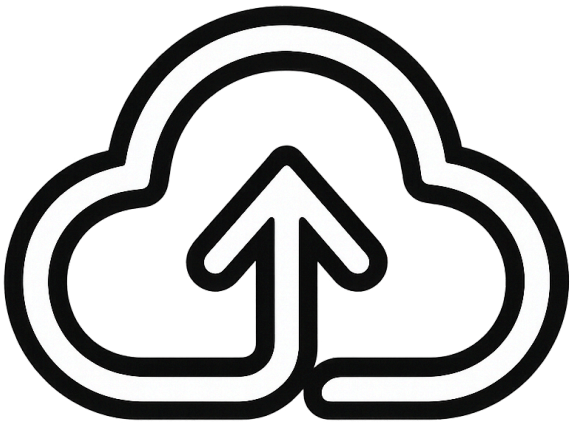


CONFIGURACIÓN SERVIDOR SECUNDARIO

ALMACENAMIENTO DE DATOS (TrueNAS CORE)

Introducción

Este documento describe la arquitectura, despliegue y configuración de el servidor secundario dedicado exclusivamente a funciones de almacenamiento, basado en el sistema operativo **TrueNAS CORE**, una distribución de código abierto especializada en almacenamiento en red (NAS) basada en FreeBSD y en el sistema de archivos **ZFS**.

El objetivo principal de este servidor es proveer **almacenamiento persistente** para los datos de los contenedores Docker desplegados en el servidor principal de cómputo. Para ello, se emplea el protocolo **iSCSI (Internet Small Computer System Interface)**, que permite exponer volúmenes de almacenamiento remotos como si fueran dispositivos locales en el servidor principal.

El diseño de esta arquitectura desacoplada, donde el servidor de cómputo y el servidor de almacenamiento trabajan de forma independiente, presenta numerosas ventajas:

- **Escalabilidad:** permite ampliar los recursos de almacenamiento sin afectar el nodo de cómputo, o viceversa.
- **Rendimiento dedicado:** el servidor de almacenamiento se optimiza para operaciones de E/S, liberando al servidor principal de dicha carga.
- **Alta disponibilidad y resiliencia:** mediante snapshots, replicación y redundancia de datos en el almacenamiento.
- **Gestión centralizada:** el almacenamiento se administra desde un único punto con herramientas especializadas como la interfaz web de TrueNAS, incluyendo soporte para monitorización, alertas, ACLs y snapshots automáticos.

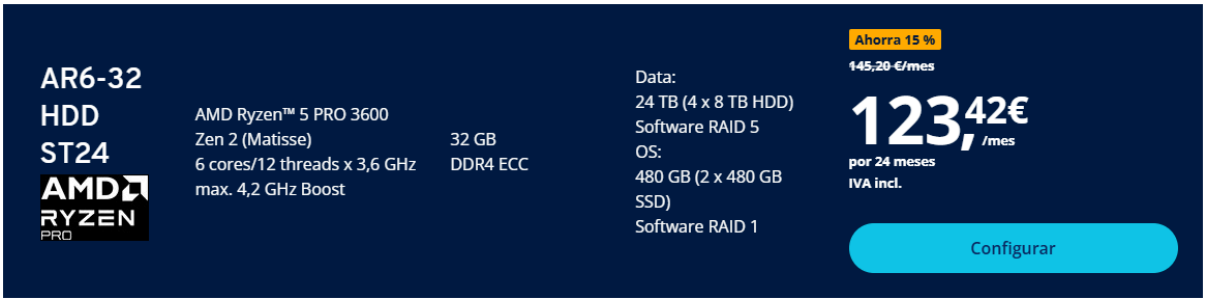
En resumen, este entorno proporciona una solución robusta y profesional para entornos multiusuario y multicliente donde se requiere almacenamiento fiable, centralizado, fácilmente escalable y gestionado con criterios de alta disponibilidad y seguridad.

Especificaciones del Servidor

El servidor se contrata a través de Ionos por un coste mensual de 145,20 € y presenta las siguientes características:

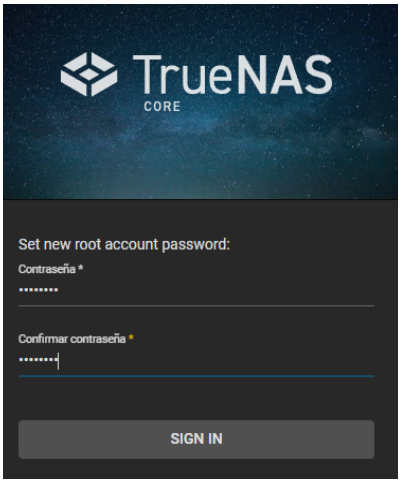
- **CPU:** AMD Ryzen™ 5 PRO 3600 (6 núcleos / 12 hilos, 3,6 GHz).
- **RAM:** 32 GB DDR4 ECC, lo que garantiza corrección de errores para mejorar la fiabilidad en un entorno de almacenamiento.
- **Almacenamiento:**
    - **Datos:** 24 TB útiles mediante 4 discos HDD de 8 TB configurados en RAID 5.
    - **SO:** 480 GB en RAID 1 con 2 SSD de 480 GB, asegurando redundancia y rápida recuperación.

