UNIVERSIDAD DE COSTA RICA
FACULTAD DE INGENIERÍA
ESCUELA DE CIENCIAS DE LA COMPUTACIÓN E INFORMÁTICA

CI-0163 Diseño y Operación de Servicios de infraestructura de TI

Prof. Jose Antonio Brenes

Etapa 4

Elaborado por:

Hellen Fernández Jiménez B42525
Yerlin Ledezma Madrigal B74096

Jueves 21 de julio del 2022

Etapa 4

Descripción

En esta etapa del proyecto la idea es establecer servicios de DHCP, DNS, FreeIPA y monitoreo de servicios, para dos sitios distintos y conectar ambos sitios mediante una conexión segura a través de IPSec. En una etapa anterior se habían simulado ambos sitios dentro de un mismo ESXi. No obstante, en esta ocasión la configuración de la conexión cambió con la intención de que se encuentre entre “dos sitios distintos” que para efectos del curso sería dos ESXi distintos. Además, se implementarán servicios de DNS los cuales puedan ser accedidos tanto por los usuarios de un sitio como los del sitio remoto. Se implementó un servicio de direccionamiento IP automático mediante DHCP para los usuarios de las LAN. Se gestiona y organiza la información de los usuarios de la organización mediante el servicios de FreeIPA. Se ofrecen servicios de aprendizaje en línea (moodle), almacenamiento en línea (nextcloud) y soporte en línea (osTicket). Además se monitorean el servicio de DNS, FreeIPA, los servicios en línea y la base de datos utilizando php server monitor. Todo lo anterior se realizó tomando en cuenta previsiones de seguridad que permitieran controlar los distintos tipos de tráfico entre ambos sitios y fue implementado mediante Iptables.

Arquitectura

1. Partes interesadas y preocupaciones

En esta sección se describen las personas que presentan interés en el sistema desarrollado, y las preocupaciones que presentan según sus intereses

1.1 Partes interesadas

- ☐ Propietarios: Dueños de la organización,
- ☐ Implementadores: Personas encargadas de implementar los centros de datos, es el personal de TI encargado de realizar la implementación y el despliegue de los diferentes servicios, así como de resolver los problemas técnicos de los usuarios.
- ☐ Personal de la organización: Personal distinto a los implementadores del centro de datos, por ejemplo, personal administrativo, secretarias, directores, supervisores.
- ☐ Usuarios: Usuarios finales a los que la organización les ofrece los servicios, dentro de los cuales se encuentran estudiantes y profesores.

1.2 Preocupaciones

- ☐ Acceso a las máquinas por medio de credenciales en cualquiera de las sedes de forma inmediata porque algunos empleados se tienen que desplazar de un sitio a otro a realizar labores y tener que estar creando usuarios y credenciales cada vez que lleguen puede ser ineficiente y tedioso.
- ☐ Intercambio de información entre las sedes de forma segura porque se tiene información privada que no debe de ser accedida ni visualizada por entes externos.
- ☐ Acceso al sistema desde cualquier sitio, es decir, lo que se hizo en el sitio dos debería de poder ser accedido desde el sitio uno.
- ☐ Poder matricular estudiantes en un curso y también que ellos se puedan matricular solos mediante el uso de una contraseña creada para el curso.

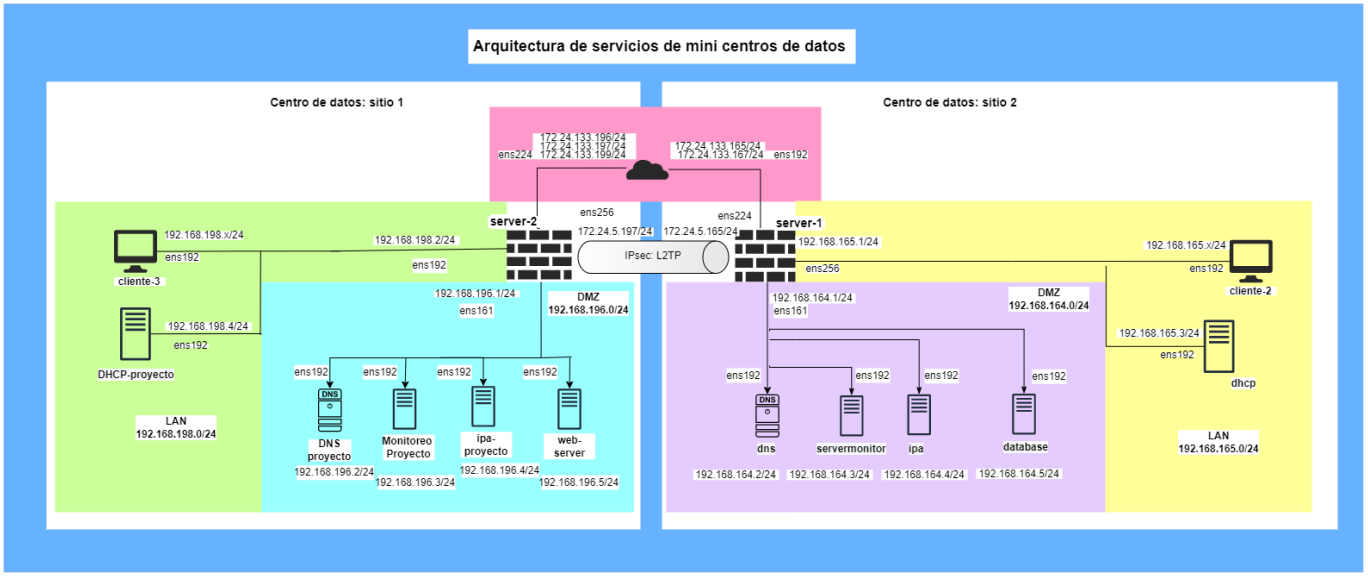
- [ ] Tener acceso a soporte cuando tenga algún incidente tecnológico o de acceso.
- [ ] Llevar control de los incidentes reportados, de los incidentes resueltos y de las categorías.
- [ ] Tener un servicio de almacenamiento en línea sin depender de terceros por cuestiones de seguridad.

2. Viewpoints

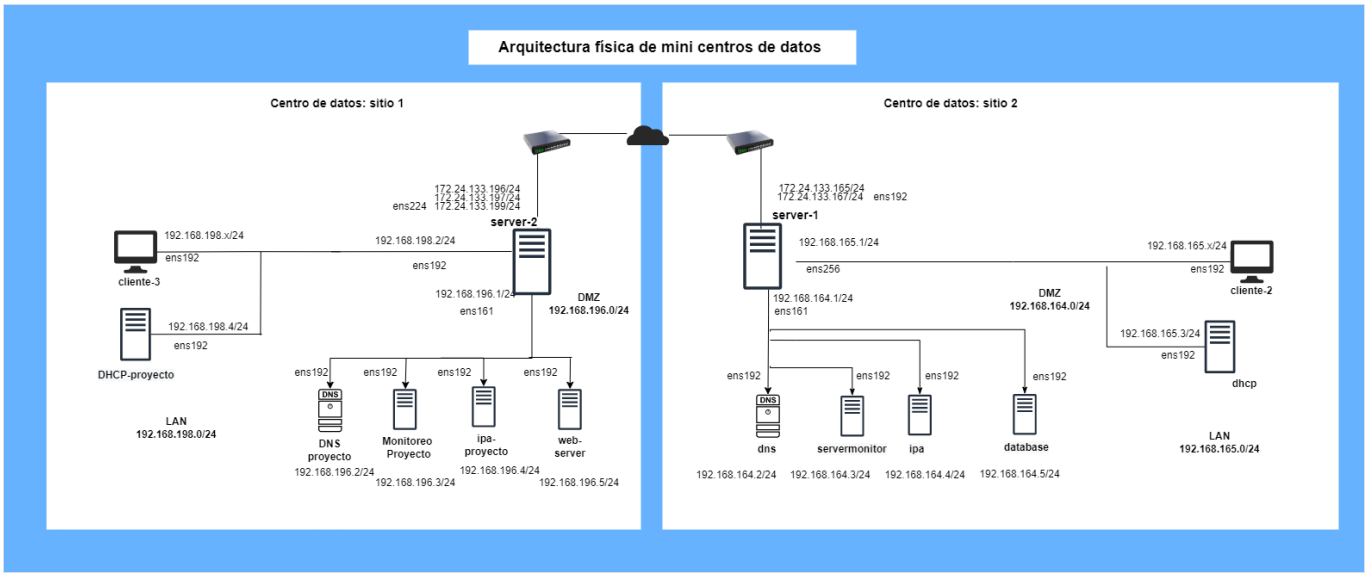
En esta sección se presenta el diagrama completo de los sitios de la organización y sus respectivos componentes. También se describe la arquitectura física, lógicas, de seguridad y de comunicación del sistema.

2.2 Arquitectura de servicios

En este caso, la arquitectura está compuesta por dos centros de datos que poseen la misma arquitectura. En la imagen 1 se aprecian los componentes de cada sitio.

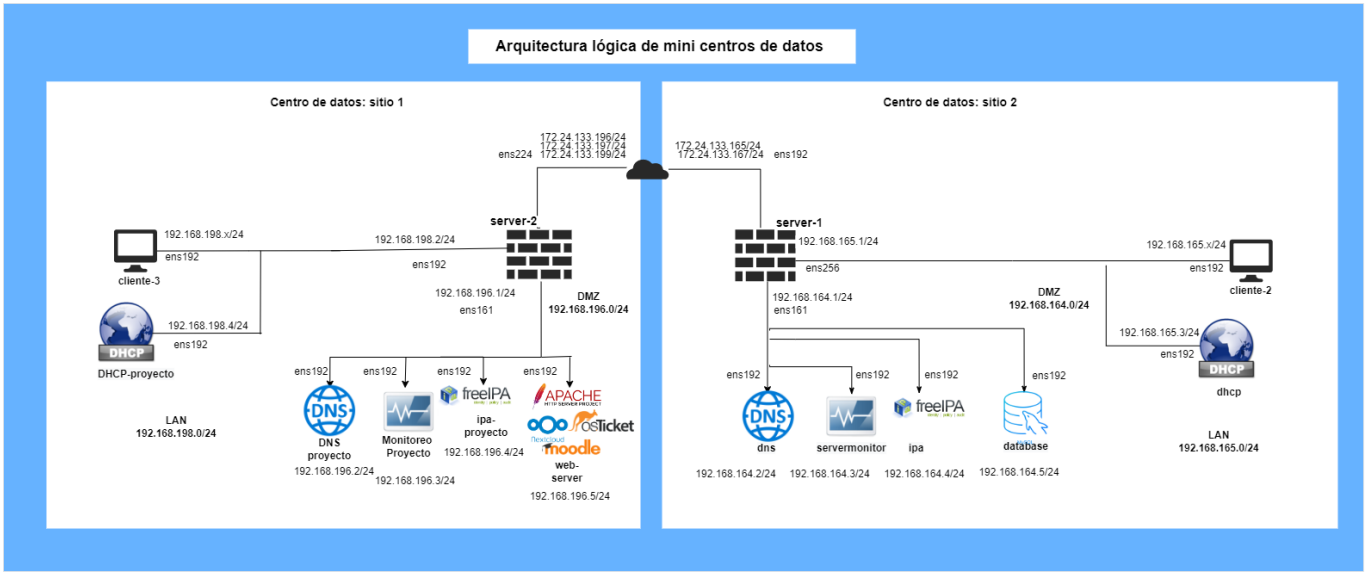


2.3 Arquitectura física



La organización se compone de dos sitios y cada sede tiene un cliente, y 6 servidores, se conectan a través de la red pública NAC. En la tabla 1 se especifican las características de los componentes (ambos sitios poseen las mismas características). Cada servidor y cliente utiliza Centos7 (minimal), tienen 16 GB de disco duro y 2048MB de memoria. Los servidores server-1 y server-2 tienen 4 tarjetas de red cada uno. Los clientes y el resto de servidores tienen una tarjeta de red.

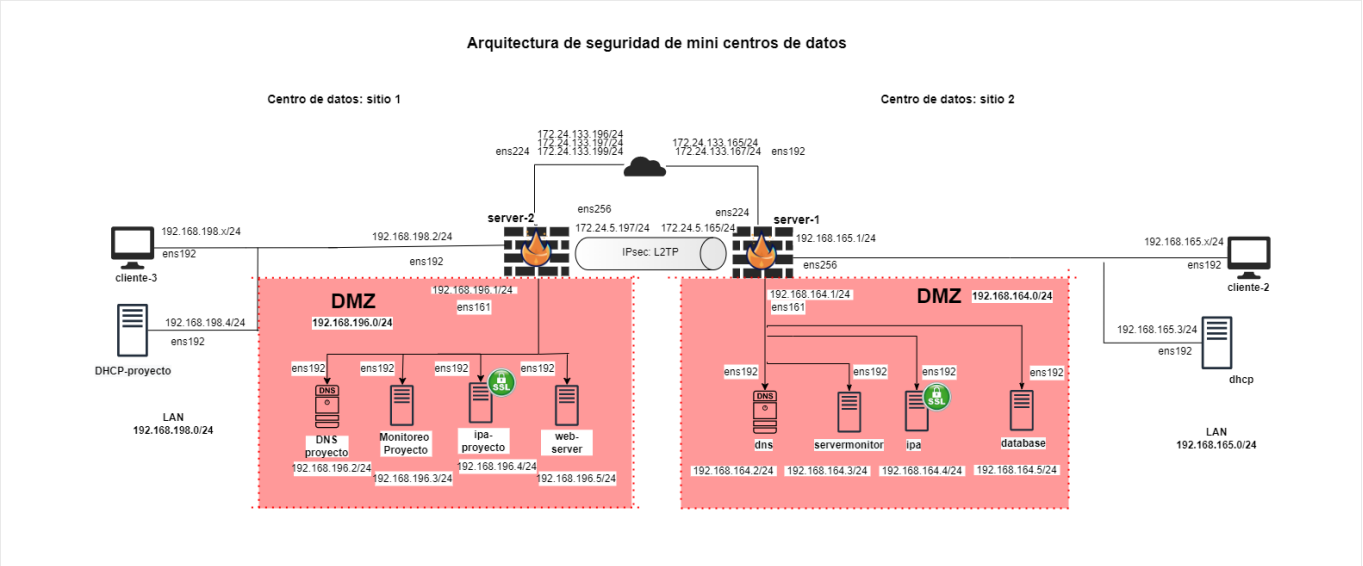
2.4 Arquitectura lógica



En cada sitio se está ejecutando un firewall, para controlar la comunicación entre, desde y hacia los distintos componentes del sistema. Un servicio de DNS para alojar el nombre de dominio externo e interno de la organización. También se ofrece el servicios de DHCP, el cual va asignando de forma dinámica direcciones ip a los clientes que se encuentran en la LAN de la organización y además, brinda el direccionamiento automático del DNS que se encuentra en la DMZ. Se ejecuta el servicio de FreeIPA, el cual es un servicio de directorio que permite almacenar y organizar la información de los usuarios de la organización. Se utiliza el servicio de hospedaje web apache, en el cual se configuran “Virtual hosts” para almacenar los sitios web del servicio de aprendizaje en línea moodle, el servicio de almacenamiento en línea nextcloud y el servicio de soporte en línea osTicket. También se está ejecutando el servicio de mysql para almacenar la información de los sitios web mencionados.Además se ha agregado un servicio de monitoreo, para vigilar el estado de los servidores de DNS, FreeIPA, Nextcloud,moodle, osTicket y mysql.

Servicio	**Sitio**
moodle	aula.quierograduarme.com
nextcloud	nube.quierograduarme.com
osTicket	soporte.quierograduarme.com

2.5 Arquitectura de seguridad



En esta sección se describen los objetivos de seguridad a cumplir y los riesgos que se buscan minimizar.. Para cumplir esos objetivos se decidió utilizar el protocolo IPSec en modo túnel, con el protocolo de encabezado ESP, lo que permite que la comunicación entre los sitios sea cifrada. Además se ha instalado una CA autofirmada en los servidores que ejecutan los servicios de directorio, con el objetivo de que la comunicación entre el servidor réplica y el servidor primario sea segura. También se implementó una zona desmilitarizada (DMZ) en la que se encuentran todos los servicios de la organización que pueden ser accedidos desde internet. El acceso de la DMZ a la red local (LAN) no está permitido, por lo tanto, en caso de que algún servicio sufra un ataque va a ser más difícil que accedan a la LAN.

2.5.1 Objetivos de seguridad y análisis de riesgos

Objetivo 1: Procurar la confidencialidad de los datos que se transmiten entre los dos minicentros de datos de la organización.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Datos	Los datos que viajan de un centro de datos a otro no están encriptados.	Intercepción de datos no encriptados.	Que los datos sean interceptados y vistos por personas no autorizadas.

Objetivo 2: Procurar la integridad de los datos que se comunican entre los dos minicentros de datos de la organización.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Datos	Los datos que viajan de un centro de datos a otro no están encriptados. No hay autenticación de ningún tipo que permita determinar que	Intercepción de datos no encriptados. Acceso a los datos por entes no autorizados.	Que personas no autorizadas puedan acceder a la red de la organización sin estar debidamente autenticado. Que personas no

	los datos están viendo por quien		autorizadas puedan interceptar los datos y conocerlos.

Objetivo 3: Requerir autenticación de identidad para el ingreso a los equipos de forma remota.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Servidores	No hay restricción de cuáles usuarios pueden acceder de forma remota a los servidores.	-Permitir el acceso a los servidores de forma remota sin solicitar autenticación. -Permitir el acceso remoto al usuario root. (Ya que es común que los hackers intenten conectarse desde el usuario root)	-Ingreso al servidor mediante el uso de técnicas de hacking con el usuario root.

Objetivo 4: Procurar únicamente el acceso autorizado a las subredes de los mini centros de datos.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Datos	No hay un sistema de autentificación que permita asegurarse de que quien está ingresando a la red es quien dice ser.	Acceso no autorizado a las redes de la organización.	Que personas no autorizadas puedan acceder a la red de la organización sin estar debidamente autenticado. Pudiendo acceder a los datos de la organización.

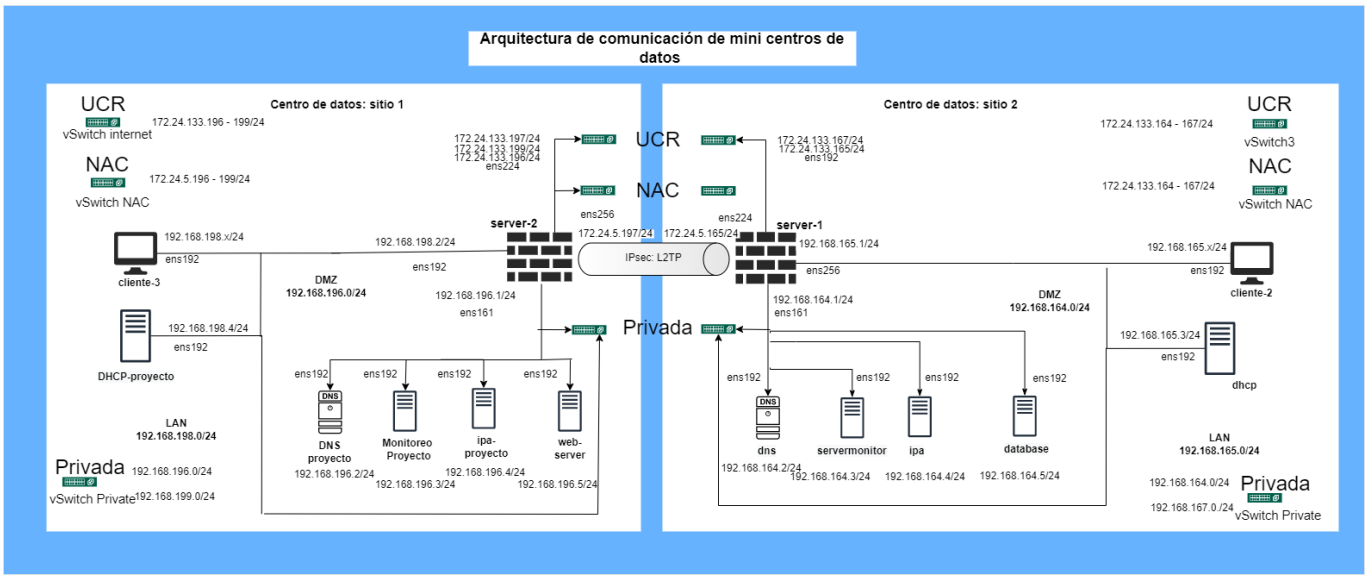
2.5.2 Accesos permitidos

Sitio 1		
LAN	DMZ	✔
DMZ	LAN	**X**

Sitio 2		
LAN	DMZ	✔
DMZ	LAN	**X**

Sitio 1 a Sitio 2 - Sitio 2 a Sitio 1		
LAN	LAN	✔
LAN	DMZ	✔
DMZ	LAN	**X**
DMZ	DMZ	✔

2.6 Arquitectura de comunicación



1. **Red de acceso a internet**
   Esta red permite las conexiones hasta y desde internet, así como a la red de la UCR. Cuentan con el siguiente direccionamiento:

Sitio 1	vSwitch	Sitio 2	vSwitch
172.24.133.196/24	vSwitch internet		
172.24.133.197/24	vSwitch internet	172.24.133.165/24	vSwitch3
172.24.133.199/24	vSwitch internet	172.24.133.167/24	vSwitch3

2. **Una red para el túnel IPsec:**

   Esta red está destinada a ser sobre la cual se monta el túnel de comunicación segura IPsec por el cual va a pasar todo el tráfico entre sitios.

Sitio 1	vSwitch	Sitio 2	vSwitch
172.24.5.197/24	vSwitch NAC	172.24.5.165/24	vSwitch2

3. **Una zona desmilitarizada para hospedar servicios:**

Esta zona está dedicada a alojar servicios que pueden ser accedidos tanto por los usuarios de la LAN como desde internet, brindando seguridad particularmente hacia la LAN. Es por esto es que decidió dedicar una red privada exclusivamente para estas zonas y se describen a continuación:

Sitio 1

DMZ 192.168.196.0/24				
Host	**Dirección ip**	**Interfaz**	**vSwitch**	**Función**
server-1	192.168.196.1	ens161	vSwitch Private	Gateway
DNS-proyecto	192.168.196.2	ens192	vSwitch Private	DNS
ipa-proyecto	192.168.196.4	ens192	vSwitch Private	FreeIPA
Monitoreo Proyecto	192.168.196.3	ens192	vSwitch Private	php server monitor
web-server	192.168.196.5	ens192	vSwitch Private	moodle
web-server	192.168.196.5	ens192	vSwitch Private	nextcloud

web-server	192.168.196.5	ens192	vSwitch Private	osTicket

Sitio 2

DMZ 192.168.164.0/24				
Host	**Dirección ip**	**Interfaz**	**vSwitch**	**Función**
server-2	192.168.164.1	ens161	vSwitch4	Gateway
dns	192.168.164.2	ens192	vSwitch4	DNS secundario
ipa	192.168.164.4	ens192	vSwitch4	FreeIPA replica
servermonitor	192.168.164.3	ens192	vSwitch4	php server monitor
database	192.168.164.5	ens192	vSwitch4	mysql

DNS

DNS de la organización	
Dominio DNS externo	quierograduarme.com
Dominio DNS interno	quierograduarme.ya

4. **Una LAN para los clientes:**

Esta red está dedicada especialmente a usuarios o clientes de los servicios que se van a ofrecer. Al estar protegida por un firewall y separada de la DMZ se espera que se brinde un mejor nivel de seguridad ya que no existe un acceso directo desde internet hasta la LAN propiamente. Además, en esta red se encuentra el servicio de DHCP.

Sitio 1

LAN 192.168.198.0/24				
Host	**Dirección ip**	**Interfaz**	**vSwitch**	**Función**
server-2	192.168.198.2/24	ens192	vSwitch Private	Gateway
DHCP-proyecto	192.168.198.4/24	ens192	vSwitch Private	DHCP
cliente-3	192.168.198.x/24	ens192	vSwitch Private	cliente de pruebas

Sitio 2

LAN 192.168.165.0/24

Host	Dirección ip	Interfaz	vSwitch	Función
server-1	192.168.165.1/24	ens256	vSwitch4	Gateway
DHCP-proyecto	192.168.165.3/24	ens192	vSwitch4	DHCP
cliente-2	192.168.165.x/24	ens192	vSwitch4	cliente de pruebas

DHCP		
	Rango	**Tipo**
Sitio1	192.168.198.10-192.168.198.100	Master
Sitio 2	192.168.165.10-192.168.165.100	Slave

3. Restricciones y limitaciones

Acceso red pública NAC: solo aquellas personas con acceso a la red pública NAC puede conectarse al sitio., por lo que siempre que deseen ingresar desde un lugar ajeno deberán utilizar una vpn.

Cantidad de almacenamiento: De momento no se cuenta con los recursos suficientes para ofrecer una gran cantidad de almacenamiento,por lo que va a ser bastante limitado y controlado hasta que se corrija la situación.

Implementación de IPSec

La configuración de IPSec se realizó con la ayuda del siguiente tutorial:
https://www.tecmint.com/setup-ipsec-vpn-with-strongswan-on-centos-rhel-8/

Configuración

Se van a presentar los pasos para configurar IPSec. Esto debe realizarse en ambos servidores que fungen como firewalls. Si el paso es el mismo para ambos, sólo se va a agregar una captura de pantalla, si tienen distintas configuraciones se mostrarán ambas capturas de pantalla.

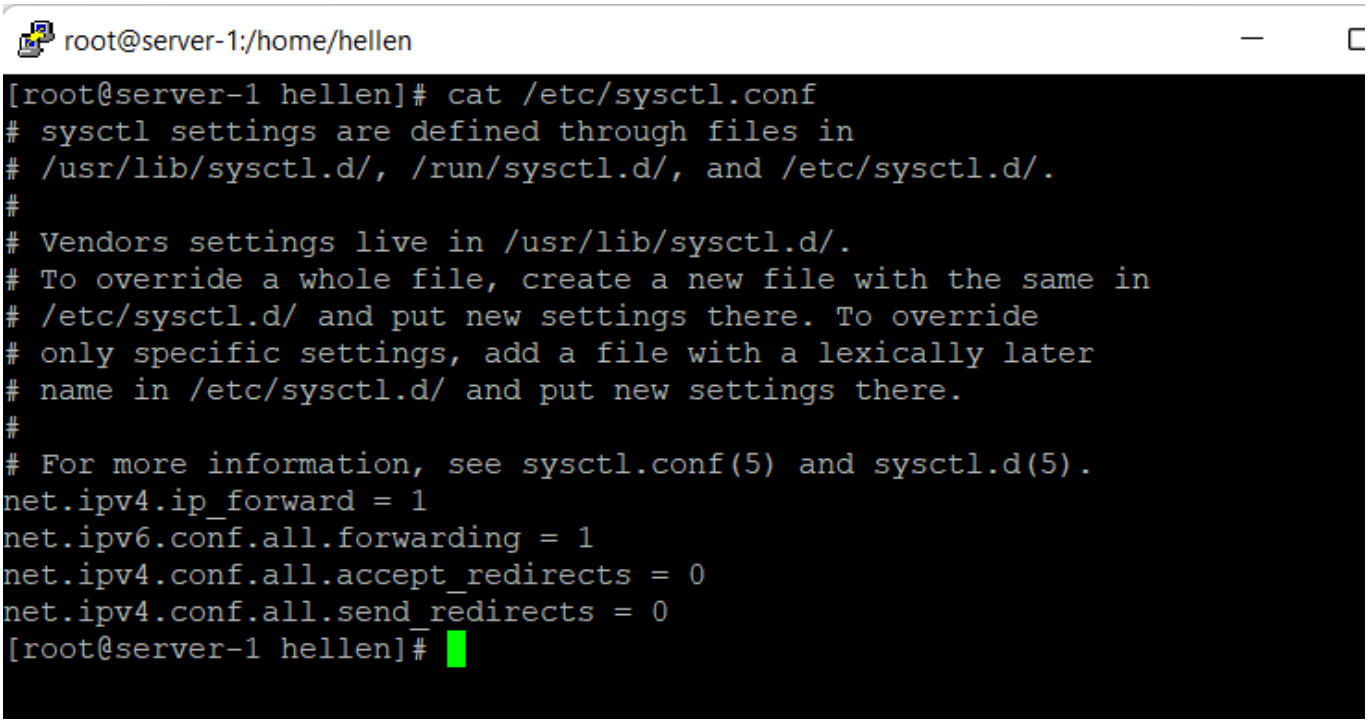
1. Habilite la funcionalidad de reenvío de IP del kernel en el archivo de configuración /etc/sysctl.conf en ambas puertas de enlace VPN.

```
# nano /etc/sysctl.conf
```

Agregue estas líneas en el archivo.

```
net.ipv4.ip_forward = 1
```

```
net.ipv6.conf.all.reenvío = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
```



2. Ejecute el siguiente comando para cargar los nuevos parámetros del kernel en tiempo de ejecución.

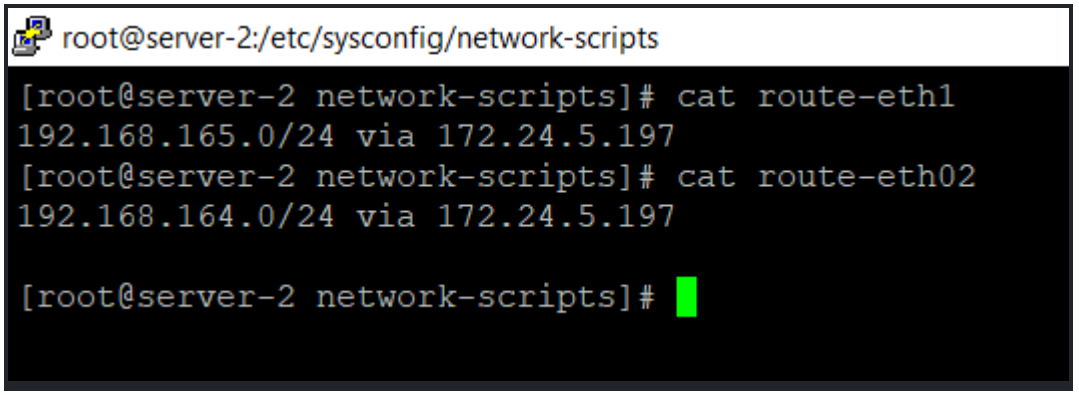
```
# sysctl-p
```

3. Cree una ruta estática permanente en el archivo /etc/sysconfig/network-scripts/route-eth0 en ambas puertas de enlace de seguridad.

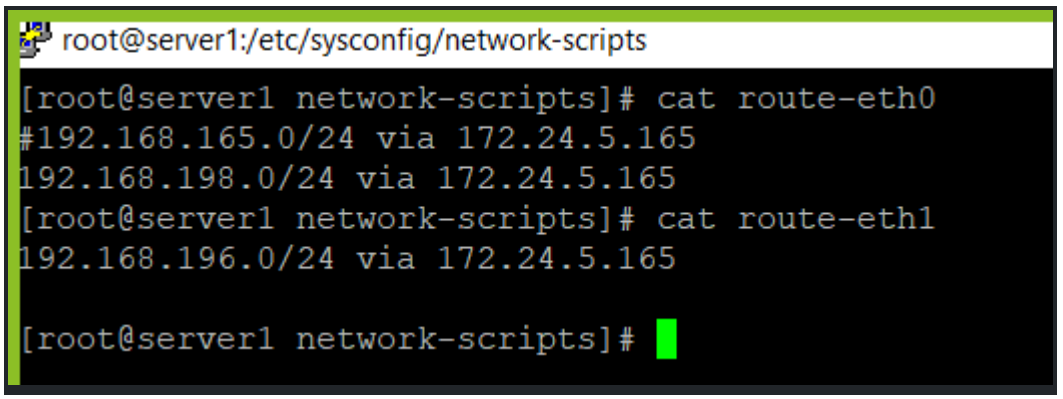
```
# nano /etc/sysconfig/network-scripts/route-eth1
```

Agregue la siguiente línea en el archivo.

```
[root@server-2 network-scripts]# cat route-eth1
192.168.165.0/24 via 172.24.5.197
[root@server-2 network-scripts]# cat route-eth02
192.168.164.0/24 via 172.24.5.197
```




```
[root@server1 network-scripts]# cat route-eth0
#192.168.165.0/24 via 172.24.5.165
192.168.198.0/24 via 172.24.5.165
[root@server1 network-scripts]# cat route-eth1
192.168.196.0/24 via 172.24.5.165
```



4. Luego reinicie el administrador de red para aplicar los nuevos cambios.

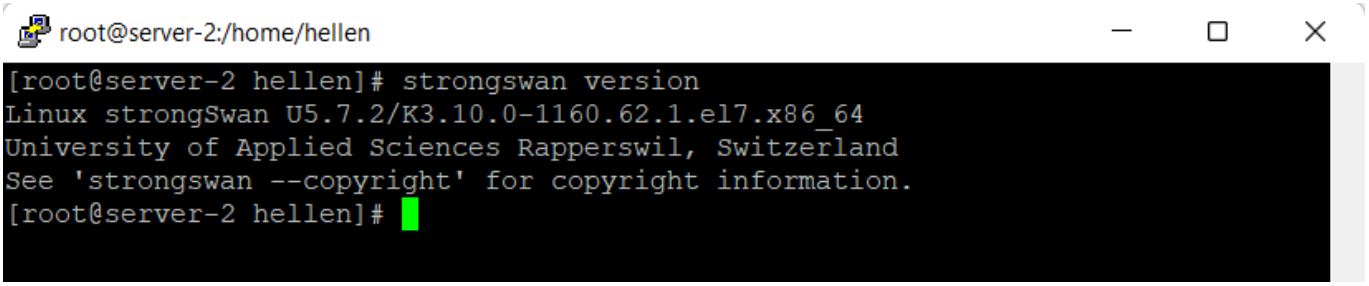
```
# systemctl reiniciar NetworkManager
```

5. Instale el paquete strongswan se proporciona en el repositorio de EPEL . Para instalarlo, debe habilitar el repositorio EPEL y luego instalar strongwan en ambas puertas de enlace de seguridad.

```
# yum install epel-release  -y
# yum install strongswan
```

6. Ejecute el siguiente comando para verificar la versión de strongswan instalada en ambas puertas de enlace.

```
# strongswan version
```



7. Inicie el servicio strongswan y habilítelo para que se inicie automáticamente al arrancar el sistema. Luego verifique el estado en ambas puertas de enlace de seguridad.

```
# systemctl start strongswan
# systemctl enable strongswan
# systemctl status strongswan
```

8. Realice una copia de seguridad del archivo original de strongswan y agregue la siguiente configuración. Nota: debe comentar una linea al inicio *config setup* para que no esté repetida dentro del archivo ya que puede dar problemas:

```
# cp /etc/strongswan/ipsec.conf /etc/strongswan/ipsec.conf.orig
# nano /etc/strongswan/ipsec.conf
```

Para el server-2 (Sitio 1)

```
config setup
        charondebug="all"
        uniqueids=yes
conn lan-sitio1-lan-sitio2
        type=tunnel
        auto=start
        keyexchange=ikev2
        authby=secret
        left=172.24.5.197
        leftsubnet=192.168.198.0/24
        right=172.24.5.165
        rightsubnet=192.168.165.1/24
        ike=aes256-sha1-modp1024!
        esp=aes256-sha1!
        aggressive=no
        keyingtries=%forever
        ikelifetime=28800s
        lifetime=3600s
        dpddelay=30s
        dpdtimeout=120s
        dpdaction=restart


conn lan-sitio1-DMZ-sitio2
```

```
        type=tunnel
        auto=start
        keyexchange=ikev2
        authby=secret
        left=172.24.5.197
        leftsubnet=192.168.198.0/24
        right=172.24.5.165
        rightsubnet=192.168.164.0/24
        ike=aes256-sha1-modp1024!
        esp=aes256-sha1!
        aggressive=no
        keyingtries=%forever
        ikelifetime=28800s
        lifetime=3600s
        dpddelay=30s
        dpdtimeout=120s
        dpdaction=restart


conn DMZ-sitio1-DMZ-sitio2
        type=tunnel
        auto=start
        keyexchange=ikev2
        authby=secret
        left=172.24.5.197
        leftsubnet=192.168.196.1/24
        right=172.24.5.165
        rightsubnet=192.168.164.1/24
        ike=aes256-sha1-modp1024!
        esp=aes256-sha1!
        aggressive=no
        keyingtries=%forever
        ikelifetime=28800s
        lifetime=3600s
        dpddelay=30s
        dpdtimeout=120s
        dpdaction=restart
```

Para el server-1 (sitio 2)

```
conn gateway1-to-gateway2
        type=tunnel
        auto=start
        keyexchange=ikev2
        authby=secret
        left= 172.24.5.165
        leftsubnet=192.168.165.1/24
```

```
        right=172.24.5.197
        rightsubnet=192.168.198.2/24
        ike=aes256-sha1-modp1024!
        esp=aes256-sha1!
        aggressive=no
        keyingtries=%forever
        ikelifetime=28800s
        lifetime=3600s
        dpddelay=30s
        dpdtimeout=120s
        dpdaction=restart


conn LAN-to-DMZ
        type=tunnel
        auto=start
        keyexchange=ikev2
        authby=secret
        left= 172.24.5.165
        leftsubnet=192.168.165.1/24
        right=172.24.5.197
        rightsubnet=192.168.196.1/24
        ike=aes256-sha1-modp1024!
        esp=aes256-sha1!
        aggressive=no
        keyingtries=%forever
        ikelifetime=28800s
        lifetime=3600s
        dpddelay=30s
        dpdtimeout=120s
        dpdaction=restart

conn DMZ-to-DMZ
        type=tunnel
        auto=start
        keyexchange=ikev2
        authby=secret
        left= 172.24.5.165
        leftsubnet=192.168.164.1/24
        right=172.24.5.197
        rightsubnet=192.168.196.1/24
        ike=aes256-sha1-modp1024!
        esp=aes256-sha1!
        aggressive=no
        keyingtries=%forever
        ikelifetime=28800s
        lifetime=3600s
        dpddelay=30s
        dpdtimeout=120s
```

```
        dpdaction=restart
```

9. Genere un PSK fuerte para que lo utilicen los pares para la autenticación de la siguiente manera.

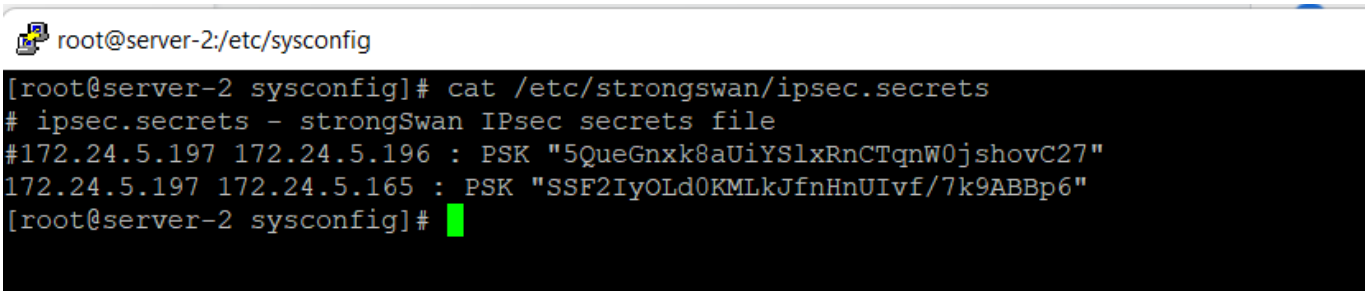
```
# head -c 24 /dev/urandom | base64
```

10. Agregue el PSK en el archivo /etc/strongswan/ipsec.conf en ambas puertas de enlace de seguridad, se agrega la misma PSK a ambos archivos.

```
# nano /etc/strongswan/ipsec.secrets
```

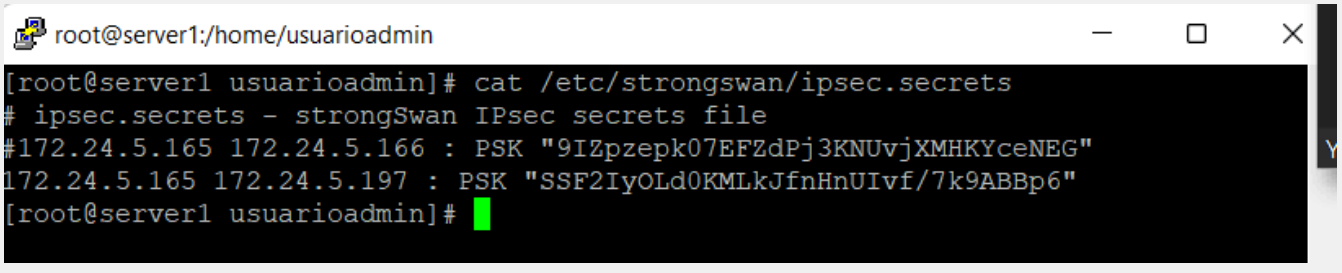
Server-2 (sitio 1)

```
# ipsec.secrets - strongSwan IPsec secrets file
172.24.5.197 172.24.5.165 : PSK "SSF2IyOLd0KMLkJfnHnUIvf/7k9ABBp6"
```



Server-1 (sitio 2)

```
# ipsec.secrets - strongSwan IPsec secrets file
172.24.5.165 172.24.5.197 : PSK "SSF2IyOLd0KMLkJfnHnUIvf/7k9ABBp6"
```



11. Luego inicie el servicio strongswan y verifique el estado de las conexiones.

```
# systemctl restart strongswan
# strongswan status
```

root@server-2:/etc/sysconfig

```
[root@server-2 sysconfig]# strongswan status
Security Associations (1 up, 0 connecting):
lan-sitio1-lan-sitio2[1]: ESTABLISHED 4 hours ago, 172.24.5.197[172.24.5.197]...172.24.5.165[172.24.5.165]
DMZ-sitio1-DMZ-sitio2{13}:  INSTALLED, TUNNEL, reqid 2, ESP SPIs: c367c968_i cc583846_o
DMZ-sitio1-DMZ-sitio2{13}:   192.168.196.0/24 === 192.168.164.0/24
lan-sitio1-lan-sitio2{14}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c638f595_i c3a411b9_o
lan-sitio1-lan-sitio2{14}:   192.168.198.0/24 === 192.168.165.0/24
[root@server-2 sysconfig]#
```

root@server1:/home/usuarioadmin

```
[root@server1 usuarioadmin]# strongswan status
Security Associations (1 up, 0 connecting):
gateway1-to-gateway2[2]: ESTABLISHED 4 hours ago, 172.24.5.165[172.24.5.165]...172.24.5.197[172.24.5.197]
  DMZ-to-DMZ{15}:  INSTALLED, TUNNEL, reqid 4, ESP SPIs: cc583846_i c367c968_o
  DMZ-to-DMZ{15}:   192.168.164.0/24 === 192.168.196.0/24
gateway1-to-gateway2{16}:  INSTALLED, TUNNEL, reqid 3, ESP SPIs: c3a411b9_i c638f595_o
gateway1-to-gateway2{16}:   192.168.165.0/24 === 192.168.198.0/24
[root@server1 usuarioadmin]#
```

Sistema de seguridad básico

Iptables

Configuración para sitio 1

Poner entrada, salida y reenvío en drop.

```
:INPUT DROP [4:1248]
:FORWARD DROP [2:158]
:OUTPUT DROP [0:0]
```

Permitir que las conexiones de input, output, forward related y established.

```
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Permitir ssh para administración propia

```
-A INPUT -s 172.17.0.0/16 -d 172.24.133.197/32 -p tcp -m state --state NEW -m tcp
--dport 22 -j ACCEPT
```

Permitir ssh desde la LAN

```
-A FORWARD -i ens192 -o ens161 -p tcp -m tcp --dport 22 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

Salida de la DMZ a internet

```
-A POSTROUTING -s 192.168.196.0/24 -o ens224 -j MASQUERADE
```

Permitir acceso desde DMZ hacia el internet

```
-A FORWARD -i ens161 -o ens224 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

Permitir acceso de internet a DMZ

```
-A FORWARD -i ens224 -o ens161 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

Permitir acceso desde la LAN hacia la DMZ

```
-A FORWARD -i ens192 -o ens161 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

Impedir el acceso de la DMZ a la LAN

```
-A FORWARD -i ens161 -o ens192 -j DROP
```

Permitir el acceso de la LAN al DNS

```
-A FORWARD -i ens192 -o ens161 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens192 -o ens161 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

Permitir el acceso desde internet al DNS

```
-A PREROUTING -d 172.24.133.197/32 -i ens224 -p udp -m udp --dport 53 -j DNAT
--to-destination 192.168.196.2:53

-A FORWARD -i ens224 -o ens161  -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

Permitir reenvío de tráfico de LAN hacia internet

```
-A FORWARD -i ens192 -o ens224 -p tcp -m tcp --dport 443 -m conntrack --ctstate
```

```
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens192 -o ens224 -p tcp -m tcp --dport 80 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

Salida de la LAN hacia internet

```
-A POSTROUTING -s 192.168.198.0/24 -o ens224 -j MASQUERADE
```

Permitir acceso desde DNS hacia internet

```
-A FORWARD -i ens161 -o ens224 -p tcp -m tcp --dport 443 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens161 -o ens224 -p tcp -m tcp --dport 80 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

Conexión desde el sitio 1 al sitio 2

Permitir el envío de tráfico a través del túnel:

```
-A FORWARD -i ens256 -m policy --dir in --pol ipsec --proto esp -j ACCEPT

-A FORWARD -o ens256 -m policy --dir out --pol ipsec --proto esp -j ACCEPT

-A FORWARD -o ens256  -p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -o ens256  -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens256-p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256  -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A OUTPUT -o ens256  -p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o ens256  -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o ens256 -p esp  -j ACCEPT

-A INPUT -i ens256 -p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A INPUT -i ens256  -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A INPUT -i ens256 -p esp  -j ACCEPT
```

Permitir acceso desde LAN-sitio-1 a LAN-sitio-2 y de LAN-sitio-1 a DMZ-sitio-2

```
 -A FORWARD -i ens192 -o ens256 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens256 -o ens192 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

Permitir echo request y echo reply

```
-A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
-A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

-A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
-A INPUT -p icmp --icmp-type echo-request -j ACCEPT

-A FORWARD -p icmp --icmp-type echo-request -j ACCEPT
-A FORWARD -p icmp --icmp-type echo-reply -j ACCEPT
```

Permitir acceso desde DMZ -sitio-1 a DMZ-sitio-2

```
-A FORWARD -i ens161 -o ens256  -d 192.168.165.0/24 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens161 -d 192.168.196.0/24 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

Permitir el acceso desde LAN-sitio-1 al DNS de la DMZ del sitio-2

```
-A FORWARD -i ens192 -o ens256 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens256 -o ens192 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens192 -o ens256 -p tcp -m tcp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens256 -o ens192 -p tcp -m tcp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

Permitir el acceso del DNS-sitio-1 hacia el DNS-sitio-2

```
-A FORWARD -i ens161 -o ens256 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens256 -o ens161 -p udp -m udp --dport 53 -m conntrack --ctstate
```

```
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens161 -o ens256 -p tcp -m tcp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens256 -o ens161 -p tcp -m tcp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

22. Prohibir el acceso de la DMZ del sitio 1 a la LAN del sitio 2

```
-A FORWARD -i ens161 -o ens256 -d 192.168.165.0/24 -j DROP
```

23. Permitir reenvío para servicios web a los distintos servidores de la DMZ

```
 -A FORWARD -i ens224 -o ens161  -p tcp -m tcp --dport 443 -j ACCEPT
-A FORWARD -i ens224 -o ens161  -p tcp -m tcp --dport 80 -j ACCEPT
-A FORWARD -i ens161 -o ens224 -p tcp -m tcp --dport 443 -j ACCEPT
-A FORWARD -i ens224 -o ens161  -p tcp -m tcp --dport 80 -j ACCEPT
```

24. Permitir el acceso desde internet al Server de monitoreo

```
-A PREROUTING -d 172.24.133.197/32 -i ens224 -p tcp -m tcp --dport 443 -j DNAT
--to-destination 192.168.196.3:443

-A PREROUTING -d 172.24.133.197/32 -i ens224 -p tcp -m tcp --dport 80 -j DNAT
--to-destination 192.168.196.3:80

-A FORWARD -i ens224 -o ens161  -p tcp -m tcp --dport 443 -j ACCEPT
-A FORWARD -i ens224 -o ens161  -p tcp -m tcp --dport 80 -j ACCEPT
-A FORWARD -i ens161 -o ens224 -p tcp -m tcp --dport 443 -j ACCEPT
-A FORWARD -i ens224 -o ens161  -p tcp -m tcp --dport 80 -j ACCEPT
```

25. Agregar reglas de input y output para servidor web

```
-A INPUT -i ens161 -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -i ens161 -p tcp -m tcp --dport 80 -j ACCEPT

-A OUTPUT -o ens161 -p tcp -m tcp --dport 443 -j ACCEPT
-A OUTPUT -o ens161 -p tcp -m tcp --dport 80 -j ACCEPT
```

26. Permitir acceso web al servidor de free ipa

```
-A PREROUTING -d 172.24.133.196/32 -i ens224 -p tcp -m tcp --dport 443 -j DNAT
--to-destination 192.168.196.4:443
-A PREROUTING -d 172.24.133.196/32 -i ens224 -p tcp -m tcp --dport 80 -j DNAT
--to-destination 192.168.196.4:80
```

#27. Permitir acceso desde la LAN al free ipa

```
-A FORWARD -i ens192 -o ens161 -p tcp --match multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens161 -o ens192 -p tcp --match multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate ESTABLISHED -j ACCEPT

-A FORWARD -i ens192 -o ens161 -p udp --match multiport --dports 88,464,123,53 -m
conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens161 -o ens192 -p udp --match multiport --dports 88,464,123,53 -m
conntrack --ctstate ESTABLISHED -j ACCEPT
```

28. Permitir comunicación desde DMZ1 a la DMZ2 para servicios del free ipa

```
-A FORWARD -i ens256 -o ens161 -p tcp --match multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens161 -o ens256 -p tcp --match multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate ESTABLISHED -j ACCEPT

-A FORWARD -i ens256 -o ens161 -p udp --match multiport --dports 88,464,123,53 -m
conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens161 -o ens256 -p udp --match multiport --dports 88,464,123,53 -m
conntrack --ctstate ESTABLISHED -j ACCEPT
```

29. Permitir el acceso de ssh desde el firewall a la DMZ

```
-A OUTPUT -o ens161 -p tcp -m tcp --dport 22 -j ACCEPT
```

30. Permitir el acceso de ssh desde el firewall a la LAN

```
-A OUTPUT -o ens192 -p tcp -m tcp --dport 22 -j ACCEPT
```

31. Permitir el acceso desde internet hacia los servicios de nextcloud, osticket y moodle

```
-A PREROUTING -d 172.24.133.199/32 -i ens193 -p tcp --match tcp --dport 80 -j DNAT
--to-destination 192.168.196.5
-A PREROUTING -d 172.24.133.199/32 -i ens193 -p tcp --match tcp --dport 443 -j
DNAT  --to-destination 192.168.196.5
```

32. Permitir acceso a la base de datos

```
-A FORWARD -i ens161 -o ens256 -p tcp --match tcp --dport 3306 -j ACCEPT
-A FORWARD -i ens256 -o ens161 -p tcp --match tcp --dport 3306 -j ACCEPT
```

Configuración final

```
# Generated by iptables-save v1.4.21 on Fri May 20 00:14:14 2022
*filter
:INPUT DROP [4:1248]
:FORWARD DROP [2:158]
:OUTPUT DROP [0:0]

-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT

#3. Permitir ssh para administración propia
-A INPUT -s 172.17.0.0/16 -d 172.24.133.197/32 -p tcp -m state --state NEW -m tcp
--dport 22 -j ACCEPT

#18. Permitir echo request y echo reply
-A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
-A INPUT -p icmp --icmp-type echo-request -j ACCEPT

#16. Permitir recibir trafico del tunel
-A INPUT -i ens256 -p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A INPUT -i ens256  -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A INPUT -i ens256 -p esp  -j ACCEPT

#25. Agregar reglas de input y output para servidor web
-A INPUT -i ens161 -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -i ens161 -p tcp -m tcp --dport 80 -j ACCEPT

-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT


#4. Permitir ssh desde la LAN
-A FORWARD -i ens192 -o ens161 -p tcp -m tcp --dport 22 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

#5. Permitir ssh al dns desde internet
-A FORWARD -i ens224 -o ens161 -p tcp -m tcp --dport 62212 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

#7. Permitir acceso desde DMZ hacia el internet
-A FORWARD -i ens161 -o ens224 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

#8. Permitir acceso de internet a DMZ
-A FORWARD -i ens224 -o ens161 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

#9. Permitir acceso desde la LAN hacia la DMZ
```

```
-A FORWARD -i ens192 -o ens161 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT


#11. Permitir el acceso de la LAN al DNS
-A FORWARD -i ens192 -o ens161 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

#-A FORWARD -i ens224 -o ens161  -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

#12. Permitir el acceso desde internet al DNS
-A FORWARD -i ens224 -o ens161  -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

#10. Impedir el acceso de la DMZ a la LAN
-A FORWARD -i ens161 -o ens192 -j DROP

#13. Permitir  reenvio de tráfico de LAN hacia internet
-A FORWARD -i ens192 -o ens224 -p tcp -m tcp --dport 443 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens192 -o ens224 -p tcp -m tcp --dport 80 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

#15. Permitir acceso desde DNS hacia internet
-A FORWARD -i ens161 -o ens224 -p tcp -m tcp --dport 443 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens224 -p tcp -m tcp --dport 80 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT


#16. Permitir el envío de trafico a traves del tunel
-A FORWARD -i ens256 -m policy --dir in --pol ipsec --proto esp -j ACCEPT
-A FORWARD -o ens256 -m policy --dir out --pol ipsec --proto esp -j ACCEPT
-A FORWARD -o ens256  -p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -o ens256  -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

#17. Permitir acceso desde LAN-sitio-1 a LAN-sitio-2 y a DMZ-sitio-2
-A FORWARD -i ens192 -o ens256 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens192 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

#22. Prohibir el acceso de la DMZ del sitio 1 a la LAN del sitio 2
-A FORWARD -i ens161 -o ens256 -d 192.168.165.0/24 -j DROP
```

```
#19.  Permitir acceso desde DMZ -sitio-1 a DMZ-sitio-2 y viceversa
-A FORWARD -i ens161 -o ens256  -d 192.168.165.0/24 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens161 -d 192.168.196.0/24 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT


#20. Permitir el acceso desde LAN-sitio-1 al DNS de la DMZ del sitio-2
-A FORWARD -i ens192 -o ens256 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens192 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens192 -o ens256 -p tcp -m tcp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens192 -p tcp -m tcp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

#21. Permitir el acceso del DNS-sitio-1 hacia el DNS-sitio-2
-A FORWARD -i ens161 -o ens256 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens161 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens256 -p tcp -m tcp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens161 -p tcp -m tcp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT


#18. Permitir reenvio de echo request y echo reply
-A FORWARD -p icmp --icmp-type echo-request -j ACCEPT
-A FORWARD -p icmp --icmp-type echo-reply -j ACCEPT

#24. Permitir el acceso desde internet al Server de monitoreo
-A FORWARD -i ens224 -o ens161  -p tcp -m tcp --dport 443 -j ACCEPT
-A FORWARD -i ens224 -o ens161  -p tcp -m tcp --dport 80 -j ACCEPT
-A FORWARD -i ens161 -o ens224 -p tcp -m tcp --dport 443 -j ACCEPT
-A FORWARD -i ens161 -o ens224  -p tcp -m tcp --dport 80 -j ACCEPT


#26. Permitir acceso web
#-A FORWARD -i ens193 -o ens161 -p tcp -m tcp --dport 443 -j ACCEPT
#-A FORWARD -i ens193 -o ens161 -p tcp -m tcp --dport 80 -j ACCEPT
#-A FORWARD -i ens161 -o ens193 -p tcp -m tcp --dport 443 -j ACCEPT
#-A FORWARD -i ens161 -o ens193 -p tcp -m tcp --dport 80 -j ACCEPT

#27. Permitir acceso desde la LAN al free ipa
-A FORWARD -i ens192 -o ens161 -p tcp --match multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens192 -p tcp --match multiport --dports
```

```
80,443,389,636,88,464,53 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens192 -o ens161 -p udp --match multiport --dports 88,464,123,53 -m
conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens192 -p udp --match multiport --dports 88,464,123,53 -m
conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

#28. Permitir comunicacion desde DMZ1 a la DMZ2 para servicios del free ipa
-A FORWARD -i ens256 -o ens161 -p tcp --match multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens256 -p tcp --match multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens161 -p udp --match multiport --dports 88,464,123,53 -m
conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens256 -p udp --match multiport --dports 88,464,123,53 -m
conntrack --ctstate ESTABLISHED -j ACCEPT


#32. Permitir acceso a la base de datos
-A FORWARD -i ens161 -o ens256 -p tcp --match tcp --dport 3306 -j ACCEPT
-A FORWARD -i ens256 -o ens161 -p tcp --match tcp --dport 3306 -j ACCEPT


-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#18. Permitir echo request y echo reply
-A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
-A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

#16. Permitir el trafico a traves del tunel
-A OUTPUT -o ens256  -p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o ens256  -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o ens256 -p esp  -j ACCEPT


#25. Agregar reglas de input y output para servidor web
-A OUTPUT -o ens161 -p tcp -m tcp --dport 443 -j ACCEPT
-A OUTPUT -o ens161 -p tcp -m tcp --dport 80 -j ACCEPT

#29. Permitir el acceso de ssh desde el firewall a la DMZ
-A OUTPUT -o ens161 -p tcp -m tcp --dport 22 -j ACCEPT

#30. Permitir el acceso de ssh desde el firewall a la LAN
-A OUTPUT -o ens192 -p tcp -m tcp --dport 22 -j ACCEPT



COMMIT
```

```
# Completed on Fri May 20 00:14:14 2022
# Generated by iptables-save v1.4.21 on Fri May 20 00:14:14 2022
*nat
:PREROUTING ACCEPT [6:1406]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]



# 12. Permitir el acceso desde internet al DNS

-A PREROUTING -d 172.24.133.197/32 -i ens224 -p udp -m udp --dport 53 -j DNAT
--to-destination 192.168.196.2:53


#6. Salida de la DMZ a internet
-A POSTROUTING -s 192.168.196.0/24 -o ens224 -j MASQUERADE

#14. Salida de la LAN hacia internet
-A POSTROUTING -s 192.168.198.0/24 -o ens224 -j MASQUERADE


#24. Permitir el acceso desde internet al Server de monitoreo
-A PREROUTING -d 172.24.133.199/32 -i ens224 -p tcp -m tcp --dport 443 -j DNAT
--to-destination 192.168.196.3:443
-A PREROUTING -d 172.24.133.199/32 -i ens224 -p tcp -m tcp --dport 80 -j DNAT
--to-destination 192.168.196.3:80


#26. Permitir acceso  al servidor de free ipa desde web
-A PREROUTING -d 172.24.133.196/32 -i ens224 -p tcp -m tcp --dport 443 -j DNAT
--to-destination 192.168.196.4:443
-A PREROUTING -d 172.24.133.196/32 -i ens224 -p tcp -m tcp --dport 80 -j DNAT
--to-destination 192.168.196.4:80

#31. Permitir el acceso desde internet hacia los servicios
-A PREROUTING -d 172.24.133.197/32 -i ens224 -p tcp --match tcp --dport 80 -j DNAT
--to-destination 192.168.196.5:80
-A PREROUTING -d 172.24.133.197/32 -i ens224 -p tcp --match tcp --dport 443 -j
DNAT  --to-destination 192.168.196.5:443
```

Configuración para sitio 2

1. Poner entrada, salida y reenvío en drop.

```
:INPUT DROP [4:1248]
:FORWARD DROP [2:158]
:OUTPUT DROP [0:0]
```

2. Permitir que las conexiones de input, output, forward related y established.

