

**Open Source**  
STORAGE PLATFORM

**FreeBSD® 8.2**  
BASED OPERATING SYSTEM

**Includes ZFS**  
MAXIMUM STORAGE & INTEGRATION

**FreeNAS™ 8.0.3 Guide**  
Edited by Dru Lavigne



# FreeNAS™

## 8.0.3 USERS GUIDE

# FreeNAS™

## 8.0.3 USERS GUIDE



*FreeNAS™ is © 2011, 2012 iXsystems*  
*FreeNAS™ is a trademark of iXsystems*  
*FreeBSD is a registered trademark of the FreeBSD Foundation*  
*Cover art by Jenny Rosenberg*

## Table of Contents

# Section 1: Introduction and Installation

1	<a href="#">Introduction</a>	8
	<a href="#">1.1 Hardware Requirements</a>	9
	<a href="#">1.1.1 Architecture</a>	9
	<a href="#">1.1.2 RAM</a>	9
	<a href="#">1.1.3 Compact or USB Flash</a>	10
	<a href="#">1.1.4 Storage Disks and Controllers</a>	10
	<a href="#">1.1.5 Network Interfaces</a>	11
	<a href="#">1.1.6 RAID Overview</a>	11
	<a href="#">1.1.7 ZFS Overview</a>	13
	<a href="#">1.2 What's New</a>	14
	<a href="#">1.3 Features</a>	15
	<a href="#">1.4 Known Issues</a>	16
	<a href="#">1.5 Roadmap for 8.2</a>	16
2	<a href="#">Installing FreeNAS™</a>	17
	<a href="#">2.1 Getting FreeNAS™</a>	18
	<a href="#">2.2 Installing from CDROM</a>	19
	<a href="#">2.3 Installing from the Image</a>	21
	<a href="#">2.3.1 Using xzcat and dd on a FreeBSD or Linux System</a>	21
	<a href="#">2.3.2 Using Keka and dd on an OS X System</a>	22
	<a href="#">2.3.3 Using physdiskwrite on Windows</a>	22
	<a href="#">2.4 Initial Setup</a>	23
	<a href="#">2.5 Upgrading FreeNAS™</a>	25
	<a href="#">2.5.1 Using the ISO</a>	26
	<a href="#">2.5.2 From the GUI</a>	28
	<a href="#">2.5.2.1 If Something Goes Wrong</a>	30

# Section 2: Using the Graphical Interface

3	<a href="#">Account Configuration</a>	30
	<a href="#">3.1 My Account</a>	31
	<a href="#">3.2 Groups</a>	32
	<a href="#">3.3 Users</a>	34
4	<a href="#">System Configuration</a>	36
	<a href="#">4.1 Reporting</a>	37
	<a href="#">4.2 Settings</a>	37
	<a href="#">4.2.1 General Tab</a>	38
	<a href="#">4.2.2 Advanced Tab</a>	39
	<a href="#">4.2.3 Email Tab</a>	41
	<a href="#">4.2.4 SSL Tab</a>	42
	<a href="#">4.3 System Information</a>	43
	<a href="#">4.4 Cron Jobs</a>	44

4.5	<a href="#">Loaders</a>	45
4.5.1	<a href="#">Recovering From Incorrect Loaders</a>	47
4.6	<a href="#">Rsync Tasks</a>	48
4.6.1	<a href="#">Creating an Rsync Task</a>	48
4.6.2	<a href="#">Configuring Rsync Between Two FreeNAS™ Systems</a>	50
4.7	<a href="#">S.M.A.R.T. Tests</a>	51
4.8	<a href="#">Sysctls</a>	53
5	<a href="#">Network Configuration</a>	54
5.1	<a href="#">Global Configuration</a>	54
5.2	<a href="#">Network Summary</a>	55
5.3	<a href="#">Interfaces</a>	56
5.4	<a href="#">Link Aggregations</a>	57
5.5	<a href="#">Static Routes</a>	61
5.6	<a href="#">VLANs</a>	61
6	<a href="#">Storage Configuration</a>	62
6.1	<a href="#">Periodic Snapshot Tasks</a>	62
6.2	<a href="#">Replication Tasks</a>	65
6.2.1	<a href="#">Configuring SSH Key Based Authentication</a>	66
6.2.2	<a href="#">Creating the Replication Task</a>	68
6.2.3	<a href="#">Testing Replication</a>	69
6.2.4	<a href="#">Troubleshooting</a>	70
6.3	<a href="#">Volumes</a>	71
6.3.1	<a href="#">Auto Importing Volumes</a>	71
6.3.2	<a href="#">Importing Volumes</a>	72
6.3.3	<a href="#">Creating Volumes</a>	73
6.3.4	<a href="#">Adding to an Existing Volume</a>	75
6.3.5	<a href="#">Creating ZFS Datasets</a>	75
6.3.6	<a href="#">Creating a zvol</a>	77
6.3.7	<a href="#">Setting Permissions</a>	78
6.3.8	<a href="#">Viewing Volumes</a>	79
6.3.9	<a href="#">Replacing a Failed Drive</a>	82
6.3.10	<a href="#">Hot Swapping a ZFS Failed Drive</a>	84
7	<a href="#">Sharing Configuration</a>	84
7.1	<a href="#">AFP Shares</a>	85
7.1.1	<a href="#">Creating AFP Shares</a>	85
7.1.2	<a href="#">Connecting to AFP Shares As Guest</a>	87
7.1.3	<a href="#">Using Time Machine</a>	90
7.2	<a href="#">CIFS Shares</a>	91
7.2.1	<a href="#">Creating CIFS Shares</a>	92
7.2.2	<a href="#">Configuring Anonymous Access</a>	93
7.2.3	<a href="#">Configuring Local User Access</a>	98
7.3	<a href="#">NFS Shares</a>	102
7.3.1	<a href="#">Creating NFS Shares</a>	102
7.3.2	<a href="#">Sample NFS Share Configuration</a>	103
7.3.3	<a href="#">Connecting to the NFS Share</a>	104
	<a href="#">7.3.3.1 From BSD or Linux Clients</a>	104
	<a href="#">7.3.3.2 From Microsoft Clients</a>	104

7.3.3.3	<a href="#">From Mac OS X Clients</a>	105
7.3.4	<a href="#">Troubleshooting</a>	106
8	<a href="#">Services Configuration</a>	107
8.1	<a href="#">Control Services</a>	107
8.2	<a href="#">AFP</a>	108
8.3	<a href="#">Active Directory</a>	109
8.3.1	<a href="#">Troubleshooting Tips</a>	112
8.4	<a href="#">CIFS</a>	112
8.4.1	<a href="#">Troubleshooting Tips</a>	115
8.5	<a href="#">Dynamic DNS</a>	115
8.6	<a href="#">FTP</a>	117
8.6.1	<a href="#">Anonymous FTP</a>	119
8.6.2	<a href="#">Specified User Access in chroot</a>	120
8.6.3	<a href="#">Encrypting FTP</a>	123
8.6.4	<a href="#">Troubleshooting</a>	123
8.7	<a href="#">LDAP</a>	124
8.8	<a href="#">NFS</a>	125
8.9	<a href="#">S.M.A.R.T.</a>	126
8.10	<a href="#">SNMP</a>	127
8.11	<a href="#">SSH</a>	128
8.11.1	<a href="#">Chrooting SFTP users</a>	130
8.11.2	<a href="#">Troubleshooting SSH Connections</a>	134
8.12	<a href="#">TFTP</a>	134
8.13	<a href="#">UPS</a>	135
8.14	<a href="#">iSCSI</a>	136
8.14.1	<a href="#">Target Global Configuration</a>	137
8.14.2	<a href="#">Authorized Accesses</a>	140
8.14.3	<a href="#">Device Extents</a>	141
8.14.4	<a href="#">Extents</a>	143
8.14.5	<a href="#">Initiators</a>	143
8.14.6	<a href="#">Portals</a>	145
8.14.7	<a href="#">Targets</a>	145
8.14.8	<a href="#">Target/Extents</a>	147
8.14.9	<a href="#">Connecting to iSCSI Share</a>	147
8.15	<a href="#">Rsync</a>	148
8.15.1	<a href="#">Rsync Modules</a>	148
9	<a href="#">Additional Options</a>	150
9.1	<a href="#">Display System Processes</a>	150
9.2	<a href="#">Reboot</a>	150
9.3	<a href="#">Shutdown</a>	151
9.4	<a href="#">Log Out</a>	151
9.5	<a href="#">Help</a>	152
9.6	<a href="#">Alert</a>	152

# Section 3: Getting Help

- 10 [FreeNAS™ Support Resources](#).....152
  - [10.1 Website and Social Media](#).....153
  - [10.2 Trac Database](#).....153
  - [10.3 IRC](#).....153
  - [10.4 Mailing Lists](#).....154
  - [10.5 Forums](#).....154
  - [10.6 Instructional Videos](#).....156
  - [10.7 Professional Support](#).....156
  - [10.8 FAQs](#).....156
    - [10.8.1 Can a RAID-Z array be expanded? For example, if I start off with a 8x2TB RAID-Z2 array can I add more drives to it in the future?](#) .....156
    - [10.8.2 Is there a command to force FreeBSD to scan for new disks? I'm trying to add some disks to my array using the hot-swappable bays and a 3ware SATA card. The drives go in fine and light up, but the operating system can't see them.](#) .....157
    - [10.8.3 If my hardware/motherboard dies, can I rebuild with new/different hardware and still import/read the data from my disks? What about my datasets?](#).....157
    - [10.8.4 How do I replace a bad drive?](#).....157
    - [10.8.5 Can I share files from my external USB drive?](#).....158
    - [10.8.6 Can I mount my MAC formatted drive?](#).....158
    - [10.8.7 How do I get to the command line /CLI/shell?](#).....158
    - [10.8.8 Does FreeNAS support 4k sector drives? How do I check if it is configured?](#).....158
    - [10.8.9 My network transfer speeds are very slow, what is wrong?](#).....158
    - [10.8.10 Why do changes I make at the command line to config files or settings disappear after a reboot?](#).....159

# Section 4: Contributing to FreeNAS™

- 11 [How to Get Involved](#).....159
  - [11.1 Assist with Localization](#) .....159
  - [11.2 Submit Bug Reports](#).....161
  - [11.3 Test Upcoming Versions](#).....163
    - [11.3.1 Upcoming Version 8.2](#).....163
    - [11.3.2 Testing a Nightly Snapshot](#).....163
    - [11.3.3 Rolling Your Own Testing Snapshot](#).....163

# Section 1: Introduction and Installation

## Preface

Written by users of the FreeNAS™ network-attached storage operating system.

Version 8.0.3

Published January 17, 2012

Copyright © 2011, 2012 [iXsystems](#).

This Guide covers the installation and use of FreeNAS™ 8.0.3. *If you are running a version of FreeNAS™ 8.x that is earlier than FreeNAS™ 8.0.3, it is strongly recommended that you upgrade to or install FreeNAS™ 8.0.3.* This version fixes many bugs from previous 8.x versions and several features mentioned in this Guide were not available or did not work as documented in earlier versions of FreeNAS™ 8.x.

The FreeNAS™ Users Guide is a work in progress and relies on the contributions of many individuals. If you are interested in helping us to improve the Guide, visit [doc.freenas.org](http://doc.freenas.org) and create a wiki login account. If you use IRC Freenode, you are welcome to join the #freenas channel where you will find other FreeNAS™ users.

The FreeNAS™ Users Guide is freely available for sharing and redistribution under the terms of the [Creative Commons Attribution License](#). This means that you have permission to copy, distribute, translate, and adapt the work as long as you attribute iXsystems as the original source of the Guide.

FreeNAS™ is a trademark of iXsystems.

FreeBSD and the FreeBSD logo are registered trademarks of the [FreeBSD Foundation](#).

## Typographic Conventions

The FreeNAS™ 8.0.3 Guide uses the following typographic conventions:

**bold text:** represents a command written at the command line. In usage examples, the font is changed to `Courier 10` with any command output displayed in unbolded text.

*italic text:* used to represent device names or file name paths.

***bold italic text:*** used to emphasize an important point.

## 1 Introduction

FreeNAS™ is an embedded open source network-attached storage (NAS) system based on FreeBSD and released under a BSD license. A NAS provides an operating system that has been optimized for file storage and sharing.

The FreeNAS™ Project was originally founded by Olivier Cochard-Labbé in 2005 and was based on [m0n0wall](#), an embedded firewall based on FreeBSD. It was PHP based, easy-to-use, and had lots of features. In December of 2009, Olivier announced that the .7 branch would be placed in maintenance-only mode as he no longer had time to devote to further FreeNAS™ development. Volker Theile, a FreeNAS™ developer who also develops on Debian in his day job, decided to start the [OpenMediaVault](#) project, which would be a rewrite of FreeNAS™ based on Debian Linux and released



under the terms of the GpLv3 license. Many FreeNAS™ users were not pleased about the change of license and the loss of kernel-based ZFS support due to GPL incompatibilities with the CDDL license.

iXsystems, a provider of FreeBSD-based hardware solutions and professional support, took the initiative to continue the development of a BSD licensed FreeNAS™ solution based on FreeBSD. They took the opportunity to analyze the positives (lots of cool features) and negatives (monolithic, everything-but-the-kitchen-sink design that was difficult to maintain and support). It was decided that the next version would be rewritten from scratch using a modular design that would support plugins. This would allow FreeNAS™ to have a small footprint that was easy to support while allowing users to just install the plugins for the features they desired. It would have the added benefit of allowing users to create and contribute plugins for niche features, allowing its usage cases to grow with users' needs.

Work on the new design began in 2010 and the initial redesigned version, FreeNAS™ 8.0, was released on May 2, 2011. Working with the community to fix the bugs and add the features needed within the core portion of the NAS resulted in FreeNAS™ 8.0.1 which was released on September 30, 2011. FreeNAS™ 8.0.2 was released on October 13, 2011 and provided additional bug fixes. FreeNAS™ 8.0.3 was released on January 3, 2012. This latest release provides full NAS functionality suited for both home use and production environments. It does not contain all of the features provided by FreeNAS .7--the upcoming 8.2 release and its plugin architecture will allow the creation of plugins so that missing features can be installed by the users that require them.

## 1.1 Hardware Requirements

Since FreeNAS™ 8.0.3 is based on FreeBSD 8.2, it supports the same hardware found in the amd64 and i386 sections of the [FreeBSD 8.2 Hardware Compatibility List](#).

Actual hardware requirements will vary depending upon what you are using your FreeNAS™ system for. This section provides some guidelines to get you started. You should also skim through the [FreeNAS™ Hardware Forum](#) for performance tips from other FreeNAS™ users. The Hardware Forum is also an excellent place to post questions regarding your hardware setup or the hardware best suited to meet your requirements.

### 1.1.1 Architecture

While FreeNAS™ is available for both 32-bit and 64-bit architectures, you should use 64-bit hardware if you care about speed or performance. A 32-bit system can only address up to 4GB of RAM, making it poorly suited to the RAM requirements of ZFS. If you only have access to a 32-bit system, consider using UFS instead of ZFS.

### 1.1.2 RAM

The best way to get the most out of your FreeNAS™ system is to install as much RAM as possible. If your RAM is limited, consider using UFS until you can afford better hardware. ZFS typically requires a minimum of 6 GB of RAM in order to provide good performance; in practical terms (what you can actually install), this means that the minimum is really 8 GB. The more RAM, the better the performance, and the Forums provide anecdotal evidence from users on how much performance is gained by adding more RAM. For systems with large disk capacity (greater than 6 TB), a general rule of thumb is 1GB of RAM for every 1TB of storage.

**NOTE:** by default, ZFS disables pre-fetching (caching) for systems containing less than 4 GB of

*usable* RAM. Not using pre-fetching can really slow down performance. 4 GB of usable RAM is not the same thing as 4 GB of installed RAM as the operating system resides in RAM. This means that the practical pre-fetching threshold is 6 GB, or 8 GB of installed RAM. You can still use ZFS with less RAM, but performance will be effected.

If you are installing FreeNAS™ on a headless system, disable the shared memory settings for the video card in the BIOS.

### 1.1.3 Compact or USB Flash

The FreeNAS™ operating system is a running image that needs to be installed onto a USB or compact flash device that is at least 2 GB in size. A list of compact flash drives known to work with FreeNAS™ can be found on the [.7 wiki](#). If you don't have compact flash, you can instead use a USB thumb drive that is dedicated to the running image and which stays inserted in the USB slot. While technically you can install FreeNAS™ onto a hard drive, this is discouraged as you will lose the storage capacity of the drive. In other words, the operating system will take over the drive and will not allow you to store data on it, regardless of the size of the drive.

The FreeNAS™ installation will partition the operating system drive into two ~1GB partitions. One partition holds the current operating system and the other partition is used when you upgrade. This allows you to safely upgrade to a new image or to revert to an older image should you encounter problems.

### 1.1.4 Storage Disks and Controllers

The [Disk section](#) of the FreeBSD Hardware List lists the supported disk controllers. In addition, support for 3ware 6gbps RAID controllers has been added along with the CLI utility `tw_cli` for managing 3ware RAID controllers.

FreeNAS™ supports [hot pluggable](#) drives. Make sure that AHCI is enabled in the BIOS and that you have read [Hot Swapping a ZFS Failed Drive](#) before implementing this feature.

If you have some money to spend and wish to optimize your disk subsystem, consider your read/write needs, your budget, and your RAID requirements.

For example, moving the the [ZIL](#) (ZFS Intent Log) to a dedicated SSD only helps performance if you have synchronous writes, like a database server. SSD cache devices only help if your working set is larger than system RAM, but small enough that a significant percentage of it will fit on the SSD.

If you have steady, non-contiguous writes, use disks with low seek times. Examples are 10K or 15K SAS drives which cost about \$1/GB. An example configuration would be six 15K SAS drives in a RAID 10 which would yield 1.8 TB of usable space or eight 15K SAS drives in a RAID 10 which would yield 2.4 TB of usable space.

7200 RPM SATA disks are designed for single-user sequential I/O and are not a good choice for multi-user writes.

If you have the budget and high performance is a key requirement, consider a [Fusion-I/O card](#) which is optimized for massive random access. These cards are expensive and are suited for high end systems that demand performance. A Fusion-I/O can be formatted with a filesystem and used as direct storage; when used this way, it does not have the write issues typically associated with a flash device. A Fusion-I/O can also be used as a cache device when your ZFS dataset size is bigger than your RAM. Due to the

increased throughput, systems running these cards typically use multiple 10 GigE network interfaces.

If you will be using ZFS, [Disk Space Requirements for ZFS Storage Pools](#) recommends a minimum of 16 GB of disk space. Due to the way that ZFS creates swap, you can not format less than 3GB of space with ZFS. However, on a drive that is below the minimum recommended size you lose a fair amount of storage space to swap: for example, on a 4 GB drive, 2GB will be reserved for swap.

If you are new to ZFS and are purchasing hardware, read through [ZFS Storage Pools Recommendations](#) first.

### 1.1.5 Network Interfaces

The FreeBSD [Ethernet section](#) of the Hardware Notes indicates which interfaces are supported by each driver. While many interfaces are supported, FreeNAS™ users have seen the best performance from Intel and Chelsio interfaces, so consider these brands if you are purchasing a new interface.

At a minimum you will want to use a GigE interface. While GigE interfaces and switches are affordable for home use, it should be noted that modern disks can easily saturate 110 MB/s. If you require a higher network throughput, you can "bond" multiple GigE cards together using the LACP type of [Link Aggregation](#). However, any switches will need to support LACP which means you will need a more expensive managed switch rather than a home user grade switch.

If network performance is a requirement and you have some money to spend, use 10 GigE interfaces and a managed switch. If you are purchasing a managed switch, consider one that supports LACP and jumbo frames as both can be used to increase network throughput.

**NOTE:** at this time the following are *not* supported: InfiniBand, FibreChannel over Ethernet, or wireless interfaces.

If network speed is a requirement, consider both your hardware and the type of shares that you create. On the same hardware, CIFS will be slower than FTP or NFS as Samba is [single-threaded](#). If you will be using CIFS, use a fast CPU.

### 1.1.6 RAID Overview

Data redundancy and speed are important considerations for any network attached storage system. Most NAS systems use multiple disks to store data, meaning you should decide what type of [RAID](#) to use *before* installing FreeNAS™. This section provides an overview of RAID types to assist you in deciding which type best suits your requirements.

**RAID 0:** uses data striping to store data across multiple disks. It provides zero fault tolerance, meaning if one disk fails, all of the data on all of the disks is lost. The more disks in the RAID 0, the more likely the chance of a failure.

**RAID 1:** all data is mirrored onto two disks, creating a redundant copy should one disk fail. If the disks are on separate controllers, this form of RAID is also called duplexing.

**RAID 5:** requires a minimum of 3 disks and can tolerate the loss of one disk without losing data. Disk reads are fast but write speed can be reduced by as much as 50%. If a disk fails, it is marked as degraded but the system will continue to operate until the drive is replaced and the RAID is rebuilt. However, should another disk fail before the RAID is rebuilt, all data will be lost. If your FreeNAS™ system will be used for steady writes, RAID 5 is a poor choice due to the slow write speed.

**RAID 6:** requires a minimum of 4 disks and can tolerate the loss of 2 disks without losing data. Benefits from having many disks as performance, fault tolerance, and cost efficiency are all improved relatively with more disks. The larger the failed drive, the longer it takes to rebuild the array. Reads are very fast but writes are slower than a RAID 5.

**RAID 10:** requires a minimum of 4 disks and number of disks is always even as this type of RAID mirrors striped sets. Offers faster writes than RAID 5. Can tolerate multiple disk loss without losing data, as long as both disks in a mirror are not lost.

**RAID 60:** requires a minimum of 8 disks. Combines RAID 0 striping with the distributed double parity of RAID 6 by striping 2 4-disk RAID 6 arrays. RAID 60 rebuild times are half that of RAID 6.

**RAIDZ1:** ZFS software solution that is equivalent to RAID5. Its advantage over RAID 5 is that it avoids the [write-hole](#) and doesn't require any special hardware, meaning it can be used on commodity disks. If your FreeNAS™ system will be used for steady writes, RAIDZ is a poor choice due to the slow write speed. Requires a minimum of 3 disks though 5 disks is recommended (over 3, 4, or 6 disks). It should be noted that you cannot add additional drives to expand the size of a RAIDZ1 after you have created it. The only way to increase the size of a RAIDZ1 is to replace each drive with a larger drive one by one while allowing time for restriping between each drive swap out. However, you can combine two existing RAIDZ1's to increase the size of a ZFS volume (pool).

**RAIDZ2:** double-parity ZFS software solution that is similar to RAID-6. Its advantage over RAID 5 is that it avoids the [write-hole](#) and doesn't require any special hardware, meaning it can be used on commodity disks. Requires a minimum of 3 disks. RAIDZ2 allows you to lose 1 drive without any degradation as it basically becomes a RAIDZ1 until you replace the failed drive and restripe. At this time, RAIDZ2 on FreeBSD is slower than RAIDZ1.

**NOTE:** It isn't recommended to mix ZFS RAID with hardware RAID. It is recommended that you place your hardware RAID controller in JBOD mode and let ZFS handle the RAID. According to [Wikipedia](#): *ZFS can not fully protect the user's data when using a hardware RAID controller, as it is not able to perform the automatic self-healing unless it controls the redundancy of the disks and data. ZFS prefers direct, exclusive access to the disks, with nothing in between that interferes. If the user insists on using hardware-level RAID, the controller should be configured as JBOD mode (i.e. turn off RAID-functionality) for ZFS to be able to guarantee data integrity. Note that hardware RAID configured as JBOD may still detach disks that do not respond in time; and as such may require TLER/CCTL/ERC-enabled disks to prevent drive dropouts. These limitations do not apply when using a non-RAID controller, which is the preferred method of supplying disks to ZFS.*

When comparing hardware RAID types conventional wisdom recommends the following in order of preference: Raid6, Raid10, Raid5, then Raid0. If using ZFS, the recommended preference changes to RAIDZ2. These forum posts are also worth reading:

- [What is the Best RAIDZ Configuration](#)
- [Getting the Most out of ZFS Pools](#)
- [RAIDZ Configuration Requirements and Recommendations](#)

**NOTE: NO RAID SOLUTION PROVIDES A REPLACEMENT FOR A RELIABLE BACKUP STRATEGY. BAD STUFF CAN STILL HAPPEN AND YOU WILL BE GLAD THAT YOU BACKED UP YOUR DATA WHEN IT DOES.** See [section 6.1 Periodic Snapshot Tasks](#) and [section 6.2 Replication Tasks](#) if you would like to use ZFS snapshots and rsync as part of your backup strategy.

### 1.1.7 ZFS Overview

While ZFS isn't hardware (it is a filesystem), an overview is included in this section as the decision to use ZFS may impact on your hardware choices and whether or not to use hardware RAID.

If you're new to ZFS, the [Wikipedia entry on ZFS](#) provides an excellent starting point to learn about its features. These resources are also useful to bookmark and refer to as needed:

- [ZFS Evil Tuning Guide](#)
- [FreeBSD ZFS Tuning Guide](#)
- [ZFS Best Practices Guide](#)
- [ZFS Administration Guide](#)
- [Becoming a ZFS Ninja \(video\)](#)

ZFS version numbers change as features are introduced and are incremental, meaning that a version includes all of the features introduced by previous versions. Table 1.1a summarizes various ZFS versions, the features which were added by that ZFS version, and in which version of FreeNAS™ that ZFS version was introduced. Recent versions of FreeNAS™ .7.x use ZFS version 13 which is why you can't downgrade a ZFS volume from FreeNAS™ 8.x to FreeNAS™ .7.x. FreeNAS™ 8.0.3 uses ZFS version 15, meaning that it includes all of the features that were introduced between versions 13 to 15.

**Table 1.1a: Summary of ZFS Versions**

ZFS Version	Features Added	FreeNAS™ Version
10	cache devices	.7.x
11	improved scrub performance	.7.x
12	snapshot properties	.7.x
13	snapused property	.7.x
14	passthrough-x aclinherit property	8.0
15	user and group space accounting	8.0
16	STMF property support	on roadmap
17	RAIDZ3	on roadmap
18	snapshot user holds	on roadmap
19	log device removal	on roadmap
20	compression using zle (zero-length encoding)	on roadmap
21	deduplication	on roadmap
22	received properties	on roadmap
23	deferred update (slim ZIL)	on roadmap
24	system attributes	on roadmap
25	improved scrub stats	on roadmap
26	improved snapshot deletion performance	on roadmap
27	improved snapshot creation performance	on roadmap

ZFS Version	Features Added	FreeNAS™ Version
28	multiple vdev replacements	on roadmap
30	encryption	Oracle has not released as open source

ZFS uses the [ZIL](#) (ZFS Intent Log) to manage writes. If you are using VMWare, the speed of the ZIL device is essentially the write performance bottleneck when using NFS. In this scenario, iSCSI will perform better than NFS. If you decide to create a dedicated cache device to speed up NFS writes, it can be half the size of system RAM as anything larger than that is unused capacity. Mirroring the ZIL device won't increase the speed, but it will help performance and reliability if one of the drives fails.

## 1.2 What's New

The FreeNAS™ 8 series represents an entire rewrite from the .7 series of FreeNAS™. In other words, FreeNAS™ was rewritten from scratch and features were added as the new base stabilized. This means that not every feature in the .7 series was re-implemented and some features that are not available in FreeNAS™ .7 are available in FreeNAS™ 8.x. Notable differences between the two implementations are as follows:

- versioning numbers have changed with the intent to have the version number reflect the base version of FreeBSD. FreeNAS™ 8.0.3 is based on FreeBSD 8.2; as the 8 branch of FreeNAS™ becomes feature complete, its version number will increment to 8.2.
- based on [NanoBSD](#) rather than [m0n0wall](#)
- design was changed from monolithic to modularized to allow for the creation of plugins so that users can install and configure only the modules they need
- GUI rewritten in Django to allow for future expansion
- new GUI is the default with the original GUI still available by entering the appname after the FreeNAS™ system's URL (e.g. <http://192.168.1.1/services>)
- improved management of ownership/group/permissions of volumes and datasets
- ZFS parameters per dataset, such as quotas, were added
- LSI 6 gbps HBAs are now supported
- migrated to rc.d init system
- ports updated to FreeBSD 8.2
- iSCSI support added
- support for 3ware 6bps RAID controllers has been added along with the CLI utility **tw\_cli** for managing 3ware RAID controllers
- added the ability to create periodic snapshot jobs, create one-time snapshots, clone snapshots which can then be exported as shares like any other dataset, and rollback to a previous snapshot

## 1.3 Features

Notable features in FreeNAS™ 8.0.3 include:

- supports AFP, CIFS, FTP, NFS, SSH (including SFTP), and TFTP as file sharing mechanisms
- supports exporting file or device extents via iSCSI
- supports Active Directory or LDAP for user authentication
- supports UFS2 based volumes, including gmirror, gstripe, and graid3
- supports ZFS as the primary filesystem, enabling many features not available in UFS2 such as quotas, snapshots, compression, replication, and datasets for sharing subsets of volumes
- upgrade procedure takes advantage of NanoBSD by writing the operating system to an inactive partition, allowing for an easy reversal of an undesirable upgrade
- automatic system notifications about LSI RAID controller events (requires email service to be configured)
- Django-driven graphical user interface
- rsync configuration through the graphical interface
- cron management through the graphical interface
- menu localization
- the SCSI serial number can be set on a per target basis, fixing an issue where MMIO was seeing different FreeNAS™ servers as the same device
- multiple IPs can now be specified per iSCSI portal
- ssh daemon now logs to /var/log/auth.log
- CIFS now defaults to AIO enabled
- ZFS hot spare cutover helper application within GUI
- SMART monitoring in GUI
- UPS management in GUI
- USB 3.0 support
- ACLs and UNIX file system permissions work properly on both UFS and ZFS volumes
- periodic ZFS snapshots are now exported to CIFS shares and are visible in Windows as shadow copies
- read-only is enabled on creation of remote filesystem to prevent accidental writes to the replica which would break replication
- added [tmux](#), a BSD-licensed utility similar to GNU screen
- added [dmidecode](#) which can provide very useful hardware diagnostic information
- updated the version of Intel NIC drivers to handle Intel's latest round of hardware



- added support for Marvell MX2 SATA controllers, sold with some WD 3TB drives
- netatalk (AFP) is now compatible with OS X 10.7

## 1.4 Known Issues

Before installing FreeNAS™ you should be aware of the following known issues:

- **UPGRADES FROM FreeNAS™ 0.7x ARE UNSUPPORTED.** The system has no way to import configuration settings from 0.7x versions of FreeNAS™, but the volume importer should be able to handle volumes created with FreeNAS™ 0.7x. Please note that zpool upgrade is a one way street and upgraded volumes will not be usable with FreeNAS™ 0.7x.
- The ZFS upgrade procedure is non-reversible and must be run manually. Please do not upgrade your pools unless you are absolutely sure that you'll never want to go back to other systems. For clarity, zpool upgrade is a ONE-WAY street. There is no reversing it, and there is no way for a system with an older version of ZFS to access pools that have been upgraded.
- The iSCSI target does not support a configuration reload meaning that changes to the configuration restart the daemon.
- Disks with certain configurations can get probed by GEOM and become essentially unwritable without manual intervention. For instance, if you use disks that previously had a gmirror on them, the system may pick that up and the disks will be unavailable until the existing gmirror is stopped and destroyed.
- In a departure from FreeNAS™ 0.7x, the operating system drive can not be used as a component for a volume, nor can it be partitioned for sharing.
- Some Atom-based systems with Realtek GigE interfaces have network performance issues with FreeBSD 8.2.

## 1.5 Roadmap for 8.2

8.2 is expected to be released by the end of the first quarter of 2012. Originally, this release was to be named 8.1, but it was decided to change the upcoming release name to 8.2 to better reflect the FreeBSD version it is based upon.

Table 1.7 lists the features which are currently being worked on and should be implemented for the 8.2 release:

**Table 1.7: 8.2 Features Roadmap**

Feature	Status	Notes
migration utility from .7 to 8.x		
rsync over SSH	committed	
plugin system which will allow the installation of additional applications through the <a href="#">PBI system</a>	in-progress	



Feature	Status	Notes
UPS client		
Wake on LAN support		
split NTP server and options into several fields in the GUI	committed	
SNMP connection to UPS	committed (and available to some degree via nut in 8.0.3)	
transmission support	committed	GUI and plugin support still not enabled
uPnP/DAAP/DLNA support		<a href="#">firefly</a> support committed; GUI / plugin support still not enabled <a href="#">minidlna</a> support committed; GUI / plugin support still not enabled

The following features will not make it into 8.2 and are being considered for a later version of FreeNAS™:

- encryption (with GELI?)
- automated mechanism for error reporting and user feedback
- more detailed system information
- network bandwidth reporting
- Unison

## 2 Installing FreeNAS™

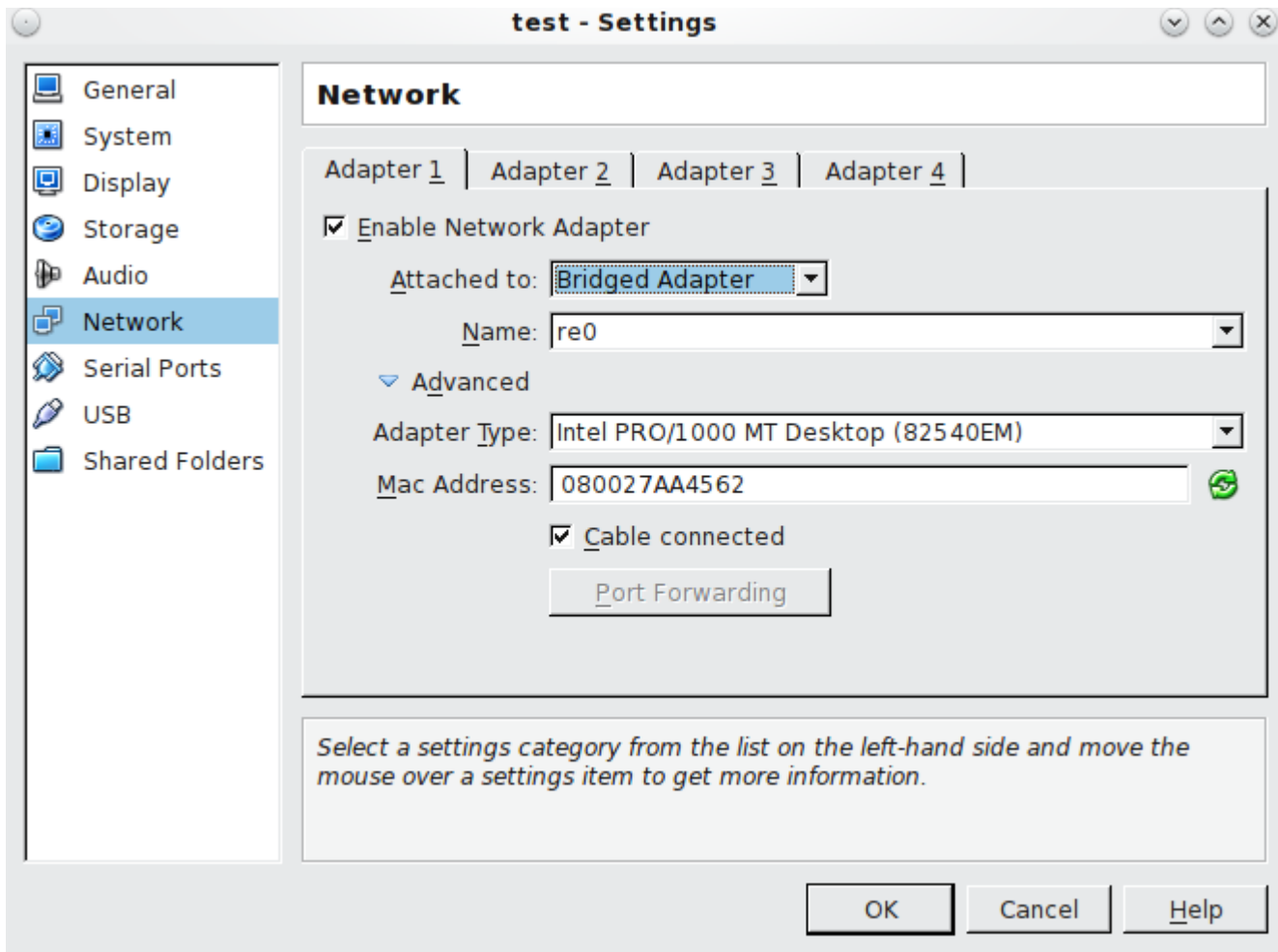
Before installing, it is important to remember that the FreeNAS™ operating system must be installed on a separate device from the drive(s) that will hold the storage data. In other words, if you only have one disk drive you will be able to use the FreeNAS™ graphical interface but won't be able to store any data, which after all, is the whole point of a NAS system. If you are a home user who is experimenting with FreeNAS™, you can install FreeNAS™ on an inexpensive USB thumb drive and use the computer's disk(s) for storage.

This section describes how to:

- [Getting FreeNAS™](#)
- [Installing from CDROM](#)
- [Installing from the Image](#)
- [Initial Setup](#)
- [Upgrading FreeNAS™](#)

If you are installing FreeNAS™ into a VirtualBox as a testing environment, you will need to configure the vbox interface for bridging in order to access the FreeNAS™ GUI through a web browser. To do this in VirtualBox, go to Settings -> Network. In the Attached to drop-down menu select Bridged Adapter and select the name of the physical interface from the Name drop-down menu. In the example shown in Figure 2a, the Intel Pro/1000 Ethernet card is attached to the network and has a device name of re0.

**Figure 2a: Configuring a Bridged Adapter in VirtualBox**



You will also need to create at least 2 virtual disks: the primary master should be **at least 4 GB in size** to hold the operating system and swap and the other virtual disk(s) can be used as data storage.

## 2.1 Getting FreeNAS™

FreeNAS™ 8.0.3 can be downloaded from the [FreeNAS-8 Sourceforge page](#). FreeNAS™ is available for 32-bit (x386) and 64-bit (x64) architectures. You should download the architecture type that matches your CPU's capabilities..

The download page contains the following types of files:

- **GUI\_upgrade.xz:** this is a compressed firmware upgrade image and requires a previous installation of FreeNAS™ 8.x. If your intent is to upgrade FreeNAS™, download the correct .xz file for your architecture and see [section 2.5 Upgrading FreeNAS™](#).
- **Full\_Install.xz:** this is a compressed image of the full image disk that needs to be written to a USB or compact flash device. [Section 2.3 Installing from the Image](#) describes how to use this image.
- **.iso:** this is a bootable image that can be written to CDROM. Installing from the CDROM is described in more detail in the next section.

The download directory also contains a ReleaseNotes for that version of FreeNAS™. This file contains the changes introduced by that release, any known issues, and the SHA256 checksums of the files in the download directory. The command you use to verify the checksum varies by operating system:

- on a BSD system use the command **sha256 name\_of\_file**
- on a Linux system use the command **sha256sum name\_of\_file**
- on a Mac system use the command **shasum -a 256 name\_of\_file**
- on a Windows system install a utility such as [HashCalc](#) or [HashTab](#) (which is also available for Mac)

## 2.2 Installing from CDROM

If you prefer to install FreeNAS™ using a menu-driven installer, download the ISO image that matches the architecture of the system you will install onto (32 or 64 bit) and burn it to a CDROM.

**NOTE:** the installer on the CDROM will recognize if a previous version of FreeNAS™ 8.x is already installed, meaning the CDROM can also be used to upgrade FreeNAS™. However, the installer can not perform an upgrade from a FreeNAS™ 7.x system.

Insert the CDROM into the system and boot from it. Once the media has finished booting, you will be presented with the console setup menu seen in Figure 2.2a.

**NOTE:** if the installer does not boot, check that the CD drive is listed first in the boot order in the BIOS. Some motherboards may require you to connect the CD-ROM to SATA0 (the first connector) in order to boot from CD-ROM. If it stalls during boot, check the SHA256 hash of your ISO against that listed in the README file; if the hash does not match, re-download the file. If the hash is correct, try reburning the CD at a lower speed.

Press enter to select the default option of “1 Install/Upgrade to hard drive/flash device, etc.”. The next menu, seen in Figure 2.2b, will list all available drives, including any inserted USB thumb drives which will begin with "da". In this example, the user is installing into VirtualBox and has created a 4GB virtual disk to hold the operating system.

Use your arrow keys to highlight the USB or compact flash device then tab to OK and press enter. FreeNAS™ will issue the warning seen in Figure 2.2c, reminding you not to install on a hard drive.

Figure 2.2a: FreeNAS™ Console Setup



Figure 2.2b: Selecting Which Drive to Install Into

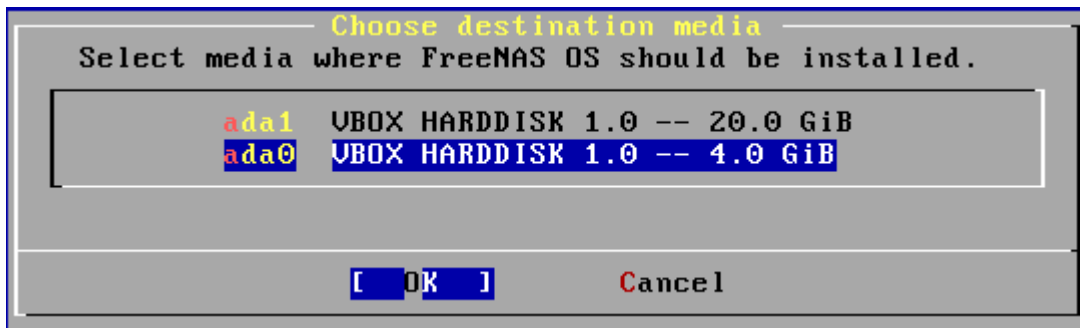
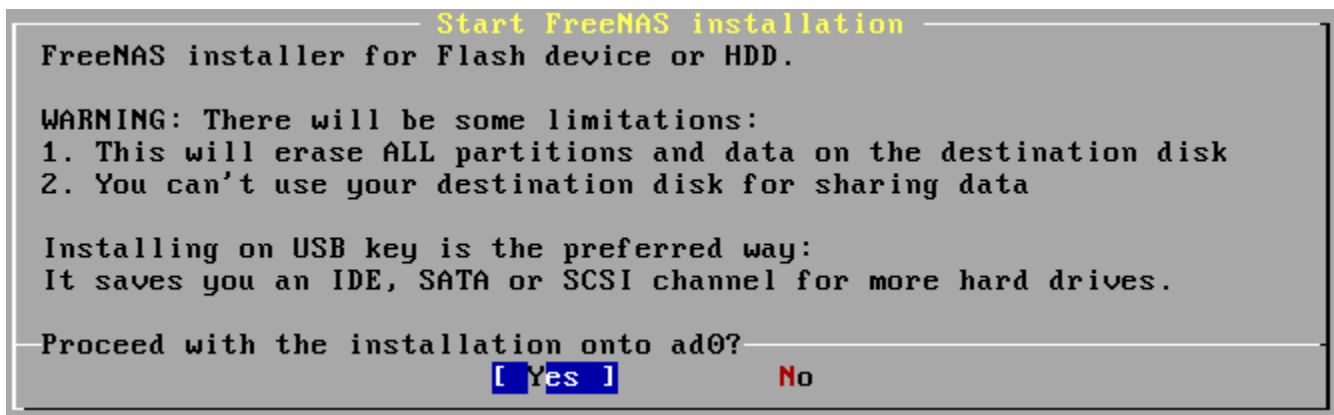
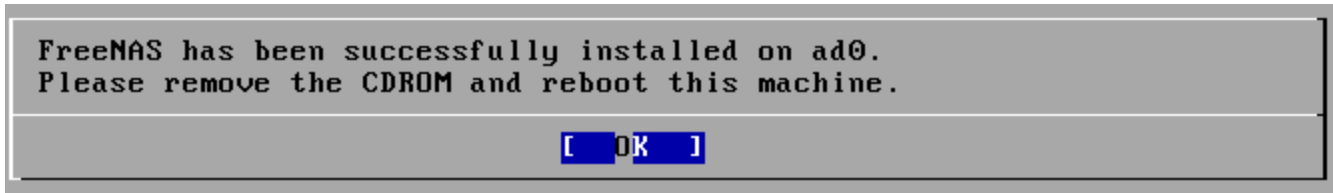


Figure 2.2c: FreeNAS™ Warning on Why You Should Install onto USB Flash Drive



Press enter and FreeNAS™ will extract the running image from the ISO and transfer it to the device. Once the installation is complete, you should see the message in Figure 2.2d.

**Figure 2.2d: FreeNAS™ Installation Complete**



Press enter and you'll return to the first menu, seen in Figure 2.2a. Highlight “3 Reboot System” and press enter. Remove the CDROM. If you installed onto a USB thumb drive, leave the thumb drive inserted. Make sure that the device you installed to is listed as the first boot entry in the BIOS so that the system will boot from it. FreeNAS™ should now be able to boot into the Console setup menu described in [section 2.4 Initial Setup](#).

## 2.3 Installing from the Image

If your system does not have a CDROM or you prefer to manually write the running image, download the `Full_Install.xz` file. This file will need to be uncompressed and then written to a CF card or USB thumbdrive that is 2GB or larger.

**NOTE:** any data currently saved on the flash device will be erased. If you are writing the image to a CF card, make sure that it is MSDOS formatted.

**DANGER!** The `dd` command is very powerful and can destroy any existing data on the specified device. Be *very sure* that you know the device name representing the USB thumb drive and make sure you do not typo the device name when using `dd`!

### 2.3.1 Using `xzcat` and `dd` on a FreeBSD or Linux System

On a FreeBSD or Linux system, the `xzcat` and `dd` commands can be used to uncompress and write the `.xz` image to an inserted USB thumb drive or compact flash device. Example 2.3a demonstrates writing the image to the first USB device (`/dev/da0`) on a FreeBSD system. Substitute the filename of your ISO and the device name representing the device to write to on your system.

#### Example 2.3a: Writing the `Full_Install` Image to a USB Thumb Drive

```
xzcat FreeNAS-8.0.3-RELEASE-x64-Full_Install.xz | dd of=/dev/da0 bs=64k
0+244141 records in
0+244141 records out
2000000000 bytes transferred in 326.345666 secs (6128471 bytes/sec)
```

When using the `dd` command:

- `of=` refers to the output file; in our case, the device name of the flash card or removable USB drive. You may have to increment the number in the name if it is not the first USB device. On Linux, use `/dev/sda` to refer to the first USB device.
- `bs=` refers to the block size

### 2.3.2 Using Keka and dd on an OS X System

On an OS X system, you can download and install [Keka](#) to uncompress the image. In FINDER, navigate to the location where you saved the downloaded .xz file. Shift+Click (or right-click) on the .xz file and select 'Open With Keka'. After a few minutes you'll have a large file with the same name, but no extension.

Insert the USB thumb drive and go to Launchpad -> Utilities -> Disk Utility. Unmount any mounted partitions on the USB thumb drive. Check that the USB thumb drive has only one partition (if not you will get GPT partition table errors on boot). Use Disk Utility to setup one partition on the USB drive; "free space" works fine.

Next, determine the device name of the inserted USB thumb drive. From TERMINAL, navigate to your Desktop then type this command:

```
diskutil - list
```

This will show you what devices are available to the system. Locate your USB stick and record the path. If you are not sure which path is the correct one for the USB stick, remove the device, run the command again, and compare the difference. Once you are sure of the device name, navigate to the Desktop from TERMINAL and use the **dd** command with the USB stick inserted. In Example 2.3b, the USB thumb drive is `/dev/disk8`. Substitute the name of your uncompressed file and the correct path to your USB thumb drive.

#### Example 2.3b: Using dd on an OS X System

```
dd if=FreeNAS-8.0.3-RELEASE-x64-Full_Install of=/dev/disk8 bs=64k
```

**NOTE:** If you get the error "Resource busy" when you run the **dd** command, go to Applications -> Utilities -> Disk Utility, find your USB thumb drive, and click on its partitions to make sure all of them are unmounted.

The **dd** command will take some minutes to complete. Wait until you get a prompt back and a message that displays how long it took to write the image to the USB drive.

Once you have a running image, make sure the boot order in the BIOS is set to boot from the device containing the image and boot the system. It should boot into the Console setup menu described in [section 2.4 Initial Setup](#).

**NOTE:** if the image does not boot, check the BIOS and 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. Some users have also found that some cheap 2GB USB sticks don't work as they are not really 2GB in size, but changing to a 4GB stick fixes the problem.

### 2.3.3 Using physdiskwrite on Windows

Windows users will need to download a utility that can uncompress xz files and a utility that can create a USB bootable image. A detailed how-to for using 7zip and physdiskwrite can be found in the forum post [How to write the embedded FreeNAS 8 image under Windows](#).

## 2.4 Initial Setup

The first time you reboot into FreeNAS™, you will be presented with the Console Setup screen shown in Figure 2.4a.

**NOTE:** if you receive a boot error, check your BIOS settings to make sure that the device you installed FreeNAS™ to is listed first in the boot order. Also check the settings for that device. For example, a BIOS may require you to change from floppy emulation mode to hard disk mode. If your BIOS is too old to support a USB boot device, see if a BIOS update is available. If you receive a "primary GPT is corrupt" error, you will need to use the **dd** command to remove both partition tables as described in this [forum post](#). You should then be able to reinstall FreeNAS™ and successfully boot into the new installation.

FreeNAS™ will automatically try to connect to a DHCP server on any live interfaces. If it successfully receives an IP address, it will display what IP address can be used to access the graphical console. In the example seen in Figure 2.4a, the FreeNAS™ system is accessible from `http://10.0.2.15`.

**Figure 2.4a: FreeNAS™ Console Setup Menu**

```
Mon Jun 27 11:48:27 PDT 2011
FreeBSD/i386 (freenas.local) (ttyv0)

Console setup
-----
1) Configure Network Interfaces
2) Configure Link Aggregation
3) Create VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset WebGUI login credentials
8) Reset to factory defaults
9) Shell
10) Reboot
11) Shutdown

You may try the following URLs to access the web user interface:
http://10.0.2.15/
Enter an option from 1-11: █
```

If your FreeNAS™ server is not connected to a network with a DHCP server, you will need to manually configure the interface as seen in Example 2.4a. In this example, the FreeNAS™ system has one network interface (*em0*).

## Example 2.4a: Manually Setting an IP Address from the Console Menu

```
Enter an option from 1-11: 1
1) em0
Select an interface (q to quit): 1
Delete existing config? (y/n) n
Configure interface for DHCP? (y/n) n
Configure IPv4? (y/n) y
Interface name: (press enter as 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
You may try the following URLs to access the web user interface:
http://192.168.1.108
```

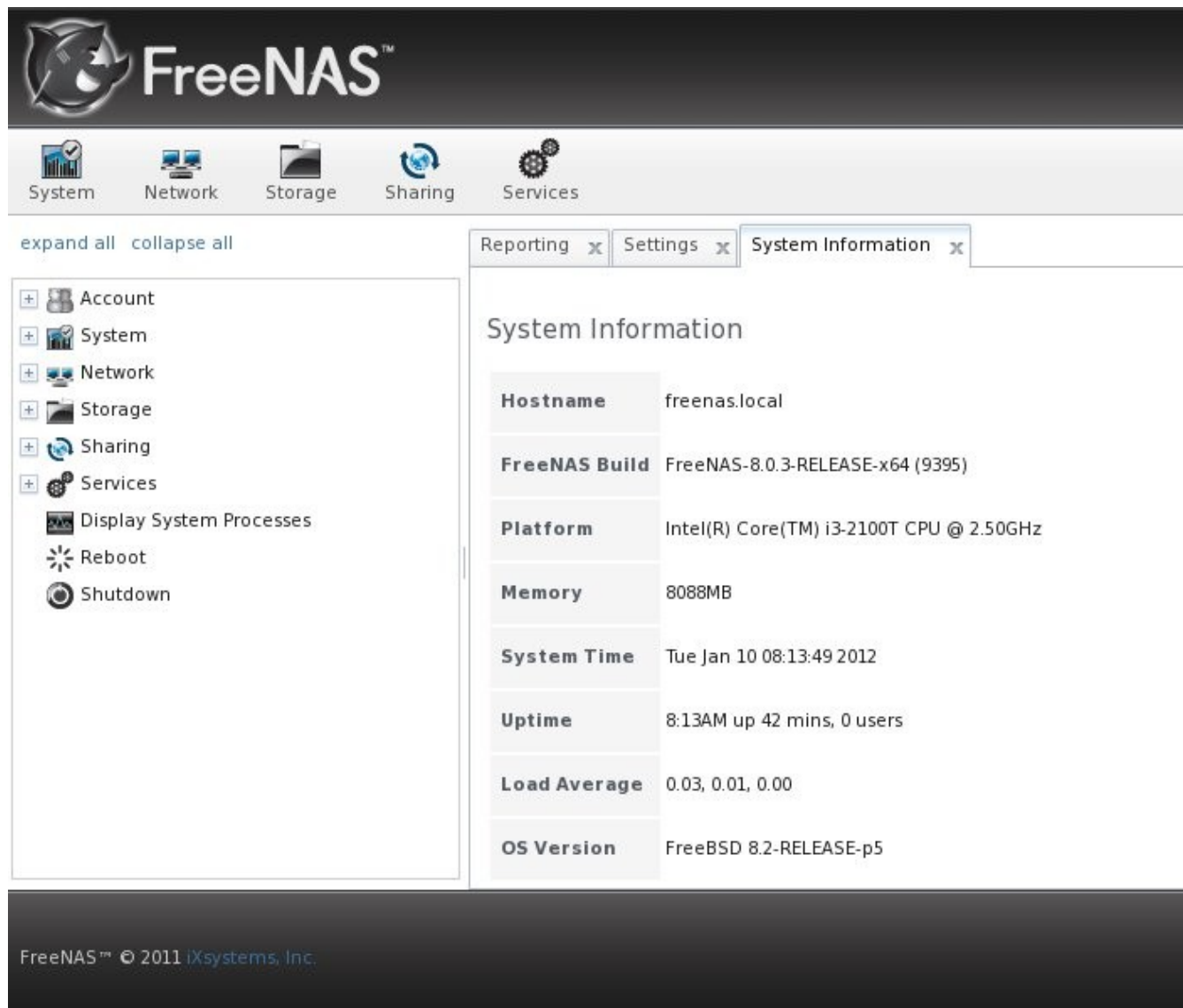
From another system with a graphical web browser, input the IP address for your FreeNAS™ installation. The administrative GUI, shown in Figure 2.4b should be displayed. If it does not appear, check that your browser configuration does not have any proxy settings enabled. If it does, disable them and try again. Also, IE9 has known issues. If you can't login using Internet Explorer, use [Firefox](#) instead.

