



TUTORIAL TRUENAS

IMPLANTACIÓN DE S.O.

Autor: Jorge Navarrete, 1º ASIR.
Jaén, a 30 de Abril de 2021.



ÍNDICE

Introducción	4
Obtención de la imagen ISO	4
Creación de la máquina virtual	5
Requisitos	5
Máquina virtual en VMware	6
Instalación de TrueNAS	10
Configuración inicial de TrueNAS	12
Consola	12
Interfaz gráfica	13
Configuración de discos	16
Configuración de usuarios	21
Creación de grupos	21
Creación de usuarios	22
Compartir volúmenes	25
Permisos y privilegios	27
Volumen 1	27
Volumen 2	29
Permisos avanzados	30
Comprobación de usuarios y SMB	30
Profesores	31
Grupo “Primeros”	32
Grupo “Segundos”	33
Servicio FTP	33
Activar servicio	33
Demostración de funcionamiento	35
Cuotas de disco por usuario	36
Establecer cuotas	36
Demostración de funcionamiento	37
Anexos	38
Quemar ISO en un Pendrive	38
Recursos de la máquina virtual	39
Documento de configuración de servidor	40



1. Introducción

En este documento se detallará el proceso de configuración de un dispositivo NAS con el sistema operativo TrueNAS, utilizando la mayor cantidad posible de capturas de pantalla para representar lo mejor posible el proceso, aunque, la explicación en texto tendrá gran importancia, ya que no es lo más adecuado llenar un PDF de imágenes si se puede explicar correctamente de forma escrita.

Al final de los apartados regulares del documento se encontrará un anexo donde se mencionarán y explicarán los cambios o errores que se hayan realizado en un primer momento,

además del documento de configuración del servidor donde se reflejarán los usuarios, grupos y privilegios.

Mediante este método podremos convertir un ordenador en un servidor NAS, pero, ¿qué es un NAS?

Cuando hablamos de un NAS, nos referimos a un dispositivo de almacenamiento conectado a la red, una máquina que nos proporcionará almacenamiento seguro y fiable a través de la red.

En este caso lo simularemos mediante una máquina virtual, pero a niveles prácticos el proceso será el mismo.

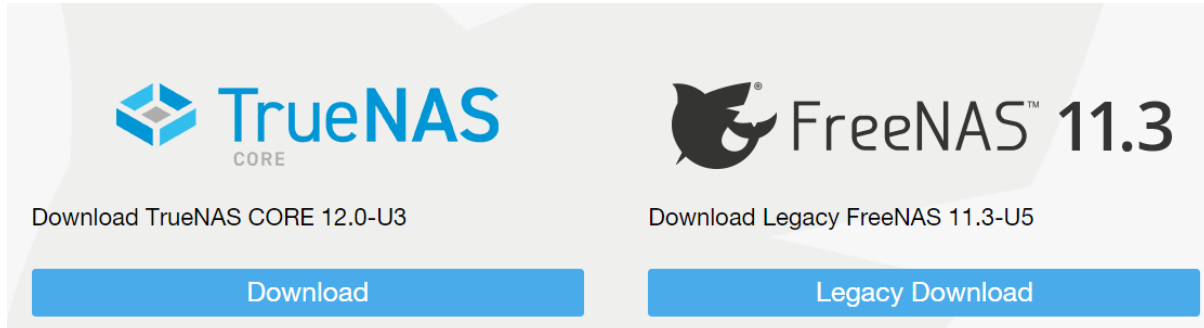
2. Obtención de la imagen ISO

Con el objetivo de realizar una actividad actualizada y útil, usaré la última versión disponible de TrueNAS, esta será la CORE 12.0-U3. Este sistema operativo proviene del antiguo FreeNAS, que llegó hasta la versión 11.

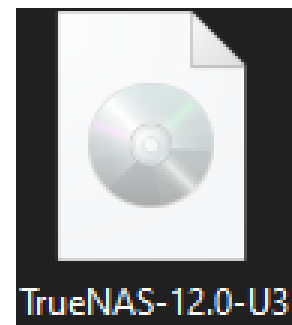
Estos sistemas operativos están basados en FreeBSD, aunque según su propia información, esto cambiará en un futuro cercano, y TrueNAS en versiones más adelantadas estará basado en alguna distribución de Linux.



Para la descarga de este sistema operativo en su versión 12, lo haremos siempre desde su [página web oficial](#), asegurándonos así de que será una ISO correcta y segura.

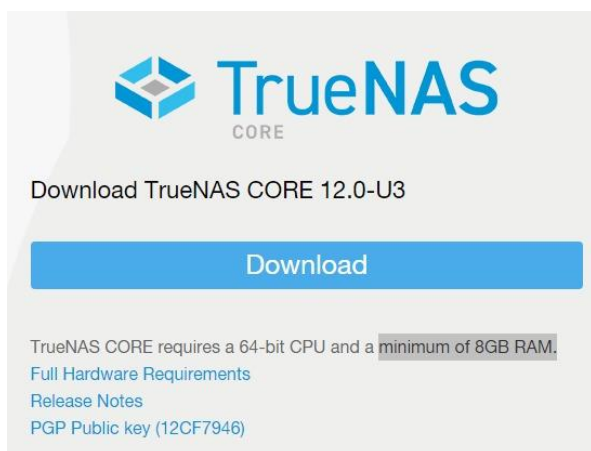


Tras pulsar sobre el botón de descargar, empezará la bajada de la imagen ISO. Dependiendo totalmente de nuestra velocidad de Internet de bajada, podrá tardar unos segundos o unos minutos, ya que pesa unos 900MB. Esta será la ISO que directamente usaremos en nuestra máquina virtual, para instalarla en una máquina física a través de USB, habrá que quemarla en un Pendrive (**véase Anexo 1*).



3. Creación de la máquina virtual

a. Requisitos



Para crear nuestra máquina virtual revisaremos los requisitos hardware que se nos indica en la página web de TrueNAS. En el manual de [este enlace](#) podemos encontrar una completa información sobre el hardware necesario, pero nos centraremos, principalmente, en la cantidad de memoria RAM.

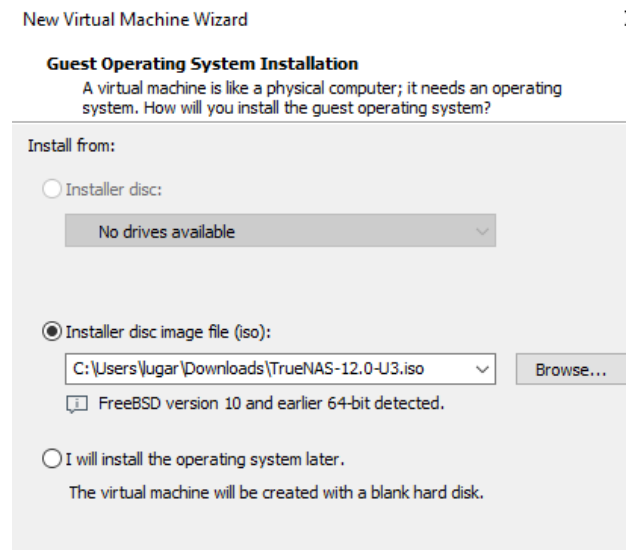


Tal y como se ve en la imagen anterior, usaremos 8GB de RAM, aunque posteriormente comprobaremos si son realmente necesarios para un caso como este. En cuanto a procesador, discos, etc. no habrá apenas limitaciones en máquinas relativamente actuales.

b. Máquina virtual en VMware

Usando el hipervisor VMware Workstation 16, se creará una máquina virtual para simular un dispositivo NAS físico en nuestra red.

Empezaremos pues, indicando al asistente de creación de una nueva máquina virtual que usaremos la configuración avanzada para poder personalizar totalmente nuestro hardware.



Seguidamente, en la siguiente ventana seleccionaremos el archivo ISO que descargamos previamente, con la ruta que corresponda.

VMware detectará que es una versión de FreeBSD, y a continuación nos recomendará una serie de recursos hardware debido a esto.



A continuación indicaremos un nombre para nuestra máquina virtual, así como la ruta donde se guardarán sus archivos necesarios, configuraciones etc. En mi caso lo haré todo en el HDD, ya que será más real para un NAS doméstico o de una PYME.

Respecto al procesador, usaremos lo recomendado: 4 hilos de ejecución. En este caso, se usarán 2 núcleos físicos con 2 hilos cada uno de mi Ryzen 3800X. Durante toda esta actividad estarán en modo ECO a solo 4075Mhz.

En cuanto a la cantidad de memoria RAM, VMware nos recomienda únicamente 256MB al detectar simplemente un sistema operativo FreeBSD, pero, siguiendo las recomendaciones oficiales de TrueNAS, usaremos 8GB de memoria RAM, en este caso siendo DDR4 a 3600Mhz.

En el segundo anexo, tras probar la máquina con TrueNAS valoraremos si de verdad necesitamos 8GB para un sistema como este.



New Virtual Machine Wizard

Select a Disk Type

What kind of disk do you want to create?

Virtual disk type

☐ IDE

☐ SCSI (Recommended)

☒ SATA

☐ NVMe

Con su tamaño pasará algo similar que con la memoria RAM. En la página web de TrueNAS no se nos indica de forma clara y concisa el tamaño recomendado del disco duro donde se instalará este sistema operativo, y VMware nos recomienda 20GB. En principio, usaremos esta capacidad de 20GB, que probablemente sea excesiva. En el mismo segundo anexo trataremos también este tema.

New Virtual Machine Wizard

Specify Disk File

Where would you like to store the disk file?

Disk file

One 20 GB disk file will be created using this file name.

D:\VMV\NAS.vmdk Browse...

El resto de la máquina virtual, la configura VMware por defecto, teniendo una tarjeta de red NAT, que será suficiente para conectarnos de forma local a través del host, y nos evitamos los problemas que suele dar la Bridge en VMware.

Tras establecer y definir los recursos para el CPU y la RAM, nos toca indicar el tipo de disco duro principal de la máquina. Siguiendo el concepto de intentar simular un NAS real, usaremos discos SATA.

New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

Maximum disk size (GB):

Recommended size for FreeBSD version 10 and earlier 64-bit: 20 GB

☐ Allocate all disk space now.

Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

☒ Store virtual disk as a single file

☐ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Este disco duro, al igual que los archivos de configuración de la máquina virtual, estará guardado en mi disco duro mecánico de 7200rpm SATA 3, siendo así una situación bastante realista.

The virtual machine will be created with the following settings:

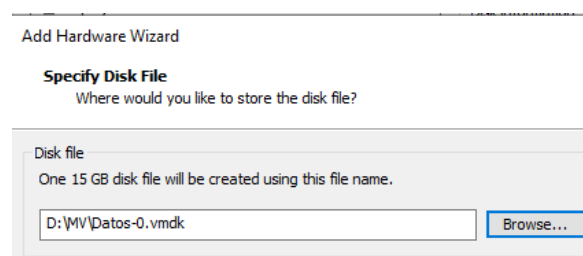
Name:	NAS
Location:	D:\VMV
Version:	Workstation 16.x
Operating System:	FreeBSD version 10 and earlier 64-bit
Hard Disk:	20 GB
Memory:	8192 MB
Network Adapter:	NAT
Other Devices:	4 CPU cores, CD/DVD, USB Controller, Sound Card

Customize Hardware...



Teniendo ya nuestro dispositivo NAS, debemos instalar los discos que usaremos para datos. En este caso, siendo un ejemplo práctico con fines educativos, usaremos únicamente discos de 15GB. Solo tendremos que pulsar sobre el botón “Add” sobre la máquina en VMware y establecer el tamaño del nuevo disco.

Los discos de datos también los guardaré en el disco duro mecánico, en el mismo. Esto perjudicará levemente al rendimiento en un entorno RAID, ya que será únicamente un disco duro físico.



	Hard Disk (SATA)	20 GB
	New Hard Disk (SATA)	15 GB
	New Hard Disk (SATA)	15 GB
	New Hard Disk (SATA)	15 GB

Este mismo proceso se repetirá exactamente igual otras dos veces, pero cambiando el nombre de los discos duros, para tener así tres discos duros de 15GB para datos, y el disco del sistema operativo TrueNAS.

