

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

Descripción	3
Partes interesadas y preocupaciones	3
1.1 Partes interesadas	3
1.2 Preocupaciones	3
2. Viewpoints	4
2.2 Arquitectura de servicios	4
2.3 Arquitectura física	4
2.4 Arquitectura lógica	5
2.5 Arquitectura de seguridad	6
2.5.1 Objetivos de seguridad y análisis de riesgos	6
2.5.2 Accesos permitidos	8
2.6 Arquitectura de comunicación	8
3. Restricciones y limitaciones	11
Implementación de IPSec	11
Configuración	11
Sistema de seguridad básico	18
Iptables	18
Configuración para sitio 1	18
Configuración para sitio 2	29
Servicios	36
Configuración de DHCP	36
Configuración del DNS	39
Configuración del FreeIPA	46
Configuración del FreeIPA primario	46
CA en el servidor primario	48
Configuración de un cliente para el free ipa primario	49
Instalación FreeIPA réplica	52
Configuración de un cliente para el free ipa réplica	55
Instalación de la CA en la réplica	57
Base de datos	58
Instalación de MariaDB 10.4.25	58
Servidor web	61
Instalación de apache	61
Instalación de PHP 7.4	61
Instalación de un ERP: Osticket	62
Instalación web	63
Instalación LDAP	65
Instalación de un servicio de aprendizaje en línea: Moodle	71
Instalación web	72
Instalación LDAP	77
Instalación de un servicio de almacenamiento en línea: Nextcloud	85
Instalación web	86
Configuración LDAP	88
Monitoreo de servicios: php server monitor	94

Pruebas	107
Cliente sitio 1 a cliente sitio 2	107
Cliente sitio 1 a DMZ sitio 1	107
Cliente sitio 1 a DMZ sitio 2	108
DMZ sitio 1 a cliente sitio 1	108
DMZ sitio 2 a cliente sitio 2	109
Cliente sitio 1 a DNS	109
Cliente sitio 2 a DNS	110
Cliente sitio 1 a internet	110
Cliente sitio 2 a internet	111
Internet a DNS	112
SSH cliente sitio 1 a DNS	113
SSH cliente sitio 2 a DNS	113
SSH internet a DNS sitio 1	113
SSH internet a DNS sitio 2	114
Funcionamiento de réplica sin CA	115
Funcionamiento de réplica con CA	119
Prueba NextCloud	120
Prueba Osticket	125
Prueba Moodle	129
Prueba phpmonitor	134

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 accedita 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.

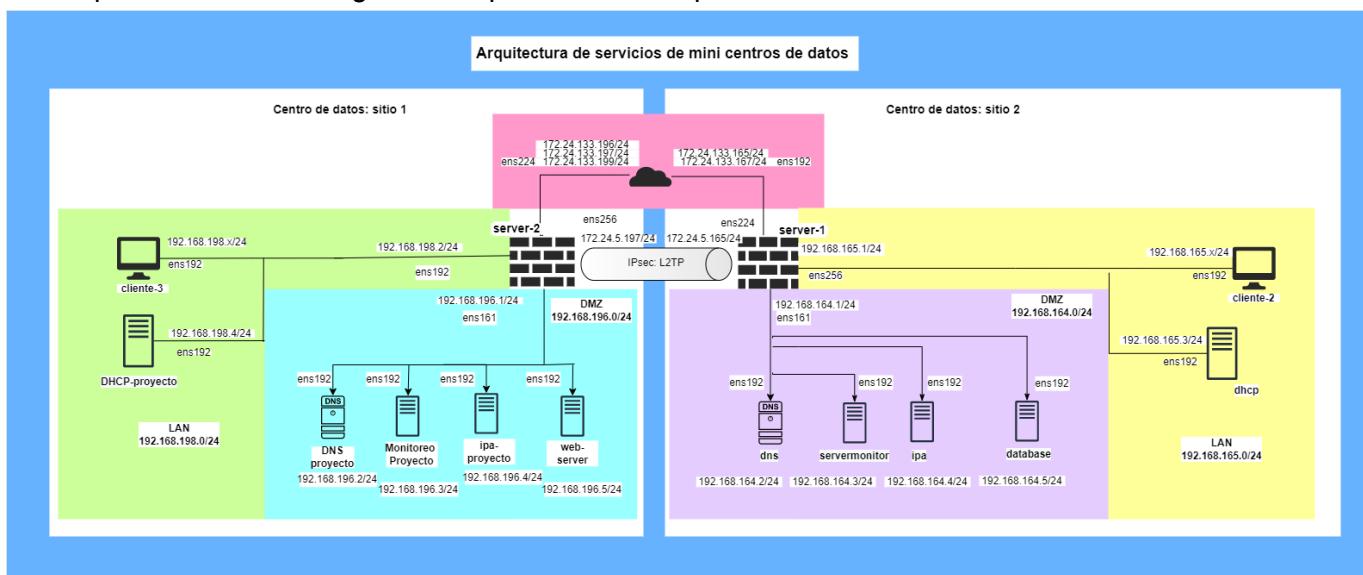
- Tener acceso a soporte cuando tenga algún incidente tecnológico o de acceso.
- Llevar control de los incidentes reportados, de los incidentes resueltos y de las categorías.
- Tener un servicio de almacenamiento en línea sin depender de terceros por cuestiones de seguridad.

2. Viewpoints

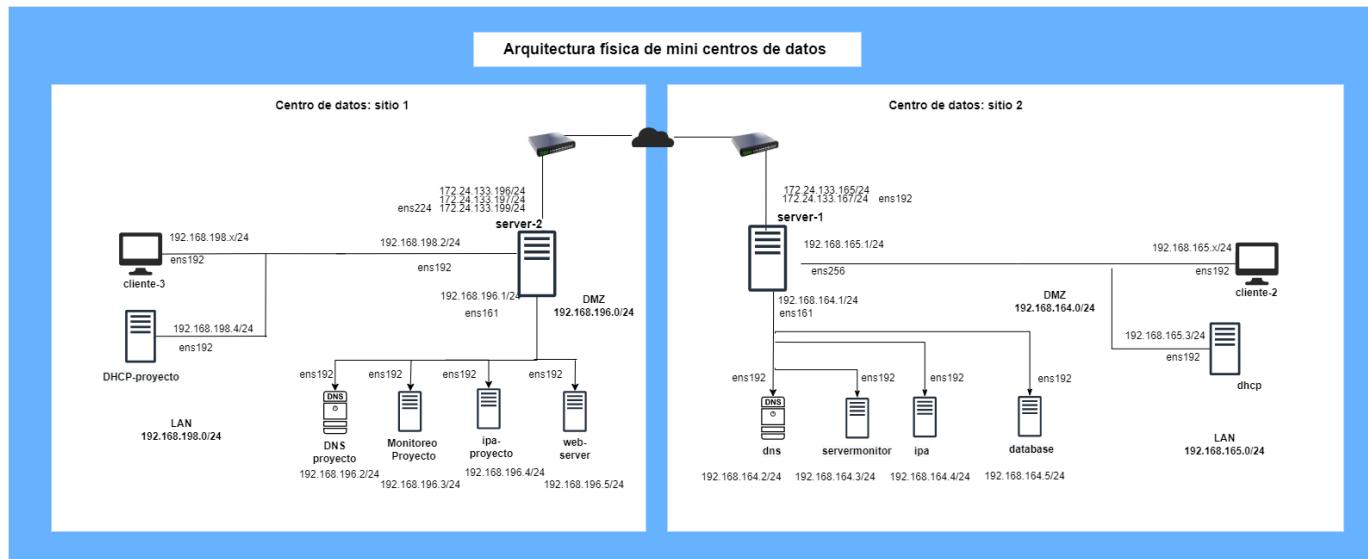
En esta sección se presenta el diagrama completo de los sitios de la organización y sus respectivos componentes. También se describe la arquitectura física, lógicas, de seguridad y de comunicación del sistema.

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.

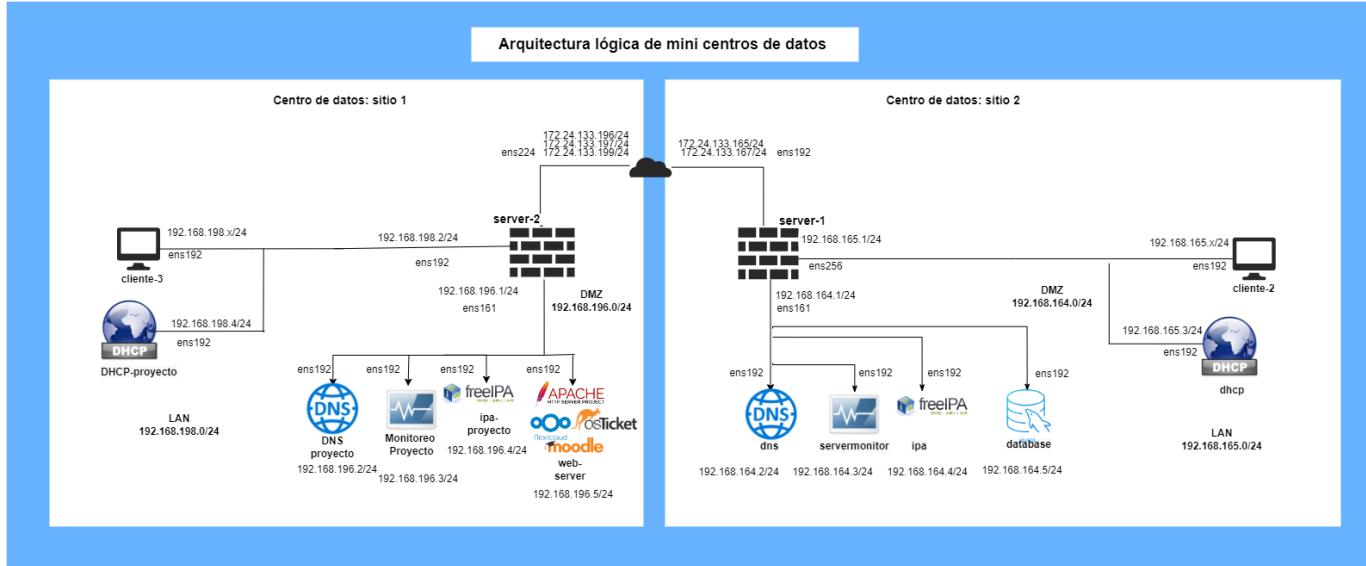


2.3 Arquitectura física



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 utilizan 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.

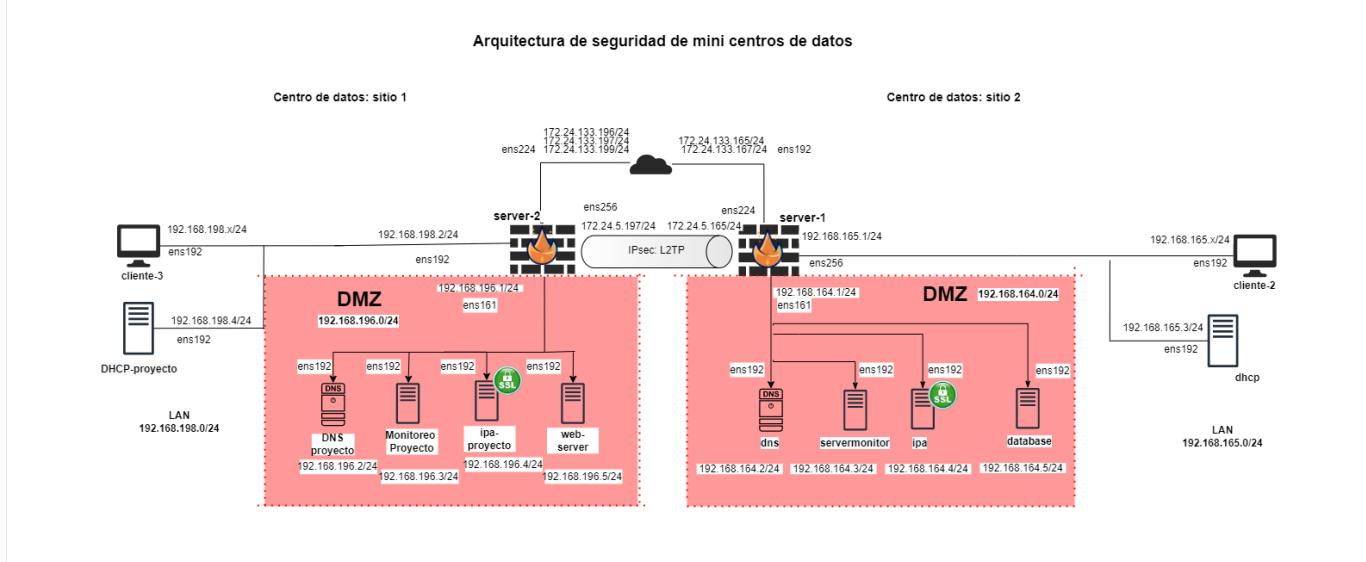
2.4 Arquitectura lógica



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.quierograduar.me.com
nextcloud	nube.quierograduar.me.com
osTicket	soporte.quierograduar.me.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.

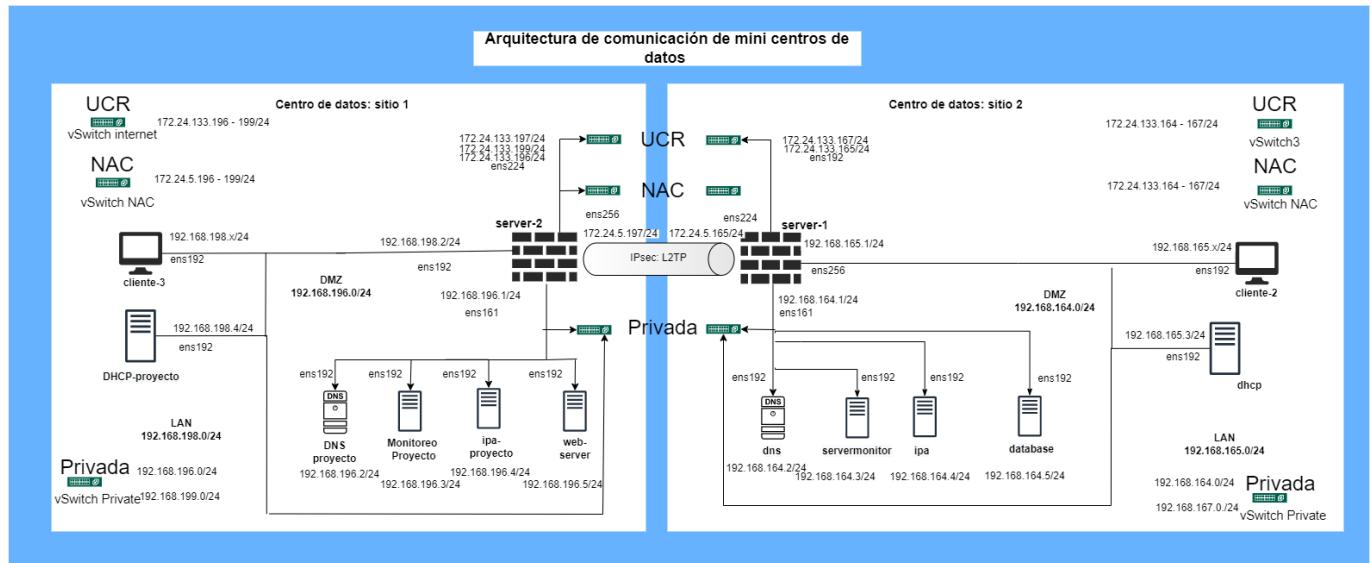
2.5.2 Accesos permitidos

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	quierograduar.me.com
Dominio DNS interno	quierograduar.me.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 funcionen 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
```

```
[root@server-1 hellen]# cat /etc/sysctl.conf  
# sysctl settings are defined through files in  
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.  
#  
# Vendors settings live in /usr/lib/sysctl.d/.  
# To override a whole file, create a new file with the same in  
# /etc/sysctl.d/ and put new settings there. To override  
# only specific settings, add a file with a lexically later  
# name in /etc/sysctl.d/ and put new settings there.  
#  
# For more information, see sysctl.conf(5) and sysctl.d(5).  
net.ipv4.ip_forward = 1  
net.ipv6.conf.all.forwarding = 1  
net.ipv4.conf.all.accept_redirects = 0  
net.ipv4.conf.all.send_redirects = 0  
[root@server-1 hellen]#
```

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

```
# sysctl -p
```

- 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@server-2 ~]# cat /etc/sysconfig/network-scripts/route-eth1  
192.168.165.0/24 via 172.24.5.197  
[root@server-2 ~]# cat /etc/sysconfig/network-scripts/route-eth0  
192.168.164.0/24 via 172.24.5.197  
  
[root@server-2 ~]#
```

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

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

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

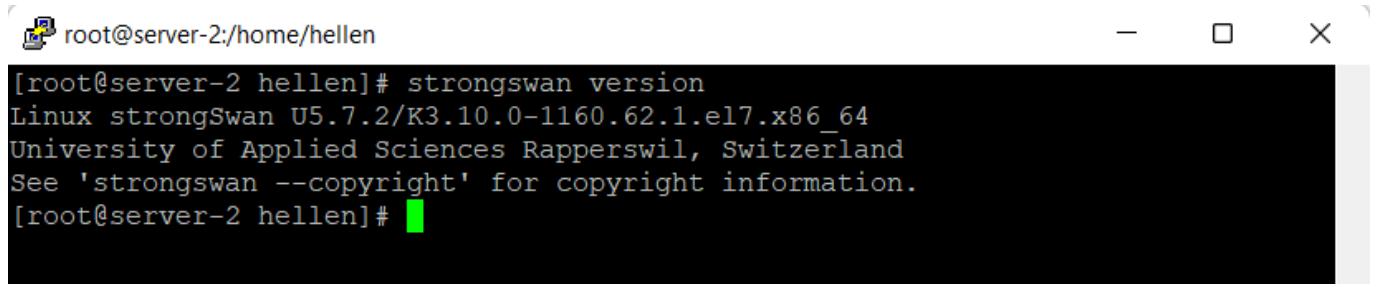
```
# systemctl restart NetworkManager
```

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
```



```
[root@server-2 hellen]# strongswan version
Linux strongSwan U5.7.2/K3.10.0-1160.62.1.el7.x86_64
University of Applied Sciences Rapperswil, Switzerland
See 'strongswan --copyright' for copyright information.
[root@server-2 hellen]#
```

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 "SSF2Iy0Ld0KMLkJfnHnUIvf/7k9ABBp6"
```

```
[root@server-2:/etc/sysconfig]
[root@server-2 sysconfig]# cat /etc/strongswan/ipsec.secrets
# ipsec.secrets - strongSwan IPsec secrets file
#172.24.5.197 172.24.5.196 : PSK "5QueGnxk8aUiYSlxRnCTqnW0jshovC27"
172.24.5.197 172.24.5.165 : PSK "SSF2Iy0Ld0KMLkJfnHnUIvf/7k9ABBp6"
[root@server-2 sysconfig]#
```

Server-1 (sitio 2)

```
# ipsec.secrets - strongSwan IPsec secrets file
172.24.5.165 172.24.5.197 : PSK "SSF2Iy0Ld0KMLkJfnHnUIvf/7k9ABBp6"
```

```
[root@server1:/home/usuarioadmin]
[root@server1 usuarioadmin]# cat /etc/strongswan/ipsec.secrets
# ipsec.secrets - strongSwan IPsec secrets file
#172.24.5.165 172.24.5.166 : PSK "9IZpzepl07EFZdPj3KNUvjXMHKYceNEG"
172.24.5.165 172.24.5.197 : PSK "SSF2Iy0Ld0KMLkJfnHnUIvf/7k9ABBp6"
[root@server1 usuarioadmin]#
```

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

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

```
[root@server-2 ~]# 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 ~]#
```

```
[root@server1 ~]# 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 ~]#
```

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 través 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
```

```
[root@localhost dhcpcd]# cat /etc/sysconfig/dhcpd
# WARNING: This file is NOT used anymore.

# If you are here to restrict what interfaces should dhcpcd listen on,
# be aware that dhcpcd listens *only* on interfaces for which it finds subnet
# declaration in dhcpcd.conf . It means that explicitly enumerating interfaces
# also on command line should not be required in most cases.

# If you still insist on adding some command line options,
# copy dhcpcd.service from /lib/systemd/system to /etc/systemd/system and modify
# it there.
# https://fedoraproject.org/wiki/Systemd#How_do_I_customize_a_unit_file.ZF_add_a_custom_unit_file.3F

# example:
# $ cp /usr/lib/systemd/system/dhcpcd.service /etc/systemd/system/
# $ vi /etc/systemd/system/dhcpcd.service
# $ ExecStart=/usr/sbin/dhcpcd -f -cf /etc/dhcp/dhcpcd.conf -user dhcpcd -group dhcpcd --no-pid <your_interface_name(s)>
# $ systemctl --system daemon-reload
# $ systemctl restart dhcpcd.service
DHCPDARGS="ens192"
[root@localhost dhcpcd]#
```

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/dhcpcd.conf.ejemplo /etc/dhcp/dhcpcd.conf
```

```
nano /etc/dhcp/dhcpcd.conf
```

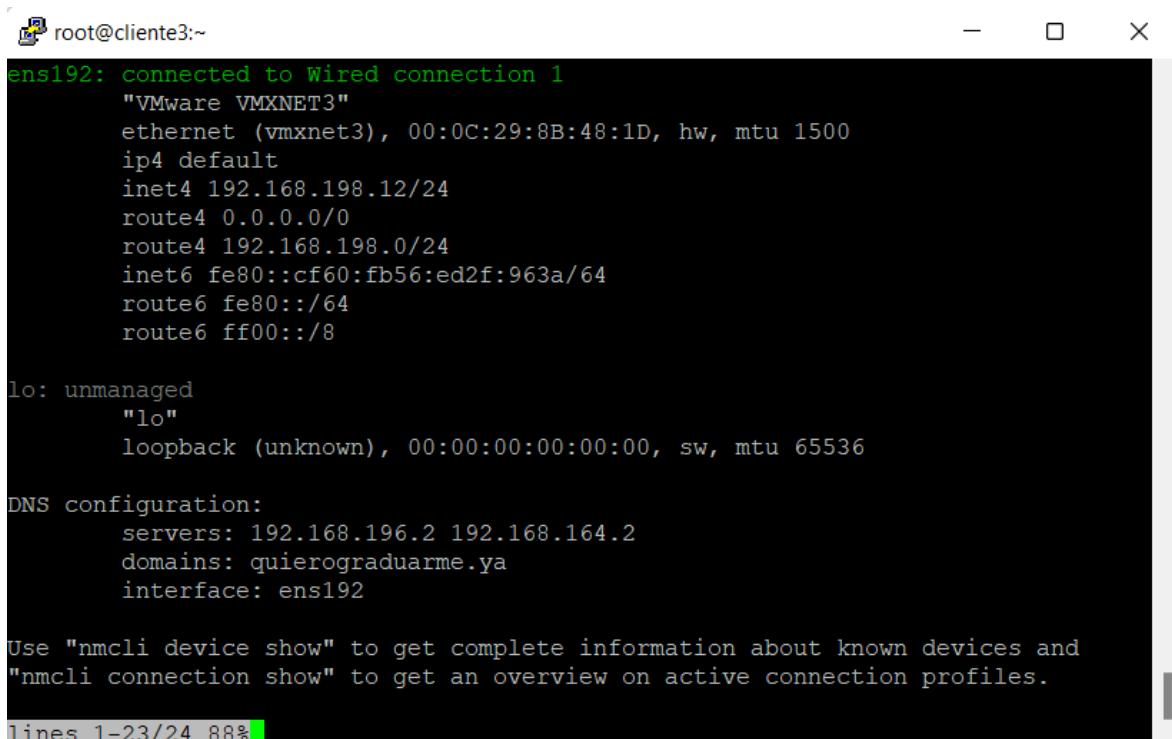
Y modifique esta sección de acuerdo a sus valores de la infraestructura:

```
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 "quierograduar.me.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 dhcpcd  
# systemctl enable dhcpcd  
# systemctl enable dhcpcd
```

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 quierograduar.me.ya:



A screenshot of a terminal window titled "root@cliente3:~". The window displays the output of the command "nmcli connection show". The output shows a connection named "ens192" connected to "Wired connection 1" (VMware VMXNET3). It details an ethernet interface (vmxnet3) with MAC address 00:0C:29:8B:48:1D, MTU 1500, and IP4 configuration (inet4) with address 192.168.198.12/24. It also lists routes (route4) and IPv6 information (inet6, route6). Another interface, "lo", is shown as unmanaged. DNS configuration includes servers at 192.168.196.2 and 192.168.164.2, and domains quierograduar.me.ya. A message at the bottom indicates how to get complete device and connection profiles.

```
ens192: connected to Wired connection 1  
    "VMware VMXNET3"  
    ethernet (vmxnet3), 00:0C:29:8B:48:1D, hw, mtu 1500  
    ip4 default  
    inet4 192.168.198.12/24  
        route4 0.0.0.0/0  
        route4 192.168.198.0/24  
    inet6 fe80::cf60:fb56:ed2f:963a/64  
        route6 fe80::/64  
        route6 ff00::/8  
  
lo: unmanaged  
    "lo"  
    loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536  
  
DNS configuration:  
    servers: 192.168.196.2 192.168.164.2  
    domains: quierograduar.me.ya  
    interface: ens192  
  
Use "nmcli device show" to get complete information about known devices and  
"nmcli connection show" to get an overview on active connection profiles.  
lines 1-23/24 88%
```

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:

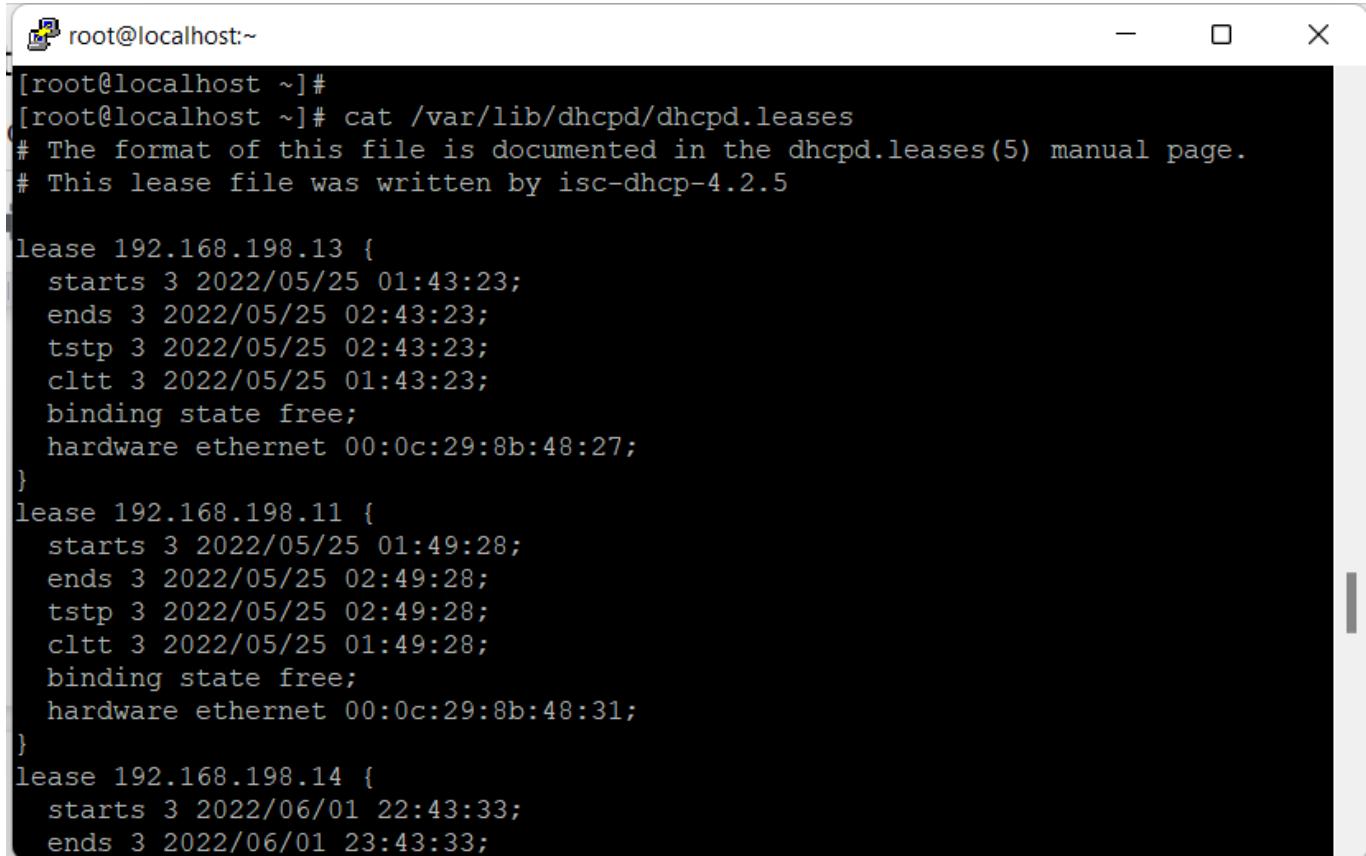
```
BOOTPROTO=dhcp  
TYPE=Ethernet  
ONBOOT=yes
```

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 dhcpcd.leases
```



A terminal window titled "root@localhost:~" showing the contents of the dhcpcd.leases file. The file lists three leases for IP addresses 192.168.198.13, 192.168.198.11, and 192.168.198.14, each with their respective start and end times, TSTP, CLTT, and hardware information.

