

VIRTUALIZACIÓN, CONFIGURACIÓN Y SEGURIDAD DE UN SERVIDOR



U0282978

Contenido

Introducción	3
ProxMox	3
¿Qué es ProxMox?	3
Instalación	3
Creación de la máquina virtual (OPCIONAL)	4
Instalación de ProxMox.....	4
Configuración	8
Ubuntu Server	17
¿Por qué Ubuntu Server?	17
Instalación	17
Apache.....	24
¿Qué es Apache?	24
Instalación	25
Configuración	25
Cloudflare	29
¿Qué es Cloudflare?	29
Configuración	30
Firewall	33
¿Qué es un Firewall?	33
Configuración	33
Extra	35
Bibliografía	35

Introducción

Este trabajo trata sobre la instalación de un hipervisor que permita virtualizar un servidor (en este caso usaremos mi propio equipo como tal) con Ubuntu Server y simular lo que sería un Servidor KVM. También crearemos una página web abierta a internet mediante Apache y mostraremos los riesgos existentes y herramientas que pueden ayudarnos a proteger el servidor como Cloudflare o UFW.

Proxmox

¿Qué es Proxmox?

Proxmox o (Proxmox Virtual Environment) es un hipervisor basado en la distribución de GNU/Linux Debian que permite virtualizar un equipo en varias partes con sus respectivos sistemas operativos deseados, al igual que permite virtualizar contenedores de Docker.

He decidido escoger esta herramienta debido a varias características que tiene, aunque la principal y más importante es que es de código abierto y gratuito frente a sus competidores como Hyper-V de Windows Server o VMware ESXi.

Aunque posee muchas más características interesantes:

- Es de código abierto
- Permite la migración en vivo
- Dispone de una alta habilitación de puentes de red
- Plantillas de construcción de SO
- Copias de seguridad programadas
- Herramientas de línea de comandos

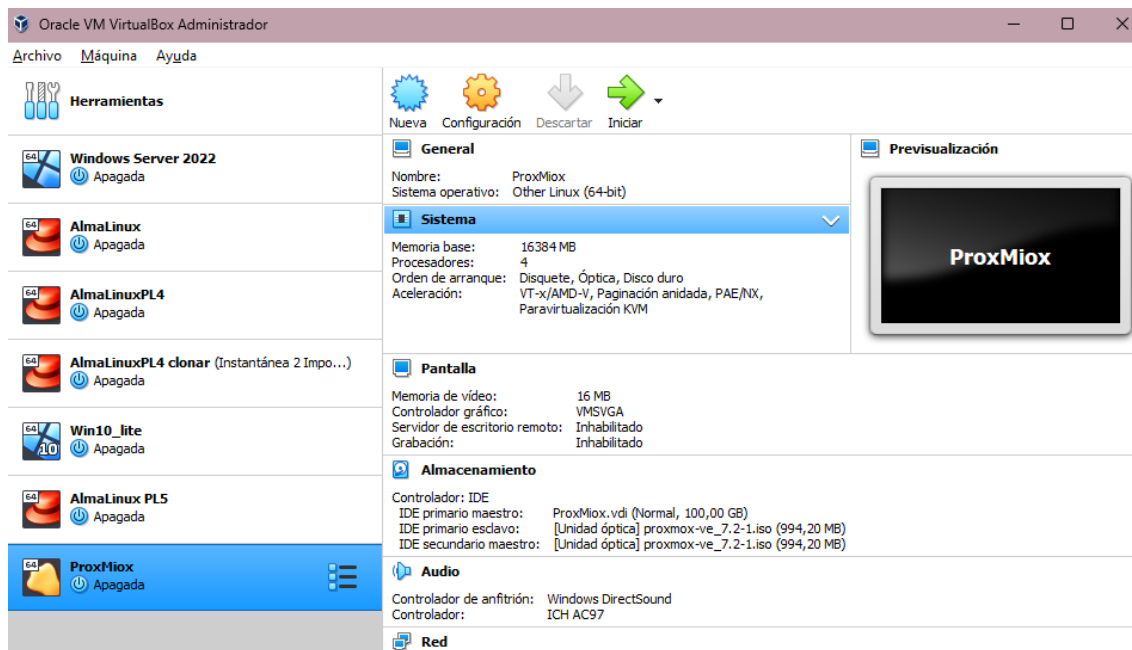
(Wikipedia, s.f.)

Instalación

Debido a que para este trabajo voy a usar mi equipo personal y no cuento con un equipo al que poder instalar Proxmox nativamente voy a virtualizarlo en Virtualbox y simularemos que es un equipo ya sea dedicado o un equipo que podemos tener por casa y darle un uso de servidor doméstico gracias a esta herramienta.

Creación de la máquina virtual (OPCIONAL)

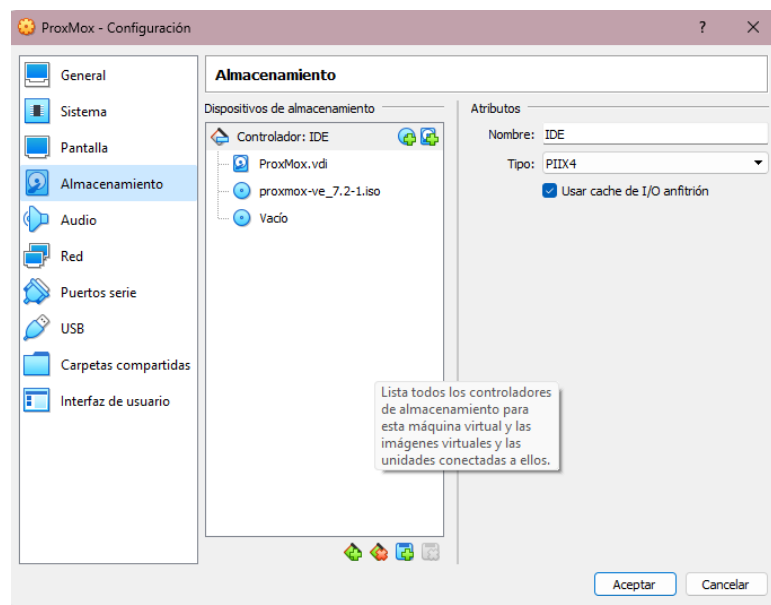
En este paso voy a crear la máquina virtual para poder virtualizar Proxmox, este paso sería opcional ya que podríamos disponer de un equipo y no sería necesario este paso.



Instalación de Proxmox

Procedemos a iniciar la instalación de Proxmox y explicarla paso a paso.

En caso de tratarse de un equipo real procederíamos a grabar la ISO de Proxmox en una memoria USB e insertarla al equipo para proceder a bootearla. Como en este caso estoy virtualizando Proxmox dentro de mi equipo con Windows 11 en Virtualbox procedería a añadir la imagen ISO como hemos ya hecho en la clase de prácticas de laboratorio.



Proxmox VE 7.2 (iso release 1) - <https://www.proxmox.com/>

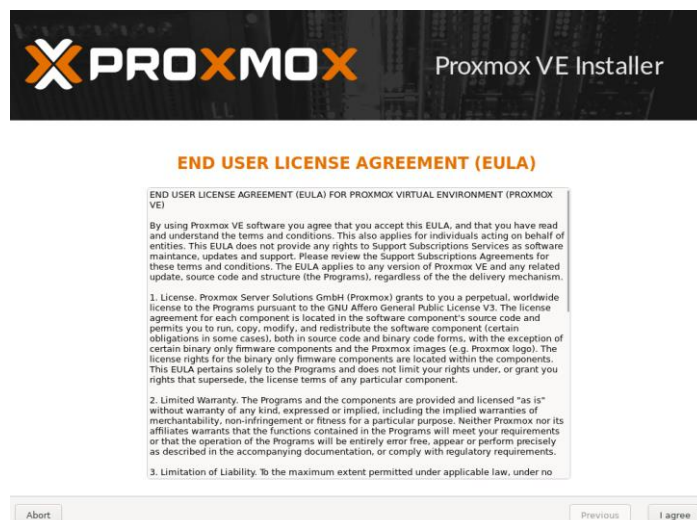


Welcome to Proxmox Virtual Environment

Install Proxmox VE
Advanced Options

enter: select, arrow keys: navigate, esc: back

Aquí tendríamos el menú de la ISO de Proxmox donde podemos escoger entre instalar Proxmox o abrir opciones avanzadas, en este caso procedemos a instalar Proxmox. En caso de querer saltar la explicación del proceso de instalación haga [click](#).



Primer paso de proceso de instalación, aceptar el EULA o Acuerdo de Licencia del Usuario Final.



Proxmox Virtual Environment (PVE)

The Proxmox Installer automatically partitions your hard disk. It installs all required packages and makes the system bootable from the hard disk. All existing partitions and data will be lost.

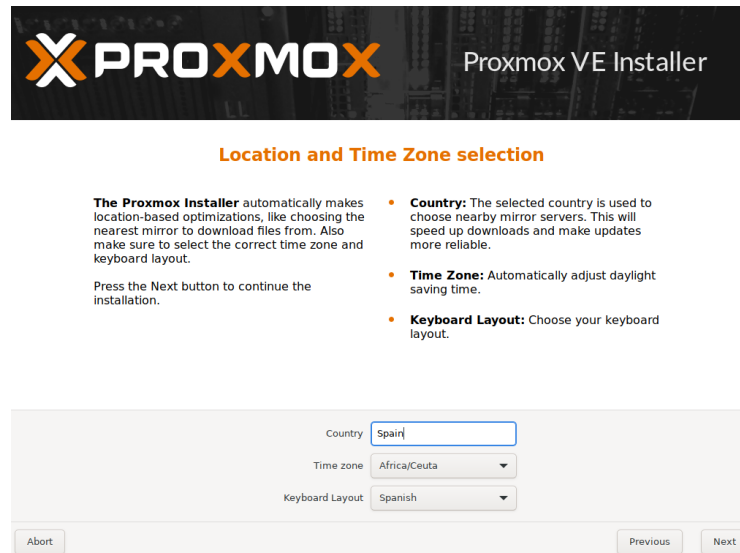
Press the Next button to continue the installation.

- Please verify the installation target**
The displayed hard disk will be used for the installation.
Warning: All existing partitions and data will be lost.
- Automatic hardware detection**
The installer automatically configures your hardware.
- Graphical user interface**
Final configuration will be done on the graphical user interface, via a web browser.

Target Harddisk: /dev/sda (40.00GiB, VBOX HARDDISK) Options

Abort Previous Next

Selección de disco para la instalación de ProxMox



Location and Time Zone selection

The Proxmox Installer automatically makes location-based optimizations, like choosing the nearest mirror to download files from. Also make sure to select the correct time zone and keyboard layout.

Press the Next button to continue the installation.

- Country:** The selected country is used to choose nearby mirror servers. This will speed up downloads and make updates more reliable.
- Time Zone:** Automatically adjust daylight saving time.
- Keyboard Layout:** Choose your keyboard layout.

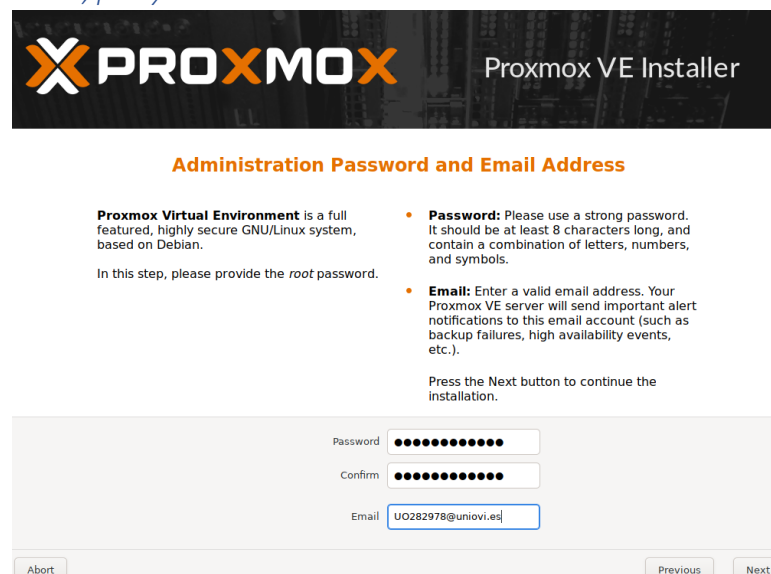
Country: Spain

Time zone: Africa/Ceuta

Keyboard Layout: Spanish

Abort Previous Next

Selección de zona horaria, país y distribución de teclado.