4. Instalación de TrueNAS

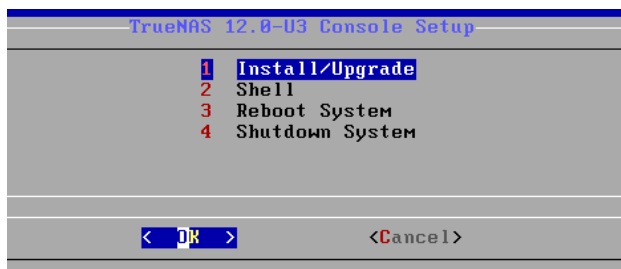
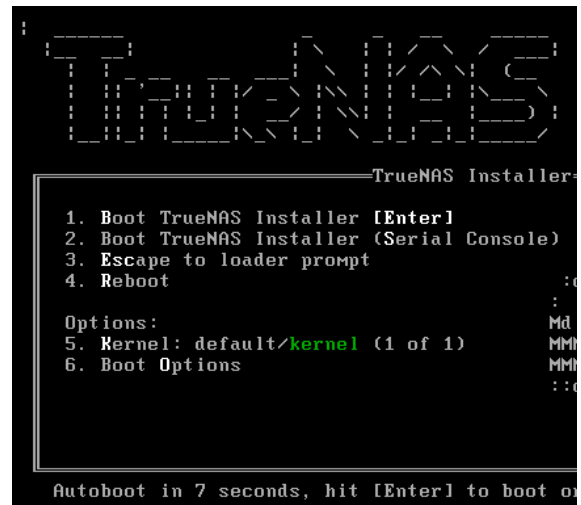
Una vez creada la máquina virtual procedemos a iniciarla, con la ISO ya seleccionada en el lector de discos virtual, esto ya se hizo automáticamente cuando le

indicamos a VMware el archivo ISO que íbamos a utilizar, en el caso de una máquina física, debemos indicar en el orden de Boot que arranque desde el PenDrive USB.



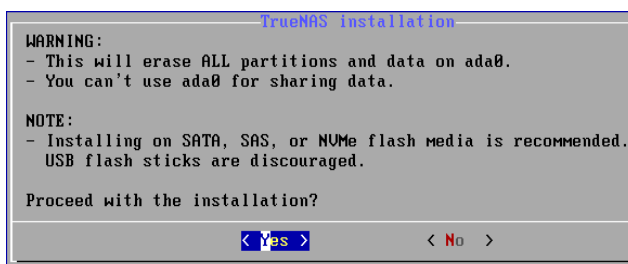
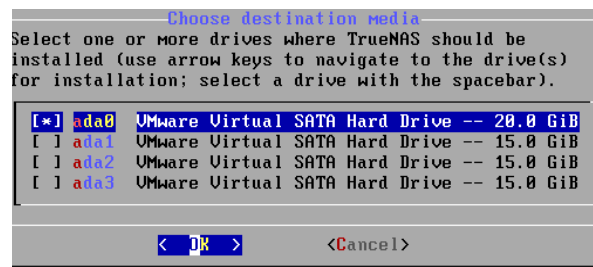
Después de unos segundos tras encender la máquina desde el dispositivo USB o desde la ISO, aparecerá en pantalla el curioso menú de instalación de TrueNAS.

Como queremos instalarlo de forma estándar, le daremos al “1” en nuestro teclado o esperaremos al Autoboot.



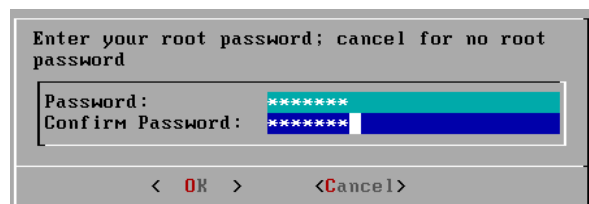
Con una interfaz muy básica volveremos a seleccionar que deseamos instalar TrueNAS y daremos enter sobre el OK para continuar.

A continuación debemos seleccionar con el espacio el disco duro donde se instalará TrueNAS, lo podemos identificar por el modelo, por el puerto donde está conectado, o por el tamaño.



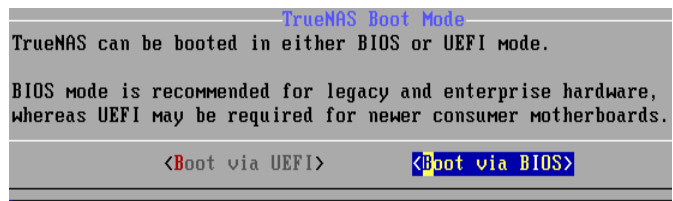
Después de seleccionar el disco, tendremos que confirmar que perderemos todas las particiones del disco, y que no podremos usar ese disco para compartir datos.

En la siguiente ventana únicamente tenemos que escribir nuestra contraseña para el usuario root, y la confirmación de la misma.

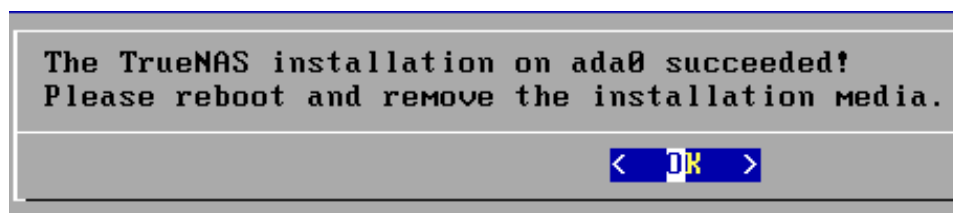




El proceso continúa preguntando si queremos iniciar TrueNAS en BIOS o UEFI. En este caso será BIOS ya que la máquina se creó como tal.



Por último el asistente de instalación nos confirmará que TrueNAS ha sido correctamente instalado en el disco ada0, y que reiniciemos la máquina quitando la imagen ISO usada para el proceso (O el Pendrive USB en el otro caso.)



5. Configuración inicial de TrueNAS

a. Consola

La primera vez que iniciemos nuestra máquina con TrueNAS tardará unos minutos en estar lista completamente, ya que tendrá que checkear ciertos aspectos del hardware, red etc.

Una vez se haya iniciado, nos aparecerá en pantalla la configuración de la máquina desde la consola de FreeBSD, indicándonos 11 opciones de configuración y la IP local para acceder al dispositivo NAS, en este caso la 192.168.49.129.





```
1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset Configuration to Defaults
9) Shell
10) Reboot
11) Shut Down

The web user interface is at:

http://192.168.48.129
https://192.168.48.129

Enter an option from 1-11: 4
Configure IPv4 Default Route? (y/n)y
IPv4 Default Route:192.168.1.1
```

Para evitarnos errores según en la red que podamos tener el NAS, le indicaremos manualmente la dirección IPv4 por defecto del router, en mi caso la 192.168.1.1.

Esto lo haremos mediante la opción 4, confirmando que sí queremos hacerlo, y escribiendo la dirección IP manualmente. Esta dirección, aunque por defecto suele ser esta, habrá que comprobarla en cada red.

Desde la consola podemos también configurar el servicio DNS en caso de que el servicio del router no se lo haya proporcionado y queramos que el sistema NAS tenga acceso a Internet.

Esto lo haremos mediante la opción de configuración 6, y tendremos tres opciones de direcciones DNS.

```
1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset Configuration to Defaults
9) Shell
10) Reboot
11) Shut Down

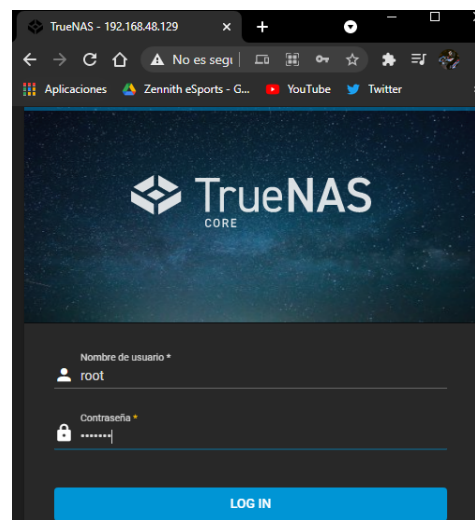
The web user interface is at:

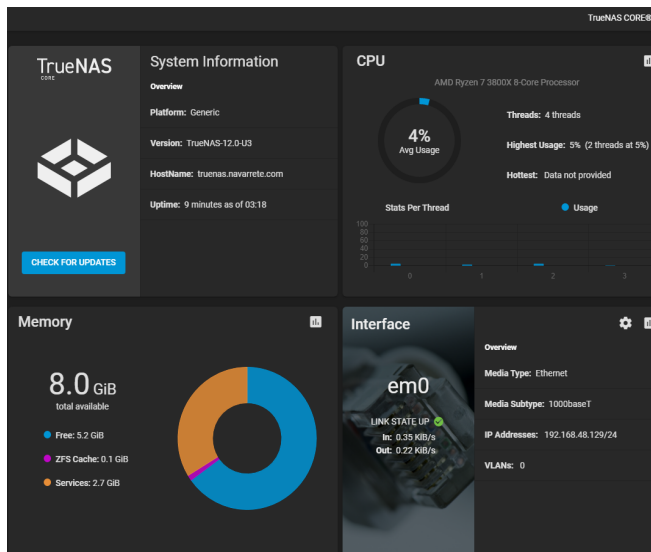
http://192.168.48.129
https://192.168.48.129

Enter an option from 1-11: 6
DNS Domain [local:navarrete.com]
Enter nameserver IPs, an empty value ends input
DNS Nameserver 1:8.8.8.8
DNS Nameserver 2:1.1.1.1
DNS Nameserver 3:8.8.4.4
```

b. Interfaz gráfica

Una vez configurados los aspectos básicos del sistema desde la consola, el resto de parámetros los podemos cambiar y administrar desde la interfaz web gráfica. Como es lógico, se accederá a ella desde la dirección local 192.168.48.129 en mi caso, o la que indique el sistema NAS por pantalla cuando se haya iniciado.



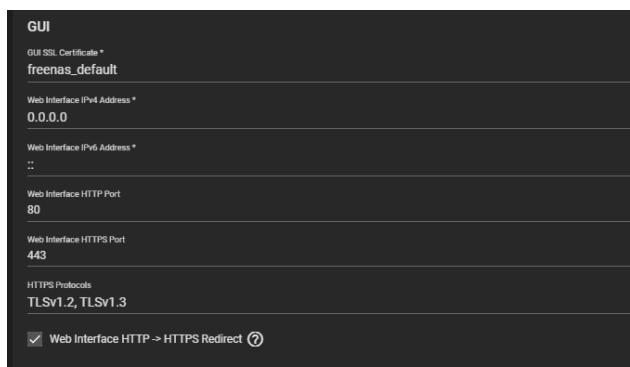
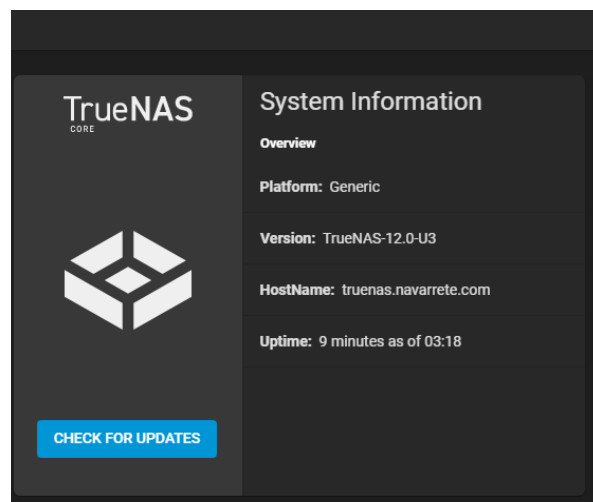


Accederemos a ella mediante el usuario “root” y la contraseña que establecimos en su instalación, y nos encontraremos con el dashboard en primer plano.

