de tener muchas funcionalidades

Instalación en servidor

Instalación

Para instalarlo tendremos que crear una máquina virtual en la que le meteremos las iso de truenas para instalarlo, es una instalación sin interfaz gráfica pero es muy sencillo de instalar solo rellenamos los campos que necesitamos con el nombre de usuario la contraseña

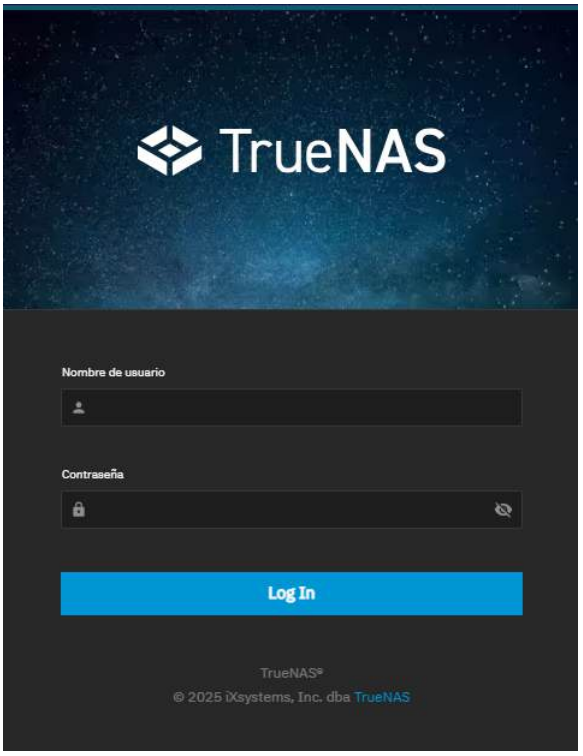




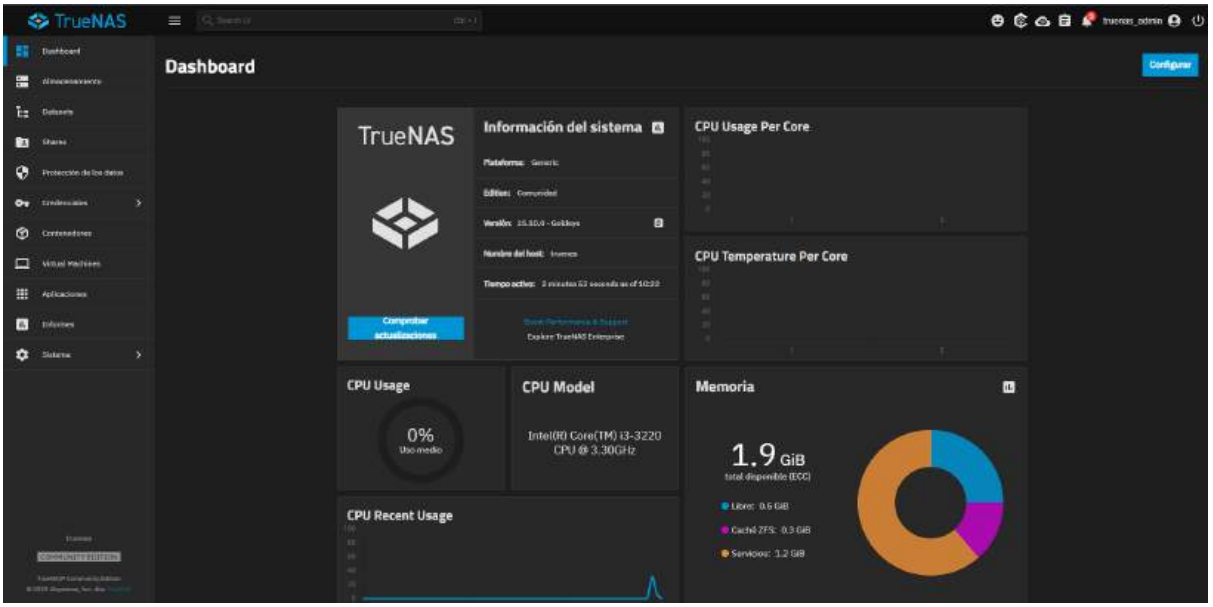
Y con estas simples configuraciones y estaría instalado