Sistema Operativo: TrueNAS CORE (anteriormente FreeNAS).



Instalación de TrueNAS CORE

Tras contratar el servidor, se selecciona la imagen ISO de TrueNAS CORE.



Una vez instalado el sistema operativo, se podrá acceder a la interfaz web de administración mediante la IP pública del servidor usando el puerto 443 (HTTPS habilitado por defecto), lo que proporciona acceso seguro.

En el primer inicio se solicita establecer la contraseña para el usuario root.

Configuración del Almacenamiento

Una vez finalizada la instalación de TrueNAS CORE y tras acceder mediante la interfaz web de administración, se procede a la configuración detallada del sistema de almacenamiento. Este servidor dispone de una capacidad total de 32 TB (4 discos de 8 TB cada uno), que se ha configurado en **RAID 5** mediante ZFS, el sistema de archivos nativo de TrueNAS.

RAID 5 con ZFS

La elección de RAID 5 proporciona una buena combinación entre rendimiento y tolerancia a fallos. En este nivel de RAID, uno de los discos se reserva para almacenar información de paridad distribuida, permitiendo de esta forma la recuperación de los datos en caso de que falle alguno de los discos. De esta forma, de los 32 TB totales disponibles, se obtiene una capacidad útil aproximada de 24 TB, lo cual maximiza la cantidad de almacenamiento manteniendo una redundancia básica, previniendo así la pérdida de datos.

Zettabyte File System (ZFS), además de implementar el RAID de forma nativa, añade funciones importantes para cualquier entorno de almacenamiento moderno:

- Integridad de datos de extremo a extremo mediante checksums.
- Detección y corrección automática de errores silenciosos (bit rot).
- Snapshots, clones y replicación incorporados en el sistema de archivos.
- Compresión y deduplicación (opcional) para optimizar el uso del espacio.
- Gestión avanzada de pools y volúmenes virtuales con escalabilidad vertical y horizontal.