**NOTE:** earlier versions of FreeNAS™ 8 required you to login using the default credentials of *admin* for the username and *freenas* for the password.

If you click the flashing Alert icon in the upper right corner, it will alert you that you should immediately change the password for the admin user as currently no password is required to login. You can do so in Account -> My Account -> Change Password. Once you do so, the Alert icon will change to a solid green.



Figure 2.4b: FreeNAS™ Graphical Configuration Menu



## 2.5 Upgrading FreeNAS™

**NOTE:** Before performing an upgrade you must always backup your configuration file, system disk, and all of your data.

**UPGRADES FROM FreeNAS™ 0.7x ARE NOT SUPPORTED:** the system has no way to import configuration settings from 0.7 versions of FreeNAS™, nor is there any sort of volume importer yet that will preserve data on existing volumes. Attempting to upgrade from 0.7 will result in the loss of your configuration and data.

The image size was increased from 1GB to 2GB between 8.01-BETA2 and 8.0.1-BETA3. **THIS MEANS THAT A GUI UPGRADE FROM AN EARLIER 8.X VERSION TO AN 8.0.1-BETA3 OR HIGHER VERSION WILL FAIL.** However, a CD upgrade will succeed and will save all of your configuration settings. If you are unable to perform a CD upgrade, you will need to: 1) backup your

configuration using System -> Settings -> General -> Save Config; 2) perform a full install; and 3) restore your configuration using System -> Settings -> General -> Upload Config. The GUI upgrade can be used to upgrade a system from BETA3 to BETA4.

Beginning with FreeNAS™ 8.0, FreeNAS™ supports two operating systems on the operating system device: the current “running” operating system and, if you have performed an upgrade, your previous version of the operating system. When you upgrade, FreeNAS™ automatically backs up your configuration and preserves the initial operating system. This means that it is easy to rollback to the previous version and its configuration should you experience a problem with the upgraded version. The upgrade automatically configures the system to boot from the new operating system; a rollback configures the system to boot from the previous operating system. Should you ever be unable to boot into a newly upgraded operating system, simply select **F2** at the FREENAS™ console when you see this screen at the very beginning of the boot process:

```
F1 FreeBSD
F2 FreeBSD
Boot: F1
```

There are 2 ways to upgrade a FreeNAS™ 8.x system: from the ISO or from the xz file. Both methods are described below.

### 2.5.1 Using the ISO

To upgrade from the CDROM, download the latest version of the ISO image that matches the architecture of the system (32 or 64 bit) and burn it to a CDROM.

**NOTE:** the installer on the CDROM will recognize if a previous version of FreeNAS™ 8.x is already installed, meaning the CDROM can also be used to upgrade FreeNAS™. However, the installer can not perform an upgrade from a FreeNAS™ 7.x system.

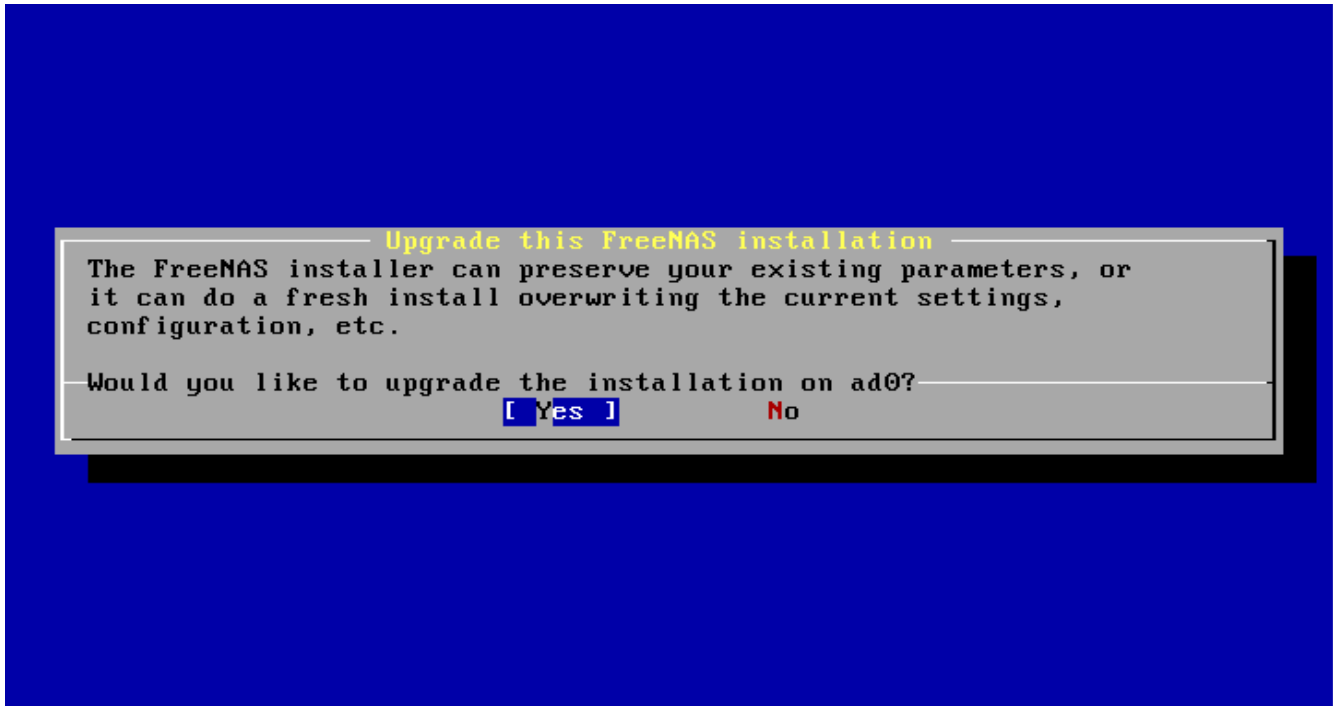
Insert the CDROM into the system and boot from it. Once the media has finished booting into the installation menu, press enter to select the default option of "1 Install/Upgrade to hard drive/flash device, etc." As with a fresh install, the installer will present a screen showing all available drives (see Figure 2.2b); select the drive FreeNAS™ is installed into and press enter.

The installer will recognize that an earlier version of FreeNAS™ is installed on the drive and will present the message shown in Figure 2.5a.

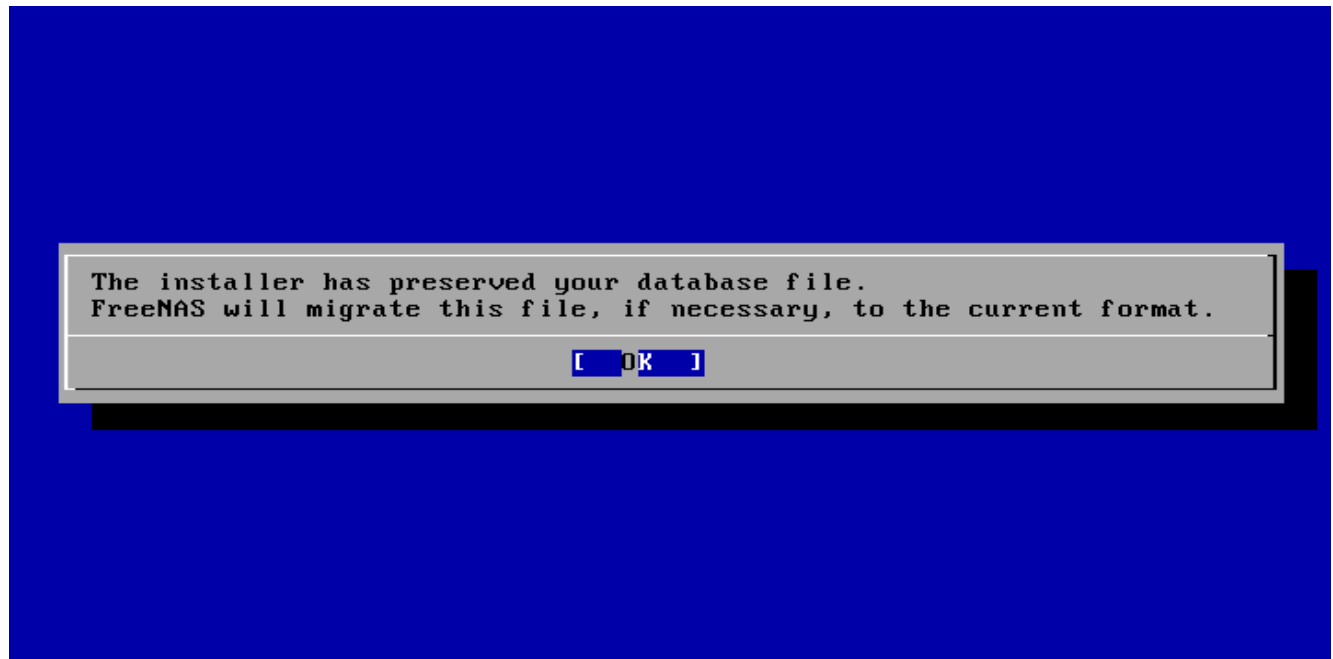
If you select NO at this screen, the installer will do a fresh install of the version on the CD rather than upgrading the previous version. To upgrade, press enter to accept the default of Yes. Again, the installer will remind you that the operating system should be installed on a thumb drive (seen in Figure 2.2c). Press enter to start the upgrade. Once the installer has finished unpacking the new image, you will see the menu shown in Figure 2.5b.

The database file that is preserved and migrated contains your FreeNAS™ configuration settings. Press enter and FreeNAS™ will indicate that the upgrade is complete and that you should reboot, as seen in Figure 2.5c.

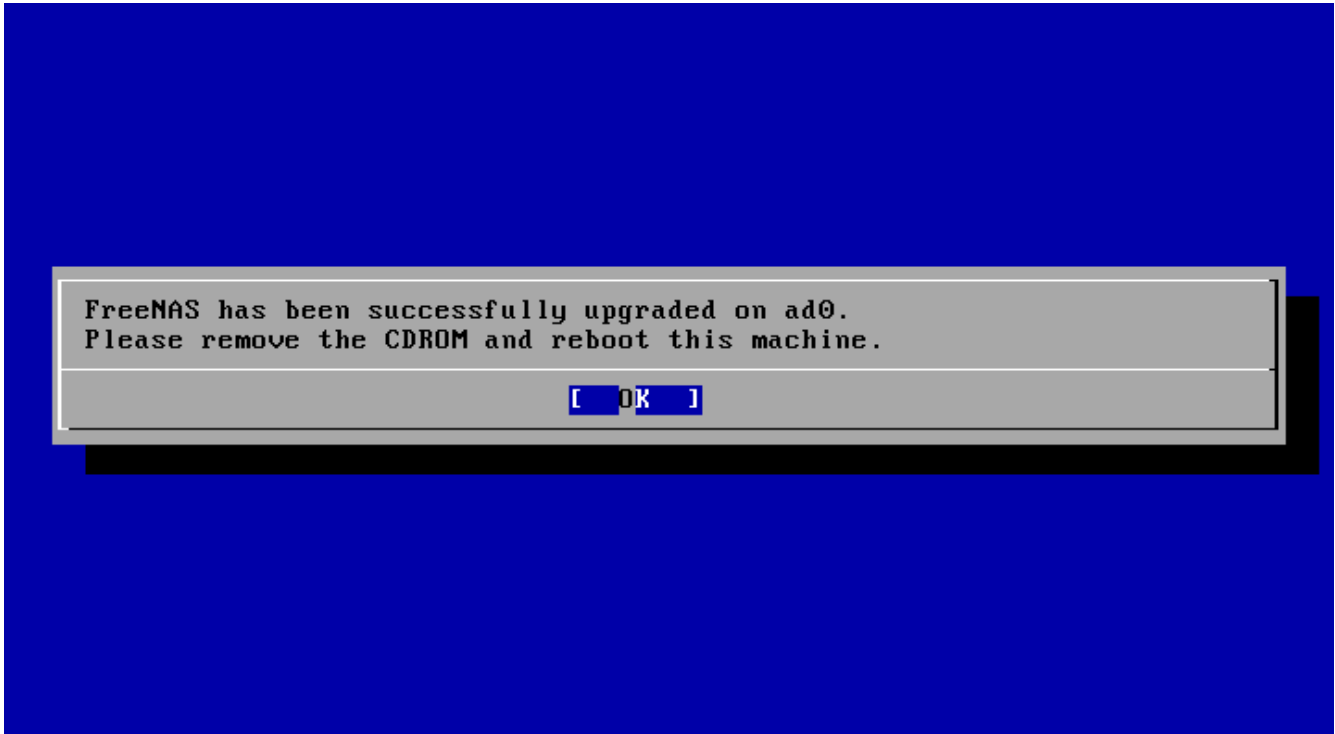
**Figure 2.5a: Upgrading a FreeNAS™ Installation**



**Figure 2.5b: FreeNAS™ will Preserve and Migrate Settings**



**Figure 2.5c: Upgrade is Complete**



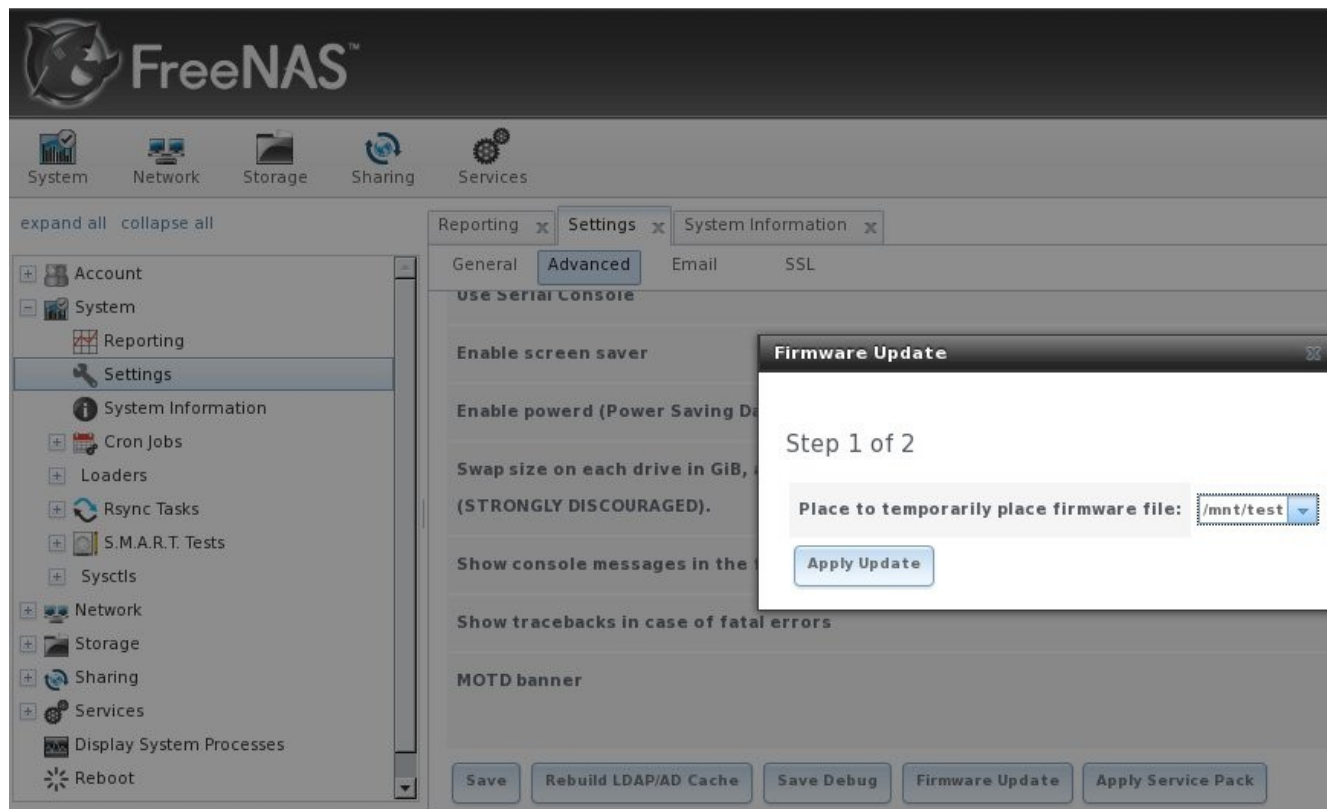
## 2.5.2 From the GUI

Before upgrading FreeNAS™:

1. Download the *\*.GUI\_upgrade.xz* image file that matches your architecture; download this file to the computer that you use to access the FreeNAS™ system.
2. Download the ReleaseNotes for that version; towards the bottom you will find the SHA256 hash for the *\*.GUI\_upgrade.xz* image file.
3. Backup the FreeNAS™ configuration in System -> Settings -> General -> Upload Config.
4. Warn all network users that the FreeNAS™ shares will be unavailable during the upgrade; you should schedule the upgrade for a time that will least impact users.
5. Stop all services in Services -> Control Services.
6. Go to System -> Settings -> Advanced, check the box “Show console messages in the footer (Requires UI reload)”, and refresh your browser. This way you can watch the progress of the upgrade until the first reboot.

To perform the upgrade, go to System -> Settings -> Advanced -> Firmware Update as shown in Figure 2.5d.

**Figure 2.5d: Upgrading FreeNAS™ From the GUI**



Use the drop-down menu to select a volume to temporarily place the firmware file during the upgrade, then click the Update button. You will be prompted to browse to the location of the downloaded .xz file and to paste the SHA256 sum. The SHA256 sum in the ReleaseNotes will look similar to this:

```
Filename :  
FreeNAS-8.0.3-RELEASE-x64-GUI_Upgrade.xz  
SHA256 Hash :  
cdcd02b2bc4cbd0b2bc92153ddc2f0f73780572f877789b21d6ef32135c7e3722b224
```

When finished, click the Apply Update button which will change to "please Wait...". Behind the scenes, the following steps are occurring:

- the SHA256 hash is confirmed and an error will display if it does not match; if you get this error, double-check that you pasted the correct checksum and try pasting again
- the new image is uncompressed and written to the USB compact or flash drive; this can take 10 to 15 minutes so be patient
- once the new image is written, you will momentarily lose your connection as the FreeNAS™ system will automatically reboot into the new version of the operating system
- FreeNAS™ will actually reboot twice: once the new operating system loads the upgrade process applies the new database schema and reboots again
- assuming all went well, the FreeNAS™ system will receive the same IP from the DHCP server; refresh your browser after a moment to see if you access the system

### 2.5.2.1 If Something Goes Wrong

If the FreeNAS™ system does not become available after the upgrade, you will need physical access to the system to find out what went wrong. From the console menu you can determine if it received an IP address and use option "1) Configure Network Interfaces" if it did not.

If this does not fix the problem, go into option "9) Shell" and read the system log with this command:

```
more /var/log/messages
```

If the problem is not obvious or you are unsure how to fix it, see [section 10 FreeNAS Support Resources](#).

If the system remains inaccessible and you wish to revert back to the previous installation, type **reboot** from the shell or select "10) Reboot" from the console menu. Watch the boot screens and press F2 when you see this menu:

```
F1 FreeBSD  
F2 FreeBSD  
Boot: F1
```

## Section 2: Using the Graphical Interface

This section of the Guide describes all of the configuration screens available within the FreeNAS™ graphical administrative interface. The screens are listed in the order that they appear within the tree, or the left frame of the GUI.

**NOTE:** It is important to use the GUI (or the console) for all configuration changes. FreeNAS™ uses a configuration database to store its settings. While you can use the command line to modify your configuration, changes made at the command line are not written to the configuration database. This means that any changes made at the command line will not persist after a reboot and will be overwritten by the values in the configuration database during an upgrade.

## 3 Account Configuration

The account section of the GUI allows you to change the administrative password and manage users and groups.

FreeNAS™ supports users, groups, and permissions, allowing great flexibility in configuring which users have access to the data stored on FreeNAS.™ Before you can assign permissions which will be used by shares, you will need to do one of the following:

1. Create one guest account that all users will use. OR
2. Create a user account for every user in the network where the name of each account is the same as a logon name used on a computer. For example, if a Windows system has a login name of bobsmith, you should create a user account with the name bobsmith on FreeNAS™. If your intent is to assign groups of users different permissions to shares, you will need to also create groups and assign users to the groups. OR
3. If your network uses Active Directory to manage user accounts and permissions, enable the Active Directory service.

This section describes how to manage the administrative account, users, and groups using the FreeNAS™ GUI.

### 3.1 My Account

By default no password is required to access the FreeNAS™ administrative interface using the built-in *admin* account. For security reasons, you should immediately change the default administrative account name and set a password for that account. To change the administrative account name, go to Account -> My Account -> Change Admin User. This will open the screen shown in Figure 3.1a.

**Figure 3.1a: Changing the FreeNAS™ Administrative Account**



Replace *admin* with the name of the account that will be used to login to the FreeNAS™ system. The First and Last name fields are optional. Click the Change Admin User to save your changes.

**NOTE:** in FreeNAS™ the administrative account is not the same as the *root* user account. The administrative account is used to access the graphical administrative interface. This separation makes it possible to disable root logins while maintaining the ability of logging into the graphical administrative interface.

To change the password of the administrative account, click on Account -> My Account -> Change Password. This will open the screen shown in Figure 3.1b.

**Figure 3.1b: Setting the FreeNAS™ Administrative Password**



Since there is no default password, leave the old password field blank. Type in and confirm the password which will be used when accessing the graphical administrative interface. If you wish to allow root logins using the same password, leave the "Change root password as well" box checked. If you wish to use a different root password, uncheck this box and set the root password in Account -> Users -> View All Users -> root -> Change Password.

## 3.2 Groups

The Groups interface allows you to manage UNIX-style groups on the FreeNAS™ system. Creating a share that will be accessed by some users but not others is a three step process:

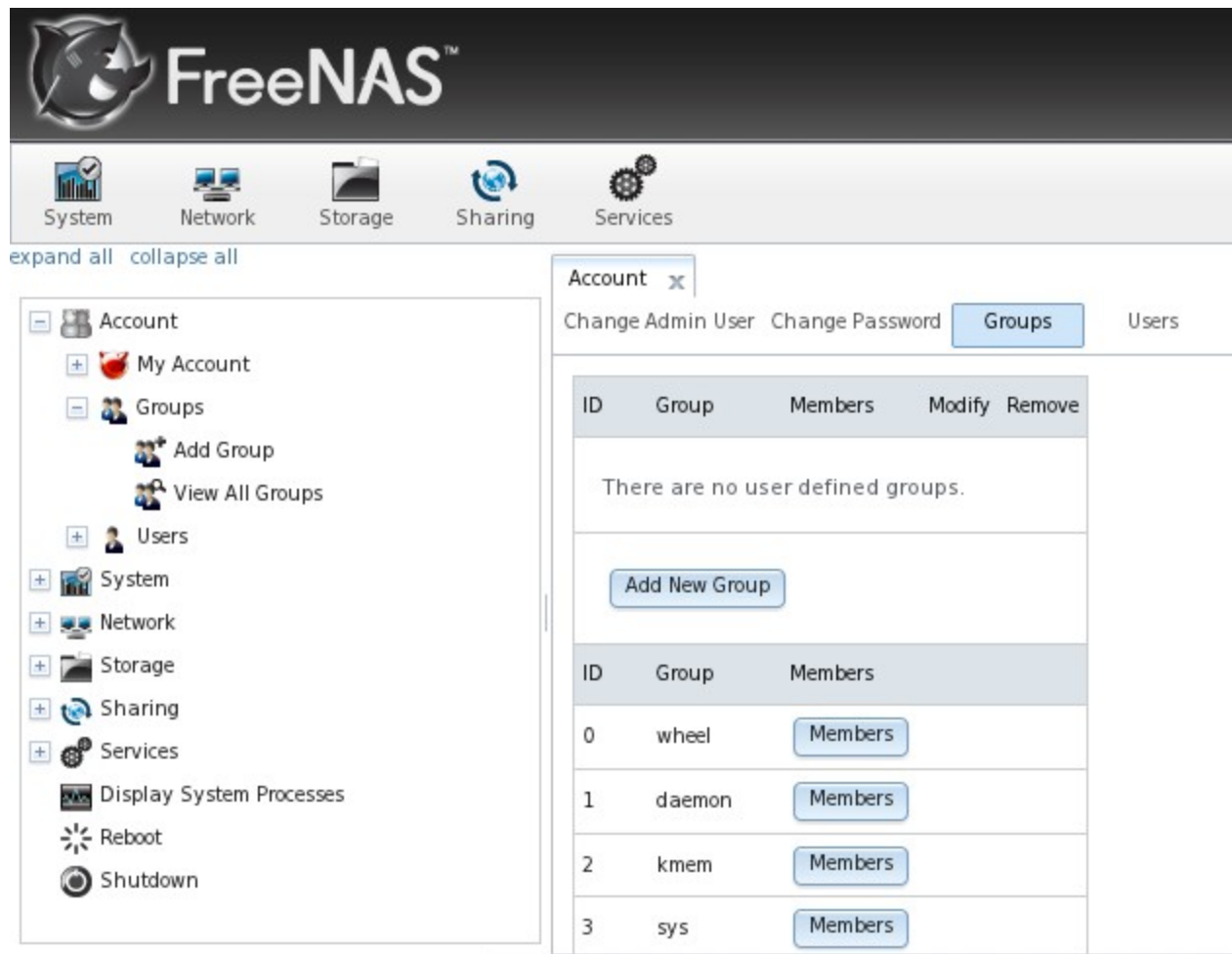
1. Create a user account for each user in Account -> Users -> Add User.
2. Add the user accounts to a group that you create in Account -> Groups -> Add Group.
3. In Storage -> create a volume or ZFS dataset and assign permission to the group for that volume or dataset.

This section describes step 2 or how to create the group and assign it user accounts. The next section will describe step 1 or how to create user accounts. [Section 6.3 Volumes](#) describes step 3 or how to create volumes/datasets and set their permissions.

If you click Groups -> View All Groups, you will see a screen similar to Figure 3.2a.



Figure 3.2a: FreeNAS™ Groups Management

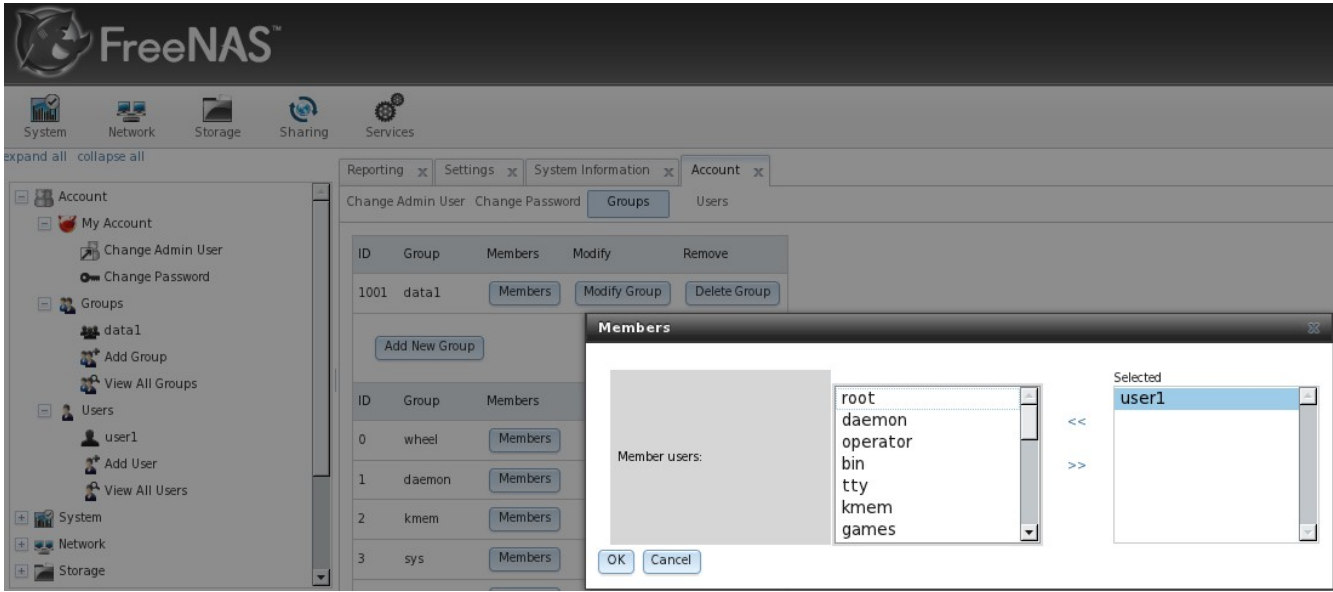


All groups that came with the operating system will be listed and the screen will indicate if any additional groups have been defined by the administrator. Each group has an entry indicating the group ID and group name; click the group's Members button to view and modify that group's membership.

If you click the Add New Group button, you will be prompted to enter the group's name. The next available group ID will be suggested for you, though you can change it to another value. By convention, UNIX groups containing user accounts have an ID greater than 1000 and groups required by a service have an ID equal to the default port number used by the service (e.g. the sshd group has an ID of 22).

Once the group and users are created, assign the users as members to the group. In the example shown in Figure 3.2b, a group called *data1* has been created and a user account named *user1* has also been created. Click on View All Groups then the Members button for the group you wish to assign users to. Highlight the user in the Member users list (which shows all user accounts on the system) and click the >> to move that user to the right frame. Whatever user accounts appear in the right frame will be members of that group.

**Figure 3.2b: Assigning a User as a Member of a Group**

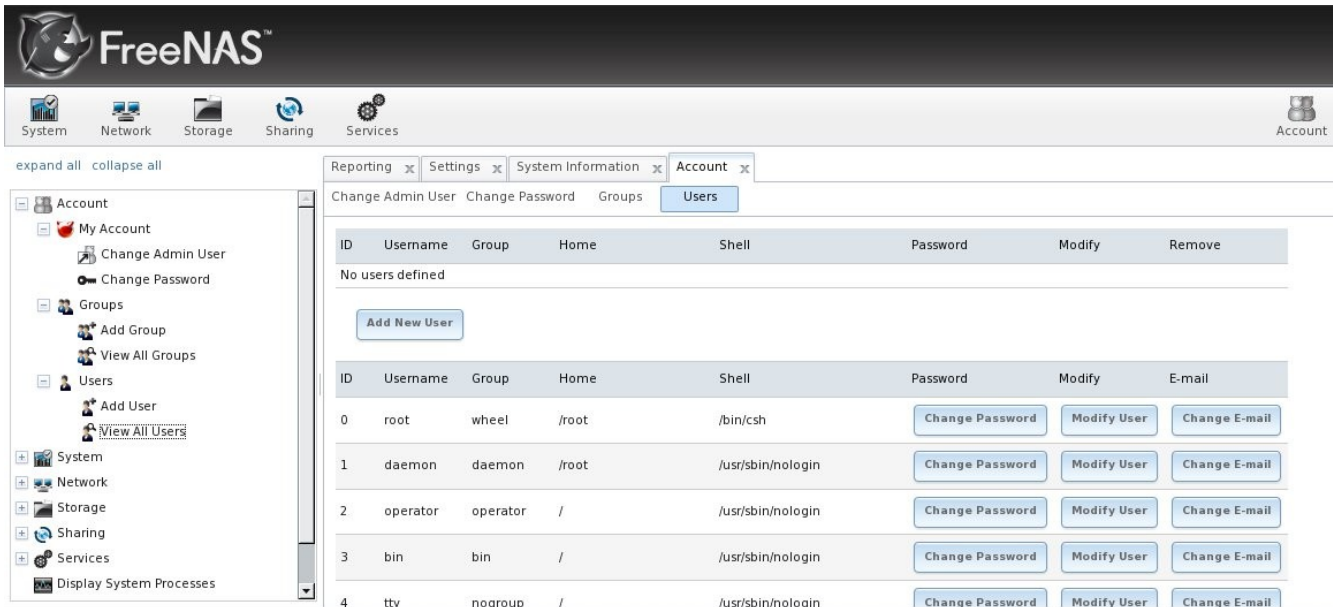


### 3.3 Users

If you wish to set permissions on your volumes or datasets, you will need to create at least one user account and assign that user account the required permissions. If you also wish to create groups to manage permissions, you should create the user accounts first, then assign the accounts as members of the groups. This section demonstrates how to create a user account.

If you click Account -> Users -> View All Users, you will see a listing of all of the user accounts that were created with the FreeNAS™ system, as shown in Figure 3.3a:

**Figure 3.3a: Managing User Accounts**



Each account entry indicates the user ID, account name, default group, home directory, default shell, and offers buttons to change the user's password, the user's account settings, and email address. Every user account, except for the root user, that came with the FreeNAS™ system is a system account. This means that it is used by a service and should not be available for use as a login account. For this reason, the default shell is [nologin\(8\)](#). For security reasons (and to prevent breakage of system services) you should not modify the system accounts.

**TIP:** for security reasons, you should change the root password from the default value.

To create a user account, click the Add New User button to open the screen shown in Figure 3.3b. Table 3.3a summarizes the options available in this screen.

**Figure 3.3b: Adding a User Account**

**Table 3.3a: User Account Configuration**

Setting	Value	Description
User ID	integer	can accept default; by convention, user accounts have an ID greater than 1000 and system accounts have an ID equal to the default port number used by the service
Username	string	maximum 30 characters, can include numerals, can not include a space; due to a limitation in FreeBSD, usernames that exceed 17 characters are unable to create cron jobs or be used in rsync tasks

Setting	Value	Description
Primary Group	drop-down menu	if left empty this will create a group with the same name; don't add to wheel group unless you mean to give superuser access; don't add to a system group unless you are creating a system account required by that group
Home Directory	string	needs to be changed to the name of an existing volume or dataset that the user will be assigned permission to access
Shell	drop-down menu	if creating a system account, choose nologin; if creating a user account, select shell of choice
Full Name	string	mandatory, may contain spaces
Password	string	mandatory unless check box to disable logins
Password confirmation	string	must match Password
Disable logins	checkbox	check this box for system accounts and for user accounts who aren't allowed to login to the FreeNAS™ system
SSH Public Key	string	paste the user's <b>public</b> key which can be used for SSH authentication (do not paste the private key!)
Lock user	checkbox	a checked box prevents user from logging in until the account is unlocked (box is unchecked)

## 4 System Configuration

The System icon contains the following tabs:

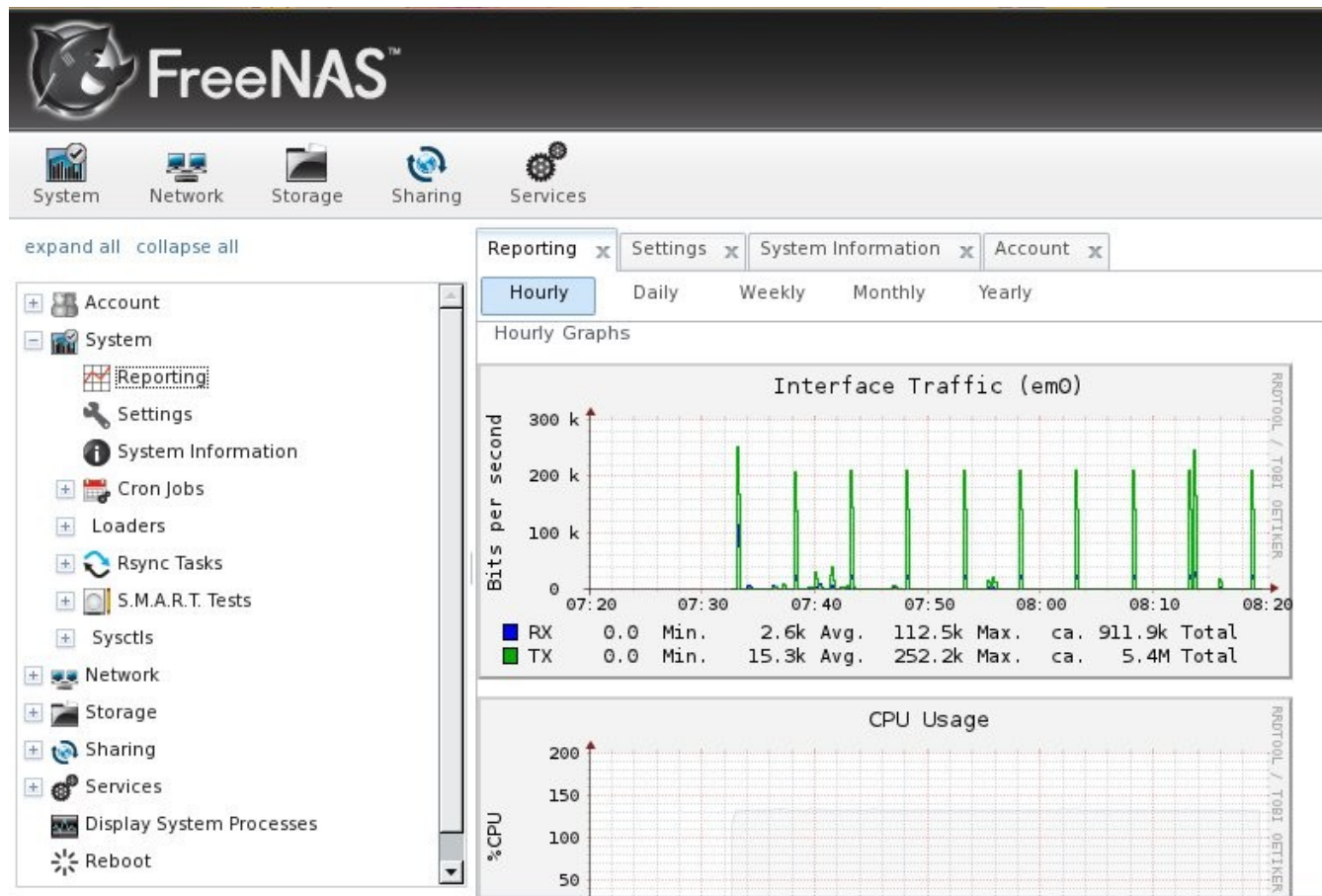
- **Reporting:** provides reports and graphs monitoring the system's CPU, disk capacity and other metrics.
- **Settings:** used to configure system wide settings such as timezone, email setup, HTTPS access and firmware upgrades.
- **System information:** provides general FreeNAS™ system information such as hostname, operating system version, platform and uptime.
- **CronJobs:** provides a graphical front-end to [crontab\(5\)](#).
- **Rsync Tasks:** allows you to schedule rsync tasks.
- **S.M.A.R.T. Tests:** allows you to schedule which S.M.A.R.T. tests to run on a per-disk basis.

Each of these is described in more detail in this section.

## 4.1 Reporting

If you click the Reporting tab, several graphs will load as seen in the example in Figure 4.1a.

**Figure 4.1a: Reporting Graphs Showing the Load on the System**

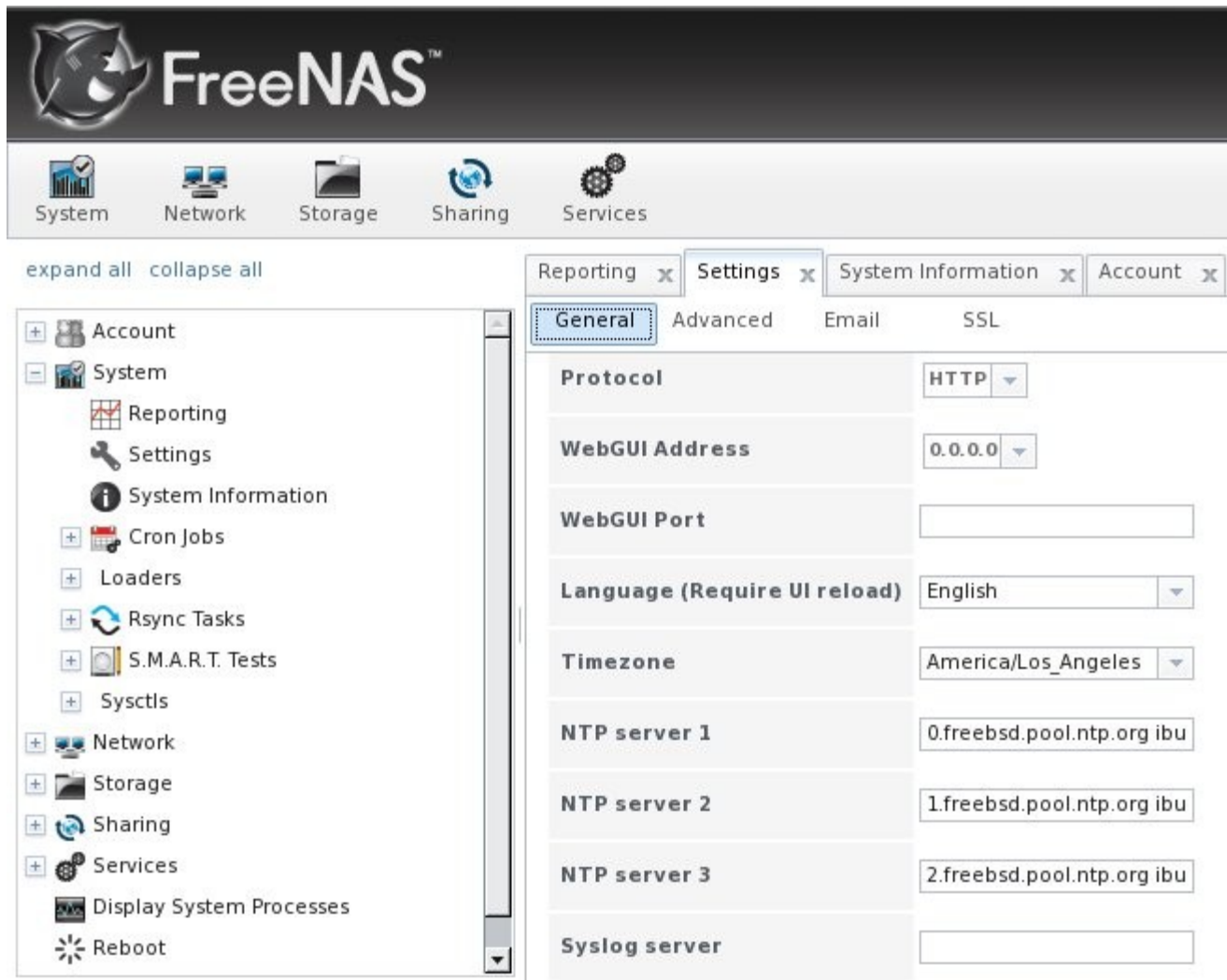


The graphs will display the current interface traffic (for each configured interface), CPU usage, physical memory utilization, system load, processes, swap utilization, and disk space (for each configured volume). Reporting data is saved, allowing you to view and monitor usage trends hourly, daily, weekly, monthly, and yearly.

## 4.2 Settings

The Settings tab, shown in Figure 4.2a, contains 4 tabs: General, Advanced, Email, and SSL.

**Figure 4.2a: General Tab of Settings**



### 4.2.1 General Tab

Table 4.2a summarizes the settings that can be configured using the General tab:

**Table 4.2a: General Tab's Configuration Settings**

Setting	Value	Description
Protocol	drop-down menu	protocol to use when connecting to the administrative GUI from a browser
WebGUI Address	drop-down menu	choose from a list of recent IP addresses for the one to use when accessing the administrative GUI; the built-in HTTP server will automatically bind to the wildcard address of 0.0.0.0 (any address) if the configured address becomes unavailable and issue an alert
WebGUI Port	integer	allows you to configure a non-standard port for accessing the administrative GUI

Setting	Value	Description
Language	drop-down menu	select the localization from the drop-down menu; requires a browser reload; you can view the status of localization at <a href="http://pootle.freenas.org">pootle.freenas.org</a>
Timezone	drop-down menu	select the timezone from the drop-down menu
NTP server	string	input the IP address or name of up to 3 NTP servers; options from <a href="#">ntp.conf(5)</a> such as “iburst maxpoll 9” can be included
Syslog server	IP address	allows you to send FreeNAS™ logs to specified remote syslog server

If you make any changes, click the Save button.

This tab also contains the following three buttons:

**Factory Restore:** replaces current configuration with the factory default. This means that all of your customizations will be erased, but can be handy if you mess up your system or wish to return a test system to the original configuration.

**Save Config:** allows you to browse to location to make a backup copy of the current configuration in the format *hostname-YYYYMMDDhhmmss.db*. You should always do this before upgrading your system.

**Upload Config:** allows you to browse to location of saved configuration file in order to restore that configuration.

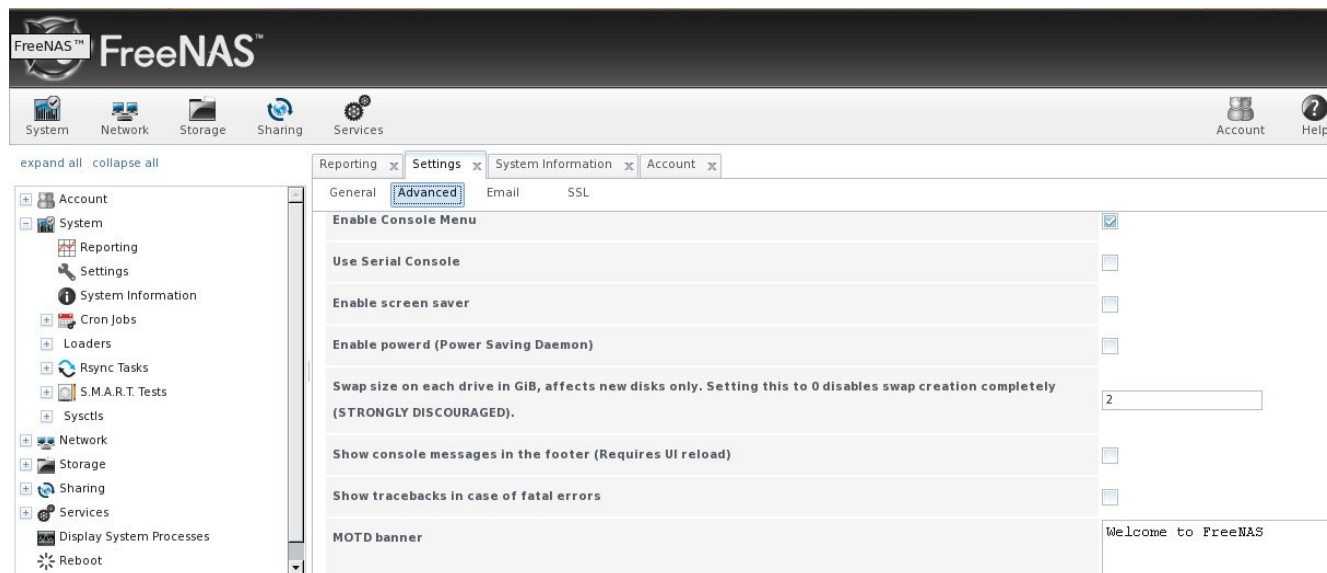
**NOTE:** If you intend to recreate volumes and restore the default configuration, delete the volumes first in Storage -> Volumes.

#### 4.2.2 Advanced Tab

The Advanced tab, shown in Figure 4.2b, allows you to set some miscellaneous settings on the FreeNAS™ system. The configurable settings are summarized in Table 4.2b.



**Figure 4.2b: Advanced Tab**



**Table 4.2b: Advanced Tab's Configuration Settings**

Setting	Value	Description
Enable Console Menu	checkbox	unchecking this box removes the console menu shown in Figure 2.4a
Use Serial Console	checkbox	do <b>not</b> check this box if your serial port is disabled
Enable screen saver	checkbox	enables/disables the console screen saver (see ticket <a href="#">566</a> )
Enable powerd (Power Saving Daemon)	checkbox	used to spin down disks, see <a href="#">powerd(8)</a> ; this <a href="#">forum post</a> demonstrates how to determine if a drive has spun down
Swap size	non-zero integer representing GB	effects new disks only
Show console messages in the footer	checkbox	requires you to refresh browser; will display console messages in real time at bottom of browser
Show tracebacks in case of fatal errors	checkbox	enable this when troubleshooting to get more diagnostic information to display in a GUI error message
MOTD banner	string	input the message you wish to be seen when user logs in via SSH

If you make any changes, click the Save button.

This tab also contains the following buttons:

**Rebuild LDAP/AD Cache:** click if you add a user to AD who needs immediate access to FreeNAS™; otherwise this occurs automatically once a day as a cron job.



**Save Debug:** creates a text file of diagnostic information which includes the FreeNAS™ version, the status of all services and their settings, the contents of all \*.conf files, the debug log, and hardware information.

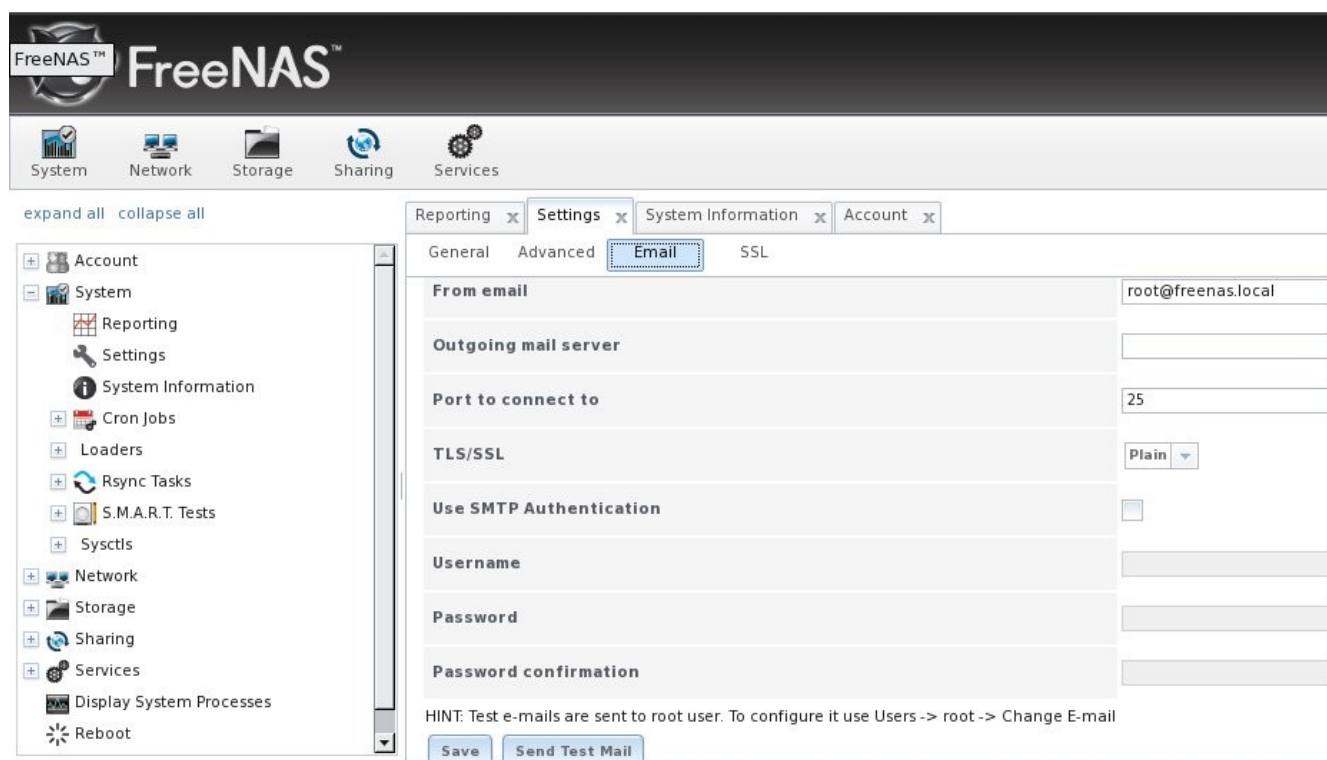
**Firmware Update:** used to Upgrade FreeNAS™. See [section 2.5.2 Upgrading FreeNAS™ From the GUI](#) for details.

**Apply Service Pack:** future versions of FreeNAS™ will provide service packs to address bugs and security fixes.

### 4.2.3 Email Tab

The Email tab, shown in Figure 4.2c, is used to configure the email settings on the FreeNAS™ system. Table 4.2c summarizes the settings that can be configured using the Email tab.