```
[root@localhost ~]# cat /var/lib/dhcpd/dhcpcd.leases
# The format of this file is documented in the dhcpcd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.2.5

lease 192.168.198.13 {
    starts 3 2022/05/25 01:43:23;
    ends 3 2022/05/25 02:43:23;
    tstp 3 2022/05/25 02:43:23;
    cltt 3 2022/05/25 01:43:23;
    binding state free;
    hardware ethernet 00:0c:29:8b:48:27;
}
lease 192.168.198.11 {
    starts 3 2022/05/25 01:49:28;
    ends 3 2022/05/25 02:49:28;
    tstp 3 2022/05/25 02:49:28;
    cltt 3 2022/05/25 01:49:28;
    binding state free;
    hardware ethernet 00:0c:29:8b:48:31;
}
lease 192.168.198.14 {
    starts 3 2022/06/01 22:43:33;
    ends 3 2022/06/01 23:43:33;
```

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	quierograduar.me.com	Servicios de dominio externo para web.

Interno	quierograduar.me.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 "quierograduar.me.com" IN {
type master;
file "forward.quierograduar.me";
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.quierograduar.me";
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.quierograduar.mesitio2";
allow-update { none; };
allow-transfer {192.168.164.2; };
forwarders {
163.178.88.2;
163.178.84.4;
```

```

};

};

zone "quierograduar.me.ya" IN {
type master;
file "forward.quierograduar.me.interno";
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.quierograduar.me.interno";
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.quierograduar.me.interno.sitio2";
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.quierograduar.me
```

Así es como quedaría la configuración:

```
$TTL 86400  
@ IN SOA masterdns.quierograduar.me. secondarydns.quierograduar.me. (  
    2022072007 ;Serial  
    3600        ;Refresh  
    1800        ;Retry  
    604800      ;Expire  
    86400       ;Minimum TTL  
)  
  
@ IN NS masterdns.quierograduar.me.  
@ IN NS secondarydns.quierograduar.me.  
@ 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  
wwwaula IN A 192.168.196.5  
nube IN A 192.168.196.5  
wwwnube IN A 192.168.196.5  
soporte IN A 192.168.196.5  
wwwsoporte IN A 192.168.196.5  
ipa1.quierograduar.me.ya IN A 192.168.196.4  
ipareplica.quierograduar.me.ya IN A 192.168.164.4
```

Ahora para la zona interna:

```
nano forward.quierograduar.me.interno
```

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

```

$TTL 86400
@  IN  SOA      masterdns.quierograduar.me. root.quierograduar.me. (
    20223434 ;Serial
    3600    ;Refresh
    1800    ;Retry
    604800  ;Expire
    86400   ;Minimum TTL
)
@  IN  NS       masterdns.quierograduar.me.
@  IN  NS       secondarydns.quierograduar.me.
@  IN  PTR      quierograduar.me.
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.quierograduar.me.
4  IN  PTR      ipa1.quierograduar.me.ya.
5  IN  PTR      nube.quierograduar.me.
5  IN  PTR      aula.quierograduar.me.
5  IN  PTR      soporte.quierograduar.me.

```

Para la zona externa en sitio 2:

```
nano reverse.quierograduar.me.sitio2
```

```

$TTL 86400
@  IN  SOA      secondary.quierograduar.me. root.quierograduar.me. (
    202207462 ;Serial
    3600    ;Refresh
    1800    ;Retry
    604800  ;Expire

```

```

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

```

Para la zona interna en sitio 1:

```
nano reverse.quierograduar.me.ya
```

```

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

```

Para la zona interna en sitio 2:

```
nano reverse.quierograduar.meinternositio2
```

```

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

```

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

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

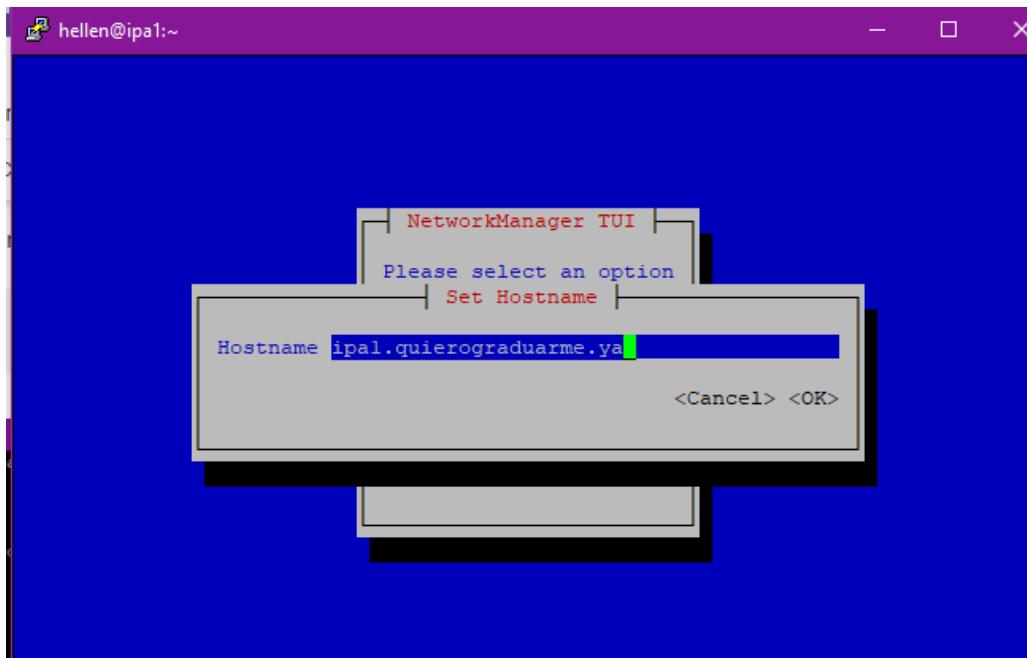
Configuración del FreeIPA

Freipa 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 (quierograduar.me.ya).

Configuración del FreeIPA primario

Para instalar y configurar el servidor primario de Freipa 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.quierograduar.me.ya*:



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

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

```

hellen@ipa1:~
[hellen@ipa1 ~]$ hostname -f
ipal.quierograduarne.ya
[hellen@ipa1 ~]$ 

```

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.quierograduarne.ya' --mkhomedir
--domain=quierograduarne.ya --realm=QUIEROGRADUARME.YA --ds-password=maggielu2.
--admin-password=maggielu2. --no-ntp
```

```

root@ipa1:/home/hellen
[root@ipa1 hellen]# hostname -f
ipal.quierograduarne.ya
[root@ipa1 hellen]# ipa-server-install --hostname='ipa1.quierograduarne.ya' --mkhomedir --domain=quierograduarne.ya --realm=QUIEROGRADUARME.YA --ds-password=maggielu2. --admin-password=maggielu2. --no-ntp

The log file for this installation can be found in /var/log/ipaserver-install.log
=====
This program will set up the IPA Server.

This includes:
 * Configure a stand-alone CA (dogtag) for certificate management
 * Create and configure an instance of Directory Server
 * Create and configure a Kerberos Key Distribution Center (KDC)
 * Configure Apache (httpd)
 * Configure the KDC to enable PKIT

Excluded by options:
 * Configure the Network Time Daemon (ntpd)

To accept the default shown in brackets, press the Enter key.

Do you want to configure integrated DNS (BIND)? [no]: no

The IPA Master Server will be configured with:
Hostname: ipal.quierograduarne.ya
IP address(es): 192.168.196.4
Domain name: quierograduarne.ya
Realm name: QUIEROGRADUARME.YA

Continue to configure the system with these values? [no]: yes
The following operations may take some minutes to complete.
Please wait until the prompt is returned.

Configuring directory server (dirsrv). Estimated time: 30 seconds
 [1/45]: creating directory server instance
 [2/45]: enabling ldapi
 [3/45]: configure autorebind for root
 [4/45]: stopping directory server
 [5/45]: updating configuration in dse.ldif
 [6/45]: starting directory server
 [7/45]: adding default schema
 [8/45]: enabling memberof plugin

```

```

root@ipa1:/home/hellen
Configured sudoers in /etc/nsswitch.conf
Configured /etc/sssd/sssd.conf
trying https://ipa.quierograduar.me.ya/ipa/json
[try 1]: Forwarding 'schema' to json server 'https://ipa.quierograduar.me.ya/ipa/json'
trying https://ipa.quierograduar.me.ya/ipa/session/json
[try 1]: Forwarding 'ping' to json server 'https://ipa.quierograduar.me.ya/ipa/session/json'
[try 1]: Forwarding 'ca_is_enabled' to json server 'https://ipa.quierograduar.me.ya/ipa/session/json'
Systemwide CA database updated.
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
[try 1]: Forwarding 'host mod' to json server 'https://ipa.quierograduar.me.ya/ipa/session/json'
Could not update DNS SSHFP records.
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring quierograduar.me.ya as NIS domain.
Client configuration complete.
The ipa-client-install command was successful

Please add records in this file to your DNS system: /tmp/ipa.system.records.oFOOMt.db
=====
Setup complete

Next steps:
1. You must make sure these network ports are open:
   TCP Ports:
   * 80, 443: HTTP/HTTPS
   * 389, 636: LDAP/LDAPS
   * 88, 464: kerberos
   UDP Ports:
   * 88, 464: kerberos

2. You can now obtain a kerberos ticket using the command: 'kinit admin'
   This ticket will allow you to use the IPA tools (e.g., ipa user-add)
   and the web user interface.
3. Kerberos requires time synchronization between clients
   and servers for correct operation. You should consider enabling ntpd.

Be sure to back up the CA certificates stored in /root/cacert.p12
These files are required to create replicas. The password for these
files is the Directory Manager password
[root@ipa1 hellen]#

```

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
```

```

root@ipa1 hellen]# yum -y update nss
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.epn.edu.ec
 * extras: mirror.epn.edu.ec
 * updates: mirror.epn.edu.ec
Resolving Dependencies
There are unfinished transactions remaining. You might consider running yum-complete-transaction, or "yum-complete-transaction --cleanup-only" and "yum history redo last", first to finish them. If those don't work you'll have to try removing/installing packages by hand (maybe package-cleanup can help).
The program yum-complete-transaction is found in the yum-utils package.
--> Running transaction check
--> Package nss.x86_64 0:3.44.0-7.el7_7 will be updated
--> Processing Dependency: nss = 3.44.0-7.el7_7 for package: nss-sysinit-3.44.0-7.el7_7.x86_64
--> Processing Dependency: nss(x86-64) = 3.44.0-7.el7_7 for package: nss-tools-3.44.0-7.el7_7.x86_64
--> Package nss.x86_64 0:3.67.0-4.el7_9 will be an update
--> Processing Dependency: nss-util >= 3.67.0-1 for package: nss-3.67.0-4.el7_9.x86_64
--> Processing Dependency: nss-softokn(x86-64) >= 3.67.0-1 for package: nss-3.67.0-4.el7_9.x86_64
--> Processing Dependency: nspr >= 4.31.0 for package: nss-3.67.0-4.el7_9.x86_64
--> Processing Dependency: libnssutil3.so(NSSUTIL_3.59) (64bit) for package: nss-3.67.0-4.el7_9.x86_64
--> Running transaction check
--> Package nspr.x86_64 0:4.21.0-1.el7 will be updated
--> Package nspr.x86_64 0:4.32.0-1.el7_9 will be an update
--> Package nss-softokn.x86_64 0:3.44.0-8.el7_7 will be updated
--> Package nss-softokn.x86_64 0:3.67.0-3.el7_9 will be an update
--> Processing Dependency: nss-softokn-freebl(x86-64) >= 3.67.0-3.el7_9 for package: nss-softokn-3.67.0-3.el7_9.x86_64
--> Package nss-sysinit.x86_64 0:3.44.0-7.el7_7 will be updated
--> Package nss-sysinit.x86_64 0:3.67.0-4.el7_9 will be an update
--> Package nss-tools.x86_64 0:3.44.0-7.el7_7 will be updated

```

```
Password for admin@QUIEROGRADUARME.YA:
Successfully retrieved CA cert
  Subject: CN=Certificate Authority,O=QUIEROGRADUARME.YA
  Issuer:  CN=Certificate Authority,O=QUIEROGRADUARME.YA
  Valid From: 2022-06-21 04:24:45
  Valid Until: 2042-06-21 04:24:45

Enrolled in IPA realm QUIEROGRADUARME.YA
Created /etc/ipa/default.conf
New SSSD config will be created
Configured sudoers in /etc/nsswitch.conf
Configured /etc/sssd/sssd.conf
Configured /etc/krb5.conf for IPA realm QUIEROGRADUARME.YA
trying https://ipa1.quierograduarne.ya/ipa/json
[try 1]: Forwarding 'schema' to json server 'https://ipa1.quierograduarne.ya/ipa/json'
trying https://ipa1.quierograduarne.ya/ipa/session/json
[try 1]: Forwarding 'ping' to json server 'https://ipa1.quierograduarne.ya/ipa/session/json'
[try 1]: Forwarding 'ca_is_enabled' to json server 'https://ipa1.quierograduarne.ya/ipa/session/json'

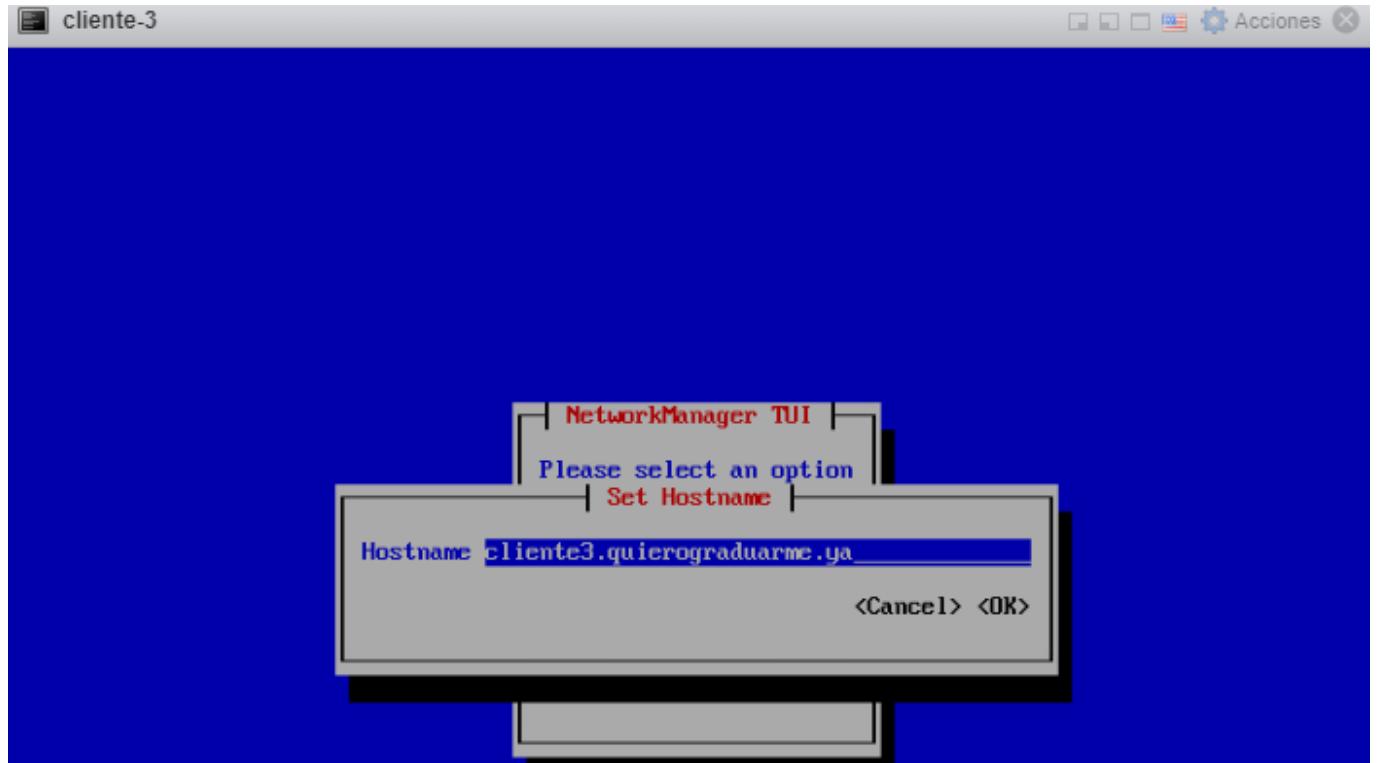
Systemwide CA database updated.
Hostname (cliente3.quierograduarne.ya) does not have A/AAAA record.
Failed to update DNS records.
Missing A/AAAA record(s) for host cliente3.quierograduarne.ya: 192.168.198.12.
Missing reverse record(s) for address(es): 192.168.198.12.
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
[try 1]: Forwarding 'host_mod' to json server 'https://ipa1.quierograduarne.ya/ipa/session/json'
Could not update DNS SSHFP records.
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring quierograduarne.ya as NIS domain.
Client configuration complete.
The ipa-client-install command was successful
[root@cliente3 hellen]# _
```

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.quierograduarne.ya' --mkhomedir  
--server=ipa1.quierograduarne.ya --domain=quierograduarne.ya  
--realm=QUIEROGRADUARME.YA --no-ntp -p admin
```

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

```
cliente-3
cliente-3
Password for admin@QUIEROGRADUARME.YA:
Successfully retrieved CA cert
  Subject: CN=Certificate Authority,O=QUIEROGRADUARME.YA
  Issuer:  CN=Certificate Authority,O=QUIEROGRADUARME.YA
  Valid From: 2022-06-21 04:24:45
  Valid Until: 2042-06-21 04:24:45

Enrolled in IPA realm QUIEROGRADUARME.YA
Created /etc/ipa/default.conf
New SSSD config will be created
Configured sudoers in /etc/nsswitch.conf
Configured /etc/sssd/sssd.conf
Configured /etc/krb5.conf for IPA realm QUIEROGRADUARME.YA
trying https://ipa1.quierograduarne.ya/ipa/json
[try 1]: Forwarding 'schema' to json server 'https://ipa1.quierograduarne.ya/ipa/json'
trying https://ipa1.quierograduarne.ya/ipa/session/json
[try 1]: Forwarding 'ping' to json server 'https://ipa1.quierograduarne.ya/ipa/session/json'
[try 1]: Forwarding 'ca_is_enabled' to json server 'https://ipa1.quierograduarne.ya/ipa/session/json'

Systemwide CA database updated.
Hostname (cliente3.quierograduarne.ya) does not have A/AAAA record.
Failed to update DNS records.
Missing A/AAAA record(s) for host cliente3.quierograduarne.ya: 192.168.198.12.
Missing reverse record(s) for address(es): 192.168.198.12.
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
[try 1]: Forwarding 'host_mod' to json server 'https://ipa1.quierograduarne.ya/ipa/session/json'
Could not update DNS SSHFP records.
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring quierograduarne.ya as NIS domain.
Client configuration complete.
The ipa-client-install command was successful
[root@cliente3 hellen]# _
```

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

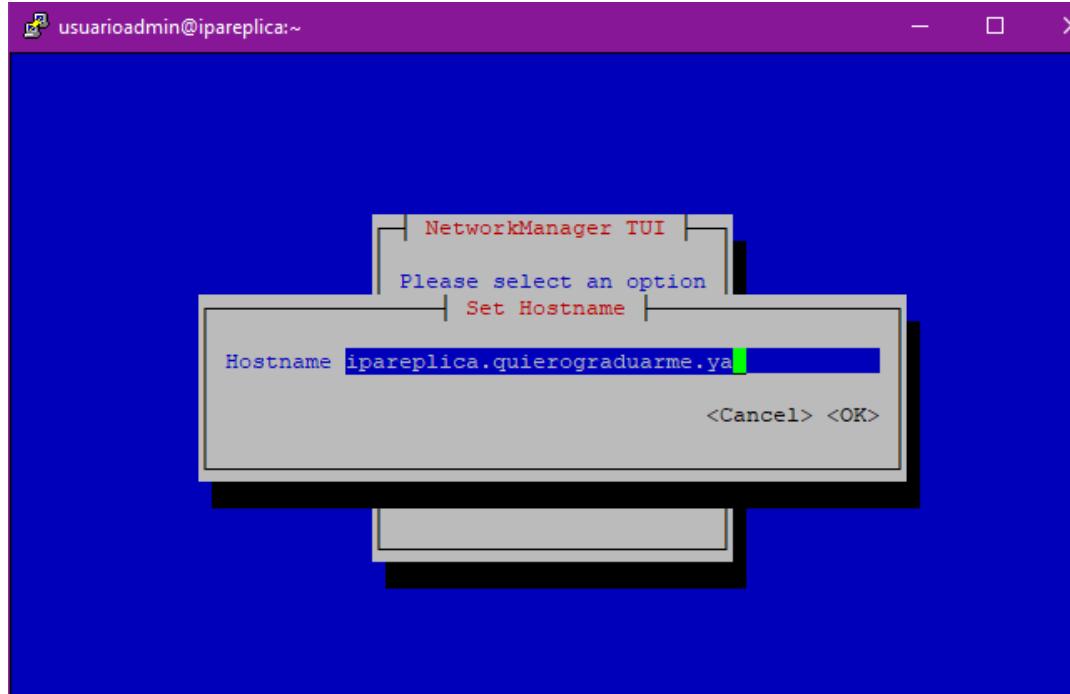
```
kinit admin
```

```
cliente-3
cliente-3
[root@cliente3 hellen]# kinit admin
Password for admin@QUIEROGRADUARME.YA:
[root@cliente3 hellen]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@QUIEROGRADUARME.YA

Valid starting     Expires            Service principal
06/21/2022 08:48:55  06/22/2022 08:48:48  krbtgt/QUIEROGRADUARME.YA@QUIEROGRADUARME.YA
[root@cliente3 hellen]#
```

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.quierograduar.me.ya*:



```
[usuarioadmin@ipareplica:~]$ hostname -f  
ipareplica.quierograduar.me.ya  
[usuarioadmin@ipareplica:~]$
```

A screenshot of a terminal window titled "usuarioadmin@ipareplica:~". The user has run the command "hostname -f" followed by the new hostname "ipareplica.quierograduar.me.ya". The terminal prompt "[usuarioadmin@ipareplica:~]\$" is visible at the bottom.

2. Se instala y se configura como cliente:

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

```

root@ipa2:/home/usuarioadmin
Run /usr/sbin/ipa-server-install --uninstall to clean up.

ipapython.admintool: ERROR    Configuration of client side components failed!
ipapython.admintool: ERROR    The ipa-replica-install command failed. See /var/log/ipareplica-install.log for more information
[root@ipa2 usuarioadmin]#
[root@ipa2 usuarioadmin]# ipa-replica-install --hostname='ipa2.quierograduarne.ya' --mkhomedir --server=ipal.quierograduarne.ya --domain=quierograduarne.ya --realm=QUIEROGRADUARME.YA --no-ntp -p admin
Configuring client side components
Client hostname: ipa2.quierograduarne.ya
Realm: QUIEROGRADUARME.YA
DNS Domain: quierograduarne.ya
IPA Server: ipal.quierograduarne.ya
BaseDN: dc=quierograduarne,dc=ya

Skipping synchronizing time with NTP server.
Downloading the CA certificate via HTTP, this is INSECURE
Successfully retrieved CA cert
  Subject: CN=Certificate Authority,O=QUIEROGRADUARME.YA
  Issuer:  CN=Certificate Authority,O=QUIEROGRADUARME.YA
  Valid From: 2022-06-21 04:24:45
  Valid Until: 2042-06-21 04:24:45

Joining realm failed: TLSMC: MozNSS compatibility interception begins.
tlsmc_convert: WARN: extracted cert file is not present.
tlsmc_convert: WARN: extracted key file is not present.
tlsmc_intercept_initialization: INFO: successfully intercepted TLS initialization. Continuing with OpenSSL only.
TLSMC: MozNSS compatibility interception ends.
Bind failed: Invalid credentials

Installation failed. Rolling back changes.
Unconfigured autount client failed: Command '/usr/sbin/ipa-client-autounmount --uninstall --debug' returned non-zero exit status 1
Disabling client Kerberos and LDAP configurations
Redundant SSSD configuration file /etc/sssd/sssd.conf was moved to /etc/sssd/sssd.conf.deleted
nsqd daemon is not installed, skip configuration
nsld daemon is not installed, skip configuration
Client uninstall complete.
The ipa-client-install command failed. See /var/log/ipaclient-install.log for more information
Removing client side components
IPA client is not configured on this system.
The ipa-client-install command failed.