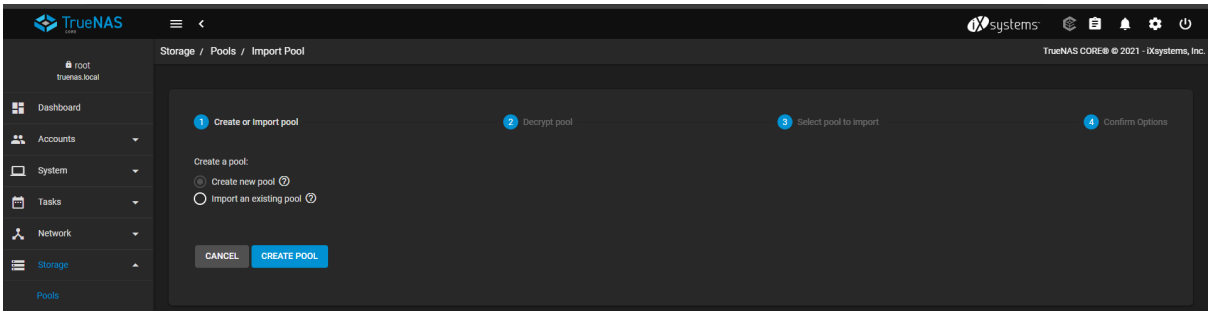
Pool de Datos

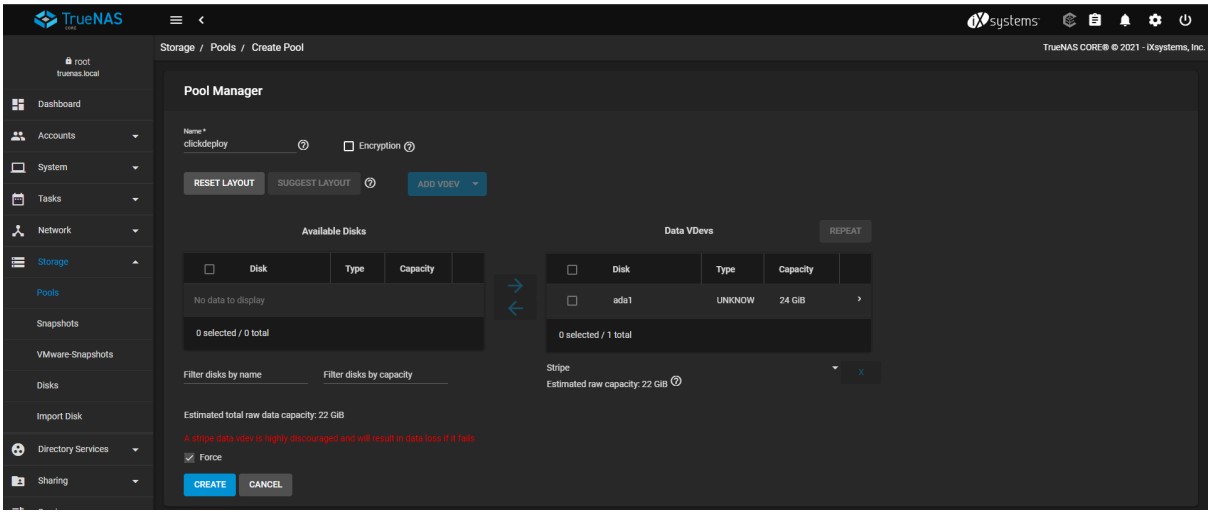
El primer paso es la creación del **pool de almacenamiento ZFS**, que agrupará físicamente los discos duros y actuará como el entorno de almacenamiento base. En este caso, se crea un pool con el nombre **clickdeploy**, el cual aloja múltiples volúmenes virtuales **(ZVols)** destinados a distintos fines dentro del proyecto:

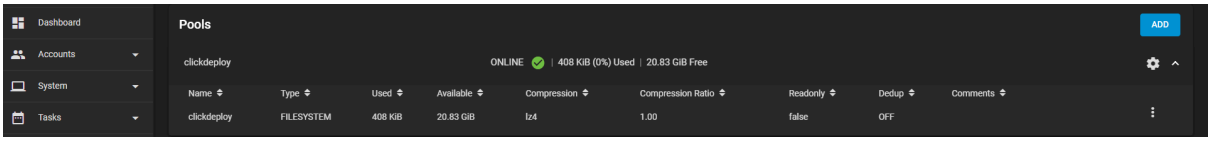
- Alojamiento persistente para contenedores Docker.
- Almacenamiento de copias de seguridad periódicas.

Se realiza la configuración desde el menú **Storage > Pools** en la interfaz de TrueNAS, se elige la capacidad máxima, 24 TB, ya que el servidor cuenta con RAID 5, de forma que:

- Optimiza la eficiencia del almacenamiento (75% del espacio total disponible).
- Mantiene la tolerancia a fallos de un disco.
- Facilita la expansión futura del pool agregando nuevos vdevs.







Volumen para contenedores

Dentro del pool clickdeploy, el primer recurso que se configura es un ZVol (ZFS Volume) de 10 TB, específicamente dedicado al almacenamiento persistente de los contenedores Docker desplegados y ejecutados en el servidor principal.

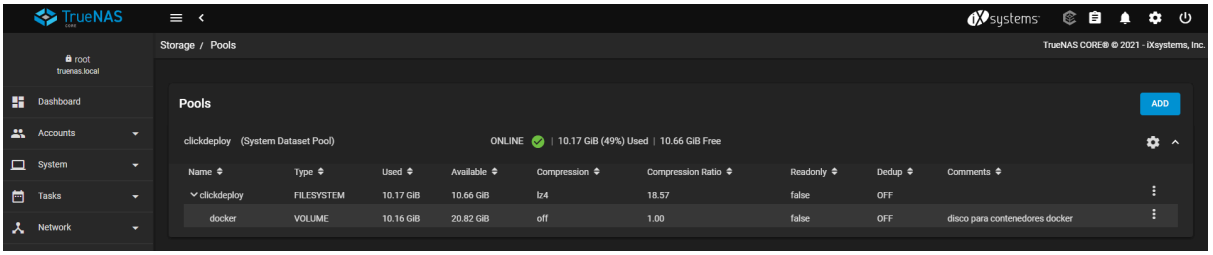
Un **ZVol** en ZFS representa un **dispositivo de bloque virtual**, que puede ser exportado a través de protocolos como **iSCSI**, lo que lo convierte en una opción de las más interesantes para servidores o sistemas que actúan como cliente que necesitan formatear el volumen con su propio sistema de archivos, en este caso **EXT4**, desde el nodo principal de cómputo. Esto es esencial cuando se gestionan múltiples contenedores con distintos orígenes de datos, como bases de datos MySQL, documentos en Nextcloud o archivos multimedia.