**Figure 4.2c: Email Tab**



**Table 4.2c: Email Tab's Configuration Settings**

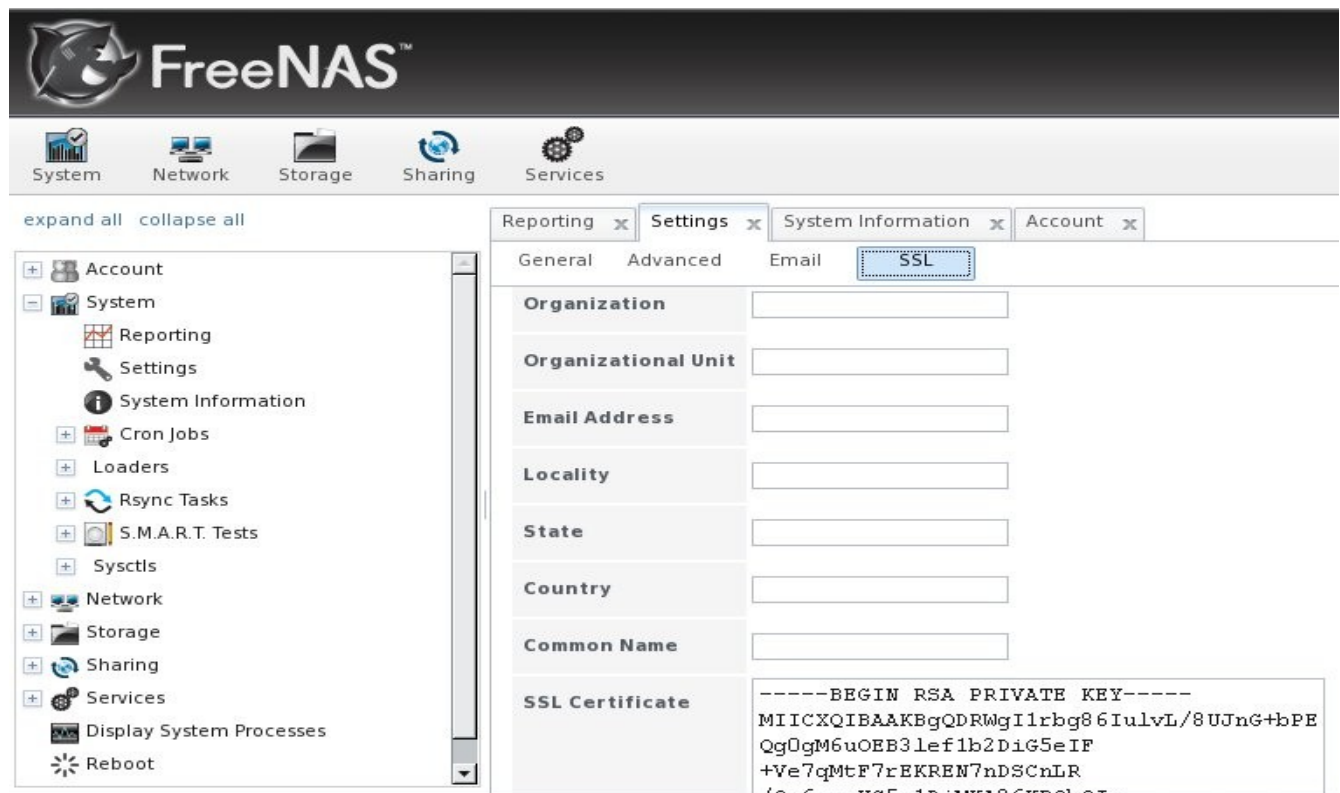
Setting	Value	Description
From email	string	the <b>From</b> email address to be used when sending email notifications; the <b>To</b> email address is sent to the root user account and you can set that email address by clicking the Change E-mail button for the root account in Accounts -> Users -> View All Users
Outgoing mail server	string or IP address	hostname or IP address of SMTP server

Setting	Value	Description
Port to connect to	integer	SMTP port number, typically 25, 465 (secure SMTP), or 587 (submission)
TLS/SSL	drop-down menu	encryption type; choices are plain, SSL, or TLS
Use SMTP Authentication	checkbox	enables/disables <a href="#">SMTP AUTH</a> using PLAIN SASL
Username	string	used to authenticate with SMTP server
Password	string	used to authenticate with SMTP server
Send Test Mail	button	click to check that configured email settings are working; this will fail if you do not set the <b>To</b> email address first

#### 4.2.4 SSL Tab

During installation, an unsigned RSA certificate and key are auto-generated for you. You can view these in System -> Settings -> SSL, as seen in Figure 4.2d. If you already have your own signed certificate that you wish to use for SSL/TLS connections, replace the values in the SSL certificate field with a copy/paste of your own key and certificate. The certificate can be used to secure the HTTP connection (enabled in the Settings -> General Tab) to the FreeNAS™ system, as well as to secure FTP connections (described in [section 8.6.4 Encrypting FTP](#)). Table 4.2d summarizes the settings that can be configured using the SSL tab. This [howto](#) shows how to generate a certificate using OpenSSL and provides some examples for the values shown in Table 4.2d.

Figure 4.2d: SSL Tab



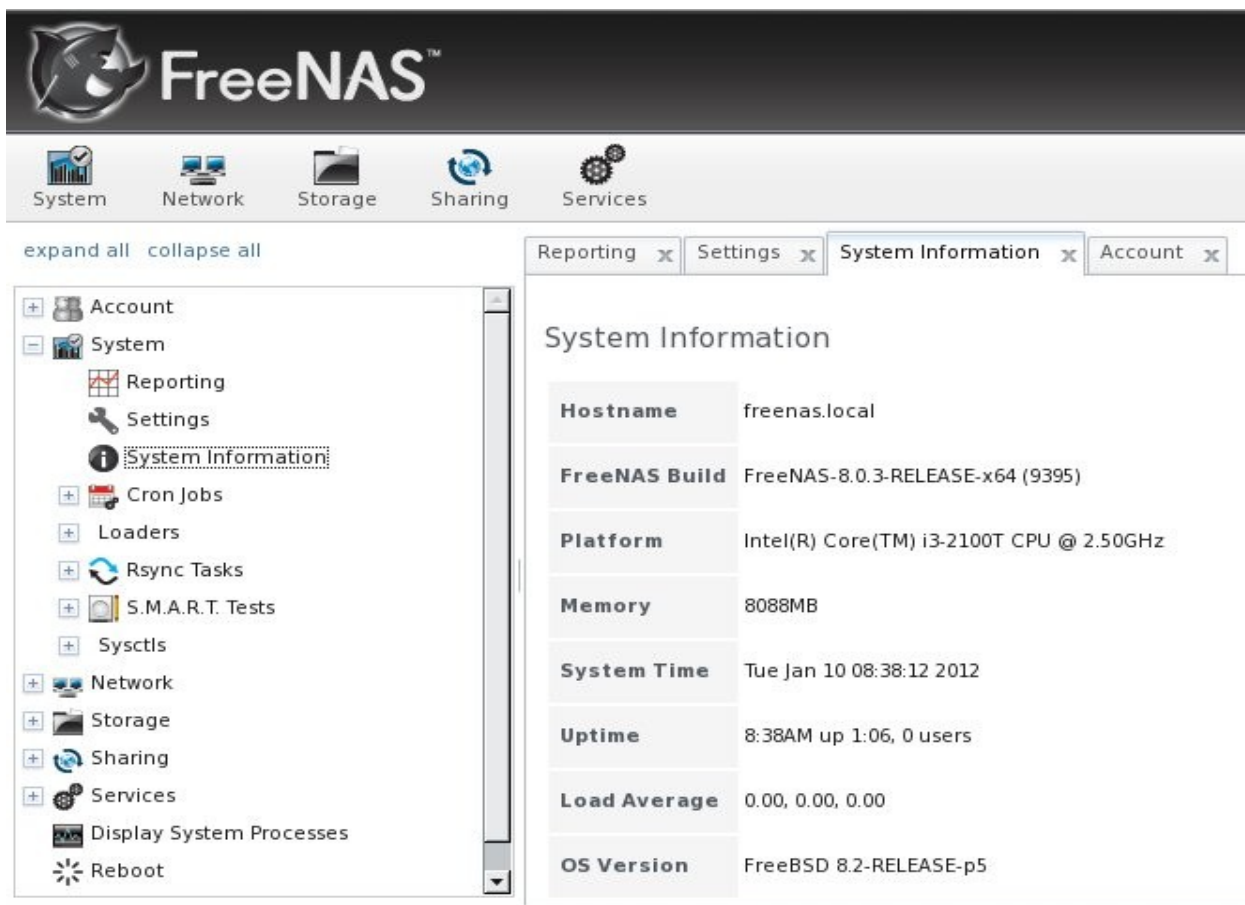
**Table 4.2d: SSL Tab's Configuration Settings**

Setting	Value	Description
Organization	string	optional
Organizational Unit	string	optional
Email Address	string	optional
Locality	string	optional
State	string	optional
Country	string	optional
Common Name	string	optional
SSL Certificate	string	paste the RSA private key and certificate into the box

### 4.3 System Information

The system information tab will display general information about the FreeNAS™ system. The information includes the hostname, underlying FreeBSD version, type of CPU (platform), the amount of memory, the current system time, the system's uptime, the current load average, and the FreeNAS™ build version. An example is seen in Figure 4.3a:

**Figure 4.3a: System Information Tab**



## 4.4 Cron Jobs

[cron\(8\)](#) is a daemon that runs a command or script on a regular schedule as a specified user. Typically, the user who wishes to schedule a task manually creates a [crontab\(5\)](#) using syntax that can be perplexing to new Unix users. The FreeNAS™ GUI makes it easy to schedule when you would like the task to occur.

**NOTE:** due to a limitation in FreeBSD, users with account names that exceed 17 characters are unable to create cron jobs.

Figure 4.4a shows the screen that opens when you click System -> Cron Jobs -> Add Cron Job.

**Figure 4.4a: Creating a Cron Job**

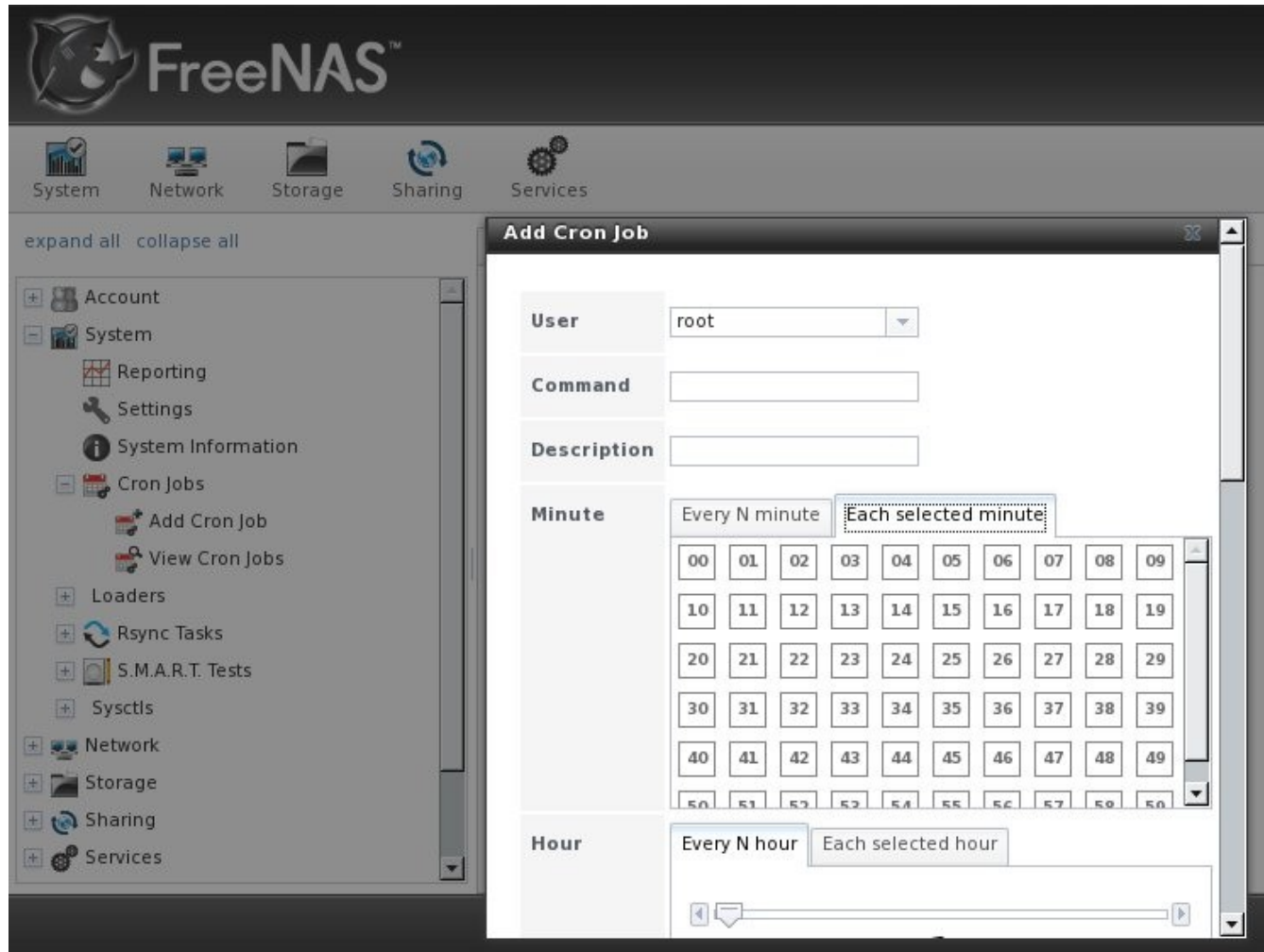


Table 4.4a summarizes the configurable options when creating a cron job.

**Table 4.4a: Cron Job Options**

Setting	Value	Description
User	drop-down menu	make sure the selected user has permission to run the specified command or script

Setting	Value	Description
Command	string	the full path to the command or script to be run; if it is a script, test it at the command line first to make sure that it works as expected
Description	string	optional
Minute	slider or checkboxes	if use the slider, cron job occurs every N minutes; if use check boxes, cron job occurs at the selected moments
Hour	slider or checkboxes	if use the slider, cron job occurs every N hours; if use check boxes, cron job occurs at the selected hours
Day of month	slider or checkboxes	if use the slider, cron job occurs every N days; if use check boxes, cron job occurs on the selected days of the selected months
Month	slider or checkboxes	if use the slider, cron job occurs every N months; if use check boxes, cron job occurs on the selected months
Day of week	slider or checkboxes	if use the slider, cron job occurs every N days; if use check boxes, cron job occurs on the selected days
Enabled	checkbox	uncheck if you would like to disable the cron job without deleting it

## 4.5 Loaders

When a FreeBSD-based system boots, [loader.conf\(5\)](#) is read to determine if any parameters should be passed to the kernel or if any additional kernel modules (such as drivers) should be loaded. Since loader values are specific to the kernel parameter or driver to be loaded, descriptions can be found in the man page for the specified driver and in many sections of the [FreeBSD Handbook](#).

Beginning with version 8.0.3, FreeNAS™ provides a graphical interface for managing loader values. This advanced functionality is intended to make it easier to load additional kernel modules at boot time. A typical usage would be to load a FreeBSD hardware driver that does not automatically load after a FreeNAS™ installation. The default FreeNAS™ image does not load every possible hardware driver. This is a necessary evil as some drivers conflict with one another or cause stability issues, some are rarely used, and some drivers just don't belong on a standard NAS system. If you need a driver that is not automatically loaded, you need to add a loader.

**DANGER:** changing the value of a loader is an advanced feature that could adversely effect the ability of the FreeNAS™ system to successfully boot. It is *very important* that you do not have a typo when adding a loader value as this could halt the boot process. Fixing this problem requires physical access to the FreeNAS™ system and knowledge of how to use the boot loader prompt as described in [section 4.5.1 Recovering From Incorrect Loaders](#). This means that you should always test the impact of any changes on a test system first.

Additionally, certain changes could make your system unsupported by the FreeNAS™ team and can break assumptions made by the software. Some examples include:

- setting kernel tunables to arbitrarily low or high limits, e.g. kern.hz=1 or kern.hz=100000
- disabling or enabling certain features such as vfs.zfs.zil\_disable=1
- overriding default loader values, unless directed to do so by a developer affiliated with the

## FreeNAS™ project

To add a loader value, go to System -> Loaders -> Add Loader, as seen in Figure 4.5a.

**Figure 4.5a: Adding a Loader Value**



Table 4.5a summarizes the options when adding a loader.

**Table 4.5a: Adding a Loader**

Setting	Value	Description
Variable	string	typically the name of the driver to load, as indicated by its man page
Value	integer or string	value to associate with variable; typically this is set to <i>YES</i> to enable the driver specified by the variable
Comment	string	optional, but a useful reminder for the reason behind adding this loader

The changes you make will not take effect until the system is rebooted as loader settings are only read when the kernel is loaded at boot time. As long as the loader exists, your changes will persist at each boot and across upgrades.

Any loaders that you add will be listed in System -> Loaders -> View Loaders. To change the value of a loader, click its Edit button. To remove a loader, click its Delete button.

At this time, the GUI does not display the loaders that are pre-set in the installation image. FreeNAS™ 8.0.3 ships with the following loaders set:

```
autoboot_delay="2"  
loader_logo="freenas"  
kern.cam.boot_delay=10000  
fuse_load="YES"  
geom_mirror_load="YES"  
geom_stripe_load="YES"  
geom_raid3_load="YES"  
geom_gate_load="YES"  
debug.debugger_on_panic=1  
hw.hpttr.attach_generic=0
```

You should not add or edit the default loaders in the GUI as doing so will overwrite the default values which may render the system unusable.

#### 4.5.1 Recovering From Incorrect Loaders

If a loader is preventing the system from booting, you will need physical access to the FreeNAS™ system. Watch the boot messages and press the number 6 key to select "6. Escape to loader prompt" when you see the FreeNAS™ boot menu shown in Figure 4.5b.

Figure 4.5b: FreeNAS™ Boot Menu



The boot loader prompt provides a minimal set of commands described in [loader\(8\)](#). Once at the prompt, use the **unset** command to disable a problematic value, the **set** command to modify the problematic value, or the **unload** command to prevent the problematic driver from loading.

Example 4.5a demonstrates several examples using these commands at the boot loader prompt. The first command disables the current value associated with the `kern.ipc.nmbclusters` MIB and will fail with a "no such file or directory" error message if a current loader does not exist to set this value. The second command disables ACPI. The third command instructs the system not to load the fuse driver. When finished, type **boot** to continue the boot process.

#### Example 4.5a: Sample Commands at the Boot Loader Prompt

```
Type '?' for a list of commands, 'help' for more detailed help.
OK unset kern.ipc.nmbclusters
OK set hint.acpi.0.disabled=1
OK unload fuse
OK boot
```

Any changes made at the boot loader prompt only effect the current boot. This means that you need to



edit or remove the problematic loader in System -> Loaders -> View Loaders to make your change permanent and to prevent future boot errors.

## 4.6 Rsync Tasks

[Rsync](#) is a utility that automatically copies specified data from one system to another over a network. Once the initial data is copied, rsync reduces the amount of data sent over the network by sending only the differences between the source and destination files. Rsync can be used for backups, mirroring data on multiple systems, or for copying files between systems.

To configure rsync, you need to configure both ends of the connection:

- **the rsync server:** this system pulls (receives) the data. In the FreeNAS™ GUI, the server is configured in Services -> [Rsync](#).
- **the rsync client:** this system pushes (sends) the data. In the FreeNAS™ GUI, the client is configured in System -> Rsync Tasks.

This section summarizes the options when creating an Rsync Task. It then provides a configuration example for setting up rsync between two FreeNAS™ systems.

### 4.6.1 Creating an Rsync Task

Figure 4.6a shows the screen that appears when you click System -> Rsync Tasks -> Add Rsync Task.

Table 4.6a summarizes the options that can be configured when creating an rsync task.

**Figure 4.6a: Adding an Rsync Task**

The screenshot shows the 'Add Rsync' configuration window. It includes the following elements:

- Path:** A text input field with a 'Browse' button.
- Remote Host:** A text input field.
- Remote Module Name:** A text input field.
- Short description:** A text input field.
- Minute:** A section containing two radio buttons: 'Every N minute' (selected) and 'Each selected minute'. Below 'Each selected minute' is a grid of 60 buttons numbered 00 to 59.
- Hour:** A section containing two radio buttons: 'Every N hour' and 'Each selected hour'.
- Slider:** A horizontal slider with arrows at both ends and a '1' below it.



**Table 4.6a: Rsync Configuration Options**

Setting	Value	Description
Path	Browse button	select the volume/dataset/directory that you wish to copy
Remote Host	string	IP address or hostname of the remote system that will store the copy
Remote Module Name	string	name must be defined in <a href="#">rsyncd.conf(5)</a> of rsync server or in Rsync Module of another FreeNAS™ system
Short Description	string	optional
Minute	slider or checkboxes	if use the slider, sync occurs every N minutes; if use check boxes, sync occurs at the selected moments
Hour	slider or checkboxes	if use the slider, sync occurs every N hours; if use check boxes, sync occurs at the selected hours
Day of month	slider or checkboxes	if use the slider, sync occurs every N days; if use check boxes, sync occurs on the selected days
Month	checkboxes	task occurs on the selected months
Day of week	checkboxes	task occurs on the selected days of the week
User	drop-down menu	specified user must have permission to write to the specified directory on the remote system; due to a limitation in FreeBSD, the user name can not exceed 17 characters
Recursive	checkbox	if checked, copy will include all subdirectories of the specified volume
Times	checkbox	preserve modification times of files
Compress	checkbox	recommended on slow connections as reduces size of data to be transmitted
Archive	checkbox	equivalent to -rlptgoD (recursive, copy symlinks as symlinks, preserve permissions, preserve modification times, preserve group, preserve owner (super-user only), and preserve device files (super-user only) and special files)
Delete	checkbox	delete extraneous files from destination directory
Quiet	checkbox	suppresses information messages from the remote server
Preserve permissions	checkbox	preserves file permissions
Preserve extended attributes	checkbox	both systems must support <a href="#">extended attributes</a>
Extra options	string	<a href="#">rsync(1)</a> options not covered by the GUI

## 4.6.2 Configuring Rsync Between Two FreeNAS™ Systems

This configuration example will configure rsync between the two following FreeNAS™ systems:

- 192.168.2.2 has existing data in `/mnt/local/images`. It will be the rsync client, meaning that an rsync task needs to be defined.
- 192.168.2.6 has an existing volume named `/mnt/remote`. It will be the rsync server, meaning that it will receive the contents of `/mnt/local/images`. An rsync module needs to be defined on this system and the `rsyncd` service needs to be started.

On the client system (192.168.2.2), an rsync task is defined in System -> Rsync Tasks -> Add Rsync Task as shown in Figure 4.6b. In this example:

- the Path points to `/usr/local/images`, the directory to be copied
- the Remote Host points to `192.168.2.6`, the IP address of the rsync server
- the Remote Module Name is `backups`; this will need to be defined on the rsync server
- the rsync is scheduled to occur every 15 minutes
- the User is set to `root` so it has permission to write anywhere
- the Preserve Permissions checkbox is checked so that the original permissions are not overwritten by the root user

**Figure 4.6b: Configuring the Rsync Client**

<b>Path</b>	<input type="text" value="/mnt/local/images"/>	<input type="button" value="Browse"/>
<b>Remote Host</b>	<input type="text" value="192.168.2.6"/>	
<b>Remote Module Name</b>	<input type="text" value="backups"/>	
<b>Short description</b>	<input type="text"/>	
<b>Minute</b>	Every N minute <input checked="" type="radio"/> Each selected minute <input type="radio"/> <input type="range" value="15"/>	
<b>Hour</b>	Every N hour <input type="radio"/> Each selected hour <input checked="" type="radio"/>	

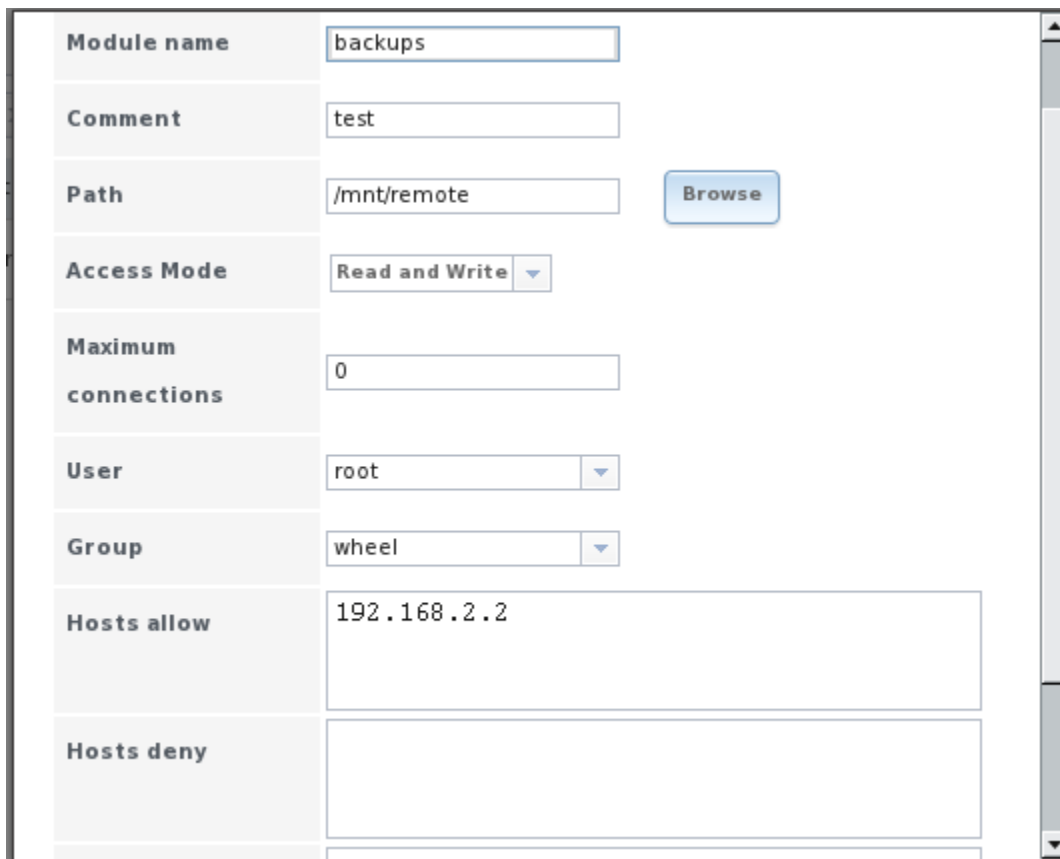
On the server system (192.168.2.6), an rsync module is defined in Services -> Rsync Modules -> Add Rsync Module as shown in Figure 4.6c. In this example:

- the Module Name is *backups*; this needs to match the setting on the rsync client
- the Path is */mnt/remote*; a directory called *images* will be created to hold the contents of */usr/local/images*
- the User is set to *root* so it has permission to write anywhere
- Hosts allow is set to *192.168.2.2*, the IP address of the rsync client

Descriptions of the configurable options can be found in [section 8.15.2 Rsync Modules](#).

To finish the configuration, start the rsync service on the server in Services -> Control Services.

**Figure 4.6c: Configuring the Rsync Server**



The screenshot shows a configuration window for an Rsync module. The fields are as follows:

Module name	backups
Comment	test
Path	/mnt/remote <input type="button" value="Browse"/>
Access Mode	Read and Write
Maximum connections	0
User	root
Group	wheel
Hosts allow	192.168.2.2
Hosts deny	

## 4.7 S.M.A.R.T. Tests

[S.M.A.R.T.](#) (Self-Monitoring, Analysis and Reporting Technology) is a monitoring system for computer hard disk drives to detect and report on various indicators of reliability. When a failure is anticipated by S.M.A.R.T., the drive should be replaced. Most modern ATA, IDE and SCSI-3 hard drives support S.M.A.R.T.--refer to your drive's documentation if you are unsure.

Figure 4.7a shows the configuration screen that appears when you click System -> S.M.A.R.T. Tests ->

Add S.M.A.R.T. Test. You should create a test for each drive that you wish to monitor. After creating your tests, check the configuration in Services -> S.M.A.R.T, then click the slider to ON for the S.M.A.R.T service in Services -> Control Services.

**NOTE:** the S.M.A.R.T service will not start if you have not created any volumes.

**Figure 4.7a: Adding a S.M.A.R.T Test**

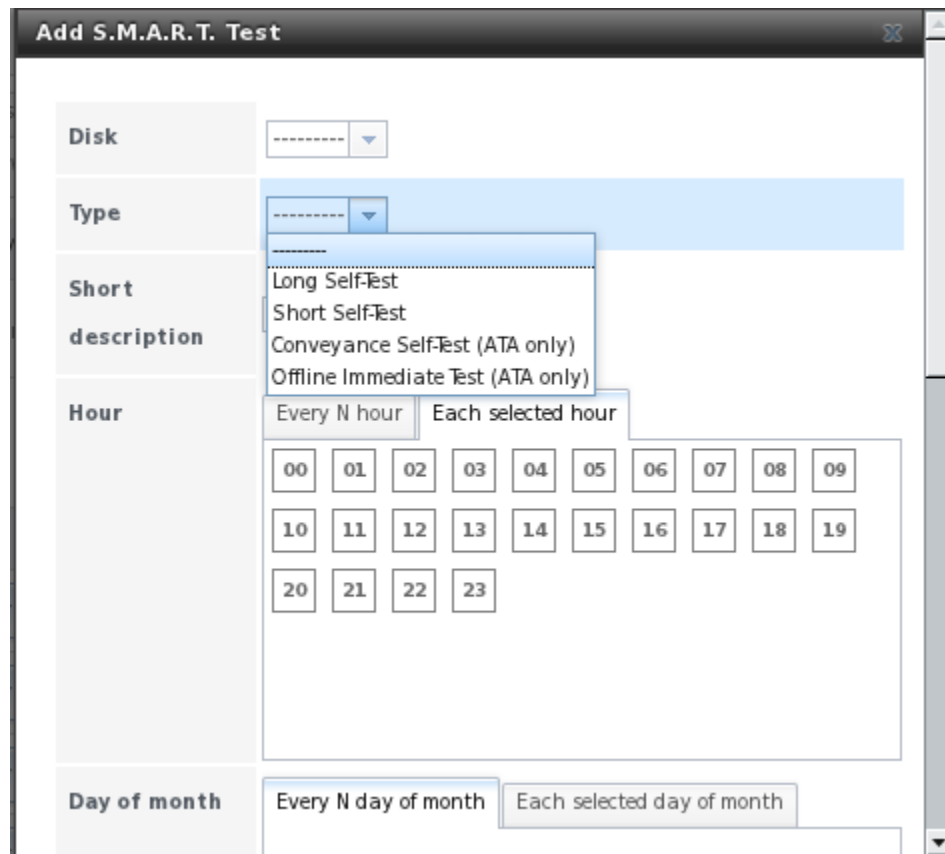


Table 4.7a summarizes the configurable options when creating a S.M.A.R.T test.

**Table 4.7a: S.M.A.R.T Test Options**

Setting	Value	Description
Disk	drop-down menu	select disk to monitor
Type	drop-down menu	select type of list to run; see <a href="#">smartctl(8)</a> for a description of each type of test
Short description	string	optional
Hour	slider or checkboxes	if use the slider, test occurs every N hours; if use check boxes, test occurs at the selected hours
Day of month	slider or checkboxes	if use the slider, test occurs every N days; if use check boxes, test occurs on the selected days
Month	checkboxes	select the months when you wish the test to occur

Setting	Value	Description
Day of week	checkboxes	select the days of the week when you wish the test to occur

## 4.8 Sysctls

[sysctl\(8\)](#) is an interface that is used to make changes to the underlying FreeBSD kernel running on a FreeNAS™ system. It can be used to tune the system in order to meet the specific needs of a network. Over five hundred system variables can be set using [sysctl\(8\)](#). Each variable is known as a MIB as it is comprised of a dotted set of components. Since these MIBs are specific to the kernel feature that is being tuned, descriptions can be found in many FreeBSD man pages (e.g. [sysctl\(3\)](#), [tcp\(4\)](#) and [tuning\(7\)](#)) and in many sections of the [FreeBSD Handbook](#).

**DANGER:** changing the value of a sysctl MIB is an advanced feature that immediately effects the kernel of the FreeNAS™ system. Do not change a MIB on a production system unless you understand the caveats associated with that change. A badly configured MIB could cause the system to become unbootable, unreachable via the network, or can cause the system to panic under load. Certain changes may make your system unsupported by the FreeNAS™ team and can break assumptions made by the software. This means that you should always test the impact of any changes on a test system first.

Beginning with version 8.0.3, FreeNAS™ provides a graphical interface for managing sysctl MIBs. To add a sysctl, go to System -> Sysctls -> Add Sysctl, shown in Figure 4.8a.

**Figure 4.8a: Adding a Sysctl**

Table 4.8a summarizes the options when adding a sysctl.

**Table 4.8a: Adding a Sysctl**

Setting	Value	Description
Variable	string	must be in dotted format e.g. kern.ipc.shmmax
Value	integer or string	value to associate with MIB; do not make this up, refer to the suggested values in a man page, FreeBSD Handbook page, or tutorial
Comment	string	optional, but a useful reminder for the reason behind using this MIB/value

As soon as you add or edit a sysctl, the running kernel will change that variable to the value you specify. As long as the sysctl exists, that value will persist across reboots and upgrades.

Any MIBs that you add will be listed in System -> Sysctls -> View Sysctls. To change the value of a MIB, click its Edit button. To remove a MIB, click its Delete button.

At this time, the GUI does not display the sysctl MIBs that are pre-set in the installation image. FreeNAS™ 8.0.3 ships with the following MIBs set:

```
debug.debugger_on_panic=0
kern.metadelay=3
kern.dirdelay=4
kern.filedelay=5
kern.coredump=0
```

You should not add the default MIBs as sysctls as doing so will overwrite the default values which may render the system unusable.

## 5 Network Configuration

The Network section of the administrative GUI contains the following components for viewing and configuring the FreeNAS™ system's network settings:

- [Global Configuration](#)
- [Network Summary](#)
- [Interfaces](#)
- [Link Aggregations](#)
- [Static Routes](#)
- [VLANs](#)

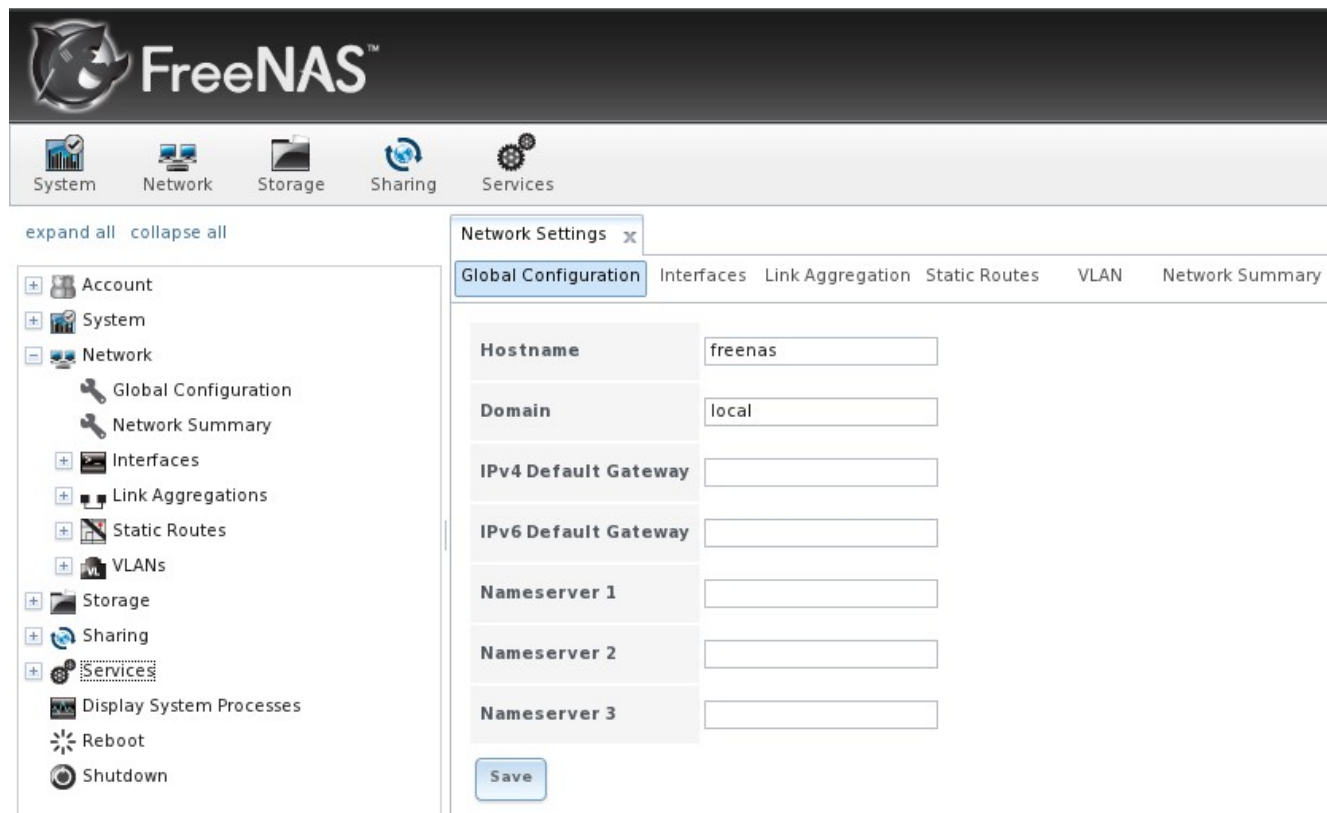
Each of these is described in more detail below.

### 5.1 Global Configuration

The global configuration tab, shown in Figure 5.1a, allows you to set non-interface specific network settings.

Table 5.1a summarizes the settings that can be configured using the Global Configuration tab. The hostname and domain will be pre-filled for you, as seen in Figure 5.1a, but can be changed to meet the local network's requirements. The other settings are optional and can reduce the security of the FreeNAS™ system (by making it Internet accessible) if it is not properly protected by a firewall.

**Figure 5.1a: Sample Global Configuration**



**Table 5.1a: Global Configuration Settings**

Setting	Value	Description
Hostname	string	system host name
Domain	string	system domain name
IPv4 Default Gateway	IP address	typically not set to prevent NAS from being accessible from the Internet
IPv6 Default Gateway	IP address	Typically not set
Nameserver 1	IP address	primary DNS server (typically in Windows domain)
Nameserver 2	IP address	secondary DNS server
Nameserver 3	IP address	tertiary DNS server

## 5.2 Network Summary

The Network Summary tab allows you to quickly view the addressing information of every configured interface. It will show the interface name, IP address, DNS server(s), and default gateway.

## 5.3 Interfaces

The interfaces tab allows you to view which interfaces have been configured, to add an interface to configure, and to edit an interface's current configuration. Figure 5.3a shows the screen that opens when you click Interfaces -> Add Interface.

Table 5.3a summarizes the configuration options when you Add an interface or Edit an already configured interface.

**Figure 5.3a: Editing an Interfaces Configuration**

**Table 5.3a: Interface Configuration Settings**

Setting	Value	Description
NIC	drop-down menu	select the FreeBSD device name; will be read-only field when edit an interface
Interface Name	string	description of interface
DHCP	checkbox	requires manual IPv4 or IPv6 configuration if unchecked
IPv4 Address	IP address	set if DHCP unchecked
IPv4 Netmask	drop-down menu	set if DHCP unchecked
Auto configure IPv6	checkbox	if checked, use <a href="#">rtsol(8)</a> to configure the interface; requires manual configuration if unchecked and wish to use IPv6



Setting	Value	Description
IPv6 Address	IPv6 address	must be unique on network
IPv6 Prefix Length	drop-down menu	match the prefix used on network
Options	string	additional parameters from <a href="#">ifconfig(8)</a> , one per line; for example: <b>mtu 9000</b> will increase the MTU for interfaces that support jumbo frames

This screen also allows you to configure an alias for the interface. If you wish to set multiple aliases, click the "Add extra alias" link for each alias you wish to configure.

## 5.4 Link Aggregations

FreeNAS™ uses FreeBSD's [lagg\(4\)](#) interface to provide link aggregation and link failover. The lagg interface allows aggregation of multiple network interfaces into a single virtual lagg interface, providing fault-tolerance and high-speed multi-link throughput. The aggregation protocols supported by lagg determine which ports are used for outgoing traffic and whether a specific port accepts incoming traffic. Lagg's interface link state is used to validate if the port is active or not.

Aggregation works best on switches supporting LACP, which distributes traffic bi-directionally while responding to failure of individual links. FreeNAS™ also supports active/passive failover between pairs of links.

**Important notice regarding aggregation performance:** the LACP, FEC and load-balance modes select the output interface using a hash that includes the Ethernet source and destination address, VLAN tag (if available), IP source and destination address, and flow label (IPv6 only). The benefit can only be observed when multiple clients are transferring files *from* your NAS. The flow entering *into* your NAS depends on the Ethernet switch load-balance algorithm.

**NOTE:** LACP and other forms of link aggregation generally do not work well with virtualization solutions. In a virtualized environment, consider the use of iSCSI MPIO through the creation of an iSCSI Portal as demonstrated in [section 8.14.6](#). This allows an iSCSI initiator to recognize multiple links to a target, utilizing them for increased bandwidth or redundancy. This [how-to](#) contains instructions for configuring MPIO on ESXi.

The lagg driver currently supports the following aggregation protocols:

**Failover:** the default protocol. Sends traffic only through the active port. If the master port becomes unavailable, the next active port is used. The first interface added is the master port; any interfaces added after that are used as failover devices. By default, received traffic is only accepted when received through the active port. This constraint can be relaxed by setting the `net.link.lagg.failover_rx_all` [sysctl\(8\)](#) variable to a nonzero value, which is useful for certain bridged network setups.

**FEC:** supports Cisco EtherChannel. This is a static setup and does not negotiate aggregation with the peer or exchange frames to monitor the link.

**LACP:** supports the IEEE 802.3ad Link Aggregation Control Protocol (LACP) and the Marker Protocol. LACP will negotiate a set of aggregable links with the peer into one or more link aggregated groups (LAG). Each LAG is composed of ports of the same speed, set to full-duplex operation. The traffic will be balanced across the ports in the LAG with the greatest total speed; in most cases there will only be one LAG which contains all ports. In the event of changes in physical connectivity, link aggregation will quickly converge to a new configuration. LACP must be configured on the switch as well.

**Load Balance:** balances outgoing traffic across the active ports based on hashed protocol header information and accepts incoming traffic from any active port. This is a static setup and does not negotiate aggregation with the peer or exchange frames to monitor the link. The hash includes the Ethernet source and destination address, VLAN tag (if available), and IP source and destination address.

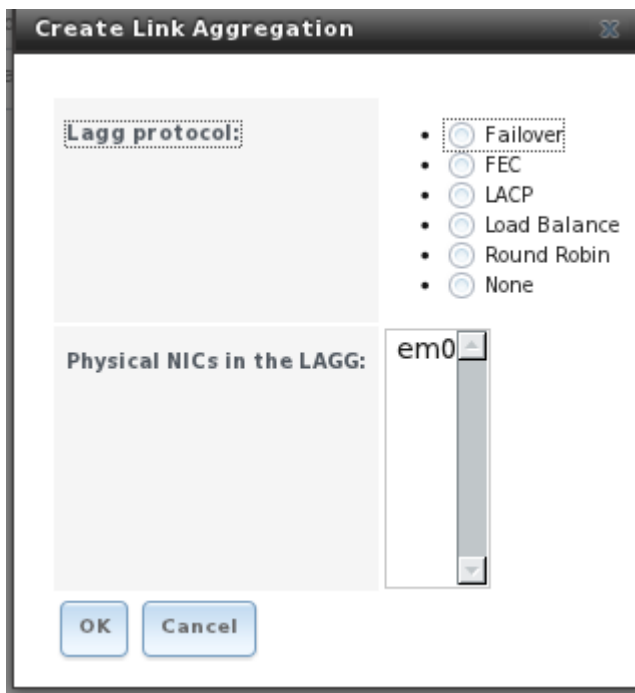
**Round Robin:** distributes outgoing traffic using a round-robin scheduler through all active ports and accepts incoming traffic from any active port.

**None:** this protocol is intended to do nothing: it disables any traffic without disabling the lagg interface itself.

**NOTE:** The FreeNAS™ system must be rebooted after configuring the lagg device, which requires console access to the FreeNAS™ system. TCP access will be lost during reboot. The interfaces used in the lagg device should not be configured before creating the lagg device.

Figure 5.4a shows the configuration options when adding a lagg interface.

**Figure 5.4a: Creating a lagg Interface**



**NOTE:** if interfaces are installed but do not appear in the Physical NICs in the LAGG list, check that a FreeBSD driver for the interface exists [here](#).

Select the desired aggregation protocol, highlight the interface(s) to associate with the lagg device, and click the OK button.

Once the lagg device has been created, it will appear in View All Link Aggregations. Click its Edit Interface button to open the screen shown in Figure 5.4b.

**Figure 5.4b: Edit lagg Interface**

The screenshot shows a window titled "Edit Interface" with a close button in the top right corner. The window contains several configuration fields:

- NIC:** A text input field containing "lagg0".
- Interface Name:** A text input field containing "lagg0".
- DHCP:** A checkbox that is currently unchecked.
- IPv4 Address:** An empty text input field.
- IPv4 Netmask:** A dropdown menu showing "-----" with a downward arrow.
- Auto configure IPv6:** A checkbox that is currently unchecked.
- IPv6 Address:** An empty text input field.
- IPv6 Prefix Length:** A dropdown menu showing "-----" with a downward arrow.
- Options:** An empty text input field.

Table 5.4a describes the options in this screen:

**Table 5.4a: Configurable Options for a lagg Interface**

Setting	Value	Description
NIC	string	read-only as automatically assigned next available numeric ID
Interface Name	string	by default same as device (NIC) name, can be changed to a more descriptive value
DHCP	checkbox	check if the lagg device gets its IP address info from DHCP server
IPv4 Address	string	mandatory if DHCP is left unchecked
IPv4 Netmask	drop-down menu	mandatory if DHCP is left unchecked
Auto configure IPv6	checkbox	check only if DHCP server available to provide IPv6 address info
IPv6 Address	string	optional

Setting	Value	Description
IPv6 Prefix Length	drop-down menu	required if input IPv6 address
Options	string	additional <a href="#">ifconfig(8)</a> options

This screen also allows you to configure an alias for the lagg interface. If you wish to set multiple aliases, click the "Add extra alias" link for each alias you wish to configure.

If you click a lagg device's Edit Members button, then the Edit button under the Action column, you will see the screen shown in Figure 5.4c. This screen allows you to configure the individual physical (parent) interface that you specified. The configurable options are summarized in Table 4.4b.

**Figure 5.4c: Editing a Member Interface**

**Table 5.4b: Configuring a Member Interface**

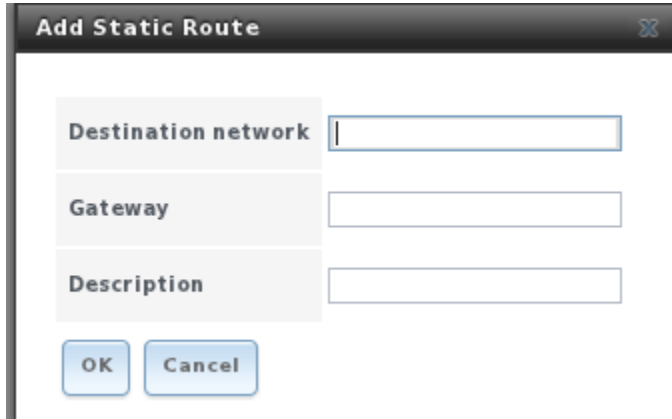
Setting	Value	Description
LAGG Interface group	drop-down menu	select the member interface to configure
LAGG Priority Number	integer	order of selected interface within the lagg
Physical NIC	drop-down menu	physical interface of the selected member
Options	string	additional parameters from <a href="#">ifconfig(8)</a>

**NOTE:** you can set options such as the MTU (to enable jumbo frames) at either the lagg level or the individual parent interface level. You do not have to set the option at both levels as each level will automatically inherit its options from the other. However, it makes sense to set it at the lagg level (Figure 5.4b) as each interface member will inherit from the lagg. If you set it at the interface level (Figure 5.4c), you will have to repeat for each interface within the lagg. It is important to not set differing options at the lagg and the interface level as this will confuse the lagg device. Also, do not set jumbo frames if the attached switch does not support jumbo frames.

## 5.5 Static Routes

For security reasons, no static routes are defined on the FreeNAS™ system. Should you need a static route to reach portions of your network, you can add and view all static routes using Network -> Static Routes. If you click "Add Static Route" you will see the screen shown in Figure 5.5a.

**Figure 5.5a: Adding a Static Route**



The screenshot shows a dialog box titled "Add Static Route". It features three input fields: "Destination network", "Gateway", and "Description". Below these fields are two buttons: "OK" and "Cancel". The dialog box has a dark title bar with a close button (X) on the right.

The destination network and gateway fields are mandatory; the description field is optional.

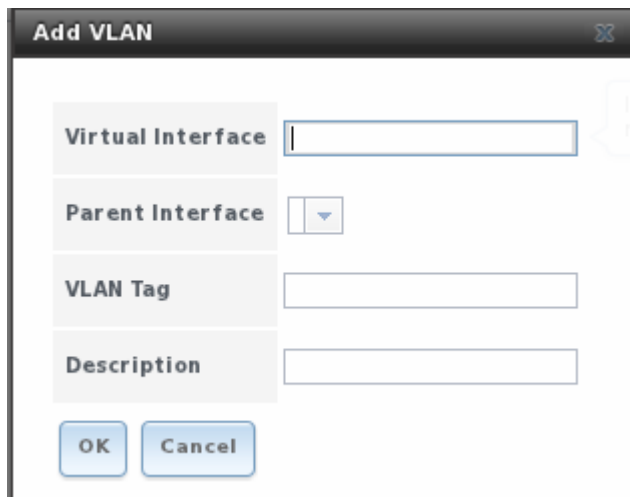
If you add any static routes, they will show in "View All Static Routes". Each route will have an action of Edit or Delete.

## 5.6 VLANs

FreeNAS™ uses FreeBSD's [vlan\(4\)](#) interface to demultiplex frames with IEEE 802.1q tags. This allows nodes on different VLANs to communicate through a layer 3 switch or router. A vlan interface must be assigned a parent interface and a numeric VLAN tag. A single parent can be assigned to multiple vlan interfaces provided they have different tags. If you click Network -> VLANs -> Add VLAN, you will see the screen shown in Figure 5.6a.

**NOTE:** VLAN tagging is the only 802.1Q feature that is implemented. Additionally, not all Ethernet interfaces support full VLAN processing—see the **HARDWARE** section of [vlan\(4\)](#) for details.

**Figure 5.6a: Adding a VLAN**



The image shows a dialog box titled "Add VLAN" with a close button (X) in the top right corner. The dialog contains four input fields: "Virtual Interface" (a text box), "Parent Interface" (a dropdown menu), "VLAN Tag" (a text box), and "Description" (a text box). At the bottom of the dialog are two buttons: "OK" and "Cancel".

Table 5.6a describes the various fields.

**Table 5.6a: Adding a VLAN**

Setting	Value	Description
Virtual Interface	string	Use the format vlanX where X is a number representing the vlan interface
Parent Interface	select from drop-down menu	usually an Ethernet card connected to a properly configured switch port
VLAN Tag	integer	should match a numeric tag set up in the switched network
Description	string	optional

## 6 Storage Configuration

The Storage section of the graphical interface allows you to configure the following:

- [Periodic Snapshot Tasks](#)
- [Replication Tasks](#)
- [Volumes](#)

These configurations are described in more detail in this section.

### 6.1 Periodic Snapshot Tasks

FreeNAS™ ZFS volumes support snapshots, a read-only version of a ZFS volume or dataset at a given point in time. Snapshots can be created quickly and, if little data changes, new snapshots take up very little space. For example, a snapshot where no files have changed takes 0MB of storage, but if you change a 10GB file it will keep a copy of both the old and the new 10GB version. Snapshots provide a clever way of keeping a history of files, should you need to recover an older copy or even a deleted file.

For this reason, many administrators take snapshots often (e.g. every 15 minutes), store them for a period of time (e.g. for a month), and store them on another system (e.g. using Replication Tasks). Such a strategy allows the administrator to roll the system back to a specific time or, if there is a catastrophic loss, an off-site snapshot can restore the system up to the last snapshot interval (e.g. within 15 minutes of the data loss). Snapshots can be cloned or rolled back, but the files on the snapshot cannot be accessed independently.

Before you can create a snapshot, you need to have an existing ZFS volume. How to do this is described in [section 6.3.3 Creating Volumes](#).

To create a ZFS snapshot, click Storage -> Periodic Snapshot Tasks -> Add Periodic Snapshot which will open the screen shown in Figure 6.1a.

