
FreeNAS Documentation

Release 9.10.1-U2

iXsystems

Oct 23, 2016

CONTENTS

1	Introduction	3
1.1	What Is New in 9.10.1	3
1.2	What Has Changed Since 9.10.1	3
1.3	Hardware Recommendations	4
1.3.1	RAM	4
1.3.2	The Operating System Device	5
1.3.3	Storage Disks and Controllers	5
1.3.4	Network Interfaces	6
1.4	Getting Started with ZFS	6
2	Installing and Upgrading FreeNAS®	7
2.1	Getting FreeNAS®	7
2.2	Preparing the Media	8
2.2.1	On FreeBSD or Linux	8
2.2.2	On OS X	9
2.2.3	On Windows	9
2.3	Performing the Installation	10
2.4	Installation Troubleshooting	14
2.5	Upgrading	14
2.5.1	Caveats:	15
2.5.2	Initial Preparation	16
2.5.3	Upgrading Using the ISO	16
2.5.4	Upgrading From the GUI	18
2.5.5	If Something Goes Wrong	18
2.5.6	Upgrading a ZFS Pool	19
2.6	Virtualization	20
2.6.1	VirtualBox	20
2.6.2	VMware ESXi	24
3	Booting Into FreeNAS®	35
3.1	Initial Configuration Wizard	38
4	Account	45
4.1	Groups	45
4.2	Users	48
5	System	53
5.1	Information	53
5.2	General	53
5.3	Boot	57
5.3.1	Mirroring the Boot Device	60

5.4	Advanced	61
5.4.1	Autotune	64
5.5	Email	64
5.6	System Dataset	65
5.7	Tunables	66
5.8	Update	68
5.8.1	Preparing for Updates	68
5.8.2	Updates and Trains	69
5.8.3	Checking for Updates	70
5.8.4	Applying Updates	70
5.9	CAs	71
5.10	Certificates	73
5.11	Support	76
6	Tasks	79
6.1	Cron Jobs	79
6.2	Init/Shutdown Scripts	80
6.3	Rsync Tasks	81
6.3.1	Rsync Module Mode	84
6.3.2	Rsync over SSH Mode	84
6.4	S.M.A.R.T. Tests	87
7	Network	91
7.1	Global Configuration	91
7.2	Interfaces	92
7.3	IPMI	94
7.4	Link Aggregations	96
7.4.1	LACP, MPIO, NFS, and ESXi	97
7.4.2	Creating a Link Aggregation	97
7.5	Network Summary	101
7.6	Static Routes	101
7.7	VLANs	102
8	Storage	105
8.1	Volumes	105
8.1.1	Volume Manager	105
	Encryption	107
	Manual Setup	108
	Extending a ZFS Volume	109
8.1.2	Change Permissions	110
8.1.3	Create Dataset	111
	Deduplication	113
	Compression	114
8.1.4	Create zvol	114
8.1.5	Import Disk	115
8.1.6	Import Volume	116
	Importing an Encrypted Pool	117
8.1.7	View Disks	117
8.1.8	View Volumes	119
	Managing Encrypted Volumes	123
8.1.9	View Multipaths	124
8.1.10	Replacing a Failed Drive	124
	Replacing an Encrypted Drive	125
	Removing a Log or Cache Device	127

8.1.11	Replacing Drives to Grow a ZFS Pool	127
8.2	Periodic Snapshot Tasks	127
8.3	Replication Tasks	129
8.3.1	Configure PULL	129
8.3.2	Configure PUSH	130
8.3.3	Troubleshooting Replication	132
8.4	Scrubs	133
8.5	Snapshots	134
8.6	VMware-Snapshot	136
9	Directory Service	139
9.1	Active Directory	139
9.1.1	Troubleshooting Tips	143
9.1.2	If the System Will not Join the Domain	143
9.2	LDAP	144
9.3	NIS	146
9.4	NT4	147
9.5	Kerberos Realms	148
9.6	Kerberos Keytabs	148
9.7	Kerberos Settings	150
10	Sharing	151
10.1	Apple (AFP) Shares	152
10.1.1	Creating AFP Guest Shares	154
10.1.2	Creating Authenticated and Time Machine Shares	156
10.2	Unix (NFS) Shares	159
10.2.1	Example Configuration	163
10.2.2	Connecting to the Share	163
From BSD or Linux	164	
From Microsoft	164	
From Mac OS X	166	
10.2.3	Troubleshooting NFS	166
10.3	WebDAV Shares	168
10.4	Windows (SMB) Shares	169
10.4.1	Configuring Unauthenticated Access	172
10.4.2	Configuring Authenticated Access Without a Domain Controller	173
10.4.3	Configuring Shadow Copies	176
10.5	Block (iSCSI)	178
10.5.1	Target Global Configuration	179
10.5.2	Portals	180
10.5.3	Initiators	181
10.5.4	Authorized Accesses	182
10.5.5	Targets	184
10.5.6	Extents	184
10.5.7	Target/Extents	187
10.5.8	Connecting to iSCSI	187
10.5.9	Growing LUNs	188
Zvol Based LUN	188	
File Extent Based LUN	188	
11	Services Configuration	191
11.1	Control Services	191
11.2	AFP	193
11.2.1	Troubleshooting AFP	193

11.3	Domain Controller	195
11.4	Dynamic DNS	196
11.5	FTP	197
11.5.1	Anonymous FTP	198
11.5.2	FTP in chroot	200
11.5.3	Encrypting FTP	201
11.5.4	Troubleshooting FTP	202
11.6	iSCSI	202
11.7	LLDP	202
11.8	NFS	203
11.9	Rsync	204
11.9.1	Configure Rsyncd	204
11.9.2	Rsync Modules	205
11.10	S.M.A.R.T.	206
11.11	SMB	207
11.11.1	Troubleshooting SMB	210
11.12	SNMP	211
11.13	SSH	213
11.13.1	SCP Only	215
11.13.2	Troubleshooting SSH	215
11.14	TFTP	215
11.15	UPS	216
11.16	WebDAV	219
12	Plugins	221
12.1	Installing Plugins	221
12.2	Updating Plugins	225
12.3	Uploading Plugins	225
12.4	Deleting Plugins	226
12.5	Available Plugins	226
13	Jails	229
13.1	Jails Configuration	230
13.2	Adding Jails	232
13.2.1	Managing Jails	234
Accessing a Jail Using SSH	236	
Add Storage	236	
13.2.2	Installing FreeBSD Packages	239
13.2.3	Compiling FreeBSD Ports	240
13.2.4	Starting Installed Software	243
13.3	Using the phpVirtualBox Template	244
13.4	Managing Jail Templates	245
13.5	Using iohyve	248
14	Reporting	251
15	Display System Processes	253
16	Shell	255
17	Log Out	257
18	Reboot	259
19	Shutdown	261

20	Support Icon	263
21	Guide	265
22	Alert	267
23	Support Resources	269
23.1	Website and Social Media	269
23.2	Forums	269
23.3	IRC	271
23.4	Mailing Lists	271
23.5	Videos	272
23.6	Professional Support	272
24	Command Line Utilities	273
24.1	Iperf	273
24.2	Netperf	276
24.3	IOzone	277
24.4	arcstat	280
24.5	tw_cli	285
24.6	MegaCli	287
24.7	freenas-debug	287
24.8	tmux	287
24.9	Dmidecode	288
25	Contributing to FreeNAS®	289
25.1	Localize	289
26	ZFS Primer	291
27	Using the API	295
27.1	A Simple API Example	295
27.2	A More Complex Example	297
Index		301

FreeNAS® is © 2011-2016 iXsystems

FreeNAS® and the FreeNAS® logo are registered trademarks of iXsystems.

FreeBSD® is a registered trademark of the FreeBSD Foundation

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

Version 9.10.1-U2

Copyright © 2011-2016 iXsystems

This Guide covers the installation and use of FreeNAS® 9.10.1-U2.

The FreeNAS® User 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, read the instructions in the [README](#). IRC Freenode users are welcome to join the `#freenas` channel where you will find other FreeNAS® users.

The FreeNAS® User 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® and the FreeNAS® logo are registered trademarks of iXsystems.

Active Directory® is a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Apple, Mac and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries.

Avago is a trademark of Avago Technologies.

Broadcom is a trademark of Broadcom Corporation.

Chelsio® is a registered trademark of Chelsio Communications.

Cisco® is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Django® is a registered trademark of Django Software Foundation.

Facebook® is a registered trademark of Facebook Inc.

FreeBSD® and the FreeBSD® logo are registered trademarks of the FreeBSD Foundation®.

Fusion-io is a trademark or registered trademark of Fusion-io, Inc.

Intel, the Intel logo, Pentium Inside, and Pentium are trademarks of Intel Corporation in the U.S. and/or other countries.

LinkedIn® is a registered trademark of LinkedIn Corporation.

Linux® is a registered trademark of Linus Torvalds.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

Twitter is a trademark of Twitter, Inc. in the United States and other countries.

UNIX® is a registered trademark of The Open Group.

VirtualBox® is a registered trademark of Oracle.

VMware® is a registered trademark of VMware, Inc.

Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Windows® is a registered trademark of Microsoft Corporation in the United States and other countries.

Typographic Conventions

The FreeNAS® 9.10.1-U2 User Guide uses these typographic conventions:

Table 1: Text Format Examples

Item	Visual Example
Graphical elements: buttons, icons, fields, columns, and boxes	Click the <i>Import CA</i> button.
Menu selections	Select System → Information.
Commands	Use the scp command.
File names and volume and dataset names	Locate the /etc/rc.conf file.
Keyboard keys	Press the Enter key.
Important points	This is important.
Values entered into fields, or device names	Enter <i>127.0.0.1</i> in the address field.

INTRODUCTION

FreeNAS® is an embedded open source network-attached storage (NAS) operating system based on FreeBSD and released under a 2-clause BSD license. A NAS has an operating system optimized for file storage and sharing.

FreeNAS® provides a browser-based, graphical configuration interface. The built-in networking protocols provide storage access to multiple operating systems. A plugin system is provided for extending the built-in features by installing additional software.

1.1 What Is New in 9.10.1

- Added support for Avago/Broadcom Cutlass 12 Gbps 16-port controllers.
- When security certificates or SSH keys are generated, the fingerprints are logged in `/var/log/messages`, `var/log/debug.log`, and the console.
- Samba has been updated to version 4.3.11 ([changelog](#)).
- Dashes have been added to the characters allowed in jail names.
- Duplicate MAC addresses are not allowed in jails.

1.2 What Has Changed Since 9.10.1

FreeNAS® uses a “rolling release” model instead of point releases. The [Update](#) mechanism makes it easy to keep up-to-date with the latest security fixes, bug fixes, and new features. Some updates affect the user interface, so this section lists any functional changes that have occurred since 9.10.1 was released.

Note: The screenshots in this documentation assume that the system has been fully updated to the latest STABLE version of FreeNAS® 9.10.1. If a screen on your system is not the same as shown in this guide, make sure that all outstanding updates are applied.

- OpenSSL has been updated to [version 1.1.0b](#) which addresses a use-after-free security issue.
- Netatalk has been updated to [version 3.1.10](#).
- [Broadcom bge](#) revision 5717 C0 Ethernet cards are now supported.
- The mps driver for 6 G Avago SAS HBAs is version 21, which requires phase 20 firmware on the controller.
- Support for many old and obsolete 10/100 Ethernet cards has been removed.
- The *Auto* option has been removed from the *LUN ID* menu of Sharing → Block (iSCSI) → Associated Targets → Add Target/Extent .

- Deletion of in-use LUNs is not allowed.
- The CIFS service has been renamed to *SMB*.
- Allow customization of UPS shutdown command.
- *cmdwatch* is now included in the base operating system.
- *Midnight Commander* is now included in the base operating system.

1.3 Hardware Recommendations

FreeNAS® 9.10.1-U2 is based on FreeBSD 10.3 and supports the same hardware found in the [FreeBSD Hardware Compatibility List](#). Supported processors are listed in section [2.1 amd64](#). FreeNAS® is only available for 64-bit processors. This architecture is called *amd64* by AMD and *Intel 64* by Intel.

Note: FreeNAS® boots from a GPT partition. This means that the system BIOS must be able to boot using either the legacy BIOS firmware interface or EFI.

Actual hardware requirements vary depending on the usage of the FreeNAS® system. This section provides some starter guidelines. The [FreeNAS® Hardware Forum](#) has performance tips from FreeNAS® users and is a place to post questions regarding the hardware best suited to meet specific requirements. [Hardware Recommendations](#) gives detailed recommendations for system components, with the [FreeNAS® Quick Hardware Guide](#) providing short lists of components for various configurations. [Building, Burn-In, and Testing your FreeNAS® system](#) has detailed instructions on testing new hardware.

1.3.1 RAM

The best way to get the most out of a FreeNAS® system is to install as much RAM as possible. The recommended minimum is 8 GB of RAM. The more RAM, the better the performance, and the [FreeNAS® Forums](#) provide anecdotal evidence from users on how much performance is gained by adding more RAM.

Depending upon the use case, your system may require more RAM. Here are some general rules of thumb:

- To use Active Directory with many users, add an additional 2 GB of RAM for winbind's internal cache.
- When [Using the phpVirtualBox Template](#), increase the minimum RAM size by the amount of virtual memory configured for use in virtual machines. For example, if there will be two virtual machines, each with 4 GB of virtual memory, the system needs at least 16 GB of RAM.
- For iSCSI, install at least 16 GB of RAM if performance is not critical, or at least 32 GB of RAM if good performance is a requirement.
- When installing FreeNAS® on a headless system, disable the shared memory settings for the video card in the BIOS.
- To use ZFS deduplication, ensure the system has at least 5 GB of RAM per TB of storage to be deduplicated.

If the hardware supports it and the budget allows for it, install ECC RAM. While more expensive, ECC RAM is highly recommended as it prevents in-flight corruption of data before the error-correcting properties of ZFS come into play, thus providing consistency for the checksumming and parity calculations performed by ZFS. If you consider your data important, use ECC RAM. This [Case Study](#) describes the risks associated with memory corruption.

Unless the system has at least 8 GB of RAM, consider adding RAM before using FreeNAS® to store data. Many users expect FreeNAS® to function with less memory, just at reduced performance. The bottom line is that these minimums are based on feedback from many users. Requests for help in the forums or IRC are sometimes ignored when the

installed system does not have at least 8 GB of RAM because of the abundance of information that FreeNAS® may not behave properly with less memory.

1.3.2 The Operating System Device

The FreeNAS® operating system is installed to at least one device that is separate from the storage disks. The device can be a USB stick, SSD, compact flash, or DOM (Disk on Module). Installation to a hard drive is discouraged as that drive is then not available for data storage.

Note: To write the installation file to a USB stick, **two** USB ports are needed, each with an inserted USB device. One USB stick contains the installer. The other USB stick is the destination for the FreeNAS® installation. Take care to select the correct USB device for the FreeNAS® installation. It is **not** possible to install FreeNAS® onto the same USB stick containing the installer. After installation, remove the installer USB stick. It might also be necessary to adjust the BIOS configuration to boot from the new FreeNAS® USB stick.

When determining the type and size of the target device where FreeNAS® will be installed, keep these points in mind:

- the *bare minimum* size is 8 GB. This provides room for the operating system and several boot environments. Since each update creates a boot environment, this is the *recommended* minimum. 32 GB provides room for more boot environments.
- if you plan to make your own boot environments, budget about 1 GB of storage per boot environment. Consider deleting older boot environments after making sure they are no longer needed. Boot environments can be created and deleted using System → Boot .
- use quality, name-brand USB sticks, as ZFS will quickly reveal errors on cheap, poorly-made sticks.
- for a more reliable boot disk, use two identical devices and select them both during the installation. This will create a mirrored boot device.

1.3.3 Storage Disks and Controllers

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

FreeNAS® supports hot pluggable drives. Using this feature requires enabling AHCI in the BIOS.

Reliable disk alerting and immediate reporting of a failed drive can be obtained by using an HBA such as an Avago MegaRAID controller or a 3Ware twa-compatible controller.

Suggestions for testing disks before adding them to a RAID array can be found in this [forum post](#).

If the budget allows optimization of the disk subsystem, consider the read/write needs and RAID requirements:

- For 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 600 GB 15K SAS drives in a RAID 10 which would yield 1.8 TB of usable space, or eight 600 GB 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.

When high performance is a key requirement and budget permits, 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 card 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 card 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.

For 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, **it is not possible to format less than 3 GB of space with ZFS**. However, on a drive that is below the minimum recommended size, a fair amount of storage space is lost to swap: for example, on a 4 GB drive, 2 GB will be reserved for swap.

Users new to ZFS who are purchasing hardware should read through [ZFS Storage Pools Recommendations](#) first.

ZFS *vdevs*, groups of disks that act like a single device, can be created using disks of different sizes. However, the capacity available on each disk is limited to the same capacity as the smallest disk in the group. For example, a *vdev* with one 2 TB and two 4 TB disks will only be able to use 2 TB of space on each disk. In general, use disks that are the same size for the best space usage and performance.

1.3.4 Network Interfaces

The [Ethernet section](#) of the FreeBSD 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 when purchasing a new NIC. Realtek cards often perform poorly under CPU load as interfaces with these chipsets do not provide their own processors.

At a minimum, a GigE interface is recommended. While GigE interfaces and switches are affordable for home use, modern disks can easily saturate their 110 MB/s throughput. For higher network throughput, multiple GigE cards can be bonded together using the LACP type of [Link Aggregations](#). The Ethernet switch must support LACP, which means a more expensive managed switch is required.

When network performance is a requirement and there is some money to spend, use 10 GigE interfaces and a managed switch. Managed switches with support for LACP and jumbo frames are preferred, as both can be used to increase network throughput. Refer to the [10 Gig Networking Primer](#) for more information.

Note: At present, these are not supported: InfiniBand, FibreChannel over Ethernet, or wireless interfaces.

Both hardware and the type of shares can affect network performance. On the same hardware, SMB is slower than FTP or NFS because Samba is [single-threaded](#). So a fast CPU can help with SMB performance.

Wake on LAN (WOL) support depends on the FreeBSD driver for the interface. If the driver supports WOL, it can be enabled using [ifconfig\(8\)](#). To determine if WOL is supported on a particular interface, use the interface name with the following command. In this example, the capabilities line indicates that WOL is supported for the *re0* interface:

```
ifconfig -m re0
re0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=42098<VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM,WOL_MAGIC,VLAN_HWTSO>
    capabilities=5399b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM,TSO4,WOL_
    ↪UCAST,WOL_MCAST, WOL_MAGIC,VLAN_HWFILTER,VLAN_H_WTSO>
```

If WOL support is shown but not working for a particular interface, create a bug report using the instructions in [Support](#).

1.4 Getting Started with ZFS

Readers new to ZFS should take a moment to read the [ZFS Primer](#).

CHAPTER TWO

INSTALLING AND UPGRADING FREENAS®

Please note that the FreeNAS® operating system must be installed on a separate device from the drives which hold the storage data. In other words, with only one disk drive, the FreeNAS® graphical interface is available, but there is no place to store any data. And storing data is, after all, the whole point of a NAS system. Home users experimenting with FreeNAS® can install FreeNAS® on an inexpensive USB thumb drive and use the computer's disks for storage.

This section describes:

- *Getting FreeNAS®*
- *Preparing the Media*
- *Performing the Installation*
- *Installation Troubleshooting*
- *Upgrading*
- *Virtualization*

2.1 Getting FreeNAS®

The latest STABLE version of FreeNAS® 9.10.1-U2 can be downloaded from <http://download.freenas.org/>.

Note: FreeNAS® can only be installed on 64-bit hardware.

The download page contains these types of files:

- **.iso:** this is a bootable installer that can be written to either a CD or USB flash as described in *Preparing the Media*.
- **.GUI_Upgrade.txz:** this is a compressed firmware upgrade image. To upgrade FreeNAS®, download this file and see the section on *Upgrading*.

Each file has an associated `sha256.txt` file which should be used to verify the integrity of the downloaded file. The command 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`
- Windows or Mac users can install additional utilities like [HashCalc](#) or [HashTab](#)

The value produced by running the command must match the value shown in the `sha256.txt` file. Checksum values that do not match indicate a corrupted installer file that should not be used.

2.2 Preparing the Media

The FreeNAS® installer can run from either a CD or a USB memory stick.

Writing the `.iso` file to a CD requires CD burning utility.

The command used to burn the `.iso` file to a USB memory stick or Compact Flash card depends on the operating system. This section demonstrates utilities for several operating systems.

Note: To install from a USB stick to another USB stick, **two** USB ports are needed, each with an inserted USB device. One USB stick contains the installer. The other USB stick is the destination for the FreeNAS® installation. Take care to select the correct USB device for the FreeNAS® installation. It is **not** possible to install FreeNAS® onto the same USB stick containing the installer. After installation, remove the installer USB stick. It might also be necessary to adjust the BIOS configuration to boot from the new FreeNAS® USB stick.

Make sure that the boot device order in the BIOS is set to boot from the device containing the FreeNAS® installer media, then boot the system to start the installation.

2.2.1 On FreeBSD or Linux

On a FreeBSD or Linux system, the `dd` command can be used to write the `.iso` file to an inserted USB thumb drive or Compact Flash device. *Example: Writing the *.iso* file to a USB Thumb Drive* demonstrates writing the image to the first USB device (`/dev/da0`) on a FreeBSD system. Substitute the filename of the `.iso` file and the device name representing the device to write to on your system.

Warning: The `dd` command is very powerful and can destroy any existing data on the specified device. Make **absolutely sure** of the device name to write to and do not mistype the device name when using `dd`! If you are uncomfortable using this command, write the `.iso` file to a CD instead.

Writing the `.iso` file to a USB Thumb Drive

```
dd if=FreeNAS-9.10-RELEASE-x64.iso of=/dev/da0 bs=64k
6117+0 records in
6117+0 records out
400883712 bytes transferred in 88.706398 secs (4519220 bytes/sec)
```

When using the `dd` command:

- **if=** refers to the input file, or the name of the file to write to the device.
- **of=** refers to the output file; in this case, the device name of the flash card or removable USB drive. Note that USB device numbers are dynamic, and the target device might be `da1` or `da2` or another name depending on which devices are attached. Before attaching the target USB drive, use `ls /dev/da*`. Then attach the target USB drive, wait ten seconds, and run `ls /dev/da*` again to see the new device name and number of the target USB drive. On Linux, use `/dev/sdX`, where `X` refers to the letter of the USB device.
- **bs=** refers to the block size, the amount of data to write at a time. The larger 64K block size shown here helps speed up writes to the USB drive.

2.2.2 On OS X

Insert the USB thumb drive. In the Finder, go to Applications → Utilities → Disk Utility . Unmount any mounted partitions on the USB thumb drive. Check that the USB thumb drive has only one partition, or partition table errors will be shown on boot. If needed, use Disk Utility to set up one partition on the USB drive. Selecting *Free space* when creating the partition works fine.

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

```
diskutil list
/dev/disk0

#: TYPE NAME          SIZE      IDENTIFIER
0: GUID_partition_scheme *500.1 GB   disk0
1: EFI                 209.7 MB  disk0s1
2: Apple_HFS Macintosh HD 499.2 GB  disk0s2
3: Apple_Boot Recovery HD 650.0 MB  disk0s3

/dev/disk1
#: TYPE NAME          SIZE      IDENTIFIER
0: FDisk_partition_scheme *8.0 GB    disk1
1: DOS_FAT_32 UNTITLED     8.0 GB   disk1s1
```

This shows which devices are available to the system. Locate the target 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, unmount the USB stick, and use the **dd** command to write the image to the USB stick. In *Example: Using dd on an OS X System*, the USB thumb drive is `/dev/disk1`, which is first unmounted. The **dd** command uses `/dev/rdisk1` (note the extra *r*) to write to the raw device, which is faster. When running these commands, substitute the name of the installation file and the correct path to the USB thumb drive.

Example: Using dd on an OS X System

```
diskutil unmountDisk /dev/disk1
Unmount of all volumes on disk1 was successful

dd if=FreeNAS-9.10-RELEASE-x64.iso of=/dev/rdisk1 bs=64k
```

Note: If the error “Resource busy” is shown when the **dd** command is run, go to Applications → Utilities → Disk Utility , find the USB thumb drive, and click on its partitions to make sure all of them are unmounted. If the error “dd: /dev/disk1: Permission denied” is shown, run the **dd** command by typing **sudo dd if=FreeNAS-9.10-RELEASE-x64.iso of=/dev/rdisk1 bs=64k**. This will prompt for your password.

The **dd** command can take some minutes to complete. Wait until the prompt returns and a message is displayed with information about how long it took to write the image to the USB drive.

2.2.3 On Windows

Windows provides the USB/DVD Download Tool to create a USB bootable image from an `.iso` file. Follow [these instructions](#), but enter the name of the downloaded `.iso` into the *SOURCE FILE* box.

2.3 Performing the Installation

With the installation media inserted, boot the system from that media. The FreeNAS® installer GRUB menu is displayed as is shown in [Figure 2.1](#).

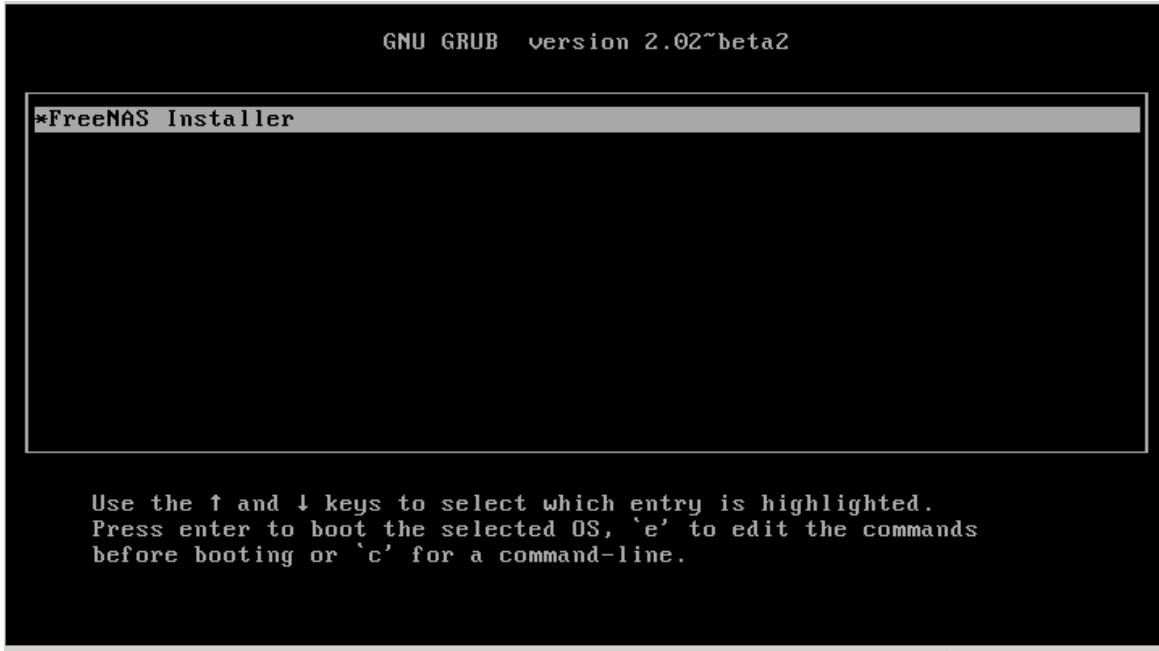


Fig. 2.1: Grub Menu

Note: If the installer does not boot, verify that the installation device is listed first in the boot order in the BIOS. When booting from a CD, some motherboards may require connecting the CD device to SATA0 (the first connector) to boot from CD. If the installer stalls during bootup, double-check the SHA256 hash of the .iso file. If the hash does not match, re-download the file. If the hash is correct, burn the CD again at a lower speed or write the file to a different USB stick.

Wait for the menu to time out or press `Enter` to boot into the installer. After the media boots, the console setup menu is displayed as shown in [Figure 2.2](#).

Press `Enter` to select the default option, *I Install/Upgrade*. The next menu, shown in [Figure 2.3](#), lists all available drives. This includes any inserted USB thumb drives, which have names beginning with *da*.

In this example, the user is performing a test installation using VirtualBox and has created a 16 GB virtual disk to hold the operating system.

Use the arrow keys to highlight the destination USB drive, SSD, DOM (Disk on Module), Compact Flash device, or virtual disk. Press the `spacebar` to select it. To mirror the boot device, move to the second device and press `spacebar` to select it also. After making these selections, press `Enter`. The warning shown in [Figure 2.4](#) is displayed, a reminder not to install the operating system on a drive that is meant for storage. Press `Enter` to continue on to the screen shown in [Figure 2.6](#).

Note: A minimum of 8 GB of space on the boot device is required. However, 32 GB is recommended to provide room for future additions and boot environments. When using mirrored boot devices, it is best to use devices of the

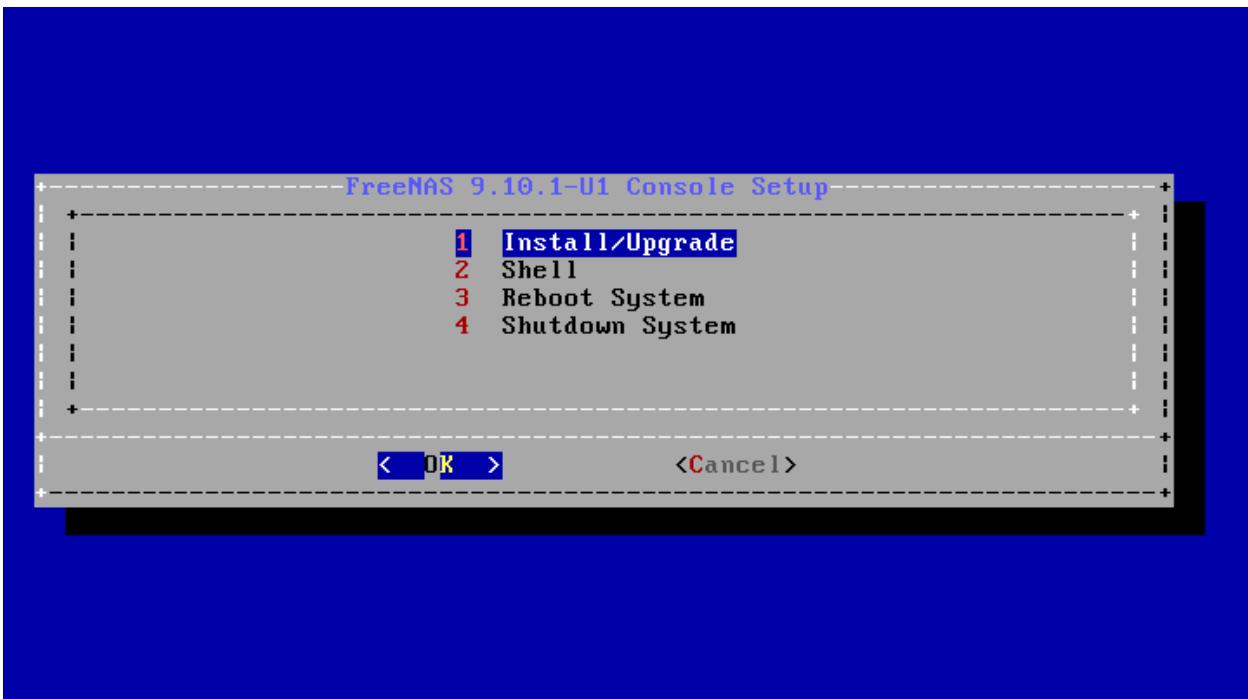


Fig. 2.2: Console Setup

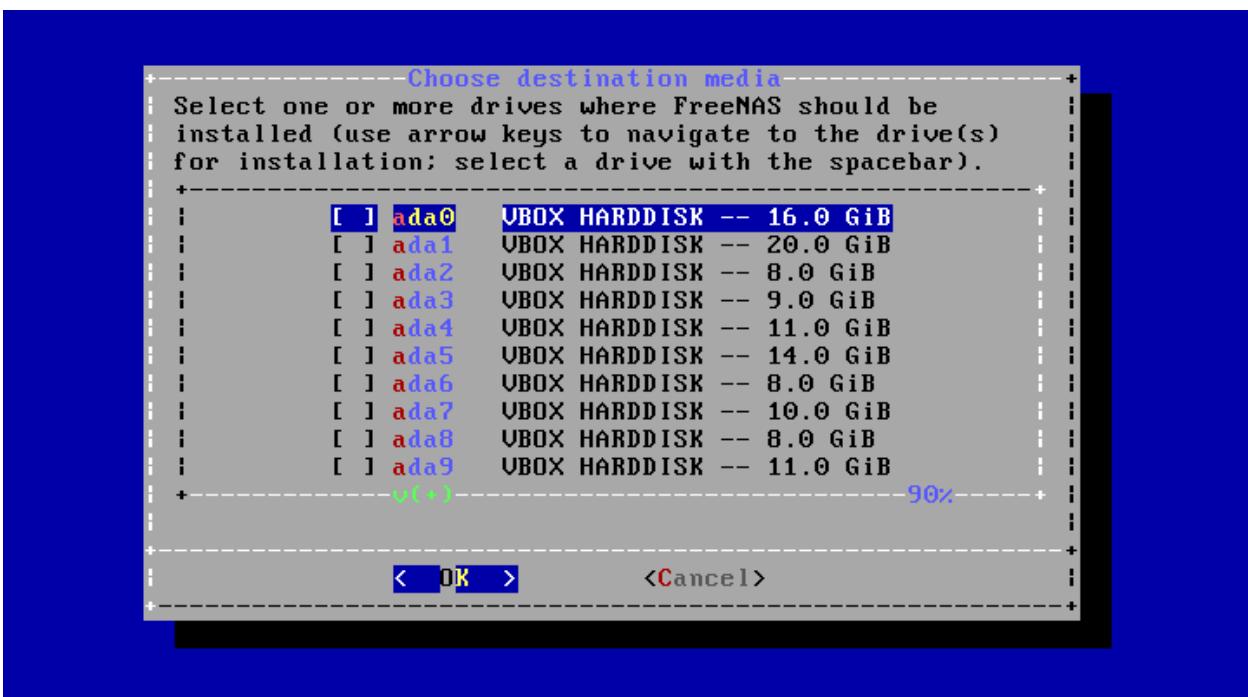


Fig. 2.3: Selecting the Install Drive

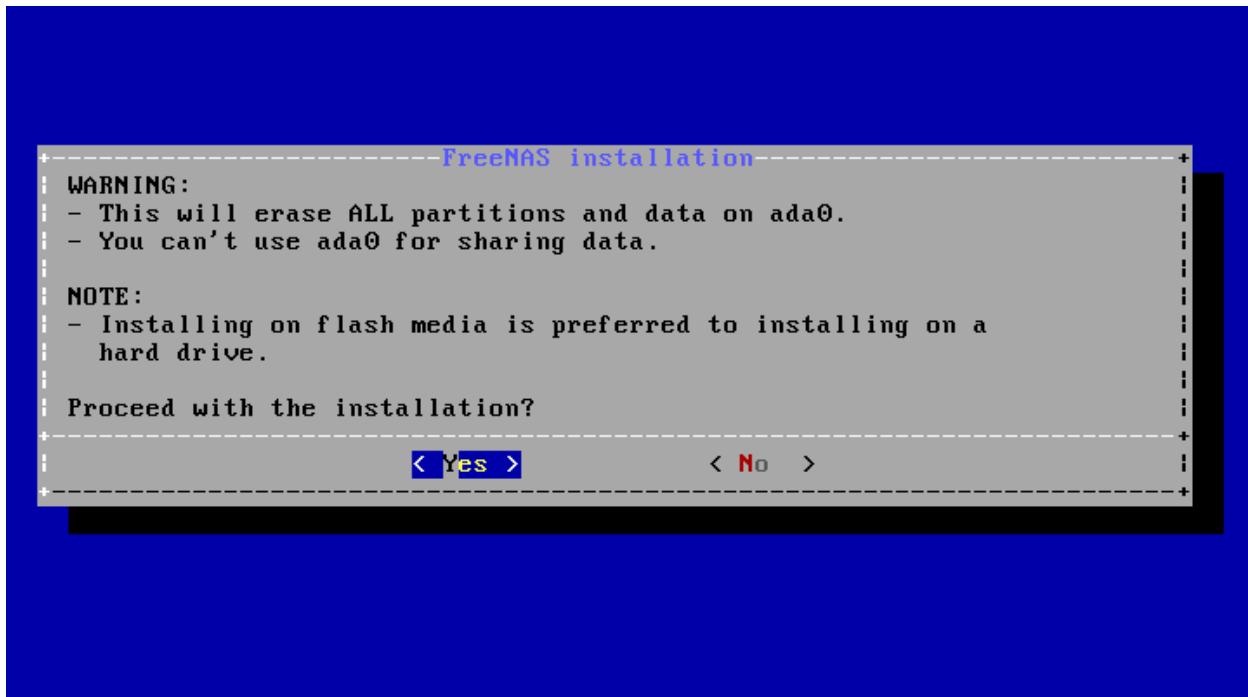


Fig. 2.4: Installation Warning

same size. If the device sizes are different, the mirror is limited to the size of the smaller device.

The installer recognizes existing installations of previous versions of FreeNAS® 8.x or 9.x. When an existing installation is present, the menu shown in [Figure 2.5](#) is displayed. To overwrite an existing installation, use the arrows to move to *Fresh Install* and press `Enter` twice to continue to the screen shown in [Figure 2.6](#).

The screen shown in [Figure 2.6](#) prompts for the *root* password which is used to log in to the administrative graphical interface.

Setting a password is mandatory and the password cannot be blank. Since this password provides access to the administrative GUI, it should be hard to guess. Enter the password, press the down arrow key, and confirm the password. Then press `Enter` to continue with the installation.

Note: For security reasons, the SSH service and *root* SSH logins are disabled by default. Unless these are set, the only way to access a shell as *root* is to gain physical access to the console menu or to access the web shell within the administrative GUI. This means that the FreeNAS® system should be kept physically secure and that the administrative GUI should be behind a properly configured firewall and protected by a secure password.

The message in [Figure 2.7](#) is shown after the installation is complete.

Press `Enter` to return to the first menu, shown in [Figure 2.1](#). Highlight *3 Reboot System* and press `Enter`. If booting from CD, remove the CDROM. As the system reboots, make sure that the device where FreeNAS® was installed is listed as the first boot entry in the BIOS so the system will boot from it. FreeNAS® boots into the *Console Setup* menu described in [Initial Configuration Wizard](#).

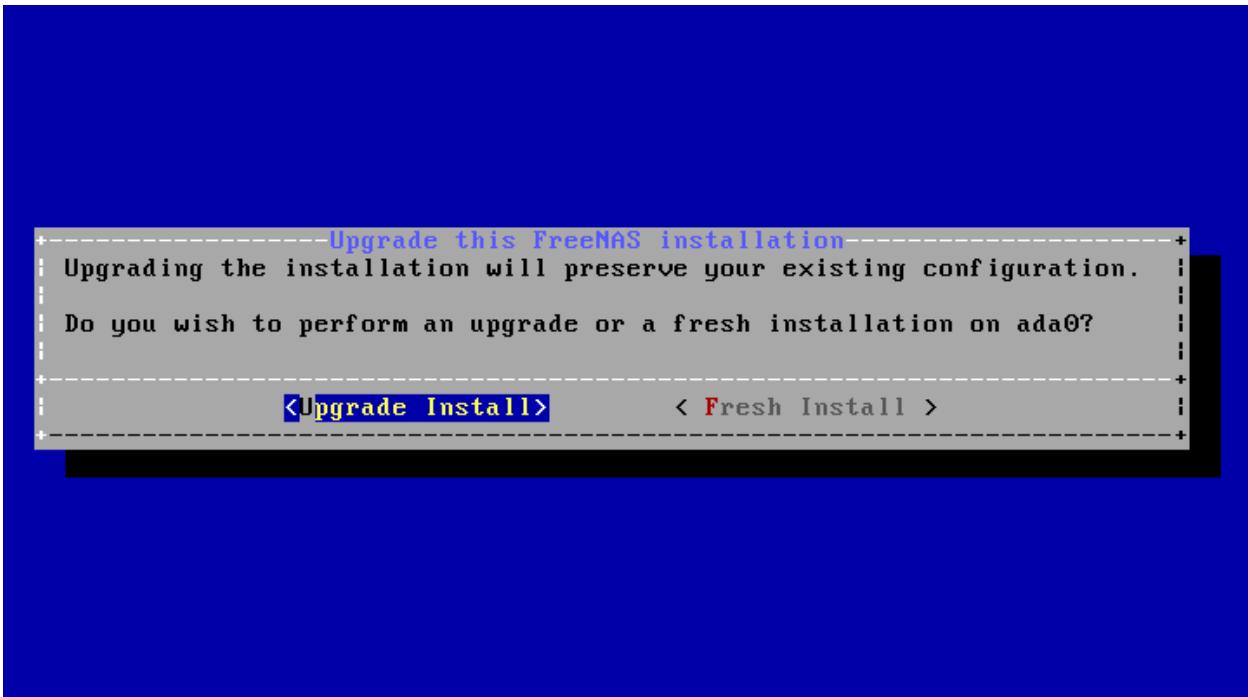


Fig. 2.5: Performing a Fresh Install

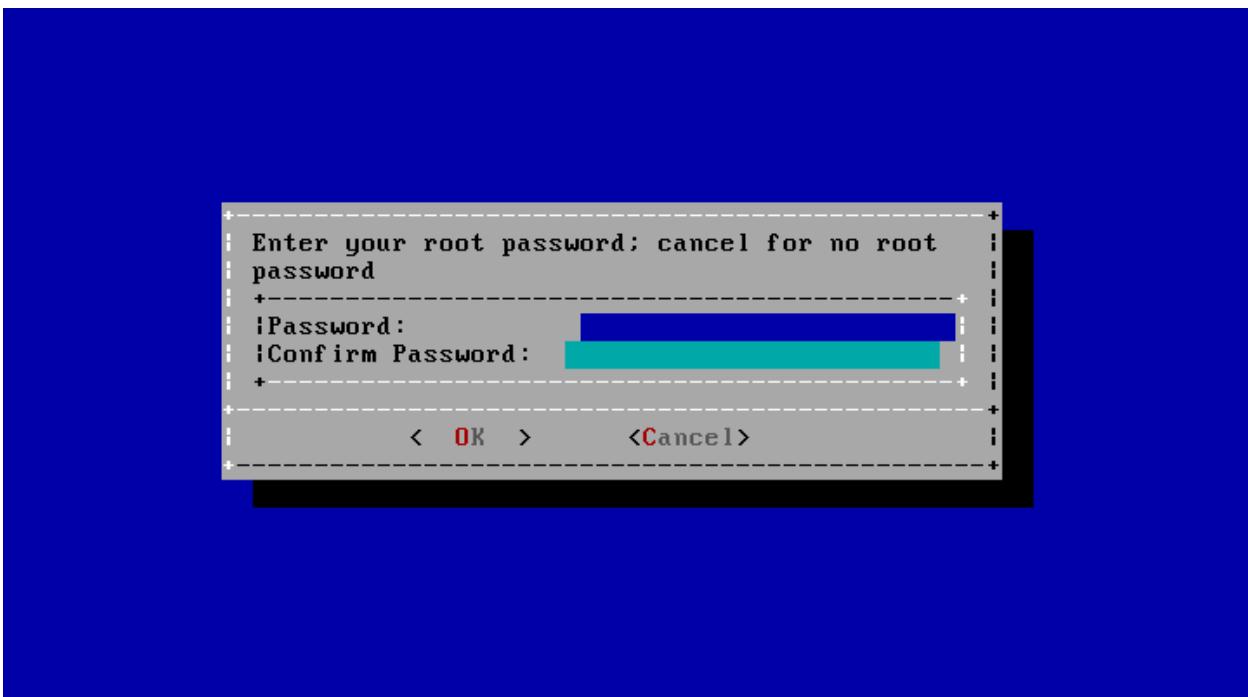


Fig. 2.6: Set the Root Password

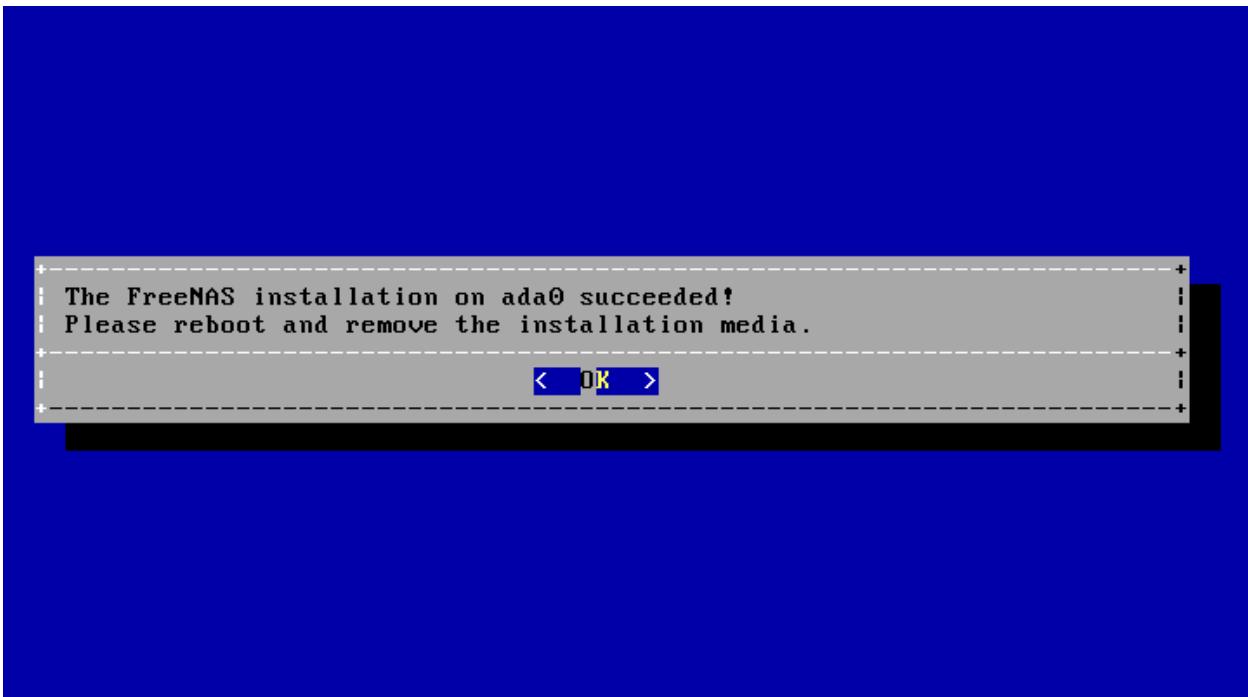


Fig. 2.7: Installation Complete

2.4 Installation Troubleshooting

If the system does not boot into FreeNAS®, there are several things that can be checked to resolve the situation.

Check the system BIOS and see if there is an option to change the USB emulation from CD/DVD/floppy to hard drive. If it still will not boot, check to see if the card/drive is UDMA compliant.

If the system BIOS does not support EFI with BIOS emulation, see if it has an option to boot using legacy BIOS mode.

When the system starts to boot but hangs with this repeated error message:

```
run_interrupt_driven_hooks: still waiting after 60 seconds for xpt_config
```

go into the system BIOS and look for an onboard device configuration for a 1394 Controller. If present, disable that device and try booting again.

If the system starts to boot but hangs at a *mountroot>* prompt, follow the instructions in [Workaround/Semi-Fix for Mountroot Issues with 9.3](#).

If the burned image fails to boot and the image was burned using a Windows system, wipe the USB stick before trying a second burn using a utility such as [Active@ KillDisk](#). Otherwise, the second burn attempt will fail as Windows does not understand the partition which was written from the image file. Be very careful to specify the correct USB stick when using a wipe utility!

2.5 Upgrading

FreeNAS® provides flexibility for keeping the operating system up-to-date:

1. Upgrades to major releases, for example from version 9.3 to 9.10, can still be performed using either an ISO or the graphical administrative interface. Unless the Release Notes for the new major release indicate that the current version requires an ISO upgrade, either upgrade method can be used.
2. Minor releases have been replaced with signed updates. This means that it is not necessary to wait for a minor release to update the system with a system update or newer versions of drivers and features. It is also no longer necessary to manually download an upgrade file and its associated checksum to update the system.
3. The updater automatically creates a boot environment, making updates a low-risk operation. Boot environments provide the option to return to the previous version of the operating system by rebooting the system and selecting the previous boot environment from the boot menu.

This section describes how to perform an upgrade from an earlier version of FreeNAS® to 9.10.1-U2. After 9.10.1-U2 has been installed, use the instructions in [Update](#) to keep the system updated.

2.5.1 Caveats:

Be aware of these caveats **before** attempting an upgrade to 9.10.1-U2:

- **Upgrades from FreeNAS® 0.7x are not supported.** The system has no way to import configuration settings from 0.7x versions of FreeNAS®. The configuration must be manually recreated. If supported, the FreeNAS® 0.7x volumes or disks must be manually imported.
- **Upgrades on 32-bit hardware are not supported.** However, if the system is currently running a 32-bit version of FreeNAS® **and** the hardware supports 64-bit, the system can be upgraded. Any archived reporting graphs will be lost during the upgrade.
- **UFS is no longer supported.** If your data currently resides on **one** UFS-formatted disk, you will need to create a ZFS volume using **other** disks after the upgrade, then use the instructions in [Import Disk](#) to mount the UFS-formatted disk to copy the data to the ZFS volume. With only one disk, back up its data to another system or media before the upgrade, format the disk as ZFS after the upgrade, then restore the backup. If your data currently resides on a UFS RAID of disks, you will not be able to import that data to the ZFS volume. Instead, back up that data before the upgrade, create a ZFS volume after the upgrade, then restore the data from backup.
- The initial configuration wizard will not recognize an encrypted ZFS pool. If your ZFS pool is GELI-encrypted and the [Initial Configuration Wizard](#) starts after the upgrade, cancel the wizard and use the instructions in [Importing an Encrypted Pool](#) to import the encrypted volume. You can then rerun the wizard afterwards if you wish to use it for post-configuration, and it will recognize that the volume has been imported and will not prompt to reformat the disks.
- **DO NOT upgrade the ZFS pool unless you are absolutely sure that you will never want to go back to the previous version.** For this reason, the update process will not automatically upgrade the ZFS pool, though the [Alert](#) system shows when newer feature flags are available for the pool. Unless you need a new feature flag, it is safe to leave the ZFS pool at its current version and uncheck the alert. If you do decide to upgrade the pool, you will not be able to boot into a previous version that does not support the newer feature flags.
- The *mps* driver for 6 G Avago SAS HBAs is version 21, which requires phase 20 firmware on the controller and the *mpr* driver for 12 G Avago SAS HBAs is version 13 which requires P12 firmware. It is recommended to upgrade the firmware before installing FreeNAS® or immediately after upgrading FreeNAS®, using the instructions in [Alert](#). Running older firmware can cause many woes, including the failure to probe all of the attached disks, which can lead to degraded or unavailable arrays. While you can mismatch your firmware version with a higher version and things will “probably still work”, there are no guarantees as that driver and firmware combination is untested.
- If you are upgrading from 9.3.x, read the [FAQ: Upgrading from 9.3 to 9.10](#) first.

2.5.2 Initial Preparation

Before upgrading the operating system, perform the following steps:

1. **Back up the FreeNAS® configuration** in System → General → Save Config.
2. If any volumes are encrypted, **make sure** that you have set the passphrase and have a copy of the encryption key and the latest recovery key. After the upgrade is complete, use the instructions in *Importing an Encrypted Pool* to import the encrypted volume.
3. Warn users that the FreeNAS® shares will be unavailable during the upgrade; you should schedule the upgrade for a time that will least impact users.
4. Stop all services in Services → Control Services.

2.5.3 Upgrading Using the ISO

To perform an upgrade using this method, [download](#) the .iso to the computer that will be used to prepare the installation media. Burn the downloaded .iso file to a CD or USB thumb drive using the instructions in [Preparing the Media](#).

Insert the prepared media into the system and boot from it. After the media finishes booting into the installation menu, press Enter to select the default option of *1 Install/Upgrade*. The installer presents a screen showing all available drives.

Warning: All drives are shown, including boot drives and storage drives. Only choose boot drives when upgrading. Choosing the wrong drives to upgrade or install will cause loss of data. If unsure about which drives contain the FreeNAS® operating system, reboot and remove the install media. In the FreeNAS® GUI, use System → Boot to identify the boot drives. More than one drive is shown when a mirror has been used.

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

The installer recognizes earlier version of FreeNAS® installed on the boot drive or drives and presents the message shown in [Figure 2.8](#).

Note: If you choose a *Fresh Install*, the backup of your configuration data must be restored using System → General → Upload Config after booting into the new operating system.

To perform an upgrade, press Enter to accept the default of *Upgrade Install*. Again, the installer will remind you that the operating system should be installed on a disk that is not used for storage. Press Enter to start the upgrade. The installer unpacks the new image and displays the menu shown in [Figure 2.9](#). 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. Press OK, highlight *3 Reboot System*, and press Enter to reboot the system. If the upgrade installer was booted from CD, remove the CDROM.

During the reboot there may be a conversion of the previous configuration database to the new version of the database. This happens during the “Applying database schema changes” line in the reboot cycle. This conversion can take a long time to finish, sometimes fifteen minutes or more, so be patient and the boot will complete normally. If database errors are shown but the graphical administrative interface is accessible, go to Settings → General and use the *Upload Config* button to upload the configuration that you saved before starting the upgrade.

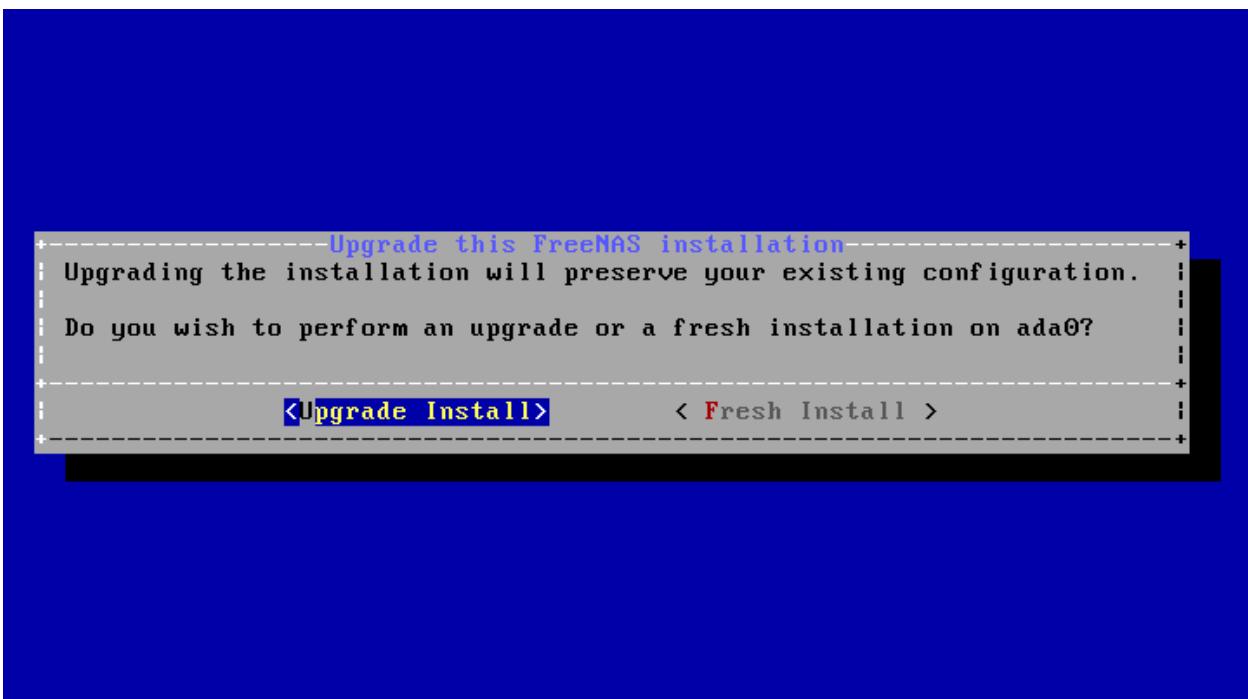


Fig. 2.8: Upgrading a FreeNAS® Installation



Fig. 2.9: Preserve and Migrate Settings

2.5.4 Upgrading From the GUI

To perform an upgrade using this method, go to `System → Update`.

After the update is complete, you will temporarily lose your connection as the FreeNAS® system reboots into the new version of the operating system. The FreeNAS® system will normally receive the same IP address from the DHCP server. Refresh your browser after a moment to see if you can access the system.

2.5.5 If Something Goes Wrong

If an update fails, an alert is issued and the details are written to `/data/update.failed`.

To return to a previous version of the operating system, physical or IPMI access to the FreeNAS® console is needed. Reboot the system and watch for the boot menu. In the example shown in [Figure 2.10](#), the first boot menu entry, *FreeNAS (default)*, refers to the initial installation, before the update was applied. The second boot entry, *FreeNAS-1415259326*, refers to the current version of the operating system, after the update was applied. This second entry is highlighted and begins with a star, indicating that this is the environment the system will boot unless another entry is manually selected. Both entries include a date and timestamp showing when that boot environment was created.

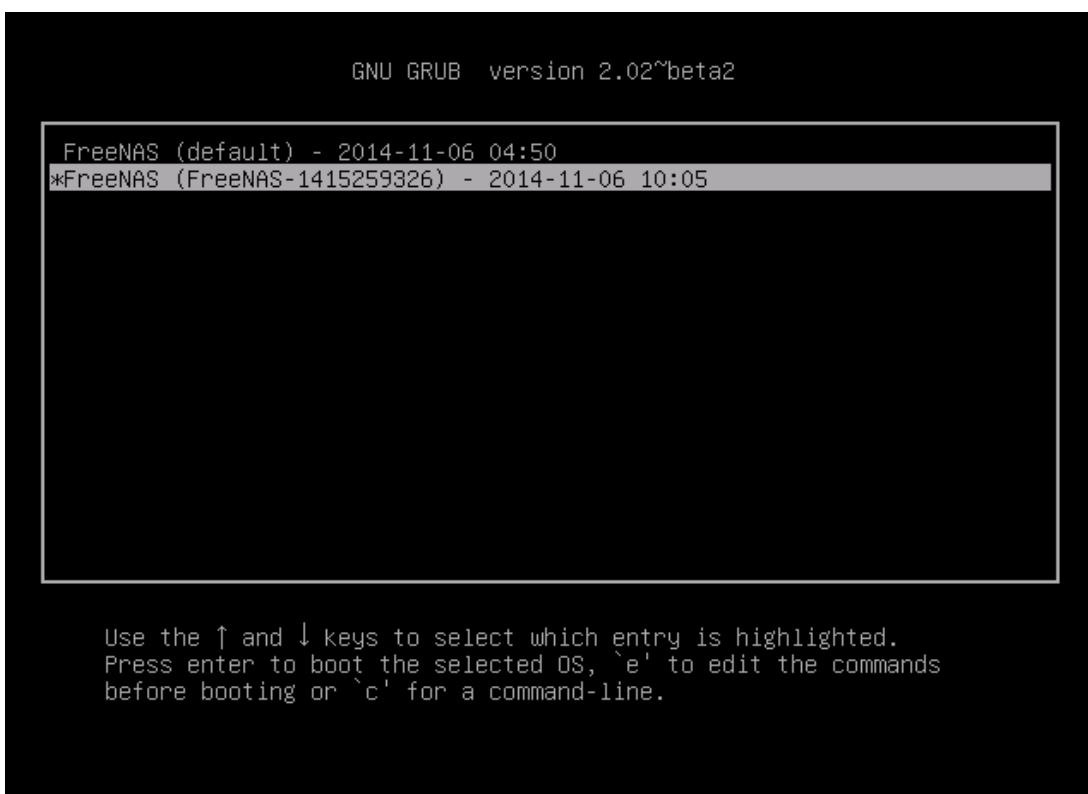


Fig. 2.10: Boot Menu

To boot into the previous version of the operating system, use the up or down arrow to select it and press `Enter`.

If a boot device fails and the system no longer boots, don't panic. The data is still on your disks and you still have a copy of your saved configuration. You can always:

1. Perform a fresh installation on a new boot device.
2. Import your volumes in `Storage → Auto Import Volume`.

3. Restore the configuration in System → General → Upload Config.

Note: You cannot restore a saved configuration which is newer than the installed version. For example, if you reboot into an older version of the operating system, you cannot restore a configuration that was created in a later version.

2.5.6 Upgrading a ZFS Pool

In FreeNAS®, ZFS pools can be upgraded from the graphical administrative interface.

Before upgrading an existing ZFS pool, be aware of these caveats first:

- the pool upgrade is a one-way street, meaning that **if you change your mind you cannot go back to an earlier ZFS version or downgrade to an earlier version of the software that does not support those feature flags**.
- before performing any operation that may affect the data on a storage disk, **always back up your data first and verify the integrity of the backup**. While it is unlikely that the pool upgrade will affect the data, it is always better to be safe than sorry.
- upgrading a ZFS pool is **optional**. It is not necessary to upgrade the pool if you do not need newer feature flags or if you want to keep the possibility of reverting to an earlier version of FreeNAS® or repurposing the disks in another operating system that supports ZFS. If you decide to upgrade the pool to the latest feature flags, it will not be possible to import that pool into another operating system that does not yet support those feature flags.

To perform the ZFS pool upgrade, go to Storage → Volumes → View Volumes and highlight the volume (ZFS pool) to upgrade. Click the *Upgrade* button as shown in [Figure 2.11](#).

Note: If the *Upgrade* button does not appear, the pool is already at the latest feature flags and does not need to be upgraded.

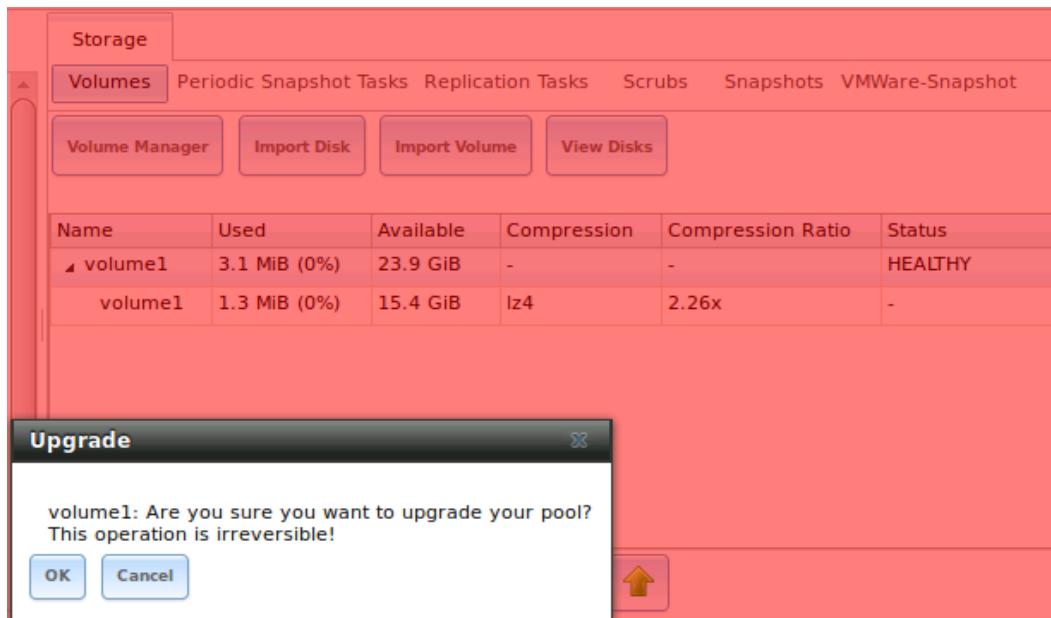


Fig. 2.11: Upgrading a ZFS Pool

The warning reminds you that a pool upgrade is irreversible. Click *OK* to proceed with the upgrade.

The upgrade itself only takes a few seconds and is non-disruptive. It is not necessary to stop any sharing services to upgrade the pool. However, it is best to upgrade when the pool is not being heavily used. The upgrade process will suspend I/O for a short period, but is nearly instantaneous on a quiet pool.

2.6 Virtualization

FreeNAS® can be run inside a virtual environment for development, experimentation, and educational purposes. Please note that running FreeNAS® in production as a virtual machine is [not recommended](#). If you decide to use FreeNAS® within a virtual environment, [read this post first](#) as it contains useful guidelines for minimizing the risk of losing data.

To install or run FreeNAS® within a virtual environment, create a virtual machine that meets these minimum requirements:

- **at least 8192 MB (8 GB) base memory size**
- a virtual disk **at least 8 GB in size** to hold the operating system and boot environments
- at least one additional virtual disk **at least 4 GB in size** to be used as data storage
- a bridged network adapter

This section demonstrates how to create and access a virtual machine within VirtualBox and VMware ESXi environments.

2.6.1 VirtualBox

[VirtualBox](#) is an open source virtualization program originally created by Sun Microsystems. VirtualBox runs on Windows, BSD, Linux, Macintosh, and OpenSolaris. It can be configured to use a downloaded FreeNAS® .iso file, and makes a good testing environment for practicing configurations or learning how to use the features provided by FreeNAS®.

To create the virtual machine, start VirtualBox and click the *New* button, shown in [Figure 2.12](#), to start the new virtual machine wizard.

Click the *Next* button to see the screen in [Figure 2.13](#). Enter a name for the virtual machine, click the *Operating System* drop-down menu and select *BSD*, and select *FreeBSD (64-bit)* from the *Version* dropdown.

Click *Next* to see the screen in [Figure 2.14](#). The base memory size must be changed to **at least 8192 MB**. When finished, click *Next* to see the screen in [Figure 2.15](#).

Click *Create* to launch the *Create Virtual Hard Drive Wizard* shown in [Figure 2.16](#).

Select *VDI* and click the *Next* button to see the screen in [Figure 2.17](#).

Choose either *Dynamically allocated* or *Fixed-size* storage. The first option uses disk space as needed until it reaches the maximum size that is set in the next screen. The second option creates a disk the full amount of disk space, whether it is used or not. Choose the first option to conserve disk space; otherwise, choose the second option, as it allows VirtualBox to run slightly faster. After selecting *Next*, the screen in [Figure 2.18](#) is shown.

This screen is used to set the size (or upper limit) of the virtual disk. **Increase the default size to 8 GB**. Use the folder icon to browse to a directory on disk with sufficient space to hold the virtual disk files. Remember that there will be a system disk of at least 8 GB and at least one data storage disk of at least 4 GB.

After making a selection and pressing *Next*, a summary of the configuration options chosen is shown. Use the *Back* button to return to a previous screen if any values need to be modified. Otherwise, click *Finish* to complete the wizard. The new virtual machine is listed in the left frame, as shown in the example in [Figure 2.19](#).

Create the virtual disks to be used for storage. Click the *Storage* hyperlink in the right frame to access the storage screen seen in [Figure 2.20](#).

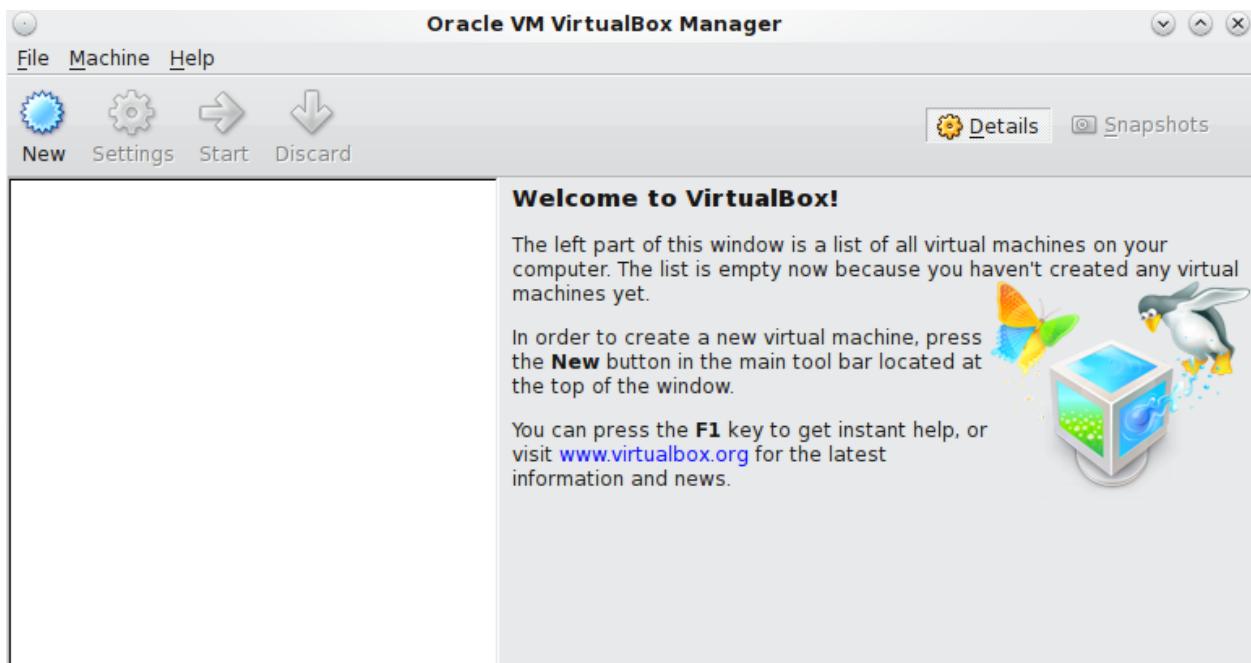


Fig. 2.12: Initial VirtualBox Screen

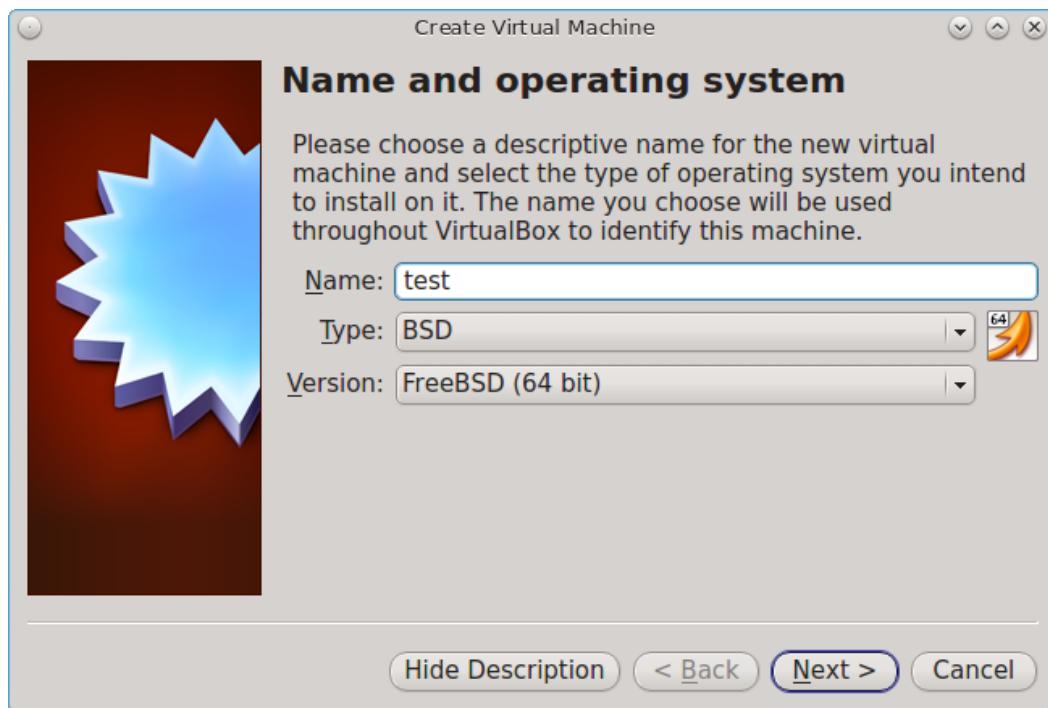


Fig. 2.13: Type in a Name and Select the Operating System for the New Virtual Machine

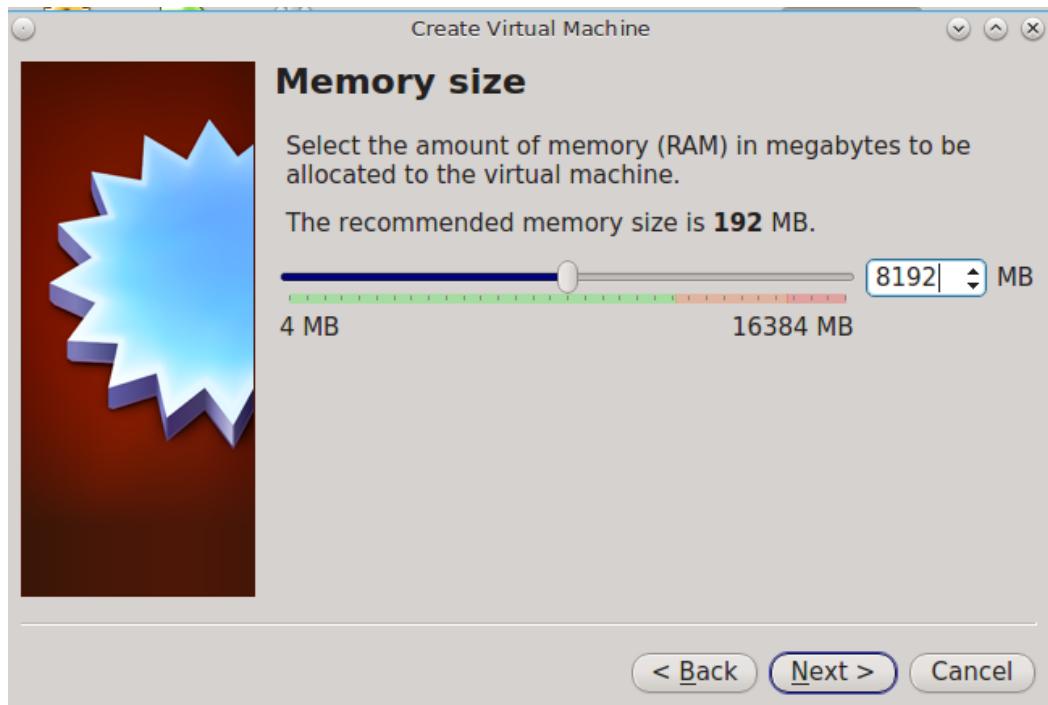


Fig. 2.14: Select the Amount of Memory Reserved for the Virtual Machine

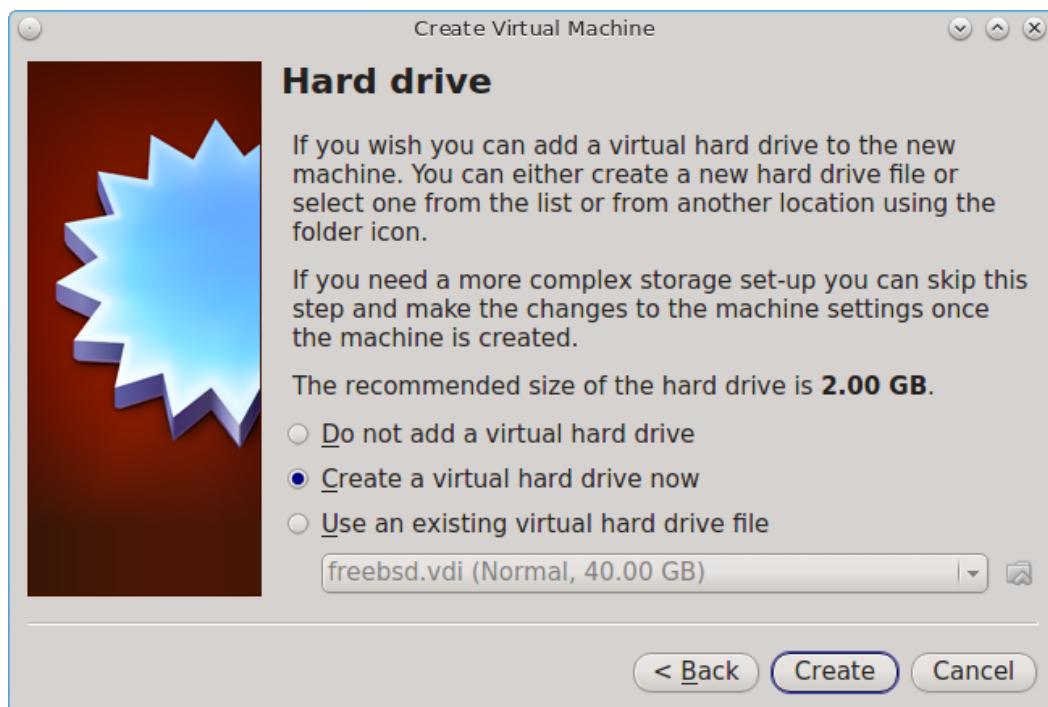


Fig. 2.15: Select Existing or Create a New Virtual Hard Drive



Fig. 2.16: Create New Virtual Hard Drive Wizard

Click the *Add Attachment* button, select *Add Hard Disk* from the pop-up menu, then click the *Create New Disk* button. This launches the Create New Virtual Hard Drive Wizard (seen in [Figure 2.16](#) and [2.17](#)). This disk will be used for storage, so create a size appropriate to your needs, making sure that it is **at least 4 GB**. To practice with RAID configurations, create as many virtual disks as needed. Two disks can be created on each IDE controller. For additional disks, click the *Add Controller* button to create another controller for attaching additional disks.

Create a device for the installation media. Highlight the word “Empty”, then click the *CD* icon as shown in [Figure 2.21](#).

Click *Choose a virtual CD/DVD disk file...* to browse to the location of the `.iso` file. If the `.iso` was burned to CD, select the detected *Host Drive*.

Depending on the extensions available in the host CPU, it might not be possible to boot the VM from `.iso`. If “your CPU does not support long mode” is shown when trying to boot the `.iso`, the host CPU either does not have the required extension or AMD-V/VT-x is disabled in the system BIOS.

Note: If you receive a kernel panic when booting into the ISO, stop the virtual machine. Then, go to *System* and check the box *Enable IO APIC*.

To configure the network adapter, go to *Settings* → *Network*. In the *Attached to* drop-down menu select *Bridged Adapter*, then choose the name of the physical interface from the *Name* drop-down menu. In the example shown in [Figure 2.22](#), the Intel Pro/1000 Ethernet card is attached to the network and has a device name of `em0`.

After configuration is complete, click the *Start* arrow and install FreeNAS® as described in [Performing the Installation](#). Once FreeNAS® is installed, press F12 when the VM starts to boot to access the boot menu. Select the primary hard disk as the boot option. You can permanently boot from disk by removing the *CD/DVD* device in *Storage* or by

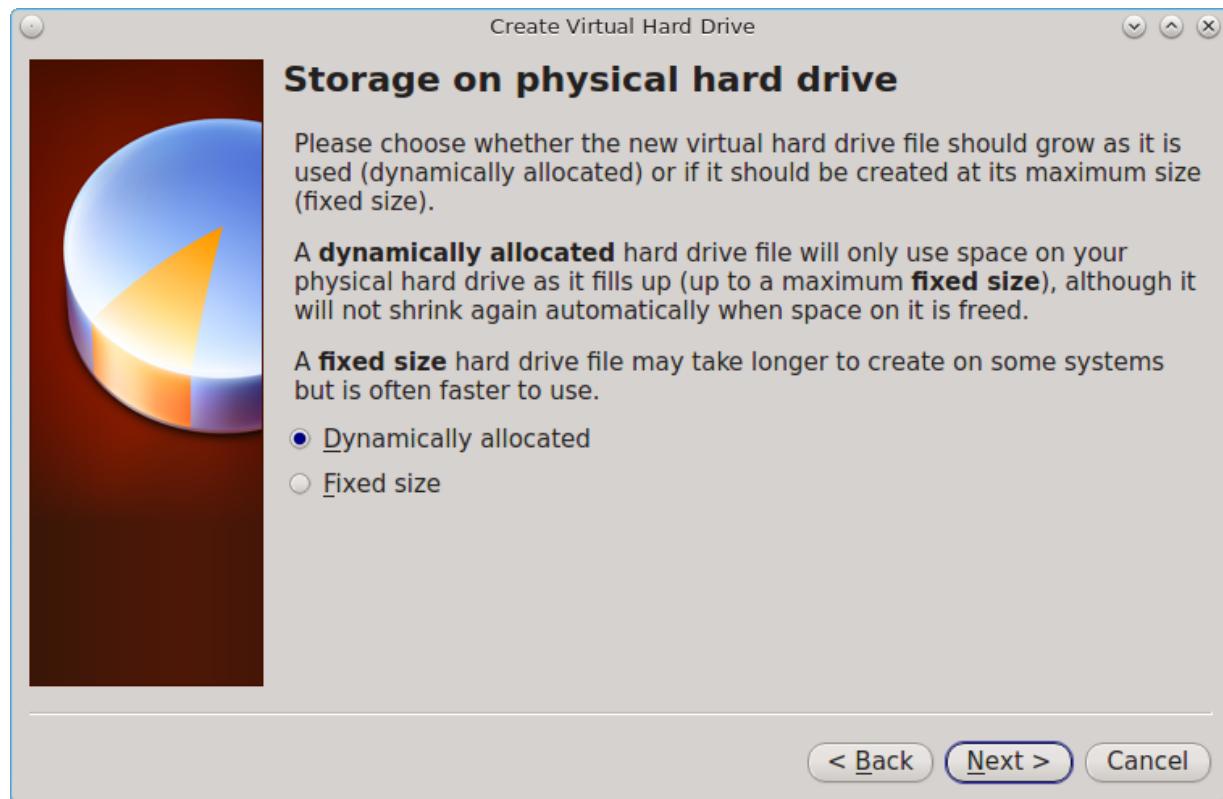


Fig. 2.17: Select Storage Type for Virtual Disk

unchecked *CD/DVD-ROM* in the *Boot Order* section of *System*.

2.6.2 VMware ESXi

Before using ESXi, read [this post](#) for an explanation of why iSCSI will be faster than NFS.

ESXi is a bare-metal hypervisor architecture created by VMware Inc. Commercial and free versions of the VMware vSphere Hypervisor operating system (ESXi) are available from the [VMware website](#). After the operating system is installed on supported hardware, use a web browser to connect to its IP address. The welcome screen provides a link to download the VMware vSphere client which is used to create and manage virtual machines.

Once the VMware vSphere client is installed, use it to connect to the ESXi server. To create a new virtual machine, click *File* → *New* → *Virtual Machine*. The New Virtual Machine Wizard will launch as shown in [Figure 2.23](#).

Click *Next* and enter a name for the virtual machine. Click *Next* and highlight a datastore. An example is shown in [Figure 2.24](#). Click *Next*. In the screen shown in [Figure 2.25](#), click *Other*, then select a FreeBSD 64-bit architecture.

Click *Next* and create a virtual disk file of **8 GB** to hold the FreeNAS® operating system, as shown in [Figure 2.26](#).

Click *Next* and *Finish*. The new virtual machine is listed in the left frame. Right-click the virtual machine and select *Edit Settings* to access the screen shown in [Figure 2.27](#).

Increase the *Memory Configuration* to **at least 8192 MB**.

Under *CPUs*, make sure that only one virtual processor is listed, otherwise it will not be possible to start any FreeNAS® services.

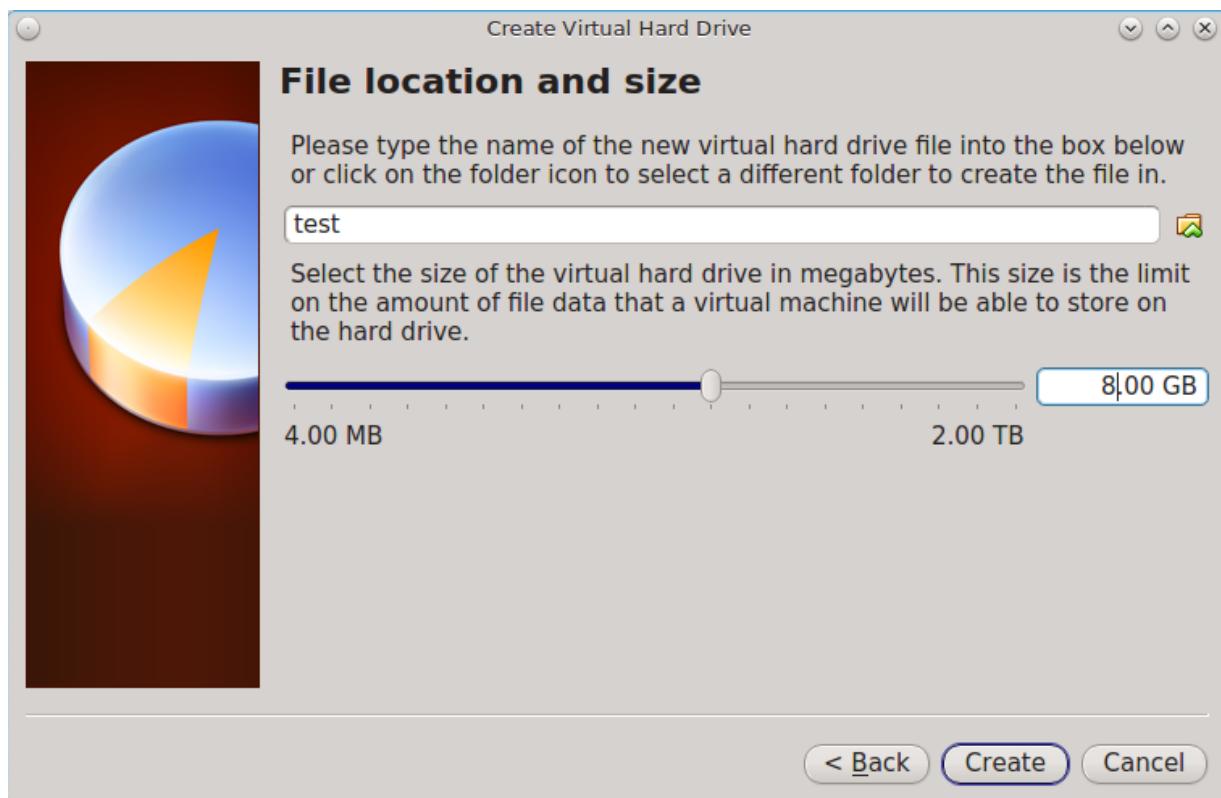


Fig. 2.18: Select File Name and Size of Virtual Disk

To create a storage disk, click `Hard disk 1 → Add`. In the *Device Type* menu, highlight *Hard Disk* and click *Next*. Select *Create a new virtual disk* and click *Next*. In the screen shown in Figure 2.28, select the size of the disk. To dynamically allocate space as needed, check the box *Allocate and commit space on demand (Thin Provisioning)*. Click *Next*, then *Next*, then *Finish* to create the disk. Repeat to create the amount of storage disks needed to meet your requirements.

For ESX 5.0, Workstation 8.0, or Fusion 4.0 or higher, additional configuration is needed so that the virtual HPET setting does not prevent the virtual machine from booting.

If you are running ESX, while in *Edit Settings*, click *Options → Advanced → General → Configuration Parameters*. Change `hpet0.present` from *true* to *false*, then click *OK* twice to save the setting.

For Workstation or Player, while in *Edit Settings*, click *Options → Advanced → File Locations*. Locate the path for the Configuration file named `filename.vmx`. Open that file in a text editor, change `hpet0.present` from *true* to *false*, and save the change.

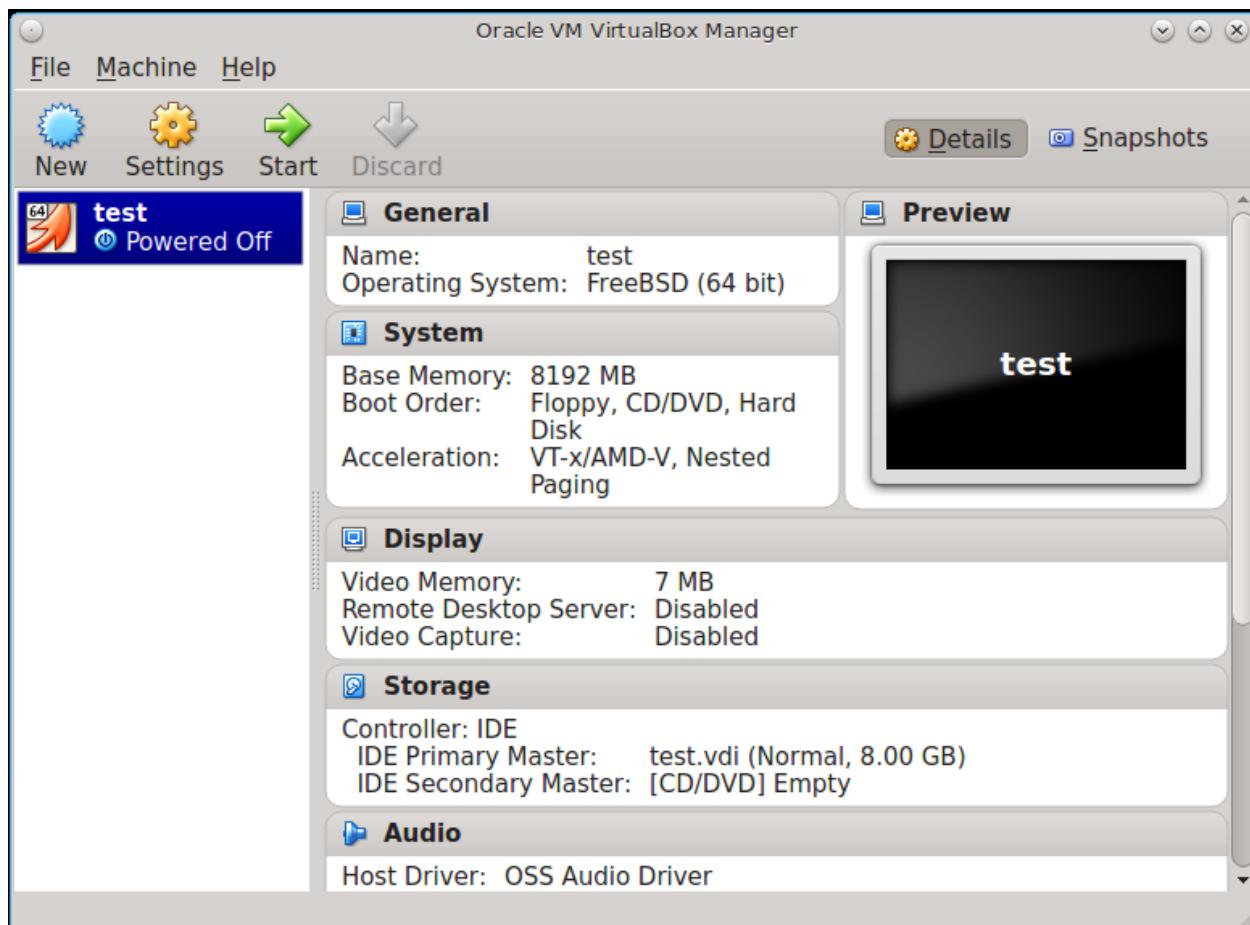


Fig. 2.19: The New Virtual Machine

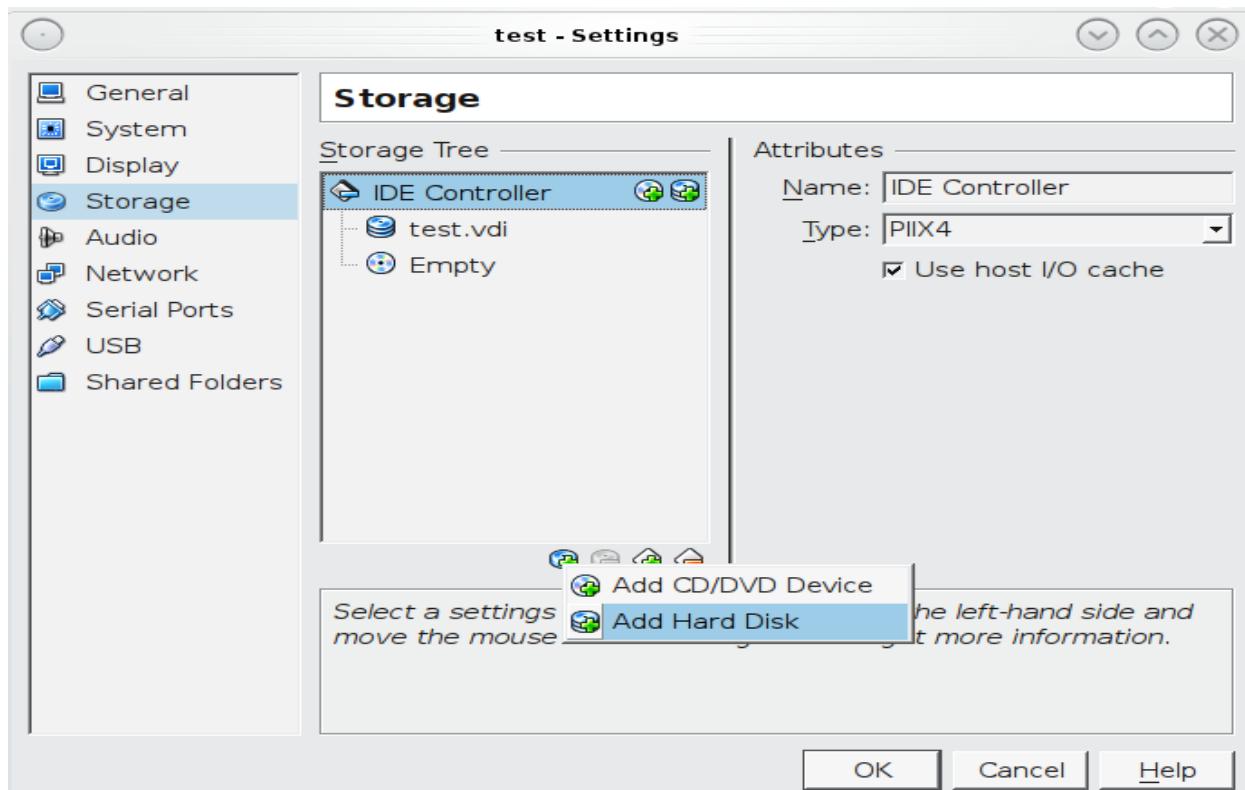


Fig. 2.20: Storage Settings of the Virtual Machine

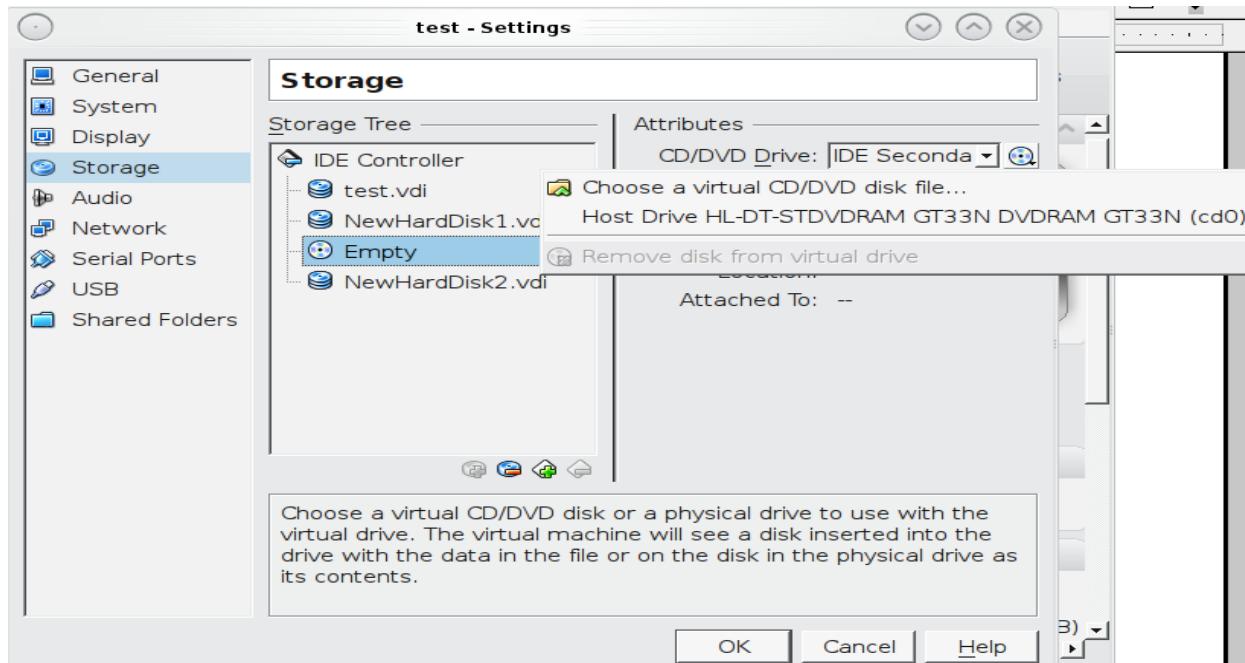


Fig. 2.21: Configuring ISO Installation Media

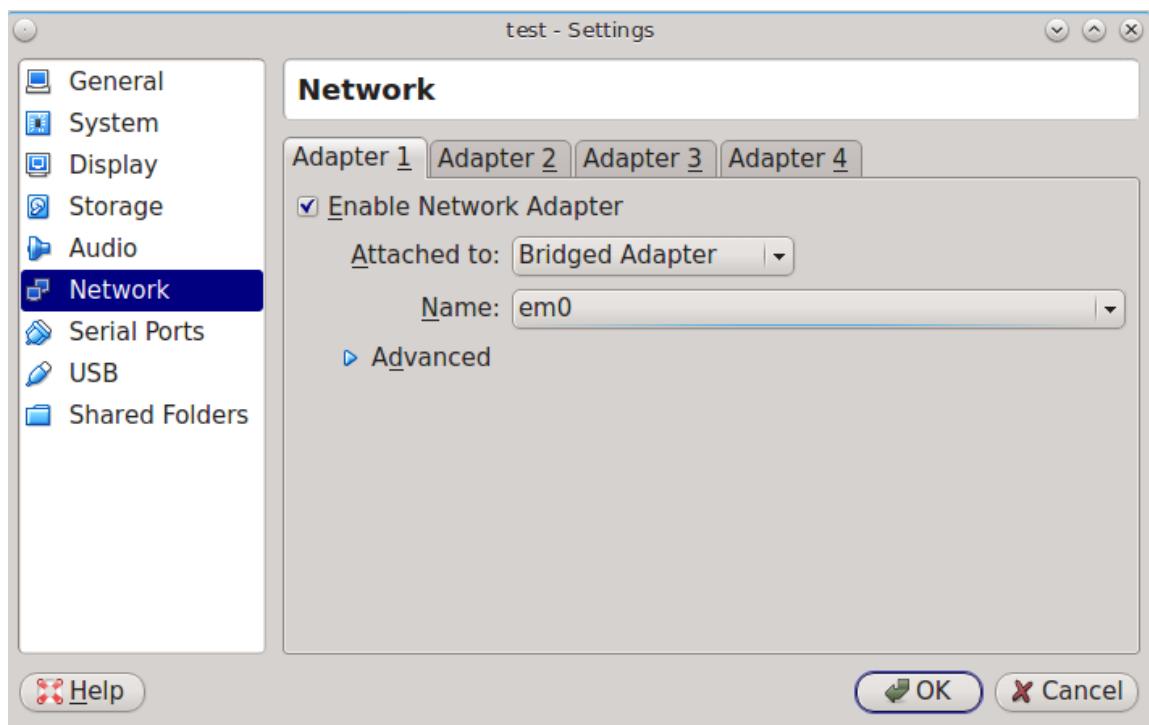


Fig. 2.22: Configuring a Bridged Adapter in VirtualBox

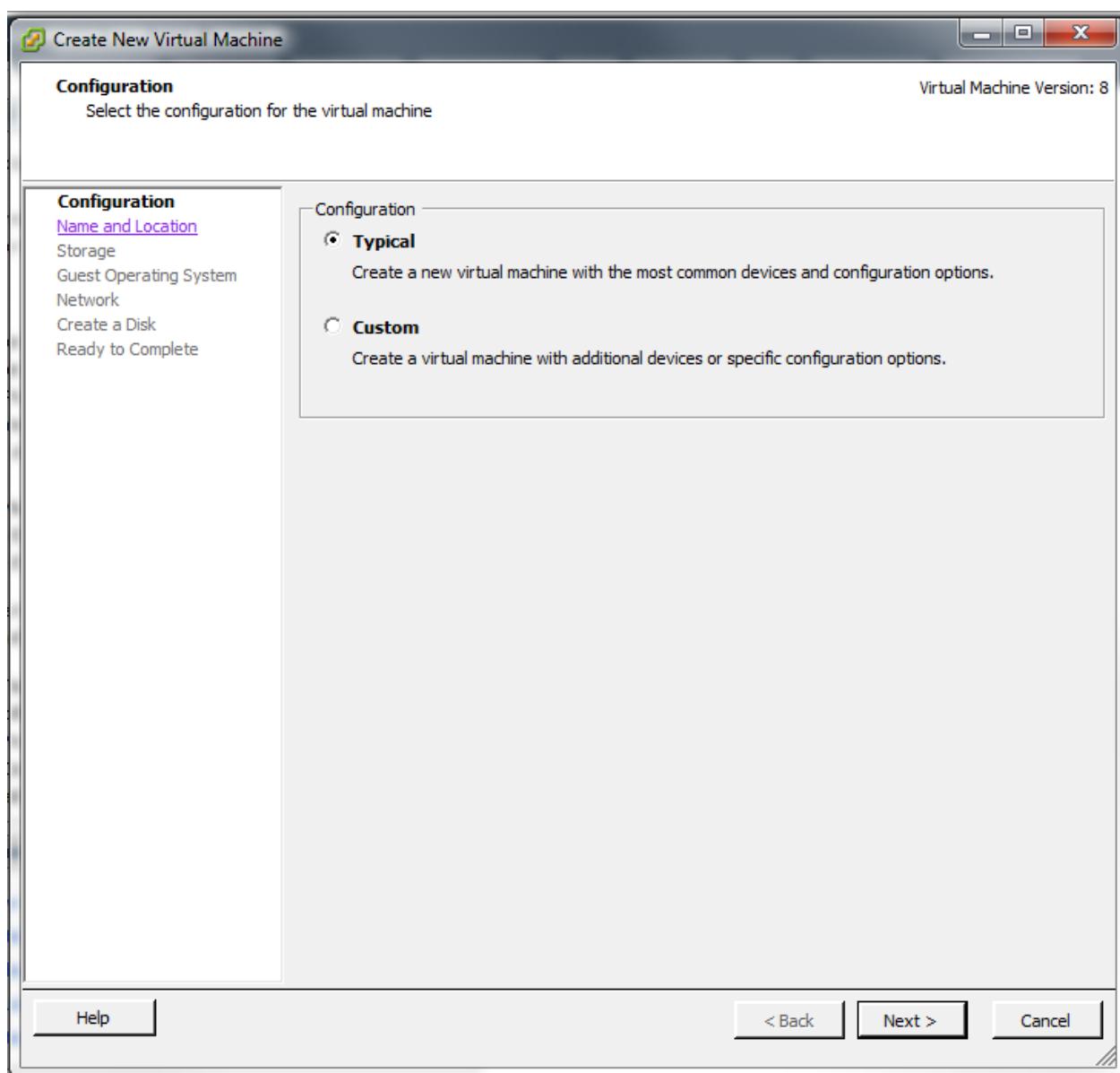


Fig. 2.23: New Virtual Machine Wizard

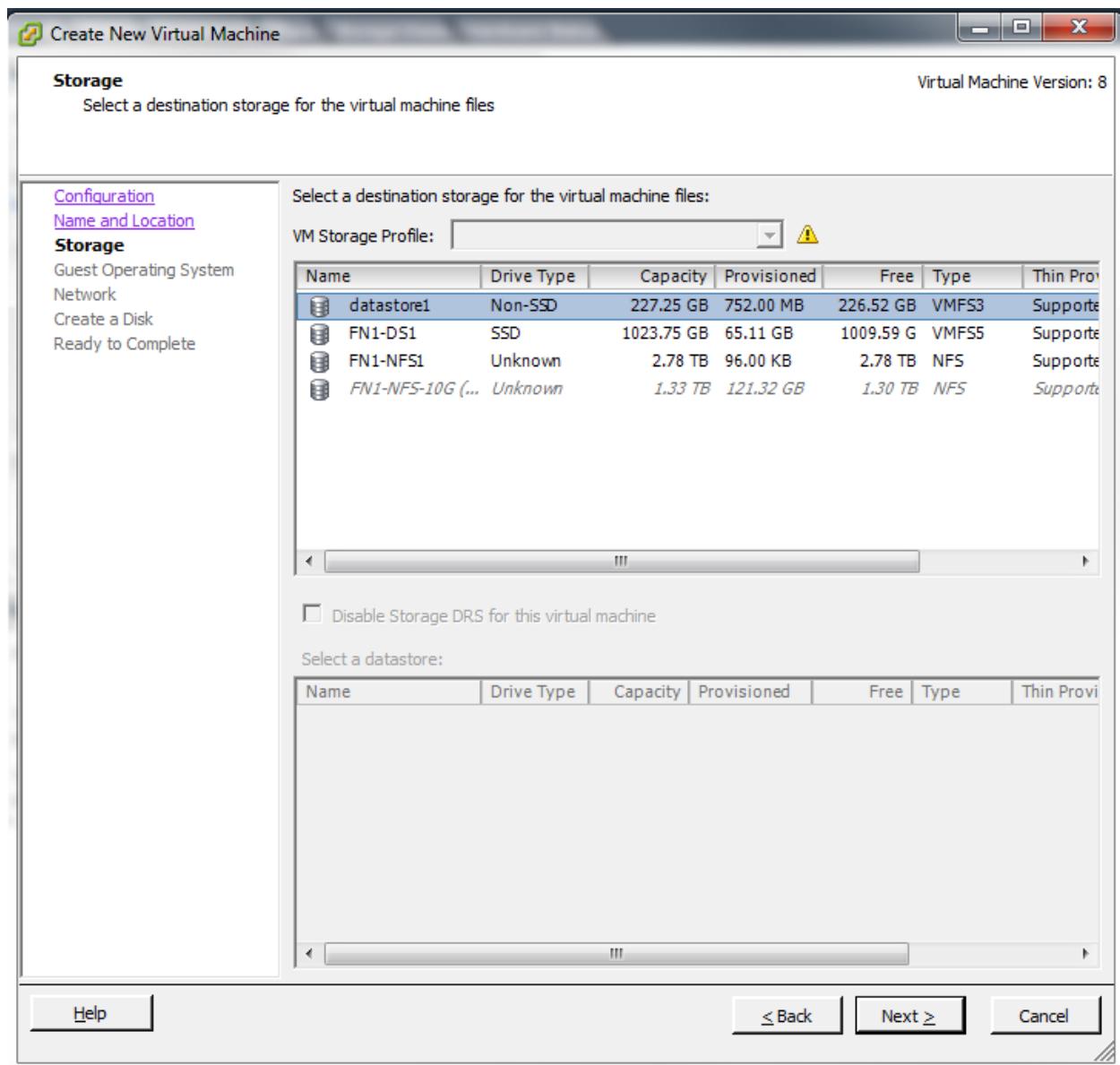


Fig. 2.24: Select Datastore

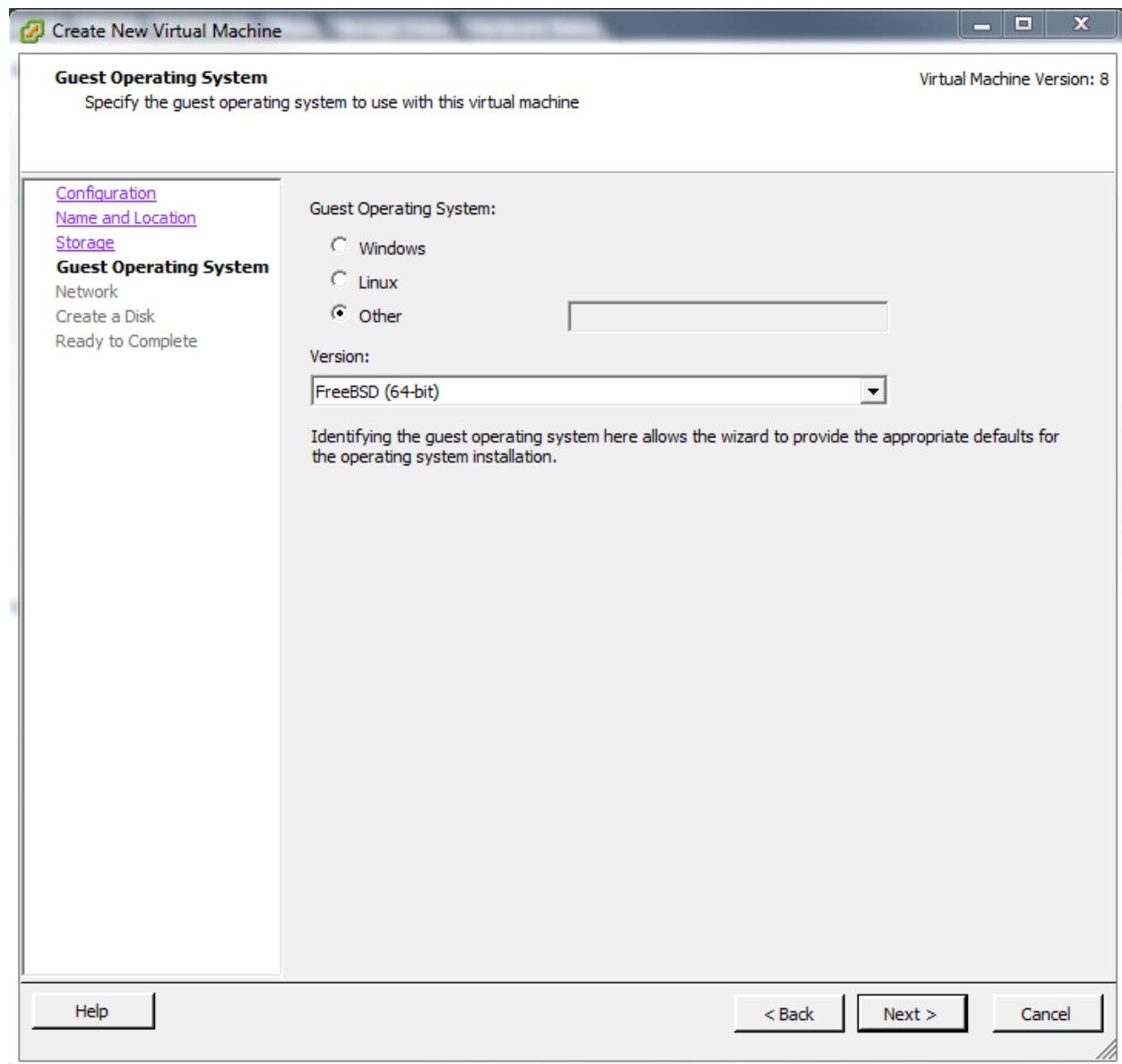


Fig. 2.25: Select Operating System

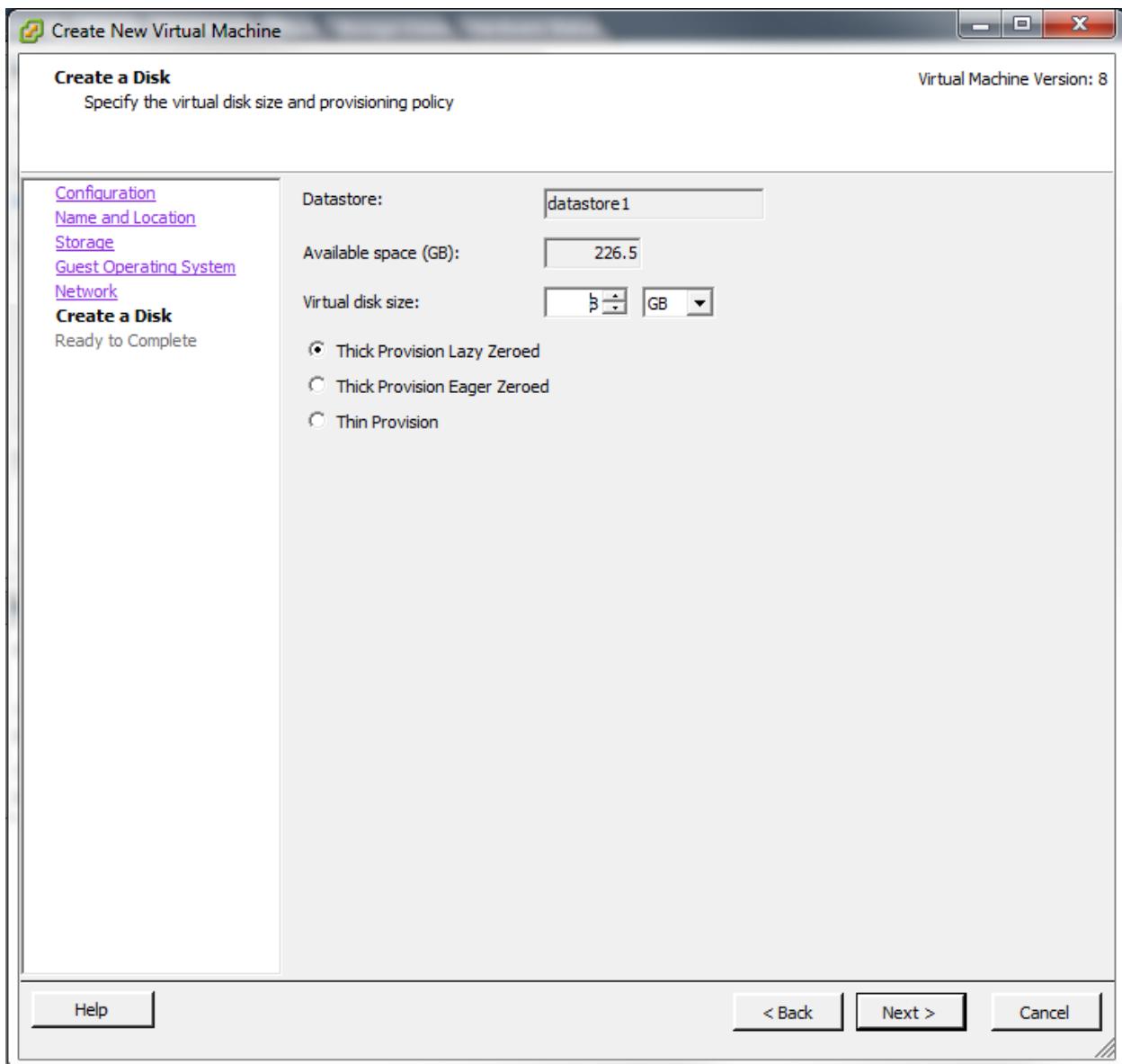


Fig. 2.26: Create Disk for the Operating System

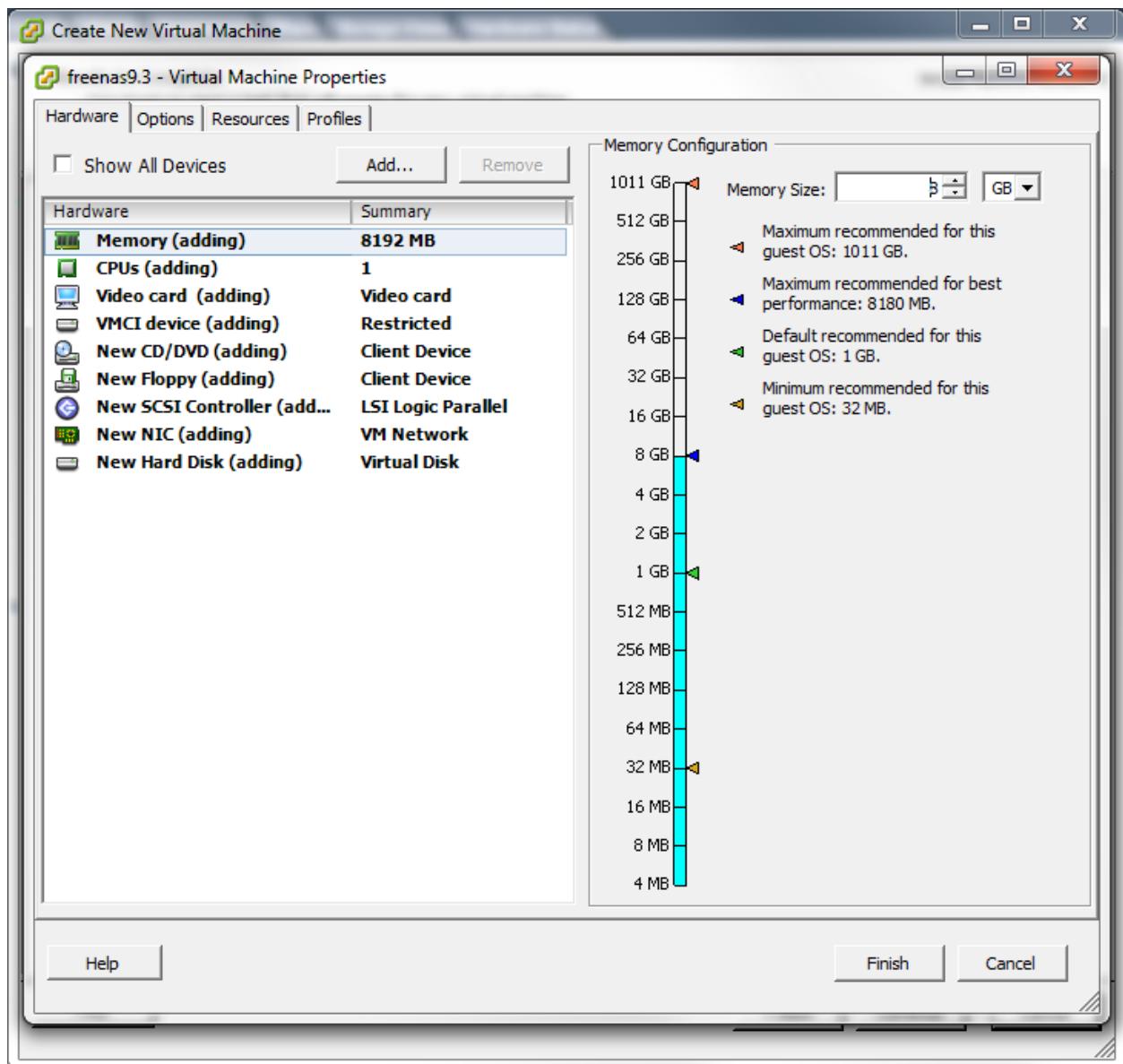


Fig. 2.27: Virtual Machine Settings

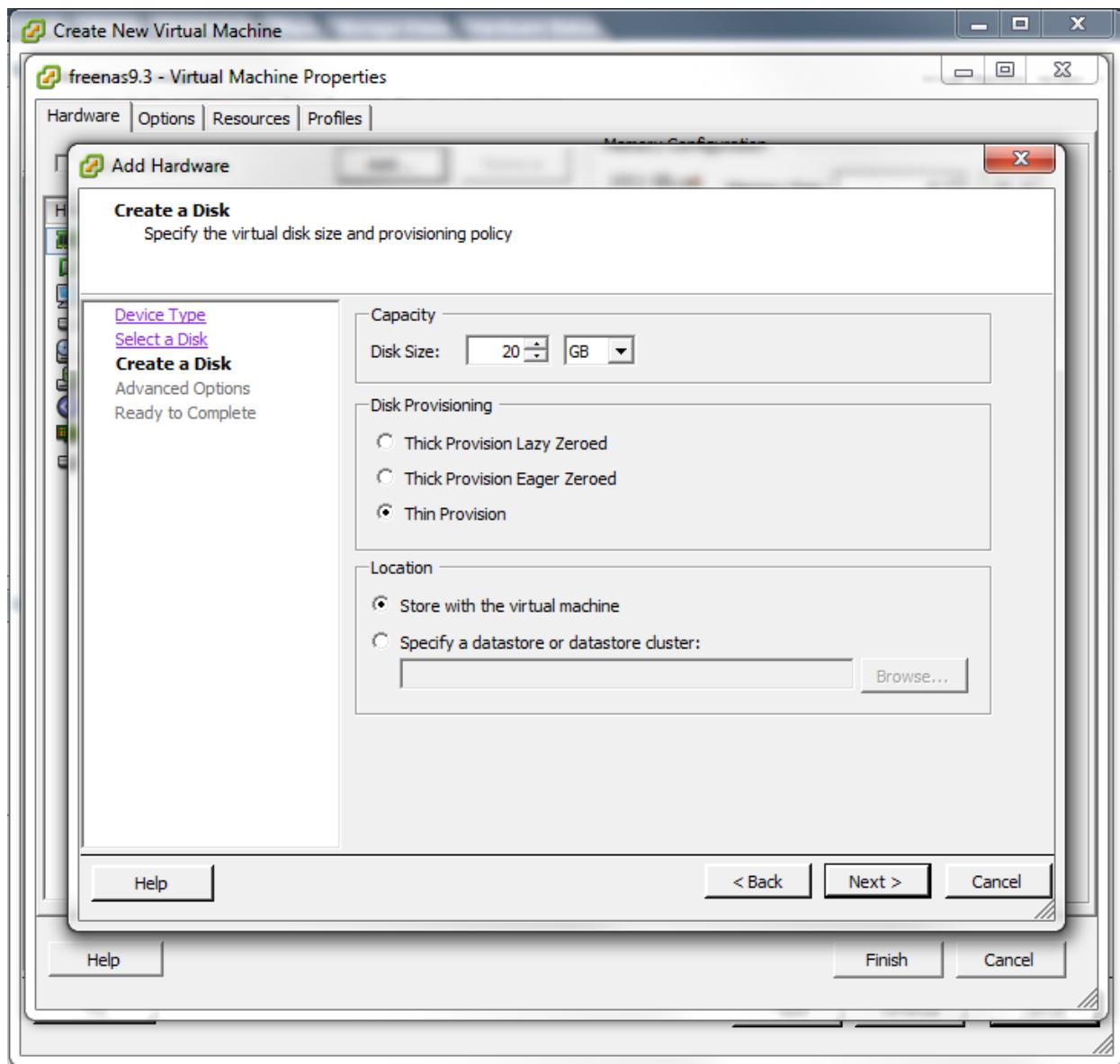
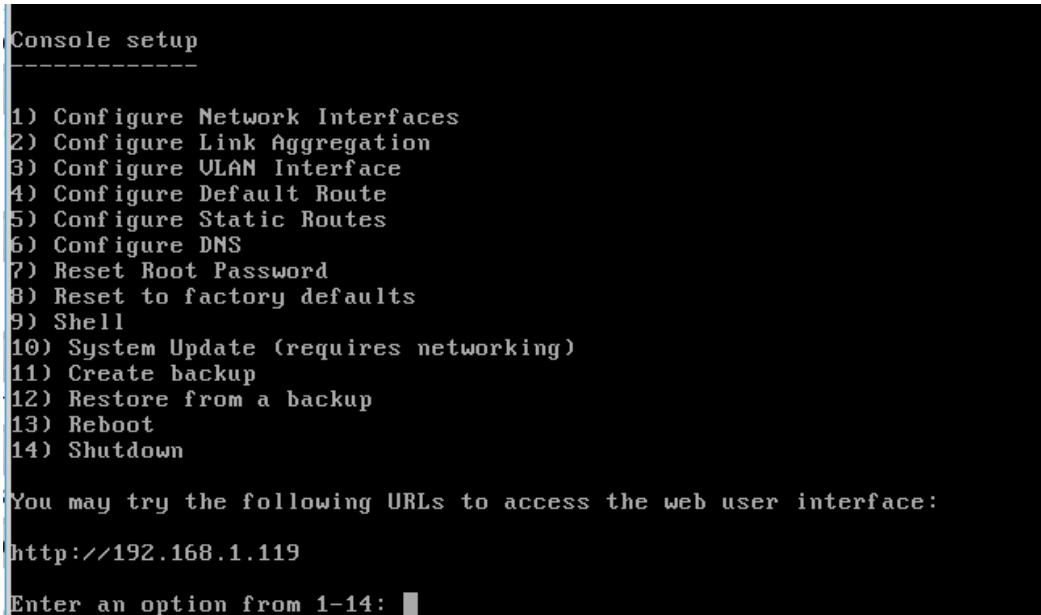


Fig. 2.28: Creating a Storage Disk

BOOTING INTO FREEFAS®

The Console Setup menu, shown in [Figure 3.1](#), appears at the end of the boot process. If access to the FreeNAS® system's keyboard and monitor is available, this Console Setup menu can be used to administer the system if the administrative GUI is not available.

Note: The Console Setup menu can be accessed from within the FreeNAS® GUI by typing `/etc/netcli` from *Shell*. The Console Setup menu can be disabled by unchecking the *Enable Console Menu* in System → Settings → Advanced .



A terminal window showing the FreeNAS Console Setup menu. The menu lists 14 options numbered 1 to 14. Options 1 through 13 are listed, while option 14 is partially visible. The menu includes a note about web access and a URL for the web interface. A cursor is visible at the bottom, prompting for an option number.

```
Console setup
-----
1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset to factory defaults
9) Shell
10) System Update (requires networking)
11) Create backup
12) Restore from a backup
13) Reboot
14) Shutdown

You may try the following URLs to access the web user interface:
http://192.168.1.119

Enter an option from 1-14: █
```

Fig. 3.1: Console Setup Menu

The menu provides these options:

- 1) **Configure Network Interfaces:** provides a configuration wizard to configure the system's network interfaces.
- 2) **Configure Link Aggregation:** allows creating a new link aggregation or deleting an existing link aggregation.
- 3) **Configure VLAN Interface:** is used to create or delete a VLAN interface.
- 4) **Configure Default Route:** is used to set the IPv4 or IPv6 default gateway. When prompted, enter the IP address of the default gateway.

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

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

7) Reset Root Password: if you are unable to log in to the graphical administrative interface, select this option and follow the prompts to set the `root` password.

8) Reset to factory defaults: to delete **all** of the configuration changes made in the administrative GUI, select this option. Once the configuration is reset, the system will reboot. It will be necessary to use `Storage → Volumes → Import Volume` to re-import any volumes.

9) Shell: starts a shell for running FreeBSD commands. To leave the shell, type `exit`.

10) System Update: checks for system updates. If any new updates are available, they are automatically be downloaded and applied. This is a simplified version of the [Update](#) option available in the web interface. Updates are applied immediately for the currently selected train and access to the GUI is not required. For more advanced update options like switching trains, use [Update](#).

11) Create backup: backs up the FreeNAS® configuration and ZFS layout, and, optionally, the data, to a remote system over an encrypted connection. The remote system must have sufficient space to hold the backup and be running an SSH server on port 22. The remote system does not have to be formatted with ZFS, as the backup will be saved as a binary file. When this option is selected, it prompts for the hostname or IP address of the remote system, the name of a user account on that system, the user account password, the full path to a directory on the remote system to save the backup, whether to also back up all of the data, whether to compress the data, and a confirmation to save the values. `y` starts the backup, `n` repeats the configuration, and `q` quits the backup wizard. If the password is left empty, key-based authentication is used instead. This requires that the public key of the `root` user has been stored in `~root/.ssh/authorized_keys` on the remote system and that the key is **not** protected by a passphrase. Refer to [Rsync over SSH Mode](#) for instructions on generating a key pair.

12) Restore from a backup: restores from an existing backup created with 11) *Create backup* or `System → Advanced → Backup`. It prompts for the hostname or IP address of the remote system holding the backup, the username that was used, the password (leave empty if key-based authentication was used), the full path of the remote directory storing the backup, and a confirmation that the values are correct. `y` starts the restore, `n` repeats the configuration, and `q` quits the restore wizard. The restore indicates if it can log into the remote system, find the backup, and whether the backup contains data. It then prompts to restore FreeNAS® from that backup. Note that if `y` is pressed to perform the restore, the system will be returned to the database configuration, ZFS layout, and optionally the data, at the point in time when the backup was created. The system reboots after the restore completes.

Warning: The backup and restore options are meant for disaster recovery. If you restore a system, it is returned to the point in time that the backup was created. If you select the option to save the data, any data created after the backup was made will be lost. If you do **not** select the option to save the data, the system will be recreated with the same ZFS layout, but with **no** data.

Warning: The backup function **IGNORES ENCRYPTED POOLS**. Do not use it to back up systems with encrypted pools.

13) Reboot: reboots the system.

14) Shutdown: halts the system.

During boot, FreeNAS® automatically attempts to connect to a DHCP server from all live interfaces. If it successfully receives an IP address, the address is displayed so it can be used to access the graphical console. In the example seen in [Figure 3.1](#), the FreeNAS® system is accessible from <http://192.168.1.119>.

If the FreeNAS® server is not connected to a network with a DHCP server, use the network configuration wizard to manually configure the interface as seen in *Example: Manually Setting an IP Address from the Console Menu*. In this example, the FreeNAS® system has one network interface (*em0*).

Manually Setting an IP Address from the Console Menu

```
Enter an option from 1-14: 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
```

Once the system has an IP address, enter that address into a graphical web browser from a computer capable of accessing the network containing the FreeNAS® system. The password for the root user is requested as shown in Figure 3.2.

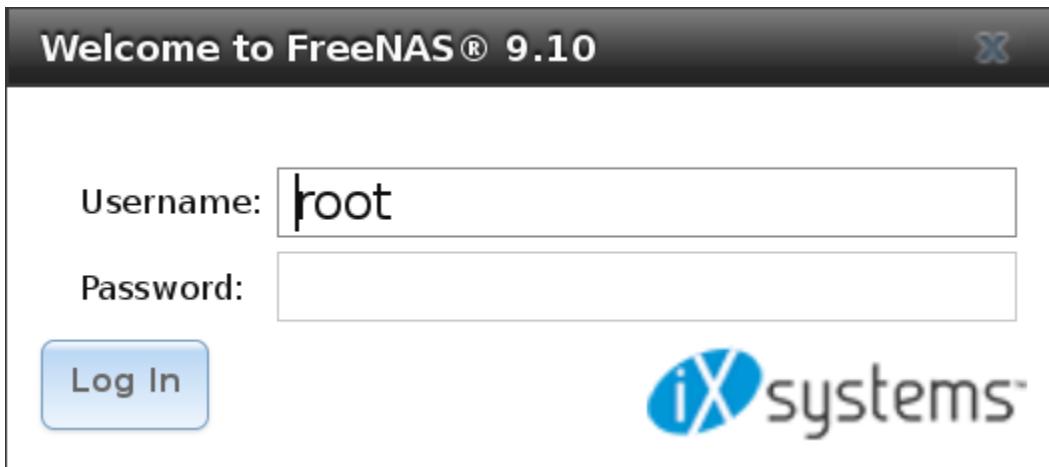


Fig. 3.2: Enter the Root Password

Enter the password created during the installation. You should then see the administrative GUI as shown in the example in Figure 3.3.

If you are unable to access the IP address from a browser, check the following:

- Are proxy settings enabled in the browser configuration? If so, disable the settings and try connecting again.
- If the page does not load, make sure that you can **ping** the FreeNAS® system's IP address. If the address is in a private IP address range, you will only be able to access the system from within the private network.

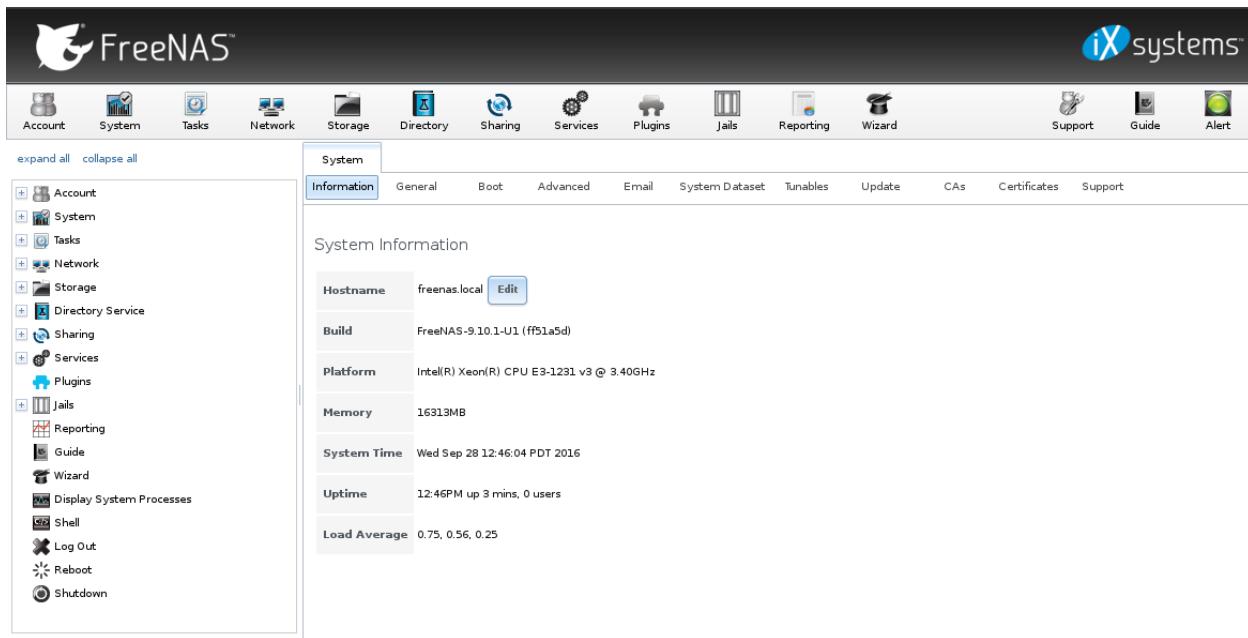


Fig. 3.3: FreeNAS® Graphical Configuration Menu

- If the user interface loads but is unresponsive or seems to be missing menu items, try using a different web browser. IE9 has known issues and will not display the graphical administrative interface correctly if compatibility mode is turned on. If you can't access the GUI using Internet Explorer, use [Firefox](#) instead.
- If you receive *An error occurred!* messages when attempting to configure an item in the GUI, make sure that the browser is set to allow cookies from the FreeNAS® system.

This [blog post](#) describes some applications which can be used to access the FreeNAS® system from an iPad or iPhone.

3.1 Initial Configuration Wizard

A configuration wizard automatically starts the first time the FreeNAS® GUI is accessed. This wizard walks you through the steps needed to quickly configure FreeNAS® to start serving data over a network. This section describes these configuration steps. If you wish to use the wizard again after the initial configuration, click the *Wizard* icon.

Figure 3.4 shows the first wizard configuration screen.

Language:	<input type="button" value="English"/>
Console Keyboard Map:	<input type="button" value="----"/>
Timezone:	<input type="button" value="America/Los_Angeles"/>
Next	Exit

Fig. 3.4: Configuration Wizard

Note: You can exit the wizard at any time by clicking the *Exit* button. However, exiting the wizard will not save any selections. The wizard can always be run again by clicking the *Wizard* icon. Alternately, the FreeNAS® GUI can be used to configure the system, as described in the rest of this Guide.

This screen can be used to change the default language, keyboard map, and timezone. After making your selections, click *Next*. The next screen depends on whether or not the storage disks have already been formatted into a ZFS pool.

Figure 3.5 shows the configuration screen that appears if the storage disks have not yet been formatted.

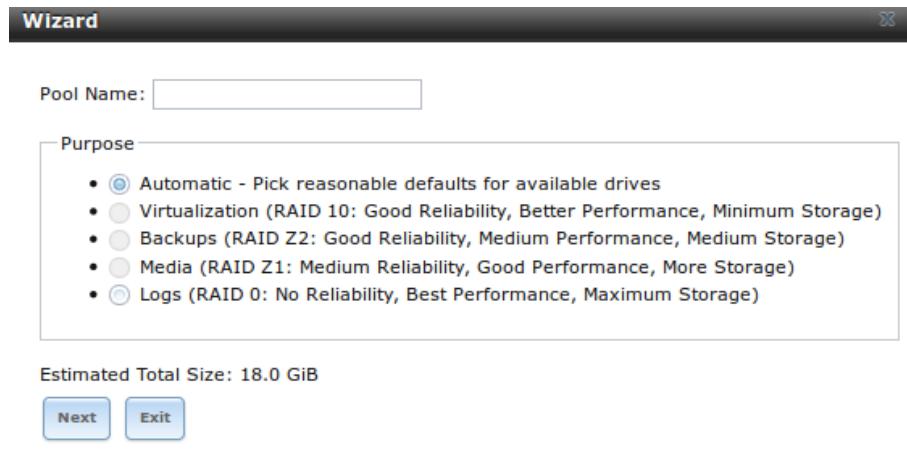


Fig. 3.5: Volume Creation Wizard

Note: The wizard will not recognize an **encrypted** ZFS pool. If your ZFS pool is GELI-encrypted, cancel the wizard and use the instructions in [Importing an Encrypted Pool](#) to import the encrypted volume. You can then rerun the wizard afterwards, if you wish to use it for post-configuration, and it will recognize that the volume has been imported and will not prompt to reformat the disks.

Enter a name for the ZFS pool that conforms to these [naming conventions](#). It is recommended to choose a name that will stick out in the logs (e.g. **not** `data` or `freenas`).

Decide if the pool should provide disk redundancy, and if so, which type. The [ZFS Primer](#) discusses RAIDZ redundancy in more detail. If you prefer to make a more complex configuration, click the *Exit* button to close the wizard and instead use [Volume Manager](#).

These redundancy types are available:

- **Automatic:** automatically creates a mirrored, RAIDZ1, or RAIDZ2 pool, depending upon the number of disks. If you prefer to control the type of redundancy, select one of the other options.
- **RAID 10:** creates a striped mirror and requires a minimum of 4 disks.
- **RAIDZ2:** requires a minimum of 4 disks. Up to 2 disks can fail without data loss.
- **RAIDZ1:** requires a minimum of 3 disks. Up to 1 disk can fail without data loss.
- **Stripe:** requires a minimum of 1 disk. Provides **no** redundancy, meaning if any of the disks in the stripe fails, all data in the stripe is lost.

Once you have made your selection, click *Next* to continue.

If the disks have already been formatted with ZFS and the disks have **not** been encrypted, the next screen will instead prompt to import the volume, as shown in [Figure 3.6](#).



Fig. 3.6: Volume Import Screen

Select the existing volume from the drop-down menu and click *Next* to continue.

The next screen in the wizard is shown in [Figure 3.7](#).

Directory Service:	Active Directory
Domain Name (DNS/Realm-Name):	
Domain Account Name:	
Domain Account Password:	

Fig. 3.7: Directory Service Selection

If the FreeNAS® system is on a network that does not contain an Active Directory, LDAP, NIS, or NT4 server, click *Next* to skip to the next screen.

However, if the FreeNAS® system is on a network containing an Active Directory, LDAP, NIS, or NT4 server and you wish to import the users and groups from that server, select the type of directory service in the *Directory Service* drop-down menu. The rest of the fields in this screen will vary, depending upon which directory service is selected. Available configuration options for each directory service are summarized in Tables 3.1 through 3.4.

Note: Additional configuration options are available for each directory service. The wizard can be used to set the initial values required to connect to that directory service. You can then review the other available options in [Directory Service](#) to determine if additional configuration is required.

Table 3.1: Active Directory Options

Setting	Value	Description
Domain Name	string	name of Active Directory domain (e.g. <i>example.com</i>) or child domain (e.g. <i>sales.example.com</i>)
Domain Account Name	string	name of the Active Directory administrator account
Domain Account Password	string	password for the Active Directory administrator account

Table 3.2: LDAP Options

Setting	Value	Description
Hostname	string	hostname or IP address of LDAP server
Base DN	string	top level of the LDAP directory tree to be used when searching for resources (e.g. <i>dc=test,dc=org</i>)
Bind DN	string	name of administrative account on LDAP server (e.g. <i>cn=Manager,dc=test,dc=org</i>)
Base password	string	password for

Table 3.3: NIS Options

Setting	Value	Description
NIS domain	string	name of NIS domain
NIS servers	string	comma delimited list of hostnames or IP addresses
Secure mode	checkbox	if checked, <code>ypbind(8)</code> will refuse to bind to any NIS server that is not running as root on a TCP port number over 1024
Many-cast	checkbox	if checked, <code>ypbind</code> will bind to the server that responds the fastest; this is useful when no local NIS server is available on the same subnet

Table 3.4: NT4 Options

Setting	Value	Description
Domain Controller	string	hostname of domain controller
NetBIOS Name	string	hostname of FreeNAS® system; cannot be greater than 15 characters or the same as the <i>Workgroup Name</i>
Workgroup Name	string	name of Windows server's workgroup
Administrator Name	string	name of the domain administrator account
Administrator Password	string	input and confirm the password for the domain administrator account

The next configuration screen, shown in [Figure 3.8](#), is used to create network shares.

FreeNAS® supports several types of shares for providing storage data to the clients in a network. The initial wizard can be used to quickly make shares using default permissions which should “just work” for common scenarios. For more complex scenarios, refer to the section on [Sharing](#).

To create a share using the wizard, enter a name for the share, then select the *Purpose* of the share:

- **Windows (SMB):** this type of share can be accessed by any operating system using a SMB client. Check the box for *Allow Guest* to allow users to access the share without a password. SMB shares created with the wizard can be fine-tuned afterward with [Windows \(SMB\) Shares](#).
- **Mac OS X (AFP):** this type of share can be accessed by Mac OS X users. Check the box for *Time Machine* if Mac users will be using the FreeNAS® system as a backup device. AFP shares created with the wizard can be fine-tuned afterward with [Apple \(AFP\) Shares](#).
- **Generic Unix (NFS):** this type of share can be accessed by any operating system using a NFS client. NFS shares created using the wizard can be fine-tuned afterward with [Unix \(NFS\) Shares](#).
- **Block Storage (iSCSI):** this type of share can be accessed by any operating system using iSCSI initiator software. Enter the size of the block storage to create in the format *20G* (for 20 GB). iSCSI shares created with the wizard can be fine-tuned afterward with [iSCSI](#).

After selecting the *Purpose*, click the *Ownership* button to see the screen shown in [Figure 3.9](#).

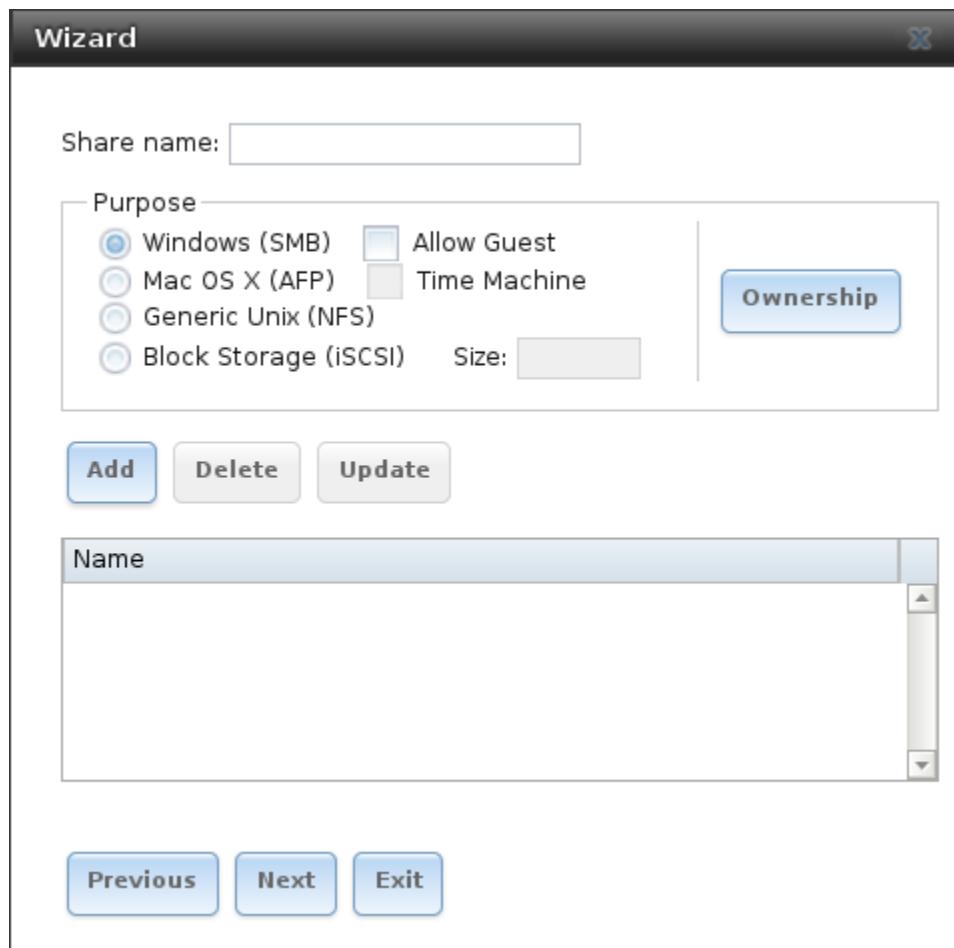


Fig. 3.8: Network Shares

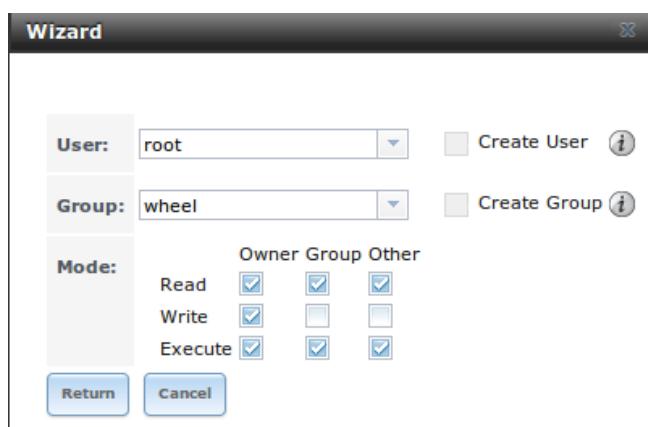


Fig. 3.9: Share Permissions

The default permissions for the share are displayed. To create a user or group, enter the desired name, then check the *Create User* box to create that user and the *Create Group* box to create the group. Check or uncheck the boxes in the *Mode* section to set the initial access permissions for the share. When finished, click the *Return* button to return to the share creation screen. Click the *Add* button to finish creating that share, which will then appear in the *Name* frame.

The *Delete* button can be used to remove the share highlighted in the *Name* frame. To edit a share, highlight it, make the change, then press the *Update* button.

When finished making shares, click the *Next* button to advance to the screen shown in Figure 3.10.

Console messages:	
<input type="checkbox"/>	(i)
Root E-mail:	<input type="text"/>
From email:	<input type="text" value="root@freenas.local"/>
Outgoing mail server:	<input type="text"/>
Port to connect to:	<input type="text" value="25"/>
TLS/SSL:	<input type="text" value="Plain"/>
Use SMTP Authentication:	<input type="checkbox"/>
Username:	<input type="text"/>
Password:	<input type="text"/>
Password confirmation:	<input type="text"/>

Buttons at the bottom: Previous, Send Test Mail, Next, Exit

Fig. 3.10: Miscellaneous Settings

This screen can be used to configure these settings:

- **Console messages:** check this box if you would like to view system messages at the bottom of the graphical administrative interface. This can be handy when troubleshooting a service that will not start. When using the console message view, if you click the console messages area, it will pop-up as a window, allowing you to scroll through the output and to copy its contents.
- **Root E-mail:** FreeNAS® provides an “Alert” icon in the upper right corner to provide a visual indication of events that warrant administrative attention. The alert system automatically emails the *root* user account whenever an alert is issued. **It is important** to enter the email address of the person to receive these alerts and other administrative emails. The rest of the email settings in this screen should also be reviewed and edited as necessary. Before leaving this screen, click the “Send Test Mail” button to ensure that email notifications are working correctly.
- **From email:** the from email address to use when sending email notifications.
- **Outgoing mail server:** hostname or IP address of SMTP server.
- **Port to connect to:** port number used by the SMTP server.
- **TLS/SSL:** encryption type used by the SMTP server.

- **Use SMTP Authentication:** check this box if the SMTP server requires authentication.
- **Username:** enter the username if the SMTP server requires authentication.
- **Password:** enter the password if the SMTP server requires authentication.

When finished, click *Next*. A message will indicate that the wizard is ready to perform all of the saved actions. To make changes, click the *Return to Wizard* button to review your edits. If you click the *Exit without saving* button, none of your selections will be saved. To save your edits, click the *Confirm* button. A status bar will indicate when the wizard has completed applying the new settings.

In addition to the settings that you specify, the wizard will automatically enable *S.M.A.R.T. Tests*, create a boot environment, and add the new boot environment to the boot menu. If you also wish to save a backup of the configuration database to the system being used to access the administrative graphical interface, go to *System → General*, click the *Save Config* button, and browse to the directory where the configuration will be saved. **Always back up your configuration after making any configuration changes.**

The rest of this Guide describes the FreeNAS® graphical interface in more detail. The layout of this Guide follows the order of the menu items in the tree located in the left frame of the graphical interface.

Note: It is important to use the GUI (or the Console Setup menu) for all configuration changes. FreeNAS® uses a configuration database to store its settings. While it is possible to 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.

ACCOUNT

The Account Configuration section of the administrative GUI describes how to manually create and manage users and groups. This section contains these entries:

- *Groups*: used to manage UNIX-style groups on the FreeNAS® system.
- *Users*: used to manage UNIX-style accounts on the FreeNAS® system.

Each entry is described in more detail in this section.

4.1 Groups

The Groups interface provides management of UNIX-style groups on the FreeNAS® system.

Note: If a directory service is running on the network, it is not necessary to recreate the network's users or groups. Instead, import the existing account information into FreeNAS®. Refer to [Directory Service](#) for details.

This section describes how to create a group and assign user accounts to it. The next section, [Users](#), describes creating user accounts.

Click [Groups](#) → [View Groups](#) to see a screen like [Figure 4.1](#).

All groups that came with the operating system will be listed. Each group has an entry indicating the group ID, group name, whether or not it is a built-in group which was installed with FreeNAS®, and whether or not the group members are allowed to use **sudo**. Clicking a group entry causes a *Members* button to appear. Click the button to view and modify the group membership.

The [Add Group](#) button opens the screen shown in [Figure 4.2](#). [Table 4.1](#) summarizes the available options when creating a group.

The screenshot shows the 'Groups' tab selected under the 'Account' menu. A table lists 28 system groups with their corresponding Group ID, Group Name, Built-in Group status, and Permit Sudo setting. The 'Members' button is visible at the bottom left of the table.

Group ID	Group Name	Built-in Group	Permit Sudo
0	wheel	true	false
1	daemon	true	false
2	kmem	true	false
3	sys	true	false
4	tty	true	false
5	operator	true	false
6	mail	true	false
7	bin	true	false
8	news	true	false
9	man	true	false
13	games	true	false
14	ftp	true	false
20	staff	true	false
22	sshd	true	false
25	smmfsp	true	false
26	mailnull	true	false
31	guest	true	false
53	bind	true	false

Fig. 4.1: Group Management

The dialog box is titled 'Add Group'. It contains fields for 'Group ID' (set to 1001), 'Group Name' (empty), 'Permit Sudo' (unchecked), and 'Allow repeated GIDs' (unchecked). At the bottom are 'OK' and 'Cancel' buttons.

Group ID:	1001
Group Name:	
Permit Sudo:	<input type="checkbox"/>
Allow repeated GIDs:	<input type="checkbox"/>

OK Cancel

Fig. 4.2: Creating a New Group

Table 4.1: Group Creation Options

Setting	Value	Description
Group ID	string	the next available group ID will be suggested for you; 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)
Group Name	string	mandatory
Permit Sudo	checkbox	if checked, members of the group have permission to use sudo; when using sudo, a user will be prompted for their own password
Allow repeated GIDs	checkbox	allows multiple groups to share the same group id (GID); this is useful when a GID is already associated with the UNIX permissions for existing data

After a group and users are created, users can be made members of a group. Highlight the group where users will be assigned, then click the *Members* button. Highlight the user in the *Member users* list (which shows all user accounts on the system) and click *>>* to move that user to the right frame. The user accounts which appear in the right frame are added as members of the group.

In the example shown in Figure 4.3, the *data1* group has been created and the *user1* user account has been created with a primary group of *user1*. The *Members* button for the *data1* group has been selected and *user1* has been added as a member of the group.

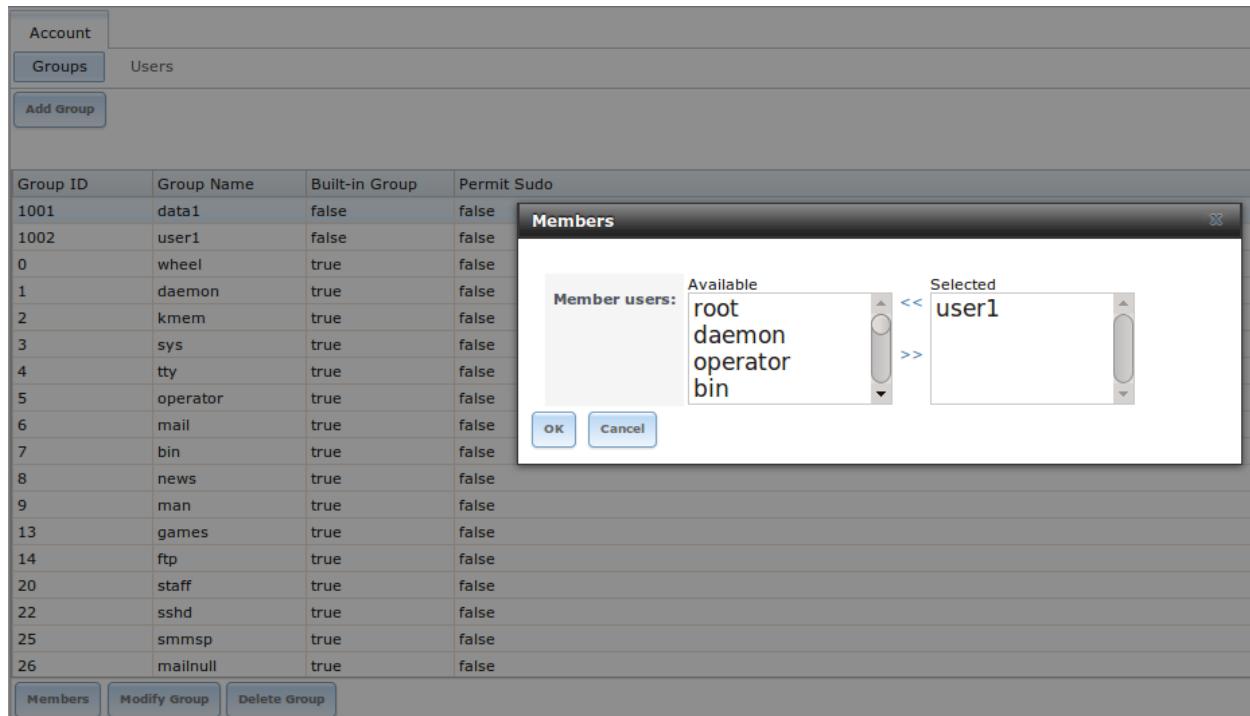


Fig. 4.3: Assigning a User to a Group

The *Delete Group* button deletes a group. The pop-up message asks if you also want to delete all members of that group. Note that the built-in groups do not provide a *Delete Group* button.

4.2 Users

FreeNAS® supports users, groups, and permissions, allowing great flexibility in configuring which users have access to the data stored on FreeNAS®. To assign permissions to shares, **one of the following** must be done:

1. Create a guest account that all users will use or 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*, create a user account with the name *bobsmith* on FreeNAS®. A common strategy is to create groups with different sets of permissions on shares, then assign users to those groups.
2. If your network uses a directory service, import the existing account information using the instructions in *Directory Service*.

Account → Users → View Users provides a listing of all of the system accounts that were installed with the FreeNAS® operating system, as shown in Figure 4.4.

The screenshot shows the 'Users' tab selected in the navigation bar. A table lists 26 system users with the following columns: User ID, Username, Primary Group ID, Home Directory, Shell, Full Name, Built-in User, E-mail, Disable password login, Lock user, Permit Sudo, and Microsoft Account. The table includes rows for root, daemon, operator, bin, tty, kmem, games, news, man, ftp, sshd, smmsp, and mailnull. Buttons for 'Modify User' and 'Change E-mail' are visible at the bottom left of the table area.

User ID	Username	Primary Group ID	Home Directory	Shell	Full Name	Built-in User	E-mail	Disable password login	Lock user	Permit Sudo	Microsoft Account
0	root	0	/root	/bin/csh	root	true		false	false	false	false
1	daemon	1	/root	/usr/sbin/nologin	Owner of many system processes	true		false	false	false	false
2	operator	5	/	/usr/sbin/nologin	System & Binaries	true		false	false	false	false
3	bin	7	/	/usr/sbin/nologin	Commands and Source	true		false	false	false	false
4	tty	65533	/	/usr/sbin/nologin	Tty Sandbox	true		false	false	false	false
5	kmem	2	/	/usr/sbin/nologin	KMem Sandbox	true		false	false	false	false
7	games	13	/	/usr/sbin/nologin	Games pseudo-user	true		false	false	false	false
8	news	8	/	/usr/sbin/nologin	News Subsystem	true		false	false	false	false
9	man	9	/usr/share/man	/usr/sbin/nologin	Mister Man Pages	true		false	false	false	false
14	ftp	14	/nonexistent	/bin/csh		true		false	false	false	false
22	sshd	22	/var/empty	/usr/sbin/nologin	Secure Shell Daemon	true		false	false	false	false
25	smmsp	25	/var/spool/clientmqueue	/usr/sbin/nologin	Sendmail Submission User	true		false	false	false	false
26	mailnull	26	/var/spool	/usr/sbin/nologin	Sendmail Default	true		false	false	false	false

Fig. 4.4: Managing User Accounts

Each account entry indicates the user ID, username, primary group ID, home directory, default shell, full name, whether it is a built-in user that came with the FreeNAS® installation, the email address, whether logins are disabled, whether the user account is locked, whether the user is allowed to use **sudo**, and if the user connects from a Windows 8 or higher system. To reorder the list, click the desired column name. An arrow indicates which column controls the view sort order. Click the arrow to reverse the sort order.

Click a user account to cause these buttons to appear:

- **Modify User:** used to modify the account's settings, as listed in Table 4.2.
- **Change E-mail:** used to change the email address associated with the account.

Note: It is important to set the email address for the built-in *root* user account as important system messages are sent to the *root* user. For security reasons, password logins are disabled for the *root* account and changing this setting is highly discouraged.

Except for the *root* user, the accounts that come with FreeNAS® are system accounts. Each system account is used by a service and should not be used as a login account. For this reason, the default shell on system accounts is *nologin(8)*. For security reasons, and to prevent breakage of system services, do not modify the system accounts.

The *Add User* button opens the screen shown in Figure 4.5. Some settings are only available in *Advanced Mode*. To see these settings, either click the *Advanced Mode* button or configure the system to always display these settings by checking the box *Show advanced fields by default* in System → Advanced . Table 4.2 summarizes the options which are available when user accounts are created or modified.

The screenshot shows the 'Add User' dialog box with the following fields:

- User ID: 1001
- Username: (empty)
- Create a new primary group for the user:
- Primary Group: -----
- Create Home Directory In: /nonexistent
- Shell: csh
- Full Name: (empty)
- E-mail: (empty)
- Password: (empty)
- Password confirmation: (empty)
- Disable password login:
- Lock user:

Fig. 4.5: Adding or Editing a User Account

Table 4.2: User Account Configuration

Setting	Value	Description
User ID	integer	grayed out if user already created; when creating an account, the next numeric ID will be suggested; 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	grayed out if user already created; maximum 16 characters though a maximum of 8 is recommended for interoperability; cannot begin with a hyphen, if a \$ is used it can only be the last character, and it cannot contain a space, tab, or the characters , : + & # % ^ & () ! @ ~ * ? < > = “
Create a new primary group	check-box	by default, a primary group with the same name as the user will be created; uncheck this box to select a different primary group name
Primary Group	drop-down menu	must uncheck <i>Create a new primary group</i> to access this menu; for security reasons, FreeBSD will not give a user su permissions if <i>wheel</i> is their primary group; to give a user su access, add them to the <i>wheel</i> group in <i>Auxiliary groups</i>
Create Home Directory In	browse button	browse to the name of an existing volume or dataset that the user will be assigned permission to access
Home Directory Mode	check-boxes	only available in <i>Advanced Mode</i> and will be read-only for built-in users; sets default Unix permissions of user’s home directory
Shell	drop-down menu	select shell to use for local and SSH logins; see Table 4.3 for an overview of available shells
Full Name	string	mandatory, may contain spaces
E-mail	string	email address associated with the account
Password	string	mandatory unless check box <i>Disable password login</i> ; cannot contain a ?
Password confirmation	string	must match the value of <i>Password</i>
Disable password login	check-box	when checked, disables password logins and authentication to SMB shares; to undo this setting, set a password for the user using the <i>Modify User</i> button for the user in <i>View Users</i> ; checking this box will gray out <i>Lock user</i> and <i>Permit Sudo</i> , which are mutually exclusive
Lock user	check-box	a checked box prevents user from logging in until the account is unlocked (box is unchecked); checking this box will gray out <i>Disable password login</i> which is mutually exclusive
Permit Sudo	check-box	if checked, members of the group have permission to use sudo ; when using sudo, a user will be prompted for their own password
Microsoft Account	check-box	check this box if the user will be connecting from a Windows 8 or higher system
SSH Public Key	string	paste the user’s public key to be used for SSH key authentication (do not paste the private key!)
Auxiliary groups	mouse selection	highlight the group(s) you wish to add the user to and use the >> button to add the user to the highlighted groups

Note: Some fields cannot be changed for built-in users and will be grayed out.

Table 4.3: Available Shells

Shell	Description
net-cli.sh	user can access the Console Setup menu shown in Figure 3.1 , even if it is disabled in System → Advanced → Enable Console Menu
csh	C shell
sh	Bourne shell
tcsh	Enhanced C shell
nologin	use when creating a system account or to create a user account that can authenticate with shares but which cannot login to the FreeNAS system using ssh
bash	Bourne Again shell
ksh93	Korn shell
mksh	mirBSD Korn shell
rbash	Restricted bash
rzsh	Restricted zsh
scponly	select scponly to restrict the user's SSH usage to only the scp and sftp commands
zsh	Z shell
git-shell	restricted git shell

The System section of the administrative GUI contains these entries:

- *Information*: provides general FreeNAS® system information such as hostname, operating system version, platform, and uptime
- *General*: used to configure general settings such as HTTPS access, the language, and the timezone
- *Boot*: used to create, rename, and delete boot environments
- *Advanced*: used to configure advanced settings such as the serial console, swap, and console messages
- *Email*: used to configure the email address to receive notifications
- *System Dataset*: used to configure the location where logs and reporting graphs are stored
- *Tunables*: provides a front-end for tuning in real-time and to load additional kernel modules at boot time
- *Update*: used to perform upgrades and to check for system updates
- *CAs*: used to import or create an internal or intermediate CA (Certificate Authority)
- *Certificates*: used to import existing certificates or to create self-signed certificates
- *Support*: used to report a bug or request a new feature.

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

5.1 Information

System → Information displays general information about the FreeNAS® system. An example is seen in Figure 5.1.

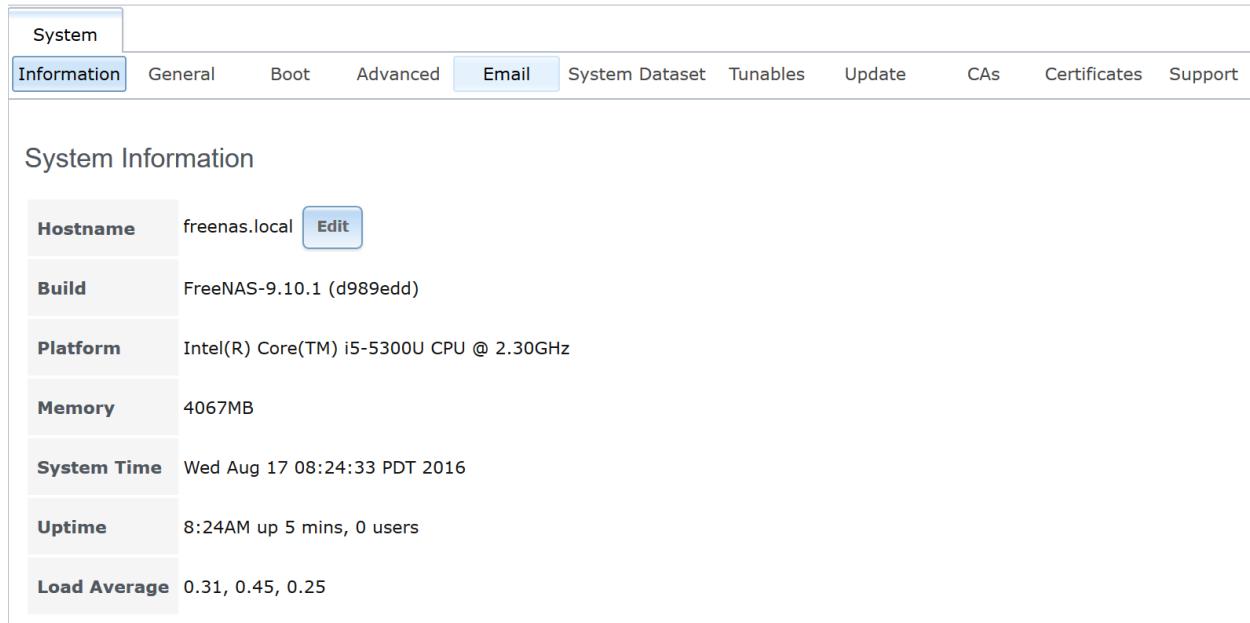
The information includes the hostname, the build version, type of CPU (platform), the amount of memory, the current system time, the system's uptime, and the current load average.

To change the system's hostname, click its *Edit* button, type in the new hostname, and click *OK*. The hostname must include the domain name. If the network does not use a domain name add *.local* to the end of the hostname.

5.2 General

System → General is shown in Figure 5.2.

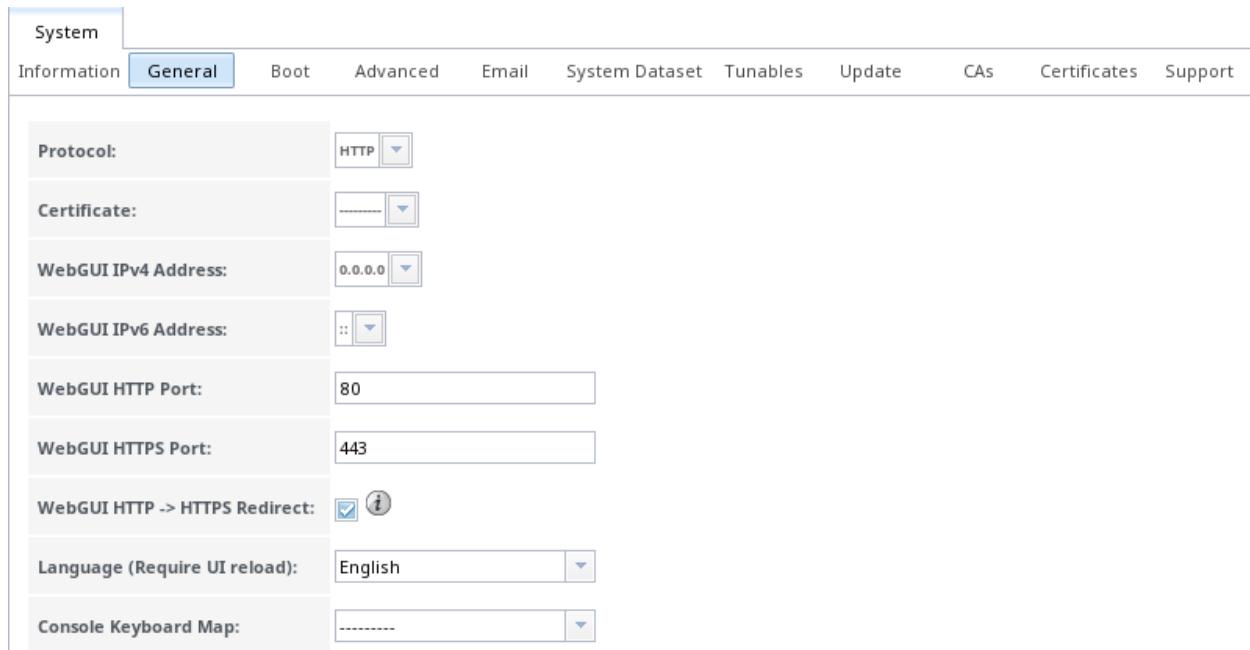
Table 5.1 summarizes the settings that can be configured using the General tab:



The screenshot shows the 'System' tab selected in the top navigation bar. Below it, the 'Information' tab is also selected. The main content area displays various system statistics:

Hostname	freenas.local	Edit
Build	FreeNAS-9.10.1 (d989edd)	
Platform	Intel(R) Core(TM) i5-5300U CPU @ 2.30GHz	
Memory	4067MB	
System Time	Wed Aug 17 08:24:33 PDT 2016	
Uptime	8:24AM up 5 mins, 0 users	
Load Average	0.31, 0.45, 0.25	

Fig. 5.1: System Information Tab



The screenshot shows the 'System' tab selected in the top navigation bar. Below it, the 'General' tab is selected. The main content area contains several configuration fields:

Protocol:	HTTP	<input type="button" value="▼"/>
Certificate:	-----	<input type="button" value="▼"/>
WebGUI IPv4 Address:	0.0.0.0	<input type="button" value="▼"/>
WebGUI IPv6 Address:	::	<input type="button" value="▼"/>
WebGUI HTTP Port:	80	
WebGUI HTTPS Port:	443	
WebGUI HTTP -> HTTPS Redirect:	<input checked="" type="checkbox"/> ⓘ	
Language (Require UI reload):	English	<input type="button" value="▼"/>
Console Keyboard Map:	-----	<input type="button" value="▼"/>

Fig. 5.2: General Screen

Table 5.1: General Configuration Settings

Setting	Value	Description
Protocol	drop-down menu	protocol to use when connecting to the administrative GUI from a browser; if you change the default of <i>HTTP</i> to <i>HTTPS</i> or to <i>HTTP+HTTPS</i> , select the certificate to use in <i>Certificate</i> ; if you do not have a certificate, first create a CA (in CAs), then the certificate itself (in Certificates)
Certificate	drop-down menu	required for <i>HTTPS</i> ; browse to the location of the certificate to use for encrypted connections
WebGUI IPv4 Address	drop-down menu	choose from a list of recent IP addresses to limit the one to use when accessing the administrative GUI; the built-in HTTP server will automatically bind to the wildcard address of <i>0.0.0.0</i> (any address) and will issue an alert if the specified address becomes unavailable
WebGUI IPv6 Address	drop-down menu	choose from a list of recent IPv6 addresses to limit the one to use when accessing the administrative GUI; the built-in HTTP server will automatically bind to any address and will issue an alert if the specified address becomes unavailable
WebGUI HTTP Port	integer	allows you to configure a non-standard port for accessing the administrative GUI over HTTP; changing this setting may require you to change a firefox configuration setting
WebGUI HTTPS Port	integer	allows you to configure a non-standard port for accessing the administrative GUI over HTTPS
WebGUI HTTPS → HTTPS Redirect	checkbox	when this box is checked, <i>HTTP</i> connections will be automatically redirected to <i>HTTPS</i> if <i>HTTPS</i> is selected in <i>Protocol</i> , otherwise such connections will fail
Language	drop-down menu	select the localization from the drop-down menu and reload the browser; view the status of localization at pootle.freenas.org
Console Keyboard Map	drop-down menu	select the keyboard layout
Timezone	drop-down menu	select the timezone from the drop-down menu
Syslog level	drop-down menu	when <i>Syslog server</i> is defined, only logs matching this level are sent
Syslog server	string	<i>IP address_or_hostname:optional_port_number</i> of remote syslog server to send logs to; once set, log entries will be written to both the console and the remote server

After making any changes, click the *Save* button.

This screen also contains these buttons:

Factory Restore: resets the configuration database to the default base version. However, it does not delete user SSH keys or any other data stored in a user's home directory. Since any configuration changes stored in the configuration database will be erased, this option is handy if you mess up your system or wish to return a test system to the original configuration.

Save Config: saves a backup copy of the current configuration database in the format *hostname-version-architecture* to the system being used to access the administrative interface. It is recommended to always save the configuration after making any configuration changes. FreeNAS® automatically backs up the configuration database to the system dataset every morning at 3:45. However, this backup will not occur if the system is shut down at that time. If the system dataset is stored on the boot pool and the boot pool becomes unavailable, the backup will not be available. The

location of the system dataset can be viewed or set using System → System Dataset .

Warning: Passwords are backed up with the system configuration. There are two types of passwords. User account passwords for the base operating system are stored as hashed values, do not need to be encrypted to be secure, and are saved in the system configuration backup. Other passwords, like iSCSI CHAP passwords or Active Directory bind credentials, must be stored in an encrypted form to prevent them from being visible as plain text in the saved system configuration. The key for this encryption is stored on the boot device. If FreeNAS® is installed on a new boot device and a backup system configuration is moved to that new boot device, the key is not present and these other passwords must be re-entered.

Upload Config: allows you to browse to the location of a previously saved configuration file in order to restore that configuration. The screen will turn red as an indication that the system will need to reboot in order to load the restored configuration.

NTP Servers: The network time protocol (NTP) is used to synchronize the time on the computers in a network. Accurate time is necessary for the successful operation of time sensitive applications such as Active Directory or other directory services. By default, FreeNAS® is pre-configured to use three public NTP servers. If your network is using a directory service, ensure that the FreeNAS® system and the server running the directory service have been configured to use the same NTP servers. To add a NTP server on the FreeNAS® system, click NTP Servers → Add NTP Server to open the screen shown in Figure 5.3. Table 5.2 summarizes the options available when adding an NTP server. [ntp.conf\(5\)](#) explains these options in more detail.

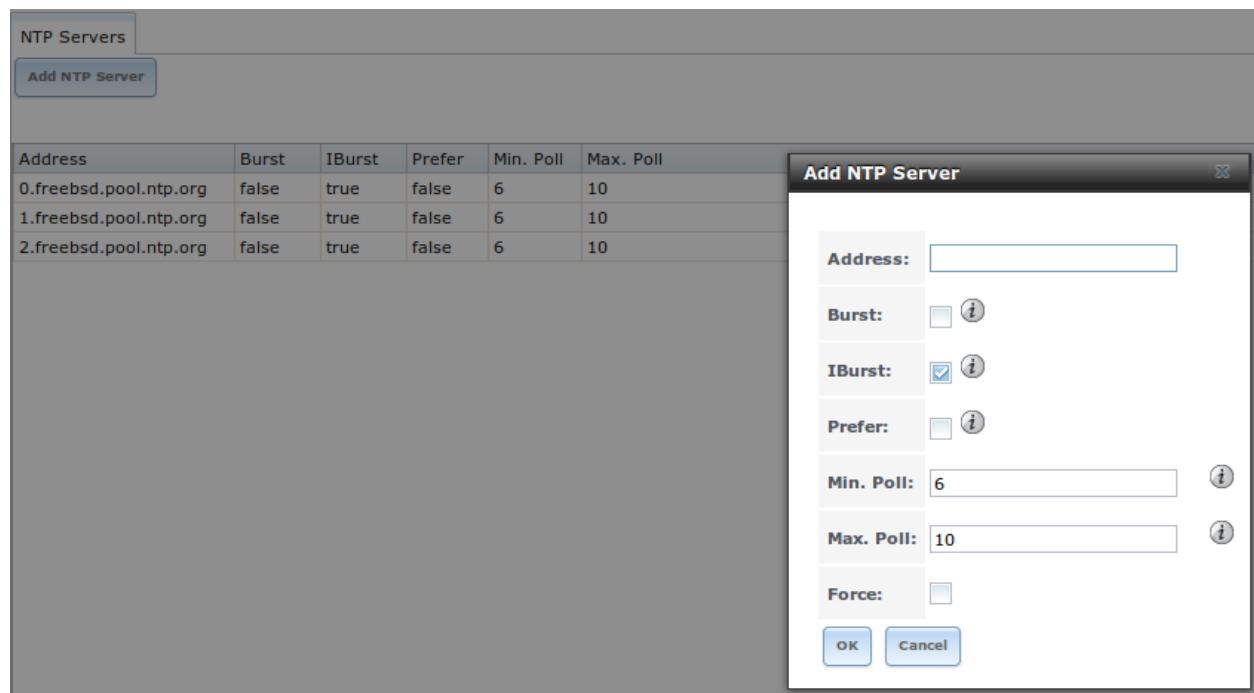


Fig. 5.3: Add an NTP Server

Table 5.2: NTP Servers Configuration Options

Setting	Value	Description
Ad-dress	string	name of NTP server
Burst	check-box	recommended when <i>Max. Poll</i> is greater than 10; only use on your own servers i.e. do not use with a public NTP server
IBurst	check-box	speeds the initial synchronization (seconds instead of minutes)
Prefer	check-box	should only be used for NTP servers that are known to be highly accurate, such as those with time monitoring hardware
Min. Poll	integer	power of 2 in seconds; cannot be lower than 4 or higher than <i>Max. Poll</i>
Max. Poll	integer	power of 2 in seconds; cannot be higher than 17 or lower than <i>Min. Poll</i>
Force	check-box	forces the addition of the NTP server, even if it is currently unreachable

5.3 Boot

FreeNAS® supports a feature of ZFS known as multiple boot environments. With multiple boot environments, the process of updating the operating system becomes a low-risk operation as the updater automatically creates a snapshot of your current boot environment and adds it to the boot menu before applying the update. If the update fails, simply reboot the system and select the previous boot environment from the boot menu to instruct the system to go back to that system state.

Note: Do not confuse boot environments with the configuration database. Boot environments are a snapshot of the *operating system* at a specified time. When a FreeNAS® system boots, it loads the specified boot environment, or operating system, then reads the configuration database in order to load the current configuration values. If your intent is to make configuration changes, rather than operating system changes, make a backup of the configuration database first using *System → General → Save Config*.

As seen in [Figure 5.4](#), two boot environments are created when FreeNAS® is installed. The system will boot into the *default* boot environment and users can make their changes and update from this version. The other boot environment, named *Initial-Install* can be booted into if the system needs to be returned to a pristine, non-configured version of the installation.

If you used the [Initial Configuration Wizard](#), a third boot environment called *Wizard-date* is also created indicating the date and time the wizard was run.

Each boot environment entry contains this information:

- **Name:** the name of the boot entry as it will appear in the boot menu.
- **Active:** indicates which entry will boot by default if the user does not select another entry in the boot menu.
- **Created:** indicates the date and time the boot entry was created.
- **Keep:** indicates whether or not this boot environment can be pruned if an update does not have enough space to proceed. Click the entry's *Keep* button if that boot environment should not be automatically pruned.

Highlight an entry to view its configuration buttons. These configuration buttons are shown:

- **Rename:** used to change the name of the boot environment.

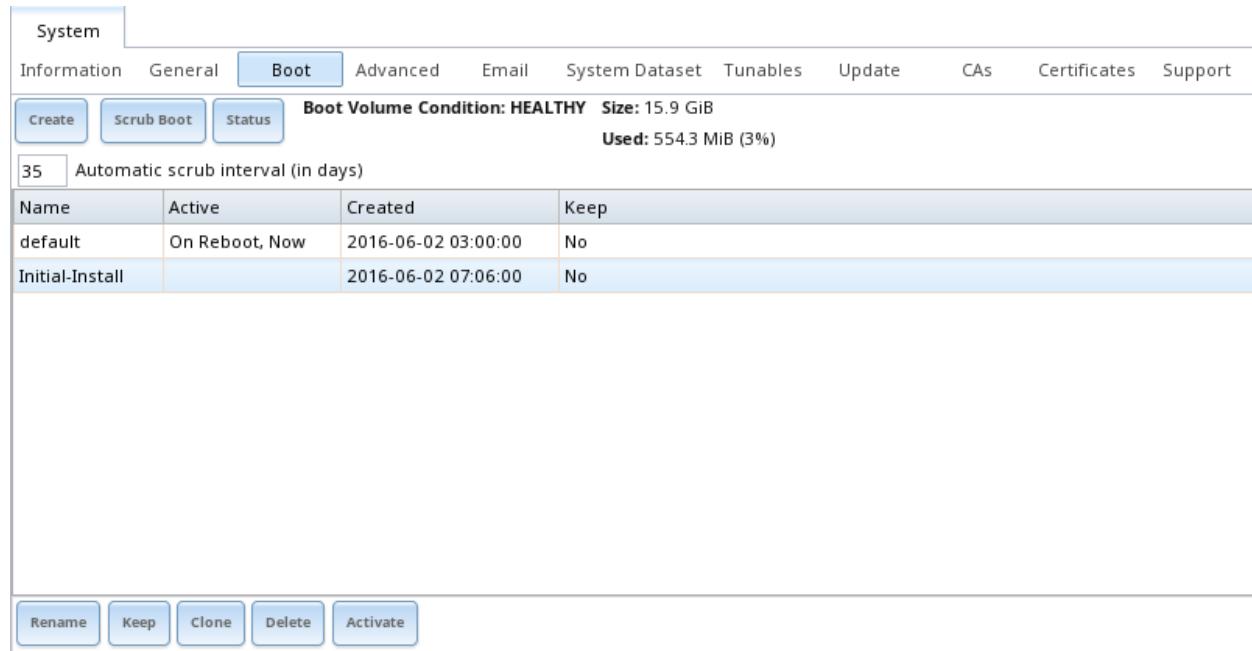


Fig. 5.4: Viewing Boot Environments

- **Keep/Unkeep:** used to toggle whether or not the updater can prune (automatically delete) this boot environment if there is not enough space to proceed with the update.
- **Clone:** used to create a copy of the highlighted boot environment.
- **Delete:** used to delete the highlighted entry, which also removes that entry from the boot menu. Since you cannot delete an entry that has been activated, this button will not appear for the active boot environment. If you need to delete an entry that is currently activated, first activate another entry, which will clear the *On reboot* field of the currently activated entry. Note that this button will not be displayed for the *default* boot environment as this entry is needed in order to return the system to the original installation state.
- **Activate:** only appears on entries which are not currently set to *Active*. Changes the selected entry to the default boot entry on next boot. Its status changes to *On Reboot* and the current *Active* entry changes from *On Reboot, Now* to *Now*, indicating that it was used on the last boot but will not be used on the next boot.

The buttons above the boot entries can be used to:

- **Create:** a manual boot environment. A pop-up menu will prompt you to input a “Name” for the boot environment. When entering the name, only alphanumeric characters, underscores, and dashes are allowed.
- **Scrub Boot:** can be used to perform a manual scrub of the boot devices. By default, the boot device is scrubbed every 35 days. To change the default interval, input a different number in the *Automatic scrub interval (in days)* field. The date and results of the last scrub are also listed in this screen. The condition of the boot device should be listed as *HEALTHY*.
- **Status:** click this button to see the status of the boot devices. In the example shown in Figure 5.5, there is only one boot device and it is *ONLINE*.

If this system has a mirrored boot device and one of the boot devices has a *Status* of *OFFLINE*, click the device to replace, then click its *Replace* button to rebuild the boot mirror.

Note that **you cannot replace the boot device if it is the only boot device** as it contains the operating system itself.

Figure 5.6 shows a sample boot menu.

Boot Status				
Name	Read	Write	Checksum	Status
▲ freenas-boot	0	0	0	ONLINE
▲ stripe	0	0	0	ONLINE
da0p2	0	0	0	ONLINE

Fig. 5.5: Viewing the Status of the Boot Device

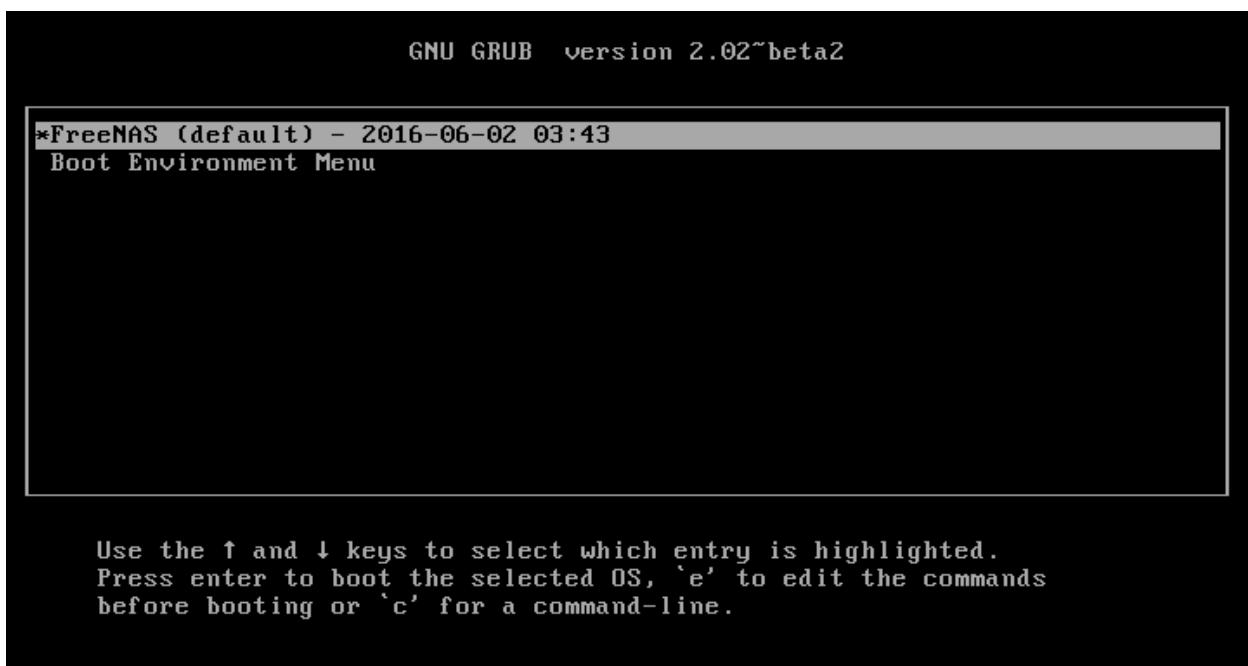


Fig. 5.6: Boot Environments in Boot Menu

The first entry is the active boot environment, or the one that the system has been configured to boot into. To boot into a different boot environment, press the `spacebar` to pause this screen, use the down arrow to select *Boot Environment Menu*, and press `Enter`. A menu displays the other available boot environments. Use the up/down arrows to select the desired boot environment and press `Enter` to boot into it. To always boot into that boot environment, go to `System → Boot`, highlight that entry, and click the *Activate* button.

5.3.1 Mirroring the Boot Device

If the system is currently booting from one device, you can add another device to create a mirrored boot device. This way, if one device fails, the system still has a copy of the boot file system and can be configured to boot from the remaining device in the mirror.

Note: When adding another boot device, it must be the same size (or larger) as the existing boot device. Different models of USB devices which advertise the same size may not necessarily be the same size. For this reason, it is recommended to use the same model of USB drive.

In the example shown in [Figure 5.7](#), the user has clicked `System → Boot → Status` to display the current status of the boot device. The example indicates that there is currently one device, `ada0p2`, its status is *ONLINE*, and it is currently the only boot device as indicated by the word *stripe*. To create a mirrored boot device, click either the entry called *freenas-boot* or *stripe*, then click the *Attach* button. If another device is available, it appears in the *Member disk* drop-down menu. Select the desired device, then click *Attach Disk*.

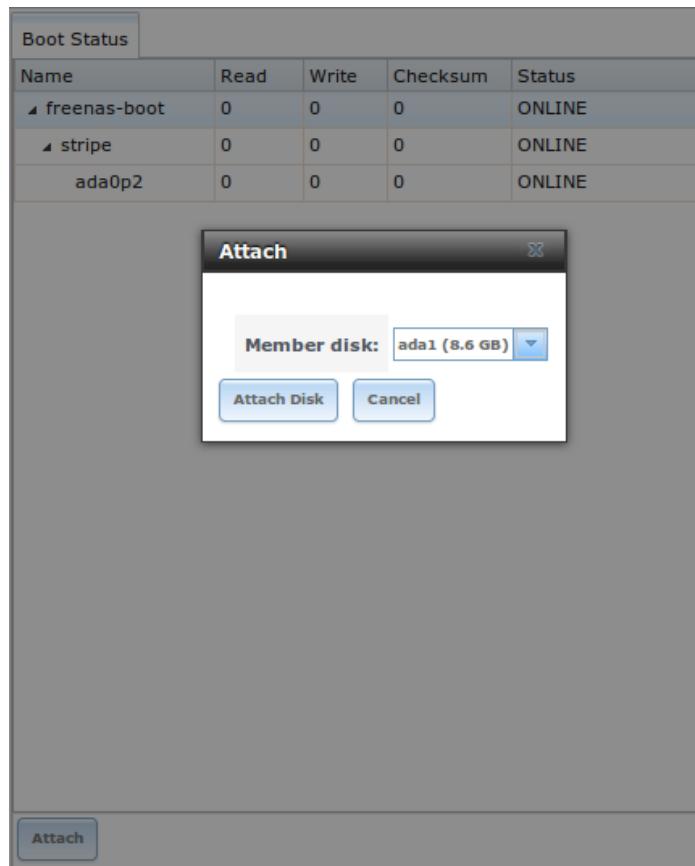


Fig. 5.7: Mirroring a Boot Device

Once the mirror is created, the *Status* screen indicates that it is now a *mirror*. The number of devices in the mirror are shown, as seen in the example in Figure 5.8.

Boot Status				
Name	Read	Write	Checksum	Status
↳ freenas-boot	0	0	0	ONLINE
↳ mirror-0	0	0	0	ONLINE
ada1p2	0	0	0	ONLINE
ada0p2	0	0	0	ONLINE

Fig. 5.8: Viewing the Status of a Mirrored Boot Device

5.4 Advanced

System → Advanced is shown in Figure 5.9. The configurable settings are summarized in Table 5.3.

System	
Information	General
Boot	Advanced
Email	
System Dataset	
Tunables	
Update	
CAs	
Certificates	
Support	

Enable Console Menu:	<input checked="" type="checkbox"/>
Use Serial Console:	<input type="checkbox"/>
Serial Port Address:	0x2f8 <input type="button" value="▼"/> <input type="button" value="i"/>
Serial Port Speed:	9600 <input type="button" value="▼"/> <input type="button" value="i"/>
Enable screen saver:	<input type="checkbox"/>
Enable powerd (Power Saving Daemon):	<input type="checkbox"/>
Swap size on each drive in GiB, affects new disks only. Setting this to 0 disables swap creation completely (STRONGLY DISCOURAGED).	2 <input type="text"/>
Show console messages in the footer:	<input type="checkbox"/>
Show tracebacks in case of fatal errors:	<input checked="" type="checkbox"/>
Show advanced fields by default:	<input type="checkbox"/>
Enable autotune:	<input type="checkbox"/>
Enable debug kernel:	<input type="checkbox"/>

Fig. 5.9: Advanced Screen

Table 5.3: Advanced Configuration Settings

Setting	Value	Description
Enable Console Menu	checkbox	unchecked this box removes the console menu shown in Figure 3.1
Use Serial Console	checkbox	do not check this box if your serial port is disabled
Serial Port Address	string	serial port address written in hex
Serial Port Speed	drop-down menu	select the speed used by the serial port
Enable screen saver	checkbox	enables/disables the console screen saver
Enable powerd (Power Saving Daemon)	checkbox	powerd(8) monitors the system state and sets the CPU frequency accordingly
Swap size	non-zero integer representing GB	by default, all data disks are created with this amount of swap; this setting does not affect log or cache devices as they are created without swap
Show console messages in the footer	checkbox	will display console messages in real time at bottom of browser; click the console to bring up a scrollable screen; check the <i>Stop refresh</i> box in the scrollable screen to pause updating and uncheck the box to continue to watch the messages as they occur
Show tracebacks in case of fatal errors	checkbox	provides a pop-up of diagnostic information when a fatal error occurs
Show advanced fields by default	checkbox	several GUI menus provide an <i>Advanced Mode</i> button to access additional features; enabling this shows these features by default
Enable autotune	checkbox	enables <i>Autotune</i> which attempts to optimize the system depending upon the hardware which is installed
Enable debug kernel	checkbox	if checked, next boot will boot into a debug version of the kernel
Enable automatic upload of kernel crash dumps and daily telemetry	checkbox	if checked, kernel crash dumps and telemetry (some system stats, collectd RRDs, and select syslog messages) are automatically sent to the development team for diagnosis
MOTD banner	string	input the message to be seen when a user logs in via SSH
Periodic Notification User	drop-down menu	select the user to receive security output emails; this output runs nightly but only sends an email when the system reboots or encounters an error
Remote Graphite Server hostname	string	input the IP address or hostname of a remote server that is running a Graphite server

If you make any changes, click the *Save* button.

This tab also contains these buttons:

Backup: used to backup the FreeNAS® configuration and ZFS layout, and, optionally, the data, to a remote system over an encrypted connection. Click this button to open the configuration screen shown in [Figure 5.10](#). [Table 5.4](#) summarizes the configuration options. The only requirement for the remote system is that it has sufficient space to hold the backup and it is running an SSH server on port 22. The remote system does not have to be formatted with ZFS as the backup will be saved as a binary file. To restore a saved backup, use the *12) Restore from a backup* option of the FreeNAS® console menu shown in [Figure 3.1](#).

Warning: The backup and restore options are meant for disaster recovery. If you restore a system, it will be returned to the point in time that the backup was created. If you select the option to save the data, any data created after the backup was made will be lost. If you do **not** select the option to save the data, the system will be recreated with the same ZFS layout, but with **no** data.

Warning: The backup function **IGNORES ENCRYPTED POOLS**. Do not use it to backup systems with encrypted pools.

Save Debug: used to generate a text file of diagnostic information. Once the debug is created, it will prompt for the location to save the generated ASCII text file.

Fig. 5.10: Backup Configuration Screen

Table 5.4: Backup Configuration Settings

Setting	Value	Description
Hostname or IP address	string	input the IP address of the remote system, or the hostname if DNS is properly configured
User name	string	the user account must exist on the remote system and have permissions to write to the <i>Remote directory</i>
Password	string	input and confirm the password associated with the user account
Remote directory	string	the full path to the directory to save the backup to
Backup data	checkbox	by default, the backup is very quick as only the configuration database and the ZFS pool and database layout are saved; check this box to also save the data (which may take some time, depending upon the size of the pool and speed of the network)
Compress backup	checkbox	if checked, gzip will be used to compress the backup which reduces the transmission size when <i>Backup data</i> is checked
Use key authentication	checkbox	if checked, the public key of the <i>root</i> user must be stored in <code>~root/.ssh/authorized_keys</code> on the remote system and that key should not be protected by a passphrase; see <i>Rsync over SSH Mode</i> for instructions on how to generate a key pair

5.4.1 Autotune

FreeNAS® provides an autotune script which attempts to optimize the system depending upon the hardware which is installed. For example, if a ZFS volume exists on a system with limited RAM, the autotune script will automatically adjust some ZFS sysctl values in an attempt to minimize ZFS memory starvation issues. It should only be used as a temporary measure on a system that hangs until the underlying hardware issue is addressed by adding more RAM. Autotune will always slow the system down as it caps the ARC.

The *Enable autotune* checkbox in System → Advanced is unchecked by default. Check this box to run the autotuner at boot time. If you would like the script to run immediately, the system must be rebooted.

If the autotune script finds any settings that need adjusting, the changed values will appear in System → Tunables . If you do not like the changes, you can modify the values that are displayed in the GUI and your changes will override the values that were created by the autotune script. However, if you delete a tunable that was created by autotune, it will be recreated at next boot. This is because autotune only creates values that do not already exist.

If you are trying to increase the performance of your FreeNAS® system and suspect that the current hardware may be limiting performance, try enabling autotune.

If you wish to read the script to see which checks are performed, the script is located in /usr/local/bin/autotune .

5.5 Email

System → Email , shown in Figure 5.11, is used to configure the email settings on the FreeNAS® system. Table 5.5 summarizes the settings that can be configured using the Email tab.

Note: It is important to configure the system so that it can successfully send emails. An automatic script sends a nightly email to the *root* user account containing important information such as the health of the disks. *Alert* events are also emailed to the *root* user account.

Table 5.5: Email Configuration Settings

Setting	Value	Description
From email	string	the from email address to be used when sending email notifications
Outgoing mail server	string or IP address	hostname or IP address of SMTP server
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 <i>Plain</i> , <i>SSL</i> , or <i>TLS</i>
Use SMTP Authentication	checkbox	enables/disables SMTP AUTH using PLAIN SASL; if checked, enter the required <i>Username</i> and <i>Password</i>
Username	string	enter the username if the SMTP server requires authentication
Password	string	enter the password if the SMTP server requires authentication

Click the *Send Test Mail* button to verify that the configured email settings are working. If the test email fails, double-check the destination email address by clicking the *Change E-mail* button for the *root* account in Account → Users → View Users . Test mail cannot be sent unless the *root* email address has been set.

From email: ⓘ

Outgoing mail server: ⓘ

Port to connect to: ⓘ

TLS/SSL: Plain ⓘ

Use SMTP Authentication:

Username: ⓘ

Password:

Password confirmation: ⓘ

HINT: Test e-mails are sent to root user. To configure it use Account -> Users -> View Users -> root -> Change E-mail

Fig. 5.11: Email Screen

5.6 System Dataset

System → System Dataset , shown in Figure 5.12, is used to select the pool which will contain the persistent system dataset. The system dataset stores debugging core files and Samba4 metadata such as the user/group cache and share level permissions. If the FreeNAS® system is configured to be a Domain Controller, all of the domain controller state is stored there as well, including domain controller users and groups.

System dataset pool: ⓘ

Syslog:

Reporting Database: ⓘ

Note: Encrypted volumes are not displayed in the System dataset pool drop-down menu.

Fig. 5.12: System Dataset Screen

Note: Encrypted volumes are not displayed in the *System dataset pool* drop-down menu.

The system dataset can optionally be configured to also store the system log and *Reporting* information. If there are lots of log entries or reporting information, moving these to the system dataset will prevent `/var/` on the device

holding the operating system from filling up as `/var/` has limited space.

Use the drop-down menu to select the ZFS volume (pool) to contain the system dataset. Whenever the location of the system dataset is changed, a pop-up warning will indicate that the SMB service needs to be restarted, which will result in a temporary outage of any active SMB connections.

To store the system log on the system dataset, check the *Syslog* box.

To store the reporting information on the system dataset, check the *Reporting Database* box.

If you make any changes, click the *Save* button to save them.

If you change the pool storing the system dataset at a later time, FreeNAS® will automatically migrate the existing data in the system dataset to the new location.

5.7 Tunables

System → Tunables can be used to manage the following:

1. **FreeBSD sysctls:** a `sysctl(8)` makes changes to the FreeBSD kernel running on a FreeNAS® system and can be used to tune the system.
2. **FreeBSD loaders:** a loader is only loaded when a FreeBSD-based system boots and can be used to pass a parameter to the kernel or to load an additional kernel module such as a FreeBSD hardware driver.
3. **FreeBSD rc.conf options:** `rc.conf(5)` is used to pass system configuration options to the system startup scripts as the system boots. Since FreeNAS® has been optimized for storage, not all of the services mentioned in `rc.conf(5)` are available for configuration. Note that in FreeNAS®, customized `rc.conf` options are stored in `/tmp/rc.conf.freenas`.

Warning: Adding a sysctl, loader, or `rc.conf` option is an advanced feature. A sysctl immediately affects the kernel running the FreeNAS® system and a loader could adversely affect the ability of the FreeNAS® system to successfully boot. **Do not create a tunable on a production system unless you understand and have tested the ramifications of that change.**

Since sysctl, loader, and `rc.conf` values are specific to the kernel parameter to be tuned, the driver to be loaded, or the service to configure, descriptions and suggested values can be found in the man page for the specific driver and in many sections of the [FreeBSD Handbook](#).

To add a loader, sysctl, or `rc.conf` option, go to System → Tunables → Add Tunable , to access the screen shown in seen in Figure 5.13.

Table 5.6 summarizes the options when adding a tunable.

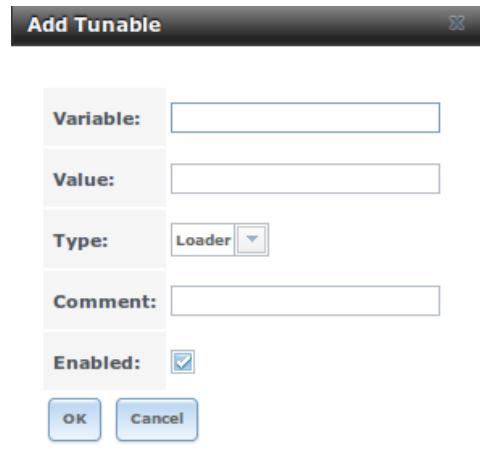


Fig. 5.13: Adding a Tunable

Table 5.6: Adding a Tunable

Setting	Value	Description
Variable	string	typically the name of the sysctl or driver to load, as indicated by its man page
Value	integer or string	value to associate with <i>Variable</i> ; typically this is set to <i>YES</i> to enable the sysctl or driver specified by the “Variable”
Type	drop-down menu	choices are <i>Loader</i> , <i>rc.conf</i> , or <i>Sysctl</i>
Comment	string	optional, but a useful reminder for the reason behind adding this tunable
Enabled	checkbox	uncheck if you would like to disable the tunable without deleting it

Note: As soon as a *Sysctl* is added or edited, the running kernel changes that variable to the value specified. However, when a *Loader* or *rc.conf* value is changed, it does not take effect until the system is rebooted. Regardless of the type of tunable, changes persist at each boot and across upgrades unless the tunable is deleted or its *Enabled* checkbox is unchecked.

Any tunables that you add will be listed in *System → Tunables*. To change the value of an existing tunable, click its *Edit* button. To remove a tunable, click its *Delete* button.

Some sysctls are read-only, meaning that they require a reboot in order to enable their setting. You can determine if a sysctl is read-only by first attempting to change it from *Shell*. For example, to change the value of *net.inet.tcp.delay_ack* to *1*, use the command `sysctl net.inet.tcp.delay_ack=1`. If the sysctl value is read-only, an error message will indicate that the setting is read-only. If you do not get an error, the setting is now applied. For the setting to be persistent across reboots, the sysctl must still be added in *System → Tunables*.

The GUI does not display the sysctls that are pre-set when FreeNAS® is installed. FreeNAS® 9.10.1-U2 ships with the following sysctls set:

```
kern.metadelay=3
kern.dirdelay=4
kern.filedelay=5
kern.coredump=1
```

```
kern.sugid_coredump=1  
net.inet.tcp.delayed_ack=0  
vfs.timestamp_precision=3
```

Do not add or edit these default sysctls as doing so may render the system unusable.

The GUI does not display the loaders that are pre-set when FreeNAS® is installed. FreeNAS® 9.10.1-U2 ships with these loaders set:

```
autoboot_delay="2"  
loader_logo="freenas"  
loader_menu_title="Welcome to FreeNAS"  
loader_brand="freenas-brand"  
loader_version=" "  
kern.cam.boot_delay="30000"  
debug.debugger_on_panic=1  
debug.ddb.textdump.pending=1  
hw.hptrr.attach_generic=0  
vfs.mountroot.timeout="30"  
ispfw_load="YES"  
hint.isp.0.role=2  
hint.isp.1.role=2  
hint.isp.2.role=2  
hint.isp.3.role=2  
module_path="/boot/kernel;/boot/modules;/usr/local/modules"  
net.inet6.ip6.auto_linklocal="0"  
vfs.zfs.vol.mode=2  
kern.geom.label.disk_ident.enable="0"  
hint.ahciem.0.disabled="1"  
hint.ahciem.1.disabled="1"  
kern.msgbufsize="524288"  
hw.usb.no_shutdown_wait=1
```

Do not add or edit the default tunables as doing so might make the system unusable.

The ZFS version used in 9.10.1-U2 deprecates these tunables:

```
vfs.zfs.write_limit_override  
vfs.zfs.write_limit_inflated  
vfs.zfs.write_limit_max  
vfs.zfs.write_limit_min  
vfs.zfs.write_limit_shift  
vfs.zfs.no_write_throttle
```

If you upgrade from an earlier version of FreeNAS® where these tunables are set, they will automatically be deleted for you. You should not try to add these tunables back.

5.8 Update

FreeNAS® has an integrated update system to make it easy to keep up to date.

5.8.1 Preparing for Updates

It is best to perform updates at times the FreeNAS® system is idle, with no clients connected and no scrubs or other disk activity going on. A reboot is required after most updates, so they are often planned for scheduled maintenance

times to avoid disrupting user activities.

5.8.2 Updates and Trains

FreeNAS® is updated with signed update files. This provides flexibility in deciding when to upgrade the system with patches, new drivers, or new features. It also allows “test driving” an upcoming release. Combined with boot environments, new features or system patches can be tested while still being able to revert to a previous version of the operating system (see [If Something Goes Wrong](#)). Digital signing of update files eliminates the need to manually download both an upgrade file and the associated checksum to verify file integrity.

Figure 5.14 shows an example of the System → Update screen.

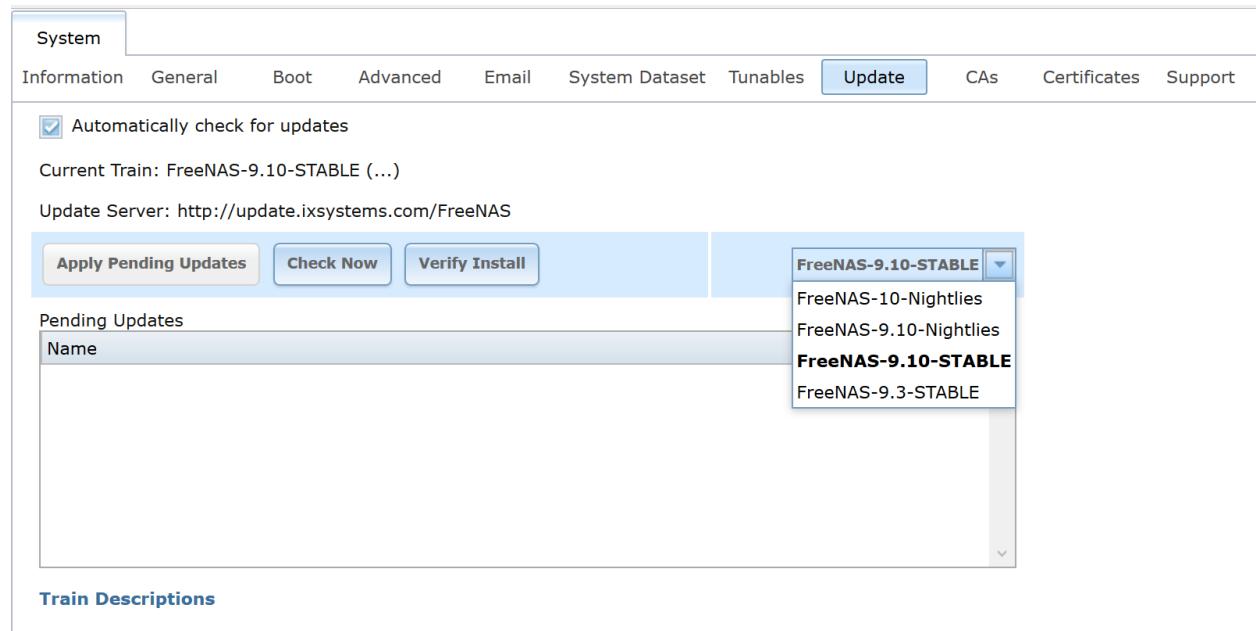


Fig. 5.14: Update Options

By default, the system automatically checks for updates and issues an alert when a new update becomes available. The automatic check can be disabled by unchecking *Automatically check for updates*.

This screen also shows which software branch, or *train*, is being tracked for updates. These trains are available:

- **FreeNAS-10-Nightlies:** this train should **not be used in production**. It represents the experimental branch for the future 10 version and is meant only for bleeding edge testers and developers.
- **FreeNAS-9.10-Nightlies:** this train has the latest, but still being tested, fixes and features. Unless you are testing a new feature, you do not want to run this train in production.
- **FreeNAS-9.10-STABLE:** this is the **recommended train for production use**. Once new fixes and features have been tested, they are added to this train. It is recommended to follow this train and to apply any of its pending updates.
- **FreeNAS-9.3-STABLE:** this is the maintenance-only mode for an older version of FreeNAS®. It is recommended to upgrade to *FreeNAS-9.10-STABLE*, by selecting that train, to ensure that the system receives bug fixes and new features.

To change the train, use the drop-down menu to make a different selection.

Note: The train selector does not allow downgrades. For example, the STABLE train cannot be selected while booted into a Nightly boot environment, or a 9.3 train cannot be selected while booted into a 9.10 boot environment. If you have been testing or running a more recent version and wish to go back to an earlier version, reboot and select a boot environment for that earlier version. You can then use this screen to see if any updates are available for that train.

This screen also lists the URL of the official update server should that information be needed in a network with outbound firewall restrictions.

The *Verify Install* button goes through the operating system files in the current installation, looking for any inconsistencies. When finished, a pop-up menu lists any files with checksum mismatches or permission errors.

5.8.3 Checking for Updates

To see if any updates are available, make sure the desired train is selected and click the *Check Now* button. Any available updates are listed. In the example shown in [Figure 5.15](#), the numbers which begin with a # represent the bug report number from bugs.freenas.org. Numbers which do not begin with a # represent a git commit. Click the *ChangeLog* hyperlink to open the log of changes in a web browser. Click the *ReleaseNotes* hyperlink to open the Release Notes in the browser.

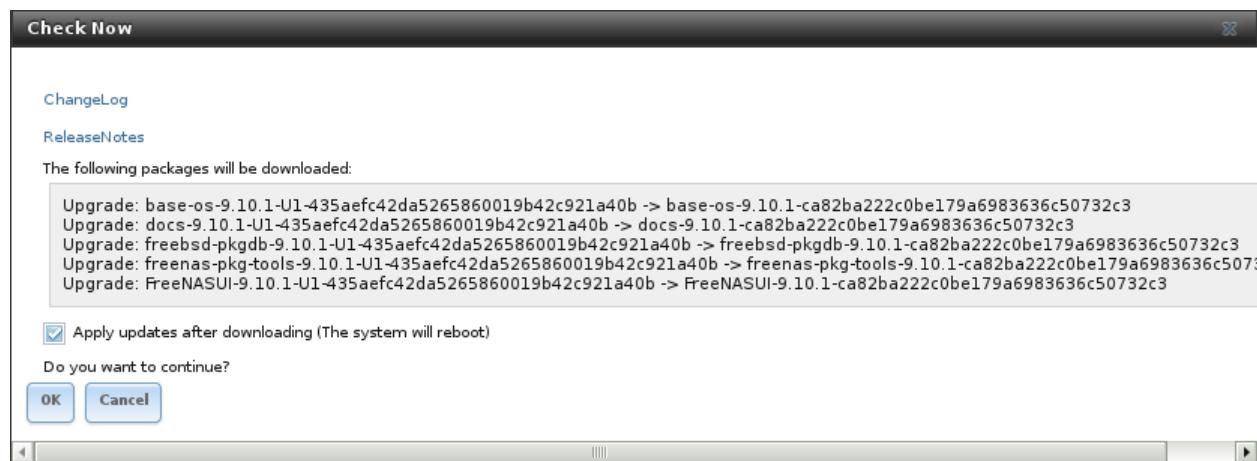


Fig. 5.15: Reviewing Updates

5.8.4 Applying Updates

Make sure the system is in a low-usage state as described above in [Preparing for Updates](#).

Click the *OK* button to download and apply the updates. Be aware that some updates automatically reboot the system after they are applied.

Warning: Each update creates a boot environment. If the update process needs more space, it attempts to remove old boot environments. Boot environments marked with the *Keep* attribute as shown in [Boot](#) will not be removed. If space for a new boot environment is not available, the upgrade fails. Space on the boot device can be manually freed using [System → Boot](#). Review the boot environments and remove the *Keep* attribute or delete any boot environments that are no longer needed.

Updates can also be downloaded and applied later. To do so, uncheck the *Apply updates after downloading* box before pressing *OK*. In this case, this screen closes after updates are downloaded. Downloaded updates are listed in the *Pending Updates* section of the screen shown in [Figure 5.14](#). When ready to apply the previously downloaded updates, click the *Apply Pending Updates* button. Remember that the system might reboot after the updates are applied.

Warning: After updates have completed, reboot the system. Configuration changes made after an update but before that final reboot will not be saved.

5.9 CAs

FreeNAS® can act as a Certificate Authority (CA). If you plan to use SSL or TLS to encrypt any of the connections to the FreeNAS® system, you will need to first create a CA, then either create or import the certificate to be used for encrypted connections. Once you do this, the certificate will appear in the drop-down menus for all the services that support SSL or TLS.

[Figure 5.16](#) shows the screen after clicking System → CAs .

Name	Internal	Issuer	Certificates	Distinguished Name	From	Until
No entry has been found						

Fig. 5.16: Initial CA Screen

If your organization already has a CA, the CA's certificate and key can be imported. Click the *Import CA* button to open the configuration screen shown in [Figure 5.17](#). The configurable options are summarized in [Table 5.7](#).

Table 5.7: Importing a CA Options

Setting	Value	Description
Name	string	mandatory; enter a descriptive name for the CA
Certificate	string	mandatory; paste in the certificate for the CA
Private Key	string	if there is a private key associated with the <i>Certificate</i> , paste it here
Passphrase	string	if the <i>Private Key</i> is protected by a passphrase, enter it here and repeat it in the “Confirm Passphrase” field
Serial	string	mandatory; enter the serial number for the certificate

To instead create a new CA, first decide if it will be the only CA which will sign certificates for internal use or if the CA will be part of a [certificate chain](#).

To create a CA for internal use only, click the *Create Internal CA* button which will open the screen shown in [Figure 5.18](#).

The configurable options are described in [Table 5.8](#). When completing the fields for the certificate authority, supply the information for your organization.

Import Certificate Authority

Name:	<input type="text"/>	i
Certificate:	<input type="text"/>	i
Private Key:	<input type="text"/>	i
Passphrase:	<input type="text"/>	i
Confirm Passphrase:	<input type="text"/>	
Serial:	<input type="text"/>	i

OK Cancel

Fig. 5.17: Importing a CA

Create Internal CA

Name:	<input type="text"/>	i
Key length:	2048	▼
Digest Algorithm:	SHA256	▼
Lifetime:	3,650	
Country:	United States	▼ i
State:	<input type="text"/>	i
Locality:	<input type="text"/>	i
Organization:	<input type="text"/>	i
Email Address:	<input type="text"/>	i
Common Name:	<input type="text"/>	i

OK Cancel

Fig. 5.18: Creating an Internal CA

Table 5.8: Internal CA Options

Setting	Value	Description
Name	string	required; enter a descriptive name for the CA
Key Length	drop-down menu	for security reasons, a minimum of 2048 is recommended
Digest Algorithm	drop-down menu	the default is acceptable unless your organization requires a different algorithm
Lifetime	integer	in days
Country	drop-down menu	select the country for the organization
State	string	required; enter the state or province of the organization
Locality	string	required; enter the location of the organization
Organization	string	required; enter the name of the company or organization
Email Address	string	required; enter the email address for the person responsible for the CA
Common Name	string	required; enter the fully-qualified hostname (FQDN) of the FreeNAS® system

To instead create an intermediate CA which is part of a certificate chain, click the *Create Intermediate CA* button. This screen adds one more option to the screen shown in [Figure 5.18](#):

- **Signing Certificate Authority:** this drop-down menu is used to specify the root CA in the certificate chain. This CA must first be imported or created.

Any CAs that you import or create will be added as entries in `System → CAs`. The columns in this screen will indicate the name of the CA, whether or not it is an internal CA, whether or not the issuer is self-signed, the number of certificates that have been issued by the CA, the distinguished name of the CA, the date and time the CA was created, and the date and time the CA expires.

If you click the entry for a CA, the following buttons become available:

- **Export Certificate:** will prompt to browse to the location, on the system being used to access the FreeNAS® system, to save a copy of the CA's X.509 certificate.
- **Export Private Key:** will prompt to browse to the location, on the system being used to access the FreeNAS® system, to save a copy of the CA's private key. Note that this option only appears if the CA has a private key.
- **Delete:** will prompt to confirm before deleting the CA.

5.10 Certificates

FreeNAS® can import existing certificates, create new certificates, and issue certificate signing requests so that created certificates can be signed by the CA which was previously imported or created in [CAs](#).

[Figure 5.19](#) shows the initial screen if you click `System → Certificates`.

To import an existing certificate, click the *Import Certificate* button to open the configuration screen shown in [Figure 5.20](#). When importing a certificate chain, paste the primary certificate, followed by any intermediate certificates, followed by the root CA certificate.

The configurable options are summarized in [Table 5.9](#).

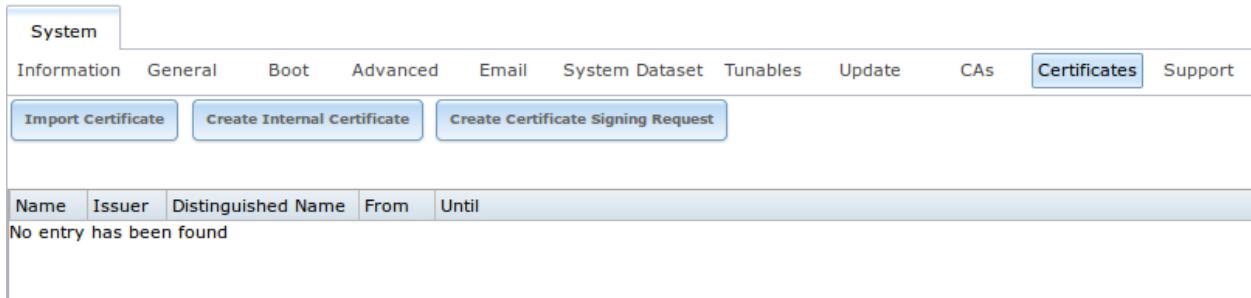


Fig. 5.19: Initial Certificates Screen

The dialog box is titled 'Import Certificate'. It contains five input fields: 'Name' (with a red border), 'Certificate' (with an info icon), 'Private Key' (with an info icon), 'Passphrase' (with an info icon), and 'Confirm Passphrase' (with an info icon). At the bottom are 'OK' and 'Cancel' buttons.

Fig. 5.20: Importing a Certificate

Table 5.9: Certificate Import Options

Setting	Value	Description
Name	string	required; enter a descriptive name for the certificate; cannot contain the “ (quote) character
Certificate	string	required; paste the contents of the certificate
Private Key	string	required; paste the private key associated with the certificate
Passphrase	string	if the private key is protected by a passphrase, enter it here and repeat it in the <i>Confirm Passphrase</i> field

To instead create a new self-signed certificate, click the *Create Internal Certificate* button to see the screen shown in Figure 5.21. The configurable options are summarized in Table 5.10. When completing the fields for the certificate authority, use the information for your organization. Since this is a self-signed certificate, use the CA that you imported or created using *CA*s as the signing authority.

Fig. 5.21: Creating a New Certificate

Table 5.10: Certificate Creation Options

Setting	Value	Description
Signing Certificate Authority	drop-down menu	required; select the CA which was previously imported or created using CAs
Name	string	required; enter a descriptive name for the certificate; cannot contain the “ (quote) character
Key Length	drop-down menu	for security reasons, a minimum of 2048 is recommended
Digest Algorithm	drop-down menu	the default is acceptable unless your organization requires a different algorithm
Lifetime	integer	in days
Country	drop-down menu	select the country for the organization
State	string	required; enter the state or province for the organization
Locality	string	required; enter the location for the organization
Organization	string	required; enter the name of the company or organization
Email Address	string	required; enter the email address for the person responsible for the CA
Common Name	string	required; enter the fully-qualified hostname (FQDN) of the FreeNAS® system

If you need to use a certificate that is signed by an external CA, such as Verisign, instead create a certificate signing request. To do so, click the *Create Certificate Signing Request* button. A screen like the one in [Figure 5.21](#) opens, but without the *Signing Certificate Authority* field.

All certificates that you import, self-sign, or make a certificate signing request for will be added as entries to System → Certificates. In the example shown in [Figure 5.22](#), a self-signed certificate and a certificate signing request have been created for the fictional organization *My Company*. The self-signed certificate was issued by the internal CA named *My Company* and the administrator has not yet sent the certificate signing request to Verisign so that it can be signed. Once that certificate is signed and returned by the external CA, it should be imported using the *Import Certificate* button so that is available as a configurable option for encrypting connections.

If you click an entry, it will activate the following configuration buttons:

- **View:** once a certificate is created, it cannot be edited. The *Name*, *Certificate*, and *Private Key* fields can be viewed. If a certificate must be changed, *Delete* and recreate it.
- **Export Certificate:** used to save a copy of the certificate or certificate signing request to the system being used to access the FreeNAS® system. For a certificate signing request, send the exported certificate to the external signing authority so that it can be signed.
- **Export Private Key:** used to save a copy of the private key associated with the certificate or certificate signing request to the system being used to access the FreeNAS® system.
- **Delete:** used to delete a certificate or certificate signing request.

5.11 Support

The FreeNAS® *Support* tab, shown in [Figure 5.23](#), provides a built-in ticketing system for generating bug reports and feature requests.

This screen provides a built-in interface to the FreeNAS® bug tracker located at bugs.freenas.org. If you have not yet used the FreeNAS® bug tracker, you must first go to that website, click the *Register* link, fill out the form, and reply to the registration email. This will create a username and password which can be used to create bug reports and receive notifications as the reports are actioned.

The screenshot shows the 'Certificates' tab of the FreeNAS System configuration. At the top, there are three buttons: 'Import Certificate', 'Create Internal Certificate', and 'Create Certificate Signing Request'. Below this is a table listing certificates:

Name	Issuer	Distinguished Name	From	Until
self-signed cert	myCA	/C=US/ST=CA/L=San Jose/O=My Company/CN=Cert Wrangler/emailAddress=2014	Thu Nov 20 20:30:39 2024	Sun Nov 17 20:30:39 2024
versign cert	external - signature pending	/C=US/ST=CA/L=San Jose/O=My Company/CN=Cert Wrangler/emailAddress=		

At the bottom, there are four buttons: 'View', 'Export Certificate', 'Export Private Key', and 'Delete'.

Fig. 5.22: Managing Certificates

The screenshot shows the 'Support' tab of the FreeNAS System configuration. It includes a message about reporting bugs and a registration link. Below is a form for creating a new support ticket:

If you do not have an account, please [register](#).

Before filing a bug report or feature request, search <http://bugs.freenas.org> to ensure the issue has not already been reported. If it has, add a comment to the existing issue instead of creating a new one.
For enterprise-grade storage solutions and support, please visit <http://www.ixsystems.com/storage/>.

Username:

Password:

Type:

Category:

Attach Debug Info:

Subject:

Description:

Fig. 5.23: Support Tab

Before creating a bug report or feature request, ensure that an existing report does not already exist at bugs.freenas.org. If you find a similar issue that is not yet marked as *closed* or *resolved*, add a comment to that issue if you have new information to provide that can assist in resolving the issue. If you find a similar issue that is marked as *closed* or *resolved*, you can create a new issue and refer to the earlier issue number.

Note: If you are not updated to the latest version of STABLE, do that first to see if it resolves your issue.

To generate a report using the built-in *Support* screen, complete the following fields:

- **Username:** enter the login name created when registering at bugs.freenas.org.
- **Password:** enter the password associated with the registered login name.
- **Type:** select *Bug* when reporting an issue or *Feature* when requesting a new feature.
- **Category:** this drop-down menu is empty a registered “Username” and “Password” are entered. An error message is displayed if either value is incorrect. After the *Username* and *Password* are validated, possible categories are populated to the drop-down menu. Select the one that best describes the bug or feature being reported.
- **Attach Debug Info:** it is recommended to leave this box checked so that an overview of the system’s hardware, build string, and configuration is automatically generated and included with the ticket.
- **Subject:** input a descriptive title for the ticket. A good *Subject* makes it easy for you and other users to find similar reports.
- **Description:** input a 1 to 3 paragraph summary of the issue that describes the problem, and if applicable, what steps one can do to reproduce it.
- **Attachments:** this is the only optional field. It is useful for including configuration files or screenshots of any errors or tracebacks.

Once you have finished completing the fields, click the *Submit* button to automatically generate and upload the report to bugs.freenas.org. A pop-up menu provides a clickable URL so to view status or add additional information to the report.

**CHAPTER
SIX**

TASKS

The Tasks section of the administrative GUI can be used to configure the following repetitive tasks:

- *Cron Jobs*: allows you to schedule a command or script to automatically execute at a specified time
- *Init/Shutdown Scripts*: used to configure a command or script to automatically execute during system startup or shutdown
- *Rsync Tasks*: allows you to schedule data synchronization to another system
- *S.M.A.R.T. Tests*: allows you to schedule how often disk tests occur

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

Note: By default, *Scrubs* are run once a month by an automatically-created task. *S.M.A.R.T. Tests* and *Periodic Snapshot Tasks* must be set up manually.

6.1 Cron Jobs

crond(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.

Figure 6.1 shows the screen that opens when you click Tasks → Cron Jobs → Add Cron Job .

Table 6.1 summarizes the configurable options when creating a cron job.

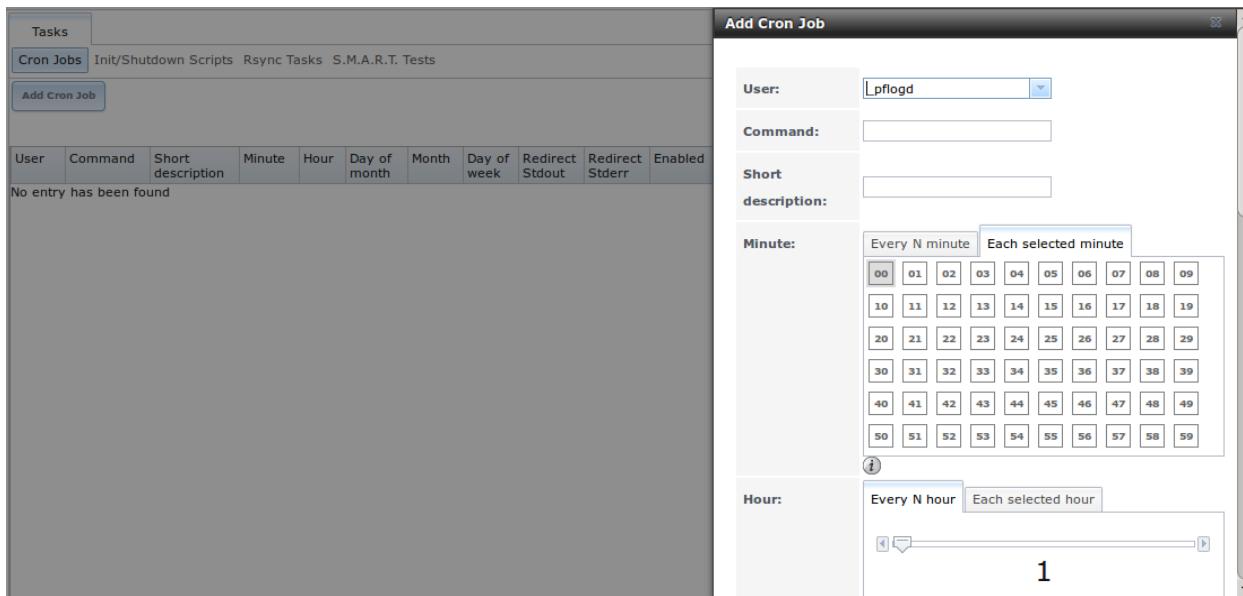


Fig. 6.1: Creating a Cron Job

Table 6.1: Cron Job Options

Setting	Value	Description
User	drop-down menu	make sure the selected user has permission to run the specified command or script
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
Short description	string	optional
Minute	slider or minute selections	with the slider, the cron job occurs every N minutes; with minute selections, the cron job occurs at the highlighted minutes
Hour	slider or hour selections	with the slider, the cron job occurs every N hours; with hour selections, the cron job occurs at the highlighted hours
Day of month	slider or month selections	with the slider, cron job occurs every N days; with day selections, cron job occurs on the highlighted days each month
Month	checkboxes	cron job occurs on the selected months
Day of week	checkboxes	cron job occurs on the selected days
Redirect Stdout	checkbox	disables emailing standard output to the <i>root</i> user account
Redirect Stderr	checkbox	disables emailing errors to the <i>root</i> user account
Enabled	checkbox	uncheck disable the cron job without deleting it

Created cron jobs will be listed in *View Cron Jobs*. Highlight a cron job entry to display buttons to *Edit*, *Delete*, or *Run Now*.

6.2 Init/Shutdown Scripts

FreeNAS® provides the ability to schedule commands or scripts to run at system startup or shutdown.

Figure 6.2 shows the screen that opens when you click Tasks → Init/Shutdown Scripts → Add Init/Shutdown Script. Table 6.2 summarizes the available options.

When scheduling a command, make sure that the command is in your path or give the full path to the command. One way to test the path is to type **which command_name**. If the command is not found, it is not in your path.

When scheduling a script, make sure that the script is executable and has been fully tested to ensure that it achieves the desired results.

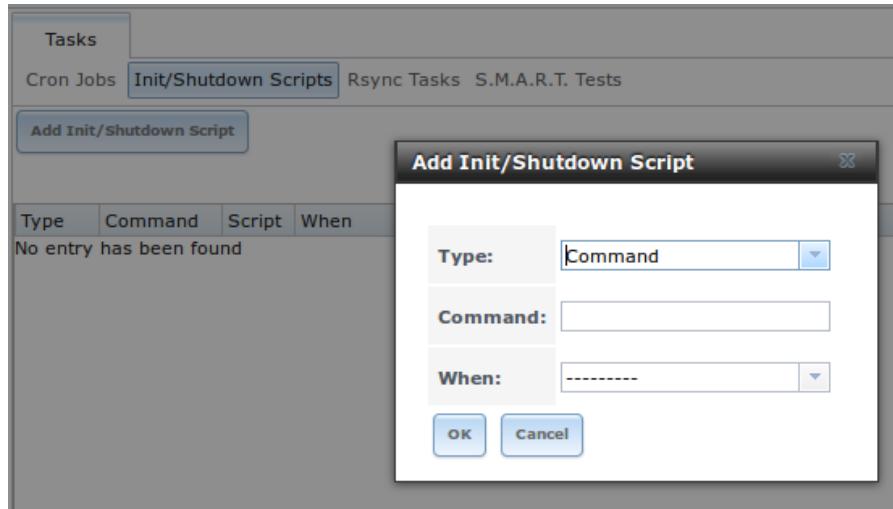


Fig. 6.2: Add an Init/Shutdown Script

Table 6.2: Options When Adding an Init/Shutdown Script

Setting	Value	Description
Type	drop-down menu	select from <i>Command</i> (for an executable) or <i>Script</i> (for an executable script)
Command	string	if <i>Command</i> is selected, input the command plus any desired options; if <i>Script</i> is selected, browse to the location of the script
When	drop-down menu	select when the command/script will run; choices are <i>Pre Init</i> (very early in boot process before filesystems are mounted), <i>Post Init</i> (towards end of boot process before FreeNAS services are started), or <i>Shutdown</i>

6.3 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. This system is referred to as *PULL* in the configuration examples.

- **the rsync client:** this system pushes (sends) the data. This system is referred to as *PUSH* in the configuration examples.

FreeNAS® can be configured as either an rsync client or an rsync server. The opposite end of the connection can be another FreeNAS® system or any other system running rsync. In FreeNAS® terminology, an rsync task defines which data is synchronized between the two systems. If you are synchronizing data between two FreeNAS® systems, create the rsync task on the rsync client.

FreeNAS® supports two modes of rsync operation:

- **rsync module mode:** exports a directory tree, and its configured settings, as a symbolic name over an unencrypted connection. This mode requires that at least one module be defined on the rsync server. It can be defined in the FreeNAS® GUI under Services → Rsync → Rsync Modules . In other operating systems, the module is defined in `rsyncd.conf(5)`.
- **rsync over SSH:** synchronizes over an encrypted connection. Requires the configuration of SSH user and host public keys.

This section summarizes the options when creating an Rsync Task. It then provides a configuration example between two FreeNAS® systems for each mode of rsync operation.

Note: If there is a firewall between the two systems or if the other system has a built-in firewall, make sure that TCP port 873 is allowed.

Figure 6.3 shows the screen that appears when you click Tasks → Rsync Tasks → Add Rsync Task . Table 6.3 summarizes the options that can be configured when creating an rsync task.

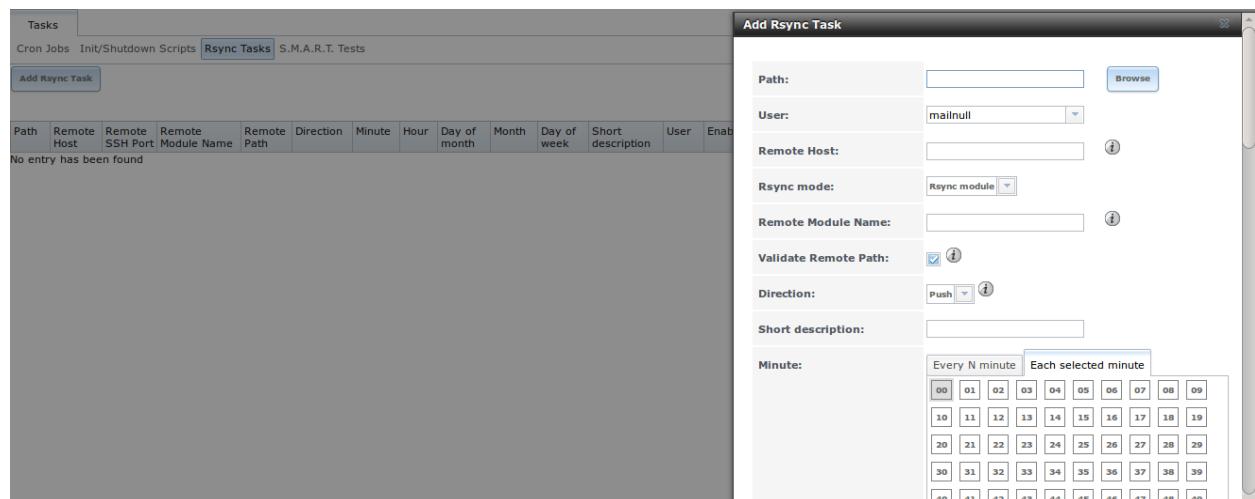


Fig. 6.3: Adding an Rsync Task

Table 6.3: Rsync Configuration Options

Setting	Value	Description
Path	browse button	browse to the path that you wish to copy; note that a path length greater than 255 characters will fail
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 cannot contain spaces or exceed 17 characters
Remote Host	string	IP address or hostname of the remote system that will store the copy; use the format <i>username@remote_host</i> if the username differs on the remote host
Remote SSH Port	integer	only available in <i>Rsync over SSH</i> mode; allows you to specify an alternate SSH port other than the default of 22
Rsync mode	drop-down menu	choices are <i>Rsync module</i> or <i>Rsync over SSH</i>
Remote Module Name	string	only appears when using <i>Rsync module</i> mode, at least one module must be defined in rsyncd.conf(5) of rsync server or in the <i>Rsync Modules</i> of another system
Remote Path	string	only appears when using <i>Rsync over SSH</i> mode, enter the existing path on the remote host to sync with (e.g. <i>/mnt/volume</i>); note that maximum path length is 255 characters
Validate Remote Path	checkbox	if the <i>Remote Path</i> does not yet exist, check this box to have it automatically created
Direction	drop-down menu	choices are <i>Push</i> or <i>Pull</i> ; default is to push to a remote host
Short Description	string	optional
Minute	slider or minute selections	if use the slider, sync occurs every N minutes; if use minute selections, sync occurs at the highlighted minutes
Hour	slider or hour selections	if use the slider, sync occurs every N hours; if use hour selections, sync occurs at the highlighted hours
Day of month	slider or day selections	if use the slider, sync occurs every N days; if use day selections, sync occurs on the highlighted days
Month	checkboxes	task occurs on the selected months
Day of week	checkboxes	task occurs on the selected days of the week
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 files in destination directory that don't exist in sending directory
Quiet	checkbox	suppresses informational messages from the remote server
Preserve permissions	checkbox	preserves original file permissions; useful if User is set to <i>root</i>
Preserve extended attributes	checkbox	both systems must support extended attributes
Delay Updates	checkbox	when checked, the temporary file from each updated file is saved to a holding directory until the end of the transfer, when all transferred files are renamed into place
Extra options	string	rsync(1) options not covered by the GUI; note that if the “*” character is used, it must be escaped between single quotes (e.g. ‘*.txt’)
Enabled Rsync Tasks	checkbox	uncheck if you would like to disable the rsync task without deleting it; note that when the <i>Rsync</i> service is OFF, the rsync task will continue to look for the server unless this checkbox is unchecked

If the rsync server requires password authentication, input `-password-file=/PATHTO/FILENAME` in the *Extra options* box, replacing `/PATHTO/FILENAME` with the appropriate path to the file containing the value of the password.

Created rsync tasks will be listed in *View Rsync Tasks*. Highlight the entry for an rsync task to display buttons for *Edit*, *Delete*, or *Run Now*.

6.3.1 Rsync Module Mode

This configuration example configures rsync module mode 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. It will be referred to as *PUSH*.
- 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. It will be referred to as *PULL*.

On *PUSH*, an rsync task is defined in `Tasks → Rsync Tasks → Add Rsync Task`. 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 *Rsync Mode* is *Rsync module*
- the *Remote Module Name* is *backups*; this will need to be defined on the rsync server
- the *Direction* is *Push*
- 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

On *PULL*, an rsync module is defined in `Services → Rsync Modules → Add Rsync Module`. 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 *Rsync Modules*.

To finish the configuration, start the rsync service on *PULL* in `Services → Control Services`. If the rsync is successful, the contents of `/mnt/local/images/` will be mirrored to `/mnt/remote/images/`.

6.3.2 Rsync over SSH Mode

SSH replication mode does not require the creation of an rsync module or for the rsync service to be running on the rsync server. It does require SSH to be configured before creating the rsync task:

- a public/private key pair for the rsync user account (typically *root*) must be generated on *PUSH* and the public key copied to the same user account on *PULL*
- to mitigate the risk of man-in-the-middle attacks, the public host key of *PULL* must be copied to *PUSH*

- the SSH service must be running on *PULL*

To create the public/private key pair for the rsync user account, open *Shell* on *PUSH* and run **ssh-keygen**. The following example generates an RSA type public/private key pair for the *root* user. When creating the key pair, do not enter the passphrase as the key is meant to be used for an automated task.

```
ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
f5:b0:06:d1:33:e4:95:cf:04:aa:bb:6e:a4:b7:2b:df root@freenas.local
The key's randomart image is:
+--[ RSA 2048]----+
|          .o. oo   |
|          o+o. .   |
|          . =o +   |
|          + +     o |
|          S o .   |
|          .o       |
|          o.       |
|          o oo    |
|          **oE    |
+-----+
|           |
|           |
```

FreeNAS® supports the following types of SSH keys: DSA, and RSA. When creating the key, specify the type you wish to use or, if you are generating the key on another operating system, select a type of key the key generation software supports.

Note: If a different user account is used for the rsync task, use the **su** – command after mounting the filesystem but before generating the key. For example, if the rsync task is configured to use the *user1* user account, use this command to become that user:

```
su - user1
```

Next, view and copy the contents of the generated public key:

```
more .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQQC11BEXRgw1W8y8k+1XP1VR3xsmVSjtsoyIzV/P1QPo
SrWotUQzqILq0SmUpViAAv4Ik3T8NtxXyoKmFNbBczU6tEsVGHo/2BLjvKiSHRPHC/1DX9hofcFti4h
dcD7Y5mvU3MAEeDClt02/xoi5xs/RLxgPOR5dNrakw958Yn001sJS9VMf528fknUmasti00qmDDcp/kO
xT+S6DFNBy6IYQN4heqmhTPRXqPhXqcD1G+rWr/nZK4H8Ckzy+19RaEXMRuTyQgqJB/rsRcmJX5fApd
DmNfwrRSxLjDvUzfywnjFH1Kk/+TQIT1gg1QQaj21PJD9pnDVFOAiJrWyWnR root@freenas.local
```

Go to *PULL* and paste (or append) the copied key into the *SSH Public Key* field of *Account* → *Users* → *View Users* → *root* → *Modify User*, or the username of the specified rsync user account. The paste for the above example is shown in [Figure 6.4](#). When pasting the key, ensure that it is pasted as one long line and, if necessary, remove any extra spaces representing line breaks.

While on *PULL*, verify that the SSH service is running in *Services* → *Control Services* and start it if it is not.

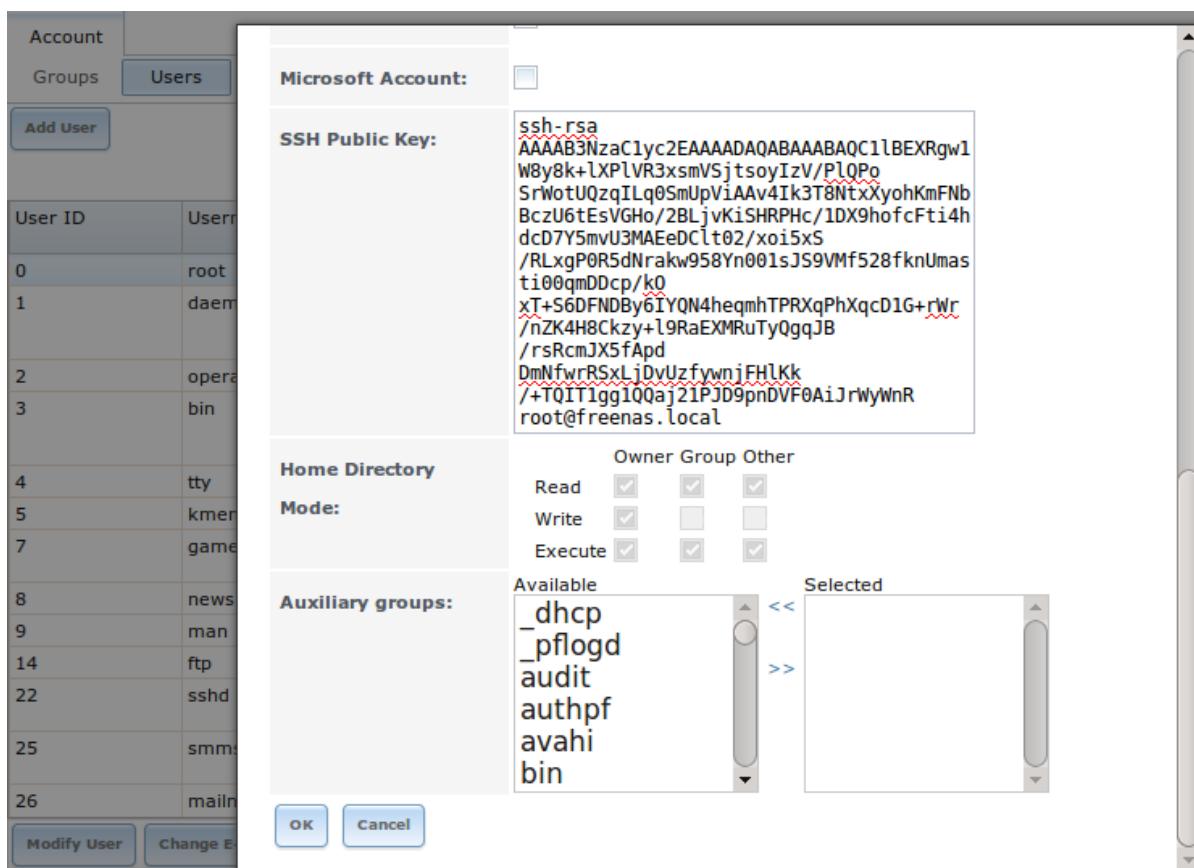


Fig. 6.4: Pasting the User's SSH Public Key

Next, copy the host key of *PULL* using Shell on *PUSH*. The following command copies the RSA host key of the *PULL* server used in our previous example. Be sure to include the double bracket >> to prevent overwriting any existing entries in the `known_hosts` file:

```
ssh-keyscan -t rsa 192.168.2.6 >> /root/.ssh/known_hosts
```

Note: If *PUSH* is a Linux system, use the following command to copy the RSA key to the Linux system:

```
cat ~/.ssh/id_rsa.pub | ssh user@192.168.2.6 'cat >> .ssh/authorized_keys'
```

You are now ready to create the rsync task on *PUSH*. To configure rsync SSH mode using the systems in our previous example, the configuration would be as follows:

- the *Path* points to `/mnt/local/images`, the directory to be copied
- the *Remote Host* points to `192.168.2.6`, the IP address of the rsync server
- the *Rsync Mode* is *Rsync over SSH*
- the rsync is scheduled to occur every 15 minutes
- the *User* is set to `root` so it has permission to write anywhere; the public key for this user must be generated on *PUSH* and copied to *PULL*
- the *Preserve Permissions* checkbox is checked so that the original permissions are not overwritten by the `root` user

Save the rsync task and the rsync will automatically occur according to the schedule. In this example, the contents of `/mnt/local/images/` will automatically appear in `/mnt/remote/images/` after 15 minutes. If the content does not appear, use Shell on *PULL* to read `/var/log/messages`. If the message indicates a `n` (newline character) in the key, remove the space in your pasted key—it will be after the character that appears just before the `n` in the error message.

6.4 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 6.5 shows the configuration screen that appears when you click Tasks → S.M.A.R.T. Tests → Add S.M.A.R.T. Test. The tests that you create will be listed under *View S.M.A.R.T. Tests*. 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. The S.M.A.R.T. service will not start if you have not created any volumes.

Note: To prevent problems, do not enable the S.M.A.R.T. service if your disks are controlled by a RAID controller as it is the job of the controller to monitor S.M.A.R.T. and mark drives as Predictive Failure when they trip.

Table 6.4 summarizes the configurable options when creating a S.M.A.R.T. test.

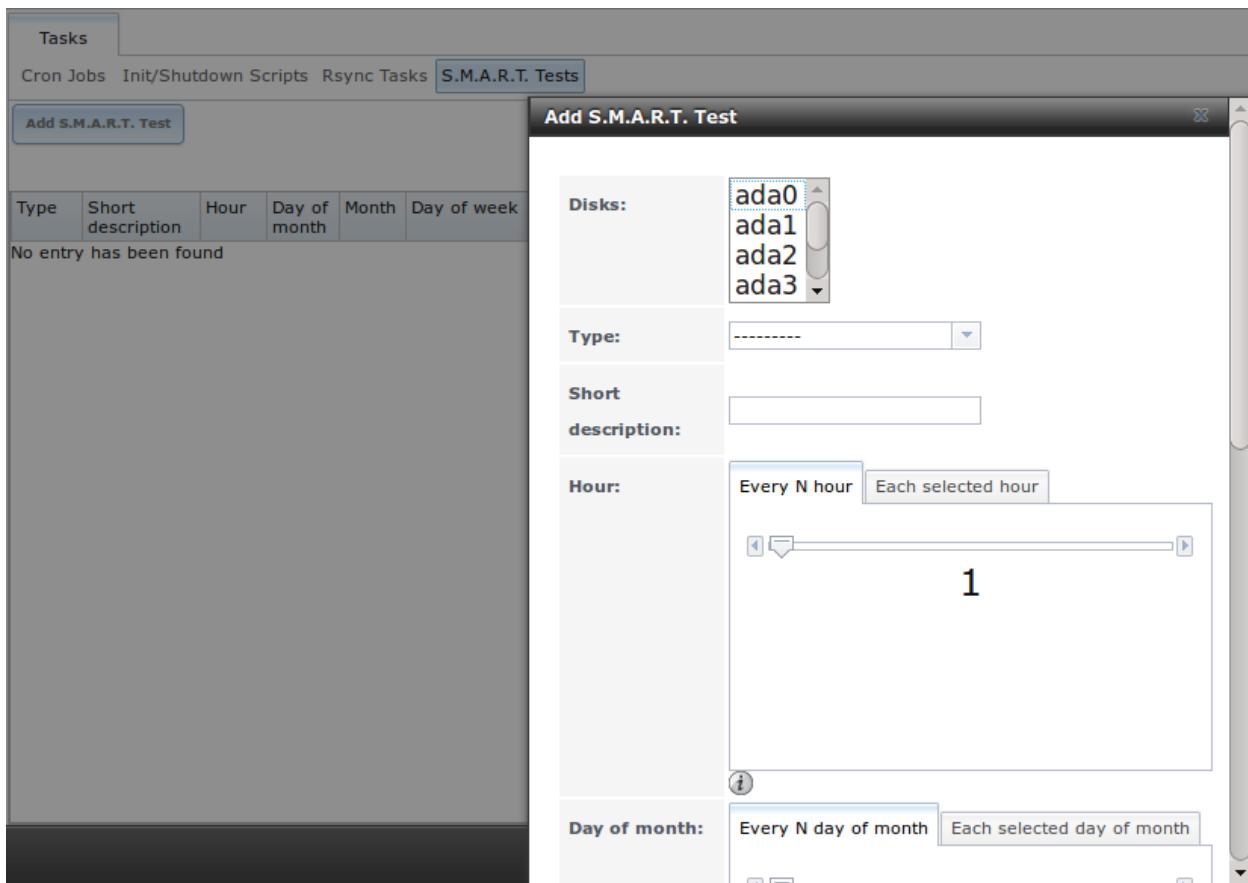


Fig. 6.5: Adding a S.M.A.R.T. Test

Table 6.4: S.M.A.R.T. Test Options

Setting	Value	Description
Disks	list	highlight disk(s) to monitor
Type	drop-down menu	select type of test to run; see smartctl(8) for a description of each type of test (note that some test types will degrade performance or take disks offline; do not schedule S.M.A.R.T. tests at the same time as a scrub or during a resilver operation)
Short description	string	optional
Hour	slider or hour selections	if use the slider, test occurs every N hours; if use hour selections, test occurs at the highlighted hours
Day of month	slider or day selections	if use the slider, test occurs every N days; if use day selections, test occurs on the highlighted days
Month	checkboxes	select the months when you wish the test to occur
Day of week	checkboxes	select the days of the week when you wish the test to occur

An example configuration is to schedule a *Short Self-Test* once a week and a *Long Self-Test* once a month. These tests should not have a performance impact, as the disks prioritize normal I/O over the tests. If a disk fails a test, even if the overall status is *Passed*, start to think about replacing that disk.

Warning: Some S.M.A.R.T. tests cause heavy disk activity and can drastically reduce disk performance. Do not schedule S.M.A.R.T. tests to run at the same time as scrub or resilver operations or during other periods of intense disk activity.

Which tests will run and when can be verified by typing **smartd -q showtests** within [Shell](#).

The results of a test can be checked from [Shell](#) by specifying the name of the drive. For example, to see the results for disk *ada0*, type:

```
smartctl -l selftest /dev/ada0
```

If you enter an email address in the *Email to report* field of Services → S.M.A.R.T., the system will email the specified address when a test fails.

CHAPTER SEVEN

NETWORK

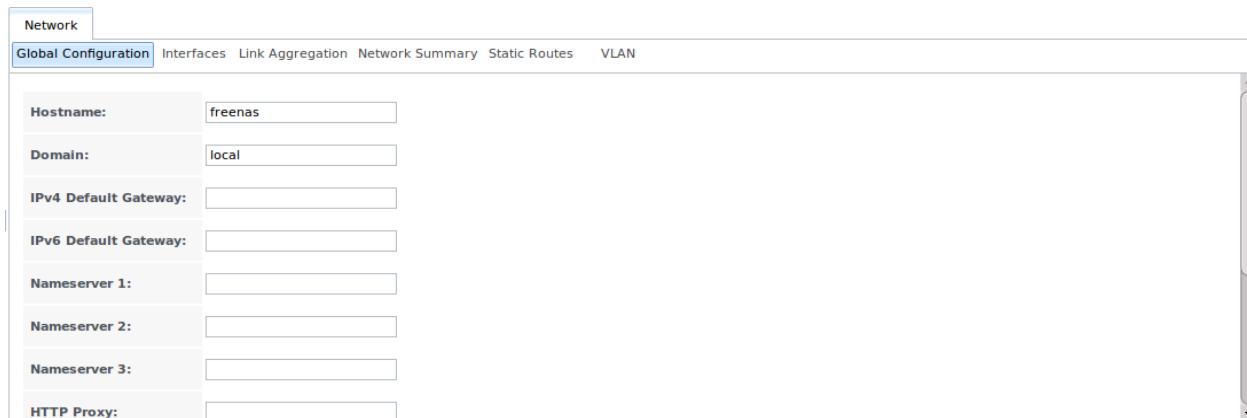
The Network section of the administrative GUI contains these components for viewing and configuring network settings on the FreeNAS® system:

- *Global Configuration*: general network settings.
- *Interfaces*: settings for each network interface.
- *IPMI*: settings controlling connection to the appliance through the hardware side-band management interface if the graphical user interface becomes unavailable.
- *Link Aggregations*: settings for network link aggregation and link failover.
- *Network Summary*: display an overview of the current network settings.
- *Static Routes*: add static routes.
- *VLANs*: configure IEEE 802.1q tagging for virtual LANs.

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

7.1 Global Configuration

Network → Global Configuration , shown in Figure 7.1, is for general network settings that are not unique to any particular network interface.



The screenshot shows the 'Global Configuration' tab selected in the top navigation bar. The page displays various network settings fields:

Setting	Value
Hostname:	freenas
Domain:	local
IPv4 Default Gateway:	[empty]
IPv6 Default Gateway:	[empty]
Nameserver 1:	[empty]
Nameserver 2:	[empty]
Nameserver 3:	[empty]
HTTP Proxy:	[empty]

Fig. 7.1: Global Network Configuration

Table 7.1 summarizes the settings on the Global Configuration tab. Hostname and domain fields are pre-filled as shown in Figure 7.1, but can be changed to meet requirements of the local network.

Table 7.1: Global Configuration Settings

Setting	Value	Description
Hostname	string	system host name
Domain	string	system domain name
IPv4 Default Gateway	IP address	typically not set (see NOTE below)
IPv6 Default Gateway	IP address	typically not set (see NOTE below)
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
HTTP Proxy	string	enter the proxy information for the network in the format <i>http://my.proxy.server:3128</i> or <i>http://user@password:my.proxy.server:3128</i>
Enable netwait feature	checkbox	if enabled, network services are not started at boot until the interface is able to ping the addresses listed in <i>Netwait IP list</i>
Netwait IP list	string	if <i>Enable netwait feature</i> is checked, list of IP addresses to ping; otherwise, ping the default gateway
Host name database	string	used to add one entry per line which will be appended to <i>/etc/hosts</i> ; use the format <i>IP_address space hostname</i> where multiple hostnames can be used if separated by a space

When Active Directory is being used, set the IP address of the realm's DNS server in the *Nameserver 1* field.

If the network does not have a DNS server, or NFS, SSH, or FTP users are receiving “reverse DNS” or timeout errors, add an entry for the IP address of the FreeNAS® system in the *Host name database* field.

Note: In many cases, a FreeNAS® configuration does not include default gateway information as a way to make it more difficult for a remote attacker to communicate with the server. While this is a reasonable precaution, such a configuration does **not** restrict inbound traffic from sources within the local network. However, omitting a default gateway will prevent the FreeNAS® system from communicating with DNS servers, time servers, and mail servers that are located outside of the local network. In this case, it is recommended to add *Static Routes* to be able to reach external DNS, NTP, and mail servers which are configured with static IP addresses. When a gateway to the Internet is added, make sure that the FreeNAS® system is protected by a properly configured firewall.

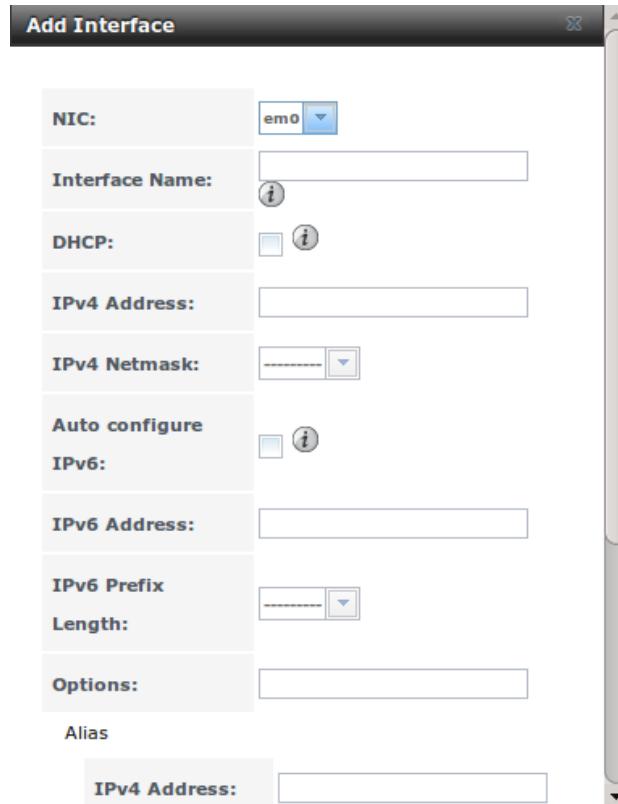
7.2 Interfaces

`Network → Interfaces` shows which interfaces have been manually configured and allows adding or editing a manually configured interface.

Note: Typically, the interface used to access the FreeNAS® administrative GUI is configured by DHCP. This interface

does not appear in this screen, even though it is already dynamically configured and in use.

Figure 7.2 shows the screen that opens on clicking `Interfaces → Add Interface`. Table 7.2 summarizes the configuration options shown when adding an interface or editing an already configured interface. Note that if any changes to this screen require a network restart, the screen will turn red when the *OK* button is clicked and a pop-up message will point out that network connectivity to the FreeNAS® system will be interrupted while the changes are applied.



The screenshot shows the 'Add Interface' dialog box with the following fields:

- NIC:** em0 (dropdown menu)
- Interface Name:** (text input field with info icon)
- DHCP:** (checkbox with info icon)
- IPv4 Address:** (text input field)
- IPv4 Netmask:** (text input field with dropdown arrow)
- Auto configure:** (checkbox with info icon)
- IPv6:** (checkbox with info icon)
- IPv6 Address:** (text input field)
- IPv6 Prefix:** (text input field with dropdown arrow)
- Length:** (text input field with dropdown arrow)
- Options:** (text input field)
- Alias** (label)
- IPv4 Address:** (text input field)

Fig. 7.2: Adding or Editing an Interface

Table 7.2: Interface Configuration Settings

Setting	Value	Description
NIC	drop-down menu	select the FreeBSD device name; is a read-only field when editing an interface
Interface Name	string	description of interface
DHCP	check-box	requires static IPv4 or IPv6 configuration if unchecked; note that only one interface can be configured for DHCP
IPv4 Address	IP address	enter a static IP address if <i>DHCP</i> is unchecked
IPv4 Netmask	drop-down menu	enter a netmask if <i>DHCP</i> is unchecked
Auto configure IPv6	check-box	only one interface can be configured for this option; if unchecked, manual configuration is required to use IPv6
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 <code>ifconfig(8)</code> , separate multiple parameters with a space; for example: <code>mtu 9000</code> will increase the MTU for interfaces that support jumbo frames

This screen also provides for the configuration of IP aliases, making it possible for a single interface to have multiple IP addresses. To set multiple aliases, click the *Add extra alias* link for each alias. Aliases are deleted by clicking the interface in the tree, clicking the *Edit* button, checking the *Delete* checkbox below the alias, then clicking the *OK* button.

Warning: Aliases are deleted by checking the *Delete* checkbox in the alias area, then clicking *OK* for the interface. **Do not** click the *Delete* button at the bottom of this screen, which deletes the entire interface.

Multiple interfaces **cannot** be members of the same subnet. Check the subnet mask if an error is shown when setting the IP addresses on multiple interfaces.

This screen will not allow an interface's IPv4 and IPv6 addresses to both be set as primary addresses. An error is shown if both the *IPv4 address* and *IPv6 address* fields are filled in. Instead, set only one of these address fields and create an alias for the other address.

7.3 IPMI

Beginning with version 9.2.1, FreeNAS® provides a graphical screen for configuring an IPMI interface. This screen will only appear if the system hardware includes a Baseboard Management Controller (BMC).

IPMI provides side-band management if the graphical administrative interface becomes unresponsive. This allows for a few vital functions, such as checking the log, accessing the BIOS setup, and powering on the system without requiring physical access to the system. IPMI can also be used to allow another person remote access to the system to assist with a configuration or troubleshooting issue. Before configuring IPMI, ensure that the management interface is physically connected to the network. The IPMI device may share the primary Ethernet interface, or it may be a dedicated separate IPMI interface.

Warning: It is recommended to first ensure that the IPMI has been patched against the Remote Management Vulnerability before enabling IPMI. This [article](#) provides more information about the vulnerability and how to fix it.

IPMI is configured from Network → IPMI . The IPMI configuration screen, shown in [Figure 7.3](#), provides a shortcut to the most basic IPMI configuration. Those already familiar with IPMI management tools can use them instead. [Table 7.3](#) summarizes the options available when configuring IPMI with the FreeNAS® GUI.

The screenshot shows the IPMI configuration interface. The 'IPMI' tab is active. The configuration fields are as follows:

- Channel:** 1
- Password:** (empty field)
- Password confirmation:** (empty field) with an info icon (i)
- DHCP:** checked
- IPv4 Address:** 10.5.65.21
- IPv4 Netmask:** /16 (255.255.0.0)
- IPv4 Default Gateway:** 10.5.0.1
- VLAN ID:** (empty field)

At the bottom left are the **OK** and **Cancel** buttons.

Fig. 7.3: IPMI Configuration

Table 7.3: IPMI Options

Setting	Value	Description
Channel	drop-down menu	select the channel to use
Password	string	enter the password used to connect to the IPMI interface from a web browser
DHCP	checkbox	if left unchecked, the following three fields must be set
IPv4 Address	string	IP address used to connect to the IPMI web GUI
IPv4 Netmask	drop-down menu	subnet mask associated with the IP address
IPv4 Default Gateway	string	default gateway associated with the IP address
VLAN ID	string	enter the VLAN identifier if the IPMI out-of-band management interface is not on the same VLAN as management networking

After configuration, the IPMI interface is accessed using a web browser and the IP address specified in the configuration. The management interface prompts for a username and the configured password. Refer to the IPMI device's

documentation to determine the default administrative username.

After logging in to the management interface, the default administrative username can be changed, and additional users created. The appearance of the IPMI utility and the functions that are available vary depending on the hardware.

7.4 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. The link state of the lagg interface is used to validate whether the port is active.

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. 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* the NAS. The flow entering *into* the NAS depends on the Ethernet switch load-balance algorithm.

The lagg driver currently supports several aggregation protocols, although only *Failover* is recommended on network switches that do not support LACP:

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, which is useful for certain bridged network setups, by creating a tunable with a *Variable* of `net.link.lagg.failover_rx_all`, a *Value* of a non-zero integer, and a *Type* of `Sysctl` in `System → Tunables → Add Tunable`.

FEC: supports Cisco EtherChannel on older Cisco switches. 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 negotiates a set of aggregable links with the peer into one or more link aggregated groups (LAGs). Each LAG is composed of ports of the same speed, set to full-duplex operation. Traffic is 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, and LACP does not support mixing interfaces of different speeds. Only interfaces that use the same driver, like two `igb` ports, are recommended for LACP. Using LACP for iSCSI is not recommended, as iSCSI has built-in multipath features which are more efficient.

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. Requires a switch which supports IEEE 802.3ad static link aggregation.

Round Robin: distributes outgoing traffic using a round-robin scheduler through all active ports and accepts incoming traffic from any active port. This mode can cause unordered packet arrival at the client. This has a side effect of limiting throughput as reordering packets can be CPU intensive on the client. Requires a switch which supports IEEE 802.3ad static link aggregation.

None: this protocol disables any traffic without disabling the lagg interface itself.

Note: When using LACP, verify that the switch is configured for active LACP, as passive LACP is not supported.

7.4.1 LACP, MPIO, NFS, and ESXi

LACP bonds Ethernet connections to improve bandwidth. For example, four physical interfaces can be used to create one mega interface. However, it cannot increase the bandwidth for a single conversation. It is designed to increase bandwidth when multiple clients are simultaneously accessing the same system. It also assumes that quality Ethernet hardware is used and it will not make much difference when using inferior Ethernet chipsets such as a Realtek.

LACP reads the sender and receiver IP addresses and, if they are deemed to belong to the same TCP connection, always sends the packet over the same interface to ensure that TCP does not need to reorder packets. This makes LACP ideal for load balancing many simultaneous TCP connections, but does nothing for increasing the speed over one TCP connection.

MPIO operates at the iSCSI protocol level. For example, if four IP addresses are created and there are four simultaneous TCP connections, MPIO will send the data over all available links. When configuring MPIO, make sure that the IP addresses on the interfaces are configured to be on separate subnets with non-overlapping netmasks, or configure static routes to do point-to-point communication. Otherwise, all packets will pass through one interface.

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. 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.

NFS does not understand MPIO. Therefore, one fast interface is needed, since creating an iSCSI portal will not improve bandwidth when using NFS. LACP does not work well to increase the bandwidth for point-to-point NFS (one server and one client). LACP is a good solution for link redundancy or for one server and many clients.

7.4.2 Creating a Link Aggregation

Before creating a link aggregation, double-check that no interfaces have been manually configured in Network → Interfaces → View Interfaces .

If any manually-configured interfaces exist, delete them as **lagg creation will fail if any interfaces are manually configured**.

Figure 7.4 shows the configuration options when adding a lagg interface using Network → Link Aggregations → Create Link Aggregation .

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

To create a link aggregation, select the desired *Protocol Type*, highlight the interfaces to associate with the lagg device, and click the *OK* button.

Once the lagg device has been created, click its entry to enable its *Edit*, *Delete*, and *Edit Members* buttons.

Clicking the *Edit* button for a lagg opens the configuration screen shown in Figure 7.5. Table 7.4 describes the options in this screen.

After creating the lagg interface, set the IP address manually or with DHCP. The connection to the web interface may be temporarily lost at this point as the network is restarted. The switch settings may also have to be changed to communicate through the new lagg interface. If the IP address was set manually, it might also be necessary to

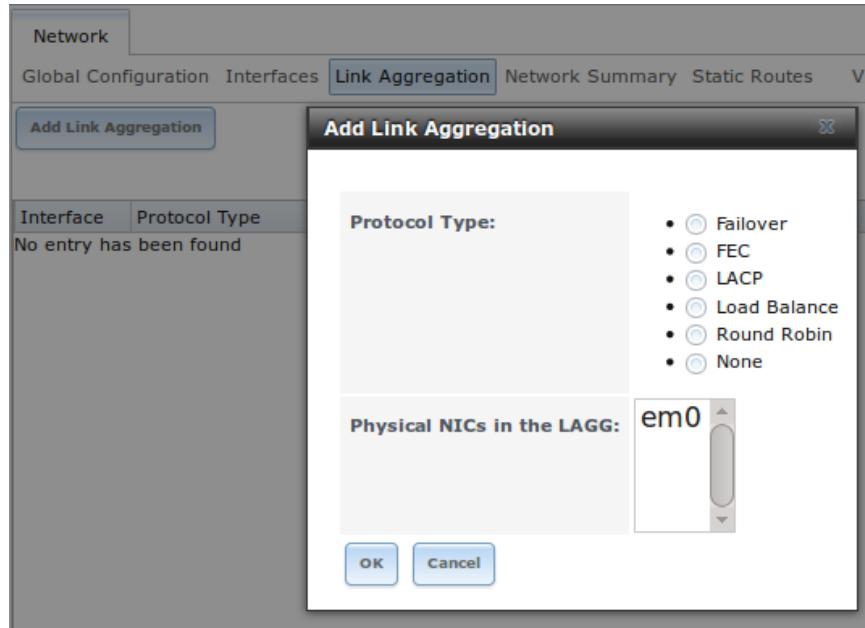


Fig. 7.4: Creating a lagg Interface

manually enter a default gateway from the console setup menu option to get access into the GUI through the new lagg interface.

Table 7.4: Configurable Options for a lagg

Setting	Value	Description
NIC	string	read-only; automatically assigned the 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 will get IP address info from DHCP server
IPv4 Address	string	enter a static IP address if <i>DHCP</i> is left unchecked
IPv4 Netmask	drop-down menu	enter a netmask if <i>DHCP</i> is left unchecked
Auto configure IPv6	checkbox	check only if DHCP server available to provide IPv6 address info
IPv6 Address	string	optional
IPv6 Prefix Length	drop-down menu	required if an IPv6 address is entered
Options	string	additional <code>ifconfig(8)</code> options

This screen also allows the configuration of an alias for the lagg interface. Multiple aliases can be added with the *Add extra Alias* link.

Click the *Edit Members* button, click the entry for a member, then click its *Edit* button to see the configuration screen shown in Figure 7.6. The configurable options are summarized in Table 7.5.

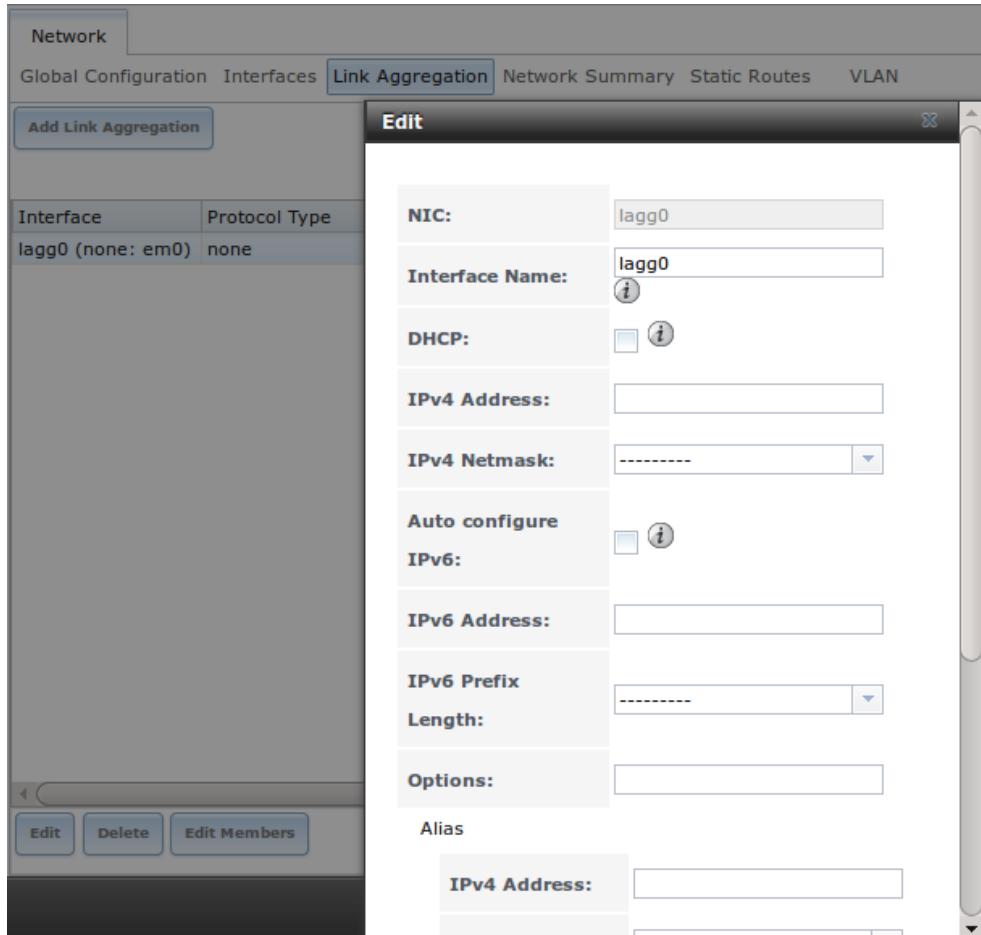


Fig. 7.5: Editing a lagg

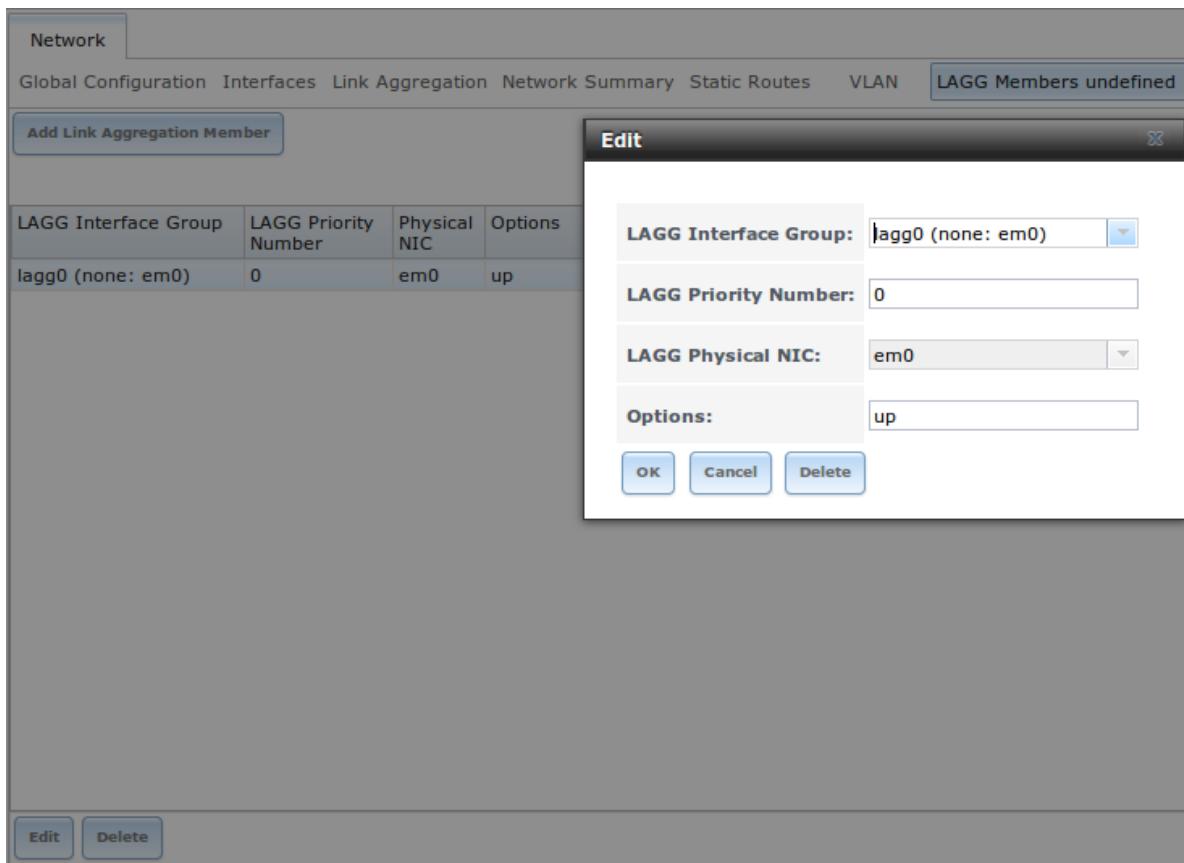


Fig. 7.6: Editing a Member Interface

Table 7.5: 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; configure a failover to set the master interface to 0 and the other interfaces to 1, 2, etc.
LAGG Physical NIC	drop-down menu	physical interface of the selected member
Options	string	additional parameters from <code>ifconfig(8)</code>

Options can be set at the lagg level using the *Edit* button, or at the individual parent interface level using the *Edit Members* button. Changes are typically made at the lagg level (Figure 7.5) as each interface member will inherit from the lagg. To configure at the interface level (Figure 7.6) instead, the configuration must be repeated for each interface within the lagg. However, some lagg options can only be set by editing the interface. For instance, the MTU of a lagg is inherited from the interface, so setting the MTU on a lagg requires setting all of the interfaces to the same MTU **before** creating the lagg.

Note: When changing the MTU to create a jumbo frame lagg, a reboot is required.

To see if the link aggregation is load balancing properly, run this command from *Shell*:

```
systat -ifstat
```

More information about this command can be found at [systat\(1\)](#).

7.5 Network Summary

Network → Network Summary shows a quick summary of the addressing information of every configured interface. For each interface name, the configured IPv4 and IPv6 addresses, DNS servers, and default gateway are displayed.

7.6 Static Routes

No static routes are defined on a default FreeNAS® system. If a static route is required to reach portions of the network, add the route with Network → Static Routes → Add Static Route, shown in Figure 7.7.

The available options are summarized in Table 7.6.

Table 7.6: Static Route Options

Setting	Value	Description
Destination network	integer	use the format $A.B.C.D/E$ where E is the CIDR mask
Gateway	integer	enter the IP address of the gateway
Description	string	optional

Added static routes are shown in *View Static Routes*. Click a route's entry to access the *Edit* and *Delete* buttons.

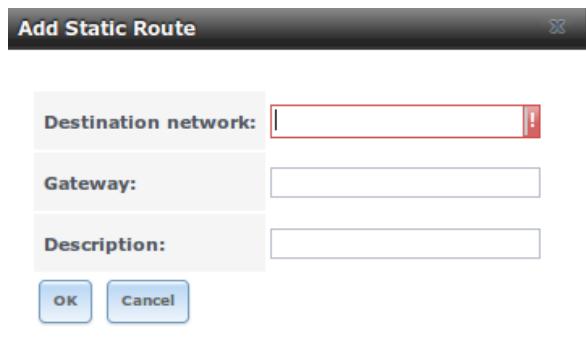


Fig. 7.7: Adding a Static Route

7.7 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.

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.

Click Network → VLANs → Add VLAN , to see the screen shown in Figure 7.8.

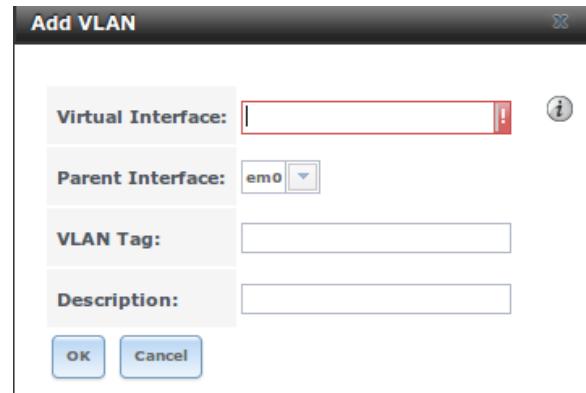


Fig. 7.8: Adding a VLAN

Table 7.7 summarizes the configurable fields.

Table 7.7: Adding a VLAN

Setting	Value	Description
Virtual Interface	string	use the format <i>vlanX</i> where <i>X</i> is a number representing a vlan interface not currently being used as a parent
Parent Interface	drop-down menu	usually an Ethernet card connected to a properly configured switch port; note that newly created <i>Link Aggregations</i> will not appear in the drop-down until the system is rebooted
VLAN Tag	integer	number between 1 and 4095 which matches a numeric tag set up in the switched network
Description	string	optional

The parent interface of a VLAN must be up, but it can have an IP address or it can be unconfigured, depending upon the requirements of the VLAN configuration. This makes it difficult for the GUI to do the right thing without trampling the configuration. To remedy this, after adding the VLAN, go to Network → Interfaces → Add Interface . Select the parent interface from the *NIC* drop-down menu and in the *Options* field, type **up**. This will bring up the parent interface. If an IP address is required, it can be configured using the rest of the options in the *Add Interface* screen.

Warning: Creating a vlan will cause network connectivity to be interrupted. Accordingly, the GUI will provide a warning and an opportunity to cancel the vlan creation.

STORAGE

The Storage section of the graphical interface allows configuration of these options:

- *Volumes*: used to create and manage storage volumes.
- *Periodic Snapshot Tasks*: used to schedule the automatic creation of filesystem snapshots.
- *Replication Tasks*: used to schedule the replication of snapshots to a remote system.
- *Scrubs*: used to schedule scrubs as part of ongoing disk maintenance.
- *Snapshots*: used to manage local snapshots.
- *VMware-Snapshot*: is used to coordinate ZFS snapshots with a VVware datastore.

These configurations are described in more detail in this section.

8.1 Volumes

The *Volumes* section of the FreeNAS® graphical interface can be used to format ZFS pools, import a disk to copy its data into an existing pool, or import an existing ZFS pool. It can also be used to create ZFS datasets and zvols and to manage their permissions.

Note: In ZFS terminology, the storage that is managed by ZFS is referred to as a pool. The FreeNAS® graphical interface uses the term *volume* to refer to a ZFS pool.

Proper storage design is important for any NAS. **Please read through this entire chapter before configuring storage disks. All of the features are described to help make it clear which will be the most benefit for your uses, and caveats or caveats or hardware restrictions which could limit their use.**

8.1.1 Volume Manager

Volume Manager is used to add disks to a ZFS pool. Any old data on added disks is overwritten, so save it elsewhere before reusing a disk. Please see the [ZFS Primer](#) for information on ZFS redundancy with multiple disks before using *Volume Manager*.

Selecting *Storage* → *Volumes* → *Volume Manager* opens a screen like the example shown in [Figure 8.1](#).

[Table 8.1](#) summarizes the configuration options of this screen.

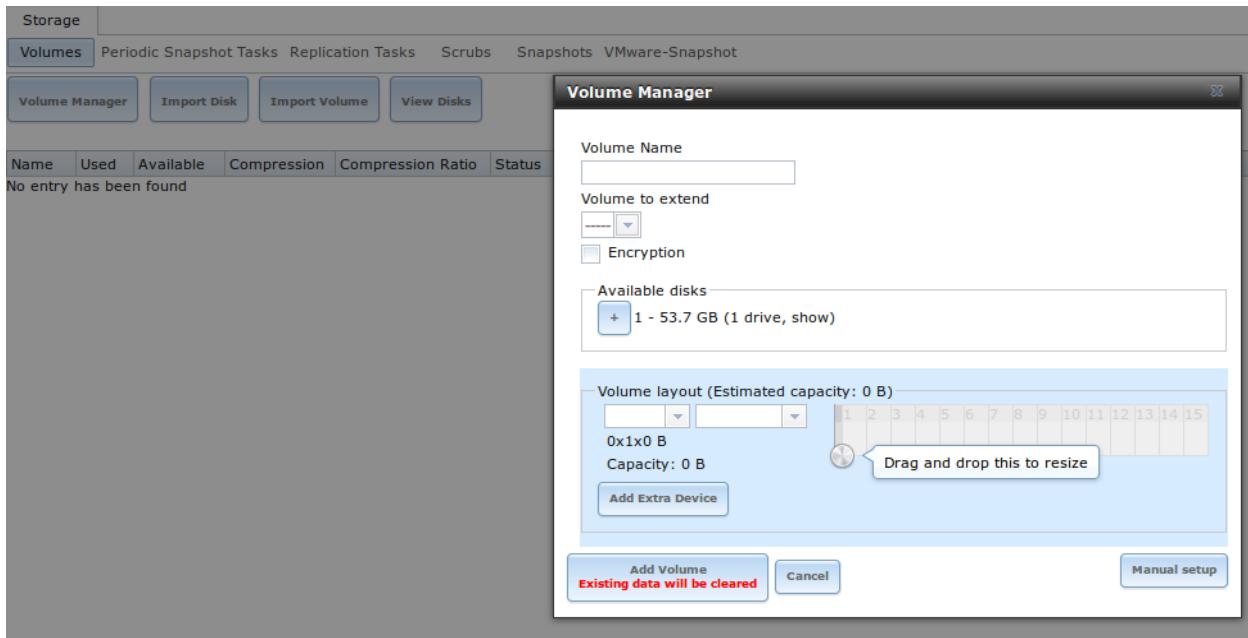


Fig. 8.1: Creating a ZFS Pool Using Volume Manager

Table 8.1: Options When Creating a ZFS Volume

Setting	Value	Description
Volume name	string	ZFS volumes must conform to these naming conventions ; it is recommended to choose a name that will stick out in the logs (e.g. not data or freenas)
Volume to extend	drop-down menu	used to extend an existing ZFS pool; see Extending a ZFS Volume for instructions
Encryption	check-box	read the section on Encryption before choosing to use encryption
Available disks	display	displays the number and size of available disks; hover over show to list the available device names; click the + to add all of the disks to the pool
Volume layout	drag and drop	click and drag the icon to select the desired number of disks for a vdev; once at least one disk is selected, the layouts supported by the selected number of disks will be added to the drop-down menu
Add Extra Device	button	used to configure multiple vdevs or to add log or cache devices during pool creation
Manual setup	button	used to make a non-optimal pool (not recommended); see Manual Setup for details

Drag the slider to select the desired number of disks. *Volume Manager* will display the resulting storage capacity, taking swap space into account. To change the layout or the number of disks, use the mouse to drag the slider to the desired volume layout. The *Volume layout* drop-down menu can also be clicked if a different level of redundancy is required.

Note: For performance and capacity reasons, this screen does not allow creating a volume from disks of differing sizes. While it is not recommended, it is possible to create a volume in this situation by using the *Manual setup* button and following the instructions in [Manual Setup](#).

Volume Manager only allows choosing a configuration if enough disks have been selected to create that configuration. These layouts are supported:

- **Stripe:** requires at least one disk
- **Mirror:** requires at least two disks
- **RAIDZ1:** requires at least three disks
- **RAIDZ2:** requires at least four disks
- **RAIDZ3:** requires at least five disks
- **log device:** requires at least one dedicated device, SSD is recommended
- **cache device:** requires at least one dedicated device, SSD is recommended

When more than five disks are being used, consideration must be given to the optimal layout for the best performance and scalability. An overview of the recommended disk group sizes as well as more information about log and cache devices can be found in the [ZFS Primer](#).

The *Add Volume* button warns that **existing data will be cleared**. In other words, creating a new volume reformats the selected disks. If the existing data is meant to be preserved, click the *Cancel* button and refer to [Import Disk](#) and [Import Volume](#) to see if the existing format is supported. If so, perform that supported action instead. If the current storage format is not supported, it is necessary to back up the data to external media, format the disks, then restore the data to the new volume.

Depending upon the size and number of disks, the type of controller, and whether encryption is selected, creating the volume may take some time. After the volume is created, the screen will refresh and the new volume is listed in the tree under *Storage → Volumes*. Click the + next to the volume name to access its [Change Permissions](#), [Create Dataset](#), and [Create zvol](#) options.

Encryption

Beginning with 8.3.1, FreeNAS® supports [GELI](#) full disk encryption when creating ZFS volumes. It is important to understand the following when considering whether or not encryption is right for your FreeNAS® system:

- This is **not** the encryption method used by Oracle's version of ZFS as that version is not open source and is the property of Oracle.
- This is full disk encryption and **not** per-filesystem encryption. The underlying drives are first encrypted, then the pool is created on top of the encrypted devices.
- This type of encryption is primarily targeted at users who store sensitive data and want to retain the ability to remove disks from the pool without having to first wipe the disk's contents.
- This design is only suitable for safe disposal of disks independent of the encryption key. As long as the key and the disks are intact, the system is vulnerable to being decrypted. The key should be protected by a strong passphrase and any backups of the key should be securely stored.
- On the other hand, if the key is lost, the data on the disks is inaccessible. Always back up the key!
- The encryption key is per ZFS volume (pool). If you create multiple pools, each pool has its own encryption key.
- If the system has a lot of disks, there will be a performance hit if the CPU does not support [AES-NI](#) or if no crypto hardware is installed. Without hardware acceleration, there will be about a 20% performance hit for a single disk. Performance degradation will continue to increase with more disks. As data is written, it is automatically encrypted and as data is read, it is decrypted on the fly. If the processor does support the AES-NI instruction set, there should be very little, if any, degradation in performance when using encryption. This [forum post](#) compares the performance of various CPUs.

- Data in the ARC cache and the contents of RAM are unencrypted.
- Swap is always encrypted, even on unencrypted volumes.
- There is no way to convert an existing, unencrypted volume. Instead, the data must be backed up, the existing pool must be destroyed, a new encrypted volume must be created, and the backup restored to the new volume.
- Hybrid pools are not supported. In other words, newly created vdevs must match the existing encryption scheme. When extending a volume, Volume Manager will automatically encrypt the new vdev being added to the existing encrypted pool.

Note: The encryption facility used by FreeNAS® is designed to protect against physical theft of the disks. It is not designed to protect against unauthorized software access. Ensure that only authorized users have access to the administrative GUI and that proper permissions are set on shares if sensitive data is stored on the system.

To create an encrypted volume, check the *Encryption* box shown in Figure 8.1. A pop-up message will remind you that **it is extremely important** to make a backup of the key as without it the data on the disks is inaccessible. Refer to *Managing Encrypted Volumes* for instructions.

Manual Setup

The *Manual Setup* button shown in Figure 8.1 can be used to create a non-optimal ZFS volume. While this is **not** recommended, it can, for example, be used to create a volume containing disks of different sizes.

Note: When using disks of differing sizes, the volume is limited by the size of the smallest disk. For this reason, it is recommended to instead use *Volume Manager* with same-size disks.

Figure 8.2 shows the *Manual Setup* screen and Table 8.2 summarizes the available options.

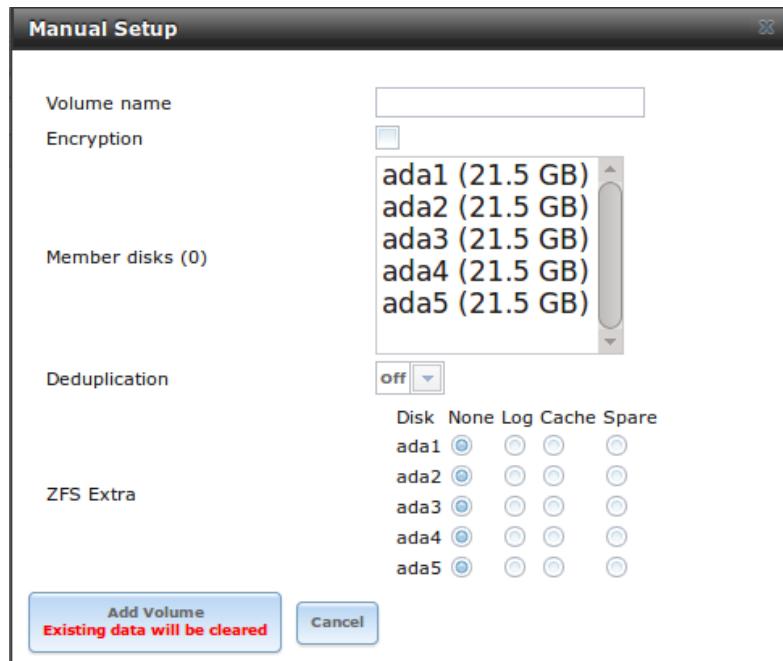


Fig. 8.2: Creating a Non-Optimal ZFS Volume

Table 8.2: Manual Setup Options

Setting	Value	Description
Volume name	string	ZFS volumes must conform to these naming conventions ; it is recommended to choose a name that will stick out in the logs (e.g. not <code>data</code> or <code>freenas</code>)
Encryption	checkbox	read the section on Encryption before choosing to use encryption
Member disks	list	highlight desired number of disks from list of available disks
Deduplication	drop-down menu	choices are <i>Off</i> , <i>Verify</i> , and <i>On</i> ; carefully consider the section on Deduplication before changing this setting
ZFS Extra	bullet selection	used to specify if disk is used for storage (<i>None</i>), a log device, a cache device, or a spare

Extending a ZFS Volume

The *Volume to extend* drop-down menu in `Storage → Volumes → Volume Manager`, shown in [Figure 8.1](#), can be used to add additional disks to an existing ZFS volume. This drop-down menu will be empty if no ZFS volume exists.

Note: If the existing volume is encrypted, a warning message will remind you that the operation of extending a volume will reset the passphrase and recovery key. After extending the volume, you should immediately recreate both using the instructions in [Managing Encrypted Volumes](#).

After an existing volume has been selected from the drop-down menu, drag and drop the desired disks and select the desired volume layout. For example, you can:

- select an SSD with a volume layout of *Log (ZIL)* to add a log device to the ZFS pool. Selecting 2 SSDs will create a mirrored log device.
- select an SSD with a volume layout of *Cache (L2ARC)* to add a cache device to the ZFS pool.
- add additional disks to increase the capacity of the ZFS pool. The caveats to doing this are described below.

When adding disks to increase the capacity of a volume, ZFS supports the addition of virtual devices, known as vdevs, to an existing ZFS pool. A vdev can be a single disk, a stripe, a mirror, a RAIDZ1, RAIDZ2, or a RAIDZ3. **After a vdev is created, more drives cannot be added to that vdev**; however, you can stripe a new vdev (and its disks) with another of the **same type of existing vdev** to increase the overall size of ZFS the pool. In other words, when you extend a ZFS volume, you are really striping similar vdevs. Here are some examples:

- to extend a ZFS stripe, add one or more disks. Since there is no redundancy, you do not have to add the same amount of disks as the existing stripe.
- to extend a ZFS mirror, add the same number of drives. The resulting striped mirror is a RAID 10. For example, if you have 10 drives, you could start by creating a mirror of two drives, extending this mirror by creating another mirror of two drives, and repeating three more times until all 10 drives have been added.
- to extend a three drive RAIDZ1, add three additional drives. The result is a RAIDZ+0, similar to RAID 50 on a hardware controller.
- to extend a RAIDZ2 requires a minimum of four additional drives. The result is a RAIDZ2+0, similar to RAID 60 on a hardware controller.

If you try to add an incorrect number of disks to the existing vdev, an error message will appear, indicating the number of disks that are needed. You will need to select the correct number of disks in order to continue.

8.1.2 Change Permissions

Setting permissions is an important aspect of configuring volumes. 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 should be used to fine-tune the permissions of the files and directories that are created by the client.

The chapter on *Sharing* contains configuration examples for several types of permission scenarios. This section provides an overview of the screen that is used to set permissions.

Note: For users and groups to be available, they must either be first created using the instructions in *Account* or imported from a directory service using the instructions in *Directory Service*. If more than 50 users or groups are available, the drop-down menus described in this section will automatically truncate their display to 50 for performance reasons. In this case, start to type in the desired user or group name so that the display narrows its search to matching results.

After a volume or dataset is created, it is listed by its mount point name in *Storage → Volumes → View Volumes*. Clicking the *Change Permissions* icon for a specific volume/dataset displays the screen shown in Figure 8.3. Table 8.3 summarizes the options in this screen.

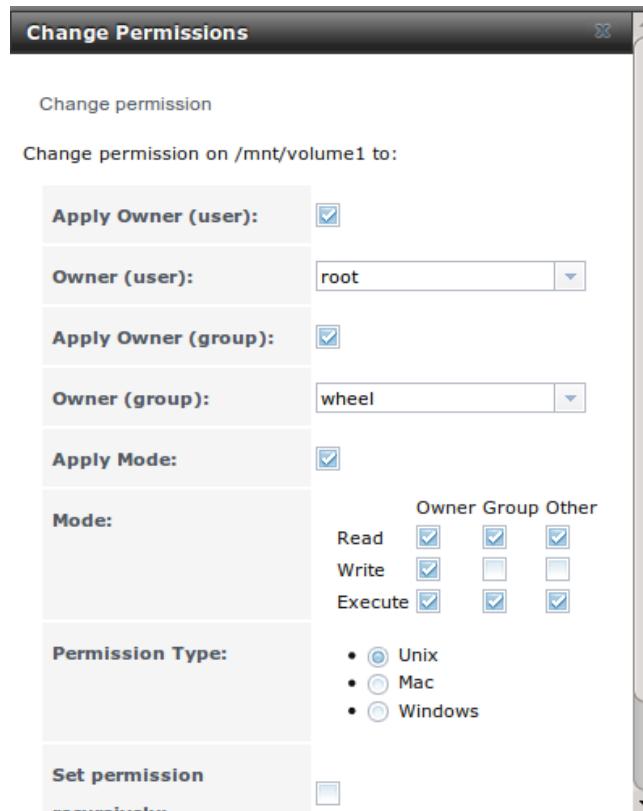


Fig. 8.3: Changing Permissions on a Volume or Dataset

Table 8.3: Options When Changing Permissions

Setting	Value	Description
Apply Owner (user)	check-box	uncheck to prevent new permission change from being applied to <i>Owner (user)</i> , see Note below
Owner (user)	drop-down menu	user to control the volume/dataset; users which were manually created or imported from a directory service will appear in the drop-down menu
Apply Owner (group)	check-box	uncheck to prevent new permission change from being applied to <i>Owner (group)</i> , see Note below
Owner (group)	drop-down menu	group to control the volume/dataset; groups which were manually created or imported from a directory service will appear in the drop-down menu
Apply Mode	check-box	uncheck to prevent new permission change from being applied to <i>Mode</i> , see Note below
Mode	check-boxes	only applies to the <i>Unix</i> or <i>Mac</i> “Permission Type” so will be grayed out if <i>Windows</i> is selected
Permission Type	bullet selection	choices are <i>Unix</i> , <i>Mac</i> or <i>Windows</i> ; select the type which matches the type of client accessing the volume/dataset
Set permission recursively	check-box	if checked, permissions will also apply to subdirectories of the volume/dataset; if data already exists on the volume/dataset, change the permissions on the client side to prevent a performance lag

Note: The *Apply Owner (user)*, *Apply Owner (group)*, and *Apply Mode* checkboxes allow fine-tuning of the change permissions behavior. By default, all boxes are checked and FreeNAS® resets the owner, group, and mode when the *Change* button is clicked. These checkboxes allow choosing which settings to change. For example, to change just the *Owner (group)* setting, uncheck the boxes *Apply Owner (user)* and *Apply Mode*.

If a mix of operating systems or clients will be accessing the volume/dataset using a non-SMB share, select the *Unix Permission Type*, as all clients understand them.

The *Windows Permission Type* augments traditional *Unix* permissions with ACLs. Use the *Windows Permission Type* for SMB shares or when the FreeNAS® system is a member of an Active Directory domain.

If you change your mind about the *Permission Type*, it is not necessary to recreate the volume/dataset, as existing data is not lost. However, changing from *Windows* to *Unix* or *Mac* will remove the extended permissions provided by ACLs from existing files.

When the *Windows Permission Type* is set, the ACLs are set to what Windows sets on new files and directories by default. The Windows client should then be used to fine-tune the permissions as required.

8.1.3 Create Dataset

An existing ZFS volume can be divided into datasets. Permissions, compression, deduplication, and quotas can be set on a per-dataset basis, allowing more granular control over access to storage 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 properties such as quotas and compression as well as create snapshots.

Note: ZFS provides thick provisioning using quotas and thin provisioning using reserved space.

Selecting an existing ZFS volume in the tree and clicking *Create Dataset* shows the screen in Figure 8.4.

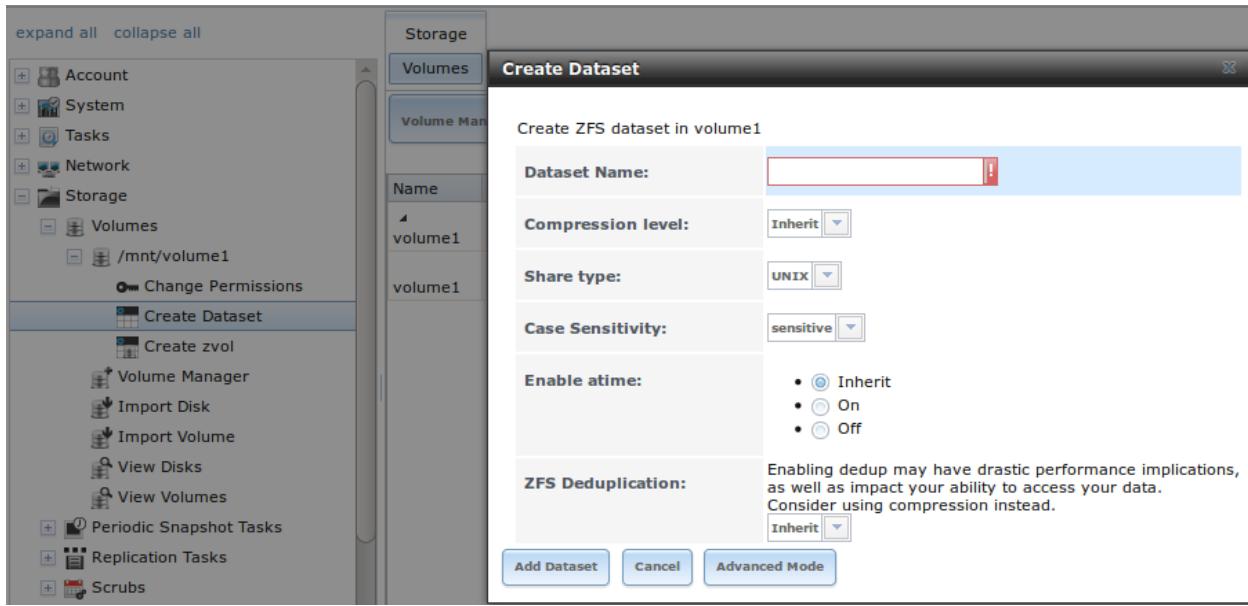


Fig. 8.4: Creating a ZFS Dataset

Table 8.4 summarizes the options available when creating a ZFS dataset. Some settings are only available in *Advanced Mode*. To see these settings, either click the *Advanced Mode* button, or configure the system to always display these settings by checking the box *Show advanced fields by default* in *System → Advanced*. Most attributes, except for the *Dataset Name*, *Case Sensitivity*, and *Record Size*, can be changed after dataset creation by highlighting the dataset name and clicking its *Edit Options* button in *Storage → Volumes → View Volumes*.

Table 8.4: ZFS Dataset Options

Setting	Value	Description
Dataset Name	string	mandatory; input a unique name for the dataset
Compression Level	drop-down menu	see the section on Compression for a description of the available algorithms
Share type	drop-down menu	select the type of share that will be used on the dataset; choices are <i>UNIX</i> for an NFS share, <i>Windows</i> for a SMB share, or <i>Mac</i> for an AFP share
Case Sensitivity	drop-down menu	choices are <i>sensitive</i> (default, assumes filenames are case sensitive), <i>insensitive</i> (assumes filenames are not case sensitive), or <i>mixed</i> (understands both types of filenames)
Enable atime	Inherit, On, or Off	controls whether the access time for files is updated when they are read; setting this property to <i>Off</i> avoids producing log traffic when reading files and can result in significant performance gains
Quota for this dataset	integer	only available in <i>Advanced Mode</i> ; default of 0 disables quotas; specifying a value means to use no more than the specified size and is suitable for user datasets to prevent users from hogging available space
Quota for this dataset and all children	integer	only available in <i>Advanced Mode</i> ; a specified value applies to both this dataset and any child datasets
Reserved space for this dataset	integer	only available in <i>Advanced Mode</i> ; default of 0 is unlimited; specifying a value means to keep at least this much space free and is suitable for datasets containing logs which could take up all available free space
Reserved space for this dataset and all children	integer	only available in <i>Advanced Mode</i> ; a specified value applies to both this dataset and any child datasets
ZFS Deduplication	drop-down menu	read the section on Deduplication before making a change to this setting
Record Size	drop-down menu	only available in <i>Advanced Mode</i> ; while ZFS automatically adapts the record size dynamically to adapt to data, if the data has a fixed size (e.g. a database), matching that size may result in better performance

After a dataset is created, you can click on that dataset and select *Create Dataset*, thus creating a nested dataset, or a dataset within a dataset. A zvol can also be created within a dataset. When creating datasets, double-check that you are using the *Create Dataset* option for the intended volume or dataset. If you get confused when creating a dataset on a volume, click all existing datasets to close them—the remaining *Create Dataset* will be for the volume.

Deduplication

Deduplication is the process of not creating duplicate copies of data in order to save space. Depending upon the amount of duplicate data, deduplicaton can improve storage capacity as less data is written and stored. However, the process of deduplication is RAM intensive and a general rule of thumb is 5 GB RAM per TB of storage to be deduplicated. **In most cases, using compression instead of deduplication will provide a comparable storage gain with less impact on performance.**

In FreeNAS®, deduplication can be enabled during dataset creation. Be forewarned that **there is no way to undedup the data within a dataset once deduplication is enabled**, as disabling deduplication has **NO EFFECT** on existing data. The more data you write to a deduplicated dataset, the more RAM it requires and when the system starts storing the DDTs (dedup tables) on disk because they no longer fit into RAM, performance craters. Furthermore, importing an unclean pool can require between 3-5 GB of RAM per TB of deduped data, and if the system does not have the needed RAM, it will panic, with the only solution being to add more RAM or to recreate the pool. **Think carefully before**

enabling dedup! This [article](#) provides a good description of the value versus cost considerations for deduplication.

Unless you have a lot of RAM and a lot of duplicate data, do not change the default deduplication setting of “Off”. For performance reasons, consider using compression rather than turning this option on.

If deduplication is changed to *On*, duplicate data blocks are removed synchronously. The result is that only unique data is stored and common components are shared among files. If deduplication is changed to *Verify*, ZFS will do a byte-to-byte comparison when two blocks have the same signature to make sure that the block contents are identical. Since hash collisions are extremely rare, *Verify* is usually not worth the performance hit.

Note: once deduplication is enabled, the only way to disable it is to use the `zfs set dedup=off dataset_name` command from [Shell](#). However, any data that is already stored as deduplicated will not be undeduplicated as only newly stored data after the property change will not be deduplicated. The only way to remove existing deduplicated data is to copy all of the data off of the dataset, set the property to off, then copy the data back in again. Alternately, create a new dataset with *ZFS Deduplication* left disabled, copy the data to the new dataset, and destroy the original dataset.

Compression

When selecting a compression type, you need to balance performance with the amount of disk space saved by compression. Compression is transparent to the client and applications as ZFS automatically compresses data as it is written to a compressed dataset or zvol and automatically decompresses that data as it is read. These compression algorithms are supported:

- **lz4:** recommended compression method as it allows compressed datasets to operate at near real-time speed. This algorithm only compresses the files that will benefit from compression. By default, ZFS pools made using FreeNAS® 9.2.1 or higher use this compression method, meaning that this algorithm is used if the *Compression level* is left at *Inherit* when creating a dataset or zvol.
- **gzip:** varies from levels 1 to 9 where *gzip fastest* (level 1) gives the least compression and *gzip maximum* (level 9) provides the best compression but is discouraged due to its performance impact.
- **zle:** fast but simple algorithm to eliminate runs of zeroes.
- **lzjb:** provides decent data compression, but is considered deprecated as *lz4* provides much better performance.

If you select *Off* as the *Compression level* when creating a dataset or zvol, compression will not be used on the dataset/zvol. This is not recommended as using *lz4* has a negligible performance impact and allows for more storage capacity.

8.1.4 Create zvol

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

To create a zvol, select an existing ZFS volume or dataset from the tree then click *Create zvol* to open the screen shown in [Figure 8.5](#).

The configuration options are described in [Table 8.5](#). Some settings are only available in *Advanced Mode*. To see these settings, either click the *Advanced Mode* button or configure the system to always display these settings by checking *Show advanced fields by default* in *System → Advanced*.

Fig. 8.5: Creating a zvol

Table 8.5: zvol Configuration Options

Setting	Value	Description
zvol Name	string	mandatory; input a name for the zvol
Size for this zvol	integer	specify size and value such as <i>10Gib</i> ; if the size is more than 80% of the available capacity, the creation will fail with an “out of space” error unless <i>Force size</i> is checked
Force size	check-box	by default, the system will not let you create a zvol if that operation will bring the pool to over 80% capacity; while NOT recommended , checking this box will force the creation of the zvol in this situation
Com-pression level	drop-down menu	see the section on <i>Compression</i> for a description of the available algorithms
Sparse volume	check-box	used to provide thin provisioning; use with caution for when this option is selected, writes will fail when the pool is low on space
Block size	drop-down menu	only available in <i>Advanced Mode</i> and by default is based on the number of disks in pool; can be set to match the block size of the filesystem which will be formatted onto the iSCSI target

8.1.5 Import Disk

The Volume → Import Disk screen, shown in Figure 8.6, is used to import a **single** disk that has been formatted with the UFS, NTFS, MSDOS, or EXT2 filesystem. The import is meant to be a temporary measure to copy the data from a disk to an existing ZFS dataset. Only one disk can be imported at a time.

Note: Imports of EXT3 or EXT4 filesystems are possible in some cases, although neither is fully supported. EXT3 journaling is not supported, so those filesystems must have an external *fsck* utility, like the one provided by [E2fsprogs utilities](#), run on them before import. EXT4 filesystems with extended attributes or inodes greater than 128 bytes are not supported. EXT4 filesystems with EXT3 journaling must have an *fsck* run on them before import, as described

above.

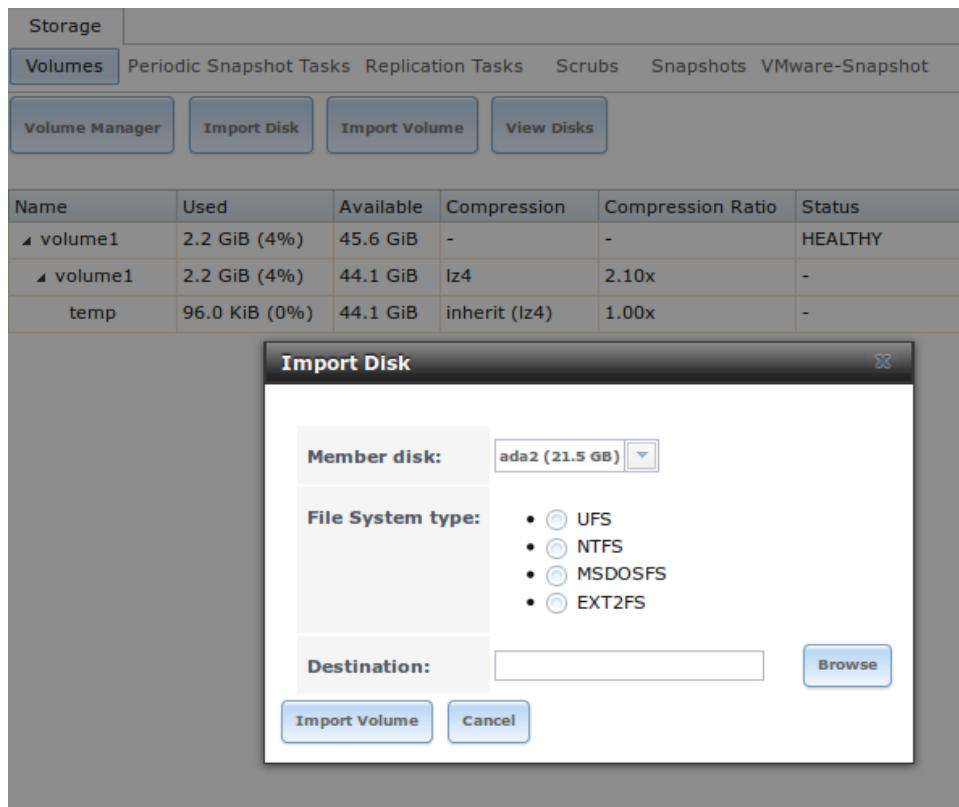


Fig. 8.6: Importing a Disk

Use the drop-down menu to select the disk to import, select the type of filesystem on the disk, and browse to the ZFS dataset that will hold the copied data. When you click *Import Volume*, the disk is mounted, its contents are copied to the specified ZFS dataset, and the disk is unmounted after the copy operation completes.

8.1.6 Import Volume

If you click `Storage → Volumes → Import Volume`, you can configure FreeNAS® to use an **existing ZFS pool**. This action is typically performed when an existing FreeNAS® system is re-installed. Since the operating system is separate from the storage disks, a new installation does not affect the data on the disks. However, the new operating system needs to be configured to use the existing volume.

Figure 8.7 shows the initial pop-up window that appears when you import a volume.

If you are importing an unencrypted ZFS pool, select *No: Skip to import* to open the screen shown in Figure 8.8.

Existing volumes should be available for selection from the drop-down menu. In the example shown in Figure 8.8, the FreeNAS® system has an existing, unencrypted ZFS pool. Once the volume is selected, click the *OK* button to import the volume.

If an existing ZFS pool does not show in the drop-down menu, run `zpool import` from *Shell* to import the pool.

If you plan to physically install ZFS formatted disks from another system, be sure to export the drives on that system to prevent an “in use by another machine” error during the import.

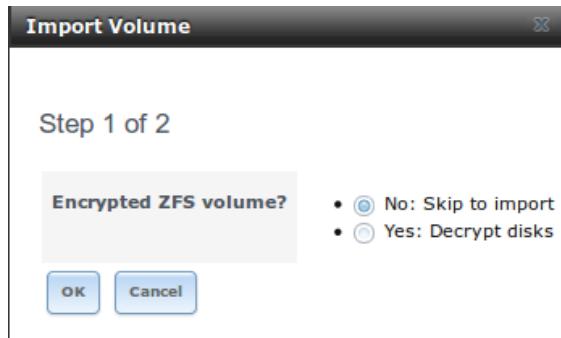


Fig. 8.7: Initial Import Volume Screen



Fig. 8.8: Importing a Non-Encrypted Volume

If you suspect that your hardware is not being detected, run `camcontrol devlist` from [Shell](#). If the disk does not appear in the output, check to see if the controller driver is supported or if it needs to be loaded using [Tunables](#).

Importing an Encrypted Pool

If you are importing an existing GELI-encrypted ZFS pool, you must decrypt the disks before importing the pool. In [Figure 8.7](#), select *Yes: Decrypt disks* to access the screen shown in [Figure 8.9](#).

Select the disks in the encrypted pool, browse to the location of the saved encryption key, input the passphrase associated with the key, then click *OK* to decrypt the disks.

Note: The encryption key is required to decrypt the pool. If the pool cannot be decrypted, it cannot be re-imported after a failed upgrade or lost configuration. This means that it is **very important** to save a copy of the key and to remember the passphrase that was configured for the key. Refer to [Managing Encrypted Volumes](#) for instructions on how to manage the keys for encrypted volumes.

Once the pool is decrypted, it will appear in the drop-down menu of [Figure 8.8](#). Click the *OK* button to finish the volume import.

8.1.7 View Disks

[Storage](#) → [Volumes](#) → [View Disks](#) shows all of the disks recognized by the FreeNAS® system. An example is shown in [Figure 8.10](#).

The current configuration of each device is displayed. Click a disk's entry and then its *Edit* button to change its configuration. The configurable options are described in [Table 8.6](#).

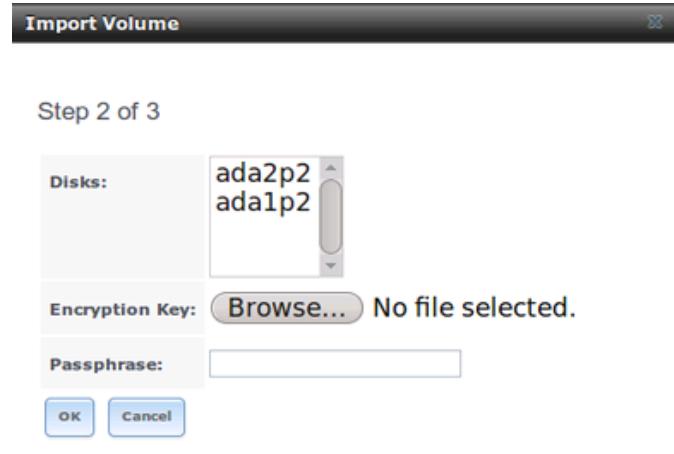


Fig. 8.9: Decrypting Disks Before Importing a ZFS Pool

View Disks									
Name	Serial	Disk Size	Description	Transfer Mode	HDD Standby	Advanced Power Management	Acoustic Level	Enable S.M.A.R.T.	S.M.A.R.T. extra options
ada0	JP2940HZ3SNPDC	1.0 TB		Auto	Always On	Disabled	Disabled	true	
ada1	JP2940HZ3SN61C	1.0 TB		Auto	Always On	Disabled	Disabled	true	
ada2	JP2940HZ3SNPVC	1.0 TB		Auto	Always On	Disabled	Disabled	true	
ada3	JP2940HZ3SK5VC	1.0 TB		Auto	Always On	Disabled	Disabled	true	
da1	0			Auto	Always On	Disabled	Disabled	true	
da2	0			Auto	Always On	Disabled	Disabled	true	

At the bottom left of the table area are 'Edit' and 'Wipe' buttons.

Fig. 8.10: Viewing Disks

Table 8.6: Disk Options

Setting	Value	Description
Name	string	read-only value showing FreeBSD device name for disk
Serial	string	read-only value showing the disk's serial number
Description	string	optional
HDD Standby	drop-down menu	indicates the time of inactivity (in minutes) before the drive enters standby mode in order to conserve energy; this forum post demonstrates how to determine if a drive has spun down
Advanced Power Management	drop-down menu	default is <i>Disabled</i> , can select a power management profile from the menu
Acoustic Level	drop-down menu	default is <i>Disabled</i> ; can be modified for disks that understand AAM
Enable S.M.A.R.T.	checkbox	enabled by default if the disk supports S.M.A.R.T.; unchecking this box will disable any configured S.M.A.R.T. Tests for the disk
S.M.A.R.T. extra options	string	additional smartctl(8) options

Clicking a disk's entry will also display its *Wipe* button which can be used to blank a disk while providing a progress bar of the wipe's status. Use this option before discarding a disk.

Note: If a disk's serial number is not displayed in this screen, use the [smartctl](#) command from [Shell](#). For example, to determine the serial number of disk *ada0*, type `smartctl -a /dev/ada0 | grep Serial`.

8.1.8 View Volumes

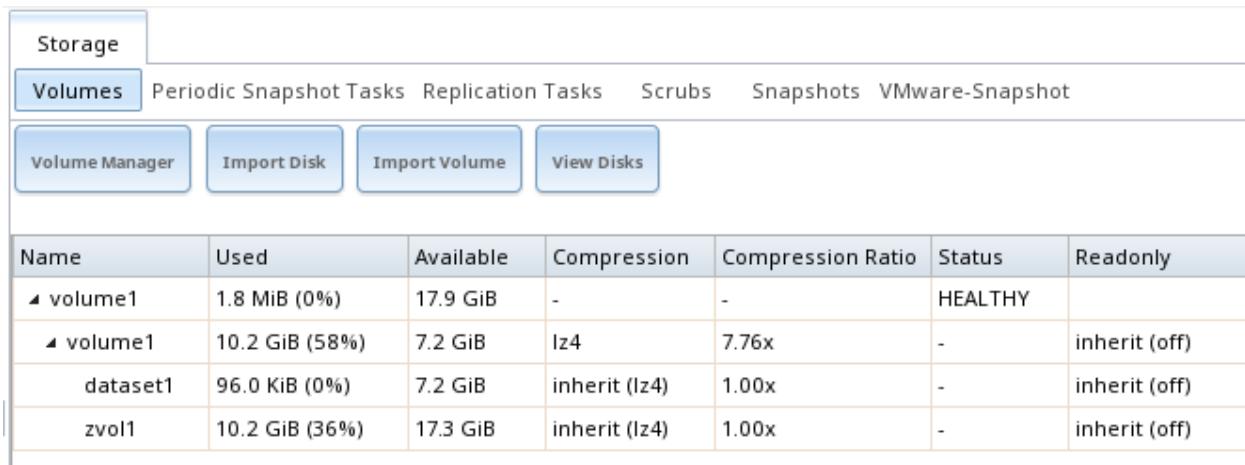
Storage → Volumes → View Volumes is used to view and further configure existing ZFS pools, datasets, and zvols. The example shown in [Figure 8.11](#) shows one ZFS pool (*volume1*) with two datasets (the one automatically created with the pool, *volume1*, and *dataset1*) and one zvol (*zvol1*).

Note that in this example, there are two datasets named *volume1*. The first represents the ZFS pool and its *Used* and *Available* entries reflect the total size of the pool, including disk parity. The second represents the implicit or root dataset and its *Used* and *Available* entries indicate the amount of disk space available for storage.

Buttons are provided for quick access to *Volume Manager*, *Import Disk*, *Import Volume*, and *View Disks*. If the system has multipath-capable hardware, an extra button will be added, *View Multipaths*. For each entry, the columns indicate the *Name*, how much disk space is *Used*, how much disk space is *Available*, the type of *Compression*, the *Compression Ratio*, the *Status*, and whether it is mounted as read-only.

Clicking the entry for a pool causes several buttons to appear at the bottom of the screen. The buttons perform these actions:

Detach Volume: allows you to either export the pool or to delete the contents of the pool, depending upon the choice you make in the screen shown in [Figure 8.12](#). The *Detach Volume* screen displays the current used space and indicates if there are any shares, provides checkboxes to *Mark the disks as new (destroy data)* and to *Also delete the share's configuration*, asks if you are sure that you want to do this, 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 the box to mark the disks as new, 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 pool from one system to another, perform this export action first as it flushes any unwritten data to disk, writes data to the disk indicating that the export was done, and removes all knowledge of the



The screenshot shows the FreeNAS Storage Volumes interface. At the top, there are tabs for Storage, Volumes (which is selected), Periodic Snapshot Tasks, Replication Tasks, Scrubs, Snapshots, and VMware-Snapshot. Below the tabs are buttons for Volume Manager, Import Disk, Import Volume, and View Disks. The main area displays a table of volumes and datasets:

Name	Used	Available	Compression	Compression Ratio	Status	Readonly
volume1	1.8 MiB (0%)	17.9 GiB	-	-	HEALTHY	
volume1	10.2 GiB (58%)	7.2 GiB	lz4	7.76x	-	inherit (off)
dataset1	96.0 KiB (0%)	7.2 GiB	inherit (lz4)	1.00x	-	inherit (off)
zvol1	10.2 GiB (36%)	17.3 GiB	inherit (lz4)	1.00x	-	inherit (off)

Fig. 8.11: Viewing Volumes

pool from the system. **If you do check the box to mark the disks as new, the pool and all the data in its datasets, zvols, and shares will be destroyed and the underlying disks will be returned to their raw state.**

Scrub Volume: scrubs and how to schedule them are described in more detail in [Scrubs](#). This button allows you to manually initiate a scrub. Since a scrub is I/O intensive and can negatively impact performance, you should not initiate one while the system is busy. A *Cancel* button is provided to cancel a scrub. If a scrub is cancelled, the next scrub will start over from the beginning, not where the cancelled scrub left off. To view the current status of a running scrub or the statistics from the last completed scrub, click the *Volume Status* button.

Volume Status: as shown in the example in [Figure 8.13](#), this screen shows the device name and status of each disk in the ZFS pool as well as any read, write, or checksum errors. It also indicates the status of the latest ZFS scrub. Clicking the entry for a device causes buttons to appear to edit the device's options (shown in [Figure 8.14](#)), offline or online the device, or replace the device (as described in [Replacing a Failed Drive](#)).

Upgrade: used to upgrade the pool to the latest ZFS features, as described in [Upgrading a ZFS Pool](#). This button will not appear if the pool is running the latest versions of feature flags.

Selecting a disk in *Volume Status* and clicking its *Edit Disk* button shows the screen in [Figure 8.14](#). [Table 8.6](#) summarizes the configurable options.

Note: Versions of FreeNAS® prior to 8.3.1 required a reboot to apply changes to the *HDD Standby*, *Advanced Power Management*, and *Acoustic Level* settings. As of 8.3.1, changes to these settings are applied immediately.

Clicking a dataset in *Storage* → *Volumes* → *View Volumes* causes buttons to appear at the bottom of the screen, providing these options:

Change Permissions: edit the dataset's permissions as described in [Change Permissions](#).

Create Snapshot: create a one-time snapshot. To schedule the regular creation of snapshots, instead use [Periodic Snapshot Tasks](#).

Destroy Dataset: clicking the *Destroy Dataset* button causes the browser window to turn red to indicate that this is a destructive action. The *Destroy Dataset* screen forces you to check the box *I'm aware this will destroy all child datasets and snapshots within this dataset* before it will perform this action.

Edit Options: edit the volume's properties described in [Table 8.4](#). Note that it will not allow changing the dataset's name.

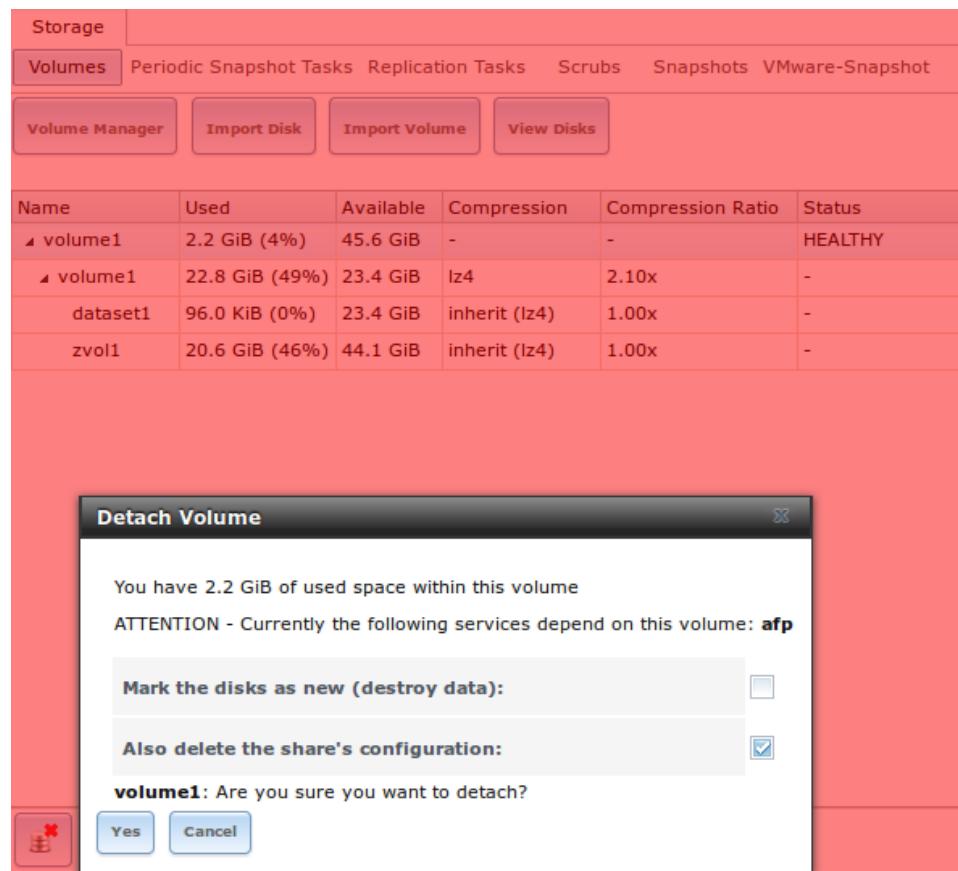


Fig. 8.12: Detach or Delete a Volume

Volume Status				
Scrub				
Status: Completed				
Errors: 0 Repaired: 0 Date: Fri Aug 29 10:31:21 2014				
Name	Read	Write	Checksum	Status
volume1	0	0	0	ONLINE
raidz2-0	0	0	0	ONLINE
ada4p2	0	0	0	ONLINE
ada3p2	0	0	0	ONLINE
ada2p2	0	0	0	ONLINE
ada1p2	0	0	0	ONLINE

Fig. 8.13: Volume Status

Edit

Name:	ada0
Serial:	JP2940HZ3SNPDC
Description:	
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:	

OK Cancel

Fig. 8.14: Editing a Disk

Create Dataset: used to create a child dataset within this dataset.

Create zvol: create a child zvol within this dataset.

Clicking a zvol in Storage → Volumes → View Volumes causes icons to appear at the bottom of the screen: *Create Snapshot*, *Edit zvol*, and *Destroy zvol*. Similar to datasets, a zvol's name cannot be changed, and destroying a zvol requires confirmation.

Managing Encrypted Volumes

If the *Encryption* box is checked during the creation of a pool, additional buttons appear in the entry for the pool in Storage → Volumes → View Volumes. An example is shown in Figure 8.15.

Name	Used	Available	Compression	Compression Ratio	Status
volume1	1.3 MiB (0%)	47.7 GiB	-	-	HEALTHY
volume1	932.0 KiB (0%)	46.3 GiB	lz4	1.00x	-

Fig. 8.15: Encryption Icons Associated with an Encrypted Pool

These additional encryption buttons are used to:

Create/Change Passphrase: click this button to set and confirm the passphrase associated with the GELI encryption key. You will be prompted to enter and repeat the desired passphrase and a red warning reminds you to *Remember to add a new recovery key as this action invalidates the previous recovery key*. Unlike a password, a passphrase can contain spaces and is typically a series of words. A good passphrase is easy to remember (like the line to a song or piece of literature) but hard to guess (people who know you should not be able to guess the passphrase). **Remember this passphrase as you cannot re-import an encrypted volume without it.** In other words, if you forget the passphrase, the data on the volume can become inaccessible if you need to re-import the pool. Protect this passphrase as anyone who knows it could re-import your encrypted volume, thwarting the reason for encrypting the disks in the first place.

Once the passphrase is set, the name of this button will change to *Change Passphrase*. After setting or changing the passphrase, it is important to immediately create a new recovery key by clicking the *Add recovery key* button. This way, if the passphrase is forgotten, the associated recovery key can be used instead.

Download Key: click this icon to download a backup copy of the GELI encryption key. The encryption key is saved to the client system, not on the FreeNAS® system. You will be prompted to input the password used to access the FreeNAS® administrative GUI before the selecting the directory in which to store the key. Since the GELI encryption key is separate from the FreeNAS® configuration database, **it is highly recommended to make a backup of the key. If the key is every lost or destroyed and there is no backup key, the data on the disks is inaccessible.**

Encryption Re-key: generates a new GELI encryption key. Typically this is only performed when the administrator suspects that the current key may be compromised. This action also removes the current passphrase.

Add recovery key: generates a new recovery key. This screen prompts for entry of the password used to access the FreeNAS® administrative GUI and then to select the directory in which to save the key. Note that the recovery key is saved to the client system, not on the FreeNAS® system. This recovery key can be used if the passphrase is forgotten. **Always immediately** add a recovery key whenever the passphrase is changed.

Remove recover key: Typically this is only performed when the administrator suspects that the current recovery key may be compromised. **Immediately** create a new passphrase and recovery key.

Note: The passphrase, recovery key, and encryption key must be protected. Do not reveal the passphrase to others. On the system containing the downloaded keys, take care that the system and its backups are protected. Anyone who has the keys has the ability to re-import the disks if they are discarded or stolen.

Warning: If a re-key fails on a multi-disk system, an alert is generated. **Do not ignore this alert** as doing so may result in the loss of data.

8.1.9 View Multipaths

FreeNAS® uses [gmultipath\(8\)](#) to provide multipath I/O support on systems containing hardware that is capable of multipath. An example would be a dual SAS expander backplane in the chassis or an external JBOD.

Multipath hardware adds fault tolerance to a NAS as the data is still available even if one disk I/O path has a failure.

FreeNAS® automatically detects active/active and active/passive multipath-capable hardware. Any multipath-capable devices that are detected will be placed in multipath units with the parent devices hidden. The configuration will be displayed in *Storage → Volumes → View Multipaths*. Note that this option is not be displayed in the *Storage → Volumes* tree on systems that do not contain multipath-capable hardware.

8.1.10 Replacing a Failed Drive

With any form of redundant RAID, failed drives must be replaced as soon as possible to repair the degraded state of the RAID. Depending on the hardware's capabilities, it might be necessary to reboot to replace the failed drive. Hardware that supports AHCI does not require a reboot.

Note: Striping (RAID0) does not provide redundancy. If a disk in a stripe fails, the volume will be destroyed and must be recreated and the data restored from backup.

Note: If your pool is encrypted with GELI, refer to [Replacing an Encrypted Drive](#) before proceeding.

Before physically removing the failed device, go to *Storage → Volumes → View Volumes*. Select the volume's name. At the bottom of the interface are several icons, one of which is *Volume Status*. Click the *Volume Status* icon and locate the failed disk. Then perform these steps:

1. If the disk is formatted with ZFS, click the disk's entry then its *Offline* button in order to change that disk's status to OFFLINE. This step is needed to properly remove the device from the ZFS pool and to prevent swap issues. If the hardware supports hot-pluggable disks, click the disk's *Offline* button, pull the disk, then skip to step 3. If there is no *Offline* button but only a *Replace* button, the disk is already offline and you can safely skip this step.

Note: If the process of changing the disk's status to OFFLINE fails with a “disk offline failed - no valid replicas” message, the ZFS volume must be scrubbed first with the *Scrub Volume* button in *Storage → Volumes → View Volumes*. After the scrub completes, try to *Offline* the disk again before proceeding.

2. If the hardware is not AHCI capable, shut down the system to physically replace the disk. When finished, return to the GUI and locate the OFFLINE disk.
3. After the disk has been replaced and is showing as OFFLINE, click the disk again and then click its *Replace* button. Select the replacement disk from the drop-down menu and click the *Replace Disk* button. After clicking the *Replace Disk* button, the ZFS pool starts to resilver and the status of the resilver is displayed.
4. After the drive replacement process is complete, re-add the replaced disk in the [S.M.A.R.T. Tests](#) screen.

In the example shown in [Figure 8.16](#), a failed disk is being replaced by disk *ada5* in the volume named *volume1*.

After the resilver is complete, *Volume Status* shows a *Completed* resilver status and indicates any errors. [Figure 8.17](#) indicates that the disk replacement was successful in this example.

Replacing an Encrypted Drive

If the ZFS pool is encrypted, additional steps are needed when replacing a failed drive.

First, make sure that a passphrase has been set using the instructions in [Encryption before](#) attempting to replace the failed drive. Then, follow the steps 1 and 2 as described above. During step 3, you will be prompted to input and confirm the passphrase for the pool. Enter this information then click the *Replace Disk* button. Wait until the resilvering is complete.

Next, restore the encryption keys to the pool. **If the following additional steps are not performed before the next reboot, you may lose access to the pool permanently.**

1. Highlight the pool that contains the disk you just replaced and click the *Encryption Re-key* button in the GUI. You will need to enter the *root* password.
2. Highlight the pool that contains the disk you just replaced and click *Create Passphrase* and enter the new passphrase. The old passphrase can be reused if desired.
3. Highlight the pool that contains the disk you just replaced and click the *Download Key* button in order to save the new encryption key. Since the old key will no longer function, any old keys can be safely discarded.
4. Highlight the pool that contains the disk you just replaced and click the *Add Recovery Key* button in order to save the new recovery key. The old recovery key will no longer function, so it can be safely discarded.

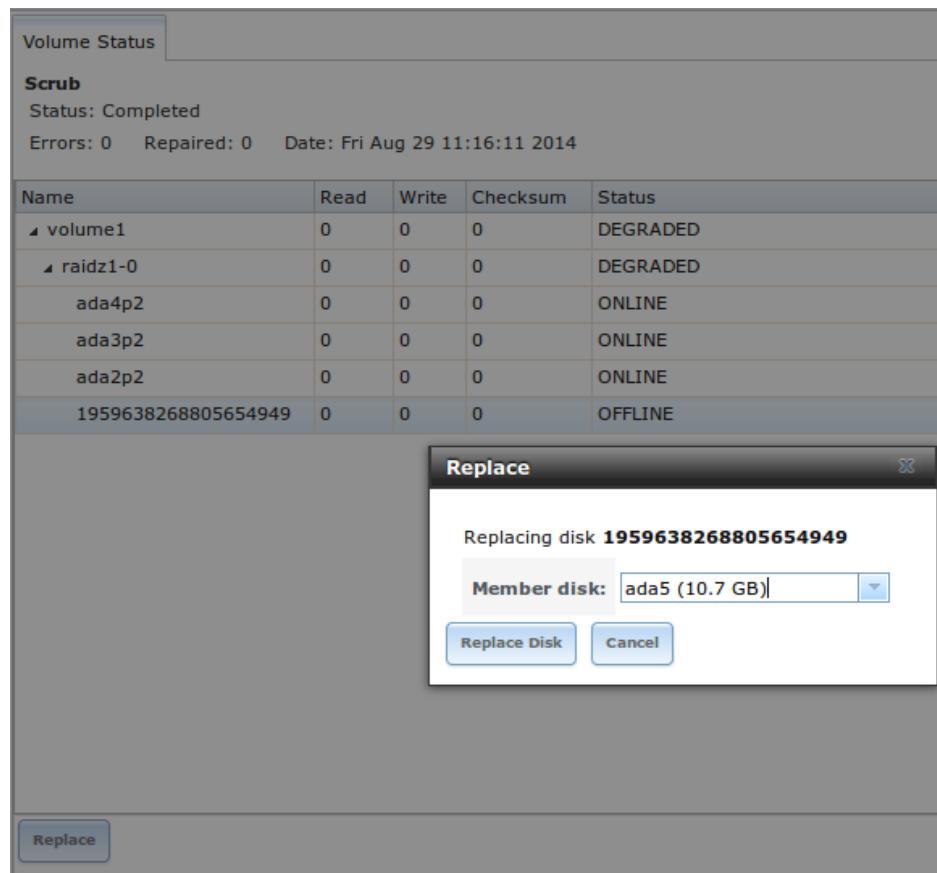


Fig. 8.16: Replacing a Failed Disk

The screenshot shows the FreeNAS Volume Status interface. It displays the results of a completed resilvering operation. Below this is a table of volume components:

Name	Read	Write	Checksum	Status
volume1	0	0	0	ONLINE
raidz1-0	0	0	0	ONLINE
ada4p2	0	0	0	ONLINE
ada3p2	0	0	0	ONLINE
ada2p2	0	0	0	ONLINE
ada5p2	0	0	0	ONLINE

Fig. 8.17: Disk Replacement is Complete

Removing a Log or Cache Device

Added log or cache devices appear in Storage → Volumes → View Volumes → Volume Status . Clicking the device enables its *Replace* and *Remove* buttons.

Log and cache devices can be safely removed or replaced with these buttons. Both types of devices improve performance, and throughput can be impacted by their removal.

8.1.11 Replacing Drives to Grow a ZFS Pool

The recommended method for expanding the size of a ZFS pool is to pre-plan the number of disks in a vdev and to stripe additional vdevs using *Volume Manager* as additional capacity is needed.

However, this is not an option if there are no open drive ports and a SAS/SATA HBA card cannot be added. In this case, one disk at a time can be replaced with a larger disk, waiting for the resilvering process to incorporate the new disk into the pool, then repeating with another disk until all of the original disks have been replaced.

The safest way to perform this is to use a spare drive port or an eSATA port and a hard drive dock. The process follows these steps:

1. Shut down the system.
2. Install one new disk.
3. Start up the system.
4. Go to Storage → Volumes , select the pool to expand and click the *Volume Status* button. Select a disk and click the *Replace* button. Choose the new disk as the replacement.
5. The status of the resilver process can be viewed by running `zpool status`. When the new disk has resilvered, the old one will be automatically offline. The system is then shut down to physically remove the replaced disk. One advantage of this approach is that there is no loss of redundancy during the resilver.

If a spare drive port is not available, a drive can be replaced with a larger one using the instructions in *Replacing a Failed Drive*. This process is slow and places the :system in a degraded state. Since a failure at this point could be disastrous, **do not attempt this method unless the system has a reliable backup**. Replace one drive at a time and wait for the resilver process to complete on the replaced drive before replacing the next drive. After all the drives are replaced and the final resilver completes, the added space will appear in the pool.

8.2 Periodic Snapshot Tasks

A periodic snapshot task allows scheduling the creation of read-only versions of ZFS volumes and datasets 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 0 MB of storage, but as changes are made to files, the snapshot size changes to reflect the size of the changes.

Snapshots provide a clever way of keeping a history of files, providing a way to recover an older copy or even a deleted file. For this reason, many administrators take snapshots often (perhaps every 15 minutes), store them for a period of time (possibly a month), and store them on another system (typically 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.

An existing ZFS volume is required before creating a snapshot. Creating a volume is described in *Volume Manager*.

To create a periodic snapshot task, click Storage → Periodic Snapshot Tasks → Add Periodic Snapshot which opens the screen shown in [Figure 8.18](#). [Table 8.7](#) summarizes the fields in this screen.

Note: If only a one-time snapshot is needed, instead use Storage → Volumes → View Volumes and click the *Create Snapshot* button for the volume or dataset to snapshot.

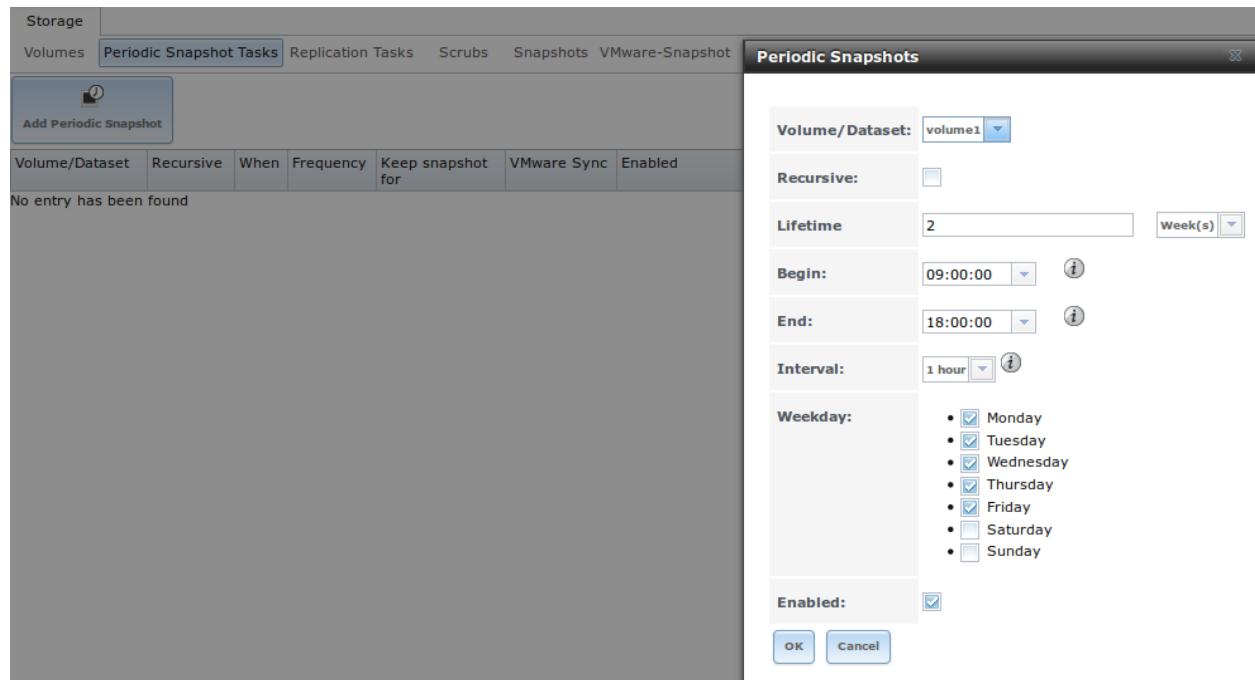


Fig. 8.18: Creating a Periodic Snapshot

Table 8.7: Options When Creating a Periodic Snapshot

Setting	Value	Description
Vol- ume/Dataset	drop-down menu	select an existing ZFS volume, dataset, or zvol
Recur- sive	checkbox	select this box to take separate snapshots of the volume/dataset and each of its child datasets; if unchecked, a single snapshot is taken of only the specified volume/dataset, but not any child datasets
Life- time	integer and drop-down menu	how long to keep the snapshot on this system; if the snapshot is replicated, it is not removed from the receiving system when the lifetime expires
Begin	drop-down menu	do not create snapshots before this time of day
End	drop-down menu	do not create snapshots after this time of day
Interval	drop-down menu	how often to take snapshot between <i>Begin</i> and <i>End</i> times
Week- day	checkboxes	which days of the week to take snapshots
En- abled	checkbox	uncheck to disable the scheduled snapshot task without deleting it

If the *Recursive* box is checked, you do not need to create snapshots for every dataset individually as they are included in the snapshot. The downside is that there is no way to exclude certain datasets from being included in a recursive snapshot.

When the *OK* button is clicked, a snapshot is taken and the task will be repeated according to your settings.

After creating a periodic snapshot task, an entry for the snapshot task will be added to *View Periodic Snapshot Tasks*. Click an entry to access its *Edit* and *Delete* buttons.

8.3 Replication Tasks

A replication task makes it possible to automate the copy of ZFS snapshots to another system over an encrypted connection. This allows you to create an off-site backup of a ZFS dataset or pool.

This section will refer to the system generating the ZFS snapshots as *PUSH* and the system receiving a copy of the ZFS snapshots as *PULL*.

These prerequisites must be met before replication tasks can be configured:

- a ZFS pool must exist on both *PUSH* and *PULL*.
- a periodic snapshot task must be created on *PUSH*. You will not be able to create a replication task before the first snapshot exists.
- the SSH service must be enabled on *PULL*. The first time the service is enabled, it will generate the required SSH keys.

A replication task uses the following keys:

- `/data/sshreplication.pub` : the RSA public key used for authenticating the *PUSH* replication user. This key needs to be copied to the replication user account on *PULL*.
- `/etc/ssh/ssh_host_rsa_key.pub` : the RSA host public key of *PULL* used to authenticate the receiving side in order to prevent a man-in-the-middle attack. This key needs to be copied to the replication task on *PUSH*.

This section demonstrates how to configure a replication task between these two FreeNAS® systems:

- 192.168.2.2 will be referred to as *PUSH*. This system has a periodic snapshot task for the ZFS dataset `/mnt/local/data`.
- 192.168.2.6 will be referred to as *PULL*. This system has an existing ZFS volume named `/mnt/remote` which will store the pushed snapshots.

8.3.1 Configure PULL

A copy of the public key for the replication user on *PUSH* needs to be pasted to the public key of the replication user on the *PULL* system.

To obtain a copy of the replication key: on *PUSH* go to Storage → Replication Tasks → View Replication Tasks . Click the *View Public Key* button and copy its contents. An example is shown in Figure 8.19.

Go to *PULL* and click Account → Users → View Users . Click the *Modify User* button for the user account you will be using for replication (by default this is the *root* user). Paste the copied key into the *SSH Public Key* field and click *OK*. If a key already exists, append the new text after the existing key.

On *PULL*, ensure that the SSH service is enabled in Services → Control Services . Start it if it is not already running.

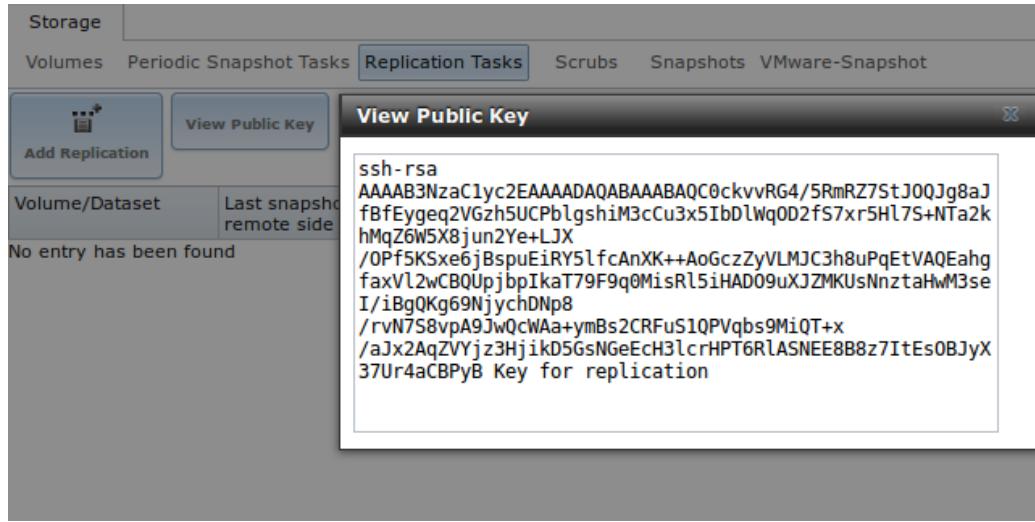


Fig. 8.19: Copy the Replication Key

8.3.2 Configure PUSH

On *PUSH*, verify that a periodic snapshot task has been created and that at least one snapshot is listed in Storage → Snapshots .

To create the replication task, click Storage → Replication Tasks → Add Replication which opens the screen shown in Figure 8.20. For this example, the required configuration is as follows:

- the Volume/Dataset is local/data
- the Remote ZFS Volume/Dataset is remote
- the Remote hostname is 192.168.2.6
- the Begin and End times are at their default values, meaning that replication will occur whenever a snapshot is created
- once the Remote hostname is input, click the *SSH Key Scan* button; if the address is reachable and the SSH service is running on *PULL*, its key will automatically be populated to the *Remote hostkey* box

Table 8.8 summarizes the available options in the *Add Replication* screen.

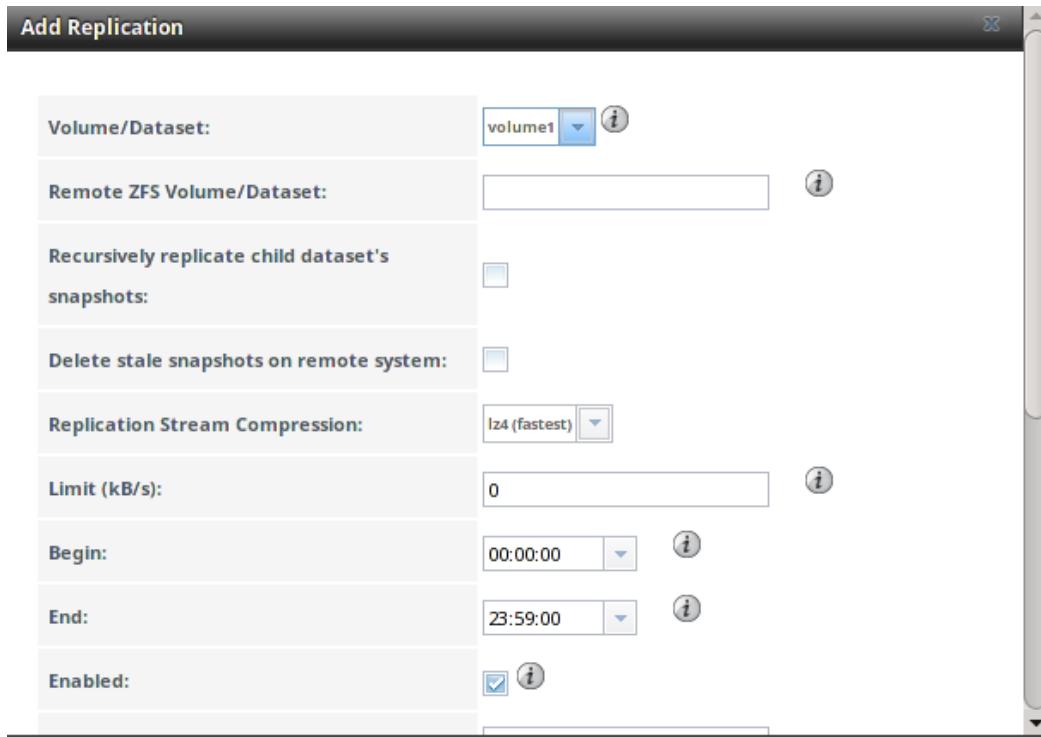


Fig. 8.20: Adding a Replication Task

Table 8.8: Adding a Replication Task

Setting	Value	Description
Volume/Dataset	drop-down menu	the ZFS volume or dataset on <i>PUSH</i> containing the snapshots to be replicated; the drop-down menu will be empty if a snapshot does not already exist
Remote ZFS Volume/Dataset	string	the ZFS volume on <i>PULL</i> that will store the snapshots; <code>/mnt/</code> is assumed and should not be included in the path
Recursively replicate	check-box	if checked will also replicate child datasets
Delete stale snapshots	check-box	if checked, will delete any previous snapshots on <i>PULL</i> which are no longer stored on <i>PUSH</i>
Replication Stream Compression	drop-down menu	choices are <i>lz4 (fastest)</i> , <i>pigz (all rounder)</i> , <i>plzip (best compression)</i> , or <i>Off</i> (no compression); selecting a compression algorithm can reduce the size of the data being replicated
Limit (kB/s)	integer	limits replication speed to specified value in kilobytes/second; default of <i>0</i> is unlimited
Begin	drop-down menu	the replication cannot start before this time; the times selected in the <i>Begin</i> and <i>End</i> fields set the replication window for when replication can occur
End	drop-down menu	the replication must start by this time; once started, replication will occur until it is finished (see NOTE below)
Enabled	check-box	uncheck to disable the scheduled replication task without deleting it
Remote hostname	string	IP address or DNS name of <i>PULL</i>
Remote port	string	must match port being used by SSH service on <i>PULL</i>
Dedicated User Enabled	check-box	allows a user account other than root to be used for replication
Dedicated User	drop-down menu	only available if <i>Dedicated User Enabled</i> is checked; select the user account to be used for replication

By default, replication occurs when snapshots occur. For example, if snapshots are scheduled for every 2 hours, replication occurs every 2 hours. The initial replication can take a significant period of time, from many hours to possibly days, as the structure of the entire ZFS pool needs to be recreated on the remote system. The actual time will depend upon the size of the pool and the speed of the network. Subsequent replications will take far less time, as only the modified data will be replicated.

The *Begin* and *End* times can be used to create a window of time where replication occurs. The default times allow replication to occur at any time of the day a snapshot occurs. Change these times if snapshot tasks are scheduled during office hours but the replication itself should occur after office hours. For the *End* time, consider how long replication will take so that it finishes before the next day's office hours begin.

After the replication task is saved, *PUSH* will immediately attempt to replicate its latest snapshot to *PULL*. If the replication is successful, the snapshot appears in the *Storage → Snapshots* tab of *PULL*. Also, the *Last snapshot sent to remote side* and *Status* fields of *Storage → Snapshots* on *PUSH* indicate when the last snapshot was successfully sent to that *Remote Hostname*. If the snapshot is not replicated, refer to [Troubleshooting Replication](#) for troubleshooting tips.

8.3.3 Troubleshooting Replication

If you have followed all of the steps above and *PUSH* snapshots are not replicating to *PULL*, check to see if SSH is working properly. On *PUSH*, open Shell and try to **ssh** into *PULL*. Replace **hostname_or_ip** with the value for *PULL*:

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

This command should not ask for a password. If it asks for a password, SSH authentication is not working. Go to *Storage → Replication Tasks* and click the *View Public Key* button. Make sure that it matches one of the values in *~/ssh/authorized_keys* on *PULL*, where ~ represents the home directory of the replication user.

Also check */var/log/auth.log* on *PULL* and */var/log/messages* on *PUSH* to see if either log gives an indication of the error.

If the key is correct and replication is still not working, try deleting all snapshots on *PULL* except for the most recent one. In *Storage → 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, open Shell on *PUSH* and use the **zfs send** command. To continue our example, the ZFS snapshot on the *local/data* dataset of *PUSH* is named *auto-20110922.1753-2h*, the IP address of *PULL* is *192.168.2.6*, and the ZFS volume on *PULL* is *remote*. Note that the @ is used to separate the volume/dataset name from the snapshot name:

```
zfs send local/data@auto-20110922.1753-2h | ssh -i /data/ssh/replication 192.168.2.6  
→zfs receive local/data@auto-20110922.1753-2h
```

Note: If the **zfs send** fails, open *Shell* on *PULL* and use the **zfs destroy -R volume_name@snapshot_name** command to delete the stuck snapshot. You can then use the **zfs list -t snapshot** on *PULL* to confirm if the snapshot successfully replicated.

After successfully transmitting the snapshot, check 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 the specified snapshot with this command:

```
zfs send local/data@auto-20110922.1753-2h | ssh -i /data/ssh/replication 192.168.2.6  
→zfs receive local/data@auto-20110922.1753-2h
```

8.4 Scrubs

Storage → Scrubs allows scheduling and managing scrubs on a ZFS volume. Performing a ZFS scrub on a regular basis helps to identify data integrity problems, detects silent data corruptions caused by transient hardware issues, and provides early alerts to disk failures. If you have consumer-quality drives, consider a weekly scrubbing schedule. If you have datacenter-quality drives, consider a monthly scrubbing schedule.

Depending upon the amount of data, a scrub can take a long time. Scrubs are I/O intensive and can negatively impact performance. They should be scheduled for evenings or weekends to minimize the impact to users.

A ZFS scrub only checks used disk space. To check unused disk space, schedule *S.M.A.R.T. Tests* of *Type of Long Self-Test* to run once or twice a month.

When you create a volume that is formatted with ZFS, a ZFS scrub is automatically scheduled. An entry of the same volume name is added to Storage → Scrubs and a summary of this entry can be viewed in Storage → Scrubs → View Scrubs. Figure 8.21 displays the default settings for the volume named `volume1`. In this example, the entry has been highlighted and the *Edit* button clicked to display the *Edit* screen. Table 8.9 summarizes the options in this screen.

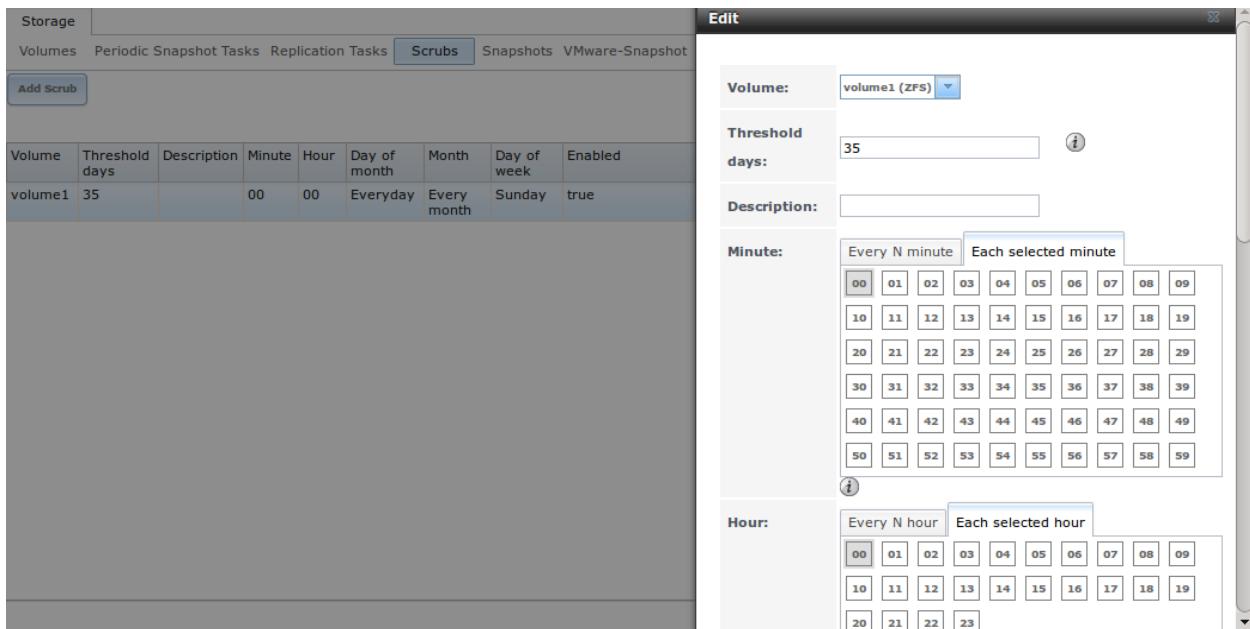


Fig. 8.21: Viewing a Volume’s Default Scrub Settings

Table 8.9: ZFS Scrub Options

Setting	Value	Description
Volume	drop-down menu	select ZFS volume to scrub
Threshold days	integer	number of days since the last scrub completed before the next scrub can occur, regardless of the calendar schedule; the default is a multiple of 7 which should ensure that the scrub always occurs on the same day of the week
Description	string	optional
Minute	slider or minute selections	if use the slider, scrub occurs every N minutes; if use minute selections, scrub starts at the highlighted minutes
Hour	slider or hour selections	if use the slider, scrub occurs every N hours; if use hour selections, scrub occurs at the highlighted hours
Day of Month	slider or month selections	if use the slider, scrub occurs every N days; if use month selections, scrub occurs on the highlighted days of the selected months
Month	checkboxes	scrub occurs on the selected months
Day of week	checkboxes	scrub occurs on the selected days; default is <i>Sunday</i> to least impact users
Enabled	checkbox	uncheck to disable the scheduled scrub without deleting it

Review the default selections and, if necessary, modify them to meet the needs of your environment.

While a **Delete** button is provided, **deleting a scrub is not recommended as a scrub provides an early indication of disk issues that could lead to a disk failure.** If you find that a scrub is too intensive for your hardware, consider unchecking the *Enabled* button for the scrub as a temporary measure until the hardware can be upgraded.

8.5 Snapshots

The *Snapshots* tab can be used to review the listing of available snapshots. An example is shown in Figure 8.22.

Note: If snapshots do not appear, check that the current time configured in *Periodic Snapshot Tasks* does not conflict with the *Begin*, *End*, and *Interval* settings. If the snapshot was attempted but failed, an entry is added to `/var/log/messages`. This log file can be viewed in [Shell](#).

The listing will include the name of the volume or dataset, the name of each snapshot, and the amount of used and referenced data, where:

Used: indicates the amount of space consumed by this dataset and all its descendants. This value is checked against this dataset's quota and reservation. The space used does not include this dataset's reservation, but does take into account the reservations of any descendent datasets. The amount of space that a dataset consumes from its parent, as well as the amount of space that are freed if this dataset is recursively destroyed, is the greater of its space used and its reservation. When a snapshot is created, its space is initially shared between the snapshot and the filesystem, and possibly with previous snapshots. As the filesystem changes, space that was previously shared becomes unique to the snapshot, and is counted in the snapshot's space used. Additionally, deleting snapshots can increase the amount of space unique to (and used by) other snapshots. The amount of space used, available, or referenced does not take into account pending changes. While pending changes are generally accounted for within a few seconds, disk changes do not necessarily guarantee that the space usage information is updated immediately.

Volume/Dataset	Snapshot Name	Used	Refer	Replication	Available Actions
volume1	auto-20150204.0959-2h	100.0 kB	684.0 kB		
volume1	auto-20150204.1004-2h	0	664.0 kB		

Fig. 8.22: Viewing Available Snapshots

Refer: indicates the amount of data that is accessible by this dataset, which may or may not be shared with other datasets in the pool. When a snapshot or clone is created, it initially references the same amount of space as the file system or snapshot it was created from, since its contents are identical.

It will also indicate if the snapshot has been replicated to a remote system.

The most recent snapshot shows icons that allow:

Clone Snapshot: prompt for the name of the clone to create. The clone will be a writable copy of the snapshot. Since a clone is really a dataset which can be mounted, the clone will appear in the *Active Volumes* tab, instead of the *Periodic Snapshots* tab, and will have the word *clone* in its name.

Destroy Snapshot: a pop-up message will ask you to confirm this action. Child clones must be destroyed before their parent snapshot can be destroyed. While creating a snapshot is instantaneous, deleting a snapshot can be I/O intensive and can take a long time, especially when deduplication is enabled. In order to delete a block in a snapshot, ZFS has to walk all the allocated blocks to see if that block is used anywhere else; if it is not, it can be freed.

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 in the Active Volumes tab.

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

Periodic snapshots can be configured to appear as shadow copies in newer versions of Windows Explorer, as described in [Configuring Shadow Copies](#). Users can access the files in the shadow copy using Explorer without requiring any interaction with the FreeNAS® graphical administrative interface.

The ZFS Snapshots screen allows the creation of filters to view snapshots by selected criteria. To create a filter, click the *Define filter* icon (near the text *No filter applied*). When creating a filter:

- select the column or leave the default of *Any Column*.
- select the condition. Possible conditions are: *contains* (default), *is*, *starts with*, *ends with*, *does not contain*, *is not*, *does not start with*, *does not end with*, and *is empty*.
- enter a value that meets your view criteria.
- click the *Filter* button to save your filter and exit the define filter screen. Alternately, click the + button to add another filter.

If you create multiple filters, select the filter to use before leaving the define filter screen. Once a filter is selected, the *No filter applied* text changes to *Clear filter*. If you click *Clear filter*, a pop-up message indicates that this removes the filter and all available snapshots are listed.

8.6 VMware-Snapshot

Storage → VMware-Snapshot allows you to coordinate ZFS snapshots when using FreeNAS® as a VMware datastore. Once this type of snapshot is created, FreeNAS® will automatically snapshot any running VMware virtual machines before taking a scheduled or manual ZFS snapshot of the dataset or zvol backing that VMware datastore. The temporary VMware snapshots are then deleted on the VMware side but still exist in the ZFS snapshot and can be used as stable resurrection points in that snapshot. These coordinated snapshots will be listed in *Snapshots*.

Figure 8.23 shows the menu for adding a VMware snapshot and Table 8.10 summarizes the available options.

The screenshot shows a dialog box titled "Add VMware-Snapshot". It contains the following fields:

- Hostname:** An input field with a placeholder " ".
- Username:** An input field with a placeholder " ".
- Password:** An input field with a placeholder " ".
- ZFS Filesystem:** A dropdown menu set to "volume1".
- Datastore:** An input field with a dropdown arrow and a help icon (i).

At the bottom are three buttons: "OK", "Cancel", and "Fetch Datastores".

Fig. 8.23: Adding a VMware Snapshot

Table 8.10: VMware Snapshot Options

Setting	Value	Description
Host-name	string	IP address or hostname of VMware host; when clustering, this is the vCenter server for the cluster
User-name	string	user on VMware host with enough permission to snapshot virtual machines
Pass-word	string	password associated with <i>Username</i>
ZFS Filesystem	drop-down menu	the filesystem to snapshot
Datastore	drop-down menu	after entering the <i>Hostname</i> , <i>Username</i> , and <i>Password</i> , click <i>Fetch Datastores</i> to populate the menu and select the datastore with which to synchronize

DIRECTORY SERVICE

FreeNAS® supports integration with these directory services:

- *Active Directory* (for Windows 2000 and higher networks)
- *LDAP*
- *NIS*
- *NT4* (for Windows networks older than Windows 2000)

It also supports *Kerberos Realms*, *Kerberos Keytabs*, and the ability to add additional parameters to *Kerberos Settings*.

This section summarizes each of these services and their available configurations within the FreeNAS® GUI.

9.1 Active Directory

Active Directory (AD) is a service for sharing resources in a Windows network. AD can be configured on a Windows server that is running Windows Server 2000 or higher or on a Unix-like operating system that is running [Samba version 4](#). Since AD provides authentication and authorization services for the users in a network, it is not necessary to recreate these user accounts on the FreeNAS® system. Instead, configure the Active Directory service so that it can import the account information and imported users can be authorized to access the SMB shares on the FreeNAS® system.

Note: If the network contains an NT4 domain controller, or any domain controller containing a version which is earlier than Windows 2000, configure *NT4* instead.

Many changes and improvements have been made to Active Directory support within FreeNAS®. It is strongly recommended to update the system to the latest FreeNAS® 9.10.1-U2 before attempting Active Directory integration.

Before configuring the Active Directory service, ensure name resolution is properly configured by **ping**ing the domain name of the Active Directory domain controller from *Shell* on the FreeNAS® system. If the **ping** fails, check the DNS server and default gateway settings in *Network* → *Global Configuration* on the FreeNAS® system.

Next, add a DNS record for the FreeNAS® system on the Windows server and verify that the hostname of the FreeNAS® system can be pinged from the domain controller.

Active Directory relies on Kerberos, which is a time sensitive protocol. The time on both the FreeNAS® system and the Active Directory Domain Controller cannot 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* → *NTP Servers* on the FreeNAS® system)
- have the same timezone

- be set to either localtime or universal time at the BIOS level

Figure 9.1 shows the screen that appears when Directory Service → Active Directory is chosen. Table 9.1 describes the configurable options. Some settings are only available in Advanced Mode. To see these settings, either click the *Advanced Mode* button or configure the system to always display these settings by checking the box *Show advanced fields by default* in System → Advanced.

The screenshot shows the 'Directory Service' configuration page. At the top, there are tabs for 'Active Directory', 'LDAP', 'NIS', 'NT4', 'Kerberos Realms', and 'Kerberos Keytabs'. The 'Active Directory' tab is selected. Below the tabs, there are four input fields: 'Domain Name (DNS/Realm-Name)' with a placeholder 'domain.com' and an info icon; 'Domain Account Name' with a placeholder 'Administrator' and an info icon; 'Domain Account Password' with a placeholder 'password' and an info icon; and 'Enable' with a checked checkbox and an info icon. At the bottom, there are three buttons: 'Save', 'Advanced Mode' (which is currently selected), and 'Rebuild Directory Service Cache'.

Fig. 9.1: Configuring Active Directory

Table 9.1: Active Directory Configuration Options

Setting	Value	Description
Domain Name	string	name of Active Directory domain (e.g. <i>example.com</i>) or child domain (e.g. <i>sales.example.com</i>); this setting is mandatory and the GUI will refuse to save the settings if the domain controller for the specified domain cannot be found
Domain Account Name	string	name of the Active Directory administrator account; this setting is mandatory and the GUI will refuse to save the settings if it cannot connect to the domain controller using this account name
Domain Account Password	string	password for the Active Directory administrator account; this setting is mandatory and the GUI will refuse to save the settings if it can not connect to the domain controller using this password
NetBIOS Name	string	only available in <i>Advanced Mode</i> ; limited to 15 characters; automatically populated with the original hostname of the system; use caution when changing this setting , as setting an incorrect value can corrupt an AD installation
Encryption Mode	drop-down menu	only available in <i>Advanced Mode</i> ; choices are <i>Off</i> , <i>SSL</i> , or <i>TLS</i>
Certificate	drop-down menu	only available in <i>Advanced Mode</i> ; select the certificate of the LDAP server if SSL connections are used; if a certificate does not exist yet, create a CA (in <i>CAs</i>), then create a certificate on the Active Directory server and import it to the FreeNAS® system with <i>Certificates</i>
Verbose logging	checkbox	only available in <i>Advanced Mode</i> ; if checked, logs attempts to join the domain to <i>/var/log/messages</i>
UNIX extensions	checkbox	only available in <i>Advanced Mode</i> ; only check this box if the AD server has been explicitly configured to map permissions for UNIX users; checking this box provides persistent UIDs and GUIDs, otherwise, users/groups get mapped to the UID/GUID range configured in Samba
Allow Trusted Domains	checkbox	only available in <i>Advanced Mode</i> ; should only be enabled if network has active <i>domain/forest trusts</i> and you need to manage files on multiple domains; use with caution as it will generate more winbindd traffic, slowing down the ability to filter through user/group information
Use Default Domain	checkbox	only available in <i>Advanced Mode</i> ; when unchecked, the domain name is prepended to the username; if <i>Allow Trusted Domains</i> is checked and multiple domains use the same usernames, uncheck this box to prevent name collisions
Allow DNS updates	checkbox	when unchecked, disables Samba from doing DNS updates when joining a domain
Disable Active Directory user/group cache	checkbox	when checked, disables caching AD users and groups; useful if you cannot bind to a domain with a large number of users or groups
Site Name	string	only available in <i>Advanced Mode</i> ; the relative distinguished name of the site object in Active Directory
Domain Controller	string	only available in <i>Advanced Mode</i> ; will automatically be added to the SRV record for the domain and, when multiple controllers are specified, FreeNAS® selects the closest DC which responds
Global Catalog Server	string	only available in <i>Advanced Mode</i> ; if the hostname of the global catalog server to use is specified, make sure it is resolvable
Kerberos Realm	drop-down menu	only available in <i>Advanced Mode</i> ; select the realm created using the instructions in <i>Kerberos Realms</i>
Kerberos Principal	drop-down menu	only available in <i>Advanced Mode</i> ; browse to the location of the keytab created using the instructions in <i>Kerberos Keytabs</i>
AD timeout	integer	only available in <i>Advanced Mode</i> ; in seconds, increase if the AD service does not start after connecting to the domain
DNS timeout 9.1. Active Directory	integer	only available in <i>Advanced Mode</i> ; in seconds, increase if AD DNS queries timeout
Idmap backend	drop-down menu and Edit	only available in <i>Advanced Mode</i> ; select the backend to use to map Windows security identifiers (SIDs) to UNIX UIDs and GIDs; see Table 9.2 for a summary of the available backends; click the <i>Edit</i> link to configure that

Table 9.2 summarizes the backends which are available in the *Idmap backend* drop-down menu. Each backend has its own [man page](#) which gives implementation details. Since selecting the wrong backend will break Active Directory integration, a pop-up menu will appear whenever changes are made to this setting.

Table 9.2: ID Mapping Backends

Value	Description
ad	AD server uses RFC2307 or Services For Unix schema extensions; mappings must be provided in advance by adding the uidNumber attributes for users and gidNumber attributes for groups in the AD
adex	AD server uses RFC2307 schema extensions and supports domain trusts as well as two-way cross-forest trusts; mappings must be provided in advance by adding the POSIX attribute information to the users and groups objects in AD using a tool such as “Identity Services for Unix” on Windows 2003 R2 and later
au-torid	similar to <i>rid</i> , but automatically configures the range to be used for each domain, so there is no need to specify a specific range for each domain in the forest; the only needed configuration is the range of UID/GIDs to use for user/group mappings and an optional size for the ranges
hash	uses a hashing algorithm for mapping and can be used to support local name mapping files
ldap	stores and retrieves mapping tables in an LDAP directory service; default for LDAP directory service
nss	provides a simple means of ensuring that the SID for a Unix user is reported as the one assigned to the corresponding domain user
rfc2307	an AD server is required to provide the mapping between the name and SID and an LDAP server is required to provide the mapping between the name and the UID/GID
rid	default for AD and NT4 directory services; requires an explicit idmap configuration for each domain, using disjoint ranges where a writeable default idmap range should be defined, using a backend like tdb or ldap
tdb	default backend used by winbindd for storing mapping tables
tdb2	substitute for tdb used by winbindd in clustered environments

Click the *Rebuild Directory Service Cache* button if a new Active Directory user needs immediate access to FreeNAS®; otherwise this occurs automatically once a day as a cron job.

Note: Active Directory places restrictions on which characters are allowed in Domain and NetBIOS names, a limits the length of those names to 15 characters. If there are problems connecting to the realm, [verify](#) that your settings do not include any disallowed characters. Also, the Administrator account password cannot contain the \$ character. If a \$ exists in the domain administrator’s password, **kinit** will report a “Password Incorrect” error and **ldap_bind** will report an “Invalid credentials (49)” error.

It can take a few minutes after configuring the Active Directory service for the AD 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. For performance reasons, every available user may not show in the listing. However, it will autocomplete all applicable users when typing in a username.

The Active Directory users and groups that have been imported to the FreeNAS® system can be shown by using these commands from the FreeNAS® *Shell*. To view users:

```
wbinfo -u
```

To view groups:

```
wbinfo -g
```

In addition, **wbinfo -t** will test the connection and, if successful, will show a message similar to:

```
checking the trust secret for domain YOURDOMAIN via RPC calls succeeded
```

To manually check that a specified user can authenticate:

```
net ads join -S dcname -U username
```

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

```
getent passwd
```

```
getent group
```

If the **wbinfo** commands display the network users, but they do not show up in the drop-down menu of a *Permissions* screen, it may be because it is taking longer than the default ten seconds for the FreeNAS® system to join Active Directory. Try bumping up the value of *AD timeout* to 60 seconds.

9.1.1 Troubleshooting Tips

When running AD in a 2003/2008 mixed domain, [refer to](#) for instructions on how to prevent the secure channel key from becoming corrupt.

Active Directory 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](#).

The realm that is used depends upon the priority in the SRV DNS record, meaning that DNS can override your Active Directory settings. When unable to connect to the correct realm, check the SRV records on the DNS server. [This article](#) describes how to configure KDC discovery over DNS and provides some examples of records with differing priorities.

If the cache becomes out of sync due to an AD server being taken off and back online, resync the cache using `Directory Service → Active Directory → Rebuild Directory Service Cache`.

An expired password for the administrator account will cause kinit to fail, so ensure that the password is still valid. Also, double-check that the password on the AD account being used does not include any spaces or special symbols, and is not unusually long.

If the Windows server version is lower than 2008 R2, try creating a *Computer* entry on the Windows server's OU. When creating this entry, enter the FreeNAS® hostname in the *name* field. Make sure that it is under 15 characters and that it is the same name as the one set in the *Hostname* field in `Network → Global Configuration` and the *NetBIOS Name* in `Directory Service → Active Directory` settings. Make sure the hostname of the domain controller is set in the *Domain Controller* field of `Directory Service → Active Directory`.

9.1.2 If the System Will not Join the Domain

If the system will not join the Active Directory domain, run these commands in the order listed. If any of the commands fail or result in a traceback, create a bug report at [bugs.freenas.org](#) that includes the commands in the order in which they were run and the exact wording of the error message or traceback.

Start with these commands, where the **echo** commands should return a value of *0* and the **klist** command should show a Kerberos ticket:

```
sqlite3 /data/freenas-v1.db "update directoryservice_activedirectory set ad_enable=1;"  
echo $?  
service ix-kerberos start  
service ix-nsswitch start  
service ix-kinit start
```

```
service ix-kinit status
echo $?
klist
```

Next, only run these two commands **if** the *Unix extensions* box is checked in *Advanced Mode* and a keytab has been uploaded using *Kerberos Keytabs*:

```
service ix-sssd start
service sssd start
```

Finally, run these commands. Again, the **echo** command should return a *0*:

```
python /usr/local/www/freenasUI/middleware/notifier.py start cifs
service ix-activedirectory start
service ix-activedirectory status
echo $?
python /usr/local/www/freenasUI/middleware/notifier.py restart cifs
service ix-pam start
service ix-cache start &
```

9.2 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, configure the FreeNAS® LDAP service so network users can authenticate to the LDAP server and have authorized access to the data stored on the FreeNAS® system.

Note: LDAP authentication for SMB shares will be disabled unless the LDAP directory has been configured for and populated with Samba attributes. The most popular script for performing this task is `smbldap-tools` and instructions for using it can be found at [The Linux Samba-OpenLDAP Howto](#). In addition, the LDAP server must support SSL/TLS and the certificate for the LDAP server must be imported with `System → Certificates → Import Certificate`.

Figure 9.2 shows the LDAP Configuration screen that is seen after clicking `Directory Service → LDAP`.

Table 9.3 summarizes the available configuration options. Some settings are only available in Advanced Mode. To see these settings, either click the *Advanced Mode* button or configure the system to always display these settings by checking the box *Show advanced fields by default* in `System → Advanced`.

Those who are new to LDAP terminology should skim through the [OpenLDAP Software 2.4 Administrator's Guide](#).

The screenshot shows the 'Directory Service' configuration page. The 'LDAP' tab is active. The form contains the following fields:

- Hostname:** [Text input field]
- Base DN:** [Text input field]
- Bind DN:** [Text input field]
- Bind password:** [Text input field]
- Enable:** [checkbox]

Below the form are three buttons: **Save**, **Advanced Mode** (which is highlighted), and **Rebuild Directory Service Cache**.

Fig. 9.2: Configuring LDAP

Table 9.3: LDAP Configuration Options

Setting	Value	Description
Hostname	string	hostname or IP address of LDAP server
Base DN	string	top level of the LDAP directory tree to be used when searching for resources (e.g. <i>dc=test,dc=org</i>)
Bind DN	string	name of administrative account on LDAP server (e.g. <i>cn=Manager,dc=test,dc=org</i>)
Bind password	string	password for <i>Root bind DN</i>
Allow Anonymous Binding	checkbox	only available in <i>Advanced Mode</i> ; instructs LDAP server to not provide authentication and to allow read and write access to any client
User Suffix	string	only available in <i>Advanced Mode</i> and optional; can be added to name when user account added to LDAP directory (e.g. dept. or company name)
Group Suffix	string	only available in <i>Advanced Mode</i> and optional; can be added to name when group added to LDAP directory (e.g. dept. or company name)
Password Suffix	string	only available in <i>Advanced Mode</i> and optional; can be added to password when password added to LDAP directory
Machine Suffix	string	only available in <i>Advanced Mode</i> and optional; can be added to name when system added to LDAP directory (e.g. server, accounting)
SUDO Suffix	string	only available in <i>Advanced Mode</i> ; use if LDAP-based users need superuser access
Kerberos Realm	drop-down menu	only available in <i>Advanced Mode</i> ; select the realm created using the instructions in <i>Kerberos Realms</i>
Kerberos Keytab	drop-down menu	only available in <i>Advanced Mode</i> ; browse to the location of the keytab created using the instructions in <i>Kerberos Keytabs</i>
Encryption Mode	drop-down menu	only available in <i>Advanced Mode</i> ; choices are <i>Off</i> , <i>SSL</i> , or <i>TLS</i> ; note that either <i>SSL</i> or <i>TLS</i> and a <i>Certificate</i> must be selected in order for authentication to work
Certificate	drop-down menu	only available in <i>Advanced Mode</i> ; select the certificate of the LDAP server or the CA that signed that certificate (required if authentication is used); if your LDAP server does not already have a certificate, create a CA using <i>CAs</i> , then the certificate using <i>Certificates</i> and install the certificate on the LDAP server
LDAP timeout	integer	increase this value (in seconds) if obtaining a Kerberos ticket times out
DNS timeout	integer	increase this value (in seconds) if DNS queries timeout
Idmap backend	drop-down menu and Edit	only available in <i>Advanced Mode</i> ; select the backend to use to map Windows security identifiers (SIDs) to UNIX UIDs and GIDs; see Table 9.2 for a summary of the available backends; click the <i>Edit</i> link to configure that backend's editable options
Samba	checkbox	only available in <i>Advanced Mode</i> ; only check this box if you need LDAP

Click the *Rebuild Directory Service Cache* button after adding a user to LDAP who needs immediate access to FreeNAS®. Otherwise this occurs automatically once a day as a cron job.

Note: FreeNAS® automatically appends the root DN. This means that the scope and root DN should not be included when configuring the user, group, password, and machine suffixes.

LDAP users and groups appear in the drop-down menus of the *Permissions* screen of a volume/dataset after configuring the LDAP service. Type **getent passwd** from *Shell* to verify that the users have been imported. Type **getent group** to verify that the groups have been imported.

If the users and groups are not listed, refer to [Common errors encountered when using OpenLDAP Software](#) for common errors and how to fix them. When troubleshooting LDAP, open *Shell* and look for error messages in */var/log/auth.log*.

9.3 NIS

Network Information Service (NIS) is a service which maintains and distributes a central directory of Unix user and group information, hostnames, email aliases, and other text-based tables of information. If a NIS server is running on your network, the FreeNAS® system can be configured to import the users and groups from the NIS directory.

Figure 9.3 shows the configuration screen which opens when you click *Directory Service* → *NIS*. Table 9.4 summarizes the configuration options.

NIS domain:	<input type="text"/>	<i>i</i>
NIS servers:	<input type="text"/>	<i>i</i>
Secure mode:	<input checked="" type="checkbox"/>	<i>i</i>
Multicast:	<input checked="" type="checkbox"/>	<i>i</i>
Enable:	<input type="checkbox"/>	
Save Rebuild Directory Service Cache		

Fig. 9.3: NIS Configuration

Table 9.4: NIS Configuration Options

Setting	Value	Description
NIS domain	string	name of NIS domain
NIS servers	string	comma delimited list of hostnames or IP addresses
Secure mode	checkbox	if checked, <code>ypbind(8)</code> will refuse to bind to any NIS server that is not running as root on a TCP port number over 1024
Many-cast	checkbox	if checked, <code>ypbind</code> will bind to the server that responds the fastest; this is useful when no local NIS server is available on the same subnet
Enable	checkbox	uncheck to disable the configuration without deleting it

Click the *Rebuild Directory Service Cache* button after adding a user to NIS who needs immediate access to FreeNAS®. Otherwise this occurs automatically once a day as a cron job.

9.4 NT4

This service should only be configured if the Windows network's domain controller is running NT4. If the network's domain controller is running a more recent version of Windows, you should configure [Active Directory](#) instead.

Figure 9.4 shows the configuration screen that appears when *Directory Service → NT4* is clicked. These options are summarized in Table 9.5. Some settings are only available in Advanced Mode. To see these settings, either click the *Advanced Mode* button or configure the system to always display these settings by checking the box *Show advanced fields by default* in *System → Advanced*.

The screenshot shows the FreeNAS Directory Service configuration interface. The top navigation bar has tabs for Active Directory, LDAP, NIS, NT4 (which is selected and highlighted in blue), Kerberos Realms, and Kerberos Keytabs. Below the tabs is a form with the following fields:

- Domain Controller:** (Input field)
- NetBIOS Name:** (Input field, value: FREENAS)
- Workgroup Name:** (Input field)
- Administrator Name:** (Input field)
- Administrator Password:** (Input field)
- Confirm Administrator Password:** (Input field)
- Enable:** (checkbox)

At the bottom of the form are three buttons: **Save**, **Advanced Mode** (which is also highlighted in blue), and **Rebuild Directory Service Cache**.

Fig. 9.4: NT4 Configuration Options

Table 9.5: NT4 Configuration Options

Setting	Value	Description
Domain Controller	string	hostname of domain controller
NetBIOS Name	string	hostname of FreeNAS system ; cannot be longer than 15 characters; cannot be the same as the <i>Workgroup Name</i>
Workgroup Name	string	name of Windows server's workgroup
Administrator Name	string	name of the domain administrator account
Administrator Password	string	input and confirm the password for the domain administrator account
Use default domain	checkbox	only available in <i>Advanced Mode</i> ; when unchecked, the domain name is prepended to the username
Idmap backend	drop-down and Edit menu	only available in <i>Advanced Mode</i> ; select the backend to use to map Windows security identifiers (SIDs) to UNIX UIDs and GIDs; see Table 9.2 for a summary of the available backends; click the <i>Edit</i> link to configure that backend's editable options
Enable	checkbox	uncheck to disable the configuration without deleting it

Click the *Rebuild Directory Service Cache* button after adding a user to Active Directory who needs immediate access to FreeNAS®. Otherwise this occurs automatically once a day as a cron job.

9.5 Kerberos Realms

A default Kerberos realm is created for the local system in FreeNAS®. [Directory Service → Kerberos Realms](#) can be used to view and add Kerberos realms. If the network contains a KDC, click the *Add kerberose realm* button to add the Kerberos realm. This configuration screen is shown in [Figure 9.5](#).

[Table 9.6](#) summarizes the configurable options. Some settings are only available in Advanced Mode. To see these settings, either click the *Advanced Mode* button or configure the system to always display these settings by checking the box *Show advanced fields by default* in [System → Advanced](#).

Table 9.6: Kerberos Realm Options

Setting	Value	Description
Realm	string	mandatory; name of the realm
KDC	string	only available in <i>Advanced Mode</i> ; name of the Key Distribution Center
Admin Server	string	only available in <i>Advanced Mode</i> ; server where all changes to the database are performed
Password Server	string	only available in <i>Advanced Mode</i> ; server where all password changes are performed

9.6 Kerberos Keytabs

Kerberos keytabs are used to do Active Directory or LDAP joins without a password. This means that the password for the Active Directory or LDAP administrator account does not need to be saved into the FreeNAS® configuration database, which is a security risk in some environments.

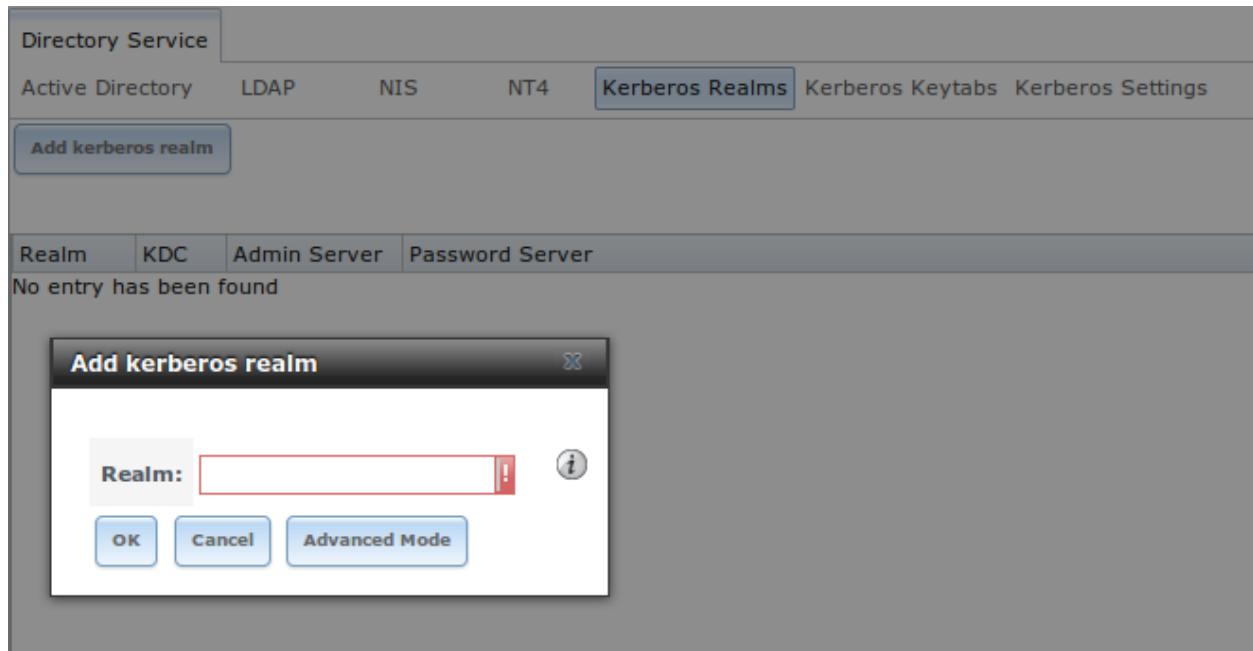


Fig. 9.5: Adding a Kerberos Realm

When using a keytab, it is recommended to create and use a less privileged account for performing the required queries as the password for that account will be stored in the FreeNAS® configuration database. To create the keytab on a Windows system, use these commands:

```
ktpass.exe -out hostname.keytab host/ hostname@DOMAINNAME -ptype KRB5_NT_PRINCIPAL -  
-mapuser DOMAIN\username -pass userpass  
  
setspn -A host/ hostname@DOMAINNAME DOMAIN\username
```

where:

- **hostname** is the fully qualified hostname of the domain controller
- **DOMAINNAME** is the domain name in all caps
- **DOMAIN** is the pre-Windows 2000 short name for the domain
- **username** is the privileged account name
- **userpass** is the password associated with username

This will create a keytab with sufficient privileges to grant tickets.

Once the keytab is generated, use Directory Service → Kerberos Keytabs → Add kerberos keytab to add it to the FreeNAS® system.

To instruct the Active Directory service to use the keytab, select the installed keytab using the drop-down *Kerberos keytab* menu in Directory Service → Active Directory . When using a keytab with Active Directory, make sure that the “username” and “userpass” in the keytab matches the “Domain Account Name” and “Domain Account Password” fields in Directory Service → Active Directory .

To instruct LDAP to use the keytab, select the installed keytab using the drop-down “Kerberos keytab” menu in Directory Service → LDAP .

9.7 Kerberos Settings

To configure additional Kerberos parameters, use Directory Service → Kerberos Settings . Figure 9.6 shows the fields available:

- **Appdefaults auxiliary parameters:** contains settings used by some Kerberos applications. The available settings and their syntax are listed in the [appdefaults] section of `krb.conf(5)`.
- **Libdefaults auxiliary parameters:** contains settings used by the Kerberos library. The available settings and their syntax are listed in the [libdefaults] section of `krb.conf(5)`.

The screenshot shows the 'Kerberos Settings' tab selected under the 'Directory Service' menu. The interface includes tabs for Active Directory, LDAP, NIS, NT4, Kerberos Realms, Kerberos Keytabs, and Kerberos Settings. Below the tabs are two main configuration sections: 'Appdefaults auxiliary parameters:' and 'Libdefaults auxiliary parameters:', each with a large text input area. At the bottom left is a 'Save' button.

Fig. 9.6: Additional Kerberos Settings

SHARING

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, your security requirements, and expectations for network transfer speeds.

FreeNAS® provides an *Initial Configuration Wizard* for creating shares. The Wizard will automatically create the correct type of dataset and permissions for the type of share, set the default permissions for the share type, and start the service needed by the share. It is recommended to use the Wizard to create shares, fine-tune the share settings using the instructions in the rest of this chapter if needed, then to fine-tune the default permissions from the client operating system to meet the requirements of the network.

Note: Shares are created to provide and control access to an area of storage. Before creating your shares, it is recommended to make a list of the users that will need access to storage data, which operating systems these users are using, whether or not all users should have the same permissions to the stored data, and whether or not these users should authenticate before accessing the data. This information can help you determine which type of share(s) you need to create, whether or not you need to create multiple datasets in order to divide up the storage into areas with differing access and permission requirements, and how complex it will be to setup your permission requirements. It should be noted that a share is used to provide access to data. If you delete a share, it removes access to data but does not delete the data itself.

These types of shares and services are available:

- *Apple (AFP) Shares*: the Apple File Protocol (AFP) type of share is a good choice if all of your computers run Mac OS X.
- *Unix (NFS) Shares*: the Network File System (NFS) type of share is accessible by Mac OS X, Linux, BSD, and the professional and 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.
- *WebDAV Shares*: this type of share is accessible using an authenticated web browser (read-only) or *WebDAV client* running on any operating system.
- *Windows (SMB) Shares*: the Server Message Block type of share, also known as Common Internet File System (SMB), 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. It provides more configuration options than NFS and is a good choice on a network containing any Windows systems. However, it is a poor choice if the CPU on the FreeNAS® system is limited; if the CPU is maxed out, upgrade the CPU or consider another type of share.
- *Block (iSCSI) shares*: this type of share appears as an unformatted disk to clients running iSCSI initiator software or a virtualization solution such as VMware.

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*. Secure

FTP can be configured if the data needs to be encrypted.

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 or dataset 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 SMB, 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. 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. If you need to support multiple types of shares, divide the volume into datasets and use one dataset per share.

This section will demonstrate how to fine-tune the configuration of AFP, NFS, SMB, WebDAV, and iSCSI shares. FTP and SSH configurations are described in [Services Configuration](#).

10.1 Apple (AFP) Shares

FreeNAS® uses the [Netatalk](#) AFP server to share data with Apple systems. This section describes the configuration screen for fine-tuning AFP shares created using the [Initial Configuration Wizard](#). It then provides configuration examples for using the Wizard to create a guest share, configuring Time Machine to backup to a dataset on the FreeNAS® system, and for connecting to the share from a Mac OS X client.

To view the AFP share created by the Wizard, click [Sharing](#) → [Apple \(AFP\)](#) and highlight the name of the share. Click its *Edit* button to see the configuration options shown in [Figure 10.1](#). The values showing for these options will vary, depending upon the information given when the share was created.

Note: While [Table 10.1](#) summarizes the available options for fine-tuning an AFP share, you typically should not change the default settings of an AFP share as doing so may cause the share to not work as expected. Most settings are only available when you click *Advanced Mode*. Do **not** change an advanced option without fully understanding the function of that option. Refer to [Setting up Netatalk](#) for a more detailed explanation of the available options.

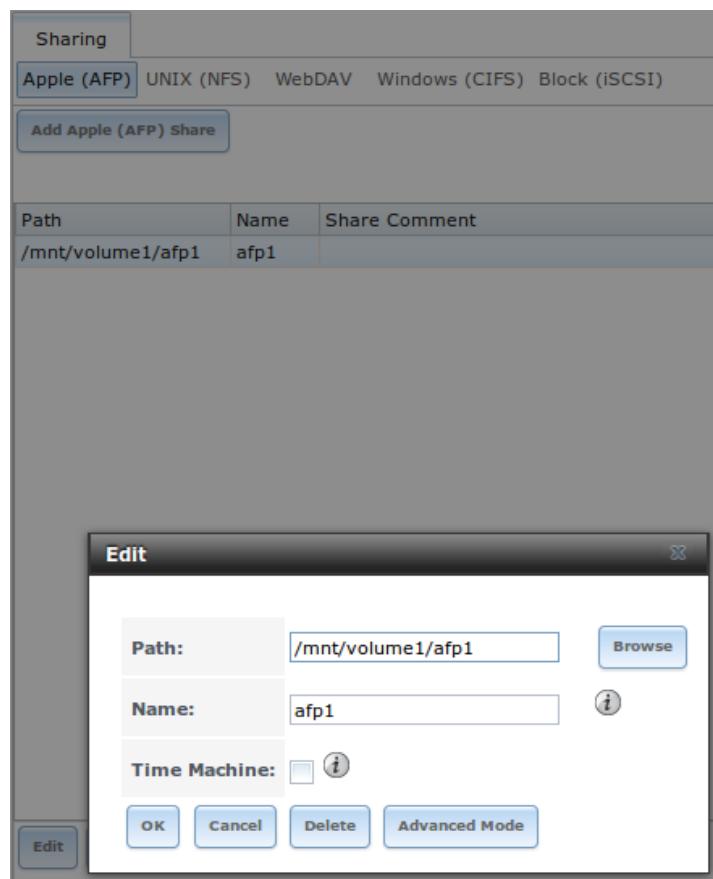


Fig. 10.1: Creating an AFP Share

Table 10.1: AFP Share Configuration Options

Setting	Value	Description
Path	browse button	browse to the volume/dataset to share; do not nest additional volumes, datasets, or symbolic links beneath this path because Netatalk lacks complete support
Name	string	volume name that will appear in the Mac computer's <i>connect to server</i> dialog; limited to 27 characters and cannot contain a period
Share Comment	string	only available in <i>Advanced Mode</i> ; optional
Allow List	string	only available in <i>Advanced Mode</i> ; comma delimited list of allowed users and/or groups where groupname begins with a @; note that adding an entry will deny any user/group that is not specified
Deny List	string	only available in <i>Advanced Mode</i> ; comma delimited list of denied users and/or groups where groupname begins with a @; note that adding an entry will allow all users/groups that are not specified
Read-only Access	string	only available in <i>Advanced Mode</i> ; comma delimited list of users and/or groups who only have read access where groupname begins with a @
Read-write Access	string	only available in <i>Advanced Mode</i> ; comma delimited list of users and/or groups who have read and write access where groupname begins with a @
Time Machine	check-box	when checked, FreeNAS® advertises itself as a Time Machine disk so it can be found by Macs; due to a limitation in how the Mac deals with low-diskspace issues when multiple Macs share the same volume, checking <i>Time Machine</i> on multiple shares could result in intermittent failed backups
Zero Device Numbers	check-box	only available in <i>Advanced Mode</i> ; enable when the device number is not constant across a reboot
No Stat	check-box	only available in <i>Advanced Mode</i> ; if checked, AFP won't stat the volume path when enumerating the volumes list; useful for automounting or volumes created by a pexec script
AFP3 UNIX Privs	check-box	only available in <i>Advanced Mode</i> ; enables Unix privileges supported by OSX 10.5 and higher; do not enable if the network contains Mac OS X 10.4 clients or lower as they do not support these
Default file permission	check-boxes	only available in <i>Advanced Mode</i> ; only works with Unix ACLs; new files created on the share are set with the selected permissions
Default directory permission	check-boxes	only available in <i>Advanced Mode</i> ; only works with Unix ACLs; new directories created on the share are set with the selected permissions
Default umask	integer	only available in <i>Advanced Mode</i> ; umask for newly created files, default is 000 (anyone can read, write, and execute)
Hosts Allow	string	only available in <i>Advanced Mode</i> ; comma, space, or tab-delimited list of allowed hostnames or IP addresses
Hosts Deny	string	only available in <i>Advanced Mode</i> ; comma, space, or tab-delimited list of denied hostnames or IP addresses

10.1.1 Creating AFP Guest Shares

AFP supports guest logins, meaning that all of your Mac OS X users can access the AFP share without requiring their user accounts to first be created on or imported into the FreeNAS® system.

Note: If you create a guest share as well a share that requires authentication, AFP will only map users who login as guest to the guest share. This means that if a user logs in to the share that requires authentication, the permissions on the guest share may prevent that user from writing to the guest share. The only way to allow both guest and authenticated

users to write to a guest share is to set the permissions on the guest share to 777 or to add the authenticated users to a guest group and set the permissions to 77x.

Before creating a guest share, go to *Services* → *AFP* and make sure that the *Guest Access* box is checked.

To create the AFP guest share, click *Wizard*, then click the *Next* button twice to display the screen shown in Figure 10.2. Complete these fields in this screen:

1. **Share name:** enter a name for the share that is useful to you but which is under 27 characters and does not contain a period. In this example, the share is named *afp_guest*.
2. Click the button for *Mac OS X (AFP)*.
3. Click the *Ownership* button. Click the drop-down *User* menu and select *nobody*. Click the *Return* button to return to the previous screen.
4. Click the *Add* button. **If you forget to do this, the share will not be created.** Clicking the *Add* button adds an entry to the *Name* frame with the name that was entered in *Share name*.

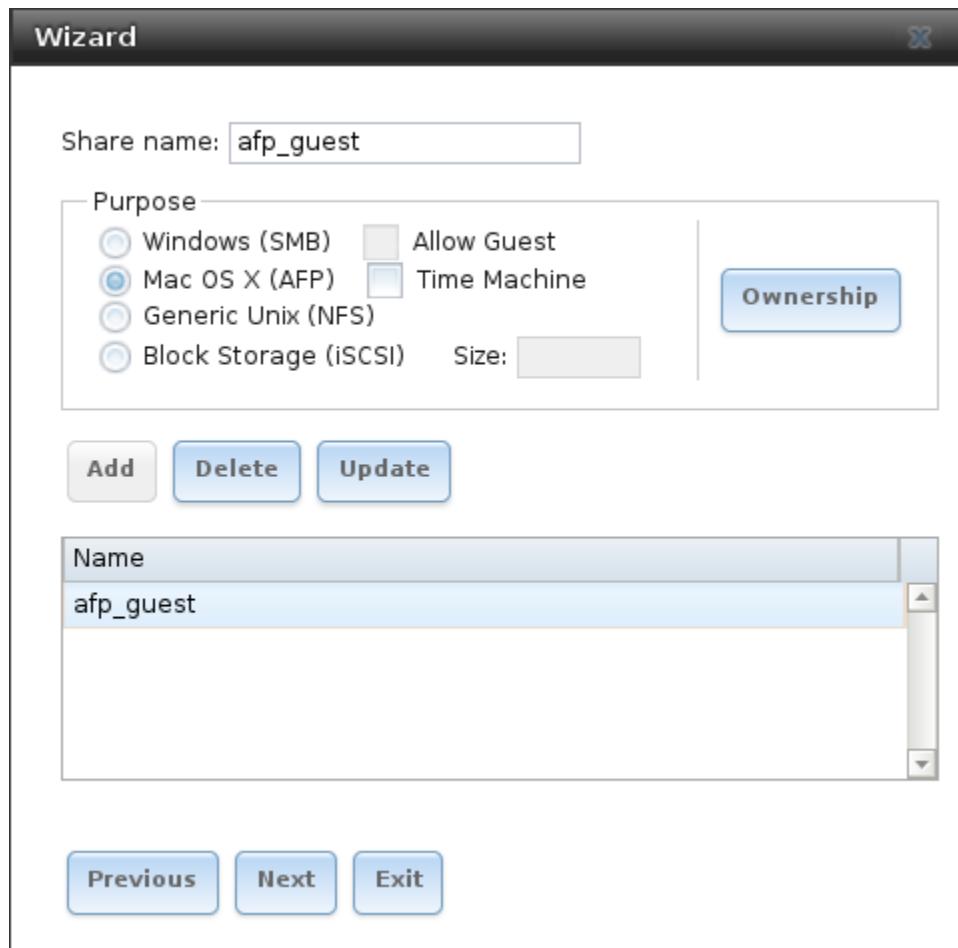


Fig. 10.2: Creating a Guest AFP Share

Click the *Next* button twice, then the *Confirm* button to create the share. The Wizard automatically creates a dataset for the share that contains the correct default permissions and starts the AFP service so the share is immediately available. The new share is also added as an entry to *Sharing* → *Apple (AFP)*.

Mac OS X users can connect to the guest AFP share by clicking *Go* → *Connect to Server*. In the example shown in [Figure 10.3](#), the user has entered *afp://* followed by the IP address of the FreeNAS® system.

Click the *Connect* button. Once connected, Finder opens automatically. The name of the AFP share is displayed in the SHARED section in the left frame and the contents of any data saved in the share is displayed in the right frame.

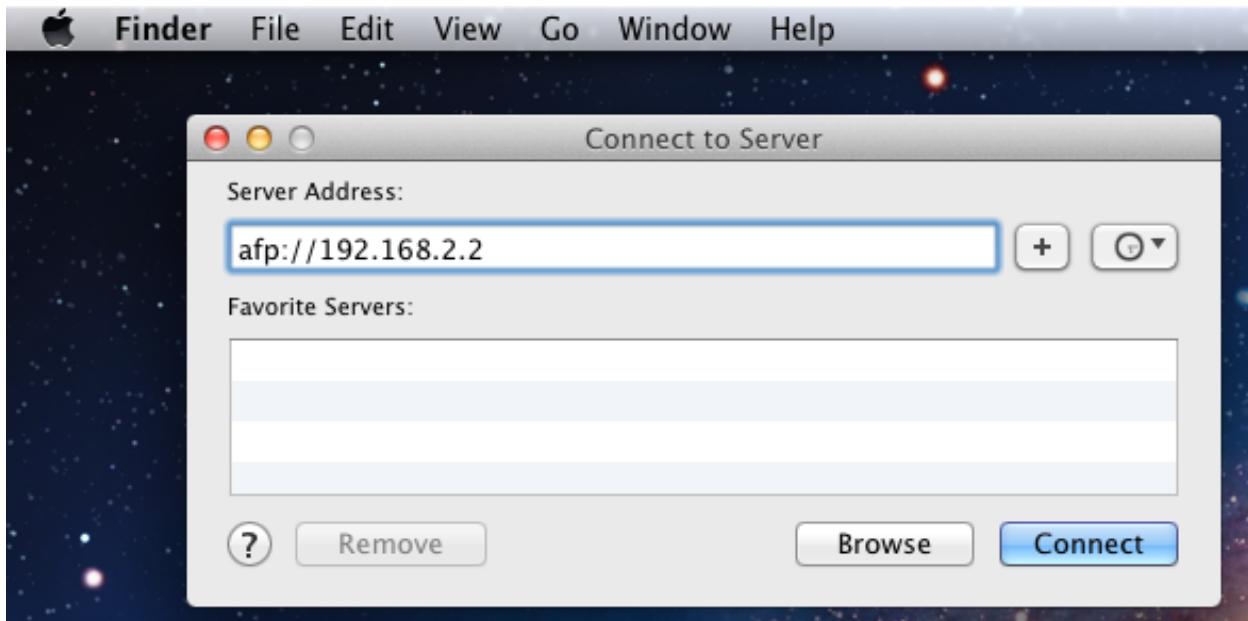


Fig. 10.3: Connect to Server Dialogue

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

10.1.2 Creating Authenticated and Time Machine Shares

Mac OS X includes the Time Machine application which can be used to schedule automatic backups. In this configuration example, a Time Machine user will be configured to backup to an AFP share on a FreeNAS® system. It is recommended to create a separate Time Machine share for each user that will be using Time Machine to backup their Mac OS X system to FreeNAS®. The process for creating an authenticated share for a user is the same as creating a Time Machine share for that user.

To use the Wizard to create an authenticated or Time Machine share, enter the following information, as seen in the example in [Figure 10.4](#).

1. **Share name:** input a name for the share that is useful to you but which is under 27 characters and does not contain a period. In this example, the share is named *backup_user1*.
2. Click the button for *Mac OS X (AFP)* and check the box for *Time Machine*. If the user will not be using Time Machine, leave the box unchecked.
3. Click the *Ownership* button. If the user already exists on the FreeNAS® system, click the drop-down *User* menu to select their user account. If the user does not yet exist on the FreeNAS® system, type their name into the *User* field and check the *Create User* checkbox. If the user will be a member of a group that already exists on the FreeNAS® system, click the drop-down *Group* menu to select the group name. To create a new group to be used by Time Machine users, enter the name in the *Group* field and check the *Create Group* checkbox. Otherwise, enter the same name as the user. In the example shown in [Figure 10.5](#), both a new *user1* user and a new *tm_backups* group will be created. Since a new user is being created, this screen prompts for the user

password to be used when accessing the share. It also provides an opportunity to change the default permissions on the share. When finished, click *Return* to return to the screen shown in Figure 10.4.

4. Click the *Add* button. **If you forget to do this, the share will not be created.** Clicking the *Add* button adds an entry to the *Name* frame with the name that was entered in *Share name*.

To configure multiple authenticated or Time Machine shares, repeat for each user, giving each user their own *Share name* and *Ownership*. When finished, click the *Next* button twice, then the *Confirm* button to create the shares. The Wizard automatically creates a dataset for each share with the correct ownership and starts the AFP service so the shares are immediately available. The new shares are also added to *Sharing → Apple (AFP)*.

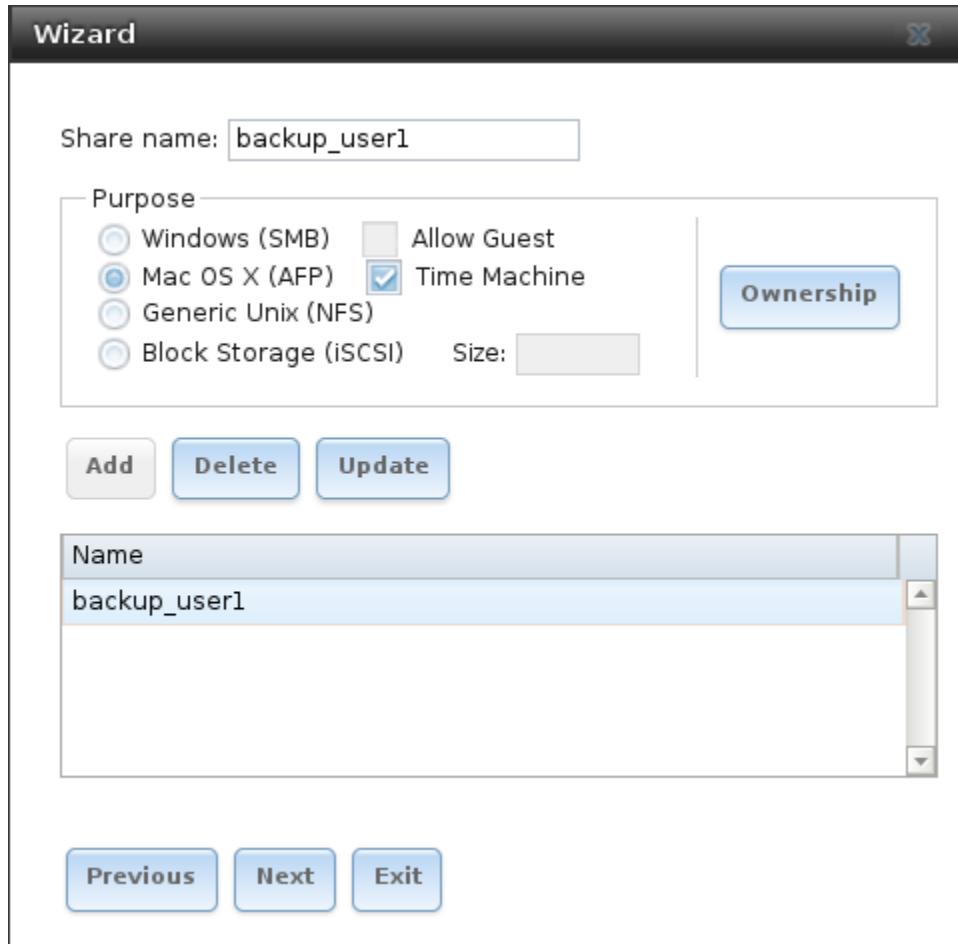


Fig. 10.4: Creating a Time Machine Share

At this point, it may be desirable to configure a quota for each Time Machine share, to restrict backups from using all of the available space on the FreeNAS® system. The first time Time Machine makes a backup, it 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 a Time Machine share becomes full, make sure that the quota size you set is sufficient to hold the desired number of backups.** Note that a default installation of Mac OS X is ~21 GB in size.

To configure a quota, go to *Storage → Volumes* and highlight the entry for the share. In the example shown in Figure 10.6, the Time Machine share name is *backup_user1*. Click the *Edit Options* button for the share, then *Advanced Mode*. Enter a value in the *Quota for this dataset* field, then click *Edit Dataset* to save the change. In this example, the Time Machine share is restricted to 200 GB.

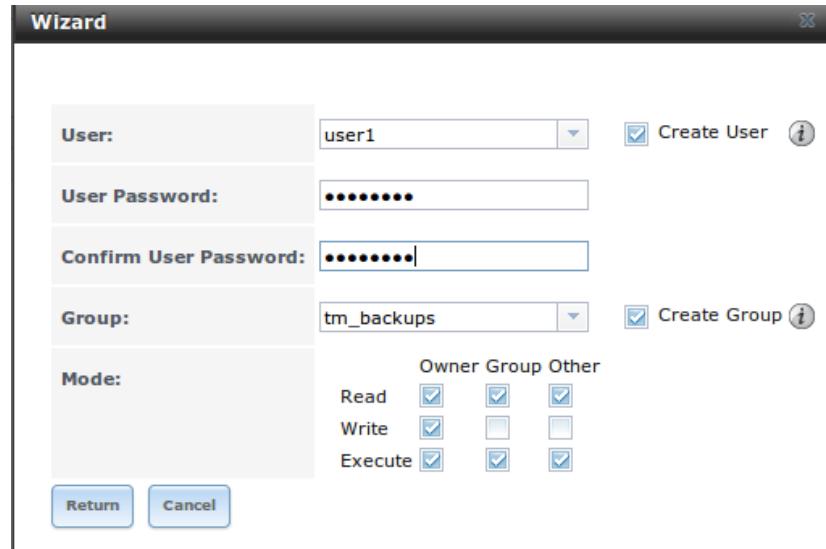


Fig. 10.5: Creating an Authenticated User

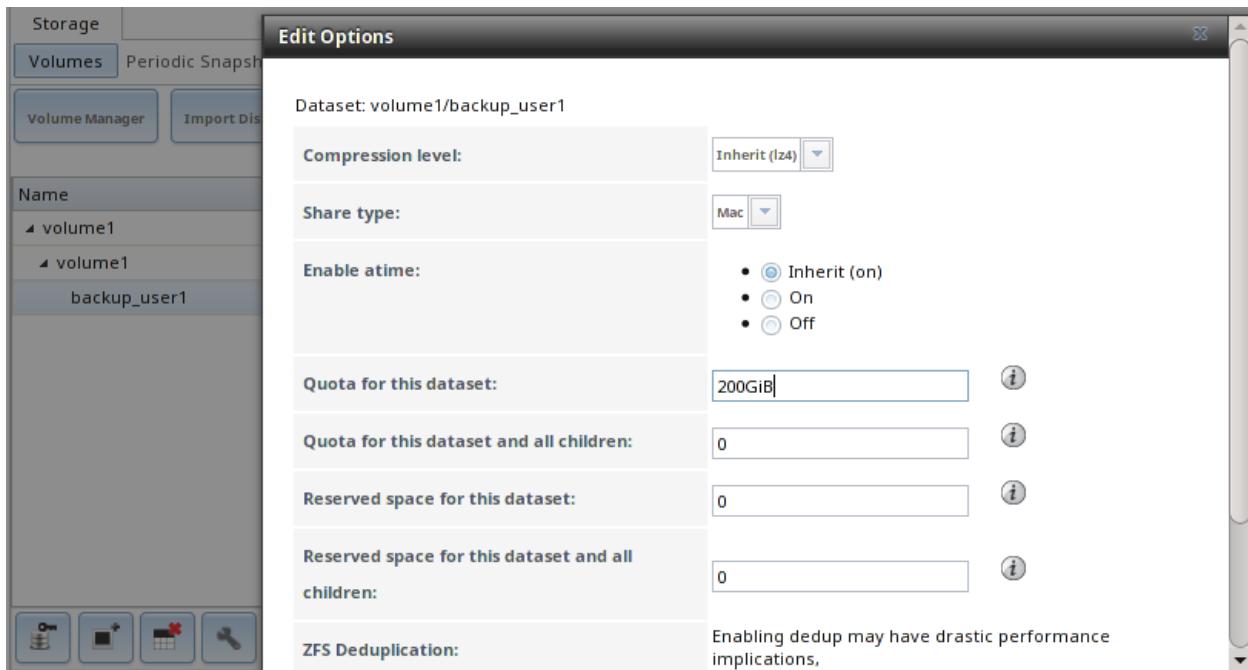


Fig. 10.6: Setting a Quota

To configure Time Machine on the Mac OS X client, go to System Preferences → Time Machine which opens the screen shown in [Figure 10.7](#). Click *ON* and a pop-up menu shows the FreeNAS® system as a backup option. In our example, it is listed as *backup_user1 on “freenas”*. Highlight the FreeNAS® system and click *Use Backup Disk*. A connection bar opens and prompts for the user account’s password—in this example, the password that was set for the *user1* account.



Fig. 10.7: Configuring Time Machine on Mac OS X Lion

If *Time Machine could not complete the backup. The backup disk image could not be created (error 45)* is shown when backing up to the FreeNAS® system, a sparsebundle image must be created using [these instructions](#).

If *Time Machine completed a verification of your backups. To improve reliability, Time Machine must create a new backup for you.* is shown, and you do not want to perform another complete backup or lose past backups, follow the instructions in [this post](#).

10.2 Unix (NFS) Shares

FreeNAS® supports sharing over the Network File System (NFS). Clients use the `mount` command to mount the share. Once mounted, the NFS 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. On Windows systems, enable Services for NFS in the Ultimate or Enterprise editions or install an NFS client application.

Note: For performance reasons, iSCSI is preferred to NFS shares when FreeNAS® is installed on ESXi. If you are considering creating NFS shares on ESXi, read through the performance analysis at [Running ZFS over NFS](#) as a

VMware Store.

To create an NFS share using the Wizard, click the *Next* button twice to display the screen shown in Figure 10.8. Enter a *Share name* which makes sense to you, but does not contain a space. Click the button for *Generic Unix (NFS)*, then click *Add* so the share's name appears in the *Name* frame. When finished, click the *Next* button twice, then the *Confirm* button to create the share. Creating an NFS share using the wizard automatically creates a new dataset for the share, starts the services required for NFS, and adds an entry in *Sharing → Unix (NFS) Shares*. Depending on your requirements, you may wish to fine-tune which IP addresses are allowed to access the NFS share or to restrict the permissions of the mounted share.

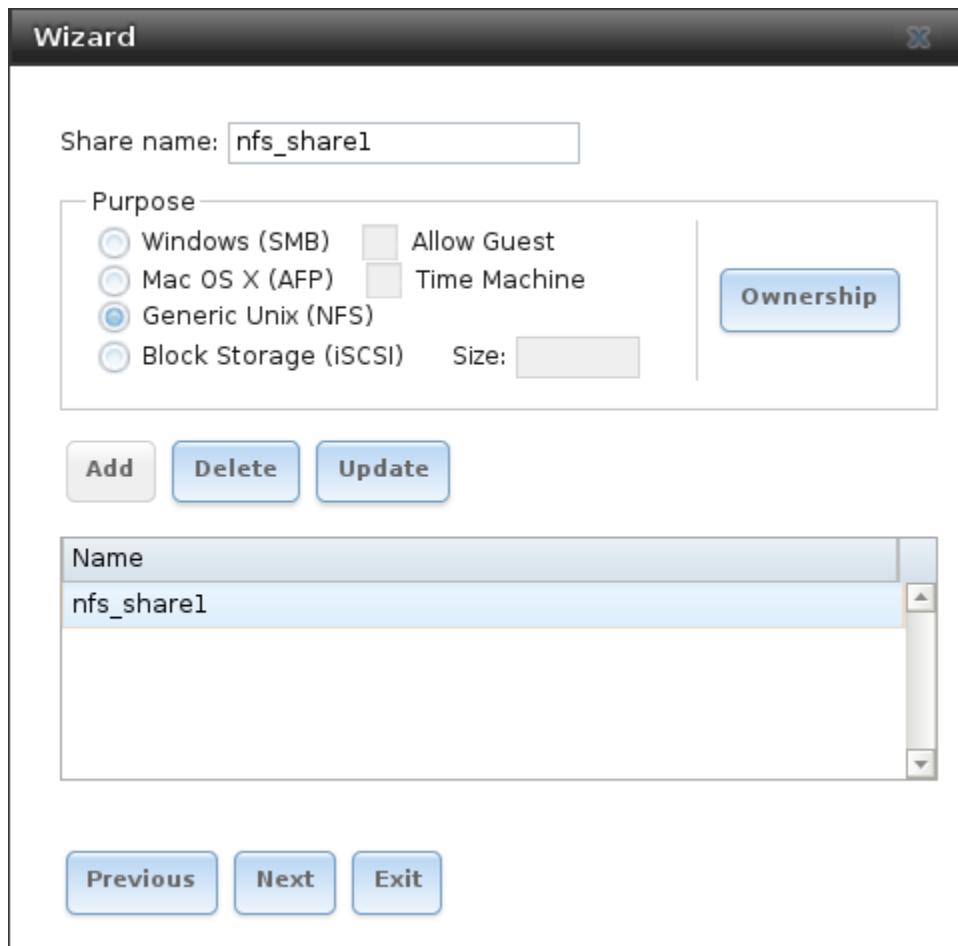


Fig. 10.8: NFS Share Wizard

To edit the NFS share, click *Sharing → Unix (NFS)*, highlight the entry for the share, and click its *Edit* button. In the example shown in Figure 10.9, the configuration screen is open for the *nfs_share1* share.

Table 10.2 summarizes the available configuration options in this screen. Some settings are only available by clicking the *Advanced Mode* button.

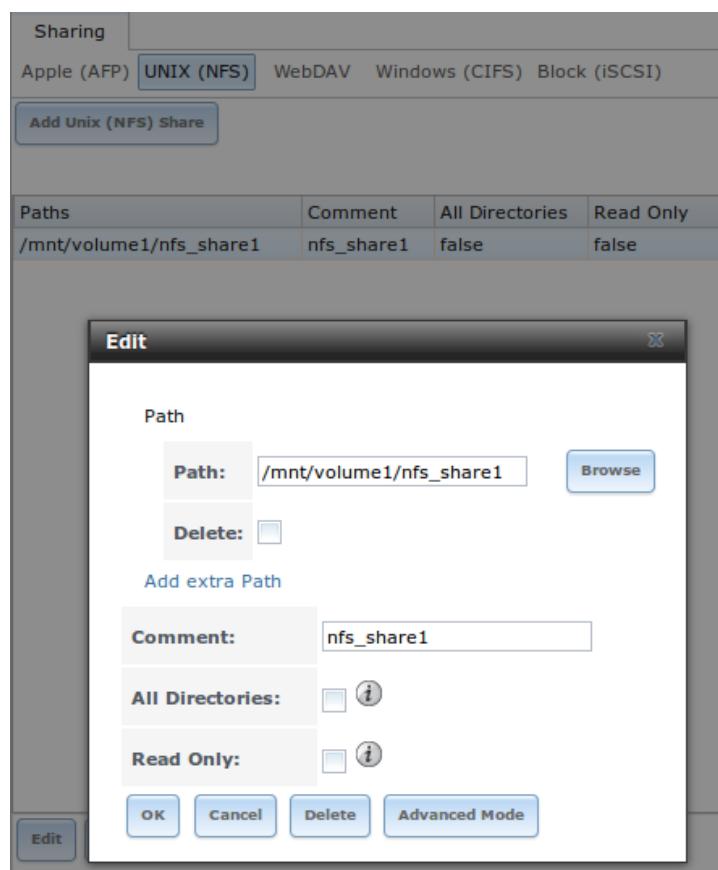


Fig. 10.9: NFS Share Settings

Table 10.2: NFS Share Options

Setting	Value	Description
Path	browse button	the path that clients will use when mounting the share; click <i>Add extra path</i> to select multiple paths
Comment	string	used to set the share name; if left empty, share name is the list of selected <i>Path</i> entries
Authorized networks	string	only available in <i>Advanced Mode</i> ; space delimited list of allowed network addresses in the form 1.2.3.0/24 where the number after the slash is a CIDR mask
Authorized IP addresses or hosts	string	only available in <i>Advanced Mode</i> ; space delimited list of allowed IP addresses or hostnames
All directories	check-box	if checked, the client can mount any subdirectory within the <i>Path</i>
Read only	check-box	prohibit writing to the share
Quiet	check-box	only available in <i>Advanced Mode</i> ; inhibits some syslog diagnostics which can be useful to avoid some annoying error messages; see exports(5) for examples
Maproot User	drop-down menu	only available in <i>Advanced Mode</i> ; if a user is selected, the <i>root</i> user is limited to that user's permissions
Maproot Group	drop-down menu	only available in <i>Advanced Mode</i> ; if a group is selected, the <i>root</i> user will also be limited to that group's permissions
Mapall User	drop-down menu	only available in <i>Advanced Mode</i> ; the specified user's permissions are used by all clients
Mapall Group	drop-down menu	only available in <i>Advanced Mode</i> ; the specified group's permission are used by all clients
Security	selection	only available in <i>Advanced Mode</i> and only appears if <i>Enable NFSv4</i> is checked in Services → NFS ; choices are <i>sys</i> or these Kerberos options: <i>krb5</i> (authentication only), <i>krb5i</i> (authentication and integrity), or <i>krb5p</i> (authentication and privacy); if multiple security mechanisms are added to the <i>Selected</i> column using the arrows, use the <i>Up</i> or <i>Down</i> buttons to list in order of preference

When creating NFS shares, keep the following points in mind:

1. The *Maproot* and *Mapall* options are exclusive, meaning only one can be used—the GUI does not allow both. The *Mapall* options supersede the *Maproot* options. To restrict only the *root* user's permissions, set the *Maproot* option. To restrict permissions of all users, set the *Mapall* options.
2. Each volume or dataset is considered to be its own filesystem and NFS is not able to cross filesystem boundaries.
3. The network or host must be unique per share and per filesystem or directory.
4. The *All directories* option can only be used once per share per filesystem.

To better understand these restrictions, consider the following scenario where there are:

- 2 networks named *10.0.0.0/8* and *20.0.0.0/8*
- a ZFS volume named *volume1* with 2 datasets named *dataset1* and *dataset2*
- *dataset1* has a directory named *directory1*

Because of restriction #3, an error is shown if you try to create one NFS share like this:

- *Authorized networks* set to `10.0.0.0/8 20.0.0.0/8`
- *Path* set to `/mnt/volume1/dataset1` and `/mnt/volume1/dataset1/directory1`

Instead, you should set a *Path* of `/mnt/volume1/dataset1` and check the *All directories* box.

However, you could restrict that directory to one of the networks by creating two shares instead:

First NFS share:

- *Authorized networks* set to `10.0.0.0/8`
- *Path* set to `/mnt/volume1/dataset1`

Second NFS share:

- *Authorized networks* set to `20.0.0.0/8`
- *Path* set to `/mnt/volume1/dataset1/directory1`

Note that this requires the creation of two shares as it cannot be done with only one share.

10.2.1 Example Configuration

By default, the *Mapall* options 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 complete access to the share.

A better scenario is to do the following:

1. Specify the built-in *nobody* account to be used for NFS access.
2. In the *Change Permissions* screen of the volume/dataset that is being shared, change the owner and group to *nobody* and set the permissions according to your requirements.
3. Select *nobody* in the *Mapall User* and *Mapall Group* drop-down menus for the share in *Sharing → Unix (NFS) Shares*.

With this configuration, it does not matter which user account connects to the NFS share, as it will be mapped to the *nobody* user account and will only have the permissions that were specified on the volume/dataset. For example, even if the *root* user is able to connect, it will not gain *root* access to the share.

10.2.2 Connecting to the Share

In the following examples, an NFS share on a FreeNAS® system with the IP address of `192.168.2.2` 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 these attributes:
 - *Path*: `/mnt/data`
 - *Authorized Network*: `192.168.2.0/24`
 - *MapAll User* and *MapAll Group* are both set to *nobody*
 - the *All Directories* checkbox has been checked

From BSD or Linux

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 on each client that needs access to the NFS share:

```
mount -t nfs 192.168.2.2:/mnt/data /mnt
```

The **mount** command uses these:

- **-t nfs**: specifies the type of share.
- **192.168.2.2**: replace with the IP address of the FreeNAS® system
- **/mnt/data**: replace with the name of the NFS share
- **/mnt**: a mount point on the client system. This must be an existing, **empty** directory. The data in the NFS share will be made available to the client in this directory.

The **mount** command should return to the command prompt without any error messages, indicating that the share was successfully mounted.

Note: If this command fails on a Linux system, make sure that the **nfs-utils** package is installed.

Once mounted, this configuration allows users on the client system to copy files to and from **/mnt** (the mount point) and all files will be owned by *nobody:nobody*. Any changes to **/mnt** will be saved to the FreeNAS® system's **/mnt/data** volume.

Should you wish to make any changes to the NFS share's settings or wish to make the share inaccessible, first unmount the share on the client as the superuser:

```
umount /mnt
```

From Microsoft

Windows systems can connect to NFS shares using Services for NFS (refer to the documentation for your version of Windows for instructions on how to find, activate, and use this service) or a third-party NFS client.

Nekodrive provides an open source graphical NFS client. To use this client, you will need to install the following on the Windows system:

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

After everything is installed, run the NFSClient executable to start the GUI client. In the example shown in [Figure 10.10](#), the user has connected to the example **/mnt/data** share of the FreeNAS® system at **192.168.2.2**.

Note: Nekodrive does not support Explorer drive mapping via NFS. If you need this functionality, [try this utility](#) instead.

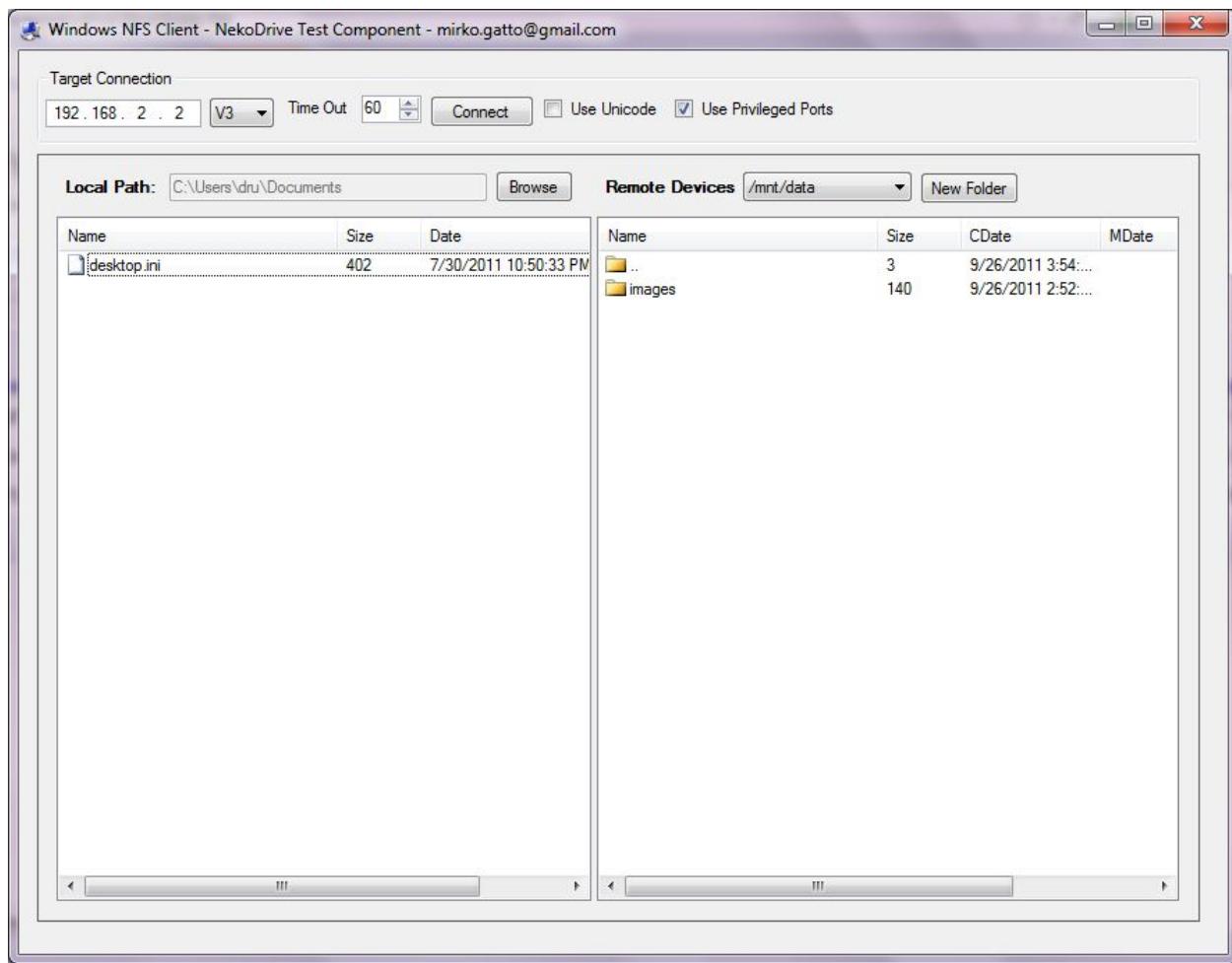


Fig. 10.10: Using the Nekodrive NFSClient from Windows 7 Home Edition

From Mac OS X

To mount the NFS volume from a Mac OS X client, click on Go → Connect to Server. In the *Server Address* field, enter *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 10.11 continues with our example of *192.168.2.2:/mnt/data*.

Once connected, Finder opens automatically. The IP address of the FreeNAS® system is displayed in the SHARED section in the left frame and the contents of the share are displayed in the right frame. In the example shown in Figure 10.12, */mnt/data* has one folder named *images*. The user can now copy files to and from the share.

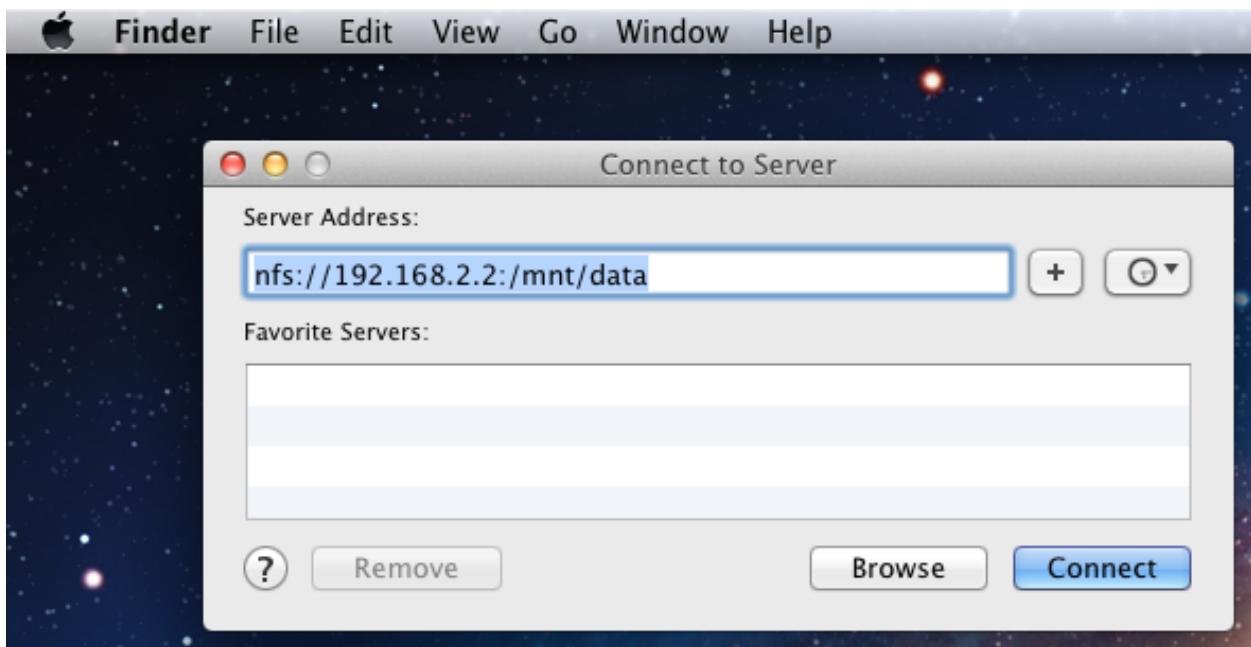


Fig. 10.11: Mounting the NFS Share from Mac OS X

10.2.3 Troubleshooting NFS

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, add the option **-o nolock** when running the **mount** command on the client in order to allow write access to the NFS share.

If a “time out giving up” error is shown when trying to mount the share from a Linux system, make sure that the portmapper service is running on the Linux client. If portmapper is running and timeouts are still shown, force the use of TCP by including **-o tcp** in the **mount** command.

If a “RPC: Program not registered” error is shown, upgrade to the latest version of FreeNAS® and restart the NFS service after the upgrade to clear the NFS cache.

If clients see “reverse DNS” errors, add the FreeNAS® IP address in the *Host name database* field of Network → Global Configuration.

If clients receive timeout errors when trying to mount the share, add the client IP address and hostname to the *Host name data base* field in Network → Global Configuration.

Some older versions of NFS clients default to UDP instead of TCP and do not auto-negotiate for TCP. By default, FreeNAS® uses TCP. To support UDP connections, go to Services → NFS and check the box *Serve UDP NFS*.

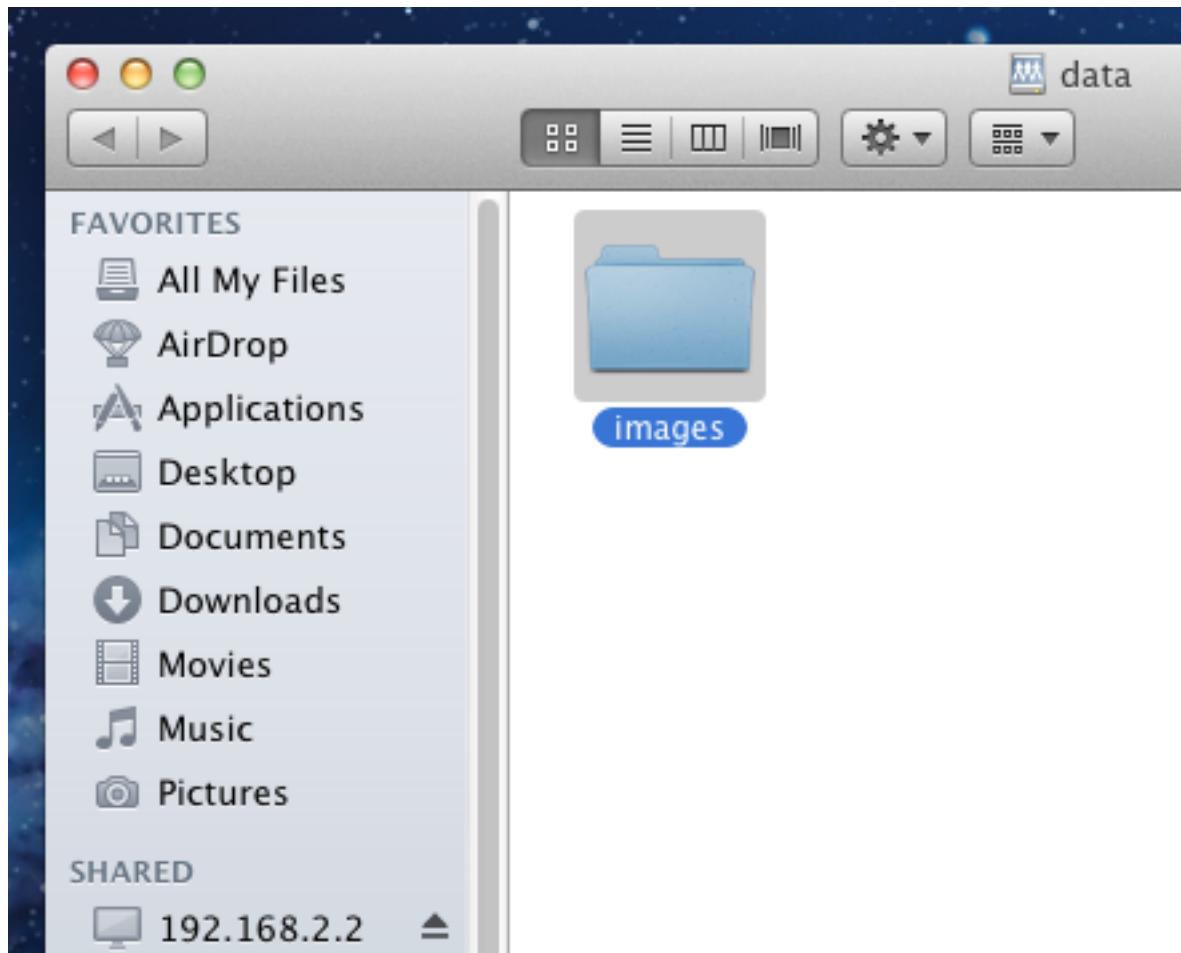


Fig. 10.12: Viewing the NFS Share in Finder

clients.

10.3 WebDAV Shares

In FreeNAS®, WebDAV shares can be created so that authenticated users can browse the contents of the specified volume, dataset, or directory from a web browser.

Configuring WebDAV shares is a two step process. First, create the WebDAV share(s) to specify which data can be accessed. Then, configure the WebDAV service by specifying the port, authentication type, and authentication password. Once the configuration is complete, the share can be accessed using a URL in the format:

```
protocol://IP_address:port_number/share_name
```

where:

- **protocol:** is either *http* or *https*, depending upon the *Protocol* configured in Services → WebDAV .
- **IP address:** is the IP address or hostname of the FreeNAS® system. Take care when configuring a public IP address to ensure that the network's firewall only allows access to authorized systems.
- **port_number:** is configured in Services → WebDAV . If the FreeNAS® system is to be accessed using a public IP address, consider changing the default port number and ensure that the network's firewall only allows access to authorized systems.
- **share_name:** is configured in Sharing → WebDAV Shares .

Entering the URL in a web browser brings up an authentication pop-up message. Enter a username of *webdav* and the password configured in Services → WebDAV .

Warning: At this time, only the *webdav* user is supported. For this reason, it is important to set a good password for this account and to only give the password to users which should have access to the WebDAV share.

To create a WebDAV share, click Sharing → WebDAV Shares → Add WebDAV Share which will open the screen shown in Figure 10.13.

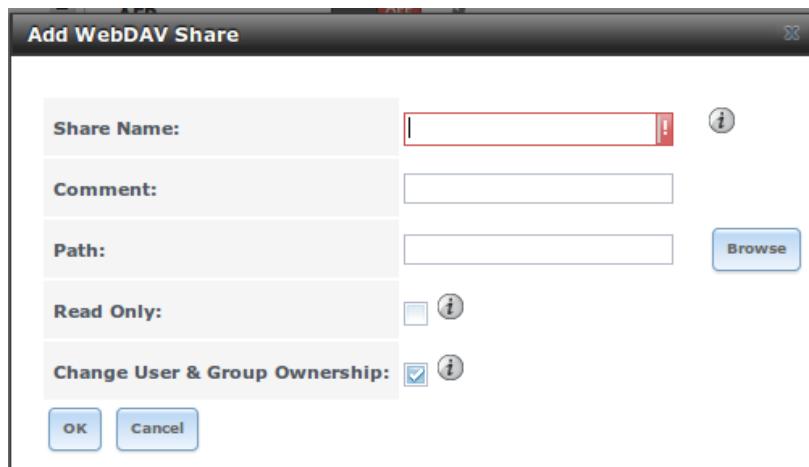


Fig. 10.13: Adding a WebDAV Share

Table 10.3 summarizes the available options.

Table 10.3: WebDAV Share Options

Setting	Value	Description
Share Path Name	string	input a name for the share
Comment	string	optional
Path	browse button	browse to the volume/dataset to share
Read Only	checkbox	if checked, users cannot write to the share
Change User & Group Ownership	checkbox	if checked, automatically sets the share's contents to the <i>webdav</i> user and group

After clicking *OK*, a pop-up asks about enabling the service. Once the service starts, review the settings in *Services* → *WebDAV* as they are used to determine which URL is used to access the WebDAV share and whether or not authentication is required to access the share. These settings are described in *WebDAV*.

10.4 Windows (SMB) Shares

FreeNAS® uses *Samba* to share volumes using Microsoft's SMB protocol. SMB is built into the Windows and Mac OS X operating systems and most Linux and BSD systems pre-install the Samba client in order to provide support for SMB. If your distro did not, install the Samba client using the distro's software repository.

The SMB protocol supports many different types of configuration scenarios, ranging from the very simple to quite complex. The complexity of the scenario depends upon the types and versions of the client operating systems that will connect to the share, whether the network has a Windows server, and whether Active Directory is being used. Depending on the authentication requirements, it might be necessary to create or import users and groups.

This chapter starts by summarizing the available configuration options. It will then demonstrate some common configuration scenarios as well as offer some troubleshooting tips. It is recommended to first read through this entire chapter before creating any SMB shares so that you have a good idea of the best configuration scenario to meet your network's needs.

Tip: *SMB Tips and Tricks* shows helpful hints for configuring and managing SMB networking.

Figure 10.14 shows the configuration screen that appears after clicking *Sharing* → *Windows (SMB Shares)* → *Add Windows (SMB) Share*.

Table 10.4 summarizes the options when creating a SMB share. Some settings are only available after clicking the *Advanced Mode* button. For simple sharing scenarios, *Advanced Mode* options are not needed. For more complex sharing scenarios, only change an *Advanced Mode* option after fully understanding the function of that option. *smb.conf(5)* provides more details for each configurable option.

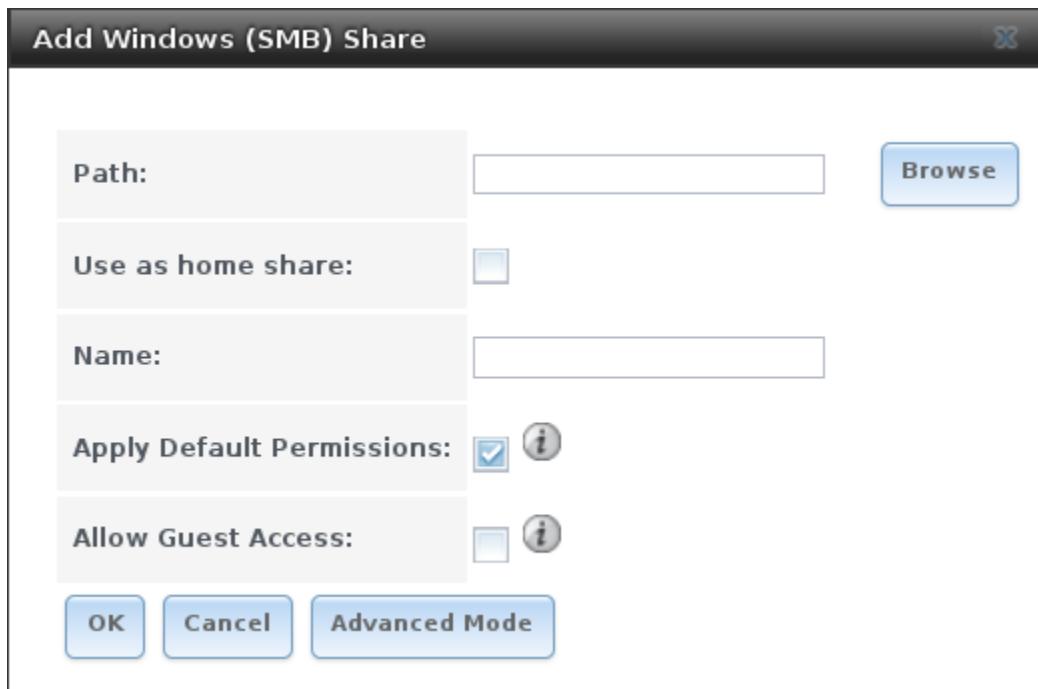


Fig. 10.14: Adding an SMB Share

Table 10.4: Options for a SMB Share

Setting	Value	Description
Path	browse button	select volume/dataset/directory to share
Use as home share	checkbox	check this box if the share is meant to hold user home directories; only one share can be homes share
Name	string	mandatory; name of share
Comment	string	only available in <i>Advanced Mode</i> ; optional description
Apply Default Permissions	checkbox	sets the ACLs to allow read/write for owner/group and read-only for others; should only be unchecked when creating a share on a system that already has custom ACLs set
Export Read Only	checkbox	only available in <i>Advanced Mode</i> ; prohibits write access to the share
Browsable to Network Clients	checkbox	only available in <i>Advanced Mode</i> ; when checked, users see the contents of <code>/homes</code> (including other home directories of other users) and when unchecked, users see only their own home directory
Export Recycle Bin	checkbox	only available in <i>Advanced Mode</i> ; deleted files are instead moved to a hidden <code>.recycle</code> directory in the root folder of the share
Show Hidden Files	checkbox	only available in <i>Advanced Mode</i> ; if enabled, the Windows hidden attribute is not set when filenames that begin with a dot (a Unix hidden file) are created; existing files are not affected
Allow Guest Access	checkbox	if checked, no password is required to connect to the share and all users share the permissions of the guest user defined in the SMB service
Only Allow Guest Access	checkbox	only available in <i>Advanced Mode</i> ; requires <i>Allow guest access</i> to also be checked; forces guest access for all connections
Hosts Allow	string	only available in <i>Advanced Mode</i> ; comma-, space-, or tab-delimited list of allowed hostnames or IP addresses
Hosts Deny	string	only available in <i>Advanced Mode</i> ; comma-, space-, or tab-delimited list of denied hostnames or IP addresses; allowed hosts take precedence so can use <code>ALL</code> in this
170		field and specify allowed hosts in <i>Hosts Allow</i>
VFS Objects	selection	only available in <i>Advanced Mode</i> ; adds virtual file system modules to enhance functionality; Table 10.5 summarizes the available modules
Periodic	drop-	used to configure home directory shadow copies on a per-share basis; select the

Note the following regarding some of the *Advanced Mode* settings:

- Hostname lookups add some time to accessing the SMB share. If you only use IP addresses, uncheck the *Hostnames lookup* box in Services → SMB.
- 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. However, they can still access the share from the command line. Unchecking this option provides limited security and is not a substitute for proper permissions and password control.
- If some files on a shared volume should be hidden and inaccessible to users, put a *veto files=* line in the *Auxiliary Parameters* field. The syntax for the *veto files* option and some examples can be found [here](#).

To configure support for OS/2 clients, add this line to *Auxiliary Parameters*:

```
lanman auth = yes
```

To configure lanman authentication for pre-NT authentication, add these lines instead:

```
client lanman auth = yes
client plaintext auth = yes
```

Table 10.5 provides an overview of the available VFS modules. Be sure to research each module **before** adding or deleting it from the *Selected* column of the *VFS Objects* field of the share. Some modules need additional configuration after they are added. Refer to [Stackable VFS modules](#) and the [vfs_*](#) man pages for more details.

Table 10.5: Available VFS Modules

Value	Description
acl_tdb	stores NTFS ACLs in a tdb file in order to enable full mapping of Windows ACLs
acl_xattr	stores NTFS ACLs in Extended Attributes (EAs) in order to enable the full mapping of Windows ACLs
aio_fork	enables async I/O
aio_posix	enables asynchronous I/O on systems running POSIX kernels
aio_pthread	implements async I/O in Samba vfs using a pthread pool instead of the internal Posix AIO interface
audit	logs share access, connects/disconnects, directory opens/creates/removes, and file opens/closes/renames/unlinks
cacheprime	primes the kernel file data cache
cap	translates filenames to and from the CAP encoding format, commonly used in Japanese language environments
catia	creates filenames that use characters that are illegal in SMB filenames
commit	tracks the amount of data written to a file and synchronizes it to disk when a specified amount accumulates
crossrename	allows server side rename operations even if source and target are on different physical devices
default_quota	stores the default quotas that are reported to a windows client in the quota record of a user
dfs_samba4	distributed file system for providing an alternative name space, load balancing, and automatic failover
dirsort	sorts directory entries alphabetically before sending them to the client
expand_msdfs	enables support for Microsoft Distributed File System (DFS)
extd_audit	sends <i>audit</i> logs to both syslog and the Samba log files
fake_acls	stores file ownership and ACLs as extended attributes
fake_perms	allows roaming profile files and directories to be set as read-only
fruit	enhances OS X support by providing the SMB2 AAPL extension and Netatalk interoperability (see NOTE below)
full_audit	records selected client operations to the system log
linux_xfs_sgid	used to work around an old Linux XFS bug
media_harmony	allows Avid editorial workstations to share a network drive
netatalk	eases the co-existence of SMB and AFP shares
posix_eadb	provides Extended Attributes (EAs) support so they can be used on filesystems which do not provide native su

Table 10.5 – continued from previous page

Value	Description
preopen	useful for video streaming applications that want to read one file per frame
readahead	useful for Windows Vista clients reading data using Windows Explorer
readonly	marks a share as read-only for all clients connecting within the configured time period
scannedonly	ensures that only files that have been scanned for viruses are visible and accessible
shadow_copy	allows Microsoft shadow copy clients to browse shadow copies on Windows shares
shadow_copy_test	shadow copy testing
shell_snap	provides shell-script callouts for snapshot creation and deletion operations issued by remote clients using the FRSVP protocol
skel_opaque	implements dummy versions of all VFS modules (useful to VFS module developers)
skel_transparent	implements dummy passthrough functions of all VFS modules (useful to VFS module developers)
smb_traffic_analyzer	logs Samba read and write operations through a socket to a helper application
snapper	provides the ability for remote SMB clients to access shadow copies of FRSVP snapshots using Windows Explorer
streams_depot	experimental module to store alternate data streams in a central directory
streams_xattr	enables storing of NTFS alternate data streams in the file system
syncops	ensures metadata operations are performed synchronously
time_audit	logs system calls that take longer than the number of defined milliseconds
unityed_media	allows multiple Avid clients to share a network drive
worm	controls the writability of files and folders depending on their change time and an adjustable grace period
xattr_tdb	stores Extended Attributes (EAs) in a tdb file so they can be used on filesystems which do not provide support

Note: When using *fruit*, also add the *streams_xattr* and *catia* VFS objects and be sure to configure **all** SMB shares this way. Reboot the Mac client after making this change.

These VFS objects do not appear in the drop-down menu as they are always enabled:

- **recycle:** moves deleted files to the recycle directory instead of deleting them
- **shadow_copy2:** a more recent implementation of *shadow_copy* with some additional features
- **zfs_space:** correctly calculates ZFS space used by share, including any reservations or quotas
- **zfsacl:**

10.4.1 Configuring Unauthenticated Access

SMB supports guest logins, meaning that users can access the SMB share without needing to provide a username or password. This type of share is convenient as it is easy to configure, easy to access, and does not require any users to be configured on the FreeNAS® system. This type of configuration is also the least secure as anyone on the network can access the contents of the share. Additionally, since all access is as the guest user, even if the user inputs a username or password, there is no way to differentiate which users accessed or modified the data on the share. This type of configuration is best suited for small networks where quick and easy access to the share is more important than the security of the data on the share.

To configure an unauthenticated SMB share, click *Wizard*, then click the *Next* button twice to display the screen shown in Figure 10.15. Complete the following fields in this screen:

1. **Share name:** enter a name for the share that is useful to you. In this example, the share is named *smb_insecure*.
2. Click the button for *Windows (SMB)* and check the box for *Allow Guest*.
3. Click the *Ownership* button. Click the drop-down *User* menu and select *nobody*. Click the *Return* button to return to the previous screen.

4. Click the *Add* button. **If you forget to do this, the share will not be created.** Clicking the *Add* button adds an entry to the *Name* frame with the name that was entered in *Share name*.

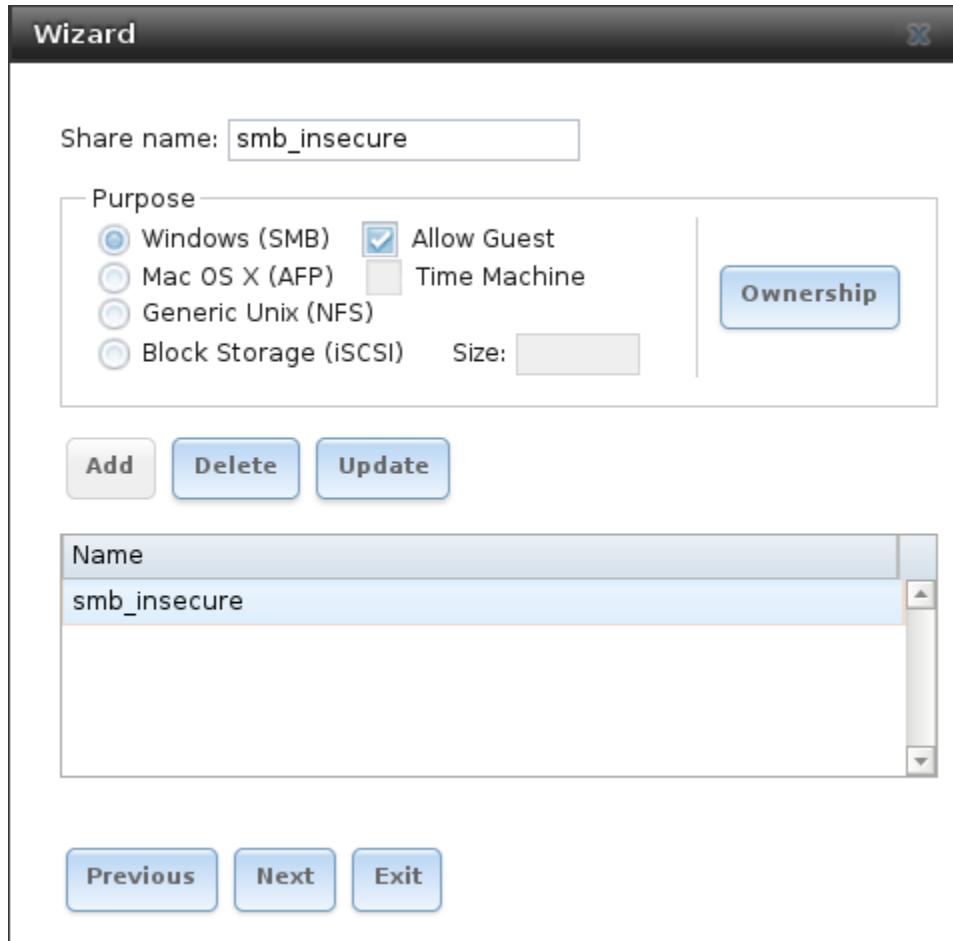


Fig. 10.15: Creating an Unauthenticated SMB Share

Click the *Next* button twice, then the *Confirm* button to create the share. The Wizard automatically creates a dataset for the share and starts the SMB service so the share is immediately available. The new share is also be added to Sharing → Windows (SMB).

Users can now access the share from any SMB client and will not be prompted for their username or password. For example, to access the share from a Windows system, open Explorer and click on *Network*. For this configuration example, a system named *FREENAS* appears with a share named *insecure_smb*. The user can copy data to and from the unauthenticated SMB share.

10.4.2 Configuring Authenticated Access Without a Domain Controller

Most configuration scenarios require each user to have their own user account and to authenticate before accessing the share. This allows the administrator to control access to data, provide appropriate permissions to that data, and to determine who accesses and modifies stored data. A Windows domain controller is not needed for authenticated SMB shares, which means that additional licensing costs are not required. However, since there is no domain controller to provide authentication for the network, each user account needs to be created on the FreeNAS® system. This type of configuration scenario is often used in home and small networks as it does not scale well if many users accounts are needed.

Before configuring this scenario, determine which users will need authenticated access. While not required for the configuration, it eases troubleshooting if the username and password that will be created on the FreeNAS® system matches that information on the client system. Next, determine if each user should have their own share to store their own data or if several users will be using the same share. The simpler configuration is to make one share per user as it does not require the creation of groups, adding the correct users to the groups, and ensuring that group permissions are set correctly.

To use the Wizard to create an authenticated SMB share, enter the following information, as shown in the example in Figure 10.16.

1. **Share name:** enter a name for the share that is useful to you. In this example, the share is named *smb_user1*.
2. Click the button for *Windows (SMB)*.
3. Click the *Ownership* button. To create the user account on the FreeNAS® system, type their name into the *User* field and check the *Create User* checkbox. The user's password is then entered and confirmed. **If the user will not be sharing this share with other users**, type their name into the *Group* field and click *Create Group*. **If, however, the share will be used by several users**, instead type in a group name and check the *Create Group* box. In the example shown in Figure 10.17, *user1* has been used for both the user and group name, meaning that this share will only be used by *user1*. When finished, click *Return* to return to the screen shown in Figure 10.16.
4. Click the *Add* button. **If you forget to do this, the share will not be created.** Clicking the *Add* button adds an entry to the *Name* frame with the name that was entered in *Share name*.

If you wish to configure multiple authenticated shares, repeat for each user, giving each user their own *Share name* and *Ownership*. When finished, click *Next* twice, then *Confirm* to create the shares. The Wizard automatically creates a dataset with the correct ownership for each share and starts the SMB service so the shares are available immediately. The new shares are also added to *Sharing → Windows (SMB)*.

Authenticated share can now be tested from any SMB client. For example, to test an authenticated share from a Windows system, open Explorer and click on *Network*. For this configuration example, a system named *FREENAS* appears with a share named *smb_user1*. If you click on *smb_user1*, a Windows Security pop-up screen prompts for that user's username and password. Enter the values that were configured for that share, in this case user *user1*. After authentication, the user can copy data to and from the SMB share.

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....* Choose a drive letter from the drop-down menu and click the *Finish* button.

Note that Windows systems cache a user's credentials. This can cause issues when testing or accessing multiple authenticated shares as only one authentication is allowed at a time. If you are having problems authenticating to a share and are sure that you are entering the correct username and password, type **cmd** in the *Search programs and files* box and use the following command to see if you have already authenticated to a share. In this example, the user has already authenticated to the *smb_user1* share:

```
net use
New connections will be remembered.

Status      Local      Remote          Network
-----
OK           \\FREENAS\smb_user1 Microsoft Windows Network
The command completed successfully.
```

To clear the cache:

```
net use * /DELETE
You have these remote connections:
    \\FREENAS\smb_user1
```

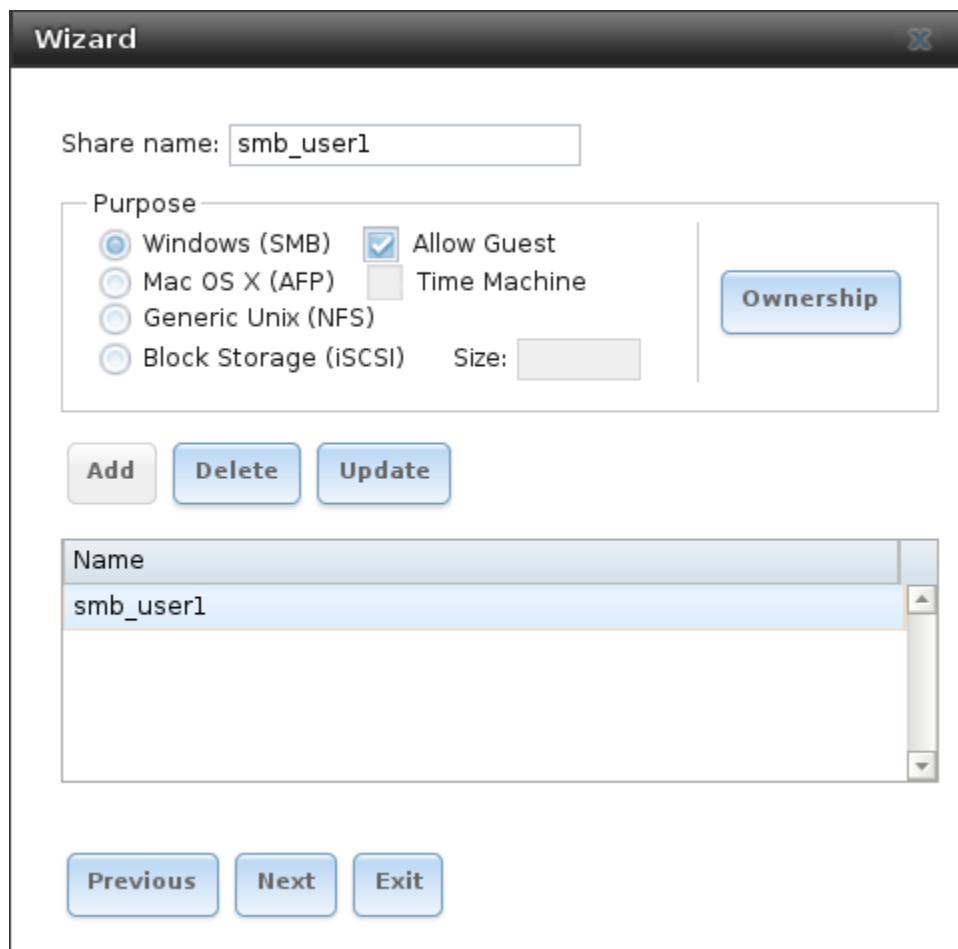


Fig. 10.16: Creating an Authenticated SMB Share

The screenshot shows the 'Wizard' window for creating a user and group. It has fields for 'User:' (set to 'user1'), 'User Password:', 'Confirm User Password:', 'Group:' (set to 'user1'), and checkboxes for 'Create User' and 'Create Group'. Below these are 'Mode:' settings for 'Owner', 'Group', and 'Other' users, with checkboxes for 'Read', 'Write', and 'Execute' permissions. At the bottom are 'Return' and 'Cancel' buttons.

Fig. 10.17: Creating the User and Group

```
Continuing will cancel the connections.
```

```
Do you want to continue this operation? <Y/N> [N]: y
```

An additional warning is shown if the share is currently open in Explorer:

```
There are open files and/or incomplete directory searches pending on the connection  
to \\FREENAS\smb_user1.
```

```
Is it OK to continue disconnecting and force them closed? <Y/N> [N]: y  
The command completed successfully.
```

The next time a share is accessed with Explorer, you will be prompted to authenticate.

10.4.3 Configuring Shadow Copies

[Shadow Copies](#), also known as the Volume Shadow Copy Service (VSS) or Previous Versions, is a Microsoft service for creating volume snapshots. Shadow copies allow you to easily restore previous versions of files from within Windows Explorer. Shadow Copy support is built into Vista and Windows 7. Windows XP or 2000 users need to install the [Shadow Copy client](#).

When you create a periodic snapshot task on a ZFS volume that is configured as a SMB share in FreeNAS®, it is automatically configured to support shadow copies.

Before using shadow copies with FreeNAS®, be aware of the following caveats:

- If the Windows system is not fully patched to the latest service pack, Shadow Copies may not work. If you are unable to see any previous versions of files to restore, use Windows Update to make sure that the system is fully up-to-date.
- Shadow copy support only works for ZFS pools or datasets. This means that the SMB share must be configured on a volume or dataset, not on a directory.
- Datasets are filesystems and shadow copies cannot traverse filesystems. If you want to be able to see the shadow copies in your child datasets, create separate shares for them.
- Shadow copies will not work with a manual snapshot, you must create a periodic snapshot task for the pool or dataset being shared by SMB or a recursive task for a parent dataset.
- The periodic snapshot task should be created and at least one snapshot should exist **before** creating the SMB share. If the SMB share was created first, restart the SMB service in [Services → Control Services](#).
- Appropriate permissions must be configured on the volume/dataset being shared by SMB.
- Users cannot delete shadow copies on the Windows system due to the way Samba works. Instead, the administrator can remove snapshots from the FreeNAS® administrative GUI. The only way to disable shadow copies completely is to remove the periodic snapshot task and delete all snapshots associated with the SMB share.

To configure shadow copy support, use the instructions in [Configuring Authenticated Access Without a Domain Controller](#) to create the desired number of shares. In this configuration example, a Windows 7 computer has two users: *user1* and *user2*. For this example, two authenticated shares are created so that each user account has their own share. The first share is named *user1* and the second share is named *user2*. Then:

1. Use [Storage → Periodic Snapshot Tasks → Add Periodic Snapshot](#) to create at least one periodic snapshot task. You can either create a snapshot task for each user's dataset, in this example the datasets `/mnt/volumel/user1` and `/mnt/volumel/user2`, or you can create one periodic snapshot task for the entire volume, in this case `/mnt/volumel`. **Before continuing to the next step**, confirm that at least one snapshot for each defined task is displayed in the [Storage → Snapshots](#) tab. When creating

the schedule for the periodic snapshot tasks, keep in mind how often your users need to access modified files and during which days and time of day they are likely to make changes.

2. Go to Sharing → Windows (SMB) Shares . Highlight a share and click *Edit*, then *Advanced Mode*. Click the *Periodic Snapshot Task* drop-down menu and select the periodic snapshot task to use for that share. Repeat for each share being configured as a shadow copy. For this example, the share named /mnt/volume1/user1 is configured to use a periodic snapshot task that was configured to take snapshots of the /mnt/volume1/user1 dataset and the share named /mnt/volume1/user2 is configured to use a periodic snapshot task that was configured to take snapshots of the /mnt/volume1/user2 dataset.
3. Verify that the SMB service is set to *ON* in Services → Control Services .

Figure 10.18 provides an example of using shadow copies while logged in as *user1* on the Windows system. In this example, the user right-clicked *modified file* and selected *Restore previous versions* from the menu. This particular file has three versions: the current version, plus two previous versions stored on the FreeNAS® system. The user can choose to open one of the previous versions, copy a previous version to the current folder, or restore one of the previous versions, overwriting the existing file on the Windows system.

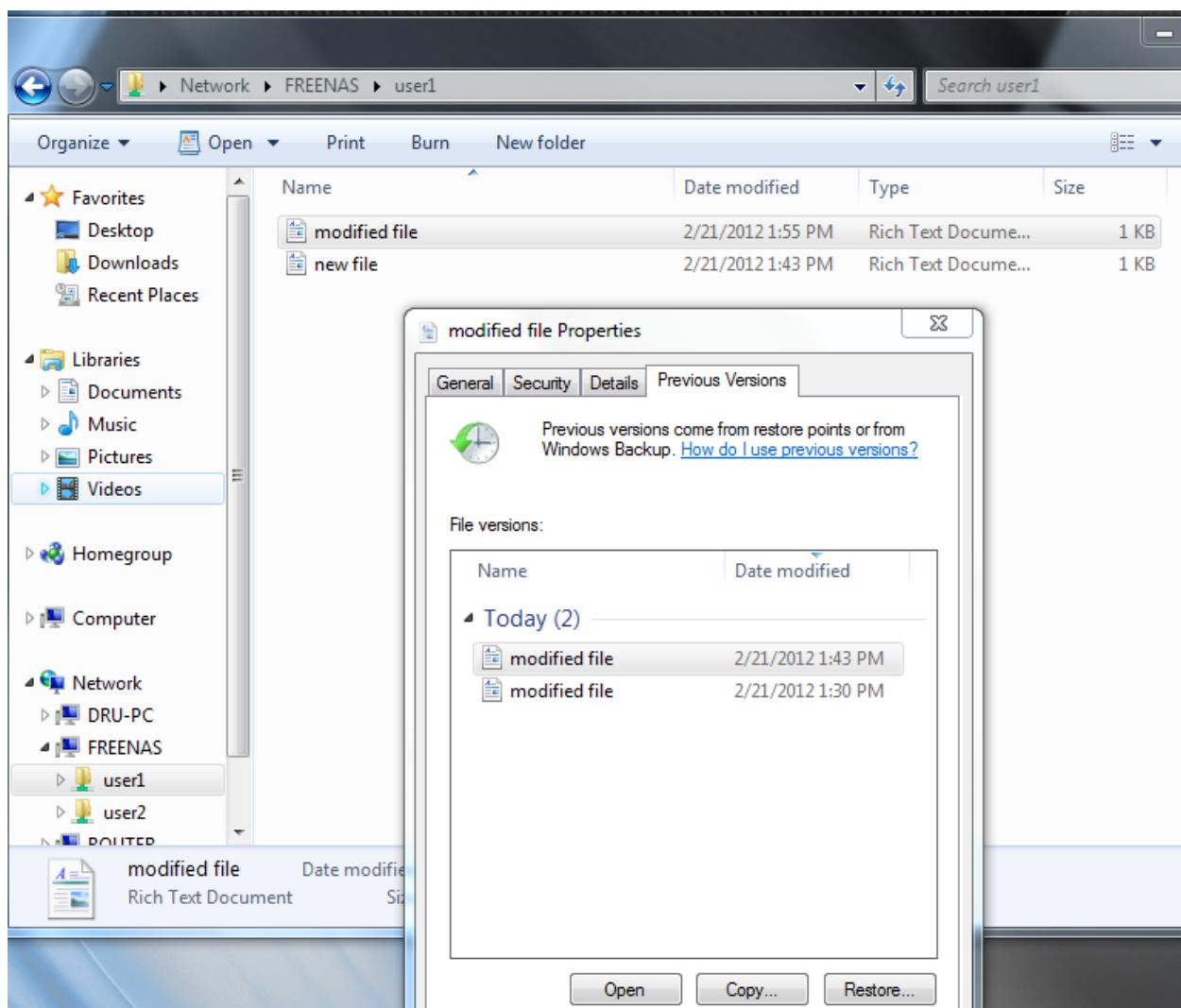


Fig. 10.18: Viewing Previous Versions within Explorer

10.5 Block (iSCSI)

iSCSI is a protocol standard for 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 discrete 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 the iSCSI service, be familiar with this iSCSI terminology:

CHAP: an authentication method which 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. In iSCSI, the initiator (client) performs the CHAP authentication.

Mutual CHAP: a superset of CHAP in that both ends of the communication authenticate to each other.

Initiator: a client which has authorized access to the storage data on the FreeNAS® system. The client requires initiator software in order to initiate the connection to the iSCSI share.

Target: a storage resource on the FreeNAS® system. Every target has a unique name known as an iSCSI Qualified Name (IQN).

Internet Storage Name Service (iSNS): protocol for the automated discovery of iSCSI devices on a TCP/IP network.

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

Portal: indicates which IP(s) and port(s) to listen on for connection requests.

LUN: stands for Logical Unit Number and represents a logical SCSI device. An initiator negotiates with a target to establish connectivity to a LUN; the result is an iSCSI connection that emulates a connection to a SCSI hard disk. Initiators treat iSCSI LUNs the same way as they would a raw SCSI or IDE hard drive; rather than mounting remote directories, initiators format and directly manage filesystems on iSCSI LUNs. When configuring multiple iSCSI LUNs, create a new target for each LUN. Since iSCSI multiplexes a target with multiple LUNs over the same TCP connection, you will experience contention from TCP if there is more than one target per LUN.

In FreeNAS®, iSCSI is built into the kernel. This version of iSCSI supports Microsoft Offloaded Data Transfer (ODX), meaning that file copies happen locally, rather than over the network. It also supports the following VAAI (vStorage APIs for Array Integration) primitives, where VAAI is VMware’s API framework that enables certain storage tasks, such as large data moves, to be offloaded from the virtualization hardware to the storage array.

- **unmap:** tells ZFS that the space occupied by deleted files should be freed. Without unmap, ZFS is unaware of freed space made when the initiator deletes files. For this feature to work, the initiator must support the unmap command.
- **atomic test and set:** allows multiple initiators to synchronize LUN access in a fine-grained manner rather than locking the whole LUN, which would prevent other hosts from accessing the same LUN simultaneously.
- **write same:** when allocating virtual machines with thick provisioning, the necessary write of zeroes is done locally, rather than over the network, so virtual machine creation is much quicker.
- **xcopy:** similar to Microsoft ODX, copies happen locally rather than over the network.
- **stun:** if a volume runs out of space, this feature pauses any running virtual machines so that the space issue can be fixed, instead of reporting write errors.
- **threshold warning:** the system reports a warning when a configurable capacity is reached. In FreeNAS®, this threshold can be configured at the pool level when using zvols (see [Table 10.6](#)) or at the extent level (see [Table 10.11](#)) for both file- and device-based extents. Typically, the warning is set at the pool level, unless file extents are used, in which case it must be set at the extent level.

- **LUN reporting:** the LUN reports that it is thin provisioned.

To take advantage of these VAAI primitives, create a zvol using the instructions in [Create zvol](#) and use it to create a device extent, as described in [Extents](#).

To configure iSCSI:

1. Review the target global configuration parameters.
2. Create at least one portal.
3. Determine which hosts are allowed to connect using iSCSI and create an initiator.
4. Decide if you will use authentication, and if so, whether it will be CHAP or mutual CHAP. If using authentication, create an authorized access.
5. Create a target.
6. Create either a device or a file extent to be used as storage.
7. Associate a target with an extent.
8. Start the iSCSI service in Services → Control Services.

The rest of this section describes these steps in more detail.

10.5.1 Target Global Configuration

Sharing → Block (iSCSI) → Target Global Configuration , shown in [Figure 10.19](#), contains settings that apply to all iSCSI shares. [Table 10.6](#) summarizes the settings that can be configured in the Target Global Configuration screen.

Fig. 10.19: iSCSI Target Global Configuration Variables

Table 10.6: Target Global Configuration Settings

Setting	Value	Description
Base Name	string	see the “Constructing iSCSI names using the iqn. format” section of RFC 3721 if unfamiliar with this format
ISNS Servers	string	space delimited list of hostnames or IP addresses of ISNS servers with which to register the system’s iSCSI targets and portals
Pool Available Space Threshold	integer	enter the percentage of free space that should remain in the pool; when this percentage is reached, the system will issue an alert, but only if zvols are used

10.5.2 Portals

A portal specifies the IP address and port number to be used for iSCSI connections. Sharing → Block (iSCSI) → Portals → Add Portal brings up the screen shown in [Figure 10.20](#).

[Table 10.20](#) summarizes the settings that can be configured when adding a portal. If you need to assign additional IP addresses to the portal, click the link *Add extra Portal IP*.

The screenshot shows the FreeNAS web interface under the 'Sharing' tab, specifically the 'Block (iSCSI)' section. The 'Portals' tab is selected. A modal dialog box titled 'Add Portal' is open in the foreground. The dialog contains fields for 'Comment' (with an info icon), 'Discovery Auth Method' (set to 'None'), 'Discovery Auth Group' (set to 'None'), 'Portal IP' (IP Address: '0.0.0.0', Port: '3260'), and a link 'Add extra Portal IP'. At the bottom are 'OK' and 'Cancel' buttons.

Fig. 10.20: Adding an iSCSI Portal

Table 10.7: Portal Configuration Settings

Setting	Value	Description
Comment	string	optional description; portals are automatically assigned a numeric group ID
Discovery Auth Method	drop-down menu	configures the authentication level required by the target for discovery of valid devices, where <i>None</i> will allow anonymous discovery while <i>CHAP</i> and <i>Mutual CHAP</i> require authentication
Discovery Auth Group	drop-down menu	select a user created in <i>Authorized Access</i> if the <i>Discovery Auth Method</i> is set to <i>CHAP</i> or <i>Mutual CHAP</i>
IP address	drop-down menu	select the IP address associated with an interface or the wildcard address of <i>0.0.0.0</i> (any interface)
Port	integer	TCP port used to access the iSCSI target; default is <i>3260</i>

FreeNAS® systems with multiple IP addresses or interfaces can use a portal to provide services on different interfaces or subnets. This can be used to configure multi-path I/O (MPIO). MPIO is more efficient than a link aggregation.

If the FreeNAS® system has multiple configured interfaces, portals can also be used to provide network access control. For example, consider a system with four interfaces configured with the following addresses:

192.168.1.1/24
192.168.2.1/24
192.168.3.1/24
192.168.4.1/24

You could create a portal containing the first two IP addresses (group ID 1) and a portal containing the remaining two IP addresses (group ID 2). You could then create a target named A with a Portal Group ID of 1 and a second target named B with a Portal Group ID of 2. In this scenario, the iSCSI service would listen on all four interfaces, but connections to target A would be limited to the first two networks and connections to target B would be limited to the last two networks.

Another scenario would be to create a portal which includes every IP address **except** for the one used by a management interface. This would prevent iSCSI connections to the management interface.

10.5.3 Initiators

The next step is to configure authorized initiators, or the systems which are allowed to connect to the iSCSI targets on the FreeNAS® system. To configure which systems can connect, use *Sharing* → *Block (iSCSI)* → *Initiators* → *Add Initiator*, shown in [Figure 10.21](#).

[Table 10.8](#) summarizes the settings that can be configured when adding an initiator.

Table 10.8: Initiator Configuration Settings

Setting	Value	Description
Initiators	string	use <i>ALL</i> keyword or a list of initiator hostnames separated by spaces
Authorized network	string	use <i>ALL</i> keyword or a network address with CIDR mask such as <i>192.168.2.0/24</i>
Comment	string	optional description

In the example shown in [Figure 10.22](#), two groups have been created. Group 1 allows connections from any initiator on any network. Group 2 allows connections from any initiator on the *10.10.1.0/24* network. Click an initiator's entry to display its *Edit* and *Delete* buttons.



Fig. 10.21: Adding an iSCSI Initiator

Note: Attempting to delete an initiator causes a warning that indicates if any targets or target/extent mappings depend upon the initiator. Confirming the delete causes these to be deleted as well.

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

Fig. 10.22: Sample iSCSI Initiator Configuration

10.5.4 Authorized Accesses

If you will be using CHAP or mutual CHAP to provide authentication, you must create an authorized access in Sharing → Block (iSCSI) → Authorized Accesses → Add Authorized Access . This screen is shown in Figure 10.23.

Note: This screen sets login authentication. This is different from discovery authentication which is set in [Target Global Configuration](#).

Table 10.9 summarizes the settings that can be configured when adding an authorized access:

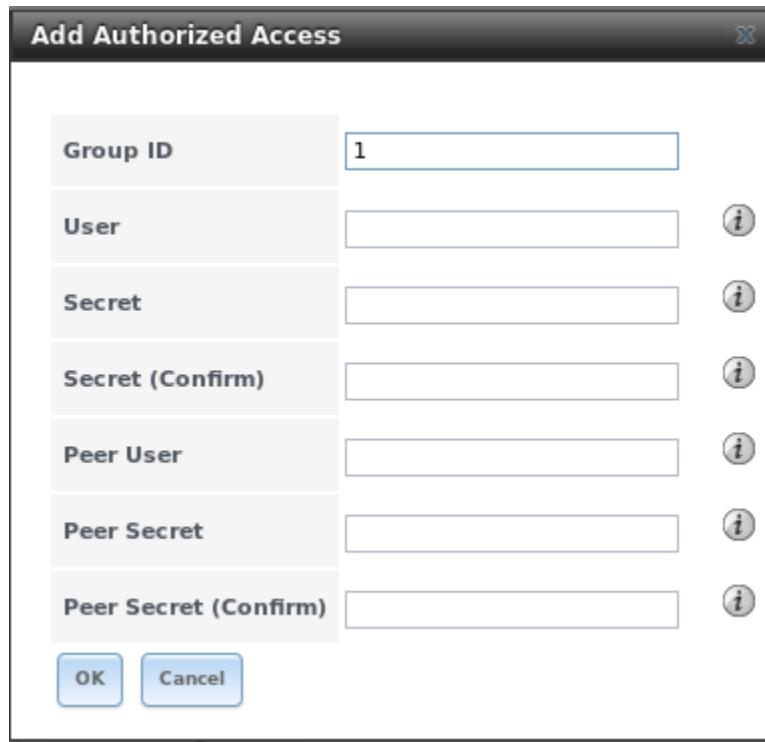


Fig. 10.23: Adding an iSCSI Authorized Access

Table 10.9: Authorized Access Configuration Settings

Setting	Value	Description
Group ID	integer	allows different groups to be configured with different authentication profiles; for instance, all users with a Group ID of 1 will inherit the authentication profile associated with Group 1
User	string	name of user account to create for CHAP authentication with the user on the remote system; many initiators default to using the initiator name as the user
Secret	string	password to be associated with <i>User</i> ; the iSCSI standard requires that this be between 12 and 16 characters
Peer User	string	only input when configuring mutual CHAP; in most cases it will need to be the same value as <i>User</i>
Peer Secret	string	the mutual secret password which must be different than the <i>Secret</i> ; required if <i>Peer User</i> is set

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

As authorized accesses are added, they will be listed under *View Authorized Accesses*. In the example shown in Figure 10.24, three users (*test1*, *test2*, and *test3*) and two groups (1 and 2) have been created, with group 1 consisting of one CHAP user and group 2 consisting of one mutual CHAP user and one CHAP user. Click an authorized access entry to display its *Edit* and *Delete* buttons.

Group ID	User	Peer User
1	test1	
2	test2	test2
2	test3	

Fig. 10.24: Viewing Authorized Accesses

10.5.5 Targets

Next, create a Target using Sharing → Block (iSCSI) → Targets → Add Target , as shown in [Figure 10.25](#). A target combines a portal ID, allowed initiator ID, and an authentication method. [Table 10.10](#) summarizes the settings that can be configured when creating a Target.

Note: An iSCSI target creates a block device that may be accessible to multiple initiators. A clustered filesystem is required on the block device, such as VMFS used by VMware ESX/ESXi, in order for multiple initiators to mount the block device read/write. If a traditional filesystem such as EXT, XFS, FAT, NTFS, UFS, or ZFS is placed on the block device, care must be taken that only one initiator at a time has read/write access or the result will be filesystem corruption. If multiple clients need access to the same data on a non-clustered filesystem, use SMB or NFS instead of iSCSI, or create multiple iSCSI targets (one per client).

Table 10.10: Target Settings

Setting	Value	Description
Target Name	string	required value; base name will be appended automatically if it does not start with <i>iqn</i>
Target Alias	string	optional user-friendly name
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 <i>None</i> , <i>Auto</i> , <i>CHAP</i> , or <i>Mutual CHAP</i>
Authentication Group number	drop-down menu	<i>None</i> or integer representing number of existing authorized access

10.5.6 Extents

In iSCSI, the target virtualizes something and presents it as a device to the iSCSI client. That something can be a device extent or a file extent:

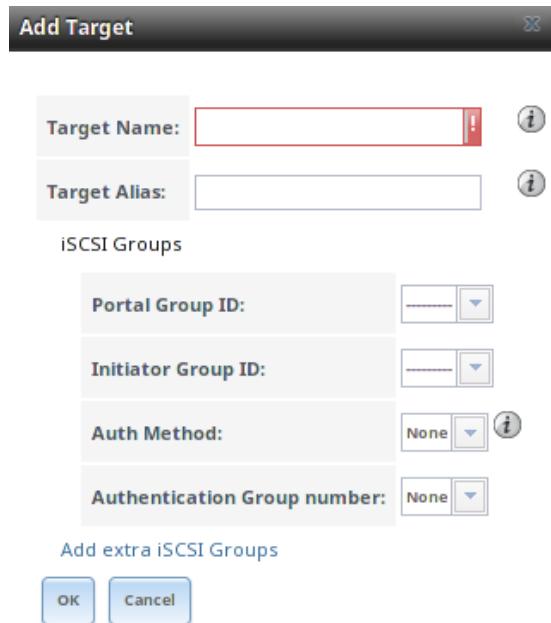


Fig. 10.25: Adding an iSCSI Target

Device extent: virtualizes an unformatted physical disk, RAID controller, zvol, zvol snapshot, or an existing [HAST device](#).

Virtualizing a single disk is slow as there is no caching, but virtualizing a hardware RAID controller has higher performance due to its cache. This type of virtualization does a pass-through to the disk or hardware RAID controller. None of the benefits of ZFS are provided and performance is limited to the capabilities of the disk or controller.

Virtualizing a zvol adds the benefits of ZFS, such as its read cache and write cache. Even if the client formats the device extent with a different filesystem, as far as FreeNAS® is concerned, the data benefits from ZFS features such as block checksums and snapshots.

When determining whether to use a file or a device extent, be aware that a zvol is required to take advantage of all VAAI primitives and is recommended when using virtualization software as the iSCSI initiator. The ATS, WRITE SAME, XCOPY and STUN, primitives are supported by both file and device extents. The UNMAP primitive is supported by zvols and raw SSDs. The threshold warnings primitive is fully supported by zvols and partially supported by file extents.

File extent: allows you to export a portion of a ZFS volume. The advantage of a file extent is that you can create multiple exports per volume.

Warning: For performance reasons and to avoid excessive fragmentation, it is recommended to keep the used space of the pool below 50% when using iSCSI. As required, you can increase the capacity of an existing extent using the instructions in [Growing LUNs](#).

To add an extent, go to Sharing → Block (iSCSI) → Extents → Add Extent . In the example shown in Figure 10.26, the device extent is using the export zvol that was previously created from the /mnt/volume1 volume.

Table 10.11 summarizes the settings that can be configured when creating an extent. Note that **file extent creation will fail if you do not append the name of the file to be created to the volume/dataset name.**

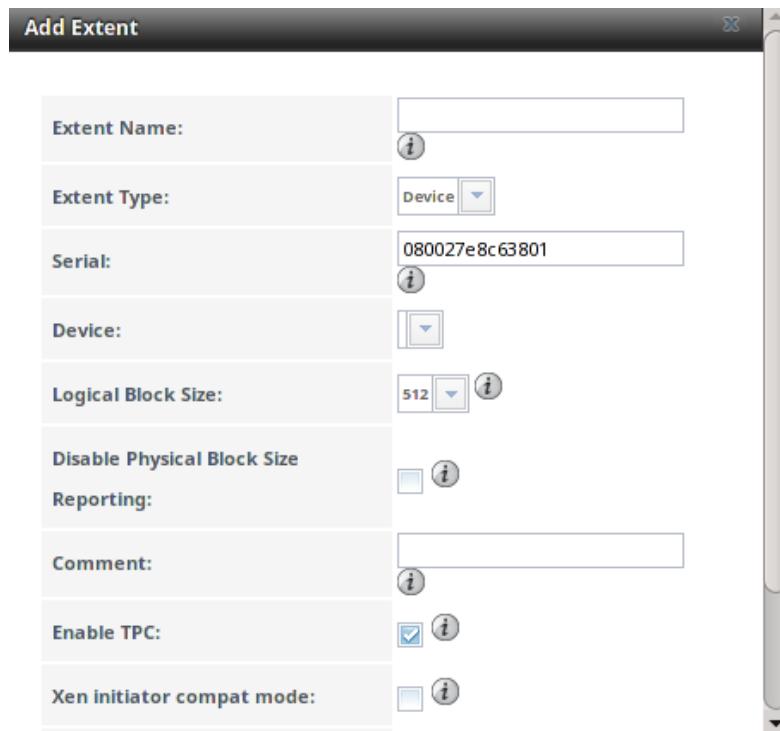


Fig. 10.26: Adding an iSCSI Extent

Table 10.11: Extent Configuration Settings

Setting	Value	Description
Extent Name	string	name of extent; if the <i>Extent size</i> is not <i>0</i> , it cannot be an existing file within the volume/dataset
Extent Type	drop-down menu	select from <i>File</i> or <i>Device</i>
Serial	string	unique LUN ID; the default is generated from the system's MAC address
Path to the extent	browse button	only appears if <i>File</i> is selected; either browse to an existing file and use <i>0</i> as the <i>Extent size</i> , or browse to the volume or dataset, click <i>Close</i> , append the <i>Extent Name</i> to the path, and specify a value in <i>Extent size</i>
Device	drop-down menu	only appears if <i>Device</i> is selected; select the unformatted disk, controller, zvol, zvol snapshot, or HAST device
Extent size	integer	only appears if <i>File</i> is selected; if the size is specified as <i>0</i> , the file must already exist and the actual file size will be used; otherwise, specify the size of the file to create
Logical Block Size	drop-down menu	only override the default if the initiator requires a different block size
Disable Physical Block Size Reporting	check-box	if the initiator does not support physical block size values over 4K (MS SQL), check this box
Available Space Threshold	string	only appears if <i>File</i> or a zvol is selected; when the specified percentage of free space is reached, the system will issue an alert
Comment	string	optional
Enable TPC	check-box	if checked, an initiator can bypass normal access control and access any scannable target; this allows xcopy operations otherwise blocked by access control
Xen initiator compat mode	check-box	check this box when using Xen as the iSCSI initiator
LUN RPM	drop-	do NOT change this setting when using Windows as the initiator; only needs to

10.5.7 Target/Extents

The last step is associating an extent to a target within Sharing → Block (iSCSI) → Associated Targets → Add Target/Extent. This screen is shown in [Figure 10.27](#). Use the drop-down menus to select the existing target and extent. Click *OK* to add an entry for the LUN.

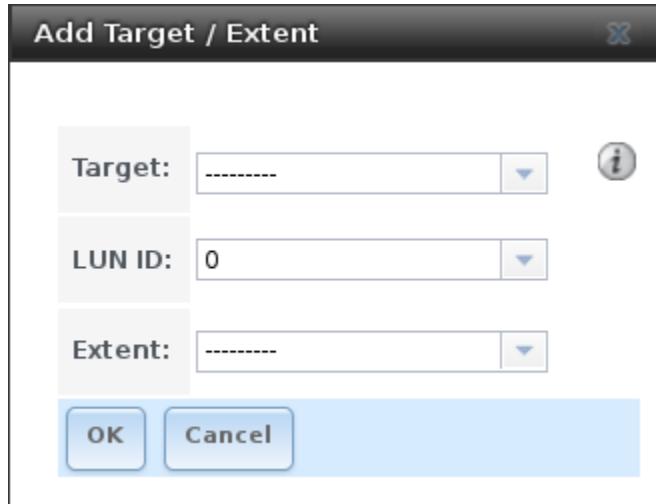


Fig. 10.27: Associating a Target With an Extent

Table 10.12 summarizes the settings that can be configured when associating targets and extents.

Table 10.12: Target/Extents Configuration Settings

Setting	Value	Description
Target	drop-down menu	select the pre-created target
LUN ID	drop-down menu	select the value of the ID or type in the desired value
Extent	drop-down menu	select the pre-created extent

It is recommended to always associate extents to targets in a one-to-one manner, even though the GUI will allow multiple extents to be associated with the same target.

Note: Each LUN entry has *Edit* and *Delete* buttons for modifying the settings or deleting the LUN entirely. A verification popup appears when the *Delete* button is clicked. If an initiator has an active connection to the LUN, it is indicated in red text. It is recommended to clear initiator connections to a LUN before deleting it.

After iSCSI has been configured, remember to start it in Services → Control Services. Click the red *OFF* button next to iSCSI. After a second or so, it will change to a blue *ON*, indicating that the service has started.

10.5.8 Connecting to iSCSI

In order to access the iSCSI target, 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](#). A client for Windows 2000, XP, and 2003 can be found [here](#). This [how-to](#) shows how to create an iSCSI target for a Windows 7 system.

Mac OS X does not include an initiator. [globalSAN](#) is a commercial, easy-to-use Mac initiator.

BSD systems provide command line initiators: `iscontrol(8)` comes with FreeBSD versions 9.x and lower, `iscsictl(8)` comes with FreeBSD versions 10.0 and higher, `iscsi-initiator(8)` comes with NetBSD, and `iscsid(8)` comes with OpenBSD.

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

If you add a LUN while `iscsiadm` is already connected, it will not see the new LUN until you rescan using `iscsiadm -m node -R`. Alternately, use `iscsiadm -m discovery -t st -p portal_IP` to find the new LUN and `iscsiadm -m node -T LUN_Name -l` to log into the LUN.

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.

If you can see the target but not connect to it, check the *Discovery Auth* settings in *Target Global Configuration*.

If the LUN is not discovered by ESXi, make sure that promiscuous mode is set to *Accept* in the vSwitch.

10.5.9 Growing LUNs

The method used to grow the size of an existing iSCSI LUN depends on whether the LUN is backed by a file extent or a zvol. Both methods are described in this section.

After the LUN is expanded using one of the methods below, use the tools from the initiator software to grow the partitions and the filesystems it contains.

Zvol Based LUN

To grow a zvol based LUN, go to *Storage* → *Volumes* → *View Volumes*, highlight the zvol to be grown, and click *Edit zvol*. In the example shown in [Figure 10.28](#), the current size of the zvol named `zvol1` is 4GB.

Enter the new size for the zvol in the *Size* field and click *Edit ZFS Volume*. This menu closes and the new size for the zvol is immediately shown in the *Used* column of the *View Volumes* screen.

Note: The GUI does not allow reducing (shrinking) the size of the zvol, as doing so could result in loss of data. It also does not allow increasing the size of the zvol past 80% of the volume size.

File Extent Based LUN

To grow a file extent based LUN, go to *Services* → *iSCSI* → *File Extents* → *View File Extents* to determine the path of the file extent to grow. Open Shell to grow the extent. This example grows `/mnt/volume1/data` by 2 G:

```
truncate -s +2g /mnt/volume1/data
```

Go back to *Services* → *iSCSI* → *File Extents* → *View File Extents* and click the *Edit* button for the file extent. Set the size to *0* as this causes the iSCSI target to use the new size of the file.

The screenshot shows the FreeNAS Storage interface. At the top, there's a navigation bar with tabs for Storage, Volumes (which is selected), Periodic Snapshot Tasks, Replication Tasks, Scrubs, Snapshots, and VMware-Snapshot. Below the navigation bar are several buttons: Volume Manager, Import Disk, Import Volume, View Disks, and View Enclosure. The main area displays a table of volumes:

Name	Used	Available	Compression	Compression Ratio	Status
volume1	7.1 MiB (0%)	49.7 GiB	-	-	HEALTHY
volume1	4.1 GiB (8%)	44.1 GiB	lz4	1.92x	-
zvol1	4.1 GiB (8%)	48.2 GiB	inherit (lz4)	1.00x	-

Below the table, an 'Edit zvol' dialog is open. It contains the following fields:

- Compression level:** Inherit (lz4) dropdown menu.
- ZFS Deduplication:** A note stating "Enabling dedup may have drastic performance implications, as well as impact your ability to access your data. Consider using compression instead." with an "Inherit (off)" dropdown below it.
- Size:** A text input field containing "4G" with an information icon (i) next to it.

At the bottom of the dialog are "Edit ZFS Volume" and "Cancel" buttons, along with two small icons.

Fig. 10.28: Editing an Existing Zvol

SERVICES CONFIGURATION

The Services section of the GUI is where various services that ship with the FreeNAS® system are configured, started, or stopped. FreeNAS® includes these built-in services:

- *AFP*
- *Domain Controller*
- *Dynamic DNS*
- *FTP*
- *iSCSI*
- *LLDP*
- *NFS*
- *Rsync*
- *S.M.A.R.T.*
- *SMB*
- *SNMP*
- *SSH*
- *TFTP*
- *UPS*
- *WebDAV*

This section demonstrates starting a FreeNAS® service and the available configuration options for each FreeNAS® service.

11.1 Control Services

Services → Control Services , shown in Figure 11.1, shows which services are currently running and can start, stop, or configure them. The S.M.A.R.T. service is enabled by default, but only runs if the storage devices support S.M.A.R.T. data. Other services default to off until started.

A service is stopped if its icon is a red *OFF*. A service is running if the icon is a blue *ON*. To start or stop a service, click the *ON/OFF* icon.

To configure a service, click the wrench icon associated with the service or click the name of the service in the *Services* section of the tree menu.

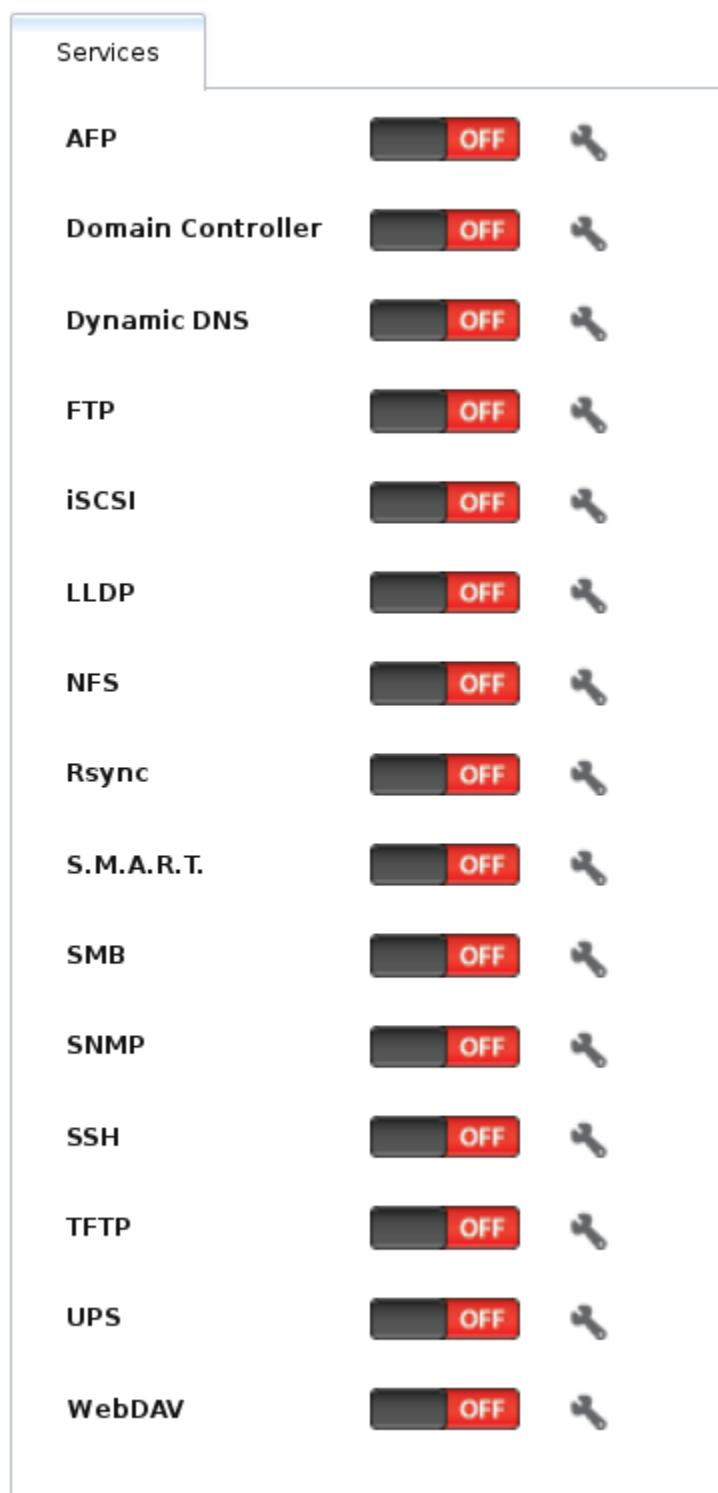


Fig. 11.1: Control Services

If a service does not start, go to System → Advanced and check the box *Show console messages in the footer*. Console messages will now show at the bottom of the browser. Clicking the console messages area will make it into a pop-up window, allowing scrolling through the output and copying messages. Watch these messages for errors when stopping or starting the problematic service.

To read the system logs for more information about a service failure, open *Shell* and type **more /var/log/messages**.

11.2 AFP

The settings that are configured when creating AFP Shares in Sharing → Apple (AFP) Shares → Add Apple (AFP) Share are specific to each configured AFP Share. In contrast, global settings which apply to all AFP shares are configured in Services → AFP .

Figure 11.2 shows the available global AFP configuration options which are described in Table 11.1.

Table 11.1: Global AFP Configuration Options

Setting	Value	Description
Guest Access	check-box	if checked, clients will not be prompted to authenticate before accessing AFP shares
Guest account	drop-down menu	select account to use for guest access; the selected account must have permissions to the volume or dataset being shared
Max Connections	integer	maximum number of simultaneous connections
Enable home directories	check-box	if checked, any user home directories located under <i>Home directories</i> will be available over the share
Home directories	browse button	select the volume or dataset which contains user home directories
Home share name	string	overrides default home folder name with the specified value
Database Path	browse button	select the path to store the CNID databases used by AFP (default is the root of the volume); the path must be writable
Global auxiliary parameters	string	additional <code>afp.conf(5)</code> parameters not covered elsewhere in this screen
Map ACLs	drop-down menu	choose mapping of effective permissions for authenticated users; <i>Rights</i> (default, Unix-style permissions), <i>Mode</i> (ACLs), or <i>None</i>
Bind IP Addresses	selection	specify the IP addresses to listen for FTP connections; highlight the desired IP addresses in the <i>Available</i> list and use the >> button to add to the <i>Selected</i> list

When configuring home directories, it is recommended to create a dataset to hold the home directories which contains a child dataset for each user. As an example, create a dataset named `volumel/homedirs` and browse to this dataset when configuring the *Home directories* field of the AFP service. Then, as you create each user, first create a child dataset for that user. For example, create a dataset named `volumel/homedirs/user1` . When you create the `user1` user, browse to the `volumel/homedirs/user1` dataset in the *Home Directory* field of the *Add New User* screen.

11.2.1 Troubleshooting AFP

You can determine which users are connected to an AFP share by typing `afpusers`.

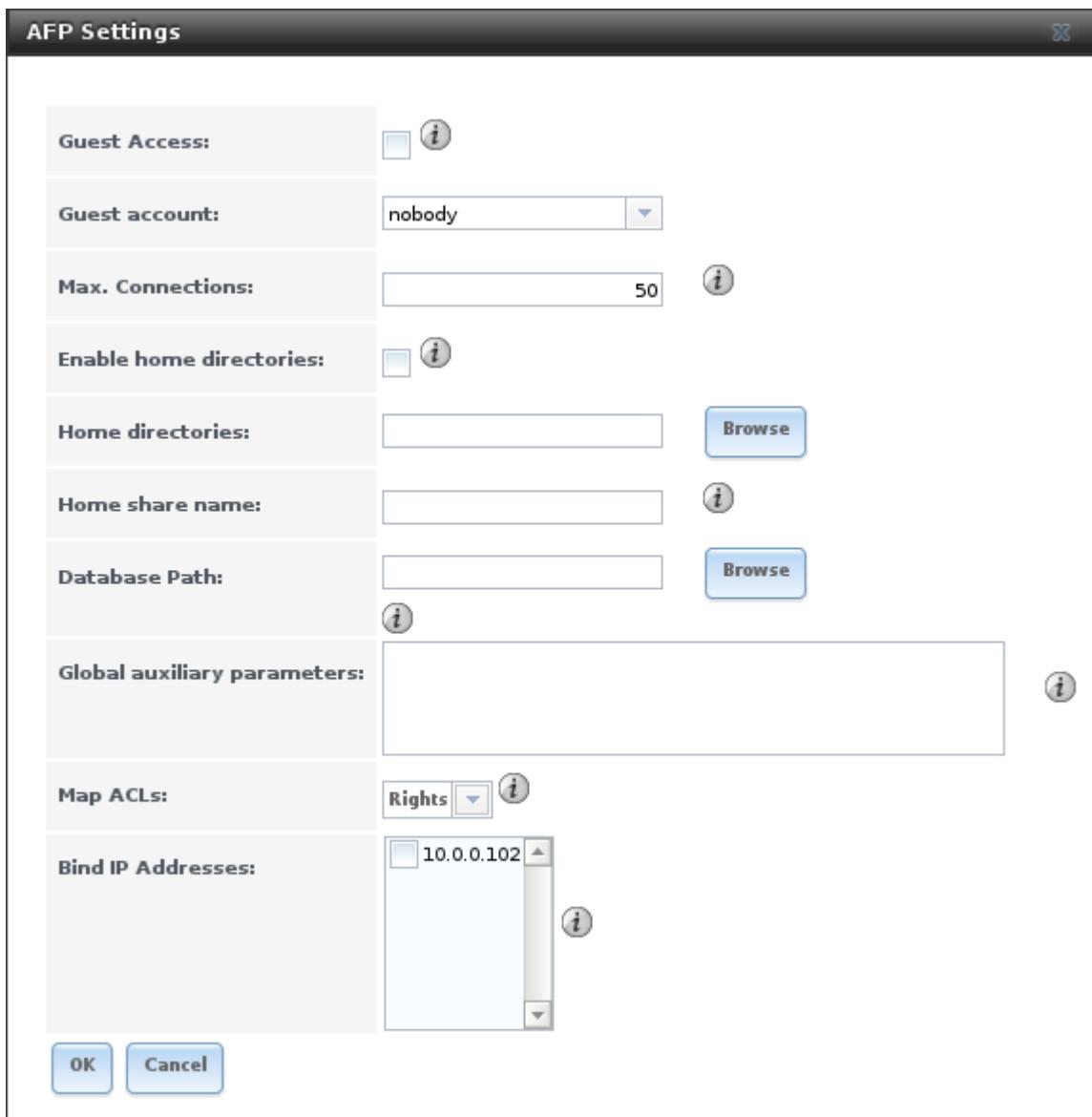


Fig. 11.2: Global AFP Configuration

If *Something wrong with the volume's CNID DB* is shown, run this command from [Shell](#), replacing the path to the problematic AFP share:

```
dbd -rf /path/to/share
```

This command may take a while, depending upon the size of the volume or dataset being shared. This command will wipe the CNID database and rebuild it from the CNIDs stored in the AppleDouble files.

11.3 Domain Controller

FreeNAS® can be configured to act either as the domain controller for a network or to join an existing [Active Directory](#) network as a domain controller.

Note: This section demonstrates how to configure the FreeNAS® system to act as a domain controller. If your goal is to integrate with an existing [Active Directory](#) network to access its authentication and authorization services, configure [Active Directory](#) instead.

Be aware that configuring a domain controller is a complex process that requires a good understanding of how [Active Directory](#) works. While Services → Domain Controller makes it easy to input the needed settings into the administrative graphical interface, it is up to you to understand what those settings should be. Before beginning your configuration, read through the [Samba AD DC HOWTO](#). After FreeNAS® is configured, use the RSAT utility from a Windows system to manage the domain controller. The Samba AD DC HOWTO includes instructions for installing and configuring RSAT.

Figure 11.3 shows the configuration screen for creating a domain controller and Table 11.2 summarizes the available options.

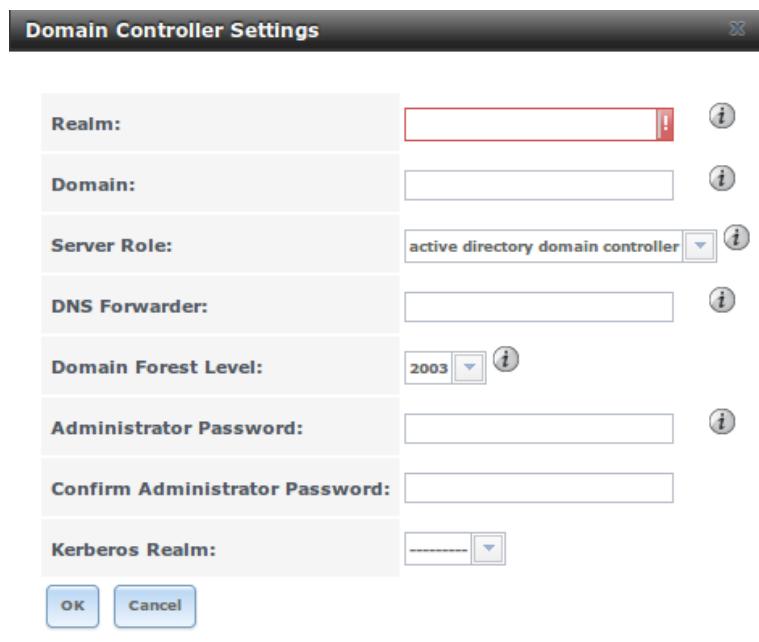


Fig. 11.3: Domain Controller Settings

Table 11.2: Domain Controller Configuration Options

Setting	Value	Description
Realm	string	capitalized DNS realm name
Domain	string	capitalized domain name
Server Role	drop-down menu	at this time, the only supported role is as the domain controller for a new domain
DNS Forwarder	string	IP address of DNS forwarder; required for recursive queries when <i>SAMBA_INTERNAL</i> is selected
Domain Forest Level	drop-down menu	choices are <i>2000</i> , <i>2003</i> , <i>2008</i> , or <i>2008_R2</i> ; refer to Understanding Active Directory Domain Services (AD DS) Functional Levels for details
Administrator password	string	password to be used for the <i>Active Directory</i> administrator account
Kerberos Realm	drop-down menu	this drop-down menu will auto-populate using the information from <i>Realm</i> when the settings in this screen are saved

11.4 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 11.4 shows the DDNS configuration screen and Table 11.3 summarizes the configuration options. The values to enter will be provided by the DDNS provider. After configuring DDNS, remember to start the DDNS service in *Services → Control Services*.

Table 11.3: DDNS Configuration Options

Setting	Value	Description
Provider	drop-down menu	several providers are supported; if your provider is not listed, leave this field blank and specify the custom provider in the <i>Auxiliary parameters</i> field
IP Server	string	can be used to specify the hostname and port of the IP check server
Domain name	string	fully qualified domain name (e.g. <i>yourname.dyndns.org</i>)
Username	string	username used 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	how often the IP is checked in seconds
Forced update period	integer	how often the IP should be updated, even if it has not changed, in seconds
Auxiliary parameters	string	additional parameters passed to the provider during record update; an example of specifying a custom provider is <i>dyndns_system default@provider.com</i>

If you are using “freedns.afraid.org”, see [this forum post](#) for an example working configuration.

If you are using “he.net”, input the domain name for *Username* and input the DDNS key generated for that domain’s A entry at the he.net website for *Password*.

The screenshot shows a configuration dialog titled "Dynamic DNS Settings". It includes the following fields:

- Provider:** A dropdown menu currently showing a placeholder value.
- IP Server:** An input field with an information icon.
- Domain name:** An input field with an information icon.
- Username:** An input field containing "admin".
- Password:** An input field.
- Confirm Password:** An input field.
- Update period:** An input field with an information icon.
- Forced update period:** An input field.
- Auxiliary parameters:** A large input field with an information icon.

At the bottom are "OK" and "Cancel" buttons.

Fig. 11.4: Configuring DDNS

11.5 FTP

FreeNAS® uses the `proftpd` FTP server to provide FTP services. Once the FTP service is configured and started, clients can browse and download data using a 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 Encrypting FTP.

This section provides an overview of the FTP configuration options. It then provides examples for configuring anonymous FTP, specified user access within a chroot environment, encrypting FTP connections, and troubleshooting tips.

Figure 11.5 shows the configuration screen for Services → FTP . Some settings are only available in *Advanced Mode*. To see these settings, either click the *Advanced Mode* button or configure the system to always display these settings by checking the box *Show advanced fields by default* in System → Advanced .

Table 11.4 summarizes the available options when configuring the FTP server.

Table 1

Setting	Value	Description
Port	integer	port the FTP service listens on
Clients	integer	maximum number of simultaneous clients
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 you have many failed logins
Timeout	integer	maximum client idle time in seconds before client is disconnected
Allow Root Login	checkbox	discouraged as increases security risk

Table 11.4

Setting	Value	Description
Allow Anonymous Login	checkbox	enables anonymous FTP logins with access to the directory specified in Path
Path	browse button	root directory for anonymous FTP connections
Allow Local User Login	checkbox	required if <i>Anonymous Login</i> is disabled
Display Login	string	message displayed to local login users after authentication; not displayed to anonymous users
File Permission	checkboxes	only available in <i>Advanced Mode</i> ; sets default permissions for newly created files
Directory Permission	checkboxes	only available in <i>Advanced Mode</i> ; sets default permissions for newly created directories
Enable FXP	checkbox	only available in <i>Advanced Mode</i> ; enables File eXchange Protocol which allows for faster transfers between two hosts
Allow Transfer Resumption	checkbox	allows FTP clients to resume interrupted transfers
Always Chroot	checkbox	a local user is only allowed access to their home directory unless the user has write permission to it
Require IDENT Authentication	checkbox	only available in <i>Advanced Mode</i> ; will result in timeouts if identd is not running
Perform Reverse DNS Lookups	checkbox	perform reverse DNS lookups on client IPs; can cause long delays if reverse lookups are enabled for many clients
Masquerade address	string	public IP address or hostname; set if FTP clients cannot connect through a firewall
Minimum passive port	integer	only available in <i>Advanced Mode</i> ; used by clients in PASV mode, default is 1024
Maximum passive port	integer	only available in <i>Advanced Mode</i> ; used by clients in PASV mode, default is 65295
Local user upload bandwidth	integer	only available in <i>Advanced Mode</i> ; in KB/s, default of 0 means unlimited
Local user download bandwidth	integer	only available in <i>Advanced Mode</i> ; in KB/s, default of 0 means unlimited
Anonymous user upload bandwidth	integer	only available in <i>Advanced Mode</i> ; in KB/s, default of 0 means unlimited
Anonymous user download bandwidth	integer	only available in <i>Advanced Mode</i> ; in KB/s, default of 0 means unlimited
Enable TLS	checkbox	only available in <i>Advanced Mode</i> ; enables encrypted connections and requires a certificate
TLS policy	drop-down menu	only available in <i>Advanced Mode</i> ; the selected policy defines whether the server supports TLS 1.0, 1.1, or 1.2
TLS allow client renegotiations	checkbox	only available in <i>Advanced Mode</i> ; checking this box is not recommended
TLS allow dot login	checkbox	only available in <i>Advanced Mode</i> ; if checked, the user's home directory is the current working directory
TLS allow per user	checkbox	only available in <i>Advanced Mode</i> ; if checked, the user's password may be required for each connection
TLS common name required	checkbox	only available in <i>Advanced Mode</i> ; if checked, the common name in the certificate must match the host name
TLS enable diagnostics	checkbox	only available in <i>Advanced Mode</i> ; if checked when troubleshooting a connection, provides detailed information about the connection
TLS export certificate data	checkbox	only available in <i>Advanced Mode</i> ; if checked, exports the certificate envelope to a file
TLS no certificate request	checkbox	only available in <i>Advanced Mode</i> ; try checking this box if the client cannot verify the server's certificate
TLS no empty fragments	checkbox	only available in <i>Advanced Mode</i> ; checking this box is not recommended
TLS no session reuse required	checkbox	only available in <i>Advanced Mode</i> ; checking this box reduces the security risk of session reuse attacks
TLS export standard vars	checkbox	only available in <i>Advanced Mode</i> ; if checked, sets several environment variables for the client
TLS DNS name required	checkbox	only available in <i>Advanced Mode</i> ; if checked, the client's DNS name must match the common name in the certificate
TLS IP address required	checkbox	only available in <i>Advanced Mode</i> ; if checked, the client's certificate must contain the IP address of the client
Certificate	drop-down menu	the SSL certificate to be used for TLS FTP connections; to create a certificate, see Chapter 11, Services Configuration
Auxiliary parameters	string	only available in <i>Advanced Mode</i> ; used to add proftpd(8) parameters not listed in the table

This example demonstrates the auxiliary parameters that prevent all users from performing the FTP DELETE command:

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

11.5.1 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 it is not necessary to manage changed passwords on the FreeNAS® system.

To configure anonymous FTP:

The screenshot shows the 'FTP Settings' configuration window. At the top, there is a navigation bar with tabs: Services, Plugins, Tasks, Reporting, and Missed. Below the title 'FTP Settings', there is a list of configuration options:

Port:	21	i
Clients:	5	i
Connections:	2	i
Login Attempts:	1	i
Timeout:	600	i
Allow Root Login:	<input type="checkbox"/>	
Allow Anonymous Login:	<input type="checkbox"/>	
Path:	<input type="text"/>	Browse
Allow Local User Login:	<input type="checkbox"/>	
Display Login:	<input type="text"/>	i
Allow Transfer Resumption:	<input type="checkbox"/>	

Fig. 11.5: Configuring FTP

- Give the built-in ftp user account permissions to the volume/dataset to be shared in Storage → Volumes as follows:

- Owner(user)*: select the built-in *ftp* user from the drop-down menu
- Owner(group)*: select the built-in *ftp* group from the drop-down menu
- Mode*: review that the permissions are appropriate for the share

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.

- Configure anonymous FTP in Services → FTP by setting the following attributes:

- check the box *Allow Anonymous Login*
- Path*: browse to the volume/dataset/directory to be shared

- Start the FTP service in Services → 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.

- Test the connection from a client using a utility such as [Filezilla](#).

In the example shown in Figure 11.6, the user has entered the following information into the Filezilla client:

- IP address of the FreeNAS® server: 192.168.1.113
- Username*: anonymous
- Password*: the email address of the user

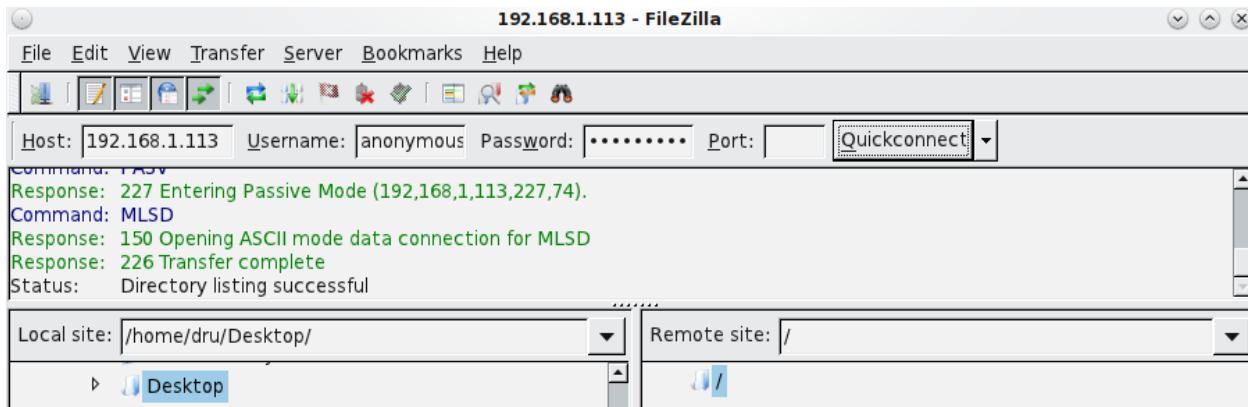


Fig. 11.6: Connecting Using Filezilla

The messages within the client indicate that the FTP connection is successful. The user can now navigate the contents of the root folder on the remote site—this is the volume/dataset that was specified in the FTP service configuration. The user can also transfer files between the local site (their system) and the remote site (the FreeNAS® system).

11.5.2 FTP in chroot

If you require your users to authenticate before accessing the data on the FreeNAS® system, you will need to either create a user account for each user or import existing user accounts using [Active Directory](#) or LDAP. If you then 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. Datasets provide the added benefit of configuring a quota so that the size of the user's home directory is limited to the size of the quota.

To configure this scenario:

1. Create a ZFS dataset for each user in Storage → Volumes . Click an existing ZFS volume → Create ZFS Dataset and set an appropriate quota for each dataset. Repeat this process to create a dataset for every user that needs access to the FTP service.
2. If you are not using AD or LDAP, create a user account for each user in Account → Users → Add User . For each user, browse to the dataset created for that user in the *Home Directory* field. Repeat this process to create a user account for every user that needs access to the FTP service, making sure to assign each user their own dataset.
3. Set the permissions for each dataset in Storage → Volumes . Click the *Change Permissions* button for a dataset to assign a user account as *Owner* of that dataset and to set the desired permissions for that user. Repeat for each dataset.

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.

4. Configure FTP in Services → FTP with these attributes:
 - *Path*: browse to the parent volume containing the datasets
 - 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 Services → 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.

To test this configuration in Filezilla, 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. The messages should indicate that the authorization and the FTP connection are successful. The user can now navigate the contents of the root folder on the remote site—this time it is not the entire volume but the dataset that was created for that user. The user should be able to transfer files between the local site (their system) and the remote site (their dataset on the FreeNAS® system).

11.5.3 Encrypting FTP

To configure any FTP scenario to use encrypted connections:

1. Import or create a certificate authority using the instructions in [CAs](#). Then, import or create the certificate to use for encrypted connections using the instructions in [Certificates](#).
2. In Services → FTP , check the box *Enable TLS* and select the certificate in the *Certificate* drop-down menu.
3. 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 a user connects, they will be presented with the certificate of the FreeNAS® system. Click *OK* to accept the certificate and negotiate an encrypted connection.
4. To force encrypted connections, select *on* for the *TLS Policy*.

11.5.4 Troubleshooting FTP

The FTP service will not start if it cannot resolve the system's hostname to an IP address using DNS. To see if the FTP service is running, open [Shell](#) and issue the command:

```
sockstat -4p 21
```

If there is nothing listening on port 21, the FTP service is not running. To see the error message that occurs when FreeNAS® tries to start the FTP service, go to System → Advanced, check the box *Show console messages in the footer* and click *Save*. Next, go to Services → Control Services and switch the FTP service off, then back on. Watch the console messages at the bottom of the browser for errors.

If the error refers to DNS, either create an entry in the local DNS server with the FreeNAS® system's hostname and IP address or add an entry for the IP address of the FreeNAS® system in the *Host name database* field of Network → Global Configuration .

11.6 iSCSI

Refer to [Block \(iSCSI\)](#) for instructions on configuring iSCSI. To start the iSCSI service, click its entry in *Services*.

Note: A warning message is shown if you stop the iSCSI service when initiators are connected. Type **ctladm islist** to determine the names of the connected initiators.

11.7 LLDP

The Link Layer Discovery Protocol (LLDP) is used by network devices to advertise their identity, capabilities, and neighbors on an Ethernet network. FreeNAS® uses the `ladvd` LLDP implementation. If your network contains managed switches, configuring and starting the LLDP service will tell the FreeNAS® system to advertise itself on the network.

Figure 11.7 shows the LLDP configuration screen and Table 11.5 summarizes the configuration options for the LLDP service.

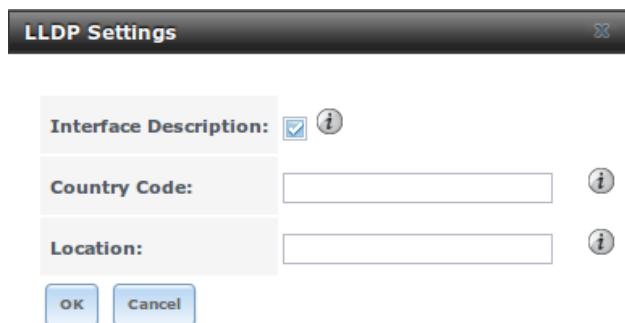


Fig. 11.7: Configuring LLDP

Table 11.5: LLDP Configuration Options

Setting	Value	Description
Interface Description	checkbox	when checked, receive mode is enabled and received peer information is saved in interface descriptions
Country Code	string	required for LLDP location support; input 2 letter ISO 3166 country code
Location	string	optional; specify the physical location of the host

11.8 NFS

The settings that are configured when creating NFS Shares in Sharing → Unix (NFS) Shares → Add Unix (NFS) Share are specific to each configured NFS Share. In contrast, global settings which apply to all NFS shares are configured in Services → NFS.

Figure 11.8 shows the configuration screen and Table 11.6 summarizes the configuration options for the NFS service.

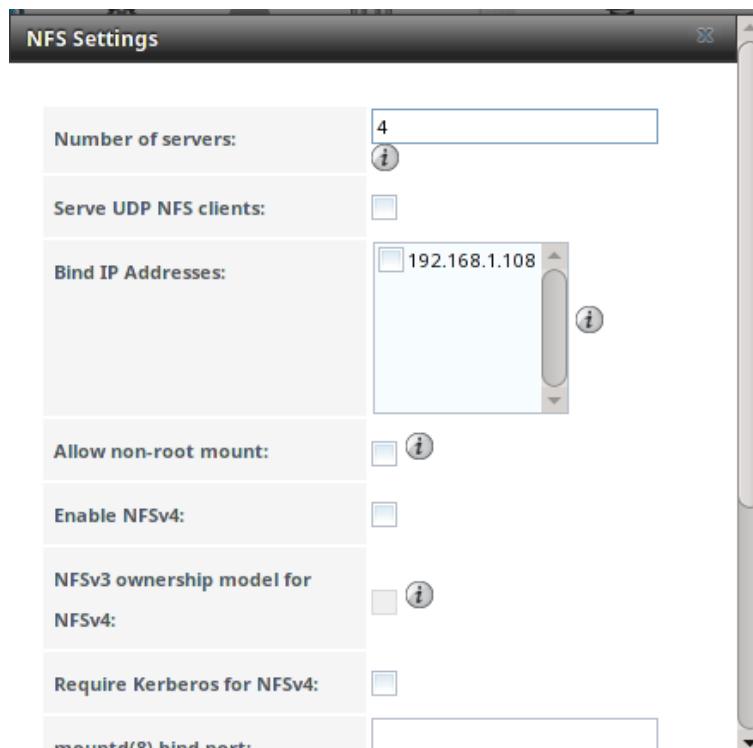


Fig. 11.8: Configuring NFS

Table 11.6: NFS Configuration Options

Setting	Value	Description
Number of servers	integer	run <code>sysctl -n kern.smp.cpus</code> from Shell to determine the number; do not exceed the number listed in the output of that command
Serve UDP NFS clients	checkbox	check if NFS client needs to use UDP
Bind IP Addresses	checkboxes	select the IP address(es) to listen for NFS requests; if left unchecked, NFS will listen on all available addresses
Allow non-root mount	checkbox	check this box only if the NFS client requires it
Enable NFSv4	checkbox	the default is to use NFSv3, check this box to switch to NFSv4
NFSv3 ownership model for NFSv4	checkbox	grayed out unless <i>Enable NFSv4</i> is checked and, in turn, will gray out <i>Support>16 groups</i> which is incompatible; check this box if NFSv4 ACL support is needed without requiring the client and the server to sync users and groups
Require Kerberos for NFSv4	checkbox	when checked, NFS shares will fail if the Kerberos ticket is unavailable
mountd(8) bind port	integer	optional; specify port for <code>mountd(8)</code> to bind to
rpc.statd(8) bind port	integer	optional; specify port for <code>rpc.statd(8)</code> to bind to
rpc.lockd(8) bind port	integer	optional; specify port for <code>rpc.lockd(8)</code> to bind to
Support>16 groups	checkbox	check this box if any users are members of more than 16 groups (useful in AD environments); note that this assumes that group membership has been configured correctly on the NFS server

11.9 Rsync

Services → Rsync is used to configure an rsync server when using rsync module mode. See the section on Rsync Module Mode for a configuration example.

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

11.9.1 Configure Rsynacd

Figure 11.9 shows the rsynacd configuration screen which is accessed from Services → Rsync → Configure Rsynacd .

Table 11.7 summarizes the options that can be configured for the rsync daemon:

Table 11.7: Rsynacd Configuration Options

Setting	Value	Description
TCP Port	integer	port for <code>rsynacd</code> to listen on, default is 873
Auxiliary parameters	string	additional parameters from <code>rsynacd.conf(5)</code>



Fig. 11.9: Rsyncd Configuration

11.9.2 Rsync Modules

Figure 11.10 shows the configuration screen that appears after clicking Services → Rsync → Rsync Modules → Add Rsync Module.

Table 11.8 summarizes the options that can be configured when creating a rsync module.

The screenshot shows the "Add Rsync Module" dialog. It includes fields for "Module name", "Comment", "Path" (with a "Browse" button), "Access Mode" (set to "Read and Write"), "Maximum connections" (set to 0), "User" (set to "nobody"), "Group" (set to "nobody"), "Hosts allow", and "Hosts deny". Each field has an "info" icon (i) next to it. A vertical scroll bar is visible on the right side of the dialog.

Fig. 11.10: Adding an Rsync Module

Table 11.8: Rsync Module Configuration Options

Setting	Value	Description
Module name	string	mandatory; needs to match the setting on the rsync client
Comment	string	optional description
Path	browse button	volume/dataset to hold received data
Access Mode	drop-down menu	choices are <i>Read and Write</i> , <i>Read-only</i> , or <i>Write-only</i>
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 rsyncd.conf(5) for allowed formats
Hosts deny	string	see rsyncd.conf(5) for allowed formats
Auxiliary parameters	string	additional parameters from rsyncd.conf(5)

11.10 S.M.A.R.T.

FreeNAS® uses the [smartd\(8\)](#) service to monitor disk S.M.A.R.T. data for disk health. To fully configure S.M.A.R.T. you need to:

1. Schedule when to run the S.M.A.R.T. tests in Tasks → S.M.A.R.T. Tests → Add S.M.A.R.T. Test .
2. Enable or disable S.M.A.R.T. for each disk member of a volume in Volumes → View Volumes . By default, this is already enabled on all disks that support S.M.A.R.T.
3. Check the configuration of the S.M.A.R.T. service as described in this section.
4. Start the S.M.A.R.T. service in Services → Control Services .

Figure 11.11 shows the configuration screen that appears after clicking Services → S.M.A.R.T.

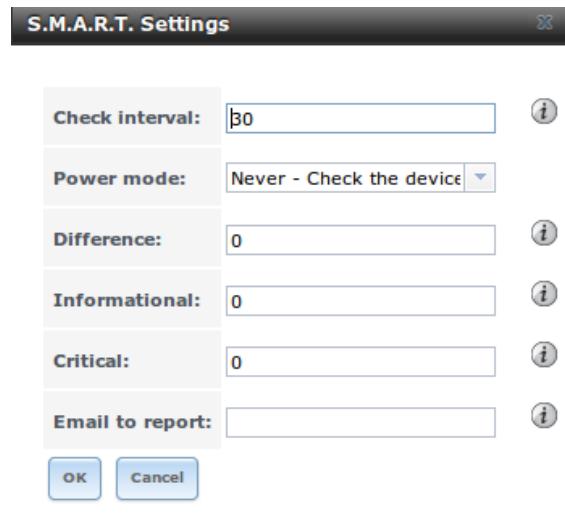


Fig. 11.11: S.M.A.R.T Configuration Options

Note: `smartd` wakes up at every configured *Check Interval*. It checks the times configured in Tasks → S.M.A.R.T. Tests to see if any tests should be run. Since the smallest time increment for a test is an hour (60 minutes), it does not make sense to set a *Check Interval* value higher than 60 minutes. For example, if the *Check Interval* is set to 120 minutes and the smart test to every hour, the test will only be run every two hours because the daemon only wakes up every two hours.

Table 11.9 summarizes the options in the S.M.A.R.T configuration screen.

Table 11.9: S.M.A.R.T Configuration Options

Setting	Value	Description
Check interval	integer	in minutes, how often to wake up <code>smartd</code> to check to see if any tests have been configured to run
Power mode	drop-down menu	the configured test is not performed if the system enters the specified power mode; choices are: <i>Never</i> , <i>Sleep</i> , <i>Standby</i> , or <i>Idle</i>
Difference	integer in degrees Celsius	default of 0 disables this check, otherwise reports if the temperature of a drive has changed by N degrees Celsius since last report
Informational	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 specified degrees in 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 specified degrees in Celsius
Email to report	string	email address of person or alias to receive S.M.A.R.T. alerts

11.11 SMB

The settings that are configured when creating SMB Shares in Sharing → Windows (SMB) Shares → Add Windows (SMB) Share are specific to each configured SMB Share. In contrast, global settings which apply to all SMB shares are configured in Services → SMB .

Note: After starting the SMB service, it may take several minutes for the master browser election to occur and for the FreeNAS® system to become available in Windows Explorer.

Figure 11.12 shows the global SMB configuration options which are described in Table 11.10. This configuration screen is really a front-end to `smb4.conf`.

SMB Settings

NetBIOS name:	freenas
NetBIOS alias:	
Workgroup:	WORKGROUP i
Description:	FreeNAS Server i
DOS charset:	CP437 ▼
UNIX charset:	UTF-8 ▼
Log level:	Minimum ▼
Use syslog only:	<input type="checkbox"/>
Local Master:	<input checked="" type="checkbox"/>
Domain logons:	<input type="checkbox"/>
Time Server for Domain:	<input checked="" type="checkbox"/>
Guest account:	nobody ▼ i
File mask:	
Directory mask:	
Allow Empty Password:	<input type="checkbox"/>
Auxiliary parameters:	
Unix Extensions:	<input checked="" type="checkbox"/> i
Zeroconf share discovery:	<input checked="" type="checkbox"/> i
Hostnames lookups:	<input checked="" type="checkbox"/> i
Server minimum protocol:	----- ▼ i

Fig. 11.12: Global SMB Configuration

Table 11.10: Global SMB Configuration Options

Setting	Value	Description
NetBIOS Name	string	automatically populated with the system's original hostname; limited to 15 characters; it must be different from the <i>Workgroup</i> name
Workgroup	string	must match Windows workgroup name; this setting is ignored if the <i>Active Directory</i> or <i>LDAP</i> service is running
Description	string	optional
DOS charset	drop-down menu	the character set Samba uses when communicating with DOS and Windows 9x/ME clients; default is <i>CP437</i>
UNIX charset	drop-down menu	default is <i>UTF-8</i> which supports all characters in all languages
Log level	drop-down menu	choices are <i>Minimum</i> , <i>Normal</i> , or <i>Debug</i>
Use syslog only	check-box	when checked, authentication failures are logged to <code>/var/log/messages</code> instead of the default of <code>/var/log/samba4/log.smbd</code>
Local Master	check-box	determines whether or not the system participates in a browser election; should be disabled when network contains an AD or LDAP server and is not necessary if Vista or Windows 7 machines are present
Domain logons	check-box	only check if need to provide the netlogin service for older Windows clients
Time Server for Domain	check-box	determines whether or not the system advertises itself as a time server to Windows clients; should be disabled when network contains an AD or LDAP server
Guest Account	drop-down menu	account to be used for guest access; that account must have permission to access the shared volume/dataset
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
Allow Empty Password	check-box	if checked, users can just press <code>Enter</code> when prompted for a password; requires that the username/password be the same as the Windows user account
Auxiliary parameters	string	<code>smb.conf</code> options not covered elsewhere in this screen; see the Samba Guide for additional settings
Unix Extensions	check-box	allows non-Windows SMB clients to access symbolic links and hard links, has no effect on Windows clients
Zeroconf share discovery	check-box	enable if Mac clients will be connecting to the SMB share
Hostnames lookups	check-box	allows you to specify hostnames rather than IP addresses in the <i>Hosts Allow</i> or <i>Hosts Deny</i> fields of a SMB share; uncheck if IP addresses are used to avoid the delay of a host lookup
Server minimum protocol	drop-down menu	the minimum protocol version the server will support where the default sets automatic negotiation; refer to Table 11.11 for descriptions
Server maximum protocol	drop-down menu	the maximum protocol version the server will support; refer to Table 11.11 for descriptions
Allow execute	check-box	if checked, Samba will allow the user to execute a file, even if that user's permissions are not set to execute
Obey pam restrictions	check-box	uncheck this box to allow cross-domain authentication, to allow users and groups to be managed on another forest, or to allow permissions to be delegated from <i>Active Directory</i> users and groups to domain admins on another forest
Bind IP	check-	check the IP addresses on which SMB should listen

Table 11.11: SMB Protocol Versions

Value	Description
CORE	used by DOS
COREPLUS	used by DOS
LANMAN1	used by Windows for Workgroups, OS/2, and Windows 9x
LANMAN2	used by Windows for Workgroups, OS/2, and Windows 9x
NT1	used by Windows NT
SMB2	used by Windows 7; same as SMB2_10
SMB2_02	used by Windows Vista
SMB2_10	used by Windows 7
SMB3	used by Windows 8
SMB3_00	used by Windows 8
SMB3_02	used by Windows 8.1 and Windows Server 2012
SMB3_11	used by Windows 10

Changes to SMB settings and SMB shares take effect immediately.

Note: Do not set the *directory name cache size* as an *Auxiliary parameter*. Due to differences in how Linux and BSD handle file descriptors, directory name caching is disabled on BSD systems to improve performance.

Note: *SMB* cannot be disabled while *Active Directory* is enabled.

11.11.1 Troubleshooting SMB

Samba is single threaded, so CPU speed makes a big difference in SMB performance. A typical 2.5Ghz Intel quad core or greater should be capable of handling speeds in excess of Gb LAN while low power CPUs such as Intel Atoms and AMD C-30sE-350E-450 will not be able to achieve more than about 30-40MB/sec typically. Remember that other loads such as ZFS will also require CPU resources and may cause Samba performance to be less than optimal.

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 SMB share or to the permissions of a volume/dataset being shared by SMB and are no longer able to access the share, try logging out and back into the Windows system. Alternately, users can type **net use /delete** from the command line to clear their SMB sessions.

Windows also automatically caches login information. If you want users to be prompted to log in every time access is required, reduce the cache settings on the client computers.

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

If a particular user cannot connect to a SMB share, make sure that their password does not contain the ? character. If it does, have the user change the password and try again.

If permissions work for Windows users but not for OS X users, try disabling *Unix Extensions* and restarting the SMB service.

If the SMB service will not start, run this command from [Shell](#) to see if there is an error in the configuration:

```
testparm /usr/local/etc/smb4.conf
```

If clients have problems connecting to the SMB share, go to Services → SMB and verify that *Server maximum protocol* is set to *SMB2*.

It is recommended to use a dataset for SMB sharing. When creating the dataset, make sure that the *Share type* is set to Windows.

Do not use **chmod** to attempt to fix the permissions on a SMB share as it destroys the Windows ACLs. The correct way to manage permissions on a SMB share is to manage the share security from a Windows system as either the owner of the share or a member of the group that owns the share. To do so, right-click on the share, click *Properties* and navigate to the *Security* tab. If you already destroyed the ACLs using **chmod**, **winacl** can be used to fix them. Type **winacl** from [Shell](#) for usage instructions.

The [Common Errors](#) section of the Samba documentation contains additional troubleshooting tips.

11.12 SNMP

SNMP (Simple Network Management Protocol) is used to monitor network-attached devices for conditions that warrant administrative attention. FreeNAS® uses [Net-SNMP](#) to provide SNMP. When you start the SNMP service, the following port will be enabled on the FreeNAS® system:

- UDP 161 (listens here for SNMP requests)

Available MIBS are located in `/usr/local/share/snmp/mibs`.

Figure 11.13 shows the SNMP configuration screen. Table 11.12 summarizes the configuration options.

SNMP Settings

Location:	<input type="text"/>	i
Contact:	<input type="text"/>	i
SNMP v3 Support:	<input checked="" type="checkbox"/>	
Community:	<input type="text" value="public"/>	i
Username:	<input type="text"/>	
Authentication Type:	<input type="radio"/> SHA <input checked="" type="radio"/>	
Password:	<input type="password"/>	
Confirm Password:	<input type="password"/>	
Privacy Protocol:	<input type="radio"/> ----- <input checked="" type="radio"/>	
Privacy Passphrase:	<input type="text"/>	
Confirm Privacy Passphrase:	<input type="text"/>	
Auxiliary parameters:		

Fig. 11.13: Configuring SNMP

Table 11.12: SNMP Configuration Options

Setting	Value	Description
Location	string	optional description of system's location
Contact	string	optional email address of administrator
SNMP v3 Support	check-box	check this box to enable support for SNMP version 3
Community	string	default is public and should be changed for security reasons ; can only contain alphanumeric characters, underscores, dashes, periods, and spaces; this value can be empty for SNMPv3 networks
Username	string	only applies if <i>SNMP v3 Support</i> is checked; specify the username to register with this service; refer to snmpd.conf(5) for more information regarding the configuration of this setting as well as the <i>Authentication Type</i> , <i>Password</i> , <i>Privacy Protocol</i> , and “Privacy Passphrase” fields
Authentication Type	drop-down menu	only applies if <i>SNMP v3 Support</i> is checked; choices are <i>MD5</i> or <i>SHA</i>
Password	string	only applies if <i>SNMP v3 Support</i> is checked; specify and confirm a password of at least eight characters
Privacy Protocol	drop-down menu	only applies if <i>SNMP v3 Support</i> is checked; choices are <i>AES</i> or <i>DES</i>
Privacy Passphrase	string	if not specified, <i>Password</i> is used
Auxiliary Parameters	string	additional snmpd.conf(5) options not covered in this screen, one per line

11.13 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](#) to transfer files with SSH.

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 11.14 shows the Services → SSH configuration screen. After configuring SSH, remember to start it in Services → Control Services.

Table 11.13 summarizes the configuration options. Some settings are only available in *Advanced Mode*. To see these settings, either click the *Advanced Mode* button, or configure the system to always display these settings by checking the box *Show advanced fields by default* in System → Advanced .

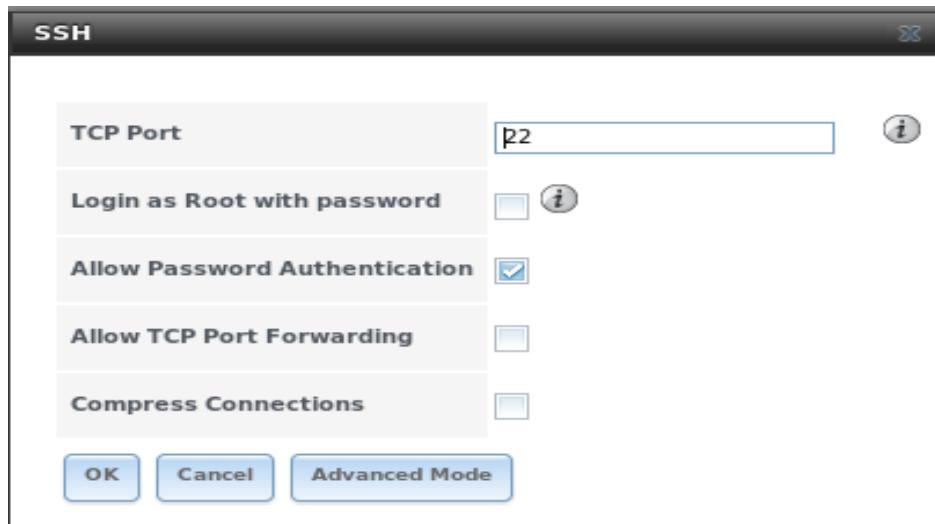


Fig. 11.14: SSH Configuration

Table 11.13: SSH Configuration Options

Setting	Value	Description
Bind Interfaces	selection	only available in <i>Advanced Mode</i> ; by default, SSH listens on all interfaces unless specific interfaces are highlighted in the <i>Available</i> field and added to the <i>Selected</i> field
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 if enabled, password must be set for <i>root</i> user in <i>View Users</i>
Allow Password Authentication	checkbox	if unchecked, key based authentication for all users is required; requires additional setup on both the SSH client and server
Allow Kerberos Authentication	checkbox	before checking this box, ensure that <i>Kerberos Realms</i> and <i>Kerberos Keytabs</i> have been configured and that the FreeNAS system can communicate with the KDC
Allow TCP Port Forwarding	checkbox	allows users to bypass firewall restrictions using SSH's port forwarding feature
Compress Connections	checkbox	may reduce latency over slow networks
SFTP Log Level	dropdown menu	only available in <i>Advanced Mode</i> ; select the syslog(3) level of the SFTP server
SFTP Log Facility	dropdown menu	only available in <i>Advanced Mode</i> ; select the syslog(3) facility of the SFTP server
Extra Options	string	only available in <i>Advanced Mode</i> ; additional sshd_config(5) options not covered in this screen, one per line; these options are case-sensitive and misspellings may prevent the SSH service from starting

A few [sshd_config\(5\)](#) options that are useful to enter in the *Extra Options* field include:

- increase the *ClientAliveInterval* if SSH connections tend to drop
- *ClientMaxStartup* defaults to 10; increase this value if you need more concurrent SSH connections

11.13.1 SCP Only

When you configure SSH, authenticated users with a user account created using Account → Users → Add User can use the **ssh** command to login to the FreeNAS® system over the network. A user's home directory will be the volume/dataset specified in the *Home Directory* field of their FreeNAS® user account. While the SSH login will default to the user's home directory, users are able to navigate outside of their home directory, which can pose a security risk.

It is possible to allow users to use the **scp** and **sftp** commands to transfer files between their local computer and their home directory on the FreeNAS® system, while restricting them from logging into the system using **ssh**. To configure this scenario, go to Account → Users → View Users, select the user and click *Modify User*, and change the user's *Shell* to *scponly*. Repeat for each user that needs restricted SSH access.

Test the configuration from another system by running the **sftp**, **ssh**, and **scp** commands as the user. The **sftp** and **scp** commands should work but the **ssh** should fail.

Note: Some utilities such as WinSCP and Filezilla can bypass the scponly shell. This section assumes that users are accessing the system using the command line versions of **scp** and **sftp**.

11.13.2 Troubleshooting SSH

When adding any *Extra Options*, 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 do not match the upper and lowercase letters of the keyword.

If your clients are receiving “reverse DNS” or timeout errors, add an entry for the IP address of the FreeNAS® system in the *Host name database* field of Network → Global Configuration .

When configuring SSH, always test your configuration as an SSH user account to ensure that the user is limited to what you have configured and that they have permission to transfer files within the intended directories. If the user account is experiencing problems, the SSH error messages are usually pretty specific to what the problem is. Type the following command within *Shell* to read these messages as they occur:

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

Additional messages regarding authentication errors may be found in `/var/log/auth.log` .

11.14 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 provides an extremely limited set of commands and provides no authentication.

If the FreeNAS® system will be used to store images and configuration files for the network's devices, configure and start the TFTP service. Starting the TFTP service will open UDP port 69.

Figure 11.15 shows the TFTP configuration screen and Table 11.14 summarizes the available options:

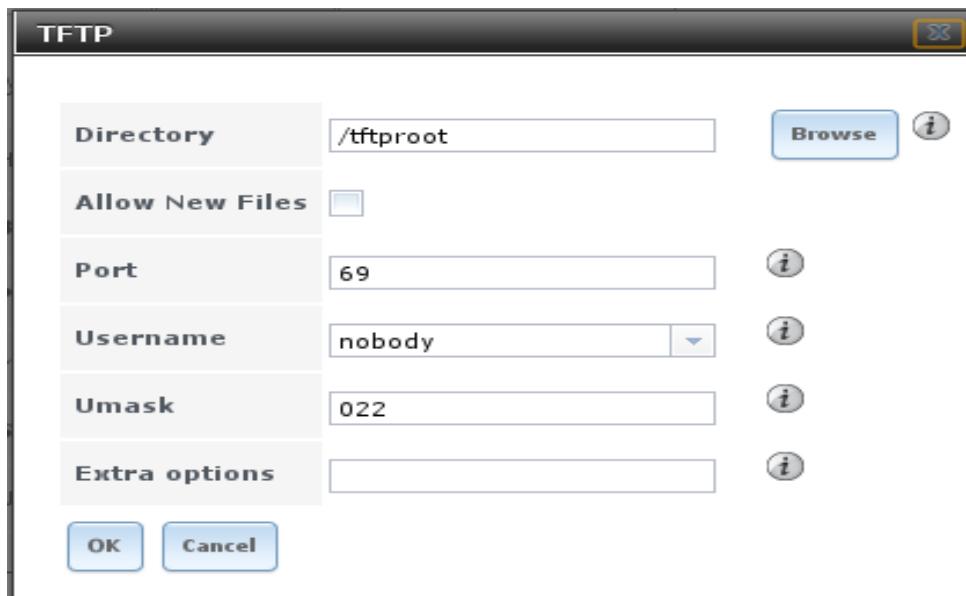


Fig. 11.15: TFTP Configuration

Table 11.14: TFTP Configuration Options

Setting	Value	Description
Directory	browse button	browse to an existing directory to be used for storage; some devices require a specific directory name, refer to the device's documentation for details
Allow New Files	checkbox	enable if network devices need to send files to the system (e.g. backup their config)
Port	integer	UDP port to listen for TFTP requests, 69 by default
User-name	drop-down menu	account used for tftp requests; must have permission to the <i>Directory</i>
Umask	integer	umask for newly created files, default is 022 (everyone can read, nobody can write); some devices require a less strict umask
Extra options	string	additional tftpd(8) options not shown in this screen, one per line

11.15 UPS

FreeNAS® uses [NUT](#) (Network UPS Tools) to provide UPS support. If the FreeNAS® system is connected to a UPS device, configure the UPS service then start it in [Services → Control Services](#).

Figure 11.16 shows the UPS configuration screen:

Table 11.15 summarizes the options in the UPS Configuration screen.

UPS Settings

UPS Mode:	<input type="button" value="Master"/>
Identifier:	<input type="text" value="ups"/> (i)
Driver:	<input type="text" value="-----"/> (i)
Port:	<input type="text"/> (i)
Auxiliary parameters (ups.conf):	
Auxiliary parameters (upsd.conf):	
Description:	<input type="text"/>
Shutdown mode:	<input type="button" value="UPS goes on battery"/>
Shutdown timer:	<input type="text" value="30"/> (i)
Shutdown Command:	<input type="text" value="/sbin/shutdown -p now"/> (i)
Monitor User:	<input type="text" value="upsmon"/>
Monitor Password:	<input type="text" value="fixmepass"/>
Extra users (upsd.users):	
Remote Monitor:	<input type="checkbox"/>
Send Email Status Updates:	<input type="checkbox"/>
To email:	<input type="text"/> (i)
Email Subject:	<input type="text" value="UPS report generated by %t"/> (i)
Power Off UPS:	<input type="checkbox"/> (i)

OK **Cancel**

Fig. 11.16: UPS Configuration Screen

Table 11.15: UPS Configuration Options

Setting	Value	Description
UPS Mode	drop-down menu	select from <i>Master</i> or <i>Slave</i>
Identifier	string	can contain alphanumeric, period, comma, hyphen, and underscore characters
Driver	drop-down menu	supported UPS devices are listed at http://www.networkupstools.org/stable-hcl.html
Port	drop-down menu	select the serial or USB port the UPS is plugged into (see NOTE below)
Auxiliary Parameters (ups.conf)	string	additional options from ups.conf(5)
Auxiliary Parameters (upsd.conf)	string	additional options from upsd.conf(5)
Description	string	optional
Shutdown mode	drop-down menu	choices are <i>UPS goes on battery</i> and <i>UPS reaches low battery</i>
Shutdown timer	integer	in seconds; will initiate shutdown after this many seconds after UPS enters <i>UPS goes on battery</i> , unless power is restored
Shutdown Command	string	the command to run to shut down the computer when battery power is low or shutdown timer runs out
Monitor User	string	default is <i>upsmon</i>
Monitor Password	string	default is known value <i>fixmepass</i> and should be changed; cannot contain a space or #
Extra users	string	defines the accounts that have administrative access; see upsd.users(5) for examples
Remote monitor	checkbox	if enabled, be aware that the default is to listen on all interfaces and to use the known values user <i>upsmon</i> and password <i>fixmepass</i>
Send Email Status Updates	checkbox	if checked, activates the <i>To email</i> field
To email	email address	if <i>Send Email</i> box checked, email address to receive status updates; separate multiple email addresses with a semicolon
Email Subject	string	subject line to be used in the email
Power Off UPS	checkbox	if checked, the UPS will also power off after shutting down the FreeNAS system

Note: For USB devices, the easiest way to determine the correct device name is to check the box *Show console messages* in System → Advanced. Plug in the USB device and console messages show the name of the */dev/ugenX.X* device, where the X's are the numbers that show on the console.

[upsc\(8\)](#) can be used to get status variables from the UPS daemon such as the current charge and input voltage. It can be run from Shell using the following syntax. The man page gives some other usage examples.

```
upsc ups@localhost
```

[upscmd\(8\)](#) can be used to send commands directly to the UPS, assuming that the hardware supports the command being sent. Only users with administrative rights can use this command. These users are created in the *Extra users*

field.

11.16 WebDAV

The WebDAV service can be configured to provide a file browser over a web connection. Before starting this service, you must create at least one WebDAV share using *Sharing* → *WebDAV Shares* → *Add WebDAV Share*. Refer to [WebDAV Shares](#) for instructions on how to create a share and then how to connect to it once the service is configured and started.

The settings in the WebDAV service apply to all WebDAV shares. Figure 11.17 shows the WebDAV configuration screen. Table 11.16 summarizes the available options.

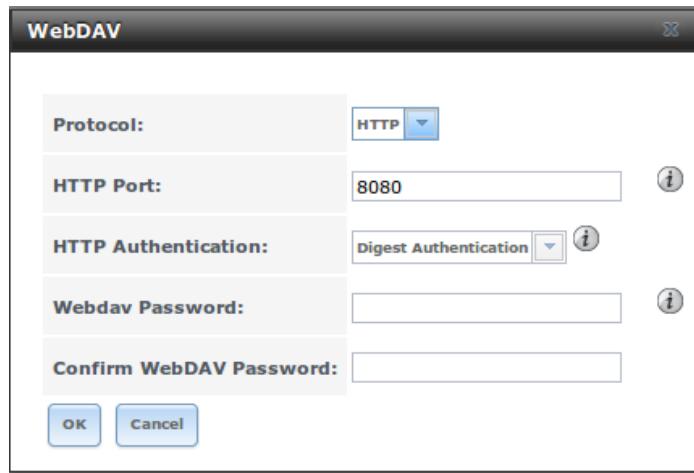


Fig. 11.17: WebDAV Configuration Screen

Table 11.16: WebDAV Configuration Options

Setting	Value	Description
Protocol	drop-down menu	choices are <i>HTTP</i> (connection always unencrypted), <i>HTTPS</i> (connection always encrypted), or <i>HTTP+HTTPS</i> (both types of connections allowed)
HTTP Port	string	only appears if the selected <i>Protocol</i> is <i>HTTP</i> or <i>HTTP+HTTPS</i> and is used to specify the port to be used for unencrypted connections; the default of 8080 should work, if you change it, do not use a port number already being used by another service
HTTPS Port	string	only appears if the selected <i>Protocol</i> is <i>HTTPS</i> or <i>HTTP+HTTPS</i> and is used to specify the port to be used for encrypted connections; the default of 8081 should work, if you change it, do not use a port number already being used by another service
Webdav SSL Certificate	drop-down menu	only appears if the selected <i>Protocol</i> is <i>HTTPS</i> or <i>HTTP+HTTPS</i> ; select the SSL certificate to be used for encrypted connections; to create a certificate, use <i>System</i> → <i>Certificates</i>
HTTP Authentication	drop-down menu	choices are <i>Basic Authentication</i> (unencrypted) or <i>Digest Authentication</i> (encrypted)
Webdav Password	string	default is <i>davtest</i> ; this should be changed as it is a known value

PLUGINS

FreeNAS® 8.2.0 introduced the ability to extend the built-in NAS services by providing a mechanism for installing additional software. This mechanism was known as the Plugins architecture and is based on FreeBSD jails and PC-BSD 9.x PBIs. This allowed users to install and configure additional applications once they had created and configured a plugins jail.

FreeNAS® 9.x simplifies this procedure by providing two methods for software installation. The Plugins method, described in this section, is meant for users who prefer to browse for, install, and configure available software using the GUI. This method is very easy to use, but is limited in the amount of software that is available. Each application will automatically be installed into its own jail, meaning that this method may not be suitable for users who wish to run multiple applications within the same jail.

The Jails method provides much more control over software installation but assumes that the user is comfortable working from the command line can and has a good understanding of networking basics and software installation on FreeBSD-based systems.

It is recommended that users skim through both the *Plugins* and *Jails* sections in order to become familiar with the features and limitations of each and to choose the method that best meets their software needs.

Note: Due to ABI (application binary interface) changes, FreeNAS® 8.x Plugins cannot be installed on a 9.x system.

12.1 Installing Plugins

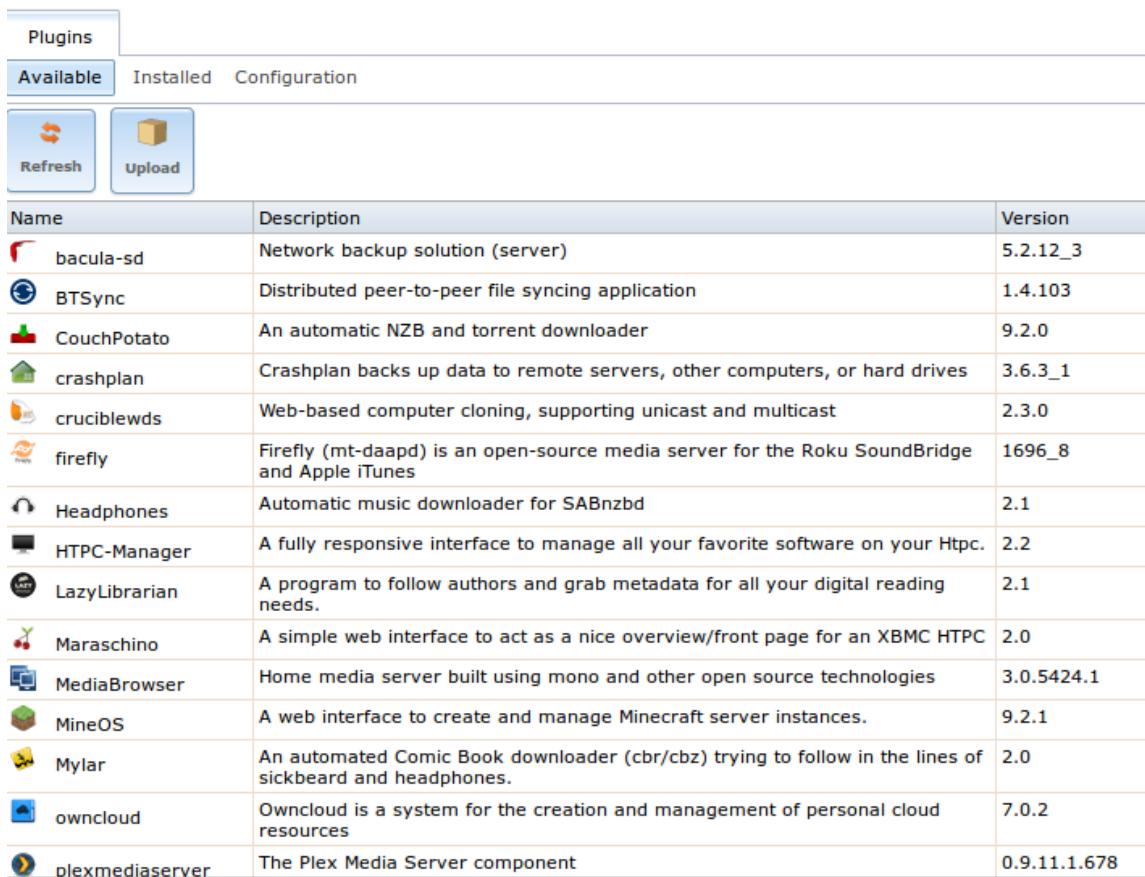
A plugin is a self-contained application installer which has been designed to integrate into the FreeNAS® GUI. A plugin offers several advantages:

- the FreeNAS® GUI provides a browser for viewing the list of available plugins
- the FreeNAS® GUI provides buttons for installing, starting, managing, and deleting plugins
- if the plugin has configuration options, a screen will be added to the FreeNAS® GUI so that these options can be configured from the GUI

To install a plugin, click *Plugins*. As seen in Figure 12.1, the list of available plugins will be displayed.

Note: if the list of available plugins is not displayed, open *Shell* and verify that the FreeNAS® system can **ping** an address on the Internet. If it cannot, you may have to add a default gateway address and/or DNS server address in *Network → Global Configuration*.

Highlight the plugin you would like to install, click its *Install* button, then click *OK*. In the example shown in Figure 12.2, SABnzbd is selected for installation.



The screenshot shows the 'Plugins' section of the FreeNAS web interface. At the top, there are tabs for 'Available', 'Installed', and 'Configuration'. Below the tabs are two buttons: 'Refresh' (with a circular arrow icon) and 'Upload' (with a folder icon). The main area is a table with columns for Name, Description, and Version. The table lists 16 available plugins:

Name	Description	Version
bacula-sd	Network backup solution (server)	5.2.12_3
BTSync	Distributed peer-to-peer file syncing application	1.4.103
CouchPotato	An automatic NZB and torrent downloader	9.2.0
crashplan	Crashplan backs up data to remote servers, other computers, or hard drives	3.6.3_1
cruciblewds	Web-based computer cloning, supporting unicast and multicast	2.3.0
firefly	Firefly (mt-daapd) is an open-source media server for the Roku SoundBridge and Apple iTunes	1696_8
Headphones	Automatic music downloader for SABnzbd	2.1
HTPC-Manager	A fully responsive interface to manage all your favorite software on your Htpc.	2.2
LazyLibrarian	A program to follow authors and grab metadata for all your digital reading needs.	2.1
Maraschino	A simple web interface to act as a nice overview/front page for an XBMC HTPC	2.0
MediaBrowser	Home media server built using mono and other open source technologies	3.0.5424.1
MineOS	A web interface to create and manage Minecraft server instances.	9.2.1
Mylar	An automated Comic Book downloader (cbr/cbz) trying to follow in the lines of sickbeard and headphones.	2.0
owncloud	Owncloud is a system for the creation and management of personal cloud resources	7.0.2
plexmediaserver	The Plex Media Server component	0.9.11.1.678

Fig. 12.1: Viewing the List of Available Plugins

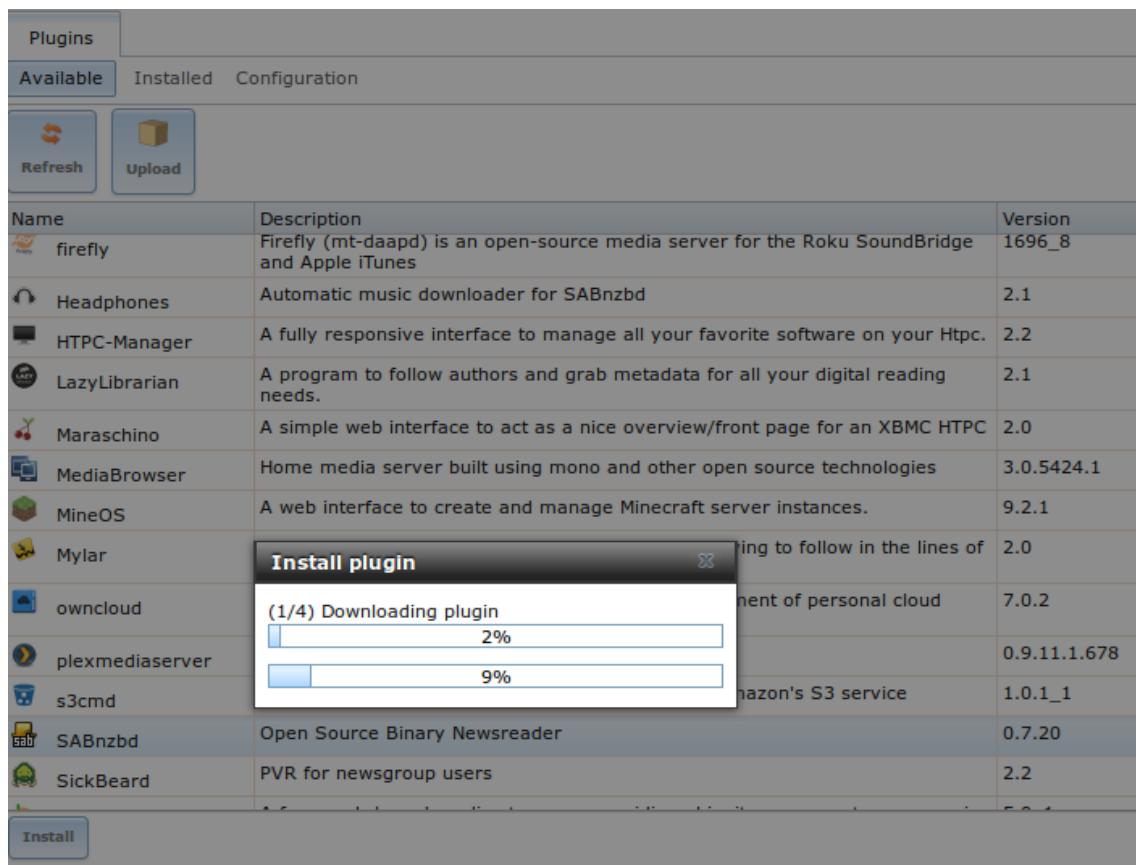


Fig. 12.2: Installing a Plugin

The installation will take a few minutes as the system will first download and configure a jail to contain the installed software. It will then install the plugin and add it to the *Installed* tab as shown in [Figure 12.3](#).

Warning: Be patient and wait for the installation to finish. Navigating away from the installation before it is finished will cause problems with the installation.

Plugin name	Version	PBI	Jail	Service status	Actions
Sabnzbd	0.7.18	sabnzbd-0.7.18-amd64	sabnzbd_1	<input type="button" value="OFF"/>	<input type="button" value="Delete"/>

Fig. 12.3: Viewing Installed PBIs

As seen in the example shown in [Figure 12.3](#), entries for the installed PBI will appear in the following locations:

- the *Installed* tab of *Plugins*
- the *Plugins* section of the tree
- the *Jails* section of the tree

The entry in the *Installed* tab of *Plugins* will display the plugin name and version, the name of the PBI that was installed, the name of the jail that was created, whether the application status is *ON* or *OFF*, and a button to delete the application and its associated jail. If a newer version of the application is available as a plugin, a button to update the application will also appear.

Note: The *Service status* of a plugin must be turned to *ON* before the installed application is available. Before starting the service, check to see if it has a configuration menu by clicking its entry in the *Plugins* section of the tree. If the application is configurable, this will open a screen that contains the available configuration options. Plugins which are not configurable will instead display a message with a hyperlink for accessing the software. However, that hyperlink does **not** work until the plugin is started.

Always review a plugin's configuration options before attempting to start it. Some plugins have options that need to be set before their service will successfully start. If you have never configured that application before, check the

application's website to see what documentation is available. A link to the website for each available plugin can be found in [Available Plugins](#).

If the application requires access to the data stored on the FreeNAS® system, click the entry for the associated jail in the *Jails* section of the tree and add a storage as described in [Add Storage](#).

If you need to access the shell of the jail containing the application to complete or test your configuration, click the entry for the associated jail in the *Jails* section of the tree. You can then click its “shell” icon as described in [Managing Jails](#).

Once the configuration is complete, click the red *OFF* button for the entry for the plugin. If the service starts successfully, it will change to a blue *ON*. If it fails to start, click the jail’s *Shell* icon and type `tail /var/log/messages` to see if any errors were logged.

12.2 Updating Plugins

When a newer version of a plugin becomes available in the official repository, an *Update* button is added to the entry for the plugin in the *Installed* tab. In the example shown in [Figure 12.4](#), a newer version of Transmission is available.

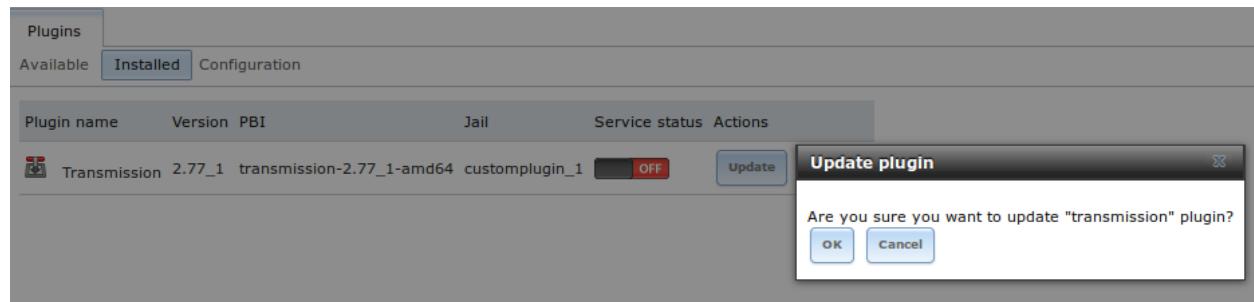


Fig. 12.4: Updating an Installed Plugin

Click the *OK* button to start the download and installation of the latest version of the plugin. Once the update is complete, the entry for the plugin will be refreshed to show the new version number and the *Update* button will disappear.

12.3 Uploading Plugins

The *Available* tab of *Plugins* contains an *Upload* button. This button allows installation of plugins that are not yet available in the official repository or which are still being tested. These plugins must be manually downloaded and should end in a `.pbi` extension. When downloading a plugin, make sure that it is 64-bit and that it was developed for 9.x as 8.x and 10.x applications will not work on a 9.x FreeNAS® system.

Upload the new plugin with the *Upload* button. As seen in the example in [Figure 12.5](#), this prompts you to browse to the location of the plugin file. Select the file and click *Upload* to begin the installation.

When the installation is complete, an entry for the plugin will be added to the *Installed* tab and its associated jail is listed under *Jails*. However, if it is not a FreeNAS® plugin, it will not be added to *Plugins* in the tree. In this case, any required jail configuration must be done from the command line of the jail’s shell instead of from the GUI.

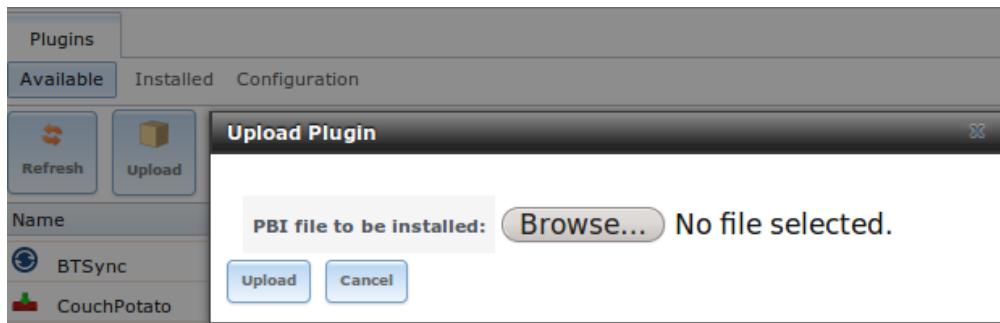


Fig. 12.5: Installing a Previously Downloaded .pbi File

12.4 Deleting Plugins

When you install a plugin, an associated jail is created. If you decide to delete a plugin, the associated jail is also deleted as it is no longer required. **Before deleting a plugin**, make sure that you do not have any data or configuration in the jail that you need to save. If you do, back up that data first, **before** deleting the plugin.

In the example shown in Figure 12.6, Sabnzbd has been installed and the user has clicked its *Delete* button. A pop-up message asks the user if they are sure that they want to delete. **This is the one and only warning**. If the user clicks *Yes*, the plugin and the associated jail are permanently deleted.

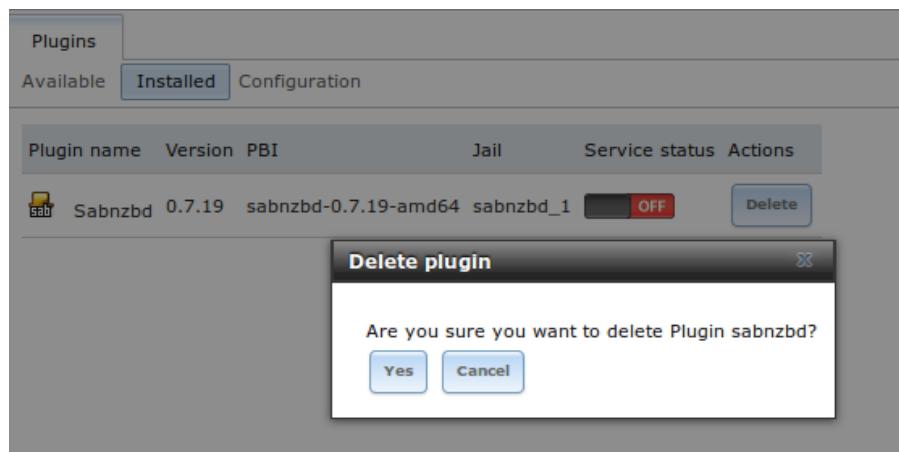


Fig. 12.6: Deleting an Installed Plugin

12.5 Available Plugins

These plugins are available for FreeNAS® 9.10.1-U2:

- bacula-sd (storage daemon)
- BTSync
- CloneDeploy
- CouchPotato
- crashplan

- Emby
- firefly
- Headphones
- HTPC-Manager
- LazyLibrarian
- Maraschino
- MineOS
- Mylar
- owncloud
- PlexMediaServer
- s3cmd
- SABnzbd
- SickBeard
- SickRage
- Sonarr
- Subsonic
- Syncthing
- Transmission
- XDM

While the FreeNAS® Plugins system makes it easy to install software, it is still up to you to know how to configure and use the installed application. When in doubt, refer to the documentation for that application.

CHAPTER
THIRTEEN

JAILS

The previous section described how to find, install, and configure software using *Plugins*.

This section describes how to use Jails, which allow users who are comfortable with the command line to have more control over software installation and management. Any software installed using Jails must be managed from the command line of the jail. If you prefer to use a GUI to manage software, use *Plugins* instead.

FreeNAS® automatically creates a jail whenever a plugin is installed, but does not let the user install multiple plugins into the same jail. In contrast, using Jails allows users to create as many jails as needed and to customize the operating system and installed software within each jail.

In FreeNAS® 9.x, two types of jails are supported:

1. By default, a [FreeBSD jail](#) is created. This provides a very light-weight, operating system-level virtualization. Consider it as another independent instance of FreeBSD running on the same hardware, without all of the overhead usually associated with virtualization. The jail will install the FreeBSD software management utilities so FreeBSD ports can be compiled and FreeBSD packages can be installed from the command line of the jail.
2. A Virtualbox template is also provided. This template installs an instance of [phpVirtualBox](#), a web-based front-end to [VirtualBox](#). This can then be used to install any operating system and to use the software management tools provided by that operating system.

It is important to understand that any users, groups, installed software, and configurations within a jail are isolated from both the FreeNAS® operating system and any other jails running on that system. During creation, the *VIMAGE* option can be selected which will also provide that jail with its own, independent networking stack. This allows that jail to do its own IP broadcasting, which is required by some applications.

Advanced users can also create custom templates to automate the creation of pre-installed and customized operating systems.

The ability to create multiple jails running different operating systems offers great flexibility regarding software management. For example, the administrator can choose to provide application separation by installing different applications in each jail, or to create one jail for all installed applications, or to mix and match how software is installed into each jail.

The rest of this section describes:

- [Jails Configuration](#)
- [Adding Jails](#)
- [Using the phpVirtualBox Template](#)
- [Managing Jail Templates](#)

13.1 Jails Configuration

Jails are stored in a volume or dataset. **Using a separate dataset for the Jail Root is strongly recommended.** The volume or dataset to be used must already exist or can be created with [Volume Manager](#).

Note: The *Jail Root* volume or dataset cannot be created on a [Share](#).

Begin global jail configuration by choosing *Jails* → *Configuration* to open the screen shown in [Figure 13.1](#). Jails are automatically installed into their own dataset under the specified path as they are created. For example, if the *Jail Root* is set to `/mnt/volume1/dataset1` and a jail named *jail1* is created, it is installed into its own dataset named `/mnt/volume1/dataset1/jail1`.

The screenshot shows a configuration interface for jails. At the top, there are two tabs: 'Jails' and 'Configuration'. The 'Configuration' tab is active. Below the tabs, there are three main configuration sections: 'Jail Root' (with a 'Browse' button), 'IPv4 DHCP' (with a checkbox), and 'IPv6 Autoconfigure' (with a checkbox). At the bottom of the configuration area are two buttons: 'Save' and 'Advanced Mode'.

Fig. 13.1: Global Jail Configuration

Warning: If any *Plugins* have already been installed, the *Jail Root*, *IPv4 Network*, *IPv4 Network Start Address*, and *IPv4 Network End Address* are automatically filled. Double-check that the pre-configured IP address values are appropriate for the jails and do not conflict with addresses used by other systems on the network.

[Table 13.1](#) summarizes the fields in this configuration screen. Refer to the text below the table for more details on how to properly configure the *Jail Root* and network settings. Some settings are only available in *Advanced Mode*. To see these settings, either click the *Advanced Mode* button or configure the system to always display these settings by checking the box *Show advanced fields by default* in *System* → *Advanced*.

Table 13.1: Jail Configuration Options

Setting	Value	Description
Jail Root	browse button	mandatory; jails cannot be added until this is set
IPv4 DHCP	check-box	check this box if the network has a DHCP server
IPv4 Network	string	only available in <i>Advanced Mode</i> ; format is IP address of <i>network/CIDR mask</i>
IPv4 Network Start Address	string	only available in <i>Advanced Mode</i> ; enter the first IP address in the reserved range in the format <i>host/CIDR mask</i>
IPv4 Network End Address	string	only available in <i>Advanced Mode</i> ; enter the last IP address in the reserved range in the format <i>host/CIDR mask</i>
IPv6 Autoconfigure	check-box	check this box if the network has a DHCPv6 server and IPv6 will be used to access jails
IPv6 Network	string	only available in <i>Advanced Mode</i> ; enter the network address for a properly configured IPv6 network
IPv6 Network Start Address	string	only available in <i>Advanced Mode</i> ; enter the first IP address in the reserved range for a properly configured IPv6 network
IPv6 Network End Address	string	only available in <i>Advanced Mode</i> ; enter the last IP address in the reserved range for a properly configured IPv6 network
Collection URL	string	only available in <i>Advanced Mode</i> ; changing the default may break the ability to install jails

When selecting the *Jail Root*, ensure that the size of the selected volume or dataset is sufficient to hold the number of jails to be installed as well as any software, log files, and data to be stored within each jail. At a bare minimum, budget at least 2 GB per jail and do not select a dataset that is less than 2 GB in size.

Note: If you plan to add storage to a jail, be aware that the path size is limited to 88 characters. Make sure that the length of the volume name plus the dataset name plus the jail name does not exceed this limit.

If the network contains a DHCP server, it is recommended to check the box *IPv4 DHCP* (or *IPv6 Autoconfigure*, for a properly configured IPv6 network). This will prevent IP address conflicts on the network as the DHCP server will automatically assign the jail the next available lease and record the lease as in use.

If a static IP address is needed so that users always know the IP address of the jail, enter the start and end address for the IPv4 and/or IPv6 network. The range defined by the start and end addresses will be automatically assigned as jails are created. For example, if you plan to create 5 jails on the 192.168.1.0 network, enter a *IPv4 Network Start Address* of 192.168.1.100 and a *IPv4 Network End Address* of 192.168.1.104.

If you create a start and end range on a network that contains a DHCP server, it is very important that you also reserve those addresses on the DHCP server. Otherwise, the DHCP server will not be aware that those addresses are being used by jails and there will be IP address conflicts and weird networking errors on the network. When troubleshooting jails that do not install or which are unavailable, double-check that the IP address being used by the jail is not also being used by another jail or system in the network.

FreeNAS® will automatically detect and display the *IPv4 Network* to which the administrative interface is connected. This setting is important. The IP addresses used by the jails must be pingable from the FreeNAS® system for the jails and any installed software to be accessible. If the network topology requires changing the default value, a default gateway and possibly a static route need to be added to the specified network. After changing this value, ensure that the subnet mask value is correct, as an incorrect mask can make the IP network unreachable. When in doubt, keep the default setting for *IPv4 Network*. With VMware, make sure that the vswitch is set to “promiscuous mode”.

After clicking the *Save* button to save the configuration, the system is ready to create and manage jails as described in the rest of this chapter.

13.2 Adding Jails

To create a jail, click `Jails` → `Add Jail` to access the screen shown in Figure 13.2.

Note: the `Add Jail` menu item will not appear until after you configure `Jails` → `Configuration`.

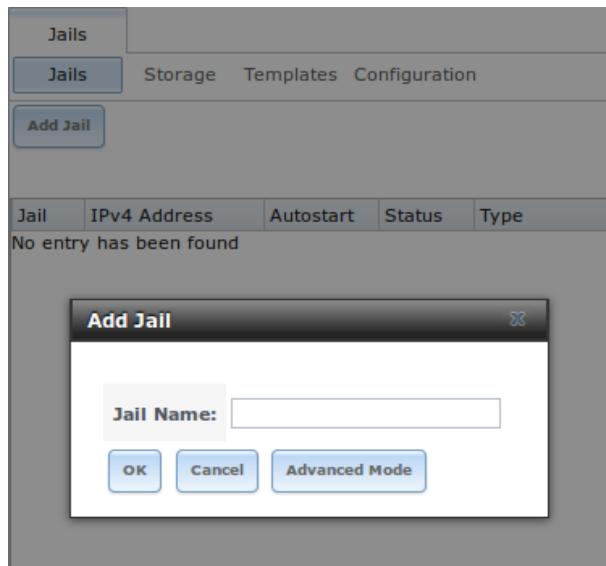


Fig. 13.2: Creating a Jail

By default, the only required value to create a jail is a name. FreeBSD jails are created by default.

Table 13.2 summarizes the available options. Most settings are only available in *Advanced Mode* and are not needed if the intent is to create a FreeBSD jail. To see these settings, either click the *Advanced Mode* button or configure the system to always display these settings by checking the box *Show advanced fields by default* in `System` → `Advanced`.

Table 13.2: Jail Configuration Options

Setting	Value	Description
Jail Name	string	mandatory; can only contain letters, numbers, dashes, or the underscore character
Template	drop-down menu	only available in <i>Advanced Mode</i> ; contains the <i>VirtualBox</i> template for creating an instance of phpVirtualBox; advanced users can create and install custom templates as described in Managing Jail Templates
IPv4 DHCP	check-box	only available in <i>Advanced Mode</i> ; if unchecked, make sure that the defined address does not conflict with the DHCP server's pool of available addresses
IPv4 address	integer	only available in <i>Advanced Mode</i> ; this and the other IPv4 settings will be grayed out if <i>IPv4 DHCP</i> is checked; input IP address that is reachable within the local network and is not in use by any other host in the network
IPv4 netmask	drop-down menu	only available in <i>Advanced Mode</i> ; select the subnet mask associated with <i>IPv4 address</i>
IPv4 bridge address	integer	only available in <i>Advanced Mode</i> and will be grayed out if <i>VIMAGE</i> is unchecked; see NOTE below
IPv4 bridge netmask	drop-down menu	only available in <i>Advanced Mode</i> ; select the subnet mask associated with <i>IPv4 bridge address</i> ; will be grayed out if <i>VIMAGE</i> is unchecked
IPv4 default gateway	string	only available in <i>Advanced Mode</i> ; will be grayed out if <i>VIMAGE</i> is unchecked
IPv6 Auto-configure	check-box	only available in <i>Advanced Mode</i> ; if unchecked, make sure that the defined address does not conflict with the DHCP server's pool of available addresses
IPv6 address	integer	only available in <i>Advanced Mode</i> ; this and the other IPv6 settings will be grayed out if <i>IPv6 Autoconfigure</i> is checked; input IPv6 address that is reachable within the local network and is not in use by any other host in the network
IPv6 prefix length	drop-down menu	only available in <i>Advanced Mode</i> ; select the prefix length associated with <i>IPv6 address</i>
IPv6 bridge address	integer	only available in <i>Advanced Mode</i> and will be grayed out if <i>VIMAGE</i> is unchecked; see NOTE below
IPv6 bridge prefix length	drop-down menu	only available in <i>Advanced Mode</i> and will be grayed out if <i>VIMAGE</i> is unchecked; select the prefix length associated with <i>IPv6 address</i>
IPv6 default gateway	string	only available in <i>Advanced Mode</i> and will be grayed out if <i>VIMAGE</i> is unchecked; used to set the jail's default gateway IPv6 address
MAC	string	only available in <i>Advanced Mode</i> and will be grayed out if <i>VIMAGE</i> is unchecked; if a static MAC address is entered, unique static MAC addresses must be entered for every jail created
NIC	drop-down menu	only available in <i>Advanced Mode</i> and will be grayed out if <i>VIMAGE</i> is checked; can be used to specify the interface to use for jail connections
Sysctls	string	only available in <i>Advanced Mode</i> ; comma-delimited list of sysctls to set inside jail (e.g. <code>allow.sysvipc=1,allow.raw_sockets=1</code>)
Autostart	check-box	only available in <i>Advanced Mode</i> ; uncheck if the jail will be started manually
VIMAGE	check-box	only available in <i>Advanced Mode</i> ; gives a jail its own virtualized network stack; requires promiscuous mode to be enabled on the interface
NAT	check-box	only available in <i>Advanced Mode</i> and will be grayed out for Linux jails or if <i>VIMAGE</i> is unchecked; enables Network Address Translation for the jail

Note: The IPv4 and IPv6 bridge interface is used to bridge the `epair(4)` device, which is automatically created for

each started jail, to a physical network device. The default network device is the one that is configured with a default gateway. So, if *em0* is the FreeBSD name of the physical interface and three jails are running, these virtual interfaces are automatically created: *bridge0*, *epair0a*, *epair1a*, and *epair2a*. The physical interface *em0* will be added to the bridge, as well as each epair device. The other half of the epair will be placed inside the jail and will be assigned the IP address specified for that jail. The bridge interface will be assigned an alias of the default gateway for that jail, if configured, or the bridge IP, if configured; either is correct.

The only time an IP address and mask are required for the bridge is when the jail will be on a different network than the FreeNAS® system. For example, if the FreeNAS® system is on the *10.0.0.0/24* network and the jail will be on the *192.168.0.0/24* network, set the *IPv4 bridge address* and *IPv4 bridge netmask* fields for the jail.

If both the *VIMAGE* and *NAT* boxes are unchecked, the jail must be configured with an IP address within the same network as the interface it is bound to, and that address will be assigned as an alias on that interface. To use a *VIMAGE* jail on the same subnet, uncheck *NAT* and configure an IP address within the same network. In both of these cases, configure only an IP address and do not configure a bridge or a gateway address.

After making selections, click the *OK* button. The jail is created and added to the *Jails* tab as well as in the tree menu under *Jails*. Jails start automatically. To prevent this, uncheck the *Autostart* box.

The first time a jail is added or used as a template, the GUI automatically downloads the necessary components from the internet. A progress bar indicates the status of the download and provides an estimated time for the process to complete. If it is unable to connect to the internet, jail creation fails.

Warning: Failure to download is often caused by the default gateway not being set, preventing internet access. See the Network [Global Configuration](#) section for information on setting the default gateway.

After the first jail is created or a template has been used, subsequent jails will be added very quickly because the downloaded base for creating the jail has been saved to the *Jail Root*.

13.2.1 Managing Jails

Click *Jails* to view and configure the added jails. In the example shown in Figure 13.3, the list entry for the jail named *xdm_1* has been clicked to enable that jail's configuration options. The entry indicates the jail name, IP address, whether it will start automatically at system boot, if it is currently running, and jail type: *standard* for a FreeBSD jail, or *pluginjail* if it was installed using *Plugins*.

From left to right, these configuration icons are available:

Edit Jail: edit the jail settings which were described in Table 13.2.

After a jail has been created, the jail name and type cannot be changed, so these fields will be grayed out.

Note: To modify the IP address information for a jail, use the *Edit Jail* button instead of the associated networking commands from the command line of the jail.

Add Storage: configure the jail to access an area of storage as described in [Add Storage](#).

Upload Plugin: manually upload a plugin previously downloaded from the [plugins repository](#).

Start/Stop: this icon changes appearance depending on the current *Status* of the jail. When the jail is not running, the icon is green and clicking it starts the jail. When the jail is already running, the icon is red and clicking it stops the jail. A stopped jail and its applications are inaccessible until it is restarted.

Restart: restart the jail.

The screenshot shows the FreeNAS Jails management interface. At the top, there is a navigation bar with tabs: 'Jails' (selected), 'Storage', 'Templates', and 'Configuration'. Below the navigation bar is a button labeled 'Add Jail'. The main area displays a table with one row of data:

Jail	IPv4 Address	Autostart	Status	Type
xdm_1	DHCP	true	Running	standard

At the bottom of the interface, there is a row of six icons with labels: a wrench (Edit), a disk (Storage), a red circle (Templates), a yellow circle with a plus (Configuration), a gear (Advanced), and a trash can (Delete).

Fig. 13.3: Viewing Jails

Shell: access a *root* command prompt to configure the selected jail from the command line. When finished, type **exit** to close the shell.

Delete: delete the jail and any periodic snapshots of it. The contents of the jail are entirely removed.

Warning: Back up data and programs in the jail before deleting it. There is no way to recover the contents of a jail after deletion.

Accessing a Jail Using SSH

ssh can be used to access a jail instead of the jail's *Shell* icon. This requires starting the **ssh** service and creating a user account for **ssh** access. Start by clicking the *Shell* icon for the desired jail.

Find the `sshd_enable=` line in the jail's `/etc/rc.conf` and set it to "YES":

```
sshd_enable="YES"
```

Then start the SSH daemon:

```
service sshd start
```

The first time the service runs, the jail's RSA key pair is generated and the key fingerprint and random art image displayed.

Add a user account by typing **adduser** and following the prompts. If the user needs superuser privileges, they must be added to the *wheel* group. For those users, enter *wheel* at this prompt:

```
Login group is user1. Invite user1 into other groups? []: wheel
```

After creating the user, set the *root* password so that the new user will be able to use the **su** command to gain superuser privilege. To set the password, type **passwd** then enter and confirm the desired password.

Finally, test from another system that the user can successfully **ssh** in and become the superuser. In this example, a user named *user1* uses **ssh** to access the jail at 192.168.2.3. The first time the user logs in, they will be asked to verify the fingerprint of the host:

```
ssh user1@192.168.2.3
The authenticity of host '192.168.2.3 (192.168.2.3)' can't be established.
RSA key fingerprint is 6f:93:e5:36:4f:54:ed:4b:9c:c8:c2:71:89:c1:58:f0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.2.3' (RSA) to the list of known hosts.
Password: type_password_here
```

Note: Each jail has its own user accounts and service configuration. These steps must be repeated for each jail that requires SSH access.

Add Storage

It is possible to give a FreeBSD jail access to an area of storage on the FreeNAS® system. This is useful for applications that store a large amount of data or if an application in a jail needs access to the data stored on the FreeNAS® system. One example is transmission, which stores torrents. The storage is added using the [mount_nullfs\(8\)](#) mechanism, which links data that resides outside of the jail as a storage area within the jail.

To add storage, click the *Add Storage* button for a highlighted jail's entry to open the screen shown in Figure 13.4. This screen can also be accessed by expanding the jail name in the tree view and clicking *Storage* → *Add Storage*.

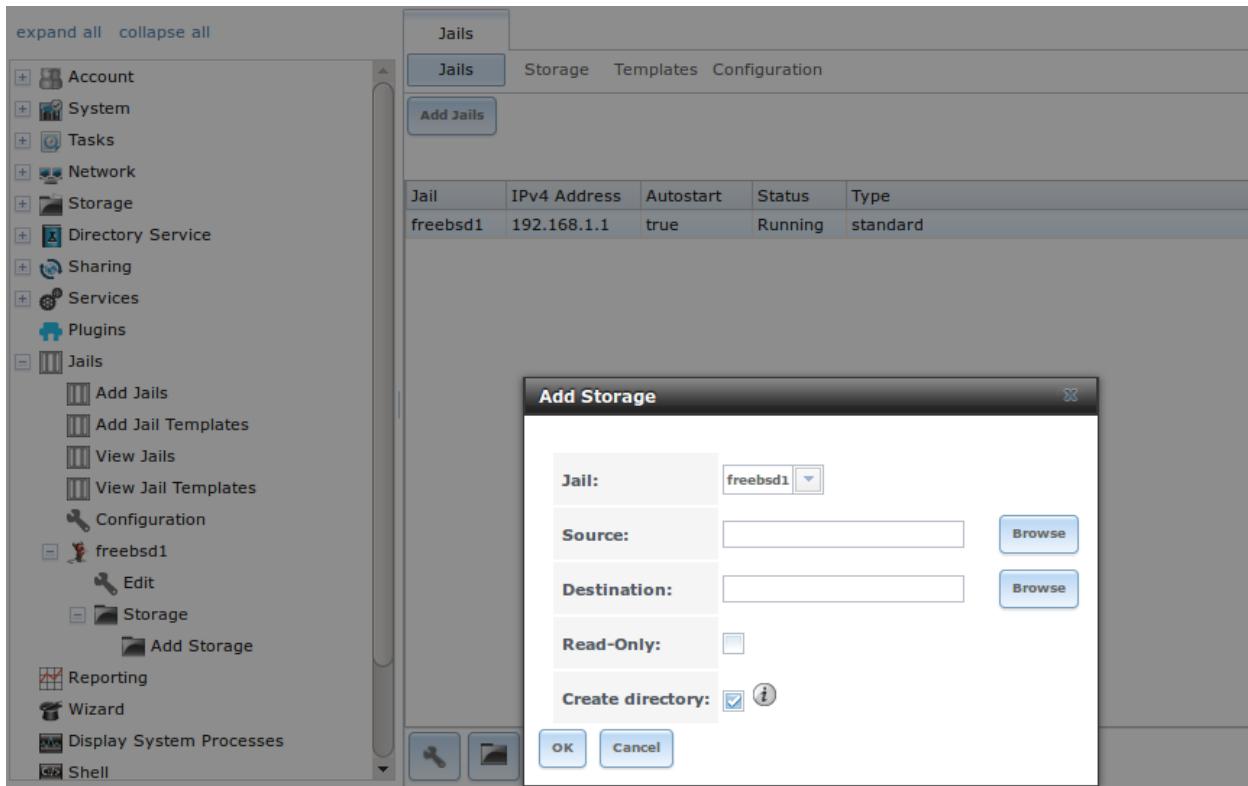


Fig. 13.4: Adding Storage to a Jail

Browse to the *Source* and *Destination*, where:

- **Source:** is the directory or dataset on the FreeNAS® system which will be accessed by the jail. This directory **must** reside outside of the volume or dataset being used by the jail. This is why it is recommended to create a separate dataset to store jails, so the dataset holding the jails is always separate from any datasets used for storage on the FreeNAS® system.
- **Destination:** select an **existing, empty** directory within the jail to link to the *Source* storage area. If that directory does not exist yet, enter the desired directory name and check the *Create directory* box.

Storage is typically added because the user and group account associated with an application installed inside of a jail needs to access data stored on the FreeNAS® system. Before selecting the *Source*, it is important to first ensure that the permissions of the selected directory or dataset grant permission to the user/group account inside of the jail. This is not the default, as the users and groups created inside of a jail are totally separate from the users and groups of the FreeNAS® system.

The workflow for adding storage usually goes like this:

1. Determine the name of the user and group account used by the application. For example, the installation of the transmission application automatically creates a user account named *transmission* and a group account also named *transmission*. When in doubt, check the files */etc/passwd* (to find the user account) and */etc/group* (to find the group account) inside the jail. Typically, the user and group names are similar to the application name. Also, the UID and GID are usually the same as the port number used by the service.

A *media* user and group (GID 8675309) are part of the base system. Having applications run as this group or

user makes it possible to share storage between multiple applications in a single jail, between multiple jails, or even between the host and jails.

2. On the FreeNAS® system, create a user account and group account that match the user and group names used by the application in the jail.
3. Decide whether the jail should have access to existing data or if a new area of storage will be set aside for the jail to use.
4. If the jail will access existing data, edit the permissions of the volume or dataset so the user and group accounts have the desired read and write access. If multiple applications or jails are to have access to the same data, create a new group and add each needed user account to that group.
5. If an area of storage is being set aside for that jail or individual application, create a dataset. Edit the permissions of that dataset so the user and group account has the desired read and write access.
6. Use the *Add Storage* button of the jail and select the configured volume/dataset as the *Source*.

To prevent writes to the storage, check the box *Read-Only*.

By default, the *Create directory* box is checked. This means that the directory will automatically be created under the specified *Destination* path if the directory does not already exist.

After storage has been added or created, it appears in the tree under the specified jail. In the example shown in Figure 13.5, a dataset named `volume1/data` has been chosen as the *Source* as it contains the files stored on the FreeNAS® system. When the storage was created, the user browsed to `/volume1/jails/freebsd1/usr/local` in the *Destination* field, then entered `test` as the directory. Since this directory did not already exist, it was created, because the *Create directory* box was left checked. The resulting storage was added to the `freenas1` entry in the tree as `/usr/local/test`. The user has clicked this `/usr/local/test` entry to access the *Edit* screen.

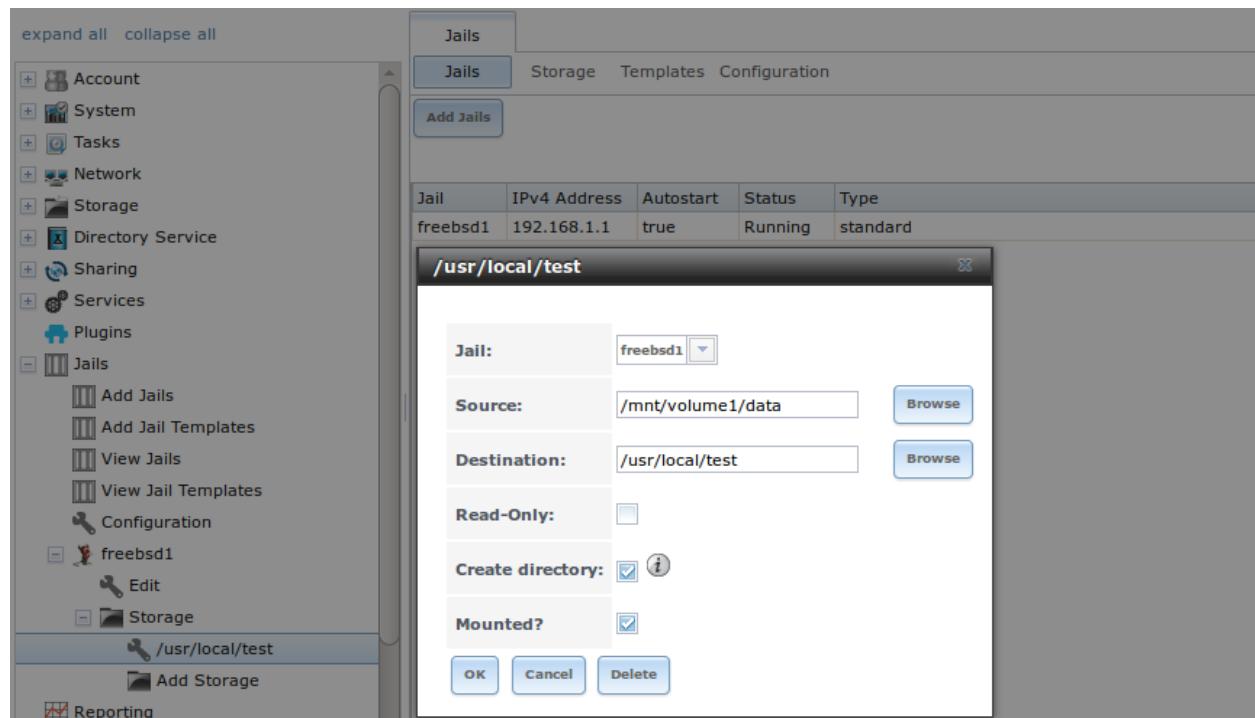


Fig. 13.5: Example Storage

Storage is normally mounted as it is created. To unmount the storage, uncheck the *Mounted?* box.

Note: A mounted dataset will not automatically mount any of its child datasets. While the child datasets may appear to be browsable inside the jail, any changes will not be visible. Since each dataset is considered to be its own filesystem, each child dataset must have its own mount point, so separate storage must be created for any child datasets which need to be mounted.

To delete the storage, click its *Delete* button.

Warning: It is important to realize that added storage is really just a pointer to the selected storage directory on the FreeNAS® system. It does **not** copy that data to the jail. **Files that are deleted from the Destination directory in the jail are really deleted from the Source directory on the FreeNAS® system.** However, removing the jail storage entry only removes the pointer, leaving the data intact but not accessible from the jail.

13.2.2 Installing FreeBSD Packages

The quickest and easiest way to install software inside the jail is to install a FreeBSD package. FreeBSD packages are pre-compiled. They contain all the binaries and a list of dependencies required for the software to run on a FreeBSD system.

A huge amount of software has been ported to FreeBSD, currently over 24,000 applications, and most of that software is available as a package. One way to find FreeBSD software is to use the search bar at [FreshPorts.org](#).

After finding the name of the desired package, use the **pkg install** command to install it. For example, to install the audiotag package, use this command:

```
pkg install audiotag
```

When prompted, type **y** to complete the installation. The installation messages will indicate if the package and its dependencies successfully download and install.

Warning: Some older versions of FreeBSD used package systems which are now obsolete. Do not use commands from those obsolete package systems in a FreeNAS® jail, as they will cause inconsistencies in the jail's package management database. Use the current FreeBSD package system as shown in these examples.

A successful installation can be confirmed by querying the package database:

```
pkg info -f audiotag
audiotag-0.19_1
Name:          audiotag
Version:       0.19_1
Installed on:  Fri Nov 21 10:10:34 PST 2014
Origin:        audio/audiotag
Architecture: freebsd:9:x86:64
Prefix:        /usr/local
Categories:   multimedia audio
Licenses:     GPLv2
Maintainer:   ports@FreeBSD.org
WWW:          http://github.com/Daenyth/audiotag
Comment:      Command-line tool for mass tagging/renaming of audio files
Options:
  DOCS:        on
  FLAC:        on
```

```
ID3:          on
MP4:          on
VORBIS:       on
Annotations:
  repo_type:   binary
  repository:  FreeBSD
Flat size:    62.8KiB
Description:  Audiotag is a command-line tool for mass tagging/renaming of audio_
  ↪files
                  it supports the vorbis comment, id3 tags, and MP4 tags.
WWW:           http://github.com/Daenyth/audiotag
```

To show what was installed by the package:

```
pkg info -l audiotag
audiotag-0.19_1:
/usr/local/bin/audiotag
/usr/local/share/doc/audiotag/COPYING
/usr/local/share/doc/audiotag/ChangeLog
/usr/local/share/doc/audiotag/README
/usr/local/share/licenses/audiotag-0.19_1/GPLv2
/usr/local/share/licenses/audiotag-0.19_1/LICENSE
/usr/local/share/licenses/audiotag-0.19_1/catalog.mk
```

In FreeBSD, third-party software is always stored in `/usr/local` to differentiate it from the software that came with the operating system. Binaries are almost always located in a subdirectory called `bin` or `sbin` and configuration files in a subdirectory called `etc`.

13.2.3 Compiling FreeBSD Ports

Software is typically installed into FreeBSD jails using packages. But sometimes there are good reasons to compile a port instead. Compiling ports offers these advantages:

- Not every port has an available package. This is usually due to licensing restrictions or known, unaddressed security vulnerabilities.
- Sometimes the package is out-of-date and a feature is needed that only became available in the newer version.
- Some ports provide compile options that are not available in the pre-compiled package. These options are used to add or remove features or options.

Compiling a port has these disadvantages:

- It takes time. Depending upon the size of the application, the amount of dependencies, the speed of the CPU, the amount of RAM available, and the current load on the FreeNAS® system, the time needed can range from a few minutes to a few hours or even to a few days.

Note: If the port does not provide any compile options, it saves time and preserves the FreeNAS® system's resources to just use the `pkg install` command instead.

The [FreshPorts.org](#) listing shows whether a port has any configurable compile options. Figure 13.6 shows the *Configuration Options* for audiotag.

This port has five configurable options (DOCS, FLAC, ID3, MP4, and VORBIS) and each option is enabled (on) by default.

The screenshot shows the FreshPorts.org website interface. The main content area displays the 'Port details' for the 'audiotag' port. Key information includes:

- Port Name:** audiotag
- Description:** Command-line tool for mass tagging/renaming of audio files
- Version:** 0.19_1
- Category:** audio
- Maintainer:** Σ=1
- Added:** 15 Apr 2008 13:43:37
- Listed In:** multimedia
- License:** GPLv2+

The page also contains links to the port's GitHub repository ([WWW](http://github.com/Daenyth/audiotag)) and PortsMon ([SVNWeb](#)). It provides instructions for installation ([To install](#), [To add the package](#)) and lists runtime dependencies (e.g., flac, id3tag, AtomicParsley, vorbiscomment, perl5) and configuration options.

On the right side of the page, there are several sidebar boxes:

- Login:** User Login, Create account
- This site:** What is FreshPorts?, About the authors, Issues, FAQ, How big is it?, The latest upgrade!, Privacy, Forums, Blog, Contact
- Search:** Enter Keywords: go, more...
- Latest Vulnerabilities:** A table listing vulnerabilities with their last update date:

file-roller	Oct 12
ImageMagick	Oct 12
ImageMagick-nox11	Oct 12
lipp	Oct 12
mupdf	Oct 12
openoffice-4	Oct 12
openoffice-devel	Oct 12
virtualbox-ose	Oct 12
zathura-pdf-mupdf	Oct 12
libvncserver	Oct 11
linux-c6-openssl*	Oct 11
openjpeg	Oct 11
openssl*	Oct 11
openssl-devel*	Oct 11

Fig. 13.6: Configuration Options for Audiotag

FreeBSD packages are always built using the default options. When compiling a port yourself, those options are presented in a menu, allowing the default values to be changed.

The Ports Collection must be installed in a jail before ports can be compiled. Inside the jail, use the **portsnap** utility. This command downloads the ports collection and extracts it to the jail's `/usr/ports/` directory:

```
portsnap fetch extract
```

Note: To install additional software at a later date, make sure the ports collection is updated with **portsnap fetch update**.

To compile a port, **cd** into a subdirectory of `/usr/ports/`. The entry for the port at FreshPorts provides the location to **cd** into and the **make** command to run. This example compiles and installs the audiotag port:

```
cd /usr/ports/audio/audiotag  
make install clean
```

Since this port has configurable options, the first time this command is run, the configure screen shown in Figure 13.7 is displayed:

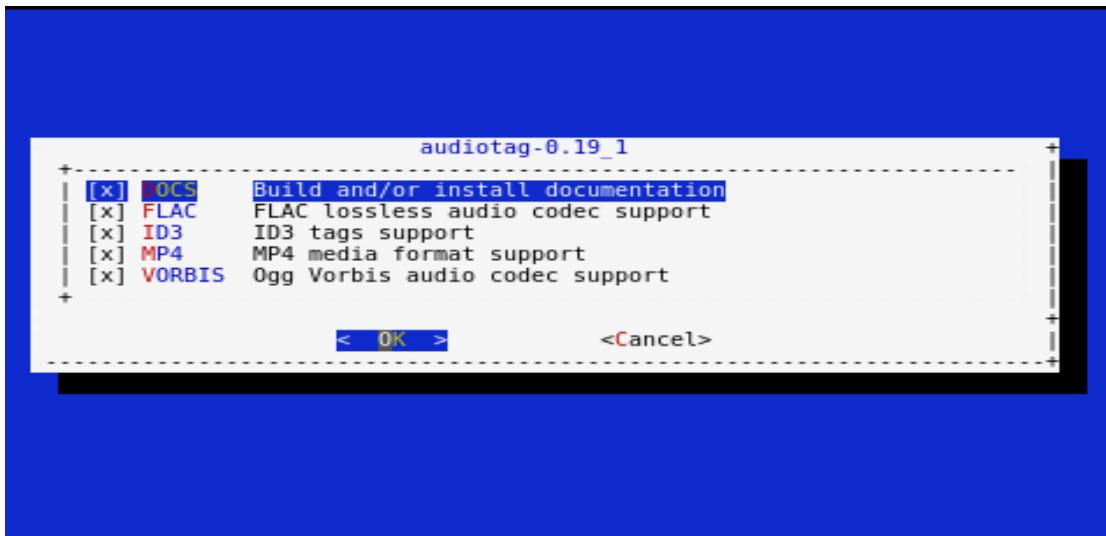


Fig. 13.7: Configuration Options for Audiotag Port

Use the arrow keys to select an option and press `spacebar` to toggle the value. When all the values are as desired, press `Enter`. The port will begin to compile and install.

Note: The configuration screen will not be shown again, even if the build is stopped and restarted. It can be redisplayed by typing **make config**. Change the settings, then rebuild with **make clean install clean**.

Many ports depend on other ports. Those other ports can also have configuration screens that will be shown before compiling begins. It is a good idea to keep an eye on the compile until it finishes and the command prompt returns.

When the port is installed, it is registered in the same package database that manages packages. The same **pkg info** command can be used to determine what was installed, as described in the previous section.

13.2.4 Starting Installed Software

After packages or ports are installed, they need to be configured and started. If you are familiar with the software, look for the configuration file in `/usr/local/etc` or a subdirectory of it. Many FreeBSD packages contain a sample configuration file as a reference. If you are unfamiliar with the software, you will need to spend some time at the software's website to learn which configuration options are available and which configuration files require editing.

Most FreeBSD packages that contain a startable service include a startup script which is automatically installed to `/usr/local/etc/rc.d/`. After the configuration is complete, the starting of the service can be tested by running the script with the `onestart` option. As an example, if openvpn is installed into the jail, these commands run its startup script and verify that the service started:

```
/usr/local/etc/rc.d/openvpn onestart
Starting openvpn.

/usr/local/etc/rc.d/openvpn onestatus
openvpn is running as pid 45560.

sockstat -4
USER COMMAND      PID      FD      PROTO      LOCAL ADDRESS      FOREIGN ADDRESS
root openvpn      48386      4      udp4      *:54789          *:*
```

If it produces an error:

```
/usr/local/etc/rc.d/openvpn onestart
Starting openvpn.
/usr/local/etc/rc.d/openvpn: WARNING: failed to start openvpn
```

Run `tail /var/log/messages` to see if any error messages hint at the problem. Most startup failures are related to a misconfiguration: either a typo or a missing option in a configuration file.

After verifying that the service starts and is working as intended, add a line to `/etc/rc.conf` to start the service automatically when the jail is started. The line to start a service always ends in `_enable="YES"` and typically starts with the name of the software. For example, this is the entry for the openvpn service:

```
openvpn_enable="YES"
```

When in doubt, the startup script shows the line to put in `/etc/rc.conf`. This is the description in `/usr/local/etc/rc.d/openvpn`:

```
# This script supports running multiple instances of openvpn.
# To run additional instances link this script to something like
# % ln -s openvpn openvpn_foo

# and define additional openvpn_foo_* variables in one of
# /etc/rc.conf, /etc/rc.conf.local or /etc/rc.conf.d /openvpn_foo

#
# Below NAME should be substituted with the name of this script. By default
# it is openvpn, so read as openvpn_enable. If you linked the script to
# openvpn_foo, then read as openvpn_foo_enable etc.
#
# The following variables are supported (defaults are shown).
# You can place them in any of
# /etc/rc.conf, /etc/rc.conf.local or /etc/rc.conf.d/NAME
#
# NAME_enable="NO"
# set to YES to enable openvpn
```

The startup script also indicates if any additional parameters are available:

```
# NAME_if=
# driver(s) to load, set to "tun", "tap" or "tun tap"
#
# it is OK to specify the if_ prefix.
#
# # optional:
# NAME_flags=
# additional command line arguments
# NAME_configfile="/usr/local/etc/openvpn/NAME.conf"
# --config file
# NAME_dir="/usr/local/etc/openvpn"
# --cd directory
```

13.3 Using the phpVirtualBox Template

If software requires a different operating system or a non-FreeBSD operating system is needed to manage software, use the VirtualBox template to create an instance of phpVirtualBox. In the *Add Jail* screen, click the *Advanced Mode* button. As shown in the example in Figure 13.8, enter a *Jail Name*, verify that the *IPv4 address* is valid and not in use by another host or jail, and select *VirtualBox* from the *Template* drop-down menu. Press the *OK* button to begin the installation.

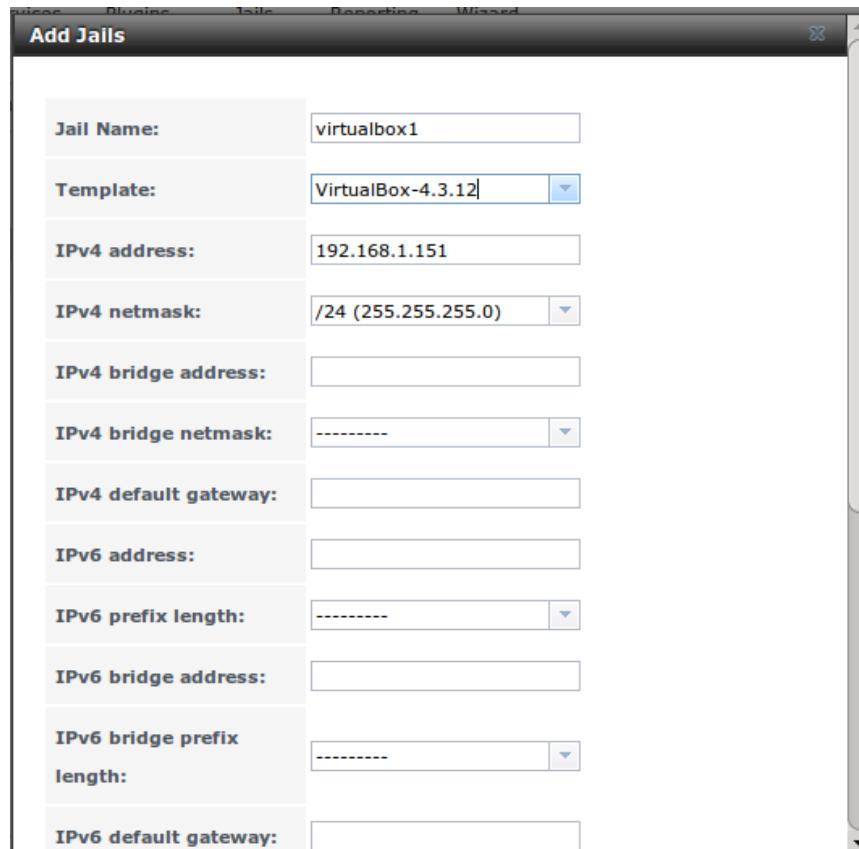


Fig. 13.8: Creating a phpVirtualBox Instance

After installation, enter the IP address of the VirtualBox jail into a web browser and enter the username and password *admin* into the login screen. After authentication, the screen shown in [Figure 13.9](#) appears in the web browser.

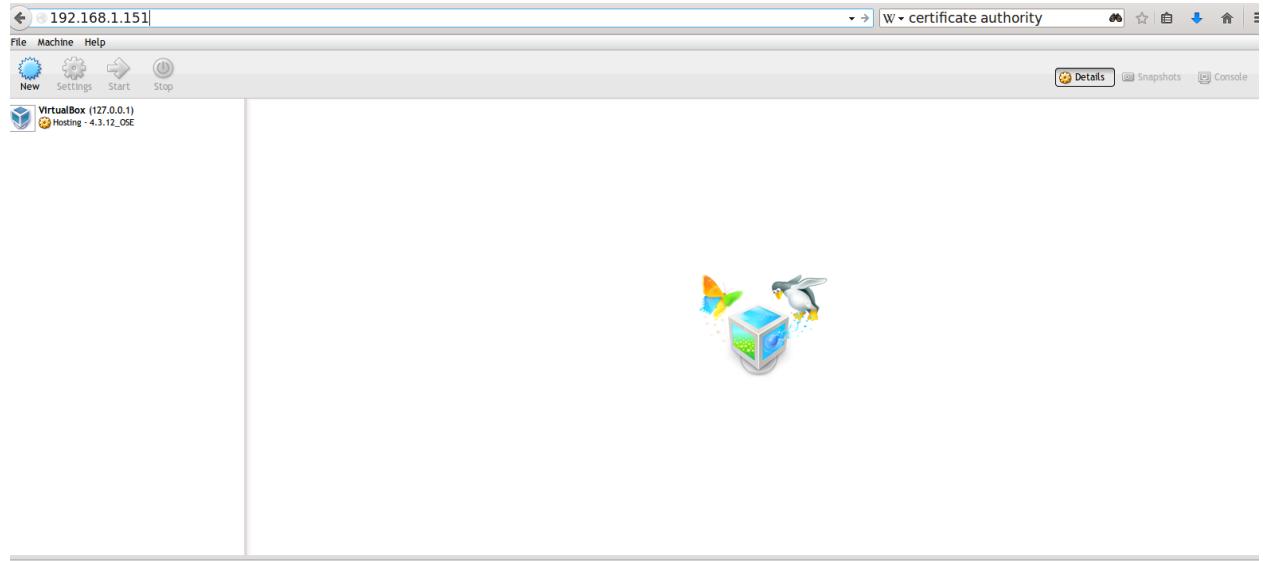


Fig. 13.9: phpVirtualBox Interface

Click the *New* button to create virtual machines. The desired operating systems and software can then be installed into the new virtual machines.

Note: By default, virtual machines are not started when the FreeNAS® system boots. To configure auto-start, refer to this [forum post](#).

13.4 Managing Jail Templates

FreeNAS® supports the ability to add custom templates to the *Templates* drop-down menu described in [Table 13.2](#).

By default, FreeNAS® provides the *VirtualBox* template. To view the default and any customized templates, click *Jails* → *Templates*. A listing showing the default template is seen in [Figure 13.10](#).

The listing contains these columns:

- **Name:** appears in the *Template* drop-down menu when adding a new jail.
- **URL:** when adding a new jail using this template, the template is downloaded from this location.
- **Instances:** indicates if the template has been used to create a jail. In this example, the template has not yet been used so its *Instances* shows *0*.

To create a custom template, first install the desired operating system and configure it as needed. The installation can be either to an existing jail or on another system.

Next, create an mtree specification using this command, replacing */path/to/jail* with the actual path to the jail:

```
mtree -c -p /path/to/jail -k sha256digest > file.mtree
```

Name	URL	Instances
VirtualBox-4.3.12	http://download.freenas.org/jails/9.2/x64/freenas-virtualbox-4.3.12.tgz	0

Fig. 13.10: Default Jail Templates

After configuration is complete, create a tarball of the entire operating system to be used as a template. This tarball needs to be compressed with **gzip** and end in a **.tgz** extension. Be careful when creating the tarball as it is possible to end up in a recursive loop. In other words, the resulting tarball must be saved outside of the operating system being tarballed, such as to an external USB drive or network share. Alternately, create a temporary directory within the operating system and use the **-exclude** switch to **tar** to exclude this directory from the tarball. The exact **tar** command to use will vary, depending upon the operating system being used to create the tarball.

Save the generated **.mtree** and **.tgz** files to either an FTP share or an HTTP server. The FTP or HTTP URL is needed to add the template to the list of available templates.

To add the template, click Jails → Templates → Add Jail Templates which opens the screen shown in Figure 13.11.

Name:	<input type="text"/>
OS:	<input type="text"/> <input type="button" value="▼"/>
Architecture:	<input type="text"/> <input type="button" value="▼"/>
URL:	<input type="text"/>
Mtree:	<input type="text"/> <input type="button" value="i"/>
Read-only:	<input type="checkbox"/>
OK	Cancel

Fig. 13.11: Adding A Custom Jail Template

Table 13.3 summarizes the fields in this screen.

Table 13.3: Jail Template Options

Setting	Value	Description
Name	string	value appears in the <i>Name</i> column of <i>View Jail Templates</i>
OS	drop-down menu	choices are <i>FreeBSD</i> or <i>Linux</i>
Architecture	drop-down menu	choices are <i>x86</i> (32-bit) or <i>x64</i> (64-bit)
URL	string	enter the full URL to the <i>.tgz</i> file, including the protocol (<i>ftp://</i> or <i>http://</i>)
Mtree	string	paste the mtree specification for the template
Read-only	checkbox	when checked, the <i>Name</i> and <i>URL</i> of the template cannot be changed after creation

After adding a template, click the entry for the template to access the *Edit* and *Delete* buttons. Clicking a template's *Edit* button opens the configuration screen shown in Figure 13.12.

Note: The *Delete* button is not available for the built-in *VirtualBox* template and the *Edit* button opens it as read-only.

The screenshot shows the FreeNAS web interface for managing jail templates. At the top, there is a navigation bar with tabs: 'Jails' (selected), 'Storage', 'Templates' (selected), and 'Configuration'. Below the navigation bar, there is a button labeled 'Add Jail Templates'. The main area displays a table of existing templates:

Name	URL	Instances
VirtualBox-4.3.12	http://download.freenas.org/jails/9.2/x64/freenas-virtualbox-4.3.12.tgz	1
customfreebsd	http://myurl.com	0

Below the table, an 'Edit' dialog box is open, overlaid on the page. The dialog box has a title 'Edit' and contains the following fields:

- Name:** customfreebsd
- OS:** FreeBSD
- Architecture:** x64
- URL:** <http://myurl.com>
- Mtree:** (empty input field with an info icon)

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

Fig. 13.12: Editing Template Options

Clicking a template's *Delete* button shows a warning message that prompts for confirmation of the deletion. Note

that once a template is deleted, it is removed from the *Templates* drop-down menu and will no longer be available for creating new jails.

13.5 Using iohyve

Beginning with FreeNAS® 9.10, the **iohyve** command line utility is included for creating, managing, and launching **bhyve** guests.

Note: This type of virtualization requires an Intel processor with Extended Page Tables (EPT) or an AMD processor with Rapid Virtualization Indexing (RVI) or Nested Page Tables (NPT).

To verify that an Intel processor has the required features, use *Shell* to run **grep VT-x /var/run/dmesg.boot**. If the *EPT* and *UG* features are shown, this processor can be used with **bhyve** and **iohyve**.

To verify that an AMD processor has the required features, use *Shell* to run **grep POPCNT /var/run/dmesg.boot**. If the output shows the *POPCNT* feature, this processor can be used with **bhyve** and **iohyve**.

Run this command to initialize **iohyve**, substituting the name of the pool to hold the **bhyve** guests and the name of the network interface:

```
iohyve setup pool=volume1 kmod=1 net=em0
Setting up iohyve pool...
Loading kernel modules...
Setting up bridge0 on em0...
net.link.tap.up_onopen: 0 -> 1

ln -s /mnt/iohyve /iohyve
```

The next step is to tell **iohyve** which installation ISO to download. This example shows fetching the 64-bit version of FreeBSD 10.3, then verify that the fetch was successful:

```
iohyve fetch ftp://ftp.freebsd.org/pub/FreeBSD/releases/amd64/amd64/ISO-IMAGES/10.3/
  ↳FreeBSD-10.3-RELEASE-amd64-bootonly.iso
Fetching ftp://ftp.freebsd.org/pub/FreeBSD/releases/amd64/amd64/ISO-IMAGES/10.3/
  ↳FreeBSD-10.3-RELEASE-amd64-bootonly.iso...
/iohyve/ISO/FreeBSD-10.3-RELEASE-amd64-bootonly.iso 100% of 232 MB 2443 kBps 01m38s

iohyve isolist
Listing ISO's...
FreeBSD-10.3-RELEASE-amd64-bootonly.iso
```

Specify the name and size of the guest to create it and verify its status:

```
iohyve create freebsd10.3 8G
Creating freebsd10.3...

iohyve list
Guest          VMM?    Running?      rcboot?      Description
freebsd10.3   NO      NO           NO          Thu_Mar_24_09:37:30_PDT_2016
```

The newly created guest is not yet running, nor is it set to automatically start (rcboot) when **iohyve** starts.

Install a guest using a specified ISO:

```
iohyve install freebsd10.3 FreeBSD-10.3-RELEASE-amd64-bootonly.iso  
Installing freebsd10.3...
```

More information on iohyve:

- [Forum post on iohyve](#)
- [Running virtual machines using iohyve on FreeNAS® 9.10](#)

CHAPTER FOURTEEN

REPORTING

Reporting displays several graphs, as seen in the example in Figure 14.1. Click the tab for a device type to see its graphs.

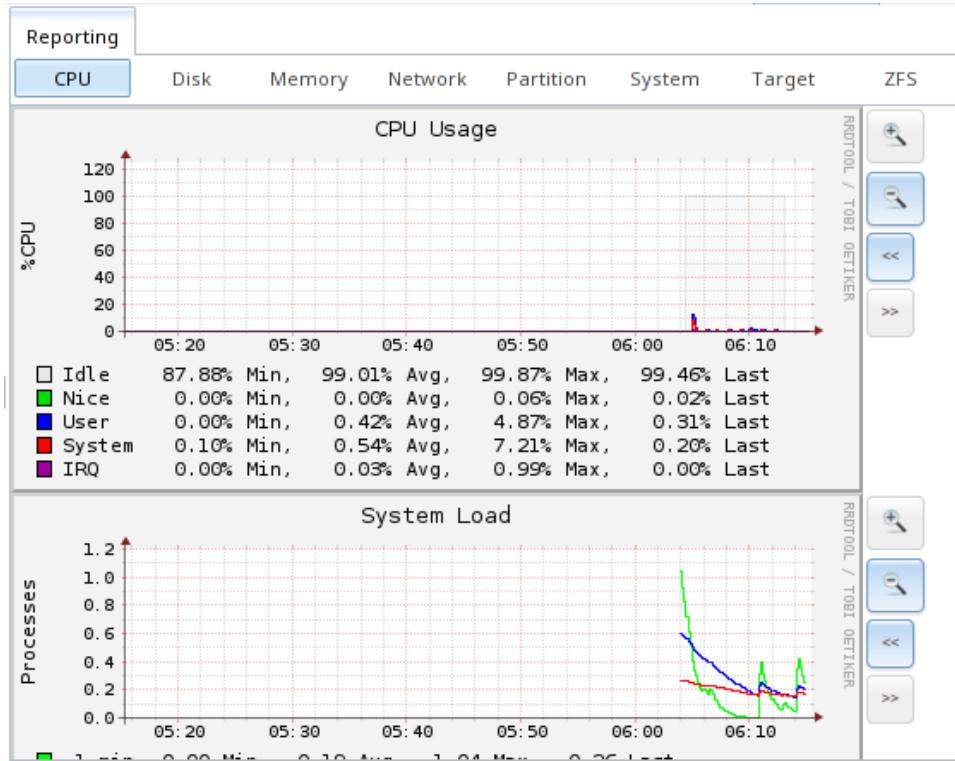


Fig. 14.1: Reporting Graphs

FreeNAS® uses `collectd` to provide reporting statistics. The following collectd plugins are enabled in `/conf/base/etc/local/collectd.conf`, and thus provide reporting graphs:

- `CPU usage` : collects the amount of time spent by the CPU in various states such as executing user code, executing system code, and being idle.
- `system load` : provides a rough overview of system utilization over a one, five, and fifteen minute average.
- `disk` : shows the average time a disk I/O operation took to complete.
- `physical memory` : displays physical memory usage.
- `swap utilization` : displays the amount of free and used swap space.

- [interface](#) : shows received and transmitted traffic in bits per second for each configured interface.
- [disk space](#) : displays free and used space for each volume and dataset. However, the disk space used by an individual zvol is not displayed as it is a block device.
- [processes](#) : displays the number of processes, grouped by state.
- [uptime](#) : keeps track of the system uptime, the average running time, and the maximum reached uptime.
- [target](#): contains bandwidth statistics for iSCSI ports.
- [zfs](#) : shows ARC size, hit ratio, and requests.

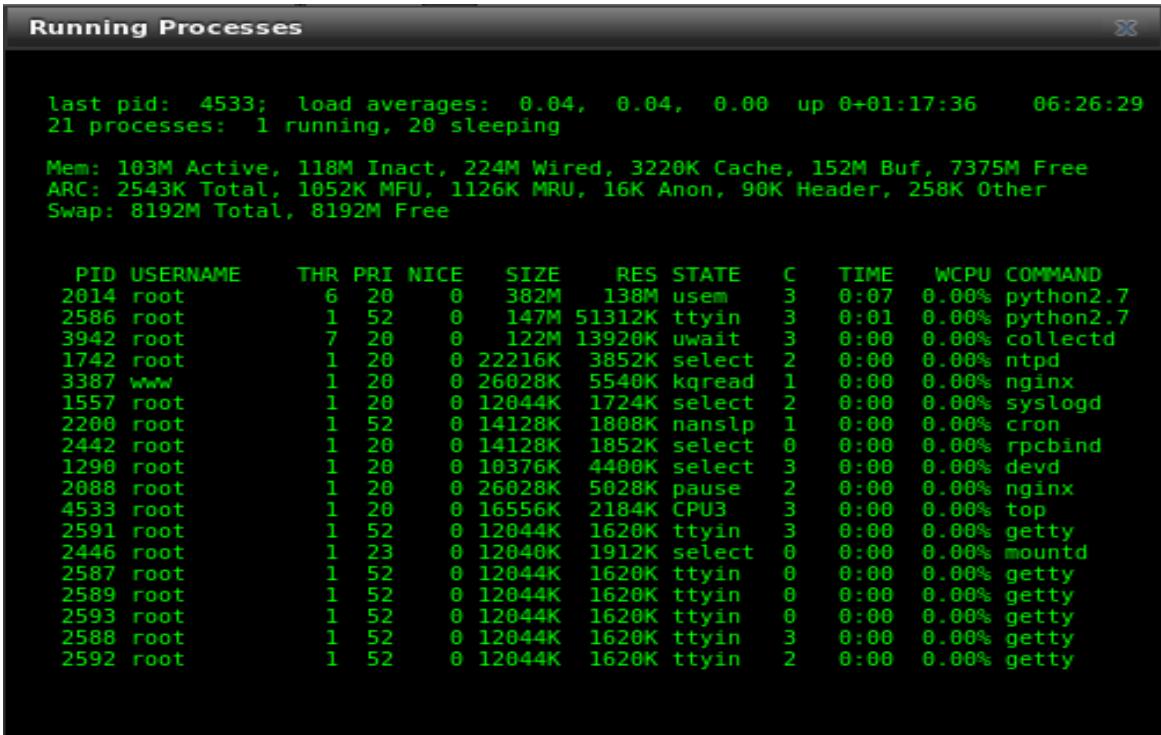
Reporting data is saved, allowing you to view and monitor usage trends over time. By default, reporting data is saved to `/data/rrd_dir.tar.bz2` and should be preserved across system upgrades and at shutdown. To instead save this data to the system dataset, check the *Reporting database* box in System → System Dataset .

Use the magnifier buttons next to each graph to increase or decrease the displayed time increment from 10 minutes, hourly, daily, weekly, or monthly. You can also use the << and >> buttons to scroll through the output.

[Update on using Graphite with FreeNAS](#) contains instructions for sending the collected information to a Graphite server.

DISPLAY SYSTEM PROCESSES

Clicking *Display System Processes* opens a screen showing the output of `top(1)`. An example is shown in Figure 15.1.



The screenshot shows a terminal window titled "Running Processes". The output of the `top` command is displayed, providing real-time information about system processes. The top section shows summary statistics: last pid (4533), load averages (0.04, 0.04, 0.00), system up time (0+01:17:36), and current time (06:26:29). It also lists the number of processes (21) and their states (1 running, 20 sleeping). Below this, memory usage details are provided: Active (103M), Inact (118M), Wired (224M), Cache (3220K), Buf (152M), and Free (7375M). ARC statistics show Total (2543K), MFU (1052K), MRU (1126K), Anon (16K), Header (90K), and Other (258K). Swap usage is shown as Total (8192M) and Free (8192M). The main part of the output is a table of processes, each row containing fields such as PID, USERNAME, THR, PRI, NICE, SIZE, RES, STATE, C, TIME, WCPU, and COMMAND. The table lists numerous processes including root, www, ntpd, collectd, cron, rpcbind, devd, nginx, syslogd, and several getty entries. The processes are sorted by CPU usage.

PID	USERNAME	THR	PRI	NICE	SIZE	RES	STATE	C	TIME	WCPU	COMMAND
2014	root	6	20	0	382M	138M	usem	3	0:07	0.00%	python2.7
2586	root	1	52	0	147M	51312K	ttyin	3	0:01	0.00%	python2.7
3942	root	7	20	0	122M	13920K	uwait	3	0:00	0.00%	collectd
1742	root	1	20	0	22216K	3852K	select	2	0:00	0.00%	ntpd
3387	www	1	20	0	26028K	5540K	kqread	1	0:00	0.00%	nginx
1557	root	1	20	0	12044K	1724K	select	2	0:00	0.00%	syslogd
2200	root	1	52	0	14128K	1808K	nanslp	1	0:00	0.00%	cron
2442	root	1	20	0	14128K	1852K	select	0	0:00	0.00%	rpcbind
1290	root	1	20	0	10376K	4400K	select	3	0:00	0.00%	devd
2088	root	1	20	0	26028K	5028K	pause	2	0:00	0.00%	nginx
4533	root	1	20	0	16556K	2184K	CPU3	3	0:00	0.00%	top
2591	root	1	52	0	12044K	1620K	ttyin	3	0:00	0.00%	getty
2446	root	1	23	0	12040K	1912K	select	0	0:00	0.00%	mountd
2587	root	1	52	0	12044K	1620K	ttyin	0	0:00	0.00%	getty
2589	root	1	52	0	12044K	1620K	ttyin	0	0:00	0.00%	getty
2593	root	1	52	0	12044K	1620K	ttyin	0	0:00	0.00%	getty
2588	root	1	52	0	12044K	1620K	ttyin	3	0:00	0.00%	getty
2592	root	1	52	0	12044K	1620K	ttyin	2	0:00	0.00%	getty

Fig. 15.1: System Processes Running on FreeNAS®

The display will automatically refresh itself. Click the *X* in the upper right corner to close the display. Note that the display is read-only, meaning that you will not be able to issue a `kill` command within it.

CHAPTER
SIXTEEN

SHELL

Beginning with version 8.2.0, the FreeNAS® GUI provides a web shell, making it convenient to run command line tools from the web browser as the *root* user. The link to Shell is the fourth entry from the bottom of the menu tree. In Figure 16.1, the link has been clicked and Shell is open.

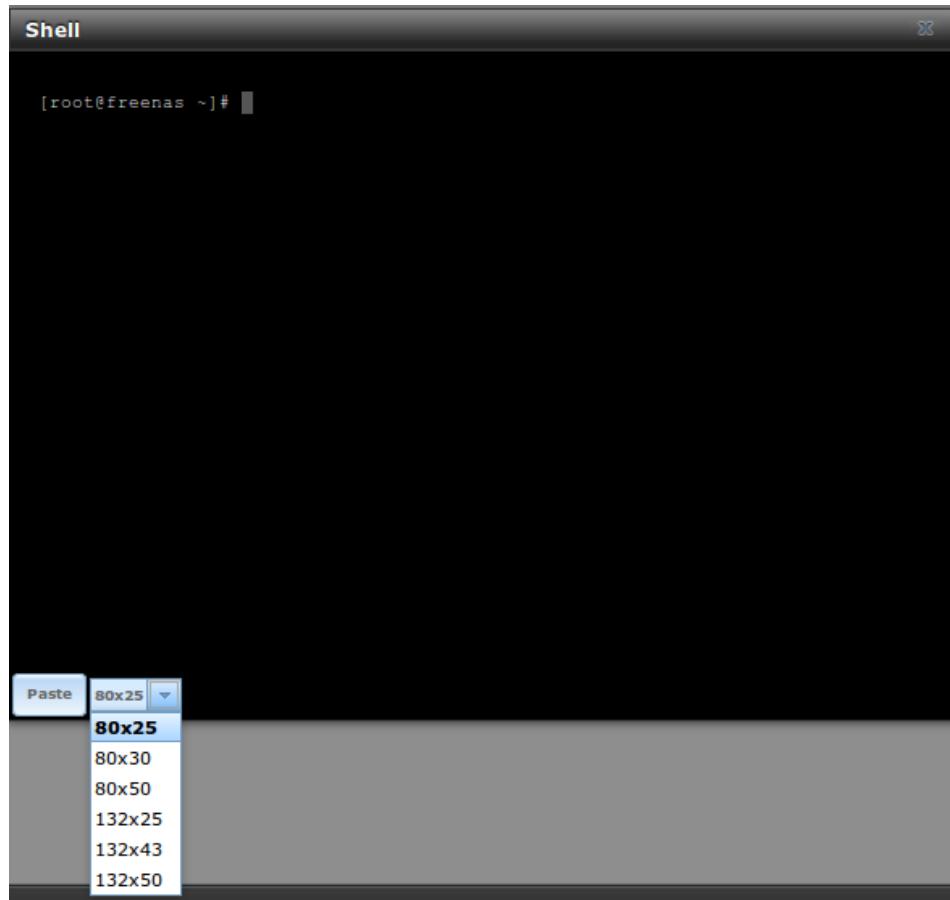


Fig. 16.1: Web Shell

The prompt indicates that the current user is *root*, the hostname is *freenas*, and the current working directory is ~ (*root*'s home directory).

To change the size of the shell, click the *80x25* drop-down menu and select a different size.

To copy text from shell, highlight the text, right-click, and select *Copy* from the right-click menu. To paste into the

shell, click the *Paste* button, paste the text into the box that opens, and click the *OK* button to complete the paste operation.

Shell provides history (use your up arrow to see previously entered commands and press `Enter` to repeat the currently displayed command) and tab completion (type a few letters and press tab to complete a command name or filename in the current directory). When you are finished using Shell, type `exit` to leave the session.

While you are in Shell, you will not have access to any of the other GUI menus. If you need to have access to a prompt while using the GUI menus, use `tmux` instead as it supports multiple shell sessions and the detachment and reattachment of sessions.

Note: Not all of Shell's features render correctly in Chrome. Firefox is the recommended browser for using Shell.

Most FreeBSD command line utilities are available in Shell. Additional troubleshooting utilities that are provided by FreeNAS® are described in [Command Line Utilities](#).

CHAPTER
SEVENTEEN

LOG OUT

Click the *Log Out* entry in the FreeNAS® GUI to log out.

After logging out, a message appears with a link to log back in. When logging back in, the *root* password is required.

CHAPTER
EIGHTEEN

REBOOT

Clicking the *Reboot* entry in the tree shows the warning message in Figure 18.1. The browser screen color changes to red to indicate that this option will negatively impact current users of the FreeNAS® system.

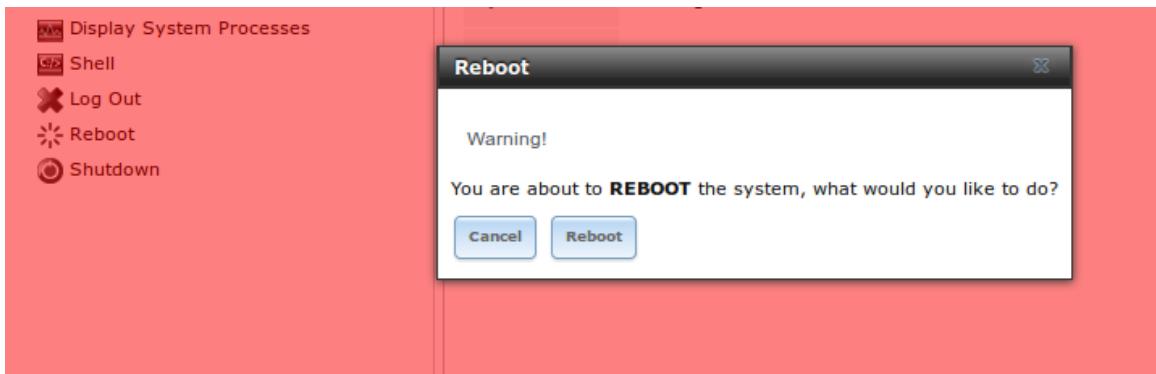


Fig. 18.1: Reboot Warning Message

If a scrub or resilver is in progress when a reboot is requested, an additional warning will ask you to make sure that you wish to proceed. In this case, it is recommended to *Cancel* the reboot request and to periodically run `zpool status` from Shell until it is verified that the scrub or resilver process is complete. Once complete, the reboot request can be re-issued.

Click the *Cancel* button to cancel the reboot request. Otherwise, click the *Reboot* button to reboot the system. Rebooting the system disconnects all clients, including the web administration GUI. The URL in the web browser changes 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, the the GUI login screen will appear. If the login screen does not appear, physical access to the FreeNAS® system's monitor and keyboard is needed to determine what problem is preventing the system from resuming normal operation.

SHUTDOWN

Clicking the *Shutdown* entry in the tree opens the warning message shown in Figure 19.1. The browser window color changes to red to indicate that this command will negatively impact current users of the FreeNAS® system.



Fig. 19.1: Shutdown Warning Message

If a scrub or resilver is in progress when a shutdown is requested, an additional warning will ask if you wish to proceed. In this case, it is recommended to *Cancel* the shutdown request and to periodically run `zpool status` from *Shell* until the scrub or resilver process is complete. Once complete, the shutdown request can be re-issued.

Click the *Cancel* button to cancel the shutdown request. Otherwise, click the *Shutdown* button to halt the system. Shutting down the system disconnects all clients, including the web administration GUI, and powers off the FreeNAS® system. Physical access to the FreeNAS® system will be needed to turn it back on.

CHAPTER
TWENTY

SUPPORT ICON

The *Support* icon, the third icon from the left in the top menubar, provides a shortcut to System → Support . This screen can be used to create a support ticket. Refer to *Support* for detailed usage instructions.

**CHAPTER
TWENTYONE**

GUIDE

The *Documentation* icon, the second icon from the left in the top menubar, provides a built-in browser to the FreeNAS® User Guide (this documentation).

CHAPTER
TWENTYTWO

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 flashes red when there is an outstanding alert. In the example alert shown in Figure 22.1, the system is warning that the S.M.A.R.T. service is not running.



Fig. 22.1: Example Alert Message

Informational messages have a green *OK*, warning messages flash yellow, and messages requiring attention are listed as a red *CRITICAL*. CRITICAL messages are also emailed to the root user account. If you are aware of a critical condition but wish to remove the flashing alert until you deal with it, uncheck the box next to that message.

Behind the scenes, an alert daemon checks for various alert conditions, such as volume and disk status, and writes the current conditions to `/var/tmp/alert`. The daemon retrieves the current alert status every minute and will change the solid green alert icon to flashing red if a new alert is detected.

Current alerts can also be viewed from the Shell option of the Console Setup Menu (Figure 3.1) or from the Web Shell (Figure 16.1) by running `alertcli.py`.

Some of the conditions that trigger an alert include:

- used space on a volume goes over 80%
- new OpenZFS feature flags are available for the pool; this alert can be unchecked if you choose not to upgrade the pool at this time
- a new update is available
- non-optimal multipath states detected
- ZFS pool status changes from *HEALTHY*
- a S.M.A.R.T. error occurs
- the system dataset does not reside on the boot pool
- the system is unable to bind to the *WebGUI IPv4 Address* set in *System → General*
- the system can not find an IP address configured on an iSCSI portal
- a periodic snapshot or replication task fails

- a VMware login or a *VMware-Snapshot* task fails
- deleting a VMware snapshot fails
- a Certificate Authority or certificate is invalid or malformed
- an update failed, or the system needs to reboot to complete a successful update
- a re-key operation fails on an encrypted pool
- the status of an Avago MegaRAID SAS controller has changed; [mfiutil\(8\)](#) is included for managing these devices

An alert is also generated when the Avago HBA firmware version does not match the driver version. To resolve this alert, download the IT (integrated target) firmware, not the IR (integrated RAID) firmware, from the Avago website. Specify the name of the firmware image and BIOS as well as the controller to flash:

```
sas2flash -o -f firmwareimagename -b biosname -c controllernumber
```

When finished, reboot the system. The new firmware version will appear in the system messages and the alert will be cleared.

CHAPTER
TWENTYTHREE

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.

The rest of this section discusses the following resources which are available to FreeNAS® users:

- *Website and Social Media*
- *Forums*
- *IRC*
- *Mailing Lists*
- *Videos*
- *Professional Support*

23.1 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
- Twitter

23.2 Forums

The FreeNAS® Forums are another information source which contains categorized user-contributed tips and guides. This makes it an ideal resource for learning more about a certain aspect of FreeNAS®. A search bar is included for searching by keyword. Or click a category to browse through the threads that exist for that topic.

These categories are available under **Forum Information**:

- **Forum Guidelines:** read this first before creating a forum post.

- [Announcements](#): subscribe to this forum if you wish to receive announcements about new FreeNAS® versions and features.

These categories are available under **Help and Support**:

- [New to FreeNAS®?](#): 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.
- [Bug Reporting](#): use this forum if 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.
- [Plugins](#): provides a discussion area for creating and troubleshooting PBIs.

These categories are available under **Development**:

- [FreeNAS](#): general development discussion.
- [nanobsd](#): the embedded operating system on which FreeNAS® is based.
- [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.

These 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.
- [Useful Scripts](#): user-contributed scripts.

For tips on testing and increasing the performance of your system, check out the [Performance](#) forum.

These 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 the 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.

These language-specific categories are available under **International**, allowing FreeNAS® users to interact with each other in their native language:

- [Dutch - Nederlands](#)
- [French - Francais](#)

- German - Deutsch
- Italian - Italiano
- Portuguese - Português
- Russian
- Spanish - Espanol
- Swedish - Svenske
- Turkish - Türkçe

To ask a question on the forum, click the *Sign Up Now!* link to create an account and log in using that account.

When asking a question on the forum, it is important to:

- First check to see if the question has already been asked. If a similar question exists, do not create a new thread. Instead use the *Reply* link at the bottom of the post 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 but before clicking the *Create Thread* button, make sure the *Watch this thread...* box is checked. To be notified by email, also check the *and receive email notifications* box. You will be notified whenever anyone answers your question.

23.3 IRC

To ask a question in real time, you can use the `#freenas` channel on IRC Freenode. Depending on the time of day and your time zone, FreeNAS® developers or other users may be available to provide assistance. If no one answers right away, remain on the channel, as other users tend to read the channel history to answer questions as time permits.

Typically, an IRC [client](#) is used to access the `#freenas` IRC channel. Alternately, use [webchat](#) from a web browser.

To get the most out of the IRC channel, keep these points in mind:

- Do not ask “can anyone help me?”. Just ask the question. If someone knows the answer, they will try to help.
- Do not ask a question and then leave. Users who know the answer cannot help you if you disappear.
- Do not 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 difficult, 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 have missed anything.
- Do not post error messages in the channel as the IRC software will probably kick you out. Instead, use a pasting service such as [pastebin](#) and paste the resulting URL into the IRC discussion.

23.4 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.

These 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 <<http://doc.freenas.org/>>`_.
- [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 <<http://pootle.freenas.org/>>`_ and translating FreeNAS® documentation.

Note: The mailing lists were migrated from SourceForge to Mailman in December, 2013. Archives of the SourceForge mailing lists are available at [Gmane](#).

23.5 Videos

A series of instructional videos are available for FreeNAS®:

- [Changes in FreeNAS® 9.3](#)
- [FreeNAS 9.3 Updates](#)
- [How to Upgrade FreeNAS® 9.3](#)
- [How to Install FreeNAS® 9.3](#)
- [FreeNAS® 9.3 Shares Overview \(AFP, NFS, CIFS, + New WebDAV\)](#)
- [How to Replace HDD in FreeNAS® 9.3](#)
- [TrueNAS® 9.3 Snapshots Setup](#)
- [Install Murmur \(Mumble server\) on FreeNAS/FreeBSD](#)
- [FreeNAS® 9.3 - First Time Setup Wizard](#)
- [FreeNAS® 9.3 Permissions Overview](#)
- [FreeNAS® 9.3 iSCSI Overview](#)
- [FreeNAS® 9.10 - Certificate Authority & SSL Certificates](#)
- [How to Update FreeNAS® 9.10](#)
- [FreeNAS® 9.10 LAGG & VLAN Overview](#)

23.6 Professional Support

In addition to the freely available community resources, professional support may be available through iXsystems' network of third-party consultants. Submit a support inquiry using the form at <https://www.ixsystems.com/freenas-commercial-support/>.

CHAPTER
TWENTYFOUR

COMMAND LINE UTILITIES

Several command line utilities which are provided with FreeNAS® are demonstrated in this section.

The following utilities can be used for benchmarking and performance testing:

- *Iperf*: used for measuring maximum TCP and UDP bandwidth performance
- *Netperf*: a tool for measuring network performance
- *IOzone*: filesystem benchmark utility used to perform a broad filesystem analysis
- *arcstat*: used to gather ZFS ARC statistics

The following utilities are specific to RAID controllers:

- *tw_cli*: used to monitor and maintain 3ware RAID controllers
- *MegaCli*: used to configure and manage Avago MegaRAID SAS family of RAID controllers

This section also describes the following utilities:

- *freenas-debug*: the backend used to dump FreeNAS® debugging information
- *tmux*: a terminal multiplexer similar to GNU screen
- *Dmidecode*: reports information about system hardware as described in the system's BIOS

24.1 Iperf

Iperf is a utility for measuring maximum TCP and UDP bandwidth performance. It can be used to chart network throughput over time. For example, you can use it to test the speed of different types of shares to determine which type best performs on your network.

FreeNAS® includes the Iperf server. To perform network testing, you will need to install an Iperf client on a desktop system that has network access to the FreeNAS® system. This section will demonstrate how to use the *xiperf GUI client* as it works on Windows, Mac OS X, Linux, and BSD systems.

Since this client is java based, you will also need to install the appropriate *JRE* for the client operating system.

Linux and BSD users will need to install the *iperf* package using their operating system's package management system.

To start xiperf on Windows: unzip the downloaded file, start Command Prompt in Run as administrator mode, *cd* to the unzipped folder, and run **jperf.bat**.

To start xiperf on Mac OS X, Linux, or BSD, unzip the downloaded file, *cd* to the unzipped directory, type **chmod u+x jperf.sh**, and run **./jperf.sh**.

Once the client is ready, you need to start the Iperf server on FreeNAS®. To see the available server options, open Shell and type:

```
iperf --help | more
Usage: iperf [-s|-c host] [options]
iperf [-h|--help] [-v|--version]

Client/Server:
-f, --format [kmKM]  format to report: Kbits, Mbits, KBytes, MBytes
-i, --interval       # seconds between periodic bandwidth reports
-l, --len   #[KM]    length of buffer to read or write (default 8 KB)
-m, --print_mss      print TCP maximum segment size (MTU - TCP/IP header)
-o, --output <filename> output the report or error message to this specified file
-p, --port   #       server port to listen on/connect to
-u, --udp      use UDP rather than TCP
-w, --window #[KM]  TCP window size (socket buffer size)
-B, --bind     <host> bind to <host>, an interface or multicast address
-C, --compatibility for use with older versions does not send extra msgs
-M, --mss     #       set TCP maximum segment size (MTU - 40 bytes)
-N, --nodelay      set TCP no delay, disabling Nagle's Algorithm
-V, --IPv6Version Set the domain to IPv6

Server specific:
-s, --server        run in server mode
-U, --single_udp    run in single threaded UDP mode
-D, --daemon         run the server as a daemon

Client specific:
-b, --bandwidth #[KM]      for UDP, bandwidth to send at in bits/sec
                           (default 1 Mbit/sec, implies -u)
-c, --client <host>    run in client mode, connecting to <host>
-d, --dualtest        Do a bidirectional test simultaneously
-n, --num   #[KM]      number of bytes to transmit (instead of -t)
-r, --tradeoff        Do a bidirectional test individually
-t, --time   #       time in seconds to transmit for (default 10 secs)
-F, --fileinput <name>    input the data to be transmitted from a file
-I, --stdin           input the data to be transmitted from stdin
-L, --listenport #    port to receive bidirectional tests back on
-P, --parallel        #       number of parallel client threads to run
-T, --ttl    #       time-to-live, for multicast (default 1)
-Z, --linux-congestion <algo> set TCP congestion control algorithm (Linux only)

Miscellaneous:
-x, --reportexclude [CDMSV] exclude C(connection) D(data) M(multicast) S(settings) ↵
                           V(server) reports
-y, --reportstyle C      report as a Comma-Separated Values
-h, --help              print this message and quit
-v, --version           print version information and quit

[KM] Indicates options that support a K or M suffix for kilo- or mega-
```

The TCP window size option can be set by the environment variable `TCP_WINDOW_SIZE`. Most other options can be set by an environment variable `IPERF_<long option name>`, such as `IPERF_BANDWIDTH`.

For example, to perform a TCP test and start the server in daemon mode (so that you get your prompt back), type:

```
iperf -sD
-----
Server listening on TCP port 5001
```

```
TCP window size: 64.0 KByte (default)
```

```
Running Iperf Server as a daemon
The Iperf daemon process ID: 4842
```

Note: If you close *Shell*, the daemon process will stop. Have your environment set up (e.g. shares configured and started) **before** starting the iperf process.

From your desktop, open the client. Enter the IP of address of the FreeNAS® system, specify the running time for the test under Application layer options → Transmit (the default test time is 10 seconds), and click the *Run Iperf!* button. Figure 24.1 shows an example of the client running on a Windows system while an SFTP transfer is occurring on the network.

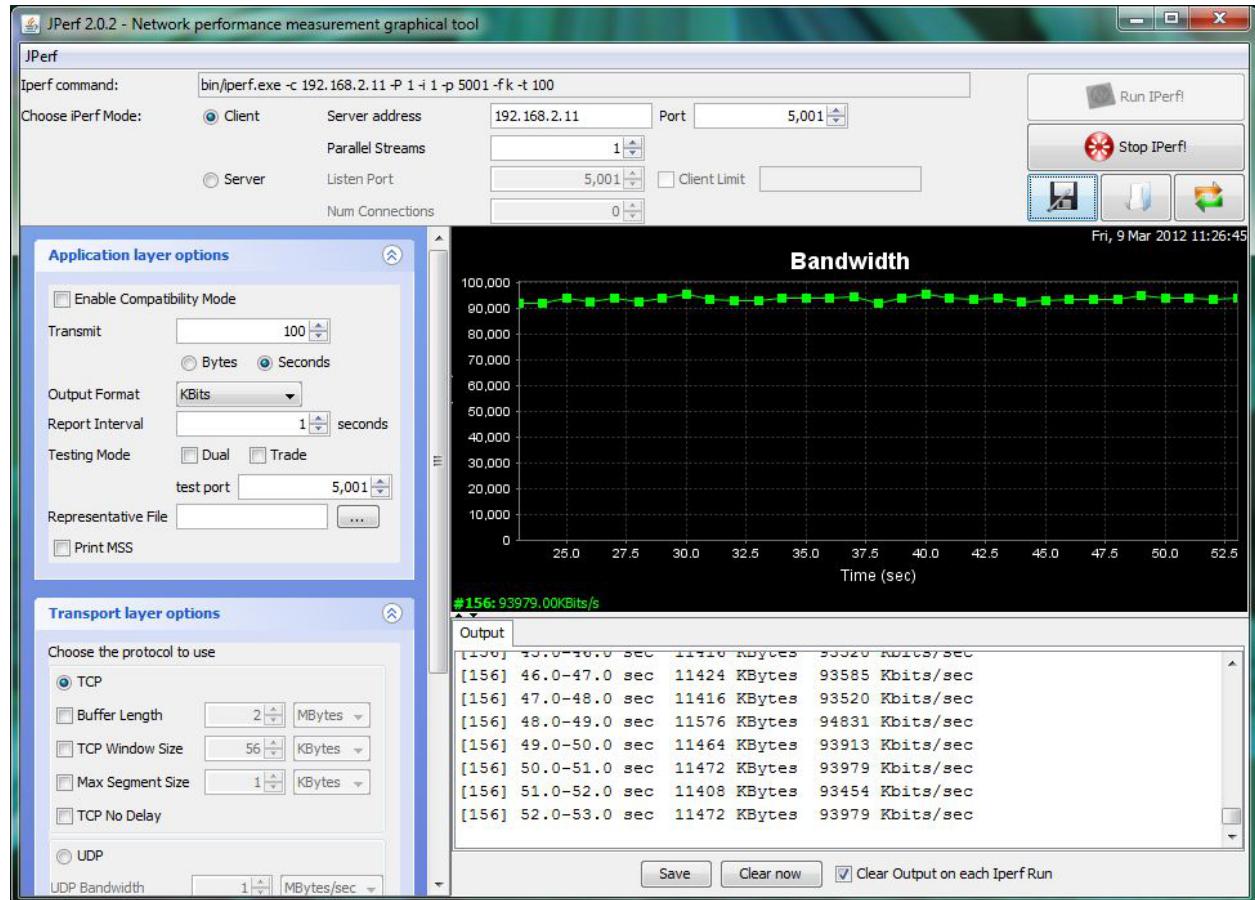


Fig. 24.1: Viewing Bandwidth Statistics Using xjperf

Depending upon the traffic being tested (e.g. the type of share running on your network), you may need to test UDP instead of TCP. To start the iperf server in UDP mode, use **iperf -sDu** as the **u** specifies UDP; the startup message should indicate that the server is listening for UDP datagrams. If you are not sure if the traffic that you wish to test is UDP or TCP, run this command to determine which services are running on the FreeNAS® system:

```
sockstat -4 | more
USER      COMMAND PID      FD PROTO      LOCAL ADDRESS      FOREIGN ADDRESS
root      iperf    4870      6  udp4          *:5001          *:*
```

root	iperf	4842	6	tcp4	*:5001	*:*
www	nginx	4827	3	tcp4	127.0.0.1:15956	127.0.0.1:9042
www	nginx	4827	5	tcp4	192.168.2.11:80	192.168.2.26:56964
www	nginx	4827	7	tcp4	*:80	*:*
root	sshd	3852	5	tcp4	*:22	*:*
root	python	2503	5	udp4	*:*	*:*
root	mountd	2363	7	udp4	*:812	*:*
root	mountd	2363	8	tcp4	*:812	*:*
root	rpcbind	2359	9	udp4	*:111	*:*
root	rpcbind	2359	10	udp4	*:886	*:*
root	rpcbind	2359	11	tcp4	*:111	*:*
root	nginx	2044	7	tcp4	*:80	*:*
root	python	2029	3	udp4	*:*	*:*
root	python	2029	4	tcp4	127.0.0.1:9042	*:*
root	python	2029	7	tcp4	127.0.0.1:9042	127.0.0.1:15956
root	ntpd	1548	20	udp4	*:123	*:*
root	ntpd	1548	22	udp4	192.168.2.11:123	*:*
root	ntpd	1548	25	udp4	127.0.0.1:123	*:*
root	syslogd	1089	6	udp4	127.0.0.1:514	*:*

When you are finished testing, either type **killall iperf** or close Shell to terminate the iperf server process.

24.2 Netperf

Netperf is a benchmarking utility that can be used to measure the performance of unidirectional throughput and end-to-end latency.

Before you can use the **netperf** command, you must start its server process using this command:

```
netserver
Starting netserver with host 'IN(6)ADDR_ANY' port '12865' and family AF_UNSPEC
```

The following command will display the available options for performing tests with the **netperf** command. The [Netperf Manual](#) describes each option in more detail and explains how to perform many types of tests. It is the best reference for understanding how each test works and how to interpret your results. When you are finished with your tests, type **killall netserver** to stop the server process.

```
netperf -h |more
Usage: netperf [global options] -- [test options]
Global options:
  -a send,recv      Set the local send,recv buffer alignment
  -A send,recv      Set the remote send,recv buffer alignment
  -B brandstr       Specify a string to be emitted with brief output
  -c [cpu_rate]     Report local CPU usage
  -C [cpu_rate]     Report remote CPU usage
  -d               Increase debugging output
  -D [secs,units] * Display interim results at least every secs seconds
                     using units as the initial guess for units per second
  -f G|M|K|g|m|k   Set the output units
  -F fill_file      Pre-fill buffers with data from fill_file
  -h               Display this text
  -H name|ip,fam * Specify the target machine and/or local ip and family
  -i max,min        Specify the max and min number of iterations (15,1)
  -I lvl[,intvl]   Specify confidence level (95 or 99) (99)
                   and confidence interval in percentage (10)
  -j               Keep additional timing statistics
```

-l testlen	Specify test duration (>0 secs) (<0 bytes trans)
-L name ip,fam *	Specify the local ip name and address family
-o send,recv	Set the local send,recv buffer offsets
-O send,recv	Set the remote send,recv buffer offset
-n numcpu	Set the number of processors for CPU util
-N	Establish no control connection, do 'send' side only
-p port,lport*	Specify netserver port number and/or local port
-P 0 1	Don't/Do display test headers
-r	Allow confidence to be hit on result only
-s seconds	Wait seconds between test setup and test start
-S	Set SO_KEEPALIVE on the data connection
-t testname	Specify test to perform
-T lcpu,rcpu	Request netperf/netserver be bound to local/remote cpu
-v verbosity	Specify the verbosity level
-W send,recv	Set the number of send,recv buffers
-v level	Set the verbosity level (default 1, min 0)
-V	Display the netperf version and exit

For those options taking two parms, at least one must be specified; specifying one value without a comma will set both parms to that value, specifying a value with a leading comma will set just the second parm, a value with a trailing comma will set just the first. To set each parm to unique values, specify both and separate them with a comma.

For these options taking two parms, specifying one value with no comma will only set the first parms and will leave the second at the default value. To set the second value it must be preceded with a comma or be a comma-separated pair. This is to retain previous netperf behaviour.

24.3 IOzone

IOzone is a disk and filesystem benchmarking tool. It can be used to test file I/O performance for the following operations: read, write, re-read, re-write, read backwards, read strided, fread, fwrite, random read, pread, mmap, aio_read, and aio_write.

FreeNAS® ships with IOzone, meaning that it can be run from Shell. When using IOzone on FreeNAS®, **cd** to a directory in a volume that you have permission to write to, otherwise you will get an error about being unable to write the temporary file.

Before using IOzone, read through the [IOzone documentation PDF](#) as it describes the tests, the many command line switches, and how to interpret your results.

If you have never used this tool before, these resources provide good starting points on which tests to run, when to run them, and how to interpret the results:

- [How To Measure Linux Filesystem I/O Performance With iozone](#)
- [Analyzing NFS Client Performance with IOzone](#)
- [10 iozone Examples for Disk I/O Performance Measurement on Linux](#)

You can receive a summary of the available switches by typing the following command. As you can see from the number of options, IOzone is comprehensive and it may take some time to learn how to use the tests effectively.

Starting with version 9.2.1, FreeNAS® enables compression on newly created ZFS pools by default. Since IOzone creates test data that is compressible, this can skew test results. To configure IOzone to generate incompressible test data, include the options **-+w 1 -+y 1 -+C 1**.

Alternatively, consider temporarily disabling compression on the ZFS pool or dataset when running IOzone benchmarks.

Note: If you prefer to visualize the collected data, scripts are available to render IOzone's output in Gnuplot.

```
iozone -h | more
iozone: help mode
Usage: iozone[-s filesize_Kb] [-r record_size_Kb] [-f [path]filename] [-h]
      [-i test] [-E] [-p] [-a] [-A] [-z] [-Z] [-m] [-M] [-t children]
      [-l min_number_procs] [-u max_number_procs] [-v] [-R] [-x] [-o]
      [-d microseconds] [-F path1 path2...] [-V pattern] [-j stride]
      [-T] [-C] [-B] [-D] [-G] [-I] [-H depth] [-k depth] [-U mount_point]
      [-S cache_size] [-O] [-L cacheline_size] [-K] [-g maxfilesize_Kb]
      [-n minfilesize_Kb] [-N] [-Q] [-P start_cpu] [-e] [-c] [-b Excel.xls]
      [-J milliseconds] [-X write_telemetry_filename] [-w] [-W]
      [-Y read_telemetry_filename] [-y minrecsize_Kb] [-q maxrecsize_Kb]
      [-+u] [-+m cluster_filename] [-+d] [-+x multiplier] [-+p # ]
      [-+r] [-+t] [-+X] [-+Z] [-+w percent dedupable] [-+y percent_interior_
→dedup]
      [-+C percent_dedup_within]
-a Auto mode
-A Auto2 mode
-b Filename Create Excel worksheet file
-B Use mmap() files
-c Include close in the timing calculations
-C Show bytes transferred by each child in throughput testing
-d # Microsecond delay out of barrier
-D Use msync(MS_ASYNC) on mmap files
-e Include flush (fsync,fflush) in the timing calculations
-E Run extension tests
-f filename to use
-F filenames for each process/thread in throughput test
-g # Set maximum file size (in Kbytes) for auto mode (or #m or #g)
-G Use msync(MS_SYNC) on mmap files
-h help
-H # Use POSIX async I/O with # async operations
-i # Test to run (0=write/rewrite, 1=read/re-read, 2=random-read/write
     3=Read-backwards, 4=Re-write-record, 5=stride-read, 6=fwrite/re-fwrite
     7=fread/Re-fread, 8=random_mix, 9=pwrite/Re-pwrite, 10=pread/Re-pread
     11=pwritev/Re-pwritev, 12=preadv/Re-preadv
-I Use VxFS VX_DIRECT, O_DIRECT,or O_DIRECTIO for all file operations
-j # Set stride of file accesses to (# * record size)
-J # milliseconds of compute cycle before each I/O operation
-k # Use POSIX async I/O (no bcopy) with # async operations
-K Create jitter in the access pattern for readers
-l # Lower limit on number of processes to run
-L # Set processor cache line size to value (in bytes)
-m Use multiple buffers
-M Report uname -a output
-n # Set minimum file size (in Kbytes) for auto mode (or #m or #g)
-N Report results in microseconds per operation
-o Writes are synch (O_SYNC)
-O Give results in ops/sec.
-p Purge on
-P # Bind processes/threads to processors, starting with this cpu
-q # Set maximum record size (in Kbytes) for auto mode (or #m or #g)
-Q Create offset/latency files
-r # record size in Kb
or -r #k .. size in Kb
```

```

or -r #m .. size in Mb
or -r #g .. size in Gb
-R Generate Excel report
-s # file size in Kb
or -s #k .. size in Kb
or -s #m .. size in Mb
or -s #g .. size in Gb
-S # Set processor cache size to value (in Kbytes)
-t # Number of threads or processes to use in throughput test
-T Use POSIX pthreads for throughput tests
-u # Upper limit on number of processes to run
-U Mount point to remount between tests
-v version information
-V # Verify data pattern write/read
-w Do not unlink temporary file
-W Lock file when reading or writing
-x Turn off stone-walling
-X filename Write telemetry file. Contains lines with (offset reclen_
→compute_time) in ascii
-y # Set minimum record size (in Kbytes) for auto mode (or #m or #g)
-Y filename Read telemetry file. Contains lines with (offset reclen compute_
→time) in ascii
-z Used in conjunction with -a to test all possible record sizes
-Z Enable mixing of mmap I/O and file I/O
-+E Use existing non-Iozone file for read-only testing
-+K Sony special. Manual control of test 8.
-+m Cluster_filename Enable Cluster testing
-+d File I/O diagnostic mode. (To troubleshoot a broken file I/O subsystem)
-+u Enable CPU utilization output (Experimental)
-+x # Multiplier to use for incrementing file and record sizes
-+p # Percentage of mix to be reads
-+r Enable O_RSYNC|O_SYNC for all testing.
-+t Enable network performance test. Requires -+m
-+n No retests selected.
-+k Use constant aggregate data set size.
-+q Delay in seconds between tests.
-+l Enable record locking mode.
-+L Enable record locking mode, with shared file.
-+B Sequential mixed workload.
-+A # Enable madvise. 0 = normal, 1=random, 2=sequential 3=dontneed,_
→4=willneed
-+N Do not truncate existing files on sequential writes.
-+S # Dedup-able data is limited to sharing within each numerically_
→identified file set
-+V Enable shared file. No locking.
-+X Enable short circuit mode for filesystem testing ONLY
    ALL Results are NOT valid in this mode.
-+Z Enable old data set compatibility mode. WARNING.. Published
    hacks may invalidate these results and generate bogus, high values for_
→results.
-+w ## Percent of dedup-able data in buffers.
-+y ## Percent of dedup-able within & across files in buffers.
-+c ## Percent of dedup-able within & not across files in buffers.
-+H Hostname Hostname of the PIT server.
-+P Service Service of the PIT server.
-+z Enable latency histogram logging.

```

24.4 arcstat

Arcstat is a script that prints out ZFS ARC statistics. Originally it was a perl script created by Sun. That perl script was ported to FreeBSD and was then ported as a Python script for use on FreeNAS®.

Watching ARC hits/misses and percentages will provide an indication of how well your ZFS pool is fetching from the ARC rather than using disk I/O. Ideally, you want as many things fetching from cache as possible. Keep your load in mind as you review the stats. For random reads, expect a miss and having to go to disk to fetch the data. For cached reads, expect it to pull out of the cache and have a hit.

Like all cache systems, the ARC takes time to fill with data. This means that it will have a lot of misses until the pool has been in use for a while. If there continues to be lots of misses and high disk I/O on cached reads, there is cause to investigate further and tune the system.

The [FreeBSD ZFS Tuning Guide](#) provides some suggestions for commonly tuned **sysctl** values. It should be noted that performance tuning is more of an art than a science and that any changes you make will probably require several iterations of tune and test. Be aware that what needs to be tuned will vary depending upon the type of workload and that what works for one person's network may not benefit yours.

In particular, the value of pre-fetching depends upon the amount of memory and the type of workload, as seen in these two examples:

- Understanding ZFS: Prefetch
- ZFS prefetch algorithm can cause performance drawbacks

FreeNAS® provides two command line scripts which can be manually run from [Shell](#):

- **arc_summary.py**: provides a summary of the statistics
- **arcstat.py**: used to watch the statistics in real time

The advantage of these scripts is that they can be used to provide real time (right now) information, whereas the current GUI reporting mechanism is designed to only provide graphs charted over time.

This [forum post](#) demonstrates some examples of using these scripts with hints on how to interpret the results.

To view the help for arcstat.py:

```
arcstat.py -h
Usage: arcstat [-hv] [-f fields] [-o file] [-s string] [interval [count]]
-h: Print this help message
-v: List all possible field headers and definitions
-x: Print extended stats
-f: Specify specific fields to print (see -v)
-o: Redirect output to the specified file
-s: Override default field separator with custom character or string

Examples:
arcstat -o /tmp/a.log 2 10
arcstat -s "," -o /tmp/a.log 2 10
arcstat -v
arcstat -f time,hit%,dh%,ph%,mh% 1
```

To view ARC statistics in real time, specify an interval and a count. This command will display every 1 second for a count of five.

```
arcstat.py 1 5
    time   read  miss  miss%   dmis   dm%   pmis   pm%   mmis   mm%   arczs      c
06:19:03      7      0      0      0      0      0      0      0      0     153M   6.6G
06:19:04     257      0      0      0      0      0      0      0      0     153M   6.6G
```

06:19:05	193	0	0	0	0	0	0	0	153M	6.6G
06:19:06	193	0	0	0	0	0	0	0	153M	6.6G
06:19:07	255	0	0	0	0	0	0	0	153M	6.6G

Table 24.1 briefly describes the columns in the output.

Table 24.1: arcstat Column Descriptions

Column	Description
read	total ARC accesses/second
miss	ARC misses/second
miss%	ARC miss percentage
dmis	demand data misses/second
dm%	demand data miss percentage
pmis	prefetch misses per second
pm%	prefetch miss percentage
mmis	metadata misses/second
mm%	metadata miss percentage
arcsz	arc size
c	arc target size

To receive a summary of statistics, use:

```
arcsummary.py
System Memory:
    2.36% 93.40 MiB Active,      8.95% 353.43 MiB Inact
    8.38% 330.89 MiB Wired,      0.15% 5.90 MiB Cache
    80.16% 3.09 GiB Free,        0.00% 0 Bytes Gap
    Real Installed:              4.00 GiB
    Real Available:              99.31% 3.97 GiB
    Real Managed:                97.10% 3.86 GiB
    Logical Total:                4.00 GiB
    Logical Used:                13.93% 570.77 MiB
    Logical Free:                 86.07% 3.44 GiB
Kernel Memory:
    Data:                         69.91% 61.25 MiB
    Text:                          30.09% 26.37 MiB
Kernel Memory Map:
    Size:                          5.11% 201.70 MiB
    Free:                          94.89% 3.66 GiB
ARC Summary: (HEALTHY)
    Storage pool Version:          5000
    Filesystem Version:             5
    Memory Throttle Count:          0
ARC Misc:
    Deleted:                      8
    Mutex Misses:                  0
    Evict Skips:                   0
ARC Size:
    Target Size: (Adaptive)       100.00% 2.86 GiB
    Min Size (Hard Limit):         12.50% 365.69 MiB
    Max Size (High Water):          8:1   2.86 GiB
ARC Size Breakdown:
    Recently Used Cache Size:     50.00% 1.43 GiB
    Frequently Used Cache Size:    50.00% 1.43 GiB
ARC Hash Breakdown:
    Elements Max:                  5.90k
```

Elements Current:	100.00%	5.90k
Collisions:	72	
Chain Max:	1	
Chains:	23	
ARC Total accesses:		954.06k
Cache Hit Ratio:	99.18%	946.25k
Cache Miss Ratio:	0.82%	7.81k
Actual Hit Ratio:	98.84%	943.00k
Data Demand Efficiency:	99.20%	458.77k
CACHE HITS BY CACHE LIST:		
Anonymously Used:	0.34%	3.25k
Most Recently Used:	3.73%	35.33k
Most Frequently Used:	95.92%	907.67k
Most Recently Used Ghost:	0.00%	0
Most Frequently Used Ghost:	0.00%	0
CACHE HITS BY DATA TYPE:		
Demand Data:	48.10%	455.10k
Prefetch Data:	0.00%	0
Demand Metadata:	51.56%	487.90k
Prefetch Metadata:	0.34%	3.25k
CACHE MISSES BY DATA TYPE:		
Demand Data:	46.93%	3.66k
Prefetch Data:	0.00%	0
Demand Metadata:	49.76%	3.88k
Prefetch Metadata:	3.30%	258
ZFS Tunable (sysctl):		
kern.maxusers		590
vm.kmem_size		4141375488
vm.kmem_size_scale		1
vm.kmem_size_min		0
vm.kmem_size_max		1319413950874
vfs.zfs.vol.unmap_enabled		1
vfs.zfs.vol.mode		2
vfs.zfs.sync_pass_rewrite		2
vfs.zfs.sync_pass_dont_compress		5
vfs.zfs.sync_pass_deferred_free		2
vfs.zfs.zio.exclude_metadata		0
vfs.zfs.zio.use_uma		1
vfs.zfs.cache_flush_disable		0
vfs.zfs.zil_replay_disable		0
vfs.zfs.version.zpl		5
vfs.zfs.version.spa		5000
vfs.zfs.version.acl		1
vfs.zfs.version.ioctl		5
vfs.zfs.debug		0
vfs.zfs.super_owner		0
vfs.zfs.min_auto_ashift		9
vfs.zfs.max_auto_ashift		13
vfs.zfs.vdev.write_gap_limit		4096
vfs.zfs.vdev.read_gap_limit		32768
vfs.zfs.vdev.aggregation_limit		131072
vfs.zfs.vdev.trim_max_active		64
vfs.zfs.vdev.trim_min_active		1
vfs.zfs.vdev.scrub_max_active		2
vfs.zfs.vdev.scrub_min_active		1
vfs.zfs.vdev.async_write_max_active		10
vfs.zfs.vdev.async_write_min_active		1
vfs.zfs.vdev.async_read_max_active		3

```

vfs.zfs.vdev.async_read_min_active      1
vfs.zfs.vdev.sync_write_max_active    10
vfs.zfs.vdev.sync_write_min_active    10
vfs.zfs.vdev.sync_read_max_active     10
vfs.zfs.vdev.sync_read_min_active     10
vfs.zfs.vdev.max_active              1000
vfs.zfs.vdev.async_write_active_max_dirty_percent 60
vfs.zfs.vdev.async_write_active_min_dirty_percent 30
vfs.zfs.vdev.mirror.non_rotating_seek_incl
vfs.zfs.vdev.mirror.non_rotating_inc   0
vfs.zfs.vdev.mirror.rotating_seek_offset 1048576
vfs.zfs.vdev.mirror.rotating_seek_inc  5
vfs.zfs.vdev.mirror.rotating_inc       0
vfs.zfs.vdev.trim_on_init             1
vfs.zfs.vdev.larger_ashift_minimal   0
vfs.zfs.vdev.bio_delete_disable      0
vfs.zfs.vdev.bio_flush_disable       0
vfs.zfs.vdev.cache.bshift            16
vfs.zfs.vdev.cache.size              0
vfs.zfs.vdev.cache.max               16384
vfs.zfs.vdev.metaslabs_per_vdev      200
vfs.zfs.vdev.trim_max_pending        10000
vfs.zfs.txg.timeout                 5
vfs.zfs.trim.enabled                1
vfs.zfs.trim.max_interval           1
vfs.zfs.trim.timeout                30
vfs.zfs.trim.txg_delay              32
vfs.zfs.space_map_blkSz             4096
vfs.zfs.spa_slop_shift              5
vfs.zfs.spa_asize_inflation         24
vfs.zfs.deadman_enabled             1
vfs.zfs.deadman_checktime_ms        5000
vfs.zfs.deadman_synctime_ms         1000000
vfs.zfs.recover                     0
vfs.zfs.spa_load_verify_data        1
vfs.zfs.spa_load_verify_metadata    1
vfs.zfs.spa_load_verify_maxinflight 10000
vfs.zfs.check_hostid                1
vfs.zfs.mg_fragmentation_threshold  85
vfs.zfs.mg_noalloc_threshold        0
vfs.zfs.condense_pct                200
vfs.zfs.metaslab.bias_enabled       1
vfs.zfs.metaslab.lba_weighting_enabled 1
vfs.zfs.metaslab.fragmentation_factor_enabled 1
vfs.zfs.metaslab.preload_enabled    1
vfs.zfs.metaslab.preload_limit      3
vfs.zfs.metaslab.unload_delay       8
vfs.zfs.metaslab.load_pct           50
vfs.zfs.metaslab.min_alloc_size     33554432
vfs.zfs.metaslab.df_free_pct        4
vfs.zfs.metaslab.df_alloc_threshold 131072
vfs.zfs.metaslab.debug_unload      0
vfs.zfs.metaslab.debug_load         0
vfs.zfs.metaslab.fragmentation_threshold 70
vfs.zfs.metaslab.gang_bang          16777217
vfs.zfs.free_bpobj_enabled          1
vfs.zfs.free_max_blocks             18446744073709551615
vfs.zfs.no_scrub_prefetch          0

```

vfs.zfs.no_scrub_io	0
vfs.zfs.resilver_min_time_ms	3000
vfs.zfs.free_min_time_ms	1000
vfs.zfs.scan_min_time_ms	1000
vfs.zfs.scan_idle	50
vfs.zfs.scrub_delay	4
vfs.zfs.resilver_delay	2
vfs.zfs.top_maxinflight	32
vfs.zfs.delay_scale	500000
vfs.zfs.delay_min_dirty_percent	60
vfs.zfs.dirty_data_sync	67108864
vfs.zfs.dirty_data_max_percent	10
vfs.zfs.dirty_data_max_max	4294967296
vfs.zfs.dirty_data_max	426512793
vfs.zfs.max_recordsize	1048576
vfs.zfs.zfetch.array_rd_sz	1048576
vfs.zfs.zfetch.max_distance	8388608
vfs.zfs.zfetch.min_sec_reap	2
vfs.zfs.zfetch.max_streams	8
vfs.zfs.prefetch_disable	1
vfs.zfs.mdcomp_disable	0
vfs.zfs.nopwrite_enabled	1
vfs.zfs.dedup.prefetch	1
vfs.zfs.l2c_only_size	0
vfs.zfs.mfu_ghost_data_lsize	0
vfs.zfs.mfu_ghost_metadata_lsize	0
vfs.zfs.mfu_ghost_size	0
vfs.zfs.mfu_data_lsize	26300416
vfs.zfs.mfu_metadata_lsize	1780736
vfs.zfs.mfu_size	29428736
vfs.zfs.mru_ghost_data_lsize	0
vfs.zfs.mru_ghost_metadata_lsize	0
vfs.zfs.mru_ghost_size	0
vfs.zfs.mru_data_lsize	122090496
vfs.zfs.mru_metadata_lsize	2235904
vfs.zfs.mru_size	139389440
vfs.zfs.anon_data_lsize	0
vfs.zfs.anon_metadata_lsize	0
vfs.zfs.anon_size	163840
vfs.zfs.l2arc_norw	1
vfs.zfs.l2arc_feed_again	1
vfs.zfs.l2arc_noprefetch	1
vfs.zfs.l2arc_feed_min_ms	200
vfs.zfs.l2arc_feed_secs	1
vfs.zfs.l2arc_headroom	2
vfs.zfs.l2arc_write_boost	8388608
vfs.zfs.l2arc_write_max	8388608
vfs.zfs.arc_meta_limit	766908416
vfs.zfs.arc_free_target	7062
vfs.zfs.arc_shrink_shift	7
vfs.zfs.arc_average_blocksize	8192
vfs.zfs.arc_min	383454208
vfs.zfs.arc_max	3067633664

When reading the tunable values, 0 means no, 1 typically means yes, and any other number represents a value. To receive a brief description of a “sysctl” value, use **sysctl -d**. For example:

```
sysctl -d vfs.zfs.zio.use_uma
vfs.zfs.zio.use_uma: Use uma(9) for ZIO allocations
```

The ZFS tunables require a fair understanding of how ZFS works, meaning that you will be reading man pages and searching for the meaning of acronyms you are unfamiliar with. **Do not change a tunable's value without researching it first.** If the tunable takes a numeric value (rather than 0 for no or 1 for yes), do not make one up. Instead, research examples of beneficial values that match your workload.

If you decide to change any of the ZFS tunables, continue to monitor the system to determine the effect of the change. It is recommended that you test your changes first at the command line using `sysctl`. For example, to disable pre-fetch (i.e. change disable to 1 or yes):

```
sysctl vfs.zfs.prefetch_disable=1
vfs.zfs.prefetch_disable: 0 -> 1
```

The output will indicate the old value followed by the new value. If the change is not beneficial, change it back to the original value. If the change turns out to be beneficial, you can make it permanent by creating a `sysctl` using the instructions in [Tunables](#).

24.5 tw_cli

FreeNAS® includes the `tw_cli` command line utility for providing controller, logical unit, and drive management for AMCC/3ware ATA RAID Controllers. The supported models are listed in the man pages for the `twe(4)` and `twa(4)` drivers.

Before using this command, read its [man page](#) as it describes the terminology and provides some usage examples.

If you type `tw_cli` in Shell, the prompt will change, indicating that you have entered interactive mode where you can run all sorts of maintenance commands on the controller and its arrays.

Alternately, you can specify one command to run. For example, to view the disks in the array:

tw_cli /c0 show								
Unit	UnitType	Status	%RCmpl	%V/I/M	Stripe	Size (GB)	Cache	AVrfy
u0	RAID-6	OK	-	-	256K	5587.88	RiW	ON
u1	SPARE	OK	-	-	-	931.505	-	OFF
u2	RAID-10	OK	-	-	256K	1862.62	RiW	ON
VPort	Status	Unit	Size	Type	Phy	Encl-Slot	Model	
p8	OK	u0	931.51 GB	SAS	-	/c0/e0/slta0	SEAGATE	ST31000640SS
p9	OK	u0	931.51 GB	SAS	-	/c0/e0/slta1	SEAGATE	ST31000640SS
p10	OK	u0	931.51 GB	SAS	-	/c0/e0/slta2	SEAGATE	ST31000640SS
p11	OK	u0	931.51 GB	SAS	-	/c0/e0/slta3	SEAGATE	ST31000640SS
p12	OK	u0	931.51 GB	SAS	-	/c0/e0/slta4	SEAGATE	ST31000640SS
p13	OK	u0	931.51 GB	SAS	-	/c0/e0/slta5	SEAGATE	ST31000640SS
p14	OK	u0	931.51 GB	SAS	-	/c0/e0/slta6	SEAGATE	ST31000640SS
p15	OK	u0	931.51 GB	SAS	-	/c0/e0/slta7	SEAGATE	ST31000640SS
p16	OK	u1	931.51 GB	SAS	-	/c0/e0/slta8	SEAGATE	ST31000640SS
p17	OK	u2	931.51 GB	SATA	-	/c0/e0/slta9	ST31000340NS	
p18	OK	u2	931.51 GB	SATA	-	/c0/e0/slta10	ST31000340NS	
p19	OK	u2	931.51 GB	SATA	-	/c0/e0/slta11	ST31000340NS	
p20	OK	u2	931.51 GB	SATA	-	/c0/e0/slta15	ST31000340NS	
Name	OnlineState	BBUReady		Status	Volt	Temp	Hours	LastCapTest

bbu	On	Yes	OK	OK	OK	212	03-Jan-2012
-----	----	-----	----	----	----	-----	-------------

Or, to review the event log:

tw_cli /c0 show events		Severity	AEN Message
Ctl	Date		
c0	[Thu Feb 23 2012 14:01:15]	INFO	Battery charging started
c0	[Thu Feb 23 2012 14:03:02]	INFO	Battery charging completed
c0	[Sat Feb 25 2012 00:02:18]	INFO	Verify started: unit=0
c0	[Sat Feb 25 2012 00:02:18]	INFO	Verify started: ↵
↳unit=2,subunit=0			
c0	[Sat Feb 25 2012 00:02:18]	INFO	Verify started: ↵
↳unit=2,subunit=1			
c0	[Sat Feb 25 2012 03:49:35]	INFO	Verify completed: ↵
↳unit=2,subunit=0			
c0	[Sat Feb 25 2012 03:51:39]	INFO	Verify completed: ↵
↳unit=2,subunit=1			
c0	[Sat Feb 25 2012 21:55:59]	INFO	Verify completed: unit=0
c0	[Thu Mar 01 2012 13:51:09]	INFO	Battery health check started
c0	[Thu Mar 01 2012 13:51:09]	INFO	Battery health check completed
c0	[Thu Mar 01 2012 13:51:09]	INFO	Battery charging started
c0	[Thu Mar 01 2012 13:53:03]	INFO	Battery charging completed
c0	[Sat Mar 03 2012 00:01:24]	INFO	Verify started: unit=0
c0	[Sat Mar 03 2012 00:01:24]	INFO	Verify started: ↵
↳unit=2,subunit=0			
c0	[Sat Mar 03 2012 00:01:24]	INFO	Verify started: ↵
↳unit=2,subunit=1			
c0	[Sat Mar 03 2012 04:04:27]	INFO	Verify completed: ↵
↳unit=2,subunit=0			
c0	[Sat Mar 03 2012 04:06:25]	INFO	Verify completed: ↵
↳unit=2,subunit=1			
c0	[Sat Mar 03 2012 16:22:05]	INFO	Verify completed: unit=0
c0	[Thu Mar 08 2012 13:41:39]	INFO	Battery charging started
c0	[Thu Mar 08 2012 13:43:42]	INFO	Battery charging completed
c0	[Sat Mar 10 2012 00:01:30]	INFO	Verify started: unit=0
c0	[Sat Mar 10 2012 00:01:30]	INFO	Verify started: ↵
↳unit=2,subunit=0			
c0	[Sat Mar 10 2012 00:01:30]	INFO	Verify started: ↵
↳unit=2,subunit=1			
c0	[Sat Mar 10 2012 05:06:38]	INFO	Verify completed: ↵
↳unit=2,subunit=0			
c0	[Sat Mar 10 2012 05:08:57]	INFO	Verify completed: ↵
↳unit=2,subunit=1			
c0	[Sat Mar 10 2012 15:58:15]	INFO	Verify completed: unit=0

If you add some disks to the array and they are not showing up in the GUI, try running this command:

```
tw_cli /c0 rescan
```

Use the drives to create units and export them to the operating system. When finished, run **camcontrol rescan all** and they should now be available in the FreeNAS® GUI.

This [forum post](#) contains a handy wrapper script that will notify you of errors.

24.6 MegaCli

MegaCli is the command line interface for the Avago :MegaRAID SAS family of RAID controllers. FreeNAS® also includes the **mfiutil(8)** utility which can be used to configure and manage connected storage devices.

The **MegaCli** command is quite complex with several dozen options. The commands demonstrated in the [Emergency Cheat Sheet](#) can get you started.

24.7 freenas-debug

The FreeNAS® GUI provides an option to save debugging information to a text file using System → Advanced → Save Debug . This debugging information is created by the **freenas-debug** command line utility and a copy of the information is saved to /var/tmp/fndebug .

This command can be run manually from [Shell](#) to gather specific debugging information. To see the available options, type:

```
freenas-debug
usage: /usr/local/bin/freenas-debug <options>
Where options is:
  -e      A list of comma delimited list of email addresses to email the debug_
→log to.
  -a      Dump Active Directory Configuration
  -c      Dump (AD|LDAP) Cache
  -C      Dump CIFS Configuration
  -D      Dump Domain Controller Configuration
  -d      Dump dtrace scripts
  -g      Dump GEOM configuration
  -h      Dump Hardware Configuration
  -I      Dump IPMI Configuration
  -i      Dump iSCSI Configuration
  -j      Dump jails Information
  -l      Dump LDAP Configuration
  -T      Loader Configuration Information
  -n      Dump Network Configuration
  -N      Dump NFS Configuration
  -S      Dump SMART information
  -s      Dump SSL Configuration
  -y      Dump Sysctl Configuration
  -t      Dump System Information
  -v      Dump Boot System File Verification Status and Inconsistencies (if any)
  -z      Dump ZFS configuration
```

For example, when troubleshooting an Active Directory configuration, use:

```
freenas-debug -a
```

24.8 tmux

tmux is a terminal multiplexer which enables a number of :terminals to be created, accessed, and controlled from a single :screen. **tmux** is an alternative to GNU **screen**. Similar to screen, **tmux** can be detached from a screen and continue running in the background, then later reattached. Unlike [Shell](#), **tmux** allows you to have access to a command prompt while still providing access to the graphical administration screens.

To start a session, simply type **tmux**. As seen in Figure 24.2, a new session with a single window opens with a status line at the bottom of the screen. This line shows information on the current session and is used to enter interactive commands.

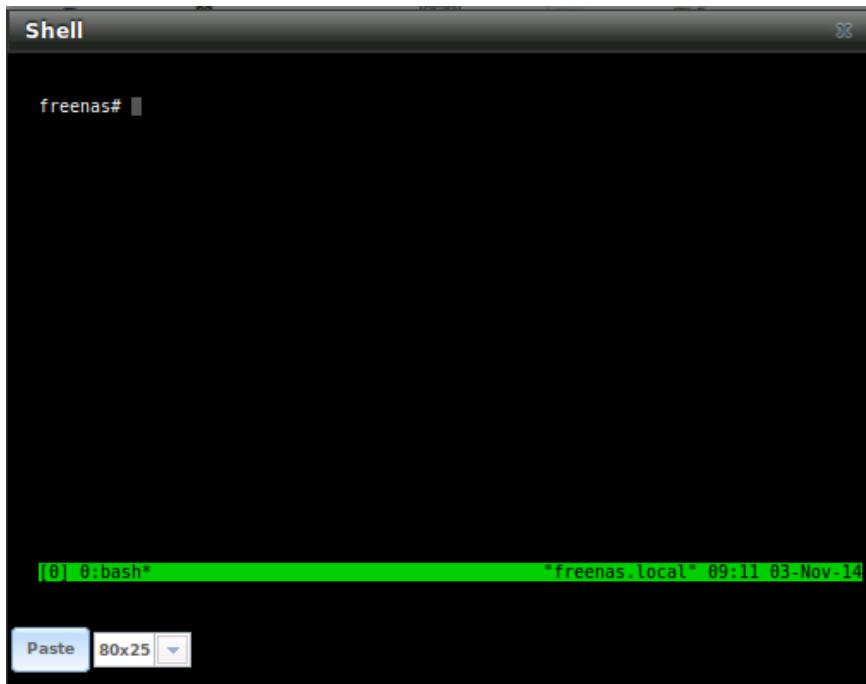


Fig. 24.2: tmux Session

To create a second window, press **Ctrl+b** then **"**. To close a window, type **exit** within the window.

tmux(1) lists all of the key bindings and commands for interacting with **tmux** windows and sessions.

If you close **Shell** while **tmux** is running, it will detach its session. The next time you open Shell, run **tmux attach** to return to the previous session. To leave the **tmux** session entirely, type **exit**. If you have multiple windows running, you will need to **exit** out of each first.

These resources provide more information about using **tmux**:

- A **tmux Crash Course**
- **TMUX - The Terminal Multiplexer**

24.9 Dmidecode

Dmidecode reports hardware information as reported by the system BIOS. Dmidecode does not scan the hardware, it only reports what the BIOS told it to. A sample output can be seen [here](#).

To view the BIOS report, type the command with no arguments:

```
dmidecode | more
```

dmidecode(8) describes the supported strings and types.

CONTRIBUTING TO FREEFAS®

FreeNAS® is an open source community, relying on the input and expertise of its users to help grow and improve FreeNAS®. When you take 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 *Support Resources*.

This section demonstrates how you can:

- *Localize*

25.1 Localize

FreeNAS® uses the open source application [Pootle](#) to manage 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 yet been localized. 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 pootle.freenas.org in a browser, as shown in [Figure 25.1](#).

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 are not translated will appear in English instead of in that language.

To help localize your language, join the [translations mailing list](#), introduce yourself, and point out which languages you can help translate. This will allow you to meet other volunteers as well as keep abreast of any notices or updates that may affect the translations. You will also need to click on the *Register* link to create a Pootle login account.

On the first login to the FreeNAS® Pootle interface, there is a prompt to select your language so that you can access that language's translation whenever you log in. 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 *djang.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 to translate the text. In the example shown in [Figure 25.2](#), a user has selected string number 46 in the German translation. The other strings in the screenshot have already been translated:

Type in the translated text and click the *Submit* button to save the change.

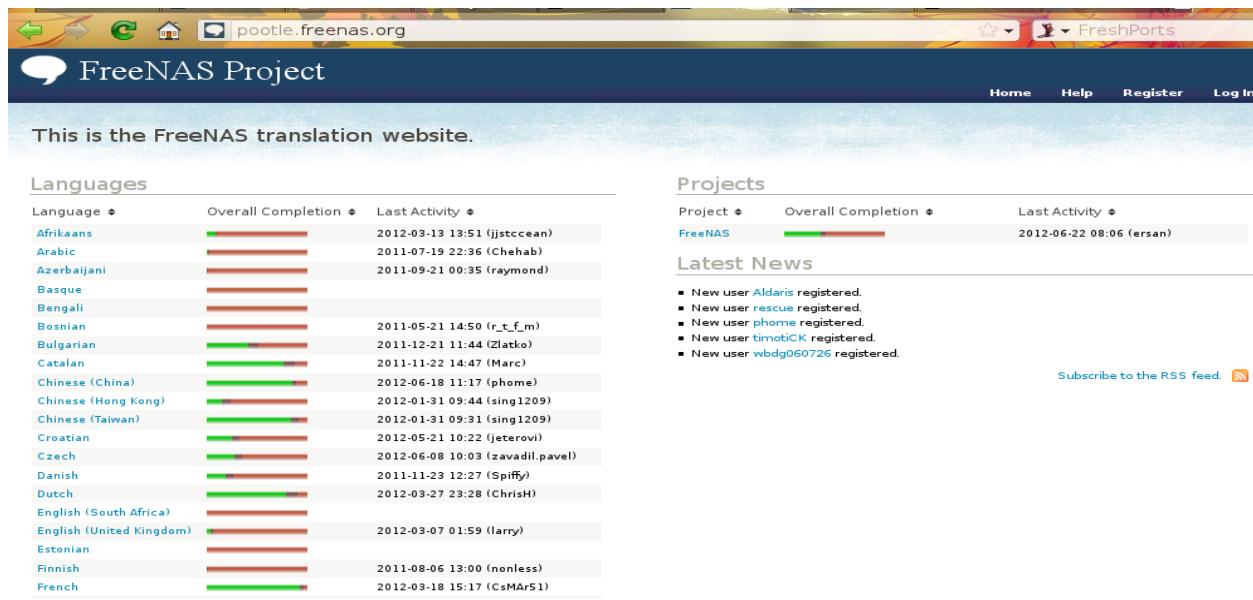


Fig. 25.1: FreeNAS® Localization System

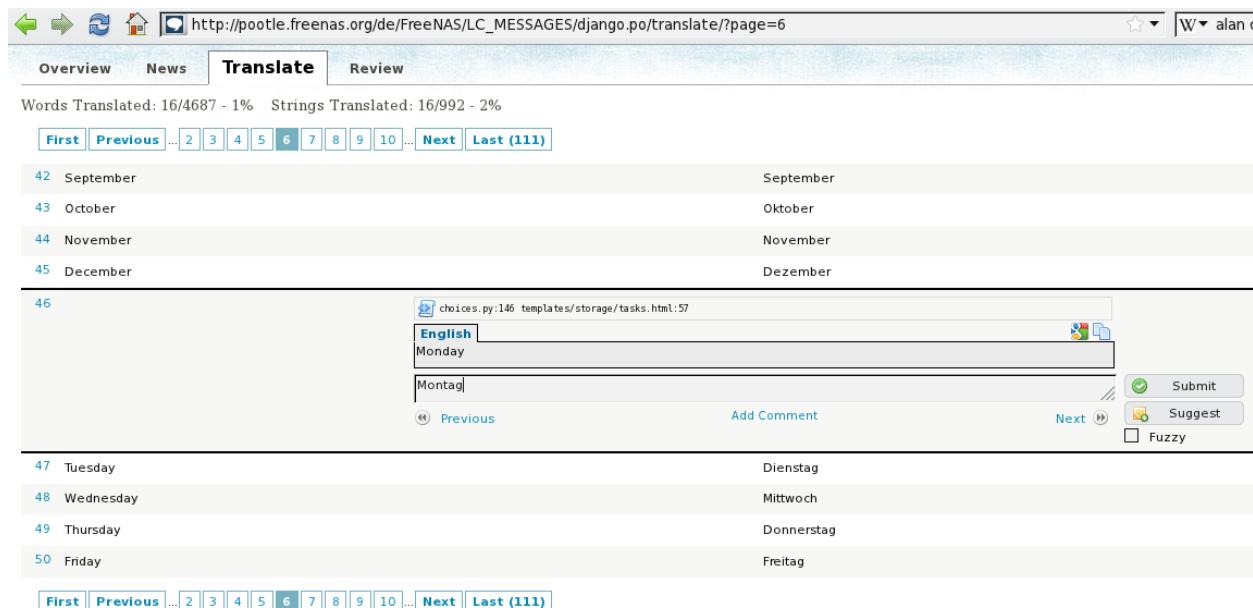


Fig. 25.2: Using the Pootle Interface to Edit a Translation String

CHAPTER
TWENTYSIX

ZFS PRIMER

ZFS is an advanced, modern filesystem that was specifically designed to provide features not available in traditional UNIX filesystems. It was originally developed at Sun with the intent to open source the filesystem so that it could be ported to other operating systems. After the Oracle acquisition of Sun, some of the original ZFS engineers founded [OpenZFS](#) to provided continued, collaborative development of the open source version. To differentiate itself from Oracle ZFS version numbers, OpenZFS uses feature flags. Feature flags are used to tag features with unique names in order to provide portability between OpenZFS implementations running on different platforms, as long as all of the feature flags enabled on the ZFS pool are supported by both platforms. FreeNAS® uses OpenZFS and each new version of FreeNAS® keeps up-to-date with the latest feature flags and OpenZFS bug fixes.

Here is an overview of the features provided by ZFS:

ZFS is a transactional, Copy-On-Write (COW) filesystem. For each write request, a copy is made of the associated disk blocks and all changes are made to the copy rather than to the original blocks. Once the write is complete, all block pointers are changed to point to the new copy. This means that ZFS always writes to free space and most writes will be sequential. When ZFS has direct access to disks, it will bundle multiple read and write requests into transactions; most filesystems cannot do this as they only have access to disk blocks. A transaction either completes or fails, meaning there will never be a [write-hole](#) and a filesystem checker utility is not necessary. Because of the transactional design, as additional storage capacity is added it becomes immediately available for writes; to rebalance the data, one can copy it to re-write the existing data across all available disks. As a 128-bit filesystem, the maximum filesystem or file size is 16 exabytes.

ZFS was designed to be a self-healing filesystem. As ZFS writes data, it creates a checksum for each disk block it writes. As ZFS reads data, it validates the checksum for each disk block it reads. Media errors or “bit rot” can cause data to change, and the checksum no longer matches. When ZFS identifies a disk block checksum error on a pool that is mirrored or uses RAIDZ*, it replaces the corrupted data with the correct data. Since some disk blocks are rarely read, regular scrubs should be scheduled so that ZFS can read all of the data blocks to validate their checksums and correct any corrupted blocks. While multiple disks are required in order to provide redundancy and data correction, ZFS will still provide data corruption detection to a system with one disk. FreeNAS® automatically schedules a monthly scrub for each ZFS pool and the results of the scrub are displayed in [View Volumes](#). Reading scrub results can provide an early indication of possible disk failure.

Unlike traditional UNIX filesystems, **it is not necessary to define partition sizes at filesystem creation time**. Instead, a group of disks (known as a vdev) are built into a ZFS pool. Filesystems are created from the pool as needed. As more capacity is needed, identical vdevs can be striped into the pool. In FreeNAS®, [Volume Manager](#) can be used to create or extend ZFS pools. After a pool is created, it can be divided into dynamically-sized datasets or fixed-size zvols as needed. Datasets can be used to optimize storage for the type of data being stored as permissions and properties such as quotas and compression can be set on a per-dataset level. A zvol is essentially a raw, virtual block device which can be used for applications that need raw-device semantics such as iSCSI device extents.

ZFS supports real-time data compression. Compression happens when a block is written to disk, but only if the written data will benefit from compression. When a compressed block is accessed, it is automatically decompressed. Since compression happens at the block level, not the file level, it is transparent to any applications accessing the

compressed data. By default, ZFS pools made using FreeNAS® version 9.2.1 or later will use the recommended LZ4 compression algorithm.

ZFS provides low-cost, instantaneous snapshots of the specified pool, dataset, or zvol. Due to COW, the initial size of a snapshot is 0 bytes and the size of the snapshot increases over time as changes to the files in the snapshot are written to disk. Snapshots can be used to provide a copy of data at the point in time the snapshot was created. When a file is deleted, its disk blocks are added to the free list; however, the blocks for that file in any existing snapshots are not added to the free list until all referencing snapshots are removed. This means that snapshots provide a clever way of keeping a history of files, should you need to recover an older copy of a file or 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. 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 are stored locally but can also be replicated to a remote ZFS pool. During replication, ZFS does not do a byte-for-byte copy but instead converts a snapshot into a stream of data. This design means that the ZFS pool on the receiving end does not need to be identical and can use a different RAIDZ level, volume size, compression settings, etc.

ZFS boot environments provide a method for recovering from a failed upgrade. In FreeNAS®, a snapshot of the dataset the operating system resides on is automatically taken before an upgrade or a system update. This saved boot environment is automatically added to the GRUB boot loader. Should the upgrade or configuration change fail, simply reboot and select the previous boot environment from the boot menu. Users can also create their own boot environments in `System → Boot` as needed, for example before making configuration changes. This way, the system can be rebooted into a snapshot of the system that did not include the new configuration changes.

ZFS provides a write cache in RAM as well as a ZFS Intent Log ([ZIL](#)). The ZIL is a storage area that temporarily holds *synchronous* writes until they are written to the ZFS pool. Adding a fast (low-latency), power-protected SSD as a SLOG (*Separate Log*) device permits much higher performance. This is a necessity for NFS over ESXi, and highly recommended for database servers or other applications that depend on synchronous writes. More detail on SLOG benefits and usage is available in these blog and forum posts:

- [The ZFS ZIL and SLOG Demystified](#)
- [Some insights into SLOG/ZIL with ZFS on FreeNAS®](#)
- [ZFS Intent Log](#)

Synchronous writes are relatively rare with SMB, AFP, and iSCSI, and adding a SLOG to improve performance of these protocols only makes sense in special cases. The `zilstat` utility can be run from [Shell](#) to determine if the system will benefit from a SLOG. See [this website](#) for usage information.

ZFS currently uses 16 GB of space for SLOG. Larger SSDs can be installed, but the extra space will not be used. SLOG devices cannot be shared between pools. Each pool requires a separate SLOG device. Bandwidth and throughput limitations require that a SLOG device must only be used for this single purpose. Do not attempt to add other caching functions on the same SSD, or performance will suffer.

In mission-critical systems, a mirrored SLOG device is highly recommended. Mirrored SLOG devices are *required* for ZFS pools at ZFS version 19 or earlier. ZFS pool version can be checked from the [Shell](#) with `zpool get version poolname`. A version value of - means the ZFS pool is version 5000 (also known as *Feature Flags*) or later.

ZFS provides a read cache in RAM, known as the ARC, to reduce read latency. FreeNAS® adds ARC stats to `top(1)` and includes the `arc_summary.py` and `arcstat.py` tools for monitoring the efficiency of the ARC. If an SSD is dedicated as a cache device, it is known as an [L2ARC](#) and ZFS uses it to store more reads which can increase random read performance. However, adding an L2ARC is **not** a substitute for insufficient RAM as L2ARC needs RAM in order to function. If you do not have enough RAM for a good sized ARC, you will not be increasing performance, and in most cases you will actually hurt performance and could potentially cause system instability. RAM is always faster than disks, so always add as much RAM as possible before determining if the system would benefit from a L2ARC device. If you have a lot of applications that do large amounts of **random** reads, on a dataset small enough to fit into the L2ARC, read performance may be increased by adding a dedicated cache device using [Volume Manager](#). SSD cache devices only help if your active data is larger than system RAM, but small enough that a significant percentage

of it will fit on the SSD. As a general rule of thumb, an L2ARC should not be added to a system with less than 64 GB of RAM and the size of an L2ARC should not exceed 5x the amount of RAM. In some cases, it may be more efficient to have two separate pools: one on SSDs for active data and another on hard drives for rarely used content. After adding an L2ARC, monitor its effectiveness using tools such as [arcstat](#). If you need to increase the size of an existing L2ARC, you can stripe another cache device using [Volume Manager](#). The GUI will always stripe L2ARC, not mirror it, as the contents of L2ARC are recreated at boot. Losing an L2ARC device will not affect the integrity of the pool, but may have an impact on read performance, depending upon the workload and the ratio of dataset size to cache size. Note that a dedicated L2ARC device cannot be shared between ZFS pools.

ZFS was designed to provide redundancy while addressing some of the inherent limitations of hardware RAID such as the write-hole and corrupt data written over time before the hardware controller provides an alert. ZFS provides three levels of redundancy, known as RAIDZ*, where the number after the RAIDZ indicates how many disks per vdev can be lost without losing data. ZFS also supports mirrors, with no restrictions on the number of disks in the mirror. ZFS was designed for commodity disks so no RAID controller is needed. While ZFS can also be used with a RAID controller, it is recommended that the controller be put into JBOD mode so that ZFS has full control of the disks. When determining the type of ZFS redundancy to use, consider whether your goal is to maximize disk space or performance:

- RAIDZ1 maximizes disk space and generally performs well when data is written and read in large chunks (128K or more).
- RAIDZ2 offers better data availability and significantly better mean time to data loss (MTTDL) than RAIDZ1.
- A mirror consumes more disk space but generally performs better with small random reads. For better performance, a mirror is strongly favored over any RAIDZ, particularly for large, uncacheable, random read loads.
- Using more than 12 disks per vdev is not recommended. The recommended number of disks per vdev is between 3 and 9. If you have more disks, use multiple vdevs.
- Some older ZFS documentation recommends that a certain number of disks is needed for each type of RAIDZ in order to achieve optimal performance. On systems using LZ4 compression, which is the default for FreeNAS® 9.2.1 and higher, this is no longer true. See [ZFS RAIDZ stripe width](#), or: [How I Learned to Stop Worrying and Love RAIDZ](#) for details.

These resources can also help you determine the RAID configuration best suited to your storage needs:

- [Getting the Most out of ZFS Pools](#)
- [A Closer Look at ZFS, Vdevs and Performance](#)

Warning: 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 [Periodic Snapshot Tasks](#) and [Replication Tasks](#) if you would like to use replicated ZFS snapshots as part of your backup strategy.

While ZFS provides many benefits, there are some caveats to be aware of:

- At 90% capacity, ZFS switches from performance- to space-based optimization, which has massive performance implications. For maximum write performance and to prevent problems with drive replacement, add more capacity before a pool reaches 80%. If you are using iSCSI, it is recommended to not let the pool go over 50% capacity to prevent fragmentation issues.
- When considering the number of disks to use per vdev, consider the size of the disks and the amount of time required for resilvering, which is the process of rebuilding the vdev. The larger the size of the vdev, the longer the resilvering time. When replacing a disk in a RAIDZ*, it is possible that another disk will fail before the resilvering process completes. If the number of failed disks exceeds the number allowed per vdev for the type of RAIDZ, the data in the pool will be lost. For this reason, RAIDZ1 is not recommended for drives over 1 TB in size.

- It is recommended to use drives of equal sizes when creating a vdev. While ZFS can create a vdev using disks of differing sizes, its capacity will be limited by the size of the smallest disk.

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

- FreeBSD ZFS Tuning Guide
- ZFS Administration Guide
- Becoming a ZFS Ninja (video)
- Slideshow explaining VDev, zpool, ZIL and L2ARC and other newbie mistakes!
- A Crash Course on ZFS
- ZFS: The Last Word in File Systems - Part 1 (video)

CHAPTER TWENTYSEVEN

USING THE API

A REST API is provided to be used as an alternate mechanism for remotely controlling a FreeNAS® system.

REST provides an easy-to-read, HTTP implementation of functions, known as resources, which are available beneath a specified base URL. Each resource is manipulated using the HTTP methods defined in [RFC 2616](#), such as GET, PUT, POST, or DELETE.

As shown in [Figure 27.1](#), an online version of the API is available at api.freenas.org.



Fig. 27.1: API Documentation

The rest of this section shows code examples to illustrate the use of the API.

27.1 A Simple API Example

The `api` directory of the FreeNAS® [github repository](#) contains some API usage examples. This section provides a walk-through of the `newuser.py` script, shown below, as it provides a simple example that creates a user.

A FreeNAS® system running at least version 9.2.0 is required when creating a customized script based on this example. To test the scripts directly on the FreeNAS® system, create a user account and select an existing volume or dataset for the user's *Home Directory*. After creating the user, start the SSH service using *Services* → *Control Services*. That user will now be able to `ssh` to the IP address of the FreeNAS® system to create and run scripts. Alternately, scripts can be tested on any system with the required software installed as shown in the previous section.

To customize this script, copy the contents of this example into a filename that ends in `.py`. The text that is highlighted in red below can be modified in the new version to match the needs of the user being created. The text in black should not be changed. After saving changes, run the script by typing `python scriptname.py`. If all goes well, the new user account will appear in Account → Users → View Users in the FreeNAS® GUI.

Here is the example script with an explanation of the line numbers below it.

```
1 import json
2 import requests
3 r = requests.post(
4     'https://freenas.mydomain/api/v1.0/account/users/',
5     auth=('root', 'freenas'),
6     headers={'Content-Type': 'application/json'},
7     verify=False,
8     data=json.dumps({
9         'bsdusr_uid': '1100',
10        'bsdusr_username': 'myuser',
11        'bsdusr_mode': '755',
12        'bsdusr_creategroup': 'True',
13        'bsdusr_password': '12345',
14        'bsdusr_shell': '/usr/local/bin/bash',
15        'bsdusr_full_name': 'Full Name',
16        'bsdusr_email': 'name@provider.com',
17    })
18 )
19 print r.text
```

Where:

Lines 1-2: import the Python modules used to make HTTP requests and handle data in JSON format.

Line 4: replace `freenas.mydomain` with the `Hostname` value in System → System Information. Note that the script will fail if the machine running it is not able to resolve that hostname. Change `https` to `http` to use HTTP rather than HTTPS to access the FreeNAS® system.

Line 5: replace `freenas` with the password used to access the FreeNAS® system.

Line 7: if you are using HTTPS and want to force validation of the SSL certificate, change `False` to `True`.

Lines 8-16: set the values for the user being created. The `Users` resource describes this in more detail. Allowed parameters are listed in the JSON Parameters section of that resource. Since this resource creates a FreeBSD user, the values entered must be valid for a FreeBSD user account. [Table 27.1](#) summarizes acceptable values. This resource uses JSON, so the boolean values are `True` or `False`.

Table 27.1: JSON Parameters for Users Create Resource

JSON Parameter	Type	Description
bs-dusr_username	string	maximum 32 characters, though a maximum of 8 is recommended for interoperability; can include numerals but cannot include a space
bs-dusr_full_name	string	may contain spaces and uppercase characters
bs-dusr_password	string	can include a mix of upper and lowercase letters, characters, and numbers
bsdusr_uid	integer	by convention, user accounts have an ID greater than 1000 with a maximum allowable value of 65,535
bsdusr_group	integer	if <i>bsdusr_creategroup</i> is set to <i>False</i> , specify the numeric ID of the group to create
bs-dusr_creategroup	boolean	if set to <i>True</i> , a primary group with the same numeric ID as <i>bsdusr_uid</i> will be created automatically
bsdusr_mode	string	sets default numeric UNIX permissions of user's home directory
bsdusr_shell	string	specify full path to a UNIX shell that is installed on the system
bs-dusr_password_disabled	boolean	if set to <i>True</i> , user is not allowed to log in
bsdusr_locked	boolean	if set to <i>True</i> , user is not allowed to log in
bsdusr_sudo	boolean	if set to <i>True</i> , sudo is enabled for the user
bs-dusr_sshpubkey	string	contents of SSH authorized keys file

Note: When using boolean values, JSON returns raw lowercase values but Python uses uppercase values. So use *True* or *False* in Python scripts even though the example JSON responses in the API documentation are displayed as *true* or *false*.

27.2 A More Complex Example

This section provides a walk-through of a more complex example found in the `startup.py` script. Use the searchbar within the API documentation to quickly locate the JSON parameters used here. This example defines a class and several methods to create a ZFS volume, create a ZFS dataset, share the dataset over CIFS, and enable the CIFS service. Responses from some methods are used as parameters in other methods. In addition to the import lines seen in the previous example, two additional Python modules are imported to provide parsing functions for command line arguments:

```
import argparse
import sys
```

It then creates a *Startup* class which is started with the hostname, username, and password provided by the user via the command line:

```
1 class Startup(object):
2     def __init__(self, hostname, user, secret):
3         self._hostname = hostname
4         self._user = user
5         self._secret = secret
6         self._ep = 'http://{:s}/api/v1.0' % hostname
7     def request(self, resource, method='GET', data=None):
```

```
8     if data is None:
9         data =
10        r = requests.request(
11            method,
12            '%s/%s/' % (self._ep, resource),
13            data=json.dumps(data),
14            headers={'Content-Type': "application/json"},
15            auth=(self._user, self._secret),
16        )
17    if r.ok:
18        try:
19            return r.json()
20        except:
21            return r.text
22    raise ValueError(r)
```

A *get_disks* method is defined to get all the disks in the system as a *disk_name* response. The *create_pool* method uses this information to create a ZFS pool named *tank* which is created as a stripe. The *volume_name* and *layout* JSON parameters are described in the “Storage Volume” resource of the API documentation.

```
1 def _get_disks(self):
2     disks = self.request('storage/disk')
3     return [disk['disk_name'] for disk in disks]
4
5 def create_pool(self):
6     disks = self._get_disks()
7     self.request('storage/volume', method='POST', data={
8         'volume_name': 'tank',
9         'layout': [
10             {'vdevtype': 'stripe', 'disks': disks},
11         ],
12     })
```

The *create_dataset* method is defined which creates a dataset named MyShare :

```
1 def create_dataset(self):
2     self.request('storage/volume/tank/datasets', method='POST', data={
3         'name': 'MyShare',
4     })
```

The *create_cifs_share* method is used to share /mnt/tank/MyShare with guest-only access enabled. The *cifs_name*, *cifs_path*, *cifs_guestonly* JSON parameters, as well as the other allowable parameters, are described in the “Sharing CIFS” resource of the API documentation.

```
1 def create_cifs_share(self):
2     self.request('sharing/cifs', method='POST', data={
3         'cifs_name': 'My Test Share',
4         'cifs_path': '/mnt/tank/MyShare',
5         'cifs_guestonly': True
6     })
```

Finally, the *service_start* method enables the CIFS service. The *srv_enable* JSON parameter is described in the Services resource.

```
1 def service_start(self, name):
2     self.request('services/services/%s' % name, method='PUT', data={
3         'srv_enable': True,
```

```
4
5 } )
```


Symbols

802.1Q, 101

A

Add Group, 45
 Add Jail, 231
 Add User, 48
 AFP, 152, 193
 Alert, 265
 API, 294
 Apple Filing Protocol, 152, 193
 arstat, 279
 Autotune, 63

B

bhyve, 248
 Boot Environments, 57
 Burn ISO, 7

C

CA, 71
 Certificate Authority, 71
 Certificates, 73
 Checksum, 7
 CIFS, 169, 207
 Compression, 114
 Configuration Wizard, 38
 Create Dataset, 111
 Create Group, 45
 Create Jail, 231
 Create User, 48
 Cron Jobs, 79

D

DC, 195
 DDNS, 196
 Deduplication, 113
 Delete Group, 47
 Dmidecode, 288
 Domain Controller, 195
 Download, 7
 Dynamic DNS, 196

E

Email, 64
 Encryption, 107
 EtherChannel, 96

F

File Transfer Protocol, 196
 Forums, 269
 freenas-debug, 287
 FTP, 196

G

Getting FreeNAS\ :sup:‘®’, 7
 Groups, 45
 Guide, 263

H

Hardware Recommendations, 4

I

Initial Configuration Wizard, 38
 Install, 9
 Internet Small Computer System Interface, 177
 iohyve, 248
 IOzone, 277
 Iperf, 273
 IRC, 271
 iSCSI, 177
 ISO, 7

J

Jails, 227

L

LACP, 96
 LAGG, 96
 Link Aggregation, 96
 Link Layer Discovery Protocol, 202
 LLDP, 202
 Localize, 289
 Log Out, 256

M

Mailing Lists, 271
MegaCli, 286
Mirroring the Boot Device, 60
Multiple Boot Environments, 57

N

Netperf, 276
Network File System, 159, 203
Network Settings, 89
New Group, 45
New Jail, 231
New User, 48
NFS, 159, 203

P

Periodic Snapshot, 127
phpVirtualBox Template, 244
Plugin, 219
Professional Support, 272

R

Reboot, 257
Remove Group, 47
Replace Failed Drive, 124
Replication, 129
Reporting, 249
RFC
 RFC 2616, 295
 RFC 3721, 180
Route, 101
Rsync, 204
Rsync Tasks, 81

S

S.M.A.R.T., 206
S.M.A.R.T. Tests, 87
Samba, 169, 207
SCP, 215
Scrub, 132
Secure Copy, 215
Secure Shell, 213
Services, 188
Shadow Copies, 176
Shell, 253
Shutdown, 259
Simple Network Management Protocol, 211
SMB, 169, 207
Snapshot, 127
Snapshots, 134
SNMP, 211
SSH, 213
Start Service, 191

Static Route, 101
Stop Service, 191
Support, 76, 261
System Dataset, 64

T

Tasks, 78
TFTP, 215
Time Machine, 156
tmux, 287
Translate, 289
Trivial File Transfer Protocol, 215
Trunking, 101
Tunables, 66
tw_cli, 285

U

Uninterruptible Power Supply, 216
Upgrade, 14
Upgrade ZFS Pool, 19
UPS, 216
USB Stick, 7
Users, 47

V

VirtualBox Jail, 244
VirtualBox Template, 244
Virtualization, 20
VLAN, 101
VM, 20
VMware Snapshot, 136
Volumes, 105

W

WebDAV, 168, 219
Windows File Share, 207
Windows Shares, 169
Wizard, 38

Z

ZVOL, 114