El volumen está pensado para **almacenar** los datos de **todos** los **contenedores** docker.

Configuraciones clave del ZVol:

- **Tamaño fijo:** 10 TiB asignados directamente para evitar sobreaprovisionamiento.
- **Bloque de tamaño:** 16K (recomendado para sistemas de archivos tipo EXT4 y aplicaciones que realizan lecturas/escrituras en bloques pequeños).
- **Thin Provisioning** (deshabilitado): se preasigna el tamaño completo del ZVol para asegurar rendimiento constante y evitar fragmentación.
- **Compression:** habilitado con algoritmo lz4, proporcionando ahorro de espacio sin penalización de rendimiento notable.

Gracias al protocolo iSCSI, este ZVol es visible como un disco físico en el servidor principal, donde se puede formatear, montar y usar como cualquier dispositivo local.



Volumen para backups

El segundo volumen virtual creado dentro del mismo pool clickdeploy es un **ZVol** de **14 TB**, destinado exclusivamente al **almacenamiento de copias de seguridad** tanto de los contenedores como de las bases de datos y configuraciones relevantes de Clickdeploy.

Este volumen tiene como objetivo centralizar y retener de forma segura los respaldos programados y manuales, permitiendo restauraciones rápidas ante fallos o corrupción de datos. Al ser gestionado desde TrueNAS, el volumen también tiene acceso a:

- **Snapshots programados:** que permiten mantener versiones incrementales y eficientes.
- **Compresión automática:** con algoritmos ligeros como **lz4** o **zstd** para reducir el espacio ocupado sin impactar el rendimiento.
- **Replicación futura:** posibilidad de replicar el ZVol completo a un servidor terciario o NAS externo para políticas de copia fuera del sitio (offsite backup).

Este ZVol puede exportarse vía iSCSI, NFS o SMB al servidor principal. En este caso se opta por mantenerlo aislado siempre que no se hagan copias de seguridad.
Las estrategias de copia pueden incluir:

- Copias completas semanales.
- Versionado de archivos y bases de datos.
- Archivos comprimidos y cifrados para clientes específicos.

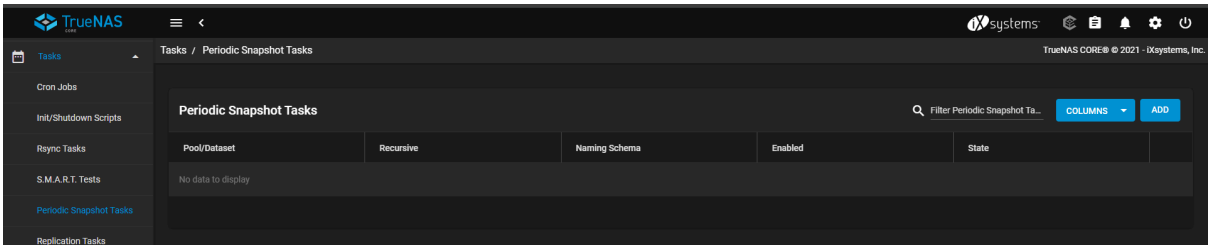
Adicionalmente, la separación lógica entre datos activos (contenedores) y copias de seguridad garantiza una arquitectura más segura, permitiendo aplicar políticas de retención y cifrado específicas a los backups, sin interferir en el rendimiento de los contenedores en producción.

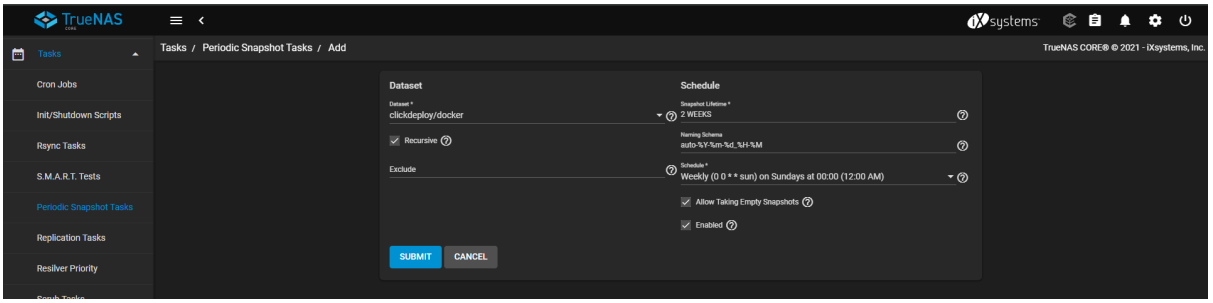
Snapshots y Replicación

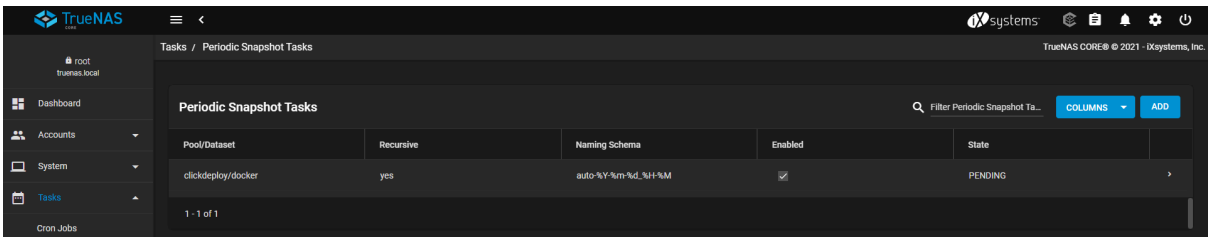
Para asegurar la integridad de los datos y facilitar la recuperación ante fallos, se configuran tareas periódicas de snapshots:

- Frecuencia: Semanal.
- Retención: 2 semanas.

Estas copias se gestionan desde el módulo Tasks > Periodic Snapshot Tasks de TrueNAS, permitiendo versiones históricas de los datos sin afectar el rendimiento.







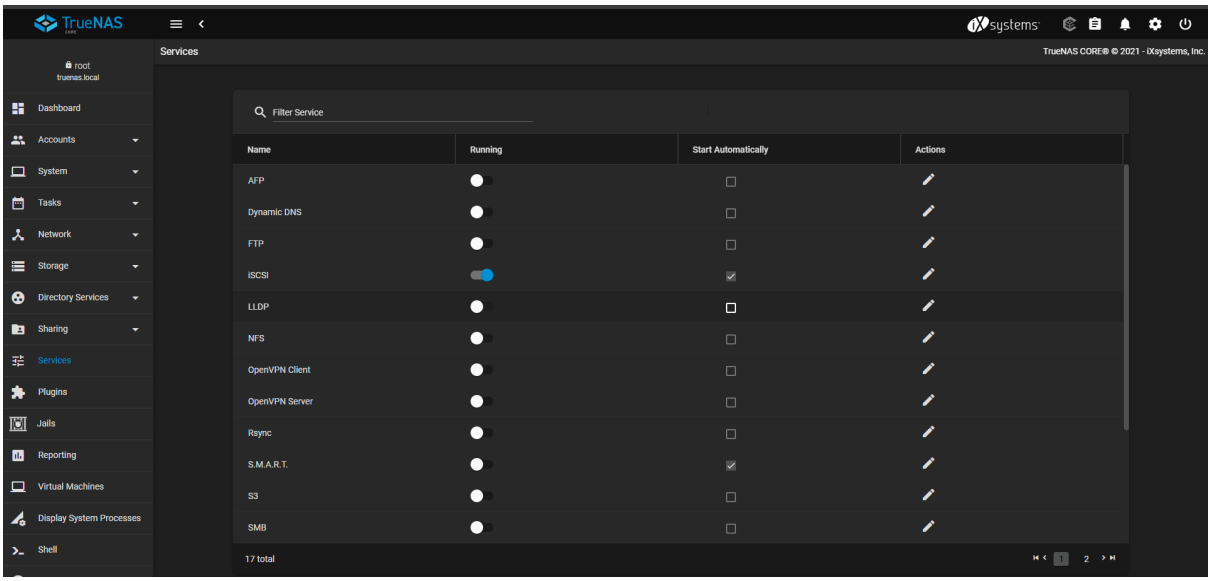
Configuración del Servicio iSCSI

Para que el servidor principal acceda al volumen de contenedores como si fuese un disco local, se habilita y configura el servicio iSCSI en TrueNAS:

Habilitar iSCSI

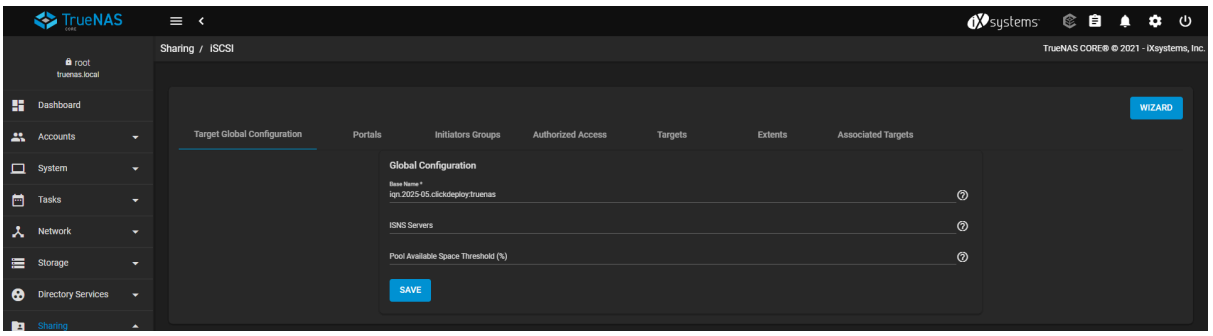
Navegar a **Services > iSCSI.**

Activar el servicio y marcar como “Start Automatically”.



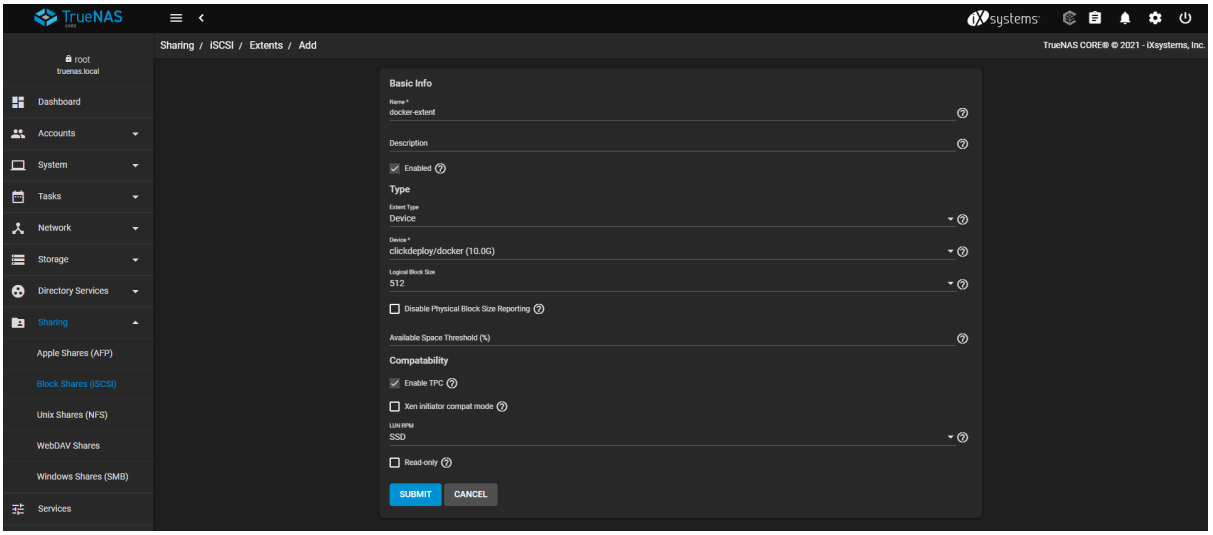
Configurar Target Global

Se define una configuración global para el target iSCSI, especificando parámetros generales como el nombre base IQN y las opciones predeterminadas para las conexiones.



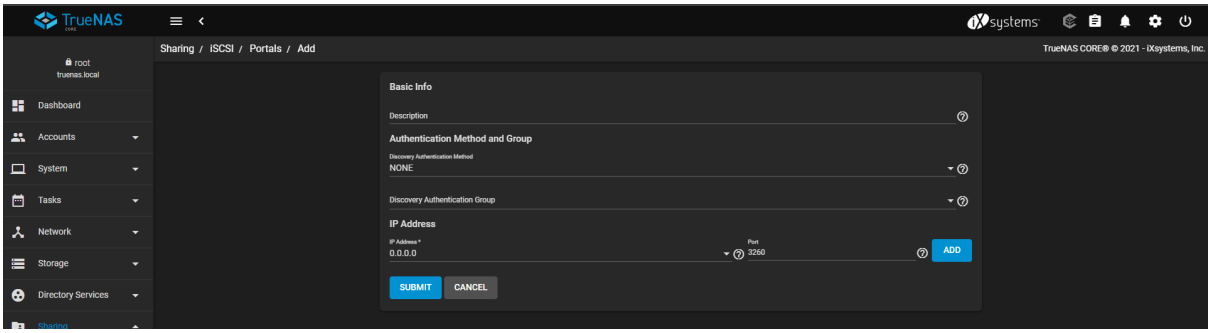
Crear Extent

Se crea un Extent que vincula el ZVol (10 TB para contenedores) con el sistema iSCSI, definiendo el tipo como "Device" y seleccionando el ZVol como backend.