Administration Password and Email Address

Proxmox Virtual Environment is a full featured, highly secure GNU/Linux system, based on Debian.

In this step, please provide the *root* password.

- Password:** Please use a strong password. It should be at least 8 characters long, and contain a combination of letters, numbers, and symbols.
- Email:** Enter a valid email address. Your Proxmox VE server will send important alert notifications to this email account (such as backup failures, high availability events, etc.).

Press the Next button to continue the installation.

Password: ●●●●●●●●

Confirm: ●●●●●●●●

Email: UO282978@uniovi.es

Abort Previous Next

Creación de contraseña y vinculación de email.**Management Network Configuration**

Please verify the displayed network configuration. You will need a valid network configuration to access the management interface after installing.

After you have finished, press the Next button. You will be shown a list of the options that you chose during the previous steps.

- **IP address (CIDR):** Set the main IP address and netmask for your server in CIDR notation.
- **Gateway:** IP address of your gateway or firewall.
- **DNS Server:** IP address of your DNS server.

Management Interface: enp0s3 - 08:00:27:f0:7f:8e (e1000) ▼

Hostname (FQDN): pve.example.example

IP Address (CIDR): 192.168.0.14 / 24

Gateway: 192.168.0.1

DNS Server: 212.142.173.64

Buttons: Abort, Previous, Next

Configuración de red y conectividad a interfaz web**Summary**

Please confirm the displayed information. Once you press the **Install** button, the installer will begin to partition your drive(s) and extract the required files.

Option	Value
Filesystem:	ext4
Disk(s):	/dev/sda
Country:	Spain
Timezone:	Africa/Ceuta
Keymap:	es
Email:	UO282978@uniovi.es
Management Interface:	enp0s3
Hostname:	pve
IP CIDR:	192.168.0.14/24
Gateway:	192.168.0.1
DNS:	212.142.173.64

☒ Automatically reboot after successful installation

Buttons: Abort, Previous, Install

Detalles finales de la instalación



Virtualization Platform

Open Source Virtualization Platform

- Enterprise ready
- Central Management
- Clustering
- Online Backup solution
- Live Migration
- 32 and 64 bit guests

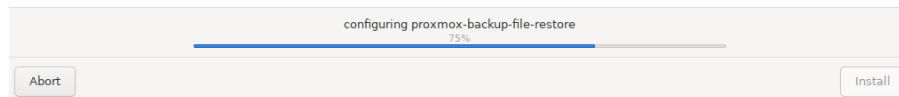
Visit www.proxmox.com for additional information and the Wiki about Proxmox VE.

Container Virtualization

Only 1-3% performance loss using OS virtualization as compared to using a standalone server.

Full Virtualization (KVM)

Run unmodified virtual servers - Linux or Windows.



Proceso de Instalación

Instalación terminada.



Installation successful!

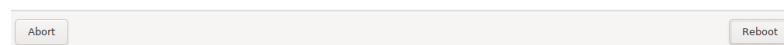
Proxmox VE is now installed and ready to use.

Next steps

Reboot and point your web browser to the selected IP address on port 8006:

<https://192.168.0.14:8006>

Also visit www.proxmox.com for more information.



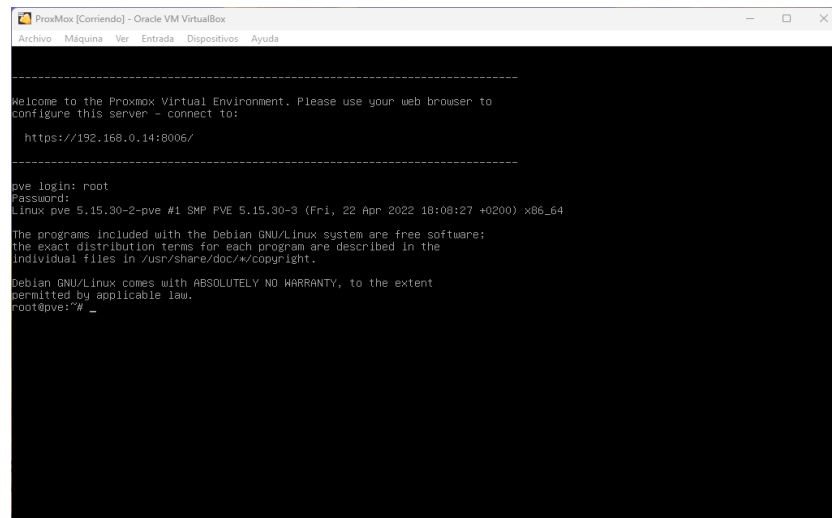
Instalación terminada, hay que destacar que señala que reiniciemos el equipo y nos conectemos vía http por un navegador a 192.168.0.14 y puerto 8006.

Esta IP sería la IP local de la máquina donde instalamos Proxmox y el puerto el asignado a la interfaz web de Proxmox.

Configuración

Una vez ya instalado Proxmox procederíamos a desconectar del equipo el USB con la ISO o bien en VirtualBox la propia ISO.

Arrancaríamos el equipo e iniciaríamos sesión con root y la contraseña introducida durante la instalación.



```
Proxmox [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

-----
Welcome to the Proxmox Virtual Environment. Please use your web browser to
configure this server - connect to:

https://192.168.0.14:8006/

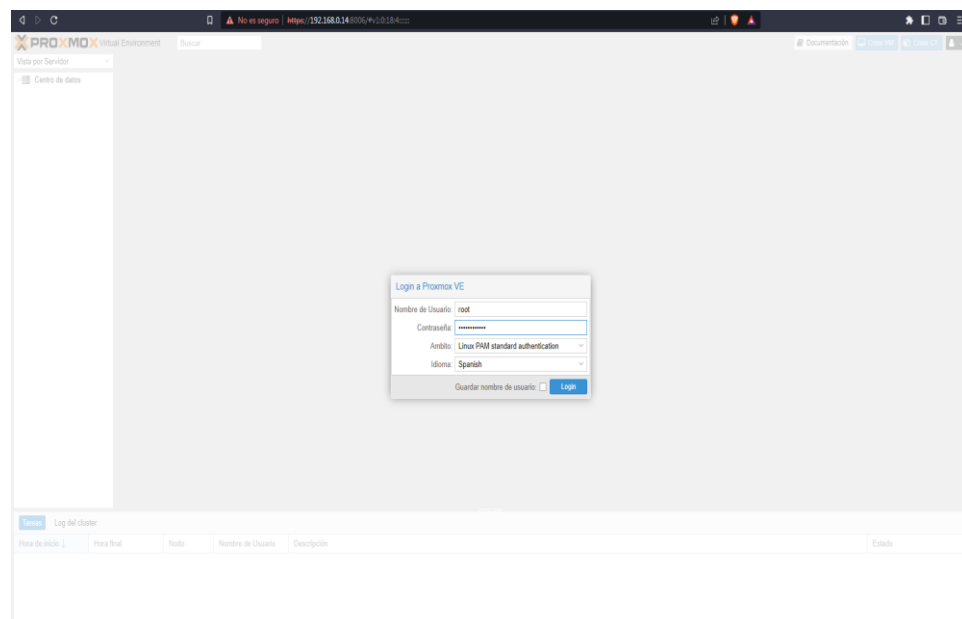
-----

pve login: root
Password:
Linux pve 5.15.30-2-pve #1 SMP PVE 5.15.30-3 (Fri, 22 Apr 2022 10:08:27 +0200) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@pve:~# _
```

Como podemos observar nos indica una IP y puerto al que conectarnos mediante el navegador.



Iniciaríamos sesión como en el servidor con el usuario root y la contraseña.

Proxmox Virtual Environment 7.2-3

Centro de datos

Tipo	Descripción	Uso de dis...	Memoria - ...	Uso de CPU	Tiempo de uso	Host CPU ...	Host Mem...
node	pve	26.1 %	8.4 %	0.6% of 4 ...	00:09:42		
storage	local (pve)	26.1 %					
storage	local-lvm (pve)	0.0 %					

Tareas Log del cluster

Hora de inicio	Hora final	Nodo	Nombre de Usuario	Descripción	Estado
Nov 07 23:04:35	Nov 07 23:04:35	pve	root@pam	Inicio de todas las VMs y Contenedores	OK

Aquí tendríamos el panel de Proxmox con todas las opciones que tiene.

En caso de estar interesado en leer el manual de administración hacer [click](#).

Allí se explicaría el proceso de instalación en más profundidad al igual que muchas más opciones, aun así, me centrare en mostrar las opciones que vamos a usar y más importantes procediendo a virtualizar una nueva máquina con Ubuntu Server.

Para poder crear una nueva máquina primero debemos cargar una ISO en la propia máquina.

Proxmox Virtual Environment 7.2-3

Almacenamiento 'local' en el nodo 'pve'

Resumen

Backups

ISO Images

CT Templates

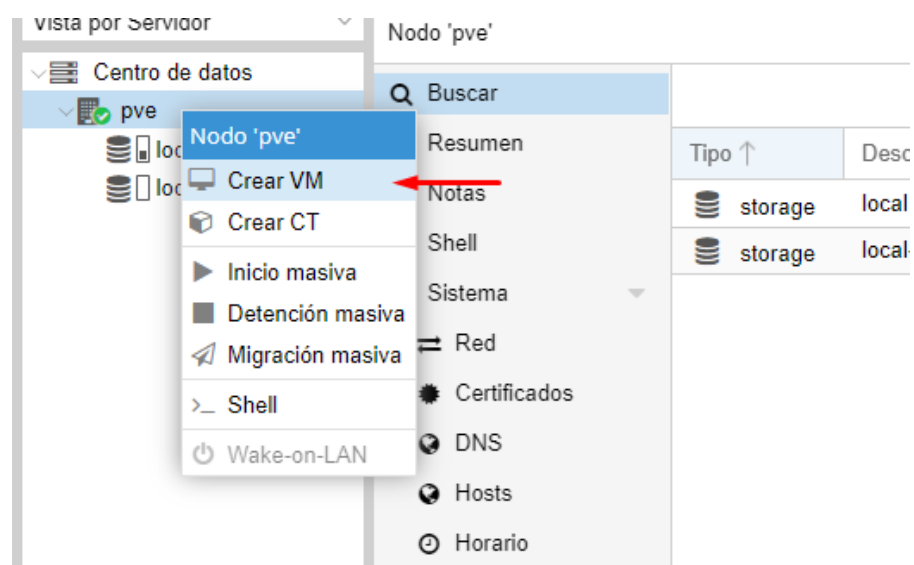
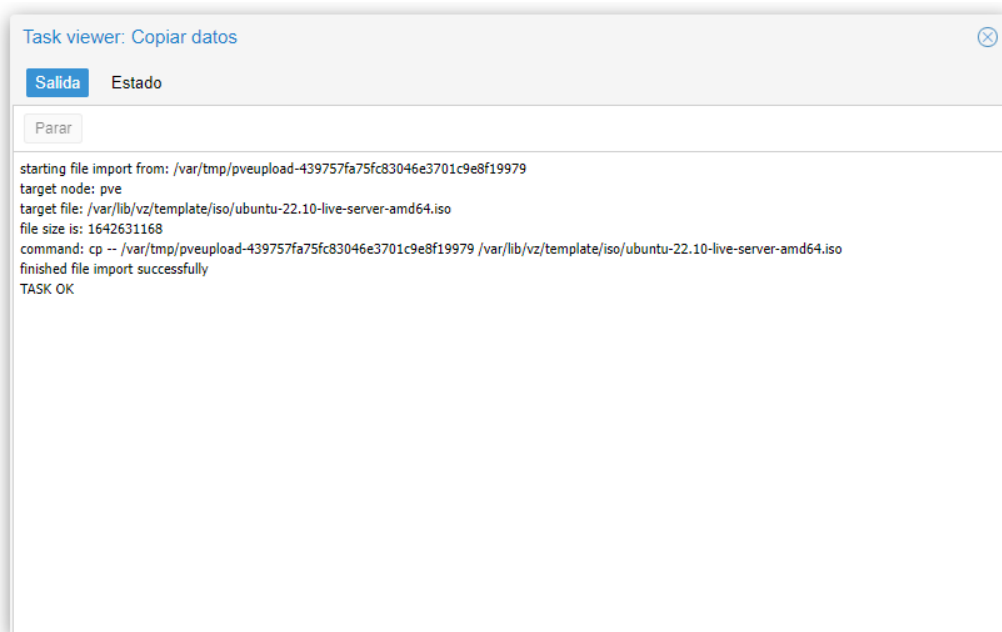
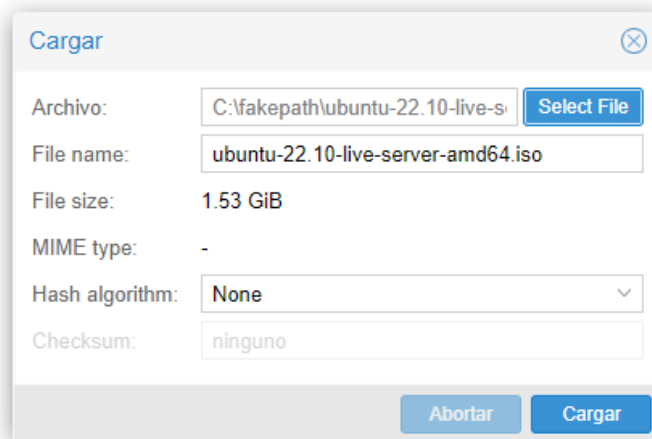
Permisos