Your system may be partly configured.
Run /usr/sbin/ipa-server-install --uninstall to clean up.

```

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

```

root@ipa2:/home/usuarioadmin
Client hostname: ipa2.quierograduarne.ya
Realm: QUIEROGRADUARME.YA
DNS Domain: quierograduarne.ya
IPA Server: ipal.quierograduarne.ya
BaseDN: dc=quierograduarne,dc=ya

Continue to configure the system with these values? [no]: yes
Skipping synchronizing time with NTP server.
Password for admin@QUIEROGRADUARME.YA:
Successfully retrieved CA cert
  Subject: CN=Certificate Authority,O=QUIEROGRADUARME.YA
  Issuer:  CN=Certificate Authority,O=QUIEROGRADUARME.YA
  Valid From: 2022-06-21 04:24:45
  Valid Until: 2042-06-21 04:24:45

Enrolled in IPA realm QUIEROGRADUARME.YA
Created /etc/ipa/default.conf
New SSSD config will be created
Configured sudoers in /etc/nsswitch.conf
Configured /etc/sssd/sssd.conf
Configured /etc/krb5.conf for IPA realm QUIEROGRADUARME.YA
trying https://ipal.quierograduarne.ya/ipa/json
[try 1]: Forwarding 'schema' to json server 'https://ipal.quierograduarne.ya/ipa/json'
trying https://ipal.quierograduarne.ya/ipa/session/json
[try 1]: Forwarding 'ping' to json server 'https://ipal.quierograduarne.ya/ipa/session/json'
[try 1]: Forwarding 'ca_is_enabled' to json server 'https://ipal.quierograduarne.ya/ipa/session/json'
Systemwide CA database updated.
Hostname (ipa2.quierograduarne.ya) does not have A/AAAA record.
Failed to update DNS records.
Missing A/AAAA record(s) for host ipa2.quierograduarne.ya: 192.168.164.4.
Missing reverse record(s) for address(es): 192.168.164.4.
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
[try 1]: Forwarding 'host_mod' to json server 'https://ipal.quierograduarne.ya/ipa/session/json'
Could not update DNS SSHFP records.
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring quierograduarne.ya as NIS domain.
Client configuration complete.
The ipa-client-install command was successful
[root@ipa2 usuarioadmin]#

```

3. Se agrega al grupo de servers de ipa:

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

```
root@ipareplica:~# ipa hostgroup-add-member ipaservers --hosts ipareplica.quierograduar.me.ya
Host-group: ipaservers
Description: IPA server hosts
Member hosts: ipa1.quierograduar.me.ya, ipareplica.quierograduar.me.ya
-----
Number of members added 1
-----
root@ipareplica:~#
```

4. Se instala la réplica

ipa-replica-install

```
root@ipareplica:~# ipa-replica-install
-----
WARNING: conflicting time&date synchronization service 'chrony' will
be disabled in favor of ntpd

ipaserver.install.installutils: ERROR      Unable to resolve the IP address 192.16
8.196.4 to a host name, check /etc/hosts and DNS name resolution
Run connection check to master
Connection check OK
Configuring NTP daemon (ntpd)
[1/4]: stopping ntpd
[2/4]: writing configuration
[3/4]: configuring ntpd to start on boot
[4/4]: starting ntpd
Done configuring NTP daemon (ntpd).
Configuring directory server (dirsrv). Estimated time: 30 seconds
[1/42]: creating directory server instance
[2/42]: enabling ldapi
[3/42]: configure autbind for root
[4/42]: stopping directory server
[5/42]: updating configuration in dse.ldif
[6/42]: starting directory server
[7/42]: adding default schema
[8/42]: enabling memberof plugin
```

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

```
root@ipareplica:/home/usuarioadmin
Configuring Kerberos KDC (krb5kdc)
[1/1]: installing X509 Certificate for PKINIT
Done configuring Kerberos KDC (krb5kdc).
Applying LDAP updates
Upgrading IPA.. Estimated time: 1 minute 30 seconds
[1/10]: stopping directory server
[2/10]: saving configuration
[3/10]: disabling listeners
[4/10]: enabling DS global lock
[5/10]: disabling Schema Compat
[6/10]: starting directory server
[7/10]: upgrading server
[8/10]: stopping directory server
[9/10]: restoring configuration
[10/10]: starting directory server
Done.
Finalize replication settings
Restarting the KDC

WARNING: The CA service is only installed on one server (ipa1.quierograduar.me.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
```

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.quierograduar.me.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.quierograduar.me.ya' --mkhomedir
--server=ipa1.quierograduar.me.ya --domain=quierograduar.me.ya
--realm=QUIEROGRADUARME.YA --no-ntp -p admin
```

```
cliente1
Issuer: CN=Certificate Authority,O=QUIEROGRADUARME.YA
Valid From: 2022-06-21 04:24:45
Valid Until: 2042-06-21 04:24:45

Enrolled in IPA realm QUIEROGRADUARME.YA
Created /etc/ipa/default.conf
New SSSD config will be created
Configured sudoers in /etc/nsswitch.conf
Configured /etc/sssd/sssd.conf
Configured /etc krb5.conf for IPA realm QUIEROGRADUARME.YA
trying https://ipareplica.quierograduarne.ya/ipa/json
[try 1]: Forwarding 'schema' to json server 'https://ipareplica.quierograduarne.ya/ipa/json'
trying https://ipareplica.quierograduarne.ya/ipa/session/json
[try 1]: Forwarding 'ping' to json server 'https://ipareplica.quierograduarne.ya/ipa/session/json'
[try 1]: Forwarding 'ca_is_enabled' to json server 'https://ipareplica.quierograduarne.ya/ipa/session/json'
Systemwide CA database updated.
Hostname (clienterep.quierograduarne.ya) does not have A/AAAA record.
Failed to update DNS records.
Missing A/AAAA record(s) for host clienterep.quierograduarne.ya: 192.168.165.128.
Missing reverse record(s) for address(es): 192.168.165.128.
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
[try 1]: Forwarding 'host_mod' to json server 'https://ipareplica.quierograduarne.ya/ipa/session/json'
Could not update DNS SSHFP records.
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring quierograduarne.ya as NIS domain.
Client configuration complete.
The ipa-client-install command was successful
[root@clienterep usuarioadmin]# ipa-client-install --hostname='clienterep.quierograduarne.ya' --mkhomedir --server=ipareplica.quierograduarne.ya --domain=quierograduarne.ya --realm=QUIEROGRADUARME.YA --no-ntp -p admin
```

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

```
kinit admin
```

```
Client configuration complete.
The ipa-client-install command was successful
[root@clienterep usuarioadmin]# kinit admin
Password for admin@QUIEROGRADUARME.YA:
[root@clienterep usuarioadmin]# klist
Ticket cache: KEYRING:persistent:8:8
Default principal: admin@QUIEROGRADUARME.YA

Valid starting     Expires            Service principal
06/21/2022 19:53:17 06/22/2022 19:53:11  krbtgt/QUIEROGRADUARME.YA@QUIEROGRADUARME.YA
[root@clienterep usuarioadmin]# _
```

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.quierograduar.me.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:

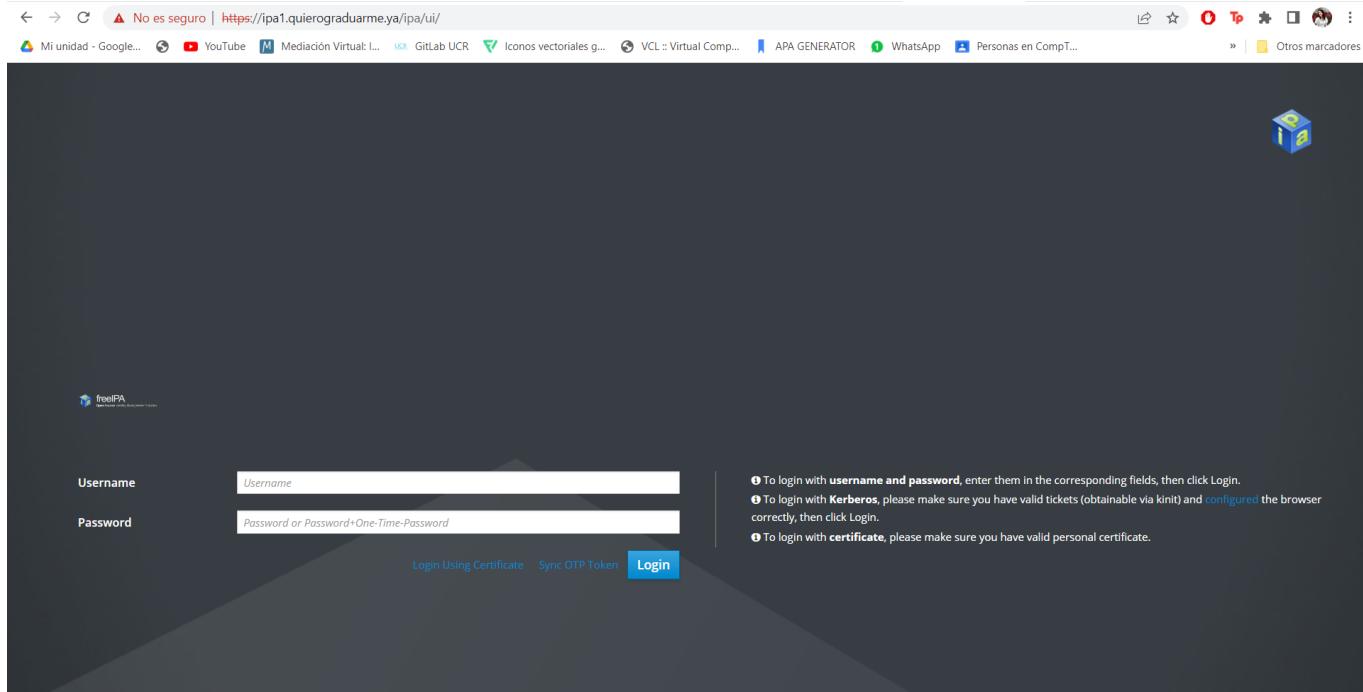
```
ipa-ca-install
```

```
[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]# ]
```

Freelpa Web

1. Se accede al siguiente sitio web y se inicia sesión:

<https://ipa1.quierograduar.me.ya/ipa/ui/>



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

User login	First name	Last name	Status	UID	Email address	Telephone Number	Job Title
admin		Aurelio	✓ Enabled	1559600000	aurelio@quierograduarne.ya		
aurelio	Aurelio	Bonillo	✓ Enabled	1559700503	aurelio@quierograduarne.ya		
diego	Diego	Madrigal	✓ Enabled	1559600005	diego@quierograduarne.ya		
hellen	Hellen	Fernandez	✓ Enabled	1559600007	hellen@quierograduarne.ya		
irvin	Irvin	Chavarria	✓ Enabled	1559700502	irvin@quierograduarne.ya		
johel	Johel	Phillips	✓ Enabled	1559600006	johel@quierograduarne.ya		
jose	Jose	Brenes	✓ Enabled	1559700505	jose@quierograduarne.ya		
jostyn	Jostyn	Delgado	✓ Enabled	1559700506	jostyn@quierograduarne.ya		
ifernandez	Lucy	Fernandez	✓ Enabled	1559600004	ifernandez@quierograduarne.ya		
maria	Maria	Peraza	✓ Enabled	1559700501	maria@quierograduarne.ya		
mfernandez	Maggie	Fernandez	✓ Enabled	1559600001	mfernandez@quierograduarne.ya		
reichel	Reichel	Mora	✓ Enabled	1559700504	reichel@quierograduarne.ya		
yerlin	Yerlin	Ledezma	✓ Enabled	1559700507	yerlin@quierograduarne.ya		
yledezma	Yerlin	Ledezma	✓ Enabled	1559600003	yledezma@quierograduarne.ya		

Showing 1 to 14 of 14 entries.

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...

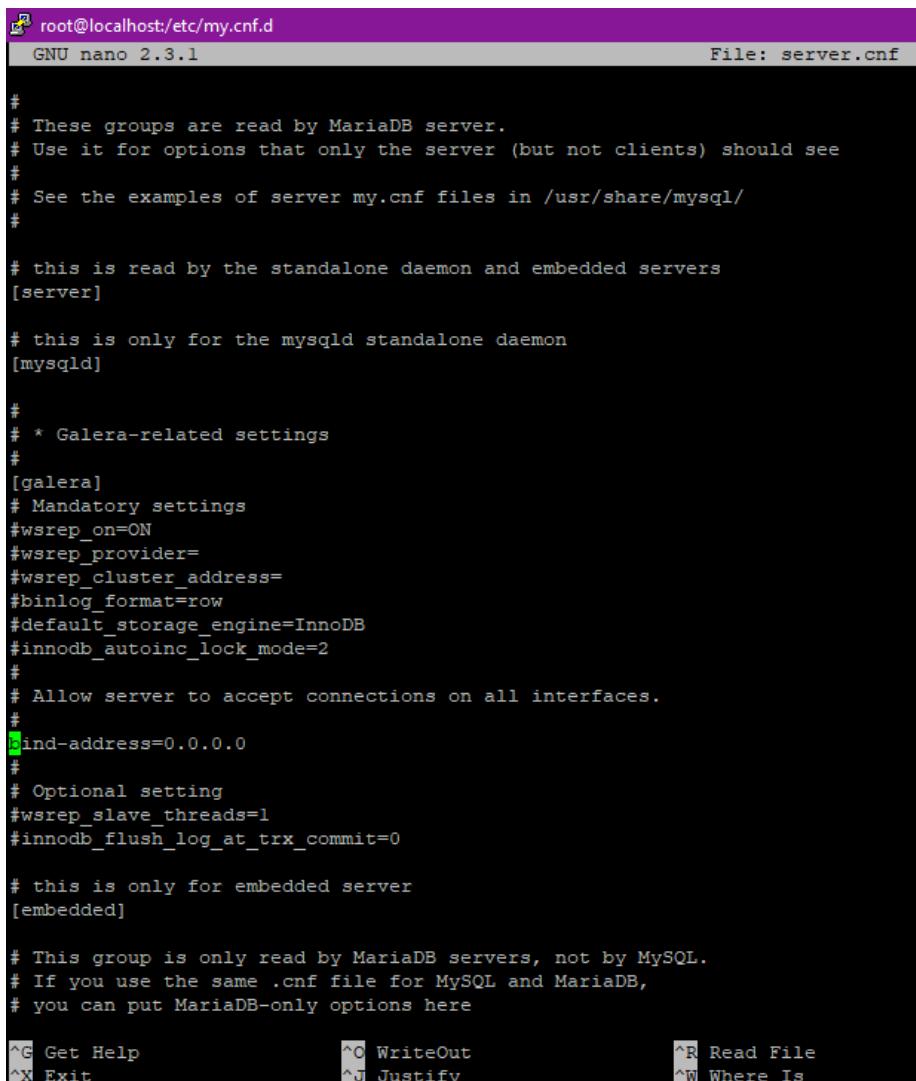
All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

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

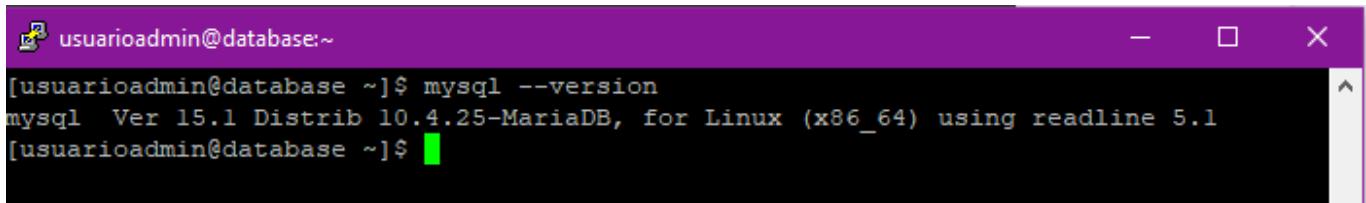
# this is only for embedded server
[embedded]

# 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



```
[usuarioadmin@database:~]$ mysql --version
mysql Ver 15.1 Distrib 10.4.25-MariaDB, for Linux (x86_64) using readline 5.1
[usuarioadmin@database ~]$
```

Usuario	Contraseña
root	maggie2.

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:

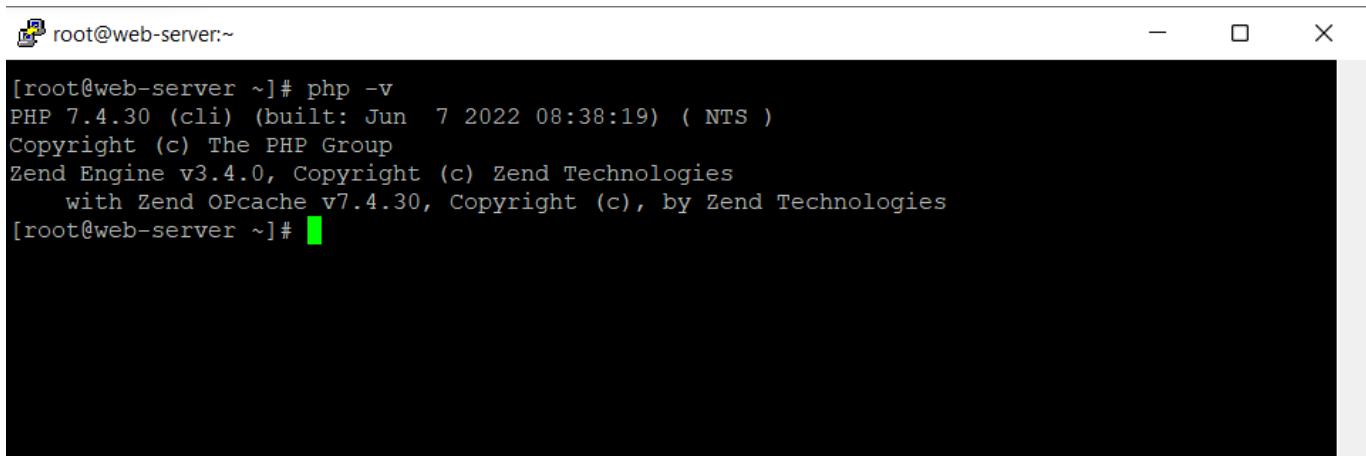
```
# yum install yum-utils
```

1. Habilite el repositorio remi-php74

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

1. Verifique la versión de PHP instalada:

```
# php -v
```



```
[root@web-server ~]# php -v
PHP 7.4.30 (cli) (built: Jun 7 2022 08:38:19) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
    with Zend OPcache v7.4.30, Copyright (c), by Zend Technologies
[root@web-server ~]#
```

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.quierograduar.me.com
```

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

```
sudo chown -R apache:apache /var/www/soporte.quierograduar.me.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.zip
```

```
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.quierograduar.me.com/osticket/upload/include/ost-sampleconfig.php  
/var/www/soporte.quierograduar.me.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.quierograduar.me.com  
sudo chmod -R 775 /var/www/soporte.quierograduar.me.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.quierograduar.me.com.conf
```

```
<VirtualHost *:80>  
    ServerName soporte.quierograduar.me.com  
    ServerAlias www.soporte.quierograduar.me.com  
  
    DirectoryIndex index.php index.html  
    DocumentRoot /var/www/soporte.quierograduar.me.com/osticket/upload  
  
    ErrorLog /var/log/httpd/soporte.quierograduar.me.com-error.log  
    CustomLog /var/log/httpd/soporte.quierograduar.me.com-access.log common  
  
    <Directory /var/www/soporte.quierograduar.me.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.quierograduar.me.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:

The screenshot shows the osTicket Installer setup page. At the top, it says "Thank You for Choosing osTicket!" and "Installing osTicket v1.15.1". It includes links for "Installation Guide", "Get Professional Help", and "Contact Us". A sidebar on the right titled "Need Help?" offers professional installation services and access to the development team. The main content area lists "Prerequisites" (PHP 7.2+, MySQLi extension) and "Recommended" extensions (Gdlib, PHP IMAP, PHP XML, PHP XML-DOM, PHP JSON, Mbstring, Phar, Intl, APCu). The background features a decorative header with silhouettes of people.

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

Error installing osTicket. Correct any errors below and try again.

System Settings

The URL of your helpdesk, its name, and the default system email address

Helpdesk URL:

<http://soporte.quierograduarne.com/>

Helpdesk Name:

Quiero Graduarne Support

Default Email:

yerlin.ledezma@ucr.ac.cr

Primary Language:

English (United States)

Admin User

Your primary administrator account - you can add more users later.

First Name:

Hellen

Last Name:

Fernandez

Email Address:

hellenfdz12@gmail.com

Conflicts with system email above

Username:

hellenfdz12

Password:

Retype Password:

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

Database Settings

Database connection information

MySQL Table Prefix:

MySQL Hostname:

MySQL Database:

MySQL Username:

MySQL Password:

Install Now

Si la configuración fue exitosa se mostrará la siguiente pantalla:

The screenshot shows the 'osTicket Installer' interface after a successful installation. The main content area displays the following information:

- Congratulations!**: Your osTicket installation has been completed successfully.
- Config file permission:** Instructions to change permissions of `ost-config.php` to remove write access.
- What's Next?** section:
 - Post-Install Setup:** You can now log in to [Admin Panel](#) with the username and password you created during the install process.
 - Commercial Support Available:** Don't let technical problems impact your osTicket implementation. Get guidance and hands-on expertise to address unique challenges and make sure your osTicket runs smoothly, efficiently, and securely. [Learn More!](#)
- Useful Links:**
 - Your osTicket URL: <http://soporte.quierograduarne.com/>
 - Your Staff Control Panel: <http://soporte.quierograduarne.com/scp>
 - osTicket Forums: <https://forum.osticket.com/>
 - osTicket Documentation: <https://docs.osticket.com/>

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.quierograduarne.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
```

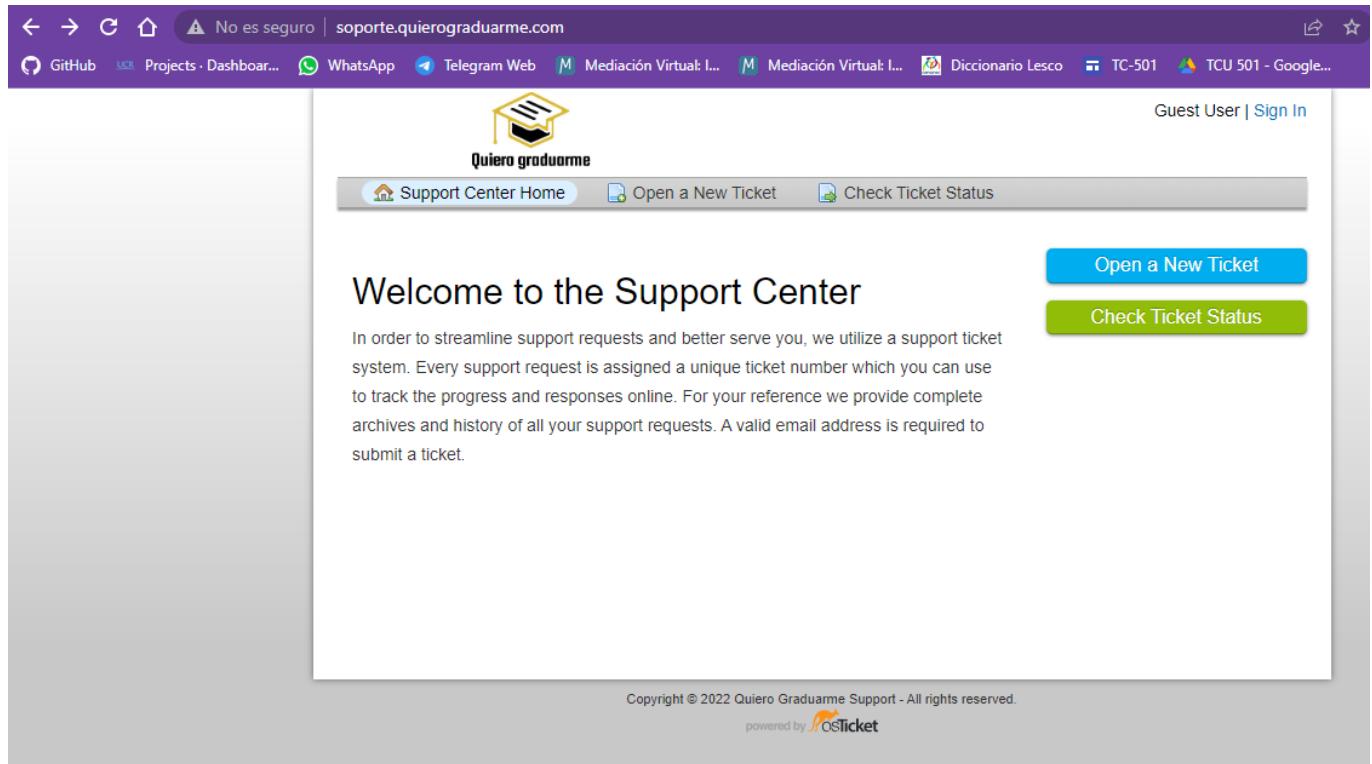
5. Construir los plugins