Configuración Web

Una vez instalado el nas se abrirá una interfaz web en la que podemos configurarlo como queramos



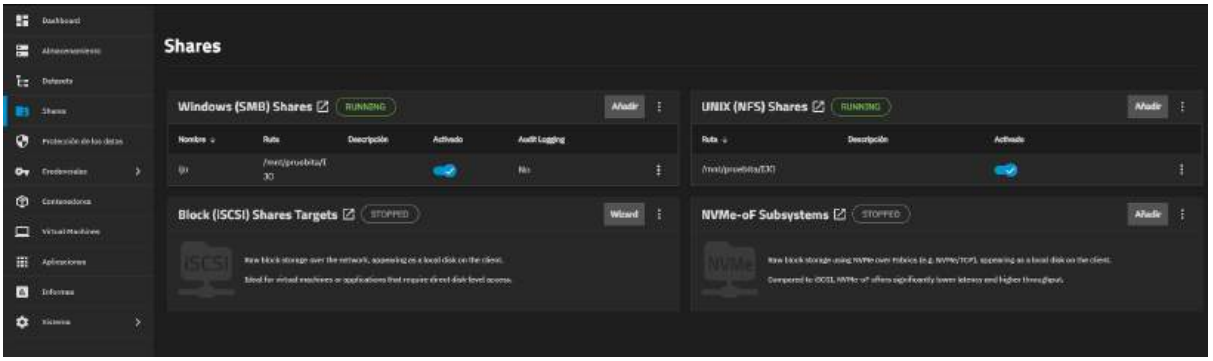
El usuario es truenas_admin y la contraseña es la que configuremos en el terminal del NAS



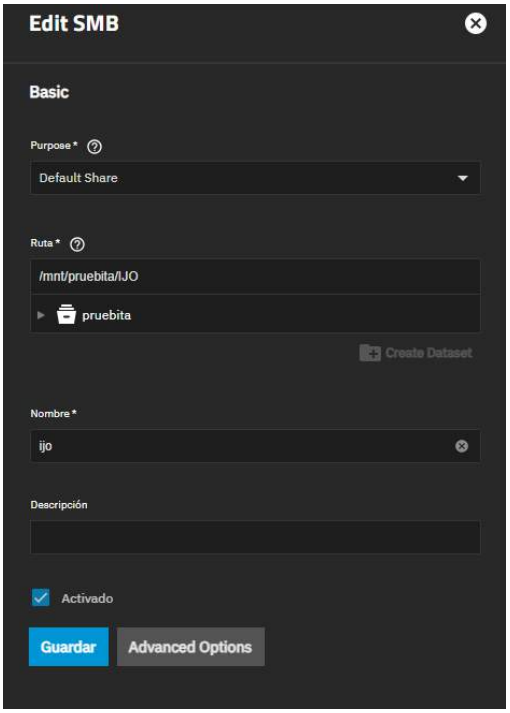
Una vez dentro tendremos antes de todo que añadir como mínimo un nuevo disco a nuestro nas desde la interfaz de proxmox este debe ser de un tamaño considerable ya que es donde se guardaran los archivos, después de añadirlo es importante que cambiemos los id de los discos con este comando en el terminal de proxmox

qm set (ID de la maquina) -scsi(numero del disco) local-lvm:vm-(ID de la maquina)-disk-(numero del disco),serial=SDD123456

Este comando sirve para que proxmox cambie los IDs de los disco ya que por defecto pone los mismo a todos. Una vez hecho esto empezamos a crear un volumen para ello accedemos a su apartado en la interfaz web y seleccionamos el nuevo disco con la opción stripe ya que solo tenemos un disco lo ideal sería usar la opción de RAID ya que es la más segura para no perder los datos una vez hecho esto creamos el volumen



Después de crear el volumen iremos a la pestaña de shares y seleccionaremos el volumen creado viendo esta pantalla que sera para seleccionar la manera en la que queremos compartir los archivos del NAS, en mi caso he utilizado smb por su facil configuracion



Es tan fácil de configurar como poner la carpeta que queremos compartir y y el nombre del smb y listo