Cargar

Download from URL

Eliminar

Nombre



Crear: Máquina Virtual

General SO Sistema Discos CPU Memoria Red Confirmar

Nodo: pve Conjunto de Recursos:

VM ID: 100

Nombre: UbuntuServer

Ayuda Avanzado ☐ Atrás Siguiente

Crear: Máquina Virtual

General SO Sistema Discos CPU Memoria Red Confirmar

☒ Usar imagen de disco (ISO) de CD/DVD : Sistema operativa guest:

Almacenamiento: local Tipo: Linux

Imagen ISO: Imagen ISO: Versión: 5.x - 2.6 Kernel

☐ Usar lector físico

☐ No usar ningún

Nombre	For...	Tamaño
ubuntu-22.10-live-server-amd64.iso	iso	1.64 GB

Avanzado ☐ Atrás Siguiente

Crear: Máquina Virtual

General SO **Sistema** Discos CPU Memoria Red Confirmar

Tarjeta gráfica: Por defecto

Machine: Por defecto (i440fx)

Firmware

BIOS: Por defecto (SeaBIOS)

Controlador SCSI: VirtIO SCSI

Qemu Agent: ☐

Add TPM: ☐

Ayuda Avanzado ☐ Atrás Siguiente

Crear: Máquina Virtual

General SO Sistema **Discos** CPU Memoria Red Confirmar

scsi0

Disco Bandwidth

Bus/Dispositivo: SCSI 0

Caché: Por defecto (No hay)

Controlador SCSI: VirtIO SCSI

Descartar: ☐

Almacenamiento: local-lvm

Tamaño de disco (GiB): 10

Formato: Imagen de disco RAW

Agregar

Ayuda Avanzado ☐ Atrás Siguiente

Crear: Máquina Virtual

General

SO

Sistema

Discos

CPU

Memoria

Red

Confirmar

Sockets:

1

Tipo:

Por defecto (kvm64)

Núcleos:

1

Total de Núcleos:

1

Ayuda

Avanzado ☐

Atrás

Siguiente

Crear: Máquina Virtual

General

SO

Sistema

Discos

CPU

Memoria

Red

Confirmar

Memoria (MiB):

2048

Ayuda

Avanzado ☐

Atrás

Siguiente

Crear: Máquina Virtual

GeneralSO Sistema Discos CPU Memoria **Red** Confirmar

☐ Sin dispositivo de red

Puente:

Modelo:

Etiqueta VLAN:

Dirección MAC:

Cortafuego: ☒

Ayuda

Avanzado ☐

Atrás

Siguiente

Crear: Máquina Virtual

GeneralSO Sistema Discos CPU Memoria Red **Confirmar**

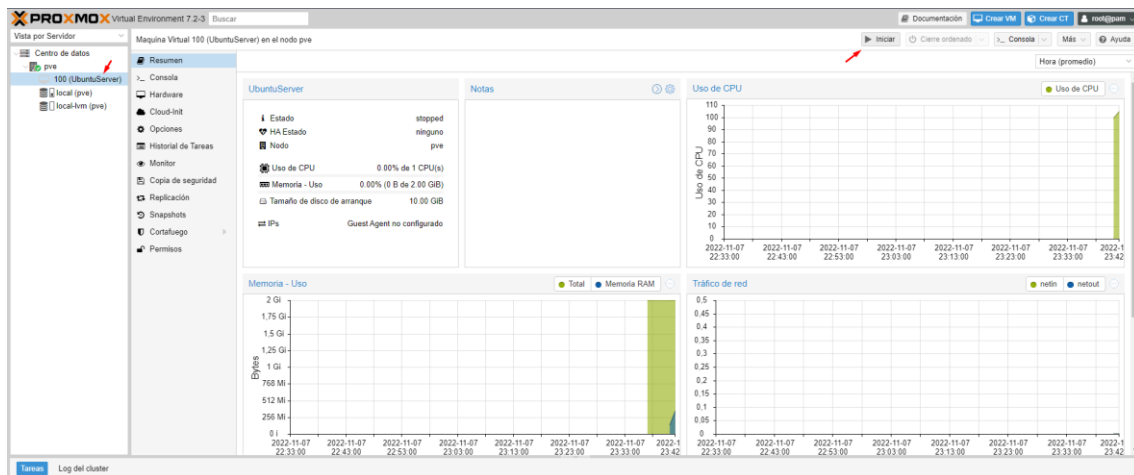
Key ↑	Value
cores	1
ide2	local:iso/ubuntu-22.10-live-server-amd64.iso,media=cdrom
memory	2048
name	UbuntuServer
net0	virtio,bridge=vmbr0,firewall=1
nodename	pve
numa	0
ostype	l26
scsi0	local-lvm:10
scsihw	virtio-scsi-pci
sockets	1
vmid	100

☐ Start after created

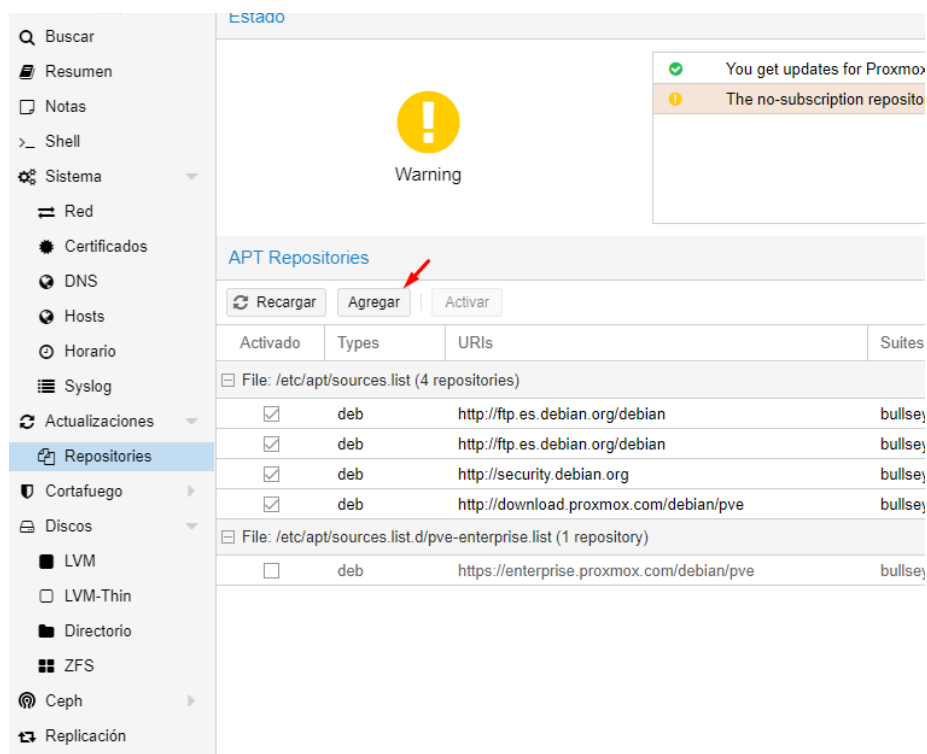
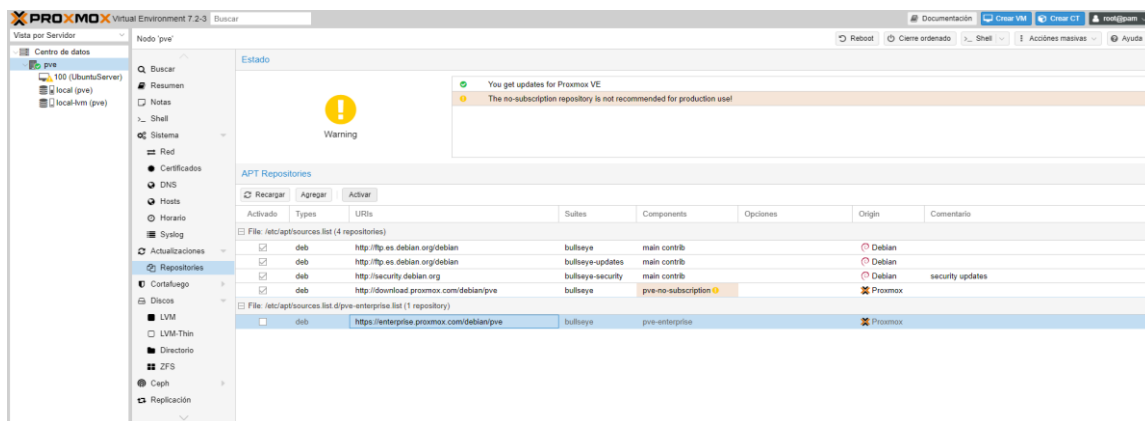
Avanzado ☐

Atrás

Finalizar



Por defecto Proxmox tiene repositorios de suscripción mientras que nosotros no tenemos. Así que debemos añadirnos un repositorio de tipo “No suscripción” e inhabilitar el de tipo suscripción.



Agregar: Repository

Repository: No-Subscription

Descripción: This is the recommended repository for testing and non-production use. Its packages are not as heavily tested and validated as the production ready enterprise repository. You don't need a subscription key to access this repository.

Estado: Configured: enabled

Ayuda

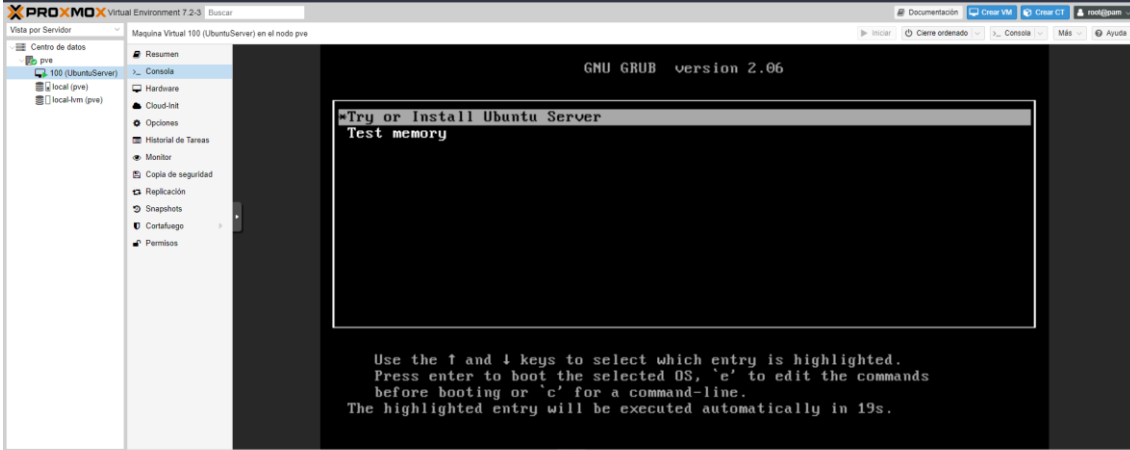
Agregar

Ubuntu Server

¿Por qué Ubuntu Server?