```
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.quierograduar.me.com/osTicket-plugins/auth-ldap.phar  
/var/www/soporte.quierograduar.me.com/osticket/upload/include/plugins/auth-ldap.pha  
r
```

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



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

No es seguro | soporte.quierograduarne.com/login.php

GitHub Projects · Dashboard WhatsApp Telegram Web Mediación Virtual I... Mediación Virtual I... Diccionario Lesco TC-501 TCU 501 - Google...

Quiero graduarme

Guest User | Sign In

Support Center Home Open a New Ticket Check Ticket Status

Sign in to Quiero Graduarne Support

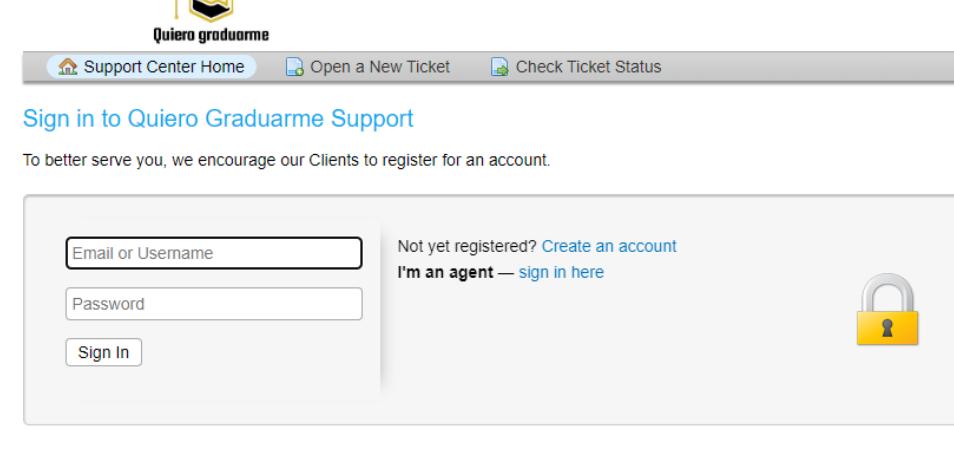
To better serve you, we encourage our Clients to register for an account.

Email or Username
Password
Sign In

Not yet registered? [Create an account](#)
I'm an agent — [sign in here](#)

If this is your first time contacting us or you've lost the ticket number, please [open a new ticket](#)

Copyright © 2022 Quiero Graduarne Support - All rights reserved.
powered by 



9. Para registrarse se usan las credenciales de administrador:

Usuario: hellenfdz12

Contraseña: maggielu2.

No es seguro | soporte.quierograduarne.com/scp/login.php

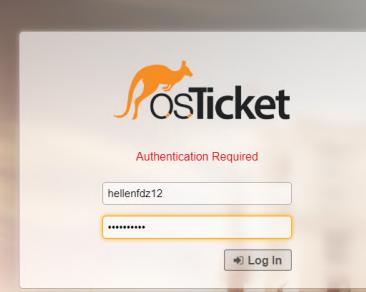
Mi unidad - Google... YouTube Mediación Virtual I... GitLab UCR Iconos vectoriales g... VCL : Virtual Comp... APA GENERATOR WhatsApp Personas en CompT... Otros marcadores

OSTicket

Authentication Required

hellenfdz12
.....
Log In

Copyright © Quiero Graduarne Support



10. Acceder a Agent Panel

The screenshot shows the OSTicket system logs. At the top, there is a yellow warning message: "Please take a minute to delete setup directory (./setup/) for security reasons." Below this is the OSTicket logo and the navigation menu: Dashboard, Settings, Manage, Emails, Agents. Under Manage, the "System Logs" tab is selected. A search bar allows filtering by date ("Between:"), file ("Log Level:" set to All), and a "Go!" button. The main area is titled "System Logs" and displays a table of log entries. The first entry is: "osTicket installed!" (Log Type: Debug, Log Date: Friday, July 15, 2022 at 11:47 PM, IP Address: 172.17.0.18). Below the table are buttons for "Delete Selected Entries" and "Select: All None Toggle". The footer of the page includes the copyright notice "Copyright © 2006-2022 Quiero Graduarne Support All Rights Reserved."

11. Instalar el plugin

The screenshot shows the OSTicket Manage Plugins page. At the top, there is a yellow warning message: "Please take a minute to delete setup directory (./setup/) for security reasons." Below this is the OSTicket logo and the navigation menu: Dashboard, Settings, Manage, Emails, Agents. Under Manage, the "Plugins" tab is selected. A green success message box says "Successfully installed a plugin". Below it, the heading "Currently Installed Plugins" is followed by a table. The table has columns: Plugin Name, Version, Status, and Date Installed. There is one entry: "LDAP Authentication and Lookup" (Version: 0.6.2, Status: Disabled, Date Installed: 7/19/22 11:33 PM). Below the table are buttons for "Add New Plugin" and "More". The footer of the page includes the copyright notice "Copyright © 2006-2022 Quiero Graduarne Support All Rights Reserved."

12. Habilitar el plugin

A No es seguro | sопorte.quierograduarne.com/scp/plugins.php

ts · Dashboard... WhatsApp Telegram Web M Mediación Virtual I... M Mediación Virtual I... Diccionario Lesco TC-501 TCU 501 - Google... » | Otra

OSTicket

Welcome, Hellen. | Agent Panel | Profile | Log Out

Manage

Dashboard Settings Manage Emails Agents

Help Topics Filters SLA Schedules API Pages Forms Lists Plugins

Currently Installed Plugins

Plugin Name	Version	Status	Date Installed
LDAP Authentication and Lookup	0.6.2	Disabled	7/19/22

Select: All None Toggle Page: [1]

Add New Plugin More ▾

- Enable
- Disable
- Delete

Copyright © 2006-2022 Quiero Graduarne Support All Rights Reserved.

A No es seguro | sопorte.quierograduarne.com/scp/plugins.php

ts · Dashboard... WhatsApp Telegram Web M Mediación Virtual I... M Mediación Virtual I... Diccionario Lesco TC-501 TCU 501 - Google... » | Otra

OSTicket

Welcome, Hellen. | Agent Panel | Profile | Log Out

Manage

Dashboard Settings Manage Emails Agents

Help Topics Filters SLA Schedules API Pages Forms Lists Plugins

Currently Installed Plugins

Plugin Name	Version	Status	Date Installed
LDAP Authentication and Lookup	0.6.2	Enabled	7/19/22 11:33 PM

Select: All None Toggle Page: [1]

Add New Plugin More ▾

Copyright © 2006-2022 Quiero Graduarne Support All Rights Reserved.

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: quierograduarne.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=quierograduarne,dc=ya
Password: maggielu2.
Search Base: dc=quierograduarne,dc=ya
```

A No es seguro | soporte.quierograduarne.com/scp/plugins.php?id=1

Projects · Dashboard... WhatsApp Telegram Web M Mediación Virtual I... M Mediación Virtual I... Diccionario Lesco TC-501 TCU 501 - Google...

Please take a minute to delete **setup** directory (**./setup/**) for security reasons.

OSTicket

Welcome, Hellen. | Agent Panel | Profile | Log Out

Dashboard Settings **Manage** Emails Agents

Help Topics Filters SLA Schedules API Pages Forms Lists Plugins

Manage Plugin — LDAP Authentication and Lookup

Configuration

Microsoft® Active Directory

This section should be all that is required for Active Directory domains

Default Domain:

Default domain used in authentication and searches

DNS Servers:

(optional) DNS servers to query about AD servers. Useful if the AD server is not on the same network as this web server or does not have its DNS configured to point to the AD servers

Generic configuration for LDAP

Not necessary if Active Directory is configured above

LDAP servers:

Use "server" or "server:port". Place one server entry per line

C Home A No es seguro | soporte.quierograduarne.com/scp/plugins.php?id=1

Projects · Dashboard... WhatsApp Telegram Web M Mediación Virtual I... M Mediación Virtual I... Diccionario Lesco TC-501 TCU 501 - Google...

Use TLS: Use TLS to communicate with the LDAP server

Connection Information

Useful only for information lookups. Not necessary for authentication. NOTE that this data is not necessary if your server allows anonymous searches

Search User:

Bind DN (distinguished name) to bind to the LDAP server as in order to perform searches

Password:

Search Base:

Used when searching for users

LDAP Schema:

Authentication Modes

Authentication modes for clients and staff members can be enabled independently

Staff Authentication: Enable authentication of staff members

Client Authentication: Enable authentication of clients

Copyright © 2006-2022 Quiero Graduarne Support All Rights Reserved.

Si la configuración fue exitosa verá el siguiente mensaje:

No es seguro | soporte.quierograduarne.com/scp/plugins.php?id=1

Projects - Dashboard... WhatsApp Telegram Web Mediación Virtual: I... Mediación Virtual: I... Diccionario Lesco TC-501 TCU 501 - Google... » Otros marcadores

Please take a minute to delete setup directory (./setup/) for security reasons.



Welcome, Hellen. | Agent Panel | Profile | Log Out

Dashboard Settings **Manage** Emails Agents

Help Topics Filters SLA Schedules API Pages Forms Lists Plugins

LDAP configuration updated successfully

Manage Plugin — LDAP Authentication and Lookup

Configuration

Microsoft® Active Directory
This section should be all that is required for Active Directory domains

Default Domain: Default domain used in authentication and searches

DNS Servers: (optional) DNS servers to query about AD servers. Useful if the AD server is not on the same network as this web server or does not have its DNS configured to point to the AD servers

Generic configuration for LDAP
Not necessary if Active Directory is configured above

No es seguro | soporte.quierograduarne.com/scp/users.php

Projects - Dashboard... WhatsApp Telegram Web Mediación Virtual: I... Mediación Virtual: I... Diccionario Lesco TC-501 TCU 501 - Google... »



Welcome, Hellen. | Admin Panel | Profile | Log Out

Dashboard **Users** Tasks Tickets Knowledgebase

User Directory Organizations

Add User Import More

	Name	Status	Created	Updated
<input type="checkbox"/>	Irvin Chavarria	Active (Registered)	7/20/22	7/20/22 9:50 AM
<input type="checkbox"/>	osTicket Support	Guest	7/15/22	7/15/22 11:47 PM
<input type="checkbox"/>	Yerlin Ledezma	Active (Registered)	7/20/22	7/20/22 9:53 AM

Select: All None Toggle
Page: [1] Export

Copyright © 2006-2022 Quiero Graduarne Support All Rights Reserved.

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

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

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

3. Crear el archivo de virtual hosts con la configuración

```
sudo nano /etc/httpd/conf.d/aula.quierograduar.me.com.conf
```

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

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

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

    <Directory /var/www/aula.quierograduar.me.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.quierograduar.me.com, en la primera pantalla le van a solicitar seleccionar el idioma

Language

Please choose a language for the installation. This language will also be used as the default language for the site, though it may be changed later.

Language English (en)

Next >

moodle

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

Web address: <http://aula.quierograduarne.com>

Moodle directory: /var/www/aula.quierograduarne.com/moodle

Data directory: /var/www/aula.quierograduarne.com/moodledata

redirect for each of the other addresses.

If your site is accessible both from the Internet, and from an internal network (sometimes called an Intranet), then use the public address here.

If the current address is not correct, please change the URL in your browser's address bar and restart the installation.

Moodle directory
The full path to the directory containing the Moodle code.

Data directory
A directory where Moodle will store all file content uploaded by users.

This directory should be both readable and writeable by the web server user (usually 'www-data', 'nobody', or 'apache').

It must not be directly accessible over the web.

If the directory does not currently exist, the installation process will attempt to create it.

Web address

Moodle directory

Data directory

« Previous Next >

3. Especificar el driver de la base de datos

Installation

Database

Choose database driver

Moodle supports several types of database servers. Please contact server administrator if you do not know which type to use.

Type

« Previous

Next »



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

Database settings

MariaDB (native/mariadb)

The database is where most of the Moodle settings and data are stored and must be configured here.

The database name, username, and password are required fields; table prefix is optional.

The database name may contain only alphanumeric characters, dollar (\$) and underscore (_).

If the database currently does not exist, and the user you specify has permission, Moodle will attempt to create a new database with the correct permissions and settings.

This driver is not compatible with legacy MyISAM engine.

Database host

Database name

Database user

Database password

Tables prefix

Database port

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    = 'mysqli';
$CFG->dblibrary = 'native';
$CFG->dbhost   = '192.168.164.5';
$CFG->dbname   = 'moodle';
$CFG->dbuser   = 'moodleuser';
$CFG->dbpass   = 'maggie1u2.';
$CFG->prefix   = 'mdl_';
$CFG->dboptions = array (
    'dbpersist' => 0,
    'dbport' => 3306,
    'dbsocket' => '',
    'dbcollation' => 'utf8mb4_general_ci',
);

$CFG->wwwroot   = 'http://aula.quierograduarne.com';
$CFG->dataroot  = '/var/www/aula.quierograduarne.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?



Installation

System

Success

antivirus_clamav

Success

availability_completion

Success

availability_date

Success

availability_grade

tinymce_spellchecker

Success

tinymce_wrap

Success

logstore_database

Success

logstore_legacy

Success

logstore_standard

Success

Continue



6. Realizar la configuración general

Username: admin

New password: maggieLu2.

First name: admin

Surname: User

Email address: hellenfdz12@gmail.com

No es seguro | aula.quierograduar.me.com/user/editadvanced.php?id=2

Mi unidad - Google... YouTube Mediación Virtual: I... GitLab UCR Iconos vectoriales g... VCL :: Virtual Comp... APA GENERATOR WhatsApp Personas en CompT... » Otros marcadores

General

Username	<input type="text" value="admin"/>
Choose an authentication method	<input checked="" type="radio"/> Manual accounts
The password must have at least 8 characters, at least 1 digit(s), at least 1 lower case letter(s), at least 1 upper case letter(s), at least 1 special character(s) such as *, -, or #	
New password	<input type="password" value="maggieLu2."/> <input type="checkbox"/> Force password change
First name	<input type="text" value="Admin"/>
Surname	<input type="text" value="User"/>
Email address	<input type="text" value="hellenfdz12@gmail.com"/>
Email display	<input type="text" value="Allow everyone to see my email address"/>
City/town	<input type="text" value="Montes de Oca"/>
Select a country	<input type="text" value="Costa Rica"/>
Timezone	<input type="text" value="America/Costa_Rica"/>

7. Agregar la información del sitio

No es seguro | aula.quierograduar.me.com/admin/upgradesettings.php?return=site

Mi unidad - Google... YouTube Mediación Virtual: I... GitLab UCR Iconos vectoriales g... VCL :: Virtual Comp... APA GENERATOR WhatsApp Personas en CompT... » Otros marcadores

Installation

New settings - Site home settings

Full site name fullname	<input type="text" value="Quiero graduarme"/>
Short name for site (eg single word) shortname	<input type="text"/>
Site home summary summary	<input type="text" value=""/>

Instalación LDAP

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

The screenshot shows a browser window with the URL aula.quierograduar.me.com/admin/search.php#linkmodules. The address bar has a warning icon indicating it's not secure. The page title is "Quiero graduarme". The top navigation bar includes links for GitHub, Projects, WhatsApp, Telegram Web, Mediación Virtual I..., Mediación Virtual II..., Diccionario Lesco, TC-501, and TCU 501 - Google... A "Site administration" link is also present. Below the navigation, there are links for "Accessibility toolkit settings", "Reports", and "Recycle bin".

Quiero graduarme Home Dashboard My courses Site administration

[Accessibility toolkit settings](#)

[Reports](#)

[Recycle bin](#)

Antivirus plugins

Manage antivirus plugins

Authentication

Manage authentication

Email-based self-registration

Manual accounts

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

The screenshot shows the Moodle admin settings page for managing authentication methods. The URL is aula.quierograduar.me.com/admin/settings.php?section=manageauths. The page lists four authentication methods: "Manual accounts" (2 users), "No login" (0 users), "Email-based self-registration" (0 users), and "LDAP server" (0 users). Each method has a "Settings" button. The "LDAP server" row also has "Test settings" and "Uninstall" buttons.

Quiero graduarme Home Dashboard My courses Site administration

Edit mode

Manual accounts

2

[Settings](#)

No login

0

Email-based self-registration

0



[Settings](#)

[Uninstall](#)

LDAP server

0



[Settings](#)

[Test settings](#)

3. Agregar la siguiente configuración:

LDAP server settings

Host URL: 192.168.196.4; 192.168.164.4

Lo demás se mantuvo por defecto

The screenshot shows the Moodle admin settings page for LDAP server configuration. The URL is aula.quierograduar.me.com/admin/settings.php?section=authsettingldap. The page has a header with "Edit mode" and other navigation links. The main section is titled "LDAP server settings". It contains several configuration fields: "Host URL" (value: 192.168.196.4; 192.168.164.4, default: Empty), "Version" (value: 3, default: 3), "Use TLS" (value: No, default: No), "LDAP encoding" (value: utf-8, default: utf-8), and "Page size" (value: 250, default: 250).

Quiero graduarme Home Dashboard My courses Site administration

Edit mode

LDAP server settings

Host URL
auth_ldap | host_url

192.168.196.4; 192.168.164.4

Default: Empty

Specify LDAP host in URL-form like 'ldap://ldap.myorg.com/' or 'ldaps://ldap.myorg.com/'. Separate multiple servers with ';' to get failover support.

Version
auth_ldap | ldap_version

3

Default: 3

The version of the LDAP protocol your server is using.

Use TLS
auth_ldap | start_tls

No

Default: No

Use regular LDAP service (port 389) with TLS encryption

LDAP encoding
auth_ldap | idapencoding

utf-8

Default: utf-8

Encoding used by the LDAP server, most likely utf-8. If LDAP v2 is selected, Active Directory uses its configured encoding, such as cp1252 or cp1250.

Page size
auth_ldap | pagesize

250

Default: 250

Bind settings

Prevent password caching: yes

Distinguished name: uid=admin,cn=user,cn=accounts,dc=quierograduararme,dc=ya

Password: maggielu2.

User lookup settings

Contexts: cn=user,cn=accounts,dc=quierograduararme,dc=ya

User attribute: uid

Los otros campos se quedaron con la configuración por defecto

The screenshot shows the 'Bind settings' section of the Moodle admin settings. It includes fields for 'Prevent password caching' (set to 'Yes'), 'Distinguished name' (set to 'uid=admin,cn=users,cn=accounts,dc=quierogra'), and 'Password' (a masked input). Below these are 'User lookup settings' with 'User type' set to 'Default' and 'Contexts' set to 'cn=users,cn=accounts,dc=quierogra'.

Bind settings

Prevent password caching
auth_ldap | preventpasswords

Yes Default: No

Select yes to prevent passwords from being stored in Moodle's DB.

Distinguished name
auth_ldap | bind_dn

uid=admin,cn=users,cn=accounts,dc Default: Empty

If you want to use bind-user to search users, specify it here. Something like 'cn=ldapuser,ou=public,o=org'

Password
auth_ldap | bind_pw

..... Default: Empty

Password for bind-user.

User lookup settings

User type
auth_ldap | user_type

Default Default: Default

Select how users are stored in LDAP. This setting also specifies how login expiry, grace logins and user creation will work.

Contexts
auth_ldap | contexts

cn=users,cn=accounts,dc=quierogra Default: Empty

List of contexts where users are located. Separate different contexts with ','. For example: 'ou=users,o=org; ou=others,o=org'

The screenshot shows the 'User lookup settings' section of the Moodle admin settings. It includes fields for 'User attribute' (set to 'uid'), 'Suspended attribute' (empty), 'Member attribute' (empty), 'Member attribute uses dn' (set to 'No'), and 'Object class' (empty). Below these are sections for 'Force change password' and 'Advanced settings'.

Determines how aliases are handled during search. Select one of the following values: "No" (LDAP_DEREF_NEVER) or "Yes" (LDAP_DEREF_ALWAYS)

User attribute
auth_ldap | user_attribute

uid Default: Empty

Optional: Overrides the attribute used to name/search users. Usually 'cn'.

Suspended attribute
auth_ldap | suspended_attribute

Default: Empty

Optional: When provided this attribute will be used to enable/suspend the locally created user account.

Member attribute
auth_ldap | memberattribute

Default: Empty

Optional: Overrides user member attribute, when users belongs to a group. Usually 'member'

Member attribute uses dn
auth_ldap | memberattribute_dn

No Default: No

Overrides handling of member attribute values

Object class
auth_ldap | objectclass

Default: Empty

Optional: Overrides objectClass used to name/search users on ldap_user_type. Usually you don't need to change this.

Force change password

No es seguro | aula.quierograduar.me.com/admin/settings.php?section=authsettingldap

GitHub Projects · Dashboard WhatsApp Telegram Web Mediación Virtual I... Mediación Virtual II... Diccionario Lesco TC-501 TCU 501 - Google... Otros marcadores

Quiero graduarme Home Dashboard My courses Site administration

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.quierograduar.me.com/admin/settings.php?section=authsettingldap

GitHub Projects · Dashboard WhatsApp Telegram Web Mediación Virtual I... Mediación Virtual II... Diccionario Lesco TC-501 TCU 501 - Google... Otros marcadores

Quiero graduarme Home Dashboard My courses Site administration

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

No es seguro | aula.quierograduar.me.com/admin/settings.php?section=authsettingldap

GitHub Projects - Dashboard WhatsApp Telegram Web Mediación Virtual I... Mediación Virtual I... Diccionario Lesco TC-501 TCU 501 - Google... Otros

Quiero graduarme Home Dashboard My courses Site administration AU Edit mode

Optional: Overrides grace login attribute

Enable user creation

Create users externally auth_ldap | auth_user_create

No Default: No

New (anonymous) users can create user accounts on the external authentication source and confirmed via email. If you enable this, remember to also configure module-specific options for user creation.

Context for new users auth_ldap | create_context

[] Default: Empty

If you enable user creation with email confirmation, specify the context where users are created. This context should be different from other users to prevent security issues. You don't need to add this context to ldap_context-variable. Moodle will search for users from this context automatically.
Note! You have to modify the method user_create() in file auth/ldap/auth.php to make user creation work

System role mapping

Manager context auth_ldap | managercontext

[] Default: Empty

LDAP context used to select for *Manager* mapping. Separate multiple groups with ':'. Usually something like "cn=manager,ou=first-ou-with-role-groups,o=myorg; cn=manager,ou=second-ou-with-role-groups,o=myorg".

Course creator context auth_ldap | coursecreatorcontext

[] Default: Empty

LDAP context used to select for *Course creator* mapping. Separate multiple groups with ':'. Usually something like "cn=coursecreator,ou=first-ou-with-role-groups,o=myorg; cn=cc" Herramienta Recortes Id-ou-with-role-groups,o=myorg".

User account synchronisation

Removed ext user: Full delete internal

No es seguro | aula.quierograduar.me.com/admin/settings.php?section=authsettingldap

GitHub Projects - Dashboard WhatsApp Telegram Web Mediación Virtual I... Mediación Virtual I... Diccionario Lesco TC-501 TCU 501 - Google... Otros

Quiero graduarme Home Dashboard My courses Site administration AU Edit mode

auth_ldap | coursecreatorcontext

LDAP context used to select for *Course creator* mapping. Separate multiple groups with ':'. Usually something like "cn=coursecreator,ou=first-ou-with-role-groups,o=myorg; cn=coursecreator,ou=second-ou-with-role-groups,o=myorg".

User account synchronisation

Removed ext user auth_ldap | removeuser

Full delete internal Default: Keep internal

Specify what to do with internal user account during mass synchronisation when user was removed from external source. Only suspended users are automatically restored if they reappear in the external source.

Synchronise local user suspension status auth_ldap | sync_suspended

No Default: No

If enabled, the suspended attribute will be used to update the local user account's suspension status.

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*

Name	Component	Edit	Logs	Last run	Next run	Minute	Hour	Day	Day of week	Month	Fail delay	Default
Prepare submissions for annotation \assignfeedback_editpdf\task\convert_submissions	Annotate PDF assignfeedback_editpdf			Never	ASAP	*/15	*	*	*	*	0	Yes
CAS users sync job \auth_cas\task\sync_task	CAS server (SSO) auth_cas			Never	Plugin disabled	0	0	*	*	*	0	Yes
Synchronise users task \auth_db\task\sync_users	External database auth_db			Never	Plugin disabled	53	16	*	*	*	0	Yes
Synchronise system roles from LDAP \auth_ldap\task\sync_roles	LDAP server auth_ldap			Never	Task disabled	0	0	*	*	*	0	Yes
LDAP users sync job \auth_ldap\task\sync_task	LDAP server auth_ldap			Never	Task disabled	0	0	*	*	*	0	Yes

5. Agregar cada cuánto se quieren hacer la sincronización y guardar los cambios Se va a realizar cada 5 minutos

Quiero graduarme: Administratio X +

No es seguro | aula.quierograduar.me.com/admin/t... 🔍 ↗ ⭐

GitHub Projects · Dashboard WhatsApp Telegram Web Mediación Virtual: I...

Quiero graduarme Home Dashboard My courses Site administration AU

General Users Courses Grades Plugins Appearance Server Reports Development

Edit task schedule: LDAP users sync job

\auth_ldap\task\sync_task
From component: LDAP server auth_ldap

Last run	Never
Next run	Task disabled
Minute	<input type="text" value="*/5"/> Default: 0
Hour	<input type="text" value="*"/> Default: 0
Day	<input type="text" value="*"/> Default: *
Month	<input type="text" value="*"/> Default: *
Day of week	<input type="text" value="*"/> Default: *
<input type="checkbox"/> Disabled ?	
<input type="checkbox"/> Reset task schedule to defaults ?	