**Figure 6.1a: Creating a ZFS Periodic Snapshot**

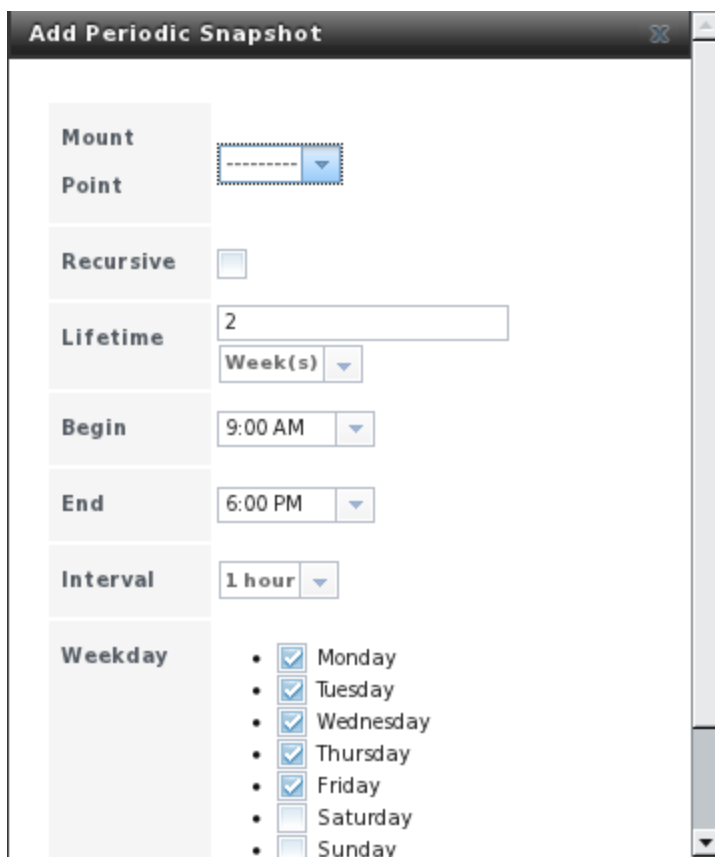


Table 6.1a summarizes the fields in this screen:

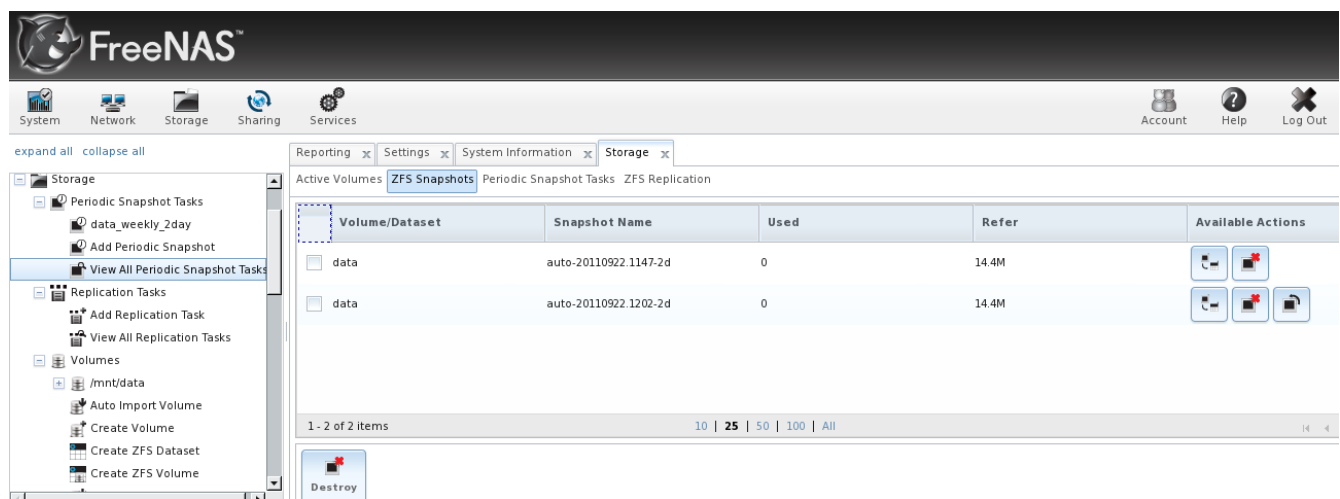
**Table 6.1a: Options When Creating a Periodic Snapshot**

Setting	Value	Description
Mount Point	drop-down menu	select the mount point of an existing ZFS volume or dataset
Recursive	checkbox	recursive snapshots are created as one atomic operation across descendent file systems, meaning that the snapshot data is taken at one consistent time

Setting	Value	Description
Lifetime	integer and drop-down menu	how long to keep the snapshot
Begin	drop-down menu	time of first snapshot
End	drop-down menu	time of last snapshot
Interval	drop-down menu	how often to take snapshot between Begin and End times
Weekday	checkboxes	which days of the week to take snapshots

Once you click the OK button, a snapshot will be taken and this task will be repeated according to your settings. If you click ZFS Snapshots, you will see a listing of available snapshots as seen in the example in Figure 6.1b:

**Figure 6.1b: Viewing Available Snapshots**



The most recent snapshot will be listed last and will have 3 icons instead of 2. The icons associated with a snapshot allow you to:

**Clone Snapshot:** will prompt you for the name of the clone. The clone will be a writable copy of the snapshot and can only be created on the same ZFS volume. Clones do not inherit the properties of the parent dataset, but rather inherit the properties based on where the clone is created in the ZFS pool. Because a clone initially shares all its disk space with the original snapshot, its used property is initially zero. As changes are made to the clone, it uses more space.

**Destroy Snapshot:** a pop-up message will ask you to confirm this action. Note that clones must be destroyed before the parent snapshot can be destroyed.

**Rollback Snapshot:** a pop-up message will ask if you are sure that you want to rollback to this snapshot state. If you click Yes, any files that have changed since the snapshot was taken will be reverted back to their state at the time of the snapshot.

**NOTE:** rollback is a potentially dangerous operation and will cause any configured replication tasks to fail as the replication system uses the existing snapshot when doing an incremental backup. If you do need 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 FreeNAS™ system.
3. Once users have recovered the needed data, destroy the clone.

This approach will never destroy any on-disk data and has no impact on replication.

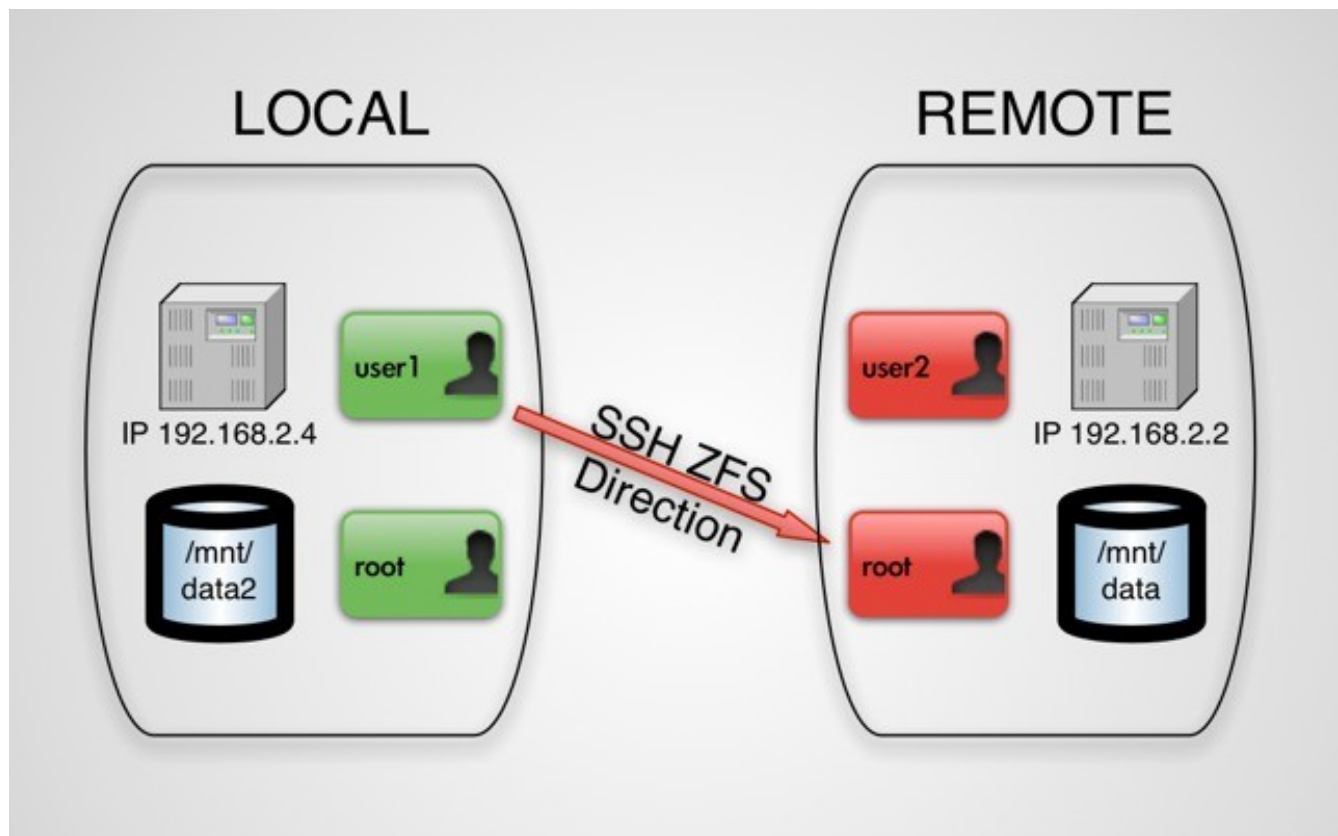
Alternatively, periodic snapshots will appear as shadow copies in newer versions of Windows Explorer. Users can access the files in the shadow copy using Explorer without requiring any interaction with the FreeNAS™ graphical administrative interface.

## 6.2 Replication Tasks

FreeNAS™ supports the secure replication of ZFS snapshots to another remote FreeNAS™ system (or any other system running the same version of ZFS and a listening SSH server). This allows you to create an off-site backup of the storage data.

This section demonstrates how to setup SSH replication between two FreeNAS™ systems. We will use the terms LOCAL (to represent the system that will send the snapshots) and REMOTE (to represent the system to receive the snapshots). In this example, LOCAL has an IP address of 192.168.2.4 and REMOTE has an IP address of 192.168.2.2. An overview is seen in Figure 6.2a.

**Figure 6.2a: Overview of Configuration Example**



In order to replicate ZFS snapshots you will need the following:

- a ZFS volume created on both LOCAL and REMOTE (see [section 6.3.3 Creating Volumes](#) for instructions on how to do this)
- a periodic snapshot task must be created on LOCAL (see [section 6.1 Periodic Snapshot Tasks](#) for instructions on how to do this)
- both systems configured for SSH key based authentication

### 6.2.1 Configuring SSH Key Based Authentication

In order to setup SSH key based authentication, you will need to temporarily use SSH password based authentication so that you can copy the SSH key information to the required locations. The configuration steps are as follows:

1. If you haven't already, create on LOCAL a user account which will be used to **ssh** into LOCAL. Make the user a member of the *wheel* group and set their home directory to the full path of the ZFS volume. In the example shown in Figure 6.2b, a user account named *user1* has a home directory pointing to the ZFS volume named */mnt/data2*. Create a similar user on REMOTE.
2. If you haven't done so already, set the root password in Account -> Users -> View All Users on both systems.
3. Use an SSH client (e.g. the **ssh** command from a command prompt or [PuTTY](#) from a Windows system) to login into LOCAL. In the example shown in Figure 6.2b, *user1* is using the **ssh** command to login to the LOCAL FreeNAS™ system with an IP address of *192.168.2.4*. Once logged in, copy the contents of */data/ssh/replication.pub* to a temporary file. This is the public key of LOCAL. To get the public key of REMOTE, issue the **ssh-keyscan** command with the IP address of REMOTE and add that public key as a separate line in your temporary file. In the example shown in Figure 6.2c, the REMOTE IP address is *192.168.2.2*.

**NOTE:** make sure that each key is pasted as one long line.

Figure 6.2b: Create a User

User ID	1001
Username	user1
Primary Group	wheel
Home Directory	/mnt/data2
Shell	tcsh
Full Name	ssh user
E-mail	user1@somecompany.com
Password	*****
Password confirmation	*****
Disable logins	<input type="checkbox"/>

OK Cancel

Figure 6.2c: Copying the Replication Keys for LOCAL and REMOTE

```
[dru@pcbsd-3971] ~-> ssh user1@192.168.2.4
user1@192.168.2.4's password:
Last login: Thu Sep 22 14:00:17 2011 from 192.168.2.5
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
    The Regents of the University of California.  All rights reserved.

FreeBSD 8.2-RELEASE-p2 (FREENAS.i386) #2: Sun Sep 18 10:15:40 PDT 2011

    FreeNAS nanobsd (c) 2009-2010, The FreeNAS Development Team
    All rights reserved.
    FreeNAS is under the modified BSD license.

    For more information, documentation, help or support, go here:
    http://freenas.org
Welcome to FreeNAS
[user1@freenas] ~-> su
Password:
[user1@freenas] /mnt/data2# more /data/ssh/replication.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAwCwt6Fb1JthH6xPtmN5SzlqEjggZCH/wwWQsYKEH0/vdwXLri8
J+Pn/oPMM3GLRRbYhB+vpnAxrTt1uiLREtenp0hSb56RIWyyZ6m1FrXs+QSaDKCpM6+XRrQtLPd+VSoGDWsz6tK
8mV7vpfk3X77w1Y0PZDZy0j1aZnEE447WtEtCAgYcaH3+4G6mWzoK8Rf7yXakNV+R08Vu+40+H5qoqTAWk+rNI5
ZYcl8p7JiqxXLPgJ6lPr5p9jqYsWqE23bwmpGr0ZF1J9rd+hKv9jfxqW86Am/izWASYfy6qEIP4haYCo5oo09pq
o0k17bDRNbPvFZ58aYadjvaap8YB5z0t Key for replication
[user1@freenas] /mnt/data2# ssh-keyscan 192.168.2.2
# 192.168.2.2 SSH-2.0-OpenSSH_5.4p1 FreeBSD-20100308
192.168.2.2 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAwCrF1/MRk3I1wJm4708lyugDmGd6JFeJonoe0N
3wCRVxmtUh7nKp1PXnagnbVFmq7aXIBs7Jd/Gd0WjousAI9G3qcn/tUf6A+AqcMk4cl9BURDX6xMSotmAn4m6Y
uKQffACv86eIo69Xn7xVKVD8s8c70K0/XnstPrL0NPBmpfHa04P5NZoe2C06CJKQCzKJGNJ/pmlbE0CogVHf5AJ
T1NtEQd78a75qrQK30MlkIzjCVD3WvchWJp8hr3TCs5F1Tclay5EU2ZvLwR8txaswuLyG33DKcE2SVRG5t+LD0
S7wuvATTWrzS0QTpeZoiZDw70f3kkjpm14UFnLsCjs9
[user1@freenas] /mnt/data2#
```

4. Now you will create an `authorized_keys` file on each system and paste the opposite system's key to that file. In Example 6.2a, *user1* is still logged into LOCAL. Once the REMOTE key is copied into LOCAL's `authorized_keys`, *user1* logs into REMOTE as *user2* and creates an `authorized_keys` file containing the LOCAL key. When finished, the user types **exit** four times to leave both `ssh` sessions.

**NOTE:** when creating the `authorized_keys` file, make sure that the correct key is pasted as one long line.

### Example 6.2a: Creating the `authorized_keys` Files

```
mount -uw /
mkdir -p /root/.ssh/
chmod 700 /root/.ssh
nano /root/.ssh/authorized_keys
192.168.2.2 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCrF1/MRk3I1wJm47081
yugDmGd6JFfeJonoeON3wCRVxmtUh7nKp1PXnagnbVFmq7aXIBs7Jd/GdOWjousAIT9G3qcn/tUf6A+AqcMk
4c19BURDX6xMSotmAn4m6YuKQffACv86eIo69Xn7xVKVD8s8c7OKO/XnstPrL0NPBmpfHa04P5NZoe2C06C
JKQCzKJGNJ/pm1bE0CogVHF5AJT1NtEQkd78a7SqrQK30M1kIzjCVD3WvchWJp8hr3TCs5F1Tc1ay5EU2Zv
LwR8txaswuLyG33DKcE2SVRG5t+LD0S7wuvATTWrzSOQTpeZoizDw7Qf3kkjpmt14UFnLsCjs9
ssh user2@192.168.2.2
su
mkdir -p /root/.ssh/
chmod 700 /root/.ssh
nano /root/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAw6Fb1JthH6xPtmN5Sz1qEjggZCH/
wwWQsYKEHO/vdwXLri8J+Pn/oPMM3G1RRbYhB+vpnAxrTtluilREtenpQhSb56RIWyyZ6m1FrXs+QSaDKCp
M6+XRrQtLPd+VSoGDWsz6tK8mV7vpfk3X77w1Y0PZDZyOjlaZnEE447WtEtCAGYcaH3+4G6mWzoK8Rf7yXa
kNV+RO8Vu+40+H5qoqTAWk+rNIsZYc18p7JiqxXLPgj6lPr5p9jqYsWqE23bwmpGrOZF1J9rd+hKv9jfxqW
86Am/izWASYfy6qEIp4haYCo5oo09pqoOk17bDRNbPvFZ58aYadjvaap8YB5z0t Key for replication
exit
exit (exits superuser and then REMOTE)
exit
exit (exits superuser and then LOCAL)
```

## 6.2.2 Creating the Replication Task

You are now ready to create a replication task. On *LOCAL*, click Storage -> Replication Tasks -> Add Replication Task. In the example shown in Figure 6.2d, the LOCAL ZFS volume is `/mnt/data2`, the REMOTE ZFS filesystem is `data`, and the REMOTE key has been pasted into the box. Note that for the remote ZFS filesystem, `/mnt/` is assumed and should not be included in the path.

**Figure 6.2d: Adding a Replication Task**

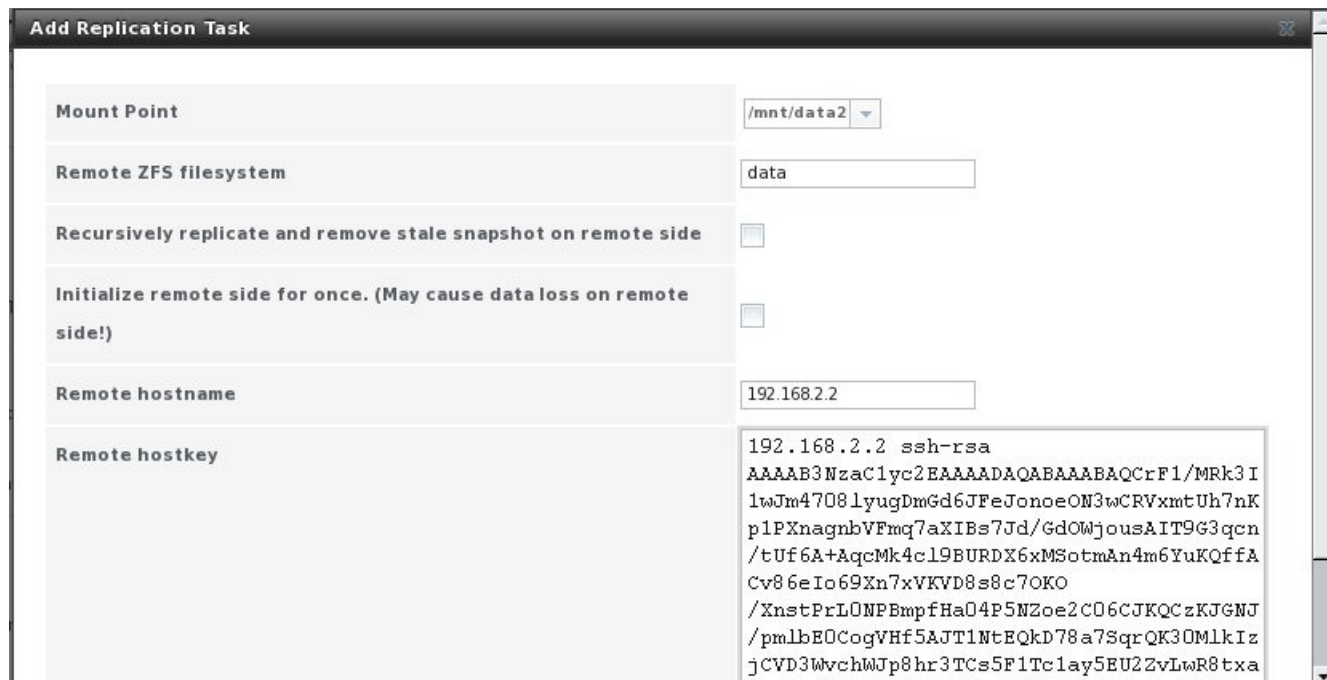


Table 6.2a summarizes the options in the Add Replication Task screen.

**Table 6.2a: Adding a Replication Task**

Setting	Value	Description
Mount Point	drop-down menu	the ZFS volume on LOCAL containing the snapshots to be replicated
Remote ZFS filesystem	string	the ZFS volume on REMOTE that will store the snapshots
Recursively replicate	checkbox	if checked will replicate child datasets and replace previous dataset on remote system
Initialize remote side	checkbox	does a reset once operation which destroys the replication data on the remote target and then reverts to normal operation
Remote hostname	string	IP address or DNS name of remote system
Remote hostkey	string	mandatory; paste the public key of the remote system (this will be the second line in the temporary file you created above)

### 6.2.3 Testing Replication

If you have followed all of the steps above and have LOCAL snapshots that are not replicating to REMOTE, try deleting all snapshots on LOCAL except for the most recent one. In Storage -> Periodic Snapshot Tasks -> View All Snapshot Tasks -> ZFS Snapshots check the box next to every snapshot except for the last one (the one with 3 icons instead of 2), then click the global Destroy button at the

bottom of the screen.

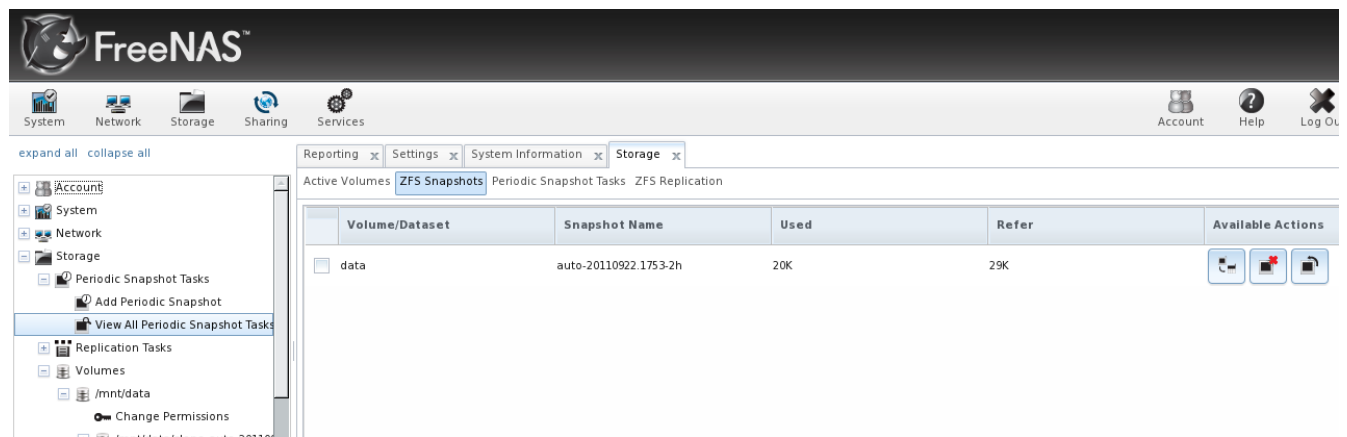
Once you have only one snapshot, **ssh** into LOCAL and use the **zfs send** command. In the following example, the ZFS snapshot on LOCAL is on ZFS volume *data2* and is named *auto-20110922.1753-2h*, the IP address of REMOTE is *192.168.2.2*, and the ZFS volume on REMOTE is *data*. Note that the **@** is used to separate the volume/dataset name from the snapshot name.

```
zfs send data2@auto-20110922.1753-2h | ssh -i /data/ssh/replication 192.168.2.2 \  
zfs receive data@auto-20110922.1753-2h
```

**NOTE:** if this command fails with the error "cannot receive new filesystem stream: destination has snapshots", check the box "initialize remote side for once" in the replication task and try again. If the **zfs send** command still fails, you will need to **ssh** into REMOTE and use the **zfs destroy -R volume\_name@snapshot\_name** command to delete the stuck snapshot.

You can confirm that the replication was successful by going to Storage -> Periodic Snapshot Tasks -> View All Periodic Snapshot Tasks -> ZFS Snapshots on REMOTE. Figure 6.2e shows the successful replication for our example:

**Figure 6.2e: Viewing the Replicated Snapshot From REMOTE**



## 6.2.4 Troubleshooting

If replication is not working, check to see if SSH is working properly. **ssh** into LOCAL and try to **ssh** into REMOTE. Replace *hostname\_or\_ip* with the value for REMOTE:

```
ssh -i /data/ssh/replication hostname_or_ip
```

This command should not ask for a password. If it asks for a password, key based authentication is not working. Check that the correct keys have been copied into the *authorized\_key* files as described in section [6.2.1 Configuring SSH Key Based Authentication](#).

If SSH is working correctly, check if the snapshot has replicated. **ssh** into REMOTE and run the command:

```
zfs list -t snapshot
```

It should list the snapshots replicated from LOCAL. If it does not, run the **zfs send** command as

demonstrated in [section 6.2.3 Testing Replication](#).

After successfully transmitting the snapshot, recheck again after the time period between snapshots lapses to see if the next snapshot successfully transmitted. If it is still not working, you can manually send an incremental backup of the last snapshot that is on both systems to the current one with this command:

```
zfs send data2@auto-20110922.1753-2h | ssh -i /data/ssh/replication 192.168.2.2 \  
zfs receive data@auto-20110922.1753-2h
```

## 6.3 Volumes

Since the storage disks are separate from the FreeNAS™ operating system, you don't actually have a NAS (network-attached storage) system until you configure your disks into at least one volume. FreeNAS™ supports the creation of both [UFS](#) and [ZFS](#) volumes; however, ZFS volumes are recommended to get the most out of your FreeNAS™ system. This section demonstrates how to perform the following actions:

- If your disks are using an existing UFS or ZFS software RAID, see [section 6.3.1 Auto Importing Volumes](#).
- If your disks are already formatted with UFS, NTFS, MSDOS, or EXT2, see [section 6.3.2 Importing Volumes](#).
- If you wish to format your disks into a UFS volume or ZFS pool, see section [6.3.3 Creating Volumes](#).
- If you wish to grow the size of an existing ZFS pool, see section [6.3.4 Adding to an Existing Volume](#).
- If you wish to divide an existing ZFS pool into datasets, see section [6.3.5 Creating ZFS Datasets](#).
- If you wish to create a ZFS block device to use as an iSCSI device extent, see [section 6.3.6 Creating a zvol](#).
- If you wish to control user/group access to an existing UFS volume, ZFS pool, or ZFS dataset, see section [6.3.7 Setting Permissions](#).

### 6.3.1 Auto Importing Volumes

If you click Storage -> Volumes -> Auto Import Volume, you can configure FreeNAS™ to use an existing software UFS or ZFS RAID volume. Supported volumes are UFS GEOM stripes (RAID0), UFS GEOM mirrors (RAID1), UFS GEOM RAID3, as well as existing ZFS pools. UFS RAID5 is not supported as it is an unmaintained summer of code project which was never integrated into FreeBSD.

**NOTE:** since .7 versions of FreeNAS™ use an earlier version of ZFS, importing ZFS pools into FreeNAS™ 8 is a one-way street. In other words, once you import a ZFS volume, you can not revert back to a previous version of ZFS. FreeNAS™ 8.0.3 does not currently support deduplication, compatibility with [Nexenta](#) pools, or Linux fuse-zfs.

If you have an existing software RAID volume, you will be able to select it from the drop-down menu.

In the example shown in Figure 6.3a, the FreeNAS™ system has an existing ZFS RAIDZ1 named backups. Once the volume is selected, click the "Import Volume" button.

**Figure 6.3a: Importing an Existing RAID Volume**



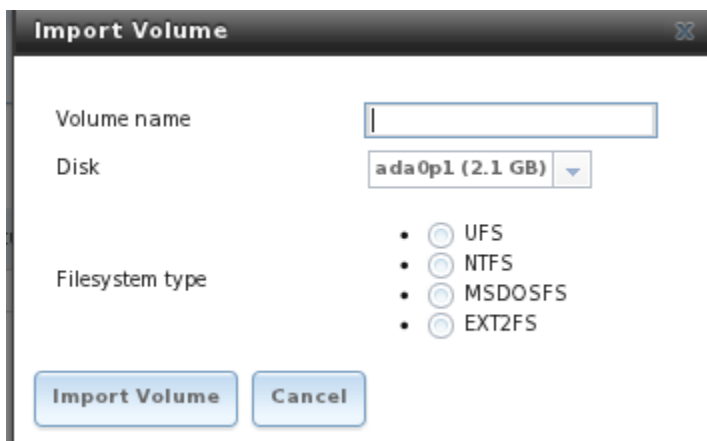
Once the import is complete you may have to refresh your browser in order for it to appear in the View All Volumes list.

**NOTE:** FreeNAS™ will not import a dirty volume. If your existing volume does not show in the drop-down menu, you will need to access the console in order to fsck the volume.

### 6.3.2 Importing Volumes

The import volume screen is used to import disks with existing filesystems so that they can be configured for use by FreeNAS™. If you click Import Volume, you'll see the screen shown in Figure 6.3b:

**Figure 6.3b: Importing a Volume**



Input a name for the volume, use the drop-down menu to select the volume that you wish to import, and select the type of filesystem on the disk. At this time, FreeNAS™ supports the import of disks that have been formatted with UFS, NTFS, MSDOS, or EXT2.

Before importing a disk, be aware of the following caveats:



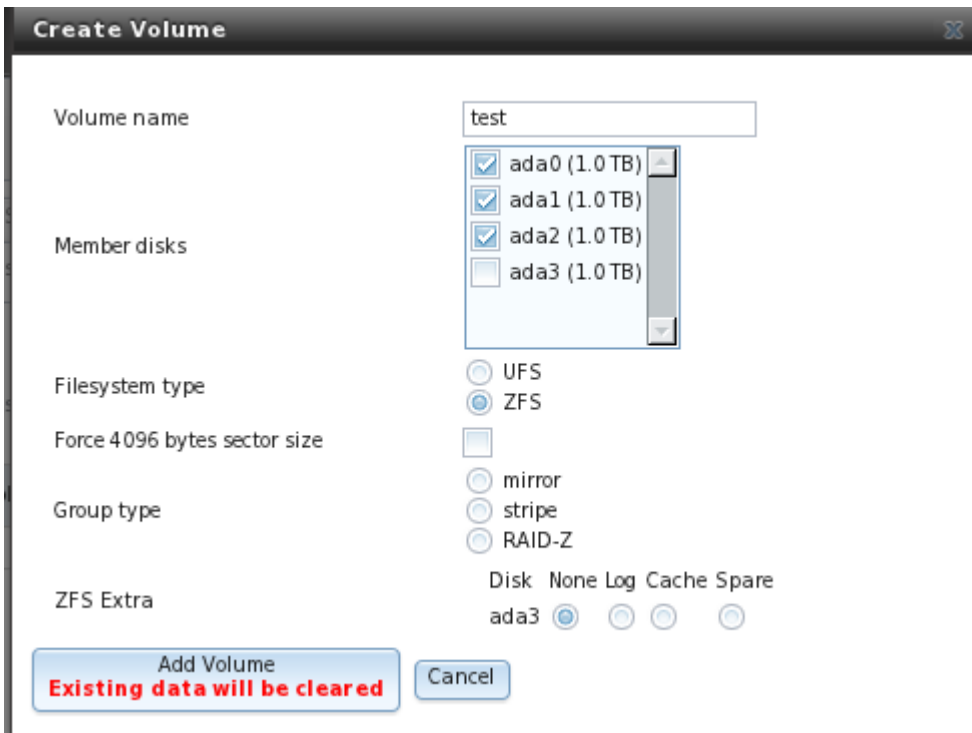
- FreeNAS™ will not import a dirty filesystem. If a supported filesystem does not show in the drop-down menu, you will need to access the console in order to **fsck** the filesystem.
- earlier versions of FreeNAS™ 8 had a bug that prevented the successful import of NTFS drives. Don't try to import NTFS if you are running a version earlier than FreeNAS™ 8.0.1-RC1.
- due to the current GEOM implementation, FreeNAS™ can not import dynamic NTFS volumes at this time. A future version of FreeBSD may address this issue.

### 6.3.3 Creating Volumes

If you have unformatted disks or wish to overwrite the filesystem (and data) on your disks, use the Create Volume screen to format the desired disks as a UFS volume or a ZFS pool.

If you click on Storage -> Volumes -> Create Volume, you will see a screen similar to the example shown in Figure 6.3c.

**Figure 6.3c: Creating a ZFS Volume**



The options that are available in this screen differ depending upon the filesystem that is selected and the number of disks available:

- if you select one disk, you can only choose to format with UFS or ZFS
- if you select two disks, you can create a UFS or ZFS mirror or stripe
- if you select three disks, you can create a UFS or ZFS stripe, a UFS RAID3, or a ZFS RAIDZ1
- if you select four disks, you can create a UFS or ZFS mirror or stripe, or a ZFS RAIDZ1 or RAIDZ2

Table 6.3a summarizes the configuration options of this screen.

**Table 6.3a: Options When Creating a ZFS Volume**

Setting	Value	Description
Volume name	string	up to 9 alphanumeric characters. If an existing volume name is specified, the volume being created will be added to the existing volume as a stripe. This allows for complex volumes such as RAID 10, RAIDZ+0, and RAIDZ2+0. The top level group is implicitly a stripe and there is no provision to build a mirror of mirrors, a RAIDZ of mirrors, or a mirror of RAIDZs.
Member disks	checkboxes	select desired number of disks from list of available disks
Filesystem type	button	select either UFS or ZFS
Force 4096 bytes sector size	checkbox	the system will automatically create the volume with 4K sectors if the underlying disk is using Advanced Format. Checking this option creates 4K sector size (instead of 512 bytes) regardless of the underlying hardware.
ZFS extra	select for each member disk	only available when select ZFS. Choose from: None, Log, Cache, Spare. See note below for descriptions of each option.

The Add Volume button warns that creating a volume **destroys all existing data on selected disk(s)**.

The ZFS extra options can be used to increase performance. They are as follows:

**None:** selected disk(s) will be used for storing data.

**Log:** selected disk will be dedicated for storing the ZIL (ZFS Intent Log). See [the Separate Log Devices](#) section of the ZFS Best Practices Guide for size recommendations. When two or more log devices are specified, FreeNAS™ will mirror them as suggested by the ZFS Best Practices Guide. This is a prevention measure because losing the ZIL could lead to disastrous results such as making the entire pool inaccessible.

Putting the ZIL on high speed devices can also improve performance for certain workloads, especially those requiring synchronous writes such as NFS clients connecting to FreeNAS™ running on VMWare ESXi. In such cases, a dedicated ZIL will make a big difference in performance. Applications that do not do a lot of synchronous writes are less likely to benefit from having dedicated ZIL devices. For VMWare, if a high speed ZIL device is not an option, using iSCSI instead of NFS is a workaround to achieve better performance.

**Cache:** selected disk will be dedicated to L2ARC on-disk cache. Typically, one would select a fast disk, such as an SSD. See [the Separate Cache Devices](#) section of the ZFS Best Practices Guide for size recommendations. Losing an L2ARC device has no implications at all, other than read access can slow down.

**Spare:** will create a hot spare that is only used when another disk fails. Hot spares speed up healing in the face of hardware failures and are critical for high mean time to data loss (MTTDL) environments. One or two spares for a 40-disk pool is a commonly used configuration. Use this option with caution as there is a [known bug](#) in the current FreeBSD implementation.

The volume creation screen allows for advanced scenarios:

- **to create a mirror (RAID 1):** check the 2 disks to go into the mirror from the list of available disks
- **to create a striped mirror (RAID 10):** create 2 mirrors with the *same volume name*
- **to add an SSD as hybrid storage:** check the box for the device, select ZFS, and choose Cache for that device in the ZFS Extra section
- **to add a cache drive** which will help read performance when the working set is smaller than the cache drive, but larger than the size of RAM available to the system: check the box for the device, select ZFS, and choose Cache for that device in the ZFS Extra section

An overview of the various RAID levels can be found in [section 1.1.6 RAID Overview](#).

### 6.3.4 Adding to an Existing Volume

ZFS supports the addition of virtual devices (vdevs) to an existing volume (ZFS pool). A RAIDZ1 is an example of a vdev. Once a vdev is created, you can not add more drives to that vdev. However, if you have an existing RAIDZ1, you can stripe it with a new RAIDZ1 (and its disks). This will increase the overall size of the pool.

To combine two vdevs in the graphical administrative interface, go to Storage -> Volumes -> Create Volume. In the Volume Name section, input the *same name* as an existing vdev, select the disk(s) that you wish to add, the type of RAID (which has to be the same as the existing one), choose ZFS as the filesystem, and click Add Volume.

### 6.3.5 Creating ZFS Datasets

An existing ZFS volume can be divided into datasets. This allows you to create a share per dataset, allowing for more granularity on which users have access to which data. A dataset is similar to a folder in that you can set permissions; it is also similar to a filesystem in that you can set quotas and compression.

**NOTE:** if your goal is to share an entire ZFS volume, you don't have to create datasets. If you wish to divide up a ZFS volume's data into different shares, create a dataset for each share.

If you click Volumes -> Create ZFS Dataset, you will see the screen shown in Figure 6.3d. Note that this menu option is not available until after you have created a ZFS volume.

Table 6.3b summarizes the options available when creating a ZFS dataset.

**Figure 6.3d: Creating a ZFS Dataset**

**Table 6.3b: ZFS Dataset Options**

Setting	Value	Description
Volume	drop-down menu	select an existing ZFS volume
Dataset Name	string	mandatory
Compression Level	drop-down menu	choose from: inherit, off, lzjb (optimized for performance while providing decent data compression), gzip level 6, gzip fastest (level 1), gzip maximum (level 9, best compression but slow); see NOTE below
Enable atime	inherit, on, or off	controls whether the access time for files is updated when they are read. Turning this property off avoids producing write traffic when reading files and can result in significant performance gains, though it might confuse mailers and other similar utilities.
Quota for dataset	integer	default of 0 is off; can specify M (megabyte), G (gigabyte), or T (terabyte) as in 20G for 20 GB
Quota for dataset and children	integer	default of 0 is off; can specify M (megabyte), G (gigabyte), or T (terabyte) as in 20G for 20 GB

Setting	Value	Description
Reserved space for dataset	integer	default of 0 is unlimited (besides hardware); can specify M (megabyte), G (gigabyte), or T (terabyte) as in 20G for 20 GB
Reserved space for dataset and children	integer	default of 0 is unlimited (besides hardware); can specify M (megabyte), G (gigabyte), or T (terabyte) as in 20G for 20 GB

**NOTE on compression:** most media (e.g. .mp3, .mp4, .avi) is already compressed, meaning that you'll increase CPU utilization for no gain if you store these files on a compressed dataset. However, if you have raw .wav rips of CDs or .vob rips of DVDs, you'll see a performance gain using a compressed dataset.

### 6.3.6 Creating a zvol

A zvol (ZFS volume) is a feature of ZFS that creates a device block over ZFS. This allows you to use a zvol as an iSCSI device extent.

To create a zvol, go to Storage -> Volumes -> Create ZFS Volume which will open the screen shown in Figure 6.3e. Note that this menu option is not available until after you have created a ZFS volume.

**Figure 6.3e: Creating a zvol**

The configuration options are described in Table 6.3c:

**Table 6.3c: zvol Configuration Options**

Setting	Value	Description
Existing Volume	drop-down menu	select existing ZFS pool to create the zvol from
ZFS Volume Name	string	input a name for the zvol
Size	integer	specify size and value such as 10G

Setting	Value	Description
Compression Level	drop-down menu	inherit means it will use the same compression level as the existing zvol used to create the zvol

### 6.3.7 Setting Permissions

Setting permissions is an important aspect of configuring a share so that FreeNAS™ volumes are accessible to the clients in your network. The graphical administrative interface is meant to set the initial permissions for a volume or dataset in order to make it available as a share. Once a share is available, the client operating system can be used to fine-tune the permissions of the files and directories that are created by the client.

[Section 7 Sharing](#) contains configuration examples for several types of permission scenarios. This section provides an overview of the screen that is used to set those permissions.

Once a volume or dataset is created, it will be listed by its mount point name in Storage -> View All Volumes. If you click the Change Permissions icon for a specific volume/dataset, you will see the screen shown in Figure 6.3f. Table 6.3d summarizes the options in this screen.

**Figure 6.3f: Changing Permissions on a Volume or Dataset**

The screenshot shows a 'Change Permissions' dialog box with the following fields and options:

- Change permission on /mnt/backups to:**
  - Owner (user):** root
  - Owner (group):** wheel
- Mode:**

	Owner	Group	Other
Read	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Execute	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- Type of ACL:**
  - Unix
  - Windows
- Set permission recursively:**
- Buttons:** Change, Cancel

**Table 6.3d: Options When Changing Permissions**

Setting	Value	Description
Owner(user)	drop-down menu	user to have permission to the volume/dataset; user must be created first if it does not already exist
Owner(group)	drop-down menu	group to have permission to the volume/dataset; group must be created first if it does not already exist and desired users need to be added as members of the group
mode	checkboxes	check the desired permissions for user, group, and other
Type of ACL	bullet selection	Unix and Windows ACLs are mutually exclusive, this means that <b>you must select the correct type of ACL to match the share</b> ; see the NOTE below for more details
recursive	checkbox	if checked, permissions will also apply to subdirectories of the volume or dataset; if you edit the owner and/or group at a later time, be sure to check this box so that the change is populated to all of the directories

**NOTE regarding Type of ACL:** when in doubt, or if you have a mix of operating systems in your network, always select Unix ACLs as all clients understand them. The only time there is a benefit to picking Windows ACLs is when your network only contains Windows clients *and* you are configuring CIFS shares. You will also want to use Windows ACLs if you are configuring the Active Directory service for a network that only contains Windows clients. Windows ACLs add a superset of permissions that augment those provided by Unix ACLs. This means that only Windows clients understand Windows ACLs. While Windows clients can understand Unix ACLs, they won't benefit from the extra permissions provided by Active Directory and Windows ACLs when Unix ACLs are used.

### 6.3.8 Viewing Volumes

If you click View All Volumes, you can view and further configure each volume and dataset, as seen in the example shown in Figure 6.3g.

The five icons towards the top of the right frame allow you to: create another volume, create a ZFS dataset, create a ZFS volume, import a volume, and auto import a volume.

The seven icons associated with a ZFS volume entry allow you to:

- **Export Volume:** this button will perform an export or a delete, depending upon the choice you make in the screen that pops up when you click this button. The pop-up message, seen in Figure 6.3h, will show the current used space, provide the check box "Mark the disks as new (destroy data)", prompt you to make sure that you want to do this, warn you if the volume has any associated shares and ask if you wish to delete them, and the browser will turn red to alert you that you are about to do something that will make the data inaccessible. If you *do not* check that box, the volume will be exported. This means that the data is not destroyed and the volume can be re-imported at a later time. If you will be moving a ZFS drive from one system to another, you should first [export](#) it. This operation flushes any unwritten data to disk, writes data to the disk indicating that the export was done, and removes all knowledge of the pool from the system. If you *do* check that box, the volume and all of its data will be destroyed and the

underlying disks will be returned to their raw state.

Figure 6.3g: Viewing Volumes

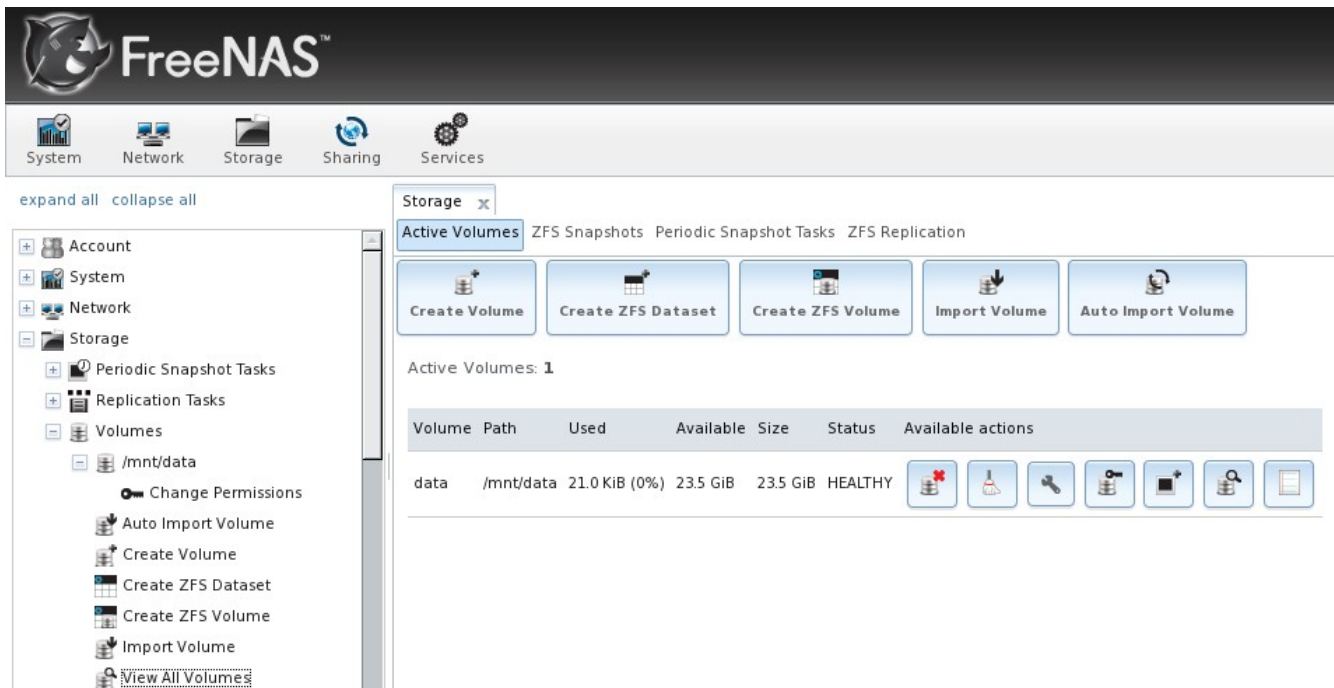
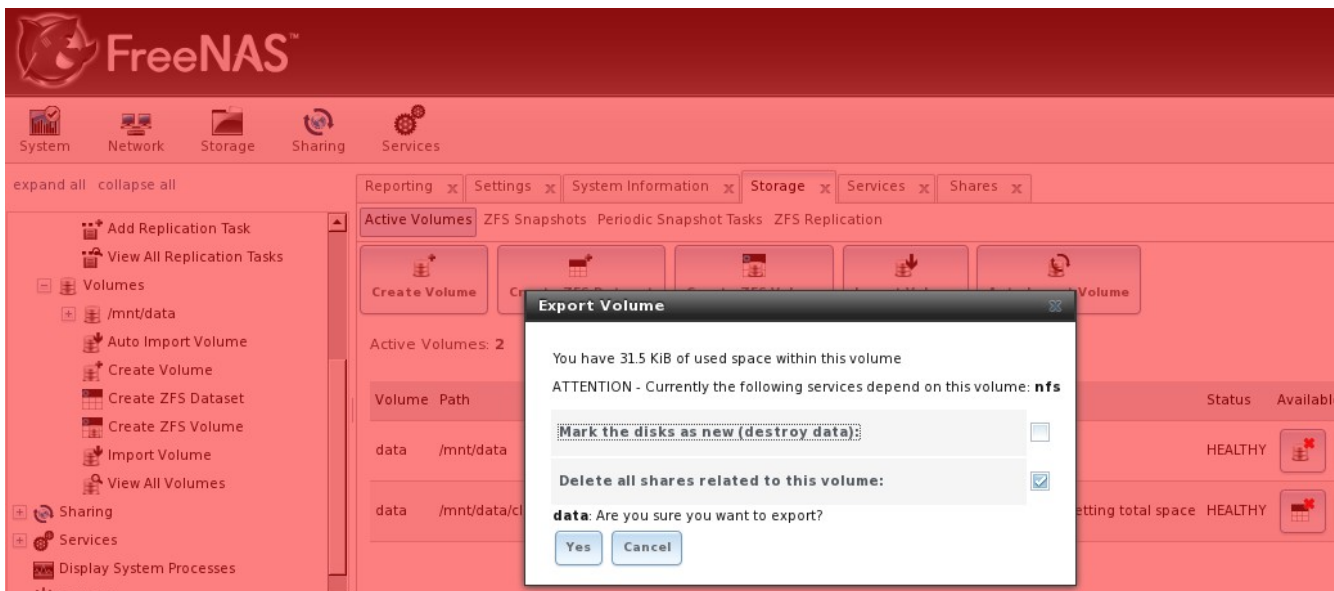


Figure 6.3h: Exporting or Deleting a Volume



- **Scrub Volume:** the [ZFS Best Practices Guide](#) recommends that you should run a ZFS scrub on a regular basis to identify data integrity problems. If you have consumer-quality drives, consider a weekly scrubbing schedule. If you have datacenter-quality drives, consider a monthly scrubbing schedule. You should also scrub a volume prior to replacing any of its drives.



- **Edit ZFS Options:** allows you to edit the volume's compression level, atime setting, dataset quota, and reserved space for quota.
- **Change Permissions:** allows you to edit the volume's user, group, Unix rwx permissions, and to enable recursive permissions on the volume's subdirectories.
- **Create Snapshot:** allows you to configure the snapshot's name and whether or not it is recursive before manually creating a snapshot of the ZFS volume.
- **View Disks:** will display each disk's numeric ID, FreeBSD device name, serial number, UUID, description, transfer mode, HDD standby setting, advanced power management setting, acoustic level, whether S.M.A.R.T is enabled, S.M.A.R.T extra options, and group membership. An Edit button is included should you wish to modify any of these settings. A Replace button is included should the disk fail and ZFS needs to be made aware that the disk has been replaced.
- **zpool status:** will show the device name and status of each disk in the ZFS pool.

If you click the View Disks icon → Edit, you'll see the screen shown in Figure 6.3i.

**Figure 6.3i: Editing a Volume's Disk Options**

Property	Value
Name	ada0p2
Identifier	{uuid}66f5ce4f-c83f-11e0-87
Description	Member of backups stripe
Transfer Mode	Auto
HDD Standby	Always On
Advanced Power Management	Disabled
Acoustic Level	Disabled
Enable S.M.A.R.T.	<input checked="" type="checkbox"/>
S.M.A.R.T. extra options	

Table 6.3d summarizes the configurable options.

**Table 6.3d: Editable Options for a Volume's Disk**

Setting	Value	Description
Name	string	read-only value showing FreeBSD device name for disk
Identifier	string	read-only value showing the UUID of the disk (name may change with hot-swappable devices but the UUID does not)
Description	string	by default will show name of volume
Transfer Mode	drop-down menu	default is auto, can also specify transfer mode used by hardware
HDD Standby	drop-down menu	indicates the time of inactivity (in minutes) before the drive enters standby mode in order to conserve energy; the default is always on
Advanced Power Management	drop-down menu	default is disabled, can select a power management profile from the menu
Acoustic Level	drop-down menu	default is disabled, can be modified for disks that understand <a href="#">AAM</a>
Enable <a href="#">S.M.A.R.T</a>	checkbox	on by default
S.M.A.R.T extra options	string	smartctl(8) options
Group Membership	drop-down menu	the volume the disk is a member of

### 6.3.9 Replacing a Failed Drive

If you are using any form of RAID, you should replace a failed drive as soon as possible to repair the degraded state of the RAID. Go to Storage -> Volumes -> View All Volumes. Click the View Disks button of the associated volume which will list all of the disks within the volume. Locate the failed disk and click its Replace button. Select an unused drive from the drop-down menu in the pop-up menu that appears, then click the Replace disk button. In the example shown in Figure 6.3j, failed disk *ada0* is being replaced by disk *ada3*.

As seen in the example shown in Figure 6.3k, once you click the Replace disk button, the failed disk will be placed at the bottom of the list and will now have a Detach button. Click Yes to confirm and the disk will be removed from the list of member disks.