Acceso desde cliente

Ahora para poder acceder desde un cliente tendremos que poner estos comandos para habilitar el SMB y conectarme a nuestra carpeta del NAS

```
Enable-WindowsOptionalFeature -FeatureName NFS-Administration -Online -All
Enable-WindowsOptionalFeature -FeatureName ClientForNFS-Infrastructure -Online -All
New-PSDrive -Name "Z" -PSProvider FileSystem -Root "\\10.10.16.89\mnt\pruebita\IJO" -Persist
```

Y para los permisos es tan fácil como poner este comando en el shell del NAS

```
sudo chmod 777 (Carpeta que queremos compartir)
```

Intranet

En el servidor **SRV-AD**, existe una **carpeta compartida** que alberga una **página de inicio interna** para todos los usuarios del dominio.
Esa página actúa como **portal de acceso** a los servicios esenciales: GLPI, Wiki, Nextcloud, Rocket.Chat, etc.
Además, la experiencia se adapta según el rol del usuario:

- Los miembros de **IT** y **Secretaría** ven un panel con herramientas administrativas.

- El resto de los departamentos accede a un panel simplificado, con accesos directos a los servicios cotidianos.

Una **GPO** configura **Microsoft Edge** para abrir automáticamente la intranet en cada inicio de sesión y en las nuevas pestañas, creando un entorno uniforme, coherente y accesible para todos.

5. Clientes y usuarios / Gestión de perfiles

Para garantizar que cada miembro de la ONG disponga de un entorno adaptado a sus necesidades, se implementan **políticas de grupo (GPOs)** sobre los equipos del dominio. Estas políticas controlan:

- Fondo de pantalla según departamento (IT, Secretaría, Veterinarios, Voluntarios).
- Horarios de uso del equipo según turno (mañana o tarde).
- Instalación automática de aplicaciones esenciales: **GLPI Agent, Nextcloud Files y Rocket.chat**.
- Accesos a recursos compartidos y scripts internos.

Crear la carpeta compartida

En el servidor AD, se crea una carpeta compartida que servirá de base para todas las políticas y archivos de configuración. Aquí se almacenan:

- Scripts de instalación de aplicaciones.
- Imágenes de fondo de pantalla.
- Archivos de configuración de turno y permisos.

Distribuir los archivos

Dentro de la carpeta compartida se organizan los archivos por tipo de política:

- **Fondos de pantalla:** por departamento.
- **Scripts de instalación:** automatizan la instalación de aplicaciones críticas.
- **Configuración de horarios:** define restricciones de inicio/cierre según el turno asignado.

Aplicar políticas

Desde la **consola de AD**, se crean las GPOs correspondientes y se vinculan a las **OU** de usuarios y equipos:

- **GPO Fondos de pantalla:** asigna imágenes según OU=IT, OU=Secretaria, OU=Voluntarios, OU=Veterinarios.
- **GPO Restricción horaria:** limita horarios según turno.
- **GPO Instalación aplicaciones:** instala automáticamente Nextcloud, GLPI y Rocket.chat en los equipos correspondientes.

6. Conclusiones

Este ecosistema no es solo una infraestructura tecnológica; es el resultado de semanas interminables y noches sin dormir, de decisiones críticas tomadas entre café y cansancio, de pruebas que a veces fallaban y que exigían volver a empezar desde cero. Cada servidor, cada contenedor, cada política de Active Directory y cada GPO aplicada representa horas de dedicación

absoluta, de atención a los mínimos detalles y de una pasión que roza la obsesión.

Tras todo esto, no solo hay líneas de código o configuraciones: hay dolor, esfuerzo y compromiso, una montaña de trabajo silenciosa que garantiza que cada usuario tenga su equipo perfectamente adaptado, cada servicio funcione seguro y cada documento esté donde debe, accesible y ordenado.

Este proyecto refleja el precio de la excelencia: la tecnología puesta al servicio de la ONG, diseñada para que nadie note el trabajo que hay detrás, pero cada fallo que evitamos, cada proceso automatizado, cada acceso seguro habilitado, es la evidencia de noches interminables y de una voluntad férrea. IJO's & Monkeys no solo cuenta con un sistema eficiente; cuenta con un ecosistema construido con sangre, sudor y pasión, un esfuerzo que nadie ve pero que sostiene todo lo que nuestra ONG representa.