Save changes Cancel

Quiero graduarme: Administración											
Quiero graduarme: Administración											
Quiero graduarme: Administración											
Quiero graduarme	Home	Dashboard	My courses	Site administration						AU	Edit mode
Prepare submissions for annotation \auth:feedback:editpdf:task:convert_submissions	Annotate PDF assignfeedback_editpdf			Never	ASAP		*/15	*	*	*	0 Yes
CAS users sync job \auth:cas:task:sync_task	CAS server (SSO) auth_cas			Never	Plugin disabled		0	0	*	*	0 Yes
Synchronise users task \auth:db:task:sync_users	External database auth_db			Never	Plugin disabled	53	16	*	*	*	0 Yes
Synchronise system roles from LDAP \auth:ldap:task:sync_roles	LDAP server auth_ldap			Never	Task disabled	0	0	*	*	*	0 Yes
LDAP users sync job \auth:ldap:task:sync_task	LDAP server auth_ldap			Never	Wednesday, 20 July 2022, 12:50 PM	*/5 Default: 0	*	*	*	*	0 No

6. Entrar al servidor y ejecutar actualizar usuarios

```
sudo php
```

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

The screenshot shows a terminal window with the following output:

```
root@web-server:~ Execute scheduled task: LDAP users sync job (auth_ldap\task\sync_task) Connecting to LDAP server... Creating temporary table tmp_extuser .....Got 14 records from LDAP No user entries to be removed User entries to be added: 13 Inserted user aurelio id 3 Inserted user diego id 4 Inserted user hellen id 5 Inserted user irvin id 6 Inserted user johel id 7 Inserted user jose id 8 Inserted user jostyn id 9 Inserted user lfernandez id 10 Inserted user maria id 11 Inserted user mfernandez id 12 Inserted user reichel id 13 Inserted user yerlin id 14 Inserted user yledezma id 15 ... used 171 dbqueries ... used 0.85353088378906 seconds Scheduled task complete: LDAP users sync job (auth_ldap\task\sync_task)
```

[root@web-server ~]# sudo php /var/www//aula.quierograduar.me.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.quierograduar.me.com/moodle/admin/tool/task/cli/cron_auth_ldap.sh
#!/bin/sh
sudo php /var/www/aula.quierograduar.me.com/moodle/admin/tool/task/cli/schedule_task.php
--execute="\auth_ldap\task\sync_task"
```

The screenshot shows a terminal window with the following output:

```
root@web-server:~ GNU nano 2.3.1 File: ...oodle/admin/tool/task/cli/cron_auth_ldap.sh Modified
#!/bin/sh
sudo php /var/www/aula.quierograduar.me.com/moodle/admin/tool/task/cli/schedule_
```

8. Dar permisos de ejecución

```
sudo chmod +x /var/www//aula.quierograduar.me.com/moodle/admin/tool/task/cli/cron_auth_ldap.sh
```

```
[root@web-server ~]# sudo nano /var/www/aula.quierograduar.me.com/moodle/admin/tool/task/cli/cron_auth_ldap.sh
[root@web-server ~]# sudo chmod +x /var/www//aula.quierograduar.me.com/moodle/admin/tool/task/cli/cron_auth_ldap.sh
[root@web-server ~]#
```

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.quierograduar.me.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.quierograduar.me.com
```

3. Acceder a la carpeta creada

```
sudo cd /var/www/nube.quierograduar.me.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.quierograduar.me.com
sudo chmod -R 775 /var/www/nube.quierograduar.me.com
```

7. Crear el archivo de configuración de nextcloud

```
sudo nano /etc/httpd/conf.d/nube.quierograduar.me.com.conf
```

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

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

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

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

    <Directory /var/www/nube.quierograduar.me.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

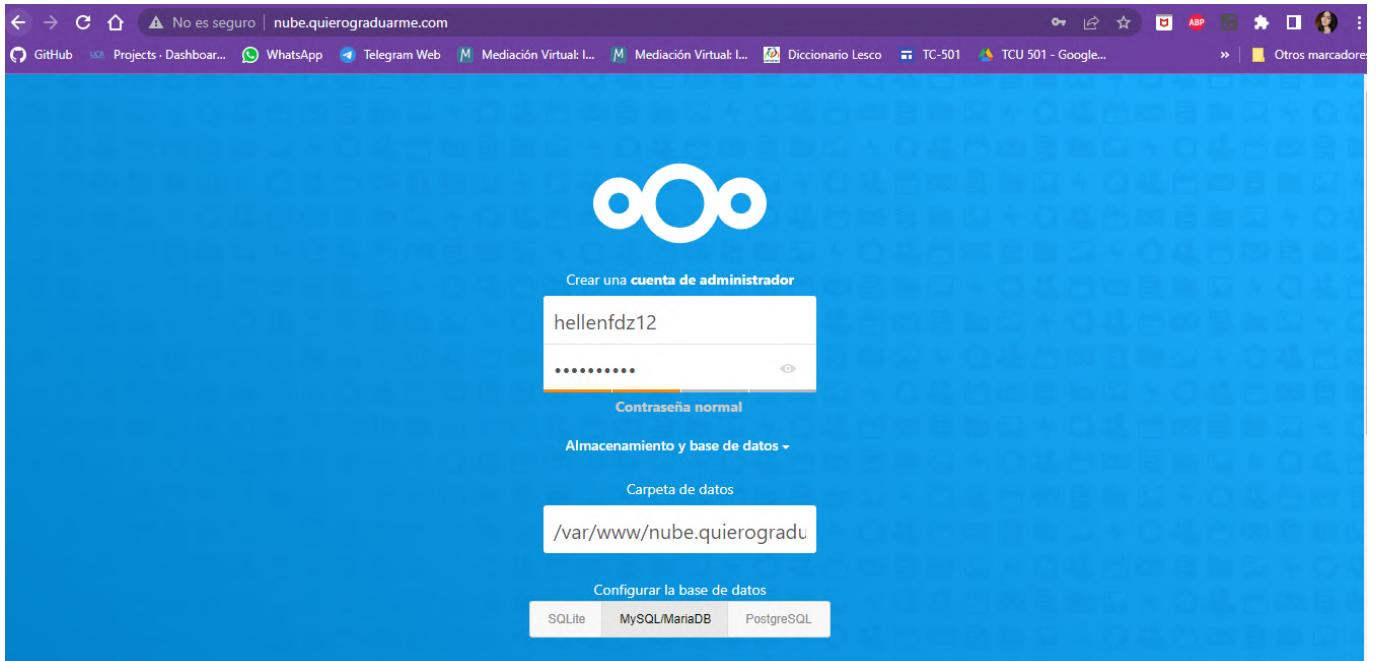
1. Ingrese a la página de nextcloud y configurelo de la siguiente manera:

cuenta de administrador:

hellenfzd12

Contraseña: maggielu2.

Carpeta de datos: /var/www/quierograduar.me.com/nextcloud/data



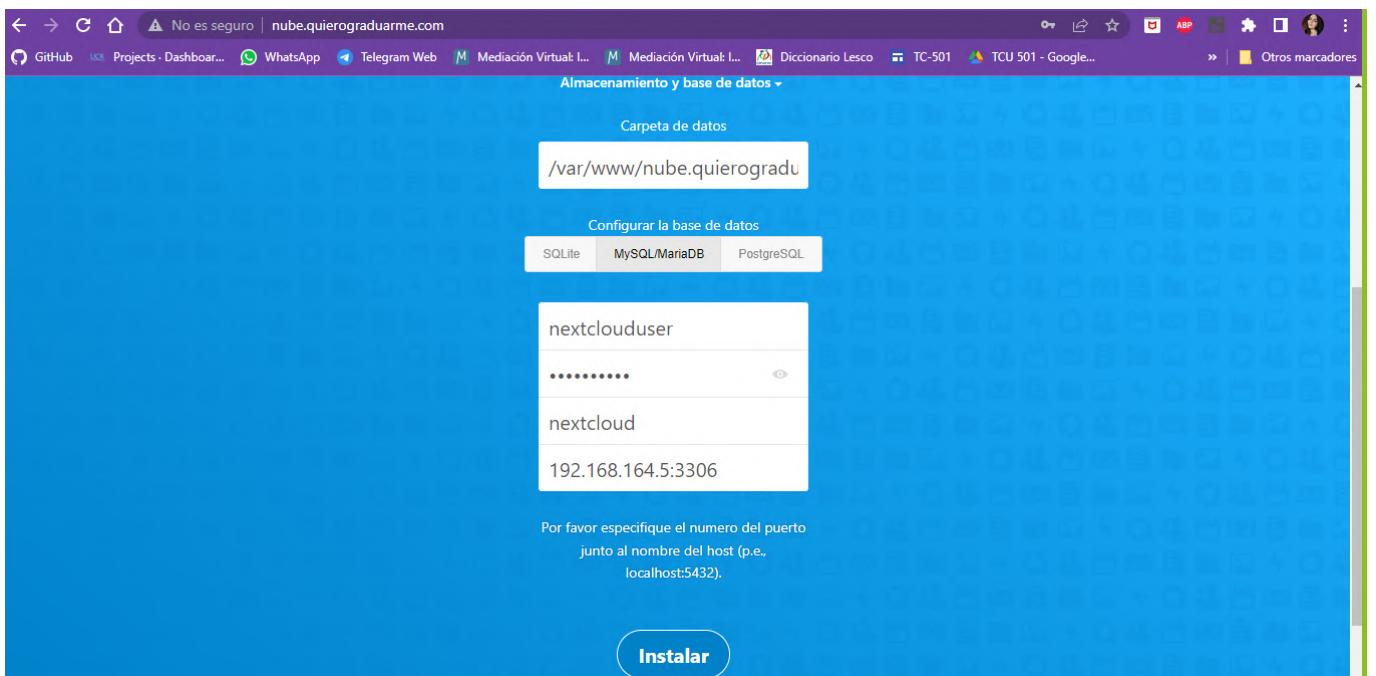
2. Seleccionar la base de datos MariaDB

User: nextclouduser

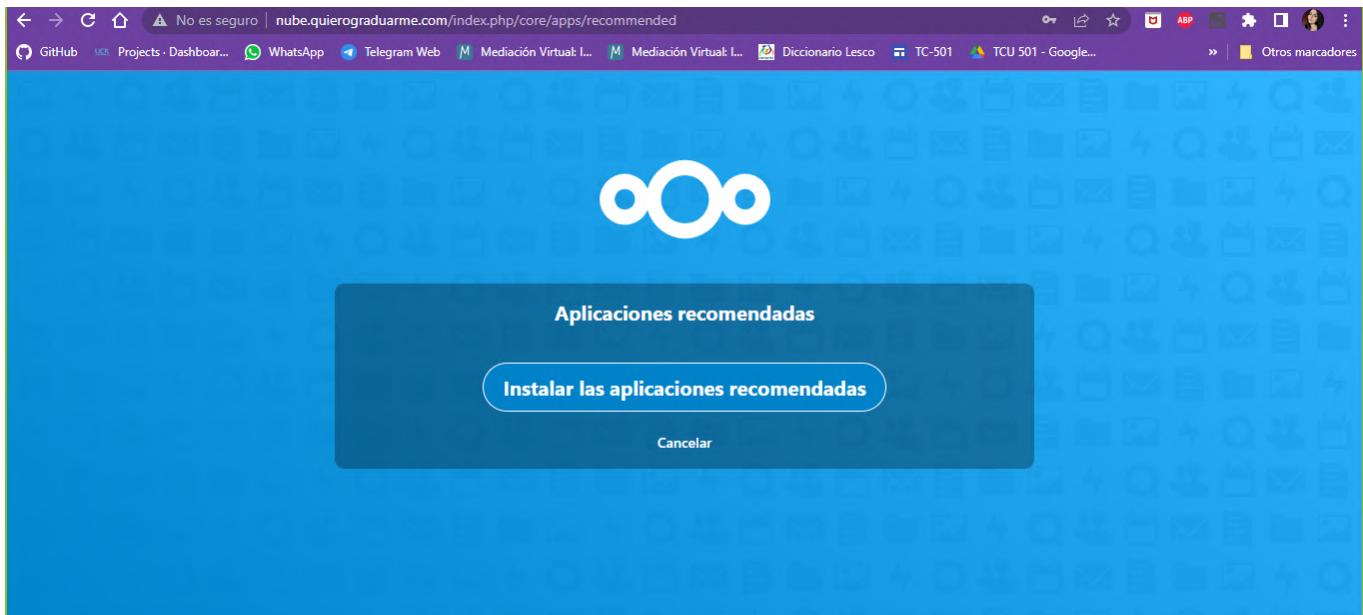
Password: maggielu2.

Database: nextcloud

Host: 192.168.164.5:3306

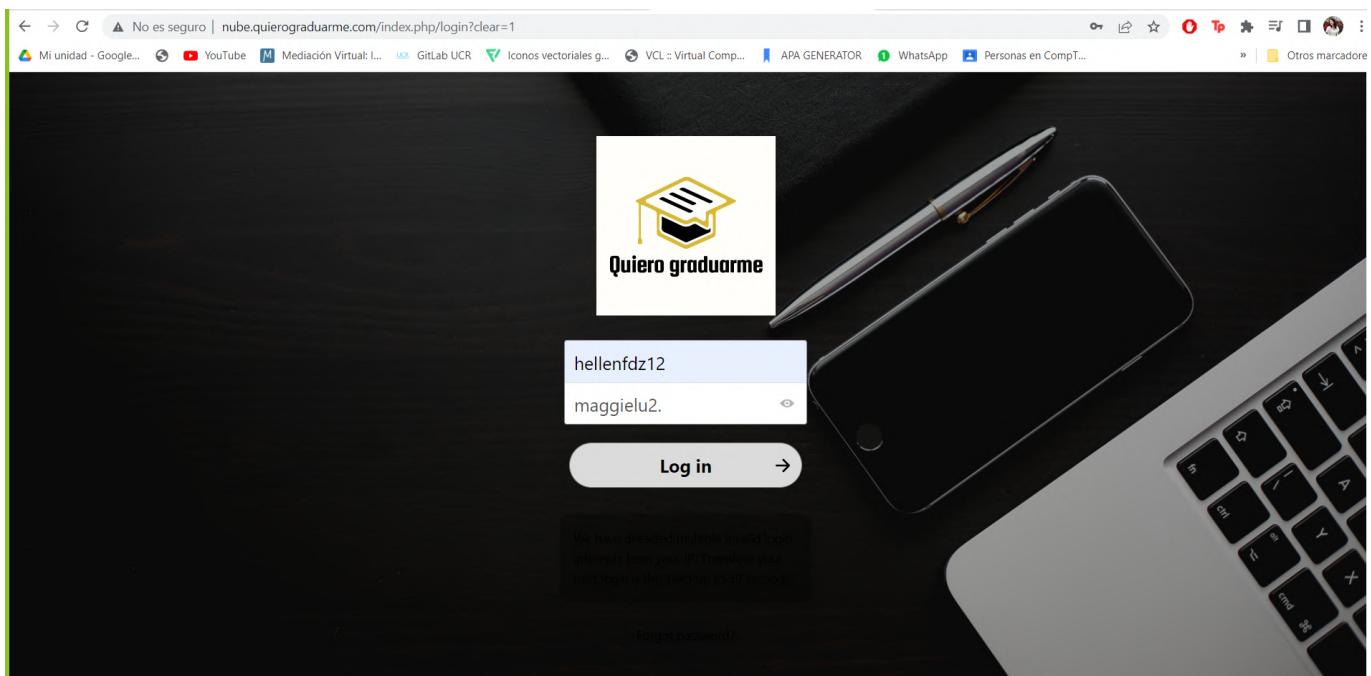


3. Darle click a Instalar las aplicaciones recomendadas.

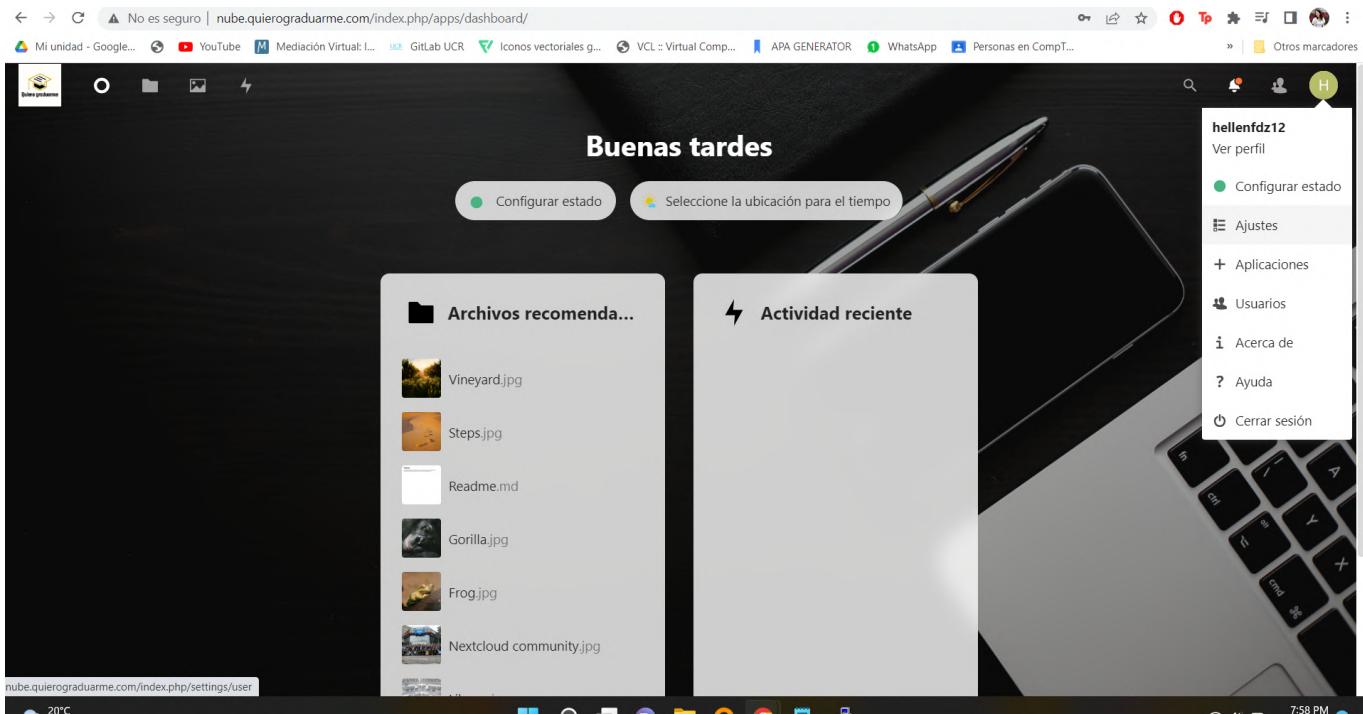


Configuración LDAP

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.quierograduarne.ya
basedn = dc=quierograduarne,dc=ya
realm = QUIEROGRADUARME.YA
domain = quierograduarne.ya
xmlrpc_uri = https://ipa1.quierograduarne.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:

The screenshot shows the 'Integración LDAP/AD' configuration interface. On the left, there's a sidebar with sections like Personal, Administración, and various system icons. The main area is titled 'Integración LDAP/AD' and has tabs for 'Servidor', 'Usuarios', 'Atributos de inicio de sesión', and 'Grupos'. The 'Servidor' tab is active, showing fields for '1. Servidor: ipa1.quierograduarne.ya' (with a dropdown menu), a password field containing '*****', and a base DN field with 'dc=quierograduarne,dc=ya'. Buttons for 'Detectar puerto', 'Guardar credenciales', 'Detectar Base DN', and 'Probar Base DN' are present. A checkbox for 'Introduzca manualmente los filtros LDAP (recomendado para directorios grandes)' is checked. At the bottom, a green status bar says 'Configuración correcta' and a 'Continuar' button is visible.

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

The screenshot shows the 'Integración LDAP/AD' configuration interface with the 'Usuarios' tab selected. The sidebar remains the same. The main area shows a note about filtering users by object classes and a dropdown for 'Sólo estas clases de objetos'. Below it, another dropdown for 'Sólo desde estos grupos' is shown with 'Seleccionar grupos'. A link '↓ Editar consulta LDAP' is present. In the bottom right, a text input field contains '(objectclass=*)'. At the bottom, a green status bar says 'Configuración correcta' and buttons for 'Atrás', 'Continuar', and 'Ayuda' are visible.

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.quierograduar.me/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...

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:

[↓ Editar consulta LDAP](#)

(&(objectclass="*)(!(cn=%uid)!(mailPrimaryAddress=%uid)(mail=%uid)))

Verificar configuración

Configuración correcta Atrás Continuar Ayuda

No es seguro | nube.quierograduar.me/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...

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:

[↓ Editar consulta LDAP](#)

(&(objectclass="*)(!(cn=%uid)!(mailPrimaryAddress=%uid)(mail=%uid)))

Verificar configuración

Configuración correcta Atrás Continuar Ayuda

No es seguro | nube.quierograduar.me/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

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=pausers))

Verifique los ajustes y cuente los grupos

Configuración correcta Atrás Ayuda

Personal

- Información personal
- Seguridad
- Notificaciones
- Móvil y escritorio
- Accesibilidad
- Compartir
- Groupware
- Flujo
- Privacidad

Administración

- Vista general
- Soporte
- Ajustes básicos

No es seguro | nube.quierograduar.me/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

Integración LDAP/AD

Servidor Usuarios Atributos de inicio de sesión Grupos Avanzado Experto

Configuración de conexión

Configuración activa

Servidor de copia de seguridad (Replica)

Puerto para copias de seguridad (Replica)

Deshabilitar servidor principal

Desactivar la validación por certificado SSL

Cache TTL 600

Configuración de directorio

Atributos especiales

Personal

- Información personal
- Seguridad
- Notificaciones
- Móvil y escritorio
- Accesibilidad
- Compartir
- Groupware
- Flujo
- Privacidad

Administración

- Vista general
- Soporte
- Ajustes básicos

No es seguro | nube.quierograduar.me/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

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=quierograduar.me,dc=ya

Atributos de la búsqueda de usuario: Opcional; un atributo por linea

Campo de nombre de grupo a mostrar: cn

Árbol base de grupo: cn=groups,cn=accounts,dc=quierograduar.me,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.quierograduar.me/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

Configuración de conexión

Configuración 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

The screenshot shows a web application for managing LDAP/AD integration. On the left, a sidebar lists various administrative categories like Personal, Administración, and Soporte. The main panel is titled 'Integración LDAP/AD' and contains three main sections: 'Configuración de conexión', 'Configuración de directorio', and 'Atributos especiales'. Under 'Atributos especiales', there are several input fields: 'Cuota' set to '35MB', 'Cuota por defecto', 'E-mail' set to 'mail', 'Regla para la carpeta Home de usuario' set to 'cn', and 'Campo reservado '\$home''. At the bottom of the panel, there are buttons for 'Configuración de prueba' and 'Ayuda'. A message box at the top right indicates that the configuration is valid and the connection is established.