```
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

3. Permitir ssh para administración propia

```
-A INPUT -s 172.17.0.0/16 -d 172.24.133.165/32 -p tcp -m state --state NEW -m tcp
--dport 22 -j ACCEPT
```

4. Permitir ssh desde la LAN hacia la DMZ

```
-A INPUT -s 172.17.0.0/16 -d 172.24.133.165/32 -p tcp -m state --state NEW -m tcp
--dport 22 -j ACCEPT
```

5. Salida de la DMZ a internet

```
-A POSTROUTING -s 192.168.164.0/24 -o ens192 -j MASQUERADE
```

6. Permitir acceso desde DMZ hacia el internet

```
-A FORWARD -i ens161 -o ens192 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

7. Permitir acceso de internet a DMZ

```
-A FORWARD -i ens192 -o ens161 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

8. Permitir acceso desde la LAN hacia la DMZ

```
 -A FORWARD -i ens256 -o ens161 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

9. Impedir el acceso de la DMZ a la LAN

```
-A FORWARD -i ens161 -o ens256 -j DROP
```

10. Permitir el acceso de la LAN al DNS

```
-A FORWARD -i ens256 -o ens161 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

11. Permitir el acceso desde internet al DNS

```
-A PREROUTING -d 172.24.133.165/32 -i ens192 -p udp -m udp --dport 53 -j DNAT
--to-destination 192.168.164.2:53

-A FORWARD -i ens192 -o ens161  -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

13. Permitir reenvío de tráfico de LAN hacia internet

```
-A FORWARD -i ens256 -o ens192 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens256 -o ens192 -p tcp -m tcp --dport 443 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens256 -o ens192 -p tcp -m tcp --dport 80 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

14. Salida de la LAN hacia internet

```
-A POSTROUTING -s 192.168.165.0/24 -o ens192 -j MASQUERADE
```

15. Permitir acceso desde DNS hacia internet

```
-A FORWARD -i ens161 -o ens192 -p tcp -m tcp --dport 443 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens161 -o ens192 -p tcp -m tcp --dport 80 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

Conexión desde el sitio 2 al sitio 1

16. Permitir el envío de tráfico a traves del tunel

-

```
A FORWARD -i ens224 -m policy --dir in --pol ipsec --proto esp -j ACCEPT
-A FORWARD -o ens224 -m policy --dir out --pol ipsec --proto esp -j ACCEPT
-A FORWARD -o ens224   -p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -o ens224  -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens224 -p udp -m udp --dport 500 -m conntrack --ctstate
```

```
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens224  -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o ens224  -p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o ens224 -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o ens224 -p esp  -j ACCEPT
-A INPUT -i ens224 -p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A INPUT -i ens224  -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A INPUT -i ens224 -p esp  -j ACCEPT
```

17. Permitir acceso desde LAN-sitio-2 a LAN-sitio-1 y de LAN-sitio-2 a DMZ-sitio-1

```
-A FORWARD -i ens256 -o ens224 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens224 -o ens256 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

18. Permitir echo request y echo reply

```
-A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
-A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

-A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
-A INPUT -p icmp --icmp-type echo-request -j ACCEPT

-A FORWARD -p icmp --icmp-type echo-request -j ACCEPT
-A FORWARD -p icmp --icmp-type echo-reply -j ACCEPT
```

22. Prohibir el acceso de la DMZ del sitio 2 a la LAN del sitio 1

```
-A FORWARD -i ens161 -o ens224 -d 192.168.198.0/24 -j DROP
```

19. Permitir acceso desde DMZ -sitio-2 a DMZ-sitio-1 y a LAN-sitio-1

```
-A FORWARD -i ens161 -o ens224 -d 192.168.196.0 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens224 -o ens161 -d 192.168.165.0 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

20.Permitir el acceso desde LAN-sitio-2 al DNS de la DMZ del sitio-1

```
-A FORWARD -i ens256 -o ens224 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

```
-A FORWARD -i ens224 -o ens256 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

21. Permitir el acceso del DNS-sitio-2 hacia el DNS-sitio-1

```
-A FORWARD -i ens161 -o ens224 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens224 -o ens161 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens161 -o ens224 -p tcp -m tcp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens224 -o ens161 -p tcp -m tcp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

24. Permitir el acceso desde internet al Server de monitoreo

```
-A PREROUTING -d 172.24.133.165/32 -i ens192 -p tcp -m tcp --dport 443 -j DNAT
--to-destination 192.168.164.3:443
-A PREROUTING -d 172.24.133.165/32 -i ens192 -p tcp -m tcp --dport 80 -j DNAT
--to-destination 192.168.164.3:80

-A FORWARD -i ens192 -o ens161  -p tcp -m tcp --dport 443 -j ACCEPT

-A FORWARD -i ens192 -o ens161  -p tcp -m tcp --dport 80 -j ACCEPT
```

```
-A FORWARD -i ens161 -o ens192 -p tcp -m tcp --dport 443 -j ACCEPT

-A FORWARD -i ens192 -o ens161  -p tcp -m tcp --dport 80 -j ACCEPT
```

```
-A FORWARD -i ens192 -o ens161 -p tcp -m tcp --dport 62214 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

26. Permitir acceso a los puertos 80 y 443 free ipa

```
-A PREROUTING -d 172.24.133.167/32 -i ens193 -p tcp -m tcp --dport 443 -j DNAT
--to-destination 192.168.164.4:443

-A FORWARD -i ens161 -o ens193 -p tcp -m tcp --dport 443 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens193 -o ens161 -p tcp -m tcp --dport 443 -m conntrack --ctstate
```

```
NEW,ESTABLISHED -j ACCEPT

-A PREROUTING -d 172.24.133.167/32 -i ens193 -p tcp -m tcp --dport 80 -j DNAT
--to-destination 192.168.164.4:80

-A FORWARD -i ens193 -o ens161 -p tcp -m tcp --dport 80 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens161 -o ens193 -p tcp -m tcp --dport 80 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

27. Permitir acceso de dmz sitio 2 a dmz sitio1

```
-A FORWARD -i ens224 -o ens161 -p tcp --match multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens161 -o ens224 -p tcp --match multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate ESTABLISHED -j ACCEPT

-A FORWARD -i ens224 -o ens161 -p udp --match multiport --dports 88,464,123,53 -m
conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens161 -o ens224 -p udp --match multiport --dports 88,464,123,53 -m
conntrack --ctstate ESTABLISHED -j ACCEPT
```

28. Permitir el acceso de la LAN al free ipa replica

```
-A FORWARD -i ens256 -o ens161 -p tcp --match multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens161 -o ens256 -p tcp --match multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate ESTABLISHED -j ACCEPT

-A FORWARD -i ens256 -o ens161 -p udp --match multiport --dports 88,464,123,53 -m
conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i ens161 -o ens256 -p udp --match multiport --dports 88,464,123,53 -m
conntrack --ctstate ESTABLISHED -j ACCEPT
```

29. Permitir el acceso de ssh desde el firewall a la DMZ

```
-A OUTPUT -o ens161 -p tcp -m tcp --dport 22 -j ACCEPT
```

30. Permitir el acceso de ssh desde el firewall a la LAN

```
-A OUTPUT -o ens256 -p tcp -m tcp --dport 22 -j ACCEPT
```

```
31. Permitir el acceso a los servicios
```

```
32. Permitir el acceso a la base de datos
-A FORWARD -i ens224 -o ens161 -p tcp --match tcp --dport 3306 -j ACCEPT
-A FORWARD -i ens161 -o ens224 -p tcp --match tcp --dport 3306 -j ACCEPT
```

Configuracion final

```
# Generated by iptables-save v1.4.21 on Sun Jul 17 17:35:09 2022
*nat
:PREROUTING ACCEPT [61945:5078676]
:INPUT ACCEPT [2586:844552]
:OUTPUT ACCEPT [3197:230808]
:POSTROUTING ACCEPT [36778:2541489]
-A PREROUTING -d 172.24.133.165/32 -i ens192 -p udp -m udp --dport 53 -j DNAT
--to-destination 192.168.164.2:53
-A PREROUTING -d 172.24.133.165/32 -i ens192 -p tcp -m tcp --dport 443 -j DNAT
--to-destination 192.168.164.3:443
-A PREROUTING -d 172.24.133.165/32 -i ens192 -p tcp -m tcp --dport 80 -j DNAT
--to-destination 192.168.164.3:80
-A PREROUTING -d 172.24.133.167/32 -i ens192 -p tcp -m tcp --dport 443 -j DNAT
--to-destination 192.168.164.4:443
-A PREROUTING -d 172.24.133.167/32 -i ens192 -p tcp -m tcp --dport 80 -j DNAT
--to-destination 192.168.164.4:80
-A POSTROUTING -s 192.168.164.0/24 -o ens192 -j MASQUERADE
-A POSTROUTING -s 192.168.165.0/24 -o ens192 -j MASQUERADE
COMMIT
# Completed on Sun Jul 17 17:35:09 2022
# Generated by iptables-save v1.4.21 on Sun Jul 17 17:35:09 2022
*filter
:INPUT ACCEPT [177897:56733532]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [6344:456488]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s 172.17.0.0/16 -d 172.24.133.165/32 -p tcp -m state --state NEW -m tcp
--dport 22 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -i ens224 -p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A INPUT -i ens224 -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A INPUT -i ens224 -p esp -j ACCEPT
-A INPUT -i ens161 -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -i ens161 -p tcp -m tcp --dport 80 -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens161 -p tcp -m tcp --dport 22 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens192 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens192 -o ens161 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens192 -o ens161 -p tcp -m tcp --dport 443 -j ACCEPT
-A FORWARD -i ens192 -o ens161 -p tcp -m tcp --dport 80 -j ACCEPT
-A FORWARD -i ens161 -o ens192 -p tcp -m tcp --dport 443 -j ACCEPT
-A FORWARD -i ens192 -o ens161 -p tcp -m tcp --dport 80 -j ACCEPT
```

```
-A FORWARD -i ens256 -o ens161 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens161 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens161 -p tcp -m tcp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens192 -o ens161 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens192 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens192 -p tcp -m tcp --dport 443 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens192 -p tcp -m tcp --dport 80 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens192 -p tcp -m tcp --dport 443 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens192 -p tcp -m tcp --dport 80 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens224 -m policy --dir in --pol ipsec --proto esp -j ACCEPT
-A FORWARD -o ens224 -m policy --dir out --pol ipsec --proto esp -j ACCEPT
-A FORWARD -o ens224 -p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -o ens224 -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens224 -p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens224 -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens224 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens224 -o ens256 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -d 192.168.196.0/24 -i ens161 -o ens224 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -d 192.168.165.0/24 -i ens224 -o ens161 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens224 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens224 -o ens256 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens224 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens224 -o ens161 -p udp -m udp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens224 -p tcp -m tcp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens224 -o ens161 -p tcp -m tcp --dport 53 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
#-A FORWARD -i ens161 -o ens193 -p tcp -m tcp --dport 443 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
#-A FORWARD -i ens193 -o ens161 -p tcp -m tcp --dport 443 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
#-A FORWARD -i ens193 -o ens161 -p tcp -m tcp --dport 80 -m conntrack --ctstate
```

```
NEW,ESTABLISHED -j ACCEPT
#-A FORWARD -i ens161 -o ens193 -p tcp -m tcp --dport 80 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens224 -o ens161 -p tcp -m multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens224 -p tcp -m multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate ESTABLISHED -j ACCEPT
-A FORWARD -i ens224 -o ens161 -p udp -m multiport --dports 88,464,123,53 -m
conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens224 -p udp -m multiport --dports 88,464,123,53 -m
conntrack --ctstate ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens161 -p tcp -m multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens256 -p tcp -m multiport --dports
80,443,389,636,88,464,53 -m conntrack --ctstate ESTABLISHED -j ACCEPT
-A FORWARD -i ens256 -o ens161 -p udp -m multiport --dports 88,464,123,53 -m
conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A FORWARD -i ens161 -o ens256 -p udp -m multiport --dports 88,464,123,53 -m
conntrack --ctstate ESTABLISHED -j ACCEPT
-A FORWARD -i ens224 -o ens161 -p tcp -m tcp --dport 3306 -j ACCEPT
-A FORWARD -i ens161 -o ens224 -p tcp -m tcp --dport 3306 -j ACCEPT
-A FORWARD -i ens161 -o ens256 -j DROP
-A FORWARD -d 192.168.198.0/24 -i ens161 -o ens224 -j DROP
-A FORWARD -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A OUTPUT -o ens224 -p udp -m udp --dport 500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o ens224 -p udp -m udp --dport 4500 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o ens224 -p esp -j ACCEPT
-A OUTPUT -o ens161 -p tcp -m tcp --dport 443 -j ACCEPT
-A OUTPUT -o ens161 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -o ens161 -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -o ens256 -p tcp -m tcp --dport 22 -j ACCEPT
COMMIT
# Completed on Sun Jul 17 17:35:09 2022
```

Servicios

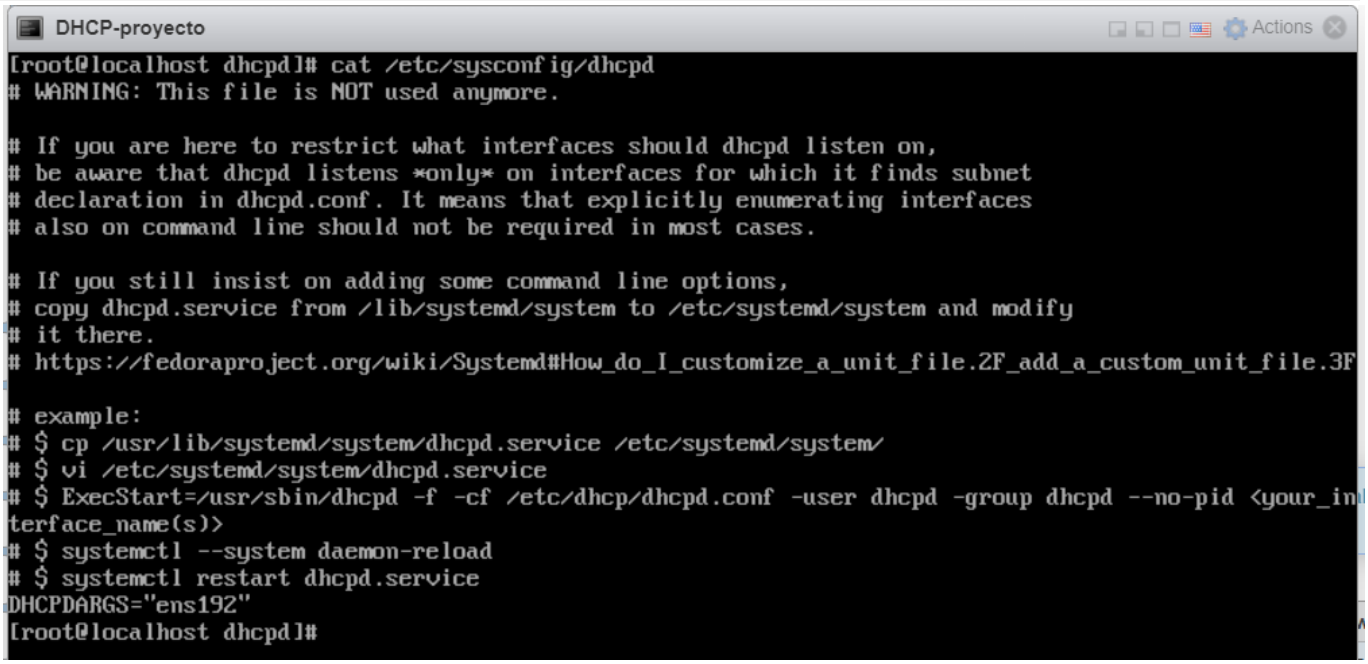
Configuración de DHCP

1. El paquete del servidor DCHP está disponible en los repositorios oficiales de las principales distribuciones de Linux, la instalación es bastante fácil, simplemente ejecute el siguiente comando.

```
yum install dhcp
```

2. Configure la interfaz en la que desea que el daemon DHCP atienda las solicitudes en el archivo de configuración /etc/sysconfig/dhcpd y configure la interfaz, en este caso “ens192”

```
nano /etc/sysconfig/dhcpd
```



3. Configure el archivo principal de dhcp. Para esto, copie y pegue la siguiente configuracion de ejemplo:

```
cp /usr/share/doc/dhcp-4.2.5/dhcpd.conf.ejemplo /etc/dhcp/dhcpd.conf

nano /etc/dhcp/dhcpd.conf
```

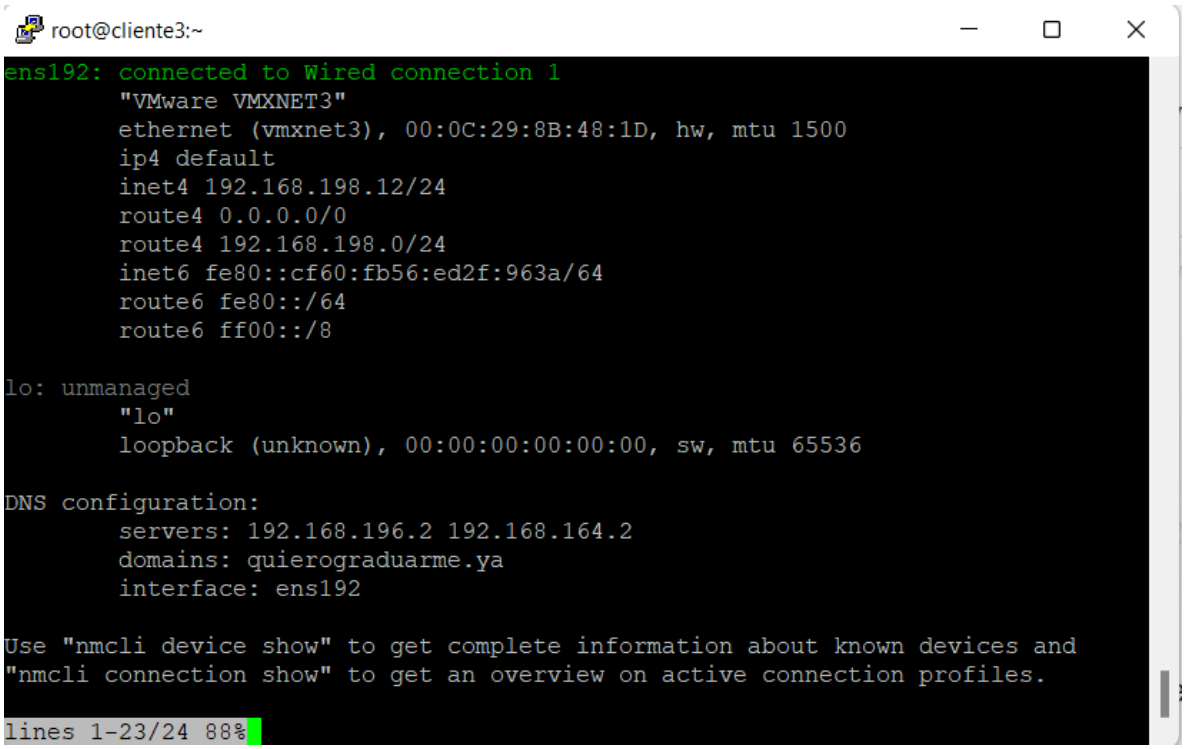
Y modifique esta sección de acuerdo a sus valores de la infraestructura:

```
subnet 192.168.198.0 netmask 255.255.255.0 {
        option routers 192.168.198.2;
        option subnet-mask 255.255.255.0;
        option domain-search "quierograduarme.ya";
        option domain-name-servers 192.168.196.2, 192.168.164.2;
        range 192.168.198.10 192.168.198.100;
```

4. Ahora inicie y habilite el servicio

```
# systemctl start dhcpd
# systemctl enable dhcpd
# systemctl enable dhcpd
```

Para comprobar que funciona correctamente, agregue una tarjeta de red a algún cliente. Esta tarjeta de red debe ser correspondiente a la red privada, de manera que como DHCP se encuentra en la misma LAN, le va a asignar direccionamiento dinámico, al encender la máquina, revisamos que se le haya asignado correctamente y que se encuentra unido al dominio de búsqueda quierograduarme.ya:



Como se puede observar se asignó la dirección ip 192.168.198.12/24. Así mismo, se le asignó a la interfaz la configuración del dns y el dominio de dns de forma automática. Lo cual es uno de los beneficios del DHCP.
Esta asignación sucede porque la máquina viene por defecto con la opción de configuración automática. No obstante, si la interfaz no recibiera automáticamente la dirección ip. Diríjase a la siguiente ruta:

```
cd /etc/sysconfig/network-scripts/
nano ifcfg-ens192
```

Y verifique que las opciones estén establecidas de la siguiente manera:

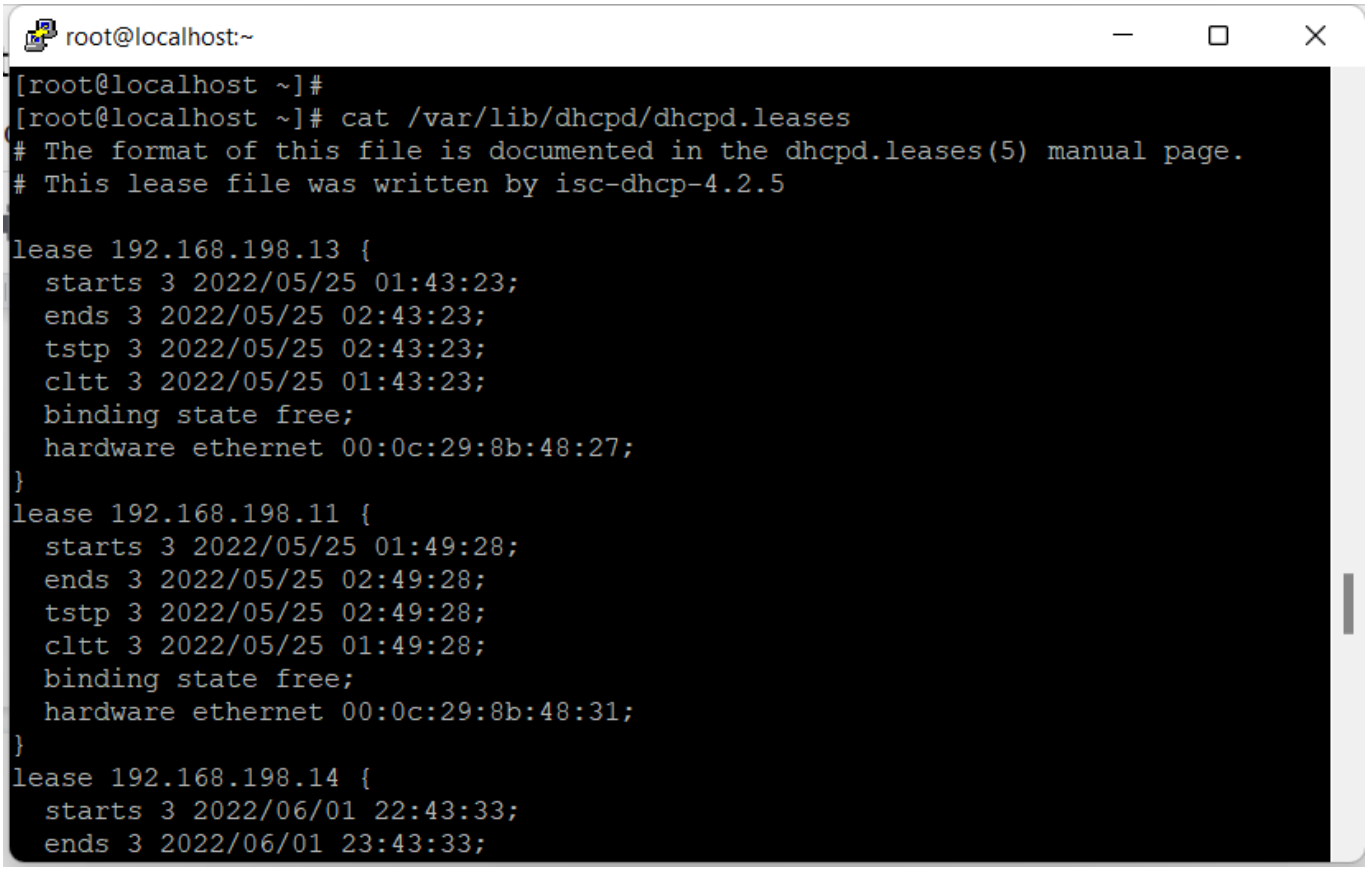
```
BOOTPROTO=dhcp
TYPE=Ethernet
ONBOOT=yes
```

Una vez realizados los cambios escriba el siguiente comando:

```
systemctl restart NetworkManager
```

Para probar que funciona correctamente desde el servidor de DHCP diríjase a la siguiente dirección y vea el archivo:

```
cd /var/lib/dhcpd
ls
cat dhcpd.leases
```



Configuración del DNS

1. Se instala el DNS con el siguiente comando:

```
yum install bind bind-utils -y
```

Para esta etapa el DNS se tienen actualmente dos dominios por lo que se debe actualizar la configuración actual de manera que se incluyan los dominios internos y externos:

Dominios	Nombre de dominio	Función
Externo	quierograduarme.com	Servicios de dominio externo para web.

Interno	quierograduarme.ya	Servicios de dominio interno para Freelpa entre otros servicios.

2. Editar el archivo named.conf para agregar la configuración de las zonas y queda de la siguiente manera:

```
nano /etc/named.conf
```

```
// // named.conf // // Provided by Red Hat bind package to configure the ISC BIND
named(8) DNS // server as a caching only nameserver (as a localhost DNS
//resolver only). // // See /usr/share/doc/bind*/sample/ for example named
configuration files. // // See the BIND Administrator's Reference Manual (ARM) for
//details about the // configuration located in
/usr/share/doc/bind-{version}/Bv9ARM.html

options {
        listen-on port 53 { 127.0.0.1; 192.168.196.2;};
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { localhost; 192.168.196.0/24; 192.168.198.0/24;
172.24.133.0/24;192.168.165.0/24;192.168.164.0/24; any;};
        allow-transfer {localhost; 192.168.164.2; };
        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable
recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to
enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable
access
           control to limit queries to your legitimate users. Failing to do so
will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.root.key";
```

```
        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

zone "quierograduarme.com" IN {
type master;
file "forward.quierograduarme";
allow-update { none; };
allow-transfer {192.168.164.2; };
forwarders {
163.178.88.2;
163.178.84.4;
};
};
zone "196.168.192.in-addr.arpa" IN {
type master;
file "reverse.quierograduarme";
allow-update { none; };
allow-transfer {192.168.164.2; };
forwarders {
163.178.88.2;
163.178.84.4;
};

};

zone "164.168.192.in-addr.arpa" IN {
type master;
file "reverse.quierograduarmesitio2";
allow-update { none; };
allow-transfer {192.168.164.2; };
forwarders {
163.178.88.2;
163.178.84.4;
```

```
};

};


zone "quierograduarme.ya" IN {
type master;
file "forward.quierograduarmeinterno";
allow-update { none; };
allow-transfer {192.168.164.2; };
forwarders {
192.168.196.2;
192.168.164.2;
};

};
zone "198.168.192.in-addr.arpa" IN {
type master;
file "reverse.quierograduarmeinterno";
allow-update { none; };
allow-transfer {192.168.164.2; };
forwarders {
192.168.196.2;
192.168.164.2;
};
};


zone "165.168.192.in-addr.arpa" IN {
type master;
file "reverse.quierograduarmeinternositio2";
allow-update { none; };
allow-transfer {192.168.164.2; };
forwarders {
192.168.196.2;
192.168.164.2;
};

};


include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

3. Se crean los archivos de forward para ambas zonas en la siguiente ruta:

> Vale la pena aclarar que en esta sección se añaden los registros A de cada servicio y que es importante cambiar el número serial a algo actualizado ya que de lo contrario pueden haber problemas al enviar actualizaciones a la réplica.

```
cd /var/named
nano forward.quierograduarme
```

Así es como quedaría la configuración:

```
$TTL 86400
@   IN  SOA     masterdns.quierograduarme.com. secondarydns.quierograduarme.com. (
        2022072007  ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
        86400       ;Minimum TTL
)

@       IN NS           masterdns.quierograduarme.com.
@       IN NS           secondarydns.quierograduarme.com.
@       IN  A           192.168.196.2
@       IN  A           192.168.196.5
@       IN  A           192.168.164.2
@       IN  A           192.168.196.4
@       IN  A           192.168.164.4
masterdns IN  A         192.168.196.2
secondarydns IN  A      192.168.164.2
aula IN A            192.168.196.5
www.aula IN A        192.168.196.5
nube IN A            192.168.196.5
www.nube IN A            192.168.196.5
soporte IN A            192.168.196.5
www.soporte IN A            192.168.196.5
ipa1.quierograduarme.ya IN A 192.168.196.4
ipareplica.quierograduarme.ya IN A 192.168.164.4
```

Ahora para la zona interna:

```
nano forward.quierograduarme.interno
```

```
$TTL 86400
@   IN  SOA     masterdns.quierograduarme.ya. secondarydns.quierograduarme.ya. (
        2022071815  ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
        86400       ;Minimum TTL
)
@       IN  NS          masterdns.quierograduarme.ya.
@       IN  NS          secondarydns.quierograduarme.ya.
```

```
@       IN  A           192.168.196.2
@       IN  A           192.168.164.2
@       IN  A           192.168.196.4
@       IN  A           192.168.164.4
ipa1 IN A               192.168.196.4
ipareplica IN A          192.168.164.4
masterdns IN A          192.168.196.2
secondarydns IN A       192.168.164.2
```

4. En la misma ruta se crean los archivos de reverse:

Para la zona externa en sitio 1:

```
nano reverse.quierograduarme
```

```
$TTL 86400
@   IN  SOA     masterdns.quierograduarme.com. root.quierograduarme.com. (
        20223434  ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
        86400       ;Minimum TTL
)
@       IN  NS           masterdns.quierograduarme.com.
@       IN  NS          secondarydns.quierograduarme.com.
@       IN  PTR         quierograduarme.com.
masterdns IN  A         192.168.196.2
secondarydns IN A       192.168.164.2
nube IN A               192.168.196.5
aula IN A               192.168.196.5
soporte IN A            192.168.196.5
2 IN  PTR          masterdns.quierograduarme.com.
4 IN PTR                ipa1.quierograduarme.ya.
5 IN PTR                nube.quierograduarme.com.
5 IN PTR                aula.quierograduarme.com.
5 IN PTR                soporte.quierograduarme.com.
```

Para la zona externa en sitio 2:

```
nano reverse.quierograduarme.sitio2
```

```
$TTL 86400
@   IN  SOA     secondary.quierograduarme.com. root.quierograduarme.com. (
        202207462  ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
```

```
        86400       ;Minimum TTL
)
@       IN  NS          secondarydns.quierograduarme.com.
@       IN  PTR         quierograduarme.com.
secondarydns IN A       192.168.164.2
2       IN PTR          secondarydns.quierograduarme.com.
4       IN PTR          ipareplica.quierograduarme.ya.
```

Para la zona interna en sitio 1:

```
nano reverse.quierograduarme.ya
```

```
$TTL 86400
@   IN  SOA     masterdns.quierograduarme.ya. secondarydns.quierograduarme.ya. (
        2011071002  ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
        86400       ;Minimum TTL
)
@       IN  NS          masterdns.quierograduarme.ya.
@       IN  NS          secondarydns.quierograduarme.ya.
@       IN  PTR         quierograduarme.ya.
```

Para la zona interna en sitio 2:

```
nano reverse.quierograduarmeinternositio2
```

```
$TTL 86400
@   IN  SOA     masterdns.quierograduarme.ya. secondarydns.quierograduarme.ya. (
        2022075243  ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
        86400       ;Minimum TTL
)
@       IN  NS          masterdns.quierograduarme.ya.
@       IN  NS          secondarydns.quierograduarme.ya.
@       IN  PTR         quierograduarme.ya.
```

5. Una vez que se edita la configuración se reinicia el servicio:

root@proyecto-dns:/home/hellen

```
[root@proyecto-dns hellen]# nano /etc/named.conf
[root@proyecto-dns hellen]# systemctl restart named
[root@proyecto-dns hellen]#
```

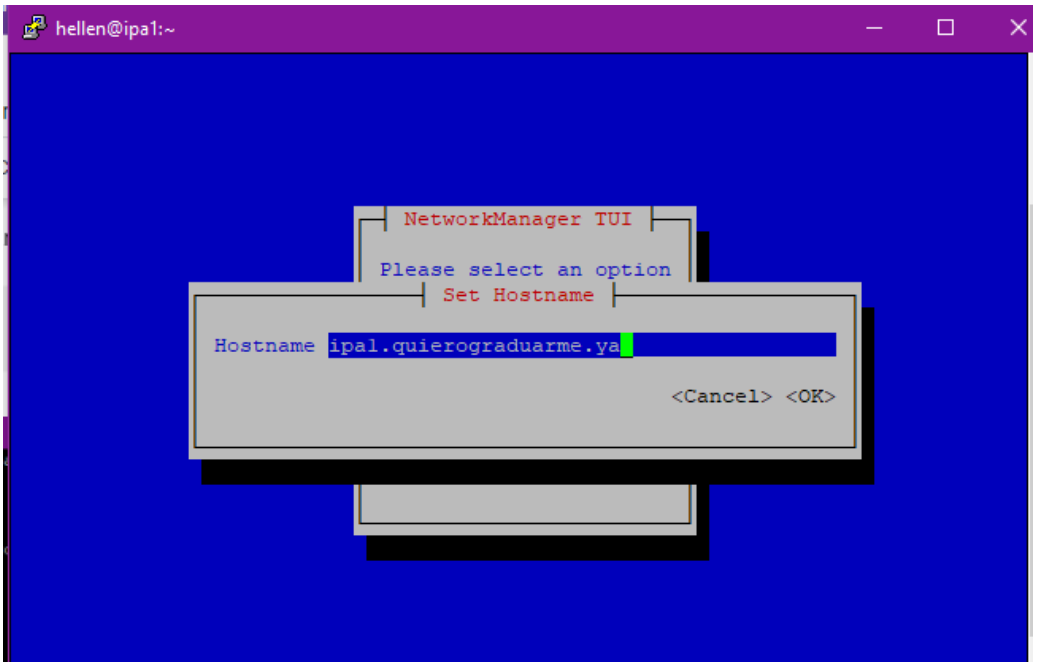
Configuración del FreeIPA

Freelpa es una herramienta de instalación y un entorno de administración de servicios e identidades, para esta infraestructura se plantea establecer un servidor primario en un sitio y su réplica en el otro sitio.
Para esto, se debe utilizar el nuevo dominio interno creado previamente en el DNS (quierograduarme.ya).

Configuración del FreeIPA primario

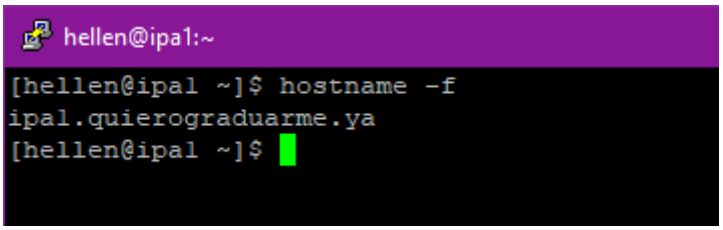
Para instalar y configurar el servidor primario de Freelpa realice los siguientes pasos:

1. Cambiar el nombre del servidor de free ipa mediante nmtui a un nombre que pertenezca al dominio interno, en este caso *ipa1.quierograduarme.ya*:



2. Se reinicia el NetworkManager y se revisa que realmente se cambiara el nombre del host:

```
systemctl restart NetworkManager
sudo bash
hostname -f
```

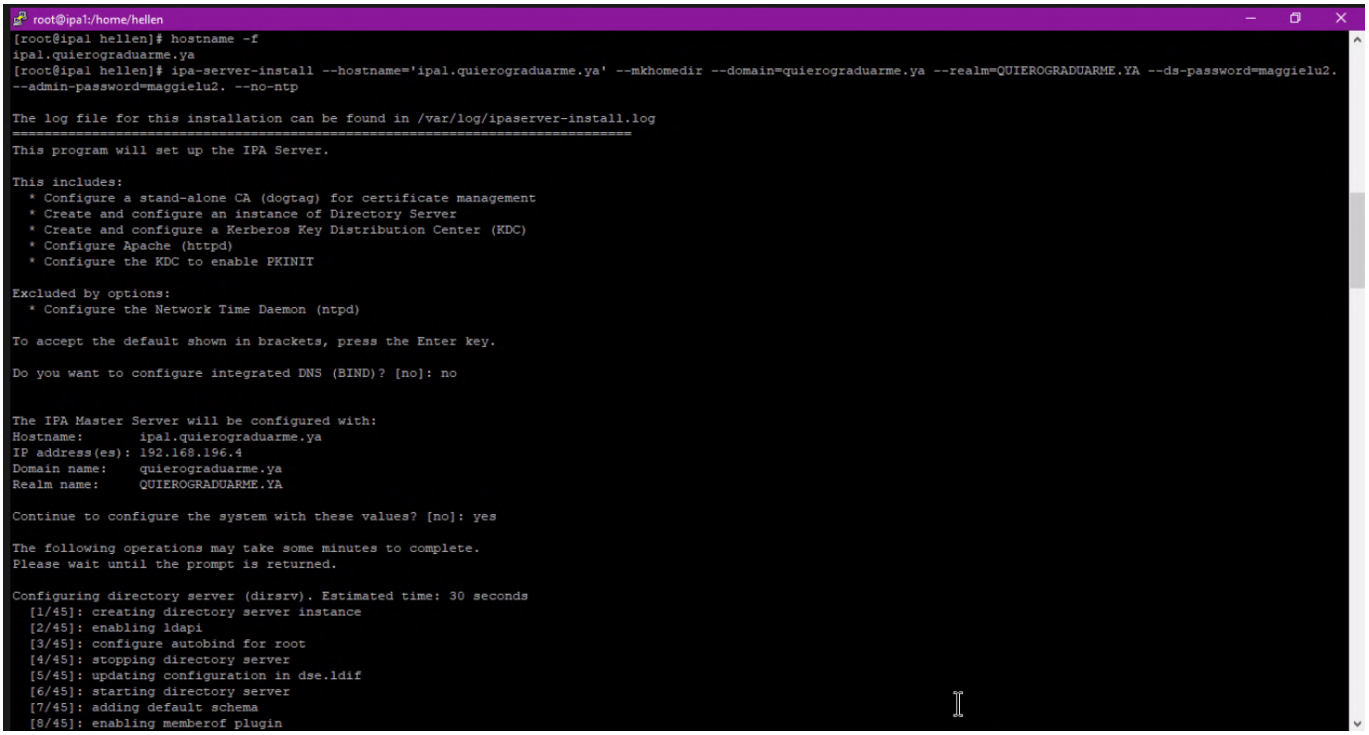


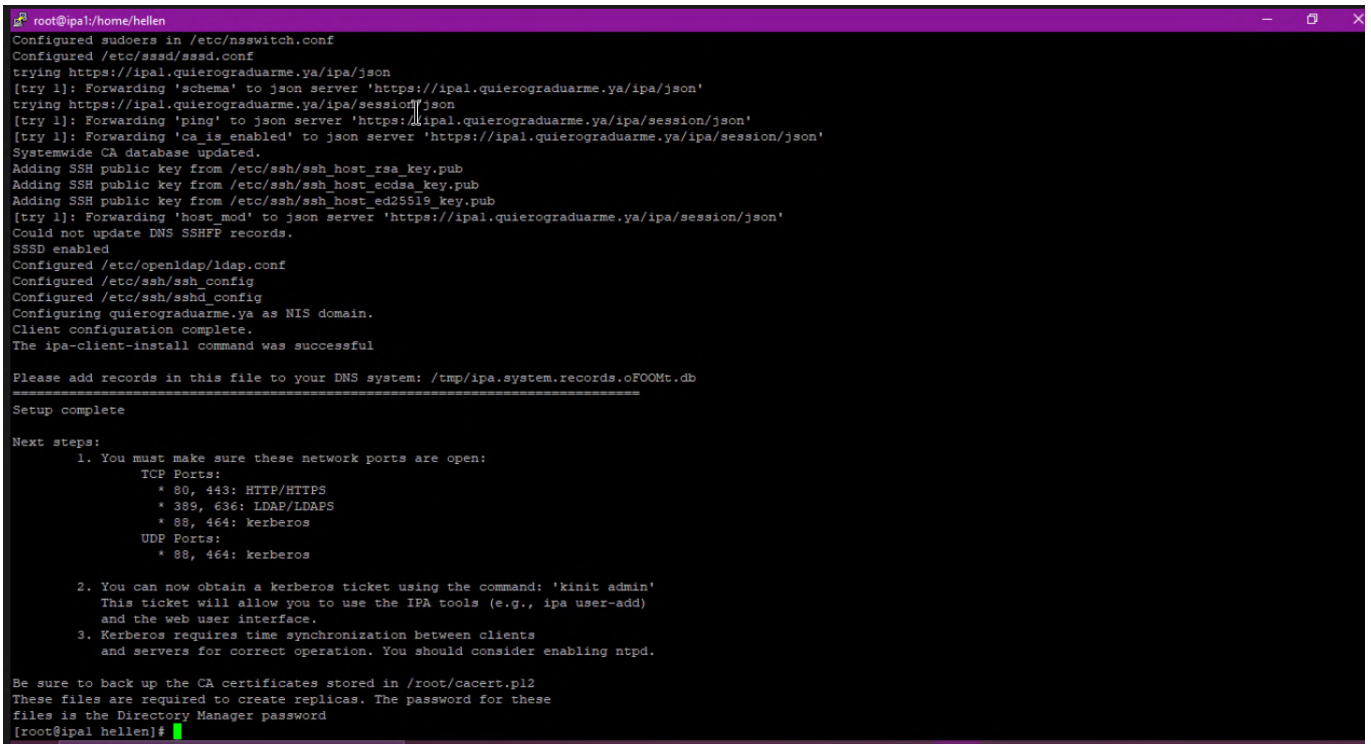
3. Instale free ipa en el servidor con el siguiente comando:

```
sudo yum -y install ipa-server
```

4. Configure el servidor de free ipa con el dominio interno del DNS de la siguiente manera:

```
ipa-server-install --hostname='ipa1.quierograduarme.ya' --mkhomedir
--domain=quierograduarme.ya --realm=QUIEROGRADUARME.YA --ds-password=maggielu2.
--admin-password=maggielu2. --no-ntp
```

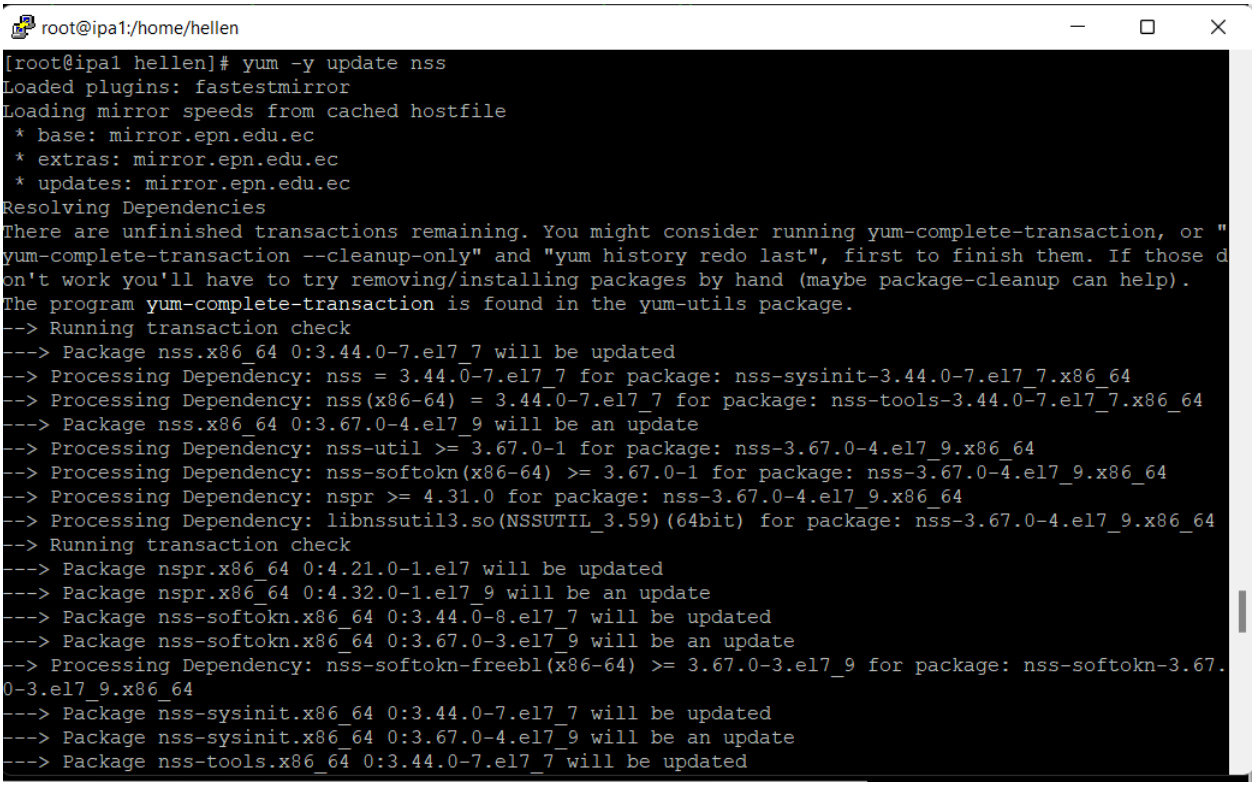


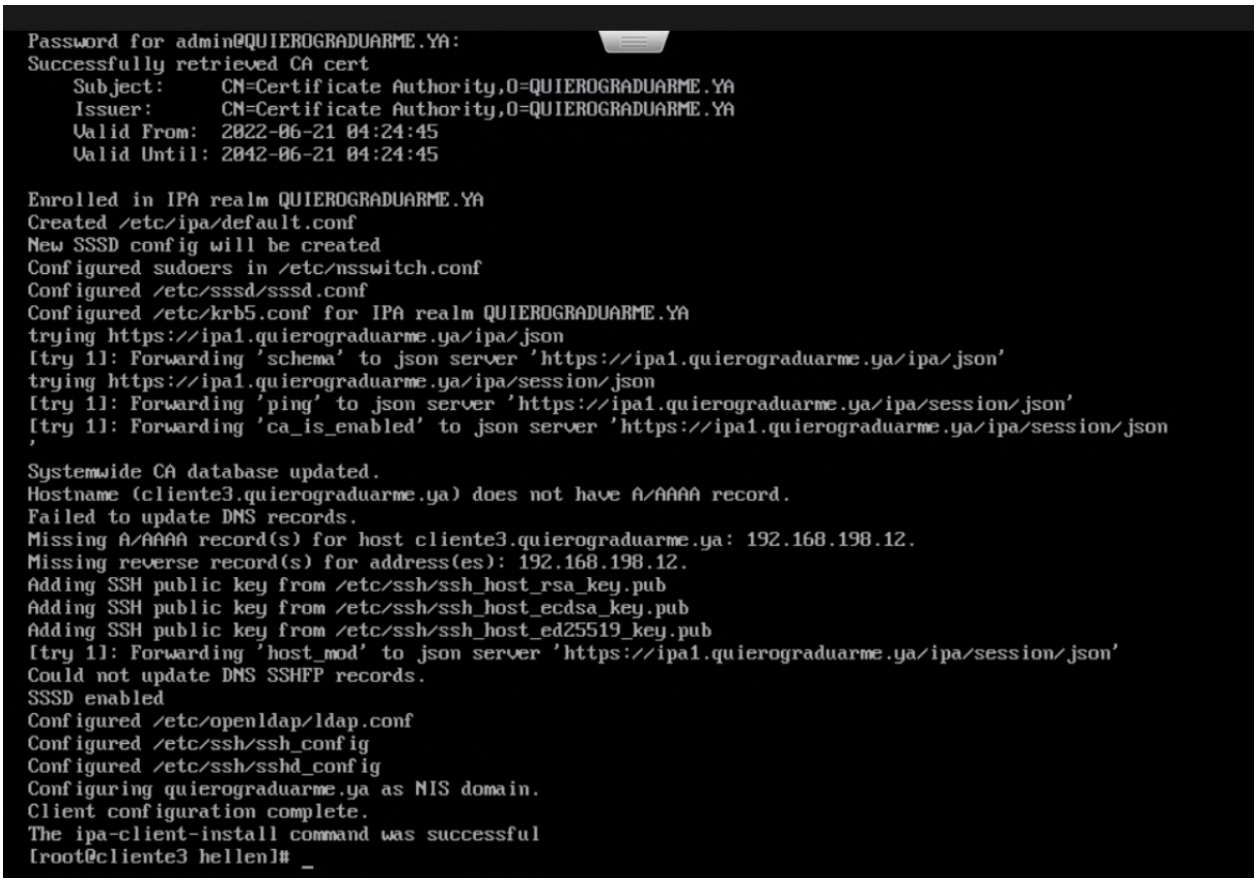


CA en el servidor primario

En este punto es importante aclarar que con la instalación del servidor primario ya se traen los CA, eso lo indica en la salida de la instalación y que los mismos se encuentran en la carpeta /root/cacert.p12.

`yum -y update nss`



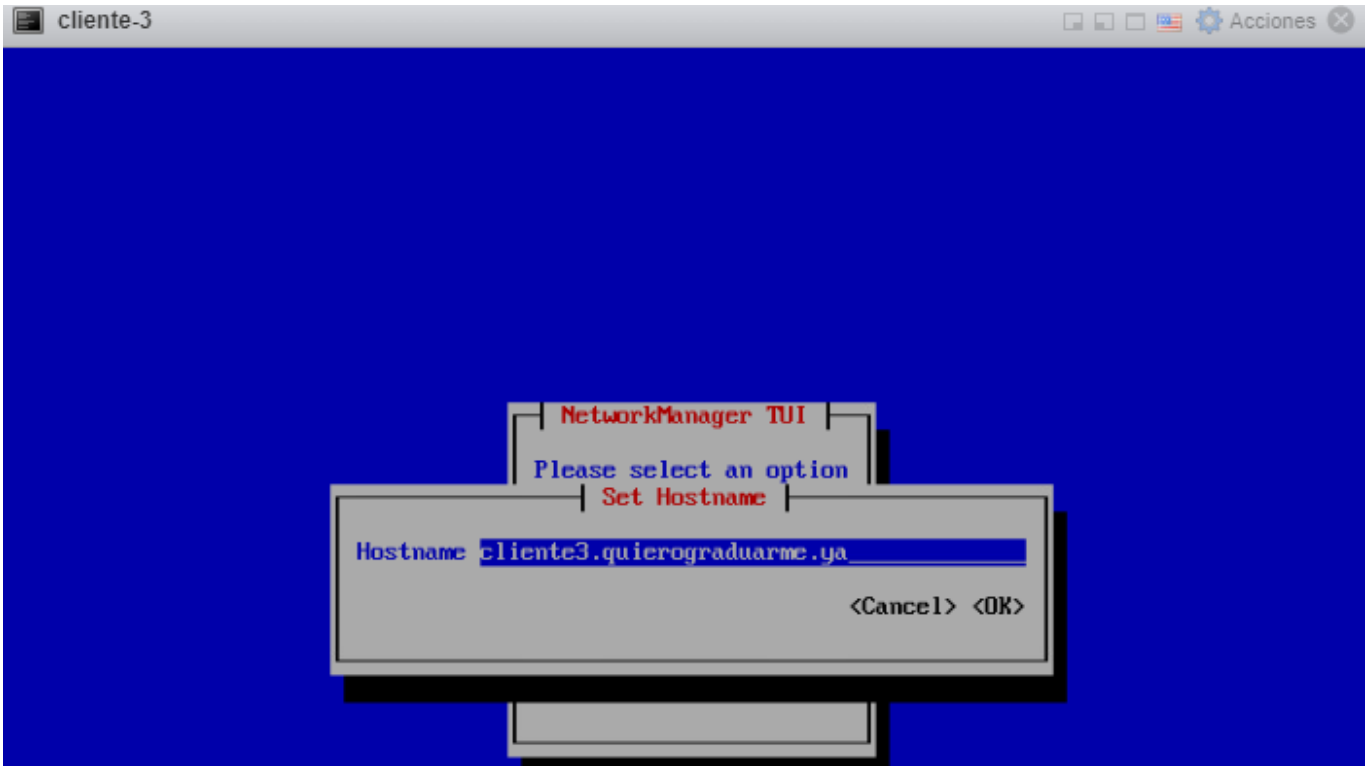


Configuración de un cliente para el free ipa primario

1. Se instala free-ipa en el cliente con el siguiente comando:

```
sudo yum -y install freeipa-client
```

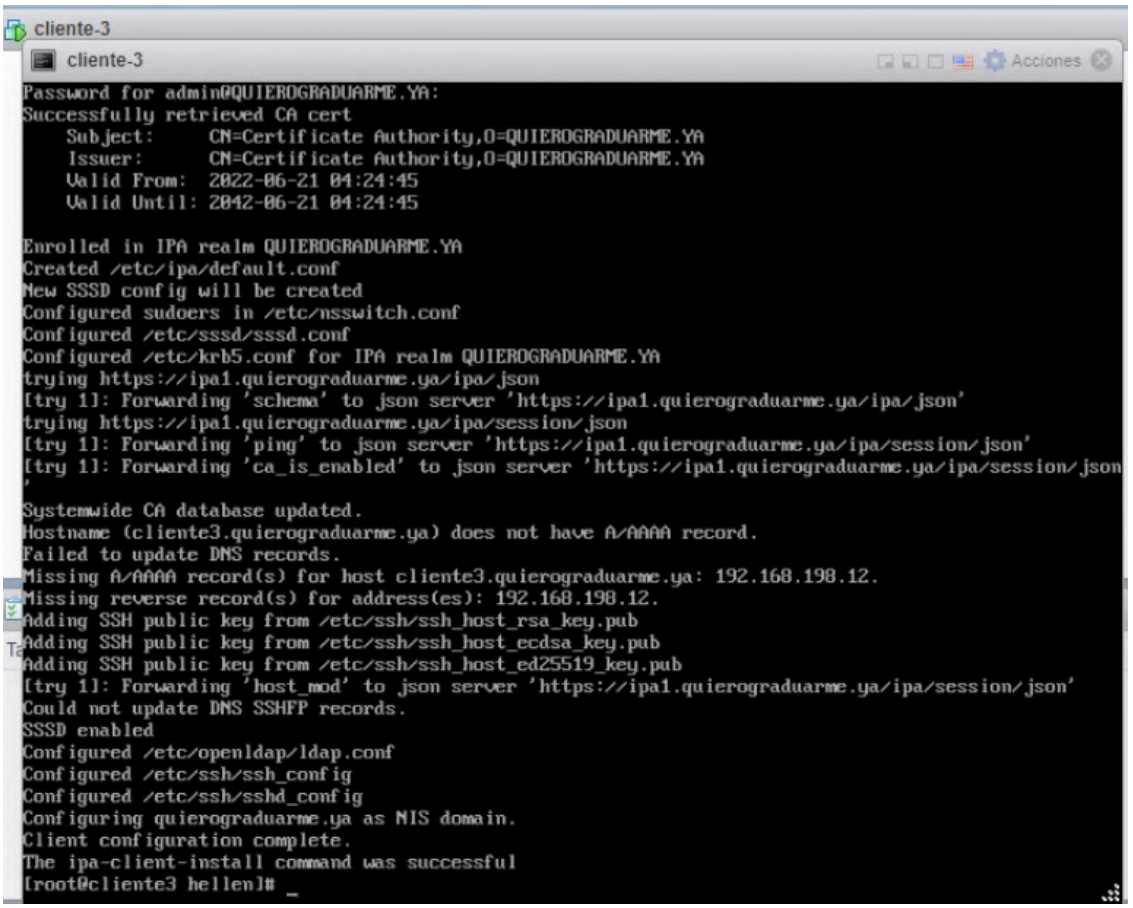
2. Se le cambia el nombre a la máquina a su FQDN del cliente mediante nmtui:



3. Se configura el cliente con el siguiente comando:

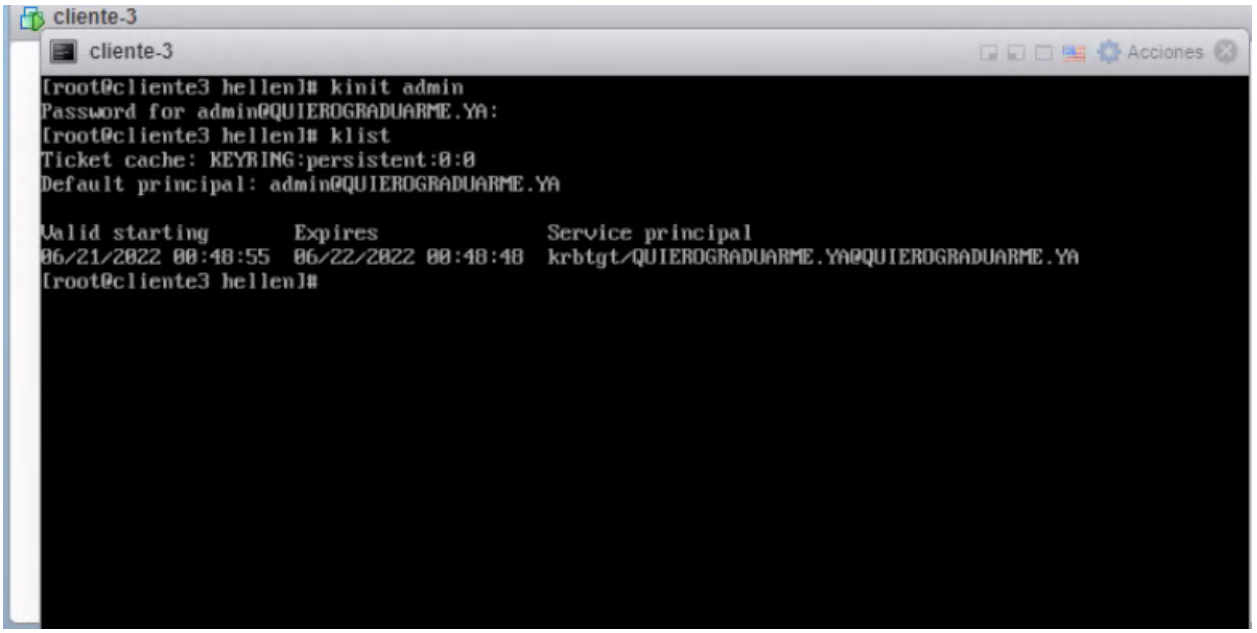
```
ipa-client-install --hostname='cliente3.quierograduarme.ya' --mkhomedir
--server=ipa1.quierograduarme.ya --domain=quierograduarme.ya
--realm=QUIEROGRADUARME.YA --no-ntp -p admin
```

Se espera que se obtenga la siguiente salida si la instalación del cliente fue exitosa:



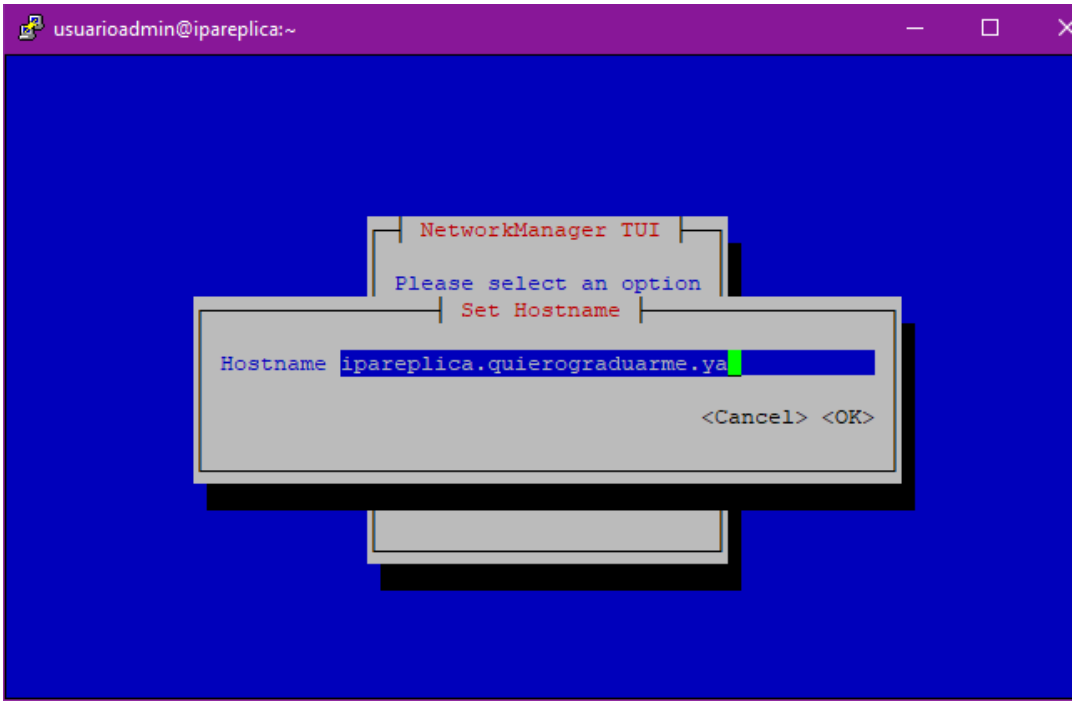
4. Compruebe que la instalación fue correcta con el siguiente comando:

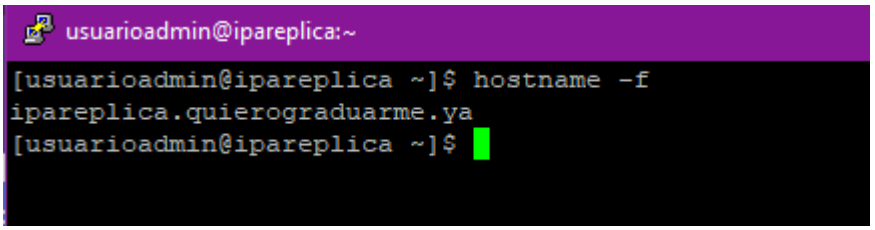
```
kinit admim
```



Instalación FreeIPA réplica

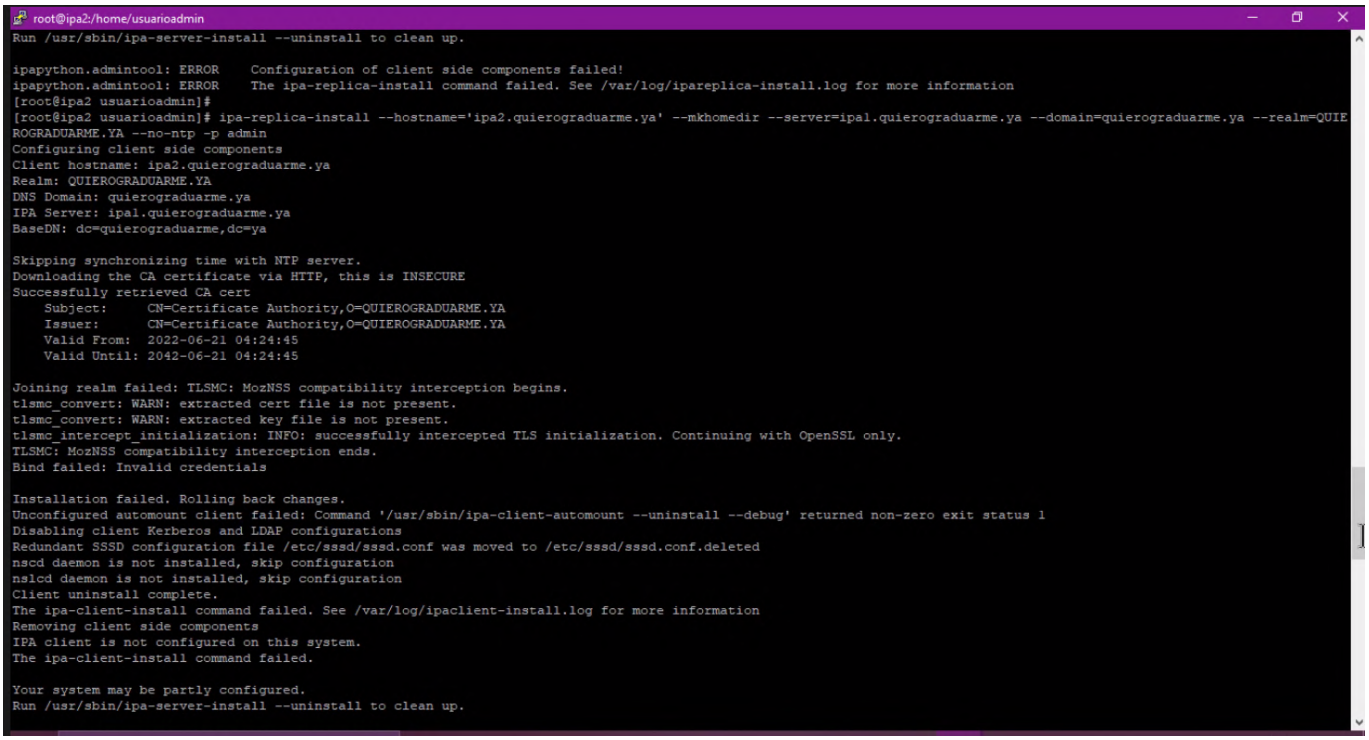
1. Se le cambia el nombre al servidor mediante nmtui a un nombre que pertenezca al dominio interno, en este caso *ipa1.quierograduarme.ya*:



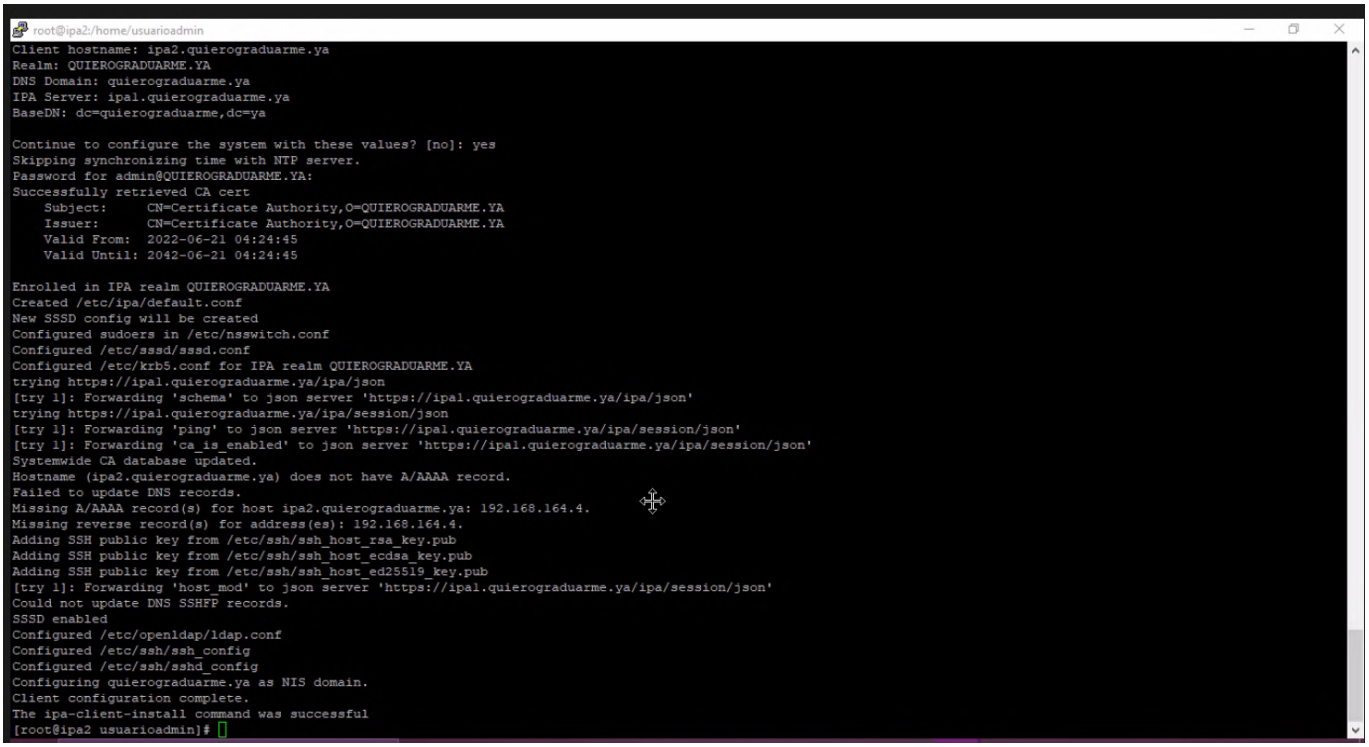


2. Se instala y se configura como cliente:

```
ipa-client-install --hostname='ipareplica.quierograduarme.ya' --mkhomedir
--server=ipa1.quierograduarme.ya --domain=quierograduarme.ya
--realm=QUIEROGRADUARME.YA --no-ntp -p admin
```

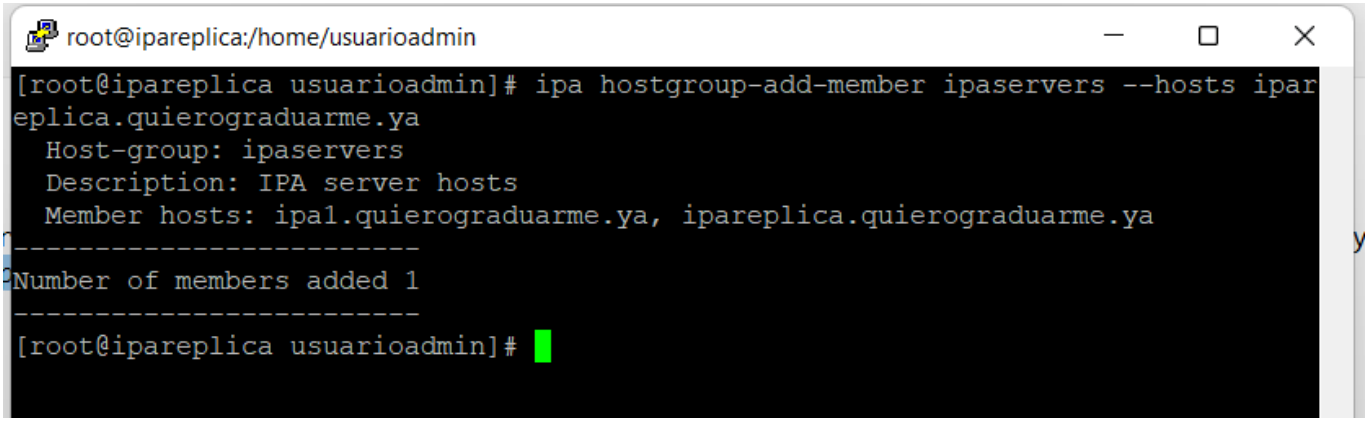


Si la instalación del cliente fue exitosa debería de tener la siguiente salida:



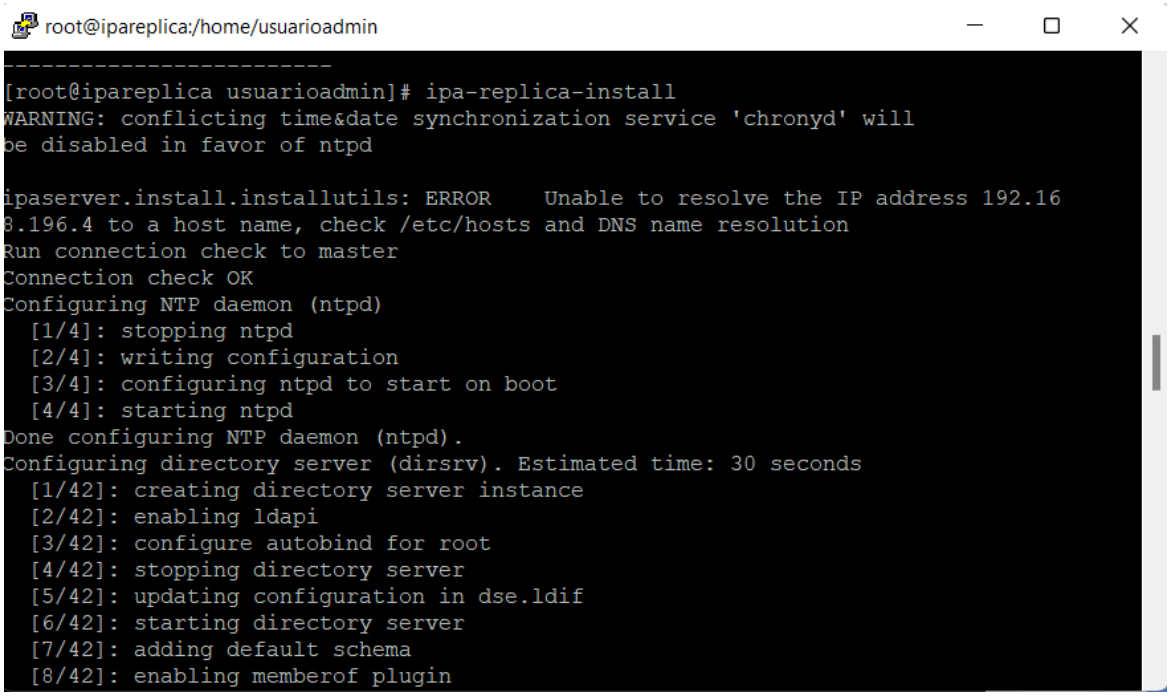
3. Se agrega al grupo de servers de ipa:

```
ipa hostgroup-add-member ipaservers --hosts ipareplica.quierograduarme.ya
```

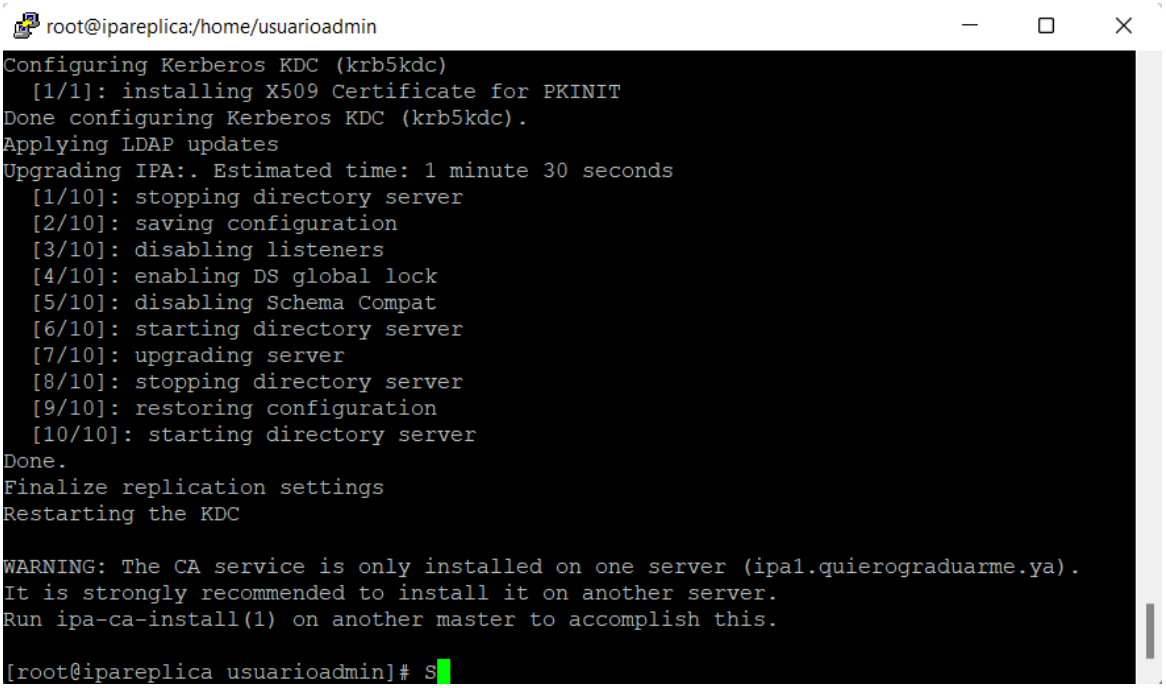


4. Se instala la réplica

```
ipa-replica-install
```



Si la instalación fue exitosa debería de tener la siguiente salida:



Configuración de un cliente para el free ipa réplica

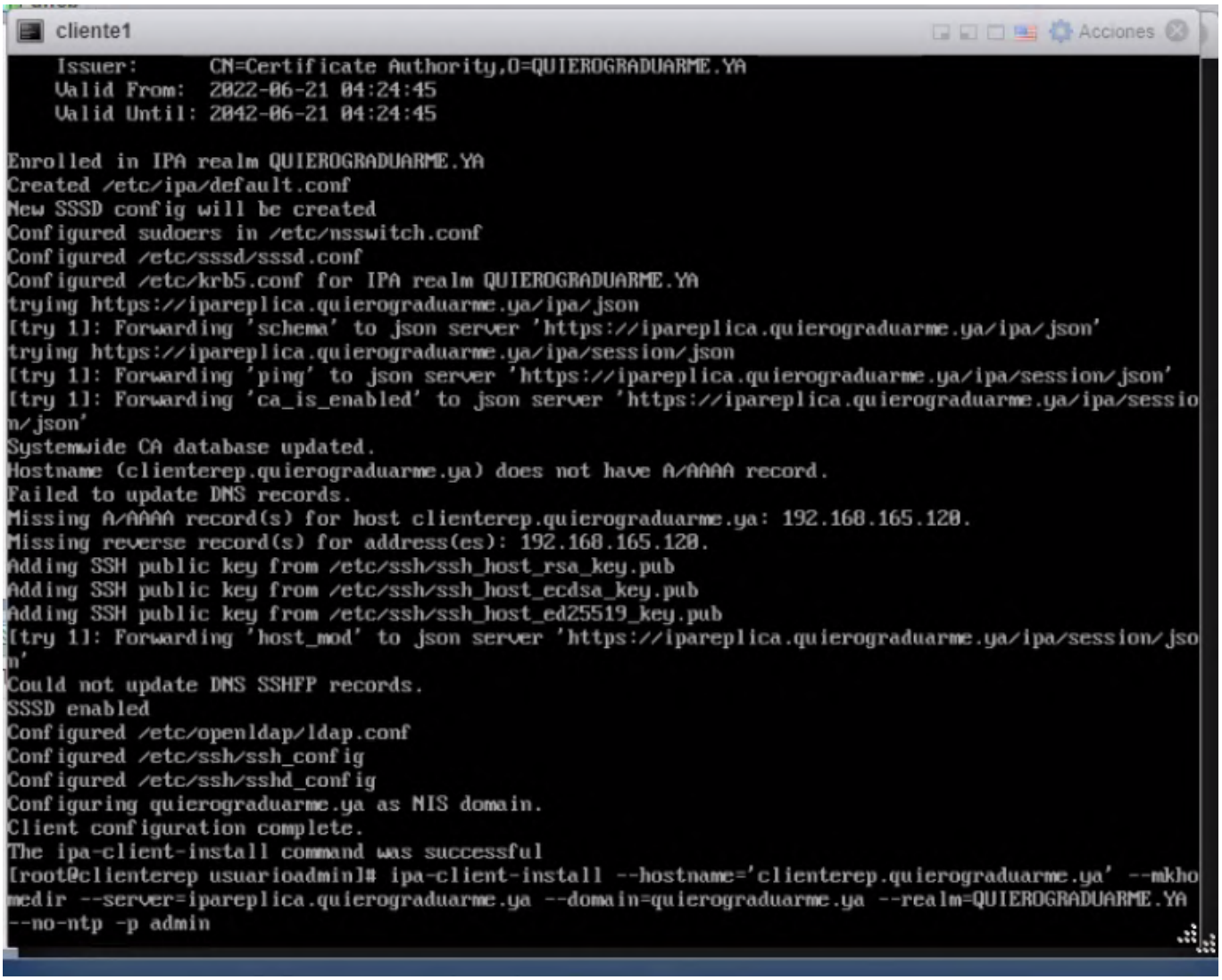
1. Cambie el nombre del cliente en nmtui a su respectivo FQDN como en los pasos anteriores, en este caso, el FQDN será *clienterep.quierograduarme.ya*.

2. Instale el ipa-client con el siguiente comando:

```
sudo yum -y install freeipa-client
```

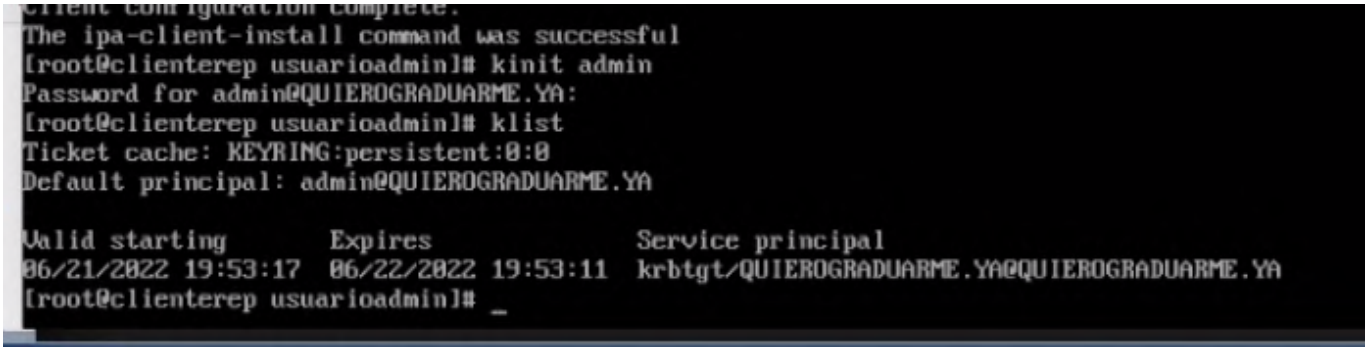
3. Configure el host como cliente de ipa con el siguiente comando:

```
ipa-client-install --hostname='clienterep.quierograduarme.ya' --mkhomedir
--server=ipa1.quierograduarme.ya --domain=quierograduarme.ya
--realm=QUIEROGRADUARME.YA --no-ntp -p admin
```



4. Compruebe que realmente se puede ingresar al FreeIpa mediante el siguiente comando:

```
kinit admin
```



Instalación de la CA en la réplica

Para la instalación de la CA, debemos tomar en cuenta el siguiente mensaje al instalar la réplica el cual indicaba el comando para instalar la CA:

```
Done.
Finalize replication settings
Restarting the KDC

WARNING: The CA service is only installed on one server (ipa1.quierograduarme.ya).
It is strongly recommended to install it on another server.
Run ipa-ca-install(1) on another master to accomplish this.