No es obligatorio usar Ubuntu Server, perfectamente podríamos usar por ejemplo tanto la versión minimal como la del servidor con interfaz de usuario de AlmaLinux. En este caso he decidido usar Ubuntu Server debido a que es una de las distribuciones de Linux más utilizadas.

Instalación



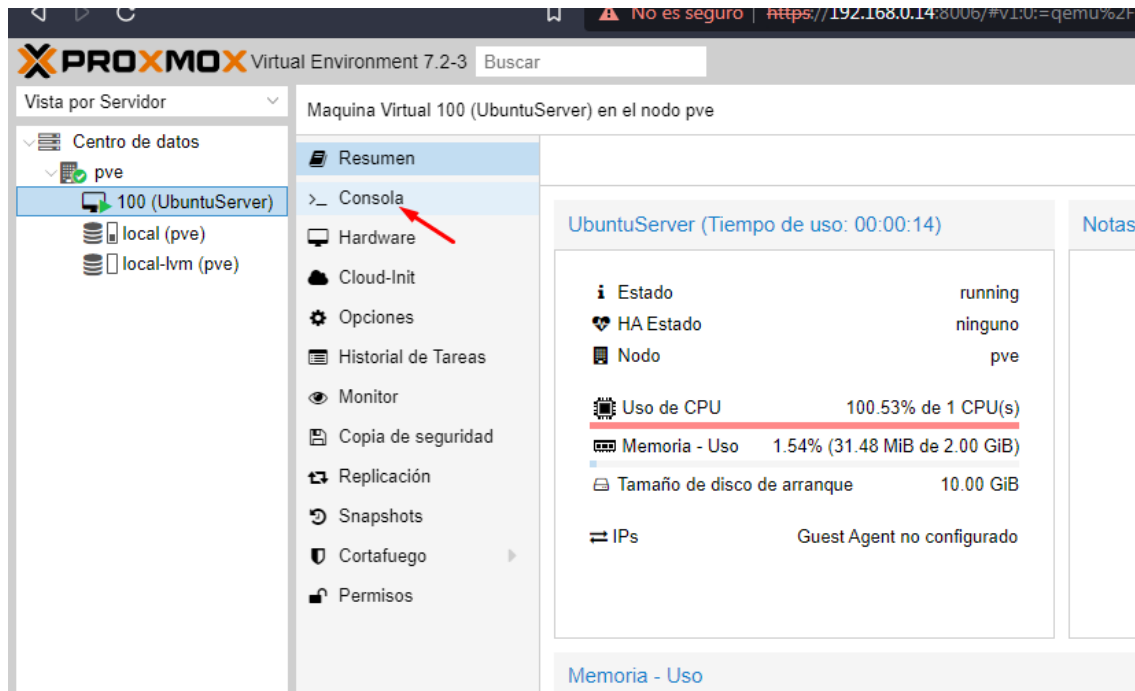
GNU GRUB version 2.06

Try or install Ubuntu Server

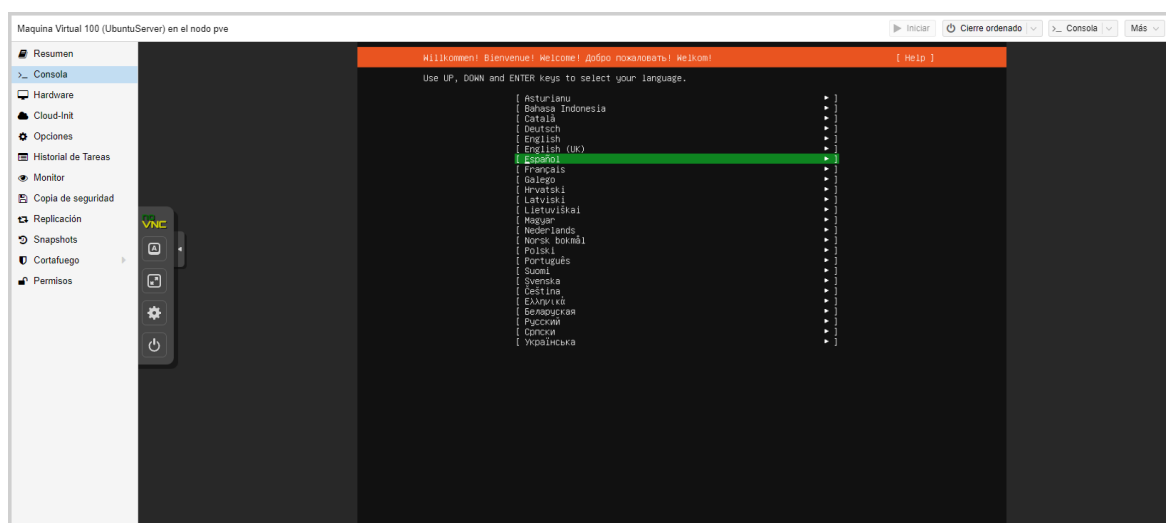
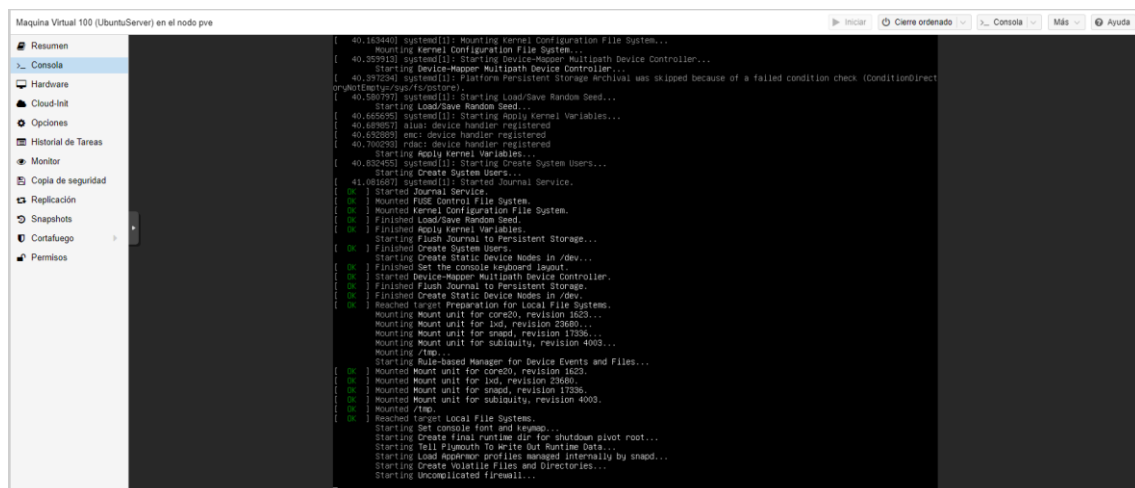
Test memory

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands before booting or 'c' for a command-line.
The highlighted entry will be executed automatically in 19s.

Tareas						
Log del cluster	Hora de inicio	Hora final	Nodo	Nombre de Usuario	Descripción	Estado
	Nov 07 23:40:00		pve	root@pam	VMCT 100 - Console	
	Nov 07 23:39:56	Nov 07 23:39:56	pve	root@pam	VM 100 - Iniciar	OK
	Nov 07 23:39:31	Nov 07 23:39:31	pve	root@pam	Inicio de todas las VMs y Contenedores	OK
	Nov 07 23:35:44	Nov 07 23:35:44	pve	root@pam	VM 100 - Iniciar	Error: KVM virtualisation con...
	Nov 07 23:35:36	Nov 07 23:35:37	pve	root@pam	VM 100 - Crear	OK

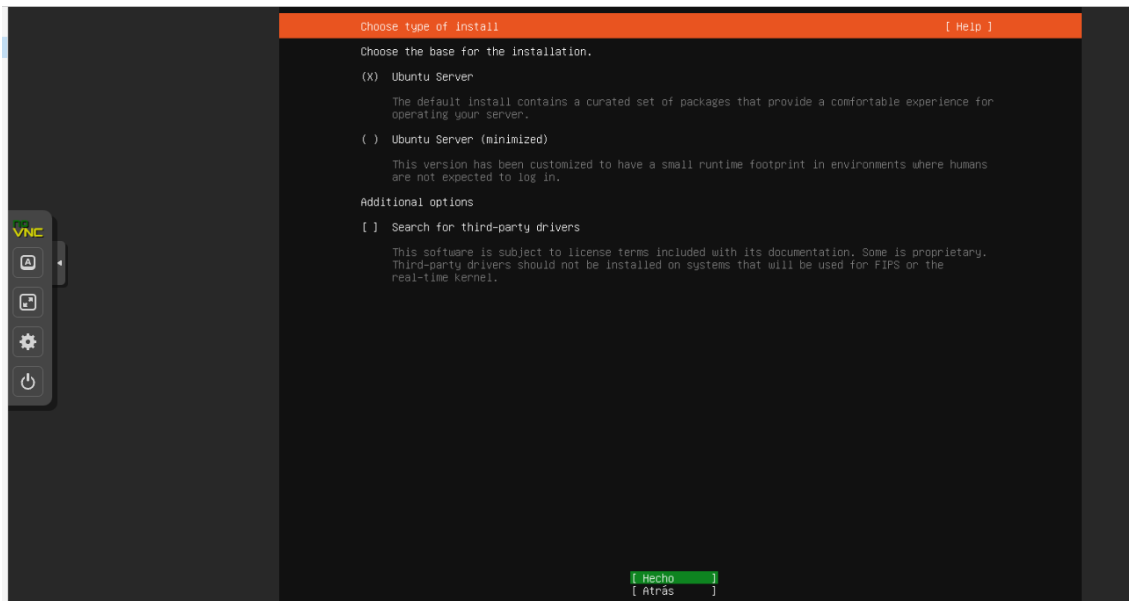


- Si deseas saltar la parte de instalación de Ubuntu Server haz [click](#).