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 'maggie1u2.';  
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
```

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Install" for "PHP Server Monitor". The page features a logo of a blue line graph. Below it, a message says: "Welcome to the installation of PHP Server Monitor. This page will guide you through the steps to install or upgrade your monitor." A note below states: "Before we start, we need to verify your system meets the requirements. If you see any errors in the list below, you may still continue, but PHP Server Monitor may not work correctly. It is recommended you fix any errors before continuing." Two green "success" status boxes are present: one for "PHP version: 7.2.34" and another for "PHP cURL module found". A large blue "Let's go" button is at the bottom.

13. Establecer un usuario con contraseña y un correo:

user:hellen

password: maggielu2.

email:hellenfdz12@gmail.com

The screenshot shows a continuation of the "Install" process for "PHP Server Monitor". The page displays a message: "Sweet, your database connection is up and running! Next, please set up a new account to access your monitor." Below this, there is a form for creating an administrator account. The "Username" field contains "hellen", the "Password" field contains "*****", and the "Password repeat" field also contains "*****". The "Email" field is filled with "hellenfdz12@gmail.com". A green "Install" button is at the bottom of the form.

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

SERVER MONITOR - Mozilla Firefox

File Edit View History Bookmarks Tools Help

SERVER MONITOR +

192.168.5.112/phpservermon/install.php?action=config

SERVER MONITOR

Please enter your database info:

Database host: localhost

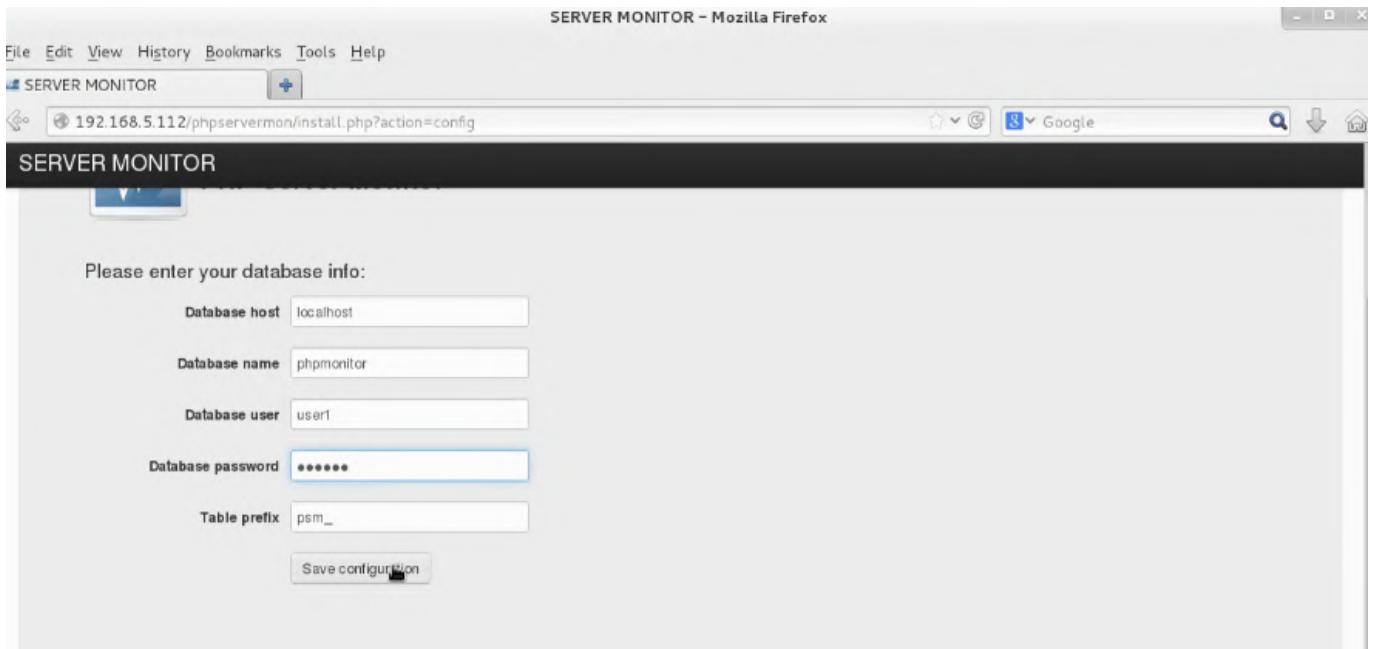
Database name: phpmonitor

Database user: user1

Database password: *****

Table prefix: psm_

Save configuration



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:

SERVER MONITOR

Install

PHP Server Monitor

installation process started.

success Table monitor_config added.

info Table monitor_users added.

info Table monitor_users_preferences added.

info Table monitor_users_servers added.

info Table monitor_log added.

info Table monitor_log_users added.

info Table monitor_servers added.

info Table monitor_servers_uptime added.

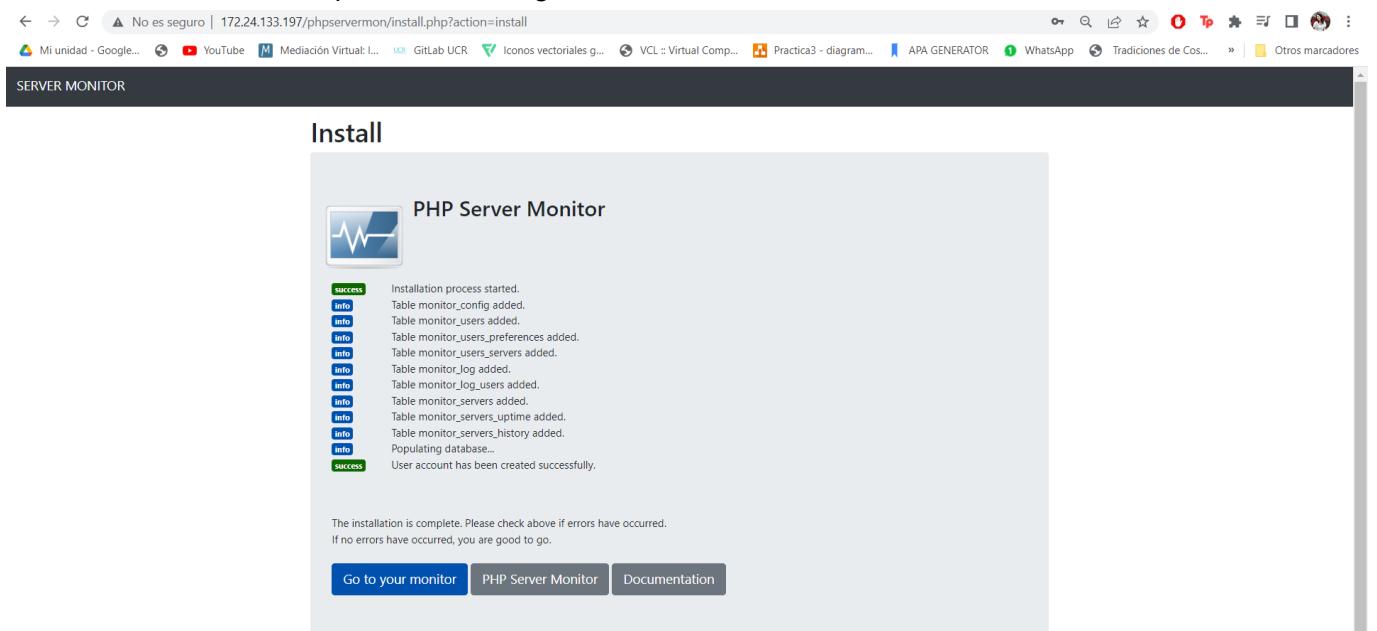
info Table monitor_servers_history added.

success Populating database...

success User account has been created successfully.

The installation is complete. Please check above if errors have occurred.
If no errors have occurred, you are good to go.

Go to your monitor PHP Server Monitor Documentation



17. Iniciar sesión con el usuario previamente creado:

SERVER MONITOR

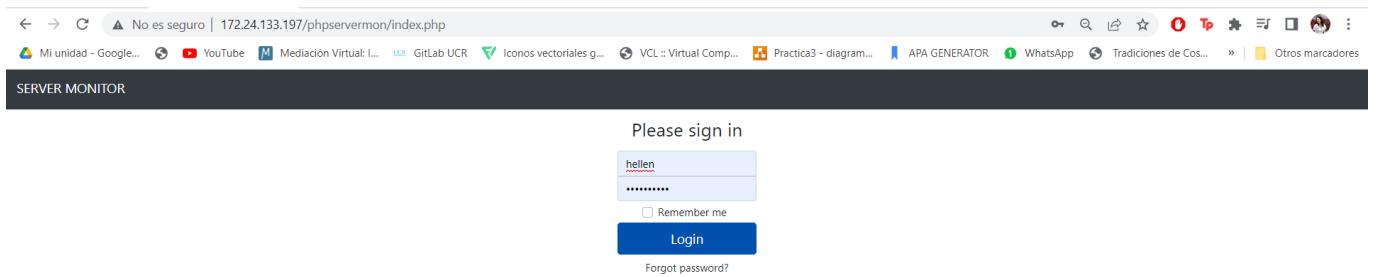
Please sign in

hellen

Remember me

Login

Forgot password?



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:

The screenshot shows a Telegram chat with BotFather (@botfather). The conversation starts with BotFather displaying its help command list. A user then sends the command `/newbot`. BotFather prompts for a bot name, which is then set to `server_monitor_sitio_1`. BotFather then guides the user through creating a bot username, ending with a note that it must end in `'bot'`. Finally, BotFather provides the generated API token: `5591740653:AAEeNVqWkM80s0QiNiQ2t8p_nwIV2i40SAU`.

BotFather
bot

/setcommands - change the list of commands
/deletebot - delete a bot

Bot Settings
/token - generate authorization token
/revoke - revoke bot access token
/setinline - toggle [inline mode](#)
/setinlinegeo - toggle inline [location requests](#)
/setinlinefeedback - change [inline feedback](#) settings
/setjoininggroups - can your bot be added to groups?
/setprivacy - toggle [privacy mode](#) in groups

Games
/mygames - edit your [games](#) [beta]
/newgame - create a new [game](#)
/listgames - get a list of your games
/editgame - edit a game
/deletetgame - delete an existing game

00:06

/newbot 00:17 ✓

Alright, a new bot. How are we going to call it? Please choose a name for your bot.

00:17

server_monitor_sitio_1 00:20 ✓

Good. Now let's choose a username for your bot. It must end in 'bot'. Like this, for example: TetrisBot or tetris_bot.

00:20

server_monitor_sitio_1_bot 00:21 ✓

Done! Congratulations on your new bot. You will find it at t.me/server_monitor_sitio_1_bot. You can now add a description, about section and profile picture for your bot, see [/help](#) for a list of commands. By the way, when you've finished creating your cool bot, ping our Bot Support if you want a better username for it. Just make sure the bot is fully operational before you do this.

Use this token to access the HTTP API:
`5591740653:AAEeNVqWkM80s0QiNiQ2t8p_nwIV2i40SAU`
Keep your token secure and store it safely, it can be used by anyone to control your bot.

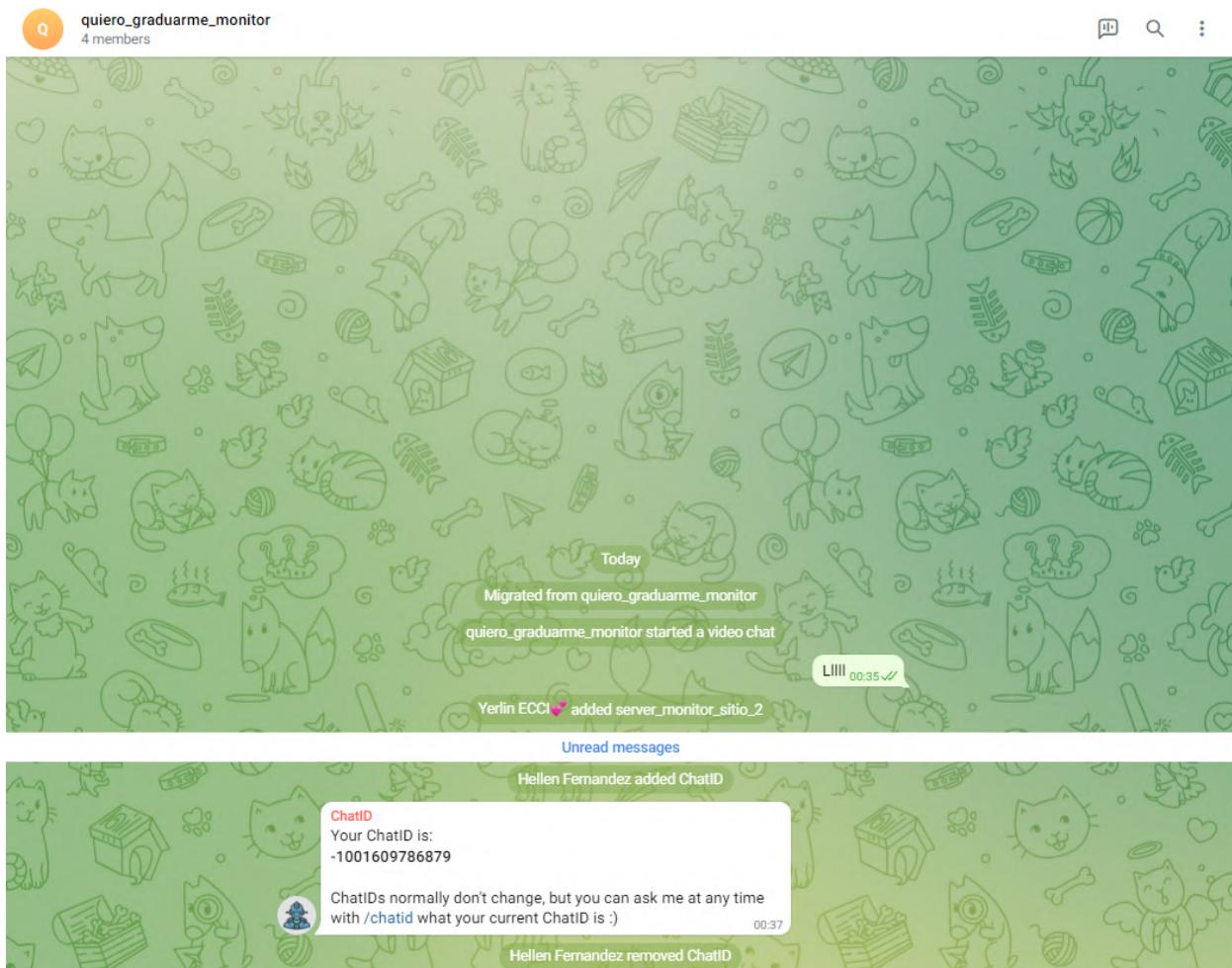
For a description of the Bot API, see this page:
<https://core.telegram.org/bots/api>

00:21

Message

API sitio 2:5385663947:AAEeNVqWkM80s0QiNiQ2t8p_nwIV2i40SAU

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:

SERVER MONITOR Status Servers Log Users Config Update Welcome, usuarioadmin ▾

Pushover Device

Pushover Device

Telegram

Telegram is a chat app that makes it easy to get real-time notifications. Visit the [documentation](#) for more info and an install guide.

[Click here to get your chat id](#)

Telegram chat id

-1001609786879

[Activate Telegram notifications](#)

Jabber

Jabber

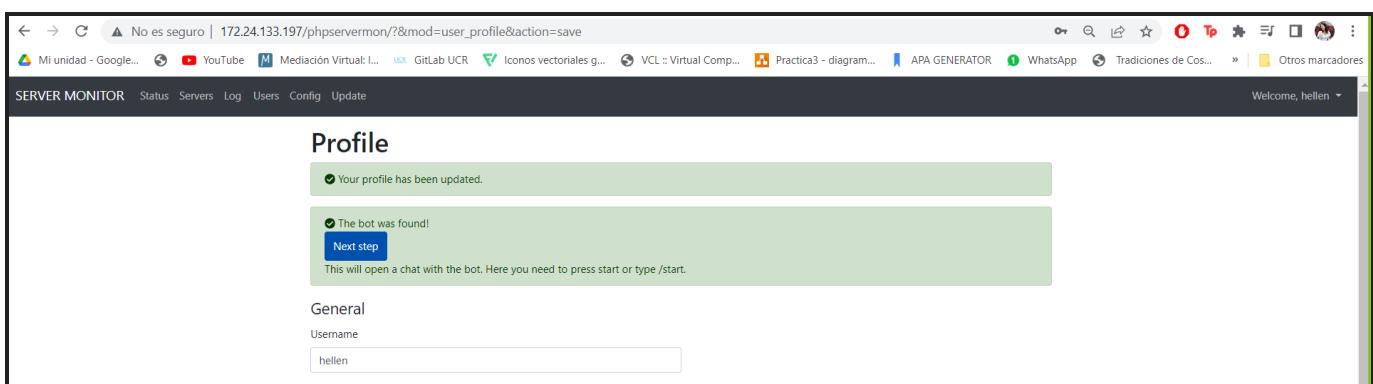
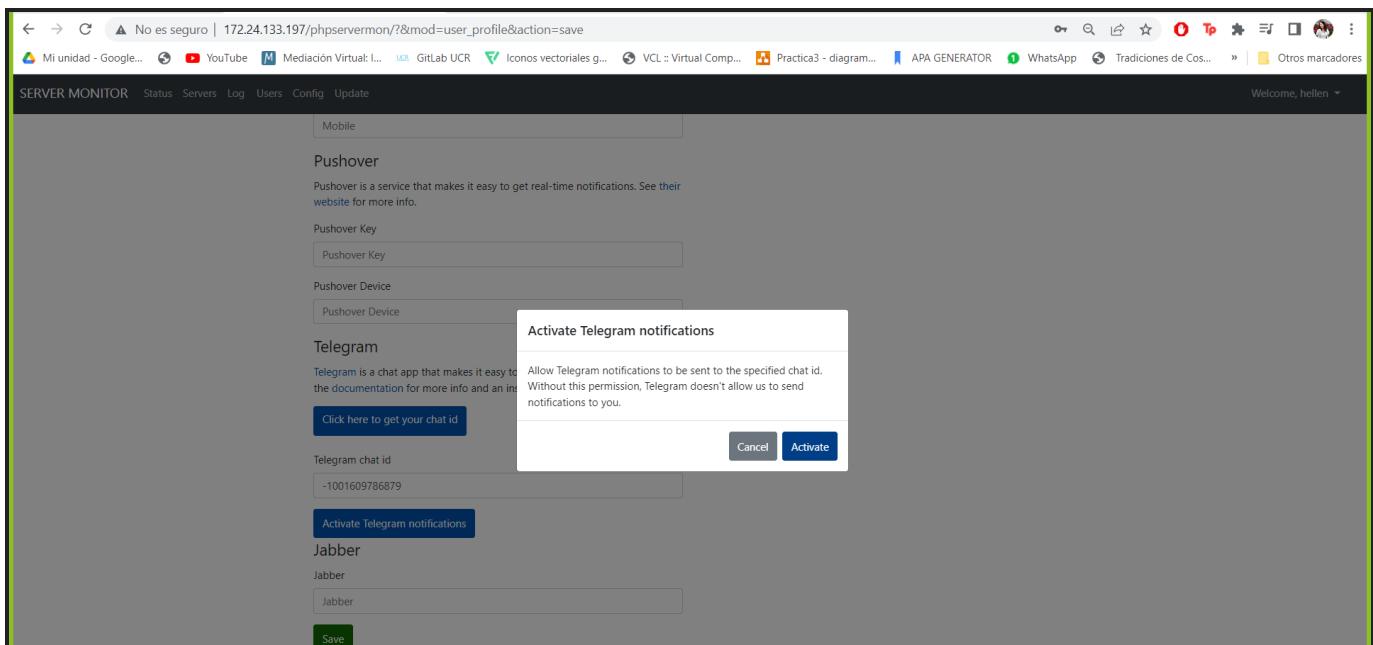
[Save](#)

22. Ahora copiar 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.

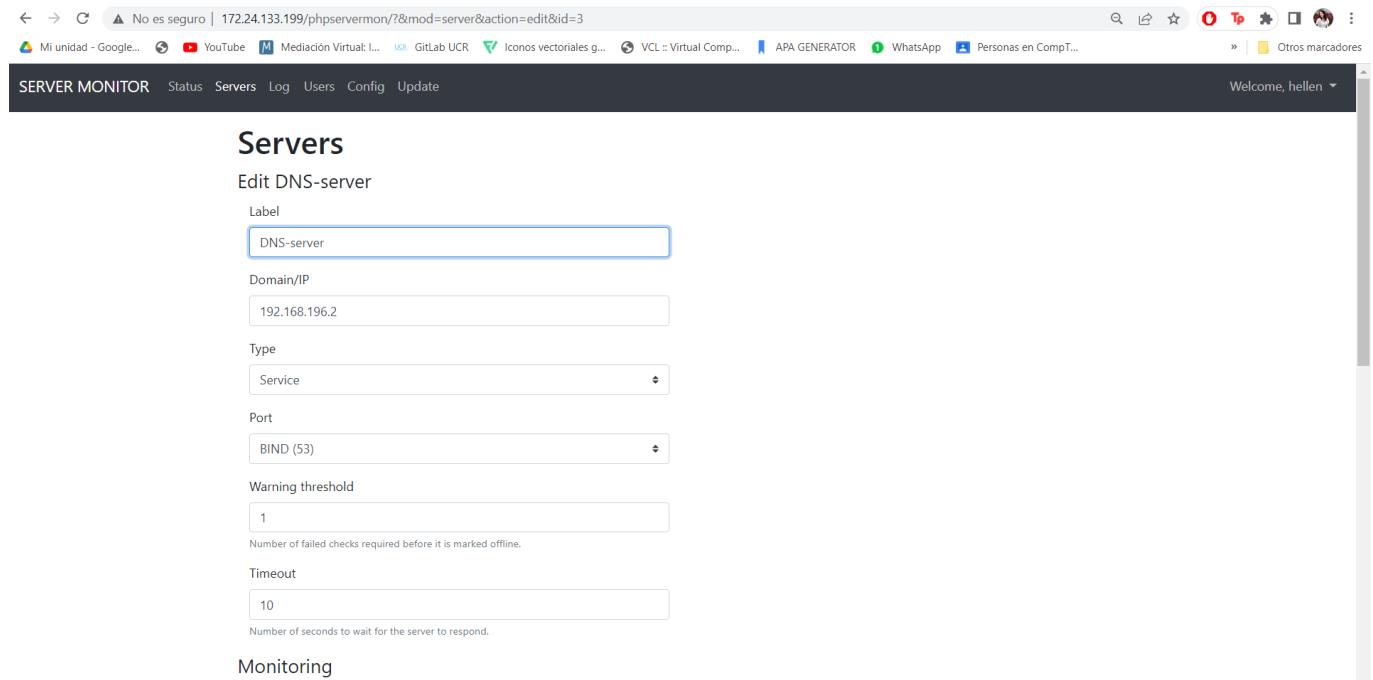
The screenshot shows the 'Config' tab selected in the top navigation bar. Below it, two green success messages are displayed: 'The configuration has been updated.' and 'Telegram notification sent'. A horizontal navigation bar below the messages includes tabs for General, Email, SMS, Pushover, **Telegram**, and Jabber. Under the 'Telegram' tab, the 'Telegram settings' section is visible. It contains a brief description of what Telegram is, a note about getting an API token, and two configuration options: 'Allow sending Telegram messages' (unchecked) and 'Log Telegram messages sent by the script' (checked). A text input field contains the API token: 5385663947:AAEeNVqWkM80s0QiNiQ2t8p_nwlV2i4OSAU. At the bottom of the section are 'Test' and 'Save' buttons.

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

The screenshot shows the 'Config' tab selected in the top navigation bar. Below it, the Pushover and Telegram sections are visible. The Pushover section contains fields for 'Pushover Key' and 'Pushover Device'. The Telegram section contains a note about getting a chat ID, a text input field with the value '-1001609786879', and a blue 'Activate Telegram notifications' button. At the bottom of the page are 'Save' and 'Cancel' buttons.



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



No es seguro | 172.24.133.199/phpservermon/?&mod=server&action=edit&id=3

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 ▾

Monitoring Yes

Send Email No

⚠ SMS notifications are disabled.

Send SMS No

⚠ Pushover notifications are disabled.

Send Pushover notification No

Send Telegram notification Yes

Send Jabber notification Yes

Permissions

Server will be visible for the following users hellen ▾

Save Go back

No es seguro | 172.24.133.197/phpservermon/?&mod=server_status

Mi unidad - Google... YouTube Mediación Virtual I... GitLab UCR Iconos vectoriales g... VCL :: Virtual Comp... Práctica3 - diagram... APA GENERATOR WhatsApp Tradiciones de Cos... » Otros marcadores

SERVER MONITOR Status Servers Log Users Config Update Welcome, hellen ▾

Status

#	Last online	Last check	Latency
Gmail SMTP	Never	a second ago	
SourceForge	Never	a second ago	
#	Last online	Last offline	Latency
DNS-server	a second ago	24 minutes ago (30 seconds)	0.0012300s

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. :

No es seguro | https://172.24.131.76/ui/#/host/vms/16

Mi unidad - Google... YouTube Mediación Virtual I... GitLab UCR » Otros marcadores

vmware ESXi hellen fernandezjmenez@172.24.131.76 ▾ Help ▾ Search ▾

DNS-projecto

```
[root@tarea-dns etc]# systemctl stop named
[root@tarea-dns etc]#
```

SERVER MONITOR Status Servers Log Users Config Update Welcome, hellen ▾

Status

#	Last online	Last check	Latency
DNS-server	5 minutes ago	a second ago	
Gmail SMTP	Never	a second ago	
SourceForge	Never	6 seconds ago	



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:

The screenshot shows two browser windows. The left window is a terminal session on an ESXi host, showing the command: [root@tarea-dns etc]# systemctl stop named; [root@tarea-dns etc]# systemctl restart named; [root@tarea-dns etc]#. The right window is a "SERVER MONITOR" interface showing the "Status" table:

#	Last online	Last check	Latency
Gmail SMTP	Never	4 seconds ago	
SourceForge	Never	4 seconds ago	
#	Last online	Last offline	Latency
DNS-server	3 seconds ago	about a minute ago (1 minute 30 seconds)	0.0011160s

The bottom part of the screenshot shows a green-themed monitoring interface with a message bubble: "server_monitor_sitio_1 Failed to connect to the following server: Server: DNS-server IP: [192.168.196.2](#) Port: 53 Error: Connection refused Date: 2022-06-02 01:48:27" and "Server 'DNS-server' is running again, it was down for: 1 minute 30 seconds". The time "01:48" is at the bottom left and "01:50" is at the bottom right.

Para la interfaz web tenemos las siguientes credenciales:

Sitio	Usuario	Contraseña
Sitio1	hellen	maggie1u2.
Sitio2	root	disenodisen022

27. Agregue la siguiente linea 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
```

```
HELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .---- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .--- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | |
# * * * * * user-name command to be executed

*/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

Domain/IP

Type

SSL Certificate Validity
The minimum remaining days the SSL certificate is still valid. Use 0 to disable check.

Request method

Post field
The data that will be send using the request method above.

Search string/pattern

← → ⌂ ▲ 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

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
Mark website as online. HTTP Status codes lower than 400 are marked as online by default. Separate with |.

Header name Header value
Case-sensitive. Regular expressions are allowed.

Warning threshold
Number of failed checks required before it is marked offline.

Timeout
Number of seconds to wait for the server to respond.

Authentication Settings (Optional)

Username

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 ▾

Monitoring

Monitoring Yes

Send Email No

⚠ SMS notifications are disabled.

Send SMS No

⚠ Pushover notifications are disabled.

Send Pushover notification No

Send Telegram notification Yes

Send Jabber notification No

Permissions

Server will be visible for the following users Please select ▾

Save

Progress bar: 100%

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

No es seguro | 172.24.133.199/phpservermon/?&mod=server_status

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 ▾

Status

aula	DNS-server	Free-Ipa	nube
Last online: a second ago Last offline: Never Latency: 0.3065300	Last online: a second ago Last offline: Monday at 14:51 (3 minutes) Latency: 0.0011289	Last online: a second ago Last offline: 13 hours ago (37 seconds) Latency: 0.0010152	Last online: a second ago Last offline: 13 hours ago (8 minutes) Latency: 0.3433678
soporte	web-server		
Last online: a second ago Last offline: Never Latency: 0.1374161	Last online: a second ago Last offline: 19 hours ago (1 minute) Latency: 0.0010321		

No es seguro | 172.24.133.199/phpservermon/?&mod=server

Mi unidad - Google... YouTube Mediación Virtual:... 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 ▾

+ Add new ⚙ Update

🔍

Label	Domain/IP	Port	Type	Latency	Last online	Last offline	Monitoring	
aula	http://aula.quierograduar.me.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.quierograduar.me.com	80	Website	0.3434	26 seconds ago	13 hours ago	⌚ ⓘ	⋮
soporte	http://soporte.quierograduar.me.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

```
client1
[usuarioadmin@client1 network-scripts]$ ip -br a
lo UNKNOWN 127.0.0.1/8 ::1/128
ens192 UP 192.168.165.11/24 fe80::6f60:ed2f:963a/64
ens224 UP
[usuarioadmin@client1 network-scripts]$ ping 192.168.198.12
PING 192.168.198.12 (192.168.198.12) 56(84) bytes of data.
64 bytes from 192.168.198.12: icmp_seq=1 ttl=62 time=5.23 ms
64 bytes from 192.168.198.12: icmp_seq=2 ttl=62 time=2.93 ms
64 bytes from 192.168.198.12: icmp_seq=3 ttl=62 time=2.70 ms
64 bytes from 192.168.198.12: icmp_seq=4 ttl=62 time=3.02 ms
64 bytes from 192.168.198.12: icmp_seq=5 ttl=62 time=2.70 ms
64 bytes from 192.168.198.12: icmp_seq=6 ttl=62 time=3.25 ms
64 bytes from 192.168.198.12: icmp_seq=7 ttl=62 time=3.81 ms
64 bytes from 192.168.198.12: icmp_seq=8 ttl=62 time=2.90 ms
64 bytes from 192.168.198.12: icmp_seq=9 ttl=62 time=2.70 ms
64 bytes from 192.168.198.12: icmp_seq=10 ttl=62 time=2.88 ms
64 bytes from 192.168.198.12: icmp_seq=11 ttl=62 time=2.51 ms
64 bytes from 192.168.198.12: icmp_seq=12 ttl=62 time=2.79 ms
64 bytes from 192.168.198.12: icmp_seq=13 ttl=62 time=3.00 ms
64 bytes from 192.168.198.12: icmp_seq=14 ttl=62 time=2.61 ms
64 bytes from 192.168.198.12: icmp_seq=15 ttl=62 time=3.13 ms
64 bytes from 192.168.198.12: icmp_seq=16 ttl=62 time=2.93 ms
64 bytes from 192.168.198.12: icmp_seq=17 ttl=62 time=3.25 ms
64 bytes from 192.168.198.12: icmp_seq=18 ttl=62 time=3.36 ms
^C
--- 192.168.198.12 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 176ms
rtt min/avg/max/mdev = 2.510/3.854/5.232/0.578 ms
[usuarioadmin@client1 network-scripts]$
```

```
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]# ping 192.168.165.11
PING 192.168.165.11 (192.168.165.11) 56(84) bytes of data.
64 bytes from 192.168.165.11: icmp_seq=1 ttl=62 time=2.83 ms
64 bytes from 192.168.165.11: icmp_seq=2 ttl=62 time=2.63 ms
64 bytes from 192.168.165.11: icmp_seq=3 ttl=62 time=2.70 ms
64 bytes from 192.168.165.11: icmp_seq=4 ttl=62 time=3.20 ms
64 bytes from 192.168.165.11: icmp_seq=5 ttl=62 time=3.07 ms
64 bytes from 192.168.165.11: icmp_seq=6 ttl=62 time=2.94 ms
64 bytes from 192.168.165.11: icmp_seq=7 ttl=62 time=3.05 ms
64 bytes from 192.168.165.11: icmp_seq=8 ttl=62 time=2.88 ms
64 bytes from 192.168.165.11: icmp_seq=9 ttl=62 time=2.91 ms
64 bytes from 192.168.165.11: icmp_seq=10 ttl=62 time=2.67 ms
^C
--- 192.168.165.11 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9815ms
rtt min/avg/max/mdev = 2.634/2.892/3.201/0.109 ms
[root@cliente-3 hellen]#
```

Cliente sitio 1 a DMZ sitio 1

```
client1
[usuarioadmin@client1 network-scripts]$ ping 192.168.164.1
PING 192.168.164.1 (192.168.164.1) 56(84) bytes of data.
64 bytes from 192.168.164.1: icmp_seq=1 ttl=64 time=0.765 ms
64 bytes from 192.168.164.1: icmp_seq=2 ttl=64 time=0.535 ms
64 bytes from 192.168.164.1: icmp_seq=3 ttl=64 time=0.459 ms
^C
```

Cliente sitio 1 a DMZ sitio 2

```
[usuarioadmin@client1 network-scripts]$ ping 192.168.196.1
PING 192.168.196.1 (192.168.196.1) 56(84) bytes of data.
64 bytes from 192.168.196.1: icmp_seq=1 ttl=63 time=2.72 ms
64 bytes from 192.168.196.1: icmp_seq=2 ttl=63 time=1.53 ms
64 bytes from 192.168.196.1: icmp_seq=3 ttl=63 time=1.55 ms
64 bytes from 192.168.196.1: icmp_seq=4 ttl=63 time=1.67 ms
64 bytes from 192.168.196.1: icmp_seq=5 ttl=63 time=1.46 ms
^C
```

DMZ sitio 1 a cliente sitio 1

```
[usuarioadmin@client1 network-scripts]$ ip 'br a
> ^C
[usuarioadmin@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
[usuarioadmin@client1 network-scripts]$
```

```
[root@dns etc]$ ping 192.168.165.11
PING 192.168.165.11 (192.168.165.11) 56(84) bytes of data.
^C
--- 192.168.165.11 ping statistics ---
17 packets transmitted, 0 received, 100% packet loss, time 16000ms
```

DMZ sitio 2 a cliente sitio 2

The screenshot shows two terminal windows. The top window, titled 'cliente-3', displays the command 'ip -br a' and its output:

```
[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]#
```

The bottom window, titled 'DNS-proyecto', displays the command 'ping 192.168.198.12' and its output:

```
[root@tarea-dns etc]# ping 192.168.198.12
PING 192.168.198.12 (192.168.198.12) 56(84) bytes of data.
^C
--- 192.168.198.12 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2000ms
[root@tarea-dns etc]#
```

Cliente sitio 1 a DNS

The screenshot shows a terminal window titled 'client1' displaying the command 'dig querograduar.me.com' and its output:

```
[root@client1 network-scripts]# dig querograduar.me.com

; <>> DIG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <>> querograduar.me.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60614
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

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

;; ANSWER SECTION:
quierograduar.me.    86400   IN      A      192.168.164.2
quierograduar.me.    86400   IN      A      192.168.196.2

;; AUTHORITY SECTION:
quierograduar.me.    86400   IN      NS     secondarydns.quierograduar.me.
quierograduar.me.    86400   IN      NS     masterdns.quierograduar.me.

