TrueNAS CORE and Enterprise

- 1: Getting Started
  - 1.1: CORE Hardware Guide
  - 1.2: Install
  - 1.3: Console Setup Menu
  - 1.4: Logging In
  - 1.5: Storage Configuration
  - 1.6: Sharing Storage
  - 1.7: Data Backups
  - 1.8: Applications

- 2: Accounts
  - 2.1: Groups
  - 2.2: Users

- 3: System
  - 3.1: General
    - 3.1.1: Settings
    - 3.1.2: System Config Backups
    - 3.1.3: Managing TLS Ciphers
  - 3.2: NTP Servers
  - 3.3: Boot
    - 3.3.1: Boot Screen
    - 3.3.2: Mirroring the Boot Pool
  - 3.4: Advanced
  - 3.5: View Enclosure
  - 3.6: Email
  - 3.7: System Dataset
  - 3.8: Reporting
  - 3.9: Alert
  - 3.10: Cloud Credentials
  - 3.11: SSH
  - 3.12: Tunables
  - 3.13: Update
  - 3.14: CAs
  - 3.15: Certificates
  - 3.16: ACME DNS
  - 3.17: KMIP
  - 3.18: Failover (HA)
  - 3.19: Support
  - 3.20: 2FA (Two-Factor Authentication)

- 4: Tasks
  - 4.1: Cron Jobs
  - 4.2: Init/Shutdown Scripts
  - 4.3: Rsync Tasks
  - 4.4: S.M.A.R.T. Tests
  - 4.5: Periodic Snapshot Tasks
  - 4.6: Replication Tasks
    - 4.6.1: Local
    - 4.6.2: Remote
    - 4.6.3: Advanced
    - 4.6.4: Troubleshooting Tips
  - 4.7: Resilver Priority
  - 4.8: Scrub Tasks
  - 4.9: Cloud Sync Tasks
  - 4.10: How To Back Up Google Drive to TrueNAS CORE
5: Network
   5.1: Network Summary
   5.2: Global Configuration
   5.3: Interfaces
      ■ 5.3.1: Setting a Static IP Address for the TrueNAS UI
      ■ 5.3.2: Editing a Physical Interface
   5.4: Static Routes
   5.5: Enabling WireGuard
   5.6: IPMI

6: Storage
   6.1: Pools
      ■ 6.1.1: Pool Creation
      ■ 6.1.2: Pool Import
      ■ 6.1.3: Managing Pools
      ■ 6.1.4: Datasets
      ■ 6.1.5: Zvols
      ■ 6.1.6: Permissions
      ■ 6.1.7: Storage Encryption
      ■ 6.1.8: Fusion Pools
      ■ 6.1.9: SLOG Overprovisioning
   6.2: Snapshots
   6.3: VMware-Snapshots
   6.4: Disks
      ■ 6.4.1: Wipe
      ■ 6.4.2: Replacement
   6.5: Self-Encrypting Drives
   6.6: Import Disk

7: Directory Services
   7.1: Active Directory
   7.2: LDAP
   7.3: NIS
   7.4: Kerberos

8: Sharing
   8.1: Apple Shares (AFP)
      ■ 8.1.1: Share Creation
   8.2: Block Shares (iSCSI)
      ■ 8.2.1: iSCSI Shares
      ■ 8.2.2: Fibre Channel
   8.3: Unix Shares (NFS)
      ■ 8.3.1: Share Creation
   8.4: WebDAV Shares
      ■ 8.4.1: Share Creation
   8.5: Windows Shares (SMB)
      ■ 8.5.1: Share Creation
      ■ 8.5.2: Home Shares
      ■ 8.5.3: Shadow Copies

9: Services
   9.1: Dynamic DNS
   9.2: FTP, SFTP, and TFTP
   9.3: LLDP
   9.4: OpenVPN
   9.5: S3
   9.6: SNMP
   9.7: SSH
   9.8: UPS

10: Applications
   10.1: Jails
      ■ 10.1.1: Create
      ■ 10.1.2: Manage
      ■ 10.1.3: Installing Software
TrueNAS is the world’s most popular Open Source storage operating system and is the most efficient solution for managing and sharing data over a network. It is the simplest way to create a safe, secure, centralized, and easily accessible place for your data. TrueNAS Open Storage provides unified storage for file, block, object, and application data.
TrueNAS can be installed on virtually any hardware platform and is suitable for home, business, and enterprise applications. There are three editions of TrueNAS that enable a broad range of applications while sharing common management tools and enabling data transfers:

**TrueNAS CORE** is free and Open Source and is the successor to the wildly popular FreeNAS. It runs on virtually any x86_64 system and provides a broad set of features for many users. Plugin applications like Plex, NextCloud, and Asigra allow the functionality of a system to be customized for many use cases.

**TrueNAS Enterprise** is provided as a system with either single or dual controllers to enable High Availability (HA). It can also be provided with Enterprise-grade support from iXsystems. Coupled with the TrueNAS M-Series system, it scales to 15GB/s and 20 PB with five 9's of uptime.

**TrueNAS SCALE** is the latest member of the TrueNAS family and provides Open Source HyperConverged Infrastructure including Linux containers and VMs. TrueNAS SCALE includes the ability to cluster systems and provide scale-out storage with capacities of up to hundreds of Petabytes. It is currently in development and will be available for deployment in 2021.

TrueNAS Software products offer market-leading features to be the most effective NAS solution:

- **OpenZFS for Maximum Protection and Performance**

All TrueNAS editions leverage the enterprise-grade OpenZFS file system to provide an all-inclusive data management solution that is designed for decades of continuous use. To provide the perfect balance between total storage capacity and data redundancy, storage pools can be configured in a variety of RAIDZ or Mirrored configurations. Pools can even be expanded when new disks or SSDs are added to the system, allowing your storage environment to grow with application requirements.
ZFS protects your data with features like Copy-on-Write, Checksums, Scrubbing, and 2-Copy Metadata. Automated replication ensures you can keep a bit-for-bit identical copy of your data safe in a remote storage location and fast resilvering times mean that if a disk fails, a replacement disk can be quickly integrated into the degraded data storage pool. ZFS uses efficient snapshot and cloning techniques to maximize available space, as well as in-line data compression, thin provisioning, and deduplication.

- **Security-focused to give you Peace of Mind**

TrueNAS supports a variety of security solutions including self-encrypted drives (SEDs) and ZFS native dataset encryption. Access control lists are fully customizable and provide another layer of protection for sensitive data. TrueNAS supports FIPS 140-2 Level 2 drives and installs with secure defaults in place, including encryption for file transfers and disabling SSH. Local users and groups can be managed, along with integrating TrueNAS with LDAP, Active Directory, Kerberos, and NIS. For enterprises, centralized key management (KMIP) is also available.

- **Sharing Your Data has Never Been Easier**

TrueNAS supports all the prominent network file sharing and remote backup options, and can even be expanded with applications from FreeBSD or Linux. Supported sharing protocols include NFS (v3,4), SMB (v1,2,3,4), AFP, FTP, WebDAV, and rsync. TrueNAS fully supports block sharing (iSCSI, Fibre Channel) and has been certified for use with vSphere, Citrix, and Veeam. Want to securely import or back up data with a Cloud Storage Provider? No problem! TrueNAS can even store and sync your S3 data with an automated schedule.

- **TrueNAS Delivers a Rich Set of Features**

There are an enormous number of features in each TrueNAS edition. You can read the Open Source software, try out TrueNAS in a VM at zero cost, or have a look through this chart which summarizes the key features (TrueNAS 12.0 features are in blue).
TrueNAS SCALE uses much of the same TrueNAS CORE source code, but adds a few different capabilities which are defined by this acronym:

- **S**cale-out ZFS
- **C**onverged
- **A**ctive-active
- **L**inux containers
- **E**asy-to-manage

Run TrueNAS on Any System

TrueNAS delivers Software Defined Storage (SDS) and runs on any x86_64 server, no matter how old or modern. Intel and AMD processors or any generation are supported, whether it’s a single core or a sixty-four core behemoth. The TrueNAS hardware guide provides recommendations to assist you in building your own systems.

TrueNAS software has been developed under the sponsorship of iXsystems since 2009 and uses a large team of professionals who develop, build, QA, document, and support the Open Source software and the TrueNAS community. Since the TrueNAS software is free, iXsystems grows its business by building professional and enterprise-grade systems that have similar reliability to the major NAS vendors, but at a much lower Total Cost of Ownership (TCO). The iXsystems proposition is that TrueNAS enables dramatic storage cost savings through Open Source economics. TrueNAS provides the industry’s most powerful Open Storage.
TrueNAS can be downloaded from this page.

The current TrueNAS systems available cover a wide range of sizes and use cases! Go to the hardware section to learn more about each family of TrueNAS hardware.

**Join the Expert Community**

TrueNAS comprises both the Open Source software and an experienced and expert community developed over the last dozen years. Ask for advice and contribute your experiences for others to use. The community can save you many hours and be a great resource for new projects and applications. If you need more professional support, iXsystems offers Bronze/Silver/Gold Enterprise support including 24x365 coverage and onsite support with its systems.

**TrueCommand Manages your NAS Fleet**

TrueCommand is a single Pane-of-Glass management application that takes the repetitive work out of multi-TrueNAS management by centralizing system alerts, reports, and analytics in one easy to use interface. It supports users and teams with 24x365 global operations, role-based access control, and a full log of every TrueNAS configuration change. TrueCommand runs on docker, VMs, or as a cloud service and is free to users with less than 50 drives and affordable for those with larger installations. Read more information about TrueCommand in the overview article.
1 - Getting Started

This section guides you through installing and accessing TrueNAS, storing and backing up data, sharing data over a network, and expanding TrueNAS with different applications solutions.

For more detailed interface reference articles, configuration instructions, and tuning recommendations, see the remaining sections in this topic. Content sections are organized by order of appearance in the web interface.
1.1 - CORE Hardware Guide

- **Minimum Hardware Requirements**
- **Storage Considerations**
  - Storage Media
  - Storage Solutions
  - Storage Device Sizing
  - Storage Device Burn-In
  - Storage Controllers
  - SAS Expanders
  - Storage Device Cooling
- **Memory, CPU, and Network Considerations**
  - Memory Sizing
  - Error Correcting Code Memory
  - Central Processing Unit (CPU) Selection
  - Remote Management: IPMI
  - Power Supply Units
  - Uninterruptible Power Supplies
  - Ethernet Networking
  - High-Speed Interconnects
- **Virtualized TrueNAS CORE**

---

From repurposed systems to highly-custom builds, the fundamental freedom of TrueNAS is the ability to run it on almost any x86 computer.

**Minimum Hardware Requirements**

The recommended system requirements to install TrueNAS:

<table>
<thead>
<tr>
<th>Processor</th>
<th>Memory</th>
<th>Boot Device</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-Core Intel 64-Bit or AMD x86_64 Processor</td>
<td>16 GiB Memory</td>
<td>16 GB SSD Boot Device</td>
<td>Two identically-sized devices for a single storage pool</td>
</tr>
</tbody>
</table>

The TrueNAS installer recommends 8 GB of RAM. TrueNAS installs, runs, operates jails, hosts SMB shares, and replicates TBs of data with less. ixsystems recommends the above for better performance and fewer issues.

You don’t need an SSD boot device, but we discourage using a spinner or a USB stick for obvious reasons. We do not recommend installing TrueNAS on a single disk or striped pool unless you have a good reason to do so. You can install and run TrueNAS without any data device, but we strongly discourage it.

TrueNAS does not require two cores, as most halfway-modern 64-bit CPUs likely already have at least two.

For help building a system according to your unique performance, storage, and networking requirements, read on!

**Storage Considerations**

The heart of any storage system is the symbiotic pairing of its file system and physical storage devices. The ZFS file system in TrueNAS provides the best available data protection of any file system at any cost and makes very effective use of both spinning-disk and all-flash storage or a mix of the two. ZFS is prepared for the eventual failure of storage devices. It is highly configurable to achieve the perfect balance of redundancy and performance to meet any storage goal. A properly-configured TrueNAS system can tolerate the failure of multiple storage devices and even recreate its boot media with a copy of the configuration file.

**Storage Media**

Choosing storage media is the first step in designing the storage system to meet immediate objectives and prepare for
future capacity expansion.

- **Spinning Disks**
  Until the next scientific breakthrough in storage media, spinning hard disks are here to stay thanks to their balance of capacity and cost. The arrival of double-digit terabyte consumer and enterprise drives provides more choices to TrueNAS users than ever. TrueNAS Mini systems ship with Western Digital NAS and NL-SAS for good reason. Understanding the alternatives explains this decision.

- **SATA NAS Disks**
  Serial Advanced Technology Attachment (SATA) is still the de facto standard disk interface found in many desktop/laptop computers, servers, and some non-enterprise storage arrays. SATA disks first arrived offering double-digit gigabyte capacities and are now produced to meet many capacity, reliability, and performance goals. While consumer desktop SATA disks don’t have the problematic overall reliability issues they once had, they are still not designed or warrantied for continuous operation or use in RAID groups. Enterprise SATA disks address the always-on factor, vibration tolerance, and drive error handling required in storage systems. However, the price gap between desktop and enterprise SATA drives is vast enough that it forces users to push their consumer drives into 24/7 service to pursue cost savings.

  Drive vendors, likely tired of honoring warranties for failed desktop drives used in incorrect applications, responded to this gap in the market by producing NAS drives. NAS drives achieved fame from the original Western Digital (WD) Red™ drives with CMR/PMR technology (now called WD Red Plus). Western Digital designed the WD Red™ Plus NAS drives (non-SMR) for systems with up to 8 hard drives, the WD Red™ Pro for systems with up to 16 drives, and the WD UltraStar™ for systems beyond 16 drives.

  The iXsystems Community Forum regards WD drives as the preferred hard drives for TrueNAS builds due to their exceptional quality and reliability. All TrueNAS Minis ship with WD Red™ Plus drives unless requested otherwise.

- **Nearline SAS Disks**
  Nearline SAS (NL-SAS) disks are 7200 RPM enterprise SATA disks with the industry-standard SAS interface found in most enterprise storage systems. SAS stands for **Serial Attached SCSI**, with the traditional SCSI disk interface in serial form. SAS systems, designed for data center storage applications, have accurate, verbose error handling, predictable failure behavior, reliable hot swapping, and the added feature of multipath support. Multipath access means that each drive has two interfaces and can connect to two storage controllers or one controller over two cables. This redundancy protects against cable, controller card, or complete system failure in the case of the TrueNAS high-availability architecture in which each controller is an independent server that accesses the same set of NL-SAS drives. NL-SAS drives are also robust enough to handle the rigors of systems with more than 16 disks. So, capacity-oriented TrueNAS systems ship with Western Digital UltraStar NL-SAS disks thanks to the all-around perfect balance of capacity, reliability, performance, and flexibility that NL-SAS drives offer.

- **SAS Disks**
  Enterprise SAS disks, built for the maximum performance and reliability that a spinning platter can provide, are the traditional heavy-lifters of the enterprise storage industry. SAS disk capacities are low compared to NL-SAS or NAS drives due to the speed at which the platters spin, reaching as high as 15,000 RPMs. While SAS drives may sound like the ultimate answer for high-performance storage, many consumer and enterprise flash-based options have come onto the market and significantly reduced the competitiveness of SAS drives. For example, enterprise SAS drives discontinued from the TrueNAS product lines were almost completely replaced by flash drives (SSDs or NVMe) in 2016 due to their superior performance/cost ratio.

- **SATA & SAS Flash Storage SSDs**
  Flash storage technology has progressed significantly in recent years, leading to a revolution in mobile devices and the rise of flash storage in general-purpose PCs and servers. Unlike hard disks, flash storage is not sensitive to vibration and can be much faster with comparable reliability. Flash storage remains more expensive per gigabyte, but is becoming more common in TrueNAS systems as the price gap narrows.

  The shortest path for introducing flash storage into the mainstream market was for vendors to use standard SATA/SAS hard disk interfaces and form factors that emulate standard hard disks but without moving parts. For this reason, flash storage Solid State Disks (SSDs) have SATA interfaces and are the size of 2.5” laptop hard disks, allowing them to be drop-in replacements for traditional hard disks. Flash storage SSDs can replace HDDs for primary storage on a TrueNAS system, resulting in a faster, though either a smaller or more expensive storage solution. If you plan to go all-flash, buy the highest-quality flash storage SSDs your budget allows with a focus on power, safety, and write endurance that matches your expected write workload.
While SSDs pretending to be HDDs made sense for rapid adoption, the Non-Volatile Memory Express (NVMe) standard is a native flash protocol that takes full advantage of flash storage’s non-linear, parallel nature.

The main advantage of NVMe is generally its low-latency performance, and it’s becoming a mainstream option for boot and other tasks. At first, NVMe was limited to expansion-card form factors such as PCIe and M.2. The new U.2 interface offers a universal solution that includes the 2.5” drive form factor and an externally accessible (but generally not hot-swappable) NVMe interface.

Note: NVMe devices can run quite hot and may need dedicated heat sinks.

Avoid using USB-connected hard disks for primary storage with TrueNAS. You can use USB Hard Disks for very basic backups in a pinch. While TrueNAS does not automate this process, you can connect a USB HDD, replicate at the command line, and then take it off-site for safekeeping.

Warning: USB-connected media (including SSDs) may report their serial numbers inaccurately, making them indistinguishable from each other.

These storage device media arrange together to create powerful storage solutions.

Storage Solutions

Hybrid Storage & Flash Cache (SLOG/ZIL/L2ARC)

With hard disks providing double-digit terabyte capacities and flash-based options providing even higher performance, a best of both worlds option is available. With TrueNAS and OpenZFS, you can merge both flash and disk to create hybrid storage that makes the most of both storage types. Hybrid setups use high-capacity spinning disks to store data while DRAM and flash perform hyper-fast read and write caching. The technologies work together with a flash-based separate write log (SLOG). Think of it as a write cache keeping the ZFS-intent log (ZIL) used to speed up writes. On the read side, flash is a level two adaptive replacement (read) cache (L2ARC) to keep the hottest data sets on the faster flash media. Workloads with synchronous writes such as NFS and databases benefit from SLOG devices, while workloads with frequently-accessed data might benefit from an L2ARC device. An L2ARC device is not always the best choice because the level one ARC in RAM always provide a faster cache, and the L2ARC table uses some RAM.

SLOG devices don’t need to be large, since they only need to service five seconds of data writes delivered by the network or a local application. A high-endurance, low-latency device between 8 GB and 32 GB in size is adequate for most modern networks, and you can strip or mirror several devices for either performance or redundancy. Pay attention to the device’s published endurance claims since a SLOG acts as the funnel point for most of the writes made to the system.

SLOG devices also need power protection. The purpose of the ZFS intent log (ZIL), and thus the SLOG, is to keep sync writes safe during a crash or power failure. If the SLOG isn’t power-protected and loses data after a power failure, it defeats the purpose of using a SLOG in the first place. Check the manufacturer’s specifications to ensure the SLOG device is power-safe or has power loss/failure protection.

The most important quality to look for in an L2ARC device is random read performance. The device needs to support more IOPS than the primary storage media it caches. For example, using a single SSD as an L2ARC is ineffective in front of a pool of 40 SSDs, as the 40 SSDs can handle far more IOPS than the single L2ARC drive. As for capacity, 5x to 20x larger than RAM size is a good guideline. High-end TrueNAS systems can have NVMe-based L2ARC in double-digit terabyte sizes.

Keep in mind that for every data block in the L2ARC, the primary ARC needs an 88-byte entry. Poorly-designed systems can cause an unexpected fill-up in the ARC and reduce performance in a p. For example, a 480 GB L2ARC filled with 4KiB blocks needs more than 10GiB of metadata storage in the primary ARC.

Self Encrypting Drives

TrueNAS supports two forms of data encryption at rest to achieve privacy and compliance objectives: Native ZFS
** encryption and Self Encrypting Drives (SEDs)**. SEDs do not experience the performance overhead introduced by software partition encryption but aren’t as readily available as non-SED drives (and thus can cost a little more).

**Boot Devices**

Booting legacy FreeNAS systems from 8 GB or larger USB flash drives was once very popular. We recommend looking at other options since USB drive quality varies widely and modern TrueNAS versions perform increased drive writes to the boot pool. For this reason, all pre-built TrueNAS Systems ship with either M.2 drives or SATA DOMs.

SATA DOMs, or disk-on-modules, offer reliability close to that of consumer 2.5” SSDs with a smaller form factor that mounts to an internal SATA port and doesn’t use a drive bay. Because SATA DOMs and motherboards with m.2 slots are not as common as the other storage devices mentioned here, users often boot TrueNAS systems from 2.5” SSDs and HDDs (often mirrored for added redundancy). The recommended size for the TrueNAS boot volume is 8 GB, but using 16 or 32 GB (or a 120 GB 2.5” SATA SSD) provides room for more boot environments.

**Hot Swapability**

TrueNAS systems come in all shapes and sizes. Many users want to have external access to all storage devices for efficient replacement if issues occur. Most hot-swap drive bays need a proprietary drive tray into which you install each drive. These bay and tray combinations often include convenient features like activity and identification lights to visualize activity and illuminate a failed drive with sesutil(8) (https://www.freebsd.org/cgi/man.cgi?query=sesutil&sektion=8 for CORE, https://manpages.debian.org/testing/sg3-utils/sg3_utils.8.en.html for SCALE). TrueNAS Mini systems ship with four or more hot-swap bays. TrueNAS R-Series systems can support dozens of drives in their head units and external expansion shelves. Pre-owned or repurposed hardware is popular among TrueNAS users.

Pay attention to the maximum performance offered by the hot-swap backplanes of a given system. Aim for at least 6 Gbps SATA III support. Note that hot-swapping PCIe NVMe devices is not currently supported.

**Storage Device Sizing**

Zpool layout (the organization of LUNs and volumes, in TrueNAS/ZFS parlance) is outside of the scope of this guide. The availability of double-digit terabyte drives raises a question TrueNAS users now have the luxury of asking: How many drives should I use to achieve my desired capacity? You can mirror two 16TB drives to achieve 16TB of available capacity, but that doesn’t mean you should. Mirroring two large drives offers the advantage of redundancy and balancing reads between the two devices, which could lower power draw, but little else. The write performance of two large drives, at most, is that of a single drive. By contrast, an array of eight 4TB drives offers a wide range of configurations to optimize performance and redundancy at a lower cost. If configured as striped mirrors, eight drives could yield four times greater write performance with a similar total capacity. You might also consider adding a hot-spare drive with any zpool configuration, which lets the zpool automatically rebuild itself if one of its primary drives fails.

**Storage Device Burn-In**

Spinning disk hard drives have moving parts that are highly sensitive to shock and vibration and wear out with use. Consider pre-flighting every storage device before putting it into production, paying attention to:

- Start a long HDD self-test (smartctl -t long /dev/), and after the test completes (could take 12+ hrs)
- Check the results (smartctl -a /dev/)
- Check pending sector reallocations (smartctl -a /dev/ | grep Current_Pending_Sector)
- Check reallocated sector count (smartctl -a /dev/ | grep Reallocated_Sector_Ct)
- Check the UDMA CRC errors (smartctl -a /dev/ | grep UDMA_CRC_Error_Count)
- Check HDD and SSD write latency consistency (diskinfo -wS) Unformatted drives only!
- Check HDD and SSD hours (smartctl -a /dev/ | grep Power_On_Hours)
- Check NVMe percentage used (nvmecontrol logpage -p 2 nvme0 | grep “Percentage used”)

Take time to create a pool before deploying the system. Subject it to as close to a real-world workload as possible to reveal individual drive issues and help determine if an alternative pool layout is better suited to that workload. Be cautious of used drives as vendors may not be honest or informed about their age and health. Check the number of hours on all new drives using smartctl(8) to verify they aren’t recertified. A drive vendor could also zero the hours of a drive during recertification, masking its true age. iXsystems tests all storage devices it sells for at least 48 hours before shipment.
Storage Controllers

The uncontested most popular storage controllers used with TrueNAS are the 6 and 12 Gbps (Gigabits per second, sometimes expressed as Gb/s) Broadcom (formerly Avago, formerly LSI) SAS host bus adapters (HBA). Controllers ship embedded on some motherboards but are generally PCIe cards with four or more internal or external SATA/SAS ports. The 6 Gbps LSI 9211 and its rebranded siblings that also use the LSI SAS2008 chip, such as the IBM M1015 and Dell H200, are legendary among TrueNAS users who build systems using parts from the second-hand market. Flash using the latest IT or Target Mode firmware to disable the optional RAID functionality found in the IR firmware on Broadcom controllers. For those with the budget, newer models like the Broadcom 9300/9400 series give 12 Gbps SAS capabilities and even NVMe to SAS translation abilities with the 9400 series. TrueNAS includes the `sas2flash`, `sas3flash`, and `storcli` commands to flash or perform re-flashing operations on 9200, 9300, and 9400 series cards.

Onboard SATA controllers are popular with smaller builds, but motherboard vendors are better at catering to the needs of NAS users by including more than the traditional four SATA interfaces. Be aware that many motherboards ship with a mix of 3 Gbps and 6 Gbps onboard SATA interfaces and that choosing the wrong one could impact performance. If a motherboard includes hardware RAID functionality, do not use or configure it, but note that disabling it in the BIOS might remove some SATA functionality depending on the motherboard. Most SATA compatibility-related issues are immediately apparent.

There are countless warnings against using hardware RAID cards with TrueNAS. ZFS and TrueNAS provide a built-in RAID that protects your data better than any hardware RAID card. You can use a hardware RAID card if it’s all you have, but there are limitations. First and most importantly, do not use their RAID facility if your hardware RAID card supports HBA mode, also known as passthrough or JBOD mode (there is one caveat in the bullets below). When used, it allows it to perform indistinguishably from a standard HBA. If your RAID card does not have this mode, you can configure a RAID0 for every single disk in your system. While not the ideal setup, it works in a pinch. If repurposing hardware RAID cards with TrueNAS, be aware that some hardware RAID cards:

- Could mask disk serial number and S.M.A.R.T. health information
- Could perform slower than their HBA equivalents
- Could cause data loss if using a write cache with a dead battery backup unit (BBU)

SAS Expanders

A direct-attached system, where every disk connects to an interface on the controller card, is optimal but not always possible. A SAS expander (a port multiplier or splitter) enables each SAS port on a controller card to service many disks. You find SAS expanders only on the drive backplane of servers or JBODs with more than twelve drive bays. For example, a TrueNAS JBOD that eclipses 90 drives in only four rack units of space wouldn’t be possible without SAS expanders. Imagine how many eight-port HBAs you would need to access 90 drives without SAS expanders.

While SAS expanders, designed for SAS disks, can often support SATA disks via the SATA Tunneling Protocol or STP, we still prefer SAS disks for reasons mentioned in the NL-SAS section above (SATA disks function on a SAS-based backplane). Note that the opposite is not true: you can’t use a SAS drive in a port designed for SATA drives.

Storage Device Cooling

A much-cited study floating around the Internet asserts that drive temperature has little impact on drive reliability. The study makes for a great headline or conversation starter, but carefully reading the report indicates that the drives were tested under optimal environmental conditions. The average temperature that a well-cooled spinning hard disk reaches in production is around 28 °C, and one study found that disks experience twice the number of failures for every 12 °C increase in temperature. Before adding drive cooling that often comes with added noise (especially on older systems), know that you risk throwing money away by running a server in a data center or closet without noticing that the internal cooling fans are set to their lowest setting. Pay close attention to drive temperature in any chassis that supports 16 or more drives, especially if they are exotic, high-density designs. Every chassis has certain areas that are warmer for whatever reason. Watch for fan failures and the tendency for some models of 8TB drives to run hotter than other drive capacities. In general, try to keep drive temperatures below the drive vendor’s specification.

Memory, CPU, and Network Considerations
Memory Sizing

TrueNAS has higher memory requirements than many Network Attached Storage solutions for good reason: it shares dynamic random-access memory (DRAM or simply RAM) between sharing services, add-on plugins, jails, and virtual machines, and sophisticated read caching. RAM rarely goes unused on a TrueNAS system and enough RAM is key to maintaining peak performance. You should have at least 8 GB of RAM for basic TrueNAS operations with up to eight drives. Other use cases each have distinct RAM requirements:

- Add 1 GB for each drive added after eight to benefit most use cases.
- Add extra RAM (in general) if more clients will connect to the TrueNAS system. A 20 TB pool backing lots of high-performance VMs over iSCSI might need more RAM than a 200 TB pool storing archival data. If using iSCSI to back VMs, plan to use at least 16 GB of RAM for reasonable performance and 32 GB or more for optimal performance.
- Add 2 GB of RAM for directory services for the winbind internal cache.
- Add more RAM as required for plugins and jails as each has specific application RAM requirements.
- Add more RAM for virtual machines with a guest operating system and application RAM requirements.
- Add the suggested 5 GB per TB of storage for deduplication that depends on an in-RAM deduplication table.
- Add approximately 1 GB of RAM (conservative estimate) for every 50 GB of L2ARC in your pool. Attaching an L2ARC drive to a pool uses some RAM, too. ZFS needs metadata in ARC to know what data is in L2ARC.

Error Correcting Code Memory

Electrical or magnetic interference inside a computer system can cause a spontaneous flip of a single bit of RAM to the opposite state, resulting in a memory error. Memory errors can cause security vulnerabilities, crashes, transcription errors, lost transactions, and corrupted or lost data. So RAM, the temporary data storage location, is one of the most vital areas for preventing data loss.

Error-correcting code or ECC RAM detects and corrects in-memory bit errors as they occur. If errors are severe enough to be uncorrectable, ECC memory causes the system to hang (become unresponsive) rather than continue with errored bits. For ZFS and TrueNAS, this behavior virtually eliminates any chances that RAM errors pass to the drives to cause corruption of the ZFS pools or file errors.

The lengthy, Internet-wide debate on whether to use error-correcting code (ECC) system memory with OpenZFS and TrueNAS summarizes as:

- ECC RAM is strongly recommended as another data integrity defense

However:

- Some CPUs or motherboards support ECC RAM but not all
- Many TrueNAS systems operate every day without ECC RAM
- RAM of any type or grade can fail and cause data loss
- RAM is most likely to fail in the first three months so test all RAM before deployment.

Central Processing Unit (CPU) Selection

Choosing ECC RAM limits your CPU and motherboard options, but that can be a good thing. Intel® makes a point of limiting ECC RAM support to their lowest and highest-end CPUs, cutting out the mid-range i5 and i7 models.

Which CPU to choose can come down to a short list of factors:

- An underpowered CPU can create a performance bottleneck because of how OpenZFS does checksums, and compresses and (optional) encrypts data.
- A higher-frequency CPU with fewer cores usually performs best for SMB only workloads because of Samba, the lightly-threaded TrueNAS SMB daemon.
- A higher-core-count CPU is better suited for parallel encryption and virtualization.
- A CPU with AES-NI encryption acceleration support improves the speed of the file system and network encryption.
- A server-class CPU is recommended for its power and ECC memory support.
- A Xeon E5 CPU (or similar) is recommended for software-encrypted pools.
An Intel Ivy Bridge CPU or later recommended for virtual machine use.

Watch for VT-d/AMD-Vi device virtualization support on the CPU and motherboard to pass PCIe devices to virtual machines. Be aware if a given CPU contains a GPU or requires an external one. Also, note that many server motherboards include a BMC chip with a built-in GPU. See below for more details on BMCS.

AMD CPUs are making a comeback thanks to the Ryzen and EPYC (Naples/Rome) lines. Support for these platforms is limited on FreeBSD and, by extension, TrueNAS CORE. However, Linux has significant support, and TrueNAS SCALE should work with AMD CPUs without issue.

**Remote Management: IPMI**

As a courtesy to further limit the motherboard choices, consider the Intelligent Platform Management Interface or IPMI (a.k.a. baseboard management controller, BMC, iLo, iDrac, and other names depending on the vendor) if you need:

- Remote power control and monitoring of remote systems
- Remote console shell access for configuration or data recovery
- Remote virtual media for TrueNAS installation or reinstallation

TrueNAS relies on its web-based user interface (UI), but you might occasionally need console access to make network configuration changes. TrueNAS administration and sharing default to a single network interface, which can be challenging when you need to upgrade features like LACP aggregated networking. The ideal solution is to have a dedicated subnet to access the TrueNAS web UI, but not all users have this luxury. The occasional visit to the hardware console is necessary for global configuration and even for system recovery. The latest TrueNAS Mini and R-Series systems ship with full-featured, HTML5-based IPMI support on a dedicated gigabit network interface.

**Power Supply Units**

The top criteria to consider for a power supply unit (or PSU) on a TrueNAS system are its:

- Power capacity (in watts) for the motherboard and number of drives it must support
- Reliability
- Efficiency rating
- Relative noise
- Optional redundancy to keep important systems running if one power supply fails

Select a PSU rated for the initial and a future load placed on it. Have a PSU with adequate power to migrate from a large-capacity chassis to a fully-populated chassis. Also, consider a hot-swappable redundant PSU to help guarantee uptime. Users on a budget can keep a cold spare PSU to limit their potential downtime to hours rather than days. A good, modern PSU is efficient and completely integrates into the IPMI management system to provide real-time fan, temperature, and load information.

Most power supplies carry a certified efficiency rating known as an 80 Plus rating. The 80 plus rating indicates the power drawn from the wall is lost as heat, noise, and vibration, instead of doing useful work like powering your components. If a power supply needs to draw 600 watts from the wall to provide 500 watts of power to your components, it’s operating at \( \frac{500}{600} = 83\% \) efficiency. The other 100 watts get lost as heat, noise, and vibration. Power supplies with higher ratings are more efficient but also far more expensive. Do some return-on-investment calculations if you’re unsure what efficiency to buy. For example, if an 80 Plus Platinum PSU costs $50 more than the comparable 80 Plus Gold, it should save you at least $10 per year on your power bill for that investment to pay off over five years. You can read more about 80 Plus ratings in this post.

**Uninterruptible Power Supplies**

TrueNAS provides the ability to communicate with a battery-backed, uninterruptible power supply (UPS) over a traditional serial or USB connection to coordinate a graceful shutdown in the case of power loss. TrueNAS works well with APC brand UPSs, followed by CyberPower. Consider budgeting for a UPS with pure sine wave output. Some models of SSD can experience data corruption on power loss. If several SSDs experience simultaneous power loss, it could cause total pool failure, making a UPS a critical investment.
**Ethernet Networking**

The network in Network Attached Storage is as important as storage, but the topic reduces to a few key points:

- **Simplicity** - Simplicity is often the secret to reliability with network configurations.
- **Individual interfaces** - Faster individual interfaces such as 10/25/40/100GbE are preferable to aggregating slower interfaces.
- **Interface support** - Intel and Chelsio interfaces are the best-supported options.
- **Packet fragmentation** - Only consider using jumbo frames with dedicated connections such as between servers or video editors and TrueNAS that are unlikely to experience packet fragmentation.
- **LRO/LSO offload features** - Interfaces with LRO and LSO offload features generally alleviates the need for jumbo frames and their use can result in lower CPU overhead.

**High-Speed Interconnects**

Higher band hardware is becoming more accessible as the hardware development pace increases and enterprises upgrade more quickly. Home labs can now deploy and use 40 GB and higher networking components. Home users are now discovering the same issues and problems with these higher speeds found by Enterprise customers.

iXsystems recommends using optical fiber over direct attached copper (DAC) cables for the high speed interconnects listed below:

- 10Gb NICs: SFP+ connectors
- 25Gb NICs: SFP28 connectors
- 40Gb NICs: QSFP+ connectors
- 100Gb NICs: QSFP28 connectors
- 200Gb NICs: QSFP56 connectors
- 400Gb NICs: QSFP-DD connectors

iXsystems also recommends using optical fiber for any transceiver form factors mentioned when using fiber channels. Direct attached copper (DAC) cables could create interoperability issues between the NIC, cable, and switch.

**Virtualized TrueNAS CORE**

Finally, the ultimate TrueNAS hardware question is whether to use actual hardware or choose a virtualization solution. TrueNAS developers virtualize TrueNAS every day as part of their work, and cloud services are popular among users of all sizes. TrueNAS’s design has OpenZFS at its heart. The design from day one works with physical storage devices. It is aware of their strengths and compensates for their weaknesses. When the need arises to virtualize TrueNAS:

- Pass hardware disks or the entire storage controller to the TrueNAS VM if possible (requires VT-d/AMD-Vi support).
- Disable automatic scrub pools on virtualized storage such as VMFS, and never scrub a pool while also running storage repair tasks on another layer.
- Use at least three vdevs to provide adequate metadata redundancy, even with a striped pool.
- Provide one or more 8 GB or larger boot devices.
- Provide the TrueNAS VM with adequate RAM per its usual requirements.
- Consider jumbo frame networking if all devices support it.
- Understand that the guest tools in FreeBSD might lack features found in other guest operating systems.
- Enable MAC address spoofing on virtual interfaces and enable promiscuous mode to use VNET jail and plugins.
1.2 - Install

Now that the .iso file is downloaded, you can start installing TrueNAS!

**Major Upgrades**

The install process can be repeated with newer installation files when the system already has TrueNAS installed. This is used for major version upgrades.

**ISO Verification**

The iXsystems Security Team cryptographically signs TrueNAS ISO files so that users can verify the integrity of their downloaded file. This section demonstrates how to verify an ISO file using the Pretty Good Privacy (PGP) and SHA256 methods.

**PGP ISO Verification**

You will need an OpenPGP encryption application for this method of ISO verification. There are many different free applications available, but the OpenPGP group provides a list of available software for different operating systems at [https://www.openpgp.org/software/](https://www.openpgp.org/software/). The examples in this section show verifying the TrueNAS .iso using `gnupg2` in a command prompt, but `Gpg4win` is also a good option for Windows users.

To verify the .iso source, go to [https://www.truenas.com/download-tn-core/](https://www.truenas.com/download-tn-core/), expand the Security option, and click PGP Signature to download the GNU Privacy Guard (.gpg) signature file. The PGP Public Key can be downloaded from either [pgp.mit.edu](http://pgp.mit.edu) (search for security-officer@ixsystems.com) or [keys.openpgp.org](http://keys.openpgp.org).

Open the PGP Public key link and note the address in your browser and Search results for string.

Use one of the OpenPGP encryption tools mentioned above to import the public key and verify the PGP signature.

Go to the .iso and .iso.gpg download location and import the public key using the keyserver address and search results string:

```
q5sys@athena /tmp> gpg --keyserver keys.gnupg.net --recv-keys
0xc8d62def767c1db0dff4e6ec358ea9112cf7946
```

```
gpg: requesting key 12CF7946 from hkp server keys.gnupg.net

q5sys@athena /tmp> gpg: key 12CF7946: "IX SecTeam <security-officer@ixsystems.com>" not changed

q5sys@athena /tmp>
```

Use `gpg --verify` to compare the .iso and .iso.gpg files:

```
q5sys@athena /tmp> gpg --verify TrueNAS-12.0-BETA2.1.iso.gpg TrueNAS-12.0-BETA2.iso
```

```
gpg: Good signature from "IX SecTeam <security-officer@ixsystems.com>"
```

```
gpg: WARNING: This key is not certified with a trusted signature!
```

```
Primary key fingerprint: C8D6 2DEF 767C 1DB0 DFF4 E6EC 358E AA91 12CF 7946
```

This response means the signature is correct but still untrusted. Go back to the browser page that has the PGP Public key open and manually confirm that the key was issued for IX SecTeam <security-officer@ixsystems.com> (IX Security Team) on October 15, 2019 and has been signed by an iXsystems account.

**SHA256 Verification**

The command to verify the checksum varies by operating system:

- **BSD**: `sha256 isofile`
- **Linux**: `sha256sum isofile`
- **Mac**: `shasum -a 256 isofile`
- Windows or Mac users can install additional utilities like [HashCalc](https://www.gethashcalc.com/) or [HashTab](https://www.hashingtoolkit.com/).
The value produced by running the command must match the value shown in the sha256.txt file. Different checksum values indicate a corrupted installer file that should not be used.

Choose the install type to see specific instructions:

- **Physical Hardware**

  **Hardware Considerations**

  TrueNAS is very flexible and can run on most x86 computers. However, there are many different hardware considerations when building a NAS! If you’re still researching what kind of hardware to use with TrueNAS, read over the very detailed [CORE Hardware Guide](https://www.corehq.org/docs/).  

**Prepare the Install File**

Physical hardware typically requires burning the TrueNAS installer to a physical device. In general a CD or removable USB device is used. This device is temporarily attached to the system to install TrueNAS to the system’s permanent boot device.

Headless, or remote, installation is possible when the system has IPMI available and can create a virtual media CD-ROM using a locally stored .iso.

The method of writing the installer to a device varies between operating systems. Click [Windows](#) or [Linux](#) to see instructions for your Operating System, or [CD](#) for generic CD burning guidance.

**CD**

To use the installer with a CD, download your favorite CD burning utility and burn the .iso file to the CD. Insert the CD into the TrueNAS system and boot from the CD.

**Windows**

To write the TrueNAS installer to a USB stick on Windows, plug the USB stick into the system and use a program like [Rufus](#) to write the .iso file to the memory stick. When Rufus prompts for which write method to use, make sure `dd mode` is selected.

The USB stick is not recognized by Windows after the TrueNAS installer writes to it. To reclaim the USB stick after installing TrueNAS, use Rufus to write a “Non bootable” image, then remove and reinsert the USB stick.

**Linux**

To write the TrueNAS installer to a USB stick on Linux, plug the USB stick into the system and open a terminal.

Start by making sure the USB stick connection path is correct. There are many ways to do this in Linux, but a quick option is to enter `lsblk -po +vendor,model` and note the path to the USB stick. This shows in the `NAME` column of the `lsblk` output.

Next, use `dd` to write the installer to the USB stick.

Be very careful when using `dd`, as choosing the wrong `of=` device path can result in irretrievable data loss!

Enter `dd status=progress if=path/to/.iso of=path/to/USB` in the CLI. If this results in a “permission denied” error, use `sudo dd` with the same parameters and enter the administrator password.

**Headless Install**

Systems with IPMI connectivity, like the TrueNAS Mini, can use the Virtual Media feature with an .iso to create a
virtual boot device for installation. Mounting the .iso in a virtual CD-ROM, allows installing or updating headless servers remotely through the console.

Here is an example of setting up a virtual CD-ROM with a SUPERMICRO IPMI:

1. From the Virtual Media menu, select CD-ROM Image.
2. Fill in the details:
   1. Shared Host: The IP address of the system storing the .iso.
   2. Path to Image: The path to the image file. Example: install/iso/SCALEAngelfish.iso
3. Click Mount.
4. Click Refresh Status and confirm a disk is being emulated.
5. Click Save.

Install Process

With the installer added to a device, you can now install TrueNAS onto the desired system. Insert the install media, or load the iso using IPMI, and reboot or boot the system. At the motherboard splash screen, use the hotkey defined by your motherboard manufacturer to boot into the motherboard UEFI/BIOS.

Choose to boot in UEFI mode or legacy CSM/BIOS mode. When installing TrueNAS, make the matching choice for the installation. For Intel chipsets manufactured in 2020 or later, UEFI is likely the only option.

If your system supports SecureBoot, you will need to either disable it or set it to “Other OS” to be able to boot the install media.

Select the install device as the boot drive, exit, and reboot the system. If the USB stick is not shown as a boot option, try a different USB slot. Which slots are available for boot differs by hardware.

After the system has booted into the installer, follow these steps.

Select Install/Upgrade.

Select the desired install drive.
Select **Yes**

**WARNING:**
- This will erase ALL partitions and data on ada4.
- You can’t use ada4 for sharing data.

**NOTE:**
- Installing on flash media is preferred to installing on a hard drive.

**Proceed with the installation?**

Select **Fresh Install** to do a clean install of the downloaded version of TrueNAS. **This will erase the contents of the selected drive.**!
When the operating system device has enough additional space, you can choose to allocate some space for a swap partition to improve performance.

Enter a password for the root user to log in to the web interface.
After following the steps to install, reboot the system and remove the install media.

## Troubleshooting

If the system does not boot into TrueNAS, there are several things that can be checked to resolve the situation:

- Check the system BIOS and see if there is an option to change the USB emulation from CD/DVD/floppy to hard drive. If it still will not boot, check to see if the card/drive is UDMA compliant.
- If the system BIOS does not support EFI with BIOS emulation, see if it has an option to boot using legacy BIOS mode.
- If the system starts to boot but hangs with this repeated error message: `run_interrupt_driven_hooks: still waiting after 60 seconds for xpt_config`, go into the system BIOS and look for an onboard device configuration for a 1394 Controller. If present, disable that device and try booting again.
- If the burned image fails to boot and the image was burned using a Windows system, wipe the USB stick before trying a second burn using a utility such as Active@KillDisk. Otherwise, the second burn attempt will fail as Windows does not understand the partition which was written from the image file. Be very careful to specify the correct USB stick when using a wipe utility!

## Virtual Machine

Because TrueNAS is built and provided as a `.iso` file, it works on all virtual machine solutions (VMware, VirtualBox, Citrix Hypervisor, etc). This section demonstrates installing with VMware Workstation Player on Windows.

### Minimum Virtual Machine Settings

Regardless of virtualization application, use these minimum settings:

- RAM: at least 8192MB (8GB)
- DISKS: one virtual disk with at least 8GB for the operating system and boot environments and at least one additional virtual disk with at least 4GB to be used as data storage.
- NETWORK: Use NAT, Bridged, or Host-only depending on your host network configuration.

### FreeBSD UEFI Bug with ESXi

**VMware products and EFI boot mode:** A third party bug currently affects EFI (UEFI) booting on VMWare products. TrueNAS should be installed in BIOS mode until this is resolved. See VMware article [Host Fails to Boot](#).
After You Install ESXi in UEFI Mode

Networking checks for VMware

When installing TrueNAS in a VMware VM, double check the virtual switch and VMware port group. Network connection errors for plugins or jails inside the TrueNAS VM can be caused by a misconfigured virtual switch or VMware port group. Make sure MAC spoofing and promiscuous mode are enabled on the switch first, and then the port group the VM is using.

Jail Networking

If you have installed TrueNAS in VMware, you will need functional networking to create a jail.

For the jail to have functional networking, you have to change the VMware settings to allow Promiscuous, MAC address changes, and Forged Transmits.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promiscuous Mode</td>
<td>When enabled at the virtual switch level, objects defined within all portgroups can receive all incoming traffic on the vSwitch.</td>
</tr>
<tr>
<td>MAC Address Changes</td>
<td>When set to Accept, ESXi accepts requests to change the effective MAC address to a different address than the initial MAC address.</td>
</tr>
<tr>
<td>Forged Transmits</td>
<td>When set to Accept, ESXi does not compare source and effective MAC addresses.</td>
</tr>
</tbody>
</table>

Generic VM Creation Process

For most hypervisors, the procedure for creating a TrueNAS VM is the same:

1. Create a new Virtual Machine as usual, taking note of the following settings.
2. The virtual hardware has a bootable CD/DVD device pointed to the TrueNAS installer image (this is usually an .iso).
3. The virtual network card is configured so it can be reached from your network. bridged mode is optimal as this treats the network card as if it is plugged into a simple switch on the existing network.
4. Some products require identifying the OS being installed on the VM. The ideal option is FreeBSD 12 64 bit. If this is not available, try options like FreeBSD 12, FreeBSD 64 bit, 64 bit OS, or Other. Do not choose a Windows or Linux related OS type.
5. For VMWare hypervisors, install in BIOS mode.
6. The VM has sufficient memory and disk space. TrueNAS needs at least 8 GB RAM and 20 GB disk space. Not all hypervisors allocate enough memory by default.
7. Boot the VM and install TrueNAS as usual.
8. When installation is complete, shut down the VM instead of rebooting, and disconnect the CD/DVD from the VM before rebooting the VM.
9. After rebooting into TrueNAS, install VM tools if applicable for your VM, and if they exist for FreeBSD 12, or ensure they are loaded on boot.

Example installation for VMWare Player 15.5

Open VMware Player and click Create a New Virtual Machine to enter the New Virtual Machine Wizard.

1. Installer disk image file

Select the Installer disk image file (iso) option, click Browse…, and upload the TrueNAS Core .iso downloaded earlier.

2. Name the Virtual Machine
In this step, the virtual machine name and location can be changed.

3. Specify Disk Capacity

Specify the maximum disk size for the initial disk. The default 20GB is enough for TrueNAS. Next, select *Store virtual disk as a single file.*

4. Review Virtual Machine

Review the virtual machine configuration before proceeding. By default, VMware Player doesn’t set enough RAM for the virtual machine. Click *Customize Hardware... > Memory.* Drag the slider up to 8GB and click *Ok.* If you wish to power on the machine after creation, select *Power on this virtual machine after creation.*

Add Virtual Disks for Storage

After the virtual machine has been created, select it from the virtual machine list and click *Edit virtual machine settings.* Click *Add...* and select *Hard Disk.* Select *SCSI* as the virtual disk type. Select *Create a new virtual disk.* Specify the maximum size of this additional virtual disk. This disk stores data in TrueNAS. If desired, allocate the disk space immediately by setting *Allocate all disk space now.* Select *Store virtual disk as single file.* Finally, name and chose a location for the new virtual disk.

Repeat this process until enough disks are available for TrueNAS to create ideal storage pools. This depends on your specific TrueNAS use case. See Pool Creation for descriptions of the various pool (“vdev”) types and layouts.

TrueNAS Installer

Select the virtual machine from the list and click *Play virtual machine.* The machine starts and boots into the TrueNAS installer. Select *Install/Upgrade.*

Select the desired disk for the boot environments.
Select Yes. This will erase all contents on the disk!

Set a password for root login.
Select **Boot via BIOS**.

After the TrueNAS installation is complete, reboot the system. The **Console Setup Menu** displays when the system boots successfully.

**VMWare post-install expand □**

After installing TrueNAS in a VMware VM, it is recommended to configure and use the **vmx(4)** drivers on TrueNAS. To load the VMX driver when TrueNAS boots, log in to the web interface and go to **System > Tunables**. Click **Add** and create a new tunable with the **Variable** `if_vmx_load`, **Value** "YES", and **Type** `loader`, and save the tunable:
Congratulations, TrueNAS is now installed!

The next step is to [log in to the web interface](#) and begin configuring the system.
1.3 - Console Setup Menu

The Console Setup menu displays at the end of the boot process. If the TrueNAS system has a keyboard and monitor, this menu can be used to administer the system.

When connecting with SSH or the web shell, the Console Setup menu is not shown by default. It can be started by the root user or another user with root permissions by entering /etc/netcli.

To disable the Console Setup menu, go to System > Advanced and unset Show Text Console without Password Prompt.

On HA systems, some of these menu options are not available unless HA has been administratively disabled.

The menu provides these options:

1. **Configure Network Interfaces** provides a configuration wizard to set up the system’s network interfaces. If the system has been licensed for High Availability (HA), the wizard prompts for IP addresses for both “This Controller” and “TrueNAS Controller 2”.

2. **Configure Link Aggregation** is for creating or deleting link aggregations.

3. **Configure VLAN Interface** is used to create or delete VLAN interfaces.

4. **Configure Default Route** is used to set the IPv4 or IPv6 default gateway. When prompted, enter the IP address of the default gateway.

5. **Configure Static Routes** prompts for the destination network and gateway IP address. Re-enter this option for each static route needed.

6. **Configure DNS** prompts for the name of the DNS domain and the IP address of the first DNS server. When adding multiple DNS servers, press Enter to enter the next one. Press Enter twice to leave this option.

7. **Reset Root Password** is used to reset a lost or forgotten root password. Select this option and follow the prompts to set the password.

8. **Reset Configuration to Defaults** *Caution!* This option deletes all of the configuration settings made in the administrative GUI and is used to reset TrueNAS® back to defaults. Before selecting this option, make a full backup of all data and make sure all encryption keys and passphrases are known! After this option is selected, the configuration is reset to defaults and the system reboots. Storage Pools Import Pool can be used to re-import pools.

9. **Shell** starts a shell for running FreeBSD commands. To leave the shell, type exit.
10. **Reboot** reboots the system.

11. **Shut Down** shuts down the system.

The numbering and quantity of options on this menu can change due to software updates, service agreements, or other factors. Please carefully check the menu before selecting an option, and keep this in mind when writing local procedures.

During boot, TrueNAS automatically attempts to connect to a DHCP server from all live interfaces. If it successfully receives an IP address, the address is displayed so it can be used to access the graphical user interface. In the example shown above, TrueNAS is accessible at 10.0.0.102.

Some TrueNAS systems are set up without a monitor, making it challenging to determine which IP address has been assigned. On networks that support Multicast DNS (mDNS), the hostname and domain can be entered into the address bar of a browser. By default, this value is `truenas.local`.

If TrueNAS is not connected to a network with a DHCP server, use the console network configuration menu to manually configure the interface as shown here. In this example, the TrueNAS system has one network interface, `em0`.

```
Enter an option from 1-12: 1
1) em0
Select an interface (q to quit): 1
Remove the current settings of this interface? (This causes a momentary disconnection of the network.) (y/n) n
Configure interface for DHCP? (y/n) n
Configure IPv4? (y/n) y
Interface name: (press enter, the name can be blank)
Several input formats are supported
Example 1 CIDR Notation:
192.168.1.1/24
Example 2 IP and Netmask separate:
IP: 192.168.1.1
Netmask: 255.255.255.0, or /24 or 24
IPv4 Address: 192.168.1.108/24
Saving interface configuration: Ok
Configure IPv6? (y/n) n
Restarting network: ok
...
The web user interface is at
http://192.168.1.108
```
1.4 - Logging In

Now that TrueNAS is installed, it’s time to log in to the web interface and begin managing data!

Can I configure TrueNAS using a CLI? expand  
After installing TrueNAS, configuring and using the system is all managed through the web interface. It is important to only use the web interface to make configuration changes to the system. By default, using the command-line interface (CLI) to modify the system does not modify the settings database. Any changes made in the command line are lost and reverted to the original database settings whenever the system restarts. TrueNAS automatically creates a number of ways to access the web interface, but you might need to adjust the default settings to better fit the system in your network environment.

Web Interface Access

By default, TrueNAS provides a default address for logging in to the web interface. To view the web interface IP address or reconfigure web interface access, you will need to connect a monitor and keyboard to your TrueNAS system or connect with IPMI for out-of-band system management.

○ CORE Defaults

When powering on a TrueNAS system, the system attempts to connect to a DHCP server from all live interfaces and provide access to the web interface. On networks that support Multicast Domain Name Services (mDNS), a hostname and domain can be used to access the TrueNAS web interface. By default, TrueNAS is configured to use the hostname and domain truenas.local You can change this after logging in to the web interface by going to Network > Global Configuration and setting a new Hostname and Domain.

If an IP address is needed, connect a monitor to the TrueNAS system and view the console setup menu that displays at the end of the boot process.

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

The web user interface is at:
http://10.238.15.194
https://10.238.15.194

Enter an option from 1-11: 10
```

When able to automatically configure a connection, the system shows the web interface IP address at the bottom of the console setup menu. If needed, you can reset the root password in the TrueNAS console setup menu or by clicking Settings > Change Password in the web interface. To require logging in to the system before showing the system console menu, go to System > Advanced and unset Show Text Console without Password Prompt.

○ Enterprise Defaults

TrueNAS Enterprise hardware from iXsystems is preconfigured with your provided networking details. The IP address of the TrueNAS web interface is provided on the system sales order or configuration sheet. Please contact iX Support if the TrueNAS web interface IP address has not been provided with these documents or cannot be identified from the TrueNAS system console.
Customers who purchase iXsystems hardware or that want additional support must have a support contract to use iXsystems Support Services. The TrueNAS Community forums provides free support for users without an iXsystems Support contract.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td><a href="https://support.ixsystems.com">https://support.ixsystems.com</a></td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:support@ixsystems.com">support@ixsystems.com</a></td>
</tr>
<tr>
<td>Telephone</td>
<td>Monday - Friday, 6:00AM to 6:00PM Pacific Standard Time:</td>
</tr>
<tr>
<td></td>
<td>US-only toll-free: 1-855-473-7449 option 2</td>
</tr>
<tr>
<td></td>
<td>Local and international: 1-408-943-4100 option 2</td>
</tr>
<tr>
<td>Telephone</td>
<td>After Hours (24x7 Gold Level Support only):</td>
</tr>
<tr>
<td></td>
<td>US-only toll-free: 1-855-499-5131</td>
</tr>
<tr>
<td></td>
<td>International: 1-408-878-3140 (international calling rates apply)</td>
</tr>
</tbody>
</table>

## Configuring Web Interface Access

If the TrueNAS system is not connected to a network with a DHCP server, you can use the console network configuration menu to manually **Configure Network Interfaces**.

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

The web user interface is at:

http://10.238.15.194
https://10.238.15.194

Enter an option from 1-11: 1

This example shows configuring a single interface, **em0**:

```
Enter an option from 1-12: 1
1) em0
Select an interface (q to quit): 1
Remove the current settings of this interface? (This causes a momentary disconnection of the network.) (y/n) n
Configure interface for DHCP? (y/n) n
Configure IPv4? (y/n) y
Interface name: (press enter, the name can be blank)
Several input formats are supported
Example 1 CIDR Notation:
192.168.1.1/24
Example 2 IP and Netmask separate:
   IP: 192.168.1.1
   Netmask: 255.255.255.0, or /24 or 24
IPV4 Address: 192.168.1.108/24
Saving interface configuration: Ok
Configure IPv6? (y/n) n
Restarting network: ok
```

The web user interface is at
Depending on the network environment, review the Configure Default Route option to define your IPv4 or IPv6 default gateway. Configure Static Routes allows adding destination network and gateway IP addresses, one for each route. To change the DNS domain and add nameservers, select Configure DNS.

These settings can be adjusted later in the various Network options available in the web interface.

Logging In

On a computer that can access the same network as the TrueNAS system, enter the hostname and domain or IP address in a web browser to connect to the web interface.

Only the root username is used to log in to the web interface. Enter the root account password that was created during installation.

Troubleshooting expand □

If the user interface is not accessible by IP address from a browser, check these things:

- Are proxy settings enabled in the browser configuration? If so, disable the settings and try connecting again.
- If the page does not load, make sure that a ping reaches the TrueNAS system IP address. If the address is in a private IP address range, it is only accessible from within that private network.

If the web interface is shown but seems unresponsive or incomplete:

- Make sure the browser allows cookies, Javascript, and custom fonts from the TrueNAS system.
- Try a different browser. Firefox is recommended.

If the UI becomes unresponsive after an upgrade or other system operation, clear the site data and refresh the browser (Shift+F5).

Dashboard

After logging in, the system Dashboard is shown. Basic information about the installed version, systems component usage and network traffic are all presented on this screen. For users with compatible TrueNAS Hardware,
clicking the system image will take you to the **System > View Enclosure** page.

The **Dashboard** provides access to all TrueNAS management options. Across the top row are links to outside resources and buttons to control the system. There is also a column of options at the left hand side of the screen for accessing the various TrueNAS Configuration screens.

Logos in the top row are links to iXsystems sites. The button next to the iXsystems logo shows TrueCommand connection options. The next two buttons show information about what is happening on the system, like active or previous tasks and any alerts generated by a system condition. The remaining buttons link to system configuration option or can be used to logout, restart, or shutdown the physical system.

The top row has buttons to hide the left side column. The top of this column shows the system hostname and the active user. TrueNAS configuration screens are linked in the left hand column.

Now that you can access the TrueNAS web interface and see all the management options, it’s time to begin storing data!
1.5 - Storage Configuration

- Requirements
- Simple Storage Setup
  - Adding Datasets or Zvols

Now that we’re logged in to the web interface, it’s time to set up TrueNAS storage. These instructions demonstrate a simple mirrored pool setup, where one disk is used for storage and the other for data protection. However, there are a vast number of configuration possibilities for your storage environment! You can read more about these options in the in-depth Pool Creation article.

Requirements

At minimum, the system needs at least two identically sized disks to create a mirrored storage pool. While a single-disk pool is technically allowed, it is not recommended. The disk used for the TrueNAS installation does not count toward this limit.

Data backups can be configured in several ways and have different requirements. Backing data up in the Cloud requires a 3rd party Cloud Storage provider account. Backups with Replication requires either additional storage on the TrueNAS system or (ideally) another TrueNAS system in a different location.

Simple Storage Setup

Go to Storage > Pools and click ADD. Set Create a new pool and click CREATE POOL.

For the Name, enter tank or any other preferred name. In the Available Disks, set two identical disks and click the to move them to the Data VDevs area.

TrueNAS automatically suggests Mirror as the ideal layout for maximized data storage and protection.
Review the **Estimated total raw data capacity** and click **CREATE**. TrueNAS wipes the disks and adds **tank** to the **Storage > Pools** list.

### Adding Datasets or Zvols

New pools have a “root” dataset that allows further division into new **datasets** or **zvols**. A **dataset** is a file system that stores data and has specific permissions. A **zvol** is a virtual block device that has a predefined storage size. To create either one, go to **Storage > Pools**, click , and select **Add Dataset** or **Add Zvol**.

These are often created as part of configuring specific data sharing situations:

- Setting a dataset **Share Type** to **SMB** optimizes that dataset for the Windows sharing protocol.
- Block device sharing (iSCSI) requires a zvol.

Organize the pool with additional datasets or zvols according to your access and data sharing requirements before moving any data into the pool.

When you’re finished building and organizing your TrueNAS pools, move on to configuring how the system shares data.
With TrueNAS Storage configured and backed up, it’s time to begin sharing data. There are several available sharing solutions, but we’ll look at the most common in this article. Choose a tab to get started with simple sharing examples:

**Sharing Data**

- **Windows (SMB)**

**Requirements**

- Dataset with **Share Type** set to **SMB**.
- TrueNAS user accounts with **Samba Authentication** set.

**Set Permissions**

Go to **Storage > Pools** and find the dataset to share. Click and **Edit Permissions**.
Click **SELECT AN ACL PRESET**, open the drop down, and choose **OPEN**. Click **SAVE**.

**Create the Share**

Go to **Sharing > Windows Shares (SMB)** and click **ADD**.
Only the Path and Name are initially required. The Path is the directory tree on TrueNAS that is shared using the SMB protocol. The Name forms part of the “full share pathname” when SMB clients connect.

Click SUBMIT to save the configuration to Sharing > Windows Shares (SMB).

Activate the Service

Go to Services and toggle SMB. Set Start Automatically when you want the share to become accessible immediately after TrueNAS boots.

Connecting to the Share

On a Windows 10 system, open the File Browser.
In the navigation bar, enter `\` and the TrueNAS system name. When prompted, enter the TrueNAS user account credentials and begin browsing the dataset.

- **Unix-like (NFS)**

**Requirements**

- TrueNAS dataset to share.
- Client systems might require additional packages like `nfs-common`.

**Creating the Share**

Go to **Sharing > Unix Shares (NFS)** and click **ADD**.
Use the file browser to select the dataset to be shared and click **SUBMIT**. When prompted, click **ENABLE SERVICE** to immediately begin sharing the dataset.

**Accessing the Dataset**

On a Unix-like system, open a command line. Enter `showmount -e IPADDRESS`, replacing **IPADDRESS** with your TrueNAS system address:

```
tmoore@ChimaeraPrime:~$ showmount -e 10.238.15.194
Export list for 10.238.15.194:
/mnt/pool1/testds (everyone)
```

Now make a local directory for the NFS mount:

```
tmoore@ChimaeraPrime:~$ sudo mkdir nfstemp/
```

Finally, mount the shared directory:

```
tmoore@ChimaeraPrime:~$ sudo mount -t nfs 10.238.15.194:/mnt/pool1/testds nfstemp/
```

From here, `cd` into the local directory and view or modify the files as needed.

**Block Shares (iSCSI)**

Block sharing is a complicated scenario that requires detailed configuration steps and knowledge of your network environment. A simple configuration is beyond the scope of this getting started guide, but detailed articles are available in the [iSCSI Sharing topic](http://example.com).
1.7 - Data Backups

With storage created and shared, it’s time to ensure TrueNAS data is effectively backed up. TrueNAS offers several options for backing up data.

😊 Cloud Sync

This option requires an account with the Cloud Storage provider and a storage location created with the provider, like an Amazon S3 bucket. Major providers like Amazon S3, Google Cloud, Box and Microsoft Azure are supported, along with a variety of other vendors. These can charge fees for data transfers and storage, so please review your cloud storage provider’s policies before transferring any data.

You can configure TrueNAS to send, receive, or synchronize data with a Cloud Storage provider. Configuring a Cloud Sync task allows you to transfer data a single time or set up a recurring schedule to periodically transfer data.

Add the Credential

Go to **System > Cloud Credentials > ADD**. Enter a **Name** and choose the **Provider** from the dropdown menu. The authentication options change depending on the selected **Provider**. Credentials either must be entered manually or a single provider login is required and the credentials add automatically.

After entering the **Provider** credentials, click **VERIFY CREDENTIAL**. When verification is confirmed, click **SUBMIT**.

Add the Data Transfer Task

Go to **Tasks > Cloud Sync Tasks** and click **ADD**.
Select the previously saved Credential to populate the Remote section.

Add a Description for the task, select PUSH or PULL as the Direction and COPY as the Transfer Mode. Under Directory/Files, choose the tank dataset previously created.

Now, use the Control options to define how often this task runs. Open the Schedule drop down and choose a preset time when running the task is least intrusive to your network. When the task only needs to run once, unset Enabled. The task can then be triggered a single time from the Tasks > Cloud Sync Tasks list to do the initial migration or backup.

To test your task, click DRY RUN. When the test run is successful, click SUBMIT to save the task and add it to Tasks > Cloud Sync Tasks.

To manually run the task, go to Tasks > Cloud Sync Tasks, click > to expand the new task, and click RUN NOW.
The **Status** shows success or failure. Click the status entry to see a detailed log of the action.

**Replication**

Replication is the process of taking a moment in time “snapshot” of the data and copying that snapshot to another location. Snapshots typically use less storage than full file backups and have more management options. This instruction shows using the TrueNAS Wizard to create a simple replication.

Go to **Tasks > Replication Tasks** and click **ADD**. Set the source location to the local system and pick which datasets to snapshot. The wizard takes new snapshots of the sources when no existing source snapshots are found.

Set the destination to the local system and define the path to the storage location for replicated snapshots. When manually defining the destination, be sure to type the full path to the destination location.

You can define a specific schedule for this replication or choose to run it immediately after saving the new task. Unscheduled tasks are still saved in the replication task list and can be run manually or edited later to add a schedule.
Clicking **START REPLICATION** saves the new task and immediately attempts to replicate snapshots to the destination.

To confirm that snapshots have been replicated, go to **Storage > Snapshots** and verify the destination dataset has new snapshots with correct timestamps.

TrueNAS is now accessible and configured to store, share, and back up your data!

If you need to expand the system capabilities, see the remaining article about additional **Applications**. When you’re ready to fine-tune the system configuration or learn more about the advanced features, see the remaining sections in the TrueNAS CORE and Enterprise section. These sections are organized in order of appearance in the TrueNAS interface, with additional topics for **3rd party solutions**, **API reference guide**, official **notices** from iXsystems, Inc, and **community recommendations**.
1.8 - Applications

With the rest of the system configured and data being shared over a network, the final step to consider for first time setup is installing any application solutions. Applications or features added to TrueNAS are created in separate “Plugins”, Jails”, or “Virtual Machines” that are kept separate from the base TrueNAS operating system. If anything goes wrong or a security vulnerability is exploited in one of these application environments, TrueNAS remains unaffected. These solutions safely expand TrueNAS’ capabilities in a restricted, safeguarded way.

The primary method to install applications is to use Plugins. These are pre-packaged applications that quickly install in a tailor-made environment. Some plugins are supported by iXsystems while others are provided and maintained by the open source community.

A Jail is a restricted FreeBSD operating system installed as a separate subset of TrueNAS. Jails can install a wide variety of applications and be tuned to very specific use cases, but require more extensive knowledge of FreeBSD and command line operation.

A Virtual Machine is a fully independent operating system installation. This reserves or splits the available hardware resources to create a different, full operating system experience. TrueNAS can install Windows or Unix-like operating systems in a Virtual Machine (VM), but regular system performance is reduced while virtual machines are running.

Click one of the tabs below to see instructions on installing your preferred application solution.

<table>
<thead>
<tr>
<th>Network Hardware Offloading expand □</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugins</td>
</tr>
<tr>
<td>Plugins that use a network interface need to Disable Hardware Offloading in Network -&gt; Interface. Disabling hardware offloading can reduce general network performance for that interface, so it is recommended to use a secondary interface for application environments.</td>
</tr>
</tbody>
</table>

Plugins

This instruction demonstrates plugins by walking you through installing the community-favorite Plex application. You will need an account with Plex to follow these instructions.

Installing Plex

Create a dataset called audio and a dataset called video to be used as mount points for Plex. Next, go to the Plugins page.

Installing a basic PlexMedia Plugin:

1. Select the Plex Media Server plugin and click INSTALL.
2. Under **Jail Name**, enter whatever name you’d like (i.e. “Plex”).
3. **DHCP** is set automatically.
4. Click **SAVE**.

5. A dialog window shows the installation progress.
When available, *Plugin Installation Notes* display when the install completes.

6. The plugin *Status* shows as **up**, with the *Boot* option set.
7. Click > to expand the Plex table entry:

![Expanded Plex Table Entry]

8. Stop the **up** plugin.
9. Click **MOUNT POINTS**.

![MOUNT POINTS Section]

10. Click **Actions** and **Add**.
11. Fill out one mount point for each previously created dataset. The *Source* is the created dataset and the *Destination* is the media directory with `/datasetname` appended (see example):
12. Click **Submit**. Do this for as many mount points as needed. In this example, we have **audio** and **video**.

13. Go to **Storage > Pools** and click **more_vert > Edit Permissions** for your source datasets.
14. Click *Create a custom ACL* and *Continue*.

15. Click *ADD ACL ITEM* and enter the values pictured below:
Set *Apply permissions recursively* and click *Save.*

16. Go to **Plugins**, find the **Plex** entry, and click the **Start** the plugin.

### Accessing Plex

1. When the **Plex** plugin status is **up**, click the **Manage**.

2. Enter your Plex login information.
Plex Web

would like to sign in to your Plex account

⚠️ This application is at 10.215.6.70 and is not hosted by Plex. Continue only if you recognize this server and wish to grant access.

Continue with Google
Continue with Facebook
Continue with Apple
Continue with Email

By creating an account or continuing to use a Plex application, website, or software, you acknowledge and agree that you have accepted the Terms of Service and have reviewed the Privacy Policy.
FreeBSD Jails

Installing a Jail

1. Go to the Jails page and click ADD.

2. Enter a jail Name, select the Release version, and click NEXT.
3. To allow the jail access to the internet, set DHCP Autoconfigure IPv4 and click NEXT. Additional defaults are set when the DHCP option is set.
4. Review the **Jail Summary** and click **SUBMIT**.

![Jail Summary and Options](image)

**Accessing a Jail**

1. Go to **Jails** and click the > next to the newly created jail. Click **START**.

![Jails with newjail](image)

2. When the jail **State** changes to **up**, click > **SHELL** to see the jail command line.
Virtual Machines

Installing a Virtual Machine

Virtual Machines require uploading an Operating System .iso to TrueNAS. This example shows using an Ubuntu .iso:

1. Go to Virtual Machines and click ADD.

2. Select a Guest Operating System and enter a Name. For this example the Guest Operating System is set to Linux. Click NEXT.
3. Now enter the physical resources to give the VM. Larger numbers of Virtual CPUs, Cores, Threads, and Memory allow the VM to perform better, but reduces the performance of the TrueNAS system. Click NEXT.

4. Set Create a new disk image and select a Zvol Location for the VM storage. Enter a usable storage Size (example shows 50 GiB) and click the NEXT button.
5. **Network Interface** automatically detects the hardware and sets defaults that allow network access. Make sure these settings are valid, then click **NEXT**.

6. Set **Upload an installer image file** to see additional options. Select an **ISO save location** on the TrueNAS system. Now click **Choose File** and browse to the OS installation .iso. Click **UPLOAD** and wait for the process to finish (this can take some time). Click **NEXT**.
7. Confirm the VM configuration is correct and click **SUBMIT**.

### Accessing a Virtual Machine

1. Go to **Virtual Machines** and click  > next to the newly created VM. Click **START**.
2. When the VM **State** changes to **up**, click **VNC** to see the VM display.

Because this example used an Ubuntu .iso, the Ubuntu installation screen is shown.
From here, install the OS as normal.

3. When the OS install completes, go back to **Virtual Machines**, toggle the **State**, and click **DEVICES**.

Find the **CDROM** entry and click **Delete** to remove it. This removes the installation .iso from the VM and allows it to boot into the full OS the next time the VM activates.
2 - Accounts

2.1 - Groups

- View Existing Groups
- Add a New Group
- Group Member Management

Using groups in TrueNAS can be an efficient way of managing permissions for many similar user accounts. See Users for managing users. The interface provides management of UNIX-style groups. If the network uses a directory service, import the existing account information using the instructions in Active Directory.

**View Existing Groups**

To see saved groups, go to Accounts > Groups

![Groups Interface](image)

By default, groups built in to the system are hidden. To see built-in groups, click settings and SHOW.

**Add a New Group**

To create a new group, go to Accounts > Groups and click ADD.

![Group Configuration](image)

Each group is assigned a Group ID (GID). Enter a number above 1000 for a group with user accounts. The GID cannot be changed later. Groups used by a system service must have an ID that matches the default port number used by the service.

Next, enter a descriptive group Name. Group names cannot begin with a hyphen (-) or contain a space, tab, or these characters: , : + & # ^ ( ) ! @ ~ ? < > =.

By default, the Permit Sudo option is unset. Setting allows group members to act as the root account by using sudo. A common security practice is to leave this disabled.

The option Samba Authentication is set by default. This allows group members to be used for SMB permissions and authentication.
Finally, *Allow Duplicate GIDs* allows setting a duplicate group ID, but can greatly complicate system configurations. Leaving this option unset is recommended.

**Group Member Management**

Register user accounts to a group to simplify permissions and access to large numbers of user accounts. To manage group membership, go to **Accounts > Groups**, click the **navigate_next** for a group, and click **group MEMBERS**:

To add user accounts to the group, select them in **All users** and click ****. Select multiple users by holding **CTRL** while clicking each entry.
2.2 - Users

In TrueNAS, user accounts allow flexibility for accessing shared data. A common practice is to create users and assign them to groups. This allows for efficient permissions tuning for large numbers of users.

Only the root user account can log in to the TrueNAS web interface.

When the network uses a directory service, import the existing account information using the instructions in Directory Services. Using Active Directory requires setting Windows user passwords inside Windows.

To see user accounts, go to Accounts > Users.

TrueNAS hides all built-in users by default. To see all built-in users, click settings and SHOW.

Creating User Accounts

To create a new user, go to Accounts > Users and click ADD.
Account options are subdivided into groups of similar options.

**Identification**

Enter the **Full Name** of the user. A simplified **Username** is suggested from the **Full Name**, but can be overridden with your own choice.

An **Email** address can be associated with an user account.

Set and confirm a password for the user.
User ID and Groups

Next, a user ID must be set. TrueNAS automatically suggests the user ID, starting at $1000$. This suggestion can be changed if desired. It is recommended to use an ID of $1000$ or more for non built-in users.

By default, TrueNAS creates a new primary group with the same name as the user. To instead add the user to an existing primary group, unset New Primary Group and select an existing group from the Primary Group drop-down. The user can be added to additional groups using the Auxiliary Groups drop-down.

Directories and Permissions

When creating a user, the home directory path is set to /nonexistent. This does not create a home directory for the user. To set a home directory for the user, select a path using the file browser. If the directory exists and matches the user name, it is set as the user home directory. When the path does not end with a subdirectory matching the user name, a new subdirectory is created. The full path to the users home directory is shown here when editing a user.

Directly under the file browser, the home directory permissions can be set. TrueNAS default user accounts cannot have their permissions changed.

Authentication

A public SSH key can be assigned to a user for key based authentication. Just paste the public key into the SSH Public Key field. If you are using an SSH public key, it is always a good idea to keep a backup of the key. Click DOWNLOAD SSH PUBLIC KEY to download the pasted key as a .txt file.

When Disable Password is Yes, the Password field becomes unavailable. Any existing password is removed from the account. The Lock User and Permit Sudo options are also removed. The account is then restricted from password-based logins for services. For example, disabling the password prevents using account credentials to log in to an SMB share or open an SSH session on the system. By default, Disable Password is No.

A specific shell can be set for the user from the Shell drop-down:

<table>
<thead>
<tr>
<th>Shell</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>csh</td>
<td>C shell, for UNIX system interactions.</td>
</tr>
<tr>
<td>sh</td>
<td>Bourne shell</td>
</tr>
<tr>
<td>tcsh</td>
<td>Enhanced C shell, that includes editing and name completion.</td>
</tr>
<tr>
<td>bash</td>
<td>Bourne Again shell, for the GNU operating system.</td>
</tr>
<tr>
<td>ksh93</td>
<td>Korn shell, that incorporates features from both csh and sh.</td>
</tr>
<tr>
<td>mksh</td>
<td>MirBSD Korn Shell</td>
</tr>
<tr>
<td>rbash</td>
<td>Restricted bash</td>
</tr>
<tr>
<td>rzsh</td>
<td>Restricted zsh</td>
</tr>
<tr>
<td>scponly</td>
<td>scponly, restricts the user’s SSH usage to only the scp and sftp commands.</td>
</tr>
<tr>
<td>zsh</td>
<td>Z shell</td>
</tr>
<tr>
<td>git-shell</td>
<td>restricted git shell</td>
</tr>
<tr>
<td>nologin</td>
<td>Use when creating a system account or to create a user account that can authenticate with shares but which cannot log in to the TrueNAS system using ssh.</td>
</tr>
</tbody>
</table>
Setting *Lock User* disables all password-based functionality for this account until the option is unset.

*Permit Sudo* allows this account to act as the system administrator using the `sudo` command. For better security, leave this option disabled.

When the user account is going to be using a *Windows 8* or newer client to access data stored on TrueNAS, set *Microsoft Account*. This enables additional authentication methods available from those operating systems.

By default, *Samba Authentication* is enabled. This allows using the account credentials to access data shared with SMB.
3 - System

3.1 - General

3.1.1 - Settings

TrueNAS has numerous settings contained inside System > General. These allow a wide range of system customization, from changing the web interface address, localization options, and data collection to SED, console, and storage options.

<table>
<thead>
<tr>
<th>GUI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI SSL Certificate *</td>
<td>The system uses a self-signed certificate to enable encrypted web interface connections. To change the default certificate, select a different certificate that was created or imported in the Certificates menu.</td>
</tr>
<tr>
<td>Web Interface IPv4 Address *</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Web Interface IPv6 Address *</td>
<td>::</td>
</tr>
<tr>
<td>Web Interface HTTP Port</td>
<td>80</td>
</tr>
<tr>
<td>Web Interface HTTPS Port</td>
<td>443</td>
</tr>
<tr>
<td>HTTPS Protocols</td>
<td>TLSv1.2, TLSv1.3</td>
</tr>
<tr>
<td>Web Interface HTTP -&gt; HTTPS Redirect</td>
<td></td>
</tr>
</tbody>
</table>

Localization

<table>
<thead>
<tr>
<th>Language</th>
<th>Console Keyboard Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td></td>
</tr>
</tbody>
</table>

Sort languages by: Name, Language code

Data Format

<table>
<thead>
<tr>
<th>Data Format</th>
<th>Time Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-12-11</td>
<td>08:01:05 (24 Hours)</td>
</tr>
</tbody>
</table>

Other Options

- Crash reporting
- Usage collection
Choose a recent IP address to limit the usage when accessing the administrative GUI. The built-in HTTP server binds to the wildcard address of 0.0.0.0 (any address) and issues an alert if the specified address becomes unavailable.

Choose a recent IPv6 address to limit the usage when accessing the administrative GUI. The built-in HTTP server binds to the wildcard address of 0.0.0.0 (any address) and issues an alert if the specified address becomes unavailable.

Allow configuring a non-standard port to access the GUI over HTTP. Changing this setting might require changing a Firefox configuration setting.

Allow configuring a non-standard port to access the GUI over HTTPS.

Cryptographic protocols for securing client/server connections. Select which Transport Layer Security (TLS) versions TrueNAS can use for connection security.

Redirect HTTP connections to HTTPS. A GUI SSL Certificate is required for HTTPS. Activating this also sets the HTTP Strict Transport Security (HSTS) maximum age to 31536000 seconds (one year). This means that after a browser connects to the web interface for the first time, the browser continues to use HTTPS and renews this setting every year.

Choose a language from the drop-down menu.

Select a date format.

Select a keyboard layout.

Select a time zone.

Select a time format.

Send failed HTTP request data which can include client and server IP addresses, failed method call tracebacks, and middleware log file contents to iXsystems.

Enable sending anonymous usage statistics to iXsystems.

After making any changes, click **SAVE**. Changes to any of the web interface fields can interrupt web interface connectivity while the new settings are applied.

This screen also contains these buttons:

- **SAVE CONFIG**

Saves a backup copy of the current configuration database in the format `hostname-version-architecture`. This file is downloaded to the computer accessing the web interface. Saving the configuration after making any configuration changes is highly recommended.

See [System Config Backups](#) for more details about backing up the system configuration.
**UPLOAD CONFIG**

Changes the system configuration settings. Browse to a previously saved configuration file to restore that configuration.

This can cause unexpected changes to system settings. Investigate both the current system settings and the settings stored in the other configuration file before uploading a config file to TrueNAS.

**RESET CONFIG**

Reset the configuration database to the default base version. This does not delete user SSH keys or any other data stored in a user home directory. Since configuration changes stored in the configuration database are erased, this option is useful when correcting mistakes or returning a test system to the original configuration.
3.1.2 - System Config Backups

We highly recommend backing up the system configuration regularly. Doing so preserves settings when migrating, restoring, or fixing the system if it runs into any issues. Save the configuration file each time the system configuration changes.

**Manual Backup**

To back up the system configuration, go to **System > General** and click **SAVE CONFIG**, then enter your password.

The configuration file contains sensitive data about the TrueNAS system. Ensure that it is stored somewhere safe.

**Automatic Backup**

TrueNAS automatically backs up the configuration database to the **system dataset** every morning at 3:45 (relative to system time settings). However, this backup does not occur if the system is shut down at that time. When the system dataset is stored on the boot pool and the boot pool becomes unavailable, the backup also loses availability.

SSH keys are not stored in the configuration database and must be backed up separately. System host keys are files with names beginning with `ssh_host_` in `/usr/local/etc/ssh/`. The root user keys are stored in `/root/.ssh`.

**Passwords**

The system backup affects two types of passwords: hashed and encrypted:

- **Hashed**
  TrueNAS stores user account passwords for the base operating system as hashed values. The system will save them in the system configuration backup, so they do not need to be encrypted to be secure.

- **Encrypted**
  The system will save other passwords, like iSCSI CHAP passwords, Active Directory bind credentials, and cloud credentials in an encrypted form to prevent them from being visible as plain text in the saved system configuration. The key or seed for this encryption is normally stored only on the operating system device.

There are two options after clicking **SAVE CONFIG**:

1. **Export Password Secret Seed** includes encrypted passwords in the configuration file. This allows the configuration file to be restored to a different operating system device where the decryption seed is not already present. Users must physically secure configuration backups containing the seed to prevent unauthorized access or password decryption.

2. **Export Legacy Encryption (GELI) Keys** includes encrypted legacy encryption keys in the configuration file.
Users can restore the encryption keys by uploading the configuration file to the system using `UPLOAD CONFIG`.

---

### Save Configuration

**WARNING:** This configuration file contains system passwords and other sensitive data.

**WARNING:** SSH keys in `/root/.ssh` are **NOT** backed up by this operation.

- [ ] Export Secret Seed
- [ ] Export Legacy Encryption (GELI) Keys

**Root Password** *

Including the Password Secret Seed allows using this configuration file with a new boot device. This also decrypts all system passwords for reuse when the configuration file is uploaded.

*Keep the configuration file safe and protect it from unauthorized access!*

---

### Backup Contents

Backup configs store information for accounts, network, services, and system settings, as well as settings for tasks and virtual machines.

Backup configs also index ID’s and credentials for account, network, and system services. Users can view the contents of the backup config using database viewing software like [SQLite DB Browser](https://sqlitebrowser.org/).

### Resetting and Restoring Configurations

Reset Configuration
Users can reset their system’s configuration to factory settings by going to System > General and clicking *RESET CONFIG*.

**Save the system’s current configuration before resetting the configuration.**

If you do not save the system configuration before resetting it, you may lose any data that was not backed up and will not be able to revert back the previous settings.

After resetting the system configuration, the system will restart and you will have to set a new login password.

**Restore Configuration**

Users can restore configurations by going to System > General and clicking *UPLOAD CONFIG*.

When uploading a config, users can select any previously saved config files for their system.
3.1.3 - Managing TLS Ciphers

- Allowing or Restricting TLS Ciphers

This feature was introduced in TrueNAS 12.0

TrueNAS accepts different Transport Layer Security (TLS) cipher suites for secure connections to the web interface. For best security, only use TLS 1.2 or newer. By default, all options are available if you need to adjust this setting to match your particular network environment or security concerns.

Allowing or Restricting TLS Ciphers

Log in to the web interface and go to System > General:

Click on HTTPS Protocols to open a dropdown menu with the various cipher suites.
- **TLSv1**
  Introduced in 1999, TLSv1.0 provides Internet communication security using encryption and other secure messaging techniques. While not officially deprecated, this suite has been considered obsolete since 2008 and replaced by newer versions of the suite. For security reasons, users are encouraged to avoid enabling this suite unless required by the network environment.

- **TLSv1.1**
  Introduced in 2006, TLSv1.1 is a small revision of v1.0 with additional protections against CBC attacks. While not officially deprecated, this suite has been considered obsolete since 2008 and replaced by newer versions of the suite. For security reasons, users are encouraged to avoid enabling this suite unless required by the network environment.

- **TLSv1.2**
  Introduced in 2008, TLSv1.2 greatly increases the protocol’s ability to handle cryptographic algorithms. This represents a major step forward in security effectiveness and resulted in the “soft” deprecation of TLS versions 1.0 and 1.1.

- **TLSv1.3**
  Introduced in 2018, TLSv1.3 represents another major improvement to the protocol. Legacy or insecure encryption algorithms are removed, additional encryption for handshake messages added, and authentication and key exchange concepts are separated.

Unsetting a cipher restricts its use in TrueNAS. After enabling or disabling a cipher, the TrueNAS system must be rebooted.
3.2 - NTP Servers

Network Time Protocol (NTP) servers sync the local system time with an accurate external reference. By default, new installations use several existing NTP servers. TrueNAS supports adding custom NTP servers.

Adding a Custom NTP Server

Go to System > NTP Servers to view, edit, or remove NTP Servers:

Several default servers are listed. To register a new server, click ADD and configure the options.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Enter the hostname or IP address of the NTP server.</td>
</tr>
<tr>
<td>Burst</td>
<td>Recommended when Max. Poll is greater than 10. Only use on personal NTP servers or those under direct control. Do not enable when using public NTP servers.</td>
</tr>
<tr>
<td>IBurst</td>
<td>Speeds up the initial synchronization (seconds instead of minutes).</td>
</tr>
<tr>
<td>Prefer</td>
<td>Should only be used for highly accurate NTP servers such as those with time monitoring hardware.</td>
</tr>
<tr>
<td>Min Poll</td>
<td>The minimum polling interval, in seconds, as a power of 2. For example, 6 means 2^6, or 64 seconds. The default is 6, minimum value is 4.</td>
</tr>
<tr>
<td>Max Poll</td>
<td>The maximum polling interval, in seconds, as a power of 2. For example, 10 means 2^10, or 1,024 seconds. The default is 10, maximum value is 17.</td>
</tr>
<tr>
<td>Force</td>
<td>Forces the addition of the NTP server, even if it is currently unreachable.</td>
</tr>
</tbody>
</table>
3.3 - Boot

3.3.1 - Boot Screen

- Managing Boot Environments
- Boot Actions
- Changing Boot Environments

TrueNAS supports a ZFS feature known as boot environments. These are snapshot clones that TrueNAS can boot into. Only one boot environment can be used for booting.

How does this help me? expand □
A boot environment allows rebooting into a specific point in time and greatly simplifies recovering from system misconfigurations or other potential system failures. With multiple boot environments, the process of updating the operating system becomes a low-risk operation. The updater automatically creates a snapshot of the current boot environment and adds it to the boot menu before applying the update. If anything goes wrong during the update, the system administrator can boot TrueNAS into the previous environment to restore system functionality.

Go to System > Boot to see a boot environment list.

Managing Boot Environments

To view the list of boot environments on the system, go to System > Boot. Each boot environment entry contains this information:

- **Name**: the name of the boot entry as it appears in the boot menu.
- **Active**: indicates which entry boots by default if a boot environment is not active.
- **Created**: indicates the boot environment creation date and time.
- **Space**: shows boot environment size.
- **Keep**: indicates whether or not TrueNAS deletes this boot environment when a system update does not have enough space to proceed.

To access more options for a boot environment, click □:

- **Activate**: Only appears on entries which are not currently set to Active. Activating an environment means the system boots into the point of time saved in that environment the next time it is started. The status changes to Reboot and the current Active entry changes from Now/Reboot to Now, indicating that it is the currently booted environment but will not be used on next boot.
- **Clone**: Copy the selected boot environment into a new entry. The clone Name only allows alphanumeric characters, dashes (-), underscores (_), and periods (.) are allowed.
- **Rename**: Changes the boot environment name. Alphanumeric characters, dashes (-), underscores (_), and periods (.) are allowed.
- **Delete**: Removes the highlighted entry and also removes that entry from the boot menu. The default and any Active entries cannot be deleted. Because an activated entry cannot be deleted, this button does not appear for the active boot environment. To delete a currently Active entry, first activate another entry.
- **Keep**: Toggles whether or not the updater can prune (automatically delete) this boot environment if there is not enough space to proceed with the update.

Boot Actions
Click ACTIONS to:

- **Add**

Make a new boot environment from the active environment:

Only alphanumeric characters, dashes (-), and underscores (_) are allowed in the Name. Name the new boot environment and click SUBMIT.

- **Stats/Settings**
  Display statistics for the operating system device: condition, total and used size, and date and time of the last scrub. By default, the operating system device is scrubbed every 7 days. To change the default, input a different number in the Automatic scrub interval (in days) field and click UPDATE INTERVAL.

- **Boot Pool Status**
  Shows the status of each device in the operating system device (boot-pool), including any read, write, or checksum errors.

- **Scrub Boot Pool**
  Perform a manual “scrub” (data integrity check) of the operating system device.

### Changing Boot Environments

Sometimes, rolling back to an older boot environment can be useful. For example, if an update process doesn’t go as planned, it is easy to roll back to a previous boot environment. TrueNAS automatically creates a boot environment when the system updates.

There are two different methods for changing the active boot environment: using the web interface and through a Command Line Interface (CLI)

- **Web Interface**
  To activate a different boot environment, go to System > Boot and click more_vert for the desired boot environment. Next, click Activate. This boot environment shows Reboot in the Active column. This means the boot environment becomes active on the next system boot. The system configuration also changes to the state it was in when the boot environment was created.

- **Command Line Interface**

  If the web interface is inaccessible but physical access to the system is still possible, the boot environment can be changed at the welcome screen of the CLI.

  Reboot the system. When the welcome screen appears, press the key that corresponds with the option Boot Environments. In the image below, the key to select the Boot Environments option is 7.

  The Boot Environments options does not appear when no additional boot environments are present.
After selecting the *Boot Environment* option, choose the new boot environment to activate. Press the corresponding key for the *Active:* option. In the picture below, the key is 2.

Press the key to cycle through existing boot environments. When the desired boot environment is selected, press *Backspace* to return to the welcome menu. Then, press 4 to reboot the system. The selected boot environment is used when the system reboots.
3.3.2 - Mirroring the Boot Pool

Adding a second storage device to the boot pool changes the configuration to a **Mirror**. This allows one of the devices to fail and the system still boots. If one of the two devices were to fail, that device is easily detached and replaced.

View the current boot pool status by going to **System > Boot > ACTIONS > Boot Pool Status**.

On this page you will find the list and status of each boot pool on the system. By default, this pool is named **boot-pool**.

When adding a second device to create a mirrored boot pool, consider these caveats:

- **Capacity**: The new device must have at least the same capacity as the existing device. Larger capacity devices can be added, but the mirror will only have the capacity of the smallest device. Different models of devices which advertise the same nominal size are not necessarily the same actual size. For this reason, adding another device of the same model of is recommended.

- **Device Type**: It is **strongly recommended** to use SSDs rather than USB devices when creating a mirrored boot pool.

Click  on the boot device entry to see all possible actions. These are used to mirror the boot pool or maintain it later:

- **Attach**

Add another disk to the pool. For the system boot pool, this is used to create a mirrored configuration. Click **Attach** and select the new **Member Disk**.

- **Use all disk space option expand**

This option controls the available capacity for the device. By default, the new device is partitioned to the same size as the existing device. When **Use all disk space** is enabled, the entire capacity of the new device is used.

If the original operating system device fails and is detached, the boot mirror changes to consist of just the newer device and grows to whatever capacity it provides. However, new devices added to this mirror must now be as large as the new capacity.

Click **SAVE** to attach the new device to the mirror.

- **Detach**

Removes the device from the pool.

**Removing devices from storage pools can result in data loss!**

When the device is critical to the pool, the pool status changes to **Degraded** or even **Failed**. This is part of the disk replacement procedure.

- **Replace**

Integrates a new disk into the current location of this disk. Part of the disk replacement procedure. **Detach** the failed device, **Replace** and select the new **Member Disk**, and **Save** to rebuild the mirror.
3.4 - Advanced

**System > Advanced** contains more advanced options for configuring system settings.

These options have reasonable defaults in place. Make sure you are comfortable with ZFS, FreeBSD, and system configuration backup and restoration before making any changes.

---

**Console**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Text Console without Password Prompt</td>
<td>Unset to add a login prompt to the system before the console menu is shown.</td>
</tr>
<tr>
<td>Enable Serial Console</td>
<td>Do not set this if the Serial Port is disabled. <strong>Serial Port</strong> and <strong>Serial Speed</strong> options are visible when this is set.</td>
</tr>
<tr>
<td>Serial Port</td>
<td>When <strong>Enable Serial Console</strong> is set, the available serial port hex addresses are 0x2F8 or 0x3F8.</td>
</tr>
<tr>
<td>Serial Speeds</td>
<td>When <strong>Enable Serial Console</strong> is set, the available serial speeds that can be used by the serial port are 9600 bps, 19200 bps, 38400 bps, 57600 bps, or 115200bps.</td>
</tr>
<tr>
<td>MOTD Banner</td>
<td>The message to show when a user logs in with SSH.</td>
</tr>
</tbody>
</table>

---

**Storage**
### Swap Size in GiB (CORE only)

By default, all data disks are created with the amount of swap specified. Changing the value does not affect the amount of swap on existing disks, only disks added after the change. Does not affect log or cache devices as they are created without swap. Setting to 0 disables swap creation completely. **STRONGLY DISCOURAGED**

### LOG (Write Cache) Overprovision Size in GiB

Overprovisioning a ZFS Log SSD can increase its performance and lifespan by distributing writes and erases across more drive flash blocks. Defining a number of GiB here overprovisions ZFS Log disks during pool creation or extension. Examples: 50 GiB, 10G, 5GB

### GUI

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Console Messages</td>
<td>Display console messages in real time at the bottom of the browser.</td>
</tr>
<tr>
<td>Show Advanced Fields by Default</td>
<td>Set to always show advanced fields, when available.</td>
</tr>
</tbody>
</table>

### Kernel

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Console Messages</td>
<td>Display console messages in real time at the bottom of the browser.</td>
</tr>
<tr>
<td>Show Advanced Fields by Default</td>
<td>Set to always show advanced fields, when available.</td>
</tr>
</tbody>
</table>

### Self-Encrypting Drive

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATA Security User</td>
<td>User passed to camcontrol security -u to unlock SEDs</td>
</tr>
<tr>
<td>SED Password</td>
<td>Global password to unlock SEDs.</td>
</tr>
</tbody>
</table>

### Syslog

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use FQDN for Logging</td>
<td>Set to include the Fully-Qualified Domain Name (FQDN) in logs to precisely identify systems with similar hostnames.</td>
</tr>
<tr>
<td>Syslog Level</td>
<td>When Syslog Server is defined, only logs matching this level are sent.</td>
</tr>
<tr>
<td>Syslog Server</td>
<td>Remote syslog server DNS hostname or IP address. Nonstandard port numbers can be used by adding a colon and the port number to the hostname, like mysyslogserver:1928. Log entries are written to local logs and sent to the remote syslog server.</td>
</tr>
<tr>
<td>Syslog Transport</td>
<td><strong>Transport Protocol</strong>[1] for the remote system log server connection. Choosing Transport Layer Security (TLS) also requires selecting a preconfigured system Certificate.</td>
</tr>
</tbody>
</table>

There is also an option to **SAVE DEBUG**. This generates text files that contain diagnostic information. After the debug data is collected, the system prompts for a location to save the compressed .tar file.

### Autotuning

TrueNAS provides an autotune script that optimizes the system depending on the installed hardware.

**Is this script available somewhere?** expand □
To see which checks are performed, the autotune script is located in /usr/local/bin/autotune.

For example, if a pool exists on a system with limited RAM, the autotune script automatically adjusts some ZFS sysctl values in an attempt to minimize memory starvation issues. Autotuning can introduce system performance issues and must only be used as a temporary measure on a system until the underlying hardware issue is addressed. Autotune always slows a RAM-starved system, as it caps the ARC.

Using the autotuning script is not recommended for TrueNAS Enterprise customers as this can override any specific tunings made by iXsystems Support.

Enabling autotuning runs the autotuner script at boot. To run the script immediately, reboot the system.

Any tuned settings appear in **System > Tunables.**

**Can I manually tune a setting controlled by the autotuner?**

Deleting tunables created by the autotune only affects the current session. Autotune-set tunables are recreated every time the system boots. This means any setting controlled by the autotuner does not allow for further manual tuning.

To permanently change a value set by autotune, change the description of the tunable. For example, changing the description to manual override prevents autotune from reverting that tunable back to the autotune default value.

When attempting to increase the performance of the TrueNAS system, and particularly when the current hardware is limiting performance, try enabling autotune.
3.5 - View Enclosure

Only compatible TrueNAS hardware and expansion shelves available from iXsystems allow seeing the View Enclosure option. To learn more about available iXsystems products, see the TrueNAS Systems Overview or browse the Hardware documentation.

Go to System > View Enclosure to display the status of connected disks and hardware.

The screen shows the primary system. Other detected TrueNAS hardware is available from a column on the right side of the screen. Click an enclosure to show details about that hardware.

The screen is divided into different tabs. These tabs reflect the sensors that are active in the chosen hardware. Some or all of these can show in the View Enclosure screen. The system can be renamed from any tab by clicking EDIT LABEL.

 Collider Disks

Shows a graphic representation of the TrueNAS hardware and details about connected disks.
Click any disk slot to see specific details about the disk like the device name, vdev assignment, function, drive slot number, serial number, and current drive settings. *IDENTIFY DRIVE* flashes the identification LED for the chosen drive.

The **Disks Overview** shows statistics about the enclosure pools, status, and detected expanders. There are options to show more details about pools in the enclosure, disk status, and expansion shelf status. Clicking any of the buttons changes the graphic to show the requested details.

**Cooling**

Shows the current status and RPM of each connected fan.
<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Status</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Fan Group #1_PS A</td>
<td>OK</td>
<td>6660 RPM</td>
</tr>
<tr>
<td>Virtual Fan Group #2_PS B</td>
<td>OK</td>
<td>6710 RPM</td>
</tr>
<tr>
<td>Fan #1_Virtual Fan Group #1_PS A</td>
<td>OK</td>
<td>7600 RPM</td>
</tr>
<tr>
<td>Fan #2_Virtual Fan Group #1_PS A</td>
<td>OK</td>
<td>5700 RPM</td>
</tr>
<tr>
<td>Fan #3_Virtual Fan Group #1_PS A</td>
<td>OK</td>
<td>7700 RPM</td>
</tr>
<tr>
<td>Fan #4_Virtual Fan Group #1_PS A</td>
<td>OK</td>
<td>5600 RPM</td>
</tr>
<tr>
<td>Fan #5_Virtual Fan Group #1_PS A</td>
<td>OK</td>
<td>7600 RPM</td>
</tr>
<tr>
<td>Fan #6_Virtual Fan Group #1_PS A</td>
<td>OK</td>
<td>5700 RPM</td>
</tr>
<tr>
<td>Fan #7_Virtual Fan Group #1_PS A</td>
<td>OK</td>
<td>8000 RPM</td>
</tr>
<tr>
<td>Fan #8_Virtual Fan Group #1_PS A</td>
<td>OK</td>
<td>8000 RPM</td>
</tr>
<tr>
<td>Fan #1_Virtual Fan Group #2_PS B</td>
<td>OK</td>
<td>7800 RPM</td>
</tr>
<tr>
<td>Fan #2_Virtual Fan Group #2_PS B</td>
<td>OK</td>
<td>5700 RPM</td>
</tr>
<tr>
<td>Fan #3_Virtual Fan Group #2_PS B</td>
<td>OK</td>
<td>7700 RPM</td>
</tr>
<tr>
<td>Fan #4_Virtual Fan Group #2_PS B</td>
<td>OK</td>
<td>5700 RPM</td>
</tr>
<tr>
<td>Fan #5_Virtual Fan Group #2_PS B</td>
<td>OK</td>
<td>7700 RPM</td>
</tr>
<tr>
<td>Fan #6_Virtual Fan Group #2_PS B</td>
<td>OK</td>
<td>5800 RPM</td>
</tr>
<tr>
<td>Fan #7_Virtual Fan Group #2_PS B</td>
<td>OK</td>
<td>7600 RPM</td>
</tr>
<tr>
<td>Fan #8_Virtual Fan Group #2_PS B</td>
<td>OK</td>
<td>5700 RPM</td>
</tr>
</tbody>
</table>

- **Enclosure Services Controller Electronics**

  Shows the enclosure status.
### Power Supply

Shows details about each power supply.

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Status</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESCE_A_500E0ECA06BFFEDBE</td>
<td>OK</td>
<td>256</td>
</tr>
<tr>
<td>ESCE_B_500E0ECA06BFFEDFE</td>
<td>OK</td>
<td>256</td>
</tr>
</tbody>
</table>

### SAS Connector

Shows the status of the SAS connector components.

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Status</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS_A_010=-_CCCT16496699</td>
<td>OK</td>
<td>None</td>
</tr>
<tr>
<td>PS_B_010=-_CCCT16076228</td>
<td>OK</td>
<td>None</td>
</tr>
</tbody>
</table>
### Temperature Sensor

Shows the current temperature of each expansion shelf and the disk chassis.

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Status</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Connector_ESCE A</td>
<td>OK</td>
<td>Mini SAS HD 4x receptacle (SFF-8644) [max 4 phys]</td>
</tr>
<tr>
<td>Downlink Connector_ESCE B</td>
<td>OK</td>
<td>Mini SAS HD 4x receptacle (SFF-8644) [max 4 phys]</td>
</tr>
</tbody>
</table>
Voltage Sensor

Shows the current voltage for each sensor, VCCP, and VCC.
<table>
<thead>
<tr>
<th>Descriptor</th>
<th>Status</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.7V_scfuse_mfd_ESCE A</td>
<td>OK</td>
<td>1.68V</td>
</tr>
<tr>
<td>0.6V_prtt_ddr_fd_ESCE A</td>
<td>OK</td>
<td>0.6V</td>
</tr>
<tr>
<td>1.05V_mfd_ESCE A</td>
<td>OK</td>
<td>1.05V</td>
</tr>
<tr>
<td>1.5V_pch_fd_ESCE A</td>
<td>OK</td>
<td>1.48V</td>
</tr>
<tr>
<td>0.9V_mf_ESCE A</td>
<td>OK</td>
<td>0.91V</td>
</tr>
<tr>
<td>0.92V_f_ESCE A</td>
<td>OK</td>
<td>0.96V</td>
</tr>
<tr>
<td>1.3V_lhrv_mfd_ESCE A</td>
<td>OK</td>
<td>1.28V</td>
</tr>
<tr>
<td>1.2V_wddq_cpu_fd_ESCE A</td>
<td>OK</td>
<td>1.2V</td>
</tr>
<tr>
<td>1.65V_pmcore_cpu_fd_ESCE A</td>
<td>OK</td>
<td>1.78V</td>
</tr>
<tr>
<td>1.8V_mf_ESCE A</td>
<td>OK</td>
<td>1.79V</td>
</tr>
<tr>
<td>12.0V_amfd_ESCE A</td>
<td>OK</td>
<td>12.0V</td>
</tr>
<tr>
<td>3.3V_amfd_ESCE A</td>
<td>OK</td>
<td>3.31V</td>
</tr>
<tr>
<td>3.3V_bat_ESCE A</td>
<td>OK</td>
<td>3.18V</td>
</tr>
<tr>
<td>1.7V_scfuse_mfd_ESCE B</td>
<td>OK</td>
<td>1.68V</td>
</tr>
<tr>
<td>0.6V_prtt_ddr_fd_ESCE B</td>
<td>OK</td>
<td>0.6V</td>
</tr>
<tr>
<td>1.05V_mfd_ESCE B</td>
<td>OK</td>
<td>1.05V</td>
</tr>
<tr>
<td>1.5V_pch_fd_ESCE B</td>
<td>OK</td>
<td>1.48V</td>
</tr>
<tr>
<td>0.9V_mf_ESCE B</td>
<td>OK</td>
<td>0.9V</td>
</tr>
<tr>
<td>0.92V_f_ESCE B</td>
<td>OK</td>
<td>0.95V</td>
</tr>
<tr>
<td>1.3V_lhrv_mfd_ESCE B</td>
<td>OK</td>
<td>1.28V</td>
</tr>
<tr>
<td>1.2V_wddq_cpu_fd_ESCE B</td>
<td>OK</td>
<td>1.19V</td>
</tr>
</tbody>
</table>
An automatic script sends a nightly email to the administrator (root) account containing important information such as the health of the disks. Alert events are also emailed to the root user account. Configure the system to send these emails to the administrator’s remote email account for fast awareness and resolution of any critical issues.

Scrub Task issues and S.M.A.R.T. reports are mailed separately to the address configured in those services.

TrueNAS Root Email Address

Before configuring anything else, set the root account email address. Go to Accounts > Users, click more_vert and Edit for the root user. In the Email field, enter a remote email address that is regularly monitored by the system administrator, like admin@example.com and click SAVE.

Email Options

The remaining configuration is done from System > Email.

General Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Email</td>
<td>The user account Email address to use for the envelope From email address. The user account Email in Accounts &gt; Users &gt; Edit must be configured first.</td>
</tr>
<tr>
<td>From Name</td>
<td>The friendly name to show in front of the sending email address. Example: Storage System 01<a href="mailto:it@example.com">it@example.com</a></td>
</tr>
</tbody>
</table>

Send Mail Method

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP</td>
<td>Shows SMTP configuration options.</td>
</tr>
<tr>
<td>GMail OAuth</td>
<td>Shows GMail authentication options.</td>
</tr>
</tbody>
</table>

Changing the Send Mail Method shows different options:

SMTP
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outgoing Mail Server</td>
<td>Hostname or IP address of SMTP server used for sending email.</td>
</tr>
<tr>
<td>Mail Server Port</td>
<td>SMTP port number. Typically 25/465 (secure SMTP), or 587 (submission).</td>
</tr>
<tr>
<td>Security</td>
<td>Choose an encryption type. Choices are Plain (No Encryption), SSL (Implicit TLS), or TLS (STARTTLS).</td>
</tr>
<tr>
<td>SMTP Authentication</td>
<td>Set when the SMTP server uses authentication credentials. Shows additional credentials options.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the SMTP username when the SMTP server requires authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the SMTP account password if needed for authentication. Only plain text characters (7-bit ASCII) are allowed in passwords. UTF or composed characters are not allowed.</td>
</tr>
</tbody>
</table>

GMail OAuth

To use Gmail OAuth, select the option and click **LOG IN TO GMAIL.**
Log into a GMail account as normal for TrueNAS to autoconfigure the connection to GMail.

Click **SEND TEST MAIL** to verify the configured email settings are working. If the test email fails, double-check that the *Email* field of the root user is correctly configured by clicking the **Edit** button for the *root* account in **Accounts > Users**.
The system dataset stores debugging core files, encryption keys for encrypted pools, and Samba4 metadata such as the user and group cache and share level permissions.

To view the current location of the system dataset, go to **System > System Dataset**.

**Change System Dataset**

Users can change the system dataset by selecting an existing pool from the **System Dataset Pool** dropdown.

Users can also move the system dataset to unencrypted pools or encrypted pools that do not have passphrases.

Moving the system dataset to an encrypted pool disables that volume’s passphrase capability.

You cannot move the system dataset to a passphrase-encrypted pool or a read-only pool.

**Reboots Required**

- The SMB service must restart, which causes a brief outage for any active SMB connections.
- Highly Available TrueNAS systems must reboot the standby controller when the system dataset moves.

If a user changes the pool storing the system dataset later, TrueNAS will migrate the existing data in the system dataset to the new location.

**Storing the System Log**

Users can store the system log on the system dataset. We recommend users store the log information on the system dataset when the system generates large amounts of data and has limited memory or a limited capacity operating system device.

Set **Syslog** to store the system log on the system dataset. Leave unset to store the system log in /var on the operating system device.
3.8 - Reporting

TrueNAS has a built in reporting engine that gives helpful graphs and information about the system.

What does TrueNAS use for reporting? expand □

TrueNAS uses Graphite for metric gathering and visualizations.

The options in System > Reporting control how the graphs in Reporting appear:

General Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report CPU usage in Percent</td>
<td>Reports CPU usage in percent instead of units of kernel time.</td>
</tr>
<tr>
<td>Graphite Separate Instances</td>
<td>Sends the plugin instance and type instance to Graphite as separate path components: host.cpu.0.cpu.idle. Disabling sends the plugin and plugin instance as one path component and type and type instance as another: host.cpu-0.cpu-idle.</td>
</tr>
<tr>
<td>Remote Graphite Server Hostname</td>
<td>Remote Graphite server Hostname or IP address.</td>
</tr>
<tr>
<td>Graph age in Months</td>
<td>Maximum time (in months) TrueNAS stores a graph (allowed values are 1-60). Changing this value causes the Confirm RRD Destroy dialog to appear. Changes do not take effect until TrueNAS destroys the existing reporting database.</td>
</tr>
<tr>
<td>Number of Graph Points</td>
<td>The number of points for each hourly, daily, weekly, monthly, or yearly graph (allowed values are 1-4096). Changing this value displays the Confirm RRD Destroy dialog. Changes do not take effect until TrueNAS destroys the existing reporting database.</td>
</tr>
<tr>
<td>Force</td>
<td>Forces TruNAS to add the NTP server, even if it is unreachable.</td>
</tr>
</tbody>
</table>

Report history is cleared when Report CPU, Graph Age, or Graph Points are changed.

Reporting data is saved and preserved across system upgrades and reboots. This allows viewing usage trends over time. This data is frequently written and should not be stored on the boot pool or operating system device. Reporting data is saved in `/var/db/collectd/rrd/`. 
The alert system integrates with various third-party services. Tuning alerts also helps personalize TrueNAS to any highly-sensitive issues.

### Alert Services

Alert Services are the various methods built into TrueNAS that can notify you of a system alert.

Some of alert services are third-party integrations that can charge for message or data usage.

### Adding a Service

To add a new alert service, go to **System > Alert Services** and click **ADD**.

#### Name and Type

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the new alert service.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Unset to disable this service without deleting it.</td>
</tr>
<tr>
<td>Type</td>
<td>Choose an alert service to display options for that service.</td>
</tr>
<tr>
<td>Level</td>
<td>Select the level of severity.</td>
</tr>
</tbody>
</table>

Choosing a **Type** adds options specific to that alert service:

#### AWS

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Region</td>
<td>Enter the <a href="#">AWS account region</a>.</td>
</tr>
<tr>
<td>Key ID</td>
<td>Access Key ID for the linked AWS account.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>Secret Access Key for the linked AWS account.</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------</td>
</tr>
</tbody>
</table>

**Email**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Address</td>
<td>Enter a valid email address to receive alerts from this system.</td>
</tr>
</tbody>
</table>

**InfluxDB**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the InfluxDB hostname.</td>
</tr>
<tr>
<td>Username</td>
<td>Username for this service.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter password.</td>
</tr>
<tr>
<td>Database</td>
<td>Name of the InfluxDB database.</td>
</tr>
<tr>
<td>Series</td>
<td>InfluxDB time series name for collected points.</td>
</tr>
</tbody>
</table>

**Mattermost**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webhook URL</td>
<td>Enter or paste the incoming webhook URL associated with this service.</td>
</tr>
<tr>
<td>Username</td>
<td>Mattermost username.</td>
</tr>
<tr>
<td>Channel</td>
<td>Name of the channel to receive notifications. This overrides the default channel in the incoming webhook settings.</td>
</tr>
</tbody>
</table>

**OpsGenie**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Key</td>
<td>Enter or paste the API key. Find the API key by signing into the OpsGenie web interface and going to Integrations/Configured Integrations. Click the desired integration, Settings, and read the API Key field.</td>
</tr>
<tr>
<td>API URL</td>
<td>Leave empty for default OpsGenie API.</td>
</tr>
</tbody>
</table>

**Pager Duty**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Key</td>
<td>Enter or paste the “integration/service” key for this system to access the PagerDuty API.</td>
</tr>
<tr>
<td>Client Name</td>
<td>PagerDuty client name.</td>
</tr>
</tbody>
</table>

**Slack**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webhook URL</td>
<td>Paste the incoming webhook URL associated with this service.</td>
</tr>
</tbody>
</table>

**SNMP Trap**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Hostname or IP address of the system to receive SNMP trap notifications.</td>
</tr>
<tr>
<td>Port</td>
<td>UDP port number on the system receiving SNMP trap notifications. The default is 162.</td>
</tr>
<tr>
<td>SNMPv3 Security Model</td>
<td>Enable the SNMPv3 security model.</td>
</tr>
<tr>
<td>SNMP Community</td>
<td>Network community string. The community string acts like a user ID or password. A user with the correct community string has access to network information. The default is public. For more information, see this helpful SNMP Community Strings tutorial.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>API Key</td>
<td>Enter or paste the VictorOps API key.</td>
</tr>
<tr>
<td>Routing Key</td>
<td>Enter or paste the VictorOps routing key.</td>
</tr>
</tbody>
</table>

Test the service configuration by clicking **SEND TEST ALERT**.

**Alert Settings**

To modify the default system alerts, go to **System > Alert Settings**.
The alerts are grouped into sections based on type. For example, alerts that are related to pools appear in the **Storage** alert section.

### Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Warning Level</td>
<td>Customizes the importance of the alert. Each level of importance has a different icon and color to express the level of importance: <em>Info, Notice, Warning, Error, Critical</em> (Default), <em>Alert</em>, and <em>Emergency</em>.</td>
</tr>
</tbody>
</table>
Adjust how often alert notifications are sent. Setting the Frequency to NEVER prevents that alert from being added to alert notifications, but the alert can still show in the web interface if it is triggered. Options: *Immediately* (Default), *Hourly*, *Daily*, and *Never*.

Changing any of these options affects every configured alert service.

**Alert Warning Levels**

Each warning level has a different icon and color to express its importance. To make the system email you when alerts with a specific warning level trigger, set up an email Alert Service with that warning level.

<table>
<thead>
<tr>
<th>Level</th>
<th>Icon</th>
<th>Alert Notification?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 INFO</td>
<td>![i icon]</td>
<td>No</td>
</tr>
<tr>
<td>2 NOTICE</td>
<td>![i icon]</td>
<td>Yes</td>
</tr>
<tr>
<td>3 WARNING</td>
<td>![! icon]</td>
<td>Yes</td>
</tr>
<tr>
<td>4 ERROR</td>
<td>![! icon]</td>
<td>Yes</td>
</tr>
<tr>
<td>5 CRITICAL</td>
<td>![! icon]</td>
<td>Yes</td>
</tr>
<tr>
<td>6 ALERT</td>
<td>![i icon]</td>
<td>Yes</td>
</tr>
<tr>
<td>7 EMERGENCY</td>
<td>![i icon]</td>
<td>Yes</td>
</tr>
</tbody>
</table>
To begin integrating TrueNAS with a Cloud Storage provider, register the account credentials on the system. After saving any credentials, a Cloud Sync Task allows sending or receiving data from that Cloud Storage Provider.

## Saving a Cloud Storage Credential

Transferring data from TrueNAS to the Cloud requires saving Cloud Storage Provider credentials on the system.

### Is this secure? expand

To maximize security, these credentials are encrypted when saved. However, this means that to restore any cloud credentials from a TrueNAS configuration file, you must enable Export Password Secret Seed when generating that configuration backup. Remember to protect any downloaded TrueNAS configuration files.

It is recommended to have another browser tab open and logged in to the Cloud Storage Provider account you intend to link with TrueNAS. Some providers require additional information that is generated on the storage provider account page. For example, saving an Amazon S3 credential on TrueNAS could require logging in to the S3 account and generating an access key pair on the Security Credentials > Access Keys page.

To save cloud storage provider credentials, go to System > Cloud Credentials and click Add.

![Cloud Credential Form]

Enter a credential Name and choose a Provider. The rest of the options change according to the chosen Provider:

⊙ **Amazon S3**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Key ID</td>
<td>Amazon Web Services Key ID. This is found on Amazon AWS by going through My account &gt; Security Credentials &gt; Access Keys (Access Key ID and Secret Access Key). Must be alphanumeric and between 5 and 20 characters.</td>
</tr>
<tr>
<td>Secret Access Key</td>
<td>Amazon Web Services password. If the Secret Access Key cannot be found or remembered, go to Account &gt; Security Credentials &gt; Access Keys and create a new key pair. Must be alphanumeric and between 8 and 40 characters.</td>
</tr>
<tr>
<td>Maximum Upload</td>
<td>Define the maximum number of chunks for a multipart upload. This can be useful if a service does not support the 10,000 chunk AWS S3 specification.</td>
</tr>
<tr>
<td>Ports</td>
<td></td>
</tr>
</tbody>
</table>

- **Saving a Cloud Storage Credential**
- **Automatic Authentication**
### Amazon S3 Advanced Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Endpoint URL</strong></td>
<td><strong>S3 API endpoint URL.</strong> When using AWS, the endpoint field can be empty to use the default endpoint for the region, and available buckets are automatically fetched. Refer to the AWS Documentation for a list of <a href="https://docs.aws.amazon.com/AmazonS3/latest/userguide/website-endpoint.html">Simple Storage Service Website Endpoints</a>.</td>
</tr>
<tr>
<td><strong>Region</strong></td>
<td><strong>AWS resources in a geographic area.</strong> Leave empty to automatically detect the correct public region for the bucket. Entering a private region name allows interacting with Amazon buckets created in that region. For example, enter us-gov-east-1 to discover buckets created in the eastern AWS GovCloud region.</td>
</tr>
<tr>
<td><strong>Disable Endpoint Region</strong></td>
<td>Skip automatic detection of the Endpoint URL region. Set this when configuring a custom Endpoint URL.</td>
</tr>
<tr>
<td><strong>User Signature Version 2</strong></td>
<td>Force using <a href="https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-intro-security-encryption.html">Signature Version 2</a> to sign API requests. Set this when configuring a custom Endpoint URL.</td>
</tr>
</tbody>
</table>

#### BackBlaze B2

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key ID</strong></td>
<td>Alphanumeric <a href="https://www.backblaze.com/">Backblaze B2</a> Application Key ID. To generate a new application key, log in to the Backblaze account, go to the App Keys page, and add a new application key. Copy the application keyID string to this field.</td>
</tr>
<tr>
<td><strong>Application Key</strong></td>
<td>Backblaze B2 Application Key. To generate a new application key, log in to the Backblaze account, go to the App Keys page, and add a new application key. Copy the applicationKey string to this field.</td>
</tr>
</tbody>
</table>

#### Box

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Token</strong></td>
<td>A User Access Token for <a href="https://www.box.com">Box</a>. An <a href="https://www.box.com/">access token</a> enables Box to verify a request belongs to an authorized session. Example token: T9cE5asGnuvYCCqlZFoWjFHvNbvVqHjl.</td>
</tr>
</tbody>
</table>

#### Dropbox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Token</strong></td>
<td>Access Token for a Dropbox account. A <a href="https://www.dropbox.com/">token must be generated</a> by the <a href="https://www.dropbox.com/">Dropbox account</a> before adding it here.</td>
</tr>
</tbody>
</table>

#### FTP

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong></td>
<td>FTP Host to connect to. Example: ftp.example.com.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>FTP Port number. Leave blank to use the default port 21.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>A username on the FTP Host system. This user must already exist on the FTP Host.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Password for the user account.</td>
</tr>
</tbody>
</table>

#### Google Cloud Storage

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preview JSON Service Account Key</strong></td>
<td>Contents of the uploaded Service Account JSON file.</td>
</tr>
<tr>
<td><strong>Choose File</strong></td>
<td>Upload a Google <a href="https://console.cloud.google.com/iam/service-account">Service Account credential file</a>. The file is created with the <a href="https://cloud.google.com">Google Cloud Platform Console</a>.</td>
</tr>
</tbody>
</table>

#### Google Drive

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Token</strong></td>
<td>Token created with <a href="https://drive.google.com">Google Drive</a>. Access Tokens expire periodically and must be refreshed.</td>
</tr>
<tr>
<td>Team Drive ID</td>
<td>Only needed when connecting to a Team Drive. The ID of the top level folder of the Team Drive.</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>

**HTTP**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>HTTP host URL.</td>
</tr>
</tbody>
</table>

**Hubic**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Token</td>
<td>Access Token generated by a Hubic account</td>
</tr>
</tbody>
</table>

**Mega**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>MEGA account username.</td>
</tr>
<tr>
<td>Password</td>
<td>MEGA account password.</td>
</tr>
</tbody>
</table>

**Microsoft Azure Blob Storage**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>Microsoft Azure account name.</td>
</tr>
<tr>
<td>Account Key</td>
<td>Base64 encoded key for Azure Account</td>
</tr>
</tbody>
</table>

**Microsoft One Drive**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Token</td>
<td>Microsoft Onedrive Access Token. Log in to the Microsoft account to add an access token.</td>
</tr>
<tr>
<td>Drives List</td>
<td>Drives and IDs registered to the Microsoft account. Selecting a drive also fills the Drive ID field.</td>
</tr>
<tr>
<td>Drive Account Type</td>
<td>Type of Microsoft account. Logging in to a Microsoft account automatically chooses the correct account type. Options: Personal, Business, Document_Library</td>
</tr>
<tr>
<td>Drive ID</td>
<td>Unique drive identifier. Log in to a Microsoft account and choose a drive from the Drives List dropdown to add a valid ID.</td>
</tr>
</tbody>
</table>

**OpenStack Swift**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Openstack user name for login. This is the OS_USERNAME from an credentials file.</td>
</tr>
<tr>
<td>API Key or Password</td>
<td>Openstack API key or password. This is the OS_PASSWORD from an credentials file.</td>
</tr>
<tr>
<td>Authentication URL</td>
<td>Authentication URL for the server. This is the OS_AUTH_URL from an credentials file.</td>
</tr>
<tr>
<td>Auth Version</td>
<td>AuthVersion - optional - set to (1,2,3) if your auth URL has no version (rclone documentation).</td>
</tr>
<tr>
<td>Authentication Advanced Options</td>
<td>This is the OS_TENANT_NAME from an OpenStack credentials file.</td>
</tr>
<tr>
<td>Tenant ID</td>
<td>Tenant ID - optional for v1 auth, this or tenant required otherwise (rclone documentation).</td>
</tr>
<tr>
<td>Auth Token</td>
<td>Auth Token from alternate authentication - optional (rclone documentation).</td>
</tr>
</tbody>
</table>

**Advanced Options**
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region Name</td>
<td>Region name - optional (rclone documentation).</td>
</tr>
<tr>
<td>Storage URL</td>
<td>Storage URL - optional (rclone documentation).</td>
</tr>
<tr>
<td>Endpoint Type</td>
<td>Endpoint type to choose from the service catalogue. Public is recommended, see the rclone documentation.</td>
</tr>
</tbody>
</table>

- **pCloud**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Token</td>
<td>pCloud Access Token. These tokens can expire and require extension.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Enter the hostname to connect to.</td>
</tr>
</tbody>
</table>

- **SFTP**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>SSH Host to connect to.</td>
</tr>
<tr>
<td>Port</td>
<td>SSH port number. Leave empty to use the default port 22.</td>
</tr>
<tr>
<td>Username</td>
<td>SSH Username.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the SSH Username account.</td>
</tr>
<tr>
<td>Private Key ID</td>
<td>Import the private key from an existing SSH keypair or select Generate New to create a new SSH key for this credential.</td>
</tr>
</tbody>
</table>

- **WebDav**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>URL of the HTTP host to connect to.</td>
</tr>
<tr>
<td>WebDav Service</td>
<td>Name of the WebDAV site, service, or software being used.</td>
</tr>
<tr>
<td>Username</td>
<td>WebDAV account username.</td>
</tr>
<tr>
<td>Password</td>
<td>WebDAV account password.</td>
</tr>
</tbody>
</table>

- **Yandex**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Token</td>
<td>Yandex Access Token.</td>
</tr>
</tbody>
</table>

Enter the required Authentication strings to enable saving the credential.

**Automatic Authentication**

Some providers can automatically populate the required Authentication strings by logging in to the account. To automatically configure the credential, click **Login to Provider** and entering your account username and password.
It is recommended to verify the credential before saving it.
Secure Socket Shell (SSH) is a network protocol that provides a secure method to access and transfer files between two hosts while using an unsecure network. SSH can use user account credentials to establish secure connections, but often uses key pairs shared between host systems for authentication.

Creating an SSH Keypair

TrueNAS generates and stores RSA-encrypted SSH public and private keypairs in System > SSH Keypairs. These are generally used when configuring SSH Connections or SFTP Cloud Credentials. Encrypted keypairs or keypairs with passphrases are not supported.

Keypairs are automatically generated as needed when creating new SSH Connections or Replication tasks. To manually generate a new keypair, go to System > SSH Keypairs, click ADD, and give the keypair a unique Name.

Clicking the button to generate a keypair adds values to the public and private key fields. Copy these strings or download them into text files for later use.

SSH Connections

Semi-Automatic

TrueNAS offers a semi-automatic setup mode that simplifies setting up an SSH connection with another FreeNAS or TrueNAS system without having to log in to that system to transfer SSH keys. This requires an SSH keypair on the local system and administrator account credentials for the remote TrueNAS. The remote system must also be configured to allow root access with SSH. The keypair can be generated as part of the semiautomatic configuration or manually created in System > SSH Keypairs.

Go to System > SSH Connections and click ADD.
Name and Method

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of this SSH connection. SSH connection names must be unique.</td>
</tr>
</tbody>
</table>

Setup Method
- **Manual** requires configuring authentication on the remote system. This can include copying SSH keys and modifying the root user account on that system.
- **Semi-automatic** only works when configuring an SSH connection with a remote TrueNAS system. This method uses the URL and login credentials of the remote system to connect and exchange SSH keys.

Authentication

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrueNAS URL</td>
<td>Hostname or IP address of the remote system. A valid URL scheme is required. Example: <a href="https://10.231.3.76">https://10.231.3.76</a></td>
</tr>
<tr>
<td>Username</td>
<td>Username for logging in to the remote system.</td>
</tr>
<tr>
<td>Password</td>
<td>User account password for logging into the remote system.</td>
</tr>
<tr>
<td>Private Key</td>
<td>Choose a saved SSH Keypair or select Generate New to create a new keypair and use it for this connection.</td>
</tr>
</tbody>
</table>

More Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cipher</td>
<td><strong>Standard</strong> is most secure, but has the greatest impact on connection speed.</td>
</tr>
<tr>
<td></td>
<td><strong>Fast</strong> is less secure than Standard but can give reasonable transfer rates for devices with limited cryptographic speed.</td>
</tr>
<tr>
<td></td>
<td><strong>Disabled</strong> removes all security in favor of maximizing connection speed. Disabling the security should only be used within a secure, trusted network.</td>
</tr>
<tr>
<td>Connect Timeout</td>
<td>Time (in seconds) before the system stops attempting to establish a connection with the remote system.</td>
</tr>
</tbody>
</table>
Be sure to use a valid URL scheme for the remote TrueNAS URL. Leave the username as root and enter the account password for the remote TrueNAS system. The private key can be imported from a previously created SSH keypair or created with a new SSH keypair.

Saving the new configuration automatically opens a connection to the remote TrueNAS and exchanges SSH keys.

- Manual

Choosing to manually set up the SSH connection requires copying a public encryption key from the local to remote system. This allows a secure connection without a password prompt.

**Adding a Public SSH Key to the TrueNAS Root Account**

Log in to the TrueNAS system that generated the SSH keypair and go to System > SSH Keypairs. Open the keypair to use for the SSH connection and copy the text of the public SSH key or download the public key as a text file.

Log in to the TrueNAS system that needs to register the public key and go to Accounts > Users. Edit the root account. Paste the SSH public key text into the SSH Public Key field.
Start by generating a new SSH keypair in **System > SSH Keypairs**. Copy or download the value for the public key. The public key needs to be added to the remote NAS. When the remote NAS is not a TrueNAS system, please see the documentation for that system for instructions on adding a public SSH key.

**Manually Configuring the SSH Connection on the Local TrueNAS**

Log back in to the local TrueNAS system and go to **System > SSH Connections** and add a new connection. Change the setup method over to **Manual**.
Name and Method

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of this SSH connection. SSH connection names must be unique.</td>
</tr>
<tr>
<td>Manual</td>
<td>Requires configuring authentication on the remote system. This can include copying SSH keys and modifying the root user account on that system.</td>
</tr>
<tr>
<td>Semi-automatic</td>
<td>Only works when configuring an SSH connection with a remote TrueNAS system. This method uses the URL and login credentials of the remote system to connect and exchange SSH keys.</td>
</tr>
</tbody>
</table>

Authentication

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Hostname or IP address of the remote system. A valid URL scheme is required. Example: <a href="https://10.231.3.76">https://10.231.3.76</a></td>
</tr>
<tr>
<td>Port</td>
<td>Port number on the remote system to use for the SSH connection.</td>
</tr>
<tr>
<td>Username</td>
<td>Username for logging in to the remote system.</td>
</tr>
<tr>
<td>Private Key</td>
<td>Choose a saved SSH Keypair or select Generate New to create a new keypair and use it for this connection.</td>
</tr>
<tr>
<td>Remote Host Key</td>
<td>Remote system SSH key for this system to authenticate the connection. When all other fields are properly configured, click DISCOVER REMOTE HOST KEY to query the remote system and automatically populate this field.</td>
</tr>
</tbody>
</table>

Discover Remote Host Key connects to the remote host and attempts to copy the key string to the related TrueNAS field.

More Options

<p>| Name | Description |</p>
<table>
<thead>
<tr>
<th>Cipher</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard</strong></td>
<td>is most secure, but has the greatest impact on connection speed.</td>
</tr>
<tr>
<td><strong>Fast</strong></td>
<td>is less secure than Standard but can give reasonable transfer rates for devices with limited cryptographic speed.</td>
</tr>
<tr>
<td><strong>Disabled</strong></td>
<td>removes all security in favor of maximizing connection speed. Disabling the security should only be used within a secure, trusted network.</td>
</tr>
</tbody>
</table>

| Connect Timeout | Time (in seconds) before the system stops attempting to establish a connection with the remote system. |

Make sure to select the private key from the SSH keypair that was used to transfer the public key on the remote NAS.
3.12 - Tunables

TrueNAS allows you to add system tunables from the web interface. These can be manually defined or TrueNAS can run an autotuning script to attempt to optimize the system. Tunables are used to manage TrueNAS sysctls, loaders, and rc.conf options.

- **loader**: specifies parameters to pass to the kernel or load additional modules at boot time.
- **rc.conf**: enables system services and daemons and only take effect after a reboot.
- **sysctl**: configures kernel parameters while the system is running and generally take effect immediately.

Adding a sysctl, loader, or rc.conf option is an advanced feature. A sysctl immediately affects the kernel running the TrueNAS system and a loader could adversely affect the ability of the TrueNAS system to successfully boot. Do not create a tunable on a production system before testing the ramifications of that change.

Configuring System Tunables

To configure a tunable, go to **System > Tunables** and click **ADD**.

First, select the **Type** of tunable to add or modify. Enter the name of the **loader**, **sysctl**, or **rc.conf** variable to configure.

Next, enter the value to use for the **loader**, **sysctl**, or **rc.conf**. An optional description can be given.

If you wish to create the system tunable but not immediately enable it, unset the **Enable** checkbox. Configured tunables remain in effect until deleted or **Enabled** is unset.

Restarting the TrueNAS system after making sysctl changes is recommended. Some sysctls only take effect at system startup, and restarting the system guarantees that the setting values correspond with what is being used by the running system.

Be careful when adding or editing the default tunables. Changing the default tunables can make the system unusable.

**UI Field Reference**

<table>
<thead>
<tr>
<th>Tunable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the loader, sysctl, or rc.conf variable to configure. Loader tunables are used to</td>
</tr>
</tbody>
</table>
Variable: Specify parameters to pass to the kernel or load additional modules at boot time. `rc.conf` tunables are for enabling system services and daemons and only take effect after a reboot. `sysctl` tunables are used to configure kernel parameters while the system is running and generally take effect immediately.

<table>
<thead>
<tr>
<th><strong>Variable</strong></th>
<th><strong>Value</strong></th>
<th><strong>Type</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a value to use for the <a href="#">loader</a>, <a href="#">sysctl</a>, or <a href="#">rc.conf</a> variable.</td>
<td>Creating or editing a <code>sysctl</code> immediately updates the Variable to the configured Value. A restart is required to apply loader or <code>rc.conf</code> tunables. Configured tunables remain in effect until deleted or <code>Enabled</code> is unset.</td>
<td>Enter a description of the tunable.</td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
<td>Enable this tunable. Unset to disable this tunable without deleting it.</td>
<td></td>
</tr>
</tbody>
</table>
3.13 - Update

- Preparing Systems for Updates and Upgrades
- Update and Upgrade Instructions

Preparing Systems for Updates and Upgrades

Preparation and precautions for a system upgrade, or update, vary. CORE Updates, ENTERPRISE (HA) Updates, and Major Version Upgrades each have several specific things that should be addressed before you proceed.

 Preconditions for CORE Update

TrueNAS CORE

TrueNAS CORE has an integrated update system to make it easy to keep up to date.

Preparation

It is best to perform updates at times the TrueNAS system is idle, with no clients connected and no scrubs or other disk activity happening. Most updates require a system reboot. Plan updates around scheduled maintenance times to avoid disrupting user activities.

The update process does not proceed unless there is enough free space in the boot pool for the new update files. If a space warning is shown, go to System > Boot to remove unneeded boot environments.

Updates and Trains

Cryptographically signed update files are used to update TrueNAS. Update files provide flexibility in deciding when to upgrade the system. Updates are installed in a new Boot Environment, giving you the opportunity to install and test an update, but revert to a previous Boot Environment in System > Boot if anything goes wrong.

TrueNAS defines software branches, known as trains. There are several trains available for updates, but the web interface only displays trains that can be selected as an upgrade.

Update trains are labeled with a numeric version followed by a short description. The current version receives regular bug fixes and new features. Supported older versions of TrueNAS only receive maintenance updates. See the Software Development Life Cycle for more details about the development and support timeline for TrueNAS versions.

Several specific words are used to describe the type of train:

**STABLE**: Bug fixes and new features are available from this train. Upgrades available from a STABLE train are tested and ready to apply to a production environment.

**Nightlies**: Experimental train used for testing future versions of TrueNAS.

**SDK**: Software Developer Kit train. This has additional tools for testing and debugging TrueNAS.

The UI shows a warning when the currently selected train is not suited for production use. Before using a non-production train, be prepared to experience bugs or problems. Testers are encouraged to submit bug reports at the provided URL.

Preparing for ENTERPRISE (HA) Update

TrueNAS Enterprise (HA)
Updating a TrueNAS Enterprise system that is configured for High Availability (HA) has a slightly different flow from non-HA systems or TrueNAS Core. The system downloads the update to both controllers, updates and reboots the standby TrueNAS controller, and finally fails over from and updates the active TrueNAS controller.

**Preparation**

An update usually takes between thirty minutes and an hour. A reboot is required after the update, so it is recommended to schedule updates during a maintenance window, allowing two to three hours to update, test, and possibly roll back if issues appear. On very large systems, a proportionally longer maintenance window is recommended.

For individual support during an upgrade, please contact iXsystems Support to schedule your upgrade.

### Contacting iXsystems Support

Customers who purchase iXsystems hardware or that want additional support must have a support contract to use iXsystems Support Services. The [TrueNAS Community forums](https://support.ixsystems.com) provides free support for users without an iXsystems Support contract.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td><a href="https://support.ixsystems.com">https://support.ixsystems.com</a></td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:support@ixsystems.com">support@ixsystems.com</a></td>
</tr>
</tbody>
</table>
| Telephone      | Monday - Friday, 6:00AM to 6:00PM Pacific Standard Time:  
US-only toll-free: 1-855-473-7449 option 2  
Local and international: 1-408-943-4100 option 2 |
| Telephone      | After Hours (24x7 Gold Level Support only):  
US-only toll-free: 1-855-499-5131  
International: 1-408-878-3140 (international calling rates apply) |

Scheduling at least two days in advance of a planned upgrade gives time to make sure a specialist is available for assistance. Updating from earlier than version 9.3 of TrueNAS must be scheduled with iXsystems Support.

The update process will not proceed unless there is enough free space in the boot pool for the new update files. If a space warning is shown, go to **System > Boot** and remove any unneeded boot environments.

Operating system updates only modify the operating system devices and do not affect end-user data on storage drives.

An update could involve upgrading the version of ZFS that is installed on the storage drives. When a ZFS version upgrade is available, an **notifications Alert** appears in the web interface. Upgrading the ZFS version on storage drives is not recommended until it has been verified that rolling back to previous versions of the operating system is not necessary and that swapping the storage drives with another system that has an earlier ZFS version is not needed. After a ZFS version upgrade, the storage devices will not be accessible by earlier TrueNAS versions.

### Preparing for Major System Upgrades

#### Major Version Upgrades

TrueNAS provides flexibility for keeping the operating system up-to-date:
1. Upgrades to major releases, for example from version 9.3 to 9.10, can still be performed using either an ISO or the web interface. Unless the Release Notes for the new major release indicate that the current version requires an ISO upgrade, either upgrade method can be used.

2. Minor releases have been replaced with signed updates. This means that it is not necessary to wait for a minor release to update the system with a system update or newer versions of drivers and features. It is also no longer necessary to manually download an upgrade file and its associated checksum to update the system.

3. The updater automatically creates a boot environment, making updates a low-risk operation. Boot environments provide the option to return to the previous version of the operating system by rebooting the system and selecting the previous boot environment from the System > Boot menu.

The upgrade instructions describe how to use an .iso file to perform a major version upgrade from an earlier version of FreeNAS/TrueNAS. See the Updating article for instructions about using the web interface to keep the system updated.

The upgrade path for major versions of FreeNAS/TrueNAS is \textbf{9.3 > 9.10 > 11.1 > 11.3 > 12.0}. It is always recommended to upgrade to a supported version of the software.

\section*{Caveats}

Be aware of these caveats before attempting a major version upgrade:

\textbf{Upgrading a data storage pool can make it impossible to go back to a previous version.} For this reason, the update process does not automatically upgrade storage pools, though the system shows an alert when a pool can be upgraded. Unless new ZFS feature flags are needed, it is safe to leave the pool at the current version. If the pool is upgraded, it isn’t possible to boot into a previous TrueNAS version that does not support the newer feature flags.

We recommend upgrading Broadcom SAS HBAs to the latest version.

\textbf{When upgrading from 9.3.x to 9.10}, read this [changes FAQ](https://www.truenas.com/docs/files/Notice-9.3 to 9.10 FAQ.pdf) first.

\textbf{TrueNAS does not support upgrades from FreeNAS 0.7x.} The system has no way to import configuration settings from FreeNAS 0.7x versions. The configuration must be manually recreated. If supported, the FreeNAS 0.7x pools or disks must be manually imported.

\textbf{TrueNAS does not support upgrades on 32-bit hardware.} However, if the system is currently running a 32-bit version of FreeNAS/TrueNAS and the hardware supports 64-bit, the system can be upgraded. Any archived reporting graphs will be lost during the upgrade.

\textbf{TrueNAS does not support UFS.} If the data currently resides on one UFS-formatted disk, create a ZFS pool using other disks after the upgrade, then use the instructions in Importing a Disk to mount the UFS-formatted disk and copy the data to the ZFS pool. With only one disk, back up its data to another system or media before the upgrade, format the disk as ZFS after the upgrade, then restore the backup. If the data currently resides on a UFS RAID of disks, it is not possible to directly import that data to the ZFS pool. Instead, back up the data before the upgrade, create a ZFS pool after the upgrade, then restore the data from the backup.

\textbf{TrueNAS 12.0 or newer does not support GELI-encrypted pools.} If you have GELI-encrypted pools and are upgrading to TrueNAS 12.0 or newer, you might want to migrate data out of the GELI-encrypted pools into ZFS-encrypted pools. The GELI pools cannot be converted; the data must be migrated to a new ZFS pool. See the Encryption article for more details.

\section*{Preparation}

Before upgrading the operating system, follow these steps:

1. Back up the TrueNAS configuration in System > General > Save Config.
2. Back up any or have the keys or passphrases for encrypted data available.
3. Warn users that TrueNAS shared data will be unavailable during the upgrade. It is recommended to schedule the upgrade for a time that will least impact users.
4. Stop all system Services.

Update and Upgrade Instructions

 Updating CORE

Checking for Updates

The system checks daily for updates and downloads an update if one is available. An alert is issued when a new update becomes available. The automatic check and download of updates is disabled by unsetting Check for Updates Daily and Download if Available. Click ◀ (Refresh) to perform another check for updates. To change the train, use the drop-down menu to make a different selection.

The train selector does not allow downgrades. For example, the STABLE train cannot be selected while booted into a Nightly boot environment, or a 9.10 train cannot be selected while booted into a 11 boot environment. To go back to an earlier version after testing or running a more recent version, reboot and select a boot environment for that earlier version. This screen can then be used to check for updates that train.

Information about the update is displayed along with a link to the release notes. It is important to read the release notes before updating to determine if any of the changes in that release impact the use of the system.

Saving the Configuration File

A dialog to save the system configuration file appears before installing updates.
Save configuration settings from this machine before updating?

**WARNING**: This configuration file contains system passwords and other sensitive data.

Include Password Secret Seed

Including the Password Secret Seed allows using this configuration file with a new boot device. It also decrypts all passwords used on this system. **Keep the configuration file safe and protect it from unauthorized access!**

[NO] [SAVE CONFIGURATION]

Keep the system configuration file secure after saving it. The security information in the configuration file could be used for unauthorized access to your TrueNAS system.

**Applying Updates**

Make sure the system is in a low-usage state as described above in *Preparing for Updates*. Click **DOWNLOAD UPDATES** to immediately download and install an update.

The **Save Configuration** dialog appears so the current configuration can be saved to external media.

A confirmation window appears before the update is installed. When **Apply updates and reboot system after downloading** is set, clicking **CONTINUE** downloads and applies the update, then reboots the system. The update can be downloaded for a later manual installation by unsetting **Apply updates and reboot system after downloading**.

**APPLY PENDING UPDATE** is visible when an update is downloaded and ready to install. Click this button to see a confirmation window. Setting **Confirm** and clicking **CONTINUE** installs the update and reboots the system.

Each update creates a boot environment. If the update process needs more space, it attempts to remove old boot environments. Boot environments marked with the **Keep** attribute as shown in **System > Boot** are not removed. If space for a new boot environment is not available, the upgrade fails. Space on the operating system device can be manually freed by going to **System > Boot** and removing the **Keep** attribute or deleting any boot environments that are no longer needed.

**Can I force a full update? expand □**

The TrueNAS updater defaults to delta packages for updates. During an update, only files that changed in the base operating system since the previous update are downloaded. Delta update packages are generally preferred over full update packages, providing a faster update and taking less bandwidth. By contrast, a full update package downloads all of the files included in the base system, even if those files have not changed.

While the full package might require more time to install, there are some rare cases where it is necessary, such as when a patch has been applied as a temporary fix to a local system. A patch is a piece of software that is used to fix...
a bug within the main codebase. While software patches are often used to fix bugs, they can also repair security issues or add new features.

To force a full update, open the web interface and enter this command in the console:

```
freenas-update -C /tmp/update-$$ -no-delta -reboot update
```

The updater downloads the full package, which contains all of the files from the latest software release. When the download completes, the system reboots with the standard configuration.

---

**Manual Updates**

Updates can also be manually downloaded and applied in **System > Update**.

**Manual updates cannot be used to upgrade from older major versions.**


Download the desired update file to your local system. Log in to the TrueNAS web interface and go to **System > Update**. Click **INSTALL MANUAL UPDATE FILE**.

The **Save Configuration** dialog opens. This makes it possible to save a copy of the current configuration to external media for backup in case of an update problem.

After the dialog closes, the manual update screen is shown. The current version of TrueNAS is shown for verification.

Select the manual update file that was saved to your local system using **Browse**. Set **Reboot After Update** to reboot the system after the update has been installed. Click **APPLY UPDATE** to begin the update.

---

**Update in Progress**

Starting an update shows a progress dialog. When an update is in progress, the web interface shows an animated `system_update_alt` icon in the top row. Dialogs also appear in every active web interface session to warn that a system update is in progress. **Do not** interrupt a system update.

- Updating ENTERPRISE (HA)

**Starting the Update**

In the web interface **Dashboard**, find the entry for the active TrueNAS controller and click **CHECK FOR UPDATES**. This button changes to **UPDATES AVAILABLE** when there is an available update.
Clicking the button goes to **System > Update** and shows the option to **Download Updates** or, when the system has already detected and staged an update, **Apply Pending Update**.

When **Download Updates** or **Apply Pending Update** is clicked, it first gives an opportunity to save the current system configuration. Backing up the system configuration is strongly recommended before starting the update. Including the **Password Secret Seed** in the system configuration removes the encryption from sensitive system data, like stored passwords. When enabling this option, take extra precautions to store the downloaded system configuration file in a secure location.

After downloading the system configuration, you can continue to download and/or apply the system update. This will start the process to update and reboot the TrueNAS controllers. HA and other system services will be briefly unavailable.

Other users that are logged in to the web interface will see a warning dialog. A **System Updating** icon is shown in the top bar of the web interface while the update is in progress.

Update progress is shown for both TrueNAS controllers. The standby TrueNAS controller reboots when it is finished updating. This can take several minutes. When the standby controller has finished booting, the system must fail over to update and reboot the active TrueNAS controller.

**Fail Over to Complete the Update**

To deactivate the active TrueNAS controller and finish the update, go to the **Dashboard**, find the entry for the **Standby** controller, and click **INITIATE FAILOVER**.
Initiating the failover briefly interrupts TrueNAS services and availability. The browser logs out of the web interface while the active TrueNAS controller deactivates and the standby TrueNAS controller is brought online. The web interface login screen reappears when the standby TrueNAS controller finishes activating.
Log in to the web interface and check the cloud HA status in the top toolbar. This icon shows that HA is unavailable while the previously active TrueNAS controller reboots. When HA is available, a dialog asks to finish the update. Click CONTINUE to finish updating the previously active TrueNAS controller.

Verify that the update is complete by going to the Dashboard and confirming that the Version is the same on both TrueNAS controllers.

**Reverting an Update expand □**

If the update did not install on one of the controllers, the web interface generates an alert about a mismatch between controller versions.

If something else goes wrong with the update, the system generates an alert and writes details to /data/update.failed.

You can return the system to its pre-update state by activating a previous boot environment during system boot. To ensure the versions match, do this procedure for both TrueNAS controllers. This requires physical or IPMI access to the TrueNAS controller console.
Reboot the system and press the space bar when the boot menu appears, pausing the boot process.

Open the **Boot Environments** menu and cycle the **Active** boot environment until one that is dated prior to the update is selected.

Return to the first screen and press **Enter** to boot into the version of TrueNAS that was installed on that date.

**Manually Updating an Enterprise HA System**

Enterprise customers should contact iX Support for assistance updating their TrueNAS system.

- Download the manual update file located at the [TrueNAS/FreeNAS Download Page](#).
- Go to **System -> Update**.
- Click the **INSTALL MANUAL UPDATE** button.
- Set the **Include Password Secret Seed** checkbox and click the **Save Configuration** button.
Select the Update File Temporary Storage Location, click the Choose File button. Select the manual upgrade file that was downloaded. Wait for the file to upload and then click the APPLY UPDATE button. The Manual update will upload the file, install the file to both controllers, and then reboot the Standby Controller. To complete the upgrade process click the Close button in the dialog box. Initiate a failover of the standby controller, as instructed, by clicking INITIATE FAILOVER from the Standby Controller’s Dashboard card.

- Log into the system.
- Click the Continue button at the Pending Upgrade dialog box and the standby controller will reboot completing the upgrade.

○ Major Version Upgrades

ISO Upgrades

To upgrade TrueNAS using an .iso file, go to https://www.truenas.com/download-truenas-core/ (TrueNAS CORE latest release) or https://download.freenas.org to download the .iso to the computer that will be used to prepare the installation media. For example, this is the path to download an .iso of the latest FreeNAS 11.3 release:

```
<table>
<thead>
<tr>
<th>File</th>
<th>Date</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>FreeNAS-11.3-U4.1.debug.txz</td>
<td>28-Jul-2020 17:31</td>
<td>633545937</td>
</tr>
<tr>
<td>FreeNAS-11.3-U4.1.debug.txz.sha256</td>
<td>28-Jul-2020 17:31</td>
<td>137</td>
</tr>
<tr>
<td>FreeNAS-11.3-U4.1.iso</td>
<td>28-Jul-2020 17:35</td>
<td>788678856</td>
</tr>
<tr>
<td>FreeNAS-11.3-U4.1.iso.sha256</td>
<td>29-Jul-2020 13:59</td>
<td>566</td>
</tr>
<tr>
<td>FreeNAS-11.3-U4.1.iso.png</td>
<td>28-Jul-2020 17:35</td>
<td>151</td>
</tr>
</tbody>
</table>
```

Burn the downloaded .iso file to a CD or USB stick. Refer to the Prepare the Install File instructions in the Installation article for tips about burning the .iso to media using different Operating Systems.

Insert the prepared media into the system and boot from it. The installer waits ten seconds in the installer boot menu before booting the default option. If needed, press Spacebar to stop the timer and choose another boot option. After the media finishes booting into the installation menu, press Enter to select the default option 1 Install/Upgrade. The installer presents a screen showing all available drives.

All drives are shown, including boot drives and storage drives. Only choose boot drives when upgrading. **Choosing the wrong drives to upgrade or install will cause loss of data.** If unsure about which drives contain the TrueNAS operating system, reboot and remove the install media. Log in to the TrueNAS web interface and go to System > Boot > ACTIONS > Boot Pool Status to identify the boot drives. More than one drive is shown when a mirror has been used.

Highlight the drive where TrueNAS is installed and press Spacebar to mark it with a star. If a mirror has been used for the operating system, mark all of the drives where the TrueNAS operating system is installed. Press Enter when done.

The installer recognizes earlier versions of FreeNAS/TrueNAS installed on the boot drives and asks to either upgrade or do a fresh install:
To perform an upgrade, press Enter to accept the default Upgrade Install. The installer will display another reminder that the operating system should be installed on a disk that is not used for storage.

The updated system can be installed in a new boot environment, or the entire operating system device can be formatted to start fresh. Installing into a new boot environment preserves the old code, allowing a roll-back to previous versions if necessary. Formatting the boot device is usually not necessary but can reclaim space. User data and settings are preserved when installing to a new boot environment and also when formatting the operating system device. Move the highlight to one of the options and press Enter to start the upgrade.

The installer unpacks the new image and checks for upgrades to the existing database file. The database file that is preserved and migrated contains your TrueNAS configuration settings.
Press Enter. TrueNAS indicates that the upgrade is complete and a reboot is required. Press OK, highlight 3 Reboot System, then press Enter to reboot the system. If the upgrade installer was booted from CD, remove the CD.

During the reboot there can be a conversion of the previous configuration database to the new version of the database. This happens during the Applying database schema changes line in the reboot cycle. This conversion can take a long time to finish, sometimes fifteen minutes or more, and can cause the system to reboot again. The system will start normally afterwards. If database errors are shown but the web interface is accessible, log in, go to System > General, and use the UPLOAD CONFIG button to upload the configuration backup that was downloaded before starting the upgrade.
3.14 - CAs

TrueNAS can act as a Certificate Authority (CA). When encrypting SSL or TLS connections to the TrueNAS system, you can either import an existing CA, or create a CA and certificate on the TrueNAS system. This certificate will appear in the drop-down menus for services that support SSL or TLS. To add or import a CA, go to System > CAs and click ADD. Enter the name for the CA, then choose the Type. The three type options are Internal CA, Intermediate CA, and Import CA. The process for each type is slightly different. Use the tabs below to jump to the appropriate section based on your desired type.

**Internal CA**

**Identifier and Type**

Select Internal CA as the Type.

If you want, you can select a profile for the CA. Selecting a profile automatically sets certain options such as Key Type, Key Length, Digest Algorithm, and more. If you would like to set each option manually, do not select a profile from the Profiles dropdown.

**Certificate Options**

1. Select a Key Type from the dropdown. We recommend the RSA key type.
2. Select the Key Length. We recommend a minimum of 2048 for security reasons.
3. Select a Digest Algorithm. We recommend SHA256.
4. Enter the Lifetime of the CA in days to set how long the CA will remain valid.
Certificate Subject

1. Fill out the geographic information of the certificate by entering the Country, Locality, Organizational Unit (optional), Common Name, State, Organization, Email, and Subject Alternate Names.
2. The Common Name is the fully-qualified hostname (FQDN) and must be unique within a certificate chain.

Basic Constraints

1. If you would like to have Basic Constraints, set them to Enabled and more options will appear.
2. Set a Path Length to determine how many non-self-issued intermediate certificates can follow this certificate in a valid certification path. Entering 0 allows a single additional certificate to follow in the certificate path.
3. Select the Basic Constraints Config. You can select more than one from the dropdown.
Authority Key Identifier

If you want an Authority Key Identifier, set it to Enabled, then select the Authority Key Config. You can select more than one from the dropdown.

Key Usage

Extended Key Usage is typically used for end entity certificates.

1. If you want to utilize Extended Key Usage, set it to Enabled, then select the usage for the public key from the Usages dropdown. You can select multiple usages in the dropdown.
2. Enable Critical Extension if you want to identify this extension as critical for the certificate. Do not enable Critical Extension if Usages contains ANY_EXTENDED_KEY_USAGE.

Using both Extended Key Usage and Key Usage extensions requires that the purpose of the certificate is consistent with both extensions. See RFC 3280, section 4.2.1.13 for more details.

Intermediate CA

Identifier and Type
Select *Intermediate CA* as the *Type*.

If you want, you can select a profile for the CA. Selecting a profile automatically sets certain options such as *Key Type*, *Key Length*, *Digest Algorithm*, and more. If you would like to set each option manually, do not select a profile from the *Profiles* dropdown.

**Certificate Options**

1. Select a *Signing Certificate Authority* from the dropdown.
2. Select a *Key Type* from the dropdown. We recommend the *RSA* key type.
3. Select the *Key Length*. We recommend a minimum of 2048 for security reasons.
4. Select a *Digest Algorithm*. We recommend *SHA256*.
5. Enter the *Lifetime* of the CA in days to set how long the CA will remain valid.
Certificate Subject

1. Fill out the geographic information of the certificate by entering the Country, Locality, Organizational Unit (optional), Common Name, State, Organization, Email, and Subject Alternate Names.
2. The Common Name is the fully-qualified hostname (FQDN) and must be unique within a certificate chain.

Basic Constraints

1. If you would like to have Basic Constraints, set them to Enabled and more options will appear.
2. Set a Path Length to determine how many non-self-issued intermediate certificates can follow this certificate in a valid certification path. Entering 0 allows a single additional certificate to follow in the certificate path.
3. Select the Basic Constraints Config. You can select more than one from the dropdown.
Authority Key Identifier

If you want an Authority Key Identifier, set it to Enabled, then select the Authority Key Config. You can select more than one from the dropdown.

Key Usage

Extended Key Usage is typically used for end entity certificates.

1. If you want to utilize Extended Key Usage, set it to Enabled, then select the usage for the public key from the Usages dropdown. You can select multiple usages in the dropdown.
2. Enable Critical Extension if you want to identify this extension as critical for the certificate. Do not enable Critical Extension if Usages contains ANY_EXTENDED_KEY_USAGE.

Using both Extended Key Usage and Key Usage extensions requires that the purpose of the certificate is consistent with both extensions. See RFC 3280, section 4.2.1.13 for more details.

Import CA

Identifier and Type
Select *Import a CA* as the *Type*.

**Certificate Subject**

1. Copy the certificate for the CA you want to import and paste it in the *Certificate* field.
2. Paste the *Private Key* associated with the Certificate when available. Provide a key at least 1024 bits long.
3. Enter and confirm the *Passphrase* for the Private Key.
3.15 - Certificates

By default, TrueNAS comes equipped with an internal, self-signed certificate that enables encrypted access to the web interface. You can either import or create a Certificate or Signing Request by navigating to **System > Certificates** and clicking **ADD**. Enter the name for the certificate, then choose the **Type**. The four options are **Internal Certificate**, **Certificate Signing Request** (CSR), **Import Certificate**, and **Import Certificate Signing Request**. The process for each type is slightly different. Use the tabs below to jump to the appropriate section based on your desired type.

**Internal**

**Identifier and Type**

Select **Internal Certificate** as the **Type**.

If you want, you can select a profile for the CA. Selecting a profile automatically sets certain options such as **Key Type**, **Key Length**, **Digest Algorithm**, and more. If you would like to set each option manually, do not select a profile from the **Profiles** dropdown.

**Certificate Options**

1. Select a **Signing Certificate Authority** from the dropdown.
2. Select a **Key Type** from the dropdown. We recommend the **RSA** key type.
3. Select the **Key Length**. We recommend a minimum of **2048** for security reasons.
4. Select a **Digest Algorithm**. We recommend **SHA256**.
5. Enter the **Lifetime** of the CA in days to set how long the CA will remain valid.
Certificate Subject

1. Fill out the geographic information of the certificate by entering the Country, Locality, Organizational Unit (optional), Common Name, State, Organization, Email, and Subject Alternate Names.
2. The Common Name is the fully-qualified hostname (FQDN) and must be unique within a certificate chain.
Basic Constraints

1. If you would like to have **Basic Constraints**, set them to **Enabled** and more options will appear.
2. Set a **Path Length** to determine how many non-self-issued intermediate certificates can follow this certificate in a valid certification path. Entering 0 allows a single additional certificate to follow in the certificate path.
3. Select the **Basic Constraints Config**. You can select more than one from the dropdown.

Authority Key Identifier

If you want an **Authority Key Identifier**, set it to **Enabled**, then select the **Authority Key Config**. You can select
more than one from the dropdown.

---

**Key Usage**

Extended Key Usage is typically used for end entity certificates.

1. If you want to utilize *Extended Key Usage*, set it to *Enabled*, then select the usage for the public key from the *Usages* dropdown. You can select multiple usages in the dropdown.  
2. Enable *Critical Extension* if you want to identify this extension as critical for the certificate. Do not enable *Critical Extension* if *Usages* contains *ANY_EXTENDED_KEY_USAGE*.

Using both *Extended Key Usage* and *Key Usage* extensions requires that the purpose of the certificate is consistent with both extensions. See RFC 3280, section 4.2.1.13 for more details.

---

**Certificate Signing Request**

**Identifier and Type**

1. Select *Certificate Signing Request* as the *Type*.  
2. If you want, you can select a profile for the CA. Selecting a profile automatically sets certain options such as *Key Type*, *Key Length*, and *Digest Algorithm*. If you would like to set options manually, do not select a profile from the *Profiles* dropdown.
Certificate Options

1. Select a Key Type from the dropdown. We recommend the RSA key type.
2. Select a Digest Algorithm. We recommend SHA256.

Certificate Subject

Fill out the geographic information of the certificate by entering the Country, Locality, Organizational Unit (optional), Common Name, State, Organization, Email, and Subject Alternate Names. The Common Name is the fully-qualified hostname (FQDN) and must be unique within a certificate chain.
Basic Constraints

1. If you would like to have Basic Constraints, set them to Enabled and more options will appear.
2. Set a Path Length to determine how many non-self-issued intermediate certificates can follow this certificate in a valid certification path. Entering 0 allows a single additional certificate to follow in the certificate path.
3. Select the Basic Constraints Config. You can select more than one from the dropdown.

Authority Key Identifier

If you want an Authority Key Identifier, set it to Enabled, then select the Authority Key Config. You can select more than one from the dropdown.

Key Usage

1. Extended Key Usage is typically used for end entity certificates. If you want to utilize Extended Key Usage, set it to Enabled, then select the usage for the public key from the Usages dropdown. You can select multiple usages in the dropdown.
2. Do not set the Critical Extension when the Usages contains \texttt{ANY\_EXTENDED\_KEY\_USAGE}.

Using both \textit{Extended Key Usage} and \textit{Key Usage} extensions requires that the purpose of the certificate is consistent with both extensions. See RFC 3280, section 4.2.1.13 for more details.

- Import Certificate

\textbf{Identifier and Type}

Select \textit{Import Certificate} as the Type.

\textbf{Certificate Options}

If you want to import a CSR that is already on the system, enable \textit{CSR exists on this system}, then select the one you want to use from the drop-down.

\textbf{Certificate Subject}

1. Copy the certificate for the CA you want to import and paste it in the Certificate field.
2. Paste the Private Key associated with the Certificate when available. Provide a key at least 1024 bits long.
3. Enter and confirm the Passphrase for the Private Key.
Import Certificate Signing Request

Import Certificate Signing Request

Identifier and Type

Select *Import Certificate* as the *Type*.

Certificate Subject

1. Copy the contents of the Certificate Signing Request you want to import and paste it in the *Signing Request* field.
2. Paste the *Private Key* associated with the Certificate when available. Provide a key at least 1024 bits long.
3. Enter and confirm the *Passphrase* for the Private Key.
3.16 - ACME DNS

- ACME DNS Authenticators
- Creating ACME Certificates

This feature is only available in the open source supported TrueNAS CORE.

**Automatic Certificate Management Environment (ACME)** is available for automating certificate issuing and renewal. The user must verify ownership of the domain before certificate automation is allowed.

An ACME DNS Authenticator is required to configure ACME certificate automation. This also requires a [Certificate Signing Request](#).

**ACME DNS Authenticators**

Go to **System > ACME DNS** and click **ADD**.

![Add DNS Authenticator](image)

Enter a name for the authenticator. This is only used to identify the authenticator in the TrueNAS web interface. Choose a DNS provider and configure any required **Authenticator Attributes**:

- **Route 53**: Amazon DNS web service. Requires entering an Amazon account **Access ID Key** and **Secret Access Key**. See the [AWS documentation](#) for more details about generating these keys.

Click **SUBMIT** to register the DNS Authenticator and add it to the list of authenticator options for ACME Certificates.

**Creating ACME Certificates**

ACME certificates can be created for existing certificate signing requests. These certificates use an ACME DNS authenticator to confirm domain ownership, then are automatically issued and renewed. To create a new ACME certificate, go to **System > Certificates**, click **□ (Options)** for an existing certificate signing request, and click **Create ACME Certificate**.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>Internal identifier of the certificate. Only alphanumeric characters, dash (-), and underline (_) are allowed.</td>
</tr>
<tr>
<td>Terms of Service</td>
<td>Please accept the terms of service for the given ACME Server.</td>
</tr>
<tr>
<td>Renew Certificate Day</td>
<td>Number of days to renew certificate before expiring.</td>
</tr>
<tr>
<td>ACME Server Directory URI</td>
<td>URI of the ACME Server Directory. Choose a preconfigured URI or enter a custom URI.</td>
</tr>
<tr>
<td>Authenticator for Domain Name (Domain Name dynamically changes)</td>
<td>Authenticator to validate the domain. Choose a previously configured ACME DNS authenticator.</td>
</tr>
</tbody>
</table>
3.17 - KMIP

KMIP is only available for TrueNAS Enterprise licensed systems. Please contact the iXsystems Sales Team to inquire about purchasing TrueNAS Enterprise licenses.

- Connecting TrueNAS to a KMIP Server
  - Configuring KMIP in TrueNAS

The Key Management Interoperability Protocol (KMIP) is an extensible client/server communication protocol for the storage and maintenance of keys, certificates, and secret objects. KMIP on TrueNAS Enterprise is used to integrate the system within an existing centralized key management infrastructure and use a single trusted source for creating, using, and destroying SED passwords and ZFS encryption keys.

Keys can be created on a single server and then retrieved by TrueNAS. Keys wrapped within keys, symmetric, and asymmetric keys are supported. Alternately, KMIP can be used for clients to ask a server to encrypt or decrypt data without the client ever having direct access to a key. KMIP also can be used to sign certificates.

Requirements expand □
You will need to have a KMIP server available with certificate authorities and certificates that can be imported into TrueNAS. Have the KMIP server configuration open in a separate browser tab or copy the KMIP server certificate string and private key string to later paste into the TrueNAS web interface. This helps simplify the TrueNAS connection process.

Connecting TrueNAS to a KMIP Server

To connect TrueNAS to a KMIP server, import a Certificate Authority (CA) and Certificate from the KMIP server, then configure the KMIP options.

How do I import these? expand □
Log in to the TrueNAS web interface and go to System > CAs and click ADD. In the Type drop down menu, select Import CA. Enter a memorable Name for the CA, then paste the KMIP server Certificate and Private Key strings into the related fields. Leave the Passphrase empty and click Submit.

Next, go to System > Certificates and click ADD. In the Type drop down menu, select Import Certificate. Enter a memorable Name for the certificate and paste the KMIP server Certificate and Private Key strings into the related TrueNAS fields. Leave the Passphrase empty and click Submit.

For security reasons, it is strongly recommended to protect the CA and Certificate values.

Configuring KMIP in TrueNAS

Go to System > KMIP to complete the configuration.
Enter the central key server **Server** host name or IP address and the number of an open connection **Port** on the key server. Select the **Certificate** and **Certificate Authority** that were just imported from the central key server. To check that the Certificate and CA chain is correct, set **Validate Connection** and click **SAVE**.

When the certificate chain is verified, choose the encryption values, SED passwords, or ZFS data pool encryption keys to move to the central key server. Set **Enabled** to begin moving the passwords and keys immediately after clicking **SAVE**.

Refreshing the **KMIP** page shows the current **KMIP Key Status**.

To cancel a pending key synchronization, set **Force Clear** and click **SAVE**.
3.18 - Failover (HA)

- Configuring High Availability (HA)
  - Networking
  - Failover

**Warning:** To avoid the potential for data loss, *iXsystems must be contacted* before replacing a controller or upgrading to High Availability.

<table>
<thead>
<tr>
<th>Process Summary expand □</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System &gt; Support</strong></td>
</tr>
<tr>
<td>Update license</td>
</tr>
<tr>
<td><strong>Network &gt; Global Configuration</strong></td>
</tr>
<tr>
<td>Set the hostnames for both TrueNAS controllers</td>
</tr>
<tr>
<td>Set a virtual hostname</td>
</tr>
<tr>
<td><strong>Network &gt; Interfaces</strong></td>
</tr>
<tr>
<td>Interfaces cannot be edited when HA is enabled</td>
</tr>
<tr>
<td>Define the failover group</td>
</tr>
<tr>
<td>Set IP addresses for the controllers</td>
</tr>
<tr>
<td>Set the virtual IP address</td>
</tr>
<tr>
<td>This IP address is used to log in to the web interface from this point forward</td>
</tr>
<tr>
<td><strong>System &gt; Failover</strong></td>
</tr>
<tr>
<td>Designate the default TrueNAS controller</td>
</tr>
<tr>
<td>Define how long to wait after a network interruption to trigger a failover</td>
</tr>
</tbody>
</table>

### Configuring High Availability (HA)

To configure HA, turn on both units in the array and log in to the web interface for one of the units. If this is the first login, the UI shows a dialog to upload the TrueNAS Enterprise License. Otherwise, go to **System > Support** and update the license.

Paste the HA license received from iXsystems and save it. The license contains the serial numbers for both units in the chassis. Activating an HA license adds the **System > Failover** screen and modifies fields throughout the UI so that hostnames and IP addresses can be configured for both controllers.

After HA is configured, an icon shows when HA is active or unavailable. When HA is disabled by the system administrator, the status icon changes to show HA is unavailable. If the standby TrueNAS controller is not available because it is powered off, still starting up, disconnected from the network, or if failover has not been configured, the status icon changes to show HA is unavailable. HA also becomes unavailable if a different number of disks are connected to each controller.

If both TrueNAS controllers reboot simultaneously, the passphrase for an encrypted pool must be entered at the web
interface login screen.

**Networking**

To make sure system networking is configured for HA, first go to **Network > Global Configuration**.

You can set the host names for both controllers and a virtual host name that reaches whichever controller is currently active.

Next, go to **Network > Interfaces** and edit the primary interface.

Editing interfaces is disabled when HA is active. To disable HA, go to **System > Failover** and disable failover. Edit the interface, then reactivate failover immediately. TrueNAS automatically synchronizes the configuration changes to the standby controller.

You can designate the interface as critical for failover and combine multiple interfaces into a failover group. There are also options to configure IP addresses for each controller and a virtual IP address with virtual host ID to use for administrative access.

After the network configuration is complete, log out and log back in, this time using the virtual IP address. Pools and shares can now be configured as usual and configuration automatically synchronizes between the active and standby TrueNAS controllers.

All subsequent logins should use the virtual IP address. Connecting directly to the standby TrueNAS controller with a browser does not allow web interface logins.

When troubleshooting HA networking, the `ifconfig` command adds two additional fields to the output to help with failover troubleshooting: **CriticalGroup** and **Interlink**.
Failover

To make general changes to the Failover settings, go to System > Failover

You can manually disable failover on this screen.

Make sure to set one of the controllers as the default, so that the default controller becomes active when both boot simultaneously. Booting an HA pair with failover disabled causes both TrueNAS controllers to come up in standby mode. In this situation, the web interface shows an option to force a TrueNAS controller to become active.

To have the system wait to failover during a network timeout, replace \(0\) with a new number of seconds.

Do not `sync` the TrueNAS configuration unless directed by an iXsystems Support Engineer! TrueNAS is designed to automatically synchronize the system configuration and the manual sync options are only for dangerous or high-risk troubleshooting situations.
3.19 - Support

There are a number of options to get support for your TrueNAS installation. TrueNAS CORE users can engage with the TrueNAS community to answer questions and resolve issues, while TrueNAS Enterprise hardware customers can also access the fast and effective support directly provided by iXsystems.

Support Options

○ TrueNAS CORE

There are a number of resources available to TrueNAS CORE users for answering usage questions or troubleshooting system configurations. It is always recommended to search through the software documentation and community resources for answers to these questions.

Users are also welcome to report bugs, vote for, or suggest new TrueNAS features in the project Jira instance.

Customers who purchase iXystems hardware or that want additional support must have a support contract to use iXsystems Support Services.

TrueNAS Community

The TrueNAS Community is an active online resource for asking questions, troubleshooting issues, and sharing information with other TrueNAS users. Registration is required for posting. New users are encouraged to provide a brief introduction of themselves and to review the forum rules before posting.

Community Resources are user contributed articles about every facet of using TrueNAS. They are organized into broad categories and incorporate a community rating system to better highlight content that the whole community finds helpful.

Social Media

You are always welcome to network with other TrueNAS users using the various social media platforms!

- Reddit
- Twitter
- LinkedIn
- Facebook

Reporting a Bug

If you encounter a bug or other issue while using TrueNAS, create a bug report in the TrueNAS Jira Project. The web interface provides a form to report issues without having to log out. It is recommended to search the project first to see if the issue is already reported. You need to create a Jira account before creating a bug ticket.

To report an issue using the web interface, go to System > Support.
Enter your Jira information in the **Username** and **Password** fields to verify your account credentials and activate the **Submit** button. The **Category** dropdown list has a large number of options. Choose the category that best fits where you encountered the issue.

Attach a debug file and any screenshot to your bug ticket helps speed up the response and resolution to find and fix the bug. Debug files are always attached to the ticket privately and are deleted when the ticket is resolved.

Keep the information in **Subject** brief and informative. Provide a short, descriptive subject to help the community find and respond to your issue. The information in **Description** should contain more details about the problem. It is recommended to keep the description less than three paragraphs and include any steps to reproduce the issue or error.

**Creating a Debug File**

The TrueNAS web interface allows users to save debugging information to a text file.

Go to **System > Advanced** (or **System Settings > Advanced** in TrueNAS SCALE) and click **SAVE DEBUG**. Click **PROCEED** to generate the debug file. You cannot click options in the web interface while generating the debug file. A dialogue box displays debug file creation progress.

After generating the debug file, TrueNAS prompts you to save it to your local system (e.g. Downloads), or it automatically downloads to your specified downloaded files location.

Debugging information is collected by the **freenas-debug** command-line utility. A copy of the information is saved to `/var/tmp/fndebug`.

**Suggest New Features**

Want to see a new feature added to TrueNAS? You can see and vote for community-proposed features in the TrueNAS Jira project and make your feature suggestions. To see the list of community-proposed features, go to the TrueNAS Jira project and [search for open suggestions](#). If you find a suggestion that you want to see implemented, open that ticket and click **Vote for this issue** in the **People** section.
To suggest a new feature, go to https://jira.ixsystems.com/projects/NAS/, log in to your Jira account, and click Create.

Enter a brief description for the new feature you’d like to see added to the software in the Summary section. After creating your feature suggestion, it moves to the Gathering Interest stage, where the community can review and vote for the feature. After gathering enough interest, the TrueNAS Release Council reviews the suggestion for feasibility and to determine where to add the feature in the software roadmap.

TrueNAS Enterprise

In addition to all the TrueNAS CORE support options, TrueNAS Enterprise customers who purchase hardware from iXsystems can receive assistance from iXsystems if an issue occurs with the system.

Silver and Gold level Support customers can also enable Proactive Support on their hardware to automatically notify iXsystems if an issue occurs. To find more details about the different Warranty and Service Level Agreement (SLA) options available, see https://www.ixsystems.com/support/.

License Information

The License Information area contains the system model, serial numbers, additional hardware, licensed features, support contract type, and support contract expiration date information. The ability to mark the system as a production system is also available.
Production System Reporting

When the system is ready to be in production, update the status by selecting the *This is a production system* checkbox and clicking the **Update Status** button. This sends an email to Support declaring that the system is in production. There is also an option to include a debug in this email that could assist support in the future.

Configuring Proactive Support

Proactive Support notifies iXsystems by email whenever hardware conditions on the system require attention. This feature is available to iXsystems Silver and Gold Support customers.

Be sure to add valid email addresses and phone numbers for the contacts to be quickly notified of any issues.

You can also enable automatic iXsystems support alerts in the system console menu (`/etc/netcli` in the **Shell**). Failover on TrueNAS High Availability systems must be disabled before activating automatic alerts. To use the web interface to disable failover, go to **System > Failover**.

Filing a Support Ticket

TrueNAS Enterprise customers can file tickets directly with iXsystems Support by going to **System > Support** in the web interface.
Enter a valid email and phone number. iXsystems Support uses this information to respond to and resolve the issue. You can also indicate the system current use and identify how critical the issue is to system usability.

Attaching a debug and screenshots is always recommended to help speed up diagnosing and resolving the issue. It is also helpful to provide a brief summary in the **Subject** and **Description** fields that describes the problem and any steps to reproduce the issue.

Click **SUBMIT** to generate and send the support ticket to iXsystems. This process can take several minutes while information is collected and sent. TrueNAS sends an email alert if ticket creation fails while Proactive Support is active.

After the new ticket is created, the URL displays which allows you to view or update the ticket with more information. An iXsystems Support account is required to view the ticket. Click the URL to log in or register with the support portal. Use the same e-mail address submitted with the ticket when registering.

**Contacting iXsystems Support**

Customers who purchase iXsystems hardware or that want additional support must have a support contract to use iXsystems Support Services. The [TrueNAS Community forums](https://community.ixsystems.com) provides free support for users without an iXsystems Support contract.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td><a href="https://support.ixsystems.com">https://support.ixsystems.com</a></td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:support@ixsystems.com">support@ixsystems.com</a></td>
</tr>
<tr>
<td>Telephone</td>
<td>Monday - Friday, 6:00AM to 6:00PM Pacific Standard Time: US-only toll-free: 1-855-473-7449 option 2 Local and international: 1-408-943-4100 option 2</td>
</tr>
<tr>
<td>Telephone</td>
<td>After Hours (24x7 Gold Level Support only): US-only toll-free: 1-855-499-5131 International: 1-408-878-3140 (international calling rates apply)</td>
</tr>
</tbody>
</table>
For increased security, two-factor authentication is highly desirable. TrueNAS offers Two-Factor Authentication (2FA) to ensure that a compromised administrator (root) password cannot be used by itself to gain access to the administrator interface. You need a mobile device with the current time and date that has Google Authenticator installed to use 2FA.

Two-Factor authentication is time based and requires that the system is set correctly. Making sure NTP is functional before enabling is strongly recommended!

### What is 2FA and why would I want to enable it? expand □
Two-Factor Authentication (2FA) is an extra layer of security that is added to your system to prevent someone from logging in, even if they have your password. This extra security measure requires you to verify your identity using a randomized 6-digit code that is re-generated every 30 seconds, unless the interval is modified, to use when you to log in.

### Benefits
- 2FA provides an extra layer of security: By requiring a second form of identification 2FA decreases the probability that an unauthorized user can gain access to the system. An unauthorized user won’t have the second element required to authenticate their login.
- Increase productivity and flexibility: As the workforce becomes more mobile, employees can securely access systems from virtually any device or location-without putting sensitive information at risk.
- Internet access on the TrueNAS system is not required to use 2FA.

### Drawbacks
- An app is required to access the generated 2FA Code.
- If the the 2FA code isn’t working, or there is no access to the 2FA Password, the system is inaccessible through the UI and SSH (if that option has been set).

To unlock 2FA in the cli, enter:
```
midclt call auth.twofactor.update '{ "enabled":false }'
```

### 2FA Options
Two-factor authentication is time-based and requires that the system time is set correctly.

**User Settings**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Time Password (OTP) Digits</td>
<td>The number of digits in the One-Time Password. The default is 6, which is Google’s standard OTP length. Check your app/device settings before selecting this.</td>
</tr>
<tr>
<td>Interval</td>
<td>The lifespan (in seconds) of each OTP. Default is 30 seconds. The minimum is 5 seconds.</td>
</tr>
<tr>
<td>Window</td>
<td>Extends password validity beyond the Interval setting. For example, 1 means that one password before and after the current one is valid, leaving three valid passwords. Extending the window is useful in high-latency situations.</td>
</tr>
<tr>
<td>Enable Two-Factor Auth for SSH</td>
<td>Enable 2FA for system SSH access. We recommend leaving this DISABLED until after you successfully test 2FA with the UI.</td>
</tr>
</tbody>
</table>

**System Generated Settings**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret (Read-only)</td>
<td>The secret TrueNAS creates and uses to generate OTPs when you first enable 2FA.</td>
</tr>
<tr>
<td>Provisioning URI (includes Secret - Read-only)</td>
<td>The URI used to provision an OTP. TrueNAS encodes the URI (which contains the secret) in a QR Code. To set up an OTP app like Google Authenticator, use the app to scan the QR code or enter the secret manually into the app. TrueNAS produces the URI when you first activate 2FA.</td>
</tr>
</tbody>
</table>

**Enabling Two-Factor Authentication.**
Set up a second 2FA device as a backup before proceeding.

- Go to **System > 2FA**.

- Click **Enable Two Factor Authentication** and **Save**.

- Click **Confirm**.

- Click **Show QR**.
On the mobile device start Google Authentication and scan the QR code.

Using 2FA to Log in to TrueNAS

Enabling 2FA changes the log in process for both the TrueNAS web interface and SSH logins:

○ Web Interface

- The log in screen adds another field for the randomized authenticator code. If this field isn’t immediately visible, try refreshing the browser.
- Enter the code on the mobile device (complete without the space) in the login window with the root Username and Password.
SSH Logins

- Confirm that *Enable Two-Factor Auth for SSH* is set in **System > 2FA**.
- Go to **Services > SSH** and edit the service. Set *Log in with root password* and SAVE. Toggle the **SSH** service and wait for the status to show that it is **Running**.
- Open the Google Authentication app on your mobile device.
- Open a Terminal window and SSH into the system using the system hostname or IP address, *root* account username and password, and the 2FA code from the mobile device.
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.

```
Bonnie-iMac:~ bonniefollweiler$ ssh root@f0n07.lab.ixsystems.com
The authenticity of host 'fn07.lab.ixsystems.com (10.215.6.5)' can't be established.
ECDSA key fingerprint is SHA256:vRe6YASFYHroju87IYyV1amWGEXkOHWG52xRMLdYcc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'fn07.lab.ixsystems.com,10.215.6.5' (ECDSA) to the list of known hosts.
Password for root@freenas.ixsystems.net:
One-time password (OATH) for 'root': ✨
```
4 - Tasks

TrueNAS includes an easy to use interface for common tasks a sysadmin needs to perform on a NAS on a regular basis. These can roughly be broken down into three groups.

- System level tasks
  - Cron Jobs
  - Init and Shutdown scripts
  - S.M.A.R.T. tests
- Data backup tasks
  - Rsync tasks
  - Cloud Sync tasks
- ZFS tasks
  - Snapshots
  - Resilvers
  - Scrubs
  - Replication

Ready to get started? Choose a topic or article from the left-side Navigation pane. Click the < symbol to expand the menu to show the topics under this section.
4.1 - Cron Jobs

- Creating a Cron Job
- Managing a Cron Job

TrueNAS allows users to run specific commands or scripts on a regular schedule using `cron(8)`. This can be helpful for running repetitive tasks.

**Creating a Cron Job**

To create a cron job, go to **Tasks > Cron Jobs** and click **ADD**.

The **Description** helps identify the cron job’s purpose and is optional.

Next, enter the exact **Command** to run on the **Schedule**. Alternately, enter the path to a script file to run instead of a specific command.

Don’t forget to define the shell type when using a path to a script file. For example, a script written for `sh` must be specified as `sh /mnt/pool1/helloWorld.sh`.

Select an existing TrueNAS user account with the necessary permissions to run the command or script.

Next, define the **Command Schedule**. Various preset schedules are available. There is also an advanced scheduler for very specific schedule requirements.
Choosing a **Presets** option populates the rest of the fields. To customize a schedule, enter cron values for the Minutes/Hours/Days.

These fields accept standard cron values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering `10` means that the job runs when the time is ten minutes past the hour.

An asterisk (`*`) means match all values.

Specific time ranges are set by entering hyphenated number values. For example, entering `30-35` in the Minutes field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.

You can also enter lists of values. Enter individual values separated by a comma (,). For example, entering `1,14` in the Hours field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).

A slash (`/`) designates a step value. For example, while entering `*` in Days means the task runs every day of the month, `*/2` means the task runs every other day.

Combining all the above examples together creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

There is an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days. This is in addition to any listed days. For example, entering `7` in Days and setting **Wed** for Days of Week creates a schedule that starts a task on the first day of the month *and* every Wednesday of the month.
The **Schedule Preview** displays when the current settings mean the task runs.

### Examples of CRON syntax

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Meaning</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Every item.</td>
<td>*(minutes) = every minute of the hour. *(days) = every day.</td>
</tr>
</tbody>
</table>
| */N      | Every N \textsuperscript{th} item. | */15 (minutes) = every 15th minute of the hour (every quarter hour).  
*3 (days) = every 3rd day.  
*3 (months) = every 3rd month. |
| Comma and hyphen/dash | Each stated item (comma) Each item in a range (hyphen/dash). | 1,31 (minutes) = on the 1st and 31st minute of the hour.  
1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour.  
mon-fri (days) = every Monday to Friday inclusive (every weekday).  
mar,jun,sep,dec (months) = every March, June, September, December. |

Days can be specified as days of month, or days of week.

With these options, you can create flexible schedules similar to these examples:

<table>
<thead>
<tr>
<th>Desired schedule</th>
<th>Values to enter</th>
</tr>
</thead>
</table>
| 3 times a day (at midnight, 08:00 and 16:00)                                   | months=\*; days=\*; hours=0/8 or 0,8,16; minutes=0  
(Meaning: every day of every month, when hours=0/8/16 and minutes=0)          |
| Every Monday, Wednesday and Friday, at 8.30 pm                                  | months=\*; days=mon,wed,fri; hours=20; minutes=30                                                                                       |
| 1st and 15th day of the month, during October to June, at 00:01 am             | months=oct-dec, jan-jun; days=1,15; hours=0; minutes=1                                                                                     |
| Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday | Note that this requires two tasks to achieve:  
(1) months=\*; days=mon-fri; hours=8-18; minutes= */15  
(2) months=\*; days=mon-fri; hours=19; minutes=0  
We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00. |

Additional Options: When **Hide standard output** (stdout) is unset, any standard output is mailed to the user account used to run the command.

When **Hide Standard Error** (stderr) is unset, any error output is mailed to the user account used to run the command. This can be useful to help debug the command or script if an error occurs.

Unsetting **Enabled** only keeps the task from automatically running. You can still save the cron job and run it manually.

### Managing a Cron Job

To see all created cron jobs, go to **Tasks > Cron Jobs**. Click the **show** next to an entry to see details and options.
Clicking *RUN NOW* immediately starts the job *Command*, separately from any *Schedule*. *EDIT* changes any setting available during task creation. *DELETE* removes the cron job from TrueNAS. Once a cron job is deleted, the job configuration cannot be restored.
4.2 - Init/Shutdown Scripts

TrueNAS can schedule commands or scripts to run at system startup or shutdown. To create a new script, go to **Tasks > Init/Shutdown Scripts** and click **ADD**.

### Init/Shutdown Script

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Comments about this script.</td>
</tr>
<tr>
<td>Type</td>
<td>Select Command for an executable or Script for an executable script.</td>
</tr>
<tr>
<td>Command</td>
<td>Enter the command with any options. When <em>Script</em> is selected, click the folder to define the path to the script file.</td>
</tr>
<tr>
<td>When</td>
<td><strong>Pre Init</strong> is early in the boot process, after mounting filesystems and starting networking. <strong>Post Init</strong> is at the end of the boot process, before TrueNAS services start. <strong>Shutdown</strong> is during the system power off process.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enable this task. Unset to disable the task without deleting it.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Automatically stop the script or command after the specified seconds.</td>
</tr>
</tbody>
</table>

**Can I use a path for the Command? expand □**

You can also include the full path to a command in the entry. Scheduled commands must be in the default path. The path can be tested with `which {COMMAND}` in the **Shell**. When available, the path to the command is shown:

```
[root@freenas ~]# which ls
/bin/ls
```

Always test the script first to verify it is executable and achieves the desired results. All init/shutdown scripts are run with `sh`.

All saved Init/Shutdown tasks are shown in **Tasks > Init/Shutdown Scripts**. Click □ (Options) next to a task to **EDIT** or **DELETE** that task.
4.3 - Rsync Tasks

- Basic Requirements
- Creating an Rsync Task
- Rsync Service and Modules

You often need to copy data to another system for backup or when migrating to a new system. A fast and secure way of doing this is by using `rsync`. These instructions assume that both sides of the rsync task, host and remote, use a TrueNAS system.

Basic Requirements

Rsync requires a dataset with the needed data on the host or remote system. Rsync provides the ability to either push or pull data. When using the Rsync Tasks function to push, data is copied from a host system to a remote system. When using the Rsync Tasks function to pull, it pulls data from a remote system and puts it on the host system.

The remote system must have the rsync service activated. Additional requirements are listed further down for either rsynch module or SSH tasks.

Creating an Rsync Task

Go to Tasks > Rsync Tasks and click ADD. The Rsync Mode field has two primary rsync modes: Module and SSH. Each mode has different requirements. See the related tab for each rsync mode.

○ Module

Module Requirements

Before you create an rsync task on the host system, you must create a module on the remote system. When TrueNAS is the remote system, create a module. Go to Services and click edit for the rsync service. Click the Rsync Module tab, then click ADD. See the specific configuration instructions in the Rsync Service section of this article.

Rsync Module Process

Log in to the host system interface, go to Tasks > Rsync Tasks, and click ADD.
Select the source dataset to use with the rsync task and a user account to run the rsync task. Choose a direction for the rsync task.

Select a schedule for the rsync task. If you need a custom schedule, select Custom.

Advanced Scheduler expand □
Choosing a **Presets** option populates the rest of the fields. To customize a schedule, enter **crontab** values for the Minutes/Hours/Days.

These fields accept standard **cron** values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering **10** means that the job runs when the time is ten minutes past the hour.

An asterisk ( * ) means match all values.

Specific time ranges are set by entering hyphenated number values. For example, entering **30-35** in the Minutes field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.

You can also enter lists of values. Enter individual values separated by a comma ( , ). For example, entering **1,14** in the Hours field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).

A slash ( / ) designates a step value. For example, while entering * in Days means the task runs every day of the month, * /2 means the task runs every other day.

Combining all the above examples together creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

There is an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days. This is in addition to any listed days. For example, entering **7** in Days and setting **Wed** for Days of Week creates a schedule that starts a task on the first day of the month and every Wednesday of the month.
The Schedule Preview displays when the current settings mean the task runs.

### Examples of CRON syntax

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Meaning</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Every item.</td>
<td>* (minutes) = every minute of the hour. * (days) = every day.</td>
</tr>
<tr>
<td>*/N</td>
<td>Every N\textsuperscript{th} item.</td>
<td>*/15 (minutes) = every 15th minute of the hour (every quarter hour). */3 (days) = every 3rd day. */3 (months) = every 3rd month.</td>
</tr>
<tr>
<td>Comma and hyphen/dash</td>
<td>Each stated item (comma) Each item in a range (hyphen/dash).</td>
<td>1,31 (minutes) = on the 1st and 31st minute of the hour. 1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour. mon-fri (days) = every Monday to Friday inclusive (every weekday). mar,jun,sep,dec (months) = every March, June, September, December.</td>
</tr>
</tbody>
</table>

Days can be specified as days of month, or days of week.

With these options, you can create flexible schedules similar to these examples:

<table>
<thead>
<tr>
<th>Desired schedule</th>
<th>Values to enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 times a day (at midnight, 08:00 and 16:00)</td>
<td>months=<em>; days=</em>; hours=0/8 or 0,8,16; minutes=0 (Meaning: every day of every month, when hours=0/8/16 and minutes=0)</td>
</tr>
<tr>
<td>Every Monday, Wednesday and Friday, at 8.30 pm</td>
<td>months=*; days=mon,wed,fri; hours=20; minutes=30</td>
</tr>
<tr>
<td>1st and 15th day of the month, during October to June, at 00:01 am</td>
<td>months=oct-dec,jan-jun; days=1,15; hours=0; minutes=1</td>
</tr>
<tr>
<td>Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday</td>
<td>Note that this requires two tasks to achieve: (1) months=<em>; days=mon-fri; hours=8-18; minutes=</em>/15  (2) months=*; days=mon-fri; hours=19; minutes=0  We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00.</td>
</tr>
</tbody>
</table>

Next, enter the Remote Host IP address or hostname. Use the format `username@remote_host` when the username differs from the host entered into the Remote Host field. Select Module on the Rsync Mode dropdown. Enter the Remote Module Name exactly as it appears on the remote system.

Configure the remaining options according to your specific needs.
specified directory on the remote host.

**Direction**
Direct the flow of data to the remote host. During a **push**, the dataset transfers to the remote module. During a **pull**, the dataset stores files from the remote system.

**Description**
Enter a description of the rsync task.

<table>
<thead>
<tr>
<th>Schedule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule</td>
<td>Select a schedule preset or choose Custom to open the advanced scheduler.</td>
</tr>
<tr>
<td>Recursive</td>
<td>Set to include all subdirectories of the specified directory. When unset, only the specified directory is included.</td>
</tr>
</tbody>
</table>

**Remote**
Enter the IP address or hostname of the remote system that will store the copy. Use the format `username@remote_host` if the username differs on the remote host.

**Rsync Mode**
Choose to either use a custom-defined remote module of the rsync server or to use an SSH configuration for the rsync task.

<table>
<thead>
<tr>
<th>More Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Times</td>
<td>Set to preserve modification times of files.</td>
</tr>
<tr>
<td>Compress</td>
<td>Set to reduce the size of data to transmit. Recommended for slow connections.</td>
</tr>
<tr>
<td>Archive</td>
<td>When set, rsync is run recursively, preserving symlinks, permissions, modification times, group, and special files. When run as root, owner, device files, and special files are also preserved. Equivalent to passing the flags <code>-rlptgoD</code> to rsync.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete files in the destination directory that do not exist in the source directory.</td>
</tr>
<tr>
<td>Quiet</td>
<td>Set to suppress informational messages from the remote server.</td>
</tr>
<tr>
<td>Preserve Permissions</td>
<td>Set to preserve original file permissions. This is useful when the user is set to root.</td>
</tr>
<tr>
<td>Preserve Extended Attributes</td>
<td>Extended attributes are preserved, but must be supported by both systems.</td>
</tr>
<tr>
<td>Delay Updates</td>
<td>Set to save the temporary file from each updated file to a holding directory until the end of the transfer when all transferred files are renamed into place.</td>
</tr>
<tr>
<td>Auxiliary Parameters</td>
<td>Additional <code>rsync(1)</code> options to include. Separate entries by pressing Enter. Note: The “character must be escaped with a backslash” (<code>.txt</code>) or used inside single quotes (<code>'*.txt'</code>).</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enable this rsync task. Unset to disable this rsync task without deleting it.</td>
</tr>
</tbody>
</table>

The **Module mode** adds the **Remote Module Name** field to the **Remote** section:

You must define at least one module in `rsyncd.conf(5)` of the rsync server or in the rsync modules of another system.

If the **Enable** checkbox is not selected it disables the task schedule, but you can still save the rsync task and run it manually.
SSH

SSH Requirements

The remote system must have SSH enabled. To enable SSH in TrueNAS, go to Services and toggle SSH on.

The host system needs an established SSH connection to the remote for the rsync task. To create the connection, go to System > SSH Connections and click Add. Populate the SSH configuration screen fields as follows: Select Semi-automatic for the Setup Method and set **Private Key** to Generate New.

Can this be set up in a command line instead? expand □

To use a command line, go to the Shell on the host system. When a TrueNAS account other than root manages the rsync task, enter `su - {USERNAME}`, where `{USERNAME}` is the TrueNAS user account that runs the rsync task.

Enter `ssh-keygen -t rsa` to create the key pair. When prompted for a password, press Enter without setting a password (a password breaks the automated task). Here is an example of running the command:

```
truenas$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
```

The default public key location is ~/.ssh/id_rsa.pub. Enter `cat ~/.ssh/id_rsa.pub` to see the key and copy the file contents. Copy it to the corresponding user account on the remote system in Accounts > Users. Click EDIT and paste the key in SSH Public Key.

Next, copy the host key from the remote system to the host system user’s .ssh/known_hosts directory, using ssh-keyscan. On the host system, open the Shell and enter `ssh-keyscan -t rsa {remoteIPaddress} >> {userknown_hostsDir}` where `{remoteIPaddress}` is the remote system IP address and `{userknown_hostsDir}` is the known_hosts directory on the host system. Example: `ssh-keyscan -t rsa 192.168.2.6 >> /root/.ssh/known_hosts`.

SSH Mode Process

Go to Tasks > Rsync Tasks and click ADD.
Configure the SSH settings first by selecting **SSH** in the **Rsync Mode** drop-down and typing the **Port** number and **Remote Path**.

Next, define the **Source** dataset to use for the rsync task and select a **User** account. The **User** field entry must be identical to the **SSH Connection Username**.

Choose a **Direction** for the rsync task, either **Push** or **Pull** and then define the task **Schedule**. If you need a custom schedule, select **Custom**.

**Advanced Scheduler expand □**
Choosing a **Presets** option populates the rest of the fields. To customize a schedule, enter crontab values for the Minutes/Hours/Days.

These fields accept standard **cron** values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering 10 means that the job runs when the time is ten minutes past the hour.

An asterisk ( *) means match all values.

Specific time ranges are set by entering hyphenated number values. For example, entering 30-35 in the Minutes field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.

You can also enter lists of values. Enter individual values separated by a comma (,). For example, entering 1,14 in the Hours field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).

A slash (/) designates a step value. For example, while entering * in Days means the task runs every day of the month, */2 means the task runs every other day.

Combining all the above examples together creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

There is an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days. This is in addition to any listed days. For example, entering 7 in Days and setting Wed for Days of Week creates a schedule that starts a task on the first day of the month and every Wednesday of the month.
The **Schedule Preview** displays when the current settings mean the task runs.

### Examples of CRON syntax

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Meaning</th>
<th>Examples</th>
</tr>
</thead>
</table>
| *      | Every item. | * (minutes) = every minute of the hour.  
* (days) = every day. |
| */N    | Every Nth item. | */15 (minutes) = every 15th minute of the hour (every quarter hour).  
*/3 (days) = every 3rd day.  
*/3 (months) = every 3rd month. |
| Comma and hyphen/dash | Each stated item (comma) Each item in a range (hyphen/dash). | 1,31 (minutes) = on the 1st and 31st minute of the hour.  
1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour.  
mon-fri (days) = every Monday to Friday inclusive (every weekday).  
mar,jun,sep,dec (months) = every March, June, September, December. |

Days can be specified as days of month, or days of week.

With these options, you can create flexible schedules similar to these examples:

<table>
<thead>
<tr>
<th>Desired schedule</th>
<th>Values to enter</th>
</tr>
</thead>
</table>
| 3 times a day (at midnight, 08:00 and 16:00) | months=*; days=*; hours=0/8 or 0,8,16; minutes=0  
(Meaning: every day of every month, when hours=0/8/16 and minutes=0) |
| Every Monday, Wednesday and Friday, at 8.30 pm | months=*; days=mon,wed,fri; hours=20; minutes=30 |
| 1st and 15th day of the month, during October to June, at 00:01 am | months=oct-dec,jun-jan; days=1,15; hours=0; minutes=1 |
| Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday | Note that this requires two tasks to achieve:  
(1) months=*; days=mon-fri; hours=8-18; minutes=*/15  
(2) months=*; days=mon-fri; hours=19; minutes=0  
We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00. |

Next, enter the **Remote Host** IP address or hostname. Use the format `username@remote_host` if the username differs on the remote host. Configure the remaining options according to your specific needs.

### Options expand □

#### Source

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>Browse to the path to be copied. FreeBSD file path limits apply. Other operating systems can have different limits which might affect how they can be used as sources or destinations.</td>
</tr>
<tr>
<td>User</td>
<td>Select the user to run the rsync task. The user selected must have permissions to write to the specified directory on the remote host.</td>
</tr>
<tr>
<td>Direction</td>
<td>Direct the flow of data to the remote host. During a <strong>push</strong>, the dataset transfers to the remote module. During a <strong>pull</strong>, the dataset stores files from the <strong>remote</strong> system.</td>
</tr>
</tbody>
</table>
### Description
Enter a description of the rsync task.

### Schedule

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule</td>
<td>Select a schedule preset or choose Custom to open the advanced scheduler.</td>
</tr>
<tr>
<td>Recursive</td>
<td>Set to include all subdirectories of the specified directory. When unset, only the specified directory is included.</td>
</tr>
</tbody>
</table>

### Remote

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Host</td>
<td>Enter the IP address or hostname of the remote system that will store the copy. Use the format <code>username@remote_host</code> if the username differs on the remote host.</td>
</tr>
<tr>
<td>Rsync Mode</td>
<td>Choose to either use a custom-defined remote module of the rsync server or to use an SSH configuration for the rsync task.</td>
</tr>
</tbody>
</table>

### More Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Times</td>
<td>Set to preserve modification times of files.</td>
</tr>
<tr>
<td>Compress</td>
<td>Set to reduce the size of data to transmit. Recommended for slow connections.</td>
</tr>
<tr>
<td>Archive</td>
<td>When set, rsync is run recursively, preserving symlinks, permissions, modification times, group, and special files. When run as root, owner, device files, and special files are also preserved. Equivalent to passing the flags <code>--rlptgoD</code> to rsync.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete files in the destination directory that do not exist in the source directory.</td>
</tr>
<tr>
<td>Quiet</td>
<td>Set to suppress informational messages from the remote server.</td>
</tr>
<tr>
<td>Preserve Permissions</td>
<td>Set to preserve original file permissions. This is useful when the user is set to root.</td>
</tr>
<tr>
<td>Preserve Extended Attributes</td>
<td><code>Extended attributes</code> are preserved, but must be supported by both systems.</td>
</tr>
<tr>
<td>Delay Updates</td>
<td>Set to save the temporary file from each updated file to a holding directory until the end of the transfer when all transferred files are renamed into place.</td>
</tr>
<tr>
<td>Auxiliary Parameters</td>
<td>Additional <code>rsync(1)</code> options to include. Separate entries by pressing Enter. Note: The “<code>&quot; character must be escaped with a backslash (</code>`) or used inside single quotes (<code>'*</code>.txt`).</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enable this rsync task. Unset to disable this rsync task without deleting it.</td>
</tr>
</tbody>
</table>

Additional options for the **SSH Rsync Mod**:

- **Remote SSH Port**: Enter the SSH port number of the remote system. By default, 22 is reserved in TrueNAS.
- **Remote Path**: Browse to the existing path on the remote host to sync with. Maximum path length is 255 characters.
- **Validate Remote Path**: Set to automatically create the defined Remote Path when it does not exist.

If the **Enabled** checkbox is not selected it disables the task schedule without deleting the configuration. You can still run the rsync task by going to **Tasks > Rsync Tasks** and clicking **RUN NOW** icon.
Rsync Service and Modules

The rsync task does not work unless the related system service is turned on. To turn the rsync service on, go to Services and toggle rsync on. To activate the service whenever TrueNAS boots, select the Start Automatically checkbox.

Click the edit to configure the service on the Services > Rsync screen. There are two sections for rsync configuration: basic Configure options and Rsync Module creation and management.

○ Configure

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Port</td>
<td>rsyncd listens on this port.</td>
</tr>
<tr>
<td>Auxiliary Parameters</td>
<td>Enter any additional parameters from rsyncd.conf(5).</td>
</tr>
</tbody>
</table>

Use the default settings unless a specific change is required. Remember to click SAVE after changing any settings.

○ Rsync Module

All created modules are listed on the Rsync Module tab. To create a new module, click ADD.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Module name that matches the name requested by the rsync client.</td>
</tr>
<tr>
<td>Path</td>
<td>Browse to the pool or dataset to store received data.</td>
</tr>
<tr>
<td>Comment</td>
<td>Describe this module.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Activate this module for use with Rsync. Unset this field to deactivate the module without completely removing it.</td>
</tr>
</tbody>
</table>

**Access**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Mode</td>
<td>Choose permissions for this rsync module.</td>
</tr>
<tr>
<td>Max Connections</td>
<td>Maximum number of connections to this module. 0 is unlimited.</td>
</tr>
<tr>
<td>User</td>
<td>TrueNAS user account that runs the rsync command during file transfers to and from this module.</td>
</tr>
<tr>
<td>Group</td>
<td>TrueNAS group account that runs the rsync command during file transfers to and from this module.</td>
</tr>
<tr>
<td>Hosts Allow</td>
<td>From <code>rsyncd.conf(5)</code> A list of patterns to match with the hostname and IP address of a connecting client. The connection is rejected if no patterns match. Separate entries by pressing Enter.</td>
</tr>
<tr>
<td>Hosts Deny</td>
<td>From <code>rsyncd.conf(5)</code> A list of patterns to match with the hostname and IP address of a connecting client. The connection is rejected when the patterns match. Separate entries by pressing Enter.</td>
</tr>
</tbody>
</table>

**Other Options**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auxiliary Parameters</td>
<td>Enter any additional parameters from <code>rsyncd.conf(5)</code></td>
</tr>
</tbody>
</table>

When a **Hosts Allow** list is defined, *only* the IPs and hostnames on the list are able to connect to the module.

To **EDIT** or **DELETE** a module, go to the **Rsync Modules** list and click ▴ for an entry.
4.4 - S.M.A.R.T. Tests

- Manual S.M.A.R.T. Test
- Automatic S.M.A.R.T. Tests
- Service Options

S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) is an industry standard for disk monitoring and testing. Disks can be monitored for problems using several different kinds of self-tests. TrueNAS can adjust when and how alerts for S.M.A.R.T. are issued. When S.M.A.R.T. monitoring reports an issue, we recommend you replace that disk. Most modern ATA, IDE, and SCSI-3 hard drives support S.M.A.R.T. Refer to your respective drive documentation for confirmation.

S.M.A.R.T. tests are run on a disk. Running tests can reduce drive performance, so we recommend scheduling tests when the system is in a low-usage state. Avoid scheduling disk-intensive tests at the same time! For example, S.M.A.R.T. tests should not be scheduled on the same day as a disk scrub or resilver.

How do I check or change S.M.A.R.T. testing for a disk? expand □

Go to Storage > Disks and click chevron_right to expand an entry. Enable S.M.A.R.T. shows as true or false.

To enable or disable testing, click EDIT DISK(S) and find the Enable S.M.A.R.T. option.

Manual S.M.A.R.T. Test

To quickly test a disk for errors, go to Storage > Disks and select the disks to be tested. After selecting the desired disks, click MANUAL TEST.

Next, select the test Type. Each test type can be slightly different based on the drive connection, ATA or SCSI:

- **ATA**
  - Long - runs SMART Extended Self Test. This will scan the entire disk surface and can take many hours on large-volume disks.
  - Short - runs SMART Short Self Test (usually under ten minutes). These are basic disk tests that vary by manufacturer.
  - Conveyance - runs a SMART Conveyance Self Test. This self-test routine is intended to identify damage incurred during transporting of the device. This self-test routine requires only minutes to complete.
  - Offline - runs SMART Immediate Offline Test. The effects of this test are visible only in that it updates the SMART Attribute values, and if the test finds errors, they appear in the SMART error log.
SCSI

- **Long** - runs the “Background long” self-test.
- **Short** - runs the “Background short” self-test.
- **Offline** - runs the default self test in foreground. No entry is placed in the self test log.

For more information, refer to [smartctl(8)](https://man7.org/linux/man-pages/man8/smartctl.8.html).

Click **START** to begin the test. Depending on the test type you choose, the test can take some time to complete. TrueNAS generates alerts when tests discover issues.

**Where can I view the test results?**

Go to **Storage > Disks**, expand an entry, and click **S.M.A.R.T. TEST RESULTS**. From the **Shell**, use `smartctl` and the name of the drive: `smartctl -l selftest /dev/ada0`.

### Automatic S.M.A.R.T. Tests

To schedule recurring S.M.A.R.T. tests, go to **Tasks > S.M.A.R.T. Tests** and click **ADD**.

#### Specific Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All Disks</strong></td>
<td>Setting <em>All Disks</em> includes every disk with S.M.A.R.T. enabled. Leave unset to choose which <em>Disks</em> to test.</td>
</tr>
<tr>
<td><strong>Disks</strong></td>
<td>Select the disks to monitor.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Choose the test type. See <a href="https://man7.org/linux/man-pages/man8/smartctl.8.html">smartctl(8)</a> for descriptions of each type. Some types degrade performance or take disks offline.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter information about the S.M.A.R.T. test.</td>
</tr>
<tr>
<td><strong>Schedule</strong></td>
<td>The time the test runs. Choose a preset or select <strong>Custom</strong> to open the advanced scheduler.</td>
</tr>
</tbody>
</table>

Choose the **Disks** to test, **Type** of test to run, and **Schedule** for the task.

SMART tests can offline disks! Avoid scheduling S.M.A.R.T. tests simultaneously with scrub or resilver operations.

When the test must run on a very specific **Schedule**, set this to **Custom** to open the advanced scheduler.
Choosing a **Presets** option populates the rest of the fields. To customize a schedule, enter `crontab` values for the `Minutes/Hours/Days`.

These fields accept standard `cron` values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering `10` means that the job runs when the time is ten minutes past the hour.

An asterisk (`*`) means match all values.

Specific time ranges are set by entering hyphenated number values. For example, entering `30-35` in the `Minutes` field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.

You can also enter lists of values. Enter individual values separated by a comma (`,`). For example, entering `1,14` in the `Hours` field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).

A slash (`/`) designates a step value. For example, while entering `*` in `Days` means the task runs every day of the month, `*/2` means the task runs every other day.

Combining all the above examples together creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

There is an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days. This is in addition to any listed days. For example,
entering 1 in **Days** and setting **Wed** for **Days of Week** creates a schedule that starts a task on the first day of the month *and* every Wednesday of the month.

The **Schedule Preview** displays when the current settings mean the task runs.

**Examples of CRON syntax**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Meaning</th>
<th>Examples</th>
</tr>
</thead>
</table>
| *      | Every item. | * (minutes) = every minute of the hour.  
        |         | * (days) = every day. |
| */N    | Every N\(^{th}\) item. | */15 (minutes) = every 15th minute of the hour (every quarter hour).  
        |         | */3 (days) = every 3rd day.  
        |         | */3 (months) = every 3rd month. |
| Comma and hyphen/dash | Each stated item (comma) Each item in a range (hyphen/dash). | 1,31 (minutes) = on the 1st and 31st minute of the hour.  
        |         | 1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour.  
        |         | mon-fri (days) = every Monday to Friday inclusive (every weekday).  
        |         | mar,jun,sep,dec (months) = every March, June, September, December. |

Days can be specified as days of month, or days of week.

With these options, you can create flexible schedules similar to these examples:

<table>
<thead>
<tr>
<th>Desired schedule</th>
<th>Values to enter</th>
</tr>
</thead>
</table>
| 3 times a day (at midnight, 08:00 and 16:00) | months=*; days=*; hours=0/8 or 0,8,16; minutes=0  
        | (Meaning: every day of every month, when hours=0/8/16 and minutes=0) |
| Every Monday, Wednesday and Friday, at 8.30 pm | months=*; days=mon,wed,fri; hours=20; minutes=30 |
| 1st and 15th day of the month, during October to June, at 00:01 am | months=oct-dec,jan-jun; days=1,15; hours=0; minutes=1 |
| Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday | Note that this requires two tasks to achieve:  
        | (1) months=*; days=mon-fri; hours=8-18; minutes=*/15  
        | (2) months=*; days=mon-fri; hours=19; minutes=0  
        | We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00. |

Saved schedules appear in the **Tasks > S.M.A.R.T. Tests** list.

**CLI expand □**

To verify the schedule is saved, you can open the shell and enter `smartd -q showtests`.

**Service Options**

The S.M.A.R.T. service must be enabled for automatic S.M.A.R.T. tests to run.

**RAID controllers? expand □**

Disable the S.M.A.R.T. service when disks are controlled by a RAID controller. The controller monitors S.M.A.R.T. separately and marks disks as a **Predictive Failure** on a test failure.
To start the S.M.A.R.T. service, go to **Services** and toggle **S.M.A.R.T.**. To start the service during the TrueNAS boot process, set **Start Automatically**.

Configure the S.M.A.R.T. service by clicking **edit**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Interval</td>
<td>Minutes for <strong>smartd</strong>, to wake up and check if any tests should run.</td>
</tr>
<tr>
<td>Power Mode</td>
<td>S.M.A.R.T. only tests when the Power Mode is Never.</td>
</tr>
<tr>
<td>Difference</td>
<td>Degrees in Celsius. S.M.A.R.T. reports if a drive’s temperature has changed by N degrees Celsius since the last report.</td>
</tr>
<tr>
<td>Informational</td>
<td>Threshold temperature in Celsius. S.M.A.R.T. will message with a LOG_INFO log level if the temperature is above the threshold.</td>
</tr>
<tr>
<td>Critical</td>
<td>Threshold temperature in Celsius. S.M.A.R.T. will message with a LOG_CRIT log level and send an email if the temperature is above the threshold.</td>
</tr>
</tbody>
</table>

Don’t forget to click **SAVE** after changing any settings.
4.5 - Periodic Snapshot Tasks

- Creating a Periodic Snapshot Task
  - Process

A periodic snapshot task allows scheduling the creation of read only versions of pools and datasets at a given point in time.

**How should I use snapshots? expand □**

Snapshots do not make not copies of the data so creating one is quick and if little data changed, they take very little space. It is common to take frequent snapshots as soon as every 15 minutes, even for large and active pools. A snapshot where no files changed takes no storage space, but as files changes happen, the snapshot size changes to reflect the size of the changes. In the same way as all pool data, after deleting the last reference to the data you recover the space.

Snapshots keep a history of files, providing a way to recover an older copy or even a deleted file. For this reason, many administrators take snapshots often, store them for a period of time, and store them on another system, typically using the Replication Tasks function. Such a strategy allows the administrator to roll the system back to a specific point in time. If there is a catastrophic loss, an off-site snapshot can restore data up to the time of the last snapshot.

**Creating a Periodic Snapshot Task**

Any required datasets or zvols must exist before creating a snapshot task.

**Process**

Go to **Tasks > Periodic Snapshot Tasks** and click **ADD**.

Choose the dataset (or zvol) to schedule as a regular back up with snapshots and how long to store snapshots. Define the task **Schedule**. If you need a specific schedule, choose **Custom** and use the Advanced Scheduler section below.
Choosing a **Presets** option populates the rest of the fields. To customize a schedule, enter **crontab** values for the Minutes/Hours/Days.

These fields accept standard **cron** values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering `10` means that the job runs when the time is ten minutes past the hour.

An asterisk (`*`) means match all values.

Specific time ranges are set by entering hyphenated number values. For example, entering `30-35` in the Minutes field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.

You can also enter lists of values. Enter individual values separated by a comma (,). For example, entering `1,14` in the Hours field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).

A slash (/) designates a step value. For example, while entering `*` in Days means the task runs every day of the month, `/2` means the task runs every other day.

Combining all the above examples together creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

There is an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days. This is in addition to any listed days. For example, entering `1` in Days and setting `Wed` for Days of Week creates a schedule that starts a task on the first day of the month and every Wednesday of the month.
The **Schedule Preview** displays when the current settings mean the task runs.

## Examples of CRON syntax

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Meaning</th>
<th>Examples</th>
</tr>
</thead>
</table>
| *      | Every item. | * (minutes) = every minute of the hour.  
|        |          | * (days) = every day.            |
| */N    | Every Nth item. | */15 (minutes) = every 15th minute of the hour (every quarter hour).  
|        |          | */3 (days) = every 3rd day.        |
|        |          | */3 (months) = every 3rd month.    |
| Comma and hyphen/dash | Each stated item (comma) Each item in a range (hyphen/dash). | 1,31 (minutes) = on the 1st and 31st minute of the hour.  
|        |          | 1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour.  
|        |          | mon-fri (days) = every Monday to Friday inclusive (every weekday).  
|        |          | mar,jun,sep,dec (months) = every March, June, September, December. |

Days can be specified as days of month, or days of week.

With these options, you can create flexible schedules similar to these examples:

<table>
<thead>
<tr>
<th>Desired schedule</th>
<th>Values to enter</th>
</tr>
</thead>
</table>
| 3 times a day (at midnight, 08:00 and 16:00) | months=*; days=*; hours=0/8 or 0,8,16; minutes=0  
|            | (Meaning: every day of every month, when hours=0/8/16 and minutes=0) |
| Every Monday, Wednesday and Friday, at 8.30 pm | months=*; days=mon,wed,fri; hours=20; minutes=30 |
| 1st and 15th day of the month, during October to June, at 00:01 am | months=oct-dec,jan-jun; days=1,15; hours=0; minutes=1 |
| Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday | Note that this requires two tasks to achieve:  
|            | (1) months=*; days=mon-fri; hours=8-18; minutes=*/15  
|            | (2) months=*; days=mon-fri; hours=19; minutes=0  
|            | We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00. |

Configure the remaining options for your use case.

### Specific Options expand □

#### Dataset

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dataset</td>
<td>Select a pool, dataset, or zvol.</td>
</tr>
<tr>
<td>Recursive</td>
<td>Set to take separate snapshots of the dataset and each of its child datasets. Leave unset to take a single snapshot only of the specified dataset without child datasets.</td>
</tr>
<tr>
<td>Exclude</td>
<td>Exclude specific child datasets from the snapshot. Use with recursive snapshots. List paths to any child datasets to exclude. Example: pool1/dataset1/child1. A recursive snapshot of pool1/dataset1 will include all child datasets except child1. Separate entries by pressing Enter.</td>
</tr>
</tbody>
</table>
**Schedule**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshot Lifetime</td>
<td>Define a length of time to retain the snapshot on this system using a numeric value and a single lowercase letter for units. Examples: 3h is three hours, 1m is one month, and 1y is one year. Does not accept Minute values. After the time expires, the snapshot is removed. Snapshots which have been replicated to other systems are not affected.</td>
</tr>
<tr>
<td>Naming Schema</td>
<td>Snapshot name format string. The default is auto-%Y-%m-%d_%H-%M. Must include the strings %Y, %m, %d, %H, and %M, which are replaced with the four-digit year, month, day of month, hour, and minute as defined in strftime(3). For example, snapshots of pool1 with a Naming Schema of customsnap-%Y%m%d.%H%M have names like pool1@customsnap-20190315.0527.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Choose one of the presets or Custom to use the advanced scheduler.</td>
</tr>
<tr>
<td>Allow Taking Empty</td>
<td>Creates dataset snapshots even when there have been no changes to the dataset from the last snapshot. Recommended for long-term restore points, multiple snapshot tasks pointed at the same datasets, or compatibility with snapshot schedules or replications created in TrueNAS 11.2 and earlier. For example, allowing empty snapshots for a monthly snapshot schedule allows that monthly snapshot to be taken, even when a daily snapshot task has already taken a snapshot of any changes to the dataset.</td>
</tr>
<tr>
<td>Enabled</td>
<td>To activate this periodic snapshot schedule, set this option. To disable this task without deleting it, unset this option.</td>
</tr>
</tbody>
</table>

**Naming Schemas**

The Naming Schema determines how automated snapshot names generate. A valid schema requires the %Y (year), %m (month), %d (day), %H (hour), and %M (minute) time strings, but you can add more identifiers to the schema too, using any identifiers from the Python strftime function.

For Periodic Snapshot Tasks used to set up a replication task with the Replication Task function:

You can use custom naming schemas for full backup replication tasks. If you are going to use the snapshot for an incremental replication tasks, use the default naming schema. Go to Using a Custom Schema for additional information.

This uses some letters differently from POSIX (Unix) time functions. For example, including %z (time zone) ensures that snapshots do not have naming conflicts when daylight time starts and ends, and %S (second) adds finer time granularity.

Examples:

<table>
<thead>
<tr>
<th>Naming Scheme</th>
<th>Snapshot Names Look Like</th>
</tr>
</thead>
<tbody>
<tr>
<td>replicationsnaps-1wklife-%Y%m%d_%H:%M</td>
<td>replicationsnaps-1wklife-20210120_00:00, replicationsnaps-1wklife-20210120_06:00</td>
</tr>
<tr>
<td>autosnap_%Y.%m.%d-%H.%M.%S-%z</td>
<td>autosnap_2021.01.20-00.00.00-EST, autosnap_2021.01.20-06.00.00-EST</td>
</tr>
</tbody>
</table>

When referencing snapshots from a Windows computer, avoid using characters like : that are invalid in a Windows file path. Some applications limit filename or path length, and there might be limitations related to spaces and other characters. Always consider future uses and ensure the name given to a periodic snapshot is acceptable.

**Snapshot Lifetimes**

---

*Note: The content is from TrueNAS documentation and is a representation of the original text for educational purposes.*
TrueNAS deletes snapshots when they reach the end of their life and preserves snapshots when at least one periodic task requires it. For example, you have two schedules created where one schedule takes a snapshot every hour and keeps them for a week, and the other takes a snapshot every day and keeps them for 3 years. Each has an hourly snapshot taken. After a week, snapshots created at 01.00 through 23.00 get deleted, but you keep snapshots timed at 00.00 because they are necessary for the second periodic task. These snapshots get destroyed at the end of 3 years.

Click **SUBMIT** to save this task and add it to the list in [Tasks > Periodic Snapshot Tasks](#). You’ll find any snapshots taken using this task in [Storage > Snapshots](#).

To check the log for a saved snapshot schedule, go to [Tasks > Periodic Snapshot Tasks](#) and click the task **State**.
4.6 - Replication Tasks

The ZFS file system provides ability to create a snapshot of the file system contents and transfer the snapshot to another machine to recreate the file system on another machine. Snapshots can be created at any time and as many snapshots can be created as needed. By utilizing replication sysadmins can achieve synchronization between one or more machines.

ZFS replication relies on periodic ZFS snapshots. ZFS snapshots are an inherent feature from the ZFS file system, and are a point-in-time state of the existing ZFS file system. Snapshot can be triggered manually or scheduled. Once the ZFS replication task has been configured, the selected snapshot or snapshots will be replicated to the target ZFS dataset. Usually, the target ZFS dataset is on a secondary TrueNAS storage server, serving as a disaster recovery platform.

Ready to get started? Choose a topic or article from the left-side Navigation pane. Click the `<` symbol to expand the menu to show the topics under this section.
4.6.1 - Local

- Quick Backups with the Replication Wizard

**Process Summary**

- Requirements: Storage pools and datasets created in Storage > Pools.
- Go to Tasks > Replication Tasks and click ADD
  - Choose Sources
    - Set the source location to the local system
    - Use the file browser or type paths to the sources
  - Define a Destination path
    - Set the destination location to the local system
    - Select or manually define a path to the single destination location for the snapshot copies.
  - Set the Replication schedule to run once
  - Define how long the snapshots will be stored in the Destination
  - Clicking START REPLICATION immediately snapshots the chosen Sources and copies those snapshots to the Destination
    - Dialog might ask to delete existing snapshots from the Destination. Be sure that all important data is protected before deleting anything.
  - Clicking the task State shows the logs for that replication task.

**Quick Backups with the Replication Wizard**

TrueNAS provides a wizard for quickly configuring different simple replication scenarios.

While we recommend regularly scheduled replications to a remote location as the optimal backup scenario, the wizard can very quickly create and copy ZFS snapshots to another location on the same system. This is useful when no remote backup locations are available, or when a disk is in immediate danger of failure.

The only thing you’ll need before creating a quick local replication are datasets or zvols in a storage pool to use as the replication source and (preferably) a second storage pool to use for storing replicated snapshots. You can set up the local replication entirely in the Replication Wizard.

To open the Replication Wizard, go to Tasks > Replication Tasks and click ADD. Set the source location to the local system and pick which datasets to snapshot. The wizard takes new snapshots of the sources when no existing source snapshots are found.

Enabling Recursive replicates all snapshots contained within the selected source dataset snapshots. Local sources can also use a naming schema to identify any custom snapshots to include in the replication. A naming schema is a collection of strftime, time and date strings and any identifiers that a user might have added to the snapshot name.
Set the destination to the local system and define the path to the storage location for replicated snapshots. When manually defining the destination, be sure to type the full path to the destination location.

TrueNAS suggests a default name for the task based on the selected source and destination locations, but you can type your own name for the replication. You can load any saved replication task into the wizard to make creating new replication schedules even easier.

You can define a specific schedule for this replication or choose to run it immediately after saving the new task. Unscheduled tasks are still saved in the replication task list and can be run manually or edited later to add a schedule.

The destination lifetime is how long copied snapshots are stored in the destination before they are deleted. We usually recommend defining a snapshot lifetime to prevent storage issues. Choosing to keep snapshots indefinitely can require you to manually clean old snapshots from the system if or when the destination fills to capacity.

Clicking **START REPLICATION** saves the new task and immediately attempts to replicate snapshots to the destination. When TrueNAS detects that the destination already has unrelated snapshots, it will ask to delete the unrelated snapshots and do a full copy of the new snapshots. This can delete important data, so be sure any existing snapshots can be deleted or are backed up in another location.

The simple replication is added to the Replication task list and will show that it is currently running. Clicking the task state shows the replication log with an option to download the log to your local system.
To confirm that snapshots have been replicated, go to **Storage > Snapshots** and verify the destination dataset has new snapshots with correct timestamps.
4.6.2 - Remote

- Creating a Remote Replication Task

Configure SSH and automatic dataset snapshots in TrueNAS before creating a remote replication task. This ensures that both systems can connect to each other and new snapshots are regularly available for replication.

To streamline creating simple replication configurations, the replication wizard assists with creating a new SSH connection and automatically creates a periodic snapshot task for sources that have no existing snapshots.

Process Summary

Processes Summary

- Tasks > Replication Tasks
  - Choose sources for snapshot replication.
    - Remote sources require an SSH connection.
    - TrueNAS shows how many snapshots will be replicated.
  - Define the snapshot destination.
    - A remote destination requires an SSH connection.
    - Choose destination or define manually by typing a path.
      - Adding a new name on the end of the path creates a new dataset.
  - Choose replication security.
    - We always recommend Replication with encryption.
    - Disabling encryption is only meant for absolutely secure networks.
  - Schedule the replication.
    - Schedule can be standardized presets or a custom defined schedule.
    - Running once runs the replication immediately after creation.
      - Task is still saved and can be rerun or edited.
  - Choose how long to keep the replicated snapshots.

Creating a Remote Replication Task

To create a new replication, go to Tasks > Replication Tasks and click ADD.

You can load any saved replication to prepopulate the wizard with that configuration. Saving changes to the configuration creates a new replication task without altering the task that was loaded into the wizard. This saves some time when creating multiple replication tasks between the same two systems.

Sources

Start by configuring the replication sources. Sources are the datasets or zvols with snapshots to use for replication. Choosing a remote source requires selecting an SSH connection to that system. Expanding the directory browser shows the current datasets or zvols that are available for replication. You can select multiple sources or manually type the names into the field.
TrueNAS shows how many snapshots are available for replication. We recommend you manually snapshot the sources or create a periodic snapshot task \textit{before} creating the replication task. However, when the sources are on the local system and don’t have any existing snapshots, TrueNAS can create a basic periodic snapshot task and snapshot the sources immediately before starting the replication. Enabling \textit{Recursive} replicates all snapshots contained within the selected source dataset snapshots.

Remote sources require entering a \textit{snapshot naming schema} to identify the snapshots to replicate. A naming schema is a collection of \texttt{strftime} time and date strings and any identifiers that a user might have added to the snapshot name.

Local sources can also use a naming schema to identify any custom snapshots to include in the replication.

\textbf{Destination}

The destination is where replicated snapshots are stored. Choosing a remote destination requires an SSH connection to that system. Expanding the directory browser shows the current datasets that are available for replication. You can select a destination dataset or manually type a path in the field. Zvols cannot be used as a remote replication destination. Adding a name to the end of the path creates a new dataset in that location.

\textit{Encryption}: To use encryption when replicating data check the Encryption box. Once the box is checked additional encryption options will become available.

- \textit{Encryption Key Format} allows the user to choose between a Hex (base 16 numeral) or Passphrase
(alphanumeric) style encryption key.
- **Store Encryption key in Sending TrueNAS database** allows the user to either store the Encryption key in the sending TrueNAS database (box checked) or choose a temporary location for the encryption key that will decrypt replicated data (box unchecked).

### Security and Task Name

Using encryption for SSH transfer security is always recommended.

In situations where two systems within an absolutely secure network are used for replication, disabling encryption speeds up the transfer. However, the data is completely unprotected from malicious sources.

Choosing no encryption for the task is the same as choosing the **SSH+NETCAT** transport method from the advanced options screen. NETCAT uses common port settings, but these can be overridden by switching to the advanced options screen or editing the task after creation.

TrueNAS suggests a name based off the selected sources and destination, but this can be overwritten with a custom name.

### Schedule and Lifetime

Adding a schedule automates the task to run according to your chosen times. You can choose between a number of preset schedules or create a custom schedule for when the replication will run. Choosing to run the replication once will run the replication immediately after saving the task, but any additional replications must be triggered manually.

Finally, define how long you want to keep snapshots on the destination system. We generally recommend defining snapshot lifetime to prevent cluttering the system with obsolete snapshots.

### Starting the Replication

**Start Replication** saves the new replication task. New tasks are enabled by default and activate according to their schedule or immediately when no schedule was chosen. The first time a replication task runs, it takes longer because the snapshots must be copied entirely fresh to the destination. Later replications run faster, as only the subsequent changes to snapshots are replicated. Clicking the task state opens the log for that task.
4.6.3 - Advanced

- Creating an Advanced Replication Task

Requirements:

- Storage pools with datasets and data to snapshot.
- SSH configured with a connection to the remote system saved in **System > SSH Connections**.
- Dataset snapshot task saved in **Tasks > Periodic Snapshot Tasks**.

**Process Summary expand □**

Go to **Tasks > Replication Tasks** and click **ADD**, then select **ADVANCED REPLICAION CREATION**.

- General Options:
  - Name the task.
  - Select Push or Pull for the local system.
  - Select a replication transport method.
    - SSH is recommended.
    - SSH+Netcat is used for secured networks.
    - Local is for in-system replication.
- Configure the replication transport method:
  - Remote options require an SSH connection.
  - SSH+Netcat requires defining netcat ports and addresses.
- Sources:
  - Select sources for replication.
  - Choose a periodic snapshot task as the source of snapshots to replicate.
  - Remote sources require defining a snapshot naming schema.
- Destination:
  - Remote destination requires an SSH connection.
  - Select a destination or type a path in the field.
  - Define how long to keep snapshots in the destination.
- Scheduling:
  - Run automatically starts the replication after a related periodic snapshot task completes.
  - To automate the task according to its own schedule, set that option and define a schedule for the replication task.

**Creating an Advanced Replication Task**

To use the advanced editor to create a replication task, go to **Tasks > Replication Tasks**, click **ADD** to open the Wizard, then click **ADVANCED REPLICAION CREATION**.
Options are grouped together by category. Options can appear, disappear, or be disabled depending on the configuration choices you make. Start by configuring the General options first, then the Transport options before configuring replication Sources and Destination.

Name the task. Each task name must be unique, and we recommend you name it in a way that makes it easy to remember what the task is doing.

Choose whether the local system is sending (Push) or receiving data (Pull) and decide what Transport method to use for the replication before configuring the other sections.

○ Transport Options
The **Transport** selector determines the method to use for the replication: **SSH** is the standard option for sending or receiving data from a remote system, but **SSH+NETCAT** is available as a faster option for replications that take place within completely secure networks. **Local** is only used for replicating data to another location on the same system.

With **SSH**-based replications, configure the transport method by selecting the **SSH Connection** to the remote system that will send or receive snapshots. Options for compressing data, adding a bandwidth limit, or other data stream customizations are available. **Stream Compression** options are only available when using SSH. Before enabling **Compressed WRITE Records**, verify that the destination system also supports compressed WRITE records.

For **SSH+NETCAT** replications, you also need to define the addresses and ports to use for the Netcat connection.

![Transport Options](image)

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSH Connection</strong></td>
<td>Select the connection to the remote system that will send or receive snapshots.</td>
</tr>
<tr>
<td><strong>Stream Compression</strong></td>
<td>Options for compressing data, adding a bandwidth limit, or other data stream customizations are available. Stream Compression options are only available when using SSH. Before enabling Compressed WRITE Records, verify that the destination system also supports compressed WRITE records.</td>
</tr>
<tr>
<td><strong>Allow Blocks Larger than 128KB</strong></td>
<td>A one-way toggle. Replication tasks using large block replication will only continue to work as long as this option remains enabled.</td>
</tr>
<tr>
<td><strong>Allow Compressed WRITE Records</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Source**

The replication **Source** is the datasets or zvols to use for replication. Select the sources to use for this replication task by opening the file browser or entering dataset names in the field. Pulling snapshots from a remote source requires a valid **SSH Connection** before the file browser can show any directories. If the file browser shows a connection error after selecting the correct **SSH Connection**, you might need to log in to the remote system and make sure it is configured to allow SSH connections. In TrueNAS, this is done by going to the **Services** screen, checking the **SSH** service configuration, and starting the service.
By default, the replication task will use snapshots to quickly transfer data to the receiving system. When **Full Filesystem Replication** is set, the chosen **Source** is completely replicated, including all dataset properties, snapshots, child datasets, and clones. When choosing this option, it is recommended to allocate additional time for the replication task to run. Leaving **Full Filesystem Replication** unset but setting **Include Dataset Properties** will include just the dataset properties in the snapshots to be replicated. Additional options allow you to recursively replicate child dataset snapshots or exclude specific child datasets or properties from the replication.

Local sources are replicated by snapshots that were generated from a periodic snapshot task and/or from a defined naming schema that matches manually created snapshots. Remote sources require entering a snapshot naming schema to identify the snapshots to replicate. A naming schema is a collection of `strftime` time and date strings and any identifiers that a user might have added to the snapshot name. For example, entering the naming schema `custom-%Y-%m-%d_%H-%M` finds and replicates snapshots like `custom-2020-03-25_09-15`. Multiple schemas can be entered by pressing **Enter** to separate each schema.

To define specific snapshots from the periodic task to use for the replication, set **Replicate Specific Snapshots** and enter a schedule. The only periodically generated snapshots that will be included in the replication task are those that match your defined schedule. Alternately, you can use your **Replication Schedule** to determine which snapshots are replicated by setting **Run Automatically, Only Replicate Snapshots Matching Schedule**, and defining when the replication task will run.

When a replication task is having difficulty completing, it is a good idea to set **Save Pending Snapshots**. This prevents the source TrueNAS from automatically deleting any snapshots that are failing to replicate to the destination system.
The destination is where replicated data is stored. Choosing a remote destination requires an *SSH Connection* to that system. Expanding the file browser shows the current datasets that are available on the destination system. You can click a destination or manually type a path in the field. Adding a name to the end of the path creates a new dataset in that location.

**DO NOT** use zvols for a remote destination

By default, the destination dataset is *SET* to be *read-only* after the replication is complete. You can change the *Destination Dataset Read-only Policy* to only start replication when the destination is read-only (*REQUIRE*) or to disable checking the dataset’s read-only state (*IGNORE*).

*Encryption* adds another layer of security to replicated data by encrypting the data before transfer and decrypting it on the destination system. Setting the checkbox adds more options to choose between using a *HEX* key or defining your own encryption *PASSPHRASE*. The encryption key can be stored either in the TrueNAS system database or in a custom-defined location.

*Synchronizing Destination Snapshots With Source* destroys any snapshots in the destination that do not match the source snapshots. TrueNAS also does a full replication of the source snapshots as if the replication task had never been run before, which can lead to excessive bandwidth consumption. This can be a very destructive option, so be sure that any snapshots that will be deleted from the destination are obsolete or otherwise backed up in a different location.

Defining the *Snapshot Retention Policy* is generally recommended to prevent cluttering the system with obsolete snapshots. Choosing *Same as Source* will keep the snapshots on the destination system for the same amount of time as the defined *Snapshot Lifetime* from the source system periodic snapshot task. You can also define your own
Custom lifetime for snapshots on the destination system.

○ Schedule

By default, setting the task to *Run Automatically* starts the replication immediately after the related periodic snapshot task is complete.

Setting the *Schedule* checkbox allows scheduling the replication to run at a separate time. A specific time must be defined for the replication task to run. It is recommended to choose a time frame that both gives the replication task enough time to finish and is during a time of day when network traffic for both source and destination systems is minimal. Using the custom scheduler is recommended when you need to fine-tune an exact time or day for the replication.

### Advanced Scheduler expand □

Choosing a **Presets** option populates the rest of the fields. To customize a schedule, enter [crontab](https://en.wikipedia.org/wiki/Cron) values for the **Minutes/Hours/Days**.

These fields accept standard [cron](https://en.wikipedia.org/wiki/Cron) values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering *10* means that the job runs when the time is ten minutes past the hour.

An asterisk (*) means match all values.

Specific time ranges are set by entering hyphenated number values. For example, entering *30-35* in the **Minutes** field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.
You can also enter lists of values. Enter individual values separated by a comma (,). For example, entering 1,14 in the **Hours** field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).

A slash (/) designates a step value. For example, while entering * in **Days** means the task runs every day of the month, */2 means the task runs every other day.

Combining all the above examples together creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

There is an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days. This is in addition to any listed days. For example, entering 1 in **Days** and setting **Wed** for **Days of Week** creates a schedule that starts a task on the first day of the month and every Wednesday of the month.

The **Schedule Preview** displays when the current settings mean the task runs.

### Examples of CRON syntax

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Meaning</th>
<th>Examples</th>
</tr>
</thead>
</table>
| *      | Every item. | * (minutes) = every minute of the hour.  
* (days) = every day. |
| */N    | Every Nth item. | */15 (minutes) = every 15th minute of the hour (every quarter hour).  
*/3 (days) = every 3rd day.  
*/3 (months) = every 3rd month. |
| Comma and hyphen/dash | Each stated item (comma)  
Each item in a range (hyphen/dash). | 1,31 (minutes) = on the 1st and 31st minute of the hour.  
1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour.  
mon-fri (days) = every Monday to Friday inclusive (every weekday).  
mar,jun,sep,dec (months) = every March, June, September, December. |

Days can be specified as days of month, or days of week.

With these options, you can create flexible schedules similar to these examples:

<table>
<thead>
<tr>
<th>Desired schedule</th>
<th>Values to enter</th>
</tr>
</thead>
</table>
| 3 times a day (at midnight, 08:00 and 16:00) | months=*; days=*; hours=0/8 or 0,8,16; minutes=0  
(Meaning: every day of every month, when hours=0/8/16 and minutes=0) |
| Every Monday, Wednesday and Friday, at 8.30 pm | months=*; days=mon,wed,fri; hours=20; minutes=30 |
| 1st and 15th day of the month, during October to June, at 00:01 am | months=oct-dec,jan-jun; days=1,15; hours=0; minutes=1 |
| Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday | Note that this requires two tasks to achieve:  
(1) months=*; days=mon-fri; hours=8-18; minutes=*/15  
(2) months=*; days=mon-fri; hours=19; minutes=0  
We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00. |

Setting **Only Replicate Snapshots Matching Schedule** restricts the replication to only replicate those snapshots.
created at the same time as the replication schedule.
This article contains some advice for investigating or solving issues with a Replication task.

Using a Custom Schema

**Snapshot Tasks** that have been set up, or imported, with a custom schema name can be used for “full backup” replication tasks. Incremental replication tasks will not work.

There are several ways that a custom schema can be created:

- A ZFS dataset with snapshots has been imported into TrueNAS with a schema that doesn’t match the Truenas schema.
- A custom schema name has been created in the **Snapshot Task**. This occurs when the **Naming Schema** field in a **Periodic Snapshot Task** is used and the name of the schema is something other than the default.

Replication Task Log

To view and download the replication task log, go to **Tasks > Replication Tasks**. Click on the **state** of the replication task.
Click the **DOWNLOAD LOGS** button to download the log file.

### Editing a Replication Task

To edit the replication task, go to **Tasks > Replication Tasks**. Click the > to expand the replication task information, then click **EDIT**.
See **Replication Advanced Options** for descriptions of the available fields.

**Replication Task Alert Priorities**

To customize the importance and frequency of a Replication task alert (success or failure), go to **System > Alert Settings** and scroll down to the **Tasks** area. Set the **Warning Level** and how often the alert notification is sent.
See [Alert Settings](#) for more information about this UI screen.

**FAQ**

**Question:** If the internet connection goes down for a period of time, will the replication restart where it left off - including any intermediate snapshots? **Answer:** Yes.

**Question:** If a site changes a lot of data at one time and the internet bandwidth is not enough to finish sending the snapshot before the next one begins, will the replication jobs run one after the other and not stomp on each other? **Answer:** Yes.
4.7 - Resilver Priority

Resilvering is a process that copies data to a replacement disk and is best completed as quickly as possible. Increasing the priority of resilvers helps them finish faster. The Resilver Priority menu allows you to schedule when a resilver can become a higher priority for the system. This means scheduling resilvers when the additional I/O or CPU use does not affect normal usage.

Go to Tasks > Resilver Priority to configure the priority to a time that is most effective for your environment.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Set to run resilver tasks between the configured times.</td>
</tr>
<tr>
<td>Begin</td>
<td>Choose the hour and minute when a resilver process can run at a higher priority.</td>
</tr>
<tr>
<td>End</td>
<td>Choose the hour and minute after which a resilver process must return to running at a lower priority. A resilver process running after this time will likely take much longer to complete due to running at a lower priority compared to other disk and CPU activities, such as replications, SMB transfers, NFS transfers, Rsync transfers, S.M.A.R.T. tests, pool scrubs, user activity, etc.</td>
</tr>
<tr>
<td>Days of the Week</td>
<td>Select the days to run resilver tasks.</td>
</tr>
</tbody>
</table>

A resilver process running during the time-frame defined between “Begin Time” and “End Time” will likely work faster, as it is not being throttled to run at a lower priority. Keep in mind that it is advised to avoid putting the system under any intensive activity or heavy loads (replications, SMB transfers, NFS transfers, Rsync transfers, S.M.A.R.T. tests, pool scrubs, etc) during a resilver process.
4.8 - Scrub Tasks

- Default Scrub Tasks
- Creating New Scrub Tasks

A “scrub” is when ZFS scans the data on a pool. Scrubs identify data integrity problems, detect silent data corruptions caused by transient hardware issues, and provide early disk failure alerts.

Default Scrub Tasks

By default, TrueNAS creates a scrub task when you create a new pool. The default schedule for a scrub is to run every Sunday at 12:00 AM. To edit the default scrub, go to Tasks > Scrub Tasks, click □, and EDIT.

Creating New Scrub Tasks

A data pool must exist before creating a scrub task.

To create a scrub task for a pool, go to Tasks > Scrub Tasks and click ADD.

<table>
<thead>
<tr>
<th>Scrub Task</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool</td>
<td></td>
</tr>
<tr>
<td>Threshold days</td>
<td>35</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Schedule</td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td></td>
</tr>
</tbody>
</table>

Scrub Task

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool</td>
<td>Choose a pool to scrub.</td>
</tr>
<tr>
<td>Threshold days</td>
<td>Controls the task schedule by setting how many days must pass before a completed scrub can run again. If you schedule a scrub to run daily and set Threshold days to 7, the scrub attempts to run daily. If the scrub succeeds, it will check but won’t run again until seven days pass. Using a multiple of seven ensures the scrub runs on the same weekday.</td>
</tr>
<tr>
<td>Description</td>
<td>Describe the scrub task.</td>
</tr>
<tr>
<td>Schedule</td>
<td>How often to run the scrub task. Choose one of the presets or Custom to use the Advanced Scheduler.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Unset to disable the scheduled scrub without deleting it.</td>
</tr>
</tbody>
</table>

Advanced Scheduler expand □
Choosing a **Presets** option populates the rest of the fields. To customize a schedule, enter cron values for the Minutes/Hours/Days.

These fields accept standard cron values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering 10 means that the job runs when the time is ten minutes past the hour.

An asterisk ( *) means match all values.

Specific time ranges are set by entering hyphenated number values. For example, entering 30-35 in the Minutes field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.

You can also enter lists of values. Enter individual values separated by a comma (.). For example, entering 1,14 in the Hours field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).

A slash (/) designates a step value. For example, while entering * in Days means the task runs every day of the month, */2 means the task runs every other day.

Combining all the above examples together creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

There is an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days. This is in addition to any listed days. For example, entering 1 in Days and setting Wed for Days of Week creates a schedule that starts a task on the first day of the month and every Wednesday of the month.
The **Schedule Preview** displays when the current settings mean the task runs.

## Examples of CRON syntax

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Meaning</th>
<th>Examples</th>
</tr>
</thead>
</table>
| *      | Every item. | * (minutes) = every minute of the hour.  
|        |          | * (days) = every day.  
| */N    | Every N\textsuperscript{th} item. | */15 (minutes) = every 15th minute of the hour (every quarter hour).  
|        |          | */3 (days) = every 3rd day.  
|        |          | */3 (months) = every 3rd month.  
| Comma and hyphen/dash | Each stated item (comma)  
|          | Each item in a range (hyphen/dash). |  
|        |          | 1,31 (minutes) = on the 1st and 31st minute of the hour.  
|        |          | 1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour.  
|        |          | mon-fri (days) = every Monday to Friday inclusive (every weekday).  
|        |          | mar,jun,sep,dec (months) = every March, June, September, December.  

Days can be specified as days of month, or days of week.

With these options, you can create flexible schedules similar to these examples:

<table>
<thead>
<tr>
<th>Desired schedule</th>
<th>Values to enter</th>
</tr>
</thead>
</table>
| 3 times a day (at midnight, 08:00 and 16:00) | months=*; days=*; hours=0/8 or 0,8,16; minutes=0  
|                  | (Meaning: every day of every month, when hours=0/8/16 and minutes=0)  
| Every Monday, Wednesday and Friday, at 8.30 pm | months=*; days=mon,wed,fri; hours=20; minutes=30  
| 1st and 15th day of the month, during October to June, at 00:01 am | months=oct-dec, jan-jun; days=1,15; hours=0; minutes=1  
| Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday | Note that this requires two tasks to achieve:  
|                  | (1) months=*; days=mon-fri; hours=8-18; minutes=*/15  
|                  | (2) months=*; days=mon-fri; hours=19; minutes=0  
|                  | We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00.  

TrueNAS can send, receive, or synchronize data with a Cloud Storage provider. Cloud Sync tasks allow for single time transfers or recurring transfers on a schedule, and are an effective method to back up data to a remote location.

Using the Cloud means that data can go to a third party commercial vendor not directly affiliated with iXsystems. Please investigate and fully understand that vendor’s pricing policies and services before creating any Cloud Sync task. iXsystems is not responsible for any charges incurred from the use of third party vendors with the Cloud Sync feature.

TrueNAS supports major providers like Amazon S3, Google Cloud, and Microsoft Azure, along with a variety of other vendors. To see the full list of supported vendors, go to System > Cloud Credentials > Add and open the Provider dropdown.

Requirements

- All system Storage must be configured and ready to receive or send data.
- A Cloud Storage provider account and a cloud storage location must be available, like an Amazon S3 bucket.
- Cloud Storage account credentials must be saved to System > Cloud Credentials before creating the sync task. See Cloud Credentials for specific instructions.

Creating a Cloud Sync Task

Go to Tasks > Cloud Sync Tasks and click Add.
Give the task a memorable **Description** and select an existing cloud **Credential**. TrueNAS connects to the chosen Cloud Storage Provider and shows the available storage locations. Decide if data is transferring to (**PUSH**) or from (**PULL**) the Cloud Storage location (**Remote**). Choose a **Transfer Mode**:

- **Sync**

  **Sync** keeps all the files identical between the two storage locations. If the sync encounters an error, files are not deleted in the destination. This includes a common error when the [Dropbox copyright detector](#) flags a file as copyrighted.

Note that syncing to a Backblaze B2 bucket does not delete files from the bucket, even when those files have been deleted locally. Instead, files are tagged with a version number or moved to a hidden state. To automatically delete old or unwanted files from the bucket, adjust the [Backblaze B2 Lifecycle Rules](#).

Files stored in Amazon S3 Glacier or S3 Glacier Deep Archive cannot be deleted by a sync. These files must first be restored by another means, like the [Amazon S3 console](#).
- **Copy**
  Copy duplicates each source file into the destination, *overwriting* any files in the destination that have the same name as the source. Copying is the least potentially destructive option.

- **Move**
  Move transfers the files from the source to the destination and *deletes* the original source files. Files with the same names on the destination are overwritten.

Next, **Control** when the task runs by defining a **Schedule**. When a specific **Schedule** is required, choose **Custom** and use the **Advanced Scheduler**.

*Advanced Scheduler expand □*

Choosing a **Presets** option populates the rest of the fields. To customize a schedule, enter **crontab** values for the **Minutes/Hours/Days**.

These fields accept standard **cron** values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering **10** means that the job runs when the time is ten minutes past the hour.

An asterisk (∗) means match all values.

Specific time ranges are set by entering hyphenated number values. For example, entering **30-35** in the **Minutes** field sets the task to run at minutes 30, 31, 32, 33, 34, and 35.

You can also enter lists of values. Enter individual values separated by a comma (,). For example, entering **1,14** in the **Hours** field means the task runs at 1:00 AM (0100) and 2:00 PM (1400).
A slash ( / ) designates a step value. For example, while entering * in **Days** means the task runs every day of the month, */2 means the task runs every other day.

Combining all the above examples together creates a schedule running a task each minute from 1:30-1:35 AM and 2:30-2:35 PM every other day.

There is an option to select which **Months** the task runs. Leaving each month unset is the same as selecting every month.

The **Days of Week** schedules the task to run on specific days. This is in addition to any listed days. For example, entering 7 in **Days** and setting **Wed** for Days of Week creates a schedule that starts a task on the first day of the month and every Wednesday of the month.

The **Schedule Preview** displays when the current settings mean the task runs.

**Examples of CRON syntax**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Meaning</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Every item.</td>
<td>* (minutes) = every minute of the hour. * (days) = every day.</td>
</tr>
<tr>
<td>*/N</td>
<td>Every Nth item.</td>
<td>*/15 (minutes) = every 15th minute of the hour (every quarter hour). */3 (days) = every 3rd day. */3 (months) = every 3rd month.</td>
</tr>
<tr>
<td>Comma and hyphen/dash</td>
<td>Each stated item (comma) Each item in a range (hyphen/dash).</td>
<td>1,31 (minutes) = on the 1st and 31st minute of the hour. 1-3,31 (minutes) = on the 1st to 3rd minutes inclusive, and the 31st minute, of the hour. mon-fri (days) = every Monday to Friday inclusive (every weekday). mar,jun,sep,dec (months) = every March, June, September, December.</td>
</tr>
</tbody>
</table>

Days can be specified as days of month, or days of week.

With these options, you can create flexible schedules similar to these examples:

<table>
<thead>
<tr>
<th>Desired schedule</th>
<th>Values to enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 times a day (at midnight, 08:00 and 16:00)</td>
<td>months=<em>; days=</em>; hours=0/8 or 0,8,16; minutes=0 (Meaning: every day of every month, when hours=0/8/16 and minutes=0)</td>
</tr>
<tr>
<td>Every Monday, Wednesday and Friday, at 8.30 pm</td>
<td>months=*; days=mon,wed,fil; hours=20; minutes=30</td>
</tr>
<tr>
<td>1st and 15th day of the month, during October to June, at 00:01 am</td>
<td>months=oct-dec,jan-jun; days=1,15; hours=0; minutes=1</td>
</tr>
<tr>
<td>Every 15 minutes during the working week, which is 8am - 7pm (08:00 - 19:00) Monday to Friday</td>
<td>Note that this requires two tasks to achieve:  (1) months=<em>; days=mon-fri; hours=8-18; minutes=</em>/15  (2) months=*; days=mon-fri; hours=19; minutes=0  We need the second scheduled item, to execute at 19:00, otherwise we would stop at 18:45. Another workaround would be to stop at 18:45 or 19:45 rather than 19:00.</td>
</tr>
</tbody>
</table>

Unsetting **Enable** makes the configuration available without allowing the **Schedule** to run the task. To manually activate a saved task, go to **Tasks > Cloud Sync Tasks**, click ▼ to expand a task, and click **RUN NOW**.

The remaining options allow tuning the task to your specific requirements.
### Specific Options

#### Transfer

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a description of the Cloud Sync Task.</td>
</tr>
<tr>
<td>Direction</td>
<td>PUSH sends data to cloud storage. PULL receives data from cloud storage. Changing the direction resets the Transfer Mode to COPY.</td>
</tr>
<tr>
<td>Transfer Mode</td>
<td>SYNC: Files on the destination are changed to match those on the source. If a file does not exist on the source, it is also deleted from the destination. COPY: Files from the source are copied to the destination. If files with the same names are present on the destination, they are overwritten. MOVE: After files are copied from the source to the destination, they are deleted from the source. Files with the same names on the destination are overwritten.</td>
</tr>
<tr>
<td>Directory/Files</td>
<td>Select the directories or files to be sent to the cloud for Push syncs, or the destination to be written for Pull syncs. Be cautious about the destination of Pull jobs to avoid overwriting existing files.</td>
</tr>
</tbody>
</table>

#### Remote

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential</td>
<td>Select the cloud storage provider credentials from the list of available Cloud Credentials.</td>
</tr>
</tbody>
</table>

#### Control

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule</td>
<td>Select a schedule preset or choose Custom to open the advanced scheduler.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enable this Cloud Sync Task. Unset to disable this Cloud Sync Task without deleting it.</td>
</tr>
</tbody>
</table>

#### Advanced Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Follow Symlinks</td>
<td>Follow symlinks and copy the items to which they link.</td>
</tr>
<tr>
<td>Pre-Script</td>
<td>Script to execute before running sync.</td>
</tr>
<tr>
<td>Post-Script</td>
<td>Script to execute after running sync.</td>
</tr>
</tbody>
</table>
| Exclude      | List of files and directories to exclude from sync. Separate entries by pressing Enter. Examples of proper syntax used to exclude files/directories are:  
  - photos will exclude a file named “photos”  
  - /photos will exclude a file named “photos” from root directory (but not subdirectories)  
  - photos/ will exclude a directory named “photos”  
  - /photos/ will exclude a directory named “photos” from root directory (but not subdirectories).  
See rclone filtering for more details about the --exclude option. |

#### Advanced Remote Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUSH</td>
<td>Encrypt files before transfer and store the encrypted files on the remote system. Files are</td>
</tr>
</tbody>
</table>
Remote Encryption

Files that are encrypted using the Encryption Password and Encryption Salt values. **PULL**: Decrypt files that are being stored on the remote system before the transfer. Transferring the encrypted files requires entering the same Encryption Password and Encryption Salt that was used to encrypt the files. Additional details about the encryption algorithm and key derivation are available in the [rclone crypt](https://rclone.org/crypt/) documentation.

Transfers

Number of simultaneous file transfers. Enter a number based on the available bandwidth and destination system performance. See [rclone --transfers](https://rclone.org/).

Bandwidth limit

A single bandwidth limit or bandwidth limit schedule in rclone format. Separate entries by pressing Enter. Example: 08:00,512 12:00,10MB 13:00,512 18:00,30MB 23:00,off. Units can be specified with the beginning letter: b, k (default), M, or G. See [rclone --bwlimit](https://rclone.org/).

**Scripting and Environment Variables**

Advanced users can write scripts that run immediately **before** or **after** the Cloud Sync task. The **Post-script** field is only run when the Cloud Sync task successfully completes. You can pass a variety of task environment variables into the **Pre-** and **Post-** script fields:

- CLOUD_SYNC_ID
- CLOUD_SYNC_DESCRIPTION
- CLOUD_SYNC_DIRECTION
- CLOUD_SYNC_TRANSFER_MODE
- CLOUD_SYNC_ENCRYPTION
- CLOUD_SYNC_FILENAME_ENCRYPTION
- CLOUD_SYNC_ENCRYPTION_PASSWORD
- CLOUD_SYNC_ENCRYPTION_SALT
- CLOUD_SYNC_SNAPSHOT

There also are provider-specific variables like CLOUD_SYNC_CLIENT_ID or CLOUD_SYNC_TOKEN or CLOUD_SYNC_CHUNK_SIZE

Remote storage settings:

- CLOUD_SYNC_BUCKET
- CLOUD_SYNC_FOLDER

Local storage settings:

- CLOUD_SYNC_PATH

**Testing Settings**

Test the settings before saving by clicking **DRY RUN**. TrueNAS connects to the Cloud Storage Provider and simulates a file transfer. No data is actually sent or received. A dialog shows the test status and allows downloading the task logs.
Cloud Sync Behavior

Saved tasks are activated according to their schedule or by clicking **RUN NOW**. An in-progress cloud sync must finish before another can begin. Stopping an in-progress task cancels the file transfer and requires starting the file transfer over.

To view logs about a running or the most recent run of a task, click the task status.

Cloud Sync Restore
To quickly create a new Cloud Sync that uses the same options but reverses the data transfer, expand () an existing Cloud Sync and click **RESTORE**.

Enter a new **Description** for this reversed task and define the path to a storage location for the transferred data.

The restored cloud sync is saved as another entry in **Tasks > Cloud Sync Tasks**.

In case the restore destination dataset is the same as the original source dataset, the restored files might have their ownership altered to **root**. If the original files were not created by **root** and a different owner is required, you can recursively reset ACL Permissions of the restored dataset through the GUI or by running `chown` from the CLI.
4.10 - How To Back Up Google Drive to TrueNAS CORE

Google Drive and G Suite are widely used to create and share documents, spreadsheets, and presentations with team members. While cloud-based tools have inherent backups and replications included by the cloud provider, certain users may require additional backup or archive capabilities. For example, companies using G Suite for important work may need to keep records for years, potentially beyond the scope of the G Suite subscription. TrueNAS can easily back up Google Drive using its built-in cloud sync.

**Setting up Google Drive credentials**

Go to **System > Cloud Credentials** and click **ADD**. Name the Credential and select **Google Drive** as the Provider. Click **LOGIN TO PROVIDER** and log in with the appropriate Google user account.

Google will request permission to access all the Google Drive files for the FreeNAS device.
Authorization

Only proceed if you are setting up cloud sync on your TrueNAS system at http://192.168.1.123/ui/system/cloudcredentials/add

Proceed
Choose an account to continue to FreeNAS

JT Pennington  
jt@ixsystems.com

Jt Pennington  
jt@obs-sec.com

Use another account

Before using this app, you can review FreeNAS's privacy policy and terms of service.
FreeNAS wants to access your Google Account

This will allow FreeNAS to:

- See, edit, create, and delete all of your Google Drive files
- Send email on your behalf

Make sure you trust FreeNAS

You may be sharing sensitive info with this site or app. Learn about how FreeNAS will handle your data by reviewing its privacy policies. You can always see or remove access in your Google Account.

Learn about the risks

Cancel

Allow
Allow access and the appropriate access key will generate in the FreeNAS access token. You may assign a Team ID if necessary.

Click **VERIFY CREDENTIAL** and wait for it to verify.

Once successful, click **SUBMIT**. The new cloud credentials will be visible in the web interface.

**Set the cloud sync task**

Go to **Tasks > Cloud Sync Tasks** and set the backup time frame, frequency, and folders – both the cloud-based folder and TrueNAS dataset. Set whether the synchronization should sync all changes, copy new files, or move files. Files are removed from the cloud source or TrueNAS source depending on if the task is set to push or pull. Add a description for the task and select the cloud credentials. Choose the appropriate cloud folder target and TrueNAS storage location.

Select the file transfer mode:

- **Sync**: Keep files newly created or deleted the same.
- **Copy**: Copy new files to the appropriate target (i.e., TrueNAS pulls files from Google Drive or pushes files to Google Drive).
- **Move**: Copy files to the target and then delete them from the source. Using Move, users can set a folder in Google Drive for archival, and move older documents to that folder from their Drive account. Those files would then automatically get backed up to their TrueNAS storage.
Once you create the task, attempt a Dry Run.
If the Dry Run succeeds, click **SAVE** to save the task.

Expand the section down to see the options for the task.
Clicking **RUN NOW** will prompt the task to start immediately.
The web interface will show the status as **RUNNING** and **SUCCESS** upon completion. Details can be accessed via the Task Manager icon in the upper right-hand corner. While the task is running, clicking on the **RUNNING** button will reveal a popup log.

Once the sync reports a **SUCCESS** status, you can verify it by opening the folder on another computer if it is a share, through SSH access, or by checking the destination directory through the TrueNAS CLI.
Working with Google created content

One caveat is that Google Docs and other files created with Google tools have their own proprietary set of permissions and their read/write characteristics unknown to the system over a standard file share. Files are unreadable as a result.

To allow Google created files to become readable, allow link sharing to access the files before the backup. Doing so ensures that other users can open the files with read access, make changes, and then save as another file if further edits are needed. Note that this is only necessary if the file was created using Google Docs, Google Sheets, or Google
TrueNAS is perfect for storing content, including cloud-based content, for the long-term. Not only is it simple to sync and backup from the cloud, but users can rest assured that their data is safe, with snapshots, copy-on-write, and built-in replication functionality.
5 - Network

5.1 - Network Summary

It is recommended to set up your system connections before setting up data sharing. This allows integrating TrueNAS into your specific security and network environment before attempting to store or share critical data.

Network Summary

The Network Summary gives a concise overview of the current network setup. Information about the currently active Interfaces, Default Routes, and Nameservers is provided. These areas are not editable.

- **Interfaces** shows any configured physical, LAGG, Bridge, and VLAN interfaces. All detected physical interfaces are listed, even when unconfigured. The IPv4 or IPv6 address displays when a Static IP is saved for an interface.

- **Default Routes** lists all saved TrueNAS Default Routes. Go to Network > Global Configuration to configure Default Routes.

- **Nameservers** lists any configured DNS name servers that TrueNAS uses. To change this list, go to Network > Global Configuration. The TrueNAS Hostname and Domain, Default Gateway, and other options are available in Network > Global Configuration.

Additional Network Configuration Screens

Define any Static Routes in Network > Static Routes.

Out of Band Management is managed from Network > IPMI. This option is visible only when TrueNAS detects the appropriate physical hardware.
5.2 - Global Configuration

- Global Configuration Settings
  - Hostname and Domain
  - Service Announcement
  - DNS Servers
  - Default Gateway
  - Other Settings

Network > Global Configuration has all the general TrueNAS networking settings that are not specific to any interface.

Disruptive Change

Making changes to the network interface the web interface uses can result in losing connection to TrueNAS! Fixing any misconfigured network settings might require command line knowledge or physical access to the TrueNAS system.

Global Configuration Settings

Options are organized into several categories.
Can these options be configured elsewhere? expand □
Many of these Interface, DNS, and Gateway options are also configured in the Console Setup Menu. Be sure to check both locations when troubleshooting network connectivity issues.

Hostname and Domain

Many of these fields have default values, but can be changed to meet requirements of the local network. The Hostname and Domain display in the Dashboard > System Information card. Some options only display when the appropriate hardware is present.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>string</td>
<td>Host name of first TrueNAS controller. Upper and lower case alphanumeric, ., and - characters are allowed.</td>
</tr>
<tr>
<td>Hostname (TrueNAS Controller 2)</td>
<td>string</td>
<td>Host name of second TrueNAS controller (for HA only). Upper and lower case alphanumeric, ., and - characters are allowed.</td>
</tr>
<tr>
<td>Hostname (Virtual)</td>
<td>string</td>
<td>Virtual host name. When using a virtualhost, this is also used as the Kerberos principal name. Enter the fully qualified hostname plus the domain name. Upper and lower case alphanumeric, ., and - characters are allowed.</td>
</tr>
<tr>
<td>Domain</td>
<td>string</td>
<td>System domain name.</td>
</tr>
<tr>
<td>Additional Domains</td>
<td>string</td>
<td>Additional domains to search. Separate entries by pressing Enter. Adding search domains can cause slow DNS lookups</td>
</tr>
</tbody>
</table>

Service Announcement

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetBIOS-NS</td>
<td>checkbox</td>
<td>Legacy NetBIOS name server. Advertises the SMB service NetBIOS Name. Can be required for legacy SMB1 clients to discover the server. When advertised, the server appears in Network Neighborhood.</td>
</tr>
<tr>
<td>mDNS</td>
<td>checkbox</td>
<td>Multicast DNS. Uses the system Hostname to advertise enabled and running services. For example, this controls if the server appears under Network on MacOS clients.</td>
</tr>
<tr>
<td>WS-Discovery</td>
<td>checkbox</td>
<td>Uses the SMB Service NetBIOS Name to advertise the server to WS-Discovery clients. This causes the computer to appear in the Network Neighborhood of modern Windows OSes.</td>
</tr>
</tbody>
</table>

DNS Servers

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nameserver 1</td>
<td>IP address</td>
<td>Primary DNS server.</td>
</tr>
<tr>
<td>Nameserver 2</td>
<td>IP address</td>
<td>Secondary DNS server.</td>
</tr>
<tr>
<td>Nameserver 3</td>
<td>IP address</td>
<td>Tertiary DNS server.</td>
</tr>
</tbody>
</table>

Default Gateway

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Default Gateway</td>
<td>IP address</td>
<td>Typically not set. If set, used instead of the default gateway provided by DHCP</td>
</tr>
<tr>
<td>IPv6 Default Gateway</td>
<td>IP address</td>
<td>Typically not set.</td>
</tr>
</tbody>
</table>
## Other Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Proxy</td>
<td>string</td>
<td>Enter the proxy information for the network in the format <code>http://my.proxy.server:3128</code> or <code>http://user:password@my.proxy.server:3128</code>.</td>
</tr>
<tr>
<td>Enable Netwait Feature</td>
<td>checkbox</td>
<td>Setting this prevents network services from starting until the interface can ping the addresses listed in the <strong>Netwait IP list</strong>.</td>
</tr>
<tr>
<td>Netwait IP List</td>
<td>string</td>
<td>Only appears when <strong>Enable Netwait Feature</strong> is set. Enter a list of IP addresses to ping. Separate entries by pressing Enter. Each address is tried until one is successful or the list is exhausted. Leave empty to use the default gateway.</td>
</tr>
<tr>
<td>Host Name Database</td>
<td>string</td>
<td>Used to add one entry per line which will be appended to <code>/etc/hosts</code>. Separate entries by pressing Enter. Use the format <code>IP_address space hostname</code> where multiple hostnames can be used if separated by a space. Hosts defined here are still accessible by name even when DNS is not available. See <a href="#">hosts</a> for additional information.</td>
</tr>
</tbody>
</table>
5.3 - Interfaces

The TrueNAS CORE Interfaces section displays interface names and IP addresses, as well as their types and link states.

Adding, Editing, and Deleting Interfaces

To add a new network interface, click **ADD**.

To edit or delete an interface, click the more_vert in that interface’s row, then click **edit** or delete **DELETE**.

You can click **edit** on a phyiscal interface to set a static IP address for the TrueNAS UI.

You can also edit your TrueNAS system’s physical NICs by clicking delete **RESET CONFIGURATION**.

Be careful when configuring the network interface that controls the TrueNAS® web interface or you may lose web connectivity.

Creating LAGG, Bridge, and VLAN Interfaces

<table>
<thead>
<tr>
<th>Why should I use different interface types? expand □</th>
</tr>
</thead>
</table>

**LAGG (Link Aggregation)**

You should use LAGG if you want to optimize multi-user performance, balance network traffic, or have network failover protection.

For example, Failover LAGG prevents a network outage by dynamically reassigning traffic to another interface when one physical link (a cable or NIC) fails.

**Network Bridge**

You should use a Bridge if you want to enable communication between two networks and provide a way for them to work as a single network.

For example, bridges can serve IPs to multiple VMs on one interface, which allows your VMs to be on the same network as the host.

LAGG

A Link Aggregation (LAGG) is a general method of combining (aggregating) multiple network connections in parallel or a series to provide additional bandwidth or redundancy for critical networking situations. TrueNAS uses lagg(4) to manage LAGGs.

To set up a LAGG interface, go to Network > Interface > Add.
Set the **Type** to **Link Aggregation**.

Enter a name for the interface. The name must use the format `laggX`, where `X` is a number representing a non-parent interface. It is also recommended to add any notes or reminders about this particular LAGG in the **Description**.

Under **LAGG Settings**, set the **Lag Protocol** to configure the interface ports to match your networking needs:

**LACP**
LACP is the most commonly used LAGG protocol and is one part of [IEEE specification 802.3ad](https://standards.ieee.org/). In LACP mode, negotiation is performed with the network switch to form a group of ports that are all active at the same time. The network switch must support LACP for this option to function.

**Failover**
Failover causes traffic to be sent through the primary interface of the group. If the primary interface fails, traffic diverts to the next available interface in the LAGG.

**Load Balance**
Load Balance accepts inbound traffic on any port of the LAGG group and then balances the outgoing traffic on the
active ports in the LAGG group. It is a static setup that does not monitor the link state nor does it negotiate with the switch.

**RoundRobin**

Round robin accepts inbound traffic on any port of the LAGG group and sends outbound traffic using a round robin scheduling algorithm. Traffic is sent out in sequence using each LAGG interface in turn.

**None**

This mode disables traffic on the LAGG interface without disabling the LAGG interface.

Now define the *Lagg Interfaces* and review the remaining interface options.

**Other Settings**

Every kind of network interface has common settings:

- **Disable Hardware Offloading**
- **MTU**
- **1500**

Disabling *Hardware Offloading* is discouraged as it can reduce network performance. However, disabling this option might be needed when the interface is managing *Jails*, *Plugins*, or *Virtual Machines*.

The Maximum Transmission Unit (MTU) is the largest protocol data unit that can be communicated. What the largest workable MTU size can be will change according to your available network interfaces and other physical hardware. *1500* and *9000* are standard Ethernet MTU sizes and the recommendation is to use the default *1500*. The permissible range of MTU values is *1492-9216*. Leaving this field blank sets the default value of *1500*.

If additional tuning is needed, you can enter additional *ifconfig* settings in the **Options**

**IP Addresses**

Additional aliases for the interface can also be defined:

Either IPv4 or IPv6 addresses and subnets from *1-32* can be defined. Clicking *Add* will provide another field for defining an IP address.

- **Bridge**

A *Bridge* generally refers to various methods of combining (aggregating) multiple network connections into a single aggregate network. TrueNAS uses *bridge(4)* to manage Bridges.
To set up a bridge interface, go to **Network > Interface > Add**.

Set the **Type** to *Bridge* and enter a name for the interface. The name must use the format *bridgeX*, where *X* is a number representing a non-parent interface. It is also recommended to add any notes or reminders about this particular bridge in the **Description**.

Under **Bridge Settings**, select which interfaces will be **Bridge Members** and then configure the remaining interface options to match your networking needs.

### Other Settings

Every kind of network interface has common settings:
Disabling *Hardware Offloading* is discouraged as it can reduce network performance. However, disabling this option might be needed when the interface is managing [Jails](#), [Plugins](#), or [Virtual Machines](#).

The Maximum Transmission Unit (MTU) is the largest protocol data unit that can be communicated. What the largest workable MTU size can be will change according to your available network interfaces and other physical hardware. 1500 and 9000 are standard Ethernet MTU sizes and the recommendation is to use the default 1500. The permissible range of MTU values is 1492-9216. Leaving this field blank sets the default value of 1500.

If additional tuning is needed, you can enter additional `ifconfig` settings in the **Options**

### IP Addresses

Additional aliases for the interface can also be defined:

Either IPv4 or IPv6 addresses and subnets from 1-32 can be defined. Clicking `Add` will provide another field for defining an IP address.

**VLAN**

A virtual LAN (VLAN) is a domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). More information on VLANs can be found [here](#). TrueNAS uses `vlan(4)` to manage VLANS.

To set up a VLAN interface, go to **Network > Interface > Add**.
Set the **Type** to **VLAN** and enter a **Name** for the interface. The name must use the format `vlanX`, where `X` is a number representing a non-parent interface. It is also recommended to add any notes or reminders about this particular VLAN in the **Description**.

Enabling **DHCP** or **Autoconfigure IPv6** requires understanding how this new interface will function inside your particular network environment. By default, TrueNAS allows only one network interface to have **DHCP** enabled.

The remaining **VLAN Settings** must be configured for the interface to function properly:

- **Parent Interface** : Select the VLAN Parent Interface. This is usually an Ethernet card connected to a switch port that has already been configured for the VLAN.
- **Vlan Tag** : Enter a numeric tag for this interface. This is usually preconfigured in the switched network.
- **Priority Code Point** : Define the VLAN **Class of Service**. The available 802.1p class of service ranges from **Best effort (default)** to **Network control (highest)**.

With the VLAN-specific options set, there are a few additional interfaces options to review.

**Other Settings**
Every kind of network interface has common settings:

Disabling **Hardware Offloading** is discouraged as it can reduce network performance. However, disabling this option might be needed when the interface is managing [Jails](#), [Plugins](#), or [Virtual Machines](#).

The Maximum Transmission Unit (MTU) is the largest protocol data unit that can be communicated. What the largest workable MTU size can be will change according to your available network interfaces and other physical hardware. **1500** and **9000** are standard Ethernet MTU sizes and the recommendation is to use the default **1500**. The permissible range of MTU values is **1492-9216**. Leaving this field blank sets the default value of **1500**.

If additional tuning is needed, you can enter additional `ifconfig` settings in the **Options**

### IP Addresses

Additional aliases for the interface can also be defined:

Either IPv4 or IPv6 addresses and subnets from **1-32** can be defined. Clicking **Add** will provide another field for defining an IP address.
5.3.1 - Setting a Static IP Address for the TrueNAS UI

Disruptive Change

Making changes to the network interface the web interface uses can result in losing connection to the TrueNAS system! Fixing any misconfigured network settings might require command line knowledge or physical access to the TrueNAS system.

Process Summary

- Web UI
  - Network > Interfaces > Add or Edit
    - Type address into IP Address and select a subnet mask.
    - Add or Delete additional addresses as needed.
  - Test saved changes before permanently applying them.
    - Dialog asks to temporarily apply changes.
    - After applying the changes, you have an adjustable amount of time to verify the new settings work before permanently saving over the previous configuration.
  - Network > Network Summary summarizes addressing information of every configured interface.
- Console menu
  - Physical Interfaces: select Configure Network Interfaces (options are similar for other interface types)
    - Delete interface? n
    - Remove interface settings? n
    - Configure IPv4? y
      - Enter IP address and subnet mask
    - Configure IPv6 y
      - Enter IP address
    - Configure failover? n
  - Saving changes interrupts the web interface and could require a system reboot.

Setting Static IP Addresses

TrueNAS can configure physical network interfaces with static IP addresses in either the web interface or the system console menu.

Using the web interface for this process is recommended. There are additional safety features to prevent saving misconfigured interface settings.

Adding Static IP Addresses Using the Web Interface

Log in to the web interface and go to Network > Interfaces. This contains creation and configuration options for physical and virtual network interfaces.

You can configure static IP addresses while creating or editing an interface.
High Availability must be disabled on TrueNAS Enterprise systems before an active interface can be edited.

Type the desired address in the **IP Address** field and select a subnet mask.

Multiple interfaces cannot be members of the same subnet. See [Multiple network interfaces on a single subnet](#) for more information. Check the subnet mask if an error is shown when setting the IP addresses on multiple interfaces.

Use the buttons to **Add** and **Delete** more IP addresses as needed.

To avoid permanently saving invalid or unusable settings, network changes are applied temporarily. Saving any interface changes adds a dialog to the **Network > Interfaces** list to apply these changes.

You can adjust how long to test the network changes before they are reverted back to the previous settings. If the test is successful, another dialog allows making the network changes permanent.

To quickly view system networking settings, go to **Network > Network Summary**.
Using the System Console Menu to Assign Static IP Addresses to a Physical Interface

A monitor and keyboard attached to the system is needed to use the console, or, if the system hardware allows it, you can connect with IPMI. The console menu is shown when the system is fully booted.

Use the Configure Network Interfaces option to add static IP addresses to a physical interface. Other interface types have a similar process to add static IP addresses. Interfaces that were already configured for DHCP will have that option disabled. There are a number of prompts to answer before a static address can be added. This example shows adding static IPv4 addresses to interface igb0:

```
Enter an option from 1-11: 1
  1) igb0
  2) igb1
Select an interface (q to quit): 1
Delete interface? (y/n) n
Remove the current settings of this interface? (This causes a momentary disconnection of the network.) (y/n) n
Configure IPv4? (y/n) y
Interface name:
Several input formats are supported
Example 1 CIDR Notation:
  192.168.1.1/24
Example 2 IP and Netmask separate:
  IP: 192.168.1.1
  Netmask: 255.255.255.0, /24 or 24
IPv4 Address:10.238.15.194/22
Saving interface configuration: Ok
Configure IPv6? (y/n) n
Configure failover settings? (y/n) n
Restarting network: ok
Restarting routing: ok
```

Saving interface configuration changes will disrupt the web interface while system networking restarts. When the interface being changed is also the interface that provides the web interface, a system reboot could be required for the new settings to take effect and the web interface to become available again.
5.3.2 - Editing a Physical Interface

- **Interface Editing**
  - Interface Settings
  - Other Settings
  - IP Addresses
  - Saving Changes

**Interface Editing**

Be careful when configuring the network interface that controls the TrueNAS® web interface or you may lose web connectivity.

**Network > Interfaces** lists all the physical Network Interface Controllers (NICs) connected to your TrueNAS® system.

To edit an interface, click next to it to expand the view and provide a general description about the chosen interface, then click **EDIT**.

If you are a TrueNAS Enterprise customer, remember that you cannot edit an interface if High Availability (HA) is enabled. Go to **System > Failover** and check the **Disable Failover** box, then click **SAVE**.

An interface’s editing options are dependent on the **Type** of interface that you are modifying.

**Interface Settings**
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>string</td>
<td>Notes or explanatory text about this interface.</td>
</tr>
<tr>
<td>DHCP</td>
<td>checkbox</td>
<td>Enable DHCP to auto-assign an IPv4 address to this interface. Leave unset to create a static IPv4 or IPv6 configuration. Only one interface can be configured for DHCP.</td>
</tr>
<tr>
<td>Autoconfigure IPv6</td>
<td>checkbox</td>
<td>Automatically configure the IPv6 address with rtsol. Only one interface can be configured this way.</td>
</tr>
</tbody>
</table>

### Other Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Hardware Offloading</td>
<td>checkbox</td>
<td>Turn off hardware offloading for network traffic processing. WARNING: disabling hardware offloading can reduce network performance and is only recommended when the interface is managing jails, plugins, or virtual machines (VMs).</td>
</tr>
<tr>
<td>MTU</td>
<td>string</td>
<td>Maximum Transmission Unit, the largest protocol data unit that can be communicated. The largest workable MTU size varies with network interfaces and equipment. 1500 and 9000 are standard Ethernet MTU sizes. Leaving blank restores the field to the default value of 1500.</td>
</tr>
<tr>
<td>Options</td>
<td>string</td>
<td>Additional parameters from ifconfig. Separate multiple parameters with a space. For example: mtu 9000 increases the MTU for interfaces which support jumbo frames.</td>
</tr>
</tbody>
</table>

### IP Addresses

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>integer and drop-down menu</td>
<td>Static IPv4 or IPv6 address and subnet mask. Example: 10.0.0.3 and /24. Click add another IP address. Clicking DELETE removes that IP Address.</td>
</tr>
</tbody>
</table>

### Saving Changes

After you’re done editing, click SAVE. You have the option to TEST CHANGES or REVERT CHANGES. The default time for testing any changes is 60 seconds, but you can change it to your desired setting.

After clicking TEST CHANGES, confirm your choice and click TEST CHANGES again.
Users can either SAVE CHANGES or REVERT CHANGES. A user will have the time they specified to make their choice. If you select SAVE CHANGES, a dialog box will ask you to CANCEL or SAVE network interface changes. Click SAVE.

The system will display a dialog box to show that Network interface changes have been made permanent.
Network interface changes have been made permanent.
5.4 - Static Routes

By default, no static routes are defined on a default TrueNAS system. If a static route is required to reach portions of the network, add the route by going to **Network > Static Routes** and clicking **ADD**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>integer</td>
<td>Use the format <strong>A.B.C.D/E</strong> where <strong>E</strong> is the CIDR mask.</td>
</tr>
<tr>
<td>Gateway</td>
<td>integer</td>
<td>Enter the IP address of the gateway.</td>
</tr>
<tr>
<td>Description</td>
<td>string</td>
<td>Notes or identifiers describing the route.</td>
</tr>
</tbody>
</table>
5.5 - Enabling WireGuard

WireGuard is a popular option in the VPN marketplace due to its speed, simplicity, and modern cryptography standards. Starting with FreeNAS version 11.3-RC1 and continuing through TrueNAS 12.0, it is possible to connect your NAS directly to a WireGuard network with a few easy steps.

Start by creating some custom tunables to enable the service and give it a default interface. Log in to the TrueNAS web interface and go to System > Tunables > Add. Use these settings to enable the service:

- **Variable** = wireguard_enable
- **Value** = YES
- **Type** = rc.conf

Next, create another tunable to define the networking interface:

- **Variable** = wireguard_interfaces
- **Value** = wg0
- **Type** = rc.conf
When finished, you will have these two variables set and enabled:

Next, we need a post-init script that places the WireGuard config in the correct location at startup. Go to **Tasks > Init/Shutdown Scripts** and click **Add**. Configure the script to load the WireGuard `.conf` file each time the system boots:

- **Type** = Command
- **Command** = `mkdir -p /usr/local/etc/wireguard && cp /root/wg0.conf /usr/local/etc/wireguard/wg0.conf && /usr/local/etc/rc.d/wireguard start`
- **When** = Post Init

You can configure the `/root/wg0.conf` file and apply a WireGuard configuration to attach to whatever WireGuard network you define. It can be a single point-to-point to anything running WireGuard or even use full routing. Example use cases are:

- Access data on a NAS from your Remote Laptop
- Linking NAS to NAS for replication
- Attaching a managed NAS to a remote network
Access to your NAS from your smartphone

Now create the `/root/wg0.conf` that contains the specific WireGuard configuration to apply at boot. This file settings are dependent on your specific networking environment and requirements, which is beyond the scope of this article. There are quickstart guides and tutorials available online as well as the built-in `wg-quick` manpage.

Once you have a valid `/root/wg0.conf`, rebooting the system brings up the WireGuard interface and you’ll see a `wg0` device in the output of `ifconfig`.

```
# ifconfig wg0
wg0: flags=8051<UP,POINTOPOINT,UPDATING,RUNNING,MULTICAST> metric 0 mtu 1420
    options=8000<LINKSTATE>
    inet 192.168.X.X --> 192.168.X.X netmask 0xffffff00
    nd6 options=101<PERFORMNUD,NO_DAD>
    groups: tun
    Opened by PID 1734
```

Congratulations, you have successfully linked your TrueNAS system to a secure WireGuard tunnel!
5.6 - IPMI

IPMI requires compatible hardware! Refer to your hardware documentation to determine if this option will appear in the TrueNAS web interface.

Many TrueNAS Storage Arrays provide a built-in out-of-band management port which can be used to provide side-band management should the system become unavailable through the web interface. This allows for a few vital functions, such as checking the log, accessing the BIOS setup, and powering on the system without requiring physical access to the system. It can also be used to allow another person remote access to the system to assist with a configuration or troubleshooting issue.

Some IPMI implementations require updates to work with newer versions of Java. See PSA: Java 8 Update 131 breaks ASRock’s IPMI Virtual console for more information.

IPMI is configured from Network > IPMI. The IPMI configuration screen provides a shortcut to the most basic IPMI configuration.

**IPMI Configuration**

These options are available:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrueNAS Controller</td>
<td>drop-down menu</td>
<td>Select a TrueNAS controller. All IPMI changes are applied to that TrueNAS controller.</td>
</tr>
<tr>
<td>Channel</td>
<td>drop-down menu</td>
<td>Select the communications channel to use. Available channel numbers vary by hardware.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td><strong>string</strong></td>
<td>Enter the password used to connect to the IPMI interface from a web browser. The maximum length accepted in the UI is 20 characters, but different hardware might require shorter passwords.</td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>DHCP</strong></td>
<td><strong>checkbox</strong></td>
<td>If left unset, IPv4 Address, IPv4 Netmask, and Ipv4 Default Gateway must be set.</td>
</tr>
<tr>
<td><strong>IPv4 Address</strong></td>
<td><strong>string</strong></td>
<td>IP address used to connect to the IPMI web interface.</td>
</tr>
<tr>
<td><strong>IPv4 Netmask</strong></td>
<td><strong>drop-down menu</strong></td>
<td>Subnet mask associated with the IP address.</td>
</tr>
<tr>
<td><strong>IPv4 Default Gateway</strong></td>
<td><strong>string</strong></td>
<td>Default gateway associated with the IP address.</td>
</tr>
<tr>
<td><strong>VLAN ID</strong></td>
<td><strong>string</strong></td>
<td>Enter the VLAN identifier if the IPMI out-of-band management interface is not on the same VLAN as management networking.</td>
</tr>
<tr>
<td><strong>IDENTIFY LIGHT</strong></td>
<td><strong>button</strong></td>
<td>Show a dialog to activate an IPMI identify light on the compatible connected hardware.</td>
</tr>
</tbody>
</table>

**IPMI Options**

After saving the configuration, the IPMI interface is accessed using a web browser and the IP address specified in **Network > IPMI**. The management interface prompts for login credentials. Refer to your IPMI device documentation to learn the default administrator account credentials.

After logging in to the management interface, the default administrative user name can be changed and additional IPMI users created. The appearance of the IPMI utility and the functions that are available vary by hardware.
6 - Storage

6.1 - Pools

6.1.1 - Pool Creation

- Review Storage Needs
- Creating a Pool
  - Suggested Layout
  - Vdev Types
  - Vdev Layout

TrueNAS uses ZFS data storage “pools” to efficiently store and protect data.

**What’s a pool? expand □**

Storage pools are attached drives organized into virtual devices (vdevs). ZFS and TrueNAS periodically reviews and “heals” whenever a bad block is discovered in a pool. Drives are arranged inside vdevs to provide varying amounts of redundancy and performance. This allows for high performance pools, pools that maximize data lifetime, and all situations in between.

**Review Storage Needs**

It is strongly recommended to review the available system resources and plan the storage use case before creating a storage pool.

- When storing critical information, more drives allocated to the pool increases redundancy.
- Maximizing total available storage at the expense of redundancy or performance means allocating large volume disks and configuring the pool for minimal redundancy.
- Maximizing pool performance means installing and allocating high-speed SSD drives to the pool.

Determining your specific storage requirements is a critical step before creating a pool.

**Creating a Pool**

To create a new pool, go to **Storage > Pools** and click **ADD**. Select **Create new pool** and click **CREATE POOL** to open the **Pool Manager**.

To begin, enter a pool **Name**.

**Encryption?**
Encryption algorithms are available as an option for maximizing data security. This also complicates how data is retrieved and risks permanent data loss! Refer to the Encryption article for more details and decide if encryption is necessary for your use case before setting any Encryption options.

Next, configure the virtual devices (vdevs) that make up the pool.

**Suggested Layout**

Clicking SUGGEST LAYOUT allows TrueNAS to review all available disks and populate the primary Data vdev with identically sized drives in a balanced configuration between storage capacity and data redundancy. To clear the suggestion, click RESET LAYOUT.

To manually configure the pool, add vdevs according to your use case. Set the Disk boxes and click the ▶️ to move the disks into a vdev.

**Vdev Types**

Pools have many different kinds of vdevs available. These store data or enable unique features for the pool:

- **Data**

  Standard vdev for primary storage operations. Each storage pool requires at least one Data vdev. Data vdev configuration typically affects how the other kinds of vdevs are configured.

**Duplicating a Data vdev**

A Data VDev with disks is duplicated by clicking REPEAT. When more disks are available and equal in size, the REPEAT button creates another vdev with an identical configuration called a “mirror” of vdevs.

When even more same-size disks are available, multiple copies of the original vdev can be created.

Don’t have multiple data vdevs with different numbers of disks in each vdev. This complicates and limits the pool capabilities.

- **Cache**

  ZFS L2ARC read-cache used with fast devices to accelerate read operations. This can be added or removed after creating the pool.

- **Log**

  ZFS LOG device that improves synchronous write speeds. This can be added or removed after creating the pool.

- **Hot Spare**

  Drives reserved for inserting into Data vdevs when an active drive fails. Hot spares are temporarily used
as replacements for failed drives to prevent larger pool and data loss scenarios.

When a failed drive is replaced with a new drive, the hot spare reverts to an inactive state and is available again as a hot spare.

When the failed drive is only detached from the pool, the temporary hot spare is promoted to a full Data vdev member and is no longer available as a hot spare.

- **Metadata**
  Special Allocation class used to create Fusion Pools for increased metadata and small block I/O performance.

- **Dedup**
  Stores ZFS de-duplication. Requires allocating X GiB for every X TiB of general storage. Example: 1 GiB of Dedup vdev capacity for every 1 TiB of Data vdev availability.

To add a different vdev type during pool creation, click ADD VDEV and select the type. Select disks from Available Disks and use the ▶️ (right arrow) next to the new VDev to add it to that section.

**Vdev Layout**

Disks added to a vdev arrange in different layouts, according to the specific pool use case.

<table>
<thead>
<tr>
<th>Can I create vdevs with different layouts in one pool?</th>
<th>expand □</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding multiple vdevs with different layouts to a pool is not supported. Create a new pool when a different vdev layout is required. For example, pool1 has a data vdev in a mirror layout, so create pool2 for any raid-z vdevs.</td>
<td></td>
</tr>
</tbody>
</table>

- **Stripe**
  Each disk is used to store data. Requires at least one disk and has no data redundancy. Never use a Stripe to store critical data! A single disk failure results in losing all data in the vdev.

- **Mirror**
  Data is identical in each disk. Requires at least two disks, has the most redundancy, and the least capacity.

- **RAIDZ1**
  Uses one disk for parity while all other disks store data. Requires at least three disks.

- **RAIDZ2**
  Uses two disks for parity while all other disks store data. Requires at least four disks.

- **RAIDZ3**
  Uses three disks for parity while all other disks store data. Requires at least five disks.

The Pool Manager suggests a vdev layout from the number of disks added to the vdev. For example, if two disks are added, TrueNAS automatically configures the vdev as a Mirror, where the total available storage is the size of one added disk while the other disk provides redundancy.
To change the vdev layout, open the *Data VDevs* list and select the desired layout.
6.1.2 - Pool Import

This procedure only applies to disks with a ZFS storage pool. To import disks with different file systems, see Import Disk.

ZFS pool importing works for pools that were exported or disconnected from the current system, created on another system, and pools to reconnect after reinstalling or upgrading the TrueNAS system. To import a pool, go to Storage > Pools > ADD.

Do I need to do anything different with disks installed on a different system? expand

When physically installing ZFS pool disks from another system, use the `zpool export poolname` command in the command line or a web interface equivalent to export the pool on that system. Shut that system down and move the drives to the TrueNAS system. Shutting down the original system prevents an “in use by another machine” error during the TrueNAS import.

There are two kinds of pool imports, standard ZFS pool imports and ZFS pools with legacy GELI encryption.

- **Standard ZFS Pool**

**Standard ZFS Pools**

Select *Import Existing Pool* and click *NEXT*.

The wizard asks if the pool has legacy GELI encryption.

Select *No, continue with import* and click *NEXT*.

TrueNAS detects any pools that are present but unconnected.
Choose the ZFS pool to import and click **NEXT**.

Review the Pool Import Summary and click **IMPORT**.

- **ZFS Pool with GELI**

**Encrypted GELI Pools**

Importing a GELI-encrypted pool requires using the encryption key file and passphrase to decrypt the pool *before* importing. When a pool cannot be decrypted, it cannot be re-imported after a failed upgrade or lost configuration, and the data is irretrievable. Always have a copy of the pool GELI key file and passphrase available.

Select *Import Existing Pool* and click **NEXT**.

The wizard asks if the pool has legacy GELI encryption. Select *Yes, decrypt the disks* and review the decryption options.
Make sure the *Disks* selection shows the encrypted disks and partitions that are part of the incoming pool. Apply the GELI encryption key file by clicking *Choose File* and uploading the file from your local system.

When a passphrase is also present, enter it in the *Passphrase* field. Click *Next* and wait for the disks to decrypt.

When the disks are decrypted, select the GELI pool to import.
Review the **Pool Import Summary** and click **IMPORT**.

GELI encrypted pools show in **Storage > Pools** as *(Legacy Encryption)*.

**Back Up the Pool Key**

For security reasons, encrypted pool keys do not save to a configuration backup file. When TrueNAS is installed to a new device and restored with a saved configuration file, keys for encrypted disks are not present and the system does not request them.

To correct this, export the encrypted pool in **Storage > Pools** with **settings > Export/Disconnect**. Do not set *Destroy data on this pool?*. Now import the pool again. During the import, add the encryption keys as described previously.
6.1.3 - Managing Pools

When a pool is created, a root dataset is also automatically created with the same name as the pool. The root dataset’s permissions can’t be changed.

After creating a data storage pool, there are a variety of options to change the initial configuration of that pool. Changing a pool can be disruptive, so make sure you are aware of existing resources on the system and consider backing up any stored data before changing the pool. To find an existing pool, log in to the web interface and go to Storage > Pools.

The current status and storage usage of each pool is shown. To see more details about a pool, click the symbol on the right side of the pool entry. Click the settings for all pool management options.

- **Pool Options**

  Contains any additional high-level settings for the pool.

- **Auto TRIM** allows TrueNAS to periodically check the pool disks for storage blocks that can be reclaimed. This can have a performance impact on the pool, so the option is disabled by default. For more details about TRIM in ZFS, see the autotrim property description in `zpool.8`.

- **Export/Disconnect**

  Removes the pool from the system. Can be used to prepare drives for transfer to a new system and import the pool or completely delete the pool and any data stored on it. A dialog warns about the risks of disconnecting the pool and shows any system services that are affected by removing the pool.
Because this is a destructive action, additional checkboxes must be set and the name of the pool manually entered when also deleting stored data. Existing shares to this data can also be removed when the pool is disconnected.

- **Add Vdevs**

This opens the **Pool Manager** to add more vdevs to the pool.
Changing the original encryption and data vdev configuration is not allowed.

A new data vdev is chosen by default. To add different kinds of vdevs to the pool, click **ADD VDEV** and choose the type from the drop down.

When adding disks to increase the capacity of a pool, ZFS supports the addition of virtual devices, or vdevs, to an existing ZFS pool. **After a vdev is created, more drives cannot be added to that vdev**, but a new vdev can be striped with another of the same type to increase the overall size of the pool. To extend a pool, the vdev being added must be the same type as existing vdevs.

Some vdev extending examples:

- to extend a ZFS mirror, add the same number of drives. The result is a striped mirror. For example, if ten new drives are available, a mirror of two drives could be created initially, then extended by adding another mirror of two drives, and repeating three more times until all ten drives have been added.
- to extend a three-drive RAIDZ1, add another three drives. The resulting pool is a stripe of two RAIDZ1 vdevs, similar to RAID 50 on a hardware controller.
- to extend a four-drive RAIDZ2, add another four drives. The result is a stripe of RAIDZ2 vdevs, similar to RAID 60 on a hardware controller.
- adding a disk as a **hot spare** to the pool.

**Scrub Pool**
Initiate a data integrity check of the pool. Any problems detected during the scrub are either automatically corrected or will generate an alert in the web interface. By default, every pool is automatically checked on a reoccurring scrub schedule.

**Status**
Opens the **Pool Status** screen to show the state of the last scrub and disks in the pool.
Additional options for managing connected disks are available in this screen.

- **Expand Pool**
  Increases the size of the pool to match all available disk space. This option is typically used when virtual disks are resized apart from TrueNAS.

- **Upgrade Pool**

  This option only appears when the pool can be upgraded to use new ZFS feature flags. Before upgrading an existing pool, be aware of these caveats:
  
  ♦ Upgrading a pool is one-way, meaning that if you change your mind you cannot go back to an earlier ZFS version or downgrade to an earlier version of the software that does not support those ZFS features.
  ♦ Before performing any operation that can affect the data on a storage disk, always back up all data first and verify the integrity of the backup. While it is unlikely that the pool upgrade will affect the data, it is always better to be safe than sorry.
  ♦ Upgrading a ZFS pool is optional. Do not upgrade the pool if the possibility of reverting to an earlier version of TrueNAS or repurposing the disks in another operating system that supports ZFS is desired. It is not necessary to upgrade the pool unless the end user has a specific need for the newer ZFS Feature Flags. If a pool is upgraded to the latest feature flags, it will not be possible to import that pool into another operating system that does not yet support those feature flags.

The upgrade itself only takes a few seconds and is non-disruptive. It is not necessary to stop any sharing services to upgrade the pool. However, it is best to upgrade when the pool is not being heavily used. The upgrade process will suspend I/O for a short period, but is nearly instantaneous on a quiet pool.
6.1.4 - Datasets

- Creating a Dataset
  - Dataset Options
  - Advanced Dataset Options
- Managing Datasets
  - Quotas

A TrueNAS dataset is a file system you create within a data storage pool. Datasets can contain files, directories (child datasets), and have individual permissions or flags. You can encrypt datasets using either the pool encryption created with the pool or with a separate dataset-level encryption configuration.

We recommend you organize your pool with datasets before configuring data sharing, as this allows for more fine-tuning of access permissions and using different sharing protocols.

Creating a Dataset

To create a dataset in the desired pool, go to Storage > Pools.

Find the pool and top-level (root) dataset for that pool, then click Add Dataset.

To create a dataset with the default options, enter a name for the dataset and click SUBMIT.

If using a specific data sharing option, select the Share Type you need as you cannot change the share type after you click SUBMIT.

Dataset Options
You must configure the **Name and Options** fields to create the dataset. Datasets typically inherit most settings from the root or parent dataset, but you must enter a name before clicking **Submit**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>string</td>
<td>Unique identifier for the dataset that you cannot change after the dataset is created.</td>
</tr>
<tr>
<td>Comments</td>
<td>string</td>
<td>Notes about the dataset.</td>
</tr>
<tr>
<td>Sync</td>
<td>dropdown list</td>
<td><strong>Standard</strong> uses the sync settings that the client software requests. <strong>Always</strong> waits for data writes to complete, and <strong>Disabled</strong> never waits for writes to complete.</td>
</tr>
</tbody>
</table>
| Compression level | dropdown list | Encode information in less than space than the original data occupies. We recommend you choose a compression algorithm that balances disk performance with the amount of saved space:  
  **lz4** is a general recommendation as it maximizes performance and dynamically identifies the best files to compress.  
  **zstd** is the **Zstandard** compression algorithm that has several options for balancing speed and compression.  
  **gzip** options are similar to zstd and range from **1** for least compression with best performance, through **9** for maximum compression with greatest performance impact.  
  **zle** is a fast algorithm that only eliminates runs of zeroes.  
  **lzjb** is a legacy algorithm that is not recommended for use. |
| Enable Atime | dropdown list | **on** updates the access time for files when they are read. **off** disables creating log traffic when reading files to maximize performance. |
By default, datasets inherit the **Encryption Options** from the root or parent dataset. To configure the dataset with different encryption settings, unset **Inherit** and select the new **Encryption Options**. For detailed descriptions of the encryption options, see the Encryption article.

The **Other Options** help tune the dataset for particular data sharing protocols:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZFS Deduplication</td>
<td>dropdown list</td>
<td>Transparently reuse a single copy of duplicated data to save space. Deduplication can improve storage capacity, but is RAM intensive. Compressing data is a general recommendation before using deduplication. Deduplicating data is a one-way process. <strong>Deduplicated data cannot be un-deduplicated</strong>!</td>
</tr>
<tr>
<td>Case Sensitivity</td>
<td>dropdown list</td>
<td><strong>Sensitive</strong> assumes filenames are case sensitive. <strong>Insensitive</strong> assumes filenames are not case sensitive. <strong>Mixed</strong> understands both types of filenames. You cannot change this setting after the dataset is created.</td>
</tr>
<tr>
<td>Share Type</td>
<td>dropdown list</td>
<td>Define the type of data sharing the dataset uses to optimize the dataset for that sharing protocol. You cannot change this setting after the dataset is created. If creating an AFP share use <strong>Generic</strong>. For SMB shares select <strong>SMB</strong></td>
</tr>
</tbody>
</table>

**Advanced Dataset Options**

**Advanced Options** expand □

Clicking **ADVANCED OPTIONS** adds dataset quota management tools and a few additional fields to the **Other Options**.
Setting a quota defines the maximum allowed space for the dataset. You can also reserve a defined amount of pool space for the dataset to help prevent situations where automatically generated data like system logs consume all space on the dataset. You can configure quotas for either the new dataset or to include all child datasets in the quota.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quota for this dataset</td>
<td>integer</td>
<td>Define the maximum allowed space for the dataset.</td>
</tr>
<tr>
<td>Quota warning alert at, %</td>
<td>integer</td>
<td>Generate a warning level <a href="#">alert</a> when consumed space reaches the defined percentage. By default, the dataset inherits this value from the parent dataset. Unset <a href="#">Inherit</a> to change the value.</td>
</tr>
<tr>
<td>Quota critical alert at, %</td>
<td>integer</td>
<td>Generate a critical level <a href="#">alert</a> when consumed space reaches the defined percentage. By default, the dataset inherits this value from the parent dataset. Unset <a href="#">Inherit</a> to change the value.</td>
</tr>
</tbody>
</table>
Reserved space for this dataset | integer | Reserve additional space for datasets that contain logs which could eventually take up all the available free space. 0 is unlimited.

More fields are added to the **Other Options** setting. By default, many of these options inherit their values from the parent dataset.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read-only</td>
<td>drop-down list</td>
<td><strong>On</strong> prevents modifying the dataset. <strong>Off</strong> allows users accessing the dataset to modify its contents.</td>
</tr>
<tr>
<td>Exec</td>
<td>drop-down list</td>
<td><strong>On</strong> allows processes to execute from within this dataset. <strong>Off</strong> prevents processes from executing in the dataset. The recommended setting is <strong>On</strong>.</td>
</tr>
<tr>
<td>Snapshot directory</td>
<td>drop-down list</td>
<td>Controls visibility of the <code>.zfs</code> directory on the dataset. Choose between <strong>Visible</strong> or <strong>Invisible</strong>.</td>
</tr>
<tr>
<td>Copies</td>
<td>drop-down list</td>
<td>Duplicates ZFS user data stored on this dataset. Choose between <strong>1</strong>, <strong>2</strong>, or <strong>3</strong> redundant data copies. This can improve data protection and retention, but is not a substitute for storage pools with disk redundancy.</td>
</tr>
<tr>
<td>Record Size</td>
<td>drop-down list</td>
<td>Logical block size in the dataset. Matching the fixed size of data, as in a database, could result in better performance.</td>
</tr>
<tr>
<td>ACL Mode</td>
<td>drop-down list</td>
<td>Determine how <code>chmod</code> behaves when adjusting file ACLs. See the <code>zfs aclmode</code> property. <strong>Passthrough</strong> only updates ACL entries that are related to the file or directory mode. <strong>Restricted</strong> does not allow <code>chmod</code> to make changes to files or directories with a non-trivial ACL. An ACL is trivial if it can be fully expressed as a file mode without losing any access rules. Setting the ACL Mode to <strong>Restricted</strong> is typical to optimize a dataset for SMB sharing, but can require further optimizations. For example, configuring an <code>rsync task</code> with this dataset could require adding <code>--no-perms</code> in the task <strong>Auxiliary Parameters</strong> field.</td>
</tr>
<tr>
<td>Metadata (Special) Small Block Size</td>
<td>integer</td>
<td>Threshold block size for including small file blocks into the <strong>special allocation class (fusion pools)</strong>. Blocks smaller than or equal to this value are assigned to the special allocation class while greater blocks are assigned to the regular class. Valid values are zero or a power of two from 512B up to 1M. The default size 0 means no small file blocks are allocated in the special class. Before setting this property, you must add a <strong>special class vdev</strong> to the pool.</td>
</tr>
</tbody>
</table>

**Managing Datasets**

After creating a dataset additional management options are available by going to **Storage > Pools** and clicking **Add Dataset** for a dataset:

- **Add Dataset**: create a new dataset that is a child of this dataset. You can continue layering datasets in this manner.
- **Add Zvol**: create a new **ZFS block device** as a child of this dataset.
- **Edit Options**: opens the **dataset options** to make adjustments to the dataset configuration. You cannot change the dataset **Name, Case Sensitivity**, and **Share Type** after you click **SUBMIT**.
- **Edit Permissions**: opens the editor to set access permissions for this dataset. Depending on the dataset creation options, this can be a simple permissions editor or the full ACL editor. For more information about editing permissions, read the **permissions** article. This option is not available for the root dataset.
- **User Quotas**: shows options to set data or object quotas for user accounts cached on the system or user accounts connected to this system.
- **Group Quotas**: shows options to set data or object quotas for user groups cached on the system or user groups connected to this system.
- **Delete Dataset**: removes the dataset, all stored data, and any snapshots of the dataset from TrueNAS.

---
Deleting datasets can result in unrecoverable data loss! Be sure you move any critical data off the dataset or that it is obsolete before deleting a dataset.

- **Create Snapshot**: take a single ZFS snapshot of the dataset to provide additional data protection and mobility. Created snapshots are listed in Storage > Snapshots.

### Quotas

TrueNAS allows setting data or object quotas for user accounts and groups cached on or connected to the system.

- **User**

To view and edit user quotas, go to Storage > Pools and click to open the Dataset Actions menu and then click User Quotas.

The User Quotas page displays the names and quota data of any user accounts cached on or connected to the system.

To edit individual user quotas, go to the user row and click the and then click edit.

Use the Edit User window to edit the User Data Quota, which is the amount of disk space that each selected users can use, and the User Object Quota, which is the number of objects that each selected user can own.

To edit user quotas in bulk, click Actions and then select Set Quotas (Bulk).

Use the Set Quotas window to edit user data and object quotas after selecting any cached or connected users.
Group

Go to Storage > Pools and click □ to open the Dataset Actions menu. Click Group Quotas.

The Group Quotas page displays the names and quota data of any groups cached on or connected to the system.

To edit individual group quotas, go to the group’s row and click the > and then click edit.

Use the Edit Group window to edit the Group Data Quota and Group Object Quota.

To edit group quotas in bulk, click Actions and select Set Quotas (Bulk).

The same options for single groups display, along with choosing groups for these new quota rules.
A ZFS Volume (Zvol) is a dataset that represents a block device. These are needed when configuring an iSCSI Share.

To create a zvol in a pool, go to Storage > Pools then click and Add Zvol.

Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zvol name</td>
<td>string</td>
<td>Enter a short name for the zvol. Using a zvol name longer than 63-characters can prevent accessing zvols as devices. For example, a zvol with a 70-character filename or path cannot be used as an iSCSI extent. This setting is mandatory.</td>
</tr>
<tr>
<td>Comments</td>
<td>string</td>
<td>Enter any notes about this zvol.</td>
</tr>
<tr>
<td>Size for this zvol</td>
<td>integer</td>
<td>Specify size and value. Units like (t), (TiB), and (G) can be used. The size of the zvol can be increased later, but cannot be reduced. If the size is more than 80% of the available capacity, the creation will fail with an “out of space” error unless Force size is also enabled.</td>
</tr>
<tr>
<td>Force size</td>
<td>checkbox</td>
<td>By default, the system will not create a zvol if that operation will bring the pool to over 80% capacity. While NOT recommended, enabling this option will force the creation of the zvol.</td>
</tr>
<tr>
<td>Encryption Options</td>
<td></td>
<td>Sets the data write synchronization. Inherit inherits the sync settings from the</td>
</tr>
</tbody>
</table>
Sync drop-down menu

parent dataset, Standard uses the sync settings that have been requested by the client software, Always waits for data writes to complete, and Disabled never waits for writes to complete.

Compression level drop-down menu

Compress data to save space. Refer to Compression for a description of the available algorithms.

ZFS Deduplication drop-down menu

Do not change this setting unless instructed to do so by your iXsystems support engineer.

Sparse checkbox

Used to provide thin provisioning. Use with caution as writes will fail when the pool is low on space.

Read-only drop-down menu

Set to prevent the zvol from being modified.

Inherit (Encryption Options) checkbox

Enabling causes the zvol to use the encryption properties of the root dataset.

**Advanced Options expand □**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block size drop-down menu</td>
<td>The default is Inherit, other options include, 4KiB, 8KiB, 16KiB, 32KiB, 64KiB, 128KiB</td>
<td></td>
</tr>
</tbody>
</table>

**Optimal Zvol Block Sizes expand □**

TrueNAS automatically recommends a space-efficient block size for new zvols. This table shows the minimum volume block size values that are recommended. To manually change this value, use the Block size dropdown menu.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Number of Drives</th>
<th>Optimal Block Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirror</td>
<td>N/A</td>
<td>16k</td>
</tr>
<tr>
<td>Raidz-1</td>
<td>3</td>
<td>16k</td>
</tr>
<tr>
<td>Raidz-1</td>
<td>4/5</td>
<td>32k</td>
</tr>
<tr>
<td>Raidz-1</td>
<td>6/7/8/9</td>
<td>64k</td>
</tr>
<tr>
<td>Raidz-1</td>
<td>10+</td>
<td>128k</td>
</tr>
<tr>
<td>Raidz-2</td>
<td>4</td>
<td>16k</td>
</tr>
<tr>
<td>Raidz-2</td>
<td>5/6</td>
<td>32k</td>
</tr>
<tr>
<td>Raidz-2</td>
<td>7/8/9/10</td>
<td>64k</td>
</tr>
<tr>
<td>Raidz-2</td>
<td>11+</td>
<td>128k</td>
</tr>
<tr>
<td>Raidz-3</td>
<td>5</td>
<td>16k</td>
</tr>
<tr>
<td>Raidz-3</td>
<td>6/7</td>
<td>32k</td>
</tr>
<tr>
<td>Raidz-3</td>
<td>8/9/10/11</td>
<td>64k</td>
</tr>
<tr>
<td>Raidz-3</td>
<td>12+</td>
<td>128k</td>
</tr>
</tbody>
</table>

Additional tuning can be required for optimal performance, depending on the workload. iXsystems Engineers are available to assist Enterprise customers with tuning their TrueNAS hardware. The workload tuning chapter of the OpenZFS handbook is also a good resource.
Managing Zvols

To see options for an existing zvol, click more_vert next to the desired zvol in Storage > Pools:

- Delete zvol removes the zvol from TrueNAS.

Deleting zvols can result in unrecoverable data loss! Be sure that any critical data is moved off the zvol or is otherwise obsolete.

Deleting a zvol also deletes all snapshots of that zvol.
- Edit Zvol opens the zvol creation form for changing the previously saved settings. Similar to datasets, a zvol name cannot be changed.
- Create Snapshot takes a single current point in time image of the zvol and saves it to Storage > Snapshots. A snapshot Name is suggested and an extra option to make the snapshot Recursive is available.

When the selected zvol is cloned from an existing snapshot, Promote Dataset is available. When a clone is promoted, the original volume becomes a clone of the clone, making it possible to delete the volume that the clone was created from. Otherwise, a clone cannot be deleted while the original volume exists.

When the zvol is created with encryption enabled, additional Encryption Actions are shown.
6.1.6 - Permissions

- Basic Permissions Editor
  - Options
  - Access Control Lists
    - ACL Inheritance
    - Editing an ACL
    - Access Control List (ACEs)
      - Permissions
      - Inheritance Flags

Permissions control the actions users can perform on dataset contents. TrueNAS allows using both a simple permissions manager and editing a full Access Control List (ACL) for defining dataset permissions.

To change dataset permissions, go to Storage > Pools > more_vert > Edit Permissions for a dataset.

Basic Permissions Editor

The Permissions Editor option allows basic adjustments to a datasets ACL.

## Options

**Dataset Path** shows the full pathway to this dataset. This is set when the dataset is created and cannot be changed.

The **Owner** section controls which TrueNAS User and Group has full control of this dataset.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>User that controls the dataset. Users created manually or imported from a directory service appear in the drop-down menu.</td>
</tr>
<tr>
<td>Apply User</td>
<td>Confirms changes to User. To prevent errors, changes to the User are submitted only when this box is set.</td>
</tr>
<tr>
<td>Group</td>
<td>Group that controls the dataset. Groups created manually or imported from a directory service</td>
</tr>
</tbody>
</table>
Access Mode defines the basic Read, Write, and Execute permissions for the User, Group, and Other accounts that might access this dataset.

Advanced has several tuning options:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply Permissions</td>
<td>Apply permissions recursively to all directories and files within the current dataset.</td>
</tr>
<tr>
<td>Recursively</td>
<td></td>
</tr>
<tr>
<td>Traverse</td>
<td>Apply permissions recursively to all child datasets of the current dataset.</td>
</tr>
</tbody>
</table>

To switch from the basic editor to the advanced ACL editor, click USE ACL MANAGER.

**Access Control Lists**

An Access Control List (ACL) is a set of account permissions associated with a dataset and applied to directories or files within that dataset. ACLs are typically used to manage user interactions with shared datasets and are created when a dataset is added to a pool.

When creating a dataset, you can choose how the ACL can be modified by selecting an ACL Mode:

- **Passthrough** only updates ACL entries (ACEs) that are related to the file or directory mode.
- **Restricted** does not allow chmod to make changes to files or directories with a non-trivial ACL. An ACL is trivial if it can be fully expressed as a file mode without losing any access rules. Setting the ACL Mode to Restricted is typically used to optimize a dataset for SMB sharing, but can require further optimizations. For example, configuring an rsync task with this dataset could require adding -no-perms as an extra option for the task.

To view an ACL, go to Storage > Pools > Edit Permissions for a nested dataset within a pool.
The video at https://www.youtube.com/watch?v=p3wn0b_aXNw&t=3s shows editing ACLs for FreeNAS 11.3. However, the same process applies for TrueNAS 12.0 and later.
ACL Inheritance

The ACL for a new file or directory is typically inherited from the parent directory and is preserved when it is moved or renamed within the same dataset. An exception is when there are no File Inherit or Directory Inherit flags in the parent ACL owner@, group@, or everyone@ entries. These non-inheriting entries are added to the ACL of the newly created file or directory based on the Samba create and directory masks or the umask value.

Editing an ACL

Click ACL Manager to adjust file ownership or account permissions to the dataset. The first time viewing the ACL Manager a dialog suggests using basic presets. The ACL can be edited at any time after choosing to either apply a preset or create a custom ACL.

Choose Select a preset ACL and choose a preset. The preset options are OPEN, RESTRICTED, or HOME.

Choose Create a custom ACL to create a new list of customized permissions.

File Information

The selected User controls the dataset and always has permission to modify the ACL and other attributes. The selected Group also controls the dataset, but can have permissions changed by adding or modifying a group@ ACE. Any user accounts or groups imported from a directory service can be selected as the primary User or Group.

Access Control List (ACEs)

To add a new item to the ACL, define Who the Access Control Entry (ACE) applies to, and configure permissions and inheritance flags for the ACE.

ACL Details from Shell expand □

To view an ACL information from the console, go to System Settings > Shell and enter command:

```
getfacl /mnt/path/to/dataset
```

Permissions

Permissions are divided between Basic and Advanced options. The basic options are commonly used groups of the advanced options.

Basic Permissions

- **Read (r-x---a-R-c---):** view file or directory contents, attributes, named attributes, and ACL. Includes the Traverse permission.
- **Modify (rwxpDdaARWc--s):** adjust file or directory contents, attributes, and named attributes. Create
new files or subdirectories. Includes the Traverse permission. Changing the ACL contents or owner is not allowed.

- **Traverse (---x----a-R-c---):** Execute a file or move through a directory. Directory contents are restricted from view unless the Read permission is also applied. To traverse and view files in a directory, but not be able to open individual files, set the Traverse and Read permissions, then add the advanced Directory Inherit flag.
- **Full Control (rwxpDdaARWcCos):** Apply all permissions.

### Advanced Permissions

- **Read Data (r):** View file contents or list directory contents.
- **Write Data (w):** Create new files or modify any part of a file.
- **Append Data (a):** Add new data to the end of a file.
- **Read Named Attributes (R):** view the named attributes directory.
- **Write Named Attributes (w):** create a named attribute directory. Must be paired with the Read Named Attributes permission.
- **Execute (x):** Execute a file, move through, or search a directory.
- **Delete Children (d):** delete files or subdirectories from inside a directory.
- **Read Attributes (a):** view file or directory non-ACL attributes.
- **Write Attributes (w):** change file or directory non-ACL attributes.
- **Delete (d):** remove the file or directory.
- **Read ACL (c):** view the ACL.
- **Write ACL (c):** change the ACL and the ACL mode.
- **Write Owner (o):** change the user and group owners of the file or directory.
- **Synchronize (s):** synchronous file read/write with the server. This permission does not apply to FreeBSD clients.

### Inheritance Flags

Basic inheritance flags only enable or disable ACE inheritance. Advanced flags offer finer control for applying an ACE to new files or directories.

#### Basic Flags

- **Inherit (fd-----):** enable ACE inheritance.
- **No Inherit (-------):** disable ACE inheritance.

#### Advanced Flags

- **File Inherit (f):** The ACE is inherited with subdirectories and files. It applies to new files.
- **Directory Inherit (d):** new subdirectories inherit the full ACE.
- **No Propagate Inherit (n):** The ACE can only be inherited once.
- **Inherit Only (i):** Remove the ACE from permission checks but allow it to be inherited by new files or subdirectories. Inherit Only is removed from these new objects.
- **Inherited (I):** set when the ACE has been inherited from another dataset.
6.1.7 - Storage Encryption

- Encrypting a Storage Pool
- Encrypting a New Dataset
  - Changing Dataset Encryption
  - Locking and Unlocking Datasets
    - Locking a Dataset
    - Unlocking a Dataset
- Encrypting a Zvol
- Managing Encryption Credentials
- Unlocking a Replicated Encrypted Dataset or Zvol Without a Passphrase
- Legacy GELI Encryption
  - GELI Pool Migrations

TrueNAS supports different encryption options for critical data.

Users are responsible for backing up and securing encryption keys and passphrases! Losing the ability to decrypt data is similar to a catastrophic data loss.

Data-at-rest encryption is available with:

- Self Encrypting Drives (SEDs) using OPAL or FIPS 140.2 (Both AES 256)
- Encryption of specific datasets (AES-256-GCM in TrueNAS 12.0)

The local TrueNAS system manages keys for data-at-rest. The user is responsible for storing and securing their keys. TrueNAS 12.0 and newer includes the Key Management Interface Protocol (KMIP).

Encryption Drawbacks and Considerations expand □

Always consider the following drawbacks/considerations when encrypting data:

- Losing encryption keys and passwords means losing your data.
- Unrelated encrypted datasets do not support deduplication.
- Using GELI or ZFS encryption with deduplication is not recommended because of the sizable performance impact.
- Using many encryption and deduplication features at once requires caution since all compete for the same CPU cycles.

Encrypting a Storage Pool

Encryption is for users storing sensitive data. Pool-level encryption does NOT apply to the storage pool or the disks in the pool. It only applies to the root dataset that shares the same name as the pool. Child datasets, or zvols, inherit encryption from the parent dataset unless you overwrite encryption when creating the child datasets or zvols.

Encrypting the root dataset of a new storage pool further increases data security. Create a new pool and check the Encryption checkbox on the Pool Manager screen. TrueNAS encryption warning dialog box displays.
Read the warning, click the Confirm checkbox, and click I UNDERSTAND.

We recommend using the default encryption cipher, but other ciphers are available.

What are these options? expand

TrueNAS supports AES Galois Counter Mode (GCM) and Counter with CBC-MAC (CCM) algorithms for encryption. These algorithms provide authenticated encryption with block ciphers.

Encrypting a New Dataset

You can create new datasets within an existing storage pool as either encrypted or non-encrypted. A mix of encrypted and non-encrypted datasets can exist in a single storage pool.

To encrypt a dataset, create a new dataset and after typing a name scroll down to the Encryption Options section. The Add Dataset configuration screen encryption fields change based on the Encryption Type.

☐ Inherit Checkbox

Because child datasets inherit settings from the parent dataset, the Add Dataset configuration screen displays with the inherit checkbox already check-marked. This means the inherit checkbox text for the child configuration screen changes based on the parent encryption setting.

Inherit (encrypted) displays for an encrypted parent dataset.
Inherit (non-encrypted) displays for a parent dataset not encrypted.

You can change the inherited encrypted/non-encrypted state by unchecking the inherit box. This displays the Encryption checkbox already check-marked.

- **Encryption Checkbox**

Click the **Inherit (encrypted)** or **Inherited (non-encrypted)** checkbox with the checkmark to turn off inherited encryption settings. The Encryption checkbox displays already check-marked. You can now change this dataset’s encryption settings.

- **Encryption Options** fields change based on the Encryption Type selected. There are two options, **Key** or **Passphrase**. The default setting is **Key**.

---

If you uncheck the Encryption checkbox on the Add Dataset configuration screen, the encryption fields no longer display and the new child dataset is not encrypted.
The Generate Key checkbox defaults to check-marked. If you uncheck it, the Key* text field displays below it. Type the encryption key you want to use into this field.

If you change the Encryption Type to Passphrase new Encryption Options fields display.
If using the passphrase option choose a complex phrase not easy to guess.

Keep both encryption keys and/or passphrases safeguarded in a secure and protected place. Losing encryption keys or passphrases can result in permanent data loss!

After configuring the new dataset encryption settings and any other settings, click **SAVE**. The new dataset displays on the Storage > Pools screen below its parent dataset. If you encrypt a dataset, an unlocked icon displays to the right of its name and a locked icon displays to the right of the root dataset name. It remains unlocked until you lock it.

### Changing Dataset Encryption

Click on Encryption Options on the Dataset Action menu to change dataset encryption settings. This option only displays on the menu for datasets with encryption configured. The Edit Encryption Options configuration window displays and window name includes the dataset full path name. In the example used it includes the root dataset tank, the child dataset without encryption child1, and finally the selected child-of-the-child dataset with encryption child2-encrypt (i.e., tank/child1/child2-encrypt).
Click the **Confirm** checkbox to check-mark it and then click **SAVE** after making any changes.

Save any change to the encryption key or passphrase, update your saved passcodes and keys file, and back it up.

### Locking and Unlocking Datasets

TrueNAS displays a dataset status with icons:

- **Dataset unlocked icon:**
- **Dataset locked icon:** 🝨

The locked icon displayed beside the root dataset after adding a dataset with encryption and also beside a dataset where the pool encryption properties don’t match the root dataset is: 🝨

You can only lock and unlock an encrypted dataset when it is secured with a passphrase instead of a key file. Before locking a dataset, verify that it is not currently in use.

### Locking a Dataset

Click the dataset’s **more_vert** icon to display the **Dataset Actions** menu and then click on **Lock**. The **Lock Dataset** dialog box displays and includes the dataset full path name.
Use the **Force unmount** option only if you are certain no one is currently accessing the dataset. Click the **Confirm** checkbox to check-mark it and click **LOCK**, and then click **LOCK**. A confirmation window displays indicating the dataset is locked and the unlock icon changes to a locked icon.

You *cannot* use locked datasets.

**Unlocking a Dataset**

To unlock a dataset, click on the **more_vert** icon to display the Dataset Actions menu and then click on **Unlock**.

Type the passphrase and click **SUBMIT**. To unlock child datasets, set the **Unlock Children** checkbox. Child datasets that inherited the parent dataset’s encryption settings unlock when the parent unlocks. Users can unlock child datasets with different passphrases as the parent simultaneously by entering their passphrases.

Two confirmation windows display. Click **CONTINUE** to confirm you want to unlock the datasets or **CANCEL** to exit and keep the datasets locked. A second confirmation window displays confirming the datasets are unlocked. Click **CONTINUE** to close the second confirmation window.

**Unlocking Multiple Datasets Example:**

TrueNAS displays the dataset with the unlocked icon.

**Unlocking Multiple Datasets Example:**
The parent dataset is `media`. It has three child datasets. The `documents` child dataset inherits the parent encryption settings and its password. The other two child datasets (`audio` and `video`) have their own passphrases. After locking the parent dataset all child datasets lock too.

Open the `more_vert` for the parent dataset and click `Unlock`. To unlock all the datasets, click on the `Unlock Children` checkbox to check-mark it and type the passphrase for each dataset to unlock them.

Click the `CONTINUE` button on both confirmation windows to successfully unlock the datasets. The datasets display the unlocked icon.

**Encrypting a Zvol**

Encryption is for securing sensitive data.
You can only encrypt a zvol if you create the zvol from a dataset with encryption.

Users are responsible for backing up and securing encryption keys and passphrases! Losing the ability to decrypt data is similar to a catastrophic data loss.

Zvols, like datasets, inherit encryption settings from the parent dataset. To encrypt a zvol, select a dataset configured with encryption and then create a new zvol. Next, click the more_vert icon to display the Zvol Actions menu.

If you do not see encryption options on the menu then you created the zvol from a dataset not configured with encryption. You can delete the zvol and start over.

Click Encryption Options. The Edit Encryption Options configuration window displays with the Inherit encryption properties from parent checkbox check-marked.

Like datasets, the window name includes the full path for the zvol. In this example, the root dataset Encrypted_Pool, the encrypted child dataset Dataset2 (i.e., Encrypted_Pool/Dataset2).

If not making changes, click the Confirm checkbox to activate the SAVE button, and then click SAVE. The zvol is encrypted with settings inherited from its parent.
To change inherited encryption properties, click on the inherit checkbox to uncheck it. Additional configuration option fields display.

If **Encryption Type** is set to **Key**, type an encryption key into the **Key** field or check-mark the **Generate Key** checkbox. If set to **Passphrase**, type a passphrase at least eight characters long into both the **Passphrase** and **Confirm Passphrase** fields. After making any changes, click the **Confirm** checkbox to check-mark it and activate the **SAVE** button, and then click **SAVE**. The zvol is now encrypted with settings not inherited from its parent.

Save any change to the encryption key or passphrase, update your saved passcodes and keys file, and back up the file.

**Managing Encryption Credentials**

There are two ways to manage the encryption credentials: with key files or passphrases.

- **Key Files**

Creating a new encrypted pool automatically generates a new key file and prompts you to download it.

*Always back up the key file to a safe and secure location.*
To manually download a copy of the pool’s inherited and non-inherited encrypted dataset key files, open the pool settings menu and click on Export Dataset Keys. Enter the root password and click the CONTINUE button.

To manually download a backup a single dataset’s key file, click the dataset more_vert and click on Export Key. Next type the root password and click the CONTINUE button. Click the DOWNLOAD KEY button.

To change the key, click the dataset more_vert and Encryption Options.
Type your custom key or click **Generate Key**.

- **Passphrases**

To use a passphrase instead of a keyfile, click the dataset **more_vert** icon to display the **Dataset Actions** menu and then click **Encryption Options**. Change the **Encryption Type** from **Key** to **Passphrase**.
Set the rest of the options:

- **Passphrase**: A user-defined string at least eight characters long that is required to decrypt the dataset. Type it into the Passphrase and Confirm Passphrase fields.

> The passphrase is the only means to decrypt the information stored in this dataset.

Be sure to create a memorable passphrase or physically secure the passphrase.

- **pbkdf2iters**: The number of password-based key derivation function 2 (PBKDF2) iterations to use for reducing vulnerability to brute-force attacks. Users must enter a number greater than 100000.

**Unlocking a Replicated Encrypted Dataset or Zvol Without a Passphrase**

TrueNAS Enterprise users can connect a Key Management Interoperability Protocol (KMIP) server to centralize keys when they are not using passphrases to unlock a dataset or zvol.

Users with TrueNAS CORE or Enterprise installations without KMIP should either replicate the dataset or zvol without properties to disable encryption at the remote end or construct a special json manifest to unlock each child dataset/zvol with a unique key.

- **Method 1: Construct JSON Manifest**
  1. Replicate every encrypted dataset you want to replicate with properties.
  2. Export key for every child dataset that has a unique key.
  3. For each child dataset construct a proper json with poolname/datasetname of the destination system and key from the source system like this: 
     ```json
     {"tank/share01": "57112db4be777d93fa7b76138a68b790d46d6858569bf9d13e32eb9fda72146b"}
     ```
  4. Save this file with the extension .json.
  5. Unlock the dataset(s) on the remote system using properly constructed json files.

- **Method 2: Replicate Encrypted Dataset/Zvol without Properties**
Uncheck properties when replicating so that the destination dataset isn’t encrypted on the remote side and doesn’t require a key to unlock.

1. Go to **Tasks > Replication Tasks** and click **ADD**.
2. Click **ADVANCED REPLICATION CREATION**.
3. Fill out the form as needed and make sure **Include Dataset Properties** is **NOT** checked.
4. Click **SUBMIT**.

**NOTE:** This does not affect TrueNAS Enterprise installs with **KMIP**.

### Legacy GELI Encryption

TrueNAS no longer supports GELI encryption (deprecated).

**Can I directly convert a GELI-encrypted pool to native ZFS encryption?**

No. You must migrate data out of the GELI pool and into a ZFS encrypted pool.

### GELI Pool Migrations

You can *migrate* data from the GELI-encrypted pool to a new ZFS-encrypted pool.

Be sure to unlock the GELI-encrypted pool before attempting any data migrations. The new ZFS-encrypted pool must be at least the same size as the previous GELI-encrypted pool. Do not delete the GELI dataset until you have verified the data migration.

There are a few options to migrate data from a GELI-encrypted pool to a new ZFS-encrypted pool:

- **Replication Wizard**

**Using the Replication Wizard**

The TrueNAS web interface continues to detect and support GELI encrypted pools as *Legacy Encrypted* pools. As of TrueNAS version 12.0-U1, a decrypted GELI pool can migrate data to a new ZFS encrypted pool using the Replication Wizard.

Start the Replication Wizard by selecting **Tasks -> Replication Task -> ADD**

**Source Location:**

- Select **On this System**.
- Set the dataset to transfer.

**Destination Location:**

- Select **On a Different System**.

**SSH Connection:**

- Either create the ssh connection by clicking **Create New** or select the destination system’s ssh connection.
- In **Destination**, select the dataset to replicate the files to.
- **Set Encryption.**
- Choose either **PASSPHRASE** or **HEX** for the **Encryption Key Format**.
- If you selected **PASSPHRASE**, type the passphrase. If you selected **HEX**, set **Generate Encryption Key**.
- **Set Store Encryption key in Sending TrueNAS database.**
- Click **Next**

**Replication Schedule:**
- Set Run Once in Replication Schedule.
- Unset Make Destination Dataset Read-Only.
- Click START REPLICATION

○ File Transfer

This method does not preserve file ACLs.

The web interface supports using Tasks > Rsync Tasks to transfer files out of the GELI pool. In the Shell, `rsync` and other file transfer mechanisms (scp, cp, sftp, ftp, rdiff-backup) are available for copying data between pools.

○ ZFS Send and Receive

These instructions are an example walkthrough. It is not an exact step-by-step guide for all situations. Research ZFS send/receive before attempting this. A simple example cannot cover every edge case.

Legend:

GELI Pool = pool_a
Origin Dataset = dataset_1
Latest Snapshot of GELI Pool = snapshot_name
ZFS Native Encrypted Pool = pool_b
Receiving Dataset = dataset_2

2. Open the Shell. Make a new snapshot of the GELI pool and dataset with the data to be migrated:
   
   ```
   zfs snapshot -r pool_a/dataset_1@snapshot_name
   ```
3. Create a passphrase:
   
   ```
   echo passphrase > /tmp/pass
   ```
4. Use ZFS send/receive to transfer the data between pools:
   
   ```
   zfs send -Rv pool_a/dataset_1@snapshot_name | zfs recv -o encryption=on -o keyformat=passphrase -o keylocation=file:///tmp/pass pool_b/dataset_2
   ```
5. When the transfer is complete, go to Storage > Pools and lock the new dataset. After locking the dataset, immediately unlock it. TrueNAS prompts for the passphrase. After entering the passphrase and unlocking the pool, you can delete the /tmp/pass file used for the transfer.
6. If desired, you can convert the dataset to use a key file instead of a passphrase. To use a key file, click the dataset □ (Options) and click Encryption Options. Change the Encryption Type from Passphrase to Key and save.
7. Repeat this process for every dataset in the pool that you need to migrate.

Back up your key file immediately!
6.1.8 - Fusion Pools

Fusion Pools are also known as ZFS Allocation Classes, ZFS Special vdevs, and Metadata vdevs.

What's a special vdev? expand □
A special vdev can store meta data such as file locations and allocation tables. The allocations in the special class are dedicated to specific block types. By default, this includes all metadata, the indirect blocks of user data, and any deduplication tables. The class can also be provisioned to accept small file blocks. This is a great use case for high performance but smaller sized solid-state storage. Using a special vdev drastically speeds up random I/O and cuts the average spinning-disk I/Os needed to find and access a file by up to half.

Creating a Fusion Pool

Go to Storage > Pools, click ADD, and select Create new pool.

A pool must always have one normal (non-dedup/special) vdev before other devices can be assigned to the special class. Configure the Data VDevs, then click ADD VDEV and select Metadata.

Add SSDs to the new Metadata VDev and select the same layout as the Data VDevs.

The metadata special vdev is critical for pool operation and data integrity, so you must protect it with hot spare(s).

UPS Recommendation expand □
When using SSDs with an internal cache, add Uninterruptible Power Supply (UPS) to the system to help minimize the risk from power loss.

Using special vdevs identical to the data vdevs (so they can use the same hot spares) is recommended, but for performance reasons you can make a different type of vdev (like a mirror of SSDs). In that case you must provide hot spare(s) for that drive type as well. Otherwise, if the special vdev fails and there is no redundancy, the pool becomes corrupted and prevents access to stored data.

Drives added to a metadata vdev cannot be removed from the pool.

When more than one metadata vdev is created, then allocations are load-balanced between all these devices. If the special class becomes full, then allocations spill back into the normal class.

After the fusion pool is created, the Status shows a Special section with the metadata SSDs.

See Managing Pools.
6.1.9 - SLOG Overprovisioning

Overprovisioning SLOG SSDs is useful for different scenarios. The most useful benefit of overprovisioning is greatly extending SSD life. Overprovisioning an SSD distributes the total number of writes and erases across more flash blocks on the drive.


Some SATA devices are limited to one resize per power cycle. Some BIOS can block resize during boot and require a live power cycle.

**Web Interface**

To over provision a SLOG device, log in to TrueNAS and go to **System > Advanced**. Enter an overprovision value corresponding to the new size in GB.

When this value is applied, the overprovision value is applied whenever a pool is created with a SLOG device. It is impossible to restore an overprovisioned SLOG device back to original capacity without running `disk_resize` after first destroying the pool it was part of and issuing a full power cycle.

Only one overprovision/underprovision operation occurs per power cycle.

Erasing the overprovision setting and setting to `none` prevents future SLOG devices from being overprovisioned.

**Shell**

Use `disk_resize` in the Shell to over provision.

The command to over provision an SSD is `disk_resize {DEVICE} {SIZE}`, where `{DEVICE}` is the SSD device name and `{SIZE}` is the new provision size in GiB or TiB. Example: `disk_resize ada5 16GB`. When no size is specified, it reverts the provision back the full size of the device.
Snapshots are one of the most powerful features of ZFS. A snapshot provides a read only point-in-time copy of a file system or volume. This copy does not consume extra space in the ZFS pool. The snapshot only records the differences between storage block references whenever the data is modified.

**Why do I want to keep snapshots?**
Snapshots keep a history of files and provide a way to recover an older or even deleted files. For this reason, many administrators take regular snapshots, store them for some time, and copy them to a different system. This strategy allows an administrator to roll the system data back to a specific point in time. In the event of catastrophic system or disk failure, off-site snapshots can restore data up to the most recent snapshot.

Taking snapshots requires the system have all pools, datasets, and zvols already configured.

### Creating a Single Snapshot

Consider making a [Periodic Snapshot Task](#) to save time and create regular, fresh snapshots.

To quickly snapshot existing storage, go to [Storage > Snapshots](#) and click ADD.

Use the Dataset drop-down list to select an existing ZFS pool, dataset, or zvol to snapshot.

The TrueNAS software displays a suggested name that you can override with any custom string. To include the snapshot in [Replication Tasks](#) choose a proper naming schema. The Naming Schema drop-down list populates with schemas already created from periodic snapshot tasks.

To include child datasets with the snapshot, set Recursive.

### Managing Snapshots

Go to [Storage > Snapshots](#) to manage created snapshots.
Each entry in the list includes the dataset and snapshot names. Click chevron_right to view options for a snapshot:

- **DATE CREATED**
The exact time and date of the snapshot creation.

- **USED**
The amount of space consumed by this dataset and all of its descendants. This value, checked against the dataset quota and reservation, shows the space used but does not include the dataset reservation. It takes into account the reservations of any descendant datasets. The amount of space that a dataset consumes from its parent, and the amount of space freed if this dataset is recursively deleted, is the greater of its space used and its reservation.

At creation, a snapshot shares space between the snapshot, file system, and even with previous snapshots. File system changes reduce the shared space and count toward a snapshot’s used space. Deleting a snapshot often increases the space that is unique and used in other snapshots.

Another method to view the space used by an individual snapshot is to go to the **Shell** and enter `zfs list -t snapshot`.

The space used, available, or referenced does not account for pending changes. Pending changes generally update within a few seconds, but larger disk changes slow usage updates.

- **REFERRED**
The amount of data accessible by this dataset. This could be shared with other datasets in the pool. New snapshots or clones reference the same amount of space as the file system or snapshot it was created from, as the contents are identical.

- **DELETE**
The **Delete** option destroys the snapshot. You must delete child clones before you can delete their parent snapshot. While creating a snapshot is instantaneous, deleting one is I/O intensive and can take a long time.
time, especially when deduplication is enabled.

**Why? expand □**
ZFS has to review all allocated blocks before deletion to see if another process is using that block. If not used, the ZFS can free that block.

**CLONE TO NEW DATASET**

Creates a new snapshot *clone* (dataset) from the snapshot contents.

**What is a clone? expand □**

A *clone* is a writable copy of the snapshot. Because a clone is actually a mountable dataset, it appears in the *Pools* screen rather than the *Snapshots* screen. Creating a new snapshot adds `-clone` to the name by default.

A dialog prompts for the new dataset name. The suggested name derives from the snapshot name.

**ROLLBACK**

Revert the Dataset back to the point in time saved by the snapshot.

Rollback is a dangerous operation that causes any configured replication tasks to fail. Replications use the existing snapshot when doing an incremental backup, and rolling back can put the snapshots 'out of order'. To restore the data within a snapshot, the recommended steps are:

1. Clone the desired snapshot.
2. Share the clone with the share type or service running on the TrueNAS system.
3. Allow users to recover their needed data.
4. Delete the clone from *Storage > Pools*.

This approach does not destroy any on-disk data and has no impact on replication.

TrueNAS asks for confirmation before rolling back to the chosen snapshot state. Clicking *Yes* reverts all dataset files to the state they were in at the time of snapshot creation.

**Bulk Operations**

To delete multiple snapshots, select the left column box for each snapshot to include. Click the *delete* button that displays.

To search through the snapshots list by name, type a matching criteria into the *search Filter Snapshots* text field. The list now displays only the snapshot names that match the filter text.

**Browsing a Snapshot Collection**

Browsing a snapshot collection is an advanced capability that requires ZFS and command-line experience.

All dataset snapshots are accessible as an ordinary hierarchical file system, accessed from a hidden .zfs located at the root of every dataset.

A snapshot and any files it contains are not accessible or searchable if the snapshot mount path is longer than 88 characters. The data within the snapshot is safe but to make the snapshot accessible again shorten the mount path.
A user with permission to access the hidden file can view and explore all snapshots for a dataset from the Shell or the Sharing screen using services like SMB, NFS, and SFTP.

In summary, the main required changes to settings are:

- In dataset properties, change the ZFS properties to enable snapshot visibility.
- In the Samba auxiliary settings, change the `veto files` command to not hide the .zfs, and add the setting `zfsacl:expose_snapdir=true`.

The effect is that any user who can access the dataset contents can view the list of snapshots by going to the dataset .zfs directory. Users can browse and search any files they have permission to access throughout the entire dataset snapshot collection.

When creating a snapshot, permissions or ACLs set on files within that snapshot might limit access to the files.

Snapshots are read-only, so users do not have permission to modify a snapshot or its files, even if they had write permissions when creating the snapshot.

The ZFS `zfs diff` command, which can run in the Shell, lists all changed files between any two snapshot versions within a dataset, or between any snapshot and the current data.
6.3 - VMware-Snapshots

Storage > VMware-Snapshots coordinates ZFS snapshots when using TrueNAS as a VMware datastore. When a ZFS snapshot is created, TrueNAS automatically snapshots any running VMware virtual machines before taking a scheduled or manual ZFS snapshot of the dataset or zvol backing that VMware datastore.

Virtual machines must be powered on for TrueNAS snapshots to be copied to VMware. The temporary VMware snapshots are then deleted on the VMware side but still exist in the ZFS snapshot and are available as stable restore points. These coordinated snapshots go in the Storage > Snapshots list.

You need a paid-edition for VMware ESXi to use VMware-Snapshots. If you try to use them with ESXi free then you will see the following error message: “Error: Can't create snapshot, current license or ESXi version prohibits execution of the requested operation.”. Indeed ESXi free has locked (read-only) API that prevents using TrueNAS VMware-Snapshots. The cheapest ESXi edition that is compatible with TrueNAS VMware-Snapshots is VMware vSphere Essentials Kit.

Create a VMware Snapshot

Go to Storage > VMware Snapshots and click ADD.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>string</td>
<td>Enter the IP address or hostname of the VMware host. When clustering, use the IP address or hostname of the vCenter server for the cluster.</td>
</tr>
<tr>
<td>Username</td>
<td>string</td>
<td>Enter a user account name created on the VMware host. The account must have permission to snapshot virtual machines.</td>
</tr>
<tr>
<td>Password</td>
<td>string</td>
<td>Enter the password associated with the Username.</td>
</tr>
<tr>
<td>ZFS Filesystem</td>
<td>browse button</td>
<td>Select a filesystem to snapshot.</td>
</tr>
<tr>
<td>Datastore</td>
<td>drop-down menu</td>
<td>After entering the Hostname, Username, and Password, click FETCH DATASTORES to populate the menu. Select the datastore to synchronize.</td>
</tr>
</tbody>
</table>

TrueNAS connects to the VMware host after clicking FETCH DATASTORES. The ZFS Filesystem and Datastore drop-down menus populate from the VMware host response. Choosing a datastore also selects any previously mapped dataset.
6.4 - Disks

6.4.1 - Wipe

The wipe function deletes obsolete data off an unused disk.

This is a destructive action and results in permanent data loss! Back up any critical data off the disk to be wiped.

To wipe a disk, go to Storage > Disks. Click the chevron_right for a disk to see all the options.

The WIPE option is only available when the disk is not in use. Click WIPE to open a dialog with additional options:

The disk Name (da1, da2, ada4) helps confirm that you have selected the right disk to wipe.

The Method dropdown shows the different available wipe options available:

 окруп Quick
Erases only the partitioning information on a disk, making it easy to reuse but without clearing other old data. Quick wipes take only a few seconds.

- **Full with zeros**
  Overwrites the entire disk with zeros and can take several hours to complete.

- **Full with random**
  Overwrites the entire disk with random binary code and takes even longer than **Full with zeros** to complete.

Ensure all data is backed up and the disk is no longer in use. Triple check that the correct disk is selected for the wipe. Recovering data from a wiped disk is usually impossible.

After choosing the appropriate method, click **WIPE**. A dialog asks for confirmation of the action.

Verify the name to ensure you have the correct disk chosen. When satisfied the disk can be wiped, set **Confirm** and click **CONTINUE**. A dialog shows the wipe progress.
6.4.2 - Replacement

- Replacing a Disk
  - Offline the Failed Disk
  - Online the New Disk

Hard drives or solid-state drives (SSDs) have a finite lifetime and can fail unexpectedly. When a disk fails in a Stripe (RAID0) pool, the entire pool has to be recreated and all data restored from backups. Creating non-stripe storage pools that have disk redundancy is always recommended.

To prevent further loss of redundancy or eventual data loss, always replace a failed disk as soon as possible! TrueNAS integrates new disks into a pool to restore the pool back to full functionality.

Replacing a Disk

Another disk of the same or greater capacity is required to replace a failed disk. This disk must be installed in the TrueNAS system and not part of an existing storage pool. Any data on the replacement disk is wiped as part of the process.

The TrueNAS Dashboard shows when a disk failure degrades a pool.

![Pool Dashboard](image)

Click the **settings** on the pool card to go to the **Storage > Pools > Pool Status** screen and locate the failed disk.

Offline the Failed Disk

Clicking **more_vert** for the failed disk shows additional operations.
It is recommended to Offline the disk before starting the replacement. This removes the device from the pool and can prevent swap issues.

**Can I use a disk that is failing but still active?**

There are some situations where a disk that has not completely failed can be left online to provide additional redundancy during the replacement procedure. **This is not recommended unless the exact condition of the failing disk is known.** Attempting to replace a heavily degraded disk without off-lining it first results in a significantly slower replacement process.

**The offline failed?**

If the Offline operation fails with a “Disk offline failed - no valid replicas” message, go to **Storage > Pools**, click the settings for the degraded pool, and select **Scrub Pool**. When the scrub operation finishes, reopen the pool **Status** and try to Offline the disk again.

When the disk status shows as Offline, physically remove the disk from the system.

If the replacement disk is not already physically added to the system, add it now.

**Online the New Disk**

In the **Pool Status**, open the options for the Offline disk and click **Replace**.

Select a new member disk and click **Replace Disk**. The new disk must have the same or greater capacity as the disk being replaced. The replacement fails when the chosen disk has partitions or data present. To destroy any data on the replacement disk and allow the replacement to continue, set the **Force** option.
When the disk wipe completes and TrueNAS starts replacing the failed disk, the **Pool Status** changes to show the in-progress replacement.

TrueNAS resilvers the pool during the replacement process. For pools with large amounts of data, this can take a long time. When the resilver is complete, the pool status screen updates to show the new disk and the pool status returns to **Online**.
6.5 - Self-Encrypting Drives

- Supported Specifications
- TrueNAS Implementation
- Deploying SEDs
  - Setting a Global Password for SEDs
  - Creating Separate Passwords for Each SED
- Check SED Functionality
- Managing SED Passwords and Data

TrueNAS version 11.1-U5 introduced Self-Encrypting Drive (SED) support.

Supported Specifications

- TCG Opal 1 legacy specification.
- TCG OPAL 2 standard for newer consumer-grade devices.
- TCG Opalite is a reduced form of OPAL 2.
- TCG Pyrite Version 1 and Version 2 are similar to Opalite, but hardware encryption is removed.
  Pyrite provides a logical equivalent of the legacy ATA security for non-ATA devices. Only the drive firmware is used to protect the device.

Pyrite Version 1 SEDs do not have PSID support and can become unusable if the password is lost.

- TCG Enterprise is designed for systems with many data disks. These SEDs do not have the functionality to be unlocked before the operating system boots.

See this Trusted Computing Group and NVM Express® joint white paper for more details about these specifications.

TrueNAS Implementation

TrueNAS implements the security capabilities of camcontrol for legacy devices and sedutil-cli for TCG devices. When managing a SED from the command line, it is recommended to use the sedhelper wrapper script for sedutil-cli to ease SED administration and unlock the full capabilities of the device. Examples of using these commands to identify and deploy SEDs are provided below.

A SED can be configured before or after assigning the device to a pool.

By default, SEDs are not locked until the administrator takes ownership of them. Ownership is taken by explicitly configuring a global or per-device password in the web interface and adding the password to the SEDs. Adding SED passwords in the web interface also allows TrueNAS to automatically unlock SEDs.

A password-protected SED protects the data stored on the device when the device is physically removed from the system. This allows secure disposal of the device without having to first wipe the contents. Repurposing a SED on another system requires the SED password.

For TrueNAS High Availability (HA) systems, SED drives are only unlocked on the active controller.

Deploying SEDs

Enter sedutil-cli --scan in the Shell to detect and list devices. The second column of the results identifies the drive type:

<p>| Character | Standard |</p>
<table>
<thead>
<tr>
<th>no</th>
<th>non-SED device</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Opal V1</td>
</tr>
<tr>
<td>2</td>
<td>Opal V2</td>
</tr>
<tr>
<td>E</td>
<td>Enterprise</td>
</tr>
<tr>
<td>L</td>
<td>Opalite</td>
</tr>
<tr>
<td>p</td>
<td>Pyrite V1</td>
</tr>
<tr>
<td>P</td>
<td>Pyrite V2</td>
</tr>
<tr>
<td>r</td>
<td>Ruby</td>
</tr>
</tbody>
</table>

Example:

```
root@truenas1:~ # sedutil-cli --scan
Scanning for Opal compliant disks
/dev/ada0  No  32GB SATA Flash Drive SFDK003L
/dev/ada1  No  32GB SATA Flash Drive SFDK003L
/dev/da0   No  HGST    HUS726020AL4210  A7J0
/dev/da1   No  HGST    HUS726020AL4210  A7J0
/dev/da10  E  WDC     WUSTR1519ASS201  B925
/dev/da11  E  WDC     WUSTR1519ASS201  B925
```

TrueNAS supports setting a global password for all detected SEDs or setting individual passwords for each SED. Using a global password for all SEDs is strongly recommended to simplify deployment and avoid maintaining separate passwords for each SED.

**Setting a Global Password for SEDs**

Go to System > Advanced > SED Password and enter the password. *Record this password and store it in a safe place!*

Now the SEDs must be configured with this password. Go to the Shell and enter `sedhelper setup <password>`, where `<password>` is the global password entered in System > Advanced > SED Password.

`sedhelper` ensures that all detected SEDs are properly configured to use the provided password:

```
root@truenas1:~ # sedhelper setup abcd1234
da9                  [OK]
da10                 [OK]
da11                 [OK]
```

Rerun `sedhelper setup <password>` every time a new SED is placed in the system to apply the global password to the new SED.

**Creating Separate Passwords for Each SED**

Go to Storage > Disks. Click the three dot menu (Options) for the confirmed SED, then Edit. Enter and confirm the password in the SED Password and Confirm SED Password fields.

The Storage > Disks screen shows which disks have a configured SED password. The SED Password column shows a mark when the disk has a password. Disks that are not a SED or are unlocked using the global password are not marked in this column.

The SED must be configured to use the new password. Go to the Shell and enter `sedhelper setup --disk <da1> <password>`, where `<da1>` is the SED to configure and `<password>` is the created password from Storage > Disks > Edit Disks > SED Password.

This process must be repeated for each SED and any SEDs added to the system in the future.

Remember SED passwords! If the SED password is lost, SEDs cannot be unlocked and their data is unavailable. Always record SED passwords whenever they are configured or modified and store them in a secure place!
Check SED Functionality

When SED devices are detected during system boot, TrueNAS checks for configured global and device-specific passwords.

Unlocking SEDs allows a pool to contain a mix of SED and non-SED devices. Devices with individual passwords are unlocked with their password. Devices without a device-specific password are unlocked using the global password.

To verify SED locking is working correctly, go to the Shell. Enter `sedutil-cli --listLockingRange 0 <password> <dev/da1>`, where `<dev/da1>` is the SED and `<password>` is the global or individual password for that SED. The command returns `ReadLockEnabled: 1, WriteLockEnabled: 1, and LockOnReset: 1` for drives with locking enabled:

```
root@truenas1:~ # sedutil-cli --listLockingRange 0 abcd1234 /dev/da9
Band[0]:
    Name:        Global_Range
    CommonName:  Locking
    RangeStart:  0
    RangeLength: 0
    ReadLockEnabled: 1
    WriteLockEnabled: 1
    ReadLocked:  0
    WriteLocked:  0
    LockOnReset:  1
```

Managing SED Passwords and Data

This section contains command line instructions to manage SED passwords and data. The command used is `sedutil-cli(8)`. Most SEDs are TCG-E (Enterprise) or TCG-Opal (Opal v2.0). Commands are different for the different drive types, so the first step is identifying which type is being used.

These commands can be destructive to data and passwords. Keep backups and use the commands with caution.

Check SED version on a single drive, `/dev/da0` in this example:

```
root@truenas:~ # sedutil-cli --isValidSED /dev/da0
/dev/da0 SED --E--- Micron_5N/A U402
```

All connected disks can be checked at once:

```
root@truenas:~ # sedutil-cli --scan
Scanning for Opal compliant disks
/dev/da0 No 32GB SATA Flash Drive SFDK003L
/dev/da1 No 32GB SATA Flash Drive SFDK003L
/dev/da0 E Micron_5N/A U402
/dev/da1 E Micron_5N/A U402
/dev/da2 E SEAGATE XS3840TE70014 0103
/dev/da3 E SEAGATE XS3840TE70014 0103
/dev/da4 E Micron_5N/A U402
/dev/da5 E Micron_5N/A U402
/dev/da6 E Micron_5N/A U402
/dev/da9 E Micron_5N/A U402
No more disks present ending scan
root@truenas:~ #
```

TCG-Opal Instructions

Reset the password without losing data: `sedutil-cli --revertNoErase <oldpassword> </dev/device>`

Use both of these commands to change the password without destroying data:

```
sedutil-cli --setSIDPassword <oldpassword> <newpassword> </dev/device>
sedutil-cli --setPassword <oldpassword> Admin1 <newpassword> </dev/device>
```

Wipe data and reset password to default MSID: `sedutil-cli --revertTPer <oldpassword> </dev/device>`

Wipe data and reset password using the PSID: `sedutil-cli --
TCG-E Instructions

Change or Reset the Password without Destroying Data

These commands must be run for every LockingRange or band on the drive. To determine the number of bands on a drive, use `sedutil-cli -v --listLockingRanges /dev/device`. Increment the BandMaster number and rerun the command with `--setPassword` for every band that exists.

Use all of these commands to reset the password without losing data:

```
sedutil-cli --setSIDPassword <oldpassword> "" /dev/device
sedutil-cli --setPassword <oldpassword> EraseMaster "" /dev/device
sedutil-cli --setPassword <oldpassword> BandMaster0 "" /dev/device
sedutil-cli --setPassword <oldpassword> BandMaster1 "" /dev/device
```

Use all of these commands to change the password without destroying data:

```
sedutil-cli --setSIDPassword <oldpassword> <newpassword> /dev/device
sedutil-cli --setPassword <oldpassword> BandMaster0 <newpassword> /dev/device
sedutil-cli --setPassword <oldpassword> BandMaster1 <newpassword> /dev/device
```

Reset Password and Wipe Data

Reset to default MSID:

```
sedutil-cli --eraseLockingRange 0 <password> /dev/device
sedutil-cli --setSIDPassword <oldpassword> "" /dev/device
sedutil-cli --setPassword <oldpassword> EraseMaster "" /dev/device
```

Reset using the PSID:

```
sedutil-cli --PSIDrevertAdminSP <PSIDNODASHS> /dev/<device>
```

If it fails use:

```
sedutil-cli --PSIDrevert <PSIDNODASHS> /dev/<device>
```
6.6 - Import Disk

Use Storage > Import Disk to integrate UFS (BSD Unix), NTFS (Windows), MSDOS (FAT), or EXT2 (Linux) formatted disks into TrueNAS. This is a one-time import, copying the data from that disk into a TrueNAS dataset. Only one disk can be imported at a time, and the disk must be installed or physically connected to the TrueNAS system.

**What about EXT3 or EXT4 filesystems? expand □**

Importing an EXT3 or EXT4 filesystem is possible in some cases, although neither is fully supported. EXT3 journaling is not supported, so those filesystems must have an external `fsck` utility, like the one provided by E2fsprogs utilities, run on them before import. EXT4 filesystems with extended attributes or inodes greater than 128 bytes are not supported. EXT4 filesystems with EXT3 journaling must have an `fsck` run on them before import, as described above.

Use the drop-down menu to select the **Disk** to import.

TrueNAS attempts to detect and select the the **Filesystem type**. Selecting the MSDOSFS filesystem shows an additional **MSDOSFS locale** drop-down menu. Use this option to select the locale when non-ASCII characters are present on the disk.

Finally, browse to the ZFS dataset to hold the copied data and define the **Destination Path**.

After clicking **SAVE**, the chosen **Disk** mounts and its contents copied to the specified dataset at the end of the **Destination Path**. To monitor an in-progress import, open the Task Manager by clicking the **assignment** in the interface top bar. The disk unmounts after the copy operation completes. A dialog allows viewing or downloading the disk import log.

**The import was interrupted! expand □**

Use the same import procedure to restart the task. Choose the same **Destination Path** as the interrupted import for TrueNAS to scan the destination for previously imported files and resume importing any remaining files.
The Active Directory (AD) service shares resources in a Windows network. AD provides authentication and authorization services for the users in a network, eliminating the need to recreate the user accounts on TrueNAS.

Once joined to an AD domain, you can use domain users and groups in local ACLs on files and directories. You can also set up shares to act as a file server.

Joining an AD domain also configures the Privileged Access Manager (PAM) to let domain users log on via SSH or authenticate to local services.

Users can configure AD services on Windows or Unix-like operating systems running Samba version 4.

To configure a connection, you will need to know the Active Directory domain controller’s domain and that system’s account credentials.

**Preparation**

Users can take a few steps before configuring Active Directory to ensure the connection process goes smoothly.

- **Verify Name Resolution**

  To confirm that name resolution is functioning, go to the **Shell** and use `ping` to check the connection to the AD domain controller.
When packets are being sent and received without loss, the connection is verified. Press Ctrl + c to cancel the ping.

Another option is to use `host -t srv _ldap._tcp.domainname.com` to check the network’s SRV records and verify DNS resolution.

The ping failed! expand □
If the ping fails, go to Network > Global Configuration and update the DNS Servers and Default Gateway settings so the connection to your Active Directory Domain Controller can start. Use more than one Nameserver for the AD domain controllers so DNS queries for requisite SRV records can succeed. Using more than one Nameserver helps maintain the AD connection whenever a domain controller becomes unavailable.

Time Synchronization

Active Directory relies on Kerberos, a time-sensitive protocol. During the domain join process, the AD domain controller with the PDC Emulator FSMO Role is added as the preferred NTP server. If your environment requires something different, you can change NTP server settings in System > NTP Servers.

The local system time cannot be out of sync by more than five minutes with the AD domain controller time in a default AD environment. Use an external time source when configuring a virtualized domain controller. TrueNAS creates an Alert if the system time gets out of sync with the AD domain controller time.

There are a few options in TrueNAS to ensure both systems are synchronized:
Go to System > General and make sure the Timezone matches the AD Domain Controller.

Set either localtime or universal time in the system BIOS.

**Connect to the Active Directory Domain**

To connect to Active Directory, go to Directory Services > Active Directory and enter the AD Domain Name and account credentials. Set Enable to attempt to join the AD domain immediately after saving the configuration.

Advanced options are available for fine-tuning the AD configuration, but the preconfigured defaults are generally suitable.
I don't see any AD information! expand □

TrueNAS can take a few minutes to populate the AD information after configuring the Active Directory service. To check the AD join progress, open the assignment Task Manager in the upper-right corner. TrueNAS displays any errors during the join process in the Task Manager.

When the import is complete, AD users and groups become available while configuring basic dataset permissions or an Access Control List (ACL) with TrueNAS cache enabled (enabled by default).

Joining AD also adds default Kerberos realms and generates a default AD_MACHINE_ACCOUNT keytab. TrueNAS automatically begins using this default keytab and removes any administrator credentials stored in the TrueNAS configuration file.

**Advanced Options**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verbose logging</td>
<td>Set to log attempts to join the domain to /var/log/messages.</td>
</tr>
<tr>
<td>Allow Trusted Domains</td>
<td>When set, usernames do not include a domain name. Unset to force domain names to be prepended to user names. One possible reason for unset this value is to prevent username collisions when Allow Trusted Domains is set and there are identical usernames in more than one domain</td>
</tr>
<tr>
<td>Use Default Domain</td>
<td>Unset to prepend the domain name to the username. Unset to prevent name collisions when Allow Trusted Domains is set and multiple domains use the same username.</td>
</tr>
<tr>
<td>Allow DNS Updates</td>
<td>Set to enable Samba to do DNS updates when joining a domain.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disable FreeNAS Cache</td>
<td>Set to disable caching AD users and groups. This can help when unable to bind to a domain with a large number of users or groups.</td>
</tr>
<tr>
<td>Restrict PAM</td>
<td>Set to restrict SSH access in certain circumstances to only members of BUILTIN\Administrators.</td>
</tr>
<tr>
<td>Site Name</td>
<td>Enter the relative distinguished name of the site object in the Active Directory.</td>
</tr>
<tr>
<td>Kerberos Realm</td>
<td>Select an existing realm that was added in Directory Services &gt; Kerberos Realms.</td>
</tr>
<tr>
<td>Kerberos Principal</td>
<td>Select the location of the principal in the keytab created in Directory Services &gt; Kerberos Keytabs.</td>
</tr>
<tr>
<td>Computer Account OU</td>
<td>The OU in which new computer accounts are created. The OU string is read from top to bottom without RDNs. Slashes (&quot;&quot;) are used as delimiters, like Computers/Servers/NAS. The backslash (&quot;&quot;) is used to escape characters but not as a separator. Backslashes are interpreted at multiple levels and might require doubling or even quadrupling to take effect. When this field is blank, new computer accounts are created in the Active Directory default OU.</td>
</tr>
<tr>
<td>AD Timeout</td>
<td>Number of seconds before timeout. To view the AD connection status, open the interface Task Manager.</td>
</tr>
<tr>
<td>DNS Timeout</td>
<td>Number of seconds before a timeout. Increase this value if AD DNS queries time out.</td>
</tr>
<tr>
<td>Winbind NSS Info</td>
<td>Choose the schema to use when querying AD for user/group info. rfc2307 uses the schema support included in Windows 2003 R2, sfu is for Service For Unix 3.0 or 3.5, and sfu20 is for Service For Unix 2.0.</td>
</tr>
<tr>
<td>Netbios Name</td>
<td>Netbios Name of this NAS. This name must differ from the Workgroup name and be no greater than 15 characters.</td>
</tr>
<tr>
<td>NetBIOS alias</td>
<td>Alternative names that SMB clients can use when connecting to this NAS. Can be no greater than 15 characters.</td>
</tr>
<tr>
<td>EDIT IDMAP</td>
<td>Navigates to Directory Services &gt; Idmap so the user can edit the Active Directory’s Idmap</td>
</tr>
<tr>
<td>LEAVE DOMAIN</td>
<td>Disconnects the TrueNAS system from the Active Directory.</td>
</tr>
</tbody>
</table>

**FTP Access**

While SFTP is recommended over FTP, joined systems do allow FTP access. Please keep these caveats in mind:

- By default, authentication uses **DOMAIN\username** as the user name.
- A user home directory needs to exist before joining.
- An AD user cannot be added to the FTP group. Enable local user auth for FTP instead.
- An existing samba homes share created in the GUI is set as the **template homedir** for AD users. This means that AD user home directories are set inside that path. Proper permissions are vital.
- There are no guarantees about how proftpd handles ACLs.
- The admin (or **pam_mkhomedir**) must ensure that paths exist when AD users have populated homedir information in their LDAP schema.
- When the admin is pulling home directories from their LDAP schema, take extra caution to insure that users aren’t writing files to the boot device.

**Troubleshooting**
If the cache becomes out of sync or fewer users than expected are available in the permissions editors, resync it using **Directory Service > Active Directory > REBUILD DIRECTORY SERVICE CACHE**.

If you are using Windows Server with 2008 R2 or older, try creating a **Computer** entry on the Windows server Organizational Unit (OU). When creating this entry, enter the TrueNAS hostname in the name field. Make sure it is the same name as the one set in the **Hostname** field in **Network > Global Configuration**, and the **NetBIOS alias** from **Directory Service > Active Directory > Advanced Options**.

---

**Shell Commands**

You can go to the **Shell** and enter various commands to get more details about the AD connection and users:

- **AD current state**: `midclt call activedirectory.get_state`
- **Details about the currently connected Lightweight Directory Access Protocol (LDAP) server**: `midclt call activedirectory.domain_info | jq`

  ```bash
  truenas# midclt call activedirectory.domain_info | jq
  {
    "LDAP server": "192.168.1.125",
    "LDAP server name": "DC01.HOMEDOM.FUN",
    "Realm": "HOMEDOM.FUN",
    "Bind Path": "dc=HOMEDOM,dc=FUN",
    "LDAP port": 389,
    "Server time": 1593026080,
    "KDC server": "192.168.1.125",
    "Server time offset": 5,
    "Last machine account password change": 1592423446
  }
  ```

  - **View AD users**: `wbinfo -u`. To see more details about a user, enter `getent passwd DOMAIN\<user>`, replacing `<user>` with the desired user name. If `wbinfo -u` shows more users than appear to be available when configuring permissions and the TrueNAS cache is enabled, go to **Directory Services > Active Directory** and increase the **AD Timeout** value.
  - **View AD groups**: `wbinfo -g`. To see more details, enter `getent group DOMAIN\domain\users`.
  - **View domains**: `wbinfo -m`.
  - **Test AD connection**: `wbinfo -t`. A successful test shows a message similar to **checking the trust secret for domain YOURDOMAIN via RPC calls succeeded**.
  - **User connection test to an SMB share**: `smbclient '//127.0.0.1/smbshare -u AD01.LAB.IXSYSTEMS.COM\ixuser`, replacing 127.0.0.1 with your server address, smbshare with the SMB share name, AD01.LAB.IXSYSTEMS.COM with your trusted domain, and ixuser with the user account name for authentication testing.
TrueNAS includes an Open LDAP client for accessing information from an LDAP server. An LDAP server provides directory services for finding network resources such as users and their associated permissions.

### Does LDAP work with SMB?
LDAP authentication for SMB shares is disabled unless the LDAP directory has been configured for and populated with Samba attributes. The most popular script for performing this task is `smbldap-tools`. The LDAP server must support SSL/TLS and the certificate for the LDAP server CA must be imported. Non-CA certificates are not currently supported.

To integrate an LDAP server with TrueNAS, go to **Directory Services > LDAP**.

#### Server Credentials

- **Hostname**
- **Base DN**
- **Bind DN**
- **Bind Password**

#### What does this do?
If a host does not respond, the next host in the list is tried until a new connection is established.

Enter any LDAP server hostnames or IP addresses. Separate entries with an empty space. Entering multiple hostnames or IP addresses creates an LDAP failover priority list.

Enter the **Base DN**. This is the top level of the LDAP directory tree to be used when searching for resources. For example, `dc=test,dc=org`.

Enter the **Bind DN**. This is the administrative account name on the LDAP server. For example, `cn=Manager,dc=test,dc=org`.

Next, enter the **Bind Password**. This is the password associated with the **Bind DN** account.

The final basic option is **Enable**. Unsetting **Enable** disables the LDAP configuration without deleting it. It can be enabled at a later time without reconfiguring the options.

#### Advanced Configuration
To further modify the LDAP configuration, click **ADVANCED OPTIONS**.
Setting *Allow Anonymous Binding* disables authentication and allows read and write access to any client.

If a *Kerberos* realm has been added to TrueNAS, it can be selected from the *Kerberos Realm* dropdown. Likewise, if a Kerberos keytab has been created, select it in the *Kerberos Principal* dropdown.

If an encryption mode for the LDAP connection is desired, select one of these options from the *Encryption Mode* dropdown:

- **OFF**: do not encrypt the LDAP connection.
- **ON**: encrypt the LDAP connection with SSL on port 636.
- **START_TLS**: encrypt the LDAP connection with STARTTLS on the default LDAP port 389.

A certificate is not required when using username/password or Kerberos authentication. If certificate authentication is desired, select a certificate to use from the *Certificate* dropdown. To configure LDAP certificate-based authentication, create a Certificate Signing Request for the LDAP provider to sign.

To validate the authenticity of the certificate, set *Validate Certificates*.

Set *Disable LDAP User/Group Cache* to disable caching LDAP users and groups in large LDAP environments. When caching is disabled, LDAP users and groups do not appear in dropdown menus, but are still accepted when manually entered.

Increase *LDAP timeout* if a Kerberos ticket queries are not responding within the default time. *LDAP timeout* is in seconds. Increase *DNS timeout* if DNS queries take too long to respond. *DNS timeout* is in seconds.

*Samba Schema* is deprecated in *Samba 4.13.0*. Set *Samba Schema* if LDAP authentication for SMB shares is required and the LDAP server is already configured with Samba attributes. If *Samba Schema* is set, select the type of schema from the *Schema* dropdown.

*Auxiliary Parameters* can be specified for *nslcd.conf*. 
NIS (Network Information Service) is a client–server directory service protocol for distributing system configuration data such as user and host names between computers on a computer network.

**What exactly does this do? expand □**
A NIS system maintains and distributes a central directory of user and group information, hostnames, email aliases and other text-based tables of information in a computer network. In FreeBSD, the list of users is placed in /etc/passwd and authentication hashes in /etc/shadow. NIS adds another “global” user list to identify users on any NIS domain client.

NIS is limited in scalability and security. For modern networks, LDAP has replaced NIS.

To configure NIS, go to **Directory Services > NIS**.

Enter the **NIS Domain** name and list any **NIS Servers** (hostnames or IP addresses). Press **Enter** to separate server entries. Configure the remaining options as needed:

- **Secure Mode**: Set to have *ypbind(8)* refuse to bind to any NIS server not running as root on a TCP port over 1024.
- **Mancast**: Set for *ypbind* to bind to the fastest responding server.
- **Enable**: Unset to disable the configuration without deleting it.

When ready, SAVE the configuration.
7.4 - Kerberos

- Kerberos Realms
  - Kerberos Keytabs
    - Create Keytab on Windows Server for Active Directory
    - Add Windows Keytab to TrueNAS
  - Kerberos Settings

Kerberos is a web authentication protocol that uses strong cryptography to prove the identity of both client and server over an insecure network connection.

Kerberos uses “realms” and “keytabs” to authenticate clients and servers. A Kerberos realm is an authorized domain that a Kerberos server can use to authenticate a client. By default, TrueNAS creates a Kerberos realm for the local system. A keytab ("key table") is a file that stores encryption keys for various authentication scenarios.

TrueNAS allows configuring both Kerberos realms and keytabs.

Kerberos Realms

Your network must contain a Key Distribution Center (KDC) to add a realm. Users can configure Kerberos realms by navigating to Directory Services > Kerberos Realms and clicking ADD.

Enter the Realm name and click SUBMIT.

<table>
<thead>
<tr>
<th>Advanced Options</th>
<th>expand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>KDC</td>
<td>Enter the name of the Key Distribution Center. Separate multiple values by pressing Enter.</td>
</tr>
<tr>
<td>Admin Server</td>
<td>Define the server where all changes to the database are performed. Separate multiple values by pressing Enter.</td>
</tr>
<tr>
<td>Password Server</td>
<td>Define the server where all password changes are performed. Separate multiple values by pressing Enter.</td>
</tr>
</tbody>
</table>

Kerberos Keytabs

Kerberos keytabs allow systems and clients to join an Active Directory or LDAP without a password. With keytabs, the TrueNAS system database does not store the Active Directory or LDAP administrator account password, which can be a security risk in some environments.

When using a keytab, create and use a less privileged account to perform any required queries. The TrueNAS system database stores the password for that account.

Create Keytab on Windows Server for Active Directory

To create the keytab on a Windows Server system, open a Command Prompt and use the ktpass.
command:

ktpass -princ USERNAME@REALM.COM -pass PASSWORD -crypto ENCRYPTION TYPE -ptype KRB5_NT_PRINCIPAL -kvno 0 -out c:\PATH\KEYTABNAME.KEYTAB

USERNAME@REALM.COM is the Windows Server user and principal name written in the format username@KERBEROS.REALM. The Kerberos Realm is typically in all caps, but the Kerberos Realm case should match the realm name. See this note about using /princ for more details.

PASSWORD is the Windows Server user's password.

ENCRYPTION TYPE is the cryptographic type you want to use. Setting ENCRYPTION TYPE to ALL allows using all supported cryptographic types. Users can specify each key instead of ALL:

- DES-CBC-CRC is used for compatibility.
- DES-CBC-MD5 is used for compatibility and adheres more closely to the MIT implementation.
- RC4-HMAC-NT uses 128-bit encryption.
- AES256-SHA1 uses AES256-CTS-HMAC-SHA1-96 encryption.
- AES128-SHA1 uses AES128-CTS-HMAC-SHA1-96 encryption. Specifying cryptographic types creates a keytab with sufficient privileges to grant tickets.

PATH\KEYTABNAME.KEYTAB is the path where you want to save the keytab and the name you want it to have.

An example ktpass command would look like this:

ktpass -princ admin@WINDOWSSERVER.NET -pass Abcd1234! -crypto ALL -ptype KRB5_NT_PRINCIPAL -kvno 0 -out c:\kerberos\freenas.keytab

Add Windows Keytab to TrueNAS

After generating the keytab, add it to the TrueNAS system in Directory Services > Kerberos Keytabs > Add Kerberos Keytab.

To instruct the Active Directory service to use the keytab, go to Directory Services > Active Directory and click Advanced Options. Select the installed keytab using the Kerberos Principal drop-down.

When using a keytab with Active Directory, username and userpass in the keytab should match the Domain Account Name and Domain Account Password fields in Directory Services > Active Directory.

To instruct LDAP to use a principal from the keytab, go to Directory Services > Active Directory and click Advanced Options, then select the installed keytab using the Kerberos Principal drop-down.

Kerberos Settings

Additional Kerberos options are in Directory Services > Kerberos Settings.
- **Appdefaults Auxiliary Parameters**: Define any additional settings for use by some Kerberos applications. The available settings and syntax is listed in the [appdefaults] section of krb.conf(5).
- **Libdefaults Auxiliary Parameters**: Define any settings used by the Kerberos library. The available settings and their syntax are listed in the [libdefaults] section of krb.conf(5).
8 - Sharing

File sharing is a core benefit of a NAS. TrueNAS helps foster collaboration between users through network shares. TrueNAS can use AFP, iSCSI shares, Unix NFS shares, Windows SMB shares, and WebDAV shares.

Ready to get started? Choose a topic or article from the left-side Navigation pane. Click the < symbol to expand the menu to show the topics under this section.
The Apple Filing Protocol (AFP) is a network protocol that allows file sharing over a network. AFP is similar to SMB and NFS shares but made specifically for Apple systems.

Beginning in 2013, Apple began using the SMB sharing protocol as the default file sharing option. It has ceased development of the AFP sharing protocol. Use SMB sharing instead of AFP, unless sharing files with legacy Apple products.

If using an AFP share, create the dataset with the Share Type set to Generic.


To create a new share, make sure a dataset is available with all the data for sharing.

**AFP Share Configuration**

To configure the new share, go to Sharing > Apple Shares (AFP) and click ADD. You must confirm that you intend to create an AFP share because it is now deprecated. Next, use the file browser to select the dataset created to share and enter a descriptive name for the share.

When the share is to have Time Machine backups, set Time Machine. This advertises the share to other Mac systems as a disk that stores Time Machine backups. It is not recommended to have multiple AFP shares configured for Time Machine backups.

Setting Use as Home Share creates home directories for users that connect to the share. Only one AFP share can be a home share.

The Enable option for an AFP share is the default selection. To create the share but not immediately enable it, unset Enable. Click SUBMIT to create the share.
Opening the **ADVANCED OPTIONS** allows you to modify the share using the **Permissions**, **Description**, and **Auxiliary Parameters** settings.
To edit an existing AFP share, go to **Sharing > Apple Shares (AFP)** and click .

**AFP Service**

To begin advertising the AFP shared location, go to **Services** and use the AFP toggle to set it to running. To automatically start the service after TrueNAS boots, select **Start Automatically**.

We recommend you use the default settings for the AFP service. To adjust the service settings, click .
Connecting to the AFP Share

Use an Apple operating system to connect to the share. First, open the Apple Finder app and click Go > Connect to Server... in the Apple top menu bar. Next, enter `afp://{IPofTrueNASsystem}` and click Connect. For example, entering `afp://192.168.2.2` connects to the TrueNAS AFP share at 192.168.2.2.
8.2 - Block Shares (iSCSI)

iSCSI (Internet Small Computer Systems Interface) represents standards for using Internet-based protocols for linking binary data storage device aggregations. IBM and Cisco submitted the draft standards in March 2000. Since then, iSCSI has seen widespread adoption into enterprise IT environments.

iSCSI functions through encapsulation. The OSI (Open Systems Interconnection Model) encapsulates SCSI commands and storage data within the session stack. The OSI further encapsulates the session stack within the transport stack, the transport stack within the network stack, and the network stack within the data stack. Transmitting data this way permits block-level access to storage devices over LANs, WANs, and even the Internet itself (although performance may suffer if your data traffic is traversing the Internet).

The table below shows where iSCSI sits in the OSI network stack:

<table>
<thead>
<tr>
<th>OSI Layer Number</th>
<th>OSI Layer Name</th>
<th>Activity as it relates to iSCSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application</td>
<td>An application tells the CPU that it needs to write data to non-volatile storage.</td>
</tr>
<tr>
<td>6</td>
<td>Presentation</td>
<td>OSI creates a SCSI Command, SCSI Response, or SCSI data payload to hold the application data and communicate it to non-volatile storage.</td>
</tr>
<tr>
<td>5</td>
<td>Session</td>
<td>Communication between the source and the destination devices begins. This communication establishes when the conversation starts, what it will talk about, and when the conversation ends. This entire dialogue represents the session. OSI encapsulates the SCSI Command, SCSI Response, or SCSI data payload containing the application data within an iSCSI Protocol Data Unit (PDU).</td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
<td>OSI encapsulates the iSCSI PDU within a TCP segment.</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
<td>OSI encapsulates the TCP segment within an IP packet.</td>
</tr>
<tr>
<td>2</td>
<td>Data</td>
<td>OSI encapsulates the IP packet within the Ethernet frame.</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
<td>The Ethernet frame transmits as bits (zeros and ones).</td>
</tr>
</tbody>
</table>

Unlike other sharing protocols on TrueNAS, an iSCSI share allows block sharing and file sharing. Block sharing provides the benefit of block-level access to data on the TrueNAS. iSCSI exports disk devices (zvols on TrueNAS) over a network that other iSCSI clients (initiators) can attach and mount.

**iSCSI Terminology**

- **CHAP (Challenge-Handshake Authentication Protocol):** an authentication method that uses a shared secret and three-way authentication to determine if a system is authorized to access the storage device. It also periodically confirms that the session has not been hijacked by another system. In iSCSI, the client (initiator) performs the CHAP authentication.

- **Mutual CHAP:** a CHAP type in which both ends of the communication authenticate to each other.

- **Internet Storage Name Service (iSNS):** protocol for the automated discovery of iSCSI devices on a TCP/IP network.

- **Extent:** the storage unit to be shared. It can either be a file or a device.

- **Portal:** indicates which IP addresses and ports to listen on for connection requests.

- **Initiators and Targets:** iSCSI introduces the concept of initiators and targets which act as sources and destinations respectively. iSCSI initiators and targets follow a client/server model. Below is a diagram of a typical iSCSI network. The TrueNAS storage array acts as the iSCSI target and can be accessed by many of the different iSCSI initiator types, including software and hardware-
Accelerated initiators.

The iSCSI protocol standards require that iSCSI initiators and targets be represented as iSCSI nodes. It also requires that each node be given a unique iSCSI name. To represent these unique nodes via their names, iSCSI requires the use of one of two naming conventions and formats, IQN or EUI. iSCSI also allows the use of iSCSI aliases which are not required to be unique and can be help manage nodes.

- **LUN: Logical Unit Number** representing a logical SCSI device. An initiator negotiates with a target to establish connectivity to a LUN. The result is an iSCSI connection that emulates a connection to a SCSI hard disk. Initiators treat iSCSI LUNs as if they were a raw SCSI or SATA hard drive. Rather than mounting remote directories, initiators format and directly manage filesystems on iSCSI LUNs. When configuring multiple iSCSI LUNs, create a new target for each LUN. Since iSCSI multiplexes a target with multiple LUNs over the same TCP connection, there can be TCP contention when more than one target accesses the same LUN. TrueNAS supports up to 1024 LUNs.

- **Jumbo Frames**: Jumbo frames are the name given to Ethernet frames that exceed the default 1500 byte size. This parameter is typically referenced by the nomenclature as maximum transmission unit (MTU). MTU that exceeds the default 1500 bytes necessitates that all devices transmitting Ethernet frames between the source and destination support the specific jumbo frame MTU setting, which means that NICs, dependent hardware iSCSI, independent hardware iSCSI cards, ingress and egress Ethernet switch ports, and the NICs of the storage array must all support the same jumbo frame MTU value. So, how does one decide if they should use jumbo frames?

Administrative time is consumed configuring Jumbo Frames and troubleshooting if/when things go sideways. Some network switches might also have ASICs optimized for processing MTU 1500 frames while others might be optimized for larger frames. Systems administrators should also account for the impact on host CPU utilization. Although Jumbo Frames are designed to increase data throughput, it may measurably increase latency (as is the case with some un-optimized switch ASICs); latency is typically more important than throughput in a VMware environment. Some iSCSI applications might see a net benefit running jumbo frames despite possible increased latency. Systems administrators should test jumbo frames on their workload with lab infrastructure as much as possible before updating the MTU on their production network.

**TrueNAS Enterprise Feature:**

- **ALUA: Asymmetric Logical Unit Access** allows a client computer to discover the best path to the storage on a TrueNAS system. HA storage clusters can provide multiple paths to the same storage. For example, the disks are directly connected to the primary computer and provide high speed and bandwidth when accessed through that primary computer. The same disks are also available through the secondary computer, but speed and bandwidth are restricted. With ALUA, clients automatically ask for and use the best path to the storage. If one of the TrueNAS HA computers becomes inaccessible, the clients automatically switch to the next best alternate path to the storage. When a better path becomes available, as when the primary host becomes available again, the clients automatically switch back to that better path to the storage.

Do not enable ALUA on TrueNAS unless it is also supported by and enabled on the client computers. ALUA only works when enabled on both the client and server.
iSCSI Configuration Methods

There are a few different approaches for configuring and managing iSCSI-shared data:

- TrueNAS CORE web interface: the TrueNAS web interface is fully capable of configuring iSCSI shares. This requires creating and populating zvol block devices with data, then setting up the iSCSI Share. TrueNAS Enterprise licensed customers also have additional options to configure the share with Fibre Channel.

- TrueNAS SCALE web interface: TrueNAS SCALE offers a similar experience to TrueNAS CORE for managing data with iSCSI; create and populate the block storage, then configure the iSCSI share.

- TrueCommand instances that have many TrueNAS systems connected can manage iSCSI Volumes from the TrueCommand web interface. TrueCommand allows creating block devices and configuring iSCSI Targets and Initiators from one central location.

- TrueNAS Enterprise customers that use vCenter to manage their systems can use the TrueNAS vCenter Plugin to connect their TrueNAS systems to vCenter and create and share iSCSI datastores. This is all managed through the vCenter web interface.
8.2.1 - iSCSI Shares

- Wizard Setup
- Manual Setup
- Starting the iSCSI Service
- Using the iSCSI Share
- Expanding LUNs

To get started, make sure you have created a [zvol](#) or a [dataset](#) with at least one file to share.

Go to **Sharing > Block Shares (iSCSI)**. You can either set one up manually or use the wizard to guide you through creation.

**Wizard Setup**

- **Block Device**

First, enter a name for the iSCSI share. It can only contain lowercase alphanumeric characters plus a dot (.), dash (-), or colon (:). We recommend keeping the name short or at most 63 characters. Next, choose the **Extent Type**.

- If the **Extent Type** is **Device**, select the Zvol to share from the **Device** menu.
- If the **Extent Type** is **File**, select the path to the Extent and indicate the file size.

Select the type of platform that will be using the share. For example, if using the share from an updated Linux OS, choose **Modern OS**.

- **Portal**

Now you will either create a new portal or select an existing one from the dropdown.

If you create a new portal, you will need to select a **Discovery Authentication Method**.

If you set the **Discovery Authentication Method** to **CHAP** or **MUTUAL CHAP**, you will also need to select a **Discovery Authentication Group**. If no group exists, click **Create New** from the drop-down and enter a **Group ID**, **User**, and **Secret**.
When the *Discovery Authentication Method* is *NONE*, the *Discovery Authentication Group* can be left empty.

Select **0.0.0.0** or **::** from the *IP Address* dropdown and click *NEXT*.

**What are these options?**

- **0.0.0.0** listens on all IPv4 addresses and **::** listens on all IPv6 addresses.

**Initiator**

Decide which initiators or networks can use the iSCSI share. Leave the list empty to allow all initiators or networks, or add entries to the list to limit access to those systems.

**Confirm**

Confirm the settings are correct and click *SUBMIT*.

**Manual Setup**

**Target Global Configuration**

The *Target Global Configuration* tab lets users configure settings that will apply to all iSCSI shares.
Setting Description

Base Name Lowercase alphanumeric characters plus dot (.), dash (-), and colon (:) are allowed. See the Constructing iSCSI names using the `iqn.format` section of [RFC3721](https://www.rfc-editor.org/rfc/rfc3721).

ISNS Servers Hostnames or IP addresses of the ISNS servers to be registered with the iSCSI targets and portals of the system. Separate entries by pressing Enter.

Pool Available Space Threshold (%) Generate an alert when the pool has this percent space remaining. This is typically configured at the pool level when using zvols or at the extent level for both file and device-based extents.

Portals

The Portals tab lets users create new portals or edit existing ones in the list.

To add a new portal, click **ADD** and enter the basic and IP address information.

To edit an existing portal, click **more_vert** next to the portal and select **Edit**.

Basic Info

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Optional description. Portals are automatically assigned a numeric group.</td>
</tr>
</tbody>
</table>

Authentication Method and Group
iSCSI supports multiple authentication methods that the target uses to discover valid devices. *None* allows anonymous discovery while *CHAP* and *Mutual CHAP* require authentication.

Group ID created in Authorized Access. Required when the Discovery Authentication Method is CHAP or Mutual CHAP.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery Authentication Method</td>
<td>iSCSI supports multiple authentication methods that the target uses to discover valid devices. None allows anonymous discovery while CHAP and Mutual CHAP require authentication.</td>
</tr>
<tr>
<td>Discovery Authentication Group</td>
<td>Group ID created in Authorized Access. Required when the Discovery Authentication Method is CHAP or Mutual CHAP.</td>
</tr>
</tbody>
</table>

**IP Address**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Select the IP addresses to be listened on by the portal. Click ADD to add IP addresses with a different network port. 0.0.0.0 listens on all IPv4 addresses and :: listens on all IPv6 addresses.</td>
</tr>
<tr>
<td>Port</td>
<td>TCP port used to access the iSCSI target. Default is 3260.</td>
</tr>
<tr>
<td>ADD</td>
<td>Adds another IP address row.</td>
</tr>
</tbody>
</table>

**Initiators Groups**

The *Initiators Groups* tab lets users create new authorized access client groups or edit existing ones in the list.

To add a new initiators group, click *ADD* and either leave *Allow All Initiators* checked or configure your own allowed initiators and authorized networks.

To edit an existing initiators group, click *more_vert* next to the initiators group and select *Edit*.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow All Initiators</td>
<td>Allows All Initiators when checked.</td>
</tr>
<tr>
<td>Allowed Initiators (IQN)</td>
<td>Initiators allowed access to this system. Enter an iSCSI Qualified Name (IQN) and click + to add it to the list. Example: iqn.1994-09.org.freebsd:freenas.local.</td>
</tr>
<tr>
<td>Authorized Networks</td>
<td>Network addresses allowed use this initiator. Each address can include an optional CIDR netmask. Click + to add the network address to the list. Example: 192.168.2.0/24.</td>
</tr>
<tr>
<td>Description</td>
<td>Any notes about initiators.</td>
</tr>
</tbody>
</table>

**Authorized Access**

The *Authorized Access* tab lets users create new authorized access networks or edit existing ones in the list.
To add a new authorized access network, click **ADD** and fill out the group, user, and peer user information.

To edit an existing authorized access network, click more_vert next to it and select **Edit**.

### Group

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID</td>
<td>Allow different groups to be configured with different authentication profiles. Example: all users with a group ID of 1 will inherit the authentication profile associated with Group 1.</td>
</tr>
</tbody>
</table>

### User

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>User account to create for CHAP authentication with the user on the remote system. Many initiators use the initiator name as the user name.</td>
</tr>
<tr>
<td>Secret</td>
<td>User password. Must be at least 12 and no more than 16 characters long.</td>
</tr>
<tr>
<td>Secret (Confirm)</td>
<td>Confirm the user password.</td>
</tr>
</tbody>
</table>

### Peer User

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer User</td>
<td>Only entered when configuring mutual CHAP. Usually the same value as User.</td>
</tr>
<tr>
<td>Peer Secret</td>
<td>Mutual secret password. Required when Peer User is set. Must be different than the Secret.</td>
</tr>
<tr>
<td>Peer Secret (Confirm)</td>
<td>Confirm the mutual secret password.</td>
</tr>
</tbody>
</table>

### Targets

The **Targets** tab lets users create new TrueNAS storage resources or edit existing ones in the list.
To add a new target, click *ADD* and enter the basic and iSCSI group information.

To edit an existing target, click *more_vert* next to it and select *Edit*.

### Basic Info

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Name</td>
<td>The base name is automatically prepended if the target name does not start with iqn. Lowercase alphanumeric characters plus dot (.), dash (-), and colon (:)) are allowed. See the Constructing iSCSI names using the iqn.format section of <a href="https://tools.ietf.org/html/rfc3721">RFC3721</a>.</td>
</tr>
<tr>
<td>Target Alias</td>
<td>Optional user-friendly name.</td>
</tr>
</tbody>
</table>

### iSCSI Group

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portal Group ID</td>
<td>Leave empty or select an existing portal to use.</td>
</tr>
<tr>
<td>Initiator Group ID</td>
<td>Select which existing initiator group has access to the target.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Choices are <em>None</em>, <em>Auto</em>, <em>CHAP</em>, or <em>Mutual CHAP</em>.</td>
</tr>
<tr>
<td>Authentication Group Number</td>
<td>Select <em>None</em> or an integer. This value represents the number of existing authorized accesses.</td>
</tr>
</tbody>
</table>

### Extents

The *Extents* tab lets users create new shared storage units or edit existing ones in the list.
To add a new extent, click **ADD** and enter the basic, type, and compatibility information.

To edit an existing extent, click **more_vert** next to it and select **Edit**.

### Basic Info

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the extent. If the <em>Extent size</em> is not 0, it cannot be an existing file within the pool or dataset.</td>
</tr>
<tr>
<td>Description</td>
<td>Notes about this extent.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Set to enable the iSCSI extent.</td>
</tr>
</tbody>
</table>

### Type

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extent Type</td>
<td><em>Device</em> provides virtual storage access to zvols, zvol snapshots, or physical devices. <em>File</em> provides virtual storage access to a single file.</td>
</tr>
<tr>
<td>Device</td>
<td>Only appears if <em>Device</em> is selected. Select the unformatted disk, controller, or zvol snapshot.</td>
</tr>
<tr>
<td>Path to the Extent</td>
<td>Only appears if <em>File</em> is selected. Browse to an existing file. Create a new file by browsing to a dataset and appending /{filename.ext} to the path. Users cannot create extents inside a jail root directory.</td>
</tr>
</tbody>
</table>
### Filesize

Only appears if File is selected. Entering 0 uses the actual file size and requires that the file already exists. Otherwise, specify the file size for the new file.

### Logical Block Size

Leave at the default of 512 unless the initiator requires a different block size.

### Disable Physical Block Size Reporting

Set if the initiator does not support physical block size values over 4K (MS SQL).

### Compatibility

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable TPC</td>
<td>Set to allow an initiator to bypass normal access control and access any scannable target. This allows <code>xcopy</code> operations that are otherwise blocked by access control.</td>
</tr>
<tr>
<td>Xen initiator compat mode</td>
<td>Set when using Xen as the iSCSI initiator.</td>
</tr>
<tr>
<td>LUN RPM</td>
<td>Do NOT change this setting when using Windows as the initiator. Only needs to be changed in large environments where the number of systems using a specific RPM is needed for accurate reporting statistics.</td>
</tr>
<tr>
<td>Read-only</td>
<td>Set to prevent the initiator from initializing this LUN.</td>
</tr>
</tbody>
</table>

### Associated Targets

The Associated Targets tab lets users create new associated TrueNAS storage resources or edit existing ones in the list.

To add a new associated target, click **ADD** and fill out the information.

To edit an existing associated target, click **more_vert** next to it and select **Edit**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>Select an existing target.</td>
</tr>
<tr>
<td>LUN ID</td>
<td>Select the value or enter a value between 0 and 1023. Some initiators expect a value below 256. Leave this field blank to automatically assign the next available ID.</td>
</tr>
</tbody>
</table>
Starting the iSCSI Service

To turn on the iSCSI service, go to Services and toggle iSCSI. Set Start Automatically to start it when TrueNAS boots up.

Clicking the edit returns to the options in Sharing > iSCSI.

Using the iSCSI Share

Connecting to and using an iSCSI share can differ between operating systems:

- **Linux**

iSCSI Utilities and Service

First, open the command line and ensure that the open-iscsi utility is installed. To install the utility on an Ubuntu/Debian distribution, enter `sudo apt update && sudo apt install open-iscsi`. After the installation completes, ensure the `iscsid` service is running: `sudo service iscsid start`. With the `iscsid` service started, run the `iscsiadm` command with the discovery arguments and get the necessary information to connect to the share.

```
truenas@LinuxMachine:~$ sudo apt update && sudo apt install open-iscsi
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:1 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:1 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:1 http://us.archive.ubuntu.com/ubuntu focal-security InRelease
Reading package lists... Done
```

Discover and Log In to the iSCSI Share

Run the command `sudo iscsiadm --mode discovery --type sendtargets --portal {IPADDRESS}`. The output provides the basename and target name that TrueNAS configured.

```
truenas@LinuxMachine:~$
```

Alternatively, enter `sudo iscsiadm -m discovery -t st -p {IPADDRESS}` to get the same output. Note the basename and target name given in the output, since they you need them to log in to the iSCSI share.

When a Portal Discovery Authentication Method is CHAP, add the three following lines to `/etc/iscsi/iscsid.conf`.

```
discovery.sendtargets.auth.authmethod = CHAP
discovery.sendtargets.auth.username = user
discovery.sendtargets.auth.password = secret
```

The user for `discovery.sendtargets.auth.username` is set in the Authorized Access used by the Portal of the iSCSI share. Likewise, the password to use for `discovery.sendtargets.auth.password` is the Authorized Access secret. Without those lines, the iscsiadm will not discover the Portal with the CHAP
Next, enter `sudo iscsiadm --mode node --targetname {BASENAME}:{TARGETNAME} --portal {IPADDRESS} --login`, where `{BASENAME}` and `{TARGETNAME}` is the information from the discovery command.

```
truenas@LinuxMachine:~$ sudo iscsiadm --mode discovery --type sendtargets --portal freenas.local freenas.local:3260 -i iqn.2005-10.org.freenas.ctl:iscsi.share
truenas@LinuxMachine:~$ sudo iscsiadm --mode node --targetname iqn.2005-10.org.freenas.ctl:iscsi.share --portal freenas.local --login
truenas@LinuxMachine:~$
```

**Partition iSCSI Disk**

When the iSCSI share login succeeds, the device shared through iSCSI shows on the Linux system as an *iSCSI Disk*. To view a list of connected disks in Linux, enter `sudo fdisk -l`.

