Note: Starting with version 12.0, FreeNAS and TrueNAS are unifying (https://www.ixsystems.com/blog/freenas-truenas-unification/) into “TrueNAS”. Documentation for TrueNAS 12.0 and later releases has been unified and moved to the TrueNAS Documentation Hub (https://www.truenas.com/docs/).

FreeNAS® is © 2011-2020 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 11.3
Copyright © 2011-2020 iXsystems (https://www.ixsystems.com/)
3 Booting
3.1 Obtaining an IP Address

4 Accessing the Web Interface
4.1 Web Interface Troubleshooting

5 Settings
5.1 Change Password
5.2 Preferences
5.2.1 Web Interface Preferences
5.2.2 Themes
5.2.2.1 Create New Themes
5.3 API Documentation
5.4 About

6 Accounts
6.1 Groups
6.2 Users

7 System
7.1 General
7.2 NTP Servers
7.3 Boot
7.3.1 Operating System Device Mirroring
7.4 Advanced
7.4.1 Autotune
7.4.2 Self-Encrypting Drives
7.4.2.1 Deploying SEDs
7.4.2.2 Check SED Functionality
7.4.2.3 Managing SED Passwords and Data
7.5 Email
7.6 System Dataset
7.7 Reporting
7.8 Alert Services
7.9 Alert Settings
7.10 Cloud Credentials
7.11 SSH Connections
7.11.1 Manual Setup
7.11.2 Semi-Automatic Setup
7.12 SSH Keypairs
7.13 Tunables
7.14 Update
7.14.1 Preparing for Updates
7.14.2 Updates and Trains
7.14.3 Checking for Updates
7.14.4 Saving the Configuration File
7.14.5 Applying Updates
7.14.6 Manual Updates
7.14.7 Update in Progress
7.15 CAs
7.16 Certificates
7.16.1 ACME Certificates
7.17 ACME DNS

2.5.6 Upgrading a ZFS Pool
2.6 Virtualization
2.6.1 VirtualBox
2.6.2 VMware ESXi

66
66
66
66
66
66
66
66
78
81
83
84
86
87
87
88
89
90
91
93
94
94
96
97
101
103
104
105
105
108
108
108
109
110
111
111
112
113
116
121
122
10.3 Snapshots ................................................................. 191
  10.3.1 Browsing a Snapshot Collection ................................. 192
  10.3.2 Creating a Single Snapshot ..................................... 193
10.4 VMware-Snapshots .................................................... 194
10.5 Disks ........................................................................ 195
  10.5.1 Replacing a Failed Disk ............................................ 197
  10.5.1.1 Removing a Log or Cache Device .............................. 200
  10.5.2 Replacing Disks to Grow a Pool ................................ 200
10.6 Importing a Disk ........................................................ 201
10.7 Multipaths ............................................................... 202

11 Overprovisioning .......................................................... 203

12 Directory Services .......................................................... 204
  12.1 Active Directory ....................................................... 204
    12.1.1 Leaving the Domain .............................................. 208
    12.1.2 Troubleshooting Tips ............................................ 208
  12.2 LDAP ..................................................................... 209
  12.3 NIS ....................................................................... 212
  12.4 Kerberos Realms ....................................................... 213
  12.5 Kerberos Keytabs ....................................................... 214
  12.6 Kerberos Settings ....................................................... 215

13 Sharing ....................................................................... 216
  13.1 Apple (AFP) Shares ................................................... 217
    13.1.1 Creating AFP Guest Shares ................................... 219
  13.2 Block (iSCSI) ............................................................ 222
    13.2.1 iSCSI Wizard ...................................................... 223
    13.2.2 Target Global Configuration ................................. 224
    13.2.3 Portals .............................................................. 225
    13.2.4 Initiators ........................................................... 226
    13.2.5 Authorized Access .............................................. 227
    13.2.6 Targets ............................................................. 229
    13.2.7 Extents .............................................................. 231
    13.2.8 Associated Targets .............................................. 233
    13.2.9 Connecting to iSCSI ............................................. 234
    13.2.10 Growing LUNs .................................................. 235
      13.2.10.1 Zvol Based LUN .......................................... 235
      13.2.10.2 File Extent Based LUN ................................. 236
  13.3 Unix (NFS) Shares ...................................................... 237
    13.3.1 Example Configuration ......................................... 240
    13.3.2 Connecting to the Share ....................................... 240
      13.3.2.1 From BSD or Linux ....................................... 241
      13.3.2.2 From Microsoft ............................................. 241
      13.3.2.3 From macOS ............................................... 241
    13.3.3 Troubleshooting NFS ........................................... 243
  13.4 WebDAV Shares ........................................................ 244
  13.5 Windows (SMB) Shares .............................................. 246
    13.5.1 Configuring Unauthenticated Access ......................... 252
    13.5.2 Configuring Authenticated Access With Local Users .... 253
    13.5.3 User Quota Administration .................................... 255
    13.5.4 Configuring Shadow Copies .................................. 255
  13.6 Creating Authenticated and Time Machine Shares ............. 255
    13.6.1 Setting SMB and AFP Share Quotas ......................... 257
    13.6.2 Client Time Machine Configuration ......................... 258

14 Services ..................................................................... 259
  14.1 Configure Services .................................................. 259
18.3.3 Disk Devices ................................................................. 336
18.3.4 Raw Files ................................................................. 337
18.3.5 VNC Interface ............................................................ 338

19 Display System Processes 340

20 Shell 341

21 Log Out, Restart, or Shut Down 343
  21.1 Log Out ................................................................. 343
  21.2 Restart ................................................................. 343
  21.3 Shut Down ............................................................ 344

22 Alert 345

23 Task Manager 348

24 Support Resources 349
  24.1 User Guide ............................................................. 349
  24.2 Website and Social Media .......................................... 349
  24.3 Forums ................................................................. 349
  24.4 IRC ....................................................................... 350
  24.5 Videos ................................................................. 350
  24.6 Professional Support .................................................. 351

25 Contributing to FreeNAS® 352
  25.1 Translation ............................................................. 352
    25.1.1 Translate with GitHub ......................................... 353
    25.1.2 Download and Translate Offline ............................. 354
    25.1.3 Translation Pull Requests ..................................... 355

26 Command Line Utilities 356
  26.1 Iperf ................................................................. 356
  26.2 Netperf ............................................................... 359
  26.3 IOzone ............................................................... 360
  26.4 arcstat ............................................................... 362
  26.5 tw_cli ............................................................... 367
  26.6 MegaCli ............................................................. 369
  26.7 freenas-debug ....................................................... 369
  26.8 tmux ................................................................. 370
  26.9 Dmidecode ........................................................... 371
  26.10 Midnight Commander .............................................. 371

27 ZFS Primer 372
  27.1 ZFS Feature Flags .................................................... 375

28 OpenStack Cinder Driver 376

29 VMware Recommendations 377
  29.1 FreeNAS® as a VMware Guest ...................................... 377
  29.2 Hosting VMware Storage with FreeNAS® ......................... 377
  29.3 VAAI for iSCSI ....................................................... 377

30 Using the API 379
  30.1 A Simple API Example ............................................... 380
  30.2 A More Complex Example ........................................... 381
Welcome

This Guide covers the installation and use of FreeNAS® 11.3.

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 (https://github.com/freenas/freenas-docs/blob/master/README.md). 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 (https://creativecommons.org/licenses/by/3.0/). 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.

Asigra Inc. Asigra, the Asigra logo, Asigra Cloud Backup, Recovery is Everything, Recovery Tracker and Attack-Loop are trademarks of Asigra Inc.

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®.

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® 11.3 User Guide uses these typographic conventions:

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

Table 2: FreeNAS® Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADD</td>
<td>Add a new item.</td>
</tr>
<tr>
<td>🌈 (Settings)</td>
<td>Show a settings menu.</td>
</tr>
<tr>
<td>🟢 (Options)</td>
<td>Show an Options menu.</td>
</tr>
<tr>
<td>🌐 (Browse)</td>
<td>Shows an expandable view of system directories.</td>
</tr>
<tr>
<td>⚡ (Power)</td>
<td>Show a power options menu.</td>
</tr>
<tr>
<td>🤝 (Show)</td>
<td>Reveal characters in a password field.</td>
</tr>
<tr>
<td>📮 (Hide)</td>
<td>Hide characters in a password field.</td>
</tr>
<tr>
<td>🔧 (Configure)</td>
<td>Edit settings.</td>
</tr>
<tr>
<td>🚀 (Launch)</td>
<td>Launch a service.</td>
</tr>
<tr>
<td>🧸 (Start)</td>
<td>Start jails.</td>
</tr>
<tr>
<td>⏹️ (Stop)</td>
<td>Stop jails.</td>
</tr>
<tr>
<td>🔄 (Update)</td>
<td>Update jails.</td>
</tr>
<tr>
<td>▼ (Delete)</td>
<td>Delete jails.</td>
</tr>
<tr>
<td>🎉 (Encryption Options)</td>
<td>Encryption options for a pool.</td>
</tr>
<tr>
<td>🌐 (Pin)</td>
<td>Pin a help box to the screen.</td>
</tr>
<tr>
<td>✗ (Close)</td>
<td>Close a help box.</td>
</tr>
</tbody>
</table>
FreeNAS® is an embedded open source network-attached storage (NAS) operating system based on FreeBSD and released under a 2-clause BSD license (https://opensource.org/licenses/BSD-2-Clause). 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 New Features in 11.3

FreeNAS® 11.3 is a feature release, which includes new significant features, many improvements and bug fixes to existing features, and version updates to the operating system, base applications, and drivers. Users are encouraged to Update (page 108) to this release in order to take advantage of these improvements and bug fixes.

Major New Features and Improvements

The replication framework has been redesigned, adding new back-end systems, files, and screen options to the Replication system (page 146) and Periodic Snapshot Tasks (page 136). The redesign adds these features:

- New peers/credentials API for creating and managing credentials. The SSH Connections (page 101) and SSH Keypairs (page 105) screens have been added and a wizard makes it easy to generate new keypairs. Existing SFTP and SSH replication keys created in 11.2 or earlier will be automatically added as entries to SSH Keypairs (page 105) during upgrade.
- New transport API adds netcat support, for greatly improved speed of transfer.
- Snapshot creation has been decoupled from replication tasks, allowing replication of manually created snapshots.
- The ability to use custom names for snapshots.
- Configurable snapshot retention on the remote side.
- A new replication wizard makes it easy to configure replication scenarios, including local replication and replication to systems running legacy replication (pre-11.3).
- Replication is resumable and failed replication tasks will automatically try to resume from a previous checkpoint. Each task has its own log which can be accessed from the State column.
- Replications run in parallel as long as they do not conflict with each other. Completion time depends on the number and size of snapshots and the bandwidth available between the source and destination computers.

Network interface management (page 159) has been redesigned to streamline management of both physical and virtual interfaces using one screen. VLANs and LAGGs are now classified as interface types and support for the Bridge interface (page 161) type has been added. The addressing details for all physical interfaces, including DHCP, are now displayed but are read-only if the interface is a member of a LAGG. When applying interface changes, the web interface provides a window to cancel the change and revert to the previous network configuration. A new MTU field makes it easier to set the MTU as it no longer has to be typed in as an Auxiliary Parameter.
Automatic Certificate Management Environment (ACME) (https://ietf-wg-acme.github.io/acme/draft-ietf-acme-acme.html) support has been added. ACME simplifies the process of issuing and renewing certificates using a set of DNS challenges to verify a user is the owner of the domain. While the new API supports the addition of multiple DNS authenticators, support for Amazon Route 53 (https://aws.amazon.com/route53/) has been added as the initial implementation. The ACME DNS (page 122) screen is used for authenticator configuration which adds the ACME Certificates (page 121) option for Certificate Signing Requests. Once configured, FreeNAS® will automatically renew ACME certificates as they expire.

Support for collecting daily anonymous usage statistics has been added. Collected non-identifying data includes hardware information such as CPU type, number and size of disks, and configured NIC types as well as an indication of which services, types of shares, and Plugins are configured. The collected data will assist in determining where to best focus engineering and testing efforts. Collection is enabled by default. To opt-out, unset System → General → Usage collection.

The Alert (page 345) system has been improved:
- Support for one-shot critical alerts has been added. These alerts remain active until dismissed by the user.
- Alert Settings (page 96) has been reorganized: alerts are grouped functionally rather than alphabetically and per-alert severity and alert thresholds are configurable.
- Periodic alert scripts have been replaced by the Alert (page 345) framework. Periodic alert emails are disabled by default and previous email alert conditions have been added to the FreeNAS® alert system. E-mail or other alert methods can be configured in Alert Services (page 94).

A Task Manager (page 348) in the top menu bar displays the status and progress of configured tasks.

The Dashboard has been rewritten to provide an overview of the current state of the system rather than repeat the historical data found in Reporting (page 326). It now uses middleware to handle data collection and provide the web interface with real-time events. Line charts have been replaced with meters and gauges. CPU graphs have been consolidated into a single widget which provides average usage and per-thread statistics for both temperature and usage. Interfaces are represented as a separate card per physical NIC unless they are part of a LAGG card. Pool and Interface widgets feature mobile-inspired lateral navigation, allowing users to “drill down” into the data without leaving the page.

Reporting (page 326) has been greatly improved. Data is now prepared on the backend by the middleware and operating system. Any remaining data manipulation is done in a web worker, keeping expensive processing off of the main UI thread/context. The SVG-based charting library was replaced with a GPU-accelerated canvas-based library. Virtual scroll and lazy loading prevent overloading the browser and eliminate the need for a pager. Users can zoom by X or Y axis and reset the zoom level with a double click. Graphs do not display if there is no related data. Support for UPS and NFS statistics has been added.

Options for configuring the reporting database have been moved to System → Reporting. This screen adds the ability to configure Graph Age as well as the number of points for each hourly, daily, weekly, or yearly graph (Graph Points). The location of the reporting database defaults to tmpfs and a configurable alert if the database exceeds 1 GiB has been added to Alert Settings (page 96).

The web interface has received many improvements and bug fixes. Usability enhancements include: ability to move, pin, and copy help text, persistent layout customizations, customizable column views, size units which accept humanized input, improved caching and browser support, and improved error messages, popup dialogs, and help text. An iX Official theme has been added which is the default for new installations.

NAT support has been added as the default for most Plugins (page 290). With NAT, a plugin is contained in its own network and does not require any knowledge of the physical network to work properly. This removes the need to manually configure IP addresses or have a DHCP server running. When installing a plugin into a virtualized environment, NAT removes the requirement to enable Promiscuous Mode for the network.

The Plugins (page 290) page has been streamlined so that most operations can be performed without having to go to the jails (page 301) page. Support for collections has been added to differentiate between iXsystems plugins, which receive updates every few weeks, and Community plugins. In addition, there have been many bug fixes and improvements to iocage, the Plugins backend, resulting in a much better Plugins user experience.

An ACL Manager (page 187) has been added to Storage → Pools → (Options) and the permissions editor (page 186) has been redesigned.
A new iSCSI wizard in *Block (iSCSI)* (page 222) makes it easy to configure iSCSI shares.

There have been several *Pool Manager* (page 168) improvements. The labels and tooltips for encryption operations are clearer. Disk type, rotation rate, and manufacturer information makes it easier to differentiate between selectable disks when creating a pool. A REPEAT button makes it easy to create large pools using the same vdev layout, such as a series of striped mirrors.

Significant improvements to *SMB sharing* (https://jira.ixsystems.com/browse/NAS-102108) include ZFS user quotas support, web service discovery support, and improved directory listing performance for newly-created shares.

The middleware and websockets APIv2 rewrite is complete. APIv1 remains for backwards compatibility but will be deprecated and no longer available in the next major release.

**Deprecated and Removed Features**

- The legacy web interface has been removed and no longer appears as an option in the *login screen* (page 64).
- Warden has been removed along with all CLI and web interface support for warden jails or plugins installed using FreeNAS® 11.1 or earlier.
- Hipchat has been removed from *Alert Services* (page 94) as it has been discontinued (https://www.atlassian.com/partnerships/slack). The web interface can still be used to delete an existing Hipchat configuration.
- *Domain Controller* has been removed from *Services* (page 259).
- *Netdata* has been removed from *Services* (page 259) due to a long-standing upstream memory leak. *TrueCommand* (https://www.ixsystems.com/truecommand/) provides similar reporting plus advanced management capabilities for single or multiple FreeNAS® systems and is free to use to manage up to 50 drives.
- The built-in Docker template has been removed from *Virtual Machines* (page 328). Instructions for manually installing Docker can be found in *Installing Docker* (page 333).

**New or Updated Software**

- OS support for reporting the CPU temperature of AMD Family 15h, Model >=60h has been added.
- QLogic 10 Gigabit Ethernet driver support has been added with qlxgbe(4) (https://www.freebsd.org/cgi/man.cgi?query=qlxgbe).
- The base FreeBSD ports have been updated to their latest versions as of September 24, 2019.
- Angular has been updated to version 8.2.13 (https://github.com/angular/angular/blob/master/CHANGELOG.md).
- Samba has been updated to version 4.10.10 (https://www.samba.org/samba/history/samba-4.10.10.html).
- Netatalk has been updated to version 3.1.12_2_1 (http://netatalk.sourceforge.net/3.1/ReleaseNotes3.1.12.html).
- Rclone has been updated to version 1.49.4 (https://rclone.org/changelog/#v1-49-4-2019-09-29).
- collectd has been updated to version 5.8.1_1 (https://collectd.org/wiki/index.php/Version_5.8).
- *p7zip* (http://p7zip.sourceforge.net/) has been added.
- The *zettarepl* (https://github.com/freenas/zettarepl) replication tool has been added.

**Misc UI Changes**

- The *Hostname* and *Domain* set in *Global Configuration* (page 157) are shown under the iXsystems logo at the top left of the web interface.
- The web interface now indicates when a *system update is in progress* (page 112).
• Directory Services Monitor (page 204) has been added to the top toolbar row.
• The Theme Selector has been removed from the top navigation bar. The theme is now selected in Preferences (page 66).
• The redundant Account entry has been removed from the gear icon of the top navigation bar.
• Add to Favorites, Enable Help Text, and Enable “Save Configuration” Dialog Before Upgrade have been removed from Preferences (page 66).
• Reset Table Columns to Default has been added to Preferences (page 66).
• Right-click help dialog has been added to the Shell (page 341).

System
• The GUI SSL Certificate, WebGUI HTTP -> HTTPS Redirect, Usage collection, and Crash reporting fields have been added to and the Protocol field has been removed from General (page 78).
• The WebGUI IPv4 Address and WebGUI IPv6 Address fields in the General (page 78) system options have been updated to allow selecting multiple IP addresses.
• The Language field can now be sorted by Name or Language code.
• An Export Pool Encryption Keys option has been added to the SAVE CONFIG dialog (page 80).
• System → Boot Environments has been renamed to Boot (page 83). Automatic scrub interval (in days) and information about the operating system device have been moved to ACTIONS → Stats/Settings.
• Periodic Notification User has been removed from the Advanced (page 86) system options because periodic script notifications have been replaced by alerts.
• Show tracebacks in case of fatal error has been removed from the Advanced (page 86) system options.
• Setting messages in the Advanced (page 86) system options provides a button to show console messages on busy spinner dialogs.
• Remote Graphite Server Hostname and Report CPU usage in percentage have been moved to System Reporting (page 94).
• From Name has been added to Email (page 91).
• Reporting Database has moved from System Dataset (page 93) to System → Reporting.
• Level has been added and the SHOW SETTINGS button removed from the Alert Services (page 94) options.
• API URL has been added to the OpsGenie alert service options (page 94).
• SNMP Trap has been added to Alert Services (page 94).
• IPMI SEL Low Space Left, IPMI System Event, Device is Causing Slow I/O on Pool, Rsync Task Failed, and Rsync Task Succeeded have been added to Alert Settings (page 96). Clear All Alerts has been changed to Dismiss All Alerts.
• OAuth Client ID and OAuth Client Secret have been removed from the Box, Dropbox, Microsoft OneDrive, pCloud, and Yandex providers in the Cloud Credentials (page 97) options.
• VERIFY CREDENTIAL has been added to the Cloud Credentials (page 97) options.
• Region has been added to the Amazon S3 Cloud Credentials (page 97) options.
• PEM-encoded private key file path has been changed to Private Key ID in the SFTP cloud credential options (page 99).
• Comment has been changed to Description in Tunables (page 105).
• FETCH AND INSTALL UPDATES has been renamed to DOWNLOAD UPDATES in Update (page 108).
• Elliptic Curve Cryptography (ECC) (https://en.wikipedia.org/wiki/Elliptic-curve_cryptography) key support has been added to the options for Certificate Authorities (page 115) and Certificates (page 120).
• Organizational Unit has been added to the CAs (page 113) and Certificates (page 116) options.
• Import Certificate Signing Request has been added to the Certificates (page 116) options.

Tasks
• The icon (page 23) has been added to the Schedule column for created Tasks (page 126).
• Timeout has been added to the Init/Shutdown Scripts options (page 128).
• The log entries for individual Rsync Tasks (page 129) can be displayed and downloaded by clicking the Status of the task.
• The FreeBSD path and name length (page 20) criteria have been applied to the Path field in rsync tasks (page 130).
• All Disks has been added to the S.M.A.R.T. Tests options (page 136).
• Exclude, Snapshot Lifetime, and Allow taking empty snapshots have been added to the Periodic Snapshot task options (page 137).
• Minutes can be specified in Custom Periodic snapshot schedules (page 137).
• The replication log has been moved to /var/log/zettarepl.log. The log entries for individual Replication Tasks (page 146) can be displayed and downloaded by clicking the State of the task.
• A Last Snapshot column has been added to Replication Tasks (page 146).
• Name, Properties, and Hold Pending Snapshots have been added to the Replication Task options (page 143).
• Limit (KiBs) has been renamed to Limit (Ex. 500 KiB/s, 500M, 2 TB) in the Replication Task options (page 143) and accepts various size units like K and M.
• Stream Compression in Replication Task options (page 143). only appears when SSH is chosen for Transport type.
• Storage Class, Use -fast-list, Take Snapshot, Stop, Pre-script, Post-script, Transfers, Follow Symlinks, Bandwidth Limit, Upload Chunk Size (MiB), and Exclude have been added to the Cloud Sync Task options (page 152).
• The log entries for individual Cloud Sync Tasks (page 151) can be displayed and downloaded by clicking the Status of the task.

Network
• The Interface name field has been renamed to Description and the MTU and Disable Hardware Offloading fields have been added to Interfaces options (page 160).

Storage
• Disk type, rotation rate, and manufacturer information can be viewed on the Disks (page 195) page and when creating a pool (page 168).
• The Export/Disconnect Pool (page 175) dialog shows system services that are affected by the export action.
• The dataset permissions editor (page 186) has been redesigned. The ACL Type, Apply User, Apply Group, and Apply Access Mode fields have been removed and Traverse has been added.
• ACL Mode has been added to the Add Dataset advanced mode (page 182).
• A dataset deletion confirmation dialog with a force delete option has been added to the Delete Dataset dialog (page 183).
• Time Remaining displays when the pool has an active scrub in Pool Status (page 180).
• Naming Schema has been added to the single snapshot (page 193) options.
• Critical, Difference, Informational, and Clear SED Password fields have been added to Disk Options (page 196).
• Detach and REFRESH options have been added to Pool Status (page 197).
• The Filesystem type option behavior in Import Disk (page 201) has been updated to select the detected filesystem of the chosen disk. After importing a disk, a dialog allows viewing or downloading the disk import log.
• Adding a dataset (page 181) shows options to configure warning or critical alerts (page 182) when a dataset reaches a certain percent of the quota.

Directory Services
• Computer Account OU has been added and the Enable AD monitoring, UNIX extensions, Domain Controller, Global Catalog Server, Connectivity Check, and Recovery Attempts fields have been removed from Active Directory (page 205).

• Leave Domain dynamically appears in Active Directory (page 204) when the FreeNAS® system is joined to an Active Directory domain.

• fruit and tdb2 have been removed from the Idmap backend options (page 207).

• Validate Certificate has been added to Active Directory (page 205) and LDAP (page 210) configuration options.

• The Disable LDAP User/Group Cache checkbox has been added and the UserSuffix, GroupSuffix, PasswordSuffix, MachineSuffix, SUDO Suffix, Netbios Name, and Netbios alias fields have been removed from LDAP configuration options (page 210).

• The Hostname in LDAP (page 209) supports multiple hostnames as a failover priority list.

Sharing

• Enable Shadow Copies has been added to the Windows Shares (SMB) options (page 247). Default Permissions has been removed from Windows (SMB) Shares (page 246) as permissions are now configured using ACL manager (page 187).

• The acl_tdb, acl_xattr, aio_fork, cacheprime, cap, commit, default_quota, expand_msdfs, extd_audit, fake_perms, linux_xfs_sgid, netatalk, posix_eadb, readahead, readonly, shadow_copy, shadow_copy_zfs, shell_snap, streams_Depot, syncops, time_audit, unityed_media, virusfilter, worm, and xattr_tdb VFS objects (page 251) have been removed and the shadow_copy2 VFS object has been added.

• Comment has been renamed to Description for Block (iSCSI) (page 222) Portals, Initiators, and Extents.

Services

• Email has been removed from the S.M.A.R.T. Service Options (page 275). S.M.A.R.T. alerts are configured as part of an alert service (page 94). Note that email addresses previously configured to receive S.M.A.R.T. alerts now receive all FreeNAS® alerts (page 345).

• Time Server for Domain, File Mask, Directory Mask, Allow Empty Password, DOS Charset, and Allow Execute Always have been removed from the SMB service options (page 277).

• Unix Extensions, Domain logons, and Obey pam restrictions have been removed from the SMB services options (page 277). These options are now dynamically enabled.

• Expose zliststat via SNMP has been added to the SNMP service options (page 280).

• Host Sync has been added to the UPS service options (page 286), search functionality has been added to Driver, and USB port detection has been added to the Port or Hostname.

• UPS events now generate Alerts (page 345).

• NUT (http://networkupstools.org/) (Network UPS Tools) now listens on ::1 (IPv6 localhost) in addition to 127.0.0.1 (IPv4 localhost).

Virtual Machines

• Grub boot loader support has been added for virtual machines that will not boot with other loaders.

• Description and System Clock have been added to the Virtual Machines wizard (page 331). The Wizard now displays system memory and Delay VM boot Until VNC Connects has been added to the first step of the Wizard.

• An optional, custom name can be specified when cloning Virtual Machines (page 328).

• Log files for each VM are stored in /var/log/vm/. Log files have the same name as the VM.

Plugins and Jails

• Browse a Collection, REFRESH INDEX, and POST INSTALL NOTES have been added to Plugins (page 290).

• Template jails (page 312) can now be created from the web interface.

• allow_vmm, allow_mount_fusefs, ip_hostname, assign_localhost, Autoconfigure IPv6 with rtsold, and NAT options have been added in Advanced Jail Creation (page 304).
• NAT Port Forwarding and the associated Protocol, Jail Port Number, and Host Port Number fields have been added to the Network Properties section of Advanced Jail Creation (page 304).
• ip6_saddrsel and ip4_saddresel in Advanced Jail Creation (page 304) have been renamed to ip6.saddrsel and ip4.saddresel.
• Log files for jail status and command output are stored in /var/log/iocage.log.

1.1.1 U1

U1 is the first maintenance release to 11.3-RELEASE, including nearly one hundred bug fixes and other improvements. For a detailed change list, see the completed tickets in the FreeNAS/TrueNAS Jira Project (https://jira.ixsystems.com/issues/?jql=project%20%3D%20NAS%20AND%20resolution%20%3D%20Closed%20AND%20status%20%3D%20Done%20AND%20fixVersion%20%3D%2011.3-U1).

1.1.2 U2

This release nearly includes a combined 150 bug fixes, updates, and improvements. Some highlights of this version include:
• An update to Samba, version 4.10.13 (NAS-105349)
• Bug fix when importing a pool (NAS-105297)
• Fix for a middleware memory leak (NAS-104437)
• Mitigation for specific LSI 9X00 cards (NAS-105568)

For a complete, detailed list of updates, see the list of FreeNAS 11.3-U2 Jira tickets (https://jira.ixsystems.com/issues/?filter=4&jql=fixVersion%20IN%20(11303,11300))

The 11.3-U2.1 release is a hotfix that only addresses a critical issue when exporting and destroying pools (NAS-105782).

1.1.3 U3

FreeNAS 11.3-U3 is a maintenance release that includes over one hundred bug fixes and quality of life improvements for the software. Notable fixes include:
• Network Interfaces section updates (NAS-105964, NAS-105963, NAS-105960, NAS-105959, NAS-105958, NAS-105956)
• Allow mounting NFS shares with either Kerberos or default security when Require Kerberos for NFSv4 is disabled. (NAS-105956)
• Import a Samba 4 patch for an Apple Time Machine bug (NAS-105911)
• UI visual improvements (NAS-105909, NAS-105916, NAS-105916, NAS-105927, NAS-105907, NAS-105862, NAS-105800, NAS-105713, NAS-105661, NAS-105601, NAS-105513)
• Improve Active Directory auto-rejoin (NAS-105853)
• Merge FreeBSD patches and update FreeNAS Kernel to 11.3-RELEASE-p8 (NAS-105837)
• Improvements to the alert system (NAS-105785, NAS-105792, NAS-105833, NAS-105876, NAS-105715, NAS-105684, NAS-105664, NAS-105660)

• Make fstab handling for Jail mount points more robust (NAS-105735)

• Temperature reporting fallback for drives on a SCSI HBA (NAS-105656)

• SMB sharing improvements (NAS-105395, NAS-105443, NAS-105445, NAS-105573, NAS-105703, NAS-105833, NAS-105835, NAS-105911, NAS-106049, NAS-106047)

The Jira FreeNAS 11.3-U3 issue tracker has a full list of changes included in this release.

Note: There is a current issue where the UI can become unresponsive after upgrading. If this occurs, clear the site data and refresh the page.

1.1.4 U4

FreeNAS 11.3-U4 is another maintenance release of FreeNAS 11.3 that has over one hundred and thirty bug fixes to the FreeNAS middleware and user interface, including:

• Updating Samba to 4.10.16 (NAS-106500)

• Merging FreeBSD Security Advisory SA-20:17 (NAS-106415)

• Using a Google Team Drive with Cloud Sync Tasks (NAS-106195)

• Unlocking Self-Encrypting Drives (SEDs) (NAS-106004)

• Cloud sync to Backblaze B2 (NAS-106541)

• Recursive Replication (NAS-106435)

• OAuth client ID and Secret for Google Drive and Onedrive (NAS-106407)

• Deleting expired snapshots (NAS-105966)

For full release notes for FreeNAS 11.3-U4, see https://www.truenas.com/docs/hub/intro/release-notes/.

1.1.5 U5

iXsystems is pleased to announce the general availability of the fifth update to FreeNAS version 11.3! 11.3-U5 is a maintenance release that has over 100 bug fixes to the Middleware and Web Interface. This is now the most stable and performant release of FreeNAS 11.3, and users are encouraged to update immediately! Here is the full changelog for FreeNAS 11.3-U5:

Bug Fixes
<table>
<thead>
<tr>
<th>Key</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS-107603</td>
<td>Replication that worked in 11.3-U4 and 12.0-Beta2 fails in 12.0-U1.</td>
</tr>
<tr>
<td>NAS-107544</td>
<td>SMART and scrub tasks are not running.</td>
</tr>
<tr>
<td>NAS-107533</td>
<td>Unable to remove certificate in s3 service.</td>
</tr>
<tr>
<td>NAS-107531</td>
<td>Comment and restrict change of large blocks support in replication.</td>
</tr>
<tr>
<td>NAS-107506</td>
<td>Additional Domains don't show up on save.</td>
</tr>
<tr>
<td>NAS-107468</td>
<td>Cloud sync to Wasabi with &quot;Can't mix absolute and relative paths&quot;.</td>
</tr>
<tr>
<td>NAS-107411</td>
<td>No Task Manager Progress is shown.</td>
</tr>
<tr>
<td>NAS-107316</td>
<td>UPS Settings Saving Bug.</td>
</tr>
<tr>
<td>NAS-107315</td>
<td>middleware memory leak.</td>
</tr>
<tr>
<td>NAS-107314</td>
<td>Replicated dataset is not set to read-only.</td>
</tr>
<tr>
<td>NAS-107292</td>
<td>Unable to Delete Expired ACME Certificate.</td>
</tr>
<tr>
<td>NAS-107235</td>
<td>Error when updating a Jail 11.3-RELEASE-p6 to 11.3-RELEASE-p7.</td>
</tr>
<tr>
<td>NAS-107160</td>
<td>Apparent crash on delete of share to invalid directory.</td>
</tr>
<tr>
<td>NAS-107148</td>
<td>Generate a random default serial extent.</td>
</tr>
<tr>
<td>NAS-107133</td>
<td>unable to delete iscsi file extents.</td>
</tr>
<tr>
<td>NAS-107128</td>
<td>When creating pool, adding vdev, then removing it, leaves delete of failover_vhid to type select instead of input.</td>
</tr>
<tr>
<td>NAS-107121</td>
<td>failover_aliases and failover_virtual_aliases are being overwritten.</td>
</tr>
<tr>
<td>NAS-107120</td>
<td>change failover_vhid to type select instead of input.</td>
</tr>
<tr>
<td>NAS-107116</td>
<td>allow editing empty interfaces.</td>
</tr>
<tr>
<td>NAS-107108</td>
<td>Google Drive Cloud Sync tasks fail with exportSizeLimitExceeded error.</td>
</tr>
<tr>
<td>NAS-107107</td>
<td>Clear any potential stale state after leaving AD domain.</td>
</tr>
<tr>
<td>NAS-107104</td>
<td>ACME DNS renewals don't work.</td>
</tr>
<tr>
<td>NAS-107100</td>
<td>Do not run check_available in a tight loop in case an exception happens.</td>
</tr>
<tr>
<td>NAS-107099</td>
<td>Do not display previous replication task status after deleting it.</td>
</tr>
<tr>
<td>NAS-107096</td>
<td>Custom sync schedule forgotten when editing task.</td>
</tr>
<tr>
<td>NAS-107076</td>
<td>Expand regression tests for user api.</td>
</tr>
<tr>
<td>NAS-107074</td>
<td>Permissions are incorrect on home directory move.</td>
</tr>
<tr>
<td>NAS-107067</td>
<td>Fix chown of skel directory contents for new local users.</td>
</tr>
<tr>
<td>NAS-107055</td>
<td>Forums user reported logs filled with fruit error messages.</td>
</tr>
<tr>
<td>NAS-107053</td>
<td>Pool in dashboard omits special vdevs from count and status.</td>
</tr>
<tr>
<td>NAS-107037</td>
<td>Have ftp reload method reload proftpd rather than restart it.</td>
</tr>
<tr>
<td>NAS-107035</td>
<td>Swap size setting not honored on 4k sector disks.</td>
</tr>
<tr>
<td>NAS-107032</td>
<td>Unable to upload 8TB file to backblaze.</td>
</tr>
<tr>
<td>NAS-107029</td>
<td>Unable to configure UPS on TrueNAS 12.</td>
</tr>
<tr>
<td>NAS-107023</td>
<td>Expand list of error strings that should trigger an AD rejoin.</td>
</tr>
<tr>
<td>NAS-106993</td>
<td>Reassign sys.({stdout,stderr}) after log rollover.</td>
</tr>
<tr>
<td>NAS-106984</td>
<td>&quot;Jls&quot; hostname does not reflect modified hostname.</td>
</tr>
<tr>
<td>NAS-106978</td>
<td>Add regression tests for AD machine account keytab generation.</td>
</tr>
<tr>
<td>NAS-106966</td>
<td>collectd: blank warning emails.</td>
</tr>
<tr>
<td>NAS-106965</td>
<td>qBittorrent Plugin Not Installing.</td>
</tr>
<tr>
<td>NAS-106948</td>
<td>Recycle bin versioning not enabled.</td>
</tr>
<tr>
<td>NAS-106918</td>
<td>Replacing boot usb drive problem.</td>
</tr>
<tr>
<td>NAS-106866</td>
<td>Proper/better error for failed authentication.</td>
</tr>
<tr>
<td>NAS-106864</td>
<td>SED doesn't work for nvme.</td>
</tr>
<tr>
<td>NAS-106854</td>
<td>plugin boot checkbox re-enables itself.</td>
</tr>
<tr>
<td>NAS-106842</td>
<td>Setting IPMI to DHCP should gray-out IP addresses.</td>
</tr>
<tr>
<td>NAS-106840</td>
<td>Setting invalid VHID value fails silently.</td>
</tr>
<tr>
<td>NAS-106808</td>
<td>Ensure monpwd/monuser fields are provided for UPS service.</td>
</tr>
<tr>
<td>NAS-106798</td>
<td>api context/services/iscsi/targettoextent does not allow null value.</td>
</tr>
<tr>
<td>NAS-106797</td>
<td>Periodic Snapshot Tasks - &quot;Enabled&quot; checkboxes are not unique.</td>
</tr>
<tr>
<td>NAS-106787</td>
<td>iSCSI webUI columns COMPLETELY break when edited.</td>
</tr>
</tbody>
</table>
### Table 1.1 – continued from previous page

<table>
<thead>
<tr>
<th>Key</th>
<th>Summary</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS-106745</td>
<td>Cloud Sync Bandwidth Limit Field Validation</td>
<td></td>
</tr>
<tr>
<td>NAS-106713</td>
<td>Cron job still runs despite being deactivated and then deleted</td>
<td></td>
</tr>
<tr>
<td>NAS-106690</td>
<td>Can't clear Kerberos Principal from GUI</td>
<td></td>
</tr>
<tr>
<td>NAS-106682</td>
<td>Validation Error on creation of Manual SSH Connection for Replication</td>
<td></td>
</tr>
<tr>
<td>NAS-106675</td>
<td>dashboard is completely blank no widgets</td>
<td></td>
</tr>
<tr>
<td>NAS-106658</td>
<td>ZFS replication does not create datasets on target</td>
<td></td>
</tr>
<tr>
<td>NAS-106583</td>
<td>FreeNAS disks forget their assigned pool</td>
<td></td>
</tr>
<tr>
<td>NAS-106496</td>
<td>System crash after middlewared.set_sysctl():407 - Failed to set sysctl</td>
<td></td>
</tr>
<tr>
<td>NAS-106133</td>
<td>Categories for support proxy</td>
<td></td>
</tr>
<tr>
<td>NAS-106110</td>
<td>UPS ups is on battery power alerts since upgrade to 11.3</td>
<td></td>
</tr>
<tr>
<td>NAS-105099</td>
<td>Periodic Snapshot are missing the lifetime in its name</td>
<td></td>
</tr>
<tr>
<td>NAS-104906</td>
<td>Rsync tasks view shows incorrect remote path</td>
<td></td>
</tr>
<tr>
<td>NAS-102808</td>
<td>Running Cloud Sync tasks keep on running after deletion in GUI</td>
<td></td>
</tr>
</tbody>
</table>

Due to numerous improvements in the replication engine and ZFS, FreeNAS/TrueNAS 11.3 will no longer replicate to FreeNAS/TrueNAS 9.10 systems (or earlier). Solution: update the destination system to FreeNAS/TrueNAS 11.3 or newer.

### Known Issues

<table>
<thead>
<tr>
<th>Key</th>
<th>Summary</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>The web interface can become unresponsive after upgrading.</td>
<td>Clear the browser cache and refresh the page (Shift + F5).</td>
</tr>
<tr>
<td>NAS-106882</td>
<td>Some plugins are not showing their version and will be moved to the “Community” plugins list for TrueNAS 12.0 (NAS-106610).</td>
<td>None: some plugins remain unversioned and will be moved to the “Community” plugins list for TrueNAS 12.0 (NAS-106610).</td>
</tr>
<tr>
<td>NAS-107132</td>
<td>Replication from FreeNAS/TrueNAS 11.3 (and newer) to FreeNAS/TrueNAS 9.10 (or earlier) is not functional.</td>
<td>Update the destination system to FreeNAS/TrueNAS 11.3 or newer.</td>
</tr>
</tbody>
</table>

### 1.2 Path and Name Lengths

Names of files, directories, and devices are subject to some limits imposed by the FreeBSD operating system. The limits shown here are for names using plain-text characters that each occupy one byte of space. Some UTF-8 characters take more than a single byte of space, and using those characters reduces these limits proportionally. System overhead can also reduce the length of these limits by one or more bytes.
Table 1.2: Path and Name Lengths

<table>
<thead>
<tr>
<th>Type</th>
<th>Maximum Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Paths</td>
<td>1023 bytes</td>
<td>Total file path length (PATH_MAX). The full path includes directory separator slash characters, subdirectory names, and the name of the file itself. For example, the path /mnt/tank/mydataset/mydirectory/myfile.txt is 42 bytes long. Using very long file or directory names can be problematic. If a path with long directory and file names exceeds the 1023-byte limit, it prevents direct access to that file until the directory names or filename are shortened or the file is moved into a directory with a shorter total path length.</td>
</tr>
<tr>
<td>File and Directory Names</td>
<td>255 bytes</td>
<td>Individual directory or file name length (NAME_MAX).</td>
</tr>
<tr>
<td>Mounted Filesystem Paths</td>
<td>88 bytes</td>
<td>Mounted filesystem path length (MNAMELEN). Longer paths can prevent a device from being mounted.</td>
</tr>
<tr>
<td>Device Filesystem Paths</td>
<td>63 bytes</td>
<td>devfs(8) (<a href="https://www.freebsd.org/cgi/man.cgi?query=devfs">https://www.freebsd.org/cgi/man.cgi?query=devfs</a>) device path lengths (SPECNAMELEN). Longer paths can prevent a device from being created.</td>
</tr>
</tbody>
</table>

**Note:** 88 bytes is equal to 88 ASCII characters. The number of characters varies when using Unicode.

**Warning:** If the mounted path length for a snapshot exceeds 88 bytes, the data in the snapshot is safe but inaccessible. When the mounted path length of the snapshot is less than the 88 byte limit, the data will be accessible again.

The 88 byte limit affects automatic and manual snapshot mounts in slightly different ways:

- **Automatic mount:** ZFS temporarily mounts a snapshot whenever a user attempts to view or search the files within the snapshot. The mountpoint used will be in the hidden directory .zfs/snapshot/name within the same ZFS dataset. For example, the snapshot mypool/dataset/snap1@snap2 is mounted at /mnt/mypool/dataset/.zfs/snapshot/snap2/. If the length of this path exceeds 88 bytes the snapshot will not be automatically mounted by ZFS and the snapshot contents will not be visible or searchable. This can be resolved by renaming the ZFS pool or dataset containing the snapshot to shorter names (mypool or dataset), or by shortening the second part of the snapshot name (snap2), so that the total mounted path length does not exceed 88 bytes. ZFS will automatically perform any necessary unmount or remount of the file system as part of the rename operation. After renaming, the snapshot data will be visible and searchable again.

- **Manual mount:** The same example snapshot is mounted manually from the Shell (page 341) with mount -t zfs mypool/dataset/snap1@snap2 /mnt/mymountpoint. The path /mnt/mountpoint/ must not exceed 88 bytes, and the length of the snapshot name is irrelevant. When renaming a manual mountpoint, any object mounted on the mountpoint must be manually unmounted with the umount command before renaming the mountpoint. It can be remounted afterwards.

**Note:** A snapshot that cannot be mounted automatically by ZFS can still be mounted manually from the Shell (page 341) with a shorter mountpoint path. This makes it possible to mount and access snapshots that cannot be accessed automatically in other ways, such as from the web interface or from features such as “File History” or “Versions”.


1.3 Using the Web Interface

1.3.1 Tables and Columns

Tables show a subset of all available columns. Additional columns can be shown or hidden with the COLUMNS button. Set a checkmark by the fields to be shown in the table. Column settings are remembered from session to session.

The original columns can be restored by clicking Reset to Defaults in the column list.

Each row in a table can be expanded to show all the information by clicking the ➤ (Expand) button.

1.3.2 Advanced Scheduler

When choosing a schedule for different FreeNAS® Tasks (page 126), clicking Custom opens the custom schedule dialog.

Choosing a preset schedule fills in the rest of the fields. To customize a schedule, enter crontab (https://www.freebsd.org/cgi/man.cgi?query=crontab&sektion=5) values for the Minutes/Hours/Days.

Fig. 1.1: Creating a Custom Schedule
These fields accept standard cron values. The simplest option is to enter a single number in the field. The task runs when the time value matches that number. For example, entering 10 means that the job runs when the time is ten minutes past the hour.

An asterisk (*) means “match all values”.

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

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

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

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

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

The Days of Week schedules the task to run on specific days. This is in addition to any listed Days. For example, entering 1 in Days and setting W for Days of Week creates a schedule that starts a task on the first day of the month and every Wednesday of the month.

Schedule Preview shows when the current schedule settings will cause the task to run.

### 1.3.3 Schedule Calendar

The Schedule column has a calendar icon (📅). Clicking this icon opens a dialog showing scheduled dates and times for the related task to run.

![Example Schedule Popup](image)

**Fig. 1.2: Example Schedule Popup**

_Scrub Tasks_ (page 149) can have a number of Threshold days set. The configured scrub task continues to follow the displayed calendar schedule, but it does not run until the configured number of threshold days have elapsed.

### 1.3.4 Changing FreeNAS® Settings

It is important to use the web interface or the Console Setup menu for all configuration changes. FreeNAS® stores configuration settings in a database. Commands entered at the command line do not modify the settings database. This means that changes made at the command line will be lost after a restart and overwritten by the values in the settings database.
1.3.5 Web Interface Troubleshooting

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

- Make sure the browser allows cookies, Javascript, and custom fonts from the FreeNAS® system.
- Try a different browser. Firefox (https://www.mozilla.org/en-US/firefox/all/) is recommended.

If a web browser cannot connect to the FreeNAS® system by IP address, DNS hostname, or mDNS name:

- Check or disable proxy settings in the browser.
- Verify the network connection by pinging the FreeNAS® system by IP address from another computer on the same network. For example, if the FreeNAS® system is at IP address 192.168.1.19, enter `ping 192.168.1.19` on the command line of the other computer. If there is no response, check network configuration.

1.3.6 Help Text

Most fields and settings in the web interface have a ☰ (Help Text) icon. Additional information about the field or setting can be shown by clicking ☰ (Help Text). The help text window can be dragged to any location, and will remain there until ✗ (Close) or ☰ (Help Text) is clicked to close the window.

1.3.7 Humanized Fields

Some numeric value fields accept humanized values. This means that the field accepts numbers or numbers followed by a unit, like M or MiB for megabytes or G or GiB for gigabytes. Entering 1048576 or 1M are equivalent. Units of KiB, MiB, GiB, TiB, and PiB are available, and decimal values like 1.5 GiB are supported when the field allows them. Some fields have minimum or maximum limits on the values which can restrict the units available.

1.3.8 File Browser

Certain sections of the web interface have a built in file browser. The file browser is used to traverse through directories and choose datasets on the system. Datasets that have complex ACL permissions (page 187) are tagged so they can be distinguished from non-ACL datasets.

1.4 Hardware Recommendations

FreeNAS® 11.3 is based on FreeBSD 11.3 and supports the same hardware found in the FreeBSD Hardware Compatibility List (https://www.freebsd.org/releases/11.3R/hardware.html). Supported processors are listed in section 2.1 amd64 (https://www.freebsd.org/releases/11.3R/hardware.html#proc). 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 workflow of your FreeNAS® system. This section provides some starter guidelines. The FreeNAS® Hardware Forum (https://www.ixsystems.com/community/forums/hardware-discussion/) has performance tips from FreeNAS® users and is a place to post questions regarding the hardware best suited to meet specific requirements. The Official FreeNAS® Hardware Guide (https://www.ixsystems.com/blog/hardware-guide/) gives in-depth recommendations for every component needed in a FreeNAS® build. Building, Burn-In, and Testing your FreeNAS® system (https://forums.freenas.org/index.php?threads/building-burn-in-and-testing-your-freenas-system.17750/) has detailed instructions on testing new hardware.
1.4.1 RAM

The best way to get the most out of a FreeNAS® system is to install as much RAM as possible. More RAM allows ZFS to provide better performance. The iXsystems® Community Forums (https://www.ixsystems.com/community/) provide anecdotal evidence from users on how much performance can be gained by adding more RAM.

General guidelines for RAM:

- **A minimum of 8 GiB of RAM is required.**
  Additional features require additional RAM, and large amounts of storage require more RAM for cache. A general recommendation is to start with 8 GiB RAM and add 1 GiB RAM for each drive above 8 in the system. For example, a system with 10 drives is recommended to have at least 10 GiB RAM.
- To use Active Directory with many users, add an additional 2 GiB of RAM for the winbind internal cache.
- For iSCSI, install at least 16 GiB of RAM if performance is not critical, or at least 32 GiB of RAM if good performance is a requirement.
- **Jails** (page 301) are very memory-efficient, but can still use memory that would otherwise be available for ZFS. If the system will be running many jails, or a few resource-intensive jails, adding 1 to 4 additional gigabytes of RAM can be helpful. This memory is shared by the host and will be used for ZFS when not being used by jails.
- **Virtual Machines** (page 328) require additional RAM beyond any amounts listed here. Memory used by virtual machines is not available to the host while the VM is running, and is not included in the amounts described above. For example, a system that will be running two VMs that each need 1 GiB of RAM requires an additional 2 GiB of RAM.
- When installing FreeNAS® on a headless system, disable the shared memory settings for the video card in the BIOS.
- For ZFS deduplication, ensure the system has at least 5 GiB of RAM per terabyte of storage to be deduplicated.

If the hardware supports 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 your data is important, use ECC RAM. This Case Study (http://research.cs.wisc.edu/adsl/Publications/zfs-corruption-fast10.pdf) describes the risks associated with memory corruption.

Do not use FreeNAS® to store data without at least 8 GiB of RAM. 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 GiB of RAM because of the abundance of information that FreeNAS® may not behave properly with less memory.

1.4.2 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 an SSD, a small hard drive, or a USB stick.

**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, while the other USB stick is the destination for the FreeNAS® installation.
careful to select the correct USB device for the FreeNAS® installation. FreeNAS® cannot be installed onto the same device that contains 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® operating system device.

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

- The absolute **bare minimum** size is 8 GiB. That does not provide much room. The **recommended** minimum is 16 GiB. This provides room for the operating system and several boot environments created by updates. More space provides room for more boot environments and 32 GiB or more is preferred.
- SSDs (Solid State Disks) are fast and reliable, and make very good FreeNAS® operating system devices. Their one disadvantage is that they require a disk connection which might be needed for storage disks.
  
  Even a relatively large SSD (120 or 128 GiB) is useful as a boot device. While it might appear that the unused space is wasted, that space is instead used internally by the SSD for wear leveling. This makes the SSD last longer and provides greater reliability.
- When planning to add your own boot environments, budget about 1 GiB 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. USB sticks can also wear out or fail unexpectedly, causing system errors. It is recommended to regularly back up your system configuration and have replacement USB sticks prepared.
- For a more reliable boot disk, use two identical devices and select them both during the installation. This will create a mirrored boot device.

**Note:** Current versions of FreeNAS® run directly from the operating system device. Early versions of FreeNAS® ran from RAM, but that has not been the case for years.

### 1.4.3 Storage Disks and Controllers

The [Disk section](https://www.freebsd.org/releases/11.3R/hardware.html#disk) of the FreeBSD Hardware List shows supported disk controllers.

FreeNAS® supports hot-pluggable SATA drives when AHCI is enabled in the BIOS. The FreeNAS® team highly recommends [Western Digital Red](https://www.westerndigital.com/products/internal-drives/wd-red-hdd) NAS Disk Drives as the preferred storage drive of FreeNAS®.

Suggestions for testing disks can be found in this [forum post](https://forums.freenas.org/index.php?threads/checking-new-hdds-in-raid.12082/#post-55936). badblocks ([https://linux.die.net/man/8/badblocks](https://linux.die.net/man/8/badblocks)) is installed with FreeNAS® for disk testing.

[ZFS Disk Space Requirements for ZFS Storage Pools](https://docs.oracle.com/cd/E19253-01/819-5461/en7ht6r12/index.html) recommends a minimum of 16 GiB of disk space. FreeNAS® allocates 2 GiB of swap space on each drive.


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 TiB and two 4 TiB disks will only be able to use 2 TiB of space on each disk. In general, use disks that are the same size for the best space usage and performance.

The [ZFS Drive Size and Cost Comparison spreadsheet](https://forums.freenas.org/index.php?threads/zfs-drive-size-and-cost-comparison-spreadsheet.38092/) is available to compare usable space provided by different quantities and sizes of disks.
1.4.4 Network Interfaces

The Ethernet section (https://www.freebsd.org/releases/11.3R/hardware.html#ethernet) 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 MiB/s throughput. For higher network throughput, multiple GigE cards can be bonded together using the LACP type of Link Aggregations (page 162). 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 (https://forums.freenas.org/index.php?threads/10-gig-networking-primer.25749/) 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 (https://www.samba.org/samba/docs/old/Samba3-Developers-Guide/architecture.html). 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) (https://www.freebsd.org/cgi/man.cgi?query=ifconfig). 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 igb0 interface:

```
[root@freenas ~]# ifconfig -m igb0
igb0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=6403bb<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HNSUM,
    TS04,TS06,VLAN_HWTSO,RXCSUM_IPV6,TXCSUM_IPV6>
    capabilities=653fbb<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,
    VLAN_HNSUM,TS04,TS06,LRO,WOL_UCAST,WOL_MCAST,WOL_MAGIC,VLAN_HNFILTER,VLAN_HWTO,
    RXCSUM_IPV6,TXCSUM_IPV6>
```

If WOL support is shown but not working for a particular interface, create a bug report using the instructions in Support (page 123).

1.5 Getting Started with ZFS

Readers new to ZFS should take a moment to read the ZFS Primer (page 372).
The FreeNAS® operating system has to be installed on a separate device from the drives which hold the storage data. With only one disk drive, the FreeNAS® web 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 stick and use the computer disks for storage.

This section describes:
- Getting FreeNAS® (page 28)
- Preparing the Media (page 29)
- Performing the Installation (page 31)
- Installation Troubleshooting (page 37)
- Upgrading (page 38)
- Virtualization (page 44)

2.1 Getting FreeNAS®

The latest STABLE version of FreeNAS® 11.3 is available for download from https://www.freenas.org/download-freenas-release/.

The download page has links to FreeNAS® release notes, .iso integrity checksums, and PGP security keys.

Clicking Download opens a dialog to save an .iso file. This bootable installer must be written to physical media (page 29) before it can be used to install FreeNAS®.

2.1.1 Checking Installer Integrity

FreeNAS® uses the OpenPGP standard (https://en.wikipedia.org/wiki/Pretty_Good_Privacy#OpenPGP) to confirm that downloaded files have been provided by a trustworthy source. OpenPGP compliant software like gnupg (https://www.freebsd.org/cgi/man.cgi?query=gpg), Kleopatra (https://www.openpgp.org/software/kleopatra/), or Gpg4win (https://gpg4win.org/) can check the PGP signature of a FreeNAS® installer file.

The sha256.txt file is used to confirm the integrity of the downloaded .iso. See SHA256 Verification (page 29) for more details.

2.1.1.1 PGP Verification

To verify the .iso source, go to https://www.freenas.org/download-freenas-release/ and click PGP Signature to download the software signature file. Open the PGP Public key link and note the browser address and Search results string.

Use one of the OpenPGP encryption tools mentioned above to import the public key and verify the PGP signature. This example shows verifying the FreeNAS® .iso using gpg in a command prompt:
• Go to the .iso and .iso.gpg download location and import the public key using the keyserver address and search results string:

```
tmoore@Observer ~$ cd Downloads/
tmoore@Observer ~/Downloads> gpg --keyserver sks-keyservers.net --recv-keys
    0xe86def767c1db0df46e6c358ea9112cf7946
    gpg: /usr/home/tmoore/.gnupg/trustdb.gpg: trustdb created
    gpg: key 358EAA9112CF7946: public key "IX SecTeam <security-officer@ixsystems.com>" imported
    gpg: Total number processed: 1
    gpg: imported: 1
```  

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

```
tmoore@Observer ~/Downloads> gpg --verify FreeNAS-11.2-U6.iso.gpg FreeNAS-11.2-U6.iso
    gpg: Signature made Tue Nov 5 13:48:18 2019 EST  
    gpg: using RSA key C8D62DEF767C1DB0DFF4E6EC358EAA9112CF7946  
    gpg: Good signature from "IX SecTeam <security-officer@ixsystems.com>" [unknown]  
    gpg: WARNING: This key is not certified with a trusted signature!  
    gpg: There is no indication that the signature belongs to the owner.  
    Primary key fingerprint: C8D6 2DEF 767C 1DB0 DFF4 E6EC 358E AA91 12CF 7946  
    tmoore@Observer ~/Downloads>
```  

• This response means the signature is correct but still untrusted. Go back to the browser page that has the PGP Public key open and manually confirm that the key was issued for the iX Security Team on October 15, 2019 and has been signed by iXsystems accounts.

2.1.1.2 SHA256 Verification

The command to verify the checksum varies by operating system:

- on a BSD system use the command `sha256 isofile`
- on a Linux system use the command `sha256sum isofile`
- on a Mac system use the command `shasum -a 256 isofile`
- Windows or Mac users can install additional utilities like HashCalc (http://www.slavasoft.com/hashcalc/) or HashTab (http://implbits.com/products/hashtab/).

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

2.2 Preparing the Media

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

A CD burning utility is needed to write the .iso file to a CD.

The .iso file can also be written to a USB stick. The method used to write the file depends on the operating system. Examples for several common operating systems are shown below.

**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.

Ensure the operating system 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 is used to write the `.iso` file to an inserted USB stick.

**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`! This command can be avoided by writing the `.iso` file to a CD instead.

This example demonstrates writing the image to the first USB device connected to a FreeBSD system. This first device usually reports as `/dev/da0`. Replace `FreeNAS-RELEASE.iso` with the filename of the downloaded FreeNAS® ISO file. Replace `/dev/da0` with the device name of the device to write.

```
dd if=FreeNAS-RELEASE.iso of=/dev/da0 bs=64k
6117+0 records in
6117+0 records out
40083712 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 stick. 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 stick, use `ls /dev/da*`. Then attach the target USB stick, wait ten seconds, and run `ls /dev/da*` again to see the new device name and number of the target USB stick. 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 stick.

2.2.2 On Windows

Image Writer (https://launchpad.net/win32-image-writer/) and Rufus (http://rufus.akeo.ie/) can be used for writing images to USB sticks on Windows.

2.2.3 On macOS

Insert the USB stick. In Finder, go to *Applications → Utilities → Disk Utility*. Unmount any mounted partitions on the USB stick. Check that the USB stick 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 stick. Selecting *Free space* when creating the partition works fine.

Determine the device name of the inserted USB stick. 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. To determine the correct path for the USB stick, remove the device, run the command again, and compare the difference. Once 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 this example, the USB stick is `/dev/disk1`. It is first unmounted. The `dd` command is used to write the image to the faster "raw" version of the device (note the extra `r` in `/dev/rdisk1`).

When running these commands, replace `FreeNAS-RELEASE.iso` with the name of the FreeNAS® ISO and `/dev/rdisk1` with the correct path to the USB stick:

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

dd if=FreeNAS-RELEASE.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 stick, and click on its partitions to make sure all of them are unmounted. If a "Permission denied" error is shown, use `sudo` for elevated rights: `sudo dd if=FreeNAS-11.0-RELEASE.iso of=/dev/rdisk1 bs=64k`. This will prompt for the 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 stick.

### 2.3 Performing the Installation

With the installation media inserted, boot the system from that media.

The FreeNAS® installer boot menu is displayed as is shown in Figure 2.1.

![Fig. 2.1: Installer Boot Menu](image)
The FreeNAS® installer automatically boots into the default option after ten seconds. If needed, choose another boot option by pressing the Spacebar to stop the timer and then enter the number of the desired option.

**Tip:** The Serial Console option is useful on systems which do not have a keyboard or monitor, but are accessed through a serial port, Serial over LAN, or IPMI (page 164).

**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.

Once the installer has finished booting, the installer menu is displayed as shown in Figure 2.2.

![Fig. 2.2: Installer Menu](image)

Press Enter to select the default option, Install/Upgrade. The next menu, shown in Figure 2.3, lists all available drives. This includes any inserted operating system devices, which have names beginning with da.

**Note:** A minimum of 8 GiB of RAM is required and the installer will present a warning message if less than 8 GiB is detected.

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

Select one or more drives where FreeNAS should be installed (use arrow keys to navigate to the drive(s) for installation; select a drive with the spacebar).

+----------------+---------------------+---+----------------+---------------------+---+----------------+---------------------+---+----------------+---------------------+---+----------------+---------------------+---+----------------+---------------------+---+----------------+---------------------+---+----------------+---------------------+---+----------------+---------------------+---+----------------+---------------------+---+----------------+---------------------+---+----------------+---------------------+---+
| [ ] ada0       | VBOX HARDDISK -- 16.0 GiB |
| [ ] ada1       | VBOX HARDDISK -- 20.0 GiB |
| [ ] ada2       | VBOX HARDDISK -- 0.0 GiB  |
| [ ] ada3       | VBOX HARDDISK -- 9.0 GiB  |
| [ ] ada4       | VBOX HARDDISK -- 11.0 GiB |
| [ ] ada5       | VBOX HARDDISK -- 14.0 GiB |
| [ ] ada6       | VBOX HARDDISK -- 0.0 GiB  |
| [ ] ada7       | VBOX HARDDISK -- 10.0 GiB |
| [ ] ada8       | VBOX HARDDISK -- 8.0 GiB  |
| [ ] ada9       | VBOX HARDDISK -- 11.0 GiB |
|               |                      |   |               |                      |   |               |                      |   |               |                      |   |               |                      |   |               |                      |   |               |                      |   |               |                      |   |
| <OK>           | <Cancel>             |

Fig. 2.3: Selecting the Install Drive

Use the arrow keys to highlight the destination SSD, hard drive, USB stick, or virtual disk. Press the **spacebar** to select it.

To mirror the operating system device, move to additional devices and press **spacebar** to select them also. If all of the selected devices are larger than 64 GiB and none are connected through USB, a 16 GiB swap partition is also created.

After making 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**.
See the *operating system device* (page 25) section to ensure the minimum requirements are met.

The installer recognizes existing installations of previous versions of FreeNAS®. 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.
Fig. 2.5: Performing a Fresh Install

The screen shown in Figure 2.6 prompts for the root password which is used to log in to the web interface.

Fig. 2.6: Set the Root Password

Setting a password is mandatory and the password cannot be blank. Since this password provides access to the
web interface, it needs to be hard to guess. Enter the password, press the down arrow key, and confirm the password. Then press Enter to continue with the installation. Choosing Cancel skips setting a root password during the installation, but the web interface will require setting a root password when logging in for the first time.

**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 web interface. This means that the FreeNAS® system needs to be kept physically secure and that the web interface needs to be behind a properly configured firewall and protected by a secure password.

FreeNAS® can be configured to boot with the standard BIOS boot mechanism or UEFI booting as shown Figure 2.7. BIOS booting is recommended for legacy and enterprise hardware. UEFI is used on newer consumer motherboards.

![FreeNAS Boot Mode](image)

**Fig. 2.7: Choose UEFI or BIOS Booting**

**Note:** Most UEFI systems can also boot in BIOS mode if CSM (Compatibility Support Module) is enabled in the UEFI setup screens.

The message in Figure 2.8 is shown after the installation is complete.
Press Enter to return to Installer Menu (page 32). 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 Booting (page 62) after waiting five seconds in the boot menu (page 42). Press the Spacebar to stop the timer and use the boot menu.

### 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 (https://forums.freebsd.org/index.php?threads/workaround-semi-fix-for-mountroot-issues-with-9-3.26071/).

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 (http://how-to-erase-hard-drive.com/). 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!
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 web interface. Unless the Release Notes for the new major release indicate that the current version requires an ISO upgrade, either upgrade method can be used.

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

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

This section describes how to perform an upgrade from an earlier version of FreeNAS® to 11.3. After 11.3 has been installed, use the instructions in Update (page 108) to keep the system updated.

2.5.1 Caveats

Be aware of these caveats before attempting an upgrade to 11.3:

- **Warning:** upgrading the ZFS pool can make it impossible to go back to a previous version. For this reason, the update process does not automatically upgrade the ZFS pool, though the Alert (page 345) system shows when newer ZFS Feature Flags (page 375) are available for a pool. Unless a new feature flag is needed, it is safe to leave the pool at the current version and uncheck the alert. If the pool is upgraded, it will not be possible to boot into a previous version that does not support the newer feature flags.

- Upgrading the firmware of Broadcom SAS HBAs to the latest version is recommended.


- **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 pools 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 not supported.** If the data currently resides on one UFS-formatted disk, create a ZFS pool using other disks after the upgrade, then use the instructions in Importing a Disk (page 201) to mount the UFS-formatted disk and copy the data to the ZFS pool. With only one disk, back up its data to another system or media before the upgrade, format the disk as ZFS after the upgrade, then restore the backup. If the data currently resides on a UFS RAID of disks, it is not possible to directly import that data to the ZFS pool. Instead, back up the data before the upgrade, create a ZFS pool after the upgrade, then restore the data from the backup.

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 pools are encrypted, **remember** to set a passphrase and download a copy of the encryption key and the latest recovery key. After the upgrade is complete, use the instructions in Importing a Pool (page 177) to import the encrypted pools.
3. Warn users that the FreeNAS® shares will be unavailable during the upgrade; it is recommended to schedule the upgrade for a time that will least impact users.

4. Stop all services in Services.

2.5.3 Upgrading Using the ISO

To perform an upgrade using this method, download (http://download.freenas.org/latest/) the .iso to the computer that will be used to prepare the installation media. Burn the downloaded .iso file to a CD or USB stick using the instructions in Preparing the Media (page 29).

Insert the prepared media into the system and boot from it. The installer waits ten seconds in the installer boot menu (page 31) before booting the default option. If needed, press the Spacebar to stop the timer and choose another boot option. After the media finishes booting into the installation menu, press Enter to select the default option 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® web interface, 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 versions of FreeNAS® installed on the boot drive or drives and presents the message shown in Figure 2.9.

![Fig. 2.9: Upgrading a FreeNAS® Installation](image)

To perform an upgrade, press Enter to accept the default of Upgrade Install. Again, the installer will display a reminder that the operating system should be installed on a disk that is not used for storage.
The updated system can be installed in a new boot environment, or the entire operating system device can be formatted to start fresh. Installing into a new boot environment preserves the old code, allowing a roll-back to previous versions if necessary. Formatting the boot device is usually not necessary but can reclaim space. User data and settings are preserved when installing to a new boot environment and also when formatting the operating system device. Move the highlight to one of the options and press Enter to start the upgrade.

The installer unpacks the new image and displays the menu shown in Figure 2.11. The database file that is preserved and migrated contains your FreeNAS® configuration settings.
2.5.4 Upgrading From the Web Interface

To perform an upgrade using this method, go to System → Update. See Upgrade (page 108) for more information on upgrading the system.

The connection is lost temporarily when the update is complete. It returns after the FreeNAS® system reboots into the new version of the operating system. The FreeNAS® system normally receives the same IP address from the DHCP server. Refresh the browser after a moment to see if the system is accessible.

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:
FreeNAS® waits five seconds before booting into the default boot environment. Press the **Spacebar** to stop the automatic boot timer. Press **4** to display the available boot environments and press **3** as needed to scroll through multiple pages.
In the example shown in Figure 2.13, the first entry in Boot Environments is 11.2-MASTER-201807250900. This is the current version of the operating system, after the update was applied. Since it is the first entry, it is the default selection.

The next entry is Initial-Install. This is the original boot environment created when FreeNAS® was first installed. Since there are no other entries between the initial installation and the first entry, only one update has been applied to this system since its initial installation.

To boot into another version of the operating system, enter the number of the boot environment to set it as Active. Press Backspace to return to the Boot Menu (page 42) and press Enter to boot into the chosen Active boot environment.

If an operating system device fails and the system no longer boots, don't panic. The data is still on the disks and there is still a copy of the saved configuration. The system can be recovered with a few steps:

1. Perform a fresh installation on a new operating system device.
2. Import the pools in Storage → Auto Import Pool.
3. Restore the configuration in System → General → Upload Config.

Note: It is not possible to restore a saved configuration that is newer than the installed version. For example, if a reboot into an older version of the operating system is performed, a configuration created in a later version cannot be restored.

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 ZFS features.**

- before performing any operation that may affect the data on a storage disk, **always back up all data first and verify the integrity of the backup.** While it is unlikely that the pool upgrade will affect the data, it is always better to be safe than sorry.

- upgrading a ZFS pool is **optional.** Do not upgrade the pool if the the possibility of reverting to an earlier version of FreeNAS® or repurposing the disks in another operating system that supports ZFS is desired. It is not necessary to upgrade the pool unless the end user has a specific need for the newer ZFS Feature Flags (page 375). If a pool is upgraded to the latest feature flags, it will not be possible to import that pool into another operating system that does not yet support those feature flags.

To perform the ZFS pool upgrade, go to Storage → Pools and click ◼ (Settings) to upgrade. Click the Upgrade Pool button as shown in Figure 2.14.

Note: If the Upgrade Pool button does not appear, the pool is already at the latest feature flags and does not need to be upgraded.
Fig. 2.14: Upgrading a Pool

The warning serves as a reminder that a pool upgrade is not reversible. 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


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

- **at least** 8192 MiB (8 GiB) base memory size
- a virtual disk **at least 8 GiB in size** to hold the operating system and boot environments
- at least one additional virtual disk **at least 4 GiB 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 ([https://www.virtualbox.org/](https://www.virtualbox.org/)) 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 2.15, to start the new virtual machine wizard.

![Fig. 2.15: Initial VirtualBox Screen](image)

Click the Next button to see the screen in Figure 2.16. 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 2.17. The base memory size must be changed to at least 8192 MiB. When finished, click Next to see the screen in Figure 2.18.
Fig. 2.17: Select the Amount of Memory Reserved for the Virtual Machine
Click Create to launch the Create Virtual Hard Drive Wizard shown in Figure 2.19.
Select VDI and click the Next button to see the screen in Figure 2.20.
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 2.21 is shown.
This screen is used to set the size (or upper limit) of the virtual disk. **Set the default size to a minimum of 8 GiB.** 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 GiB and at least one data storage disk of at least 4 GiB.

Use the Back button to return to a previous screen if any values need to be modified. After making a selection and pressing Create, the new VM is created. The new virtual machine is listed in the left frame, as shown in the example in Figure 2.22. Open the Machine Tools drop-down menu and select Details to see extra information about the VM.
Create the virtual disks to be used for storage. Highlight the VM and click **Settings** to open the menu. Click the **Storage** option in the left frame to access the storage screen seen in Figure 2.23.
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 Virtual Hard Disk wizard seen in Figure 2.19 and 2.20.

Create a disk large enough to hold the desired data. The minimum size is 4 GiB. 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 2.24.
Click *Choose Virtual Optical 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 an `.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 there is 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* → *Adapter 1*. 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 2.25*, 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 (page 31). After 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 Optical device in Storage or by unchecking Optical in the Boot Order section of System.

### 2.6.2 VMware ESXi

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 (https://www.vmware.com/products/esxi-and-esx.html).

Install and use the VMware vSphere client to connect to the ESXi server. Enter the username and password created when installing ESXi to log in to the interface. After logging in, go to Storage to upload the FreeNAS®.iso. Click Datastore browser and select a datastore for the FreeNAS®.iso. Click Upload and choose the FreeNAS®.iso from the host system.

Click Create / Register VM to create a new VM. The New virtual machine wizard opens:

1. **Select creation type**: Select Create a new virtual machine and click Next.
2. **Select a name and guest OS**: Enter a name for the VM. Leave ESXi compatibility version at the default. Select **Other** as the Guest OS family. Select **FreeBSD12 or later versions (64-bit)** as the Guest OS version. Click **Next**.
3. **Select storage**: Select a datastore for the VM. The datastore must be at least 32 GiB.
4. **Customize settings**: Enter the recommended minimums of at least 8 GiB of memory and 32 GiB of storage. Select **Datastore ISO file** from the *CD/DVD Drive 1* drop-down. Use the Datastore browser to select the uploaded FreeNAS® .iso. Click *Next*. 
5. **Ready to complete**: Review the VM settings. Click *Finish* to create the new VM.
To add more disks to a VM, right-click the VM and click *Edit Settings*.

Click *Add hard disk → New standard hard disk*. Enter the desired capacity and click *Save*. 
Virtual HPET hardware can prevent the virtual machine from booting on some older versions of VMware. If the virtual machine does not boot, remove the virtual HPET hardware:

- On ESXi, right-click the VM and click **Edit Settings**. Click **VM Options → Advanced → Edit Configuration...**. Change `hpet0.present` from TRUE to FALSE and click OK. Click **Save** to save the new settings.

- On Workstation or Player, while in **Edit Settings**, click **Options → Advanced → File Locations**. Locate the path for the Configuration file named `filename.vmx`. Open the file in a text editor and change `hpet0.present` from `true` to `false`, then save the change.
The Console Setup menu, shown in Figure 3.1, appears at the end of the boot process. If the FreeNAS® system has a keyboard and monitor, this Console Setup menu can be used to administer the system.

**Note:** When connecting to the FreeNAS® system with SSH or the web Shell (page 341), the Console Setup menu is not shown by default. It can be started by the root user or another user with root permissions by typing `/etc/netcli`.

The Console Setup menu can be disabled by unchecking *Enable Console Menu* in *System → Advanced*.

The menu provides these options:

1) **Configure Network Interfaces** provides a configuration wizard to set up the system's network interfaces.
2) **Configure Link Aggregation** is for creating or deleting link aggregations.
3) **Configure VLAN Interface** is used to create or delete VLAN interfaces.
4) **Configure Default Route** is used to set the IPv4 or IPv6 default gateway. When prompted, enter the IP address of the default gateway.
5) **Configure Static Routes** prompts for the destination network and gateway IP address. Re-enter this option for each static route needed.

---

**Console setup**

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

The web user interface is at:

http://10.0.0.102

Enter an option from 1-11:  

---

Fig. 3.1: Console Setup Menu
6) **Configure DNS** prompts for the name of the DNS domain and the IP address of the first DNS server. When adding multiple DNS servers, press Enter to enter the next one. Press Enter twice to leave this option.

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

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

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

10) **Reboot** reboots the system.

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

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

### 3.1 Obtaining an IP Address

During boot, FreeNAS® automatically attempts to connect to a DHCP server from all live network interfaces. After FreeNAS® successfully receives an IP address, the address is displayed so it can be used to access the web interface. The example in Figure 3.1 shows a FreeNAS® system that is accessible at *http://10.0.0.102*.

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

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

```plaintext
Enter an option from 1-11: 1
1) em0
Select an interface (q to quit): 1
Remove the current settings of this interface? (This causes a momentary disconnection of the network.) (y/n) n
Configure interface for DHCP? (y/n) n
Configure IPv4? (y/n) y
Interface name: (press enter, the name can be blank)
Several input formats are supported
Example 1 CIDR Notation:
  192.168.1.1/24
Example 2 IP and Netmask separate:
  IP: 192.168.1.1
  Netmask: 255.255.255.0, or /24 or 24
IPv4 Address: 192.168.1.108/24
Saving interface configuration: Ok
Configure IPv6? (y/n) n
Restarting network: ok
...

The web user interface is at
http://192.168.1.108
```
ACCESSING THE WEB INTERFACE

On a computer that can access the same network as the FreeNAS® system, enter the IP address in a web browser to connect to the web interface. The password for the root user is requested.

Fig. 4.1: Login Screen

Enter the password chosen during the installation. A prompt is shown to set a root password if it was not set during installation.

The web interface is displayed after login:
The Dashboard shows details about the system. These details are grouped into sections about the hardware components, networking, storage, and other categories.

4.1 Web Interface Troubleshooting

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

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

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

The rest of this User Guide describes the FreeNAS® web interface in more detail. The layout of this User Guide follows the order of the menu items in the tree located in the left frame of the web interface.
The (Settings) menu provides options to change the administrator password, set preferences, and view system information.

5.1 Change Password

To change the root account password, click (Settings) and Change Password. The current root password must be entered before a new password can be saved.

5.2 Preferences

The FreeNAS® User Interface can be adjusted to match the user preferences. Go to the Web Interface Preferences page by clicking the (Settings) menu in the upper-right and clicking Preferences.

5.2.1 Web Interface Preferences

This page has options to adjust global settings in the web interface, manage custom themes, and create new themes. Figure 5.1 shows the different options:
These options are applied to the entire web interface:

- **Choose Theme**: Change the active theme. Custom themes are added to this list.
- **Prefer buttons with icons only**: Set to preserve screen space and only display icons and tooltips instead of text labels.
- **Enable Password Toggle**: When set, an eye icon appears next to password fields. Clicking the icon reveals the password. Clicking it again hides the password.
- **Reset Table Columns to Default**: Set to reset all tables to display default columns.

Make any changes and click **UPDATE SETTINGS** to save the new selections.

### 5.2.2 Themes

The FreeNAS® web interface supports dynamically changing the active theme and creating new, fully customizable themes.

#### 5.2.2.1 Create New Themes

This page is used to create and preview custom FreeNAS® themes. Figure 5.2 shows many of the theming and preview options:
To create a new custom theme, click *CREATE NEW THEME*. Colors from an existing theme can be used when creating a new custom theme. Select a theme from the *Load Colors from Theme* drop-down to use the colors from that theme for the new custom theme. Table 5.1 describes each option:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Theme Name</td>
<td>string</td>
<td>Enter a name to identify the new theme.</td>
</tr>
<tr>
<td>Menu Label</td>
<td>string</td>
<td>Enter a short name to use for the FreeNAS® menus.</td>
</tr>
<tr>
<td>Menu Swatch</td>
<td>dropdown menu</td>
<td>Choose a color from the theme to display next to the menu entry of the custom theme.</td>
</tr>
<tr>
<td>Description</td>
<td>string</td>
<td>Enter a short description of the new theme.</td>
</tr>
<tr>
<td>Enable Dark Logo</td>
<td>checkbox</td>
<td>Set this to give the FreeNAS® Logo a dark fill color.</td>
</tr>
<tr>
<td>Choose Primary</td>
<td>dropdown menu</td>
<td>Choose from either a generic color or import a specific color setting to use as the primary theme color. The primary color changes the top bar of the web interface and the color of many of the buttons.</td>
</tr>
<tr>
<td>Choose Accent</td>
<td>dropdown menu</td>
<td>Choose from either a generic color or import a specific color setting to use as the accent color for the theme. This color is used for many of the buttons and smaller elements in the web interface.</td>
</tr>
</tbody>
</table>

Choose the different *COLORS* for this new theme after setting these general options. Click the color swatch to open a small popup with sliders to adjust the color. Color values can also be entered as a hexadecimal value.
Changing any color value automatically updates the Theme Preview column. This section is completely interactive and shows how the custom theme is applied to all the different elements in the web interface.

Click SAVE CUSTOM THEME when finished with all the GENERAL and COLORS options. The new theme is added to the list of available themes in Web Interface Preferences.

Click PREVIEW → Global Preview to apply the unsaved custom theme to the current session of the FreeNAS® web interface. Activating Global Preview allows going to other pages in the web interface and live testing the new custom theme.

**Note:** Setting a custom theme as a Global Preview does not save that theme! Be sure to go back to Preferences → Create Custom Theme, complete any remaining options, and click SAVE CUSTOM THEME to save the current settings as a new theme.

### 5.3 API Documentation

Click API to see documentation for the websocket protocol API ([https://en.wikipedia.org/wiki/WebSocket](https://en.wikipedia.org/wiki/WebSocket)) used in FreeNAS®.

### 5.4 About

Click 🕹️ (Settings) and About to view a popup window with basic system information. This includes system Version, Hostname, Uptime, IP address, Physical Memory, CPU Model, and Average Load.
Accounts is used to manage users and groups. This section contains these entries:

- **Groups** (page 70): used to manage UNIX-style groups on the FreeNAS® system.
- **Users** (page 73): used to manage UNIX-style accounts on the FreeNAS® system.

Each entry is described in more detail in this section.

### 6.1 Groups

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

**Note:** It is unnecessary to recreate the network users or groups when a directory service is running on the same network. Instead, import the existing account information into FreeNAS®. Refer to *Directory Services* (page 204) for details.

This section describes how to create a group and assign user accounts to it. The Groups page lists all groups, including those built in and used by the operating system.
Fig. 6.1: Group Management

The table displays group names, group IDs (GID), built-in groups, and whether `sudo` is permitted. Clicking the ![Options]( Options) icon on a user-created group entry displays *Members, Edit, and Delete* options. Click *Members* to view and modify the group membership. Built-in groups are required by the FreeNAS® system and cannot be edited or deleted.

The ADD button opens the screen shown in Figure 6.2. Table 6.1 summarizes the available options when creating a group.
Table 6.1: Group Creation Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GID</td>
<td>string</td>
<td>The next available group ID is suggested. 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. Example: the <code>sshd</code> group has an ID of 22. This setting cannot be edited once the group is created.</td>
</tr>
<tr>
<td>Name</td>
<td>string</td>
<td>Enter an alphanumeric name for the new group. Group names cannot begin with a hyphen (-) or contain a space, tab, or these characters: ; : + &amp; # % ^ ( ) ! @ ~ ? &lt; &gt; = . $ can only be used as the last character of the group name.</td>
</tr>
<tr>
<td>Permit Sudo</td>
<td>checkbox</td>
<td>Set to allow group members to use <code>sudo</code> (<a href="https://www.sudo.ws/">https://www.sudo.ws/</a>). When using <code>sudo</code>, a user is prompted for their own password.</td>
</tr>
<tr>
<td>Allow Duplicate GIDs</td>
<td>checkbox</td>
<td><strong>Not recommended.</strong> Allow more than one group to have the same group ID.</td>
</tr>
</tbody>
</table>

To change which users are members of a group, expand the group from the list and click **Members**. To add users to the group, select users in the left frame and click `->`. To remove users from the group, select users in the right frame and click `<-`. Click **SAVE** when finished changing the group members.

**Figure 6.3**, shows adding a user as a member of a group.
The *Delete* button deletes a group. The pop-up message asks if all users with this primary group should also be deleted, and to confirm the action. Note built-in groups do not have a *Delete* button.

### 6.2 Users

FreeNAS® supports users, groups, and permissions, allowing flexibility in configuring which users have access to the data stored on FreeNAS®. To assign permissions to shares, select one of these options:

1. Create a guest account for all users, or create a user account for every user in the network where the name of each account is the same as a login 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 the network uses a directory service, import the existing account information using the instructions in *Directory Services* (page 204).

*Accounts → Users* lists all system accounts installed with the FreeNAS® operating system, as shown in Figure 6.4.
By default, each user entry displays the username, User ID (UID), whether the user is built into FreeNAS®, and full name. This table is adjustable by clicking COLUMNS and setting the desired columns.

Clicking a column name sorts the list by that value. An arrow indicates which column controls the view sort order. Click the arrow to reverse the sort order.

Click \(\bigtriangledown\) (Options) on the user created account to display the Edit and Delete buttons. Note built-in users do not have a Delete button.

**Note:** Setting the email address for the built-in root user account is recommended 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)` (https://www.freebsd.org/cgi/man.cgi?query=nologin). For security reasons and to prevent breakage of system services, modifying the system accounts is discouraged.

The ADD button opens the screen shown in Figure 6.5. Table 6.2 summarizes the options that are available when user accounts are created or modified.

**Warning:** When using Active Directory (page 204), Windows user passwords must be set from within Windows.
Table 6.2: User Account Configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>string</td>
<td>Usernames can be up to 16 characters long. When using NIS or other legacy software with limited username lengths, keep usernames to eight characters or less for compatibility. Usernames cannot begin with a hyphen (-) or contain a space, tab, or these characters: ; + &amp; % ^ () ! @ ~ ? &lt; &gt; = . $ can only be used as the last character of the username.</td>
</tr>
<tr>
<td>Full Name</td>
<td>string</td>
<td>This field is mandatory and may contain spaces.</td>
</tr>
<tr>
<td>Email</td>
<td>string</td>
<td>The email address associated with the account.</td>
</tr>
<tr>
<td>Password</td>
<td>string</td>
<td>Mandatory unless Disable Password is Yes. Cannot contain a ?. Click Show (Show) to view or obscure the password characters.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>string</td>
<td>Required to match the value of Password.</td>
</tr>
<tr>
<td>User ID</td>
<td>integer</td>
<td>Grayed out if the user already exists. When creating an account, the next numeric ID is 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.</td>
</tr>
<tr>
<td>New Primary Group</td>
<td>checkbox</td>
<td>Set by default to create a new a primary group with the same name as the user. Unset to select a different primary group name.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 6.2 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Group</td>
<td>drop-down menu</td>
<td>Unset <em>New Primary Group</em> to access this menu. For security reasons, FreeBSD will not give a user <em>su</em> permissions if <em>wheel</em> is not their primary group. To give a user <em>su</em> access, add them to the <em>wheel</em> group in <strong>Auxiliary groups</strong>.</td>
</tr>
<tr>
<td>Auxiliary groups</td>
<td>drop-down menu</td>
<td>Select which groups the user will be added to.</td>
</tr>
<tr>
<td>Home Directory</td>
<td>browse button</td>
<td>Choose a path to the user’s home directory. If the directory exists and matches the username, it is set as the user’s home directory. When the path does not end with a subdirectory matching the username, a new subdirectory is created. The full path to the user’s home directory is shown here when editing a user.</td>
</tr>
<tr>
<td>Home Directory Permissions</td>
<td>checkboxes</td>
<td>Sets default Unix permissions of user’s home directory. This is <em>read-only</em> for built-in users.</td>
</tr>
<tr>
<td>SSH Public Key</td>
<td>string</td>
<td>Paste the user’s public SSH key to be used for key-based authentication. <em>Do not paste the private key!</em></td>
</tr>
<tr>
<td>Disable Password</td>
<td>drop-down</td>
<td>Yes : Disables the Password fields and removes the password from the account. The account cannot use password-based logins for services. For example, disabling the password prevents using account credentials to log in to an SMB share or open an SSH session on the system. The <em>Lock User</em> and <em>Permit Sudo</em> options are also removed. No : Requires adding a Password to the account. The account can use the saved Password to authenticate with password-based services.</td>
</tr>
<tr>
<td>Shell</td>
<td>drop-down menu</td>
<td>Select the shell to use for local and SSH logins. The <em>root</em> user shell is used for web interface Shell (page 341) sessions. See Table 6.3 for an overview of available shells.</td>
</tr>
<tr>
<td>Lock User</td>
<td>checkbox</td>
<td>Prevent the user from logging in or using password-based services until this option is unset. Locking an account is only possible when <em>Disable Password</em> is <em>No</em> and a <em>Password</em> has been created for the account.</td>
</tr>
<tr>
<td>Permit Sudo</td>
<td>checkbox</td>
<td>Give this user permission to use sudo (<a href="https://www.sudo.ws/">https://www.sudo.ws/</a>). When using sudo, a user is prompted for their account Password.</td>
</tr>
<tr>
<td>Microsoft Account</td>
<td>checkbox</td>
<td>Set if the user is connecting from a Windows 8 or newer system or when using a Microsoft cloud service.</td>
</tr>
</tbody>
</table>

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

Table 6.3: Available Shells

<table>
<thead>
<tr>
<th>Shell</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>csh</td>
<td><a href="https://en.wikipedia.org/wiki/C_shell">C shell</a></td>
</tr>
<tr>
<td>sh</td>
<td><a href="https://en.wikipedia.org/wiki/Bourne_shell">Bourne shell</a></td>
</tr>
<tr>
<td>tcsh</td>
<td><a href="https://en.wikipedia.org/wiki/Tcsh">Enhanced C Shell</a></td>
</tr>
<tr>
<td>bash</td>
<td><a href="https://en.wikipedia.org/wiki/Bash_%28Unix_shell%29">Bourne Again shell</a></td>
</tr>
<tr>
<td>ksh93</td>
<td><a href="http://www.kornshell.com/">Korn shell</a></td>
</tr>
<tr>
<td>mksh</td>
<td><a href="https://www.mirbsd.org/mksh.htm">mirBSD Korn shell</a></td>
</tr>
<tr>
<td>rbash</td>
<td><a href="http://www.gnu.org/software/bash/manual/html_node/The-Restricted-Shell.html">Restricted bash</a></td>
</tr>
</tbody>
</table>

Continued on next page
Table 6.3 – continued from previous page

<table>
<thead>
<tr>
<th>Shell</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scponly</td>
<td>Select <a href="https://github.com/scponly/scponly/wiki">scponly</a> to restrict the user's SSH usage to only the <code>scp</code> and <code>sftp</code> commands.</td>
</tr>
<tr>
<td>zsh</td>
<td><a href="http://www.zsh.org/">Z shell</a></td>
</tr>
<tr>
<td>git-shell</td>
<td><a href="https://git-scm.com/docs/git-shell">restricted git shell</a></td>
</tr>
<tr>
<td>nologin</td>
<td>Use when creating a system account or to create a user account that can authenticate with shares but which cannot login to the FreeNAS system using <code>ssh</code>.</td>
</tr>
</tbody>
</table>

Built-in user accounts needed by the system cannot be removed. A Delete button appears for custom users that were added by the system administrator. Clicking Delete opens a popup window to confirm the action and offer an option to keep the user primary group when the user is deleted.
The System section of the web interface contains these entries:

- **General** (page 78) configures general settings such as HTTPS access, the language, and the timezone
- **NTP Servers** (page 81) adds, edits, and deletes Network Time Protocol servers
- **Boot** (page 83) creates, renames, and deletes boot environments. It also shows the condition of the Boot Pool.
- **Advanced** (page 86) configures advanced settings such as the serial console, swap space, and console messages
- **Email** (page 91) configures the email address to receive notifications
- **System Dataset** (page 93) configures the location where logs and reporting graphs are stored
- **Alert Services** (page 94) configures services used to notify the administrator about system events.
- **Alert Settings** (page 96) lists the available Alert (page 345) conditions and provides configuration of the notification frequency for each alert.
- **Cloud Credentials** (page 97) is used to enter connection credentials for remote cloud service providers
- **SSH Connections** (page 101) manages connecting to a remote system with SSH.
- **SSH Keypairs** (page 105) manages all private and public SSH key pairs.
- **Tunables** (page 105) provides a front-end for tuning in real-time and to load additional kernel modules at boot time
- **Update** (page 108) performs upgrades and checks for system updates
- **CAs** (page 113): import or create internal or intermediate CAs (Certificate Authorities)
- **Certificates** (page 116): import existing certificates, create self-signed certificates, or configure ACME certificates.
- **ACME DNS** (page 122): automate domain authentication for compatible CAs and certificates.
- **Support** (page 123): report a bug or request a new feature.

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

### 7.1 General

*System → General contains options for configuring the web interface and other basic system settings.*
Fig. 7.1: General System Options

### Table 7.1: General Configuration Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI SSL Certificate</td>
<td>drop-down menu</td>
<td>The system uses a self-signed <em>certificate</em> (page 116) to enable encrypted web interface connections. To change the default certificate, select a different created or imported certificate.</td>
</tr>
<tr>
<td>WebGUI IPv4 Address</td>
<td>drop-down menu</td>
<td>Choose a recent IP addresses to limit the usage when accessing the web interface. The built-in HTTP server binds to the wildcard address of 0.0.0.0 (any address) and issues an alert if the specified address becomes unavailable.</td>
</tr>
<tr>
<td>WebGUI IPv6 Address</td>
<td>drop-down menu</td>
<td>Choose a recent IPv6 addresses to limit the usage when accessing the web interface. The built-in HTTP server binds to the wildcard address of 0.0.0.0 (any address) and issues an alert if the specified address becomes unavailable.</td>
</tr>
<tr>
<td>WebGUI HTTP Port</td>
<td>integer</td>
<td>Allow configuring a non-standard port for accessing the web interface over HTTP. Changing this setting might require changing a Firefox configuration setting (<a href="https://www.redbrick.dcu.ie/~d_fens/articles/Firefox:_This_Address_is_Restricted">https://www.redbrick.dcu.ie/~d_fens/articles/Firefox:_This_Address_is_Restricted</a>).</td>
</tr>
<tr>
<td>WebGUI HTTPS Port</td>
<td>integer</td>
<td>Allow configuring a non-standard port to access the web interface over HTTPS.</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebGUI HTTP -&gt; HTTPS Redirect</td>
<td>checkbox</td>
<td>Redirect HTTP connections to HTTPS. A GUI SSL Certificate is required for HTTPS. Activating this also sets the HTTP Strict Transport Security (HSTS) (<a href="https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security">https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security</a>) maximum age to 31536000 seconds (one year). This means that after a browser connects to the FreeNAS® web interface for the first time, the browser continues to use HTTPS and renews this setting every year.</td>
</tr>
<tr>
<td>Language</td>
<td>combo box</td>
<td>Select a language from the drop-down menu. The list can be sorted by Name or Language code (<a href="https://en.wikipedia.org/wiki/List_of_ISO_639-1_codes">https://en.wikipedia.org/wiki/List_of_ISO_639-1_codes</a>). View the translated status of a language in the webui GitHub repository (<a href="https://github.com/freenas/webui/tree/master/src/assets/i18n">https://github.com/freenas/webui/tree/master/src/assets/i18n</a>). Refer to Contributing to FreeNAS® (page 352) for more information about assisting with translations.</td>
</tr>
<tr>
<td>Console Keyboard Map</td>
<td>drop-down menu</td>
<td>Select a keyboard layout.</td>
</tr>
<tr>
<td>Timezone</td>
<td>drop-down menu</td>
<td>Select a timezone.</td>
</tr>
<tr>
<td>Syslog level</td>
<td>drop-down menu</td>
<td>When Syslog server is defined, only logs matching this level are sent.</td>
</tr>
<tr>
<td>Syslog server</td>
<td>string</td>
<td>Remote syslog server DNS hostname or IP address. Nonstandard port numbers can be used by adding a colon and the port number to the hostname, like mysyslogserver:1928. Log entries are written to local logs and sent to the remote syslog server.</td>
</tr>
<tr>
<td>Crash reporting</td>
<td>checkbox</td>
<td>Send failed HTTP request data which can include client and server IP addresses, failed method call tracebacks, and middleware log file contents to iXsystems.</td>
</tr>
<tr>
<td>Usage Collection</td>
<td>checkbox</td>
<td>Enable sending anonymous usage statistics to iXsystems.</td>
</tr>
</tbody>
</table>

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

This screen also contains these buttons:

- **SAVE CONFIG**: save a backup copy of the current configuration database in the format hostname-version-architecture to the computer accessing the web interface. Saving the configuration after making any configuration changes is highly recommended. FreeNAS® automatically backs up the configuration database to the system dataset every morning at 3:45. However, this backup does 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 also not be available. The location of the system dataset can be viewed or set using System → System Dataset.

**Note**: SSH (page 281) keys are not stored in the configuration database and must be backed up separately. System host keys are files with names beginning with ssh_host_ in /usr/local/etc/ssh/. The root user keys are stored in /root/.ssh.

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, Active Directory bind credentials, and cloud credentials are stored in an encrypted form to prevent them from being visible as plain text in the saved system configuration. The key or seed for this encryption is normally stored only on the operating system device. When Save Config is chosen, a dialog gives two options. Export Password Secret Seed includes passwords in the config-
uration file which allows the configuration file to be restored to a different operating system device where the decryption seed is not already present. Configuration backups containing the seed must be physically secured to prevent decryption of passwords and unauthorized access.

**Warning:** The *Export Password Secret Seed* option is off by default and should only be used when making a configuration backup that will be stored securely. After moving a configuration to new hardware, media containing a configuration backup with a decryption seed should be securely erased before reuse.

*Export Pool Encryption Keys* includes the encryption keys of encrypted pools in the configuration file. The encryption keys are restored if the configuration file is uploaded to the system using *UPLOAD CONFIG*.

- **UPLOAD CONFIG:** allows browsing to the location of a previously saved configuration file to restore that configuration.
- **RESET CONFIG:** reset the configuration database to the default base version. This does not delete user SSH keys or any other data stored in a user home directory. Since configuration changes stored in the configuration database are erased, this option is useful when a mistake has been made or to return a test system to the original configuration.

### 7.2 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 the 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.

Available NTP servers can be found at [https://support.ntp.org/bin/view/Servers/NTPPoolServers](https://support.ntp.org/bin/view/Servers/NTPPoolServers). For time accuracy, choose NTP servers that are geographically close to the physical location of the FreeNAS® system.

Click **System → NTP Servers** and **ADD** to add an NTP server. *Figure 7.2* shows the configuration options. *Table 7.2* summarizes the options available when adding or editing an NTP server. *ntp.conf(5)* ([https://www.freebsd.org/cgi/man.cgi?query=ntp.conf](https://www.freebsd.org/cgi/man.cgi?query=ntp.conf)) explains these options in more detail.
Fig. 7.2: Add an NTP Server

Table 7.2: NTP Servers Configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>string</td>
<td>Enter the hostname or IP address of the NTP server.</td>
</tr>
<tr>
<td>Burst</td>
<td>checkbox</td>
<td>Recommended when Max. Poll is greater than 10. Only use on personal servers.</td>
</tr>
<tr>
<td>IBurst</td>
<td>checkbox</td>
<td>Speed up the initial synchronization, taking seconds rather than minutes.</td>
</tr>
<tr>
<td>Prefer</td>
<td>checkbox</td>
<td>This option is only recommended for highly accurate NTP servers, such as those with time monitoring hardware.</td>
</tr>
<tr>
<td>Min Poll</td>
<td>integer</td>
<td>The minimum polling interval, in seconds, as a power of 2. For example, 6 means 2^6, or 64 seconds. The default is 6, minimum value is 4.</td>
</tr>
<tr>
<td>Max Poll</td>
<td>integer</td>
<td>The maximum polling interval, in seconds, as a power of 2. For example, 10 means 2^10, or 1,024 seconds. The default is 10, maximum value is 17.</td>
</tr>
<tr>
<td>Force</td>
<td>checkbox</td>
<td>Force the addition of the NTP server, even if it is currently unreachable.</td>
</tr>
</tbody>
</table>
7.3 Boot

FreeNAS® supports a ZFS feature known as multiple boot environments. With multiple boot environments, the process of updating the operating system becomes a low-risk operation. The updater automatically creates a snapshot of the current boot environment and adds it to the boot menu before applying the update.

If an update fails, reboot the system and select the previous boot environment, using the instructions in *If Something Goes Wrong* (page 41), to instruct the system to go back to that system state.

**Note:** Boot environments are separate from 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 to load the current configuration values. If the intent is to make configuration changes rather than operating system changes, make a backup of the configuration database first using the instructions in *System → General* (page 78).

The example shown in Figure 7.3, includes the two boot environments that are created when FreeNAS® is installed. The *Initial-Install* boot environment can be booted into if the system needs to be returned to a non-configured version of the installation.

![Fig. 7.3: Viewing Boot Environments](image)

Each boot environment entry contains this information:

- **Name:** the name of the boot entry as it will appear in the boot menu. Alphanumeric characters, dashes (-), underscores (_), and periods (.) are allowed.
- **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.

• **Space**: displays the size of the boot environment.

• **Keep**: indicates whether or not this boot environment can be pruned if an update does not have enough space to proceed. Click † (Options) and *Keep* for an entry if that boot environment should not be automatically pruned.

Click † (Options) on an entry to access actions specific to that entry:

• **Activate**: only appears on entries which are not currently set to *Active*. Changes the selected entry to the default boot entry on next boot. The status changes to *Reboot* and the current *Active* entry changes from *Now/Reboot* to *Now*, indicating that it was used on the last boot but will not be used on the next boot.

• **Clone**: makes a new boot environment from the selected boot environment. When prompted for the name of the clone, alphanumeric characters, dashes (‐), underscores (´), and periods (.) are allowed.

• **Rename**: used to change the name of the boot environment. Alphanumeric characters, dashes (‐), underscores (´), and periods (.) are allowed.

• **Delete**: used to delete the highlighted entry, which also removes that entry from the boot menu. Since an activated entry cannot be deleted, this button does not appear for the active boot environment. To delete an entry that is currently activated, first activate another entry. Note that this button does not appear for the default boot environment as this entry is needed to return the system to the original installation state.

• **Keep**: 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.

Click **ACTIONS** to:

• **Add**: make a new boot environment from the active environment. The active boot environment contains the text *Now/Reboot* in the *Active* column. Only alphanumeric characters, underscores, and dashes are allowed in the *Name*.

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

• **Boot Pool Status**: display the status of each device in the operating system device, including any read, write, or checksum errors.

• **Scrub Boot Pool**: perform a manual scrub of the operating system device.

### 7.3.1 Operating System Device Mirroring

*System → Boot → Boot Pool Status* is used to manage the devices comprising the operating system device. An example is seen in Figure 7.4.
FreeNAS® supports 2-device mirrors for the operating system device. In a mirrored configuration, a failed device can be detached and replaced.

An additional device can be attached to an existing one-device operating system device, with these caveats:

- The new device must have at least the same capacity as the existing device. Larger capacity devices can be added, but the mirror will only have the capacity of the smallest device. Different models of devices which advertise the same nominal size are not necessarily the same actual size. For this reason, adding another device of the same model is recommended.
- It is **strongly recommended** to use SSDs rather than USB devices when creating a mirrored operating system device.

Click ![Options](Options) on a device entry to access actions specific to that device:

- **Attach**: use to add a second device to create a mirrored operating system device. If another device is available, it appears in the **Member disk** drop-down menu. Select the desired device. The **Use all disk space** option controls the capacity made available to the operating system device. By default, the new device is partitioned to the same size as the existing device. When **Use all disk space** is enabled, the entire capacity of the new device is used. If the original operating system device fails and is detached, the boot mirror will consist of just the newer drive, and will grow to whatever capacity it provides. However, new devices added to this mirror must now be as large as the new capacity. Click **SAVE** to attach the new disk to the mirror.
- **Detach**: remove the failed device from the mirror so that it can be replaced.
- **Replace**: once the failed device has been detached, select the new replacement device from the **Member disk** drop-down menu to rebuild the mirror.
### 7.4 Advanced

*System → Advanced* is shown in Figure 7.5. The configurable settings are summarized in Table 7.3.

![FreeNAS Advanced Screen](image)

**Fig. 7.5: Advanced Screen**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Text Console without Password Prompt</td>
<td>checkbox</td>
<td>Set for the text console to be available without entering a password.</td>
</tr>
<tr>
<td>Enable Serial Console</td>
<td>checkbox</td>
<td><em>Do not</em> enable this option if the serial port is disabled. Adds the <em>Serial Port</em> and <em>Serial Speed</em> fields.</td>
</tr>
<tr>
<td>Serial Port</td>
<td>string</td>
<td>Select the serial port address in hex.</td>
</tr>
<tr>
<td>Serial Speed</td>
<td>drop-down menu</td>
<td>Select the speed in bps used by the serial port.</td>
</tr>
<tr>
<td>Swap size in GiB</td>
<td>non-zero number</td>
<td>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. Setting to 0 disables swap creation completely. This is strongly discouraged.</td>
</tr>
<tr>
<td>Enable autotune</td>
<td>checkbox</td>
<td>Enable the <em>Autotune</em> (page 87) script which attempts to optimize the system based on the installed hardware. <em>Warning:</em> Autotuning is only used as a temporary measure and is not a permanent fix for system hardware issues.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 7.3 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Debug Kernel</td>
<td>checkbox</td>
<td>Use a debug version of the kernel on the next boot.</td>
</tr>
<tr>
<td>Show console messages</td>
<td>checkbox</td>
<td>Display console messages from <code>/var/log/console.log</code> in real time at bottom of browser window. Click the console to bring up a scrollable screen. Set the <code>Stop refresh</code> option in the scrollable screen to pause updates. Unset to continue watching messages as they occur. When this option is set, a button to show the console log appears on busy spinner dialogs.</td>
</tr>
<tr>
<td>MOTD banner</td>
<td>string</td>
<td>This message is shown when a user logs in with SSH.</td>
</tr>
<tr>
<td>Show advanced fields</td>
<td>checkbox</td>
<td>Show <code>Advanced Mode</code> fields by default.</td>
</tr>
<tr>
<td>Use FQDN for logging</td>
<td>checkbox</td>
<td>Include the Fully-Qualified Domain Name (FQDN) in logs to precisely identify systems with similar hostnames.</td>
</tr>
<tr>
<td>ATA Security User</td>
<td>drop-down menu</td>
<td>User passed to <code>camcontrol security -u</code> for unlocking SEDs. Values are <code>User</code> or <code>Master</code>.</td>
</tr>
<tr>
<td>SED Password</td>
<td>string</td>
<td>Global password used to unlock Self-Encrypting Drives (page 87).</td>
</tr>
<tr>
<td>Reset SED Password</td>
<td>checkbox</td>
<td>Select to clear the <code>Password for SED</code> column of Storage → Disks.</td>
</tr>
</tbody>
</table>

Click the **SAVE** button after making any changes.

This tab also contains this button:

**SAVE DEBUG**: used to generate text files that contain diagnostic information. After the debug data is collected, the system prompts for a location to save the compressed `.tar` file.

### 7.4.1 Autotune

FreeNAS® provides an autotune script which optimizes the system depending on the installed hardware. For example, if a pool exists on a system with limited RAM, the autotune script automatically adjusts some ZFS `sysctl` values in an attempt to minimize memory starvation issues. 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 such a system, as it caps the ARC.

The `Enable autotune` option in System → Advanced is off by default. Enable this option to run the autotuner at boot. To run the script immediately, reboot the system.

If the autotune script adjusts any settings, the changed values appear in System → Tunables. Note that deleting tunables that were created by autotune only affects the current session, as autotune-set tunables are recreated at boot. This means that any autotune-set value that is manually changed will revert back to the value set by autotune on reboot. To permanently change a value set by autotune, change the description of the tunable. For example, changing the description to `manual override` prevents autotune from reverting that tunable back to the autotune default value.

When attempting to increase the performance of the FreeNAS® system, and particularly when the current hardware may be limiting performance, try enabling autotune.

For those who wish to see which checks are performed, the autotune script is located in `/usr/local/bin/autotune`.

### 7.4.2 Self-Encrypting Drives

FreeNAS® version 11.1-U5 introduced Self-Encrypting Drive (SED) support.

These SED specifications are supported:

- Legacy interface for older ATA devices. **Not recommended for security-critical environments**
• TCG Opal 1 (https://trustedcomputinggroup.org/wp-content/uploads/Opal SSC_1.00_rev3.00-Final.pdf) legacy specification

• TCG OPAL 2 (https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-Opal SSC_v2.01_rev1.00.pdf) standard for newer consumer-grade devices

• TCG Opalite (https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-Opalite SSC_FAQ.pdf) is a reduced form of OPAL 2

• TCG Pyrite Version 1 (https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-Pyrite SSC_v1.00_r1.00.pdf) and Version 2 (https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-Pyrite SSC_v2.00_r1.00_PUB.pdf) are similar to Opalite, but hardware encryption is removed. Pyrite provides a logical equivalent of the legacy ATA security for non-ATA devices. Only the drive firmware is used to protect the device.

Danger: Pyrite Version 1 SEDs do not have PSID support and can become unusable if the password is lost.

• TCG Enterprise (https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-SSC_Enterprise-v1.01_r1.00.pdf) is designed for systems with many data disks. These SEDs do not have the functionality to be unlocked before the operating system boots.

See this Trusted Computing Group® and NVM Express® joint white paper (https://nvmexpress.org/wp-content/uploads/TCGandNVMe_Joint_White_Paper-TCG_Storage_Opal_and_NVMe_FINAL.pdf) for more details about these specifications.

FreeNAS® implements the security capabilities of camcontrol (https://www.freebsd.org/cgi/man.cgi?query=camcontrol) for legacy devices and sedutil-cli (https://www.mankier.com/8/sedutil-cli) for TCG devices. When managing a SED from the command line, it is recommended to use the sedhelper wrapper script for sedutil-cli to ease SED administration and unlock the full capabilities of the device. Examples of using these commands to identify and deploy SEDs are provided below.

A SED can be configured before or after assigning the device to a pool (page 168).

By default, SEDs are not locked until the administrator takes ownership of them. Ownership is taken by explicitly configuring a global or per-device password in the FreeNAS® web interface and adding the password to the SEDs. Adding SED passwords to FreeNAS® also allows FreeNAS® to automatically unlock SEDs.

A password-protected SED protects the data stored on the device when the device is physically removed from the FreeNAS® system. This allows secure disposal of the device without having to first wipe the contents. Repurposing a SED on another system requires the SED password.

### 7.4.2.1 Deploying SEDs

Run sedutil-cli --scan in the Shell (page 341) to detect and list devices. The second column of the results identifies the drive type:

- **no** indicates a non-SED device
- **1** indicates a legacy TCG OPAL 1 device
- **2** indicates a modern TCG OPAL 2 device
- **L** indicates a TCG Opalite device
- **p** indicates a TCG Pyrite 1 device
- **P** indicates a TCG Pyrite 2 device
- **E** indicates a TCG Enterprise device

Example:
FreeNAS® supports setting a global password for all detected SEDs or setting individual passwords for each SED. Using a global password for all SEDs is strongly recommended to simplify deployment and avoid maintaining separate passwords for each SED.

### Setting a Global Password for SEDs

Go to **System → Advanced → SED Password** and enter the password. **Record this password and store it in a safe place!**

Now the SEDs must be configured with this password. Go to the **Shell** (page 341) and enter `sedhelper setup password`, where password is the global password entered in **System → Advanced → SED Password**.

*sedhelper* ensures that all detected SEDs are properly configured to use the provided password:

```
root@truenas1:~ # sedhelper setup abcd1234
da9 [OK]
da10 [OK]
da11 [OK]
```

Rerun `sedhelper setup password` every time a new SED is placed in the system to apply the global password to the new SED.

### Creating Separate Passwords for Each SED

Go to **Storage → Disks**. Click ![Options](page 341) for the confirmed SED, then **Edit**. Enter and confirm the password in the **SED Password** and **Confirm SED Password** fields.

The **Storage → Disks** screen shows which disks have a configured SED password. The **SED Password** column shows a mark when the disk has a password. Disks that are not a SED or are unlocked using the global password are not marked in this column.

The SED must be configured to use the new password. Go to the **Shell** (page 341) and enter `sedhelper setup --disk da1 password`, where **da1** is the SED to configure and **password** is the created password from **Storage → Disks → Edit Disks → SED Password**.

This process must be repeated for each SED and any SEDs added to the system in the future.

**Danger:** Remember SED passwords! If the SED password is lost, SEDs cannot be unlocked and their data is unavailable. Always record SED passwords whenever they are configured or modified and store them in a secure place!

### 7.4.2.2 Check SED Functionality

When SED devices are detected during system boot, FreeNAS® checks for configured global and device-specific passwords.

Unlocking SEDs allows a pool to contain a mix of SED and non-SED devices. Devices with individual passwords are unlocked with their password. Devices without a device-specific password are unlocked using the global password.
To verify SED locking is working correctly, go to the Shell (page 341). Enter `sedutil-cli --listLockingRange 0 password dev/da1`, where `da1` is the SED and `password` is the global or individual password for that SED. The command returns `ReadLockEnabled: 1, WriteLockEnabled: 1, and LockOnReset: 1` for drives with locking enabled:

```
root@truenas1:~ # sedutil-cli --listLockingRange 0 abcd1234 /dev/da9
Band[0]:
  Name: Global_Range
  CommonName: Locking
  RangeStart: 0
  RangeLength: 0
  ReadLockEnabled: 1
  WriteLockEnabled: 1
  ReadLocked: 0
  WriteLocked: 0
  LockOnReset: 1
```

### 7.4.2.3 Managing SED Passwords and Data

This section contains command line instructions to manage SED passwords and data. The command used is `sedutil-cli(8)` ([https://www.mankier.com/8/sedutil-cli](https://www.mankier.com/8/sedutil-cli)). Most SEDs are TCG-E (Enterprise) or TCG-Opal ([Opal v2.0](https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-Opal_SSC_v2.01_rev1.00.pdf)). Commands are different for the different drive types, so the first step is identifying which type is being used.

**Warning:** These commands can be destructive to data and passwords. Keep backups and use the commands with caution.

Check SED version on a single drive, `/dev/da0` in this example:

```
root@truenas:~ # sedutil-cli --isValidSED /dev/da0
/dev/da0 SED --E--- Micron_5N/A U402
```

All connected disks can be checked at once:

```
root@truenas:~ # sedutil-cli --scan
Scanning for Opal compliant disks
/dev/da0 No 32GB SATA Flash Drive SFDK003L
/dev/da1 No 32GB SATA Flash Drive SFDK003L
/dev/da0 E Micron_SN/A U402
/dev/da1 E Micron_SN/A U402
/dev/da12 E SEAGATE XS3840TE70014 0103
/dev/da13 E SEAGATE XS3840TE70014 0103
/dev/da14 E SEAGATE XS3840TE70014 0103
/dev/da2 E Micron_SN/A U402
/dev/da3 E Micron_SN/A U402
/dev/da4 E Micron_SN/A U402
/dev/da5 E Micron_SN/A U402
/dev/da6 E Micron_SN/A U402
/dev/da9 E Micron_SN/A U402
No more disks present ending scan
root@truenas:~ #
```

**TCG-Opal Instructions**

Reset the password without losing data: `sedutil-cli --revertNoErase oldpassword /dev/device`

Use both of these commands to change the password without destroying data:
sedutil-cli --setSIDPassword oldpassword newpassword /dev/device
sedutil-cli --setPassword oldpassword Admin1 newpassword /dev/device

Wipe data and reset password to default MSID: sedutil-cli --revertPer oldpassword /dev/device
Wipe data and reset password using the PSID: sedutil-cli --yesIreallywanttoERASEALLmydatausingthePSID PSINODASHED /dev/device where PSINODASHED is the PSID located on the physical drive with no dashes (-).

TCG-E Instructions

Use all of these commands to reset the password without losing data:

sedutil-cli --setSIDPassword oldpassword "" /dev/device
sedutil-cli --setPassword oldpassword EraseMaster "" /dev/device
sedutil-cli --setPassword oldpassword BandMaster0 "" /dev/device
sedutil-cli --setPassword oldpassword BandMaster1 "" /dev/device

Use all of these commands to change the password without destroying data:

sedutil-cli --setSIDPassword oldpassword newpassword /dev/device
sedutil-cli --setPassword oldpassword EraseMaster newpassword /dev/device
sedutil-cli --setPassword oldpassword BandMaster0 newpassword /dev/device
sedutil-cli --setPassword oldpassword BandMaster1 newpassword /dev/device

Wipe data and reset password to default MSID:

sedutil-cli --eraseLockingRange 0 password /dev/<device>
sedutil-cli --setSIDPassword oldpassword "" /dev/<device>
sedutil-cli --setPassword oldpassword EraseMaster "" /dev/<device>

Wipe data and reset password using the PSID: sedutil-cli --yesIreallywanttoERASEALLmydatausingthePSID PSINODASHED /dev/device where PSINODASHED is the PSID located on the physical drive with no dashes (-).

7.5 Email

An automatic script sends a nightly email to the root user account containing important information such as the health of the disks. Alert (page 345) events are also emailed to the root user account. Problems with Scrub Tasks (page 149) are reported separately in an email sent at 03:00AM.

Note: S.M.A.R.T. (page 275) reports are mailed separately to the address configured in that service.

The administrator typically does not read email directly on the FreeNAS® system. Instead, these emails are usually sent to an external email address where they can be read more conveniently. It is important to configure the system so it can send these emails to the administrator’s remote email account so they are aware of problems or status changes.
The first step is to set the remote address where email will be sent. Go to Accounts → Users, click 📋 (Options) and Edit for the root user. In the Email field, enter the email address on the remote system where email is to be sent, like admin@example.com. Click SAVE to save the settings.

Additional configuration is performed with System → Email, shown in Figure 7.6.

![Fig. 7.6: Email Screen](image)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From E-mail</td>
<td>string</td>
<td>The envelope From address shown in the email. This can be set to make filtering mail on the receiving system easier.</td>
</tr>
<tr>
<td>From Name</td>
<td>string</td>
<td>The friendly name to show in front of the sending email address.</td>
</tr>
<tr>
<td>Outgoing Mail Server</td>
<td>string or IP address</td>
<td>Hostname or IP address of SMTP server used for sending this email.</td>
</tr>
<tr>
<td>Mail Server Port</td>
<td>integer</td>
<td>SMTP port number. Typically 25, 465 (secure SMTP), or 587 (submission).</td>
</tr>
<tr>
<td>Security</td>
<td>drop-down menu</td>
<td>Choose an encryption type. Choices are Plain (No Encryption), SSL (Implicit TLS), or TLS (STARTTLS).</td>
</tr>
<tr>
<td>SMTP Authentication</td>
<td>checkbox</td>
<td>Enable or disable SMTP AUTH (<a href="https://en.wikipedia.org/wiki/SMTP_Authentication">https://en.wikipedia.org/wiki/SMTP_Authentication</a>) using PLAIN SASL. Setting this enables the required Username and optional Password fields.</td>
</tr>
<tr>
<td>Username</td>
<td>string</td>
<td>Enter the SMTP username when the SMTP server requires authentication.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 7.4 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>string</td>
<td>Enter the SMTP account password if needed for authentication. Only plain text characters (7-bit ASCII) are allowed in passwords. UTF or composed characters are not allowed.</td>
</tr>
</tbody>
</table>

Click the **SEND TEST MAIL** button to verify that the configured email settings are working. If the test email fails, double-check that the Email field of the root user is correctly configured by clicking the **Edit** button for the root account in **Accounts → Users**.


### 7.6 System Dataset

**System → System Dataset**, shown in Figure 7.7, is used to select the pool which contains the persistent system dataset. The system dataset stores debugging core files, encryption keys (page 173) for encrypted pools, and Samba4 metadata such as the user/group cache and share level permissions.

![Fig. 7.7: System Dataset Screen](image)

Use the **System Dataset Pool** drop-down menu to select the volume (pool) to contain the system dataset. The system dataset can be moved to unencrypted volumes (pools) or encrypted volumes which do not have passphrases. If the system dataset is moved to an encrypted volume, that volume is no longer allowed to be locked or have a passphrase set.
Moving the system dataset also requires restarting the SMB (page 277) service. A dialog warns that the SMB service must be restarted, causing a temporary outage of any active SMB connections.

System logs can also be stored on the system dataset. Storing this information on the system dataset is recommended when large amounts of data is being generated and the system has limited memory or a limited capacity operating system device.

Set Syslog to store system logs on the system dataset. Leave unset to store system logs in /var on the operating system device.

Click SAVE to save changes.

If the pool storing the system dataset is changed at a later time, FreeNAS® migrates the existing data in the system dataset to the new location.

Note: Depending on configuration, the system dataset can occupy a large amount of space and receive frequent writes. Do not put the system dataset on a flash drive or other media with limited space or write life.

### 7.7 Reporting

This section contains settings to customize some of the reporting tools. These settings are described in Table 7.5

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report CPU usage in percent</td>
<td>checkbox</td>
<td>Report CPU usage in percent instead of units of kernel time.</td>
</tr>
<tr>
<td>Remote Graphite Server Host-name</td>
<td>string</td>
<td>Hostname or IP address of a remote Graphite (<a href="http://graphiteapp.org/">http://graphiteapp.org/</a>) server.</td>
</tr>
<tr>
<td>Graph Age in Months</td>
<td>integer</td>
<td>Maximum time a graph is stored in months (allowed values are 1 - 60). Changing this value causes the Confirm RRD Destroy dialog to appear. Changes do not take effect until the existing reporting database is destroyed.</td>
</tr>
<tr>
<td>Number of Graph Points</td>
<td>integer</td>
<td>Number of points for each hourly, daily, weekly, monthly, or yearly graph (allowed values are 1 - 4096). Changing this value causes the Confirm RRD Destroy checkbox to appear. Changes do not take effect until the existing reporting database is destroyed.</td>
</tr>
</tbody>
</table>

Changes to Reporting settings (page 94) clear the report history. To keep history with the old settings, cancel the warning dialog. Click RESET TO DEFAULTS to restore the original settings.

### 7.8 Alert Services

FreeNAS® can use a number of methods to notify the administrator of system events that require attention. These events are system Alerts (page 345).

Available alert services:
- AWS-SNS (https://aws.amazon.com/sns/)
- E-mail
- InfluxDB (https://www.influxdata.com/)
- Mattermost (https://about.mattermost.com/)
Warning: These alert services might use a third party commercial vendor not directly affiliated with iXsystems. Please investigate and fully understand that vendor’s pricing policies and services before using their alert service. iXsystems is not responsible for any charges incurred from the use of third party vendors with the Alert Services feature.

Select System → Alert Services to show the Alert Services screen, Figure 7.8.

Click ADD to display the Add Alert Service form, Figure 7.9.
Select the **Type** to choose an alert service to configure.

Alert services can be set for a particular severity **Level**. All alerts of that level are then sent out with that alert service. For example, if the **E-Mail** alert service **Level** is set to **Info**, any **Info** level alerts are sent by that service. Multiple alert services can be set to the same level. For instance, **Critical** alerts can be sent both by email and PagerDuty by setting both alert services to the **Critical** level.

The configurable fields and required information differ for each alert service. Set **Enabled** to activate the service. Enter any other required information and click **SAVE**.

Click **SEND TEST ALERT** to test the chosen alert service.

All saved alert services are displayed in **System → Alert Services**. To delete an alert service, click † (Options) and **Delete**. To disable an alert service temporarily, click † (Options) and **Edit**, then unset the **Enabled** option.

### 7.9 Alert Settings

**System → Alert Settings** has options to configure each FreeNAS® **Alert** (page 345).
Alerts are grouped by web interface feature or service monitor. To customize alert importance, use the Warning Level drop-down. To adjust how often alert notifications are sent, use the Frequency drop-down. Setting the Frequency to NEVER prevents that alert from being added to alert notifications, but the alert can still show in the web interface if it is triggered.

To configure where alert notifications are sent, use Alert Services (page 94).

### 7.10 Cloud Credentials

FreeNAS® can use cloud services for features like Cloud Sync Tasks (page 151). The rclone (https://rclone.org/) credentials to provide secure connections with cloud services are entered here. Amazon S3, Backblaze B2, Box, Dropbox, FTP, Google Cloud Storage, Google Drive, HTTP, hubiC, Mega, Microsoft Azure Blob Storage, Microsoft OneDrive, pCloud, SFTP, WebDAV, and Yandex are available.

**Note:** The hubiC cloud service has suspended creation of new accounts (https://www.ovh.co.uk/subscriptions-hubic-ended/).

**Warning:** Cloud Credentials are stored in encrypted form. To be able to restore Cloud Credentials from a saved configuration (page 78), “Export Password Secret Seed” must be set when saving that configuration.

Click System → Cloud Credentials to see the screen shown in Figure 7.11.
The list shows the **Account Name** and **Provider** for each credential. There are options to **Edit** and **Delete** a credential after clicking \( \text{Options} \) for a credential.

Click **ADD** to add a new cloud credential. Choose a **Provider** to display any specific options for that provider. **Figure 7.12** shows an example configuration:
Enter a descriptive and unique name for the cloud credential in the Name field. The remaining options vary by Provider, and are shown in Table 7.6. Clicking a provider name opens a new browser tab to the rclone documentation (https://rclone.org/docs/) for that provider.

### Table 7.6: Cloud Credential Options

<table>
<thead>
<tr>
<th>Provider</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon S3 (<a href="https://rclone.org/s3/">https://rclone.org/s3/</a>)</td>
<td>Access Key ID</td>
<td>Enter the Amazon Web Services Key ID. This is found on Amazon AWS (<a href="https://aws.amazon.com">https://aws.amazon.com</a>) by going through My Account -&gt; Security Credentials -&gt; Access Keys. Must be alphanumeric and between 5 and 20 characters.</td>
</tr>
<tr>
<td>Amazon S3 (<a href="https://rclone.org/s3/">https://rclone.org/s3/</a>)</td>
<td>Secret Access Key</td>
<td>Enter the Amazon Web Services password. If the Secret Access Key cannot be found or remembered, go to My Account -&gt; Security Credentials -&gt; Access Keys and create a new key pair. Must be alphanumeric and between 8 and 40 characters.</td>
</tr>
<tr>
<td>Amazon S3 (<a href="https://rclone.org/s3/">https://rclone.org/s3/</a>)</td>
<td>Endpoint URL</td>
<td>Set Advanced Settings to access this option. S3 API endpoint URL (<a href="https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteEndpoints.html">https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteEndpoints.html</a>). When using AWS, the endpoint field can be empty to use the default endpoint for the region, and available buckets are automatically fetched. Refer to the AWS Documentation for a list of Simple Storage Service Website Endpoints (<a href="https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_website_region_endpoints">https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_website_region_endpoints</a>).</td>
</tr>
<tr>
<td>Provider</td>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Amazon S3 (<a href="https://rclone.org/s3/">https://rclone.org/s3/</a>)</td>
<td>Disable Endpoint Region</td>
<td>Set Advanced Settings to access this option. Skip automatic detection of the Endpoint URL region. Set this when configuring a custom Endpoint URL.</td>
</tr>
<tr>
<td>Amazon S3 (<a href="https://rclone.org/s3/">https://rclone.org/s3/</a>)</td>
<td>Use Signature Version 2</td>
<td>Set Advanced Settings to access this option. Force using Signature Version 2 (<a href="https://docs.aws.amazon.com/general/latest/gr/signature-version-2.html">https://docs.aws.amazon.com/general/latest/gr/signature-version-2.html</a>) to sign API requests. Set this when configuring a custom Endpoint URL.</td>
</tr>
<tr>
<td>Backblaze B2 (<a href="https://rclone.org/b2/">https://rclone.org/b2/</a>)</td>
<td>Key ID, Application Key</td>
<td>Alphanumeric Backblaze B2 (<a href="https://www.backblaze.com/b2/cloud-storage.html">https://www.backblaze.com/b2/cloud-storage.html</a>) application keys. To generate a new application key, log in to the Backblaze account, go to the App Keys page, and add a new application key. Copy the keyID and applicationKey strings into the FreeNAS® web interface fields.</td>
</tr>
<tr>
<td>Box (<a href="https://rclone.org/box/">https://rclone.org/box/</a>)</td>
<td>Access Token</td>
<td>Configured with Open Authentication (page 101).</td>
</tr>
<tr>
<td>Dropbox (<a href="https://rclone.org/dropbox/">https://rclone.org/dropbox/</a>)</td>
<td>Access Token</td>
<td>Configured with Open Authentication (page 101). The access token can be manually created by going to the Dropbox App Console (<a href="https://www.dropbox.com/developers/apps">https://www.dropbox.com/developers/apps</a>). After creating an app, go to Settings and click Generate under the Generated access token field.</td>
</tr>
<tr>
<td>FTP (<a href="https://rclone.org/ftp/">https://rclone.org/ftp/</a>)</td>
<td>Host, Port</td>
<td>Enter the FTP host and port.</td>
</tr>
<tr>
<td>FTP (<a href="https://rclone.org/ftp/">https://rclone.org/ftp/</a>)</td>
<td>Username, Password</td>
<td>Enter the FTP username and password.</td>
</tr>
<tr>
<td>Google Drive (<a href="https://rclone.org/drive/">https://rclone.org/drive/</a>)</td>
<td>Access Token, Team Drive ID</td>
<td>The Access Token is configured with Open Authentication (page 101). Team Drive ID is only used when connecting to a Team Drive (<a href="https://developers.google.com/drive/api/v3/reference/teambuckets">https://developers.google.com/drive/api/v3/reference/teambuckets</a>). The ID is also the ID of the top level folder of the Team Drive.</td>
</tr>
<tr>
<td>HTTP (<a href="https://rclone.org/http/">https://rclone.org/http/</a>)</td>
<td>URL</td>
<td>Enter the HTTP host URL.</td>
</tr>
<tr>
<td>hubiC (<a href="https://rclone.org/hubic/">https://rclone.org/hubic/</a>)</td>
<td>Access Token</td>
<td>Enter the access token. See the Hubic guide (<a href="https://api.hubic.com/sandbox/">https://api.hubic.com/sandbox/</a>) for instructions to obtain an access token.</td>
</tr>
<tr>
<td>Microsoft Azure Blob Storage (<a href="https://rclone.org/azureblob/">https://rclone.org/azureblob/</a>)</td>
<td>Account Name, Account Key</td>
<td>Enter the Azure Blob Storage account name and key.</td>
</tr>
</tbody>
</table>
Table 7.6 – continued from previous page

<table>
<thead>
<tr>
<th>Provider</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>Access Token, Drives List, Drive Account Type, Drive ID</td>
<td>The Access Token is configured with Open Authentication (page 101). Authenticating a Microsoft account adds the Drives List and selects the correct Drive Account Type. The Drives List shows all the drives and IDs registered to the Microsoft account. Selecting a drive automatically fills the Drive ID field.</td>
</tr>
<tr>
<td>OneDrive</td>
<td>Access Token, Drives List, Drive Account Type, Drive ID</td>
<td>Configured with Open Authentication (page 101).</td>
</tr>
<tr>
<td>SFTP</td>
<td>Host, Port, Username, Password, Private Key ID</td>
<td>Enter the SFTP host and port. Enter an account user name that has SSH access to the host. Enter the password for that account or import the private key from an existing SSH keypair (page 105). To create a new SSH key for this credential, open the Private Key ID drop-down and select Generate New.</td>
</tr>
<tr>
<td>WebDAV</td>
<td>URL, WebDAV service</td>
<td>Enter the URL and use the dropdown to select the WebDAV service.</td>
</tr>
<tr>
<td>Yandex</td>
<td>Access Token</td>
<td>Configured with Open Authentication (page 101).</td>
</tr>
</tbody>
</table>

For Amazon S3, Access Key and Secret Key values are found on the Amazon AWS website by clicking on the account name, then My Security Credentials and Access Keys (Access Key ID and Secret Access Key). Copy the Access Key value to the FreeNAS® Cloud Credential Access Key field, then enter the Secret Key value saved when the key pair was created. If the Secret Key value is unknown, a new key pair can be created on the same Amazon screen. Open Authentication (OAuth) (https://openauthentication.org/) is used with some cloud providers. These providers have a LOGINTO PROVIDER button that opens a dialog to log in to that provider and fill the Access Token field with valid credentials.

Enter the information and click VERIFY CREDENTIAL. The Credential is valid. displays when the credential information is verified.

More details about individual Provider settings are available in the rclone documentation (https://rclone.org/about/).

7.11 SSH Connections

Secure Socket Shell (SSH) (https://searchsecurity.techtarget.com/definition/Secure-Shell) is a network protocol that provides a secure method to access and transfer files between two hosts while using an unsecure network. SSH can use user account credentials to establish secure connections, but often uses key pairs shared between host systems for authentication.

FreeNAS® uses System → SSH Connections to quickly create SSH connections and show any saved connections. These connections are required when creating a new replication (page 146) to back up dataset snapshots.

The remote system must be configured to allow SSH connections. Some situations can also require allowing root account access to the remote system. For FreeNAS® systems, go to Services and edit the SSH (page 281) service to allow SSH connections and root account access.

To add a new SSH connection, go to System → SSH Connections and click ADD.
Table 7.7: SSH Connection Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>string</td>
<td>Descriptive name of this SSH connection. SSH connection names must be unique.</td>
</tr>
</tbody>
</table>
| Setup Method  | drop-down menu | How to configure the connection:  
Manual requires configuring authentication on the remote system. This can require copying SSH keys and modifying the root user account on that system. See Manual Setup (page 103).  
Semi-automatic is only functional when configuring an SSH connection between FreeNAS® systems. After authenticating the connection, all remaining connection options are automatically configured. See Semi-Automatic Setup (page 104). |
| Host          | string     | Enter the hostname or IP address of the remote system. Only available with Manual configurations. |
| Port          | integer    | Port number on the remote system to use for the SSH connection. Only available with Manual configurations. |
| FreeNAS URL   | string     | Hostname or IP address of the remote FreeNAS® system. Only available with Semi-automatic configurations. A valid URL scheme is required. Example: `https://10.231.3.76` |
| Username      | string     | User account name to use for logging in to the remote system.  
Password       | string     | User account password used to log in to the FreeNAS® system. Only available with Semi-automatic configurations. |
| Private Key   | drop-down menu | Choose a saved SSH Keypair (page 105) or select Generate New to create a new keypair and apply it to this connection. |
| Remote Host Key | string     | Remote system SSH key for this system to authenticate the connection. Only available with Manual configurations. When all other fields are properly configured, click DISCOVER REMOTE HOST KEY to query the remote system and automatically populate this field. |
| Cipher        | drop-down menu | Connection security level:  
• Standard is most secure, but has the greatest impact on connection speed.  
• Fast is less secure than Standard but can give reasonable transfer rates for devices with limited cryptographic speed.  
• Disabled removes all security in favor of maximizing connection speed. Disabling the security should only be used within a secure, trusted network. |
| Connect Timeout | integer    | Time (in seconds) before the system stops attempting to establish a connection with the remote system. |

Saved connections can be edited or deleted. Deleting an SSH connection also deletes or disables paired SSH Keypairs (page 105), Replication Tasks (page 146), and Cloud Credentials (page 97).

### 7.11.1 Manual Setup

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

The examples here and in Semi-Automatic Setup (page 104) refer to the FreeNAS® system that is configuring a new connection in System → SSH Connections as Host 1. The FreeNAS® system that is receiving the encryption key is Host 2.

On Host 1, go to System → SSH Keypairs and create a new SSH Keypair (page 105). Highlight the entire Public Key text, right-click in the highlighted area, and click Copy.
Log in to Host 2 and go to Accounts → Users. Click ⚒ (Options) for the root account, then Edit. Paste the copied key into the SSH Public Key field and click SAVE as shown in Figure 7.13.

![Fig. 7.13: Paste the Replication Key](image)

Switch back to Host 1 and go to System → SSH Connections and click ADD. Set the Setup Method to Manual, select the previously created keypair as the Private Key, and fill in the rest of the connection details for Host 2. Click DISCOVER REMOTE HOST KEY to obtain the remote system key. Click SAVE to store this SSH connection.

### 7.11.2 Semi-Automatic Setup

FreeNAS® offers a semi-automatic setup mode that simplifies setting up an SSH connection with another FreeNAS or TrueNAS system. When administrator account credentials are known for Host 2, semi-automatic setup allows configuring the SSH connection without logging in to Host 2 to transfer SSH keys.

In Host 1, go to System → SSH Keypairs and create a new SSH Keypair (page 105). Go to System → SSH Connections and click ADD.

Choose Semi-automatic as the Setup Method. Enter the Host 2 URL in FreeNAS URL using the format http://freenas.remote, where freenas.remote is the Host 2 hostname or IP address.

Enter credentials for an Host 2 user account that can accept SSH connection requests and modify Host 2. This is typically the root account.

Select the SSH keypair that was just created for the Private Key.

Fill in the remaining connection configuration fields and click SAVE. Host 1 can use this saved configuration to establish a connection to Host 2 and exchange the remaining authentication keys.
7.12 SSH Keypairs

FreeNAS® generates and stores RSA-encrypted (https://en.wikipedia.org/wiki/RSA_%28cryptosystem%29) SSH public and private keypairs in System → SSH Keypairs. These are generally used when configuring SSH Connections (page 101) or SFTP Cloud Credentials (page 97). Encrypted keypairs or keypairs with passphrases are not supported.

To generate a new keypair, click ADD, enter a name, and click GENERATE KEYPAIR. The Private Key and Public Key fields fill with the key strings. SSH key pair names must be unique.

![Example Keypair](image)

Click SAVE to store the new keypair. These saved keypairs can be selected later in the web interface without having to manually copy the key values.

Keys are viewed or modified by going to System → SSH Keypairs and clicking (Options) and Edit for the keypair name.

Deleting an SSH Keypair also deletes any associated SSH Connections (page 101), Replication Tasks (page 146) or SFTP Cloud Credentials (page 97) that use this keypair are disabled but not removed.

7.13 Tunables

System → Tunables can be used to manage:

1. FreeBSD sysctls: a sysctl(8) (https://www.freebsd.org/cgi/man.cgi?query=sysctl) 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)` ([https://www.freebsd.org/cgi/man.cgi?query=rc.conf](https://www.freebsd.org/cgi/man.cgi?query=rc.conf)) 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 before testing 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 ([https://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/](https://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/)).

To add a loader, sysctl, or `rc.conf` option, go to **System → Tunables** and click **ADD** to access the screen shown in Figure 7.15.

![Fig. 7.15: Adding a Tunable](image)

**Table 7.8** summarizes the options when adding a tunable.

---

106
Table 7.8: Adding a Tunable

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
<td>string</td>
<td>The name of the sysctl or driver to load.</td>
</tr>
<tr>
<td>Value</td>
<td>integer or string</td>
<td>Set a value for the Variable. Refer to the man page for the specific driver or the FreeBSD Handbook (<a href="https://www.freebsd.org/doc/en_US.ISO08859-1/books/handbook/">https://www.freebsd.org/doc/en_US.ISO08859-1/books/handbook/</a>) for suggested values.</td>
</tr>
<tr>
<td>Type</td>
<td>drop-down menu</td>
<td>Choices are Loader, rc.conf, and Sysctl.</td>
</tr>
<tr>
<td>Description</td>
<td>string</td>
<td>Optional. Enter a description of this tunable.</td>
</tr>
<tr>
<td>Enabled</td>
<td>checkbox</td>
<td>Deselect this option to disable the tunable without deleting it.</td>
</tr>
</tbody>
</table>

**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 the Enabled option is deselected.

Existing tunables are listed in System → Tunables. To change the value of an existing tunable, click † (Options) and Edit. To remove a tunable, click † (Options) and Delete.

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

The web interface does not display the sysctls that are pre-set when FreeNAS® is installed. FreeNAS® 11.3 ships with the sysctls set:

```
kern.corefile=/var/tmp/%N.core
kern.metadelay=3
kern.dirdelay=4
kern.filedelay=5
kern.coredump=1
kern.sugid_coredump=1
vfs.timestamp_precision=3
net.link.lagg.lacp.default_strict_mode=0
vfs.zfs.min_auto_ashift=12
```

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

The web interface does not display the loaders that are pre-set when FreeNAS® is installed. FreeNAS® 11.3 ships with these loaders set:

```
product="FreeNAS"
autoboot_delay="5"
loader_logo="FreeNAS"
loader_menu_title="Welcome to FreeNAS"
loader_brand="FreeNAS"
loader_version=" "
kern.cam.boot_delay="30000"
d debug.debugger_on_panic=1
d debug.ddb.textdump.pending=1
hw.hptrr.attach_generic=0
vfs.mountroot.timeout="30"
ispfw_load="YES"
ipmi_load="YES"
freenas_sysctl_load="YES"
hint.isp.0.role=2
hint.isp.1.role=2
hint.isp.2.role=2
hint.isp.3.role=2
```
Do not add or edit the default tunables. Changing the default tunables can make the system unusable. The ZFS version used in 11.3 deprecates these tunables:

kvfs.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

After upgrading from an earlier version of FreeNAS®, these tunables are automatically deleted. Please do not manually add them back.

7.14 Update

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

7.14.1 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. Most updates require a system reboot. Plan updates around scheduled maintenance times to avoid disrupting user activities.

The update process will not proceed unless there is enough free space in the boot pool for the new update files. If a space warning is shown, go to Boot (page 83) to remove unneeded boot environments.

7.14.2 Updates and Trains

Cryptographically signed update files are used to update FreeNAS®. Update files provide flexibility in deciding when to upgrade the system. Go to Boot (page 41) to test an update.

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

Update trains are labeled with a numeric version followed by a short description. The current version receives regular bug fixes and new features. Supported older versions of FreeNAS® only receive maintenance updates. Several specific words are used to describe the type of train:
• **STABLE**: Bug fixes and new features are available from this train. Upgrades available from a **STABLE** train are tested and ready to apply to a production environment.

• **Nightlies**: Experimental train used for testing future versions of FreeNAS®.

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

**Warning**: The UI will warn if the currently selected train is not suited for production use. Before using a non-production train, be prepared to experience bugs or problems. Testers are encouraged to submit bug reports at [https://bugs.ixsystems.com](https://bugs.ixsystems.com).

### 7.14.3 Checking for Updates

Figure 7.16 shows an example of the **System → Update** screen.

![Update Options](image)

The system checks daily for updates and downloads an update if one is available. An alert is issued when a new update becomes available. The automatic check and download of updates is disabled by unsetting **Check for Updates Daily and Download if Available**. Click 🔄 (Refresh) to perform another check for updates.

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

**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 9.10 train cannot be selected while booted into a 11 boot environ-
ment. To go back to an earlier version after testing or running a more recent version, reboot and select a boot environment for that earlier version. This screen can then be used to check for updates that train.

In the example shown in Figure 7.17, information about the update is displayed along with a link to the release notes. It is important to read the release notes before updating to determine if any of the changes in that release impact the use of the system.

[Fig. 7.17: Reviewing Updates]

7.14.4 Saving the Configuration File

A dialog to save the system configuration file (page 80) appears before installing updates.
7.14.5 Applying Updates

Make sure the system is in a low-usage state as described above in Preparing for Updates (page 108).

Click DOWNLOAD UPDATES to immediately download and install an update.

The Save Configuration (page 110) dialog appears so the current configuration can be saved to external media.

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

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

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 inBoot (page 83) are not removed. If space for a new boot environment is not available, the upgrade fails. Space on the operating system device can be manually freed using System → Boot. Review the boot environments and remove the Keep attribute or delete any boot environments that are no longer needed.

7.14.6 Manual Updates

Updates can also be manually downloaded and applied in System → Update.
Note: Manual updates cannot be used to upgrade from older major versions.


Download the file to a desktop or laptop computer. Connect to FreeNAS® with a browser and go to System → Update. Click INSTALL MANUAL UPDATE FILE.

The Save Configuration (page 110) dialog opens. This makes it possible to save a copy of the current configuration to external media for backup in case of an update problem.

After the dialog closes, the manual update screen is shown:

The current version of FreeNAS® is shown for verification.

Select the manual update file with the Browse button. Set Reboot After Update to reboot the system after the update has been installed. Click APPLY UPDATE to begin the update.

7.14.7 Update in Progress

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

FreeNAS® can act as a Certificate Authority (CA). When encrypting SSL or TLS connections to the FreeNAS® system, either import an existing certificate, or create a CA on the FreeNAS® system, then create a certificate. This certificate will appear in the drop-down menus for services that support SSL or TLS.

For secure LDAP, the public key of an existing CA can be imported with *Import CA*, or a new CA created on the FreeNAS® system and used on the LDAP server also.

*Figure 7.18* shows the screen after clicking *System → CAs*.

![Fig. 7.18: Initial CA Screen](image)

If the organization already has a CA, the CA certificate and key can be imported. Click *ADD* and set the *Type* to *Import CA* to see the configuration options shown in *Figure 7.19*. The configurable options are summarized in Table 7.9.
Fig. 7.19: Importing a CA

Table 7.9: Importing a CA Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>string</td>
<td>Enter a descriptive name for the CA using only alphanumeric, underscore (_), and dash (-) characters.</td>
</tr>
<tr>
<td>Type</td>
<td>drop-down menu</td>
<td>Choose the type of CA. Choices are Internal CA, Intermediate CA, and Import CA.</td>
</tr>
<tr>
<td>Certificate</td>
<td>string</td>
<td>Mandatory. Paste in the certificate for the CA.</td>
</tr>
<tr>
<td>Private Key</td>
<td>string</td>
<td>If there is a private key associated with the Certificate, paste it here. Private keys must be at least 1024 bits long.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>string</td>
<td>If the Private Key is protected by a passphrase, enter it here and repeat it in the “Confirm Passphrase” field.</td>
</tr>
</tbody>
</table>

To 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 (https://en.wikipedia.org/wiki/Root_certificate).

To create a CA for internal use only, click ADD and set the Type to Internal CA. Figure 7.20 shows the available options.
The configurable options are described in Table 7.10. When completing the fields for the certificate authority, supply the information for the organization.

Table 7.10: Internal CA Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>string</td>
<td>Enter a descriptive name for the CA using only alphanumeric, underscore (_), and dash (–) characters.</td>
</tr>
<tr>
<td>Type</td>
<td>drop-down menu</td>
<td>Choose the type of CA. Choices are <em>Internal CA</em>, <em>Intermediate CA</em>, and <em>Import CA</em>.</td>
</tr>
<tr>
<td>EC Curve</td>
<td>drop-down menu</td>
<td>Elliptic curve to apply to the certificate authority key. Choose from different <em>Brainpool</em> or <em>SEC</em> curve parameters. See <em>RFC 5639</em> (<a href="https://tools.ietf.org/html/rfc5639">https://tools.ietf.org/html/rfc5639</a>) and <em>SEC 2</em> (<a href="http://www.secg.org/sec2-v2.pdf">http://www.secg.org/sec2-v2.pdf</a>) for more details. Applies to <em>EC</em> keys only.</td>
</tr>
<tr>
<td>Key Length</td>
<td>drop-down menu</td>
<td>For security reasons, a minimum of 2048 is recommended. Applies to <em>RSA</em> keys only.</td>
</tr>
<tr>
<td>Digest Algorithm</td>
<td>drop-down menu</td>
<td>The default is acceptable unless the organization requires a different algorithm.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 7.10 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifetime</td>
<td>integer</td>
<td>The lifetime of a CA is specified in days.</td>
</tr>
<tr>
<td>Country</td>
<td>drop-down menu</td>
<td>Select the country for the organization.</td>
</tr>
<tr>
<td>State</td>
<td>string</td>
<td>Enter the state or province of the organization.</td>
</tr>
<tr>
<td>Locality</td>
<td>string</td>
<td>Enter the location of the organization.</td>
</tr>
<tr>
<td>Organization</td>
<td>string</td>
<td>Enter the name of the company or organization.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>string</td>
<td>Organizational unit of the entity.</td>
</tr>
<tr>
<td>Email</td>
<td>string</td>
<td>Enter the email address for the person responsible for the CA.</td>
</tr>
<tr>
<td>Common Name</td>
<td>string</td>
<td>Enter the fully-qualified hostname (FQDN) of the system. The Common Name must be unique within a certificate chain.</td>
</tr>
<tr>
<td>Subject Alternate Names</td>
<td>string</td>
<td>Multi-domain support. Enter additional space separated domain names.</td>
</tr>
</tbody>
</table>

To create an intermediate CA which is part of a certificate chain, set the Type to Intermediate CA. This screen adds one more option to the screen shown in Figure 7.20:

- **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.

Imported or created CAs are added as entries in System → CAs. The columns in this screen indicate the name of the CA, whether it is an internal CA, whether the issuer is self-signed, the CA lifetime (in days), the common name of the CA, the date and time the CA was created, and the date and time the CA expires.

Click ✖️ (Options) on an existing CA to access these configuration buttons:

- **View**: use this option to view the contents of an existing Certificate, Private Key, or to edit the Identifier.
- **Sign CSR**: used to sign internal Certificate Signing Requests created using System → Certificates → Create CSR. Signing a request adds a new certificate to System → Certificates.
- **Export Certificate**: prompts to browse to the location to save a copy of the CA’s X.509 certificate on the computer being used to access the FreeNAS® system.
- **Export Private Key**: prompts to browse to the location to save a copy of the CA’s private key on the computer being used to access the FreeNAS® system. This option only appears if the CA has a private key.
- **Delete**: prompts for confirmation before deleting the CA.

### 7.16 Certificates

FreeNAS® can import existing certificates or certificate signing requests, 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 (page 113).

Go to System → Certificates to add or view certificates.
FreeNAS® uses a self-signed certificate to enable encrypted access to the web interface. This certificate is generated at boot and cannot be deleted until a different certificate is chosen as the GUI SSL Certificate (page 79).

To import an existing certificate, click ADD and set the Type to Import Certificate. Figure 7.22 shows the options. 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 7.11.
Table 7.11: Certificate Import Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>string</td>
<td>Enter a descriptive name for the certificate using only alphanumeric, underscore (_), and dash (-) characters.</td>
</tr>
<tr>
<td>Type</td>
<td>drop-down menu</td>
<td>Choose the type of certificate. Choices are Internal Certificate, Certificate Signing Request, Import Certificate, and Import Certificate Signing Request.</td>
</tr>
<tr>
<td>CSR exists on this system</td>
<td>checkbox</td>
<td>Set when the certificate being imported already has a Certificate Signing Request (CSR) on the system.</td>
</tr>
<tr>
<td>Signing Certificate Authority</td>
<td>drop-down menu</td>
<td>Select a previously created or imported CA. Active when CSR exists on this system is set.</td>
</tr>
<tr>
<td>Certificate</td>
<td>string</td>
<td>Paste the contents of the certificate.</td>
</tr>
<tr>
<td>Private Key</td>
<td>string</td>
<td>Paste the private key associated with the certificate. Private keys must be at least 1024 bits long. Active when CSR exists on this system is unset.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>string</td>
<td>If the private key is protected by a passphrase, enter it here and repeat it in the Confirm Passphrase field. Active when CSR exists on this system is unset.</td>
</tr>
</tbody>
</table>

Importing a certificate signing request requires copying the contents of the signing request and key files into the form. Having the signing request CERTIFICATE REQUEST and PRIVATE KEY strings visible in a separate window simplifies the import process.
Table 7.12: Certificate Signing Request Import Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>string</td>
<td>Enter a descriptive name for the certificate using only alphanumeric, underscore (_), and dash (-) characters.</td>
</tr>
<tr>
<td>Type</td>
<td>drop-down menu</td>
<td>Choose the type of certificate. Choices are Internal Certificate, Certificate Signing Request, Import Certificate, and Import Certificate Signing Request.</td>
</tr>
<tr>
<td>Signing Request</td>
<td>drop-down menu</td>
<td>Paste the CERTIFICATE REQUEST string from the signing request.</td>
</tr>
<tr>
<td>Private Key</td>
<td>string</td>
<td>Paste the private key associated with the certificate signing request. Private keys must be at least 1024 bits long.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>string</td>
<td>If the private key is protected by a passphrase, enter it here and repeat it in the Confirm Passphrase field.</td>
</tr>
</tbody>
</table>

To create a new self-signed certificate, set the Type to Internal Certificate to see the options shown in Figure 7.23. The configurable options are summarized in Table 7.13. When completing the fields for the certificate authority, use the information for the organization. Since this is a self-signed certificate, use the CA that was imported or created with CAs (page 113) as the signing authority.

![Fig. 7.23: Creating a New Certificate](image-url)
### Table 7.13: Certificate Creation Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>string</td>
<td>Enter a descriptive name for the certificate using only alphanumeric, underscore (_), and dash (-) characters.</td>
</tr>
<tr>
<td>Type</td>
<td>drop-down menu</td>
<td>Choose the type of certificate. Choices are <code>Internal Certificate</code>, <code>Certificate Signing Request</code>, and <code>Import Certificate</code>.</td>
</tr>
<tr>
<td>Signing Certificate Authority</td>
<td>drop-down menu</td>
<td>Select the CA which was previously imported or created using CA (page 113).</td>
</tr>
<tr>
<td>EC Curve</td>
<td>drop-down menu</td>
<td>Elliptic curve to apply to the certificate key. Choose from different Brainpool or SEC curve parameters. See RFC 5639 (<a href="https://tools.ietf.org/html/rfc5639">https://tools.ietf.org/html/rfc5639</a>) and SEC 2 (<a href="http://www.secg.org/sec2-v2.pdf">http://www.secg.org/sec2-v2.pdf</a>) for more details. Applies to EC keys only.</td>
</tr>
<tr>
<td>Key Length</td>
<td>drop-down menu</td>
<td>For security reasons, a minimum of 2048 is recommended. Applies to RSA keys only.</td>
</tr>
<tr>
<td>Digest Algorithm</td>
<td>drop-down menu</td>
<td>The default is acceptable unless the organization requires a different algorithm.</td>
</tr>
<tr>
<td>Lifetime</td>
<td>integer</td>
<td>The lifetime of the certificate is specified in days.</td>
</tr>
<tr>
<td>Country</td>
<td>drop-down menu</td>
<td>Select the country for the organization.</td>
</tr>
<tr>
<td>State</td>
<td>string</td>
<td>State or province of the organization.</td>
</tr>
<tr>
<td>Locality</td>
<td>string</td>
<td>Location of the organization.</td>
</tr>
<tr>
<td>Organization</td>
<td>string</td>
<td>Name of the company or organization.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>string</td>
<td>Organizational unit of the entity.</td>
</tr>
<tr>
<td>Email</td>
<td>string</td>
<td>Enter the email address for the person responsible for the CA.</td>
</tr>
<tr>
<td>Common Name</td>
<td>string</td>
<td>Enter the fully-qualified hostname (FQDN) of the system. The <code>Common Name must</code> be unique within a certificate chain.</td>
</tr>
<tr>
<td>Subject Alternate Names</td>
<td>string</td>
<td>Multi-domain support. Enter additional domain names and separate them with a space.</td>
</tr>
</tbody>
</table>

If the certificate is signed by an external CA, such as Verisign, instead create a certificate signing request. To do so, set the `Type` to `Certificate Signing Request`. The options from Figure 7.23 display, but without the `Signing Certificate Authority` and `Lifetime` fields.

Certificates that are imported, self-signed, or for which a certificate signing request is created are added as entries to `System → Certificates`. In the example shown in Figure 7.24, 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 with a new certificate set to `Import Certificate`. This makes the certificate available as a configurable option for encrypting connections.
Clicking  (Options) for an entry shows these configuration buttons:

- **View:** use this option to view the contents of an existing Certificate, Private Key, or to edit the Identifier.

- **Create ACME Certificate:** use an ACME DNS (page 122) authenticator to verify, issue, and renew a certificate. Only visible with certificate signing requests.

- **Export Certificate** saves 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** saves 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** is used to delete a certificate or certificate signing request.

### 7.16.1 ACME Certificates


ACME certificates can be created for existing certificate signing requests. These certificates use an ACME DNS (page 122) authenticator to confirm domain ownership, then are automatically issued and renewed. To create a new ACME certificate, go to System → Certificates, click  (Options) for an existing certificate signing request, and click Create ACME Certificate.
### Table 7.14: ACME Certificate Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>string</td>
<td>Internal identifier of the certificate. Only alphanumeric characters, dash (-), and underline (_) are allowed.</td>
</tr>
<tr>
<td>Terms of Service</td>
<td>checkbox</td>
<td>Please accept the terms of service for the given ACME Server.</td>
</tr>
<tr>
<td>Renew Certificate Day</td>
<td>integer</td>
<td>Number of days to renew certificate before expiring.</td>
</tr>
<tr>
<td>ACME Server Directory URI</td>
<td>drop-down menu</td>
<td>URI of the ACME Server Directory. Choose a preconfigured URI or enter a custom URI.</td>
</tr>
<tr>
<td>Authenticator for (Domain Name)</td>
<td>drop-down menu</td>
<td>Authenticator to validate the Domain. Choose a previously configured ACME DNS (page 122) authenticator.</td>
</tr>
<tr>
<td>(Domain Name) (Domain Name)</td>
<td></td>
<td>dynamically changes</td>
</tr>
</tbody>
</table>

### 7.17 ACME DNS

Go to System → ACME DNS and click ADD to show options to add a new DNS authenticator to FreeNAS®. This is used to create ACME Certificates (page 121) that are automatically issued and renewed after being validated.
Enter a name for the authenticator. This is only used to identify the authenticator in the FreeNAS® web interface. Choose a DNS provider and configure any required Authenticator Attributes:

- **Route 53**: Amazon DNS web service. Requires entering an Amazon account Access ID Key and Secret Access Key. See the AWS documentation (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html) for more details about generating these keys.

Click **SAVE** to register the DNS Authenticator and add it to the list of authenticator options for **ACME Certificates** (page 121).

### 7.18 Support

The FreeNAS® **Support** option, shown in Figure 7.27, provides a built-in ticketing system for generating bug reports and feature requests.
This screen provides a built-in interface to the FreeNAS® issue tracker located at https://bugs.ixsystems.com. An account is required to create tickets and receive notifications as issues are addressed.

Log in to an existing account to enter an issue. If you do not have an account yet, go to https://bugs.ixsystems.com, click Register, and fill out the form. Reply to the registration email to validate the account before logging in.

Before creating a bug report or feature request, ensure that an existing report does not already exist at https://bugs.ixsystems.com. If a similar issue is already present and has not been marked Closed or Resolved, comment on that issue, adding new information to help solve it. When similar issues are Closed or Resolved, create a new issue and refer to the previous issue.

**Note:** Update the system to the latest version of STABLE and retest before reporting an issue. Newer versions of the software might have already fixed the problem.

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

- **Username:** enter the login name created when registering at https://bugs.ixsystems.com.
- **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 until a registered Username and Password are entered. The field remains empty 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**: enabling this option is recommended so an overview of the system hardware, build string, and configuration is automatically generated and included with the ticket. Generating and attaching a debug to the ticket can take some time.

Debug file attachments are limited to 20 MiB. If the debug file is too large to include, unset the option to generate the debug file and let the system create an issue ticket as shown below. Manually create a debug file by going to **System → Advanced** and clicking **SAVE DEBUG**.

Go to the ticket at [https://bugs.ixsystems.com](https://bugs.ixsystems.com) and add the debug file as a private attachment.

• **Subject**: enter a descriptive title for the ticket. A good Subject makes it easy to find similar reports.

• **Description**: enter a one- to three-paragraph summary of the issue that describes the problem, and if applicable, what steps can be taken to reproduce it.

• **Attach screenshots**: select screenshots on the client system to include with the report.

Click **SUBMIT** to automatically generate and upload the report to the issue tracker ([https://bugs.ixsystems.com](https://bugs.ixsystems.com)). This process can take several minutes while information is collected and sent. All files included with the report are added to the issue tracker ticket as private attachments and can only be accessed by the creator of the ticket and iXsystems.

After the new ticket is created, the ticket URL is shown for viewing or updating with more information.
The Tasks section of the web interface is used to configure repetitive tasks:

- **Cron Jobs** (page 126) schedules a command or script to automatically execute at a specified time
- **Init/Shutdown Scripts** (page 128) configures a command or script to automatically execute during system startup or shutdown
- **Rsync Tasks** (page 129) schedules data synchronization to another system
- **S.M.A.R.T. Tests** (page 135) schedules disk tests
- **Periodic Snapshot Tasks** (page 136) schedules automatic creation of filesystem snapshots
- **Replication Tasks** (page 146) automate the replication of snapshots to a remote system
- **Resilver Priority** (page 148) controls the priority of resilvers
- **Scrub Tasks** (page 149) schedules scrubs as part of ongoing disk maintenance
- **Cloud Sync Tasks** (page 151) schedules data synchronization to cloud providers

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

**Note:** By default, **Scrub Tasks** (page 149) are run once a month by an automatically-created task. **S.M.A.R.T. Tests** (page 135) and **Periodic Snapshot Tasks** (page 136) must be set up manually.

### 8.1 Cron Jobs

cron(8) (https://www.freebsd.org/cgi/man.cgi?query=cron) is a daemon that runs a command or script on a regular schedule as a specified user.

Go to **Tasks → Cron Jobs** and click **ADD** to create a cron job.
Table 8.1 lists the configurable options for a cron job.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>string</td>
<td>Enter a description of the cron job.</td>
</tr>
<tr>
<td>Command</td>
<td>drop-down menu</td>
<td>Enter the <strong>full path</strong> to the command or script to be run. If it is a script, testing it at the command line first is recommended.</td>
</tr>
<tr>
<td>Run As User</td>
<td>string</td>
<td>Select a user account to run the command. The user must have permissions allowing them to run the command or script. Output from executing a cron task is emailed to this user if <strong>Email</strong> has been configured for that <strong>user account</strong> (page 73).</td>
</tr>
<tr>
<td>Schedule</td>
<td>drop-down menu</td>
<td>Select a schedule preset or choose <strong>Custom</strong> to open the advanced scheduler. Note that an in-progress cron task postpones any later scheduled instance of the same task until the running task is complete.</td>
</tr>
<tr>
<td>Hide Standard Output</td>
<td>checkbox</td>
<td>Hide standard output (stdout) from the command. When unset, any standard output is mailed to the user account cron used to run the command.</td>
</tr>
<tr>
<td>Hide Standard Error</td>
<td>checkbox</td>
<td>Hide error output (stderr) from the command. When unset, any error output is mailed to the user account cron used to run the command.</td>
</tr>
<tr>
<td>Enable</td>
<td>checkbox</td>
<td>Set to allow this scheduled cron task to activate. Unsetting this option disables the cron task without deleting it.</td>
</tr>
</tbody>
</table>

Cron jobs are shown in **Tasks** → **Cron Jobs**. This table displays the user, command, description, schedule, and
whether the job is enabled. This table is adjustable by setting the different column checkboxes above it. Set Toggle to display all options in the table. Click ‡ (Options) for to show the Run Now, Edit, and Delete options.

Note: % symbols are automatically escaped and do not need to be prefixed with backslashes. For example, use date ’+%Y-%m-%d’ in a cron job to generate a filename based on the date.

### 8.2 Init/Shutdown Scripts

FreeNAS® provides the ability to schedule commands or scripts to run at system startup or shutdown. Go to Tasks → Init/Shutdown Scripts and click ADD.

![Fig. 8.2: Add an Init/Shutdown Command or Script](image)

#### Table 8.2: Init/Shutdown Command or Script Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>drop-down menu</td>
<td>Select Command for an executable or Script for an executable script.</td>
</tr>
<tr>
<td>Command or Script</td>
<td>string</td>
<td>If Command is selected, enter the command with any options. When Script is selected, click  ■ (Browse) to select the script from an existing pool.</td>
</tr>
</tbody>
</table>

Continued on next page
### 8.3 Rsync Tasks

Rsync ([https://www.samba.org/ftp/rsync/rsync.html](https://www.samba.org/ftp/rsync/rsync.html)) is a utility that 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 is used for backups, mirroring data on multiple systems, or for copying files between systems.

Rsync is most effective when only a relatively small amount of the data has changed. There are also some limitations when using rsync with Windows files ([https://forums.freenas.org/index.php?threads/impaired-rsync-permissions-support-for-windows-datasets.43973/](https://forums.freenas.org/index.php?threads/impaired-rsync-permissions-support-for-windows-datasets.43973/)). For large amounts of data, data that has many changes from the previous copy, or Windows files, **Replication Tasks** (page 146) are often the faster and better solution.

Rsync is single-threaded and gains little from multiple processor cores. To see whether rsync is currently running, use `ps` from the **Shell** (page 341).

Both ends of an rsync connection must be configured:

- 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. To synchronize data between two FreeNAS® systems, create the **rsync task** on the **rsync client**.

FreeNAS® supports two modes of rsync operation:

- **Module**: exports a directory tree, and the configured settings of the tree 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® web interface under Services → Rsync Configure → Rsync Module. In other operating systems, the module is defined in rsyncd.conf(5) (https://www.samba.org/ftp/rsync/rsyncd.conf.html).

- **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 8.3 shows the screen that appears after navigating to Tasks → Rsync Tasks and clicking ADD. Table 8.3 summarizes the configuration options available when creating an rsync task.

![Fig. 8.3: Adding an Rsync Task](image)

Table 8.3: Rsync Configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>browse button</td>
<td><em>Browse</em> to the path to be copied. FreeNAS® verifies that the remote path exists. <em>[FreeBSD path length limits](page 20)</em> apply on the FreeNAS® system. Other operating systems can have different limits which might affect how they can be used as sources or destinations.</td>
</tr>
<tr>
<td>User</td>
<td>drop-down menu</td>
<td>Select the user to run the rsync task. The user selected must have permissions to write to the specified directory on the remote host.</td>
</tr>
</tbody>
</table>
### Table 8.3 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Host</td>
<td>string</td>
<td>Enter the IP address or hostname of the remote system that will store the copy. Use the format <code>username@remote_host</code> if the username differs on the remote host.</td>
</tr>
<tr>
<td>Remote SSH Port</td>
<td>integer</td>
<td>Only available in SSH mode. Allows specifying an SSH port other than the default of 22.</td>
</tr>
<tr>
<td>Rsync mode</td>
<td>drop-down menu</td>
<td>The choices are Module mode or SSH mode.</td>
</tr>
<tr>
<td>Remote Module Name</td>
<td>string</td>
<td>At least one module must be defined in <code>rsyncd.conf(5)</code> (<a href="https://www.samba.org/ftp/rsync/rsyncd.conf.html">https://www.samba.org/ftp/rsync/rsyncd.conf.html</a>) of the rsync server or in the Rsync Modules of another system.</td>
</tr>
<tr>
<td>Remote Path</td>
<td>string</td>
<td>Only appears when using SSH mode. Enter the existing path on the remote host to sync with, for example, <code>/mnt/pool</code>. Note that the path length cannot be greater than 255 characters.</td>
</tr>
<tr>
<td>Validate Remote Path</td>
<td>checkbox</td>
<td>Verifies the existence of the Remote Path.</td>
</tr>
<tr>
<td>Direction</td>
<td>drop-down menu</td>
<td>Direct the flow of the data to the remote host. Choices are Push or Pull. Default is to push to a remote host.</td>
</tr>
<tr>
<td>Short Description</td>
<td>string</td>
<td>Enter a description of the rsync task.</td>
</tr>
<tr>
<td>Schedule the Rsync Task</td>
<td>drop-down menu</td>
<td>Choose how often to run the task. Choices are Hourly, Daily, Weekly, Monthly, or Custom. Selecting Custom opens the Advanced Scheduler (page 22).</td>
</tr>
<tr>
<td>Recursive</td>
<td>checkbox</td>
<td>Set to include all subdirectories of the specified directory. When unset, only the specified directory is included.</td>
</tr>
<tr>
<td>Times</td>
<td>checkbox</td>
<td>Set to preserve the modification times of files.</td>
</tr>
<tr>
<td>Compress</td>
<td>checkbox</td>
<td>Set to reduce the size of the data to transmit. Recommended for slow connections.</td>
</tr>
<tr>
<td>Archive</td>
<td>checkbox</td>
<td>When set, rsync is run recursively, preserving symlinks, permissions, modification times, group, and special files. When run as root, owner, device files, and special files are also preserved. Equivalent to <code>rsync -rlptgoD</code>.</td>
</tr>
<tr>
<td>Delete</td>
<td>checkbox</td>
<td>Set to delete files in the destination directory that do not exist in the source directory.</td>
</tr>
<tr>
<td>Quiet</td>
<td>checkbox</td>
<td>Suppress rsync task status alerts (page 345).</td>
</tr>
<tr>
<td>Preserve permissions</td>
<td>checkbox</td>
<td>Set to preserve original file permissions. This is useful when the user is set to root.</td>
</tr>
<tr>
<td>Preserve extended attributes</td>
<td>checkbox</td>
<td>Extended attributes (<a href="https://en.wikipedia.org/wiki/Extended_file_attributes">https://en.wikipedia.org/wiki/Extended_file_attributes</a>) are preserved, but must be supported by both systems.</td>
</tr>
<tr>
<td>Delay Updates</td>
<td>checkbox</td>
<td>Set to save the temporary file from each updated file to a holding directory until the end of the transfer when all transferred files are renamed into place.</td>
</tr>
<tr>
<td>Extra options</td>
<td>string</td>
<td>Additional <code>rsync(1)</code> (<a href="http://rsync.samba.org/ftp/rsync/rsync.html">http://rsync.samba.org/ftp/rsync/rsync.html</a>) options to include. Note: The <code>*</code> character must be escaped with a backslash (<code>\*.txt</code>) or used inside single quotes. (<code>’*.txt’</code>)</td>
</tr>
<tr>
<td>Enabled</td>
<td>checkbox</td>
<td>Enable this rsync task. Unset to disable this rsync task without deleting it.</td>
</tr>
</tbody>
</table>

If the rsync server requires password authentication, enter `--password-file=/PATHTO/FILENAME` in the Extra options field, replacing `/PATHTO/FILENAME` with the appropriate path to the file containing the password.

Created rsync tasks are listed in Rsync Tasks. Click ⌁ (Options) for an entry to display buttons for Edit, Delete, or Run Now.

The Status column shows the status of the rsync task. To view the detailed rsync logs for a task, click the Status entry when the task is running or finished.
Rsync tasks also generate an Alert (page 345) on task completion. The alert shows if the task succeeded or failed.

### 8.3.1 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 pool 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**. 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 *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* option is enabled so that the original permissions are not overwritten by the *root* user

On **PULL**, an rsync module is defined in **Services → Rsync Configure → Rsync Module, ADD**. In this example:

- the *ModuleName* 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

Descriptions of the configurable options can be found in **Rsync Modules** (page 272).

- *Hosts allow* is set to `192.168.2.2`, the IP address of the rsync client

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

### 8.3.2 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** (page 341) on **PUSH** and run `ssh-keygen`. This 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.

```bash
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):
```

---

132
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:
The key’s randomart image is:
+---[ RSA 2048]---+
<p>| .o. oo |
| o+o. . |
| . =o + |
| + + o |
| S o . |
| o |
| o oo |</p>
<table>
<thead>
<tr>
<th>*oE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>-----------------</td>
</tr>
</tbody>
</table>

FreeNAS® supports RSA keys for SSH. When creating the key, use \texttt{-t rsa} to specify this type of key. Refer to Key-based Authentication (https://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/openssh.html#security-ssh-keygen) for more information.

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

\texttt{su - user1}

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

\texttt{more .ssh/id_rsa.pub}

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC1lBEXRgw1W8y8k+lXPlVR3xsmVSJtsoyIzV/PlQPo
SrWotUQzq1Lq0S5muPv1AAv41k3T8NtxXyohKmENbSbzU6tEsVGHo/2BLjvK1SHRPHo/IDX9hofcFt14h
dcD75mvU3MAEeDC1t02/xoi5xS/RLoxP0k5dNrakw958Yn001sJS9VMf528fknUma3t100qmDDpc/kO
xT+S6DFNDBy6lYQN4hecnhTPRXqPhXqcDiG+rWr/nZK4H8Ckzy+y19RaeXMRuTyQqJb/rsRcmJX5fApd
DmHwfrRSxLjDvUzfywnjFH1K/+TQITlqg1QQaj21PJD9pnDVF0AIJrWyWnR root@freenas.local

Go to \textit{PULL} and paste (or append) the copied key into the \textit{SSH Public Key} field of Accounts → Users → root → 🛠️ (Options) → Edit, or the username of the specified rsync user account. The paste for the above example is shown in Figure 8.4. 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 and start it if it is not.

Next, copy the host key of PULL using Shell on PUSH. The 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 this 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'
```

The rsync task can now be created on PUSH. To configure rsync SSH mode using the systems in our previous example, the configuration is:

- 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 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 option is enabled 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 the pasted key—it will be after the character that appears just before the \( n \) in the error message.

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


Click **Tasks → S.M.A.R.T. Tests** and **ADD** to add a new scheduled S.M.A.R.T. test. Figure 8.5 shows the configuration screen that appears. Tests are listed under **S.M.A.R.T. Tests**. After creating tests, check the configuration in **Services → S.M.A.R.T.**, then click the power button for the S.M.A.R.T. service in **Services** to activate the service. The S.M.A.R.T. service will not start if there are no pools.

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

---

**Table 8.4** summarizes the configurable options when creating a S.M.A.R.T. test.

---

![Fig. 8.5: Adding a S.M.A.R.T. Test](image-url)
Table 8.4: S.M.A.R.T. Test Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Disks</td>
<td>checkbox</td>
<td>Set to monitor all disks.</td>
</tr>
<tr>
<td>Disks</td>
<td>drop-down menu</td>
<td>Select the disks to monitor. Available when All Disks is unset.</td>
</tr>
<tr>
<td>Type</td>
<td>drop-down menu</td>
<td>Choose the test type. See <code>smartctl(8)</code> for descriptions of each type. Some test types will degrade performance or take disks offline. Avoid scheduling S.M.A.R.T. tests simultaneously with scrub or resilver operations.</td>
</tr>
<tr>
<td>Short descrip-</td>
<td>string</td>
<td>Optional. Enter a description of the S.M.A.R.T. test.</td>
</tr>
<tr>
<td>Schedule the</td>
<td>drop-down menu</td>
<td>Choose how often to run the task. Choices are Hourly, Daily, Weekly, Monthly, or Custom. Selecting Custom opens the Advanced Scheduler (page 22).</td>
</tr>
</tbody>
</table>

An example configuration is to schedule a Short Self-Test once a week and a Long Self-Test once a month. These tests do 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, consider 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 (page 341). The results of a test can be checked from Shell (page 341) by specifying the name of the drive. For example, to see the results for disk `ada0`, type:

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

### 8.5 Periodic Snapshot Tasks

A periodic snapshot task allows scheduling the creation of read-only versions of pools 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 keep a history of files, providing a way to recover an older copy or even a deleted file. For this reason, many administrators take snapshots often, store them for a period of time, and store them on another system, typically using Replication Tasks (page 146). Such a strategy allows the administrator to roll the system back to a specific point in time. If there is a catastrophic loss, an off-site snapshot can be used to restore the system up to the time of the last snapshot.

A pool must exist before a snapshot can be created. Creating a pool is described in Pools (page 168).

View the list of periodic snapshot tasks by going to Tasks → Periodic Snapshot Tasks. If a periodic snapshot task encounters an error, the status column will show ERROR. Click the status to view the logs of the task.

To create a periodic snapshot task, navigate to Tasks → Periodic Snapshot Tasks and click ADD. This opens the screen shown in Figure 8.6. Table 8.5 describes the fields in this screen.
### Fig. 8.6: Creating a Periodic Snapshot

**Table 8.5: Periodic Snapshot Options**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dataset</td>
<td>drop-down menu</td>
<td>Select a pool, dataset, or zvol.</td>
</tr>
<tr>
<td>Recursive</td>
<td>checkbox</td>
<td>Set to take separate snapshots of the dataset and each of its child datasets. Leave unset to take a single snapshot only of the specified dataset without child datasets.</td>
</tr>
<tr>
<td>Exclude</td>
<td>string</td>
<td>Exclude specific child datasets from the snapshot. Use with recursive snapshots. Comma-separated list of paths to any child datasets to exclude. Example: pool1/dataset1/child1. A recursive snapshot of pool1/dataset1 will include all child datasets except child1.</td>
</tr>
<tr>
<td>Snapshot Life-time</td>
<td>integer and drop-down menu</td>
<td>Define a length of time to retain the snapshot on this system. After the time expires, the snapshot is removed. Snapshots which have been replicated to other systems are not affected.</td>
</tr>
<tr>
<td>Snapshot Life-time Unit</td>
<td>drop-down</td>
<td>Select a unit of time to retain the snapshot on this system.</td>
</tr>
<tr>
<td>Naming Schema</td>
<td>string</td>
<td>Snapshot name format string. The default is auto-%Y-%m-%d-%H-%M. Must include the strings %Y, %m, %d, %H, and %M, which are replaced with the four-digit year, month, day of month, hour, and minute as defined in strftime(3) (<a href="https://www.freebsd.org/cgi/man.cgi?query=strftime">https://www.freebsd.org/cgi/man.cgi?query=strftime</a>). For example, snapshots of pool1 with a Naming Schema of customsnap-%Y%m%d.%H%M have names like pool1@customsnap-20190315.0527.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 8.5 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule the Periodic Snapshot Task</td>
<td>drop-down menu</td>
<td>When the periodic snapshot task runs. Choose one of the preset schedules or choose Custom to use the Advanced Scheduler (page 22).</td>
</tr>
<tr>
<td>Begin</td>
<td>drop-down menu</td>
<td>Hour and minute when the system can begin taking snapshots.</td>
</tr>
<tr>
<td>End</td>
<td>drop-down menu</td>
<td>Hour and minute the system must stop creating snapshots. Snapshots already in progress will continue until complete.</td>
</tr>
<tr>
<td>Allow Taking Empty Snapshots</td>
<td>checkbox</td>
<td>Creates dataset snapshots even when there have been no changes to the dataset from the last snapshot. Recommended for creating long-term restore points, multiple snapshot tasks pointed at the same datasets, or to be compatible with snapshot schedules or replications created in FreeNAS® 11.2 and earlier. For example, allowing empty snapshots for a monthly snapshot schedule allows that monthly snapshot to be taken, even when a daily snapshot task has already taken a snapshot of any changes to the dataset.</td>
</tr>
<tr>
<td>Enabled</td>
<td>checkbox</td>
<td>To activate this periodic snapshot schedule, set this option. To disable this task without deleting it, unset this option.</td>
</tr>
</tbody>
</table>

Setting *Recursive* adds child datasets to the snapshot. Creating separate snapshots for each child dataset is not needed.

The *Naming Schema* can be manually adjusted to include more information. For example, after configuring a periodic snapshot task with a lifetime of two weeks, it could be helpful to define a Naming Schema that shows the lifetime: `autosnap-%Y-%m-%d.%H-%M-2w`.

Click SAVE when finished customizing the task. Defined tasks are listed alphabetically in Tasks → Periodic Snapshot Tasks.

Click ‣ (Options) for a periodic snapshot task to see options to Edit or Delete the scheduled task.

Deleting a dataset does not delete snapshot tasks for that dataset. To re-use the snapshot task for a different dataset, Edit the task and choose the new Dataset. The original dataset is shown in the drop-down, but cannot be selected.

Deleting the last periodic snapshot task used by a replication task is not permitted while that replication task remains active. The replication task must be disabled before the related periodic snapshot task can be deleted.

### 8.5.1 Snapshot Autoremoval

The periodic snapshot task autoremoval process (which removes snapshots after their configured Snapshot Lifetime) is run whenever any Enabled periodic snapshot task runs.

When the autoremoval process runs, all snapshots on the system are checked for removal. First, each snapshot is matched with a periodic snapshot task according to the following criteria:

- **Dataset/Recursive**: To match a task, a snapshot must be on the same Dataset as the task, or on a child dataset if the task is marked Recursive.
- **Naming Schema**: To match a task, a snapshot’s name must match the Naming Schema defined in that task.
- **Schedule**: To match a task, the time at which the snapshot was created (according to its name and naming schema) must match the schedule defined in the task (Schedule the Periodic Snapshot Task).
- **Enabled**: To match a task, the periodic snapshot task must be Enabled.

At this point, if the snapshot does not match any periodic snapshot tasks then it is not considered for autoremoval. However, if it does match one (or possibly more than one) periodic snapshot task, it is deleted if its creation time (according to its name and naming schema) is older than the longest Snapshot Lifetime of any of the tasks it was matched with.
One notable detail of this process is that there is no saved memory of which task created which snapshot, or what
the parameters of the periodic snapshot task were at the time a snapshot was created. All checks for autoremoval
are based on the current state of the system.

These details become important when existing periodic snapshot tasks are edited, disabled, or deleted. When
editing a periodic snapshot task, if the Naming Schema is changed, Recursive is unchecked, or the task is resched-
uled (Schedule the Periodic Snapshot Task), previously created snapshots may not be automatically removed as ex-
pected since the previously created snapshots may no longer match any periodic snapshot tasks. Similarly, if a
periodic snapshot task is deleted or marked not Enabled, snapshots previously created by that task will no longer
be automatically removed.

In these cases, the user must manually remove unneeded snapshots that were previously created by the modified
or deleted periodic snapshot task.

8.6 Replication

Replication is the process of copying ZFS dataset snapshots (page 372) from one storage pool to another. Replicas-
tions can be configured to copy snapshots to another pool on the local system or send copies to a remote system
that is in a different physical location.

Replication schedules are typically paired with Periodic Snapshot Tasks (page 136) to generate local copies of impor-
tant data and replicate these copies to a remote system.

Replications require a source system with dataset snapshots and a destination that can store the copied data.
Remote replications require a saved SSH Connection (page 101) on the source system and the destination system
must be configured to allow SSH (page 281) connections. Local replications do not use SSH.

Snapshots are organized and sent to the destination according to the creation date included in the snapshot
name. When replicating manually created snapshots, make sure snapshots are named according to their actual
creation date.

First-time replication tasks can take a long time to complete as the entire dataset snapshot must be copied to the
destination system. Replicated data is not visible on the receiving system until the replication task is complete.

Later replications only send incremental snapshot changes to the destination system. This reduces both the total
space required by replicated data and the network bandwidth required for the replication to complete.

The replication task asks to destroy destination dataset snapshots when those snapshots are not related to the
replication snapshots. Verify that the snapshots in the destination dataset are unneeded or are backed up in a dif-
f erent location! Allowing the replication task to continue destroys the current snapshots in the destination dataset
and replicates a full copy of the source snapshots.

The target dataset on the destination system is created in read-only mode to protect the data. To mount or
browse the data on the destination system, use a clone of the snapshot. Clones are created in read/write mode,
making it possible to browse or mount them. See Snapshots (page 191) for more details.

Replications run in parallel as long as they do not conflict with each other. Completion time depends on the num-
ber and size of snapshots and the bandwidth available between the source and destination computers.

Examples in this section refer to the FreeNAS® system with the original datasets for snapshot and replication as
Primary and the FreeNAS® system that is storing replicated snapshots as Secondary.

8.6.1 Replication Creation Wizard

To create a new replication, go to Tasks → Replication Tasks and click ADD.
The wizard allows loading previously saved replication configurations and simplifies many replication settings. To see all possible replication creation options (page 142), click ADVANCED REPLICATION CREATION.

Using the wizard to create a new replication task begins by defining what is being replicated and where. Choosing On a Different System for either the Source Location or Destination Location requires an SSH Connection (page 101) to the remote system. Open the drop-down menu to choose an SSH connection or click Create New to add a new connection.

Start by selecting the Source datasets to be replicated. To choose a dataset, click (Browse) and select the dataset from the expandable tree. The path of the dataset can also be typed into the field. Multiple snapshot sources can be chosen using a comma (,) to separate each selection. Recursive replication will include all snapshots of any descendant datasets of the chosen Source.

Source datasets on the local system are replicated using existing snapshots of the chosen datasets. When no snapshots exist, FreeNAS automatically creates snapshots of the chosen datasets before starting the replication. To manually define which dataset snapshots to replicate, set Replicate Custom Snapshots and define a snapshot Naming Schema.

Source datasets on a remote system are replicated by defining a snapshot Naming Schema. The schema is a pattern of the name and strftime(3) (https://www.freebsd.org/cgi/man.cgi?query=strftime) %Y, %m, %d, %H, and %M strings that match names of the snapshots to include in the replication. For example, to replicate a snapshot named auto-2019-12-18.05-20 from a remote source, enter auto-%Y-%m-%d.%H-%M as the replication task Naming Schema.

The number of snapshots that will be replicated is shown. There is also a Recursive option to include child datasets with the selected datasets.

Now choose the Destination to receive the replicated snapshots. To choose a destination path, click (Browse)
and select the dataset from the expandable tree or type a path to the location in the field. Only a single Destination path can be defined.

Using an SSH connection for replication adds the SSH Transfer Security option. This sets the data transfer security level. The connection is authenticated with SSH. Data can be encrypted during transfer for security or left unencrypted to maximize transfer speed. WARNING: Encryption is recommended, but can be disabled for increased speed on secure networks.

A suggested replication Task Name is shown. This can be changed to give a more meaningful name to the task. When the source and destination have been set, click NEXT to choose when the replication will run.

![FreeNAS Replication Wizard](image)

**Fig. 8.8: Replication Wizard: When**

The replication task can be configured to run on a schedule or left unscheduled and manually activated. Choosing Run On a Schedule adds the Scheduling drop-down to choose from preset schedules or define a Custom replication schedule. Choosing Run Once removes all scheduling options.

Destination Snapshot Lifetime determines when replicated snapshots are deleted from the destination system:

- **Same as Source**: duplicate the configured Snapshot Lifetime value from the source dataset [periodic snapshot task](page 136).
- **Never Delete**: never delete snapshots from the destination system.
- **Custom**: define how long a snapshot remains on the destination system. Enter a number and choose a measure of time from the drop-down menus.

Clicking START REPLICATION saves the replication configuration and activates the schedule. When the replication configuration includes a source dataset on the local system and has a schedule, a [periodic snapshot task](page 136) of that dataset is also created.
Tasks set to *Run Once* will start immediately. If a one-time replication has no valid local system source dataset snapshots, FreeNAS® will snapshot the source datasets and immediately replicate those snapshots to the destination dataset.

All replication tasks are displayed in *Tasks → Replication Tasks*. The task settings that are shown by default can be adjusted by opening the *COLUMNS* drop-down. To see more details about the last time the replication task ran, click the entry under the *State* column. Tasks can also be expanded by clicking ➔ (Expand) for that task. Expanded tasks show all replication settings and have ➤ *RUN NOW*, ✒ *EDIT*, and ✗ *DELETE* buttons.

### 8.6.2 Advanced Replication Creation

The advanced replication creation screen has more options for fine-tuning a replication. It also allows creating local replications, legacy engine replications from FreeNAS® 11.1 or earlier, or even creating a one-time replication that is not linked to a periodic snapshot task.

Go to *System → Replication Tasks*, click *ADD* and *ADVANCED REPLICAATION CREATION* to see these options. This screen is also displayed after clicking ✖ (Options) and *Edit* for an existing replication.

The *Transport* value changes many of the options for replication. Table 8.6 shows abbreviated names of the *Transport* methods in the *Transport* column to identify fields which appear when that method is selected.

- **ALL**: All *Transport* methods
- **SSH**: *SSH*
- **NCT**: *SSH+NETCAT*
- **LOC**: *LOCAL*
### Table 8.6: Replication Task Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Transport</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>All</td>
<td>string</td>
<td>Descriptive name for the replication.</td>
</tr>
<tr>
<td>Direction</td>
<td>SSH, NCT, LEG</td>
<td>drop-down menu</td>
<td><em>PUSH</em> sends snapshots to a destination system. <em>PULL</em> connects to a remote system and retrieves snapshots matching a <em>Naming Schema</em>.</td>
</tr>
<tr>
<td>Transport</td>
<td>All</td>
<td>drop-down menu</td>
<td>Method of snapshot transfer:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <em>SSH</em> is supported by most systems. It requires a previously created <a href="#">SSH connection</a> (page 101).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <em>SSH+NETCAT</em> uses SSH to establish a connection to the destination system, then uses <a href="https://github.com/freenas/py-libzfs">py-libzfs</a> to send an un-encrypted data stream for higher transfer speeds. By default, this is supported by FreeNAS® systems with 11.2 or later installed (11.3 or later is recommended). Destination systems that do not have FreeNAS® 11.2 or later installed might have to manually install <a href="https://github.com/freenas/py-libzfs">py-libzfs</a>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <em>LOCAL</em> efficiently replicates snapshots to another dataset on the same system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <em>LEGACY</em> uses the legacy replication engine from FreeNAS® 11.2 and earlier.</td>
</tr>
<tr>
<td>SSH Connection</td>
<td>SSH, NCT, LEG</td>
<td>drop-down menu</td>
<td>Choose the <a href="#">SSH connection</a> (page 101).</td>
</tr>
<tr>
<td>Netcat Active Side</td>
<td>NCT</td>
<td>drop-down menu</td>
<td>Establishing a connection requires that one of the connection systems has open TCP ports. Choose which system (<em>LOCAL</em> or <em>REMOTE</em>) will open ports. Consult your IT department to determine which systems are allowed to open ports.</td>
</tr>
<tr>
<td>Netcat Active Side Listen Address</td>
<td>NCT</td>
<td>string</td>
<td>IP address on which the connection Active Side listens. Defaults to 0.0.0.0.</td>
</tr>
<tr>
<td>Netcat Active Side Min Port</td>
<td>NCT</td>
<td>integer</td>
<td>Lowest port number of the active side listen address that is open to connections.</td>
</tr>
<tr>
<td>Netcat Active Side Max Port</td>
<td>NCT</td>
<td>integer</td>
<td>Highest port number of the active side listen address that is open to connections. The first available port between the minimum and maximum is used.</td>
</tr>
<tr>
<td>Netcat Active Side Connect Address</td>
<td>NCT</td>
<td>string</td>
<td>Hostname or IP address used to connect to the active side system. When the active side is <em>LOCAL</em>, this defaults to the <em>SSH_CLIENT</em> environment variable. When the active side is <em>REMOTE</em>, this defaults to the SSH connection hostname.</td>
</tr>
<tr>
<td>Source</td>
<td>All</td>
<td><strong>(Browse),</strong> string</td>
<td>Define the path to a system location that has snapshots to replicate. Click the <strong>(Browse)</strong> to see all locations on the source system or click in the field to manually type a location (Example: pool1/dataset1). Multiple source locations can be selected or manually defined with a comma (literal::) separator.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 8.6 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Transport</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
<td>All</td>
<td>(Browse), string</td>
<td>Define the path to a system location that will store replicated snapshots. Click the (Browse) to see all locations on the destination system or click in the field to manually type a location path (Example: pool1/dataset1). Selecting a location defines the full path to that location as the destination. Appending a name to the path will create new zvol at that location. For example, selecting pool1/dataset1 will store snapshots in dataset1, but clicking the path and typing /zvol1 after dataset1 will create zvol1 for snapshot storage.</td>
</tr>
<tr>
<td><strong>Recursive</strong></td>
<td>All</td>
<td>checkbox</td>
<td>Replicate all child dataset snapshots. When set, Exclude Child Datasets becomes visible.</td>
</tr>
<tr>
<td><strong>Exclude Child Datasets</strong></td>
<td>SSH, NCT, LOC</td>
<td>string</td>
<td>Exclude specific child dataset snapshots from the replication. Use with Recursive replications. List child dataset names to exclude. Separate multiple entries with a comma (,). Example: pool1/dataset1/child1. A recursive replication of pool1/dataset1 Snapshots includes all child dataset snapshots except child1.</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>SSH, NCT, LOC</td>
<td>checkbox</td>
<td>Include dataset properties with the replicated snapshots.</td>
</tr>
<tr>
<td><strong>Periodic Snapshot Tasks</strong></td>
<td>SSH, NCT, LOC</td>
<td>dropdown menu</td>
<td>Snapshot schedule for this replication task. Choose from configured Periodic Snapshot Tasks (page 136). This replication task must have the same Recursive and Exclude Child Datasets values as the chosen periodic snapshot task. Selecting a periodic snapshot schedule removes the Schedule field.</td>
</tr>
<tr>
<td><strong>Naming Schema</strong></td>
<td>SSH, NCT, LOC</td>
<td>string</td>
<td>Visible with PULL replications. Pattern of naming custom snapshots to be replicated. Enter the name and strftime(3) (<a href="https://www.freebsd.org/cgi/man.cgi?query=strftime">https://www.freebsd.org/cgi/man.cgi?query=strftime</a>) %Y, %m, %d, %H, and %M strings that match the snapshots to include in the replication.</td>
</tr>
<tr>
<td><strong>Also Include Naming Schema</strong></td>
<td>SSH, NCT, LOC</td>
<td>string</td>
<td>Visible with PUSH replications. Pattern of naming custom snapshots to include in the replication with the periodic snapshot schedule. Enter the strftime(3) (<a href="https://www.freebsd.org/cgi/man.cgi?query=strftime">https://www.freebsd.org/cgi/man.cgi?query=strftime</a>) strings that match the snapshots to include in the replication. When a periodic snapshot is not linked to the replication, enter the naming schema for manually created snapshots. Has the same %Y, %m, %d, %H, and %M string requirements as the Naming Schema in a periodic snapshot task (page 137).</td>
</tr>
<tr>
<td><strong>Run Automatically</strong></td>
<td>SSH, NCT, LOC</td>
<td>checkbox</td>
<td>Set to either start this replication task immediately after the linked periodic snapshot task completes or continue to create a separate Schedule for this replication.</td>
</tr>
<tr>
<td><strong>Schedule</strong></td>
<td>SSH, NCT, LOC</td>
<td>checkbox and dropdown menu</td>
<td>Start time for the replication task. Select a preset schedule or choose Custom to use the advanced scheduler. Adds the Begin and End fields.</td>
</tr>
<tr>
<td><strong>Begin</strong></td>
<td>SSH, NCT, LOC</td>
<td>dropdown menu</td>
<td>Start time for the replication task.</td>
</tr>
<tr>
<td><strong>End</strong></td>
<td>SSH, NCT, LOC</td>
<td>dropdown menu</td>
<td>End time for the replication task. A replication that is already in progress can continue to run past this time.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 8.6 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Transport</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replicate Specific Snapshots</td>
<td>SSH, NCT, LOC</td>
<td>checkbox and drop-down menu</td>
<td>Only replicate snapshots that match a defined creation time. To specify which snapshots will be replicated, set this checkbox and define the snapshot creation times that will be replicated. For example, setting this time frame to Hourly will only replicate snapshots that were created at the beginning of each hour.</td>
</tr>
<tr>
<td>Begin</td>
<td>SSH, NCT, LOC</td>
<td>drop-down menu</td>
<td>Daily time range for the specific periodic snapshots to replicate, in 15 minute increments. Periodic snapshots created before the Begin time will not be included in the replication.</td>
</tr>
<tr>
<td>End</td>
<td>SSH, NCT, LOC</td>
<td>drop-down menu</td>
<td>Daily time range for the specific periodic snapshots to replicate, in 15 minute increments. Snapshots created after the End time will not be included in the replication.</td>
</tr>
<tr>
<td>Only Replicate Snapshots Matching Schedule</td>
<td>SSH, NCT, LOC</td>
<td>checkbox</td>
<td>Set to use the Schedule in place of the Replicate Specific Snapshots time frame. The Schedule values are read over the Replicate Specific Snapshots time frame.</td>
</tr>
<tr>
<td>Replicate from scratch if incremental is not possible</td>
<td>SSH, NCT, LOC</td>
<td>checkbox</td>
<td>If the destination system has snapshots but they do not have any data in common with the source snapshots, destroy all destination snapshots and do a full replication. Warning: enabling this option can cause data loss or excessive data transfer if the replication is misconfigured.</td>
</tr>
<tr>
<td>Hold Pending Snapshots</td>
<td>SSH, NCT, LOC</td>
<td>checkbox</td>
<td>Prevent source system snapshots that have failed replication from being automatically removed by the Snapshot Retention Policy.</td>
</tr>
<tr>
<td>Snapshot Retention Policy</td>
<td>SSH, NCT, LOC</td>
<td>drop-down menu</td>
<td>When replicated snapshots are deleted from the destination system:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Same as Source: use Snapshot Lifetime value from the source periodic snapshot task (page 136).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Custom: define a Snapshot Lifetime for the destination system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• None: never delete snapshots from the destination system.</td>
</tr>
<tr>
<td>Snapshot Lifetime</td>
<td>All</td>
<td>integer and drop-down menu</td>
<td>Added with a Custom retention policy. How long a snapshot remains on the destination system. Enter a number and choose a measure of time from the drop-down.</td>
</tr>
<tr>
<td>Stream Compression</td>
<td>SSH</td>
<td>drop-down menu</td>
<td>Select a compression algorithm to reduce the size of the data being replicated. Only appears when SSH is chosen for Transport.</td>
</tr>
<tr>
<td>Limit (Examples: 500 KiB, 500M, 2 TB)</td>
<td>SSH</td>
<td>integer</td>
<td>Limit replication speed to this number of bytes per second. Zero means no limit. This is a humanized field (page 24).</td>
</tr>
<tr>
<td>Send Deduplicated Stream</td>
<td>SSH, NCT, LOC</td>
<td>checkbox</td>
<td>Deduplicate the stream to avoid sending redundant data blocks. The destination system must also support deduplicated streams. See zfs(8) (<a href="https://www.freebsd.org/cgi/man.cgi?query=zfs">https://www.freebsd.org/cgi/man.cgi?query=zfs</a>).</td>
</tr>
<tr>
<td>Allow Blocks Larger than 128KB</td>
<td>SSH, NCT, LOC</td>
<td>checkbox</td>
<td>Allow sending large data blocks. The destination system must also support large blocks. See zfs(8) (<a href="https://www.freebsd.org/cgi/man.cgi?query=zfs">https://www.freebsd.org/cgi/man.cgi?query=zfs</a>).</td>
</tr>
<tr>
<td>Allow Compressed WRITE Records</td>
<td>SSH, NCT, LOC</td>
<td>checkbox</td>
<td>Use compressed WRITE records to make the stream more efficient. The destination system must also support compressed WRITE records. See zfs(8) (<a href="https://www.freebsd.org/cgi/man.cgi?query=zfs">https://www.freebsd.org/cgi/man.cgi?query=zfs</a>).</td>
</tr>
</tbody>
</table>

Continued on next page
Table 8.6 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Transport</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of retries for failed replications</td>
<td>SSH, NCT, LOC</td>
<td>integer</td>
<td>Number of times the replication is attempted before stopping and marking the task as failed.</td>
</tr>
<tr>
<td>Logging Level</td>
<td>All</td>
<td>drop-down menu</td>
<td>Message verbosity level in the replication task log.</td>
</tr>
<tr>
<td>Enabled</td>
<td>All</td>
<td>checkbox</td>
<td>Activates the replication schedule.</td>
</tr>
</tbody>
</table>

8.6.3 Replication Tasks

Saved replications are shown on the Replication Tasks page.

![Replication Task List](image)

The replication name and configuration details are shown in the list. To adjust the default table view, open the COLUMNS menu and select the replication details to show in the normal table view.

The State column shows the status of the replication task. To view the detailed replication logs for a task, click the State entry when the task is running or finished.

Expanding an entry shows additional buttons for starting or editing a replication task.

8.6.4 Limiting Replication Times

The Schedule, Begin, and End times in a replication task make it possible to restrict when replication is allowed. These times can be set to only allow replication after business hours, or at other times when disk or network ac-
tivity will not slow down other operations like snapshots or Scrub Tasks (page 149). The default settings allow replication to occur at any time.

These times control when replication task are allowed to start, but will not stop a replication task that is already running. Once a replication task has begun, it will run until finished.

8.6.5 Troubleshooting Replication

Replication depends on SSH, disks, network, compression, and encryption to work. A failure or misconfiguration of any of these can prevent successful replication.

Replication logs are saved in `var/log/zettarepl.log`. Logs of individual replication tasks can be viewed by clicking the replication State.

8.6.5.1 SSH

SSH (page 281) must be able to connect from the source system to the destination system with an encryption key. This is tested from Shell (page 341) by making an SSH (page 281) connection from the source system to the destination system. For example, this is a connection from Alpha to Beta at 10.0.0.118. Start the Shell (page 341) on the source machine (Alpha), then enter this command:

```
ssh -vv 10.0.0.118
```

On the first connection, the system might say

```
No matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)?
```

Verify that this is the correct destination computer from the preceding information on the screen and type yes. At this point, an SSH (page 281) shell connection is open to the destination system, Beta.

If a password is requested, SSH authentication is not working. An SSH key value must be present in the destination system `/root/.ssh/authorized_keys` file. `/var/log/auth.log` file can show diagnostic errors for login problems on the destination computer also.

8.6.5.2 Compression

Matching compression and decompression programs must be available on both the source and destination computers. This is not a problem when both computers are running FreeNAS®, but other operating systems might not have lz4, pigz, or plzip compression programs installed by default. An easy way to diagnose the problem is to set Replication Stream Compression to Off. If the replication runs, select the preferred compression method and check `/var/log/debug.log` on the FreeNAS® system for errors.

8.6.5.3 Manual Testing

On Alpha, the source computer, the `/var/log/messages` file can also show helpful messages to locate the problem.

On the source computer, Alpha, open a Shell (page 341) and manually send a single snapshot to the destination computer, Beta. The snapshot used in this example is named `auto-20161206.1110-2w`. As before, it is located in the `alphapool/alphadata` dataset. A @ symbol separates the name of the dataset from the name of the snapshot in the command.

```
zfs send alphapool/alphadata@auto-20161206.1110-2w | ssh 10.0.0.118 zfs recv betapool
```

If a snapshot of that name already exists on the destination computer, the system will refuse to overwrite it with the new snapshot. The existing snapshot on the destination computer can be deleted by opening a Shell (page 341) on Beta and running this command:
Then send the snapshot manually again. Snapshots on the destination system, Beta, are listed from the Shell (page 341) with `zfs list -t snapshot` or from Storage → Snapshots.

Error messages here can indicate any remaining problems.

### 8.7 Resilver Priority

Resilvering, or the process of copying data to a replacement disk, is best completed as quickly as possible. Increasing the priority of resilvers can help them to complete more quickly. The Resilver Priority menu makes it possible to increase the priority of resilvering at times where the additional I/O or CPU usage will not affect normal usage. Select Tasks → Resilver Priority to display the screen shown in Figure 8.10. Table 8.7 describes the fields on this screen.

![Fig. 8.10: Resilver Priority](image)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>checkbox</td>
<td>Set to run resilver tasks between the configured times.</td>
</tr>
<tr>
<td>Begin Time</td>
<td>drop-down</td>
<td>Choose the hour and minute when resilver tasks can be started.</td>
</tr>
</tbody>
</table>

Table 8.7: Resilver Priority Options

Continued on next page
Table 8.7 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End Time</td>
<td>drop-down</td>
<td>Choose the hour and minute when new resilver tasks can no longer be started. This does not affect active resilver tasks.</td>
</tr>
<tr>
<td>Days of the Week</td>
<td>checkboxes</td>
<td>Select the days to run resilver tasks.</td>
</tr>
</tbody>
</table>

8.8 Scrub Tasks

A scrub is the process of ZFS scanning through the data on a pool. Scrubs help to identify data integrity problems, detect silent data corruptions caused by transient hardware issues, and provide early alerts of impending disk failures. FreeNAS® makes it easy to schedule periodic automatic scrubs.

It is recommended that each pool is scrubbed at least once a month. Bit errors in critical data can be detected by ZFS, but only when that data is read. Scheduled scrubs can find bit errors in rarely-read data. The amount of time needed for a scrub is proportional to the quantity of data on the pool. Typical scrubs take several hours or longer.

The scrub process is I/O intensive and can negatively impact performance. Schedule scrubs for evenings or weekends to minimize impact to users. Make certain that scrubs and other disk-intensive activity like S.M.A.R.T. Tests (page 135) are scheduled to run on different days to avoid disk contention and extreme performance impacts.

Scrubs only check used disk space. To check unused disk space, schedule S.M.A.R.T. Tests (page 135) of Type Long Self-Test to run once or twice a month.

Scrubs are scheduled and managed with Tasks → Scrub Tasks.

When a pool is created, a scrub is automatically scheduled. An entry with the same pool name is added to Tasks → Scrub Tasks. A summary of this entry can be viewed with Tasks → Scrub Tasks. Figure 8.11 displays the default settings for the pool named pool1. In this example, † (Options) and Edit for a pool is clicked to display the Edit screen. Table 8.8 summarizes the options in this screen.
Review the default selections and, if necessary, modify them to meet the needs of the environment. Scrub tasks cannot run for locked or unmounted pools.

Scheduled scrubs can be deleted with the Delete button, but this is not recommended. Scrubs can provide an early indication of disk issues before a disk failure. If a scrub is too intensive for the hardware, consider temporarily deselecting the Enabled button for the scrub until the hardware can be upgraded.
8.9 Cloud Sync Tasks

Files or directories can be synchronized to remote cloud storage providers with the *Cloud Sync Tasks* feature.

**Warning:** This Cloud Sync task might go to a third party commercial vendor not directly affiliated with iXsystems. Please investigate and fully understand that vendor’s pricing policies and services before creating any Cloud Sync task. iXsystems is not responsible for any charges incurred from the use of third party vendors with the Cloud Sync feature.

"Cloud Credentials" (page 97) must be defined before a cloud sync is created. One set of credentials can be used for more than one cloud sync. For example, a single set of credentials for Amazon S3 can be used for separate cloud syncs that push different sets of files or directories.

A cloud storage area must also exist. With Amazon S3, these are called *buckets*. The bucket must be created before a sync task can be created.

After the cloud credentials have been configured, *Tasks → Cloud Sync Tasks* is used to define the schedule for running a cloud sync task. The time selected is when the Cloud Sync task is allowed to begin. An in-progress cloud sync must complete before another cloud sync can start. The cloud sync runs until finished, even after the selected ending time. To stop the cloud sync task before it is finished, click ![Options) → Stop](image).

An example is shown in Figure 8.12.

![Fig. 8.12: Cloud Sync Status](image)

The cloud sync *Status* indicates the state of most recent cloud sync. Clicking the *Status* entry shows the task logs and includes an option to download them.
Click **ADD** to display the *Add Cloud Sync* menu shown in **Figure 8.13**.

![Fig. 8.13: Adding a Cloud Sync](image)

**Table 8.9** shows the configuration options for Cloud Syncs.

**Table 8.9: Cloud Sync Options**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>string</td>
<td>A description of the Cloud Sync Task.</td>
</tr>
<tr>
<td>Direction</td>
<td>drop-down menu</td>
<td><em>PUSH</em> sends data to cloud storage. <em>PULL</em> receives data from cloud storage. Changing the direction resets the <em>Transfer Mode</em> to <em>COPY</em>.</td>
</tr>
<tr>
<td>Credential</td>
<td>drop-down menu</td>
<td>Select the cloud storage provider credentials from the list of available <em>Cloud Credentials</em> (page 97). The credential is tested and an error is displayed if a connection cannot be made. Click <em>Fix Credential</em> to go to the configuration page for that <em>Cloud Credential</em> (page 97). <em>SAVE</em> is disabled until a valid credential is selected.</td>
</tr>
<tr>
<td>Bucket/Container</td>
<td>drop-down menu</td>
<td><em>Bucket</em>: Only appears when an S3 credential is the <em>Provider</em>. Select the predefined S3 bucket to use. <em>Container</em>: The pre-configured container name. Only appears when an AZUREBLOB or hubic credential is selected as the <em>Credential</em>.</td>
</tr>
<tr>
<td>Folder</td>
<td>browse button</td>
<td>The name of the predefined folder within the selected bucket or container. Type the name or click <img src="image" alt="Browse" /> to list the remote filesystem and choose the folder.</td>
</tr>
<tr>
<td>Server Side En-</td>
<td>drop-down menu</td>
<td>Active encryption on the cloud provider account. Choose <em>None</em> or <em>AES-256</em>. Only visible when the cloud provider supports encryption.</td>
</tr>
<tr>
<td>Cryption</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 8.9 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Class</td>
<td>drop-down menu</td>
<td>Classification for each S3 object. Choose a class based on the specific use case or performance requirements. See Amazon S3 Storage Classes (<a href="https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html">https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html</a>) for more information on which storage class to choose. <em>Storage Class</em> only appears when an S3 credential is the Provider.</td>
</tr>
<tr>
<td>Upload Chunk Size (MiB)</td>
<td>integer</td>
<td>Files are split into chunks of this size before upload. The number of chunks that can be simultaneously transferred is set by the <em>Transfers</em> number. The single largest file being transferred must fit into no more than 10,000 chunks.</td>
</tr>
<tr>
<td>Use –fast-list</td>
<td>checkbox</td>
<td>Use fewer transactions in exchange for more RAM (<a href="https://rclone.org/docs/#fast-list">https://rclone.org/docs/#fast-list</a>). Modifying this setting can speed up or slow down the transfer. Only appears with a compatible Credential.</td>
</tr>
<tr>
<td>Directory/Files</td>
<td>browse button</td>
<td>Select directories or files to be sent to the cloud for <em>Push</em> syncs, or the destination to be written for <em>Pull</em> syncs. Be cautious about the destination of <em>Pull</em> jobs to avoid overwriting existing files.</td>
</tr>
</tbody>
</table>
| Transfer Mode            | drop-down menu | *SYNC:* Files on the destination are **changed** to match those on the source. If a file does not exist on the source, it is also **deleted** from the destination. There are exceptions (page 154) to this behavior.  
*COPY:* Files from the source are **copied** to the destination. If files with the same names are present on the destination, they are **overwritten**.  
*Moves:* After files are **copied** from the source to the destination, they are **deleted** from the source. Files with the same names on the destination are **overwritten**.                                                                                                                                                      |
| Take Snapshot            | checkbox       | Take a snapshot of the dataset before a *PUSH*. This cannot be enabled when the chosen dataset to *PUSH* has nested datasets.                                                                                                                                                                                                                                                                                      |
| Pre-script               | string         | A script to execute before the Cloud Sync Task is run.                                                                                                                                                                                                                                                                                                                                                     |
| Post-script              | string         | A script to execute after the Cloud Sync Task is run.                                                                                                                                                                                                                                                                                                                                                     |
| Remote Encryption        | checkbox       | Use rclone crypt (https://rclone.org/crypt/) to manage data encryption during *PUSH* or *PULL* transfers:  
*PUSH:* Encrypt files before transfer and store the encrypted files on the remote system. Files are encrypted using the *Encryption Password* and *Encryption Salt* values.  
*PULL:* Decrypt files that are being stored on the remote system before the transfer. Transferring the encrypted files requires entering the same *Encryption Password* and *Encryption Salt* that was used to encrypt the files.  
Adds the *Filename Encryption*, *Encryption Password*, and *Encryption Salt* options. Additional details about the encryption algorithm and key derivation are available in the rclone crypt File formats documentation (https://rclone.org/crypt/#file-formats). |
| Filename Encryption      | checkbox       | Encrypt (*PUSH*) or decrypt (*PULL*) file names with the rclone “Standard” file name encryption mode (https://rclone.org/crypt/#filename-encryption-modes). The original directory structure is preserved. A filename with the same name always has the same encrypted filename.  
*PULL* tasks that have *Filename Encryption* enabled and an incorrect *Encryption Password* or *Encryption Salt* will not transfer any files but still report that the task was successful. To verify that files were transferred successfully, click the finished *task status* (page 151) to see a list of transferred files. |
### Table 8.9 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Password</td>
<td>string</td>
<td>Password to encrypt and decrypt remote data. <strong>Warning</strong>: Always securely back up this password! Losing the encryption password will result in data loss.</td>
</tr>
<tr>
<td>Encryption Salt</td>
<td>string</td>
<td>Enter a long string of random characters for use as salt (<a href="https://searchsecurity.techtarget.com/definition/salt">盐</a>) for the encryption password. <strong>Warning</strong>: Always securely back up the encryption salt value! Losing the salt value will result in data loss.</td>
</tr>
<tr>
<td>Schedule the Cloud Sync Task</td>
<td>drop-down menu</td>
<td>Choose how often or at what time to start a sync. Choices are <strong>Hourly</strong>, <strong>Daily</strong>, <strong>Weekly</strong>, <strong>Monthly</strong>, or <strong>Custom</strong>. Selecting Custom opens the <strong>Advanced Scheduler</strong> (<a href="#">第22页</a>).</td>
</tr>
<tr>
<td>Transfers</td>
<td>integer</td>
<td>Number of simultaneous file transfers. Enter a number based on the available bandwidth and destination system performance. See <strong><code>rclone --transfers</code></strong> (<a href="#">第22页</a>).</td>
</tr>
<tr>
<td>Follow Sym-links</td>
<td>checkbox</td>
<td>Include symbolic link targets in the transfer.</td>
</tr>
<tr>
<td>Enabled</td>
<td>checkbox</td>
<td>Enable this Cloud Sync Task. Unset to disable this Cloud Sync Task without deleting it.</td>
</tr>
<tr>
<td>Bandwidth Limit</td>
<td>string</td>
<td>A single bandwidth limit or bandwidth limit schedule in <strong>rclone</strong> format. Example: <code>08:00,512 12:00,10MB 13:00,512 18:00,30MB 23:00,off</code>. Units can be specified with the beginning letter: b, k (default), M, or G. See <strong><code>rclone --bwlimit</code></strong>. (<a href="#">第22页</a>).</td>
</tr>
<tr>
<td>Exclude</td>
<td>string</td>
<td>List of files and directories to exclude from sync, one per line. See <strong><code>https://rclone.org/filtering/</code></strong>.</td>
</tr>
</tbody>
</table>

There are specific circumstances where a **SYNC** task does not delete files from the destination:

- If **`rclone sync`** ([第22页](#)) encounters any errors, files are not deleted in the destination. This includes a common error when the Dropbox **copyright detector** ([第22页](#)) flags a file as copyrighted.
- Syncing to a **B2 bucket** ([第22页](#)) does not delete files from the bucket, even when those files have been deleted locally. However, files are tagged with a version number or moved to a hidden state. To automatically delete old or unwanted files from the bucket, adjust the **Backblaze B2 Lifecycle Rules** ([第22页](#)).
- Files stored in Amazon S3 Glacier or S3 Glacier Deep Archive cannot be deleted by **`rclone sync`** ([第22页](#)). These files must first be restored by another means, like the **Amazon S3 console** ([第22页](#)).

To modify an existing cloud sync, click ![Options](#) to access the **Run Now**, **Edit**, and **Delete** options.

#### 8.9.1 Cloud Sync Example

This example shows a **Push** cloud sync that copies files from a FreeNAS® pool to a cloud service provider. The cloud service provider was configured with a location to store data received from the FreeNAS® system. In the FreeNAS® web interface, go to **System → Cloud Credentials** and click **ADD** to configure the cloud service provider credentials:
Go to Tasks → Cloud Sync and click ADD to create a cloud sync job. The Description is filled with a simple note describing the job. Data is being sent to cloud storage, so this is a Push. The provider comes from the cloud credentials defined in the previous step, and the destination folder was configured in the cloud provider account.

The Directory/Files is set to the file or directory to copy to the cloud provider.

The Transfer Mode is set to COPY so that only the files stored by the cloud provider are modified.

The remaining requirement is to schedule the task. The default is to send the data to cloud storage daily, but the schedule can be customized (page 22) to fine-tune when the task runs.

The Enabled field is enabled by default, so this cloud sync will run at the next scheduled time.

An example of a completed cloud sync task is shown in Figure 8.15:
Fig. 8.15: Example: Successful Cloud Sync
The Network section of the web interface contains these components for viewing and configuring network settings on the FreeNAS® system:

- **Global Configuration** (page 157): general network settings.
- **Interfaces** (page 159): settings for each network interface and options to configure **Bridge** (page 161), **Link Aggregation** (page 162), and **VLAN** (page 164) interfaces.
- **IPMI** (page 164): settings controlling connection to the appliance through the hardware side-band management interface if the user interface becomes unavailable.
- **Static Routes** (page 166): add static routes.

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

**Note:** When any network changes are made an animated icon appears in the upper-right web interface panel to show there are pending network changes. When the icon is clicked it prompts to review the recent network changes. Reviewing the network changes goes to **Network → Interfaces** where the changes can be permanently applied or discarded.

When **APPLY CHANGES** is clicked the network changes are temporarily applied for 60 seconds by default. This value can be changed by entering a positive integer in the seconds field. This feature is nice because the network settings preview can automatically roll back any configuration errors that are accidentally saved.

If the network settings applied work as intended, click **KEEP CHANGES**. Otherwise, the changes can be discarded by clicking **DISCARD CHANGES**.

### 9.1 Global Configuration

*Network → Global Configuration*, shown in **Figure 9.1**, is for general network settings that are not unique to any particular network interface.
Table 9.1 summarizes the settings on the Global Configuration tab. *Hostname* and *Domain* fields are pre-filled as shown in Figure 9.1, but can be changed to meet requirements of the local network.

### Table 9.1: Global Configuration Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>string</td>
<td>System host name. Upper and lower case alphanumeric, ., and – characters are allowed. The <em>Hostname</em> and <em>Domain</em> are also displayed under the iXsystems logo at the top left of the main screen.</td>
</tr>
<tr>
<td>Domain</td>
<td>string</td>
<td>System domain name. The <em>Hostname</em> and <em>Domain</em> are also displayed under the iXsystems logo at the top left of the main screen.</td>
</tr>
<tr>
<td>Additional Domains</td>
<td>string</td>
<td>Additional space-delimited domains to search. Adding search domains can cause slow DNS lookups.</td>
</tr>
<tr>
<td>IPv4 Default Gateway</td>
<td>IP address</td>
<td>Typically not set. See this note about Gateways (page 159). If set, used instead of the default gateway provided by DHCP.</td>
</tr>
<tr>
<td>IPv6 Default Gateway</td>
<td>IP address</td>
<td>Typically not set. See this note about Gateways (page 159).</td>
</tr>
<tr>
<td>Nameserver 1</td>
<td>IP address</td>
<td>Primary DNS server.</td>
</tr>
<tr>
<td>Nameserver 2</td>
<td>IP address</td>
<td>Secondary DNS server.</td>
</tr>
<tr>
<td>Nameserver 3</td>
<td>IP address</td>
<td>Tertiary DNS server.</td>
</tr>
<tr>
<td>HTTP Proxy</td>
<td>string</td>
<td>Enter the proxy information for the network in the format <a href="http://my.proxy.server:3128">http://my.proxy.server:3128</a> or <a href="http://user:password@my.proxy.server:3128">http://user:password@my.proxy.server:3128</a>.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 9.1 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable netwait feature</td>
<td>checkbox</td>
<td>If enabled, network services do not start at boot until the interface is able to ping the addresses listed in the Netwait IP list.</td>
</tr>
<tr>
<td>Netwait IP list</td>
<td>string</td>
<td>Only appears when Enable netwait feature is set. Enter a space-delimited list of IP addresses to ping(8). Each address is tried until one is successful or the list is exhausted. Leave empty to use the default gateway.</td>
</tr>
<tr>
<td>Host name database</td>
<td>string</td>
<td>Used to add one entry per line which will be appended to /etc/hosts. Use the format IP_address space hostname where multiple hostnames can be used if separated by a space.</td>
</tr>
</tbody>
</table>

When using Active Directory, set the IP address of the realm 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 (page 166) 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 the FreeNAS® system is protected by a properly configured firewall.

### 9.2 Interfaces

*Network → Interfaces* shows all physical Network Interface Controllers (NICs) connected to the FreeNAS® system. These can be edited or new bridge, link aggregation, or Virtual LAN (VLAN) interfaces can be created and added to the interface list.

Be careful when configuring the network interface that controls the FreeNAS® web interface or web connectivity can be lost (page 157).

To configure a new network interface, go to Network → Interfaces and click ADD.
Fig. 9.2: Adding a Network Interface

Each Type of configurable network interface changes the available options. Table 9.2 shows which settings are available with each interface type.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>drop-down menu</td>
<td>All</td>
<td>Choose the type of interface. Bridge creates a logical link between multiple networks. Link Aggregation combines multiple network connections into a single interface. A virtual LAN (VLAN) partitions and isolates a segment of the connection.</td>
</tr>
<tr>
<td>Name</td>
<td>string</td>
<td>All</td>
<td>Enter a name to use for the the interface. Use the format laggX, vlanX, or bridgeX where X is a number representing a non-parent interface.</td>
</tr>
<tr>
<td>Description</td>
<td>string</td>
<td>All</td>
<td>Notes or explanatory text about this interface.</td>
</tr>
<tr>
<td>DHCP</td>
<td>checkbox</td>
<td>All</td>
<td>Enable DHCP (<a href="https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol">https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol</a>) to auto-assign an IPv4 address to this interface. Leave unset to create a static IPv4 or IPv6 configuration. Only one interface can be configured for DHCP.</td>
</tr>
<tr>
<td>Autoconfigure IPv6</td>
<td>drop-down menu</td>
<td>All</td>
<td>Automatically configure the IPv6 address with <a href="http://www.freebsd.org/cgi/man.cgi?query=rtsol">rtsol</a> Only one interface can be configured this way.</td>
</tr>
</tbody>
</table>

Continued on next page
### Table 9.2 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Hardware Offloading</td>
<td>checkbox</td>
<td>All</td>
<td>Turn off hardware offloading for network traffic processing.  <strong>WARNING:</strong> disabling hardware offloading can reduce network performance and is only recommended when the interface is managing <em>jails</em> (page 301), <em>plugins</em> (page 290), or <em>virtual machines (VMs)</em> (page 328).</td>
</tr>
<tr>
<td>Bridge Members</td>
<td>drop-down menu</td>
<td>Bridge</td>
<td>Network interfaces to include in the bridge.</td>
</tr>
<tr>
<td>Lagg Protocol</td>
<td>drop-down menu</td>
<td>Link Aggregation</td>
<td>Select the Protocol Type (page 162). LACP is the recommended protocol if the network switch is capable of active LACP. Failover is the default protocol choice and should only be used if the network switch does not support active LACP.</td>
</tr>
<tr>
<td>Lagg Interfaces</td>
<td>drop-down menu</td>
<td>Link Aggregation</td>
<td>Select the interfaces to use in the aggregation. <strong>Warning:</strong> Lagg creation fails when the selected interfaces have manually assigned IP addresses.</td>
</tr>
<tr>
<td>Parent Interface</td>
<td>drop-down menu</td>
<td>VLAN</td>
<td>Select the VLAN Parent Interface. Usually an Ethernet card connected to a switch port configured for the VLAN. A bridge cannot be selected as a parent interface. <strong>New</strong> Link Aggregations (page 162) are not available until the system is restarted.</td>
</tr>
<tr>
<td>Vlan Tag</td>
<td>integer</td>
<td>VLAN</td>
<td>The numeric tag provided by the switched network.</td>
</tr>
<tr>
<td>Priority Code Point</td>
<td>drop-down menu</td>
<td>VLAN</td>
<td>Select the Class of Service (<a href="https://en.wikipedia.org/wiki/Class_of_service">https://en.wikipedia.org/wiki/Class_of_service</a>). The available 802.1p Class of Service ranges from <strong>Best effort</strong> (default) to <strong>Network control</strong> (highest).</td>
</tr>
<tr>
<td>MTU</td>
<td>integer</td>
<td>All</td>
<td>Maximum Transmission Unit, the largest protocol data unit that can be communicated. The largest workable MTU size varies with network interfaces and equipment. 1500 and 9000 are standard Ethernet MTU sizes. Leaving blank restores the field to the default value of 1500.</td>
</tr>
<tr>
<td>Options</td>
<td>string</td>
<td>All</td>
<td>Additional parameters from <a href="https://www.freebsd.org/cgi/man.cgi?query=ifconfig">ifconfig(8)</a>. Separate multiple parameters with a space. For example: <em>mtu</em> 9000 increases the MTU for interfaces which support jumbo frames. See this note (page 163) about MTU and lagg interfaces.</td>
</tr>
<tr>
<td>IP Address</td>
<td>integer and drop-down menu</td>
<td>All</td>
<td>Static IPv4 or IPv6 address and subnet mask. Example: 10.0.0.3 and /24. Click ADD to add another IP address. Clicking DELETE removes that IP Address.</td>
</tr>
</tbody>
</table>

Multiple interfaces **cannot** be members of the same subnet. See [Multiple network interfaces on a single subnet](https://forums.freenas.org/index.php?threads/multiple-network-interfaces-on-a-single-subnet.20204/) for more information. Check the subnet mask if an error is shown when setting the IP addresses on multiple interfaces.

Saving a new interface adds an entry to the list in **Network → Interfaces**.

Expanding an entry in the list shows further details for that interface.

Editing an interface allows changing all the interface options (page 160) except the interface **Type** and **Name**.

### 9.2.1 Network Bridges

A network bridge allows multiple network interfaces to function as a single interface.
To create a bridge, go to **Network → Interfaces** and click **ADD**. Choose **Bridge** as the Type and continue to configure the interface. See the **Interface Configuration Options table** (page 160) for descriptions of each option.

Enter `bridgeX` for the Name, where X is a unique interface number. Open the **Bridge Members** drop-down menu and select each interface that will be part of the bridge. Click **SAVE** to add the new bridge to **Network → Interfaces** and show options to confirm or revert the new network settings.

### 9.2.2 Link Aggregations

FREE NAS® uses the FreeBSD lagg(4) (https://www.freebsd.org/cgi/man.cgi?query=lagg) interface to provide link aggregation and link failover support. A lagg interface allows combining multiple network interfaces into a single virtual interface. This provides fault-tolerance and high-speed multi-link throughput. The aggregation protocols supported by lagg both determines the ports to use for outgoing traffic and if 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. FREE NAS® also supports active/passive failover between pairs of links. The LACP 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 later 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 going to **System → Tunables** and clicking **ADD** to add a tunable. Set the Variable to `net.link.lagg.failover_rx_all`, the Value to a non-zero integer, and the Type to `Sysctl`.

- **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 situations there will be a single LAG which contains all ports. In the event of changes in physical connectivity, link aggregation quickly converges to a new configuration. LACP must be configured on the network 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.

- **None**: this protocol disables any traffic without disabling the lagg interface itself.
9.2.2.1 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 with at least two network cards on different networks. This allows an iSCSI initiator to recognize multiple links to a target, using them for increased bandwidth or redundancy. This how-to (https://fojta.wordpress.com/2010/04/13/iscsi-and-esxi-multipathing-and-jumbo-frames/) 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.

9.2.2.2 Creating a Link Aggregation

Before creating a link aggregation, see this warning (page 157) about changing the interface that the web interface uses.

To create a link aggregation, go to Network → Interfaces and click ADD. Choose Link Aggregation as the Type and continue to fill in the remaining configuration options. See the Interface Configuration Options table (page 160) for descriptions of each option.

Enter laggX for the Name, where X is a unique interface number. There are several Lagg Protocol options, but LACP is preferred. Choose Failover when the network switch does not support LACP. Open the Lagg Interfaces drop-down menu to associate NICs with the lagg device. Click SAVE to add the new aggregation to Network → Interfaces and show options to confirm or revert the new network settings.

Note: If interfaces are installed but do not appear in the Lagg Interfaces list, check for a FreeBSD driver (https://www.freebsd.org/releases/11.2R/hardware.html#ethernet) for the interface.

9.2.2.3 Link Aggregation Options

Options are set at the lagg level from Network → Interfaces. Find the lagg interface, expand the entry with (Expand), and click EDIT. Scroll to the Options field. Changes are typically made at the lagg level as each interface member inherits settings from the lagg. Configuring at the interface level requires repeating the configuration for each interface within the lagg. Setting options at the individual interface level is done by editing the parent interface in the same way as the lagg interface. If the MTU settings on the lagg member interfaces are not identical, the smallest value is used for the MTU of the entire lagg.

Note: A reboot is required after changing the MTU to create a jumbo frame lagg.

Link aggregation load balancing can be tested with:
More information about this command can be found at systat(1) (https://www.freebsd.org/cgi/man.cgi?query=systat).

### 9.2.3 VLANs

FreeNAS® uses vlan(4) (https://www.freebsd.org/cgi/man.cgi?query=vlan) 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) (https://www.freebsd.org/cgi/man.cgi?query=vlan) for details.

To add a new VLAN interface, go to Network → Interfaces and click ADD. Choose VLAN as the Type and continue filling in the remaining fields. See the Interface Configuration Options table (page 160) for descriptions of each option.

The parent interface of a VLAN must be up, but it can either have an IP address or be unconfigured, depending upon the requirements of the VLAN configuration. This makes it difficult for the web interface to do the right thing without trampling the configuration. To remedy this, add the VLAN interface, then select Network → Interfaces, and click 🔄 (Options) and Edit for the parent interface. Enter up in the Options field and click SAVE. This brings up the parent interface. If an IP address is required, configure it using the rest of the options in the edit screen.

**Warning:** Creating a VLAN causes an interruption to network connectivity. The web interface requires confirming the new network configuration before it is permanently applied to the FreeNAS® system.

### 9.3 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 is also used to give 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 (https://www.ixsystems.com/blog/how-to-fix-the-ipmi-remote-management-vulnerability/) provides more information about the vulnerability and how to fix it.


IPMI is configured from Network → IPMI. The IPMI configuration screen, shown in Figure 9.3, provides a shortcut to the most basic IPMI configuration. Those already familiar with IPMI management tools can use them instead. Table 9.3 summarizes the options available when configuring IPMI with the FreeNAS® web interface.
Table 9.3: IPMI Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>string</td>
<td>Enter the password used to connect to the IPMI interface from a web browser. The maximum length accepted in the UI is 20 characters, but different hardware might require shorter passwords.</td>
</tr>
<tr>
<td>DHCP</td>
<td>checkbox</td>
<td>If left unset, IPv4 Address, IPv4 Netmask, and IPv4 Default Gateway must be set.</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>string</td>
<td>IP address used to connect to the IPMI web interface.</td>
</tr>
<tr>
<td>IPv4 Netmask</td>
<td>drop-down menu</td>
<td>Subnet mask associated with the IP address.</td>
</tr>
<tr>
<td>IPv4 Default Gateway</td>
<td>string</td>
<td>Default gateway associated with the IP address.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>string</td>
<td>Enter the VLAN identifier if the IPMI out-of-band management interface is not on the same VLAN as management networking.</td>
</tr>
<tr>
<td>IDENTIFY LIGHT</td>
<td>button</td>
<td>Show a dialog to activate an IPMI identify light on the compatible connected hardware.</td>
</tr>
</tbody>
</table>

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 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.

9.4 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, default routes, and DNS namerservers are displayed.

9.5 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 by going to *Network → Static Routes*, and clicking *ADD*. This is shown in Figure 9.4.

![Fig. 9.4: Adding a Static Route](image)

The available options are summarized in Table 9.4.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>integer</td>
<td>Use the format <em>A.B.C.D/E</em> where <em>E</em> is the CIDR mask.</td>
</tr>
<tr>
<td>Gateway</td>
<td>integer</td>
<td>Enter the IP address of the gateway.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 9.4 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>string</td>
<td>Optional. Add any notes about the route.</td>
</tr>
</tbody>
</table>

Added static routes are shown in *Network → Static Routes*. Click † (Options) on a route entry to access the *Edit* and *Delete* buttons.
The Storage section of the web interface allows configuration of these options:

- **Swap Space** (page 168): Change the swap space size.
- **Pools** (page 168): create and manage storage pools.
- **Snapshots** (page 191): manage local snapshots.
- **VMware-Snapshots** (page 194): coordinate OpenZFS snapshots with a VMware datastore.
- **Disks** (page 195): view and manage disk options.
- **Importing a Disk** (page 201): import a single disk that is formatted with the UFS, NTFS, MSDOS, or EXT2 filesystem.
- **Multipaths** (page 202): View multipath information for systems with compatible hardware.

### 10.1 Swap Space

Swap is space on a disk set aside to be used as memory. When the FreeNAS® system runs low on memory, less-used data can be “swapped” onto the disk, freeing up main memory.

For reliability, FreeNAS® creates swap space as mirrors of swap partitions on pairs of individual disks. For example, if the system has three hard disks, a swap mirror is created from the swap partitions on two of the drives. The third drive is not used, because it does not have redundancy. On a system with four drives, two swap mirrors are created.

Swap space is allocated when drives are partitioned before being added to a vdev (page 372). A 2 GiB partition for swap space is created on each data drive by default. The size of space to allocate can be changed in System → Advanced in the Swap size in Gib field. Changing the value does not affect the amount of swap on existing disks, only disks added after the change. This does not affect log or cache devices, which are created without swap. Swap can be disabled by entering 0, but that is strongly discouraged.

### 10.2 Pools

Storage → Pools is used to create and manage ZFS pools, datasets, and zvols.

Proper storage design is important for any NAS. Please read through this entire chapter before configuring storage disks. Features are described to help make it clear which are beneficial for particular uses, and caveats or hardware restrictions which limit usefulness.

#### 10.2.1 Creating Pools

Before creating a pool, determine the level of required redundancy, how many disks will be added, and if any data exists on those disks. Creating a pool overwrites disk data, so save any required data to different media before adding disks to a pool.
Go to Storage → Pools and click ADD. Select Create new pool and click CREATE POOL to open the screen shown in Figure 10.1.

![Pool Manager Screen](image)

Fig. 10.1: Creating a Pool

Enter a name for the pool in the Name field. Ensure that the chosen name conforms to these naming conventions ([https://docs.oracle.com/cd/E23824_01/html/821-1448/gbcpt.html](https://docs.oracle.com/cd/E23824_01/html/821-1448/gbcpt.html)). Choosing a name that will stick out in the logs is recommended, rather than generic names like “data” or “freenas”.

To encrypt data on the underlying disks as a protection against physical theft, set the Encryption option. A dialog displays a reminder to back up the encryption key (page 173). The data on the disks is inaccessible without the key. Select Confirm then click I UNDERSTAND.

**Warning:** Refer to the warnings in *Managing Encrypted Pools* (page 171) before enabling encryption!

From the Available Disks section, select disks to add to the pool. Enter a value in Filter disks by name or Filter disks by capacity to change the displayed disk order. These fields support PCRE regular expressions ([http://php.net/manual/en/reference.pcre.pattern.syntax.php](http://php.net/manual/en/reference.pcre.pattern.syntax.php)) for filtering. For example, to show only da and nvd disks in Available Disks, type `^ (da) | (nvd)` in Filter disks by name.

Type and maximum capacity is displayed for available disks. To show the disk Rotation Rate, Model, and Serial, click (Expand).

After selecting disks, click the right arrow to add them to the Data VDevs section. The usable space of each disk in a vdev is limited to the size of the smallest disk in the vdev. Additional data vdevs must have the same configuration as the initial vdev.
Any disks that appear in DataVDevs are used to create the pool. To remove a disk from that section, select the disk and click the left arrow to return it to the Available Disks section.

After adding one data vdev, additional data vdevs can be added with REPEAT. This creates additional vdevs of the same layout as the initial vdev. Select the number of additional vdevs and click REPEAT VDEV.

RESET LAYOUT returns all disks to the Available Disks area and closes all but one DataVDevs table.

SUGGEST LAYOUT arranges all disks in an optimal layout for both redundancy and capacity.

The pool layout is dependent upon the number of disks added to DataVDevs and the number of available layouts increases as disks are added. To view the available layouts, ensure that at least one disk appears in DataVDevs and select the drop-down menu under this section. The web interface will automatically update the Estimated total raw data capacity when a layout is selected. 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

**Warning:** Refer to the ZFS Primer (page 372) for more information on redundancy and disk layouts. When more than five disks are used, consideration must be given to the optimal layout for the best performance and scalability. It is important to realize that different layouts of virtual devices (vdevs) affect which operations can be performed on that pool later. For example, drives can be added to a mirror to increase redundancy, but that is not possible with RAIDZ arrays.

After the desired layout is configured, click CREATE. A dialog shows a reminder that all disk contents will be erased. Click Confirm, then CREATE POOL to create the pool.

**Note:** To instead preserve existing data, click the CANCEL button and refer to Importing a Disk (page 201) and Importing a Pool (page 177) to see if the existing format is supported. If so, perform that action instead. If the current storage format is not supported, it is necessary to back up the data to external media, create the pool, then restore the data to the new pool.

Depending on the size and number of disks, the type of controller, and whether encryption is selected, creating the pool may take some time. If the Encryption option was selected, a dialog provides a link to Download Recovery Key. Click the link and save the key to a safe location. When finished, click DONE.

Figure 10.2 shows the new pool1. Select the pool to see more information. The first entry in the list represents the root dataset and has the same name as the pool.

The Available column shows the estimated storage space before compression (https://en.wikipedia.org/wiki/Data_compression). The Used column shows the estimated space used after compression. These numbers come from zfs list.

Other utilities can report different storage estimates. For example, the available space shown in zpool status is the cumulative space of all drives in the pool, regardless of pool configuration or compression.

Other information shown is the type of compression, the compression ratio, whether it is mounted as read-only, whether deduplication has been enabled, the mountpoint path, and any comments entered for the pool.

Pool status is indicated by one of these symbols:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶️ HEALTHY</td>
<td>Green</td>
<td>The pool is healthy.</td>
</tr>
<tr>
<td>🔴 DEGRADED</td>
<td>Orange</td>
<td>The pool is in a degraded state.</td>
</tr>
</tbody>
</table>
Table 10.1 – continued from previous page

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚦</td>
<td>Blue</td>
<td>Pool status cannot be determined.</td>
</tr>
<tr>
<td>🟠</td>
<td>Yellow</td>
<td>The pool is locked.</td>
</tr>
<tr>
<td>🟠</td>
<td>Red</td>
<td>The pool has a critical error.</td>
</tr>
</tbody>
</table>

There is an option to **Upgrade Pool**. This upgrades the pool to the latest **ZFS Feature Flags** (page 375). See the warnings in **Upgrading a ZFS Pool** (page 43) before selecting this option. This button does not appear when the pool is running the latest version of the feature flags.

FreeNAS® uses **GELI** (https://www.freebsd.org/cgi/man.cgi?query=geli) full disk encryption for ZFS pools. This type of encryption is intended to protect against the risks of data being read or copied when the system is powered down, when the pool is locked, or when disks are physically stolen.
FreeNAS® encrypts disks and pools, not individual filesystems. The partition table on each disk is not encrypted, but only identifies the location of partitions on the disk. On an encrypted pool, the data in each partition is encrypted. These are generally called “encrypted drives”, even though the partition table is not encrypted. To use drive firmware to completely encrypt the drive, see Self-Encrypting Drives (page 87).

Note: Processors with support for the AES-NI (https://en.wikipedia.org/wiki/AES_instruction_set) instruction set are strongly recommended. These processors can handle encryption of a small number of disks with negligible performance impact. They also retain performance better as the number of disks increases. Older processors without the AES-NI instructions see significant performance impact with even a single encrypted disk. This forum post (https://forums.freenas.org/index.php?threads/encryption-performance-benchmarks.12157/) compares the performance of various processors.

All drives in an encrypted pool are encrypted, including L2ARC (read cache) and SLOG (write cache). Drives added to an existing encrypted pool are encrypted with the same method specified when the pool was created. Data in memory, including ARC, is not encrypted. ZFS data on disk, including L2ARC and SLOG, are encrypted if the underlying disks are encrypted. Swap data on disk is always encrypted.

Encryption performance depends upon the number of disks encrypted. The more drives in an encrypted pool, the more encryption and decryption overhead, and the greater the impact on performance. Encrypted pools composed of more than eight drives can suffer severe performance penalties. Please benchmark encrypted pools before using them in production.

Creating an encrypted pool means GELI encrypts the data on the disk and generates a master key to decrypt this data. This master key is also encrypted. Loss of a disk master key due to disk corruption is equivalent to any other disk failure, and in a redundant pool, other disks will contain accessible copies of the uncorrupted data. While it is possible to separately back up disk master keys, it is usually not necessary or useful.

There are two user keys that can be used to unlock the master key and then decrypt the disks. In FreeNAS®, these user keys are named the encryption key and the recovery key. Because data cannot be read without first providing a key, encrypted disks containing sensitive data can be safely removed, reused, or discarded without secure wiping or physical destruction of the media.

When discarding disks that still contain encrypted sensitive data, the encryption and recovery keys should also be destroyed or securely deleted. Keys that are not destroyed must be stored securely and kept physically separate from the discarded disks. Data is vulnerable to decryption when the encryption key is present with the discarded disks or can be obtained by the same person who gains access to the disks.

This encryption method is not designed to protect against unauthorized access when the pool is already unlocked. Before sensitive data is stored on the system, ensure that only authorized users have access to the web interface and that permissions with appropriate restrictions are set on shares.

Here are some important points about FreeNAS® behavior to remember when creating or using an encrypted pool:

• At present, there is no one-step way to encrypt an existing pool. The data must be copied to an existing or new encrypted pool. After that, the original pool and any unencrypted backup should be destroyed to prevent unauthorized access and any disks that contained unencrypted data should be wiped.

• Hybrid pools are not supported. Added vdevs must match the existing encryption scheme. Extending a Pool (page 175) automatically encrypts a new vdev being added to an existing encrypted pool.

• FreeNAS® encryption differs from the encryption used in the Oracle proprietary version of ZFS. To convert between these formats, both pools must be unlocked, and the data copied between them.

• Each pool has a separate encryption key. Pools can also add a unique recovery key to use if the passphrase is forgotten or encryption key invalidated.

• Encryption applies to a pool, not individual users. The data from an unlocked pool is accessible to all users with permissions to access it. Encrypted pools with a passphrase can be locked on demand by users that know the passphrase. Pools are automatically locked when the system is shut down.

• Encrypted data cannot be accessed when the disks are removed or the system has been shut down. On a running system, encrypted data cannot be accessed when the pool is locked.
Encrypted pools that have no passphrase are unlocked at startup. Pools with a passphrase remain locked until a user enters the passphrase to unlock them.

10.2.2.1 Encryption and Recovery Keys

FreeNAS® generates a randomized encryption key whenever a new encrypted pool is created. This key is stored in the system dataset (page 93). It is the primary key used to unlock the pool each time the system boots. Creating a passphrase for the pool adds a passphrase component to the encryption key and allows the pool to be locked.

A pool encryption key backup can be downloaded to allow disk decryption on a different system in the event of failure or to allow the FreeNAS® stored key to be deleted for extra security. The combination of encryption key location and passphrase usage provide several different security scenarios:

- **Key stored locally, no passphrase**: the encrypted pool is decrypted and accessible when the system running. Protects “data at rest” only.
- **Key stored locally, with passphrase**: the encrypted pool is not accessible until the passphrase is entered by the FreeNAS® administrator.
- **Key not stored locally**: the encrypted pool is not accessible until the FreeNAS® administrator uploads the key file. When the key also has a passphrase, it must be provided with the key file.

Encrypted pools cannot be locked in the web interface until a passphrase is created for the encryption key.

The recovery key is an optional keyfile that is generated by FreeNAS®, provided for download, and wiped from the system. It is designed as an emergency backup to unlock or import an encrypted pool if the passphrase is forgotten or the encryption key is somehow invalidated. This file is not stored anywhere on the FreeNAS® system and only one recovery key can exist for each encrypted pool. Adding a new recovery key invalidates any previously downloaded recovery key file for that pool.

Existing encryption or recovery keys can be invalidated in several situations:

- An encryption re-key invalidates all encryption and recovery keys as well as an existing passphrase.
- Using a recovery key file to import an encrypted pool invalidates the existing encryption key and passphrase for that pool. FreeNAS® generates a new encryption key for the imported pool, but a new passphrase must be created before the pool can be locked.
- Creating or changing a passphrase invalidates any existing recovery key.
- Adding a new recovery key invalidates any existing recovery key files for the pool.
- **Extending a Pool** (page 175) invalidates all encryption and recovery keys as well as an existing passphrase.

Be sure to download and securely store copies of the most current encryption and recovery keys. Protect and backup encryption key passphrases. **Losing the encryption and recovery keys or the passphrase can result in irrevocably losing all access to the data stored in the encrypted pool!**

10.2.2.2 Encryption Operations

Encryption operations are seen by clicking ✊ (Encryption Options) for the encrypted pool in Storage → Pools. These options are available:

- **Lock**: Only appears after a passphrase is created. Locking a pool restricts data accessibility in FreeNAS® until the pool is unlocked. Selecting this action requires entering the passphrase. The pool status changes to LOCKED, Pool Operations are limited to Export/Disconnect, and ✊ (Encryption Options) changes to ✊ (Unlock).
- **Unlock**: Decrypt the pool by clicking ✊ (Unlock) and entering the passphrase or uploading the recovery key file. Only the passphrase is used when both a passphrase and a recovery key are entered. The services listed in Restart Services restart when the pool is unlocked. This enables FreeNAS® to begin accessing the decrypted data. Individual services can be prevented from restarting by opening Restart Services and deselecting them. Deselecting services can prevent them from properly accessing the unlocked pool.
• **Encryption Key/Passphrase:** Create or change the encryption key passphrase and download a backup of the encryption key. Unlike a password, a passphrase can contain spaces and is typically a series of words. A good passphrase is easy to remember but hard to guess.

The administrator password is required for encryption key changes. Setting *Remove Passphrase* invalidates the current pool passphrase. Creating or changing a passphrase invalidates the pool recovery key.

• **Recovery Key:** Generate and download a new recovery key file or invalidate an existing recovery key. The FreeNAS® administrative password is required. Generating a new recovery key file invalidates previously downloaded recovery key files for the pool.

• **Reset Keys:** Reset the encryption on the pool GELI master key and invalidate all encryption keys, recovery keys, and any passphrase for the pool. A dialog opens to save a backup of the new encryption key. A new passphrase can be created and a new pool recovery key file can be downloaded. The administrator password is required to reset pool encryption.

If a key reset 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.

### 10.2.3 Adding Cache or Log Devices

**Pools** (page 168) can be used either during or after pool creation to add an SSD as a cache or log device to improve performance of the pool under specific use cases. Before adding a cache or log device, refer to the *ZFS Primer* (page 372) to determine if the system will benefit or suffer from the addition of the device.
To add a Cache or Log device during pool creation, click the Add Cache or Add Log button. Select the disk from Available Disks and use the right arrow next to Cache VDev or Log VDev to add it to that section.

To add a device to an existing pool, Extend (page 175) that pool.

### 10.2.4 Removing Cache or Log Devices

Cache or log devices can be removed by going to Storage → Pools. Choose the desired pool and click (Settings) → Status. Choose the log or cache device to remove, then click (Options) → Remove.

### 10.2.5 Adding Spare Devices

ZFS provides the ability to have “hot” spares. These are drives that are connected to a pool, but not in use. If the pool experiences the failure of a data drive, the system uses the hot spare as a temporary replacement. If the failed drive is replaced with a new drive, the hot spare drive is no longer needed and reverts to being a hot spare. If the failed drive is detached from the pool, the spare is promoted to a full member of the pool.

Hot spares can be added to a pool during or after creation. On FreeNAS®, hot spare actions are implemented by zfsd(8) (https://www.freebsd.org/cgi/man.cgi?query=zfsd).

To add a spare during pool creation, click the Add Spare button. Select the disk from Available Disks and use the right arrow next to Spare VDev to add it to the section.

To add a device to an existing pool, Extend (page 175) that pool.

### 10.2.6 Extending a Pool

To increase the capacity of an existing pool, click the pool name, (Settings), then Extend.

If the existing pool is encrypted (page 171), an additional warning message shows a reminder that extending a pool resets the passphrase and recovery key. Extending an encrypted pool opens a dialog to download the new encryption key file. Remember to use the Encryption Operations (page 173) to set a new passphrase and create a new recovery key file.

When adding disks to increase the capacity of a pool, ZFS supports the addition of virtual devices, or vdevs, to an existing ZFS pool. After a vdev is created, more drives cannot be added to that vdev, but a new vdev can be striped with another of the same type to increase the overall size of the pool. To extend a pool, the vdev being added must be the same type as existing vdevs. The EXTEND button is only enabled when the vdev being added is the same type as the existing vdevs. Some vdev extending examples:

- to extend a ZFS mirror, add the same number of drives. The result is a striped mirror. For example, if ten new drives are available, a mirror of two drives could be created initially, then extended by adding another mirror of two drives, and repeating three more times until all ten drives have been added.
- to extend a three-drive RAIDZ1, add another three drives. The resulting pool is a stripe of two RAIDZ1 vdevs, similar to RAID 50 on a hardware controller.
- to extend a four-drive RAIDZ2, add another four drives. The result is a stripe of RAIDZ2 vdevs, similar to RAID 60 on a hardware controller.

### 10.2.7 Export/Disconnect a Pool

Export/Disconnect is used to cleanly disconnect a pool from the system. This is used before physically disconnecting the pool so it can be imported on another system, or to optionally detach and erase the pool so the disks can be reused.

To export or destroy an existing pool, click the pool name, (Settings), then Export/Disconnect. A dialog shows which system Services (page 259) will be disrupted by exporting the pool and additional warnings for encrypted pools. Keep or erase the contents of the pool by setting the options shown in Figure 10.4.
Export/disconnect pool: 'crypt'

WARNING: Exporting/disconnecting pool crypt. Data on the pool will not be available after export. Data on the pool disks can be destroyed by setting the Destroy data option. Back up critical data before exporting/disconnecting the pool.

These services depend on pool crypt and will be disrupted if the pool is detached:

NFS Share:
- /mnt/crypt

SMB Share:
- crypt

'crypt' is encrypted! If the passphrase for this encrypted pool has been lost, the data will be PERMANENTLY UNRECOVERABLE! Before exporting/disconnecting encrypted pools, download and safely store the encryption key and any passphrase for it.

☐ Destroy data on this pool?

☑ Delete configuration of shares that used this pool?

☐ Confirm Export/Disconnect

Fig. 10.4: Export/Disconnect a Pool

**Warning:** Do not export/disconnect an encrypted pool if the passphrase has not been set! **An encrypted pool cannot be reimported without a passphrase!** When in doubt, use the instructions in *Managing En-
The Export/Disconnect Pool screen provides these options:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destroy data on this pool?</td>
<td>Destroy all data on the disks in the pool. <strong>This action cannot be undone.</strong></td>
</tr>
<tr>
<td>Delete configuration of shares</td>
<td>Delete any share configurations set up on the pool.</td>
</tr>
<tr>
<td>Confirm export/disconnect</td>
<td>Confirm the export/disconnect operation.</td>
</tr>
</tbody>
</table>

If the pool is encrypted, **DOWNLOAD KEY** is also shown to download the encryption key (page 173) for that pool.

To Export/Disconnect the pool and keep the data and configurations of shares, set only **Confirm export/disconnect** and click **EXPORT/DISCONNECT**.

To instead destroy the data and share configurations on the pool, also set the **Destroy data on this pool?** option. To verify that data on the pool is to be destroyed, type the name of the pool and click **EXPORT/DISCONNECT**. Data on the pool is destroyed, including share configuration, zvols, datasets, and the pool itself. The disk is returned to a raw state.

**Danger:** Before destroying a pool, ensure that any needed data has been backed up to a different pool or system.

### 10.2.8 Importing a Pool

A pool that has been exported and disconnected from the system can be reconnected with **Storage → Pools → Add**, then selecting **Import an existing pool**. This works for pools that were exported/disconnected from the current system, created on another system, or to reconnect a pool after reinstalling the FreeNAS® system.

When physically installing ZFS pool disks from another system, use the **zpool export poolname** command or a web interface equivalent to export the pool on that system. Then shut it down and connect the drives to the FreeNAS® system. This prevents an “in use by another machine” error during the import to FreeNAS®.

Existing ZFS pools can be imported by clicking **Storage → Pools and ADD**. Select **Import an existing pool**, then click **NEXT** as shown in Figure 10.5.
To import a pool, click *No, continue with import* then *NEXT* as shown in Figure 10.6.
Select the pool from the *Pool* drop-down menu and click *NEXT* to confirm the options and *IMPORT* it.

If hardware is not being detected, run `camcontrol devlist` from *Shell* (page 341). 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* (page 105).

Before importing an *encrypted pool* (page 171), disks must first be decrypted. Click *Yes, decrypt the disks*. This is shown in *Figure 10.7*. 
Use the Disks dropdown menu to select the disks to decrypt. Click Browse to select the encryption key file stored on the client system. Enter the Passphrase associated with the encryption key, then click NEXT to continue importing the pool.

**Danger:** The encryption key file and passphrase are 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 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 Pools (page 171) for instructions on managing keys.

Select the pool to import and confirm the settings. Click IMPORT to finish the process.

**Note:** For security reasons, encrypted pool keys are not saved in a configuration backup file. When FreeNAS® has been installed to a new device and a saved configuration file restored to it, the keys for encrypted disks will not be present, and the system will not request them. To correct this, export the encrypted pool with ✎ (Configure) → Export/Disconnect, making sure that Destroy data on this pool? is not set. Then import the pool again. During the import, the encryption keys can be entered as described above.

### 10.2.9 Viewing Pool Scrub Status

Scrubs and how to set their schedule are described in more detail in Scrub Tasks (page 149).
To view the scrub status of a pool, click the pool name, 🕵️ (Settings), then Status. The resulting screen will display the status and estimated time remaining for a running scrub or the statistics from the last completed scrub.

A CANCEL button is provided to cancel a scrub in progress. When a scrub is cancelled, it is abandoned. The next scrub to run starts from the beginning, not where the cancelled scrub left off.

10.2.10 Adding Datasets

An existing pool 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. Like a folder or directory, permissions can be set on dataset. Datasets are also similar to filesystems in that properties such as quotas and compression can be set, and snapshots created.

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

To create a dataset, select an existing pool in Storage → Pools, click 🛠️ (Options), then select Add Dataset. This will display the screen shown in Figure 10.8.

![Fig. 10.8: Creating a ZFS Dataset](image)

Table 10.3 shows the options available when creating a 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 advanced settings by enabling the Show advanced fields by default option in System → Advanced.
Table 10.3: Dataset Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>string</td>
<td></td>
<td>Required. Enter a unique name for the dataset.</td>
</tr>
<tr>
<td>Comments</td>
<td>string</td>
<td></td>
<td>Enter any additional comments or user notes about this dataset.</td>
</tr>
<tr>
<td>Sync</td>
<td>drop-down menu</td>
<td></td>
<td>Set the data write synchronization. <em>Inherit</em> inherits the sync settings from the parent dataset, <em>Standard</em> uses the sync settings that have been requested by the client software, <em>Always</em> waits for data writes to complete, and <em>Disabled</em> never waits for writes to complete.</td>
</tr>
<tr>
<td>Compression Level</td>
<td>drop-down menu</td>
<td></td>
<td>Refer to the section on <em>Compression</em> (page 184) for a description of the available algorithms.</td>
</tr>
<tr>
<td>Enable atime</td>
<td>Inherit, On, or Off</td>
<td></td>
<td>Choose <em>On</em> to update the access time for files when they are read. Choose <em>Off</em> to prevent producing log traffic when reading files. This can result in significant performance gains.</td>
</tr>
<tr>
<td>Quota for this dataset</td>
<td>integer</td>
<td>✓</td>
<td>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.</td>
</tr>
<tr>
<td>Quota warning alert at, %</td>
<td>integer</td>
<td>✓</td>
<td>Set <em>Inherit</em> to apply the same quota warning alert settings as the parent dataset.</td>
</tr>
<tr>
<td>Quota critical alert at, %</td>
<td>integer</td>
<td>✓</td>
<td>Set <em>Inherit</em> to apply the same quota critical alert settings as the parent dataset.</td>
</tr>
<tr>
<td>Quota for this dataset and all children</td>
<td>integer</td>
<td>✓</td>
<td>A specified value applies to both this dataset and any child datasets.</td>
</tr>
<tr>
<td>Quota warning alert at, %</td>
<td>integer</td>
<td>✓</td>
<td>Set <em>Inherit</em> to apply the same quota warning alert settings as the parent dataset.</td>
</tr>
<tr>
<td>Quota critical alert at, %</td>
<td>integer</td>
<td>✓</td>
<td>Set <em>Inherit</em> to apply the same quota critical alert settings as the parent dataset.</td>
</tr>
<tr>
<td>Reserved space for this dataset</td>
<td>integer</td>
<td>✓</td>
<td>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 otherwise take up all available free space.</td>
</tr>
<tr>
<td>Reserved space for this dataset and all children</td>
<td>integer</td>
<td>✓</td>
<td>A specified value applies to both this dataset and any child datasets.</td>
</tr>
<tr>
<td>ZFS Deduplication</td>
<td>drop-down menu</td>
<td></td>
<td>Read the section on <em>Deduplication</em> (page 184) before making a change to this setting.</td>
</tr>
<tr>
<td>Read-only</td>
<td>drop-down menu</td>
<td>✓</td>
<td>Choices are <em>Inherit</em>, <em>On</em>, or <em>Off</em>.</td>
</tr>
<tr>
<td>Exec</td>
<td>drop-down menu</td>
<td>✓</td>
<td>Choices are <em>Inherit</em>, <em>On</em>, or <em>Off</em>. Setting to <em>Off</em> prevents the installation of <em>Plugins</em> (page 290) or <em>Jails</em> (page 301).</td>
</tr>
<tr>
<td>Snapshot directory</td>
<td>drop-down menu</td>
<td>✓</td>
<td>Choose if the <code>.zfs</code> snapshot directory is Visible or Invisible on this dataset.</td>
</tr>
<tr>
<td>Copies</td>
<td>drop-down menu</td>
<td>✓</td>
<td>Set the number of data copies on this dataset.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 10.3 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record Size</td>
<td>drop-down menu</td>
<td>✓</td>
<td>While ZFS automatically adapts the record size dynamically to adapt to data, if the data has a fixed size (such as database records), matching its size might result in better performance. <strong>Warning</strong>: choosing a smaller record size than the suggested value can reduce disk performance and space efficiency.</td>
</tr>
<tr>
<td>ACL Mode</td>
<td>drop-down menu</td>
<td>✓</td>
<td>Determine how <code>chmod(2)</code> behaves when adjusting file ACLs. See the <code>zfs(8)</code> aclmode property. <strong>Passsthrough</strong> only updates ACL entries that are related to the file or directory mode. <strong>Restricted</strong> does not allow <code>chmod</code> to make changes to files or directories with a non-trivial ACL. An ACL is trivial if it can be fully expressed as a file mode without losing any access rules. Setting the <strong>ACL Mode</strong> to <strong>Restricted</strong> is typically used to optimize a dataset for <strong>SMB sharing</strong> (page 246), but can require further optimizations. For example, configuring an <code>rsync</code> (page 129) with this dataset could require adding <code>--no-perms</code> in the task <strong>Extra options</strong> field.</td>
</tr>
<tr>
<td>Case Sensitivity</td>
<td>drop-down menu</td>
<td></td>
<td>Choices are <strong>sensitive</strong> (default, assumes filenames are case sensitive), <strong>insensitive</strong> (assumes filenames are not case sensitive), or <strong>mixed</strong> (understands both types of filenames). This can only be set when creating a new dataset.</td>
</tr>
<tr>
<td>Share Type</td>
<td>drop-down menu</td>
<td></td>
<td>Select the type of share that will be used on the dataset. Choose between <strong>Generic</strong> for most sharing options or <strong>SMB</strong> for a <strong>SMB share</strong> (page 246). Choosing <strong>SMB</strong> sets the <strong>ACL Mode</strong> to <strong>Restricted</strong> and <strong>Case Sensitivity</strong> to <strong>Insensitive</strong>. This field is only available when creating a new dataset.</td>
</tr>
</tbody>
</table>

After a dataset is created it appears in **Storage → Pools**. Click ![](Options) on an existing dataset to configure these options: **Add Dataset**: create a nested dataset, or a dataset within a dataset. **Add Zvol**: add a zvol to the dataset. Refer to **Adding Zvols** (page 185) for more information about zvols. **Edit Options**: edit the pool properties described in **Table 10.8**. Note that **Dataset Name** and **Case Sensitivity** are read-only as they cannot be edited after dataset creation. **Edit Permissions**: refer to **Setting Permissions** (page 186) for more information about permissions. **Danger**: Removing a dataset is a permanent action and results in data loss! **Edit ACL**: see **ACL Management** (page 187) for details about modifying an Access Control List (ACL). **Delete Dataset**: removes the dataset, snapshots of that dataset, and any objects stored within the dataset. To remove the dataset, set **Confirm**, click **DELETE DATASET**, verify that the correct dataset to be deleted has been chosen by entering the dataset name, and click **DELETE**. When the dataset has active shares or if is still being used by other parts of the system, the dialog shows what is still using it and allows forcing the deletion anyway. **Caution**: forcing the deletion of an in-use dataset can cause data loss or other problems. **Promote Dataset**: only appears on clones. When a clone is promoted, the origin filesystem becomes a clone of the clone making it possible to destroy the filesystem that the clone was created from. Otherwise, a clone cannot be deleted while the origin filesystem exists. **Create Snapshot**: create a one-time snapshot. A dialog opens to name the snapshot. Options to include child datasets in the snapshot and synchronize with VMware can also be shown. To schedule snapshot creation, use **Periodic Snapshot Tasks** (page 136).
10.2.10.1 Deduplication

Deduplication is the process of ZFS transparently reusing a single copy of duplicated data to save space. Depending on the amount of duplicate data, deduplication can improve storage capacity, as less data is written and stored. However, deduplication is RAM intensive. A general rule of thumb is 5 GiB of RAM per terabyte of deduplicated storage. In most cases, compression provides storage gains comparable to deduplication 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 written to a deduplicated dataset, the more RAM it requires. When the system starts storing the DDTs (dedup tables) on disk because they no longer fit into RAM, performance craters. Further, importing an unclean pool can require between 3-5 GiB of RAM per terabyte of deduped data, and if the system does not have the needed RAM, it will panic. The only solution is to add more RAM or recreate the pool. **Think carefully before enabling dedup!** This article [https://constantin.glez.de/2011/07/27/zfs-to-dedupe-or-not-dedupe/](https://constantin.glez.de/2011/07/27/zfs-to-dedupe-or-not-dedupe/) provides a good description of the value versus cost considerations for deduplication.

Unless a lot of RAM and a lot of duplicate data is available, 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:** After deduplication is enabled, the only way to disable it is to use the `zfs set dedup=off` command from Shell (page 341). However, any data that has already been deduplicated will not be un-deduplicated. 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 at Off, copy the data to the new dataset, and destroy the original dataset.

---

**Tip:** Deduplication is often considered when using a group of very similar virtual machine images. However, other features of ZFS can provide dedup-like functionality more efficiently. For example, create a dataset for a standard VM, then clone a snapshot of that dataset for other VMs. Only the difference between each created VM and the main dataset are saved, giving the effect of deduplication without the overhead.

---

10.2.10.2 Compression

When selecting a compression type, balancing performance with the amount of disk space saved by compression is recommended. 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**: default and recommended compression method as it allows compressed datasets to operate at near real-time speed. This algorithm only compresses files that will benefit from compression.
- **GZIP**: levels 1, 6, and 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 which eliminates runs of zeroes.

If OFF is selected as the Compression level when creating a dataset or zvol, compression will not be used on that dataset/zvol. This is not recommended as using LZ4 has a negligible performance impact and allows for more storage capacity.
10.2.11 Adding Zvols

A zvol is a feature of ZFS that creates a raw block device over ZFS. The zvol can be used as an iSCSI device extent.

To create a zvol, select an existing ZFS pool or dataset, click \( \mathcal{O} \) (Options), then Add Zvol to open the screen shown in Figure 10.9.

![Fig. 10.9: Adding a Zvol](image)

The configuration options are described in Table 10.4.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>zvol name</td>
<td>string</td>
<td></td>
<td>Enter a short name for the zvol. Using a zvol name longer than 63-characters can prevent accessing zvols as devices. For example, a zvol with a 70-character filename or path cannot be used as an iSCSI extent. This setting is mandatory.</td>
</tr>
<tr>
<td>Comments</td>
<td>string</td>
<td></td>
<td>Enter any notes about this zvol.</td>
</tr>
<tr>
<td>Size for this zvol</td>
<td>integer</td>
<td></td>
<td>Specify size and value. Units like ( t, TiB ), and ( G ) can be used. The size of the zvol can be increased later, but cannot be reduced. If the size is more than 80% of the available capacity, the creation will fail with an “out of space” error unless Force size is also enabled.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 10.4 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force size</td>
<td>checkbox</td>
<td></td>
<td>By default, the system will not create a zvol if that operation will bring the pool to over 80% capacity. <strong>While NOT recommended</strong>, enabling this option will force the creation of the zvol.</td>
</tr>
<tr>
<td>Sync</td>
<td>drop-down menu</td>
<td></td>
<td>Sets the data write synchronization. <strong>Inherit</strong> inherits the sync settings from the parent dataset, <strong>Standard</strong> uses the sync settings that have been requested by the client software, <strong>Always</strong> waits for data writes to complete, and <strong>Disabled never</strong> waits for writes to complete.</td>
</tr>
<tr>
<td>Compression level</td>
<td>drop-down menu</td>
<td></td>
<td>Compress data to save space. Refer to <strong>Compression</strong> (page 184) for a description of the available algorithms.</td>
</tr>
<tr>
<td>ZFS Deduplication</td>
<td>drop-down menu</td>
<td></td>
<td>ZFS feature to transparently reuse a single copy of duplicated data to save space. <strong>Warning:</strong> this option is RAM intensive. Read the section on <strong>Deduplication</strong> (page 184) before making a change to this setting.</td>
</tr>
<tr>
<td>Sparse</td>
<td>checkbox</td>
<td></td>
<td>Used to provide thin provisioning. Use with caution as writes will fail when the pool is low on space.</td>
</tr>
<tr>
<td>Block size</td>
<td>drop-down menu</td>
<td>✓</td>
<td>The default is based on the number of disks in the pool. This can be set to match the block size of the filesystem which will be formatted onto the iSCSI target. <strong>Warning:</strong> Choosing a smaller record size than the suggested value can reduce disk performance and space efficiency.</td>
</tr>
</tbody>
</table>

Click † (Options) next to the desired zvol in **Storage → Pools** to access the **Delete zvol, Edit Zvol, Create Snapshot**, and, for an existing zvol snapshot, **Promote Dataset** options.

Similar to datasets, a zvol name cannot be changed.

Choosing a zvol for deletion shows a warning that all snapshots of that zvol will also be deleted.

### 10.2.12 Setting Permissions

Setting permissions is an important aspect of managing data access. The web interface is meant to set the **initial** permissions for a pool or dataset to make it available as a share. When a share is made available, the client operating system and **ACL manager** (page 187) is used to fine-tune the permissions of the files and directories that are created by the client.

**Sharing** (page 216) contains configuration examples for several types of permission scenarios. This section provides an overview of the options available for configuring the initial set of permissions.

**Note:** For users and groups to be available, they must either be first created using the instructions in **Accounts** (page 70) or imported from a directory service using the instructions in **Directory Services** (page 204). The drop-down menus described in this section are automatically truncated to 50 entries for performance reasons. To find an unlisted entry, begin typing the desired user or group name for the drop-down menu to show matching results.

To set the permissions on a dataset, select it in **Storage → Pools**, click † (Options), then **Edit Permissions**. Table 10.5 describes the options in this screen.
Table 10.5: Permission Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>string</td>
<td>Displays the path to the dataset or zvol directory.</td>
</tr>
<tr>
<td>User</td>
<td>drop-down menu</td>
<td>Select the user to control the dataset. Users created manually or imported from a directory service appear in the drop-down menu.</td>
</tr>
<tr>
<td>Group</td>
<td>drop-down menu</td>
<td>Select the group to control the dataset. Groups created manually or imported from a directory service appear in the drop-down menu.</td>
</tr>
<tr>
<td>Access Mode</td>
<td>checkboxes</td>
<td>Set the read, write, and execute permissions for the dataset.</td>
</tr>
<tr>
<td>Apply Permissions Recursively</td>
<td>checkbox</td>
<td>Apply permissions recursively to all directories and files within the current dataset.</td>
</tr>
<tr>
<td>Traverse</td>
<td>checkbox</td>
<td>Movement permission for this dataset. Allows users to view or interact with child datasets even when those users do not have permission to view or manage the contents of this dataset.</td>
</tr>
</tbody>
</table>

10.2.13 ACL Management

An Access Control List (ACL) is a set of account permissions associated with a dataset and applied to directories or files within that dataset. These permissions control the actions users can perform on the dataset contents. ACLs are typically used to manage user interactions with shared datasets (page 216). Datasets with an ACL have (ACL) appended to their name in the directory browser.
The ACL for a new file or directory is typically determined by the parent directory ACL. An exception is when there are no File Inherit or Directory Inherit flags (page 190) in the parent ACL owner@, group@, or everyone@ entries. These non-inheriting entries are appended to the ACL of the newly created file or directory based on the Samba create and directory masks (https://www.samba.org/samba/docs/using_samba/ch08.html) or the umask (https://www.freebsd.org/cgi/man.cgi?query=umask&sektion=2) value.

By default, a file ACL is preserved when it is moved or renamed within the same dataset. The SMB winmsa module (page 251) can override this behavior to force an ACL to be recalculated whenever the file moves, even within the same dataset.

Datasets optimized for SMB sharing can restrict ACL changes. See ACL Mode in the Dataset Options table (page 182). ACLs are modified by adding or removing Access Control Entries (ACEs) in Storage → Pools. Find the desired dataset, click 🔄 (Options), and select Edit ACL. The ACL Manager opens. The ACL manager must be used to modify permissions on a dataset with an ACL.

![ACL Manager](image)

Fig. 10.11: ACL Manager

The ACL Manager options are split into the File Information, Access Control List, and Advanced sections. Table 10.6 sorts these options by their section.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Section</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>File Information</td>
<td>string</td>
<td>Location of the dataset that is being modified. Read-only.</td>
</tr>
<tr>
<td>Setting</td>
<td>Section</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------</td>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User</td>
<td>File Information</td>
<td>drop-down menu</td>
<td>User who controls the dataset. This user always has permissions to read or write the ACL and read or write attributes. Users created manually or imported from a directory service (page 204) appear in the drop-down menu.</td>
</tr>
<tr>
<td>Apply User</td>
<td>File Information</td>
<td>checkbox</td>
<td>Confirm changes to User. To prevent errors, changes to the User are submitted only when this box is set.</td>
</tr>
<tr>
<td>Group</td>
<td>File Information</td>
<td>drop-down menu</td>
<td>The group which controls the dataset. This group has all permissions that are granted to the @group Tag. Groups created manually or imported from a directory service (page 204) appear in the drop-down menu.</td>
</tr>
<tr>
<td>Apply Group</td>
<td>File Information</td>
<td>checkbox</td>
<td>Confirm changes to Group. To prevent errors, changes to the Group are submitted only when this box is set.</td>
</tr>
<tr>
<td>Default ACL</td>
<td>File Information</td>
<td>drop-down menu</td>
<td>Default ACLs. Choosing an entry loads a preset ACL that is configured to match general permissions situations.</td>
</tr>
<tr>
<td>Who</td>
<td>Access Control List</td>
<td>drop-down menu</td>
<td>Access Control Entry (ACE) user or group. Select a specific User or Group for this entry, owner@ to apply this entry to the selected User, group@ to apply this entry to the selected Group, or everyone@ to apply this entry to all users and groups. See setfacl(1) NFSv4 ACL ENTRIES (<a href="https://www.freebsd.org/cgi/man.cgi?query=setfacl">https://www.freebsd.org/cgi/man.cgi?query=setfacl</a>).</td>
</tr>
<tr>
<td>User</td>
<td>Access Control List</td>
<td>drop-down menu</td>
<td>User account to which this ACL entry applies. Only visible when User is the chosen Tag.</td>
</tr>
<tr>
<td>Group</td>
<td>Access Control List</td>
<td>drop-down menu</td>
<td>Group to which this ACL entry applies. Only visible when Group is the chosen Tag.</td>
</tr>
<tr>
<td>ACL Type</td>
<td>Access Control List</td>
<td>drop-down menu</td>
<td>How the Permissions are applied to the chosen Who. Choose Allow to grant the specified permissions and Deny to restrict the specified permissions.</td>
</tr>
<tr>
<td>Permissions Type</td>
<td>Access Control List</td>
<td>drop-down menu</td>
<td>Choose the type of permissions. Basic shows general permissions. Advanced shows each specific type of permission for finer control.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Access Control List</td>
<td>drop-down menu</td>
<td>Select permissions to apply to the chosen Tag. Choices change depending on the Permissions Type. See the permissions list (page 190) for descriptions of each permission.</td>
</tr>
<tr>
<td>Flags Type</td>
<td>Access Control List</td>
<td>drop-down menu</td>
<td>Select the set of ACE inheritance Flags to display. Basic shows unspecific inheritance options. Advanced shows specific inheritance settings for finer control.</td>
</tr>
<tr>
<td>Flags</td>
<td>Access Control List</td>
<td>drop-down menu</td>
<td>How this ACE is applied to newly created directories and files within the dataset. Basic flags enable or disable ACE inheritance. Advanced flags allow further control of how the ACE is applied to files and directories in the dataset. See the inheritance flags list (page 190) for descriptions of Advanced inheritance flags.</td>
</tr>
<tr>
<td>Apply permissions recursively</td>
<td>Advanced</td>
<td>checkbox</td>
<td>Apply permissions recursively to all directories and files in the current dataset.</td>
</tr>
<tr>
<td>Apply permissions to child datasets</td>
<td>Advanced</td>
<td>checkbox</td>
<td>Apply permissions recursively to all child datasets of the current dataset. Only visible when Apply permissions recursively is set.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 10.6 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Section</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strip ACLs</td>
<td>Advanced</td>
<td>checkbox</td>
<td>Set to remove all ACLs from the current dataset. ACLs are also recursively stripped from directories and child datasets when Apply permissions recursively and Apply permissions to child datasets are set.</td>
</tr>
</tbody>
</table>

Additional ACEs are created by clicking **ADD ACL ITEM** and configuring the added fields. One ACE is required in the ACL.

See [setfacl(1)](https://www.freebsd.org/cgi/man.cgi?query=setfacl), [nfs4_acl(5)](https://linux.die.net/man/5/nfs4_acl), and [NFS Version 4 ACLs memo](https://tools.ietf.org/html/draft-falkner-nfsv4-acls-00) for more details about Access Control Lists, permissions, and inheritance flags. The following lists show each permission or flag that can be applied to an ACE with a brief description. An ACE can have a variety of basic or advanced permissions:

### Basic Permissions

- **Read**: view file or directory contents, attributes, named attributes, and ACL. Includes the Traverse permission.
- **Modify**: adjust file or directory contents, attributes, and named attributes. Create new files or subdirectories. Includes the Traverse permission. Changing the ACL contents or owner is not allowed.
- **Traverse**: Execute a file or move through a directory. Directory contents are restricted from view unless the Read permission is also applied. To traverse and view files in a directory, but not be able to open individual files, set the Traverse and Read permissions, then add the advanced Directory Inherit flag.
- **Full Control**: Apply all permissions.

### Advanced Permissions

- **Read Data**: View file contents or list directory contents.
- **Write Data**: Create new files or modify any part of a file.
- **Append Data**: Add new data to the end of a file.
- **Read Named Attributes**: View the named attributes directory.
- **Write Named Attributes**: Create a named attribute directory. Must be paired with the Read Named Attributes permission.
- **Execute**: Execute a file, move through, or search a directory.
- **Delete Children**: Delete files or subdirectories from inside a directory.
- **Read Attributes**: View file or directory non-ACL attributes.
- **Write Attributes**: Change file or directory non-ACL attributes.
- **Delete**: Remove the file or directory.
- **Read ACL**: View the ACL.
- **Write ACL**: Change the ACL and the ACL mode.
- **Write Owner**: Change the user and group owners of the file or directory.
- **Synchronize**: Synchronous file read/write with the server. This permission does not apply to FreeBSD clients.

Basic inheritance flags only enable or disable ACE inheritance. Advanced flags offer finer control for applying an ACE to new files or directories.

- **File Inherit**: The ACE is inherited with subdirectories and files. It applies to new files.
- **Directory Inherit**: New subdirectories inherit the full ACE.
- **No Propagate Inherit**: The ACE can only be inherited once.
- **Inherit Only**: Remove the ACE from permission checks but allow it to be inherited by new files or subdirectories. Inherit Only is removed from these new objects.
• *Inherited*: set when the ACE has been inherited from another dataset.

## 10.3 Snapshots

To view and manage the listing of created snapshots, use *Storage → Snapshots*. An example is shown in Figure 10.12.

**Note:** If snapshots do not appear, check that the current time configured in *Periodic Snapshot Tasks* (page 136) 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* (page 341).

![FreeNAS User Interface](image)

**Fig. 10.12:** Viewing Available Snapshots

Each entry in the list includes the name of the dataset and snapshot. Click > (Expand) to view these options:

**DATE CREATED** shows the exact time and date of the snapshot creation.

**USED** is the amount of space consumed by this dataset and all of its descendants. This value is checked against the dataset quota and reservation. The space used does not include the dataset reservation, but does take into account the reservations of any descendant datasets. The amount of space that a dataset consumes from its parent, as well as the amount of space freed if this dataset is recursively deleted, is the greater of its space used and its reservation. When a snapshot is created, the 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 used space of the snapshot. Deleting a snapshot 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.

**Tip:** Space used by individual snapshots can be seen by running `zfs list -t snapshot` from Shell (page 341).

**REFERENCED** indicates the amount of data 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 filesystem or snapshot it was created from, since its contents are identical.

**DELETE** shows a confirmation dialog. Child clones must be deleted before their parent snapshot can be deleted. 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.

**CLONE TO NEW DATASET** prompts for the name of the new dataset created from the cloned snapshot. A default name is provided based on the name of the original snapshot. Click the **SAVE** button to finish cloning the snapshot.

A clone is a writable copy of the snapshot. Since a clone is actually a dataset which can be mounted, it appears in the **Pools** screen rather than the **Snapshots** screen. By default, `-clone` is added to the name of a snapshot when a clone is created.

**Rollback:** Clicking `` (Options) → **Rollback** asks for confirmation before rolling back to the chosen snapshot state. Clicking **Yes** causes all files in the dataset to revert to the state they were in when the snapshot was created.

**Note:** Rollback is a potentially dangerous operation and causes any configured replication tasks to fail as the replication system uses the existing snapshot when doing an incremental backup. 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. After users have recovered the needed data, delete the clone in the **Active Pools** tab.

This approach does not destroy any on-disk data and has no impact on replication.

A range of snapshots can be deleted. Set the left column checkboxes for each snapshot and click the **Delete** icon above the table. Be careful when deleting multiple snapshots.

Periodic snapshots can be configured to appear as shadow copies in newer versions of Windows Explorer, as described in Configuring Shadow Copies (page 255). Users can access the files in the shadow copy using Explorer without requiring any interaction with the FreeNAS® web interface.

To quickly search through the snapshots list by name, type a matching criteria into the **Filter Snapshots** text area. The listing will change to only display the snapshot names that match the filter text.

**Warning:** A snapshot and any files it contains will not be accessible or searchable if the mount path of the snapshot is longer than 88 characters. The data within the snapshot will be safe, and the snapshot will become accessible again when the mount path is shortened. For details of this limitation, and how to shorten a long mount path, see Path and Name Lengths (page 20).

### 10.3.1 Browsing a Snapshot Collection

All snapshots for a dataset are accessible as an ordinary hierarchical filesystem, which can be reached from a hidden `.zfs` file located at the root of every dataset. A user with permission to access that file can view and explore all snapshots for a dataset like any other files - from the CLI or via File Sharing services such as Samba, NFS and FTP. This is an advanced capability which requires some command line actions to achieve. In summary, the main changes to settings that are required are:
• Snapshot visibility must be manually enabled in the ZFS properties of the dataset.
• In Samba auxiliary settings, the `veto files` command must be modified to not hide the `.zfs` file, and the setting `zfsacl:expose_snapdir=true` must be added.

The effect will be that any user who can access the dataset contents will be able to view the list of snapshots by navigating to the `.zfs` directory of the dataset. They will also be able to browse and search any files they have permission to access throughout the entire snapshot collection of the dataset.

A user's ability to view files within a snapshot will be limited by any permissions or ACLs set on the files when the snapshot was taken. Snapshots are fixed as “read-only”, so this access does not permit the user to change any files in the snapshots, or to modify or delete any snapshot, even if they had write permission at the time when the snapshot was taken.

**Note:** ZFS has a `zfs diff` command which can list the files that have changed between any two snapshot versions within a dataset, or between any snapshot and the current data.

### 10.3.2 Creating a Single Snapshot

To create a snapshot separately from a *periodic snapshot schedule* (page 136), go to `Storage → Snapshots` and click `ADD`.

Select an existing ZFS pool, dataset, or zvol to snapshot. To include child datasets with the snapshot, set `Recursive`.

![Fig. 10.13: Single Snapshot Options](image)

Select an existing ZFS pool, dataset, or zvol to snapshot. To include child datasets with the snapshot, set *Recursive.*
The snapshot can have a custom Name or be automatically named by a Naming Schema. Using a Naming Scheme allows the snapshot to be included in Replication Tasks (page 146). The Naming Schema drop-down is populated with previously created schemas from Periodic Snapshot Tasks (page 136).

10.4 VMware-Snapshots

Storage → VMware-Snapshots is used to coordinate ZFS snapshots when using FreeNAS® as a VMware datastore. When a ZFS snapshot is created, FreeNAS® automatically snapshots any running VMware virtual machines before taking a scheduled or manual ZFS snapshot of the dataset or zvol backing that VMware datastore. Virtual machines must be powered on for FreeNAS® snapshots to be copied to VMware. The temporary VMware snapshots are then deleted on the VMware side but still exist in the ZFS snapshot and can be used as stable resurrection points in that snapshot. These coordinated snapshots are listed in Snapshots (page 191).

Figure 10.14 shows the menu for adding a VMware snapshot and Table 10.7 summarizes the available options.

![Fig. 10.14: Adding a VMware Snapshot](image)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>string</td>
<td>Enter the IP address or hostname of the VMware host. When clustering, use the IP address or hostname of the vCenter server for the cluster.</td>
</tr>
<tr>
<td>Username</td>
<td>string</td>
<td>Enter a user account name created on the VMware host. The account must have permission to snapshot virtual machines.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 10.7 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>string</td>
<td>Enter the password associated with Username.</td>
</tr>
<tr>
<td>ZFS Filesystem</td>
<td>browse button</td>
<td>Browse to the filesystem to snapshot.</td>
</tr>
<tr>
<td>Datastore</td>
<td>drop-down menu</td>
<td>After entering the Hostname, Username, and Password, click FETCH DATASTORES to populate the menu, then select the datastore to be synchronized.</td>
</tr>
</tbody>
</table>

FreeNAS® connects to the VMware host after the credentials are entered. The ZFS Filesystem and Datastore drop-down menus are populated with information from the VMware host. Choosing a datastore also selects any previously mapped dataset.

### 10.5 Disks

To view all of the disks recognized by the FreeNAS® system, use Storage → Disks. As seen in the example in Figure 10.15, each disk entry displays its device name, serial number, size, advanced power management settings, acoustic level settings, and whether S.M.A.R.T. (page 275) tests are enabled. The pool associated with the disk is displayed in the Pool column. Unused is displayed if the disk is not being used in a pool. Click COLUMNS and select additional information to be shown as columns in the table. Additional information not shown in the table can be seen by clicking > (Expand).

![FreeNAS Disks Screen](image)

Fig. 10.15: Viewing Disks

To edit the options for a disk, click ![](image) (Options) on a disk, then Edit to open the screen shown in Figure 10.16. Table 10.8 lists the configurable options.
To bulk edit disks, set the checkbox for each disk in the table then click ✅ (Edit Disks). The **Bulk Edit Disks** page displays which disks are being edited and a short list of configurable options. The **Disk Options table** (page 196) indicates the options available when editing multiple disks.

To offline, online, or replace the device, see **Replacing a Failed Disk** (page 197).

![Fig. 10.16: Editing a Disk](image)

### Table 10.8: Disk Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Bulk Edit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>string</td>
<td></td>
<td>This is the FreeBSD device name for the disk.</td>
</tr>
<tr>
<td>Serial</td>
<td>string</td>
<td></td>
<td>This is the serial number of the disk.</td>
</tr>
<tr>
<td>Description</td>
<td>string</td>
<td></td>
<td>Enter any notes about this disk.</td>
</tr>
<tr>
<td>HDD Standby</td>
<td>dropdown menu</td>
<td>✓</td>
<td>Time of inactivity in minutes before the drive enters standby mode to conserve energy. This forum post (<a href="https://forums.freenas.org/index.php?threads/how-to-find-out-if-a-drive-is-spinning-down-properly.2068/">https://forums.freenas.org/index.php?threads/how-to-find-out-if-a-drive-is-spinning-down-properly.2068/</a>) shows how to determine if a drive has spun down. Temperature monitoring is disabled if the disk is set to enter standby.</td>
</tr>
<tr>
<td>Advanced Power</td>
<td>dropdown menu</td>
<td>✓</td>
<td>Select a power management profile from the menu. The default value is Disabled.</td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page
### Table 10.8 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Bulk Edit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acoustic Level</td>
<td>drop-down menu</td>
<td>✓</td>
<td>Default is Disabled. Other values can be selected for disks that understand AAM (<a href="https://en.wikipedia.org/wiki/Automatic_acoustic_management">https://en.wikipedia.org/wiki/Automatic_acoustic_management</a>).</td>
</tr>
<tr>
<td>Enable S.M.A.R.T.</td>
<td>checkbox</td>
<td>✓</td>
<td>Enabled by default when the disk supports S.M.A.R.T. Disabling S.M.A.R.T. tests prevents collecting new temperature data for this disk. Historical temperature data is still displayed in Reporting (page 326).</td>
</tr>
<tr>
<td>Critical</td>
<td>string</td>
<td></td>
<td>Threshold temperature in Celsius. If the drive temperature is higher than this value, a LOG_CRIT level log entry is created and an email is sent. 0 disables this check.</td>
</tr>
<tr>
<td>Difference</td>
<td>string</td>
<td></td>
<td>Report if the temperature of a drive has changed by this many degrees Celsius since the last report. 0 disables the report.</td>
</tr>
<tr>
<td>Informational</td>
<td>string</td>
<td></td>
<td>Report if drive temperature is at or above this temperature in Celsius. 0 disables the report.</td>
</tr>
<tr>
<td>SED Password</td>
<td>string</td>
<td></td>
<td>Set or change the password of this SED. This password is used instead of the global SED password in System → Advanced. See Self-Encrypting Drives (page 87).</td>
</tr>
<tr>
<td>Clear SED Password</td>
<td>checkbox</td>
<td></td>
<td>Clear the SED password for this disk.</td>
</tr>
</tbody>
</table>

**Tip:** If the serial number for a disk is not displayed in this screen, use the smartctl command from Shell (page 341). For example, to determine the serial number of disk ada0, type `smartctl -a /dev/ada0 | grep Serial`.

The **Wipe** function is used to discard an unused disk.

**Warning:** Ensure all data is backed up and the disk is no longer in use. Triple-check that the correct disk is being selected to be wiped, as recovering data from a wiped disk is usually impossible. If there is any doubt, physically remove the disk, verify that all data is still present on the FreeNAS® system, and wipe the disk in a separate computer.

Clicking **Wipe** offers several choices. **Quick** erases only the partitioning information on a disk, making it easy to reuse but without clearing other old data. For more security, **Full with zeros** overwrites the entire disk with zeros, while **Full with random data** overwrites the entire disk with random binary data.

Quick wipes take only a few seconds. A **Full with zeros** wipe of a large disk can take several hours, and a **Full with random data** takes longer. A progress bar is displayed during the wipe to track status.

### 10.5.1 Replacing a Failed Disk

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 capabilities, it might be necessary to reboot to replace the failed drive. Hardware that supports AHCI does not require a reboot.

Striping (RAID0) does not provide redundancy. Disk failure in a stripe results in losing the pool. The pool must be recreated and data stored in the failed stripe will have to be restored from backups.
**Warning:** Encrypted pools must have a valid passphrase to replace a failed disk. Set a passphrase and back up the encryption key using the pool *Encryption Operations* (page 173) **before** attempting to replace the failed drive.

Before physically removing the failed device, go to *Storage → Pools*. Select the pool name then click 🌟 (Settings). Select *Status* and locate the failed disk. Then perform these steps:

1. Click ✅ (Options) on the disk entry, then **Offline** to change the disk status to OFFLINE. This step removes the device from the pool and prevents swap issues. **Warning:** encrypted disks that are set **OFFLINE** cannot be set back **ONLINE**. If the hardware supports hot-pluggable disks, click the disk **Offline** button and pull the disk, then skip to step 3. If there is no **Offline** but only **Replace**, the disk is already offline and this step can be skipped.

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

2. After the disk is replaced and is showing as OFFLINE, click ✅ (Options) on the disk again and then **Replace**. Select the replacement disk from the drop-down menu and click the **REPLACE DISK** button. After clicking the **REPLACE DISK** button, the pool begins resilvering. Encrypted pools require entering the **encryption key passphrase** (page 173) when choosing a replacement disk. Clicking **REPLACE DISK** begins the process to reformat the replacement, apply the current pool encryption algorithm, and resilver the pool. The current pool encryption key and passphrase remains valid, but any pool recovery key file is invalidated by the replacement process. To maximize pool security, it is recommended to **reset pool encryption** (page 174).

3. After the drive replacement process is complete, re-add the replaced disk in the *S.M.A.R.T. Tests* (page 135) screen.

To refresh the screen with updated entries, click **REFRESH**. If any problems occur during a disk replacement process, one of the disks can be detached. To detach a disk in the replacement process, find the disk to be replaced and click ✅ (Options) → **Detach**.

**Figure 10.17** shows an example of going to *Storage → Pools → Status* and replacing a disk in an active pool.
After the resilver is complete, the pool status shows a *Completed* resilver status and indicates any errors. Figure 10.18 indicates that the disk replacement was successful in this example.

**Note:** A disk that is failing but has not completely failed can be replaced in place, without first removing it. Whether this is a good idea depends on the overall condition of the failing disk. A disk with a few newly-bad blocks that is otherwise functional can be left in place during the replacement to provide data redundancy. A drive that is experiencing continuous errors can actually slow down the replacement. In extreme cases, a disk with serious problems might spend so much time retrying failures that it could prevent the replacement resilvering from completing before another drive fails.
10.5.1.1 Removing a Log or Cache Device

Added log or cache devices appear in Storage → Pools → Pool Status. Clicking the device enables the 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.

10.5.2 Replacing Disks to Grow a 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 from Pools (page 168) as additional capacity is needed.

But adding vdevs is not an option if there are not enough unused disk ports. If there is at least one unused disk port or drive bay, a single disk at a time can be replaced with a larger disk, waiting for the resilvering process to include the new disk into the pool, removing the old disk, then repeating with another disk until all of the original disks have been replaced. At that point, the pool capacity automatically increases to include the new space.

One advantage of this method is that disk redundancy is present during the process.

**Note:** A pool that is configured as a stripe (https://en.wikipedia.org/wiki/Standard_RAJD_levels#RAID_0) can only be increased by following the steps in Extending a Pool (page 175).

1. Connect the new, larger disk to the unused disk port or drive bay.
2. Go to Storage → Pools.
3. Select the pool and click ⚙ (Settings) → Status.
4. Select one of the old, smaller disks in the pool. Click ☰ (Options) → Replace. Choose the new disk as the replacement.

The status of the resilver process is shown on the screen, or can be viewed with `zpool status`. When the new disk has resilvered, the old one is automatically offline. It can then be removed from the system, and that port or bay used to hold the next new disk.

If a unused disk port or bay is not available, a drive can be replaced with a larger one as shown in Replacing a Failed Disk (page 197). 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 appears in the pool.

### 10.6 Importing a Disk

The Storage → Import Disk screen, shown in Figure 10.19, is used to import disks that are formatted with UFS (BSD Unix), FAT (MSDOS) or NTFS (Windows), or EXT2 (Linux) filesystems. This is a designed to be used as a one-time import, copying the data from that disk into a dataset on the FreeNAS® system. 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 (http://e2fsprogs.sourceforge.net/), run on them before import. EXT4 filesystems with extended attributes or inodes greater than 128 bytes are not supported. EXT4 filesystems with EXT3 journaling must have an `fsck` run on them before import, as described above.
Use the drop-down menu to select the disk to import, confirm the detected filesystem is correct, and browse to the ZFS dataset that will hold the copied data. If the MSDOSFS filesystem is selected, an additional MSDOSFS locale drop-down menu is displayed. Use this menu to select the locale if non-ASCII characters are present on the disk.

After clicking SAVE, the disk is mounted and its contents are copied to the specified dataset. The disk is un-mounted after the copy operation completes.

After importing a disk, a dialog allows viewing or downloading the disk import log.

### 10.7 Multipaths

This option is only displayed on systems that contain multipath-capable hardware like a chassis equipped with a dual SAS expander backplane or an external JBOD that is wired for multipath.

FreeNAS® uses `gmultipath(8)` (https://www.freebsd.org/cgi/man.cgi?query=gmultipath) to provide multipath I/O (https://en.wikipedia.org/wiki/Multipath_I/O) support on systems containing multipath-capable hardware.

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. Discovered multipath-capable devices are placed in multipath units with the parent devices hidden. The configuration is displayed in *Storage → Multipaths*. 
Overprovisioning SSDs can be done using the `disk_resize` command in the Shell (page 341). This can be useful for many different scenarios. Perhaps the most useful benefit of overprovisioning is that it can extend the life of an SSD greatly. Overprovisioning an SSD distributes the total number of writes and erases across more flash blocks on the drive. Read more about overprovisioning SSDs here (https://www.seagate.com/tech-insights/ssd-over-provisioning-benefits-master-ti/).

The command to overprovision an SSD is `disk_resize device size`, where `device` is the device name of the SSD and `size` is the desired size of the provision in GB or TB. Here is an example of the command: `disk_resize ada5 16GB`. When no size is specified, it reverts the provision back the full size of the device.

![Fig. 11.1: disk_resize Command](image)

**Note:** Some SATA devices may be limited to one resize per power cycle. Some BIOS may block resize during boot and require a live power cycle.
FreeNAS® supports integration with these directory services:

- **Active Directory** (page 204) (for Windows 2000 and higher networks)
- **LDAP** (page 209)
- **NIS** (page 212)

FreeNAS® also supports **Kerberos Realms** (page 213), **Kerberos Keytabs** (page 214), and the ability to add more parameters to **Kerberos Settings** (page 215).

This section summarizes each of these services and the available configuration options within the FreeNAS® web interface. After successfully enabling a directory service, appears in the top toolbar row. Click to show the Directory Services Monitor menu. This menu shows the name and status of each directory service.

### 12.1 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 (https://wiki.samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller#Provisioning_a_Samba_Active_Directory).

Since AD provides authentication and authorization services for the users in a network, it is not necessary to recreate the same user accounts on the FreeNAS® system. Instead, configure the Active Directory service so account information and imported users can be authorized to access the SMB shares on the FreeNAS® system.

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® 11.3 before attempting Active Directory integration.

Ensure name resolution is properly configured before configuring the Active Directory service. ping the domain name of the Active Directory domain controller from Shell (page 341) on the FreeNAS® system. If the ping fails, check the DNS server and default gateway settings in Network → Global Configuration on the FreeNAS® system.

By default, **Allow DNS updates** in the **Active Directory options** (page 205) is enabled. This adds FreeNAS® SMB 'Bind IP Addresses' (page 277) DNS records to the Active Directory DNS when the domain is joined. Disabling **Allow DNS updates** means that the Active Directory DNS records must be updated manually.

Active Directory relies on Kerberos, a time-sensitive protocol. During the domain join process the PDC emulator FSMO role (https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/f96ff8ec-c660-4d6c-924f-c0dbbcac1527) server is added as the preferred NTP server. The time on the FreeNAS® system and the Active Directory Domain Controller cannot be out of sync by more than five minutes in a default Active Directory environment. An **Alert** (page 345) is sent when the time is out of sync.

To ensure both systems are set to the same time:

- use the same NTP server (set in System → NTP Servers on the FreeNAS® system)
- set the same timezone
- set either localtime or universal time at the BIOS level
Figure 12.1 shows Directory Services → Active Directory settings.

![Fig. 12.1: Configuring Active Directory](image)

Table 12.1 describes the configurable options. Some settings are only available in Advanced Mode. Click the Advanced Mode button to show the Advanced Mode settings. Go to System → Advanced and set the Show advanced fields by default option to always show advanced options.

Table 12.1: Active Directory Configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>string</td>
<td></td>
<td>Name of the Active Directory domain (example.com) or child domain (sales.example.com). This field is mandatory. Save will be inactive until valid input is entered. Hidden when a Kerberos Principal is selected.</td>
</tr>
<tr>
<td>Domain Account Name</td>
<td>string</td>
<td></td>
<td>Name of the Active Directory administrator account. This field is mandatory. Save will be inactive until valid input is entered. Hidden when a Kerberos Principal is selected.</td>
</tr>
<tr>
<td>Domain Account Password</td>
<td>string</td>
<td></td>
<td>Password for the Active Directory administrator account. Required the first time a domain is configured. After initial configuration, the password is not needed to edit, start, or stop the service.</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Mode</td>
<td>drop-down</td>
<td>✓</td>
<td>Choices are Off, SSL (LDAPS protocol port 636), or TLS (LDAP protocol port 389). See <a href="http://info.ssl.com/article.aspx?id=10241">http://info.ssl.com/article.aspx?id=10241</a> and <a href="https://hpbn.co/transport-layer-security-tls/">https://hpbn.co/transport-layer-security-tls/</a> for more information about SSL and TLS.</td>
</tr>
<tr>
<td>Certificate</td>
<td>drop-down menu</td>
<td>✓</td>
<td>Select the Active Directory server certificate if SSL connections are used. If a certificate does not exist, create or import a Certificate Authority (page 113), then create a certificate on the Active Directory server. Import the certificate to the FreeNAS® system using the Certificates (page 116) menu. It is recommended to leave this drop-down unset when configuring LDAPs. To clear a saved certificate, choose the blank entry and click SAVE.</td>
</tr>
<tr>
<td>Validate Certificate</td>
<td>checkbox</td>
<td>✓</td>
<td>Check server certificates in a TLS session.</td>
</tr>
<tr>
<td>Verbose logging</td>
<td>checkbox</td>
<td>✓</td>
<td>Set to log attempts to join the domain to /var/log/messages.</td>
</tr>
<tr>
<td>Allow Trusted Domains</td>
<td>checkbox</td>
<td>✓</td>
<td>Do not set this unless the network has active domain/forest trusts (<a href="https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc757352(v=ws.10)">https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc757352(v=ws.10)</a>) and managing files on multiple domains is required. Setting this option generates more winbindd traffic and slows down filtering with user and group information. If enabled, also configuring the idmap ranges and a backend for each trusted domain in the environment is recommended.</td>
</tr>
<tr>
<td>Use Default Domain</td>
<td>checkbox</td>
<td>✓</td>
<td>Unset to prepend the domain name to the username. Unset to prevent name collisions when Allow Trusted Domains is set and multiple domains use the same username.</td>
</tr>
<tr>
<td>Allow DNS updates</td>
<td>checkbox</td>
<td>✓</td>
<td>Set to enable Samba to do DNS updates when joining a domain.</td>
</tr>
<tr>
<td>Disable FreeNAS Cache</td>
<td>checkbox</td>
<td>✓</td>
<td>Disable caching AD users and groups. Setting this hides all AD users and groups from web interface drop-down menus and auto-completion suggestions, but manually entering names is still allowed. This can help when unable to bind to a domain with a large number of users or groups.</td>
</tr>
<tr>
<td>Site Name</td>
<td>string</td>
<td>✓</td>
<td>Auto-detected site name. Do not change this unless the detected site name is incorrect for the particular AD environment.</td>
</tr>
<tr>
<td>Kerberos Realm</td>
<td>drop-down menu</td>
<td>✓</td>
<td>Select the realm created using the instructions in Kerberos Realms (page 213).</td>
</tr>
<tr>
<td>Kerberos Principal</td>
<td>drop-down menu</td>
<td>✓</td>
<td>Select a keytab created using the instructions in Kerberos Keytabs (page 214). Selecting a principal hides the Domain Account Name and Domain Account Password fields. An existing account name is not overwritten by the principal.</td>
</tr>
<tr>
<td>Computer Account OU</td>
<td>string</td>
<td>✓</td>
<td>The OU in which new computer accounts are created. The OU string is read from top to bottom without RDNs. Slashes (/) are used as delimiters, like Computers/Servers/NAS. The backslash () is used to escape characters but not as a separator. Backslashes are interpreted at multiple levels and might require doubling or even quadrupling to take effect. When this field is blank, new computer accounts are created in the Active Directory default OU.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 12.1 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD Timeout</td>
<td>integer</td>
<td>✓</td>
<td>Increase the number of seconds before timeout if the AD service does not immediately start after connecting to the domain.</td>
</tr>
<tr>
<td>DNS Timeout</td>
<td>integer</td>
<td>✓</td>
<td>Increase the number of seconds before a timeout occurs if AD DNS queries timeout.</td>
</tr>
<tr>
<td>Idmap backend</td>
<td>drop-down menu and Edit Idmap button</td>
<td>✓</td>
<td>Choose the backend to map Windows security identifiers (SIDs) to UNIX UIDs and GIDs. See Table 12.2 for a summary of the available backends. Click Edit Idmap to configure the selected backend.</td>
</tr>
<tr>
<td>Windbind NSS Info</td>
<td>drop-down menu</td>
<td>✓</td>
<td>Choose the schema to use when querying AD for user/group information.RFC2307 uses the RFC2307 schema support included in Windows 2003 R2, sfu is for Services For Unix 3.0 or 3.5, and sfu20 is for Services For Unix 2.0.</td>
</tr>
<tr>
<td>SASL wrapping</td>
<td>drop-down menu</td>
<td>✓</td>
<td>Choose how LDAP traffic is transmitted. Choices are PLAIN (plain text), SIGN (signed only), or SEAL (signed and encrypted). Windows 2000 SP3 and newer can be configured to enforce signed LDAP connections. This should be set to PLAIN when using Microsoft Active Directory. This can be set to SIGN or SEAL when using Samba Active Directory if allowsaslovertls has been explicitly enabled in the Samba Domain Controller configuration.</td>
</tr>
<tr>
<td>Enable (requires password or Kerberos principal)</td>
<td>checkbox</td>
<td>✓</td>
<td>Activate the Active Directory service.</td>
</tr>
<tr>
<td>Netbios Name</td>
<td>string</td>
<td>✓</td>
<td>Name for the computer object generated in AD. Limited to 15 characters. Automatically populated with the original hostname of the system. This must be different from the Workgroup name.</td>
</tr>
<tr>
<td>NetBIOS alias</td>
<td>string</td>
<td>✓</td>
<td>Limited to 15 characters.</td>
</tr>
</tbody>
</table>

Table 12.2 summarizes the backends which are available in the Idmap backend drop-down menu. Each backend has its own man page (http://samba.org.ru/samba/docs/man/manpages/) that gives implementation details.

Changing idmap backends automatically refreshes the windbind resolver cache by sending SIGHUP (signal hang up) to the parent windbinddd process. To find this parent process, start an SSH (page 281) session with the FreeNAS® system and enter service samba_server status. To manually send the SIGHUP, enter kill -HUP pid, where pid is the parent process ID.

Table 12.2: ID Mapping Backends

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ad</td>
<td>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.</td>
</tr>
<tr>
<td>autorid</td>
<td>Similar to rid, 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 or GIDs to use for user and group mappings and an optional size for the ranges.</td>
</tr>
<tr>
<td>ldap</td>
<td>Stores and retrieves mapping tables in an LDAP directory service. Default for LDAP directory service.</td>
</tr>
<tr>
<td>nss</td>
<td>Provides a simple means of ensuring that the SID for a Unix user is reported as the one assigned to the corresponding domain user.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 12.2 – continued from previous page

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfc2307</td>
<td>IDs for AD users stored as RFC2307 (<a href="https://tools.ietf.org/html/rfc2307">https://tools.ietf.org/html/rfc2307</a>) ldap schema extensions. This module can either look up the IDs in the AD LDAP servers or an external (non-AD) LDAP server.</td>
</tr>
<tr>
<td>rid</td>
<td>Default for AD. Requires an explicit idmap configuration for each domain, using disjoint ranges where a writeable default idmap range is to be defined, using a backend like tdb or ldap.</td>
</tr>
<tr>
<td>script</td>
<td>Stores mapping tables for clustered environments in the winbind_cache tdb.</td>
</tr>
<tr>
<td>tdb</td>
<td>Default backend used by winbindd for storing mapping tables.</td>
</tr>
</tbody>
</table>

**REBUILD DIRECTORY SERVICE CACHE** immediately refreshes the web interface directory service cache. This occurs automatically once a day as a cron job.

If there are problems connecting to the realm, verify (https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and) the settings do not include any disallowed characters. Active Directory does not allow $ characters in Domain or NetBIOS names. The length of those names is also limited to 15 characters. The Administrator account password cannot contain the $ character.

It can take a few minutes after configuring the Active Directory service for the AD information to be populated to the FreeNAS® system. To check the AD join progress, open the web interface Task Manager in the upper-right corner. Any errors during the join process are also displayed in the Task Manager.

Once populated, the AD users and groups will be available in the drop-down menus of the Permissions screen of a dataset.

The Active Directory users and groups that are imported to the FreeNAS® system are shown by typing commands in the FreeNAS® Shell (page 341):

- View users: `wbinfo -u`
- View groups: `wbinfo -g`

In addition, `wbinfo -m` shows the domains and `wbinfo -t` tests the connection. When successful, `wbinfo -t` shows a message similar to:

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

To manually check that a specified user can authenticate, open the Shell (page 341) and enter `smbclient //127.0.0.1/SHARE -U DOMAIN\username`, where `SHARE` is the SMB share name, `DOMAIN` is the name of the trusted domain, and `username` is the user account for authentication testing.

`getent passwd` and `getent group` can provide more troubleshooting information if no users or groups are listed in the output.

**Tip:** Sometimes network users do not appear in the drop-down menu of a Permissions screen but the `wbinfo` commands display these users. This is typically due to the FreeNAS® system taking longer than the default ten seconds to join Active Directory. Increase the value of `AD timeout` to 60 seconds.

### 12.1.1 Leaving the Domain

A Leave Domain button appears on the service dialog when a domain is connected. To leave the domain, click the button and enter credentials with privileges sufficient to permit leaving.

### 12.1.2 Troubleshooting Tips

Active Directory uses DNS to determine the location of the domain controllers and global catalog servers in the network. Use `host -t srv ldap._tcp.domainname.com` to determine the SRV records of the net-
work and 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](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759550(v=ws.10)).

The realm used depends on the priority in the SRV DNS record. DNS can override the system Active Directory settings. When unable to connect to the correct realm, check the SRV records on the DNS server.

An expired password for the administrator account will cause `kinit` to fail. Ensure the password is still valid and double-check the password on the AD account being used does not include any spaces, 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 Organizational Unit (OU). When creating this entry, enter the FreeNAS® hostname in the name field. Make sure it is under 15 characters, the same name as the one set in the Hostname field in Network → Global Configuration, and the same NetBIOS alias in Directory Service → Active Directory → Advanced settings.

If the cache becomes out of sync due to an AD server being taken off and back online, resync the cache using `DirectoryService → ActiveDirectory → REBUILDDIRECTORYSERVICECACHE`.

If any of the commands fail or result in a traceback, create a bug report at [https://bugs.ixsystems.com](https://bugs.ixsystems.com). Include the commands in the order in which they were run and the exact wording of the error message or traceback.

### 12.2 LDAP

FreeNAS® includes an [OpenLDAP](http://www.openldap.org/) 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 Mac OS X Server, Novell eDirectory, and OpenLDAP running on a BSD or Linux system. If an LDAP server is running on the 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 is disabled unless the LDAP directory has been configured for and populated with Samba attributes. The most popular script for performing this task is `smbldap-tools` ([https://wiki.samba.org/index.php/4.1_smbldap-tools](https://wiki.samba.org/index.php/4.1_smbldap-tools)). The LDAP server must support SSL/TLS and the certificate for the LDAP server CA must be imported with `System → CAs → Import CA`. Non-CA certificates are not currently supported.


Figure 12.2 shows the LDAP Configuration section from Directory Services → LDAP.
Fig. 12.2: Configuring LDAP

Table 12.3 summarizes the available configuration options. Some settings are only available in Advanced Mode. Click the ADVANCED MODE button to show the Advanced Mode settings. Go to System → Advanced and set the Show advanced fields by default option to always show advanced options.

Those new to LDAP terminology should read the OpenLDAP Software 2.4 Administrator’s Guide (http://www.openldap.org/doc/admin24/).

Table 12.3: LDAP Configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>string</td>
<td></td>
<td>LDAP server hostnames or IP addresses. Separate entries with an empty space. Multiple hostnames or IP addresses can be entered to create an LDAP failover priority list. If a host does not respond, the next host in the list is tried until a new connection is established.</td>
</tr>
<tr>
<td>Base DN</td>
<td>string</td>
<td></td>
<td>Top level of the LDAP directory tree to be used when searching for resources (Example: dc=test,dc=org).</td>
</tr>
<tr>
<td>Bind DN</td>
<td>string</td>
<td></td>
<td>Administrative account name on the LDAP server (Example: cn=Manager,dc=test,dc=org).</td>
</tr>
<tr>
<td>Bind Password</td>
<td>string</td>
<td></td>
<td>Password for the Bind DN. Click SHOW/HIDE PASSWORDS to view or obscure the password characters.</td>
</tr>
<tr>
<td>Allow Anonymous Binding</td>
<td>checkbox</td>
<td>✓</td>
<td>Instruct the LDAP server to disable authentication and allow read and write access to any client.</td>
</tr>
</tbody>
</table>

Continued on next page
### Table 12.3 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos Realm</td>
<td>drop-down menu</td>
<td>✓</td>
<td>The realm created using the instructions in <em>Kerberos Realms</em> (page 213).</td>
</tr>
<tr>
<td>Kerberos Principal</td>
<td>drop-down menu</td>
<td>✓</td>
<td>The location of the principal in the keytab created as described in <em>Kerberos Keytabs</em> (page 214).</td>
</tr>
</tbody>
</table>
| Encryption Mode         | drop-down menu| ✓             | Options for encrypting the LDAP connection:  
• **OFF**: do not encrypt the LDAP connection.  
• **ON**: encrypt the LDAP connection with SSL on port 636.  
• **START_TLS**: encrypt the LDAP connection with START-TLS on the default LDAP port 389. |
| Certificate              | drop-down menu| ✓             | Certificate (page 116) to use when performing LDAP certificate-based authentication. To configure LDAP certificate-based authentication, create a Certificate Signing Request for the LDAP provider to sign. A certificate is not required when using username/password or Kerberos authentication. |
| Validate Certificate     | checkbox      | ✓             | Verify certificate authenticity.                                                                                                             |
| Disable LDAP User/Group Cache | checkbox | ✓             | Disable caching LDAP users and groups in large LDAP environments. When caching is disabled, LDAP users and groups do not appear in dropdown menus, but are still accepted when manually entered. |
| 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| ✓             | Backend used to map Windows security identifiers (SIDs) to UNIX UIDs and GIDs. See Table 12.2 for a summary of the available backends. To configure the selected backend, click EDIT IDMAP. |
| Samba Schema             | checkbox      | ✓             | Set if LDAP authentication for SMB shares is required and the LDAP server is already configured with Samba attributes.                        |
| Auxiliary Parameters     | string        | ✓             | Additional options for ns1cd.conf (https://arthurdejong.org/nss-pam-ldapd/ns1cd.conf.5).                                                      |
| Schema                   | drop-down menu| ✓             | If Samba Schema is set, select the schema to use. Choices are rfc2307 and rfc2307bis.                                                       |
| Enable                   | checkbox      |               | Unset to disable the configuration without deleting it.                                                                                     |

LDAP users and groups appear in the drop-down menus of the *Permissions* screen of a dataset after configuring the LDAP service. Type `getent passwd` in the FreeNAS® *Shell* (page 341) to verify the users have been imported. Type `getent group` to verify the groups have been imported. When the *Samba Schema* is enabled, LDAP users also appear in the output of `pdbedit -L`.

If the users and groups are not listed, refer to Common errors encountered when using OpenLDAP Software (http://www.openldap.org/doc/admin24/app/appendix-common-errors.html) for common errors and how to fix them.

Any LDAP bind errors are displayed during the LDAP bind process. When troubleshooting LDAP, you can open the FreeNAS® *Shell* (page 341) and find ns1cd.conf errors in `/var/log/messages`. When *Samba schema* is enabled, any Samba errors are recorded in `/var/log/samba4/log.smbd`. Additional details are saved in `/var/log/middlewared.log`.

To clear LDAP users and groups from FreeNAS®, go to *Directory Services* → *LDAP*, clear the *Hostname* field, unset *Enable*, and click *SAVE*. Confirm LDAP users and groups are cleared by going to the *Shell* and viewing the output of the `getent passwd` and `getent group` commands.
12.3 NIS

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

Click the Rebuild Directory Service Cache button if a new NIS user needs immediate access to FreeNAS®. This occurs automatically once a day as a cron job.


Figure 12.3 shows the Directory Services → NIS section. Table 12.4 summarizes the configuration options.

Table 12.4: NIS Configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIS domain</td>
<td>string</td>
<td>Name of NIS domain.</td>
</tr>
<tr>
<td>NIS servers</td>
<td>string</td>
<td>Comma-delimited list of hostnames or IP addresses.</td>
</tr>
</tbody>
</table>
Table 12.4 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure mode</td>
<td>checkbox</td>
<td>Set to have <code>ypbind(8)</code> (<a href="https://www.freebsd.org/cgi/man.cgi?query=ypbind">https://www.freebsd.org/cgi/man.cgi?query=ypbind</a>) refuse to bind to any NIS server not running as root on a TCP port over 1024.</td>
</tr>
<tr>
<td>Manycast</td>
<td>checkbox</td>
<td>Set to have <code>ypbind</code> to bind to the server that responds the fastest. This is useful when no local NIS server is available on the same sub-net.</td>
</tr>
<tr>
<td>Enable</td>
<td>checkbox</td>
<td>Unset to disable the configuration without deleting it.</td>
</tr>
</tbody>
</table>

### 12.4 Kerberos Realms

A default Kerberos realm is created for the local system in FreeNAS®. Directory Services → Kerberos Realms can be used to view and add Kerberos realms. If the network contains a Key Distribution Center (KDC), click **ADD** to add the realm. The configuration screen is shown in **Figure 12.4**.

Fig. 12.4: Adding a Kerberos Realm

Table 12.5 summarizes the configurable options. Some settings are only available in Advanced Mode. To see these settings, either click **ADVANCED MODE** or configure the system to always display these settings by setting **Show advanced fields by default** in System → Advanced.
Table 12.5: Kerberos Realm Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realm</td>
<td>string</td>
<td></td>
<td>Name of the realm.</td>
</tr>
<tr>
<td>KDC</td>
<td>string</td>
<td>✓</td>
<td>Name of the Key Distribution Center.</td>
</tr>
<tr>
<td>Admin Server</td>
<td>string</td>
<td>✓</td>
<td>Server where all changes to the database are performed.</td>
</tr>
<tr>
<td>Password Server</td>
<td>string</td>
<td>✓</td>
<td>Server where all password changes are performed.</td>
</tr>
</tbody>
</table>

12.5 Kerberos Keytabs

Kerberos keytabs are used to do Active Directory or LDAP joins without a password. This means 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.

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 the `ktpass` (https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ktpass) command:

```
ktpass.exe /out freenas.keytab /princ http/useraccount@EXAMPLE.COM /mapuser useraccount /ptype... → KRB5_NT_PRINCIPAL /crypto ALL /pass userpass
```

where:

- `freenas.keytab` is the file to upload to the FreeNAS® server.
- `http/useraccount@KERBEROS.REALM` is the principal name written in the format `host/user.account@KERBEROS.REALM`. By convention, the kerberos realm is written in all caps, but make sure the case used for the Kerberos Realm (page 213) matches the realm name. See this note (https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ktpass#BKMK_remarks) about using `/princ` for more details.
- `userpass` is the password associated with `useraccount`.

Setting `/crypto` to `ALL` allows using all supported cryptographic types. These keys can be specified instead of `ALL`:

- `DES-CBC-CRC` is used for compatibility.
- `DES-CBC-MD5` adheres more closely to the MIT implementation and is used for compatibility.
- `RC4-HMAC-NT` uses 128-bit encryption.
- `AES256-SHA1` uses AES256-CTS-HMAC-SHA1-96 encryption.
- `AES128-SHA1` uses AES128-CTS-HMAC-SHA1-96 encryption.

This will create a keytab with sufficient privileges to grant tickets.

After the keytab is generated, add it to the FreeNAS® system using Directory Services → Kerberos Keytabs → Add Kerberos Keytab.

To instruct the Active Directory service to use the keytab, select the installed keytab using the drop-down Kerberos Principal menu in Directory Services → Active Directory Advanced Mode. When using a keytab with Active Directory, make sure that username and userpass in the keytab matches the Domain Account Name and Domain Account Password fields in Directory Services → Active Directory.

To instruct LDAP to use a principal from the keytab, select the principal from the drop-down Kerberos Principal menu in Directory Services → LDAP Advanced Mode.
12.6 Kerberos Settings

Configure additional Kerberos parameters in the Directory Services → Kerberos Settings section. Figure 12.5 shows the fields available:

- **Appdefaults Auxiliary Parameters**: Define any additional settings for use by some Kerberos applications. The available settings and syntax is listed in the [appdefaults] section of krb.conf(5) (http://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/krb5_conf.html#appdefaults).

- **Libdefaults Auxiliary Parameters**: Define any settings used by the Kerberos library. The available settings and their syntax are listed in the [libdefaults] section of krb.conf(5) (http://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/krb5_conf.html#libdefaults).
Shares provide and control access to an area of storage. Consider factors like operating system, security, transfer speed, and user access before creating a new share. This information can help determine the type of share, if multiple datasets are needed to divide the storage into areas with different access and permissions, and the complexity of setting up permissions.

Note that shares are only used to provide access to data. Deleting a share configuration does not affect the data that was being shared.

These types of shares and services are available:

- **AFP** (page 217): Apple Filing Protocol shares are used when the client computers all run macOS. Apple has deprecated AFP in favor of **SMB** (page 246). Using AFP in modern networks is no longer recommended.

- **Unix (NFS)** (page 237): Network File System shares are accessible from macOS, Linux, BSD, and the professional and enterprise versions (but not the home editions) of Windows. This can be a good choice when the client computers do not all run the same operating system but NFS client software is available for all of them.

- **WebDAV** (page 244): WebDAV shares are accessible using an authenticated web browser (read-only) or WebDAV client (https://en.wikipedia.org/wiki/WebDAV#Client_support) running on any operating system.

- **SMB** (page 246): Server Message Block shares, also known as Common Internet File System (CIFS) shares, are accessible by Windows, macOS, Linux, and BSD computers. Access is slower than an NFS share due to the single-threaded design of Samba. SMB provides more configuration options than NFS and is a good choice on a network for Windows or Mac systems. However, it is a poor choice if the CPU on the FreeNAS® system is limited. If it is maxed out, upgrade the CPU or consider a different type of share.

- **Block (iSCSI)** (page 222): Block or iSCSI shares appear as an unformatted disk to clients running iSCSI initiator software or a virtualization solution such as VMware. These are usually used as virtual drives.

Fast access from any operating system can be obtained by configuring the **FTP** (page 263) service instead of a share and using a cross-platform FTP file manager application such as Filezilla (https://filezilla-project.org/). Secure FTP can be configured if the data needs to be encrypted.

When data security is a concern and the network users are familiar with SSH command line utilities or WinSCP (https://winscp.net/eng/index.php), consider using the **SSH** (page 281) service instead of a share. It is slower than unencrypted FTP due to the encryption overhead, but the data passing through the network is encrypted.

**Note:** It is generally a mistake to share a pool or dataset with more than one share type or access method. Different types of shares and services use different file locking methods. For example, if the same pool is configured to use both NFS and FTP, NFS will lock a file for editing by an NFS user, but an FTP user can simultaneously edit or delete that file. This results in lost edits and confused users. Another example: if a pool is configured for both AFP and SMB, Windows users can be confused by the “extra” filenames used by Mac files and delete them. This corrupts the files on the AFP share. Pick the one type of share or service that makes the most sense for the types of clients accessing that pool, and use that single type of share or service. To support multiple types of shares, divide the pool into datasets and use one dataset per share.

This section demonstrates configuration and fine-tuning of AFP, NFS, SMB, WebDAV, and iSCSI shares. FTP and SSH configurations are described in **Services** (page 259).
13.1 Apple (AFP) Shares

FreeNAS® uses the Netatalk (http://netatalk.sourceforge.net/) AFP server to share data with Apple systems. This section describes the configuration screen for fine-tuning AFP shares. It then provides configuration examples for configuring Time Machine to back up to a dataset on the FreeNAS® system and for connecting to the share from a macOS client.

Create a share by clicking Sharing → Apple (AFP), then ADD.

New AFP shares are visible in the Sharing → Apple (AFP) menu.

The configuration options shown in Figure 13.1 appear after clicking (Options) on an existing share, and selecting the Edit option. The values showing for these options will vary, depending upon the information given when the share was created.

![Fig. 13.1: Creating an AFP Share](image)

**Note:** Table 13.1 summarizes the options available to fine-tune an AFP share. Leaving these options at the default settings is recommended as changing them can cause unexpected behavior. Most settings are only available with Advanced Mode. Do not change an advanced option without fully understanding the function of that option. Refer to Setting up Netatalk (http://netatalk.sourceforge.net/2.2/htmldocs/configuration.html) for a more detailed explanation of these options.
Table 13.1: AFP Share Configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>browse button</td>
<td></td>
<td>Browse to the pool or dataset to share. Do not nest additional pools, datasets, or symbolic links beneath this path because Netatalk does not fully support that.</td>
</tr>
<tr>
<td>Name</td>
<td>string</td>
<td></td>
<td>Enter the pool name that appears in macOS after selecting Go → Connect to server in the Finder menu. Limited to 27 characters and cannot contain a period.</td>
</tr>
<tr>
<td>Comment</td>
<td>string</td>
<td>✓</td>
<td>Optional comment.</td>
</tr>
<tr>
<td>Allow list</td>
<td>string</td>
<td>✓</td>
<td>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.</td>
</tr>
<tr>
<td>Deny list</td>
<td>string</td>
<td>✓</td>
<td>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.</td>
</tr>
<tr>
<td>Read Only Access</td>
<td>string</td>
<td>✓</td>
<td>Comma-delimited list of users and/or groups who only have read access where groupname begins with a @.</td>
</tr>
<tr>
<td>Read/Write Access</td>
<td>string</td>
<td>✓</td>
<td>Comma-delimited list of users and/or groups who have read and write access where groupname begins with a @.</td>
</tr>
<tr>
<td>Time Machine</td>
<td>checkbox</td>
<td></td>
<td>Set to advertise FreeNAS® as a Time Machine disk so it can be found by Macs. Setting multiple shares for Time Machine use is not recommended. When multiple Macs share the same pool, low diskspace issues and intermittently failed backups can occur.</td>
</tr>
<tr>
<td>Time Machine Quota</td>
<td>integer</td>
<td></td>
<td>Appears when Time Machine is set. Enter a storage quota for each Time Machine backup on this share. The share must be remounted for any changes to this value to take effect.</td>
</tr>
<tr>
<td>Use as home share</td>
<td>checkbox</td>
<td></td>
<td>Allows the share to host user home directories. Each user is given a personal home directory when connecting to the share which is not accessible by other users. This allows for a personal, dynamic share. Only one share can be used as the home share.</td>
</tr>
<tr>
<td>Zero Device Numbers</td>
<td>checkbox</td>
<td>✓</td>
<td>Enable when the device number is not constant across a reboot.</td>
</tr>
<tr>
<td>No Stat</td>
<td>checkbox</td>
<td>✓</td>
<td>If set, AFP does not stat the pool path when enumerating the pools list. Useful for automounting or pools created by a preexec script.</td>
</tr>
<tr>
<td>AFP3 UNIX Privs</td>
<td>checkbox</td>
<td>✓</td>
<td>Set to enable Unix privileges supported by Mac OS X 10.5 and higher. Do not enable if the network has Mac OS X 10.4 or lower clients. Those systems do not support this feature.</td>
</tr>
<tr>
<td>Default file permissions</td>
<td>checkboxes</td>
<td>✓</td>
<td>Only works with Unix ACLs. New files created on the share are set with the selected permissions.</td>
</tr>
<tr>
<td>Default directory permissions</td>
<td>checkboxes</td>
<td>✓</td>
<td>Only works with Unix ACLs. New directories created on the share are set with the selected permissions.</td>
</tr>
<tr>
<td>Default umask</td>
<td>integer</td>
<td>✓</td>
<td>Umask is used for newly created files. Default is 000 (anyone can read, write, and execute).</td>
</tr>
<tr>
<td>Hosts Allow</td>
<td>string</td>
<td>✓</td>
<td>Enter a list of allowed hostnames or IP addresses. Separate entries with a comma, space, or tab. Please see the note (page ??) for more information.</td>
</tr>
<tr>
<td>Hosts Deny</td>
<td>string</td>
<td>✓</td>
<td>Enter a list of denied hostnames or IP addresses. Separate entries with a comma, space, or tab. Please see the note (page ??) for more information.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 13.1 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auxiliary Parameters</td>
<td>string</td>
<td>✓</td>
<td>Enter any additional afp.conf parameters not covered by other option fields.</td>
</tr>
</tbody>
</table>

Note: If neither Hosts Allow or Hosts Deny contains an entry, then AFP share access is allowed for any host.

If there is a Hosts Allow list but no Hosts Deny list, then only allow hosts on the Hosts Allow list.

If there is a Hosts Deny list but no Hosts Allow list, then allow all hosts that are not on the Hosts Deny list.

If there is both a Hosts Allow and Hosts Deny list, then allow all hosts that are on the Hosts Allow list. If there is a host not on the Hosts Allow and not on the Hosts Deny list, then allow it.

13.1.1 Creating AFP Guest Shares

AFP supports guest logins, meaning that macOS users can access the AFP share without requiring their user accounts to first be created on or imported into the FreeNAS® system.

Note: When a guest share is created along with a share that requires authentication, AFP only maps users who log in as guest to the guest share. If a user logs in to the share that requires authentication, permissions on the guest share can 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 click the sliding button to turn on the service. Click (Configure) to open the screen shown in Figure 13.2. For Guest Account, use the drop-down to select Nobody, set Guest Access, and click SAVE.
Next, create a dataset for the guest share. Refer to Adding Datasets (page 181) for more information about dataset creation.

After creating the dataset for the guest share, go to Storage → Pools, click the ▼ (Options) button for the dataset, then click Edit Permissions. Complete the fields shown in Figure 13.3.

1. **User**: Use the drop-down to select Nobody.
2. Click SAVE.
To create a guest AFP share:

1. Go to Sharing → Apple (AFP) Shares and click ADD.
2. Browse to the dataset created for the guest share.
3. Fill out the other required fields, then press SAVE.

macOS users can use Finder to connect to the guest AFP share by clicking Go → Connect to Server. In the example shown in Figure 13.4, the user 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.
To disconnect from the pool, click the eject button in the Shared sidebar.

13.2 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 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 addresses and ports to listen on for connection requests.

**LUN**: Logical Unit Number representing a logical SCSI device. An initiator negotiates with a target to establish connectivity to a LUN. The result is an iSCSI connection that emulates a connection to a SCSI hard disk. Initiators treat
iSCSI LUNs as if they were a raw SCSI or SATA hard drive. Rather than mounting remote directories, initiators format and directly manage filesystems on iSCSI LUNs. When configuring multiple iSCSI LUNs, create a new target for each LUN. Since iSCSI multiplexes a target with multiple LUNs over the same TCP connection, there can be TCP contention when more than one target accesses the same LUN. FreeNAS® supports up to 1024 LUNs.

In FreeNAS®, iSCSI is built into the kernel. This version of iSCSI supports Microsoft Offloaded Data Transfer (ODX) (https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/ hh831628(v=ws.11)), meaning that file copies happen locally, rather than over the network. It also supports the VAAI (page 377) (vStorage APIs for Array Integration) primitives for efficient operation of storage tasks directly on the NAS. To take advantage of the VAAI primitives, create a zvol (page 185) and use it to create a device extent (page 231).

### 13.2.1 iSCSI Wizard

To configure iSCSI, click WIZARD and follow each step:

1. **Create or Choose Block Device**:
   - **Name**: Enter a name for the block device. Keeping the name short is recommended. Using a name longer than 63 characters can prevent access to the block device.
   - **Type**: Select *File* or *Device* as the type of block device. *Device* provides virtual storage access to zvols, zvol snapshots, or physical devices. *File* provides virtual storage access to an individual file.
   - **Device**: Select the unformatted disk, controller, zvol, or zvol snapshot. Select Create New for options to create a new zvol. If Create New is selected, use the browser to select an existing pool or dataset to store the new zvol. Enter the desired size of the zvol in Size. Only displayed when Type is set to *Device*.
   - **File**: Browse to an existing file. Create a new file by browsing to a dataset and appending the file name to the path. When the file already exists, enter a size of 0 to use the actual file size. For new files, enter the size of the file to create. Only displayed when Type is set to *File*.
   - **What are you using this for**: Choose the platform that will use this share. The associated options are applied to this share.

2. **Portal**
   - **Portal**: Select an existing portal or choose Create New to configure a new portal.
   - **Discovery Auth Method**: NONE allows anonymous discovery while CHAP and Mutual CHAP require authentication.
   - **Discovery Auth Group**: Choose an existing Authorized Access (page 227) group ID or create a new authorized access. This is required when the Discovery Auth Method is set to CHAP or Mutual CHAP.
   - **IP**: Select IP addresses to be listened on by the portal. Click ADD to add IP addresses with a different network port. The address 0.0.0.0 can be selected to listen on all IPv4 addresses, or :: to listen on all IPv6 addresses.
   - **Port**: TCP port used to access the iSCSI target. Default is 3260.

3. **Initiator**
   - **Initiators**: Leave blank to allow all or enter a list of initiator hostnames separated by spaces.
   - **Authorized Networks**: Network addresses allowed to use this initiator. Leave blank to allow all networks or list network addresses with a CIDR mask. Separate multiple addresses with a space: 192.168.2.0/24 192.168.2.1/12.

4. **Confirm Options**
   - Review the configuration and click SUBMIT to set up the iSCSI share.

The rest of this section describes iSCSI configuration in more detail.
13.2.2 Target Global Configuration

Sharing → Block (iSCSI) → Target Global Configuration contains settings that apply to all iSCSI shares. Table 13.2 describes each option.

Some built-in values affect iSNS usage. Fetching of allowed initiators from iSNS is not implemented, so target ACLs must be configured manually. To make iSNS registration useful, iSCSI targets should have explicitly configured port IP addresses. This avoids initiators attempting to discover unconfigured target portal addresses like 0.0.0.0.

The iSNS registration period is 900 seconds. Registered Network Entities not updated during this period are unregistered. The timeout for iSNS requests is 5 seconds.

![Fig. 13.5: iSCSI Target Global Configuration Variables](image)

Table 13.2: Target Global Configuration Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Name</td>
<td>string</td>
<td>Lowercase alphanumeric characters plus dot (.), dash (-), and colon (:), and colon (:) are allowed. See the “Constructing iSCSI names using the iqn. format” section of <a href="https://tools.ietf.org/html/rfc3721.html">RFC 3721</a>.</td>
</tr>
<tr>
<td>ISNS Servers</td>
<td>string</td>
<td>Enter the hostnames or IP addresses of ISNS servers to be registered with iSCSI targets and portals of the system. Separate each entry with a space.</td>
</tr>
<tr>
<td>Pool Available Space Threshold</td>
<td>integer</td>
<td>Enter the percentage of free space to remain in the pool. When this percentage is reached, the system issues an alert, but only if zvols are used. See [VAAI](page 377) Threshold Warning for more information.</td>
</tr>
</tbody>
</table>
13.2.3 Portals

A portal specifies the IP address and port number to be used for iSCSI connections. Go to Sharing → Block (iSCSI) → Portals and click ADD to display the screen shown in Figure 13.6.

Table 13.6 summarizes the settings that can be configured when adding a portal.

Table 13.3: Portal Configuration Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>string</td>
<td>Optional description. Portals are automatically assigned a numeric group.</td>
</tr>
<tr>
<td>Discovery Auth Method</td>
<td>drop-down menu</td>
<td>iSCSI (page 268) supports multiple authentication methods that are used by the target to discover valid devices. None allows anonymous discovery while CHAP and Mutual CHAP both require authentication.</td>
</tr>
<tr>
<td>Discovery Auth Group</td>
<td>drop-down menu</td>
<td>Select a Group ID created in Authorized Access if the Discovery Auth Method is set to CHAP or Mutual CHAP.</td>
</tr>
<tr>
<td>IP address</td>
<td>drop-down menu</td>
<td>Select IP addresses to be listened on by the portal. Click ADD to add IP addresses with a different network port. The address 0.0.0.0 can be selected to listen on all IPv4 addresses, or :: to listen on all IPv6 addresses.</td>
</tr>
<tr>
<td>Port</td>
<td>integer</td>
<td>TCP port used to access the iSCSI target. Default is 3260.</td>
</tr>
</tbody>
</table>

FreeNAS® systems with multiple IP addresses or interfaces can use a portal to provide services on different inter-
faces 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 these addresses:

192.168.1.1/24
192.168.2.1/24
192.168.3.1/24
192.168.4.1/24

A portal containing the first two IP addresses (group ID 1) and a portal containing the remaining two IP addresses (group ID 2) could be created. Then, a target named A with a Portal Group ID of 1 and a second target named B with a Portal Group ID of 2 could be created. 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.

### 13.2.4 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, go to **Sharing → Block (iSCSI) → Initiators** and click **ADD** as shown in [Figure 13.7](#).

![Fig. 13.7: Adding an iSCSI Initiator](#)
Table 13.4 summarizes the settings that can be configured when adding an initiator.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow All Initiators</td>
<td>checkbox</td>
<td>Accept all detected initiators. When set, all other initiator fields are</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disabled.</td>
</tr>
<tr>
<td>Connected Initiators</td>
<td>string</td>
<td>Initiators currently connected to the system. Shown in IQN format with an IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>address. Set initiators and click an ✖ to add the initiators to either the</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Allowed Initiators</strong> or <strong>Authorized Networks</strong> lists. Clicking <strong>REFRESH</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>updates the <strong>Connected Initiators</strong> list.</td>
</tr>
<tr>
<td>Allowed Initiators (IQN)</td>
<td>string</td>
<td>Initiators allowed access to this system. Enter an iSCSI Qualified Name (IQN)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(<a href="https://tools.ietf.org/html/rfc3720#section-3.2.6">https://tools.ietf.org/html/rfc3720#section-3.2.6</a>) and click + to add it</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to the list. Example: iqn.1994-09.org.freebsd:freenas.local</td>
</tr>
<tr>
<td>Authorized Networks</td>
<td>string</td>
<td>Network addresses allowed to use this initiator. Each address can include</td>
</tr>
<tr>
<td></td>
<td></td>
<td>an optional CIDR (<a href="https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing">https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing</a>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>netmask. Click + to add the network address to the list. Example: 192.168.2.0/24</td>
</tr>
<tr>
<td>Description</td>
<td>string</td>
<td>Any notes about initiators.</td>
</tr>
</tbody>
</table>

Click ✖ (Options) on an initiator entry for options to Edit or Delete it.

### 13.2.5 Authorized Access

When using CHAP or mutual CHAP to provide authentication, creating authorized access is recommended. Do this by going to **Sharing → Block (iSCSI) → Authorized Access** and clicking **ADD**. The screen is shown in Figure 13.8.

**Note:** This screen sets login authentication. This is different from discovery authentication which is set in **Global Configuration** (page 157).
Table 13.5 summarizes the settings that can be configured when adding an authorized access:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID</td>
<td>integer</td>
<td>Allow different groups to be configured with different authentication profiles. Example: enter 1 for all users in Group 1 to inherit the Group 1 authentication profile. Group IDs that are already configured with authorized access cannot be reused.</td>
</tr>
<tr>
<td>User</td>
<td>string</td>
<td>User account to create for CHAP authentication with the user on the remote system. Many initiators use the initiator name as the user name.</td>
</tr>
<tr>
<td>Secret</td>
<td>string</td>
<td>User password. Must be at least 12 and no more than 16 characters long.</td>
</tr>
<tr>
<td>Peer User</td>
<td>string</td>
<td>Only entered when configuring mutual CHAP. Usually the same value as User.</td>
</tr>
<tr>
<td>Peer Secret</td>
<td>string</td>
<td>Mutual secret password. Required when Peer User is set. Must be different than the Secret. Must be at least 12 and no more than 16 characters long.</td>
</tr>
</tbody>
</table>

**Note:** CHAP does not work with GlobalSAN initiators on macOS.

New authorized accesses are visible from the **Sharing → Block (iSCSI) → Authorized Access** menu. In the example
shown in Figure 13.9, 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.

Fig. 13.9: Viewing Authorized Accesses

13.2.6 Targets

Next, create a Target by going to Sharing → Block (iSCSI) → Targets and clicking ADD as shown in Figure 13.10. A target combines a portal ID, allowed initiator ID, and an authentication method. Table 13.6 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 13.6: Target Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Name</td>
<td>string</td>
<td>Required. The base name is automatically prepended if the target name does not start with <code>iqn</code>. Lowercase alphanumeric characters plus dot (<code>.</code>), dash (<code>-</code>), and colon (<code>:</code>) are allowed. See the “Constructing iSCSI names using the <code>iqn</code> format” section of RFC 3721 (<a href="https://tools.ietf.org/html/rfc3721.html">https://tools.ietf.org/html/rfc3721.html</a>).</td>
</tr>
<tr>
<td>Target Alias</td>
<td>string</td>
<td>Enter an optional user-friendly name.</td>
</tr>
<tr>
<td>Portal Group ID</td>
<td>drop-down</td>
<td>Leave empty or select number of existing portal to use.</td>
</tr>
<tr>
<td>Initiator Group ID</td>
<td>drop-down</td>
<td>Select which existing initiator group has access to the target.</td>
</tr>
<tr>
<td>Auth Method</td>
<td>drop-down</td>
<td><code>None</code>, <code>Auto</code>, <code>CHAP</code>, or <code>Mutual CHAP</code>.</td>
</tr>
<tr>
<td>Authentication Group number</td>
<td>drop-down</td>
<td>Select <code>None</code> or an integer. This number represents the number of existing authorized accesses.</td>
</tr>
</tbody>
</table>
### 13.2.7 Extents

iSCSI targets provide virtual access to resources on the FreeNAS® system. Extents are used to define resources to share with clients. There are two types of extents: *device* and *file*.

**Device extents** provide virtual storage access to zvols, zvol snapshots, or physical devices like a disk, an SSD, or a hardware RAID volume.

**File extents** provide virtual storage access to an individual file.

---

**Tip:** For typical use as storage for virtual machines where the virtualization software is the iSCSI initiator, **device extents with zvols provide the best performance and most features**. For other applications, device extents sharing a raw device can be appropriate. File extents do not have the performance or features of device extents, but do allow creating multiple extents on a single filesystem.

---

Virtualized zvols support all the FreeNAS® *VAAI* (page 377) primitives and are recommended for use with 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.

Virtualizing a raw device like a single disk or hardware RAID volume limits performance to the abilities of the device. Because this bypasses ZFS, such devices do not benefit from ZFS caching or provide features like block checksums or snapshots.

Virtualizing a zvol adds the benefits of ZFS, such as read and write cache. Even if the client formats a device extent with a different filesystem, the data still resides on a ZFS pool and benefits from ZFS features like block checksums and snapshots.

---

**Warning:** For performance reasons and to avoid excessive fragmentation, keep the used space of the pool below 80% when using iSCSI. The capacity of an existing extent can be increased as shown in *Growing LUNs* (page 235).

---

To add an extent, go to **Sharing → Block (iSCSI) → Extents** and click **ADD**. In the example shown in Figure 13.11, the device extent is using the *export zvol* that was previously created from the */mnt/pool1* pool.

Table 13.7 summarizes the settings that can be configured when creating an extent. Note that **file extent creation fails unless the name of the file to be created is appended to the pool or dataset name.**
**Fig. 13.11: Adding an iSCSI Extent**

Table 13.7: Extent Configuration Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extent name</td>
<td>string</td>
<td>Enter the extent name. If the Extent size is not 0, it cannot be an existing file within the pool or dataset.</td>
</tr>
<tr>
<td>Extent type</td>
<td>drop-down menu</td>
<td><em>File</em> shares the contents of an individual file. <em>Device</em> shares an entire device.</td>
</tr>
<tr>
<td>Path to the extent</td>
<td>browse button</td>
<td>Only appears when <em>File</em> is selected. Browse to an existing file. Create a new file by browsing to a dataset and appending the file name to the path. Extents cannot be created inside a jail root directory.</td>
</tr>
<tr>
<td>Extent size</td>
<td>integer</td>
<td>Only appears when <em>File</em> is selected. Entering 0 uses the actual file size and requires that the file already exists. Otherwise, specify the file size for the new file.</td>
</tr>
<tr>
<td>Device</td>
<td>drop-down menu</td>
<td>Only appears when <em>Device</em> is selected. Select the unformatted disk, controller, zvol, or zvol snapshot.</td>
</tr>
<tr>
<td>Logical block size</td>
<td>drop-down menu</td>
<td>Leave at the default of 512 unless the initiator requires a different block size.</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable physical block size reporting</td>
<td>checkbox</td>
<td>Set if the initiator does not support physical block size values over 4K (MS SQL). Setting can also prevent constant block size warnings (<a href="https://www.virten.net/2016/12/the-physical-block-size-reported-by-the-device-is-not-supported/">https://www.virten.net/2016/12/the-physical-block-size-reported-by-the-device-is-not-supported/</a>) when using this share with ESXi.</td>
</tr>
<tr>
<td>Available space threshold</td>
<td>string</td>
<td>Only appears if File or a zvol is selected. When the specified percentage of free space is reached, the system issues an alert. See VAAI (page 377) Threshold Warning.</td>
</tr>
<tr>
<td>Description</td>
<td>string</td>
<td>Notes about this extent.</td>
</tr>
<tr>
<td>Enable TPC</td>
<td>checkbox</td>
<td>Set to allow an initiator to bypass normal access control and access any scannable target. This allows xcopy (<a href="https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc771254(v=ws.11)">https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc771254(v=ws.11)</a>) operations which are otherwise blocked by access control.</td>
</tr>
<tr>
<td>Xen initiator compat mode</td>
<td>checkbox</td>
<td>Set when using Xen as the iSCSI initiator.</td>
</tr>
<tr>
<td>LUN RPM</td>
<td>drop-down</td>
<td>Do NOT change this setting when using Windows as the initiator. Only needs to be changed in large environments where the number of systems using a specific RPM is needed for accurate reporting statistics.</td>
</tr>
<tr>
<td>Read-only</td>
<td>checkbox</td>
<td>Set to prevent the initiator from initializing this LUN.</td>
</tr>
<tr>
<td>Enable</td>
<td>checkbox</td>
<td>Set to enable the iSCSI extent.</td>
</tr>
</tbody>
</table>

New extents have been added to `Sharing → Block (iSCSI) → Extents`. The associated Serial and Network Address Authority (NAA) are shown along with the extent name.

### 13.2.8 Associated Targets

The last step is associating an extent to a target by going to `Sharing → Block (iSCSI) → Associated Targets` and clicking `ADD`. The screen is shown in Figure 13.12. Use the drop-down menus to select the existing target and extent. Click `SAVE` to add an entry for the LUN.
Table 13.8 summarizes the settings that can be configured when associating targets and extents.

Table 13.8: Associated Target Configuration Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>drop-down menu</td>
<td>Select an existing target.</td>
</tr>
<tr>
<td>LUN ID</td>
<td>integer</td>
<td>Select or enter a value between 0 and 7023. Some initiators expect a value less than 256. Leave this field blank to automatically assign the next available ID.</td>
</tr>
<tr>
<td>Extent</td>
<td>drop-down menu</td>
<td>Select an existing extent.</td>
</tr>
</tbody>
</table>

Always associating extents to targets in a one-to-one manner is recommended, even though the web interface 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. Clearing the initiator connections to a LUN before deleting it is recommended.

After iSCSI has been configured, remember to start the service in Services → iSCSI by clicking the Ω (Power) button.

13.2.9 Connecting to iSCSI

To access the iSCSI target, clients must use iSCSI initiator software.

macOS does not include an initiator. globalSAN (http://www.studionetworksolutions.com/globalsan-iscsi-initiator/) is a commercial, easy-to-use Mac initiator.


Some Linux distros provide the command line utility iscsiadm from Open-iSCSI (http://www.open-iscsi.com/). Use a web search to see if a package exists for the distribution should the command not exist on the Linux system.

If a LUN is added while iscsiadm is already connected, it will not see the new LUN until rescanned with 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)(https://www.vladan.fr/how-to-configure-freenas-8-for-iscsi-and-connect-to-esxi/). 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 (https://www.vmware.com/pdf/vsphere4/r41/vsp_41_iscsi_sanCfg.pdf) for details.

The VMware firewall only allows iSCSI connections on port 3260 by default. If a different port has been selected, outgoing connections to that port must be manually added to the firewall before those connections will work.

If the target can be seen but does not connect, check the DiscoveryAuth 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.

### 13.2.10 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.

Enlarging a LUN with one of the methods below gives it more unallocated space, but does not automatically resize filesystems or other data on the LUN. This is the same as binary-copying a smaller disk onto a larger one. More space is available on the new disk, but the partitions and filesystems on it must be expanded to use this new space. Resizing virtual disk images is usually done from virtual machine management software. Application software to resize filesystems is dependent on the type of filesystem and client, but is often run from within the virtual machine. For instance, consider a Windows VM with the last partition on the disk holding an NTFS filesystem. The LUN is expanded and the partition table edited to add the new space to the last partition. The Windows disk manager must still be used to resize the NTFS filesystem on that last partition to use the new space.

#### 13.2.10.1 Zvol Based LUN

To grow a zvol-based LUN, go to Storage → Pools, click † (Options) on the zvol to be grown, then click Edit zvol. In the example shown in Figure 13.13, the current size of the zvol named zvol1 is 4 GiB.
Enter the new size for the zvol in the **Size for this zvol** field and click **SAVE**. The new size for the zvol is immediately shown in the **Used** column of the **Storage → Pools** table.

**Note:** The web interface does not allow reducing 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 pool size.

### 13.2.10.2 FileExtent Based LUN

To grow a file extent-based LUN:

Go to **Services → iSCSI → CONFIGURE → Extents**. Click **† (Options)**, then **Edit**. Ensure the **Extent Type** is set to file and enter the **Path to the extent**. Open the **Shell** (page 341) to grow the file extent. This example grows `/mnt/pool1/data` by 2 GiB:

```
truncate -s +2g /mnt/pool1/data
```

Return to **Services → iSCSI → CONFIGURE → Extents**, click **† (Options)** on the desired file extent, then click **Edit**. Set the size to 0 as this causes the iSCSI target to use the new size of the file.
13.3 Unix (NFS) Shares

FreeNAS® supports sharing pools, datasets, and directories over the Network File System (NFS). Clients use the `mount` command to mount the share. Mounted NFS shares appear as another directory on the client system. Some Linux distros require the installation of additional software to mount an NFS share. Windows systems must 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. When considering creating NFS shares on ESXi, read through the performance analysis presented in [Running ZFS over NFS as a VMware Store](https://tinyurl.com/archive-zfs-over-nfs-vmware).

Create an NFS share by going to `Sharing → Unix (NFS) Shares` and clicking `ADD`. Figure 13.14 shows an example of creating an NFS share.

![NFS Share Creation](image)

Fig. 13.14: NFS Share Creation

Remember these points when creating NFS shares:

1. Clients specify the *Path* when mounting the share.
2. The *Maproot* and *Mapall* options cannot both be enabled. The *Mapall* options supersede the *Maproot* options. To restrict only the *root* user permissions, set the *Maproot* option. To restrict permissions of all users, set the *Mapall* options.
3. Each pool or dataset is considered to be a unique filesystem. Individual NFS shares cannot cross filesystem boundaries. Adding paths to share more directories only works if those directories are within the same filesystem.
4. The network and host must be unique to both each created share and the filesystem or directory included in that share. Because `/etc/exports` is not an access control list (ACL), the rules contained in `/etc/exports` become undefined with overlapping networks or when using the same share with multiple hosts.

5. The `All dirs` option can only be used once per share per filesystem.

To better understand these restrictions, consider scenarios where there are:

- two networks, `10.0.0.0/8` and `20.0.0.0/8`
- a ZFS pool named `pool1` with a dataset named `dataset1`
- `dataset1` contains directories named `directory1`, `directory2`, and `directory3`

Because of restriction #3, an error is shown when trying to create one NFS share like this:

- `Authorized Networks` set to `10.0.0.0/8 20.0.0.0/8`
- `Path` set to the dataset `/mnt/pool1/dataset1`. An additional path to directory `/mnt/pool1/dataset1/directory1` is added.

The correct method to configure this share is to set the `Path` to `/mnt/pool1/dataset1` and set the `All dirs` box. This allows the client to also mount `/mnt/pool1/dataset1/directory1` when `/mnt/pool1/dataset1` is mounted.

Additional paths are used to define specific directories to be shared. For example, `dataset1` has three directories. To share only `/mnt/pool1/dataset1/directory1` and `/mnt/pool1/dataset1/directory2`, create paths for `directory1` and `directory2` within the share. This excludes `directory3` from the share.

Restricting a specific directory to a single network is done by creating a share for the volume or dataset and a share for the directory within that volume or dataset. Define the authorized networks for both shares.

First NFS share:

- `Authorized Networks` set to `10.0.0.0/8`
- `Path` set to `/mnt/pool1/dataset1`

Second NFS share:

- `Authorized Networks` set to `20.0.0.0/8`
- `Path` set to `/mnt/pool1/dataset1/directory1`

This requires the creation of two shares. It cannot be done with only one share.

**Table 13.9** summarizes the available configuration options in the `Sharing/NFS/Add` screen. Click `ADVANCED MODE` to see all settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>browse but-&lt;br&gt;ton</td>
<td></td>
<td>Browse to the dataset or directory to be shared. Click <code>ADD</code> to specify multiple paths.</td>
</tr>
<tr>
<td>Comment</td>
<td>string</td>
<td></td>
<td>Text describing the share. Typically used to name the share. If left empty, this shows the <code>Path</code> entries of the share.</td>
</tr>
<tr>
<td>All dirs</td>
<td>checkbox</td>
<td></td>
<td>Allow the client to also mount any subdirectories of the selected pool or dataset.</td>
</tr>
<tr>
<td>Read only</td>
<td>checkbox</td>
<td></td>
<td>Prohibit writing to the share.</td>
</tr>
<tr>
<td>Quiet</td>
<td>checkbox</td>
<td>✓</td>
<td>Restrict some syslog diagnostics to avoid some error messages. See <code>exports(5)</code> (<a href="https://www.freebsd.org/cgi/man.cgi?query=exports">https://www.freebsd.org/cgi/man.cgi?query=exports</a>) for examples.</td>
</tr>
<tr>
<td>Setting</td>
<td>Value</td>
<td>Advanced Mode</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authorized networks</td>
<td>string</td>
<td>✓</td>
<td>Space-delimited list of allowed networks in network/mask CIDR notation. Example: 1.2.3.0/24. Leave empty to allow all.</td>
</tr>
<tr>
<td>Authorized Hosts and IP addresses</td>
<td>string</td>
<td>✓</td>
<td>Space-delimited list of allowed IP addresses or hostnames. Leave empty to allow all.</td>
</tr>
<tr>
<td>Maproot User</td>
<td>drop-down menu</td>
<td>✓</td>
<td>When a user is selected, the root user is limited to permissions of that user.</td>
</tr>
<tr>
<td>Maproot Group</td>
<td>drop-down menu</td>
<td>✓</td>
<td>When a group is selected, the root user is also limited to permissions of that group.</td>
</tr>
<tr>
<td>Mapall User</td>
<td>drop-down menu</td>
<td>✓</td>
<td>FreeNAS® user or user imported with Active Directory (page 204). The specified permissions of that user are used by all clients.</td>
</tr>
<tr>
<td>Mapall Group</td>
<td>drop-down menu</td>
<td>✓</td>
<td>FreeNAS® group or group imported with Active Directory (page 204). The specified permissions of that group are used by all clients.</td>
</tr>
<tr>
<td>Security</td>
<td>selection</td>
<td>✓</td>
<td>Only appears if Enable NFSv4 is enabled in Services → NFS. Choices are sys or these Kerberos options: krb5 (authentication only), krb5i (authentication and integrity), or krb5p (authentication and privacy). If multiple security mechanisms are added to the Selected column using the arrows, use the Up or Down buttons to list in order of preference.</td>
</tr>
</tbody>
</table>

Go to Sharing → Unix (NFS) and click ➕ (Options) and Edit to edit an existing share. Figure 13.15 shows the configuration screen for the existing nfs_share1 share. Options are the same as described in NFS Share Options (page 238).
13.3.1 Example Configuration

By default, the `Mapall` fields are not set. This means that when a user connects to the NFS share, the user has 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 option is to do this:

1. Specify the built-in `nobody` account to be used for NFS access.
2. In the `Change Permissions` screen of the pool or dataset that is being shared, change the owner and group to `nobody` and set the permissions according to the desired 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 pool or dataset. For example, even if the `root` user is able to connect, it will not gain `root` access to the share.

13.3.2 Connecting to the Share

The following examples share this configuration:

1. The FreeNAS® system is at IP address `192.168.2.2`.
2. A dataset named `/mnt/pool1/nfs_share1` is created and the permissions set to the `nobody` user account and the `nobody` group.
3. An NFS share is created with these attributes:
   - **Path**: /mnt/pool1/nfs_share1
   - **Authorized Networks**: 192.168.2.0/24
   - **All dirs** option is enabled
   - **MapAll User** is set to nobody
   - **MapAll Group** is set to nobody

### 13.3.2.1 From BSD or Linux

NFS shares are mounted on BSD or Linux clients with this command executed as the superuser (root) or with `sudo`:

```
mount -t nfs 192.168.2.2:/mnt/pool1/nfs_share1 /mnt
```

- `-t nfs` specifies the filesystem type of the share
- `192.168.2.2` is the IP address of the FreeNAS® system
- `/mnt/pool1/nfs_share1` is the name of the directory to be shared, a dataset in this case
- `/mnt` is the mountpoint on the client system. This must be an existing, empty directory. The data in the NFS share appears in this directory on the client computer.

Successfully mounting the share returns to the command prompt without any status or error messages.

**Note:** If this command fails on a Linux system, make sure that the `nfs-utils` ([https://sourceforge.net/projects/nfs/files/nfs-utils/](https://sourceforge.net/projects/nfs/files/nfs-utils/)) package is installed.

This configuration allows users on the client system to copy files to and from `/mnt` (the mount point). All files are owned by nobody:nobody. Changes to any files or directories in `/mnt` write to the FreeNAS® system `/mnt/pool1/nfs_share1` dataset.

NFS share settings cannot be changed when the share is mounted on a client computer. The `umount` command is used to unmount the share on BSD and Linux clients. Run it as the superuser or with `sudo` on each client computer:

```
umount /mnt
```

### 13.3.2.2 From Microsoft

Windows NFS client support varies with versions and releases. For best results, use *Windows (SMB) Shares* (page 246).

### 13.3.2.3 From macOS

A macOS client uses Finder to mount the NFS volume. Go to 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 pool or dataset being shared by NFS. The example shown in Figure 13.16 continues with the example of `192.168.2.2:/mnt/pool1/nfs_share1`.

Finder opens automatically after connecting. The IP address of the FreeNAS® system displays in the SHARED section of the left frame and the contents of the share display in the right frame. Figure 13.17 shows an example where `/mnt/data` has one folder named `images`. The user can now copy files to and from the share.
Fig. 13.16: Mounting the NFS Share from macOS
13.3.3 Troubleshooting NFS

Some NFS clients do not support the NLM (Network Lock Manager) protocol used by NFS. 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 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 database` 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 → Configure` and enable the `Serve UDP NFS clients` option.
The `nfsstat -c` or `nfsstat -s` commands can be helpful to detect problems from the Shell (page 341). A high proportion of retries and timeouts compared to reads usually indicates network problems.

### 13.4 WebDAV Shares

In FreeNAS®, WebDAV shares can be created so that authenticated users can browse the contents of the specified pool, dataset, or directory from a web browser.

Configuring WebDAV shares is a two step process. First, create the WebDAV shares 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 → Configure`.
- **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 firewall only allows access to authorized systems.
- **port_number**: is configured in `Services → WebDAV → Configure`. If the FreeNAS® system is to be accessed using a public IP address, consider changing the default port number and ensure that the network firewall only allows access to authorized systems.
- **share_name**: is configured by clicking `Sharing → WebDAV Shares`, then `ADD`.

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 → Configure`.

**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, go to `Sharing → WebDAV Shares` and click `ADD`, which will open the screen shown in Figure 13.18.
Fig. 13.18: Adding a WebDAV Share

Table 13.10 summarizes the available options.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share Path Name</td>
<td>string</td>
<td>Enter a name for the share.</td>
</tr>
<tr>
<td>Comment</td>
<td>string</td>
<td>Optional.</td>
</tr>
<tr>
<td>Path</td>
<td>browse button</td>
<td>Enter the path or Browse to the pool or dataset to share. Appending a new name to the path creates a new dataset. Example: /mnt/pool1/newdataset.</td>
</tr>
<tr>
<td>Read Only</td>
<td>checkbox</td>
<td>Set to prohibit users from writing to the share.</td>
</tr>
<tr>
<td>Change User &amp; Group</td>
<td>checkbox</td>
<td>Ownership of all files in the share will be changed to user webdav and group webdav. Existing permissions will not be changed, but the ownership change might make files inaccessible to their original owners. This operation cannot be undone! If unset, ownership of files to be accessed through WebDAV must be manually set to the webdav or www user/group.</td>
</tr>
</tbody>
</table>

Click SAVE to create the share. Then, go to Services → WebDAV and click the ⚪️ (Power) button to turn on the service.

After the service starts, review the settings in Services → WebDAV → CONFIGURE 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 (page 288).
FreeNAS® uses Samba (https://www.samba.org/) to share pools using Microsoft's SMB protocol. SMB is built into the Windows and macOS operating systems and most Linux and BSD systems pre-install the Samba client in order to provide support for SMB. If the distro did not, install the Samba client using the distro software repository.

The SMB protocol supports many different types of configuration scenarios, ranging from the simple to 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.

Samba supports server-side copy of files on the same share with clients from Windows 8 and higher. Copying between two different shares is not server-side. Windows 7 clients support server-side copying with Robocopy (https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc733145(v=ws.11)).

This chapter starts by summarizing the available configuration options. It demonstrates some common configuration scenarios as well as offering some troubleshooting tips. Reading through this entire chapter before creating any SMB shares is recommended to gain a better understanding of the configuration scenario that meets the specific network requirements.


**Warning:** SMB1 is disabled by default for security (https://www.ixsystems.com/blog/library/do-not-use-smb1/). If necessary, SMB1 can be enabled in Services → SMB Configure.

Figure 13.19 shows the configuration screen that appears after clicking Sharing → Windows (SMB Shares), then ADD.
Table 13.11 summarizes the options available when creating a SMB share. Some settings are only configurable 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)](https://www.freebsd.org/cgi/man.cgi?query=smb.conf) provides more details for each configurable option.

### Table 13.11: SMB Share Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>browse button</td>
<td></td>
<td>Select the pool, dataset, or directory to share. The same path can be used by more than one share.</td>
</tr>
<tr>
<td>Name</td>
<td>string</td>
<td></td>
<td>Name the new share. Each share name must be unique. The names <code>global</code>, <code>homes</code>, and <code>printers</code> are reserved and cannot be used.</td>
</tr>
</tbody>
</table>

Fig. 13.19: Adding an SMB Share
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use as home share</td>
<td>checkbox</td>
<td></td>
<td>Set to allow this share to hold user home directories. Only one share can be the home share. Note that lower case names for user home directories are strongly recommended, as Samba maps usernames to all lower case. For example, the username John will be mapped to a home directory named john. If the Path to the home share includes an upper case username, delete the existing user and recreate it in Accounts → Users with an all lower case Username. Return to Sharing → SMB to create the home share, and select the Path that contains the new lower case username.</td>
</tr>
<tr>
<td>Description</td>
<td>string</td>
<td></td>
<td>Description of the share or notes on how it is used.</td>
</tr>
<tr>
<td>Export Read Only</td>
<td>checkbox</td>
<td>✓</td>
<td>Prohibit write access to this share.</td>
</tr>
<tr>
<td>Browsable to NetworkClients</td>
<td>checkbox</td>
<td>✓</td>
<td>Determine whether this share name is included when browsing shares. Home shares are only visible to the owner regardless of this setting.</td>
</tr>
<tr>
<td>Export Recycle Bin</td>
<td>checkbox</td>
<td>✓</td>
<td>Files that are deleted from the same dataset are moved to the Recycle Bin and do not take any additional space. This is only applies over the SMB protocol. Deleting files over NFS will remove the files permanently. When the files are in a different dataset or a child dataset, they are copied to the dataset where the Recycle Bin is located. To prevent excessive space usage, files larger than 20 MiB are deleted rather than moved. Adjust the Auxiliary Parameter crossrename:sizelimit= setting to allow larger files. For example, crossrename:sizelimit=50 allows moves of files up to 50 MiB in size. The recyle bin has read-write functionality. This means files can be permanently deleted or moved from the recylce bin. This is not a replacement for ZFS Snapshots (page 191).</td>
</tr>
<tr>
<td>Show Hidden Files</td>
<td>checkbox</td>
<td>✓</td>
<td>Disable the Windows hidden attribute on a new Unix hidden file. Unix hidden filenames start with a dot: .foo. Existing files are not affected.</td>
</tr>
<tr>
<td>Allow Guest Access</td>
<td>checkbox</td>
<td></td>
<td>Privileges are the same as the guest account. Guest access is disabled by default in Windows 10 version 1709 and Windows Server version 1903. Additional client-side configuration is required to provide guest access to these clients. MacOS clients: Attempting to connect as a user that does not exist in FreeNAS® does not automatically connect as the guest account. The Connect As: Guest option must be specifically chosen in MacOS to log in as the guest account. See the Apple documentation (<a href="https://support.apple.com/guide/mac-help/connect-mac-shared-computers-servers-mchlp1140/">https://support.apple.com/guide/mac-help/connect-mac-shared-computers-servers-mchlp1140/</a>) for more details.</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only Allow Guest Access</td>
<td>checkbox</td>
<td>✓</td>
<td>Requires <em>Allow guest access</em> to also be enabled. Forces guest access for all connections.</td>
</tr>
<tr>
<td>Access Based Share Enumeration</td>
<td>checkbox</td>
<td>✓</td>
<td>Restrict share visibility to users with a current Windows Share ACL access of read or write. Use Windows administration tools to adjust the share permissions. See smb.conf(5) (<a href="https://www.freebsd.org/cgi/man.cgi?query=smb.conf">https://www.freebsd.org/cgi/man.cgi?query=smb.conf</a>).</td>
</tr>
<tr>
<td>Hosts Allow</td>
<td>string</td>
<td>✓</td>
<td>Enter a list of allowed hostnames or IP addresses. Separate entries with a comma (,), space, or tab. Please see the note (page ??) for more information.</td>
</tr>
<tr>
<td>Hosts Deny</td>
<td>string</td>
<td>✓</td>
<td>Enter a list of denied hostnames or IP addresses. Specify ALL and list any hosts from Hosts Allow to have those hosts take precedence. Separate entries with a comma (,), space, or tab. Please see the note (page ??) for more information.</td>
</tr>
<tr>
<td>VFS Objects</td>
<td>selection</td>
<td>✓</td>
<td>Add virtual file system objects to enhance functionality. Table 13.12 summarizes the available objects.</td>
</tr>
<tr>
<td>Auxiliary Parameters</td>
<td>string</td>
<td>✓</td>
<td>Additional smb4.conf (<a href="https://www.freebsd.org/cgi/man.cgi?query=smb.conf">https://www.freebsd.org/cgi/man.cgi?query=smb.conf</a>) parameters not covered by other option fields.</td>
</tr>
</tbody>
</table>

**Note:** If neither *Hosts Allow* or *Hosts Deny* contains an entry, then SMB share access is allowed for any host.

If there is a *Hosts Allow* list but no *Hosts Deny* list, then only allow hosts on the *Hosts Allow* list.

If there is a *Hosts Deny* list but no *Hosts Allow* list, then allow all hosts that are not on the *Hosts Deny* list.

If there is both a *Hosts Allow* and *Hosts Deny* list, then allow all hosts that are on the *Hosts Allow* list. If there is a host not on the *Hosts Allow* and not on the *Hosts Deny* list, then allow it.

Here are some notes about **ADVANCED MODE** settings:

- **Hostname lookups add some time to accessing the SMB share.** If only using IP addresses, unset the *Hostnames Lookups* setting in Services → SMB → (Configure).

- **When the Browsable to Network Clients option is selected,** the share is visible through Windows File Explorer or through `net view`. When the *Use as home share* option is selected, deselecting the *Browsable to Network Clients* option hides the share named *homes* so that only the dynamically generated share containing the authenticated user home directory will be visible. By default, the *homes* share and the user home directory are both visible. Users are not automatically granted read or write permissions on browsable shares. This option provides no real security because shares that are not visible in Windows File Explorer can still be accessed with a UNC path.

- **If some files on a shared pool 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 in the smb.conf manual page (https://www.freebsd.org/cgi/man.cgi?query=smb.conf).

Samba disables NTLMv1 authentication by default for security. Standard configurations of Windows XP and some configurations of later clients like Windows 7 will not be able to connect with NTLMv1 disabled. Security guidance for NTLMv1 and LM network authentication (https://support.microsoft.com/en-us/help/2793313/security-guidance-for-ntlmv1-and-lm-network-authentication) has information about the security implications and ways to
enable NTLMv2 on those clients. If changing the client configuration is not possible, NTLMv1 authentication can be enabled by selecting the `NTLMv1 auth` option in `Services → SMB → ✔ (Configure).

Table 13.12 provides an overview of the available VFS objects. Be sure to research each object before adding or deleting it from the `Selected` column of the `VFS Objects` field of the share. Some objects need additional configuration after they are added. Refer to Stackable VFS modules (https://www.samba.org/samba/docs/old/Samba3-HOWTO/VFS.html) and the `vfs_*` man pages (https://www.samba.org/samba/docs/current/man-html/) for more details.
Table 13.12: Available VFS Objects

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>audit</td>
<td>Log share access, connects/disconnects, directory opens/creates/removes, and file opens/closes/renames/unlinks/chmods to syslog.</td>
</tr>
<tr>
<td>catia</td>
<td>Improve Mac interoperability by translating characters that are unsupported by Windows.</td>
</tr>
<tr>
<td>crossrename</td>
<td>Allow server side rename operations even if source and target are on different physical devices. Required for the recycle bin to work across dataset boundaries. Automatically added when Export Recycle Bin is enabled.</td>
</tr>
<tr>
<td>dirsort</td>
<td>Sort directory entries alphabetically before sending them to the client.</td>
</tr>
<tr>
<td>fruit</td>
<td>Enhance macOS support by providing the SMB2 AAPL extension and Netatalk interoperability. Automatically loads catia and streams_xattr, but see the warning (page 252) below.</td>
</tr>
<tr>
<td>full_audit</td>
<td>Record selected client operations to the system log.</td>
</tr>
<tr>
<td>ixnas</td>
<td>Improves ACL compatibility with Windows, stores DOS attributes as file flags, optimizes share case sensitivity to improve performance, and enables User Quota Administration (page 255) from Windows. Enabled by default. Several Auxiliary Parameters are available with ixnas. Userspace Quota Settings:</td>
</tr>
<tr>
<td></td>
<td>• ixnas:base_user_quota = sets a ZFS user quota on every user that connects to the share. Example: ixnas:base_user_quota = 80G sets the quota to 80 GiB.</td>
</tr>
<tr>
<td></td>
<td>• ixnas:zfs_quota_enabled = enables support for userspace quotas. Choices are True or False. Default is True. Example: ixnas:zfs_quota_enabled = True.</td>
</tr>
<tr>
<td></td>
<td>Home Dataset Settings:</td>
</tr>
<tr>
<td></td>
<td>• ixnas:chown_homedir = changes the owner of a created home dataset to the currently authenticated user. ixnas:zfs_auto_homedir must be set to True. Choices are True or False. Example: ixnas:chown_homedir = True.</td>
</tr>
<tr>
<td></td>
<td>• ixnas:homendir_quota = sets a quota on new ZFS datasets. ixnas:zfs_auto_homedir must be set to True. Example: ixnas:homendir_quota = 20G sets the quota to 20 GiB.</td>
</tr>
<tr>
<td></td>
<td>• ixnas:zfs_auto_homedir = creates new ZFS datasets for users connecting to home shares instead of folders. Choices are True or False. Default is False. Example: ixnas:zfs_auto_homedir = False.</td>
</tr>
<tr>
<td>media_harmony</td>
<td>Allow Avid editing workstations to share a network drive.</td>
</tr>
<tr>
<td>noacl</td>
<td>Disable NT ACL support. If an extended ACL is present in the share connection, all access to this share will be denied. When the Read-only attribute (<a href="https://www.oreilly.com/openbook/samba/book/ch05_03.html">https://www.oreilly.com/openbook/samba/book/ch05_03.html</a>) is enabled, all access is denied.</td>
</tr>
<tr>
<td>zfs_space</td>
<td>Correctly calculate ZFS space used by the share, including space used by ZFS snapshots, quotas, and reservations.</td>
</tr>
<tr>
<td>zfsacl</td>
<td>Provide ACL extensions for proper integration with ZFS.</td>
</tr>
</tbody>
</table>
Warning: Be careful when using multiple SMB shares, some with and some without fruit. macOS clients negotiate SMB2 AAPL protocol extensions on the first connection to the server, so mixing shares with and without fruit will globally disable AAPL if the first connection occurs without fruit. To resolve this, all macOS clients need to disconnect from all SMB shares and the first reconnection to the server has to be to a fruit-enabled share.

These VFS objects do not appear in the drop-down menu:
- **recycle**: moves deleted files to the recycle directory instead of deleting them. Controlled by `Export Recycle Bin` in the SMB share options (page 247).

Creating or editing an SMB share on a dataset with a trivial Access Control List (ACL) (https://www.ixsystems.com/community/threads/methods-for-fine-tuning-samba-permissions.50739/) prompts to configure the ACL (page 187) for the dataset.

To view all active SMB connections and users, enter `smbstatus` in the Shell (page 341). To log more details for clients that are attempting to authenticate to an SMB share, open the Service → SMB options and add `log level = 1, auth_audit:5` to the Auxiliary Parameters.

### 13.5.1 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.

**Note:** Windows 10, Windows Server 2016 version 1709, and Windows Server 2019 disable SMB2 guest access. Read the Microsoft security notice (https://support.microsoft.com/en-hk/help/4046019/guest-access-in-smb2-disabled-by-default-in-windows-10-and-windows-ser) for details about security vulnerabilities with SMB2 guest access and instructions to re-enable guest logins on these Microsoft systems.

To configure an unauthenticated SMB share:

1. Go to Sharing → Windows (SMB) Shares and click ADD.
2. Fill out the the fields as shown in Figure 13.20.
3. Enable Allow Guest Access.
4. Press SAVE.

**Note:** If a dataset for the share has not been created, refer to Adding Datasets (page 181) to find out more about dataset creation.
The new share appears in Sharing → Windows (SMB) Shares.

By default, users that access the share from an SMB client will not be prompted for a username or password. For example, to access the share from a Windows system, open Explorer and click on Network. In this example, a system named FREENAS appears with a share named p2ds2-smb. The user can copy data to and from this share.

The guest account can be changed by opening the Services → SMB options and selecting a different account from the GuestAccount dropdown.

The guest account can also have an Access Control Entry (ACE) (page 187) that governs the permissions of the guest account to access the different pools and datasets on the system. To change the guest account permissions, edit the dataset Access Control List (ACL) and add a new item with the Who set to User and User set to the account used for guest access (nobody by default). The ACE can then be adjusted to define the access level required for guest sessions. See ACL Management (page 187) for more details about each available setting.

Changing the Guest Account permissions will not grant access for anonymous sessions. This is best accomplished by creating or editing the everyone@ ACE in the dataset ACL. Note that anonymous sessions also do not have the guest SID in the security token.

### 13.5.2 Configuring Authenticated Access With Local Users

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, because there is no domain controller to provide authentication for the network, each user account must 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 user accounts are needed.

To configure authenticated access for an SMB share, first create a group (page 70) for all the SMB user accounts in FreeNAS®. Go to Accounts → Groups and click ADD. Use a descriptive name for the group like local_smb_users. Configure the SMB share dataset with permissions for this new group. When creating a new dataset (page 181), set the Share Type to SMB. After the dataset is created, open the dataset Access Control List (ACL) (page 187) and add a new entry. Set Who to Group and select the SMB group for the Group. Finish defining the permissions (page 190) for the SMB group. Any members of this group (page 70) now have access to the dataset.

Determine which users need authenticated access to the dataset and create new accounts (page 73) in FreeNAS®. It is recommended to use the same username and password from the client system for the associated FreeNAS® user account. Add the SMB group to the Auxiliary Groups list during account creation.

Finally, create the SMB share (page 246). Make sure the Path is pointed to the dataset that has defined permissions for the SMB group and that the SMB (page 277) service is active.

Testing the Share

The authenticated share can be tested from any SMB client. For example, to test an authenticated share from a Windows system with network discovery enabled, open Explorer and click on Network. If network discovery is disabled, open Explorer and enter \HOST in the address bar, where HOST is the IP address or hostname of the share system. This example shows a system named FREENAS with a share named smb_share.

After clicking smb_share, a Windows Security dialog prompts for the username and password of the user associated with smb_share. After authenticating, the user can copy data to and from the SMB share.
Map the share as a network drive to prevent Windows Explorer from hanging when accessing the share. Right-click the share and select *Map network drive...*. Choose a drive letter from the drop-down menu and click *Finish*.

Windows caches user account credentials with the authenticated share. This sometimes prevents connection to a share, even when the correct username and password are provided. Logging out of Windows clears the cache. The authentication dialog reappears the next time the user connects to an authenticated share.

### 13.5.3 User Quota Administration

File Explorer can manage quotas on SMB shares connected to an *Active Directory* (page 204) server. Both the share and dataset being shared must be configured to allow this feature:

- Create an authenticated share with *domain admins* as both the user and group name in *Ownership*.
- Edit the SMB share and add *ixnas* to the list of selected *VFS Object* (page 251).
- In Windows Explorer, connect to and map the share with a user account which is a member of the *domain admins* group. The *Quotas* tab becomes active.

### 13.5.4 Configuring Shadow Copies

[Shadow Copies](https://en.wikipedia.org/wiki/Shadow_copy), also known as the Volume Shadow Copy Service (VSS) or Previous Versions, is a Microsoft service for creating volume snapshots. Shadow copies can be used to restore previous versions of files from within Windows Explorer. Shadow Copy support is built into Vista and Windows 7. Windows XP or 2000 users need to install the [Shadow Copy client](http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=16220).

When a periodic snapshot task is created on a ZFS pool 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 no previous versions of files to restore are visible, use Windows Update to ensure the system is fully up-to-date.
- Shadow copy support only works for ZFS pools or datasets. This means that the SMB share must be configured on a pool or dataset, not on a directory.
- Datasets are filesystems and shadow copies cannot traverse filesystems. To see the shadow copies in the child datasets, create separate shares for them.
- Shadow copies will not work with a manual snapshot. Creating a periodic snapshot task for the pool or dataset being shared by SMB or a recursive task for a parent dataset is recommended.
- 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*.
- Appropriate permissions must be configured on the pool or 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® web interface. 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 With Local Users* (page 253) to create the desired number of shares.

To enable shadow copies, check the *Enable Shadow Copies* setting when creating an *smb share* (page 246).

### 13.6 Creating Authenticated and Time Machine Shares

macOS includes the [Time Machine](https://support.apple.com/en-us/HT201250) feature which performs automatic backups. FreeNAS® supports Time Machine backups for both *SMB* (page 246) and *AFP* (page 217) shares.
The process for creating an authenticated share for a user is the same as creating a Time Machine share for that user.

Create Time Machine or authenticated shares on a **new dataset** (page 181).

Change permissions on the new dataset by going to Storage → Pools. Select the dataset, click  
(Options), Change Permissions.

Enter these settings:

1. **User**: Use the drop-down to select the desired user account. If the user does not yet exist on the FreeNAS® system, create one with Accounts → Users. See users (page 73) for more information.

2. **Group**: Select the desired group name. If the group does not yet exist on the FreeNAS® system, create one with Accounts → Groups. See groups (page 70) for more information.

3. Click SAVE.

Create the authenticated or Time Machine share:

1. Go to Sharing → Windows (SMB) Shares or Sharing → Apple (AFP) Shares and click ADD. Apple deprecated the AFP protocol [https://support.apple.com/en-us/HT207828](https://support.apple.com/en-us/HT207828) and recommends using SMB.

2. **Browse** to the dataset created for the share.

3. When creating a Time Machine share, set the **Time Machine** option.

4. Fill out the other required fields.

5. Click SAVE.

When creating multiple authenticated or Time Machine shares, repeat this process for each user. Figure 13.22 shows creating a Time Machine Share in Sharing → Apple (AFP) Shares.

---

Fig. 13.22: Creating an Authenticated or Time Machine Share
Configuring a quota for each Time Machine share helps prevent backups from using all available space on the FreeNAS® system. Time Machine waits two minutes before creating a full backup. It then creates ongoing hourly, daily, weekly, and monthly backups. The oldest backups are deleted when a Time Machine share fills up, so make sure that the quota size is large enough to hold the desired number of backups. Note that a default installation of macOS is over 20 GiB.


13.6.1 Setting SMB and AFP Share Quotas

**SMB Quota**

Go to Sharing → Windows (SMB) Shares, click ☰ (Options) on the Time Machine share, and Edit. Click Advanced Mode and enter a vfs_fruit(8) (https://www.samba.org/samba/docs/current/man-html/vfs_fruit.8.html) parameter in the Auxiliary Parameters. Time Machine quotas use the fruit:time machine max size parameter. For example, to set a quota of 500 GiB, enter fruit:time machine max size = 500 G.

**AFP Quota**

Go to Sharing → Apple (AFP) Shares, click ☰ (Options) on the Time Machine share, and Edit. In the example shown in Figure 13.23, the Time Machine share name is backup_user1. Enter a value in the TimeMachineQuota field, and click SAVE. In this example, the Time Machine share is restricted to 200 GiB.

![Fig. 13.23: Setting an AFP Share Quota](image-url)
13.6.2 Client Time Machine Configuration

**Note:** The example shown here is intended to show the general process of adding a FreeNAS® share in Time Machine. The example might not reflect the exact process to configure Time Machine on a specific version of macOS. See the Apple documentation (https://support.apple.com/en-us/HT201250) for detailed Time Machine configuration instructions.

To configure Time Machine on the macOS client, go to System Preferences → Time Machine, and click ON in the left panel.

![Fig. 13.24: Configuring Time Machine on macOS](image)

Click *Select Disk...* in the right panel to find the FreeNAS® system with the share. Highlight the share and click *Use Backup Disk*. A connection dialog prompts to log in to the FreeNAS® system.

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](https://community.netgear.com/t5/Stora-Legacy/Solution-to-quot-Time-Machine-could-not-complete-the-backup/td-p/294697).

If Time Machine completed a verification of your backups. To improve reliability, Time Machine must create a new backup for you. *is shown, follow the instructions in this post* (http://www.garth.org/archives/2011,08,27,169,fix-time-machine-sparsebundle-nas-based-backup-errors.html) to avoid making another backup or losing past backups.
Services that ship with FreeNAS® are configured, started, or stopped in Services. FreeNAS® includes these built-in services:

- **AFP** (page 260)
- **Dynamic DNS** (page 262)
- **FTP** (page 263)
- **iSCSI** (page 268)
- **LLDP** (page 268)
- **NFS** (page 269)
- **Rsync** (page 271)
- **S3** (page 274)
- **S.M.A.R.T.** (page 275)
- **SMB** (page 277)
- **SNMP** (page 279)
- **SSH** (page 281)
- **TFTP** (page 284)
- **UPS** (page 285)
- **WebDAV** (page 288)

This section demonstrates starting a FreeNAS® service and the available configuration options for each FreeNAS® service.

### 14.1 Configure Services

The Services page, shown in Figure 14.1, lists all services. The list has options to activate the service, set a service to **Start Automatically** at system boot, and configure a service. 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** (https://en.wikipedia.org/wiki/S.M.A.R.T.). Other services default to **off** until started.
Stopped services show the sliding button on the left. Active services show the sliding button on the right. Click the slider to start or stop a service. Stopping a service shows a confirmation dialog.

**Tip:** Using a proxy server can prevent the list of services from being displayed. If a proxy server is used, do not configure it to proxy local network or websocket connections. VPN software can also cause problems. If the list of services is displayed when connecting on the local network but not when connecting through the VPN, check the VPN software configuration.

Services are configured by clicking 🍏 (Configure).

If a service does not start, go to System → Advanced and enable Show console messages. Console messages appear at the bottom of the browser. Clicking the console message area makes it into a pop-up window, allowing scrolling through or copying the 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 (page 341) and type `more /var/log/messages`.

### 14.2 AFP

The settings that are configured when creating AFP shares in are specific to each configured AFP share. An AFP share is created by navigating to Sharing → Apple (AFP), and clicking ADD. In contrast, global settings which apply to all AFP shares are configured in Services → AFP → Configure.
Figure 14.2 shows the available global AFP configuration options which are described in Table 14.1.

![Global AFP Configuration](image)

**Table 14.1: Global AFP Configuration Options**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest Account</td>
<td>drop-down menu</td>
<td>Select an account to use for guest access. The account must have permissions to the pool or dataset being shared.</td>
</tr>
<tr>
<td>Guest Access</td>
<td>checkbox</td>
<td>If enabled, clients are not prompted to authenticate before accessing AFP shares.</td>
</tr>
<tr>
<td>Max. Connections</td>
<td>integer</td>
<td>Maximum number of simultaneous connections permitted via AFP. The default limit is 50.</td>
</tr>
<tr>
<td>Database Path</td>
<td>browse button</td>
<td>Sets the database information to be stored in the path. Default is the root of the pool. The path must be writable even if the pool is read only.</td>
</tr>
<tr>
<td>Chmod Request</td>
<td>drop-down menu</td>
<td>Set how ACLs are handled. Choices are: <em>Ignore, Preserve, or Simple.</em></td>
</tr>
<tr>
<td>Map ACLs</td>
<td>drop-down menu</td>
<td>Choose mapping of effective permissions for authenticated users: <em>Rights</em> (default, Unix-style permissions), <em>Mode</em> (ACLs), or <em>None</em>.</td>
</tr>
<tr>
<td>Bind Interfaces</td>
<td>selection</td>
<td>Specify the IP addresses to listen for FTP connections. Select the desired IP addresses in the list to add them to the <em>Bind Interfaces</em> list.</td>
</tr>
</tbody>
</table>
14.2.1 Troubleshooting AFP

Check for error messages in /var/log/afp.log.

Determine which users are connected to an AFP share by typing afpusers.

If Something wrong with the volume's CNID DB is shown, run this command from Shell (page 341), replacing the path to the problematic AFP share:

```
dbd -rf /path/to/share
```

This command can take some time, depending upon the size of the pool or dataset being shared. The CNID database is wiped and rebuilt from the CNIDs stored in the AppleDouble files.

14.3 Dynamic DNS

Dynamic DNS (DDNS) is useful if the 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 access to the FreeNAS® system even if the IP address changes. DDNS requires registration with a DDNS service such as DynDNS (https://dyn.com/dns/).

Figure 14.3 shows the DDNS configuration screen and Table 14.2 summarizes the configuration options. The values for these fields are provided by the DDNS provider. After configuring DDNS, remember to start the DDNS service in Services → Dynamic DNS.

![Fig. 14.3: Configuring DDNS](image)
Table 14.2: DDNS Configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider</td>
<td>drop-down menu</td>
<td>Several providers are supported. If a specific provider is not listed, select Custom Provider and enter the information in the Custom Server and Custom Path fields.</td>
</tr>
<tr>
<td>CheckIP Server SSL</td>
<td>checkbox</td>
<td>Use HTTPS for the connection to the CheckIP Server.</td>
</tr>
<tr>
<td>CheckIP Server</td>
<td>string</td>
<td>Name and port of the server that reports the external IP address. For example, entering checkip.dyndns.org:80 uses Dyn IP detection (<a href="https://help.dyn.com/remote-access-api/checkip-tool/">https://help.dyn.com/remote-access-api/checkip-tool/</a>) to discover the remote socket IP address.</td>
</tr>
<tr>
<td>CheckIP Path</td>
<td>string</td>
<td>Path to the CheckIP Server. For example, no-ip.com uses a CheckIP Server of dynamic.zoneedit.com and CheckIP Path of /checkip.html.</td>
</tr>
<tr>
<td>SSL</td>
<td>checkbox</td>
<td>Use HTTPS for the connection to the server that updates the DNS record.</td>
</tr>
<tr>
<td>Custom Server</td>
<td>string</td>
<td>DDNS server name. For example, members.dyndns.org denotes a server similar to dyndns.org.</td>
</tr>
<tr>
<td>Custom Path</td>
<td>string</td>
<td>DDNS server path. Path syntax varies by provider and must be obtained from that provider. For example, /update?hostname= is a simple path for the update.twodns.de Custom Server. The hostname is automatically appended by default. More examples are in the In-A-Dyn documentation (<a href="https://github.com/troglobit/inadyn#custom-ddns-providers">https://github.com/troglobit/inadyn#custom-ddns-providers</a>).</td>
</tr>
<tr>
<td>Domain name</td>
<td>string</td>
<td>Fully qualified domain name of the host with the dynamic IP address. Separate multiple domains with a space, comma (,), or semicolon (;). Example: myname.dyndns.org;myothername.dyndns.org</td>
</tr>
<tr>
<td>Username</td>
<td>string</td>
<td>Username for logging in to the provider and updating the record.</td>
</tr>
<tr>
<td>Password</td>
<td>string</td>
<td>Password for logging in to the provider and updating the record.</td>
</tr>
<tr>
<td>Update period</td>
<td>integer</td>
<td>How often the IP is checked in seconds.</td>
</tr>
</tbody>
</table>

When using the he.net Provider, enter the domain name for Username and enter the DDNS key generated for that domain's A entry at the he.net (https://he.net) website for Password.

14.4 FTP

FreeNAS® uses the proftpd (http://www.proftpd.org/) 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 concerned about sensitive data, see Encrypting FTP (page 268).

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 14.4 shows the configuration screen for Services → FTP → Configure. 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 setting the Show advanced fields by default option in System → Advanced.
Fig. 14.4: Configuring FTP

Table 14.3 summarizes the available options when configuring the FTP server.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>integer</td>
<td></td>
<td>Set the port the FTP service listens on.</td>
</tr>
<tr>
<td>Clients</td>
<td>integer</td>
<td></td>
<td>Maximum number of simultaneous clients.</td>
</tr>
<tr>
<td>Connections</td>
<td>integer</td>
<td></td>
<td>Set the maximum number of connections per IP address. 0 means unlimited.</td>
</tr>
<tr>
<td>Login Attempts</td>
<td>integer</td>
<td></td>
<td>Enter the maximum number of attempts before the client is disconnected.</td>
</tr>
<tr>
<td>Timeout</td>
<td>integer</td>
<td></td>
<td>Maximum client idle time in seconds before client is disconnected.</td>
</tr>
<tr>
<td>Allow Root Login</td>
<td>checkbox</td>
<td></td>
<td>Setting this option is discouraged as it increases security risk.</td>
</tr>
<tr>
<td>Allow Anonymous Login</td>
<td>checkbox</td>
<td></td>
<td>Allow anonymous FTP logins with access to the directory specified in the Path.</td>
</tr>
<tr>
<td>Path</td>
<td>browse button</td>
<td></td>
<td>Set the root directory for anonymous FTP connections.</td>
</tr>
<tr>
<td>Allow Local User Login</td>
<td>checkbox</td>
<td></td>
<td>Allow any local user to log in. By default, only members of the ftp group are allowed to log in.</td>
</tr>
<tr>
<td>Display Login</td>
<td>string</td>
<td></td>
<td>Specify the message displayed to local login users after authentication. Not displayed to anonymous login users.</td>
</tr>
</tbody>
</table>

Continued on next page
### Table 14.3 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Transfer Resumption</td>
<td>checkbox</td>
<td></td>
<td>Set to allow FTP clients to resume interrupted transfers.</td>
</tr>
<tr>
<td>Always Chroot</td>
<td>checkbox</td>
<td></td>
<td>When set a local user is only allowed access to their home directory when they are a member of the wheel group.</td>
</tr>
<tr>
<td>Perform Reverse DNS Lookups</td>
<td>checkbox</td>
<td></td>
<td>Set to perform reverse DNS lookups on client IPs. Can cause long delays if reverse DNS is not configured.</td>
</tr>
<tr>
<td>Masquerade address</td>
<td>string</td>
<td></td>
<td>Public IP address or hostname. Set if FTP clients cannot connect through a NAT device.</td>
</tr>
<tr>
<td>Certificate</td>
<td>drop-down menu</td>
<td></td>
<td>Select the SSL certificate to be used for TLS FTP connections. Go to System → Certificates to create a certificate.</td>
</tr>
<tr>
<td>TLS No Certificate Request</td>
<td>checkbox</td>
<td></td>
<td>Set if the client cannot connect, and it is suspected the client is not properly handling server certificate requests.</td>
</tr>
<tr>
<td>File Permission</td>
<td>checkboxes</td>
<td>✓</td>
<td>Sets default permissions for newly created files.</td>
</tr>
<tr>
<td>Directory Permission</td>
<td>checkboxes</td>
<td>✓</td>
<td>Sets default permissions for newly created directories.</td>
</tr>
<tr>
<td>Enable FXP</td>
<td>checkbox</td>
<td>✓</td>
<td>Set to enable the File eXchange Protocol. This is discouraged as it makes the server vulnerable to FTP bounce attacks.</td>
</tr>
<tr>
<td>Require IDENT Authentication</td>
<td>checkbox</td>
<td>✓</td>
<td>Setting this option results in timeouts if identd is not running on the client.</td>
</tr>
<tr>
<td>Minimum Passive Port</td>
<td>integer</td>
<td>✓</td>
<td>Used by clients in PASV mode, default of 0 means any port above 1023.</td>
</tr>
<tr>
<td>Maximum Passive Port</td>
<td>integer</td>
<td>✓</td>
<td>Used by clients in PASV mode, default of 0 means any port above 1023.</td>
</tr>
<tr>
<td>Local User Upload Bandwidth</td>
<td>integer</td>
<td>✓</td>
<td>Defined in KiB/s, default of 0 means unlimited.</td>
</tr>
<tr>
<td>Local User Download Bandwidth</td>
<td>integer</td>
<td>✓</td>
<td>Defined in KiB/s, default of 0 means unlimited.</td>
</tr>
<tr>
<td>Anonymous User Upload Bandwidth</td>
<td>integer</td>
<td>✓</td>
<td>Defined in KiB/s, default of 0 means unlimited.</td>
</tr>
<tr>
<td>Anonymous User Download Bandwidth</td>
<td>integer</td>
<td>✓</td>
<td>Defined in KiB/s, default of 0 means unlimited.</td>
</tr>
<tr>
<td>Enable TLS</td>
<td>checkbox</td>
<td>✓</td>
<td>Set to enable encrypted connections. Requires a certificate to be created or imported using Certificates (page 116).</td>
</tr>
<tr>
<td>TLS Policy</td>
<td>drop-down menu</td>
<td>✓</td>
<td>The selected policy defines whether the control channel, data channel, both channels, or neither channel of an FTP session must occur over SSL/TLS. The policies are described here (<a href="http://www.proftpd.org/docs/directives/linked/config_ref_TLSRequired.html">http://www.proftpd.org/docs/directives/linked/config_ref_TLSRequired.html</a>).</td>
</tr>
<tr>
<td>TLS Allow Client Renegotiations</td>
<td>checkbox</td>
<td>✓</td>
<td>Setting this option is not recommended as it breaks several security measures. For this and the rest of the TLS fields, refer to mod_tls (<a href="http://www.proftpd.org/docs/contrib/mod_tls.html">http://www.proftpd.org/docs/contrib/mod_tls.html</a>) for more details.</td>
</tr>
<tr>
<td>TLS Allow Dot Login</td>
<td>checkbox</td>
<td>✓</td>
<td>If set, the user home directory is checked for a .tlslogin file which contains one or more PEM-encoded certificates. If not found, the user is prompted for password authentication.</td>
</tr>
<tr>
<td>TLS Allow Per User</td>
<td>checkbox</td>
<td>✓</td>
<td>If set, the user password may be sent unencrypted.</td>
</tr>
<tr>
<td>TLS Common Name Required</td>
<td>checkbox</td>
<td>✓</td>
<td>When set, the common name in the certificate must match the FQDN of the host.</td>
</tr>
</tbody>
</table>

Continued on next page
### Table 14.3 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS Enable Diagnostics</td>
<td>checkbox</td>
<td>✓</td>
<td>If set when troubleshooting a connection, logs more verbosely.</td>
</tr>
<tr>
<td>TLS Export Certificate Data</td>
<td>checkbox</td>
<td>✓</td>
<td>If set, exports the certificate environment variables.</td>
</tr>
<tr>
<td>TLS No Certificate Request</td>
<td>checkbox</td>
<td>✓</td>
<td>Set if the client cannot connect and it is suspected the client is poorly handling the server certificate request.</td>
</tr>
<tr>
<td>TLS No Empty Fragments</td>
<td>checkbox</td>
<td>✓</td>
<td>Setting this option is <strong>not</strong> recommended as it bypasses a security mechanism.</td>
</tr>
<tr>
<td>TLS No Session Reuse Required</td>
<td>checkbox</td>
<td>✓</td>
<td>Setting this option reduces the security of the connection. Only use if the client does not understand reused SSL sessions.</td>
</tr>
<tr>
<td>TLS Export Standard Vars</td>
<td>checkbox</td>
<td>✓</td>
<td>If enabled, sets several environment variables.</td>
</tr>
<tr>
<td>TLS DNS Name Required</td>
<td>checkbox</td>
<td>✓</td>
<td>If set, the client DNS name must resolve to its IP address and the cert must contain the same DNS name.</td>
</tr>
<tr>
<td>TLS IP Address Required</td>
<td>checkbox</td>
<td>✓</td>
<td>If set, the client certificate must contain the IP address that matches the IP address of the client.</td>
</tr>
<tr>
<td>Auxiliary Parameters</td>
<td>string</td>
<td>✓</td>
<td>Used to add proftpd(8) (<a href="https://www.freebsd.org/cgi/man.cgi?query=proftpd">https://www.freebsd.org/cgi/man.cgi?query=proftpd</a>) parameters not covered elsewhere in this screen.</td>
</tr>
</tbody>
</table>

This example demonstrates the auxiliary parameters that prevent all users from performing the FTP DELETE command:

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

### 14.4.1 Anonymous FTP

Anonymous FTP may be appropriate for a small network where the FreeNAS® system is not accessible from the Internet and everyone in the internal network needs easy access to the stored data. Anonymous FTP does not require 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:

1. Give the built-in ftp user account permissions to the pool or dataset to be shared in **Storage → Pools → Edit Permissions**:
   - **User**: select the built-in ftp user from the drop-down menu
   - **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 Unix ACLs are used even if Windows clients are accessing FreeNAS® via FTP.

2. Configure anonymous FTP in **Services → FTP → Configure** by setting these attributes:
   - **Allow Anonymous Login**: set this option
   - **Path**: browse to the pool/dataset/directory to be shared

3. Start the FTP service in **Services**. Click the sliding button on the **FTP row**. The FTP service takes a second or so to start. The sliding button moves to the right when the service is running.
4. Test the connection from a client using a utility such as Filezilla (https://filezilla-project.org/).

In the example shown in Figure 14.5, The user has entered this information into the Filezilla client:

- IP address of the FreeNAS® server: 192.168.1.113
- Username: anonymous
- Password: the email address of the user

![Filezilla Connection](image)

**Fig. 14.5: Connecting Using Filezilla**

The messages within the client indicate the FTP connection is successful. The user can now navigate the contents of the root folder on the remote site. This is the pool or dataset 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).

### 14.4.2 FTP in chroot

If users are required to authenticate before accessing the data on the FreeNAS® system, either create a user account for each user or import existing user accounts using Active Directory (page 204) or LDAP (page 209). Create a ZFS dataset for each user, then chroot each user so 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 a user home directory is limited to the size of the quota.

To configure this scenario:

1. Create a ZFS dataset for each user in Storage → Pools. Click the ![Options] button, then Add Dataset. 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. When Active Directory (page 204) or LDAP (page 209) are not being used, create a user account for each user by navigating to Accounts → Users, and clicking ADD. 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 by navigating to Storage → Pools, and clicking the ![Options] on the desired dataset. Click the Edit Permissions button, then assign a user account as User of that dataset. 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 Unix ACLs are always used, even if Windows clients will be accessing FreeNAS® via FTP.

4. Configure FTP in Services → FTP → Configure with these attributes:

- **Path:** browse to the parent pool containing the datasets.
- Make sure the options for Allow Root Login and Allow Anonymous Login are unselected.
- Select the Allow Local User Login option to enable it.
- Select the Always Chroot option to enable it.
5. Start the FTP service in Services → FTP. Click the sliding button on the FTP row. The FTP service takes a second or so to start. The sliding button moves to the right to show the service is running.

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 is associated with a dataset, and the Password for that user. The messages will indicate 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 pool but the dataset created for that user. The user can transfer files between the local site (their system) and the remote site (their dataset on the FreeNAS® system).

### 14.4.3 Encrypting FTP

To configure any FTP scenario to use encrypted connections:

1. Import or create a certificate authority using the instructions in CAs (page 113). Then, import or create the certificate to use for encrypted connections using the instructions in Certificates (page 116).

2. In Services → FTP → Configure, click ADVANCED, choose the certificate in Certificate, and set the Enable TLS option.

3. Specify secure FTP when accessing the FreeNAS® system. For example, in Filezilla enter 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 SAVE to accept the certificate and negotiate an encrypted connection.

4. To force encrypted connections, select On for the TLS Policy.

### 14.4.4 Troubleshooting FTP

The FTP service will not start if it cannot resolve the system hostname to an IP address with DNS. To see if the FTP service is running, open Shell (page 341) 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, enable Show console messages, and click SAVE. Go to 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 hostname and IP address, or add an entry for the IP address of the FreeNAS® system in the Network → Global Configuration Host name database field.

### 14.5 iSCSI

Refer to Block (iSCSI) (page 222) for instructions on configuring iSCSI. Start the iSCSI service in Services by clicking the sliding button in the iSCSI row.

**Note:** A warning message is shown the iSCSI service stops when initiators are connected. Open the Shell (page 341) and type `ctladm islist` to determine the names of the connected initiators.

### 14.6 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 (https://github.com/sspans/ladvd) LLDP implemen-
tation. If the network contains managed switches, configuring and starting the LLDP service will tell the FreeNAS® system to advertise itself on the network.

Figure 14.6 shows the LLDP configuration screen and Table 14.4 summarizes the configuration options for the LLDP service.

![Configuring LLDP](image)

**Fig. 14.6: Configuring LLDP**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Description</td>
<td>checkbox</td>
<td>Set to enable receive mode and to save and received peer information in interface descriptions.</td>
</tr>
<tr>
<td>Country Code</td>
<td>string</td>
<td>Required for LLDP location support. Enter a two-letter ISO 3166 country code.</td>
</tr>
<tr>
<td>Location</td>
<td>string</td>
<td>Optional. Specify the physical location of the host.</td>
</tr>
</tbody>
</table>

### 14.7 NFS

The settings that are configured when creating NFS shares in are specific to each configured NFS share. An NFS share is created by going to *Sharing → Unix (NFS) Shares* and clicking *ADD*. Global settings which apply to all NFS shares are configured in *Services → NFS → Configure*.

Figure 14.7 shows the configuration screen and Table 14.5 summarizes the configuration options for the NFS service.
Table 14.5: NFS Configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of servers</td>
<td>integer</td>
<td>Specify how many servers to create. Increase if NFS client responses are slow. To limit CPU context switching, keep this number less than or equal to the number of CPUs reported by <code>sysctl -n kern.smp.cpu</code>s.</td>
</tr>
<tr>
<td>Serve UDP NFS clients</td>
<td>checkbox</td>
<td>Set if NFS clients need to use UDP.</td>
</tr>
<tr>
<td>Bind IP Addresses</td>
<td>drop-down</td>
<td>Select IP addresses to listen on for NFS requests. When all options are unset, NFS listens on all available addresses.</td>
</tr>
<tr>
<td>Allow non-root mount</td>
<td>checkbox</td>
<td>Set only if required by the NFS client.</td>
</tr>
<tr>
<td>Enable NFSv4</td>
<td>checkbox</td>
<td>Set to switch from NFSv3 to NFSv4. The default is NFSv3.</td>
</tr>
<tr>
<td>NFSv3 ownership model for NFSv4</td>
<td>checkbox</td>
<td>Grayed out unless <strong>Enable NFSv4</strong> is selected and, in turn, grays out <code>Support&gt;16 groups</code> which is incompatible. Set this option if NFSv4 ACL support is needed without requiring the client and the server to sync users and groups.</td>
</tr>
<tr>
<td>Require Kerberos for NFSv4</td>
<td>checkbox</td>
<td>Set to force NFS shares to fail if the Kerberos ticket is unavailable. Disabling this option allows using either default NFS or Kerberos authentication.</td>
</tr>
</tbody>
</table>

Continued on next page
### 14.8 Rsync

*Services → Rsync* is used to configure an rsync server when using rsync module mode. Refer to *Rsync Module Mode* (page 132) for a configuration example.

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

#### 14.8.1 Configure Rsyncd

To configure the *rsyncd* server, go to *Services* and click ✨ *EDIT* for the *Rsync* service.

---

**Table 14.5 – continued from previous page**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mountd(8) bind port</td>
<td>integer</td>
<td>Optional. Specify the port that <a href="https://www.freebsd.org/cgi/man.cgi?query=mountd">mountd</a> binds to.</td>
</tr>
<tr>
<td>rpc.statd(8) bind port</td>
<td>integer</td>
<td>Optional. Specify the port that <a href="https://www.freebsd.org/cgi/man.cgi?query=rpc.statd">rpc.statd</a> binds to.</td>
</tr>
<tr>
<td>rpc.lockd(8) bind port</td>
<td>integer</td>
<td>Optional. Specify the port that <a href="https://www.freebsd.org/cgi/man.cgi?query=rpc.lockd">rpc.lockd</a> binds to.</td>
</tr>
<tr>
<td>Support &gt;16 groups</td>
<td>checkbox</td>
<td>Set this option if any users are members of more than 16 groups (useful in AD environments). Note this assumes group membership is configured correctly on the NFS server.</td>
</tr>
<tr>
<td>Log mountd(8) requests</td>
<td>checkbox</td>
<td>Enable logging of <a href="https://www.freebsd.org/cgi/man.cgi?query=mountd">mountd</a> requests by syslog.</td>
</tr>
<tr>
<td>Log rpc.statd(8) and rpc.lockd(8) requests by syslog.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** NFSv4 sets all ownership to *nobody:nobody* if user and group do not match on client and server.
Table 14.6 summarizes the configuration options for the rsync daemon:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Port</td>
<td>integer</td>
<td>\texttt{rsyncd} listens on this port. The default is 873.</td>
</tr>
<tr>
<td>Auxiliary parameters</td>
<td>string</td>
<td>Enter any additional parameters from \texttt{rsyncd.conf(5)} (<a href="https://www.freebsd.org/cgi/man.cgi?query=rsyncd.conf">https://www.freebsd.org/cgi/man.cgi?query=rsyncd.conf</a>).</td>
</tr>
</tbody>
</table>

### 14.8.2 Rsync Modules

To add a new Rsync module, go to \textit{Services}, click \textit{EDIT} for the Rsync service, select the \textit{Rsync Module} tab, and click \textit{ADD}.
Table 14.7 summarizes the configuration options available when creating a rsync module.

Table 14.7: Rsync Module Configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>string</td>
<td>Module name that matches the name requested by the rsync client.</td>
</tr>
<tr>
<td>Comment</td>
<td>string</td>
<td>Describe this module.</td>
</tr>
<tr>
<td>Path</td>
<td>file browser</td>
<td>Browse to the pool or dataset to store received data.</td>
</tr>
<tr>
<td>Access Mode</td>
<td>drop-down menu</td>
<td>Choose permissions for this rsync module.</td>
</tr>
<tr>
<td>Maximum connections</td>
<td>integer</td>
<td>Maximum connections to this module. 0 is unlimited.</td>
</tr>
<tr>
<td>User</td>
<td>drop-down menu</td>
<td>User to run as during file transfers to and from this module.</td>
</tr>
<tr>
<td>Group</td>
<td>drop-down menu</td>
<td>Group to run as during file transfers to and from this module.</td>
</tr>
<tr>
<td>Hosts Allow</td>
<td>string</td>
<td>From rsyncd.conf(5) (<a href="https://www.freebsd.org/cgi/man.cgi?query=rsyncd.conf">https://www.freebsd.org/cgi/man.cgi?query=rsyncd.conf</a>). A list of patterns to match with the hostname and IP address of a connecting client. The connection is rejected if no patterns match. Separate patterns with whitespace or a comma.</td>
</tr>
<tr>
<td>Hosts Deny</td>
<td>string</td>
<td>From rsyncd.conf(5) (<a href="https://www.freebsd.org/cgi/man.cgi?query=rsyncd.conf">https://www.freebsd.org/cgi/man.cgi?query=rsyncd.conf</a>). A list of patterns to match with the hostname and IP address of a connecting client. The connection is rejected when the patterns match. Separate patterns with whitespace or a comma.</td>
</tr>
</tbody>
</table>
14.9 S3

S3 is a distributed or clustered filesystem protocol compatible with Amazon S3 cloud storage. The FreeNAS® S3 service uses Minio (https://minio.io/) to provide S3 storage hosted on the FreeNAS® system itself. Minio also provides features beyond the limits of the basic Amazon S3 specifications.

Figure 14.10 shows the S3 service configuration screen and Table 14.8 summarizes the configuration options. After configuring the S3 service, start it in Services.

![Fig. 14.10: Configuring S3](image)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>drop-down menu</td>
<td>Enter the IP address to run the S3 service. 0.0.0.0 sets the server to listen on all addresses.</td>
</tr>
<tr>
<td>Port</td>
<td>string</td>
<td>Enter the TCP port on which to provide the S3 service. Default is 9000.</td>
</tr>
<tr>
<td>Access Key</td>
<td>string</td>
<td>Enter the S3 access ID. See Access keys (<a href="https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html#access-keys-and-secret-access-keys">https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html#access-keys-and-secret-access-keys</a>) for more information.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>string</td>
<td>Enter the S3 secret access key. See Access keys (<a href="https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html#access-keys-and-secret-access-keys">https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html#access-keys-and-secret-access-keys</a>) for more information.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 14.8 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm Secret Key</td>
<td>string</td>
<td>Re-enter the S3 password to confirm.</td>
</tr>
<tr>
<td>Disk</td>
<td>browse</td>
<td>Directory where the S3 filesystem will be mounted. Ownership of this directory and all subdirectories is set to <code>minio:minio</code>. Create a separate dataset (page 181) for Minio to avoid issues with conflicting directory permissions or ownership.</td>
</tr>
<tr>
<td>Enable Browser</td>
<td>checkbox</td>
<td>Set to enable the web user interface for the S3 service. Access the minio web interface by entering the IP address and port number separated by a colon in the browser address bar.</td>
</tr>
<tr>
<td>Certificate</td>
<td>drop-down menu</td>
<td>Add the SSL certificate (page 116) to be used for secure S3 connections.</td>
</tr>
</tbody>
</table>

14.10 S.M.A.R.T.

S.M.A.R.T., or Self-Monitoring, Analysis, and Reporting Technology (https://en.wikipedia.org/wiki/S.M.A.R.T.), is an industry standard for disk monitoring and testing. Drives can be monitored for status and problems, and several types of self-tests can be run to check the drive health.

Tests run internally on the drive. Most tests can run at the same time as normal disk usage. However, a running test can greatly reduce drive performance, so they should be scheduled at times when the system is not busy or in normal use. It is very important to avoid scheduling disk-intensive tests at the same time. For example, do not schedule S.M.A.R.T. tests to run at the same time, or preferably, even on the same days as Scrub Tasks (page 149).

Of particular interest in a NAS environment are the Short and Long S.M.A.R.T. tests. Details vary between drive manufacturers, but a Short test generally does some basic tests of a drive that takes a few minutes. The Long test scans the entire disk surface, and can take several hours on larger drives.

FreeNAS® uses the smartd(8) (https://www.smartmontools.org/browser/trunk/smartmontools/smartd.8.in) service to monitor S.M.A.R.T. information, including disk temperature. A complete configuration consists of:

2. Enabling or disabling S.M.A.R.T. for each disk member of a pool in `Storage → Pools`. This setting is enabled by default for disks that support S.M.A.R.T.
3. Checking the configuration of the S.M.A.R.T. service as described in this section.

Figure 14.11 shows the configuration screen that appears after going to `Services → S.M.A.R.T` and clicking ☑ (Configure).
Note: smartd wakes up at the configured Check Interval. It checks the times configured in Tasks → S.M.A.R.T. Tests to see if a test must begin. Since the smallest time increment for a test is an hour, 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 smartd only activates every two hours.

Table 14.9 summarizes the options in the S.M.A.R.T configuration screen.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Interval</td>
<td>integer</td>
<td>Define in minutes how often smartd activates to check if any tests are configured to run.</td>
</tr>
<tr>
<td>Power Mode</td>
<td>drop-down menu</td>
<td>Tests are only performed when Never is selected. Choices are: Never, Sleep, Standby, or Idle.</td>
</tr>
<tr>
<td>Difference</td>
<td>integer in degrees Celsius</td>
<td>Enter number of degrees in Celsius. S.M.A.R.T reports if the temperature of a drive has changed by N degrees Celsius since the last report. Default of 0 disables this option.</td>
</tr>
<tr>
<td>Informational</td>
<td>integer in degrees Celsius</td>
<td>Enter a threshold temperature in Celsius. S.M.A.R.T will message with a log level of LOG_INFO if the temperature is higher than the threshold. Default of 0 disables this option.</td>
</tr>
<tr>
<td>Critical</td>
<td>integer in degrees Celsius</td>
<td>Enter a threshold temperature in Celsius. S.M.A.R.T will message with a log level of LOG_CRIT and send an email if the temperature is higher than the threshold. Default of 0 disables this option.</td>
</tr>
</tbody>
</table>
14.11 SMB

Note: After starting the SMB service, it can take several minutes for the master browser election (https://www.samba.org/samba/docs/old/Samba3-HOWTO/NetworkBrowsing.html#id2581357) to occur and for the FreeNAS® system to become available in Windows Explorer.

Figure 14.12 shows the global configuration options which apply to all SMB shares. This configuration screen displays the configurable options from smb4.conf (https://www.freebsd.org/cgi/man.cgi?query=smb4.conf). These options are described in Table 14.10.

![Fig. 14.12: Global SMB Configuration](image)

### Table 14.10: Global SMB Configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetBIOS Name</td>
<td>string</td>
<td>Automatically populated with the original hostname of the system. Limited to 15 characters. It must be different from the Workgroup name.</td>
</tr>
<tr>
<td>NetBIOS Alias</td>
<td>string</td>
<td>Enter any aliases, separated by spaces. Each alias cannot be longer than 15 characters.</td>
</tr>
<tr>
<td>Workgroup</td>
<td>string</td>
<td>Must match the Windows workgroup name. This setting is ignored if the Active Directory (page 204) or LDAP (page 209) service is running.</td>
</tr>
<tr>
<td>Description</td>
<td>string</td>
<td>Enter a server description. Optional.</td>
</tr>
</tbody>
</table>
Table 14.10 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SMB1 support</td>
<td>checkbox</td>
<td>Allow legacy SMB clients to connect to the server. <strong>Warning:</strong> SMB1 is not secure and has been deprecated by Microsoft. See <a href="https://www.ixsystems.com/blog/library/do-not-use-smb1/">Do Not Use SMB1</a>.</td>
</tr>
<tr>
<td>UNIX Charset</td>
<td>drop-down menu</td>
<td>Default is <strong>UTF-8</strong> which supports all characters in all languages.</td>
</tr>
<tr>
<td>Log Level</td>
<td>drop-down menu</td>
<td>Choices are <strong>Minimum</strong>, <strong>Normal</strong>, or <strong>Debug</strong>.</td>
</tr>
<tr>
<td>Use syslog only</td>
<td>checkbox</td>
<td>Set to log authentication failures in <code>/var/log/messages</code> instead of the default of <code>/var/log/samba4/log.smbd</code>.</td>
</tr>
<tr>
<td>Local Master</td>
<td>checkbox</td>
<td>Set to determine if the system participates in a browser election. Disable when network contains an AD or LDAP server or Vista or Windows 7 machines are present.</td>
</tr>
<tr>
<td>Guest Account</td>
<td>drop-down menu</td>
<td>Account to be used for guest access. Default is <em>nobody</em>. The chosen account is required to have permissions to the shared pool or dataset. To adjust permissions, edit the dataset Access Control List (ACL), add a new entry for the chosen guest account, and configure the permissions in that entry. If the selected Guest Account is deleted the field resets to <em>nobody</em>.</td>
</tr>
<tr>
<td>Administrators Group</td>
<td>drop-down menu</td>
<td>Members of this group are local admins and automatically have privileges to take ownership of any file in an SMB share, reset permissions, and administer the SMB server through the Computer Management MMC snap-in.</td>
</tr>
<tr>
<td>Auxiliary Parameters</td>
<td>string</td>
<td>Enter additional <a href="https://www.freebsd.org/cgi/man.cgi?query=smb.conf">smb.conf</a> options. See the <a href="http://www.oreilly.com/openbook/samba/book/appb_02.html">Samba Guide</a> for more information on the available settings. To log more details when a client attempts to authenticate to the share, add <code>log level = 1, auth_audit:5</code>.</td>
</tr>
<tr>
<td>Zeroconf share</td>
<td>checkbox</td>
<td>Enable if Mac clients will be connecting to the SMB share.</td>
</tr>
<tr>
<td>discovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTLMv1 Auth</td>
<td>checkbox</td>
<td>Set to allow NTLMv1 authentication. Required by Windows XP clients and sometimes by clients in later versions of Windows.</td>
</tr>
<tr>
<td>Bind IP Addresses</td>
<td>checkboxes</td>
<td>Static IP addresses which SMB listens on for connections. Leaving all unselected defaults to listening on all active interfaces.</td>
</tr>
<tr>
<td>Range Low</td>
<td>integer</td>
<td>Range Low and Range High set the range of UID/GID numbers which this IDMap backend translates. If an external credential like a Windows SID maps to a UID or GiD number outside this range, the external credential is ignored.</td>
</tr>
<tr>
<td>Range High</td>
<td>integer</td>
<td></td>
</tr>
</tbody>
</table>

Changes to SMB settings take effect immediately. Changes to share settings only take effect after the client and server negotiate a new session.

**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 (page 277) cannot be disabled while Active Directory (page 204) is enabled.

### 14.11.1 Troubleshooting SMB

Connecting to SMB shares as root, and adding the root user in the SMB user database is not recommended. 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.

Windows automatically caches file sharing information. If changes are made to an SMB share or to the permissions of a pool or dataset being shared by SMB and the share becomes inaccessible, log out and back in to 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. To require users to log in every time they access the system, 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 (https://www.oreilly.com/openbook/samba/book/ch05_04.html) explains in more detail.

If the SMB service will not start, run this command from Shell (page 341) to see if there is an error in the configuration:

```
 testparm /usr/local/etc/smb4.conf
```

Using a dataset for SMB sharing is recommended. When creating the dataset, make sure that the Share type is set to SMB.

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 use the ACL manager (page 187).


Directory listing speed in folders with a large number of files is sometimes a problem. A few specific changes can help improve the performance. However, changing these settings can affect other usage. In general, the defaults are adequate. Do not change these settings unless there is a specific need.

- *LogLevel* can also have a performance penalty. When not needed, it can be disabled or reduced in the global SMB service options (page 277).
- Create as SMB-style dataset and enable the *ixnas* auxiliary parameter
- Disable as many *VFS Objects* as possible in the *share settings* (page 247). Many have performance overhead.

## 14.12 SNMP

SNMP (Simple Network Management Protocol) is used to monitor network-attached devices for conditions that warrant administrative attention. FreeNAS® uses Net-SNMP (http://net-snmp.sourceforge.net/) to provide SNMP. When starting the SNMP service, this 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 14.13 shows the Services → SNMP → Configure screen. Table 14.11 summarizes the configuration options.
Fig. 14.13: Configuring SNMP

Table 14.11: SNMP Configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>string</td>
<td>Enter the location of the system.</td>
</tr>
<tr>
<td>Contact</td>
<td>string</td>
<td>Enter an email address to receive messages from the SNMP service.</td>
</tr>
<tr>
<td>Community</td>
<td>string</td>
<td>Change from public to increase system security. Can only contain alphanumeric characters, underscores, dashes, periods, and spaces. This can be left empty for SNMPv3 networks.</td>
</tr>
<tr>
<td>Username</td>
<td>string</td>
<td>Only applies if SNMP v3 Support is set. Enter a username to register with this service.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>drop-down menu</td>
<td>Only applies if SNMP v3 Support is enabled. Choices are MD5 or SHA.</td>
</tr>
<tr>
<td>Password</td>
<td>string</td>
<td>Only applies if SNMP v3 Support is enabled. Enter and confirm a password of at least eight characters.</td>
</tr>
<tr>
<td>Privacy Protocol</td>
<td>drop-down menu</td>
<td>Only applies if SNMP v3 Support is enabled. Choices are AES or DES.</td>
</tr>
<tr>
<td>Privacy Passphrase</td>
<td>string</td>
<td>Enter a separate privacy passphrase. Password is used when this is left empty.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 14.11 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auxiliary Par-</td>
<td>string</td>
<td>Enter additional snmpd.conf(5) (<a href="https://www.freebsd.org/cgi/man.cgi?query=snmpd.conf">https://www.freebsd.org/cgi/man.cgi?query=snmpd.conf</a>) options. Add one option for each line.</td>
</tr>
<tr>
<td>rameters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expose zilstat</td>
<td>checkbox</td>
<td>Enabling this option may have pool performance implications.</td>
</tr>
<tr>
<td>via SNMP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log Level</td>
<td>drop-down menu</td>
<td>Choose how many log entries to create. Choices range from the least log entries (Emergency) to the most (Debug).</td>
</tr>
</tbody>
</table>


### 14.13 SSH

Secure Shell (SSH) is used to transfer files securely over an encrypted network. When a FreeNAS® system is used as an SSH server, the users in the network must use SSH client software (https://en.wikipedia.org/wiki/Comparison_of_SSH_clients) 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 14.14 shows the Services → SSH → Configure screen.

**Note:** After configuring SSH, remember to start it in Services by clicking the sliding button in the SSH row. The sliding button moves to the right when the service is running.
Table 14.12 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 enabling the Show advanced fields by default option in System → Advanced.

Table 14.12: SSH Configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind interfaces</td>
<td>selection</td>
<td>✓</td>
<td>By default, SSH listens on all interfaces unless specific interfaces are selected in this drop-down menu.</td>
</tr>
<tr>
<td>TCP port</td>
<td>integer</td>
<td></td>
<td>Port to open for SSH connection requests. 22 by default.</td>
</tr>
<tr>
<td>Log in as root with password</td>
<td>checkbox</td>
<td></td>
<td><strong>As a security precaution, root logins are discouraged and disabled by default.</strong> If enabled, password must be set for the root user in Users.</td>
</tr>
<tr>
<td>Allow password authentication</td>
<td>checkbox</td>
<td></td>
<td>Unset to require key-based authentication for all users. This requires additional setup (<a href="http://the.earth.li/~sgtatham/putty/0.55/htmldoc/Chapter8.html">http://the.earth.li/~sgtatham/putty/0.55/htmldoc/Chapter8.html</a>) on both the SSH client and server.</td>
</tr>
<tr>
<td>Allow kerberos authentication</td>
<td>checkbox</td>
<td>✓</td>
<td>Ensure Kerberos Realms (page 213) and Kerberos Keytabs (page 214) are configured and FreeNAS® can communicate with the Kerberos Domain Controller (KDC) before enabling this option.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 14.12 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Advanced Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow TCP port forwarding</td>
<td>checkbox</td>
<td></td>
<td>Set to allow users to bypass firewall restrictions using the SSH port forwarding feature (<a href="https://www.symantec.com/connect/articles/ssh-port-forwarding">https://www.symantec.com/connect/articles/ssh-port-forwarding</a>).</td>
</tr>
<tr>
<td>Compress connections</td>
<td>checkbox</td>
<td></td>
<td>Set to attempt to reduce latency over slow networks.</td>
</tr>
<tr>
<td>SFTP log level</td>
<td>drop-down menu</td>
<td>✓</td>
<td>Select the syslog(3) (<a href="https://www.freebsd.org/cgi/man.cgi?query=syslog">https://www.freebsd.org/cgi/man.cgi?query=syslog</a>) level of the SFTP server.</td>
</tr>
<tr>
<td>SFTP log facility</td>
<td>drop-down menu</td>
<td>✓</td>
<td>Select the syslog(3) (<a href="https://www.freebsd.org/cgi/man.cgi?query=syslog">https://www.freebsd.org/cgi/man.cgi?query=syslog</a>) facility of the SFTP server.</td>
</tr>
<tr>
<td>Extra options</td>
<td>string</td>
<td>✓</td>
<td>Add any additional sshd_config(5) (<a href="https://www.freebsd.org/cgi/man.cgi?query=sshd_config">https://www.freebsd.org/cgi/man.cgi?query=sshd_config</a>) options not covered in this screen, one per line. These options are case-sensitive and misspellings can prevent the SSH service from starting.</td>
</tr>
</tbody>
</table>

Here are some recommendations for the Extra options:

- Add NoneEnabled no to disable the insecure none cipher.
- Increase the ClientAliveInterval if SSH connections tend to drop.
- ClientMaxStartup defaults to 10. Increase this value when more concurrent SSH connections are required.

### 14.13.1 SCP Only

When SSH is configured, authenticated users with a user account can use ssh to log into the FreeNAS® system over the network. User accounts are created by navigating to Accounts → Users, and clicking ADD. The user home directory is the pool or dataset specified in the Home Directory field of the FreeNAS® account for that user. While the SSH login defaults to the user home directory, users are able to navigate outside their home directory, which can pose a security risk.

It is possible to allow users to use scp and sftp 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 Accounts → Users, click ☰ (Options) for the user, and then Edit. Change the Shell to scponly. Repeat for each user that needs restricted SSH access.

Test the configuration from another system by running the sftp, ssh, and scp commands as the user. sftp and scp will work but ssh will fail.

Note: Some utilities like WinSCP and Filezilla can bypass the scponly shell. This section assumes users are accessing the system using the command line versions of scp and sftp.

### 14.13.2 Troubleshooting SSH

Keywords listed in sshd_config(5) (https://www.freebsd.org/cgi/man.cgi?query=sshd_config) are case sensitive. This is important to remember when adding any Extra options. The configuration will not function as intended if the upper and lowercase letters of the keyword are not an exact match.

If 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 the configuration as an SSH user account to ensure the user is limited by the configuration and they have permission to transfer files within the intended directories. If the user account is experiencing problems, the SSH error messages are specific in describing the problem. Type this command within Shell (page 341) to read these messages as they occur:

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

Additional messages regarding authentication errors are found in `/var/log/auth.log`.

### 14.14 TFTP

Trivial File Transfer Protocol (TFTP) is a light-weight version of FTP typically used to transfer configuration or boot files between machines, such as routers, in a local environment. TFTP provides an extremely limited set of commands and provides no authentication.

If the FreeNAS® system will be used to store images and configuration files for network devices, configure and start the TFTP service. Starting the TFTP service opens UDP port 69.

Figure 14.15 shows the TFTP configuration screen and Table 14.13 summarizes the available options.
### Table 14.13: TFTP Configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>Browse button</td>
<td>Browse to an <strong>existing</strong> directory to be used for storage. Some devices require a specific directory name, refer to the device documentation for details.</td>
</tr>
<tr>
<td>Allow New Files</td>
<td>checkbox</td>
<td>Set when network devices need to send files to the system. For example, to back up their configuration.</td>
</tr>
<tr>
<td>Host</td>
<td>IP address</td>
<td>The default host to use for TFTP transfers. Enter an IP address. Example: 192.0.2.1.</td>
</tr>
<tr>
<td>Port</td>
<td>integer</td>
<td>The UDP port number that listens for TFTP requests. Example: 8050.</td>
</tr>
<tr>
<td>Username</td>
<td>drop-down menu</td>
<td>Select the account to use for TFTP requests. This account must have permission to the <strong>Directory</strong>.</td>
</tr>
<tr>
<td>File Permissions</td>
<td>checkboxes</td>
<td>Set permissions for newly created files. The default is everyone can read and only the owner can write. Some devices require less strict permissions.</td>
</tr>
<tr>
<td>Extra options</td>
<td>string</td>
<td>Add more options from <strong>tftpd(8)</strong> <a href="https://www.freebsd.org/cgi/man.cgi?query=tftpd">https://www.freebsd.org/cgi/man.cgi?query=tftpd</a> Add one option on each line.</td>
</tr>
</tbody>
</table>

### 14.15 UPS

FreeNAS® uses **NUT** [https://networkupstools.org/](https://networkupstools.org/) (Network UPS Tools) to provide UPS support. If the FreeNAS® system is connected to a UPS device, configure the UPS service in **Services → UPS → Configure**.

**Figure 14.16** shows the UPS configuration screen:
Table 14.14 summarizes the options in the UPS Configuration screen.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPS Mode</td>
<td>drop-down menu</td>
<td>Select <em>Master</em> if the UPS is plugged directly into the system serial port. The UPS will remain the last item to shut down. Select <em>Slave</em> to have the system shut down before <em>Master</em>.</td>
</tr>
<tr>
<td>Identifier</td>
<td>string</td>
<td>Required. Describe the UPS device. Can contain alphanumeric, period, comma, hyphen, and underscore characters.</td>
</tr>
<tr>
<td>Driver / Remote Host</td>
<td>combo-box</td>
<td>Required. For a list of supported devices, see the Network UPS Tools compatibility list (<a href="https://networkupstools.org/stable-hcl.html">https://networkupstools.org/stable-hcl.html</a>). The field suggests drivers based on the text entered. To search for a specific driver, begin typing the name of the driver. The search is case sensitive. The <em>Driver</em> field changes to <em>Remote Host</em> when <em>UPS Mode</em> is set to <em>Slave</em>. Enter the IP address of the system configured as the UPS <em>Master</em> system. See this post (<a href="https://forums.freenas.org/index.php?resources/configuring-ups-support-for-single-or-multiple-freenas-servers.30/">https://forums.freenas.org/index.php?resources/configuring-ups-support-for-single-or-multiple-freenas-servers.30/</a>) for more details about configuring multiple systems with a single UPS.</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port or Hostname</td>
<td>drop-down menu</td>
<td>Serial or USB port connected to the UPS. To automatically detect and manage the USB port settings, open the drop-down menu and select <code>auto</code>. If the specific USB port must be chosen, see this note (page 287) about identifying the USB port used by the UPS. When an SNMP driver is selected, enter the IP address or hostname of the SNMP UPS device. Port or Hostname becomes Remote Port when the UPS Mode is set to Slave. Enter the open network port number of the UPS Master system. The default port is 3493.</td>
</tr>
<tr>
<td>Auxiliary Parameters (ups.conf)</td>
<td>string</td>
<td>Enter any additional options from <code>ups.conf(5)</code> (<a href="https://www.freebsd.org/cgi/man.cgi?query=ups.conf">https://www.freebsd.org/cgi/man.cgi?query=ups.conf</a>).</td>
</tr>
<tr>
<td>Description</td>
<td>string</td>
<td>Optional. Describe the UPS service.</td>
</tr>
<tr>
<td>Shutdown Mode</td>
<td>drop-down menu</td>
<td>Choose when the UPS initiates shutdown. Choices are <code>UPS goes on battery</code> and <code>UPS reaches low battery</code>.</td>
</tr>
<tr>
<td>Shutdown Timer</td>
<td>integer</td>
<td>Select a value in seconds for the UPS to wait before initiating shutdown. Shutdown will not occur if the power is restored while the timer is counting down. This value only applies when Shutdown Mode is set to <code>UPS goes on battery</code>.</td>
</tr>
<tr>
<td>Shutdown Command</td>
<td>string</td>
<td>Enter the command to run to shut down the computer when battery power is low or shutdown timer runs out.</td>
</tr>
<tr>
<td>No Communication Warning Time</td>
<td>string</td>
<td>Enter a value in seconds to wait before alerting that the service cannot reach any UPS. Warnings continue until the situation is fixed.</td>
</tr>
<tr>
<td>Monitor User</td>
<td>string</td>
<td>Required. Enter a user to associate with this service. The recommended default user is <code>upsmon</code>.</td>
</tr>
<tr>
<td>Monitor Password</td>
<td>string</td>
<td>Required. Default is the known value <code>fixmepass</code>. Change this to enhance system security. Cannot contain a space or <code>#</code>.</td>
</tr>
<tr>
<td>Extra Users</td>
<td>string</td>
<td>Enter accounts that have administrative access. See <code>upsd.users(5)</code> (<a href="https://www.freebsd.org/cgi/man.cgi?query=upsd.users">https://www.freebsd.org/cgi/man.cgi?query=upsd.users</a>) for examples.</td>
</tr>
<tr>
<td>Remote Monitor</td>
<td>checkbox</td>
<td>Set for the default configuration to listen on all interfaces using the known values of user: <code>upsmon</code> and password: <code>fixmepass</code>.</td>
</tr>
<tr>
<td>Send Email Status Updates</td>
<td>checkbox</td>
<td>Set to enables the FreeNAS® system to send email updates to the configured Email field.</td>
</tr>
<tr>
<td>Email</td>
<td>email address</td>
<td>Enter any email addresses to receive status updates. Separate multiple addresses with a semicolon (;).</td>
</tr>
<tr>
<td>Email Subject</td>
<td>string</td>
<td>Enter a subject line for email status updates.</td>
</tr>
<tr>
<td>Power Off UPS</td>
<td>checkbox</td>
<td>Set for the UPS to power off after shutting down the FreeNAS® system.</td>
</tr>
<tr>
<td>Host Sync</td>
<td>integer</td>
<td>Enter a time in seconds for <code>UPSMON(8)</code> (<a href="https://www.freebsd.org/cgi/man.cgi?query=upsmon">https://www.freebsd.org/cgi/man.cgi?query=upsmon</a>) to wait in master mode for the slaves to disconnect during a shutdown.</td>
</tr>
</tbody>
</table>

**Note:** For USB devices, the easiest way to determine the correct device name is to enable the `Show console messages` option in `System → Advanced`. Plug in the USB device and look for a `/dev/ugen` or `/dev/uhid` device name in the console messages.

Some UPS models might be unresponsive with the default polling frequency. This can show in FreeNAS® logs as a recurring error like: `libusb_get_interrupt: Unknown error`. If this error occurs, decrease the polling frequency by adding an entry to `Auxiliary Parameters (ups.conf)`: 287
pollinterval = 10. The default polling frequency is two seconds.

upsc(8) (https://www.freebsd.org/cgi/man.cgi?query=upsc) 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 (page 341) using this syntax:

```
upsc ups@localhost
```

The upsc(8) (https://www.freebsd.org/cgi/man.cgi?query=upsc) man page gives some other usage examples.

upscmd(8) (https://www.freebsd.org/cgi/man.cgi?query=upscmd) can be used to send commands directly to the UPS, assuming the hardware supports the command being sent. Only users with administrative rights can use this command. These users are created in the Extra users field.

### 14.15.1 Multiple Computers with One UPS

A UPS with adequate capacity can power multiple computers. One computer is connected to the UPS data port with a serial or USB cable. This *master* makes UPS status available on the network for other computers. These *slave* computers are powered by the UPS, but receive UPS status data from the master computer. See the NUT User Manual (https://networkupstools.org/docs/user-manual.chunked/index.html) and NUT User Manual Pages (https://networkupstools.org/docs/man/index.html#User_man).

### 14.16 WebDAV

The WebDAV service can be configured to provide a file browser over a web connection. Before starting this service, at least one WebDAV share must be created by navigating to Sharing → WebDAV Shares, and clicking ADD. Refer to WebDAV Shares (page 244) for instructions on how to create a share and connect to it after the service is configured and started.

The settings in the WebDAV service apply to all WebDAV shares. Figure 14.17 shows the WebDAV configuration screen. Table 14.15 summarizes the available options.
### Fig. 14.17: WebDAV Configuration Screen

### Table 14.15: WebDAV Configuration Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>drop-down menu</td>
<td>HTTP keeps the connection unencrypted. HTTPS encrypts the connection. HTTP+HTTPS allows both types of connections.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>string</td>
<td>Specify a port for unencrypted connections. The default port 8080 is recommended. Do not use a port number already being used by another service.</td>
</tr>
<tr>
<td>HTTPS Port</td>
<td>string</td>
<td>Specify a port for encrypted connections. The default port 8081 is recommended. Do not use a port number already being used by another service.</td>
</tr>
<tr>
<td>Webdav SSL Certificate</td>
<td>drop-down menu</td>
<td>Select the SSL certificate to be used for encrypted connections. To create a certificate, use System → Certificates.</td>
</tr>
<tr>
<td>HTTP Authentication</td>
<td>drop-down menu</td>
<td>Choices are No Authentication, Basic Authentication (unencrypted) or Digest Authentication (encrypted).</td>
</tr>
<tr>
<td>Webdav Password</td>
<td>string</td>
<td>Default is davtest. Change this password as it is a known value.</td>
</tr>
</tbody>
</table>
FreeNAS® provides the ability to extend the built-in NAS services by providing two methods for installing additional software.

Plugins (page 290) allow the user to browse, install, and configure pre-packaged software from the web interface. This method is easy to use, but provides a limited amount of available software. Each plugin is automatically installed into its own limited FreeBSD jail (https://en.wikipedia.org/wiki/Freebsd_jail) that cannot install additional software.

Jails (page 301) provide more control over software installation, but requires working from the command line and a good understanding of networking basics and software installation on FreeBSD-based systems.

Look through the Plugins (page 290) and Jails (page 301) sections to become familiar with the features and limitations of each. Choose the method that best meets the needs of the application.

Note: Jail Storage (page 301) must be configured before plugins are available on FreeNAS®. This means having a suitable pool (page 168) created to store plugins.

15.1 Installing Plugins

A plugin is a self-contained application installer designed to integrate into the FreeNAS® web interface. A plugin offers several advantages:

- the FreeNAS® web interface provides a browser for viewing the list of available plugins
- the FreeNAS® web interface provides buttons for installing, starting, managing, and uninstalling plugins
- if the plugin has configuration options, a management screen is added to the FreeNAS® web interface for these options to be configured

View available plugins by clicking Plugins.

Figure 15.1 shows some of the available plugins.
Note: If the list of available plugins is not displayed, open Shell (page 341) and verify that the FreeNAS® system can ping an address on the Internet. If it cannot, add a default gateway address and DNS server address in Network → Global Configuration.

Click Browse a Collection to toggle the plugins list between ixsystems plugins (https://www.freenas.org/plugins/), which receive updates every few weeks, and Community plugins (https://github.com/ix-plugin-hub/iocage-plugin-index).

Click REFRESH INDEX to refresh the current list of plugins.

Click a plugin icon to see the description, whether it is an Official or Community plugin, the version available, and the number of installed instances.

To install the selected plugin, click INSTALL.
Enter a jail Name. A unique name is required, since multiple installations of the same plugin are supported. Names can contain letters, numbers, periods (.), dashes (-), and underscores (_).

Most plugins default to NAT. This setting is recommended as it does not require manual configuration of multiple available IP addresses and prevents addressing conflicts on the network.

Some plugins default to DHCP as their management utility conflicts with NAT. Keep these plugins set to DHCP unless manually configuring an IP address is preferred.

If both NAT and DHCP are unset, an IPv4 or IPv6 address can be manually entered. If desired, an IPv4 or IPv6 interface can be selected. If no interface is selected the jail IP address uses the current active interface. The IPv4 or IPv6 address must be in the range of the local network.

Click ADVANCED PLUGIN INSTALLATION to show all options for the plugin jail. The options are described in Advanced Jail Creation (page 304).

To start the installation, click SAVE.

Depending on the size of the application, the installation can take several minutes to download and install. A confirmation message is shown when the installation completes, along with any post-installation notes.

Installed plugins appear on the Plugins page as shown in Figure 15.3.

Note: Plugins are also added to Jails as a pluginv2 jail. This type of jail is editable like a standard jail, but the UUID
cannot be altered. See *Managing Jails* (page 312) for more details about modifying jails.

Plugins are immediately started after installation. By default, all plugins are started when the system boots. Un-setting *Boot* means the plugin will not start when the system boots and must be started manually.

In addition to the *Jail* name, the *Columns* menu can be used to display more information about installed Plugins. More information such as *RELEASE* and *VERSION* is shown by clicking > (Expand). Options to *RESTART, STOP, UPDATE, MANAGE, and UNINSTALL* the plugin are also displayed. If an installed plugin has notes, the notes can be viewed by clicking *POST INSTALL NOTES*.

Plugins with additional documentation also have a *DOCUMENTATION* button which opens the README in the plugin repository.

The plugin must be started before the installed application is available. Click > (Expand) and *START*. The plugin *Status* changes to *up* when it starts successfully.

Stop and immediately start an *up* plugin by clicking > (Expand) and *RESTART*.

Click > (Expand) and *MANAGE* to open a management or configuration screen for the application. Plugins with a management interface show the IP address and port to that page in the *Admin Portal* column.

**Note:** Not all plugins have a functional management option. See *Managing Jails* (page 312) for more instructions about interacting with a plugin jail with the shell.

Some plugins have options that need to be set before their service will successfully start. Check the website of the
If the application requires access to the data stored on the FreeNAS® system, click the entry for the associated jail in the **Jails** page and add storage as described in **Additional Storage** (page 316).

Click **(Options)** and **Shell** for the plugin jail in the **Jails** page. This will give access to the shell of the jail containing the application to complete or test the configuration.

If a plugin jail fails to start, open the plugin jail shell from the **Jail** page and type `tail /var/log/messages` to see if any errors were logged.

### 15.2 Updating Plugins

When a newer version of a plugin or release becomes available in the official repository, click **(Expand)** and **UPDATE**. Updating a plugin updates the operating system and version of the plugin.

![Fig. 15.4: Updating a Plugin](image)

Updating a plugin also restarts that plugin. To update or upgrade the plugin jail operating system, see **Jail Updates and Upgrades** (page 314).

### 15.3 Uninstalling Plugins

Installing a plugin creates an associated jail. Uninstalling a plugin deletes the jail because it is no longer required. This means all datasets or snapshots that are associated with the plugin are also deleted. Make sure to back
up any important data from the plugin before uninstalling it.

Figure 15.5 shows an example of uninstalling a plugin by expanding the plugin's entry and clicking UNINSTALL. A two-step dialog opens to confirm the action. **This is the only warning.** Enter the plugin name, set the Confirm checkbox, and click DELETE to remove the plugin and the associated jail, dataset, and snapshots.

![Fig. 15.5: Uninstalling a Plugin and its Associated Jail and Dataset](image)

### 15.4 Create a Plugin

If an application is not available as a plugin, it is possible to create a new plugin for FreeNAS® in a few steps. This requires an existing GitHub (https://github.com) account.

**Create a new artifact repository on GitHub (https://github.com).**

Refer to table 15.1 for the files to add to the artifact repository.

<table>
<thead>
<tr>
<th>Directory/File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>post_install.sh</td>
<td>This script is run inside the jail after it is created and any packages installed. Enable services in /etc/rc.conf that need to start with the jail and apply any configuration customizations with this script.</td>
</tr>
<tr>
<td>ui.json</td>
<td>JSON file that accepts the key or value options. For example: adminportal: &quot;http://%%IP%%/&quot; designates the web-interface of the plugin.</td>
</tr>
<tr>
<td>Directory/File</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>overlay/</td>
<td>Directory of files overlaid on the jail after install. For example, <code>usr/local/bin/myfile</code> is placed in the <code>/usr/local/bin/myfile</code> location of the jail. Can be used to supply custom files and configuration data, scripts, and any other type of customized files to the plugin jail.</td>
</tr>
</tbody>
</table>
| settings.json  | JSON file that manages the settings interface of the plugin. Required fields include:  
  - "servicerestart": "service foo restart"  
    Command to run when restarting the plugin service after changing settings.  
  - "serviceget": "/usr/local/bin/myget"  
    Command used to get values for plugin configuration. Provided by the plugin creator. The command accepts two arguments for key or value pair.  
  - "options":  
    This subsection contains arrays of elements, starting with the “key” name and required arguments for that particular type of setting.  
    See `options subsection example` (page 296) below.  

This example `settings.json` file is used for the `Quasselcore` plugin. It is also available online in the `iocage-plugin-quassel` artifact repository (https://github.com/freenas/iocage-plugin-quassel/blob/master/settings.json).

```json
{
    "servicerestart": "service quasselcore restart",
    "serviceget": "/usr/local/bin/quasselget",
    "serviceset": "/usr/local/bin/quasselset",
    "options": {
        "adduser": {
            "type": "add",
            "name": "Add User",
            "description": "Add new quasselcore user",
            "requiredargs": {
                "username": {
                    "type": "string",
                    "description": "Quassel Client Username"
                },
                "password": {
                    "type": "password",
                    "description": "Quassel Client Password"
                },
                "fullname": {
                    "type": "string",
                    "description": "Quassel Client Full Name"
                }
            },
            "optionalargs": {
                "adminuser": {
                    "type": "bool",
                    "description": "Can this user administrate quasselcore?"
                }
            }
        },
        "port": {
            "type": "int",
            "name": "Quassel Core Port",
            "description": "Port for incoming quassel connections",
            "range": "1024-32000",
            "default": "4242",
            "requirerestart": true
        }
    }
}
```
Create and submit a new JSON file for the plugin:

Clone the iocage-plugin-index (https://github.com/ix-plugin-hub/iocage-plugin-index) GitHub repository.

Tip: Full tutorials and documentation for GitHub and git commands are available on GitHub Guides (https://guides.github.com/).

On the local copy of iocage-plugin-index, create a new JSON file for the FreeNAS® plugin. The JSON file describes the plugin, the packages it requires for operation, and other installation details. This file is named pluginname.json. For example, the Madsonic (https://github.com/ix-plugin-hub/iocage-plugin-index/blob/master/madsonic.json) plugin is named madsonic.json.

The fields of the file are described in table 15.2.

<table>
<thead>
<tr>
<th>Data Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;name&quot;:</td>
<td>Name of the plugin.</td>
</tr>
<tr>
<td>&quot;plugin_schema&quot;:</td>
<td>Optional. Enter 2 if simplified post-install information has been supplied in post_install.sh. After specifying 2, echo the information to be presented to the user in /root/PLUGIN_INFO inside the post_install.sh file. See the rslsync.json (page 298) and rslsync post_install.sh (page 298) examples.</td>
</tr>
<tr>
<td>&quot;release&quot;:</td>
<td>FreeBSD RELEASE to use for the plugin jail.</td>
</tr>
<tr>
<td>&quot;artifact&quot;:</td>
<td>URL of the plugin artifact repository.</td>
</tr>
<tr>
<td>&quot;pkgs&quot;:</td>
<td>The FreeBSD packages required by the plugin.</td>
</tr>
<tr>
<td>&quot;packagesite&quot;:</td>
<td>Content Delivery Network (CDN) used by the plugin jail. Default for the TrueOS CDN is <a href="http://pkg.cdn.trueos.org/iocage">http://pkg.cdn.trueos.org/iocage</a>.</td>
</tr>
</tbody>
</table>
Table 15.2 – continued from previous page

<table>
<thead>
<tr>
<th>Data Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;fingerprints&quot;:</td>
<td>&quot;function&quot;: Default is sha256. &quot;fingerprint&quot;: The pkg fingerprint for the artifact repository. Default is 226efd3a126fb86e71d60a37353d17f57af816d1c7ecad0623c21f0bf73eb0c7</td>
</tr>
<tr>
<td>&quot;official&quot;:</td>
<td>Define whether this is an official iXsystems-supported plugin. Enter true or false.</td>
</tr>
</tbody>
</table>

Listing 15.1: rslsync.json

```json
{
  "name": "rslsync",
  "plugin_schema": "2",
  "release": "11.2-RELEASE",
  "artifact": "https://github.com/freenas/iocage-plugin-btsync.git",
  "pkgs": [
    "net-p2p/rslsync"
  ],
  "packagesite": "http://pkg.cdn.trueos.org/iocage/unstable",
  "fingerprints": {
    "iocage-plugins": [
      {
        "function": "sha256",
        "fingerprint": "226efd3a126fb86e71d60a37353d17f57af816d1c7ecad0623c21f0bf73eb0c7"
      }
    ],
    "official": true
  }
}
```

Listing 15.2: post_install.sh

```bash
#!/bin/sh -x

# Enable the service
sysrc -f /etc/rc.conf rslsync_enable="YES"
# Start the service
service rslsync start 2>/dev/null

echo "rslsync now installed" > /root/PLUGIN_INFO

Here is quasselcore.json reproduced as an example:

```json
{
  "name": "Quasselcore",
  "release": "11.1-RELEASE",
  "artifact": "https://github.com/freenas/iocage-plugin-quassel.git",
  "pkgs": [
    "irc/quassel-core"
  ],
  "packagesite": "http://pkg.cdn.trueos.org/iocage",
  "fingerprints": {
    "iocage-plugins": [
      {
        "function": "sha256",
        "fingerprint": "226efd3a126fb86e71d60a37353d17f57af816d1c7ecad0623c21f0bf73eb0c7"
      }
    ]
  }
}
```
The correct directory and package name of the plugin application must be used for the "pkgs": value. Find the package name and directory by searching FreshPorts (https://www.freshports.org/) and checking the “To install the port:” line. For example, the Quasselcore plugin uses the directory and package name /irc/quassel-core.

Now edit iocage-plugin-index/INDEX. Add an entry for the new plugin that includes these fields:

- "MANIFEST": Add the name of the newly created plugin.json file here.
- "name": Use the same name used within the .json file.
- "icon": Most plugins will have a specific icon. Search the web and save the icon to the iocage-plugin-index/icons/ directory as a .png. The naming convention is pluginname.png. For example, the Madsonic plugin has the icon file madsonic.png.
- "description": Describe the plugin in a single sentence.
- "official": Specify if the plugin is supported by iXsystems. Enter false.

See the INDEX (https://github.com/ix-plugin-hub/iocage-plugin-index/blob/master/INDEX) for examples of INDEX entries.

Submit the plugin

Open a pull request for the iocage-plugin-index repo (https://github.com/ix-plugin-hub/iocage-plugin-index). Make sure the pull request contains:

- the new plugin.json file.
- the plugin icon .png added to the iocage-plugin-index/icons/ directory.
- an update to the INDEX file with an entry for the new plugin.
- a link to the artifact repository populated with all required plugin files.

15.4.1 Test a Plugin

Warning: Installing experimental plugins is not recommended for general use of FreeNAS®. This feature is meant to help plugin creators test their work before it becomes generally available on FreeNAS®.

Plugin pull requests are merged into the master branch of the iocage-plugin-index (https://github.com/ix-plugin-hub/iocage-plugin-index) repository. These plugins are not available in the web interface until they are tested and added to a RELEASE branch of the repository. It is possible to test an in-development plugin by using this iocage command:

```
iocage fetch -P --name PLUGIN IPADDRESS_PROPS --branch 'master'
```

This will install the plugin, configure it with any chosen properties, and specifically use the master branch of the repository to download the plugin.

Here is an example of downloading and configuring an experimental plugin with the FreeNAS® Shell:

```
[root@freenas ~]# iocage fetch -P --name mineos ip4_addr="em0|10.231.1.37/24" --branch 'master'
Plugin: mineos
  Official Plugin: False
  Using RELEASE: 11.2-RELEASE
  Using Branch: master
  Post-install Artifact: https://github.com/jseqaert/iocage-plugin-mineos.git
These pkgs will be installed:
...
```
This plugin appears in the \textit{Jails} and \textit{Plugins} screens as \texttt{mineos} and can be tested with the FreeNAS\textsuperscript{®} system.

\section*{15.5 Asigra Plugin}

The Asigra plugin connects FreeNAS\textsuperscript{®} to a third party service and is subject to licensing. Please read the \texttt{Asigra Software License Agreement} (https://www.asigra.com/legal/software-license-agreement) before using this plugin.

To begin using Asigra services after installing the plugin, open the plugin options and click \texttt{Register}. A new browser tab opens to register a user with Asigra (https://licenseportal.asigra.com/licenseportal/user-registration.do).

The FreeNAS\textsuperscript{®} system must have a public static IP address for Asigra services to function.

Refer to the Asigra documentation for details about using the Asigra platform:


- \texttt{DS-Client Installation Guide} (https://s3.amazonaws.com/asigra-documentation/Guides/Cloud%20Backup/v14.1/Client_Software_Installation_Guide.pdf): How to install the \texttt{DS-Client} system. \texttt{DS-Client} aggregates backup content from endpoints and transmits it to the \texttt{DS-System} service.

- \texttt{DS-Client Management Guide} (https://s3.amazonaws.com/asigra-documentation/Help/v14.1/DS-Client%20Help/index.html): Managing the \texttt{DS-Client} system after it has been successfully installed at one or more locations.
Jails are a lightweight, operating-system-level virtualization. One or multiple services can run in a jail, isolating those services from the host FreeNAS® system. FreeNAS® uses iocage for jail and plugin management. The main differences between a user-created jail and a plugin are that plugins are preconfigured and usually provide only a single service.

By default, jails run the FreeBSD operating system. These jails are independent instances of FreeBSD. The jail uses the host hardware and runs on the host kernel, avoiding most of the overhead usually associated with virtualization. The jail installs FreeBSD software management utilities so FreeBSD packages or ports can be installed from the jail command line. This allows for FreeBSD ports to be compiled and FreeBSD packages to be installed from the command line of the jail.

It is important to understand that users, groups, installed software, and configurations within a jail are isolated from both the FreeNAS® host operating system and any other jails running on that system.

The ability to create multiple jails offers flexibility regarding software management. For example, an administrator can choose to provide application separation by installing different applications in each jail, to create one jail for all installed applications, or to mix and match how software is installed into each jail.

### 16.1 Jail Storage

A pool must be created before using jails or Plugins. Make sure the pool has enough storage for all the intended jails and plugins. The Jails screen displays a message and button to CREATE POOL if no pools exist on the FreeNAS® system.

If pools exist, but none have been chosen for use with jails or plugins, a dialog appears to choose a pool. Select a pool and click CHOOSE.

To select a different pool for jail and plugin storage, click (Settings). A dialog shows the active pool. A different pool can be selected from the drop-down.

Jails and downloaded FreeBSD release files are stored in a dataset named iocage/.

Notes about the iocage/ dataset:

- At least 10 GiB of free space is recommended.
- Cannot be located on a Share.
- iocage automatically uses the first pool that is not a root pool for the FreeNAS® system.
- A defaults.json file contains default settings used when a new jail is created. The file is created automatically if not already present. If the file is present but corrupted, iocage shows a warning and uses default settings from memory.
- Each new jail installs into a new child dataset of iocage/. For example, with the iocage/jails dataset in pool1, a new jail called jail1 installs into a new dataset named pool1/iocage/jails/jail1.
FreeBSD releases are fetched as a child dataset into the /iocage/download dataset. This dataset is then extracted into the /iocage/releases dataset to be used in jail creation. The dataset in /iocage/download can then be removed without affecting the availability of fetched releases or an existing jail.

iocage/ datasets on activated pools are independent of each other and do not share any data.

**Note:** iocage jail configs are stored in /mnt/poolname/iocage/jails/jailname. When iocage is updated, the config.json configuration file is backed up as /mnt/poolname/iocage/jails/jailname/config_backup.json. The backup file can be renamed to config.json to restore previous jail settings.

### 16.2 Creating Jails

FreeNAS® has two options to create a jail. The **Jail Wizard** makes it easy to quickly create a jail. **ADVANCED JAIL CREATION** is an alternate method, where every possible jail option is configurable. There are numerous options spread across four different primary sections. This form is recommended for advanced users with very specific requirements for a jail.

#### 16.2.1 Jail Wizard

New jails can be created quickly by going to jails → ADD. This opens the wizard screen shown in Figure 16.1.

![Fig. 16.1: Jail Creation Wizard](image)

The wizard provides the simplest process to create and configure a new jail.
Enter a **Jail Name**. Names can contain letters, numbers, periods (.), dashes (–), and underscores (_).

Choose a **Jail Type**: *Default (Clone Jail)* or *Basejail*. Clone jails are clones of the specified FreeBSD RELEASE. They are linked to that RELEASE, even if they are upgraded. Basejails mount the specified RELEASE directories as nullfs mounts over the jail directories. Basejails are not linked to the original RELEASE when upgraded.

Jails can run FreeBSD versions up to the same version as the host FreeNAS® system. Newer releases are not shown.

**Tip:** Versions of FreeBSD are downloaded the first time they are used in a jail. Additional jails created with the same version of FreeBSD are created faster because the download has already been completed.

Click **NEXT** to see a simplified list of networking options. Jails support several different networking solutions:

- **VNET** can be set to add a virtual network interface to the jail. This interface can be used to set NAT, DHCP, or static jail network configurations. Since VNET provides the jail with an independent networking stack, it can broadcast an IP address, which is required by some applications.

- The jail can use **Network Address Translation (NAT)** ([https://en.wikipedia.org/wiki/Network_address_translation](https://en.wikipedia.org/wiki/Network_address_translation)), which uses the FreeNAS® IP address and sets a unique port for the jail to use. VNET is required when NAT is selected.

- Configure the jail to receive its IP address from a DHCP server by setting **DHCP Autoconfigure IPv4**.

- Networking can be manually configured by entering values for the **IPv4 Address** or **IPv6 Address** fields. Any combination of these fields can be configured. Multiple interfaces are supported for IPv4 and IPv6 addresses. To add more interfaces and addresses, click **ADD**. Setting the **IPv4 Default Router** and **IPv6 Default Router** fields to **auto** automatically configures these values. VNET must be set to enable the IPv4 Default Router field. If no interface is selected when manually configuring IP addresses, FreeNAS® automatically assigns the given IP address of the jail to the current active interface of the host system.

- Leaving all checkboxes unset and fields empty initializes the jail without any networking abilities. Networking can be added to the jail after creation by going to **Jails → ▼ (Expand) → EDIT → Basic Properties**.

Setting a proxy in the FreeNAS® **network settings** (page 157) also configures new jails to use the proxy settings, except when performing DNS lookups. Make sure a firewall is properly configured to maximize system security.

When pairing the jail with a physical interface, edit the **network interface** (page 159) and set **Disable Hardware Offloading**. This prevents a network interface reset when the jail starts.
16.2.2 Advanced Jail Creation

The advanced jail creation form is opened by clicking **Jails → ADD** then **Advanced Jail Creation**. The screen in Figure 16.3 is shown.

Click **NEXT** to view a summary screen of the chosen jail options. Click **SUBMIT** to create the new jail. After a few moments, the new jail is added to the primary jails list.
A usable jail can be quickly created by setting only the required values, the *Jail Name* and *Release*. Additional settings are in the *Jail Properties*, *Network Properties*, and *Custom Properties* sections. Table 16.1 shows the available options of the *Basic Properties* of a new jail.

### Table 16.1: Basic Properties

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>string</td>
<td>Required. Can contain letters, numbers, periods (.), dashes (−), and underscores (_).</td>
</tr>
<tr>
<td>Jail Type</td>
<td>drop-down</td>
<td><em>Default (Clone Jail)</em> are clones of the specified RELEASE. They are linked to that RELEASE, even if they are upgraded. <em>Basejail</em> mount the specified RELEASE directories as nullfs mounts over the jail directories. Basejails are not linked to the original RELEASE when upgraded.</td>
</tr>
<tr>
<td>Release</td>
<td>drop-down menu</td>
<td>Required. Jails can run FreeBSD versions up to the same version as the host FreeNAS® system. Newer releases are not shown.</td>
</tr>
<tr>
<td>DHCP Autoconfigure IPv4</td>
<td>checkbox</td>
<td>Automatically configure IPv4 networking with an independent VNET stack. <em>VNET</em> and <em>Berkeley Packet Filter</em> must also be checked. If not set, ensure the defined address in <em>IPv4 Address</em> does not conflict with an existing address.</td>
</tr>
</tbody>
</table>

Continued on next page
### Table 16.1 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NAT</strong></td>
<td>checkbox</td>
<td>Network Address Translation (NAT). When set, the jail is given an internal IP address and connections are forwarded from the host to the jail. When NAT is set, <em>Berkeley Packet Filter</em> cannot be set. Adds the <em>NAT Port Forwarding</em> options to the jail <em>Network Properties</em> (page 310).</td>
</tr>
<tr>
<td><strong>VNET</strong></td>
<td>checkbox</td>
<td>Use VNET to emulate network devices for this jail and create a fully virtualized per-jail network stack. See <em>VNET(9)</em> (<a href="https://www.freebsd.org/cgi/man.cgi?query=vnet">https://www.freebsd.org/cgi/man.cgi?query=vnet</a>) for more details.</td>
</tr>
<tr>
<td><strong>Berkeley Packet Filter</strong></td>
<td>checkbox</td>
<td>Use the Berkeley Packet Filter to data link layers in a protocol independent fashion. Unset by default to avoid security vulnerabilities. See <em>BPF(4)</em> (<a href="https://www.freebsd.org/cgi/man.cgi?query=bpf">https://www.freebsd.org/cgi/man.cgi?query=bpf</a>) for more details. Cannot be set when <em>NAT</em> is set.</td>
</tr>
<tr>
<td><strong>vnet_default_interface</strong></td>
<td>drop-down</td>
<td>Set the default VNET interface. Only takes effect when <em>VNET</em> is set. Choose a specific interface, or set to <em>auto</em> to use the interface that has the default route. Choose <em>none</em> to not set a default VNET interface.</td>
</tr>
<tr>
<td><strong>IPv4 Interface</strong></td>
<td>drop-down menu</td>
<td>Choose a network interface to use for this IPv4 connection. See <em>note</em> (page ??) to add more.</td>
</tr>
<tr>
<td><strong>IPv4 Address</strong></td>
<td>string</td>
<td>This and the other IPv4 settings are grayed out if <em>DHCP autoconfigure IPv4</em> is set. Configures the interface to use for network or internet access for the jail. Enter an IPv4 address for this IP jail. Example: 192.168.0.10. See <em>note</em> (page ??) to add more.</td>
</tr>
<tr>
<td><strong>IPv4 Netmask</strong></td>
<td>drop-down menu</td>
<td>Choose a subnet mask for this IPv4 Address.</td>
</tr>
<tr>
<td><strong>IPv4 Default Router</strong></td>
<td>string</td>
<td>Type <em>none</em> or a valid IP address. Setting this property to anything other than <em>none</em> configures a default route inside a VNET jail.</td>
</tr>
<tr>
<td><strong>Auto Configure IPv6</strong></td>
<td>checkbox</td>
<td>Set to use SLAAC (Stateless Address Auto Configuration) to autoconfigure IPv6 in the jail.</td>
</tr>
<tr>
<td><strong>IPv6 Interface</strong></td>
<td>drop-down menu</td>
<td>Choose a network interface to use for this IPv6 connection. See <em>note</em> (page ??) to add more.</td>
</tr>
<tr>
<td><strong>IPv6 Address</strong></td>
<td>string</td>
<td>Configures network or internet access for the jail. Type the IPv6 address for VNET and shared IP jails. Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334. See <em>note</em> (page ??) to add more.</td>
</tr>
<tr>
<td><strong>IPv6 Prefix</strong></td>
<td>drop-down menu</td>
<td>Choose a prefix for this IPv6 Address.</td>
</tr>
<tr>
<td><strong>IPv6 Default Router</strong></td>
<td>string</td>
<td>Type <em>none</em> or a valid IP address. Setting this property to anything other than <em>none</em> configures a default route inside a VNET jail.</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td>string</td>
<td>Enter any notes or comments about the jail.</td>
</tr>
<tr>
<td><strong>Auto-start</strong></td>
<td>checkbox</td>
<td>Start the jail at system startup.</td>
</tr>
</tbody>
</table>

**Note:** For static configurations not using DHCP or NAT, multiple IPv4 and IPv6 addresses and interfaces can be added to the jail by clicking *ADD*.

Similar to the *Jail Wizard* (page 302), configuring the basic properties, then clicking *SAVE* is often all that is needed to quickly create a new jail. To continue configuring more settings, click *NEXT* to proceed to the *Jail Properties* section of the form. *Table 16.2* describes each of these options.
Table 16.2: Jail Properties

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>devfs_ruleset</td>
<td>integer</td>
<td>Number of the <code>devfs(8)</code> (<a href="https://www.freebsd.org/cgi/man.cgi?query=devfs">https://www.freebsd.org/cgi/man.cgi?query=devfs</a>) ruleset to enforce when mounting <code>devfs</code> in the jail. The default value of 0 means no ruleset is enforced. Mounting <code>devfs</code> inside a jail is only possible when the <code>allow_mount</code> and <code>allow_mount_devfs</code> permissions are enabled and <code>enforce_statfs</code> is set to a value lower than 2.</td>
</tr>
<tr>
<td>exec.start</td>
<td>string</td>
<td>Commands to run in the jail environment when a jail is created. Example: <code>sh /etc/rc</code>. See <code>jail(8)</code> (<a href="https://www.freebsd.org/cgi/man.cgi?query=jail">https://www.freebsd.org/cgi/man.cgi?query=jail</a>) for more details.</td>
</tr>
<tr>
<td>exec.stop</td>
<td>string</td>
<td>Commands to run in the jail environment before a jail is removed and after any <code>exec_prestop</code> commands are complete. Example: <code>sh /etc/rc.shutdown</code>.</td>
</tr>
<tr>
<td>exec_prestart</td>
<td>string</td>
<td>Commands to run in the system environment before a jail is started.</td>
</tr>
<tr>
<td>exec_poststart</td>
<td>string</td>
<td>Commands to run in the system environment after a jail is started and after any <code>exec_start</code> commands are finished.</td>
</tr>
<tr>
<td>exec_prestop</td>
<td>string</td>
<td>Commands to run in the system environment before a jail is stopped.</td>
</tr>
<tr>
<td>exec_poststop</td>
<td>string</td>
<td>Commands to run in the system environment after a jail is started and after any <code>exec_start</code> commands are finished.</td>
</tr>
<tr>
<td>exec_clean</td>
<td>checkbox</td>
<td>Run commands in a clean environment. The current environment is discarded except for <code>$HOME</code>, <code>$SHELL</code>, <code>$TERM</code> and <code>$USER</code>. <code>$HOME</code> and <code>$SHELL</code> are set to the target login. <code>$USER</code> is set to the target login. <code>$TERM</code> is imported from the current environment. The environment variables from the login class capability database for the target login are also set.</td>
</tr>
<tr>
<td>exec_timeout</td>
<td>integer</td>
<td>The maximum amount of time in seconds to wait for a command to complete. If a command is still running after the allotted time, the jail is terminated.</td>
</tr>
<tr>
<td>stop_timeout</td>
<td>integer</td>
<td>The maximum amount of time in seconds to wait for the jail processes to exit after sending a SIGTERM signal. This happens after any <code>exec_stop</code> commands are complete. After the specified time, the jail is removed, killing any remaining processes. If set to 0, no SIGTERM is sent and the jail is immediately removed.</td>
</tr>
<tr>
<td>exec_jail_user</td>
<td>string</td>
<td>Enter either <code>root</code> or a valid <code>username</code>. Inside the jail, commands run as this user.</td>
</tr>
<tr>
<td>exec_system_jail_user</td>
<td>string</td>
<td>Set to <code>True</code> to look for the <code>exec.jail_user</code> in the system <code>passwd(5)</code> (<a href="https://www.freebsd.org/cgi/man.cgi?query=passwd">https://www.freebsd.org/cgi/man.cgi?query=passwd</a>) file instead of the jail <code>passwd</code>.</td>
</tr>
<tr>
<td>exec_system_user</td>
<td>string</td>
<td>Run commands in the jail as this user. By default, commands are run as the current user.</td>
</tr>
<tr>
<td>mount_devfs</td>
<td>checkbox</td>
<td>Mount a <code>devfs(5)</code> (<a href="https://www.freebsd.org/cgi/man.cgi?query=devfs">https://www.freebsd.org/cgi/man.cgi?query=devfs</a>) filesystem on the chrooted <code>/dev</code> directory and apply the ruleset in the <code>devfs_ruleset</code> parameter to restrict the devices visible inside the jail.</td>
</tr>
</tbody>
</table>
Table 16.2 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enforce_statfs</td>
<td>drop-down</td>
<td>Determine which information processes in a jail are able to obtain about mount points. The behavior of multiple syscalls is affected: statfs(2), fstatfs(2), getfsstat(2), fhstatfs(2), and other similar compatibility syscalls. All mount points are available without any restrictions if this is set to 0. Only mount points below the jail chroot directory are available if this is set to 1. Set to 2, the default option only mount points where the jail chroot directory is located are available.</td>
</tr>
<tr>
<td>children_max</td>
<td>integer</td>
<td>Number of child jails allowed to be created by the jail or other jails under this jail. A limit of 0 restricts the jail from creating child jails. Hierarchical jails in the jail(8) man page explains the finer details.</td>
</tr>
<tr>
<td>login_flags</td>
<td>string</td>
<td>Flags to pass to login(1) when logging in to the jail using the console function.</td>
</tr>
<tr>
<td>securelevel</td>
<td>integer</td>
<td>Value of the jail securelevel (<a href="https://www.freebsd.org/doc/faq/security.html">https://www.freebsd.org/doc/faq/security.html</a>) sysctl. A jail never has a lower securelevel than the host system. Setting this parameter allows a higher securelevel. If the host system securelevel is changed, jail securelevel will be at least as secure. Securelevel options are: 3, 2 (default), 1, 0, and -1.</td>
</tr>
<tr>
<td>sysvmsg</td>
<td>drop-down</td>
<td>Allow or deny access to SYSV IPC message primitives. Set to Inherit: All IPC objects on the system are visible to the jail. Set to New: Only objects the jail created using the private key namespace are visible. The system and parent jails have access to the jail objects but not private keys. Set to Disable: The jail cannot perform any sysvmsg related system calls.</td>
</tr>
<tr>
<td>sysvsem</td>
<td>drop-down</td>
<td>Allow or deny access to SYSV IPC semaphore primitives. Set to Inherit: All IPC objects on the system are visible to the jail. Set to New: Only objects the jail creates using the private key namespace are visible. The system and parent jails have access to the jail objects but not private keys. Set to Disable: The jail cannot perform any sysvsem related system calls.</td>
</tr>
<tr>
<td>sysvshm</td>
<td>drop-down</td>
<td>Allow or deny access to SYSV IPC shared memory primitives. Set to Inherit: All IPC objects on the system are visible to the jail. Set to New: Only objects the jail creates using the private key namespace are visible. The system and parent jails have access to the jail objects but not private keys. Set to Disable: The jail cannot perform any sysvshm related system calls.</td>
</tr>
<tr>
<td>allow_set_hostname</td>
<td>checkbox</td>
<td>Allow the jail hostname to be changed with hostname(1) or sethostname(3) (<a href="https://www.freebsd.org/cgi/man.cgi?query=hostname">https://www.freebsd.org/cgi/man.cgi?query=hostname</a>) or sethostname(3).</td>
</tr>
<tr>
<td>allow_sysvipc</td>
<td>checkbox</td>
<td>Choose whether a process in the jail has access to System V IPC primitives. Equivalent to setting sysvmsg, sysvsem, and sysvshm to Inherit. Deprecated in FreeBSD 11.0 and later! Use sysvmsg, sysvsem, and sysvshm instead.</td>
</tr>
</tbody>
</table>
Table 16.2 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow_raw_sockets</td>
<td>checkbox</td>
<td>Allow the jail to use raw sockets (<a href="https://en.wikipedia.org/wiki/Network_socket#Raw_socket">https://en.wikipedia.org/wiki/Network_socket#Raw_socket</a>). When set, the jail has access to lower-level network layers. This allows utilities like ping(<a href="https://www.freebsd.org/cgi/man.cgi?query=ping">https://www.freebsd.org/cgi/man.cgi?query=ping</a>) and traceroute(<a href="https://www.freebsd.org/cgi/man.cgi?query=traceroute">https://www.freebsd.org/cgi/man.cgi?query=traceroute</a>) to work in the jail, but has security implications and should only be used on jails running trusted software.</td>
</tr>
<tr>
<td>allow_chflags</td>
<td>checkbox</td>
<td>Treat jail users as privileged and allow the manipulation of system file flags. <code>securelevel</code> constraints are still enforced.</td>
</tr>
<tr>
<td>allow_mlock</td>
<td>checkbox</td>
<td>Allow jail to run services that use mlock(<a href="https://www.freebsd.org/cgi/man.cgi?query=mlock">https://www.freebsd.org/cgi/man.cgi?query=mlock</a>) to lock physical pages in memory.</td>
</tr>
<tr>
<td>allow_mount</td>
<td>checkbox</td>
<td>Allow privileged users inside the jail to mount and unmount filesystem types marked as jail-friendly.</td>
</tr>
<tr>
<td>allow_mount_devfs</td>
<td>checkbox</td>
<td>Allow privileged users inside the jail to mount and unmount the devfs(5) device filesystem (<a href="https://www.freebsd.org/cgi/man.cgi?query=devfs">https://www.freebsd.org/cgi/man.cgi?query=devfs</a>). This permission is only effective when <code>allow_mount</code> is set and <code>enforce_statfs</code> is set to a value lower than 2.</td>
</tr>
<tr>
<td>allout_mount_fusefs</td>
<td>checkbox</td>
<td>Allow privileged users inside the jail to mount and unmount fusefs. The jail must have FreeBSD 12.0 or newer installed. This permission is only effective when <code>allow_mount</code> is set and <code>enforce_statfs</code> is set to a value lower than 2.</td>
</tr>
<tr>
<td>allow_mount_nullfs</td>
<td>checkbox</td>
<td>Allow privileged users inside the jail to mount and unmount the nullfs(5) file system (<a href="https://www.freebsd.org/cgi/man.cgi?query=nullfs">https://www.freebsd.org/cgi/man.cgi?query=nullfs</a>). This permission is only effective when <code>allow_mount</code> is set and <code>enforce_statfs</code> is set to a value lower than 2.</td>
</tr>
<tr>
<td>allow_mount_procfs</td>
<td>checkbox</td>
<td>Allow privileged users inside the jail to mount and unmount the procfs(5) file system (<a href="https://www.freebsd.org/cgi/man.cgi?query=procfs">https://www.freebsd.org/cgi/man.cgi?query=procfs</a>). This permission is only effective when <code>allow_mount</code> is set and <code>enforce_statfs</code> is set to a value lower than 2.</td>
</tr>
<tr>
<td>allow_mount_tmpfs</td>
<td>checkbox</td>
<td>Allow privileged users inside the jail to mount and unmount the tmpfs(5) file system (<a href="https://www.freebsd.org/cgi/man.cgi?query=tmpfs">https://www.freebsd.org/cgi/man.cgi?query=tmpfs</a>). This permission is only effective when <code>allow_mount</code> is set and <code>enforce_statfs</code> is set to a value lower than 2.</td>
</tr>
<tr>
<td>allow_mount_zfs</td>
<td>checkbox</td>
<td>Allow privileged users inside the jail to mount and unmount the ZFS file system. This permission is only effective when <code>allow_mount</code> is set and <code>enforce_statfs</code> is set to a value lower than 2. The ZFS(<a href="https://www.freebsd.org/cgi/man.cgi?query=zfs">https://www.freebsd.org/cgi/man.cgi?query=zfs</a>) man page has information on how to configure the ZFS filesystem to operate from within a jail.</td>
</tr>
<tr>
<td>allow_vmm</td>
<td>checkbox</td>
<td>Grants the jail access to the Bhyve Virtual Machine Monitor (VMM). The jail must have FreeBSD 12.0 or newer installed with the vmm(4) (<a href="https://www.freebsd.org/cgi/man.cgi?query=vmm">https://www.freebsd.org/cgi/man.cgi?query=vmm</a>) kernel module loaded.</td>
</tr>
<tr>
<td>allow_quotas</td>
<td>checkbox</td>
<td>Allow the jail root to administer quotas on the jail filesystems. This includes filesystems the jail shares with other jails or with non-jailed parts of the system.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 16.2 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow_socket_af</td>
<td>checkbox</td>
<td>Allow access to other protocol stacks beyond IPv4, IPv6, local (UNIX), and route. <strong>Warning</strong>: jail functionality does not exist for all protocol stacks.</td>
</tr>
<tr>
<td>vnet_interfaces</td>
<td>string</td>
<td>Space-delimited list of network interfaces to attach to a VNET-enabled jail after it is created. Interfaces are automatically released when the jail is removed.</td>
</tr>
</tbody>
</table>

Click **NEXT** to view all jail **Network Properties**. These are shown in **Table 16.3**:

Table 16.3: Network Properties

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interfaces</td>
<td>string</td>
<td>Enter up to four interface configurations in the format <code>interface:bridge</code>, separated by a comma (, ). The left value is the virtual VNET interface name and the right value is the bridge name where the virtual interface is attached.</td>
</tr>
<tr>
<td>host_hostname</td>
<td>string</td>
<td>Enter a hostname for the jail. By default, the system uses the jail NAME/UUID.</td>
</tr>
<tr>
<td>exec_fib</td>
<td>integer</td>
<td>Enter a number to define the routing table (FIB) to set when running commands inside the jail.</td>
</tr>
<tr>
<td>ip4.saddrsel</td>
<td>checkbox</td>
<td>Disables IPv4 source address selection for the jail in favor of the primary IPv4 address of the jail. Only available when the jail is not configured to use VNET.</td>
</tr>
<tr>
<td>ip4</td>
<td>drop-down</td>
<td>Control the availability of IPv4 addresses. Set to <strong>Inherit</strong>: allow unrestricted access to all system addresses. Set to <strong>New</strong>: restrict addresses with <code>ip4_addr</code>. Set to <strong>Disable</strong>: stop the jail from using IPv4 entirely.</td>
</tr>
<tr>
<td>ip6.saddrsel</td>
<td>string</td>
<td>Disable IPv6 source address selection for the jail in favor of the primary IPv6 address of the jail. Only available when the jail is not configured to use VNET.</td>
</tr>
<tr>
<td>ip6</td>
<td>drop-down</td>
<td>Control the availability of IPv6 addresses. Set to <strong>Inherit</strong>: allow unrestricted access to all system addresses. Set to <strong>New</strong>: restrict addresses with <code>ip6_addr</code>. Set to <strong>Disable</strong>: stop the jail from using IPv6 entirely.</td>
</tr>
<tr>
<td>resolver</td>
<td>string</td>
<td>Add lines to <code>resolv.conf</code> in file. Example: <code>nameserver IP;search domain.local</code>. Fields must be delimited with a semicolon (;), this is translated as new lines in <code>resolv.conf</code>. Enter <strong>none</strong> to inherit <code>resolv.conf</code> from the host.</td>
</tr>
<tr>
<td>mac_prefix</td>
<td>string</td>
<td>Optional. Enter a valid MAC address vendor prefix. Example: <strong>E4F4C6</strong></td>
</tr>
<tr>
<td>vnet0_mac</td>
<td>string</td>
<td>Leave this blank to generate random MAC addresses for the host and jail. To assign fixed MAC addresses, enter the host MAC address and the jail MAC address separated by a space.</td>
</tr>
<tr>
<td>vnet1_mac</td>
<td>string</td>
<td>Leave this blank to generate random MAC addresses for the host and jail. To assign fixed MAC addresses, enter the host MAC address and the jail MAC address separated by a space.</td>
</tr>
<tr>
<td>vnet2_mac</td>
<td>string</td>
<td>Leave this blank to generate random MAC addresses for the host and jail. To assign fixed MAC addresses, enter the host MAC address and the jail MAC address separated by a space.</td>
</tr>
</tbody>
</table>

Continued on next page
Table 16.3 – continued from previous page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vnet3_mac</td>
<td>string</td>
<td>Leave this blank to generate random MAC addresses for the host and jail. To assign fixed MAC addresses, enter the host MAC address and the jail MAC address separated by a space.</td>
</tr>
</tbody>
</table>

The final set of jail properties are contained in the *Custom Properties* section. Table 16.4 describes these options.

Table 16.4: Custom Properties

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>owner</td>
<td>string</td>
<td>The owner of the jail. Can be any string.</td>
</tr>
<tr>
<td>priority</td>
<td>integer</td>
<td>The numeric start priority for the jail at boot time. <strong>Smaller</strong> values mean a higher priority. At system shutdown, the priority is reversed. Example: 99</td>
</tr>
<tr>
<td>hostid</td>
<td>string</td>
<td>A new a jail hostid, if necessary. Example hostid: Ta2bc345-678d-90e1-23fa-4b56c78901de.</td>
</tr>
<tr>
<td>hostid_strict_check</td>
<td>checkbox</td>
<td>Check the jail hostid property. Prevents the jail from starting if the hostid does not match the host.</td>
</tr>
<tr>
<td>comment</td>
<td>string</td>
<td>Comments about the jail.</td>
</tr>
<tr>
<td>depends</td>
<td>string</td>
<td>Specify any jails the jail depends on. Child jails must already exist before the parent jail can be created.</td>
</tr>
<tr>
<td>mount_procs</td>
<td>checkbox</td>
<td>Allow mounting of a procs(5) filesystems in the jail /dev/proc directory.</td>
</tr>
<tr>
<td>mount_linprofs</td>
<td>checkbox</td>
<td>Allow mounting of a linprofs(5) filesystem in the jail.</td>
</tr>
<tr>
<td>template</td>
<td>checkbox</td>
<td>Convert the jail into a template. Template jails can be used to quickly create jails with the same configuration.</td>
</tr>
<tr>
<td>host_time</td>
<td>checkbox</td>
<td>Synchronize the time between jail and host.</td>
</tr>
<tr>
<td>jail_zfs</td>
<td>checkbox</td>
<td>Enable automatic ZFS jailing inside the jail. The assigned ZFS dataset is fully controlled by the jail. Note: allow_mount, enforce_statfs, and allow_mount_zfs must all be set for ZFS management inside the jail to work correctly.</td>
</tr>
<tr>
<td>jail_zfs_dataset</td>
<td>string</td>
<td>Define the dataset to be jailed and fully handed over to a jail. Enter a ZFS filesystem name without a pool name. jail_zfs must be set for this option to work.</td>
</tr>
<tr>
<td>jail_zfs_mountpoint</td>
<td>string</td>
<td>The mountpoint for the jail_zfs_dataset. Example: /data/example-dataset-name</td>
</tr>
<tr>
<td>allow_tun</td>
<td>checkbox</td>
<td>Expose host tun(4) devices in the jail. Allow the jail to create tun devices.</td>
</tr>
<tr>
<td>Autoconfigure IPv6 with rtsold</td>
<td>checkbox</td>
<td>Use rtsold(8) as part of IPv6 autoconfiguration. Send ICMPv6 Router Solicitation messages to interfaces to discover new routers.</td>
</tr>
<tr>
<td>ip_hostname</td>
<td>checkbox</td>
<td>Use DNS records during jail IP configuration to search the resolver and apply the first open IPv4 and IPv6 addresses. See jail(8).</td>
</tr>
<tr>
<td>assign_localhost</td>
<td>checkbox</td>
<td>Add network interface lo0 to the jail and assign it the first available localhost address, starting with 127.0.0.2. VNET cannot be set. Jails using VNET configure a localhost as part of their virtualized network stack.</td>
</tr>
</tbody>
</table>

Click **SAVE** when the desired jail properties have been set. New jails are added to the primary list in the *Jails* menu.
16.2.2.1 Creating Template Jails

Template jails are basejails that can be used as a template to efficiently create jails with the same configuration. These steps create a template jail:

1. Go to **Jails → ADD → ADVANCED JAIL CREATION**.
2. Select **Basejail** as the **Jail Type**. Configure the jail with desired options.
3. Set **template** in the **Custom Properties** tab.
4. Click **Save**.
5. Click **ADD**.
6. Enter a name for the template jail. Leave **Jail Type as Default (Clone Jail)**. Set **Release** to **basejailname(template)**, where **basejailname** is the name of the base jail created earlier.
7. Complete the jail creation wizard.

16.3 Managing Jails

Clicking **Jails** shows a list of installed jails. An example is shown in Figure 16.4.

![Fig. 16.4: Jail Overview Section](image)

Operations can be applied to multiple jails by selecting those jails with the checkboxes on the left. After selecting one or more jails, icons appear which can be used to ▶️ (Start), ◼️ (Stop), ⚙️ (Update), or ■ (Delete) those jails.
More information such as \textit{IPV4}, \textit{IPV6}, \textit{TYPE} of jail, and whether it is a \textit{TEMPLATE} jail or \textit{BASEJAIL} can be shown by clicking \(\Rightarrow\) (Expand). Additional options for that jail are also displayed. These are described in Table 16.5. Figure 16.5 shows the menu that appears.

\begin{table}[h]
\centering
\begin{tabular}{|l|l|}
\hline
\textbf{Option} & \textbf{Description} \\
\hline
EDIT & Used to modify the settings described in Advanced Jail Creation (page 304). A jail cannot be edited while it is running. The settings can be viewed, but are read only. \\
MOUNT POINTS & Select an existing mount point to \textit{EDIT} or click \textit{ACTIONS} \(\Rightarrow\) Add Mount Point to create a mount point for the jail. A mount point gives a jail access to storage located elsewhere on the system. A jail must be stopped before adding, editing, or deleting a mount point. See Additional Storage (page 316) for more details. \\
RESTART & Stop and immediately start an \textit{up} jail. \\
START & Start a jail that has a current \textit{STATE} of \textit{down}. \\
STOP & Stop a jail that has a current \textit{STATE} of \textit{up}. \\
\hline
\end{tabular}
\end{table}

\textbf{Warning:} Modify the IP address information for a jail by clicking \(\Rightarrow\) (Expand) \(\Rightarrow\) \textit{EDIT} instead of issuing the networking commands directly from the command line of the jail. This ensures the changes are saved and will survive a jail or FreeNAS\textsuperscript{®} reboot.
### 16.3.1 Jail Updates and Upgrades

Click ➔ (Expand) ➔ *Update* to update a jail to the most current patch level of the installed FreeBSD release. This does **not** change the release. For example, a jail installed with *FreeBSD 11.2-RELEASE* can update to *p15* or the latest patch of 11.2, but not an 11.3-RELEASE-p# version of FreeBSD.

A jail *upgrade* replaces the jail FreeBSD operating system with a new release of FreeBSD, such as taking a jail from FreeBSD 11.2-RELEASE to 11.3-RELEASE. Upgrade a jail by stopping it, opening the *Shell* (page 341) and entering `iocage upgrade name -r release`, where *name* is the plugin jail name and *release* is the desired release to upgrade to.

**Tip:** It is possible to *manually remove* (page 183) unused releases from the `/iocage/releases/` dataset after upgrading a jail. The release **must** not be in use by any jail on the system!

### 16.3.2 Accessing a Jail Using SSH

The ssh daemon `sshd(8)` must be enabled in a jail to allow SSH access to that jail from another system.

The jail *STATE* must be *up* before the *SHELL* option is available. If the jail is not up, start it by clicking *Jails ➔ ➔ START* for the desired jail. Click ➔ (Expand) ➔ *SHELL* to open a shell in the jail. A jail root shell is shown in this example:

```
Last login: Fri Apr 6 07:57:04 on pts/12
FreeBSD 11.1-STABLE (FreeNAS.amd64) #0 0ale9f753(freenas/11-stable): Fri Apr 6 04:46:31 UTC 2018
Welcome to FreeBSD!

FreeBSD FAQ: https://www.FreeBSD.org/faq/
FreeBSD Forums: https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/ directory, or can be installed later with: pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed: freebsd-version ; uname -a
```
**FreeNAS® 11.3-U5 User Guide, Release 11.3**

---

Please include that output and any error messages when posting questions.

**Introduction to manual pages:** man man

**FreeBSD directory layout:** man hier

Edit /etc/motd to change this login announcement.

```
root@jailexamp:~ #
```

---

**Tip:** A root shell can also be opened for a jail using the FreeNAS® UI Shell. Open the Shell, then type `iocage console jailname`.

---

**Enable sshd:**

```
sysrc ssdh_enable="YES"
sshd_enable: NO -> YES
```

**Tip:** Using `sysrc` to enable sshd verifies that sshd is enabled.

---

**Start the SSH daemon:** service sshd start

The first time the service runs, the jail RSA key pair is generated and the key fingerprint is displayed.

Add a user account with `adduser`. Follow the prompts, `Enter` will accept the default value offered. Users that require root access must also be a member of the `wheel` group. Enter `wheel` when prompted to `invite user into other groups`?[ ]:

```
root@jailexamp:~ # adduser
Username: jailuser
Full name: Jail User
Uid (Leave empty for default):
Login group [jailuser]:
Login group is jailuser. Invite jailuser into other groups? [ ]: wheel
Login class [default]:
Shell (sh csh tcsh git-shell zsh rzsh nologin) [sh]: csh
Home directory [/home/jailuser]:
Home directory permissions (Leave empty for default):
Use password-based authentication? [yes]:
Use an empty password? (yes/no) [no]:
Use a random password? (yes/no) [no]:
Enter password:
Enter password again:
Lock out the account after creation? [no]:
Username : jailuser
Password : *****
Full Name : Jail User
Uid : 1002
Class :
Groups : jailuser wheel
Home : /home/jailuser
Home Mode :
Shell : /bin/csh
Locked : no
OK? (yes/no): yes
adduser: INFO: Successfully added (jailuser) to the user database.
Add another user? (yes/no): no
Goodbye!
root@jailexamp:~
```

After creating the user, set the jail root password to allow users to use `su` to gain superuser privileges. To set the jail root password, use `passwd`. Nothing is echoed back when using `passwd`.
Finally, test that the user can successfully `ssh` into the jail from another system and gain superuser privileges. In the example, a user named `jailuser` uses `ssh` to access the jail at 192.168.2.3. The host RSA key fingerprint must be verified the first time a user logs in.

```
ssh jailuser@192.168.2.3
The authenticity of host ’192.168.2.3 (192.168.2.3)’ can’t be established.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added ’192.168.2.3’ (RSA) to the list of known hosts.
Password:
```

**Note:** Every jail has its own user accounts and service configuration. These steps must be repeated for each jail that requires SSH access.

### 16.3.3 Additional Storage

Jails can be given access to an area of storage outside of the jail that is configured on the FreeNAS® system. It is possible to give a FreeBSD jail access to an area of storage on the FreeNAS® system. This is useful for applications or plugins that store large amounts of data or if an application in a jail needs access to data stored on the FreeNAS® system. For example, Transmission is a plugin that stores data using BitTorrent. The FreeNAS® external storage is added using the `mount_nullfs(8)` mechanism, which links data that resides outside of the jail as a storage area within a jail.

> (Expand) → **MOUNT POINTS** shows any added storage and allows adding more storage.

**Note:** A jail must have a **STATE** of **down** before adding a new mount point. Click > (Expand) and **STOP** for a jail to change the jail **STATE** to **down**.

Storage can be added by clicking **Jails** → > (Expand) → **MOUNT POINTS** for the desired jail. The **MOUNT POINT** section is a list of all of the currently defined mount points.

**Go to** **MOUNT POINTS** → **ACTIONS** → **Add Mount Point** to add storage to a jail. This opens the screen shown in Figure 16.6.
Browse to the Source and Destination, where:

- **Source**: is the directory or dataset on the FreeNAS® system which will be accessed by the jail. FreeNAS® creates the directory if it does not exist. This directory must reside outside of the pool or dataset being used by the jail. This is why it is recommended to create a separate dataset to store jails, so the dataset holding the jails is always separate from any datasets used for storage on the FreeNAS® system.

- **Destination**: Browse to an existing and empty directory within the jail to link to the Source storage area. It is also possible to add / and a name to the end of the path and FreeNAS® automatically creates a new directory. New directories created must be within the jail directory structure. Example: /mnt/iocage/jails/samplejail/root/new-destination-directory.

Storage is typically added because the user and group account associated with an application installed inside of a jail needs to access data stored on the 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 will be given access to existing data or a new storage area will be allocated.

4. If the jail accesses existing data, edit the permissions of the pool 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 jail > (Expand) → MOUNT POINTS → ACTIONS → Add Mount Point to select the Source of the data and the Destination where it will be mounted in the jail.

To prevent writes to the storage, click Read-Only.

After storage has been added or created, it appears in the MOUNT POINTS for that jail. In the example shown in Figure 16.7, a dataset named pool1/smb-backups has been chosen as the Source as it contains the files stored on the FreeNAS® system. The user entered /mnt/iocage/jails/jail1/root/mounted as the directory to be mounted in the Destination field. To users inside the jail, this data appears in the /root/mounted directory.

Fig. 16.7: Example Storage

Storage is automatically mounted as it is created.

**Note:** Mounting a dataset does not automatically mount any child datasets inside it. Each dataset is a separate
filesystem, so child datasets must each have separate mount points.

Click \( \text{(Options)} \) \( \rightarrow \) \text{Delete} to delete the storage.

**Warning:** Remember that added storage is 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. This leaves the data intact but not accessible from the jail.

### 16.4 Jail Software

A jail is created with no software aside from the core packages installed as part of the selected version of FreeBSD. To install more software, start the jail and click \( > \) SHELL.

#### 16.4.1 Installing FreeBSD Packages

The quickest and easiest way to install software inside the jail is to install a FreeBSD package. FreeBSD packages are precompiled and contain all the binaries and a list of dependencies required for the software to run on a FreeBSD system.

A huge amount of software has been ported to FreeBSD. Most of that software is available as packages. One way to find FreeBSD software is to use the search bar at [FreshPorts.org](https://www.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 the command `pkg install audiotag`

When prompted, press `y` to complete the installation. Messages will show the download and installation status.

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/re naming 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/re naming 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`.

### 16.4.2 Compiling FreeBSD Ports

Compiling a port is another option. Compiling ports offer these advantages:

- Not every port has an available package. This is usually due to licensing restrictions or known, unaddressed security vulnerabilities.
- Sometimes the package is out-of-date and a feature is needed that only became available in the newer version.
- Some ports provide compile options that are not available in the pre-compiled package. These options are used to add or remove features or options.
Compiling a port has these disadvantages:

- It takes time. Depending upon the size of the application, the amount of dependencies, the speed of the CPU, the amount of RAM available, and the current load on the 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 resources to use the `pkg install` command instead.

The FreshPorts.org (https://www.freshports.org/) listing shows whether a port has any configurable compile options. Figure 16.8 shows the Configuration Options for audiotag, a utility for renaming multiple audio files.
Packages are built with default options. Ports let the user select options.

The Ports Collection must be installed in the jail before ports can be compiled. Inside the jail, use the `portsnap` utility. This command downloads the ports collection and extracts it to the `/usr/ports/` directory of the jail:

```
portsnap fetch extract
```

**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
```

The first time this command is run, the configure screen shown in Figure 16.9 is displayed:

![Fig. 16.9: Configuration Options for Audiotag Port](image)

This port has several configurable options: **DOCS, FLAC, ID3, MP4, and VORBIS**. Selected options are shown with a *.

Use the arrow keys to select an option and press `spacebar` to toggle the value. Press `Enter` when satisfied with the options. The port begins to compile and install.

**Note:** After options have been set, the configuration screen is normally not shown again. Use `make config` to display the screen and change options before rebuilding the port with `make clean install clean`.

Many ports depend on other ports. Those other ports also have configuration screens that are shown before compiling begins. It is a good idea to watch the compile until it finishes and the command prompt returns.

Installed ports are registered in the same package database that manages packages. The `pkg info` can be used to determine which ports were installed.

### 16.4.3 Starting Installed Software

After packages or ports are installed, they must be configured and started. Configuration files are usually in `/usr/local/etc` or a subdirectory of it. Many FreeBSD packages contain a sample configuration file as a reference.
Take some time to read the software documentation to learn which configuration options are available and which configuration files require editing.

Most FreeBSD packages that contain a startable service include a startup script which is automatically installed to /usr/local/etc/rc.d/. After the configuration is complete, test starting the service by running the script with the onestart option. For example, with openvpn installed in the jail, these commands are run to 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.
```

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 any error messages if an issue is found. Most startup failures are related to a misconfiguration in a configuration file.

After verifying that the service starts and is working as intended, add a line to `/etc/rc.conf` to start the service automatically when the jail is started. The line to start a service always ends in `_enable="YES"` and typically starts with the name of the software. For example, this is the entry for the openvpn service:

```
openvpn_enable="YES"
```

When in doubt, the startup script shows the line to put in `/etc/rc.conf`. This is the description in `/usr/local/etc/rc.d/openvpn`:

```
# 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

# NAME_if=
# driver(s) to load, set to "tun", "tap" or "tun tap"
# it is OK to specify the if_ prefix.
```

The startup script also indicates if any additional parameters are available:
# # 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
CHAPTER SEVENTEEN

REPORTING

Reporting displays several graphs, as seen in Figure 17.1. Choose a category from the drop-down menu to view those graphs. There are also options to change the graph view and number of graphs on each page.

Fig. 17.1: Reporting Graphs

FreeNAS® uses collectd (https://collectd.org/) to provide reporting statistics. For a clearer picture, hover over a point in the graph to show exact numbers for that point in time. Use the magnifier buttons next to each graph to increase or decrease the displayed time increment from 10 minutes, hourly, daily, weekly, or monthly. The << and >> buttons scroll through the output.

Note: Reporting graphs do not appear if there is no related data.

Graphs are grouped by category on the Reporting page:
• **CPU**
  - CPU ([https://collectd.org/wiki/index.php/Plugin:CPU](https://collectd.org/wiki/index.php/Plugin:CPU)) shows the amount of time spent by the CPU in various states such as executing user code, executing system code, and being idle. Graphs of short-, mid-, and long-term load are shown, along with CPU temperature graphs.

• **Disk**
  - Disk ([https://collectd.org/wiki/index.php/Plugin:Disk](https://collectd.org/wiki/index.php/Plugin:Disk)) shows read and write statistics on I/O, percent busy, latency, operations per second, pending I/O requests, and disk temperature. Choose the **DEVICES** and **METRICS** to view the selected metrics for the chosen devices.

  **Note:** Temperature monitoring for the disk is disabled if **HDD Standby** is enabled in **Disks** (page 195).

• **Memory**
  - Swap ([https://collectd.org/wiki/index.php/Plugin:Swap](https://collectd.org/wiki/index.php/Plugin:Swap)) displays the amount of free and used swap space.

• **Network**
  - Interface ([https://collectd.org/wiki/index.php/Plugin:Interface](https://collectd.org/wiki/index.php/Plugin:Interface)) shows received and transmitted traffic in megabytes per second for each configured interface.

• **NFS**
  - NFS ([https://collectd.org/wiki/index.php/Plugin:NFS](https://collectd.org/wiki/index.php/Plugin:NFS)) shows information about the number of procedure calls for each procedure and whether the system is a server or client.

• **Partition**
  - Disk space ([https://collectd.org/wiki/index.php/Plugin:DF](https://collectd.org/wiki/index.php/Plugin:DF)) displays free, used, and reserved space for each pool and dataset. However, the disk space used by an individual zvol is not displayed as it is a block device.

• **System**

• **Target**
  - Target shows bandwidth statistics for iSCSI ports.

• **UPS**

• **ZFS**

Reporting data is saved to permit viewing and monitoring usage trends over time. This data is preserved across system upgrades and restarts.

Data files are saved in `/var/db/collectd/rrd/`.

**Warning:** Reporting data is frequently written and should not be stored on the boot pool or operating system device.
A Virtual Machine (VM) is an environment on a host computer that can be used as if it were a separate physical computer. VMs can be used to run multiple operating systems simultaneously on a single computer. Operating systems running inside a VM see emulated virtual hardware rather than the actual hardware of the host computer. This provides more isolation than Jails (page 301), although there is additional overhead. A portion of system RAM is assigned to each VM, and each VM uses a zvol (page 185) for storage. While a VM is running, these resources are not available to the host computer or other VMs.

FreeNAS® VMs use the bhyve(8) (https://www.freebsd.org/cgi/man.cgi?query=bhyve) virtual machine software. This type of virtualization requires an Intel processor with Extended Page Tables (EPT) or an AMD processor with Rapid Virtualization Indexing (RVI) or Nested Page Tables (NPT). VMs cannot be created unless the host system supports these features.

To verify that an Intel processor has the required features, use Shell (page 341) to run `grep VT-x /var/run/dmesg.boot`. If the EPT and UG features are shown, this processor can be used with bhyve.

To verify that an AMD processor has the required features, use Shell (page 341) to run `grep POPCNT /var/run/dmesg.boot`. If the output shows the POPCNT feature, this processor can be used with bhyve.

**Note:** AMD K10 “Kuma” processors include POPCNT but do not support NRIPS, which is required for use with bhyve. Production of these processors ceased in 2012 or 2013.

By default, new VMs have the bhyve(8) (https://www.freebsd.org/cgi/man.cgi?query=bhyve) --host option set. This causes the virtual CPU thread to yield when a HLT instruction is detected and prevents idle VMs from consuming all of the host CPU.

Virtual Machines shows a list of installed virtual machines and available memory. The available memory changes depending on what the system is doing, including which virtual machines are running.

A log file for each VM is written to `/var/log/vm/vmname`. 
Name, State, and Autostart are displayed on the Virtual Machines page. Click -expand to view additional options for controlling and modifying VMs:

- **Start** boots a VM. VMs can also be started by clicking the slide toggle on the desired VM.

  If there is insufficient memory to start the VM, a dialog will prompt to Overcommit Memory. Memory overcommitment allows the VM to launch even though there is insufficient free memory. Proceeding with the overcommitment option should be used with caution.

  To start a VM when the host system boots, set Autostart. If Autostart is set and the VM is in an encrypted, locked pool, the VM starts when the pool is unlocked.

- **Edit** changes VM settings.

- **Delete** removes the VM. Zvols (page 185) used in disk devices (page 336) and image files used in raw file (page 337) devices are not removed when a VM is deleted. These resources can be removed manually in Storage → Pools after it is determined that the data in them has been backed up or is no longer needed.

- **Devices** is used to add, remove, or edit devices attached to a virtual machine.

- **Clone** copies the VM. A new name for the clone can be specified. If a custom name is not entered, the name assigned is vmname_cloneN, where vmname is the original VM name and N is the clone number. Each clones is given a new VNC port.

These additional options in -expand are available when a VM is running:

- **Power off** immediately halts the VM. This is equivalent to unplugging the power cord from a computer.

- **Stop** shuts down the VM.

- **Restart** shuts down and immediately starts the VM.
• VMs with *Enable VNC* set show a VNC button. VNC connections permit remote graphical access to the VM.

• SERIAL opens a connection to a virtual serial port on the VM. /dev/nmdm1B is assigned to the first VM, /dev/nmdm2B is assigned to the second VM, and so on. These virtual serial ports allow connections to the VM console from the Shell (page 341).

**Tip:** The [nmdm](https://www.freebsd.org/cgi/man.cgi?query=nmdm) device is dynamically created. The actual nmdm XY name varies on each VM.

To connect to the first VM, type `cu -l /dev/nmdm1B -s 9600` in the Shell (page 341). See [cu(1)](https://www.freebsd.org/cgi/man.cgi?query=cu) for more information.

### 18.1 Creating VMs

Click **ADD** to open the wizard in **Figure 18.2**:

![Figure 18.2: Add VM](image)

The configuration options for a Virtual Machine (VM) type are described in **Table 18.1**.
### Table 18.1: VM Wizard Options

<table>
<thead>
<tr>
<th>Screen #</th>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Guest Operating System</td>
<td>dropdown menu</td>
<td>Choose the VM operating system type. Choices are: Windows, Linux, or FreeBSD. See this guide (<a href="https://github.com/FreeBSD-UPB/freebsd/wiki/How-to-launch-different-guest-OS">https://github.com/FreeBSD-UPB/freebsd/wiki/How-to-launch-different-guest-OS</a>) for detailed instructions about using a different guest OS.</td>
</tr>
<tr>
<td>1</td>
<td>Name</td>
<td>string</td>
<td>Name of the VM. Alphanumeric characters and _ are allowed. The name must be unique.</td>
</tr>
<tr>
<td>1</td>
<td>Description</td>
<td>string</td>
<td>Description (optional).</td>
</tr>
<tr>
<td>1</td>
<td>System Clock</td>
<td>dropdown menu</td>
<td>Virtual Machine system time. Options are Local and UTC. Local is default.</td>
</tr>
<tr>
<td>1</td>
<td>Boot Method</td>
<td>dropdown menu</td>
<td>Choices are UEFI, UEFI-CSM, and Grub. Select UEFI for newer operating systems, or UEFI-CSM (Compatibility Support Mode) for older operating systems that only understand BIOS booting. VNC connections are only available with *UEFI. Grub is not supported by Windows guest operating systems.</td>
</tr>
<tr>
<td>1</td>
<td>Start on Boot</td>
<td>checkbox</td>
<td>Set to start the VM when the system boots.</td>
</tr>
<tr>
<td>1</td>
<td>Enable VNC</td>
<td>checkbox</td>
<td>Add a VNC remote connection. Requires UEFI booting.</td>
</tr>
<tr>
<td>1</td>
<td>Delay VM Boot Until VNC Connects</td>
<td>checkbox</td>
<td>Wait to start VM until VNC client connects. Only appears when Enable VNC is set.</td>
</tr>
<tr>
<td>1</td>
<td>Bind</td>
<td>dropdown menu</td>
<td>VNC network interface IP address. The primary interface IP address is the default. A different interface IP address can be chosen.</td>
</tr>
<tr>
<td>2</td>
<td>Virtual CPUs</td>
<td>integer</td>
<td>Number of virtual CPUs to allocate to the VM. The maximum is 16 unless limited by the host CPU. The VM operating system might also have operational or licensing restrictions on the number of CPUs.</td>
</tr>
<tr>
<td>2</td>
<td>Memory Size</td>
<td>integer</td>
<td>Set the amount of RAM for the VM. Allocating too much memory can slow the system or prevent VMs from running. This is a humanized field (page 24).</td>
</tr>
<tr>
<td>3</td>
<td>Disk image</td>
<td>check option with custom fields</td>
<td>Select Create new disk image to create a new zvol on an existing dataset. This is used as a virtual hard drive for the VM. Select Use existing disk image and choose an existing zvol from the Select Existing zvol drop-down.</td>
</tr>
<tr>
<td>3</td>
<td>Select Disk Type</td>
<td>dropdown menu</td>
<td>Select the disk type. Choices are AHCI and VirtIO. Refer to Disk Devices (page 336) for more information about these disk types.</td>
</tr>
<tr>
<td>3</td>
<td>Size (Examples: 500 KiB, 500M, 2TB)</td>
<td></td>
<td>Allocate the amount of storage for the zvol. This is a humanized field (page 24). Numbers without unit letters are interpreted as megabytes. For example, 500 sets the zvol size to 500 megabytes.</td>
</tr>
<tr>
<td>3</td>
<td>Zvol Location</td>
<td></td>
<td>When Create new disk image is chosen, select a pool or dataset for the new zvol.</td>
</tr>
<tr>
<td>3</td>
<td>Select existing zvol</td>
<td>dropdown menu</td>
<td>When Use existing disk image is chosen, select an existing zvol for the VM.</td>
</tr>
<tr>
<td>4</td>
<td>Adapter Type</td>
<td>dropdown menu</td>
<td>Intel e82545 (e1000) emulates the same Intel Ethernet card. This provides compatibility with most operating systems. VirtIO provides better performance when the operating system installed in the VM supports VirtIO paravirtualized network drivers.</td>
</tr>
<tr>
<td>4</td>
<td>MAC Address</td>
<td>string</td>
<td>Enter the desired MAC address to override the auto-generated randomized MAC address.</td>
</tr>
</tbody>
</table>

Continued on next page
The final screen of the Wizard displays the chosen options for the new Virtual Machine (VM) type. Click SUBMIT to create the VM or BACK to change any settings.

After the VM has been installed, remove the install media device. Go to Virtual Machines → ⦿ (Options) → Devices. Remove the CDROM device by clicking ⦿ (Options) → Delete. This prevents the virtual machine from trying to boot with the installation media after it has already been installed.

This example creates a FreeBSD VM:

1. Guest Operating System is set to FreeBSD. Name is set to samplevm. Other options are left at defaults.
2. Virtual CPUs is set to 2 and Memory Size (MiB) is set to 2048.
3. Create new disk image is selected. The zvol size is set to 20 GiB and stored on the pool named pool1.
4. Network settings are left at default values.
5. A FreeBSD ISO installation image has been selected and uploaded to the FreeNAS® system. The Choose installation media image field is populated when the upload completes.
6. After verifying the VM Summary is correct, SUBMIT is clicked.

Figure 18.3 shows the confirmation step and basic settings for the new virtual machine:
18.2 Installing Docker

Docker (https://www.docker.com/) can be used on FreeNAS® by installing it on a Linux virtual machine. Choose a Linux distro and install it on FreeNAS® by following the steps in Creating VMs (page 330). Using Ubuntu (https://ubuntu.com/) is recommended.

After the Linux operating system has been installed, start the VM. Connect to it by clicking ➔ (Expand) → VNC. Follow the Docker documentation (https://docs.docker.com/) for Docker installation and usage.

18.3 Adding Devices to a VM

Go to Virtual Machines, ➔ (Options) → Devices, and click ADD to add a new VM device.
Select the new device from the *Type* field. These devices are available:

- **CD-ROM** (page 334)
- **NIC (Network Interface Card)** (page 335)
- **Disk Device** (page 336)
- **Raw File** (page 337)
- **VNC Interface** (page 338) (only available on virtual machines with *Boot Loader Type* set to *UEFI*)

*Virtual Machines* → † (Options) → *Devices* is also used to edit or delete existing devices. Click † (Options) for a device to display *Edit, Delete, Change Device Order, and Details* options:

- **Edit** modifies a device.
- **Delete** removes the device from the VM.
- **Change Device Order** sets the priority number for booting this device. Smaller numbers are higher in boot priority.
- **Details** shows additional information about the specific device. This includes the physical interface and MAC address in a NIC device, the path to the zvol in a DISK device, and the path to an `.iso` or other file for a CDROM device.

### 18.3.1 CD-ROM Devices

Adding a CD-ROM device makes it possible to boot the VM from a CD-ROM image, typically an installation CD. The image must be present on an accessible portion of the FreeNAS® storage. In this example, a FreeBSD installation
image is shown:

Fig. 18.5: CD-ROM Device

**Note:** VMs from other virtual machine systems can be recreated for use in FreeNAS®. Back up the original VM, then create a new FreeNAS® VM with virtual hardware as close as possible to the original VM. Binary-copy the disk image data into the *zvol* (page 185) created for the FreeNAS® VM with a tool that operates at the level of disk blocks, like `dd(1)` ([https://www.freebsd.org/cgi/man.cgi?query=dd](https://www.freebsd.org/cgi/man.cgi?query=dd)). For some VM systems, it is best to back up data, install the operating system from scratch in a new FreeNAS® VM, and restore the data into the new VM.

### 18.3.2 NIC (Network Interfaces)

Figure 18.6 shows the fields that appear after going to `Virtual Machines → Options → Devices`, clicking `ADD`, and selecting `NIC` as the `Type`. 
The **Adapter Type** can emulate an Intel e82545 (e1000) Ethernet card for compatibility with most operating systems. **VirtIO** can provide better performance when the operating system installed in the VM supports VirtIO paravirtualized network drivers.

By default, the VM receives an auto-generated random MAC address. To override the default with a custom value, enter the desired address in **MAC Address**. Click **GENERATE MAC ADDRESS** to automatically populate **MAC Address** with a new randomized MAC address.

If the system has multiple physical network interface cards, use the **NIC to attach** drop-down menu to specify which physical interface to associate with the VM. To prevent a network interface reset when the VM starts, edit the **network interface** (page 159) and set **Disable Hardware Offloading**.

Set a **Device Order** number to determine the boot order of this device. A lower number means a higher boot priority.

**Tip:** To check which interface is attached to a VM, start the VM and go to the **Shell** (page 341). Type `ifconfig` and find the **tap** (https://en.wikipedia.org/wiki/TUN/TAP) interface that shows the name of the VM in the description.

### 18.3.3 Disk Devices

**Zvols** (page 185) are typically used as virtual hard drives. After **creating a zvol** (page 185), associate it with the VM by clicking **Virtual Machines** → ³ (Options) → **Devices**, clicking **ADD**, and selecting **Disk** as the **Type**.
Open the drop-down menu to select a created Zvol, then set the disk Mode:

- **AHCI** emulates an AHCI hard disk for best software compatibility. This is recommended for Windows VMs.
- **VirtIO** uses paravirtualized drivers and can provide better performance, but requires the operating system installed in the VM to support VirtIO disk devices.

If a specific sector size is required, enter the number of bytes in *Disk sector size*. The default of 0 uses an autotune script to determine the best sector size for the zvol.

Set a *Device Order* number to determine the boot order of this device. A lower number means a higher boot priority.

### 18.3.4 Raw Files

*Raw Files* are similar to Zvol (page 185) disk devices, but the disk image comes from a file. These are typically used with existing read-only binary images of drives, like an installer disk image file meant to be copied onto a USB stick.

After obtaining and copying the image file to the FreeNAS® system, click *Virtual Machines → Options → Devices*, click ADD, then set the *Type* to *Raw File*. 
Click ☐ (Browse) to select the image file. If a specific sector size is required, choose it from Disk sector size. The Default value automatically selects a preferred sector size for the file.

Setting disk Mode to AHCI emulates an AHCI hard disk for best software compatibility. VirtIO uses paravirtualized drivers and can provide better performance, but requires the operating system installed in the VM to support VirtIO disk devices.

Set a Device Order number to determine the boot order of this device. A lower number means a higher boot priority.

Set the size of the file in GiB.

### 18.3.5 VNC Interface

VMs set to UEFI booting are also given a VNC (Virtual Network Computing) remote connection. A standard VNC (https://en.wikipedia.org/wiki/Virtual_Network_Computing) client can connect to the VM to provide screen output and keyboard and mouse input.

Each VM can have a single VNC device. An existing VNC interface can be changed by clicking ☐ (Options) and Edit.

**Note:** Using a non-US keyboard with VNC is not yet supported. As a workaround, select the US keymap on the system running the VNC client, then configure the operating system running in the VM to use a keymap that matches the physical keyboard. This will enable passthrough of all keys regardless of the keyboard layout.

Figure 18.9 shows the fields that appear after going to Virtual Machines → ☐ (Options) → Devices, and clicking ☐ (Options) → Edit for VNC.
Setting `Port` to 0 automatically assigns a port when the VM is started. If a fixed, preferred port number is needed, enter it here.

Set `Delay VM Boot until VNC Connects` to wait to start the VM until a VNC client connects.

`Resolution` sets the default screen resolution used for the VNC session.

Use `Bind` to select the IP address for VNC connections.

To automatically pass the VNC password, enter it into the `Password` field. Note that the password is limited to 8 characters.

To use the VNC web interface, set `Web Interface`.

**Tip:** If a RealVNC 5.X Client shows the error `RFB protocol error: invalid message type`, disable the `Adapt to network speed` option and move the slider to `Best quality`. On later versions of RealVNC, select `File → Preferences`, click `Expert, ProtocolVersion`, then select 4.1 from the drop-down menu.

Set a `Device Order` number to determine the boot order of this device. A lower number means a higher boot priority.
Clicking Display System Processes opens a screen showing the output of `top(1)` (https://www.freebsd.org/cgi/man.cgi?query=top). An example is shown in Figure 19.1.

![Figure 19.1: System Processes Running on FreeNAS®](image)

The display automatically refreshes itself. The display is read-only.
The FreeNAS® web interface provides a web shell, making it convenient to run command line tools from the web browser as the root user.

![Fig. 20.1: Web Shell](image)

The prompt shows that the current user is root, the hostname is freenas, and the current working directory is ~, the home directory of the logged-in user.

**Note:** The default shell for a new install of FreeNAS® is zsh (https://www.freebsd.org/cgi/man.cgi?query=zsh). FreeNAS® systems which have been upgraded from an earlier version will continue to use csh as the default shell. The default shell can be changed in Accounts → Users. Click † (Options) and Edit for the root user. Choose the desired shell from the Shell drop-down and click SAVE.
The *Set font size* slider adjusts the size of text displayed in the Shell. Click *RESTORE DEFAULT* to reset the shell font and size.

A history of previous commands is available. Use the up and down arrow keys to scroll through previously entered commands. Edit the command if desired, then press *Enter* to re-enter the command.

Home, End, and Delete keys are supported. Tab completion is also available. Type a few letters and press Tab to complete a command name or filename in the current directory. Right-clicking in the terminal window displays a reminder about using Command+c and Command+v or Ctrl+Insert and Shift+Insert for copy and paste operations in the FreeNAS® shell.

Type *exit* to leave the session.

Clicking other web interface menus closes the shell session and stops commands running in the shell. *tmux* (page 370) provides the ability to detach shell sessions and then reattach to them later. Commands continue to run in a detached session.

**Note:** Not all shell features render correctly in Chrome. Firefox is the recommended browser when using the shell.

Most FreeBSD *command line utilities* (page 356) are available in the Shell, including additional troubleshooting applications for FreeNAS®.
LOG OUT, RESTART, OR SHUT DOWN

The \(\Phi\) (Power) button is used to log out of the web interface or restart or shut down the FreeNAS® system.

21.1 Log Out

To log out, click \(\Phi\) (Power), then Log Out. After logging out, the login screen is displayed.

21.2 Restart

To restart the system, click \(\Phi\) (Power), then Restart. A confirmation screen asks for verification of the restart. Figure 21.1. Click Confirm to confirm the action, then click RESTART to restart the system.

Fig. 21.1: Restart Warning Message
An additional warning message appears when a restart is attempted when a scrub or resilver is in progress. When that warning appears, the recommended steps are to CANCEL the restart request and to periodically run `zpool status` from Shell (page 341) until it shows that the scrub or verify has completed. Then the restart request can be entered again.

To complete the restart request, click the Confirm checkbox and then the RESTART button. Restarting the system disconnects all clients, including the web administration interface. Wait a few minutes for the system to boot, then use the back button in the browser to return to the IP address of the FreeNAS® system. The login screen appears after a successful reboot. If the login screen does not appear, using a monitor and keyboard to physically access the FreeNAS® system is required to determine the issue preventing the system from resuming normal operation.

### 21.3 Shut Down

Click ⚫️ (Power) and Shut Down to shut down the system. The warning message shown in Figure 21.2 is displayed.

![Fig. 21.2: Shut Down Warning Message](image_url)

Click Confirm and then SHUT DOWN to shut down the system. Shutting down the system disconnects all clients, including the web interface. Physical access to the FreeNAS® system is required to turn it back on.
The FreeNAS® alert system provides a visual warning of any conditions that require administrative attention. The Alert icon in the upper right corner has a notification badge that displays the total number of unread alerts. In the example alert shown in Figure 22.1, the system is warning that a pool is degraded.

![Fig. 22.1: Example Alert Message](image)

Table 22.1 shows the icons that indicate notification, warning, critical, and one-shot critical alerts. Critical messages are also emailed to the root account. One-shot critical alerts must be dismissed by the user.
Table 22.1: FreeNAS® Alert Icons

<table>
<thead>
<tr>
<th>Alert Level</th>
<th>Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification</td>
<td>⚠</td>
</tr>
<tr>
<td>Warning</td>
<td>⚠</td>
</tr>
<tr>
<td>Critical</td>
<td>⚠</td>
</tr>
<tr>
<td>One-shot Critical</td>
<td>⚠</td>
</tr>
</tbody>
</table>

Close an alert message by clicking Dismiss. There is also an option to Dismiss All Alerts. Dismissing all alerts removes the notification badge from the alerts icon. Dismissed alerts can be re-opened by clicking Re-Open.

Behind the scenes, an alert daemon checks for various alert conditions, such as pool and disk status, and writes the current conditions to the system RAM. These messages are flushed to the SQLite database periodically and then published to the user interface.

Current alerts are viewed from the Shell option of the Console Setup Menu (Figure 3.1) or the Web Shell (Figure 20.1) by running midclt call alert.list.

Notifications for specific alerts are adjusted in the Alert Settings (page 96) menu. An alert message can be set to publish IMMEDIATELY, HOURLY, DAILY, or NEVER.

Some of the conditions that trigger an alert include:

- used space on a pool, dataset, or zvol goes over 80%; the alert goes red at 95%
- new ZFS Feature Flags (page 375) are available for the pool; this alert can be adjusted in Alert Settings (page 96) if a pool upgrade is not desired at present
- a new update is available
- hardware events detected by an attached IPMI (page 164) controller
- an error with the Active Directory (page 204) connection
- ZFS pool status changes from HEALTHY
- a S.M.A.R.T. error occurs
- 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
- the NTP server cannot be contacted
- syslog-ng(8) (https://www.freebsd.org/cgi/man.cgi?query=syslog-ng) is not running
- a periodic snapshot or replication task fails
- a VMware login or a VMware-Snapshots (page 194) task fails
- a Cloud Sync task (page 151) 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
- an Active Directory domain goes offline; by default the winbindd connection manager will try to reconnect every 30 seconds and will clear the alert when the domain comes back online
- LDAP failed to bind to the domain
- any member interfaces of a lagg interface are not active
- a device is slowing pool I/O
- Rsync task (page 129) status
- the status of an Avago MegaRAID SAS controller has changed; mfiutil(8) (https://www.freebsd.org/cgi/man.cgi?query=mfiutil) is included for managing these devices
• a scrub has been paused for more than eight hours
• a connected Uninterruptible Power Supply (UPS) switches to battery power, switches to line power, communication with the UPS is lost or established, the battery is low, or the battery needs to be replaced
The task manager shows a list of tasks performed by the FreeNAS® system starting with the most recent. Click a task name to display its start time, progress, finish time, and whether the task succeeded. If a task failed, the error status is shown.

Tasks with log file output have a View Logs button to show the log files.

The task manager can be opened by clicking 🛠️ (Task Manager). Close the task manager by clicking CLOSE, clicking anywhere outside the task manager dialog, or by pressing Esc.
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 an issue occurs while using FreeNAS®, it can be helpful to spend a few minutes searching the Internet for the word FreeNAS with some keywords that describe the error message or function that is being implemented.

The section discusses resources available to FreeNAS® users:

- **User Guide** (page 349)
- **Website and Social Media** (page 349)
- **Forums** (page 349)
- **IRC** (page 350)
- **Videos** (page 350)
- **Professional Support** (page 351)

### 24.1 User Guide

The FreeNAS® User Guide with complete configuration instructions is available either by clicking Guide in the FreeNAS® user interface or going to https://www.ixsystems.com/documentation/freenas/

### 24.2 Website and Social Media

The FreeNAS® website (http://www.freenas.org/) 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 (https://www.linkedin.com/groups/3903140/profile)
- Facebook FreeNAS Community (https://www.facebook.com/freenascommunity)
- Facebook FreeNAS Consortium (please request to be added) (https://www.facebook.com/groups/1707686686200221)
- Twitter (https://mobile.twitter.com/freenas)

### 24.3 Forums

The FreeNAS Forums (https://forums.freenas.org/index.php) are an active online resource where people can ask questions, receive help, and share findings with other FreeNAS® users. New users are encouraged to post a brief message about themselves and how they use FreeNAS® in the Introductions (https://forums.freenas.org/index.php?forums/introductions.25/) forum.
The Resources (https://forums.freenas.org/index.php?resources/) section contains categorized, user-contributed guides on many aspects of building and using FreeNAS® systems.

Language-specific categories are available under International.

- Chinese (https://forums.freenas.org/index.php?forums/chinese-%E4%B8%AD%E6%96%87.60/)
- German - Deutsch (https://forums.freenas.org/index.php?forums/german-deutsch.31/)
- Portuguese - Português (https://forums.freenas.org/index.php?forums/portuguese-portugu%C3%AAs.44/)
- Romanian - Română (https://forums.freenas.org/index.php?forums/romanian-rom%C3%A2n%C4%83.53/)
- Russian - Русский (https://forums.freenas.org/index.php?forums/russian-%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9.38/)
- Spanish - Español (https://forums.freenas.org/index.php?forums/spanish-espa%C3%B1ol.33/)
- Swedish - Svenske (https://forums.freenas.org/index.php?forums/swedish-svenske.51/)
- Turkish - Türkçe (https://forums.freenas.org/index.php?forums/turkish-%C3%BCrk%C3%A7e.36/)

To join the forums, create an account with the Sign Up Now! link.

Before asking a question on the forums, check the Resources (https://forums.freenas.org/index.php?resources/) to see if the information is already there. See the Forum Rules (https://forums.freenas.org/index.php?threads/updated-forum-rules-4-11-17.45124/) for guidelines on posting your hardware information and how to ask a questions that will get a response.

### 24.4 IRC

To ask a question in real time, use the #freenas channel on IRC Freenode (http://freenode.net/). Depending on the time of day and the 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 (https://en.wikipedia.org/wiki/Comparison_of_Internet_Relay_Chat_clients) is used to access the #freenas IRC channel. Alternately, use webchat (http://webchat.freenode.net/?channels=freenas) 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.
- Do not ask a question and leave. Users who know the answer cannot help you if you disappear.
- If no one answers, the question may be difficult to answer or it has been asked before. Research other resources while waiting for the question to be answered.
- Do not post error messages in the channel. Instead, use a pasting service such as pastebin (https://pastebin.com/) and paste the resulting URL into the IRC discussion.

### 24.5 Videos

A series of instructional videos are available for FreeNAS®:

- Install Murmur (Mumble server) on FreeNAS/FreeBSD (https://www.youtube.com/watch?v=aAeZRNFjarJc)
- FreeNAS® 9.10 - Certificate Authority & SSL Certificates (https://www.youtube.com/watch?v=OT1Le5VQIc0)
- How to Update FreeNAS® 9.10 (https://www.youtube.com/watch?v=2nvb90AhgL8)
• FreeNAS® 9.10 LAGG & VLAN Overview (https://www.youtube.com/watch?v=wqSH_uQSArQ)
• FreeNAS 9.10 and Samba (SMB) Permissions (https://www.youtube.com/watch?v=RxggaE935PM)
• FreeNAS® 11 - What's New (https://www.youtube.com/watch?v=-uJ_7eG88zk)
• FreeNAS® 11 - How to Install (https://www.youtube.com/watch?v=R3f-Sr6y-c4)

24.6 Professional Support

In addition to free community resources, support might be available in your area through third-party consultants. Submit a support inquiry using the form at https://www.ixsystems.com/freenas-commercial-support/.
CONTRIBUTING TO FREenas®

FreeNAS® is an open source community, relying on the input and expertise of users to grow and improve. When users take time to assist the community, their contributions benefit everyone.

This section describes how to participate and contribute to FreeNAS®. It is by no means an exhaustive list. If you have an idea that will benefit the community, bring it up on one of the resources mentioned in Support Resources (page 349).

This section demonstrates how to:

• Help with Translation (page 352)

25.1 Translation

FreeNAS® is developed and documented in English. Having complete translations of the user interface into other languages helps make FreeNAS® much more useful to communities around the world.

FreeNAS® uses .po files stored in the webui GitHub repository (https://github.com/freenas/webui/tree/master/src/assets/i18n) to manage the translation of text shown in the FreeNAS® graphical administrative interface. GitHub provides an easy to use web-based editor, making it possible for individuals to assist with translation or comment on existing translations.

To view translation files, open the /src/assets/i18n directory of the FreeNAS® webui repository (https://github.com/freenas/webui/tree/master/src/assets/i18n), as shown in Figure 25.1.
To assist with translating FreeNAS®, first create an account with GitHub (https://github.com/) and Fork the freenas/webui (https://github.com/freenas/webui) repository.

There are two methods for committing translations:

1. Use the GitHub website to edit the .po files.

OR

2. Make a local copy of the forked repository and use a text editor for translations.

### 25.1.1 Translate with GitHub

Open a browser and go to your GitHub profile. Select the Repositories tab and open your fork of the freenas/webui repository. Click src → assets → i18n to open the translations directory. Click on the desired language .po file to begin translating.

**Tip:** Here is a list of common language abbreviations (https://www.abbreviations.com/acronyms/LANGUAGES2L)

Click the Pencil icon in the upper right area to open the online file editor. **Figure 25.2** shows the page that appears:
There are numerous `msgid ""` and `msgstr ""` entries in the file. Read the `msgid` text and enter the translation between the `msgstr` quotes.

Scroll to the bottom of the page when finished entering translations. Enter a descriptive title and summary of changes for the edits and click `Commit changes`.

### 25.1.2 Download and Translate Offline


These instructions show using the Command Line Interface (CLI) with `git`, but many graphical utilities are available.

Create a suitable directory to store the local copy of the forked repository. Download the repository with `git clone`:

```bash
% git clone https://github.com/ghuser/webui.git
```

The download can take several minutes, depending on connection speed.

Use `cd` to go to the `i18n` directory:

```bash
% cd src/assets/i18n/
```

Use a `po` editor to add translations to the desired language file. Any capable editor will work, but `poedit` ([https://poedit.net/](https://poedit.net/)) and `gtranslator` ([https://wiki.gnome.org/Apps/Gtranslator](https://wiki.gnome.org/Apps/Gtranslator)) are two common options.

Commit any file changes with `git commit`.
% git commit ar.po

Enter a descriptive message about the changes and save the commit.

When finished making commits to the branch, use `git push` to send your changes to the online fork repository.

### 25.1.3 Translation Pull Requests

When ready to merge translations in the original `freenas/webui` repository, open a web browser and go to your forked repository on GitHub. Select the Code tab and click New pull request. Set the base repository drop-down to `freenas/webui` and the head repository to your fork. Click Create pull request, write a title and summary of your proposed changes, and click Create pull request again to submit your translations to the `freenas/webui` repository.

The FreeNAS® project automatically tests pull requests for compatibility. If there are any issues with a pull request, either the automated system will update the request or a FreeNAS® team member will leave a message in the comment section of the request.

All assistance with translations helps to benefit the FreeNAS® community. Thank you!
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** (page 356): used for measuring maximum TCP and UDP bandwidth performance
- **Netperf** (page 359): a tool for measuring network performance
- **IOzone** (page 360): filesystem benchmark utility used to perform a broad filesystem analysis
- **arcstat** (page 362): used to gather ZFS ARC statistics

The following utilities are specific to RAID controllers:

- **tw_cli** (page 367): used to monitor and maintain 3ware RAID controllers
- **MegaCli** (page 369): used to configure and manage Broadcom MegaRAID SAS family of RAID controllers

This section also describes these utilities:

- **freenas-debug** (page 369): the backend used to dump FreeNAS® debugging information
- **tmux** (page 370): a terminal multiplexer similar to GNU screen
- **Dmidecode** (page 371): reports information about system hardware as described in the system's BIOS

### 26.1 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, it is used to test the speed of different types of shares to determine which type performs best on the network.

FreeNAS® includes the iperf server. To perform network testing, install an iperf client on a desktop system that has network access to the FreeNAS® system. This section demonstrates how to use the xjperf user interface client (https://code.google.com/archive/p/xjperf/downloads) as it works on Windows, macOS, Linux, and BSD systems.

Since this client is Java-based, the appropriate JRE (http://www.oracle.com/technetwork/java/javase/downloads/index.html) must be installed on the client computer.

Linux and BSD users will need to install the iperf package using the package management system for their operating system.

To start xjperf 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 xjperf on macOS, Linux, or BSD, unzip the downloaded file, cd to the unzipped directory, type chmod u+x jperf.sh, and run ./jperf.sh.

Start the iperf server on FreeNAS® when the client is ready.
Note: Beginning with FreeNAS® version 11.1, both iperf2 (https://sourceforge.net/projects/iperf2/) and iperf3 (http://software.es.net/iperf/) are pre-installed. To use iperf2, use `iperf`. To use iperf3, instead type `iperf3`. The examples below are for iperf2.

To see the available server options, open Shell and type:

```
iperf --help | more
```

or:

```
iperf3 --help | more
```

For example, to perform a TCP test and start the server in daemon mode (to get the 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: The daemon process stops when Shell (page 341) closes. Set up the environment with shares configured and started before starting the Iperf process.

From the 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 26.1 shows an example of the client running on a Windows system while an SFTP transfer is occurring on the network.
Check the type of traffic before testing UDP or TCP. The iperf server is used to get additional details for services using TCP `iperf -sD` or UDP `iperf -sDu`. The startup message indicates when the server is listening for TCP or UDP. The `sockstat -4 | more` command gives an overview of the services running on the FreeNAS® system. This helps to determine if the traffic to test is UDP or TCP.

```
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 192.168.2.11:1180 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 :*
```
When testing is finished, either type `killall iperf` or close Shell to terminate the iperf server process.

### 26.2 Netperf

Netperf is a benchmarking utility that can be used to measure the performance of unidirectional throughput and end-to-end latency.

Before using the `netperf` command, start its server process with this command:

```bash
netserver
Starting netserver with host 'IN(6)ADDR_ANY' port '12865' and family AF_UNSPEC
```

The following command displays the available options for performing tests with the `netperf` command. The [Netperf Manual](https://hewlettpackard.github.io/netperf/) 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 the results. When testing is finished, type `killall netserver` to stop the server process.

```bash
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, and specifying a
value with a trailing comma will set 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 behavior.

26.3 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 so it can be run from Shell. When using IOzone on FreeNAS®, cd to a directory in a pool that you have permission to write to, otherwise an error about being unable to write the temporary file will occur.

Before using IOzone, read through the IOzone documentation PDF (http://www.iozone.org/docs/IOzone_msword_98.pdf) as it describes the tests, the many command line switches, and how to interpret the results.

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](https://www.cyberciti.biz/tips/linux-filesystem-benchmarking-with-iozone.html)
- [Analyzing NFS Client Performance with IOzone](http://www.iozone.org/docs/NFSClientPerf_revised.pdf)
- [10 iozone Examples for Disk I/O Performance Measurement on Linux](https://www.thegeekstuff.com/2011/05/iozone-examples/)

Type the following command to receive a summary of the available switches. IOzone is comprehensive so 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 a visual representation of the collected data is preferred, scripts are available to render IOzone’s output in [Gnuplot](http://www.gnuplot.info/).

```bash
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]
        [-1 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 File name to use
-F File names 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=stripe-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
-U Mount point to remount between tests
-v version information
-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
-2 Enable mixing of mmap I/O and file I/O
26.4 arcstat

Arcstat is a script that prints out ZFS ARC (https://en.wikipedia.org/wiki/Adaptive_replacement_cache) statistics. Originally it was a perl script created by Sun. That perl script was ported to FreeBSD and then ported as a Python script for use on FreeNAS®.

Watching ARC hits/misses and percentages shows how well the ZFS pool is fetching from the ARC rather than using disk I/O. Ideally, there will be as many things fetching from cache as possible. Keep the load in mind while reviewing 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 (https://wiki.freebsd.org/ZFSTuningGuide) 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 made 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 one network may not benefit another.

In particular, the value of pre-fetching depends upon the amount of memory and the type of workload, as seen in Understanding ZFS: Prefetch (http://cuddletech.com/?page_id=834&id=1040)

FreeNAS® provides two command line scripts which can be manually run from Shell (page 341):

- 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 provide real time information, whereas the current web interface reporting mechanism is designed to only provide graphs charted over time.
This forum post (https://forums.freenas.org/index.php?threads/benchmarking-zfs.7928/) 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
[-havxp] [-f fields] [-o file] [-s string] [interval [count]]

-h : Print this help message
-a : Print all possible stats
-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
-p : Disable auto-scaling of numerical fields
```

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
```

Table 26.1 briefly describes the columns in the output.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>read</td>
<td>total ARC accesses/second</td>
</tr>
<tr>
<td>miss</td>
<td>ARC misses/second</td>
</tr>
<tr>
<td>miss%</td>
<td>ARC miss percentage</td>
</tr>
<tr>
<td>dmis</td>
<td>demand data misses/second</td>
</tr>
<tr>
<td>dm%</td>
<td>demand data miss percentage</td>
</tr>
<tr>
<td>pmis</td>
<td>prefetch misses per second</td>
</tr>
<tr>
<td>pm%</td>
<td>prefetch miss percentage</td>
</tr>
<tr>
<td>mmis</td>
<td>metadata misses/second</td>
</tr>
<tr>
<td>mm%</td>
<td>metadata miss percentage</td>
</tr>
<tr>
<td>arksz</td>
<td>arc size</td>
</tr>
<tr>
<td>c</td>
<td>arc target size</td>
</tr>
</tbody>
</table>

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
```
<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Total</td>
<td>4.00 GiB</td>
</tr>
<tr>
<td>Logical Used</td>
<td>13.93% 570.77 MiB</td>
</tr>
<tr>
<td>Logical Free</td>
<td>86.07% 3.44 GiB</td>
</tr>
<tr>
<td>Kernel Memory</td>
<td>87.62 MiB</td>
</tr>
<tr>
<td>Data:</td>
<td>69.91% 61.25 MiB</td>
</tr>
<tr>
<td>Text:</td>
<td>30.09% 26.37 MiB</td>
</tr>
<tr>
<td>Kernel Memory Map</td>
<td>3.86 GiB</td>
</tr>
<tr>
<td>Size:</td>
<td>5.11% 201.70 MiB</td>
</tr>
<tr>
<td>Free:</td>
<td>94.89% 3.66 GiB</td>
</tr>
<tr>
<td>ARC Summary</td>
<td>HEALTHY</td>
</tr>
<tr>
<td>Storage pool Version</td>
<td>5000</td>
</tr>
<tr>
<td>Filesystem Version</td>
<td>5</td>
</tr>
<tr>
<td>Memory Throttle Count</td>
<td>0</td>
</tr>
<tr>
<td>ARC Misc</td>
<td></td>
</tr>
<tr>
<td>Deleted</td>
<td>8</td>
</tr>
<tr>
<td>Mutex Misses</td>
<td>0</td>
</tr>
<tr>
<td>Evict Skips</td>
<td>0</td>
</tr>
<tr>
<td>ARC Size</td>
<td>5.83% 170.45 MiB</td>
</tr>
<tr>
<td>Target Size (Adaptive)</td>
<td>100.00% 2.86 GiB</td>
</tr>
<tr>
<td>Min Size (Hard Limit)</td>
<td>12.50% 365.69 MiB</td>
</tr>
<tr>
<td>Max Size (High Water)</td>
<td>8:1 2.86 GiB</td>
</tr>
<tr>
<td>ARC Size Breakdown</td>
<td></td>
</tr>
<tr>
<td>Recently Used Cache Size</td>
<td>50.00% 1.43 GiB</td>
</tr>
<tr>
<td>Frequently Used Cache Size</td>
<td>50.00% 1.43 GiB</td>
</tr>
<tr>
<td>ARC Hash Breakdown</td>
<td></td>
</tr>
<tr>
<td>Elements Max</td>
<td>5.90k</td>
</tr>
<tr>
<td>Elements Current</td>
<td>100.00% 5.90k</td>
</tr>
<tr>
<td>Collisions</td>
<td>72</td>
</tr>
<tr>
<td>Chain Max</td>
<td>1</td>
</tr>
<tr>
<td>Chains</td>
<td>23</td>
</tr>
<tr>
<td>ARC Total accesses</td>
<td>954.06k</td>
</tr>
<tr>
<td>Cache Hit Ratio</td>
<td>99.18% 946.25k</td>
</tr>
<tr>
<td>Cache Miss Ratio</td>
<td>0.82% 7.81k</td>
</tr>
<tr>
<td>Actual Hit Ratio</td>
<td>98.84% 943.00k</td>
</tr>
<tr>
<td>Data Demand Efficiency</td>
<td>99.20% 458.77k</td>
</tr>
<tr>
<td>CACHE HITS BY CACHE LIST</td>
<td></td>
</tr>
<tr>
<td>Anonymously Used</td>
<td>0.34% 3.25k</td>
</tr>
<tr>
<td>Most Recently Used</td>
<td>3.73% 35.33k</td>
</tr>
<tr>
<td>Most Frequently Used</td>
<td>95.92% 907.67k</td>
</tr>
<tr>
<td>Most Recently Used Ghost</td>
<td>0.00% 0</td>
</tr>
<tr>
<td>Most Frequently Used Ghost</td>
<td>0.00% 0</td>
</tr>
<tr>
<td>CACHE HITS BY DATA TYPE</td>
<td></td>
</tr>
<tr>
<td>Demand Data</td>
<td>48.10% 455.10k</td>
</tr>
<tr>
<td>Prefetch Data</td>
<td>0.00% 0</td>
</tr>
<tr>
<td>Demand Metadata</td>
<td>51.56% 487.90k</td>
</tr>
<tr>
<td>Prefetch Metadata</td>
<td>0.34% 3.25k</td>
</tr>
<tr>
<td>CACHE MISSES BY DATA TYPE</td>
<td></td>
</tr>
<tr>
<td>Demand Data</td>
<td>46.93% 3.66k</td>
</tr>
<tr>
<td>Prefetch Data</td>
<td>0.00% 0</td>
</tr>
<tr>
<td>Demand Metadata</td>
<td>49.76% 3.88k</td>
</tr>
<tr>
<td>Prefetch Metadata</td>
<td>3.30% 258</td>
</tr>
<tr>
<td>ZFS Tunable (sysctl):</td>
<td></td>
</tr>
<tr>
<td>kern.maxusers</td>
<td>590</td>
</tr>
<tr>
<td>vm.kmem_size</td>
<td>4141375488</td>
</tr>
<tr>
<td>vm.kmem_size_scale</td>
<td>1</td>
</tr>
<tr>
<td>vm.kmem_size_min</td>
<td>0</td>
</tr>
<tr>
<td>vm.kmem_size_max</td>
<td>1319413950874</td>
</tr>
<tr>
<td>vfs.zfs.vol.unmap_enabled</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.vol.mode</td>
<td>2</td>
</tr>
<tr>
<td>vfs.zfs.sync_pass_rewrite</td>
<td>2</td>
</tr>
<tr>
<td>vfs.zfs.sync_pass_dont_compress</td>
<td>5</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>vfs.zfs.sync_pass_deferred_free</td>
<td>2</td>
</tr>
<tr>
<td>vfs.zfs.zio.exclude_metadata</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.zio.use_uma</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.cache_flush_disable</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.zil_replay_disable</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.version.zpl</td>
<td>5</td>
</tr>
<tr>
<td>vfs.zfs.version.spa</td>
<td>5000</td>
</tr>
<tr>
<td>vfs.zfs.version.acl</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.version.ioctl</td>
<td>5</td>
</tr>
<tr>
<td>vfs.zfs.debug</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.super_owner</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.min_auto_ashift</td>
<td>9</td>
</tr>
<tr>
<td>vfs.zfs.max_auto_ashift</td>
<td>13</td>
</tr>
<tr>
<td>vfs.zfs.vdev.write_gap_limit</td>
<td>4096</td>
</tr>
<tr>
<td>vfs.zfs.vdev.read_gap_limit</td>
<td>32768</td>
</tr>
<tr>
<td>vfs.zfs.vdev.aggregation_limit</td>
<td>131072</td>
</tr>
<tr>
<td>vfs.zfs.vdev.trim_max_active</td>
<td>64</td>
</tr>
<tr>
<td>vfs.zfs.vdev.trim_min_active</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.vdev.scrub_max_active</td>
<td>2</td>
</tr>
<tr>
<td>vfs.zfs.vdev.scrub_min_active</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.vdev.async_write_max_active</td>
<td>10</td>
</tr>
<tr>
<td>vfs.zfs.vdev.async_write_min_active</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.vdev.async_read_max_active</td>
<td>3</td>
</tr>
<tr>
<td>vfs.zfs.vdev.async_read_min_active</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.vdev.sync_write_max_active</td>
<td>10</td>
</tr>
<tr>
<td>vfs.zfs.vdev.sync_write_min_active</td>
<td>10</td>
</tr>
<tr>
<td>vfs.zfs.vdev.sync_read_max_active</td>
<td>10</td>
</tr>
<tr>
<td>vfs.zfs.vdev.sync_read_min_active</td>
<td>10</td>
</tr>
<tr>
<td>vfs.zfs.vdev.max_active</td>
<td>1000</td>
</tr>
<tr>
<td>vfs.zfs.vdev.async_write_active_max_dirty_percent60</td>
<td></td>
</tr>
<tr>
<td>vfs.zfs.vdev.async_write_active_min_dirty_percent30</td>
<td></td>
</tr>
<tr>
<td>vfs.zfs.vdev.mirror.non_rotating_seek_inc</td>
<td></td>
</tr>
<tr>
<td>vfs.zfs.vdev.mirror.non_rotating_inc</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.vdev.mirror.rotating_seek_offset</td>
<td>1048576</td>
</tr>
<tr>
<td>vfs.zfs.vdev.mirror.rotating_seek_inc</td>
<td>5</td>
</tr>
<tr>
<td>vfs.zfs.vdev.mirror.rotating_inc</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.vdev.trim_on_init</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.vdev.larger_ashift_minimal</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.vdev.bio_delete_disable</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.vdev.bio_flush_disable</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.vdev.cache.bshift</td>
<td>16</td>
</tr>
<tr>
<td>vfs.zfs.vdev.cache.size</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.vdev.cache.max</td>
<td>16384</td>
</tr>
<tr>
<td>vfs.zfs.vdev.metaslabs_per_vdev</td>
<td>200</td>
</tr>
<tr>
<td>vfs.zfs.vdev.trim_max_pending</td>
<td>10000</td>
</tr>
<tr>
<td>vfs.zfs.txg.timeout</td>
<td>5</td>
</tr>
<tr>
<td>vfs.zfs.trim.enabled</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.trim.max_interval</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.trim.timeout</td>
<td>30</td>
</tr>
<tr>
<td>vfs.zfs.trim.txg_delay</td>
<td>32</td>
</tr>
<tr>
<td>vfs.zfs.space_map_blksz</td>
<td>4096</td>
</tr>
<tr>
<td>vfs.zfs.spa_slop_shift</td>
<td>5</td>
</tr>
<tr>
<td>vfs.zfs.spa_asize_inflation</td>
<td>24</td>
</tr>
<tr>
<td>vfs.zfs.deadman_enabled</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.deadman_checktime_ms</td>
<td>5000</td>
</tr>
<tr>
<td>vfs.zfs.deadman_synctime_ms</td>
<td>1000000</td>
</tr>
<tr>
<td>vfs.zfs.recover</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.spa_load_verify_data</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.spa_load_verify_metadata</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.spa_load_verify_maxinflight</td>
<td>10000</td>
</tr>
<tr>
<td>vfs.zfs.check_hostid</td>
<td>1</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>vfs.zfs.mg_fragmentation_threshold</td>
<td>85</td>
</tr>
<tr>
<td>vfs.zfs.mg_noallocate_threshold</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.condense_pct</td>
<td>200</td>
</tr>
<tr>
<td>vfs.zfs.metaslab.bias_enabled</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.metaslab.lba_weighting_enabled</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.metaslab.fragmentation_factor_enabled1</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.metaslab.preload_enabled</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.metaslab.preload_limit</td>
<td>3</td>
</tr>
<tr>
<td>vfs.zfs.metaslab.unload_delay</td>
<td>8</td>
</tr>
<tr>
<td>vfs.zfs.metaslab.load_pct</td>
<td>50</td>
</tr>
<tr>
<td>vfs.zfs.metaslab.min_alloc_size</td>
<td>33554432</td>
</tr>
<tr>
<td>vfs.zfs.metaslab.df_free_pct</td>
<td>4</td>
</tr>
<tr>
<td>vfs.zfs.metaslab.df_alloc_threshold</td>
<td>131072</td>
</tr>
<tr>
<td>vfs.zfs.metaslab.debug_unload</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.metaslab.debug_load</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.metaslab.fragmentation_threshold</td>
<td>70</td>
</tr>
<tr>
<td>vfs.zfs.metaslab.gang_bang</td>
<td>16777217</td>
</tr>
<tr>
<td>vfs.zfs.free_bpoolj_enabled</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.free_max_blocks</td>
<td>18446744073709551615</td>
</tr>
<tr>
<td>vfs.zfs.no_scrub_prefetch</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.no_scrub_io</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.resilver_min_time_ms</td>
<td>3000</td>
</tr>
<tr>
<td>vfs.zfs.free_min_time_ms</td>
<td>1000</td>
</tr>
<tr>
<td>vfs.zfs.scan_min_time_ms</td>
<td>1000</td>
</tr>
<tr>
<td>vfs.zfs.scan_idle</td>
<td>50</td>
</tr>
<tr>
<td>vfs.zfs.scrub_delay</td>
<td>4</td>
</tr>
<tr>
<td>vfs.zfs.resilver_delay</td>
<td>2</td>
</tr>
<tr>
<td>vfs.zfs.top_maxinflight</td>
<td>32</td>
</tr>
<tr>
<td>vfs.zfs.delay_scale</td>
<td>5000000</td>
</tr>
<tr>
<td>vfs.zfs.delay_min_dirty_percent</td>
<td>60</td>
</tr>
<tr>
<td>vfs.zfs.dirty_data_sync</td>
<td>67108864</td>
</tr>
<tr>
<td>vfs.zfs.dirty_data_max_percent</td>
<td>10</td>
</tr>
<tr>
<td>vfs.zfs.dirty_data_max_max</td>
<td>4294967296</td>
</tr>
<tr>
<td>vfs.zfs.dirty_data_max_max</td>
<td>426512793</td>
</tr>
<tr>
<td>vfs.zfs.max_recordsize</td>
<td>1048576</td>
</tr>
<tr>
<td>vfs.zfs.zfetch.array_rd_sz</td>
<td>1048576</td>
</tr>
<tr>
<td>vfs.zfs.zfetch.max_distance</td>
<td>8388608</td>
</tr>
<tr>
<td>vfs.zfs.zfetch.min_sec_reap</td>
<td>2</td>
</tr>
<tr>
<td>vfs.zfs.zfetch.max_streams</td>
<td>8</td>
</tr>
<tr>
<td>vfs.zfs.prefetch_disable</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.mdcomp_disable</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.nopwrite_enabled</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.dedup.prefetch</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.l2c_only_size</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.mfu_ghost_data_lsize</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.mfu_ghost_metadata_lsize</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.mfu_ghost_size</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.mfu_data_lsize</td>
<td>26300416</td>
</tr>
<tr>
<td>vfs.zfs.mfu_metadata_lsize</td>
<td>1780736</td>
</tr>
<tr>
<td>vfs.zfs.mfu_size</td>
<td>29428736</td>
</tr>
<tr>
<td>vfs.zfs.mru_ghost_data_lsize</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.mru_ghost_metadata_lsize</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.mru_ghost_size</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.mru_data_lsize</td>
<td>122090496</td>
</tr>
<tr>
<td>vfs.zfs.mru_metadata_lsize</td>
<td>2235904</td>
</tr>
<tr>
<td>vfs.zfs.mru_size</td>
<td>139389440</td>
</tr>
<tr>
<td>vfs.zfs.anon_data_lsize</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.anon_metadata_lsize</td>
<td>0</td>
</tr>
<tr>
<td>vfs.zfs.anon_size</td>
<td>163840</td>
</tr>
<tr>
<td>vfs.zfs.l2arc_norw</td>
<td>1</td>
</tr>
<tr>
<td>vfs.zfs.l2arc_feed_again</td>
<td>1</td>
</tr>
</tbody>
</table>
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 reading man pages and searching for the meaning of unfamiliar acronyms is required. **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 the workload.

If any of the ZFS tunables are changed, continue to monitor the system to determine the effect of the change. It is recommended that the changes are tested first at the command line using `sysctl`. For example, to disable prefetch (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, it can be made permanent by creating a `sysctl` using the instructions in **Tunables** (page 105).

### 26.5 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)` (https://www.freebsd.org/cgi/man.cgi?query=twe) and `twa(4)` (https://www.freebsd.org/cgi/man.cgi?query=twa) drivers.

Before using this command, read its man page (https://www.cyberciti.biz/files/tw_cli.8.html) as it describes the terminology and provides some usage examples.

When `tw_cli` in Shell is entered, the prompt will change, indicating that interactive mode is enabled where all sorts of maintenance commands on the controller and its arrays can be run.

Alternately, one command can be specified 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/slt0 SEAGATE ST31000640SS
```
Or, to review the event log:

```
tw_cli /c0 show events
```

Use the drives to create units and export them to the operating system. When finished, run `camcontrol rescan all` to make them available in the FreeNAS® web interface.

26.6 MegaCli

MegaCli is the command line interface for the Broadcom 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 (http://tools.rapidsoft.de/perc/perc-cheat-sheet.html) can get you started.

26.7 freenas-debug

The FreeNAS® web interface 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 (page 341) to gather specific debugging information. To see a usage explanation listing all options, run the command without any options:

```
freenas-debug
Usage: /usr/local/bin/freenas-debug <options>
Where options are:

-A Dump all debug information
-B Dump System Configuration Database
-C Dump SMB Configuration
-I Dump IPMI Configuration
-M Dump SATA DOMs Information
-N Dump NFS Configuration
-S Dump SMART Information
-T Loader Configuration Information
-Z Remove old debug information
-a Dump Active Directory Configuration
-c Dump (AD|LDAP) Cache
-e Email debug log to this comma-delimited list of email addresses
-f Dump AFP Configuration
-g Dump GEOM Configuration
-h Dump Hardware Configuration
-i Dump iSCSI Configuration
-j Dump Jail Information
-l Dump LDAP Configuration
-n Dump Network Configuration
-s Dump SSL Configuration
-t Dump System Information
-v Dump Boot System File Verification Status and Inconsistencies
-y Dump Sysctl Configuration
-z Dump ZFS Configuration
```

Individual tests can be run alone. For example, when troubleshooting an Active Directory configuration, use:

```
freenas-debug -a
```

To collect the output of every module, use -A:

```
freenas-debug -A
```

For collecting debug information about a single pool, use zdb with -U /data/zfs/zpool.cache followed by the name of the pool:
zdb -U /data/zfs/zpool.cache pool1

See the [zdb(8) manual page](https://www.freebsd.org/cgi/man.cgi?query=zdb) for more information.

## 26.8 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* (page 341), *tmux* provides access to a command prompt while still giving access to the graphical administration `screen`

To start a session, simply type `tmux`. As seen in Figure 26.2, 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. 26.2: tmux Session](image)

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 *Shell* (page 341) is closed while *tmux* is running, it will detach its session. The next time Shell is open, run `tmux attach` to return to the previous session. To leave the *tmux* session entirely, type `exit`. If multiple windows are running, it is required to `exit` out of each first.

These resources provide more information about using *tmux*.
• A tmux Crash Course (https://robots.thoughtbot.com/a-tmux-crash-course)
• TMUX - The Terminal Multiplexer (http://blog.hawkhost.com/2010/06/28/tmux-the-terminal-multiplexer/)

## 26.9 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 (http://www.nongnu.org/dmidecode/sample/dmidecode.txt).

To view the BIOS report, type the command with no arguments:

```
$ dmidecode | more
```

dmidecode(8) (https://linux.die.net/man/8/dmidecode) describes the supported strings and types.

## 26.10 Midnight Commander

Midnight Commander is a program used to manage files from the shell. Open the application by running `mc`. The arrow keys are used to navigate and select files. Function keys are used to perform operations such as renaming, editing, and copying files. These resources provide more information about using Midnight Commander:

• Midnight Commander wikipedia page (https://en.wikipedia.org/wiki/Midnight_Commander)
• Midnight Commander website (https://midnight-commander.org/)
• `mc(1)` (https://www.freebsd.org/cgi/man.cgi?query=mc)
• Basic Tutorial (http://linuxcommand.org/lc3_adv_mc.php)
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 provide continued, collaborative development of the open source version.

Here is an overview of the features provided by ZFS:

**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 by selecting the **Pools** (page 168), clicking **Settings**, then the **Status** button. Checking scrub results can provide an early indication of potential disk problems.

Unlike traditional UNIX filesystems, **it is not necessary to define partition sizes when filesystems are created**. 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®, **Pools** (page 168) is used to create or extend 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. ZFS pools created on FreeNAS® version 9.2.1 or later use the recommended LZ4 compression algorithm.

**ZFS provides low-cost, instantaneous snapshots** of the specified pool, dataset, or zvol. Due to COW, snapshots initially take no additional space. The size of a 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 taken.
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 makes snapshots a clever way to keep a history of files, useful for recovering an older copy of a file or a deleted file. For this reason, many administrators take snapshots often, store them for a period of time, and store them on another system. Such a strategy allows the administrator to roll the system back to a specific time. If there is a catastrophic loss, an off-site snapshot can restore the system up to the last snapshot interval, within 15 minutes of the data loss, for example. 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, pool size, or compression settings.

**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 (https://pthree.org/2013/04/19/zfs-administration-appendix-a-visualizing-the-zfs-intent-log/). 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 (http://www.freenas.org/blog/zfs-zil-and-slog-demystified/)
- ZFS Intent Log (http://nex7.blogspot.com/2013/04/zfs-intent-log.html)

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** (page 341) to determine if the system will benefit from a SLOG. See this website (http://www.richardelling.com/Home/scripts-and-programs-1/zilstat) for usage information.

ZFS currently uses 16 GiB 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. The ZFS pool version is checked from the **Shell** (page 341) 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, which reduces read latency. FreeNAS® adds ARC stats to `top(1)` (https://www.freebsd.org/cgi/man.cgi?query=top) 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 (http://www.brendangregg.com/blog/2008-07-22/zfs-l2arc.html). Additional read data is cached here, which can increase random read performance. L2ARC does **not** reduce the need for sufficient RAM. In fact, L2ARC needs RAM to function. If there is not enough RAM for a adequately-sized ARC, adding an L2ARC will not increase performance. Performance actually decreases in most cases, potentially causing system instability. RAM is always faster than disks, so always add as much RAM as possible before considering whether the system can benefit from an L2ARC device.

When applications perform large amounts of **random** reads on a dataset small enough to fit into L2ARC, read performance can be increased by adding a dedicated cache device. SSD cache devices only help if the active data is larger than system RAM but small enough that a significant percentage fits on the SSD. As a general rule, L2ARC should not be added to a system with less than 32 GiB of RAM, and the size of an L2ARC should not exceed ten times 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 device, monitor its effectiveness using tools such as `arcstat`.

To increase the size of an existing L2ARC, stripe another cache device with it. The web interface will always stripe L2ARC, not mirror it, as the contents of L2ARC are recreated at boot. Failure of an individual SSD from an L2ARC pool will not affect the integrity of the pool, but may have an impact on read performance, depending on the workload and the ratio of dataset size to cache size. Note that dedicated L2ARC devices 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 the 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. With 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 (https://www.delphix.com/blog/delphix-engineering/zfs-raidz-stripe-width-or-how-i-learned-stop-worrying-and-love-raidz) for details.

These resources can also help determine the RAID configuration best suited to the specific storage requirements:


**Warning:** RAID AND DISK REDUNDANCY ARE NOT A SUBSTITUTE FOR A RELIABLE BACKUP STRATEGY. BAD THINGS HAPPEN AND A GOOD BACKUP STRATEGY IS STILL REQUIRED TO PROTECT VALUABLE DATA. See Periodic Snapshot Tasks (page 136) and Replication Tasks (page 146) to use replicated ZFS snapshots as part of a backup strategy.

ZFS manages devices. When an individual drive in a mirror or RAID fails and is replaced by the user, ZFS adds the replacement device to the vdev and copies redundant data to it in a process called resilvering. Hardware RAID controllers usually have no way of knowing which blocks were in use and must copy every block to the new device. ZFS only copies blocks that are in use, reducing the time it takes to rebuild the vdev. Resilvering is also interruptable. After an interruption, resilvering resumes where it left off rather than starting from the beginning.

While ZFS provides many benefits, there are some caveats:

- 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%.
- 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 TiB in size.

- Using drives of equal sizes is recommended 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.

For those new to ZFS, the Wikipedia entry on ZFS (https://en.wikipedia.org/wiki/Zfs) provides an excellent starting point to learn more about its features. These resources are also useful for reference:

- Becoming a ZFS Ninja Part 1 (video) (https://www.youtube.com/watch?v=tPsV_8k-aVU) and Becoming a ZFS Ninja Part 2 (video) (https://www.youtube.com/watch?v=wy6cjRVHiYU)
- ZFS: The Last Word in File Systems - Part 1 (video) (https://www.youtube.com/watch?v=aTXKxpL_0OI&list=PL5AD0E439599D3FA)
- The Zettabyte Filesystem (https://www.youtube.com/watch?v=ptY6-K78McY)

### 27.1 ZFS Feature Flags

To differentiate itself from Oracle ZFS version numbers, OpenZFS uses feature flags. Feature flags are used to tag features with unique names 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.

See zpool-features(7) (https://www.freebsd.org/cgi/man.cgi?query=zpool-features) for a complete listing of all OpenZFS feature flags available on FreeBSD.
An open source, community-supported FreeNAS® driver for OpenStack is available at https://github.com/ixsystems/cinder.
This section offers FreeNAS® configuration recommendations and troubleshooting tips when using FreeNAS® with a VMware (https://www.vmware.com/) hypervisor.

### 29.1 FreeNAS® as a VMware Guest

This section has recommendations for configuring FreeNAS® when it is installed as a Virtual Machine (VM) in VMware.

To create a new FreeNAS® Virtual Machine in VMware, see the VMware ESXi (page 55) section of this guide.

Configure and use the vmx(4) (https://www.freebsd.org/cgi/man.cgi?query=vmx) drivers for the FreeNAS® system.


Make sure MAC spoofing and promiscuous mode are enabled on the switch first, and then the port group the VM is using.

### 29.2 Hosting VMware Storage with FreeNAS®

This section has recommendations for configuring FreeNAS® when the system is being used as a VMware datastore.

Make sure guest VMs have the latest version of vmware-tools installed. VMware provides instructions to install VMware Tools (https://www.vmware.com/support/ws5/doc/new_guest_tools_ws.html) on different guest operating systems.

Increase the VM disk timeouts to better survive long disk operations. Set the timeout to a minimum of 300 seconds. See the guest operating system documentation for setting disk timeouts. VMware provides instructions for setting disk timeouts on some specific guest operating systems:

- Linux guests running kernel version 2.6: https://kb.vmware.com/s/article/1009465

When FreeNAS® is used as a VMware datastore, coordinated ZFS and VMware snapshots (page 194) can be used.

### 29.3 VAAI for iSCSI

VMware’s vStorage APIs for Array Integration, or VAAI, allows storage tasks such as large data moves to be offloaded from the virtualization hardware to the storage array. These operations are performed locally on the NAS without transferring bulk data over the network.
VAAI for iSCSI supports these operations:

- **Atomic Test and Set (ATS)** allows multiple initiators to synchronize LUN access in a fine-grained manner rather than locking the whole LUN and preventing other hosts from accessing the same LUN simultaneously.

- **Clone Blocks (XCOPY)** copies disk blocks on the NAS. Copies occur locally rather than over the network. This operation is similar to [Microsoft ODX](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831628(v=ws.11)).

- **LUN Reporting** allows a hypervisor to query the NAS to determine whether a LUN is using thin provisioning.

- **Stun** pauses virtual machines when a pool runs out of space. The space issue can then be fixed and the virtual machines can continue rather than reporting write errors.

- **Threshold Warning** the system reports a warning when a configurable capacity is reached. In FreeNAS®, this threshold is configured at the pool level when using zvols (see Table 13.2) or at the extent level (see Table 13.7) for both file and device based extents. Typically, the warning is set at the pool level, unless file extents are used, in which case it must be set at the extent level.

- **Unmap** informs FreeNAS® that the space occupied by deleted files should be freed. Without unmap, the NAS is unaware of freed space created when the initiator deletes files. For this feature to work, the initiator must support the unmap command.

- **Zero Blocks** or **Write Same** zeros out disk regions. When allocating virtual machines with thick provisioning, the zero write is done locally, rather than over the network. This makes virtual machine creation and any other zeroing of disk regions much quicker.
A REST (https://en.wikipedia.org/wiki/Representational_state_transfer) 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 (https://tools.ietf.org/html/rfc2616.html), such as GET, PUT, POST, or DELETE.

As shown in Figure 30.1, an online version of the API is available at api.ixsystems.com/freenas (https://api.ixsystems.com/freenas/).

The rest of this section shows code examples to illustrate the use of the API.

**Note:** A new API was released with FreeNAS® 11.1. The previous API is still present and in use because it is feature-complete. Documentation for the new API is available on the FreeNAS® system at the /api/docs/ URL. For example, if the FreeNAS® system is at IP address 192.168.1.119, enter http://192.168.1.119/api/docs/ in a browser to see the API documentation. Work is under way to make the new API feature-complete. The new APIv2 uses WebSockets (https://developer.mozilla.org/en-US/docs/Web/API/WebSockets_API). This advanced technology
makes it possible to open interactive communication sessions between web browsers and servers, allowing event-driven responses without the need to poll the server for a reply. When APIv2 is feature-complete, the FreeNAS® documentation will include relevant examples that make use of the new API.

30.1 A Simple API Example

The API directory of the FreeNAS® GitHub repository (https://github.com/freenas/freenas/tree/master/examples/api) 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 pool or dataset for the user Home Directory. After creating the user, start the SSH service in Services → SSH. 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. Do not change the text in black. After saving changes, run the script by typing `python scriptname.py`. The new user account will appear in Accounts → Users in the FreeNAS® web interface.

Here is the example script with an explanation of the line numbers below it.

```python
import json
import requests
r = requests.post('https://freenas.mydomain/api/v1.0/account/users/',
 auth=('root', 'freenas'),
 headers={'Content-Type': 'application/json'},
 verify=False,
 data=json.dumps(
    {'bsdusr_uid': '1100',
     'bsdusr_username': 'myuser',
     'bsdusr_mode': '755',
     'bsdusr_creategroup': 'True',
     'bsdusr_password': '12345',
     'bsdusr_shell': '/usr/local/bin/bash',
     'bsdusr_full_name': 'Full Name',
     'bsdusr_email': 'name@provider.com',
   })
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 Network → Global Configuration. Note that the script will fail if the machine running it is unable to resolve that hostname. Go to System → General and set the Protocol to HTTP.

**Line 5:** replace `freenas` with the password used to access the FreeNAS® system.

**Line 7:** to force validation of the SSL certificate while using HTTPS, change `False` to `True`.

**Lines 8-16:** set the values for the user being created. The user section at api.ixsystems.com/freenas (https://api.ixsystems.com/freenas) 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 30.1 summarizes acceptable values. This resource uses JSON, so the boolean values are `True` or `False`.

Table 30.1
### Table 30.1: JSON Parameters for Users Create Resource

<table>
<thead>
<tr>
<th>JSON Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bsdusr_username</td>
<td>string</td>
<td>Maximum 32 characters, though a maximum of 8 is recommended for interoperability. Can include numerals but cannot include a space.</td>
</tr>
<tr>
<td>bsdusr_full_name</td>
<td>string</td>
<td>May contain spaces and uppercase characters.</td>
</tr>
<tr>
<td>bsdusr_password</td>
<td>string</td>
<td>Can include a mix of upper and lowercase letters, characters, and numbers.</td>
</tr>
<tr>
<td>bsdusr_uid</td>
<td>integer</td>
<td>By convention, user accounts have an ID greater than 1000 with a maximum allowable value of 65,535.</td>
</tr>
<tr>
<td>bsdusr_group</td>
<td>integer</td>
<td>If bsdusr_creategroup is set to False, specify the numeric ID of the group to create.</td>
</tr>
<tr>
<td>bsdusr_creategroup</td>
<td>boolean</td>
<td>Set True to automatically create a primary group with the same numeric ID as bsdusr_uid.</td>
</tr>
<tr>
<td>bsdusr_mode</td>
<td>string</td>
<td>Sets default numeric UNIX permissions of a user home directory.</td>
</tr>
<tr>
<td>bsdusr_shell</td>
<td>string</td>
<td>Specify the full path to a UNIX shell that is installed on the system.</td>
</tr>
<tr>
<td>bsdusr_password_disabled</td>
<td>boolean</td>
<td>Set to True to disable user login.</td>
</tr>
<tr>
<td>bsdusr_locked</td>
<td>boolean</td>
<td>Set to True to disable user login.</td>
</tr>
<tr>
<td>bsdusr_sudo</td>
<td>boolean</td>
<td>Set to True to enable sudo for the user.</td>
</tr>
<tr>
<td>bsdusr_sshpubkey</td>
<td>string</td>
<td>Contents of SSH authorized keys file.</td>
</tr>
</tbody>
</table>

**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`.

## 30.2 A More Complex Example

This section provides a walk-through of a more complex example found in the `startup.py` script. Use the search bar within the API documentation to quickly locate the JSON parameters used here. This example defines a class and several methods to create a ZFS pool, 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 Python modules are imported to provide parsing functions for command line arguments:

```python
import argparse
import sys
```

It then creates a `Startup` class which is started with the hostname, username, and password provided by the user through the command line:

```python
class Startup(object):
    def __init__(self, hostname, user, secret):
        self._hostname = hostname
        self._user = user
        self._secret = secret
        self._ep = 'http://%s/api/v1.0' % hostname

    def request(self, resource, method='GET', data=None):
        if data is None:
            data = ''
        r = requests.request(
            method,
            '%s/%s' % (self._ep, resource),
            data=json.dumps(data),
            headers={'Content-Type': "application/json"},
            auth=(self._user, self._secret),
```
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:

```python
def _get_disks(self):
    disks = self.request('storage/disk')
    return [disk['disk_name'] for disk in disks]

def create_pool(self):
    disks = self._get_disks()
    self.request('storage/volume', method='POST', data={
        'volume_name': 'tank',
        'layout': [
            {'vdevtype': 'stripe', 'disks': disks},
        ]
    })
```

The `create_dataset` method is defined which creates a dataset named `MyShare`:

```python
def create_dataset(self):
    self.request('storage/volume/tank/datasets', method='POST', data={
        'name': 'MyShare',
    })
```

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:

```python
def create_cifs_share(self):
    self.request('sharing/cifs', method='POST', data={
        'cifs_name': 'My Test Share',
        'cifs_path': '/mnt/tank/MyShare',
        'cifs_guestonly': True
    })
```

Finally, the `service_start` method enables the CIFS service. The `srv_enable` JSON parameter is described in the `Services` resource:

```python
def service_start(self, name):
    self.request('services/services/%s' % name, method='PUT', data={
        'srv_enable': True,
    })
```