;; ADDITIONAL SECTION:
masterdns.quierograduar.me. 86400 IN A      192.168.196.2
secondarydns.quierograduar.me. 86400 IN A      192.168.164.2

;; Query time: 5 msec
;; SERVER: 192.168.196.2#53(192.168.196.2)
;; WHEN: Thu May 26 10:41:14 EDT 2022
;; MSG SIZE  rcvd: 163
```

Cliente sitio 2 a DNS

```
[root@cliente-3 hellen]# digquierograduarne.com
; <>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <>>quierograduarne.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55799
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 4096
;; QUESTION SECTION:
;quierograduarne.com. IN A
;; ANSWER SECTION:
quierograduarne.com. 86400 IN A 192.168.164.2
quierograduarne.com. 86400 IN A 192.168.196.2
;; AUTHORITY SECTION:
quierograduarne.com. 86400 IN NS secondarydns.quierograduarne.com.
quierograduarne.com. 86400 IN NS masterdns.quierograduarne.com.
;; ADDITIONAL SECTION:
masterdns.quierograduarne.com. 86400 IN A 192.168.196.2
secondarydns.quierograduarne.com. 86400 IN A 192.168.164.2
;; Query time: 7 msec
;; SERVER: 192.168.196.2#53(192.168.196.2)
;; WHEN: Thu May 26 10:42:34 EDT 2022
;; MSG SIZE rcvd: 163

[root@cliente-3 hellen]# _
```

Cliente sitio 1 a internet

```
[root@client1 network-scripts]# 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=51.0 ms
64 bytes from mia07s62-in-f14.1e100.net (142.250.217.238): icmp_seq=2 ttl=114 time=51.3 ms
64 bytes from mia07s62-in-f14.1e100.net (142.250.217.238): icmp_seq=4 ttl=114 time=51.3 ms
64 bytes from mia07s62-in-f14.1e100.net (142.250.217.238): icmp_seq=5 ttl=114 time=52.1 ms
64 bytes from mia07s62-in-f14.1e100.net (142.250.217.238): icmp_seq=6 ttl=114 time=51.9 ms
64 bytes from mia07s62-in-f14.1e100.net (142.250.217.238): icmp_seq=7 ttl=114 time=53.0 ms
^C
```

```
[client1] 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] 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] 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.unimadalena.edu.co
 * extras: mirror.unimadalena.edu.co
 * updates: mirror.unimadalena.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 ~]# 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

[usuarioradmin@server2 ~]$ configuration:
  servers: 172.24.133.197 172.24.133.165
  interface: ens224
```

```
server2 ~]# [usuarioradmin@server2 ~]$ digquierograduarne.com
: <>> DIG 9.11.4-P2-RedHat-9.11.4-26.P2.e17_9.9 <>>quierograduarne.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:
;quierograduarne.com. IN A
;; ANSWER SECTION:
quierograduarne.com. 86400 IN A 192.168.164.2
quierograduarne.com. 86400 IN A 192.168.196.2
;; AUTHORITY SECTION:
quierograduarne.com. 86400 IN NS secondarydns.quierograduarne.com.
quierograduarne.com. 86400 IN NS masterdns.quierograduarne.com.
;; ADDITIONAL SECTION:
masterdns.quierograduarne.com. 86400 IN A 192.168.196.2
secondarydns.quierograduarne.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 18:50:49 EDT 2022
;; MSG SIZE rcvd: 163
[usuarioradmin@server2 ~]$
```

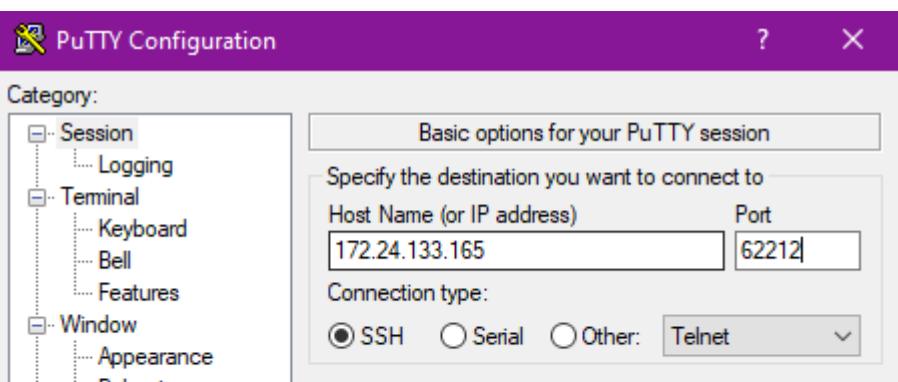
SSH cliente sitio 1 a DNS

```
[client1] client1
[root@localhost ~]# exit
logout
Connection to 192.168.164.2 closed.
[root@client1 network-scripts]# ssh 192.168.164.2 -p 22
root@192.168.164.2's password:
Last login: Thu May 26 12:01:38 2022 from 192.168.165.11
[root@localhost ~]#
```

SSH cliente sitio 2 a DNS

```
[cliente-3] cliente-3
[root@cliente-3 hellen]# ssh 192.168.196.2
^C
[root@cliente-3 hellen]# ssh 192.168.196.2 -p 22
root@192.168.196.2's password:
Last login: Wed May 25 01:58:31 2022
[root@proyecto-dns ~]#
```

SSH internet a DNS sitio 1

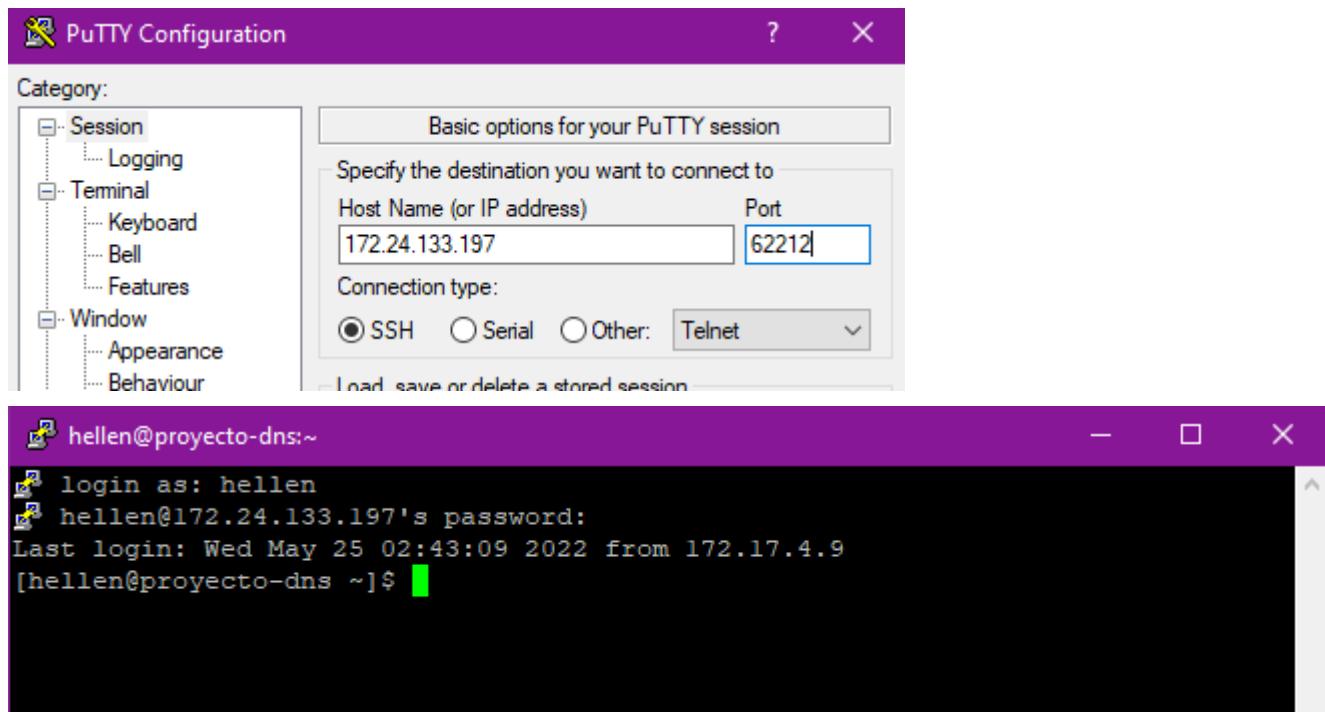


The PuTTY Configuration window shows the following session details:

- Host Name (or IP address):** 172.24.133.165
- Port:** 62212
- Connection type:** SSH (radio button selected)

```
usuarioadmin@dns:~$ 
login as: usuarioadmin
usuarioadmin@172.24.133.165's password:
Last login: Thu May 26 12:07:01 2022 from 10.232.110.27
[usuarioadmin@dns ~]$
```

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”:

```
root@ipa1:/home/hellen
06/22/2022 23:06:14 06/23/2022 23:05:59 krbtgt/QUIEROGRADUARME.YA@QUIEROGRADUARME.YA
[root@ipa1 hellen]# ipa user-add --password
First name: Maggie
Last name: Fernandez
User login [mfernandez]:
Password:
Enter Password again to verify:
-----
Added user "mfernandez"
-----
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
Password: True
Member of groups: ipausers
Kerberos keys available: True
```

2. Se comprueba que el usuario fue agregado:

```
root@ipa1:/home/hellen
dn: uid=mfernandez,cn=users,cn=accounts,dc=quierograduarne,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@quierograduarne.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=quierograduarne,dc=ya
objectclass: top, person, organizationalperson, inetorgperson, inetuser, posixaccount,
            krbprincipalaux, krbticketpolicyaux, ipaobject, ipasshuser,
            ipaSshGroupOfPubKeys, mepOriginEntry
-----
Number of entries returned 2
-----
[root@ipa1 hellen]#
```

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=quierograduarne,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: AAIPSSrFicm9vdC9hZGlpbkBRVU1FUk9HUKFEVUFSTUUuWUEA  
krblastpwdchange: 20220621043319Z  
objectclass: top, person, posixaccount, krbprincipalaux, krbticketpolicyaux,  
inetuser, ipaobject, ipasshuser, ipaSshGroupOfPubKeys  
  
dn: uid=mfernandez,cn=users,cn=accounts,dc=quierograduarne,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@quierograduarne.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: AAIPSrFicm9vdC9hZGlpbkBRVU1FUk9HUhFEVUFSTUUuWUEA  
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: AAL52LNicm9vdC9hZGlpbkBRVU1FUk9HUhFEVUFSTUUuWUEA  
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:

```
root@ipa1:/home/hellen
[root@ipa1 hellen]# ipa user-add --password
First name: Yerlin
Last name: Ledezma
User login [yledezma]:
Password:
Enter Password again to verify:
-----
Added user "yledezma"
-----
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@quierograduar.me.ya
UID: 1559600003
GID: 1559600003
Password: True
Member of groups: ipausers
Kerberos keys available: True
[root@ipa1 hellen]#
```

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

root@ipareplica:/home/usuarioadmin