[root@ipareplica usuarioadmin]# S
```

Este paso es recomendable ejecutarlo justo después de la instalación de la réplica.

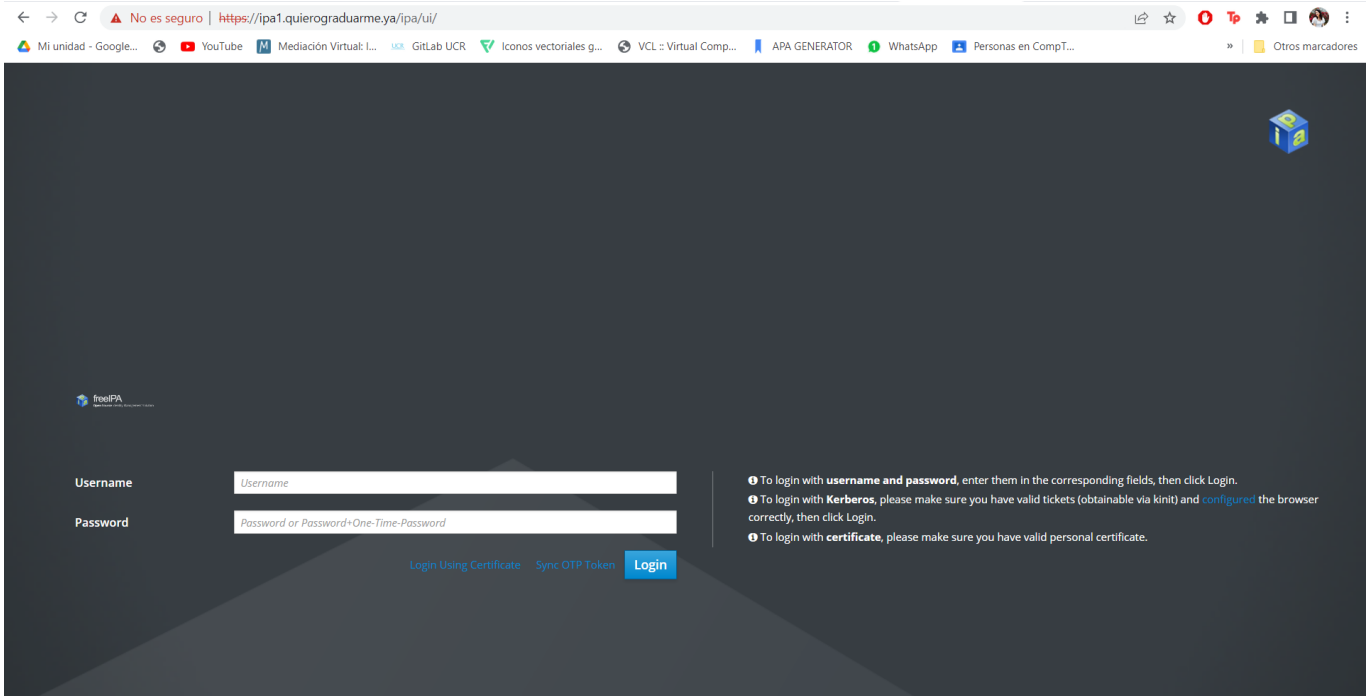
1. Ejecute el siguiente comando:

```
ipa-ca-install
```

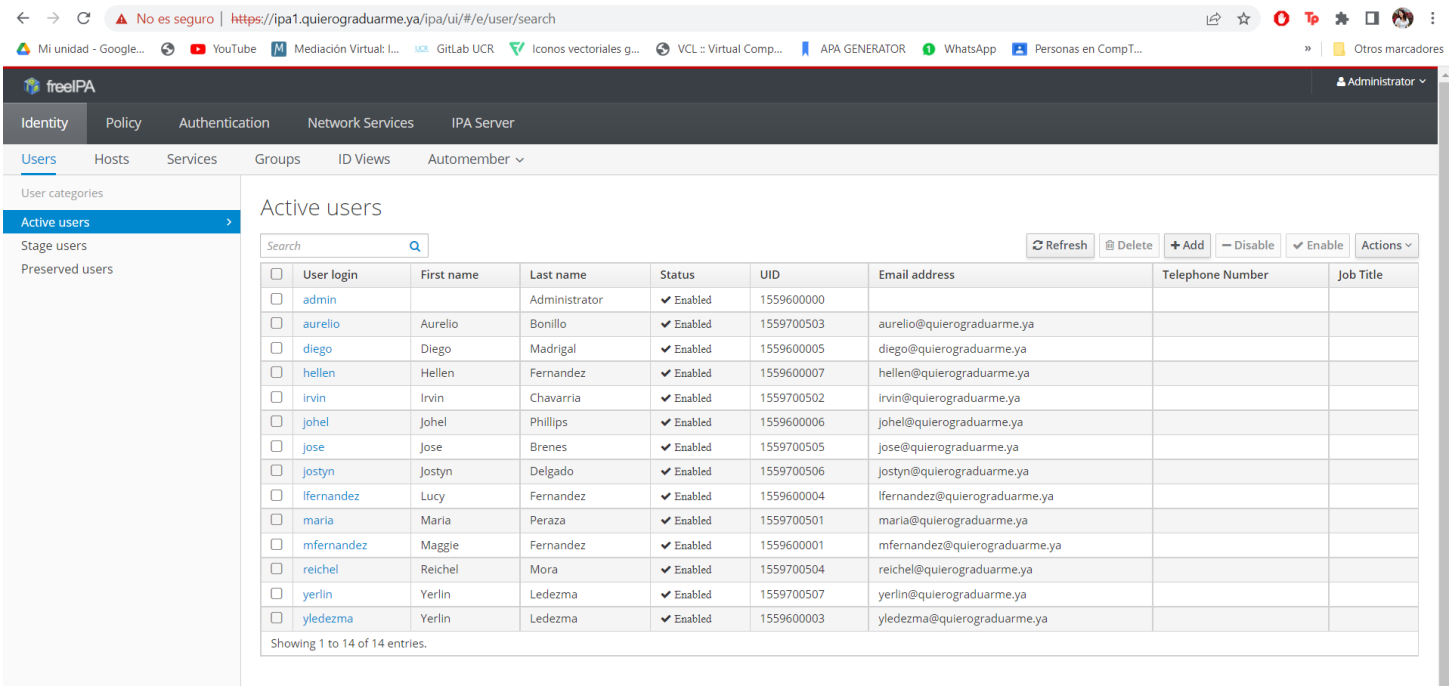
```
root@ipareplica:/home/usuarioadmin
[root@ipareplica usuarioadmin]# ipa-ca-install
Directory Manager (existing master) password:

Run connection check to master
Connection check OK
Configuring certificate server (pki-tomcatd). Estimated time: 3 minutes
  [1/28]: creating certificate server db
  [2/28]: setting up initial replication
Starting replication, please wait until this has completed.
Update in progress, 5 seconds elapsed
Update succeeded

  [3/28]: creating ACIs for admin
  [4/28]: creating installation admin user
  [5/28]: configuring certificate server instance
  [6/28]: secure AJP connector
  [7/28]: reindex attributes
  [8/28]: exporting Dogtag certificate store pin
  [9/28]: stopping certificate server instance to update CS.cfg
  [10/28]: backing up CS.cfg
  [11/28]: disabling nonces
  [12/28]: set up CRL publishing
  [13/28]: enable PKIX certificate path discovery and validation
  [14/28]: destroying installation admin user
  [15/28]: starting certificate server instance
  [16/28]: Finalize replication settings
  [17/28]: setting audit signing renewal to 2 years
  [18/28]: restarting certificate server
  [19/28]: authorizing RA to modify profiles
  [20/28]: authorizing RA to manage lightweight CAs
  [21/28]: Ensure lightweight CAs container exists
  [22/28]: configure certificate renewals
  [23/28]: configure Server-Cert certificate renewal
  [24/28]: Configure HTTP to proxy connections
  [25/28]: restarting certificate server
  [26/28]: updating IPA configuration
  [27/28]: enabling CA instance
  [28/28]: configuring certmonger renewal for lightweight CAs
Done configuring certificate server (pki-tomcatd).
[root@ipareplica usuarioadmin]#
```

FreeIpa Web

1. Se accede al siguiente sitio web y se inicia sesión: https://ipa1.quierograduarme.ya/ipa/ui/



2. Se agregan los usuarios, estos por defecto van a pertenecer al dominio interno que se le asignó el FreeIpa que fue el quierograduarme.ya



Base de datos

Instalación de MariaDB 10.4.25

1. Crear archivo al cual agregar la ruta del repositorio del cual se va a traer la mariadb

```
sudo nano /etc/yum.repos.d/mariadb.repo
```

2. Agregar la siguiente información

```
[mariadb]
name = MariaDB
baseurl = http://yum.mariadb.org/10.4/centos7-amd64
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1
```

3. Instalar la base de datos

```
sudo yum install MariaDB-server -y
```

4. Ejecutar el Script de seguridad

```
mariadb-secure-installation
```

Configuración del script

```
[root@mariadb usuarioadmin]# mariadb-secure-installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

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

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

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

Switch to unix_socket authentication [Y/n] Y
Enabled successfully!
Reloading privilege tables..
 ... Success!


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

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


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

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

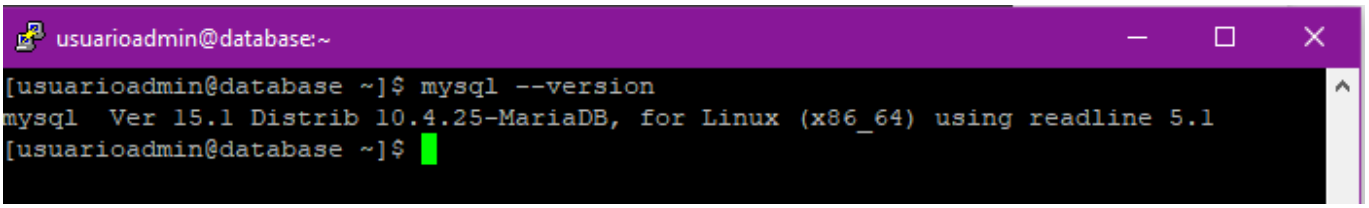
```
Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] n
 ... skipping.

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

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

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

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

Cleaning up...

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

Thanks for using MariaDB!
```

5. Editar el archivo a server.cnf para permitir acceso a la base de datos

```
nano /etc/my.cnf.d/server.cnf
```

```
root@localhost:/etc/my.cnf.d
  GNU nano 2.3.1                                File: server.cnf

#
# These groups are read by MariaDB server.
# Use it for options that only the server (but not clients) should see
#
# See the examples of server my.cnf files in /usr/share/mysql/
#

# this is read by the standalone daemon and embedded servers
[server]

# this is only for the mysqld standalone daemon
[mysqld]

#
# * Galera-related settings
#
[galera]
# Mandatory settings
#wsrep_on=ON
#wsrep_provider=
#wsrep_cluster_address=
#binlog_format=row
#default_storage_engine=InnoDB
#innodb_autoinc_lock_mode=2
#
# Allow server to accept connections on all interfaces.
#
bind-address=0.0.0.0
#
# Optional setting
#wsrep_slave_threads=1
#innodb_flush_log_at_trx_commit=0

# this is only for embedded server
[embedded]

# This group is only read by MariaDB servers, not by MySQL.
# If you use the same .cnf file for MySQL and MariaDB,
# you can put MariaDB-only options here

^G Get Help                ^O WriteOut                ^R Read File
^X Exit                    ^J Justify                 ^W Where Is
```

Versión instalada



Usuario	Contraseña
root	maggielu2.

Servidor web

Instalación de apache

Apache es el servidor http que va a ser utilizado en este caso para que soporte los tres servicios web que se van a brindar desde este servidor. Para instalarlo siga los siguientes pasos:

1. Instale apache con el comando:

```
yum install httpd -y
```

1. Inicie el servicio con el comando:

```
systemctl start httpd
```

1. Habilite la opción de que apache inicie cuando se reinicie la máquina:

```
sudo systemctl enable httpd
```

Instalación de PHP 7.4

Para este paso es importante revisar la versión de php con la que trabajan los distintos servicios web a instalar para que exista una compatibilidad con los tres. En nuestro caso la versión que nos fue conveniente instalar es la 7.4.3 y su instalación se realiza de la siguiente manera:

1. Obtenga la última liberación de php versión 7.

```
# yum install
https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm -y
```

1. Instale el repositorio que cuenta con la versión 7 de PHP:

```
# yum install http://rpms.remirepo.net/enterprise/remi-release-7.rpm -y
```

1. Instale el paquete yum-utils:

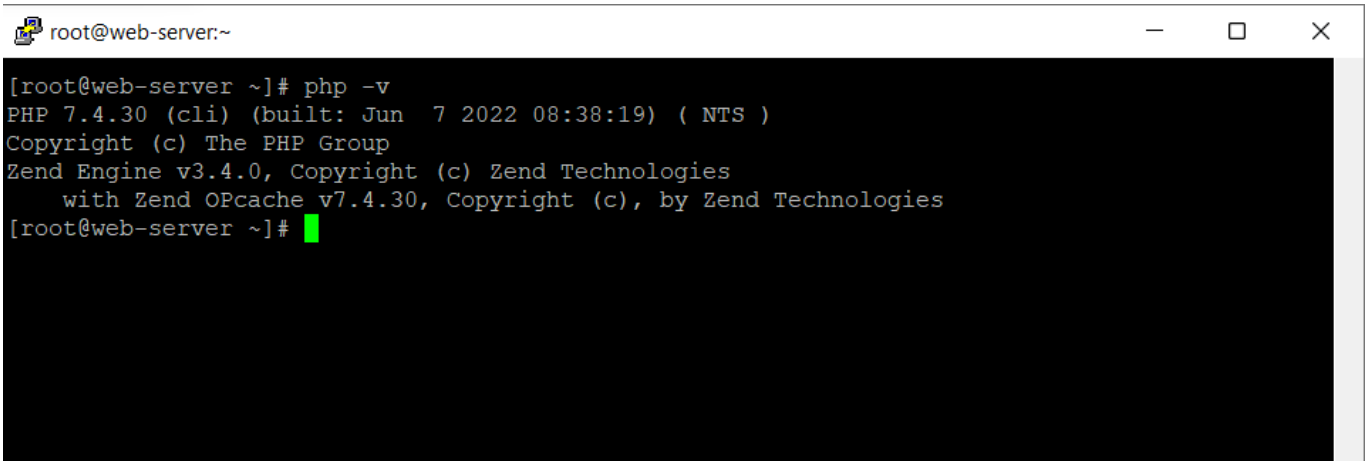
```
# yum install yum-utils
```

1. Habilite el repositorio remi-php74

```
# yum-config-manager --enable remi-php74
```

1. Verifique la versión de PHP instalada:

```
# php -v
```



Instalación de un ERP: Osticket

osTicket es un sistema de emisión de tickets de soporte de código abierto ampliamente utilizado y confiable. Para instalar este servicio de tickets para soporte se realizaron los siguientes pasos:

1. Crear un directorio en el cual se va a alojar la carpeta del servicio de Osticket.

```
sudo mkdir -p /var/www/soporte.quierograduarme.com
```

2. Brindar los permisos de apache sobre la carpeta recién creada y su contenido:

```
sudo chown -R apache:apache /var/www/soporte.quierograduarme.com
```

3. Instalar los siguientes paquetes de php:

```
sudo yum install php php-ctype php-curl php-dom php-filter php-gd php-hash
php-json php-libxml php-mbstring php-openssl php-posix php-session php-simplexml
php-xmlreader php-xmlwriter php-zip php-zlib php-pdo_mysql php-fileinfo php-bz2
php-intl -y
```

4. Descargar y descomprimir la versión v1.15.1 de osticket (Para que tenga compatibilidad con el php descargado)

```
sudo wget
https://github.com/osTicket/osTicket/releases/download/v1.15.1/osTicket-v1.15.8.zi
p
```

```
sudo unzip osTicket-v1.15.1.zip -d osticket
```

5. Copiar el archivo ost-sampleconfig.php en la siguiente ruta, de manera que reemplace el archivo ost-config.php .

```
sudo cp
/var/www/soporte.quierograduarme.com/osticket/upload/include/ost-sampleconfig.php
/var/www/soporte.quierograduarme.com/osticket/upload/include/ost-config.php
```

6. Otorgarle la propiedad y permisos a apache para que se pueda acceder a la carpeta:

```
sudo chown -R apache:apache /var/www/soporte.quierograduarme.com
sudo chmod -R 775 /var/www/soporte.quierograduarme.com
sudo chmod -R 755 /var/www
```

7. Crear el archivo de virtual host y agregar la siguiente configuración:

```
sudo nano /etc/httpd/conf.d/soporte.quierograduarme.com.conf
```

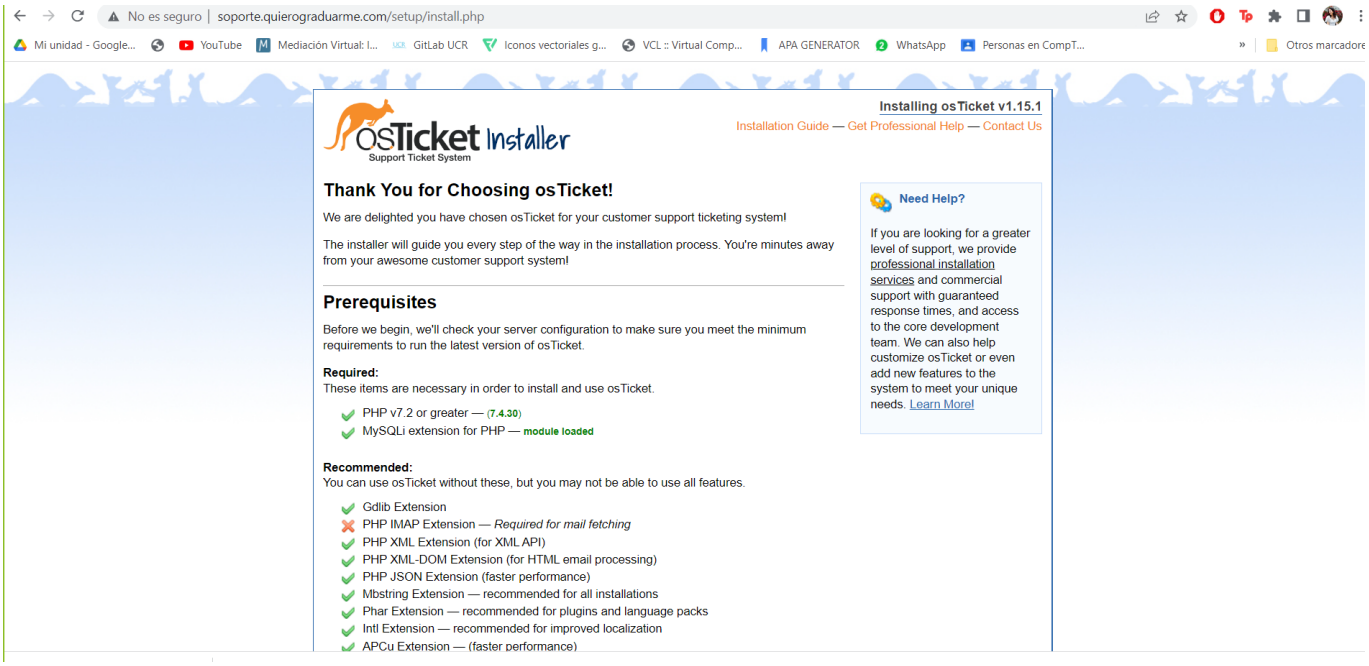
```
<VirtualHost *:80>
    ServerName soporte.quierograduarme.com
    ServerAlias www.soporte.quierograduarme.com

    DirectoryIndex index.php index.html
    DocumentRoot /var/www/soporte.quierograduarme.com/osticket/upload

    ErrorLog /var/log/httpd/soporte.quierograduarme.com-error.log
    CustomLog /var/log/httpd/soporte.quierograduarme.com-access.log common

    <Directory /var/www/soporte.quierograduarme.com/osticket>
        Options FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

8. Reiniciar apache:

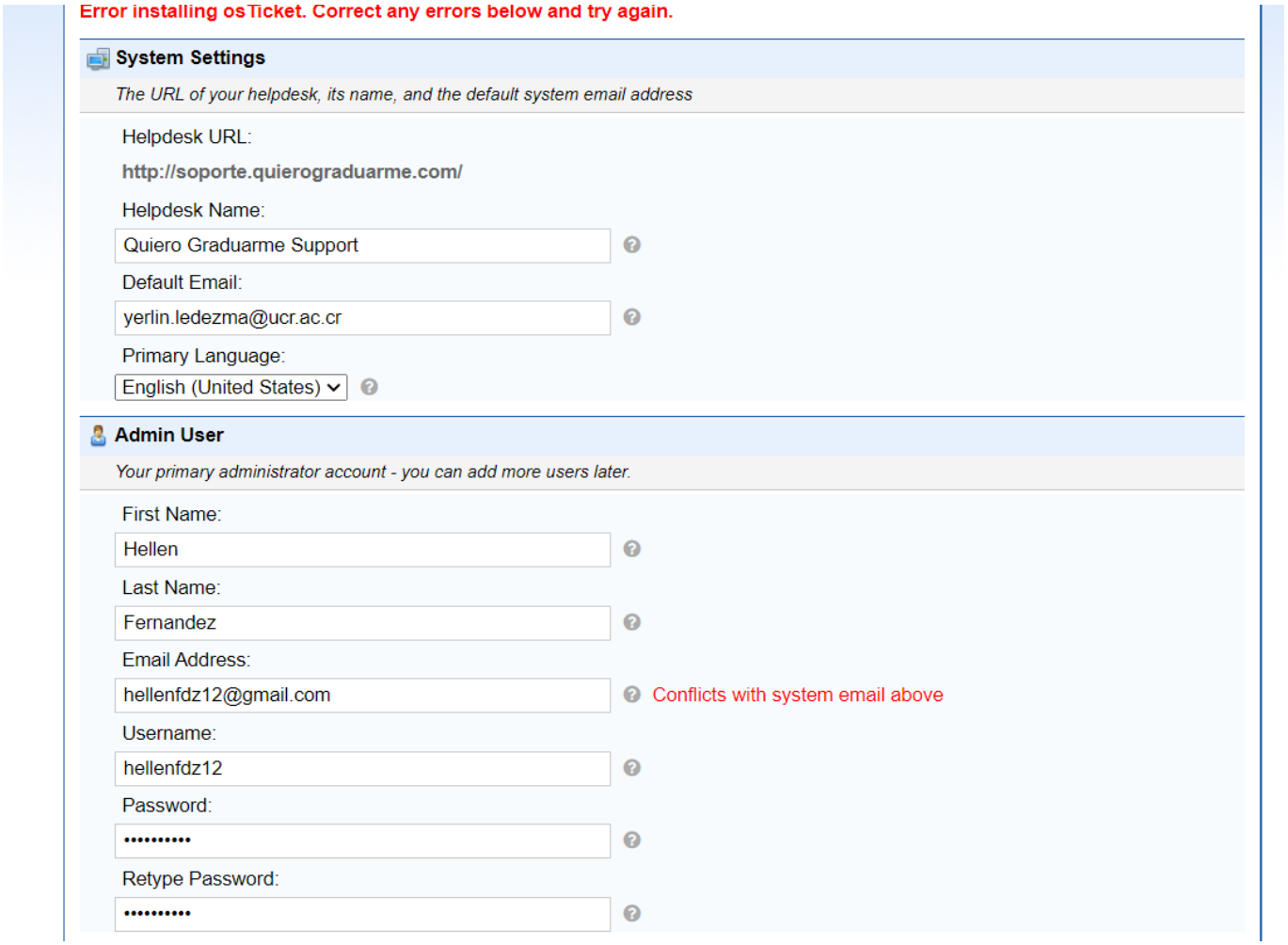
```
sudo systemctl restart httpd
```

Instalación web

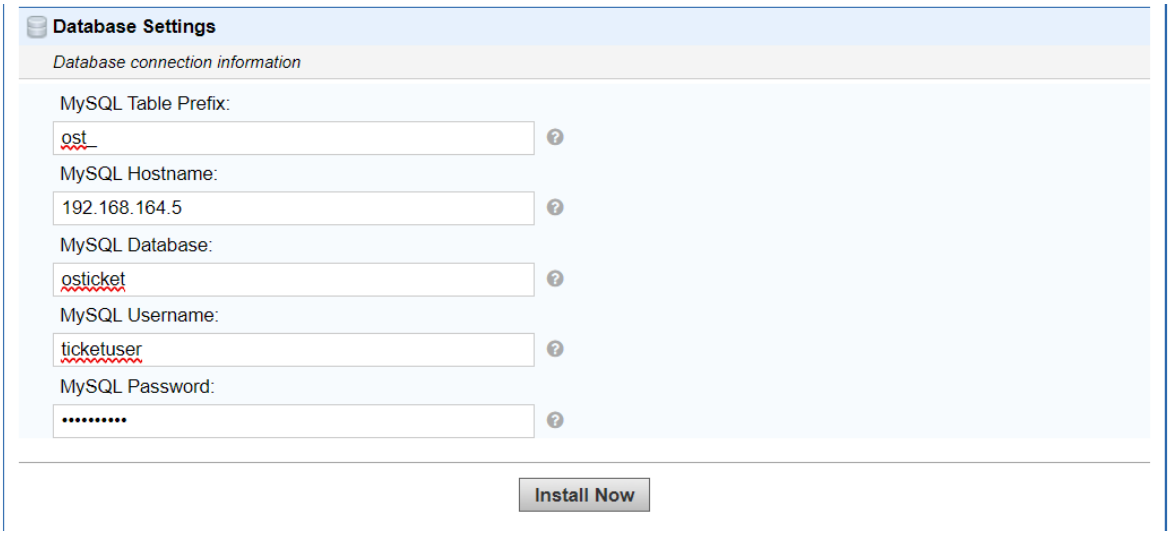
1. Ingresar al sitio web: soporte.quierograduarme.com, debería de salir la siguiente página, en la cual se deben cumplir con los requisitos. Se le da click en next hacia al siguiente paso:



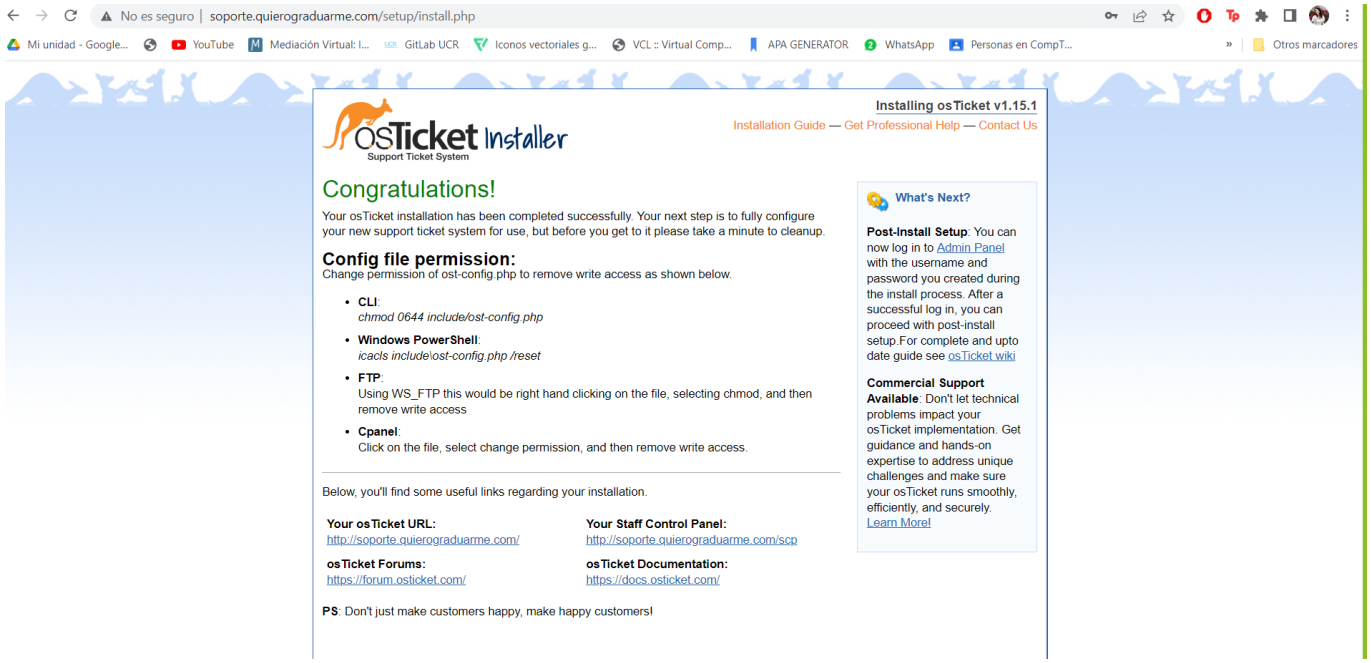
2. El siguiente paso es especificar el correo del sistema y el correo del administrador



3. Se agrega la información de la base de datos como: la ip, el nombre de la base de datos, el usuario y la contraseña



Si la configuración fue exitosa se mostrará la siguiente pantalla:



Instalación LDAP

Para utilizar LDAP es necesario instalar el plugin LDAP Authentication and lookup

1. Acceder a la carpeta creada para el servicio de soporte

```
cd /var/www/soporte.quierograduarme.com/
```

2. Clonar el repositorio de plugins

```
sudo git clone https://github.com/osTicket/osTicket-plugins.git
```

3. Acceder a la carpeta de plugins

```
cd ./osTicket-plugins/
```

4. Hidratar el repositorio descargando las dependencias de la biblioteca de terceros

```
sudo php make.php hydrate
```

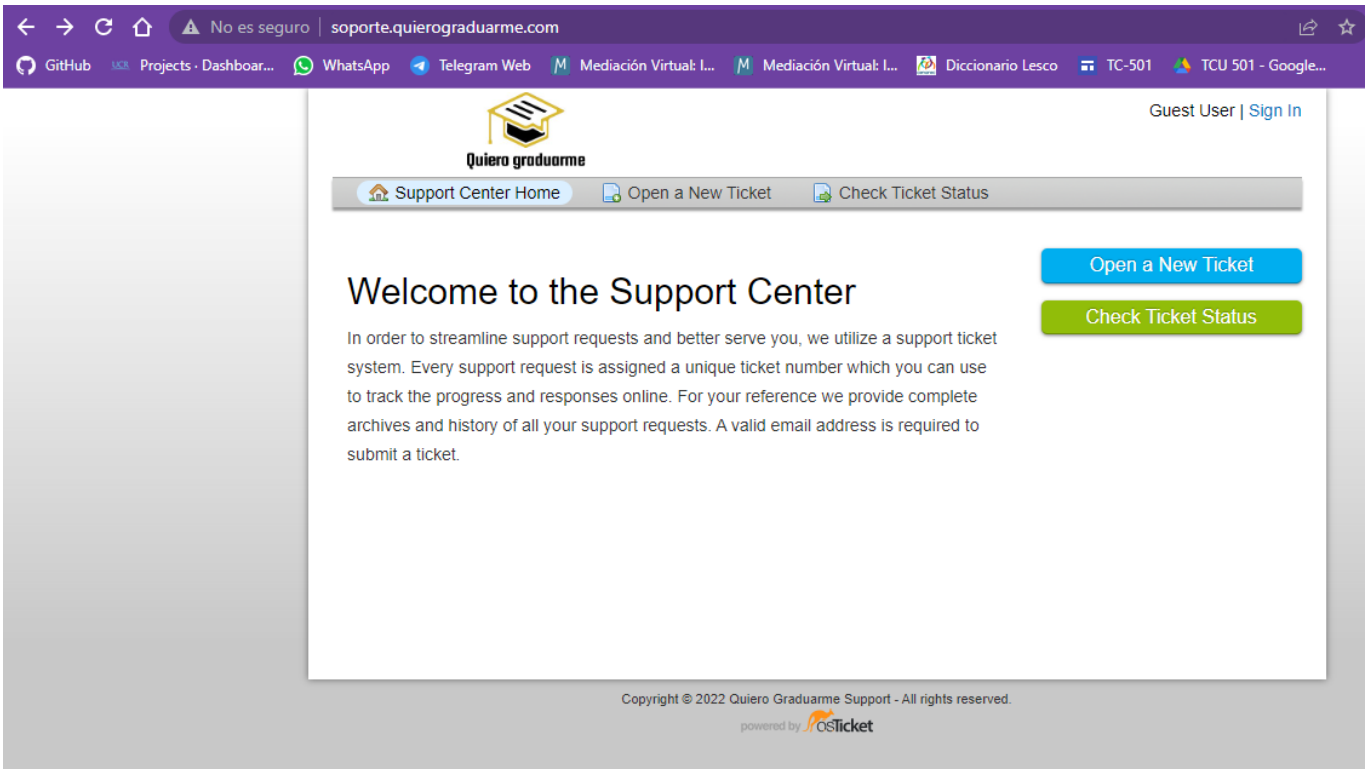
5. Construir los plugins

```
sudo php -dphar.readonly=0 make.php build auth-ldap
```

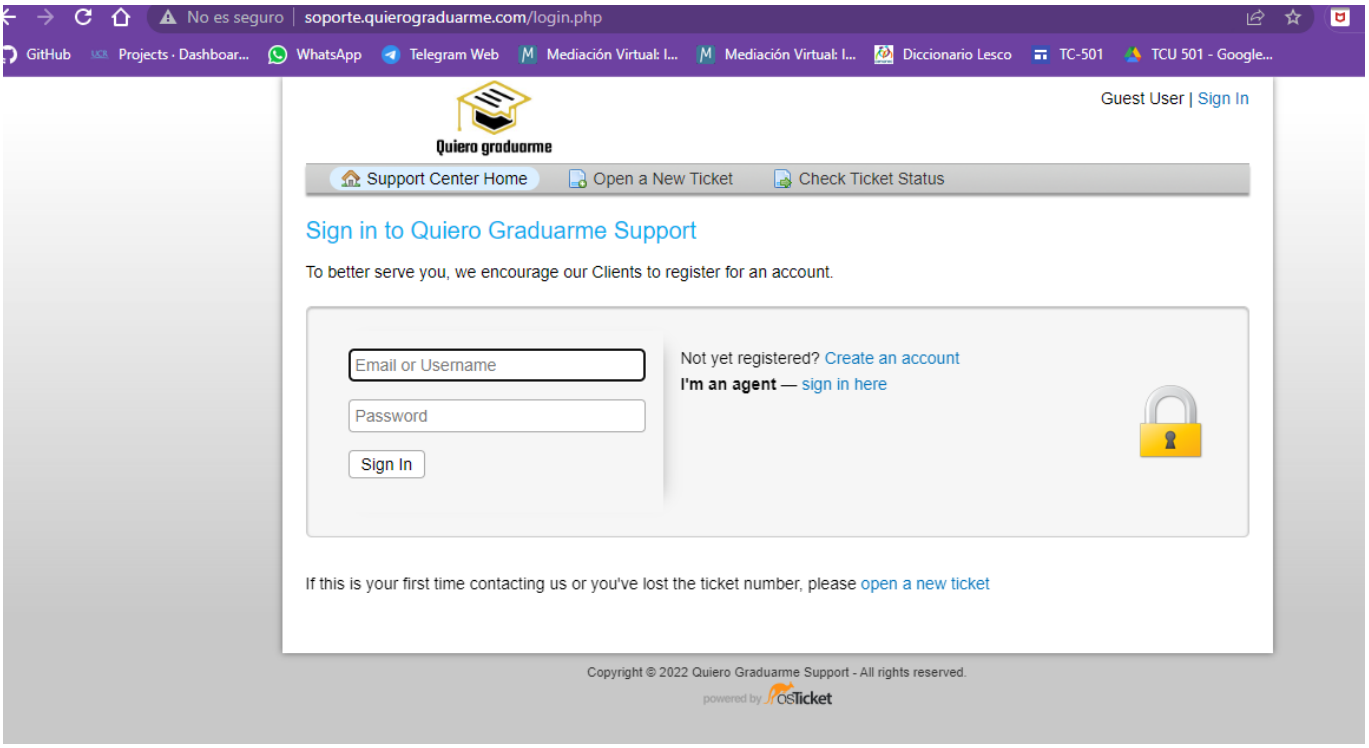
6. Mover el plugin a la la carpeta de plugins de ostickets

```
sudo mv /var/www/soporte.quierograduarme.com/osTicket-plugins/auth-ldap.phar
/var/www/soporte.quierograduarme.com/osticket/upload/include/plugins/auth-ldap.pha
r
```

7. Acceder nuevamente al sitio web: soporte.quierograduarme.com, presionar donde dice *sign in*.



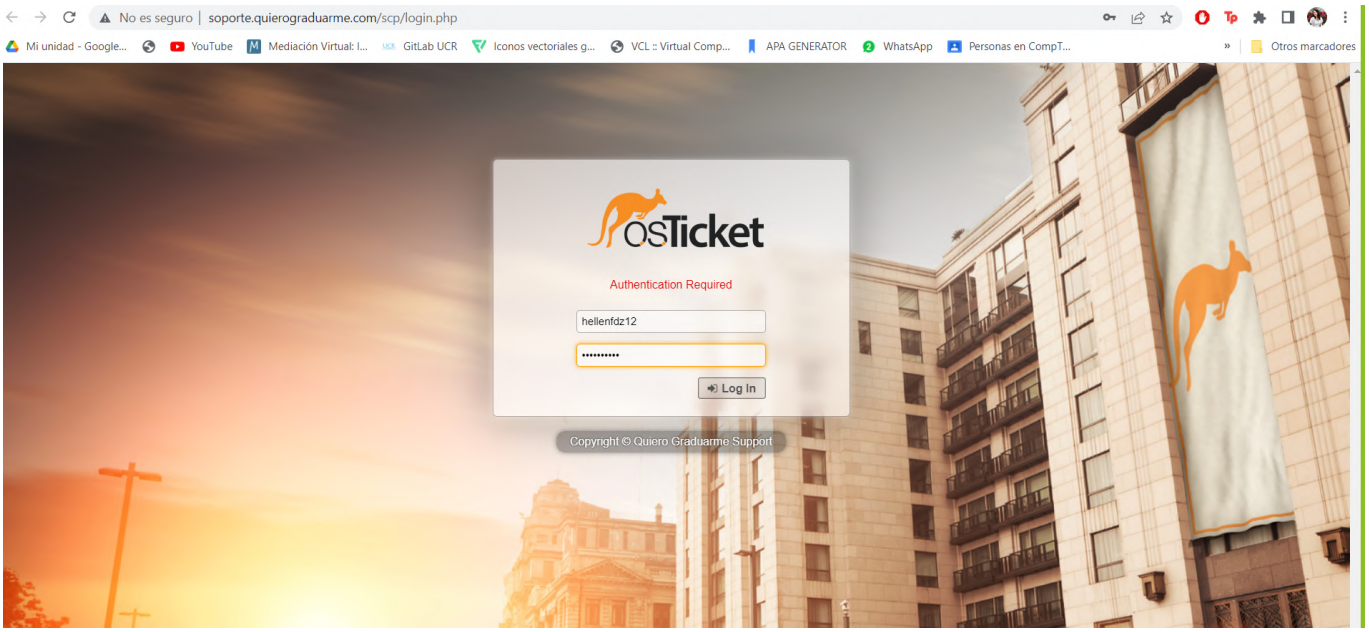
8. Para registrarse como administrador, presionar *sign in here* al lado de *I'm an agent*



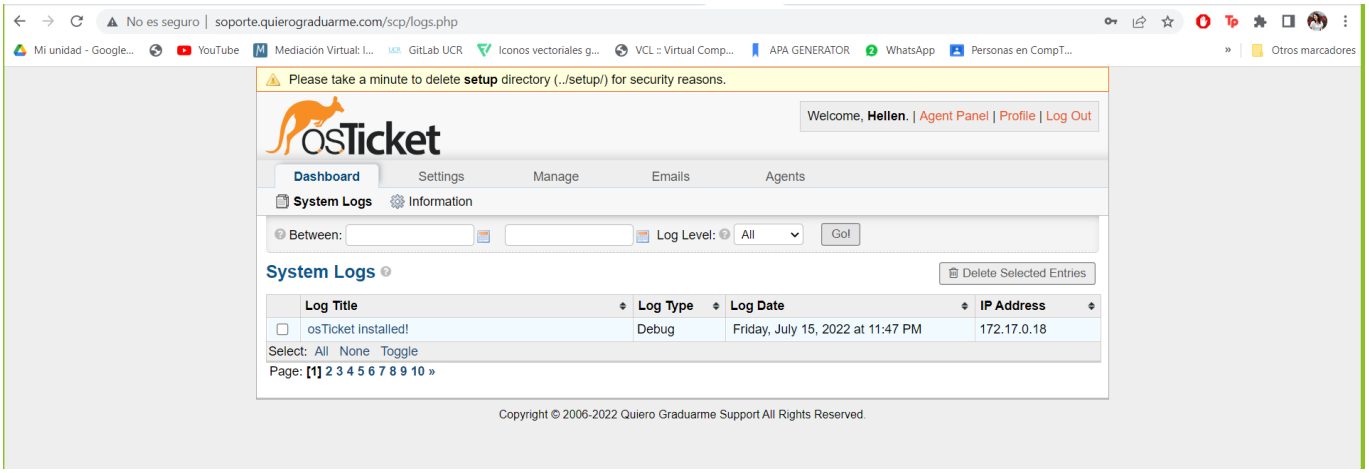
9. Para registrarse se usan las credenciales de administrador:

Usuario: hellenfdz12

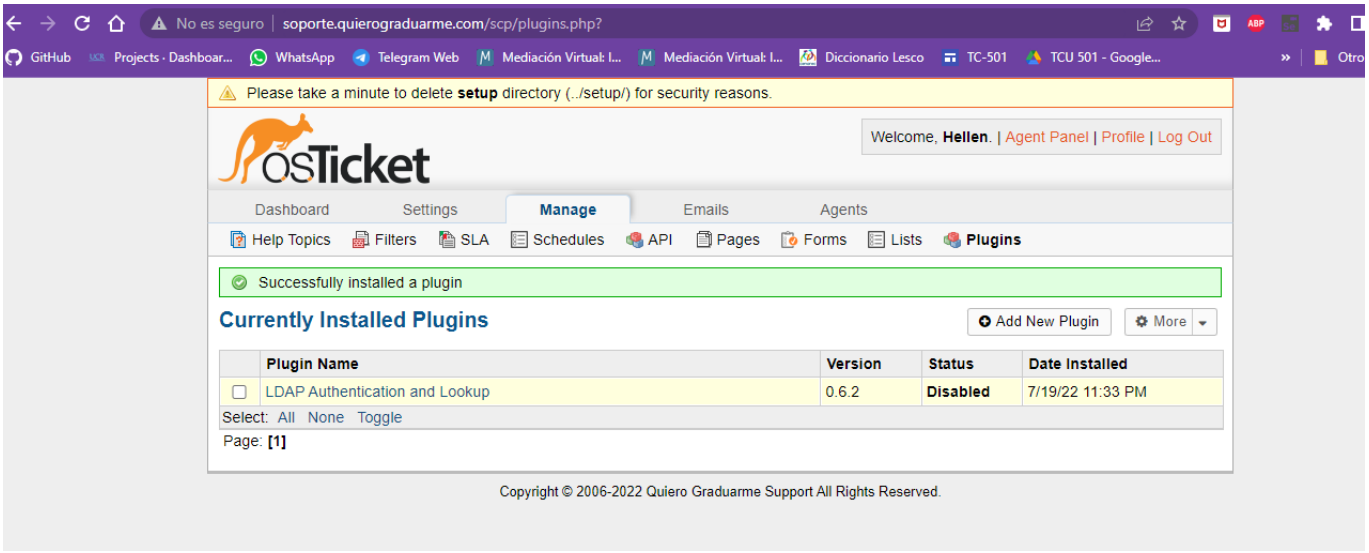
Contraseña: maggielu2.



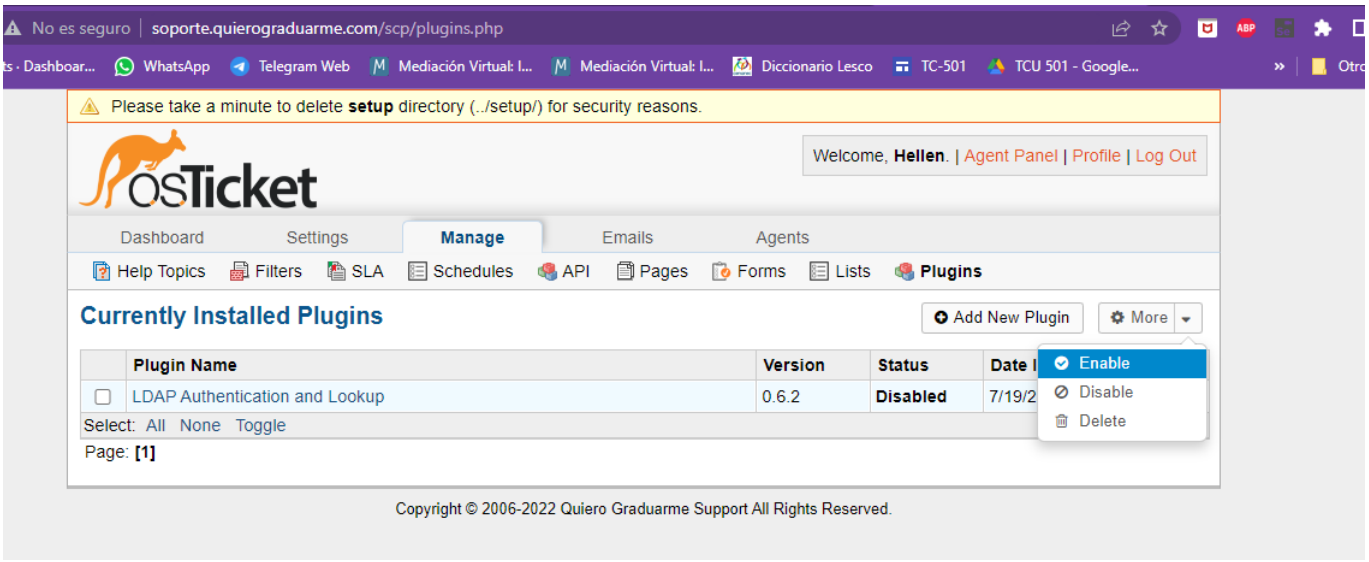
10. Acceder a *Agent Panel*

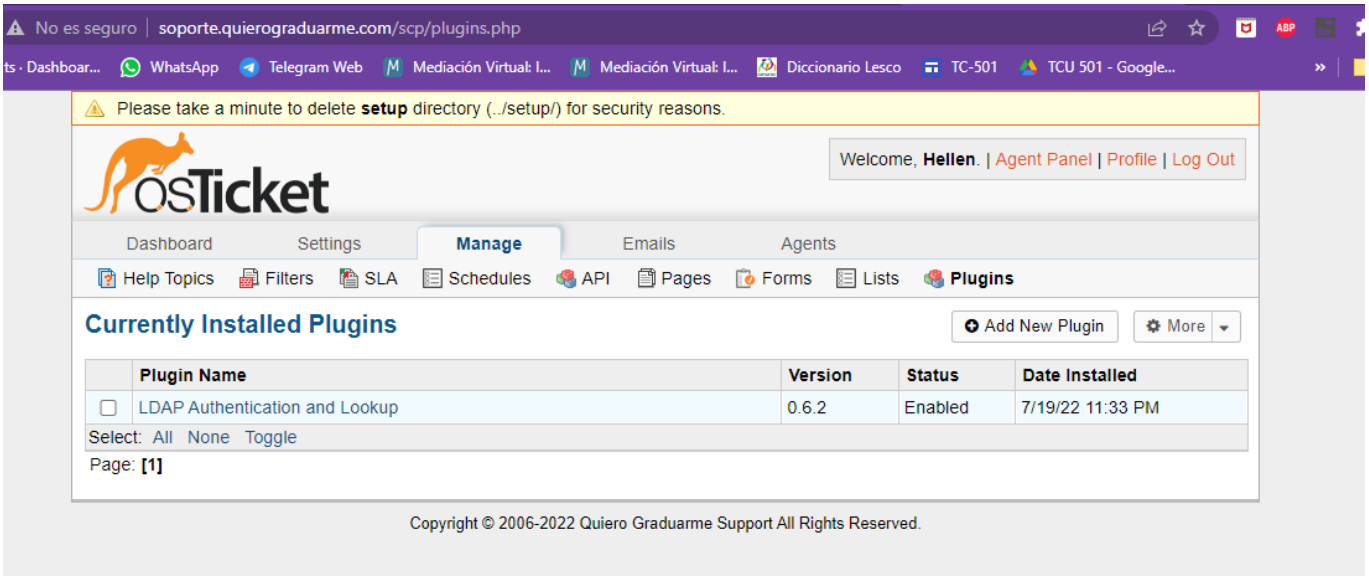


11. Instalar el plugin



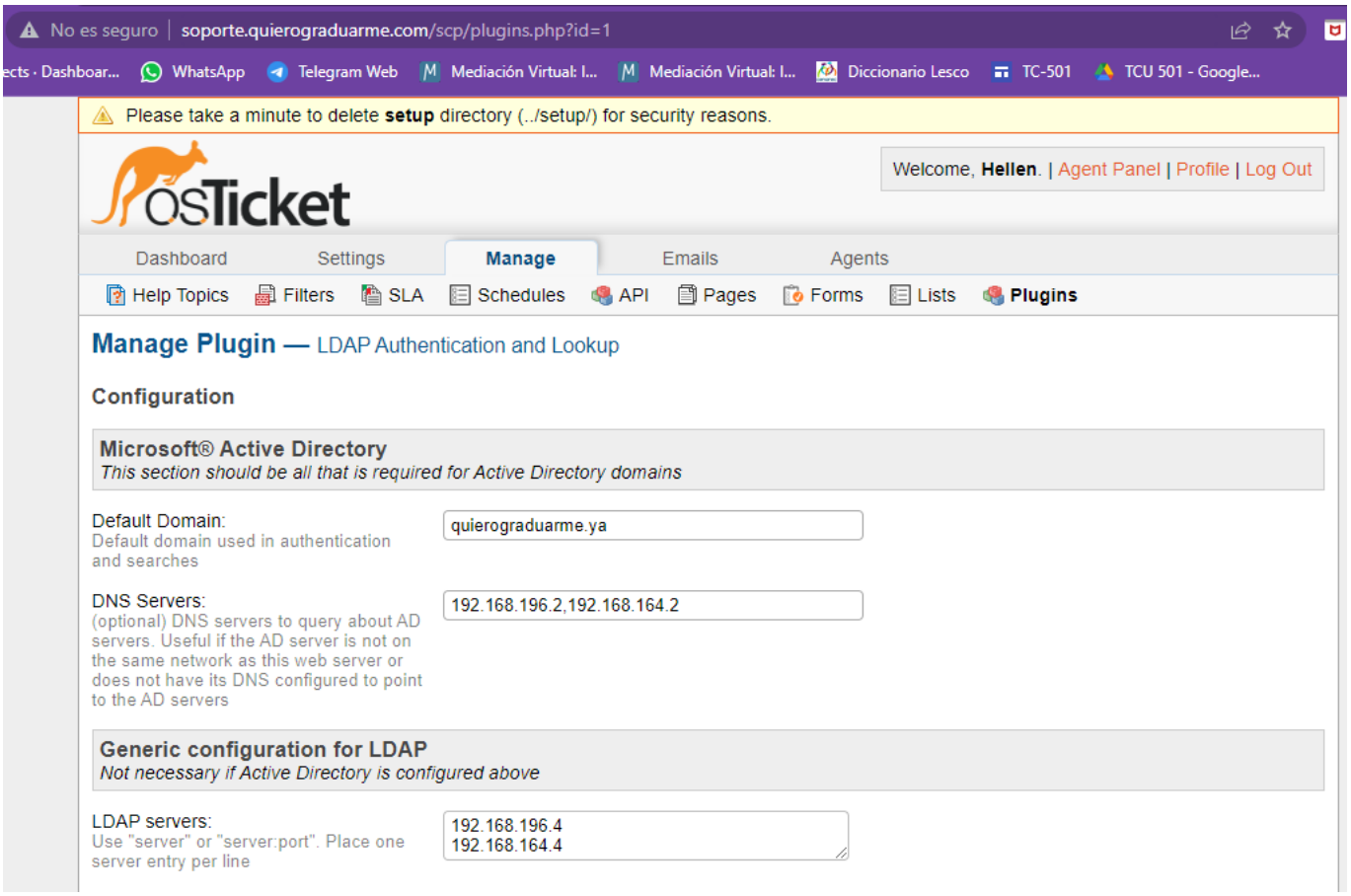
12. Habilitar el plugin

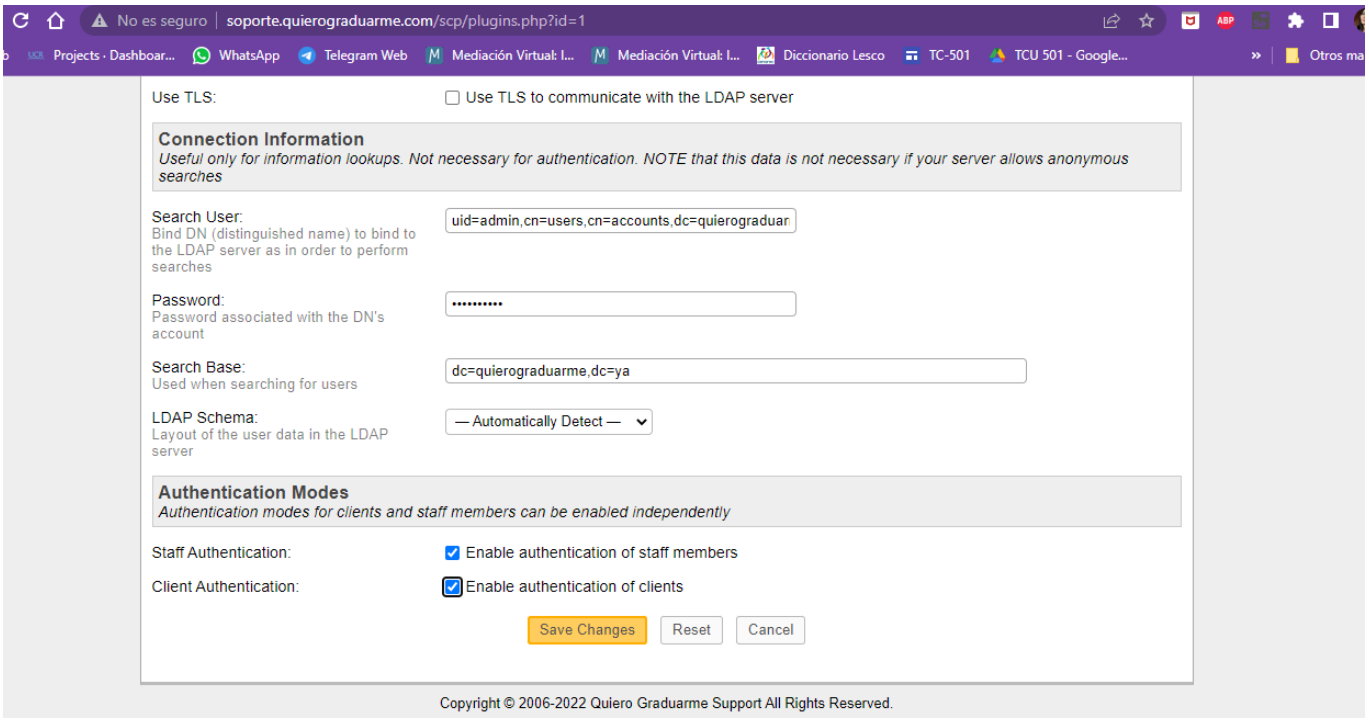




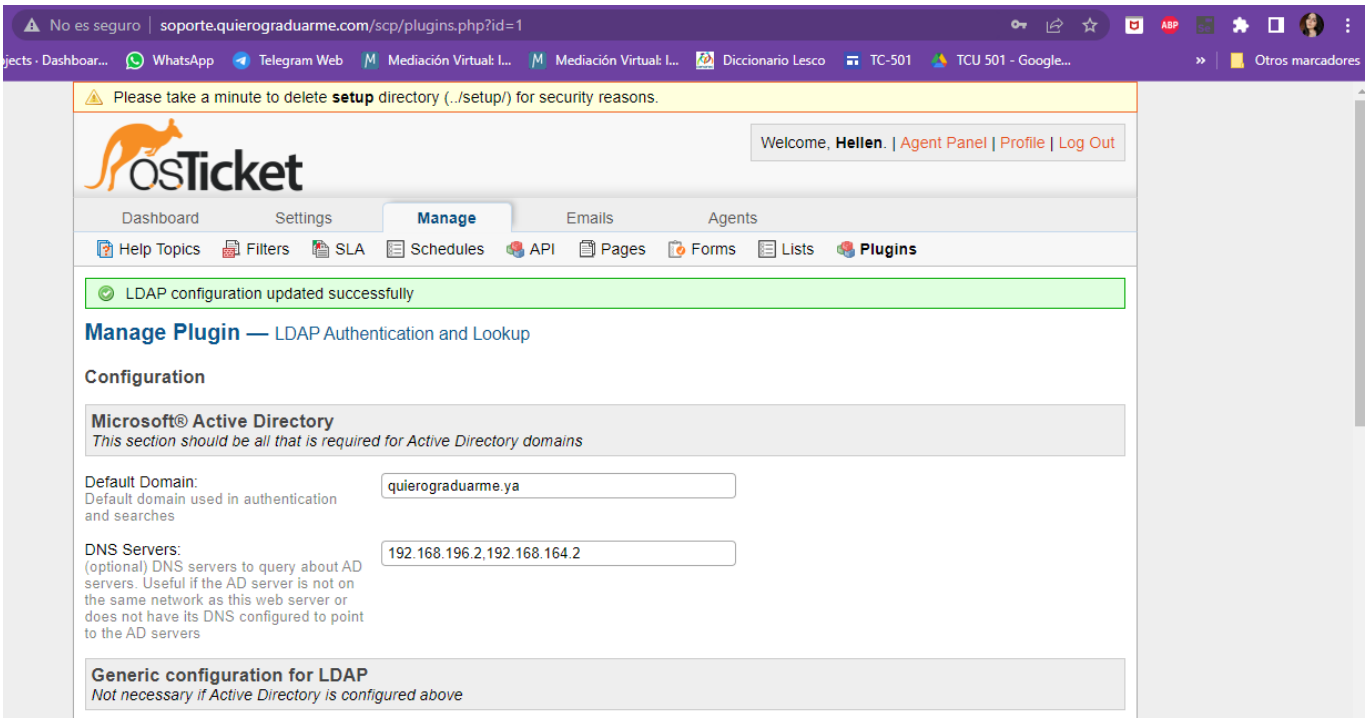
13. Presionar sobre el nombre del plugin para acceder a la configuración agregar la siguiente información, habilitar que los clientes y el staff se puedan autenticar y guardar los cambios:

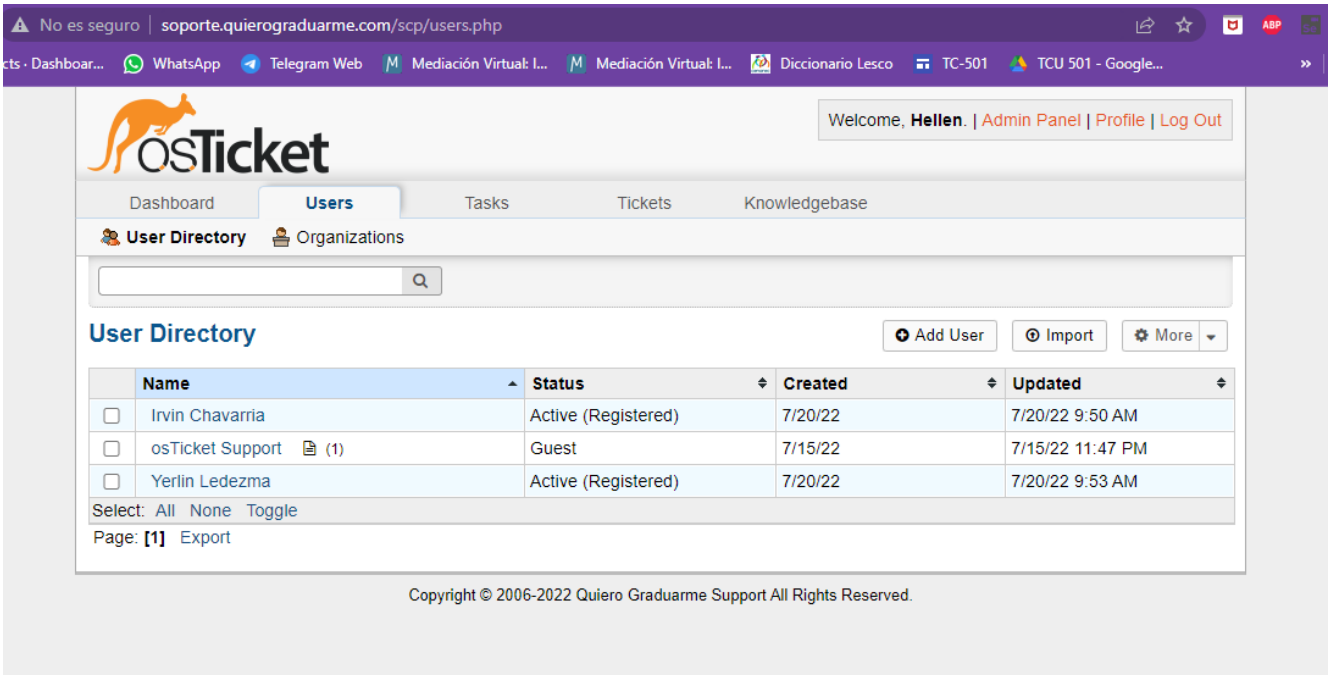
```
Default Domain: quierograduarme.ya
DNS Servers: 192.168.196.2, 192.168.164.2
LDAP Servers: 192.168.196.4
              192.168.164.4
Search User: uid=admin,cn=user,cn=accounts,dc=quierograduarme,dc=ya
Password: maggielu2.
Search Base:  dc=quierograduarme,dc=ya
```





Si la configuración fue exitosa verá el siguiente mensaje:





Instalación de un servicio de aprendizaje en línea: Moodle

Moodle es una plataforma de aprendizaje diseñada para proporcionar a educadores, administradores y estudiantes un sistema integrado único, robusto y seguro para crear ambientes de aprendizaje personalizados. Para instalar este servicio web se deben de seguir los siguientes pasos:

1. Crear dos carpetas, una para almacenar a moodle y otra para los datos que van a almacenarse en la base de datos.