Aquí se representará el uso de la RAM en un gráfico, el uso del CPU y la temperatura si tuviésemos sensores físicos, así como la interfaz de red de la máquina.

Desde este mismo dashboard será desde donde podremos tener nuestro sistema operativo actualizado, cualquier actualización definitiva del software la podremos checkear, descargar e instalar desde aquí.

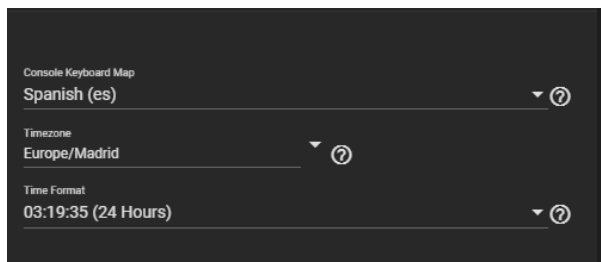
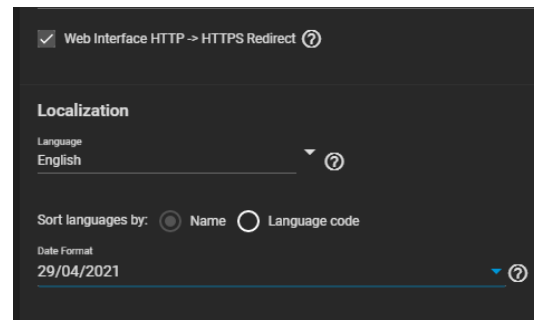
Esto es algo recomendable, ya que suelen arreglar problemas de estabilidad, configuraciones etc.



Desde esta interfaz web tenemos la posibilidad de configurar casi totalmente nuestro dispositivo NAS. En la configuración general podemos hacer que cada usuario que se conecte por HTTP sea redirigido a HTTPS, y a su vez seleccionar el tipo de protección del HTTPS.

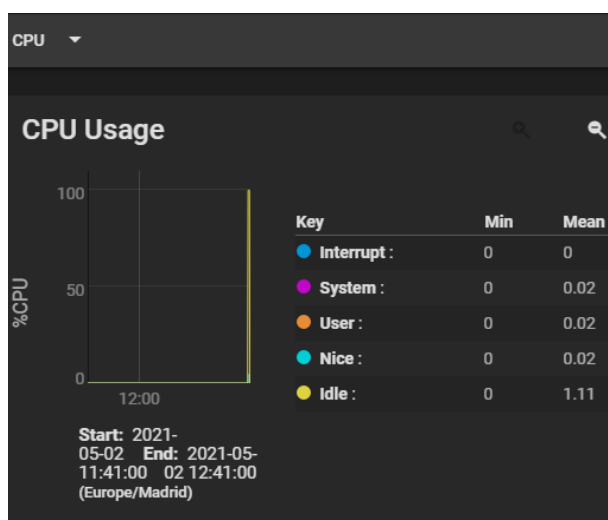
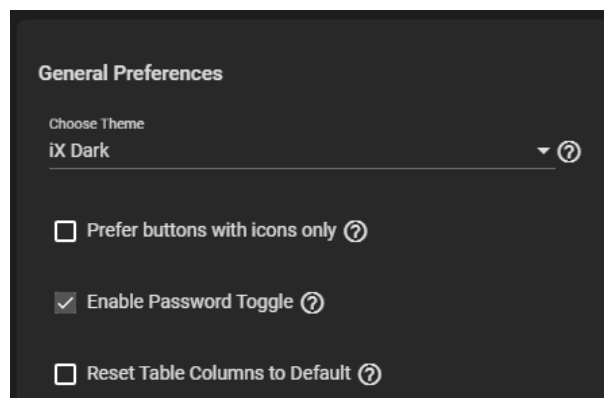


Se nos proporciona también la configuración de cambiar el idioma, aunque no es recomendable ya que las traducciones no son perfectas. Lo que no nos dará ningún problema es cambiar el formato de la fecha a uno con el que estemos cómodos, y no el americano.



Desde este mismo menú de configuración es desde donde se cambiará el mapeado de teclas de nuestro teclado, la zona horario y el formato de hora del sistema NAS.

En las preferencias generales de la interfaz web, TrueNAS nos permite trabajar de forma más cómoda pudiendo cambiar el tema oscuro a cualquier otro más clásico, claro, con menos colores etc, así como poder elegir si queremos solo botones, sin letras, usar el logo clásico etc.



En general hay gran aspectos que van cambiando levemente con cada versión, y que nos permiten personalizar y configurar la máquina, pero también monitorizar y revisar su funcionamiento desde el apartado de reports o System. De esta forma podemos asegurarnos que el hardware está correcto y que no se está usando a ciertas horas o bajo mucha carga.



6. Configuración de discos

Disks				
Filter Disks				
<input type="checkbox"/>	Name	Serial	Disk Size	Pool
<input type="checkbox"/>	ada0	0000000000000000	20 GiB	N/A
<input type="checkbox"/>	ada1	0100000000000000	15 GiB	N/A
<input type="checkbox"/>	ada2	0200000000000000	15 GiB	N/A
<input type="checkbox"/>	ada3	0300000000000000	15 GiB	N/A

En nuestro NAS tenemos ya los discos duros conectados, pero no podremos compartirlos aún de ninguna manera. Antes de comenzar el proceso para ello, comprobaremos desde el menú discos (Otro más del panel izquierdo) que están todos correctos.

Una vez haya confirmado que están todos, con su capacidad y puerto correcto, y sin ningún Pool, lo que debemos hacer es precisamente esto, crear pools.

Un pool se utiliza para agrupar los diferentes volúmenes que podremos usar en nuestro NAS, para administrarlos así de forma más sencilla.

Storage / Pools / Import Pool

1 Create or Import pool 2 Decrypt pool 3 Select disks

Create a pool:

☒ Create new pool ?

☐ Import an existing pool ?

CANCEL CREATE POOL

Desde el Pool manager seleccionaremos todos los discos que queramos usar para este Pool llamado “Datos” y los llevaremos a la parte derecha mediante un click en la flecha.

Name * Datos ?

☐ Encryption ?

RESET LAYOUT SUGGEST LAYOUT ? ADD VDEV

Available Disks

<input checked="" type="checkbox"/>	Disk	Type	Capacity	
<input checked="" type="checkbox"/>	ada1	UNKNO	15 GiB	>
<input checked="" type="checkbox"/>	ada2	UNKNO	15 GiB	>
<input checked="" type="checkbox"/>	ada3	UNKNO	15 GiB	>

3 selected / 3 total

Data VDevs

REPEAT

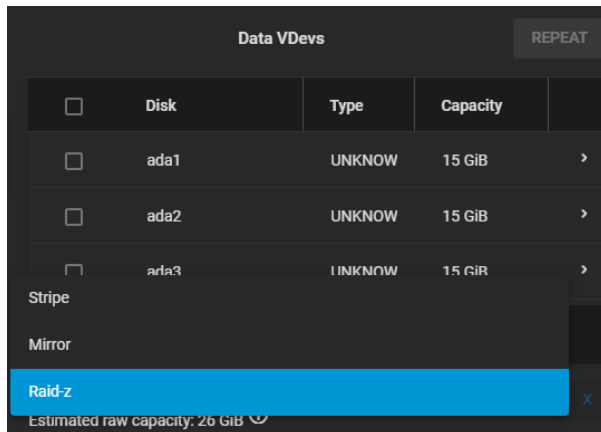
☐ Disk Type Capacity

No data to display

0 selected / 0 total

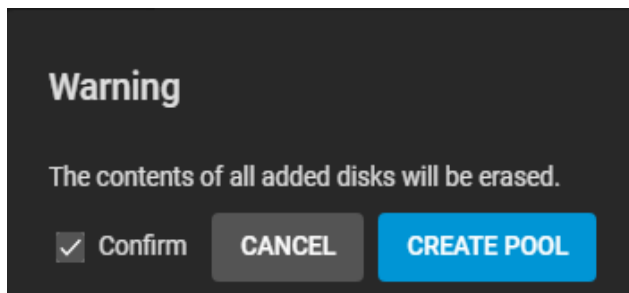
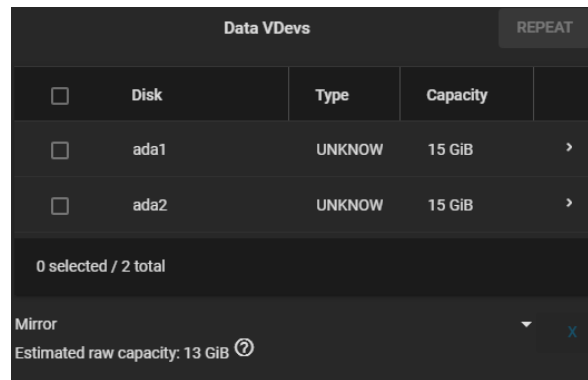
Stripe

Estimated raw capacity: 0 B ?



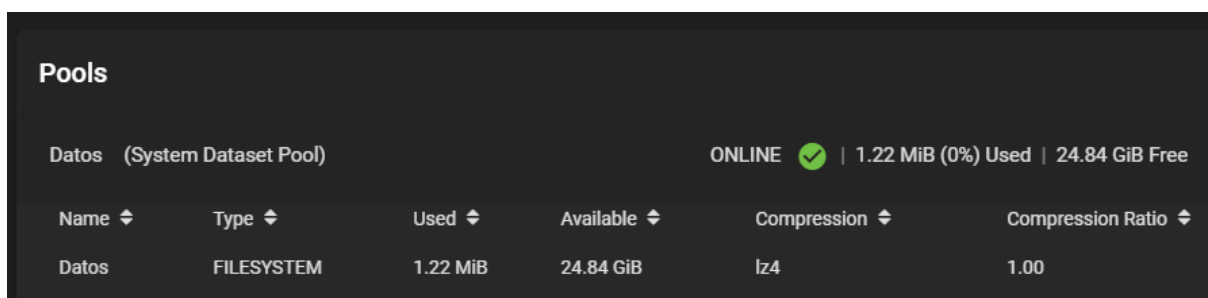
Una vez los discos estén en la parte derecha del Pool manager, podremos elegir qué tipo de Raid usar. En este caso usaré un Raid 5, con bits de paridad entre los tres discos duros para asegurarnos la seguridad de la información aunque un disco falle, y “perdiendo” solo un 33,3% de capacidad.

Si deseamos usar únicamente dos discos duros y un Raid 1, debemos usar la opción “Mirror”, haciendo así que los dos discos duros tengan la misma información, de forma redundante. Así también podrá fallarnos un disco y seguir teniendo la información, pero perderemos un disco duro de capacidad.



Una vez hayamos creado el Pool según nuestra necesidad, con el nombre personalizado y eligiendo o no si queremos encriptarlo, debemos confirmar que se perderá el contenido de los discos al crear el pool.

A continuación, cuando clickemos sobre “Pools” en el menú vertical izquierdo, ya tendremos el llamado “Datos” creado con el tamaño indicado.





Name and Options

Name
Datos

Comments

Sync
Standard

Compression level
LZ4

Enable Atime
on

Other Options

ZFS Deduplication
off

Case Sensitivity
Sensitive

SAVE CANCEL ADVANCED OPTIONS

Una vez hemos creado el pools, podemos editar su configuración, dentro de las muchísimas opciones avanzadas que hay, una básica interesante puede ser el nivel de compresión.

