

TrueNAS SCALE® Evaluation Guide

Getting Started with TrueNAS®

Chris Peredun, Technical Marketing Engineer

Document Version & Date:
V0.3 Q3-2023

Copyright 2023 iXsystems, Inc. | marketing@ixsystems.com

CONTENTS

Executive Summary
1. Welcome
2. Recommended Hardware and Preparing for Installation
    2.1 Minimum Required Hardware
    2.2 Start with a Solid Foundation
    2.3 Provide a Large Amount of RAM
    2.4 ECC RAM is Strongly Recommended
    2.5 CPU Selection is Core to your Success
    2.6 Storage Controllers
    2.7 Drive Type and Count
        2.7.1 Magnetic Hard Disk Drives (HDDs)
        2.7.1.1 Avoid Shingled Magnetic Recording (SMR) Drives
        2.7.2 Solid-State Drives (SSDs)
        2.7.3 NVMe (Non-Volatile Memory Express) SSDs
3. Creating your Install Media and Installing TrueNAS
    3.1. Choosing your Installation Method
    3.2. Creating an Install USB
    3.3. Installing TrueNAS SCALE
4. The First Boot
    4.1. Checking For DHCP - Assigning an IP Address
    4.2. Changing Hostname, setting Gateway and DNS
    4.3. Signing into the Web UI
5. Getting Started with your Storage
    5.1. Confirming Disk Count
    5.2. Build your First Pool
    5.3. Make a Dataset
    5.4. Creating a Group and a User
    5.5. Share the Dataset over SMB
6. Data Protection, Previous Versions, and Snapshot Scheduling
    6.1. Taking a Manual ZFS Snapshot
    6.2. Going Back in Time
    6.3. Automated Snapshots and Scheduling
7. Drive Failure, VDEV Removal, and Extending your Pool
    7.1. Simulating a Drive Failure
    7.2. Removing a VDEV
    7.3. Adding a VDEV
8. Replication - Local and Remote
    8.1. Important Notes - Upgrade to SCALE 22.12.2
    8.2. Local Replication
    8.3. Remote Replication - Hardware and Network Prerequisites
    8.4. Remote Replication - PUSH vs PULL Style
    8.5. Remote Replication - PUSH - Dataset & User Configuration on Destination
    8.6. Remote Replication - PUSH - Configure Replication
    8.7. Remote Replication - PULL - Dataset & User Configuration on Source
    8.8. Remote Replication - PULL - Configure Replication

CONTENTS - Continued

9. Security Best Practices
    9.1 Stay Up to Date with TrueNAS Patches
    9.2. Use Strong Passwords - and Don't Re-Use Them
    9.3. Configure Two-Factor Authentication (2FA)
    9.4. Secure the Physical Machine Itself
    9.5. Limit Access to Authorized Networks at the Protocol Level
10 Installing and Using the App Catalog
    10.1. Selecting an App Pool
    10.2. Host Path Safety Checks
    10.3. Create and Share a Dataset for Host Path Sharing
    10.4. Installing a TrueNAS SCALE App
    10.5. Assigning Storage - ixVolumes
    10.6. Assigning Storage - Host Path
    10.7. Launching Docker Images
    10.8. Removing TrueNAS SCALE Apps
    10.9. Built-In Apps
11. Wrapping Up

Executive Summary

The TrueNAS SCALE Evaluation guide provides guidelines on the installation, configuration, features, and general usage of TrueNAS SCALE. This document is not intended to replace TrueNAS Documentation, rather, it is a “springboard” or “quick start” to help a new user become familiar with TrueNAS SCALE and its features quickly and efficiently.

1 Welcome

This evaluation guide details the easy process of downloading, deploying, and evaluating TrueNAS SCALE in less than one hour. TrueNAS SCALE is free to use on your own infrastructure and is also available on a family of appliances with enterprise support. With traditional storage, evaluating its full potential is not possible without testing on proprietary hardware. This guide describes the easy steps that anyone can take, using any hardware (or virtual hardware) to experience the full potential of TrueNAS SCALE.

2 Recommended Hardware and Preparing for Installation

TrueNAS SCALE will install on almost any x86-64 hardware. For evaluation purposes, iXsystems has also made a pre-packaged OVF (Open Virtualization Format) template available for download. If you choose to install on physical hardware, we can use the information gathered by both iXsystems and the TrueNAS community to help make some optimal decisions.

2.1 Minimum Required Hardware

TrueNAS SCALE requires a minimum of a dual-core x86-64 processor, 8 GB of memory, and a 16 GB boot device. You’ll also want some additional drives to use to create your storage pool (at least two of them for a mirrored device), but four or more drives are recommended in order to make the most of the settings and scenarios demonstrated in this evaluation guide.

If you’re installing TrueNAS just to get a feel for the web UI, create and populate a few test shares, and familiarize yourself with its use and administration, the minimum resources will suffice In fact, you can even use a virtual machine provided by your favorite hypervisor, and virtual disks instead of physical. For more detailed guidance, read on!

2.2 Start with a Solid Foundation

While TrueNAS will install on just about any existing hardware, choosing a solid base system will provide the best results. Select hardware that is designed for reliability and uptime, such as an existing server or professional workstation, as these platforms tend to offer the highest potential for large amounts of primary memory (RAM), support for Error-Correcting Code (ECC) memory, multiple PCI Express (PCIe) expansion cards, and quality of life enhancements such as hot-swap drive trays and remote console access through Intelligent Platform Management Interface (IPMI).

2.3 Provide a Large Amount of RAM

TrueNAS has a higher suggested memory requirement than many other Network Attached Storage software solutions, and for good reason; the OpenZFS file system uses system RAM for a sophisticated caching algorithm known as the Adaptive Replacement Cache or ARC. This algorithm adjusts itself dynamically to balance between your most recently used and most frequently used data, in order to provide peak performance for reads. In addition to caching, RAM is also used to support the different sharing protocols, directory services, plug-ins, or applications, and is used for virtual machines. There are many “guidance rules” that exist, but in general:

- Add 1 GB per drive above eight, for handling ZFS metadata
- Add 2 GB if binding to Active Directory, for internal caching of these objects
- If serving highly random, latency-sensitive data (such as virtual machine hosting over NFS or iSCSI), consider a *minimum* of 32 GB and strongly consider a platform that permits scaling to much larger capacities (256 GB+) over one that is limited at 32/64 GB
- If you are considering using a second-level read cache, or “L2ARC”, add approximately 1 GB per 100 GB of cache (as a conservative estimate) to be used to index the contents of these additional cache devices

- OpenZFS deduplication puts significant additional workload on the memory capacity of your machine. Provide an additional 5 GB per 1 TB of data to be deduplicated if storing files and 20 GB per 1 TB of data to be deduplicated if storing virtual machines

If additional RAM is provided beyond the suggested minimum, TrueNAS will increase the size of the ARC in order to utilize the space.

2.4 ECC RAM is Strongly Recommended

For testing purposes, ECC is not required, but ECC RAM is strongly recommended to protect against memory errors. These errors can result from interference inside the system or be an early indicator of a failing piece of hardware. Using ECC RAM can correct, and depending on the system, report the occurrence of these errors, providing a benefit to overall system stability. This type of memory is often the standard for server and workstation platforms, but may not be supported on desktop systems.

2.5 CPU Selection is Core to your Success

The selection of a server/workstation platform and the recommendation for ECC RAM may introduce some limitations on the CPU that can be selected for your TrueNAS system. See below for some guidance on selecting the correct processor.

- Both Intel and AMD CPUs can be chosen for TrueNAS SCALE
    - 12th-generation and newer Intel Core-series processors may have unexpected performance variations due to the presence of both P-core (performance) and E-core (efficiency) processors
- An underpowered CPU can create performance bottlenecks due to the OpenZFS checksum calculations and in-line data compression
- If primary sharing will be done over SMB, select a CPU with a higher peak frequency and fewer cores, as TrueNAS uses the Samba software, which is lightly-threaded
- Where multiple applications or virtual machines will be used, consider a CPU with a greater core count to avoid contention between different programs
- Hardware support for AES-NI encryption extensions is available in most modern processors, but it is worth confirming the presence of these instructions if data or network encryption will be used in your TrueNAS operations
- Dual-socket platforms will typically require the presence of a second CPU in order to make use of all available memory sockets and PCIe slots. Check your server or motherboard manual for a “block diagram” that will outline which CPU sockets connect to which memory sockets and expansion slots

If using a workstation or desktop motherboard, consider whether or not your CPU contains an integrated graphics processing unit (iGPU) or if a separate card will be required to obtain the initial console output needed to set up TrueNAS. Server motherboards often contain a Baseband Management Controller (BMC) with its own video output that can be used for this. Some systems can be run “headless” without a GPU following the initial installation, but this is not universally consistent across hardware vendors.

2.6 Storage Controllers

The de facto standard for a storage controller in TrueNAS is a Broadcom (formerly Avago, formerly LSI) SAS Host Bus Adapter (HBA). These are available in 6 Gbps SAS, 12 Gbps SAS, or newer “Tri-Mode” cards with NVMe support. It is recommended to avoid the earliest 3 Gbps SAS generation as they were limited to 2 TB per device in addition to their reduced performance versus newer hardware. These HBAs are often rebranded for use in OEM servers. E include (but are not limited to) the Dell PERC H200/H310, HPE H220, IBM/Lenovo M1015, and Fujitsu D2607. These cards can often be converted to use the original LSI firmware through a process known as “cross-flashing,” which is outside the scope of this guide. Use the latest available “Initiator/Target” or “IT” firmware available for these cards.

Other vendors of HBAs can be used (eg: Microsemi), but the Broadcom cards are strongly preferred due to their long history and mature storage driver.

For smaller-scale systems, the onboard SATA controller of the motherboard can be used. When using these controllers, note that many motherboards often contain a mixture of 3 Gbps and 6 Gbps SATA This may impact performance, especially when connecting a solid-state drive (SSD). Some motherboards also allow for SATA ports to be configured as

"RAID." It is important to disable this functionality by selecting the "AHCI" or "Non-RAID" options.

RAID controllers are strongly discouraged for use with TrueNAS and OpenZFS. These controllers can cause performance or stability issues, mask hardware serial numbers and SMART health, or introduce the potential for data loss if write caching is used on the controller. If a RAID controller is the only available option, consider taking the following steps:

- Enable "HBA Mode", "Drive Passthrough", or "JBOD mode" if possible
- Configure each drive as an individual RAID0 device and continue to use TrueNAS to provide redundancy

Note that the failure of a RAID controller with write-back cache is likely to result in data loss. ***It is suggested to use systems with RAID controllers only to gain familiarity with the TrueNAS software, and not for performance testing or storing critical data. RAID controllers are not supported for production TrueNAS systems.***

TrueNAS fully supports the use of SAS expanders, whether on an internal backplane or in an external disk shelf. Other types of external storage, such as SATA-based port multipliers and USB JBOD enclosures, may cause unexpected issues with pool creation, disconnects under workload, or poor performance.

2.7 Drive Type and Count

TrueNAS SCALE has been validated for up to 250 drives in a single storage array. This offers an unparalleled level of flexibility, allowing you to design a solution that best fits your needs. A combination of magnetic HDDs, SATA or SAS-based NAND, and NVMe devices can be combined in varying roles within TrueNAS.

2.7.1 Magnetic Hard Disk Drives (HDDs)

Until there is a major scientific breakthrough in storage, magnetic spinning hard disks remain the ideal choice for solutions where both high capacity and low cost are desired. With hard drives well into the double-digit terabyte size, a system can be built with a small physical footprint that delivers big usable capacity.

2.7.1.1 Avoid Shingled Magnetic Recording (SMR) Drives

While HDD manufacturers are always seeking to improve the density of their storage and pack more bits into a platter, one particular method of improving this density has been proven to be particularly problematic for copy-on-write filesystems including ZFS.

Shingled Magnetic Recording (SMR) is a term used to describe a method of tightly packing the data tracks on magnetic media together to the point at which they overlap, similar to shingles on the roof of a structure. Much like roofing shingles, the data tracks need to be written "in order," which causes additional "read-modify-write" cycles when data that is "lower in the pile" needs to be overwritten. This extra work causes the drives to perform significantly slower than conventional non-shingled drives and may even result in data integrity issues during a power loss event.

Due to these compatibility issues, iXsystems recommends that you do not use shingled magnetic recording drives with TrueNAS. Please carefully review your drive vendor's datasheet, and if procuring drives specifically for use with TrueNAS, explicitly state that SMR drives are not compatible and should not be supplied.

2.7.2 Solid-State Drives (SSDs)

Thanks to a rapid progression in flash storage technology, solid-state drives have become a common sight in general-purpose PCs and servers. Due to their lack of moving parts, flash drives are not sensitive to vibration and can offer a much higher level of random I/O performance.

2.7.3 NVMe (Non-Volatile Memory Express) SSDs

NVMe SSDs can offer improvements in both bandwidth and latency over SATA and SAS SSDs, as these devices connect to the PCI Express bus, offering multiple gigabytes per second to each connected device. This same connection can introduce challenges for hot-plugging devices. SATA and SAS hotplug is generally well-supported on a variety of hardware, but NVMe devices may not be recognized without a reboot.

While the legacy FreeNAS operating system was often run from small USB thumb drives, modern versions of TrueNAS

generate a higher write workload to the boot device, which can quickly consume the endurance available on a typical consumer thumb drive. For this reason, all pre-built TrueNAS storage systems ship with M.2 or SATADOM (Disk On Module) devices.

3 Creating your Install Media and Installing TrueNAS

The first step in creating your install media is to download the TrueNAS SCALE installation ISO file from our website, at https://www.truenas.com/download-truenas-scale/.

3.1 Choosing your Installation Method

While the ISO is downloading, you'll need to determine your installation method. Many servers have the ability to mount an ISO remotely through an out-of-band management interface, presenting it as a virtual optical drive. If this is the case with your hardware, you don't need to create physical installation media.You can simply present the ISO to your server and continue on to section **3.3. Installing TrueNAS SCALE**. Installing on a virtual machine is similar. Use your hypervisor or virtualization software to present the downloaded ISO as a virtual optical drive to your new VM.

TrueNAS SCALE can be installed from a physical DVD if you choose. If this is your preferred method, simply record the ISO to a disc with your preferred media creation software - but it can also be transferred to a bootable USB drive of at least 2 GB in size.

3.2 Creating an Install USB

Depending on your operating system, there are a variety of programs that can be used to transfer the downloaded TrueNAS SCALE ISO to a USB stick. iXsystems does not recommend any specific program, but some examples are:

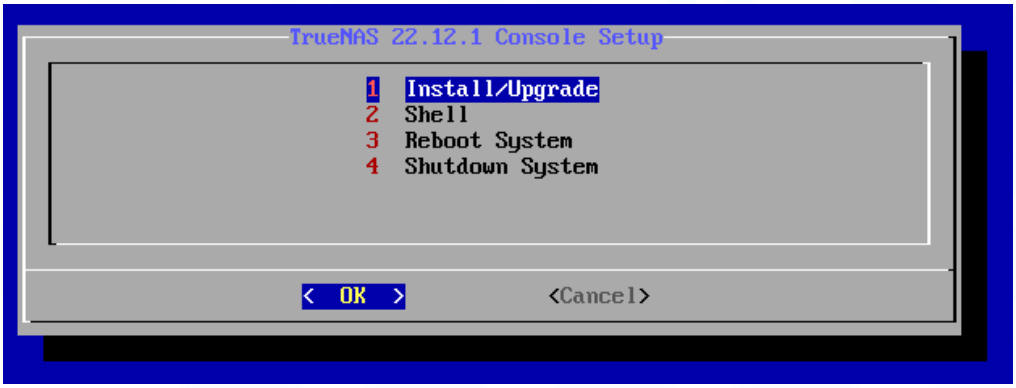
balenaEtcher (etcher.io) - Windows, macOS, Linux
Rufus (rufus.ie) - Windows
dd command-line - Linux

When creating your USB installation device, note that any existing data on your USB device will be overwritten. If prompted by your media creation program, select to use "DD mode," and configure the boot to include "BIOS + EFI" depending on your hardware platform.

3.3 Installing TrueNAS SCALE

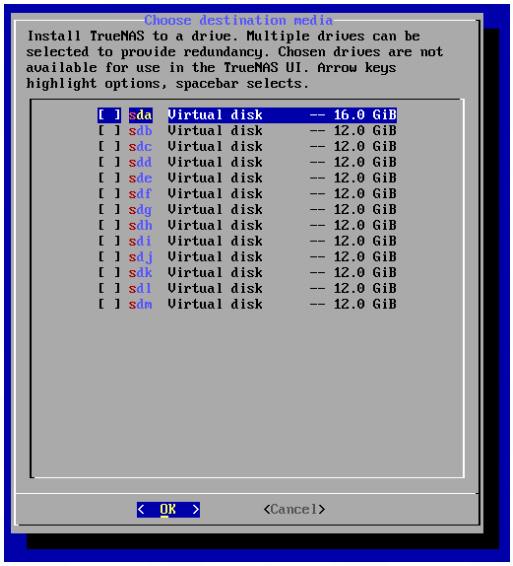
Insert or attach your boot device to the system you'll be installing TrueNAS SCALE on. You may need to press a specific function key during the BIOS or EFI boot process to select a specific boot device.

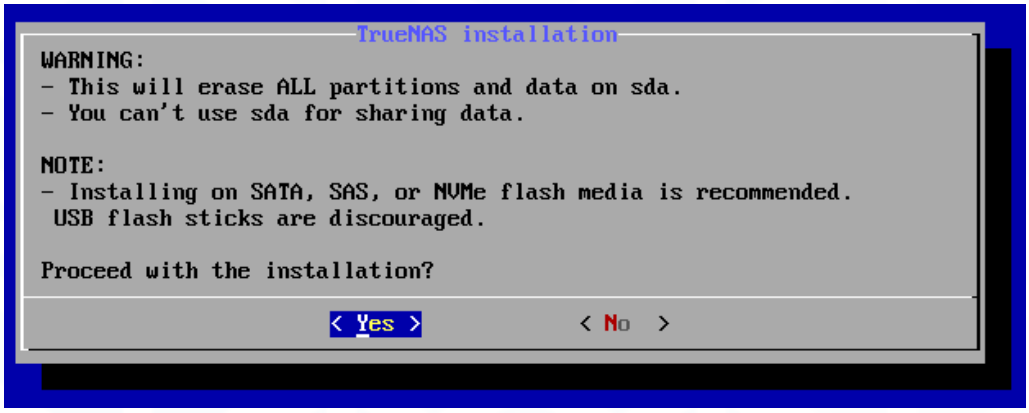
Once you've booted up, you'll see the TrueNAS SCALE console installation menu. Press Enter to begin the installation or wait for the installer to continue on its own after 15 seconds. The Linux-based installer will perform some initial startup tasks before presenting the TrueNAS Console Setup screen.



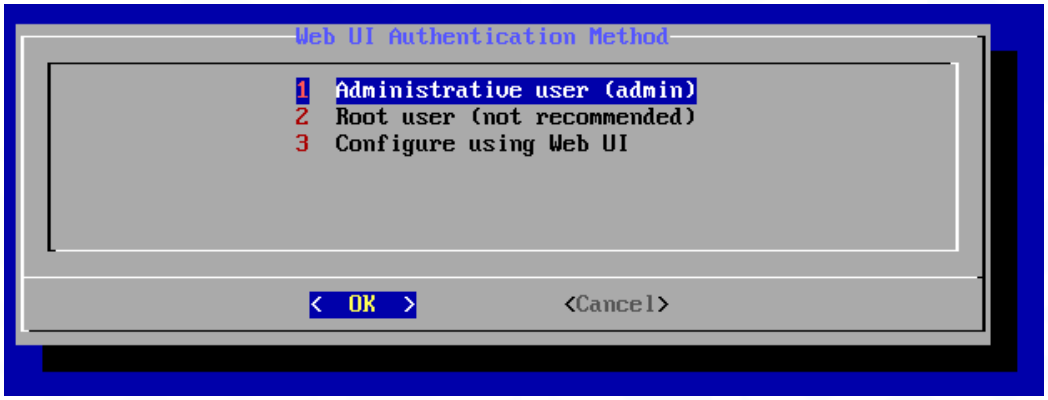
From here, select **Option 1 Install/Upgrade** with the Enter key.

Next, you'll be prompted to select the drive (or drives) to install TrueNAS SCALE on. In our example, we have one 16 GB drive, and twelve 12 GB drives. We'll select the single 16 GB drive with the Spacebar before using the arrow keys to navigate to the OK button at the bottom. Note that any drives chosen for installation and booting are not usable for data storage.

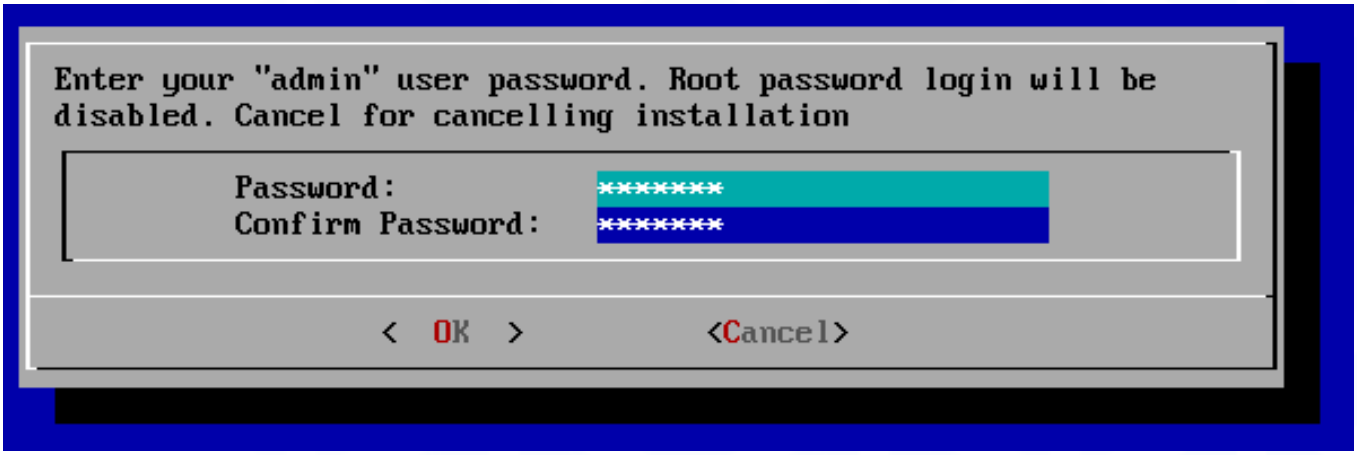




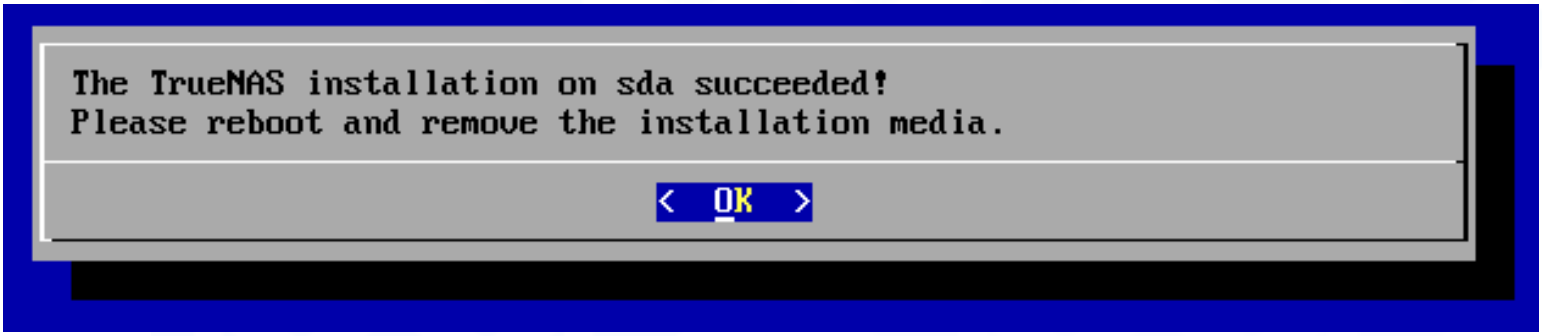
You'll be prompted to select the authentication method for the TrueNAS SCALE Web UI. We recommend the first option of **Administrative user (admin)** to separate the system super-user of "root" from the web UI administrator role.



After making your selection, you'll be prompted to enter the administrator password twice. If this password is forgotten, it can be reset from the TrueNAS SCALE console after installation.



Select the **OK** button using the arrow and **Enter** keys, and the installation will begin. Depending on the speed of your system and the installation method (virtual DVD, physical DVD, USB), this may take several minutes. Once this is complete, you should see a "succeeded!" message.



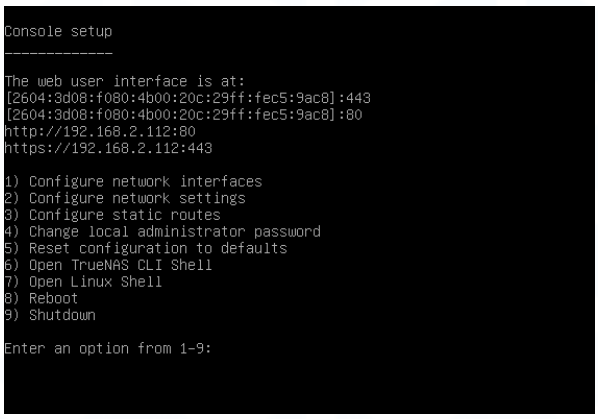
Remove the installation media, and choose to either reboot or shut down the system.

4 The First Boot

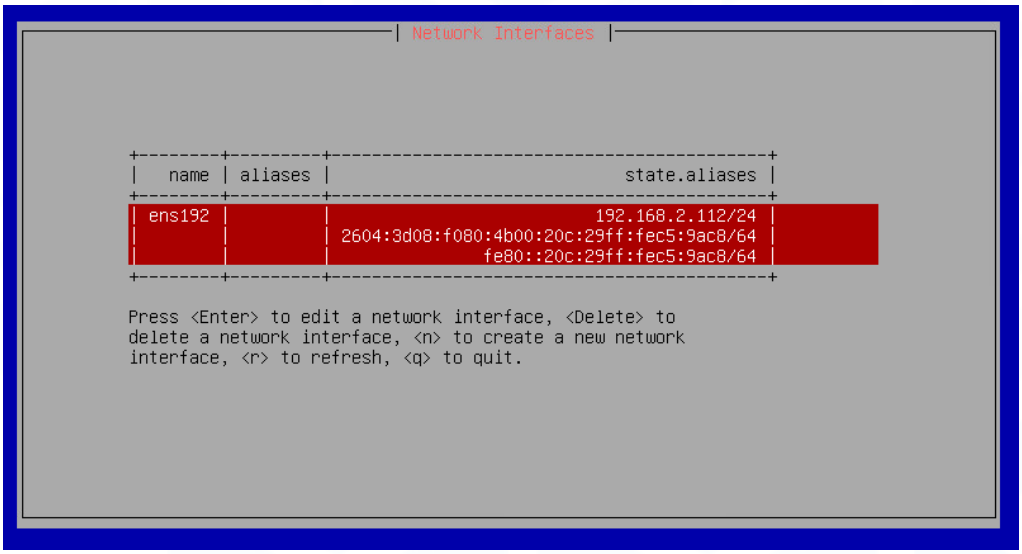
Now that you have TrueNAS installed, attach a single network cable to an available port on your hardware. During the initial setup process, you should only attach a single cable to prevent multiple IP addresses from being claimed on the same network. Once that's done, power your system on and begin the initial startup phase.

4.1 Checking For DHCP - Assigning an IP Address

The first boot of TrueNAS will take slightly longer as it will be generating a few encryption secrets. Please be patient and wait for the initial console menu screen to appear, as shown below.



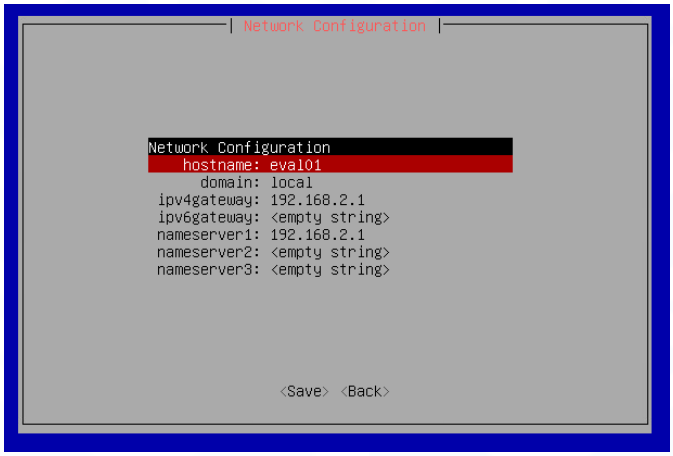
TrueNAS SCALE will attempt to obtain a DHCP lease on any physically connected interface. Even if DHCP is available on your connected network, it is suggested that you configure a fixed or "static" IP address instead for stability purposes. Use the console menu to select `1. Configure Network Interfaces` to launch the menu.



If you have multiple network adapters, you will see them in this menu. TrueNAS SCALE uses network device naming conventions based on the physical location of the adapter. Onboard devices may be referred to as "eno" with add-in cards being labeled as "ens" or "enp" depending on your hardware configuration. In our example, we'll be setting a fixed IP address for the connected "ens192" interface. Press **Enter** to edit the interface. Using the arrow keys and **Enter** to navigate the interface, move down to the **ipv4_dhcp** item, select it, and choose the **No** option. Move to the **Aliases** field, and add a new IP address with subnet bits. We'll choose 192.168.2.65. For most home networks, the subnet will be a "slash 24," but please check with your network administrator if you're unsure. Choose to **Save** these changes, and you'll be prompted to apply the pending changes. Press **(a)** to do so and test your ability to reach the TrueNAS system through a web browser, or with a **ping** test from a client machine. Once you've confirmed that network access is functioning correctly, use the **(p)** key to make the changes permanent, then use the **(q)** key to leave the configuration menu.

4.2 Changing Hostname, setting Gateway and DNS

While we at iX consider "TrueNAS" to be a fine name, it may not work as a hostname for your particular environment. You may want to set up two or more systems on the same domain. Select option `2. Configure Network Settings` from the console menu.

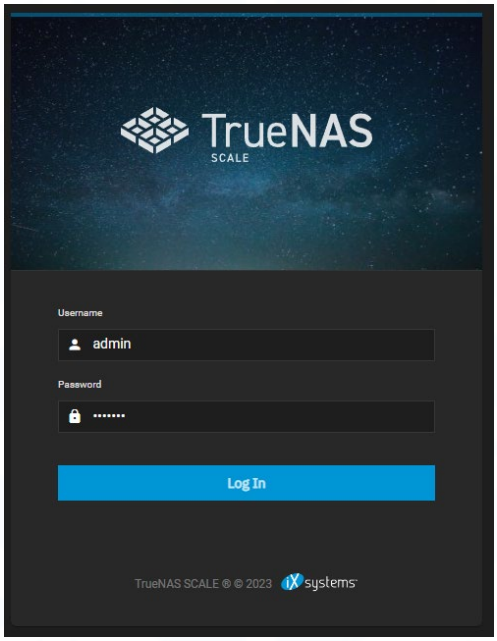


Enter your preferred hostname, domain name, the default gateway, and DNS server (or servers) for your network. If you're unsure of these values, check with your network administrator.

Once you've completed the console configuration, it's time to connect to your TrueNAS system from a web browser.

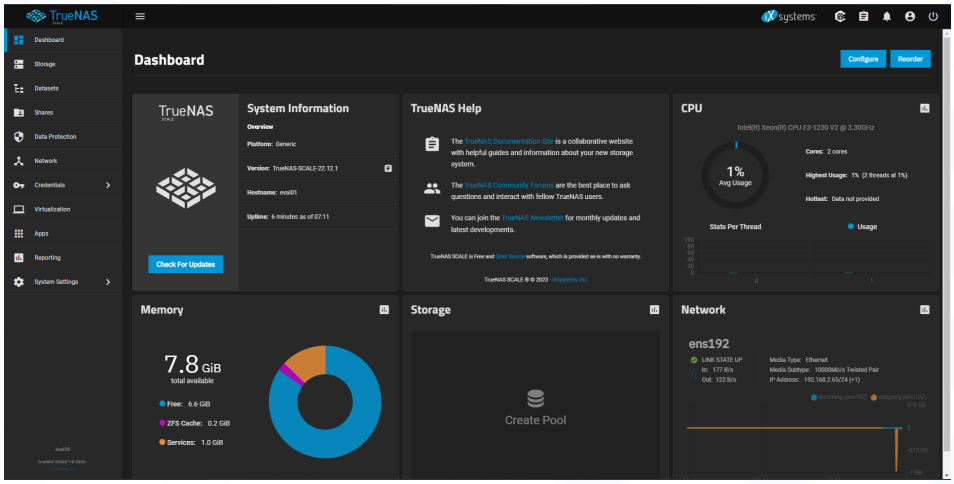
4.3 Signing into the Web UI

TrueNAS SCALE is intended to be operated through an HTML5 interface loaded through a web browser. Once TrueNAS has an IP address, it will advertise itself over the network using the Multicast DNS (mDNS) service with the hostname that was configured above. You can always enter the IP address directly into your browser using either HTTP or HTTPS.



If you're not able to load the TrueNAS logon page, check to see that you can reach the system via ping on the configured IP address, and that there are no network proxy or firewall/ACL rules that would prevent your browser client from reaching that IP address.

If you selected the "rootless" option during the installation of TrueNAS SCALE, the username is "admin." Use the password that was set during the installation process. Once you're logged in, the TrueNAS dashboard should be visible. Verify that the CPU and Memory widgets show the correct thread count and total memory capacity.

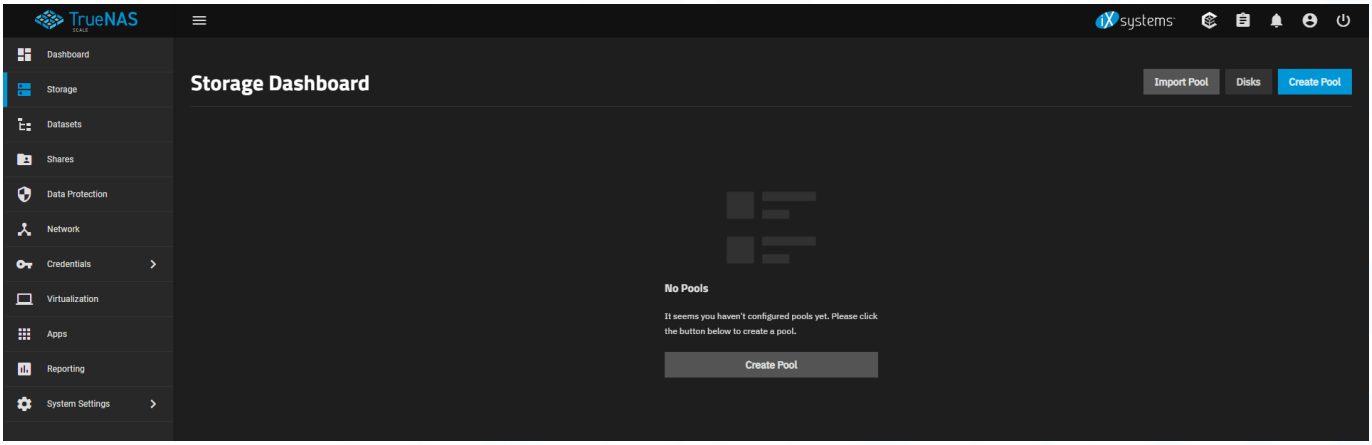


5 Getting Started with your Storage

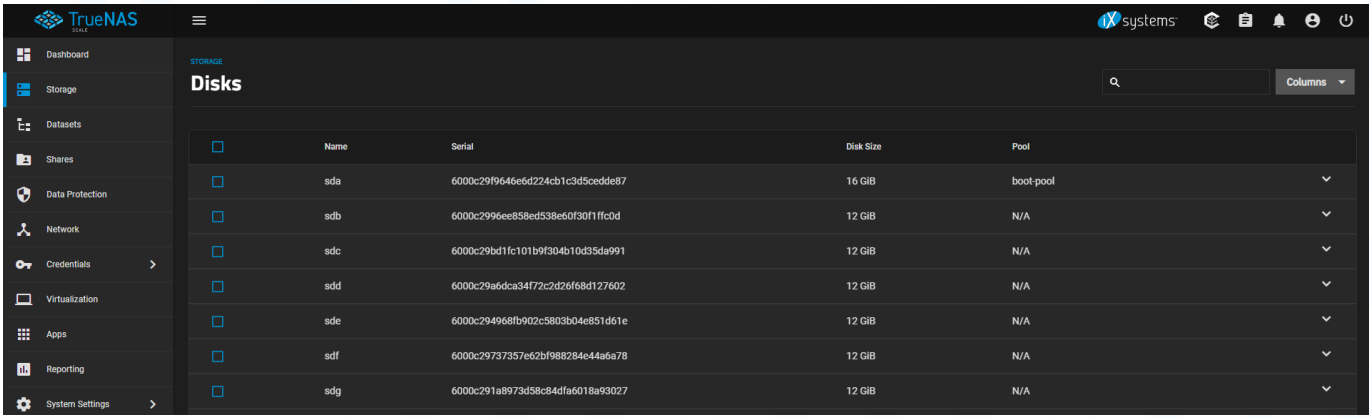
In this section, we'll create a **pool** (the top-level storage element of OpenZFS), provision a **dataset** (like a file system) inside that pool, and then share that pool over SMB.

5.1 Confirming Disk Count

From the menu on the left-hand side of the screen, click on the **Storage** tab, and then the **Disks** button in the top right corner of the new screen.



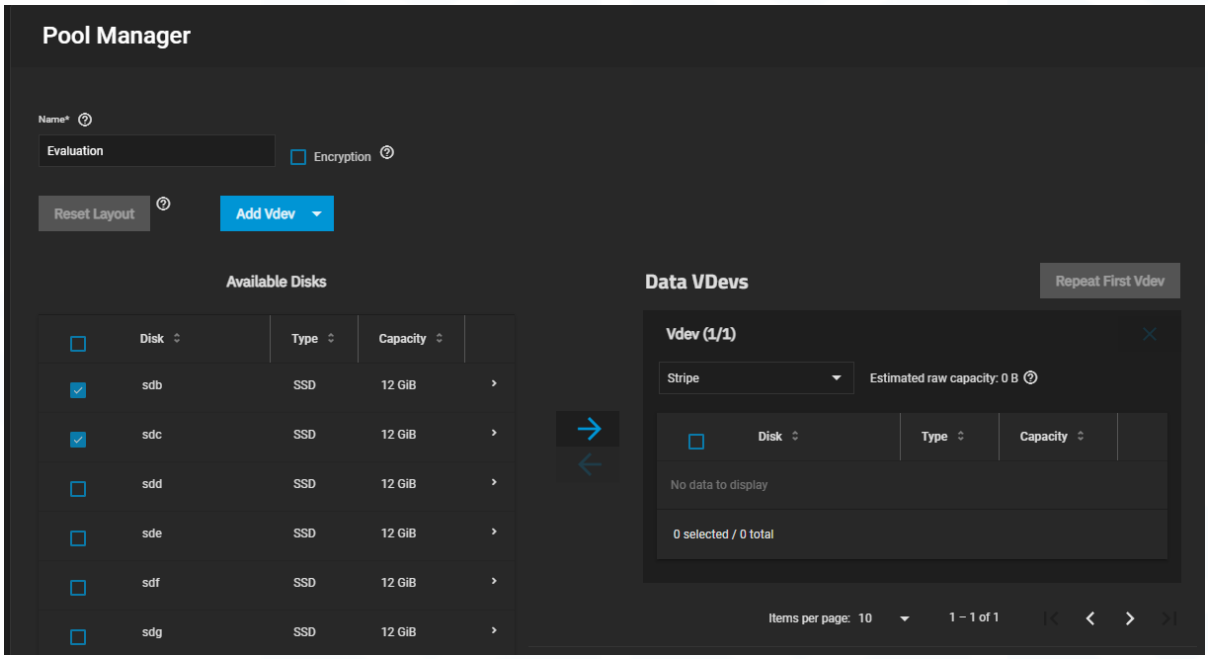
The Disks view should show that you have several unassigned disks. Any disks that you selected during the installation process will be shown as a member of the “boot-pool” and will not be usable for data storage. If you have fewer disks than expected here, check that your internal cable connections are secure. If you have more disks than expected, you may be using SAS devices with a dual-path enclosure.



5.2 Build your First Pool

Click on the **Storage** tab again, and this time use the **Create Pool** button in the top-right corner of the dashboard to start the Pool Manager. Enter a name of your choice in the “Name” field. This name won’t be visible to regular network clients, only to administrators logging in to TrueNAS, so pick one that describes it well for your storage team. The pool name can be changed after creation, but it requires the pool to be taken offline to do so. For this demonstration, we’ll use “Evaluation.”

There are numerous different storage configurations that can be used, and their performance and redundancy characteristics will be discussed further in the guide, but for ease of use and feature demonstration, we will create a pool made from **mirror vdevs**. In a conventional storage system, this might be referred to as a “RAID10” configuration. Use the checkboxes to identify two disks from the “Available Disks” list and click the “Right Arrow” button next to “Data VDevs | Vdev (1/1).”



You should now see the two disks in the vdev type of "Mirror." If you have additional disks available, click the **Repeat First Vdev** button and you'll be given the option to have TrueNAS automatically create additional vdevs using matching pairs that have been found in your system.

Important Troubleshooting Note:

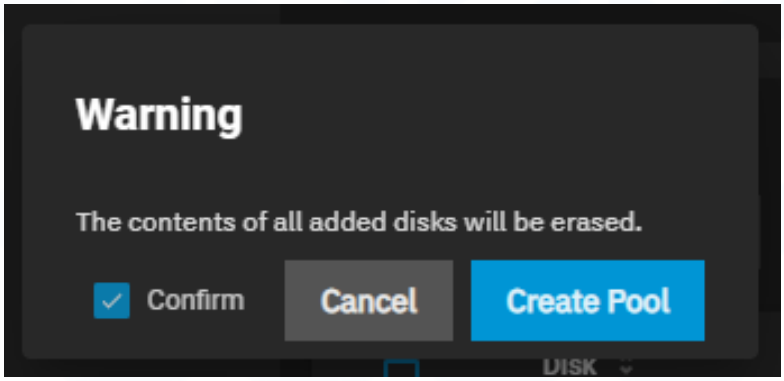
If you are unable to see your disks in the Pool Manager, but did see them in the previous Storage Dashboard, this may be a result of one of the following conditions:

1. Your storage controller is obscuring or failing to pass the drive serial numbers
2. You have installed TrueNAS as a VM on a VMware ESXi machine without vCenter or have used a virtualization platform that doesn't generate serial numbers for virtual disks

For the former, TrueNAS expects to be able to uniquely identify each storage device. Multi-drive enclosures and some consumer-grade single-drive enclosures have been observed reusing serial numbers across multiple pieces of equipment. You can check the "Show disks with non-unique serial numbers" dialog option or try to resolve this by changing the storage controller.

For the latter, you'll need to power off your TrueNAS VM and adjust your hypervisor settings to generate serial numbers. For VMware ESXi without vCenter, check the VM advanced configuration (Edit - Advanced, Configuration Settings) and create the advanced variable `disk.EnableUUID` with a value of `true`, then power the VM on again.

Once all drives have been assigned to vdevs, click the large "Create Pool" button. A warning will be shown indicating that existing data on the drives will be removed. Once you've confirmed that no data is remaining on those drives, check the "Confirm" button and proceed with pool creation.



5.3 Make a Dataset

A ZFS dataset can be thought of as analogous to a typical file system, but we can define some additional ZFS properties on a per-dataset basis, such as cache behavior, storage quota, and the compression algorithm to use. Datasets can be nested, similar to folders in a traditional file system, and will inherit settings from their parent dataset.

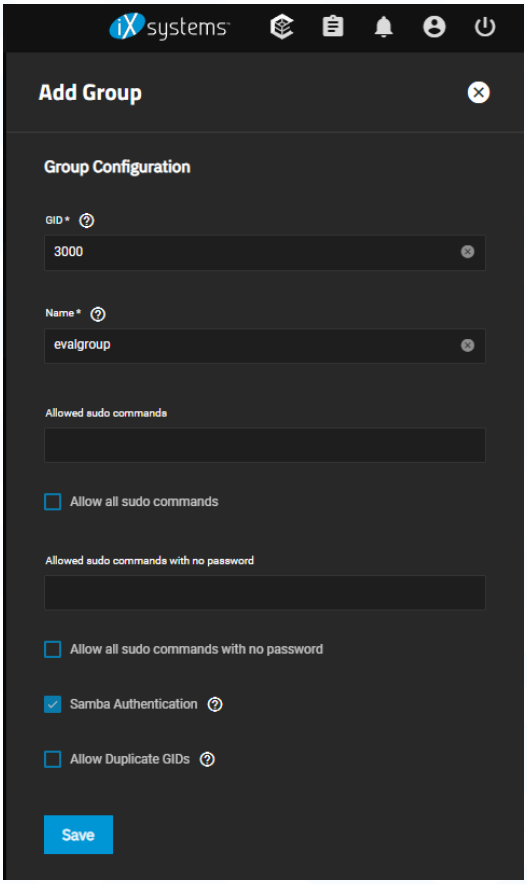
Navigate to the **Datasets** page, select your pool on the left-hand pane, and press the blue **Add Dataset** button on the far right.

Provide a dataset name. In our case, we'll use "EvalData." Scroll to the bottom of the window and change the Share Type from **Generic** to **SMB** which will set the **Case Sensitivity** option to **Disabled**. Once this is finished, click **Save** to create the dataset.

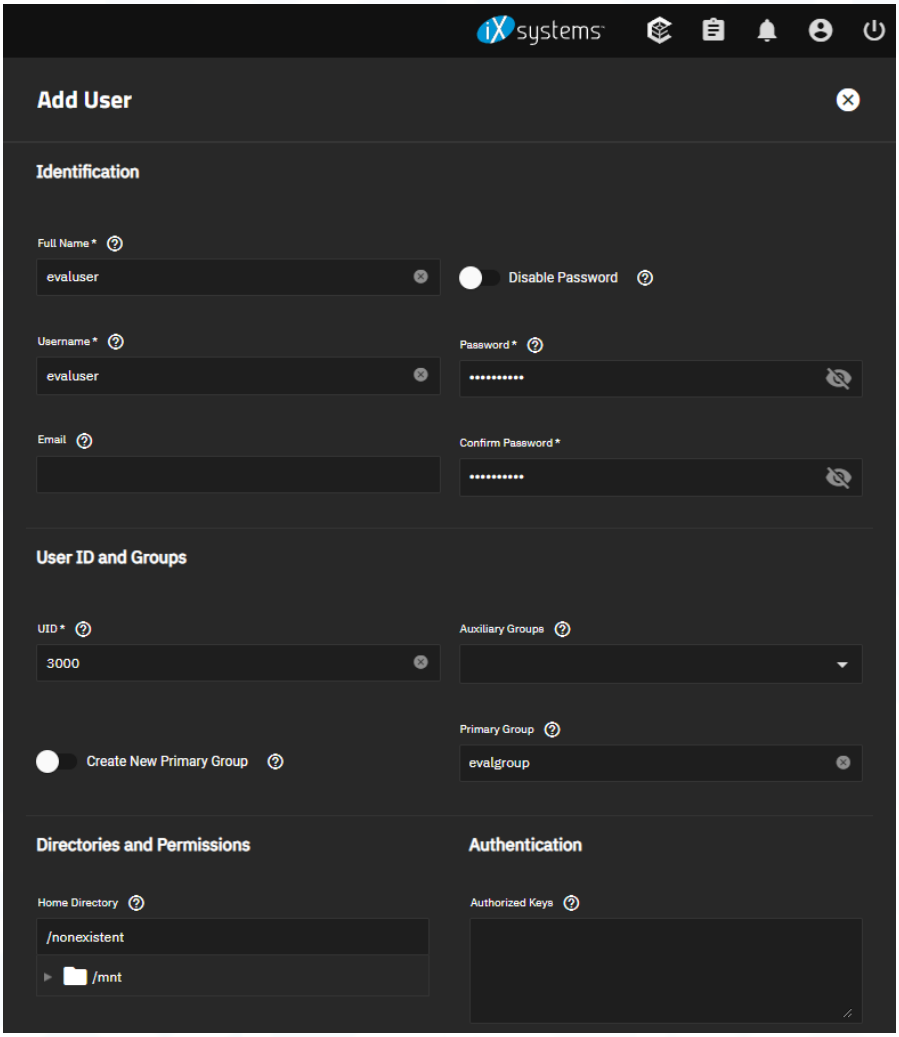
5.4 Creating a Group and a User

Since you don't want to use administrative credentials to map shared network resources, let's create a new group and user for authentication. Open the **Credentials → Local Groups** menu and choose the **Add** button.

The "GID" or "Group ID" is a numeric identifier used by the TrueNAS system. Leave the default value in place and set the name to evalgroup before continuing. Enable the "Samba Authentication" checkbox, as we want to be able to use this group to grant access to a shared folder later.



Next, let's create a local user. Open the **Credentials → Local Users** menu and choose the **Add** button



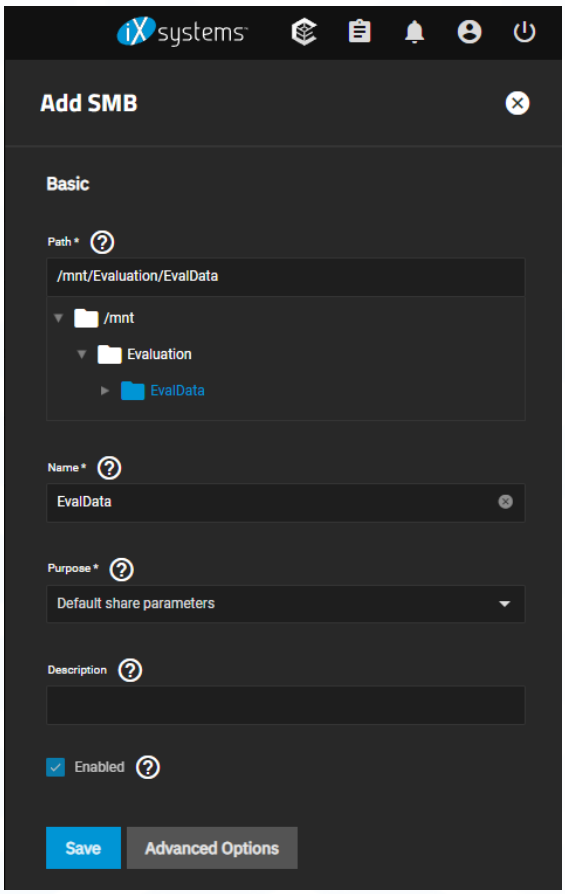
.

Set the full name to `evaluser` and set a password for remote access. Pay special attention to the limitations on characters that are and aren't allowed in a username. Disable the "Create

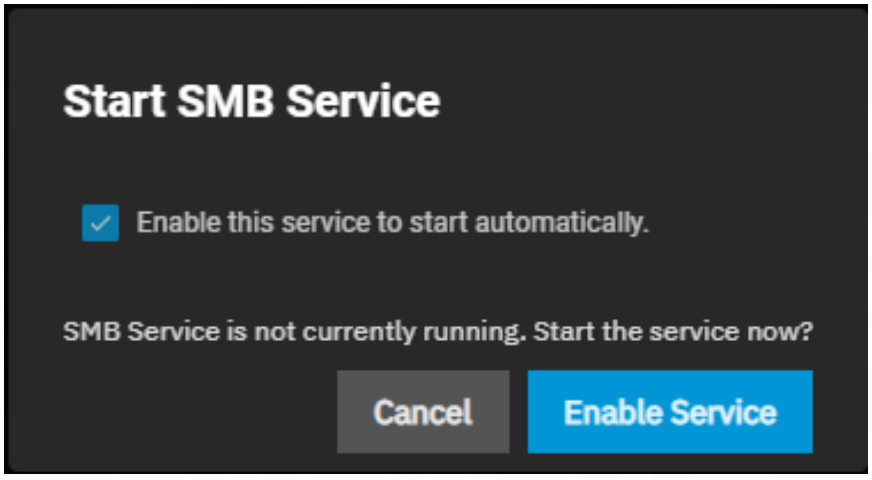
New Primary Group" slider, and search for the "evalgroup" to assign as the Primary Group. Scroll down, and leave the "Home Directory" field set to the default "/nonexistent" for now. Note how the "Samba Authentication" checkbox defaults to Enabled for user account creation, as opposed to when a group was created above.

5.5 Share the Dataset over SMB

Navigate to the **Shares** page. Choose the **Add** button beside **Windows (SMB)** Shares. Select the path to your newly created dataset, and accept the default share name or enter a new one. Leave the "Purpose" as "Default Share Parameters" for now and add a description if desired, which will be visible to clients. Click **Save** and wait for the share to be created.



As this is the first share you've created, you'll be prompted to start the SMB service. Set the "Enable this service to start automatically" checkbox and then click "Enable Service."



Congratulations! You've made your first share available from TrueNAS. Access the system via your previously configured hostname (such as truenas.local) or IP address through a file browser (`\\eval01.local\EvalData` or `\\192.168.2.65\EvalData`) and use the "evaluser" user credentials and password configured previously to sign in.

6 Data Protection, Previous Versions, and Snapshot Scheduling

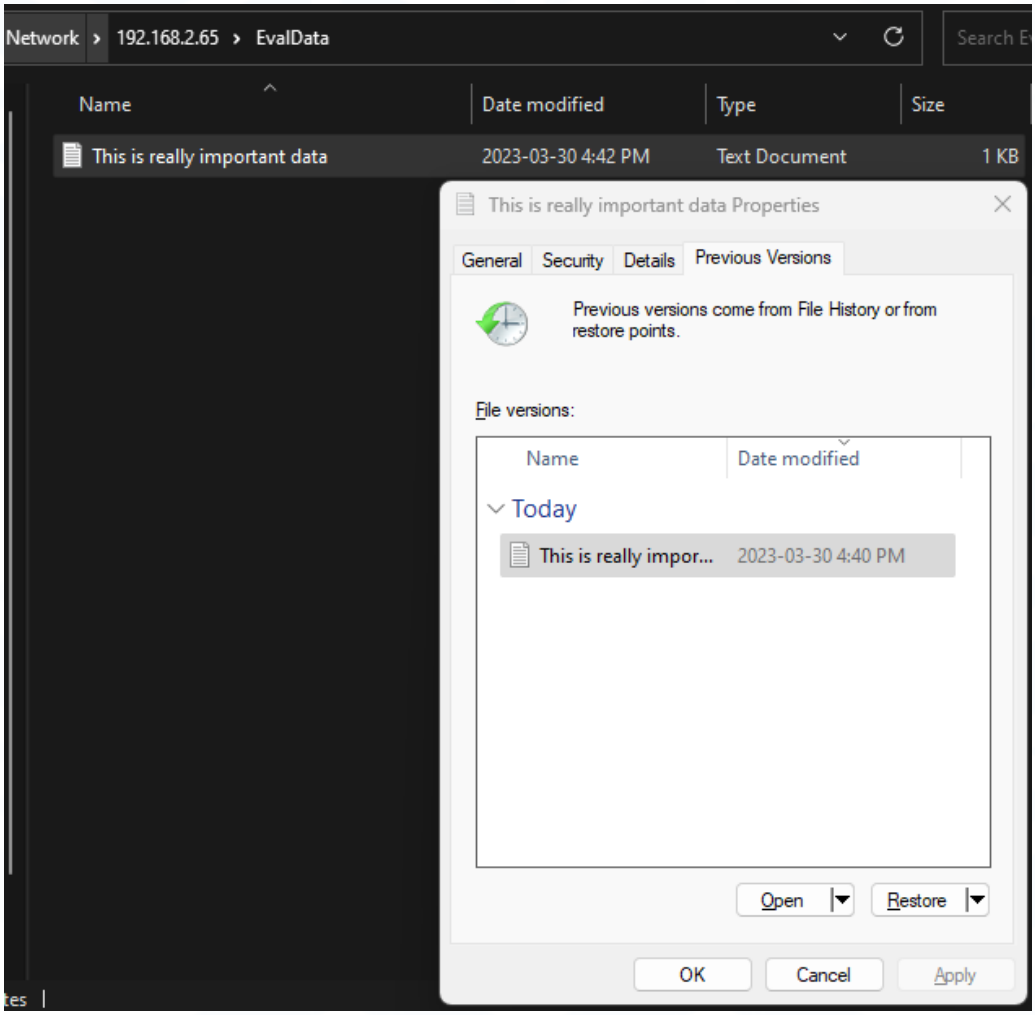
TrueNAS uses ZFS snapshots for recovery, which leverage the copy-on-write behavior of ZFS. Even when overwriting existing data, the older copy is kept, and marked for preservation by this snapshot. We'll demonstrate that using your shared folder. Access your system through a file browser using the hostname or IP address, and sign in using the user credentials you created above. Create a new text file or copy an existing document (a word processor or spreadsheet file is fine) to the shared folder. If you've created a new text file, write a quick note to yourself to represent data you want to protect from changes. Save and then close the file.

6.1 Taking a Manual ZFS Snapshot

From your TrueNAS console, navigate to **Data Protection**, select **Snapshots**, and click the blue **Add** button in the top-right corner. You'll be prompted to select your dataset. For our example, we would use `Evaluation/EvalData`. A snapshot name will automatically be generated with the format of `manual-YYYY-MM-DD_HH-MM` using the current date and a 24-hour clock. Leave "Recursive" unchecked for now, as we have no nested datasets beneath this folder to capture. Click **Save** and you'll be taken back to the Snapshot page almost immediately.

6.2 Going Back in Time

Return back to your shared folder through SMB and modify or delete some of the files you've created. Don't worry, as they are protected through the TrueNAS snapshot operating behind the scenes using the copy-on-write behavior of ZFS. Save any changes to the files and close them again. From here, right-click on the file (if using Windows 11, you may need to shift+right-click or select **Show More Options** (from the context menu) and select the **Restore Previous Versions** dialog. If you have edited multiple files, or deleted any files, navigate up a folder level and right-click on the "EvalData" folder itself before selecting the **Restore Previous Versions** option.

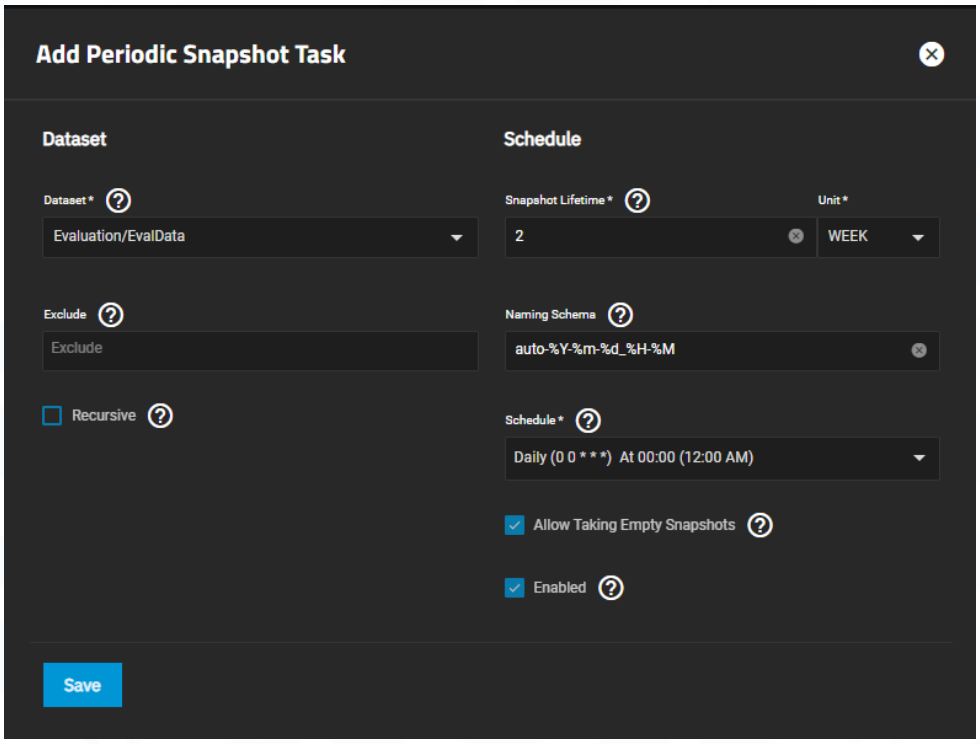


From here, you can double-click to open the previous version of the shared folder. Inside, you'll see the documents from the time of the snapshot, including any that have been deleted since. You can open and review the files there and copy deleted files back to their original location.

6.3 Automated Snapshots and Scheduling

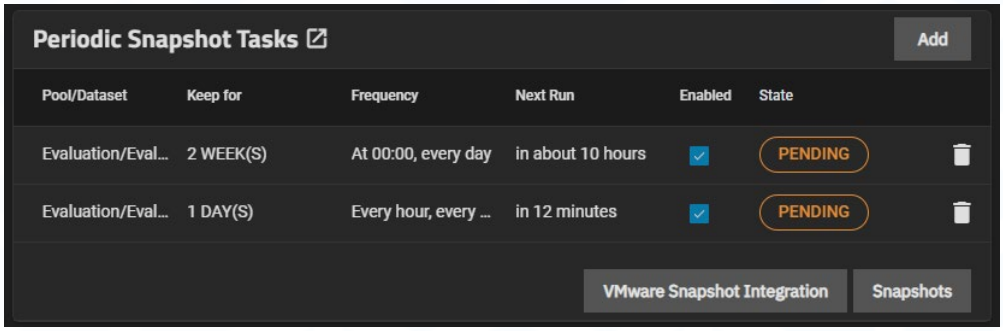
Return to your web browser, which should still be on the **Snapshots** page, and click on **Data Protection** once again. Manual snapshots are fine, but scheduled snapshots allow for this level of protection to be automatically refreshed on a regular basis. In the **Periodic Snapshot Tasks** panel, choose the **Add** button.

In your new side panel, select your dataset from the drop-down list. The default schedule creates a snapshot every day at midnight in your local time zone, and these snapshots are retained for two weeks. Once a snapshot is older than two weeks, it is automatically removed from the system to prevent excess disk consumption.



The snapshot schedule has pre-populated schedules for snapshots every hour, day, week, or month. With the "Allow Taking Empty Snapshots" option checked, snapshot schedules can overlap. A "Daily" and "Weekly" snap of the same dataset can happen at the same time and the "empty" snap will still exist to be retained for a longer lifetime.

For example, select your dataset, and change the "Schedule" to "Hourly" with a "Snapshot Lifetime" of one day. Save this task, and then create a second task with a "Daily" schedule and two week "Lifetime." With this configuration, files can be restored with one-hour accuracy for a 24-hour period, and after that, with one-day accuracy to a two-week period.



Snapshots are also crucial in the use of replication tasks - sending the data to another pool, to another TrueNAS system, or to another OpenZFS replication target.

7 Drive Failure, vdev Removal, and Extending your Pool

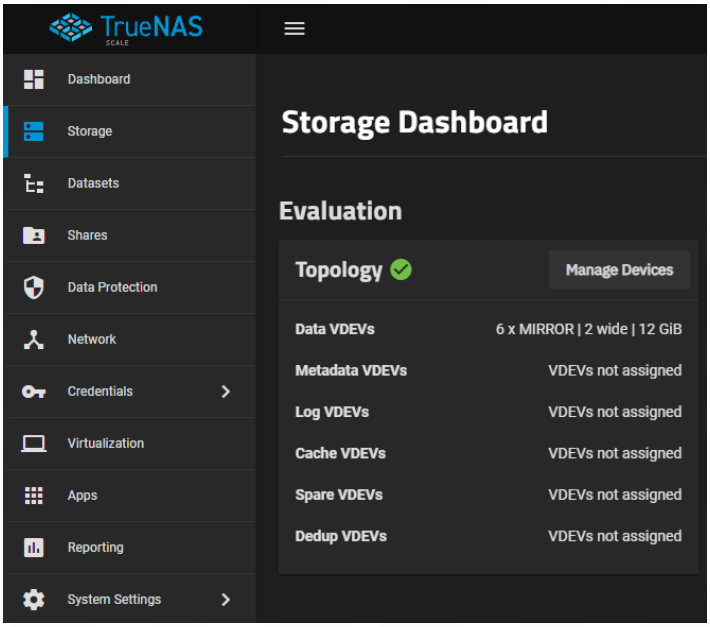
While ZFS is not the same as a traditional RAID array, it does share the first letter of the acronym in that it can provide *redundancy*. A core difference to understand is that redundancy within ZFS is built at the vdev level, not the pool level. Consider the concept of a traditional RAID60, where disks are configured into double-parity groups, and then data is distributed across multiple groups. There is no ZFS equivalent to a "RAID61" where the disks are configured into double-parity and data is then mirrored between them.

In our example, we've created six vdevs that are two-way mirrors. It's important to take note of your configuration and adjust your failure simulation appropriately.

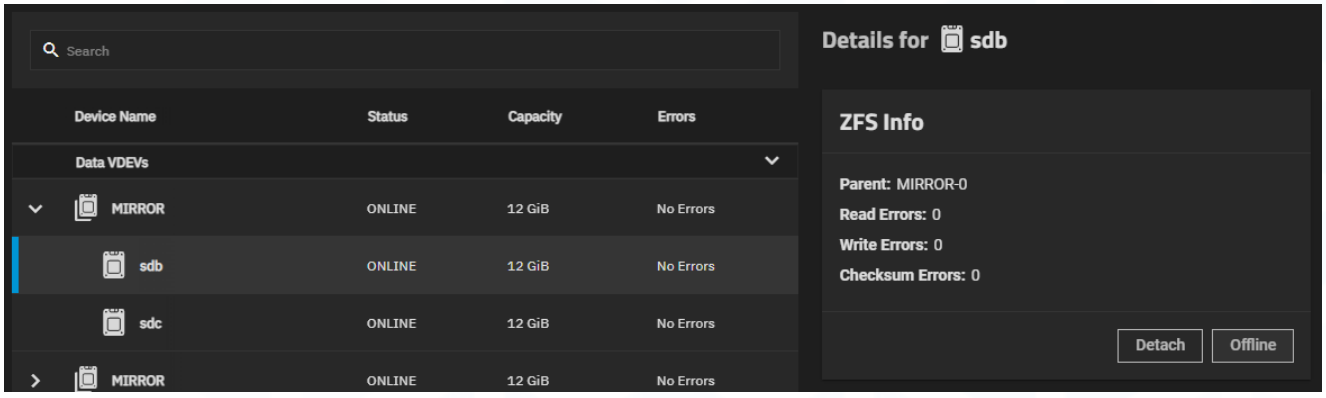
7.1 Simulating a Drive Failure

We can simulate a drive failure by setting a drive to an offline state. From the TrueNAS web UI, navigate to **Storage** and then select the **Manage Devices** button associated with your pool, in the **Topology** pane.

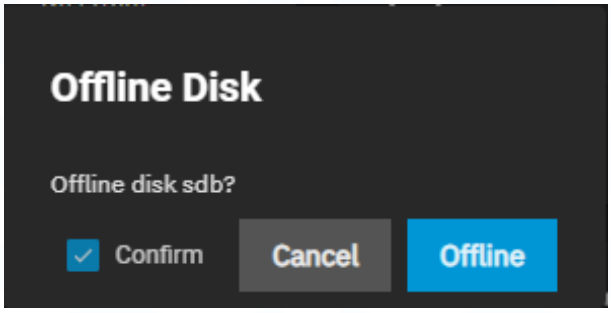
Note: Those who are evaluating TrueNAS SCALE on a hot-swap capable system can also choose to physically remove a disk from their server to test the behavior, rather than simulating a failure. Note that you should not attempt to hot-plug drives unless they are in a system designed for it. If in doubt, use the "simulated failure" approach discussed below.



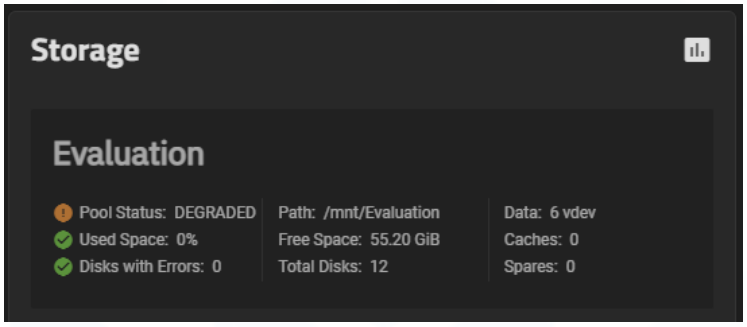
Within the **Storage - Devices** view, expand a MIRROR vdev object in the left-hand pane, and select one of the disks within it. Under the **ZFS Info** pane, choose the **Offline** button.



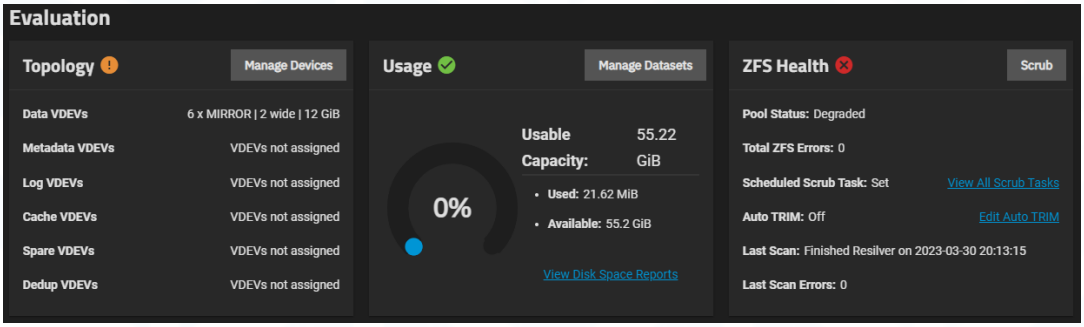
Performing the OFFLINE will treat the disk as failed, but leave an entry for it in the MIRROR vdev. Confirm the operation and click the blue **Offline** button.



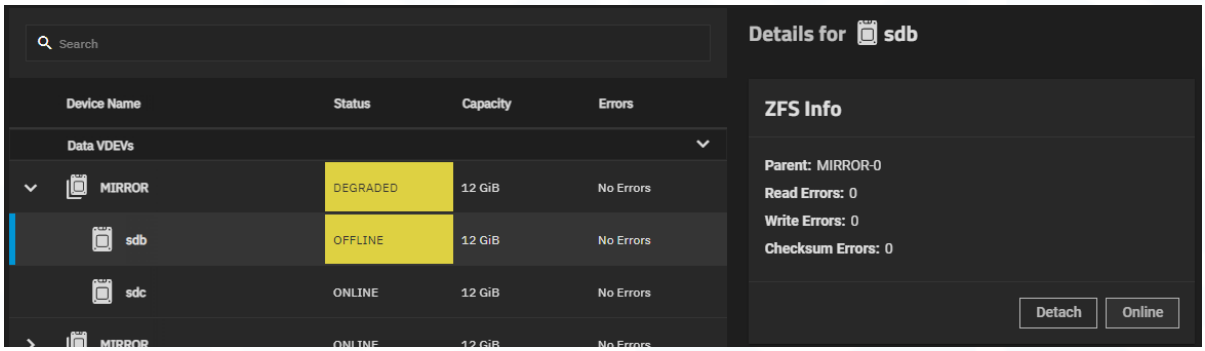
Once the display refreshes, the mirror vdev will immediately change to a status of **DEGRADED**. Click on the **Dashboard** tab on the left-hand side to see how the main screen would look in this scenario. You'll notice that the **Storage** pane will show your **Evaluation** pool with an overall status of **DEGRADED**.



Click on the **Storage** tab on the left-hand side and note the alerts raised in the **Topology** and **ZFS Health** categories:



As the disk is still present in the system, it can easily be replaced. Click the **Manage Devices** button, expand your DEGRADED vdev, select the OFFLINE disk, and click the **Online** button.

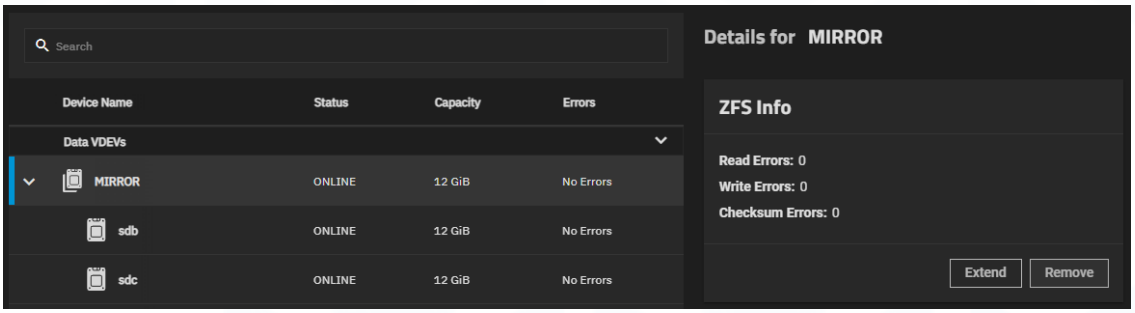


Confirm the operation, and the vdev will return to a healthy state. If data was added to the TrueNAS system while the disk was offline, a process called *resilvering* will begin to restore the redundancy level of the vdev.

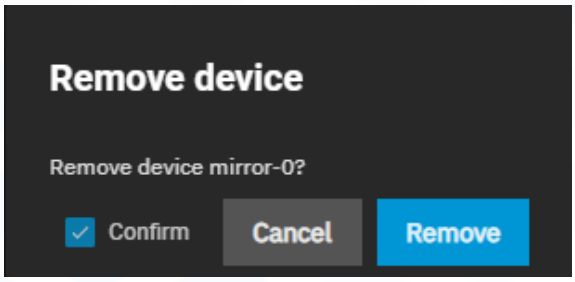
7.2 Removing a vdev

It may occasionally be necessary to remove disks from a pool permanently, perhaps to repurpose them for a second pool within the system, or to correct an inadvertent misconfiguration, such as two disks being added as individual drives rather than a single mirrored pair. With a pool that is composed of only stripe or mirror vdevs, ZFS allows for the removal of an entire vdev, assuming that enough capacity is provided by all remaining disks.

Click the **Storage** tab, and then **Manage Devices** on your pool. Click the first MIRROR vdev in your listing, and choose the **Remove** button in the **ZFS Info** pane.



Confirm the removal and click the **Remove** button again.

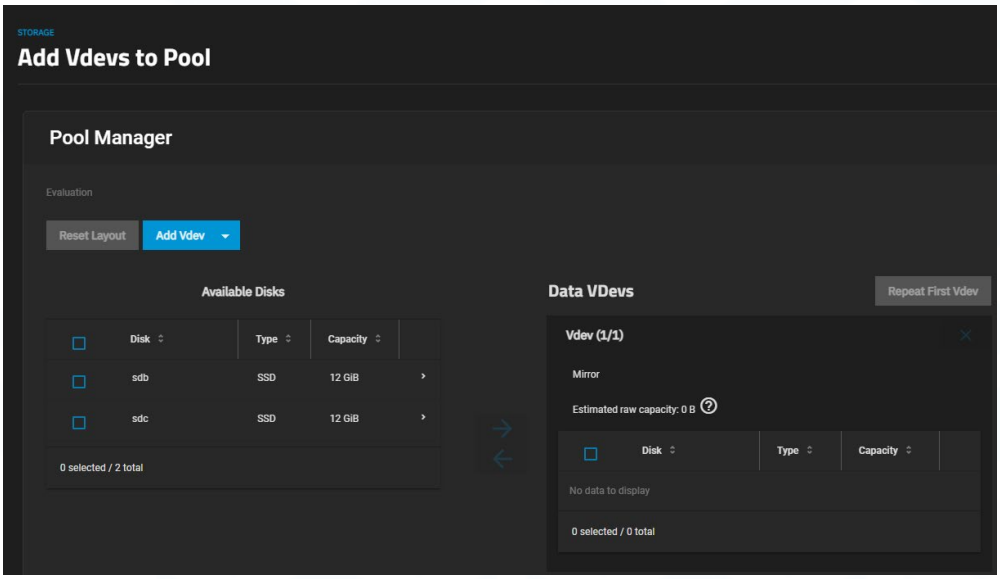


The disks will be marked for evacuation. This process may take a significant amount of time, depending on the amount of data stored on them.

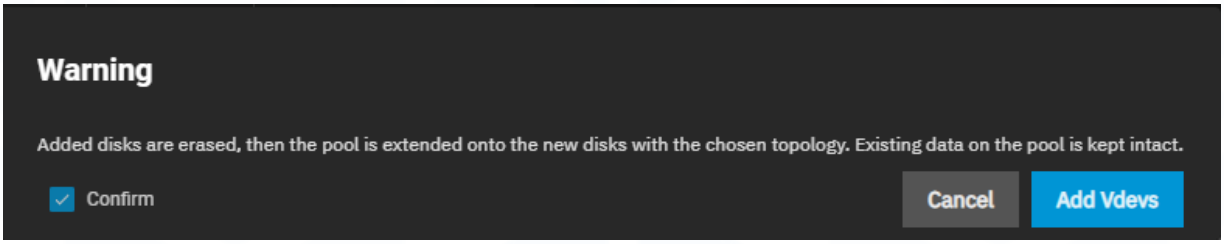
Once the process completes, the pool will be reduced to a smaller number of physical disks.

7.3 Adding a vdev

Much more common than the removal of existing disks is the addition of new ones. Click on the **Add Vdev** button in the top right corner of the **Storage - Devices** window. You'll be presented with a familiar dialog, which is the same **Pool Manager** we used to create the pool initially.



You'll notice that the vdev on the right-hand side is already configured as a MIRROR. Select only the first disk and choose the right arrow button, and note that TrueNAS presents you with a pair of warnings in red text, one indicating that the mirror requires a minimum of two disks, and the second indicating that it is not recommended to use a different number of disks to extend a pool. Select your second disk and use the right arrow button to move it to the vdev, and these errors will disappear. Click the **Add Vdevs** button at the bottom of the screen.



You'll need to confirm that the disks will be erased. Note that existing data on the pool is kept intact and not migrated to the new disks immediately. ZFS will begin to direct new writes to these disks, as well as any data being overwritten that may exist elsewhere. Again, this is due to the copy-on-write nature of ZFS.

8 Replication - Local and Remote

We've used snapshots as one level of data protection in Section 6. To extend this protection further, we can use TrueNAS SCALE's replication functionality to send your data both within your system and to another separate TrueNAS SCALE system.

8.1 Important Notes - Upgrade to SCALE 22.12.2

Before proceeding with the replication chapter, especially the Remote Replication component, make sure that your evaluation machines are running at least TrueNAS SCALE 22.12.2 - or if you're reading this in the future, the latest available revision. TrueNAS SCALE 22.12.2, released on April 11, 2023, brought several additional enhancements to the replication workflow that we'll be making use of.

8.2 Local Replication

Local replication can be used for replicating between datasets or pools on the same system. This is useful if you are replicating from a smaller pool, such as one consisting of SSDs, to a larger pool made from HDDs. Two pools on the same system may also have different vdev layouts and capacities, or be configured with different levels of compression on their datasets.

For this example, we'll create a second dataset on our existing pool, but we'll increase the compression level. From the TrueNAS webUI, navigate to **Datasets** and select your **Evaluation** pool. Click the **Add Dataset** button on the top right.

Create a new dataset named **LocalReplica** and set the **Compression Level** to **GZIP-9**. This compression can yield improvements in space savings compared to the standard **LZ4** algorithm, but at reduced speeds. For live data, this might not be ideal; but as a target for replication purposes, the slower speed might be an acceptable tradeoff, especially as only changed data is replicated after the initial snapshot is taken.

From your TrueNAS webUI, navigate to **Data Protection** and under **Replication Tasks** choose the **Add** button. Select a **Source** and **Destination Location** and choose **On this System**. Use the tree view to select **Evaluation/EvalData** as the source folder, and Evaluation/LocalReplica as the destination.

Because we're moving quickly through the evaluation guide, the automatic snapshots configured in section 6.3 may not have had time to be captured yet. To ensure that we have at least one snapshot to replicate, check off the box indicating **Replicate Custom Snapshots** and adjust the naming schema from**auto-%Y-%m-%d_%H-%M to manual-%Y-%m-%d_%H-M** to capture the manual snapshot we created. If enough time has elapsed between configuration of automatic snapshots and replication for these snapshots to be populated, you can instead leave the default settings to replicate the existing automatic snapshots. Once you've completed this configuration, choose the **Next** button.

Adjust the **Replication Schedule** option to **Run Once** and uncheck the **Make Destination Dataset Read-Only** box. Adjust the **Destination Snapshot Lifetime** option to **Custom** and increase the retention period to **2 Months**. Choose the **Start Replication** button.

The replication task should enter the "PENDING" state. Once it changes to "SUCCESS" you can click on the green "SUCCESS" status to review the logs - it should indicate that a successful PUSH replication was completed. If the status does not automatically change, navigate to the **Dashboard** and then back to the **Data Protection** tab again.

8.3 Remote Replication - Hardware and Network Prerequisites

Local replication is excellent for having a second logical copy of the data, but it is still sharing the same hardware as the primary copy, which leaves the data vulnerable to physical incidents such as fire, flooding, or network and power outages, all of which could render the data temporarily or permanently inaccessible. To mitigate the impact of this issue, and add another layer to our data protection, the next step is to replicate the data to a remote TrueNAS system.

For prerequisites, the obvious first requirement is to have a second TrueNAS system. In this example, we're specifying TrueNAS SCALE 22.12.2 in order to leverage some additional features to enhance security. Your second evaluation system can be physical or virtual, provided that it contains sufficient usable storage to hold the test dataset to be replicated. For the purposes of this guide, we will refer to your existing system as **eval01** and the new system as **eval02**.

Ensure that both systems have the ability to connect to each other over TCP port 22 for SSH sessions, as well as TCP 80 and 443 for HTTP/HTTPS. This is typically possible if both systems are on the same subnet, but may not be guaranteed if there is a security device such as a firewall or intrusion detection and prevention system in place on your network. Check with your network administrator as any of these ports being closed will prevent replication from working properly.

8.4 Remote Replication - PUSH vs PULL Style

Two types of replication are supported with TrueNAS SCALE, termed as "PUSH" and "PULL" with the difference between the two being the location of the source data relative to the system that is initiating the replication operation. In our example, we have two systems, **eval01** and **eval02**:

If **eval01** is the primary system, and it runs a scheduled job to send a dataset to **eval02** it is considered a PUSH replication. If **eval01** is the primary system, but **eval02** runs the scheduled job, **eval02** is running a PULL replication. Both methods accomplish the same end result of data existing in both locations. PUSH replication has the advantage of synchronizing with the snapshots, but PULL replication carries security advantages. Both methods will be demonstrated in this section.

8.5 Remote Replication - PUSH - Dataset & User Configuration on Destination

In a PUSH replication, the source **eval01** system will be logging in to the receiving **eval02** system to send the data. This is useful for situations where the same data may be replicated to multiple target systems. In order to set this up, we will need to configure a limited user account on the **eval02** system before continuing.

On your secondary **eval02** system, go through the same initial steps of configuring a pool outlined in Section 5.2, using a different name for the pool such as **ArchivePool**. Create one new dataset called **homedirs** and a second called **PushReplica** using the steps outlined in Section 5.3.

While still on the **eval02** system, navigate to the **Credentials → Local Users** screen and choose the **Add** button. Name your user **pushrepl** and enable the slider beside **Disable Password** - this will prevent this user from inadvertently being used for administrative sign-in or access to shared folders. Scroll down to **Directories and Permissions**, and navigate to your dataset for **/mnt/ArchivePool/homedirs** - select the **homedirs** folder. Scroll down further and check the box for **Create Home Directory** to create a new folder for this user. Finally, **uncheck** the **Samba Authentication** box, and click **Save**. As configured, this user will not be able to sign into the TrueNAS SCALE administrative UI, cannot SSH with a password, or connect to any shared folders over SMB.

8.6 Remote Replication - PUSH - Configure Replication

Return to the **eval01** system. Open the **Data Protection** menu, and under **Replication Tasks**, choose the **Add** button. Select your **Source Location** as **On this System** and use the tree view to select **Evaluation/EvalData** as the source folder.

For **Destination Location**, select **On a Different System**. This will cause a new drop-down option to appear for **SSH Connections**. From this drop-down, select **Create New** which will cause a window to appear for **New SSH Connection**.

In the **New SSH Connection** window, enter a name to save this connection. Using a descriptive name that includes the system names and direction of transfer such as **"eval01-to-eval02"** can help streamline future administration tasks. For **Setup Method** leave the selected **Semi-automatic (TrueNAS only)** as we will be establishing an SSH connection between two TrueNAS SCALE systems.

In **Authentication**, enter **https://** followed by the URL or IP of your secondary TrueNAS SCALE system **eval02** that will be used as the PUSH replication target. Enter the **Admin Username** as **admin** and the password you set on your second TrueNAS SCALE system for **Admin Password**. In the next **Username** field, enter your newly created **pushrepl** user, and for the **Private Key** select **Generate New**. Check the box for **Enable passwordless sudo for zfs commands**. Leave the **Cipher** option as **Standard**, noting that the options for reduced security should only be used within secure and trusted networks. Click **Save**. A separate dialog box will appear asking you to confirm the use of the **sudo** command for privilege elevation. Click **Use Sudo for ZFS Commands** on this new dialog to ensure functionality of replication.

Back in the **Replication Task Wizard** window, use the tree view under **Destination Location** to select **ArchivePool/Pull-Replica** as the destination dataset location. Determine if you need to check off the box indicating **Replicate Custom Snapshots**, as identified previously in section 8.2 for local replication. If enough time has elapsed, no changes are necessary, but if there are no snapshots detected by the replication wizard, please check the **Replicate Custom Snapshots** box and adjust the naming schema from **auto-%Y-%m-%d_%H-%M to manual-%Y-%m-%d_%H-M** to capture the manual snapshot. Choose the **Next** button.

Adjust the **Replication Schedule** option to **Run Once** and uncheck the **Make Destination Dataset Read-Only** box. Adjust the **Destination Snapshot Lifetime** option to **Custom** and increase the retention period to **2 Months**. Choose the **Start Replication** button.

Similar to our local replication task, this new task will enter the "PENDING" state, and change to "SUCCESS" upon completion. Change your browser to your secondary **eval02** system, and click on **Datasets** in the left pane and then your **PushReplica** dataset. Confirm that a non-zero number of snapshots exists under the **Data Protection - Total Snapshots** value on the right.

The same SSH connection can be used for multiple PUSH replication jobs from **eval01** to **eval02**, for different datasets or on different schedules.

8.7 Remote Replication - PULL - Dataset & User Configuration on Source

In contrast to the PUSH replication, the PULL replication causes the receiving **eval02** system to sign in to the source **eval01** system. This scenario is beneficial for an isolated "recovery vault" that does not accept incoming connections. With the primary system having no ability to sign into the destination, the second copy cannot be deleted inadvertently by administrator error or deliberately by malicious action such as ransomware.

Using the TrueNAS web UI on your primary **eval01** system, repeat the steps in section 5.3 to create a dataset called **homedirs** on your existing pool named **Evaluation**. Navigate to **Credentials → Local Users**, and choose the Add button. Similarly to section 8.5 above, create a user named **pullrepl** with a disabled password. Ensure that you set the home directory to **/mnt/Evaluation/homedirs** and check the **Create Home Directory** box before clicking the **Save** button. Return to the secondary **eval02** system and use the **Datasets** window to add a new dataset named **PullReplica**.

8.8 Remote Replication - PULL - Configure Replication

On your secondary **eval02** system, navigate to the **Data Protection** screen. Note that the PUSH replication job configured on **eval01** is not shown here. Under **Replication Tasks**, click **Add**. Select your **Source Location** as **On a Different System**, causing the **SSH Connections** drop-down option to appear. As the SSH connection created in our previous PUSH replication was one-direction-only, select **Create New** from this drop-down to prompt the **New SSH Connection** window to appear again.

In the **New SSH Connection** window, enter the "reverse order" of the name used in the previous PUSH replication, in this case using **"eval02-to-eval01"** for similar reasons of clarity. For **Setup Method** leave the selected **Semi-automatic (TrueNAS only)** as we will be establishing an SSH connection between two TrueNAS SCALE systems once again.

In **Authentication**, enter **https://** followed by the URL or IP of your source TrueNAS SCALE system **eval01** that will be used as the PULL replication source. Enter the **Admin Username** as **admin** and the password you set on your first TrueNAS SCALE system for **Admin Password**. In the next **Username** field, enter your newly created **pullrepl** user, and for the P**rivate Key** select **Generate New**. Check the box for **Enable passwordless sudo for ZFS commands**. Leave the **Cipher** option as **Standard**, noting that the options for reduced security should only be used within secure and trusted networks. Click **Save**. A separate dialog box will appear asking you to confirm the use of the **sudo** command for privilege elevation. Click **Use Sudo for ZFS Commands** on this new dialog to ensure functionality of replication.

Back in the **Replication Task Wizard** window, use the tree view to select **Evaluation/EvalData** as the source folder. For **Destination Location**, note that the drop-down option has been set to **On this System** and cannot be changed. Use the tree view to select **ArchivePool/PullReplica** as the destination dataset location. Note that unlike PUSH replication, the only option for PULL is to identify snapshots using either a name or regular expression match. Leave the **Naming Schema** radio option selected, and determine if the naming schema should be adjusted from **auto-%Y-%m-%d_%H-%M** to **manual-%Y-%m-%d_%H-M** if the only snapshots present were manually taken. Choose the **Next** button.

Adjust the **Replication Schedule** option to **Run Once** and uncheck the **Make Destination Dataset Read-Only** box. Adjust the **Destination Snapshot Lifetime** option to **Custom** and increase the retention period to **2 Months**. Choose the **Start Replication** button. Finally, click on **Datasets** in the left pane and then your **PullReplica** dataset. Confirm that a non-zero number of snapshots exists under the **Data Protection - Total Snapshots** value on the right.

9 Security Best Practices

At this point in the evaluation guide, the test data on your TrueNAS SCALE system has been shared out over SMB, with recurring snapshots configured on both an hourly and daily basis with different retention periods to ensure a combination of space efficiency and granular restore options. This section reviews some of the methods available to you for securing your TrueNAS system and protecting your data from threats like ransomware.

9.1 Stay Up to Date with TrueNAS Patches

Updates to both TrueNAS SCALE and CORE are released frequently by iXsystems, and detailed on the Software Status page. These updates contain feature enhancements, bug fixes, and security patches to not just TrueNAS itself, but other services and open source software used within TrueNAS. Typically new updates are released for general use, but if your organization considers itself particularly conservative or uses TrueNAS in a "mission critical" environment, waiting for additional validation in complex environments may be preferred.

By default, TrueNAS SCALE will check for updates on a daily basis and automatically download them. You can check under **System Settings → Update** manually, or if you receive a notification that an update is ready to be applied.

9.2 Use Strong Passwords - and Don't Re-Use Them

When configuring your TrueNAS SCALE administrative account, use a strong, unique password containing a mix of uppercase and lowercase letters, numbers, and special characters. Avoid reusing passwords from other systems or services, and especially ensure that you set different administrative passwords on two machines that are replicating data to or from each other. This will ensure that even in case of credential compromise, only one system is impacted.

9.3 Configure Two-Factor Authentication (2FA)

To help further safeguard your administrative account, TrueNAS supports two-factor authentication using Time-based One Time Passwords (TOTP).

Since TOTP codes are time-based, as the name suggests, it's important to confirm that your TrueNAS SCALE hardware has the ability to keep time accurately. Use the Coordinated Universal Time (UTC) standard when setting your hardware clock in your BIOS or EFI firmware, and set the correct time zone within TrueNAS under **System → General**. Once you've confirmed that the time is correct, use the same screen to configure one or more Network Time Protocol (NTP) servers.

By default, TrueNAS SCALE uses publicly available servers from the Debian Linux NTP pool, but if your organization has its own internal NTP server, or you wish to prevent TrueNAS SCALE from requiring an Internet connection, configure it as the primary time source here.

Before enabling 2FA, ensure that you have a TOTP-compatible authenticator application downloaded onto your smartphone or other device. Navigate to the **Credentials** section of the SCALE UI and then the 2FA option. Choose the large **Enable Two-Factor Authentication** button. Confirm that you want to enable 2FA, and then, using your mobile device, scan the provided QR code. Ensure that your device has registered a new account for your TrueNAS system with a name of **hostname@TrueNAS**, then choose the Power icon in the top-right corner of the screen and select Log Out. On the new sign-in screen, enter your administrative username and password, as well as the new TOTP code.

Note that enabling 2FA is a system-wide setting, and the 2FA code is unique to the server. Even if an additional administrative account is created manually with a separate name and password, access to the webUI will require the 2FA code.

9.4 Secure the Physical Machine Itself

One of the original "Ten Immutable Laws of Security" from the turn of the millennium refers to this concept. The third of these ten laws states "if a bad guy has unrestricted physical access to your computer, it's not your computer anymore" - and this applies to TrueNAS just as much as a desktop or laptop computer. The TrueNAS SCALE console offers a useful fail-safe ability to reset a forgotten root password, disable the two-factor authentication that we enabled, and recover from a network misconfiguration, but this access should be restricted to trusted users only.

You can improve physical security by securing your TrueNAS server in a room or area with access controls such as physical, electronic, or biometric locks. Only approved administrators or maintenance personnel should be provided with access to the room, and ensure that these access logs are audited regularly.

The TrueNAS console itself can be locked down to require a root login before allowing actions as well. Navigate to the **System → Advanced** menu, and uncheck the setting for **Show Text Console without Password Prompt**. Save your changes, then open the console for your TrueNAS system. You'll need to enter the TrueNAS CLI, and then enter the command `exit` to log out.

9.5 Limit Access to Authorized Networks at the Protocol Level

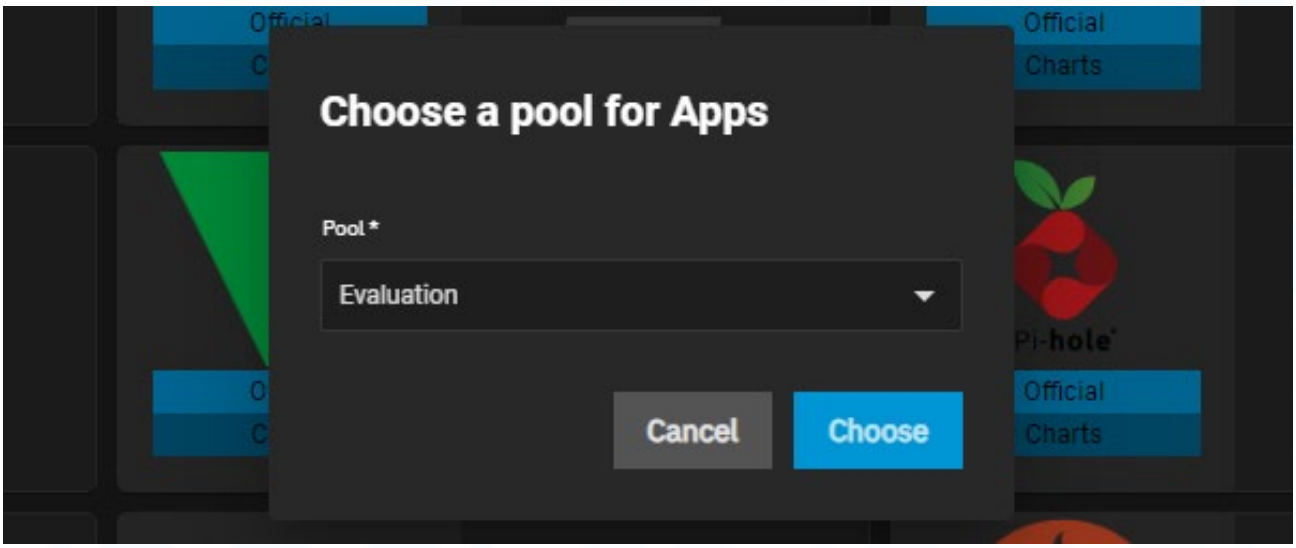
The sharing protocols on TrueNAS can be configured to allow or deny access to clients by their IP address or network range. This can be done on a per-share basis, and works in addition to existing access control list (ACL) and username/password requirements, allowing for further levels of granular control such as preventing direct access from users connected from a specific site or over a VPN. Each protocol has a different method of controlling access; SMB uses the Hosts Allow field, NFS controls via the Allowed Networks function, and iSCSI can use initiator names and CHAP authentication. Further information is available for reading in the linked sections of the TrueNAS Documentation site above.

10 Installing and Using the App Catalog

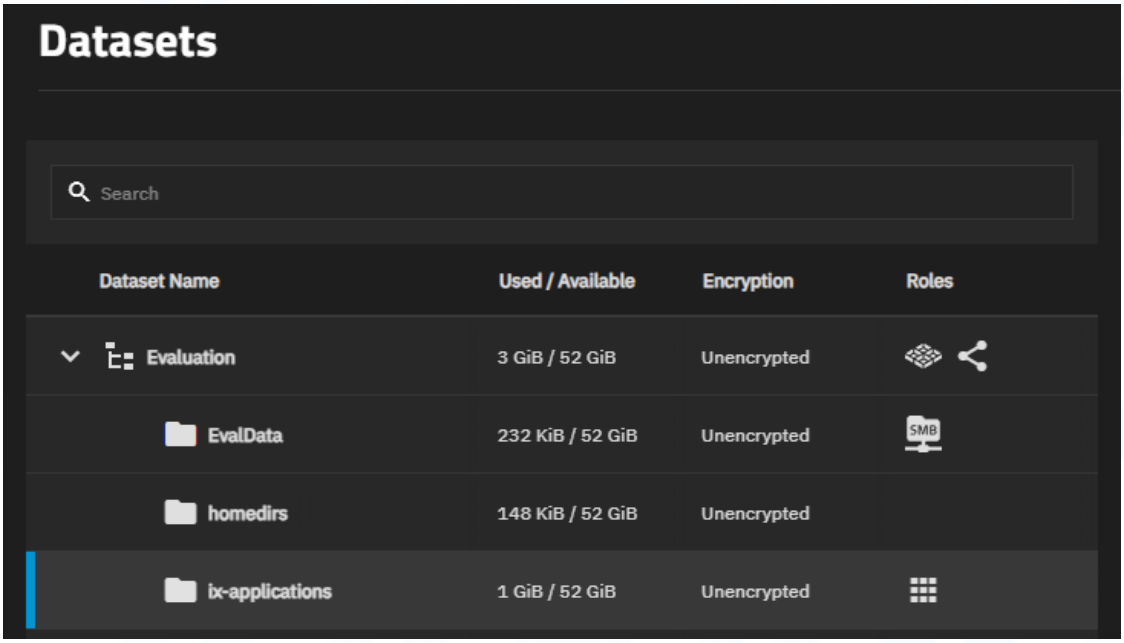
One of the major new features that TrueNAS SCALE introduced over CORE was the inclusion of easy-to-deploy applications through the TrueNAS Apps Catalog. These Apps can be run directly on your TrueNAS SCALE machine, with much less overhead than traditional virtual machines, and closer access to your storage. To get started, navigate to the **Apps** page in the sidebar.

10.1 Selecting an App Pool

You'll be asked to select a pool for the Apps. This is where the Apps themselves will be downloaded to, and where they will be launched from. Your Apps pool doesn't have to be the same pool as the Apps will read or write data to; for best performance, this could be a pool made of solid-state devices, but because Apps also benefit from ZFS read and write acceleration, hard drive based pools can work just as well for light workloads.



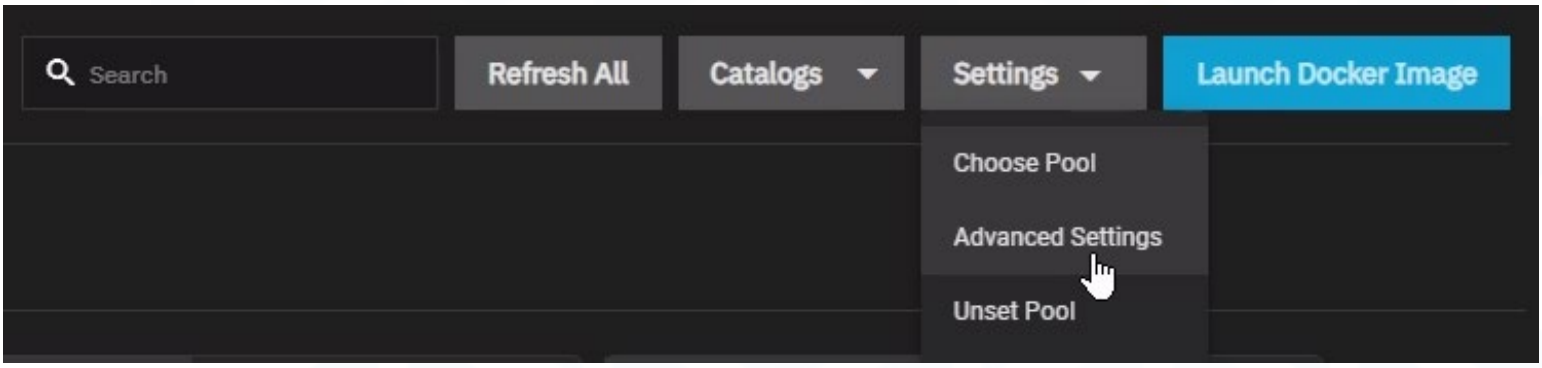
Once a pool is chosen, TrueNAS SCALE will automatically create an "ix-applications" dataset that can be seen under the **Datasets** page.



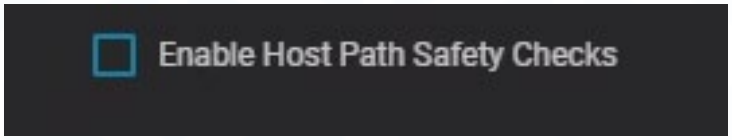
Once the initial configuration is complete, you can check out the listing of available applications. Some Apps are designated as “Official” TrueNAS Apps, such as NextCloud or PiHole, while others are community-supported, such as the popular open-source media server Jellyfin. Other applications have received additional testing by iXsystems and are listed under the “Enterprise” category. We’ll install the Jellyfin media server as our example App, but before we continue, we’ll make a quick change to the **Advanced Settings** in the Apps page.

10.2 Host Path Safety Checks

In **Advanced Settings**, we’ll need to uncheck the **Enable Host Path Safety Checks** option, in order to allow simultaneous sharing of folders between NAS protocols such as SMB, and applications.



Uncheck the setting shown below, and carefully read the warning prompt that appears.



Because this setting allows for both the App and another source to access the files simultaneously, data safety issues can arise if both the app and a connected client modify the files at the same time. Since the Jellyfin app is only reading from the shared files, the risk here is smaller; but for applications such as NextCloud that might be writing to files, it’s a good idea to set up regular ZFS snapshots (see Section 6) to protect your data from accidental damage.

Acknowledge the warning, click **Continue**, and then scroll to the bottom of the **Advanced Settings** pane and click **Save**.

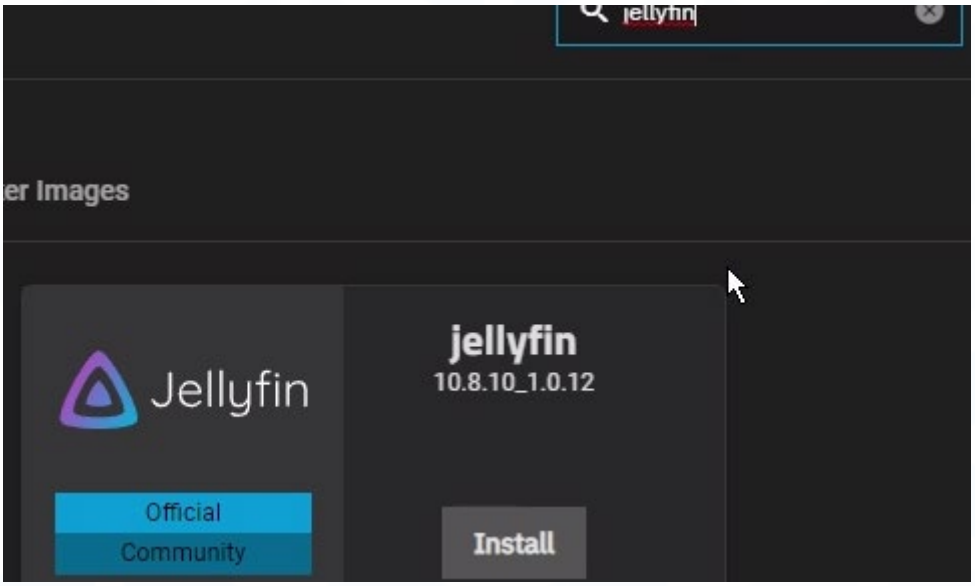
10.3 Create and Share a Dataset for Host Path Sharing

Once the setting is saved and updated, we’ll want to create a folder to use with the Jellyfin app. Return to **Datasets**, and create a new dataset called **Media**. At the bottom of this section, select a **share type** of **Apps** which will automatically give the TrueNAS SCALE Apps user access to this folder. Once the dataset is created, you can see under the **Permissions** section that the Apps user has been allowed **Special** access.

Follow the instructions from Section 5.5 to share this new **Media** folder over SMB, so that you can add a sample media file.

10.4 Installing a TrueNAS SCALE App

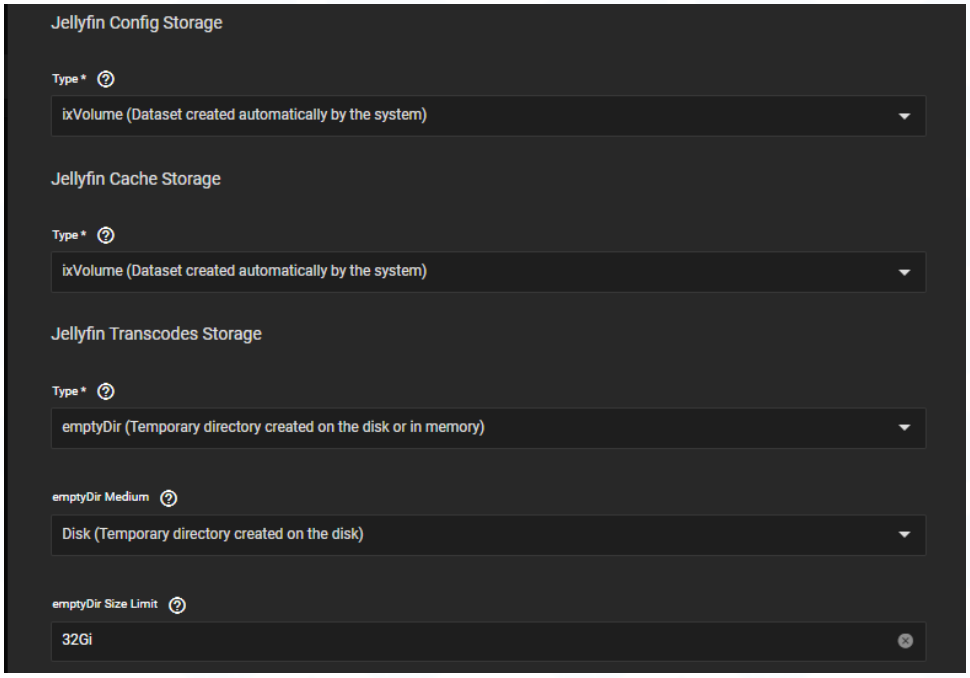
Once you've confirmed that your share can be accessed over the network, return to the **Apps** page in TrueNAS, navigate to the **Available Applications** tab at the top, and search for the **Jellyfin** App using the Search dialog box. Choose the **Install** button.



For Official and many Community applications, a large number of the chart options are pre-populated, with available tooltips for more information on whether or not they need to be changed from their defaults. Under the User and Group Configuration, we can see a user and group ID of number 568, which is assigned to the "apps" user that we gave permission to the dataset beforehand. Like most official Apps, the Jellyfin chart is provided with a pre-configured network port value. Network ports for TrueNAS SCALE Apps may be different from the default ports used by the software when it is installed standalone or on other platforms, so take note of this for future use when configuring and connecting client applications.

10.5 Assigning Storage - ixVolumes

The next step is to assign storage to the App. Each App can have a different number of required volumes, so it's important to understand what the App will do with each volume, and the nature of the data stored there.

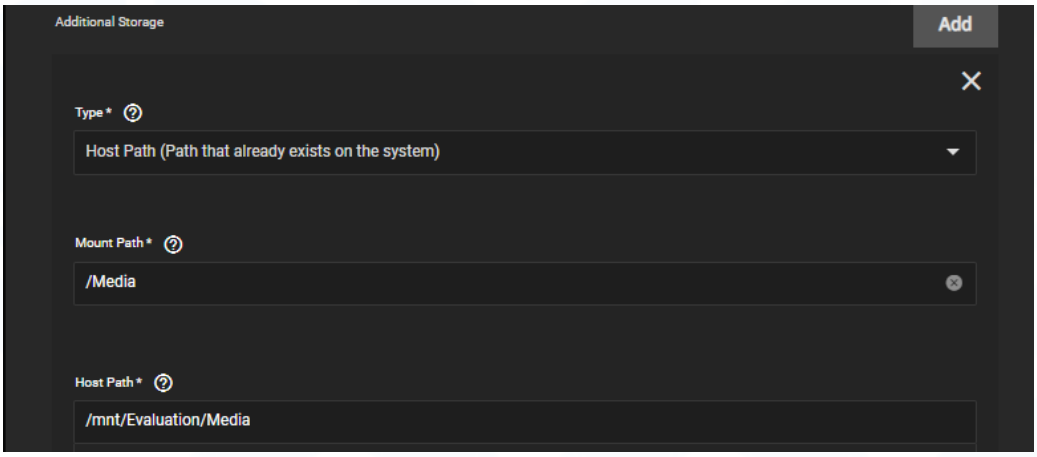


Most apps will have a “configuration” volume at the minimum, where the app itself stores its settings. By default, TrueNAS Apps use an ixVolume, which is an app-specific dataset in the same pool that you selected during the initial configuration, nested under the automatically created ix-applications dataset. An ixVolume isn’t deleted when the container is stopped or removed, but it also can’t be shared through other means such as SMB or NFS. These are ideal for data that is only needed by the App itself. Some Apps are configured to use multiple paths for different types of data; our example App Jellyfin uses a separate volume for caching media metadata such as thumbnails, ratings, and reviews. Because this metadata is different from traditional ZFS metadata, it needs to be stored in a format that Jellyfin understands and a location it can access.

Finally, an emptyDir volume can be used to hold temporary files that don’t need to be retained when the App is shut down, such as transcoded media files for streaming to mobile devices or web clients. These volumes can use either the “Disk” or “Memory” storage type. For most cases, the “Disk” storage type is safer for use, as the “Memory” type will consume some of your available memory that might otherwise be used by TrueNAS for ZFS read and write acceleration, or for the App itself to work with. Because each App may have different requirements, it’s important to consult the documentation provided by the app developer themselves to determine how best to set up the storage volumes. In this case, we’ll use a “Disk” type medium, and set the size to 32GiB to allow for multiple simultaneous transcodes to occur if needed.

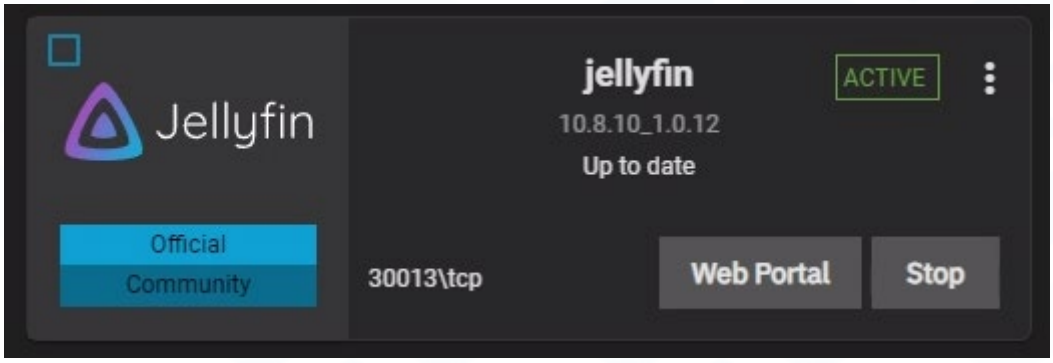
10.6 Assigning Storage - Host Path

Once we’ve configured the storage for the app itself, we need to attach our Media folder. Choose to **Add** an **Additional Storage** type, and change it from ixVolume to a Host Path which lets us present a dataset directly from your ZFS pool. Select the **Media** dataset under the **Evaluation** pool as the **Host Path**, and then enter a **mount path** that will be shown inside the application itself, such as /Media - note the name of the **mount path** for later.

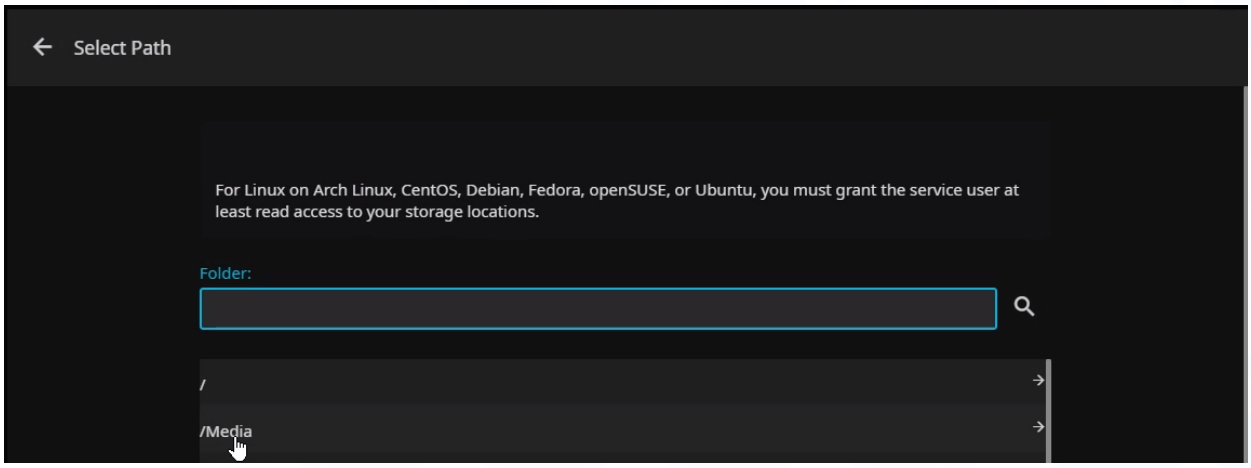


Each App can also have a limit set for both CPU and memory utilization - this will allow for performance For some applications, a **GPU** resource can be added in order to accelerate specific workloads, such as media transcoding or machine learning. Most recent Intel and NVIDIA GPUs can be used, but it’s important to check both the TrueNAS SCALE release notes and the App’s compatibility listing before making any hardware purchases.

Click **SAVE** and TrueNAS SCALE will validate your configuration, then return to the Installed Applications page to monitor the download and deployment of the application. Once the app becomes Active, you can see the port number assigned, as well as click on the Web Portal button to launch the app itself.



While configuring the application, note that setting up the media library requires the use of the **Mount Path** folder of /Media rather than its **Host Path** of /mnt/evaluation/media. We'll complete the setup and sign in, then we'll copy a movie over to the shared Media folder.



Because the App has access to the same shared folder, Jellyfin can automatically rescan and refresh its media libraries; and if available, the copied file will have been indexed, with a thumbnail, rating, and summary populated.

10.7 Launching Docker Images

iXsystems has worked to bring many of the most common and popular apps to TrueNAS SCALE through both the Official and Community catalogs. If you're not able to find your desired app through the catalog, or you're an experienced Docker user, there's also the option to launch a Docker image manually using the blue **Launch Docker Image** button from the **Apps** page in the top-right hand corner. Using the manual image launch process exposes much more of the Docker configuration steps, such as container entry points, environment variables, and custom network settings. Each Docker container will require different settings; a simple NGINX web server may only need a port forwarding rule to make its internal HTTP port 80 visible on the node's port of 9080, but a more complicated application may require additional configuration. Note that when installing custom Docker containers, TrueNAS SCALE requires that you choose external node ports with a value of over 9000, as ports below this value are reserved.

10.8 Removing TrueNAS SCALE Apps

If you decide you no longer need an application, you can stop it from within the TrueNAS Apps page, and then delete it from the additional menu. If you don't plan to reinstall the application later, you can also choose to delete the Docker Image itself. Note that if you delete an application with data saved in an ixVolume, that data will be permanently removed as well - but any data stored in a shared **Host Path** will be retained.

10.9 Built-In Apps

Some selected apps which start on the TrueNAS Apps page become integrated into the TrueNAS SCALE management interface directly, as a service. One such built-in App is the iX-Storj service, which can be used to connect to the Storj globally distributed storage network for S3-compatible storage for backup, replication, and other uses for offsite cloud storage.

Built-in Apps are integrated into appropriate sections in the TrueNAS SCALE UI, such as the "Data Protection" and "Cloud Credentials" pages for iX-Storj, and typically require a minimal amount of configuration to enable, such as entering credentials, synchronization direction, and remote folder path. For details on iX-Storj, see the micro-site at truenas.com/ix-storj/ and follow our easy video tutorial to configure iX-Storj as an additional backup target.

11 Wrapping Up

At this point, we've created a data pool, experimented with adding and removing drives, as well as presented a dataset over SMB to a network client, and shown the value of TrueNAS SCALE's immutable snapshot technology to restore the previous versions of files and folders. Replication was used to add an additional layer of data protection by syncing our data to a second pool, and also a second system. We looked at some suggested practices to enhance the security of our TrueNAS SCALE system, and dipped our toes into the sea of available TrueNAS SCALE Apps that can let us run popular software directly from the system itself, with close access to the storage.

While this guide covers the process of configuring the most commonly used features, TrueNAS SCALE has an abundance of additional features and value. We are looking to create a series of videos to compliment this guide that will go deeper into topics for technical enthusiasts and IT experts.

- User and Group Management
- File System Permissions and Access Control Lists (ACLs)
- iSCSI
- NFS
- Object Storage
- Performance optimization
- Advanced Administration

We welcome suggestions and feedback at marketing@ixsystems.com.

We hope that you have found the time learning about TrueNAS to be well-spent, and you have a better understanding of where you can use TrueNAS in your environment on your quest for True Data Freedom.

©2023 iXsystems, Inc. All rights reserved. TrueNAS®, TrueNAS SCALE®, TrueCommand®, and all associated logos and designs are trademarks or registered trademarks of iXsystems Corporation. All other registered trademarks or trademarks are the property of their respective owners.