```
sudo mkdir -p /var/www/aula.quierograduarme.com
sudo mkdir -p /var/www/aula.quierograduarme.com/moodledata
```

2. Brindar los permisos necesarios a las carpetas para que apache los pueda leer:

```
sudo chown -R apache:apache /var/www/aula.quierograduarme.com/moodledata
sudo chmod -R 775 /var/www/aula.quierograduarme.com/moodledata
sudo chmod -R 775 /var/www/aula.quierograduarme.com
```

3. Crear el archivo de virtual hosts con la configuración

```
sudo nano /etc/httpd/conf.d/aula.quierograduarme.com.conf
```

```
<VirtualHost *:80>
    ServerName aula.quierograduarme.com
    ServerAlias www.aula.quierograduarme.com

    DirectoryIndex index.html index.php
    DocumentRoot /var/www/aula.quierograduarme.com/moodle/

    ErrorLog /var/log/httpd/aula.quierograduarme.com-error.log
    CustomLog /var/log/httpd/aula.quierograduarme.com-access.log common

    <Directory /var/www/aula.quierograduarme.com/moodle>
        Options FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

4. Instalar moodle:

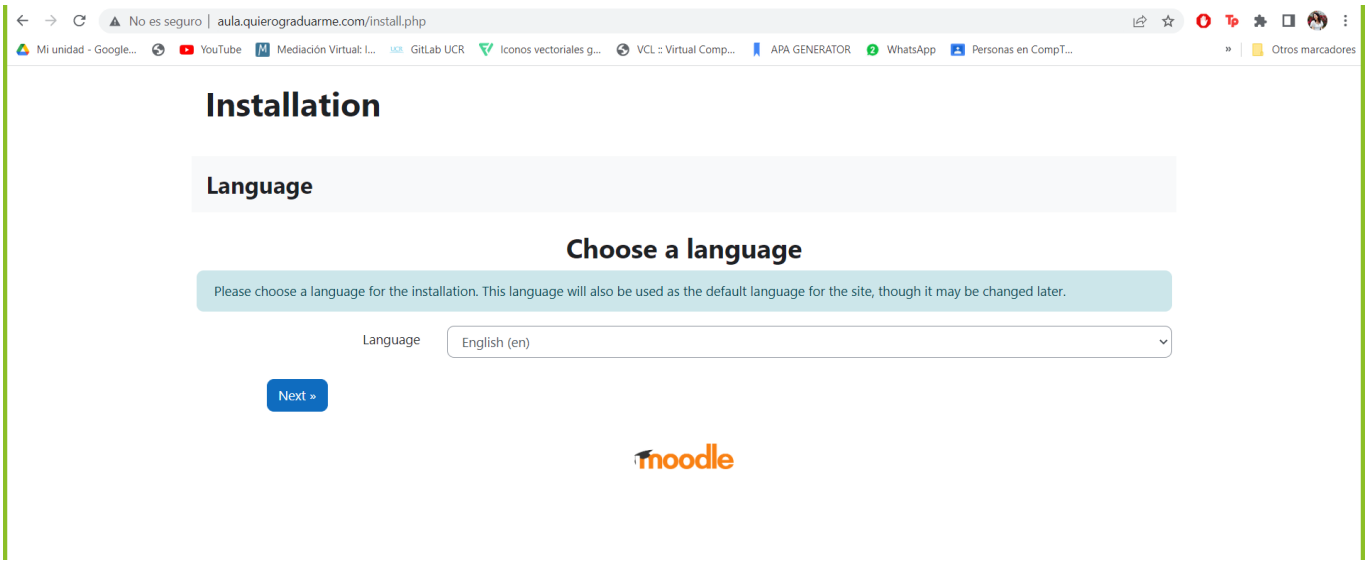
```
sudo wget
https://download.moodle.org/download.php/direct/stable400/moodle-4.0.2.tgz
sudo tar -xvzf moodle-4.0.2.tgz -C /var/www/aula.unixmen.bo
```

5. Reinicie el servidor web:

```
sudo systemctl restart httpd
```

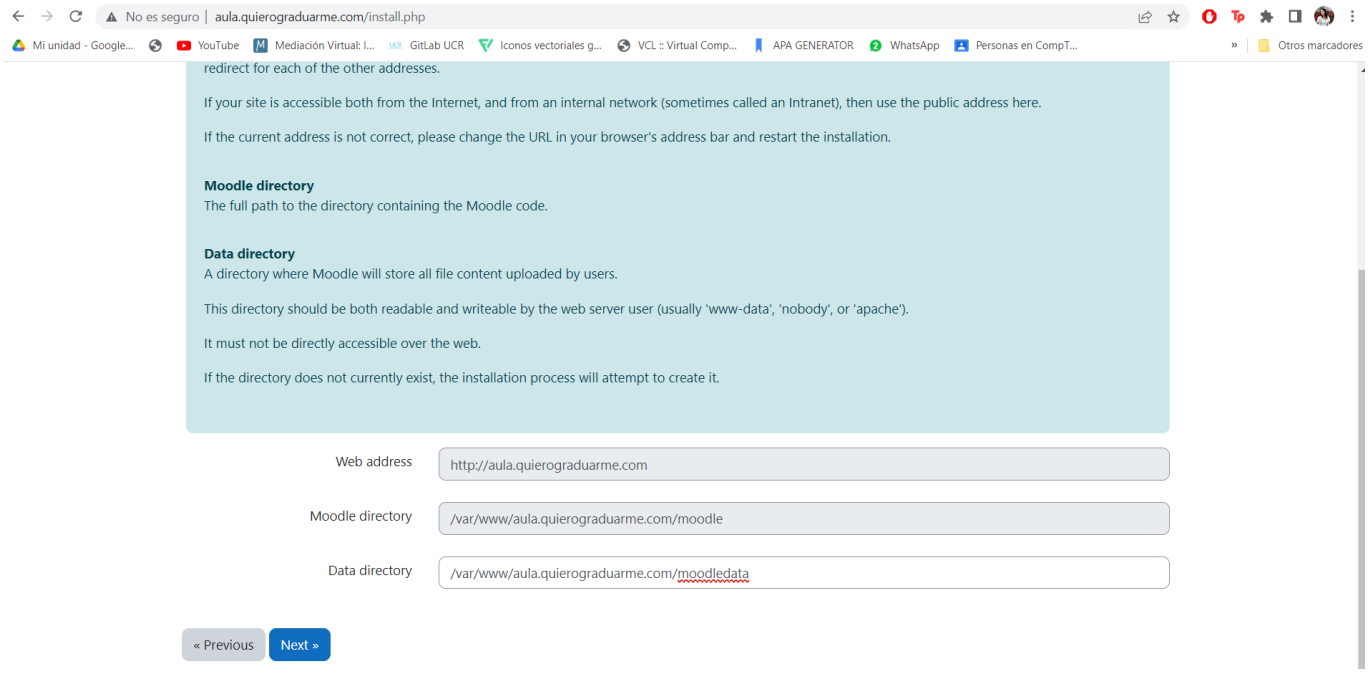
Instalación web

1. Ingresar al sitio web: aula.quierograduarme.com, en la primera pantalla le van a solicitar seleccionar el idioma

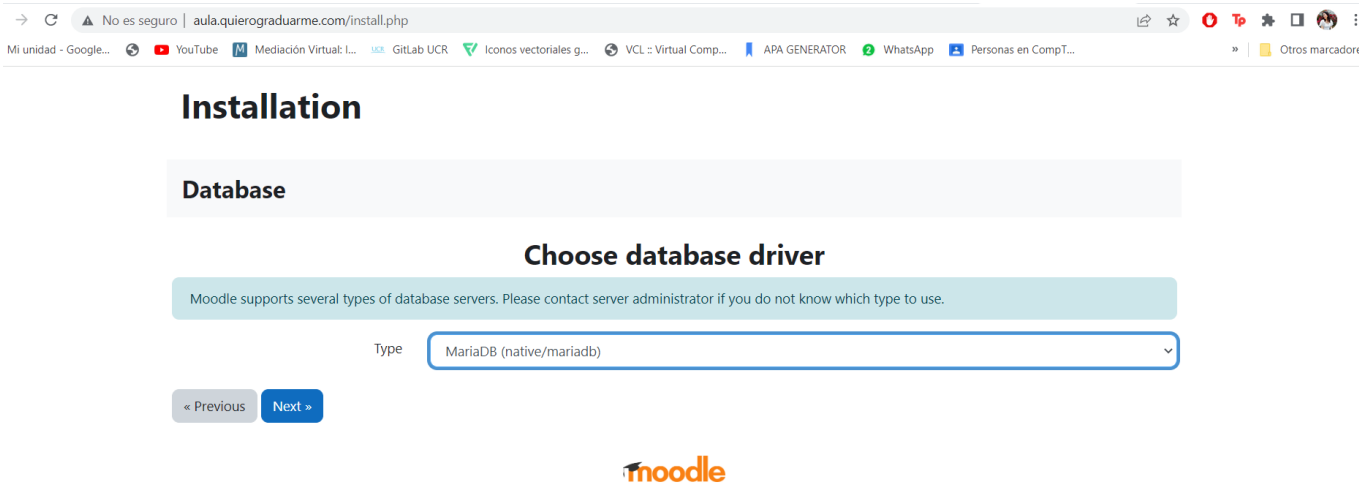


2. Agregar la dirección web, el directorio de moodle y el directorio de los datos de moodle

Web address: http://aula.quierograduarme.com
Moodle directory: /var/www/aula.quierograduarme.com/moodle
Data directory: /var/www/aula.quierograduarme.com/moodledata

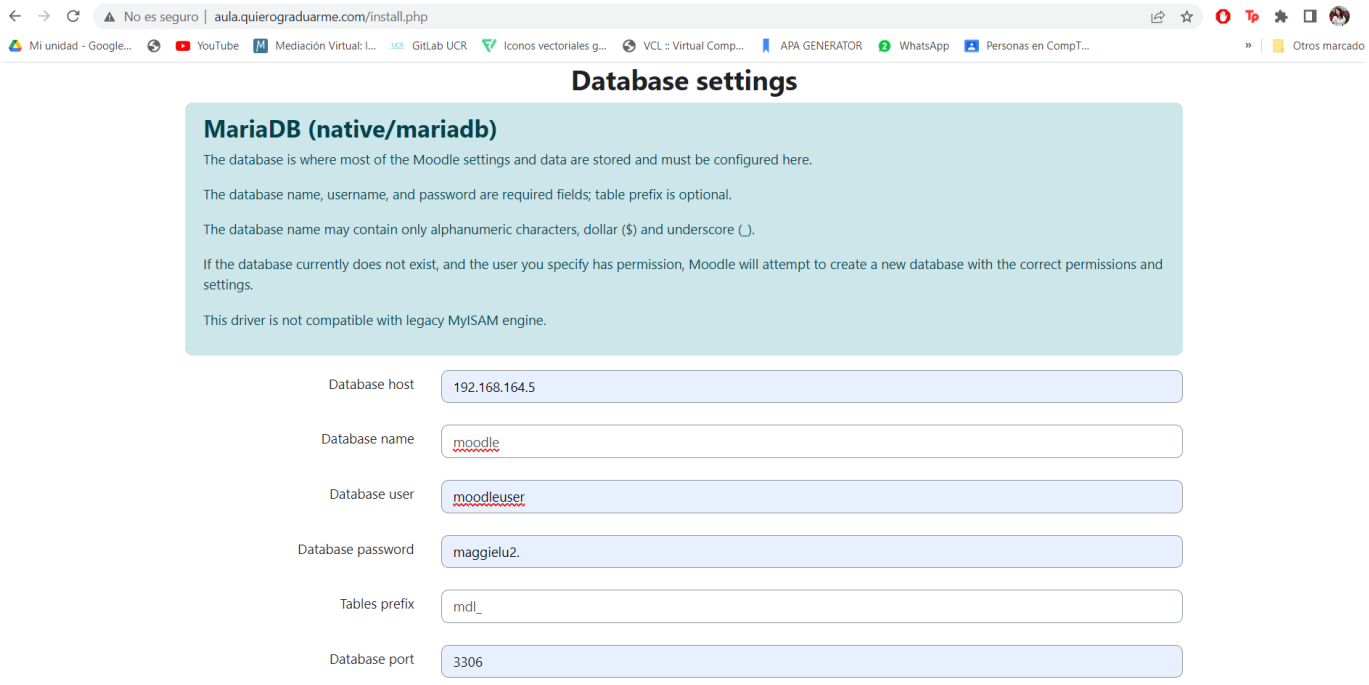


3. Especificar el driver de la base de datos

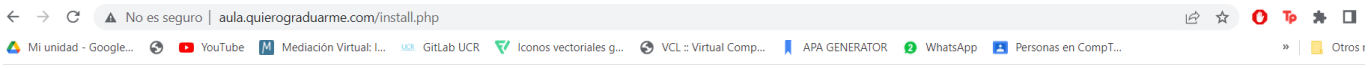


4. Agregar la configuración de la base de datos

```
Database host: 192.168.164.5
Database name: moodle
Database user: moodleuser
Database password: maggielu2.
Tables prefix: mdl_
Database port: 3306
```



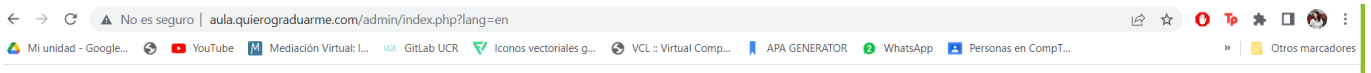
5. Una vez que la configuración ha sido completada observarán las siguientes pantalla, presionar en continuar



Configuration completed

Moodle made an attempt to save your configuration in a file in the root of your Moodle installation.The installer script was not able to automatically create a config.php file containing your chosen settings, probably because the Moodle directory is not writeable. You can manually copy the following code into a file named config.php within the root directory of Moodle.

```
<?php  // Moodle configuration file

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype    = 'mariadb';
$CFG->dblibrary = 'native';
$CFG->dbhost    = '192.168.164.5';
$CFG->dbname    = 'moodle';
$CFG->dbuser    = 'moodleuser';
$CFG->dbpass    = 'maggielu2.';
$CFG->prefix    = 'mdl_';
$CFG->dboptions = array (
  'dbpersist' => 0,
  'dbport' => 3306,
  'dbsocket' => '',
  'dbcollation' => 'utf8mb4_general_ci',
);

$CFG->wwwroot   = 'http://aula.quierograduarme.com';
$CFG->dataroot  = '/var/www/aula.quierograduarme.com/moodledata';
$CFG->admin     = 'admin';

$CFG->directorypermissions = 0777;

require_once(__DIR__ . '/lib/setup.php');
```



Installation

Moodle - Modular Object-Oriented Dynamic Learning Environment

Copyright notice

Copyright (C) 1999 onwards Martin Dougiamas (https://moodle.com)

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

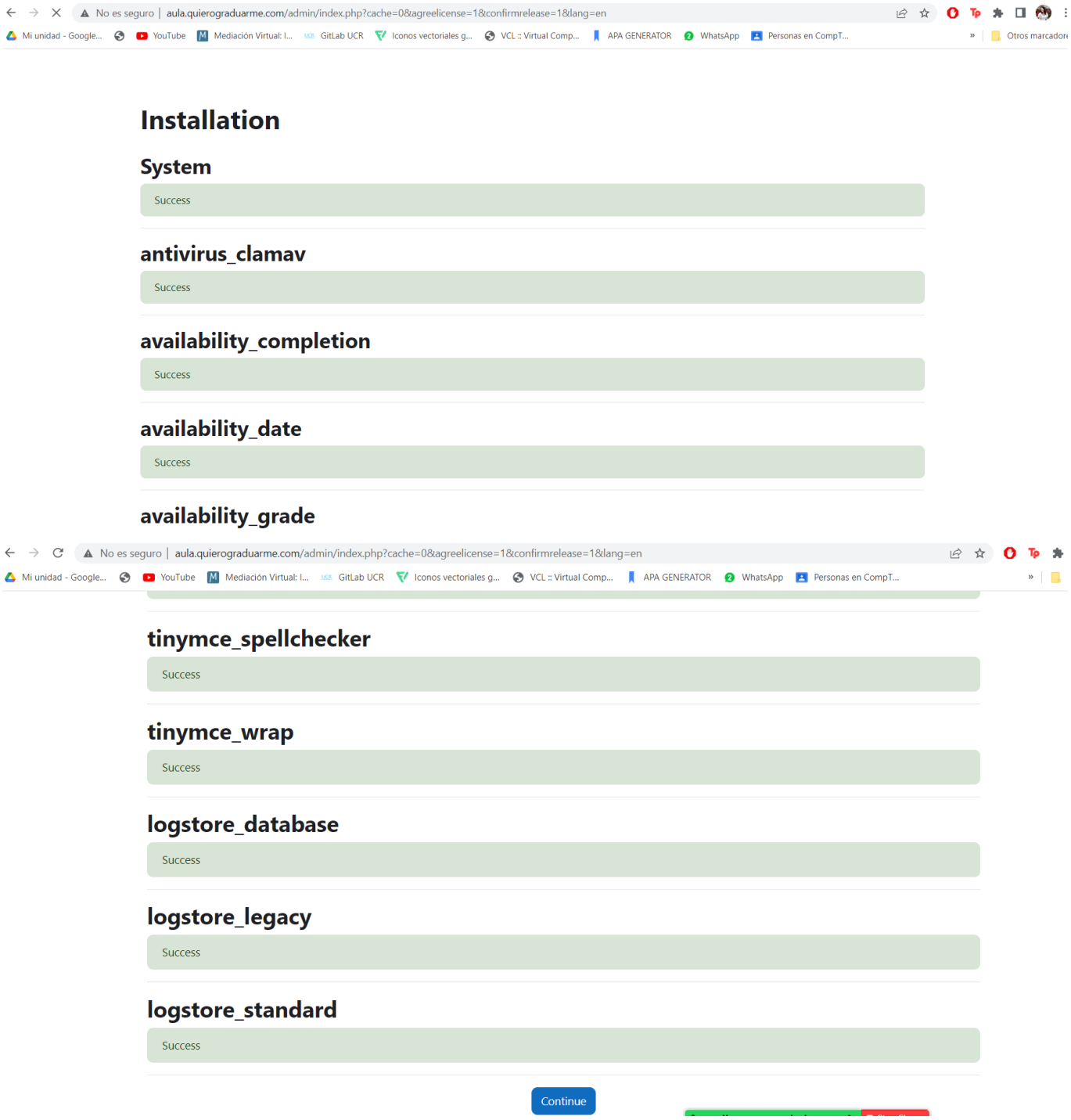
See the Moodle License information page for full details: https://docs.moodle.org/dev/License

Confirm

Have you read these conditions and understood them?

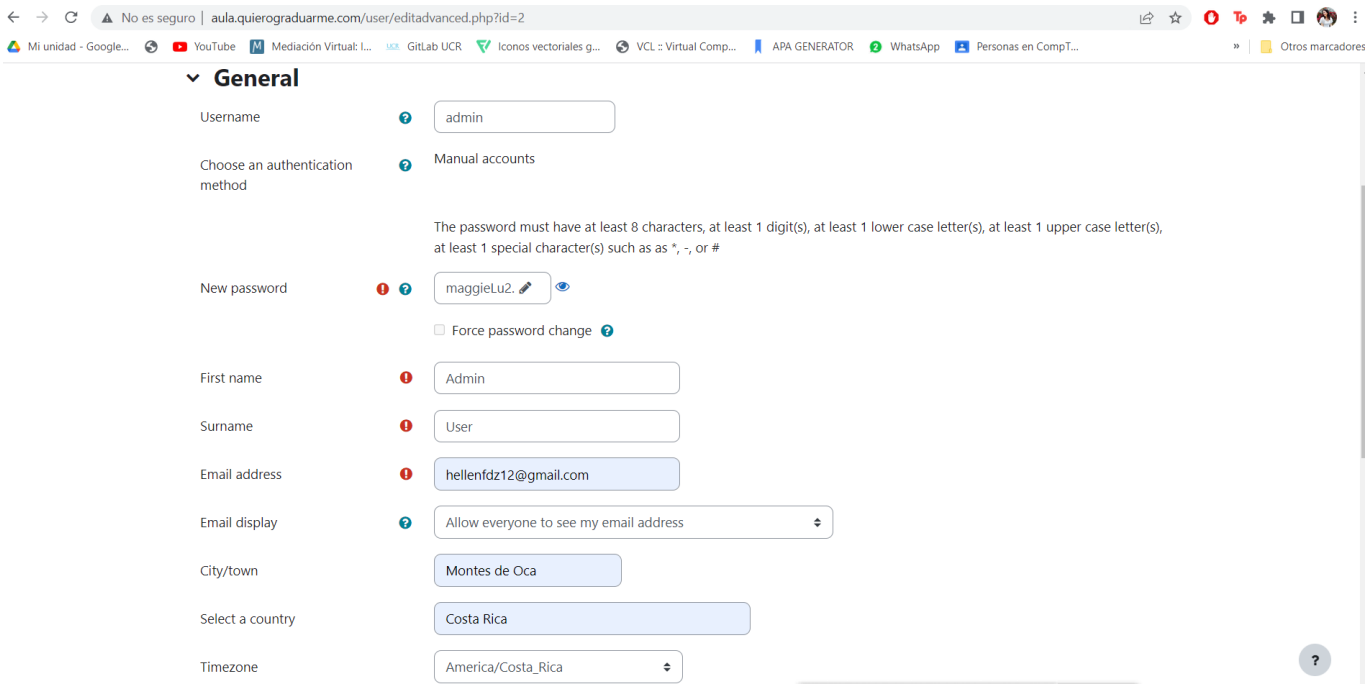
Continue Cancel

?

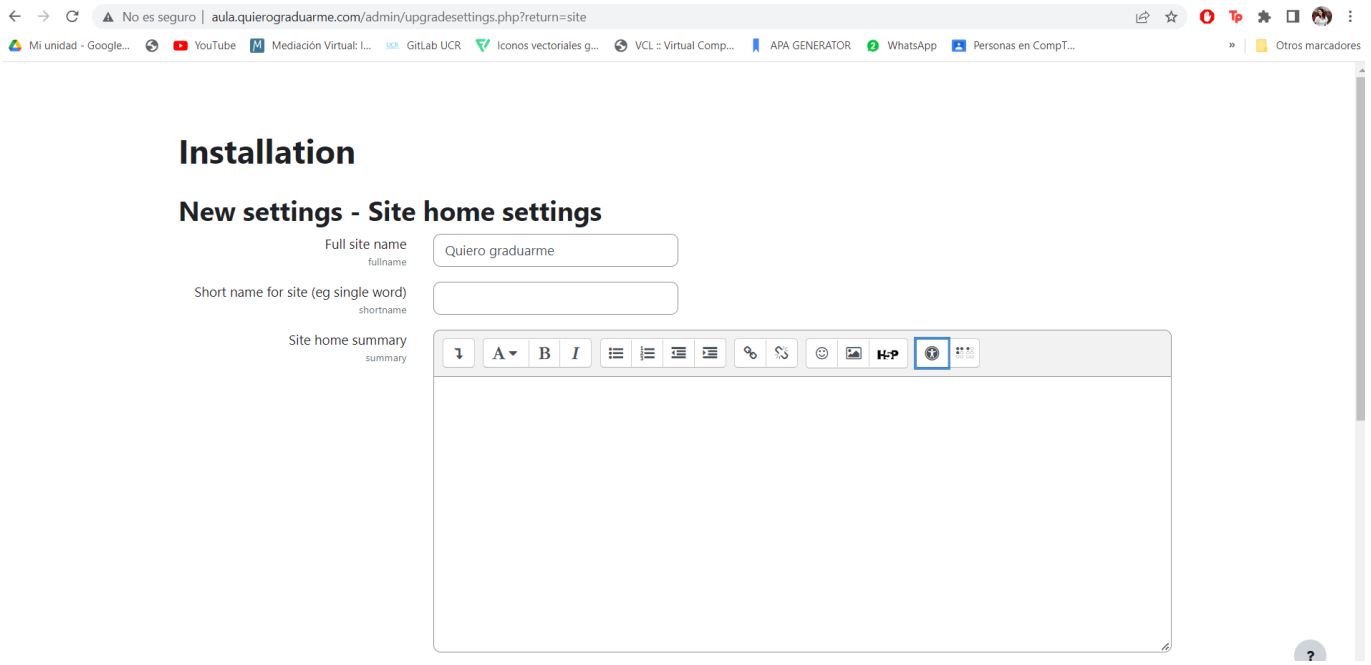


6. Realizar la configuración general

```
Username: admin
New password: maggieLu2.
First name: admin
Surname: User
Email address: hellenfdz12@gmail.com
```

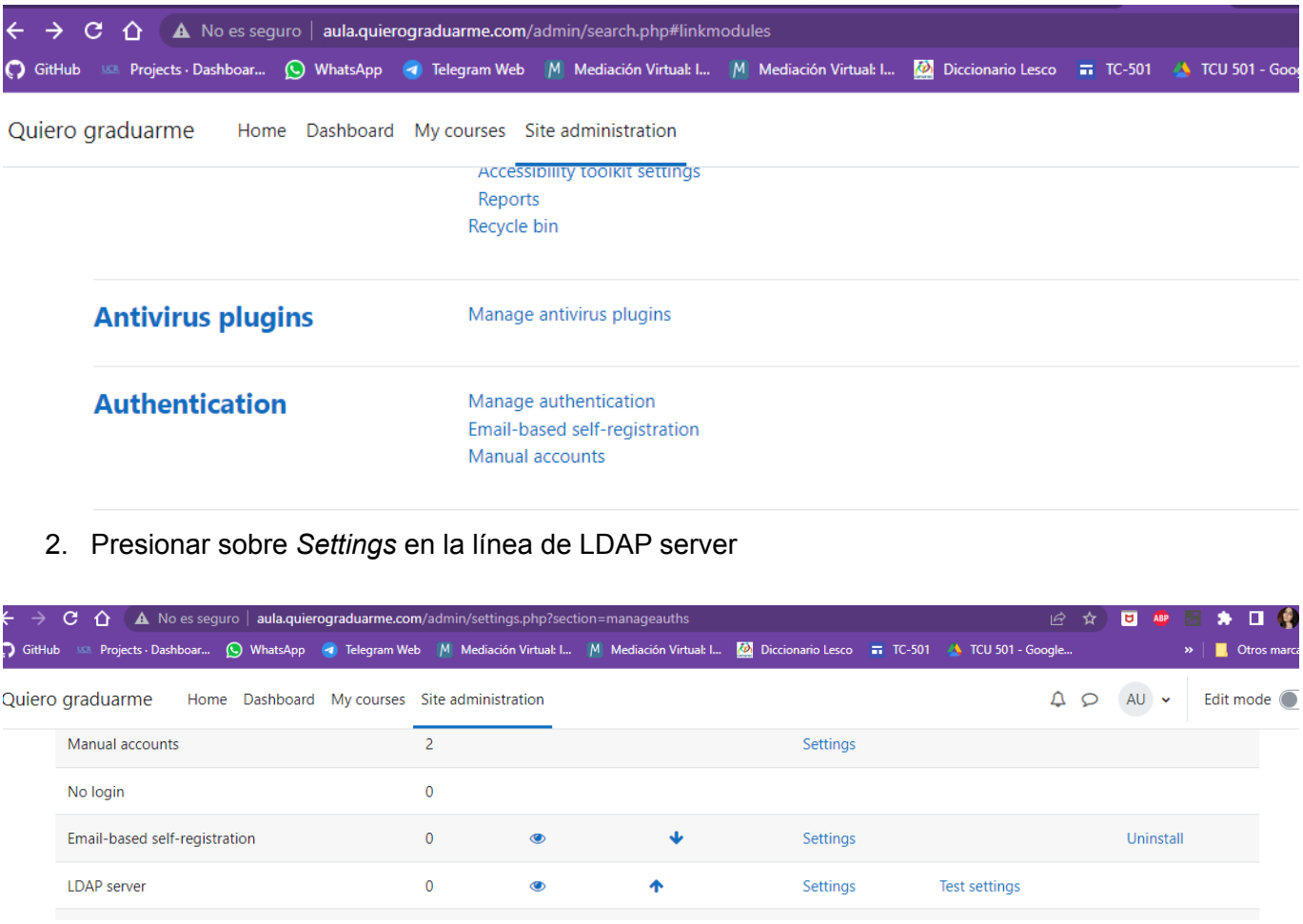


7. Agregar la información del sitio



Instalación LDAP

1. Ingrear a aula.quierograduarme.com, dirigirse a la sección *Site administration,* desplazarse hacia abajo hasta encontrar *authentication*, presionar sobre *Manage authentication*



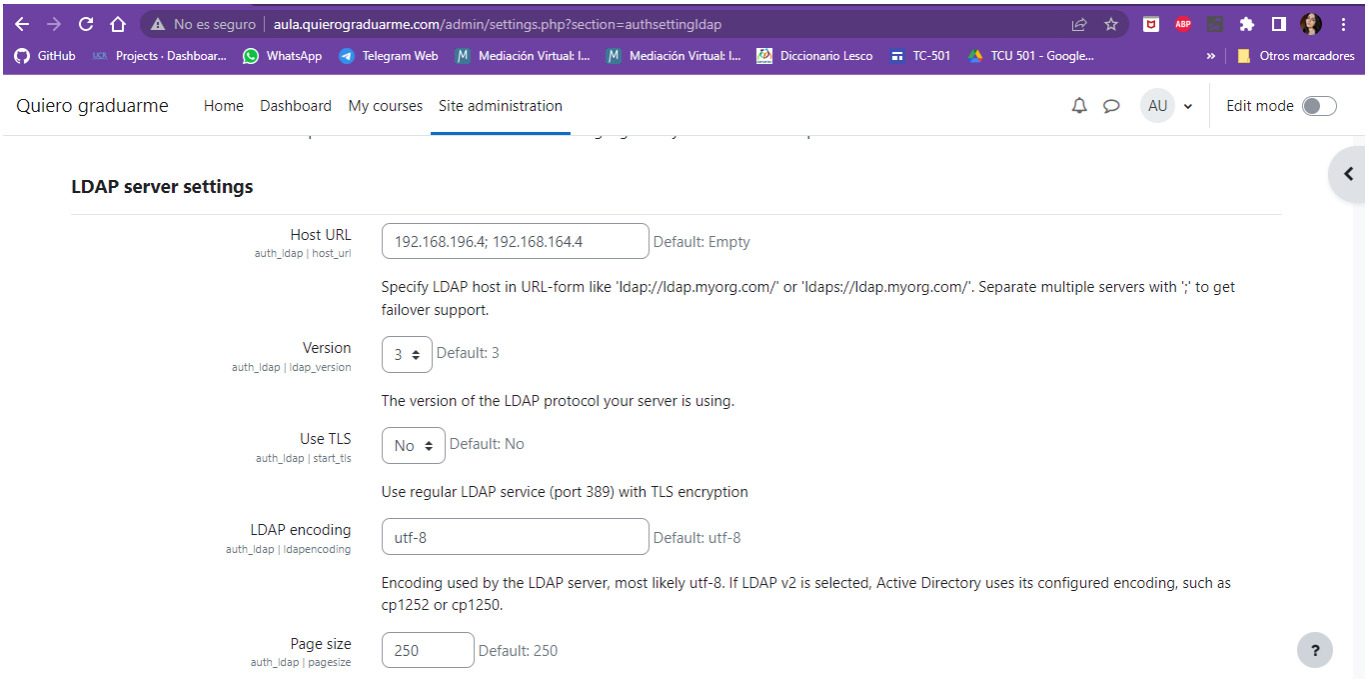
2. Presionar sobre *Settings* en la línea de LDAP server

3. Agregar la siguiente configuración:

LDAP server settings

Host URL: 192.168.196.4; 192.168.164.4

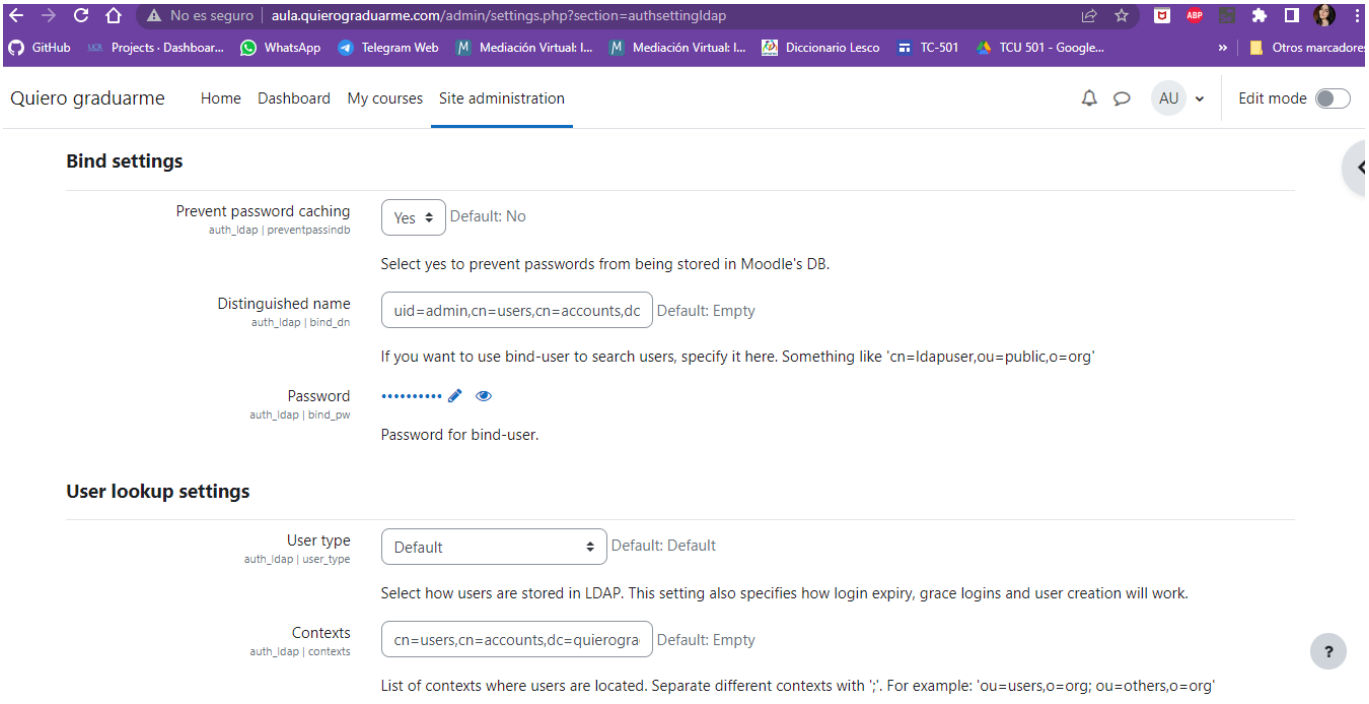
Lo demás se mantuvo por defecto

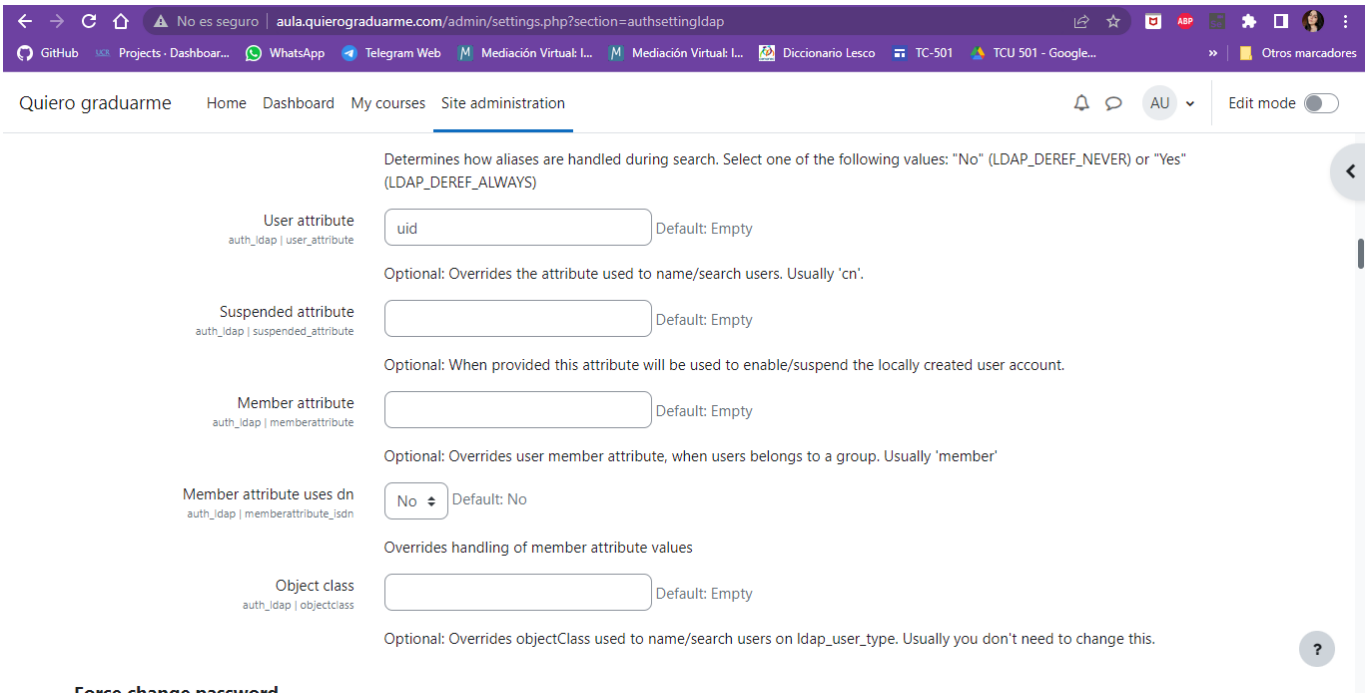


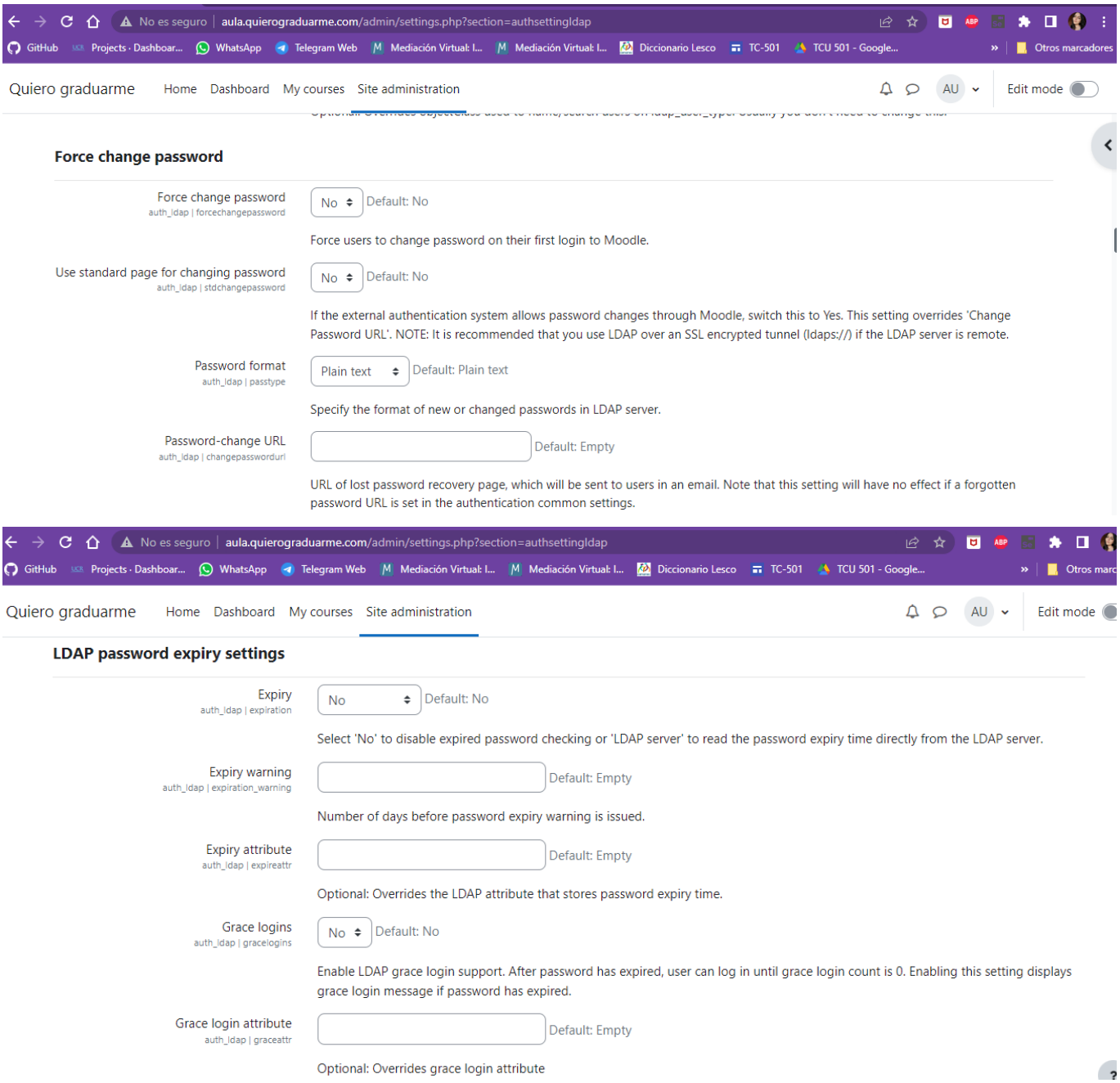
Bind settings

Prevent password caching: yes
Distinguished name: uid=admin,cn=user,cn=accounts,dc=quierograduarme,dc=ya
Password: maggielu2.

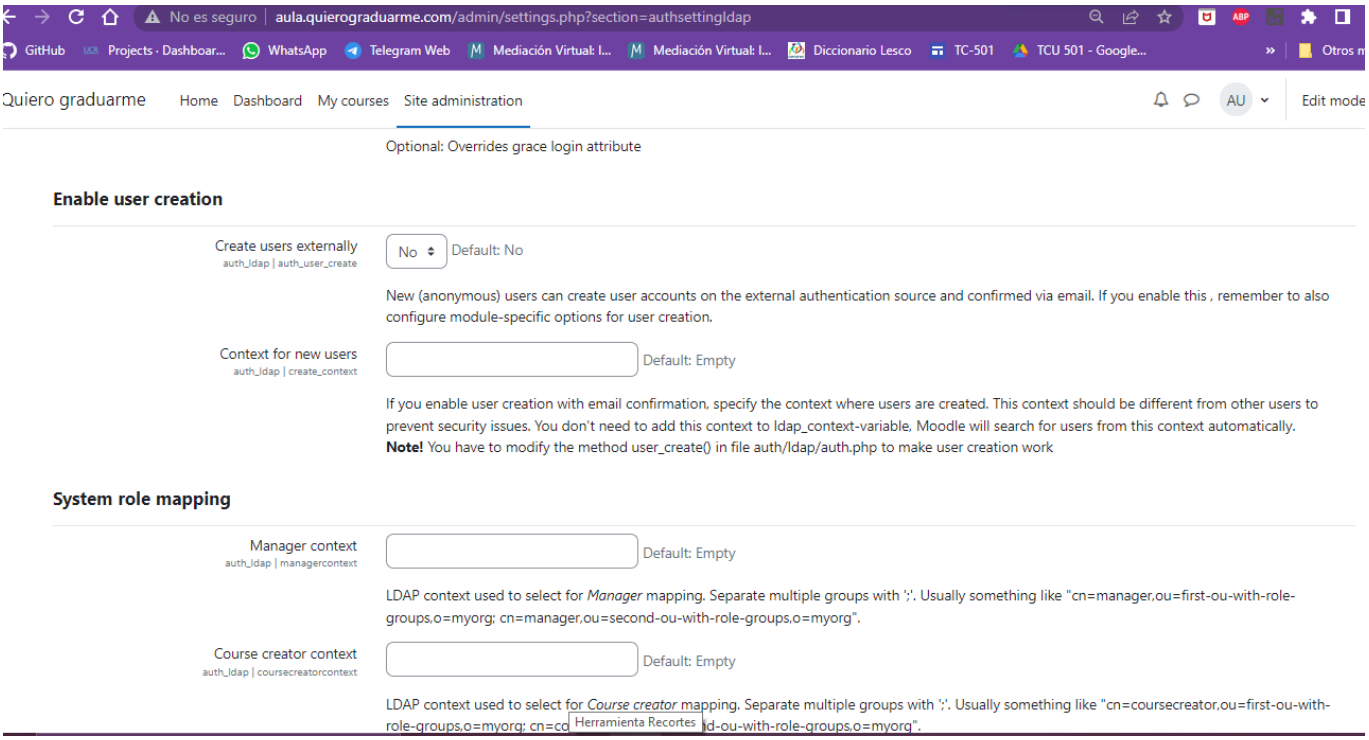
User lookup settings
Contexts: cn=user,cn=accounts,dc=quierograduarme,dc=ya
User attribute: uid
Los otros campos se quedaron con la configuración por defecto





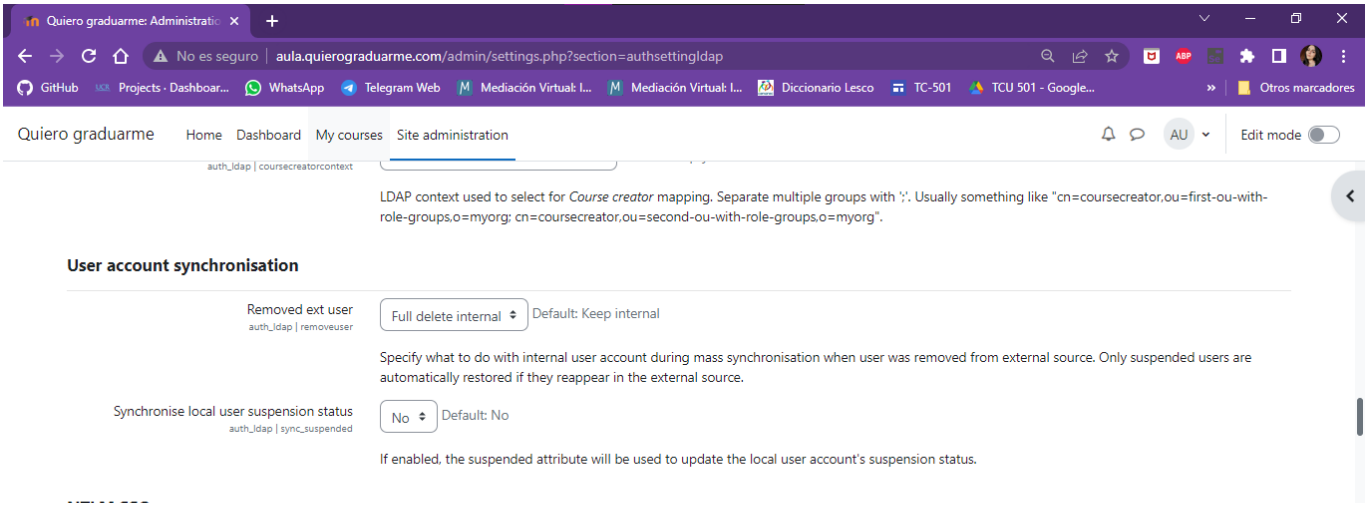

No es seguro | aula.quierograduarme.com/admin/settings.php?section=authsettingldap
GitHub
Projects · Dashboar...
WhatsApp
Telegram Web
Mediación Virtual: I...
Mediación Virtual: I...
Diccionario Lesco
TC-501
TCU 501 - Google...
Otros marcadores
Quiero graduarme
Home
Dashboard
My courses
Site administration
AU
Edit mode
Force change password
Force change password
auth_ldap | forcechangepassword
No
Default: No
Force users to change password on their first login to Moodle.
Use standard page for changing password
auth_ldap | stdchangepassword
No
Default: No
If the external authentication system allows password changes through Moodle, switch this to Yes. This setting overrides 'Change Password URL'. NOTE: It is recommended that you use LDAP over an SSL encrypted tunnel (ldaps://) if the LDAP server is remote.
Password format
auth_ldap | passtype
Plain text
Default: Plain text
Specify the format of new or changed passwords in LDAP server.
Password-change URL
auth_ldap | changepasswordurl
Default: Empty
URL of lost password recovery page, which will be sent to users in an email. Note that this setting will have no effect if a forgotten password URL is set in the authentication common settings.

No es seguro | aula.quierograduarme.com/admin/settings.php?section=authsettingldap
GitHub
Projects · Dashboar...
WhatsApp
Telegram Web
Mediación Virtual: I...
Mediación Virtual: I...
Diccionario Lesco
TC-501
TCU 501 - Google...
Quiero graduarme
Home
Dashboard
My courses
Site administration
AU
Edit mode
LDAP password expiry settings
Expiry
auth_ldap | expiration
No
Default: No
Select 'No' to disable expired password checking or 'LDAP server' to read the password expiry time directly from the LDAP server.
Expiry warning
auth_ldap | expiration_warning
Default: Empty
Number of days before password expiry warning is issued.
Expiry attribute
auth_ldap | expireattr
Default: Empty
Optional: Overrides the LDAP attribute that stores password expiry time.
Grace logins
auth_ldap | gracelogins
No
Default: No
Enable LDAP grace login support. After password has expired, user can log in until grace login count is 0. Enabling this setting displays grace login message if password has expired.
Grace login attribute
auth_ldap | graceattr
Default: Empty
Optional: Overrides grace login attribute



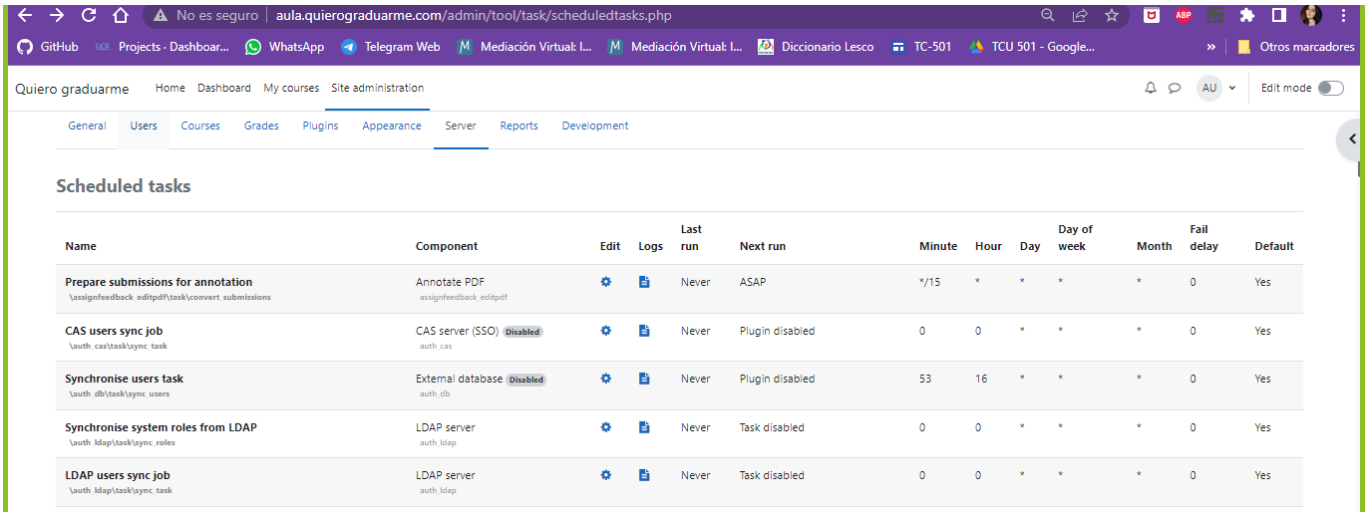
User account synchronisation

Removed ext user: Full delete internal



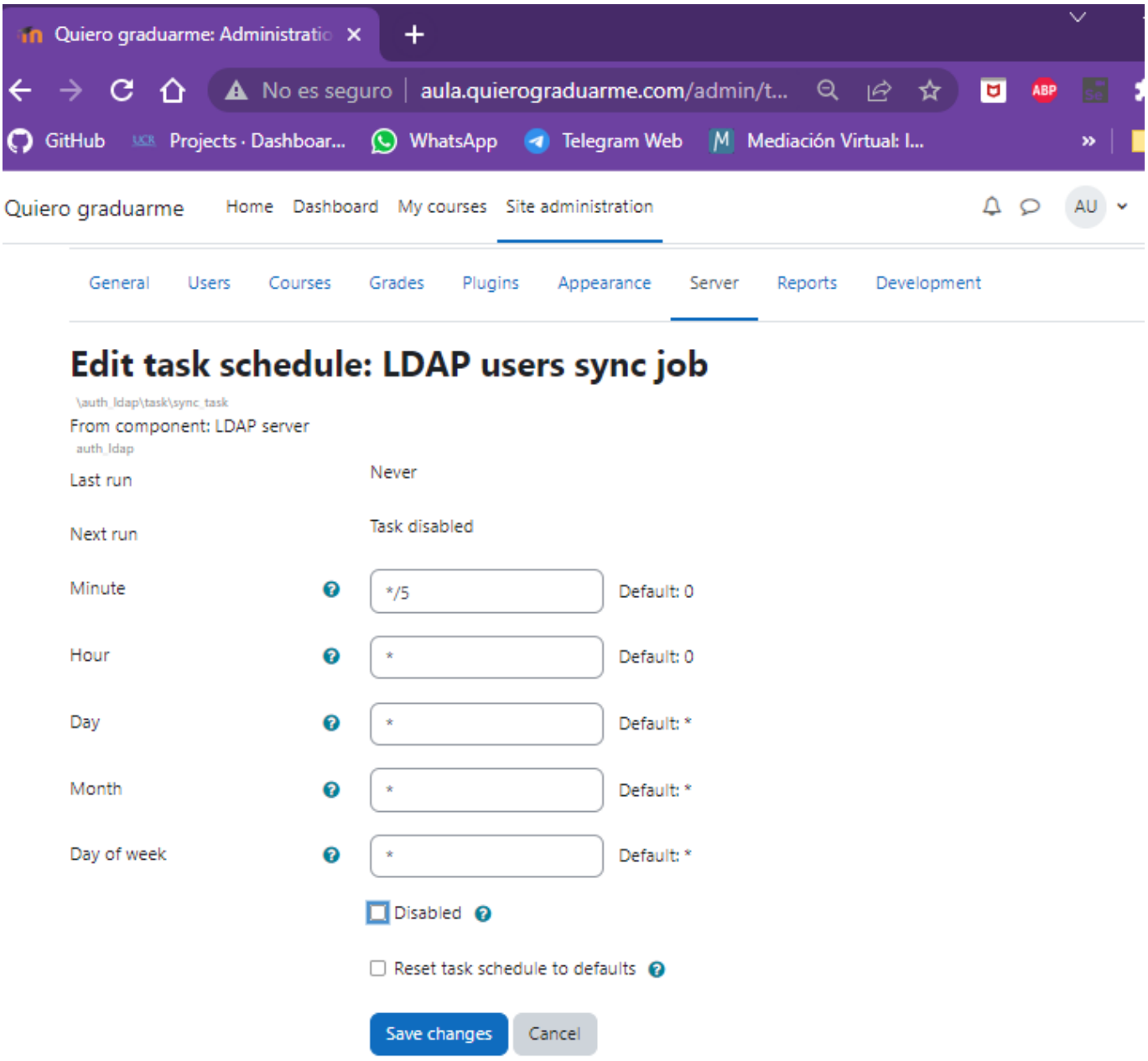
A partir de este punto se dejaron las configuraciones por defecto y se guardaron los cambios.

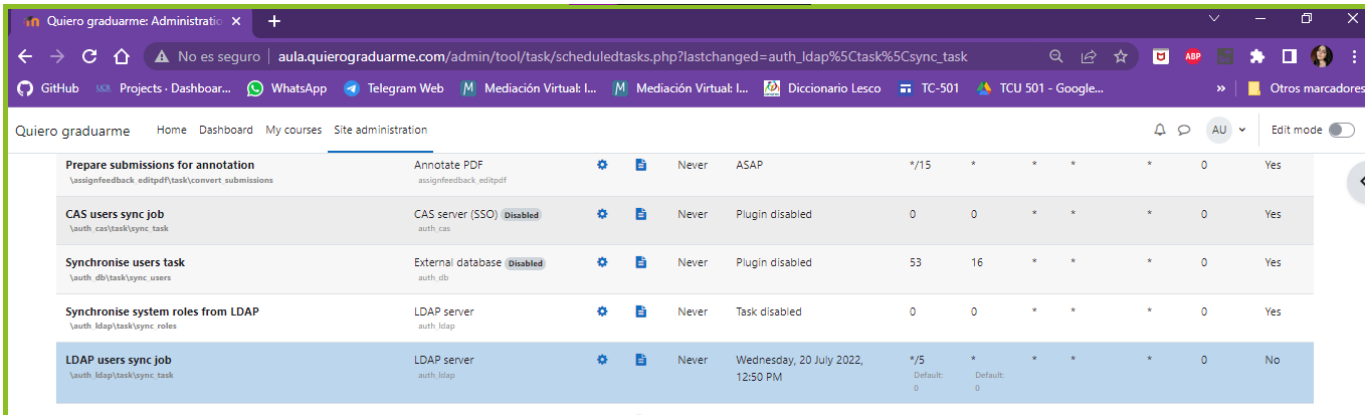
4. Dirigirse a la sección llamada *Server* y editar *LDAP users sync job*



5. Agregar cada cuánto se quieren hacer la sincronización y guardar los cambios

Se va a realizar cada 5 minutos

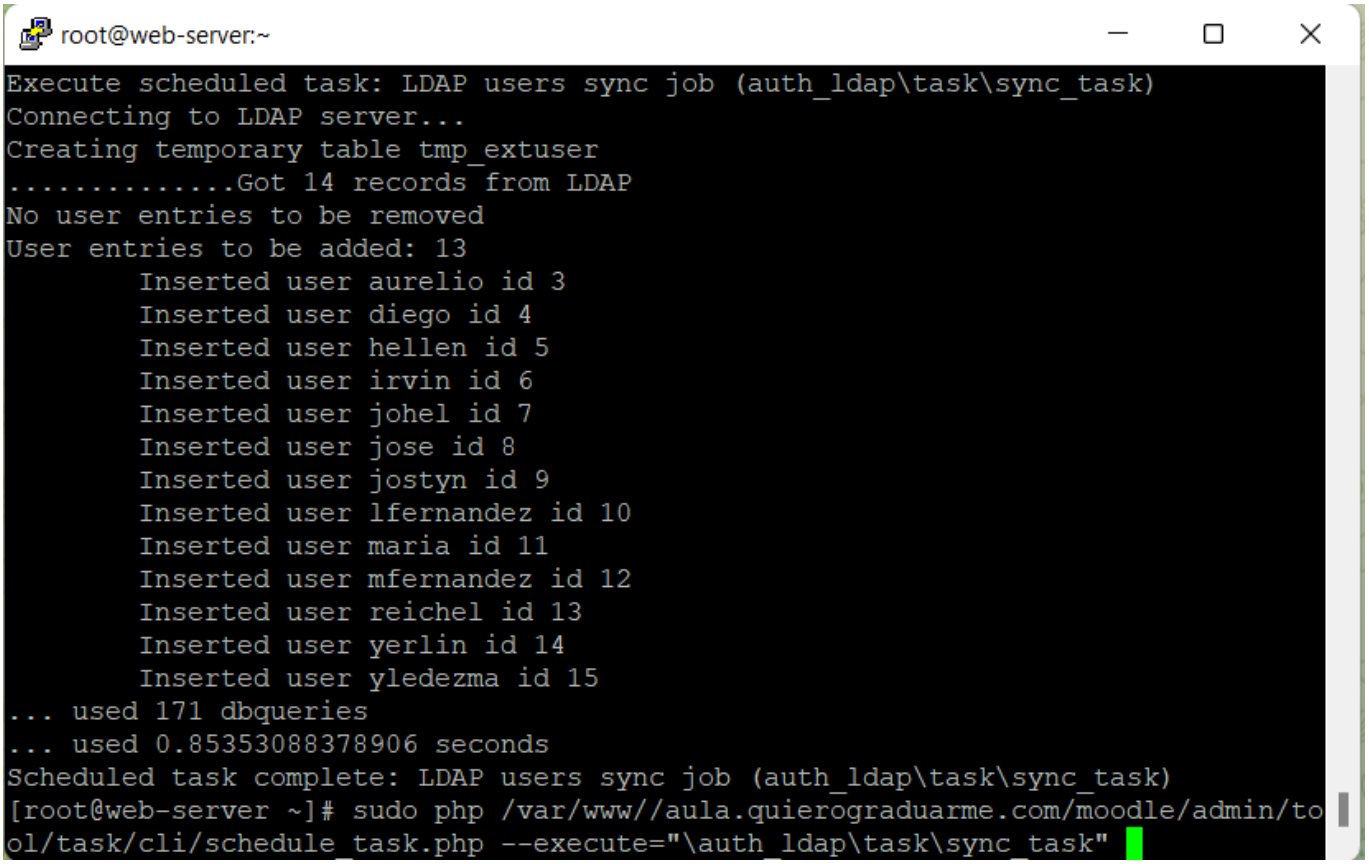




6. Entrar al servidor y ejecutar actualizar usuarios

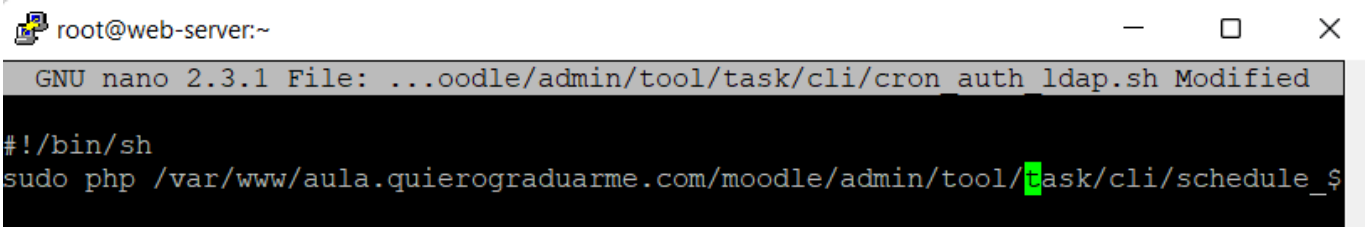
```
sudo php
```

```
/var/www//aula.quierograduarme.com/moodle/admin/tool/task/cli/schedule_task
.php --execute="\auth_ldap\task\sync_task"
```



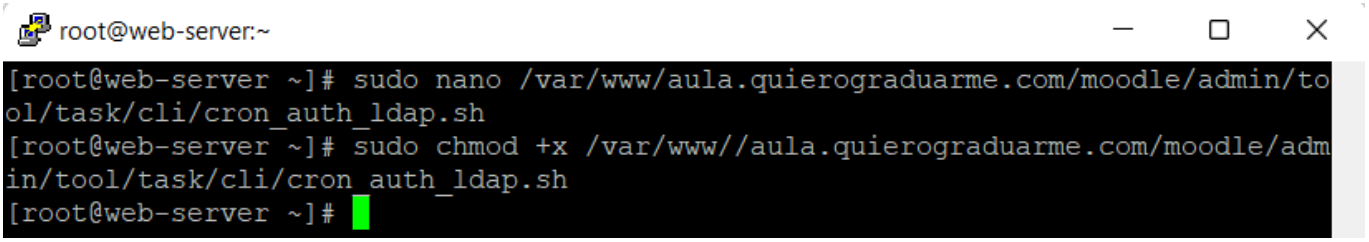
7. Crear script para actualizar los registros de usuario

```
sudo nano
/var/www/aula.quierograduarme.com/moodle/admin/tool/task/cli/cron_auth_ldap.sh
#!/bin/sh
sudo php
/var/www/aula.quierograduarme.com/moodle/admin/tool/task/cli/schedule_task.php
--execute="\auth_ldap\task\sync_task"
```



8. Dar permisos de ejecución

```
sudo chmod +x
/var/www//aula.quierograduarme.com/moodle/admin/tool/task/cli/cron_auth_lda
p.sh
```



9. Crear un scheduled task para que se ejecute la actualización de los registros de usuario, en este caso se agrega que se realice cada 5 minutos

```
sudo crontab -e
*/5 * * * *
/var/www/aula.quierograduarme.com/moodle/admin/tool/task/cli/cron_auth_ldap
.sh
```

Si desea ver si se agregó puede ejecutar:

```
sudo crontab -l
```

Instalación de un servicio de almacenamiento en línea: Nextcloud

1. Instalar dependencias de php requerida

```
sudo yum install php php-ctype php-curl php-dom php-filter php-gd php-hash
php-json php-libxml php-mbstring php-openssl php-posix php-session php-simplexml
php-xmlreader php-xmlwriter php-zip php-zlib php-pdo_mysql php-fileinfo php-bz2
php-intl -y
```

2. Crear la carpeta para el servicio de nextcloud

```
sudo mkdir -p /var/www/nube.quierograduarme.com
```

3. Acceder a la carpeta creada

```
sudo cd/var/www/nube.quierograduarme.com
```

4. Descargar nextcloud

```
sudo wget https://download.nextcloud.com/server/releases/nextcloud-23.0.6.zip
```

5. Descomprimir el paquete descargado

```
sudo unzip nextcloud-23.0.6.zip -d nextcloud
```

6. Otorgar permisos de apache a la carpeta creada

```
sudo chown -R apache:apache /var/www/nube.quierograduarme.com
sudo chmod -R 775 /var/www/nube.quierograduarme.com
```

7. Crear el archivo de configuración de nextcloud

```
sudo nano /etc/httpd/conf.d/nube.quierograduarme.com.conf
```

8. Agregar la siguiente de la configuración al archivo previamente creado

```
<VirtualHost *:80>
    ServerName nube.quierograduarme.com
    ServerAlias www.nube.quierograduarme.com

    DirectoryIndex index.php index.html
    DocumentRoot /var/www/nube.quierograduarme.com/nextcloud/

    ErrorLog /var/log/httpd/nube.quierograduarme.com-error.log
    CustomLog /var/log/httpd/nube.quierograduarme.com-access.log common

    <Directory /var/www/nube.quierograduarme.com/nextcloud>
        Options FollowSymLinks MultiViews
        AllowOverride All
        Require all granted
        <IfModule mod_dav.c>
            Dav off
        </IfModule>
    </Directory>
</VirtualHost>
```

9. Reiniciar apache

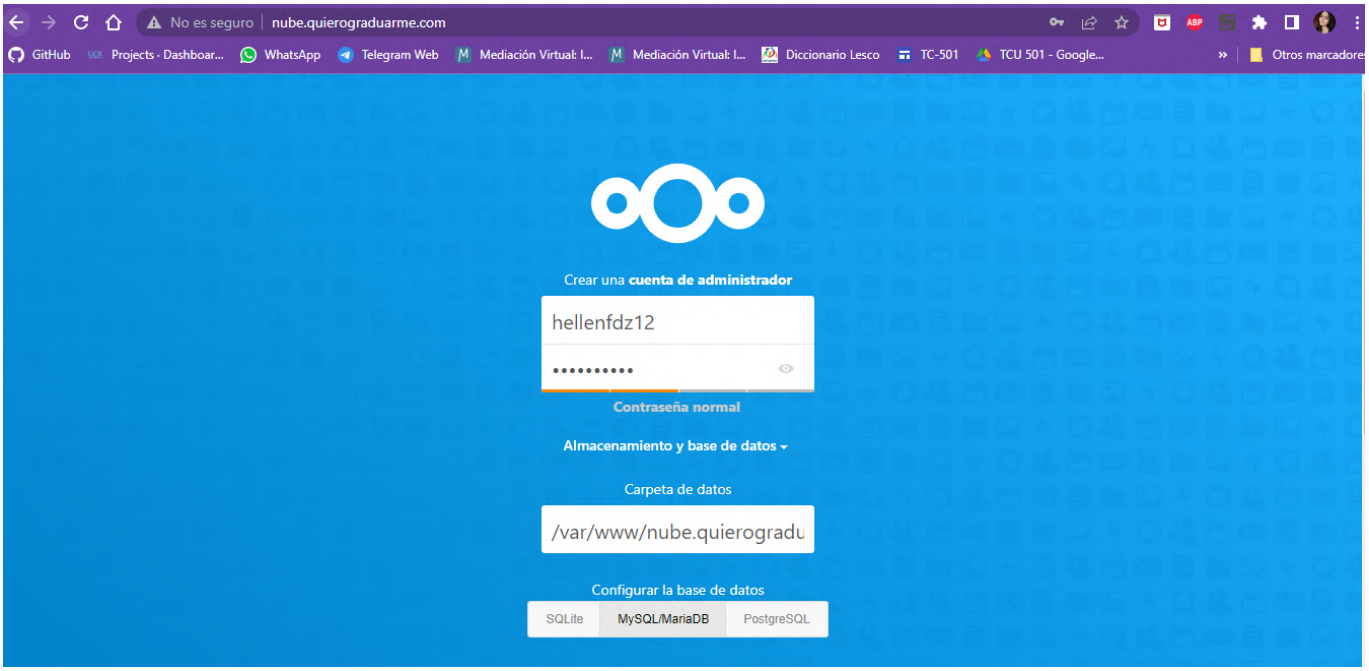
```
sudo systemctl restart httpd
```

Instalación web

1. Ingrese a la página de nextcloud y configurelo de la siguiente manera:

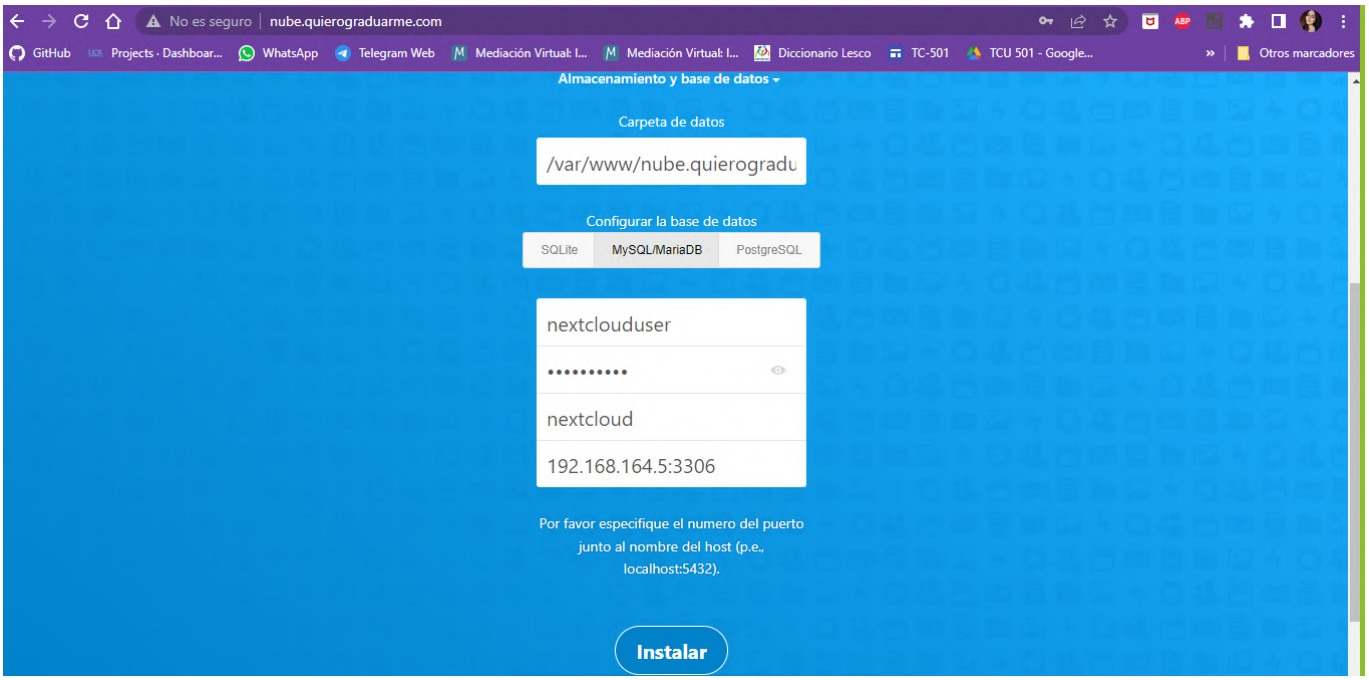
cuenta de administrador:
hellenfzd12
Contraseña: maggielu2.

Carpeta de datos: /var/www/quierograduarme.com/nextcloud/data

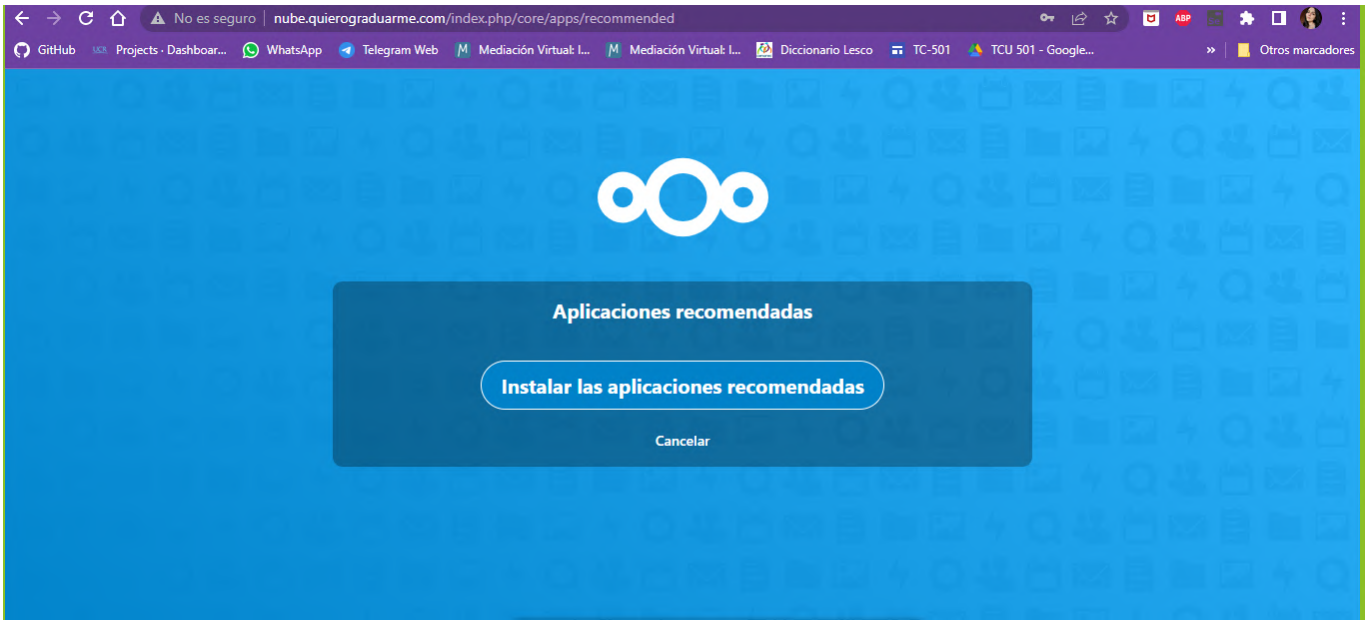


2. Seleccionar la base de datos MariaDB

User: nextclouduser
Password: maggielu2.
Database: nextcloud
Host: 192.168.164.5:3306

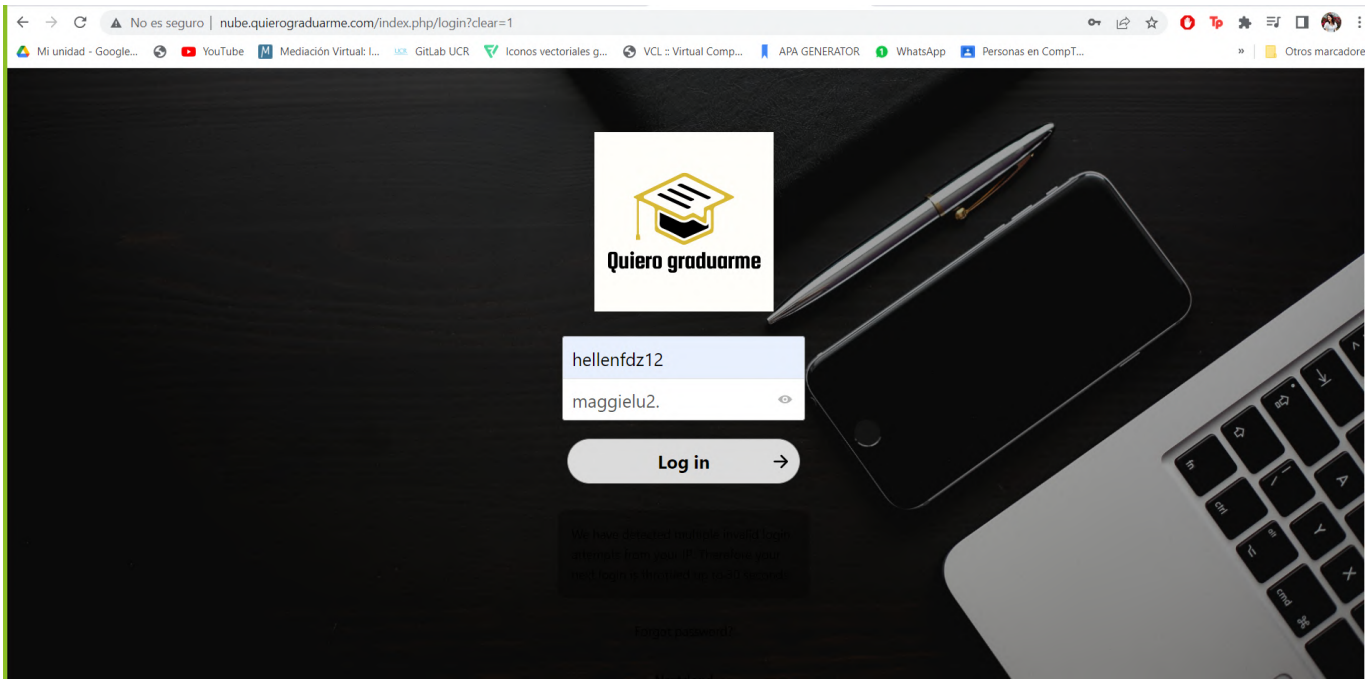


3. Darle click a Instalar las aplicaciones recomendadas.

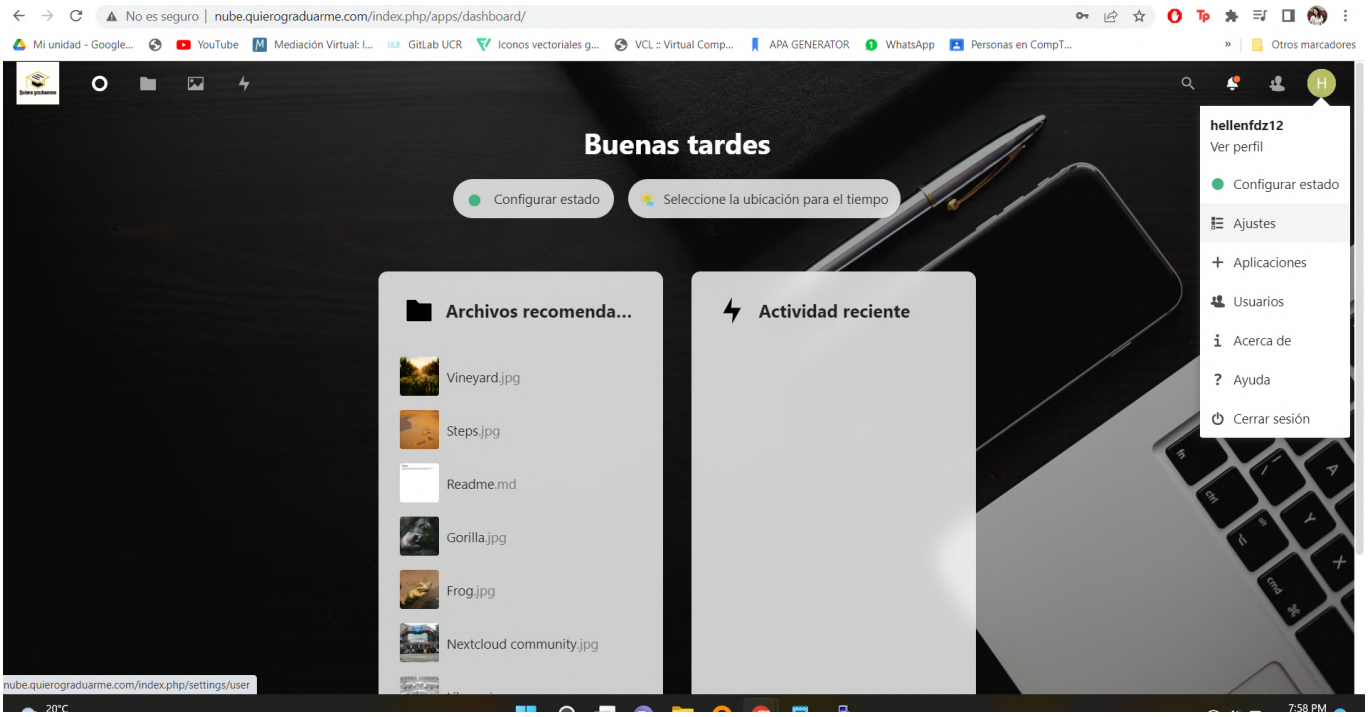


Configuración LDAP

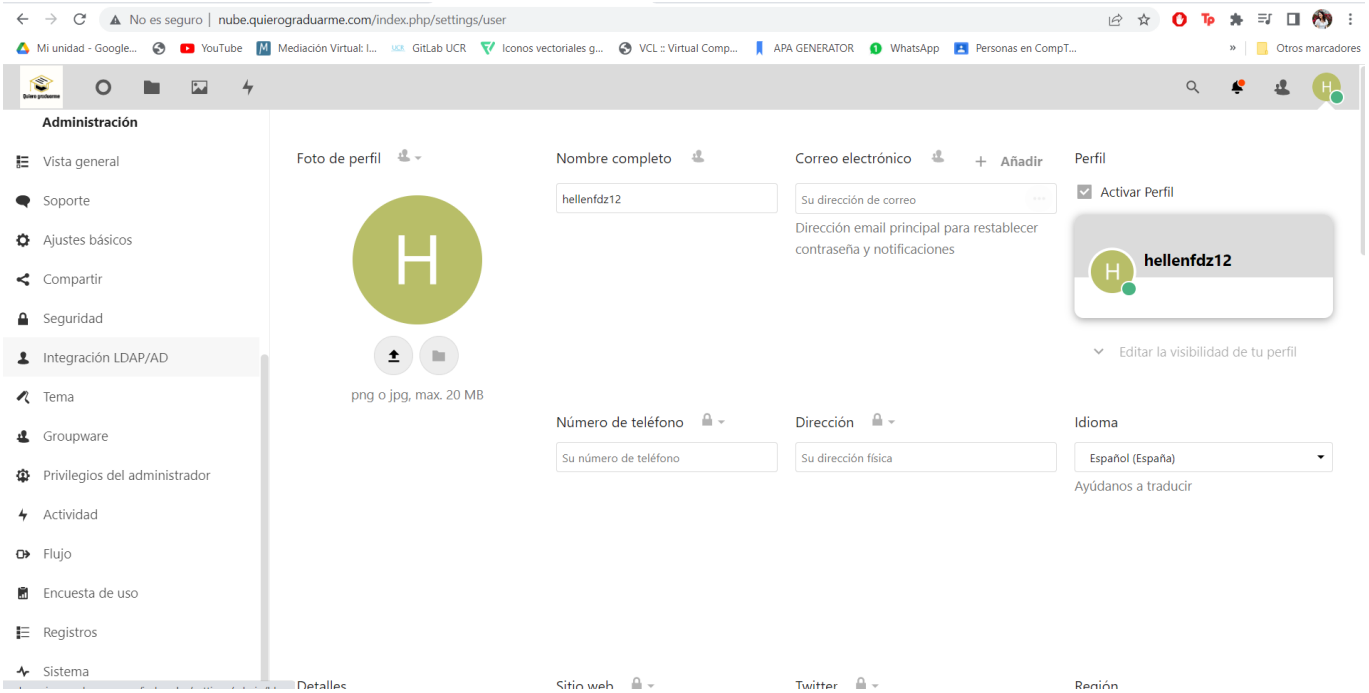
1. Iniciar sesión con la cuenta del administrador



2. Dirigirse a ajustes:



3. Bajar en el panel de administración hasta que llegue a integración LDAP/AD

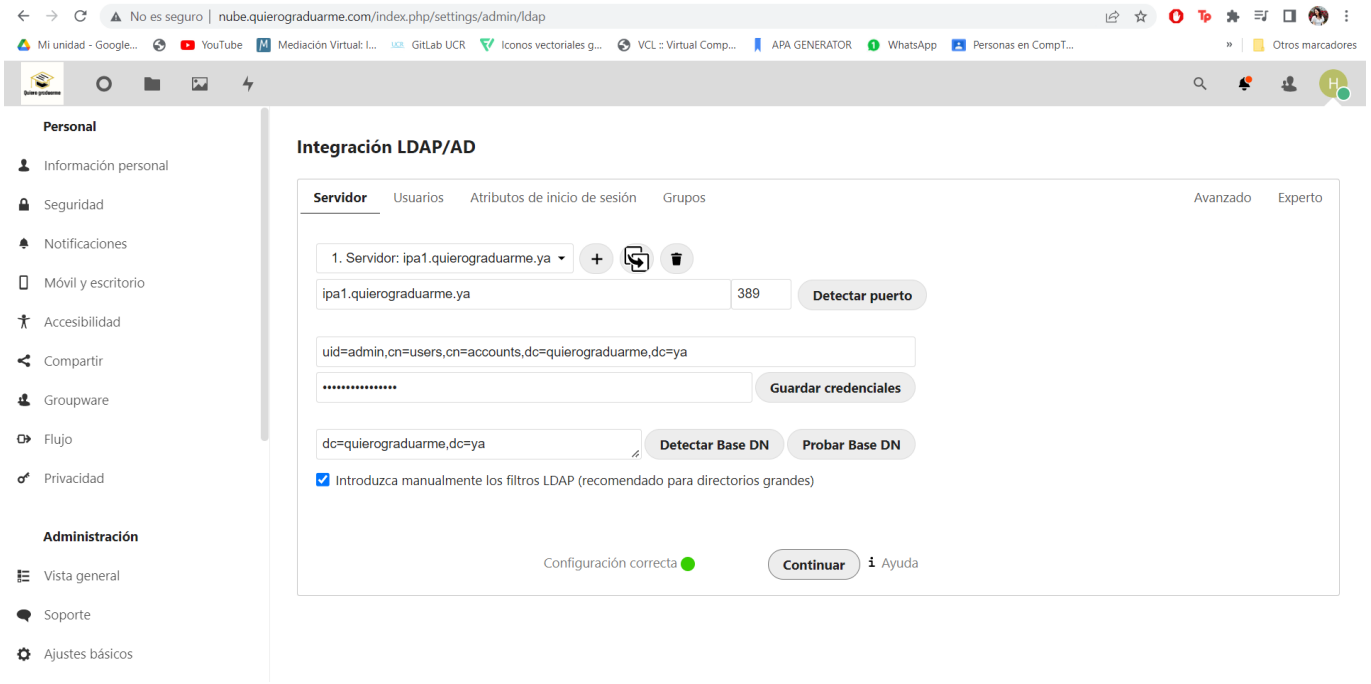


4. Visualice el siguiente archivo para identificar algunas de las variables necesarias para la configuración.

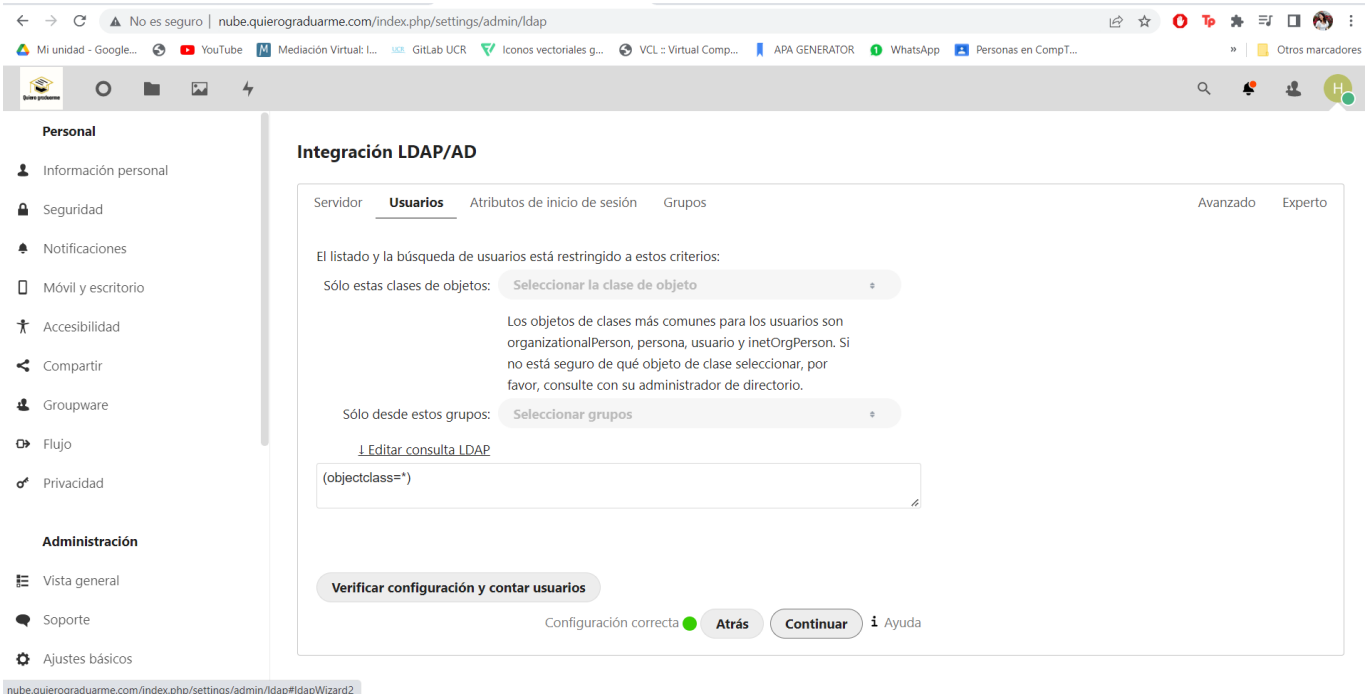
```
[root@ipa1 ~]# cat /etc/ipa/default.conf
[global]
host = ipa1.quierograduarme.ya
basedn = dc=quierograduarme,dc=ya
realm = QUIEROGRADUARME.YA
domain = quierograduarme.ya
xmlrpc_uri = https://ipa1.quierograduarme.ya/ipa/xml
ldap_uri = ldapi://%2fvar%2frun%2fslapd-QUIEROGRADUARME-YA.socket
enable_ra = True
ra_plugin = dogtag
```

```
dogtag_version = 10
mode = production
```

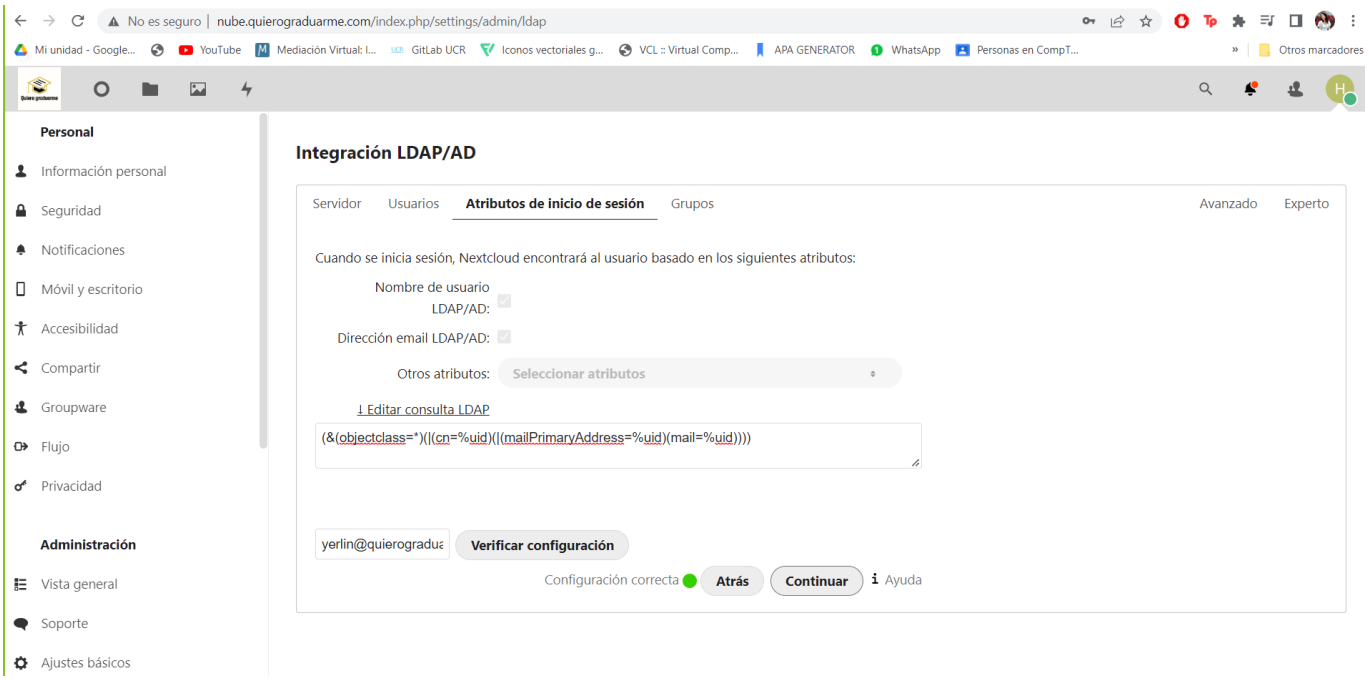
5. Configure de la siguiente forma el apartado del servidor:

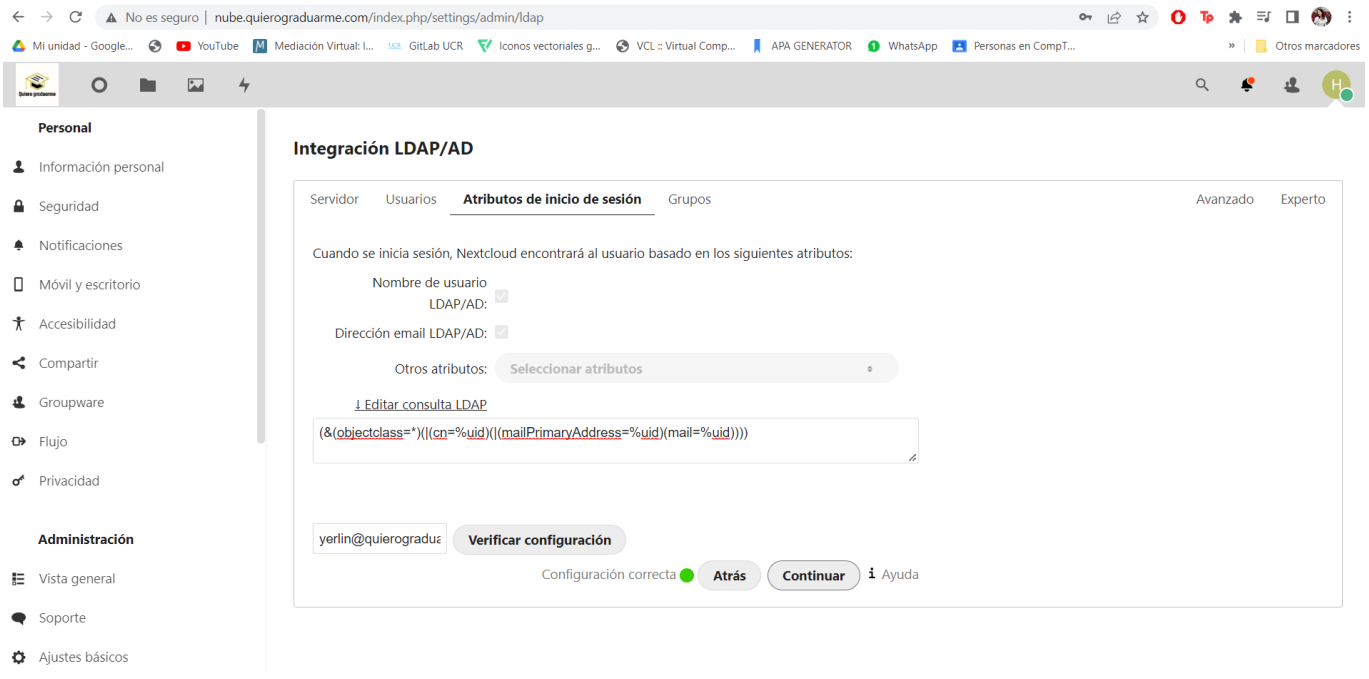


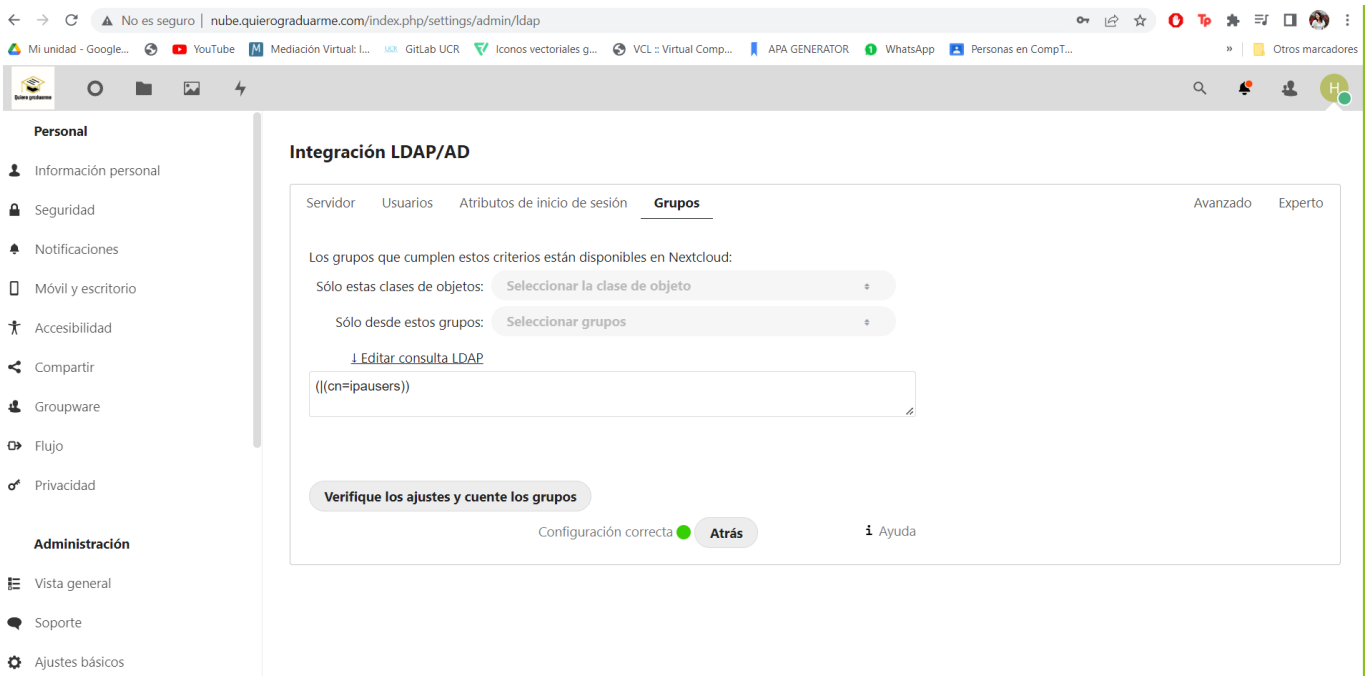
6. Configure de la siguiente forma el apartado de usuarios. En este caso fue necesario modificar la consulta de LDAP por (objectclass=*):

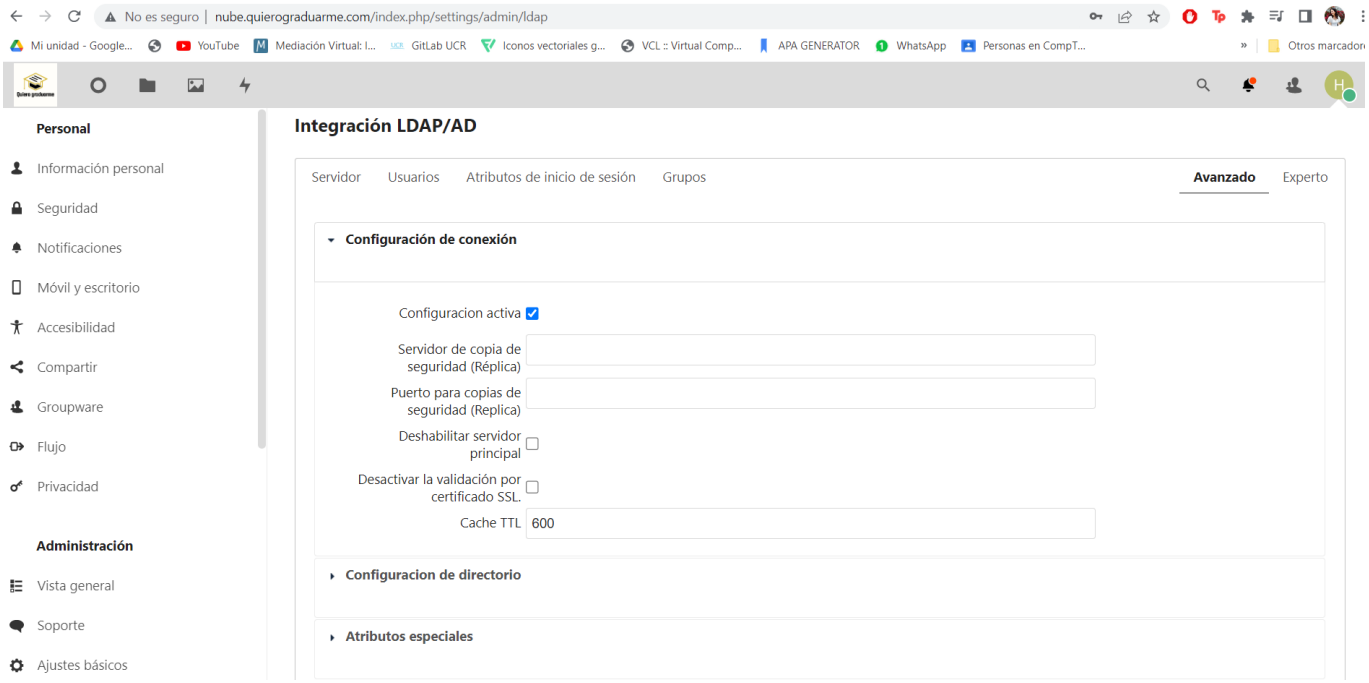


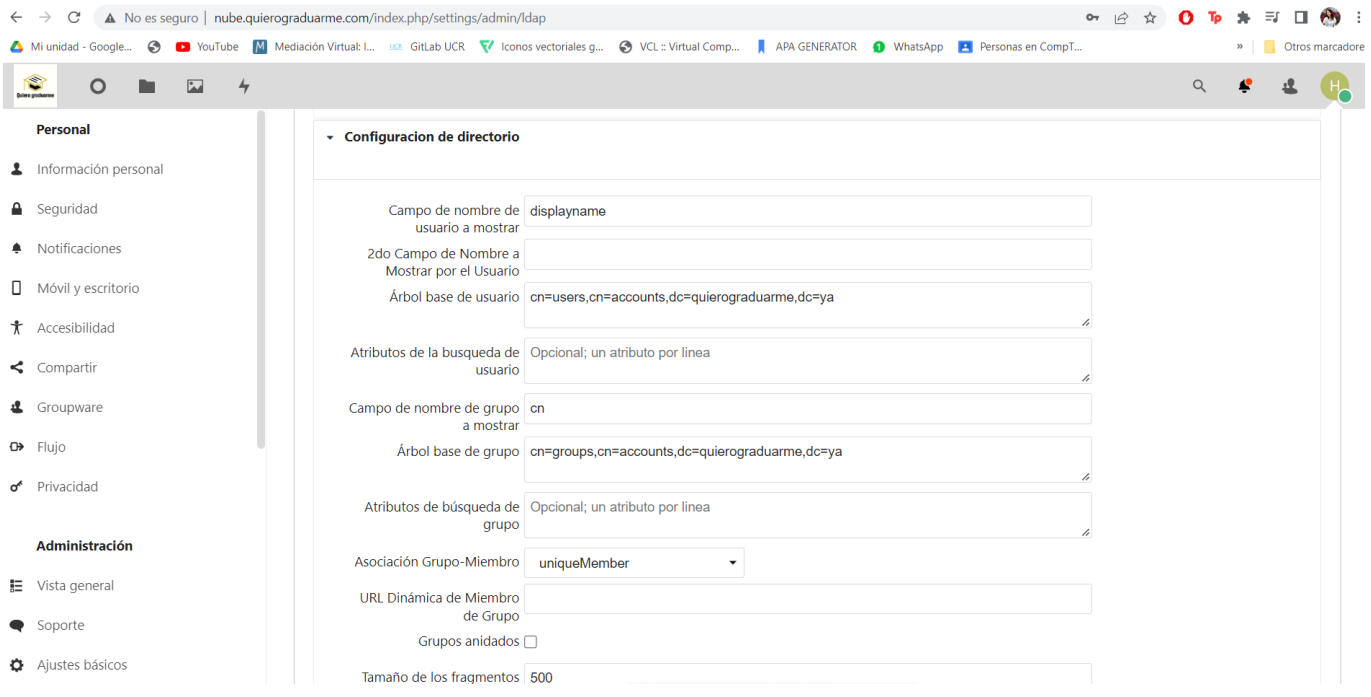
7. Modifique los atributos de inicio de sesión de la siguiente forma, en esta ocasión : (&(objectclass=*)(|(cn=%uid)(|(mailPrimaryAddress=%uid)(mail=%uid))))

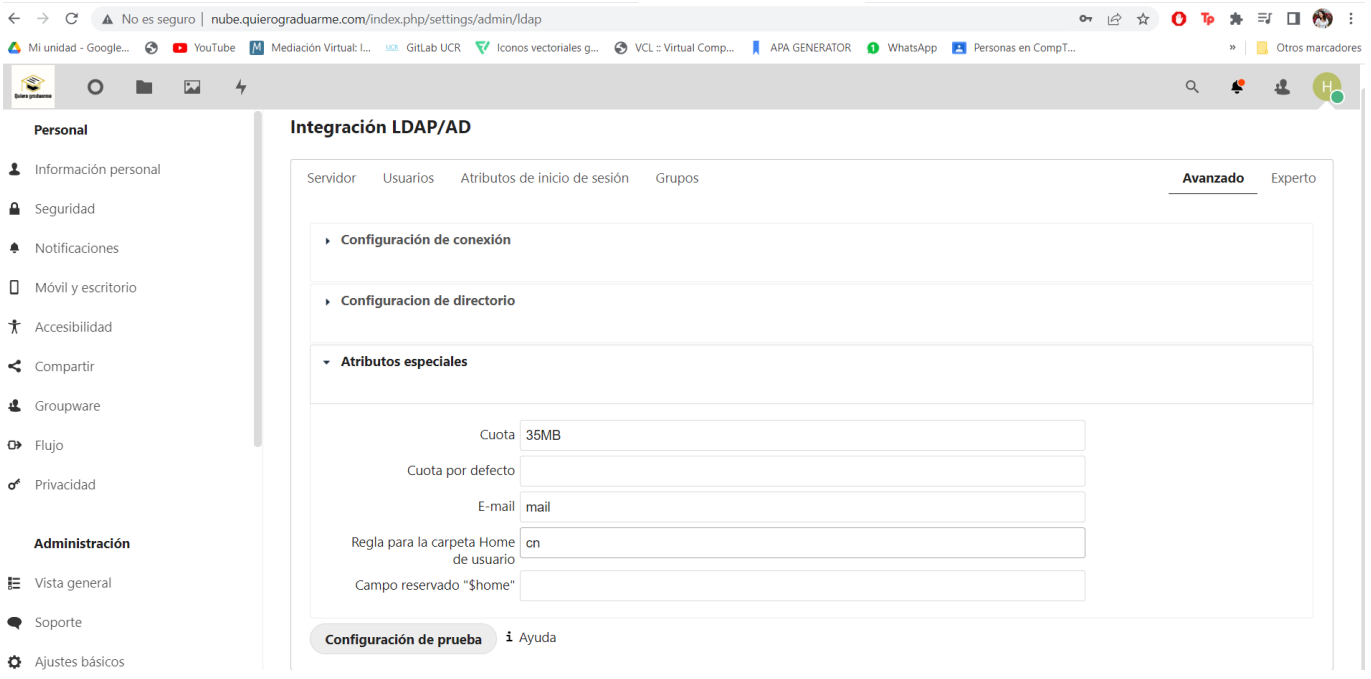

No es seguro | nube.quierograduarme.com/index.php/settings/admin/ldap
Mi unidad - Google...
YouTube
Mediación Virtual: I...
GitLab UCR
Iconos vectoriales g...
VCL :: Virtual Comp...
APA GENERATOR
WhatsApp
Personas en CompT...
Otros marcadores
Personal
Información personal
Seguridad
Notificaciones
Móvil y escritorio
Accesibilidad
Compartir
Groupware
Flujo
Privacidad
Administración
Vista general
Soporte
Ajustes básicos
Integración LDAP/AD
Servidor
Usuarios
Atributos de inicio de sesión
Grupos
Avanzado
Experto
Cuando se inicia sesión, Nextcloud encontrará al usuario basado en los siguientes atributos:
Nombre de usuario LDAP/AD:
Dirección email LDAP/AD:
Otros atributos:
Seleccionar atributos
Editar consulta LDAP
(&(objectclass=*)(|(cn=%uid)(|(mailPrimaryAddress=%uid)(mail=%uid))))
yerlin@quierograduа
Verificar configuración
Configuración correcta
Atrás
Continuar
Ayuda

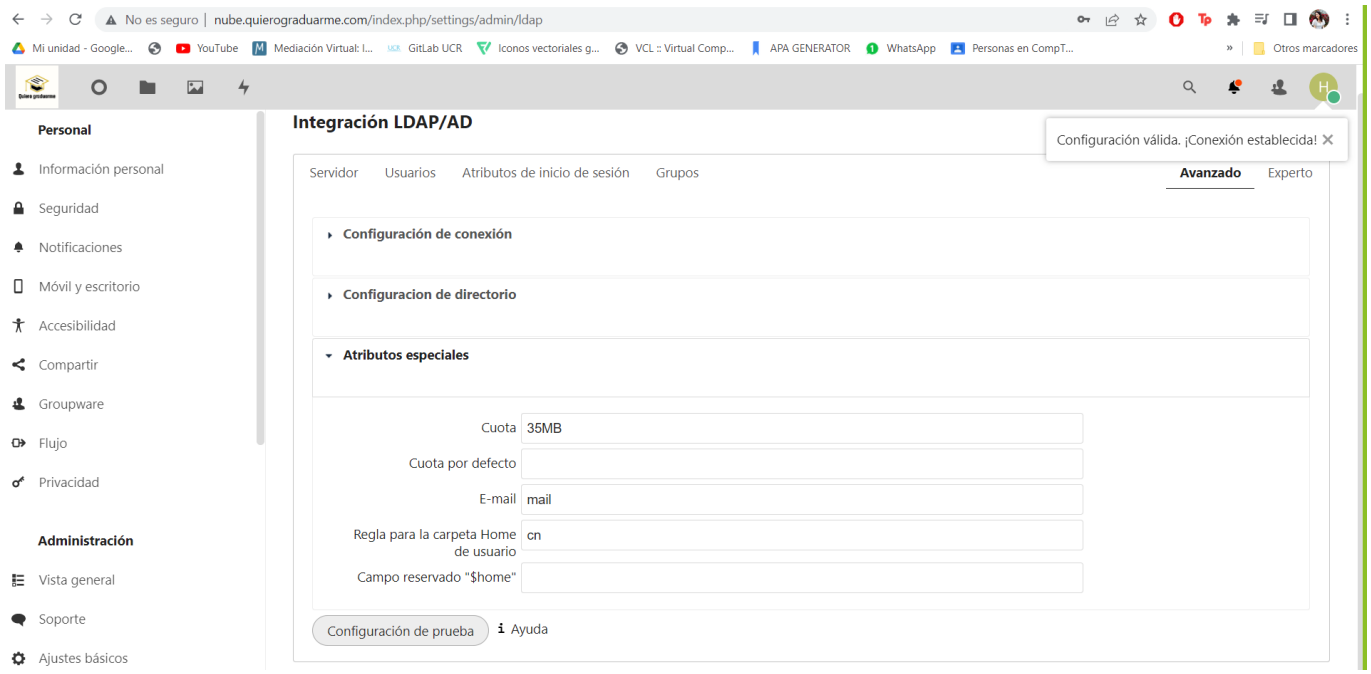

No es seguro | nube.quierograduarme.com/index.php/settings/admin/ldap
Mi unidad - Google...
YouTube
Mediación Virtual: I...
GitLab UCR
Iconos vectoriales g...
VCL :: Virtual Comp...
APA GENERATOR
WhatsApp
Personas en CompT...
Otros marcadores
Personal
Información personal
Seguridad
Notificaciones
Móvil y escritorio
Accesibilidad
Compartir
Groupware
Flujo
Privacidad
Administración
Vista general
Soporte
Ajustes básicos
Integración LDAP/AD
Servidor
Usuarios
Atributos de inicio de sesión
Grupos
Avanzado
Experto
Cuando se inicia sesión, Nextcloud encontrará al usuario basado en los siguientes atributos:
Nombre de usuario LDAP/AD:
Dirección email LDAP/AD:
Otros atributos:
Seleccionar atributos
Editar consulta LDAP
(&(objectclass=*)(|(cn=%uid)(|(mailPrimaryAddress=%uid)(mail=%uid))))
yerlin@quierograduа
Verificar configuración
Configuración correcta
Atrás
Continuar
Ayuda


No es seguro | nube.quierograduarme.com/index.php/settings/admin/ldap
Personal
Información personal
Seguridad
Notificaciones
Móvil y escritorio
Accesibilidad
Compartir
Groupware
Flujo
Privacidad
Administración
Vista general
Soporte
Ajustes básicos
Integración LDAP/AD
Servidor
Usuarios
Atributos de inicio de sesión
Grupos
Avanzado
Experto
Los grupos que cumplen estos criterios están disponibles en Nextcloud:
Sólo estas clases de objetos:
Seleccionar la clase de objeto
Sólo desde estos grupos:
Seleccionar grupos
Editar consulta LDAP
(|(cn=ipausers))
Verifique los ajustes y cuente los grupos
Configuración correcta
Atrás
Ayuda


No es seguro | nube.quierograduarme.com/index.php/settings/admin/ldap
Personal
Información personal
Seguridad
Notificaciones
Móvil y escritorio
Accesibilidad
Compartir
Groupware
Flujo
Privacidad
Administración
Vista general
Soporte
Ajustes básicos
Integración LDAP/AD
Servidor
Usuarios
Atributos de inicio de sesión
Grupos
Avanzado
Experto
Configuración de conexión
Configuracion activa
Servidor de copia de seguridad (Réplica)
Puerto para copias de seguridad (Replica)
Deshabilitar servidor principal
Desactivar la validación por certificado SSL.
Cache TTL
600
Configuracion de directorio
Atributos especiales


No es seguro | nube.quierograduarme.com/index.php/settings/admin/ldap
Personal
Información personal
Seguridad
Notificaciones
Móvil y escritorio
Accesibilidad
Compartir
Groupware
Flujo
Privacidad
Administración
Vista general
Soporte
Ajustes básicos
Configuracion de directorio
Campo de nombre de usuario a mostrar
displayname
2do Campo de Nombre a Mostrar por el Usuario
Árbol base de usuario
cn=users,cn=accounts,dc=quierograduarme,dc=ya
Atributos de la busqueda de usuario
Opcional; un atributo por linea
Campo de nombre de grupo a mostrar
cn
Árbol base de grupo
cn=groups,cn=accounts,dc=quierograduarme,dc=ya
Atributos de búsqueda de grupo
Opcional; un atributo por linea
Asociación Grupo-Miembro
uniqueMember
URL Dinámica de Miembro de Grupo
Grupos anidados
Tamaño de los fragmentos
500


No es seguro | nube.quierograduarme.com/index.php/settings/admin/ldap
Personal
Información personal
Seguridad
Notificaciones
Móvil y escritorio
Accesibilidad
Compartir
Groupware
Flujo
Privacidad
Administración
Vista general
Soporte
Ajustes básicos
Integración LDAP/AD
Servidor
Usuarios
Atributos de inicio de sesión
Grupos
Avanzado
Experto
Configuración de conexión
Configuracion de directorio
Atributos especiales
Cuota
35MB
Cuota por defecto
E-mail
mail
Regla para la carpeta Home de usuario
cn
Campo reservado "$home"
Configuración de prueba
Ayuda



Monitoreo de servicios: php server monitor

1. Instalar los siguientes paquetes:

```
yum install httpd mariadb-server php php-curl php-cli php-mysql php-pdo -y
```

2. Ejecutar los siguientes comandos para poner a funcionar el servicio de base de datos de mariadb

```
systemctl start  mariadb.service
systemctl start  httpd.service
```

3. Instalar la base de datos con el siguiente comando:

```
mysql_secure_installation
```

4. Crear una base de datos y usuario para el PHP server monitor:

```
mysql -u root -p
create database phpmonitor;
grant all on phpmonitor.* to 'hellen' @' localhost'  identified by 'maggielu2.';
flush privileges;
exit
```

5. Pasarse hacia la siguiente ruta y obtener el comprimido de phpserver monitor.

```
cd /var/www/html/
wget --no-check-certificate
'https://docs.google.com/uc?export=download&id=1G3V0WMAv8Ns6XA_GXvhz1Gy_bUYj_o5U'
-O phpservermon-3.5.2.tar.gz
```

6. Descomprimir el archivo

```
tar -xvzf phpservermon-3.5.2.tar.gz
```

7. Moverlo a la carpeta phpserver mon

```
mv phpservermon-3.5.2 phpservermon
```

8. Cambiarle el ownership del directorio hacia apache:

chown -R apache:apache /var/www/html/phpservermon

9. Establecer la zona horaria como America/Costa Rica

```
nano /etc/php.ini
America/Costa_Rica
```

10. Reinciar el servicio de mariadb

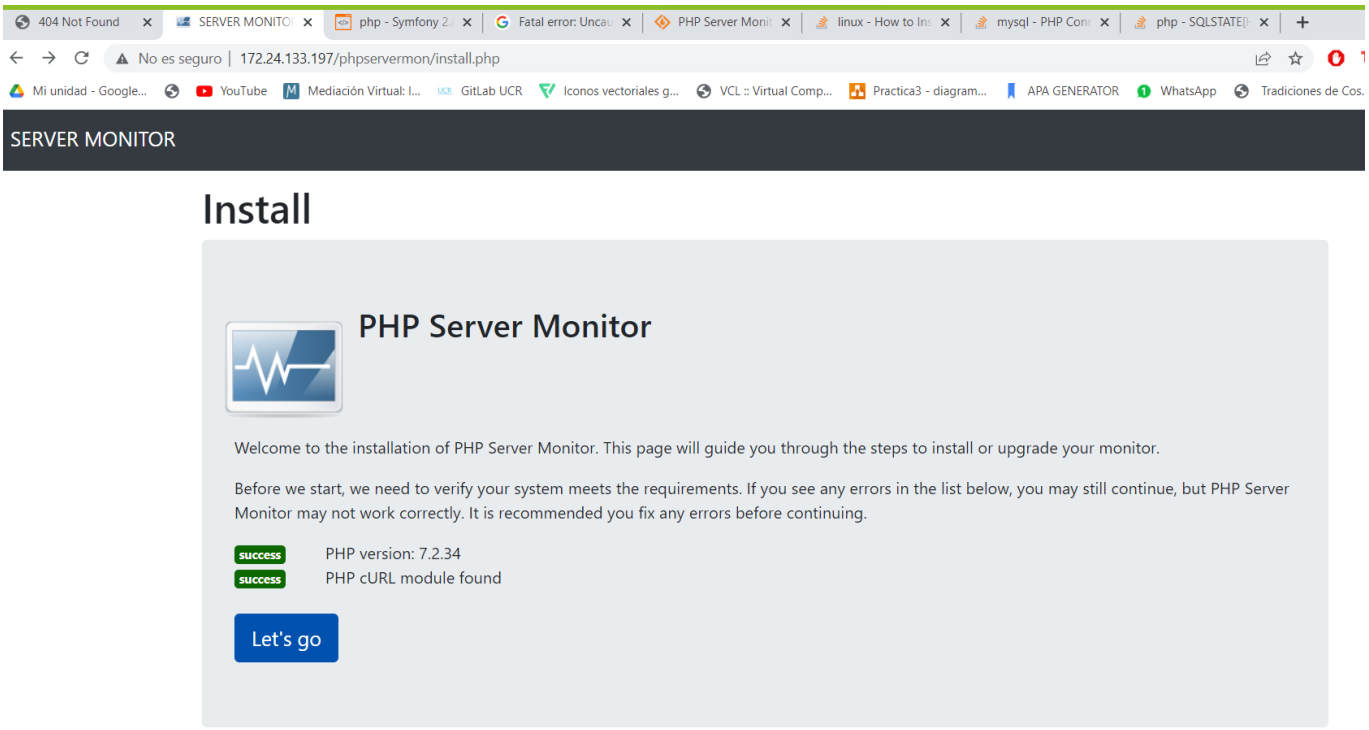
```
systemctl restart mariadb
```

11. Reiniciar el servicio de apache.

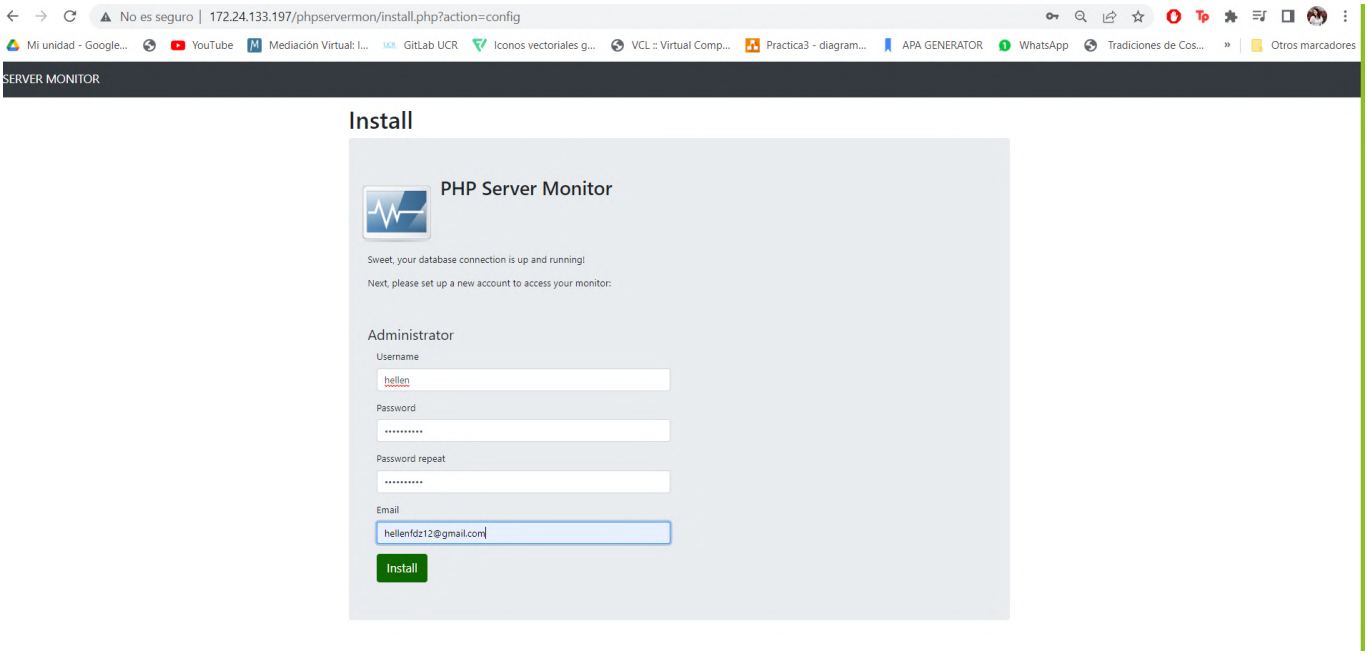
```
systemctl restart httpd
```

12. Ingresar al sitio y clickar en Let’s go:

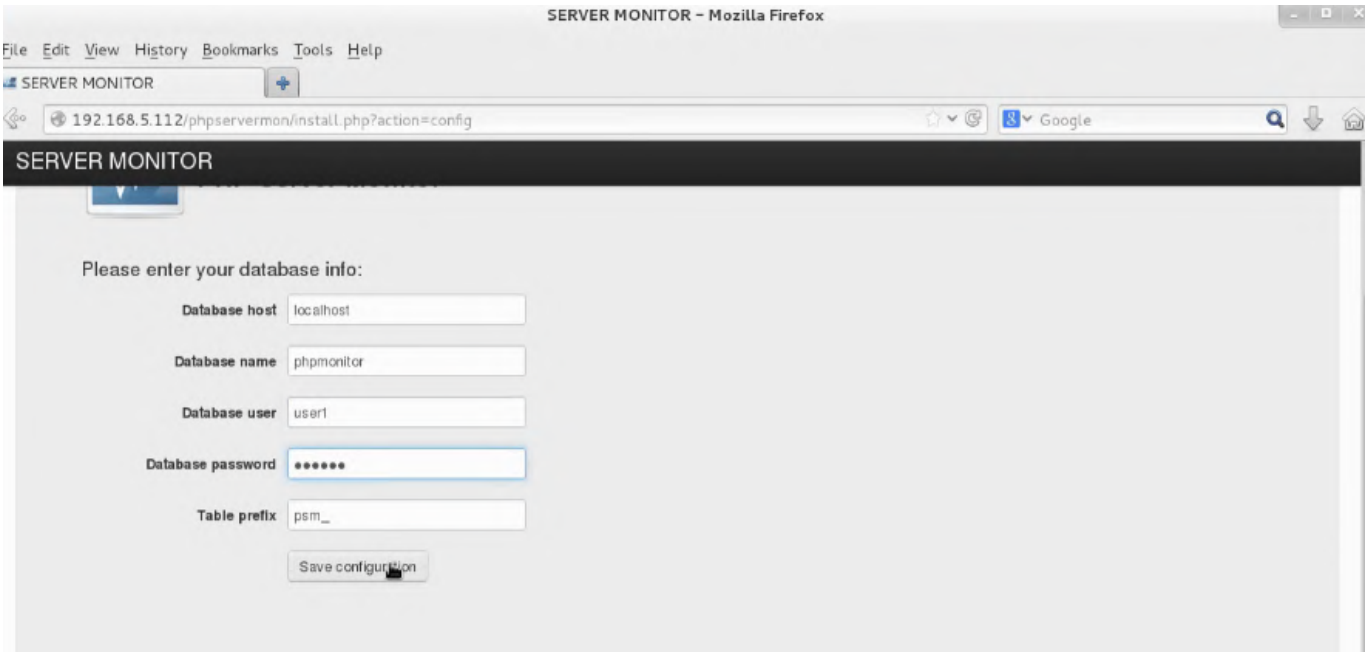
```
http://172.24.133.199/phpservermon
```



13. Establecer un usuario con contraseña y un correo:
    user:hellen
    password: maggielu2.
    email:hellenfdz12.gmail.com



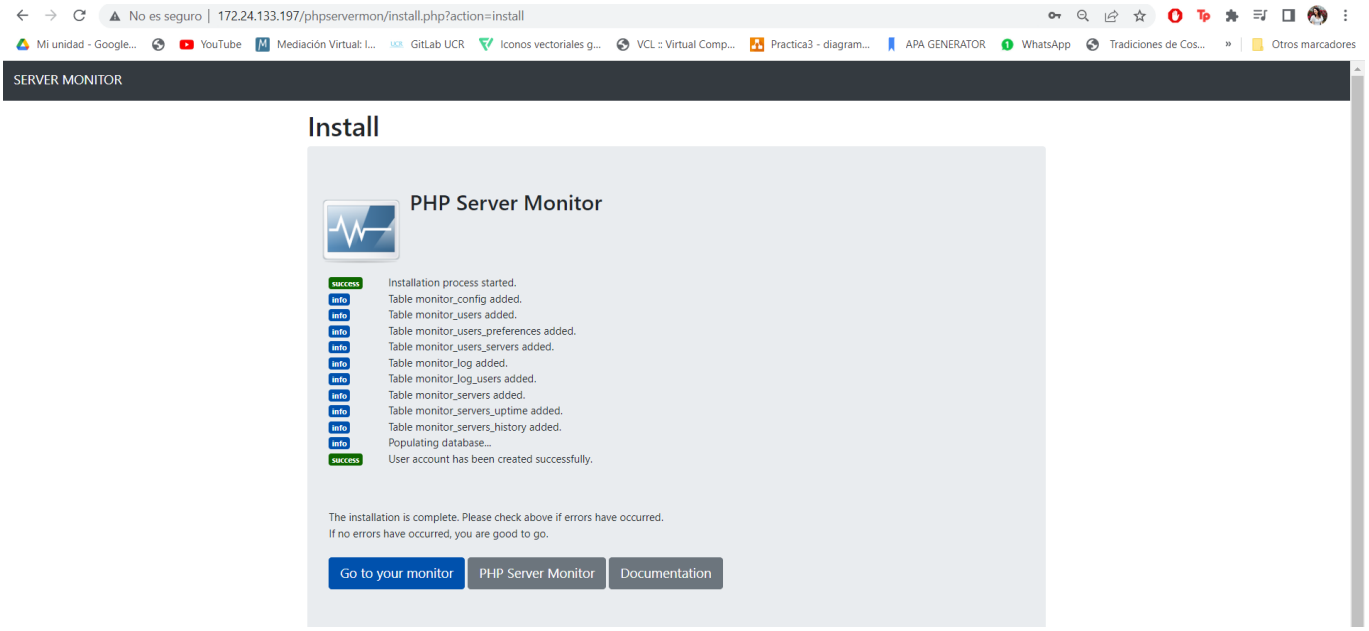
14. Rellenar con la información de la base de datos antes propuesta:



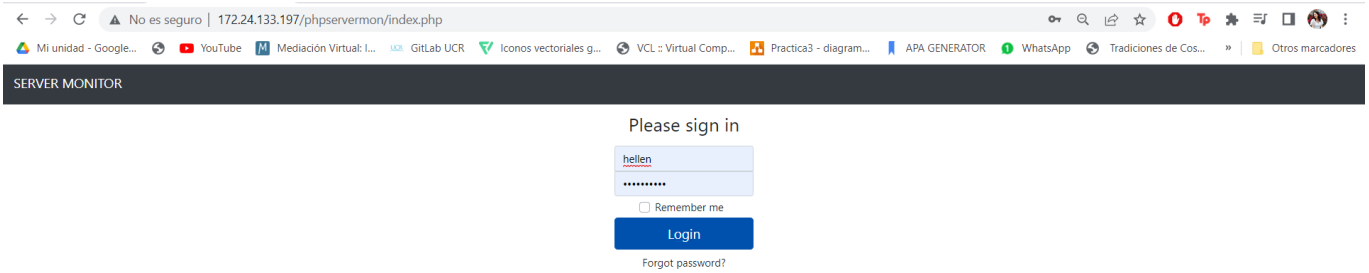
15. Cambiar los permisos de la siguiente ruta para que apache pueda acceder a ella:

```
chown -R apache:apache /var/www/html/phpservermon
```

16. Si todo está bien quedará de la siguiente manera:

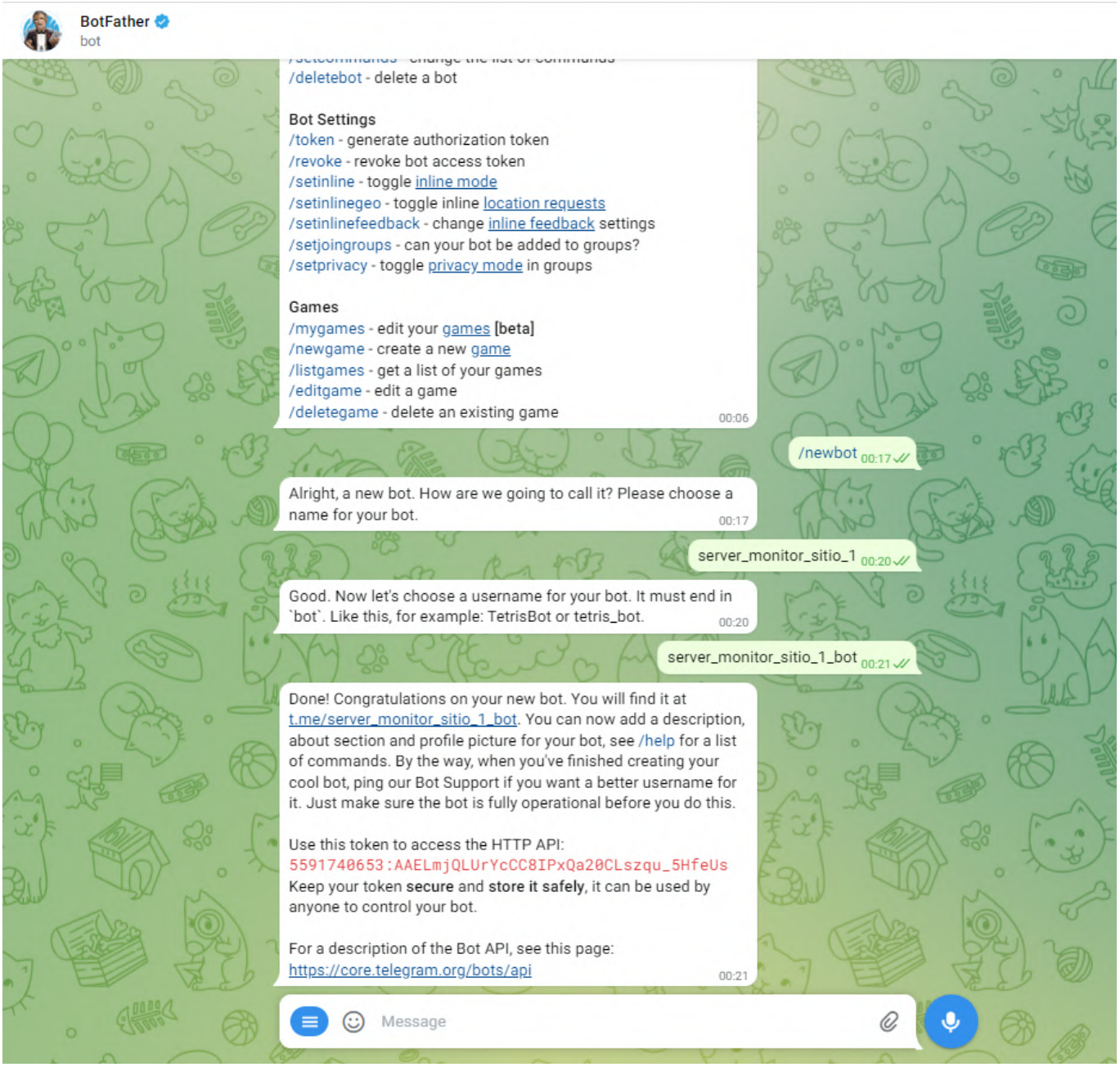


17. Iniciar sesión con el usuario previamente creado:



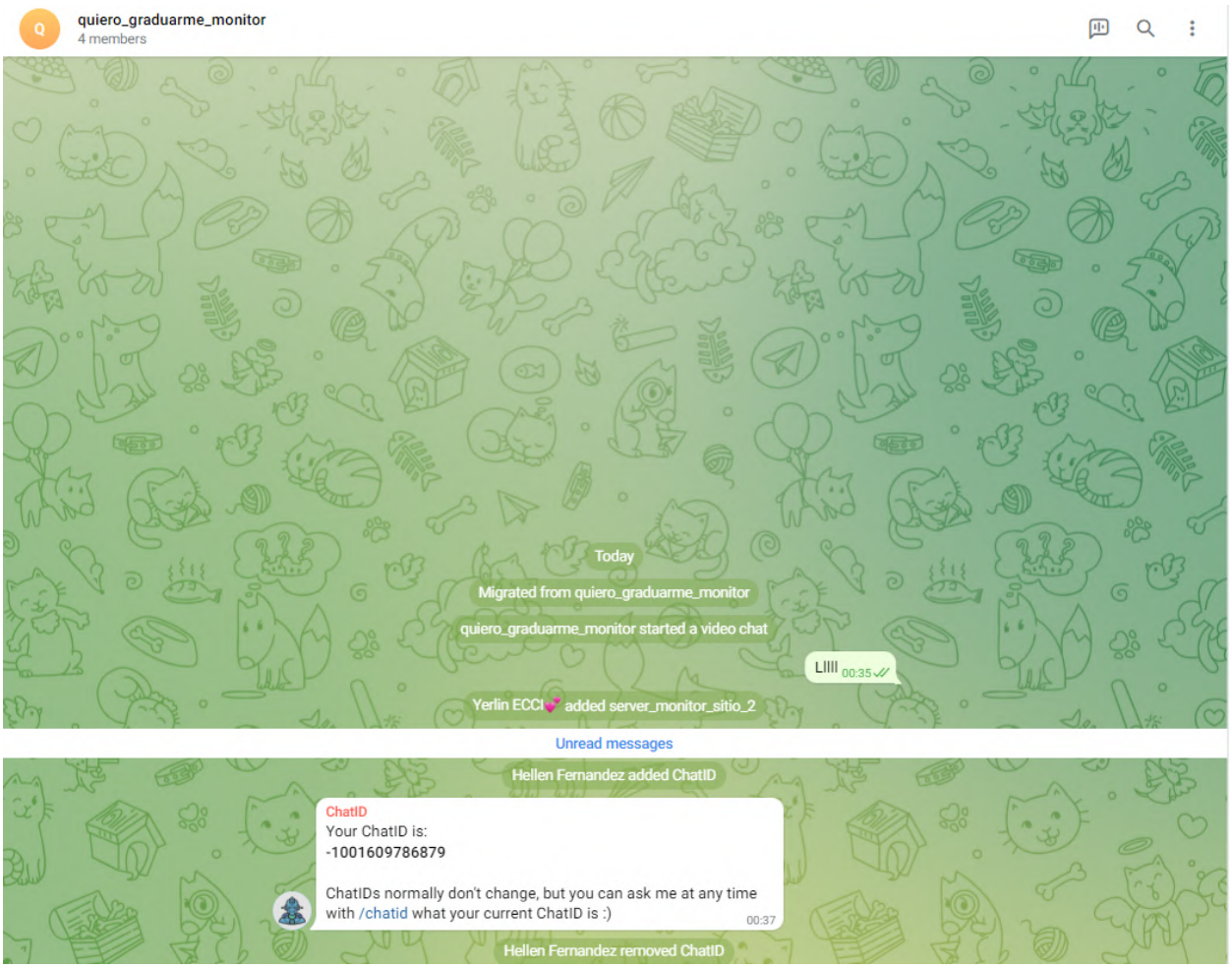
18. Si se quiere un servicio de alertas con Telegram, configure un bot de la siguiente manera: Telegram bot http://docs.phpservermonitor.org/en/latest/faq.html#notifications .

Desde Telegram ir a @botfather y escribir start, escribir /newbot escribir el nombre del nuevo bot y guardar al API token generado:



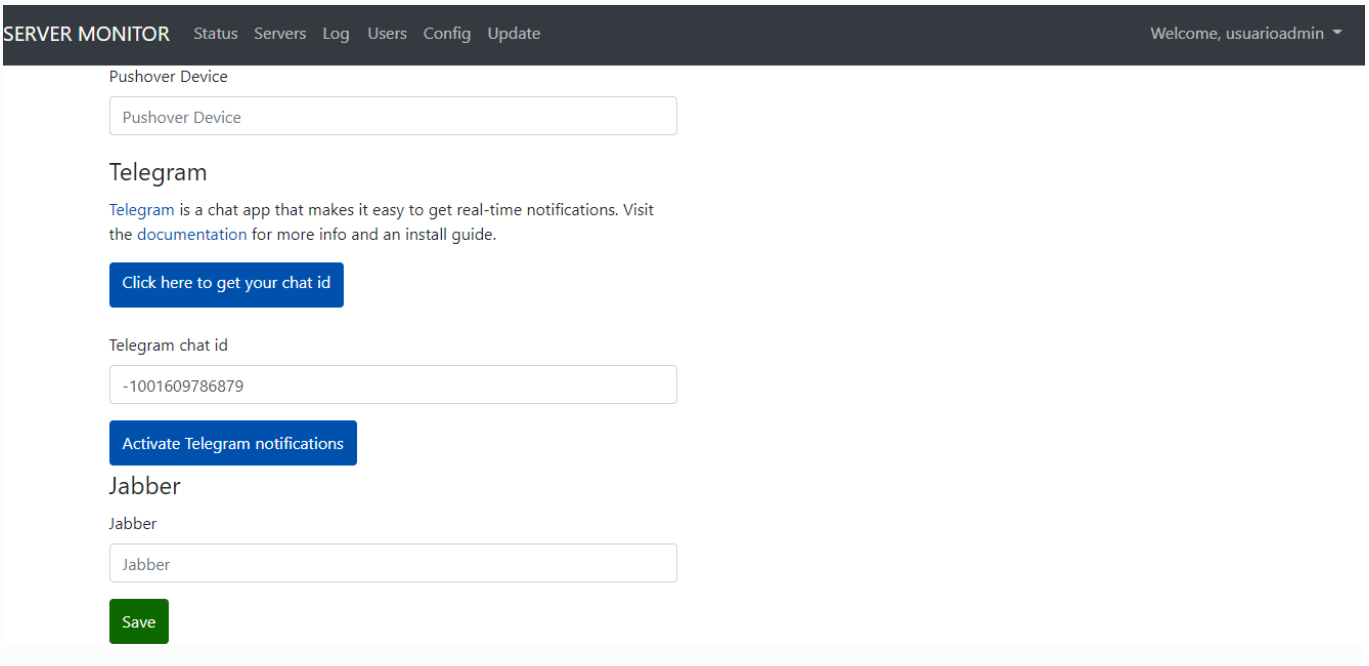

```
API sitio 2:5385663947:AAEeNVqWkM80s0QiNiQ2t8p_nwIV2i4OSAU
```

19. Para enviar notificaciones a un grupo, crear el nuevo grupo y añadir miembros en el grupo de telegram, en esta parte se añade al siguiente bot al grupo @cid_bot y salvar el chat ID:

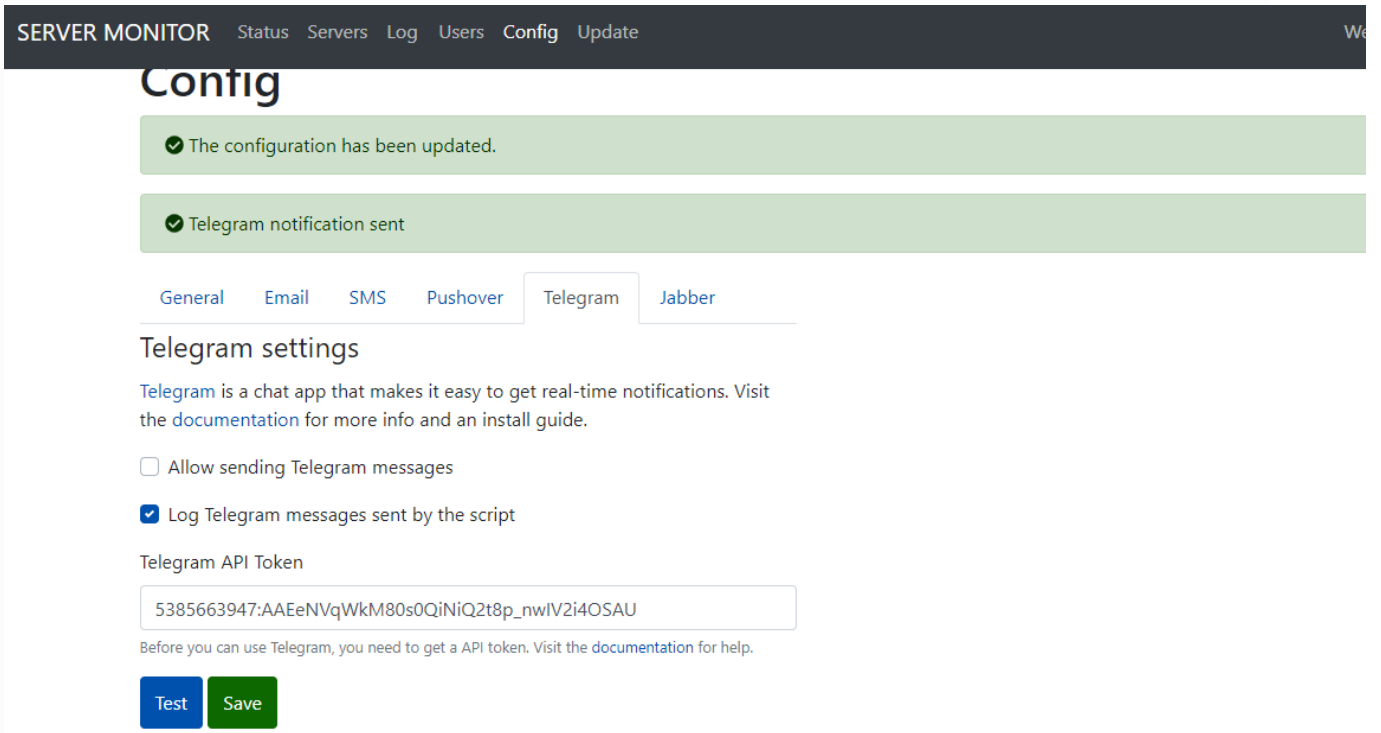


Your ChatID is: -1001609786879

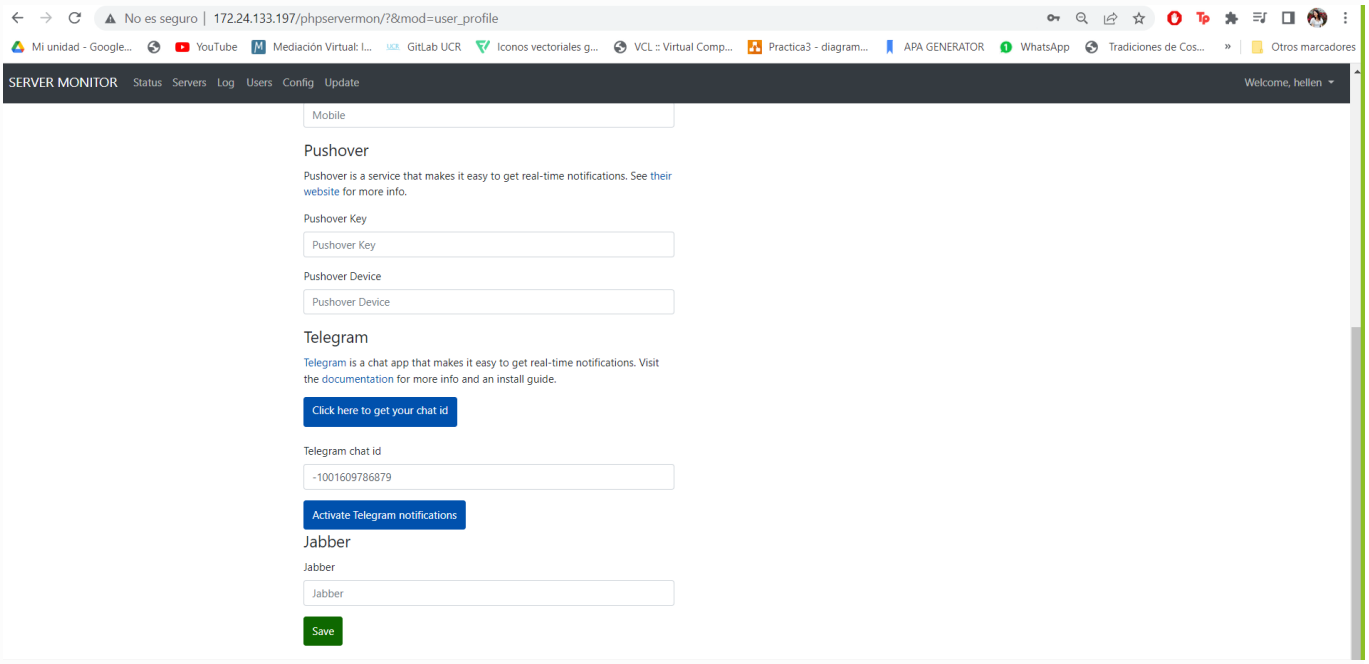
20. Eliminar al bot @cid_bot del grupo y añadir los bots que antes fueron creados.
21. En phpserver monitor en la parte de Users, y la pestaña de telegram copiar el chat id obtenido anteriormente:

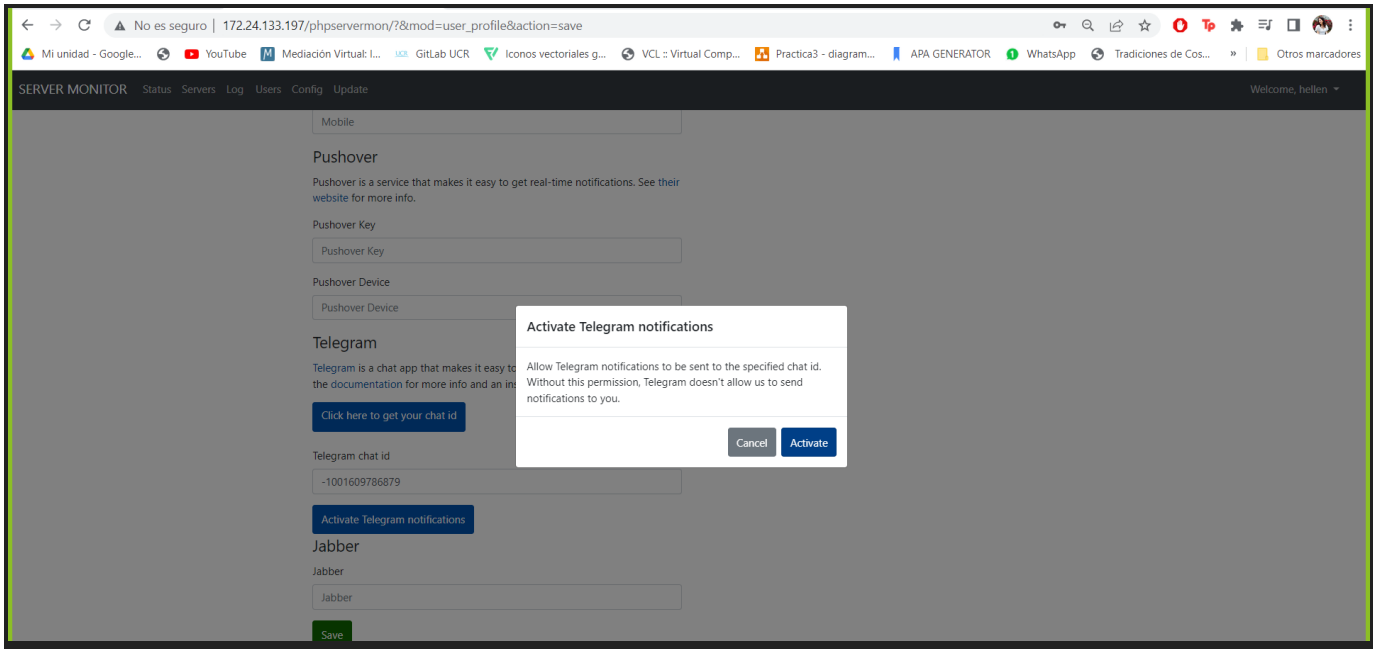


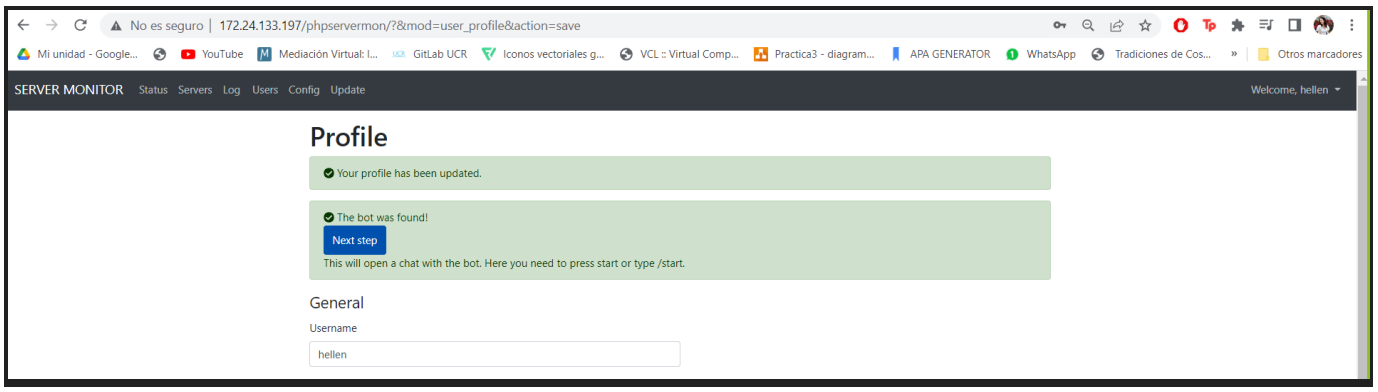
22. Ahora copar el API token, hacer una prueba y si llega una notificación de prueba al grupo significa que esto significa correctamente, en ese caso se le da save.



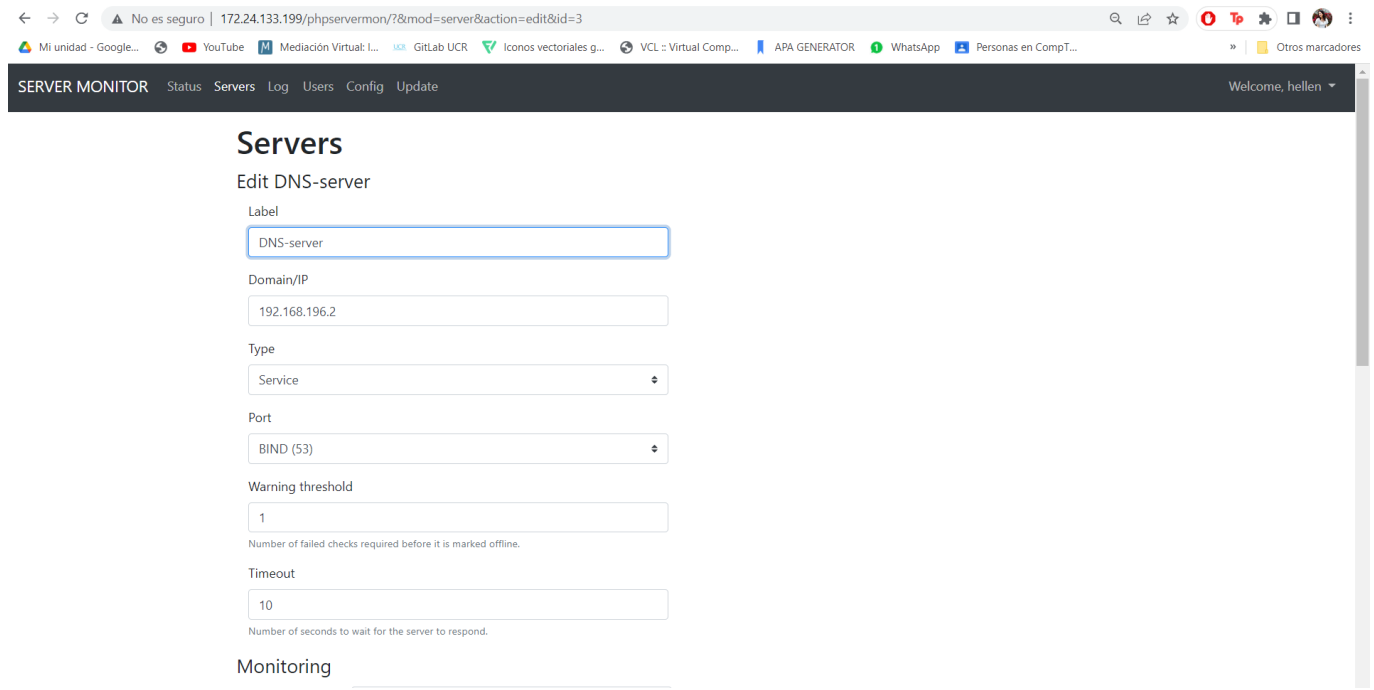
23. Se da click en activate notifications y se confima:

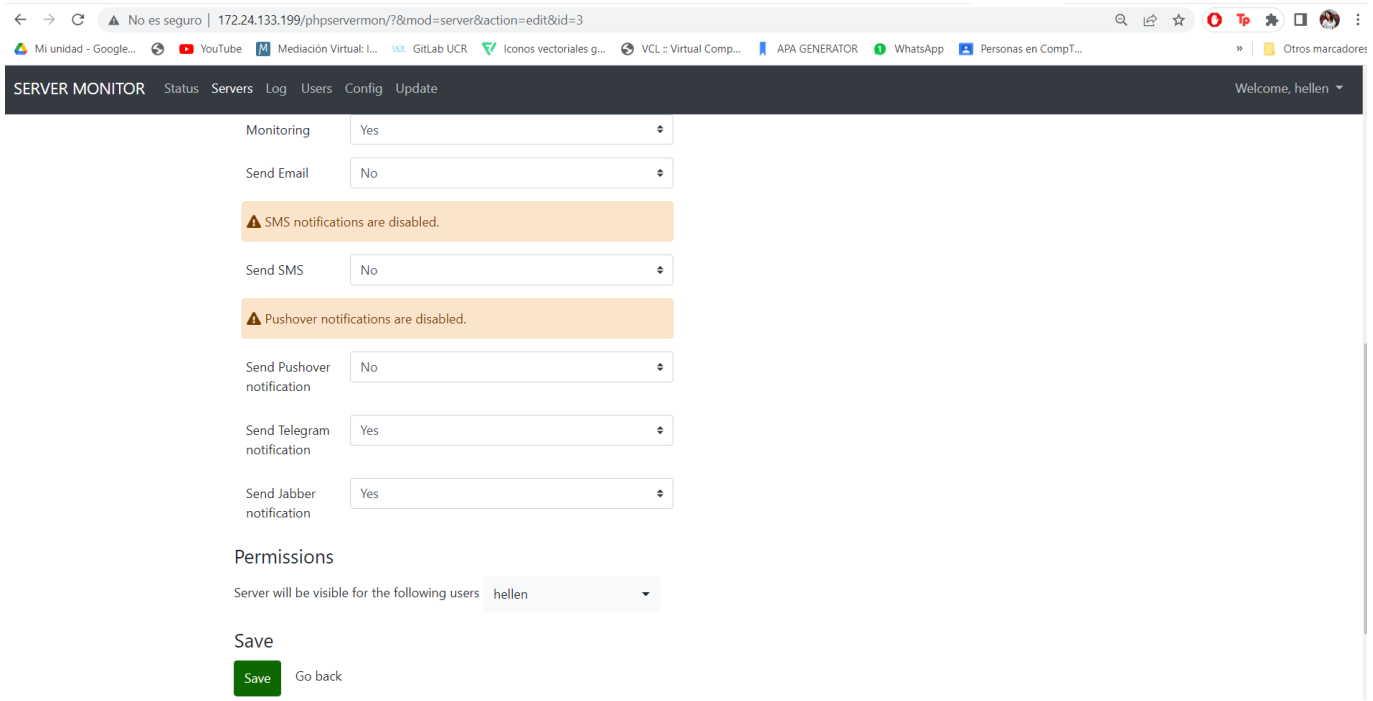


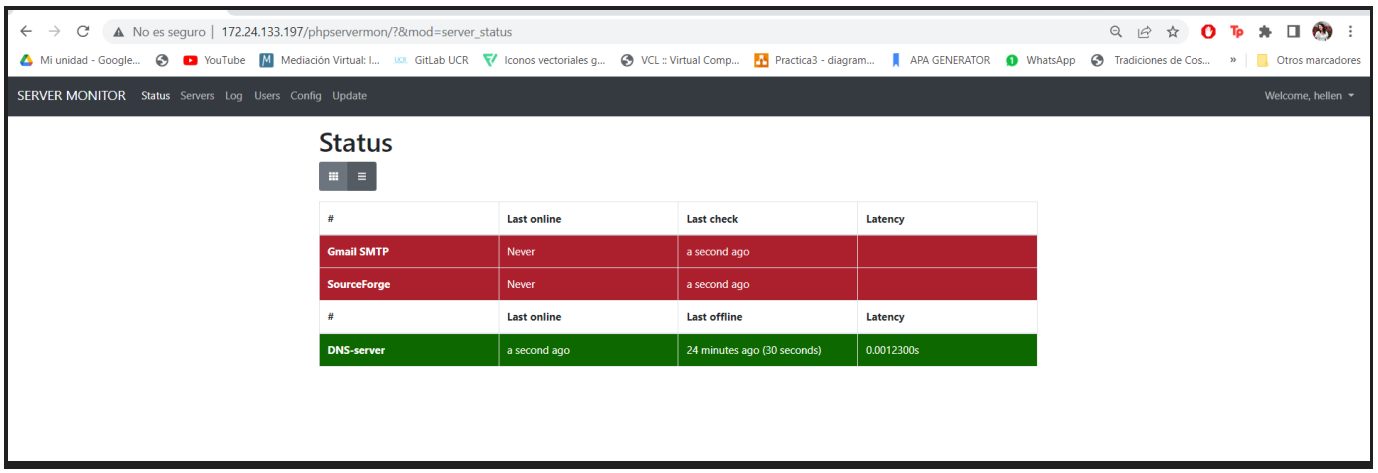




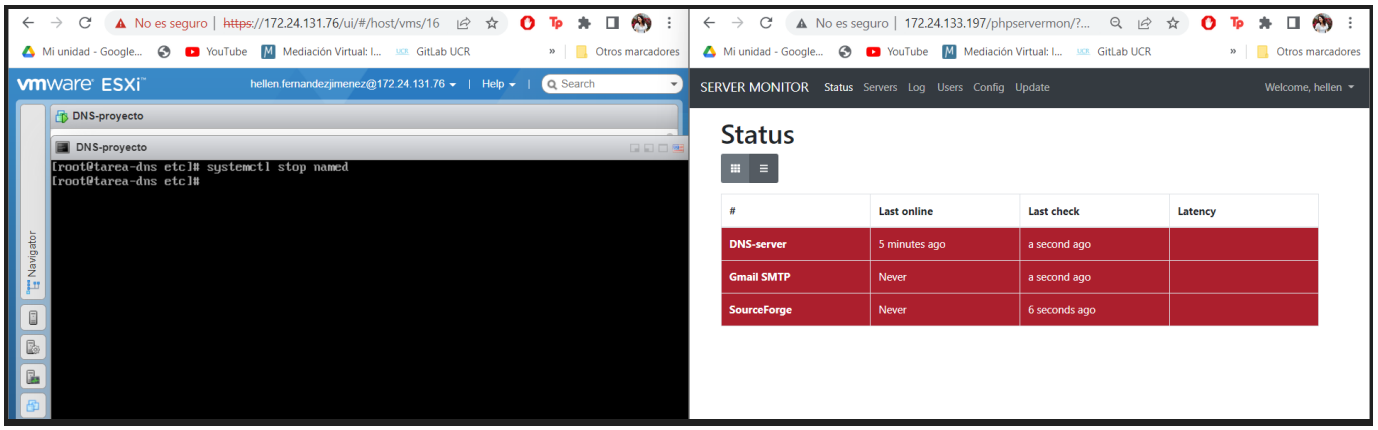
24. Añadir monitoreo al servicio de DNS de la siguiente forma y dar click en save:



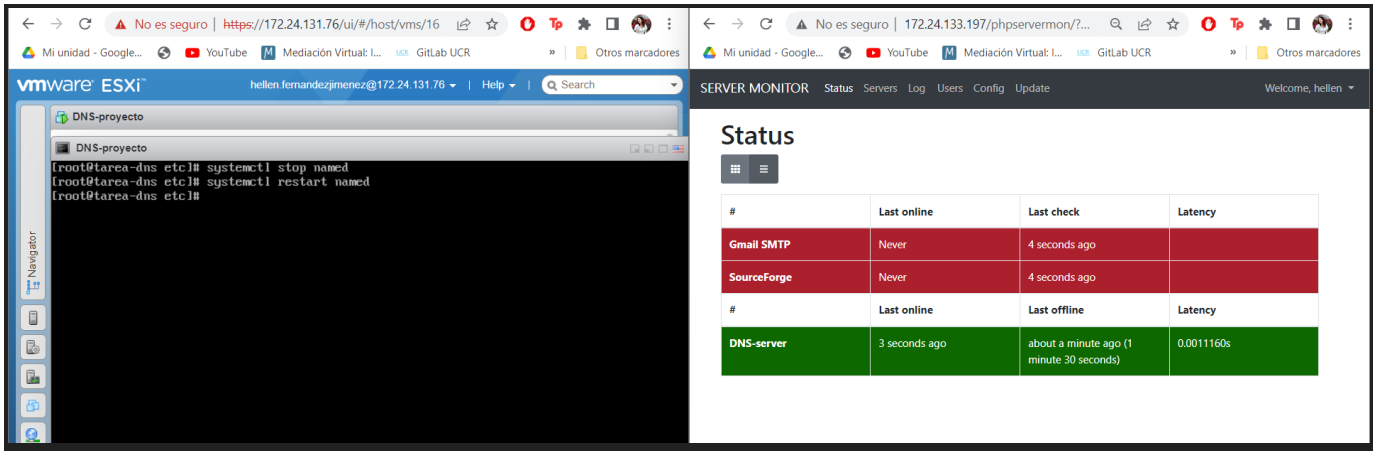


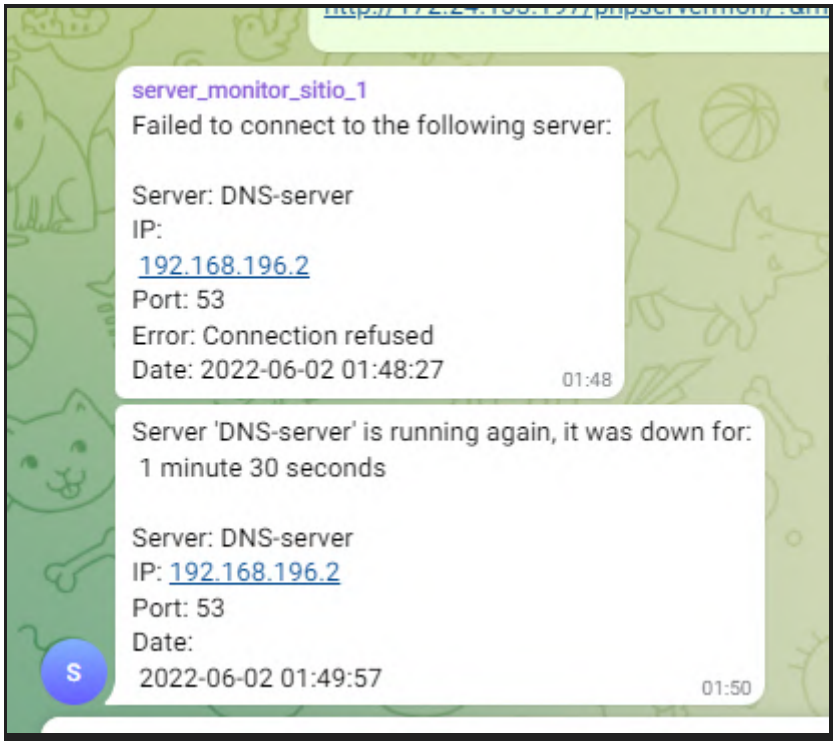


25. Asegurarse de que el servicio funciona parando el servicio de dns, en ese caso debería de verse de la siguiente forma en php monitor y llegar una notificación al grupo de Telegram creado. :



26. Restablecer el servicio y verificar que nuevamente aparezca en verde el servicio así como un nuevo mensaje telegram alertando que el servicio está corriendo nuevamente:





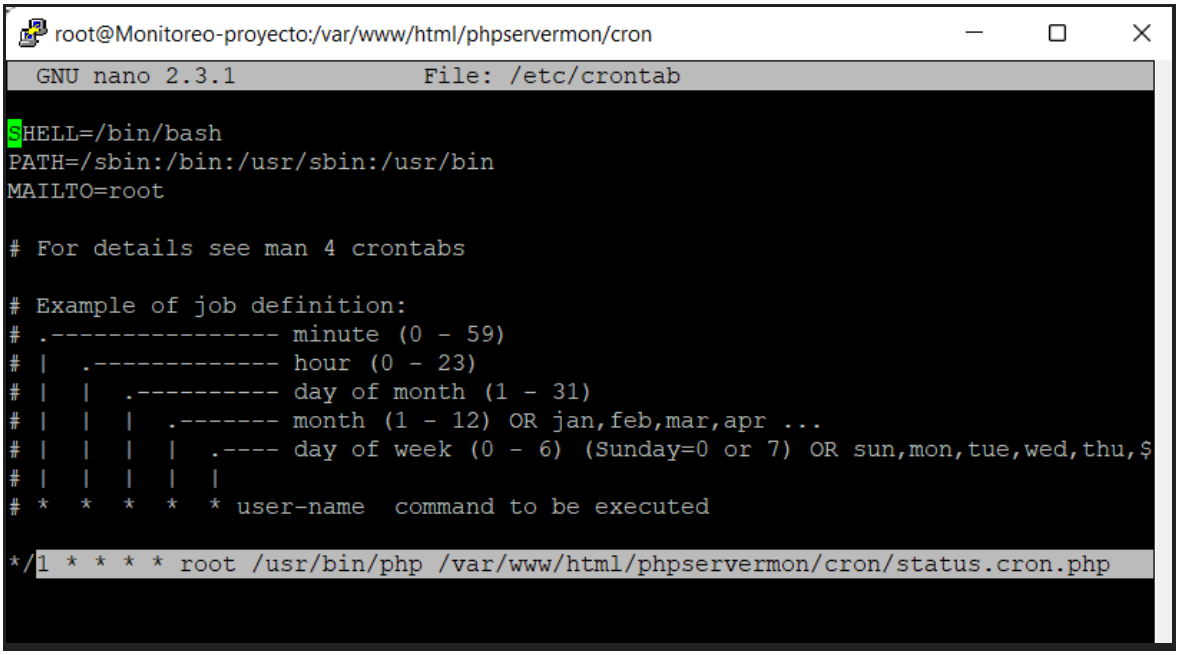
Para la interfaz web tenemos las siguientes credenciales:

Sitio	Usuario	Contraseña
Sitio1	hellen	maggielu2.
Sitio2	root	disenodiseno22

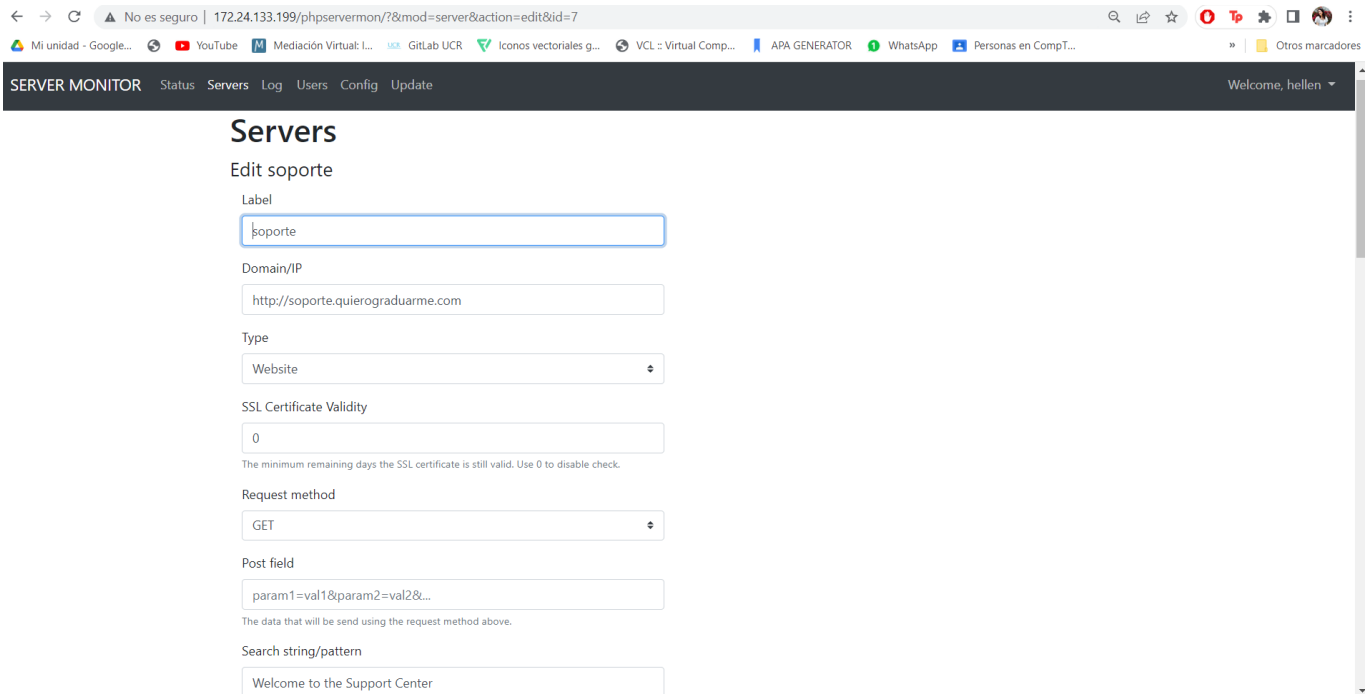
27. Agregue la siguiente el línea para que se ejecute en una frecuencia de 1 minuto el script que verifica el estado de los servidores:

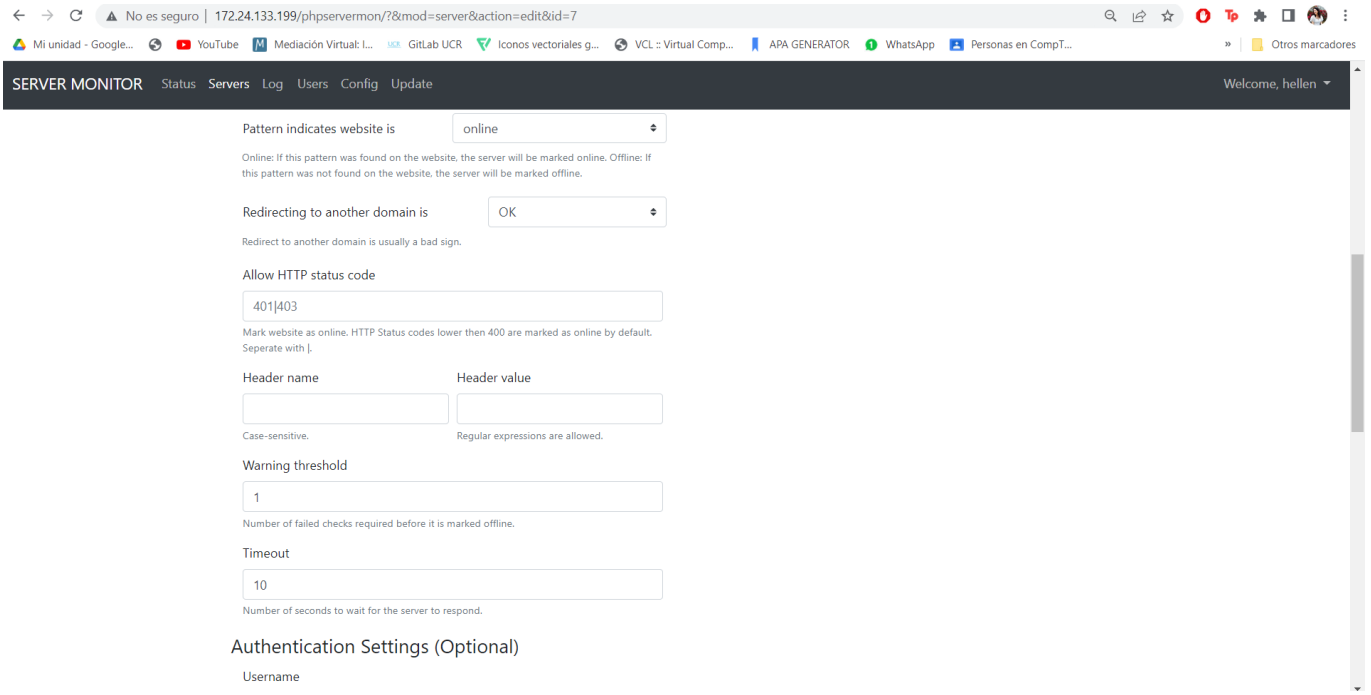
http://docs.phpservermonitor.org/en/latest/install.html

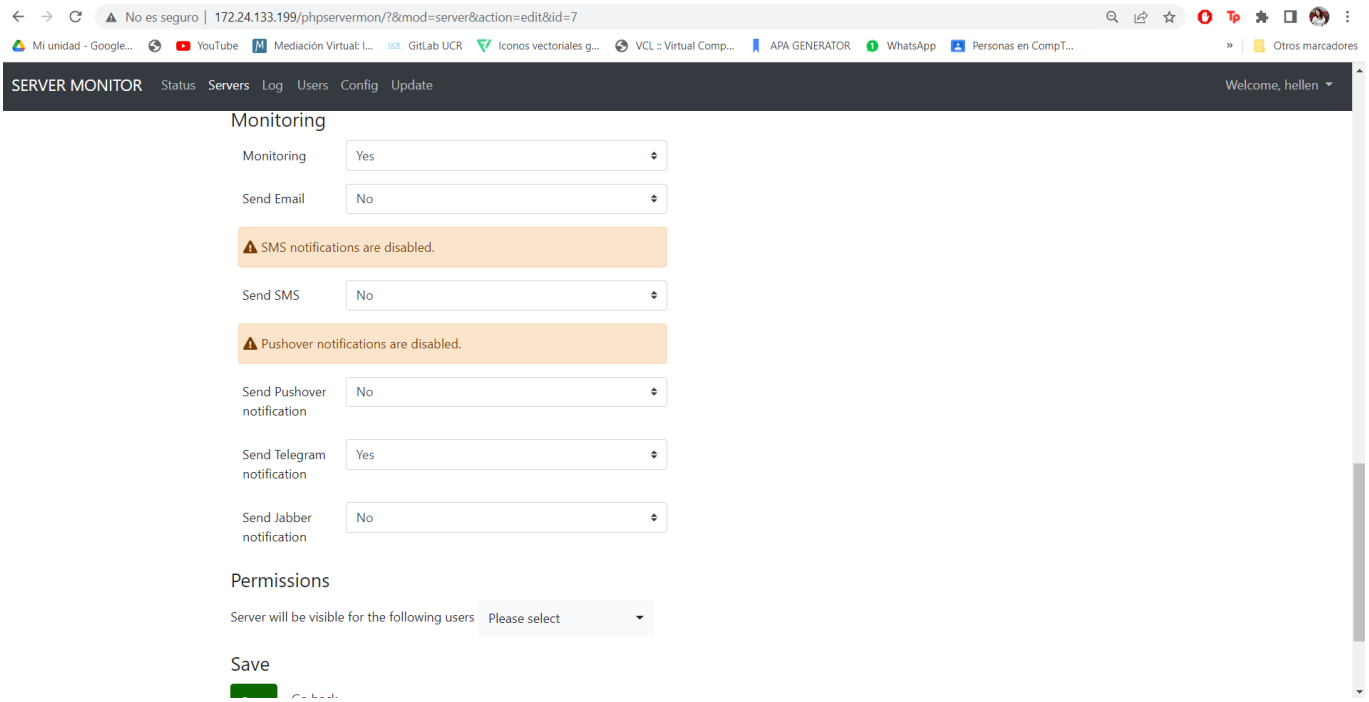
```
nano /etc/crontab
1 * * * * root /usr/bin/php /var/www/html/phpservermon/cron/status.cron.php
```



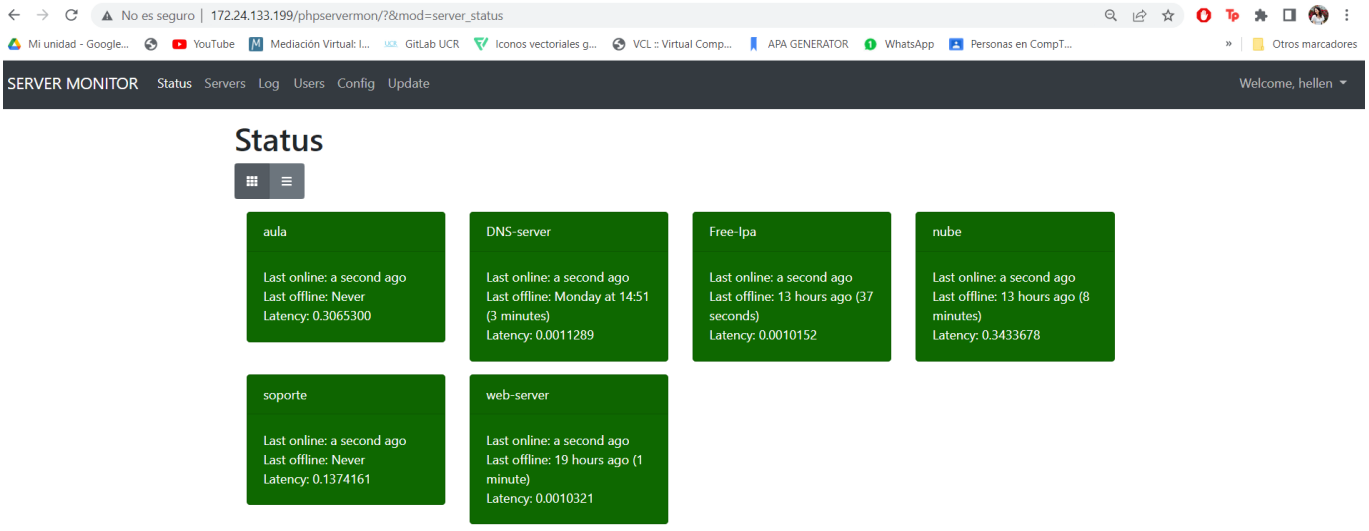
28. Monitorear un servicio web:

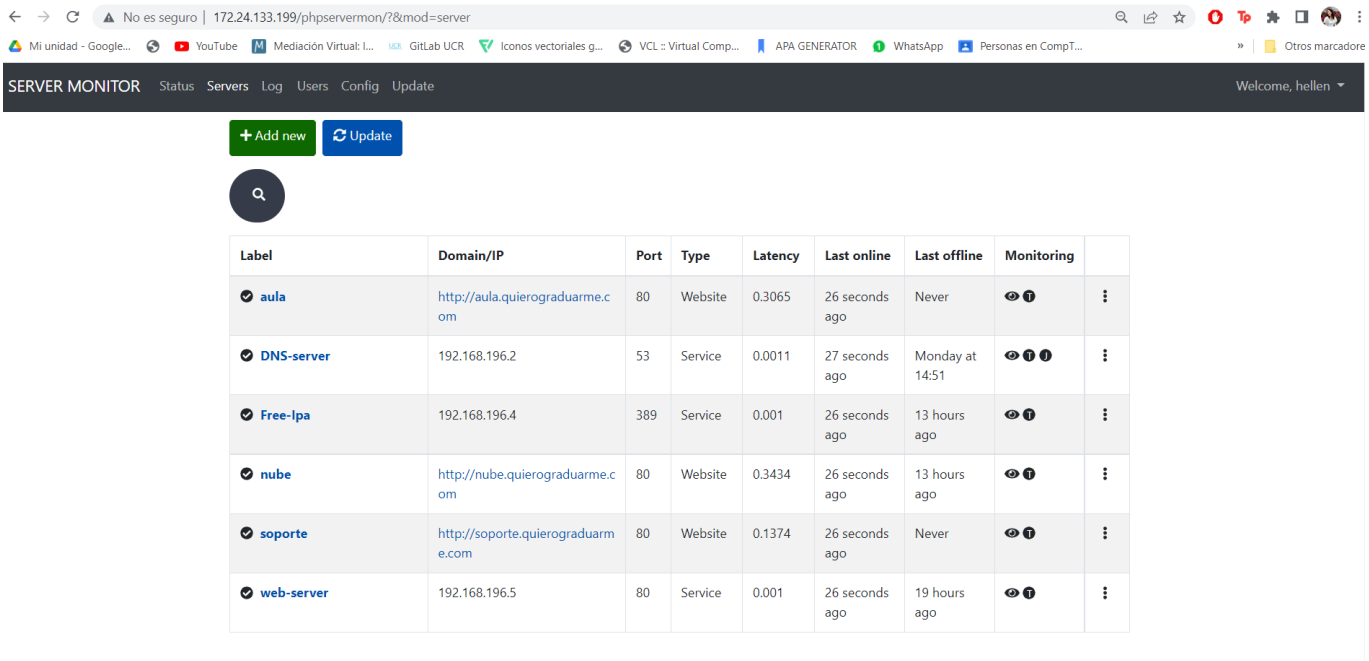

No es seguro | 172.24.133.199/phpservermon/?&mod=server&action=edit&id=7
Mi unidad - Google...
YouTube
Mediación Virtual: I...
GitLab UCR
Iconos vectoriales g...
VCL :: Virtual Comp...
APA GENERATOR
WhatsApp
Personas en CompT...
Otros marcadores
SERVER MONITOR
Status
Servers
Log
Users
Config
Update
Welcome, hellen
Servers
Edit soporte
Label
soporte
Domain/IP
http://soporte.quierograduarme.com
Type
Website
SSL Certificate Validity
0
The minimum remaining days the SSL certificate is still valid. Use 0 to disable check.
Request method
GET
Post field
param1=val1&param2=val2&...
The data that will be send using the request method above.
Search string/pattern
Welcome to the Support Center


No es seguro | 172.24.133.199/phpservermon/?&mod=server&action=edit&id=7
SERVER MONITOR
Status
Servers
Log
Users
Config
Update
Welcome, hellen
Pattern indicates website is
online
Online: If this pattern was found on the website, the server will be marked online. Offline: If this pattern was not found on the website, the server will be marked offline.
Redirecting to another domain is
OK
Redirect to another domain is usually a bad sign.
Allow HTTP status code
401|403
Mark website as online. HTTP Status codes lower then 400 are marked as online by default. Seperate with |.
Header name
Header value
Case-sensitive.
Regular expressions are allowed.
Warning threshold
1
Number of failed checks required before it is marked offline.
Timeout
10
Number of seconds to wait for the server to respond.
Authentication Settings (Optional)
Username



29. Así se ve al final todos los servicios que están siendo monitoreados:

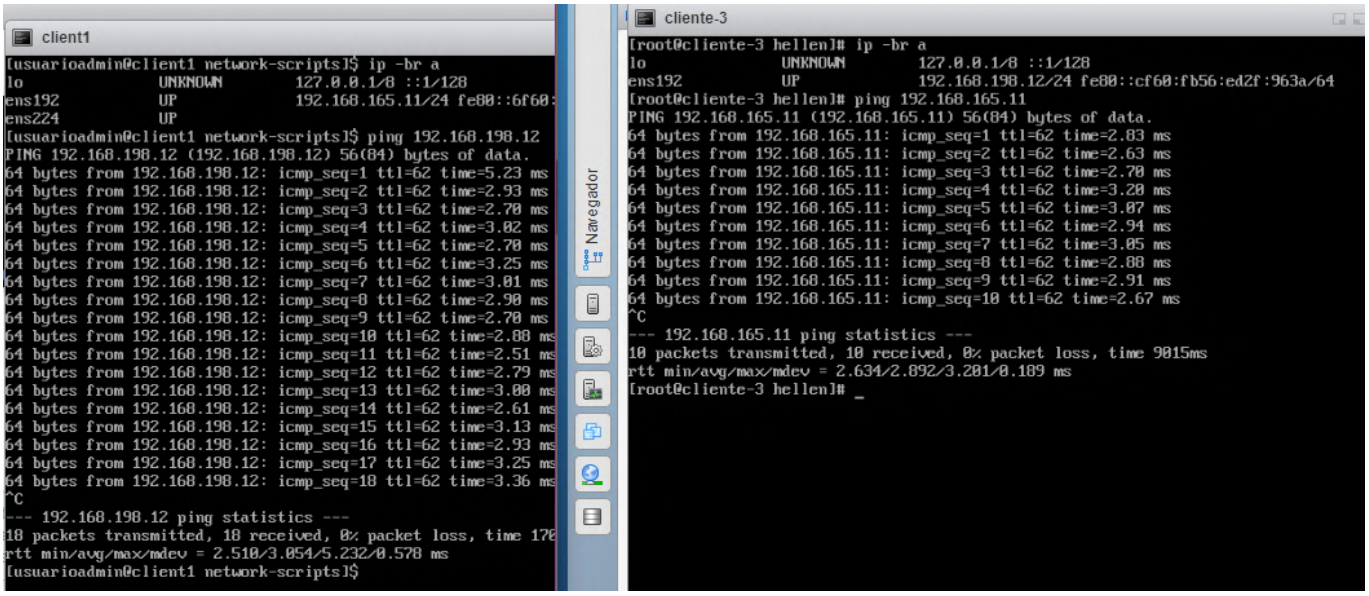




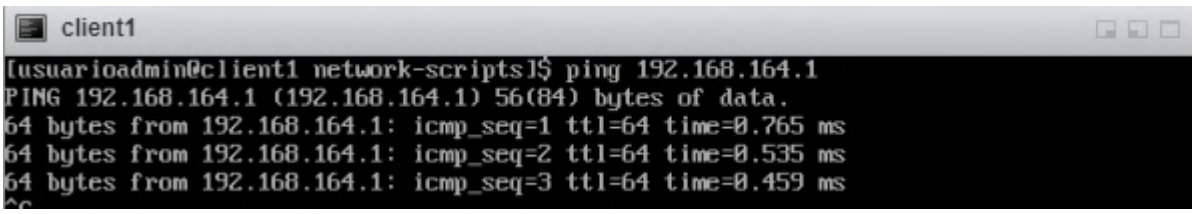
Label	Domain/IP	Port	Type	Latency	Last online	Last offline	Monitoring
aula	http://aula.quierograduarme.com	80	Website	0.3065	26 seconds ago	Never	
DNS-server	192.168.196.2	53	Service	0.0011	27 seconds ago	Monday at 14:51	
Free-Ipa	192.168.196.4	389	Service	0.001	26 seconds ago	13 hours ago	
nube	http://nube.quierograduarme.com	80	Website	0.3434	26 seconds ago	13 hours ago	
soporte	http://soporte.quierograduarme.com	80	Website	0.1374	26 seconds ago	Never	
web-server	192.168.196.5	80	Service	0.001	26 seconds ago	19 hours ago	

Pruebas

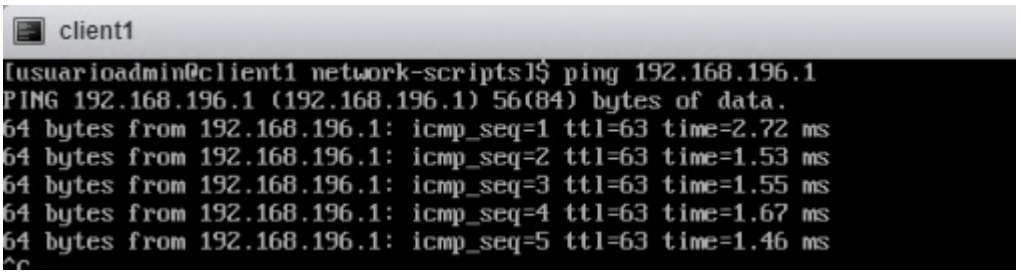
Cliente sitio 1 a cliente sitio 2



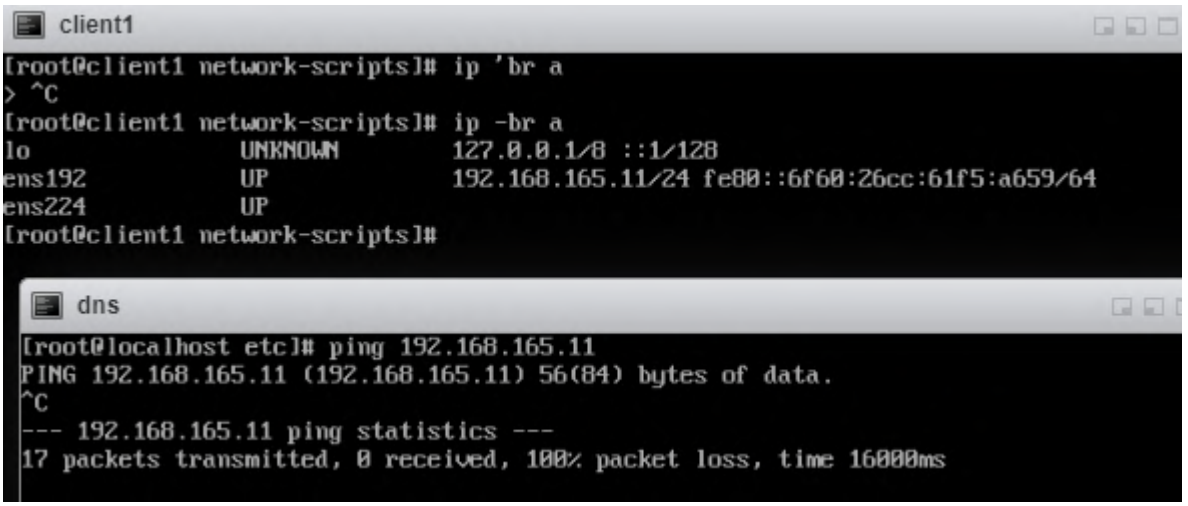
Cliente sitio 1 a DMZ sitio 1



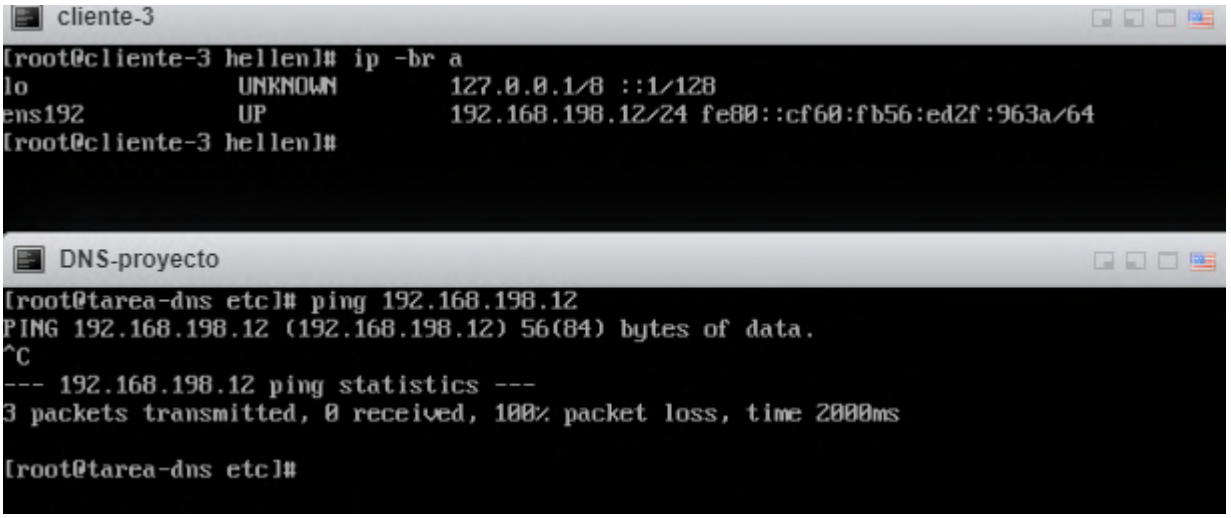
Cliente sitio 1 a DMZ sitio 2



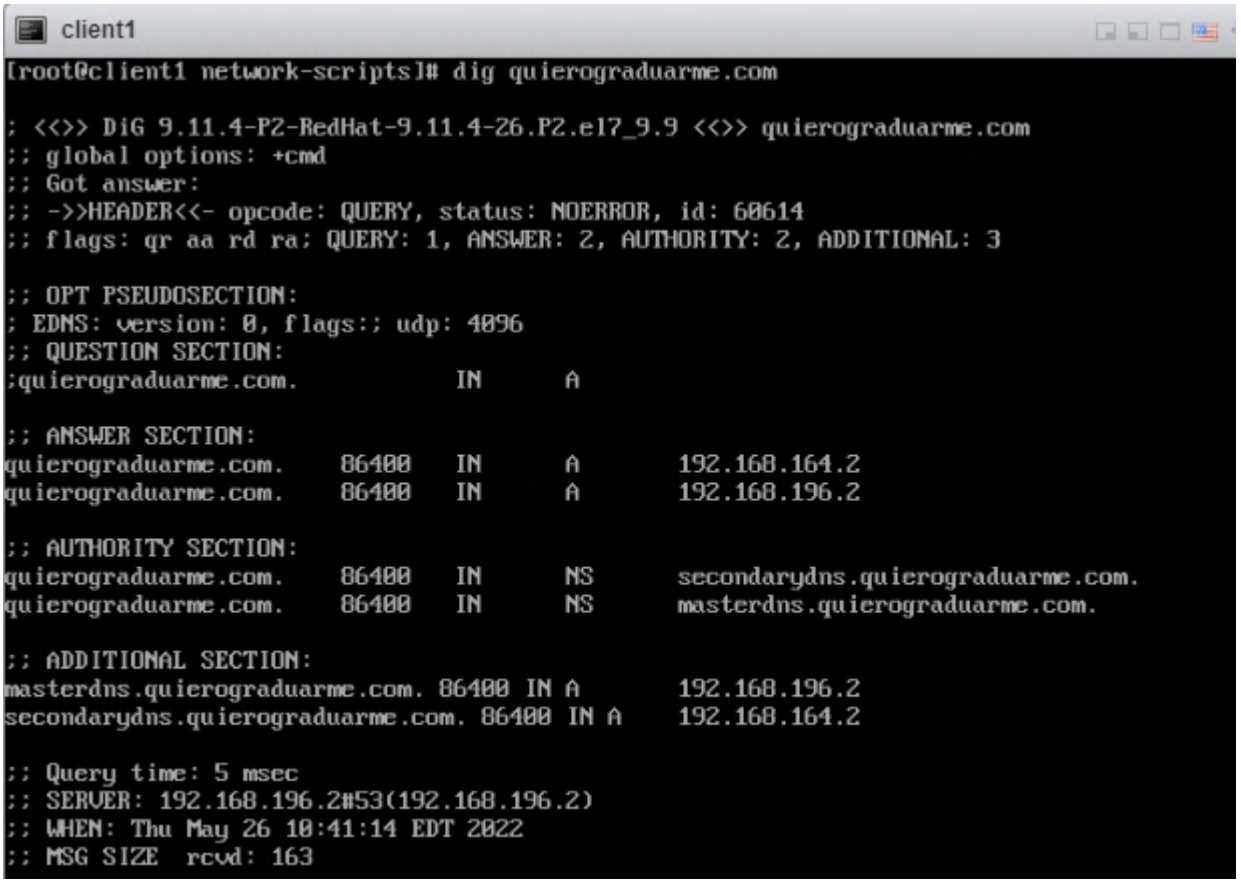
DMZ sitio 1 a cliente sitio 1



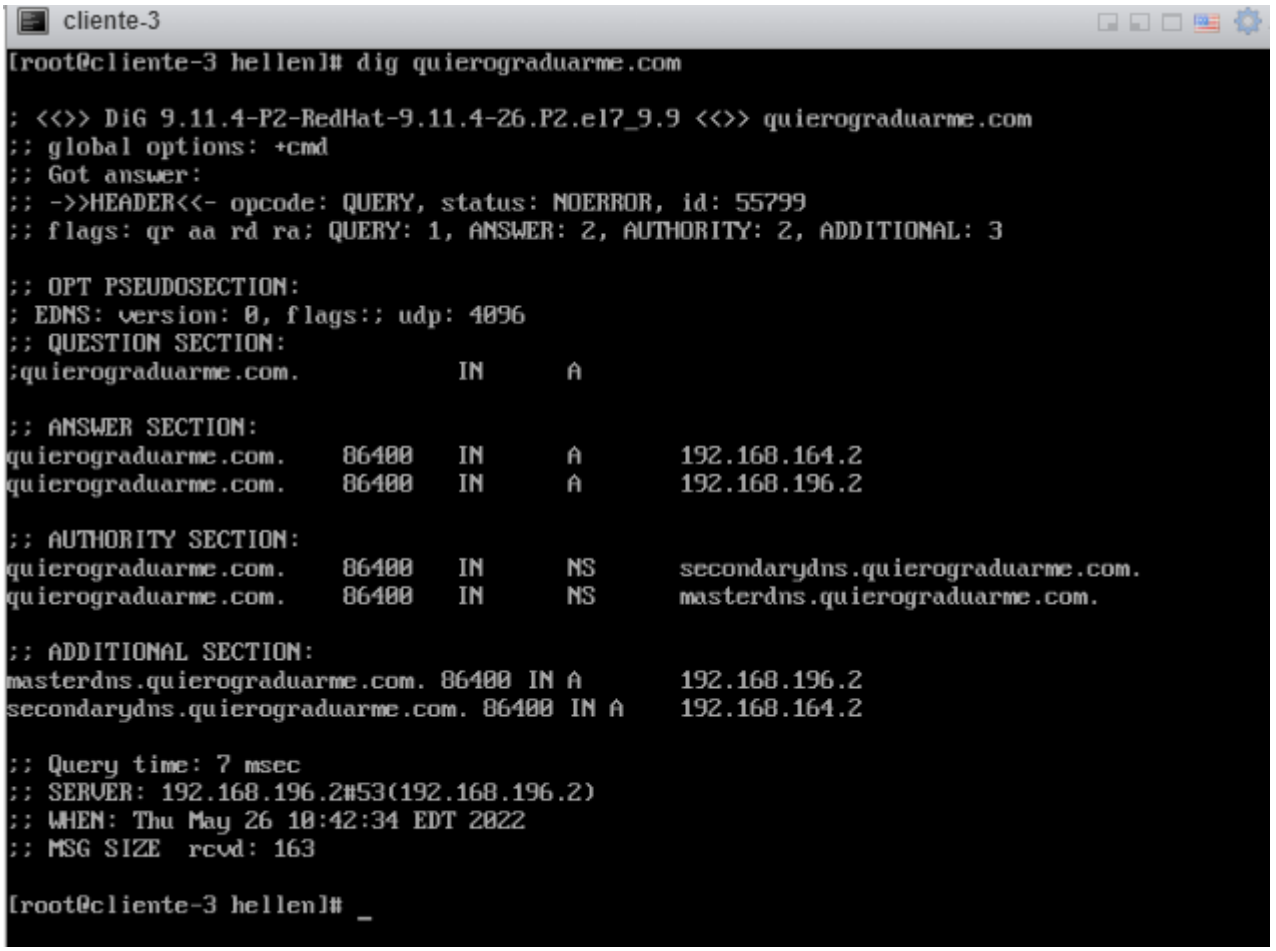
DMZ sitio 2 a cliente sitio 2



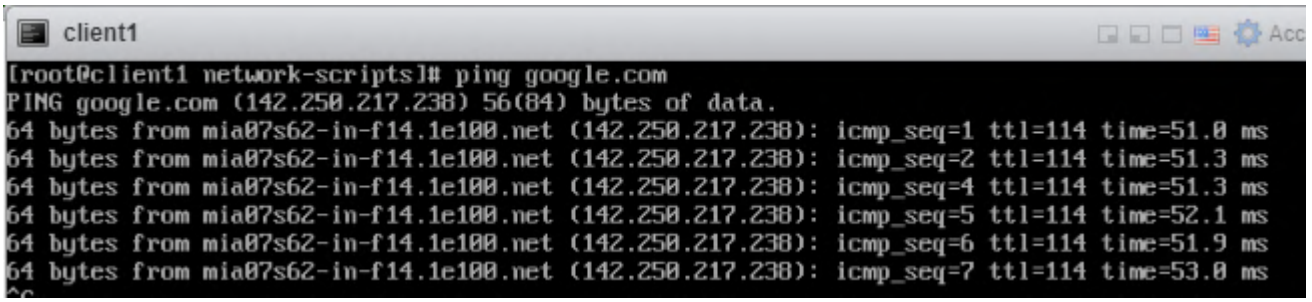
Cliente sitio 1 a DNS



Cliente sitio 2 a DNS



Cliente sitio 1 a internet



client1

```
[root@client1 network-scripts]# ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens192           UP             192.168.165.11/24 fe80::6f60:26cc:61f5:a659/64
ens224           UP
[root@client1 network-scripts]# sudo yum install nc -y
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.ueb.edu.ec
 * extras: mirror.ueb.edu.ec
 * updates: mirror.ueb.edu.ec
Package 2:nmap-ncat-6.40-19.el7.x86_64 already installed and latest version
Nothing to do
[root@client1 network-scripts]# _
```

Cliente sitio 2 a internet

cliente-3

```
[root@cliente-3 hellen]# ping google.com
PING google.com (142.250.217.238) 56(84) bytes of data.
64 bytes from mia07s62-in-f14.1e100.net (142.250.217.238): icmp_seq=1 ttl=114 time=51.8 ms
64 bytes from mia07s62-in-f14.1e100.net (142.250.217.238): icmp_seq=2 ttl=114 time=52.7 ms
64 bytes from mia07s62-in-f14.1e100.net (142.250.217.238): icmp_seq=3 ttl=114 time=53.1 ms
64 bytes from mia07s62-in-f14.1e100.net (142.250.217.238): icmp_seq=4 ttl=114 time=52.0 ms
```

cliente-3

```
[root@cliente-3 hellen]# ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens192           UP             192.168.198.12/24 fe80::cf60:fb56:ed2f:963a/64
[root@cliente-3 hellen]# sudo yum install nc -y
Loaded plugins: fastestmirror
Determining fastest mirrors
 * base: mirror.unimagdalena.edu.co
 * extras: mirror.unimagdalena.edu.co
 * updates: mirror.unimagdalena.edu.co
base                                                     | 3.6 kB  00:00:00
extras                                                   | 2.9 kB  00:00:00
updates                                                  | 2.9 kB  00:00:00
Package 2:nmap-ncat-6.40-19.el7.x86_64 already installed and latest version
Nothing to do
[root@cliente-3 hellen]# _
```

Internet a DNS

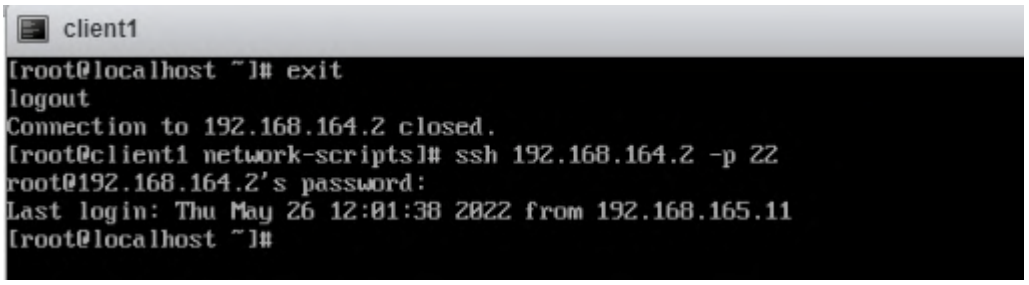
server2 — Acciones

```
ens224: connected to UCR_NETWORK
        "VMware VMXNET3"
        ethernet (vmxnet3), 00:0C:29:71:C3:B4, hw, mtu 1500
        ip4 default
        inet4 172.24.133.166/24
        route4 0.0.0.0/0
        route4 172.24.133.0/24
        inet6 fe80::c412:f2d5:ea8d:2750/64
        route6 fe80::/64
        route6 ff00::/8

ens192: connected to PRIVATE_NETWORK
        "VMware VMXNET3"
        ethernet (vmxnet3), 00:0C:29:71:C3:AA, hw, mtu 1500
        inet4 192.168.166.1/24
        route4 192.168.166.0/24
        inet6 fe80::3e73:7639:caf5:6733/64
        route6 fe80::/64
        route6 ff00::/8

ens256: connected to NAC
        "VMware VMXNET3"
        ethernet (vmxnet3), 00:0C:29:71:C3:BE, hw, mtu 1500
        inet4 172.24.5.166/24
        route4 172.24.5.0/24
        inet6 fe80::3a15:4369:a4e8:b6b7/64
        route6 fe80::/64
        route6 ff00::/8

lo: unmanaged
        "lo"
        loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536

DNS configuration:
        servers: 172.24.133.197 172.24.133.165
        interface: ens224
```

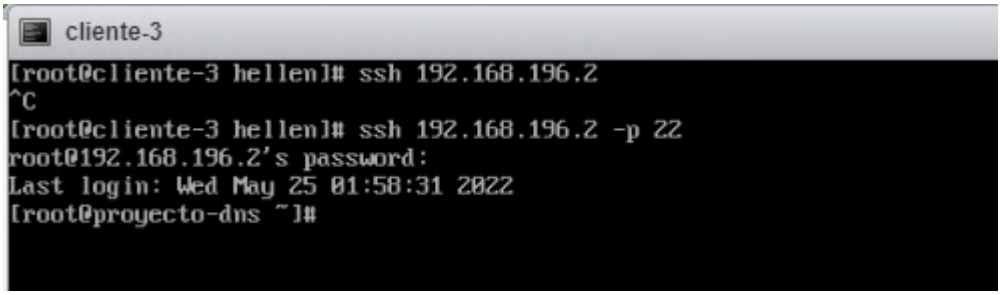
server2 — Acciones

```
[usuarioadmin@server2 ~]$ dig quierograduarme.com

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> quierograduarme.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34948
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;quierograduarme.com.           IN      A

;; ANSWER SECTION:
quierograduarme.com.    86400   IN      A       192.168.164.2
quierograduarme.com.    86400   IN      A       192.168.196.2

;; AUTHORITY SECTION:
quierograduarme.com.    86400   IN      NS      secondarydns.quierograduarme.com.
quierograduarme.com.    86400   IN      NS      masterdns.quierograduarme.com.

;; ADDITIONAL SECTION:
masterdns.quierograduarme.com. 86400 IN A       192.168.196.2
secondarydns.quierograduarme.com. 86400 IN A    192.168.164.2

;; Query time: 4 msec
;; SERVER: 172.24.133.197#53(172.24.133.197)
;; WHEN: Thu May 26 10:50:49 EDT 2022
;; MSG SIZE  rcvd: 163

[usuarioadmin@server2 ~]$
```

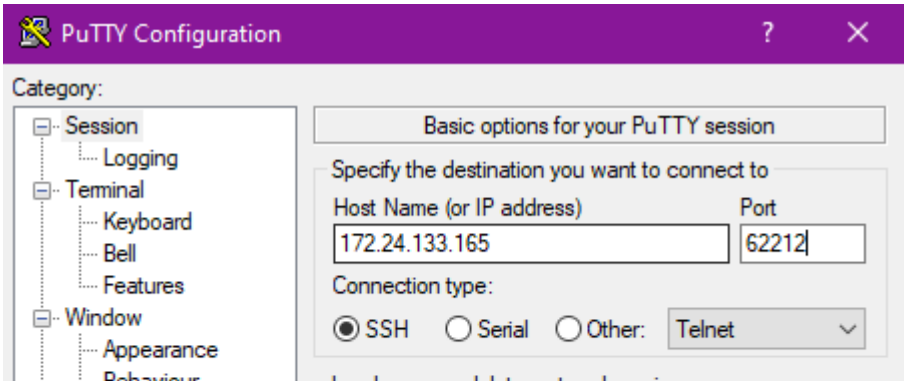
SSH cliente sitio 1 a DNS

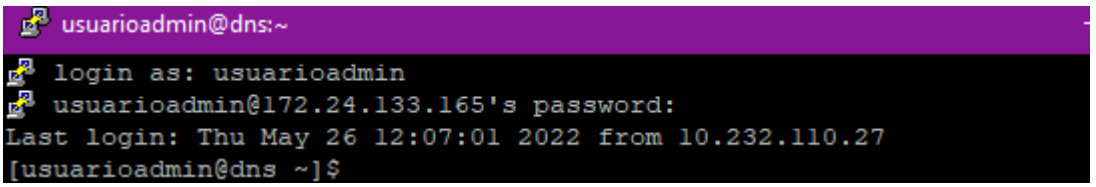


SSH cliente sitio 2 a DNS

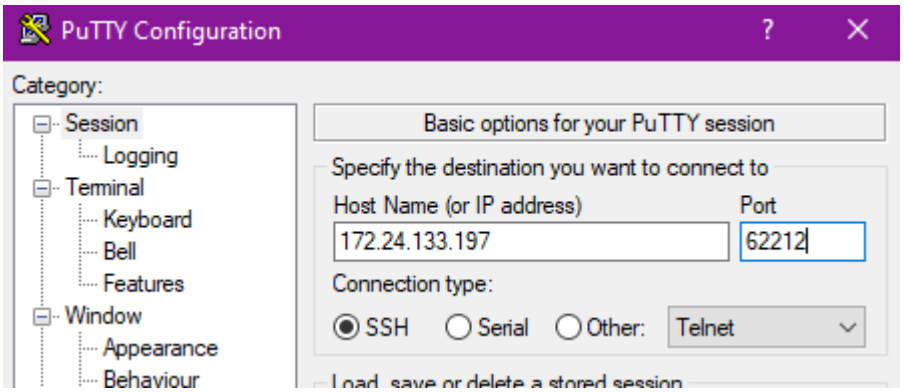


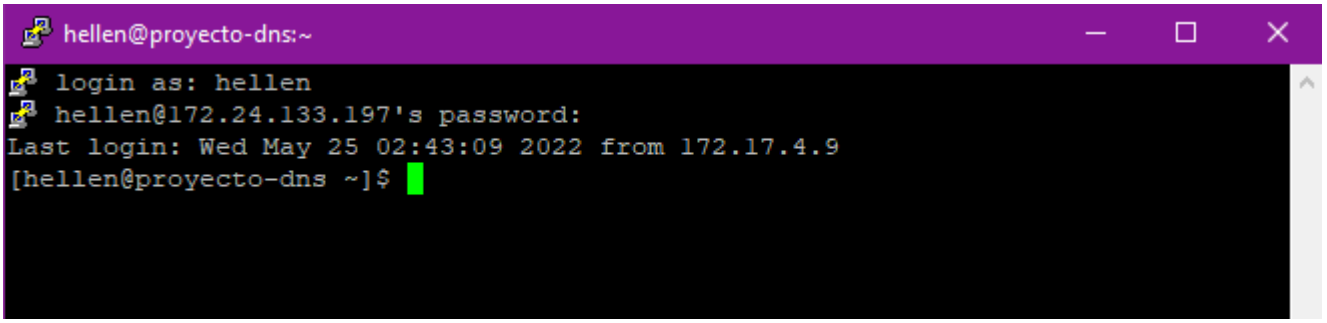
SSH internet a DNS sitio 1





SSH internet a DNS sitio 2

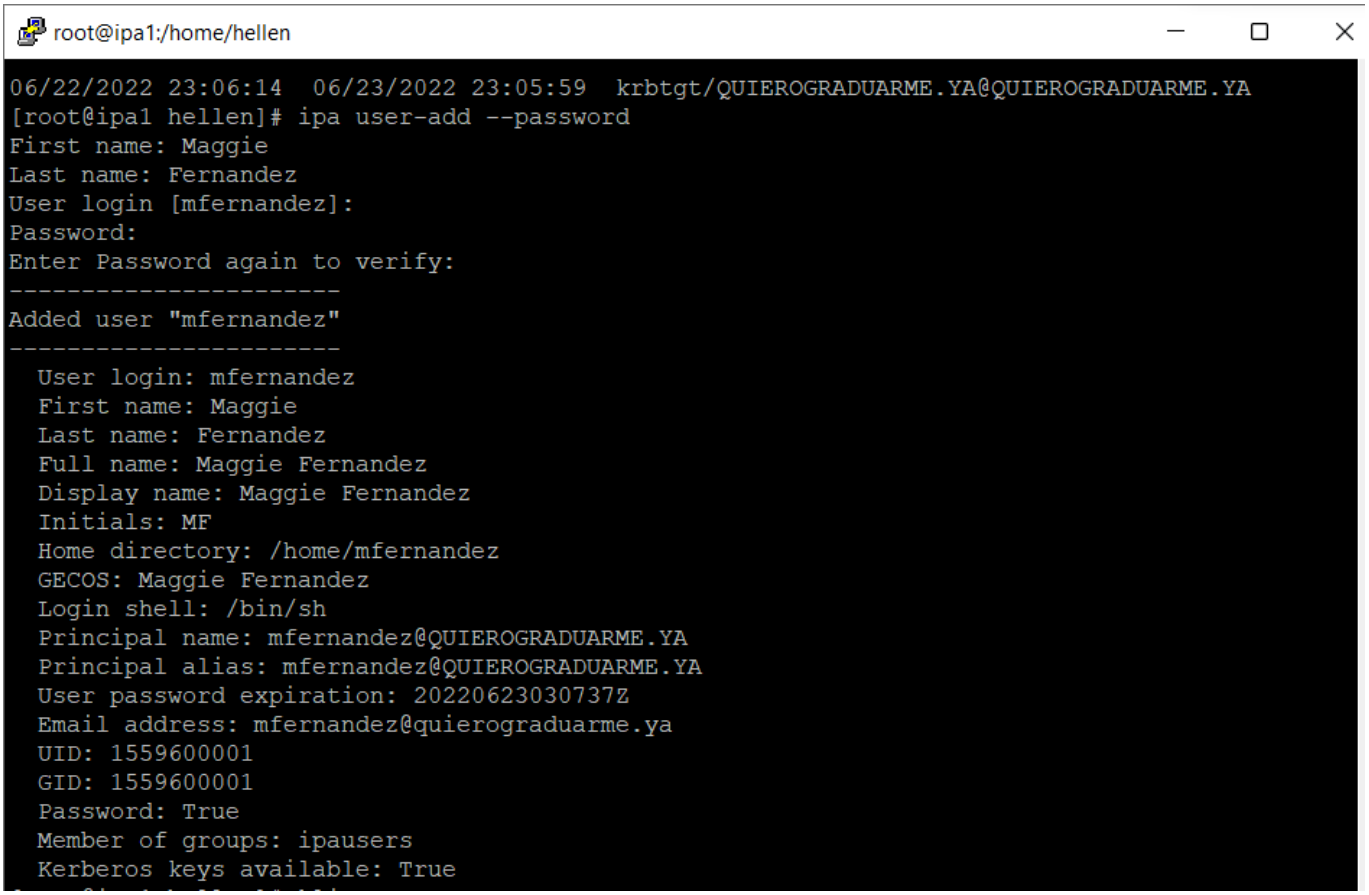




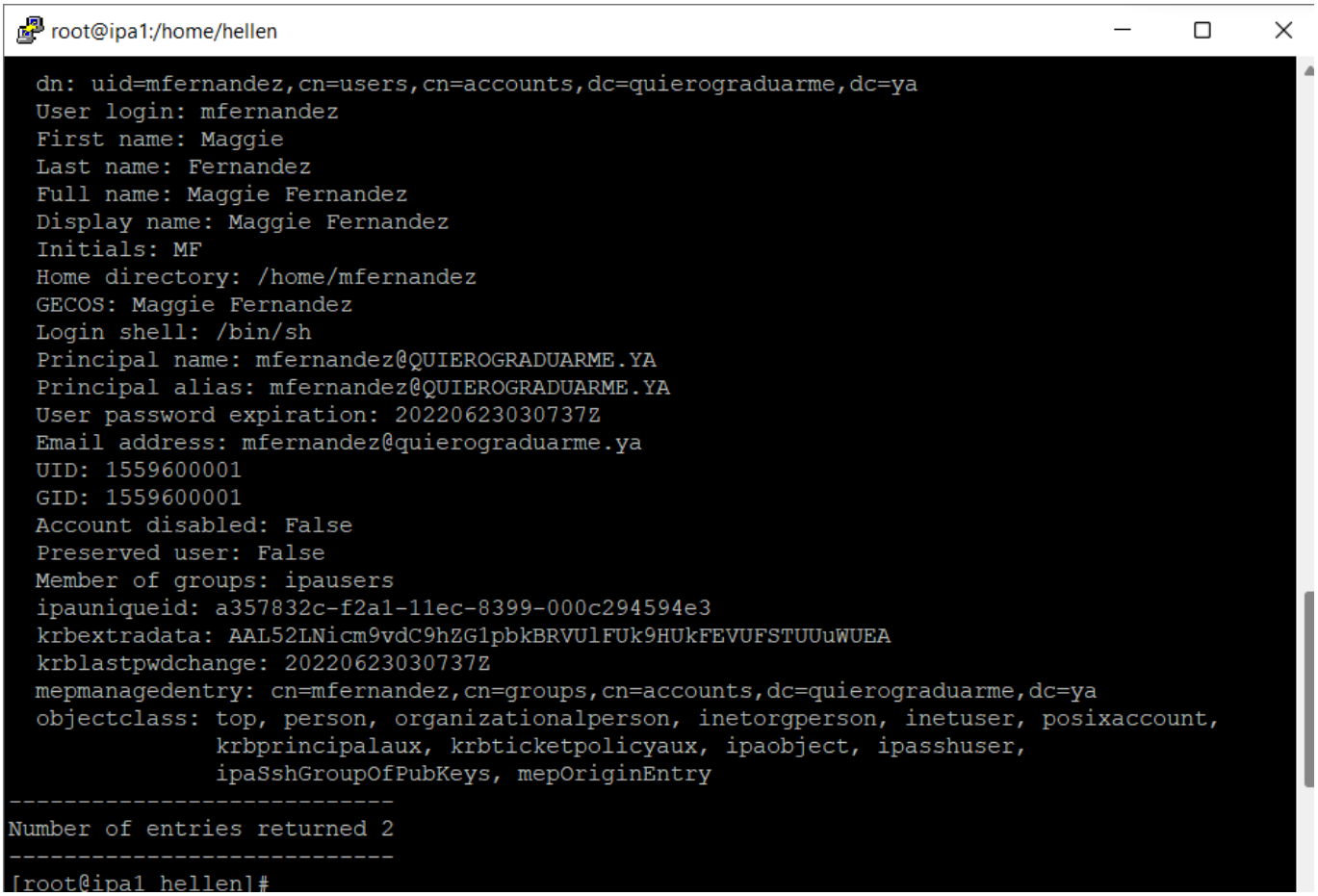
Funcionamiento de réplica sin CA

La prueba de funcionamiento de la réplica es agregar un usuario en ipa1 (el master) y verificarlo desde ipareplica:

1. Se añade el usuario en ipa1, en este caso añadimos al usuario “Maggie Fernandez”:



2. Se comprueba que el usuario fue agregado:



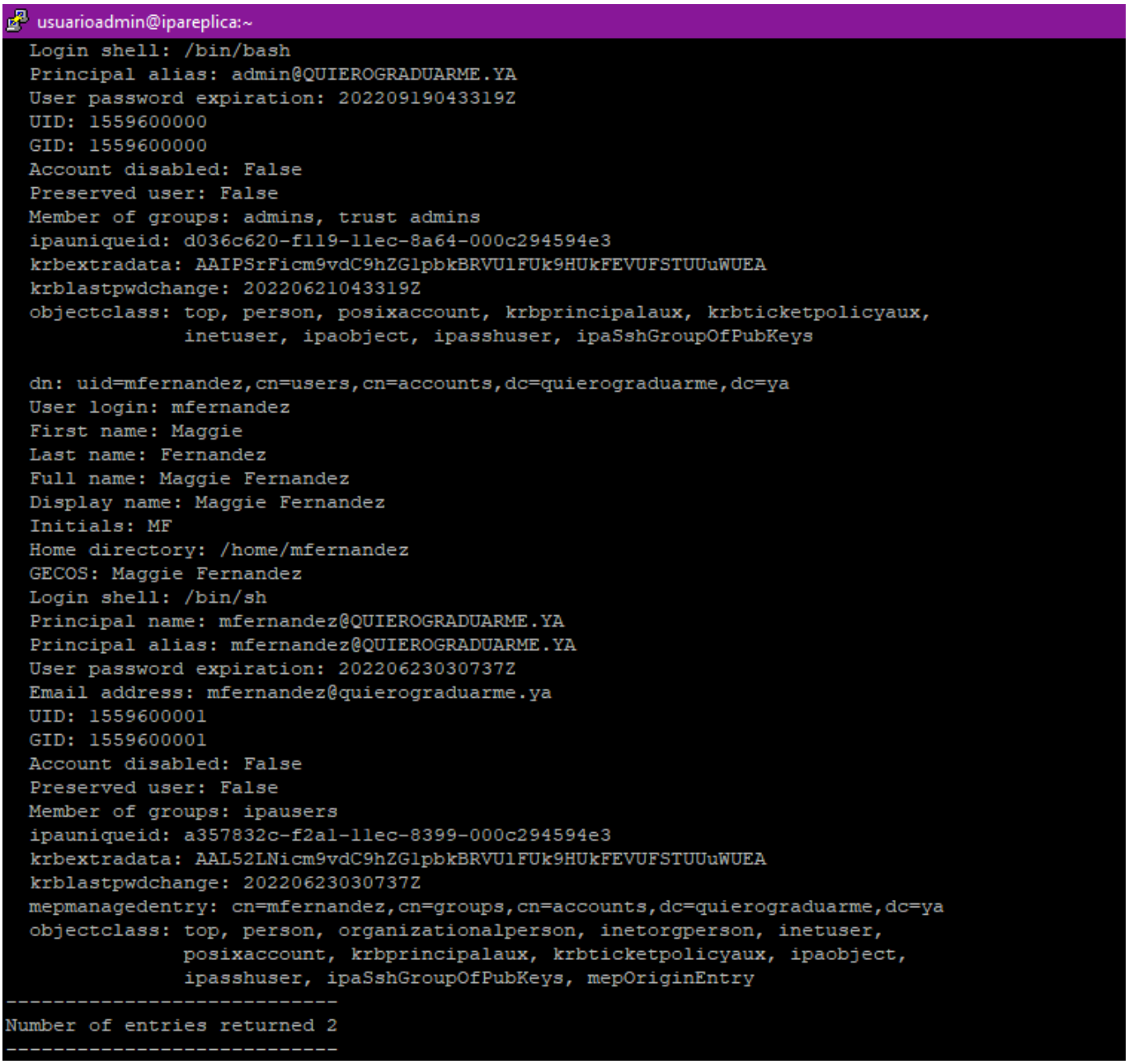
3. Desde la réplica se listan los usuarios y se comprueba que el usuario realmente se está propagando hacia la réplica:

```
ipa user-find --all
```

Como se puede notar, cuando se listan los usuarios hay 2: el de admin y Maggie Fernandez, el cual fue el usuario añadido al ipa master (ipa1):

usuarioadmin@ipareplica:~

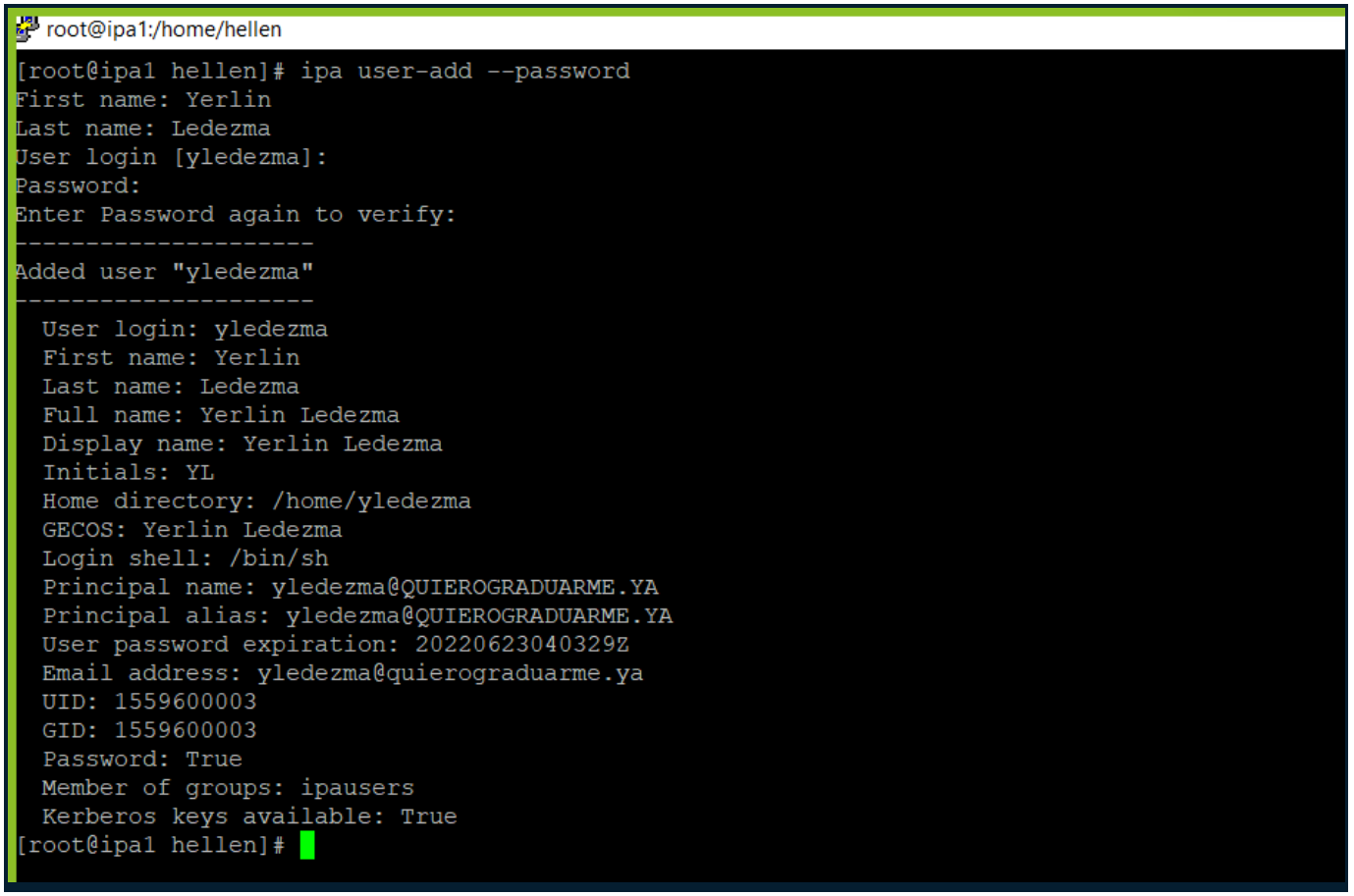
```
[usuarioadmin@ipareplica ~]$ ipa user-find --all
---------------
2 users matched
---------------
  dn: uid=admin,cn=users,cn=accounts,dc=quierograduarme,dc=ya
  User login: admin
  Last name: Administrator
  Full name: Administrator
  Home directory: /home/admin
  GECOS: Administrator
  Login shell: /bin/bash
  Principal alias: admin@QUIEROGRADUARME.YA
  User password expiration: 20220919043319Z
  UID: 1559600000
  GID: 1559600000
  Account disabled: False
  Preserved user: False
  Member of groups: admins, trust admins
  ipauniqueid: d036c620-f119-11ec-8a64-000c294594e3
  krbextradata: AAIPSrFicm9vdC9hZGlpbkBRVUlFUk9HUkFEVUFSTUUuWUEA
  krblastpwdchange: 20220621043319Z
  objectclass: top, person, posixaccount, krbprincipalaux, krbticketpolicyaux,
               inetuser, ipaobject, ipasshuser, ipaSshGroupOfPubKeys

  dn: uid=mfernandez,cn=users,cn=accounts,dc=quierograduarme,dc=ya
  User login: mfernandez
  First name: Maggie
  Last name: Fernandez
  Full name: Maggie Fernandez
  Display name: Maggie Fernandez
  Initials: MF
  Home directory: /home/mfernandez
  GECOS: Maggie Fernandez
  Login shell: /bin/sh
  Principal name: mfernandez@QUIEROGRADUARME.YA
  Principal alias: mfernandez@QUIEROGRADUARME.YA
  User password expiration: 20220623030737Z
  Email address: mfernandez@quierograduarme.ya
  UID: 1559600001
  GID: 1559600001
  Account disabled: False
  Preserved user: False
  Member of groups: ipausers
  ipauniqueid: a357832c-f2a1-11ec-8399-000c294594e3
```


usuarioadmin@ipareplica:~
Login shell: /bin/bash
Principal alias: admin@QUIEROGRADUARME.YA
User password expiration: 20220919043319Z
UID: 1559600000
GID: 1559600000
Account disabled: False
Preserved user: False
Member of groups: admins, trust admins
ipauniqueid: d036c620-f119-11ec-8a64-000c294594e3
krbextradata: AAIPSrFicm9vdC9hZG1pbkBRVUlFUk9HUkFEVUFSTUUuWUEA
krblastpwdchange: 20220621043319Z
objectclass: top, person, posixaccount, krbprincipalaux, krbticketpolicyaux,
inetuser, ipaobject, ipasshuser, ipaSshGroupOfPubKeys
dn: uid=mfernandez,cn=users,cn=accounts,dc=quierograduarme,dc=ya
User login: mfernandez
First name: Maggie
Last name: Fernandez
Full name: Maggie Fernandez
Display name: Maggie Fernandez
Initials: MF
Home directory: /home/mfernandez
GECOS: Maggie Fernandez
Login shell: /bin/sh
Principal name: mfernandez@QUIEROGRADUARME.YA
Principal alias: mfernandez@QUIEROGRADUARME.YA
User password expiration: 20220623030737Z
Email address: mfernandez@quierograduarme.ya
UID: 1559600001
GID: 1559600001
Account disabled: False
Preserved user: False
Member of groups: ipausers
ipauniqueid: a357832c-f2a1-11ec-8399-000c294594e3
krbextradata: AAL52LNicm9vdC9hZG1pbkBRVUlFUk9HUkFEVUFSTUUuWUEA
krblastpwdchange: 20220623030737Z
mepmanagedentry: cn=mfernandez,cn=groups,cn=accounts,dc=quierograduarme,dc=ya
objectclass: top, person, organizationalperson, inetorgperson, inetuser,
posixaccount, krbprincipalaux, krbticketpolicyaux, ipaobject,
ipasshuser, ipaSshGroupOfPubKeys, mepOriginEntry

Number of entries returned 2

Funcionamiento de réplica con CA

Probamos nuevamente agregar un usuario desde el ipa y verificar si se encuentra desde la réplica:




```
ipa user-find --all
```

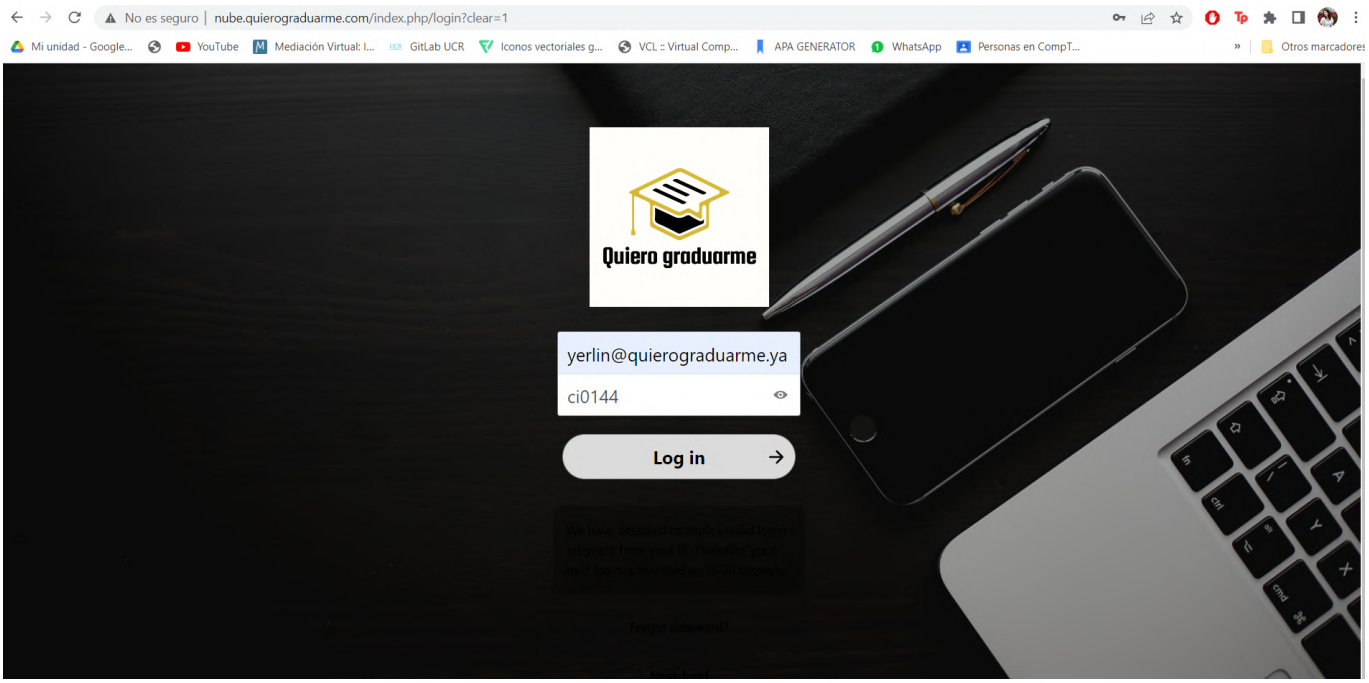
root@ipareplica:/home/usuarioadmin

```
  dn: uid=yledezma,cn=users,cn=accounts,dc=quierograduarme,dc=ya
  User login: yledezma
  First name: Yerlin
  Last name: Ledezma
  Full name: Yerlin Ledezma
  Display name: Yerlin Ledezma
  Initials: YL
  Home directory: /home/yledezma
  GECOS: Yerlin Ledezma
  Login shell: /bin/sh
  Principal name: yledezma@QUIEROGRADUARME.YA
  Principal alias: yledezma@QUIEROGRADUARME.YA
  User password expiration: 20220623040329Z
  Email address: yledezma@quierograduarme.ya
  UID: 1559600003
  GID: 1559600003
  Account disabled: False
  Preserved user: False
  Member of groups: ipausers
  ipauniqueid: 71469280-f2a9-11ec-9f0a-000c294594e3
  krbextradata: AAIR5rNicm9vdC9hZG1pbkBRVUlFUk9HUkFEVUFSTUUuWUEA
  krblastpwdchange: 20220623040329Z
  mepmanagedentry: cn=yledezma,cn=groups,cn=accounts,dc=quierograduarme,dc=ya
  objectclass: top, person, organizationalperson, inetorgperson, inetuser,
               posixaccount, krbprincipalaux, krbticketpolicyaux, ipaobject,
               ipasshuser, ipaSshGroupOfPubKeys, mepOriginEntry
----------------------------
Number of entries returned 3
```

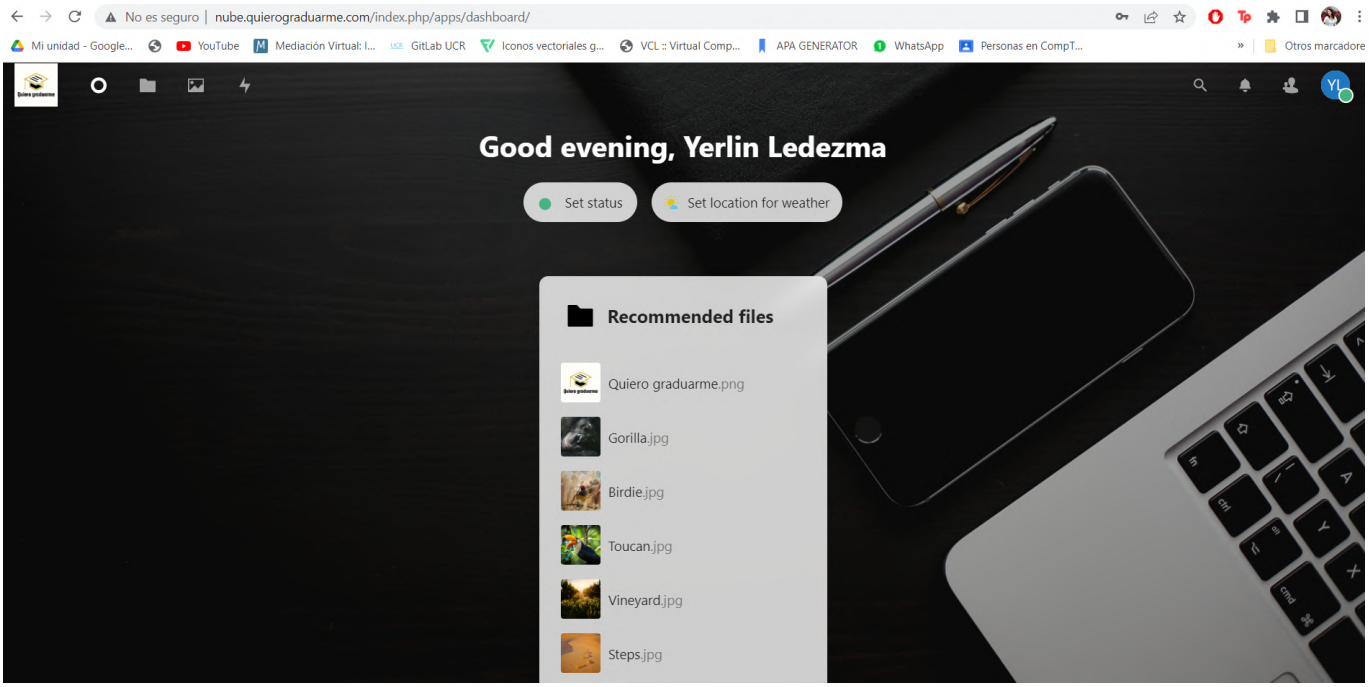
Prueba NextCloud

1. Con el correo yerlin iniciar sesión:

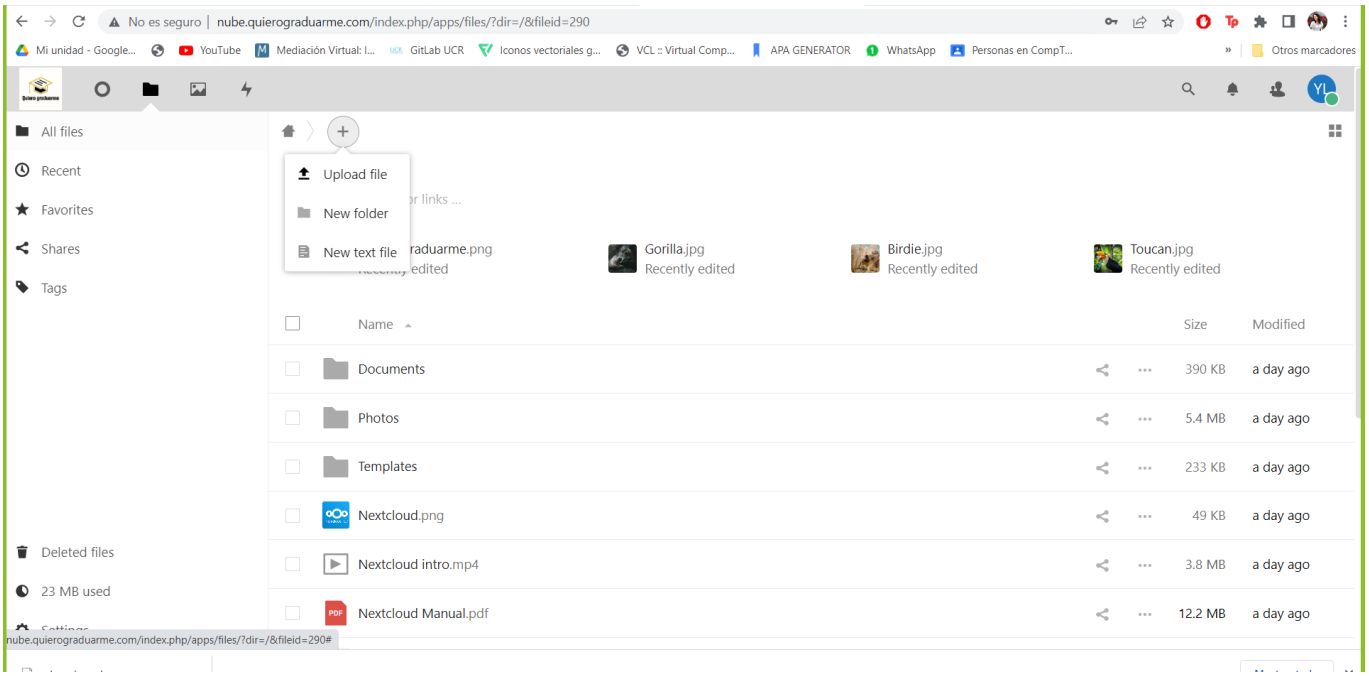
yerlin@quierograduarme.ya
ci0144

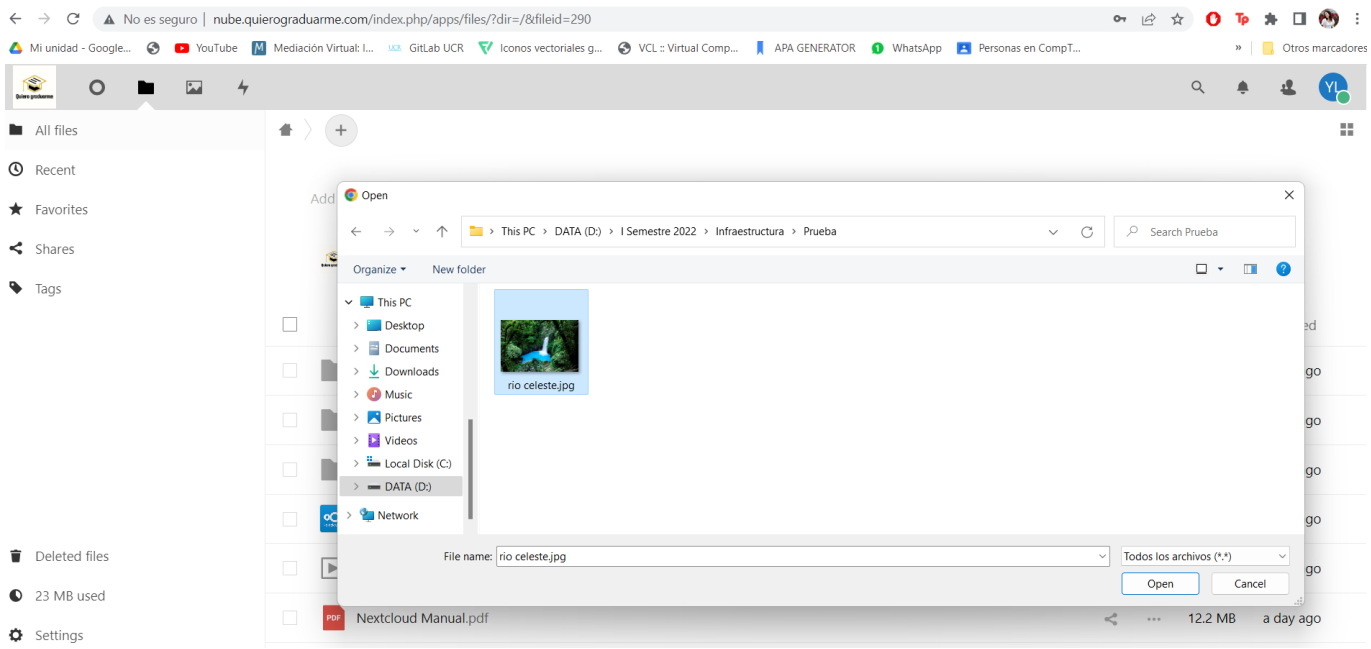


2. Al iniciar sesión diríjase al icono de carpeta.

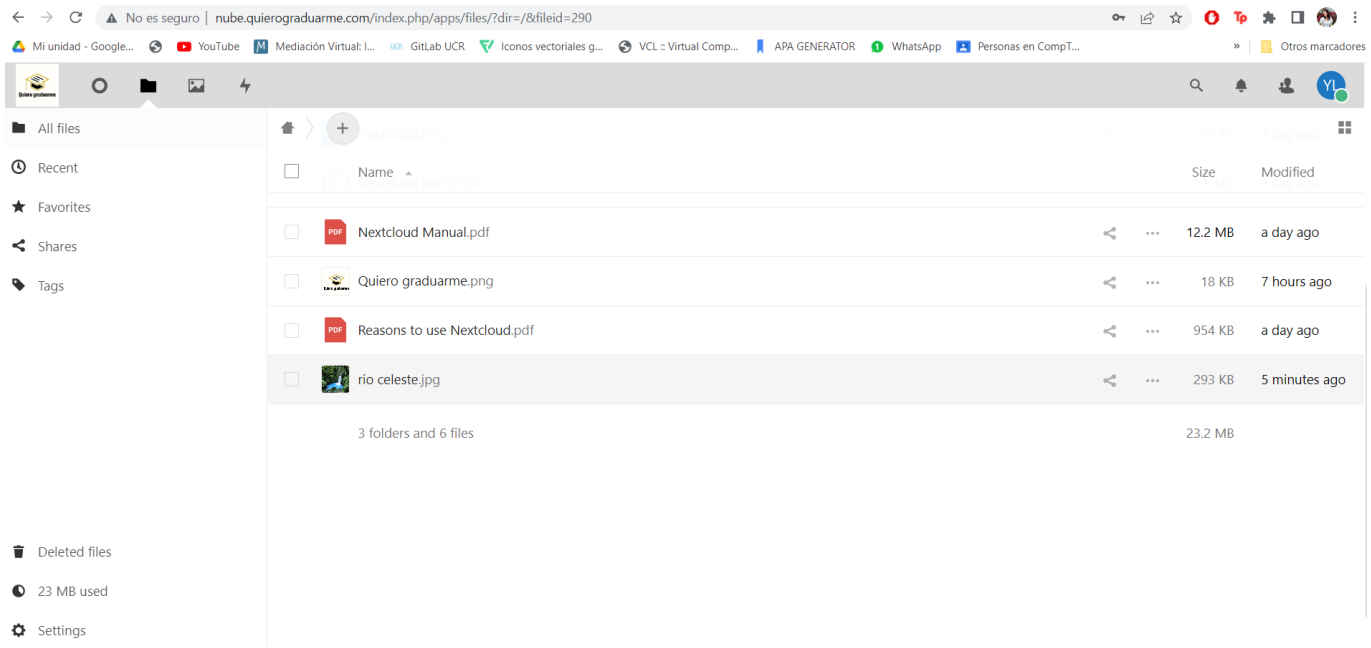


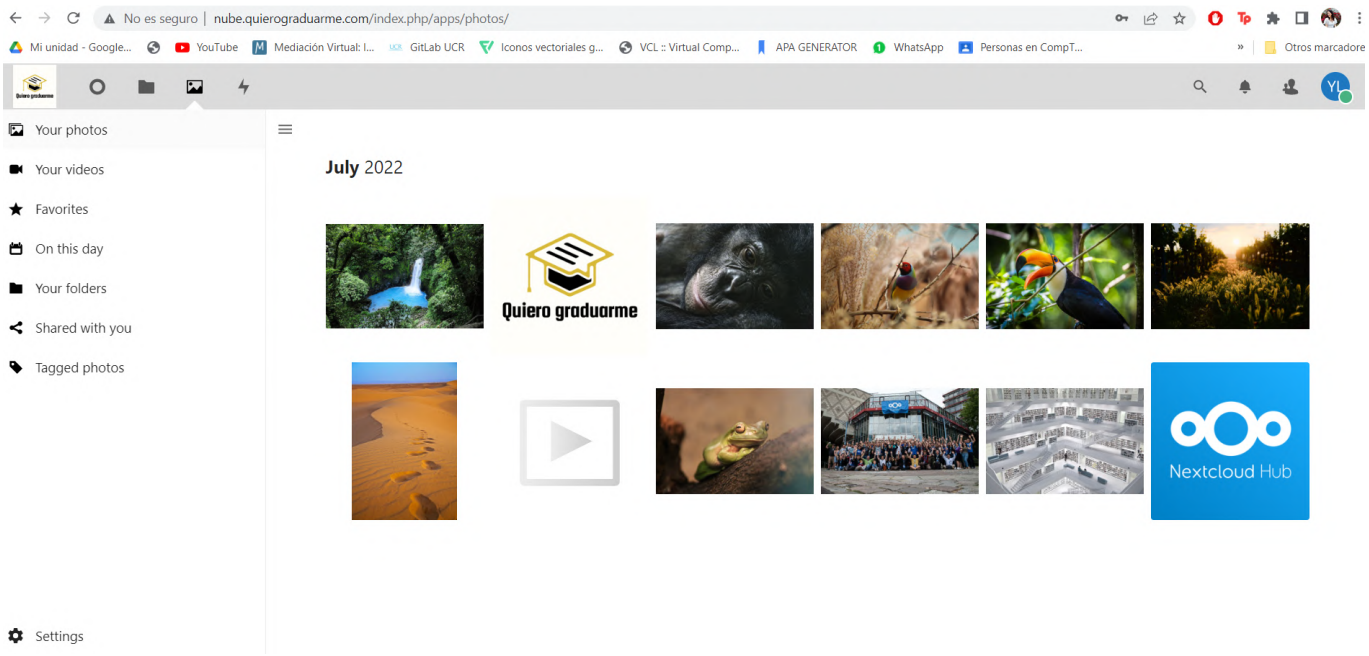
3. Subir una imagen:

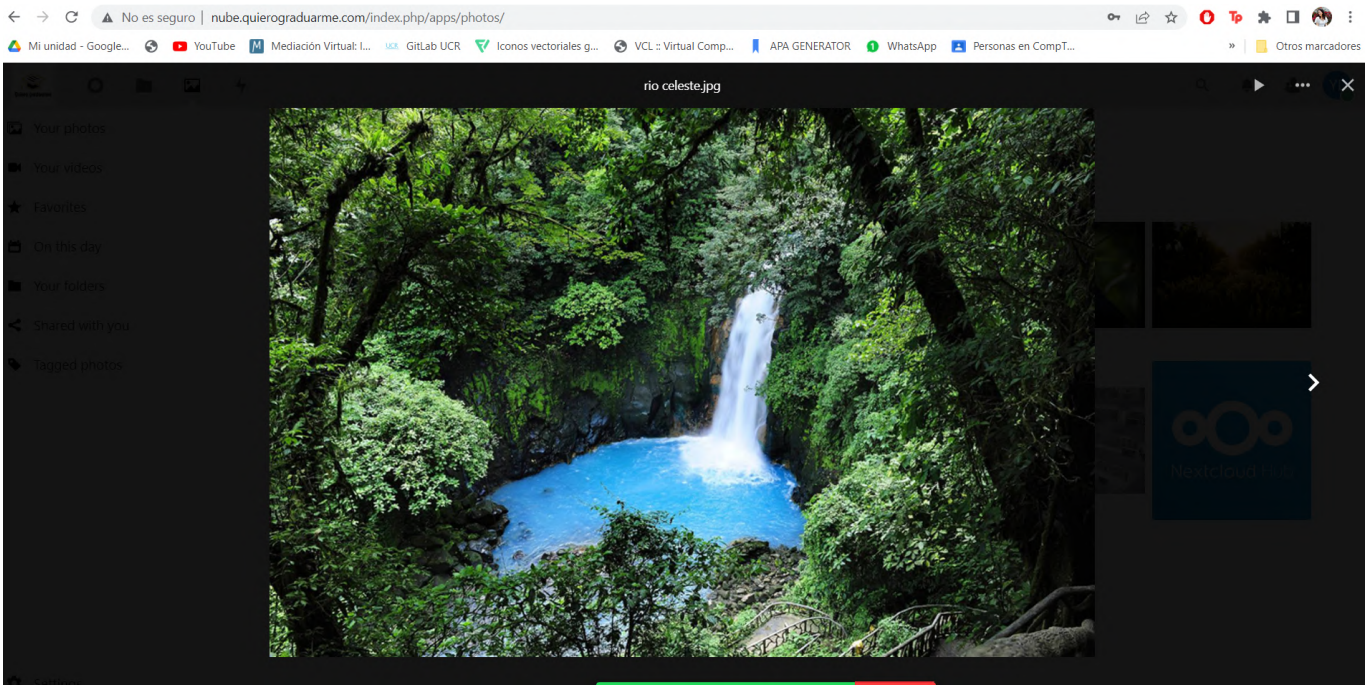


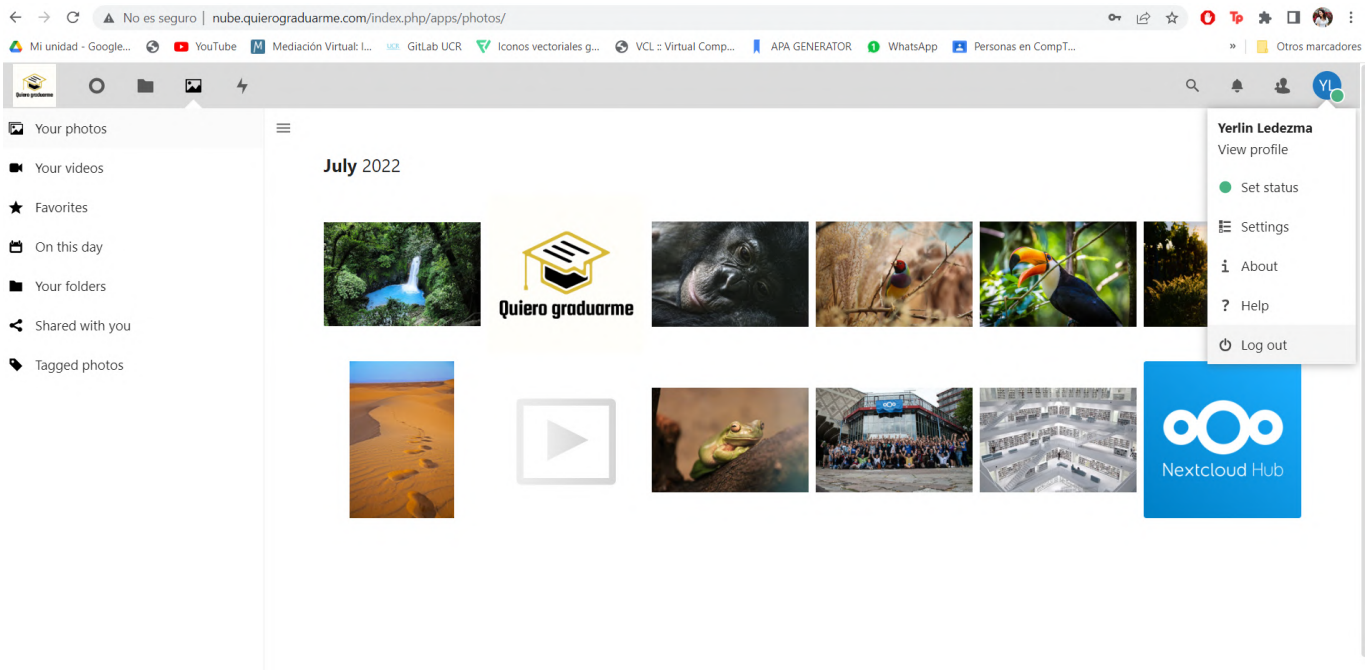


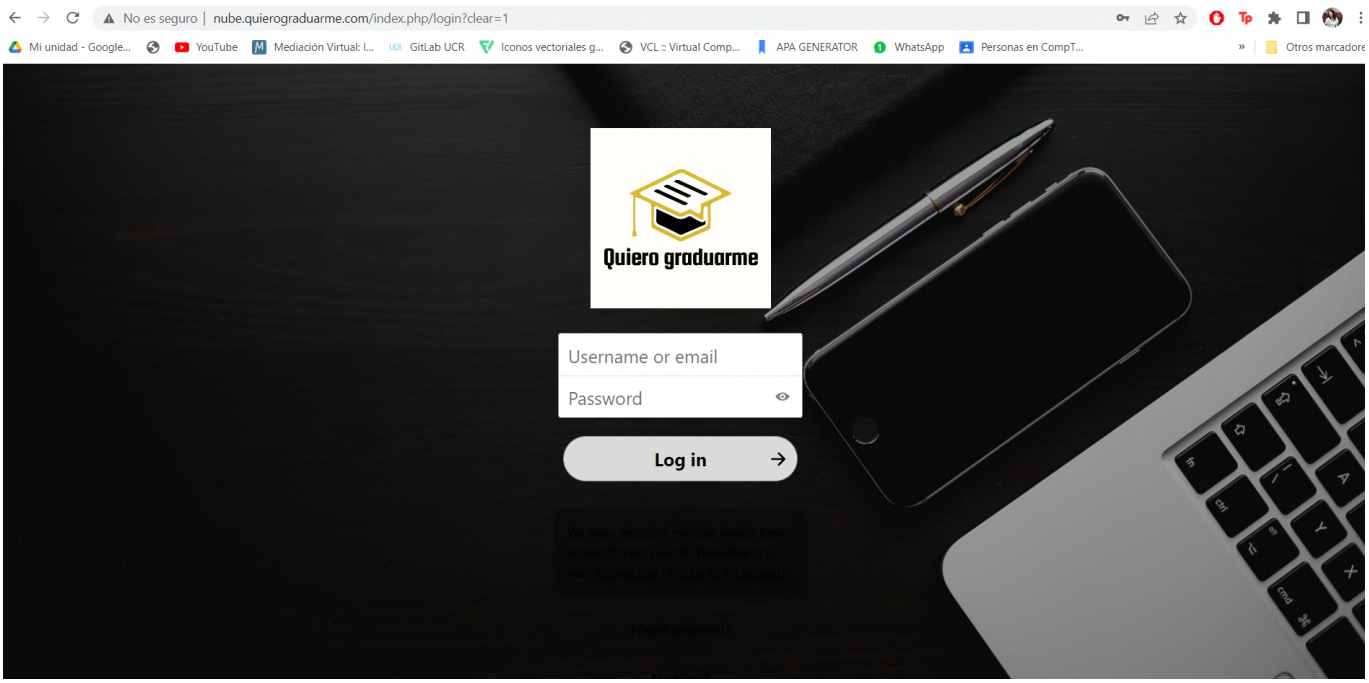
4. Verificar que se va a subió la imagen:




No es seguro | nube.quierograduarme.com/index.php/apps/photos/
Mi unidad - Google...
YouTube
Mediación Virtual: I...
GitLab UCR
Iconos vectoriales g...
VCL :: Virtual Comp...
APA GENERATOR
WhatsApp
Personas en CompT...
Otros marcadores
Your photos
Your videos
Favorites
On this day
Your folders
Shared with you
Tagged photos
Settings
July 2022
Quiero graduarme
Nextcloud Hub


No es seguro | nube.quierograduarme.com/index.php/apps/photos/
Mi unidad - Google...
YouTube
Mediación Virtual: I...
GitLab UCR
Iconos vectoriales g...
VCL :: Virtual Comp...
APA GENERATOR
WhatsApp
Personas en CompT...
Otros marcadores
rio celeste.jpg
Your photos
Your videos
Favorites
On this day
Your folders
Shared with you
Tagged photos

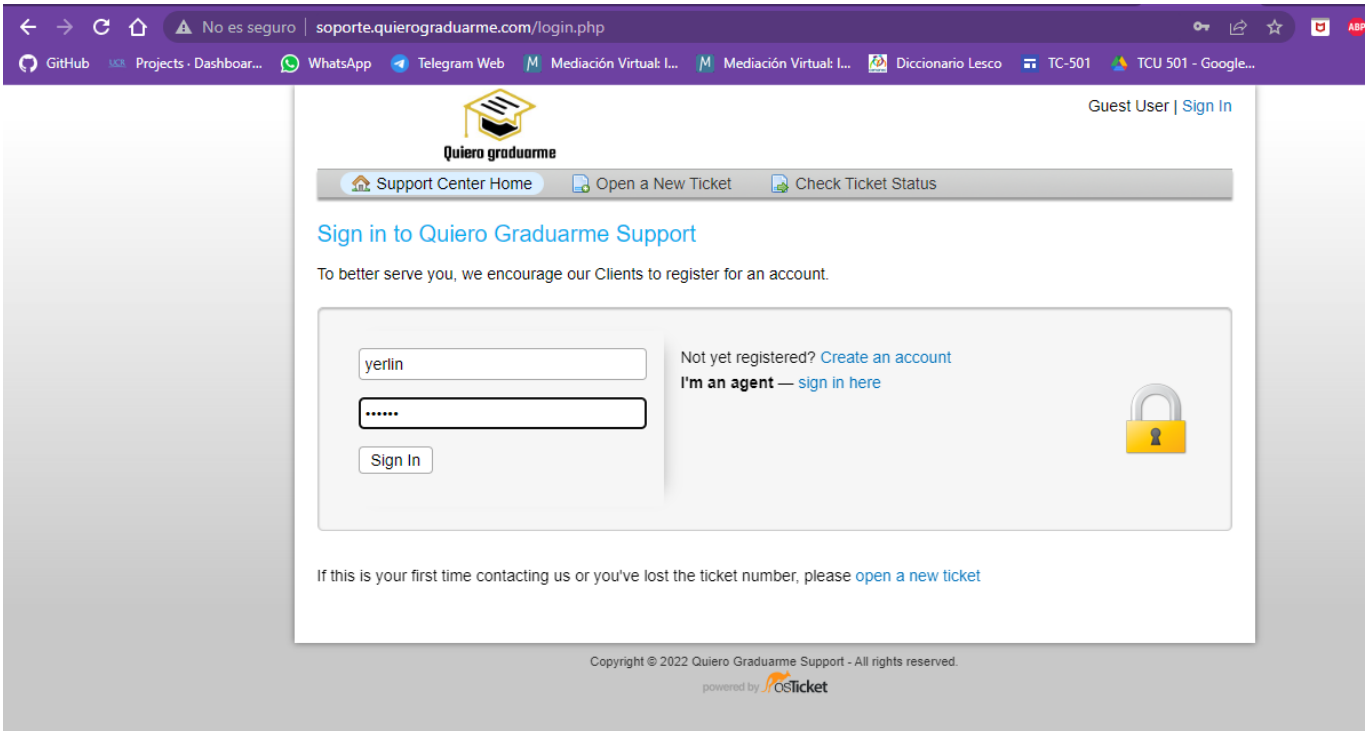

No es seguro | nube.quierograduarme.com/index.php/apps/photos/
Mi unidad - Google...
YouTube
Mediación Virtual: I...
GitLab UCR
Iconos vectoriales g...
VCL :: Virtual Comp...
APA GENERATOR
WhatsApp
Personas en CompT...
Otros marcadores
Your photos
Your videos
Favorites
On this day
Your folders
Shared with you
Tagged photos
July 2022
Quiero graduarme
Nextcloud Hub
Yerlin Ledezma
View profile
Set status
Settings
About
Help
Log out

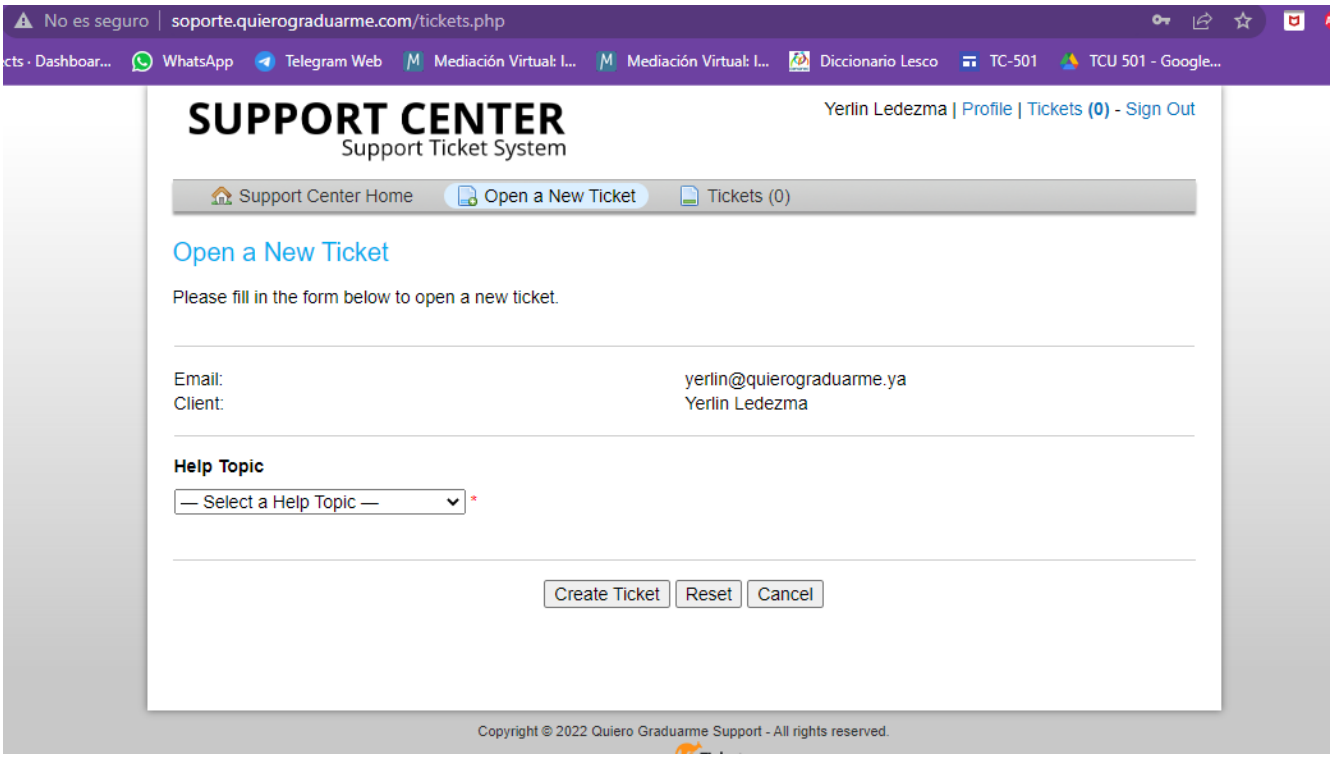

No es seguro | nube.quierograduarme.com/index.php/login?clear=1
Mi unidad - Google...
YouTube
Mediación Virtual: I...
GitLab UCR
Iconos vectoriales g...
VCL :: Virtual Comp...
APA GENERATOR
WhatsApp
Personas en CompT...
Otros marcadores
Quiero graduarme
Username or email
Password
Log in

Prueba Osticket

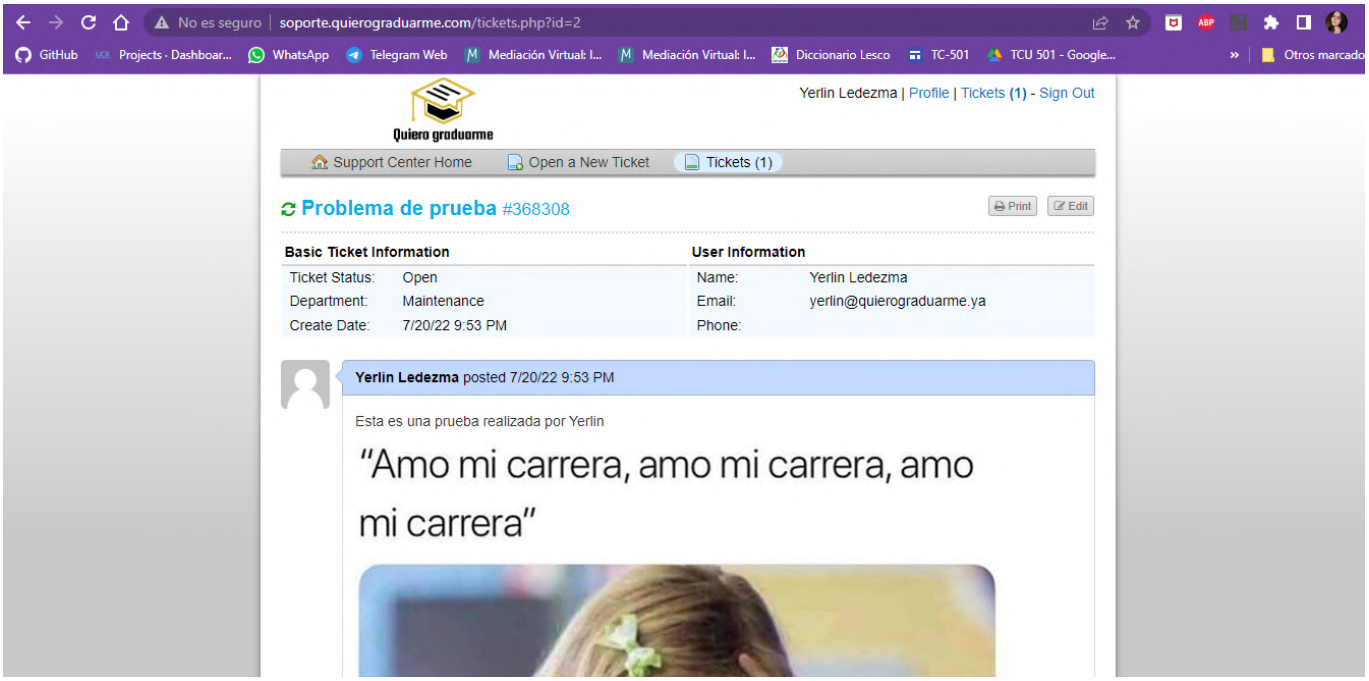
1. Iniciar sesión en la página de soporte con el siguiente usuario y contraseña

Usuario: yerlin
Contraseña: ci0144

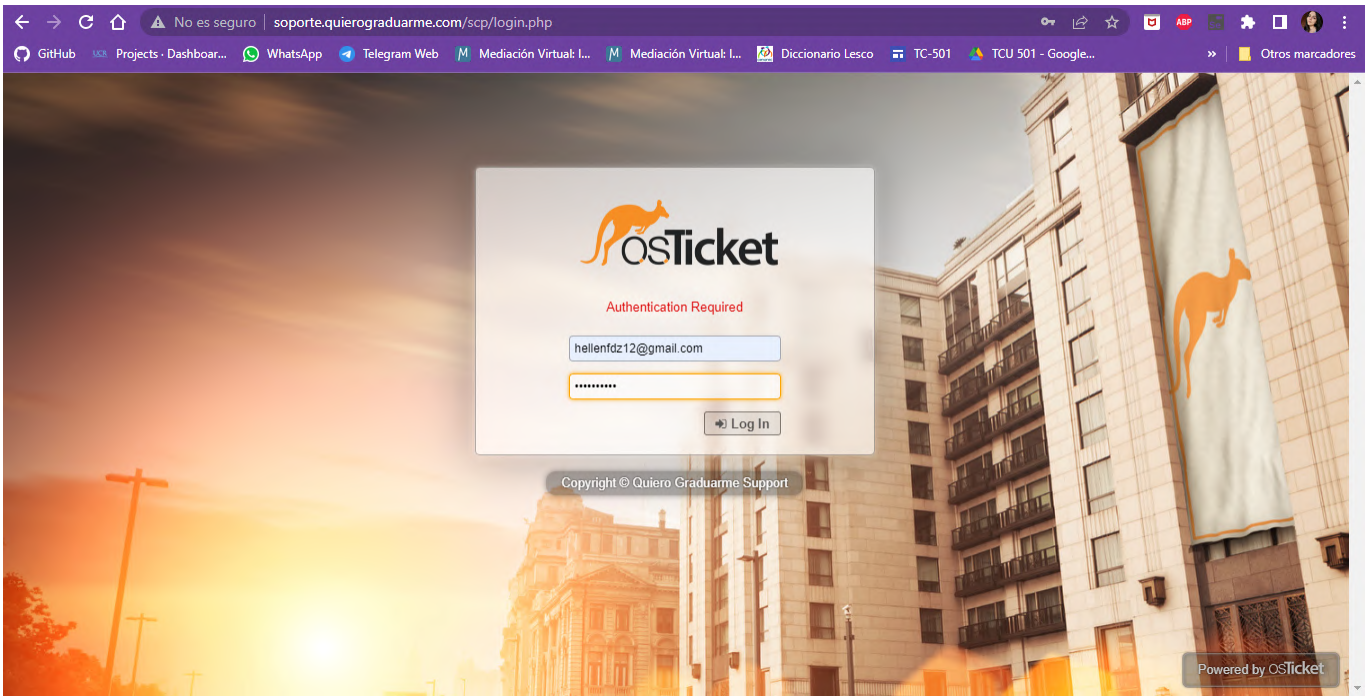




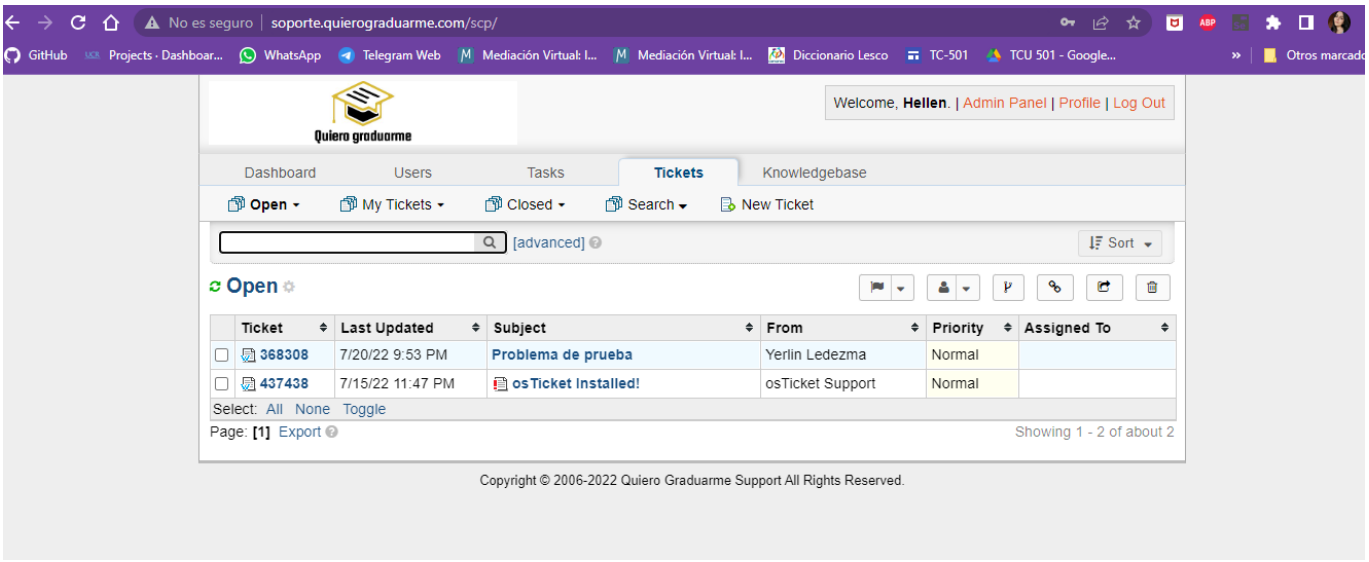
2. Crear un ticket

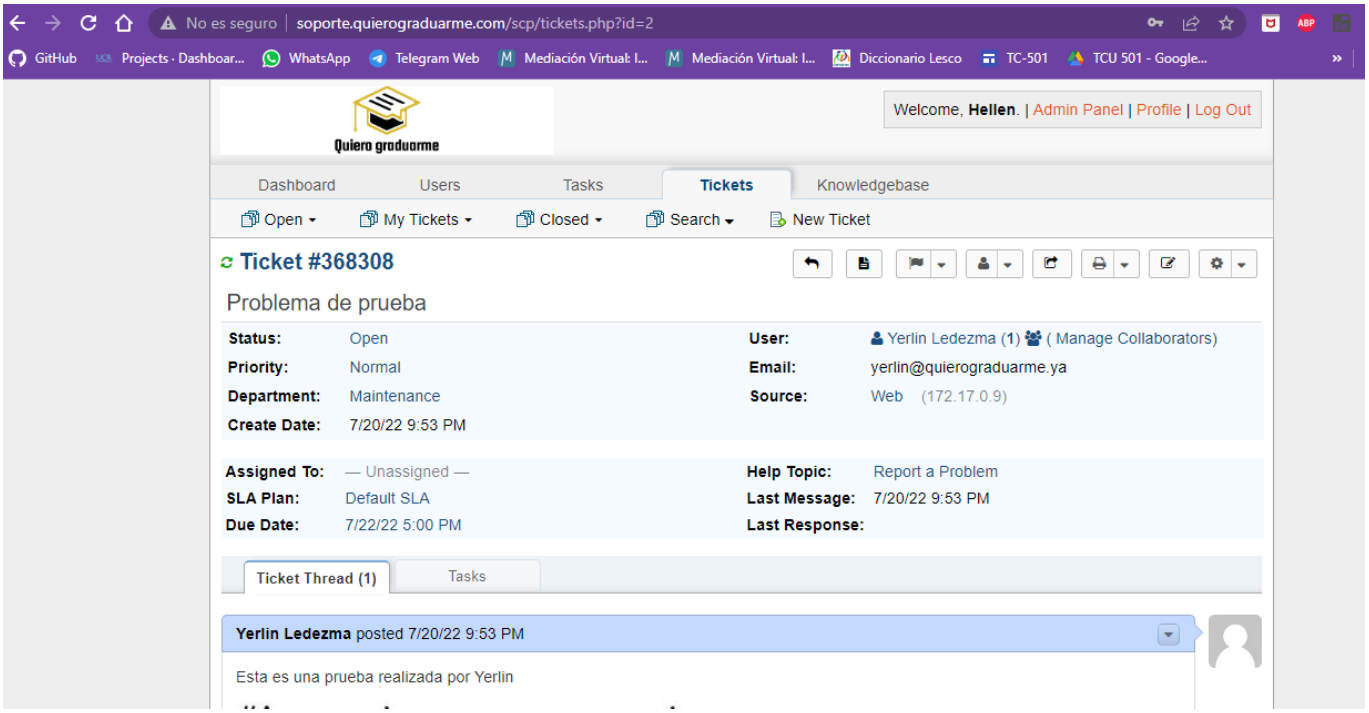


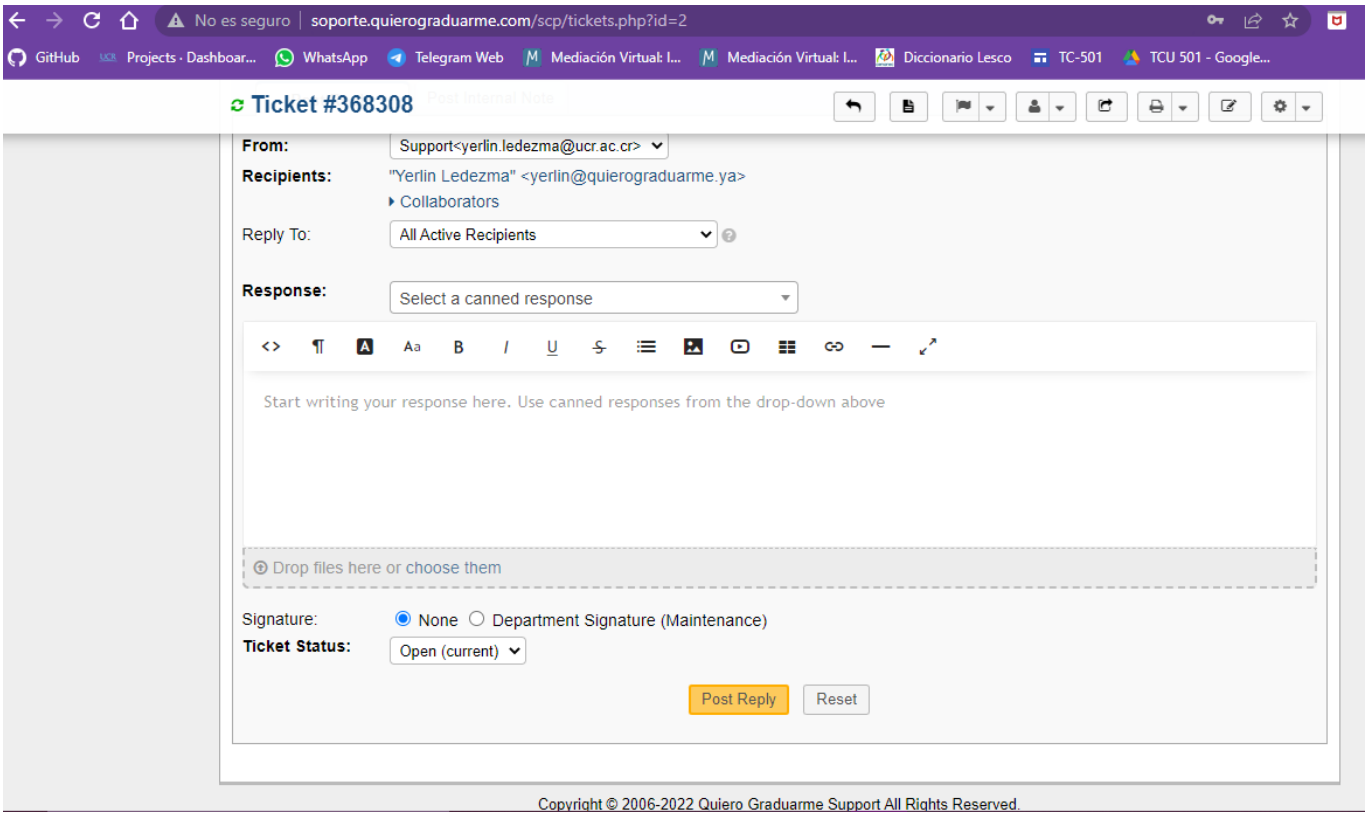
3. Ingresar al inicio de sesión del administrador



4. Verificar que se haya creado el ticket



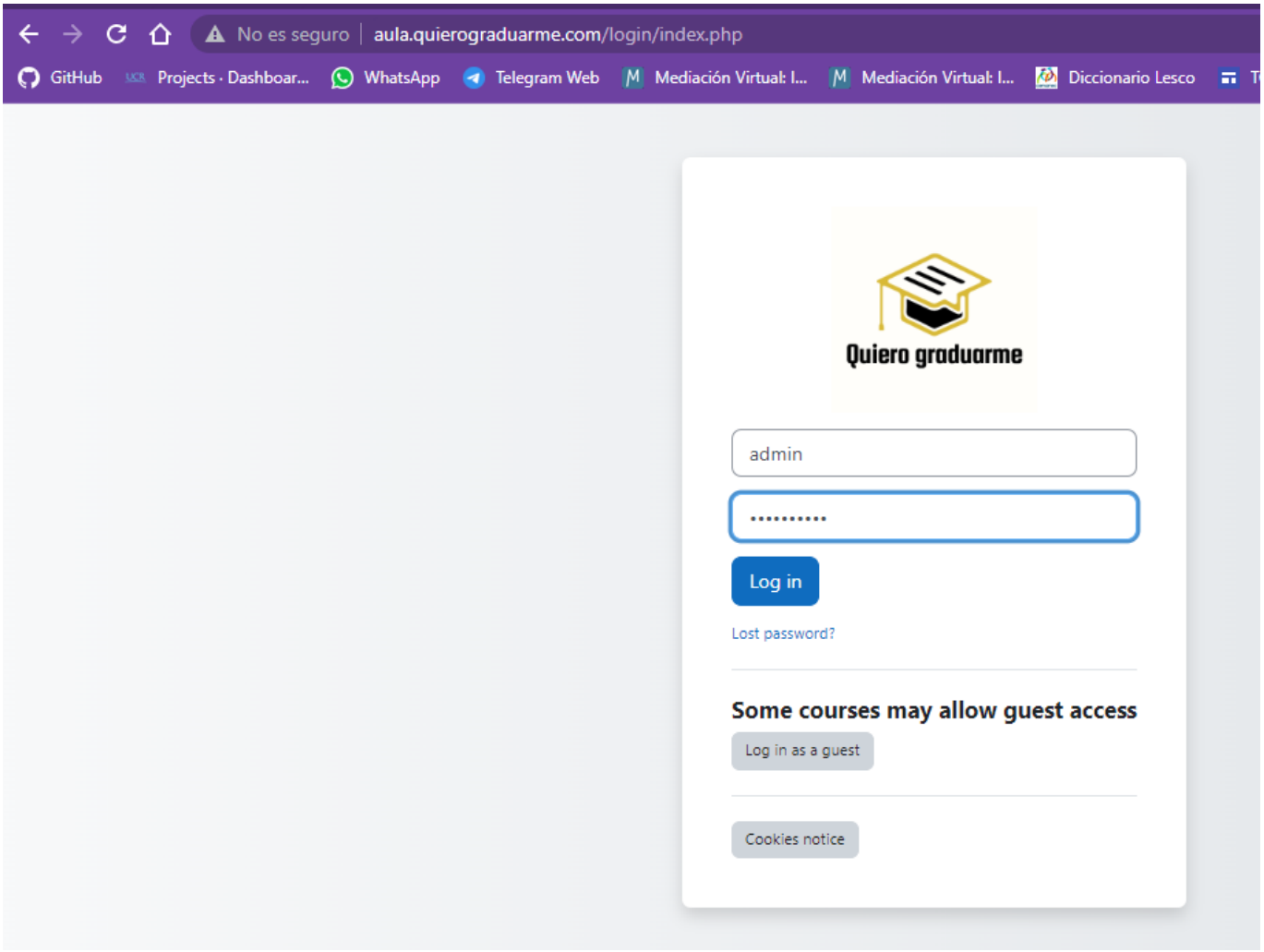



No es seguro | soporte.quierograduarme.com/scp/tickets.php?id=2
GitHub
Projects - Dashboar...
WhatsApp
Telegram Web
Mediación Virtual: I...
Mediación Virtual: I...
Diccionario Lesco
TC-501
TCU 501 - Google...
Ticket #368308
Post Internal Note
From:
Support<yerlin.ledezma@ucr.ac.cr>
Recipients:
"Yerlin Ledezma" <yerlin@quierograduarme.ya>
Collaborators
Reply To:
All Active Recipients
Response:
Select a canned response
Start writing your response here. Use canned responses from the drop-down above
Drop files here or choose them
Signature:
None
Department Signature (Maintenance)
Ticket Status:
Open (current)
Post Reply
Reset
Copyright © 2006-2022 Quiero Graduarme Support All Rights Reserved.

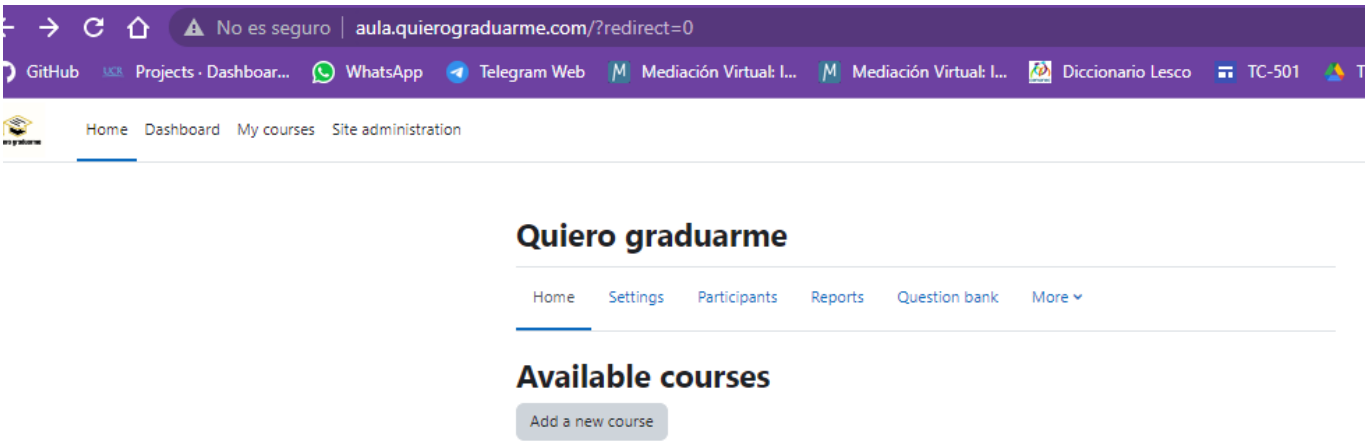
Prueba Moodle

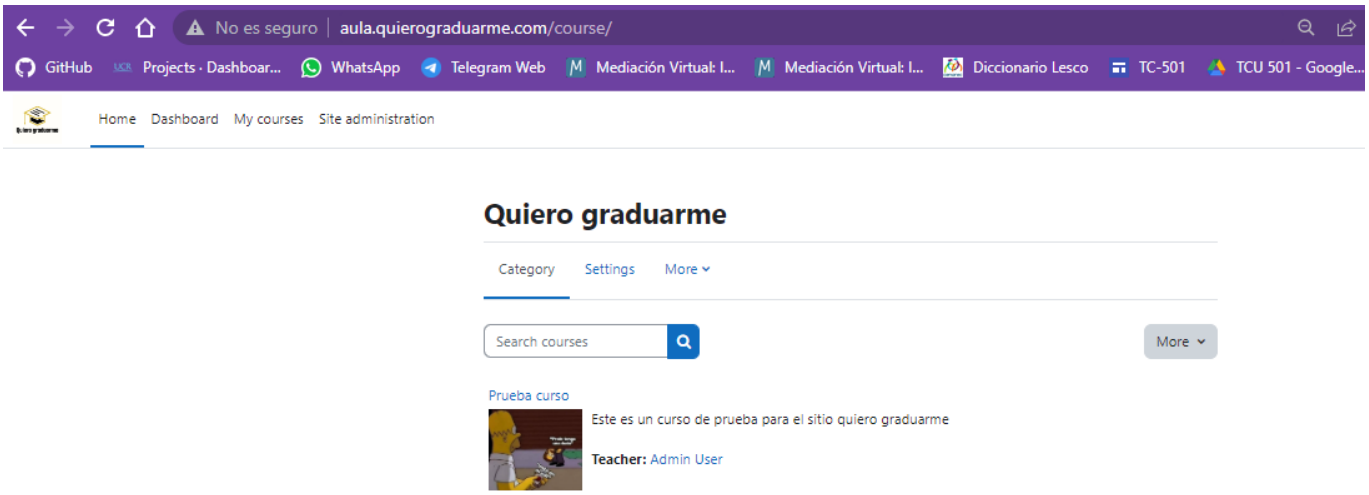
1. Ingresar a aula.quierograduarme.com con las credenciales de administrador

Usuario: admin
Contraseña: maggieLu2

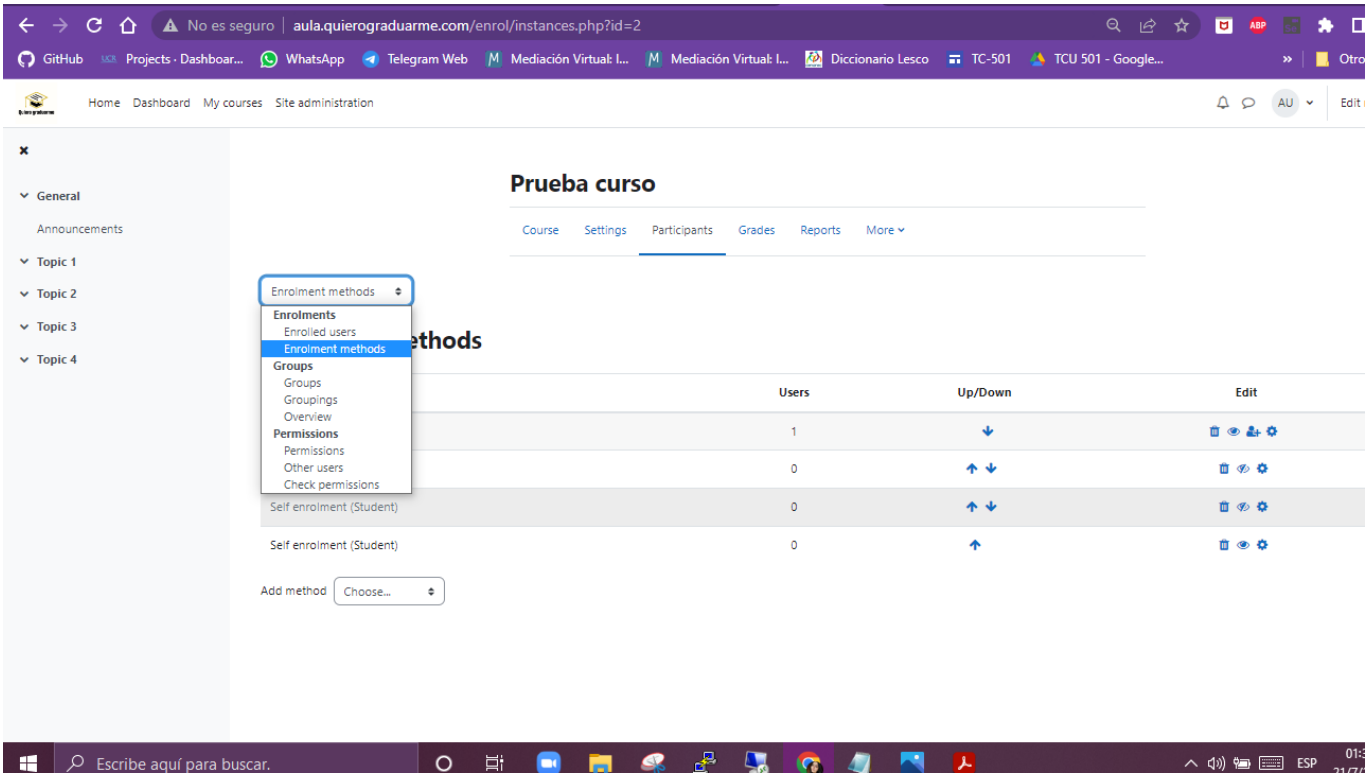


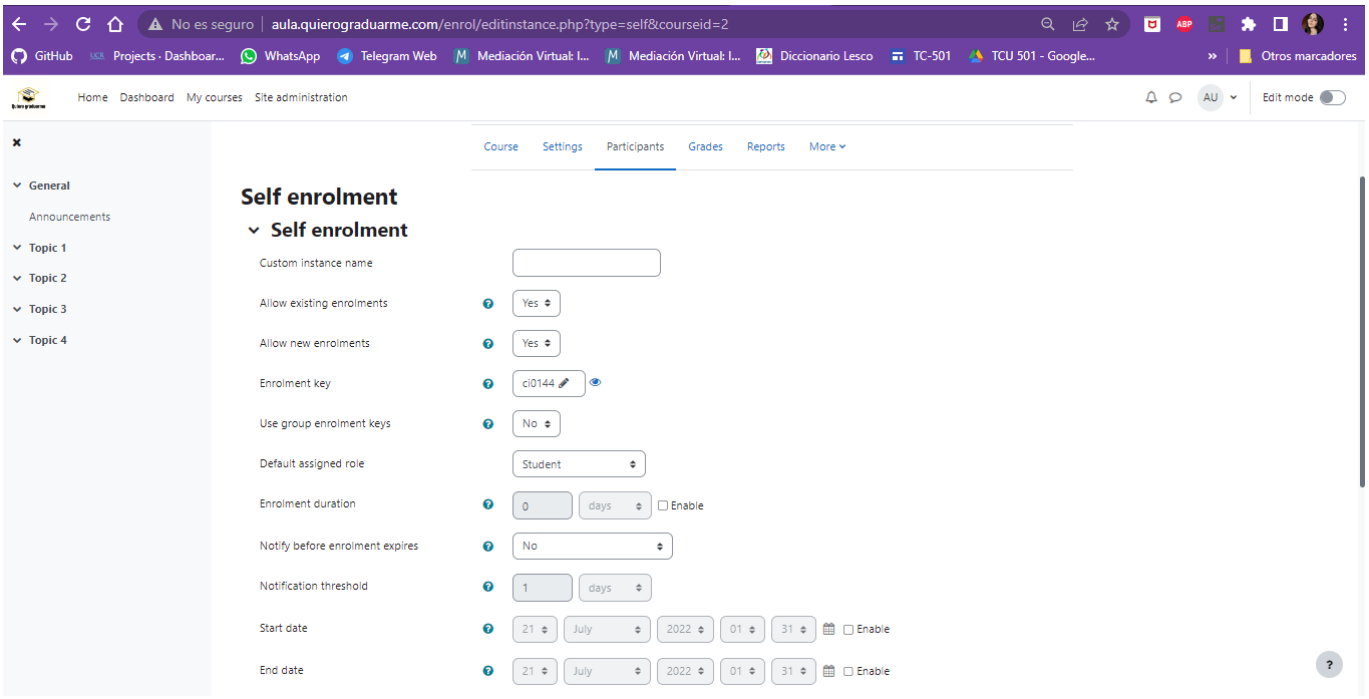
2. Agregar un nuevo curso

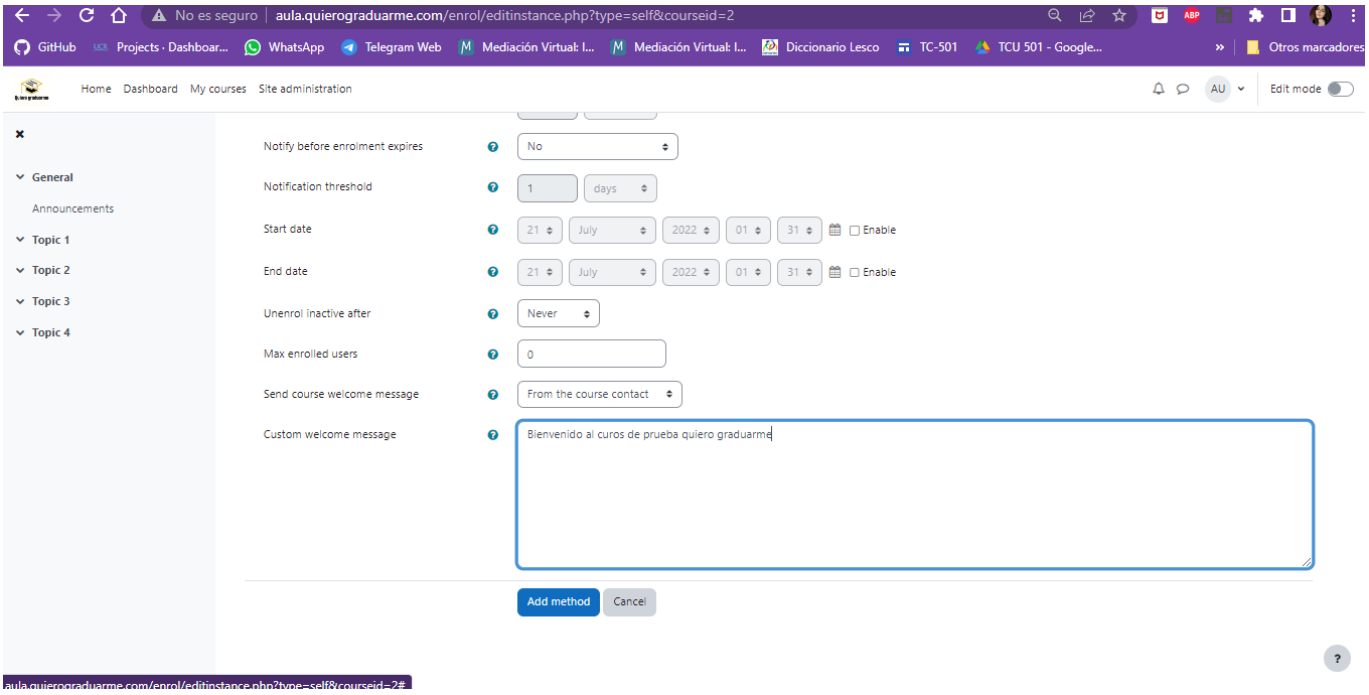




3. Permitir que los estudiantes se matriculen solos en el curso, diríjase a *Participant*, seleccione *Enrollment methods* e ingrese una contraseña para matricularse, en este caso la contraseña es ci0144.

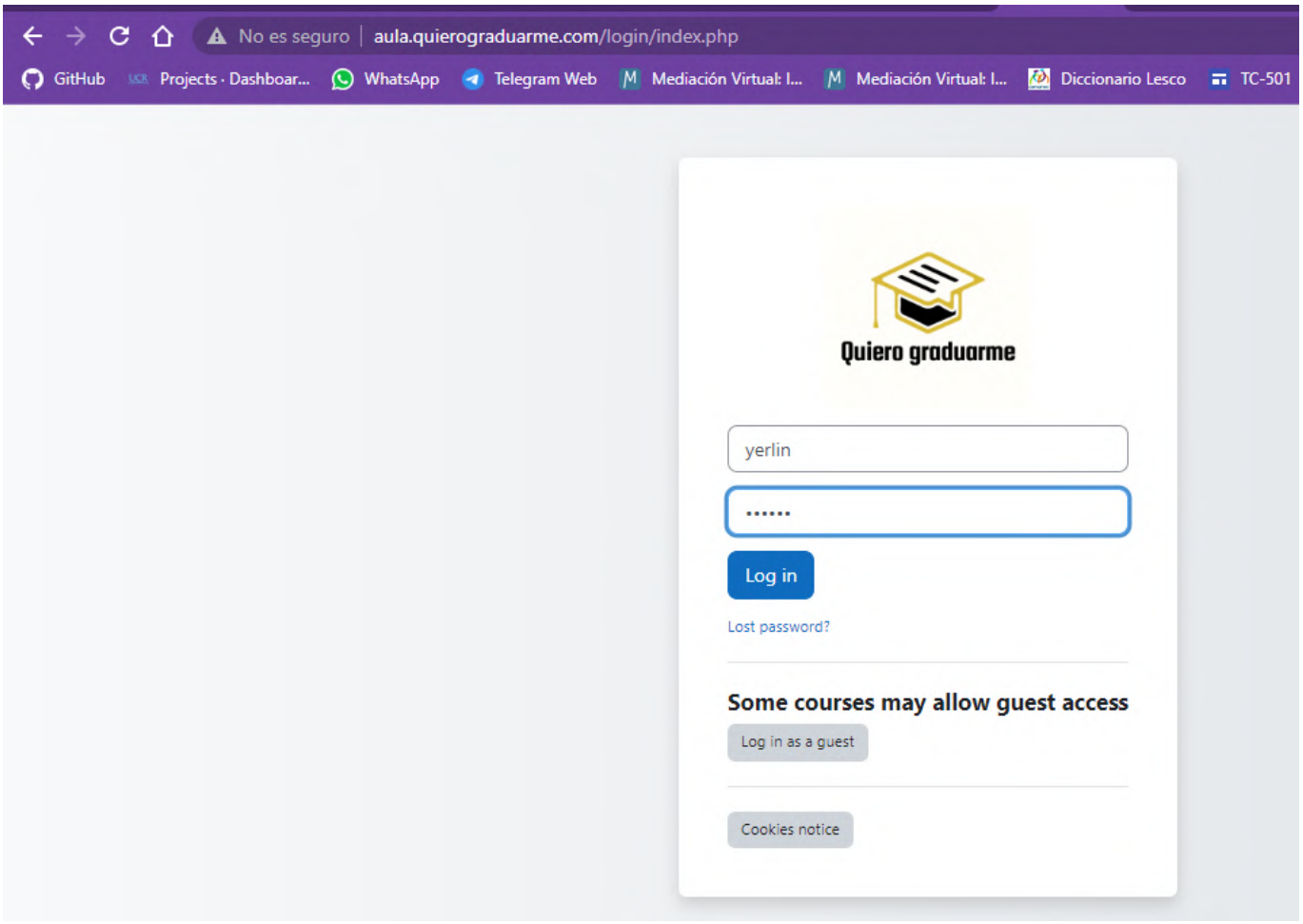




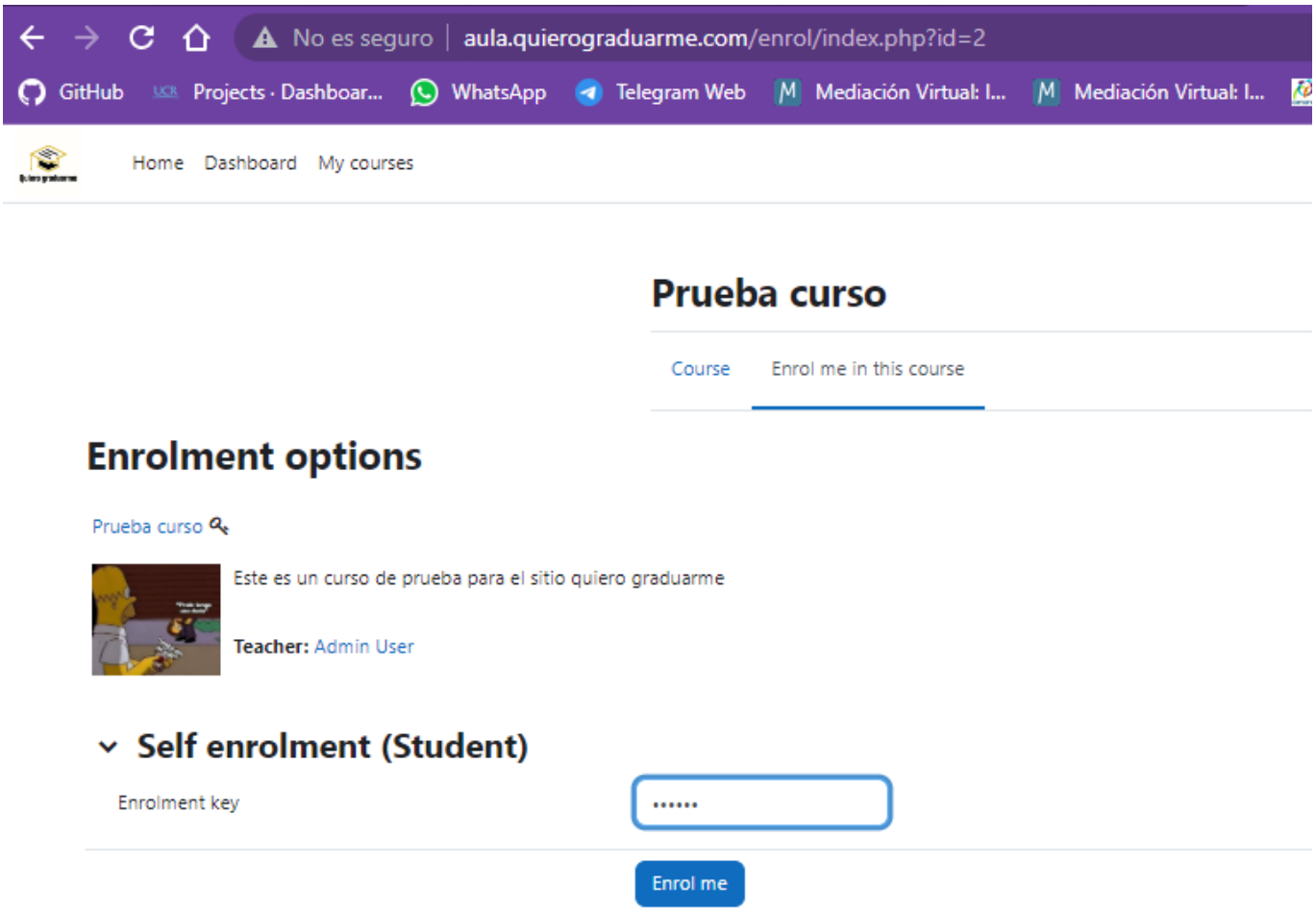


4. Ingrese al curso con un usuario y contraseña distinto al de administrador

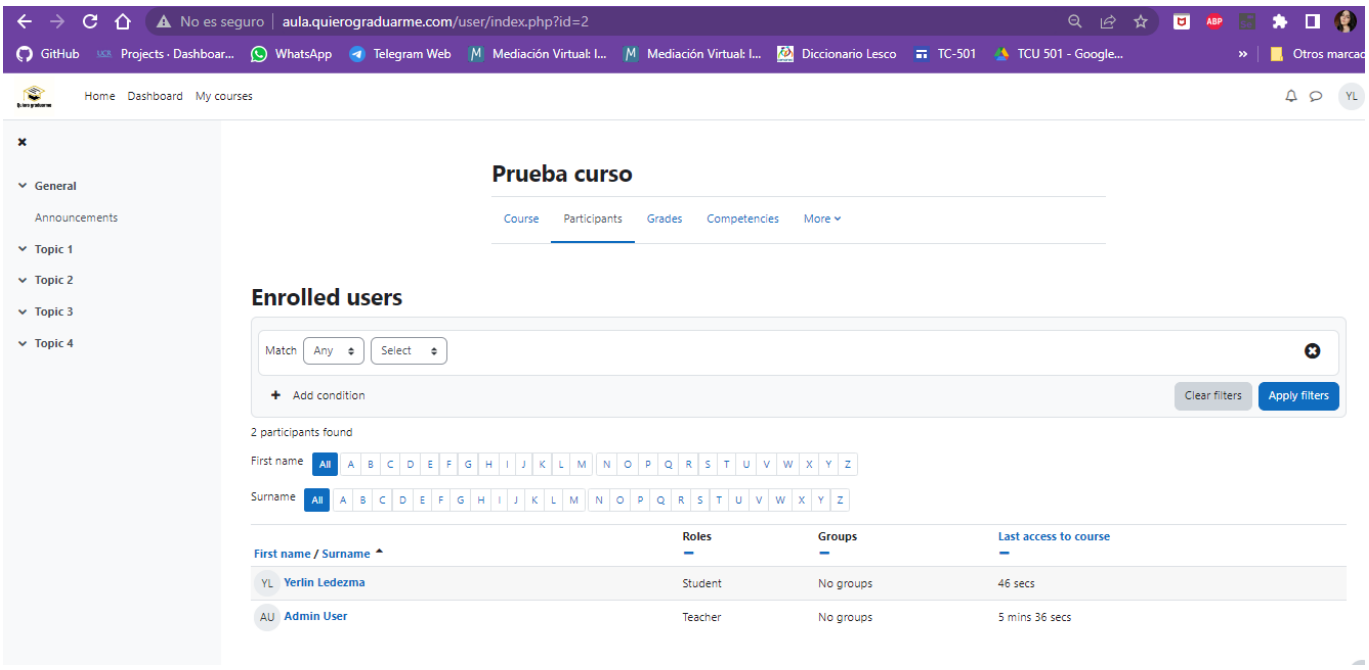
En este caso se usa el usuario yerlin


No es seguro | aula.quierograduarme.com/login/index.php
GitHub
Projects - Dashboar...
WhatsApp
Telegram Web
Mediación Virtual: I...
Mediación Virtual: I...
Diccionario Lesco
TC-501
Quiero graduarme
yerlin
Log in
Lost password?
Some courses may allow guest access
Log in as a guest
Cookies notice

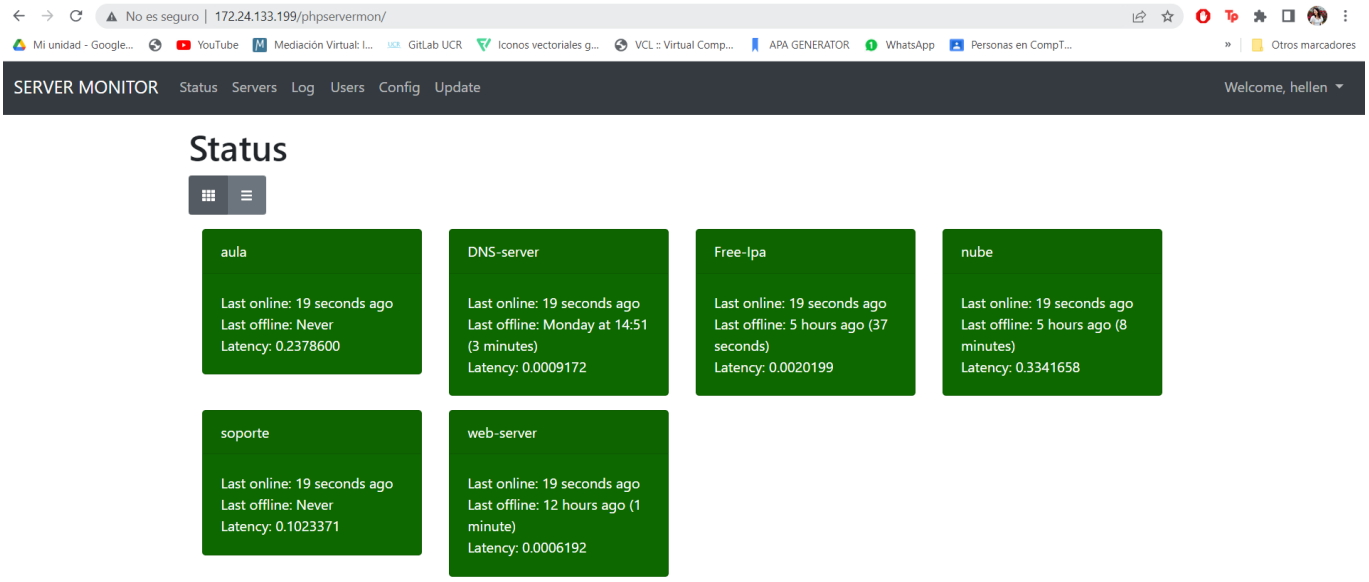
5. Ingresar la contraseña y matricularse

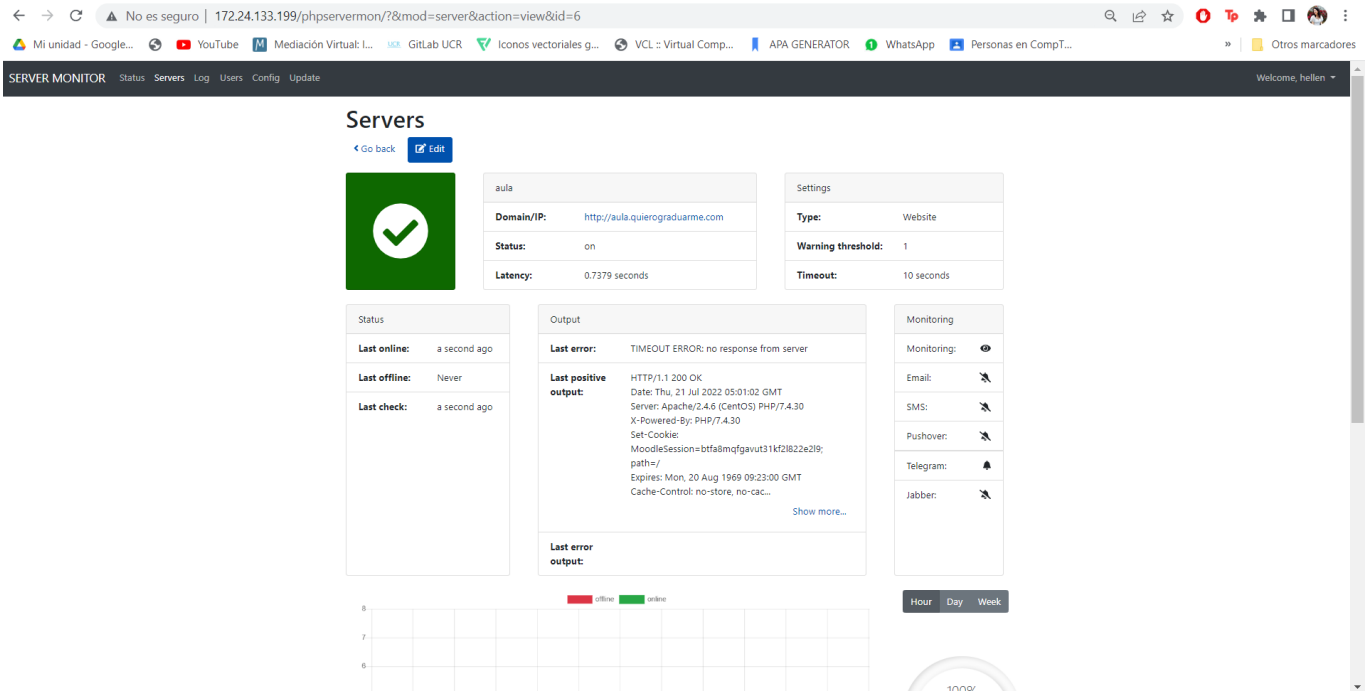


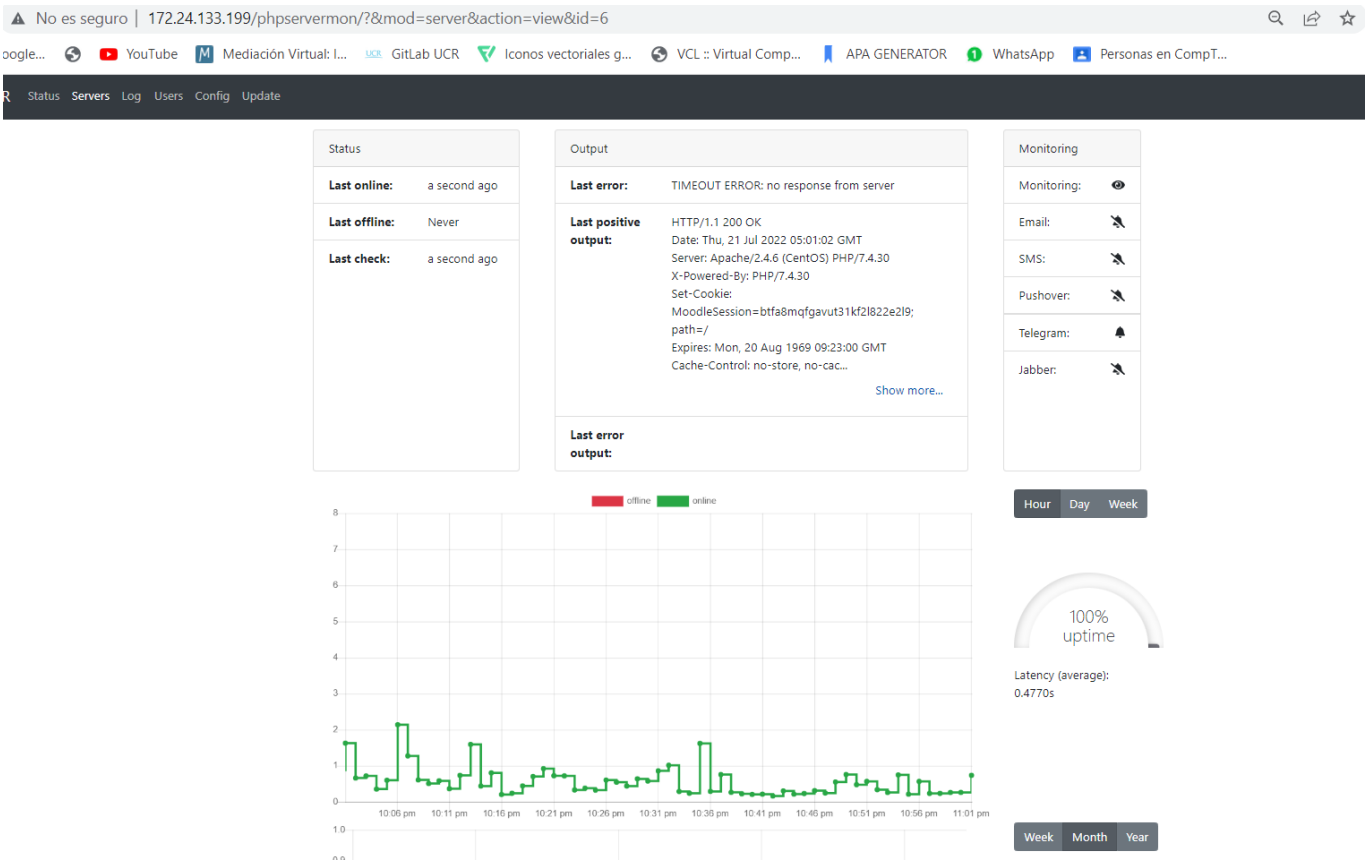
Una vez que ingresa se dirige a participantes y va a ver su nombre

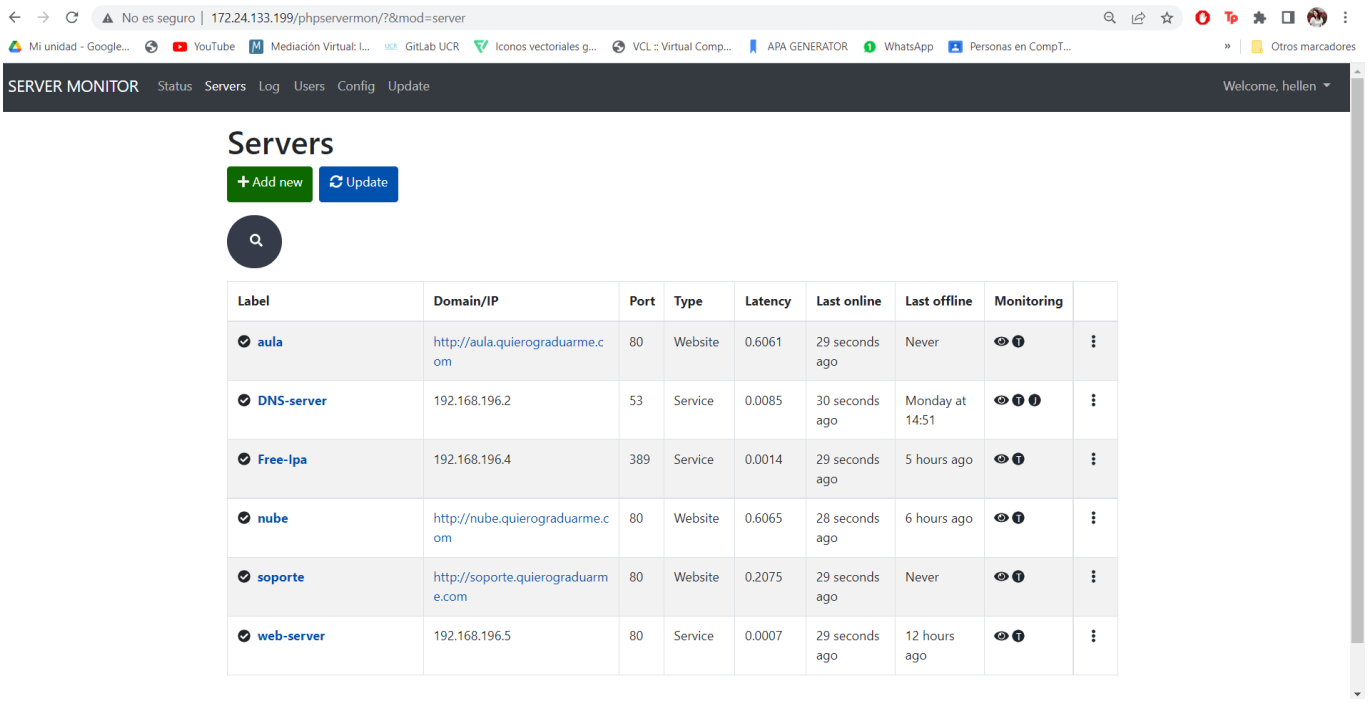


Prueba phpmonitor









Label	Domain/IP	Port	Type	Latency	Last online	Last offline	Monitoring
aula	http://aula.quierograduarme.com	80	Website	0.6061	29 seconds ago	Never	
DNS-server	192.168.196.2	53	Service	0.0085	30 seconds ago	Monday at 14:51	
Free-Ipa	192.168.196.4	389	Service	0.0014	29 seconds ago	5 hours ago	
nube	http://nube.quierograduarme.com	80	Website	0.6065	28 seconds ago	6 hours ago	
soporte	http://soporte.quierograduarme.com	80	Website	0.2075	29 seconds ago	Never	
web-server	192.168.196.5	80	Service	0.0007	29 seconds ago	12 hours ago	