Figure 6.3j: Replacing a Failed Disk

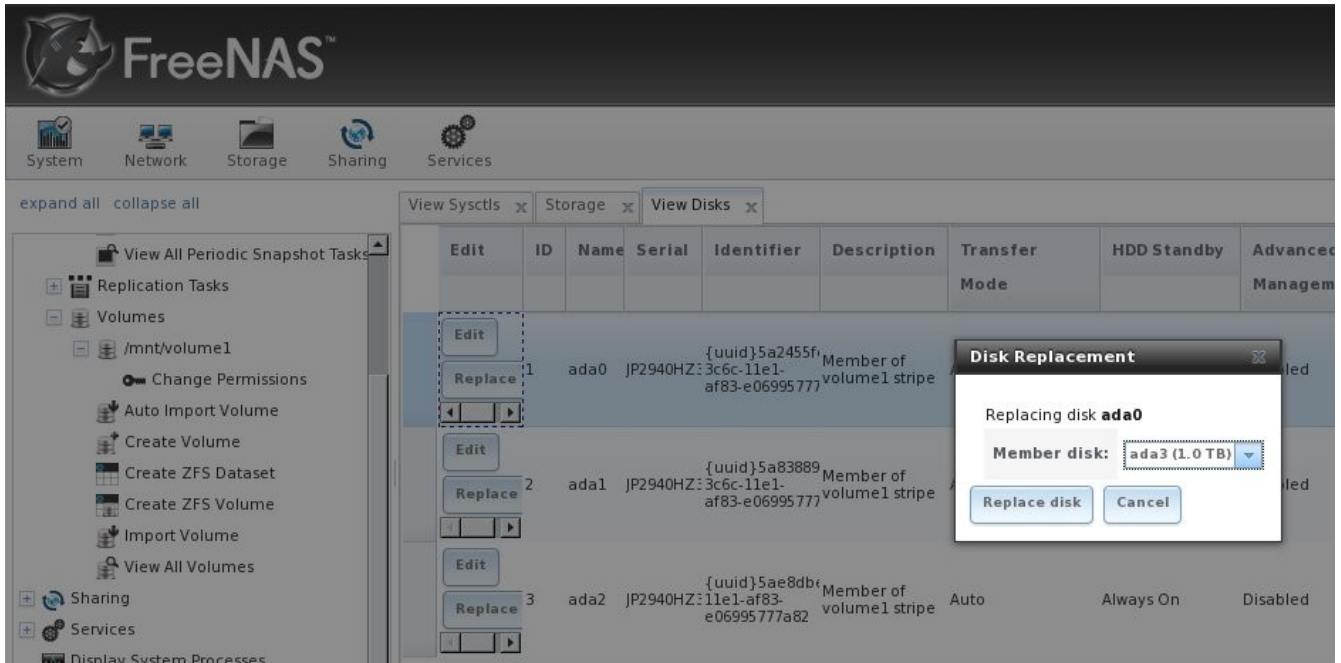
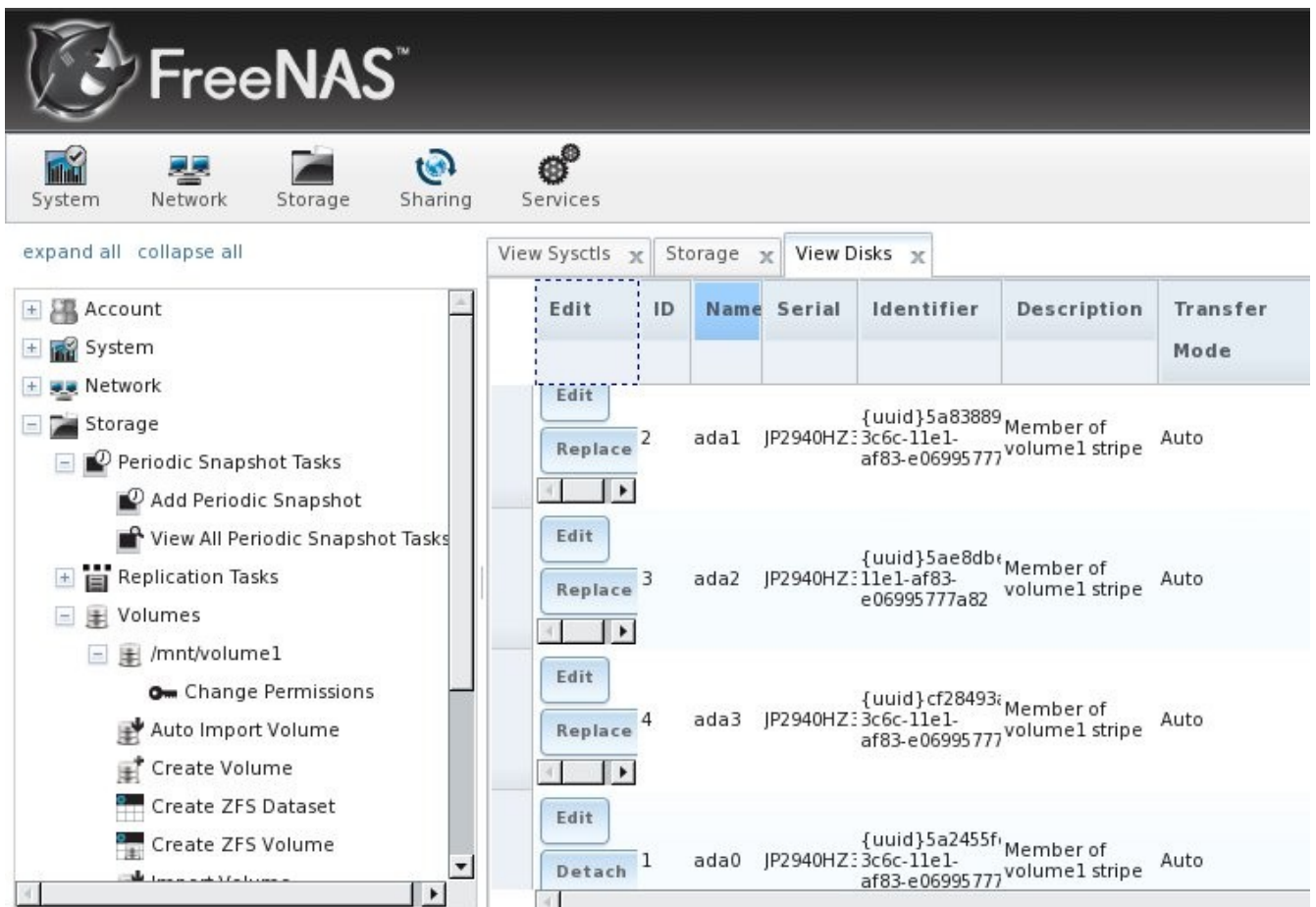


Figure 6.3k: Detaching the Failed Disk



### 6.3.10 Hot Swapping a ZFS Failed Drive

Until the hot swapping improvements that became available in FreeBSD 9.0 are backported to FreeNAS™, ZFS will not automatically detach from the underlying GEOM provider. This means that care must be taken when hot swapping a drive. The following procedure is recommended:

- **do NOT hot-pull the disk BEFORE making the operating system aware of your intent** as this could cause more problems
- from the FreeNAS™ console, use the `swapctl -l` command to determine the device name of the disk's swap partition, then run `swapoff <devicename>` to disable that swap device
- from the FreeNAS™ console, offline the disk to be removed using the command `zpool offline <poolname> <diskname>`

At this point, the disk can be hot-pulled from the system. Insert the new disk and recreate the same disk layout. **Make sure that the size of the swap partition is the same as the rest of the disks in the pool.** The following example creates a swap size of 2GB on disk `da11`:

```
gpart create -s gpt da11
gpart add -b 128 -s 4194304 -t freebsd-swap da11
gpart add -t freebsd-zfs da11
```

Next, issue the following commands to replace the disk, turn swap back on, and to detach from the pool:

```
zpool replace tank da11p2
/etc/rc.d/swap1 start
zpool detach tank da11p2/old
```

## 7 Sharing Configuration

Once you have a volume, create at least one share so that the storage is accessible by the other computers in your network. The type of share you create depends upon the operating system(s) running in your network:

**AFP Shares:** the Apple File Protocol (AFP) type of share is the best choice if all of your computers run Mac OS X.

**CIFS Shares:** the Common Internet File System (CIFS) type of share is accessible by Windows, Mac OS X, Linux, and BSD computers, but it is slower than an NFS share due to the single-threaded design of Samba. If your network contains only Windows systems, this is a good choice. However, it is a poor choice if the CPU on the FreeNAS™ system is limited; if your CPU is maxed out, you need to upgrade the CPU or consider another type of share.

**NFS Shares:** the Network File System (NFS) type of share is accessible by Mac OS X, Linux, BSD, and the professional/enterprise versions (not the home editions) of Windows. It is a good choice if there are many different operating systems in your network. Depending upon the operating system, it may require the installation or configuration of client software on the desktop.

If you are looking for a solution that allows fast access from any operating system, consider configuring the FTP service instead of a share and use a cross-platform FTP and file manager client application such as [Filezilla](#).

If data security is a concern and your network's users are familiar with SSH command line utilities or [WinSCP](#), consider configuring the SSH service instead of a share. It will be slower than unencrypted FTP due to the overhead of encryption, but the data passing through the network will be encrypted.

**NOTE:** while the GUI will let you do it, it is a bad idea to share the same volume using multiple types of access methods. Different types of shares and services use different file locking methods. For example, if the same volume is configured to use both NFS and FTP, NFS will lock a file for editing by an NFS user, but a FTP user can simultaneously edit or delete that file. This will result in lost edits and confused users. Another example: if a volume is configured for both AFP and CIFS, Windows users may be confused by the extra filenames used by Mac files and delete the ones they don't understand; this will corrupt the files on the AFP share. In other words, pick the one type of share or service that makes the most sense for the types of clients that will access that volume, and configure that volume for that one type of share or service.

## 7.1 AFP Shares

FreeNAS™ uses AFP (Apple Filing Protocol) to share data with Apple systems. Configuring AFP shares is a multi-step process that requires you to create users and groups, set volume/dataset permissions, create your AFP share(s), configure the AFP service in Services -> AFP, then enable the AFP service in Services -> Control Services. This section shows the configuration screen for creating the AFP share and demonstrates how to connect from a Mac OS X client once the AFP service has started.

### 7.1.1 Creating AFP Shares

If you click Sharing -> AFP Shares → Add AFP Share, you will see the screen shown in Figure 7.1a.

Table 7.1a summarizes the available options when creating an AFP share.

**Figure 7.1a: Creating an AFP Share**

**Table 7.1a: AFP Share Configuration Options**

Setting	Value	Description
Name	string	volume name that will appear in the Mac computer's "connect to server" dialogue; limited to 27 characters and can not contain a period
Share Comment	string	optional
Path	browse button	browse to the volume/dataset to share
Share password	string	recommended; maximum of 8 characters
Share <a href="#">Character Set</a>	string	examples include UTF8 and ISO-8859-15
Allow List	string	comma delimited list of allowed users and/or groups where groupname begins with a @
Deny List	string	comma delimited list of denied users and/or groups where groupname begins with a @
Read-only Access	string	comma delimited list of users and/or groups who only have read access where groupname begins with a @

Setting	Value	Description
Read-write Access	string	comma delimited list of users and/or groups who have read and write access where groupname begins with a @
Disk Discovery	check box	enable if there is no DNS record for the FreeNAS™ system
Disk discovery mode	drop-down menu	default or Time Machine (Apple's backup utility)
Database Path	string	by default, the CNID databases used by AFP are located the root of the volume
Cache CNID	checkbox	if checked, AFP uses the ID information stored in AppleDouble header files to reduce database load; do <b>not</b> set this option if the volume is modified by non-AFP clients (e.g. NFS or CIFS)
Translate CR/LF	checkbox	if enabled, AFP will automatically convert Macintosh line breaks into Unix ones; some older programs store binary data files as type "TEXT" when saving and switch the file type in a second step and enabling this checkbox will break those files
Windows File Names	checkbox	forces filename restrictions imposed by older versions of Windows; it is NOT recommended for volumes mainly used by Macs as it breaks some the ability of some applications to save files (e.g. OfficeX)
No <a href="#">AppleDouble</a>	checkbox	forces AFP to not create .AppleDouble directories when a non-Mac client saves a file; you can't avoid the creation of .AppleDouble directories when a Mac client writes so try to avoid this option whenever possible
Zero Device Numbers	checkbox	enable when the device number is not constant across a reboot
Disable File ID	checkbox	if enabled, AFP will not advertise createfileid, resolveid, and deleteid calls
Disable :hex Names	checkbox	if this box is checked, AFP disables :hex translations for anything except dot files; this option makes the / character illegal
ProDOS	checkbox	if checked, provides compatibility with Apple II clients
No Stat	checkbox	if checked, AFP won't stat the volume path when enumerating the volumes list; useful for automounting or volumes created by a preexec script
AFP3 Privs	UNIX checkbox	do not enable if network contains Mac OS X 10.4 clients as they do not support this

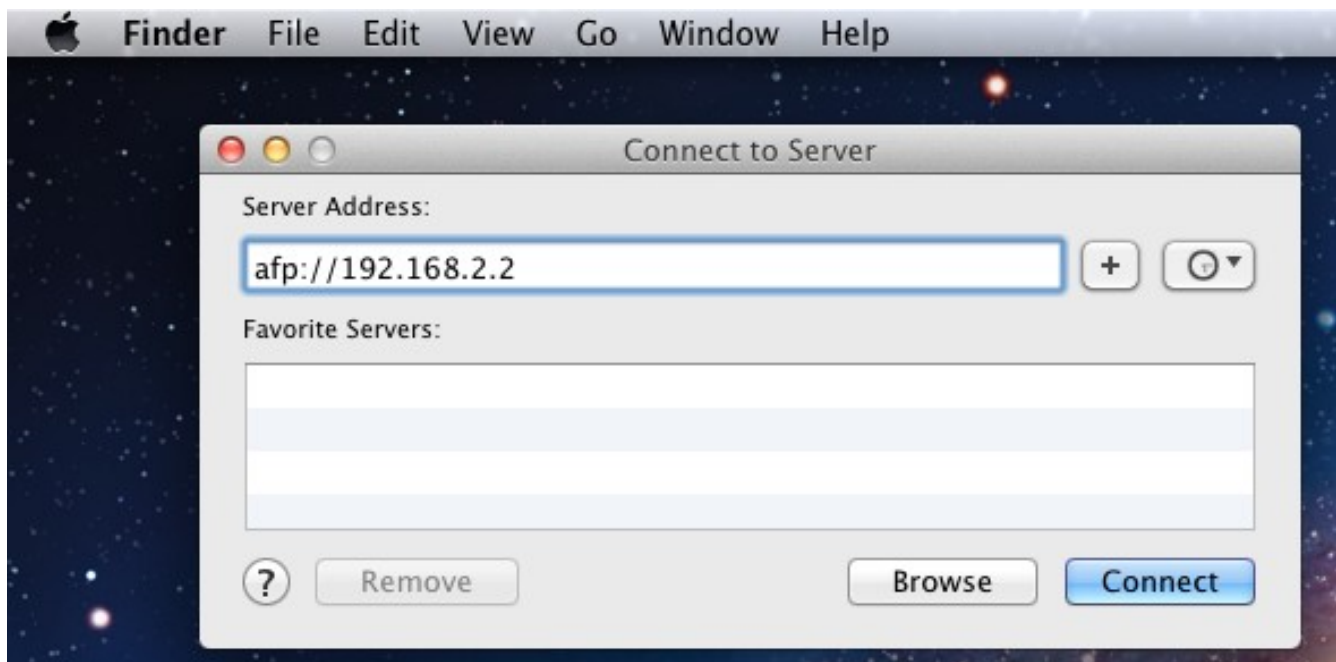
### 7.1.2 Connecting to AFP Shares As Guest

AFP supports guest logins, meaning that all of your Mac OS X users can access the AFP share without having to first create user accounts on the FreeNAS™ system or a ZFS dataset for each user. In this configuration example, the AFP share has been configured for guest access as follows:

1. A ZFS volume named `/mnt/data` has its permissions set to the `nobody` user account and the `nobody` group.
2. An AFP share with a Name of `freenas` has been created with a Path of `/mnt/data`, a Share Password has been set, the Allow List is set to `nobody` and Read-write Access has been set to `nobody`. The Disk Discovery checkbox has been checked and the IP address of the FreeNAS™ system is 192.168.2.2.
3. The Services -> AFP has been configured as follows: Server Name is `freenas`, the Guest Access checkbox is checked, `nobody` is selected in the Guest account drop-down menu, and the Local Access checkbox is unchecked.

Once the AFP service has been started in Services -> Control Services, Mac OS X users can connect to the AFP share by clicking Go -> Connect to Server. In the example shown in Figure 7.1b, the user has input `afp://` followed by the IP address of the FreeNAS™ system.

**Figure 7.1b: Connect to Server Dialogue**



Click the Connect button and a login box, seen in Figure 7.1c, will appear. Since a password has been configured for this AFP share, the user must input the share password (i.e. not their own password).

Once connected, Finder will automatically open. The name of the AFP share will be displayed in the SHARED section in the left frame and the contents of the share will be displayed in the right frame. In the example shown in Figure 7.1d, `/mnt/data` has one folder named images. The user can now copy files to and from the share.

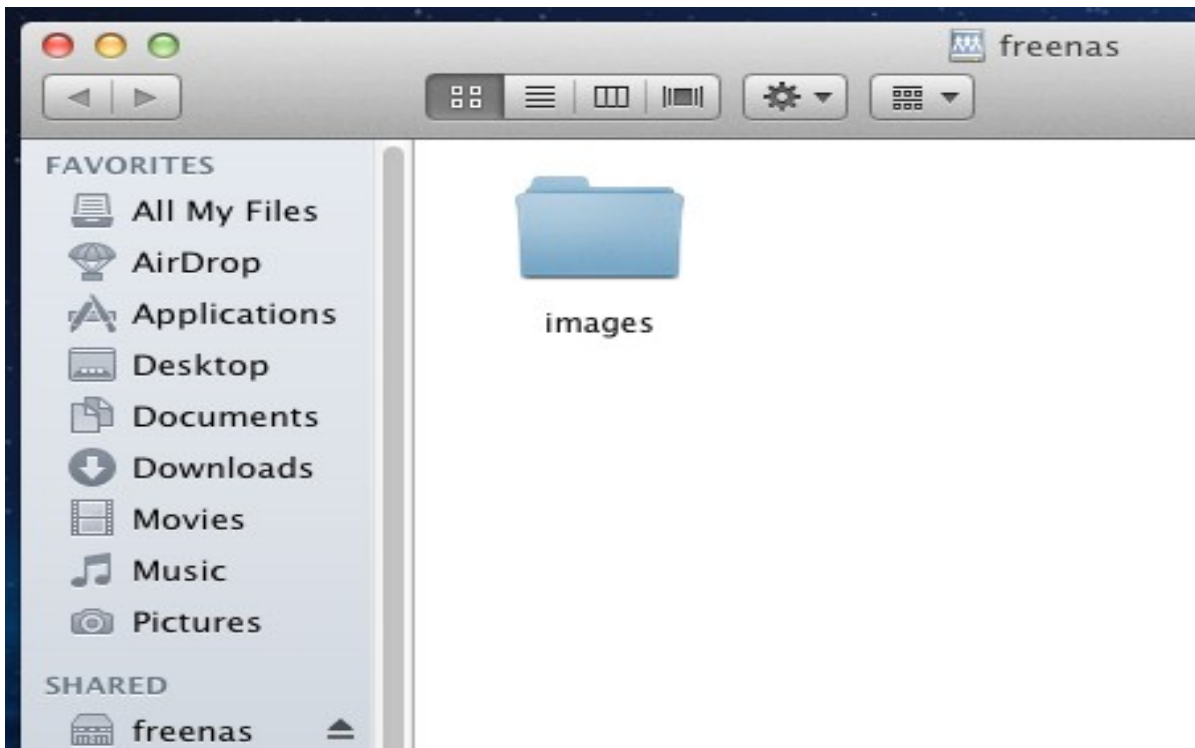
To disconnect from the volume, click the eject button in the Shared sidebar.



Figure 7.1c: Authenticating to the AFP Share



Figure 7.1d: Viewing the Contents of the Share From a Mac System



### 7.1.3 Using Time Machine

Mac OS X includes Time Machine which can be used to schedule automatic backups. In this configuration example, Time Machine will be configured to backup to an AFP share on a FreeNAS™ system. To configure the AFP share on the FreeNAS™ system:

1. A ZFS dataset named */mnt/data/backup\_user1* with a quota of 60G was created in Storage -> Create ZFS Dataset.
2. A user account was created as follows: Username of *user1*, Primary Group ID was left empty, Home Directory of */mnt/data/backup\_user1*, and the Full Name, E-mail, and Password fields were set. The Username and Password of the created account match the values on the Mac OS X system.
3. An AFP share with a Name of *backup\_user1* has been created with a Path of */mnt/data/backup\_user1*, the Allow List is set to *user1* and Read-write Access has been set to *user1*. The Disk Discovery checkbox has been checked, the Disk Discovery mode is set to *Time Machine* and the IP address of the FreeNAS™ system is 192.168.2.2.
4. Services -> AFP has been configured as follows: Server Name is *freenas*, the Guest Access checkbox is unchecked, and the Local Access checkbox is checked.
5. The AFP service has been started in Services -> Control Services.

To configure Time Machine on the Mac OS X client, go to System Preferences -> Time Machine which will open the screen shown in Figure 7.1e. Click ON and a pop-up menu should show the FreeNAS™ system as a backup option. In our example, it is listed as *backup\_user1 on "freenas"*. Highlight the entry representing the FreeNAS™ system and click the Use Backup Disk button. A connection bar will open and will prompt you for the user account's password--in this example, the password for the *user1* account.

Time Machine will create a full backup after waiting two minutes. It will then create a one hour incremental backup for the next 24 hours, and then one backup each day, each week and each month. Since the oldest backups are deleted when the ZFS dataset becomes full, make sure that the quota size you set is sufficient to hold the backups. Note that a default installation of Mac OS X is ~21GB in size.

If you receive a "Time Machine could not complete the backup. The backup disk image could not be created (error 45)" error when backing up to the FreeNAS™ system, you will need to create a sparsebundle image using [these instructions](#).

**Figure 7.1e: Configuring Time Machine on Mac OS X Lion**



## 7.2 CIFS Shares

FreeNAS™ uses [Samba](#) to share volumes using Microsoft's CIFS protocol. CIFS is built into the Windows and Mac OS X operating systems and most Linux and BSD systems pre-install the Samba client (which provides CIFS). If your distro did not, check your distro's software repository to install the Samba client.

Configuring CIFS shares is a multi-step process that requires you to set permissions, create CIFS share(s), configure the CIFS service in Services -> CIFS, then enable the CIFS service in Services -> Control Services. If your Windows network has a Windows server running Active Directory, you will also need to configure the Active Directory service in Services -> Active Directory. Depending upon your authentication requirements, you may also need to create users and groups. This section will demonstrate some common configuration scenarios:

- If you would like an overview of the configurable parameters, see [section 7.2.1 Creating CIFS Shares](#).
- If you would like an example of how to configure access that does not require authentication, see [section 7.2.2 Configuring Anonymous Access](#).
- If you would like each user to authenticate before accessing the share, see [section 7.2.3](#)

## [Configuring Local User Access.](#)

- If you are having problems accessing your CIFS share, see [Troubleshooting Tips](#).

### 7.2.1 Creating CIFS Shares

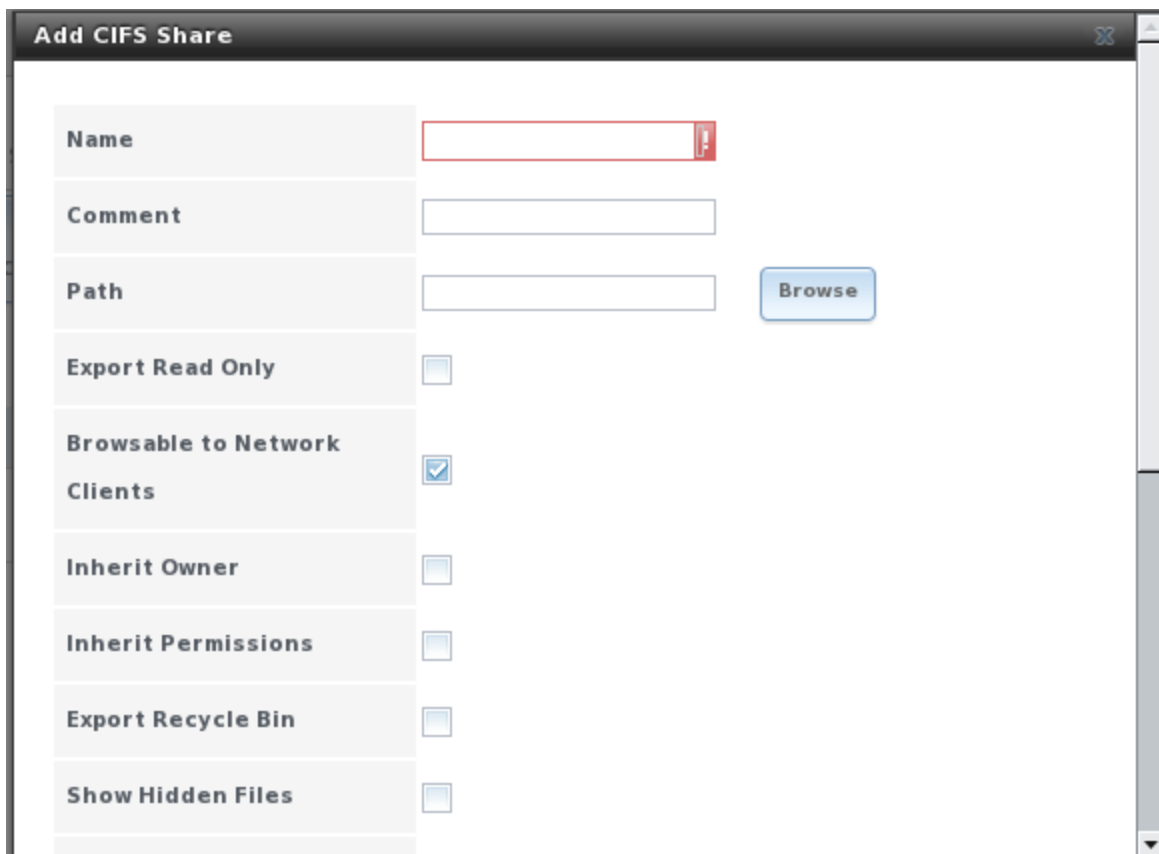
Figure 7.2a shows the configuration screen that appears when you click Sharing -> CIFS Shares -> Add CIFS Share. Table 7.2a summarizes the options when creating a CIFS share. The values you use will vary by configuration example.

If you wish some files on a shared volume to be hidden and inaccessible to users, put a **veto files=** line in the Auxiliary Parameters field. The syntax for this line and some examples can be found [here](#).

If you have created multiple CIFS shares that contain symbolic links pointing to each other, add the following lines to Auxiliary Parameters so that CIFS clients can follow the links:

```
unix extensions = no  
follow symlinks = yes  
wide links = yes
```

**Figure 7.2a: Adding a CIFS Share**



Name	<input type="text"/>
Comment	<input type="text"/>
Path	<input type="text"/> <input type="button" value="Browse"/>
Export Read Only	<input type="checkbox"/>
Browsable to Network Clients	<input checked="" type="checkbox"/>
Inherit Owner	<input type="checkbox"/>
Inherit Permissions	<input type="checkbox"/>
Export Recycle Bin	<input type="checkbox"/>
Show Hidden Files	<input type="checkbox"/>

**Table 7.2a: Options for a CIFS Share**

Setting	Value	Description
Name	string	mandatory; name of share e.g. Movies
Comment	string	optional
Path	browse button	select volume/dataset to share
Export Read Only	checkbox	prohibits write access to the share
Browsable to Network Clients	checkbox	enables Windows clients to browse the shared directory using Windows Explorer
Owner Group	checkbox	if left unchecked, the owner's group is taken from the logged in user of the share
Inherit Permissions	checkbox	if checked, permissions on new files and directories are inherited from parent directory
Export Recycle Bin	checkbox	deleted files are moved to a recycle directory instead of being deleted
Show Hidden Files	checkbox	will display hidden files
Guest Account	drop-down menu	account to use for guest access
Allow Guest Access	checkbox	guest user will not be required to login in order to access the share
Only Allow Guest Access	checkbox	forces guest access
Hosts Allow	string	comma, space, or tab delimited list of allowed hostnames or IP addresses
Hosts Deny	string	comma, space, or tab delimited list of denied hostnames or IP addresses; allowed hosts take precedence so can use ALL here and specify allowed hosts in Hosts Allow
Auxiliary Parameters	string	add additional <a href="#">smb.conf</a> parameters not covered by other option fields

### 7.2.2 Configuring Anonymous Access

If you would like to share a volume with all of the users in your network without requiring them to input a password, you can configure anonymous CIFS sharing. The following steps are needed for this type of configuration:

1. **Create a volume** in Storage -> Volumes -> Create Volume.
2. **Create a guest user account** in Account -> Users -> Add User. In the screen shown in Figure 7.2b, input the username of *guest*, input the name of the volume you created as the home directory (in this example, */mnt/shared*), input a description in the full name (in this example, *cifs anon access*), check the disable logins box, and click OK to create the account.

**Figure 7.2b: Creating a Guest Account for Anonymous Access**

The screenshot shows a window titled "Add User" with a close button in the top right corner. The window contains several input fields and a checkbox:

- User ID: 1,002
- Username: guest
- Primary Group: (empty dropdown menu)
- Home Directory: /mnt/shared
- Shell: csh (dropdown menu)
- Full Name: cifs anon access
- E-mail: (empty)
- Password: (empty)
- Password confirmation: (empty)
- Disable logins:

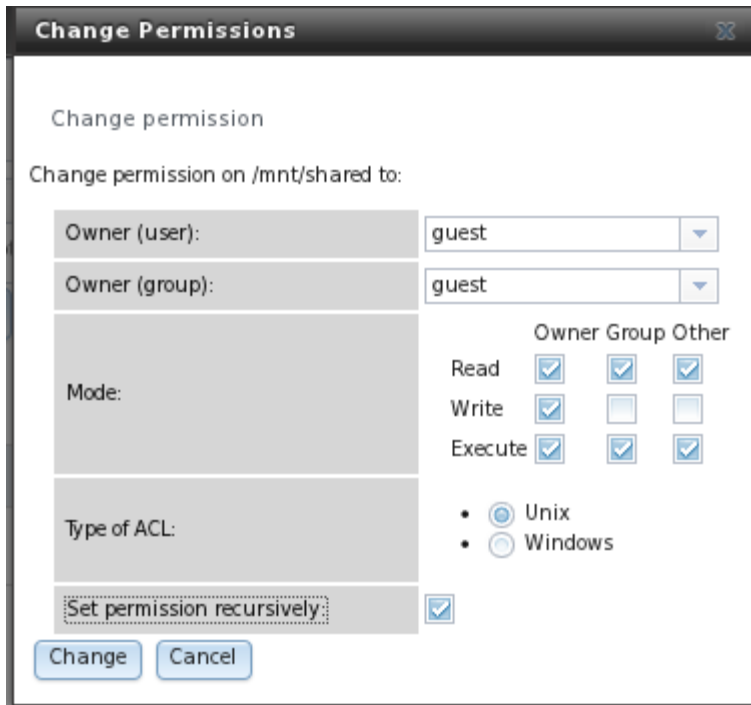
At the bottom of the window are two buttons: "OK" and "Cancel".

**3. Associate the guest account with the volume** in Storage -> Volumes. Click the volume's name then Change Permissions. In the screen shown in Figure 7.2c, select guest as the owner(user) and owner(group), check the permissions that are appropriate to your network, and check the set permissions recursively box. If non-Windows systems will be accessing the CIFS share, leave the type of permissions as Unix. Only change the type of permissions to Windows if the share is only accessed by Windows systems.

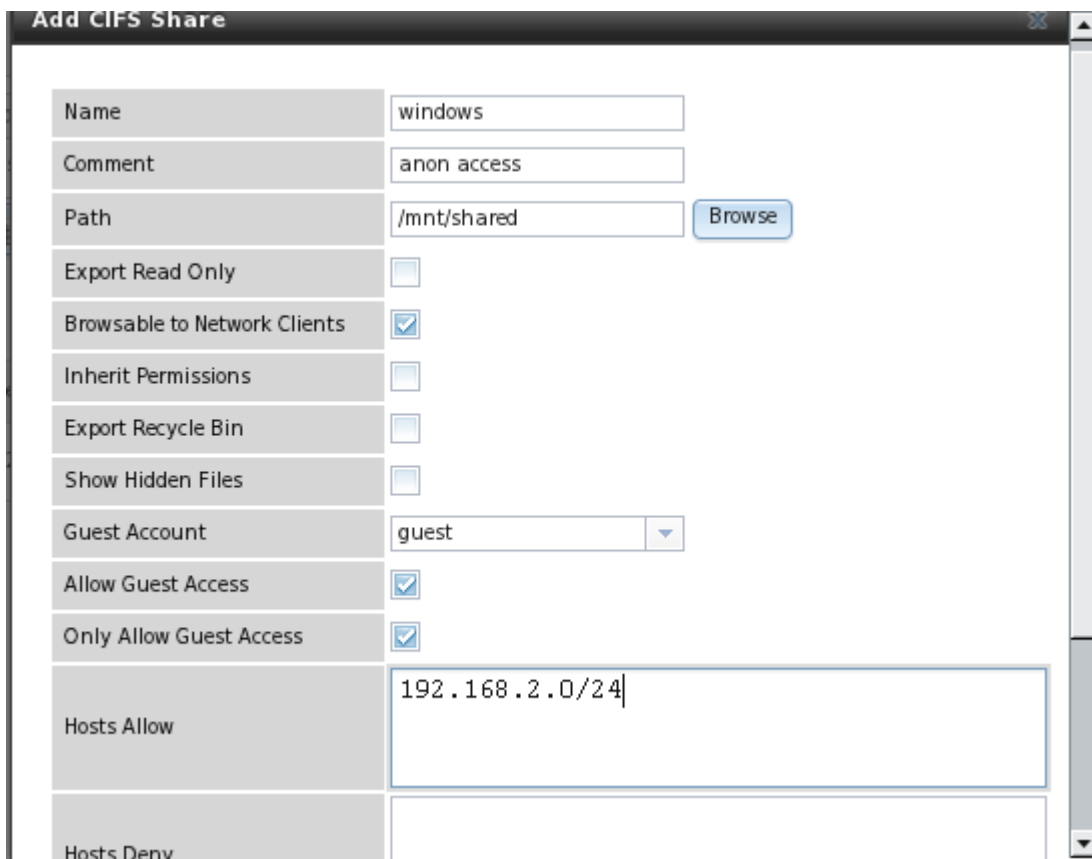
**4. Create a CIFS share** in Sharing -> CIFS Shares -> Add CIFS Share. In the screen shown in Figure 7.2d, input a name for the share (in this example, windows), input a comment (in this example, anon access), browse to the path of the volume (in this example, /mnt/shared), select guest as the guest account, check the boxes Allow Guest Access and Only Allow Guest Access, input the network address (in this example 192.168.2.0/24 will only allow hosts in the address range from 192.168.2.1 to 192.168.2.254), and click OK to create the share. If you have specific hosts on your network that you would like to exclude, you can add them in the hosts deny section. You can add a specific IP address (e.g. 192.168.2.7), one address per line, or specific subnets (for example, 192.168.2.32/27).

**5. Configure the CIFS service** in Services -> CIFS. In the screen shown in Figure 7.2e, select *Anonymous* as the authentication model, select *guest* as the guest account, check the boxes *Allow Anonymous Access*, *Only Allow Anonymous Access*, *Allow Empty Password*, and *Enable Home Directories*, browse to the volume name under home directories, and click OK.

**Figure 7.2c: Associating the Guest Account with the Volume**



**Figure 7.2d: Creating the CIFS Share**



**6. Start the CIFS service** in Services -> Control Services. Click the red OFF button next to CIFS. After a second or so, it will change to a blue ON, indicating that the service has been enabled.

**7. Test the connection.** To test from a Windows system, open Explorer, click on Network and you should see an icon named FREENAS. Since anonymous access has been configured, you should not be prompted for a username or password in order to see the share. An example is seen in Figure 7.2f.

If you click on the FREENAS icon, you can view the CIFS share that you created in step 4.

To prevent Windows Explorer from hanging when accessing the share, map the share as a network drive. To do this, right-click the share and select "Map network drive..." as seen in Figure 7.2g.

**Figure 7.2e: Configuring CIFS Service for Anonymous Access**

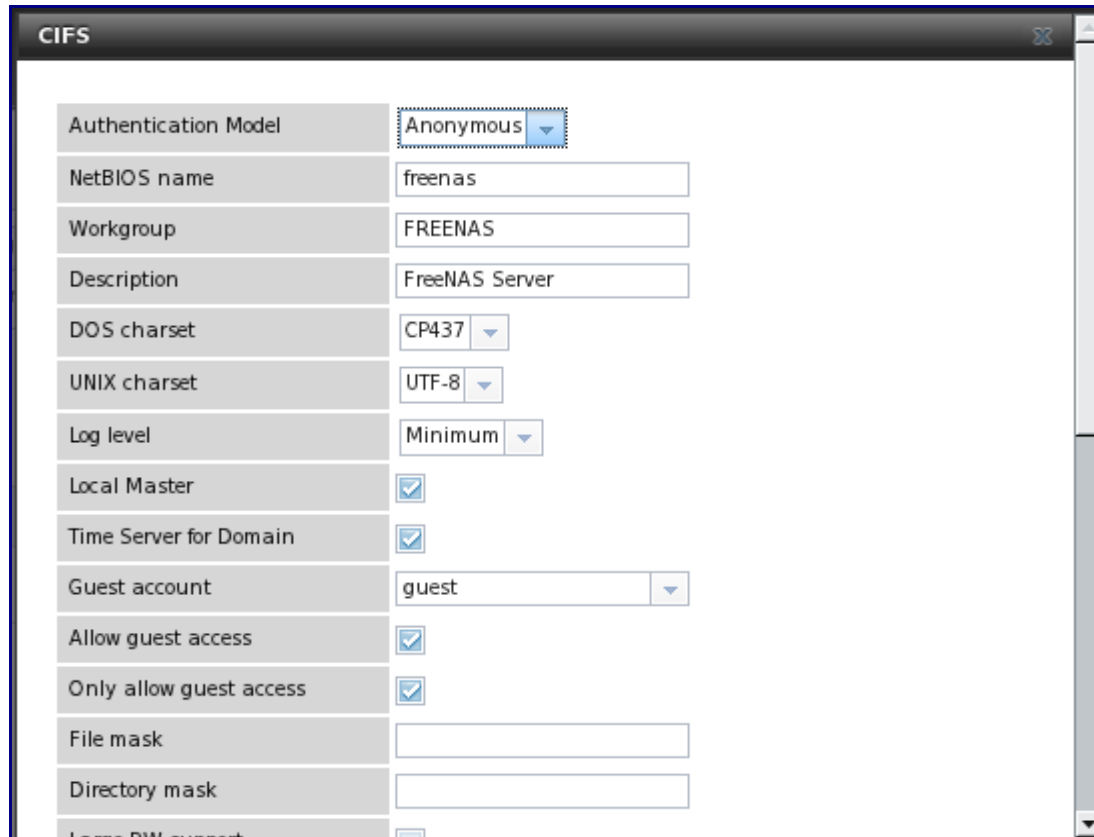




Figure 7.2f: Accessing the CIFS Share from a Windows Computer

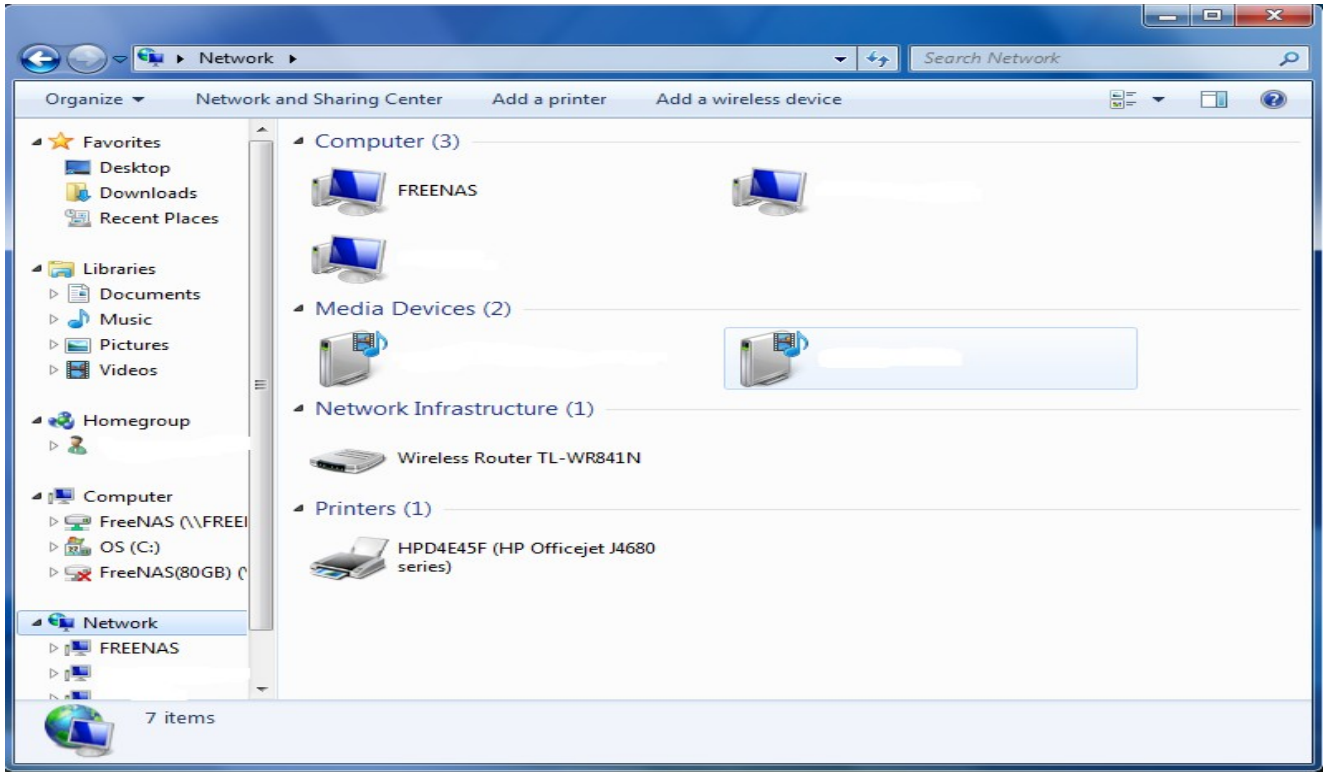
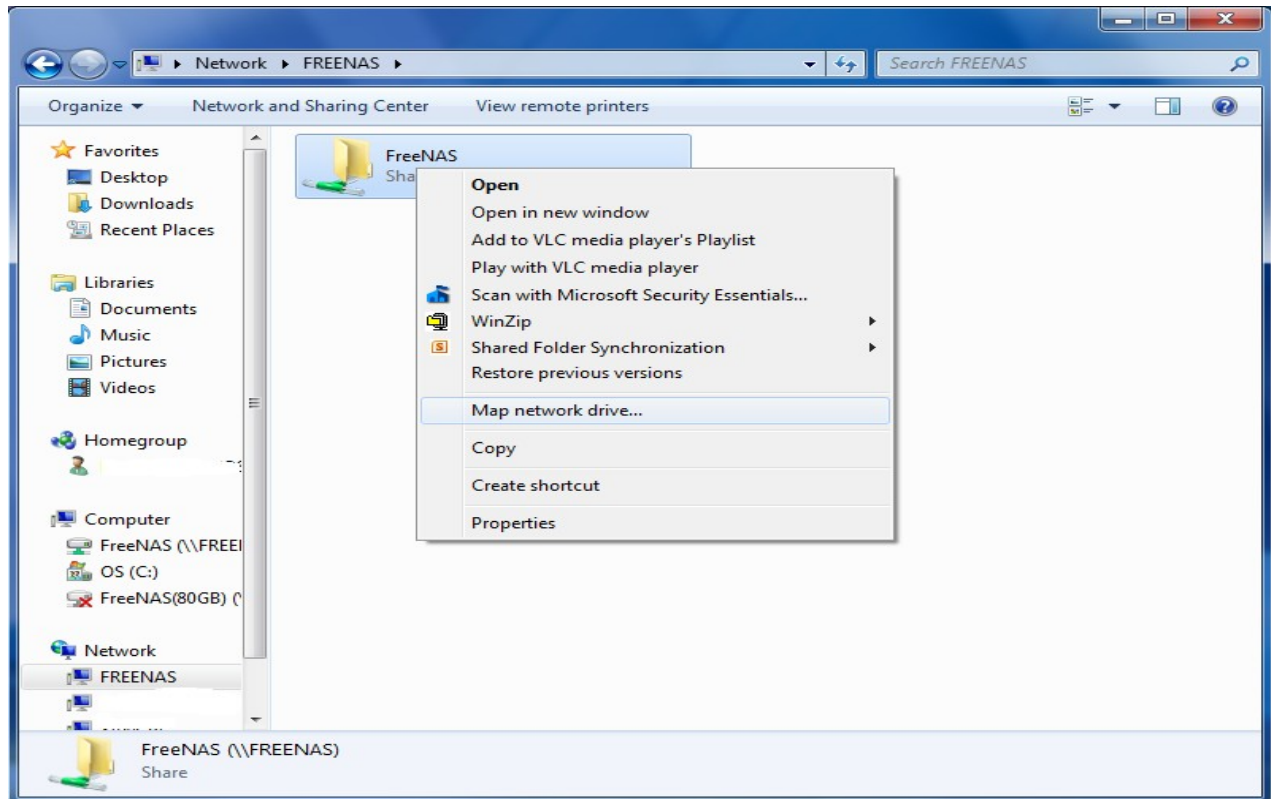
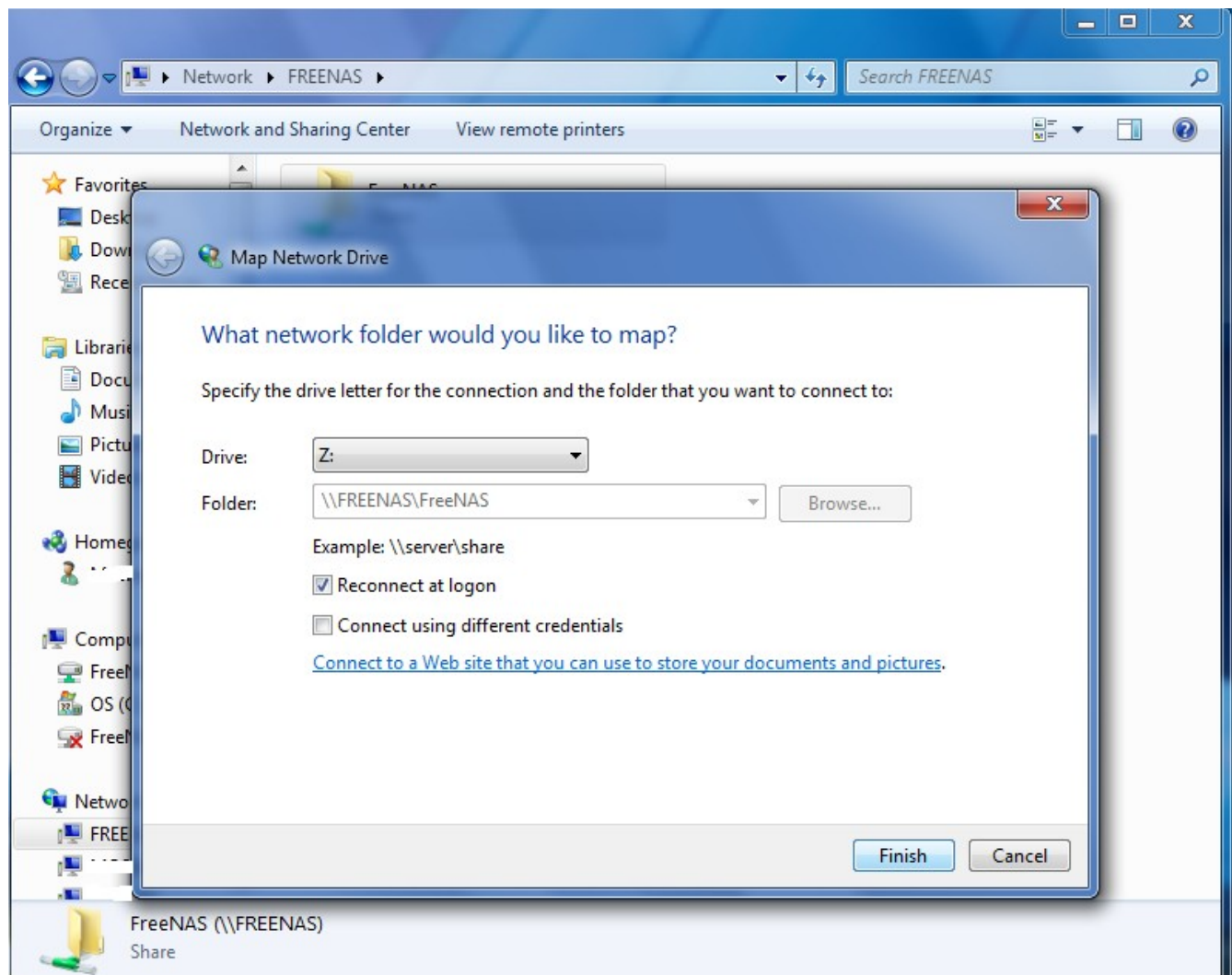


Figure 7.2g: Mapping the Share as a Network Drive



Choose a drive letter from the drop-down menu and click the Finish button as shown in Figure 7.2h.

**Figure 7.2h: Selecting the Network Drive Letter**



### 7.2.3 Configuring Local User Access

If you would like each user to authenticate before accessing the CIFS share, you need to configure local user access as follows:

- 1. Create a user account for each user** in Account -> Users -> Add User that matches their username and password on the client system. In the screen shown in Figure 7.2i, the Username is *user1* and the Home Directory points to the ZFS volume */mnt/test1*. When setting the username and password, use values that match existing user accounts that will be accessing the CIFS share; for example, use the existing Windows login names and passwords. Repeat this process to create a user account for every user that will need access to the CIFS share.

**Figure 7.2i: Creating a User Account**

User ID	1004
Username	user1
Primary Group	----- ▾
Home Directory	/mnt/test1
Shell	csh ▾
Full Name	Windows User1
E-mail	user1@somecompany.com
Password	.....
Password confirmation	.....
Disable logins	<input type="checkbox"/>

OK Cancel

**2. Create a group** in Account -> Groups -> Add Group. Once the group is created, click its Members button and add the user accounts that you created in step 1. In the example shown in Figure 7.2j, the user accounts *user1* and *user2* are being added to the group *windows*.

**3. Give the group permission to the volume** in Storage -> View All Volumes. In the example shown in Figure 7.2k, the */mnt/test1* volume is set to the user *nobody*, the group *windows*, and the write checkbox for Group has been checked as it is off by default. Make sure that you set the permissions on the volume that is the home directory for the users that you added to the group.

**4. Create a CIFS share** in Sharing -> CIFS Shares -> Add CIFS Share. In the example shown in Figure 7.2l, the Name of the share is *backups* the Path points to the ZFS volume */mnt/test1* and the Browsable to Network Clients box is checked.

**NOTE:** be careful about unchecking the Browsable to Network Clients box. When this box is checked (the default), other users will see the names of every share that exists using Windows Explorer, but they will receive a permissions denied error message if they try to access someone else's share. If this box is unchecked, even the owner of the share won't see it or be able to create a drive mapping for the share in Windows Explorer. They can still access the share from the command line, so this option may be desirable in networks where security is a concern and where users are comfortable using the command line.

Figure 7.2j: Create a Group

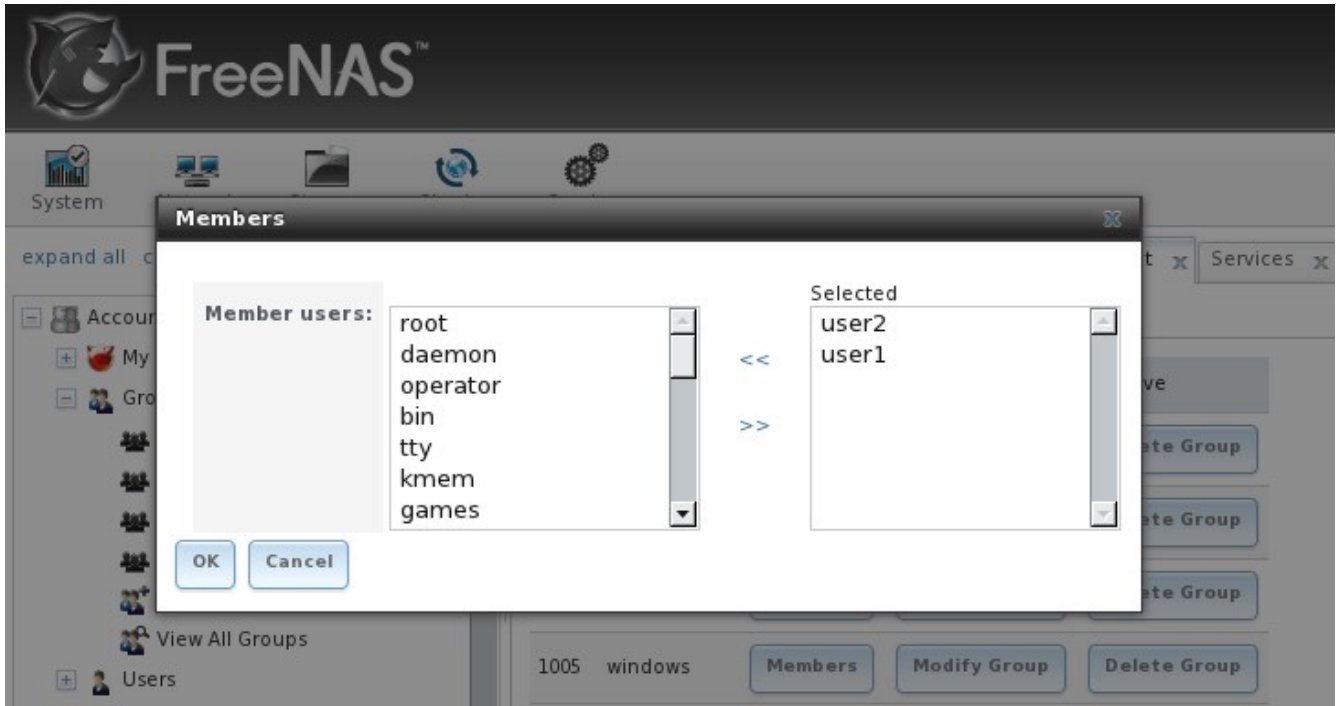
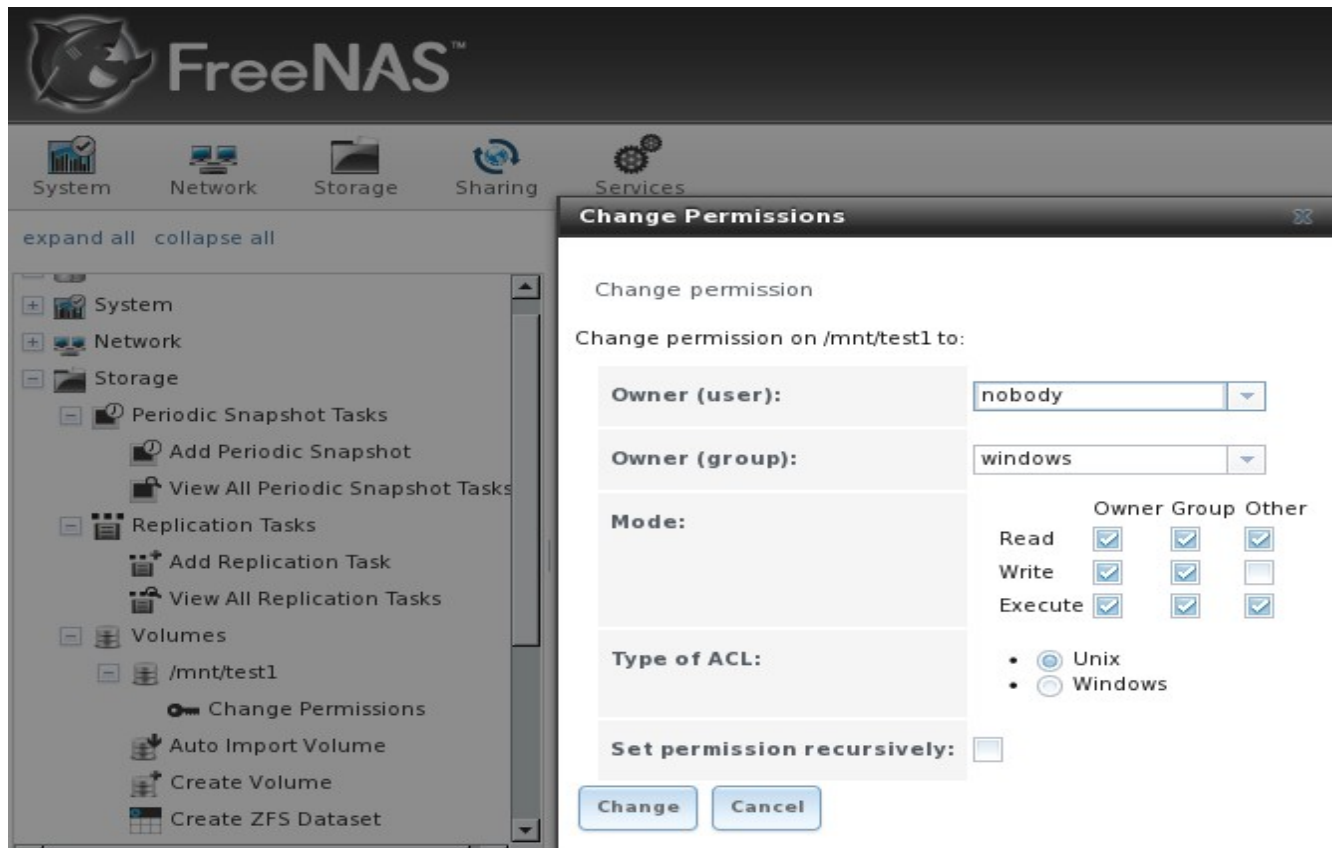


Figure 7.2k: Give the Group Permissions to the Volume



**Figure 7.2l: Creating the CIFS Share**

The screenshot shows a window titled "Add CIFS Share" with the following configuration options:

- Name:** backups
- Comment:** (empty)
- Path:** /mnt/test1 (with a "Browse" button)
- Export Read Only:**
- Browsable to Network Clients:**
- Inherit Permissions:**
- Export Recycle Bin:**
- Show Hidden Files:**
- Guest Account:** www (with a dropdown arrow)

**5. Configure the CIFS service in Services -> CIFS as follows:**

- to ensure that the user is prompted to authenticate, select Local User as the Authentication Model
- change the Workgroup name to that being used on the Windows network; unless it has been changed by the administrator, the default workgroup name is WORKGROUP

**6. Start the CIFS service** in Services -> Control Services. Click the click the red OFF button next to CIFS. After a second or so, it will change to a blue ON , indicating that the service has been enabled.