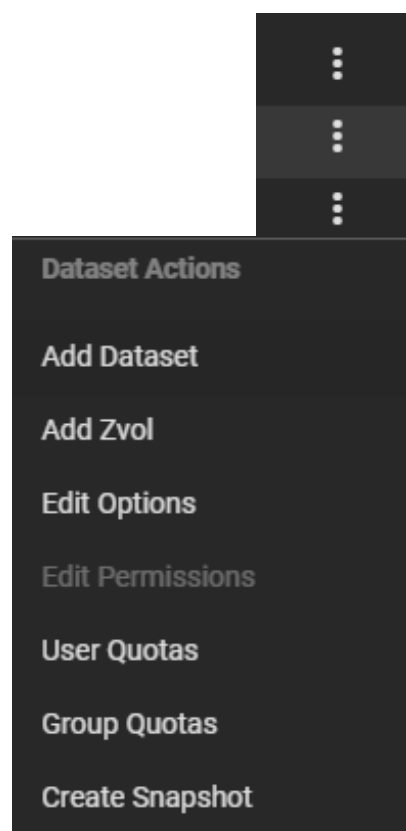
En este caso lo dejaremos por defecto con el LZ4, que es un algoritmo de compresión sin pérdida con una velocidad media, por ello es el recomendado por TrueNAS. Podemos cambiar en caso de que necesitemos más compresión o más velocidad.

Una vez tenemos nuestro pool configurado y con los discos duros agrupados tal y como queramos, debemos proceder a crear un dataset, clickando sobre los tres puntos del propio Pool.

Este dataset es simplemente un conjunto de datos, que tendrán unas características y privilegios o permisos según usuarios o grupos de usuarios.

A nivel práctico son como volúmenes o carpetas dentro del propio pool de los discos duros. Por tanto, no solo vamos a crear uno, sino que serán varios.

Será desde aquí también desde donde podemos crear una Snapshot del pool de Datos, y podemos obviamente hacer esto para cada pool que hayamos creado con nuestros discos duros.





Name and Options

Name *

Volumen1

Comments

Primer volumen

Sync

Inherit (standard)

Compression level

Inherit (lz4)

Enable Atime

Inherit (on)

This Dataset

Quota for this dataset

10 GiB

Quota warning alert at, %

80

☒ Inherit

Quota critical alert at, %

95

☒ Inherit

Reserved space for this dataset

Encryption Options

☒ Inherit (non-encrypted)

Con un menú de creación similar a los anteriores, debemos establecer un nombre personalizado obligatorio al dataset, en este caso lo llamaremos Volumen 1 siguiendo el documento de configuración del servidor (*Véase anexo C*).

Opcionalmente podemos poner un comentario como descripción del dataset, así como una forma de compresión definida o usar la heredada del pool.

Este dataset puede tener un tamaño libre y ocupar el total del Pool, o bien podemos establecer un límite como es este caso (10GiB). Tenemos la posibilidad también de cambiar los avisos de cuotas críticas o de encriptarlo de una forma diferente a lo que podría tener el pool (En este caso ninguna).

Este mismo proceso se repetirá para el segundo volumen, llamado Volumen 2 y usando la misma configuración de compresión con LZ4.

El cambio será en que este lo limitaremos de espacio a 15185MiB, es decir unos 14.84GiB que completarán el espacio total de nuestro Pool. Si lo dejásemos nulo, podría llegar hasta los 24.84GB del total del Pool.

Name and Options

Name *

Volumen2

Comments

Volumen 2 para otros usos

Sync

Inherit (standard)

Compression level

Inherit (lz4)

Enable Atime

Inherit (on)

This Dataset

Quota for this dataset

15185 MiB







Quota warning alert at, %

80

☒ Inherit



Nuestro pool configurado con dos volúmenes se vería tal que así, con el pool Datos, y dos dataset.

Pools				
Datos	(System Dataset Pool)	ONLINE  10.22 MiB (0%) Used		
Name 	Type 	Used 	Available 	Compression 
▼ Datos	FILESYSTEM	10.22 MiB	24.83 GiB	lz4
Volumen1	FILESYSTEM	127.88 KiB	10 GiB	Inherits (lz4)
Volumen2	FILESYSTEM	127.88 KiB	14.83 GiB	Inherits (lz4)

Name and Options

Name *

par

Comments

Carpeta grupo par

Sync

Inherit (standard)

Compression level

Inherit (lz4)

Enable Atime

Inherit (on)

Encryption Options

☒ Inherit (non-encrypted) 

Pero también podemos crear datasets hijos, como carpetas dentro de esos volúmenes de datos. Con el objetivo de mostrar el proceso, se hará un ejemplo donde el Volumen 1 tendrá dos hijos.

Lo haremos haciendo click en los tres puntos de configuración, pero, en lugar de hacerlo en el Pool, lo haremos sobre el dataset de, en este caso, Volumen 1.

De esta forma crearemos el dataset par e impar, dentro del propio dataset “Volumen1”, que recordamos que a su vez está en el Pool de “Datos”.

De la misma forma que antes, para que la estructura tenga sentido y lógica, y que no pueda llenarse todo el Pool llenando solo uno de los Dataset, asignaremos a ambos hijos de “Volumen1” un límite de 5 GiB (50% del Volumen 1 para cada uno).

This Dataset

Quota for this dataset

5 GiB

Quota warning alert at, %


80 ☒ Inherit

Quota critical alert at, %

95 ☒ Inherit



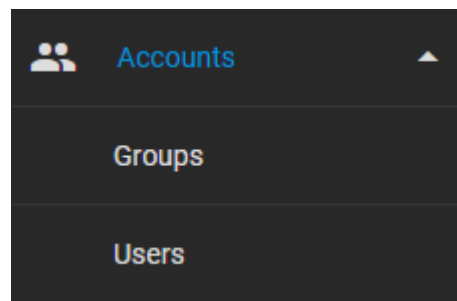
Finalmente, nuestra estructura del pool “Datos” será como se ve en esta imagen, siguiendo el documento de configuración (*Véase anexo C*).

Datos (System Dataset Pool) ONLINE  12.7 MiB (0%) Used				
Name	Type	Used	Available	Compression
▼ Datos	FILESYSTEM	12.7 MiB	24.83 GiB	lz4
▼ Volumen1	FILESYSTEM	436.91 KiB	10 GiB	Inherits (lz4)
impar	FILESYSTEM	127.88 KiB	5 GiB	Inherits (lz4)
par	FILESYSTEM	127.88 KiB	5 GiB	Inherits (lz4)
Volumen2	FILESYSTEM	181.16 KiB	14.83 GiB	Inherits (lz4)

7. Configuración de usuarios

a. Creación de grupos

Aunque podemos directamente crear usuarios y configurar los privilegios a ellos directamente, para facilitar la organización de los mismos crearemos grupos personalizados, diferentes a los definidos por defecto. Esto lo haremos desde “Groups”, ubicado en el menú izquierdo de la interfaz web.



Group Configuration

GID *

1000

Name *

Primeros

☐ Permit Sudo ?

☒ Samba Authentication ?

☐ Allow Duplicate GIDs ?

SUBMIT

CANCEL

Siguiendo el documento de configuración del servidor (*Véase anexo C*), se creará el grupo “Primeros” clickando sobre el botón “Add” en el menú de “Groups”.

Este grupo tendrá por defecto una autenticación Samba, y lo dejaremos así, permitiendo que se pueda identificar mediante este protocolo de código abierto. El ID del grupo “Primeros” por defecto será 1000.



De la misma forma, se creará el grupo “Segundos”. El ID del grupo (GID), se nos auto incrementará y tendrá por defecto el 1001.

Activaremos la autenticación Samba igual que en el caso anterior, y con ello tendremos disponible el grupo “Segundos”.

Group Configuration

GID *
1001

Name *
Segundos

Group Configuration

GID
1002

Name *
Profesores

☐ Permit Sudo ?

☒ Samba Authentication ?

Como último se creará el de “Profesores”, e, igual que en la situación anterior, el GID se auto incrementará a 1002, el cual será el que usaremos.

También siguiendo los casos anteriores activaremos la autenticación Samba y guardaremos el nuevo y último grupo, los cuales a continuación debemos asignarles a los usuarios.

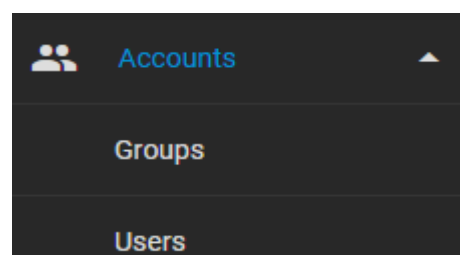
Y así será el resultado de los grupos creados en este caso. “Primeros” con GID 1000, “Segundos” con GUID 1001, y por último “Profesores con GID 1002.

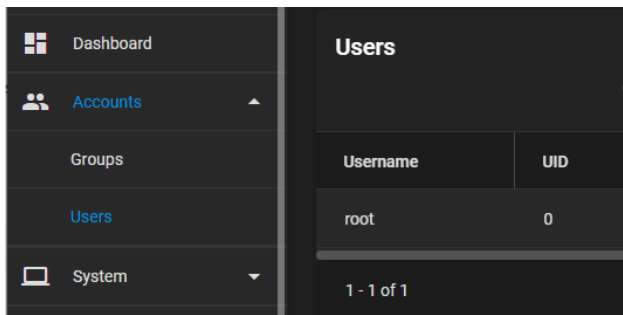
Tras comprobar que los grupos se han creado correctamente, podemos empezar a crear los usuarios.

Group	GID
Primeros	1000
Profesores	1002
Segundos	1001
1 - 3 of 3	

b. Creación de usuarios

Volviendo al menú izquierdo en la interfaz web de TrueNAS, abriremos el desplegable de “Accounts”, y posteriormente el de “Users” para acceder al menú de usuarios del servidor.





Por defecto podremos observar que únicamente tenemos creado la cuenta de “root”, con la cual instalamos el sistema operativo TrueNAS y con la que estamos trabajando.

Exactamente igual que en el caso de los grupos, haremos click en el botón azul de “Add” ubicado en la parte superior derecha de la interfaz.

Para cada usuario podremos establecer un nombre completo, así como el nombre de usuario literal con el que se iniciará sesión. Opcionalmente se podrá indicar su email.

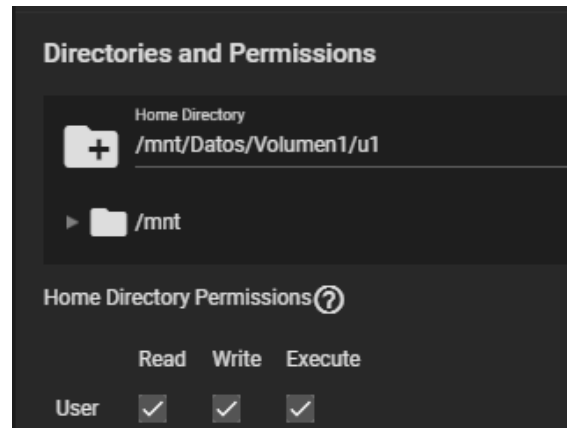
Habrà que establecer también su contraseña, y el grupo al que pertenece.

El Usuario 1 estará en el grupo de los “Primeros”, el cual seleccionaremos en el menú desplegable de “Groups”.

Activaremos también de por sí la autenticación Samba, desactivaremos que deba usar una cuenta de Microsoft y no usaremos una clave SSH.



Por último, para todos los usuarios que vayamos a crear, necesitamos establecer su directorio “home”. Como este usuario 1, perteneciente al grupo de “Primeros”, tendrá el acceso al Volumen 1, esta será su ruta Home, sobre la cual tendrá permisos de lectura, escritura y ejecución.



Identification

Full Name *
Usuario 2

Username *
u2

Email

Password *
usuario

Confirm Password *
usuario

User ID and Groups

User ID *
1001

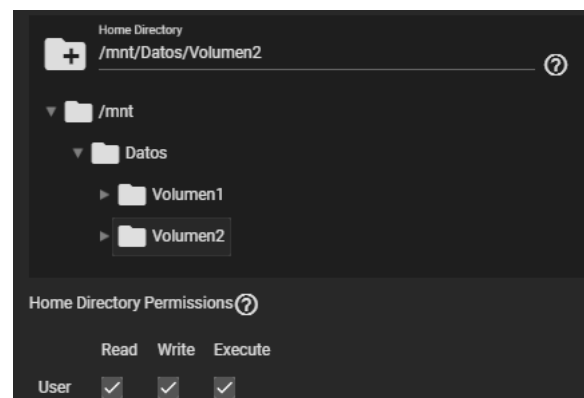
☐ New Primary Group ?

Primary Group
Segundos

El mismo procedimiento realizaremos para cada usuario que queramos crear, siguiendo siempre el documento de configuración del servidor que se encuentra en el apartado de Anexos de este mismo PDF.

El usuario 2, de igual forma, pertenecerá al grupo de los “Segundos”, y el User ID será el 1001. Este valor del ID es auto incremental y no nos debemos preocupar por él.

Siguiendo la misma lógica que con el usuario anterior, la carpeta home del usuario 2 se encontrará ubicada dentro del Volumen 2, que será al único al que tendrá acceso, además de permisos para ejecutar y escribir en él.





Identification

Full Name *
Profesor

Username *
profesor

Email

Password *

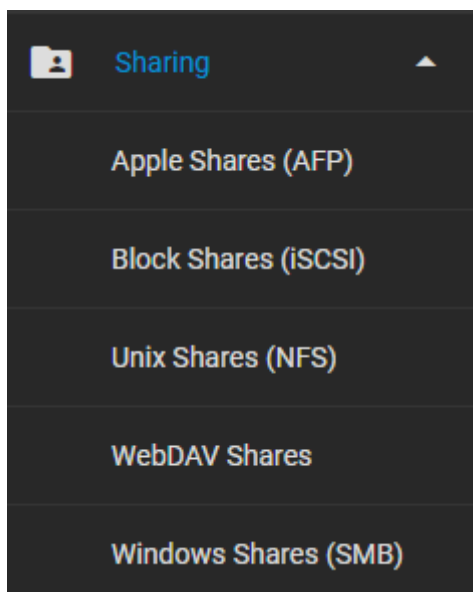
Por último en este ejemplo didáctico creándose usuarios lo haremos con el usuario “Profesor”, el cual tendrá de ID 1002 (El valor auto incremental que nos auto rellena TrueNAS), y pertenecerá, obviamente, al grupo Profesores.

Por tanto, nuestros usuarios creados para este ejemplo de estructura en nuestro NAS constará de cuatro usuarios: u1 (Usuario 1) con ID 1000, u2 (Usuario 2) con ID 1001 y profesor (Profesor) con ID 1002 , además del usuario root, que por defecto tiene el ID 0.

Username	UID
profesor	1002
root	0
u1	1000
u2	1001

8. Compartir volúmenes

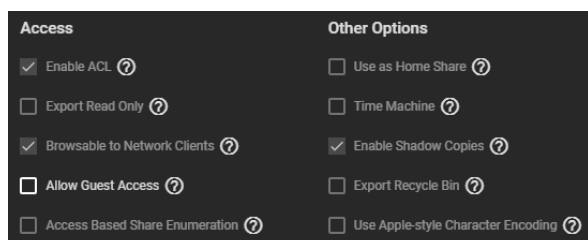
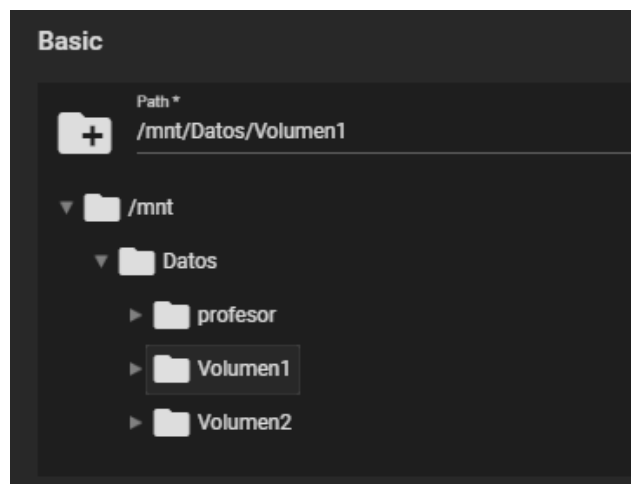
Con nuestros usuarios, grupos, pools y dataset creados, aún no podremos usar este NAS, ya que tenemos que compartir las carpetas o volúmenes creados como datasets, dentro de nuestro pool “Datos.



Para ello lo podremos hacer con diferentes métodos o protocolos. El **AFP** es el método de Apple para conectar ordenadores Macintosh, por lo que no nos interesa; **iSCSI** es un estándar muy usado y más general, por lo que puede ser una gran opción para usar nuestro NAS con diferentes sistemas operativos como clientes. **NDS** es un protocolo para Unix, y **SMB** es el protocolo de red para compartir archivos y dispositivos entre ordenadores con Windows. Usaremos este último como ejemplo de NAS usado en una red con ordenadores Windows.

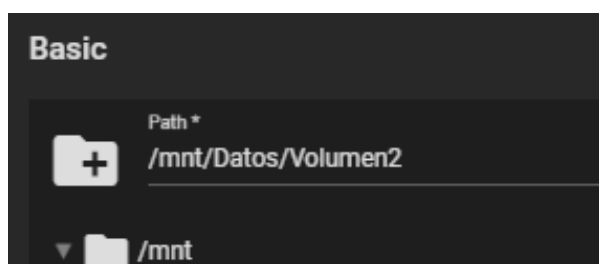
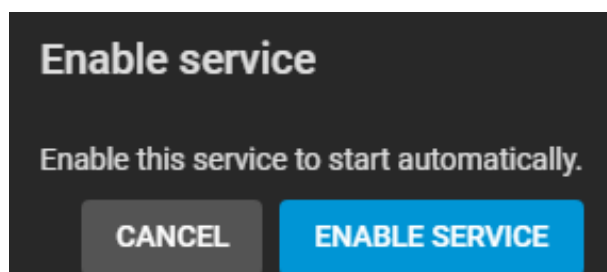


Como vamos a usar SMB para equipos Windows, clickaremos en él desde el menú izquierdo de TrueNAS Core, y pulsaremos sobre el botón azul de “Add”. Desde aquí clickaremos en la carpeta del dataset Volumen 1 para compartirlo, y activaremos mediante el tick inferior para compartirlo mediante este protocolo.



En la configuración avanzada podemos confirmar que usaremos una ACL posteriormente para establecer los privilegios y los permisos, y también podemos cambiar parámetros como que se permita el acceso de invitado.

Para confirmar la acción tendremos que pulsar sobre el botón azul de “Permitir servicio” para tener así activo el protocolo SMB en nuestro dispositivo NAS.



Haremos exactamente lo mismo con Volumen 2 para compartirlo mediante el mismo protocolo y con las mismas opciones que las del Volumen 1.

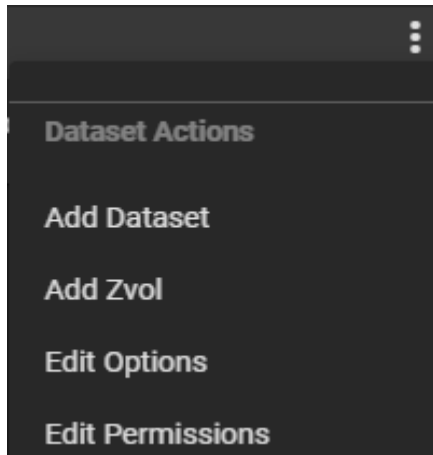
Por tanto, en nuestra ventana SMB quedarán compartidos el Volumen 1 y el Volumen 2. Habrá que configurar pues, los privilegios en ellos.

Name	Path
Volumen1	/mnt/Datos/Volur
Volumen2	/mnt/Datos/Volur



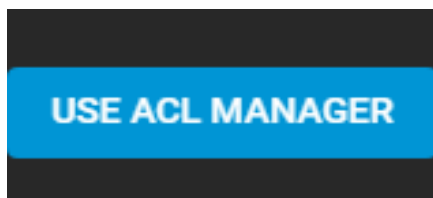
9. Permisos y privilegios

a. Volumen 1



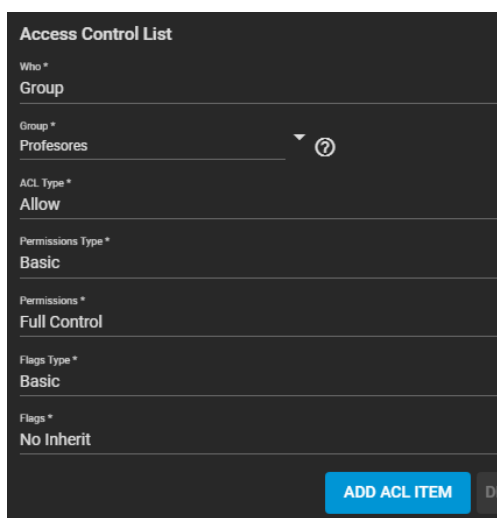
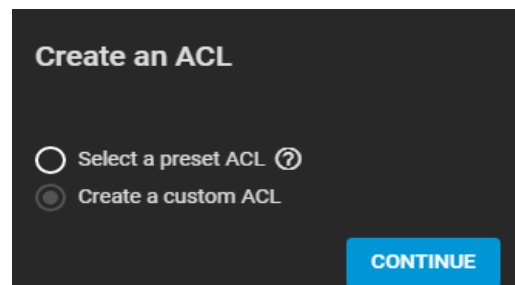
Para establecer los permisos y privilegios correctamente, lo haremos mediante listas de acceso en cada dataset. Para ello volveremos al menú de “Pools”, el cual se encontraba en el desplegable de “Storage”.

Comenzaremos con el Volumen 1, clickando sobre los tres puntos de su configuración y después en “Edit Permissions”.



Una vez en esta ventana de configuración, ignoraremos la parte superior e iremos directamente a configurar los permisos con el ACL Manager, lo cual nos lo hará más cómodo.

En caso de que se nos pregunte, seleccionaremos que vamos a crear una ACL “custom” o personalizada. Como estamos sobre el Volumen 1, debemos permitir el acceso y privilegios a profesores y al grupo de los alumnos de los “Primeros”.



Eliminaremos con el botón “Delete” las ACL que haya por defecto, y la primera que haremos nosotros será la del grupo “Profesores”, indicando en la ACL que se aplicará a un grupo en la opción “Who”. Será una ACL para permitir, y esto se indica en el tipo. Posteriormente, mediante los tipos de permisos básicos, seleccionamos que los profesores tendrán control total sobre el Volumen 1.



Sobre el mismo volumen, debemos dar privilegios a los alumnos del grupo “Primeros”; esto lo conseguiremos creando otro objeto ACL mediante el botón “Add ACL Item”.

Los alumnos tendrán permitido el acceso, lectura y modificación mediante esta ACL de tipo “Allow” sobre el grupo “Primeros”.

Who *
Group

Group *
Primeros

ACL Type *
Allow

Permissions Type *
Basic

Permissions *
Modify

Flags Type *
Basic

Flags *
Inherit

ADD ACL ITEM DELE

Access Control List

Who *
Group

Group *
Segundos

ACL Type *
Deny

Permissions Type *
Basic

Permissions *
Read

Flags Type *
Basic

Flags *
Inherit

Por último se denegará el acceso y la lectura al grupo “Segundos” sobre el Volumen 1, creando un ítem de tipo “Deny”.

Al igual que antes, en Who tendremos que seleccionar “Group” y en el desplegable seleccionar el grupo de “Segundos”.

Usaremos también la opción avanzada para usar estos permisos y tablas ACL recursivamente en los directorios que se creen en el Volumen 1 y a los dataset hijos que creamos bajo él, para no tener así que volver a repetir lo mismo.

Advanced

☒ Apply permissions recursively

☒ Apply permissions to child datasets

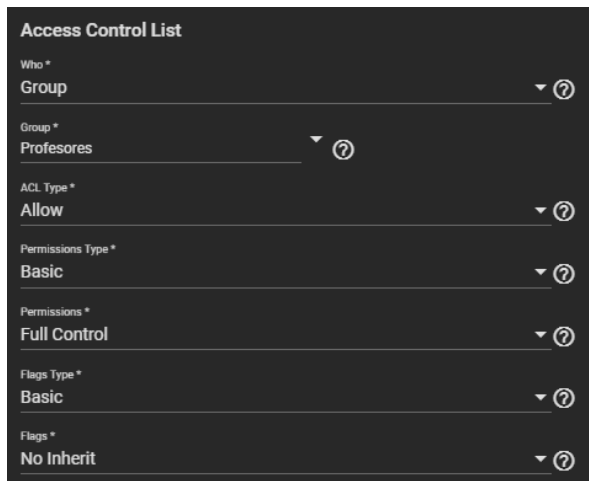
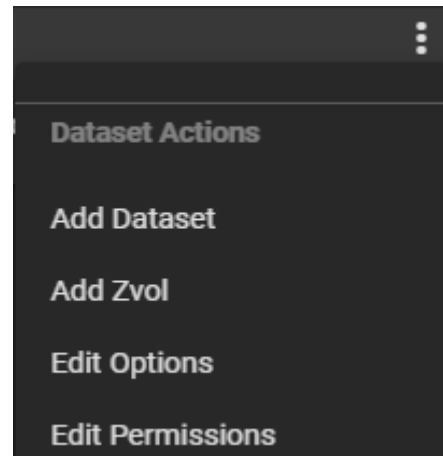
Después de esto, podremos guardar los cambios con el botón azul de “Save”, y nuestro Volumen 1 estará listo.



b. Volumen 2

El Volumen 2 está pensado para que tengan acceso los alumnos de los “Segundos”, y, que a su vez, los profesores también tengan control total sobre este mismo volumen.

Para editar sus permisos y trabajar con sus ACL, clickaremos en sus tres puntos de configuración y después en “Edit Permissions”. En esta misma ventana, igual que con el volumen 1, clickaremos en “Use ACL Manager”.

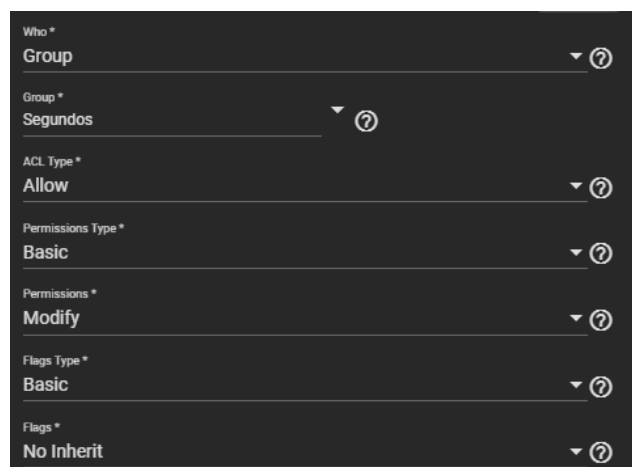


El Item de la ACL de los profesores será la misma que antes. El “Who” será sobre un grupo, y en el desplegable debemos seleccionar el grupo de “Profesores”.

El tipo de ACL será “Allow” para permitir el control total (Full control) sobre el Volumen 2 al grupo de profesores.

Al contrario que con el volumen anterior, ahora será el grupo de “Segundos” el que tendrá una ACL de tipo “Allow” para permitir el acceso, lectura y modificación al Volumen 2.

Esto lo haremos seleccionando el permiso de modificar.





Who *
Group

Group *
Primeros

ACL Type *
Deny

Permissions Type *
Basic

Permissions *
Read

Flags Type *
Basic

Flags *
No Inherit

Por último, para denegar el acceso y la lectura de los datos del Volumen 2 a los alumnos del grupo “Primeros”, crearemos otro ACL Item, de tipo denegar o “Deny”, y con que en los permisos de tipo básico le indiquemos la lectura, cualquier usuario de ese grupo ya no podrá leer ni ver los datos del Volumen 2.

c. Permisos avanzados

- ☒ Read Data
- ☐ Write Data
- ☐ Append Data
- ☒ Read Named Attributes
- ☐ Write Named Attributes
- ☒ Execute
- ☐ Delete Children
- ☒ Read Attributes
- ☐ Write Attributes
- ☐ Delete

Si deseamos una mayor precisión respecto a los permisos o privilegios que tenga un grupo o un usuario sobre un dataset, podemos usar el tipo de permisos avanzado. Seleccionando “Advanced” en el “Permissions Type” del ACL Item que deseemos, podremos elegir qué podrá o no hacer el usuario o grupo.

Diferenciando entre leer, escribir, ejecutar, eliminar etc. Con esto podemos ser más concretos y precisos a la hora de crear tablas ACL.

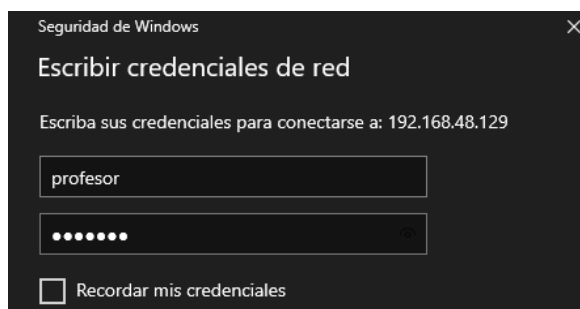
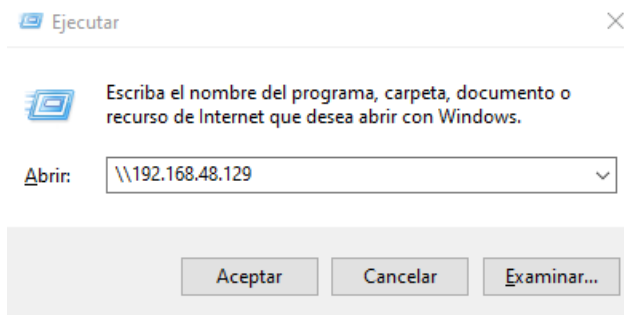
10. Comprobación de usuarios y SMB

La actividad pide que se compruebe el funcionamiento del NAS y que se refleje en el documento, así que este apartado se basará en probar y demostrar el correcto funcionamiento de todos los usuarios a través de Windows. Con todo lo que se ha hecho hasta ahora, podremos conectarnos a través del explorador de archivos de cualquier Windows, identificarnos como cualquier usuario de los creados y acceder a los volúmenes que estamos compartiendo con SMB.



a. Profesores

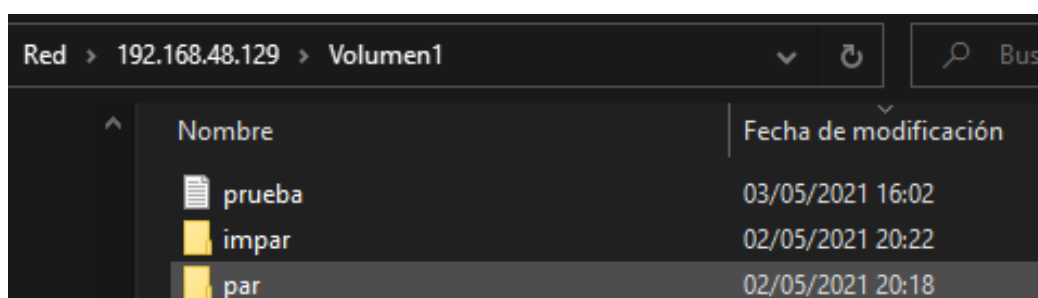
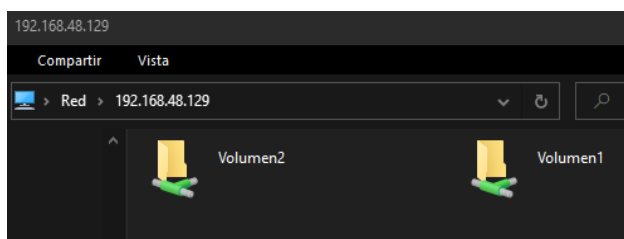
Comenzaremos demostrando que los usuarios del grupo Profesores tendrán control sobre los datos de ambos volúmenes. Para conectarnos con el dispositivo NAS a través de nuestra red local podemos escribir su dirección IP local en la ventana de ejecutar.



Una vez se conecte, que será de forma instantánea, nos pedirá credenciales.

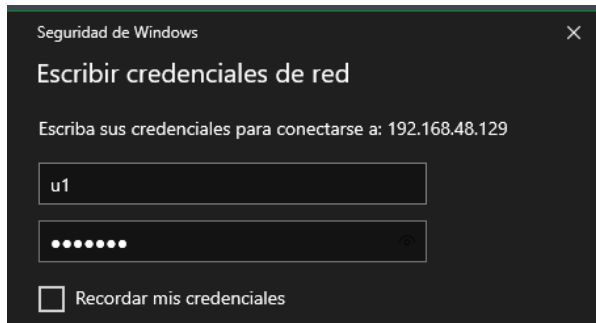
En este caso iniciaremos sesión con uno de los usuarios del grupo Profesores.

Una vez hemos iniciado sesión con este usuario, podremos acceder a cualquiera de los dos volúmenes, ver su contenido, crear contenido nuevo, eliminar y modificar.



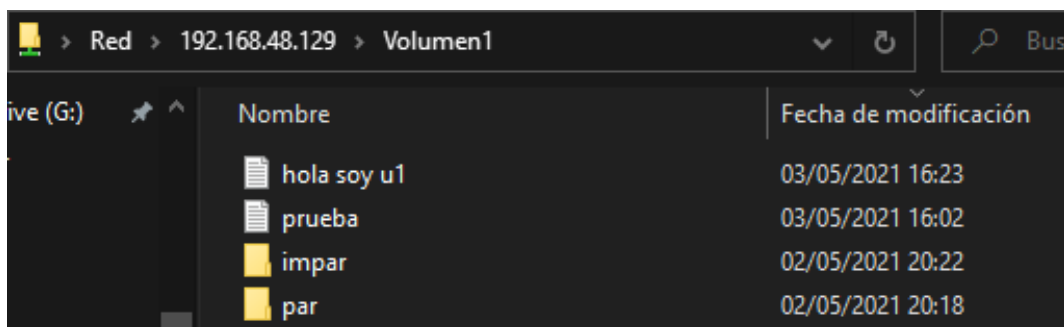


b. Grupo “Primeros”

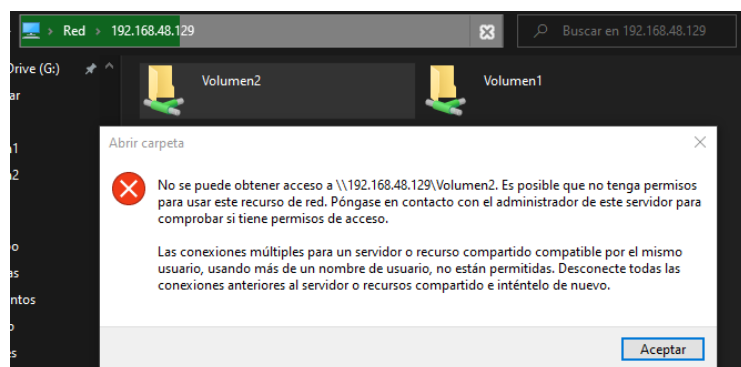


Igual que hemos comprobado que todo está correcto con el grupo de Profesores, lo haremos con el grupo de Primeros. Para ello accederemos al NAS pero con los credenciales del usuario 1 (perteneciente al grupo de Primeros).

Si accedemos al Volumen 1 no nos dará ningún problema, y podremos incluso crear archivos, moverlos, editarlos y ver los datos que hay en todo el volumen, entre los que están el que creó el profesor anteriormente.

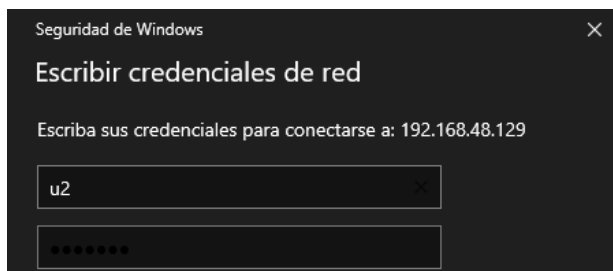


Por el contrario, si intentamos acceder al Volumen 2 con doble click, se nos denegará el acceso y Windows nos avisará de que no tenemos permisos para ello.



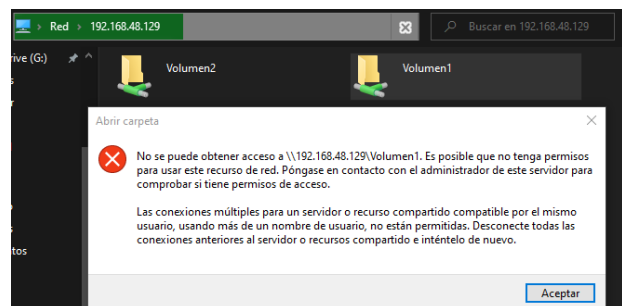


c. Grupo “Segundos”

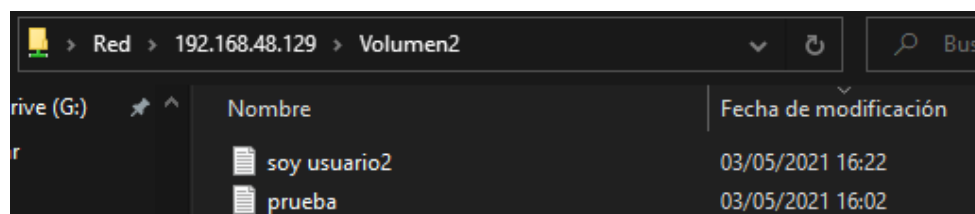


Por último comprobaremos lo mismo pero con el Usuario 2 (u2), que pertenece al grupo de “Segundos”. Como en los casos anteriores, iniciaremos sesión con sus credenciales.

Una vez hemos accedido al dispositivo NAS a través del usuario 2, no podremos acceder al Volumen 1, e igual que antes, nos avisará de que no tenemos permisos para realizar esa acción.



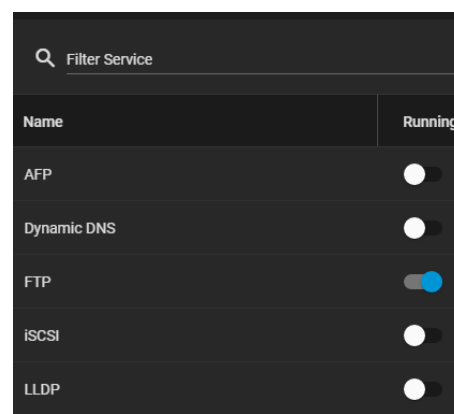
Sin embargo, sí podremos acceder al volumen 2 sin problema, leer el archivo creado anteriormente o crear y modificar otros archivos como el propio.



11. Servicio FTP

a. Activar servicio

Para que los usuarios puedan acceder al NAS, no tenemos por qué usar un servicio FTP de terceros, ya que TrueNAS tiene un servicio FTP implementado que funciona correctamente para luego conectarse desde Windows y es fácilmente configurable. Para activarlo iremos al menú de “Servicios” y clickaremos en el switch correspondiente.





General Options

Port *
21

Clients *
5

Connections *
2

Login Attempts *
1

Timeout *
600

Para configurarlo, haremos click en el icono de edición en la línea del propio servicio FTP, eso sí, después de activar el tick de “iniciar automáticamente”. El puerto por defecto es el 21, pero es recomendable cambiarlo a cualquier otro para no usar el puerto por defecto del protocolo FTP, en mi caso he puesto por ejemplo el 1702, únicamente debemos saber cuál hemos puesto para acceder al servicio posteriormente.

Tenemos la opción también de cambiar el número de clientes simultáneos máximos, las máximas conexiones con la misma dirección IP, o el tiempo de timeout.

Es muy importante marcar el tick de “Allow Local User Login” para permitir que los usuarios creados anteriormente puedan loguearse a través del protocolo FTP, ya que en caso contrario, únicamente los usuarios del grupo FTP podrán hacerlo.

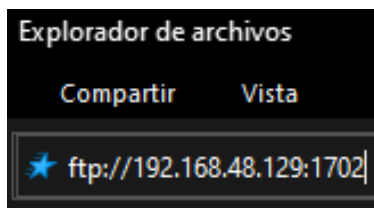
Access

☐ Always Chroot ?

☐ Allow Root Login ?

☐ Allow Anonymous Login ?

☒ Allow Local User Login ?



Una vez configurado y activo, para acceder a través de las máquinas Windows únicamente tenemos que ir al explorador de archivos y acceder a él como si fuese desde el navegador, con la dirección IP local del NAS, y el puerto separado con dos puntos. Todo esto después de “ftp://” para indicar el protocolo.

De esta forma, podremos iniciar sesión con uno de los usuarios y con su respectiva contraseña, usando un protocolo FTP gracias al servicio FTP del propio TrueNAS, sin usar software de terceros.

Archivo Inicio Compartir Vista

← → ↕ ↗ > Internet > 192.168.48.129

Iniciar sesión como

El servidor no permite los inicios de sesión anónimos o no se aceptó la dirección de correo electrónico.

Servidor FTP: 192.168.48.129

Usuario: [dropdown]

Contraseña: [input]



b. Demostración de funcionamiento

Iniciar sesión como

Escriba un nombre de usuario y una contraseña para iniciar la sesión en este servidor FTP.

Servidor FTP: 192.168.48.129

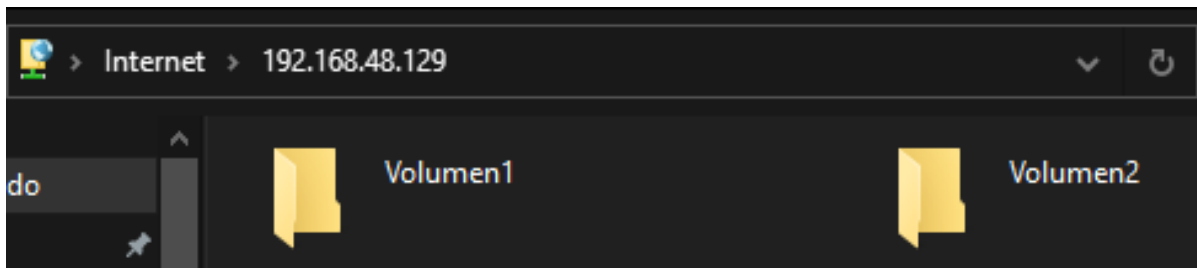
Usuario:

Contraseña:

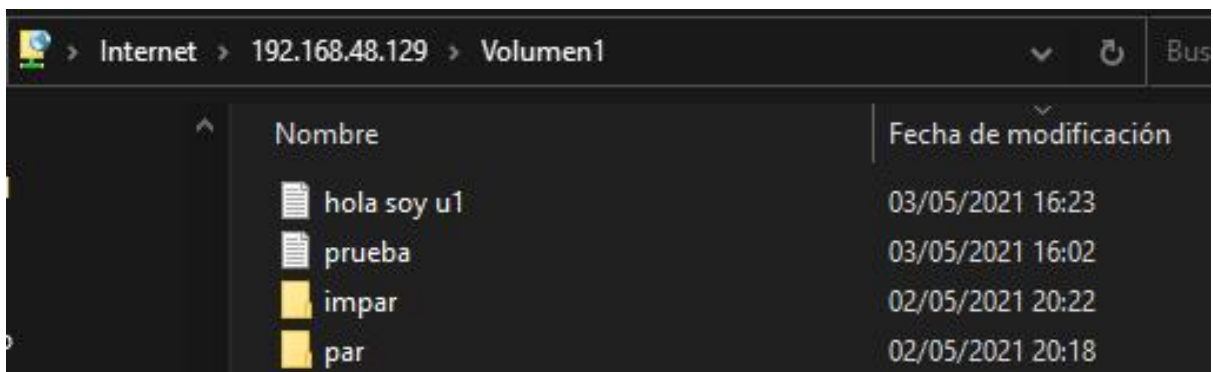
Una vez que inicie sesión, puede agregar este servidor a sus favoritos y volver a él fácilmente.

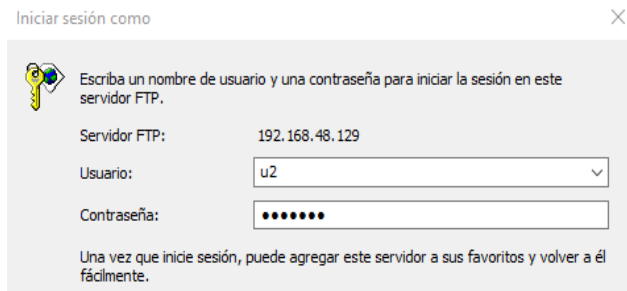
Al igual que en los casos anteriores, el siguiente subapartado está destinado únicamente a demostrar que el servicio FTP de TrueNAS activo funciona correctamente.

Tras iniciar sesión con los credenciales del usuario Profesor podemos observar las dos carpetas que representan al Volumen 1 y al Volumen 2.



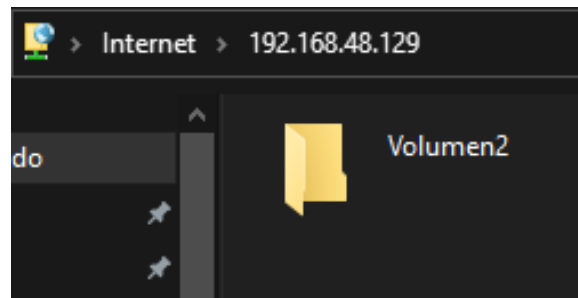
Al igual que antes, podemos acceder a ambos volúmenes y leer, modificar y editar el contenido que hay en su interior, así como añadir contenido nuevo. Es decir, seguimos teniendo los mismos permisos en el usuario que cuando usábamos SMB.





Si iniciamos sesión como uno de los usuarios del grupo “Primeros” o del grupo “Segundos”, el funcionamiento es correcto, igual que con SMB. Lo demostraremos por ejemplo con el Usuario 2 (u2).

Una vez hayamos iniciado sesión con sus credenciales, podremos ver y acceder al Volumen 1, la diferencia con cómo nos aparecía en SMB, es que ahora el usuario 2 no será consciente de la existencia del Volumen 1.



Este proceso se ha realizado usando el **cliente FTP de Windows**, a través de su Explorador de archivos, con lo que no necesitamos software de terceros como Filezilla para mover archivos entre el servidor NAS y el equipo que esté conectado.

12. Cuotas de disco por usuario

a. Establecer cuotas

Tras horas de análisis por el [foro oficial](#) de Truenas y por la [documentación](#), he considerado usar la línea de comandos para realizar esta acción, y no la interfaz gráfica.

Usando el siguiente comando de FreeBSD podemos establecer cuotas de uso de disco máximas para cada usuario en cada volumen o dataset: `zfs set userquota@domain\user=1G Volumen`. (Ejemplo con 1GB de cuota).

```
root@truenas[~]# zfs set userquota@u1=500M Datos/Volumen1
root@truenas[~]#
root@truenas[~]# zfs set userquota@u2=300M Datos/Volumen2
root@truenas[~]#
```

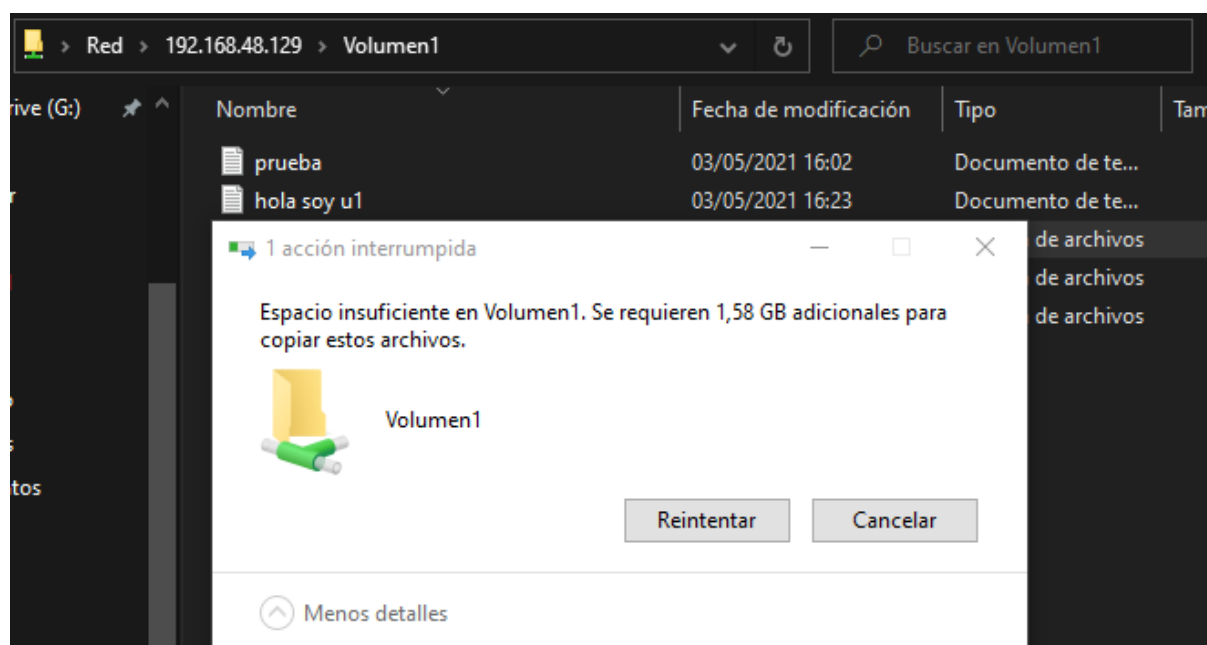


b. Demostración de funcionamiento

Con los comandos de la imagen superior hemos establecido una cuota límite de 500 MB para el Usuario 1 en el Volumen 1, y 300 MB para el Usuario 2 en el Volumen 2.

Para comprobarlo, únicamente tenemos que conectarnos al NAS a través del explorador de archivos con uno de los dos usuarios, y al intentar pasar un archivo más grande que la cuota límite de uso de disco, nos indicará que no hay espacio suficiente.

En este caso, la prueba la estoy haciendo el Usuario 1 intentando pasar un archivo de unos 2GB al Volumen 1.

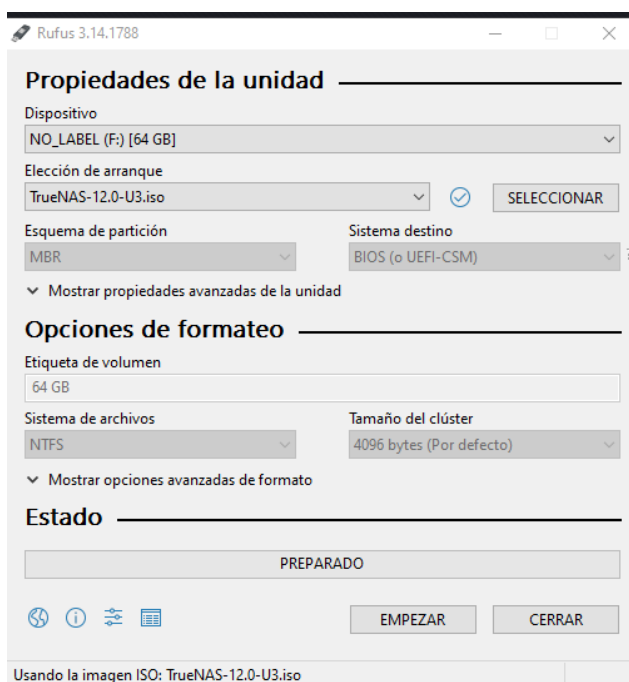
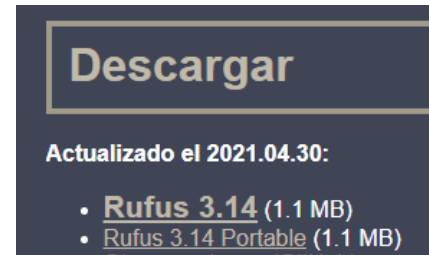




13. Anexos

a. Quemar ISO en un Pendrive

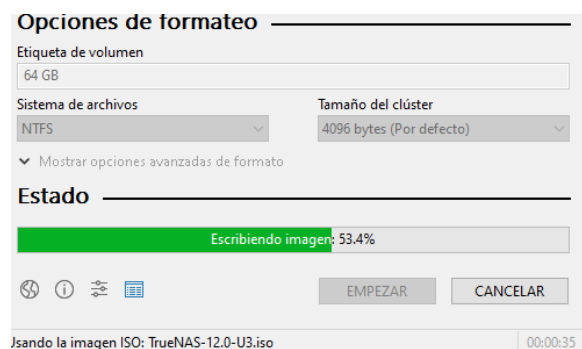
Para conseguir que cualquier archivo ISO se pueda iniciar desde una unidad USB como un Pendrive, debemos “quemar” esa ISO mediante un software como Rufus. Podemos descargar el ejecutable de este software en su sitio web oficial.



Una vez hayamos iniciado el software de Rufus o similares, debemos seleccionar nuestro Pendrive como dispositivo, e indicar la ruta de descarga de la ISO de TrueNAS para que la use como elección de arranque.

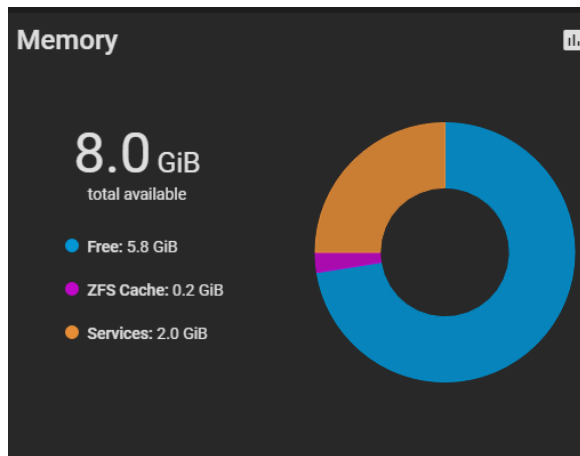
A continuación y una vez revisado que el sistema de destino deberá ser BIOS o UEFI-CSM, y que lo creará con un esquema de partición MBR, podemos darle al botón de “Comenzar”.

Rufus comenzará borrando los datos y las particiones de la unidad USB con la que estamos trabajando, y estará unos segundos copiando los archivos necesarios. Dependiendo de la velocidad de la unidad, del disco duro y del puerto USB, tardará unos segundos o unos minutos.





b. Recursos de la máquina virtual



Tras la realización de la práctica y las pruebas del dispositivo NAS en la máquina virtual, he comprobado que los recursos recomendados por TrueNAS son bastante altos, y en una máquina sencilla que no usen muchos usuarios de forma simultánea y que no tenga gran cantidad de discos duros, con 4GB de RAM puede funcionar sin problema.

El mayor uso de RAM que he tenido durante el proceso ha sido de 3 GiB, por tanto con 4GB deberíamos tener suficiente para los servicios y para el caché en un uso doméstico normal, aunque no sea recomendable en uso más profesional.

Key	Min	Mean	Max
Wired :	0	679.53 MiB	747.73 MiB
Inactive :	707.54 MiB	836.68 MiB	893.03 MiB
Laundry :	96.05 MiB	115.17 MiB	145.54 MiB
Active :	1.04 GiB	1.08 GiB	1.1 GiB
Free :	6.85 GiB	6.91 GiB	7.04 GiB

Key	Min	Mean	Max
Interrupt :	0	0.01	0.09
System :	0	0.51	2.58
User :	0	0.56	3.36
Nice :	0	0.56	3.36
Idle :	0	95.84	100

Key	Min	Mean	Max
Shortterm :	0.03	0.54	1.59
Midterm :	0.3	0.5	0.73
Longterm :	0.21	0.4	0.57

Respecto al CPU, en ningún momento he observado una carga superior al 23%.

Aunque son únicamente 2 núcleos físicos y 2 hilos en cada uno, que es lo que tiene un dispositivo NAS físico de gama baja, estamos hablando de un Ryzen con arquitectura Zen 2 a más de 4Ghz.

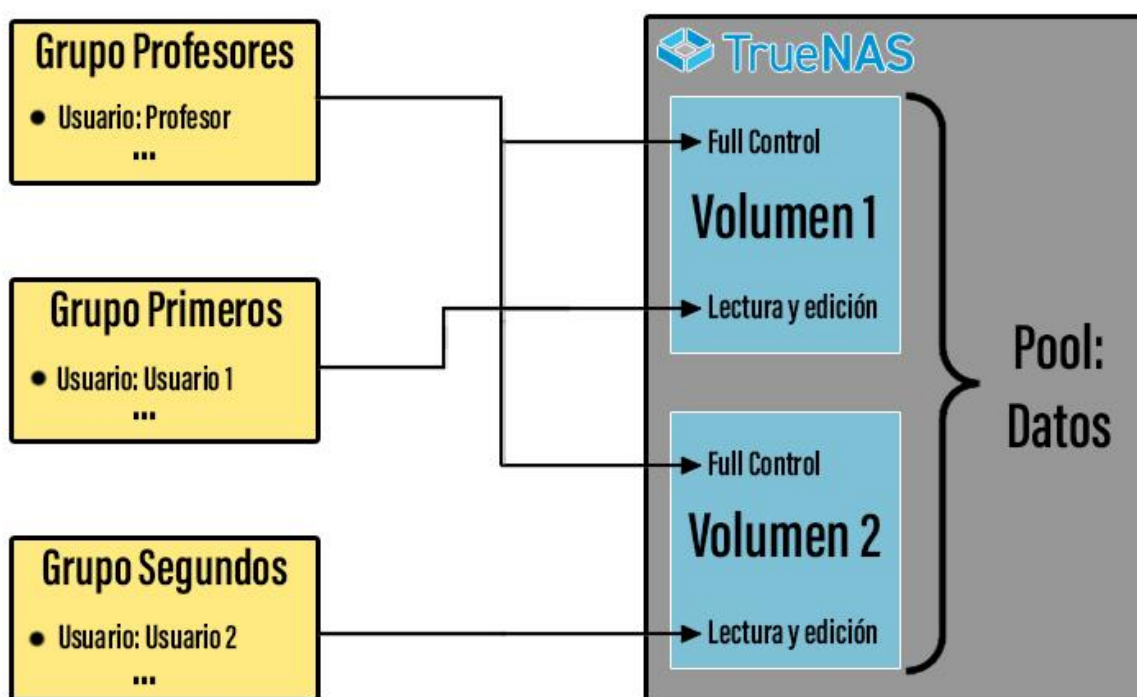
Por tanto con este tipo de rendimiento mononúcleo, 1 solo núcleo físico con 2 hilos de procesamiento es más que suficiente.



c. Documento de configuración de servidor

El dispositivo NAS consta de un pool de Datos, formado por tres discos duros en Raid 5.

Este pool de Datos estará formado por dos dataset, llamados Volumen 1 y Volumen 2, tal y como se puede observar en el siguiente diagrama realizado en Photoshop.



Existirán tres grupos, uno destinado para los profesores, otro para los alumnos de primer curso y otro para los alumnos de segundo curso.

Los profesores tendrán control total sobre los datos ambos volúmenes, mientras que, el grupo de los alumnos de primer curso llamado “Primeros”, tendrá permiso de lectura y de edición únicamente sobre el Volumen 1.,

Por otro lado, el grupo de los alumnos de segundo curso llamado “Segundos” tendrá permiso de lectura y edición sobre el Volumen 2 y sus datos.



En la siguiente tabla se muestran los usuarios, los grupos, sus contraseñas y los permisos básicos que les darán acceso a ciertos volúmenes.

Usuario	Grupo	Contraseña	Permisos en:
Profesor	Profesores	usuario	Volumen 1 y 2
Usuario 1 (u1)	Primeros	usuario	Volumen 1
Usuario 2 (u2)	Segundos	usuario	Volumen 2

Jorge Navarrete, 1º ASIR.