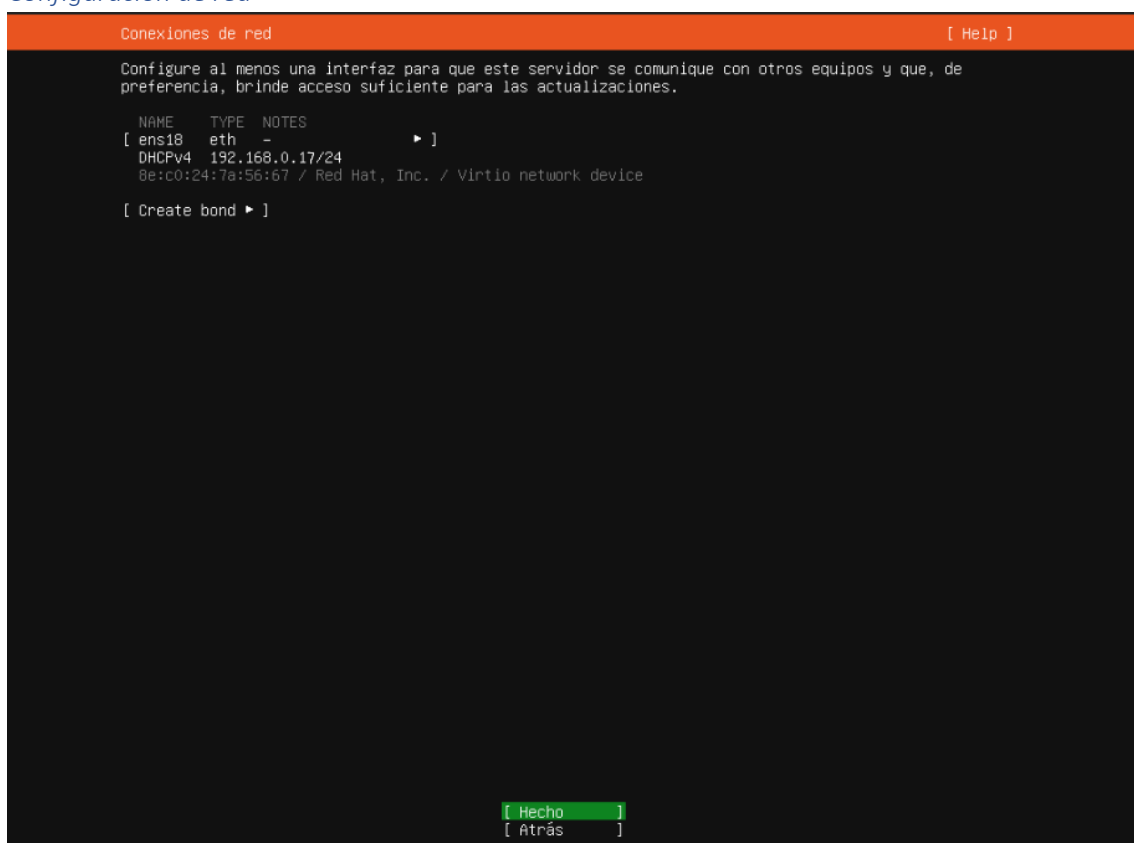


Menú de selección de idioma

Selección de instalación



Configuración de red



Configurar conexión Proxy

Configure proxy

[Help]

If this system requires a proxy to connect to the internet, enter its details here.

Proxy address:

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of "http://[[user] [:pass]@]host[:port]/".

[Hecho]

[Atrás]

Configurar mirror descargas

Configure Ubuntu archive mirror

[Help]

If you use an alternative mirror for Ubuntu, enter its details here.

Mirror address:

You may provide an archive mirror that will be used instead of the default.

[Hecho]

[Atrás]

Configuración almacenamiento

Guided storage configuration

[Help]

Configure a guided storage layout, or create a custom one:

(X) Use an entire disk

[0QEMU_QEMU_HARDDISK_drive-scsi0 local disk 10.000G ▼]

[X] Set up this disk as an LVM group

[] Encrypt the LVM group with LUKS

Passphrase:

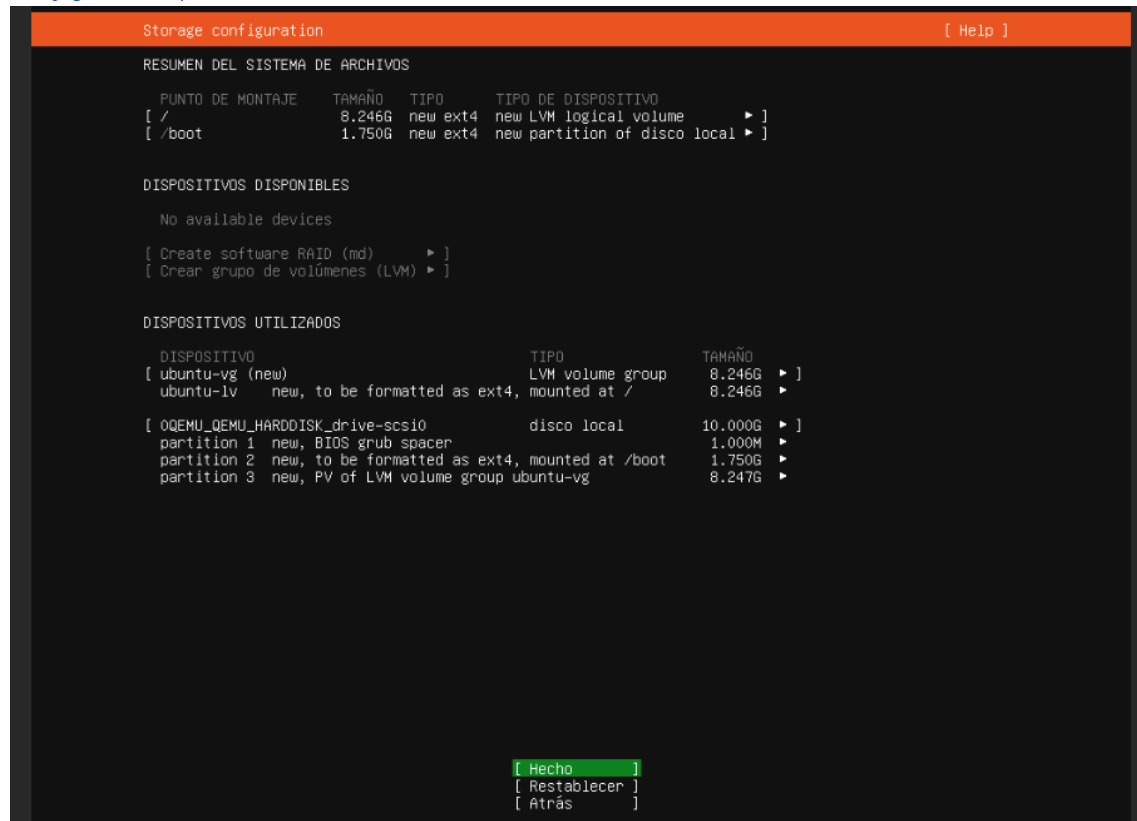
Confirm passphrase:

() Custom storage layout

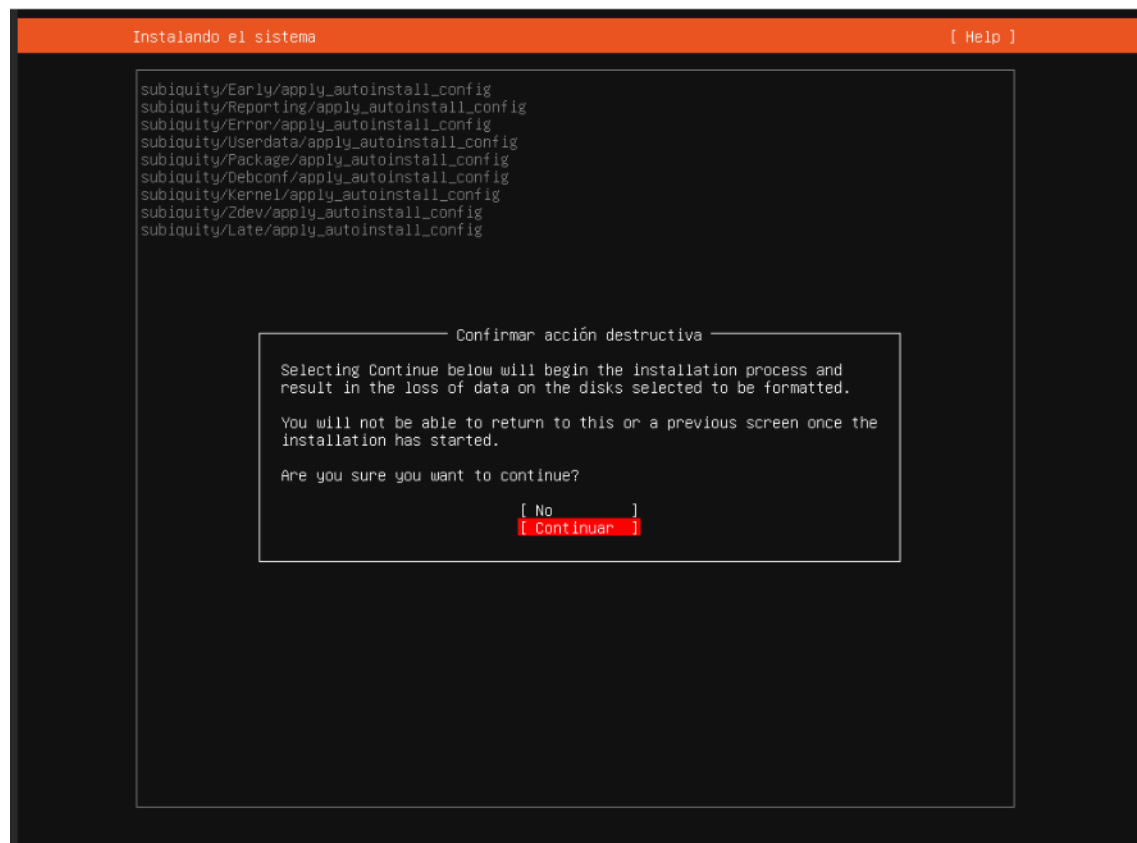
[Hecho]

[Atrás]

Configuración particiones



Instalación del sistema



Configuración perfil usuario

Configuración de perfil

[Help]

Proporcione el nombre de usuario y la contraseña que utilizará para acceder al sistema. Puede configurar el acceso SSH en la pantalla siguiente, pero aun se necesita una contraseña para sudo.

Su nombre:

El nombre del servidor:
The name it uses when it talks to other computers.

Elija un nombre de usuario:

Elija una contraseña:

Confirme la contraseña:

[Hecho]

Configuración SSH

Configuración de SSH

[Help]

You can choose to install the OpenSSH server package to enable secure remote access to your server.

☒ Instalar servidor OpenSSH

Importar identidad SSH:
You can import your SSH keys from GitHub or Launchpad.

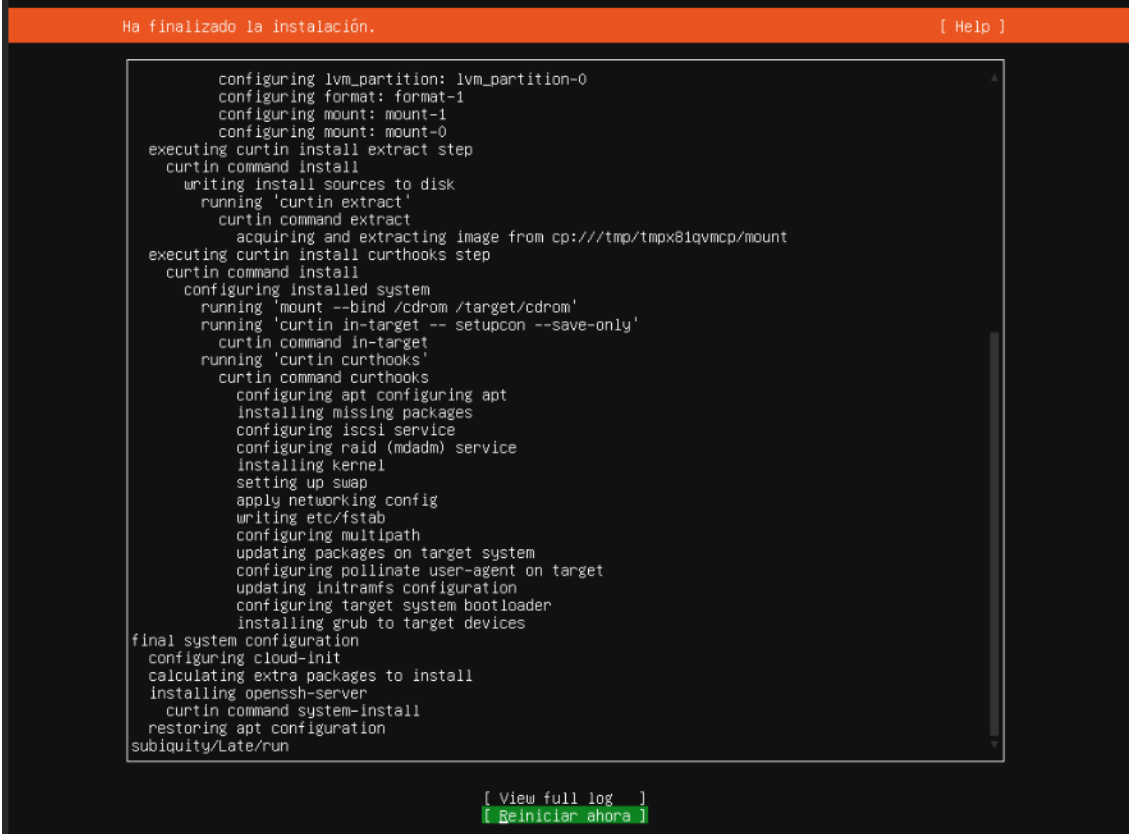
Importar nombre de usuario:

☒ Permitir autenticación con contraseña por SSH

[Hecho]

[Atrás]

Instalación terminada



```
Ha finalizado la instalación. [ Help ]

configuring lvm_partition: lvm_partition-0
configuring format: format-1
configuring mount: mount-1
configuring mount: mount-0
executing curtin install extract step
curtin command install
writing install sources to disk
running 'curtin extract'
curtin command extract
acquiring and extracting image from cp:///tmp/tmpx81qvmcp/mount
executing curtin install curthooks step
curtin command install
configuring installed system
running 'mount --bind /cdrom /target/cdrom'
running 'curtin in-target -- setupcon --save-only'
curtin command in-target
running 'curtin curthooks'
curtin command curthooks
configuring apt configuring apt
installing missing packages
configuring iscsi service
configuring raid (mdadm) service
installing kernel
setting up swap
apply networking config
writing etc/fstab
configuring multipath
updating packages on target system
configuring pollinate user-agent on target
updating initramfs configuration
configuring target system bootloader
installing grub to target devices
final system configuration
configuring cloud-init
calculating extra packages to install
installing openssh-server
curtin command system-install
restoring apt configuration
subiquity/Late/run

[ View full log ]
[ Reiniciar ahora ]
```

Apache

¿Qué es Apache?

Apache es un servidor web HTTP de código abierto (posiblemente el más usado)

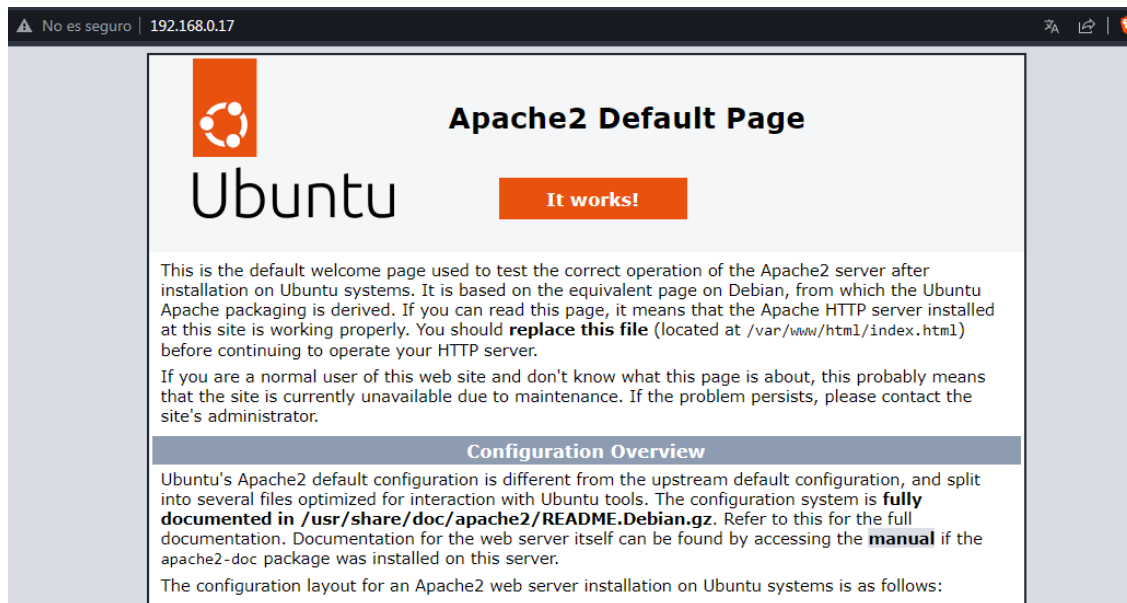
Tiene alternativas como Nginx, al final he decidido usar Apache porque es el más usado y con más información y documentación.

Instalación

En el caso de Ubuntu pondríamos el comando:

```
sudo apt install apache2
```

Una vez instalado apache procederíamos a observar que funciona apache en el navegador de nuestro ordenador conectándonos a la IP Local del servidor.



Configuración

Como podemos observar está funcionando Apache en el puerto 80 que es el por defecto para HTTP (esta información nos será más útil más tarde cuando configuremos el firewall).

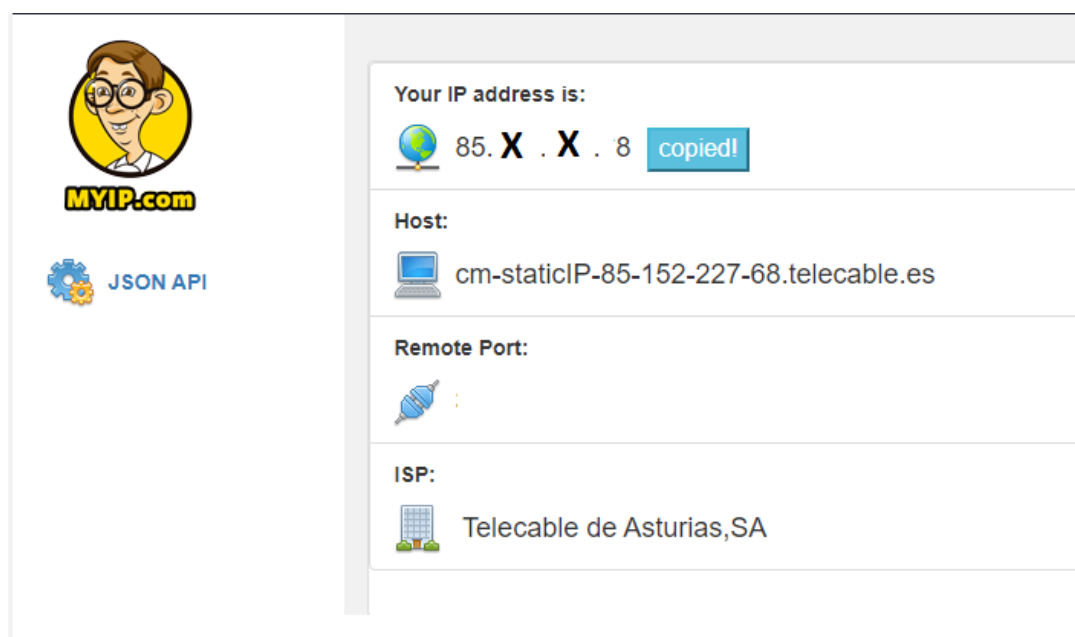
De momento la web está abierta solo a nivel local pues en la red de mi casa donde estoy ahora mismo no tengo abierto el puerto 80, por defecto si esto se tratara de un servidor alquilado de un hosting ya contaríamos con la IP Publica para conectarnos por FTP o SSH y normalmente ya tendríamos al instalar Apache nuestra página web abierta a todo el mundo.

Como estoy en mi casa voy a abrir el puerto 80 conectándome a mi router (normalmente están asignados a la IP 192.168.0.1 y tienen un panel de inicio de sesión donde por defecto tienen como contraseña y usuario "admin").



Una vez abierto el puerto 80 miraríamos cual es nuestra IP Pública.

Existen muchas webs para comprobar nuestra IP Pública como la que estoy usando ahora mismo: myip.com



Por razones de privacidad y seguridad he censurado mi IP Pública sobre todo porque es un dato que no siempre nos gustaría que fuera accesible para todo el mundo y eso mismo es algo que vamos a corregir ahora mismo.

Ahora que el servidor (al menos el puerto 80) está abierto a internet y por tanto la gente ya tiene acceso a nuestra web y una buena práctica es definir un archivo ".htaccess", archivo que reconoce Apache donde podemos por ejemplo definir el acceso de los usuarios a un directorio dentro de donde se ubicaría la página web "/var/www".

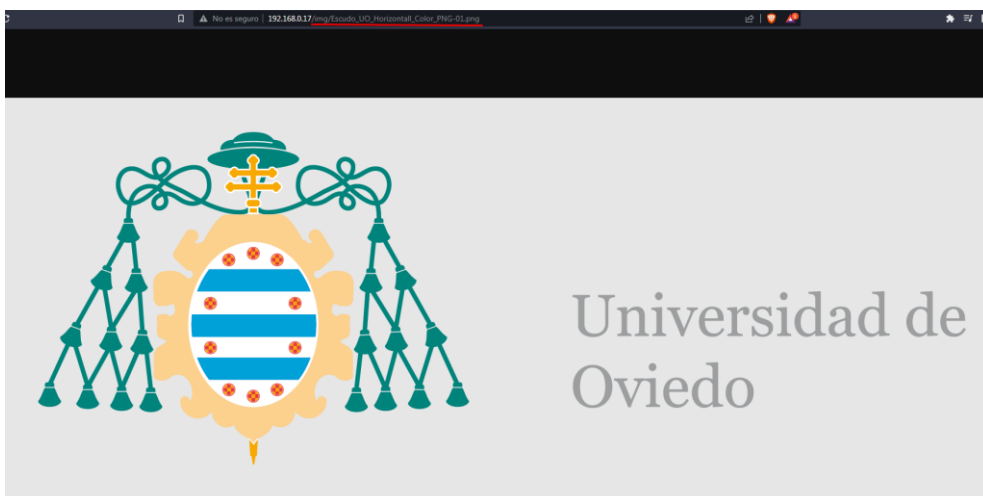
Para ilustrar un ejemplo evidente he modificado ligeramente la web por defecto de Apache añadiendo una foto de la Universidad de Oviedo para ilustrar un ejemplo del uso de un archivo “.htaccess”.



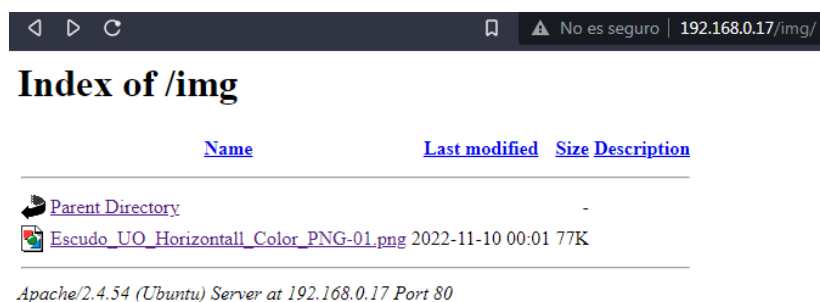
Supongamos que esta imagen es una imagen de nuestra propia web.

Esta imagen se ubica en un directorio dentro de “/var/www/html” llamado “img”.

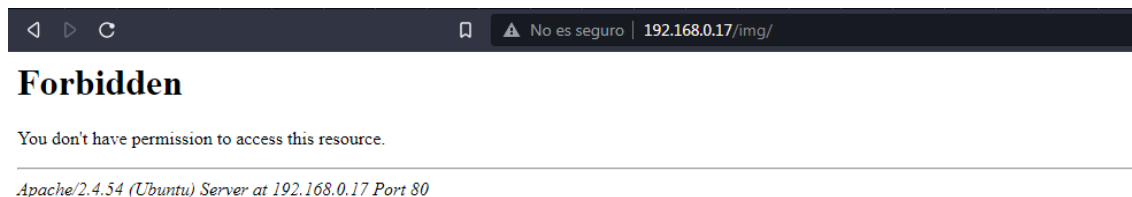
Veremos qué pasa si abro la imagen...



Como podemos observar podemos ver el directorio en el que se encuentra y que pasa si borramos la parte del path de la imagen...



Apache nos muestra lo que se ubica en ese directorio (cabe decir que solo mostraría lo que está en `"/var/www"`. Pero al no existir un archivo `".htaccess"` que defina el acceso a los directorios Apache los muestra como visibles, veamos qué pasa si creamos un archivo `".htaccess"`...



Ya no se podría acceder a los directorios dentro de `"/var/www"`.

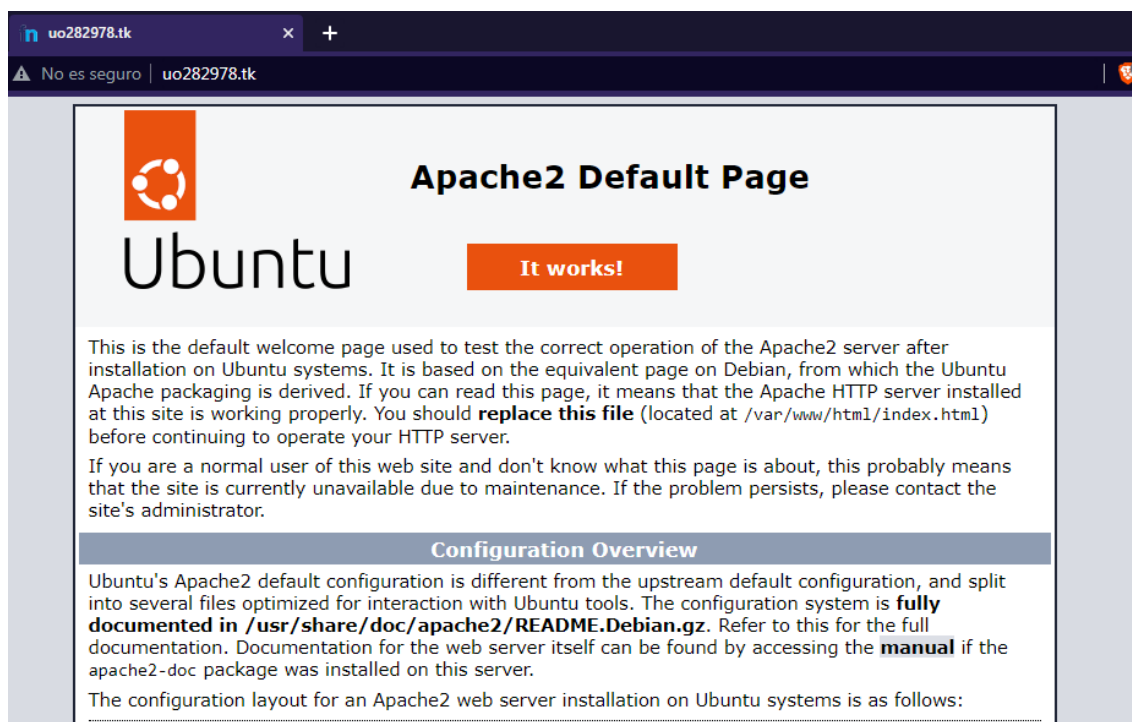
Retomando el tema de las direcciones IP, lo normal cuando nos conectamos a una página web es no memorizamos ni conectarnos por su dirección IP Pública para acceder a ella, sino que accedemos mediante un dominio (ej google.com).

Eso mismo vamos a hacer ahora, para ello he registrado un dominio gratuito .tk

El dominio sería uo282978.tk

Domain	Registration Date	Expiry date	Status	Type	
uo282978.tk	2022-11-09	2023-11-09	ACTIVE	Free	Manage Domain

Ahora habría que configurar las DNS del dominio para que apunten a mi IP Pública, aunque ya explicare más tarde que faltaría por configurar para protegernos y que grave error va a exponer nuestra IP a todo el mundo.



Ya tenemos el dominio apuntando a nuestra IP Pública entonces haciendo ping podemos comprobar como estaríamos accediendo a nuestra IP Pública

GeoIP2 Databases Demo

Show Sidebar >

IP Addresses

85. **X.X.** 8

Enter up to 25 IP addresses separated by spaces or commas. You can also [test your own IP address](#).

Submit

GeoIP2 City Plus Database Results

IP Address	Country Code	Location	Network	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
85. X.X. 8	ES	Oviedo, Asturias, Principality of Asturias, Spain, Europe	85. [redacted]	33006	43.3615, -5.8499	5	Telecable	Telecable	telecable.es	

Y con un poco de imaginación podríamos sacar la ubicación de dicha IP y hacer muchas más cosas que suponen un riesgo como un ataque DDOS, la posibilidad de que alguien trate de conectarse por SSH o FTP a nuestro equipo, buscar puertos abiertos con la herramienta “nmap” y buscar vulnerabilidades...

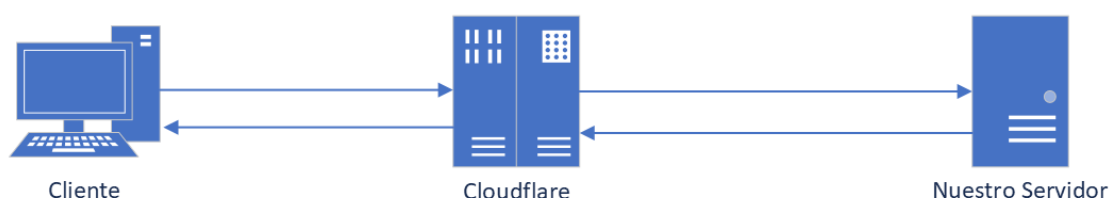
Por eso mismo existen herramientas como Cloudflare que es gratuita para particulares, la cual protegerá nuestra IP Pública haciendo que el cliente en vez de conectarse directamente al servidor pase antes por un servidor de Cloudflare el cual hará de intermediario.

Cloudflare

¿Qué es Cloudflare?

Cloudflare es un sistema gratuito para particulares que funciona como intermediario entre las conexiones del cliente-servidor, protegiendo así su IP y mejorando su velocidad debido a que almacena temporalmente contenido estático del sitio web almacenado en el servidor.

Video cloudflare: [¿Qué es Cloudflare?](#)



Entonces todo el tráfico que vaya dirigido hacia nuestro sitio web pasara por Cloudflare por tanto cuando alguien haga ping a nuestra web o utilice otras herramientas con fines mal intencionado nos veremos protegidos. Además, Cloudflare protege nuestra web contra ataques DDOS y bots.

Configuración

Inicio

Buscar sitios web en Juan... :gmail.com's Account...

Q

rufas.dev
✓ Activo

rufas.info
✓ Activo

Este sería el panel de Cloudflare donde yo ya cuento con dos páginas webs que tengo protegidas, para añadir una haríamos click sobre el botón señalado.

Seleccione un plan para **uo282978.tk** Mensual ☒ Anual

Pro

20 US\$ POR MES

Para los sitio web profesionales que no son críticos para la empresa.

Características básicas
 Todo lo que incluye el plan Free, más:

- ✓ Seguridad mejorada con WAF (firewall de aplicaciones web)
- ✓ Optimización de imagen sin pérdida
- ✓ Optimización móvil automática
- ✓ Cache Analytics
- ✓ Mitigación de bot más avanzada

20 Reglas de página

Soporte
 Correo electrónico. Normalmente en un plazo de 4 horas.

Business

200 US\$ POR MES

Para pequeñas empresas que operan en línea.

Características básicas
 Todo lo que incluye el plan Pro, más:

- ✓ SLA de 100 % de tiempo de actividad
- ✓ Soporte por chat las 24 horas, los 7 días de la semana, los 365 días del año
- ✓ Cumplimiento con la norma PCI DSS 3.2
- ✓ Compatibilidad con la configuración de CNAME
- ✓ Mitigación sofisticada de bot
- ✓ Personalizado + traer su propio SSL

50 Reglas de página

Soporte
 Chat, más correo electrónico; normalmente en un plazo de 2 horas.

Enterprise

Personalizado

Para aplicaciones críticas que son fundamentales para la empresa.

Características básicas
 Todo lo que incluye el plan Business, más:

- ✓ Intervalos IP priorizados
- ✓ Soporte técnico del ingeniero de soluciones
- ✓ Tiempo de actividad de 25x de reembolso de SLA
- ✓ Acceso a la cuenta por rol
- ✓ Mitigación para todos los bots
- ✓ Acceso ilimitado a pruebas

125 Reglas de página

Soporte
 Correo electrónico, chat y teléfono las 24 horas, los 7 días de la semana, los 365 días del año.

Free

0 US\$

Soporte
 Documentos para los desarrolladores y la comunidad.

Para proyectos personales o de pasatiempos que no son críticos para la empresa.

- ✓ DNS rápido y fácil de usar
- ✓ Protección contra DDoS no medidas
- ✓ CDN global

- ✓ Certificado SSL universal
- ✓ Conjunto de reglas administrado gratis
- ✓ Mitigación simple de bot
- ✓ Soporte de la comunidad

3 Reglas de página

[¿Qué plan es el adecuado para usted?](#)

Elegiríamos en nuestro caso el plan gratuito.

Configuraríamos las DNS

Gestión de DNS para uo282978.tk						
Buscar registros DNS <input type="text"/> <input type="button" value="Buscar"/> <input type="button" value="Avanzado"/> <input type="button" value="➕ Agregar registro"/>						
Tipo ▲	Nombre	Contenido	Estado de proxy	TTL	Acciones	
A	uo282978	85. 1. .68	Redirigido por proxy	Automático	Editar ▶	
A	www	85. 1. .68	Redirigido por proxy	Automático	Editar ▶	

Y cambiaríamos los Nameservers

Managing uo282978.tk

Information Upgrade Management Tools Manage Freenom DNS

Changes Saved Successfully!

Nameservers

You can change where your domain points to here. Please be aware changes can take up to 24 hours to propagate.

☐ Use default nameservers (Freenom Nameservers)
 ☒ Use custom nameservers (enter below)

Nameserver 1
ELMA.NS.CLOUDFLARE.COM

Nameserver 2
LYNN.NS.CLOUDFLARE.COM

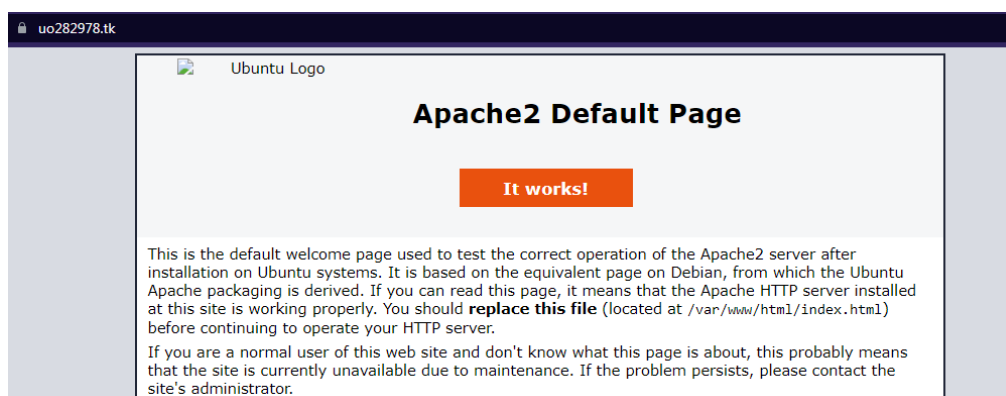
Nameserver 3

Nameserver 4

Nameserver 5

Change Nameservers

Ya teniendo Cloudflare configurado la web se vería así:



He de destacar que Cloudflare incluye un certificado SSL gratuito y una opción donde siempre nos redirige a HTTPS en vez de HTTP.

Si intentamos hacer ping al dominio protegido con Cloudflare veremos lo siguiente:

```

ruflas ~ ♥ 19:15 ping www.uo282978.tk
Haciendo ping a www.uo282978.tk [172.67.189.37] con 32 bytes de datos:
Respuesta desde 172.67.189.37: bytes=32 tiempo=35ms TTL=51
Respuesta desde 172.67.189.37: bytes=32 tiempo=34ms TTL=51
Respuesta desde 172.67.189.37: bytes=32 tiempo=31ms TTL=51
Respuesta desde 172.67.189.37: bytes=32 tiempo=32ms TTL=51

Estadísticas de ping para 172.67.189.37:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 31ms, Máximo = 35ms, Media = 33ms
  
```

Ya podemos ver que no es la IP Pública de mi casa, pero aun así vamos a tratar de identificar más información de la IP...

Si utilizamos la herramienta de whois podemos observar como la IP que nos ha aparecido al hacer ping pertenece a los servidores de Cloudflare:

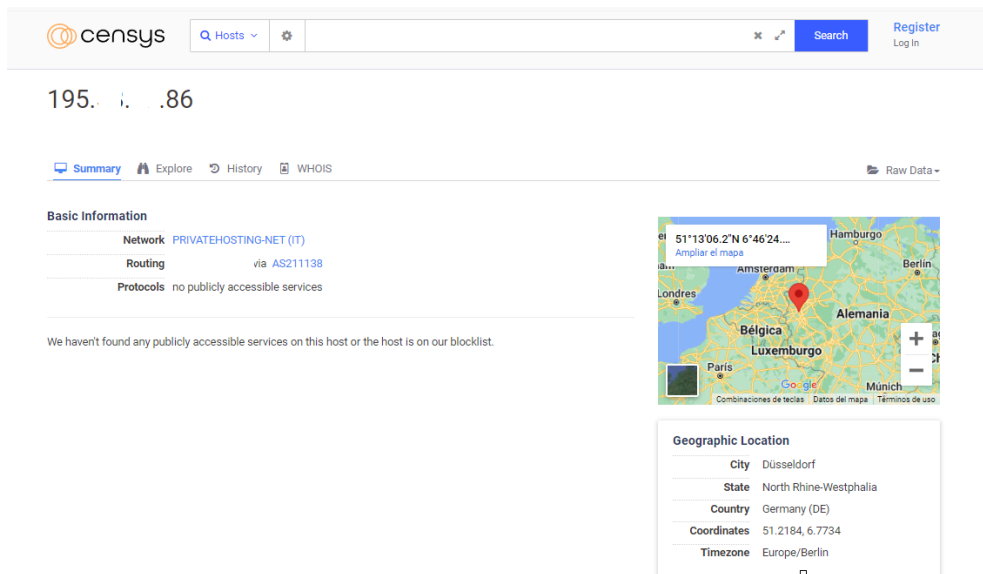
```
NetRange:      172.64.0.0 - 172.71.255.255
CIDR:          172.64.0.0/13
NetName:       CLOUDFLARENET
NetHandle:     NET-172-64-0-0-1
Parent:        NET172 (NET-172-0-0-0-0)
NetType:       Direct Allocation
OriginAS:      AS13335
Organization:  Cloudflare, Inc. (CLOUD14)
RegDate:       2015-02-25
Updated:       2021-05-26
Comment:       All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abus
Ref:           https://rdap.arin.net/registry/ip/172.64.0.0
```

Aun así, existen muchas formas de obtener la IP real que esconde un servidor protegido por Cloudflare.

Una de ellas es esta web: censys.io

En concreto con su herramienta: search.censys.io

Donde hace no mucho me encontré con que al buscar uno de mis dominios salía la IP real del servidor que tengo contratado.



195.1.1.86

Summary Explore History WHOIS Raw Data

Basic Information

Network	PRIVATEHOSTING-NET (IT)
Routing	via AS211138
Protocols	no publicly accessible services

We haven't found any publicly accessible services on this host or the host is on our blacklist.

Geographic Location

City	Düsseldorf
State	North Rhine-Westphalia
Country	Germany (DE)
Coordinates	51.2184, 6.7734
Timezone	Europe/Berlin

Además, salía información como todos los puertos que tenía abiertos.

A día de hoy ya he eliminado los datos de esta página web y voy a enseñar como protegerse de herramientas como esta.

Firewall

¿Qué es un Firewall?

Un firewall es un sistema de seguridad de red que monitoriza el tráfico entrante y saliente de nuestra red y permite o bloquea el mismo en base a un conjunto de reglas ya configuradas por defecto o por el mismo usuario en base a sus necesidades.

Configuración

Para protegernos de este tipo de herramientas de [OSINT](#) podemos ver en su propia página web como evitar que recopilen datos de nuestro servidor en este [artículo](#).

Para ello debemos de instalar un firewall en nuestro servidor si este no viene instalado por defecto y añadir reglas de excepción hacia las direcciones IP que se muestran.

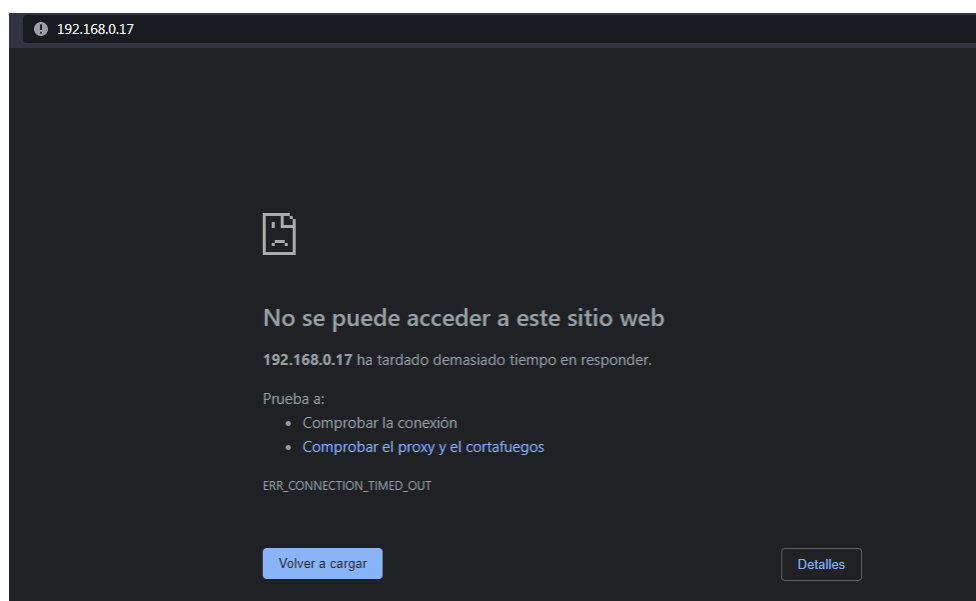
En este caso yo ya tengo instalado un firewall (UFW) pero en caso de no contar con ello puedes instalarlo con:

```
sudo apt install ufw
```

Una vez instalado debemos de activarlo, pero recordar que una vez activado tendremos que habilitar el puerto 80, al igual que cualquier puerto que use el servidor para alguna aplicación que tengamos desplegada.

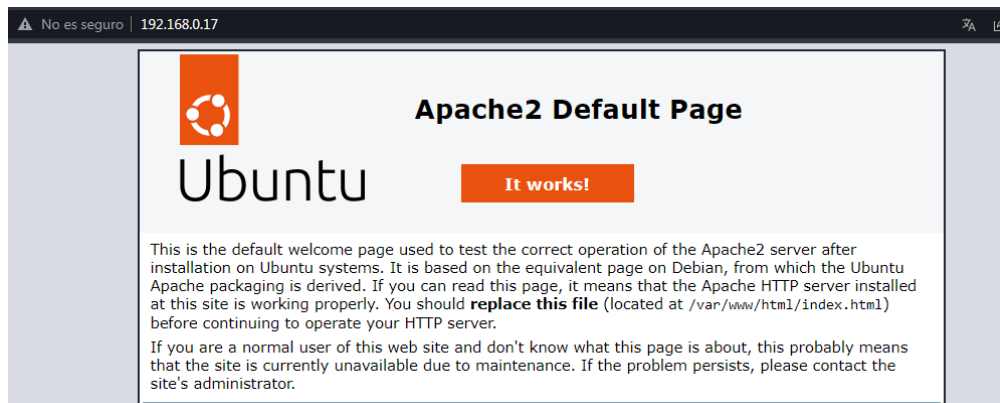
```
sudo ufw enable
```

```
root@ubuntu:~/uo282978# ufw enable
Firewall is active and enabled on system startup
root@ubuntu:~/uo282978# ufw status
Status: active
root@ubuntu:~/uo282978# _
```



Como comentaba debemos activar una regla para abrir el puerto 80 en nuestro firewall.

```
root@ubuntu00:/home/uo282978# ufw allow 80
Rule added
Rule added (v6)
root@ubuntu00:/home/uo282978#
```



Y la página web ya volvería a funcionar.

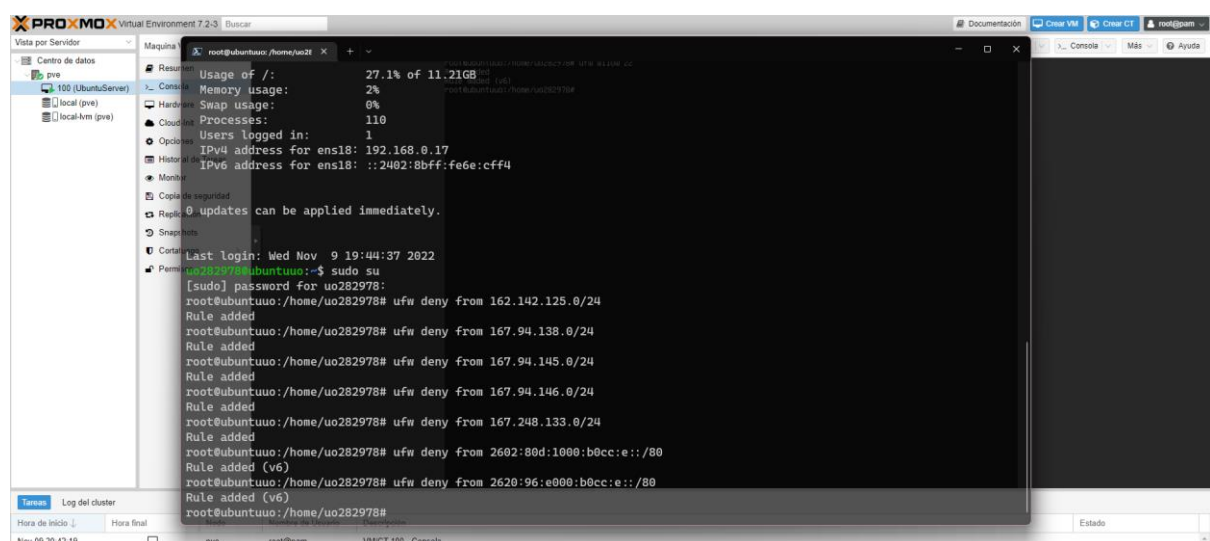
Ahora debemos de añadir reglas de excepción a las IPs de la herramienta antes mencionada.

Can I opt out of Censys data collection?

Censys scans help the scientific community accurately study the Internet. The data Censys gathers is sometimes used to detect security problems and to inform operators of vulnerable systems so that they can be fixed. If you opt out of data collection, you might not receive these important security notifications.

If you wish to opt out, you can configure your firewall to drop traffic from the subnets we use for scanning:

- 162.142.125.0/24
- 167.94.138.0/24
- 167.94.145.0/24
- 167.94.146.0/24
- 167.248.133.0/24
- 2602:80d:1000:b0cc:e::/80
- 2620:96:e000:b0cc:e::/80



En caso de encontrar otra vulnerabilidad de OSINT como podríamos encontrar en herramientas como [Shodan](#) entre otros bastaría con protegernos mediante reglas del firewall.

Extra

Me ha gustado mucho realizar este trabajo ya que nunca había usado ProxMox y aparte de conocimiento que ya tengo sobre web o servidores me ha servido para aprender mucho.

Por último, ya que no es mi intención dejar abierto para siempre el puerto 80 en mi red o tener esta maquina virtual encendida 24/7 he guardado la web en la famosa web [WayBackMachine](#).

En caso de querer revisar la web o por dejar constancia de que esta web ha existido de verdad bajo este dominio: [WEB](#)

Bibliografía

[ProxMox Wiki](#)

[Cloudflare](#)

[OSINT Engines](#)

[Apache Wiki](#)