**NOTE:** if you make changes in any of these steps after starting the CIFS service, you should restart the CIFS service to make sure that the changes are applied.

**7. Test the connection.** To test from a Windows system, open Explorer, and click on Network. For this configuration example, a system named *FREENAS* should appear with a share named *backups*. If you click on *backups*, a Windows Security pop-up screen will prompt for the user's username and password. Once authenticated the user can copy data to and from the CIFS share.

**NOTE:** since the share is group writable, any authenticated user can change the data in the share. If you wish to setup shares where a group of users have access to some folders but only individuals have access to other folders (where all these folders reside on the same volume), you will need to create these directories and set their permissions at the [console](#). Instructions for doing so can be found at the forum post [Set Permission to allow users to share a common folder & have private personal folder](#).

## 7.3 NFS Shares

FreeNAS™ supports the Network File System (NFS) for sharing volumes over a network. Once the NFS share is configured, clients use the **mount** command to mount the share. Once mounted, the share appears as just another directory on the client system. Some Linux distros require the installation of additional software in order to mount an NFS share. Windows systems may need to first enable Services for NFS.

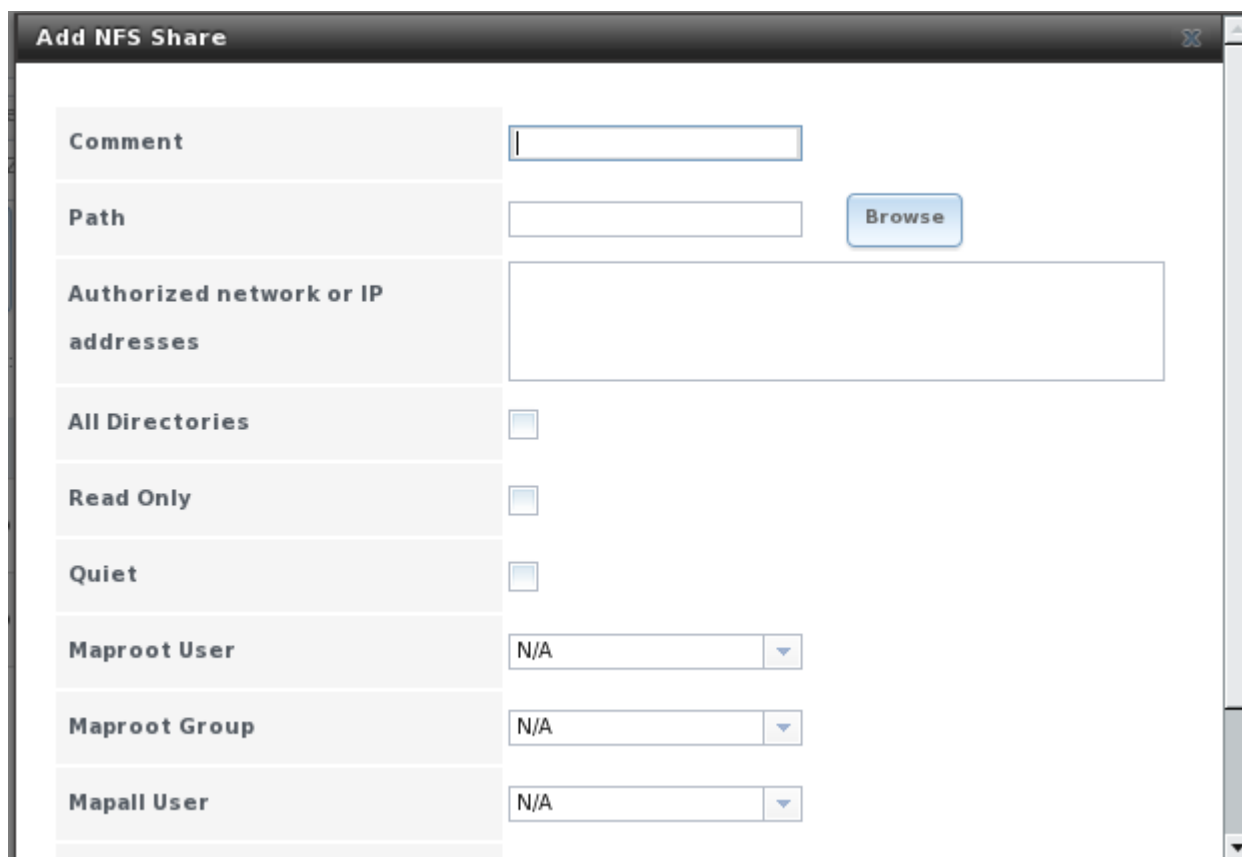
**NOTE:** Services for NFS is only available in the Ultimate or Enterprise editions of Windows.

Configuring NFS is a multi-step process that requires you to create NFS share(s), configure NFS in Services -> NFS, then start NFS in Services -> Control Panel. It does not require you to create users or groups as NFS uses IP addresses to determine which systems are allowed to access the NFS share.

### 7.3.1 Creating NFS Shares

If you click Sharing -> NFS Shares → Add NFS Share you'll see the screen shown in Figure 7.3a. Table 7.3a summarizes the options in this screen.

**Figure 7.3a: Creating an NFS Share**



The screenshot shows the 'Add NFS Share' configuration window. It features the following fields and options:

- Comment:** A text input field.
- Path:** A text input field with a 'Browse' button to its right.
- Authorized network or IP addresses:** A large text input field for specifying allowed IP addresses.
- All Directories:** A checkbox.
- Read Only:** A checkbox.
- Quiet:** A checkbox.
- Maproot User:** A dropdown menu currently set to 'N/A'.
- Maproot Group:** A dropdown menu currently set to 'N/A'.
- Mapall User:** A dropdown menu currently set to 'N/A'.

**Table 7.3a: NFS Share Options**

Setting	Value	Description
Comment	string	optional
Path	browse button	select volume/dataset to share
Authorized network	string	comma delimited list of allowed IP addresses and/or network addresses in the form 1.2.3.0/24 where the number after the slash is a CIDR mask; if you need to input network addresses with different CIDR masks, create multiple shares pointing to the same volume/dataset, one for each mask
All directories	checkbox	allows the client to mount at any point within the volume's file system
Read only	checkbox	prohibits writing to the volume
Quiet	checkbox	inhibits some syslog diagnostics which can be useful to avoid annoying error messages for known possible problems; see exports(5) for examples
Maproot User	drop-down menu	if left at N/A, the root user will not be able to modify files on the NFS share; if a user is selected, the root user is limited to that user's permissions
Maproot Group	drop-down menu	if specified, the root user will also be limited to that group's permissions (in addition to the maproot user)
Mapall User	drop-down menu	the specified user (and their permissions) is used by all clients
Mapall Group	drop-down menu	the specified group (and its permissions) is used by all clients

**NOTE:** the Maproot and Mapall options are exclusive, meaning you can only use one or the other--the GUI will not let you use both. If you only wish to restrict the root user's permissions, set the Maproot option. If you wish to restrict the permissions of all users, set the Mapall option.

### 7.3.2 Sample NFS Share Configuration

By default the Mapall options shown in Figure 7.3a show as N/A. This means that when a user connects to the NFS share, they connect with the permissions associated with their user account. This is a security risk if a user is able to connect as root as they will have root access to the share.

A better scenario is to do the following:

1. Create a user account that is specifically used for NFS access in Account -> Users -> Add User. Alternately, use the built-in *nobody* account.
2. In the volume that is being shared, change the owner and group to the NFS user account and set the permissions according to your specifications.
3. Select the NFS user and its associated group in the Mapall User and Mapall Group drop-down menus for the share in Sharing -> NFS Shares.

With this configuration, it does not matter what user account is used to connect to the NFS share, as it will be mapped to your NFS user account and will only have the permissions associated with that



account. For example, even if the root user is able to connect, it will not have root access to the share.

### 7.3.3 Connecting to the NFS Share

In the following examples, the NFS share has been configured as follows:

1. A ZFS volume named `/mnt/data` has its permissions set to the `nobody` user account and the `nobody` group.
2. A NFS share has been created with a Path of `/mnt/data`, an Authorized Network of `192.168.2.0/24`, and the MapAll User and MapAll Group of `nobody`. The All Directories checkbox has been checked and the IP address of the FreeNAS™ system is `192.168.2.2`.

#### 7.3.3.1 From BSD or Linux Clients

To make this share accessible on a BSD or a Linux system, run the following command as the superuser (or with `sudo`) from the client system (repeat for each client that needs access to the NFS share):

```
mount 192.168.2.2:/mnt/data /mnt
```

This command should return the superuser to the command prompt without any error messages, indicating that the share was successfully mounted. Users on the client system can now copy files to and from `/mnt` and all files will be owned by `nobody:nobody`. Any changes to `/mnt` will be saved to the FreeNAS™ system's `/mnt/data` ZFS volume. Should you wish to make any changes to the NFS share's settings or wish to make the share inaccessible, unmount the share first as the superuser:

```
umount /mnt
```

#### 7.3.3.2 From Microsoft Clients

Enterprise versions of Windows systems can connect to NFS shares using Services for NFS. Connecting to NFS shares is often faster than connecting to CIFS shares due to the [single-threaded limitation](#) of Samba. Instructions for connecting from an Enterprise version of Windows 7 can be found at [Mount Linux NFS Share on Windows 7](#).

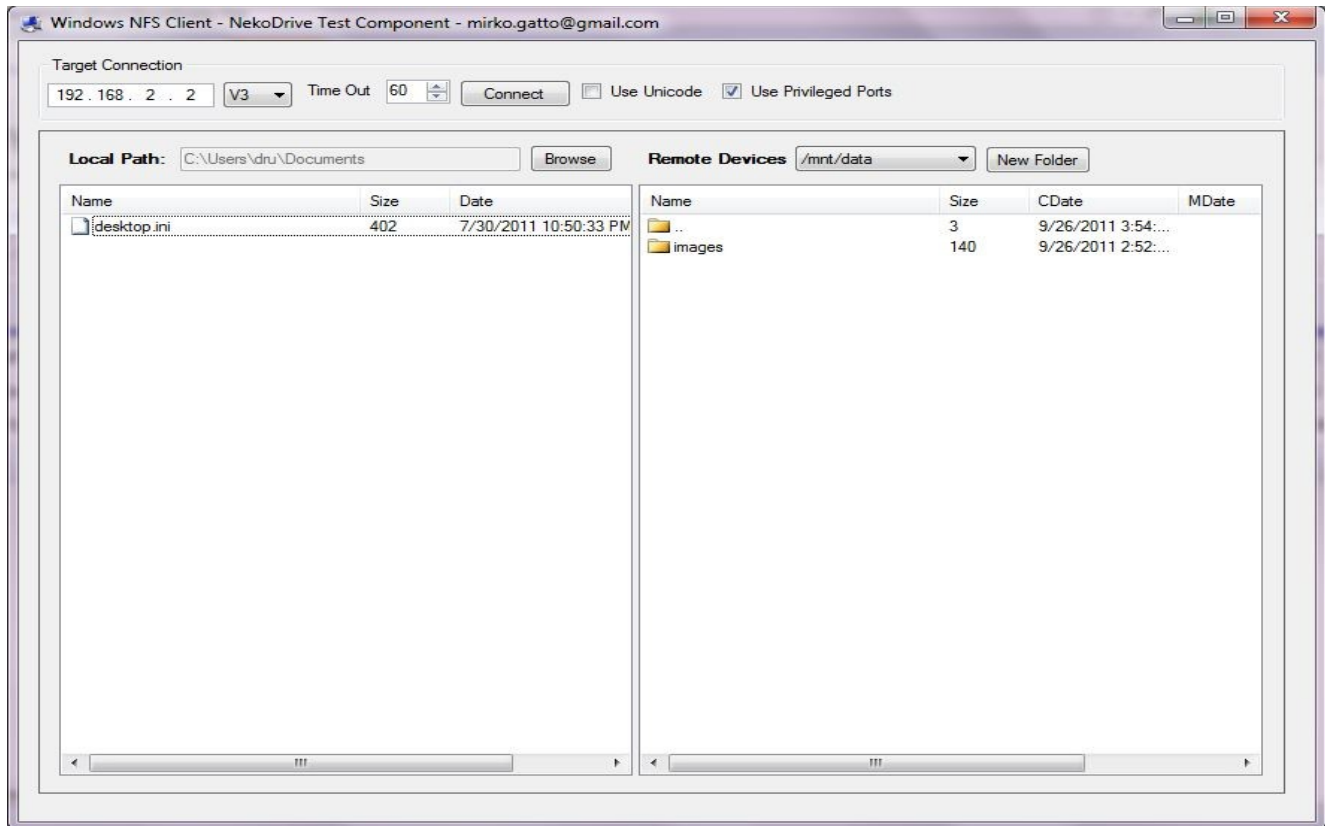
If your Windows client is running a Home Edition of Windows 7, [Nekodrive](#) provides an open source graphical NFS client. To use this client, you will need to install:

- [7zip](#) to extract the `.z` files
- NFSClient and NFSLibrary from the Nekodrive download page; once downloaded, extract these files using 7zip
- [.NET Framework 4.0](#)

Run the NFSClient executable to start the GUI client. In the example shown in Figure 7.3b, the user has connected to the example `/mnt/data` share of the FreeNAS™ system at `192.168.2.2`.



**Figure 7.3b: Using the Nekodrive NFSClient from Windows 7 Home Edition**



### 7.3.3.3 From Mac OS X Clients

To mount the NFS volume from a Mac OS X client, click on Go -> Connect to Server. In the Server Address field, input *nfs://* followed by the IP address of the FreeNAS™ system and the name of the volume/dataset being shared by NFS. The example shown in Figure 7.3c continues with our example of *192.168.2.2:/mnt/data*. Once connected, Finder will automatically open. The IP address of the FreeNAS™ system will be displayed in the SHARED section in the left frame and the contents of the share will be displayed in the right frame. In the example shown in Figure 7.3d, /mnt/data has one folder named images. The user can now copy files to and from the share.

Figure 7.3c: Mounting the NFS Share from Mac OS X

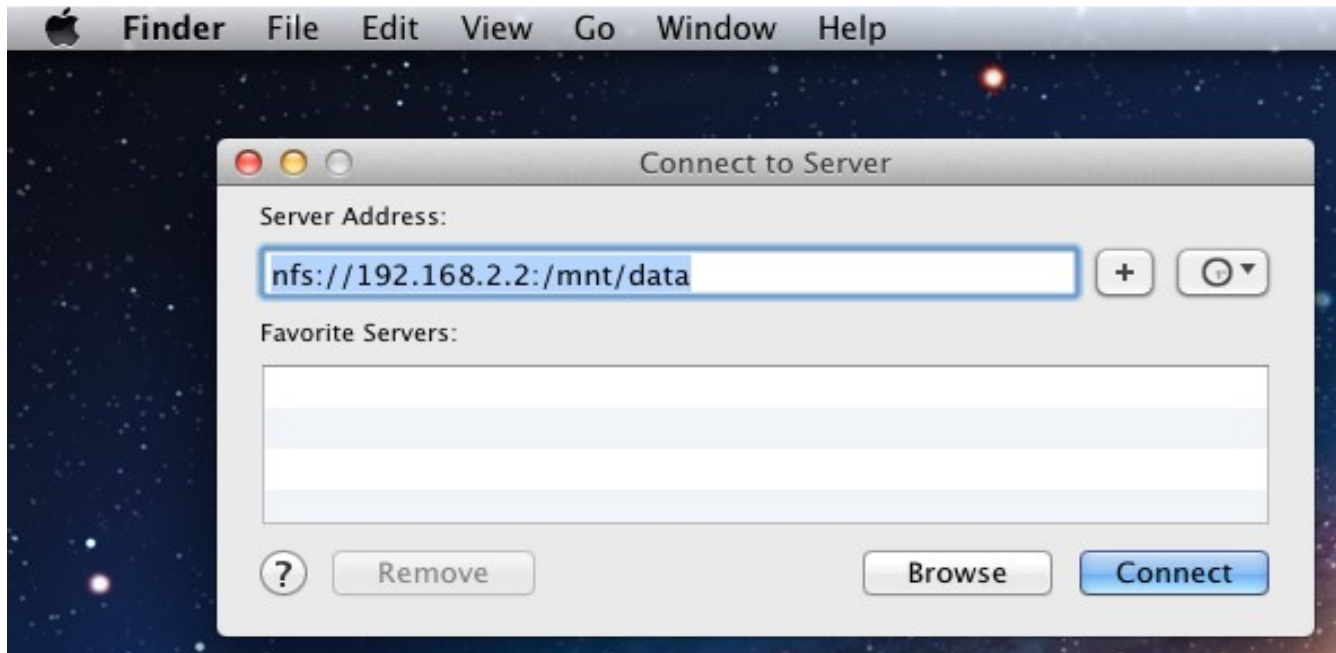
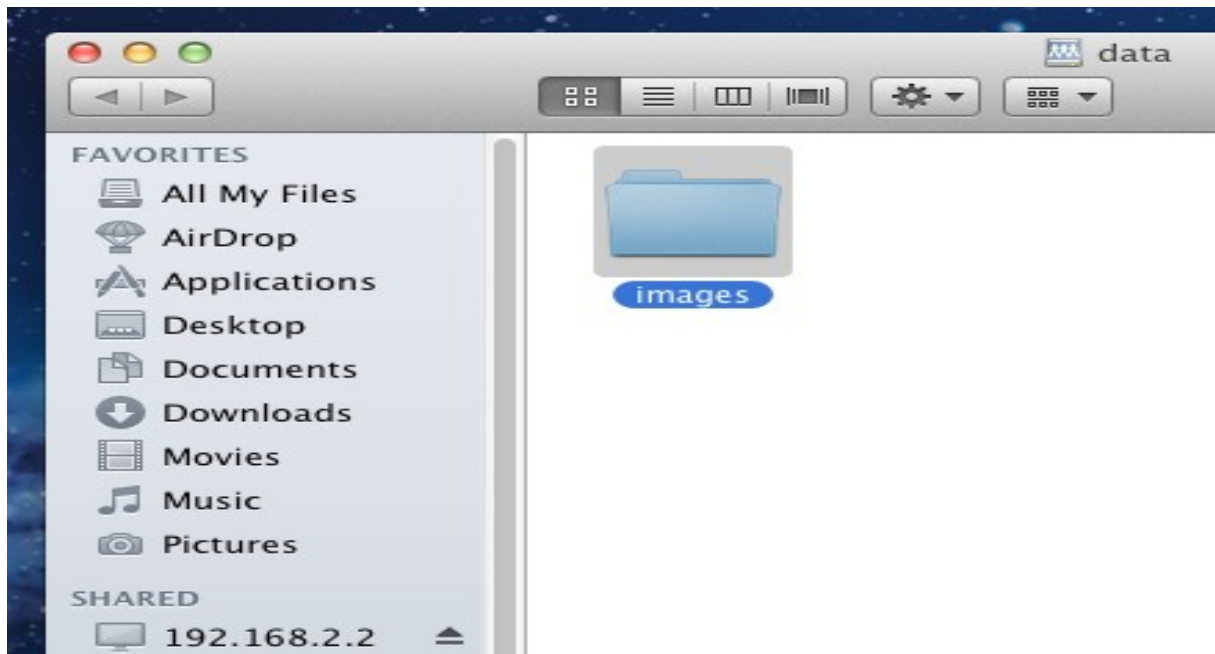


Figure 7.3d: Viewing the NFS Share in Finder



### 7.3.4 Troubleshooting

Some NFS clients do not support the NLM (Network Lock Manager) protocol used by NFS. You will know that this is the case if the client receives an error that all or part of the file may be locked when a file transfer is attempted. To resolve this error, use the option **-o nolock** when running the **mount**

command on the client in order to allow write access to the NFS share.

If you receive an error about a "time out giving up" when trying to mount the share from a Linux system, make sure that the portmapper service is running on the Linux client and start it if it is not. If portmapper is running and you still receive timeouts, force it to use TCP by including **-o tcp** in your **mount** command.

If you receive an error "RPC: Program not registered", upgrade to the latest version of FreeNAS™ and restart the NFS service after the upgrade in order to clear the NFS cache.

## 8 Services Configuration

The Services section of the GUI allows you to configure, start, and stop the various services that ship with the FreeNAS™ system. FreeNAS™ supports the following services:

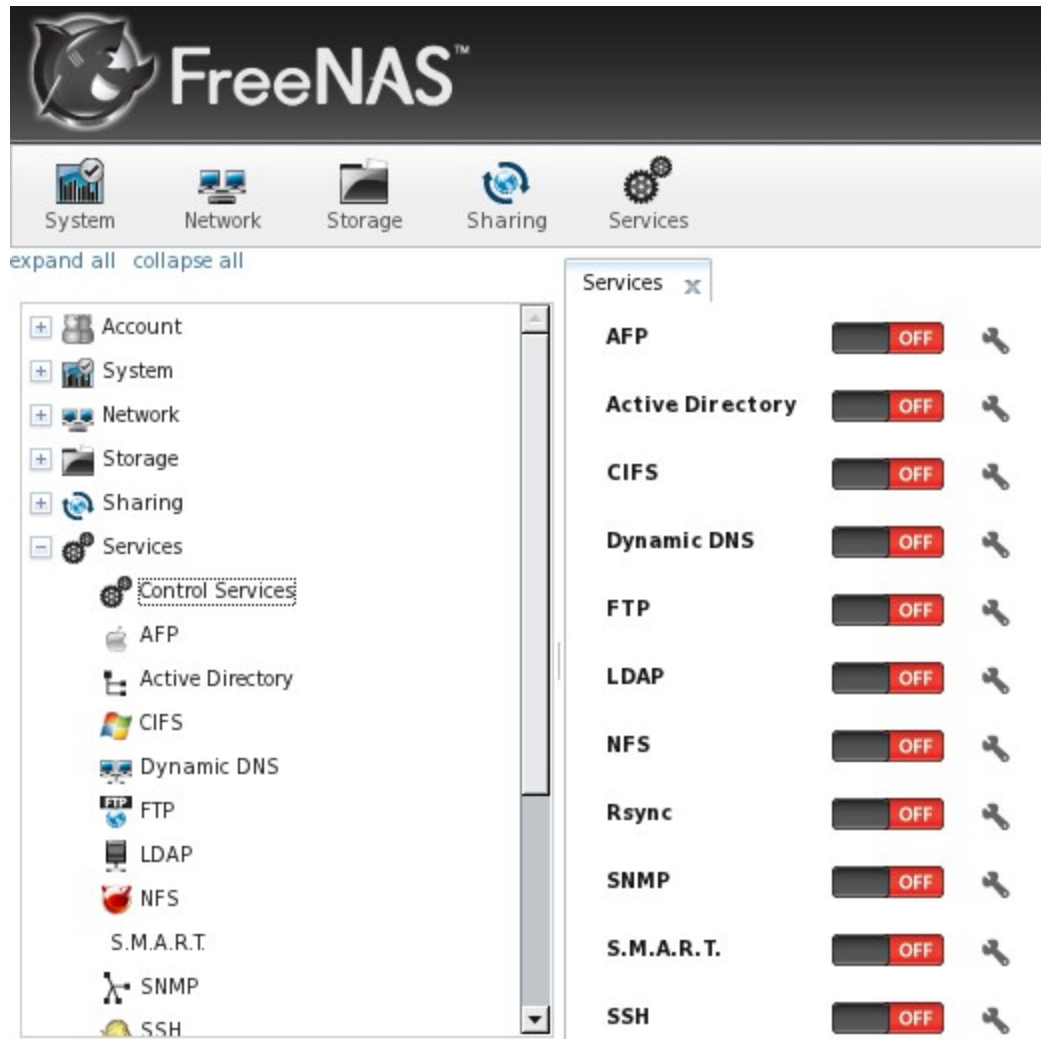
- [AFP](#)
- [Active Directory](#)
- [CIFS](#)
- [Dynamic DNS](#)
- [FTP](#)
- [LDAP](#)
- [NFS](#)
- [S.M.A.R.T.](#)
- [SNMP](#)
- [SSH](#)
- [TFTP](#)
- [UPS](#)
- [iSCSI](#)
- [Rsync](#)

This section describes the configuration options for each of these services, as well as how to start a FreeNAS™ service.

### 8.1 Control Services

The Control Services screen, shown in Figure 8.1a, allows you to quickly determine which services are currently running, enable/disable services, and configure services.

Figure 8.1a: Control Services



To enable/disable a service, click its on/off icon.

To configure a service, click the wrench icon associated with the service. The configuration options for each service are described in the rest of this section.

**NOTE:** if you are troubleshooting a service, go to System -> Settings -> Advanced and check the box “Show console messages in the footer (Requires UI reload)”. Once you refresh your browser, the console messages will show at the bottom of the screen. If you click on the console, it will pop-up as a scrolled window, allowing you to scroll through the output and to copy/paste messages. Watch these messages for errors when you stop and start the problematic service.

## 8.2 AFP

The Apple Filing Protocol (AFP) is a network protocol that offers file services for Mac computers. Before configuring this service, you should first create your AFP Shares in Sharing -> AFP Shares -> Add AFP Share. After configuring this service, go to Services -> Control Panel to start the service.

Enabling this service will open the following ports on the FreeNAS™ system:

- \* TCP 548 (afpd)
- \* TCP 4799 (cnid\_metadata)
- \* UDP 5353 and a random UDP port (avahi)

Figure 8.2a shows the configuration options which are described in Table 8.2a:

**Figure 8.2a: AFP Configuration**



**Table 8.2a: AFP Configuration Options**

Setting	Value	Description
Server Name	string	server name that will appear to Mac clients; by default it is <i>freenas</i>
Guest Access	checkbox	if checked, clients will not be prompted to authenticate before accessing the AFP share
Guest Account	drop-down menu	select account to use for guest access
Local Access	checkbox	restricts access to local network only
Max Connections	integer	maximum number of simultaneous connections

### 8.3 Active Directory

Active Directory (AD) is a service for sharing resources in a Windows network. It requires a configured system that is running at least Windows Server 2000. If you wish to share your FreeNAS™ CIFS shares with Windows systems in a network that does not have a Windows server running AD, enable and configure CIFS instead. If your network does have a Windows server running AD, configure both the Active Directory service and the CIFS service on the FreeNAS™ system so that

users can authenticate to the Windows server and be authorized to access the CIFS shares on the FreeNAS™ system.

**NOTE:** many changes and improvements have been made to Active Directory support since the release of FreeNAS™ 8.0.1. If you are not running FreeNAS™ 8.0.3-RELEASE, you should upgrade before attempting Active Directory integration.

Before configuring AD, make sure that you can resolve the Active Directory domain controller from the FreeNAS™ system by **pinging** its domain name. In order to do so, you may have to first set the network's DNS servers and default gateway from Network -> Global Configuration on the FreeNAS™ system.

Active Directory relies on Kerberos, which is a very time sensitive protocol. This means that the time on both the FreeNAS™ system and the Active Directory Domain Controller can not be out of sync by more than a few minutes. The best way to ensure that the same time is running on both systems is to configure both systems to:

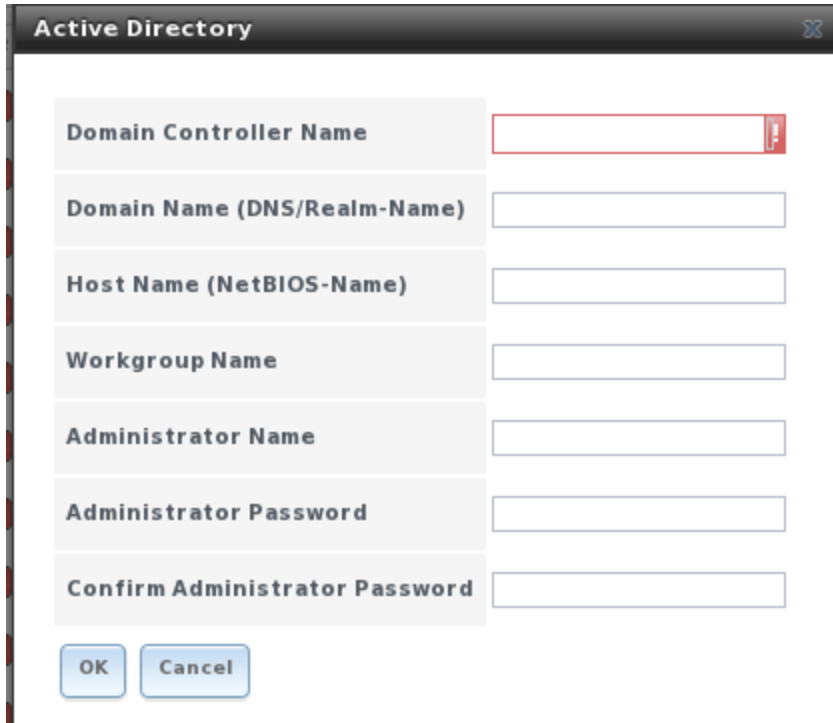
- use the same NTP server (set in System -> Settings -> General on the FreeNAS™ system)
- have the same timezone
- be set to either localtime or universal time at the BIOS level

Once you have configured the CIFS and Active Directory services, remember to start them in Services -> Control Services. It may take a few minutes for the Active Directory information to be populated to the FreeNAS™ system. Once populated, the AD users and groups will be available in the drop-down menus of the permissions screen of a volume/dataset.

**NOTE:** your FreeNAS™ system may not show up in Active Directory until you add a DNS record for the FreeNAS™ system on the Windows server.

Figure 8.3a shows the Active Directory Configuration screen and Table 8.3a describes the configurable options.

**Figure 8.3a: Configuring Active Directory**



**Table 8.3a: Active Directory Configuration Options**

Setting	Value	Description
Domain Controller Name	string	IP address or hostname of Windows PDC
Domain Name	string	name of Windows server's DNS realm
Host Name	string	hostname of FreeNAS™ system
Workgroup Name	string	name of Windows server's workgroup (for older Microsoft clients)
Administrator Name	string	name of the Active Directory Administrator account
Administrator Password	string	password for the Active Directory Administrator account

You can verify which Active Directory users and groups have been imported to the FreeNAS™ system at the FreeNAS™ command line:

```
wbinfo -u (to view users)
```

```
wbinfo -g (to view groups)
```

If no users or groups are listed in the output of those commands, these commands will provide more troubleshooting information:

```
getent passwd
```

getent group

### 8.3.1 Troubleshooting Tips

If you are running AD in a 2003/2008 mixed domain, see this [forum post](#) for instructions on how to prevent the secure channel key from becoming corrupted.

In some large domains, caching user data appears to stall the FreeNAS™ GUI or fails to populate the user cache on the PDC. If this occurs in a multi-tiered forest, specify *allow trusted domains = no* in the auxiliary parameters field of Sharing -> CIFS Shares.

The LDAP code uses DNS to determine the location of the domain controllers and global catalog servers in the network. Use the **host -t srv \_ldap.\_tcp.domainname.com** command to determine the network's SRV records and, if necessary, change the weight and/or priority of the SRV record to reflect the fastest server. More information about SRV records can be found in the Technet article [How DNS Support for Active Directory Works](#).

If the cache becomes out of sync due to an AD server being taken off and back online, resync the cache using System -> Settings -> Advanced -> Rebuild LDAP/AD Cache.

## 8.4 CIFS

The Common Internet File System (CIFS) is a network protocol that offers file services for (typically) Windows computers. FreeNAS™ uses [Samba](#) to provide CIFS capability without the need for a Windows server in the network. UNIX-like systems that provide a [CIFS client](#) can also connect to CIFS shares. Before configuring this service, you should first create your CIFS Shares in Sharing -> CIFS Shares -> Add CIFS Share. After configuring this service, go to Services -> Control Panel to start the service.

**NOTE:** after starting the CIFS service, it may take several minutes for the [master browser election](#) to occur and for the FreeNAS™ system to become available in Windows Explorer.

Starting this service will open the following ports on the FreeNAS™ system:

- TCP 139 (smbd)
- TCP 445 (smbd)
- UDP 137 (nmbd)
- UDP 138 (nmbd)

Figure 8.4a shows the configuration options which are described in Table 8.4a. This configuration screen is really a front-end to [smb.conf](#).



**Figure 8.4a: Configuring CIFS**

**Table 8.4a: CIFS Configuration Options**

Setting	Value	Description
Authentication Model	drop-down menu	anonymous or local user; if select local user, user accounts must exist on FreeNAS™ system and should match the username/password of Windows accounts needing access to the share as the user will be required to authenticate before accessing the share
NetBIOS Name	string	must be lowercase and should be same as hostname
Workgroup	string	must match Windows workgroup name; default is WORKGROUP
Description	string	optional
DOS Charset	drop-down menu	the character set Samba uses when communicating with DOS and Windows 9x/Me clients; default is CP437
UNIX Charset	drop-down menu	default is UTF-8, which is fine for most systems and covers all characters in all languages
Log Level	drop-down menu	choices are minimum, normal, full, or debug

Setting	Value	Description
Local Master	checkbox	determines whether or not the FreeNAS™ system participates in a browser election; should be disabled when network contains an AD or LDAP server and is not necessary if Windows Vista/7 machines are present
Time Server	checkbox	determines whether or not the FreeNAS™ system advertises itself as a time server to Windows clients
Guest Account	drop-down menu	account to be used for guest access
Allow guest access	checkbox	if checked, the guest account is not prompted to authenticate in order to access the CIFS share
Only allow guest access	checkbox	if checked, all access is through the guest account and subject to its permissions
File mask	integer	overrides default file creation mask of 0666 which creates files with read and write access for everybody
Directory mask	integer	overrides default directory creation mask of 0777 which grants directory read, write and execute access for everybody
Large RW support	checkbox	determines whether or not the FreeNAS™ system supports 64k streaming read/write requests introduced with Windows 2000 and which can improve performance by 10% with Windows 2000 clients
Send files with sendfile(2)	checkbox	newer Windows versions support the more efficient sendfile system call which makes Samba faster
EA Support	checkbox	enables extended attributes
Support DOS File Attributes	checkbox	allows a user who has write access to a file to modify the permissions, even if not the owner of the file
Allow Empty Password	checkbox	if checked, users can just press enter when prompted for a password; requires that the username/password be the same for the FreeNAS™ user account and the Windows user account
Auxiliary parameters	string	smb.conf options not covered elsewhere in this screen; see <a href="#">the Samba Guide</a> for additional settings
Enable home directories	checkbox	if checked, a folder with the same name as the user account will be created for each user
Enable home directories browsing	checkbox	users can browse (but not write to) other users' home directories
Home directories	browse button	select volume/dataset where the home directories will be created
Enable AIO	checkbox	enables asynchronous I/O in FreeNAS™ versions 8.0.3-RELEASE and higher; if CIFS seems slow, try disabling this setting and/or tweaking the minimum AIO read and write sizes
Minimum AIO read	integer	if set to non-zero value, Samba will read from file asynchronously

Setting	Value	Description
size		when size of request is bigger than this value in bytes
Minimum AIO write size	integer	if set to non-zero value, Samba will write from file asynchronously when size of request is bigger than this value in bytes
Zeroconf share discovery	checkbox	enable if Mac clients will be connecting to the CIFS share

**NOTE:** beginning with FreeNAS™ versions 8.0.3-RELEASE, changes to CIFS settings and CIFS shares take effect immediately. For previous versions, changes will not take effect until you manually stop and start the CIFS service.

### 8.4.1 Troubleshooting Tips

Compared to other networking protocols, CIFS is not fast. Enabling the following checkboxes may help to increase network throughput: "Large RW support", "Send files with sendfile(2)", and "Enable AIO". Adjusting the AIO minimum and maximum size settings to better fit your networking infrastructure may improve or degrade performance.

Samba's "write cache" parameter has been reported to improve write performance in some configurations and can be added to the Auxiliary Parameters field. Use an integer value which is a multiple of `_SC_PAGESIZE` (typically 4096) to avoid memory fragmentation. This will increase Samba's memory requirements and should not be used on systems with limited RAM.

If you wish to increase network performance, read the Samba section on [socket options](#). It indicates which options are available and recommends that you experiment to see which are supported by your clients and improve your network's performance.

Windows automatically caches file sharing information. If you make changes to a CIFS share or to the permissions of a volume/dataset being shared by CIFS and are no longer able to access the share, try logging out and back into the Windows system.

Where possible, avoid using a mix of case in filenames as this may cause confusion for Windows users. [Representing and resolving filenames with Samba](#) explains this in more detail.

## 8.5 Dynamic DNS

Dynamic DNS (DDNS) is useful if your FreeNAS™ system 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, allowing you to access the FreeNAS™ system even if the IP address changes. DDNS requires you to register with a DDNS service such as [DynDNS](#).

Figure 8.5a shows the DDNS configuration screen and Table 8.5a summarizes the configuration options. The values you need to input will be given to you by the DDNS provider. After configuring DDNS, don't forget to start the DDNS service in Services -> Control Services.

**Figure 8.5a: Configuring DDNS**

**Table 8.5a: DDNS Configuration Options**

Setting	Value	Description
Provider	drop-down menu	several providers are supported
Domain name	string	fully qualified domain name (e.g. yourname.dyndns.org)
Username	string	username to logon to the provider and update the record
Password	string	password used to logon to the provider and update the record
Update period	integer	in milliseconds; be careful with this setting as the provider may block you for abuse if this setting occurs more often than the IP changes
Forced update period	integer	in seconds so be careful with this setting as the provider may block you for abuse; issues a DDNS update request even when the address has not changed, so that the service provider knows that the account is still active
Auxiliary parameters	string	additional parameters passed to the provider during record update

## 8.6 FTP

FreeNAS™ allows you to configure the [proftpd](#) FTP server so that users can browse and download data using their web browser or FTP client software. The advantage of FTP is that easy-to-use cross-platform utilities are available to manage uploads to and downloads from the FreeNAS™ system. The disadvantage of FTP is that it is considered to be an insecure protocol, meaning that it should not be used to transfer sensitive files. If you are concerned about sensitive data, see [section 8.6.4 Encrypting FTP](#).

In order for FTP to work, you will need to set appropriate permissions on the storage volume, and depending upon your configuration needs, you may also need to create users and groups. This section includes configuration examples demonstrating some common scenarios.

Figure 8.6a shows the configuration screen for the FTP service:

**Figure 8.6a: Configuring FTP**

The screenshot shows the FTP configuration window with the following settings:

Setting	Value
Port	21
Clients	5
Connections	2
Login Attempts	1
Timeout	600
Allow Root Login	<input type="checkbox"/>
Allow Anonymous Login	<input type="checkbox"/>
Path	<input type="text"/> <input type="button" value="Browse"/>
Allow Local User Login	<input type="checkbox"/>
Banner	<input type="text"/>

Table 8.6a summarizes the available options when configuring the FTP server:

**Table 8.6a: FTP Configuration Options**

Setting	Value	Description
Port	integer	port to use for connection requests
Clients	integer	maximum number of simultaneous clients

Setting	Value	Description
Connections	integer	maximum number of connections per IP address where 0 means unlimited
Login Attempts	integer	maximum number of attempts before client is disconnected; ; increase this if users are prone to typos
Timeout	integer	maximum client idle time in seconds before client is disconnected
Allow Root Login	checkbox	discouraged as increases security risk
Allow Anonymous Login	checkbox	allows anyone to browse the data
Path	browse button	root directory of FTP server; must point to the volume/dataset or connections will fail
Allow Local User Login	checkbox	required if anonymous is disabled
Banner	string	message users see when access FTP server, if left empty it will show the version of FTP
File Permission	checkboxes	sets umask for newly created files
Directory Permission	checkboxes	sets umask for newly created directories
Enable <a href="#">FXP</a>	checkbox	discouraged as vulnerable to FTP bounce attacks
Allow Transfer Resumption	checkbox	if transfer is interrupted, server will resume transfer at last known point
Always Chroot	checkbox	forces users to stay in their home directory (always true for anonymous)
Require IDENT Authentication	checkbox	will result in timeouts if identd is not running on the client
Require Reverse DNS for IP	checkbox	will result in timeouts if there isn't a DNS record for the client's hostname
Masquerade address	string	IP address or hostname; use if FTP clients can not connect through a NAT device
Minimum passive port	integer	to be used by clients in PASV mode, default of 0 means any port above 1023
Maximum passive port	integer	to be used by clients in PASV mode, default of 0 means any port above 1023
Local user upload bandwidth	integer	in KB/s, default of 0 means unlimited
Local user download bandwidth	integer	in KB/s, default of 0 means unlimited
Anonymous user upload bandwidth	integer	in KB/s, default of 0 means unlimited
Anonymous user download bandwidth	integer	in KB/s, default of 0 means unlimited
Enable SSL/TLS	checkbox	enables encrypted connections; you will need to

Setting	Value	Description
		configure the certificate in System -> Settings → SSL
Auxiliary parameters	string	include proftpd(8) parameters not covered elsewhere in this screen

The following example demonstrates the auxiliary parameters that will prevent all users from performing the FTP DELETE command:

```
<Limit DELE>
  DenyAll
</Limit>
```

### 8.6.1 Anonymous FTP

Anonymous FTP may be appropriate for a small network where the FreeNAS™ system is not accessible from the Internet and everyone in your internal network needs easy access to the stored data. Anonymous FTP does not require you to create a user account for every user. In addition, passwords are not required so you don't have to manage changed passwords on the FreeNAS™ system.

To configure anonymous FTP:

- 1. Give the built-in ftp user account permissions** to the volume/dataset in Storage -> Volume -> View All Volumes. Click the Change Permissions button for the volume/dataset that you wish to share using FTP. In the screen shown in Figure 8.6b, select the *ftp* user in the drop-down menu for Owner(user), select the *ftp* group for Owner(group), review that the permissions are appropriate for your network, keep the type of ACL as Unix, check the box Set permission recursively, and click the Change button.

**NOTE:** for FTP, the type of client does not matter when it comes to the type of ACL. This means that you always use Unix ACLs, even if Windows clients will be accessing FreeNAS™ via FTP.

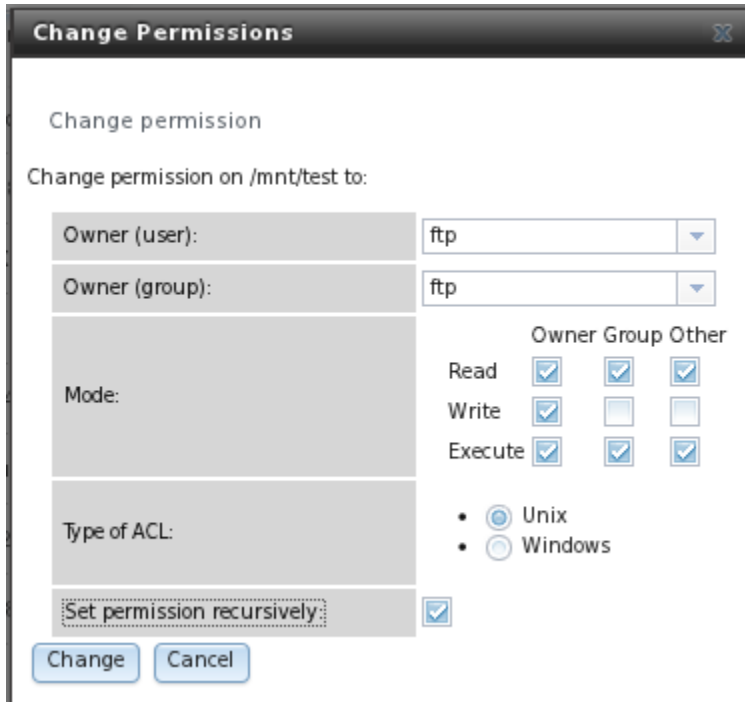
- 2. Configure anonymous FTP** in Services -> FTP. In the screen shown in Figure 8.6a:

- check the box Allow Anonymous Login
- change the path to the name of the volume/dataset

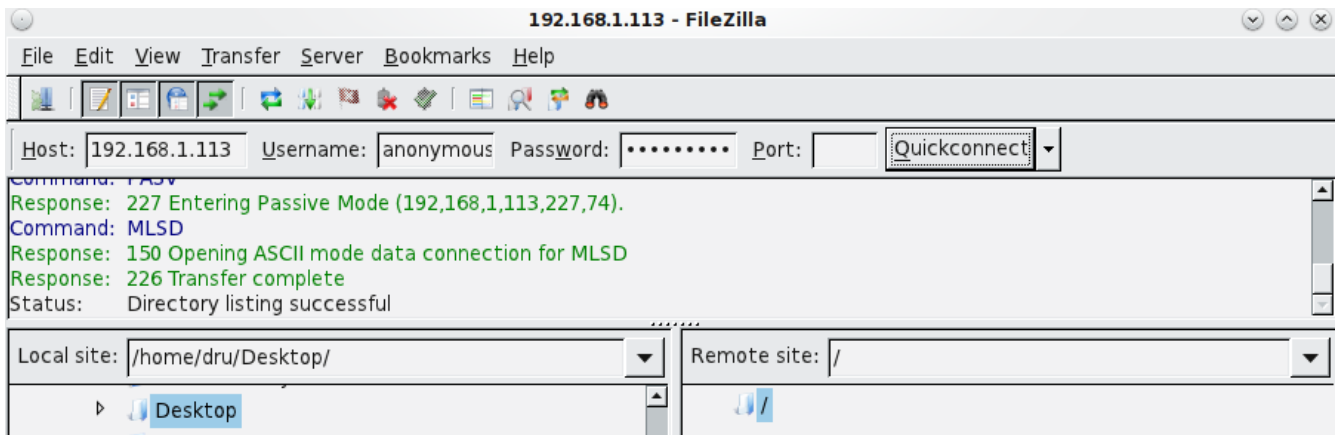
- 3. Start the FTP service** in Control Services. Click the red OFF button next to FTP. After a second or so, it will change to a blue ON , indicating that the service has been enabled.

- 4. Test the connection** from a client using a utility such as [Filezilla](#). In the example shown in Figure 8.6c, the IP address of the FreeNAS™ server is *192.168.1.113*, the Username is *anonymous*, and the Password is the email address of the user.

**Figure 8.6b: Assign ftp User Account Permissions to the Volume**



**Figure 8.6c: Connecting Using Filezilla**



### 8.6.2 Specified User Access in chroot

If you require your users to authenticate before accessing the data on the FreeNAS™ system, you will need to create a user account for each user. If you create a ZFS dataset for each user, you can chroot each user so that they are limited to the contents of their own home directory and you can also restrict the size of that home directory using a ZFS quota. To configure this scenario:

**1. Create a ZFS dataset for each user** in Storage -> Create ZFS Dataset. In the example shown in Figure 8.6d, a ZFS dataset named *user1* has been created with a ZFS quota of 20GB. In later steps, we will create a user named user1 to associate with the dataset. Repeat this process to create a dataset for



every user that will need access to the FTP service.

**Figure 8.6d: Create a ZFS Dataset with a Quota**

**Create ZFS Dataset**

Volume from which this dataset will be created on: test1

Dataset Name: user1

Compression level: Inherit

Enable atime:

- Inherit
- On
- Off

Quota for this dataset: 20G

Quota for this dataset and all children: 0

Reserved space for this dataset: 0

Reserved space for this dataset and all children: 0

Add Dataset Cancel

**2. Create a user account for each user** in Account -> Users -> Add User. In the screen shown in Figure 8.6e, input a Username for the user (in this example, *user1*), change the Home Directory to the name of an existing dataset (in our example, the dataset named */mnt/test1/user1*), input a description under Full Name, input the user's email address, input and confirm the user's password, and click the OK button. Repeat this process to create a user account for every user that will need access to the FTP service, making sure to assign each user their own dataset.

**3. Set the permissions for each dataset** in Storage -> Volume -> View All Volumes. This is how you associate a user account with a dataset and set the desired permissions for that user. Click the Change Permissions button for a dataset that you specified as the Home Directory when you created a user account. In the screen shown in Figure 8.6f, select the user in the drop-down menu for Owner(user) and Owner(group) (in this example, *user1*), keep the type of ACL as Unix, review the read and write permissions to see if they are appropriate to that user, check the box Set permission recursively, and click the Change button.

**NOTE:** for FTP, the type of client does not matter when it comes to the type of ACL. This means that you always use Unix ACLs, even if Windows clients will be accessing FreeNAS™ via FTP.

**Figure 8.6e: Creating a User Account**

User ID: 1001

Username: user1

Primary Group: [dropdown]

Home Directory: /mnt/test1/user1

Shell: csh [dropdown]

Full Name: ftp user

E-mail: user1@somedomain.com

Password: [masked]

Password confirmation: [masked]

Disable logins:

OK Cancel

**Figure 8.6f: Setting the Dataset's Permissions**

Change Permissions

Change permission

Change permission on /mnt/test1/user1 to:

Owner (user): user1 [dropdown]

Owner (group): user1 [dropdown]

	Owner	Group	Other
Read	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Execute	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Type of ACL:

- Unix
- Windows

Set permission recursively:

Change Cancel

**4. Configure FTP** in Services -> FTP. In the screen shown in Figure 8.6a:

- make sure the boxes for Allow Anonymous Login and Allow Root Login are unchecked
- check the box Allow Local User Login
- check the box Always Chroot

**5. Start the FTP service** in Control Services. Click the red OFF button next to FTP. After a second or so, it will change to a blue ON , indicating that the service has been enabled.

**6. Test the connection from a client** using a utility such as Filezilla. This time in the example shown in Figure 8.6d, use the IP address of the FreeNAS™ system, the Username of a user that has been associated with a dataset, and the Password for that user.

### 8.6.3 Encrypting FTP

During installation, an RSA certificate and key are auto-generated for you. You can view these or cut/paste your own signed certificate and key in System -> Settings -> SSL. To configure any FTP scenario to use encrypted connections:

**1. Enable SSL/TLS** in Services -> FTP. Check the box Enable SSL/TLS. Once you press OK, proftpd will automatically restart and be configured to use the certificate stored in the SSL tab.

**2. Specify secure FTP when accessing the FreeNAS™ system.** For example, in Filezilla input *ftps://IP\_address* (for an implicit connection) or *ftpes://IP\_address* (for an explicit connection) as the Host when connecting. The first time you connect, you should be presented with the certificate of the FreeNAS™ system. Click OK to accept the certificate and negotiate an encrypted connection.