```
dn: uid=yledezma,cn=users,cn=accounts,dc=quierograduararme,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@quierograduararme.ya
UID: 1559600003
GID: 1559600003
Account disabled: False
Preserved user: False
Member of groups: ipausers
ipauniqueid: 71469280-f2a9-11ec-9f0a-000c294594e3
krbextradata: AAIR5rNcm9vdC9hZG1pbkBRVUlFUK9HUKFEVUFSTUUuWUEA
krblastpwdchange: 20220623040329Z
mepmanagedentry: cn=yledezma,cn=groups,cn=accounts,dc=quierograduararme,dc=ya
objectclass: top, person, organizationalperson, inetorgperson, inetuser,
            posixaccount, krbprincipalaux, krbticketpolicyaux, ipaobject,
            ipasshuser, ipaSshGroupOfPubKeys, mepOriginEntry
```

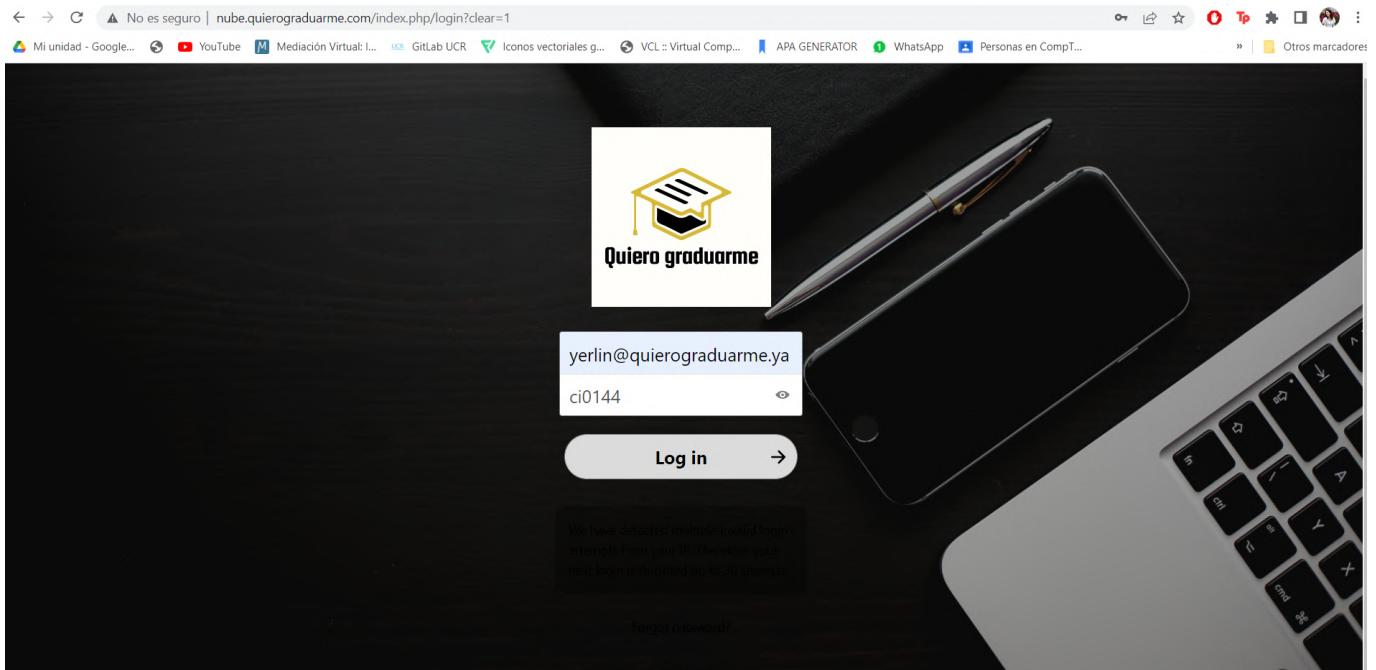
Number of entries returned 3

Prueba NextCloud

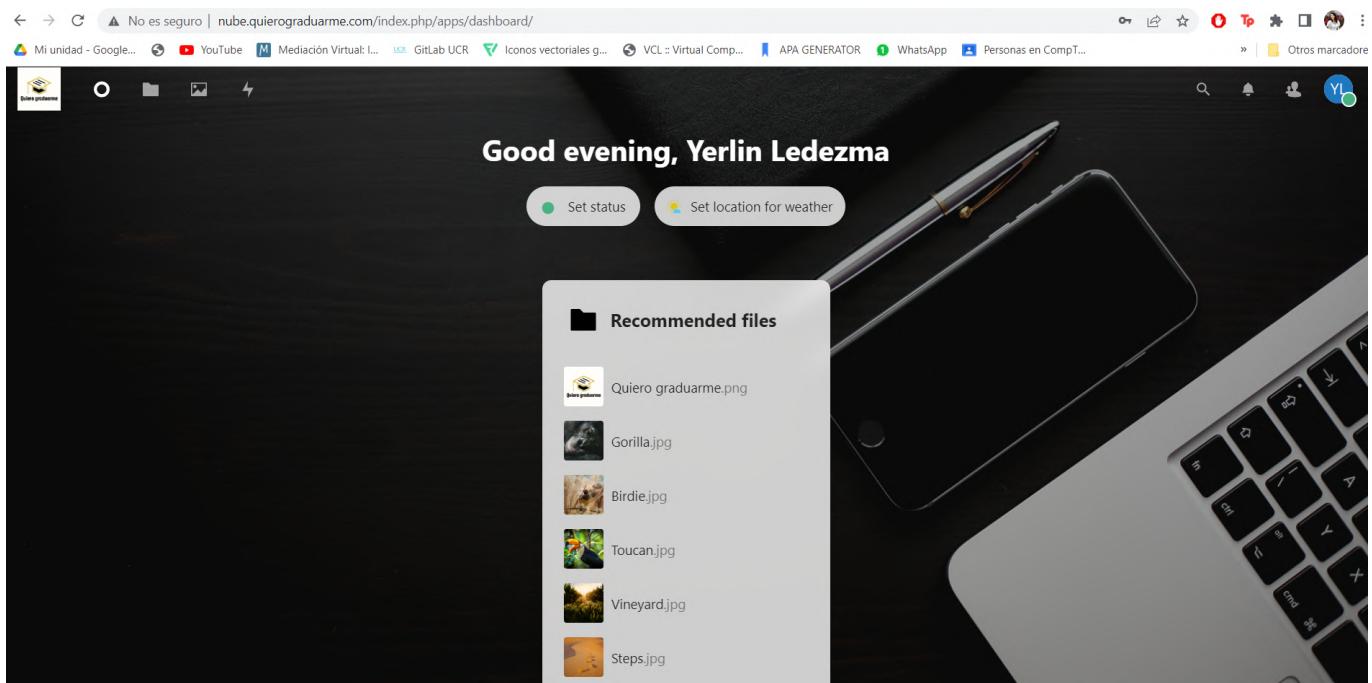
1. Con el correo yerlin iniciar sesión:

yerlin@quierograduararme.ya

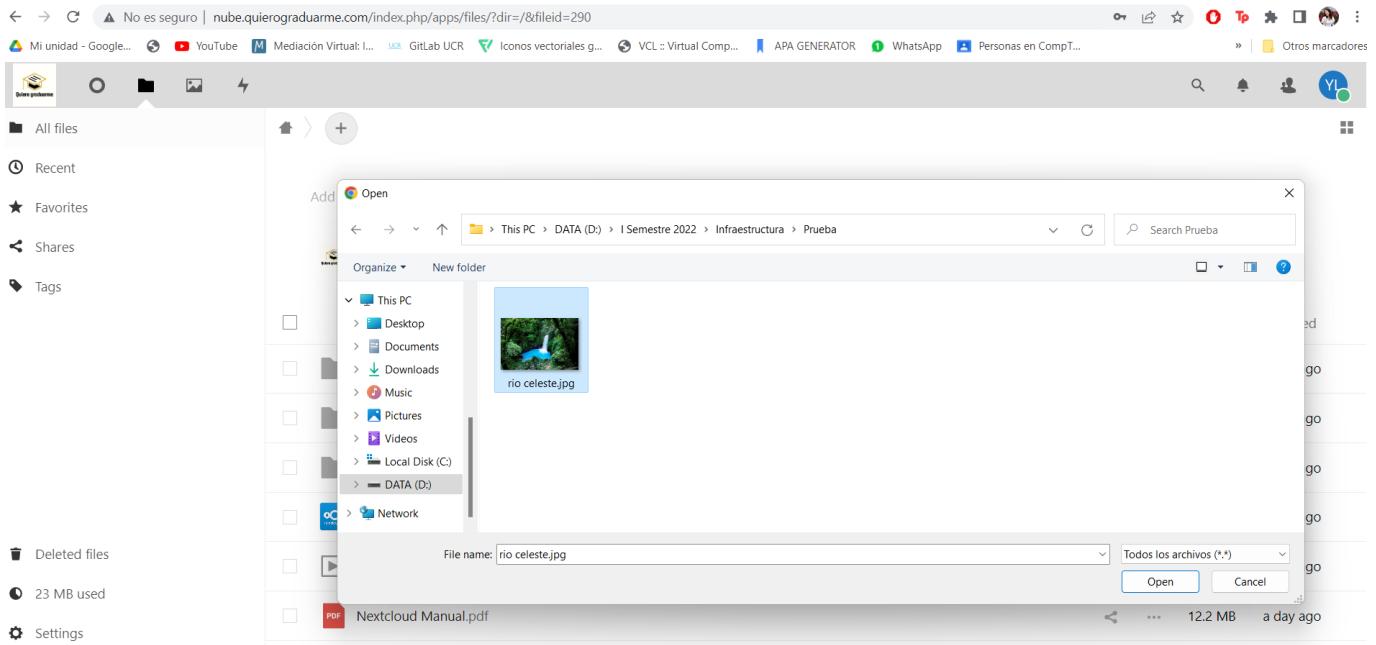
ci0144



2. Al iniciar sesión diríjase al ícono de carpeta.



3. Subir una imagen:



4. Verificar que se va a subió la imagen:

A screenshot of the Nextcloud file list. The file 'rio celeste.jpg' is listed along with other files: 'Nextcloud Manual.pdf', 'Quiero graduarme.png', and 'Reasons to use Nextcloud.pdf'. The file 'rio celeste.jpg' was uploaded 5 minutes ago. The total folder size is 23.2 MB.

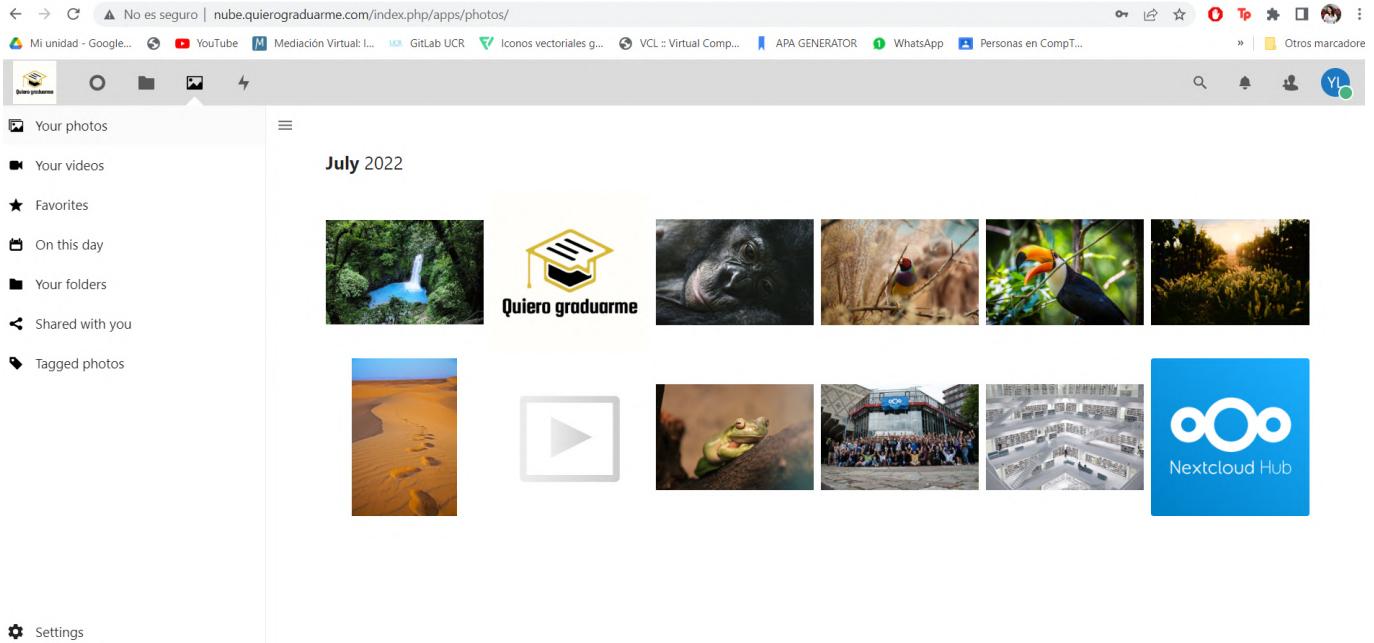
Name	Size	Modified
Nextcloud Manual.pdf	12.2 MB	a day ago
Quiero graduarme.png	18 KB	7 hours ago
Reasons to use Nextcloud.pdf	954 KB	a day ago
rio celeste.jpg	293 KB	5 minutes ago

← → ⌛ No es seguro | nube.quierograduar.me/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



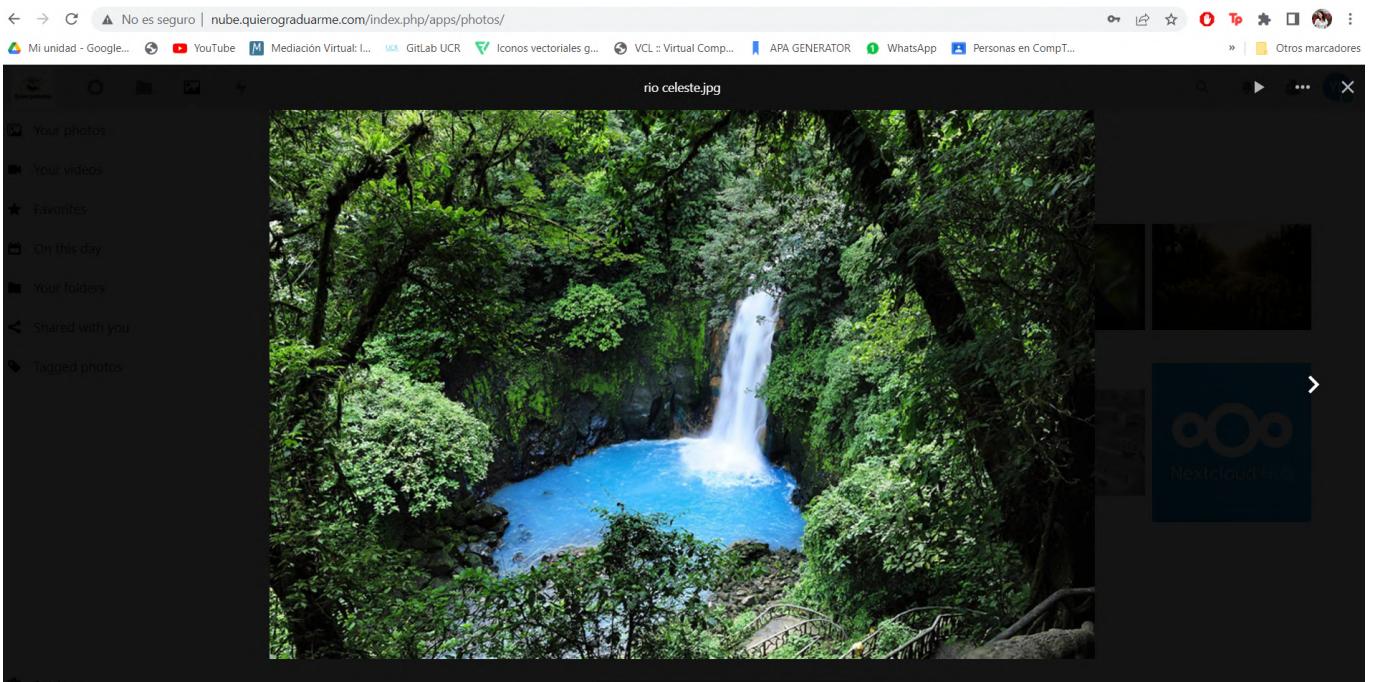
⚙ Settings

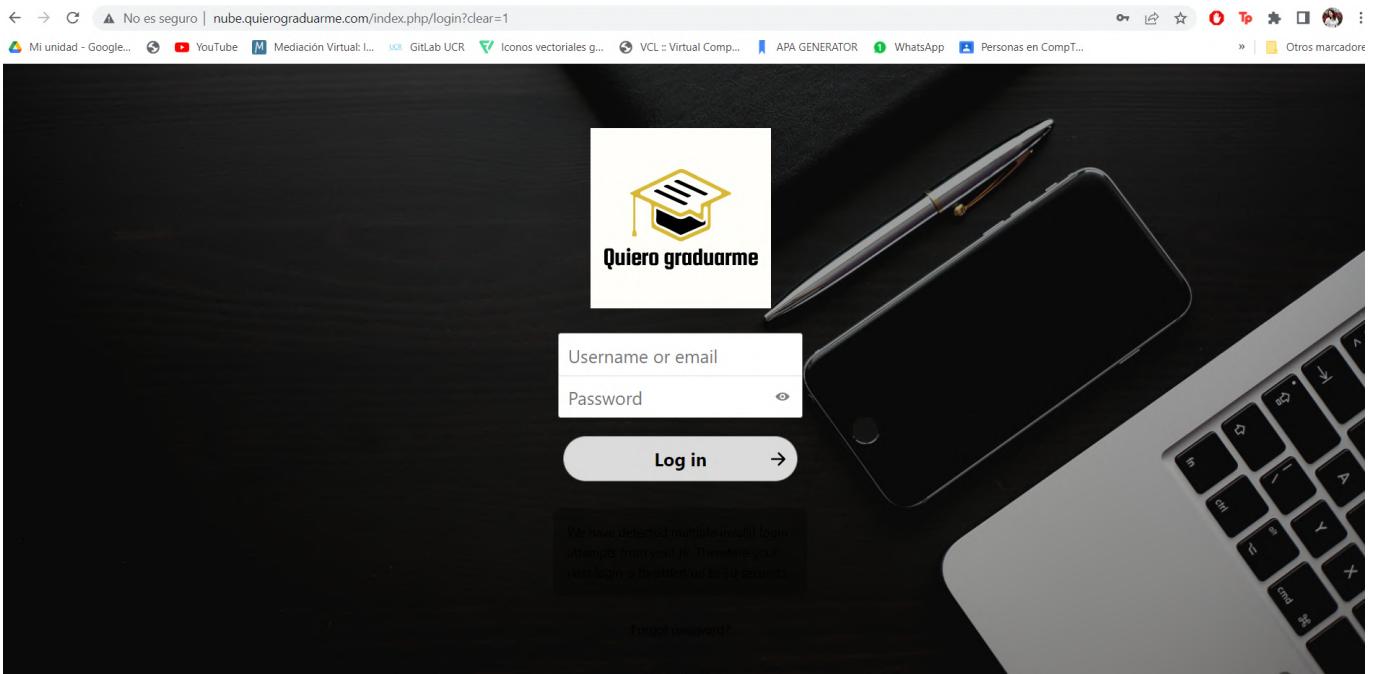
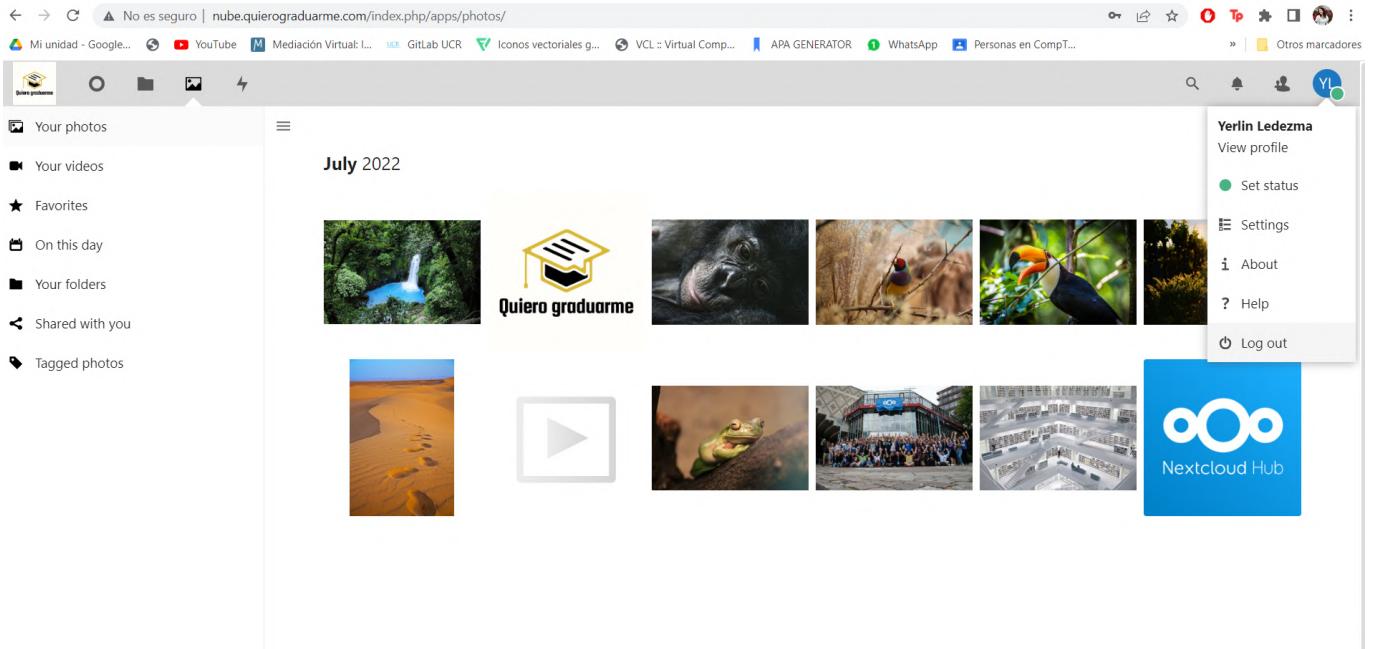
← → ⌛ No es seguro | nube.quierograduar.me/index.php/apps/photos/

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

rio celeste.jpg





Prueba Osticket

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

Usuario: yerlin

Contraseña: ci0144

The screenshot shows the 'Sign in to Quiero GraduarMe Support' page. At the top, there are input fields for 'username' (filled with 'yerlin') and 'password' (filled with '.....'). Below these is a 'Sign In' button. To the right of the input fields, there is a message: 'Not yet registered? [Create an account](#)' and 'I'm an agent — [sign in here](#)'. A yellow padlock icon is also present. At the bottom of the form area, it says: 'If this is your first time contacting us or you've lost the ticket number, please [open a new ticket](#)'. The footer contains copyright information: 'Copyright © 2022 Quiero GraduarMe Support - All rights reserved.' and 'powered by Osticket'.

The screenshot shows the 'Open a New Ticket' page. At the top, the user 'Yerlin Ledezma' is logged in, with links for 'Profile', 'Tickets (0)', and 'Sign Out'. Below this is a navigation bar with 'Support Center Home', 'Open a New Ticket', and 'Tickets (0)'. The main section is titled 'Open a New Ticket' and instructs the user to 'Please fill in the form below to open a new ticket.' It includes fields for 'Email' (set to 'yerlin@quierograduarme.ya') and 'Client' (set to 'Yerlin Ledezma'). A dropdown menu for 'Help Topic' is shown with the placeholder '— Select a Help Topic — *'. At the bottom of the form are three buttons: 'Create Ticket', 'Reset', and 'Cancel'. The footer contains copyright information: 'Copyright © 2022 Quiero GraduarMe Support - All rights reserved.' and 'powered by Osticket'.

2. Crear un ticket

The screenshot shows a web browser window with the URL soporte.quierograduar.me/tickets.php?id=2. The page title is "Yerlin Ledezma | Profile | Tickets (1) - Sign Out". At the top, there's a navigation bar with links like "GitHub", "Projects - Dashboard...", "WhatsApp", "Telegram Web", "Mediación Virtual: I...", "Mediación Virtual: I...", "Diccionario Lesco", "TC-501", "TCU 501 - Google...", and "Otros marcados". Below the navigation is the Quiero graduarme logo. The main content area has tabs for "Support Center Home", "Open a New Ticket", and "Tickets (1)". A sub-header says "Problema de prueba #368308". There are two sections: "Basic Ticket Information" and "User Information". Under "Basic Ticket Information", it shows: Ticket Status: Open, Department: Maintenance, Create Date: 7/20/22 9:53 PM. Under "User Information", it shows: Name: Yerlin Ledezma, Email: yerlin@quierograduar.me.ya, Phone: (empty). A comment from "Yerlin Ledezma" posted at 7/20/22 9:53 PM reads: "Esta es una prueba realizada por Yerlin" followed by the text "Amo mi carrera, amo mi carrera, amo mi carrera" and a small image of a person's hair.

3. Ingresar al inicio de sesión del administrador

The screenshot shows a web browser window with the URL soporte.quierograduar.me/scp/login.php. The page title is "Authentication Required". It features the OSTicket logo (an orange kangaroo icon) and the text "Authentication Required". There are two input fields: one for "Email" containing "hellenfdz12@gmail.com" and one for "Password" containing "*****". Below the password field is a "Log In" button. At the bottom of the login form, it says "Copyright © Quiero Graduarne Support". In the bottom right corner of the page, there's a banner that says "Powered by OSTicket". The background of the page is a blurred image of a city street at sunset.

4. Verificar que se haya creado el ticket

The screenshot shows the 'Tickets' section of the Quiero GraduarMe admin panel. The 'Open' tab is selected, displaying two tickets:

Ticket	Last Updated	Subject	From	Priority	Assigned To
368308	7/20/22 9:53 PM	Problema de prueba	Yerlin Ledezma	Normal	
437438	7/15/22 11:47 PM	osTicket Installed!	osTicket Support	Normal	

Below the table, there are buttons for 'Select: All', 'None', and 'Toggle'. At the bottom, it says 'Page: [1] Export' and 'Showing 1 - 2 of about 2'.

The screenshot shows a detailed view of Ticket #368308. The ticket subject is 'Problema de prueba'. The ticket details are as follows:

Status:	Open	User:	Yerlin Ledezma (1)
Priority:	Normal	Email:	yerlin@quierograduarme.ya
Department:	Maintenance	Source:	Web (172.17.0.9)
Create Date:	7/20/22 9:53 PM		

Below this, there are sections for 'Assigned To', 'SLA Plan', and 'Due Date'. The 'Assigned To' field shows '— Unassigned —'. The 'SLA Plan' is 'Default SLA' and the 'Due Date' is '7/22/22 5:00 PM'. The 'Help Topic' is 'Report a Problem'.

At the bottom, the 'Ticket Thread (1)' tab is selected, showing a message from 'Yerlin Ledezma posted 7/20/22 9:53 PM': 'Esta es una prueba realizada por Yerlin'.

No es seguro | soprote.quierograduar.me.com/scp/tickets.php?id=2

GitHub Projects - Dashboard... WhatsApp Telegram Web Mediación Virtual: I... Mediación Virtual: II... Diccionario Lesco TC-501 TCU 501 - Google...

_ticket #368308

From: Support<yerlin.ledezma@ucr.ac.cr>

Recipients: "Yerlin Ledezma" <yerlin@quierograduar.me.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 Graduar.me Support All Rights Reserved.

Prueba Moodle

1. Ingresar a aula.quierograduar.me con las credenciales de administrador

Usuario: admin

Contraseña: maggieLu2

No es seguro | aula.quierograduar.me/login/index.php

GitHub Projects · Dashboard WhatsApp Telegram Web Mediación Virtual: I... Mediación Virtual: I... Diccionario Lesco TC-501 T...

Quiero graduarme

admin

Log in

Lost password?

Some courses may allow guest access

Log in as a guest

Cookies notice

2. Agregar un nuevo curso

No es seguro | aula.quierograduar.me/?redirect=0

GitHub Projects · Dashboard WhatsApp Telegram Web Mediación Virtual: I... Mediación Virtual: I... Diccionario Lesco TC-501 T...

Home Dashboard My courses Site administration

Quiero graduarme

Home Settings Participants Reports Question bank More

Available courses

Add a new course

← → ⌛ 🏠 ⚡ No es seguro | aula.quierograduar.me.com/course/

G GitHub M Projects - Dashboard WhatsApp T Telegram Web M Mediación Virtual: I... M Mediación Virtual: I... Diccionario Lesco TC-501 TCU 501 - Google...

Home Dashboard My courses Site administration

Quiero graduarme

Category Settings More ▾

Search courses



More ▾

Prueba curso



Este es un curso de prueba para el sitio quiero graduarme

Teacher: Admin User

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.

← → ⌛ 🏠 ⚡ No es seguro | aula.quierograduar.me.com/enrolinstances.php?id=2

G GitHub M Projects - Dashboard WhatsApp T Telegram Web M Mediación Virtual: I... M Mediación Virtual: I... Diccionario Lesco TC-501 TCU 501 - Google... > | Otro

Home Dashboard My courses Site administration AU Edit

General

Announcements

Topic 1

Topic 2

Topic 3

Topic 4

Enrolment methods

- Enrolments
- Enrolled users
- Enrolment methods**
- Groups
- Groups
- Groupings
- Overview
- Permissions
- Permissions
- Other users
- Check permissions

Prueba curso

Course Settings Participants Grades Reports More ▾

Enrolment methods

	Users	Up/Down	Edit
Self enrolment (Student)	1	⬇️	🔗 🔍 🔍 🔍
Self enrolment (Student)	0	⬆️ ⬇️	🔗 🔍 🔍 🔍
Self enrolment (Student)	0	⬆️ ⬇️	🔗 🔍 🔍 🔍
Self enrolment (Student)	0	⬆️	🔗 🔍 🔍 🔍

Add method Choose... ⚡

Escribe aquí para buscar. ⌛

01:21

No es seguro | aula.quierograduar.me.com/enrol/editinstance.php?type=elf&courseid=2

GitHub Projects - Dashboard WhatsApp Telegram Web Mediación Virtual I... Mediación Virtual I... Diccionario Lesco TC-501 TCU 501 - Google... Otros marcadores

Home Dashboard My courses Site administration Edit mode

Self enrolment

Self enrolment

Custom instance name:

Allow existing enrolments: Yes

Allow new enrolments: Yes

Enrolment key: cl0144

Use group enrolment keys: No

Default assigned role: Student

Enrolment duration: 0 days

Notify before enrolment expires: No

Notification threshold: 1 days

Start date: 21 July 2022 01 31

End date: 21 July 2022 01 31

No es seguro | aula.quierograduar.me.com/enrol/editinstance.php?type=elf&courseid=2

GitHub Projects - Dashboard WhatsApp Telegram Web Mediación Virtual I... Mediación Virtual I... Diccionario Lesco TC-501 TCU 501 - Google... Otros marcadores

Home Dashboard My courses Site administration Edit mode

General

Announcements

Notify before enrolment expires: No

Notification threshold: 1 days

Start date: 21 July 2022 01 31

End date: 21 July 2022 01 31

Unenrol inactive after: Never

Max enrolled users: 0

Send course welcome message: From the course contact

Custom welcome message: Bienvenido al cursos de prueba quiero graduarme

Add method Cancel

aula.quierograduar.me.com/enrol/editinstance.php?type=elf&courseid=2#

4. Ingrese al curso con un usuario y contraseña distinto al de administrador
En este caso se usa el usuario yerlin



Quiero graduarme

Log in

[Lost password?](#)

Some courses may allow guest access

[Log in as a guest](#)

[Cookies notice](#)

5. Ingresar la contraseña y matricularse

The screenshot shows the 'Prueba curso' course page. At the top, there are navigation links for GitHub, Projects - Dashboard, WhatsApp, Telegram Web, Mediación Virtual: I..., and Mediación Virtual: I... . Below the header, there are links for Home, Dashboard, and My courses. The main title is 'Prueba curso'. There are two tabs: 'Course' and 'Enrol me in this course', with the latter being active. A sub-section titled 'Enrolment options' is visible. Below it, there is a search bar with the text 'Prueba curso' and a magnifying glass icon. A small image of Homer Simpson from 'The Simpsons' is shown with the caption 'Este es un curso de prueba para el sitio quiero graduarme'. The teacher is listed as 'Teacher: Admin User'. Under the 'Self enrolment (Student)' section, there is a field for 'Enrolment key' containing '*****' and a blue 'Enrol me' button.

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

The screenshot shows the 'Participants' page for the 'Prueba curso' course. The left sidebar has a tree view with 'General', 'Announcements', 'Topic 1', 'Topic 2', 'Topic 3', and 'Topic 4'. The main area is titled 'Prueba curso' and has tabs for Course, Participants, Grades, Competencies, and More. The 'Participants' tab is selected. A sub-section titled 'Enrolled users' is displayed. It includes filters for 'Match' (Any or Select), 'Add condition', 'Clear filters', and 'Apply filters'. Below the filters, it says '2 participants found'. There are dropdown menus for 'First name' (with letters A-Z) and 'Surname' (with letters A-Z). A table lists the participants:

First name / Surname	Roles	Groups	Last access to course
YL Yerlin Ledezma	Student	No groups	46 secs
AU Admin User	Teacher	No groups	5 mins 36 secs

Prueba phemonitor

No es seguro | 172.24.133.199/phpservermon/

Mi unidad - Google... YouTube Mediación Virtual:... GitLab UCR Iconos vectoriales g... VCL :: Virtual Comp... APA GENERATOR WhatsApp Personas en CompT... » Otros marcadores

Welcome, hellen ▾

SERVER MONITOR Status Servers Log Users Config Update

Status

■ ■ ■

aula

Last online: 19 seconds ago
Last offline: Never
Latency: 0.2378600

DNS-server

Last online: 19 seconds ago
Last offline: Monday at 14:51 (3 minutes)
Latency: 0.0009172

Free-Ipa

Last online: 19 seconds ago
Last offline: 5 hours ago (37 seconds)
Latency: 0.0020199

nube

Last online: 19 seconds ago
Last offline: 5 hours ago (8 minutes)
Latency: 0.3341658

soporte

Last online: 19 seconds ago
Last offline: Never
Latency: 0.1023371

web-server

Last online: 19 seconds ago
Last offline: 12 hours ago (1 minute)
Latency: 0.0006192

No es seguro | 172.24.133.199/phpservermon/?mod=server&action=view&id=6

Mi unidad - Google... YouTube Mediación Virtual:... GitLab UCR Iconos vectoriales g... VCL :: Virtual Comp... APA GENERATOR WhatsApp Personas en CompT... » Otros marcadores

Welcome, hellen ▾

SERVER MONITOR Status Servers Log Users Config Update

Servers

◀ Go back Edit

aula

Domain/IP: http://aula.quierogradsarme.com

Status: on

Latency: 0.7379 seconds

Status

Last online: a second ago

Last offline: Never

Last check: a second ago

Output

Last error: TIMEOUT ERROR: no response from server

Last positive output: HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 05:01:02 GMT Server: Apache/2.4.6 (CentOS) PHP/7.4.30 X-Powered-By: PHP/7.4.30 Set-Cookie: MoodleSession=bfa8mqfagavut31kf2l822e2f9; path=/ Expires: Mon, 20 Aug 1969 09:23:00 GMT Cache-Control: no-store, no-cac...

Show more...

Monitoring

Monitoring: ON

Email: OFF

SMS: OFF

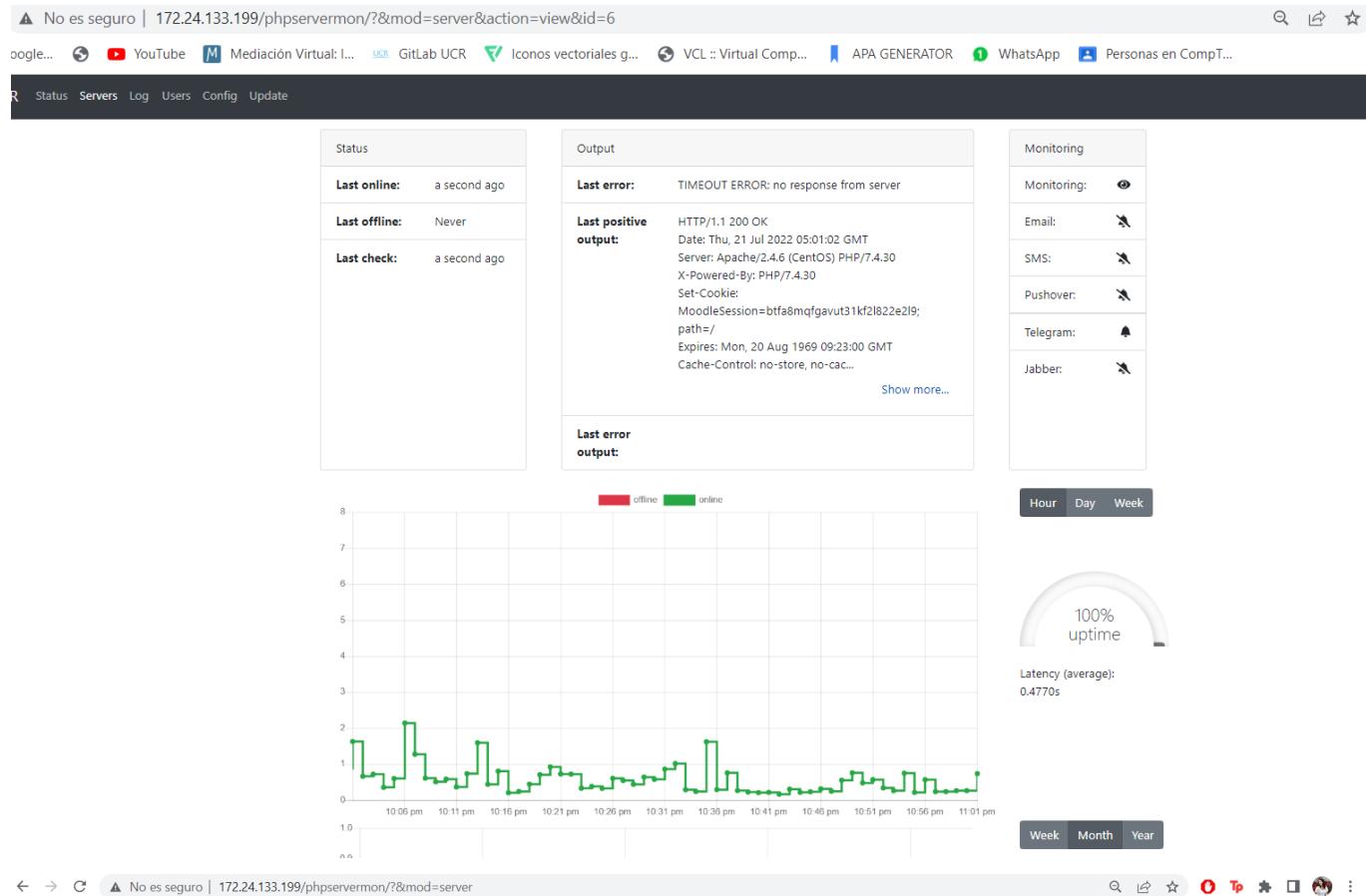
Pushover: OFF

Telegram: OFF

Jabber: OFF

Hour Day Week





No es seguro | 172.24.133.199/phpservermon/?&mod=server

Mi unidad - Google... YouTube Mediación Virtual: I... GitLab UCR Iconos vectoriales g... VCL :: Virtual Comp... APA GENERATOR WhatsApp Personas en CompT...

SERVER MONITOR Status Servers Log Users Config Update Welcome, hellen ▾

Servers

+ Add new Update

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