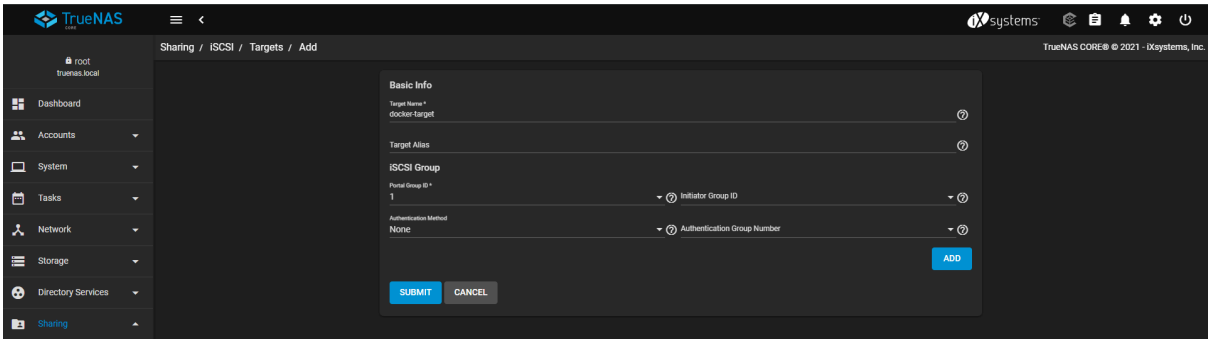
Crear Portal

Un portal iSCSI define la IP y puerto de escucha. Se configura para aceptar conexiones en la IP del servidor y el puerto estándar 3260.



Crear Target

Se crea un Target asociado al Extent y al Portal previamente definidos. El Target representa el punto de acceso lógico que usará el servidor principal.



Seguridad

La protección del servidor secundario es una prioridad absoluta, dado que actúa como repositorio crítico de datos persistentes para todos los servicios desplegados. Al estar expuesto a redes públicas y operar en una arquitectura cliente-servidor mediante iSCSI, es necesario aplicar un enfoque de defensa en profundidad, implementando múltiples capas de seguridad a nivel de red, servicio y sistema operativo.

Firewall con pf: Control de tráfico perimetral estricto

Se utiliza pf (Packet Filter) como cortafuegos nativo del sistema operativo FreeBSD (en el que se basa TrueNAS CORE). Packet Filter es la versión alternativa a ntables (disponible en Debian) del sistema operativo FreeBSD. La política del firewall se establece por defecto en block, permitiendo únicamente el tráfico explícitamente autorizado desde el servidor principal. Esto previene escaneos de puertos e intentos de acceso no autorizados

1. Configuración del archivo /etc/pf.conf:

```
ext_if="em0"
allowed_ip="(ip.del.servidor.principal)"

# Política por defecto: bloquear todo
set block-policy drop
set skip on lo
block in all
block out all

# Permitir solo desde IP del servidor principal
pass in quick on $ext_if from $allowed_ip to any port ssh
pass in quick on $ext_if from $allowed_ip to any port 3260
pass in quick on $ext_if from $allowed_ip to any port 443
pass in quick on $ext_if from $allowed_ip to any port 80

# Permitir tráfico saliente solo hacia el servidor principal
pass out quick on $ext_if from any to $allowed_ip
```

2. Activación del firewall y aplicación de reglas:

```
sysrc pf_enable="YES"
service pf start
pfctl -f /etc/pf.conf
```

Esta configuración garantiza que únicamente el servidor principal pueda comunicarse con el servidor de almacenamiento, ya sea para montar volúmenes iSCSI, acceder a la interfaz web o gestionar el sistema vía SSH. De esta forma, para poder configurar o trabajar de cara al servidor de almacenamiento, se requiere un túnel ssh desde el servidor principal

Protección contra Fuerza Bruta: sshguard

Para prevenir ataques de fuerza bruta dirigidos al servicio SSH, se implementa **sshguard**, una herramienta ligera pero eficaz que analiza los logs del sistema en tiempo real y bloquea automáticamente las direcciones IP que exceden un número configurable de intentos fallidos de autenticación.