### 8.6.4 Troubleshooting

A very common issue is that proftpd won't start if it can't resolve the system's hostname to an IP via DNS. To see if the FTP service is running, go to the console shell (or a command prompt in an SSH session) and issue the command:

```
sockstat -4p 21
```

If there is nothing listening on port 21, proftpd isn't running. To see the error message that occurs when FreeNAS™ tries to start the FTP service, go to System -> Settings -> Advanced and check the box "Show console messages in the footer (Requires UI reload)". Refresh your browser and the console messages should display at the bottom of your screen.

Next, go to Services -> Control Services and switch the FTP service off then back on in the GUI. Watch the console messages for errors.

If the error refers to DNS, either create an entry in your local DNS server with the FreeNAS™ system's hostname and IP address, or make an entry containing that information in */etc/hosts* on the FreeNAS™ server.

## 8.7 LDAP

FreeNAS™ includes an [OpenLDAP](#) 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. Examples of LDAP servers include Microsoft Server (2000 and newer), Mac OS X Server, Novell eDirectory, and OpenLDAP running on a BSD or Linux system. If an LDAP server is running on your network, you should configure the FreeNAS™ LDAP service so that the network's users can authenticate to the LDAP server and thus be provided authorized access to the data stored on the FreeNAS™ system.

Figure 8.7a shows the LDAP Configuration screen that is seen when you click Services -> LDAP.

**Figure 8.7a: Configuring LDAP**

The screenshot shows a web-based configuration interface for LDAP. The window has a title bar that says "LDAP". Below the title bar, there are several rows of configuration options, each with a label on the left and a corresponding input field on the right. The options are: "Hostname" with a text input field; "Base DN" with a text input field; "Allow Anonymous Binding" with a checkbox; "Root bind DN" with a text input field; "Root bind password" with a text input field; "Password Encryption" with a dropdown menu showing "clear"; "User Suffix" with a text input field; "Group Suffix" with a text input field; and "Password Suffix" with a text input field. There is a vertical scrollbar on the right side of the form area.

Table 8.7a summarizes the available configuration options:

**Table 8.7a: LDAP Configuration Options**

Setting	Value	Description
Hostname	hostname or IP address	of LDAP server
Base DN	integer	top level of the LDAP directory tree to be used when searching for resources

Setting	Value	Description
Allow Anonymous Binding	checkbox	instructs LDAP server to not provide authentication and to allow read/write access to any client
Root bind DN	string	used to bind with the LDAP server for administrative write access to the LDAP directory to change some attributes of an LDAP entry, such as a user's password
Root bind password	string	used for administrative write access on the LDAP server
Password Encryption	drop-down menu	select a type supported by the LDAP server, choices are: clear (unencrypted), crypt, md5, nds, racf, ad, exop
User Suffix	string	optional, can be added to name when user account added to LDAP directory (e.g. dept. or company name)
Group Suffix	string	optional, can be added to name when group added to LDAP directory (e.g. dept. or company name)
Password Suffix	string	optional, can be added to password when password added to LDAP directory
Machine Suffix	optional	can be added to name when system added to LDAP directory (e.g. server, accounting)
Encryption Mode	drop-down menu	choices are Off, SSL, or TLS
Self signed certificate	string	used to verify the certificate of the LDAP server if SSL connections are used; paste the output of the command <b>openssl s_client -connect server:port -showcerts</b>
Auxiliary Parameters	string	Ldap.conf(5) options, one per line, not covered by other options in this screen

**NOTE:** FreeNAS™ automatically appends the root DN. This means that you should not include the scope and root DN when inputting the user, group, password, and machine suffixes.

## 8.8 NFS

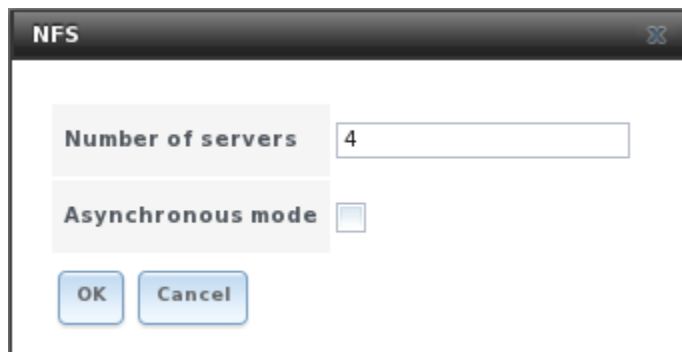
Network File System (NFS) is a protocol for sharing files on a network. Before configuring this service, you should first create your NFS Shares in Sharing -> NFS Shares -> Add NFS Share. After configuring this service, go to Services -> Control Panel to start the service.

Starting this service will open the following ports on the FreeNAS™ system:

- TCP and UDP 111 (rpcbind)
- TCP 2049 (nfsd)

Additionally, mountd and rpcbind will each bind to a randomly available UDP port. Figure 8.8a shows the configuration screen and Table 8.8a summarizes the configuration options for the NFS service.

**Figure 8.8a: Configuring NFS**



**Table 8.8a: NFS Configuration Options**

Setting	Value	Description
Number of servers	integer	can not exceed number of CPUs (run <code>sysctl -n kern.smp.cpus</code> at the FreeNAS™ console shell to determine the maximum number for that system)
Asynchronous mode	checkbox	speeds up data access but may result in corruption if a transfer is interrupted

## 8.9 S.M.A.R.T

FreeNAS™ uses the `smartd(8)` service to monitor disk S.M.A.R.T. data for signs of problems. To fully configure S.M.A.R.T. you need to:

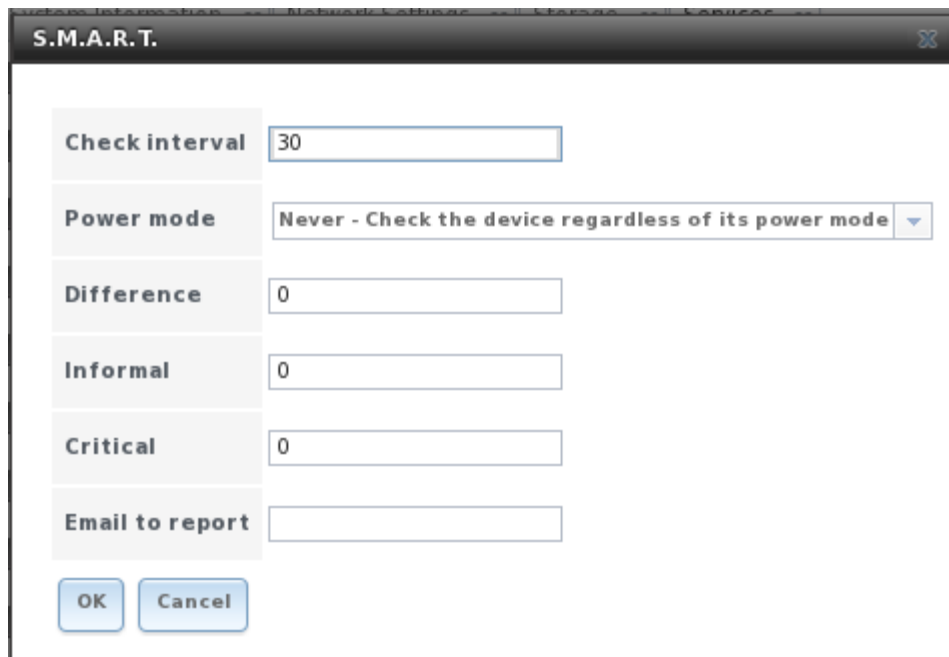
- configure when to run the S.M.A.R.T tests in System -> S.M.A.R.T Tests -> Add S.M.A.R.T. Test
- enable S.M.A.R.T. for each disk member of a volume in Volumes -> View All Volumes
- check the configuration of the S.M.A.R.T service in Services -> S.M.A.R.T.
- start the S.M.A.R.T. service in Services -> Control Services

Figure 8.9a shows the configuration screen that appears when you click Services -> S.M.A.R.T.

**NOTE:** `smartd` will wake up at every *Check Interval* you configure in Figure 8.9a. It will check the times you configured in your tests (described in Figure 4.6a) to see if any tests should be run. Since the smallest time increment for a test is an hour (60 minutes), it usually does not make sense to set a check interval value higher than 60 minutes. For example, if you set the check interval for 120 minutes and the smart test to every hour, the test will only be run every 2 hours since the daemon only wakes up every 2 hours.

Table 8.9a summarizes the options in the S.M.A.R.T Configuration screen.

**Figure 8.9a: S.M.A.R.T Configuration Options**



**Table 8.9a: S.M.A.R.T Configuration Options**

Setting	Value	Description
Check interval	integer	in minutes, how often to wake up smartd to check to see if any tests have been configured to run
Power mode	drop-down menu	can override that the configured test is not performed depending upon the power mode; choices are: never, sleep, standby, or idle
Difference	integer in degrees Celsius	default of 0 disables this check, otherwise reports if the temperature of a driver has changed by N degrees Celsius since last report
Informal	integer in degrees Celsius	default of 0 disables this check, otherwise will message with a log level of LOG_INFO if the temperature is higher than N degrees Celsius
Critical	integer in degrees Celsius	default of 0 disables this check, otherwise will message with a log level of LOG_CRIT and send an email if the temperature is higher than N degrees Celsius
Email to report	string	email address of person to receive S.M.A.R.T alert; separate multiple email recipients with a comma and no space

## 8.10 SNMP

SNMP (Simple Network Management Protocol) is a protocol used to monitor network-attached devices for conditions that warrant administrative attention. FreeNAS™ can be configured as a bsnmpd(8) server where bsnmp is FreeBSD's simple and extensible SNMP daemon. If you enable SNMP, the following port will be enabled on the FreeNAS™ system:

- UDP 161 (bsnmpd listens here for SNMP requests)

Figure 8.10a shows the SNMP configuration screen and Table 8.10a summarizes the configuration options:

**Figure 8.10a: Configuring SNMP**

**Table 8.10a: SNMP Configuration Options**

Setting	Value	Description
Location	string	optional description of FreeNAS™ system's location
Contact	string	optional e.g. email address of FreeNAS™ administrator
Community	string	password used on the SNMP network, default is public and should be changed for security reasons
Send SNMP Traps	checkbox	a trap is an event notification message
Auxiliary Parameters	string	additional bsnmpd(8) options not covered in this screen, one per line

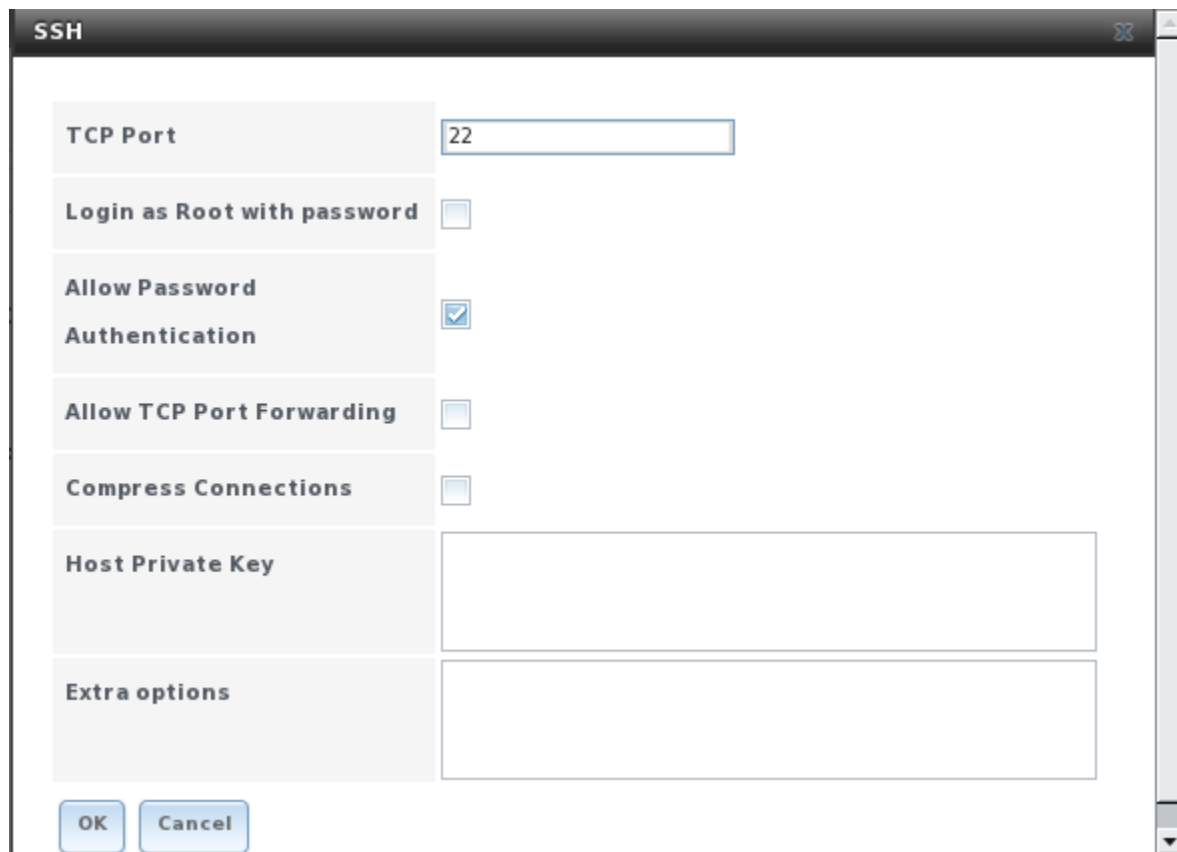
## 8.11 SSH

Secure Shell (SSH) allows for files to be transferred securely over an encrypted network. If you configure your FreeNAS™ system as an SSH server, the users in your network will need to use [SSH client software](#) in order to transfer files using SSH. You will also need to create a user account for every user requiring SSH access in Account -> Users -> Add User. When creating your users, set their home directory to the volume/dataset that you wish them to have access to. This section shows the FreeNAS™ SSH configuration options, demonstrates an example configuration that restricts users to their home directory, and provides some troubleshooting tips.



Figure 8.11a shows the Services -> SSH configuration screen and Table 8.11a summarizes the configuration options:

**Figure 8.11a: SSH Configuration**



**Table 8.11a: SSH Configuration Options**

Setting	Value	Description
TCP Port	integer	port to open for SSH connection requests, 22 by default
Login as Root with password	checkbox	for security reasons, root logins are discouraged and disabled by default
Allow Password Authentication	checkbox	if unchecked, only accepts key based authentication which is more secure but requires <a href="#">additional setup</a> on both the SSH client and server
Allow TCP Port Forwarding	checkbox	allows users to bypass firewall restrictions using SSH's <a href="#">port forwarding feature</a>
Compress Connections	checkbox	may reduce latency over slow networks
Host Private Key	string	allows you to paste a specific host key as the default key is changed with every installation
Extra Options	string	additional sshd_config(5) options not covered in this screen, one per line

A few `sshd_config(5)` options that are useful to input in the Extra Options field include:

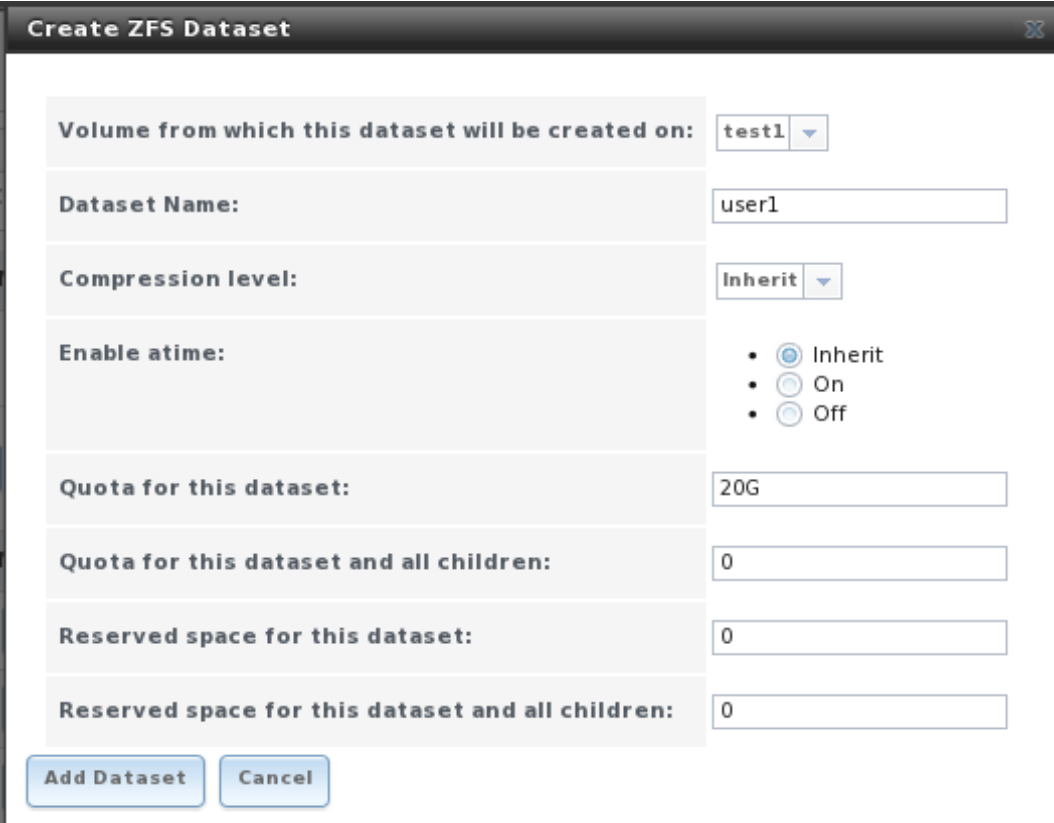
- **ClientAliveInterval:** increase this number if ssh connections tend to drop
- **ClientMaxStartup:** defaults to 10; increase if you have more users

### 8.11.1 Chrooting SFTP users

By default when you configure SSH, users can use the `ssh` command to login to the FreeNAS™ system and the `scp` and `sftp` commands to transfer files. While these commands will default to the user's home directory, users are able to navigate outside of their home directory which can pose a security risk. SSH supports using a `chroot` to confine users to only the `sftp` command and to be limited to the contents of their own home directory. To configure this scenario on FreeNAS™, perform the following steps.

**1. Create a ZFS dataset for each user requiring sftp access** in Storage -> Create ZFS Dataset. In the example shown in Figure 8.11b, a ZFS dataset named `user1` has been created on volume `/mnt/test1` with a ZFS quota of 20GB. In the next step, we will create a user named `user1` to associate with this dataset. Repeat this process to create a dataset for every user that will need access to the SSH service.

**Figure 8.11b: Create a ZFS Dataset with a Quota**



The screenshot shows a 'Create ZFS Dataset' dialog box with the following fields and values:

Volume from which this dataset will be created on:	test1
Dataset Name:	user1
Compression level:	Inherit
Enable atime:	<input checked="" type="radio"/> Inherit <input type="radio"/> On <input type="radio"/> Off
Quota for this dataset:	20G
Quota for this dataset and all children:	0
Reserved space for this dataset:	0
Reserved space for this dataset and all children:	0

Buttons: Add Dataset, Cancel

**2. Create a user account** for each user in Account -> Users -> Add User. In the screen shown in Figure 8.11c, input a Username for the user (in this example, `user1`), change the Home Directory to the name of an existing dataset (in our example, the dataset named `/mnt/test1/user1`), input a description under Full Name, input the user's email address, input and confirm the user's password, and click the OK

button. Repeat this process to create a user account for every user that will need access to the SSH service.

**Figure 8.11c: Creating a User Account**

The screenshot shows a 'Create User' dialog box with the following fields and values:

- User ID: 1001
- Username: user1
- Primary Group: (empty dropdown)
- Home Directory: /mnt/test1/user1
- Shell: csh
- Full Name: sftp chroot user
- E-mail: user1@somecompany.com
- Password: (masked with dots)
- Password confirmation: (masked with dots)
- Disable logins:

Buttons: OK, Cancel

3. **Set permissions** in Storage -> Volume -> View All Volumes. SSH chroot is *very specific* in what permissions it allows (see the *ChrootDirectory* keyword in `sshd_config(5)` for details). Your configuration will not work if the permissions on the datasets used by SSH chroot users differ from those shown in Figure 8.11d.

**Figure 8.11d: Permissions Required by SSH Chroot**

The screenshot shows the 'Change Permissions' dialog box with the following configuration:

- Change permission on: /mnt/test1/user1 to:
- Owner (user): root
- Owner (group): wheel
- Mode: (empty)
- Type of ACL: Unix
- Set permission recursively:

	Owner	Group	Other
Read	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Execute	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Buttons: Change, Cancel

**4. Create a home directory within each dataset.** Due to the permissions required by SSH chroot, the user will not have permissions to write to the root of their dataset. Since your intention is to limit them to the contents of their home directory, you can manually create a home directory for the user within their dataset. To do so, you will need to access the FreeNAS™ system's shell using the instructions in [section 10.8.7 FAQ: How do I get to the Command Line / CLI / shell](#).

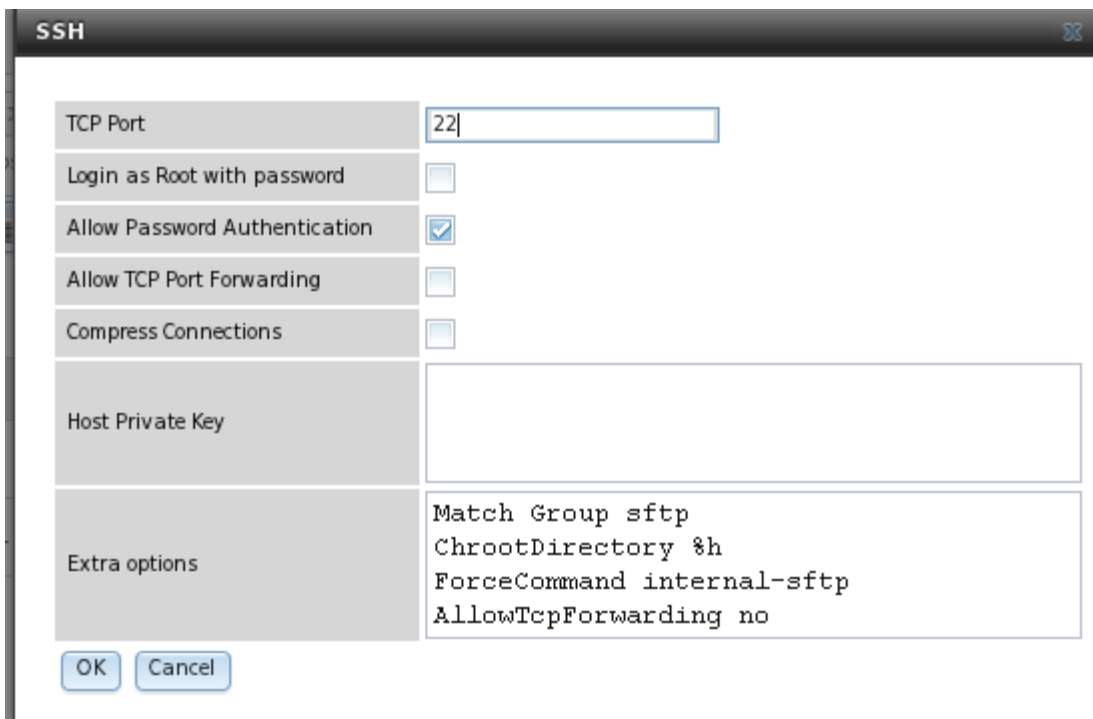
Once you have access to the FreeNAS™ console, create a home directory for each user *within their own dataset* and change the ownership of the directory to the user. Example 8.11a demonstrates the commands used to create a home directory called *user1* for the user account *user1* on dataset */mnt/test1/user1*:

**Example 8.11a: Creating a User's Home Directory**

```
mkdir /mnt/test1/user1/user1
chown user1:user1 /mnt/test1/user1/user1
```

**5. Configure SSH** in Services -> SSH. Add these lines to the Extra Options section as shown in Figure 8.11e.

**Figure 8.11e: Configure SSH for chroot**



**6. Start the SSH service** in Control Services. Click the red OFF button next to SSH. After a second or so, it will change to a blue ON, indicating that the service has been enabled.

**7. Test the connection** from a client using a utility such as [WinSCP](#). In the example shown in Figure 8.11f, *user1* is connecting to a FreeNAS™ server with an IP address of *192.168.2.9*.

Once connected, the user can see the files on their Windows system in the left frame and the files on the FreeNAS™ system in the right frame, as shown in Figure 8.11g.

Figure 8.11f: Connecting to the SSH chroot from WinSCP

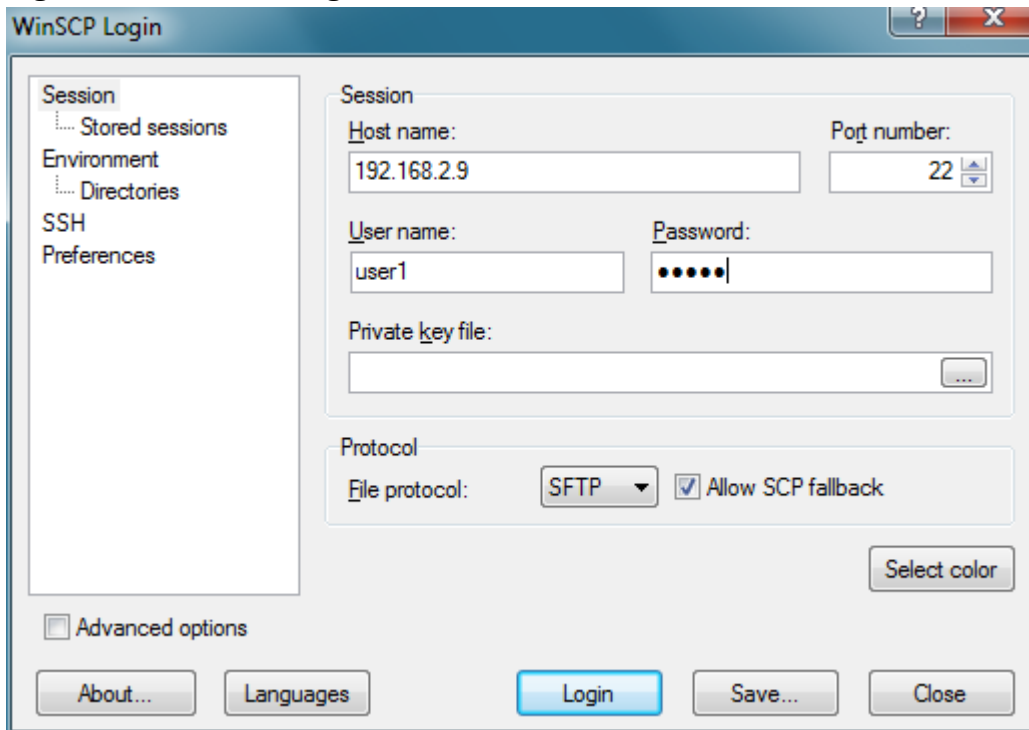
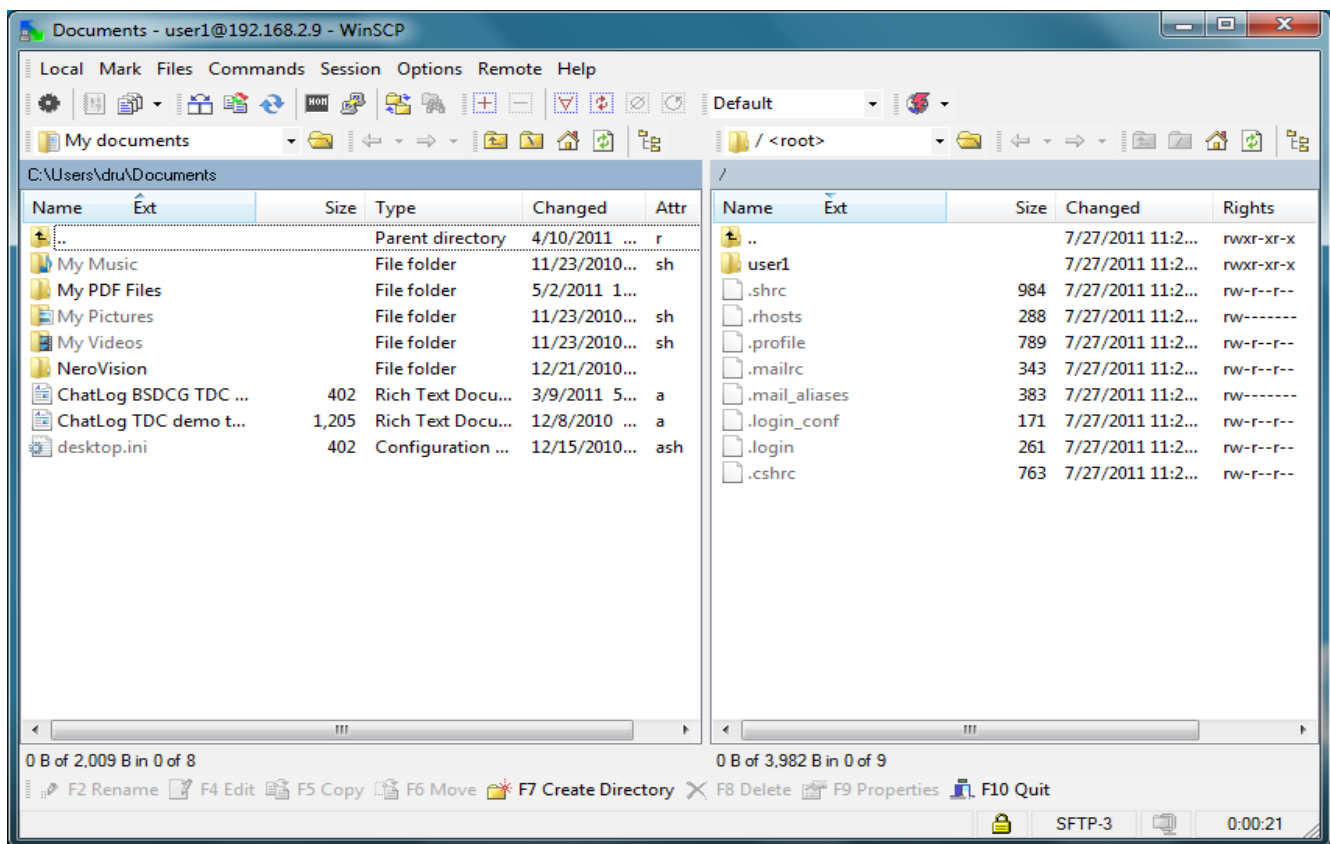


Figure 8.11g: Using WinSCP Within a chroot



Notice that the directory structure on the FreeNAS™ system starts at <root>. If the user clicks on <root>, they can not navigate to a higher folder. If the user tries to copy a file from the Windows system to <root>, the operation will fail. However, if the user clicks on their home folder (in this example, user1), they will enter that folder and can copy files to/from the Windows system within that folder.

### 8.11.2 Troubleshooting SSH Connections

If you add any Extra Options in the SSH configuration screen, be aware that the keywords listed in `sshd_config(5)` are case sensitive. This means that your configuration will fail to do what you intended if you don't match the upper and lowercase letters of the keyword.

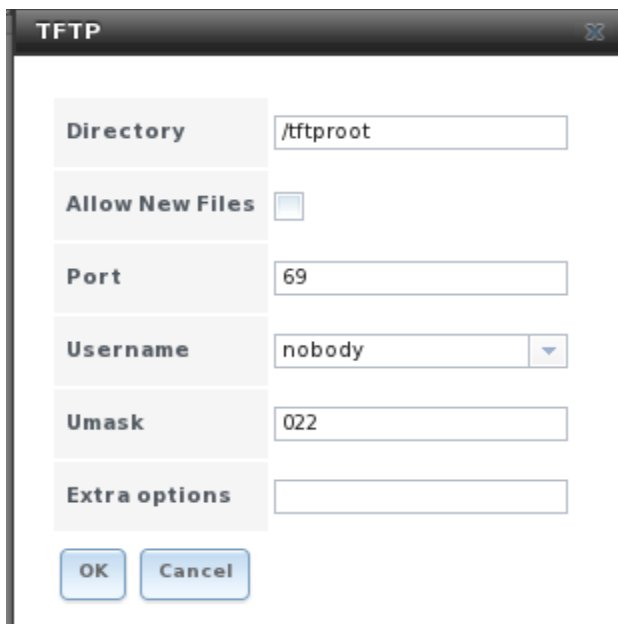
When configuring SSH, you should always test your configuration as an SSH user account to ensure that the user is limited to what you have configured and does have permission to do what you want them to do. If the user account is experiencing problems, the SSH error messages are usually pretty specific to what the problem is. You will need to access the console to read these messages with the following command:

```
tail -f /var/log/messages
```

## 8.12 TFTP

Trivial File Transfer Protocol (TFTP) is a light-weight version of FTP usually used to transfer configuration or boot files between machines, such as routers, in a local environment. TFTP is extremely limited, providing no authentication, and is rarely used interactively by a user. If you enable TFTP on your FreeNAS™ server, it will open UDP port 69. An example where this is useful is when you wish to store all of the images and configuration files for your network's devices on the FreeNAS™ system. Figure 8.12a shows the TFTP configuration screen and Table 8.12a summarizes the available options:

**Figure 8.12a: TFTP Configuration**



Directory	/tftpboot
Allow New Files	<input type="checkbox"/>
Port	69
Username	nobody
Umask	022
Extra options	

**Table 8.12a: TFTP Configuration Options**

Setting	Value	Description
Directory	string	most devices expect a path of /tftpboot
Allow New Files	checkbox	enable if network devices need to send files to the FreeNAS™ system (e.g. backup their config)
Port	integer	port to listen for TFTP requests, 69 by default
Username	drop-down menu	account used for tftp requests
Umask	integer	umask for newly created files, default is 022
Extra options	string	additional tftpd(8) options not shown in this screen, one per line

### 8.13 UPS

FreeNAS™ uses [NUT](#) (Network UPS Tools) to provide UPS support.

Figure 8.13a shows the UPS configuration screen:

**Figure 8.13a: UPS Configuration Screen**

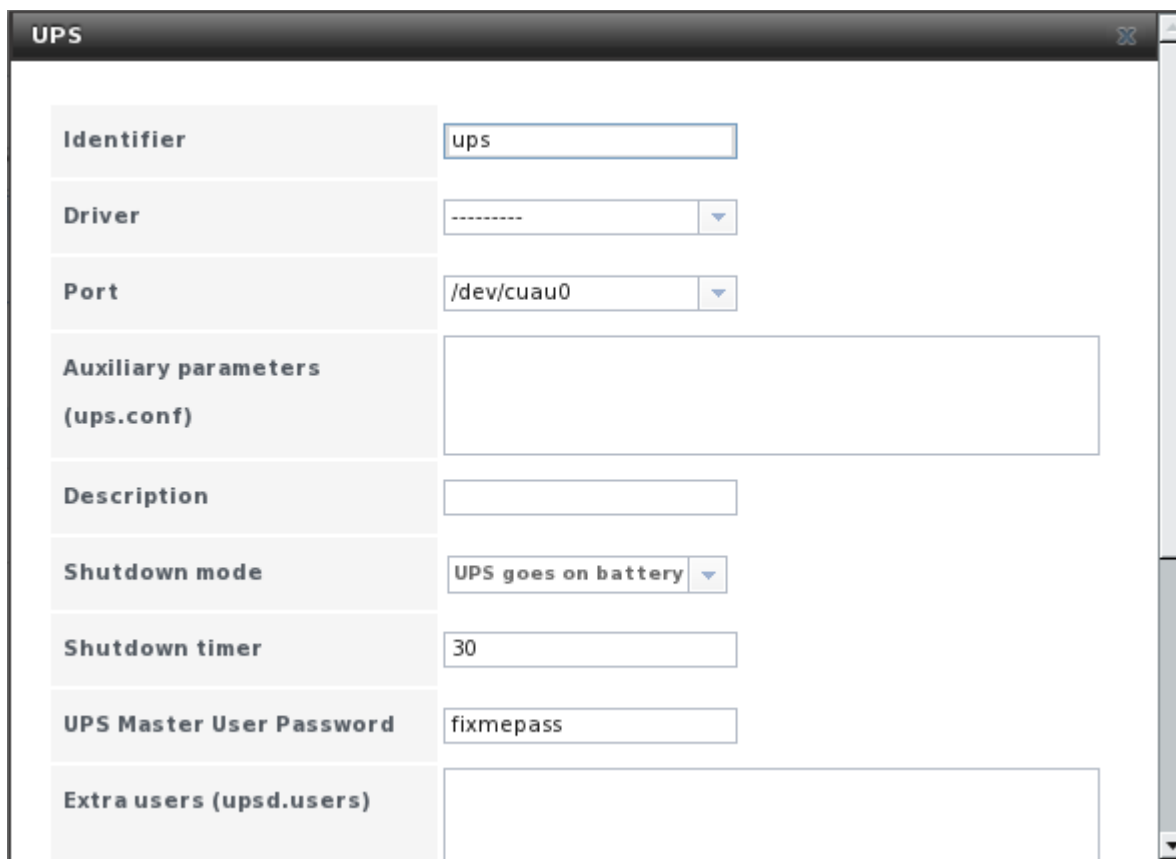


Table 8.13a summarizes the options in the UPS Configuration screen.

**Table 8.13a: UPS Configuration Options**

Setting	Value	Description
Identifier	string	input a descriptive name, default is ups
Driver	drop-down menu	supported UPS devices are listed at <a href="http://www.networkupstools.org/stable-hcl.html">http://www.networkupstools.org/stable-hcl.html</a>
Port	drop-down menu	list of available serial (e.g. /dev/cuau#) or USB ports (e.g. /dev/ugen.X.X) UPS is plugged into (see NOTE below)
Auxiliary Parameters	string	additional options from <a href="#">ups.conf(5)</a>
Description	string	optional
Shutdown mode	drop-down menu	choices are UPS goes on battery and UPS reaches low battery
Shutdown timer	integer	in seconds
UPS Master User Password	string	default is fixmepass
Extra users	string	see <a href="#">upsd.users(5)</a> for examples
Remote monitor	checkbox	defaults to listen to everything and uses the user "upsmon" and password "fixmepass"
Send Email Status Updates	checkbox	if checked, configure the To email
To email	email address	if Send Email box checked, email address of person to receive update
Email subject	string	if send Email Box checked, subject of email updates

**NOTE:** for USB devices, the easiest way to determine the correct device name is to enable console logging in System -> Settings -> Advanced -> check the box for "Show console messages". Refresh your browser and plug in the USB device. The messages will give the name of the /dev/ugenX.X device; replace the X's in your configuration with the actual numbers that show on the console.

## 8.14 iSCSI

iSCSI is a protocol standard that allows the consolidation of storage data. iSCSI allows FreeNAS™ to act like a storage area network (SAN) over an existing Ethernet network. Specifically, it exports disk devices over an Ethernet network that iSCSI clients (called initiators) can attach to and mount. Traditional SANs operate over fibre channel networks which require a fibre channel infrastructure such as fibre channel HBAs, fibre channel switches, and discreet cabling. iSCSI can be used over an existing Ethernet network, although dedicated networks can be built for iSCSI traffic in an effort to boost performance. iSCSI also provides an advantage in an environment that uses Windows shell programs; these programs tend to filter “Network Location” but iSCSI mounts are not filtered.

Before configuring iSCSI on your FreeNAS™ device, you should be familiar with the following iSCSI terminology:



**CHAP:** a protocol used for authenticating initiators (clients) by a target (server). CHAP uses a shared secret and three-way authentication to determine if a system is authorized to access the storage device and to periodically confirm that the session has not been hijacked by another system.

**Mutual CHAP:** a superset of CHAP. The target authenticates the initiator as in CHAP, and additionally the initiator uses CHAP to authenticate the target.

**Initiator:** the remote system (client) which has authorized access to the storage data on the FreeNAS™ system.

**Target:** a storage resource on the FreeNAS™ system (server).

**Extent:** the storage unit to be shared. It can either be a file or a device.

In order to configure iSCSI, you need to:

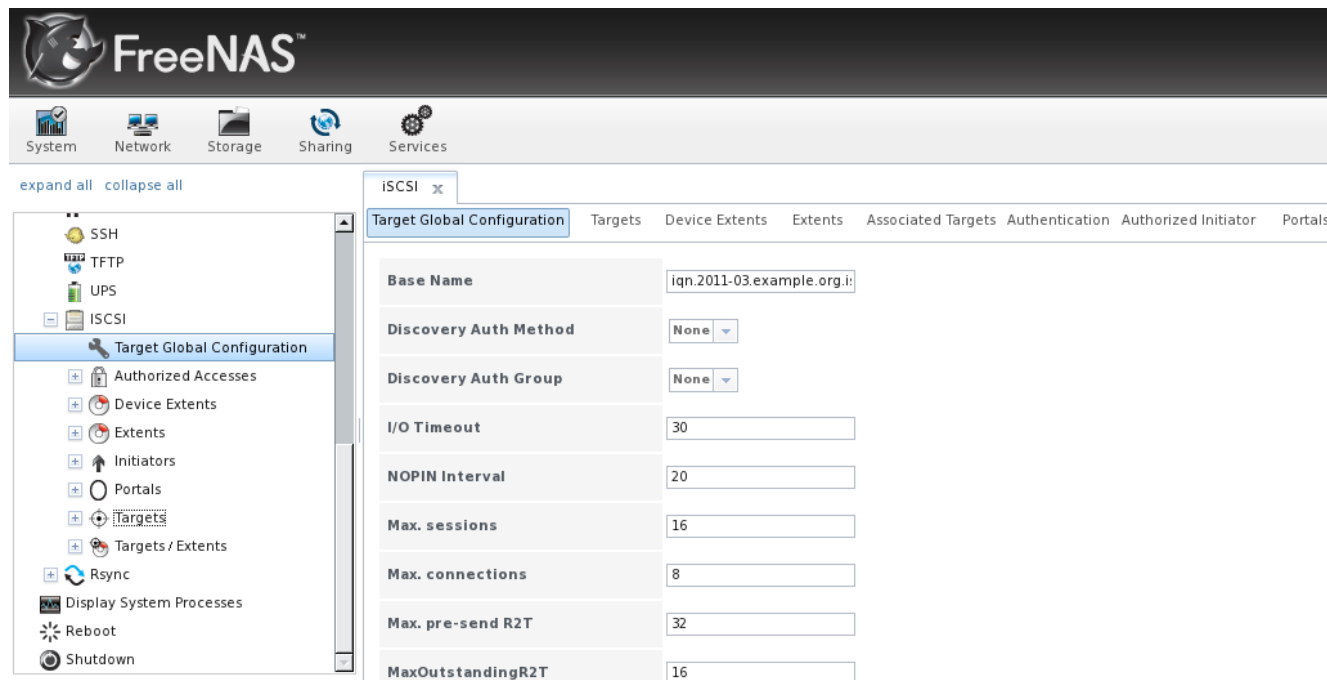
- review the Target Global Configuration parameters
- decide if you will use CHAP or mutual CHAP for authentication; if so, create an authorized access
- create either a device extent or a file extent
- determine which hosts are allowed to connect using iSCSI and create an initiator
- determine if you need to create a portal (only required when the FreeNAS™ system has multiple IP addresses or network interfaces that will be used for iSCSI connections)
- create a target
- associate a target with an extent
- start the iSCSI service in Services -> Control Services

**NOTE:** FreeNAS™ uses [istgt](#) to provide iSCSI. At this time, istgt does not support SIGHUP-style configuration reloading, meaning that FreeNAS™ has to restart istgt to make configuration changes take effect. This means that any changes to existing iSCSI shares will cause any client that happens to be writing at the time to be thrown into read-only mode. Future versions of istgt will fix this known issue. Many iSCSI initiators handle the iSCSI service dropping off fairly gracefully. VMware ESXi pauses its VMs while it tries to reconnect, offering a fairly large grace period where things will recover automatically.

### 8.14.1 Target Global Configuration

The Target Global Configuration screen, shown in Figures 8.14a, contains settings that apply to all iSCSI shares. Table 8.14a summarizes the settings that can be configured in the Target Global Configuration screen. The integer values in the table are used to tune network performance; most of these values are described in [RFC 3720](#). LUC (Logical Unit Controller) is an API provided by istgt to control removable media by providing functions to list targets, un/load a media to a unit, change media file, or reset a LUN.

**Figure 8.14a: iSCSI Target Global Configuration Variables**



**Table 8.14a: Target Global Configuration Settings**

Setting	Value	Description
Base Name	string	see the “Constructing iSCSI names using the iqn. format” section of <a href="#">RFC 3721</a> for details.
Discovery Auth Method	drop-down menu	Choices are: None, Auto, CHAP, or Mutual CHAP. Configures the authentication level required by the target for discovery of valid devices. None will allow anonymous discovery. CHAP and Mutual CHAP require authentication. Auto lets the initiator decide the authentication scheme.
Discovery Auth Group	drop-down menu	Required if Discovery Auth Method is set to CHAP or Mutual CHAP, optional if Discovery Auth Method is set to Auto, and not needed if Discovery Auth Method is set to None. In the latter two cases the config generated in the [Global] section of <i>istgt.conf</i> will be DiscoveryAuthGroup None, otherwise it will be a number like DiscoveryAuthGroup 1.
I/O Timeout	integer representing seconds	Sets the limit on how long an I/O can be outstanding before an error condition is returned. Possible values range from 0 -300 with a default value of 30.
NOPIN Interval	integer representing seconds	How often target sends a NOP-IN packet to keep a discovered session alive. Possible values range from 0 -300 with a default value of 20.

Setting	Value	Description
Max. Sessions	integer	All connections between an iSCSI initiator portal and a target portal are associated with a specific session. This option limits the number of sessions the target will create/accept. Possible values range from 1 - 64 with a default value of 16.
Max. Connections	integer	Refers to the number of connections a single initiator can make with respect to a single target. Possible values range from 1 - 64 with a default value of 8.
Max. pre-send R2T	integer	Possible values range from 1 - 255 with a default value of 32.
MaxOutstandingR2T	integer	During writes, the target pulls data from the initiator by sending R2T (ready to receive) packets. This option sets the maximum number of R2Ts the target can have outstanding for a single iSCSI command. Larger values should yield performance increases until MaxOutstandingR2T exceeds the size of the largest Write I/O divided by MaxBurstLength. Possible values range from 1 - 255 with a default value of 16.
First burst length	integer	The maximum amount in bytes of unsolicited data an iSCSI initiator may send to the target during the execution of a single SCSI command. Possible values range from 1 - 2 <sup>32</sup> with a default value of 65536.
Max burst length	integer	Maximum write size in bytes the target is willing to receive per burst of packets (i.e. between R2Ts). Possible values range from 1 - 2 <sup>32</sup> with a default value of 262144.
Max receive data segment length	integer	In bytes. Possible values range from 1 - 2 <sup>32</sup> with a default value of 262144.
DefaultTime2Wait	integer	The minimum time in seconds to wait before attempting a logout or an active task reassignment after an unexpected connection termination or reset. Possible values range from 1 - 300 with a default value of 2.
DefaultTime2Retain	integer	The maximum time in seconds after Time2Wait before which an active task reassignment is still possible after an unexpected connection termination or reset. Possible values range from 1 - 300 with a default value of 60.
Enable LUC	checkbox	Only works with removable media. If checked, the rest of the fields are required.
Controller IP address	IP address	Must be an IP address that is assigned to an interface or the daemon won't start. Generally set to 127.0.0.1.
Controller TCP port	integer	Possible values range from 1024-65535 with a default value of 3261.
Controller Authorized netmask	subnet mask	Typically set to 255.0.0.0.
Controller Auth	drop-down	Choices are None, Auto, CHAP, or mutual CHAP.

Setting	Value	Description
Method	menu	
Controller Auth Group	drop-down menu	Required if Controller Auth Method is set to CHAP or Mutual CHAP, optional if Controller Auth Method is set to Auto, and not needed if Controller Auth Method is set to None. In the latter two cases the config generated in the [Global] section of <i>istgt.conf</i> will be ControllerAuthGroup None, otherwise it will be a number like ControllerAuthGroup 1. If you wish to use authenticated discover the users must be configured prior to this step.

### 8.14.2 Authorized Accesses

If you will be using CHAP or mutual CHAP to provide authentication, you must create an authorized access. Go to Services → iSCSI → Authorized Accesses → Add Authorized Access which will open the screen seen in Figure 8.14b.

**NOTE:** CHAP does not work with GlobalSAN initiators on Mac OS X.

**Figure 8.14b: Adding Authorized Access for iSCSI**

The screenshot shows a dialog box titled "Add Authorized Access". It contains the following fields and values:

- Group ID: 1
- User: (empty)
- Secret: (empty)
- Secret (Confirm): (empty)
- Peer User: (empty)
- Initiator Secret: (empty)
- Initiator Secret (Confirm): (empty)

At the bottom of the dialog are two buttons: "OK" and "Cancel".

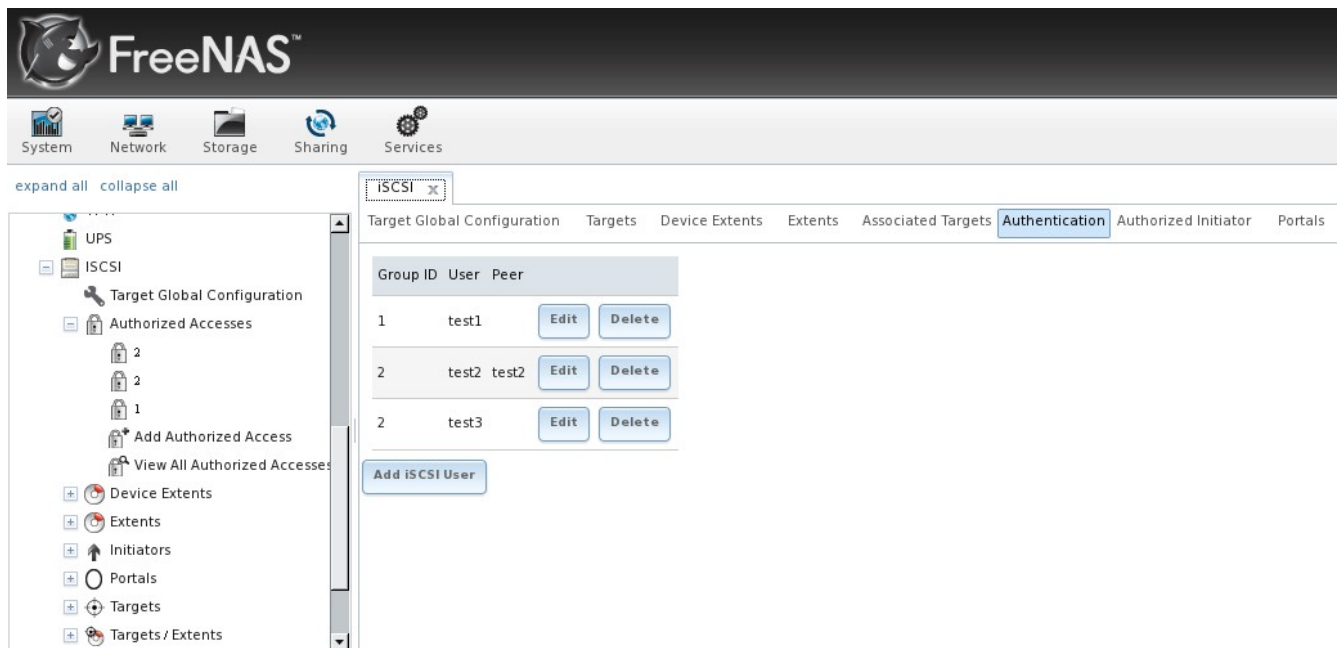
Table 8.14b summarizes the settings that can be configured when adding an authorized access:

**Table 8.14b: Authorized Access Configuration Settings**

Setting	Value	Description
Group ID	integer	The Group ID is used to build the authentication groups used by the iSCSI target software, allowing different groups to be configured with different authentication profiles. For instance, all users with a Group ID of 1 will be members of “Group 1” and will inherit the authentication profile associated with that group.
User	string	Name of user account that will be created on the FreeNAS™ device in order to CHAP authenticate with the user on the remote system. Many initiators default to using the initiator name as the user.
Secret	string	Needs to be confirmed. Password to be associated with the created user account.
Peer User	string	If this is entered it will cause the user to be a Mutual CHAP user. In most cases it will need to be the same as the User.
Initiator Secret	string	Needs to be confirmed. The mutual secret password. Must be different than the Secret. This is required if the Peer User field is set.

As users are added, they will be listed under Authorized Accesses. In the example shown in Figure 8.14c, three users (*test1*, *test2*, and *test3*) have been configured and there are two groups created, with group 1 consisting of a single CHAP user and group 2 consisting of a mutual CHAP user and a CHAP user.

**Figure 8.14c: Viewing Authorized iSCSI Users**



### 8.14.3 Device Extents

The next step is to configure the share. In iSCSI terminology, you don't share a volume; instead you share either a device extent or a file extent:

**Device extent:** allows an unformatted disk, a zvol, or an existing [HAST device](#) to be exported via iSCSI. The advantage of a device extent is that it is faster than a file extent. The disadvantage is that the entire volume is exported. If you only want to share a portion of a volume using iSCSI, either create a zvol (if it is a ZFS volume) or use a file extent. You can create a zvol by clicking Storage -> Create ZFS Volume.

**File extent:** allows you to export a portion of a volume. When creating a file extent, you can specify either a non-existing file name or an existing ZFS dataset. The advantage of file extents is that you can create multiple exports per volume. The disadvantage is that they are slower than device extents.