```
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/sda: 476.96 GB, 512110190592 bytes, 1000215216 sectors
Disk model: SAMSUNG MZNLN512
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: B709E3B8-EBE0-4CEA-9CC6-08F2918A5F6B

Device  Start  End   Sectors  Size Type
/dev/sda1  2048  1050623  1048576 512M EFI System
/dev/sda2  1050624  1000214527 999163904 476.46 Linux filesystem

Disk /dev/loop8: 240.82 MB, 252493824 bytes, 493152 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop9: 29.84 MB, 31272960 bytes, 61800 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimial): 512 bytes / 512 bytes

Disk /dev/sdb: 10 GB, 10737434424 bytes, 2621444 sectors
Disk model: tS3C Disk
Units: sectors of 1 * 4096 = 4096 bytes
Sector size (logical/physical): 4096 bytes / 16384 bytes
I/O size (minimum/optimial): 16384 bytes / 1048576 bytes

truenas@LinuxMachine:~$
```

Because the connected iSCSI disk is raw, you must partition it. Identify the iSCSI device in the list and enter `sudo fdisk {/PATH/TO/ISCSIDEVICE}`.
Shell lists the iSCSI device path in the `sudo fdisk -l` output. Use the `fdisk` command defaults when partitioning the disk.

Remember to type `w` when finished partitioning the disk. The `w` command tells `fdisk` to save any changes before quitting.

After creating the partition on the iSCSI disk, a partition slice displays on the device name. For example, `/dev/sdb1`. Enter `fdisk -l` to see the new partition slice.

### Make a Filesystem on the iSCSI Disk

Finally, use `mkfs` to make a filesystem on the device's new partition slice. To create the default filesystem (`ext2`), enter `sudo mkfs {/PATH/TO/iSCSIDEVICEPARTITIONSLICE}`.

### Mount the iSCSI Device

Now the iSCSI device can mount and share data. Enter `sudo mount`. 
For example, `sudo mount /dev/sdb1 /mnt` mounts the iSCSI device `sdb1` to `/mnt`.

**Windows**

To access the data on the iSCSI share, clients will need to use iSCSI Initiator software. An iSCSI Initiator client is pre-installed in Windows 7 to 10 Pro, and Windows Server 2008, 2012, and 2019. Windows Professional Edition is usually required.

First, click the Start Menu and search for the *iSCSI Initiator* application.

Next, go to the **Configuration** tab and click **Change** to change the iSCSI initiator to the same name created earlier. Click **OK**.

Next, switch to the **Discovery Tab**, click **Discover Portal**, and type in the TrueNAS IP address.

- If TrueNAS changed the port number from the default 3260, enter the new port number.
- If you set up CHAP when creating the iSCSI share, click **Advanced...**, set Enable CHAP log on, and enter the initiator name and the same target/secret set earlier in TrueNAS.

Click **OK**.
Go to the **Targets** tab, highlight the iSCSI target, and click **Connect**.

After Windows connects to the iSCSI target, you can partition the drive.

Search for and open the _Disk Management_ app.

Your drive should currently be *unallocated*. Right-click the drive and click **New Simple Volume**...
Complete the Wizard to format the drive and assign a drive letter and name.

Finally, go to *This PC* or *My Computer* in File Explorer. The new iSCSI volume should show up under the list of drives. You should now be able to add, delete, and modify files and folders on your iSCSI drive.

Expanding LUNs
TrueNAS lets users expand Zvol and file-based LUNs to increase the available storage that the iSCSI shares.

**Zvol LUN**

To expand a Zvol LUN, go to **Storage > Pools** and click the more_vert next to the Zvol LUN, then select **Edit Zvol**.

Enter a new size in the **Size for this zvol** field, then click **SAVE**.

To prevent data loss, the web interface does not allow users to reduce the Zvol’s size. TrueNAS also does not allow users to increase the Zvol’s size past 80% of the pool size.

**File LUN**

To expand a file-based LUN, you will need to know the path to the file. You can find the path by going to **Sharing > Block Shares (iSCSI)** and clicking the **Extents** tab. Click the more_vert next to the file-based LUN and select **Edit**.

Highlight and copy the path, then click **CANCEL**.

Go to **Shell** and input `truncate -s +[size] [path to file]`, then press Enter.

The [size] is how much space you want to grow the file by, and the [path to file] is the file path you copied earlier.
An example of the command could look like this: `truncate -s +2g /mnt/Shares/Dataset1/FileLun/FileLUN`

Lastly, go back to the extent in **Sharing > Block Shares (iSCSI)** and make sure the **Filesize** is set to 0 so that the share uses the actual file size.
8.2.2 - Fibre Channel

- Fibre Channel ISCSI Share Example
- NPIV (N_Port ID Virtualization)

Fibre Channel is a high-speed data transfer protocol providing in-order, lossless delivery of raw block data. Fibre Channel is primarily used to connect computer data storage to servers in storage area networks in commercial data centers. The Fibre Channel protocol is fast, cost effective, and reliable over a wide variety of storage workloads.

Which TrueNAS Products can use Fibre Channel? expand □
- TrueNAS R-Series (4x16 Gbps)
- TrueNAS X-10 (2x8 Gbps)
- TrueNAS X-20 (2x8 Gbps)
- TrueNAS M-40 (4x16 Gbps)
- TrueNAS M-50 (4x16 Gbps or 2x32 Gbps)
- TrueNAS M-60 (4x32 Gbps)

This is a TrueNAS Enterprise feature. TrueNAS systems licensed for Fibre Channel have Fibre Channel Ports added to Sharing > Block Shares (iSCSI).

Fibre Channel ISCSI Share Example

Initiators and Authorized Access screens only apply to iSCSI and can be ignored when configuring Fibre Channel.

Go to Storage > Pools. Find an existing pool, click □ and Add zvol to create a new zvol.
Configure these tabs in **Sharing > Block Shares (iSCSI):**

- **Portals**
  If a portal with listen interface `0.0.0.0:3260` does not exist, click *Add* and add this portal.

- **Initiators Groups**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Initiators</td>
<td>Initiators currently connected to the system. Shown in IQN format with an IP address. Set initiators and click an -&gt; (arrow) to add the initiators to either the Allowed Initiators or Authorized Networks lists. Clicking Refresh updates the Connected Initiators list.</td>
</tr>
<tr>
<td>Allowed Initiators</td>
<td>Initiators allowed access to this system. Enter an <a href="https://docs.oracle.com/cd/E19794_01/doc.151/e28700/">iSCSI Qualified Name (IQN)</a> and click + to add it to the list. Example: <code>iqn.1994-09.org.freebsd:freenas.local</code>.</td>
</tr>
<tr>
<td>Authorized Networks</td>
<td>Network addresses allowed use this initiator. Each address can include an optional <a href="https://en.wikipedia.org/wiki/CIDRnotation">CIDR netmask</a>. Click + to add the network address to the list. Example: <code>192.168.2.0/24</code>.</td>
</tr>
<tr>
<td>Description</td>
<td>Any notes about initiators.</td>
</tr>
</tbody>
</table>

- **Authorized Access**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID</td>
<td>Allow different groups to be configured with different authentication profiles. Example: all users with a group ID of 1 will inherit the authentication profile associated with Group 1.</td>
</tr>
<tr>
<td>User</td>
<td>User account to create for CHAP authentication with the user on the remote system. Many initiators use the initiator name as the user name.</td>
</tr>
<tr>
<td>Secret</td>
<td>User password. Must be at least 12 and no more than 16 characters long.</td>
</tr>
<tr>
<td>Peer User</td>
<td>Only entered when configuring mutual CHAP. Usually the same value as User.</td>
</tr>
<tr>
<td>Peer Secret</td>
<td>Mutual secret password. Required when Peer User is set. Must be different than the Secret.</td>
</tr>
</tbody>
</table>

- **Targets**

*Add* a new target.
Enter or select values specific to your use case for the **Target Name**, **Target Alias**, **Target Mode**, and **Portal Group**. The **Initiator Group ID** selects which existing initiator group has access to the target. Options for the **Authentication Method** are None, Auto, CHAP, or Mutual CHAP. **Authentication Group Number** can be set to none or an integer. This value represents the number of existing authorized accesses.

An extra **Target Mode** option appears after going to **Targets** and clicking **ADD**. This new option is to select whether the target to create is iSCSI, Fibre Channel, or both.

The **Target Reporting** tab provides Fibre Channel port bandwidth graphs.

- **Extents**

  *Add* a new extent.
<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the extent. If the Extent size is not 0, it cannot be an existing file within the pool or dataset.</td>
</tr>
<tr>
<td>Description</td>
<td>Notes about this extent.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Set to enable the iSCSI extent.</td>
</tr>
<tr>
<td>Extent Type</td>
<td>Device provides virtual storage access to zvols, zvol snapshots, or physical devices. File provides virtual storage access to a single file.</td>
</tr>
<tr>
<td>Device</td>
<td>Only appears if Device is selected. Select the unformatted disk, controller, or zvol snapshot.</td>
</tr>
<tr>
<td>Logical Block Size</td>
<td>Leave at the default of 512 unless the initiator requires a different block size.</td>
</tr>
<tr>
<td>Disable Physical Block Size Reporting</td>
<td>Set if the initiator does not support physical block size values over 4K (MS SQL).</td>
</tr>
<tr>
<td>Enable TPC</td>
<td>Set to allow an initiator to bypass normal access control and access any scannable target. This allows xcopy operations which are otherwise blocked by access control.</td>
</tr>
<tr>
<td>Xen initiator compat mode</td>
<td>Set when using Xen as the iSCSI initiator.</td>
</tr>
<tr>
<td>LUN RPM</td>
<td>Do NOT change this setting when using Windows as the initiator. Only needs to be changed in large environments where the number of systems using a specific RPM is needed for accurate reporting statistics.</td>
</tr>
<tr>
<td>Read-only</td>
<td>Set to prevent the initiator from initializing this LUN.</td>
</tr>
</tbody>
</table>
Add a new Associated Target.

Select values for Target and Extent. The LUN ID is a value between 0 and 1023. Some initiators expect a value below 256. Leave this field blank to automatically assign the next available ID.

- **Fibre Channel Ports**
  Click chevron_right to expand the option, select options as presented under test data, and Save.

The iSCSI share does not work when the service is not turned on. To turn on the iSCSI service, go to Services and toggle iSCSI.

**NPIV (N_Port ID Virtualization)**

NPIV allows the administrator to use switch zoning to configure each virtual port as if it was a physical port in order to provide access control. This is important in an environment with a mix of Windows systems and virtual machines in order to prevent automatic or accidental reformatting of targets containing unrecognized filesystems. It can also be used to segregate data; for example, to prevent the engineering department from accessing data from the human resources department. Refer to the switch documentation for details on how to configure zoning of virtual ports.

To create virtual ports on the TrueNAS system, go to System > Tunables and click ADD. Enter these options:

- **Variable**: input hint.isp.X.vports, replacing X with the number of the physical interface.
- **Value**: input the number of virtual ports to create. There cannot be more than 125 SCSI target ports, including all physical Fibre Channel ports, all virtual ports, and all configured combinations of iSCSI portals and targets.
- **Type**: make sure loader is selected.
In the example shown, two physical interfaces were each assigned 4 virtual ports. Two tunables were required, one for each physical interface. After the tunables are created, the configured number of virtual ports appears in **Sharing > Block Shares (iSCSI) > Fibre Channel Ports** screen so they can be associated with targets. They are also advertised to the switch so zoning can be configured on the switch.

After a virtual port has been associated with a target, it is added to the **Target** tab of **Reporting** where its bandwidth usage can be viewed.
8.3 - Unix Shares (NFS)

8.3.1 - Share Creation

- Creating an NFS Share
  - NFS Share Settings
- Configure the NFS Service
- Connecting to the NFS Share

Creating a Network File System (NFS) share on TrueNAS gives the benefit of making lots of data easily available for anyone with share access. Depending how the share is configured, users accessing the share can be restricted to read or write privileges.

To create a new share, make sure a dataset is available with all the data for sharing.

Creating an NFS Share

Go to Sharing > Unix Shares (NFS) and click ADD.

Use the file browser to select the dataset to be shared. An optional Description can be entered to help identify the share. Clicking SUBMIT creates the share. At the time of creation, you can select ENABLE SERVICE for the service to start and to automatically start after any reboots. If you wish to create the share but not immediately enable it, select CANCEL.
NFS Share Settings
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>file browser</td>
<td>Type or browse to the full path to the pool or dataset to share. Click <strong>ADD</strong> to configure multiple paths.</td>
</tr>
<tr>
<td>Description</td>
<td>string</td>
<td>Enter any notes or reminders about the share.</td>
</tr>
<tr>
<td>All dirs</td>
<td>checkbox</td>
<td>Set to allow the client to mount any subdirectory within the <strong>Path</strong>. Leaving disabled only allows clients to mount the <strong>Path</strong> endpoint.</td>
</tr>
<tr>
<td>Quiet</td>
<td>checkbox</td>
<td>Enabling inhibits some syslog diagnostics to avoid error messages. See <strong>exports(5)</strong> for examples. Disabling allows all syslog diagnostics, which can lead to additional cosmetic error messages.</td>
</tr>
<tr>
<td>Enabled</td>
<td>checkbox</td>
<td>Enable this NFS share. Unset to disable this NFS share without deleting the configuration.</td>
</tr>
</tbody>
</table>

**Advanced Options expand □**

Opening the **ADVANCED OPTIONS** allows tuning the share access permissions and defining authorized networks.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Only</td>
<td>checkbox</td>
<td>Prohibits writing to the share when set.</td>
</tr>
<tr>
<td>Maproot User</td>
<td>string or drop down</td>
<td>Select a user to apply that user’s permissions to the root user.</td>
</tr>
<tr>
<td>Maproot Group</td>
<td>string or drop down</td>
<td>Select a group to apply that group’s permissions to the root user.</td>
</tr>
<tr>
<td>Mapall User</td>
<td>string or drop down</td>
<td>Permissions for the chosen user applied to all clients.</td>
</tr>
<tr>
<td>Mapall Group</td>
<td>string or drop down</td>
<td>Permissions for the chosen group are applied to all clients.</td>
</tr>
<tr>
<td>Authorized Networks</td>
<td>IP address</td>
<td>Enter an allowed network in network/mask CIDR notation. Click ADD to define another authorized network. Defining an authorized network restricts access to all other networks. Leave empty to allow all networks.</td>
</tr>
<tr>
<td>Authorized Hosts and IP addresses</td>
<td>string</td>
<td>Enter a hostname or IP address to allow that system access to the NFS share. Click ADD to define another allowed system. Defining authorized systems restricts access to all other systems. Leave field empty to allow all systems access to the share.</td>
</tr>
</tbody>
</table>

To edit an existing NFS share, go to Sharing > Unix Shares (NFS) and click more_vert > Edit. The options available are identical to the share creation options.

**Configure the NFS Service**

To begin sharing the data, go to Services and click the NFS toggle. If you want NFS sharing to activate immediately after TrueNAS boots, set Start Automatically.

NFS service settings can be configured by clicking (Configure).
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of servers</td>
<td>integer</td>
<td>Specify how many servers to create. Increase if NFS client responses are slow. Keep this less than or equal to the number of CPUs reported by <code>sysctl -n kern.smp.cpus</code> to limit CPU context switching.</td>
</tr>
<tr>
<td>Bind IP Addresses</td>
<td>drop down</td>
<td>Select IP addresses to listen to for NFS requests. Leave empty for NFS to listen to all available addresses.</td>
</tr>
<tr>
<td>Enable NFSv4</td>
<td>checkbox</td>
<td>Set to switch from NFSv3 to NFSv4.</td>
</tr>
<tr>
<td>NFSv3 ownership model for NFSv4</td>
<td>checkbox</td>
<td>Set when NFSv4 ACL support is needed without requiring the client and the server to sync users and groups.</td>
</tr>
<tr>
<td>Require Kerberos for NFSv4</td>
<td>checkbox</td>
<td>Set to force NFS shares to fail if the Kerberos ticket is unavailable.</td>
</tr>
<tr>
<td>Serve UDP NFS clients</td>
<td>checkbox</td>
<td>Set if NFS clients need to use the User Datagram Protocol (UDP).</td>
</tr>
<tr>
<td>Allow non-root mount</td>
<td>checkbox</td>
<td>Set only if required by the NFS client. Set to allow serving non-root mount requests.</td>
</tr>
<tr>
<td>Support &gt;16 groups</td>
<td>checkbox</td>
<td>Set when a user is a member of more than 16 groups. This assumes group membership is configured correctly on the NFS server.</td>
</tr>
<tr>
<td>Log mountd(8)</td>
<td>checkbox</td>
<td>Set to log <code>mountd</code> syslog requests.</td>
</tr>
</tbody>
</table>
requests

<table>
<thead>
<tr>
<th>Log rpc.statd(8) and rpc.lockd(8)</th>
<th>checkbox</th>
<th>Set to log rpc.statd and rpc.lockd syslog requests.</th>
</tr>
</thead>
<tbody>
<tr>
<td>mountd(8) bind port</td>
<td>integer</td>
<td>Enter a number to bind mountd only to that port.</td>
</tr>
<tr>
<td>rpc.statd(8) bind port</td>
<td>integer</td>
<td>Enter a number to bind rpc.statd only to that port.</td>
</tr>
<tr>
<td>rpc.lockd(8) bind port</td>
<td>integer</td>
<td>Enter a number to bind rpc.lockd only to that port.</td>
</tr>
</tbody>
</table>

Unless a specific setting is needed, it is recommended to use the default settings for the NFS service. When TrueNAS is already connected to Active Directory, setting NFSv4 and Require Kerberos for NFSv4 also requires a Kerberos Keytab.

**Connecting to the NFS Share**

Although you can connect to an NFS share with various operating systems, it is recommended to use a Linux/Unix operating system. First, download the nfs-common kernel module. This can be done using the package manager of the installed distribution. For example, on Ubuntu/Debian, enter `sudo apt-get install nfs-common` in the terminal.

After installing the module, connect to an NFS share by entering `sudo mount -t nfs {IPaddressOfTrueNASsystem}:{path/to/nfsShare} {localMountPoint}`. In the above example, `{IPaddressOfTrueNASsystem}` is the IP address of the remote TrueNAS system that contains the NFS share, `{path/to/nfsShare}` is the path to the NFS share on the TrueNAS system, and `{localMountPoint}` is a local directory on the host system configured for the mounted NFS share. For example, `sudo mount -t nfs 10.239.15.110:/mnt/pool1/photoDataset /mnt` will mount the NFS share photoDataset to the local directory /mnt.

By default, anyone that connects to the NFS share only has the read permission. To change the default permissions, edit the share, open the Advanced Options, and change the Access settings.

ESXi 6.7 or later is required for read/write functionality with NFSv4 shares.
8.4 - WebDAV Shares

8.4.1 - Share Creation

- Share Configuration
- Service Activation
- Connecting to the WebDAV Share

A Web-based Distributed Authoring and Versioning (WebDAV) share makes it easy to share a TrueNAS dataset and its contents over the web.

To create a new share, make sure a dataset is available with all the data for sharing.

Share Configuration

Go to **Sharing > WebDAV Shares** and click **ADD**.

Enter a share **Name** and use the file browser to select the dataset to be shared. An optional **Description** helps to identify the share. To prevent user accounts from modifying the shared data, set **Read Only**.

By default, **Change User & Group Ownership** is set. This changes existing ownership of **ALL** files in the share to the **webdav** user and group accounts. The default simplifies WebDAV share permission, but is unexpected, so the web interface shows a warning:

**WARNING**

Ownership of all files in the share will be changed to user **webdav** and group **webdav**. Existing permissions will not be changed, but the ownership change might make files inaccessible to their original owners. This operation cannot be undone! If unset, ownership of files to be accessed through WebDAV must be manually set to the **webdav** or web user/group.

[Confirm] [CANCEL] [OK]
This warning does not show when Change User & Group Ownership is unset. In that situation, shared file ownership must be manually set to the webdav or www user and group accounts.

By default, the new WebDAV share is immediately active. To create the share but not immediately activate it, unset Enable. Click SUBMIT to create the share.

**Service Activation**

Creating a share immediately opens a dialog to activate the WebDAV service:

To later enable or disable the WebDAV system service, go to Services and toggle WebDAV. To automatically start the service when TrueNAS boots, set Start Automatically. Click the edit to change the service settings.

For better data security, set the Protocol to HTTPS. This requires choosing an SSL certificate, but the freenas_default certificate is always available. All of the Protocol options require defining a Port number. Make sure the WebDAV service port is not already used on the network.

To prevent unauthorized access to the shared data, set the HTTP Authentication to either Basic or Digest and create a new Webdav Password.

Be sure to click SAVE after making any changes.

**Connecting to the WebDAV Share**

WebDAV shared data is accessible from a web browser. To see the shared data, open a new browser tab and enter {PROTOCOL}://{TRUENASIP}:{PORT}/{SHAREPATH}. Replace the elements in curly brackets {} with your chosen settings from the WebDAV share and service. Example: https://10.2.1.1:8081/newdataset

When the Authentication WebDAV service option is set to either Basic or Digest, a user name and password is required. Enter the user name webdav and the password defined in the WebDAV service.
8.5 - Windows Shares (SMB)

8.5.1 - Share Creation

- Background
- First Steps
  - Create a Dataset
  - Create Local User Accounts
  - Tune the Dataset ACL
- Creating the SMB Share
- Share Management
  - Configure Share ACL
  - Configure Filesystem ACL
    - ACL Presets
    - Adding ACL Entries (ACEs)
- Activate the SMB Service
  - Service Configuration
- Mounting SMB Share on another machine.

Background

SMB (also known as CIFS) is the native file sharing system in Windows. SMB shares can connect to any major operating system, including Windows, MacOS, and Linux. SMB can be used in TrueNAS to share files among single or multiple users or devices.

SMB shares allow a wide range of permissions and security settings, and can support advanced permissions (ACLs) on Windows and other systems, as well as Windows Alternate Streams and Extended Metadata. SMB is suitable for the management and administration of large or small pools of data.

TrueNAS uses Samba to provide SMB services. There are multiple versions of the SMB protocol. An SMB client will typically negotiate the highest supported SMB protocol during SMB session negotiation. Industry-wide, the usage of the SMB1 protocol (sometimes referred to as NT1) is in the process of being deprecated. This deprecation is for security reasons. However, most SMB clients support SMB 2 or 3 protocols, even when they are not the default protocols.

Legacy SMB clients rely on NetBIOS Name Resolution to discover SMB servers on a network. The NetBIOS Name Server (nmbd) is disabled by default in TrueNAS. It can be enabled in Network > Global Configuration if this functionality is required.

MacOS clients use mDNS to discover the presence of SMB servers on the network. The mDNS server (avahi) is enabled by default on TrueNAS.

Windows clients use WS-Discovery to discover the presence of SMB servers, but depending on the version of the Windows client, network discovery can be disabled by default.

Discoverability through broadcast protocols is a convenience feature and not required to access a SMB server.

First Steps

Create a Dataset

It is recommended to create a new dataset and set the Share Type to SMB for the new SMB share.
What does this do? expand □

The ZFS dataset is created with these settings:

- `aclmode = "restricted"
- `case sensitivity = "insensitive"

A default Access Control List is also applied to the dataset. This default ACL is restrictive and only allows access to the dataset owner and group. This ACL can be modified later according to your use case.

Create Local User Accounts

By default, all new local users are members of a built in SMB group called ` builtin users`. This group can be used to grant access to all local users on the server. Additional `groups` can be used to fine-tune permissions to large numbers of users. User accounts built-in to TrueNAS or that do not have the `smb` flag set cannot be used for SMB access.

Why not just allow anonymous access to the share? expand □

Although anonymous or guest access to the share is possible, this is a security vulnerability and is being deprecated by the major SMB client vendors. This partly because signing and encryption are not possible for guest sessions.

What about LDAP users? expand □

When LDAP has been configured and you want users from the LDAP server to have access the SMB share, go to `Directory Services > LDAP > ADVANCED MODE` and set `Samba Schema`. However, local TrueNAS user accounts will no longer have access to the share.

Tune the Dataset ACL

After a dataset and accounts are created, you will need to investigate your access requirements and adjust the dataset ACL to match. To edit the ACL, go to `Storage > Pools`, open the options for the new dataset, and click `Edit Permissions`. Many home users typically add a new entry that grants `FULL_CONTROL` to the `builtin_users` group with the flags set to `INHERIT`. See the Permissions article for more details.

Creating the SMB Share

To create a Windows SMB share, go to `Sharing > Windows Shares (SMB)` and click ADD.
The **Path** and **Name** of the SMB share define the absolute minimum amount of information required to create a new SMB share. The **Path** is the directory tree on the local filesystem that will be exported over the SMB protocol, and the **Name** is the name of the SMB share, which forms a part of the "full share pathname" when SMB clients perform an SMB tree connect. Because of the way that the **Name** is used in the SMB protocol, it must be less than or equal to 80 characters in length, and must not contain any invalid characters as specified in Microsoft documentation MS-FSCC section 2.1.6. If a **Name** is not supplied, then the last component of the **Path** will be used as the share name.

You can set a share **Purpose** to apply and lock pre-defined advanced options for the share. To retain full control over all the share **Advanced Options**, choose **No presets**.

**What do all the presets do? expand □**

The following table shows the preset options for the different **Purposes** and if those options are locked. An [x] indicates the option is enabled, [ ] means the option is disabled, and [text] indicates a specific value:

<table>
<thead>
<tr>
<th>Default share parameters</th>
<th>Multi-user time machine</th>
<th>Multi-protocol (AFP/SMB) shares</th>
<th>Multi-protocol (NFSv3/SMB) shares</th>
<th>Private SMB Datasets and Shares</th>
<th>Files become readonly of SMB after 5 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>[x] Enable ACL (locked)</td>
<td>[x] Enable ACL (unlocked)</td>
<td>[x] Enable ACL (locked)</td>
<td>[ ] Enable ACL (locked)</td>
<td>[ ] Enable ACL (unlocked)</td>
<td>[ ] Enable ACL (unlocked)</td>
</tr>
<tr>
<td>[ ] Export Read Only (locked)</td>
<td>[ ] Export Read Only (unlocked)</td>
<td>[ ] Export Read Only (unlocked)</td>
<td>[ ] Export Read Only (unlocked)</td>
<td>[ ] Export Read Only (unlocked)</td>
<td>[ ] Export Read Only (unlocked)</td>
</tr>
<tr>
<td>[x] Browsable to Network Clients (locked)</td>
<td>[x] Browsable to Network Clients (unlocked)</td>
<td>[x] Browsable to Network Clients (unlocked)</td>
<td>[x] Browsable to Network Clients (unlocked)</td>
<td>[x] Browsable to Network Clients (unlocked)</td>
<td>[x] Browsable to Network Clients (unlocked)</td>
</tr>
<tr>
<td>[ ] Allow Guest Access (unlocked)</td>
<td>[ ] Allow Guest Access (unlocked)</td>
<td>[ ] Allow Guest Access (unlocked)</td>
<td>[ ] Allow Guest Access (unlocked)</td>
<td>[ ] Allow Guest Access (unlocked)</td>
<td>[ ] Allow Guest Access (unlocked)</td>
</tr>
<tr>
<td>[ ] Access Based Share Enumeration (locked)</td>
<td>[ ] Access Based Share Enumeration (unlocked)</td>
<td>[ ] Access Based Share Enumeration (unlocked)</td>
<td>[ ] Access Based Share Enumeration (unlocked)</td>
<td>[ ] Access Based Share Enumeration (unlocked)</td>
<td>[ ] Access Based Share Enumeration (unlocked)</td>
</tr>
<tr>
<td>[ ] Hosts Allow (locked)</td>
<td>[ ] Hosts Allow (unlocked)</td>
<td>[ ] Hosts Allow (unlocked)</td>
<td>[ ] Hosts Allow (unlocked)</td>
<td>[ ] Hosts Allow (unlocked)</td>
<td>[ ] Hosts Allow (unlocked)</td>
</tr>
<tr>
<td>[ ] Hosts Deny (locked)</td>
<td>[ ] Hosts Deny (unlocked)</td>
<td>[ ] Hosts Deny (unlocked)</td>
<td>[ ] Hosts Deny (unlocked)</td>
<td>[ ] Hosts Deny (unlocked)</td>
<td>[ ] Hosts Deny (unlocked)</td>
</tr>
<tr>
<td>[ ] Use as Home Share (locked)</td>
<td>[ ] Use as Home Share (unlocked)</td>
<td>[ ] Use as Home Share (unlocked)</td>
<td>[ ] Use as Home Share (unlocked)</td>
<td>[ ] Use as Home Share (unlocked)</td>
<td>[ ] Use as Home Share (unlocked)</td>
</tr>
<tr>
<td>[ ] Time Machine (locked)</td>
<td>[ ] Time Machine (unlocked)</td>
<td>[ ] Time Machine (unlocked)</td>
<td>[ ] Time Machine (unlocked)</td>
<td>[ ] Time Machine (unlocked)</td>
<td>[ ] Time Machine (unlocked)</td>
</tr>
<tr>
<td>[x] Enable Shadow Copies (locked)</td>
<td>[x] Enable Shadow Copies (unlocked)</td>
<td>[x] Enable Shadow Copies (unlocked)</td>
<td>[x] Enable Shadow Copies (unlocked)</td>
<td>[x] Enable Shadow Copies (unlocked)</td>
<td>[x] Enable Shadow Copies (unlocked)</td>
</tr>
<tr>
<td>[ ] Export Recycle Bin</td>
<td>[ ] Export Recycle Bin</td>
<td>[ ] Export Recycle Bin</td>
<td>[ ] Export Recycle Bin</td>
<td>[ ] Export Recycle Bin</td>
<td>[ ] Export Recycle Bin</td>
</tr>
</tbody>
</table>
An optional Description can be specified to help explain the purpose of the share.

Enabled allows this path to be shared when the SMB service is activated. Unsetting Enabled disables the share without deleting the configuration.

### Advanced Options expand □

Options are divided into Access and Other Options groups. Access options control various settings for
allowing systems or users to access or modify the shared data.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable ACL</td>
<td>checkbox</td>
<td>Set to add Access Control List (ACL) support to the share. Unsetting disables ACL support and deletes any existing ACL for the share.</td>
</tr>
<tr>
<td>Export Read Only</td>
<td>checkbox</td>
<td>Prohibits writes to the share. Unset to allow writes to the share.</td>
</tr>
<tr>
<td>Browsable to Network Clients</td>
<td>checkbox</td>
<td>Determine whether this share name is included when browsing shares. Home shares are only visible to the owner regardless of this setting.</td>
</tr>
<tr>
<td>Allow Guest Access</td>
<td>checkbox</td>
<td>Privileges are the same as the guest account. Guest access is disabled by default in Windows 10 version 1709 and Windows Server version 1903. Additional client-side configuration is required to provide guest access to these clients. MacOS clients: Attempting to connect as a user that does not exist in FreeNAS does not automatically connect as the guest account. The Connect As: Guest option must be specifically chosen in MacOS to log in as the guest account. See the Apple documentation for more details.</td>
</tr>
<tr>
<td>Access Based Share Enumeration</td>
<td>checkbox</td>
<td>Setting this restricts share visibility to users with read or write access to the share. See the smb.conf manual page.</td>
</tr>
<tr>
<td>Hosts Allow</td>
<td>string</td>
<td>Enter a list of allowed hostnames or IP addresses. Separate entries by pressing Enter. A more detailed description with examples can be found here.</td>
</tr>
<tr>
<td>Hosts Deny</td>
<td>string</td>
<td>Enter a list of denied hostnames or IP addresses. Separate entries by pressing Enter.</td>
</tr>
</tbody>
</table>

The Hosts Allow and Hosts Deny fields work together to produce different situations:

- If neither Hosts Allow or Hosts Deny contains an entry, then SMB share access is allowed for any host.
- If there is a Hosts Allow list but no Hosts Deny list, then only allow hosts on the Hosts Allow list.
- If there is a Hosts Deny list but no Hosts Allow list, then allow all hosts that are not on the Hosts Deny list.
- If there is both a Hosts Allow and Hosts Deny list, then allow all hosts that are on the Hosts Allow list. If there is a host not on the Hosts Allow and not on the Hosts Deny list, then allow it.

The Other Options have settings for improving Apple software compatibility, ZFS snapshot features, and other advanced features.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use as Home Share</td>
<td>checkbox</td>
<td>Allows the share to host user home directories. Each user is given a personal home directory when connecting to the share which is not accessible by other users. This allows for a personal, dynamic share. Only one share can be used as the home share. See the configuring Home Share article for detailed instructions.</td>
</tr>
<tr>
<td>Time Machine</td>
<td>checkbox</td>
<td>Enables Apple Time Machine backups on this share.</td>
</tr>
<tr>
<td>Enable Shadow Copies</td>
<td>checkbox</td>
<td>Export ZFS snapshots as Shadow Copies for Microsoft Volume Shadow Copy Service (VSS) clients.</td>
</tr>
</tbody>
</table>
Files that are deleted from the same dataset are moved to the Recycle Bin and do not take any additional space. **Deleting files over NFS will remove the files permanently.** When the files are in a different dataset or a child dataset, they are copied to the dataset where the Recycle Bin is located. To prevent excessive space usage, files larger than 20 MiB are deleted rather than moved. Adjust the **Auxiliary Parameter** `crossrename:sizelimit=` setting to allow larger files. For example, `crossrename:sizelimit=50` allows moves of files up to 50 MiB in size. This means files can be permanently deleted or moved from the recycle bin. **This is not a replacement for ZFS snapshots.**

By default, Samba uses a hashing algorithm for NTFS illegal characters. Enabling this option converts NTFS illegal characters in the same manner as MacOS SMB clients.

Allows multiple **NTFS data streams**. Disabling this option causes MacOS to write streams to files on the filesystem.

Allow using open file handles that can withstand short disconnections. Support for POSIX byte-range locks in Samba is also disabled. This option is not recommended when configuring multi-protocol or local access to files.

Enable support for the File Server Remote VSS Protocol (**FSVRP**). This protocol allows Remote Procedure Call (RPC) clients to manage snapshots for a specific SMB share. The share path must be a dataset mountpoint. Snapshots have the prefix `fss-` followed by a snapshot creation timestamp. A snapshot must have this prefix for an RPC user to delete it.

Appends a suffix to the share connection path. This is used to provide unique shares on a per-user, per-computer, or per-IP address basis. Suffixes can contain a macro. See the `smb.conf` manual page for a list of supported macros. The connectpath must be preset before a client connects.

Additional `smb.conf` settings.

Clicking **Submit** creates the share and adds it to the **Sharing > Windows Shares (SMB)** list. You can also choose to enable the SMB service at this time.

**Share Management**

After the SMB share is created, additional management options are available by going to **Sharing > Windows Shares (SMB)** and clicking **Edit** for a share entry:

- **Edit**: Opens the share creation screen to reconfigure the share or disable it.
- **Edit Share ACL**: Opens a screen to configure an Access Control List (ACL) for the share. This is separate from filesystem permissions, and applies at the level of the entire SMB share. Permissions defined here are not interpreted by clients of other filesharing protocols or other SMB shares that export the same share **Path**. The default is open. This ACL is used to determine the browse list if **Access Based Share Enumeration** is enabled.
- **Edit Filesystem ACL**: Opens a screen to configure an Access Control List (ACL) for the path defined in the share **Path**.
- **Delete**: Remove the share configuration from TrueNAS. Data that was being shared is unaffected.

**Configure Share ACL**

To see the share ACL options, click **more_vert > Edit Share ACL**.
The Share Name is shown, but cannot be changed. ACL Entries are listed as a block of settings. Click ADD to register a new entry.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SID</td>
<td>string</td>
<td>Who this ACL entry (ACE) applies to, shown as a Windows Security Identifier. Either a SID or a Domain with Name is required for the ACL.</td>
</tr>
<tr>
<td>Domain</td>
<td>string</td>
<td>Domain for the user Name. Required when a SID is not entered. Local users have the SMB server NetBIOS name: truenas\smbusers.</td>
</tr>
</tbody>
</table>
| Permission | drop down | Predefined permission combinations:
Read: Read access and Execute permission on the object (RX).
Change: Read access, Execute permission, Write access, and Delete object (RXWD).
Full: Read access, Execute permission, Write access, Delete object, change Permissions, and take Ownership (RXWDPO).
For more details, see smbacls(1). |
| Name    | string| Who this ACL entry applies to, shown as a user name. Requires adding the user Domain. |
| Type    | drop down| How permissions are applied to the share. Allowed denies all permissions by default except those that are manually defined. Denied allows all permissions by default except those that are manually defined. |

Clicking SAVE stores the share ACL and applies it to the share immediately.

**Configure Filesystem ACL**

Click more_vert > Edit Filesystem ACL to quickly return to Storage > Pools and edit the dataset ACL.
This ACL is used to define the user accounts or groups that own or have specific permissions to the dataset that is being shared. The User and Group values show which accounts “own”, or have full permissions to the dataset. Change the default settings to your preferred primary account and group and set the Apply check boxes before saving any changes.

**ACL Presets**

To rewrite the current ACL with a standardized preset, click **SELECT AN ACL PRESET** and choose an option:
Open

Has three entries:

- owner@ has full dataset control.
- group@ has full dataset control.
- All other accounts can modify the dataset contents.

Restricted

Has two entries:

- owner@ has full dataset control.
- group@ can modify the dataset contents.

Home

Has three entries:

- owner@ has full dataset control.
- group@ can modify the dataset contents.
- All other accounts can traverse through the dataset.

Adding ACL Entries (ACEs)

To define permissions for a specific user account or group, click ADD ACL ITEM. Open the Who drop down, select User or Group, and choose a specific User or Group account. Define how the settings are applied to the account then choose which permissions to apply to that account. For example, to only allow the tmoore user permission to view dataset contents but not make changes, set the ACL Type to Allow and Permissions to Read.

Activate the SMB Service

Connecting to an SMB share does not work when the related system service is not activated. To make SMB share available on the network, Services and click the toggle for SMB. If you want the service to activate whenever TrueNAS boots, set Start Automatically.
Service Configuration

The SMB service is configured by clicking edit. Unless a specific setting is needed or configuring for a specific network environment, it is recommended to use the default settings for the SMB service.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetBIOS Name</td>
<td>string</td>
<td>Automatically populated with the original hostname of the system. This name is limited to 15 characters and cannot be the Workgroup name.</td>
</tr>
<tr>
<td>NetBIOS Alias</td>
<td>string</td>
<td>Enter any aliases, separated by spaces. Each alias can be up to 15 characters long.</td>
</tr>
<tr>
<td>Workgroup</td>
<td>string</td>
<td>Must match the Windows workgroup name. When this is unconfigured and Active Directory or LDAP are active, TrueNAS will detect and set the correct workgroup from these services.</td>
</tr>
<tr>
<td>Description</td>
<td>string</td>
<td>This allows entering any notes or descriptive details about the service configuration.</td>
</tr>
<tr>
<td>Enable SMB1 support</td>
<td>checkbox</td>
<td>Allow legacy SMB1 clients to connect to the server. Note that SMB1 is being deprecated and it is advised to upgrade clients to operating system versions that support modern versions of the SMB protocol.</td>
</tr>
<tr>
<td>NTLMv1 Auth</td>
<td>checkbox</td>
<td>When set, smbd attempts to authenticate users with the insecure and vulnerable NTLMv1 encryption. This setting allows backward compatibility with older versions of Windows, but is not recommended and should not be used on untrusted networks.</td>
</tr>
</tbody>
</table>

Advanced Options expand □
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIX Charset</td>
<td>drop down</td>
<td>Character set used internally. UTF-8 is standard for most systems as it supports all characters in all languages.</td>
</tr>
<tr>
<td>Log Level</td>
<td>drop down</td>
<td>Record SMB service messages up to the specified log level. By default, error and warning level messages are logged. It is not recommended to use a log level above MINIMUM for production servers.</td>
</tr>
<tr>
<td>Use Syslog Only</td>
<td>checkbox</td>
<td>Set to log authentication failures in /var/log/messages instead of the default /var/log/samba4/log.smbd.</td>
</tr>
<tr>
<td>Local Master</td>
<td>checkbox</td>
<td>Set to determine if the system participates in a browser election. Unset when the network contains an AD or LDAP server, or when Vista or Windows 7 machines are present.</td>
</tr>
<tr>
<td>Enable Apple SMB2/3 Protocol Extensions</td>
<td>checkbox</td>
<td>These protocol extensions can be used by macOS to improve the performance and behavioral characteristics of SMB shares. This is required for Time Machine support.</td>
</tr>
<tr>
<td>Administrators Group</td>
<td>drop down</td>
<td>Members of this group are local administrators and automatically have privileges to take ownership of any file in an SMB share, reset permissions, and administer the SMB server through the Computer Management MMC snap-in.</td>
</tr>
<tr>
<td>Guest Account</td>
<td>drop down</td>
<td>Account to be used for guest access. Default is nobody. The chosen account is required to have permissions to the shared pool or dataset. To adjust permissions, edit the dataset Access Control List (ACL), add a new entry for the chosen guest account, and configure the permissions in that entry. If the selected Guest Account is deleted the field resets to nobody.</td>
</tr>
<tr>
<td>File Mask</td>
<td>integer</td>
<td>Overrides default file creation mask of 0666 which creates files with read and write access for everybody.</td>
</tr>
<tr>
<td>Directory Mask</td>
<td>integer</td>
<td>Overrides default directory creation mask of 0777 which grants directory read, write and execute access for everybody.</td>
</tr>
<tr>
<td>Bind IP Addresses</td>
<td>drop down</td>
<td>Static IP addresses which SMB listens on for connections. Leaving all unselected defaults to listening on all active interfaces.</td>
</tr>
<tr>
<td>Auxiliary Parameters</td>
<td>string</td>
<td>Stores additional smb.conf. Auxiliary parameters may be used to override the default SMB server configuration, but such changes may adversely affect SMB server stability or behavior.</td>
</tr>
</tbody>
</table>

**Mounting SMB Share on another machine.**

Linux
Verify that the required CIFS packages are installed for your distribution of Linux. Create a mount point:

```
sudo mkdir /mnt/smb_share.
```

**Mount the volume.**

```
sudo mount -t cifs //computer_name/share_name /mnt/smb_share.
```

If your share requires user credentials, add the switch `-o username= with your username after cifs and before the share address.

- **Windows**

To mount the SMB share to a drive letter on windows, open the command line and run the following command with the appropriate drive letter, computer name, and share name.

```
net use Z: \\computer_name\share_name /PERSISTENT:YES
```

- **Apple**

Open Finder > Go > Connect To Server Enter the SMB address: smb://192.168.1.111.

Input the username and password for the user assigned to that pool or Guest if Guest access is enabled on the share.

- **FreeBSD**

Create a mount point:

```
sudo mkdir /mnt/smb_share.
```

**Mount the volume.**

```
sudo mount_smbfs -I computer_name\share_name /mnt/smb_share.
```
TrueNAS offers the *Use as Home Share* option for organizations or SMEs that want to use a single SMB share to provide a personal directory to every user account.

The *Use as Home Share* feature is available for a single TrueNAS SMB share. You can create additional SMB shares as described in the [SMB sharing article](#) but without the *Use as Home Share* option enabled.

**Create a Pool and Join Active Directory**

First, go to **Storage > Pools** and [create a pool](#). Next, [set up the Active Directory](#) that you will want to share resources with over your network.

**Prepare a Dataset**

Go to **Storage > Pools** and open the **more_vert** next to the root dataset in the pool you just created, then click **Add Dataset**.

Name the dataset (this article uses *Home_Share_Dataset* as an example) and set the *Share Type* to *SMB*.
After creating the dataset, go to **Storage > Pools** and open more_vert next to the new dataset. Select **Edit Permissions**.

Click the **Group** drop-down menu and change the owning group to your Active Directory’s domain admins.

Click **Select an ACL Preset** and choose **HOME**. Then, click **SAVE**.
Create the Share

Go to Sharing > Windows Shares (SMB) and click ADD.

Set the Path to the prepared dataset (Home_Share_Dataset for example).

The Name automatically changes to be identical to the dataset. Leave this at the default.

Set the Purpose to No presets, then click ADVANCED OPTIONS and check Use as Home Share. Click SUBMIT.
Click SAVE and enable the SMB service in Services to make the share is available on your network.

Add Users

Go to Accounts > Users and click ADD. Create a new user name and password. By default, the user Home Directory will be titled from the user account name and added as a new subdirectory of Home_Share_Dataset.
If existing users require access to the home share, go to **Accounts > Users** and edit an existing account.

Adjust the user’s home directory to the appropriate dataset and give it a name to create their own directory.

After the user accounts have been added and permissions configured, users can log in to the share and see a folder matching their user name.
Shadow Copies, also known as the Volume Shadow Copy Service (VSS) or Previous Versions, is a Microsoft service for creating volume snapshots. Shadow copies can be used to restore previous versions of files from within Windows Explorer.

By default, all ZFS snapshots for a dataset underlying an SMB share path are presented to SMB clients through the volume shadow copy service or are accessible directly with SMB when the hidden ZFS snapshot directory is located within the path of the SMB share.

There are a few caveats about shadow copies to be aware of before activating the feature in TrueNAS:

- When the Windows system is not fully patched to the latest service pack, Shadow Copies might not work. If no previous versions of files to restore are visible, use Windows Update to ensure the system is fully up-to-date.
- Shadow copy support only works for ZFS pools or datasets.
- Appropriate permissions must be configured on the pool or dataset being shared by SMB.
- Users cannot use an SMB client to delete shadow copies. Instead, the administrator use the TrueNAS web interface to remove snapshots. Shadow copies can be disabled for an SMB share by unsetting enable shadow copies for the SMB share. This does not prevent access to the hidden .zfs/snapshot directory for a ZFS dataset when the directory is located within the Path for an SMB share.

To enable Shadow Copies, go to Sharing > Windows Shares (SMB) and Edit an existing share. Open the Advanced options, find the Other Options and set Enable Shadow Copies.

Windows 10 v2004 Issue

Some users have experienced issues in the Windows 10 v2004 release where network shares can’t be accessed. The problem appears to come from a bug in gedit.msc, the Local Group Policy Editor. Unfortunately, setting the Allow insecure guest logon flag value to Enabled in Computer Configuration > Administrative Templates > Network > Lanman Workstation appears to have no effect on the configuration.
To work around this issue, edit the Windows registry. Use *Regedit* and go to **HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters**. The **DWORD AllowInsecureGuestAuth** is an incorrect value: **0x00000000**. Change this value to **0x00000001** (Hexadecimal 1) to allow adjusting the settings in *gpedit.msc*. This can be applied to a fleet of Windows machines with a Group Policy Update.
9 - Services

Services related to data sharing or automated tasks are documented in their respective Sharing or Tasks.

9.1 - Dynamic DNS

Dynamic Domain Name Service (DDNS) is useful when TrueNAS is connected to an ISP that periodically changes the IP address of the system. With dynamic DNS, the system can automatically associate its current IP address with a domain name and continue to provide access to TrueNAS even if the system IP address changes.

Configuring Dynamic DNS

DDNS requires registration with a DDNS service such as DynDNS before configuring TrueNAS. Have the DDNS service settings available or open in another browser tab when configuring TrueNAS. Log in to the TrueNAS web interface and go to Services > Dynamic DNS.

<p>| Provider | Several providers are supported. If a specific provider is not listed, select Custom Provider and enter the information in the Custom Server and Custom Path fields. |
| CheckIP-Server SSL | Use HTTPS for the connection to the CheckIP Server. |
| CheckIP Server | Name and port of the server that reports the external IP address. For example, entering checkip.dyndns.org:80 uses Dyn IP detection, to discover the remote socket IP address. |
| CheckIP Path | Path to the CheckIP Server. For example, no-ip.com uses a CheckIP Server of dynamic.zoneedit.com and CheckIP Path of /checkip.html. |
| SSL | Use HTTPS for the connection to the server that updates the DNS record. |
| Domain Name | Fully qualified domain name of the host with the dynamic IP address. Separate multiple domains with a space, comma (,), or semicolon (;). Example: myname.dyndns.org; myothername.dyndns.org. |</p>
<table>
<thead>
<tr>
<th>Update Period</th>
<th>How often the IP is checked in seconds.</th>
</tr>
</thead>
</table>

**Credentials**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Username for logging in to the provider and updating the record.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for logging in to the provider and updating the record.</td>
</tr>
</tbody>
</table>

The required values for these fields are provided by your DDNS solution. Start the DDNS service after choosing your *Provider* options and saving the settings.
9.2 - FTP, SFTP, and TFTP

The File Transfer Protocol (FTP) is a simple option for data transfers. The additional SSH and Trivial FTP options provide secure or simple config file transfer methods, respectively.

Options for configuring FTP, SSH, and TFTP are in the system Services. Click the edit to configure the related service.

- FTP

FTP requires a new dataset and local user account.

Go to Storage > Pools to add a new dataset.

Next, go to Accounts > Users > Add to create a local user on the TrueNAS.

Assign a user name, password, and link the newly created dataset for the FTP share as the home directory of the user. This can be done on a per user basis, or a global account for FTP can also be created, for example OurOrgFTPacnt, etc.

Return to Storage > Pools, find the new dataset, and click more_vert > Edit Permissions. Set the Owner fields (user and group) to the newly created user account. Be sure to click Apply User and Apply Group before saving.

Service Configuration

To configure FTP, go to the Services page, find the FTP entry, and click the edit.
Configure the options according to your environment and security considerations.

**General Options**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Set the port the FTP service listens on.</td>
</tr>
<tr>
<td>Clients</td>
<td>The maximum number of simultaneous clients.</td>
</tr>
<tr>
<td>Connections</td>
<td>Set the maximum number of connections per IP address. 0 is unlimited.</td>
</tr>
<tr>
<td>Login Attempts</td>
<td>Enter the maximum attempts before client is disconnected. Increase if users are prone to typos.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Maximum client idle time in seconds before disconnect.</td>
</tr>
<tr>
<td>Certificate</td>
<td>The SSL certificate to be used for TLS FTP connections. To create a certificate, go to Certificates.</td>
</tr>
</tbody>
</table>

**Advanced**

**Access**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always Chroot</td>
<td>Set to only let users access their home directory if they are in the wheel group. This option increases security risk.</td>
</tr>
<tr>
<td>Allow Root Login</td>
<td>Allow anonymous FTP logins with access to the directory specified in Path.</td>
</tr>
<tr>
<td>Allow Anonymous Login</td>
<td>Allow any local user to log in. By default, only members of the ftp group are allowed to log in.</td>
</tr>
<tr>
<td>Allow Local User Login</td>
<td>Setting this option results in timeouts when identd is not running on the client.</td>
</tr>
<tr>
<td>Require IDENT Authentication</td>
<td>Sets default permissions for newly created files.</td>
</tr>
<tr>
<td>File Permissions</td>
<td>Sets default permissions for newly created directories.</td>
</tr>
</tbody>
</table>

**TLS**
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable TLS</td>
<td>Allow encrypted connections. Requires a certificate (created or imported in Certificates.)</td>
</tr>
<tr>
<td>TLS Policy</td>
<td>Define whether the control channel, data channel, both channels, or neither channel of an FTP session must occur over SSL/TLS. The policies are described here.</td>
</tr>
<tr>
<td>TLS Allow Client Renegotiations</td>
<td>We don’t recommend this, since it breaks security measures. See mod_tls for details.</td>
</tr>
<tr>
<td>TLS Allow Dot Login</td>
<td>If set, TrueNAS checks the user home directory for a .tlslogin file containing one or more PEM-encoded certificates. If not found, the user is prompted for password authentication.</td>
</tr>
<tr>
<td>TLS Allow Per User</td>
<td>If set, allows user password to be sent unencrypted.</td>
</tr>
<tr>
<td>TLS Common Name Required</td>
<td>When set, the common name in the certificate must match the FQDN of the host.</td>
</tr>
<tr>
<td>TLS Enable Diagnostics</td>
<td>If set when troubleshooting a connection, logs more verbosely.</td>
</tr>
<tr>
<td>TLS Export Certificate Data</td>
<td>Set to export the certificate environment variables.</td>
</tr>
<tr>
<td>TLS No Certificate Request</td>
<td>Set if the client cannot connect from poorly handling the server certificate request.</td>
</tr>
<tr>
<td>TLS No Empty Fragments</td>
<td>We don’t recommend this option, since it bypasses a security mechanism.</td>
</tr>
<tr>
<td>TLS No Session Reuse Required</td>
<td>This option reduces connection security. Only use it if the client does not understand reused SSL sessions.</td>
</tr>
<tr>
<td>TLS Export Standard Vars</td>
<td>If selected, sets several environment variables.</td>
</tr>
<tr>
<td>TLS DNS Name Required</td>
<td>If set, the client DNS name must resolve to its IP address and the cert must contain the same DNS name.</td>
</tr>
<tr>
<td>TLS IP Address Required</td>
<td>If set, the client certificate IP address must match the client IP address.</td>
</tr>
</tbody>
</table>

**Bandwidth**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local User Upload Bandwidth: (Examples: 500 KiB, 500M, 2 TB) *</td>
<td>This field accepts human-readable input in KiBs or greater (M, GiB, TB, etc.). Default 0 KiB is unlimited.</td>
</tr>
<tr>
<td>Local User Download Bandwidth</td>
<td>This field accepts human-readable input in KiBs or greater (M, GiB, TB, etc.). Default 0 KiB is unlimited.</td>
</tr>
<tr>
<td>Anonymous User Upload Bandwidth</td>
<td>This field accepts human-readable input in KiBs or greater (M, GiB, TB, etc.). Default 0 KiB is unlimited.</td>
</tr>
<tr>
<td>Anonymous User Download Bandwidth</td>
<td>This field accepts human-readable input in KiBs or greater (M, GiB, TB, etc.). Default 0 KiB is unlimited.</td>
</tr>
</tbody>
</table>
### Other Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Passive Port</td>
<td>Used by clients in PASV mode. A default of 0 means any port above 1023.</td>
</tr>
<tr>
<td>Maximum Passive Port</td>
<td>Used by clients in PASV mode. A default of 0 means any port above 1023.</td>
</tr>
<tr>
<td>Enable FXP</td>
<td>Enable File eXchange Protocol. We don’t recommend this, since it leaves the server vulnerable to FTP bounce attacks.</td>
</tr>
<tr>
<td>Allow Transfer Resumption</td>
<td>Set to allow FTP clients to resume interrupted transfers.</td>
</tr>
<tr>
<td>Perform Reverse DNS Lookups</td>
<td>Performs reverse DNS lookups on client IPs. Causes long delays if reverse DNS isn’t configured.</td>
</tr>
<tr>
<td>Masquerade Address</td>
<td>Public IP address or hostname. Set if FTP clients cannot connect through a NAT device.</td>
</tr>
<tr>
<td>Display Login</td>
<td>The message shown to local login users after authentication. Not shown to anonymous login users.</td>
</tr>
<tr>
<td>Auxiliary Parameters</td>
<td>Used to add additional <code>proftpd(8)</code> parameters.</td>
</tr>
</tbody>
</table>

Ensure `chroot` is enabled as this helps confine FTP sessions to a local user’s home directory and allow **Local User Login**.

Unless necessary, do **NOT** allow anonymous or root access. For better security, enable TLS when possible. This is effectively **FTPS**. When FTP is exposed to a WAN, enable TLS.

### FTP Connection

Use a browser or FTP client to connect to the TrueNAS FTP share. The images here show using **FileZilla**, a free option.

The user name and password are those of the local user account on the TrueNAS. The default directory is the same as the user’s `/home` directory. After connecting, directories can be created and files uploaded and downloaded.

#### SFTP

SFTP or SSH File Transfer Protocol, is available by enabling SSH remote access to the TrueNAS system. SFTP is more secure than standard FTP as it applies SSL encryption on all transfers by default.

Go to **Services**, find the **SSH** entry, and click the **edit**.
Set Allow Password Authentication and decide if Log in as Root with Password is needed. SSH with root is a security vulnerability as it allows full remote control over the NAS with a terminal, not just SFTP transfer access. Review the remaining options and configure according to your environment or security needs.

<table>
<thead>
<tr>
<th>SSH Service Options expand □</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Options</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Port</td>
<td>Open a port for SSH connection requests.</td>
</tr>
<tr>
<td>Log in as Root with Password</td>
<td>Root logins are discouraged. Allows root logins. A password must be set for the root user account.</td>
</tr>
<tr>
<td>Allow Password Authentication</td>
<td>Enabling allows SSH login authentication using a password. Warning: when directory services are enabled, this setting grants access to all users the directory service imported. When disabled, authentication requires keys for all users (requires additional SSH client and server setup).</td>
</tr>
<tr>
<td>Allow Kerberos Authentication</td>
<td>Before enabling, ensure valid entries exist in Directory Services (Kerberos Realms and Keytabs) and the system can communicate with the Kerberos Domain Controller.</td>
</tr>
<tr>
<td>Allow TCP Port Forwarding</td>
<td>Set to let users bypass firewall restrictions using the SSH port forwarding feature.</td>
</tr>
</tbody>
</table>

| **Advanced Options**                      |

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind Interfaces</td>
<td>Select interfaces for SSH to listen on. Leave all options unselected for SSH to listen on all interfaces.</td>
</tr>
<tr>
<td>Compress Connections</td>
<td>Select the syslog(3) level of the SFTP server.</td>
</tr>
<tr>
<td>SFTP Log Level</td>
<td>Select the syslog(3) facility of the SFTP server.</td>
</tr>
<tr>
<td>SFTP Log Facility</td>
<td>Allow more ciphers for sshd(8) in addition to the defaults in sshd_config(5). None allows unencrypted SSH connections and AES128-CBC allows the 128-bit Advanced Encryption Standard.</td>
</tr>
<tr>
<td>Weak</td>
<td>WARNING: these ciphers are security vulnerabilities. Only allow them in a secure environment.</td>
</tr>
</tbody>
</table>
Ciphers network environment.

**Auxiliary Parameters**
Add any more sshd_config(5) options not covered in this screen. Enter one option per line. These options are case-sensitive. Typos can prevent the SSH service from starting.

---

**SFTP Connections**

Similar to the FTP setup, open FileZilla or another FTP client, or command line. This article shows using FileZilla as an example. Using FileZilla, enter SFTP://'TrueNAS IP', 'username', 'password', and port 22 to connect.

**SFTP does not have chroot locking. While chroot is not 100% secure, the lack of chroot allows users to easily move up to the root directory and view internal system information. If this level of access is a concern, FTP with TLS may be the more secure choice.**

**SFTP in a TrueNAS Jail**

Another way to allow SFTP access without granting read access to other areas of the NAS itself is to set up a jail and enable SSH.

Go to Jails > Add. Provide a name for the jail and pick a target FreeBSD image. 11.3 was used for the purpose of this guide.

Set the networking options to either DHCP or a static IP and confirm to create.

![Jail Networking Configuration](image)

After the is created, open the jail menu by clicking the expand icon > on the right-hand side of the jail. Click START and open the SHELL.

Similar to the initial FTP setup, create a user in the jail. Enter adduser and follow the prompts including the password and home directory location. When complete, the jail asks to confirm the credentials.
Enable SSH by editing the `/etc/rc.conf` file. Type `vi /etc/rc.conf` or `ee /etc/rc.conf` depending on preference, add `sshd_enable = "YES"` to the file, save, and exit. Type `service sshd enabled` to enable the service (enabled vs start indicates whether sshd starts one time or on every reboot).

Using an FTP client, such as FileZilla, log in with the jail IP address and user credentials. Like with SSH on TrueNAS, browsing to other folders and locations beyond the user’s home directory is possible, but unlike running on TrueNAS directly, only the components of the jail are available.
**TFTP**

The Trivial File Transfer Protocol (TFTP) is a light-weight version of FTP typically used to transfer configuration or boot files between machines, such as routers, in a local environment. TFTP provides an extremely limited set of commands and provides no authentication.

When the TrueNAS system is only storing images and configuration files for network devices, configure and start the TFTP service. Starting the TFTP service opens UDP port 69.
### Path

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>Browse to an existing directory to use for storage. Some devices can require a specific directory name. Consult the documentation for that device to see if there are any restrictions.</td>
</tr>
</tbody>
</table>

### Connection

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>The default host to use for TFTP transfers. Enter an IP address. Example: 192.0.2.1</td>
</tr>
<tr>
<td>Port</td>
<td>The UDP port number that listens for TFTP requests. Example: 8050</td>
</tr>
<tr>
<td>Username</td>
<td>Select the account to use for TFTP requests. This account must have permission to the Directory.</td>
</tr>
</tbody>
</table>

### Access

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Permissions</td>
<td>Adjust the file permissions using the checkboxes.</td>
</tr>
<tr>
<td>Allow New Files</td>
<td>Set when network devices need to send files to the system.</td>
</tr>
</tbody>
</table>

### Other Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auxiliary Parameters</td>
<td>Add more options from tftpd. Add one option on each line.</td>
</tr>
</tbody>
</table>
Network devices use the Link Layer Discovery Protocol (LLDP) to advertise their identity, capabilities, and neighbors on an Ethernet network. TrueNAS uses the `ladvd` LLDP implementation. When the local network contains managed switches, configuring and starting the LLDP service tells the TrueNAS system to advertise itself on the network.

To configure LLDP, go to the Services page, find the LLDP entry, and click the switch.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Description</td>
<td>Enables receive mode. Any received peer information is saved in interface descriptions.</td>
</tr>
<tr>
<td>County Code</td>
<td>Two-letter ISO 3166-1 alpha-2 code used to enable LLDP location support.</td>
</tr>
<tr>
<td>Location</td>
<td>The physical location of the host.</td>
</tr>
</tbody>
</table>

Set *Interface Description* and enter a *Country Code* before turning the LLDP service on.
A virtual private network (VPN) is an extension of a private network over public resources. It allows clients to securely connect to a private network even when they are remotely using a public network. TrueNAS provides OpenVPN as a system level service to provide VPN Server or Client functionality. This means TrueNAS can act as a primary VPN server to allow remote clients access to data stored on the system using a single TCP or UDP port. Alternately, TrueNAS can integrate into a private network, even when the system is in a separate physical location or only has access to publicly visible networks.

Before configuring TrueNAS as either an OpenVPN Server or Client, you will need an existing public key infrastructure (PKI) with Certificates and Certificate Authorities created in or imported to TrueNAS.

What does this do? expand □
This allows TrueNAS to authenticate with clients or servers by confirming network credentials were signed by a valid master Certificate Authority (CA). To read more about the required PKI for OpenVPN, see the OpenVPN PKI Overview.

The general process to configure OpenVPN (server or client) on TrueNAS is to select the networking credentials, set the connection details, and choose any additional security or protocol options.

OpenVPN Client

Go to the Services page and find the OpenVPN Client entry. Click the edit to configure the service.

Choose the certificate to use as an OpenVPN client. This certificate must exist in TrueNAS and be in an
active (unrevoked) state. Enter the host name or IP address of the Remote OpenVPN server.

Continue to review and choose any other Connection Settings that fit with your network environment and performance requirements. The Device Type must match with the OpenVPN server Device Type. Nobind prevents using a fixed port for the client. By default, this is enabled to allow the OpenVPN client and server to run concurrently.

Finally, review the Security Options and choose settings that meet your network security requirements. When the OpenVPN server is using TLS Encryption, copy the static TLS encryption key and paste into the TLS Crypt Auth field.

OpenVPN Server

Go to the Services page and find the OpenVPN Server entry. Click the edit to configure the service.

Choose a Server Certificate for this OpenVPN server. The certificate must both exist on the TrueNAS system and be in an active (unrevoked) state.

Now define a IP address and netmask for the OpenVPN Server. Continue to choose the remaining Connection Settings that fit with your network environment and performance requirements. When a TUN Device Type is selected, you can choose a virtual addressing Topology for the server:

- **NET30**: Use one /30 subnet per client in a point-to-point topology. Designed for use when connecting clients are Windows systems.
- **P2P**: Point-to-point topology that points the local server and remote client endpoints to each other. Each client is given one IP address. This is only recommended when none of the clients are a Windows system.
- **SUBNET**: The interface uses an IP address and subnet. Each client is given one IP address. Windows clients require the TAP-Win32 driver version 8.2 or newer. TAP devices always use the SUBNET Topology.

The Topology selection is automatically applied to any connected clients.

When TLS Crypt Auth Enabled is set, TrueNAS generates a static key for the TLS Crypt Auth field after saving the options. To change this key, click RENEW STATIC KEY. This key is required for any clients connecting to the server. Keys are stored in the system database and are automatically included in a
generated client config file, but a good practice is to back up keys in a secure location.

Finally, review the Security Options and choose settings that meet your network security requirements.

After configuring and saving your OpenVPN Server, generate client configuration files for importing to any OpenVPN client systems that are connecting to this server. You need the certificate from the client system already imported on the system. To generate the configuration file, click DOWNLOAD CLIENT CONFIG and select the Client Certificate.

Common Options (Client or Server)

Many of the fields for configuring an OpenVPN Server or Client are identical. These fields are discussed in this section, with specific configuration options listed in the Server and Client sections.

The Additional Parameters field manually sets any of the core OpenVPN config file options. See the OpenVPN Reference Manual for descriptions of each option.

Connection Settings

- **Root CA**: The Certificate Authority (CA) must be the root CA that was used to sign the Client and Server certificates.
- **Port**: This is the port that will be used for the OpenVPN connection.
- **Compression**: Choose a compression algorithm for traffic. Leave the field empty for data to be sent uncompressed. LZO is a standard compression algorithm that is backwards compatible with previous (pre-2.4) versions of OpenVPN. LZ4 is a newer option that is typically faster with less system resources required.
- **Protocol**: Choose between UDP or TCP protocols for OpenVPN. UDP sends packets in a continuous stream while TCP sends packets sequentially. UDP is generally faster and less strict about dropped packets than TCP. To force the connection to be IPv4 or IPv6, choose one of the 4 or 6 UDP or TCP options.
- **Device Type**: use a TUN or TAP virtual networking device and layer with OpenVPN. This must be identical between the OpenVPN Server and any clients.

Security Options

Because using a VPN involves connecting to a private network while still sending data over less secure public resources, OpenVPN includes several security options. While not required, these security options help protect the data being sent into or out of the private network.

- **Authentication Algorithm**: This is used to validate packets that are sent over the network connection. Your network environment might require a specific algorithm. If no specific algorithm is required, SHA1 HMAC is a good standard algorithm to use.
- **Cipher**: This is an algorithm to encrypt data packets sent through the connection. While not required, choosing a Cipher can increase connection security. You might need to verify which ciphers are required for your networking environment. If there are no specific cipher requirements, AES-256-GCM is a good default choice.
- **TLS Encryption**: When TLS Crypt Auth Enabled is set, all TLS handshake messages are encrypted to add another layer of security. This requires a static key that is shared between OpenVPN server and clients.

Service Activation

When finished configuring the Server or Client service, click SAVE. Start the service by clicking the related toggle in Services. To check the current state of the service, hover over the toggle.

Setting Start Automatically means the service starts whenever TrueNAS completes booting and the network and data pools are running.
S3 allows you to connect to TrueNAS from a networked client system with the Minio Browser, s3cmd, or S3 Browser.

**Background**

S3 is an object storage protocol that many major cloud providers like Amazon Web Services™ use. On TrueNAS, the service is another way to store files and can be viewed with a web browser. Because S3 is the de facto standard for cloud-based storage, setting up an S3 service allows organizations or online application developers to use TrueNAS to replace or archive expensive cloud storage.

### Setting up the S3 service

Go to the Services page and find the S3 entry.

Click the toggle to start or stop the service. Setting *Start Automatically* starts the service when TrueNAS boots.

Click the edit to configure the service.
### Field Descriptions

**Expand**

#### S3 Configuration Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address that runs the S3 service. 0.0.0.0 tells the server to listen on all IPv4 addresses. :: allows the same for any IPv6 address. Select the TrueNAS IP address to constrain it to a specific network.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter a static port for the MinIO web console. Default is 9001.</td>
</tr>
<tr>
<td>Console Port</td>
<td>Enter the TCP port that provides the S3 service.</td>
</tr>
<tr>
<td>Access Key</td>
<td>Enter the S3 access ID. See Access keys for more information.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>Enter the S3 secret access key. See Access keys for more information.</td>
</tr>
<tr>
<td>Disk</td>
<td>Browse to a directory to define the S3 filesystem path.</td>
</tr>
<tr>
<td>Enable Browser</td>
<td>Enables the S3 service web UI. Access the MinIO web UI by entering the IP address and port number separated by a colon in the browser address bar. Example: 192.168.1.0:9000.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Use an SSL certificate created or imported in Credentials &gt; Certificates for secure S3 connections.</td>
</tr>
<tr>
<td>TLS Server URI</td>
<td>If using an SSL certificate, enter the MinIO server’s proxy-able address.</td>
</tr>
</tbody>
</table>

The IP address 0.0.0.0 allows the service to listen on any IPv4 address. :: allows the same for any IPv6 address. Select the TrueNAS IP address to constrain it to a specific network.

Select a clean dataset. MinIO manages files as objects and CANNOT mix them with other dataset files. You can create new datasets by going to **Storage > Pools** and clicking **Add Dataset**.

Configure the rest of the options as needed in your environment. Make sure to start the service after saving any changes.

### Minio Connections
When *Enable Browser* is set, test access to the Minio Browser by opening a web browser and typing the TrueNAS IP address with the TCP port. The network firewall must let the *Port* through to create buckets and upload files. For example: [https://192.168.0.3:9000](https://192.168.0.3:9000).

MinIO supports several connection and use methods:

- **s3cmd**

  Linux or macOS users must have the `s3cmd` service installed before beginning this setup. On Windows, users can also refer to [S3Express](https://s3express.com) for a similar command-line experience.

  Ubuntu or other Linux distributions can access the configuration by running `s3cmd --configure` to walk through critical settings.

  Enter the specified access key and the secret key. Under the *S3 Endpoint*, enter the TrueNAS IP address followed by TCP port, and reply *N* to the DNS-style bucket+hostname.

  Save the file. On Linux, the default is in the home directory `~/.s3cfg`.

  If the connection has any issues, open `.s3cfg` again to troubleshoot. In Ubuntu, use `nano .s3cfg` or `vi .s3cfg` or `gedit .s3cfg` depending on the preferred text editor. For other operating systems, `.s3cfg` file location and editing tools may vary.

  Scroll down to the `host_bucket` area and ensure the configuration has removed the `%{bucket}` portion and the address points to the `IP_address:TCP_port` for the system.

  **Correct Example**

  ```
  host_base = `192.168.123.207:9000`
  host_bucket = `192.168.123.207:9000`
  ```

  **Incorrect Example**