Instalación y activación:

```
pkg install sshguard
sysrc sshguard_enable="YES"
service sshguard start
```

sshguard se integra con el firewall del sistema (pf) y deniega tráfico desde IPs hostiles.Esto añade una capa de seguridad dinámica, reforzando la configuración estática del firewall. sshguard es la alternativa a Fail2ban, desarrollada para trabajar sobre FreeBSD.

Fortalecimiento del servicio SSH

El servicio SSH es el principal método de acceso y de administración remota del servidor, por lo que se refuerza mediante restricciones tanto de acceso como de configuración.

Se edita **/etc/ssh/sshd_config** para limitar el acceso SSH:

```
# Restringir acceso, solo al usuario desde la IP del servidor
AllowUsers david@(ip.del.servidor.principal)

PermitRootLogin no
ChallengeResponseAuthentication no

# Mejorar rendimiento y privacidad
UseDNS no

PermitEmptyPasswords no
MaxAuthTries 3
```

Reinicio del servicio para aplicar cambios:

```
service sshd restart
```

Con esta configuración, solo un usuario autorizado puede iniciar sesión desde una dirección IP específica. Además, se evita el uso de contraseñas vacías, se desactiva la resolución de nombres para reducir el tiempo de conexión y se limita el número de intentos de acceso fallido,que junto a sshguard, mitiga los ataques de diccionario.

Monitorización

Se implementan mecanismos de supervisión para garantizar disponibilidad y rendimiento:

- **SNMP:** Activado para integración con sistemas de monitorización.
- **Alertas:** Configuración de notificaciones por correo electrónico y/o Telegram.

Pruebas de Conectividad y Rendimiento

Desde el servidor principal se prueba la conectividad iSCSI:

```
iscsiadm -m discovery -t sendtargets -p ip.del.servidor.secundario
iscsiadm -m node --login
```

Una vez montado el volumen:

- Formatearlo con EXT4.
- Montarlo en **/mnt/iscsi-docker**.

Teniendo el volumen disponible, montado y formateado, se pueden realizar pruebas de rendimiento de conexión y lectura de datos con herramientas como:

- **fio** para IOPS y latencia.
- **dd** para pruebas secuenciales de lectura/escritura.

Conclusión

La implementación del servidor secundario mediante **TrueNAS CORE** representa un componente esencial en el diseño de la arquitectura de Clickdeploy, al asumir de forma especializada el papel de **almacenamiento centralizado y persistente** para todos los contenedores desplegados desde el servidor principal, y a mayores también cualquier tipo de información importante y la base de datos del servidor principal. Este enfoque desacoplado permite la separación de responsabilidades entre cómputo y almacenamiento de datos, lo que permite tener una infraestructura más escalable, mantenible y segura.

Gracias al uso del sistema de archivos **ZFS**, el servidor se beneficia de características avanzadas que permiten ampliar las capacidades de un sistema tradicional de archivos:

- **Integridad de datos de extremo a extremo**, con verificación de checksums y autocorrección ante corrupción.
- **Snapshots automáticos**, que permiten conservar diferentes versiones de los datos y recuperación ante errores, tanto humanos como lógicos.
- **Replicación**, pensada para futura alta disponibilidad o copias off-site.
- **Virtualización de volúmenes** (ZVols), que permite presentar dispositivos iSCSI a otros hosts de manera eficiente y dinámica.

La conexión mediante **iSCSI** garantiza que los volúmenes de almacenamiento puedan ser accesibles desde el servidor principal como si fueran dispositivos locales, asegurando transparencia para Docker y manteniendo el rendimiento necesario para aplicaciones en producción, en este caso WordPress, Moodle y Nextcloud.

A nivel de seguridad, el servidor ha sido configurado con diferentes medidas en diferentes capas: firewall **pf** con políticas restrictivas, bloqueo dinámico de intentos de fuerza bruta mediante **sshguard**, y una política más restrictiva del servicio SSH. Esta protección perimetral y multicapa, combinada con la gestión centralizada de los servicios desde TrueNAS, proporciona un sistema robusto y protegido ante amenazas externas.

Por último, la implementación de mecanismos de monitorización activa y la ejecución de distintas pruebas de rendimiento, mediante herramientas como **fio** y **dd**, han permitido asegurar la capacidad del servidor para operar en entornos productivos bajo cargas concurrentes, cumpliendo con los requisitos de fiabilidad y rendimiento del proyecto.

En conjunto, este servidor no solo actúa como un sistema de almacenamiento, sino que también se encarga de forma activa de tareas de backup y mantenimiento. Su integración con el servidor principal constituye una base sólida para, de cara a futuro, una posible expansión de Clickdeploy, tanto en volumen de clientes como en variedad de servicios ofrecidos.