To add a device extent, go to Services → iSCSI → Device Extents → Add Device Extent. In the example shown in Figure 8.14d, a device extent is being created using a raw (unformatted) disk.

**Figure 8.14d: Adding an iSCSI Device Extent**

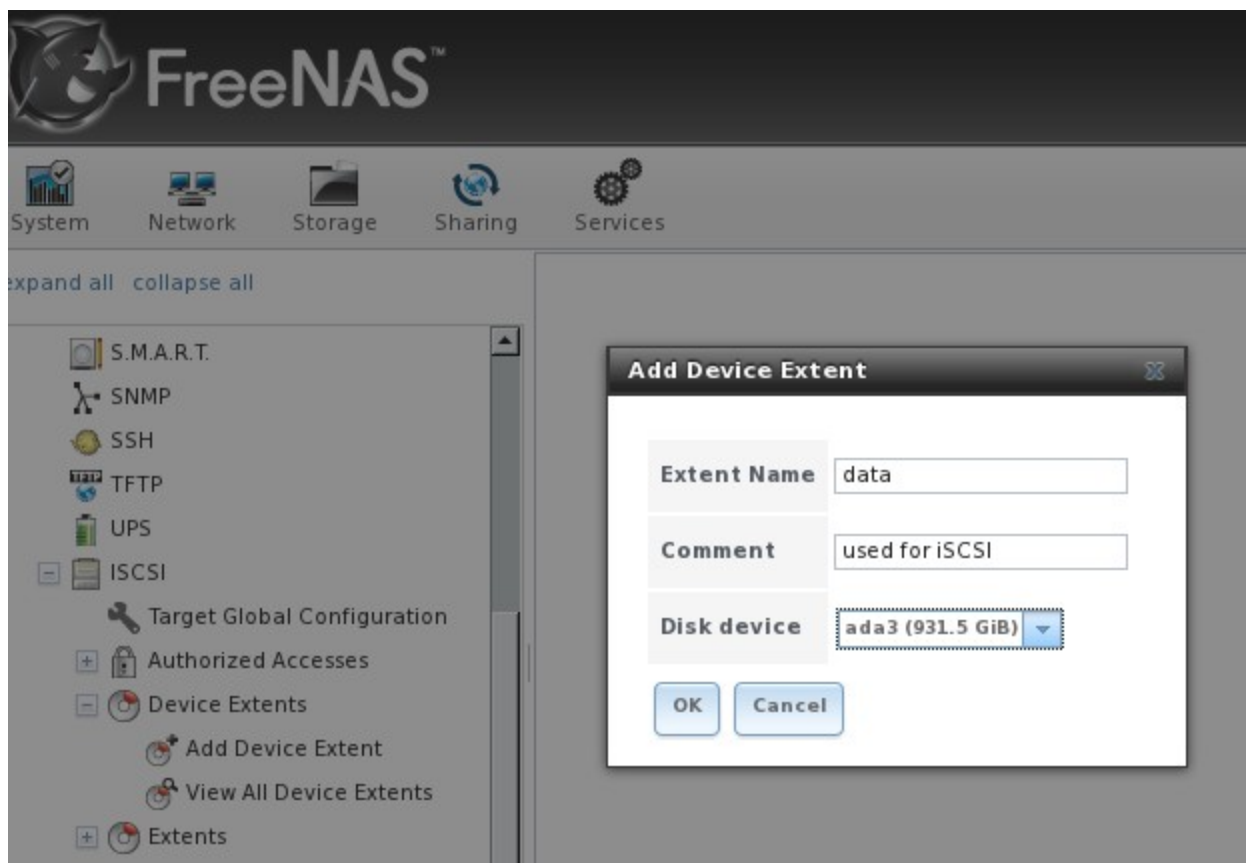


Table 8.14c summarizes the settings that can be configured when creating a device extent:

**Table 8.14c: Device Extent Configuration Settings**

Setting	Value	Description
Extent Name	string	required
Comment	string	optional
Disk device	drop-down menu	select the unformatted disk, previously created zvol, or existing HAST device

### 8.14.4 Extents

To add a file extent, go to Services → ISCSI → Extents → Add Extent. In the example shown in Figure 8.14e, a file extent named *data* with a maximum size of *20 GB* will be created on the ZFS dataset */mnt/tank/iscsi*. Note that the file extent creation will fail if you do not append the name of the file to be created to the volume/dataset name.

**Figure 8.14e: Adding an iSCSI File Extent**

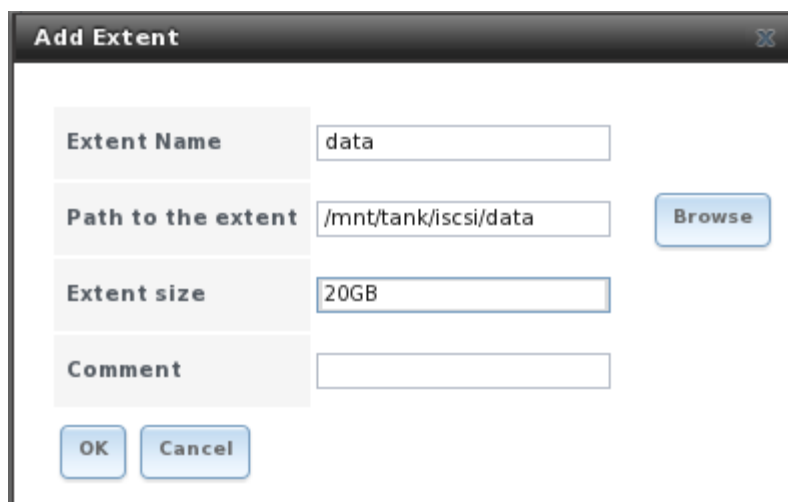


Table 8.14d summarizes the settings that can be configured when creating an File Extent:

**Table 8.14d: File Extent Configuration Settings**

Setting	Value	Description
Extent Name	string	name of file extent, can not be an existing file within the dataset
Path to the extent	browse button	browse to the path where the file will be created or to an existing dataset
Extent size	integer	if the size is specified as 0 then the actual file size will be used and the file must be created manually in the CLI
Comment	string	optional

### 8.14.5 Initiators

The next step is to configure authorized initiators, or the systems which are allowed to connect to the stored data. Going to Services → ISCSI → Initiators → Add Initiator will bring up the screen shown in Figure 8.14f. Table 8.14e summarizes the settings that can be configured when adding an initiator.

**NOTE:** at this time, the FreeNAS™ system itself can not be configured as an initiator.

**Figure 8.14f: Adding an iSCSI Initiator**

The screenshot shows a dialog box titled "Add Initiator" with a close button (X) in the top right corner. It contains three input fields: "Initiators" with the value "ALL", "Authorized network" with the value "ALL", and an empty "Comment" field. Below the fields are "OK" and "Cancel" buttons.

**Table 8.14e: Initiator Configuration Settings**

Setting	Value	Description
Initiators	string	can use ALL keyword or a list of initiator hostnames separated by commas with no space
Authorized network	string	can use ALL keyword or a network address with CIDR mask such as 192.168.2.0/24
Comment	string	optional description

In the example shown in Figure 8.14g, two groups have been created. Group 1 allows connections from any initiator on any network; Group 2 only allows connections from any initiator on the 10.10.1.0/24 network.

**Figure 8.14g: Sample iSCSI Initiator Configuration**

The screenshot shows the "iSCSI" configuration page with the "Authorized Initiator" tab selected. It displays a table with the following data:

Group ID	Initiators	Authorized Network	Comment
1	ALL	ALL	
2	ALL	10.10.1.0/24	

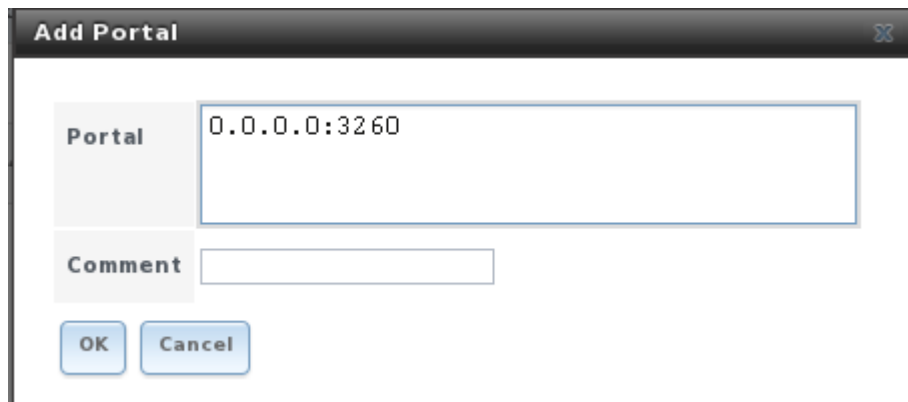
Each row in the table has "Edit" and "Delete" buttons. Below the table is an "Add Authorized Initiator" button.



### 8.14.6 Portals

A portal allows FreeNAS™ systems with multiple IP addresses or interfaces to provide services on different interfaces or subnets. Going to Services → iSCSI → Portals → Add Portal will bring up the screen shown in Figure 8.14h:

**Figure 8.14h: Adding an iSCSI Portal**



In this example, *0.0.0.0:3260* is a wildcard that will cause the system to bind to every IP address and interface. This allows you to use multi-path I/O (MPIO).

Table 8.12f summarizes the settings that can be configured when adding a portal:

**Table 8.14f: Portal Configuration Settings**

Setting	Value	Description
Portal	string	interface or subnet IP address followed by a colon and the TCP port used by iSCSI (3260 by default)
Comment	string	optional description

### 8.14.7 Targets

Next you should add a Target using Services → iSCSI → Targets → Add Target, as shown in Figure 8.14i. A target combines a portal ID, allowed initiator ID, and an authentication method.

Table 8.14g summarizes the settings that can be configured when creating a Target.

**NOTE:** multiple computers can not connect to the same iSCSI target as iSCSI acts like a physical disk rather than a share. If you need to support multiple clients to the same data, use CIFS or NFS instead of iSCSI or create multiple iSCSI targets (one per client).

**Figure 8.14i: Adding an iSCSI Target**

**Table 8.14g: Target Settings**

Setting	Value	Description
Target Name	string	required value; base name will be appended automatically if it does not start with iqn
Target Alias	string	optional user-friendly name
Serial	string	unique ID for target to allow for multiple LUNs; the default is generated from the system's MAC address
Type	drop-down menu	type of device: choices are disk, DVD, tape, or pass (choose pass in a virtual environment)
Target Flags	drop-down menu	choices are read-write or read-only
Portal Group ID	drop-down menu	leave empty or select number of existing portal to use
Initiator Group ID	drop-down menu	select which existing initiator group has access to the target
Auth Method	drop-down menu	choices are None, Auto, CHAP, or mutual CHAP
Authentication Group number	drop-down menu	none or integer representing number of existing authorized access
Queue Depth	integer	see <a href="#">this post</a> for an explanation of the math involved

Setting	Value	Description
Logical Block Size	integer	should only be changed if you need to emulate a physical disk's size or you need to increase the block size to allow for larger filesystems on operating systems limited by block count

### 8.14.8 Target/Extents

The last step is associating extents to targets within Services → iSCSI → Target/Extents → Add Target/Extent. This screen is shown in Figure 8.14j. Use the drop-down menus to select the desired target and extent.

**Figure 8.14j: Associating iSCSI Targets/Extents**

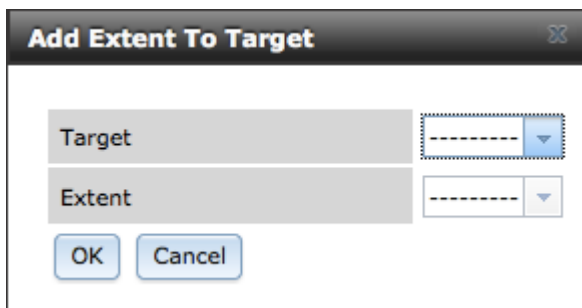


Table 8.14h summarizes the settings that can be configured when associating targets and extents:

**Table 8.14h: Target/Extents Configuration Settings**

Setting	Value	Description
Target	drop-down menu	select the pre-created target
Extent	drop-down menu	select the pre-created extent

It is best practice to associate extents to targets in a 1:1 manner, although the software will allow multiple extents to be associated to a target.

Once iSCSI has been configured, click the Services -> Control Services icon. Click the iSCSI button to change it from Off to On and thus start the iSCSI service.

### 8.14.9 Connecting to iSCSI Share

In order to access the data on the iSCSI share, clients will need to use iSCSI initiator software.

An iSCSI Initiator client is pre-installed with Windows 7. A detailed how-to for this client can be found [here](#).

Mac OS X does not include an initiator. This [how-to](#) demonstrates how to use globalSAN, a free and easy-to-use Mac initiator.

BSD systems provide command line initiators: [iscntrl\(8\)](#) comes with FreeBSD, [iscsi-initiator\(8\)](#)

comes with NetBSD, and [iscsid\(8\)](#) comes with OpenBSD.

Some Linux distros provide the command line utility **iscsiadm** from [Open-iSCSI](#). Google to see if a package exists for your distribution should the command not exist on your Linux system.

Instructions for connecting from a VMware ESXi Server can be found at [How to configure FreeNAS 8 for iSCSI and connect to ESX\(i\)](#). Note that the requirements for booting vSphere 4.x off iSCSI differ between ESX and ESXi. ESX requires a hardware iSCSI adapter while ESXi requires specific iSCSI boot firmware support. The magic is on the booting host side, meaning that there is no difference to the FreeNAS™ configuration. See the [iSCSI SAN Configuration Guide](#) for details.

## 8.15 Rsync

The Rsync section of Services is used to configure an rsync server. See [section 4.6 Rsync Tasks](#) for instructions on how to configure an rsync client and an example of configuring both ends of an rsync connection.

This section describes the configurable options for the rsyncd service and rsync modules.

Figure 8.15a shows the rsyncd configuration screen which is accessed from Services -> Rsync -> Configure Rsyncd.

**Figure 8.15a: Rsyncd Configuration**



Table 8.15a summarizes the options that can be configured for the rsync daemon:

**Table 8.15a: Rsync Configuration Options**

Setting	Value	Description
TCP Port	integer	port for rsyncd to listen on, default is 873
Auxiliary parameters	string	additional parameters from <a href="#">rsync(1)</a>

### 8.15.1 Rsync Modules

Figure 8.15b shows the configuration screen that appears when you click Services -> Rsync -> Rsync Modules -> Add Rsync Module.

**Figure 8.15b: Adding an Rsync Module**

Table 8.15b summarizes the options that can be configured when creating a rsync module:

**Table 8.15b: Rsync Module Configuration Options**

Setting	Value	Description
Module name	string	mandatory; also needs to be configured on rsync client
Comment	string	mandatory
Path	browse button	of volume/dataset to hold received data
Access Mode	drop-down menu	choices are read and write, read-only, or write-only
Maximum connections	integer	0 is unlimited
User	drop-down menu	select user that file transfers to and from that module should take place as
Group	drop-down menu	select group that file transfers to and from that module should take place as
Hosts allow	string	see <a href="#">rsyncd.conf(5)</a> for allowed formats
Hosts deny	string	see <a href="#">rsyncd.conf(5)</a> for allowed formats
Auxiliary parameters	string	additional parameters from <a href="#">rsyncd.conf(5)</a>

**NOTE:** one of the things that isn't apparent from the documentation for some versions of `rsyncd.conf(5)` is that `*` is an alias for `all`.

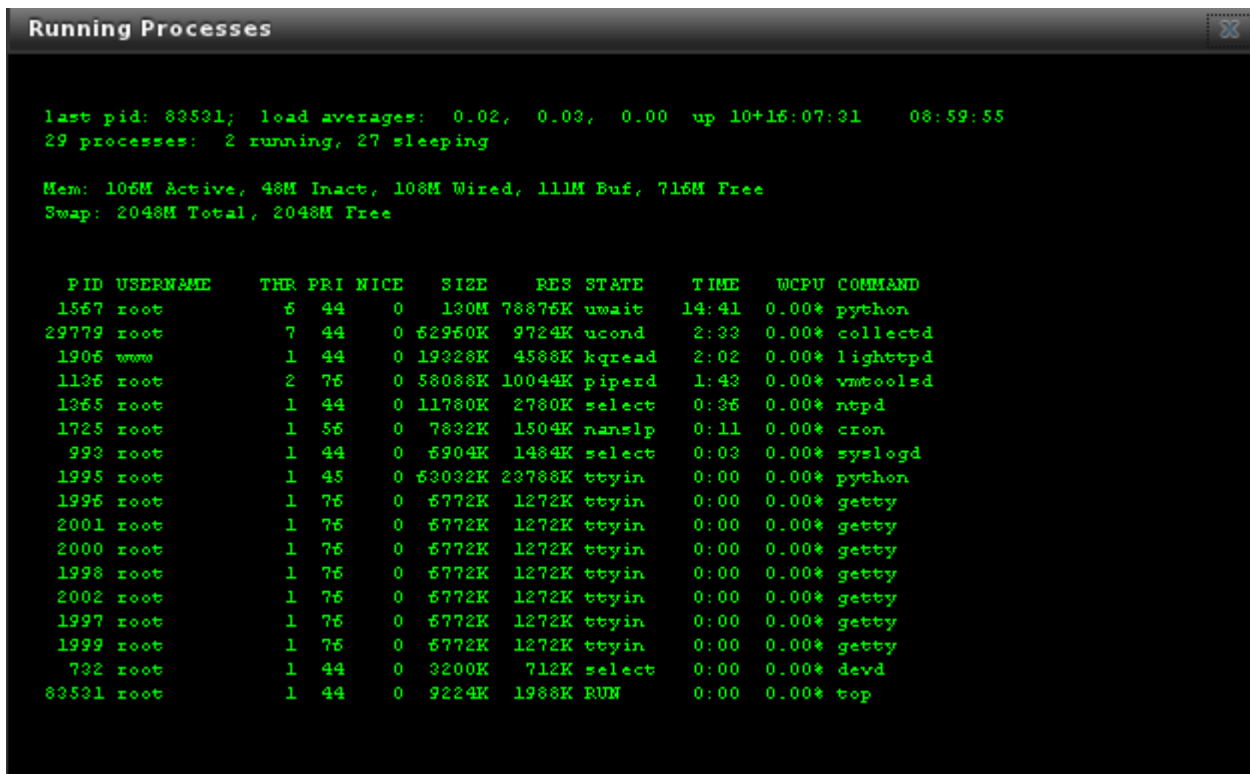
## 9 Additional Options

This section covers the remaining miscellaneous options available from the FreeNAS™ web interface.

### 9.1 Display System Processes

If you click Display System Processes, a screen will open showing the output of `top(1)`. An example is shown in Figure 9.1a.

**Figure 9.1a: System Processes Running on FreeNAS™**



```
Running Processes
last pid: 83531; load averages:  0.02,  0.03,  0.00  up 10+16:07:31   08:59:55
29 processes:  2 running, 27 sleeping

Mem: 106M Active, 48M Inact, 108M Wired, 111M Buf, 716M Free
Swap: 2048M Total, 2048M Free

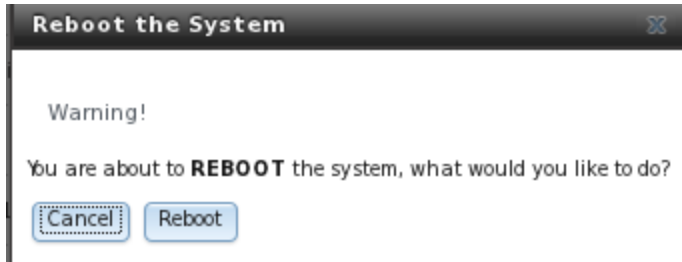
  PID USERNAME   THR PRI NICE   SIZE    RES STATE   TIME  WCPU COMMAND
1567  root          6  44   0   130M   78876K uwait   14:41  0.00% python
29779 root          7  44   0   62960K   9724K ucond    2:33  0.00% collectd
1906  www           1  44   0   19328K   4588K kqread    2:02  0.00% lighttpd
1136  root          2  75   0   58088K  10044K piperd    1:43  0.00% vmtoolsd
1365  root          1  44   0   11780K   2780K select    0:36  0.00% ntpd
1725  root          1  56   0    7832K   1504K nanslp    0:11  0.00% cron
  993  root          1  44   0    6904K   1484K select    0:03  0.00% syslogd
1995  root          1  45   0   63032K  23788K ttyin    0:00  0.00% python
1996  root          1  76   0    6772K   1272K ttyin    0:00  0.00% getty
2001  root          1  76   0    6772K   1272K ttyin    0:00  0.00% getty
2000  root          1  76   0    6772K   1272K ttyin    0:00  0.00% getty
1998  root          1  76   0    6772K   1272K ttyin    0:00  0.00% getty
2002  root          1  76   0    6772K   1272K ttyin    0:00  0.00% getty
1997  root          1  76   0    6772K   1272K ttyin    0:00  0.00% getty
1999  root          1  76   0    6772K   1272K ttyin    0:00  0.00% getty
  732  root          1  44   0    3200K    712K select    0:00  0.00% devd
83531 root          1  44   0    9224K   1988K RUN     0:00  0.00% top
```

The display will automatically refresh itself. Simply click the X in the upper right corner to close the display when you are finished. Note that the display is read-only, meaning that you won't be able to issue a **kill** command within it.

### 9.2 Reboot

If you click Reboot, you will receive the warning message shown in Figure 9.2a.

**Figure 9.2a: Reboot Warning Message**

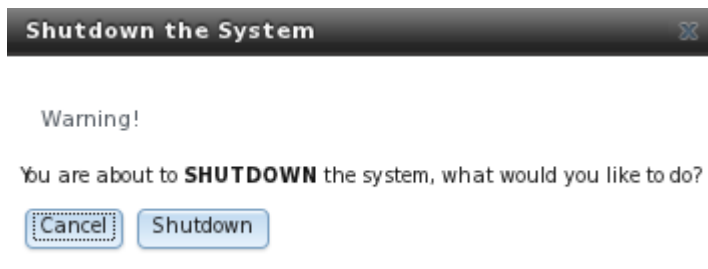


Click the Cancel button if you wish to cancel the reboot request. Otherwise, click the Reboot button to reboot the system. Rebooting the system will disconnect all clients, including the web administration GUI. The URL in your web browser will change to add /system/reboot/ to the end of the IP address. Wait a few minutes for the system to boot, then use your browser's back button to return to the FreeNAS™ system's IP address. If all went well, you should receive the GUI login menu. However, if something went wrong, you will need physical access to the FreeNAS™ system's monitor and keyboard so that you can determine what problem is preventing the system from resuming normal operation.

### 9.3 Shutdown

If you click Shutdown, you will receive the warning message shown in Figure 9.3a and your browser colour will change to red to indicate that you have selected an option that will negatively impact users of the FreeNAS™ system.

**Figure 9.3a: Shutdown Warning Message**



Click the Cancel button if you wish to cancel the shutdown request. Otherwise, click the Shutdown button to reboot the system. Shutting down the system will disconnect all clients, including the web administration GUI, and will power off the FreeNAS™ system. You will need physical access to the FreeNAS™ system in order to turn it back on.

### 9.4 Log Out

To log out of the FreeNAS™ GUI, simply click the Log Out button in the upper right corner. You will immediately be logged out. An informational message will indicate that you are logged out and will provide a hyperlink which you can click on to log back in.

## 9.5 Help

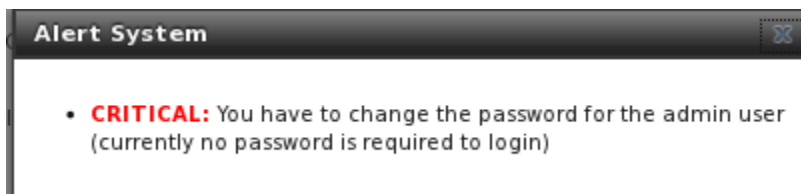
The Help button in the upper right corner provides hyperlinks to the various FreeNAS™ resources, including: forums, mailing lists, IRC channel, bug tracker, and this documentation. Each of these resources is discussed in more detail in the next section.

It also displays the currently installed FreeNAS™ version.

## 9.6 Alert

FreeNAS™ provides an alert system to provide a visual warning of any conditions that require administrative attention. The Alert button in the far right corner will flash red when there is an outstanding alert. For example, the first time you access the administrative GUI, the alert button will be flashing. If you click the icon, you will see the screen shown in Figure 9.6a:

**Figure 9.6a: Example Alert Message**



Behind the scenes, an alert script checks for various alert conditions, such as volume status, and writes these to `/var/tmp/alert`. A javascript retrieves the current alert status every 5 minutes and will change the solid green alert icon (if there are no current alert conditions) to flashing red (if a new alert is detected).

# Section 3: Getting Help

## 10 FreeNAS™ Support Resources

FreeNAS™ has a large installation base and an active user community. This means that many usage questions have already been answered and the details are available on the Internet. If you get stuck using FreeNAS™, spend a few moments searching the Internet for the word FreeNAS™ with some key words that describe your error message or the function that you are trying to implement.

FreeNAS™ 8.0 was released in May of 2011 while the original version of FreeNAS™ (now at version .7) has been around since 2005. Accordingly, much of the of information available on the Internet was written for FreeNAS™ .7.x and may or may not apply to FreeNAS™ 8.x.

The rest of this section discusses the additional resources available to FreeNAS™ 8.x users:

- [Website and Social Media](#)
- [Trac Database](#)
- [IRC](#)
- [Mailing Lists](#)



- [Forums](#)
- [Instructional Videos](#)
- [Professional Support](#)
- [FAQs](#)

## 10.1 Website and Social Media

The [FreeNAS™ website](#) contains links to all of the available documentation, support, and social media resources. Major announcements are also posted to the main page.

Users are welcome to network on the FreeNAS™ social media sites:

- [LinkedIn](#)
- [Google+](#)
- [Facebook](#)

A [twitter feed](#) is also available.

## 10.2 Trac Database

FreeNAS™ 8 uses a [trac database](#) where you can view existing support tickets to see if your issue has already been reported or create new tickets for unreported issues. You do not need to create a login account in order to view existing tickets, but you will need to use the Register link if you wish to create a ticket. See [section 11.2 Submit Bug Reports](#) if you wish to create a support ticket.

## 10.3 IRC

If you wish to ask a question in “real time”, you can try the #freenas channel on IRC Freenode. Depending upon the time of day (and your time zone), a FreeNAS™ developer or other FreeNAS™ users may be available to assist you. If you don't get an answer right away, remain on the channel as other users tend to read the channel history in order to answer questions as they are able to.

If you don't have an IRC chat client, you can use the [FreeNAS™ browser-based client](#).

To get the most out of the IRC channel, keep the following points in mind:

- don't ask "can anyone help me?"; instead, just ask your question. If someone knows the answer, they will try to assist you.
- don't ask a question and then leave. Users who know the answer can't help you if you disappear.
- don't take it personally if no one answers or demand that someone answers your question. Maybe no one who knows the answer is available, maybe your question is really hard, or maybe it is a question that has already been answered many times in the other support resources. Try asking again in a few hours or research the other resources to see if you've missed anything.
- Don't post error messages in the channel as the IRC software will probably kick you out. Instead, use a pasting service such as [pastebin](#) and refer to the URL on channel. If you prefer to paste an image of your error, you can upload it to a temporary screenshot hosting service such

as [Upload Screenshot](#) and post the URL to your uploaded image.

## 10.4 Mailing Lists

Several FreeNAS™ mailing lists are available which allow users and developers to ask and answer questions related to the topic of the mailing list. To post an email to a list, you will need to subscribe to it first. Each mailing list is archived, allowing you to browse for information by date, thread name, or author.

The following mailing lists are available:

- [freenas-announce](#): This is a low-volume, read-only list where major milestones, such as new releases, are announced.
- [freenas-commit](#): This is a read-only list. As code changes in the FreeNAS™ repository, the commit message is automatically sent to this list.
- [freenas-devel](#): FreeNAS™ developers are subscribed to this list. Technical questions about the current FreeNAS™ release can be posted here.
- [freenas-docs](#): This list is for discussion regarding [FreeNAS™ documentation](#).
- [freenas-testing](#): FreeNAS™ developers are subscribed to this list. Technical questions about the upcoming FreeNAS™ release and feedback on testing snapshots can be posted here.
- [freenas-translations](#): This list is for discussion regarding [FreeNAS™ localization](#) and translating FreeNAS™ documentation.

Archives of the mailing lists are available from [Gmane](#) which allows you to read the archives in various formats (blog style, news reader style) and to subscribe to RSS feeds for the lists.

## 10.5 Forums

Another information source for FreeNAS™ is the [Forums](#). Forums contain user-contributed tips and guides which have been categorized, making it an ideal resource if you wish to learn more about a certain aspect of FreeNAS™. A searchbar is included should you wish to search by keyword; alternately, you can click a category to browse through the threads that exist for that topic.

The following categories are available under **Help and Support**:

- [FreeNAS™ 4 N00bs](#): post here if you are new to FreeNAS™ and are unsure which category best matches your question.
- [Feature Requests](#): for the discussion of upcoming features and to request features not listed on the Roadmap.
- [Bug Reporting](#): do you think you have found a bug in FreeNAS™ and want to discuss it before creating a support ticket?
- [Hardware](#): for the discussion of hardware and tips for getting the most out of your hardware.
- [User Authentication](#): LDAP and Active Directory.
- [Sharing](#): AFP, CIFS, NFS, and iSCSI.

- [Storage](#): replication, snapshots, volumes, and ZFS.
- [Networking](#): networking hardware, performance, link aggregation, VLANs, DDNS, FTP, SNMP, SSH, and TFTP.
- [Installation](#): installing help or advice before performing the installation.

The following categories are available under **Development**:

- [FreeNAS™](#): general development discussion.
- [nanobsd](#): the embedded operating system FreeNAS™ is based upon.
- [Django](#): the web framework used by the FreeNAS™ graphical administrative interface.
- [Dojo Toolkit](#): the javascript toolkit used to create widgets and handle client side processing.

The following categories are available under **How-To Guides**:

- [Hacking](#): undocumented tricks for getting the most out of your FreeNAS™ system.
- [Installation](#): specific installation scenarios (hardware and/or software).
- [Configuration](#): specific configuration scenarios (e.g. software or client configuration).
- [Hardware](#): instructions for setting up specific hardware.

The following categories are available under **Community Forum**:

- [Off-topic](#): want to discuss something of interest to FreeNAS™ users but which is not necessarily related to FreeNAS™? This is your place.
- [Resources](#): blogs, reviews, and other sources of FreeNAS™ information not listed at freenas.org.
- [Introductions](#): FreeNAS™ Community meet 'n greet - introduce yourself and let us know who we are chatting with.

The following language-specific categories are available under **International**, allowing FreeNAS™ users to interact with each other in their native language:

- [German - Deutsch](#)
- [French - Francais](#)
- [Italian - Italiano](#)
- [Spanish - Espanol](#)

If you wish to ask a question on the forum, you will need to click the Register link to create an account and login using that account. When asking a question on the forum, it is important that you:

- first check to see if the question has already been asked. If you find a similar question, don't create a new thread. Instead use the "Reply to Thread" button to add your comments to the existing thread.
- review the available categories to see which one is most closely related to your question. Click on that category and use the "Post New Thread" button to open the editor. After typing your post and before you click the "Submit New Thread" button, make sure the "Subscribe to this thread

and notify me of changes" box is checked. That way you will be notified whenever anyone answers your question.

## 10.6 Instructional Videos

A series of instructional videos is being created for FreeNAS™ 8.x. The videos that are available so far are:

- [How to Install FreeNAS™ 8](#)
- [FreeNAS™ System Configuration Overview](#)
- [FreeNAS™ 8: Volumes Overview](#)
- [FreeNAS™ 8: Shares Overview](#)
- [FreeNAS™: Network Configuration Overview](#)
- [FreeNAS™: Active Directory](#)
- [FreeNAS™ 8: iSCSI In-depth](#)
- [FreeNAS™ 8: All in One](#)
- [FreeNAS™ 8: LAGG and VLAN](#)

The [Too Smart Guys](#) show also has a series of videos:

- [Building a FreeNAS 8 Box - Part 1 Hardware](#)
- [FreeNAS 8 - Build and Install](#)
- [FreeNAS 8 EP3 Configuration](#)

## 10.7 Professional Support

In addition to the freely available community resources, iXsystems offers professional support packages. iXsystems' development team works hard to improve new and current versions of FreeNAS™, providing them with the insight to provide expert FreeNAS™ support and consultation services. Their Professional Services team can also configure your FreeNAS™ hardware and software to deliver the highest levels of performance, stability, and security. See the [FreeNAS™ Professional Support](#) page to request a quote.

## 10.8 FAQs

This section contains some of the questions which are asked most often on the FreeNAS™ IRC channel. Additional FAQs can be found in this [forum post](#).

### 10.8.1 Can a RAID-Z array be expanded? For example, if I start off with a 8x2TB RAID-Z2 array can I add more drives to it in the future?

**A.** You can add drives to a volume, but not to a RAIDZ group. For example, if your volume is a 3 drive RAIDZ, you can add another 3 drive RAIDZ in the future, giving you a RAIDZ+0. But you can't change it to a 4 drive RAIDZ. This a limitation/feature of ZFS.

**10.8.2 Is there a command to force FreeBSD to scan for new disks? I'm trying to add some disks to my array using the hot-swappable bays and a 3ware SATA card. The drives go in fine and light up, but the operating system can't see them.**

**A.** Use the command:

```
tw_cli /c0 rescan
```

Then you use the drives to create units and export them to the operating system. When finished, run **camcontrol rescan all** and they will show up in the GUI.

**10.8.3 If my hardware/motherboard dies, can I rebuild with new/different hardware and still import/read the data from my disks? What about my datasets?**

**A.** Yes, as long as you aren't using hardware RAID and let ZFS handle the RAID, A dataset is basically a folder/directory that lives on your volume with your other files, but which has a separate mount point, such as */mnt/your-pool/dataset\_1*.

**10.8.4 How do I replace a bad drive?**

**A.** It is recommended that you first upgrade to latest version of [8.0.3](#) to make sure that your system is not effected by previously known bugs. You will also need access to the FreeNAS™ system to replace the hard drive and to run some commands from the FreeNAS™ console.

If you are replacing a disk that is a member of a RAIDZ1 or RAIDZ2:

1. Determine the device name and UUID of the disk that needs to be replaced in Storage -> Volumes -> View all Volumes -> View Disks icon for effected volume.
2. Shut down the system, pull out the failed drive, and replace it with a new disk of the same size or larger into the same port.
3. Power-on the system. At this point the RAIDZ will be in a DEGRADED state and the disk will be listed as Unavailable.
4. From the command line type **zpool replace tank ada7** where **tank** represents the pool name and **ada7** represents the device name.
5. The pool will begin re-silvering. This can take a *long time* (many hours); be patient and let it finish. You can check the status of the resilvering with **zpool status -v**. Once the resilvering finishes, **zpool status -v** will still say DEGRADED.
6. Type the command **zpool detach tank /dev/ada7/old**, replacing **tank** and **ada7** with your pool name and device name. Check the status again and the DEGRADED and */dev/ada7/old* should be gone and the pool state should be ONLINE.
7. Type the command **zpool export tank**. This will prepare the specified pool for an auto-import of the disk.
8. From the GUI go to: Storage -> Volumes -> Auto Import. Your disk should now show in the drop-down menu.
9. Should the disk not appear in the drop-down menu, make sure that you are running the latest version of FreeNAS™ upgrade if you are not. If you are running the latest FreeNAS™, try

backing up your configuration from System -> Settings -> Config -> Save Config. Then, reset the configuration to the factory defaults using the Factory Restore button, and try the auto-import again. Once your disk is imported, you can return to your saved configuration using the Upload Config button.

#### 10.8.5 Can I share files from my external USB drive?

A. No, at this time the GUI does not support this. This should be fixed in a later version.

#### 10.8.6 Can I mount my MAC formatted drive?

A. No, at this time FreeNAS™ and FreeBSD do not support mounting HFS/HFS+ filesystems.

#### 10.8.7 How do I get to the command line /CLI/shell?

A. There are 2 ways: from the console (the screen you see when you boot), and using SSH.

To use the console, you will need access to the keyboard connected to FreeNAS™. Select option "9) Shell" from the menu shown in Figure 2.4a in [section 2.4 Initial Setup](#). To return to the console menu from the shell, type **exit**.

To access the FreeNAS™ system using SSH, you will need to enable the SSH service in Control Services. You will also need a [client program](#) to make the connection. When connecting, use the IP address of the FreeNAS™ system and the username *admin*. If you need to gain root privileges during the session type **su**.

#### 10.8.8 Does FreeNAS support 4k sector drives? How do I check if it is configured?

A. Yes. FreeNAS detects and uses 4K sectors automatically.

From the command line, type these command to check if you have 512 or 4k sectors configured:

```
zpool set cachefile=/data/zfs/zpool.cache tank (change tank to your pool name)
zdb -U /data/zfs/zpool.cache | grep ashift
```

If the answer = 9, you have 512 byte sectors. If the answer = 12, you have 4k byte sectors.

Any hard drive produced after January 1, 2011 should be a 4K Advanced Format drive, though some drives retain backwards compatibility by performing 512 byte emulation. FreeNAS™ always uses 4K sector for ZFS if the underlying hard drive is advanced format in order to get maximum performance. For UFS, the format always uses 4K sectors.

When you create your volumes, you can optionally check the box to "Force 4096 bytes sector size". This will not improve performance on 512-byte sector hard drives but could be helpful in a RAIDZ that also contains advanced format drives.

#### 10.8.9 My network transfer speeds are very slow, what is wrong?

A. You need to determine whether the bottleneck is your LAN, your disks/array/controller, not enough RAM, your CPU load, a misconfiguration, the type of share in use, or that some tuning is required.

- if you're using a 10-100Mb/s wired router/switch you should get somewhere around 11-12MB/s
- if you're transferring across the Internet, your speed will only be as fast as your slowest link
- if you're using a Gig interface, check that it is properly enabled on both the switch and the FreeNAS™ system. To check the FreeNAS™ system, run this command at the console:

```
ifconfig -a grep media
```

If it is not showing at 1000Mb/s, add the following line to the Options field of the interface's settings:

```
media 1000baseTX mediaopt full-duplex
```

### 10.8.10 Why do changes I make at the command line to config files or settings disappear after a reboot?

A. FreeNAS™ is booted from a compressed filesystem and the configuration that is stored in a database is loaded into RAM. Any changes made at the command line do not get added to the configuration database. While you can make changes persist using the tips in this [forum post](#), those changes won't survive an upgrade and it is not recommended to manually add command line edits to the database. Instead, if the functionality you desire is not possible through the GUI, go to [support.freenas.org](http://support.freenas.org) and search to see if a feature request to add that functionality already exists. If there is no existing ticket, create a ticket describing the needed functionality.

## Section 4: Contributing to FreeNAS™

### 11 How to Get Involved

As an open source community, FreeNAS™ relies on the input and expertise of its users to help improve FreeNAS™. When you take some time to assist the community, your contributions benefit everyone who uses FreeNAS™.

This section describes some areas of participation to get you started. It is by no means an exhaustive list. If you have an idea that you think would benefit the FreeNAS™ community, bring it up on one of the resources mentioned in [section 10 FreeNAS™ Support Resources](#).

This section demonstrates how you can:

- [Assist with Localization](#)
- [Submit Bug Reports](#)
- [Test Upcoming Versions](#)

#### 11.1 Assist with Localization

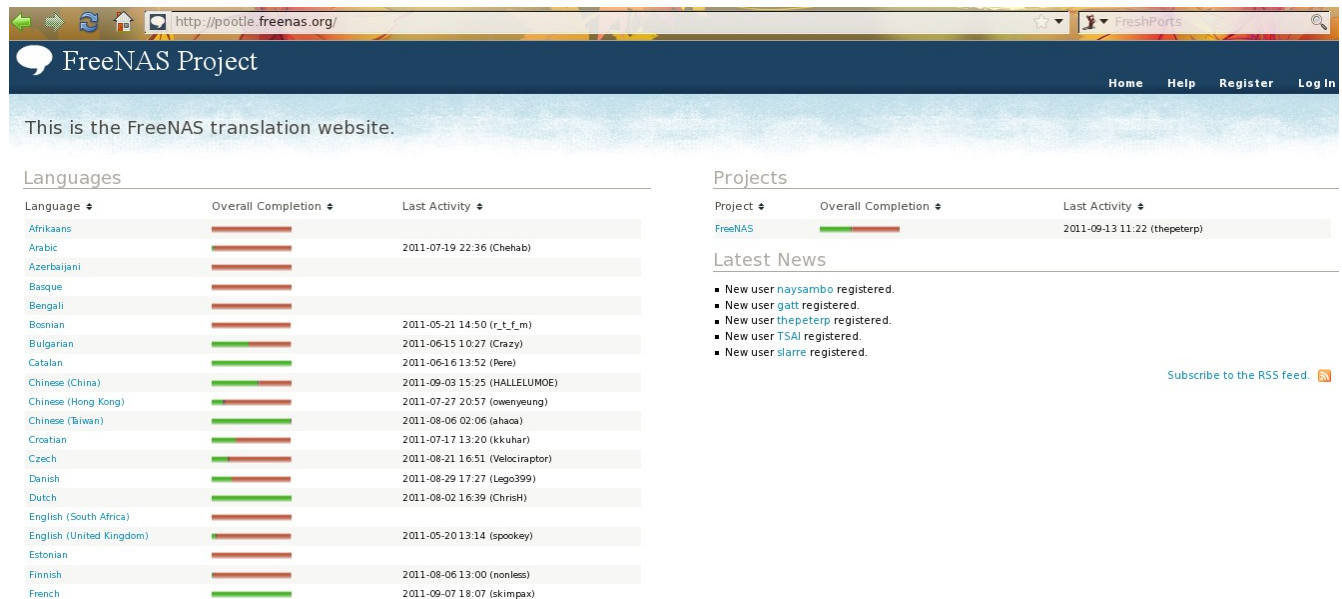
FreeNAS™ uses [Pootle](#), an open source application, for managing the localization of the menu screens used by the FreeNAS™ graphical administrative interface. Pootle makes it easy to find out the localization status of your native language and to translate the text for any menus that have not been localized yet. By providing a web editor and commenting system, Pootle allows translators to spend their time making and reviewing translations rather than learning how to use a translation submission



tool.

To see the status of a localization, open up the [FreeNAS™ Translation System](http://pootle.freenas.org) in your browser, as seen in Figure 11.1a:

**Figure 11.1a: FreeNAS™ Localization System**



The localizations FreeNAS™ users have requested are listed alphabetically on the left. If your language is missing and you would like to help in its translation, send an email to the [translations mailing list](#) so it can be added.

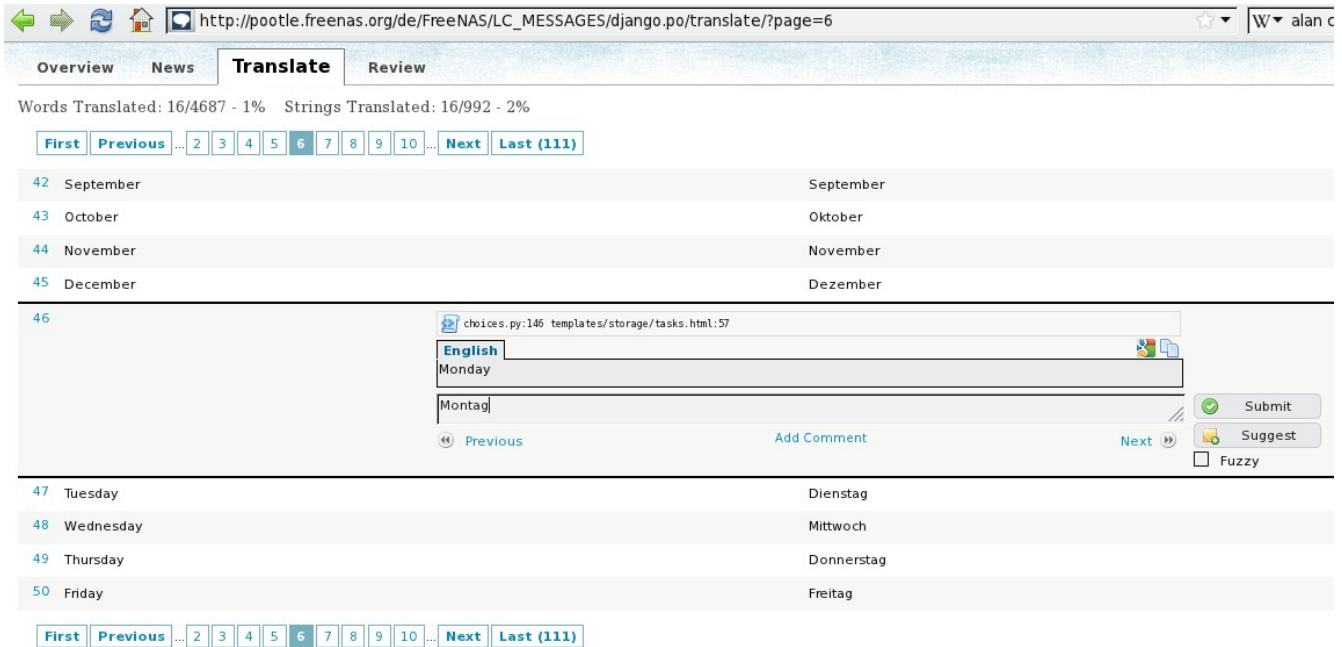
The green bar in the Overall Completion column indicates the percentage of FreeNAS™ menus that have been localized. If a language is not at 100%, it means that the menus that currently aren't translated will appear in English instead of in that language.

If you wish to help localize your language, you should first join the [translations mailing list](#) and introduce yourself and which language(s) you can assist with. This will allow you to meet other volunteers as well as keep abreast of any notices or updates that may effect the translations. You will also need to click on the Register link in order to create a Pootle login account.

The first time you log into the FreeNAS™ Pootle interface, you'll be prompted to select your language so that you can access that language's translation whenever you login. Alternately, you can click the Home link to see the status of all of the languages. To work on a translation, click the link for the language -> click the FreeNAS™ link for the project -> click the link for LC\_MESSAGES -> and click the link for django.po. Every text line available in the GUI menu screens has been assigned a string number. If you click the number, an editor will open where you can translate the text. In the example shown in Figure 11.1b, a user has selected string number 46 in the German translation; the other strings in the screenshot have already been translated:



**Figure 11.1b: Using the Pootle Interface to Edit a Translation String**



Simply type in the translated text and click the Submit button to save your change.

## 11.2 Submit Bug Reports

FreeNAS™ uses [Trac](#), an open source bug reporting system, to manage bug reports and feature requests submitted by users. You can search for existing bugs and submit a bug report at [support.freenas.org](http://support.freenas.org).

If you find a bug while using FreeNAS™ or if you would like to request a feature in an upcoming version, take the time to research your bug/feature first, before submitting your bug report. This is so that you don't end up duplicating an existing report and to ensure that your report contains the information that the developers need in order to implement the fix or the feature.

Before submitting a bug report, perform the following steps:

- determine if you are running the latest version of FreeNAS™ 8.x. FreeNAS™ developers tend to fix bugs rapidly and new features are being implemented as 8.x matures. If you are not running the latest version, it is quite likely that the bug has already been fixed or the missing feature has been implemented. If this is the case, your best course of action is to backup your data and configuration and perform an upgrade to the latest version. Note that FreeNAS™ will stabilize at version 8.2 and that the most recent version may be labelled as a beta or an RC; it will still be considered more stable than the release before it.
- if you are running the latest version, use the search feature at [support.freenas.org](http://support.freenas.org) to see if a similar report/request already exists. If one does, do not create another ticket. Instead, add a comment to the existing ticket if you have additional information to add.

If a similar report does not already exist, keep the following points in mind when you create your bug report or feature request:

- you will need to register for an account, confirm you registration email address, and be logged in before you can create a new ticket.
- in the Summary section shown in Figure 11.2a, include descriptive keywords that describe your problem or feature request. This is useful for other users who search for a similar problem. You can also include a comma separated list of keywords in the Keywords section.
- in the Description section, describe the problem, how to recreate it, and include the text of any error messages. If you are requesting a feature, describe the benefit provided by the feature and, if applicable, provide examples of other products that use that feature or the URL of the homepage for the software. If you would like to include a screenshot of your configuration or error, check the "I have files to attach to this ticket" box.
- under Type, select defect if it is a bug report or enhancement if it is a feature request.
- for bug reports, be sure to select the version of FreeNAS™ that you are using.
- press the Preview button to read through your ticket before submitting it. Make sure it includes all of the information that someone else would need to understand your problem or request. Once you are satisfied with your ticket, click the Create Ticket button to submit it.
- if you get stuck in how to fill out a field in the ticket, the [TracTickets](#) link at the bottom of the ticket creation page has several examples.

**Figure 11.2a: Creating a New Ticket**

The screenshot shows the 'Create New Ticket' page on the FreeNAS support site. The browser's address bar displays 'https://support.freenas.org/newticket'. The page features a navigation menu with links for Wiki, Timeline, Roadmap, Browse Source, View Tickets, and New Ticket. The main form is titled 'Create New Ticket' and is divided into several sections:

- Properties:**
  - Summary:** A text input field.
  - Description:** A rich text editor with a toolbar and a note: 'You may use WikiFormatting here.'
  - Type:** A dropdown menu set to 'defect'.
  - Priority:** A dropdown menu set to 'major'.
  - Milestone:** A dropdown menu.
  - Component:** A dropdown menu set to 'Backend'.
  - Version:** A dropdown menu set to '8.0-RELEASE'.
  - Keywords:** A text input field.
  - Owner:** A text input field.
  - Cc:** A text input field.
- Attachments:** A checkbox labeled 'I have files to attach to this ticket'.
- Buttons:** 'Preview' and 'Create ticket' buttons.

## 11.3 Test Upcoming Versions

### 11.3.1 Upcoming Version 8.2

A release date has not been set yet for 8.2, though it is expected to be released by the end of Q1, 2012.

Prior to 8.2 release, there will be a beta period where testing snapshots will be announced on the FreeNAS™ website, blog, and social media sites every week or so. This beta period is meant to provide users an opportunity to test the upcoming release and to provide feedback on bugs and errors so that they can be fixed prior to release. Feedback can be sent to the [Freenas-testing mailing list](#).

### 11.3.2 Testing a Nightly Snapshot

Changes to FreeNAS™ occur daily as developers address the bugs and enhancement requests reported by FreeNAS™ users. A testing version that incorporates these changes is automatically built daily and is available for download as a [nightly release](#).

If you wish to install or upgrade to the testing version of FreeNAS™ (i.e. the version that addresses all fixed bugs up to today's date) or you need to upgrade to a version that incorporates a fix you are waiting for, you can download the latest nightly version.

**NOTE:** it is possible that a recently implemented change will not work as expected or will break something else. If you experience this, take the time to add a comment to the applicable support ticket so that the developers can address the problem.

**DANGER!** upgrading from a nightly snapshot to an RC or a RELEASE *is not supported!* . Be wary of installing a nightly in a production environment and be sure to backup your configuration before attempting a full install of a later RC or RELEASE.

Nightly builds are available as ISO, GUI upgrade, or Full install images. If you are upgrading to a nightly from an earlier version of FreeNAS™ 8.x, see the section on [Upgrading FreeNAS™](#) for instructions on how to upgrade.

### 11.3.3 Rolling Your Own Testing Snapshot

Users who wish to test 8.2 prior to the testing period can download the latest source from the svn repository and generate their own ISO for testing purposes.

**NOTE:** 8.2 is currently in alpha phase and some of its new features are still broken or not fully implemented. Expect to find bugs. Do not use in a production environment! It is recommended that you read the [README](#) first so that you are aware of any gotchas and currently known limitations.

If you wish to build your own testing snapshot, you will need to install [FreeBSD 8.2](#) in a virtual environment or on a test system. If you are using a virtual environment, a 64-bit system with at least 4 GB of RAM is recommended. Download the FreeBSD version (i386 or amd64) that matches the architecture that you wish to build and when prompted to choose your distribution set during the installation, select the *Minimal* install option.

After booting into the newly installed FreeBSD system, become the superuser and run the following commands. First, install the software you'll need and refresh your path so it is aware of the new binaries:

```
pkg_add -r subversion
pkg_add -r nano
pkg_add -r cdrtools
rehash
```

You're now ready to download FreeNAS™ source:

```
cd /usr/local
svn co https://freenas.svn.sourceforge.net/svnroot/freenas/trunk
cd trunk
setenv FREEBSD_CVSUP_HOST cvsup10.freebsd.org
```

If you wish to install extra software in your snapshot, you will need to increase the size of the NanoBSD image by editing *freenas-common*. The size of the image should be double the space that it needs as the image will be formatted with two same-size partitions. This is to allow for upgrades as one partition contains the new running image and the other partition contains a copy of the backup image. When editing *freenas-common*, search for this line:

```
FlashDevice generic 1g
```

and edit it to the size you'll need. Make sure that you have a memory stick that can hold the specified size. You're now ready to build the image:

```
sh build/do_build.sh
sh build/create_iso.sh
```

Once these commands complete, you will have an image in *obj.yyyy/FreeNAS—VVVV-XXXX-yyyy.full.xz* where:

- VVVV is the release branch version
- XXXX is the svn revision from the FreeNAS™ repo
- yyyy is either i386 or amd64 depending on your platform and what was provided via `$FREEENAS_ARCH` on the command line or in an environment setting

This is a compressed raw disk image which needs to be decompressed and converted to your favorite virtual machine container format before use. There will also be a CD image called *obj.yyy/FreeNAS—VVVV-XXXX-yyyy.full.iso* that you can burn to disk and use to install or upgrade FreeNAS™.

Please see the README file for common workflows and tips.