  ```
  host_base = `192.168.123.207`
  host_bucket = `%{bucket}.192.168.123.207`
  ```

  Poll the buckets using `s3cmd ls` to see the buckets created with the Minio Browser.

  For more information on using Minio with `s3cmd`, see [https://docs.minio.io/docs/s3cmd-with-minio.html](https://docs.minio.io/docs/s3cmd-with-minio.html) and [https://s3tools.org/s3cmd](https://s3tools.org/s3cmd).

- **S3 Browser (Windows)**

  The Windows PC S3 Browser is another convenient way to connect to the Minio S3 from TrueNAS.

  To set it up, first [install the S3 Browser](https://s3browser.com).

  After installation completes, add a new account.
In the settings, select **S3 Compatible Storage** as the **Account Type**, then enter the Minio access point similar to the `s3cmd` setup (TrueNAS_IP_address:9000 or other port if set differently). Select the SSL settings appropriate for the particular setup. The S3 Browser assumes SSL by default, but it may be unset for a LAN attached session.

It is possible to access, create new buckets, or upload files to created buckets.
SNMP (Simple Network Management Protocol) monitors network-attached devices for conditions that warrant administrative attention. TrueNAS uses Net-SNMP to provide SNMP. To configure SNMP, go to the Services page, find the SNMP entry, and click the .

### Field Descriptions

**General Options**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Enter the location of the system.</td>
</tr>
<tr>
<td>Contact</td>
<td>E-mail address that receives SNMP service messages.</td>
</tr>
<tr>
<td>Community</td>
<td>Change from public to increase system security. Can only contain alphanumeric characters, underscores (_), dashes (-), periods (.), and spaces. This can be left empty for SNMPv3 networks.</td>
</tr>
</tbody>
</table>

**SNMP v3 Options**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP v3 Support</td>
<td>Set to to enable support for SNMP version 3. See snmpd.conf(5) for configuration details.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter a username to register with this service.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Choose an authentication method: --- for none, SHA, or MD5</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password of at least eight characters.</td>
</tr>
</tbody>
</table>
Privacy Protocol

Choose a privacy protocol: --- for none, AES, or DES

Privacy Passphrase

Enter a separate privacy passphrase. Password is used when this is left empty.

Other Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auxiliary Parameters</td>
<td>Enter any additional <code>snmpd.conf</code> options. Add one option for each line.</td>
</tr>
<tr>
<td>Expose zilstat via SNMP</td>
<td>Enabling this option may have performance implications on your pools.</td>
</tr>
<tr>
<td>Log Level</td>
<td>Choose how many log entries to create. Choices range from least (Emergency) to most (Debug).</td>
</tr>
</tbody>
</table>

When starting the SNMP service, port UDP 161 listens for SNMP requests.

Management Information Bases (MIBs)

Available Management Information Bases (MIBs) are located in `/usr/local/share/snmp/mibs`. This directory contains many files being routinely added or removed from the directory. Check the directory on your system by clicking Shell and entering `ls /usr/local/share/snmp/mibs`. Here is a sample of the directory contents:
root@truenas:/usr/local/share/snmp/mibs] # [Shell]
The SSH service allows connections to TrueNAS with the Secure SHell Transport Layer Protocol. When TrueNAS is used as an SSH server, the users in the network must use SSH client software to transfer files with SSH.

Allowing external connections to TrueNAS is a security vulnerability! Do not enable SSH unless external connections are required.

Activate or configure the SSH service on the Services page.

Clicking the toggle starts or stops the service, depending on the current state. Set Start Automatically for the service to start when TrueNAS boots.

To configure SSH, disable the service and click .
Configure the options as needed to match your network environment.

### SSH Service Fields

#### General Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Port</td>
<td>Open a port for SSH connection requests.</td>
</tr>
<tr>
<td>Log in as Root with Password</td>
<td>Root logins are discouraged. Allows root logins. A password must be set for the root user account.</td>
</tr>
<tr>
<td>Allow Password Authentication</td>
<td>Enabling allows SSH login authentication using a password. Warning: when directory services are enabled, this setting grants access to all users the directory service imported. When disabled, authentication requires keys for all users (requires additional SSH client and server setup).</td>
</tr>
<tr>
<td>Allow Kerberos Authentication</td>
<td>Before enabling, ensure valid entries exist in Directory Services (Kerberos Realms and Keytabs) and the system can communicate with the Kerberos Domain Controller.</td>
</tr>
<tr>
<td>Allow TCP Port Forwarding</td>
<td>Set to let users bypass firewall restrictions using the SSH port forwarding feature.</td>
</tr>
</tbody>
</table>

#### Advanced Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind Interfaces</td>
<td>Select interfaces for SSH to listen on. Leave all options unselected for SSH to listen on all interfaces.</td>
</tr>
<tr>
<td>Compress Connections</td>
<td>Select the syslog(3) level of the SFTP server.</td>
</tr>
<tr>
<td>SFTP Log Level</td>
<td>Select the syslog(3) facility of the SFTP server.</td>
</tr>
<tr>
<td>SFTP Log Facility</td>
<td>Allow more ciphers for sshd(8) in addition to the defaults in sshd_config(5). None allows unencrypted SSH connections and AES128-CBC allows the 128-bit Advanced Encryption Standard.</td>
</tr>
<tr>
<td>Weak Ciphers</td>
<td>WARNING: these ciphers are security vulnerabilities. Only allow them in a secure network environment.</td>
</tr>
</tbody>
</table>
| Auxiliary                   | Add any more sshd_config(5) options not covered in this screen. Enter one option per

---

**WARNING:** these ciphers are security vulnerabilities. Only allow them in a secure network environment.
Remote systems could require root access to the system, but have all security precautions in place before allowing root access.

There are some additional options recommendations for the SSH service:

- Add NoneEnabled no to the Auxiliary Parameters to disable the insecure none cipher.
- Increase the ClientAliveInterval if SSH connections tend to drop.
- ClientMaxStartup defaults to 10. Increase this value when more concurrent SSH connections are required.

Don’t forget to re-enable the SSH service on the Services page when all configuration changes are complete. To create and store specific SSH connections and keypairs, go to the System menu section.

### Advanced: Restricting Command Line Users to scp or sftp expand

This only works for users that use command line versions of scp and sftp. When SSH is configured, authenticated users with a user account can use ssh to log into the TrueNAS system over the network. User accounts are created by going to Accounts > Users and clicking ADD.

By default, the user sees their home directory after logging in with SSH. However, the user can still find system locations outside their home directory, so take security precautions before granting users SSH access to the system. One method to increase security is to change a user’s shell to only allow file transfers. This allows users to use scp and sftp to transfer files between their local computer and their home directory on the TrueNAS system while restricting them from logging into the system using ssh.

To configure this scenario, go to Accounts > Users and edit the desired user account. Change the Shell to scponly. Repeat for each user that needs restricted SSH access.
Test the configuration from another system by running the sftp, ssh, and scp commands as that user account. sftp and scp will work but ssh will fail.
TrueNAS uses NUT (Network UPS Tools) to provide UPS support. When the TrueNAS system is connected to a UPS device, configure the UPS service by going to Services, finding the **UPS** entry, and clicking ****.

### General Options
- **Identifier**: Describe the UPS device. It can contain alphanumeric, period, comma, hyphen, and underscore characters.

### Monitor
- **Monitor User**: upsmon
- **Monitor Password**: 
- **Remote Monitor**: 

### Specific Options expand □

### General Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>Describe the UPS device. It can contain alphanumeric, period, comma, hyphen, and underscore characters.</td>
</tr>
</tbody>
</table>
**UPS Mode**
Choose Master if the UPS is plugged directly into the system serial port. The UPS will remain the last item to shut down. Choose Slave to have this system shut down before Master. See the [Network UPS Tools Overview](#).

**Driver**
See the [Network UPS Tools compatibility list](#) for a list of supported UPS devices.

**Port or Hostname**
Serial or USB port connected to the UPS. To automatically detect and manage the USB port settings, select *auto*.

When an SNMP driver is selected, enter the IP address or hostname of the SNMP UPS device.

### Monitor

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor User</td>
<td>Enter a user to associate with this service. Keeping the default is recommended.</td>
</tr>
<tr>
<td>Monitor Password</td>
<td>Change the default password to improve system security. The new password cannot contain a space or #. Enter accounts that have administrative access. See <code>upsd.users(5)</code> for examples.</td>
</tr>
<tr>
<td>Extra Users</td>
<td>Enter accounts that have administrative access. See <code>upsd.users(5)</code> for examples.</td>
</tr>
<tr>
<td>Remote Monitor</td>
<td>Set for the default configuration to listen on all interfaces using the known values of user: <code>upsmon</code> and password: <code>fixmepass</code>.</td>
</tr>
</tbody>
</table>

### Shutdown

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown Mode</td>
<td>Choose when the UPS initiates shutdown.</td>
</tr>
<tr>
<td>Shutdown Timer</td>
<td>Enter a value in seconds for the the UPS to wait before initiating shutdown. Shutdown will not occur if power is restored while the timer is counting down. This value only applies when Shutdown mode is set to UPS goes on battery.</td>
</tr>
<tr>
<td>Shutdown Command</td>
<td>Enter a command to shut down the system when either battery power is low or the shutdown timer ends.</td>
</tr>
<tr>
<td>Power off UPS</td>
<td>Set for the UPS to power off after shutting down the system.</td>
</tr>
</tbody>
</table>

### Email

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Email Status Updates</td>
<td>Set enable sending messages to the address defined in the Email field.</td>
</tr>
<tr>
<td>Email</td>
<td>Enter any email addresses to receive status updates. Separate entries by pressing Enter.</td>
</tr>
<tr>
<td>Email Subject</td>
<td>Enter the subject for status emails.</td>
</tr>
</tbody>
</table>

### Other Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Communication Warning Time</td>
<td>Enter a number of seconds to wait before alerting that the service cannot reach any UPS. Warnings continue until the situation is fixed.</td>
</tr>
</tbody>
</table>
### Host Sync

<table>
<thead>
<tr>
<th>Description</th>
<th>Upsmon will wait up to this many seconds in master mode for the slaves to disconnect during a shutdown situation.</th>
</tr>
</thead>
</table>

| Auxiliary Parameters (ups.conf) | Enter any extra options from `ups.conf`. |

| Auxiliary Parameters (upsd.conf) | Enter any extra options from `upsd.conf`. |

Some UPS models can be unresponsive with the default polling frequency. This shows in TrueNAS logs as a recurring error like `libusb_get_interrupt: Unknown error`. If this error occurs, decrease the polling frequency by adding an entry to `Auxiliary Parameters (ups.conf)`: `pollinterval = 10`. The default polling frequency is two seconds.

`upsc(8)` can get status variables like the current charge and input voltage from the UPS daemon. Run this from the Shell using the syntax `upsc ups@localhost`. The `upsc(8)` manual page has other usage examples.

`upscmd(8)` can send commands directly to the UPS, assuming the hardware supports the command being sent. Only users with administrative rights can use this command. These users are created in the `Extra Users` field.

#### How do I find a device name? expand □
For USB devices, the easiest way to determine the correct device name is to set `Show console messages` in `System > Advanced`. Plug in the USB device and look for a `/dev/ugen` or `/dev/uhid` device name in the console messages.

#### Can I attach Multiple Computers to One UPS? expand □
A UPS with adequate capacity can power multiple computers. One computer is connected to the UPS data port with a serial or USB cable. This primary system makes UPS status available on the network for other computers. The secondary computers are powered by the UPS, but receive UPS status data from the primary computer. See the [NUT User Manual](https://nuttan.org/docs) and [NUT User Manual Pages](https://nuttan.org/docs/pages).
10 - Applications

10.1 - Jails

10.1.1 - Create

- Jail Storage
- Creating Jails
- Creating Template Jails

This feature is generally available in TrueNAS CORE and supported by the TrueNAS Community. iXsystems customers with TrueNAS Enterprise hardware and an iXsystems Support contract can contact Support about accessing these features.

Jails are a lightweight, operating-system-level virtualization. One or multiple services can run in a jail, isolating those services from the host TrueNAS system. TrueNAS uses iocage for jail and plugin management. The main differences between a user-created jail and a plugin are that plugins are preconfigured and usually provide only a single service.

Why use a Jail instead of a VM?

By default, jails run the FreeBSD operating system. These jails are independent instances of FreeBSD. The jail uses the host hardware and runs on the host kernel, avoiding most of the overhead usually associated with virtualization. The jail installs FreeBSD software management utilities so FreeBSD packages or ports can be installed from the jail command line. This allows for FreeBSD ports to be compiled and FreeBSD packages to be installed from the command line of the jail.

It is important to understand that users, groups, installed software, and configurations within a jail are isolated from both the TrueNAS host operating system and any other jails running on that system.

The ability to create multiple jails offers flexibility regarding software management. For example, an administrator can choose to provide application separation by installing different applications in each jail, to create one jail for all installed applications, or to mix and match how software is installed into each jail.

Jail Storage

A data storage pool must be created before using jails. Make sure the pool has enough storage for all the intended jails. The Jails screen displays a message and button to CREATE POOL if no pools exist on the TrueNAS system.

If pools exist, but none have been chosen for use with jails or plugins, a dialog appears to choose a pool. Select a pool and click CHOOSE.

To select a different pool for jail and plugin storage, click settings. A dialog shows the active pool. A different pool can be selected from the drop-down.

Jails and downloaded FreeBSD release files are stored in a dataset named iocage/.

The iocage dataset

- At least 10 GiB of free space is recommended.
- Cannot be located on a Share.
- iocage automatically uses the first pool that is not a root pool for the TrueNAS system.
- A defaults.json file contains default settings used when a new jail is created. The file is created automatically when not already present. When the file is present but corrupted, iocage shows a
warning and uses default settings from memory.
• Each new jail installs into a new child dataset of iocage/. For example, with the iocage/jails dataset in pool1, a new jail called jail1 installs into a new dataset named pool1/iocage/jails/jail1.
• FreeBSD releases are fetched as a child dataset into the /iocage/download dataset. This dataset is then extracted into the /iocage/releases dataset to be used in jail creation. The dataset in /iocage/download can then be removed without affecting the availability of fetched releases or an existing jail.
• iocage/ datasets on activated pools are independent of each other and do not share any data.

iocage jail configs are stored in /mnt/poolname/iocage/jails/jailname. When iocage is updated, the config.json configuration file is backed up as /mnt/poolname/iocage/jails/jailname/config_backup.json. The backup file can be renamed to config.json to restore previous jail settings.

Creating Jails

TrueNAS has two options to create a jail. The Jail Wizard makes it easy to quickly create a jail. ADVANCED JAIL CREATION is an alternate method, where every possible jail option is configurable. There are numerous options spread across four different primary sections. This form is recommended for advanced users with very specific requirements for a jail.

Additional VMware Requirements expand □

Jail Networking

If you have installed TrueNAS in VMware, you will need functional networking to create a jail.

For the jail to have functional networking, you have to change the VMware settings to allow Promiscuous, MAC address changes, and Forged Transmits.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promiscuous Mode</td>
<td>When enabled at the virtual switch level, objects defined within all portgroups can receive all incoming traffic on the vSwitch.</td>
</tr>
<tr>
<td>MAC Address Changes</td>
<td>When set to <strong>Accept</strong>, ESXi accepts requests to change the effective MAC address to a different address than the initial MAC address.</td>
</tr>
<tr>
<td>Forged Transmits</td>
<td>When set to <strong>Accept</strong>, ESXi does not compare source and effective MAC addresses.</td>
</tr>
</tbody>
</table>

** Jail Wizard

New jails can be created quickly by going to Jails > ADD.
The wizard provides the simplest process to create and configure a new jail.

Enter a **Jail Name**. Names can contain letters, numbers, periods (.), dashes (-), and underscores (_).

Choose a **Jail Type**: Default (Clone Jail) or Basejail. Clone jails are clones of the specified FreeBSD RELEASE. They are linked to that RELEASE, even if they are upgraded. Basejails mount the specified RELEASE directories as nullfs mounts over the jail directories. Basejails are not linked to the original RELEASE when upgraded.

Jails can run FreeBSD versions up to the same version as the host TrueNAS system. Newer releases are not shown.

Versions of FreeBSD are downloaded the first time they are used in a jail. Additional jails created with the same version of FreeBSD are created faster because the download has already been completed.

Click **NEXT** to see a simplified list of networking options.

Jails support several different networking solutions:

- **VNET** adds a virtual network interface to the jail. This interface can set NAT, DHCP, or static jail network configurations. Since VNET provides the jail with an independent networking stack, it can broadcast an IP address, which is required by some applications.

- **Network Address Translation (NAT)**, which uses the TrueNAS IP address and sets a unique port for the jail to use. VNET is required when NAT is selected.

- Set **DHCP Autoconfigure IPv4** for the jail to receive its IP address from a DHCP server.

- Manually configure networking by entering values for the **IPv4 Address** or **IPv6 Address** fields. Any combination of these fields can be configured. Multiple interfaces are supported for IPv4 and IPv6 addresses. To add more interfaces and addresses, click **ADD**.

  Setting the **IPv4 Default Router** and **IPv6 Default Router** fields to **auto** automatically configures these values. VNET must be set to enable the **IPv4 Default Router** field. When no interface is selected when manually configuring IP addresses, TrueNAS automatically assigns the given jail IP address to the current active interface of the host system.

- Leaving all checkboxes unset and fields empty initializes the jail without any networking abilities.
Networking is added to the jail after creation by going to **Jails**, clicking **chevron_right** for a jail, then **edit > Basic Properties**.

Setting a proxy in the TrueNAS network settings also configures new jails to use the proxy settings, except when performing DNS lookups. Make sure a firewall is properly configured to maximize system security.

When pairing the jail with a physical interface, edit the network interface and set *Disable Hardware Offloading*. This prevents a network interface reset when the jail starts.

Click **NEXT** to view a summary screen of the chosen jail options. Click **SUBMIT** to create the new jail. After a few moments, the new jail is added to the primary jails list.

- **Advanced Jail Creation**

  The advanced jail creation form is opened by clicking **Jails > ADD**, then **ADVANCED JAIL CREATION**.
Options

A usable jail without any networking can be quickly created by setting only the required **Jail Name** and **Release**. Configure the remaining **Basic Properties** when the jail needs to communicate over the local network or out to the internet.

### Basic Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Required. Can contain letters, numbers, periods (.), dashes (-), and underscores (_).</td>
</tr>
<tr>
<td>Jail Type</td>
<td>Default (Clone Jail) or Basejail. Clone jails are clones of the specified RELEASE. They are linked to that RELEASE, even if they are upgraded. Basejails mount the specified RELEASE directories as nullfs mounts over the jail directories. Basejails are not linked to the original RELEASE when upgraded.</td>
</tr>
<tr>
<td>Release</td>
<td>FreeBSD release to use as the jail operating system. Jails can run FreeBSD versions up to the same version as the host system. Newer releases are not shown.</td>
</tr>
<tr>
<td>DHCP Autoconfigure IPv4</td>
<td>Set to autoconfigure jail networking with the Dynamic Host Configuration Protocol. VNET and Berkeley Packet Filter must also be enabled.</td>
</tr>
</tbody>
</table>
NAT
Network Address Translation (NAT). Transforms local network IP addresses into a single IP address. Set when the jail will share a single connection to the Internet with other systems on the network.

VNET
Set to use VNET(9) to emulate network devices for the jail. A fully virtualized per-jail network stack will be installed.

Berkeley Packet Filter
Set to use the Berkeley Packet Filter (BPF(4)) to data link layers in a protocol independent fashion.

vnet_default_interface
Set the default VNET interface. Only takes effect when VNET is set. Choose a specific interface or set to auto to use the interface that has the default route. Choose none to not set a default VNET interface.

IPv4 Interface
IPv4 interface for the jail.

IPv4 Address
Enter the IPv4 address for VNET(9) and shared IP jails.

IPv4 Netmask
IPv4 netmask for the jail.

IPv4 Default Router
A valid IPv4 address to use as the default route. Enter none to configure the jail with no IPv4 default route. A jail without a default route will not be able to access any networks.

AutoConfigure IPv6
Set to use SLAAC (Stateless Address Auto Configuration) to autoconfigure IPv6 in the jail.

IPv6 Interface
IPv6 interface for the jail.

IPv6 Address
Enter the IPv6 address for VNET(9) and shared IP jails.

IPv6 Netmask
IPv6 prefix for the jail.

IPv6 Default Router
A valid IPv6 address to use as the default route. Enter none to configure the jail without an IPv6 default route. A jail without a default route will not be able to access any networks.

Auto Start
Set to auto-start the jail at system boot time. Jails are started and stopped based on iocage priority. Set in the priority field under Custom Properties.

Additional settings are in the Jail Properties, Network Properties, and Custom Properties sections.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>devfs_ruleset</td>
<td>The devfs(8) ruleset number to enforce when mounting devfs in the jail. The default 0 means no ruleset is enforced. Mounting devfs inside a jail is only possible when the allow_mount and allow_mount_devfs permissions are enabled and enforce_statfs is set to a value lower than 2.</td>
</tr>
<tr>
<td>exec_start</td>
<td>Commands to run in the jail environment when the jail is created. Example: sh /etc/rc. The pseudo-parameters section of JAIL(8) describes exec.start usage.</td>
</tr>
<tr>
<td>exec_stop</td>
<td>Commands to run in the jail environment before the jail is removed and after exec.prestart commands are complete. Example: sh /etc/rc.shutdown.</td>
</tr>
<tr>
<td>exec_prestart</td>
<td>Commands to run in the system environment before a jail is started.</td>
</tr>
<tr>
<td>exec_poststart</td>
<td>Commands to run in the system environment after a jail is started and after any exec_start commands are finished.</td>
</tr>
<tr>
<td>exec_prestop</td>
<td>Commands to run in the system environment before a jail is stopped.</td>
</tr>
<tr>
<td>exec_poststop</td>
<td>Commands to run in the system environment after a jail is stopped.</td>
</tr>
<tr>
<td>exec_jail_user</td>
<td>Enter either root or another valid username. Inside the jail, commands run as this user.</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>exec_system_user</td>
<td>Run commands in the jail as this user. By default, commands are run as the current user.</td>
</tr>
<tr>
<td>securelevel</td>
<td>The value of the jail securelevel sysctl. A jail never has a lower securelevel than the host system. Setting this parameter allows a higher securelevel. If the host system securelevel is changed, the jail securelevel will be at least as secure.</td>
</tr>
<tr>
<td>sysvmsg</td>
<td>Allow or deny access to SYSV IPC message primitives. Inherit: All IPC objects on the system are visible to the jail. New: Only objects the jail creates using the private key namespace are visible. The system and parent jails have access to the jail objects but not private keys. Disable: The jail cannot perform any sysvmsg related system calls.</td>
</tr>
<tr>
<td>sysvsem</td>
<td>Allow or deny access to SYSV IPC semaphore primitives. Inherit: All IPC objects on the system are visible to the jail. New: Only objects the jail creates using the private key namespace are visible. The system and parent jails have access to the jail objects but not private keys. Disable: The jail cannot perform any sysvsem related system calls.</td>
</tr>
<tr>
<td>sysvshm</td>
<td>Allow or deny access to SYSV IPC shared memory primitives. Inherit: All IPC objects on the system are visible to the jail. New: Only objects the jail creates using the private key namespace are visible. The system and parent jails have access to the jail objects but not private keys.</td>
</tr>
<tr>
<td>vnet_interfaces</td>
<td>A space-delimited list of network interfaces attached to a VNET enabled jail after it is created. Interfaces are automatically released when the jail is removed.</td>
</tr>
<tr>
<td>allow_set_hostname</td>
<td>Allow the jail hostname to be changed with hostname(1) or sethostname(3).</td>
</tr>
<tr>
<td>allow_sysvipc</td>
<td>Choose whether a process in the jail has access to System V IPC primitives. Equivalent to setting sysvmsg, sysvsem, and sysvshm to Inherit. Deprecated in FreeBSD 11.0 and newer! Use sysvmsg, sysvsem, and sysvshm instead.</td>
</tr>
<tr>
<td>allow_rawsockets</td>
<td>Set to allow raw sockets. Utilities like ping(8) and traceroute(8) require raw sockets. When set, source IP addresses are enforced to comply with the IP addresses bound to the jail, ignoring the IP_HDRINCL flag on the socket.</td>
</tr>
<tr>
<td>allow_chflags</td>
<td>Set to treat jail users as privileged and allow the manipulation of system file flags. securelevel constraints are still enforced.</td>
</tr>
<tr>
<td>allow_mlock</td>
<td>Enable running services that require mlock(2) in a jail.</td>
</tr>
<tr>
<td>allow_vmm</td>
<td>Allow the jail to access the bhyve virtual machine monitor (VMM). The jail must have FreeBSD 12.0 or newer installed with the vmm(4) kernel module loaded.</td>
</tr>
<tr>
<td>allow_quotas</td>
<td>Set to allow the jail root to administer quotas on jail filesystems. This includes filesystems the jail shares with other jails or with non-jailed parts of the system.</td>
</tr>
<tr>
<td>allow_socket_af</td>
<td>Set to allow access to other protocol stacks beyond IPv4, IPv6, local (UNIX), and route. Warning: jail functionality does not exist for all protocol stacks.</td>
</tr>
<tr>
<td>allow_mount</td>
<td>Set to allow privileged users inside the jail to mount and unmount filesystem types marked as jail-friendly.</td>
</tr>
</tbody>
</table>

### Network Properties

#### Interfaces

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter up to four interface configurations in the format interface:bridge, separated by a comma (,). The left value is the virtual VNET interface name and the right value is the bridge name where the virtual interface should be attached.</td>
<td></td>
</tr>
<tr>
<td>host_domainname</td>
<td>Enter a <strong>NIS Domain name</strong> for the jail.</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>host_hostname</td>
<td>Set the jail hostname. Defaults to the jail UUID.</td>
</tr>
<tr>
<td>resolver</td>
<td>Add lines to the jail resolv.conf. Example: nameserver IP;search domain.local. Fields must be delimited with a semicolon (;), This is translated as new lines in resolv.conf. Enter none to inherit resolv.conf from the host.</td>
</tr>
<tr>
<td>ip4.saddrsel</td>
<td>Disable IPv4 source address selection for the jail in favor of the primary IPv4 address of the jail. Only available when the jail is not configured to use VNET.</td>
</tr>
<tr>
<td>ip6.saddrsel</td>
<td>Disable IPv6 source address selection for the jail in favor of the primary IPv6 address of the jail. Only available when the jail is not configured to use VNET.</td>
</tr>
<tr>
<td>ip4</td>
<td>Control the availability of IPv4 addresses. Inherit: Allow unrestricted access to all system addresses. New: Restrict addresses with ip4_addr. Disable: Stop the jail from using IPv4 entirely.</td>
</tr>
<tr>
<td>ip6</td>
<td>Control the availability of IPv6 addresses. Inherit: Allow unrestricted access to all system addresses. New: Restrict addresses with ip6_addr. Disable: Stop the jail from using IPv6 entirely.</td>
</tr>
<tr>
<td>mac_prefix</td>
<td>Enter a valid MAC address vendor prefix. Example: E4F4C6</td>
</tr>
<tr>
<td>vnet0_mac</td>
<td>Leave this field empty to generate random MAC addresses for the host and jail. To assign fixed MAC addresses, enter the MAC address to be assigned to the host, a space, then the MAC address to be assigned to the jail.</td>
</tr>
</tbody>
</table>

**Custom Properties**

**Expand □**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>Numeric start priority for the jail at boot time. Valid priorities are between 1 and 99. Smaller values are higher priority. At system shutdown the priority is reversed. Example: 99</td>
</tr>
<tr>
<td>hostid</td>
<td>A new jail hostid, if desired. Example hostid: 1a2bc345-678d-90e1-23fa-4b56c78901de.</td>
</tr>
<tr>
<td>comment</td>
<td>Enter comments about the jail.</td>
</tr>
<tr>
<td>template</td>
<td>Set to set this jail as a template.</td>
</tr>
<tr>
<td>host_time</td>
<td>System host time to synchronize the time between jail and host.</td>
</tr>
<tr>
<td>jail_zfs</td>
<td>Set to enable automatic ZFS jailing inside the jail. The assigned ZFS dataset is fully controlled by the jail.</td>
</tr>
<tr>
<td>jail_zfs_dataset</td>
<td>Define the dataset to be jailed and fully handed over to a jail. Enter a ZFS filesystem name without a pool name. jail_zfs must be set for this option to work.</td>
</tr>
<tr>
<td>jail_zfs_mountpoint</td>
<td>Enter the mountpoint for the jail_zfs_dataset. Example: /data example-dataset- name</td>
</tr>
<tr>
<td>allow_tun</td>
<td>Reveal tun devices for the jail with an individual devfs ruleset. Allow the creation of tun devices in the jail.</td>
</tr>
<tr>
<td>Autoconfigure IPv6 with rtsold</td>
<td>Use rtsold(8) as part of IPv6 autoconfiguration. Send ICMPv6 Router Solicitation messages to interfaces to discover new routers.</td>
</tr>
<tr>
<td>ip_hostname</td>
<td>Set to use DNS records during jail IP configuration to search the resolver and apply the first open IPv4 and IPv6 addresses. See jail(8).</td>
</tr>
<tr>
<td>assign_localhost</td>
<td>Set to add network interface lo0 to the jail and assign it the first available localhost address, starting with 127.0.0.2. VNET must be unset. Jails using VNET</td>
</tr>
</tbody>
</table>
Creating Template Jails

Template jails are basejails that can efficiently create jails with the same configuration. These steps create a template jail:

- Go to Jails > ADD > ADVANCED JAIL CREATION.
- Select Basejail as the Jail Type. Configure the jail with desired options.
- Set template in the Custom Properties section.
- Click SAVE.
- Click ADD.
- Enter a name for the template jail. Leave Jail Type as Default (Clone Jail). Set Release to basejailname(template), where basejailname is the name of the base jail created earlier.
- Complete the jail creation wizard.
10.1.2 - Manage

- Updates and Upgrades
- Accessing a Jail Using SSH

Going to the Jails screen shows a list of installed jails.

Operations can be applied to multiple jails by selecting those jails with the checkboxes on the left. After selecting one or more jails, icons appear which can be used to play_arrow, stop, update, or delete those jails.

More information such as IPV4, IPV6, jail TYPE, and whether it is a TEMPLATE or BASEJAIL is seen by clicking > (Expand) for a jail. Additional options for that jail are also displayed.

Modify the IP address information for a jail by clicking chevron_right > EDIT instead of issuing the networking commands directly from the command line of the jail. This ensures changes are saved and survive a jail or TrueNAS reboot.
| **EDIT** | Used to modify the settings described in Advanced Jail Creation. A jail cannot be edited while it is running. The settings can be viewed, but are read only. |
| **MOUNT POINTS** | Select an existing mount point to **EDIT** or click **ACTIONS > Add Mount Point** to create a mount point for the jail. A mount point gives a jail access to storage located elsewhere on the system. A jail must be stopped before adding, editing, or deleting a mount point. See Additional Storage for more details. |
| **RESTART** | Stop and immediately start an up jail. |
| **START** | Start a jail that has a current **STATE** of down. |
| **STOP** | Stop a jail that has a current **STATE** of up. |
| **UPDATE** | Runs [freebsd-update](https://www.FreeBSD.org/) to update the jail to the latest patch level of the installed FreeBSD release. |
| **SHELL** | Access a root command prompt to interact with a jail directly from the command line. Type `exit` to leave the command prompt. |
| **DELETE** | Caution: deleting the jail also deletes all of the jail contents and all associated snapshots. Back up the jail data, configuration, and programs first. There is no way to recover the contents of a jail after deletion! |

Menu entries change depending on the jail state. For example, a stopped jail does not have a **STOP** or **SHELL** option.

Jail status messages and command output are stored in `/var/log/iocage.log`.

### Updates and Upgrades

Click **Update** to update a jail to the most current patch level of the installed FreeBSD release. This does not change the release. For example, a jail installed with FreeBSD 11.2-RELEASE can update to p15 or the latest patch of 11.2, but not an 11.3-RELEASE-p# version of FreeBSD.

A jail **upgrade** replaces the jail FreeBSD operating system with a new release of FreeBSD, such as taking a jail from FreeBSD 11.2-RELEASE to 11.3-RELEASE. Upgrade a jail by stopping it, opening the TrueNAS Shell and entering `iocage upgrade name -r release`, where `name` is the plugin jail name and `release` is the desired FreeBSD release.

It is possible to manually remove unused releases from the `/iocage/releases/` dataset after upgrading a jail. The release must not be in use by any jail on the system!

### Accessing a Jail Using SSH

The ssh daemon ssdhd(8) must be enabled in a jail to allow SSH access to that jail from another system.

The jail **STATE** must be up before the **SHELL** option is available. When the jail is not up, start it by clicking **Jails > chevron_right > START** for the desired jail. Click **chevron_right**, then **SHELL** to open a shell inside the jail:

```
FreeBSD 11.1-STABLE (FreeNAS.amd64) #0 0a9e9f753(freenas/11-stable): Fri Apr 6 04:46:31 UTC 2018
Welcome to FreeBSD!
```

FreeBSD FAQ: [https://www.FreeBSD.org/faq/](https://www.FreeBSD.org/faq/)
FreeBSD Forums: [https://forums.FreeBSD.org/](https://forums.FreeBSD.org/)

Documents installed with the system are in the `/usr/local/share/doc/freebsd/` directory, or can be installed later with: `pkg install en-freebsd-doc` for other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed: `freebsd-version ; uname -a` Please include that output and any error messages when posting questions.
**Introduction to manual pages:** man man
-FreeBSD directory layout: man hier

Edit /etc/motd to change this login announcement.

```bash
root@jailexamp:~ #
```

**The Shell** can also open a jail root shell. Open the **Shell** and enter `iocage console jailname`.

Enable sshd:

```bash
sysrc sshd_enable="YES"
sshd_enable: NO -> YES
```

Start the SSH daemon: `service sshd start`. The first time the service runs, the jail RSA key pair is generated and the key fingerprint is displayed. Add a user account with `adduser` and follow the prompts. `Enter` accepts the default value. Users that require root access must also be a member of the `wheel` group. `Enter` `wheel` when prompted to `invite user into other groups`?

```bash
root@jailexamp:~ # adduser
Username: jailuser
Full name: Jail User
Uid (Leave empty for default):
Login group []jailuser]:
Login group is jailuser. Invite jailuser into other groups? []: wheel
Login class [default]:
Shell (sh csh tcsh git-shell zsh rrsh nologin) [sh]: csh
Home directory / [home/jailuser]:
Home directory permissions (Leave empty for default):
Use password-based authentication? [yes]:
Use an empty password? (yes/no) [no]:
Use a random password? (yes/no) [no]:
Enter password:
Enter password again:
Lock out the account after creation? [no]:
Username : jailuser
Password : *****
Full Name : Jail User
Uid : 1002
Class :
Groups : jailuser wheel
Home : /home/jailuser
Home Mode :
Shell : /bin/csh
Locked : no
OK? (yes/no): yes
adduser: INFO: Successfully added (jailuser) to the user database.
Add another user? (yes/no): no
Goodbye!
root@jailexamp:~
```

After creating the user, set the jail root password to allow users to use `su` to gain superuser privileges. To set the jail root password, use `passwd`. Nothing is echoed back when using `passwd`:

```bash
root@jailexamp:~ # passwd
Changing local password for root
New Password:
Retype New Password:
root@jailexamp:~ #
```

Finally, test that the user can successfully `ssh` into the jail from another system and gain superuser privileges. In this example, a user named jailuser uses `ssh` to access the jail at `192.168.2.3`. The host RSA key fingerprint must be verified the first time a user logs in.

```bash
ssh jailuser@192.168.2.3
The authenticity of host '192.168.2.3 (192.168.2.3)' can't be established.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.2.3' (RSA) to the list of known hosts.
Password:
```

Every jail has its own user accounts and service configuration. These steps must be repeated for each jail that requires SSH access.
10.1.3 - Installing Software

A jail is created with no software aside from the core packages installed as part of the selected version of FreeBSD. To install more software, go to the Jails screen and expand the jail entry. Start the jail, then click > SHELL when the jail has booted.

Installing FreeBSD Packages

The quickest and easiest way to install software inside the jail is to install a FreeBSD package. FreeBSD packages are precompiled and contain all the binaries and a list of dependencies required for the software to run on a FreeBSD system.

A huge amount of software has been ported to FreeBSD. Most of that software is available as packages. One way to find FreeBSD software is to use the search bar at FreshPorts.org.

After finding the name of the desired package, use the `pkg install` command to install it. For example, to install the audiotag package, enter `pkg install audiotag`. When prompted, press `y` to complete the
installation. Messages show the download and installation status.

A successful installation is confirmed by querying the package database:

```
pkg info -f audiotag
audiotag-0.19_1
Name:           audiotag
Version:        0.19_1
Installed on:   Fri Nov 21 10:10:34 PST 2014
Origin:         audio/audiotag
Architecture:   freebsd:9:x86:64
Prefix:         /usr/local
Categories:     multimedia audio
Licenses:       GPLv2
Maintainer:     ports@FreeBSD.org
WWW:            https://github.com/Daenyth/audiotag
Comment:        Command-line tool for mass tagging/renameing of audio files
Options:
  DOCS:         on
  FLAC:         on
  ID3:          on
  MP4:          on
  VORBIS:       on
Annotations:
  repo_type:    binary
  repository:   FreeBSD
Flat size:      62.8KiB
Description:   Audiotag is a command-line tool for mass tagging/renameing of audio files
               it supports the vorbis comment, id3 tags, and MP4 tags.
WWW:           https://github.com/Daenyth/audiotag
```

To show what was installed by the package:

```
pkg info -l audiotag
audiotag-0.19_1:
  /usr/local/bin/audiotag
  /usr/local/share/doc/audiotag/COPYING
  /usr/local/share/doc/audiotag/ChangeLog
  /usr/local/share/doc/audiotag/README
  /usr/local/share/licenses/audiotag-0.19_1/GPLv2
  /usr/local/share/licenses/audiotag-0.19_1/LICENSE
  /usr/local/share/licenses/audiotag-0.19_1/catalog.mk
```

In FreeBSD, third-party software is always stored in /usr/local to differentiate it from the software that came with the operating system. Binaries are almost always located in a subdirectory called bin or sbin and configuration files in a subdirectory called etc.

**Compiling FreeBSD Ports**

Compiling a port is another option. Compiling ports offer these advantages:

- Not every port has an available package. This is usually due to licensing restrictions or known, unaddressed security vulnerabilities.
- Sometimes the package is out-of-date and a feature is needed that only became available in the newer version.
- Some ports provide compile options that are not available in the pre-compiled package. These options are used to add or remove features or options.

Compiling a port has these disadvantages:

- It takes time. Depending upon the size of the application, the amount of dependencies, the speed of the CPU, the amount of RAM available, and the current load on the TrueNAS system, the time needed can range from a few minutes to a few hours or even to a few days.
- If the port does not provide any compile options, it saves time and preserves the TrueNAS system resources to use the `pkg install` command instead. The [FreshPorts.org](https://freshports.org) listing shows whether a port has any configurable compile options.
### Commit History - (may be incomplete: see SVNWeb link above for full details)

<table>
<thead>
<tr>
<th>Date</th>
<th>By</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Sponsored by: Absolutlight</td>
</tr>
<tr>
<td>25 May 2016 15:03:34</td>
<td>mat</td>
<td>Remove useless MIME/ENC definitions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>While there, correct DEP WARNING5 when they occur.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sponsored by: Absolutlight</td>
</tr>
<tr>
<td>01 Apr 2016 12:23:17</td>
<td>mat</td>
<td>Remove 6/PORTINDIR/ from dependencies, M number and categories a, b, c.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WITH test: portmgr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sponsored by: Absolutlight</td>
</tr>
<tr>
<td>17 Jun 2016 14:29:32</td>
<td>andreus</td>
<td>Convert LICENSE-APACHE75 or later to &quot;*|&quot; License.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Approved by: portmgr, blanket</td>
</tr>
<tr>
<td>18 Nov 2015 10:14:05</td>
<td>andreus</td>
<td>Clarify LICENSE-APACHE75 or later to &quot;*|&quot; License.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>And LICENSE-PÉRECH.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>And NO ARCH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select for options helpers</td>
</tr>
<tr>
<td>02 Jun 2014 19:03:14</td>
<td>stainer</td>
<td>USE (PORTINDIR) -&gt; USE? (new:2) (new:2)</td>
</tr>
<tr>
<td>24 May 2012 10:38:49</td>
<td>kevin</td>
<td>Remove gcraft</td>
</tr>
<tr>
<td>24 Nov 2011 18:36:37</td>
<td>r.b.</td>
<td>Support staging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Use options helpers)</td>
</tr>
<tr>
<td>20 Sep 2012 14:36:37</td>
<td>r.b.</td>
<td>Add NO STAGS all over the place in preparation for the staging support (not:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port</td>
</tr>
<tr>
<td>03 Aug 2013 13:34:01</td>
<td>r.b.</td>
<td>- Convert to new port framework</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Remove MNE_ORD_SAFETY, it's the default.</td>
</tr>
<tr>
<td>06 May 2013 22:26:27</td>
<td>r.b.</td>
<td>Use checkfix</td>
</tr>
<tr>
<td>23 May 2013 19:39:24</td>
<td>r.b.</td>
<td>Fix the .GETHER in combination with MASTER_SET with which breaks WHERE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Drop maintenability</td>
</tr>
<tr>
<td>12 Dec 2012 11:51:44</td>
<td>r.b.</td>
<td>- Trim headers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Switch to USE GITMAN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Remove optional LICENSE-PÉRECH, license being plate GPL2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Various</td>
</tr>
</tbody>
</table>
Audiotag Port Information

Packages are built with default options. Ports let the user select options.

The FreeBSD Ports Collection must be installed in the jail before ports can be compiled. Inside the jail, use the `portsnap` utility. This command downloads the ports collection and extracts it to the `/usr/ports/` directory of the jail:

```
portsnap fetch extract
```

To install additional software at a later date, make sure the ports collection is updated with `portsnap fetch update`.

To compile a port, `cd` into a subdirectory of `/usr/ports/`. The entry for the port at FreshPorts provides the location to `cd` into and the `make` command to run. This example compiles and installs the `audiotag` port:

```
    cd /usr/ports/audio/audiotag
    make install clean
```

The first time this command is run, the configure screen shown.

```
    audiotag 0.19_1
    | [x] YES Build and/or install documentation
    | [x] YES FLAC full lossless audio codec support
    | [x] YES ID3 ID3 tags support
    | [x] YES MP4 MP4 media format support
    | [x] YES VORBIS Ogg Vorbis audio codec support
```

Audiotag Port Configuration Options

This port has several configurable options: `DOCS`, `FLAC`, `ID3`, `MP4`, and `VORBIS`. Selected options are shown with a `*`. 
Use the arrow keys to select an option and press **spacebar** to toggle the value. Press **Enter** when satisfied with the options. The port begins to compile and install.

After options are set, the configuration screen is normally not shown again. Use `make config` to display the screen and change options before rebuilding the port with `make clean install clean`.

Many ports depend on other ports. Those other ports also have configuration screens that are shown before compiling begins. It is a good idea to watch the compile until it finishes and the command prompt returns.

Installed ports are registered in the same package database that manages packages. `pkg info` determines which ports were installed.

### Starting Installed Software

After packages or ports are installed, they must be configured and started. Configuration files are usually in `/usr/local/etc` or a subdirectory of it. Many FreeBSD packages contain a sample configuration file as a reference. Take some time to read the software documentation to learn which configuration options are available and which configuration files require editing.

Most FreeBSD packages that contain a startable service include a startup script that is automatically installed to `/usr/local/etc/rc.d/`. After the configuration is complete, test starting the service by running the script with the `onestart` option. For example, when `openvpn` is installed in a jail, these commands verify that the service has started:

```
/usr/local/etc/rc.d/openvpn onestart
Starting openvpn.
```

```
/usr/local/etc/rc.d/openvpn onestatus
openvpn is running as pid 45560.
```

If it produces an error:

```
/usr/local/etc/rc.d/openvpn onestart
Starting openvpn.
```

```
/usr/local/etc/rc.d/openvpn: WARNING: failed to start openvpn
```

Enter `tail /var/log/messages` to see any error messages if an issue is found. Most startup failures are related to a misconfiguration in a configuration file.

After verifying that the service starts and is working as intended, add a line to `/etc/rc.conf` to start the service automatically when the jail is started. The line to start a service always ends in `_enable="YES"` and typically starts with the name of the software. For example, this is the entry for the `openvpn` service:

```
openvpn_enable="YES"
```

When in doubt, the startup script shows the line to put in `/etc/rc.conf`. This is the description in `/usr/local/etc/rc.d/openvpn`:

```
# To run additional instances link this script to something like
# % in -s openvpn openvpn_foo

# and define additional openvpn_foo.* variables in one of
# /etc/rc.conf, /etc/rc.conf.local or /etc/rc.conf.d /openvpn_foo

# Below NAME should be substituted with the name of this script. By default
# it is openvpn, so read as openvpn_enable. If you linked the script to
# openvpn_foo, then read as openvpn_foo_enable etc.

# The following variables are supported (defaults are shown).
# You can place them in any of
# /etc/rc.conf, /etc/rc.conf.local or /etc/rc.conf.d/NAME
# NAME_enable="NO"
# set To YES to enable openvpn
```

The startup script also indicates if any additional parameters are available:
NAME_if=
# driver(s) to load, set to "tun", "tap" or "tun tap"
# it is OK to specify the if_ prefix.

# optional:
NAME_flags=
# additional command line arguments
NAME_configfile="/usr/local/etc/openvpn/NAME.conf"
# --config file
NAME_dir="/usr/local/etc/openvpn"
# --cd directory
**10.1.4 - Additional Storage**

Jails can be given access to an area of storage outside of the jail that is configured on the TrueNAS system. It is possible to give a FreeBSD jail access to an area of storage on the TrueNAS system. This is useful for applications or plugins that store large amounts of data or if an application in a jail needs access to data stored on the TrueNAS system. For example, *Transmission* is a plugin that stores data using BitTorrent. The TrueNAS external storage is added using the `mount_nullfs(8)` mechanism, which links data that resides outside of the jail as a storage area within a jail.

MOUNT POINTS shows any added storage and allows adding more storage.

A jail must have a **STATE** of *down* before adding a new mount point. Click chevron_right and stop for a jail to change the jail **STATE** to down.

Storage can be added by clicking Jails > chevron_right > MOUNT POINTS for the desired jail. The MOUNT POINT section is a list of all of the currently defined mount points.

Go to MOUNT POINTS > ACTIONS > Add Mount Point to add storage to a jail.

[Image of TrueNAS interface with mount points]

Browse to the **Source** and **Destination**, where:

- **Source** is the directory or dataset on the TrueNAS system that is accessed by the jail. TrueNAS creates the directory if it does not exist. This directory must reside outside of the pool or dataset being used by the jail. This is why it is recommended to create a separate dataset to store jails. The dataset holding the jails is always separate from any datasets used for storage on the TrueNAS system.

- **Destination** is an existing and empty directory within the jail to link to the **Source** storage area. Adding / and a name to the end of the path for TrueNAS creates a new directory. New directories
created must be **within** the jail directory structure. Example: `/mnt/iocage/jails/samplejail/root/new-destination-directory`.

Storage is typically added because the user and group account associated with an application installed inside of a jail needs to access data stored on the TrueNAS system. Before selecting the **Source**, it is important to ensure that the permissions of the selected directory or dataset grant permission to the user or group account inside the jail. This is not the default, as the users and groups created inside a jail are separate from the users and groups created on the TrueNAS system.

Here is the typical workflow for adding jail storage:

- **Determine the name of the user and group account used by the application.** For example, the installation of the `transmission` application automatically creates a user account named `transmission` and a group account also named `transmission`. When in doubt, check the files `/etc/passwd` (to find the user account) and `/etc/group` (to find the group account) inside the jail.

  Typically, the user and group names are similar to the application name. Also, the UID and GID are usually the same as the port number used by the service. A `media` user and group (GID 8675309) are part of the base system. Having applications run as this group or user makes it possible to share storage between multiple applications in a single jail, between multiple jails, or even between the host and jails.

- **On the TrueNAS system, create a user account and group account that match the user and group names used by the jail application.**

- **Decide if the jail needs access to existing data or if a new storage area should be created.**

- **If the jail needs to access existing data, edit the permissions of the pool or dataset so the user and group accounts have the desired read and write access.** When multiple applications or jails need access to the same data, create a new group and add each new user account to that group.

- **If a new storage area is being set aside for that jail or application, create a dataset.** Edit the dataset permissions so the user and group account has the desired read and write access.

- **Use jail > MOUNT POINTS > ACTIONS > Add Mount Point** to select the data **Source** and the jail mount **Destination**.

To prevent writes to the storage, click **Read-Only**.

After storage has been added or created, it appears in the MOUNT POINTS for that jail.

<table>
<thead>
<tr>
<th>Mount Points of Solitary</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/mnt/a-star</code></td>
<td><code>/mnt/a-star/iocage/jails/Solitary/root/root</code></td>
</tr>
<tr>
<td>1 - 1 of 1</td>
<td></td>
</tr>
</tbody>
</table>

Storage is automatically mounted as it is created. Mounting a dataset does not automatically mount any child datasets inside it. Each dataset is a separate filesystem, so child datasets must each have separate mount points.

Click **more_vert > Delete** to delete the storage.

---

Remember that added storage is just a pointer to the selected storage directory on the TrueNAS system. It does not copy that data to the jail. Files that are deleted from the `Destination` directory in the jail are also deleted from the **Source** directory on the TrueNAS system. However, removing the jail storage entry only removes the pointer. This leaves the data intact but no longer accessible to the jail.
10.2 - Plugins

10.2.1 - Plugin Management

- **Plugin Installation**
  - Catalog
  - Install Options
- **Post-Install Configuration**
- **Removing a Plugin**
  - Backing up Jail Data
  - Uninstalling a Plugin

This feature is generally available in TrueNAS CORE and supported by the TrueNAS Community. iXsystems customers with TrueNAS Enterprise hardware and an iXsystems Support contract can contact Support about accessing these features.

Plugins allow extending the built-in NAS services by installing additional software. A plugin is a pre-packaged application that is installed into a FreeBSD Jail. The plugin jail is limited to installing and using only the plugin software.

### Before getting started...
- A data pool must be available for plugin storage.
- The system must be connected to the internet.
- Go to Network > Interfaces, edit the intended plugin interface, and set Disable Hardware Offloading.

### Plugin Installation

#### Catalog

To see the plugin catalog, go to the Plugins screen.

#### First time in this menu?

Going to the Jails or Plugins screen for the first time prompts to select a location on the system for storing Jail related data.

**Choose Pool for Plugin and Jail Storage**

Choose a pool for plugin and jail storage.

corepool

By default, this location stores all data related to jails and plugins, including downloaded applications, data managed by the jail or plugin, and any jail snapshots.

Disconnecting or deleting the pool that stores jail data can result in permanent data loss! Make
sure to back up any critical data or snapshots that are stored in a jail before changing the storage configuration.

To change the Jails and Plugins storage location, click 🗃️, select a new pool, and click CHOOSE.

I don't see anything? expand 📜

If the catalog doesn't load:

- Go to Network > Global Configuration and confirm the Default Gateway and DNS Servers addresses are correct.
- Open the Shell and ping an Internet address. The output confirms the system is connected to the Internet.

Plugins are organized into two Collections:

- iXsystems maintained plugins
- Open Source plugins created and maintained by the TrueNAS community.

By default, the iXsystems-supported plugins are shown. To view the community-supported plugins, open Browse a Collection and select Community.

Install Options

To install a plugin, click the plugin icon and Install. This example shows installing Tarsnap, a popular backup solution.

Enter a Jail Name for the plugin and adjust the networking settings as needed. Most plugins default to using Network Address Translation (NAT) for their Internet connection, but you can choose to use a dynamically-generated address with DHCP or define static IP addresses for the plugin jail. Using NAT is recommended as it does not require manual configuration of multiple available IP addresses and prevents addressing conflicts on the network.

Some plugins default to DHCP as their management utility conflicts with NAT. Keep these plugins set to DHCP unless a manually configured IP address is preferred.

Plugins can take several minutes to download and install. A dialog confirms when the installation is
complete and shows any post-install notes. You can view the post-install notes later by expanding the entry for the installed plugin in **Plugins** and clicking **Post Install Notes**.

**Troubleshooting**

If a plugin download or update fails with an error about being unable to fetch an artifact or download a package, you might need to investigate your networking environment. Some home routers can have a security feature that prevent DHCP enabled plugins (or bridged devices with virtual MAC addresses) from resolving addresses. Also, sometimes additional DNS validation is required that is not supported by the router or the router has a caching resolver that is holding on to a stale record. A couple of possible solutions are to hard reset your router to clear any stale records or try using an alternate DNS server for the plugin.

### Post-Install Configuration

After a plugin is installed, an entry is added to the **Plugins** screen.

Click **chevron_right** to manage the plugin state, update the plugin application, configure the plugin jail mount points to storage datasets, and, when supported, open a link to the management portal for the plugin application.

Plugin jails are preconfigured and require very little tuning. However, jail properties are available in the event a setting needs to change. To update or reconfigure the plugin jail, go to the **Jails** screen and expand the entry for one of the plugin jails. You need to click **** and stop the jail before changing it.

### Removing a Plugin

Uninstalling a plugin **destroys** all datasets or snapshots that are associated with the plugin. Make sure to back up any important data stored in the plugin jail before deleting it!

### Backing up Jail Data

To find a jail’s stored data, go to **Storage > Pools** and expand the entry for the pool that was chosen to store plugin and jail data. Expand the **iocage** and **jails** datasets to find the plugin jail storage dataset.
One option to back up this stored data is to create a local replication. The replication task can even be configured to run periodically and automatically back up new changes to the jail dataset.

To convert a jail snapshot into a new storage dataset, go to Storage > Snapshots and find a snapshot of the jail dataset.

Expand the snapshot entry, click filter_none, and define the path and name of the new dataset to create from the snapshot. Then go to Storage > Pools, open the more_vert for the new dataset, and click Promote Dataset.

**Uninstalling a Plugin**

To remove a plugin, go to Plugins, expand the installed plugin entry, and click delete. Confirm the plugin removal by typing in the name of the plugin jail and setting Confirm.

Uninstalling can take a few moments while the plugin deletes from both Plugins and Jails. The plugin dataset also deletes from {POOL}/iocage/jails/ and any jail snapshots from Storage > Snapshots.
10.2.2 - Custom Plugins

- Requirements
  - Creating Each Component
  - Git Repository Initialization

Plugins are a technology for easily and securely deploying 3rd party applications directly on TrueNAS storage systems. The web interface allows users to deploy, start, stop, and update applications, along with configuration tasks such as assigning storage to them. Plugins are popular for content, security, development, collaboration, and backup applications for home and business use.

This feature is generally available in TrueNAS CORE and supported by the TrueNAS Community. iXsystems customers with TrueNAS Enterprise hardware and an iXsystems Support contract can contact Support about accessing these features.

### Plugin Technology

**Jails** form the core of TrueNAS plugins. Jails are the FreeBSD container technology and are:

- resource efficient
- secure
- flexible with networking infrastructure

Additionally, TrueNAS integrates the **iocage** application for its jail container management framework.

Each of the most popular TrueNAS plugins such as Plex Media Server, NextCloud, and SyncThing begin as FreeBSD ports: `multimedia/plexmediaserver/`, `deskutils/nextcloudclient/`, and `net/syncthing/` respectively. These install to a FreeBSD system using the **pkg** package manager. For example, FreeBSD uses `pkg install plexmediaserver` and then configures the application manually.

This tutorial guides you through creating a custom plugin using the **SABnzbd** newsreader plugin as an example. A plugin adds metadata that provides an installation source, reasonable defaults, and user interface elements such as an icon. The components for the **sabnzbd** plugin are:

- **README.md**: A popular convention for a file in markdown format for describing the project.
- **sabnzbd.json**: The JSON “Artifact” file containing various plugin properties including an inventory of all other metadata components which may be in the same or a remote repo.
- **overlay/**: An optional directory containing the files to be copied into the Jail.
- **ui.json**: A file containing the plugin management interface URL and port number.
- **settings.json**: An optional JSON file that contains variables used during plugin startup and for its configuration.
- **sabnzbd.png**: A .png image such as **sabnzbd.png** that will appear in the TrueNAS plugins Index. It is used as the icon.
- **post_install.sh**: A shell script ran after jail creation to perform necessary configuration steps. It runs only once.

### Requirements

TrueNAS provides everything necessary for custom plugin development, but a FreeBSD system is also a good choice. The requirements are:

- A TrueNAS or FreeBSD system running **iocage**.
- An internet connection and at least **1 GiB** of available disk space.
- A publicly-accessible **git** repository, self-hosted or on a service like **GitHub**, **Gitea** or **GitLab**. GitLab can be run as its own plugin.
- A text editor such as **vi**, **ee**, or **nano**, all of which are available in TrueNAS.
Basic knowledge of FreeBSD and shell scripting.

Creating Each Component

// and # comments are not supported in JSON. Copy any examples from the files in the Git repo using "raw" mode.

Artifact File

sabnzbd.json (artifact file)

```json
{
  "name": "sabnzbd", //The name of the Plugin and resulting Jail
  "plugin_schema": "2", //The Plugin schema version
  "release": "11.3-RELEASE", //FreeBSD version (not significantly newer than host)
  "artifact": "https://github.com/ConorBeh/iocage-plugin-sabnzbd.git", //The Git repo containing the Plugin
  "properties": { //Jail properties that can be overridden by the user
    "nat": 1,
    "nat_forwards": "tcp(8080:8080)"
  },
  "pkgs": [ //FreeBSD packages to be installed, one per line
    "sabnzbdplus",
  ],
  "packagesite": "https://pkg.FreeBSD.org/FreeBSD:11:amd64/latest", //The package site, latest, quarterly, or self-hosted
  "fingerprints": {
    "iocage-plugins": {
      "function": "sha256",
      "fingerprint": "b0170035af3acc5f3f3ae1859dc717101b4e6c1d0a794ad554928ca0cbb2f438" //The checksum of the FreeBSD port
    }
  },
  "revision": "0" //Internal version number
}
```

Artifact File Properties

These are commonly-used properties specified in the artifact file. Any supported iocage property can be specified. Here are a few:

- **nat**: Enables Network Address Translation to utilize the host's IP address.
- **nat_forwards**: Required when NAT is enabled. Syntax: `< protocol > (< jailport >:< hostport > )`
- **dhcp**: Enables DHCP on the jail to allow it to automatically obtain an IP address.
- **allow_tun**: Allows the creation of a tun network device inside the jail, required for VPN connections.
- **allow_raw_sockets**: Allows the jail to create raw sockets.

Artifact Repository Options

The official FreeBSD repository provides latest and quarterly branches. The latest branch contains binary packages that are updated immediately, while the quarterly branch binaries are only updated every quarter, and are the default for FreeBSD releases. The fingerprint remains the same for all official FreeBSD repositories. If custom port build options are required, the preferred solution is to set up a custom Poudriere build server.

- **overlay/**

- **overlay/**

The overlay/ is a directory of files copied into the jail after creation and before the execution of post_install.sh. The layout of these files follows the same paths as in the root jail filesystem. For example, a file placed in /overlay/usr/local/www/lighttpd/ inside the Git repo goes into /usr/local/www/lighttpd in the jail. This is very useful for providing pre-made configuration files, additional scripts, or even binaries that might not be available in the pkg repository.

- **ui.json**
ui.json

This is a small JSON file containing the address of the WebUI and port. Use the variable `%%IP%%` to automatically display the correct IP address. Make sure to include any extra components in the URL following the domain name or IP address, for example /admin or /web/index.

- settings.json

settings.json

A JSON file that is used when working with generated or user-specified data such as passwords or database names. These variables can be used in post_install.sh. In addition to these variables the `servicerestart` command must also be set. This command runs when a setting changes or the jail restarts, like a web server restart.

- sabnzbd.png (Icon File)

sabnzbd.png (Icon File)

A link to a .png file to show in the TrueNAS Plugins Index. The image requires a transparent background and must be 128 pixel by 128 pixel square in size to produce quality results when automatically resized.

- post_install.sh

post_install.sh

A POSIX shell script that leverages all other files to automate plugin installation. Simple plugins typically only have a few lines in this file, to enable and start a few services. Note that iocage executes the file contents simultaneously, not line by line. Remember to make the file executable before uploading it to the Git repository.

To make `post_install.sh` executable, enter `chmod +x post_install.sh`.

Common post-installation steps include:

- Setting file and directory permissions
- Moving, copying, and editing configuration files
- Generating random passwords
- Adding a user and/or group
- Creating a database

- /root/PLUGIN_INFO

/root/PLUGIN_INFO

A text file with easily accessible information which can be recalled again from the web interface by clicking Post Install Notes. Information can be entered into this file using `echo {information/notes} >> /root/PLUGIN_INFO` in `post_install.sh`, where `{information/notes}` is the relevant information about the plugin.

Git Repository Initialization

Create and initialize a Git repository and README for the plugin. Use this naming schema `iocage-plugin-{PLUGIN_NAME}`. For example, `iocage-plugin-sabnzbd` is the name of the Github repo in this example.

Put all the necessary files and directories in the newly created artifact repo. The necessary files are listed above. Next, open a pull request to the plugin hub index that adds the artifact file, icon, and entry into the INDEX file. Remember to put a link to your newly created artifact repo in the comments of the pull request. This way a moderator can fork your repo and it can be made available in the community list of plugins.
For guides on how to use Github, see Github Guides.
10.3 - Virtual Machines

10.3.1 - Basic Management

- Creating a Virtual Machine
  - Adding and Removing Devices
- Managing the Virtual Machine

This feature is generally available in TrueNAS CORE and supported by the TrueNAS Community. iXsystems customers with TrueNAS Enterprise hardware and an iXsystems Support contract can contact Support about accessing these features.

A Virtual Machine (VM) is an environment on a host computer that can be used as if it were a separate physical computer. VMs can be used to run multiple operating systems simultaneously on a single computer. Operating systems running inside a VM see emulated virtual hardware rather than the actual hardware of the host computer. This provides more isolation than Jails, but a VM will consume more system resources.

What system resources do VMs require? expand □

A portion of system RAM and a new zvol is assigned to each VM. While a VM is running, these resources are not available to the host computer or other VMs.

TrueNAS VMs use the bhyve virtual machine software. This type of virtualization requires an Intel processor with Extended Page Tables (EPT) or an AMD processor with Rapid Virtualization Indexing (RVI) or Nested Page Tables (NPT). VMs cannot be created unless the host system supports these features.

To verify that an Intel processor has the required features, open the Shell and run `grep VT-x /var/run/dmesg.boot`. If the EPT and UG features are shown, this processor can be used with bhyve.

To verify that an AMD processor has the required features, open the Shell and run `grep POPCNT /var/run/dmesg.boot`. If the output shows the POPCNT feature, this processor can be used with bhyve. Note that AMD K10 “Kuma” processors include POPCNT but do not support NRIS, which is required for use with bhyve. Production of these processors ceased in 2012-2013.

Creating a Virtual Machine

Before creating the virtual machine, you will need an installer .iso or image file for the operating system you intend to install and a storage pool available for both the virtual disk and operating system install file.

To create a new VM, go to Virtual Machines and click Add. Configure each category of the VM according to your specifications, starting with the Operating System.
### Specific Options

#### Operating System

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest Operating System</td>
<td>Choose the VM operating system type.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter an alphanumeric name for the virtual machine.</td>
</tr>
<tr>
<td>Description</td>
<td>Description (optional).</td>
</tr>
<tr>
<td>System Clock *</td>
<td>VM system time. Default is Local.</td>
</tr>
<tr>
<td>Boot Method</td>
<td>Select UEFI for newer operating systems or UEFI-CSM (Compatibility Support Mode) for older operating systems that only support BIOS booting. Grub is not recommended but can be used when the other options do not work.</td>
</tr>
<tr>
<td>Shutdown Timeout</td>
<td>The time in seconds the system waits for the VM to cleanly shut down. During system shutdown, the system initiates poweroff for the VM after the shutdown timeout has expired.</td>
</tr>
<tr>
<td>Start on Boot</td>
<td>Set to start this VM when the system boots.</td>
</tr>
<tr>
<td>Enable VNC</td>
<td>Enable a VNC (Virtual Network Computing) remote connection. Requires UEFI booting.</td>
</tr>
<tr>
<td>Delay VM Boot Until VNC Connects</td>
<td>Wait to start VM until VNC client connects.</td>
</tr>
<tr>
<td>Bind</td>
<td>VNC network interface IP address. The primary interface IP address is the default. A different interface IP address can be chosen.</td>
</tr>
</tbody>
</table>

#### CPU and Memory

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual CPUs</td>
<td>Number of virtual CPUs to allocate to the virtual machine. The maximum is 16, or fewer if the host CPU limits the maximum. The VM operating system might also have operational or licensing restrictions on the number of CPUs.</td>
</tr>
<tr>
<td>Cores</td>
<td>Specify the number of cores per virtual CPU socket. The product of vCPUs, cores, and threads must not exceed 16.</td>
</tr>
<tr>
<td>Threads</td>
<td>Specify the number of threads per core. The product of vCPUs, cores, and threads must not exceed 16.</td>
</tr>
</tbody>
</table>
Memory Size
Allocate RAM for the VM. Minimum value is 256 MiB. This field accepts human-readable input (Ex. 50 GiB, 500M, 2 TB). If units are not specified, the value defaults to bytes.

Disks

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new disk image</td>
<td>Select Create new disk image to create a new zvol on an existing dataset. This is used as a virtual hard drive for the VM. Select Use existing disk image to use an existing zvol or file for the VM.</td>
</tr>
<tr>
<td>Select Disk Type</td>
<td>Select desired disk type.</td>
</tr>
<tr>
<td>Zvol Location</td>
<td>Select a dataset for the new zvol.</td>
</tr>
<tr>
<td>Size</td>
<td>Allocate space for the new zvol. (Examples: 500 KiB, 500M, 2 TB) MiB. Units smaller than MiB are not allowed.</td>
</tr>
</tbody>
</table>

Network Interface

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter Type</td>
<td>Intel e82545 (e1000) emulates the same Intel Ethernet card. This provides compatibility with most operating systems. VirtIO provides better performance when the operating system installed in the VM supports VirtIO paravirtualized network drivers.</td>
</tr>
<tr>
<td>Mac Address</td>
<td>Enter the desired address into the field to override the randomized MAC address.</td>
</tr>
<tr>
<td>Attach NIC</td>
<td>Select the physical interface to associate with the VM.</td>
</tr>
</tbody>
</table>

Installation Media

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Installation Media Image</td>
<td>Browse to the operating system installer image file.</td>
</tr>
<tr>
<td>Upload an Installer Image File</td>
<td>Set to display image upload options.</td>
</tr>
</tbody>
</table>

Additional notes:

- The Grub Boot Method is not supported by Windows guest operating systems.
- Compare the recommended specifications for your guest operating system with the available host system resources when allocating Virtual CPUs, Cores, Threads, and Memory Size.
- Avoid allocating too much memory to a VM. Activating a VM that has all available memory allocated to it can slow the host system or prevent other VMs from starting.
- AHCI is the recommended Disk Type for Windows VMs.
- The VirtIO Network Interface requires that the chosen guest operating system support VirtIO paravirtualized network drivers.

Adding and Removing Devices

After the VM is created, add and remove virtual devices by expanding the VM entry in Virtual Machines and clicking device_hub.
Device notes:

- The virtual machine attempts to boot from devices according to the *Device Order*, starting with 1000, then ascending.
- *CD-ROM* devices allowing booting a VM from a CD-ROM image like an installation CD. The CD image must be available in the system storage.

**Managing the Virtual Machine**

After creating the VM and configuring any devices for it, manage the VM by expanding its entry in *Virtual Machines*.

Options for *settings_ethernet* or *keyboard_arrow_right* connections are available after activating the VM. If the VNC connection screen appears garbled, try adjusting the VNC device resolution.

Using the *State* toggle or clicking *Stop* follows a standard shut down procedure to cleanly shut down the running VM. Clicking *power_settings_new* immediately halts and deactivates the VM, similar to unplugging a computer.

If the VM you created has no Guest OS installed, the VM *State* toggle and *Stop* button might not function as expected. These buttons try to send an ACPI power down command to the VM operating system, but since no OS is installed, the commands time out. Use the *POWER OFF* button instead.
11 - Administration

11.1 - Interface Preferences

- General Preferences
- Custom Themes

There are a few adjustable interface preferences and a built-in theme editor for creating your own TrueNAS color schemes.

To access user preferences, click **settings > Preferences**. This page has options to adjust global settings in the web interface, manage custom themes, and create new themes.

**General Preferences**

There are a few options for how things are displayed or behave in the web interface:

- To choose a different pre-built or saved custom color scheme for the web interface, select an option from the **Choose Theme** dropdown.
- If screen space is limited, set **Prefer buttons with icons only** to only display icons and tooltips without text labels.
- When **Enable Password Toggle** is set, **visibility** appears next to password fields. Clicking this button will show characters typed or saved in the field.
- To clear any custom display choices for interface tables, set **Reset Table Columns to Default**.
- To display the legacy FreeNAS branding, set **Retro Logo**.
- **Reset All Preferences to Default** changes all these options back to their factory default settings.
Custom Themes

If a included theme doesn’t satisfy your preference, a fully custom theme can be created. To start creating a custom theme, click CREATE NEW THEME.

Colors from an existing theme can be used when creating a new custom theme. Select a theme from the Load Colors from Theme dropdown to use the colors from that theme for the new custom theme:

- **Custom Theme Name**: Enter a name to identify the new theme.
- **Menu Label**: Enter a short name to use in the TrueNAS web interface menus.
- **Description**: Enter a short description of the new theme.
- **Choose Primary**: Choose from either a generic color or import a specific color setting to use as the primary theme color. The primary color changes the color of many of the buttons.
- **Choose Accent**: Choose from either a generic color or import a specific color setting to use as the accent color for the theme. This color is used for many of the buttons and smaller elements in the web interface.
- **Choose Topbar**: Changes the color of the top menu bar in the web interface.

For even more fine tuning, click the COLORS tab. Here, colors can be changed using the slider or by entering hexadecimal values.

When complete, click SUBMIT. TrueNAS automatically switches to newly created theme and adds it to the Choose Theme dropdown.
11.2 - Task Manager

The task manager shows a list of tasks performed by the TrueNAS system starting with the most recent. Click a task name to display its start time, progress, finish time, and whether the task succeeded. If a task fails, the error status shows.

Tasks with log file output have a View Logs button to show the log files.

The task manager is opened by clicking assignment. Close the task manager by clicking CLOSE, clicking anywhere outside the task manager dialog, or by pressing Esc.
11.3 - Alert Notifications

The alert system provides a visual warning when system conditions require administrative attention. The alert icon in the upper right corner has a notification badge that displays the total number of unread alerts.

Alert icons indicate notification, warning, critical, and one-shot critical alerts. Critical messages are also emailed to the root account. One-shot critical alerts must be dismissed by the user.

<table>
<thead>
<tr>
<th>Alert Level</th>
<th>Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification</td>
<td>□</td>
</tr>
<tr>
<td>Warning</td>
<td>□</td>
</tr>
<tr>
<td>Critical</td>
<td>□</td>
</tr>
<tr>
<td>One-shot Critical</td>
<td>□</td>
</tr>
</tbody>
</table>
11.4 - Statistics Reporting

Reporting General Settings

TrueNAS has a built in reporting engine that gives helpful graphs and information about the system. TrueNAS uses Graphite for metric gathering and visualizations. Some general settings can be found in System > Reporting.

When Report CPU usage in percent is set, it simply reports the CPU usage in percent rather than units of kernel time. When Graphite Separate Instances is set, it sends the plugin instance and type instance to Graphite as separate path components: host.cpu.0.cpu.idle. When it is not set, the plugin and plugin instance as one path component and type and type instance as another component: host.cpu-0.cpu-idle.

A Remote Graphite Server Hostname can be typed in the respective field. The Graph Age in Months field is used to set the maximum number of months a graph is stored. The Number of Graph Points field is used to set the number of points for each hourly, daily, weekly, monthly, or yearly graph.

Report history is cleared when CPU reporting, Graph Age, or Graph Points are changed.

Graphs

TrueNAS uses collectd to provide reporting statistics. A comprehensive list of graphs and reporting are found in Reporting. Change the category of reporting by selecting an option of the drop-down. Graphs can be interacted with by clicking and dragging on a certain range, or by clicking ⬇️, ⬇️, ⬇️, ⬇️.

Below is a summary of what each page of graphs displays:

CPU

CPU shows the amount of time spent by the CPU in various states such as executing user code, executing system code, and being idle. Graphs of short-, mid-, and long-term load are shown, along with CPU temperature graphs.
Disk

Disk shows read and write statistics on I/O, percent busy, latency, operations per second, pending I/O requests, and disk temperature. Choose the DEVICES and METRICS to view the selected metrics for the chosen devices.

Temperature monitoring for the disk is disabled if HDD Standby is enabled on the disk.

The default view shows a temperature graph of the first disk. To see the temperature graphs of more disks, select them from the DEVICES drop-down. To view other metrics such as Disk I/O and Disk Latency, select them from the METRICS drop-down.

Memory

Memory displays memory usage. Swap displays the amount of free and used swap space.
○ **Network**

**Network** shows received and transmitted traffic in megabytes per second for each configured interface.

○ **NFS**

**NFS** shows information about the number of procedure calls for each procedure and whether the system is a server or client.
Partition displays free, used, and reserved space for each pool and dataset. However, the disk space used by an individual zvol is not displayed as it is a block device.

System displays the number of processes. It is grouped by state.

Target shows bandwidth statistics for iSCSI ports.
UPS displays statistics about an uninterruptible power supply (UPS) using Network UPS tools. Statistics include voltages, currents, power, frequencies, load, and temperatures.

ZFS shows compressed physical ARC size, hit ratio, demand data, demand metadata, and prefetch data.
Reporting data is saved to permit viewing and monitoring usage trends over time. This data is preserved across system upgrades and restarts.

Data files are saved in `/var/db/collectd/rrd/`.

Reporting data is frequently written and should not be stored on the boot pool or operating system.
device.
11.5 - Shell

The web interface has a web shell that makes it convenient to run command line tools from the web browser as the root user.

The prompt shows that the current user is **root**, the hostname is **freenas**, and the current working directory is ~, the home directory of the logged-in user.

The default shell for a new installations is **zsh**.

**How do I change the default shell? expand □**

The default shell can be changed in **Accounts > Users**. Click **more_vert** and **Edit** for the root user.
Choose the desired shell from the Shell drop-down and click SAVE.

The Set font size slider adjusts the size of text displayed in the Shell. Click RESTORE DEFAULT to reset the shell font and size.

Shell command history is available for the current session. Use the Up and Down arrow keys to scroll through previously entered commands. Edit the command if desired, then press Enter to re-enter the command. Navigating away from the Shell screen clears the command history.

Home, End, and Delete keys are supported. Tab completion is also available. Type a few letters and press Tab to complete a command name or filename in the current directory. Right-clicking in the terminal window displays a reminder about using Command+c and Command+v or Ctrl+Insert and Shift+Insert for copy and paste operations in the shell.
Entering `exit` leaves the session. Click **Reconnect** to start a new session.

Clicking other web interface menus closes the shell session and stops commands running in the shell. **tmux** provides the ability to detach shell sessions and then reattach to them later. Commands continue to run in a detached session.

Not all shell features render correctly in Chrome. Firefox is the recommended browser when using the shell.

Most FreeBSD command line utilities are available in the Shell, including additional troubleshooting applications for TrueNAS Core and Enterprise.
For TrueNAS SCALE, most Linux command line utilities are available in the shell.
12 - Solutions

This topic covers the various third party solutions that TrueNAS can integrate with or be optimized for.

Ready to get started? Choose a topic or article from the left-side Navigation pane. Click the < symbol to expand the menu to show the topics under this section.

12.1 - Optimizations

The optimizations topic has articles discussing how best to configure TrueNAS for various use cases or specific needs. This includes Disaster Recovery configurations, Media and Entertainment tuning, and Security best practices.

Ready to get started? Choose a topic or article from the left-side Navigation pane. Click the < symbol to expand the menu to show the topics under this section.
TrueNAS supports many different disaster recovery (DR) scenarios! Some of these scenarios with recovery processes are listed here.

- **Replication**

**Point-in-Time Recovery – ZFS Replication**

Of the native ways to replicate data, ZFS replication is the most efficient and reliable method for asynchronously replicating data from one TrueNAS system to another. Replication is based on snapshots of datasets or zvols and synchronizes the snapshots of the first system to the second system. There are numerous advantages to using ZFS replication. One of those is that a snapshot is a point-in-time, read-only copy of the data. This ensures that the contents of the snapshot cannot be altered.

ZFS replication is commonly used for disaster recovery. Should the first system or site go down, the remote system can be brought back by cloning the snapshot to a new dataset and restoring the share. This recovery does require some work on the side of the admin, but it’s incredibly quick and ensures that whatever was transferred is retained. Snapshots and replications can be scheduled to run every few minutes.
Another benefit of ZFS replication is the capability for the snapshots and referenced data to be stored on systems and pools of different specs or pool configuration. All-flash, high-performance pools can be backed up to lower performance pools with traditional drives and different RAID configurations. Smaller systems can also be backed up to larger central repositories. Companies such as FirstLink and others use this to help clone edge devices like the TrueNAS Mini systems to a central core TrueNAS in their data center. ZFS replication on TrueNAS ensures data protection regardless of system complexity, size, or location.

- **Rsync**

**File-based Recovery – Rsync**

Rsync is a file-level migration that’s the same as rsync in the Linux/FreeBSD command line. It’s handy for semi-live sync of data if you need just the same files between sites each shared over a local share.

Rsync is useful for file transfer, but it’s not recommended if files are being modified. For example, if an rsync task starts while 100 GB is being written and the data is changed before the file is written, it will cause issues with versioning and data integrity. Rsync should never be used to copy active VM data stores, block-level data (iSCSI or fibre channel shares), or other data that could constantly be in use. Rsync is slower than ZFS replication, particularly for large datasets, so it’s recommended for convenience over data integrity. It can be used between TrueNAS and many other systems.

- **Cloud Sync**

**File Recovery To or From the Cloud – Cloud Sync**

TrueNAS can copy, pull, and sync data to a variety of cloud-based data storage systems, including Amazon AWS, Microsoft Azure, Google GCP, Google Drive, Backblaze B2, Dropbox, Box, and more. By integrating rclone sync for file transfers, this feature can copy files on TrueNAS into a cloud repository of a user’s choosing.
For larger datasets, TrueNAS systems are more cost-effective long term than cloud offerings, including Amazon AWS. For this reason, using TrueNAS as a backup target for protecting cloud-based data, e.g., from AWS, Dropbox, or Google Drive, is ideal because data stored in TrueNAS will get scrubbed, checked, and retained with an unlimited number of snapshots available.

**Site-to-Site Failover**

**Automatic Site-to-Site failover – DNS, Load-Balancing, Proprietary Tools**

Automatic failover between sites is beyond the scope of TrueNAS systems alone. TrueNAS is a storage system, and while it handles data replication well in a variety of ways, automatic failover to a remote site requires knowledge of the services themselves. For environments with web or video streaming services, [DNS round-robin(https://en.wikipedia.org/wiki/Round-robin_DNS)](https://en.wikipedia.org/wiki/Round-robin_DNS) with failover might be feasible. Several web servers, like [NGINX](https://www.nginx.com), also feature load-balancing services which could help mitigate service overload or downtime. TrueNAS systems provide a stable backend in this topology, with the option of also running ZFS replication for additional safety. Contact [ixsystems](https://ixsystems.com) if you need assistance with designing a storage system for your business.

An example design:
TrueNAS is a storage platform with powerful ways to ensure data integrity and consistency between local and remote sites. ZFS replication is the fastest and best way to ensure the data transferred is intact. Rsync is useful for file sync but cannot be used for live data or block-level data that could change during transfer. Cloud sync supports user workloads that archive to or from mainstream cloud providers. Beyond these tools, TrueNAS works with other systems, such as Asigra Backup and iconik smart media management, to provide an ultra-scalable backend with robust performance and a strong emphasis on data protection. The tools that TrueNAS provides combined with the flexibility to work with nearly any IT environment make it a robust system for cross-site and DR workloads.
12.1.2 - Media Workflows

- General Optimizations
- Software-specific Tuning

Developing and delivering media content that reaches audiences whenever and wherever they are has increased in importance and complexity. In today’s highly connected, entertainment-driven world, media and entertainment (M&E) companies need to stay competitive to succeed. These organizations need to produce information and entertainment in a variety of different formats to display on mobile devices, desktops, workstations, Blu-ray players, game consoles, set-top boxes, and TVs as well as in digital and analog movie theaters. Workflows grow in complexity daily and time-to-market windows continue to shrink. Where and how to store and archive all this content remains top-of-mind. M&E projects run on multiple heterogeneous environments, need an enterprise-grade storage array’s features, and require multiple protocols.

Most M&E production houses purchase data storage based on capacity and performance dictated by the needs of existing applications. As a result, businesses often end up with multiple classes of application-specific storage or storage silos including SAN, NAS, all-flash arrays, and many forms of direct attached storage (DAS) from a multitude of vendors.

Creative organizations are often forced to over-provision and over-purchase capacity or performance, or use an all-flash array to meet their production needs. This reactive purchasing drives up the cost of media production. As media files grow, it becomes complex to manage and inefficient to increase the capacity or performance of DAS or consumer-grade NAS, so many turn to cloud storage. The security risk and expense of cloud storage are a top priority of IT and Media Managers. These factors and others put intense pressure on your budget and data storage infrastructure to keep up with the demand.

A TrueNAS storage system from iXsystems brings an enterprise-grade storage solution supporting multiple protocols to M&E production houses that is capable and affordable for many M&E applications. It is designed to enable M&E customers to address media capacity and performance requirements while reducing total cost of ownership (TCO), consolidating digital assets, accelerating media workflows, and providing the features needed to protect all media assets. Read more to learn how TrueNAS can be optimized for typical M&E production house usage.

General tuning recommendations are changing constantly! Check back often to see what’s changed or add your own recommendations!

General Optimizations

- Use SMB3 sharing on both the TrueNAS and any client systems.
- A typical recommendation is to use Mixed RAID (2+1 RAIDZ) in most cases with added Read and Write cache. The Write cache is optional if the system is only using SMB sharing.

**What about RAIDZ2 Configurations?**
6 or 7 disk wide RAIDZ2 (Protection-X or Protection) is possible for tier2, nearline, or archival storage. It also works when the system has extensive data storage of a few hundred Terabytes or more.

- Setting jumbo frames (MTU: 9000) on the network, TrueNAS, and client side is important for large file streams.
- Do not store Media Cache Files and Media Cache Databases on a NAS. These files must stay local on clients. Ideally, client systems use SSDs and NVMe devices to store these files.
- With standard (non flash) systems, don’t move or copy files or footage while editing. This causes choppy playback.

Software-specific Tuning
Beyond general optimization for Media and Entertainment workflows are tunings or TrueNAS usage recommendations for specific applications.

Adobe Premiere®

System size is a primary factor when tuning TrueNAS for Adobe Premiere workflows.

4K workflows typically want 20 disks or more. 8K can be all-flash demanding, but Premiere has the proxies feature to reduce the performance impact. Make sure your client systems or other applications support this feature too.

To get some performance improvement when scrubbing through long video files with audio tracks, de-select play audio while scrubbing under Preferences > Audio

Shared projects must enable Project Locking in Premiere.
12.1.3 - Security Recommendations

When using services on TrueNAS, especially services that allow outside connections, there are some best practices to follow to ensure your system is safe and secure. Several different system services are discussed in this article.

- **iSCSI**

Follow the iSCSI creation wizard unless a specific configuration is required. To create an iSCSI share, go to **Sharing > Block Shares (iSCSI)** and click **WIZARD**. The iSCSI wizard has several additional security settings.

[iSCSI Share Creation](#) walks through share creation steps.

When creating a new **Portal**, consider adding a **Discovery Authentication Method**. This adds authentication between the initiator and the extent based on the chosen authentication method.

Entering a list of **Initiators** and **Authorized Networks** is also recommended. This allows defining which systems or networks can connect to the extent. When these options are empty, all initiators and all networks are allowed to connect to the extent.

- **NFS**

Network File System (NFS) is a sharing protocol that allows outside users to connect and view or modify shared data.

To create a share, see [NFS Share Creation](#).

NFS service settings are in **Services** after clicking the **Services** button. By default, all options are unset. Unless needed for a specific use case, keep the default NFS service settings.

During **Share Creation**, define which systems are authorized for share connections. Leaving the **Authorized Networks** or **Authorized Hosts and IP addresses** lists empty allows any system to connect to the NFS share. To define which systems can connect to the share, click the **Advanced Options** and enter all networks, hosts, and IP addresses to have share access. All other systems are denied access.

- **SMB**

Using Server Message Block (SMB) to share data is a very common situation for TrueNAS users. However, it allows outside connections to the system and must be properly used to avoid security concerns.

To create a new SMB share, see [SMB Share Creation](#).

SMB service settings are in **Services** after clicking the **Services** button.

**Do not use SMB1.**

Do not use **NTLMv1 Auth** with an untrusted network. This encryption option is insecure and vulnerable.

When using MacOS to connect to the SMB share, enable **Apple SMB2/3 Protocol Extensions**. This improves connection stability between the share and the Apple system.

If you need to add an **Administrators Group**, make sure the group members are correct. Members of the administration group have full permissions to modify or delete the share data.

During **Share Creation**, a **Purpose** can be selected. This changes the share configuration with one click. For example, when selecting **Private SMB Datasets and Shares** from the list, TrueNAS automatically tunes some settings so the share is set up for private use. To fully customize the share settings, select **No presets** for the **Purpose**. Unless a specific purpose for the share is required, it is recommended to select **Default share parameters** as the **Purpose**.
SMB Server Signing is recommended. To enable Server Signing, go to Services > SMB > Edit > Auxiliary Parameters and add this string to the Auxiliary Parameters field:

server signing = mandatory

Then save, stop, and restart the SMB service.

Ο SSH

Using Secure Shell (SSH) to connect to your TrueNAS is very helpful when issuing commands through the CLI. SSH settings are in Services after clicking the .

To make sure users cannot connect to the system as root and potentially harm the system, leave Log in as Root with Password unset. It is off by default.

Unless it is required, do not set Allow TCP Port Forwarding.

Many SSH ciphers are outdated and vulnerable. It is not safe to enable any weak SSH ciphers. Block both the CBC and Arcfour ciphers by going to Services > SSH > Edit > Advanced Options and adding this line in the Auxiliary Parameters:

Ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
12.2 - Integrations

Integrations discusses how TrueNAS can work with different third-party applications to create unique or efficient storage management environments.

Ready to get started? Choose a topic or article from the left-side Navigation pane. Click the < symbol to expand the menu to show the topics under this section.

12.2.1 - AWS Images

- Process Summary
  - Using Virtualized TrueNAS with Amazon Web Services (AWS)
    - Create TrueNAS Image
    - Upload TrueNAS Image to EC2
    - Accessing TrueNAS with the AMI
  - TrueNAS Community AMI

Process Summary

- Requirements
  - FreeBSD system
  - AWS Account
  - S3 Bucket
  - User with permissions for EC2
    - Download the user key to the local working directory and modify
    - Install bhyve and bsdec2-image-upload
    - Patch bsdec2-image-upload if needed
  - Create TrueNAS image file
    - Download TrueNAS .iso
    - Create blank image file
    - Load virtualization module
    - Create tap and bridge interface
    - Load image and iso into bhyve
    - Install TrueNAS
  - Upload image to EC2
    - Description and region name are required
  - Launch EC2 instance
    - Select name created with image
    - t2.large is the recommended instance type
    - Add HDD/SSD volumes as needed
    - Step 6: add new rule
      - Type: http
    - Launch the instance
  - Wait for AWS to finish status checks
  - Paste Public DNS or Public IP link in browser to access TrueNAS web interface

Using Virtualized TrueNAS with Amazon Web Services (AWS)

These instructions demonstrate how to create a virtualized TrueNAS image on FreeBSD, configure it with Amazon Elastic Compute Cloud (EC2), and access the TrueNAS web interface. There are a few things that must be prepared before building the image. The FreeBSD system needs two applications to create, configure, and upload the virtual machine image: bhyve and bsdec2-image-upload. The most recent version (>=1.3.1) of bsdec2-image-upload is required, otherwise an SSL error occurs when attempting to upload the image. If not available on the ports tree, the utility can be downloaded from the GitHub repository.
Currently, \textit{bsdec2-image-upload} fails on images that aren't 10GB. An issue has been created, but in the meantime a workaround is to edit main.c and replace:

"BlockDeviceMapping.1.Ebs.VolumeSize=10&"

with

"BlockDeviceMapping.1.Ebs.VolumeSize=16&"

To build, use a FreeBSD system with either \texttt{libressl-devel} or \texttt{openssl-devel}, as well as \texttt{ca_root_nss}, and run \texttt{make install}.

Create an \texttt{AWS account} with an \texttt{S3 bucket}. Record the region associated with the S3 bucket. Set the bucket lifetime policy to delete data after 1 day, as \textit{bsdec2-image-upload} does not delete files from S3 and the files are no longer needed after the AMI is registered. A \texttt{user with permissions to EC2 and S3} is must have these permissions:

\begin{itemize}
  \item \texttt{s3:PutObject}
  \item \texttt{s3:GetObject}
  \item \texttt{ec2:RegisterImage}
  \item \texttt{ec2:DescribeImages}
  \item \texttt{s3:DeleteObject}
  \item \texttt{ec2:ImportVolume}
  \item \texttt{ec2:DescribeConversionTasks}
  \item \texttt{ec2:CreateSnapshot}
  \item \texttt{ec2:DescribeSnapshots}
  \item \texttt{ec2:DescribeRegions}
  \item \texttt{ec2:CopyImage}
  \item \texttt{ec2:ModifyImageAttribute}
\end{itemize}

Alternatively, give full access to S3 and EC2.

After creating the IAM user, download an \texttt{Access Key} to the working directory on the FreeBSD system. The file has these lines:

\begin{verbatim}
Access key ID,Secret access key
{ACCESS_KEY},{SECRET}
\end{verbatim}

Open a new file called \texttt{KEY.pem} and copy the information contained in the csv file:

\begin{verbatim}
ACCESS_KEY_ID={ACCESS_KEY}
ACCESS_KEY_SECRET={SECRET}
\end{verbatim}

Create TrueNAS Image

When all the prerequisites are ready, download a TrueNAS 11.2 or later \texttt{.iso file}. Open a shell and go to your local working directory. Create an empty raw image file with \texttt{truncate -s 16G \{TRUENAS\}.img}.

Replace \{\texttt{TRUENAS}\} with a image file name. This empty image is the installation target for the TrueNAS .iso.

Next, load the virtualization module and create a tap and bridge interface:

\begin{verbatim}
kldload -n vmm
ifconfig tap0 create
sysctl net.link.tap.up_on_open=1
ifconfig bridge0 create
ifconfig bridge0 addm re0 addm tap0
ifconfig bridge0 up
\end{verbatim}

Use \texttt{bhyveload -m 4GB -d truenas.img vm0} to load the image into the hypervisor and create virtual machine \texttt{vm0} with four gigabytes of memory.

To install TrueNAS into the image, load both the image and TrueNAS .iso file into \texttt{bhyve}: \texttt{bhyve -c 2 -m 4G -H -A -P -g 0 -s 0,hostbridge -s 1,lp

\texttt{c} -s 2,virtio-net,tap0 -s 3,virtio-blk,\{TRUENAS\}.img -s 31,ahci-cd,\{TRUENAS-VERSION\}.iso -l com1,stdio vm0}. Replace \{\texttt{TRUENAS}\} with the name of the image file and \{\texttt{TRUENAS-VERSION}\} with the TrueNAS .iso file name.

The commands failed? expand □

If these commands fail, for instance an error concerning boot.lua, then try this command which uses a
combines the two previous commands in a shell script included in the bhyve installation.

```
sh /usr/share/examples/bhyve/vmrun.sh -c 2 -m 4GB -t tap0 -d {TRUENAS}.img -i -I {TRUENAS-VERSION}.iso vm0
```

When the TrueNAS installer opens, make sure boot with BIOS is chosen and start the installation. Power off the device when the installation is done.

**Why can't I just reboot? expand □**

Do not load the completed image into bhyve and boot after installation as TrueNAS will create invalid network settings. If network issues occur, boot the image and create a DHCP interface manually named xn0.

**Upload TrueNAS Image to EC2**

Now that the image is created and configured, upload it to EC2. Use `bsdec2-image-upload` with the image file:

```
bsdec2-image-upload --public {TRUENAS}.img TrueNAS {description} {region} {S3 bucket} KEY.pem. Replace {TRUENAS} with the image file name, {description} with a unique identifier for the Amazon Machine Image (AMI), {region} with your Amazon region, and {S3 bucket} with your AWS image storage location. KEY.pem is the IAM user access key that was downloaded earlier. These elements are required for the upload to start.
```

`bsdec2-image-upload` sends the image to the AWS bucket in 10 MiB segments. The upload can take several hours, depending on connection speeds and other factors.

When the S3 bucket upload completes, the script creates a snapshot, registers the AMI, and copies the AMI to all regions for mirrors.

**The upload command failed? expand □**

The upload command can fail for various reasons. For example, entering a description that already exists. If this happens, fix the error and rerun the command. When successful, the upload simply finishes.

**Accessing TrueNAS with the AMI**

With the Amazon Machine Image (AMI) created and uploaded to AWS, an EC2 instance needs to be activated before the TrueNAS interface is accessible. Log in to your Amazon Web Services account and click the EC2 Compute service.

Find the **Launch instance** section, open the **Launch instance** drop down, and click **Launch instance**.
The instance launcher follows several steps:

1. Click My AMIs and select the name that was uploaded by bsdec2-image-upload.
2. Any instance will work, but t2.large is recommended for TrueNAS given an 8GB memory recommendation.
3. Skip this step.
4. Add EBS volumes according to your TrueNAS use case. At minimum, add a couple of cold HDD volumes for a storage pool. General purpose SSD volumes can be used as L2ARC or SLOG devices.
5. Skip this step.
6. Add a rule with http. This allows you to connect to the TrueNAS web interface.

The running instance is added to the EC2 dashboard or can be seen in the Instances menu. When the image has fully started, AWS performs two status checks. The first checks for AWS up-time, and the second verifies the instance is functional. After both checks pass, paste either the Public IP or Public DNS link in a new browser window to connect to the TrueNAS web interface.

TrueNAS Community AMI

Starting with 12.0-BETA, an AMI is provided for different TrueNAS releases and is available in the Community AMI section. When using this AMI, login with the default credentials:

Username: root Password: abcd1234

To secure the system, change the password after the initial login.
12.2.2 - Asigra Plugin

Asigra provides a TrueNAS plugin to simplify cloud storage backups with their service. The Asigra plugin connects TrueNAS to a third party service and is subject to licensing. TrueNAS must have a public static IP address for Asigra services to function. Please read the Asigra Software License Agreement before using this plugin.

Follow the instructions in the Plugins section to install the Asigra Plugin. To begin using Asigra services after installing the plugin, expand the plugin options and click Register. A new browser tab opens to register a user with Asigra.

Refer to the Asigra documentation for details about using the Asigra platform:

- **DS-Operator Management Guide**: Using the DS-Operator interface to manage the plugin DS-System service. Click Management in the plugin options to open the DS-Operator interface.
- **DS-Client Installation Guide**: How to install the DS-Client system. DS-Client aggregates backup content from endpoints and transmits it to the DS-System service.
- **DS-Client Management Guide**: Managing the DS-Client system after it has been successfully installed at one or more locations.
12.2.3 - Containers

- **Features**
- **Installation**
  - Prepare TrueNAS for a Container Solution
    - Create Pools
    - Set up SSH
    - Set up NFS
    - Set up iSCSI
  - Prepare the Nodes
  - Deploy Your Orchestrator Into the Cluster
- **Additional Resources**

TrueNAS CORE & Enterprise can both be used as backing storage for container workloads.

The democratic-csi driver (available at [https://github.com/democratic-csi/democratic-csi](https://github.com/democratic-csi/democratic-csi)) allows users to integrate popular container solutions like Kubernetes, Nomad, Cloud Foundry, or Mesos into the TrueNAS CLI. The driver is sponsored by and officially supported by iXsystems for TrueNAS Enterprise Customers.

A CSI (Container Storage Interface) is an interface between container workloads and third-party storage that supports creating and configuring persistent storage external to the orchestrator, its input/output (I/O), and its advanced functionality such as snapshots and cloning.

The democratic-csi focuses on providing storage using iSCSI, NFS, and SMB protocols, and includes several ZFS features like snapshots, cloning, and resizing.

**Features**

- dynamically provisions/de-provision storage and shares it as appropriate for cluster usage
- online resize operations to dynamically expand volumes as needed
- snapshot support (using either `zfs send/receive` or `zfs snapshot`)
- cross-architecture (amd64, armv7, arm64)

**Installation**

There are 3 steps to integrating a container solution in TrueNAS:

1. Prepare TrueNAS.
2. Prepare the nodes (ie: your Kubernetes cluster nodes).
3. Deploy your container orchestrator.

**Prepare TrueNAS for a Container Solution**

We recommend using TrueNAS 12.0-U2.1+. However, the driver typically works with previous versions too, but is unsupported. Before you start, log in to TrueNAS, go to Services, and make sure iSCSI, NFS, and SSH are enabled.

**Create Pools**

Go to Storage > Pools and create the pools to include in your container.

**Set up SSH**

Now you need to ensure that a supported shell is used by the user account that your container solution can use to SSH to TrueNAS. Go to Accounts > Users and set the desired user’s Shell to either bash or
To use a non-root user for the SSH operations, you can create a `csi` user and then run `visudo` directly from the console. Make sure the line for the `csi` user has `NOPASSWD` added (this can get reset by TrueNAS if you alter the user in the GUI later):

```
csi ALL=(ALL) NOPASSWD:ALL
```

With TrueNAS CORE version 12.0+, you can use an `apiKey` instead of the `root` password for the HTTP connection.

### Set up NFS

1. Go to Services and click the icon next to NFS to edit its properties.
2. Make sure Enable NFSv4, NFSv3 ownership model for NFSv4, and Allow non-root mount are checked, then click SAVE.

### Set up iSCSI

1. Go to Sharing > Block Shares (iSCSI).
2. Use the default settings in the Target Global Configuration tab.
3. In the Portals tab, click ADD, then create a *Description*. Set the IP Address to 0.0.0.0 and the Port to 3260, then click SUBMIT.
4. In the Initiators Groups tab, click ADD. For ease of use, check the Allow ALL Initiators, then click SAVE. You can make restrictions later using the Allowed Initiators (IQN) function.
5. Kubernetes will create Targets and Extents automatically.

When using the TrueNAS API concurrently, the `/etc/ctl.conf` file on the server can become invalid. There are sample scripts in the `contrib` directory to clean things up, i.e., copy the script to the server and directly and run `-./ctld-config-watchdog-db.sh | logger -t ctld-config-watchdog-db.sh &`. Please read the scripts and set the variables as appropriate for your server.

- Ensure you have preemptively created portals, initiator groups, and authorizations
  - Make note of the respective IDs (the true ID may not reflect what is visible in the UI)
  - You can make ID’s visible by clicking the Edit link and finding the ID in the browser address bar
  - Alternately, use these commands to retrieve appropriate IDs:
    - `curl --header "Accept: application/json" --user root:<password> 'http(s)://<ip>/api/v2.0/iscsi/portal'
    - `curl --header "Accept: application/json" --user root:<password> 'http(s)://<ip>/api/v2.0/iscsi/initiator'
    - `curl --header "Accept: application/json" --user root:<password> 'http(s)://<ip>/api/v2.0/iscsi/auth`

---

### Prepare the Nodes

Install and configure the requirements for both NFS and iSCSI.

- **NFS**

  **RHEL / CentOS**

  `sudo yum install -y nfs-utils`
Ubuntu / Debian

```
sudo apt-get install -y nfs-common
```

---

### iSCSI

**Multipath is supported for the iscsi-based drivers. Configure multipath with multiple portals in the configuration as needed.**

If you are running Kubernetes with rancher/rke, please see https://github.com/rancher/rke/issues/1846.

---

RHEL / CentOS

Install these system packages:

```
sudo yum install -y lsscsi iscsi-initiator-utils sg3_utils device-mapper-multipath
```

Enable multipathing:

```
sudo mpathconf --enable --with_multipathd y
```

Ensure that **iscsid** and **multipathd** are running:

```
sudo systemctl enable iscsid multipathd
sudo systemctl start iscsid multipathd
```

Start and enable iSCSI:

```
sudo systemctl enable iscsi
sudo systemctl start iscsi
```

---

Ubuntu / Debian

Install these system packages:

```
sudo apt-get install -y open-iscsi lsscsi sg3-utils multipath-tools scsitools
```

Enable multipathing:

```
sudo tee /etc/multipath.conf <<-'EOF'
defaults {
  user_friendly_names yes
  find_multipaths yes
}
EOF
```

```
sudo systemctl enable multipath-tools.service
sudo service multipath-tools restart
```

Ensure that **open-iscsi** and **multipath-tools** are enabled and running:

```
sudo systemctl status multipath-tools
sudo systemctl enable open-iscsi.service
sudo service open-iscsi start
```

---

### SMB

---

SMB
When using Windows based machines, you might need to enable guest access, even if you are connecting with credentials.

```powershell
Set-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters
AllowInsecureGuestAuth -Value 1
Restart-Service LanmanWorkstation -Force
```

**Deploy Your Orchestrator Into the Cluster**

- **Kubernetes**

**Kubernetes** is “an open-source system for automating deployment, scaling, and management of containerized applications.”

**Deploy the Driver (Helm Installation)**

```
helm repo add democratic-csi https://democratic-csi.github.io/charts/
helm repo update

# helm v2
helm search democratic-csi/

# helm v3
helm search repo democratic-csi/

# copy proper values file from https://github.com/democratic-csi/charts/tree/master/stable/democratic-csi/examples
# edit as appropriate
# examples are from helm v2, alter as appropriate for v3

# add --create-namespace for helm v3
helm upgrade
--install
--values freenas-iscsi.yaml
--namespace democratic-csi
helm upgrade
--install
--values freenas-nfs.yaml
--namespace democratic-csi
```

**Non-standard Kubelet Paths**

When using a distribution with a non-standard kubelet path (such as minikube and microk8s), a new kubelet host path is required. Example:

```
microk8s helm upgrade
--install
--values freenas-nfs.yaml
--set node.kubeletHostPath="/var/snap/microk8s/common/var/lib/kubelet"
```

**Multiple Deployments**

You can install multiple deployments of each or any driver. You will need:

- a new helm release name for each deployment
- a unique `csiDriver.name` in the values file
- a unique name for each storage class (per cluster)
- a unique parent dataset (don’t try to use the same parent across deployments or clusters)

**Snapshot Support**

Install beta (v1.17+) CRDs (once per cluster):

```
https://github.com/kubernetes-csi/external-snapshotter/tree/master/client/config/crd
```
Install snapshot controller (once per cluster):


# replace namespace references to your liking

kubectl apply -f rbac-snapshot-controller.yaml
kubectl apply -f setup-snapshot-controller.yaml

Install democratic-csi as usual with volumeSnapshotClasses defined as appropriate.


**Openshift expand □**

*Openshift* is another addon to Kubernetes and generally works fine with the democratic-csi. You will need to set special parameters with helm (support added in chart version 0.6.1):

# for sure required
--set node.rbac.openshift.privileged=true
--set node.driver.localtimeHostPath=false

unlikely, but in special circumstances may be required

- set controller.rbac.openshift.privileged=true

You can run the `kubectl get pods -n democratic-csi -o wide` command to make sure all the democratic-csi pods are running.

You can also run the `kubectl get sc` command to make sure your storage classes are present and set a default class.

Visit the *Kubectl Cheat Sheet* or this *Kubernetes CSI guide* for more Kubernetes deployment and configuration information.

- Nomad

**Nomad**

Nomad is a “simple and flexible workload orchestrator to deploy and manage containers and non-containerized applications across on-prem and clouds at scale.”

The democratic-csi works in Nomad with limited functionality and has to be deployed as a set of jobs. The
controller job runs as a single instance, and the node job runs on every node and manages mounting the volume.

Read the Nomad Support page in the democratic-csi GitHub for detailed setup instructions. Visit the Nomad Storage Plugins page to learn how Nomad manages dynamic storage plugins.

- **Mesos**

**Mesos**

Mesos is an open source cluster manager that abstracts CPU, memory, storage, and other compute resources away from machines (physical or virtual), enabling fault-tolerant and elastic distributed systems to easily be built and run effectively.

- **Cloud Foundry**

**Cloud Foundry**

Cloud Foundry is an open source cloud platform as a service (PaaS) on which developers can build, deploy, run and scale applications.

As always, we welcome and encourage contributions from the community!

**Additional Resources**

- [https://jonathangazeley.com/2021/01/05/using-truenas-to-provide-persistent-storage-for-kubernetes/](https://jonathangazeley.com/2021/01/05/using-truenas-to-provide-persistent-storage-for-kubernetes/)
12.2.4 - Nextcloud

Nextcloud Plugin

The Nextcloud plugin is a suite of client-server software for creating and using file hosting services.

Plugins Catalog

Before getting started... expand □

- You must have a data pool available for plugin storage.
- You must connect the system to the internet. Go to Network > Interfaces, edit the intended plugin interface, and set Disable Hardware Offloading.

To see the plugin catalog, go to the Plugins screen.

First time in this menu? expand □

Going to the Jails or Plugins screen for the first time prompts to select a location on the system for storing Jail related data.

By default, this location stores all data related to jails and plugins, including downloaded applications, data managed by the jail or plugin, and any jail snapshots.

Disconnecting or deleting the pool that stores jail data can result in permanent data loss! Make sure to back up any critical data or snapshots that are stored in a jail before changing the storage configuration.

To change the Jails and Plugins storage location, click □, select a new pool, and click CHOOSE.
I don't see anything! expand

If the catalog doesn’t load:

- Go to Network > Global Configuration and confirm the Default Gateway and DNS Servers addresses are correct.
- Open the Shell and ping an Internet address. The output confirms the system is connected to the Internet.

TrueNAS organizes plugins into two Collections:

- iXsystems maintained plugins
- Open source plugins created and maintained by TrueNAS users.

By default, TrueNAS shows the iXsystems-supported plugins. To see the community plugins, open Browse a Collection and select Community.

Installation

- Basic Install

Go to Plugins and select Nextcloud, then click INSTALL.

Type a Jail Name and click SAVE.

After Nextcloud installs successfully, you can manage your instance of the plugin.
Click **POST INSTALL NOTES** to obtain your Nextcloud admin user and Nextcloud admin password information. Click **MANAGE** to access the Nextcloud login page within your browser.

Enter the credentials from **POST INSTALL NOTES** and click **Log in** to access the Nextcloud Hub.
Static IP Install

Go to Plugins and select Nextcloud, then click INSTALL.

Type a Jail Name, then disable the NAT checkbox and enter an available IP in the IPv4 Address field. Select an IPv4 Netmask (IX recommends 24), then click SAVE.

After Nextcloud installs, you must add your Nextcloud IP to your Nextcloud jail trusted domains.

Go to Jails and expand your Nextcloud jail, then click > SHELL.

Enter `ee /usr/local/www/nextcloud/config/config.php` to edit your Nextcloud config file.
Scroll to the trusted_domains section and type your Nextcloud IP as a new line item. Use the image below for reference.

```
array(
    0 => 'localhost',
    1 => '192.168.15.144',
    2 => '192.168.15.148',
),
```

Type CTRL+C to close the editor, then type `exit` to close the config file.

Go back to Plugins and expand your Nextcloud instance. Click POST INSTALL NOTES to obtain your Nextcloud admin user and Nextcloud admin password information. Click MANAGE to access the Nextcloud login page within your browser.

Enter the credentials from POST INSTALL NOTES and click Log in. You are directed to the Nextcloud Hub.

Refer to the Nextcloud documentation for details about using the Nextcloud platform:

- [Administrators Manual](#)
- [Users Manual](#)
- [Nextcloud Developer Documentation](#)
12.2.5 - OpenStack

12.2.5.1 - Cinder Driver

There is a community-supported, open source driver for Cinder available for TrueNAS, available at https://github.com/iXsystems/cinder. This is a simple driver that uses several scripts to allow block/iSCSI interactions between OpenStack Cinder and TrueNAS systems. To review the driver documentation, including minimum hardware requirements, install instructions, and basic usage, see https://github.com/iXsystems/cinder/blob/master/README.md.
12.2.6 - Veeam

- What is Needed?
- Sizing Considerations
- Advantages
- Setting Up TrueNAS as a Veeam Repository
- Performance Tuning for Veeam Backup & Replication

TrueNAS Unified Storage appliances are certified Veeam Ready and can be used to handle demanding backup requirements for file and VM backup. These certification tests measure the speed and effectiveness of the data storage repository using a testing methodology defined by Veeam for Full Backups, Full Restores, Synthetic Full Backups, and Instant VM Recovery from within the Veeam Backup & Replication environment. With the ability to seamlessly scale to petabytes of raw capacity, high-performance networking and cache, and all-flash options, TrueNAS appliances are the ideal choice for Veeam Backup & Replication repositories large and small.

**Certified Hardware**

These TrueNAS products are certified by Veeam:
This article discusses some of the best practices when deploying TrueNAS with Veeam, specific considerations users must be aware of, and some tips to help with performance. The focus will be on capabilities native to TrueNAS, and users are encouraged to also review relevant Veeam documentation, such as their help center and best practices for more information about using and optimizing Veeam.

What is Needed?

When deploying TrueNAS with Veeam users should prepare the following:

- Veeam Backup & Replication dedicated server - either physical or VM
- Windows Server and Microsoft SQL for Veeam
- TrueNAS appliance with users pre-configured as determined by the admin
- Networking - 1/10/40/100GbE infrastructure and cables
- Veeam connected to the Hypervisor or other clients to pull the data to TrueNAS
- All appropriate licenses
- Backup proxies as defined by Veeam - they can be virtual machines or physical machines or the backup server itself for low workloads

Update the TrueNAS systems to the latest version before beginning deployment. This ensures the appliance has the latest bug fixes, security updates and software enhancements to ensure maximum performance and security. If deploying on a closed network (LAN) without access to the Internet, users can also obtain and apply an update manually. For assistance, please contact TrueNAS support.

Contacting iXsystems Support

Customers who purchase iXsystems hardware or that want additional support must have a support contract to use iXsystems Support Services. The TrueNAS Community forums provides free support for users without an iXsystems Support contract.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td><a href="https://support.ixsystems.com">https://support.ixsystems.com</a></td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:support@ixsystems.com">support@ixsystems.com</a></td>
</tr>
<tr>
<td>Telephone</td>
<td>Monday - Friday, 6:00AM to 6:00PM Pacific Standard Time:</td>
</tr>
</tbody>
</table>
Sizing Considerations

TrueNAS storage appliances range from entry-level to high-end, and the user’s current usage scenario and backup demands must be considered.

Define Your Storage Usage
While this guide focuses on Veeam, the unified design of TrueNAS allows it to multitask. If TrueNAS will be handling more than backup jobs, other usage needs should be taken into account. For example, if the storage appliance has one LUN (dataset or zvol) set as a VMware datastore for hosting VMs, and another LUN set to be used for backups, both capacities must be considered.

Estimate Capacity
The first step when estimating required capacity is to understand how much capacity is currently used by existing VMs and by files that users need to back up. Veeam and the TrueNAS appliance will both apply data compression, though different file types and the structure of the data in those files will affect the achieved compression levels. Some tools for capacity estimation are listed at the end of this section, but it is always good to err on the side of caution and 3x the current storage used is not unreasonable. ZFS performs best with utilization below 80%. Snapshots, full backups, and incremental backups will all require more storage than primary storage being used today.

Estimate Network Bandwidth
Bandwidth is harder to estimate and must take into account backup timeframes, backup sizes, and available network resources. Typically, backups run during off-hours when IT equipment is under a lighter load. This timeframe can be set, but if each backup is several terabytes in size, a longer amount of time and greater bandwidth is required. iXsystems tests its Veeam backups using a 10 GbE mixed network with the datastore storage, hypervisor hosts, and backup repository (the TrueNAS) on the same network. However, shorter backup windows, heavy network usage, and dozens of VMs being backed up at the same time may require 40 or 100 GbE networking and multiple Veeam Backup Proxies used in tandem.

For example, consider a scenario of backing up 1000 VMs (each 100 GB in size) with a backup window of 8 hours. This requires around 5 virtual Proxy servers with 8 vCores (16 GB memory each) and around 3.7 GB/s of throughput. In such a scenario, iXsystems would recommend 100 GbE interconnect and TrueNAS appliances with over 100+ hard drives. However, bandwidth can be greatly reduced if users can accept incremental and staggered backups. For example, run an incremental backup on all VMs each day, and a full backup on 100 VMs per night, rotating a different 100 VMs each night. This strategy provides a 5X increase to the maximum number of VMs and reduces costs by 75%.

Choose a TrueNAS model
TrueNAS systems are excellent for backup and archiving, but must be sized correctly. Recommended sizing:

<table>
<thead>
<tr>
<th>Model</th>
<th>Backup Only?</th>
<th>Number of VMs Backed Up</th>
<th>Network Max</th>
<th>Usable Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrueNAS X10</td>
<td>Yes</td>
<td>6800</td>
<td>10 GbE</td>
<td>340 TB</td>
</tr>
<tr>
<td>TrueNAS X20</td>
<td>Yes</td>
<td>13600</td>
<td>10 GbE</td>
<td>680 TB</td>
</tr>
<tr>
<td>TrueNAS M40</td>
<td>No</td>
<td>29400</td>
<td>40 GbE</td>
<td>1.47 PB</td>
</tr>
<tr>
<td>TrueNAS M50</td>
<td>No</td>
<td>151800</td>
<td>100 GbE</td>
<td>7.59 PB</td>
</tr>
<tr>
<td>TrueNAS M60</td>
<td>No</td>
<td>303600</td>
<td>100 GbE</td>
<td>15.8 PB</td>
</tr>
</tbody>
</table>
• **Backup Only?** assumes that the storage is being used only as a backup repository. This can be understood as a recommendation, not a rule. The number of VMs is based upon conservative throughput estimates with an average VM size set as 100GB and a backup window of 8 hours running full backups. All other requirements for the number of Veeam Backup Proxies, and networking dependencies also apply.

• **Number of VMs Backed Up**: Numbers are based on max capacity and estimating 100GB per VM and a 2:1 optimal compression ratio. Compression and Deduplication settings can radically change the estimates, and Veeam allows for fine tuning.

**Configure the Pools, Datasets, and Zvols**
For high-capacity deployments, iXsystems recommends 9+2+1 RAID groups (called “Virtual Devices” or “vdevs” by ZFS terminology). This configuration consists of a RAIDZ2 (similar to RAID 6 with 2 drive parity so 2 drives can fail without data loss) with one to two global hot-spares added to the pool. Pools can include several of these groups, so the capacity can be expanded as needed. For example, 390 TB of usable space with 12 TB drives requires four groups and 48 drives. Detailed configurations can be discussed with iXsystems sales representatives and engineers.

**Storage Lifecycle Planning**
TrueNAS storage pools can be expanded online to the maximum size supported by a particular TrueNAS system. Storage pools can be expanded one vdev (RAID group) at a time so long as each vdev shares the same type. When deploying an iSCSI share requiring a zvol (LUN), users should consider thin provisioning using the **sparse option** during setup.

In addition to the above considerations, there are many tools, forums, and other discussion groups to help verify the amount of storage needed for Veeam backup. In many sites, Veeam compression or deduplication is around 1.5x to 2x, but this is more a reference than a rule. Backup types, applications, and the diversity of VMs can all factor into the true amount of storage needed. Capacity must also be considered alongside desired performance, as a smaller quantity of large drives often will not yield the same performance as a larger number of small drives. For rough calculations, additional resources are listed below.

- [Estimate Veeam space - Veeam Knowledge Space](#)
- [Sizing from Veeam Best Practices](#)
- [3rd Party Disk Space Calculator](#)
- [3rd Party Bandwidth Calculator](#)

**Advantages**
TrueNAS is a robust, unified storage system well-suited for nearly any environment. For backups, the platform takes advantage of the data integrity offered by ZFS that includes features such as copy-on-write, snapshots, and checksums that prevent bit-rot. TrueNAS appliances can also be expanded at any time simply by adding more drives so datasets can grow to keep pace with your data. Here are additional key features that are offered out-of-the-box at no extra cost to the user:

- **Self-healing file system**: ZFS places data integrity first with data scrubs and checksums to ensure files are saved correctly and preserved.
- **Native replication to TrueNAS systems**: perfect for disaster recovery and compliance.
- **High-availability (HA) architecture with 99.999% availability**: Ensure the system is always ready to receive the latest backups.
- **Triple-parity**: RAID groups (vdevs) can be configured with mirror, single-parity (RAIDZ), dual-parity (RAIDZ2), or triple-parity (RAIDZ3) levels, while copy-on-write, checksums, and data scrubbing help protect long-term data integrity.
- **Certified with VMware® and Citrix® XenServer®**: TrueNAS can be both a hypervisor datastore and a backup repository with data on different datasets and even pools. Just be mindful of the scale of the workloads being run.
- **Unrivaled scalability in a single dataset**: Scale the backup repository from terabytes to petabytes of usable capacity. No LUN limits, clustering or licenses needed.

**Setting Up TrueNAS as a Veeam Repository**
Veeam Backup & Replication runs on a Windows operating system, typically Windows Server 2012 or newer, and can connect to a variety of storage systems. iXsystems recommends using iSCSI with a Veeam scale-out repository architecture. Users can also use SMB to mount the volume to the backup server directly. With support for SMB/CIFS, NFS, AFP, iSCSI, and FC, TrueNAS offers many ways to connect to Veeam backup servers.

### Performance Tuning for Veeam Backup & Replication

**Test environment:**

- A 2TB datastore must be configured on TrueNAS System 1 utilizing the iSCSI wizard using default values. This will be the backup source.
- A 2TB datastore must be configured on TrueNAS System 2 utilizing the iSCSI wizard using default values. This will be the backup target.
- Connect the source datastore to the Hypervisor.
- Ensure the NFS ISO datastore is mounted.
- A 64-bit Microsoft Windows Server 2019 Standard VM should be constructed for Veeam Backup & Replication Server.
- Install VMware guest additions.
- Configure STATIC IP for Windows Server 2019 VM.
- Connect storage to the Veeam VM
- Install Veeam software on Veeam Backup & Replication Server.
Using a Scale-out Backup Repository, users can link multiple backup repositories (Extents) together to help with performance and load balancing across the various repositories. In the topology above, the TrueNAS is broken across four LUNs to act as the scale-out extents. Both the FreeNAS datastore and the TrueNAS backup only used one 10GbE link when connecting to the VMware server pool.

**Scale-out Backup Repository is only available in Veeam Backup & Replication 9.5 Enterprise and Enterprise Plus editions.**

**Results**

Testing in this configuration with a backup server and backup proxy, Windows Server 2019 Standard VMs, yielded excellent results with the TrueNAS R-Series platform. iXsystems reference numbers can be seen below. These were achieved with just a single Veeam Backup Server and a Veeam Backup Proxy Server. For more demanding workloads, results can be scaled by adding more VMs to act as the Veeam Backup Proxy.

<table>
<thead>
<tr>
<th>Test</th>
<th>Time Limit</th>
<th>TrueNAS Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Backup</td>
<td>30:00 Minutes</td>
<td>27:41 Minutes</td>
</tr>
<tr>
<td>Full Restore</td>
<td>25:00 Minutes</td>
<td>16:48 Minutes</td>
</tr>
<tr>
<td>Synthetic Full Backup</td>
<td>50:00 Minutes</td>
<td>37:18 Minutes</td>
</tr>
</tbody>
</table>
There are several configuration recommendations and troubleshooting tips when using TrueNAS with a VMware hypervisor.

○ **IQN**

**iSCSI** IQN is an acronym that stands for “iSCSI Qualified Name”. It is comprised of the following naming schema with a preamble, node name and unique identifier:

```
ign.1999-12.com.acmecorp.cloud1:truenas-1
```

VMware requires using an IQN in their software iSCSI implementation.

○ **Failover**

A VMware datastore backed by iSCSI-based storage will consist of at least three distinct pieces: the storage host, the switching infrastructure, and the VMware host itself. In order to maximize service availability, each of these elements needs to be able to tolerate some level of failure without significantly disrupting iSCSI traffic.

TrueNAS systems support high-availability (HA) through dual-controllers running in active/standby mode. A properly-configured HA TrueNAS system can offer up to 5x 9’s of system availability. TrueNAS also fully supports asymmetric logical unit access (ALUA) on iSCSI to significantly reduce failover time.

Network switching infrastructure can be made redundant and fault-tolerant through a number of methods, but multipathing is recommended as the best practice for iSCSI networks.

[VMware’s official documentation](https://www.vmware.com/support/pubs/vsphere-esxi-51-pubs.html) details several ways the virtualization host(s) can be made redundant, so that is not covered here.

○ **Discovery, Authentication, and Access Control**

For a VMware ESXi host to communicate with an iSCSI capable storage array, the iSCSI protocol must be configured to provide: Discovery, Authentication, and Access Control (DAAC).

**Discovery**

iSCSI offers two methods of target discovery: dynamic and static. Dynamic discovery lets the storage array respond automatically to the host initiator’s “SendTargets” request. Static discovery requires an administrator to manually add a list of the iSCSI targets to the initiator. Either method of discovery is fine, but dynamic discovery can make the iSCSI setup process easier.

**Authentication**

iSCSI authentication is handled via the Challenge Handshake Authentication Protocol, or CHAP. CHAP uses a shared secret between targets and initiators to let them validate each other’s authenticity. By default, no CHAP-based authentication is performed by the VMware iSCSI initiator. If you do decide to use
CHAP, authentication can either be unidirectional (where only the target authenticates the initiator) or bidirectional (where both the iSCSI initiator and the iSCSI target are required to authenticate to each other prior to transmitting iSCSI data).

VMware iSCSI initiators operating with unidirectional CHAP can be configured in two behavior modes. In “Required” mode, an iSCSI adapter will give precedence to non-CHAP connections, but if the iSCSI target requires it, the connection will use CHAP instead. Required mode is only supported by Software iSCSI and Dependent Hardware iSCSI adapters. Alternatively, initiators can run in “Prohibited” mode, where an iSCSI adapter will give precedence to CHAP connections, but if the iSCSI target does not support CHAP, the initiator can still connect.

Bidirectional CHAP (called “mutual CHAP” in TrueNAS) offers greater security by ensuring that both sides of the iSCSI connection authenticate against each other. Unidirectional CHAP does not let the iSCSI initiator authenticate the target, and running without CHAP obviously disables all authentication. For this reason, bidirectional CHAP is usually recommended but requires additional configuration and comes with greater administrative overhead when troubleshooting iSCSI connections.

Access Control

Access control policies are set up within a storage array to ensure only certain initiators can connect to the target (even if they possess the correct CHAP password). Access control can be performed using the initiator’s name (IQN), its IP address, or its CHAP username.

VMware and TrueNAS iSCSI Setup

The setup of vCenter iSCSI to TrueNAS requires that ESXi hosts be set up as initiators and TrueNAS storage arrays are set up as targets. To configure ESXi hosts with vCenter, see the VMware vCenter 6.7 documentation.

To configure TrueNAS Enterprise storage arrays with vCenter, iXsystems has developed a vCenter plugin. The plugin uses TrueNAS REST APIs to automate LUN creation and assignment. When an VMFS (iSCSI) datastore is created using the plugin, the TrueNAS systems automatically activate their iSCSI system services.

Hosting VMware Storage with TrueNAS

When using TrueNAS as a VMware datastore:

- Make sure guest VMs have the latest version of vmware-tools installed. VMware provides instructions to install VMware Tools on different guest operating systems.

- Increase the VM disk timeouts to better survive long reboots or other delayed disk operations. Set the timeout to a minimum of 300 seconds. VMware provides instructions for setting disk timeouts on some specific guest operating systems:
  - Linux guests running kernel version 2.6: https://kb.vmware.com/s/article/1009465

NOTE: Reboots or failovers will typically complete much faster than 300 seconds and Disk IO will resume automatically when finished.

VMware Snapshots on TrueNAS

When TrueNAS is used as a VMware datastore, you can coordinate creating and using ZFS and VMware snapshots. See VMware-Snapshots for details.

vStorage APIs for Array Integration (VAAI) for iSCSI
VMware’s VAAI allows storage tasks such as large data moves to be offloaded from the virtualization hardware to the storage array. These operations are performed locally on the NAS without transferring bulk data over the network.

VAAI for iSCSI supports these operations:

- **Atomic Test and Set (ATS)**
  Allows multiple initiators to synchronize LUN access in a fine-grained manner rather than locking the whole LUN and preventing other hosts from accessing the same LUN simultaneously.

- **Clone Blocks (XCOPY)**
  Copies disk blocks on the NAS. Copies occur locally rather than over the network. This operation is similar to Microsoft ODX.

- **LUN Reporting**
  Allows a hypervisor to query the NAS to determine whether a LUN is using thin provisioning.

- **Stun**
  Pauses virtual machines when a pool runs out of space. The space issue can be fixed and the virtual machines continue instead of reporting write errors.

- **Threshold Warning**
  The system reports a warning when a configurable capacity is reached. In TrueNAS, this threshold is configured at the storage pool level when using zvols or at the extent level for both file and device based extents. Typically, the warning is set at the pool level, unless file extents are used, in which case it must be set at the extent level.

- **Unmap**
  Informs TrueNAS that the space occupied by deleted files should be freed. Without unmap, the NAS is unaware of freed space created when the initiator deletes files. For this feature to work, the initiator must support the `unmap` command.

- **Zero Blocks or Write Same**
  Zeros out disk regions. When allocating virtual machines with thick provisioning, the zero write is done locally, rather than over the network. This makes virtual machine creation and any other zeroing of disk regions much quicker.
12.2.7.1 - TrueNAS vCenter Plugin

- Getting and Deploying the Plugin
  - Using the Plugin
  - Connecting TrueNAS Hosts
  - System Management

vCenter Server provides a web interface to manage physical and virtual machines. vCenter uses plugins to integrate server management into the vCenter application. The iXsystems TrueNAS vCenter Plugin activates management options for TrueNAS hardware attached to vCenter Server. This enables some management of TrueNAS systems from a single interface.

The current release version of the TrueNAS vCenter Plugin is 3.4.0. This version is only compatible with VMware vCenter Server version 6.7.0.

Getting and Deploying the Plugin

Currently, the plugin is only available to TrueNAS Enterprise customers. iXsystems Support staff are available to assist with deploying the TrueNAS vCenter Plugin. Please contact iXsystems Support to learn more and schedule a time to deploy the plugin.

Contacting iXsystems Support expand ❯

Customers who purchase iXsystems hardware or that want additional support must have a support contract to use iXsystems Support Services. The TrueNAS Community forums provides free support for users without an iXsystems Support contract.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td><a href="https://support.ixsystems.com">https://support.ixsystems.com</a></td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:support@ixsystems.com">support@ixsystems.com</a></td>
</tr>
</tbody>
</table>
| Telephone      | Monday - Friday, 6:00AM to 6:00PM Pacific Standard Time:  
US-only toll-free: 1-855-473-7449 option 2  
Local and international: 1-408-943-4100 option 2 |
| Telephone      | After Hours (24x7 Gold Level Support only):  
US-only toll-free: 1-855-499-5131  
International: 1-408-878-3140 (international calling rates apply) |

Using the Plugin

After being assisted with deploying the plugin, using the plugin follows a simple process of connecting TrueNAS hosts and configuring the various features to your use case. The interface suspends after several minutes of inactivity and displays a warning that the interface is suspended and must be refreshed.

Connecting TrueNAS Hosts

In a browser, go to your vCenter Server web interface, log in, and click Menu > Global Inventory Lists > Manage TrueNAS > + Add host to add TrueNAS hosts to vCenter.
Fill in the required information. A hostname or IP address can be used for the TrueNAS system. For High Availability systems, use the VIP address or hostname to ensure the plugin remains connected in the event of a system failover. Click Add Host and the TrueNAS hostname or IP address appears in the list of connected systems.

Right-click a list entry to see options to edit the host user credentials or remove that host from vCenter. Click a hostname to see the system management options. Clicking a system entry opens the management interface.

**System Management**

The system management screen shows a summary and options to modify the system.

To modify the TrueNAS system, click Configure. Each submenu has a row of buttons to add or make changes to any items in the list. vCenter works in the background when resolving change requests. Refresh updates the list to see any items that might have finished being created or modified. Tasks in progress display in the collapsible Recent Tasks area across the bottom of the screen. Naming objects in
the plugin follow a standard convention. Names can contain spaces, alphanumeric, -, and . characters.

**System Summary**

Click *Summary* to view basic information about this system. The IP address, installed version of TrueNAS, storage availability, and system service status are shown.

![System Summary](image)

**Datastores**

The vCenter plugin can create two different kinds of datastores on a TrueNAS host:

- Virtual Machine File System (VMFS) for iSCSI block-level access
- Network File System (NFS) for file-level access
vCenter has a default limit of eight NFS datastores per ESX host. See this [VMware article](#) about maximum supported volumes for more details.

The list shows Datastores that have been created and are managed by the plugin. The list does not display other types of shares created and managed through the TrueNAS web interface.

### Add Datastore

Click + (Add) to create a new datastore.

Choose an ESXi host for the datastore or an ESXi cluster to spread the reserved space across multiple systems. Clusters can be used as long as a single member of the cluster supports the datastore features. Click *Next*. 
Choose the datastore type. **VMFS** datastores provide block-level (iSCSI) storage for virtual machines. **NFS** datastores provide file-level storage access. Click **Next** to view specific options for each datastore type.

**VMFS Datastore Configuration** expand □

Enter a name for the new datastore. Enter a value and choose a unit for the **Datastore Size**. The size must be smaller than the chosen **Volume**. The minimum size for a VMFS datastore is **2GB**.

The **Data Path IP** shows the TrueNAS system’s IP address. Users can select other connected TrueNAS systems with the drop-down menu.

Select the datastore **VMFS Version** from the drop-down menu. Choose between the modern version 6 or the legacy versions 3 and 5. See the [VMware VMFS documentation](https://www.vmware.com/products/vmware-vsphere/vmfs.html) for detailed comparisons.

Enabling **Sparse Volume** reserves less than the total available size and metadata storage space, but it can cause writing to fail if the volume has little space remaining. See [zfs(8)](https://www.freebsd.org/cgi/man.cgi?query=zfs&apropos=0) for more details.

Select the TrueNAS pool to hold the datastore. The **Volume** must be large enough to contain the chosen **Datastore Size**.
If you have a high availability NAS with a Fibre Channel license and a network configured to form a Fibre Channel fabric with the NAS and ESXi, you will also be able to select a Fibre Channel port for the datastore.

Selecting a Fibre Channel port enables that port with the datastore’s target on the NAS and creates a datastore with a corresponding Fibre Channel HBA on the ESXi.

### NFS Datastore Configuration

Enter a Name for the new datastore. The Data Path IP shows the TrueNAS system’s IP address. Users can select other TrueNAS systems added to vCenter Server with the drop-down menu. Select the path to the TrueNAS NFS share from the Mount Share Path drop-down menu. Click Next.

**Review Datastore Configuration**

After configuring the VMFS or NFS datastore, vCenter will show a summary of the new datastore. To begin creating the datastore, review the settings and click Finish. The interface shows a warning when the datastore contains more than 80% of the available space. Click Refresh to see the new datastore after creating it.

**Extending a Datastore**

Users needing additional space can increase the total size of a VMFS datastore. Highlight a VMFS datastore from the list and click Edit to extend it.

The new size must be larger than the current size and less than the total available capacity. For best performance, we recommend using less than 80% of the total available size. Using decimal notation will round down the size to the nearest 1024 bytes (or whatever the volume’s configured default block size is).
Click *Extend Datastore*. Datastores reserve some available space for internal use and set the available capacity to slightly less than the chosen amount.

**Cloning Datastores**

Cloning an NFS or VMFS datastore duplicates that datastore. Select a datastore from the list and click *Clone*. Choose an ESXi host to store the new datastore and click *Next*. Enter a name for the clone and click *Clone Datastore*.

vCenter starts the cloning process and continues the task in the background. Click *Refresh* after some time to see the cloned datastore.

**RBAC**

An administrator can grant vCenter users specific role-based access to the TrueNAS systems managed by this plugin.

<table>
<thead>
<tr>
<th>Role Name</th>
<th>User is allowed to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover</td>
<td>Add TrueNAS systems to vCenter</td>
</tr>
<tr>
<td>Create Clones</td>
<td>Copy existing datastores</td>
</tr>
<tr>
<td>Create Storage</td>
<td>Create new datastores</td>
</tr>
<tr>
<td>Modify Storage</td>
<td>Edit existing datastores</td>
</tr>
<tr>
<td>Destroy Storage</td>
<td>Delete datastores</td>
</tr>
</tbody>
</table>

Each role gives the user the ability to perform the functions in that role and all of the roles that precede it in the list. For example, a user with a *Create Storage* role can create a new datastore and clone existing datastores. The vCenter administrator account always has all permissions.

New vCenter users must be created in **Menu > Administration > Single Sign On > Users and Groups**.

**Add a Role to an Existing vCenter User**

Click + to open the *Add Role Based Access Control* window. Type a user name in the form `DOMAIN_NAME\username`, where `DOMAIN_NAME` is the user Domain found in the **vCenter Menu > Administration > Single Sign On > Users and Groups** page. Open the Assign Role drop-down menu and choose a role for the user. Click *Add* to add the role.
If the entry does not appear in the list immediately, click Refresh.
TrueNAS CORE API documentation is available from the web interface by clicking settings > API Keys > DOCS.

Alternately, append /api/docs/ to your TrueNAS hostname or IP address in a browser to go directly to the API documentation.

For convenience, static builds of the current 2.0 API documentation stored on the Docs Hub:

- [Websocket Protocol](#)
- [RESTful](#)
14 - User Agreements

14.1 - TrueNAS CORE EULA

TrueNAS CORE End User License Agreement

Important - Please Read This EULA Carefully

PLEASE CAREFULLY READ THIS END USER LICENSE AGREEMENT (EULA) BEFORE CLICKING THE AGREE BUTTON. THIS AGREEMENT SERVES AS A LEGALLY BINDING DOCUMENT BETWEEN YOU AND IXSYSTEMS, INC. BY CLICKING THE AGREE BUTTON, DOWNLOADING, INSTALLING, OR OTHERWISE USING TRUENAS CORE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS IN THIS AGREEMENT, DO NOT USE OR INSTALL TRUENAS CORE SOFTWARE.

This agreement is provided in accordance with the Commercial Arbitration Rules of the American Arbitration Association (the “AAA Rules”) under confidential binding arbitration held in Santa Clara County, California. To the fullest extent permitted by applicable law, no arbitration under this EULA will be joined to an arbitration involving any other party subject to this EULA, whether through class arbitration proceedings or otherwise. Any litigation relating to this EULA shall be subject to the jurisdiction of the Federal Courts of the Northern District of California and the state courts of the State of California, with venue lying in Santa Clara County, California. All matters arising out of or relating to this agreement shall be governed by and construed in accordance with the internal laws of the State of California without giving effect to any choice or conflict of law provision or rule.

1.0 Definitions

1.1 “Company”, “iXsystems” and “iX” means iXsystems, Inc., on behalf of themselves, subsidiaries, and affiliates under common control.

1.2 “TrueNAS CORE Software” means the TrueNAS CORE storage management software.

1.3 “TrueNAS Device” means the TrueNAS storage appliances and peripheral equipment provided by iXsystems or a third party.

1.4 “Product” means, individually and collectively, the TrueNAS CORE Software and the TrueNAS Device provided by iXsystems.

1.5 “Open Source Software” means various open source software components licensed under the terms of applicable open source license agreements, each of which has its own copyright and its own applicable license terms.

1.6 “Licensee”, “You” and “Your” refers to the person, organization, or entity that has agreed to be bound by this EULA including any employees, affiliates, and third party contractors that provide services to You.

1.7 “Agreement” refers to this document, the TrueNAS End User License Agreement.

2.0 License

Subject to the terms set forth in this Agreement, iXsystems grants You a non-exclusive, non-transferable, perpetual, limited license without the option to sublicense, to use TrueNAS CORE Software on Your TrueNAS Device(s). This use includes but is not limited to using or viewing the instructions, specifications, and documentation provided with the Product.

TrueNAS CORE software is made available as Open Source Software, subject to the license conditions contained within that Open Source Software.

3.0 License Restrictions
TrueNAS CORE Software is authorized for use on any TrueNAS Device. TrueNAS Devices can include hardware provided by iXsystems or third parties. TrueNAS Devices may also include virtual machines and cloud instances. TrueNAS CORE software may not be commercially distributed or sold without an addendum license agreement and express written consent from iXsystems.

The TrueNAS CORE Software is protected by copyright laws and international treaties, as well as other intellectual property laws, statutes, and treaties. The TrueNAS CORE Software is licensed, not sold to You, the end user. You do not acquire any ownership interest in the TrueNAS CORE Software, or any other rights to the TrueNAS CORE Software, other than to use the TrueNAS CORE Software in accordance with the license granted under this Agreement, subject to all terms, conditions, and restrictions. iXsystems reserves and shall retain its entire right, title, and interest in and to the TrueNAS CORE Software, and all intellectual property rights arising out of or relating to the TrueNAS CORE Software, subject to the license expressly granted to You in this Agreement.

The TrueNAS CORE Software may contain iXsystems’ proprietary trademarks and collateral. By agreeing to this license agreement for TrueNAS CORE, You agree to use reasonable efforts to safeguard iXsystems’ intellectual property and hereby agree to not use or distribute iXsystems’ proprietary intellectual property and collateral commercially without the express written consent of iXsystems. Official iXsystems Channel Partners are authorized to use and distribute iXsystems’ intellectual property through an addendum to this license agreement. By accepting this Agreement, You are responsible and liable for all uses of the Product through access thereto provided by You, directly or indirectly.

The TrueNAS CORE software includes Open Source components and some proprietary extensions which are available through additional licences You agree to not alter the source code to take advantage of the proprietary extensions without a license to those proprietary extensions, including the TrueNAS Enterprise features sets.

4.0 General

4.1 Entire Agreement - This Agreement, together with any associated purchase order, service level agreement, and all other documents and policies referenced herein, constitutes the entire and only agreement between You and iXsystems for use of the TrueNAS CORE Software and all other prior negotiations, representations, agreements, and understandings are superseded hereby. No agreements altering or supplementing the terms hereof may be made except by means of a written document signed by Your duly authorized representatives and those of iXsystems.

4.2 Waiver and Modification - No failure of either party to exercise or enforce any of its rights under this EULA will act as a waiver of those rights. This EULA may only be modified, or any rights under it waived, by a written document executed by the party against which it is asserted.

4.3. Severability - If any provision of this EULA is found illegal or unenforceable, it will be enforced to the maximum extent permissible, and the legality and enforceability of the other provisions of this EULA will not be affected.

4.4 United States Government End Users - For any TrueNAS CORE Software licensed directly or indirectly on behalf of a unit or agency of the United States Government, this paragraph applies. Company’s proprietary software embodied in the Product: (a) was developed at private expense and is in all respects Company’s proprietary information; (b) was not developed with government funds; (c) is Company’s trade secret for all purposes of the Freedom of Information Act; (d) is a commercial item and thus, pursuant to Section 12.212 of the Federal Acquisition Regulations (FAR) and DFAR Supplement Section 227.7202, Government’s use, duplication or disclosure of such software is subject to the restrictions set forth by the Company and Licensee shall receive only those rights with respect to the Product as are granted to all other end users.

4.5 Title - iXsystems retains all rights, titles, and interest in TrueNAS CORE Software and all related copyrights, trade secrets, patents, trademarks, and any other intellectual and industrial property and proprietary rights, including registrations, applications, registration keys, renewals, and extensions of such rights. Contact Information - If You have any questions about this Agreement, or if You want to contact iXsystems for any reason, please email legal@ixsystems.com.

4.6 Maintenance and Support - You may be entitled to support services from iXsystems after purchasing a
Product or a support contract. iXsystems will provide these support services based on the length of time of the purchased support contract. This maintenance and support is only valid for the length of time that You have purchased with Your Product. iXsystems may from time to time and at their sole discretion vary the terms and conditions of the maintenance and support agreement based on different business environmental and personnel factors. Any variations will be notified via email and the support portal. For more information on our Maintenance and Support contract, refer to https://www.ixsystems.com/support/.

4.7 Force Majeure - iXsystems will not be deemed to be in default of any of the provisions of this Agreement or be liable for any delay or failure in performance due to Force Majeure, which shall include without limitation acts of God, earthquake, weather conditions, labor disputes, changes in law, regulation or government policy, riots, war, fire, epidemics, acts or omissions of vendors or suppliers, equipment failures, transportation difficulties, malicious or criminal acts of third parties, or other occurrences which are beyond iXsystems’ reasonable control.

4.8 Termination - iXsystems may cease any and all support, services, or maintenance under this Agreement without prior notice, or liability, and for any reason whatsoever, without limitation, if any of the terms and conditions of this Agreement are breached. Other provisions of this Agreement will survive termination including, without limitation, ownership provisions, warranty disclaimers, indemnity, and limitations of liability.

4.9 Open Source Software Components - iXsystems uses Open Source Software components in the development of the TrueNAS CORE Software. Open Source Software components that are used in the TrueNAS CORE Software are composed of separate components each having their own trademarks, copyrights, and license conditions.

4.10 Assignment - Licensee shall not assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance, under this Agreement, in each case whether voluntarily, involuntarily, by operation of law, or otherwise, without iXsystems’ prior written consent. No delegation or other transfer will relieve Licensee of any of its obligations or performance under this Agreement. Any purported assignment, delegation, or transfer in violation of this Section is void. iXsystems may freely assign or otherwise transfer all or any of its rights, or delegate or otherwise transfer all or any of its obligations or performance, under this Agreement without Licensee’s consent. This Agreement is binding upon and inures to the benefit of the parties hereto and their respective permitted successors and assigns.

5.0 Export Control Regulations

“The Product may be subject to export control laws. You shall not, directly or indirectly, export, re-export, or release the Product to, or make the Product accessible from, any jurisdiction or country to which export, re-export, or release is prohibited by law, rule, or regulation. You shall comply with all applicable laws, regulations, and rules, and complete all required undertakings (including obtaining any necessary export license or other governmental approval).”

6.0 Data Collection and Privacy

TrueNAS CORE Software may collect non-sensitive system information relating to Your use of the Product, including information that has been provided directly or indirectly through automated means. Usage of TrueNAS CORE Software, device status and system configuration are allowed according to iXsystems’ privacy policy.

TrueNAS CORE Software will not collect sensitive User information including email addresses, names of systems, pools, datasets, folders, files, credentials.

By accepting this Agreement and continuing to use the Product, you agree that iXsystems may use any information provided through direct or indirect means in accordance with our privacy policy and as permitted by applicable law, for purposes relating to management, compliance, marketing, support, security, update delivery, and product improvement.

7.0 Limitation of Liability and Disclaimer of Warranty
THE PRODUCT IS PROVIDED "AS IS" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY
OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, IXSYSTEMS, ON
ITS OWN BEHALF AND ON BEHALF OF ITS AFFILIATES AND ITS AND THEIR RESPECTIVE
LICENSORS AND SERVICE PROVIDERS, EXPRESSLY DISCLAIMS ALL WARRANTIES, WHETHER
EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THE PRODUCT,
INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR
PURPOSE, TITLE, AND NON-INFRINGEMENT, AND WARRANTIES THAT MAY ArISE OUT OF
COURSE OF DEALING, COURSE OF PERFORMANCE, USAGE, OR TRADE PRACTICE. WITHOUT
LIMITATION TO THE FOREGOING, IXSYSTEMS PROVIDES NO WARRANTY OR UNDERTAKING,
AND MAKES NO REPRESENTATION OF ANY KIND THAT THE PRODUCT WILL MEET THE
LICENSEE’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE, OR WORK
WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS, OR SERVICES, OPERATE WITHOUT
INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE,
OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

TO THE FULLEST EXTENT PERMITTED UNDER APPLICABLE LAW: (A) IN NO EVENT WILL
IXSYSTEMS OR ITS AFFILIATES, OR ANY OF ITS OR THEIR RESPECTIVE LICENSORS OR
SERVICE PROVIDERS, BE LIABLE TO LICENSEE, LICENSEE’S AFFILIATES, OR ANY THIRD PARTY
FOR ANY USE, INTERRUPTION, DELAY, OR INABILITY TO USE THE PRODUCT; LOST REVENUES
OR PROFITS; DELAYS, INTERRUPTION, OR LOSS OF SERVICES, BUSINESS, OR GOODWILL;
LOSS OR CORRUPTION OF DATA; LOSS RESULTING FROM SYSTEM OR SYSTEM SERVICE
FAILURE, MALFUNCTION, OR SHUTDOWN; FAILURE TO ACCURATELY TRANSFER, READ, OR
TRANSMIT INFORMATION; FAILURE TO UPDATE OR PROVIDE CORRECT INFORMATION; SYSTEM
INCOMPATIBILITY OR PROVISION OF INCORRECT COMPATIBILITY INFORMATION; OR BREACHES
IN SYSTEM SECURITY; OR FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY,
SPECIAL, OR PUNITIVE DAMAGES, WHETHER ARISING OUT OF OR IN CONNECTION WITH THIS
AGREEMENT, BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE,
REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE AND WHETHER OR NOT
IXSYSTEMS WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; (B) IN NO EVENT WILL
IXSYSTEMS' AND ITS AFFILIATES’, INCLUDING ANY OF ITS OR THEIR RESPECTIVE LICENSORS’
AND SERVICE PROVIDERS’, COLLECTIVE AGGREGATE LIABILITY UNDER OR IN CONNECTION
WITH THIS AGREEMENT OR ITS SUBJECT MATTER, UNDER ANY LEGAL OR EQUITABLE THEORY,
INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND
OTHERWISE, EXCEED THE TOTAL AMOUNT PAID TO IXSYSTEMS PURSUANT TO THIS
AGREEMENT FOR THE PRODUCT THAT IS THE SUBJECT OF THE CLAIM; (C) THE LIMITATIONS
SET FORTH IN THIS SECTION SHALL APPLY EVEN IF THE LICENSEE’S REMEDIES UNDER THIS
AGREEMENT FAIL OF THEIR ESSENTIAL PURPOSE.

You hereby acknowledge that you have read and understand this Agreement and voluntarily accept the
duties and obligations set forth herein by clicking accept on this Agreement.
14.2 - TrueNAS Enterprise EULA

TrueNAS Enterprise End User License Agreement

Important - Please Read This EULA Carefully

PLEASE CAREFULLY READ THIS END USER LICENSE AGREEMENT (EULA) BEFORE CLICKING THE AGREE BUTTON. THIS AGREEMENT SERVES AS A LEGALLY BINDING DOCUMENT BETWEEN YOU AND IXSYSTEMS, INC. BY CLICKING THE AGREE BUTTON, DOWNLOADING, INSTALLING, OR OTHERWISE USING TRUENAS SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT). IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS IN THIS AGREEMENT, DO NOT USE OR INSTALL TRUENAS SOFTWARE.

This agreement is provided in accordance with the Commercial Arbitration Rules of the American Arbitration Association (the “AAA Rules”) under confidential binding arbitration held in Santa Clara County, California. To the fullest extent permitted by applicable law, no arbitration under this EULA will be joined to an arbitration involving any other party subject to this EULA, whether through class arbitration proceedings or otherwise. Any litigation relating to this EULA shall be subject to the jurisdiction of the Federal Courts of the Northern District of California and the state courts of the State of California, with venue lying in Santa Clara County, California. All matters arising out of or relating to this agreement shall be governed by and construed in accordance with the internal laws of the State of California without giving effect to any choice or conflict of law provision or rule.

1.0 Definitions

1.1 “Company”, “iXsystems” and “iX” means iXsystems, Inc., on behalf of themselves, subsidiaries, and affiliates under common control.

1.2 “TrueNAS Software” means the TrueNAS Enterprise storage management software.

1.3 “TrueNAS Device” means the TrueNAS hardware storage appliances and peripheral equipment.

1.4 “Product” means, individually and collectively, the TrueNAS Software and the TrueNAS Device.

1.5 “Open Source Software” means various open source software components licensed under the terms of applicable open source license agreements, each of which has its own copyright and its own applicable license terms.

1.6 “Licensee”, “You” and “Your” refers to the person, organization, or entity that has agreed to be bound by this EULA including any employees, affiliates, and third party contractors that provide services to You.

1.7 “Agreement” refers to this document, the TrueNAS End User License Agreement.

2.0 License

Subject to the terms set forth in this Agreement, iXsystems grants You a non-exclusive, non-transferable, perpetual, limited license without the option to sublicense, to use TrueNAS Software on Your TrueNAS Device(s) in accordance with Your authorized purchase and use of a TrueNAS Device(s) for Your internal business purposes. This use includes but is not limited to using or viewing the instructions, specifications, and documentation provided with the Product.

3.0 License Restrictions

TrueNAS Software is only authorized for use with a TrueNAS Device identified by a specific serial number and manufactured by iXsystems. This license may be extended to a second TrueNAS Device if an additional TrueNAS Device was purchased for high availability data protection. The license is provided as a digital license key that is installed on the TrueNAS Device.
The TrueNAS Software is protected by copyright laws and international treaties, as well as other intellectual property laws, statutes, and treaties. The TrueNAS Software is licensed, not sold to You, the end user. You do not acquire any ownership interest in the TrueNAS Software, or any other rights to the TrueNAS Software, other than to use the TrueNAS Software in accordance with the license granted under this Agreement, subject to all terms, conditions, and restrictions. iXsystems reserves and shall retain its entire right, title, and interest in and to the TrueNAS Software, and all intellectual property rights arising out of or relating to the TrueNAS Software, subject to the license expressly granted to You in this Agreement.

The TrueNAS Software may contain iXsystems’ trademarks, trade secrets, and proprietary collateral. iXsystems strictly prohibits the acts of decompiling, reverse engineering, or disassembly of the TrueNAS Software. You agree to use commercially reasonable efforts to safeguard iXsystems’ intellectual property, trade secrets, or other proprietary information You may have access to, from infringement, misappropriation, theft, misuse, or unauthorized access. You will promptly notify iXsystems if You become aware of any infringement of the TrueNAS Software and cooperate with iXsystems in any legal action taken by iXsystems to enforce its intellectual property rights.

By accepting this Agreement, You agree You will not disclose, copy, transfer, or publish benchmark results relating to the Product without the express written consent of iXsystems. You agree not to use, or permit others to use, the TrueNAS Software beyond the scope of the license granted under Section 2, unless otherwise permitted by iXsystems, or in violation of any law, regulation or rule, and you will not modify, adapt, or otherwise create derivative works or improvements of the TrueNAS Software. You are responsible and liable for all uses of the Product through access thereto provided by You, directly or indirectly.

4.0 General

4.1 Entire Agreement - This Agreement, together with any associated purchase order, service level agreement, and all other documents and policies referenced herein, constitutes the entire and only agreement between You and iXsystems for use of the TrueNAS Software and all other prior negotiations, representations, agreements, and understandings are superseded hereby. No agreements altering or supplementing the terms hereof may be made except by means of a written document signed by Your duly authorized representatives and those of iXsystems.

4.2 Waiver and Modification - No failure of either party to exercise or enforce any of its rights under this EULA will act as a waiver of those rights. This EULA may only be modified, or any rights under it waived, by a written document executed by the party against which it is asserted.

4.3 Severability - If any provision of this EULA is found illegal or unenforceable, it will be enforced to the maximum extent permissible, and the legality and enforceability of the other provisions of this EULA will not be affected.

4.4 United States Government End Users - For any TrueNAS Software licensed directly or indirectly on behalf of a unit or agency of the United States Government, this paragraph applies. Company’s proprietary software embodied in the Product: (a) was developed at private expense and is in all respects Company’s proprietary information; (b) was not developed with government funds; (c) is Company’s trade secret for all purposes of the Freedom of Information Act; (d) is a commercial item and thus, pursuant to Section 12.212 of the Federal Acquisition Regulations (FAR) and DFAR Supplement Section 227.7202, Government’s use, duplication or disclosure of such software is subject to the restrictions set forth by the Company and Licensee shall receive only those rights with respect to the Product as are granted to all other end users.

4.5 Foreign Corrupt Practices Act - You will comply with the requirements of the United States Foreign Corrupt Practices Act (the “FCPA”) and will refrain from making, directly or indirectly, any payments to third parties which constitute a breach of the FCPA. You will notify Company immediately upon Your becoming aware that such a payment has been made. You will indemnify and hold harmless Company from any breach of this provision.

4.6 Title - iXsystems retains all rights, titles, and interest in TrueNAS Software and all related copyrights, trade secrets, patents, trademarks, and any other intellectual and industrial property and proprietary rights, including registrations, applications, registration keys, renewals, and extensions of such rights.

4.7 Contact Information - If You have any questions about this Agreement, or if You want to contact
4.8 Maintenance and Support - You may be entitled to support services from iXsystems after purchasing a TrueNAS Device or a support contract. iXsystems will provide these support services based on the length of time of the purchased support contract. This maintenance and support is only valid for the length of time that You have purchased with Your TrueNAS Device. iXsystems may from time to time and at their sole discretion vary the terms and conditions of the maintenance and support agreement based on different business environmental and personnel factors. Any variations will be notified via email and the support portal. For more information on our Maintenance and Support contract, refer to https://www.ixsystems.com/support/.

4.9 Force Majeure - iXsystems will not be deemed to be in default of any of the provisions of this Agreement or be liable for any delay or failure in performance due to Force Majeure, which shall include without limitation acts of God, earthquake, weather conditions, labor disputes, changes in law, regulation or government policy, riots, war, fire, epidemics, acts or omissions of vendors or suppliers, equipment failures, transportation difficulties, malicious or criminal acts of third parties, or other occurrences which are beyond iXsystems’ reasonable control.

4.10 Termination - iXsystems may terminate or suspend Your license to use the TrueNAS Software and cease any and all support, services, or maintenance under this Agreement without prior notice, or liability, and for any reason whatsoever, without limitation, if any of the terms and conditions of this Agreement are breached. Upon termination, rights to use the TrueNAS Software will immediately cease. Other provisions of this Agreement will survive termination including, without limitation, ownership provisions, warranty disclaimers, indemnity, and limitations of liability.

4.11 Open Source Software Components - iXsystems uses Open Source Software components in the development of the TrueNAS Software. Open Source Software components that are used in the TrueNAS Software are composed of separate components each having their own trademarks, copyrights, and license conditions.

4.12 Assignment - Licensee shall not assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance, under this Agreement, in each case whether voluntarily, involuntarily, by operation of law, or otherwise, without iXsystems’ prior written consent. No delegation or other transfer will relieve Licensee of any of its obligations or performance under this Agreement. Any purported assignment, delegation, or transfer in violation of this Section is void. iXsystems may freely assign or otherwise transfer all or any of its rights, or delegate or otherwise transfer all or any of its obligations or performance, under this Agreement without Licensee’s consent. This Agreement is binding upon and inures to the benefit of the parties hereto and their respective permitted successors and assigns.

5.0 Export Control Regulations

The Product may be subject to US export control laws, including the US Export Administration Act and its associated regulations. You shall not, directly or indirectly, export, re-export, or release the Product to, or make the Product accessible from, any jurisdiction or country to which export, re-export, or release is prohibited by law, rule, or regulation. You shall comply with all applicable federal laws, regulations, and rules, and complete all required undertakings (including obtaining any necessary export license or other governmental approval), prior to exporting, re-exporting, releasing, or otherwise making the Product available outside the US.

6.0 Data Collection and Privacy

TrueNAS Software may collect non-sensitive system information relating to Your use of the Product, including information that has been provided directly or indirectly through automated means. Usage of TrueNAS Software, device status and system configuration are allowed according to iXsystems’ privacy policy.

TrueNAS Software will not collect sensitive User information including email addresses, names of systems, pools, datasets, folders, files, credentials.

By accepting this Agreement and continuing to use the Product, you agree that iXsystems may use any
7.0 Limitation of Liability and Disclaimer of Warranty

THE PRODUCT IS PROVIDED "AS IS" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, IXSYSTEMS, ON ITS OWN BEHALF AND ON BEHALF OF ITS AFFILIATES AND ITS AND THEIR RESPECTIVE LICENSORS AND SERVICE PROVIDERS, EXPRESSLY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THE PRODUCT, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND WARRANTIES THAT MAY ARISE OUT OF COURSE OF DEALING, COURSE OF PERFORMANCE, USAGE, OR TRADE PRACTICE. WITHOUT LIMITATION TO THE FOREGOING, IXSYSTEMS PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE PRODUCT WILL MEET THE LICENSEE'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE, OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS, OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE, OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

TO THE FULLEST EXTENT PERMITTED UNDER APPLICABLE LAW: (A) IN NO EVENT WILL IXSYSTEMS OR ITS AFFILIATES, OR ANY OF ITS OR THEIR RESPECTIVE LICENSORS OR SERVICE PROVIDERS, BE LIABLE TO LICENSEE, LICENSEE'S AFFILIATES, OR ANY THIRD PARTY FOR ANY USE, INTERRUPTION, DELAY, OR INABILITY TO USE THE PRODUCT; LOST REVENUES OR PROFITS; DELAYS, INTERRUPTION, OR LOSS OF SERVICES, BUSINESS, OR GOODWILL; LOSS OR CORRUPTION OF DATA; LOSS RESULTING FROM SYSTEM OR SYSTEM SERVICE FAILURE, MALFUNCTION, OR SHUTDOWN; FAILURE TO ACCURATELY TRANSFER, READ, OR TRANSMIT INFORMATION; FAILURE TO UPDATE OR PROVIDE CORRECT INFORMATION; SYSTEM INCOMPATIBILITY OR PROVISION OF INCORRECT COMPATIBILITY INFORMATION; OR BREACHES IN SYSTEM SECURITY; OR FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, OR PUNITIVE DAMAGES, WHETHER ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE AND WHETHER OR NOT IXSYSTEMS WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; (B) IN NO EVENT WILL IXSYSTEMS’ AND ITS AFFILIATES’, INCLUDING ANY OF ITS OR THEIR RESPECTIVE LICENSORS’ AND SERVICE PROVIDERS’, COLLECTIVE AGGREGATE LIABILITY UNDER OR IN CONNECTION WITH THIS AGREEMENT OR ITS SUBJECT MATTER, UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE, EXCEED THE TOTAL AMOUNT PAID TO IXSYSTEMS PURSUANT TO THIS AGREEMENT FOR THE PRODUCT THAT IS THE SUBJECT OF THE CLAIM; (C) THE LIMITATIONS SET FORTH IN THIS SECTION SHALL APPLY EVEN IF THE LICENSEE’S REMEDIES UNDER THIS AGREEMENT FAIL OF THEIR ESSENTIAL PURPOSE.

You hereby acknowledge that you have read and understand this Agreement and voluntarily accept the duties and obligations set forth herein by clicking accept on this Agreement.
15 - Notices

15.1 - TrueNAS Data Collection Statement

TrueNAS collects non-sensitive system data and relays the data to a collector managed by iXsystems. This system data collection is enabled by default and can be disabled in the web interface under System > General > Usage collection. When disabled, no information about system configuration and usage is collected. The system capacity and software version is still collected.

The protocol for system data collection uses the same TCP ports as HTTPS (443) and passes through most firewalls as an outgoing web connection. If a firewall blocks the data collection or the data collection is disabled, there is no adverse impact to the TrueNAS system.

Non-sensitive system data is used to identify the quality and operational trends in the fleet of TrueNAS systems used by the entire community. The collected data helps iXsystems identify issues, plan for new features, and determine where to invest resources for future software enhancements.

The non-sensitive system data collected is clearly differentiated from sensitive user data that is explicitly not collected by TrueNAS. This table describes the differences:

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Sensitive User Data (NOT COLLECTED)</th>
<th>Non-Sensitive System Data (Optionally Collected)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Any data that includes user identity or business information</td>
<td>Data that only includes information about the TrueNAS system and its operation</td>
</tr>
<tr>
<td>Frequency</td>
<td>NEVER</td>
<td>Daily</td>
</tr>
<tr>
<td>Examples</td>
<td>Usernames, passwords, email addresses</td>
<td>Anonymous hardware inventory, faults, statistics, Pool configuration</td>
</tr>
<tr>
<td></td>
<td>User-created System and dataset names</td>
<td>Software versions, firmware versions</td>
</tr>
<tr>
<td></td>
<td>Directory, files names, user data</td>
<td>Services and features enabled, Usage and Performance statistics</td>
</tr>
</tbody>
</table>
The TrueNAS (and FreeNAS) Software Development Life Cycle (SDLC) is the process of planning, creating, testing, deploying, and maintaining TrueNAS releases.

There are five stages to the TrueNAS SDLC: requirement analysis, design and development, testing and evaluation, documentation, and maintenance.

- **Requirement Analysis**
  Determine the objectives, nature, and scope of future versions of the software. Requirement Analysis involves gathering feedback and interpreting customer needs and requirements, diagnosing existing problems, and weighing the pros and cons of potential solutions. The end result is a list of recommended improvements to be integrated into future versions of TrueNAS.

- **Design and Development**
  Required and planned changes are investigated in detail and development steps are determined. Proposed alterations are reviewed by peers for completeness, correctness, and proper coding style. TrueNAS developers then begin altering the software to include new features, resolve software bugs, or implement security improvements.

- **Testing and Evaluation**
  Code is integrated into the existing TrueNAS source tree, then built and tested by the Release Engineering (RE) department. RE verifies that all requirements and objectives are properly met and the updated software is reliable and fault-tolerant according to the determined requirements. If issues are found, code is reworked to meet the development requirements. Simultaneously, a security evaluation of the TrueNAS code is completed, with any discovered issues sent to the engineering team for resolution.

- **Documentation**
  The Validation and Documentation Team audits all development changes to the software and resolves any inconsistencies with the current software documentation. This is to verify that end user documentation is as accurate as possible. Any security notices, errata, or best practices are also drafted for inclusion on the TrueNAS Security website.

- **Maintenance**
  The new release of TrueNAS is evaluated to determine further feature development, bug fixes, or security vulnerability patches. During this stage, security patches and software erratum are corrected, updated versions of existing branches are pushed, and feedback is solicited for future versions of the software.

**SDLC Application**

The TrueNAS SDLC applies to the latest two release branches. As new releases are created for TrueNAS, the oldest TrueNAS release branch is dropped out of the SDLC and labeled as End of Life (EoL). For example, TrueNAS/FreeNAS 11.3 and TrueNAS 12.0 were in active development under the SDLC in August 2020. In early 2021, TrueNAS Core/Enterprise 12.0 and 12.1 branches were in active development under the SDLC. These versions of the software are in active development and maintenance. We encourage users to actively keep their software updated to an active development version to continue to receive security patches and other software improvements.

**TrueNAS Quality Lifecycle**

TrueNAS releases follow a general adoption guideline for their lifetime. Starting with the NIGHTLY builds, each stage of a major release incorporates more testing cycles and bug fixes that represent a maturation of the release. With each version release stage, users are encouraged to install, upgrade, or otherwise begin using the major version, depending on the specific TrueNAS deployment and use case:

<table>
<thead>
<tr>
<th>Release Stage</th>
<th>Completed QA Cycles</th>
<th>Typical Use-case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIGHTLY</td>
<td>0</td>
<td>Developers</td>
<td>Incomplete</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>ALPHA</td>
<td>1</td>
<td>Testers</td>
<td>Not much field testing</td>
</tr>
<tr>
<td>BETA</td>
<td>2</td>
<td>Enthusiasts</td>
<td>Major Feature Complete, but expect some bugs</td>
</tr>
<tr>
<td>RC</td>
<td>3</td>
<td>Home Users</td>
<td>Suitable for non-critical deployments</td>
</tr>
<tr>
<td>RELEASE</td>
<td>4</td>
<td>General Use</td>
<td>Suitable for less complex deployments</td>
</tr>
<tr>
<td>U1</td>
<td>5</td>
<td>Business Use</td>
<td>Suitable for more complex deployments</td>
</tr>
<tr>
<td>U2+</td>
<td>6+</td>
<td>Mission Critical</td>
<td>Suitable for critical uptime deployments</td>
</tr>
</tbody>
</table>
15.3 - SMB1 Security Advisory

Do not use SMB1

SMB1, also known as SMBv1, is an early version of the Windows SMB file-sharing protocol. Microsoft has deprecated the SMB1 protocol for security reasons and strongly recommends removing SMB1. SMB1 is disabled by default in FreeNAS and TrueNAS. Current SMB networking clients use later versions of the SMB protocol.

Microsoft maintains a list of older products that still require SMB1.

Windows Explorer (File Explorer) does not need SMB1, or a separate protocol called NetBIOS (sometimes called “NetBIOS over TCP/IP”), to discover and list SMB shares from a TrueNAS server. All modern versions of Windows use a newer protocol called WS-Discovery, which is more reliable and faster. TrueNAS automatically enables WS-Discovery to allow discovery of SMB shares by client devices.

Do not enable SMB1 on FreeNAS or TrueNAS without understanding the security implications and taking measures to protect the network from those risks. Contact the vendor of older products for upgrades to support newer, more secure versions of SMB, or replace older products with ones that do not require the security risks of SMB1.

Do not enable SMB1 unless it is absolutely required for essential equipment that cannot be upgraded or replaced, the security implications are understood, and steps have been taken to protect the network from those security risks.
See the TrueNAS Security Hub to get the latest information that you need to maintain the security, integrity, and availability of your data.
17 - User Recommendations

Because TrueNAS is both Open Source and complicated, the massive user community often creates recommendations for specific hardware or environments. User-created recommendations can be added in this location, but be aware these are provided “as-is” and are not officially supported by iXsystems, Inc.

17.1 - /etc/hosts IP Persistence

- **Description**
  
  Domain Name resolution, the process of mapping host or domain names, such as `mytruenas` or `truenas1.mycompany.com`, to their associated IP addresses can be achieved through a variety of methods. The quickest method is to read entries in the hosts file, which is a local text file containing a list of IP addresses mapped to domain/host names. Every operating system (OS) that communicates through the TCP/IP protocol has a hosts file.

  The hosts file can be used to speed up name resolution if a DNS server is not available on the local network. A DNS server runs networking software that allows it to join the Domain Name System, which is the standard service used on the Internet for name resolution. When adding entries to the hosts file of a TrueNAS system, use the TrueNAS web interface to save the entries directly to the configuration database. **Do not** edit the hosts file directly, as it will be overwritten by the configuration database during reboot.

- **Errors**

  I’m trying to use NFS, SSH, and FTP, but I keep receiving “reverse DNS” or timeout errors.

  The fastest domain name resolution method is for the operating system to read the hosts file, but if there are no matching entries in the hosts file, a DNS server is queried instead. This is a slower process as the OS has to find the DNS server, send it a query, and wait for an answer. Timeout errors are common for some network protocols, such as SSH, FTP and NFS, as their connection requests can time out before a DNS server replies. To speed up name resolution, add entries for commonly used hosts to the hosts file.

  **Fix**

  To add an entry to the hosts file, log in to the TrueNAS web interface using a browser, and follow these steps:

  1. Go to **Network > Global Configuration**.
  2. Scroll down to the **Host name database** field and add an entry for the TrueNAS system in the format `IP_address space hostname`.
  3. Click Save.
17.2 - Legacy Engine (11.3) Replication

This article only applies to FreeNAS or TrueNAS version 11.3. The “Legacy” replication option in this version provides compatibility with the replication engine used in FreeNAS/TrueNAS 11.2 and earlier.

Creating a legacy replication requires creating an SSH connection to the remote system and snapshots generated by a periodic snapshot task.

Process Summary

- Create SSH connection to remote system in System > SSH Connections
- Create a periodic snapshot task of the source datasets in Tasks > Periodic Snapshot Tasks
- Go to Tasks > Replication Tasks and open the advanced creation screen.
  - Set Transport to LEGACY
  - Select SSH connection to remote system
  - Choose source datasets related to the periodic snapshot task
  - Set a target location on the remote system

Creating a Legacy Engine Replication

Go to Tasks > Replication Tasks and click ADD. Select Advanced Replication.

Set the replication Transport method to LEGACY to reorganize the screen for only the relevant options.

Choose the SSH connection to a remote system that stores replicated snapshots.

Select the source datasets on the local system using the file browser or manually enter the dataset paths into the field. To also replicate snapshots of child datasets, set Recursive.

To choose the replication target, open the file browser and select the dataset to store snapshots. Entering a path to a new dataset creates that target dataset in the defined file path.

The remaining options allow defining how long to keep replicated snapshots, compressing data before replication, and setting a bandwidth limit on the transfer.
17.3 - Configuring a 3rd Party VPN service on TrueNAS

TrueNAS includes the ability to run OpenVPN. This is a short tutorial to configure the OpenVPN client on TrueNAS 12.0.

Many VPN services are provided by 3rd parties that are unaffiliated with iXsystems. Please verify compatibility and pricing with your provider before integrating with TrueNAS.

- Installing the CA
- Installing the Certificate
- Configure OpenVPN Service
- Start the service

Prerequisite: An OpenVPN server running with a similar configuration to these configuration file settings:

```plaintext
Example OpenVPN Configuration File

```
```
<ca>
-----BEGIN CERTIFICATE-----
MIIFgNGGD2bjNiJRSeJfuqreDjkghgh57w0BER8GFADBrtMtMwEQYJRDEwuPCVU
UN+1Lm6r64q+7zq14UH+f+zB566F0pEwwSjEAGEAI4UTFBEAXMRK3B1b1ZT11QT
-----END CERTIFICATE-----
</ca>
```
```
<cert>
-----BEGIN CERTIFICATE-----
MIIGGTCCBAGgIBgAwIBABqhkiG9TANBgkw0BABKJZMQsFA0bYwQDE1EQwEw
-----END CERTIFICATE-----
</cert>
```
```
<key>
-----BEGIN PRIVATE KEY-----
MIIQkgkhlGIBADABg0bWAACQEFACSwqkAwqEAAQCAoIC71VfshS9w0aSNJ
DCBPfEpUct6iMzeeeb0Di1TGNmbujIaQoDmknKkEy7InQXa+wiZiXKouFx2b7zr
-----END PRIVATE KEY-----
</key>
```
```
<tls-auth>
# 2048 bit OpenVPN static key
-----BEGIN OpenVPN Static key V1-----
31201c2093539a034a3549b8f109f7a0
-----END OpenVPN Static key V1-----
</tls-auth>
```

Installing the CA
Open **System > CA**.

Add a new certificate.

Give it a name (here VPN_CA) and select “Import CA” as type.

Copy/paste the certificate from the configuration file. The certificate can be found between the tags `<ca>` and `</ca>` of the OpenVPN config file.
Installing the Certificate

Open **System > Certificate**.

Add a certificate.
Give it a name (here VPN) and select “Import Certificate” as type. Copy and paste the certificate, it can be found in the OpenVPN config file between the tags `<cert>` and `</cert>`. Copy and paste the key between the tags `<key>` and `</key>` from the configuration file.
So now we have a CA and a certificate for the VPN connexion as below:
Configure OpenVPN Service

Go to the Services page and find the OpenVPN Client entry. Click the icon to configure the service.
Choose the certificate and Root CA we previously installed. The rest of the parameters are found in the OpenVPN configuration file. In “Additional parameters” you can add options that are in the configuration files, like the TLS key for authentication or user login/password.
Start the service

Start the service (check automatically if needed).
Test if the connection is working using `curl ifconfig.me` in a terminal for example. It should give you the IP from the VPN connection and not from your “local” connection, turn the OpenVPN client service on and off to see the difference.

Logs of the OpenVPN client can be found in `/var/log/messages` and `/var/log/daemon`. 
17.4 - Setting ACL Permissions for Jailed Applications

Various Jail Plugins will require permissions to be set on datasets so that they can access them.

Unless otherwise modified, dataset will be owned by the user root and group wheel. Jailed processes like Plex run as their own user. As a result Plex will not be able to read or write to the any datasets and thus not be able to access media files stored in those datasets.

To create an ACL for dataset for an application you need to obtain the Application user ID. Plex’s ID is 972.

Other popular Plugin user IDs include:

- Radarr = 352
- Sonarr = 351
- Transmission = 921
- Sabnzbd = 350

To create an ACL for dataset, open Storage > Pools. Click the three dot icon more_vert and select Edit Permissions. Click the Add ACL Item button to create a new entry. The new entry will appear at the bottom of the list of existing ACL items.

Continuing with Plex as our example we would enter the following:

Who: User
User: 972 (Don't worry if it says "Could not find a username for this ID")
ACL Type: Allow
Permissions Type: Basic
Permissions: Read
Flags Type: Basic
Flags: Inherit

If files already exist in the dataset, click the Apply permissions recursively checkbox and click Save.
TrueNAS uses Samba to share pools using the Microsoft SMB protocol. SMB is built into the Windows and macOS operating systems and most Linux and BSD systems pre-install an SMB client to provide support for the SMB protocol.

The SMB protocol supports many different types of configuration scenarios, ranging from simple to complex. The complexity of the scenario depends on several factors:

- Client operating system types and versions connecting to the share.
- When the network has an active Windows server.
- Active Directory is in use.

Depending on the specific authentication requirements, it can be necessary to create or import user and group accounts into FreeNAS/TrueNAS.

The videos at https://www.youtube.com/watch?v=RxggaE935PM and https://www.youtube.com/watch?v=QhwOyLtAnw0 clarify setting up permissions on SMB shares on legacy (pre-TrueNAS 12.0) versions of FreeNAS: