Spectra Verde NAS Solution

User Guide

SpectraLogic.com

Copyright

Copyright © 2013-2020 Spectra Logic Corporation. All rights reserved. This item and the information contained herein are the property of Spectra Logic Corporation.

Notices

Except as expressly stated herein, Spectra Logic Corporation makes its products and associated documentation on an "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, BOTH OF WHICH ARE EXPRESSLY DISCLAIMED. In no event shall Spectra Logic be liable for any loss of profits, loss of business, loss of use or data, interruption of business, or for indirect, special, incidental or consequential damages of any kind, even if Spectra Logic has been advised of the possibility of such damages arising from any defect or error.

Information furnished in this manual is believed to be accurate and reliable. However, no responsibility is assumed by Spectra Logic for its use. Due to continuing research and development, Spectra Logic may revise this publication from time to time without notice, and reserves the right to change any product specification at any time without notice.

Trademarks

BlackPearl, BlueScale, CC, Spectra, SpectraGuard, Spectra Logic, TeraPack, TFinity, and TranScale are registered trademarks of Spectra Logic Corporation. Eon Protect, MigrationPass, SeeVault, and Spectra StorCycle are trademarks of Spectra Logic Corporation. All rights reserved worldwide. All other trademarks and registered trademarks are the property of their respective owners.

Part Number

90990079 Revision W

Revision History

Revision	Date	Description
H	September 2015	Update for Verde 2.2 release.
I	November 2015	Additional updates for Verde 2.2 release.
J	March 2016	Update for Verde 3.1 release.
K	April 2016	Update for Verde 3.1.1 release.
L	May 2016	Update for Verde 3.1.2 release.
M	June 2016	Update for Verde 3.1.3 release.
N		Never Released.
O	December 2016	Update for Verde 3.1.4 release.
P	April 2017	Update for Verde 3.5.0 release.
Q	September 2017	Update for Verde 4.0 release.
U	January 2018	Update for Verde 4.1.1 release. Revisions R, S, & T were never released.
V	August 2018	Update for Verde 5.0 release.
W	February 2020	Update for Verde 5.1.4 release.

Note: To make sure you have the most current version of this guide check the Spectra Logic Technical Support portal at support.spectralogic.com/documentation/user-guides/.

To make sure you have the release notes for the most current version of the Verde Release Notes, check the Spectra Logic Technical Support portal at support.spectralogic.com/documentation/release-notes/. You must sign into the portal before viewing Release Notes. The release notes contain updates to the *User Guide* since the last time it was revised.

End User License Agreement

1. READ CAREFULLY

YOU SHOULD READ THE FOLLOWING TERMS AND CONDITIONS BEFORE ACCEPTING THIS END-USER LICENSE AGREEMENT ("EULA"). THIS EULA IS A LEGAL AGREEMENT BETWEEN YOUR ORGANIZATION, THE END USER, AND SPECTRA LOGIC CORPORATION ("SPECTRA") FOR THE SPECTRA SOFTWARE PRODUCT WHICH INCLUDES COMPUTER SOFTWARE AND MAY INCLUDE ASSOCIATED MEDIA, PRINTED MEDIA, AND "ONLINE" OR ELECTRONIC DOCUMENTATION (COLLECTIVELY, "SOFTWARE PRODUCT"). BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE PRODUCT, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MAY NOT INSTALL, COPY, DOWNLOAD OR USE THE SOFTWARE PRODUCT. YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

2. OWNERSHIP

It is understood and agreed that Spectra Logic Corporation, a Delaware corporation with offices at 6285 Lookout Road, Boulder, CO 80301 ("Licensor") is the owner of all right, title and interest to the Software Product, regardless of the media or form of the original download, whether by the World Wide Web, disk or otherwise. You, as licensee ("Licensee") through your downloading, installing, copying or use of this product do not acquire any ownership rights to the Software Product.

3. GENERAL

The Software Product is licensed, not sold, to you by Spectra for use only under the terms of this EULA. The Software Product is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The rights granted herein are limited to Spectra's and its licensors' intellectual property rights in the Software Product and do not include any other patents or intellectual property rights. The terms of this EULA will govern any software upgrades provided by Spectra that replace and/or supplement the original Software Product, unless such upgrade is accompanied by a separate license in which case the terms of that license will govern.

4. SOFTWARE PRODUCT

The Software Product, as used in this EULA, means, collectively and/or as applicable:

- The Software Product package;
- Any and all contents, components, attachments, software, media, and code with which this Agreement is provided and delivered;
- Any and all images, photographs, art, art work, clip art, fonts or other artistic works (the "Art Work");
- Related explanatory written materials and instructions, and any other possible documentation related thereto ("Documentation"); and
- Upgrades, modified versions, updates, additions and copies of the Software Product (the "Upgrades"), if any, licensed to by Spectra under this EULA.

5. GRANT OF LICENSE AND RESTRICTIONS

A. Spectra grants you a non-exclusive, non-transferable End-User license right to install the Software Product solely for the purpose for which it was created.

B. Unless provided otherwise in the Documentation or by prior express written consent of Spectra, you shall not display, modify, reproduce and distribute any Art Work, or portion(s) thereof, included with or relating to the Software Product, if any. Any such authorized display, modification, reproduction and distribution shall be in full accord with this EULA. Under no circumstances will your use, display, modification, reproduction and distribution of the Art Work give you any Intellectual Property or Proprietary Rights of the Art Work. All rights, title, and interest belong solely to Spectra.

C. Except for the initial loading of the Software Product, you shall not, without Spectra's express written consent:

- Copy or reproduce the Software Product; or
- Modify, adapt, or create derivative works based on the Software Product or any accompanying materials.

6. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

A. Spectra will provide you with support services related to the Software Product ("Support"). Such Support will be provided in accordance with the Spectra Master Support Agreement, available for download and viewing on the Spectra Corporate Web site. Use of Support is governed by this EULA and Spectra's Master Support Agreement.

B. Any supplemental software, code, content, or media provided to you in the course of Support shall be considered part of the Software Product and subject to the terms and conditions of this EULA.

C. Spectra retains all right, title, and interest in and to the Software Product, and any rights not granted to you herein are reserved by Spectra. You hereby expressly agree not to extract information, reverse engineer, disassemble, decompile, or translate the Software Product, or otherwise attempt to derive the source code of the Software, except to the extent allowed under any applicable law. In the event that such activities are permitted by applicable law, any information you, or your authorized agent, discover shall be promptly disclosed to Spectra and shall be deemed the confidential information of Spectra.

D. You shall not modify, sublicense, assign, or transfer the Software Product or any rights under this EULA, except as expressly provided in this EULA. Any attempt to sublicense, assign, or transfer any of the rights, duties, or obligations will be void.

E. You may permanently transfer all of your rights under this EULA, provided you retain no copies. The other party must agree to accept the terms and conditions of the EULA.

7. ALL RESERVED

All rights not expressly granted herein are reserved by Spectra.

8. TERM

A. This License is effective until terminated. Licensee may terminate it at any time by destroying the Software Product with all copies, full or partial, and removing all of its component parts.

B. Your rights under this EULA will terminate automatically without notice from Spectra if you fail to comply with any term(s) or condition(s) of this EULA. In such event, no notice shall be required by Spectra to effect such termination.

C. Upon termination of this EULA, you shall cease all use of the Software Product and destroy all copies, full or partial, together with all backup copies, modifications, printed or written materials, and merged portions in any form and remove all component parts of the Software Product.

9. INTELLECTUAL PROPERTY RIGHTS

A. Spectra shall retain all right, title, and interest in the Software Product and to any modifications or improvements made thereto, and any upgrades, updates or Documentation provided to End User. End User will not obtain any rights in the Software Product, its updates, upgrades, and Documentation, as a result of its responsibilities hereunder.

B. B. End User acknowledges Spectra's exclusive rights in the Software Product and that the Software Product is unique and original to Spectra and that Spectra is owner thereof. Unless otherwise permitted by law, End User shall not, at any time during or after the effective Term of the Agreement, dispute or contest, directly or indirectly, Spectra's exclusive right and title to the Software Product or the validity thereof.

10. U.S. GOVERNMENT END USERS

The Software Product and related documentation are "Commercial Items," as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable. The Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other End Users pursuant to the terms and conditions herein. Unpublished rights reserved under the copyright laws of the United States.

11. EXPORT LAW ASSURANCES

You may not use or otherwise export or re-export the Software Product except as authorized by United States law and the laws of the jurisdiction in which the Software Product was obtained. In particular, but without limitation, the Software Product may not be exported or re-exported (a) into (or to a nation or resident of) any U.S. embargoed countries or (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce Denied Persons List or Entity List. By installing or using any component of the Software Product, you represent and warrant that you are not located in, under control of, or a national or resident of any such country or on any such list.

12. DISCLAIMER OF WARRANTIES

YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT USE OF THE SOFTWARE PRODUCT IS AT YOUR SOLE RISK AND THAT THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT IS WITH YOU. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND EXCEPT AS MAY BE STATED IN THE SPECTRA MASTER SERVICE AGREEMENT, THE SOFTWARE PRODUCT IS PROVIDED "AS IS," WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND SPECTRA AND SPECTRA'S AFFILIATES (COLLECTIVELY REFERRED TO AS "SPECTRA" FOR THE PURPOSES OF SECTIONS 12 AND 13) HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE SOFTWARE PRODUCT, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF ACCURACY, OF QUIET ENJOYMENT, AND NON-INFRINGEMENT OF THIRD-PARTY RIGHTS. SPECTRA DOES NOT WARRANT AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE SOFTWARE PRODUCT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE PRODUCT WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE PRODUCT WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY SPECTRA OR A SPECTRA AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATION ON APPLICABLE STATUTORY RIGHTS OF A CONSUMER, SO THE ABOVE EXCLUSION AND LIMITATIONS MAY NOT APPLY TO YOU.

13. LIMITATION OF LIABILITY

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SPECTRA, ITS AFFILIATES OR LICENSEES, BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF SPECTRA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, SPECTRA'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS EULA SHALL BE LIMITED TO THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE PRODUCT; PROVIDED HOWEVER, IF YOU HAVE ENTERED INTO A MASTER SUPPORT AGREEMENT, SPECTRA'S ENTIRE LIABILITY REGARDING SUPPORT SERVICES SHALL BE GOVERNED BY THE TERMS OF THAT AGREEMENT. BECAUSE SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

14. CONTROLLING LAW AND SEVERABILITY

This EULA will be governed by and construed in accordance with the laws of the State of Colorado, as applied to agreements entered into and to be performed entirely within Colorado between Colorado residents. This EULA shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. If for any reason a court of competent jurisdiction finds any provision, or portion thereof, to be unenforceable, the remainder of this EULA shall continue in full force and effect.

Contacting Spectra Logic

To Obtain General Information

Spectra Logic Website: www.spectralogic.com

United States Headquarters

Spectra Logic Corporation
6285 Lookout Road
Boulder, CO 80301
USA
Phone: 1.800.833.1132 or 1.303.449.6400
International: 1.303.449.6400
Fax: 1.303.939.8844

European Office

Spectra Logic Europe Ltd.
329 Doncastle Road
Bracknell
Berks, RG12 8PE
United Kingdom
Phone: 44 (0) 870.112.2150
Fax: 44 (0) 870.112.2175

Spectra Logic Technical Support

Technical Support Portal: support.spectralogic.com

United States and Canada

Phone:
Toll free US and Canada: 1.800.227.4637
International: 1.303.449.0160

Europe, Middle East, Africa

Phone: 44 (0) 870.112.2185

Deutsch Sprechende Kunden

Phone: 49 (0) 6028.9796.507
Email: spectralogic@stortrec.de

Mexico, Central and South America, Asia, Australia, and New Zealand

Phone: 1.303.449.0160

Spectra Logic Sales

Website: shop.spectralogic.com

United States and Canada

Phone: 1.800.833.1132 or 1.303.449.6400
Fax: 1.303.939.8844
Email: sales@spectralogic.com

Europe

Phone: 44 (0) 870.112.2150
Fax: 44 (0) 870.112.2175
Email: eurosales@spectralogic.com

To Obtain Documentation

Spectra Logic Website: support.spectralogic.com/documentation

Contents

INTENDED AUDIENCE 15
VERDE USER INTERFACE SCREENS 15
RELATED INFORMATION 16
Related Publications 16

Chapter 1 – Product Overview 18

OVERVIEW 19
FEATURES 19
COMPONENTS 21
Front View of Master Nodes 21
Rear View of Master Nodes 23
Rear Panel of Master Nodes 25
Front View of the Verde Enterprise Expansion Node 27
Rear View of the Verde Enterprise Expansion Node 28
Front View of the Verde Archive Expansion Node 29
Rear View of the Verde Archive Expansion Node 30
Front View of the 107-Drive Disk Expansion Node 31
Rear View of the 107-Drive Disk Expansion Node 32
SOFTWARE 33
Operating System 33
Logical Volume Manager and File System 33
NFS and CIFS Servers 33
VERDE USER INTERFACE 33
Menus 34
Status Icons 37
Supported Browsers 37
COMMAND LINE INTERFACE 37

Chapter 2 – Initial Configuration 38

BEFORE YOU BEGIN 39
CONNECT ETHERNET CABLES 39
POWER ON THE VERDE NAS SOLUTION 39
Verde Master Nodes and Verde Enterprise Expansion Nodes 40
Verde NAS Solution with Archive Expansion Nodes or 107-Drive Disk Expansion Node 40

CONFIGURE THE VERDE MANAGEMENT PORT 42
AUTOMATICALLY IMPORT ACTIVATION KEYS 43
LOG IN TO THE VERDE USER INTERFACE 44
CONFIGURE THE DATA CONNECTION 46
Configure an Aggregate Port Data Connection 46
Configure a Single Port Data Connection 49
Configure a Static Route 50
CREATE A USER 52
Description of User Types 52
Create a User 53
NEXT STEPS 54

Chapter 3 – Configuring Network Attached Storage 55

OVERVIEW OF NAS STORAGE POOLS, VOLUMES, AND SHARES 56
Storage Pools 56
Volumes and Shares 56
Naming Considerations 56
CREATE A STORAGE POOL 57
CREATE A VOLUME 60
CREATE A SHARE 63
Create a CIFS Share 63
Create an NFS Share 67
CONFIGURE NAS SERVICES 68
Configure the CIFS Service 69
Configure the NFI Service 69
Configure the NFS Service 70
Configure the NAS Replication Service 70
CONFIGURE REPLICATION 71
Configure the NAS Replication Service 71
Configure the Target System 73
Configure Volumes for Replication 73

Chapter 4 – Managing Network Attached Storage 77

MANAGING STORAGE POOLS 78
Edit a Storage Pool 78
Expand a Storage Pool 79
Delete a Storage Pool 80

MANAGING VOLUMES 80
Move a Volume 81
Cancel a Volume Move 81
Edit a Volume 82
Delete a Volume 84
VOLUME SNAPSHOTS 84
Create a Snapshot 85
Create a Snapshot Schedule 86
Delete a Snapshot Schedule 88
Delete a Snapshot 89
Restore to a Snapshot 90
Retrieve a Single File from a Snapshot 91
MANAGING SHARES 92
Edit a CIFS Share 92
Edit an NFS Share 92
Delete a Share 93
MANAGING NAS REPLICATION 94
Manually Start NAS Replication 94
Cancel a NAS Replication In Progress 95
Restoring Files from a NAS Replication Target 96
Disable a NAS Replication for a Volume 96
Edit the NAS Replication Service 97
Delete the NAS Replication Service Configuration 98

Chapter 5 – Configuring a Verde NAS Solution 100

CONFIGURE NETWORK CONNECTIONS AND SETTINGS 101
Configure Ethernet Ports 101
Configure DNS Settings 107
Configure SMTP Settings 108
Configure Date and Time 109
Edit the System Name 110
CONFIGURE NETWORKING SERVICES 111
Configure the Active Directory Service 112
Configure the SNMP Service 117
CONFIGURE AND USE ENCRYPTION 119
Configure the Encryption Service 119
Change the Encryption Password 121
Unlock the Self-Encrypting Drives 122
Create an Encryption Password USB Key 122
PSID Erase an Encryption Drive 123

CONFIGURE USERS 125
Description of User Types 125
Create a User 125
Edit a User 125
Delete a User 126
CONFIGURE CERTIFICATES 126
MANUALLY ENTER ACTIVATION KEYS 127

Chapter 6 – Monitoring a Verde NAS Solution 129

MONITOR THE VERDE NAS SOLUTION 130
Front Bezel Visual Status Beacon 131
Configure the Visual Status Beacon Color 132
System Status LEDs 133
View System Messages 134
View the Status of Hardware Components 135
View the Status of Pools 136
View the Status of Volumes 139
View the Status of Shares 139
View the Status of Services 140
View Performance Metrics 141
View Reports 143
REBOOT OR SHUT DOWN A VERDE NAS SOLUTION 144
Using the Verde User Interface 144
Power-Cycle Reset 145
EXIT THE VERDE USER INTERFACE 145

Chapter 7 – Using AutoSupport 146

ABOUT AUTOSUPPORT 147
ENTER CONTACT INFORMATION 147
CONFIGURE MAIL RECIPIENTS 148
Add a New Recipient 148
Edit a Mail Recipient 149
Send a Test Email 150
Delete a Mail Recipient 151
LOG SETS 151
Configure a Log Set Schedule 152
Manually Generate Log Sets 153
Email a Log Set 153
Download a Log Set 154
Delete a Log Set 154

Chapter 8 – Maintaining a Verde NAS Solution 155

DATA INTEGRITY VERIFICATION 156
Cancel Data Integrity Verification 156
INITIATE RSC BACKUP 157
ACCESSING THE TECHNICAL SUPPORT PORTAL 157
Create an Account 157
Log Into the Portal 159
CONFIGURING AUTOMATED SOFTWARE UPLOAD 160
UPDATING SOFTWARE 161
Check the Current Software Version 161
Download and Stage the Updated Software 163
Install the Update 165
INSTALLING A NEW DATA DRIVE 166
Ensure ESD Protection 166
Install the Drive 167
REPLACING A FAILED COMPONENT 169
Identify the Failed Component 169

Chapter 9 – Troubleshooting and Support 172

RESOLVING A MANAGEMENT PORT IP ADDRESS CONFLICT . . 173
Using the Console 173
Using a Separate Computer 173
NETWORK SETUP TIPS 175
Configuration 175
Connectivity to the Network 175
Troubleshooting 178
Tools 178
SPECTRA LOGIC TECHNICAL SUPPORT 179
Before Contacting Support 179
Determine the System Serial Number 180
Open a Support Ticket 180
REMOTE SUPPORT 183
Enable Remote Support 184
Disable Remote Support 185
OVERVIEW 186
REQUIREMENTS 186
SPECIAL CONSIDERATIONS FOR READING TAPES IN A NON-BLACKPEARL ENVIRONMENT 187
CONFIGURE A BLACKPEARL SYSTEM FOR VERSIONING 188

CONFIGURE NETWORK FILE INTERFACE 191
Configure the NFI Service 191
Configure a Volume 192
NEXT STEPS 197
RESTORING FILES FROM AN NFI TARGET BLACKPEARL SYSTEM 197
Restore Files Using the Eon Browser 198
Restore Files Using the Deep Storage Browser 198
Restore Files Using a Spectra S3 Client 202
DATA STORAGE SPECIFICATIONS 204
Verde 2U and 4U Master Nodes 204
Verde Enterprise Expansion Node 204
Verde Archive Expansion Node 204
107-Drive Disk Expansion Node 205
CAPACITY 205
SYSTEM SPECIFICATION 206
Verde 2U Master Node 206
Verde 4U Master Node 207
SIZE AND WEIGHT 207
Verde 2U Master Node 207
Verde 4U Master Node and Verde Enterprise Expansion Node 208
Verde Archive Expansion Node 208
107-Drive Disk Expansion Node 209
POWER REQUIREMENTS 209
Input Power Requirements 209
Power Cords 211
INTERFACE SPECIFICATIONS 213
Verde NAS Solution Interface Connectors 213
Expansion Node Interface Connectors 213
Network Interface Cables 214
Universal Serial Bus (USB) Support 214
ENVIRONMENTAL SPECIFICATIONS 215
Verde Master Nodes and Verde Enterprise Expansion Node 215
Verde Archive Expansion Node 215
107-Drive Disk Expansion Node 216
Heat Generation 216
COMPONENTS 221
Front View of Master Nodes and Expansion Node 221
Rear View of Master Nodes 222
Rear Panel 223

SPECIFICATIONS 224
System Specification 224
Interface Specifications 225
Interface Connectors 225
Network Interface Cables 226
EU DECLARATION OF CONFORMITY 227
Certifications 228
CE MARKING 229
FCC NOTICE 229
SAFETY STANDARDS AND COMPLIANCE 229
Waste of Electronic and Electrical Equipment (WEEE) Directive . 229
Restriction of Hazardous Substances in Electrical and Electronic Equipment (RoHS) 230
RECYCLING YOUR VERDE NAS SOLUTION 230
CONFLICT MINERALS POLICY 230
APACHE 231
FREEBSD 231
JAVA 232
SAMBA 240
NGINX 240
RUBY 241
RUBY ON RAILS 242
ZFS 243
INCLUDED PACKAGES 243

About This Guide

This guide describes how to configure, monitor, and maintain the Spectra® Verde® NAS Solution master node, which is referred to as the *master node* in these instructions.

This guide also describes the site preparation requirements for the Spectra Verde enterprise expansion node, and the Verde archive expansion node, which are referred to as *expansion nodes* in these instructions. The expansion nodes are used in conjunction with the master node and cannot be used as a stand-alone product.

When instructions in this guide apply to both the Verde NAS Solution master node and expansion nodes, *the system* is used to refer to both.

This guide also describes how to use the Spectra Network File Interface, which is based on the Verde hardware platform.

Intended Audience

This guide is intended for data center administrators and operators who maintain and operate file storage systems. The information in this guide assumes a familiarity with computing terminology, RAID technology, SAS connectivity, and Ethernet networking. You also need to be familiar with installing, configuring, and using data file storage and archival software.

Verde User Interface Screens

The Verde user interface changes as new features are added or other modifications are made. Therefore, the screens you see in the Verde user interface may differ from those shown in this guide.

RELATED INFORMATION

This section contains information about this document and other documents related to the Spectra Verde NAS Solution.

Typographical Conventions

This document uses the following conventions to highlight important information:

WARNING Read text marked by the "Warning" icon for information you must know to avoid personal injury.

Caution Read text marked by the "Caution" icon for information you must know to avoid damaging the library, the tape drives, or losing data.

Important Read text marked by the "Important" icon for information that helps you complete a procedure or avoid extra steps.

Note: Read text marked with "Note" for additional information or suggestions about the current topic.

Related Publications

The following documents related to the Spectra Verde NAS solution are available on the Support Portal website at support.spectralogic.com, and from the Documentation screen on the Verde user interface.

- The *Spectra Verde NAS Solution Network Setup Tips* provide helpful instructions for troubleshooting common connectivity problems.
- The *Spectra Verde NAS Solution Quick Start Guide* provides basic instructions for the essential installation and configuration steps.
- The *Spectra Verde NAS Solution Command Line Interface Guide* describes how to configure, monitor, and maintain the Spectra Verde NAS solution through the command line interface.
- The *Spectra Verde NAS Solution Site Preparation Guide* provides important information that you should know before installing a Verde NAS solution in your storage environment.
- The *Spectra Verde NAS Solution Installation Guide* provides instructions for installing a Verde NAS solution.
- The *Spectra BlackPearl & Verde HotPair Installation & Configuration Guide* provides detailed information on installing and using a Verde NAS solution in a HotPair configuration.

The following documents are available after logging into your Support portal account at: support.spectralogic.com.

- The *Spectra Verde NAS Solution Release Notes and Documentation Updates* provide the most up-to-date information about the Verde NAS solution, including information about the latest software releases and documentation updates.
- The *Spectra 12- & 36-Drive Chassis Boot Drive Replacement Guide* provides instructions for replacing a failed boot drive in the system.
- The *Spectra 12-, 36- & 45-Drive Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive after the system is installed.
- The *Spectra 12-, 36- & 45-Drive Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in the system.
- The *Spectra 12-, 36- & 45-Drive Chassis Power Supply Replacement Guide* provides instructions for replacing a failed power supply after the system is installed.
- The *Spectra 12-Drive Chassis HBA Replacement Guide* and *Spectra 36-Drive Chassis HBA Replacement Guide* provide instructions for replacing a failed HBA in the system.
- The *Spectra 96-Drive Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive in the Verde archive expansion node.
- The *Spectra 96-Drive Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in the archive expansion node.
- The *Spectra 96-Drive Chassis Power Supply Replacement Guide* provides instructions for replacing a failed power supply in the archive expansion node.
- The *Spectra 96-Drive Chassis I/O Module Replacement Guide* provides instructions for replacing a failed I/O module in the archive expansion node.

CHAPTER 1

Product Overview

This chapter provides an overview of the Spectra Verde NAS solution's features and components.

Topic	
Overview	page 19
Features	page 19
Components	page 21
Front View of Master Nodes	page 21
Rear View of Master Nodes	page 23
Rear Panel of Master Nodes	page 25
Front View of the Verde Enterprise Expansion Node	page 27
Rear View of the Verde Enterprise Expansion Node	page 28
Front View of the Verde Archive Expansion Node	page 29
Rear View of the Verde Archive Expansion Node	page 30
Front View of the 107-Drive Disk Expansion Node	page 31
Rear View of the 107-Drive Disk Expansion Node	page 32
Software	page 33
Operating System	page 33
Logical Volume Manager and File System	page 33
NFS and CIFS Servers	page 33
Verde User Interface	page 33
Menus	page 34
Status Icons	page 37
Supported Browsers	page 37
Command Line Interface	page 37

OVERVIEW

The Verde NAS Solution provides high-density, network-attached storage for most major operating environments, including Microsoft® Windows®operating system, Apple® OS X® operating system, UNIX®, and Linux®.

Optimized for secondary storage, the highly versatile Verde NAS solutions have many applications, including use as:

- Network-Attached Storage (NAS) for sharing file-based information over an IP network.
- Bulk file storage for both general and digital preservation usage.
- Disk-to-disk data file storage, either alone or as part of a tiered storage solution.

FEATURES

The Verde NAS solution includes the following features:

Command Line Interface The Verde NAS solution can be configured, monitored, and maintained using a command line interface. The command line interface is documented in the *Spectra Verde NAS Solution Command Line Interface Guide*.

Easy Network-Based Administration The Verde NAS solution can be configured over an Ethernet network using a standard web browser.

Expansion Nodes The Verde enterprise expansion node accommodates up to 44 disk drives with an active bezel, and 45 disk drives with a passive bezel, and can be connected to a master node to increase overall capacity of the system. The Verde archive expansion node holds up to 96 disk drives. The 107-drive expansion node holds up to 107 drives.

HotPair Two Verde master nodes can be connected to multiple expansion nodes in a failover configuration. One master node acts as the primary controller, and the other acts as the secondary. In the event that the secondary controller detects a failure of the primary controller, it automatically takes over to provide uninterrupted operation, without administrative intervention.

File Sharing Connectivity for Major Operating Systems The Network File System (NFS) and Common Internet File System (CIFS) protocols provide connectivity to most major operating systems, including Microsoft Windows, Apple Macintosh, UNIX, and Linux. Solid state disk drives may be installed in your system to improve NFS performance.

Mirrored Boot Drives Two dedicated, mirrored drives provide the dedicated storage for the operating system.

Network File Interface The Network File Interface (NFI) service allows you to automatically move data from your Verde NAS solution to one or more BlackPearl® Converged Storage systems, without the need to use a Spectra S3 client. Data is transferred on a schedule and data copied from the Verde NAS solution to the BlackPearl system can be configured to be kept on the NAS solution, or deleted. When a user needs access to data deleted from the Verde NAS solution, the BlackPearl system copies it back to the Verde NAS solution.

Rack-Mount Hardware The Verde NAS solution is designed to mount in a standard 4-post, 19-inch (48.3 cm) rack using just 2U (3.5 inches, 8.9 cm) or 4U (7 inches, 17.8 cm) of rack space, depending on the size of the system. Each Verde NAS solution includes rack mounting hardware. Alternatively, you can place the system on a level tabletop or other horizontal surface.

RAID-Protected Data Disks Data drives in the Verde NAS solution provide the system's storage capacity. Disk drives are grouped into protected volumes with selectable parity options and automatic data integrity verification to protect against data corruption.

Redundant Components The Verde NAS solution features N+1 redundant power supplies and data drives that are hot-swappable for uninterrupted operation. Any data drives not configured in a storage pool act as global spares. A spare becomes active if a drive in a storage pool fails.

Replicated System Configuration The Verde master node mirrors its boot drives on to an existing storage pool on the system's data disks. If one or both boot drives fail, the system recovers automatically when replacement boot drives are installed.

Verde User Interface The Verde user interface is used to perform configuration and management tasks on the Verde NAS solution. It also lets you monitor the system hardware and view system messages.

Write Performance Drives The Verde NAS solution supports even numbers of solid state drives as Write Performance drives. The drives increase write speed to shared NFS volumes on the system.

10 Gigabit Ethernet A dual port, 10 Gigabit Ethernet (10 GigE) network interface card, optional in a 2U master node and standard in a 4U master node, provides high-speed data connections between hosts and the Verde NAS solution.

10GBase-T Ethernet Connectivity Two onboard 10 gigabit copper ports (10GBase-T) provide Ethernet connectivity for the system with one dedicated port used to access the Verde user interface, and the second 10GBase-T port can be used for data transfer.

40 Gigabit Ethernet An optional dual port, 40 Gigabit Ethernet (40 GigE) network interface card can be installed to provide high-speed data connections between hosts and the Verde NAS solution.

COMPONENTS

The following sections show the locations of, and briefly describe the Verde NAS solution's major front and rear panel components.

Front View of Master Nodes

Figure 1 and Figure 2 show the components on the front of the Verde master node with the front bezel removed.

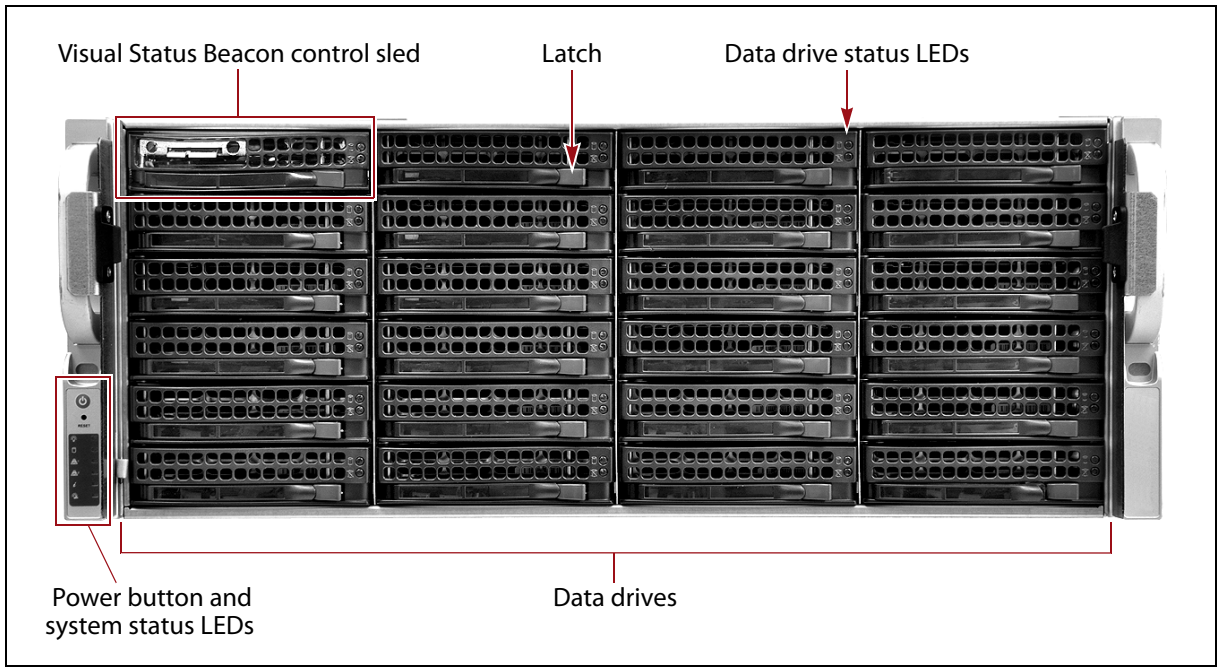


Figure 1 The front view of the Verde 4U master node (front bezel removed).

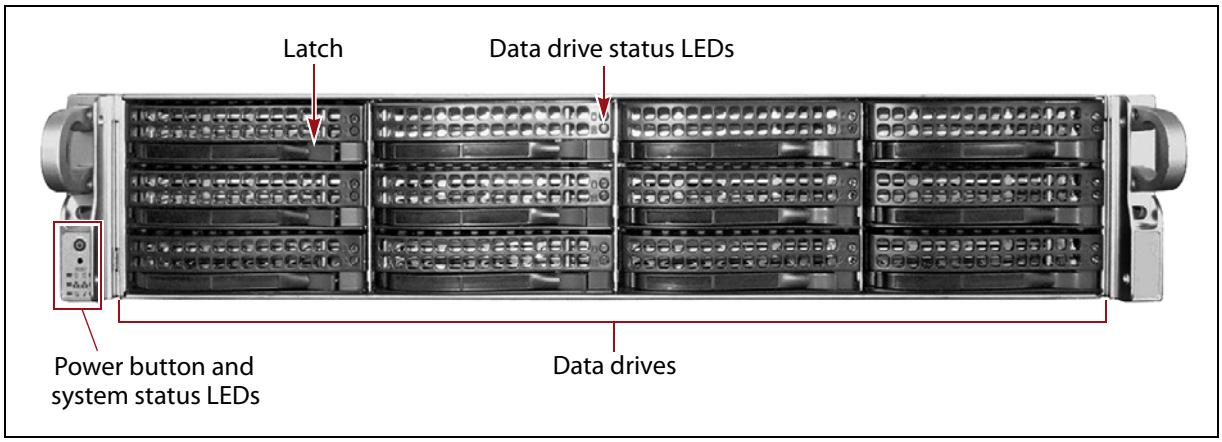


Figure 2 The front view of the Verde 2U master node (front bezel removed).

Component	Description
Front bezel (not shown)	The front bezel mounts on the front of the master node, and contains the Visual Status Beacon light bar, which provides status information for the system. See Front Bezel Visual Status Beacon on page 78 for more information. **Note:** The front bezels in the Verde 2U master nodes do not include Visual Status Beacon light bars. The 4U master node may optionally be purchased with a bezel that does not include a Visual Status Beacon.
Visual Status Beacon control sled (Verde 4U master nodes only)	▪ If the master node uses an active bezel, the drive sled in the upper left corner of the front of the expansion node provides control for the Visual Status Beacon. A disk drive cannot be installed in this position. ▪ If the master node uses a passive bezel, a disk drive is installed in this position.
Power button	The power button controls the main AC power for the Verde NAS solution.
System status LEDs	The status LEDs indicate power status, disk and network activity, as well as hardware faults. See System Status LEDs on page 80 for more information.
Data drives	The Verde 4U master nodes support up to 23 high-performance disk drives mounted on individual drive sleds in the front of the system. The Verde 2U master nodes support up to 12 data drives. Depending on your order configuration, the Verde may optionally contain solid state drives to improve write performance. See Write Performance Drives on page 20 for more information. **Note:** If the Verde 4U master node uses a bezel without a Visual Status Beacon, 24 disk drives are installed in the front of the system. The drive sleds slide into bays in the front of the Verde enclosures and lock in place. The front of each drive sled has a handle for removing the sled from the system and a latch for locking the drive sled in place.
Data drive status LEDs	Two LEDs on each drive sled indicate the status of the drive. One LED is for drive status while the other shows drive activity.
Empty drive sleds	Empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow.

Rear View of Master Nodes

Figure 3 and Figure 4 show the major components on the rear of the current chassis of the Verde master nodes.

Note: For a description of the components on the rear of the Verde 1.0 chassis, see Appendix B Verde Chassis 1.0 Overview & Specifications on page page 220.

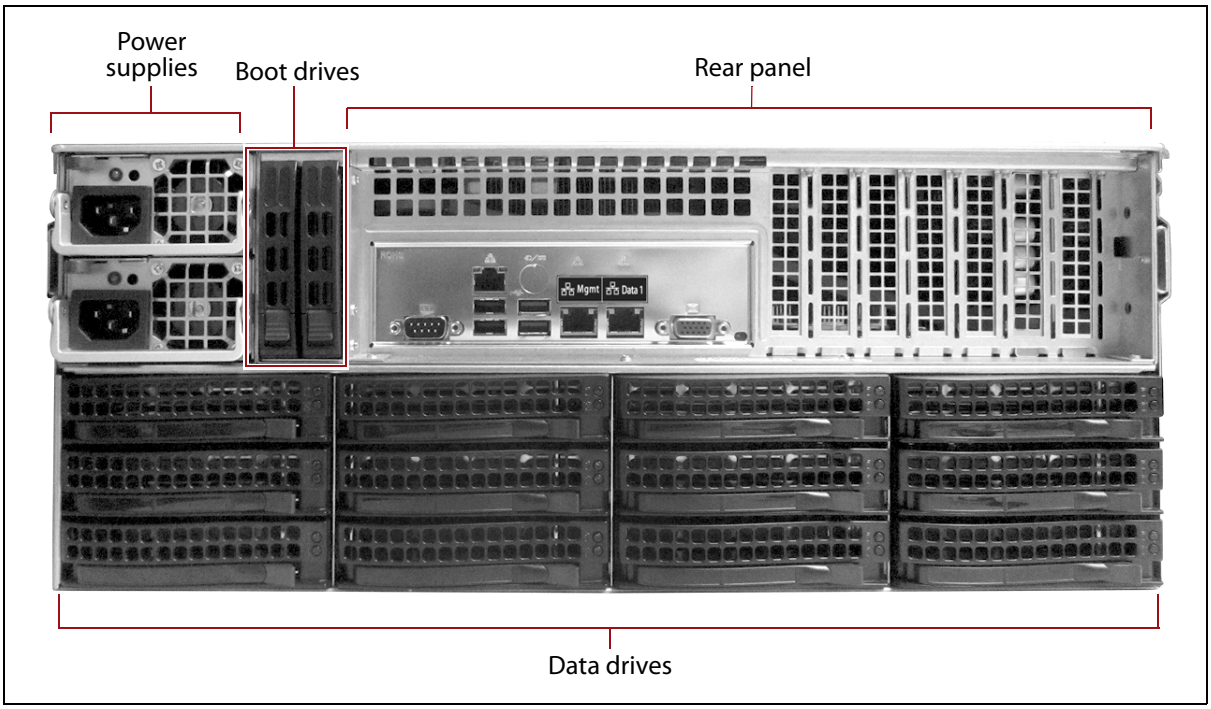


Figure 3 The rear view of the Verde 4U master node.

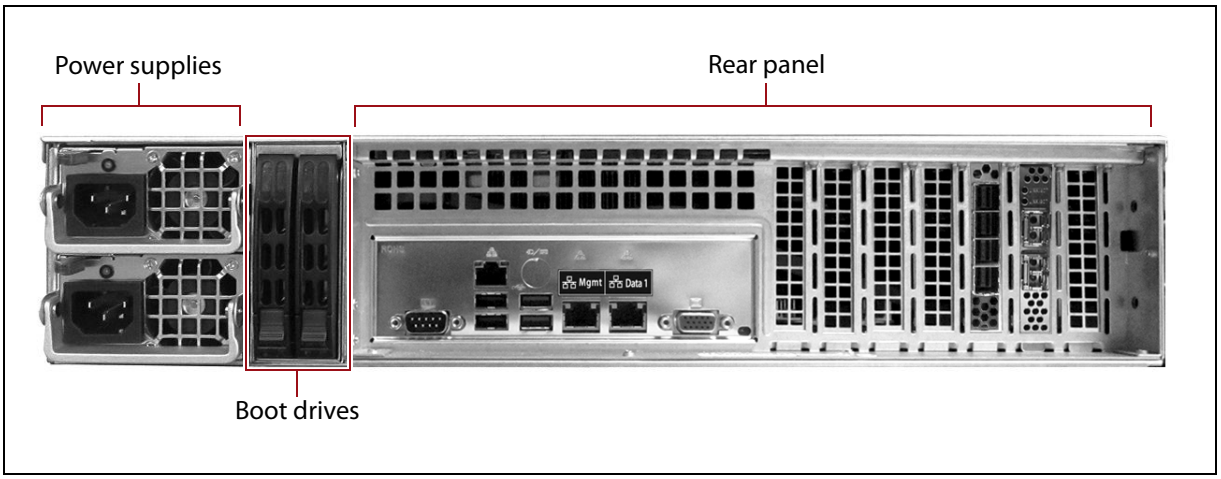


Figure 4 The rear view of the Verde 2U master node.

Component	Description
Power supplies	The Verde master node includes two power supplies to provide N+1 redundancy and fail-over protection. ▪ Each power supply has its own AC power connector. ▪ Each power supply has a single LED that lights to indicate when the power is on and functioning normally.
Rear panel	The rear panel of the Verde master node allows for Ethernet, SAS, USB, and other connections. See Rear Panel of Master Nodes on page 25 for a detailed description.
Boot drives	The boot drives provide storage for the operating system and Verde user interface. The boot drives are hot swappable which allows for uninterrupted operation during replacement.
Data drives (Verde 4U master nodes only)	The Verde 4U master nodes support up to 12 data drives in the rear of the system. Depending on your order configuration, the Verde NAS solution may optionally contain solid state drives to improve write performance. See Write Performance Drives on page 20 for more information. **Note:** The Verde master nodes do not have data drives in the rear of the system.
Empty drive sleds (Verde 4U master nodes only)	Empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow.

Rear Panel of Master Nodes

Figure 5 shows the components on the rear panel of the current chassis for the Verde master nodes.

Note: For a description of the components on the rear panel of the Verde 1.0 chassis, see Appendix B Verde Chassis 1.0 Overview & Specifications on page page 220.

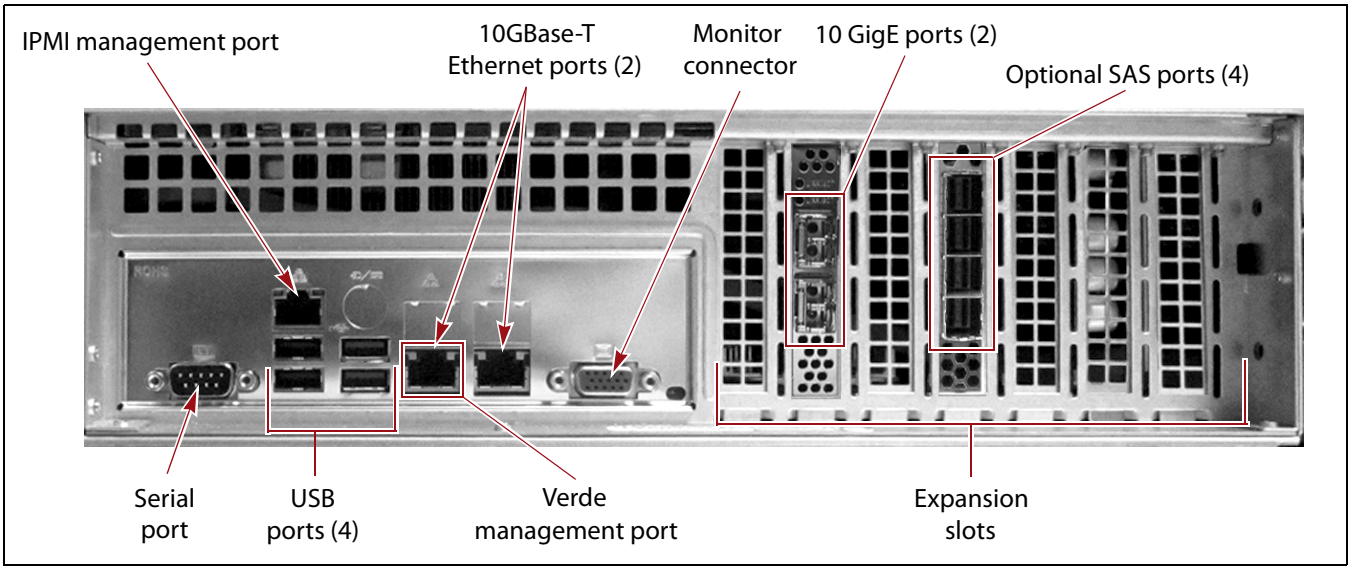


Figure 5 The Verde master node rear panel components.

Component	Description
IPMI management port	See IPMI Configuration on page 217 for instructions on using IMPI.
10GBase-T Ethernet ports	The Verde NAS solution includes two 10GBase-T ports. One of the 10GBase-T ports can be used for network connectivity on a 10GBase-T network. The left port of the two 10GBase-T ports is dedicated as the Verde management port and cannot be used for data transfer. **Notes:** ▪ The 10GBase-T ports auto-negotiate down to 1000Base-T. ▪ Spectra Logic recommends using the 40 GigE ports, or the 10 GigE ports for data transfer to ensure maximum performance.
Monitor connector	If necessary, you can connect a monitor to the SVGA connector on the Verde master node for troubleshooting purposes. Only connect a monitor for initial configuration of the BlackPearl management port, or as directed by Spectra Logic Technical Support.
10 GigE ports	The two 10 Gigabit Ethernet (10 GigE) ports can be used for network connectivity on a 10 GigE network. **Note:** The 10 GigE is optional in the Verde 2U master nodes.

Component	Description
SAS ports (Optional)	Depending on your configuration, there may be SAS cards installed in available expansion slots. Each four port SAS card provides connectivity between the master node and up to two Verde enterprise expansion nodes. Each two port SAS card provides connectivity between the master node and up to two Verde archive expansion nodes. For information on how to connect cables between the master node and expansion node, see the *Spectra Verde Nas Solution Installation Guide.*
Expansion slots	The expansion slots accommodate optional interface cards to provide additional connectivity.
Verde management port	The Verde management port is used to connect to the browser-based user interface to configure, manage, and monitor the Verde NAS solution. The Verde management port cannot be used for data transfer.
USB ports	If necessary, you can use these ports to connect a USB drive, or USB mouse and USB keyboard to the system for troubleshooting purposes, or to configure the IP addressing for the Verde management port.
Serial port	The serial port is used to connect a primary master node to a secondary master node in a HotPair configuration. The two master nodes are connected using a null modem cable. For information on connecting cables for a HotPair configuration, see the *Spectra BlackPearl & Verde HotPair Installation & Configuration Guide*.
40 GigE ports (Not shown, optional)	The two 40 Gigabit Ethernet (40 GigE) ports can be used for network connectivity on a 40 GigE network. **Note:** The 40 GigE card is not supported in 2U master nodes.

Front View of the Verde Enterprise Expansion Node

Figure 6 shows the major components on the front of the Verde enterprise expansion node.

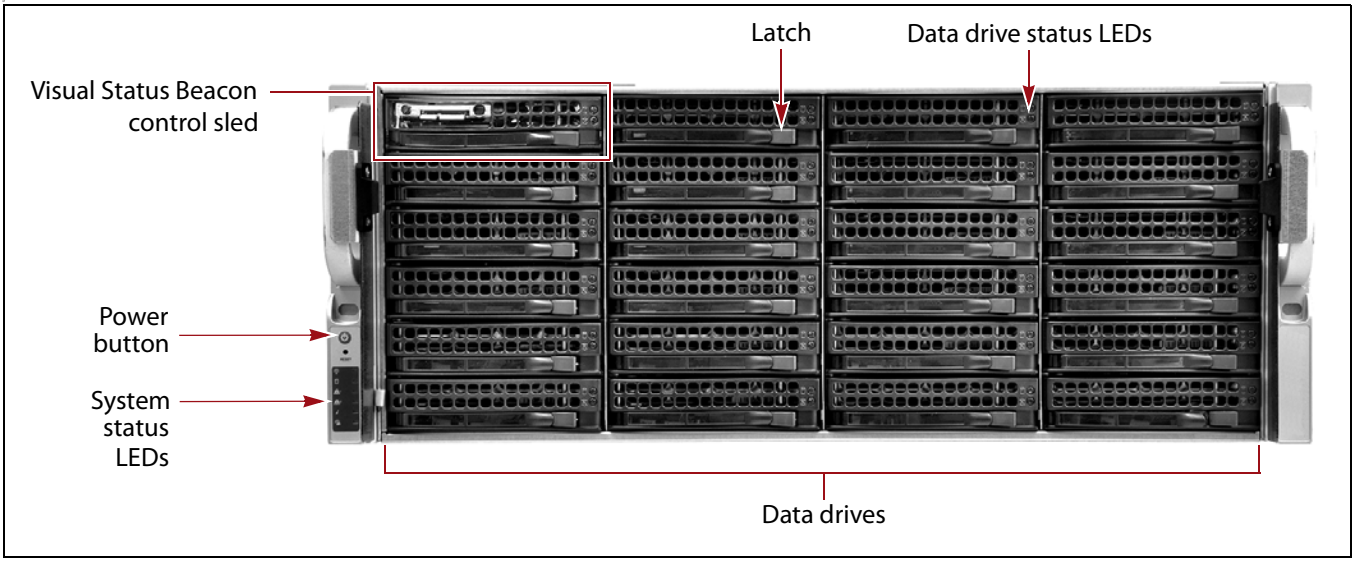


Figure 6 The front view of the Verde enterprise expansion node (Visual Status Beacon removed).

Component	Description
Front bezel (not shown)	The front bezel mounts on the front of the chassis, and may contain the Visual Status Beacon light bar, which provides status information for the system. See Front Bezel Visual Status Beacon on page 78 for more information.
Visual Status Beacon control sled	▪ If the expansion node uses an active bezel, the drive sled in the upper left corner of the front of the expansion node provides control for the Visual Status Beacon. A disk drive cannot be installed in this position. ▪ If the expansion node uses a passive bezel, a disk drive is installed in this position.
Power button	The power button controls the AC power for the enterprise expansion node.
System status LEDs	The status LEDs indicate power status, disk and network activity, as well as hardware faults. See System Status LEDs on page 80 for more information.
Data drives	The front of the Verde enterprise expansion node supports up to 23 enterprise disk drives, or 24 drives if the expansion node uses a passive bezel, mounted on individual drive sleds in the front of the chassis. The drive sleds slide into bays in the front of the enclosure and lock in place. The front of each drive sled has a handle for removing the sled from the system and a latch for locking the drive sled in place.
Data drive status LEDs	Two LEDs on each drive sled indicate the status of the drive. One LED is for drive status while the other shows drive activity.
Empty drive sleds	When fewer than the maximum number of drives are installed, empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow.

Rear View of the Verde Enterprise Expansion Node

Figure 7 shows the major components on the rear of the Verde enterprise expansion node.

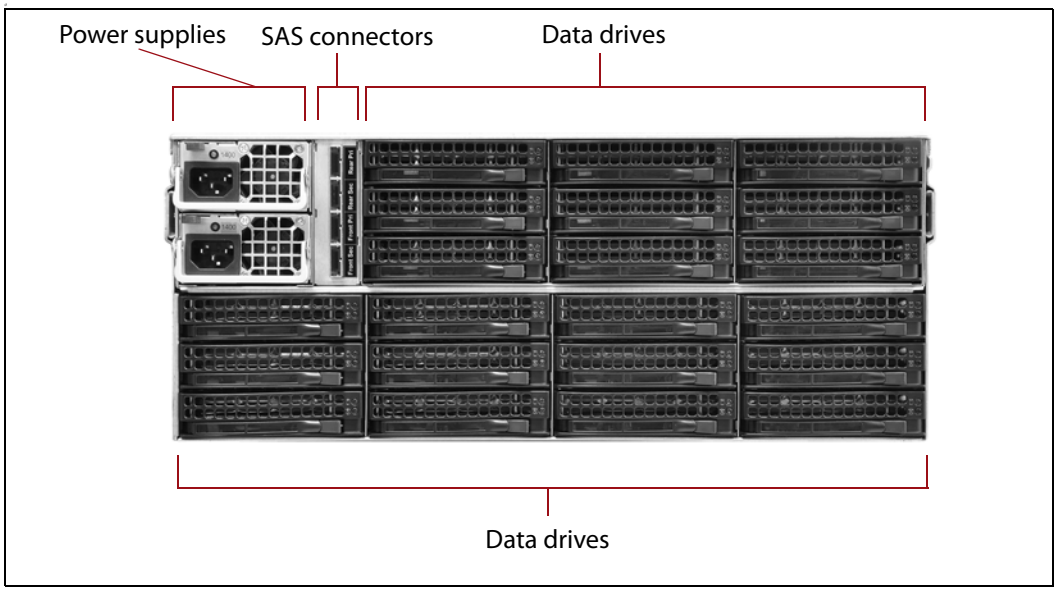


Figure 7 The rear view of the Verde enterprise expansion node.

Component	Description
Power supplies	The Verde enterprise expansion node includes two power supplies to provide N+1 redundancy and fail-over protection. ▪ Each power supply has its own AC power connector. ▪ Each power supply has a single LED that lights to indicate when the power is on and functioning normally.
SAS connectors	The rear panel of the Verde enterprise expansion node has four SAS ports used to connect an expansion node to a master node. Two ports are for primary connections and two ports are for secondary connections. Labels next to each port identify if the port is a primary or secondary connection.
Data drives	Up to 21 data drives can be installed in the rear of the expansion node.
Empty drive sleds	When fewer than the maximum number of drives are installed, empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow.

Front View of the Verde Archive Expansion Node

Figure 8 shows the major components on the front of the Verde archive expansion node.

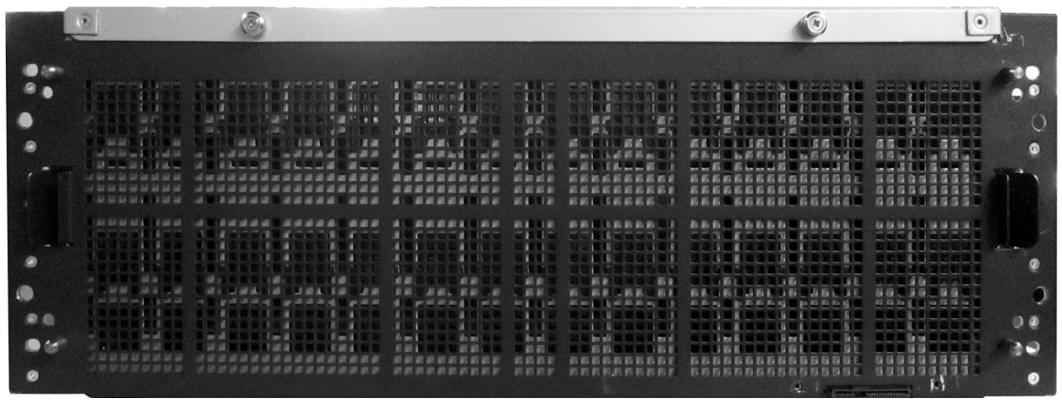


Figure 8 The front view of the Verde archive expansion node (Visual Status Beacon removed).

Component	Description
Front bezel (not shown)	The front bezel mounts on the front of the expansion node, and contains the Visual Status Beacon light bar, if included, which provides status information for the expansion node. See Front Bezel Visual Status Beacon on page 78 for more information.

Rear View of the Verde Archive Expansion Node

Figure 9 shows the major components on the rear of the Verde archive expansion node.

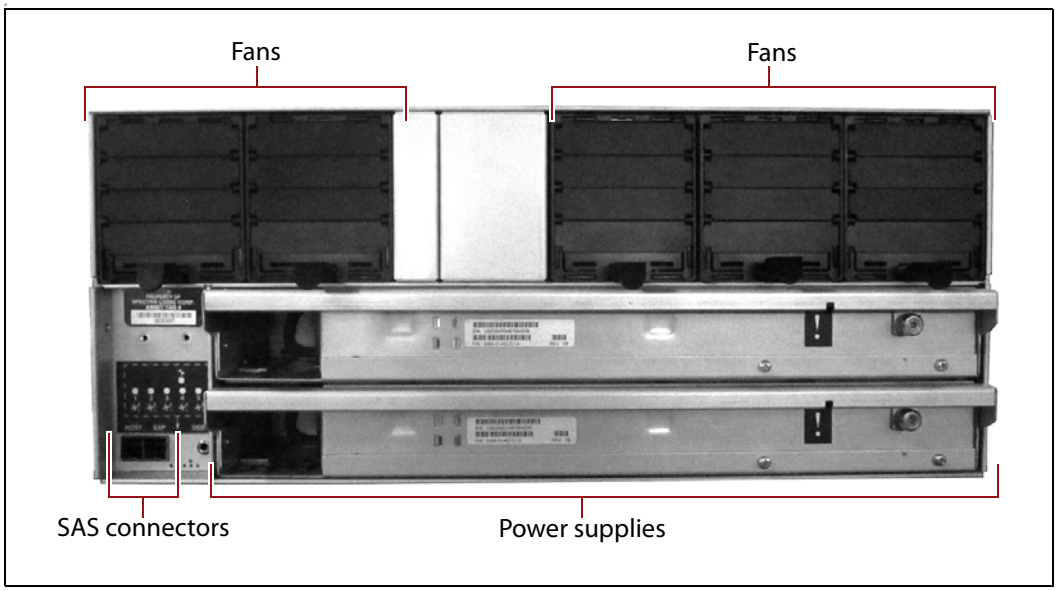


Figure 9 The rear view of the Verde archive expansion node.

Component	Description
Fans	Five hot-swappable fans provide the cooling for the Verde archive expansion node.
Power supplies	The Verde archive expansion node includes two power supplies to provide N+1 redundancy and fail-over protection. ▪ Each power supply has its own AC power connector. ▪ Each power supply has a single LED that lights to indicate when the power is on and functioning normally.
SAS connectors	The rear panel of the Verde archive expansion node has two SAS ports used to connect an expansion node to a Verde master node.

Front View of the 107-Drive Disk Expansion Node

Figure 8 shows the major components on the front of the 107-drive disk expansion node.

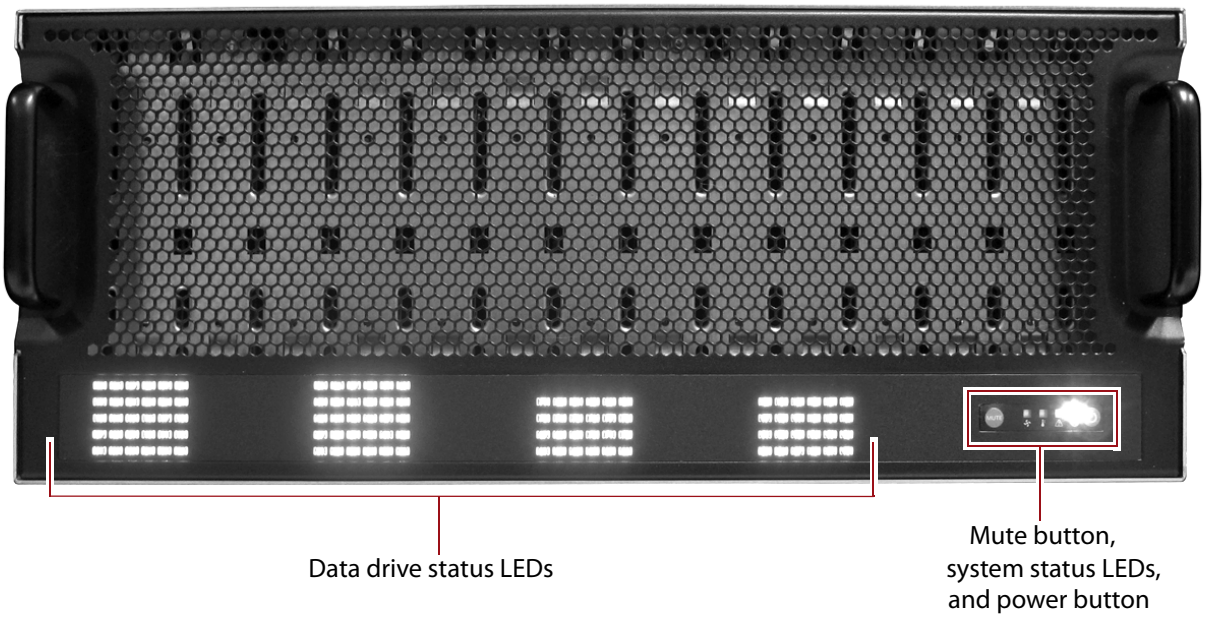


Figure 10 The front view of the 107-drive disk expansion node (front bezel removed).

Component	Description
Front bezel (not shown)	The front bezel mounts on the front of the disk solution, and contains the Visual Status Beacon light bar, if included, which provides status information for the expansion node. See Front Bezel Visual Status Beacon on page 131 for more information.
Data drive activity LEDs	Numbered LEDs indicate drive activity for each drive in the disk solution.
Mute button	The mute button silences the chassis alarm.
System status LEDs	The status LEDs indicate power status, as well as hardware faults for fans, power supplies, and temperature.
Power button	The power button controls the main AC power for the 107-drive disk expansion node.

Rear View of the 107-Drive Disk Expansion Node

Figure 9 shows the major components on the rear of the 107-drive disk expansion node.

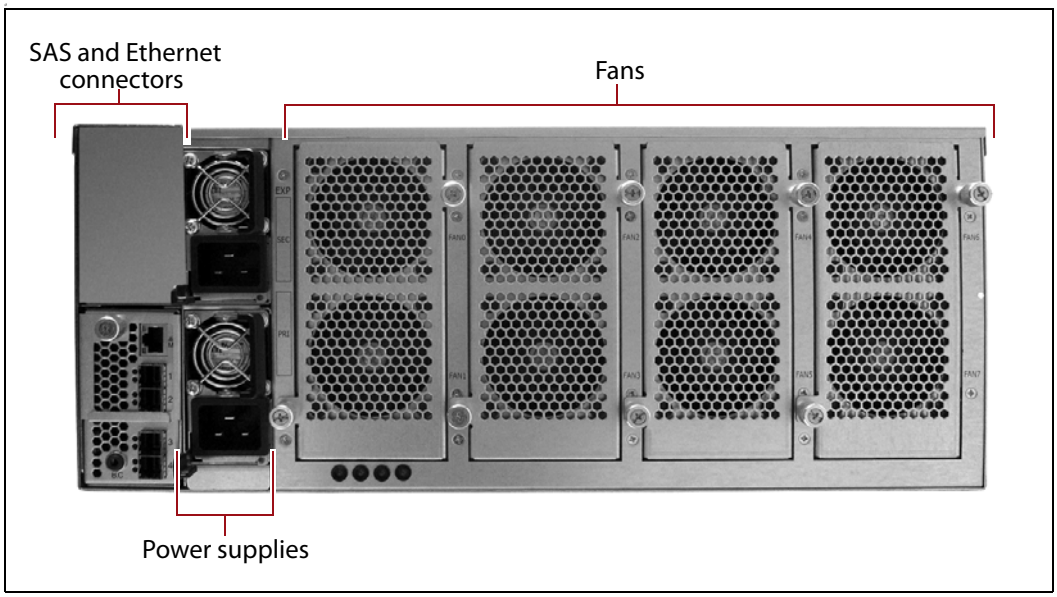


Figure 11 The rear view of the 107-drive disk expansion node.

Component	Description
SAS and Ethernet connectors	The rear panel of the 107-drive disk expansion node has one or two expander panels which include one Ethernet port and four SAS ports used to connect a 107-drive disk expansion node to a Verde.
Fans	Eight hot-swappable fans, in banks of two, provide the cooling for the 107-drive disk expansion node.
Power supplies	The 107-drive disk expansion node includes two power supplies to provide N+1 redundancy and fail-over protection. ▪ Each power supply has its own AC power connector. ▪ Each power supply has a single LED that lights to indicate when the power is on and functioning normally.

SOFTWARE

The software installed on the Verde NAS solution boot drives includes the following:

- Operating system
- Logical volume manager and file system
- NFS and CIFS servers

Operating System

The operating system, running on the integrated application server, provides the foundation for all software and applications running on the system.

Logical Volume Manager and File System

The Verde NAS solution features a combined logical volume manager and file system which controls the structure and management of the data storage on the system. The Verde NAS solution includes data verification to protect against corruption.

NFS and CIFS Servers

The NFS and CIFS servers running on the Verde NAS solution provide network file system access to host computers over an Ethernet network. NFS and CIFS shares can be accessed by most major operating environments, including Microsoft Windows operating system, Apple macOS, UNIX, and Linux.

VERDE USER INTERFACE

The Verde user interface provides browser-based configuration, management, and monitoring of the Verde NAS solution. The following sections describe the common features that appear in all screens in the user interface.

Menus

The menu bar appears along the top edge of each screen. Use the menu bar drop-down menus to navigate through the interface.

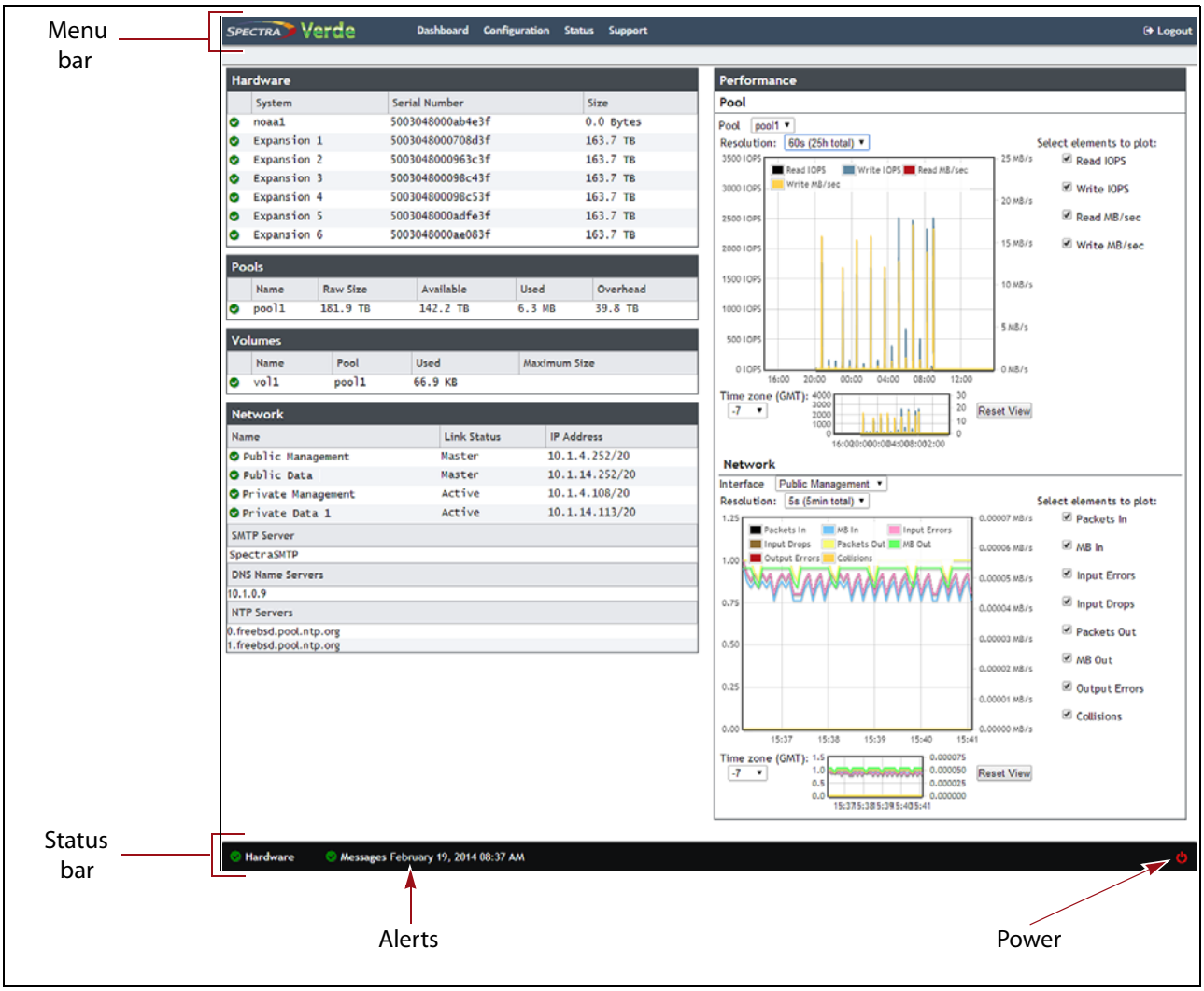


Figure 12 The Dashboard screen of the Verde user interface.

The following table provides an overview of the screens available under each menu. The previously selected screen remains displayed until you select another option.

Menu	Available Options
Dashboard	The **Dashboard** navigation link returns you to the Dashboard screen from any other screen in the interface. The Dashboard screen displays the general status of the NAS solution, storage pools, volumes, and network connections on the system. Clicking any of the panes on the Dashboard takes you to a details screen for that selection. The Dashboard screen also displays performance metrics of the system.

Menu	Available Options
Configuration	The **Configuration** menu provides access to controls for configuring all aspects of the NAS solution's operation. ▪ **NAS ⋯⁝ Pools** — Displays information about any currently configured storage pools and lets you define new pools, and edit or delete existing pools. ▪ **NAS ⋯⁝ Volumes** — Displays information about any currently configured volumes on an existing storage pool and lets you define new volumes, and edit or delete existing volumes. ▪ **NAS ⋯⁝ Shares ⋯⁝ CIFS** — Displays information about any currently configured CIFS shares and lets you define new shares, and edit or delete existing shares. ▪ **NAS ⋯⁝ Shares ⋯⁝ NFS** — Displays information about any currently configured NFS shares and lets you define new shares, and edit or delete existing shares. ▪ **Services** — Displays information about the currently configured services and lets you edit existing services. ▪ **Network** — Provides controls for configuring the Ethernet ports on the Verde NAS solution, as well as entering SMTP (Simple Mail Transport Protocol) information to allow the system to send emails. ▪ **Certificates** — Provides controls for installing signed, trusted SSL certificates for your data and management ports so that you do not need to resolve the security certificate warning when accessing these ports. ▪ **Mail Recipients** — Provides controls for configuring mail recipient accounts to receive emails when a message severity threshold is reached, or when AutoSupport Log sets (ASLs) are generated by the system. ▪ **Users** — Provides controls for creating new user accounts for accessing the Verde user interface, as well as changing the password of existing accounts.
Status	The **Status** menu provides access to the tools for monitoring the Verde NAS solution in your environment. ▪ **Hardware** — Displays information about the system and its components. Selecting the tabs on the Hardware screen displays detailed component status information. ▪ **NAS ⋯⁝ Pools** — Displays information about any currently configured storage pools. ▪ **NAS ⋯⁝ Volumes** — Displays information about any currently configured volumes on an existing storage pool. ▪ **Messages** — Displays system messages for the NAS solution. ▪ **Performance** — Displays performance metrics for storage pools, individual drives, and the CPUs in the integrated server. ▪ **Reports** — Provides controls for generating reports about the configuration and status of the NAS solution. Reports can be generated in XML or JSON (JavaScript Object Notation) formats.

Menu	Available Options
Support	The **Support** menu provides access for maintenance and troubleshooting options for the Verde NAS solution. ▪ **Software** — Provides controls for updating the Verde software. ▪ **Activation Keys** — Provides controls for entering activation keys. ▪ **Logs** — Displays any current ASL sets on the system and provides controls for generating a new log set. ▪ **Documentation** — Displays documentation links for the Verde NAS solution. ▪ **Contact Information** — Displays contact information for Spectra Logic Technical Support, as well as the part and serial numbers for the NAS solution. ▪ **Tools** — Displays tools to troubleshoot any internal or external server cabling errors.
Logout	Logs out the current user of the Verde user interface and returns to the login screen.

The information in the following table can be found on the Status bar, located at the bottom of all screens.

Status Bar	Available Options
Hardware	Provides an at-a-glance status of the overall health of the Verde NAS solution. Clicking this link takes you to the Hardware screen. For more information see View the Status of Hardware Components on page 135.
Messages	Displays the severity, date, and time of the last warning, error, or informational message that was generated. Clicking this link takes you to the Messages screen. For more information see View System Messages on page 134. **Note:** This link does not display if there are no current system messages.
Power	Provides controls for rebooting and shutting down the system. For more information see Reboot or Shut down a Verde NAS Solution on page 144. **Note:** The connection to the user interface is lost after running the reboot command. Wait while the system reboots before attempting to reconnect to the user interface.

Status Icons

Icons indicate the status of a component and the highest severity level for any system messages, as described in the following table.

Icon	Meaning
	Component OK The component is functioning correctly.
	Information An informational message about a system component is available. Check messages to determine the component.
	Warning A system component requires attention. Check messages to determine the component.
	Error A system component experienced an error condition. Check messages to determine the component and its error condition.
	Unknown The status of a system component cannot be determined. Check messages to determine the component.

Supported Browsers

The Verde user interface supports the following standard web browsers:

- Google® Chrome™ version 22 or later
- Mozilla® FireFox® version 27 or later
- Apple® Safari® version 7 or later
- Microsoft® Internet Explorer® version 11 or later

Note: Spectra Logic recommends using Google Chrome to access the Verde user interface.

COMMAND LINE INTERFACE

The command line interface provides text-based configuration, management, and monitoring of the Verde NAS solution. Use the command line interface to perform many of the tasks that are available through the Verde user interface such as configuring storage pools, volumes, and shares; network administration; and monitoring the status of the NAS solution. For a full list of the features available in the command line interface, see the *Spectra Verde NAS Solution Command Line Interface Guide*.

CHAPTER 2

Initial Configuration

This chapter describes the initial setup and configuration steps for the Verde NAS solution.

Note: If your NAS solution is a HotPair configuration, see the *Spectra BlackPearl & Verde HotPair Installation & Configuration Guide* for specific instructions on how to setup your NAS solution.

Topic	
Before You Begin	page 39
Connect Ethernet Cables	page 39
Power On the Verde NAS Solution	page 39
Verde Master Nodes and Verde Enterprise Expansion Nodes	page 40
Verde NAS Solution with Archive Expansion Nodes or 107-Drive Disk Expansion Node	page 40
Configure the Verde Management Port	page 42
Automatically Import Activation Keys	page 43
Log In to the Verde User Interface	page 44
Configure the Data Connection	page 46
Create a User	page 52
Description of User Types	page 52
Create a User	page 53
Next Steps	page 54

Before You Begin

Make sure the NAS solution is installed in accordance with the *Spectra Verde NAS Solution Installation Guide*.

Connect Ethernet Cables

Before proceeding with the below sections, you must connect Ethernet cables to the management and data ports on the Verde master node rear panel. See Rear Panel of Master Nodes on page 25 for the location of the Ethernet ports on the rear of the system.

Power On the Verde NAS Solution

Use the instructions in this section to power on a Verde NAS solution. During the power-on sequence, the Verde NAS solution initializes all of its installed components and starts the Verde web server.

How you power on the solution depends on the hardware in your configuration:

- Verde Master Nodes and Verde Enterprise Expansion Nodes on page 40.
- Verde NAS Solution with Archive Expansion Nodes or 107-Drive Disk Expansion Node on page 40.

Verde Master Nodes and Verde Enterprise Expansion Nodes

To power on a Verde NAS solution, remove the front bezel, and then gently press the power button on the front panel. If your configuration includes both a Verde master node and one or more enterprise expansion nodes, power on all chassis together. The power LED illuminates indicating that power is on. See System Status LEDs on page 133 for more information.

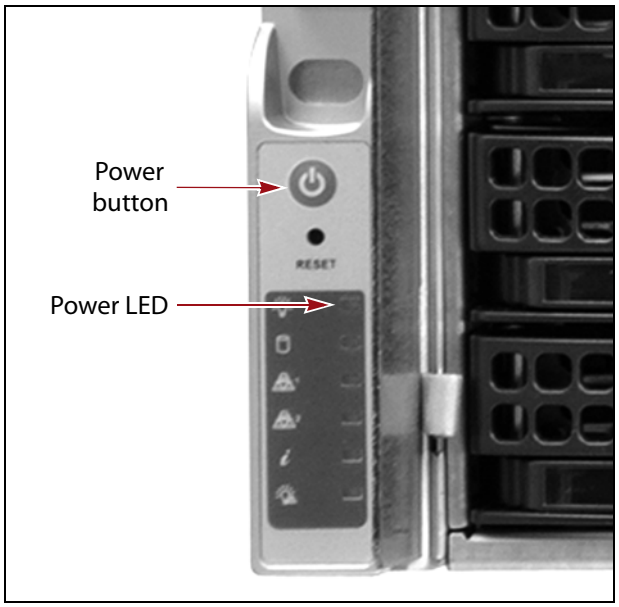


Figure 13 Press the power button.

Wait while the Verde NAS solution completes its power-on sequence, which takes approximately four minutes, depending on the configuration.

Note: Do not use the system's front panel power button to power off the NAS solution. See Reboot or Shut down a Verde NAS Solution on page 144 to reboot or shut down the system.

Verde NAS Solution with Archive Expansion Nodes or 107-Drive Disk Expansion Node

If your configuration includes one or more Verde archive expansion nodes or 107-drive disk expansion node, power on the expansion node(s) or solution(s) before powering on the master node.

To power on a Verde archive expansion node, plug both power cables on the Verde archive expansion node into power outlets near the rear of the chassis. The Verde archive expansion node immediately powers on. Wait approximately five minutes while the expansion node initializes before powering on a Verde master node.

To power on a 107-drive disk expansion node, remove the front bezel and reach into the left side (as viewed from the front) and press the power button.Wait approximately five minutes while the 107-drive disk expansion node initializes before powering on a Verde master node.

To power on a Verde NAS solution, remove the front bezel, and then gently press the power button on the front panel. The power LED illuminates indicating that power is on. See System Status LEDs on page 133 for more information.

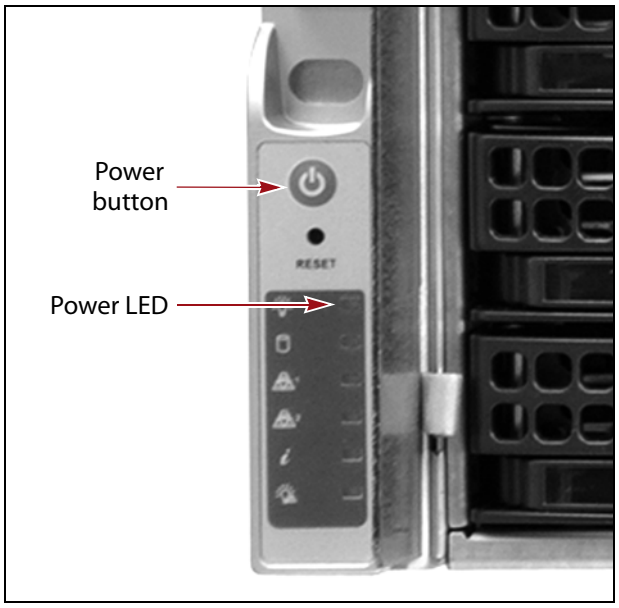


Figure 14 Press the power button.

Wait while the Verde NAS solution completes its power-on sequence, which takes approximately four minutes, depending on the configuration.

Note: Do not use the system's front panel power button to power off the NAS solution. See Reboot or Shut down a Verde NAS Solution on page 144 to reboot or shut down the system.

CONFIGURE THE VERDE MANAGEMENT PORT

The default IP address for the Verde management port is set to **10.0.0.2** with a netmask of **255.255.255.0**. If your network is already using this IP address, or you want to configure a different IP address for the management port, use the Verde master node console to configure the Verde management port IP address.

If you do not want to change the default management port IP address, skip to Log In to the Verde User Interface on page 44.

Important You must connect Ethernet cables as described in Connect Ethernet Cables on page 39 before either proceeding with the steps below or skipping this section and accepting the default IP address for the management port.

Note: Using the Verde master node console is the recommended way to change the Verde management port IP address. If you cannot use the console, see Resolving a Management Port IP Address Conflict on page 173 for information on alternate methods.

1. Connect a monitor and USB keyboard to the Verde master node. See Rear Panel of Master Nodes on page 25 to locate the monitor and USB connectors. The Console screen displays.

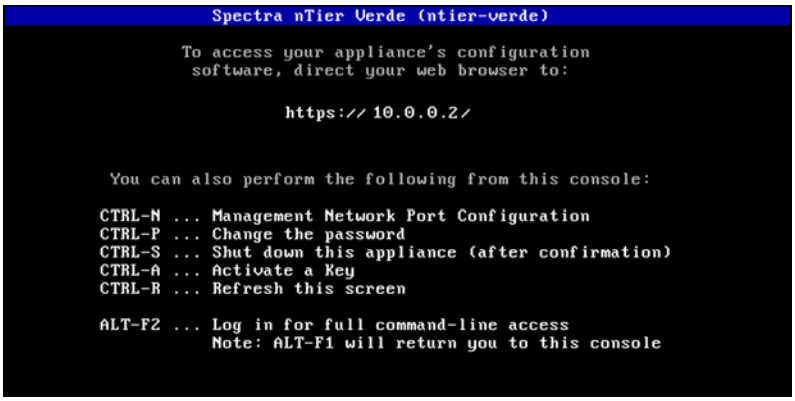


Figure 15 The Console screen.

2. Press **CTRL-N**. The Configure Management Network Interface screen displays.

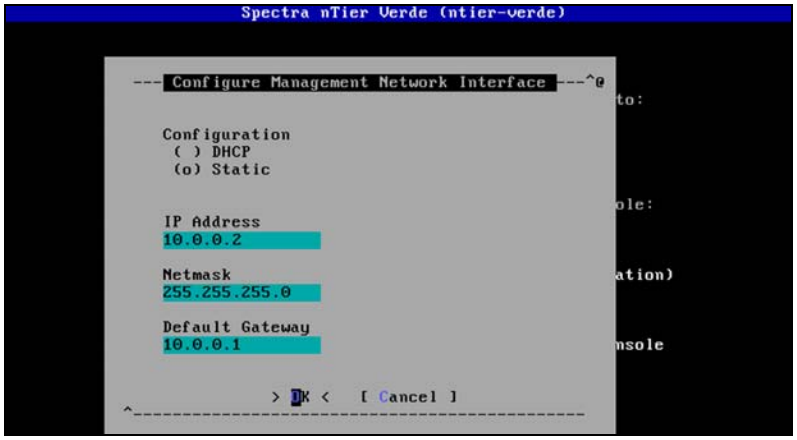


Figure 16 The Configure Management Network Interface screen.

3. Select either **DHCP** or **Static** as the addressing method.

   If you select static addressing, enter the following information:

   - **IP Address** — Enter a valid IPv4 address.
   - **Netmask** — Enter the subnet mask.
   - **Default Gateway** — Enter the default gateway.

4. Select **OK**. The console screen displays showing the new IP address.

   Note: If a new IP address does not display, you may need to manually refresh the console screen by pressing **CTRL-R**.

5. Connect a cable from your network to the Verde management port on the Verde master node. You are now able to connect to the Verde user interface with the IP address displayed in Step 4.

6. Disconnect the monitor and USB keyboard from the Verde system.

AUTOMATICALLY IMPORT ACTIVATION KEYS

Activation keys enable features on the Verde NAS solution. They are tied to the serial number of the system for which they are issued, and cannot be used on another NAS solution. Renewals of expired activation keys are obtained by contacting Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

The USB device in the Verde documentation kit contains the activation keys for the options that you purchased. Follow these steps to import the keys.

Note: If your Verde documentation kit does not contain a USB device, see Manually Enter Activation Keys on page 127 for instructions for manually entering the activation keys.

1. Insert the USB device into a USB port on the back of the NAS solution. See Figure 5 on page 25.

   When the Verde NAS solution detects the USB device it automatically imports the activation keys and power cycles the system.

2. Wait while the Verde NAS solution performs its power-on sequence and then log into the Verde user interface.

Important Do not remove the USB device until after the system power cycles and the Verde user interface displays a message that it is safe to remove the USB device.

Note: The first time that you log in after importing activation keys, an informational message displays indicating that you can now safely remove the USB device. Use the following steps to close the message:

a. Remove the USB device.

b. On the menu bar, select **Status ⋯⁘ Messages**. The messages screen displays.

c. Select the message about safely removing the USB device, and then select **Action ⋯⁘ Mark as read**. The informational message closes.

LOG IN TO THE VERDE USER INTERFACE

Use the following instructions to log into the Verde user interface.

Note: There is no limit to the number of users who can log in to the user interface. Spectra Logic recommends only one person use the interface at a time to avoid conflicting operations.

1. Using a standard web browser, enter the IP address of the Verde management port configured in Configure the Verde Management Port on page 42.

   Note: The Verde user interface uses a secure connection.

2. If necessary, resolve the security certificate warning for the Verde user interface.

   The Verde NAS solution ships with non-signed SSL certificates for both the data and management ports on the system. When using the shipped certificates, you must pass a security check every time you attempt to access the management port to view the Verde user interface, or when you attempt to transfer data using the data port.

   Notes:
   - The absence of the certificate does not affect functionality.
   - If desired, you can install signed, trusted SSL certificates for your data and management ports so that you no longer need to pass the security check when accessing these ports. See Configure Certificates on page 126.

3. Enter the primary administrator username and password.

   The default username is **Administrator**. The default password is **spectra**. The fields are case sensitive.

   Notes:
   - Spectra Logic recommends that you change the default password for the primary administrator (see Edit a User on page 125).
   - If you are upgrading from a previous version of Verde software, the existing administrator account "**spectra**" is retained. The "**Administrator"** account is automatically created without any permissions.
   - If you are upgrading from a previous Verde software version to software version 4.0, the Verde system retains any accounts created before the upgrade.

Figure 17 The Verde user interface Login screen.

4. Click ⋯ to log in.

Important The remainder of this guide assumes you are logged in to the Verde user interface.

CONFIGURE THE DATA CONNECTION

This section describes using the Verde user interface to configure the one or more data connections for the Verde master node. The NAS solution includes two 10GBase-T ports and two 10 GigE ports on the rear panel (see Figure 5 on page 25). Optionally, a 40 GigE card or 10GBase-T card can be installed in the NAS solution. The configuration steps are the same for all port types.

Notes:

- You can create one or more data connections to the NAS solution.
- You can configure link aggregation for better performance.
- While different types of Ethernet network interface cards can be installed in the same Verde NAS solution, only one type port can be used in each link aggregation configuration.
- You can only use the Verde management port to access the Verde user interface. You cannot use this port for data transfer.
- For a Verde HotPair configuration, see the *Spectra BlackPearl & Verde HotPair Installation & Configuration Guide* for information on configuring data connections.

Configure an Aggregate Port Data Connection

Link aggregation uses multiple Ethernet ports, configured with a single MAC address, to improve data transfer speeds. See Link Aggregation Notes on page 285 for more information.

Important The network switch connected to the Verde NAS solution must be configured for Level 3 LACP in order to support an aggregate data connection on the Verde NAS solution.

Use the following instructions to configure an aggregate port data connection.

1. From the menu bar, select **Configuration ···⁘ Network**, or select the Network pane from the Dashboard screen. The Network screen displays with information about the network connections of the NAS solution.

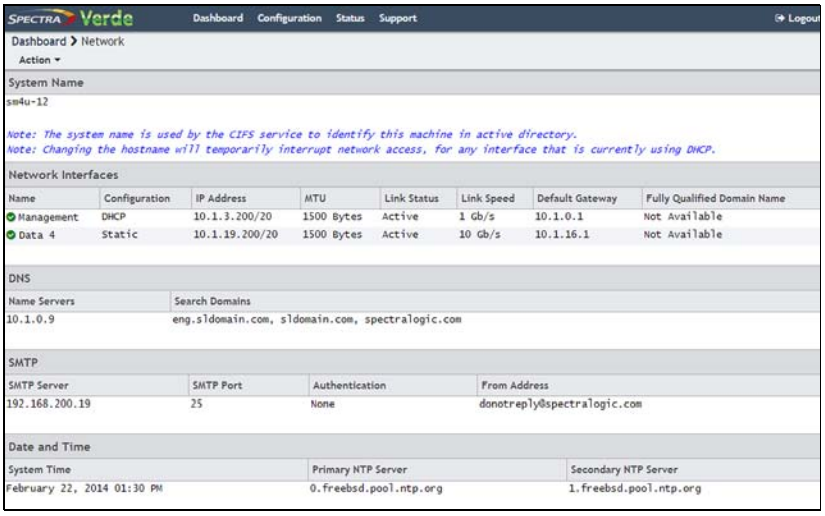


Figure 18 The Network screen.

2. From the menu bar, select **Action ···⁘ New Aggregate Interface**. The New Aggregate Interface dialog box displays.

   Note: Depending on your hardware configuration, the New Aggregate Interface dialog box may look different than what is shown below

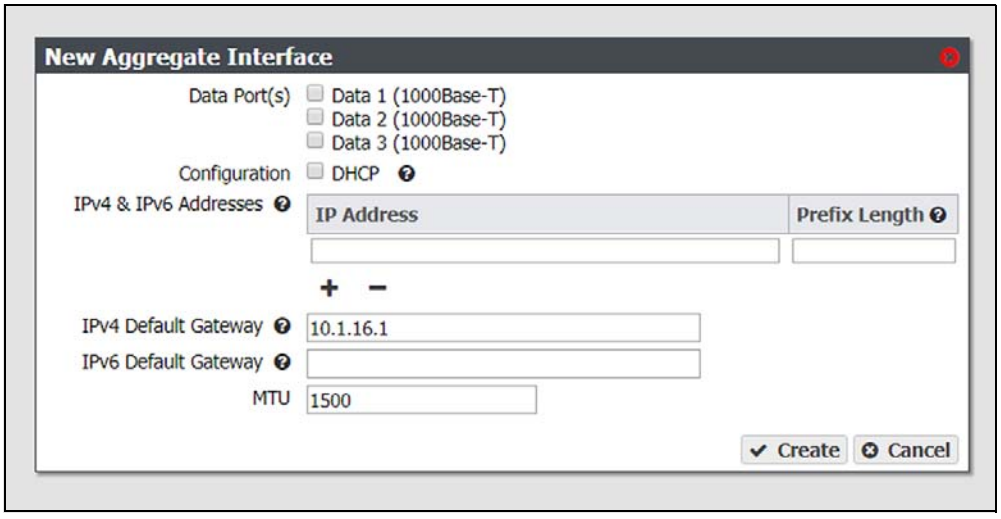


Figure 19 The New Aggregate Interface dialog box.

3. Select the **Data Port(s**) you want to configure into an aggregate data interface. Only one type of port can be used in an aggregation. For example, you cannot use both 10 GigE and 40 GigE ports in the same link aggregation.

4. Select **DHCP** to configure the system to automatically acquire an IPv4 address using DHCP. This setting does not apply to IPv6.
5. To configure a static IP address, click the **+** button and enter the following information:
   - **IP Address** — Enter a valid IPv4 or IPv6 address.

     Note: You cannot enter an IPv4 address if you selected DHCP in Step 4.
   - **Prefix Length** — Enter the subnet mask.

     Note: If desired, you can enter **Aliases**, multiple IP and prefix lengths assigned to the data port. Use the **+** button to configure additional IP and Netmask addresses. You can configure a maximum of 16 aliases.
6. If applicable, enter the **IPv4 Default Gateway**.

   Notes:
   - If you selected DHCP in Step 4, this option is unavailable.
   - The gateway entered for the last configured IPv4 connection sets the default gateway for the Verde NAS solution.
7. If applicable, enter the **IPv6 Default Gateway**.

   Notes:
   - The gateway entered for the last configured IPv6 connection sets the default gateway for the Verde NAS solution.
   - The IPv6 Gateway does not need to be configured when the Verde NAS solution is connected to a SLACC network.
8. Change the **MTU** (Maximum Transmission Unit) value, if desired. If you set the MTU value to something other than 1500, ensure that your switch configuration supports larger MTU settings, as well as all the hosts on the network.
9. Click **Save**.

Configure a Single Port Data Connection

Use the following instructions to configure a single port data connection.

1. From the menu bar, select **Configuration ···⁘ Network**, or click the Network pane on the Dashboard screen. The Network screen displays with information about the network connections of the NAS solution.

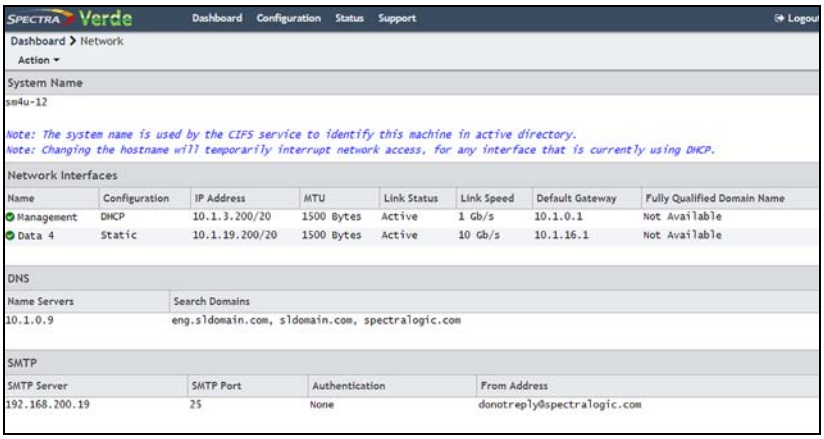


Figure 20 The Network screen.

2. Double-click the Data # row in the Network Interfaces pane for the port you want to configure, or select the Data # row and select **Action ···⁘ Edit** from the menu bar. The Edit Data # dialog box displays.

   Note: Depending on your hardware configuration, the Edit Data Ports dialog box may look different than what is shown below.

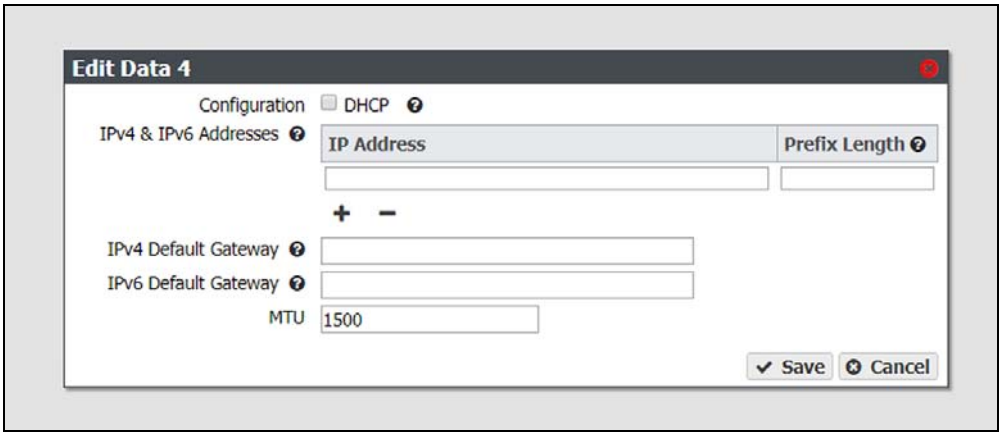


Figure 21 The Edit Data # dialog box.

3. Select **DHCP** to configure the system to automatically acquire an IPv4 address using DHCP. This setting does not apply to IPv6.

4. To configure a static IP address, click the **+** button and enter the following information:
   - **IP Address** — Enter a valid IPv4 or IPv6 address.

     Note: You cannot enter an IPv4 address if you selected DHCP in Step 3.
   - **Prefix Length** — Enter the subnet mask.

     Note: If desired, you can enter **Aliases**, multiple IP and prefix lengths assigned to the data port. Use the **+** button to configure additional IP and Netmask addresses. You can configure a maximum of 16 aliases.
5. If applicable, enter the **IPv4 Default Gateway**.

   Notes:
   - If you selected DHCP in Step 3, this option is unavailable.
   - The gateway entered for the last configured IPv4 connection sets the default gateway for the Verde NAS solution.
6. If applicable, enter the **IPv6 Default Gateway**.

   Notes:
   - The gateway entered for the last configured IPv6 connection sets the default gateway for the Verde NAS solution.
   - The IPv6 Gateway does not need to be configured when the Verde NAS solution is connected to a SLACC network.
7. Change the **MTU** (Maximum Transmission Unit) value, if desired. If you set the MTU value to something other than 1500, ensure that your switch configuration supports larger MTU settings, as well as all the hosts on the network.
8. Click **Save**.

Configure a Static Route

The Verde NAS solution only supports communication with one default gateway. When configuring a Verde NAS solution with multiple data connections, each connection communicates via the gateway entered when the connection was configured. The gateway entered for the last configured connection sets the default gateway for the Verde NAS solution.

When configuring a system with multiple data connections, if each data connection only communicates with its own network, a static route is not required. When an additional network or external network is only available from one, but not all, of the data connections configured on the Verde NAS solution, a static route is required in order for the system to communicate to the additional network.

For example, if one data connection is on the 10.2.2.x network and another connection is on the 10.2.4.x network, when the 10.2.3.x network is connected externally to the 10.2.4.x network, a static route must be configured on the Verde NAS solution to route communication with the 10.2.3.x network through the data connection on the 10.2.4.x network.

After creating the static route to the isolated network, you must create additional static routes to each specific host computer on the isolated network. If the Verde NAS solution receives a request from an IP address that is not configured to a static route, then the request is sent to the default gateway. If the default gateway is not connected to the IP address for isolation reasons, the request fails.

Note: Static routes are only used with IPv4 addresses.

Use the instructions in this section to configure a static route.

1. From the menu bar, select **Configuration ···⁘ Network**, or select the Network pane from the Dashboard screen. The Network screen displays (see Figure 20 on page 49).
2. From the menu bar, select **Action ···⁘ New Static Route**. The Static Route dialog box displays.

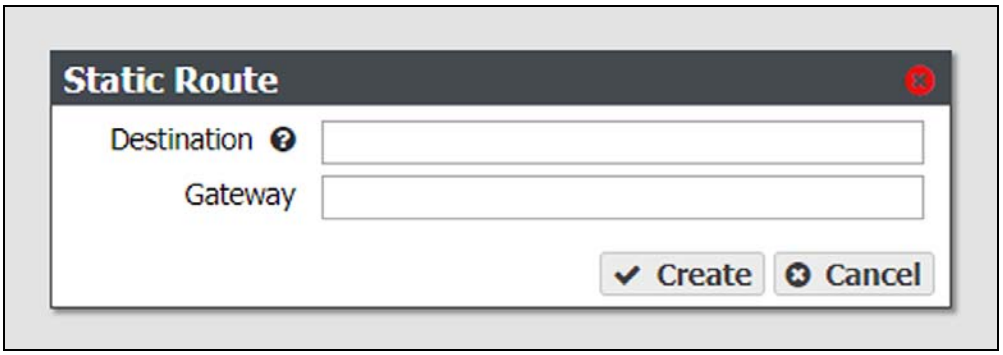


Figure 22 The Static Route dialog box.

3. In the **Destination** field, enter either an IPv4 host address or network address that you want to access through the data connection.
4. Enter the **Gateway** of the data connection used to communicate with the isolated network.
5. Click **Create**.
6. Repeat Step 2 on page 51 through Step 5 for each host computer on the isolated network.

CREATE A USER

Use the instructions in this section to create a new user.

Description of User Types

There are three different types of users in the Verde user interface. Administrator users, monitor users, and login users. Use the table below for a description of the user types.

User	Description
Administrator	An **administrator** account is created by default. This account can access the Verde user interface and has full control over all user interface functions. Starting with Verde 4.0, the default username for the primary administrator is **Administrator**, with the password **spectra**. If you upgraded from a previous version of Verde software, the existing administrator account "**spectra**" was retained and the **Administrator** account was automatically created without any permissions. **Note:** Spectra Logic recommends changing the password for the primary administrator. See Edit a User on page 125.
Monitor User	The **monitor** user account is created by default. This account can access all screens of the Verde user interface. This account is useful to view the status of the entire NAS solution. **Notes:** ▪ The monitor user can open any menu or function and attempt to edit settings, but these changes are ignored when the monitor user attempts to save the changes. ▪ For Verde software versions older than Verde 4.0, the monitor user account is created by default. If a system running Verde 3.x or older is upgraded to Verde 4.x or later, the existing monitor account is retained. ▪ The default username and password are both **monitor** using all lowercase letters. ▪ Spectra Logic recommends that you change the default password for the monitor account. See Edit a User on page 125.
Login User	A user with **Login** permissions is able to log into the Verde user interface. All users must have Login access to be able to log on to the Verde user interface.

Create a User

Use the instructions in this section to create users.

1. From the menu bar, select **Configuration ···⁘ Users.** The Users screen displays.

Figure 23 The Users screen.

2. Select **Action ···⁘ New** from the menu bar. The New User dialog box displays.

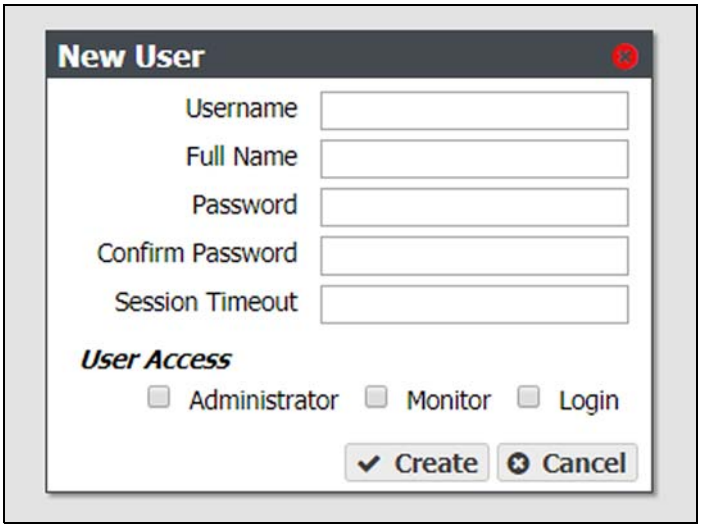


Figure 24 The New User dialog box.

3. Enter the desired **Username** for the user. The Username is limited to 16 characters and cannot contain capital letters, spaces, or special characters.
4. Enter the user's **Full Name**.
5. Enter and confirm the desired **Password** for the user.
6. If desired, enter a value for the **Session Timeout** in minutes. This value cannot exceed 999 minutes. If no value is entered, the NAS solution creates the user with the default setting of 60 minutes.
7. Select one or more **User Access** permissions. See Description of User Types on page 52 for information on each level of user access permission.

   Note: All users must have Login access to be able to log on to the Verde user interface.

8. Click **Create** to create the new user.

NEXT STEPS

The next steps depend on if you are configuring a Verde NAS solution as a standalone product, or if you plan to use your NAS solution in conjunction with a BlackPearl system.

- If you have a standalone Verde NAS solution, continue to Configuring Network Attached Storage on page 48.
- If you plan to use your Verde NAS solution with a BlackPearl system, skip to Network File Interface on page 186.

CHAPTER 3

Configuring Network Attached Storage

This chapter describes using the Verde user interface to configure Network Attached Storage (NAS) storage pools, volumes, and shares on a Verde NAS solution.

Topic	
Overview of NAS Storage Pools, Volumes, and Shares	page 56
Storage Pools	page 56
Volumes and Shares	page 56
Create a Storage Pool	page 57
Create a Volume	page 60
Create a Share	page 63
Create a CIFS Share	page 63
Create an NFS Share	page 67
Configure NAS Services	page 68
Configure the CIFS Service	page 69
Configure the NFI Service	page 69
Configure the NFS Service	page 70
Configure the NAS Replication Service	page 70
Configure Replication	page 71
Configure the NAS Replication Service	page 71
Configure the Target System	page 73
Configure Volumes for Replication	page 73

Overview of NAS Storage Pools, Volumes, and Shares

NAS Storage pools, volumes, and shares are the logical components used to interact with the data storage capacity provided by the Verde NAS solutions.

Storage Pools

A storage pool groups a set of physical drives together to create a virtual drive that the operating system treats as a single physical drive. Depending on how it is configured, a storage pool can provide mirrored, single-parity, double-parity, or triple-parity data protection. Higher levels of protection allow for more individual drives to fail before the data is compromised. The costs of higher protection are reduced storage availability and reduced performance.

Volumes and Shares

Volumes are located on each storage pool. Volumes can be configured with a minimum and maximum size. When you create a volume, you can specify whether it uses compression, and whether the time stamp for files is updated when the file is read (access time).

After the volume is created, it can be shared (made available for use by other computers on the network) via either the NFS service or the CIFS service.

Naming Considerations

When a volume is shared, the volume mount path uses a combination of the storage pool name and volume name. The combined name must have fewer than 78 ASCII characters, or the volume fails to mount. Additionally, storage pool names are limited to 48 characters, and volume names are limited to 62 characters. Even if the storage pool name is a single character, you are still restricted to 62 characters in the volume name.

CREATE A STORAGE POOL

When creating a new storage pool, keep the following in mind:

- Each storage pool requires a minimum of one drive. Spectra Logic recommends using eight drives or more in a storage pool to reduce the impact of the overhead. Overhead is the space on the storage pool used to store parity data, and not used for data storage.
- Drives can only be associated with one storage pool. To create a new storage pool using drives that are already configured in an existing storage pool, you must first delete the existing storage pool as described in Delete a Storage Pool on page 99. You can then create a new storage pool using newly available drives.
- You cannot mix drive types or sizes when creating a storage pool.
- Any drives not configured in storage pools act as global spare drives. If a drive failure occurs, the system immediately activates a global spare. If the global spare is in the same chassis as the storage pool that claimed it, when the failed drive is replaced it becomes the new global spare. If the global spare is in a different chassis than the storage pool that claimed it, when the failed drive is replaced it is rebuilt into the storage pool and the spare drive becomes a global spare again.
- Spectra Logic recommends leaving at least one drive for a global spare.

Use the following steps to create a new storage pool.

1. From the menu bar, select **Configuration ⋯⁘ NAS ⋯⁘ Pools**, or click the Pools pane on the Dashboard. The NAS Pools screen displays.

Figure 25 The NAS Pools screen.

2. Select **Action ⋯⁘ New.** A dialog box opens to show the default configuration options for the new pool.

   Note: The **Storage Pool Preview** pane does not display until you have selected the disks you want to use in the storage pool

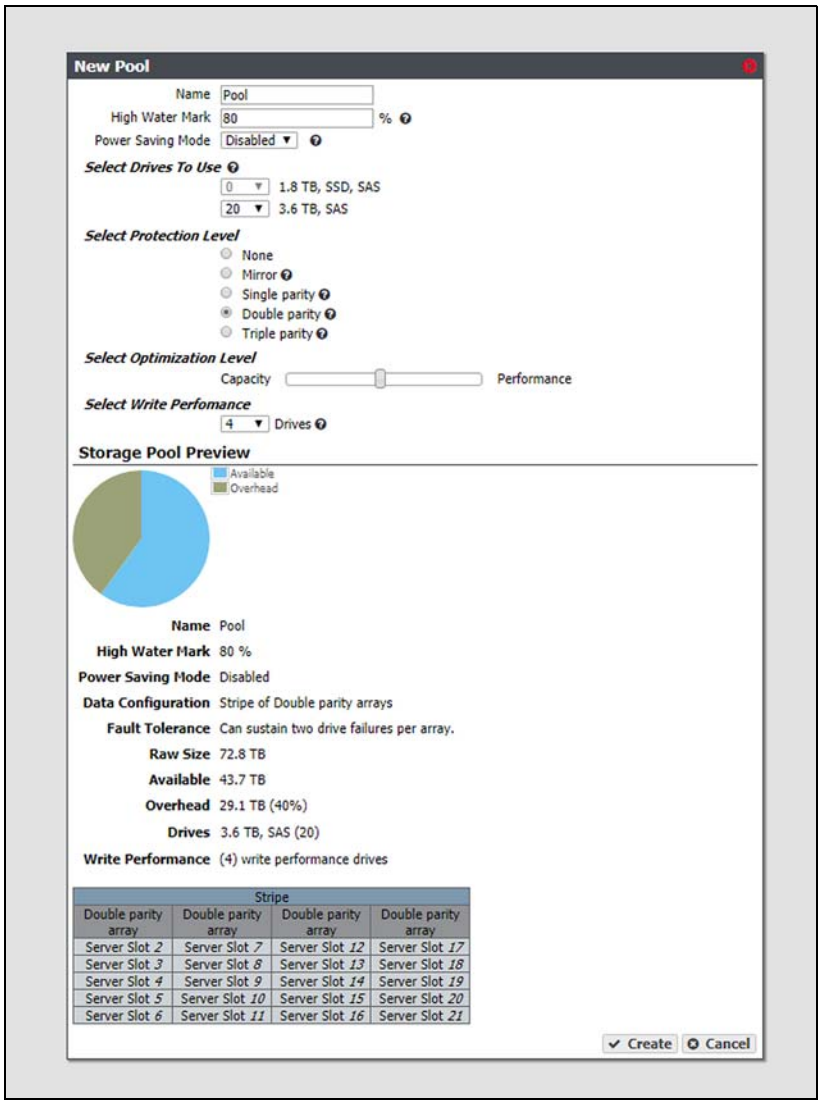


Figure 26 The New Pool dialog box.

3. Configure the storage pool as required for your environment. As you make changes, the screen updates to show the characteristics of the new pool.

For this option....	Do the following...
Name	Enter a name for the pool. Pool names are limited to 48 characters. **Notes:** ▪ The combined storage pool and volume name must be 78 characters or fewer. To avoid problems sharing volumes, Spectra Logic recommends a pool name of 32 characters or fewer. ▪ Each pool name must be unique. This field is case sensitive. Only the following special characters are allowed: hyphen (-), underscore (_), colon (:), and period(.).
High Water Mark	Enter a percentage. When the used space on the pool reaches this percentage, an alert is generated. Enter 0 if you do not want to set an alert level.
Power Saving Mode	Using the drop-down menu, select the desired **Power Saving Mode**. Enabling the power saving mode sets the standby timer to 60 minutes for all drives in the pool, but only if all drives in the pool are capable of using a standby timer. When the disk pool is idle for 60 minutes, the drives spin-down to conserve power.
Select Drives To Use	Use the drop-down menu to select the number of drives to include in the pool. If your system contains more than one type of disk drive, multiple drop-down menus are present, but only one type can be assigned to a pool. Any drive not in a storage pool acts as a global spare. A global spare drive is activated as soon as a drive configured in a storage pool fails.
Select Protection Level	Use the radio buttons to select the protection level for the pool. Only one option can be selected. Use the Storage Pool Preview information to compare the fault tolerance and required overhead for each configuration. **None** — The pool is not configured to provide data protection. Any drive failure results in data loss. **Mirror**—Data is striped across two mirrors. Any detected data corruption is corrected using checksums. This type of RAID offers the best performance for small random reads and writes. **Single parity** — Data is striped across multiple single-parity arrays, which can tolerate one drive failure without data loss. This type of RAID has faster performance than double- and triple-parity based RAIDs. **Double parity** — Data is striped across multiple double-parity arrays, which can tolerate two drive failures without data loss. In most cases, double-parity provides the best balance between data protection, performance, and storage capacity. **Triple parity** — Data is striped across multiple triple-parity arrays, which can tolerate three drive failures without data loss. This type of RAID provides the most data protection.

For this option....	Do the following...
Select Optimization Level	Use the slider to maximize either pool capacity or performance, or to mix the two options. Greater capacity means more storage space but slower performance. Higher performance means the pool is faster at reading or writing data with less overall capacity. **Note:** The Storage Pool Preview pane of the New Pool screen changes as you move the slider between Capacity and Performance to show the impact your changes have on the storage pool.
Select Write Performance	Use the drop-down menu to select the number of drives to use to increase write performance when the pool is shared using NFS. This feature is only intended for storage pools with NFS shares and typically has little impact on CIFS share performance.

4. Click **Create**. The NAS Pools screen displays. The storage pool is automatically created and is available for use immediately.

CREATE A VOLUME

Before you begin using a storage pool to store data, you must create one or more volumes to organize how the information is stored on the pool. After you create a volume, you can share the volume using NFS or CIFS, but not both.

Note: If you want to configure the volume to use the NFI service to automatically transfer files from the NAS storage to a BlackPearl system, configure the NFI service before configuring the volume. See Configure the NFI Service on page 69.

Use the following steps to create a volume on a storage pool.

1. From the menu bar, select **Configuration ⋯⁘ NAS ⋯⁘ Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays.

Figure 27 The Volumes screen.

2. Select **Action** ⋯⁘ **New**. The New Volume dialog box displays.

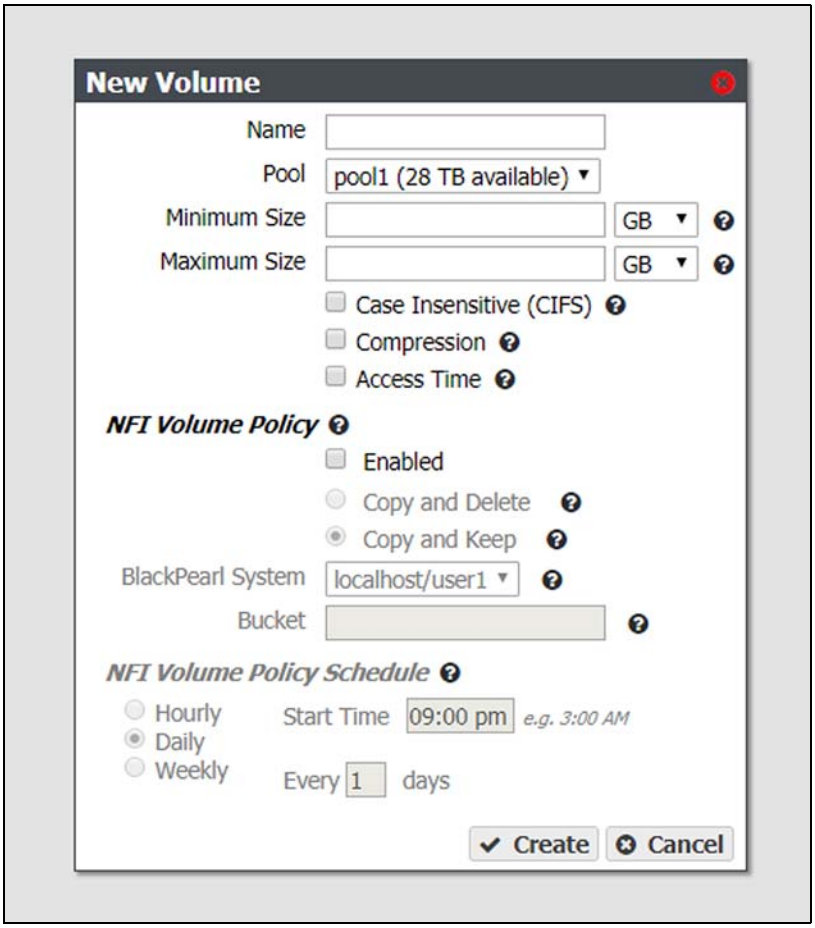


Figure 28 The New Volume dialog box.

3. Configure the volume as required for your environment.

For this option....	Do the following...
Name	Enter a name for the new volume. Volume names are limited to 62 characters or fewer. **Notes:** ▪ The combined storage pool and volume name must be 78 characters or fewer. ▪ NFS does not allow spaces in share names. As a result, any spaces in the volume name are replaced by underscores in the corresponding NFS share name. The Verde user interface displays the volume name without the underscores. For example, for a volume named **Share One**, the corresponding NFS share is named **Share_One** to external network computers, but it is named **Share One** in the Verde user interface.
Pool	Select the storage pool on which to create the volume. If there are multiple storage pools configured on the Verde NAS solution, use the drop-down menu to select the **Pool** where you want to create the volume.

For this option....	Do the following...
Minimum Size	Select the desired unit size from the drop-down menu and enter a numerical value for the minimum size in the text box to the left of the unit size drop-down menu. This space is allocated immediately if there is sufficient space available on the storage pool. If there is insufficient space available, volume creation fails. **Note:** Leave the **Minimum Size** and **Maximum Size** blank to create the volume with access to all available space on the storage pool.
Maximum Size	Select the desired unit size from the drop-down menu and enter a numerical value for the maximum size in the text box to the left of the unit size drop-down menu. **Notes:** ▪ Volumes are thin provisioned, so it is possible for the combined allocated maximum storage of all volumes to exceed the physical space available. ▪ Leave the **Minimum Size** and **Maximum Size** blank to create the volume with access to all available space on the storage pool.
Case Insensitive (CIFS)	If desired, select this option to configure the volume to treat all names as case insensitive, which can improve performance, especially in situations where directories contain a large number of files. **Note:** This option should be used for volumes shared using CIFS and **cannot** be changed after creating the volume. **CAUTION: DO NOT** enable this setting if you plan to share the volume using NFS.
Compression	If desired, select the check box to enable the Verde NAS solution to compress stored data. If the data being written is compressible there is an increase in write performance to the volume, which is dependent on how much compression occurs on the data being written. The data compression process uses CPU cycles to perform the compression. If compression is enabled and non-compressible data is written to the volume, the compression process may use an excessive number of CPU cycles, slowing the overall performance of the system.
Access Time	If desired, select the check box to configure the system to update the time stamp of a file when it is read from the volume. Selecting **Access Time** may slow performance.

Note: The options for the **NFI Volume Policy** are only used in conjunction with a BlackPearl system. To configure NFI, see Appendix A Network File Interface on page 186.

4. Click **Create**. The Volumes screen refreshes to show the new volume.

CREATE A SHARE

After you create one or more volumes, you can share a volume using either the NFS or CIFS service. Decide which method to use for sharing and follow the appropriate instructions below.

- Create a CIFS Share below
- Create an NFS Share on page 67

Note: Shares are not available until network settings are configured. See Configure the Data Connection on page 46.

Create a CIFS Share

Spectra Logic recommends using Active Directory to control access to CIFS shares on the Verde NAS solution. However, if your Windows operating system environment does not use Active Directory, you can enable local administrator status on the system to allow a specified user to access the CIFS shares in a Windows workgroup environment. The username and password configured on the Verde NAS solution are used to access the CIFS shares when using a Windows workgroup environment.

Join an Active Directory Domain

If your Windows environment uses Active Directory, you must join an Active Directory domain before creating a CIFS share. See Configure the Active Directory Service on page 112 for more information.

After joining an Active Directory domain, continue with Create a CIFS Share on page 64.

Enable Local Administrator Status

If your Windows environment does not use Active Directory and you have not previously done so, you must edit a user to enable local administrator status. If you have previously enabled local administrator status for a user, continue with Create a CIFS Share on page 64.

Note: Alternatively, you can create a new user with local administrator status. See Create a User on page 53.

1. From the menu bar, select **Configuration ⋯⁘ Users**. The Users screen displays.

Figure 29 The Users screen.

2. Double-click the row for the user for which you want to enable local administrator status, or select the user, and then select **Action ⋯⁘ Edit**. The Edit User dialog box displays.

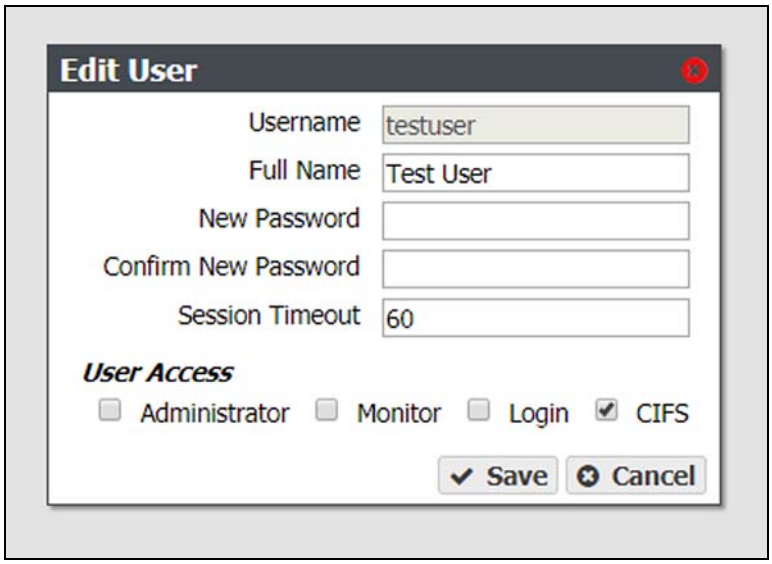


Figure 30 The Edit User dialog box.

3. Select the **CIFS** check box to configure the user with local administrator status on the system.
4. If desired, change other settings as described in Edit a User on page 125.
5. Click **Save**.

Create a CIFS Share

1. From the menu bar, select **Configuration ⋯⁘ NAS ⋯⁘ Shares ⋯⁘ CIFS**. The CIFS Shares screen displays.

Figure 31 The CIFS Shares screen.

2. Select **Action** ⋯⁘ **New**. The New CIFS Share dialog box displays to show the options for creating a new share.

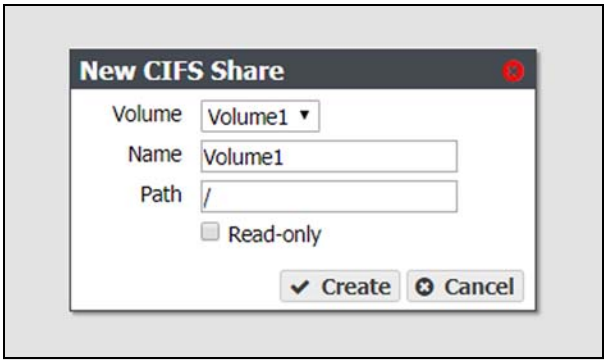


Figure 32 The New CIFS Share dialog box.

3. Use the drop-down menu to select the **Volume** you want to share.
4. Set the **Name** for the CIFS share. This is the name that is displayed in Active Directory configurations.
5. The network address displayed for **Path** is the address of the share you are currently configuring. The default path allows access to the root of the volume.

   Note: After creating the CIFS share, you can connect to it using your Windows-based host and create subdirectories in the share. You can then edit the share and use the **Path** field to allow access to specific directories by specifying the exact subdirectory (see Edit a Share on page 111).

   For example, if you enter `/home/user` in the path field, any user that connects to this CIFS share only has access to the "`user`" directory, even if the "`home`" volume contains other directories.

6. If desired, select **Read-only** to configure the CIFS share as read only.
7. Click **Create**. The newly created share is listed on the CIFS Shares screen.

Set Permissions for CIFS Share

When a CIFS share is created, the default permission is "Everyone". This allows a user creating the initial shares to easily set the proper permissions for additional users without requiring the Active Directory Domain administrator password.

1. Mount the new CIFS share to your Microsoft Windows operating system host.

2. Using Windows Explorer, right-click on the CIFS share, and select **Properties**. The General tab of the Properties window displays.

   Note: You cannot use the Computer Management panel to set permissions on CIFS shares.

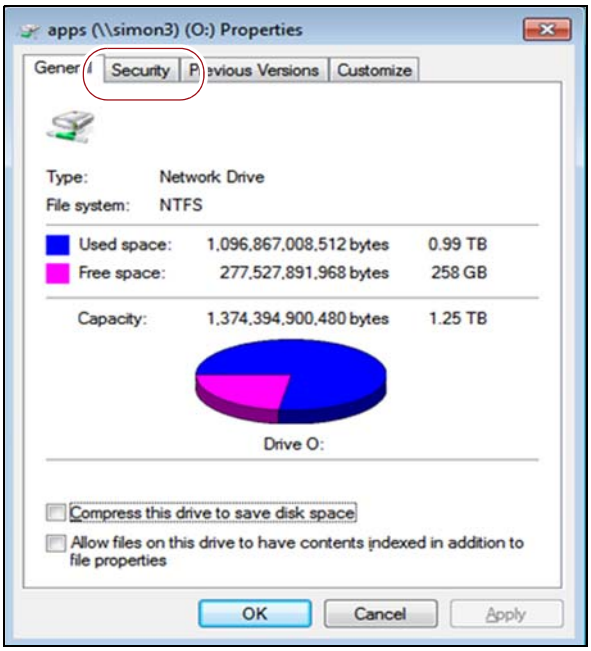


Figure 33 The Properties window.

3. Click **Security**. The Security tab displays.

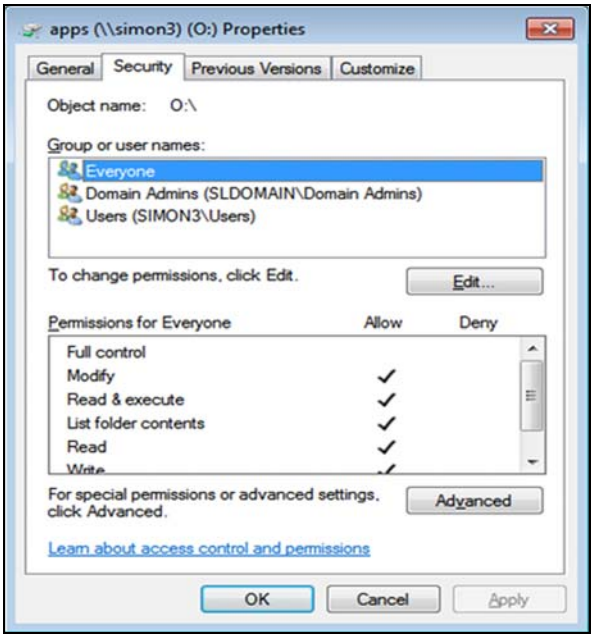


Figure 34 The Security tab.

4. Add, or remove users, or modify permissions for users as needed for your storage environment.
5. Click **OK**.

Create an NFS Share

Use the following steps to create an NFS share.

1. From the menu bar, select **Configuration ···⁘ NAS ···⁘ Shares ···⁘ NFS**. The NFS Shares screen displays.

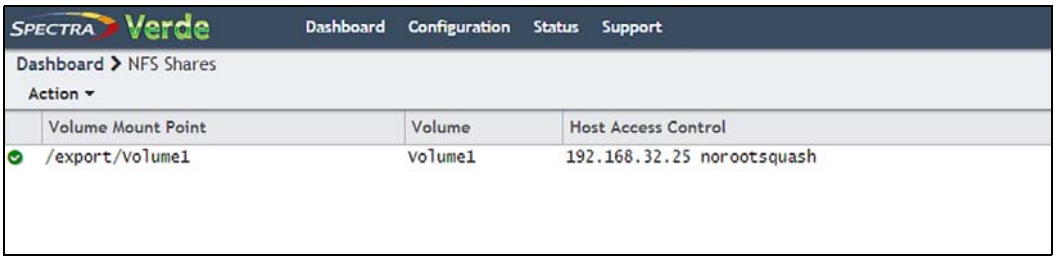


Figure 35 The NFS Shares screen.

2. Select **Action ···⁘ New**. The New NFS Share dialog box displays.

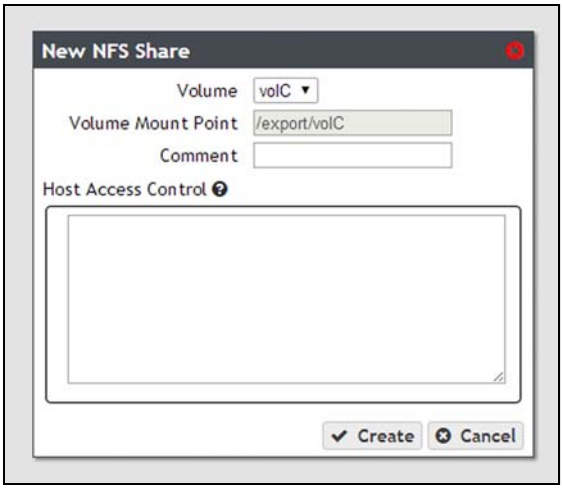


Figure 36 The New NFS Share dialog box.

3. Use the drop-down menu to select the **Volume** you want to share.
4. The network address displayed for **Volume Mount Point** is the address of the share you are currently configuring.

   Note: Before mounting an NFS share, make sure the client supports the NFSv3 protocol and properly handles file locking.

5. If desired, enter a comment in the **Comment** field. This comment only displays on the Verde user interface.

6. In the **Host Access Control** entry field, enter the IP address and permission level of all hosts that you want to access the volume. Hosts not listed are not able to access the volume. In addition to the host IP address, you must include one of the following permission parameters for each host you add to the Verde NAS solution.

Parameter	Description
norootsquash	**Root Access** — The host can access the NFS share with root access to the share. This host is used to set permissions for rootsquash users.
rootsquash	**Standard Access** — The host can access the NFS share, but does not have root access. Standard access allows write permission to the share, but does not allow the user to delete, modify, or rename files for which they do not have write permission.
ro	**Read Only** — The host can access the NFS share, but cannot write data to the shared volume.

For example, entering "`192.168.32.25 rootsquash`" allows the specified host to access the share with standard access.

If you want to allow all hosts to access the share, type `*` and include the permission parameter. For example, entering "`* norootsquash`" allows all hosts to access the share with root access.

7. Click **Create**. The newly created share is listed on the NFS Shares screen.

CONFIGURE NAS SERVICES

The NAS Services - CIFS, NFI, NFS, and Replication - are methods of sharing NAS volumes for use by other computers on the network.

Figure 37 The Services screen.

Configure the CIFS Service

There are no configurable settings for the CIFS service at this time, but you can add an advanced parameter, if desired.

Note: For information about using CIFS shares and joining an Active Directory domain, see Create a CIFS Share on page 56.

Add Advanced Parameter

Advanced parameters are used to adjust/set global or share specific Samba parameters.

Caution Improperly configuring advanced parameters can expose security vulnerabilities and other serious issues. Advanced parameters should not be configured without a full understanding of the consequences.

1. From the menu bar, select **Configuration ···⁘ Services**. The Services screen displays (see Figure 37 on page 68).
2. Double-click the **CIFS** row, or select the **CIFS** row and select **Action ···⁘ Show Details**. The CIFS details screen displays.
3. Select **Action ···⁘ Add Advanced Parameter**. The Add Advanced Parameter dialog box displays.

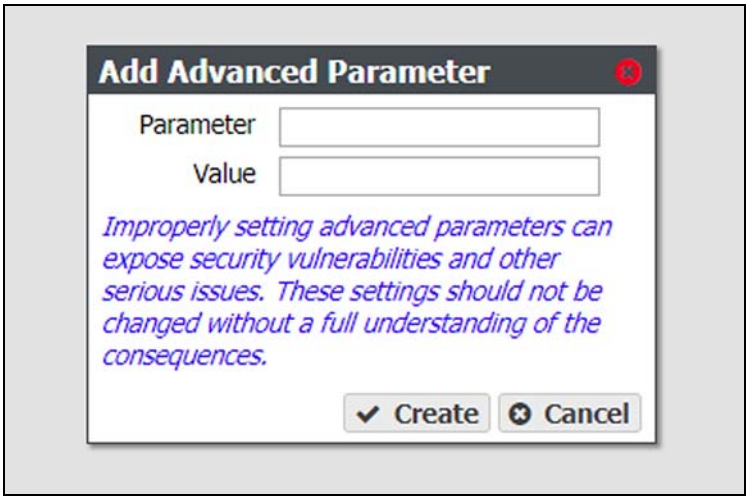


Figure 38 The Add Advanced Parameter dialog box.

4. Enter the desired **Parameter** and **Value**.
5. Click **Create**.

Configure the NFI Service

The NFI service is only used in conjunction with a BlackPearl Converged Storage system. For information on configuring the NFI service, see Appendix A Network File Interface on page 186.

Configure the NFS Service

The Verde user interface lets you configure the transmission protocols and number of threads used by the NFS service.

Use the following steps to edit the NFS service.

1. Select **Configuration ···⁘ Services** to display the Services screen (see Figure 37 on page 68).
2. Double-click the NFS service, or select the service, and then select **Action ···⁘ Show Details**. The NFS service details screen displays.
3. On the NFS service details screen, select **Action ···⁘ Edit**. The Edit NFS Service dialog box displays.

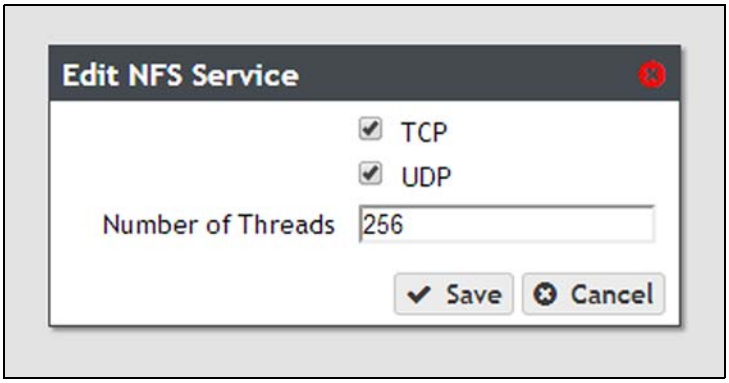


Figure 39 The Edit NFS Service dialog box.

4. Select or clear the **TCP** and **UDP** transmission protocols to enable or disable them, respectively.
5. Set the number of **Threads** for use by the service.

   Note: The default setting is sufficient for most network configurations.
6. Click **Save**.

Configure the NAS Replication Service

For instructions on configuring the NAS replication service, see Configure the NAS Replication Service on page 71.

CONFIGURE REPLICATION

If the Verde NAS solution is on a network with other Verde NAS solutions, BlackPearl NAS solutions, or BlackPearl Converged Storage systems with NAS enabled, you can select to replicate data from the NAS volumes on the system to one or multiple NAS replication targets. Replication uses the same data interface that the system uses for normal file storage operations, so replication to multiple targets may decrease transfer speeds.

Once you configure the Replication service, you need to configure each folder on the system that you want to replicate. Use the instructions in this section to configure the Replication service and to configure folders for replication.

Notes:

- This replication service is only for replicating NAS volumes on the system to other systems with NAS enabled. To replicate NAS volumes to BlackPearl managed object storage, use NFI replication (see Configure the NFI Service on page 69).
- There must be enough space on the destination system to hold the replicated data, or the replication fails.
- Multiple volumes on the source system cannot replicate to a single volume on the target. Each volume on the source system must replicate to a different volume on the target.
- If multiple Verde NAS solutions replicate to the same target, the target must use a different volume for each replication source.
- You must configure the data port on the source system and the target system(s) before you can configure replication (see Configure Ethernet Ports on page 101).
- Your firewall must allow the source system and all targets configured for replication to access port 59373 for configuring replication, and ports 59374-59400 for replication data transfers.

Configure the NAS Replication Service

Use the instruction in this section to configure the NAS replication service.

Note: For both the source system and the targets, make sure you have completed the steps in Chapter 2 – Initial Configuration starting on page page 38.

1. Select **Configuration ⋯⁘ Services** to display the Services screen (see Figure 37 on page 68).

2. Double-click the Replication service, or select the service, and then select **Action ···⁘ Show Details**. The Replication service details screen displays.

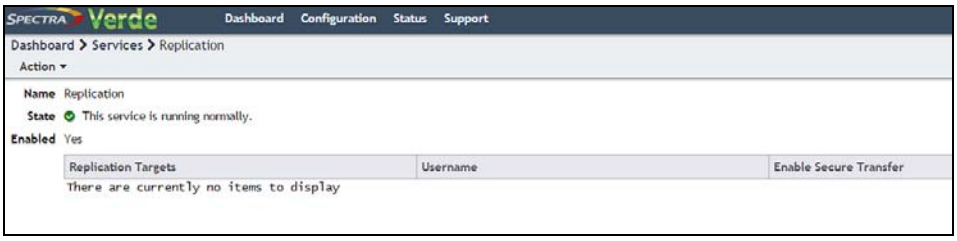


Figure 40 The Replication service details screen.

3. Select **Action ···⁘ Create**. The Add Replication Target dialog box displays.

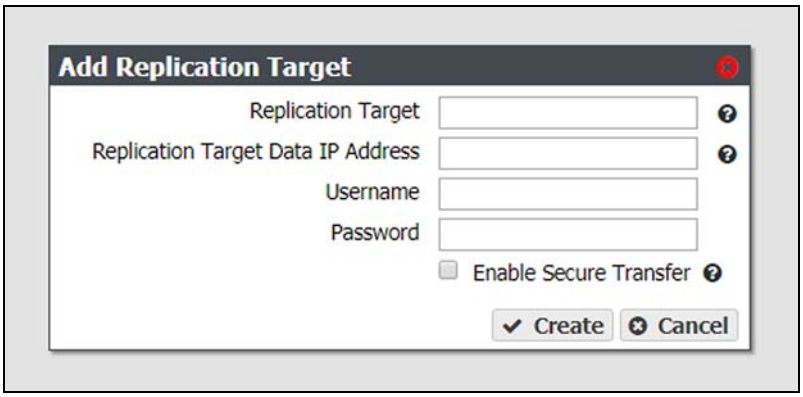


Figure 41 The Add Replication Target dialog box.

4. Enter the IP address or hostname of the target's management port in the **Replication Target** field.

   Note: Do not use http:// or https:// to precede the IP address or hostname.

5. Enter the IP address of the target's data port in the **Replication Target Data IP Address** field.

   Note: Do not use http:// or https:// to precede the IP address or hostname.

6. Enter the username of a user with administrator privileges configured on the target in the **Username** field.

7. Enter the user password in the **Password** field, if one is set. Otherwise, leave the field blank.

8. Select the **Enable Secure Transfer** check box to configure the **source system** to encrypt the replicated data before transferring it to the **target system**. Data is encrypted using Secure Socket Layer (SSL).

9. Click **Save**.

Configure the Target System

1. Log into the Verde user interface on the **target system** as described in Log In to the Verde User Interface on page 44.
2. Create one or more storage pools as described in Create a New Storage Pool on page 49.
3. Create one or more volumes as described in Create a New Volume on page 53. You must create one volume on the **target system** for each volume you want to replicate on the **source system**. Otherwise, you can create volumes when performing the steps in Configure Volumes for Replication, below.

Caution You cannot use this volume for normal data storage operations, it can only be used as a replication target. Any data in the specified target volume is deleted each time the source system replicates data to the target system.

Configure Volumes for Replication

1. In the source system's user interface, select **Configuration ⋯⁘ NAS ⋯⁘ Volumes**. The Volumes screen displays.
2. Double-click the volume name you want to configure to replicate, or select the folder and select **Action ⋯⁘ Show Details**. The details screen for the volume displays.
3. Select **Action ⋯⁘ Configure Replication**. The Configure Replication dialog box displays.

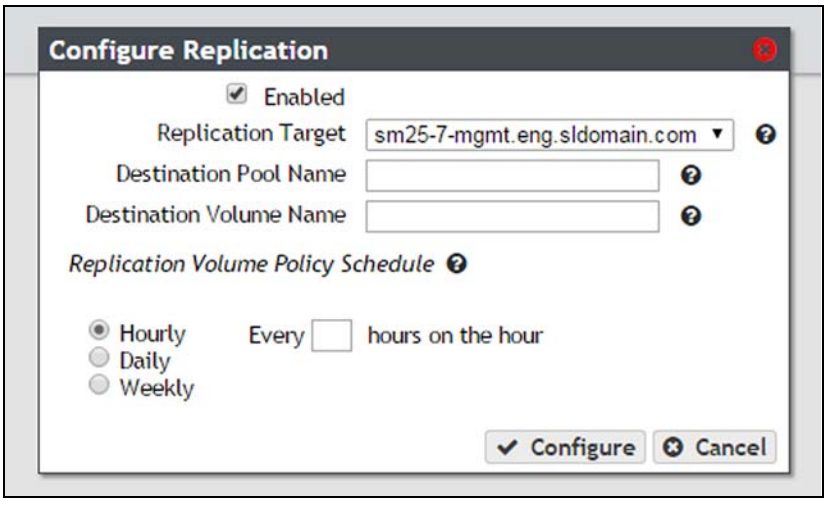


Figure 42 The Configure Replication dialog box.

4. Select the **Enabled** check box. The options below are greyed out and not configurable until this check box is selected.

5. Select the **Replication Target** from the drop-down menu. The targets are listed by the IP address or hostname entered in Step 4 on page 72. If you only configured the system to replicate to a single target, the target is preselected.
6. Enter the name of the storage pool on the target system you want to use for replication in the **Destination Pool Name**. This field is case sensitive.
7. Enter the name of a volume that resides on the target storage pool you selected in Step 6 in the **Destination Volume Name** field, or enter the name for a new volume to be created on the specified storage pool. This field is not case sensitive.

Caution You cannot use this volume for normal data storage operations, it can only be used as a replication target. Any data in the specified target volume is deleted each time the source system replicates data to the target system.

   - If the volume does not exist on the target, it is created.
   - If the volume exists on the target, a warning message displays informing you that any data currently in the target folder is erased each time data is replicated. Confirm the warning message to continue.

8. Select the Hourly, Daily, or Weekly radial button for the **Replication Volume Policy Schedule**. The dialog box changes to show the configuration options for your selection. Use one of the sections below to complete the replication configuration for this volume.
   - Create an Hourly Schedule below — Replicate data every selected number of hours.
   - Create a Daily Schedule on page 75 — Replicate data every selected number of days.
   - Create a Weekly Schedule on page 76 — Replicate data on certain days of the week.

Create an Hourly Schedule

1. Select Hourly as the interval for the replication schedule (see Figure 42 on page 73).
2. Enter a number for **Every _ hours on the hour**. This value specifies the interval, in hours, between replicating data. For example, if this value is set to 4, the system replicates data every four hours.
3. Click **Create**.

Create a Daily Schedule

1. Select **Daily** as the interval for the replication schedule. The dialog box changes to display options for the daily interval setting.

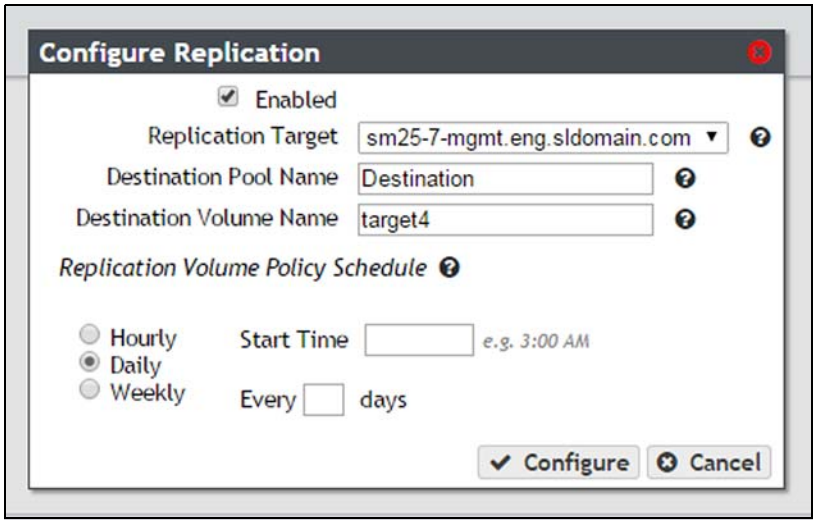


Figure 43 The Configure Replication dialog box showing the daily interval options.

2. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
3. Enter a number for **Every _ days**. This value specifies the interval, in days, between replicating data. For example, if this value is set to 2, the system replicates data every two days at the time specified in Step 2.
4. Click **Create**.

Create a Weekly Schedule

1. Select **Weekly** as the interval for the replication schedule. The dialog box changes to display options for the weekly interval setting.

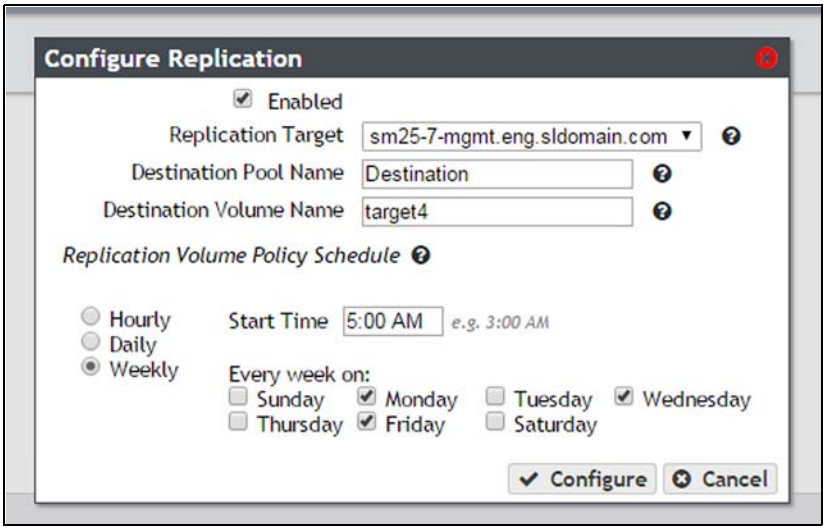


Figure 44 The Configure Replication dialog box showing the weekly interval options.

2. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
3. Select one or more days for **Every week on:**. This determines the day(s) of each week the system replicates data. For example, based on the selections in Figure 44, the system replicates data every Monday, Wednesday, and Friday at 5:00 AM.
4. Click **Create**.

CHAPTER 4

Managing Network Attached Storage

This chapter describes using the Verde user interface to manage NAS storage pools, volumes, and shares on the NAS solution after initial configuration. For initial configuration steps, see Chapter 3 – Configuring Network Attached Storage on page 55.

Topic	
Managing Storage Pools	page 78
Edit a Storage Pool	page 78
Expand a Storage Pool	page 79
Delete a Storage Pool	page 80
Managing Volumes	page 80
Move a Volume	page 81
Cancel a Volume Move	page 81
Edit a Volume	page 82
Delete a Volume	page 84
Volume Snapshots	page 84
Create a Snapshot	page 85
Create a Snapshot Schedule	page 86
Delete a Snapshot	page 89
Restore to a Snapshot	page 90
Retrieve a Single File from a Snapshot	page 91
Managing Shares	page 92
Edit a CIFS Share	page 92
Delete a Share	page 93
Managing NAS Replication	page 94
Manually Start NAS Replication	page 94
Cancel a NAS Replication In Progress	page 95
Restoring Files from a NAS Replication Target	page 96

Topic	
Disable a NAS Replication for a Volume	page 96
Edit the NAS Replication Service	page 97
Delete the NAS Replication Service Configuration	page 98

MANAGING STORAGE POOLS

After creating one or more storage pools, use the instructions in this section to edit, expand, or delete a pool.

Edit a Storage Pool

You can edit an existing storage pool to change the value of the high water mark and the number of write performance drives. Use the following steps to edit a storage pool.

1. From the menu bar, select **Configuration ···⁘ NAS ···⁘ Pools**, or click the Pools pane on the Dashboard. The NAS Pools screen displays (see Figure 25 on page 57).
2. Select the pool you want to edit and select **Action ···⁘ Edit**. The Edit *pool name* dialog box displays.

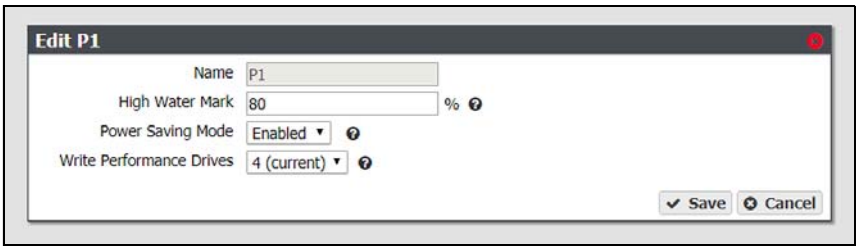


Figure 45 The Edit *pool name* dialog box.

Note: The **Name** field is greyed out and cannot be changed.

3. If desired, enter a percentage for the **High Water Mark**. When the used space on the pool reaches this percentage, an alert is generated. Enter 0 if you do not want to set an alert level.
4. If desired, enable or disable **Power Saving Mode** for the storage pool. Enabling this feature configures the standby timer to 60 minutes. When there is no I/O to the storage pool for 60 minutes, the drives in the pool spin down and use minimal power.

   Note: All drives in the storage pool must be power-saving compatible.
5. If desired, use the **Write Performance Drives** drop-down menu to select the number of write performance drives to allocate to the storage pool.
6. Click **Save**.

Expand a Storage Pool

You can resize an existing storage pool to include more physical drives present in the system. This is useful if you just purchased and installed additional drives.

Use the following steps to expand a storage pool.

1. From the menu bar, select **Configuration ···⁘ NAS ···⁘ Pools**, or click the Pools pane on the Dashboard. The NAS Pools screen displays (see Figure 18 on page 50).
2. From the list of existing storage pools, select the storage pool you want to expand, and then select **Action ···⁘ Expand**. The Expand *pool name* dialog box displays options for adding additional drives to the storage pool.

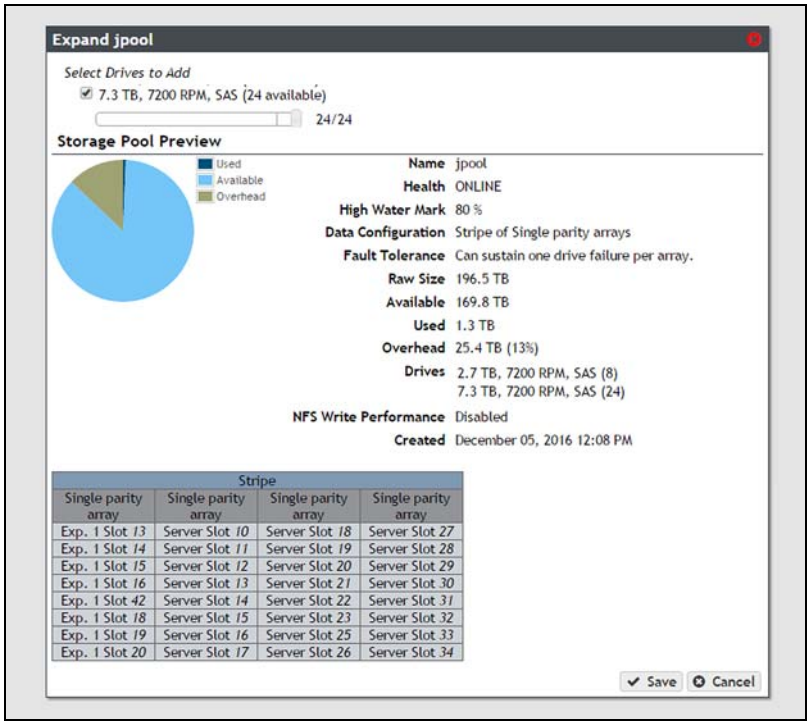


Figure 46 The Expand *pool name* dialog box.

3. Use the slider to increase the number of drives to use in the storage pool. As you make changes, the graphics beneath the slider update to show the impact your changes have on the storage pool.
4. When you are satisfied with the new configuration, click **Save**.

Delete a Storage Pool

If you want to create a new storage pool and existing storage pools use all of the available drives, you must delete an existing storage pool to make drives available for the new storage pool.

Caution When you delete a storage pool, all data on it is lost. If you want to keep the data, migrate it to another location before deleting the pool.

Use the following steps to delete a storage pool.

1. From the menu bar, select **Configuration ⋯ NAS ⋯ Pools**, or click the Pools pane on the Dashboard. The NAS Pools screen displays (see Figure 18 on page 50).
2. From the list of existing storage pools, select the storage pool you want to delete, and then select **Action ⋯ Delete**. A dialog box displays asking you to confirm the deletion.

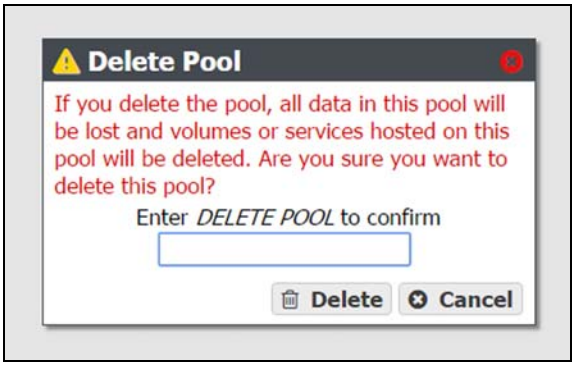


Figure 47 Confirm the storage pool deletion.

3. Type `DELETE POOL` in the entry field and click **Delete** to delete the storage pool.
4. If desired, create a new storage pool that includes the disks no longer in use, as described in Create a New Storage Pool on page 49.

MANAGING VOLUMES

After creating one or more volumes, use the instructions in this section to move, edit, or delete a volume.

Move a Volume

If desired, you can move a volume from one storage pool to another. There must be sufficient space for the volume on the destination storage pool.

Note: There is a decrease in performance in file storage operations on a volume that is being moved.

Important Access to CIFS shares is lost when moving the share and simultaneously transferring data to, or from, the share.

Use the following steps to move a volume to a different storage pool.

1. From the menu bar, select **Configuration ···⁘ NAS ···⁘ Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 20 on page 53).
2. Select the volume you want to move to a different storage pool, and then select **Action ···⁘ Move**. The Move Volume dialog box displays.

Figure 48 Select the destination pool for the volume.

3. Use the drop-down menu to select the destination pool for the volume.
4. Click **Move**. The volume is moved to the selected pool.

Cancel a Volume Move

If desired, you can cancel the move of a volume from one storage pool to another.

1. From the menu bar, select **Configuration ···⁘ NAS ···⁘ Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 27 on page 60).
2. Select the volume you want to cancel moving to a different storage pool, and then select **Action ···⁘ Cancel Move**. The Cancel Move Volume dialog box displays.
3. Confirm cancelling the in-progress volume move.

   Note: The data on the target pool is deleted. Data on the source pool is unaffected and persists on the source pool after canceling the move.

Edit a Volume

After creating a volume, you can edit it to change the volume configuration. Use the following steps to edit a volume.

1. From the menu bar, select **Configuration ···⁘ NAS ···⁘ Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 20 on page 53).
2. Double-click the volume you want to edit, or select the volume and then select **Action ···⁘ Edit**. The Edit *volume name* screen displays.

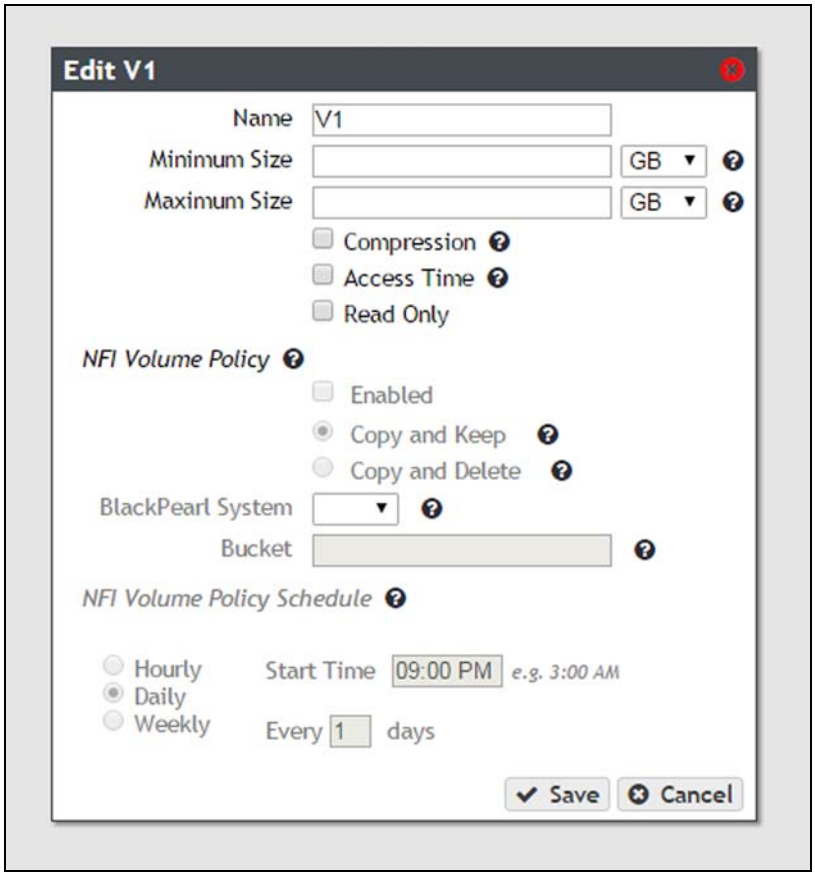


Figure 49 The Edit *volume name* screen.

3. Change the configuration of the volume as required for your environment.

For this option....	Do the following...
Name	Enter a new name for the volume. Volume names are limited to 62 characters or fewer. **Notes:** ▪ The combined storage pool and volume name must be 78 characters or fewer. ▪ NFS does not allow spaces in share names. As a result, any spaces in the volume name are replaced by underscores in the corresponding NFS share name. The Verde user interface displays the volume name without the underscores. For example, for a volume named **Share One**, the corresponding NFS share is named **Share_One** to external network computers, but it is named **Share One** in the Verde user interface. ▪ If you change the name of a volume that is being shared, the share point is maintained after the volume name change.
Minimum Size	Select the desired unit size from the drop-down menu and enter a numerical value for the minimum size in the text box to the left of the unit size drop-down menu. This space is allocated immediately if there is sufficient space available on the storage pool. If there is insufficient space available, saving the modified volume fails.
Maximum Size	Select the desired unit size from the drop-down menu and enter a numerical value for the maximum size in the text box to the left of the unit size drop-down menu. **Notes:** ▪ The maximum size must be greater than the current amount of used space on the volume. ▪ Volumes are thin provisioned, so it is possible for the combined allocated maximum storage of all volumes to exceed the physical space available.
Compression	If desired, select the check box to enable the Verde NAS solution to compress data stored on the system. **Note:** Changing the compression setting only affects data written to the volume after the compression setting is changed. It does not affect data already on the volume.
Access Time	If desired, select the check box to configure the system to update the time stamp of a file when it is read from the volume. Selecting **Access Time** may slow performance.
Read Only	If desired, select the check box to configure the volume so that data can be read, but not written to the volume.

Note: The options for the **NFI Volume Policy** are only used in conjunction with a BlackPearl system. To configure NFI, see Appendix A Network File Interface on page 186.

4. Click **Save**.

Delete a Volume

1. From the menu bar, select **Configuration ···⁘ NAS ···⁘ Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 20 on page 53).
2. Select the volume you want to delete and then select **Action ···⁘ Delete**. A dialog box displays asking you to confirm the deletion.

Caution Deleting a volume deletes all data in the volume. This action cannot be undone.

Figure 50 Confirm the volume deletion.

3. Type `DELETE VOLUME` in the entry field and click **Delete** to delete the volume.

VOLUME SNAPSHOTS

Volume Snapshots are images of a volume's configuration and data makeup as they were when the snapshot was generated. Restoring to a previously created snapshot allows you to go "back in time" and restore the volume to the state it was in when the snapshot was created. Snapshots can be useful in restoring a file that was accidentally deleted. Snapshots can be created manually or on a schedule. Volume snapshots are retained on the system until they are manually deleted, or the set Maximum Number of Snapshots limit is reached. When the limit is reached, the oldest snapshot is deleted freeing up capacity held by that snapshot.

Snapshots are created instantly without any impact to system performance. Snapshots initially occupy very little space on the storage pool, but grow as data is deleted, because this data must be retained by the snapshot.

For example, if you write 100 GB to the volume, and then make a snapshot of that data, the snapshot is only a few kilobytes in size, as it simply points to the existing data. However, if that 100 GB is deleted, the snapshot grows to 100 GB, because it must retain the data. When the snapshot containing the 100 GB of data is deleted, either manually or based on schedule retention, then 100 GB of capacity is made available for new data.

Create a Snapshot

Use the following steps to create a snapshot.

1. From the menu bar, select **Configuration ⋯⁘ NAS ⋯⁘ Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 20 on page 53).
2. Double-click the volume you want to use to create a snapshot, or select the volume, and then select **Action ⋯⁘ Show Details**. The details screen for that volume displays.

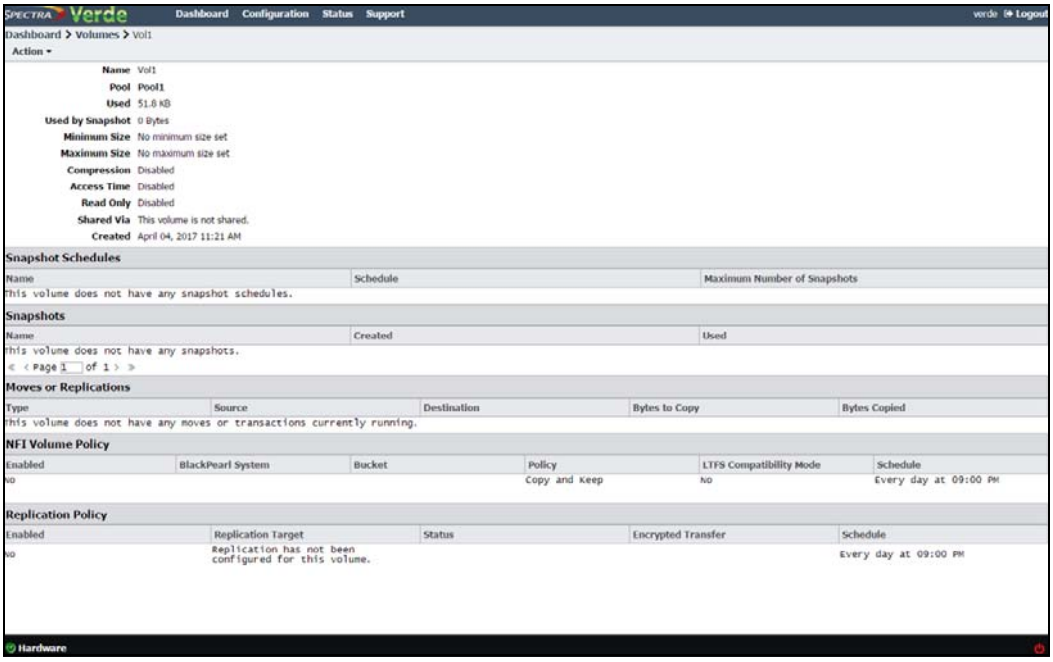


Figure 51 The Volume details screen.

3. On the Volume details screen, select **Action ⋯⁘ New Snapshot**. The New Snapshot dialog box displays.
4. Enter a name for the snapshot in the **Name** field.

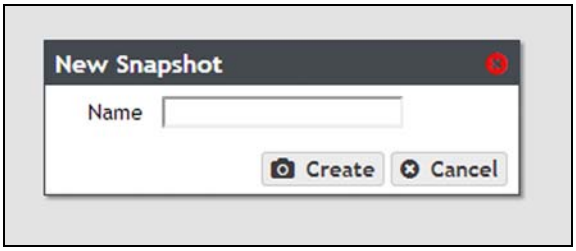


Figure 52 The New Snapshot dialog box.

5. Click **Create**. The Volume details screen displays showing the newly created snapshot.

Create a Snapshot Schedule

Snapshot schedules can be configured at intervals based on hours, number of days, or days of the week. Decide which interval to use for the schedule and follow the appropriate instructions.

- Create an Hourly Schedule below—Create snapshots every selected number of hours.
- Create a Daily Schedule on page 87—Create snapshots every selected number of days.
- Create a Weekly Schedule on page 87—Create snapshots on certain days of the week.

Create an Hourly Schedule

1. On the Volume details screen (see Figure 51 on page 85), select **Action ⋯ New Snapshot Schedule**. The New Snapshot Schedule dialog box displays.
2. Select **Hourly** as the interval for the snapshot schedule. The dialog box changes to display options for the hourly interval setting.

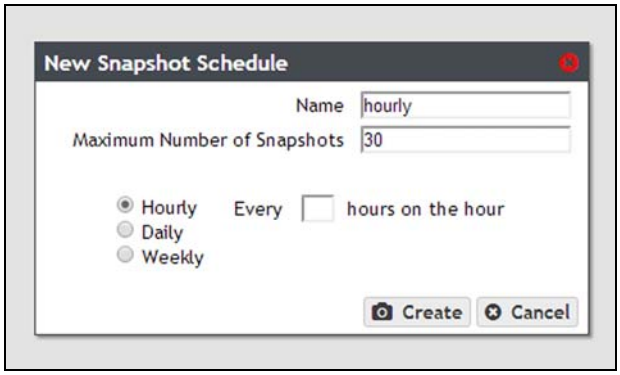


Figure 53 The New Snapshot Schedule dialog box showing the hourly interval options.

3. Change the default name of the snapshot schedule, if desired.
4. Enter a number for the **Maximum Number of Snapshots**. When the maximum number is reached, the system deletes the oldest snapshot.
5. Enter a number for **Every _ hours on the hour**. This value specifies the interval, in hours, between generating snapshots. For example, if this value is set to 4, the system creates a snapshot every four hours. The maximum setting for this field is 48, where the system creates a snapshot every two days.
6. Click **Create**.

Create a Daily Schedule

1. On the Volume details screen (see Figure 51 on page 85), select **Action ⋯⁘ New Snapshot Schedule**. The New Snapshot Schedule dialog box displays.
2. Select **Daily** as the interval for the snapshot schedule. The dialog box changes to display options for the daily interval setting.

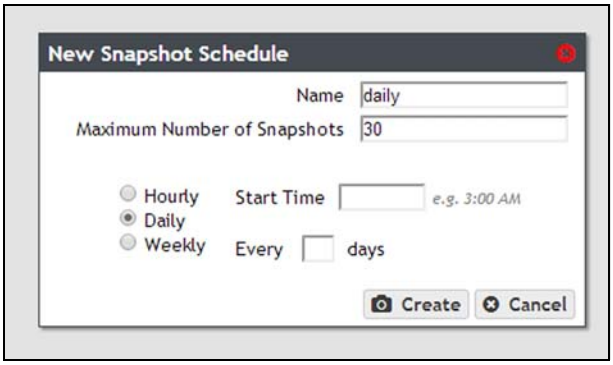


Figure 54 The New Snapshot Schedule dialog box showing the daily interval options.

3. Change the default name of the snapshot schedule, if desired.
4. Enter a number for the **Maximum Number of Snapshots**. When the maximum number is reached, the system deletes the oldest snapshot.
5. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
6. Enter a number for **Every _ days**. This value specifies the interval, in days, between generating snapshots. For example, if this value is set to 2, the system creates a snapshot every two days at the time specified in Step 5.
7. Click **Create**.

Create a Weekly Schedule

1. On the Volume details screen (see Figure 51 on page 85), select **Action ⋯⁘ New Snapshot Schedule**. The New Snapshot Schedule dialog box displays.

2. Select **Weekly** as the interval for the snapshot schedule. The dialog box changes to display options for the weekly interval setting.

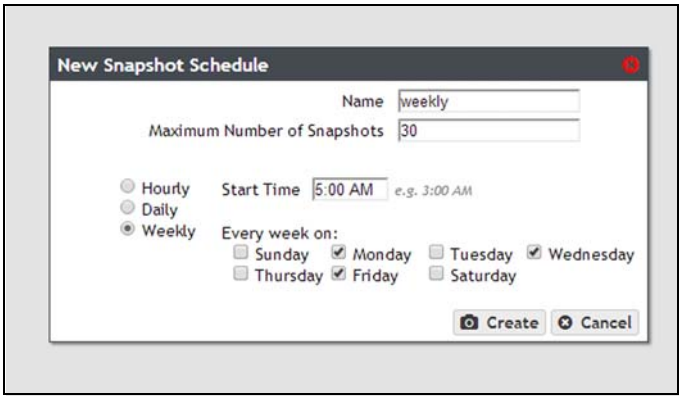


Figure 55 The New Snapshot Schedule dialog box showing the weekly interval options.

3. Change the default name of the snapshot schedule, if desired.
4. Enter a number for the **Maximum Number of Snapshots**. When the maximum number is reached, the system deletes the oldest snapshot.
5. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
6. Select one or more days for **Every week on:**. This determines the day(s) of each week the system generates snapshots. For example, based on the selections in Figure 55, the system creates a snapshot every Monday, Wednesday, and Friday at 5:00 AM.
7. Click **Create**.

Delete a Snapshot Schedule

If desired, you can delete a previously created snapshot schedule.

Note: Deleting a snapshot schedule does not delete the snapshots previously created by the snapshot schedule. To delete snapshots, see Delete a Snapshot on page 89.

Use the instructions in this section to delete a snapshot schedule.

1. From the menu bar, select **Configuration ⋯⁘ NAS ⋯⁘ Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 27 on page 60).
2. Double-click the volume for which you want to delete the snapshot schedule, or select the volume, and then select **Action ⋯⁘ Show Details**. The details screen for that volume displays.

3. Select the snapshot schedule you want to delete and select **Action** ⋯⁘ **Delete Snapshot Schedule**. A confirmation window displays.

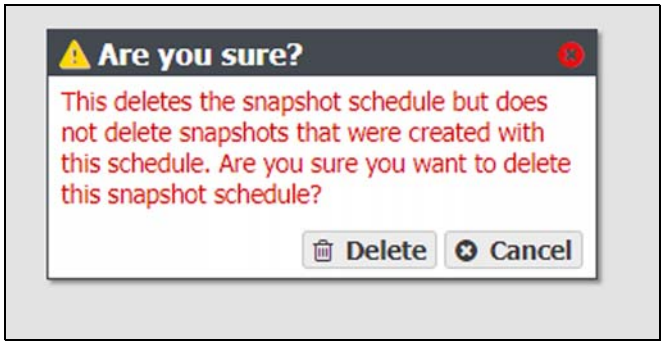


Figure 56 Confirm the snapshot schedule deletion.

4. Click **Delete**.

Delete a Snapshot

Use the following steps to delete a snapshot.

1. From the menu bar, select **Configuration** ⋯⁘ **NAS** ⋯⁘ **Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 20 on page 53).
2. Double-click the volume you for which you want to delete snapshot, or select the volume, and then select **Action** ⋯⁘ **Show Details**. The details screen for that volume displays.

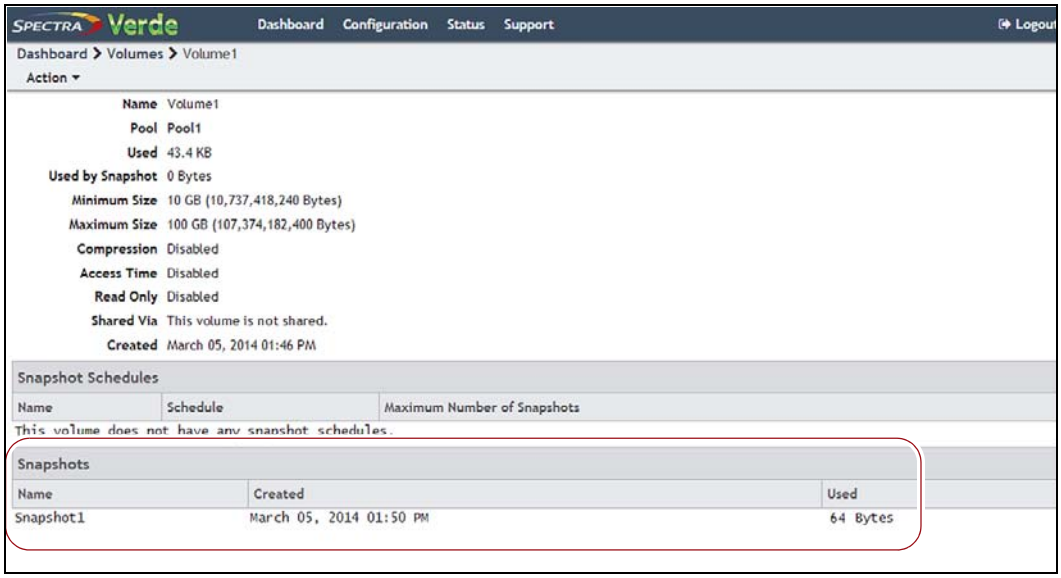


Figure 57 The Volume details screen showing a snapshot.

3. Select the snapshot you want to delete, and then select **Action ⋯⁘ Delete Snapshot**. A confirmation window displays.

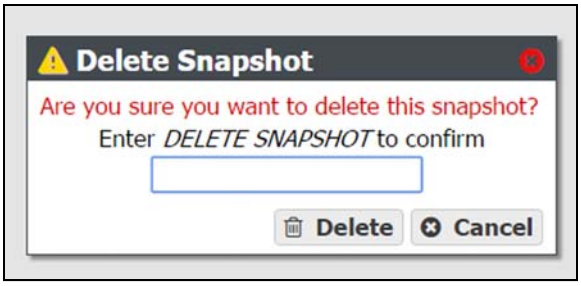


Figure 58 Confirm the snapshot deletion.

4. Type `DELETE SNAPSHOT` in the entry field and click **Delete** to delete the snapshot.

Restore to a Snapshot

Use the following instructions to restore a volume to its previous state using a previously generated snapshot.

Note: If you only want to restore a single file in the snapshot, see Retrieve a Single File from a Snapshot on page 91.

1. From the menu bar, select **Configuration ⋯⁘ NAS ⋯⁘ Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 20 on page 53).
2. Double-click the volume you want to restore using a previously generated snapshot, or select the volume, and then select **Action ⋯⁘ Show Details**. The details screen for that volume displays.

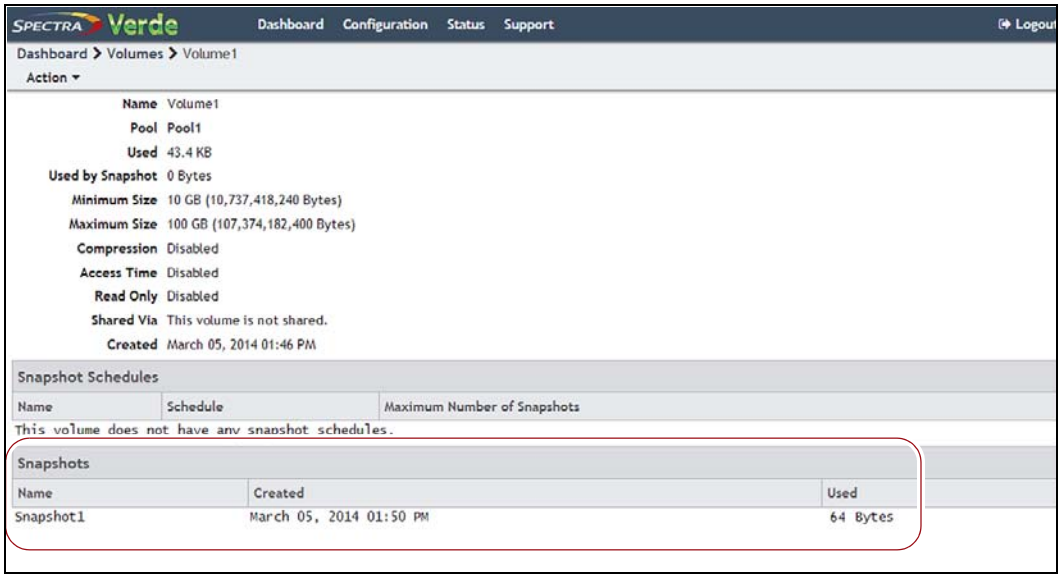


Figure 59 The Volume details screen.

3. In the snapshots list, select the snapshot you want to use to restore the volume and then select **Action ⋯ Rollback**.

Caution Rollback deletes all data changes made after the snapshot was created, and deletes any snapshots that were saved after the one you are using for the restore process. This action cannot be undone.

4. A dialog box displays, asking you to confirm the rollback. Select **Rollback** to restore the volume to its state when the snapshot was created.

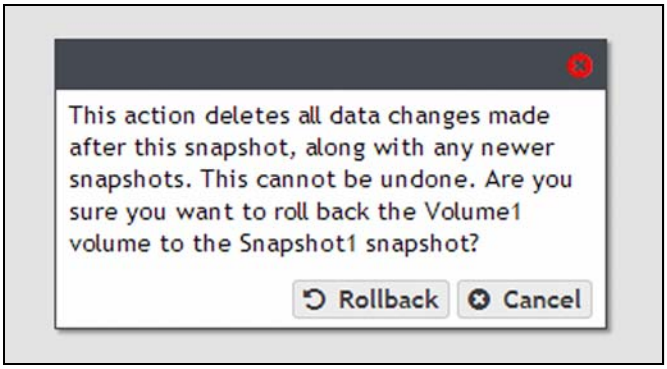


Figure 60 Confirm the volume snapshot rollback.

Retrieve a Single File from a Snapshot

If you only need to restore a single file, you do not need to restore an entire snapshot. Use the following instructions to retrieve a single file from a snapshot.

Note: Use Windows Explorer or Linux/Unix command line to complete this procedure.

Use the instructions in this section to retrieve a single file from a snapshot.

1. Using a remote host that has access to the shared volume for which you need to restore a single file, map the share containing the snapshot to the remote host (for example "Z:\")
2. You cannot browse to the snapshots directory using Windows explorer, you must enter the full path of the snapshot from which you want to retrieve a file in the Windows explorer address bar. Snapshots are organized as follows:

   Z:\zfs\snapshot*snapshot name*
3. The specified directory displays. All files contained in the snapshot display.
4. Locate the file you want to restore and copy it to the appropriate location.

MANAGING SHARES

After creating one or more shares, use the instructions in this section to edit or delete a share.

Edit a CIFS Share

After creating a CIFS share, you can edit it to change the configuration.

1. From the menu bar, select **Configuration ⋯⁘ Shares ⋯⁘ CIFS**. The CIFS Shares screen displays.
2. Select the share you want to edit, and then select **Action ⋯⁘ Edit**. The Edit CIFS Share screen displays.

Figure 61 The Edit CIFS Share dialog box.

3. Select or clear the **Read-only** check box. You cannot change the name once the CIFS share is created.
4. Click **Save**.

Edit an NFS Share

After creating an NFS share, you can edit it to change the configuration.

1. From the menu bar, select **Configuration ⋯⁘ Shares ⋯⁘ NFS**. The NFS Shares screen displays.

2. Select the share you want to edit, and then select **Action ⋯⁘ Edit**. The NFS Share Edit screen displays.

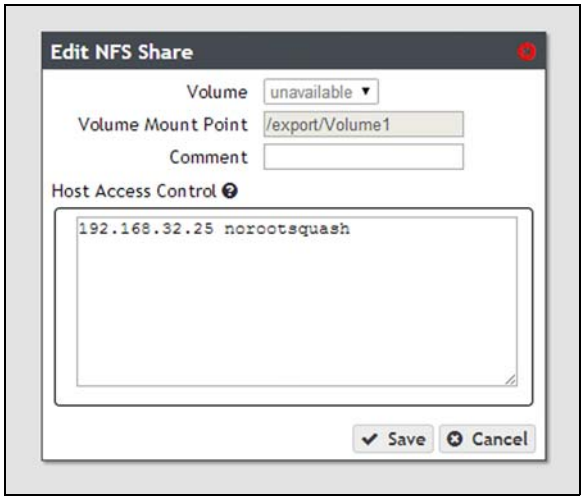


Figure 62 The Edit NFS Share dialog box.

3. Make the desired changes (see Create an NFS Share on page 67 for more information), and click **Save**.

Delete a Share

If you do not want to continue sharing a volume (that is, you do not want users accessing the Verde NAS solution over a network connection to access the volume), you can delete the share.

Use the following steps to delete the share.

1. If you need to delete a CIFS share, from the menu bar, select **Configuration ⋯⁘ Shares ⋯⁘ CIFS**. The CIFS Shares screen displays.

   —OR—

   If you need to delete an NFS share, from the menu bar, select **Configuration ⋯⁘ Shares ⋯⁘ NFS**. The NFS Shares screen displays.

2. Select the share you want to delete, and then select **Action ⋯⁘ Delete**.

3. A dialog box displays asking you to confirm the deletion. Click **Delete** to remove the share.

   Note: Clicking **Delete** does not delete the volume. It only removes the volume from the list of shares and makes it inaccessible to remote hosts. The volume is still present on the system and listed on the Volumes screen.

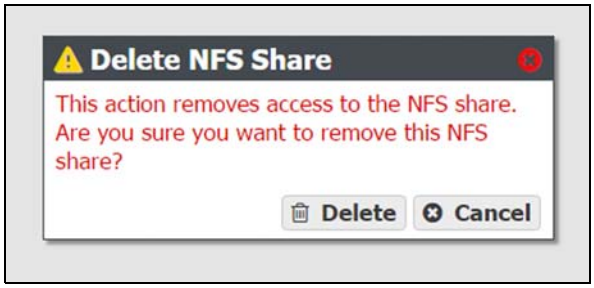


Figure 63 Confirm removing the share.

MANAGING NAS REPLICATION

After configuring replication, use the instructions in this section to manually start or cancel a volume replication, edit or delete the NAS replication configuration, and to restore replicated files.

Manually Start NAS Replication

If desired, you can initiate folder replication manually, regardless of the automatic replication schedule configured for the volume. Starting a manual NAS replication begins the replication immediately. Once complete, replication for the folder continues on its previously defined schedule.

Note: If the NAS solution is in the process of replicating data on a preconfigured schedule, the manual replication begins when the scheduled replication completes. To stop any replication in progress, see Cancel a NAS Replication In Progress below.

1. On the source system's Verde user interface, select **Configuration ···⁘ NAS ···⁘ Volumes**. The Volumes screen displays.
2. Double-click the volume name you want to replicate, or select the folder and select **Action ···⁘ Show Details**. The details screen for the volume displays.

3. Select **Action ···⁘ Replicate Now**. A confirmation window displays.

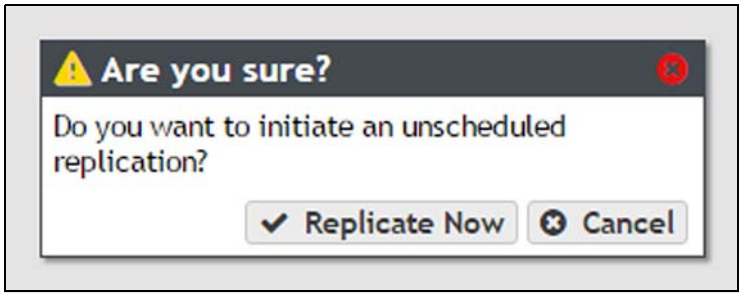


Figure 64 The Replicate Now confirmation window.

4. Click **Replicate Now** to begin manual replication.

Cancel a NAS Replication In Progress

If desired, you can cancel any NAS replications currently in progress. Canceling replication stops the replication and deletes any data the target received during the replication. Use the steps in this section to cancel a NAS replication.

1. On the **source system** user interface, select **Configuration ···⁘ NAS ···⁘ Volumes**. The Volumes screen displays.
2. Double-click the volume name for which you want to cancel replication, or select the folder and select **Action ···⁘ Show Details**. The details screen for the volume displays.
3. Select **Action ···⁘ Cancel Replication**. A confirmation window displays.

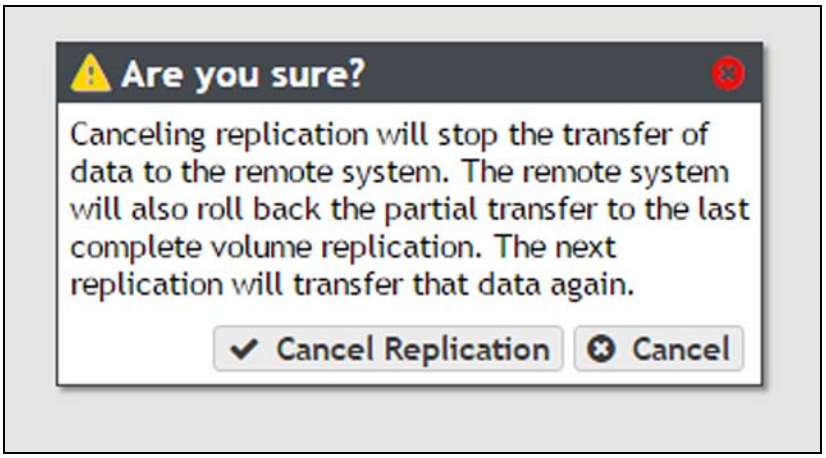


Figure 65 The Cancel Replication confirmation window.

4. Click **Cancel Replication** to stop the replication in progress. Any data that was transferred to the target system is deleted.

Restoring Files from a NAS Replication Target

If the source Verde NAS solution in a replication configuration fails, you can restore files from the replication target. Use the instructions in this section to restore files from a replication target.

1. Clear the write-protected status of the replicated volume.

   Note: You cannot share a write-protected volume.

   a. From the menu bar, select **Configuration ⋯⁘ NAS ⋯⁘ Volumes**. The Volumes screen displays.

   b. Select the replicated volume and select **Action ⋯⁘ Edit**. The Edit *volume name* dialog box displays.

   c. Clear the **Read Only** check box.

   d. Click **Save**.

2. Depending on your operating system environment, create either a CIFS or NFS share, selecting the replicated volume during the creation process. See Create a Share on page 63 for instructions.

3. If desired, write protect the replicated volume before you copy files from the volume.

   Note: Spectra Logic highly recommends that you write-protect the volume after sharing it.

   a. From the menu bar, select **Configuration ⋯⁘ NAS ⋯⁘ Volumes**. The Volumes screen displays.

   b. Select the replicated volume and select **Action ⋯⁘ Edit**. The Edit *volume name* dialog box displays.

   c. Select the **Read Only** check box.

   d. Click **Save**.

4. Using your host machine, connect to the new share on the replication target.

5. Copy the needed files from the replication target share to the source system.

6. If desired, delete the share once you have restored the needed files. See Delete a Share on page 111.

Disable a NAS Replication for a Volume

Use the instructions in this section to prevent any further replication from a volume currently configured to use NAS replication.

1. On the **source system** user interface, select **Configuration ⋯⁘ NAS ⋯⁘ Volumes**. The Volumes screen displays.

2. Double-click the volume name you want to stop replicating, or select the folder and select **Action ⋯⁘ Show Details**. The details screen for the volume displays.
3. Select **Action ⋯⁘ Configure Replication**. The Configure Replication dialog box displays.

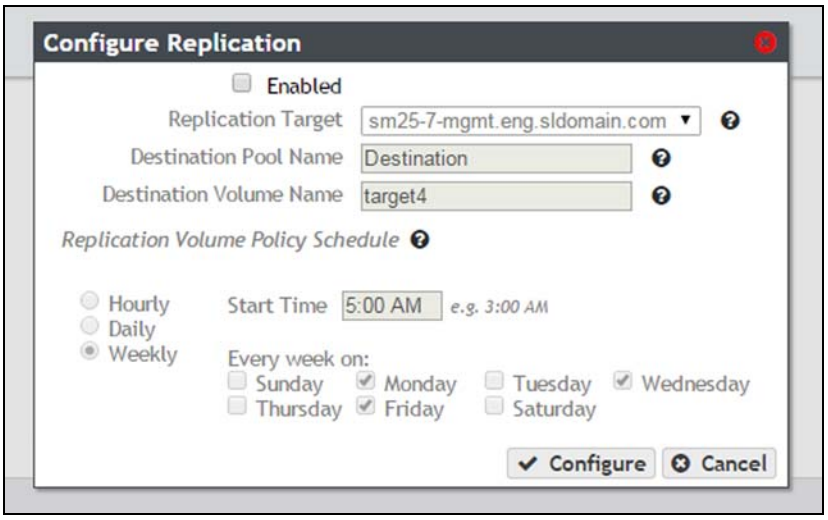


Figure 66 The Configure Replication dialog box.

4. Clear the **Enabled** check box. The other options on the dialog box grey out and become un-editable (see Figure 66).
5. Click **Configure**. The volume no longer replicates to the target.

Edit the NAS Replication Service

1. On the **source system's** Verde user interface, select **Configuration ⋯⁘ Services** to display the Services screen (see Figure 37 on page 68).
2. Double-click the Replication service, or select the service, and then select **Action ⋯⁘ Show Details**. The Replication service details screen displays.

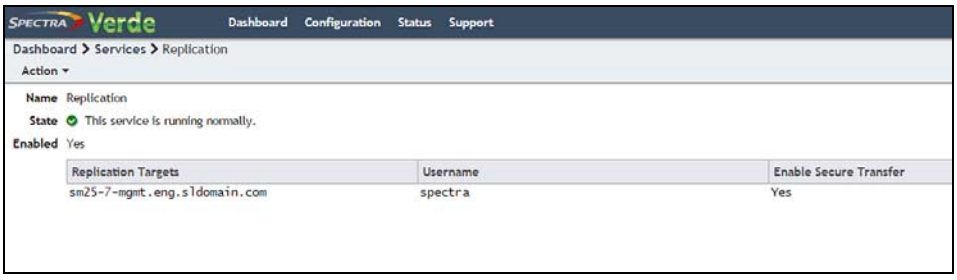


Figure 67 The Replication service details screen.

3. Select the replication target in the Replication service details screen, and select **Action ⋯⁘ Edit**. The Modify Replication Service dialog box displays.

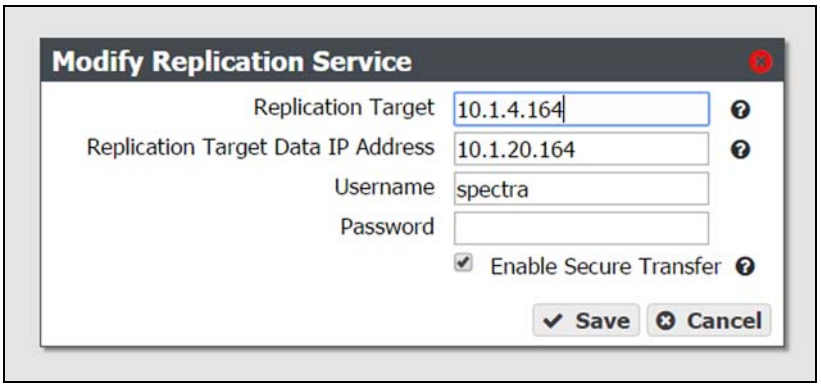


Figure 68 The Modify Replication Service dialog box.

4. If desired, modify the IP address or hostname of the management port of the target in the **Replication Target** field.

   Note: Do not use http:// or https:// to precede the IP address or hostname.

5. If desired, modify the IP address of the target's data port in the **Replication Target Data IP Address** field.

   Note: Do not use http:// or https:// to precede the IP address or hostname.

6. If desired, modify the username of a user configured on the target in the **Username** field.

   Note: Because you cannot create additional users at this time, you must use the **spectra** user account when configuring replication.

7. Enter the user password in the **Password** field, if one is set. Otherwise, leave the field blank.

8. If desired, select the **Enable Secure Transfer** check box to configure the **source system** to encrypt the replicated data before transferring it to the **target system**, or clear the check box to transfer data without encryption. Data is encrypted using Secure Socket Layer (SSL).

9. Click **Save**.

Delete the NAS Replication Service Configuration

1. On the **source system** select **Configuration ⋯⁘ Services** to display the Services screen (see Figure 37 on page 68).

2. Double-click the Replication service, or select the service, and then select **Action ⋯⁘ Show Details**. The Replication service details screen displays.

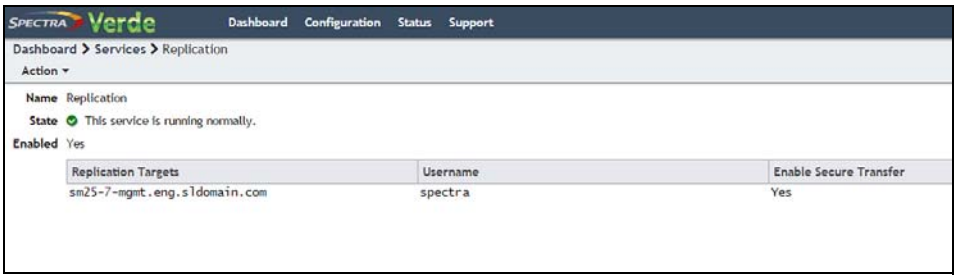


Figure 69 The Replication service details screen.

3. Select the replication target in the Replication service details screen, and select **Action ⋯⁘ Delete**. The Delete Replication Target dialog box displays.
4. Click **Delete** to remove the replication target. The source system no longer replicates data to the target system.
5. Repeat Step 3 and Step 4 to delete additional replication targets, if desired.

CHAPTER 5

Configuring a Verde NAS Solution

This chapter describes using the Verde user interface to configure the Verde NAS solution for operation in your environment.

Task	
Configure Network Connections and Settings	page 101
Configure Ethernet Ports	page 101
Configure DNS Settings	page 107
Configure SMTP Settings	page 108
Configure Date and Time	page 109
Edit the System Name	page 110
Configure Networking Services	page 111
Configure the Active Directory Service	page 112
Configure the SNMP Service	page 117
Configure Users	page 125
Description of User Types	page 125
Create a User	page 125
Edit a User	page 125
Delete a User	page 126
Configure Certificates	page 126
Manually Enter Activation Keys	page 127

CONFIGURE NETWORK CONNECTIONS AND SETTINGS

Use the Network screen to configure Ethernet ports and DNS settings, and to enter SMTP and NTP information.

Note: the *Spectra BlackPearl & Verde HotPair Installation & Configuration Guide* for instructions on configuring network connections.

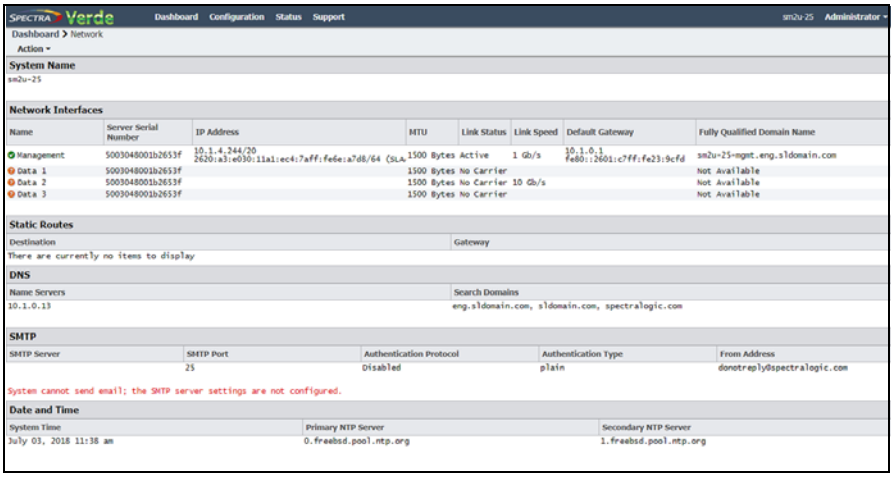


Figure 70 The Network screen.

Configure Ethernet Ports

This section describes using the Verde user interface to configure the IP addressing for the Ethernet ports in the Verde master node. The Verde NAS solution includes two 10GBase-T ports and two 10 GigE ports on the rear panel (see Figure 5 on page 25). Optionally, a two-port 40 GigE card can be installed.

Notes:

- You can create one or more data connections to the system.
- You can configure link aggregation for better performance.
- While different types of Ethernet network interface cards can be installed in the same Verde NAS solution, only one type port can be used in each link aggregation configuration.
- You can only use the Verde management port to access the Verde user interface. You cannot use this port for data transfer.
- The data connection(s) and Verde management port are initially configured in Chapter 2 – Initial Configuration on page 38. Use the instructions in this section to configure network settings after initial setup is complete.

The next steps depend on if you are configuring the data connection, the management port, or want to delete (clear) a network configuration.

- Configure the Data Connection on page 46
- Configure the Management Port below
- Edit a Data Connection on page 105
- Edit a Static Route on page 106
- Clear a Data Port Configuration on page 107

Configure the Management Port

1. From the menu bar, select **Configuration ⋯⁘ Network**, or click the Network pane on the Dashboard screen. The Network screen displays (see Figure 70 on page 101).
2. In the Network Interfaces pane, double-click the Management row, or select the Management row and then select **Action ⋯⁘ Edit** from the menu bar. The Edit Management dialog box displays.

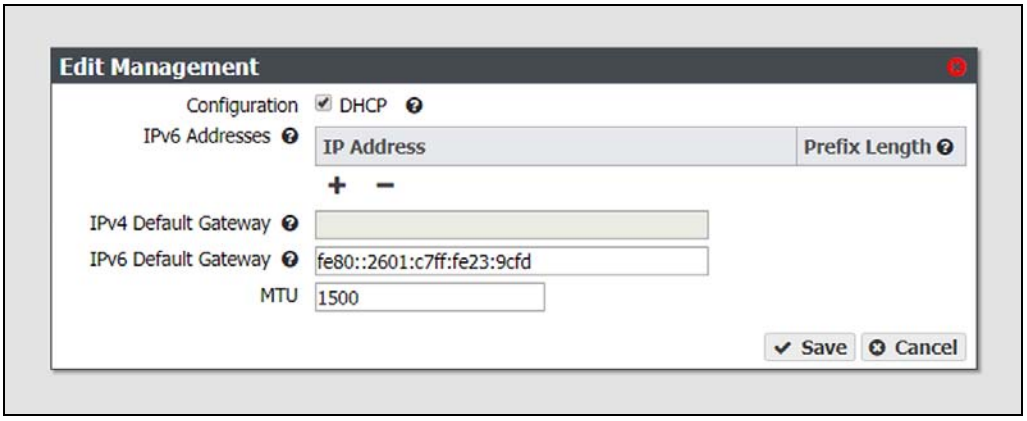


Figure 71 The Edit Management dialog box.

3. Select **DHCP** to configure the system to automatically acquire an IPv4 address using DHCP. Otherwise skip to Step 4 on page 103.

   Note: The DHCP setting does not apply to IPv6.

Important If you select DHCP, you are not able to see the IP address assigned by DHCP before you are logged out of the Verde user interface. Contact your system administrator to determine the DHCP address for the management port.

4. To configure a static IP address, click the **+** button and enter the following information:
   - **IP Address** — Enter a valid IPv4 or IPv6 address.

     Note: You cannot enter an IPv4 address if you selected DHCP in Step 3 on page 102.
   - **Prefix Length** — Enter the subnet mask.

     Note: If desired, you can enter **Aliases**, multiple IP and prefix lengths assigned to the data port. Use the **+** button to configure additional IP and Netmask addresses. You can configure a maximum of 16 aliases.
5. If applicable, enter the **IPv4 Default Gateway**.

   Notes:
   - If you selected DHCP in Step 3 on page 102, this option is unavailable.
   - The gateway entered for the last configured IPv4 connection sets the default gateway for the Verde NAS solution.
6. If applicable, enter the **IPv6 Default Gateway**.

   Notes:
   - The gateway entered for the last configured IPv6 connection sets the default gateway for the Verde NAS solution.
   - The IPv6 Gateway does not need to be configured when the Verde NAS solution is connected to a SLACC network.
7. Change the **MTU** value, if desired. If you set the MTU value to something other than 1500, ensure that your switch configuration supports larger MTU settings, as well as all the hosts on the network.
8. Click **Save**.

   Note: When you change the IP address of the Verde management port, you lose your connection to the user interface when you save your changes. To re-establish the connection, enter the new IP address in your browser and log in again.

Edit an Aggregate Data Connection

If desired, you can edit an aggregate data connection after it is created.

Important The network switch connected to the Verde NAS solution must be configured for Level 3 LACP in order to support an aggregate data connection on the Verde NAS solution.

1. From the menu bar, select **Configuration** ···⁘ **Network**, or click the Network pane from the Dashboard screen. The Network screen displays (see Figure 70 on page 101).

2. Select the row of the data connection you want to edit and select **Action ⋯ Edit**. The Edit Aggregate *Data Connection* dialog box displays.

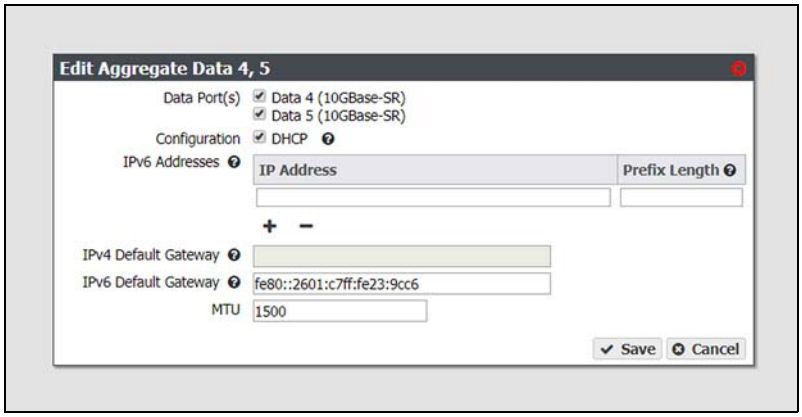


Figure 72 The Edit Aggregate *Data* #,# dialog box.

3. Select or clear the **Data Port(s)** you want to configure into an aggregate data interface. Only one type of port can be used in an aggregation. For example, you cannot use both 10 GigE and 40 GigE ports in the same link aggregation.
4. Select **DHCP** to configure the system to automatically acquire an IPv4 address using DHCP. This setting does not apply to IPv6.
5. To configure a static address, click the **+** button and enter the following information:
   - **IP Address** — Enter a valid IPv4 or IPv6 address.

     Note: You cannot enter an IPv4 address if you selected DHCP in Step 4.
   - **Prefix Length** — Enter the subnet mask.

     Note: If desired, you can enter **Aliases**, multiple IP and prefix lengths assigned to the data port. Use the **+** button to configure additional IP and Netmask addresses. You can configure a maximum of 16 aliases.

   To remove an existing static address, click the **-** button.
6. If applicable, enter the **IPv4 Default Gateway**.

   Notes:
   - If you selected DHCP in Step 4, this option is unavailable.
   - The gateway entered for the last configured IPv4 connection sets the default gateway for the Verde.
7. If applicable, enter the **IPv6 Default Gateway**.

   Notes:
   - The gateway entered for the last configured IPv6 connection sets the default gateway for the Verde NAS solution.
   - The IPv6 Gateway does not need to be configured when the Verde NAS solution is connected to a SLACC network.

8. Change the **MTU** (Maximum Transmission Unit) value, if desired. If you set the MTU value to something other than 1500, ensure that your switch configuration supports larger MTU settings, as well as all the hosts on the network.
9. Click **Save**.

Edit a Data Connection

If desired, you can edit a data connection after it is created.

1. From the menu bar, select **Configuration ⋯⁘ Network**, or click the Network pane from the Dashboard screen. The Network screen displays (see Figure 70 on page 101).
2. Select the row of the data connection you want to edit and select **Action ⋯⁘ Edit**. The Edit *Data Connection* dialog box displays.

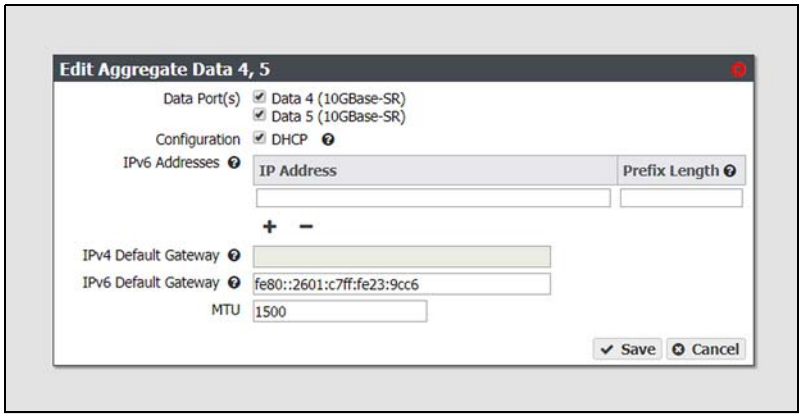


Figure 73 The Edit *Data Connection* dialog box.

3. Select **DHCP** to configure the system to automatically acquire an IPv4 address using DHCP. This setting does not apply to IPv6.
4. To configure a static IP address, click the **+** button and enter the following information:
   - **IP Address** — Enter a valid IPv4 or IPv6 address.

     Note: You cannot enter an IPv4 address if you selected DHCP in Step 3.
   - **Prefix Length** — Enter the subnet mask.

     Note: If desired, you can enter **Aliases**, multiple IP and prefix lengths assigned to the data port. Use the **+** button to configure additional IP and Netmask addresses. You can configure a maximum of 16 aliases.

   To remove an existing static address, click the **-** button.

5. If applicable, enter the **IPv4 Default Gateway**.

   Notes:
   - If you selected DHCP in Step 3, this option is unavailable.
   - The gateway entered for the last configured IPv4 connection sets the default gateway for the Verde NAS solution.

6. If applicable, enter the **IPv6 Default Gateway**.

   Notes:
   - The gateway entered for the last configured IPv6 connection sets the default gateway for the Verde NAS solution.
   - The IPv6 Gateway does not need to be configured when the Verde NAS solution is connected to a SLACC network.

7. Change the **MTU** (Maximum Transmission Unit) value, if desired. If you set the MTU value to something other than 1500, ensure that your switch configuration supports larger MTU settings, as well as all the hosts on the network.

8. Click **Save**.

Edit a Static Route

Use the instructions in this section to edit a static route.

1. From the menu bar, select **Configuration ⋯ Network**, or select the Network pane from the Dashboard screen. The Network screen displays (see Figure 70 on page 101).

2. Double-click the static route you want to edit. The Static Route dialog box displays.

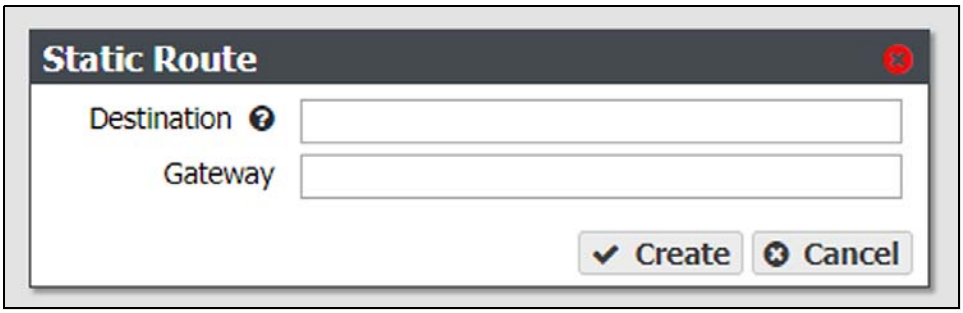


Figure 74 The Static Route dialog box.

3. If desired, in the **Destination** field, edit the network address that you want to access through the data connection.

4. If desired, edit the **Gateway** of the data connection used to communicate with the isolated network.

5. Click **Create**.

Clear a Data Port Configuration

In some cases, it may be useful to delete an existing data port configuration by clearing it. Use the instruction in this section to clear a data port configuration.

> **Note:** The management port cannot be cleared. See Configure the Management Port on page 102 to change the management port settings.

1. From the menu bar, select **Configuration ⋯⁘ Network**, or click the Network pane on the Dashboard screen. The Network screen displays (see Figure 70 on page 101).
2. Select the row of the configuration you want to clear and then select **Action ⋯⁘ Clear** from the menu bar. A confirmation window displays.
3. Click **Delete** to clear the Ethernet configuration.

Configure DNS Settings

The DNS settings on the Verde NAS solution are used to allow domain name lookup on the system. Use the following instructions to enter DNS information on the system.

1. From the menu bar, select **Configuration ⋯⁘ Network**, or click the Network pane on the Dashboard screen. The Network screen displays (see Figure 70 on page 101).
2. In the DNS pane of the Network screen, double-click the single row, or select the DNS row and then select **Action ⋯⁘ Edit**. The Edit DNS dialog box displays.

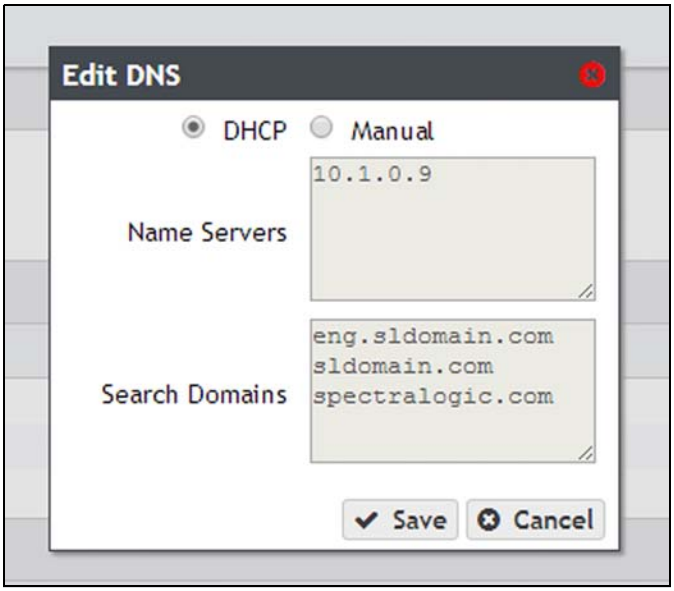


Figure 75 Edit DNS information.

3. Select **DHCP** to have the system determine the address of name servers and search domains automatically.

   —OR—

   Select **Manual** to enter information for name servers and search domains manually.

   Note: The buttons for **DHCP** and **Manual** are only usable when the Verde management interface is configured as DHCP. If the management interface is set to a static IP address, the buttons are greyed out and the information must be entered manually.

4. If you selected **Manual**, enter the following information:

   a. Enter the IP address of one or more name servers in the **Name Servers** field.

   b. Enter the URL of one or more search domains in the **Search Domains** field.

5. Click **Save**.

Configure SMTP Settings

Use the SMTP settings to associate the Verde master node with a mail server. The system uses this SMTP server to send emails whenever ASLs or certain types of messages are generated. Use the following instructions to enter SMTP information on the system.

1. From the menu bar, select **Configuration** ⋯⁘ **Network**, or select the Network pane on the Dashboard screen. The Network screen displays.

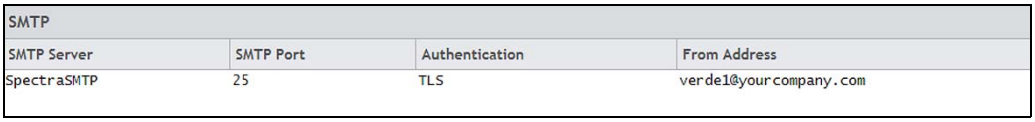


Figure 76 The SMTP pane of the Network screen.

2. Double-click the name of the SMTP server, or select the name of the SMTP server and then select **Action ⋯⁘ Edit**. The Email dialog box displays.

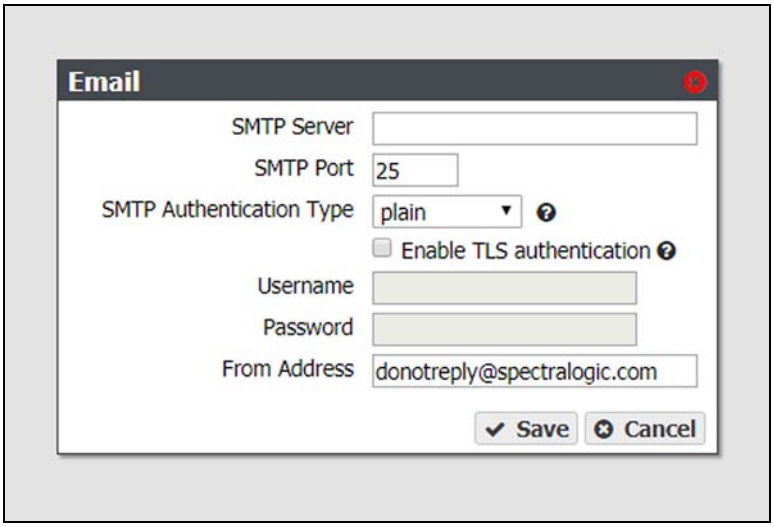


Figure 77 The Email dialog box.

3. Enter the **SMTP Server** and **SMTP Port** information.
4. Using the drop-down menu, select the **SMTP Authentication Type** required by your mail server.
5. If your SMTP server uses TLS (Transport Layer Security) authentication, select the **Enable TLS Authentication** check box and enter the required **Username** and **Password** information.
6. Enter an email address in the **From Address** field. This is the email address that displays as the sender whenever the system generates an email. This email address should uniquely identify the Verde master node to assist in troubleshooting and be recognized by the SMTP server as a valid domain address.
7. Click **Save**.

Configure Date and Time

The date and time can be set manually or using NTP (Network Time Protocol). The NTP settings are used to automatically control the current time on the Verde master node.

Note: If you plan to join an Active Directory domain, you must configure the Verde NAS solution to use NTP. If the system time and the Active Directory time are more than 5 minutes apart, joining the domain fails.

Use the following instructions to configure the date and time on the system.

1. From the menu bar, select **Configuration** ···⁘ **Network**, or select the Network pane on the Dashboard screen. The Network screen displays.

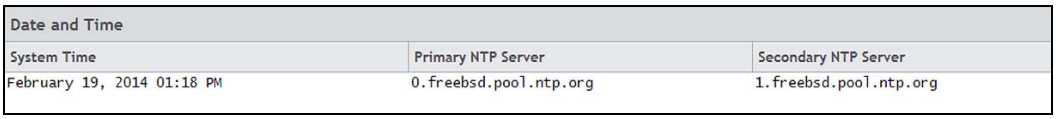


Figure 78 The Date and Time pane of the Network screen.

2. Double-click the System Time row to edit the date and time, or select the System Time row and then select **Action** ···⁘ **Edit**. The Time Settings dialog box displays.

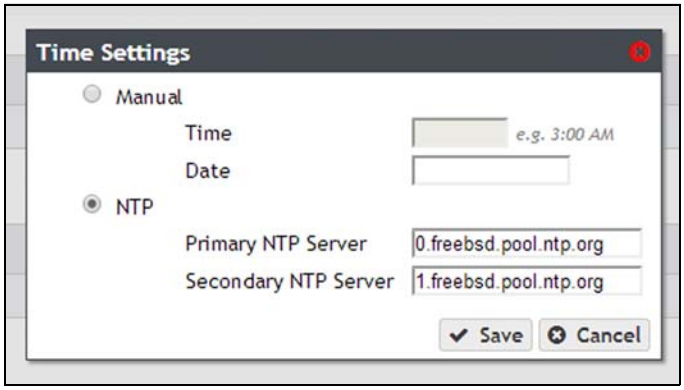


Figure 79 The Time Settings dialog box.

3. Select **Manual** or **NTP**.
   a. If you select Manual, enter the current time in the **Time** field. Enter either 12-hour time values and include AM or PM, or use 24-hour time values. Click the **Date** field. A calendar appears. Select the current date.
   b. If you select NTP, enter the NTP server information for the **Primary NTP Server**. If desired, enter the NTP server information for the **Secondary NTP Server**.
4. Click **Save**.

Edit the System Name

1. From the menu bar, select **Configuration** ···⁘ **Network**, or click the Network pane on the Dashboard screen. The Network screen displays.

2. In the Network Interfaces pane, double-click the system name, or select the system name and then select **Action ⋯⁘ Edit**. The Edit System Name dialog box displays.

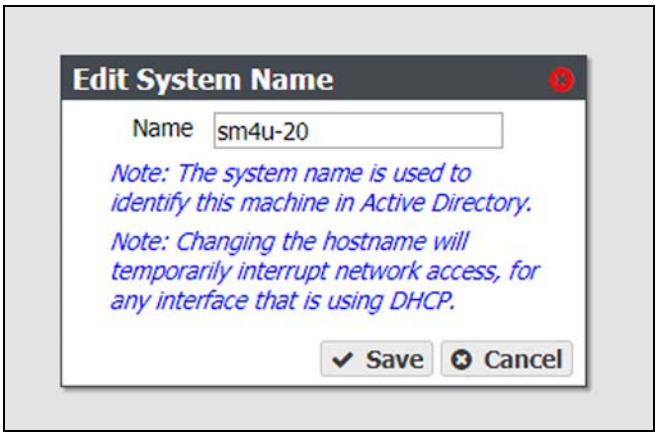


Figure 80 The Edit System Name dialog box.

3. Enter the desired **Name** for the system. The system only allows letters, numbers, the period character (.), and the hyphen character (-) in the system name.

Notes:
- The first section of the system name, up to a delimiter cannot be longer than 15 characters:
  - **Valid** - Verde.domain.com
  - **Invalid** - VerdeSystem.domain.com
- If your system is using firmware BlackPearl 3.2.2, or earlier, there are no character restrictions on system names. However, Spectra Logic recommends limiting system names to letters, numbers, and hyphens to maintain compatibility with the RFC 1123 standard.
- The system does not change previously configured system names using special characters when upgrading to BlackPearl 3.3, or later.

4. Click **Save**.

CONFIGURE NETWORKING SERVICES

Use the following instructions to configure networking services on the Verde NAS solution.

For instructions on configuring NAS services, see Configure Network Connections and Settings on page 101.

Configure the Active Directory Service

The Active Directory service in the Verde user interface is used to connect the system to a Windows Active Directory domain. Before you can join a domain, you must configure the Verde NAS solution to use NTP. See Configure Date and Time on page 109.

Note: If the Verde NAS solution time and the Active Directory domain time are more than 5 minutes apart, joining the domain fails.

Use the instructions in this section to join or leave an Active Directory domain.

Join Domain

1. From the menu bar, select **Configuration ···⁘ Services**. The Services screen displays.

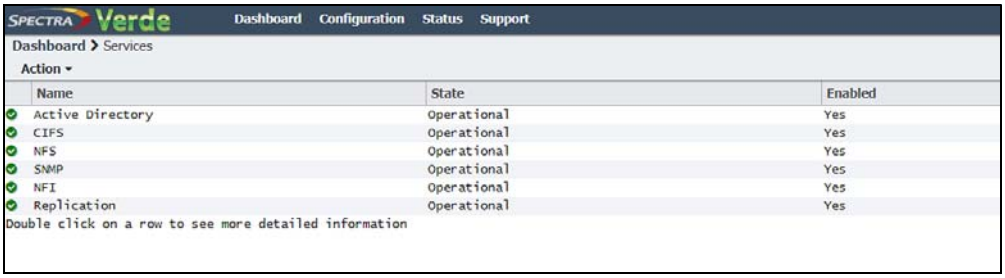


Figure 81 The Services screen.

2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action ···⁘ Show Details**. The Active Directory details screen displays.
3. On the Active Directory service details screen, select **Action ···⁘ Join Domain**. The Join Domain dialog box displays.

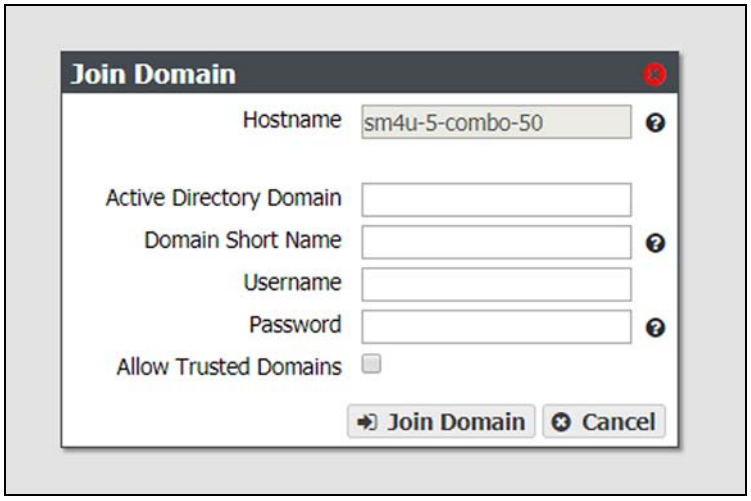


Figure 82 The Join Domain dialog box.

4. The **Hostname** identifies the Verde NAS solution in the Active Directory domain.

   Note: The hostname is greyed out and cannot be changed in the Join Domain dialog box. Use the Network screen to change the hostname if desired (see Edit the System Name on page 110).

5. Enter the name of the **Active Directory Domain** you want to join.
6. Optionally, enter the **Domain Short Name** if your domain uses a non-standard workgroup name.
7. Enter the **Username** and **Password** for a user authorized to join the specified domain.

   Notes:
   - The Verde NAS solution uses "Pre-Windows 2000"login names for Active Directory users. Login names greater than 20 characters in length, or containing special characters (for example '@') are not able to log into the Verde user interface.
   - You must enter the user name and password each time the Verde NAS solution joins an Active Directory domain. The system does not save this information.

8. If desired, select **Allow Trusted Domains** if the Active Directory domain you want to join is a trusted domain.
9. Click **Join Domain**.

Edit Domain

If desired, you can edit your Active Directory configuration to enable or disable support for trusted domains.

1. From the menu bar, select **Configuration ···⁘ Services**. The Services screen displays (see Figure 81 on page 112).
2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action ···⁘ Show Details**. The Active Directory service details screen displays.

3. Select **Action ⋯⁘ Edit**. The Edit AD Service dialog box displays.

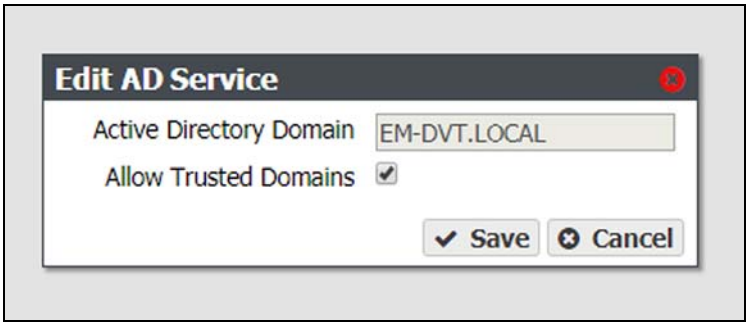


Figure 83 The Edit AD Service dialog box.

Note: The **Active Directory Domain** name is unavailable and cannot be changed.

4. Select or clear **Allow Trusted Domains**.
5. Click **Save**.

Add Advanced Parameter

Advanced Parameters are used to adjust or set global or share specific Samba parameters. These parameters are mirrored on both the Active Directory and CIFS Service pages.

Caution Improperly configuring advanced parameters can expose security vulnerabilities and other serious issues. Advanced parameters should not be configured without a full understanding of the consequences.

1. From the menu bar, select **Configuration ⋯⁘ Services**. The Services screen displays (see Figure 81 on page 112).
2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action ⋯⁘ Show Details**. The Active Directory service details screen displays.

3. Select **Action ···⁘ Add Advanced Parameter**. The Add Advanced Parameter dialog box displays.

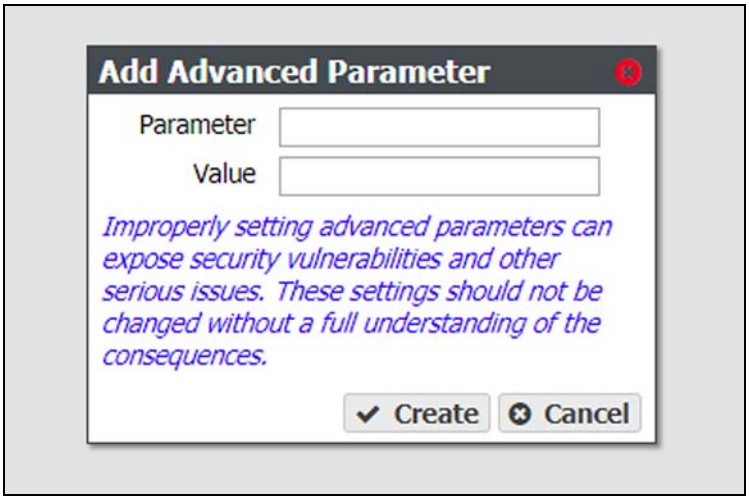


Figure 84 The Add Advanced Parameter dialog box.

4. Enter the desired **Parameter** and **Value**.
5. Click **Create**.

Edit Advanced Parameter

Caution

Improperly configuring advanced parameters can expose security vulnerabilities and other serious issues. Advanced parameters should not be configured without a full understanding of the consequences.

1. From the menu bar, select **Configuration ···⁘ Services**. The Services screen displays (see Figure 81 on page 112).
2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action ···⁘ Show Details**. The Active Directory service details screen displays.

3. Select the advanced parameter which you want to edit, then select **Action ⋯⁘ Edit Advanced Parameter**. The Edit Advanced Parameter dialog box displays.

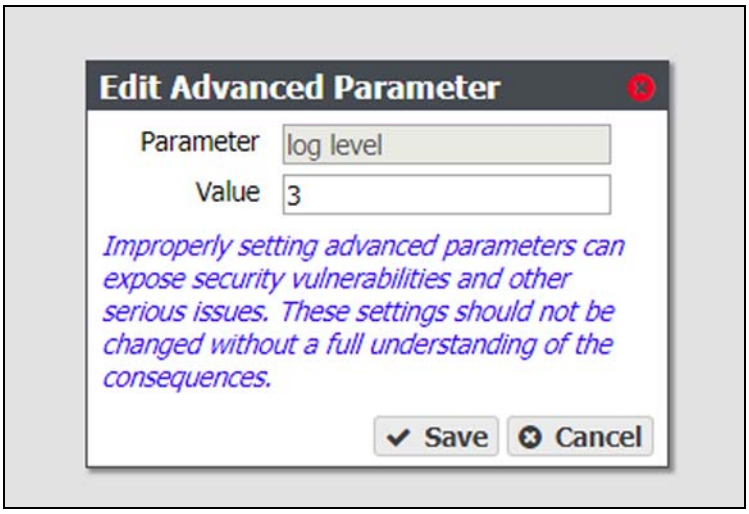


Figure 85 The Edit Advanced Parameter dialog box.

4. The **Parameter** field is greyed-out and cannot be changed.
5. Enter the desired **Value**.
6. Click **Save**.

Delete Advanced Parameter

1. From the menu bar, select **Configuration ⋯⁘ Services**. The Services screen displays (see Figure 81 on page 112).
2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action ⋯⁘ Show Details**. The Active Directory service details screen displays.
3. Select the advanced parameter which you want to delete, then select **Action ⋯⁘ Delete Advanced Parameter**. The Edit Advanced Parameter confirmation window displays.
4. Click **Delete**.

Leave Domain

1. From the menu bar, select **Configuration ···⁘ Services**. The Services screen displays.
2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action ···⁘ Show Details**. The Active Directory details screen displays.
3. Select **Action ···⁘ Leave Domain**. A confirmation window displays.
4. Click **Leave Domain**.

Configure the SNMP Service

The Verde user interface lets you configure the community and client list of the SNMP service to remotely monitor the Verde NAS solution using a network node manager program. Use the following steps to edit the SNMP service.

1. Select **Configuration ···⁘ Services** to display the Services screen (see Figure 81 on page 112).
2. Double-click the SNMP service, or select the service, and then select **Action ···⁘ Show Details**. The SNMP service details screen displays.
3. On the SNMP service details screen, select **Action ···⁘ Edit**. The Edit SNMP Service dialog box displays.

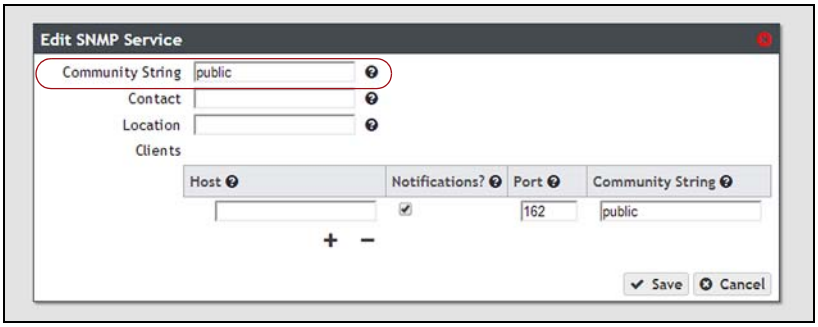


Figure 86 The Edit SNMP Service dialog box.

4. If desired, change the value of the **Community String**. Any incoming SNMP queries that use a different community string than the one set here fail. If no community string is specified, then the Verde master node responds to all SNMP queries.
5. Enter the primary contact for the Verde NAS solution in the **Contact** field.
6. Enter the physical location of the system in the **Location** field.

7. If desired, add clients that are allowed to access the system using SNMP.

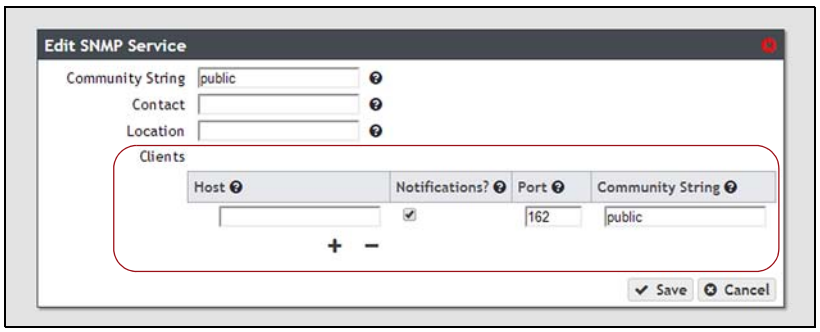


Figure 87 The Edit SNMP Service dialog box.

   a. Click the **+** sign to add additional clients.
   b. Enter the host IP address in the **Host** field.
   c. If desired, select the **Notifications** check box to indicate that the SNMP client should receive outgoing communications.
   d. Enter the port number to be used for SNMP communication in the **Port** field.
   e. Enter a community string value in the **Community String** field. This community string is set for each client. The clients monitor SNMP notifications for any that use the string specified here.
   f. Repeat Step a through Step e as needed to add additional clients.

8. Click **Save**.

Download the MIB File

If you want to communicate with the system using SNMP, you must first download the Verde NAS solution MIB (Management Information Base) file, and load the file into compatible network node manager programs, such as HP® OpenView® network node manager.

1. Select **Configuration ···⁘ Services** to display the Services screen (see Figure 81 on page 112).
2. Double-click the SNMP service, or select the service, and then select **Action ···⁘ Show Details**. The SNMP service details screen displays.

3. Click **Download MIB**. Using your web browser, save the file to your local host.

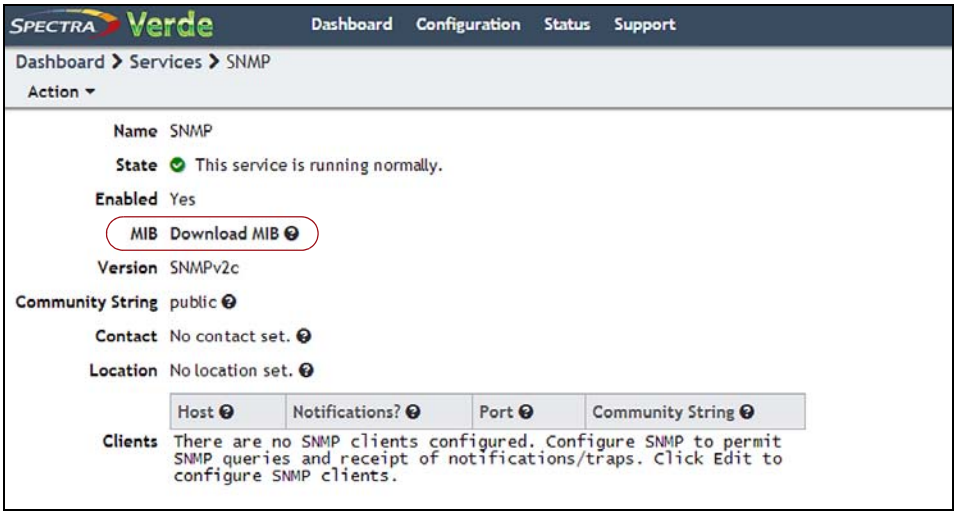


Figure 88 Download the MIB file.

4. Load the file into the network node manager program.
5. You can now use your network node manager program to communicate with the Verde master node, using the settings configured in Configure Network Connections and Settings on page 101.

CONFIGURE AND USE ENCRYPTION

If your Verde NAS solution includes Self Encrypting Drives (SEDs), use the encryption service to set the level of encryption, configure passwords, and unlock the drives so that they are usable for data transfer.

Configure the Encryption Service

Use the encryption service to set the level of encryption and create a password to unlock the drives following a system power cycle. You can select to store the password on the system, so that the drives are unlocked automatically, or to save the password to a USB key that is used when needed to unlock the drives, and is otherwise stored in a safe location.

1. From the menu bar, select **Configuration ···⁘ Services** to display the Services screen.

2. Double-click the Encryption service, or select the service, and then select **Action ···⁘ Show Details**. The details screen for the Encryption service displays.

Figure 89 The Encryption service details screen.

3. Select **Action ···⁘ Edit Service**. The Edit Encryption Service dialog box displays.

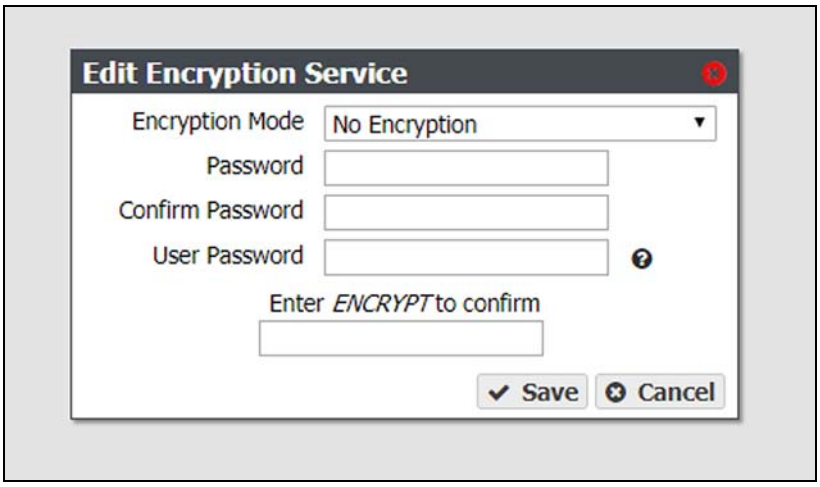


Figure 90 The Edit Encryption Service dialog box.

4. Use the **Encryption Mode** drop-down menu to set the encryption mode.

Parameter	Description
No Encryption	This setting is included in the drop-down menu as the default so that you do not accidentally select an undesired mode of encryption. If selected, the self-encrypting drives do not use encryption. Data stored on the drives is not encrypted. **Note:** This setting does not disable encryption on the drives once they are encrypted. Encryption **cannot** be disabled for encrypted drives.
Encrypt and Store Password	The self-encrypting drives encrypt data transferred to them, and the password to unlock the drives is stored on the system. The drives are automatically unlocked when the Verde NAS solution initializes.
Encrypt and Don't Store Password	The self-encrypting drives encrypt data transferred to them, but the system does not store the password to unlock the drives. You must manually enter the password each time the Verde NAS solution initializes. This setting also allows you to create a USB device with the encryption password. You can use the USB device when the system initializes to unlock the drives. Store the USB device in a safe location, not attached to the Verde NAS solution, at all other times.

5. Enter a **Password** to unlock the self-encrypting drives, and then **Confirm** the password.
6. Enter the **User Password** of the user currently logged in to the Verde user interface.
7. Enter ENCRYPT into the confirmation dialog box.
8. Click **Save**.

   Note: You may need to navigate away from the encryption details screen and then back for the system to update the information on the details screen.

Change the Encryption Password

If desired, you can change the password used to unlock the self-encrypting drives.

1. From the menu bar, select **Configuration ⋯⁘ Services** to display the Services screen.
2. Double-click the Encryption service, or select the service, and then select **Action ⋯⁘ Show Details**. The details screen for the Encryption service displays.
3. Select **Action ⋯⁘ Change Password**. The Change Password dialog box displays.

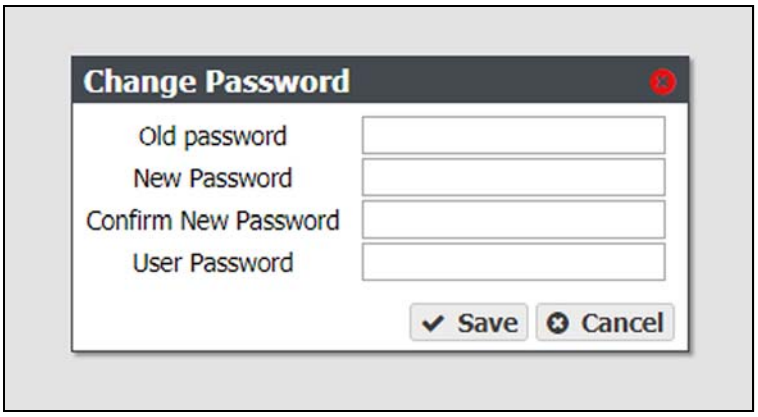


Figure 91 The Change Password dialog box.

4. Enter the (current) **Old Password**.
5. Enter the desired **New Password**, and then **Confirm** the new password.
6. Enter the **User Password** of the user currently logged in to the Verde user interface.
7. Click **Save**.

Unlock the Self-Encrypting Drives

If the encryption service is configured to not store the password on the NAS solution, use the instructions below to manually unlock the self-encrypting drives after the system initializes.

1. From the menu bar, select **Configuration ⋯⁘ Services** to display the Services screen.
2. Double-click the Encryption service, or select the service, and then select **Action ⋯⁘ Show Details**. The details screen for the Encryption service displays.
3. Select **Action ⋯⁘ Unlock Drives**. The Enter Password dialog box displays.

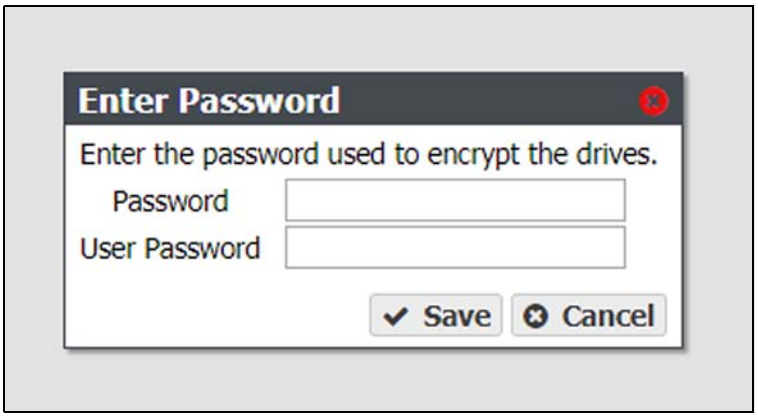


Figure 92 The Enter Password dialog box.

4. Enter the encryption **Password**.
5. Enter the **User Password** of the user currently logged in to the Verde user interface.
6. Click **Save**.

Create an Encryption Password USB Key

If the encryption service is configured to not store the password on the system, use the instructions below to create a USB key to store the encryption password that unlocks the self-encrypting drives after the system initializes. Insert the USB key when the system initializes to unlock the drives, and remove it from the system USB port and store it in a safe location at all other times.

1. From the menu bar, select **Configuration ⋯⁘ Services** to display the Services screen.
2. Double-click the Encryption service, or select the service, and then select **Action ⋯⁘ Show Details**. The details screen for the Encryption service displays.

3. Select **Action ···⁘ Create USB Key**. The Create USB Key confirmation window displays.

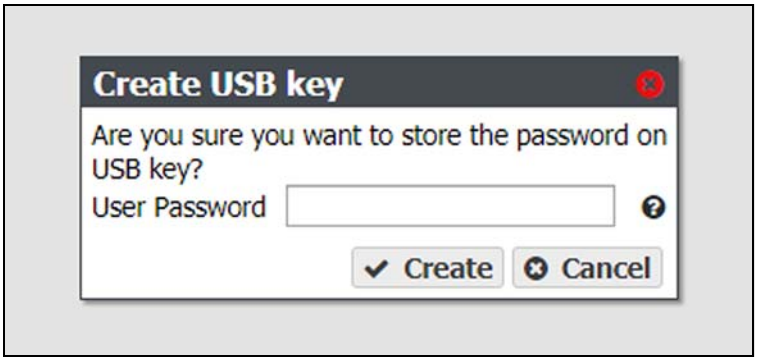


Figure 93 The Create USB Key confirmation window.

4. Enter the **User Password** of the user currently logged into the Verde user interface.
5. Click **Create**.

   Note: Once created, remove the USB key from the system and store it in a safe location until it is needed.

PSID Erase an Encryption Drive

If you forget the encryption password, you are unable to unlock the drives. If you want to reuse the drives, you need to erase the drive by entering the Physical Secure ID (PSID) in the Verde user interface.

The PSID string is printed on the label physically attached to the drive. It is not available from any other source. Before you can perform a PSID erase, you must remove the drive from the enclosure and record its PSID value.

Caution Performing a PSID Erase on a drive permanently erases all data on the drive.

Use the instructions in this section to perform a PSID erase on the drive.

1. From the menu bar, select **Status ···⁘ Hardware** or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays (see Figure 104 on page 135).
2. Click **Data Drives**. The hardware screen refreshes and displays all disk drives present in the system.
3. Record the slot number and serial number for each drive you want to PSID erase.
4. Power down the system as described in Reboot or Shut down a Verde NAS Solution on page 144.
5. Locate the drive(s) in the chassis using the slot number and verify the serial number(s) you recorded in Step 3.

6. Locate the PSID value on the drive label and record the value.
7. Repeat Step 5 on page 123 and Step 6 for any additional drives you want to erase.
8. Power on the system as described in Power On the Verde NAS Solution on page 39.
9. Log into the NAS solution as described in Log In to the Verde User Interface on page 44.
10. From the menu bar, select **Status** ⋯ **Hardware** or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays (see Figure 104 on page 135).
11. Click **Data Drives**. The hardware screen refreshes and displays all disk drives present in the system.
12. On the row of the drive you want to erase, click PSID Erase. The PSID Erase dialog box displays.

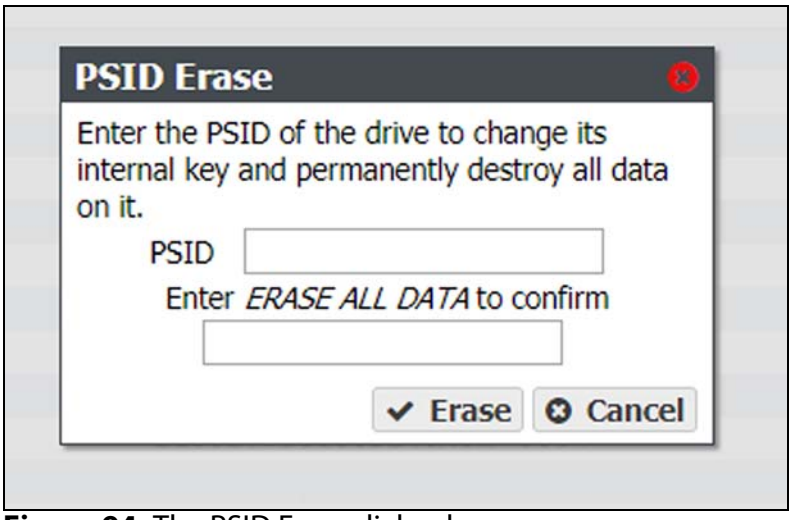


Figure 94 The PSID Erase dialog box.

13. Enter the PSID value you recorded in Step 6 in the **PSID** entry field.
14. Type ERASE ALL DATA in the confirmation entry field.

Caution Performing a PSID Erase on a drive permanently erases all data on the drive.

15. Click **Erase**.
16. Repeat Step 12 through Step 15 for any additional drives you want to erase.

CONFIGURE USERS

Use the instructions in this section to create a new user, edit existing users, change passwords, and configure the session timeout setting.

Description of User Types

See Description of User Types on page 52 for information about each user type.

Create a User

To create a user, see Create a User on page 53.

Edit a User

1. From the menu bar, select **Configuration ···⁘ Users**. The Users screen displays a list of all configured users (see Figure 23 on page 53).
2. Double-click the name of the user you want to edit, or select the user and then select **Action ···⁘ Edit**. The Edit Users dialog box displays.

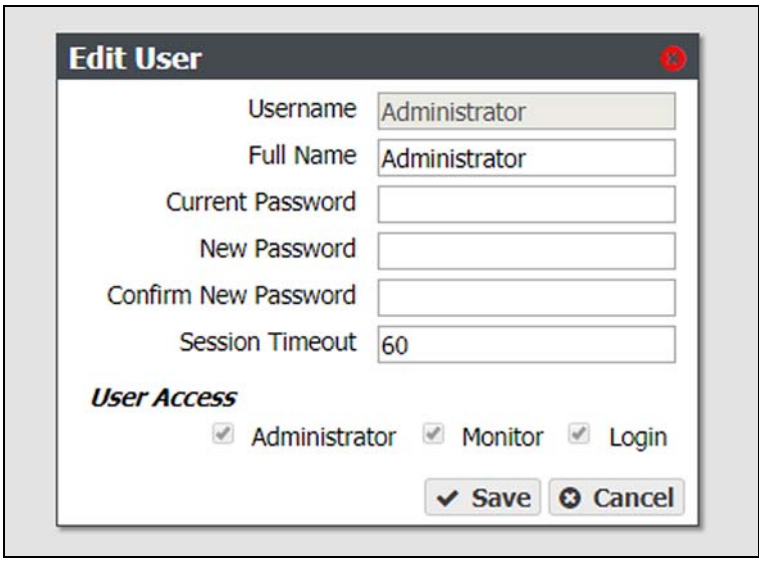


Figure 95 The Edit User dialog box.

3. The **Username** is unavailable and cannot be changed.
4. If desired, edit the user's **Full Name**.

5. If you are changing the password, enter the **Current Password**, the desired **New Password**, then **Confirm New Password**.

   Note: The new password does not take effect until after you log out of the Verde user interface (see Exit the Verde User Interface on page 145).

6. If desired, enter a value for the **Session Timeout** in minutes. This value cannot exceed 999 minutes.
7. Select one or more **User Access** permissions. See Description of User Types on page 52 for information on each level of user access permission.
8. Click **Save**.

Delete a User

1. From the menu bar, select **Configuration ···⁘ Users**. The Users screen displays a list of all configured users (see Figure 23 on page 53).
2. Select the user you want to delete, and then select **Action ···⁘ Delete**. A confirmation window displays.
3. Click **Delete** to delete the user.

CONFIGURE CERTIFICATES

The Verde NAS solution ships with non-signed SSL certificates for the management port on the system. Because the certificates are not signed, you must pass a security check every time you attempt to access the management port to view the Verde user interface.

If desired, you can install signed, trusted SSL certificates for the management port so that you no longer need to pass the security check when accessing this port.

The Verde NAS solution accepts intermediate (chain) SSL certificates, and accepts RSA, DSA, and ECC certificates.

Use the instructions in this section to install an SSL certificate.

1. From the menu bar, select **Configuration ···⁘ Certificates**. The Certificates screen displays.

Figure 96 The Certificates screen.

2. Select the **Management** row, and then select **Action ⋯⁘ Import Certificate**. The Import Certificate dialog box displays.

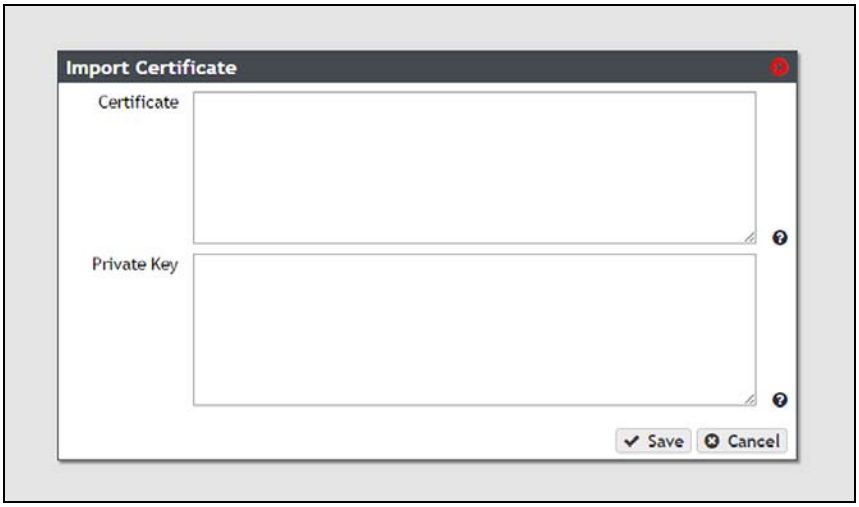


Figure 97 The Import Certificate dialog box.

3. From your source SSL certificate file, copy the certificate portion of the file into your host's cache, and then paste the contents into the **Certificate** entry box.

   Note: The certificate must be in PEM format.

4. From your source SSL certificate file, copy the private key portion of the file into your host's cache, and then paste the contents into the **Private Key** entry box.

   Note: The private key must be in PEM format.

5. Click **Save**.

MANUALLY ENTER ACTIVATION KEYS

If this is an initial installation and your Verde documentation kit included a USB device, see Automatically Import Activation Keys on page 43 for instructions for importing activation keys.

Use the following instructions to manually enter activation keys.

1. Determine the order for installing the activation keys.

- If this is not an initial installation, you can enter activation keys in any order. Proceed with Step 2 on page 128.
- If you want to manually enter the activation keys for an initial installation, they must be entered in the following order:

Important For an initial installation, the activation keys must be entered in the order described in these instructions. Failure to enter the keys in the proper order causes an error.

a. Capacity keys - There are three types of capacity keys.

Key Type	Description
EM_S3_SAS_COUNT	Enables the specified number of SAS drives present in the Verde NAS solution or Verde expansion node.
EM_S3_SATA_COUNT	Enables the specified number of SATA drives present in the ArcticBlue disk solutions.
EM_S3_SSD_COUNT	Enables the specified number of SSD drives present in the Verde 4U NAS solution.

b. All other keys - Any additional keys included on the Software Activation Key Certificate, such as the Software Update key, can be entered in any order.

2. Select **Support** ⋯⁘ **Activation Keys** to display the Activation Keys screen. Any previously entered keys are listed

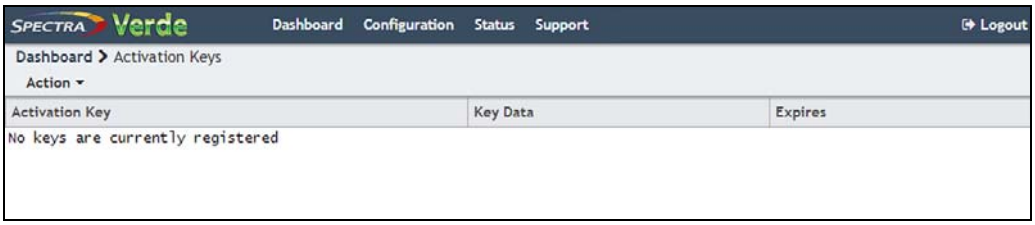


Figure 98 The Activation Keys screen.

3. Select **Action** ⋯⁘ **New**. The Enter Activation Key dialog box displays.

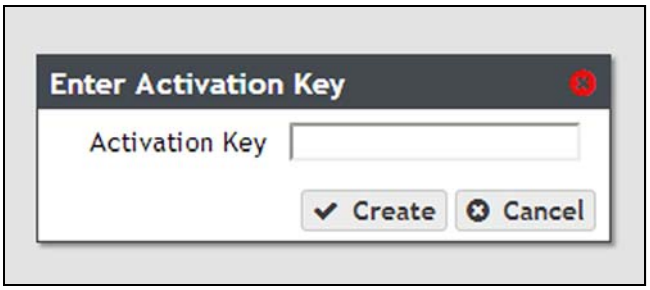


Figure 99 The Enter Activation Key dialog box.

4. Enter the key, exactly as provided, in the Activation Key field and click **Create** to save the key on the system. The Activation Keys screen displays with the newly entered key listed.
5. If necessary, repeat Step 3 and Step 4 to enter any additional keys.

CHAPTER 6

Monitoring a Verde NAS Solution

This chapter describes procedures for day-to-day monitoring and operation of a Spectra Verde NAS solution.

Topic	
Monitor the Verde NAS Solution	page 130
Front Bezel Visual Status Beacon	page 131
Configure the Visual Status Beacon Color	page 132
System Status LEDs	page 133
View System Messages	page 134
View the Status of Hardware Components	page 135
View the Status of Pools	page 136
View the Status of Volumes	page 139
View the Status of Shares	page 139
View the Status of Services	page 140
View Performance Metrics	page 141
View Reports	page 143
Reboot or Shut down a Verde NAS Solution	page 144
Using the Verde User Interface	page 144
Power-Cycle Reset	page 145
Exit the Verde User Interface	page 145

MONITOR THE VERDE NAS SOLUTION

The Visual Status Beacon and the Verde user interface combine to provide a number of tools for monitoring the health and performance of the Verde NAS solution and its components.

- The Visual Status Beacon light bar in the front bezel of the Verde NAS solution changes color to indicate the current status of the system (see Front Bezel Visual Status Beacon on page 131).

  Note: The front bezel in a Verde 2U NAS solution, and some 4U NAS solutions, do not include a Visual Status Beacon light bar.

- System messages provide important information about the Verde NAS solution and their operation (see View System Messages on page 134 for more information).
- Icons on the System screen provide overall status of the hardware components in each group (see View the Status of Hardware Components on page 135 for more information).

  Clicking the text next to each icon displays detailed status information for the components in the group.
- The system status LEDs provide information about the status of the NAS solution, its fans, network connections, and power supplies (see System Status LEDs on page 133 for more information).
- You can also use the Verde user interface to do the following on the Verde NAS solution:
  - View the status of services (see View the Status of Services on page 140).
  - View performance metrics for the drives, CPUs, storage pools, and network (see View Performance Metrics on page 141).
  - View the current network configuration settings (see Configure Network Connections and Settings on page 101).
  - Reboot or shut down the system (see Reboot or Shut down a Verde NAS Solution on page 144).

Front Bezel Visual Status Beacon

The Visual Status Beacon light bar in the front bezel provides an at-a-glance status of the system to which it is mounted. The light bar changes color to indicate the status of the system. See the chart below for each color displayed and its associated condition.

Color Display	Condition
Green Scroll	The system is operating normally. **Note:** The color displayed when the system is operating normally can be changed on the Hardware screen. See Configure the Visual Status Beacon Color on page 132 for more information.
Yellow Scroll	The system is experiencing a Warning condition. Log in to the Verde user interface to determine the cause of the warning.
Red Scroll	The system is experiencing an Error condition. Log in to the Verde user interface to determine the cause of the error.
Rainbow	The system is currently powering on and performing self-tests.
Flashing Blue	The beacon feature was activated for this system. This can help you identify a specific system when you have more than one Verde NAS solution in your environment. See View the Status of Hardware Components on page 135 for instructions on activating the beacon.
Pulsing Red	The Visual Status Beacon lost communication with the system. This can occur if the system experiences a software hang.
No Light	The Verde NAS solution is powered off.

Note: Other patterns may display if the front bezel is not properly seated on the system.

Configure the Visual Status Beacon Color

The Verde NAS solution is configured to display a green scrolling light on the Visual Status Beacon when the system has an overall status of "good". If desired, you can change the color displayed for good status.

Note: The front bezel in a Verde 2U NAS solution, and some 4U NAS solutions, do not include a Visual Status Beacon light bar.

1. From the menu bar, select **Status** ⋯ **Hardware**, or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays.
2. Click **Bezel**. The Bezel pane of the Hardware screen displays.
3. Click the colored box next to **Select Bezel Color**. The color picker window displays.

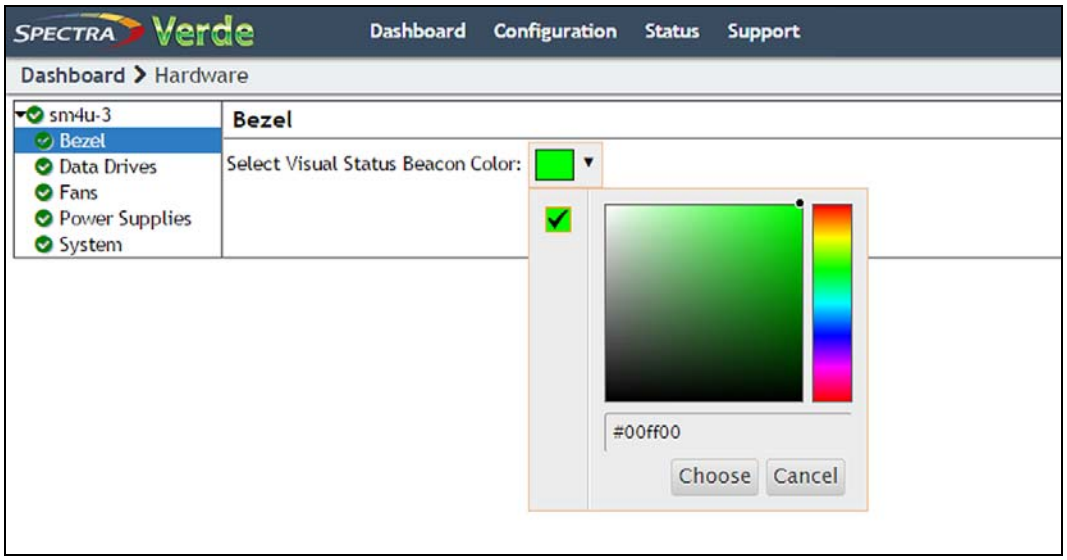


Figure 100 Use the color picker to set the color displayed on the Visual Status Beacon when the system is operating normally.

4. Use the color picker to select the color to display when the system is operating normally. Optionally, you can enter an HTML color code in the entry field.

   Note: Spectra Logic recommends against using yellow or red, so that you can more easily determine if the system is in a warning or error state.

5. Click **Choose** to set the color of the Visual Status Beacon.

System Status LEDs

The system status LEDs provide information about the status of the NAS solution, its fans, network connections, and power supplies. See the table below for a list of each system status LED and its function.

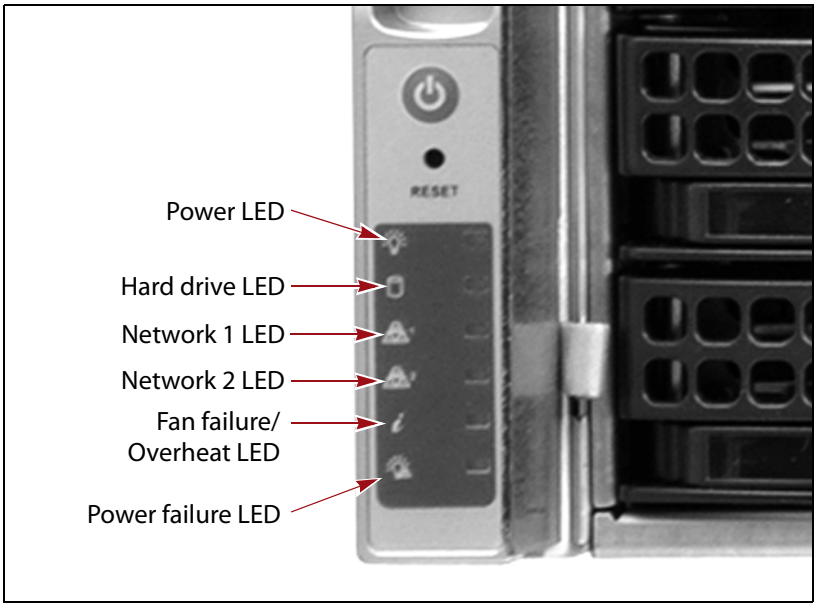


Figure 101 System status LEDs.

LED	Function
Power	Indicates if the unit is powered on.
Hard Drive	Indicates boot drive activity. To see the activity of a data drive, see Data drive status LEDs on page 22.
Network 1	Indicates network activity on the Verde management port.
Network 2	Indicates network activity on data interface 1. This LED also shows network activity if data interface 1 is configured in link aggregation mode.
Fan Failure / Overheat	▪ If the LED is blinking red, it indicates a fan failure. Log into the Verde user interface to determine which fan failed. ▪ If the LED is solid red, it indicates an overheat condition. Log into the Verde user interface to view the status of the system. If the problem persists, contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 7.
Power Failure	Indicates a power supply failure. Log into the Verde user interface to determine which power supply failed.

View System Messages

Check the system messages regularly. These messages provide important information about the Verde NAS solution and its operation. Reviewing the messages is the first step in troubleshooting.

Types of Message Severity

Messages displayed in the Verde user interface use one of the below severities:

Type	Description
Information	Notifies the user about an event that requires no action and does not fit the other categories.
Success	Notifies the user of successful completion of an event.
Alert	Notifies the user that a failure occurred which requires some sort of user interaction, and until this occurs, operation of the Verde NAS solution may be impacted.
Warning	Notifies the user of a failure that may adversely impact the Verde NAS solution.
Critical	Notifies the user of a failure that caused significant adverse impact to the Verde NAS solution.

The status bar displayed at the bottom of all Verde interface screens shows the highest severity and generation date and time for all unread messages. If there are no system messages, this text does not display.

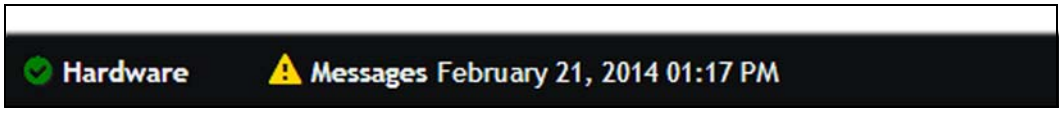


Figure 102 A system message displayed on the Verde user interface status bar.

1. From the menu bar, select **Status ···⁘ Messages,** or click the Messages link on the status bar, to display the Messages screen.

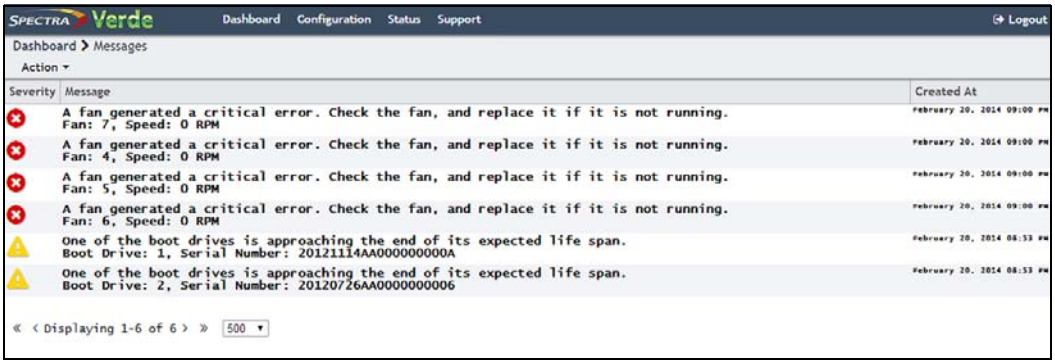


Figure 103 The Messages screen.

Pay extra attention to any messages flagged with the Warning or Error icon (see Status Icons on page 37), and follow any recommended steps. Contact Spectra Logic Technical Support if you need assistance (see Contacting Spectra Logic on page 7).

Note: You cannot delete messages. The Verde NAS solution automatically deletes the oldest messages on a first-in, first-out basis as space is required, retaining the most recent messages. The system holds 10,000 messages.

2. If desired, use the **Page Length** drop-down menu to limit the Messages screen to the specified number of messages.
3. To mark a single message as read, select the message and then select **Action ⋯⁘ Mark as read**. To mark all messages as read, select **Action ⋯⁘ Mark all as read**.

Note: Messages can also be marked as **Unread** using the **Action** menu.

View the Status of Hardware Components

The Verde user interface lets you monitor the status of hardware components without having direct physical access to the Verde NAS solution. This is especially useful when your NAS solution is operating in a "lights out" data center. Check the Verde user interface regularly to ensure that you always know the status of the hardware components.

1. From the menu bar, select **Status ⋯⁘ Hardware** or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays.

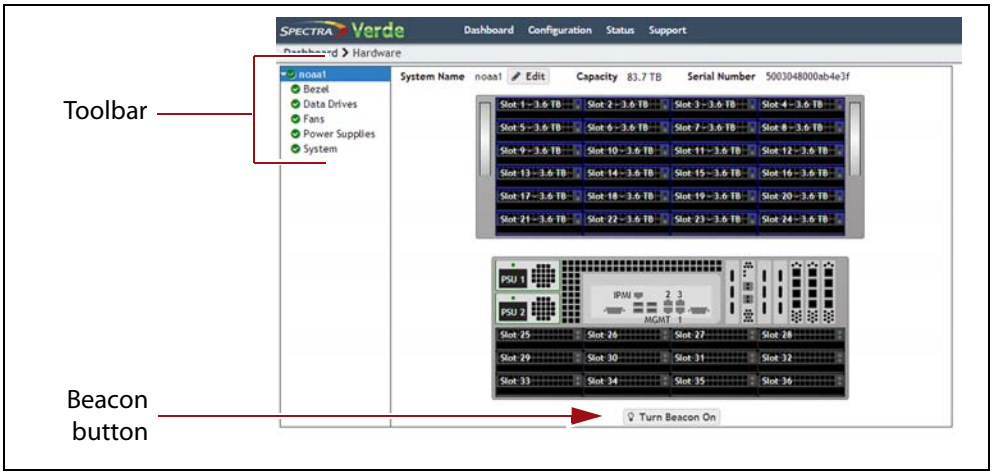


Figure 104 The Hardware screen (Verde 4U master node shown).

2. Use the toolbar menu on the left-hand side of the screen to view detailed information about component groups. The following table describes the types of information on each details screen. An icon next to each component indicates its status (see Status Icons on page 37 for a description of the icons).

Clicking...	Shows the...
Bezel	Color of the Visual Status Beacon that is displayed during normal operation. See Front Bezel Visual Status Beacon on page 131 for more information about the colors displayed by the Visual Status Beacon.
Data Drives	▪ Slot number of each drive ▪ Status of each drive ▪ Drive size, serial number, and firmware level ▪ The name of the storage pool to which the drive is assigned
Fans	▪ Status of midplane fans
Power Supplies	▪ Power supply status and wattage **Note:** Power supply information is not available for the 107-drive expansion node.
System	▪ CPU status and temperature ▪ System memory status and size ▪ Status, manufacturer, model, size, and serial number for each DOM boot drive
Turn Beacon On *(below chassis graphic)*	Click **Turn Beacon On** to cause the Visual Status Beacon light on a Verde NAS solution to flash blue. This is useful when you have multiple systems and need to locate a specific one, for example to replace a component. Click the button a second time to stop the light from flashing.

View the Status of Pools

The Pools screen provides status information about all storage pools that are configured on the system.

1. From the menu bar, select **Status** ⋯⁘ **NAS** ⋯⁘ **Pools** to display the Pools screen.

2. The status of each storage pool is indicated by the status icons on the left side of the screen.

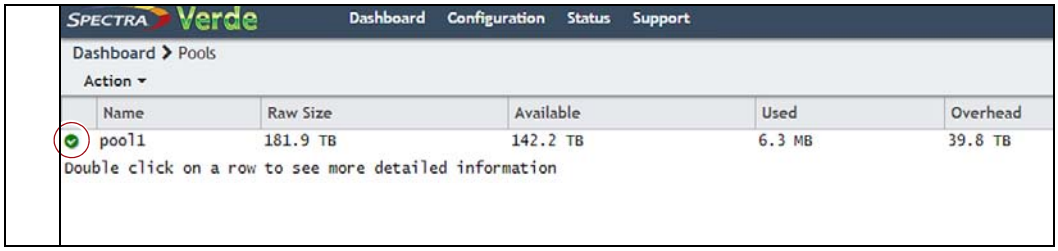


Figure 105 The Pools screen.

The Pools screen displays the following information.

This column...	Shows...
Name	The name of each NAS pool.
Health	The current health of each pool. ▪ **Online** — The cache is operating normally. ▪ **Degraded** — One or more drives in the cache is missing, or failed.
Raw Size	The total amount of storage space assigned to each pool.
Available	The amount of unused storage space in each pool.
Used	The amount of used storage space in each pool.
Overhead	The amount of disk space used for overhead, such as parity data.
Fault Tolerance	The fault tolerance setting for each pool.

3. To view additional information about a NAS pool, select the pool and then select **Action ⋯⁘ Show Details**. The *pool name* details screen displays.

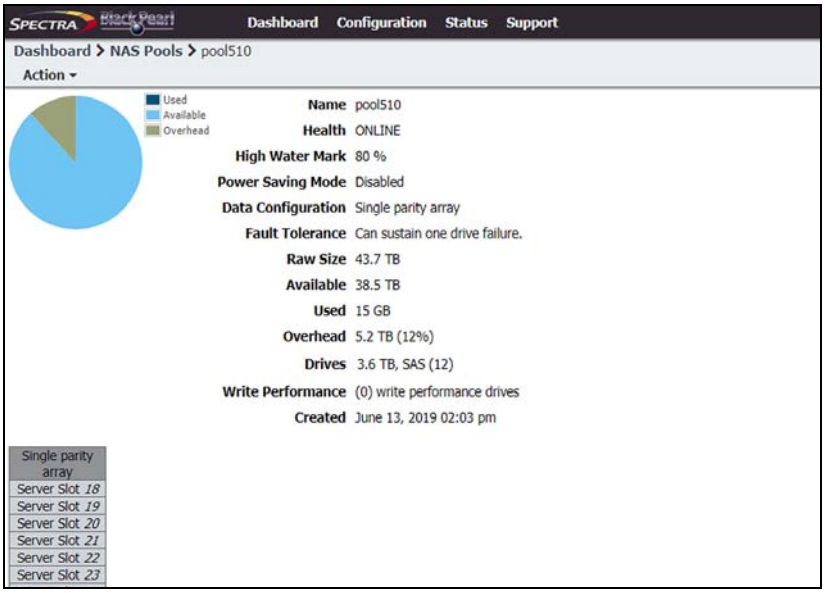


Figure 106 A NAS Pool details screen.

The *pool name* details screen displays the following information:

This row...	Shows...
Name	The name of the pool.
Health	The current health of the pool.
High Water Mark	When the used space on the pool reaches this percentage, an alert is generated. No alert is generated when the percentage is set to zero.
Power Saving Mode	Indicates if power saving mode is enabled or disabled.
Data Configuration	The protection level for the pool.
Fault Tolerance	The number of drives that can fail before data is lost.
Raw Size	The total amount of storage space assigned to the pool.
Available	The amount of available (unused) storage space in the pool.
Used	The amount of used storage space in the pool.
Overhead	The amount of disk space used for overhead, such as parity data.
Drives	The size, RPM, type, and number of drives assigned to the pool.
Write Performance	The number of write performance drives assigned to the pool.

This row...	Shows...
Created	The timestamp of when the pool was created.
Stripe	The location of all disks included in the pool.

View the Status of Volumes

The Volumes screen provides status information about all volumes that are configured on the system.

1. From the menu bar, select **Status ⋯⁝ NAS ⋯⁝ Volumes** to display the Volumes screen.
2. The status of each volume is indicated by the status icons on the left side of the screen.

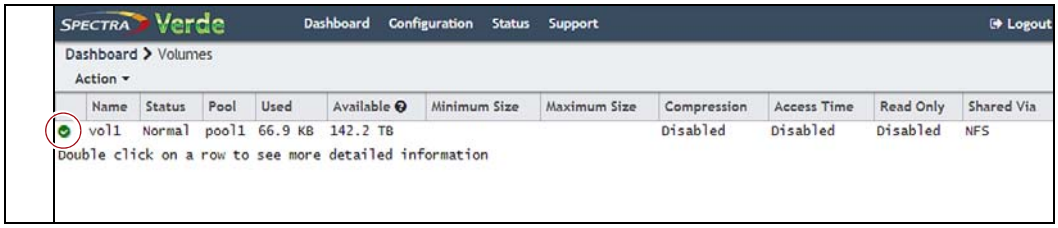


Figure 107 The Volumes screen.

View the Status of Shares

The Shares screen provides status information about all shares that are configured on the system.

1. From the menu bar, select **Configuration ⋯⁝ NAS ⋯⁝ Shares ⋯⁝ CIFS** to display the CIFS Shares screen, or select **Configuration ⋯⁝ NAS ⋯⁝ Shares ⋯⁝ NFS** to display the NFS Shares screen.
2. The status of each share is indicated by the status icons on the left side of the screen.

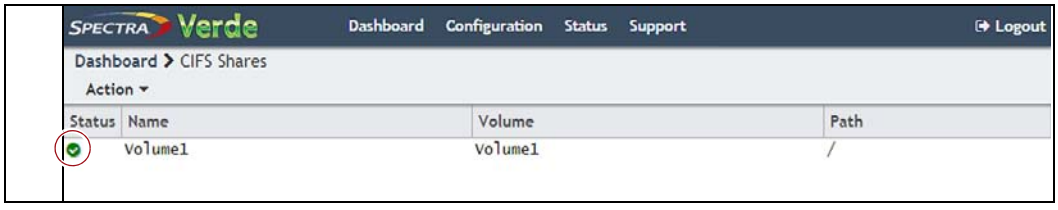


Figure 108 The CIFS Shares screen.

View the Status of Services

The Services screen provides status information about services that are currently installed on the Verde master node.

1. From the menu bar, select **Configuration ···⁝ Services** to display the Services screen.

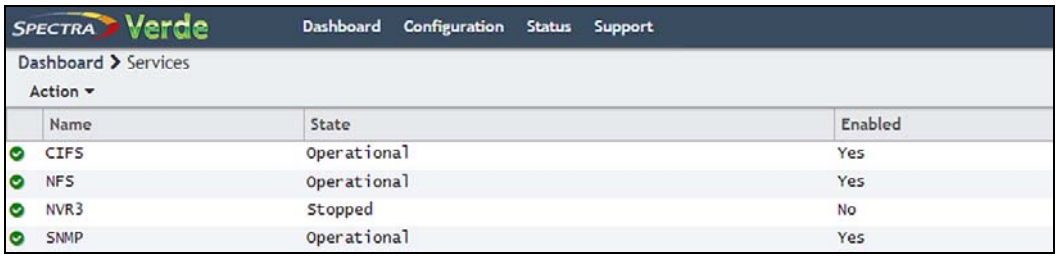


Figure 109 The Services screen.

This column...	Shows...
Name	The name of the service running on the system.
State	The status of the service on the Verde NAS solution. ▪ **Starting**—The service is starting up. ▪ **Operational**—The service is running. ▪ **Stopped**—The service is not running.
Enabled	Whether or not the service is enabled at system startup. ▪ **Yes**—Service automatically starts when the system is powered on. ▪ **No**—Service does not start when the system is powered on.

View Performance Metrics

The Performance screen displays performance metrics for the Verde NAS solution storage pools, individual data drives, CPUs, and network traffic. Performance graphs can be configured to display either the last 5 minutes of activity, or the last 25 hours.

1. From the menu bar, select **Status** ⋯⁘ **Performance** or click the Performance pane on the Dashboard. The Performance screen displays.

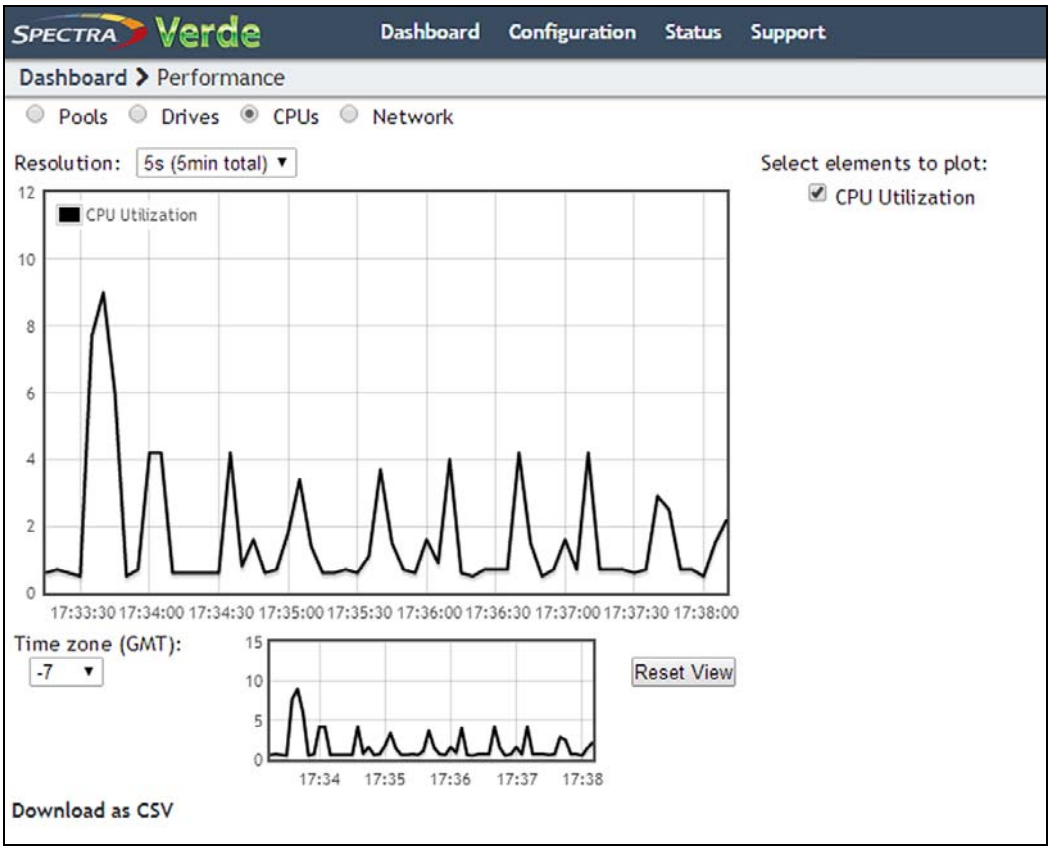


Figure 110 The Performance screen.

2. Select **Pools**, **Drives**, **CPUs**, or **Network** to display performance information about the selected component.

   Note: If you select **Pools**, **Drives**, or **Network**, use the **Pool**, **Disk**, or **Interface** drop-down menu to select a specific storage pool, disk drive, or network connection to display.

3. Select the time interval using the **Resolution** drop-down menu. The data can be displayed in 5 second increments (5 minutes total) or 60 second increments (25 hours total).

4. Select or clear options under **Select elements to plot** to indicate which graph lines to display. The graph updates as soon as you select or clear an option.

5. Set the performance graph's time values to your local time zone using the **Time zone** menu. All entries are listed in +/- GMT.

6. If desired, click **Download as CSV** in the lower, left corner of the panel, to download a comma separated value file, containing the data for the graph you are currently viewing. The file can then be imported into MicroSoft Excel or other software applications that support this file type.
7. To see the performance data in greater detail, select the desired section you want to magnify in either the main or range indicator graph. Using the mouse, click and drag the cursor horizontally over the section of the graph that you want to magnify. The highlighted section of data is shown on the main graph.

   The range indicator graph continues to display the original range of data, with the section that is currently being shown on the main graph highlighted.

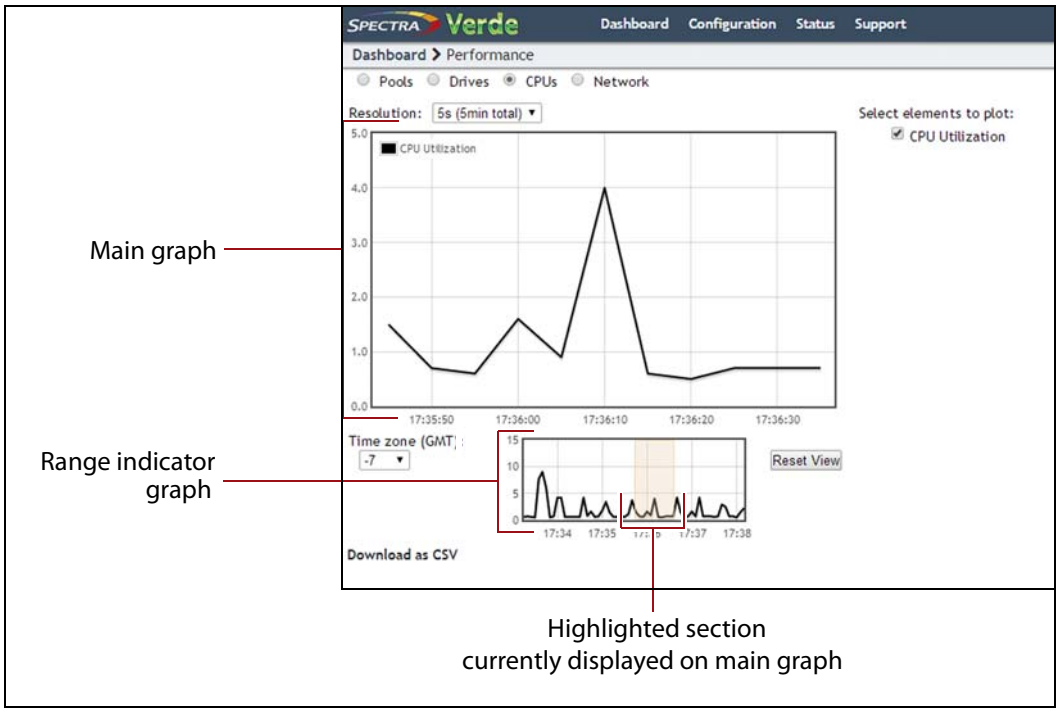


Figure 111 Highlight a section of the graph to show it in greater detail.

8. Click **Reset View** to reset the main graph to the default view.

View Reports

The Reports screen lets you to generate reports on all aspects of the Verde NAS solution, including component status and configuration. Reports can be saved in either JSON or XML format.

1. From the menu bar, select **Status** ⋯⁘ **Reports** to display the Reports screen.

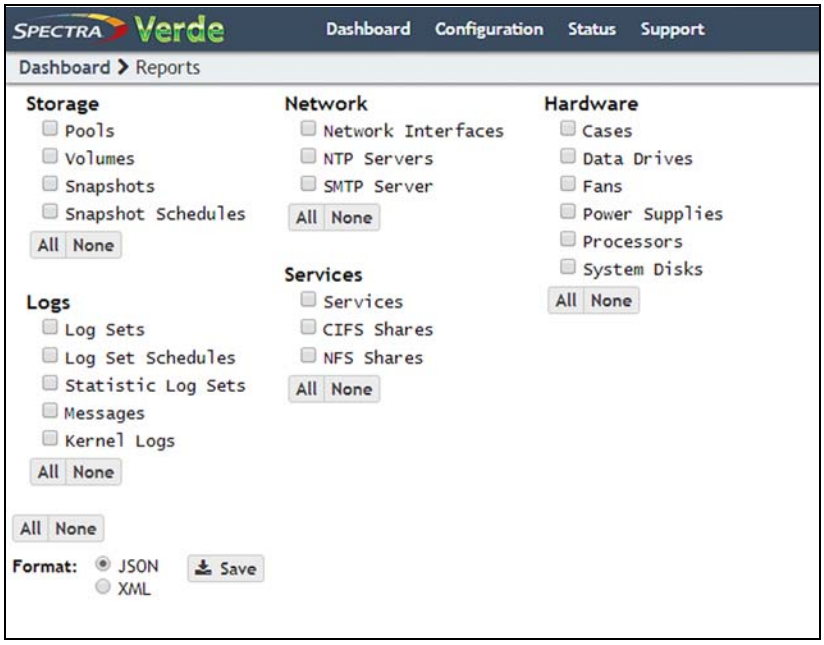


Figure 112 The Reports screen.

2. Select check boxes next to the report(s) you want to generate.

   Note: You can use the **All** or **None** buttons at the bottom of each report group to select or clear that group of reports. The **All** and **None** buttons at the bottom of the screen select or clear all reports shown on the screen.

3. Select the **Format** for the report(s). Only one format can be selected.
4. Click **Save**. The system saves the selected reports to your local host.
5. Open a report using a compatible program.

REBOOT OR SHUT DOWN A VERDE NAS SOLUTION

This section discusses rebooting or shutting down a NAS solution.

Using the Verde User Interface

Use the following instructions to reboot or shut down a system using the Verde user interface.

1. Click the power icon in the lower right-hand corner of any screen in the Verde user interface. The Power screen displays.

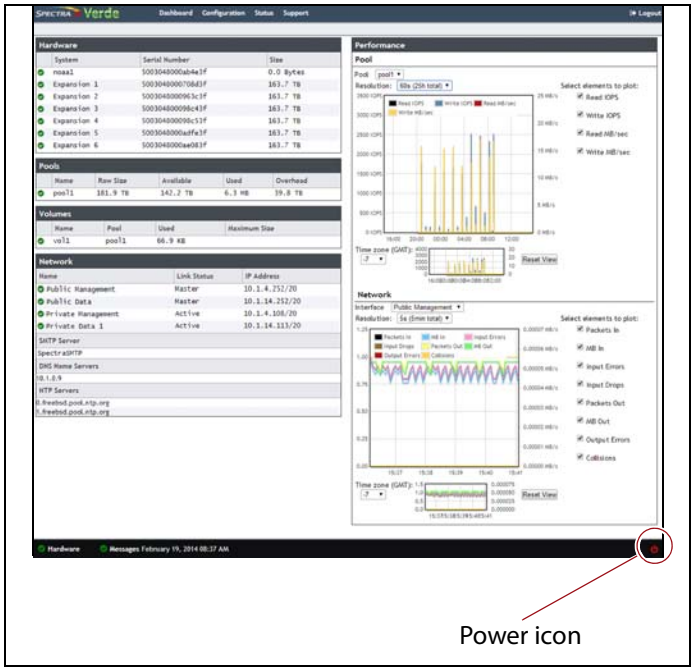


Figure 113 The Power icon.

2. Click either **Reboot** or **Shutdown**.
3. A confirmation screen appears. Confirm the selection to perform the reboot or shutdown.

Power-Cycle Reset

Under some circumstances, Spectra Logic Technical Support may direct you to perform a power-cycle reset of a Verde NAS solution to recover from an error. To power-cycle reset a Verde NAS solution, remove the front bezel, and then press and hold the front panel power button (Figure 101 on page 133) until the button's LED turns off. After a few moments, press the button again to turn the system back on.

Caution Do not use the power button to turn off a Verde NAS solution unless you are specifically instructed to do so by Spectra Logic Technical Support.

EXIT THE VERDE USER INTERFACE

To exit the Verde user interface, close the browser or click **Logout** on the right side of the menu bar. This ends the session.

If the active session is idle for more than the set session timeout, the current user is automatically logged out. The default is 60 minutes. This setting can be configured on the Users screen. See Create a User on page 53.

CHAPTER 7

Using AutoSupport

This chapter describes using the Verde user interface to configure the support features of the Verde NAS solution.

Task	
About AutoSupport	page 147
Enter Contact Information	page 147
Configure Mail Recipients	page 148
Add a New Recipient	page 148
Edit a Mail Recipient	page 149
Send a Test Email	page 150
Delete a Mail Recipient	page 151
Log Sets	page 151
Configure a Log Set Schedule	page 152
Manually Generate Log Sets	page 153
Email a Log Set	page 153
Download a Log Set	page 154
Delete a Log Set	page 154

ABOUT AUTOSUPPORT

AutoSupport lets the Verde NAS solution automatically contact mail recipients when the system generates certain kinds of messages. You can also use it to generate AutoSupport Log (ASL) sets for use by Spectra Logic Technical Support. The system can email ASL sets to Spectra Logic or mail recipients when critical events occur, or on a monthly basis.

ENTER CONTACT INFORMATION

Contact information helps Spectra Logic to contact the administrator of the Verde NAS solution during troubleshooting. Entering the contact information is typically a one-time-only process.

1. From the menu bar, select **Support** ⋯⁘ **Contact Information** to display the Contact Information screen.
2. Click **New** in the Customer Contact Information pane. The New Contact Information dialog box displays.

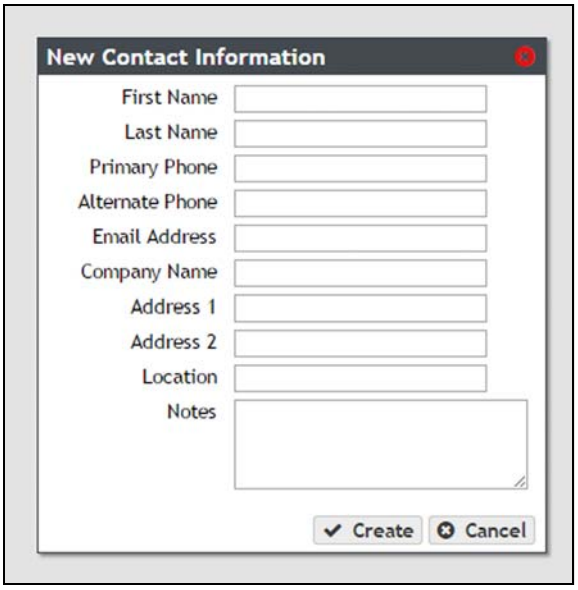


Figure 114 The New Contact Information dialog box.

3. Enter the requested information and click **Create**.

CONFIGURE MAIL RECIPIENTS

You can configure AutoSupport to email system messages and log sets as they are generated, to selected recipients. All log sets and messages are sent to a previously configured mail recipient. You cannot send log sets or messages directly to an email address. Use the Mail Recipients screen to add, edit, or delete mail recipient accounts.

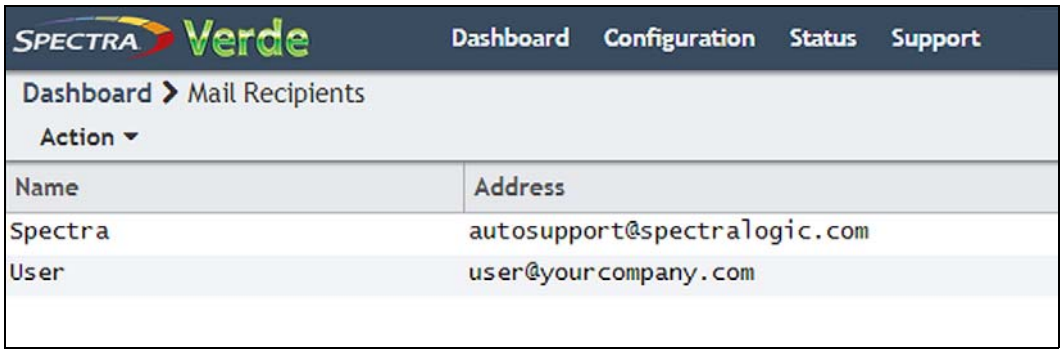


Figure 115 The Mail Recipients screen.

Add a New Recipient

Use these instructions to add a new mail recipient.

1. From the menu bar, select **Configuration ···⁘ Mail Recipients** to display the Mail Recipients screen.
2. Select **Action ···⁘ New**. The New Mail Recipient dialog box displays.

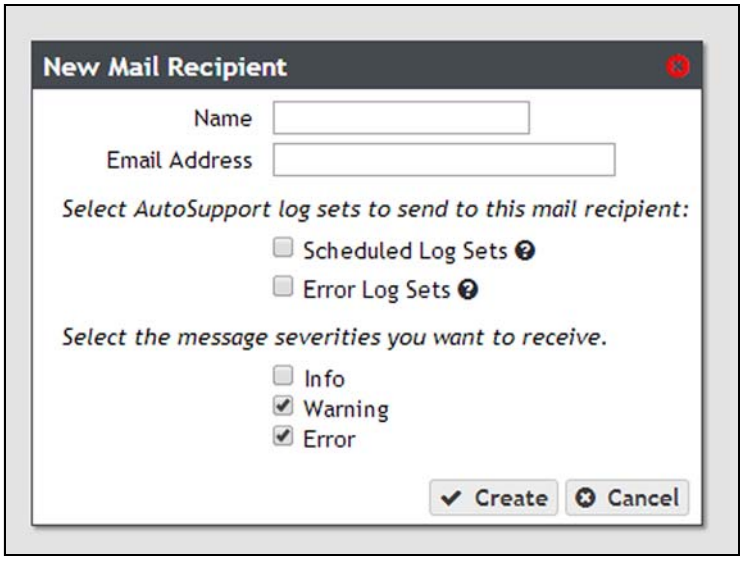


Figure 116 The New Mail Recipient dialog box.

3. Enter the following information for the mail recipient:

Field	Description
Name	The name of the recipient.
Email Address	The email address of the recipient. Be sure to use the full address using the standard email format, including the @ symbol. **Important:** The address cannot contain spaces or other non-alphanumeric characters (for example, an ampersand, &).
Select AutoSupport log sets to send to this mail recipient	Select **Scheduled Log Sets**, **Error Log Sets**, both options, or neither option for the mail recipient. Scheduled log sets are sent from the Verde NAS solution on the first of each month. Error log sets are sent anytime an error occurs that causes the system to generate a log set.
Select the message severities you want to receive	Select from the listed message types, which severities of message this mail recipient should receive. The Verde master node automatically sends email messages of the selected severity to the recipient when they are generated. For a description of message severities, see Types of Message Severity on page 134. **Note:** For the mail recipient to receive all messages generated by the system, select all boxes.

4. Click **Create** to save the information. The Mail Recipients screen re-displays with the new mail recipient added to the list of mail recipients.
5. Repeat Step 1 on page 148 through Step 4 to configure additional mail recipients.

Edit a Mail Recipient

Use the following steps to edit a mail recipient.

1. From the menu bar, select **Configuration ⋯⁘ Mail Recipients**. The Mail Recipients screen displays with any already configured mail recipients listed.

2. From the list of mail recipients, double-click the name of the recipient whose information you want to edit, or select the name, and then select **Action ⋯⁘ Edit**. The Edit Mail Recipient dialog box displays.

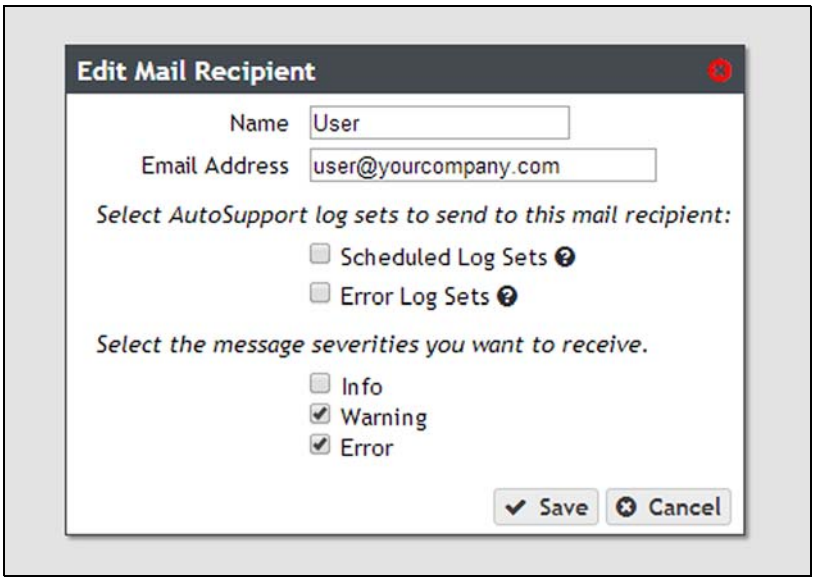


Figure 117 Edit the information for the selected mail recipient.

3. Change the information for the recipient as required and then click **Save**. See Add a New Recipient on page 148 for a explanation of the options.

Send a Test Email

Use the following steps to send a test email to a mail recipient.

1. From the menu bar, select **Configuration ⋯⁘ Mail Recipients**. The Mail Recipients screen displays with any already configured mail recipients listed.
2. From the list of mail recipients, select the name of the recipient you want to send a test email, and then select **Action ⋯⁘ Send test email**.

   The Verde master node immediately sends a test email to the selected account.
3. Verify the user received the email from the Verde master node. If the email is not received, verify that you entered the mail recipients email address and the SMTP server settings correctly (see Configure SMTP Settings on page 108).

Delete a Mail Recipient

Use the following steps to delete a mail recipient.

1. From the menu bar, select **Configuration ⋯⁘ Mail Recipients**. The Mail Recipients screen displays with any already configured mail recipients listed.
2. From the list of mail recipients, select the name of the recipient you want to delete, and then select **Action ⋯⁘ Delete**. A dialog box displays asking you to confirm the deletion of the mail recipient.

   Note: The default **Spectra** mail recipient cannot be deleted.

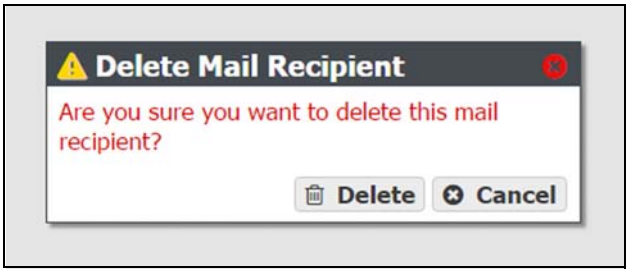


Figure 118 Delete the selected mail recipient.

3. Click **Delete** to confirm the deletion.

LOG SETS

The Verde NAS solution automatically generates log sets when errors occur. Log sets can also be generated manually, or generated on a schedule. The Verde NAS solution generates three types of log sets:

- **Log Sets** contain information about the configuration and status of the Verde NAS solution and are used for general troubleshooting. Log sets can be mailed to configured mail recipients or to Spectra Logic Technical Support.
- **Statistic Log Sets** contain performance data about the system and are used by Spectra Logic Technical Support for in-depth troubleshooting. Statistic log sets are too large to mail directly from the system and must be downloaded.
- **Kernel Log Sets** are generated whenever a process on the system fails. This log set cannot be generated manually.

Use the Logs screen to generate, email, or download log sets, as well as to configure a log set schedule.

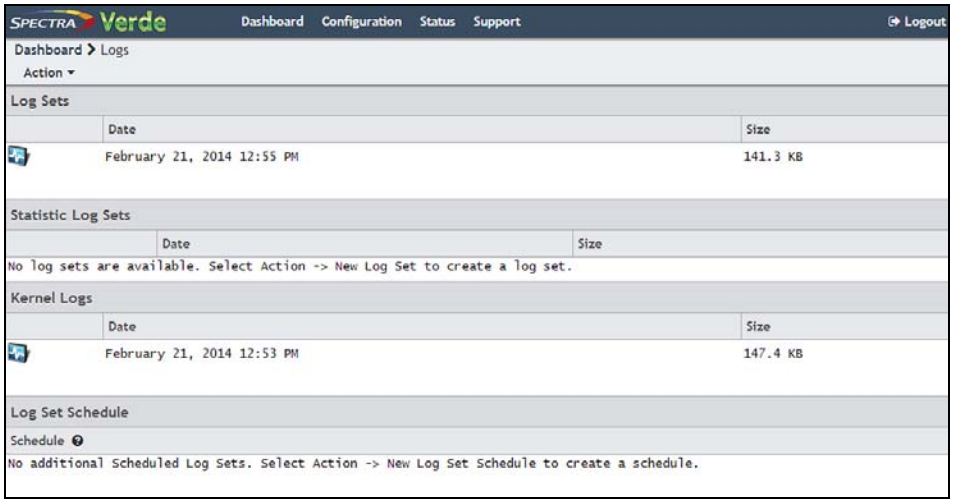


Figure 119 The Logs screen.

Configure a Log Set Schedule

Use the instructions in this section to configure a log set schedule.

1. From the menu bar, select **Support ···⁘ Logs.** The Logs screen displays.
2. Select **Action ···⁘ New Log Set Schedule**. The New Log Set Schedule dialog box displays.

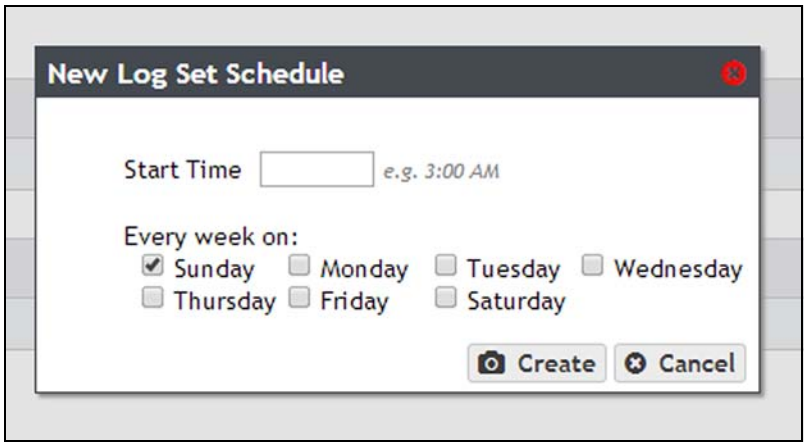


Figure 120 The New Log Set Schedule dialog box.

3. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
4. Select one or more days for **Every week on:**. This determines the day(s) of the week the system generates log sets.
5. Click **Create**. The Logs screen displays showing the newly created Log Set Schedule.

Manually Generate Log Sets

Although the Verde master node automatically generates log sets whenever errors occur, you may want to create log sets manually for troubleshooting purposes or at the request of Spectra Logic Technical Support. Use the following instructions to manually generate a log set.

1. From the menu bar, select **Support ⋯⁘ Logs.** The Logs screen displays (see Figure 119 on page 152).
2. Create the desired log set:
   - Select **Action ⋯⁘ New Log Set** to generate a log set for use in general troubleshooting. Continue with Email a Log Set below, or Download a Log Set on page 154.

     —OR—
   - Select **Action ⋯⁘ New Statistic Log Set** to generate a log set used for in-depth troubleshooting. This log is not human readable. To see performance statistics in a human readable form, see View Performance Metrics on page 141. Continue with Download a Log Set on page 154.

Email a Log Set

Use the instructions in this section to email a log set.

Note: You must configure the SMTP settings on the system before you can send emails. See Configure SMTP Settings on page 108 to configure the SMTP settings.

1. From the menu bar, select **Support ⋯⁘ Logs.** The Logs screen displays (see Figure 119 on page 152).
2. Select the log set you want to email, and then select **Action ⋯⁘ Email**. The Email Log Set dialog box displays.

   Note: Statistic Log Sets are too large to email from the system, and must be downloaded. See Download a Log Set on page 154.

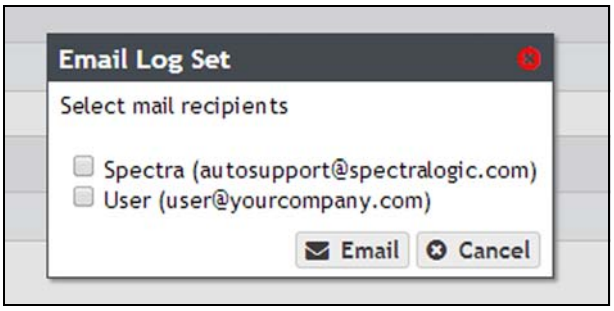


Figure 121 The Email Log Set dialog box.

3. Select the mail recipients you want to receive the log set, and click **Email**.

Download a Log Set

Use the instructions in this section to download a log set.

1. From the menu bar, select **Support ⋯⁘ Logs.** The Logs screen displays (see Figure 119 on page 152).
2. Select the log set you want to download, and then select **Action ⋯⁘ Download**. The log set begins downloading to your host computer.

Delete a Log Set

Use the instructions in this section to delete a log set.

1. From the menu bar, select **Support ⋯⁘ Logs.** The Logs screen displays (see Figure 119 on page 152).
2. Select the log set you want to delete, and select **Action ⋯⁘ Delete**. A confirmation window displays asking you to confirm the action.
3. Click **Delete** to delete the log set.
4. Optionally, use one of the following commands to delete log sets in bulk:

Command	Description
Action ⋯⁘ Delete All Log Sets	Deletes all log sets present on the system.
Action ⋯⁘ Delete All Statistic Log Sets	Deletes all statistic log sets on the system.
Action ⋯⁘ Delete All Kernel Logs	Deletes all kernel log sets on the system.

CHAPTER 8

Maintaining a Verde NAS Solution

This chapter describes the maintenance procedures for a Verde NAS solution.

Task	
Data Integrity Verification	page 156
Cancel Data Integrity Verification	page 156
Initiate RSC Backup	page 157
Accessing the Technical Support Portal	page 157
Create an Account	page 157
Log Into the Portal	page 159
Configuring Automated Software Upload	page 160
Updating Software	page 161
Check the Current Software Version	page 161
Check the Currently Released Verde Software Version	page 162
Download and Stage the Updated Software	page 163
Install the Update	page 165
Installing a New Data Drive	page 166
Ensure ESD Protection	page 166
Install the Drive	page 167
Replacing a Failed Component	page 169
Identify the Failed Component	page 169

DATA INTEGRITY VERIFICATION

The Verde NAS solution allows you to perform on-demand data integrity verifications on any disk pools connected to the system. Performing a data integrity verification on a disk pool is useful when you want to ensure the data on the disk pool is stored correctly.

Data integrity verification is a sector by sector check of the entire storage pool, not just the data contained on the pool. The duration of a data integrity verification varies based on the size of the disk pool, and in some cases can take a very long time to complete.

Use the instructions in this section to perform a data integrity verification on a disk pool.

Use the following instructions to perform a data integrity check.

1. From the menu bar, select **Support ⋯⁘ Tools ⋯⁘ Data Integrity Verification**. The Data Integrity Verification screen displays.

Figure 122 The Data Integrity Verification screen.

2. Select the storage pool you want to scan with data integrity verification, and then select **Action ⋯⁘ Start**. A confirmation screen displays.

   Note: While the verification is in progress, the disk pool may experience degraded performance. However, client access and rebuilds have priority over data integrity verification.

3. Click **Start Data Verification** to start the scan.

Cancel Data Integrity Verification

If desired, you can stop a data integrity verification while it is in progress.

1. From the menu bar, select **Support ⋯⁘ Tools ⋯⁘ Data Integrity Verification.** The Data Integrity Verification screen displays.
2. Select the pool for which you want to stop verification in the Data Integrity Verification screen, and then select **Action ⋯⁘ Cancel**.
3. A confirmation screen displays. Click **OK** to stop the verification.

INITIATE RSC BACKUP

The replicated system configuration backup stores the current configuration of all settings for the Verde NAS solution on a storage pool present in the system. This backup occurs automatically each time you create a storage pool, or once every seven days. If you make major changes to your Verde NAS solution, it is recommended that you save the configuration manually.

Use the instructions in this section to manually save the replicated system configuration.

1. From the menu bar, select **Support ···⁘ Tools ···⁘ Data Integrity Verification.** The Data Integrity Verification screen displays (see Figure 122 on page 156).
2. Select **Action ···⁘ Initiate RSC Backup.** A confirmation screen displays.
3. Click **Initiate RSC Backup** to manually save the current system configuration.

ACCESSING THE TECHNICAL SUPPORT PORTAL

The Spectra Logic Technical Support portal provides access to the Knowledge Base, the current version of Verde software for the NAS solution, and additional service and support tools. You can also open or update a support incident and upload log files.

Create an Account

Access to *User Guides* and compatibility matrices does not require you to create an account. You must create a user account and log in to access *Release Notes* or repair documents, to download the latest version of Verde software, or to open a support incident.

Note: If you have multiple Spectra Logic products, the serial numbers for all products are associated with your account. If you do not see the serial numbers for all of your products when you log in, contact Technical Support (see Contacting Spectra Logic on page 7).

1. Access the Technical Support portal login page at support.spectralogic.com.
2. On the home page, click **create an account**.

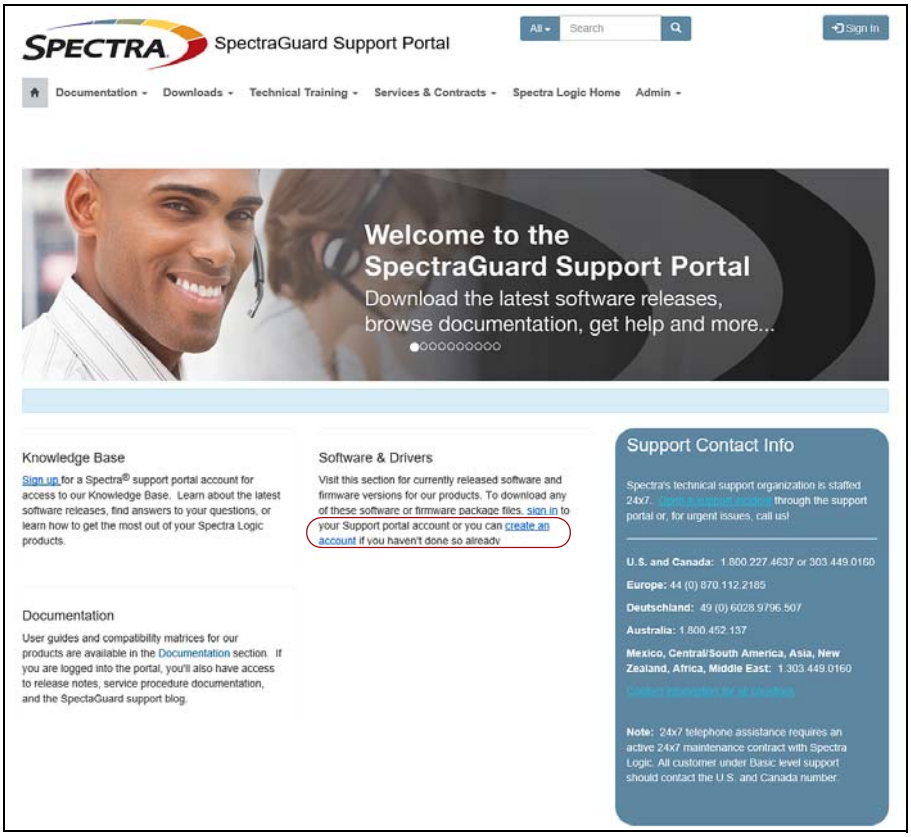


Figure 123 The Spectra Logic Technical Support portal home page.

3. Enter your registration information. Your account is automatically associated with the serial numbers of all Spectra Logic products owned by your site.
   - If you have an invitation, follow the link and enter the invitation code.

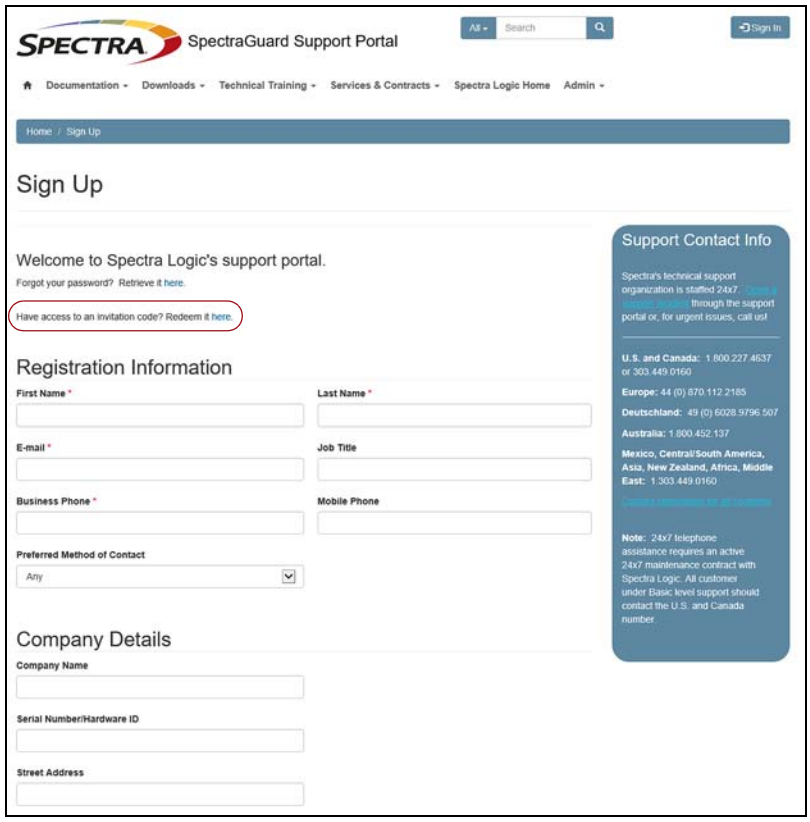


Figure 124 Follow the link to enter your invitation code or enter your registration information.

   - If you do not have an invitation, enter the requested information to create your account. When you are finished, click **Sign Up**.

When the account is approved, you receive an email with a link to setup your initial password. Use your email address and the password provided in the email to log in to your account. After you log in, you can change your password if desired.

Log Into the Portal

Access the Technical Support login page at support.spectralogic.com. Use your email address and password to log into the Technical Support Portal.

CONFIGURING AUTOMATED SOFTWARE UPLOAD

Automated Software Upload is a feature that allows the system to periodically check a specified server to determine if updated software is available for the system. The feature can also be used to automatically download the updated software package to the system.

Note: You must have a current software update key entered in the system you want to configure to use Automated Software Upload. See Manually Enter Activation Keys on page 127 for more information.

1. From the menu bar, select **Support ···⁘ Software.** The Software screen displays.
2. Select **Action ···⁘ Edit Automated Software Upload**. The Automated Software Upload dialog box displays.

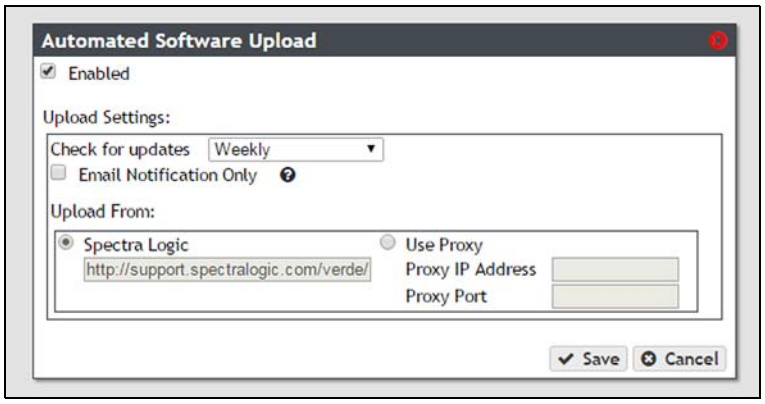


Figure 125 The Automated Software Upload dialog box.

3. Select the **Enabled** check box to enable the feature.
4. Use the drop-down menu to select the **Check for updates** frequency.
5. Optionally, select the **Email Notifications Only** check box to only receive an email when an updated software package is available instead of automatically downloading the file.
6. Select either **Spectra Logic** or **Use Proxy** as the **Upload From** location.

Important Spectra Logic recommends using the **Spectra Logic** package server.

If you select **Use Proxy**, enter the following information:

- **Proxy IP Address** — Enter a valid IPv4 address.
- **Proxy Port** — Enter the port used to access the proxy server.

7. Click **Save**.

UPDATING SOFTWARE

Some problems with the Verde NAS solution may be fixed by updating the system's software. Spectra Logic provides complete support for the most current release of software and one revision back. Customers using previously released software packages are asked to update to the current release as soon as possible.

Note: You must have a current software upgrade key entered in the system you want to update. See Manually Enter Activation Keys on page 127 for more information.

If Automated Software Upload is enabled, when a software update is available, the system sends an email to all users configured to receive Warning or Informational emails (see Configure Mail Recipients on page 148) and posts a system message to the Messages screen. If configured to do so, the system also downloads the updated software.

The method used to update the system depends on if the Automated Software Upload feature is enabled or not, and if enabled, whether it is configured to download the update software.

- If the update package downloaded automatically, skip to Install the Update on page 165.
- If you were notified that an update is required, but the update did not download automatically, skip to Download and Stage the Updated Software on page 163.
- If you do not know if the system needs an update installed, continue with Check the Current Software Version, below.

Check the Current Software Version

Use the following steps to determine the current software version running on your Verde master node.

1. From the menu bar, select **Support ⋯⁘ Software.** The Software screen displays.

2. The current software version is listed next to **Current Version** in the Software Update pane.

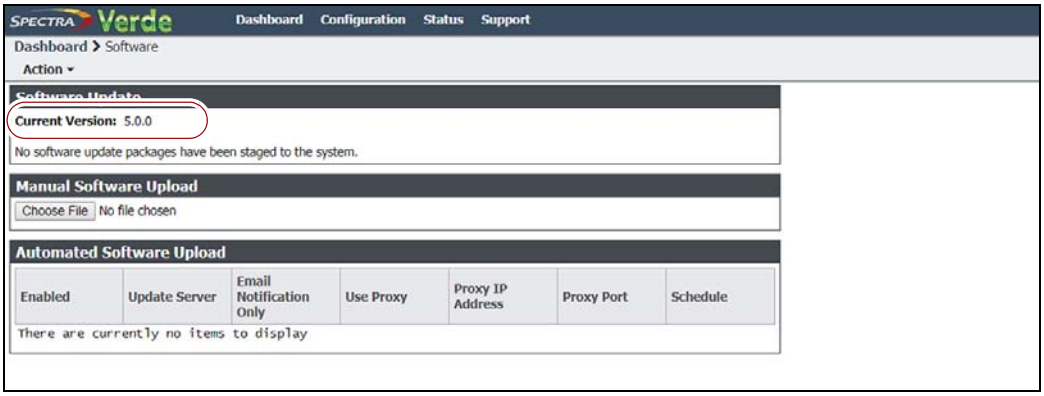


Figure 126 The current Verde software version.

3. Check the Currently Released Verde Software Version

Follow these steps to check the currently recommended Verde software version:

1. Log into your user account on the Technical Support portal at https://support.spectralogic.com.

   Note: See Create an Account on page 157 for information about creating an account and accessing the Technical Support portal.

2. Select **Downloads** ⋯⁘ **Product Software**.

3. On the Product Software page, locate the Verde NAS solution in the **Spectra Product** column. The currently released Verde version is listed in the **Current Version** column.

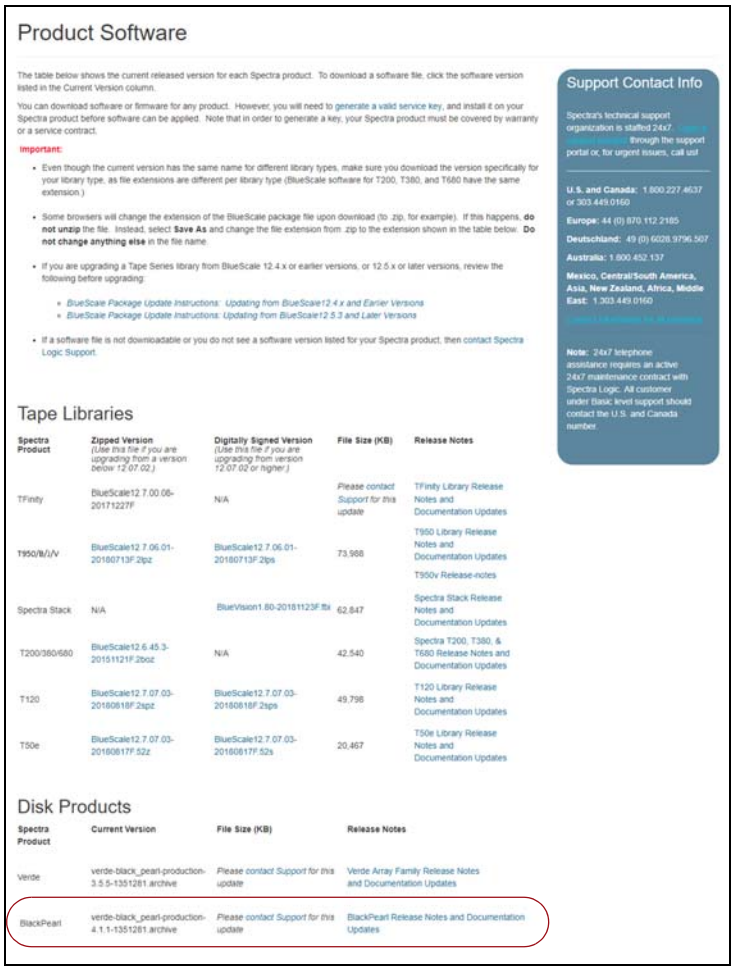


Figure 127 The Product Software screen.

4. Compare the Current Version available for the Verde NAS solution to the version installed on the system.

Download and Stage the Updated Software

Use the instructions in this section to download and install the updated software for the Verde NAS solution.

1. Log into your account on the Technical Support portal at https://support.spectralogic.com.

2. Select **Downloads ···⁘ Product Software**. The Product Software Screen displays.

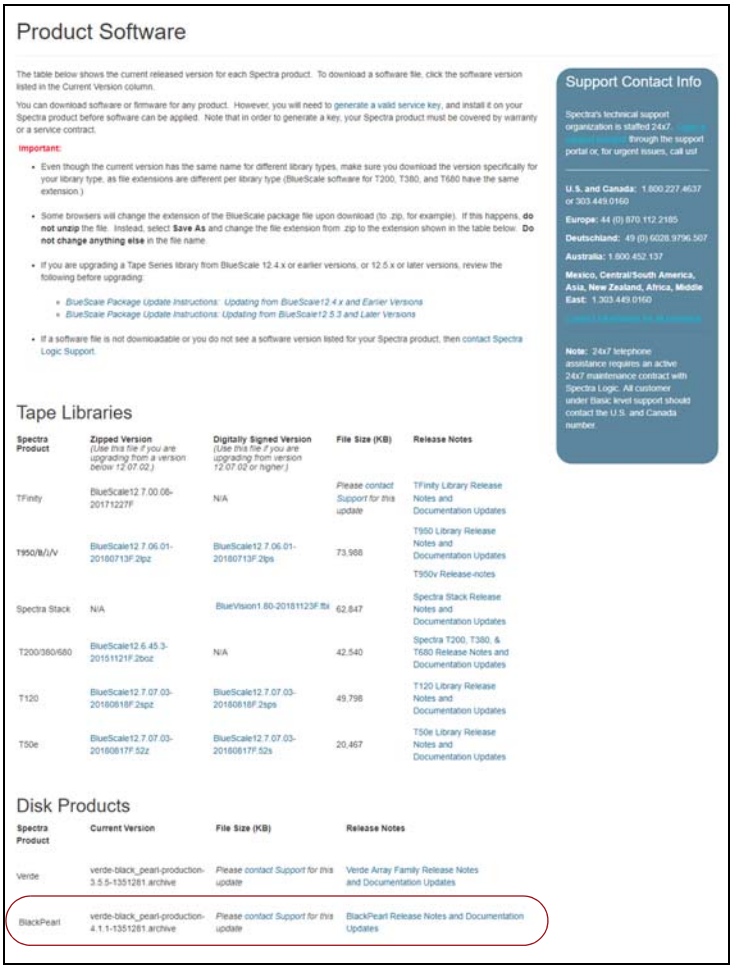


Figure 128 The Product Software screen.

3. Locate the Verde NAS solution row in the **Spectra Product** column. The currently released Verde software version is listed in the **Current Version** column.
4. Click the name of the Verde package. The package begins downloading through your web browser. Do not unzip the downloaded file.

5. From the menu bar, select **Support ···⁘ Software** to display the Software screen. Click **Choose File.** Using your web browser, browse to the location of the update file and select the file to upload. The file is staged to the system.

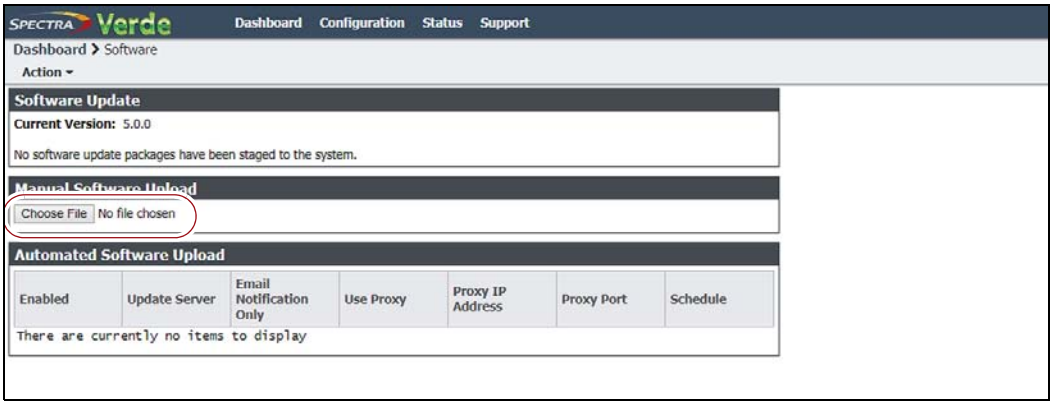


Figure 129 The Software Update screen with an available software package listed.

Install the Update

1. Discontinue all file storage operations on the Verde NAS solution. The system automatically reboots as part of the update process.
2. From the menu bar, select **Support ···⁘ Software** to display the Software screen. The Software screen displays with the software upload file staged to the system.

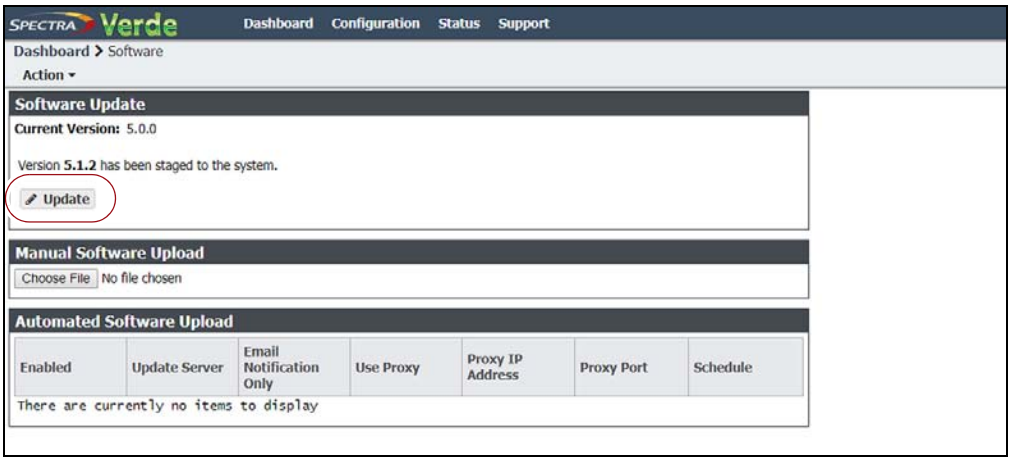


Figure 130 The Software Update screen with a software package staged to the system.

3. Click **Update**. A progress bar shows the progress of the update.

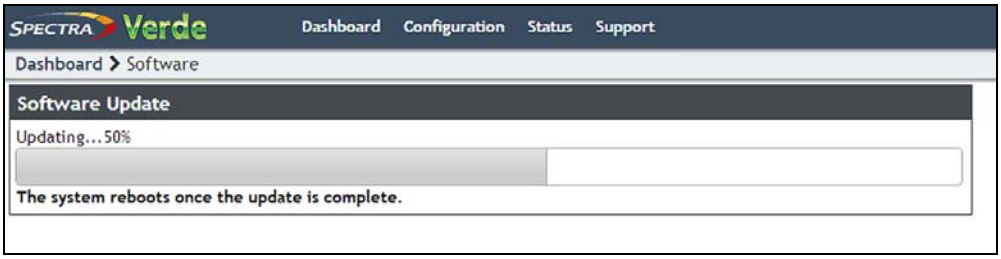


Figure 131 The Software Update screen showing the progress of an update.

4. When the update is complete, the Verde NAS solution automatically reboots to begin using the latest software.
5. Restart file storage operations.

INSTALLING A NEW DATA DRIVE

Use the following instructions to add new drives to a Verde NAS solution.

Ensure ESD Protection

The repair environment for the system must be free of conditions that could cause electrostatic discharge (ESD). To protect the system from ESD, follow these procedures when repairing or testing the system:

- Place a static protection mat on the work surface used while removing and installing system components. Use a 1-megohm resistor to ground the static protection mat.
- Wear a static protection wrist band or grounding foot strap whenever you handle system components that are removed from their anti-static bags. Connect the wrist band to the static protection mat or to other suitable ESD grounding.
- Keep all electronic components in anti-static bags when not in use.

Caution

Any damage to a Verde NAS solution caused by failure to protect it from electrostatic discharge (ESD) voids the Verde's warranty. To protect the drives from damage:

- Wear an anti-static wristband, properly grounded, throughout the procedure. If a wristband is not available, touch a known grounded surface, such as the unpainted metal chassis.
- Leave the drive in its anti-static bag until you are ready to install it.
- Do not place the un-bagged drive on any metal surfaces.

Install the Drive

The drives used in the Verde NAS solution are mounted on drive sleds that ensure proper data and electrical connection with the backplane inside the Verde NAS solution.

Remove the Front Bezel

If you are installing a new drive in the front of the system, you need to remove the front bezel prior to installing the drive. The bezel is held in place with magnets. Grasp the sides of the bezel and pull it straight off the system.

Remove the Empty Drive Sled

Use the following steps to remove an empty drive sled.

1. Put on an anti-static wristband and attach it to the anti-static mat or an unpainted metallic surface. Continue to wear the wristband throughout the entire replacement procedure.
2. Locate the empty drive bays where you want to install a new drive.

   Note: If your system includes an active bezel, do not install a drive in slot 1, which is the top left drive in the front of the system. This slot is reserved for the Visual Status Beacon control sled. The images below show a normal drive sled in slot 1 for clarity.
3. Slide the drive sled locking tab to the right to release the drive sled handle.

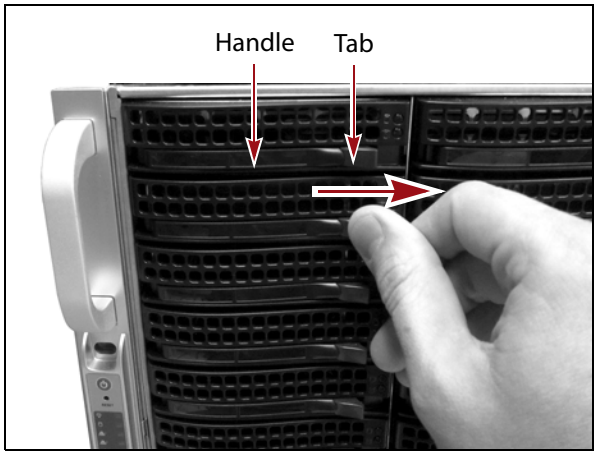


Figure 132 Slide the tab to the right to release the drive sled handle.

4. Grasp the handle and slide the sled completely out of the chassis. If the sled does not slide easily by pulling on the handle, grasp the sides of the sled and pull the sled out of the enclosure.

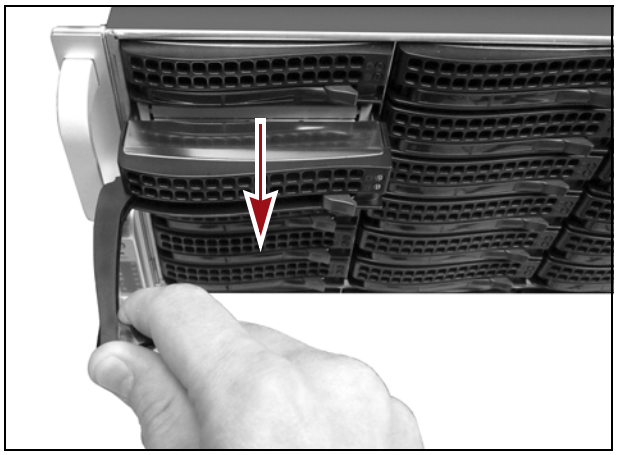


Figure 133 Pull the sled out of the system.

5. Dispose of the empty sled in accordance with your company's guidelines.

Install the New Drive

1. New drives are shipped installed in a drive sled. Slide the locking tab on the front of the drive sled to the right to release the handle.
2. With the drive handle in the open position, slide the drive sled into the chassis until the front of the drive sled is flush against the chassis. The drive sled slides in easily; do not force it.

Figure 134 Install the drive into the Verde system.

3. When the drive sled is in position, push the handle inward and to the right until the locking tab secures it in place. An audible click indicates that the drive sled is locked into position.
4. If necessary, reinstall the front bezel.

Replacing a Failed Component

If a component in a Verde NAS solution is not functioning properly, the system generates a message and the hardware icon on the status bar of the Verde user interface changes to an error icon (see Status Icons on page 37).

Identify the Failed Component

1. From the menu bar, select **Status ⋯⁘ Hardware**. The Hardware screen displays. The malfunctioning component is indicated by an error icon.

Figure 135 The Hardware screen showing a failed component.

2. If you have multiple Verde NAS solutions, you can use the beacon feature to help locate which system has the failed component. On the Hardware screen, click the system name. The screen refreshes to show the main Hardware screen

   Note: The front bezels in some Verde master nodes do not include a Visual Status Beacon light bar. However, when the beacon feature is activated, the drive lights blink blue, making it easier to locate the system with a failed component.

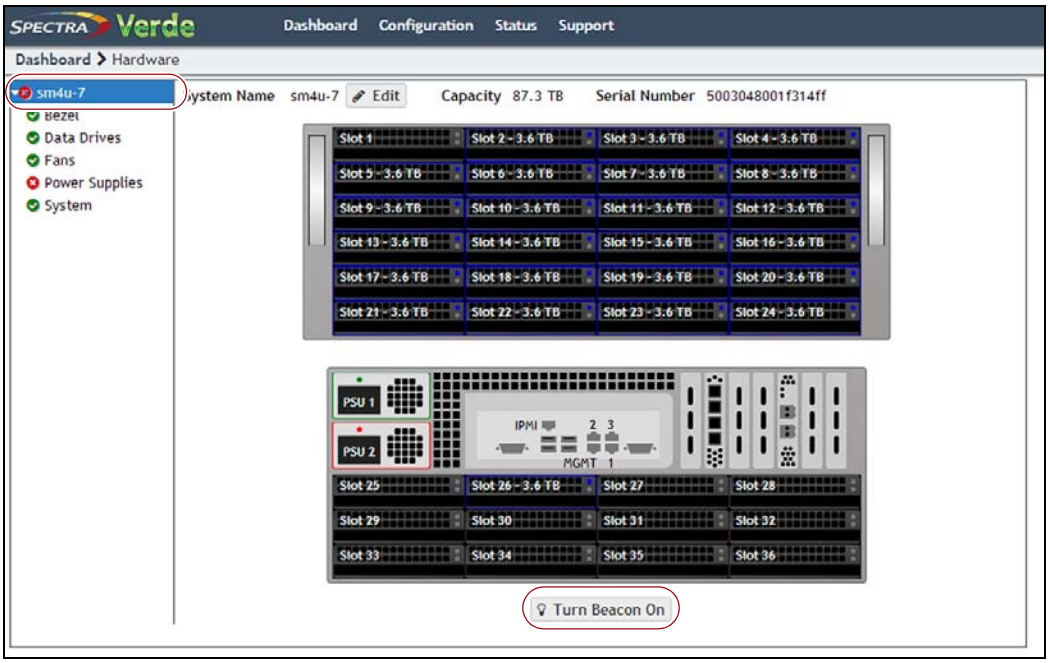


Figure 136 The Hardware screen.

3. Click **Turn Beacon On**. The Verde NAS solution Visual Status Beacon light bar flashes blue, making it easy to find.

   Note: After you locate the unit in your data center, click **Turn Beacon Off** to stop the lights from flashing.

4. For specific part replacement procedures, refer to one of the following guides, which can be found after logging into the Spectra Logic Support portal at: support.spectralogic.com.

- The *Spectra 12- & 36-Drive Chassis Boot Drive Replacement Guide* provides instructions for replacing a failed boot drive in the system.
- The *Spectra 12-, 36- & 45-Drive Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive after the system is installed.
- The *Spectra 12-, 36- & 45-Drive Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in the system.
- The *Spectra 12-, 36- & 45-Drive Chassis Power Supply Replacement Guide* provides instructions for replacing a failed power supply after the system is installed.
- The *Spectra 12-Drive Chassis HBA Replacement Guide* and *Spectra 36-Drive Chassis HBA Replacement Guide* provide instructions for replacing a failed HBA in the system.
- The *Spectra 96-Drive Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive in the Verde archive expansion node.
- The *Spectra 96-Drive Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in the Verde archive expansion node.
- The *Spectra 96-Drive Chassis Power Supply Replacement Guide* provides instructions for replacing a failed power supply in the Verde archive expansion node.
- The *Spectra 96-Drive Chassis I/O Module Replacement Guide* provides instructions for replacing a failed I/O module in the Verde archive expansion node.

CHAPTER 9

Troubleshooting and Support

Use the information in this chapter to troubleshoot problems as they arise, before contacting Spectra Logic Technical Support.

Task	
Resolving a Management Port IP Address Conflict	page 173
Using the Console	page 173
Using a Separate Computer	page 173
Network Setup Tips	page 175
Configuration	page 175
Connectivity to the Network	page 175
Troubleshooting	page 178
Tools	page 178
Spectra Logic Technical Support	page 179
Before Contacting Support	page 179
Open a Support Ticket	page 180
Remote Support	page 183
Enable Remote Support	page 184
Disable Remote Support	page 185

Resolving a Management Port IP Address Conflict

The default address of the Verde management port is set to **10.0.0.2** with a netmask of **255.255.255.0**. If your network is already using this IP address, you are not able to access the Verde user interface.

One resolution to the issue is to change the IP address of the machine already on your network to a different address. Then connect to the Verde master node as described in Log In to the Verde User Interface on page 44. If you cannot, or do not want to change the IP address of the existing machine, follow the instructions in this section to connect your Verde master node to your network.

Using the Console

Using the Verde master node console is the recommended way to change the Verde management port IP address. For instructions on using the console to configure the management port IP address, see Configure the Verde Management Port on page 42.

Using a Separate Computer

If you cannot use the console, use a computer or laptop disconnected from any existing network, to change the Verde management port IP address.

1. Gather a laptop or desktop computer not currently on any network. Disable any wireless networking, if necessary.
2. Using a standard Ethernet cable, connect the Ethernet port on the computer to the Verde management port on the Verde master node. See Software on page 33 to locate the management port.
3. Open a web browser on the computer. For a list of compatible browsers, see Supported Browsers on page 37.
4. Enter the IP address below in the browser address bar:

   ```
   https://10.0.0.2
   ```

   Notes:
   - The netmask for the default IP address is 255.255.255.0.
   - The Verde user interface uses a secure connection.
5. Resolve the security certificate warning for the Verde user interface. The warning displays because the Verde NAS solution does not have a security certificate.

   Notes:
   - Consult your browser documentation for instructions on how to resolve the security certificate warning.
   - The absence of the certificate does not affect functionality.

6. Enter the login username and password.

   The default username is **Administrator** and password is **spectra**.

7. From the menu bar, select **Configuration ···⁘ Network**, or click the Network pane from the Dashboard screen. The Network screen displays.

8. In the Network Interfaces pane, double-click the Management row, or select the Management row and then select **Action ···⁘ Edit**. The Edit Management dialog box displays.

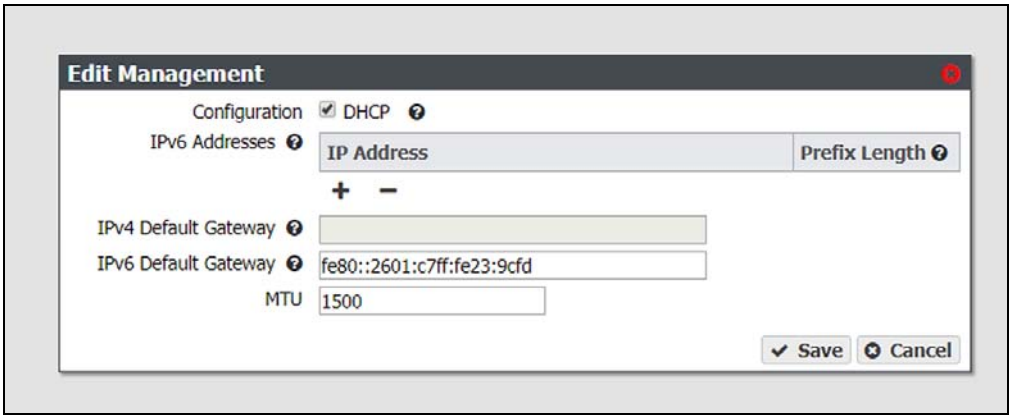


Figure 137 The Edit Management dialog box.

9. Select **DHCP** to configure the system to automatically acquire an IPv4 address using DHCP. This setting does not apply to IPv6.

Important If you select DHCP, you are not able to see the IP address assigned by DHCP before you are logged out of the Verde user interface. Contact your system administrator to determine the DHCP address for the management port.

10. To configure a static IP address, click the **+** button and enter the following information:

    - **IP Address** — Enter a valid IPv4 or IPv6 address.

      Note: You cannot enter an IPv4 address if you selected DHCP in Step 9.

    - **Prefix Length** — Enter the subnet mask.

      Note: If desired, you can enter **Aliases**, multiple IP and prefix lengths assigned to the data port. Use the **+** button to configure additional IP and Netmask addresses. You can configure a maximum of 16 aliases.

11. Enter the **IPv4 Default Gateway**.

    Note: If you selected DHCP in Step 9, this option is unavailable.

12. Enter the **IPv6 Default Gateway**.

13. Change the **MTU** value, if desired. If you set the MTU value to something other than 1500, ensure that your switch configuration supports larger MTU settings, as well as all the hosts on the network.

14. Click **Save**.

    Note: When you change the IP address of the Verde management port, you lose your connection to the user interface when you save your changes. To re-establish the connection, enter the new IP address in your browser and log in again.

15. Disconnect the Ethernet cable from the Verde management port.

16. Connect a cable from your network to the management port on the Verde master node. You are now able to connect to the system with the IP address configured in Step 9 on page 174.

NETWORK SETUP TIPS

The Verde management port is separated from the data ports. The management port and data ports have their own default routes. This does not prevent a user from having the management and data ports utilizing the same network, if desired.

The basic steps for configuring the management and data ports for access to the network are simple and straight-forward. However, each network environment is unique and may require some additional troubleshooting in order to properly connect to the Verde NAS solution and utilize the 10GBase-T, 10 GigE, or 40 GigE interfaces correctly.

Configuration

The first step is to configure the management and data ports using the Verde user interface (see Configure Network Connections and Settings on page 101), or the command line interface (see the *Spectra Verde Nas Solution Command Line Interface Guide)*. Do not attempt to access the system directly using the root console and modify interfaces. The user interface and command line interface are tightly integrated with the base operating system and configure additional features based on network changes.

Connectivity to the Network

The following configurations are supported for the data path:

Recommended:

- **For the 10 GigE optical card:**
  - Single 10 GigE logical connection using one of the 10 GigE physical ports

  —OR—

  - Single 20 GigE logical connection using two 10 GigE physical ports (link aggregation)

- **For the 40 GigE optical card:**
  - Single 40 GigE logical connection using one of the 40 GigE physical ports

  —OR—

  - Single 80 GigE logical connection using two 40 GigE physical ports (link aggregation)
- **For the 10GBase-T card:**
  - Single 20 gigabit logical connection using two 10GBase-T physical ports (link aggregation)

  —OR—

  - Single 30 gigabit logical connection using three 10GBase-T physical ports (the two ports on the card and the one spare onboard port) (link aggregation)

Not Recommended:

- Single gigabit logical connection utilizing one of the 10GBase-T physical ports and a Category 5e Ethernet cable

  —OR—

- Single 10 gigabit logical connection utilizing one of the 10GBase-T physical ports and a Category 6 Ethernet cable

Assign the appropriate IP address to the management and data ports either statically or using DHCP. If you are setting the MTU to something other than 1500, ensure that your switch configuration, as well as all the hosts on the network, support larger MTU settings. The Verde master node can support jumbo frames (MTU=9000), but all switches and hosts on the network must be configured to support jumbo frames if this is selected, or performance might be degraded.

Link Aggregation Notes

Switches use different methods of routing traffic from hosts to NAS servers. There are also many different network configurations to move data from hosts to NAS servers. For example, some Cisco switches route traffic based on the MAC address and the IP address. The Verde NAS solution presents only one MAC address and one IP address when the data ports are aggregated via DHCP. If static link aggregation is chosen, the Verde NAS solution presents only one MAC address, but can have up to 16 IP addresses aliased to the MAC address. It is up to the switch to rotate data transfers among the physical ports on the Verde NAS solution in order to achieve the highest throughput possible.

For example, if only a single host is connected to the Verde NAS solution through a link aggregated connection, the measured performance is lower than the potential maximum transfer rate because only one physical port of the three port link aggregation is being utilized by the switch. If a single share is mounted three times using different IP addresses and transfers are started to that share from three separate hosts, the resulting throughput would be approximately three times that of a single host connection. You may need to configure more than three IP addresses on the Verde NAS solution to force the switch hashing algorithm to utilize all physical ports and maximize performance.

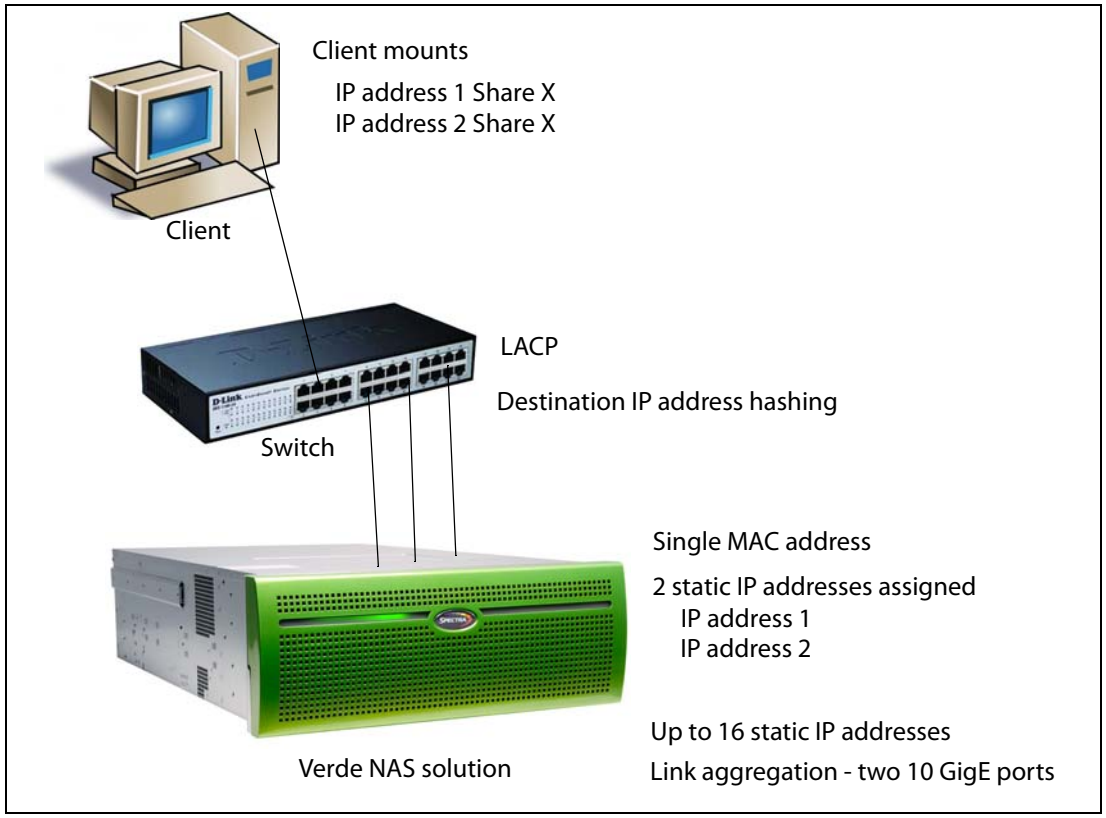


Figure 138 Connection example utilizing two IP addresses assigned to a single share.

Additionally, if link aggregation is configured for the Verde master node, then switches must also be able to support link aggregation to aggregate or "trunk" the data ports together to provide higher bandwidth into the Verde NAS solution. Switches must support link aggregation using Level 3 LACP (Link Aggregation Control Protocol), and the switches must hash the destination IP addresses. Manually configure LACP on the switch ports. LACP does not get enabled automatically.

Once configured correctly and attached to the network, the status in the user interface indicates the speed of the connection and whether the port is active. The link lights on the network ports should be on and active at both the Verde master node and the network switch.

From your network, use the "ping" command (see Ping below) to test the assigned IP address for the Verde management port or data port. If this is not successful, use the following troubleshooting tips to ascertain if the problem is a network setup issue.

Troubleshooting

Port Link LED Does Not Light

- Check the port configuration on the network switch. The Verde master node only supports auto-negotiation. Make sure the switch is configured to match speeds on both ends of the connection.
- Check the cables that connect the port to the other device. Make sure that they are connected. Verify that you are using the correct cable type and connectors. This is especially critical for 10 GigE and 40 GigE connections utilizing SFPs.
- Verify that the switch ports are not administratively disabled. Consult the switch *User Guide* for more information.

Port Link LED is Lit, But I Cannot Ping the Verde NAS Solution

- Check the LACP settings on the switch. If you are using link aggregation on the Verde NAS solution, the switch MUST be configured to use LACP on those ports. If you are not using link aggregation, the switch must be configured NOT to use LACP on those ports.
- Check the VLAN (Virtual Local Area Network) settings on the switch. Ensure that the ports are assigned to the correct VLAN.

Tools

Ping

The ping command is a simple tool, based on a request-response mechanism, to verify connectivity to a remote network node. The ping command is based on ICMP (Internet Control Message Protocol). The request is an ICMP Echo request packet and the reply is an ICMP Echo Reply. Like a regular IP packet, an ICMP packet is forwarded, based on the intermediate routers' routing table, until it reaches the destination. After it reaches the destination, the ICMP Echo Reply packet is generated and returned to the originating node.

For example, to verify the connectivity from the switch to the IP address 192.168.2.10, run the command shown below from the switch command line or client:

```
ping 192.168.2.10
```

All ICMP Echo requests should receive replies including information about the round trip time it took to receive the response. A response of 0 msec means that the time was less than 1 ms. If the request times out, then check the settings on the switch to which the Verde master node is connected.

Traceroute

You can use the traceroute command, if it is available, or something similar to not only verify connectivity to a remote network node, but to track the responses from intermediate nodes as well. The traceroute command sends a UDP packet to a port that is likely to not be used on a remote node with a TTL of 1. After the packet reaches the intermediate router, the TTL is decremented, and the ICMP time-exceeded message is sent back to the originating node, which increments the TTL to 2, and the process repeats. After the UDP packet reaches a destination host, an ICMP port-unreachable message is sent back to the sender. This action provides the sender with information about all intermediate routers on the way to the destination.

For example, in the output of the command shown below,

```
traceroute 192.168.2.10
```

displays a numbered list indicating how many hops, on the way from the switch to the Verde master node, are encountered when tracing the packet.

SPECTRA LOGIC TECHNICAL SUPPORT

Spectra Logic Technical Support provides a worldwide service and maintenance structure.

Before Contacting Support

If you have a problem with your Verde NAS solution, use the information in this section to attempt to resolve the problem.

System Messages If you are encountering problems, review any System Messages that were posted (see View System Messages on page 134) and take any action described in the message(s).

Product Support The Spectra Logic Technical Support portal at support.spectralogic.com provides information about the most current version of the Verde software, and additional service and support tools. After logging into the support portal, check the options under the **Support by Product** and **Knowledge Base** tabs for additional troubleshooting information.

Contact Support If the problem persists, open a support ticket (see Open a Support Ticket on page 180).

Determine the System Serial Number

If you have more than one Verde NAS solution, it is necessary to determine the serial number of the system before contacting Spectra Logic Technical Support. Use the following steps to determine the system serial number.

1. From the menu bar, select **Support ⋯ Contact Information.** The Contact Information screen displays.
2. The system serial number is listed in the Product Information pane.

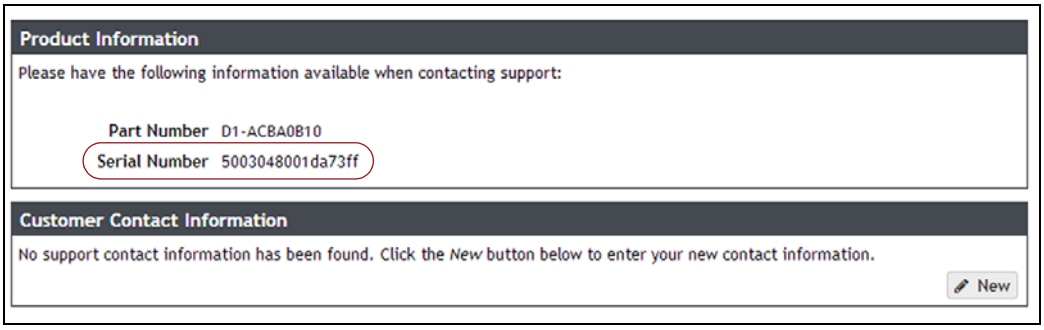


Figure 139 The system serial number.

Open a Support Ticket

You can open a support ticket using the Spectra Logic Technical Support portal or telephone.

1. Make notes about the problem, including what happened just before the problem occurred.
2. Gather the following information:
   - The system serial number (see Determine the System Serial Number on page 180)
   - Company name, contact name, phone number, and email address
   - Type of host system being used
   - Type and version of host operating system being used
   - Type and version of host file storage software being used

3. Submit a support incident.
   - To use the Spectra Logic Technical Support portal:
     a. Log into your account on the Technical Support portal at support.spectralogic.com.

     Note: See Create an Account on page 134 if you did not previously create an account on the Technical Support portal.

     b. Select **Incidents & Inventory ···⁘ Open or View Incidents,** or on the Home page, click **Open a Support Incident**.

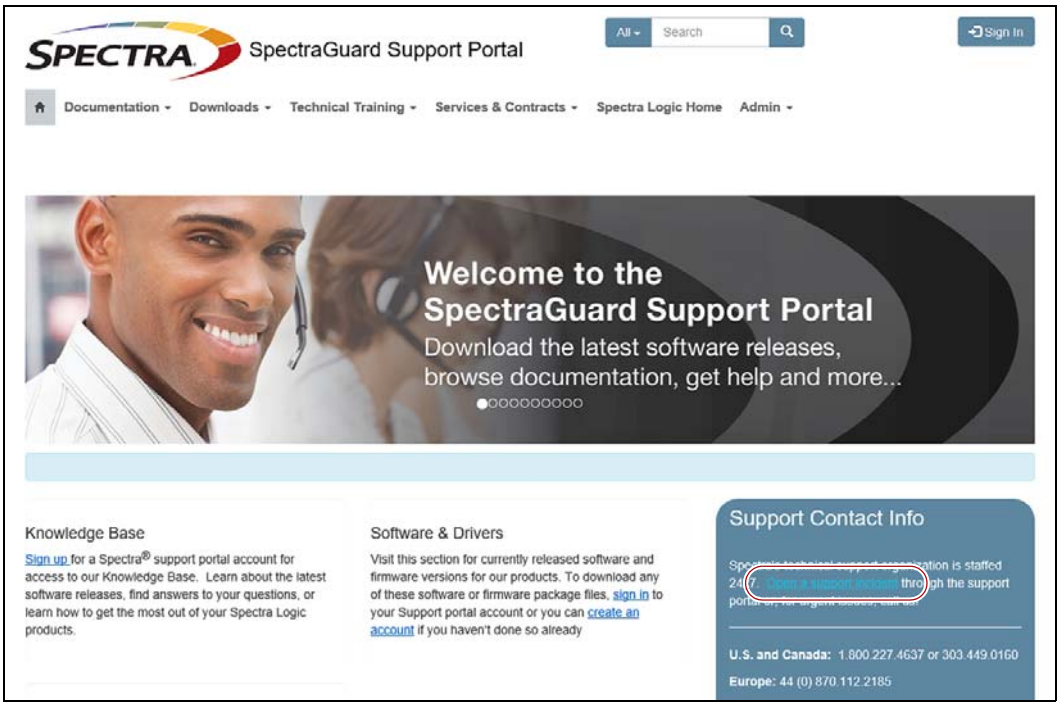


Figure 140 Select **Incidents & Inventory ···⁘ Open or View Incidents** to open a support incident.

c. On the Open or View Incidents page, you are given an opportunity to search for existing support content that may help you solve your problem immediately. If the search does not provide an answer, click **Open a New Incident**.

Note: You must perform a search before you are able to open a new support incident.

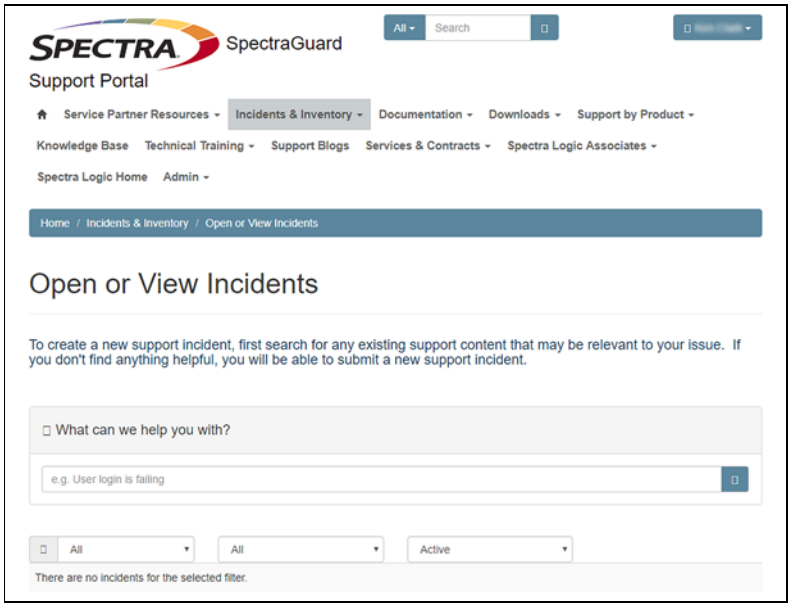


Figure 141 The Open or View Incidents page.

d. On the Create Incident page, enter the requested information providing as much detail as possible. When you are finished, click **Create Incident**.

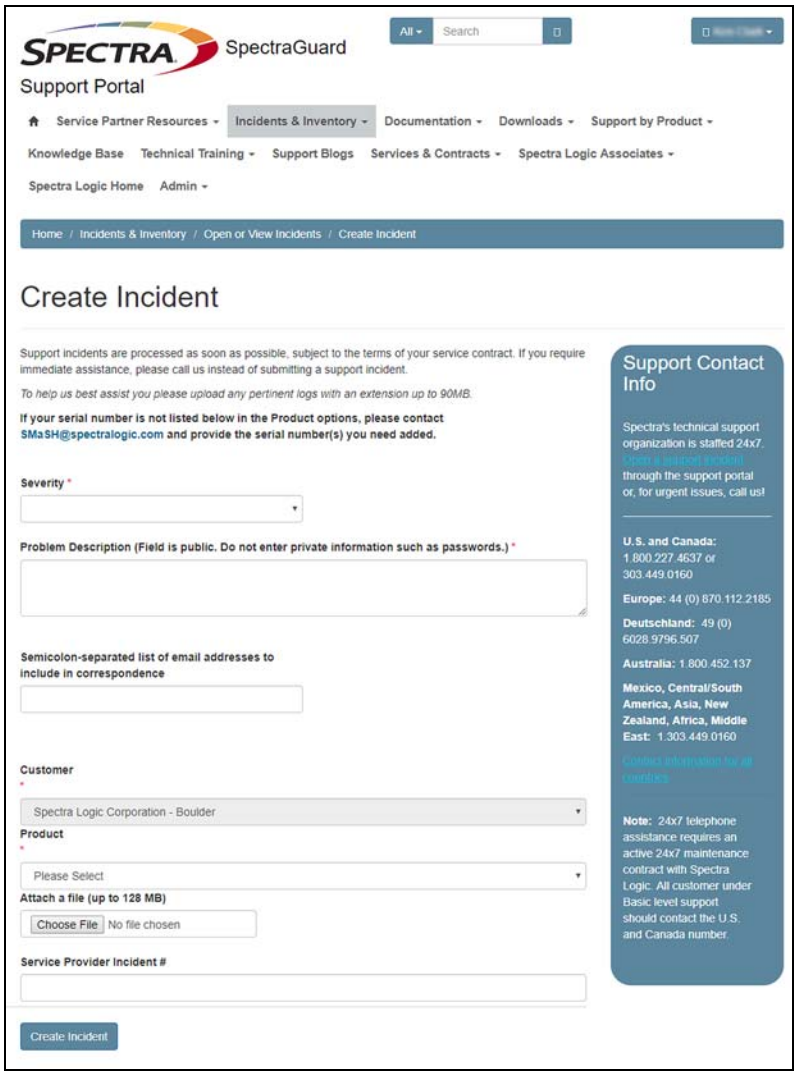


Figure 142 The Create Incident page.

- If it is within the hours of coverage provided by your support contract, you can also contact Spectra Logic Technical Support by telephone. See Contacting Spectra Logic on page 7.

REMOTE SUPPORT

Remote Support is an option that allows Spectra Logic Technical Support personnel to access the root console of the system. This option is for troubleshooting purposes only.

Enable Remote Support

1. Enter the Remote Support activation key as described in Manually Enter Activation Keys on page 127.
2. From the menu bar, select **Configuration ···⁝ Users**. The Users screen displays a list of all users configured on the system.
3. Double-click the **Administrator** account, or select the **Administrator** account, and then select **Action ···⁝ Edit**. The Edit User dialog box appears.

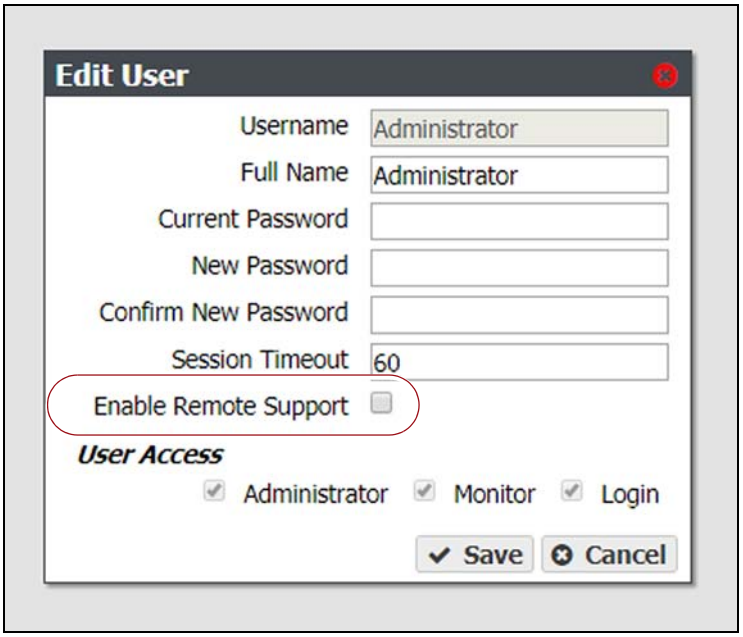


Figure 143 The Edit User dialog box.

4. Select the **Enable Remote Support** check box.

   Note: The Enable Remote Support check box does not display until you enter a Remote Support activation key.

5. Click **Save**.

Important After Spectra Logic Technical Support informs you that they no longer require root access to the system, you should disable Remote Support to prevent any potential unauthorized access to your system. See Disable Remote Support on page 185 for more information.

Disable Remote Support

Use the instruction in this section to disable Remote Support.

1. From the menu bar, select **Configuration ⋯⁘ Users**. The Users screen displays a list of all users configured on the system.
2. Double-click the **Administrator** account in the Primary Administrators pane, or select the **Administrator** account, and then select **Action ⋯⁘ Edit**. The Edit User dialog box appears.

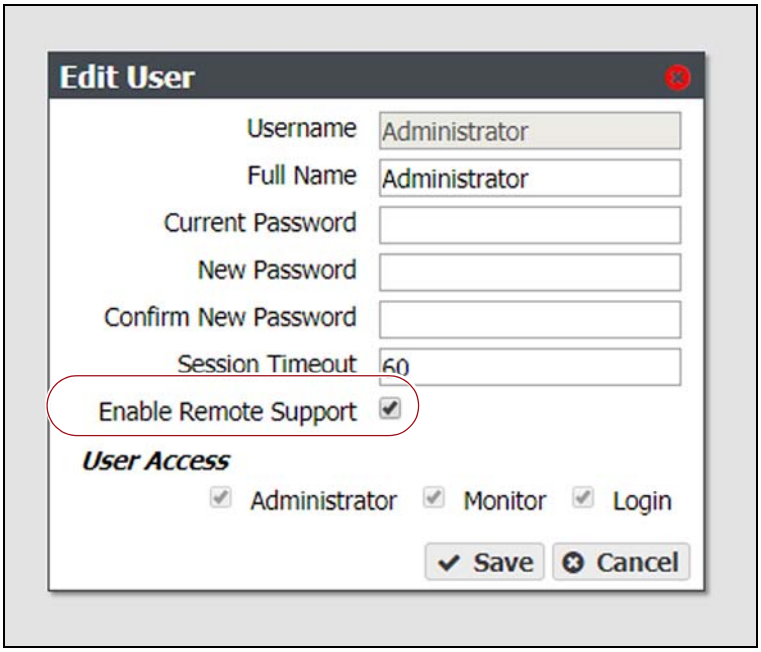


Figure 144 The Edit User dialog box.

3. Clear the **Enable Remote Support** check box.
4. Click **Save**.

APPENDIX A

Network File Interface

OVERVIEW

The Network File Interface (NFI) service allows you to automatically move data from your Verde NAS solution to one or more BlackPearl Converged Storage systems, without the need to use a Spectra S3 client. Data is transferred on a schedule and data copied from the Verde NAS solution to the system can be configured to be kept on the NAS solution or deleted.

When a user needs access to data deleted from the Verde NAS solution, they can use the Spectra Eon Browser or an API client to retrieve the files from the BlackPearl system.

Note: Beginning with Verde 3.1.4, objects sent to a BlackPearl system using the NFI service include ACL (Access Control List) metadata, such as file permissions, ownership, and groups. When the objects are retrieved, the API client needs to reconstruct the ACL metadata.

REQUIREMENTS

The Network File Interface service has the following requirements:

- Files being stored as objects to a BlackPearl Converged Storage system must follow the Amazon S3 naming restrictions. See http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html for more information.
- If the target BlackPearl system is running software version 3.0 or later, then the system has Advanced Bucket Management (ABM) capabilities. When using an ABM-enabled system with NFI, you must first configure buckets on the BlackPearl system, and configure data policies for the user using NFI to transfer data to the system. See the *Spectra BlackPearl User Guide* for instructions on creating buckets and configuring data policies.

  Note: If your NAS solution is running Verde software version 3.5.3, or later, all BlackPearl NFI targets must use BlackPearl 3.3.0, or later.

- If you plan to modify files on the Verde NAS share configured for NFI replication, you must configure the BlackPearl system as described in Configure a BlackPearl System for Versioning on page 188. If you do not plan to modify files on the Verde share, skip to Configure Network File Interface on page 191.
- If the target BlackPearl system is configured to transfer data to tape, make sure the tape library does not contain WORM (Write Once-Read Many) media. The BlackPearl system is not compatible with WORM media.

Special Considerations for Reading Tapes in a Non-BlackPearl Environment

Tape libraries associated with a BlackPearl system store data on LTO-5 or later generation tape media using the LTFS format. If you plan to eject tapes and read them in a non-BlackPearl system, you must follow the guidelines below when configuring your storage domains and data policies.

- The LTFS file name option must be set to **Object Name** when configuring a storage domain. This setting configures LTFS file names to use the format {*bucket name*}/{*object name*}, for example bucket1/video1.mov. If the tapes are ejected from the BlackPearl system and loaded into a non-BlackPearl system, the file names match the object names. If you do not configure this option, object names are assigned a UUID string, which is not human readable.
- Object names must comply with LTFS file naming rules:
  - The colon character (:) is not allowed in LTFS file names and therefore not allowed in BlackPearl object names. The slash character (/) is also technically not allowed in LTFS file names; however, the BlackPearl software can accommodate a slash in the object name and translates it as a directory in the LTFS file system (for example, directory1/directory2/video1.mov).
  - Directory names have a limit of 255 characters.
  - File names have a variable character limit. If you are using English ASCII characters, the limit is 1024 characters. If you are using a graphical language, such as Japanese, the limit is 512 characters.
  - Spectra Logic does not recommend the following characters in LTFS file names or BlackPearl object names for reasons of cross-platform compatibility: control characters such as carriage return (CR) and line feed (LF), double quotation mark (“), asterisk (*), question mark (?), less than sign (<), greater than sign (>), backslash (\), forward slash (/) vertical line (|).

- **Blobbing Enabled** should be cleared when configuring a data policy. Blobbing allows an object larger than 1 TB to be broken into multiple blobs and then stored on multiple tapes. Tapes created with blobbing disabled are always readable by a non-BlackPearl system; tapes created with blobbing enabled may not be readable by a non-BlackPearl system. With blobbing disabled, all files must have a size of 1 TB or less.
- The **Keep Latest** setting cannot be used for a data policy which uses a storage domain configured with the **LTFS File Name** option set to **Object Name**.

If you plan to eject tapes, Spectra Logic recommends the following storage domain and data policy settings:

- Set the Write Optimization setting to **Capacity** when configuring a storage domain so that data is written to as few tapes as possible.
- Enable **Bucket Isolation** when configuring a data policy. This setting configures the bucket to have its own unique set of tapes. This ensures that tape media containing one bucket of information is not mixed with another bucket, making it easier to eject a bucket.

CONFIGURE A BLACKPEARL SYSTEM FOR VERSIONING

If you plan to modify files on the Verde NAS share that is configured for NFI replication, you must configure the BlackPearl system with a storage domain and data policy that allow versioning as described in this section. If you do not plan to modify files on the Verde share, skip to Configure Network File Interface on page 191.

Once you create the required storage domain and data policy, you can then either:

- Create a bucket using the required data policy and specify that bucket when configuring the NFI service.
- Create a user and specify the required data policy as the default data policy. Then when the NFI service creates a bucket specifying that user as the owner, the bucket is created using the required data policy.

Use the instructions below to create a storage domain and data policy that allow versioning.

1. If you have not done so already, follow the instructions in the "Initial Configuration" chapter of the *Spectra BlackPearl User Guide*.

   Note: You may find it helpful to read the information in the "Understanding Spectra Advanced Bucket Management Concepts" chapter of the *Spectra BlackPearl User Guide*.

2. Log into the BlackPearl user interface as described in the *Spectra BlackPearl User Guide*.

3. From the menu bar, select **Configuration ···⁘ Advanced Bucket Management ···⁘ Storage & Policy Management**. The Advanced Bucket Management screen displays.
4. If necessary, configure disk and tape partitions on the system as described in the *Spectra BlackPearl User Guide*.
5. Select **Action ···⁘ New Storage Domain**. The New Storage Domain dialog box displays.
   a. Configure the storage domain as desired. See the *Spectra BlackPearl User Guide* for instructions.
   b. For the **LTFS File Naming** option, you must select **Object ID**.
   c. After you finish configuring the storage domain, click **Create**.
6. Select **Action ···⁘ New Data Policy**. The New Data Policy dialog box displays.
   a. Configure the data policy as desired. See the *Spectra BlackPearl User Guide* for instructions.
   b. For the **Versioning** option, you must select **Keep Latest**.
   c. After you finish configuring the data policy, click **Create**.
7. Add a data persistence rule.
   a. Double-click the data policy in the Data Policies pane, or select the data policy and select **Action ···⁘ Show Details** from the menu bar.
   b. Select **Action ···⁘ New Data Persistence Rule**. The New Data Persistence Rule dialog box displays.
   c. Use the **Storage Domain** drop-down menu to select the storage domain you created in Step 5, above.
   d. Configure the data persistence rule as desired. See the *Spectra BlackPearl User Guide* for instructions.
   e. Click **Create**. The new data persistence rule displays on the Data Policy details screen.
8. Once you create the data policy, you must either create bucket(s) using that data policy, or create a new user with the data policy you created selected as the default for that user. Chose the corresponding instructions below:
   - Create a Bucket Using the Required Data Policy below

     -OR-

   - Create a User Using the Required Data Policy on page 190

Create a Bucket Using the Required Data Policy

Use the instructions in this section to create bucket(s) on the BlackPearl system that allow versioning.

1. In the BlackPearl user interface, select **Configuration ···⁘ Buckets**. The Buckets screen displays.
2. From the menu bar, select **Action ···⁘ New Bucket**. The New Bucket dialog box displays.
   a. Configure the bucket as desired. See the *Spectra BlackPearl User Guide* for instructions.
   b. Using the **Data Policy** drop down menu, select the data policy you created in Step 6 on page 189.
3. Click **Create**. The bucket is now listed on the Buckets screen.

   Notes:
   - You must enter the name of the bucket you just created when configuring a volume to use NFI replication.
   - You need to create a bucket for each volume you plan to configure for NFI replication.
4. Continue to Configure Network File Interface below.

Create a User Using the Required Data Policy

Use the instructions in this section to create a user on the BlackPearl system with a default data policy that allows versioning.

1. In the BlackPearl user interface, select **Configuration ···⁘ Users**. The Users screen displays.
2. From the menu bar, select **Action ···⁘ New**. The New User dialog box displays.
   a. Configure the user as desired. See the *Spectra BlackPearl User Guide* for instructions.
   b. Using the **Default Data Policy** drop down menu, select the data policy you created in Step 6 on page 189.
3. Click **Create**. The new user displays on the Users Screen.

   Note: You must enter the name and S3 credentials for this user when configuring the NFI service so that buckets created for this user use the specified default data policy.
4. Continue to Configure Network File Interface below.

CONFIGURE NETWORK FILE INTERFACE

After completing the steps in Chapter 2 – Initial Configuration on page 38, and, if necessary, configuring the BlackPearl system for versioning as described in Configure a BlackPearl System for Versioning on page 188, use the instructions in the following sections to configure the Verde NAS solution to use the Network File Interface service.

Configure the NFI Service

1. From the menu bar, select **Configuration ···⁘ Services** to display the Services screen.
2. Double-click the NFI service, or select the service, and then select **Action ···⁘ Show Details**. The details screen for the NFI service displays.

Figure 145 The NFI service details screen.

3. Select **Action ···⁘ Configure**. The Configure dialog box displays.

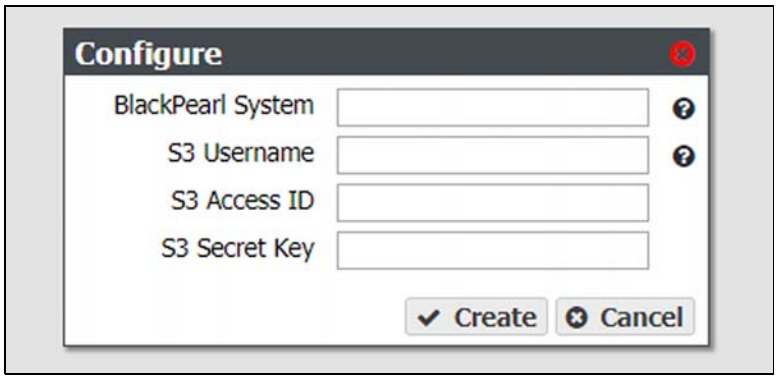


Figure 146 The Configure New BlackPearl System dialog box.

4. Enter the IP address or the DNS name of the data port of the BlackPearl system to which you want to connect in the **BlackPearl System** entry field. If you enter an IP address, it must be a valid IPv4 address. If you do not know the IP address or DNS name of the BlackPearl system, consult the *Spectra BlackPearl User Guide* for instructions.
5. Enter a value for the **S3 Username**. The S3 Username helps you identify the user credentials provided for the BlackPearl system.

6. Enter the S3 security credentials of a user previously created on the BlackPearl system in the **S3 Access ID** and **S3 Secret Key** fields. If you have not created a user in the BlackPearl user interface, or do not know the security credentials for that user, consult the *Spectra BlackPearl User Guide* for instructions.

   Notes:
   - If you plan to modify files on the Verde NAS shares and you created a data policy and assigned it to a user as described in Configure a BlackPearl System for Versioning on page 188, you must enter the username and S3 credentials for that user so that buckets created by the NFI service use the correct data policy.
   - If you plan to modify files on the Verde NAS shares and you previously created buckets with the data policy created in Configure a BlackPearl System for Versioning on page 188, you can choose any S3 user to enter here.
   - If you do not plan to modify files on the Verde NAS shares, you can choose any S3 user with access to the buckets to enter here.

7. Click **Create**.

8. If desired, repeat Step 3 on page 191 through Step 7 to configure additional BlackPearl systems.

Configure a Volume

Once the NFI service is configured to communicate with your BlackPearl system, create a volume to copy data to the BlackPearl system.

Note: Before you can create a volume, you must first create a storage pool. See Create a New Storage Pool on page 49, if necessary.

Important The combined length of the names of both the storage pool and volume used for NFI cannot exceed 52 bytes, or the NFI job fails. Most English characters are 1 byte.

1. From the menu bar, select **Configuration ···› NAS ···› Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays.

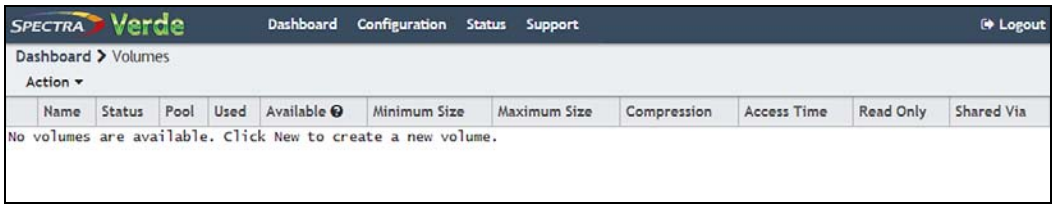


Figure 147 The Volumes screen.

   - Double-click the volume you want to edit, or select the volume and then select **Action ···› Edit**. The Edit *volume name* dialog box displays

   —OR—

- Select **Action ⋯⁘ New**. The New Volume dialog box displays.

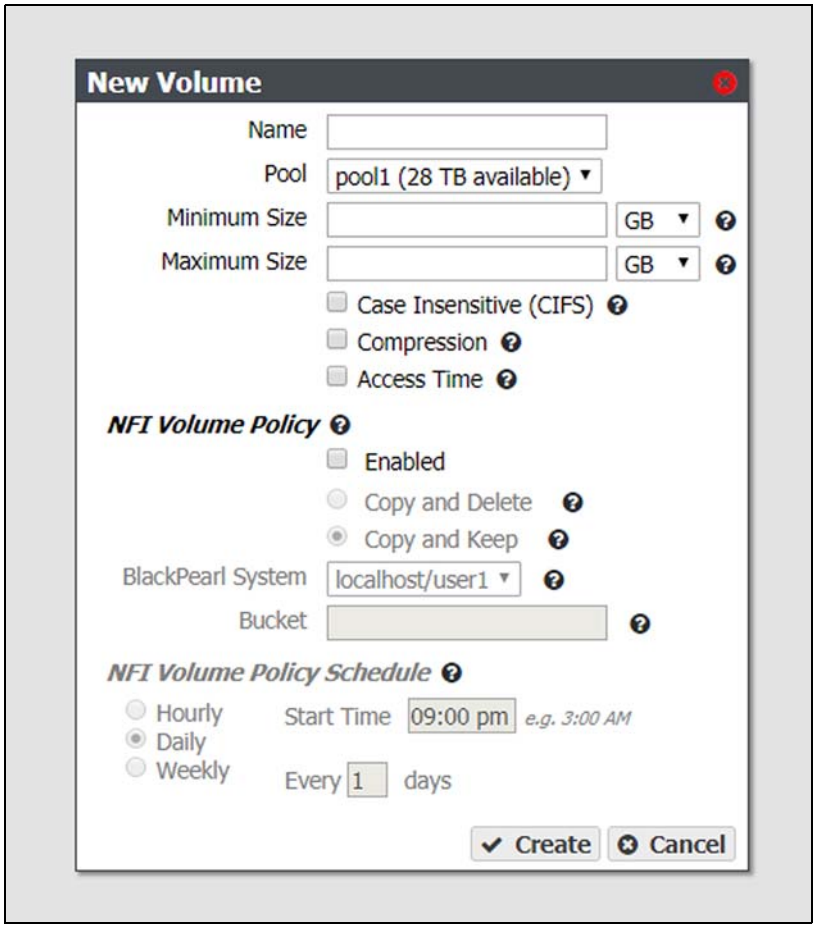


Figure 148 The New Volume dialog box.

2. Configure the volume as required for your environment.

For this option....	Do the following...
Name	Enter a name for the new volume. **Important:** The combined length of the names of both the storage pool and volume used for NFI cannot exceed 52 bytes, or the NFI job fails. Most english characters are 1 byte. **Important:** NFS does not allow spaces in share names. As a result, any spaces in the volume name are replaced by underscores in the corresponding NFS share name. The Verde user interface displays the volume name without the underscores. For example, for a volume named **Share One**, the corresponding NFS share is named **Share_One** to external network computers, but it is named **Share One** in the Verde user interface.
Pool	Select the storage pool on which to create the volume. If there are multiple storage pools configured on the Verde NAS solution, use the drop-down menu to select the pool where you want to create the volume.

For this option....	Do the following...
Minimum Size	Select the desired unit size from the drop-down menu and enter a numerical value for the minimum size in the text box to the left of the unit size drop-down menu. This space is allocated immediately if there is sufficient space available on the storage pool. If there is insufficient space available, volume creation fails. **Note:** Leave the **Minimum Size** and **Maximum Size** blank to create the volume using all available space on the storage pool.
Maximum Size	Select the desired unit size from the drop-down menu and enter a numerical value for the maximum size in the text box to the left of the unit size drop-down menu. **Notes:** ▪ Volumes are thin provisioned, so it is possible for the combined allocated maximum storage of all volumes to exceed the physical space available. ▪ Leave the **Minimum Size** and **Maximum Size** blank to create the volume using all available space on the storage pool.
Case Insensitive (CIFS)	If desired, select this option to configure the volume to treat all names as case insensitive, which can improve performance, especially in situations where directories contain a large number of files. **Note:** This option should be used for volumes shared using CIFS and **cannot** be changed after creating the volume. **CAUTION: DO NOT** enable this setting if you plan to share the volume using NFS.
Compression	If desired, select the check box to enable the Verde NAS solution to compress stored data. If the data being written is compressible there is an increase in write performance to the volume, which is dependent on how much compression occurs on the data being written. The data compression process uses CPU cycles to perform the compression. If compression is enabled and non-compressible data is written to the volume, the compression process may use an excessive number of CPU cycles, slowing the overall performance of the system.
Access Time	If desired, select the check box to configure the system to update the time stamp of a file when it is read from the volume. Selecting **Access Time** may slow performance.

3. Select the **Enabled** check box to enable the **NFI Volume Policy**.
4. Select either **Copy and Keep**, or **Copy and Delete**.

This option....	Does the following...
Copy and Keep	New or changed data in the volume is copied to the BlackPearl managed object storage and retained in the NAS volume.
Copy and Delete	Data in the volume is copied to the BlackPearl managed object storage and then deleted from the NAS volume.

5. Using the drop-down menu, select a **BlackPearl System** configured in Configure the NFI Service on page 191.

6. Enter the name of the **Bucket** to use to store the data on the BlackPearl system. If the bucket does not exist, it is automatically created.

   Notes:
   - The bucket name cannot contain a colon (:), forward slash (/), or space.
   - The bucket name cannot exceed 255 characters.
   - If you plan to modify files in the NAS volume, the target BlackPearl system must use credentials for a user with a default data policy that uses versioning, or you must enter the name of the bucket with a data policy that uses versioning. See Create a Bucket Using the Required Data Policy on page 190.
   - If the bucket data policy includes a replication rule for an Amazon S3 or Microsoft Azure target, the bucket name must also conform to the naming conventions of that cloud provider.

Important BlackPearl bucket names are case sensitive, but for some cloud targets, bucket names must be all lower case. The BlackPearl software changes bucket names with upper case letters to all lower case letters when needed. If you are using bucket names that only differ by case, the buckets are combined on the cloud target. For example, the BlackPearl buckets 'Index' and 'index' both map to the cloud bucket 'index', causing possible data collision and bucket ownership/permission problems.

7. Configure the **NFI Volume Policy Schedule**:

   The NFI Volume Policy Schedule transfers data from the Verde NAS solution to a BlackPearl system at intervals based on number of hours, days, or days of the week. Decide which interval to use for the schedule and follow the appropriate instructions.

   - Create an Hourly Schedule on page 196 — Transfer data every selected number of hours.
   - Create a Daily Schedule on page 196 — Transfer data every selected number of days.
   - Create a Weekly Schedule on page 197 — Transfer data on certain days of the week.

Create an Hourly Schedule

1. In the New Volume dialog box, select **Hourly** as the interval for the policy schedule. The dialog box changes to display options for the hourly interval setting

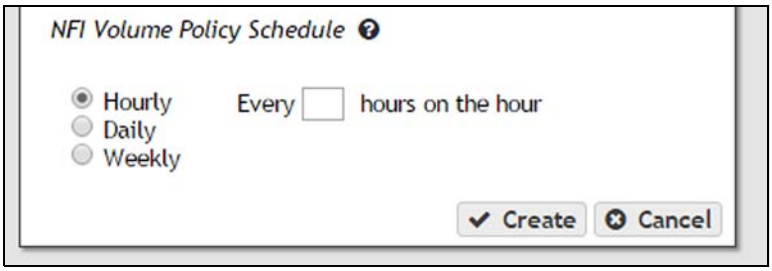


Figure 149 The New Volume dialog box showing the hourly interval options.

2. Enter a number for **Every _ hours on the hour**. This value specifies the interval, in hours, between transferring data to the BlackPearl system. For example, if this value is set to 4, the system copies data every four hours. The maximum setting for this field is 48, where the system copies data every two days.
3. Click **Create**.
4. Continue to Next Steps on page 197.

Create a Daily Schedule

1. In the New Volume dialog box, select **Daily** as the interval for the policy schedule. The dialog box changes to display options for the daily interval setting.

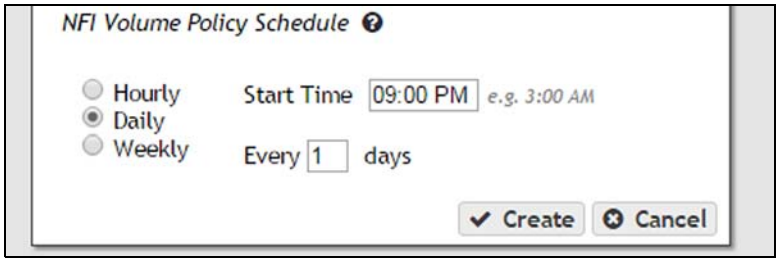


Figure 150 The New Volume dialog box showing the daily interval options.

2. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
3. Enter a number for **Every _ days**. This value specifies the interval, in days, between transferring data to the BlackPearl system. For example, if this value is set to 2, the system copies data every two days at the time specified in Step 2.
4. Click **Create**.
5. Continue to Next Steps on page 197.

Create a Weekly Schedule

1. In the New Volume dialog box, select **Weekly** as the interval for the policy schedule. The dialog box changes to display options for the weekly interval setting.

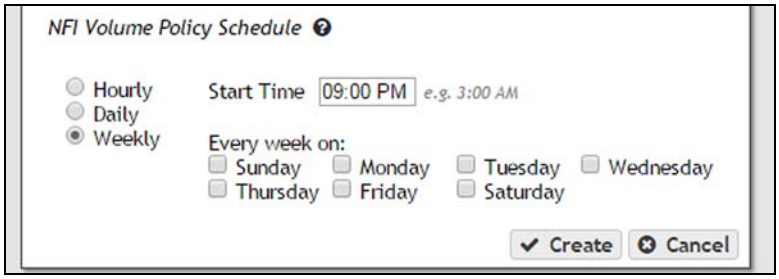


Figure 151 The New Volume dialog box showing the weekly interval options.

2. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
3. Select one or more days for **Every week on:**. This determines the day(s) of each week the system copies data to the BlackPearl system.
4. Click **Create**.
5. Continue to Next Steps below.

Next Steps

After creating a volume and configuring the NFI Volume Policy Schedule, you must create a share for the volume. See Create a New Share on page 56. Once you create a share for the volume, you can begin file storage operations.

Restoring Files From an NFI Target BlackPearl System

If files copied to the BlackPearl system using the NFI service are deleted from the Verde NAS solution, or the Verde NAS solution fails, you can retrieve files from the BlackPearl system using the Spectra Eon Browser, Spectra Deep Storage Browser, or a Spectra S3 client. If you only need to retrieve a small number of files, Spectra Logic recommends using the Eon Browser.

Restore Files Using the Eon Browser

For instructions for installing, configuring, and using the Eon Browser, see the *BlackPearl Eon Browser User Guide*.

Restore Files Using the Deep Storage Browser

Use the instructions in this section to restore files from the BlackPearl system using the Deep Storage Browser.

Retrieve S3 Credentials from the BlackPearl System

Before you can configure and use the Deep Storage Browser, you must retrieve the S3 credentials for the user configured in the Verde NAS solution NFI service.

- If you do not know which user is configured in the NFI service, see Configure Network File Interface on page 191.
- If you already know the S3 credentials of the user, skip to Download the Deep Storage Browser on page 199.

Use the instructions in this section to retrieve the S3 credentials from the BlackPearl system.

1. Log into the BlackPearl interface as described in the *Spectra BlackPearl User Guide*.
2. From the menu bar, select **Configuration ···⁘ Users.** The Users screen displays.
3. Select the user configured in the Verde NFI service from the User pane of the Users screen, and then select **Action ···⁘ Show S3 Credentials**. The S3 Credentials dialog box displays.

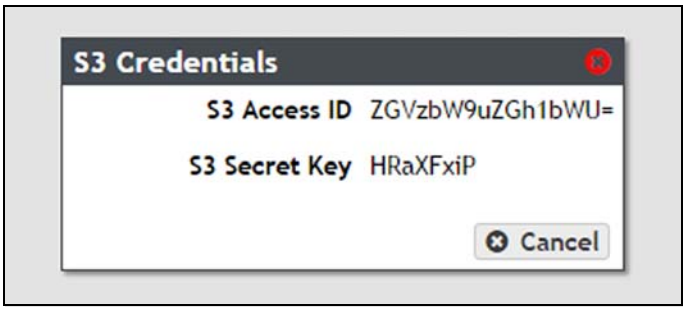


Figure 152 The S3 Credentials dialog box.

4. Record the **S3 Access ID** and **S3 Secret Key** for use when configuring the Deep Storage Browser to access the BlackPearl system.

   Note: It is helpful to leave the S3 Credentials dialog box open on the BlackPearl user interface, so that you can easily copy and paste the credential values when configuring the Deep Storage Browser.

Download the Deep Storage Browser

Use the instructions in the following sections to download the Deep Storage browser for Microsoft Windows or Apple Mac OS operating systems.

1. Using a web browser, navigate to https://developer.spectralogic.com/ds3browser.
2. Click the software download link appropriate for your operating system. The Deep Storage browser install file begins downloading through your web browser.

Install and Launch the Deep Storage Browser

Use the instruction in this section to install and launch the Deep Storage Browser. The instructions differ depending on which operating system is installed on your host machine.

Microsoft Windows

1. Right-click the .zip file you downloaded in Download the Deep Storage Browser. The context window displays.
2. Select **Extract All**. The ZIP file extracts to a folder in the same directory as the ZIP file.

   Note: If the ZIP file is on the desktop, the extracted program folder displays on the desktop.
3. Double-click the extracted folder. The contents display in a window.
4. Double-click **Deep Storage Browser.exe** to launch the program.

Apple Mac OS

1. Double-click the .dmg file you downloaded in Download the Deep Storage Browser. An icon displays on the operating system desktop.
2. Double-click the icon on the desktop. A window displays showing the DSB icon on the left side and the Applications folder icon on the right side.
3. Drag and drop the DSB icon onto the Application folder icon. The program installs.
4. Open the Application tab, and double-click **Spectra Deep Storage Browser** to launch the program.

Configure the Deep Storage Browser

Before you can retrieve files from the BlackPearl system, you must first setup the logical connection between the Deep Storage browser and the BlackPearl system.

1. Launch the Deep Storage browser using the method appropriate for your operating system (see Install and Launch the Deep Storage Browser on page 199). The New Deep Storage Browser Session dialog box displays.

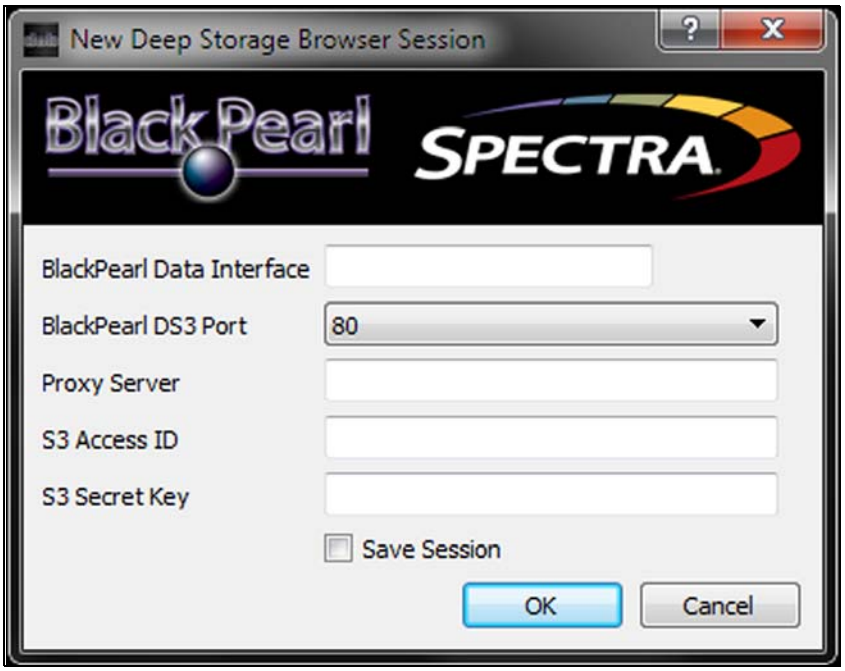


Figure 153 The New Deep Storage Browser Session dialog box.

2. Enter the IP address of the data port of the BlackPearl system in the **BlackPearl Data Interface** field. The IP address must be a valid IPv4 address. See "Configure the Data Connection" in the *Spectra BlackPearl User Guide* to determine the data port IP address.

   Note: If you enter the IP address of the BlackPearl management port, the connection to the system fails.

3. Use the **BlackPearl DS3 Port** drop down menu to select the DS3 port. The DS3 port is the port configured for use by the S3 service on the BlackPearl system. The default value is **8o**. See "Configure the Spectra S3 Service" in the *Spectra BlackPearl User Guide* to determine the DS3 port value.

4. If desired, enter the IP address of a proxy server in the **Proxy Server** field.

5. Enter the **S3 Access ID** and **S3 Secret Key** for the user configured in the Verde NAS solution NFI service that you retrieved in Retrieve S3 Credentials from the BlackPearl System on page 198.

   Notes:
   - If you left the S3 Credentials window open in the BlackPearl user interface, you can copy and paste the S3 credentials into the appropriate fields in the New Deep Storage Browser Session dialog box.
   - Only one user at a time can access the BlackPearl system using a Deep Storage browser.
   - Only the buckets assigned to the specified user are accessible using the Deep Storage browser.

6. Optionally, select the **Save Session** check box. If selected, the above information is pre-entered the next time you launch the Deep Storage Browser.

7. Click **Save**. The Spectra Logic Deep Storage Browser main window displays.

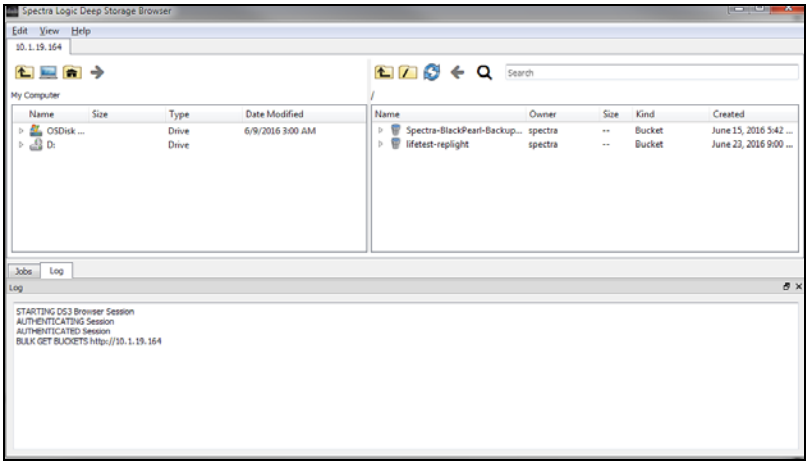


Figure 154 The Spectra Logic Deep Storage Browser main window.

Transfer Files

Use the instructions in this section to use the Deep Storage browser to copy a file from the BlackPearl system to your local host.

Note: If you are not familiar with the interface style of the Deep Storage Browser, see "Interface Overview" in the *Spectra BlackPearl User Guide.*

1. If necessary, launch the Deep Storage browser using the method appropriate for your operating system (see Install and Launch the Deep Storage Browser on page 199). The New Deep Storage Browser Session dialog box displays.
   - If you previously connected to the BlackPearl system and elected to save the session information, the login information is pre-entered in the dialog box. Click **OK**. The Deep Storage Browser main window displays.
   - If you did not save the session information or are connecting to a BlackPearl system for the first time, complete the steps in Configure the Deep Storage Browser on page 200.
2. In the Deep Storage browser main window, navigate to the target destination in the local host pane.
3. In the BlackPearl pane of the Deep Storage browser, navigate to the source bucket location.
4. In the BlackPearl pane, select the file(s) you want to transfer to the local host.

   Notes:
   - To select a consecutive group of files or folders, click the first item, press and hold down the **Shift** key, and then click the last item.
   - To select non-consecutive files or folders, press and hold down the **Ctrl** key, and then click each item that you want to select.
5. Drag the selected files from the BlackPearl pane to the local host pane. The files immediately begin copying to the local host.

Restore Files Using a Spectra S3 Client

Consult the documentation for your Spectra S3 client to restore files from an NFI target BlackPearl system.

APPENDIX B

Specifications

This appendix provides specifications for Verde master nodes, the Verde enterprise expansion node, and the Verde archive expansion node. The specifications listed here pertain to the currently shipping Verde chassis.

Notes:
- For specifications that differ for the Verde 1.0 chassis, see Appendix B Verde Chassis 1.0 Overview & Specifications on page 220.
- All specifications are subject to change without notice.

Specification	
Data Storage Specifications	page 204
Verde 2U and 4U Master Nodes	page 204
Verde Enterprise Expansion Node	page 204
Verde Archive Expansion Node	page 204
107-Drive Disk Expansion Node	page 205
Capacity	page 205
System Specification	page 206
Verde 2U Master Node	page 206
Verde 4U Master Node	page 207
Size and Weight	page 207
Verde 2U Master Node	page 207
Verde 4U Master Node and Verde Enterprise Expansion Node	page 208
Verde Archive Expansion Node	page 208
107-Drive Disk Expansion Node	page 209
Power Requirements	page 209
Input Power Requirements	page 209
Power Cords	page 211
Interface Specifications	page 213
Verde NAS Solution Interface Connectors	page 213
Expansion Node Interface Connectors	page 213
Network Interface Cables	page 214
Universal Serial Bus (USB) Support	page 214
Environmental Specifications	page 215
Verde Master Nodes and Verde Enterprise Expansion Node	page 215

Specification	
Verde Archive Expansion Node	page 215
107-Drive Disk Expansion Node	page 216
Heat Generation	page 216

DATA STORAGE SPECIFICATIONS

The following table shows the data storage specifications each system.

Verde 2U and 4U Master Nodes

Drive Purpose	Specification
Storage Pools	▪ 4, 8, or 12 TB Spinning-Disk SAS [a] ▪ 12 or 16 TB Spinning-Disk SATA ▪ 12 TB Spinning-Disk Self-Encrypting Drives

a. 1 TB is defined as 1,000,000,000,000 bytes.

Verde Enterprise Expansion Node

Drive Purpose	Specification
Storage Pools or NAS	▪ 4, 8, or 12 TB Spinning-Disk SAS [a] ▪ 12 or 16 TB Spinning-Disk SATA ▪ 12 TB Spinning-Disk Self-Encrypting Drives

a. 1 TB is defined as 1,000,000,000,000 bytes.

Verde Archive Expansion Node

Drive Purpose	Specification
Storage Pools or NAS	8, 12, or 16 TB Spinning-Disk SATA [a]

a. 1 TB is defined as 1,000,000,000,000 bytes.

107-Drive Disk Expansion Node

Drive Purpose	Specification
Storage Pools or NAS	▪ 400 GB Solid-State SAS [a] ▪ 4, 8, 12 TB Spinning-Disk SAS [b] ▪ 12 or 16 TB Spinning-Disk SATA ▪ 12 TB Spinning-Disk Self-Encrypting Drives

a. 1 GB is defined as 1,000,000,000 bytes.
b. 1 TB is defined as 1,000,000,000,000 bytes.

CAPACITY

The following table shows the native capacity of each Verde NAS solution.

Chassis	Native Capacity Options [a, b]
Verde 2U master node	44 TB (eleven 4 TB drives) 176 TB (twelve 16 TB drives)
Verde 4U master node	Minimum - 48 TB (twelve 4 TB drives) Maximum - 560 TB (thirty-five 16 TB drives)
Verde enterprise expansion node	Active Bezel Maximum [c] 44 - 4 TB drives - 176 TB 44 - 8 TB drives - 352 TB 44 - 12 TB drives - 528 TB 44 - 16 TB drives - 704 TB Passive Bezel Maximum [d] 45 - 4 TB drives - 180 TB 45 - 8 TB drives - 360 TB 45 - 12 TB drives - 540 TB
Verde archive expansion node	25 - 8 TB drives - 200 TB 25 - 12 TB drives - 300 TB 25 - 16 TB drives - 400 TB 50 - 8 TB drives - 400 TB 50 - 12 TB drives - 600 TB 50 - 16 TB drives - 800 TB 75 - 8 TB drives - 600 TB 75 - 12 TB drives - 900 TB 75 - 16 TB drives - 1200 TB 96 - 8 TB drives - 768 TB 96 - 12 TB drives - 1152 TB 81 - 16 TB drives - 1296 TB [e]

Chassis	Native Capacity Options [a, b]
107-drive disk expansion node	107 - 400 GB drives - 42.8 TB 107 - 4 TB drives - 428 TB 107 - 8 TB drives - 856 TB 107 - 12 TB drives - 1284 TB 107 - 16 TB drives - 1712 TB

a. The native capacity numbers refer to raw disk capacity; RAID configuration and system overhead reduce the actual usable space.
b. 1 TB is defined as 1,000,000,000,000 bytes.
c. A Verde expansion node with an active bezel requires a Visual Status Beacon control sled installed in one drive storage slot.
d. A Verde expansion node with a passive bezel does not require a Visual Status Beacon control sled and can hold one additional data storage drive.
e. Limited to 81 drives based on available power supply wattage.

SYSTEM SPECIFICATION

The following tables provides an overview of the system devices installed in the Verde 2U and Verde 4U master nodes.

Verde 2U Master Node

Parameter	Specifications
CPU	One multi-core processor
System disk drives	Two 500 GB SATA disk drives
Memory	32 GB (4 x 8 GB DIMMs)
Interface connections	▪ Two integrated 10GBase-T Ethernet ports [a] ▪ (Optional) One dual-port 10 Gigabit Ethernet NIC ▪ (Optional) four-port SAS card [b]

a. One port is available for data transfers, one port is dedicated to the Verde user interface for system management.
b. Each optional SAS card is used to connect the Verde master node to up to two enterprise expansion nodes. If your installation does not include an expansion node, the card is not installed.

Verde 4U Master Node

Parameter	Specifications
CPU	Two multi-core processors
System disk drives	Two 500 GB SATA disk drives
Memory	32 GB (4 x 8 GB DIMMs)
Interface connections	▪ Two integrated 10GBase-T Ethernet ports [a] ▪ One dual-port 10 Gigabit Ethernet NIC ▪ (Optional) One dual-port 40 Gigabit Ethernet NIC ▪ (Optional) One dual-port 10GBase-T Ethernet NIC ▪ (Optional) four-port SAS card [b] ▪ (Optional) two-port SAS card [c]

a. One port is available for data transfers, one port is dedicated to the Verde user interface for system management.

b. Each optional four-port SAS card is used to connect the Verde master node to up to two Verde enterprise expansion nodes, or four 107-drive disk expansion nodes. If your installation does not include an expansion node, the card is not installed.

c. Each optional two-port SAS card is used to connect the Verde master node to up to two Verde archive expansion nodes, or two107-drive disk expansion nodes. If your installation does not include an expansion node, the card is not installed.

Size and Weight

The following tables provide the size and weight of each system. Specifications are provided for each unit in both an operational environment, and in the shipping container.

Verde 2U Master Node

Parameter	Verde 2U NAS solution	Shipping Container [a]
Dimensions ▪ Height (2U) ▪ Width ▪ Depth	 3.5 in. (8.9 cm) 19 in. (48.3 cm) 27.5 in. (69.9 cm) [b]	 13.25 in. (33.6 cm) 26 in. (66 cm) 34.25 in. (87 cm)
Weight [c] ▪ Empty chassis ▪ Chassis with Twelve drives	 39.0 lb (17.7 kg) 60.6 lb (27.5 kg)	 N/A 80.5 lb (36.5 kg)

a. Includes chassis, drives, box, and packaging.

b. Includes the front bezel.

c. Weights are approximate.

Verde 4U Master Node and Verde Enterprise Expansion Node

Parameter	Verde 4U NAS solutions	Shipping Container [a]
Dimensions ▪ Height (4U) ▪ Width ▪ Depth	 7 in. (17.8 cm) 19 in. (48.3 cm) 29.5 in. (75 cm) [b]	 17.5 in. (44.5 cm) 27 in. (68.6 cm) 39 in. (99.0 cm)
Weight [c] ▪ Empty chassis ▪ Additional for each disk drive ▪ Additional for each Solid-State drive	 57 lb (25.8 kg) 1.8 lb (0.8 kg) 0.8 lb (0.4 kg)	 91.3 lb 1.8 lb (0.8 kg) 0.8 lb (0.4 kg)

a. Includes chassis and packaging.
b. Includes the front bezel.
c. Weights are approximate.

Verde Archive Expansion Node

Parameter	Verde archive expansion node	Shipping Container
Dimensions ▪ Height (4U) ▪ Width ▪ Depth	 6.9 in. (17.5 cm) 19 in. (48.3 cm) 40 in. (101.6 cm) [a]	 14 in. (35.6 cm) 24.5 in. (62.2 cm) 43.5 in. (110.5 cm)
Weight [b] ▪ Empty chassis ▪ Additional for each disk drive ▪ Additional for rack mounting kit	 76 lb (34.5 kg) 1.8 lb (0.8 kg) 21 lb (9.5 kg)	 108 lb (48.9 kg) [c] 1.8 lb (0.8 kg) 21 lb (9.5 kg)

a. Includes the front bezel.
b. Weights are approximate.
c. Includes chassis and packaging.

107-Drive Disk Expansion Node

Parameter	107-drive disk expansion node	Shipping Container
Dimensions ▪ Height (4U) ▪ Width ▪ Depth	 7 in. (17.8 cm) 17 in. (43.2 cm) 41 in. (104.1 cm) [a]	 18.4 in. (46.7 cm) 24.3 in. (61.7 cm) 52.3 in. (132.8 cm)
Weight [b] ▪ Empty chassis ▪ Additional for each disk drive ▪ Additional for rack mounting kit ▪ Fully loaded chassis	 84.4 lb (38.3 kg) 1.5 lb (0.67 kg) 21 lb (9.5 kg) 336 lb (152.4 kg)	

a. Includes the front bezel.
b. Weights are approximate.

POWER REQUIREMENTS

The Verde NAS solutions, Verde enterprise expansion nodes, and Verde archive expansion nodes, have the following power requirements.

Caution Failure to meet the cabling and power specifications could damage your system, result in data loss, or both.

Input Power Requirements

The following tables provide the input power requirements for each system or expansion node.

Verde 2U Master Node

Parameter	Requirements
Input Voltage	100–240 VAC, 11–4.5 A, 920 watts maximum
Input Frequency	50–60 Hz

Verde 4U Master Node

Parameter	Requirements
Input Voltage	100–140 VAC, 12–8 A, 1000 watts maximum 180–240 VAC, 8–6 A, 1280 watts maximum
Input Frequency	50–60 Hz

Verde Enterprise Expansion Node

Parameter	Requirements
Input Voltage	100–140 VAC, 13.5–9.5 A, 1100 watts maximum 180–240 VAC, 9.5–7 A, 1400 watts maximum
Input Frequency	50–60 Hz

Verde Archive Expansion Node

Parameter	Requirements
Input Voltage	90-264 VAC, 1100 watts maximum
Input Frequency	47–63 Hz

107-Drive Disk Expansion Node

Parameter	Requirements
Input Voltage	200–240 VAC, 15 A, 2000 watts maximum
Input Frequency	50–60 Hz

Power Cords

The power cords included with the Verde NAS solutions are considered part of the unit and are not intended for used with any other equipment.

Important Confirm the PDU used with the Verde NAS solution has enough amperage for the power supply in each chassis included in your installation.

Cables provided by Spectra Logic are between 6 ft (1.8m) to 6.5 ft (2m) in length. If you need to use a longer cord, make sure it conforms to the specifications listed below.

Power cords must comply with local electrical codes.

Note: Verde Archive expansion nodes ship with cables for use with the chassis. These power cables have a right-angled C14 connector, which is required for the Verde archive expansion node. Only use the cords provided by Spectra Logic with the Verde archive expansion node.

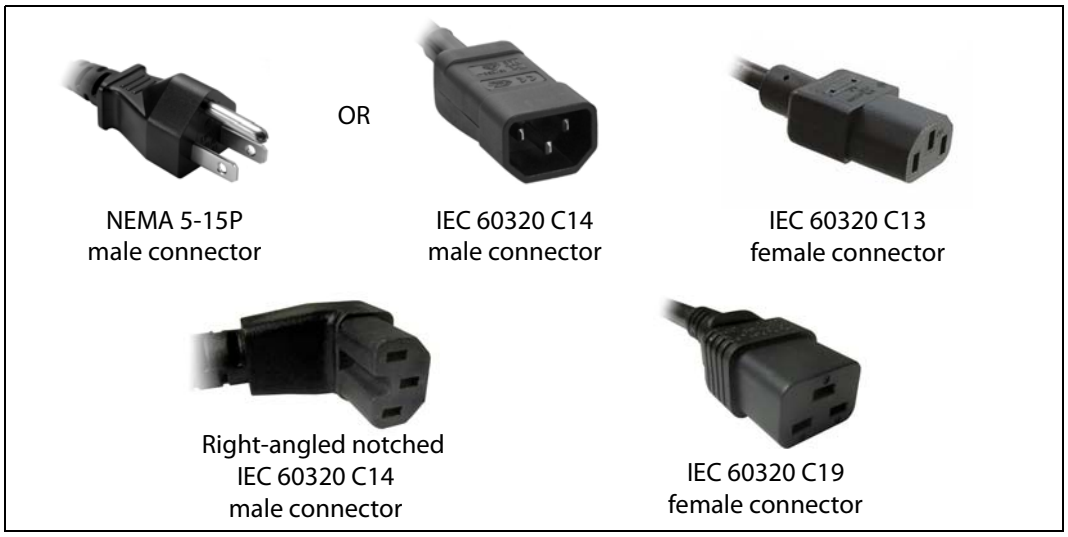
Warning

Using extension cords in conjunction with the cords provided with a Verde archive expansion node, may cause serious damage.

WARNUNG Die Verwendung von Verlängerungskabeln in Verbindung mit den mit einem Verde-Archiv-Erweiterungsknoten versehenen Kabeln kann zu schweren Schäden führen.

North American 120 Volt-AC Power Cord The criteria for a 120-volt power cord for use in the United States and Canada are as follows:

Parameter	Specification
Power cordage	Three-conductor, 14 AWG
Power input connectors	▪ **Male:** NEMA 5-15P or IEC-60320 C14 ▪ **Female:** IEC 60320 C13



North American 220 Volt-AC Power Cord The criteria for a 220-volt power cord for use in the United States and Canada are as follows:

Parameter	Specification
Power cordage	SJT type, three-conductor, 14 AWG minimum
Power input connectors	**Verde 2U and 4U Master Node:** ▪ **Male:** Connector must be of the proper type, rating, and safety approval. ▪ **Female:** IEC 60320 C13 **Verde Enterprise Expansion Node:** ▪ **Male:** Connector must be of the proper type, rating, and safety approval. ▪ **Female:** IEC 60320 C13 **Verde Archive Expansion Node:** ▪ **Male:** Connector must be of the proper type, rating, and safety approval. ▪ **Female:** Right-angled notched IEC 60320 C14 **107-Drive Chassis Expansion Node:** ▪ **Male:** Connector must be of the proper type, rating, and safety approval. ▪ **Female:** IEC 60320 C19

International 220 Volt-AC Power Cord The criteria for an international 220-volt AC power cord are as follows:

Parameter	Specification
Power cordage	Flexible, HAR (harmonized) type H05VV-F, three conductor, cord with minimum conductor size of 1.7 square millimeters (0.0026350 square inches).
Power input connectors	**Verde 2U and 4U Master Node:** ▪ **Male:** Connector must be of the proper type, rating, and safety approval. ▪ **Female:** IEC 60320 C13 **Verde Enterprise Expansion Node:** ▪ **Male:** Connector must be of the proper type, rating, and safety approval. ▪ **Female:** IEC 60320 C13 **Verde Archive Expansion Node:** ▪ **Male:** Connector must be of the proper type, rating, and safety approval. ▪ **Female:** Right-angled notched IEC 60320 C14 **107-Drive Chassis Expansion Node:** ▪ **Male:** Connector must be of the proper type, rating, and safety approval. ▪ **Female:** IEC 60320 C19

INTERFACE SPECIFICATIONS

This section provides information about the interfaces used to connect a Verde NAS solution to expansion nodes, and host systems.

Verde NAS Solution Interface Connectors

Interface Type	Number of Ports and Connector Type
Ethernet (1000BaseT, or 10GBase-T)	Two RJ-45 sockets.
Ethernet (10 GigE)	Two SFP+ optical modules with a duplex LC connector per optional 10 GigE NIC.
Ethernet (40 GigE)	Two QSFP+ optical modules with a duplex LC connector per optional 40 GigE NIC.
SAS (6 Gbps)	Four SFF-8644 sockets per optional 6 Gbps SAS card provide connections to two Verde expansion nodes, using two ports for each expansion node.
SAS (12 Gbps)	Two or four SFF-8644 sockets per optional 12 Gbps SAS card provide connections to two or four Verde archive expansion nodes, or two or four 107-drive disk solutions, using one port per expansion node.

Expansion Node Interface Connectors

Interface Type	Number of Ports and Connector Type
Verde Enterprise Expansion Node	Two SFF-8088 ports per Verde expansion node. Both ports are required to connect the enterprise expansion node to a Verde NAS solution.
Verde Archive Expansion Node	Two SFF-8644 ports per Verde archive expansion node. Only a single port is required to connect the expansion node to a Verde NAS solution.
107-Drive Disk Expansion Node	▪ Four SFF-8644 ports per expander in the 107-drive disk expansion node. Maximum of two expanders. ▪ One 1_GigE Ethernet port per expander in the 107-drive disk expansion node. Maximum of two expanders.

Network Interface Cables

The type of cables required to connect the Verde master node to an Ethernet network, or expansion node, depend on the type of interface.

Interface Type	Cable Requirements
Ethernet (10GBase-T or 10/100/1000Base-T)	**10GBase-T** - Shielded Category 6A data-grade cable with a RJ-45 connector. **10/100/1000Base-T** - Shielded Category 5 data-grade cable with a RJ-45 connector. **Note:** Cables provided by the customer.
Ethernet (10 GigE)	Multimode optical cable with duplex LC connectors. **Note:** Cables provided by the customer.
Ethernet (40 GigE)	QSFP+ transceiver MPT optical cables with duplex LC connectors, or copper cables with duplex LC connector. **Note:** Cables provided by the customer.
SAS	**Verde enterprise expansion node:** 6 Gbps 4 lane cable with SFF-8644 and SFF-8088 connectors. Two SAS cables are required for each Verde expansion node. **Note:** Two SAS cables are included with each Verde expansion node. **Verde archive expansion node:** 12 Gbps cable with SFF-8644 connectors. One SAS cable is required for each Verde archive expansion node. **107-Drive disk expansion node:** 12 Gbps cable with SFF-8644 connectors. One SAS cable is required for each 107-drive disk expansion node. **Note:** One SAS cable is included with each Verde archive or 107-drive disk expansion node.

Universal Serial Bus (USB) Support

Spectra Logic supports using the USB ports on the system for the following:

- USB mass storage devices (for example, flash drives)
- Keyboards & pointer devices (for example, a computer mouse)
- CD or DVD drives with USB interface

Spectra Logic does not support using the USB ports for the following:

- Cameras
- Multimedia devices (for example, MP3 players)

ENVIRONMENTAL SPECIFICATIONS

Verde Master Nodes and Verde Enterprise Expansion Node

Parameter	Operating Environment [a]	Storing and Shipping (Non-Operating) Environment [b]
Humidity	8% to 90% (non-condensing)	5% to 95% (non-condensing)
Temperature	50° F to 95° F (10° C to 35° C)	–40° F to 158° F (–40° C to 70° C)
Altitude	Sea level to 10,000 feet (3,048 meters)	Sea level to 39,370 feet (12,000 meters)
Maximum wet bulb temperature	84° F (29° C)	95° F (35° C)

a. When moving the Verde master node or enterprise expansion node from a cold storage environment to a warm operating environment, it must acclimate in its packaging for at least 12 hours before opening to prevent serious condensation damage.

b. Specifications are for the Verde system in its original packaging. The packaging protects the Verde NAS solution from condensation caused by extreme temperature variations (27° F per hour or 15° C per hour, or more).

Verde Archive Expansion Node

Parameter	Operating Environment [a]	Storing and Shipping (Non-Operating) Environment [b]
Humidity	20% to 80% (non-condensing)	10% to 90% (non-condensing)
Temperature	41° F to 95° F (5° C to 35° C)	–40° F to 140° F (–40° C to 60° C)
Altitude	-200 feet to 10,000 feet (-61 meters to 3,048 meters)	-200 feet to 40,000 feet (-61 meters to 12,192 meters)

a. When moving the Verde archive expansion from a cold storage environment to a warm operating environment, it must acclimate in its packaging for at least 12 hours before opening to prevent serious condensation damage.

b. Specifications are for the Verde archive expansion node is in its original packaging. The packaging is designed to protect the Verde archive expansion node from condensation caused by extreme temperature variations (27° F per hour or 15° C per hour, or more).

107-Drive Disk Expansion Node

Parameter	Operating Environment [a]	Storing and Shipping (Non-Operating) Environment [b]
Humidity	20% to 80% (non-condensing)	10% to 90% (non-condensing)
Temperature	32° F to 95° F (0° C to 35° C)	–4° F to 140° F (–20° C to 60° C)
Altitude	-200 feet to 10,000 feet (-61 meters to 3,048 meters)	-200 feet to 40,000 feet (-61 meters to 12,192 meters)

a. When moving the 107-drive disk expansion node from a cold storage environment to a warm operating environment, it must acclimate in its packaging for at least 12 hours before opening to prevent serious condensation damage.

b. Specifications are for the 107-drive disk expansion node is in its original packaging. The packaging is designed to protect the 107-drive disk expansion node from condensation caused by extreme temperature variations (27° F per hour or 15° C per hour, or more).

Heat Generation

The following table shows the heat generation of each Verde NAS solution.

Chassis	Heat Generation at Maximum Wattage
Verde 2U master node	3138 BTUs/hour
Verde 4U master node	3410 - 4365 BTUs/hour
Verde enterprise expansion node	3751 - 4775 BTUs/hour
Verde archive expansion node	3751 BTUs/hour
107-drive disk expansion node	6820 BTUs/hour

APPENDIX A

IPMI Configuration

This appendix provides instructions for configuring IPMI for the Verde NAS solution using the system BIOS.

Caution **DO NOT** make any changes in the BIOS other than changing the IPMI settings as described below. Changing any other setting is not supported by Spectra Logic and may cause adverse system performance.

1. If the Verde NAS solution is currently powered on, shut down the system as described in Reboot or Shut down a Verde NAS Solution on page 144.
2. Connect a monitor and USB keyboard to the rear of the Verde NAS solution. See Rear Panel of Master Nodes on page 25 to locate the monitor and USB connectors.
3. Power on the NAS solution as described in Power On the Verde NAS Solution on page 39.
4. When prompted by the system, press **DEL** to enter the system BIOS.

   Note: The system only displays this prompt for a few seconds. If you do not press **DEL** in time to enter the BIOS, let the system complete it's boot process, then reboot the system and repeat Step 4.

5. Using the keyboard, navigate to the **IPMI** tab and then select **BMC Network Configuration**. The current settings of the BMC configuration display.

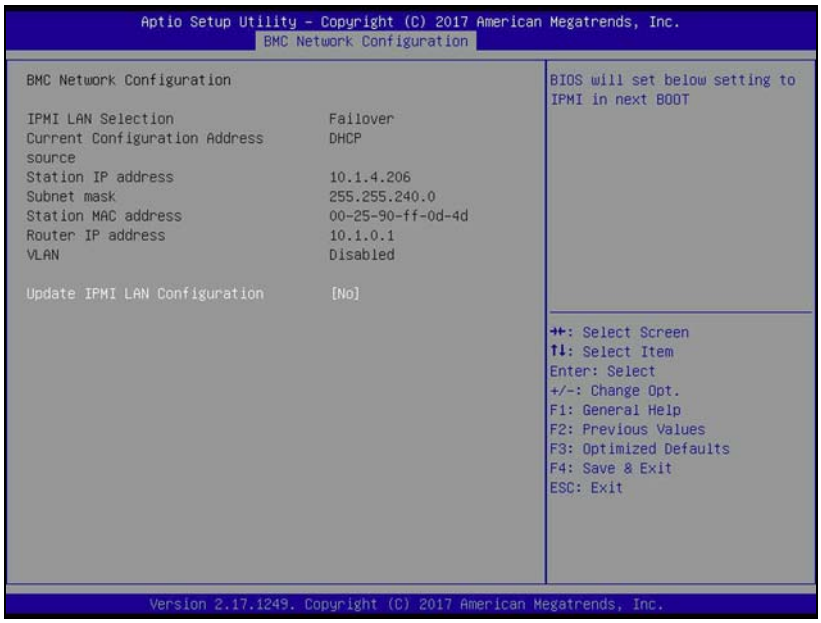


Figure 155 The BMC Configuration screen.

6. Using the keyboard, select **Update IMPI LAN Configuration**. A confirmation window displays. Select **YES** to continue. The current IMPI settings display.

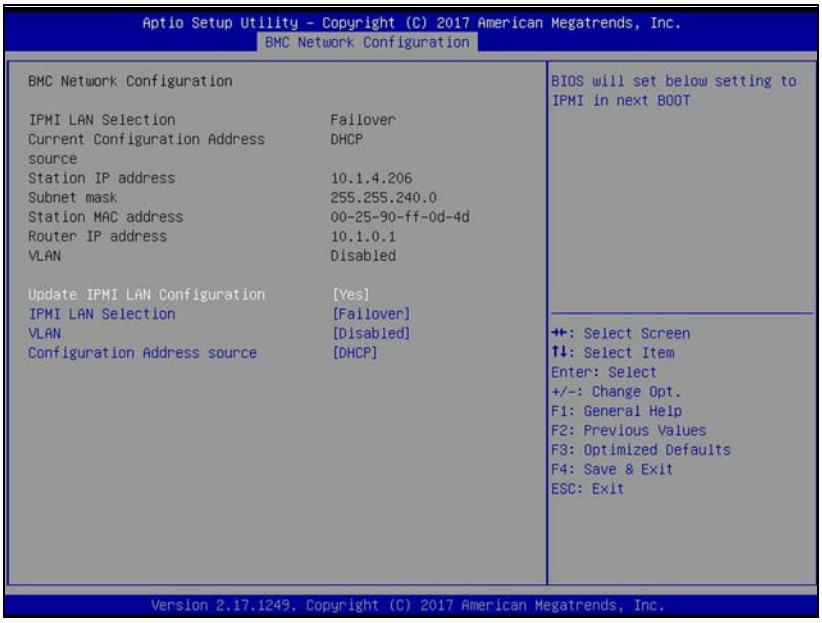


Figure 156 Current IPMI settings.

7. If desired, select **IPMI LAN Selection**. Change the configured setting as needed.
   - **Dedicated** - Always uses the dedicated IPMI port for IPMI traffic.
   - **Shared** - Always uses the LAN1 port for IPMI traffic.
   - **Failover** - On system startup, detect if the dedicated IPMI port is connected. If not, the system uses the LAN1 port for IPMI traffic.
8. If desired, select **VLAN** to enable or disable VLAN as needed.
9. To change the IPMI address settings, select **Configuration Address source**. The current address source information displays.
10. Select **Static** or **DHCP** addressing.
    - If you select **DHCP**, skip to Step 12.
    - If you select **Static**, IP addressing fields display.

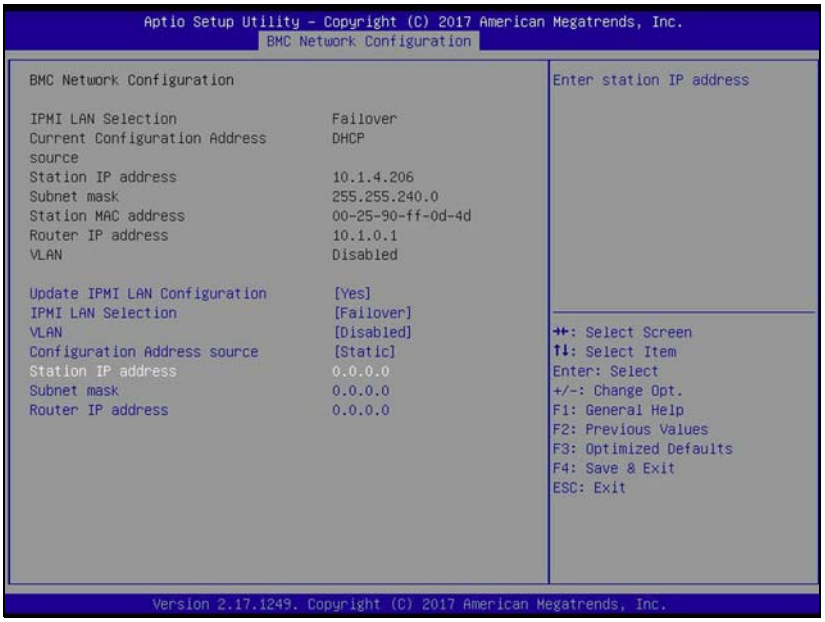


Figure 157 Enter Static IP information.

11. Configure the **Station IP address**, **Subnet mask**, and **Router IP address** with the desired address values.

    Note: Only IPv4 addresses are valid.
12. Press **F4** to exit the BIOS and save the entered settings. The Verde NAS solution reboots.

APPENDIX B

Verde Chassis 1.0 Overview & Specifications

This chapter provides an overview and specifications for the Spectra Logic Verde NAS solution chassis 1.0.

Topic	
Components	page 221
Front View of Master Nodes and Expansion Node	page 221
Rear View of Master Nodes	page 222
Rear Panel	page 223
Specifications	page 224
System Specification	page 224
Interface Specifications	page 225
Interface Connectors	page 225
Network Interface Cables	page 226

COMPONENTS

The following sections show the locations of and briefly describe the Verde chassis 1.0 major front and rear panel components.

Front View of Master Nodes and Expansion Node

Figure 158 and Figure 159 show the components on the front of the Verde NAS solutions with the front bezel removed.

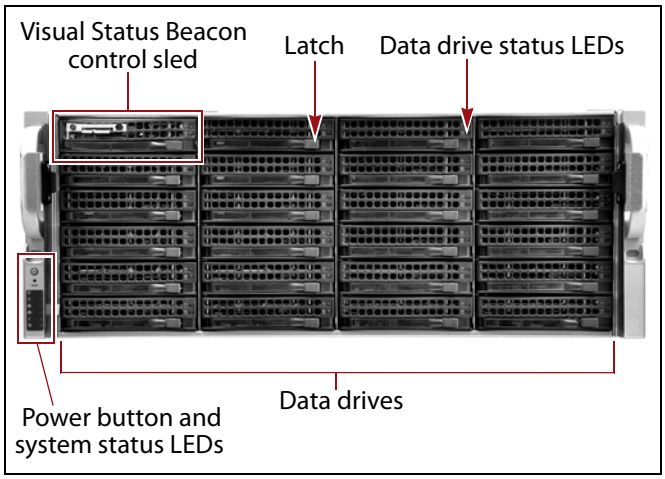


Figure 158 The front view of the Verde 4U master and expansion nodes (front bezel removed).

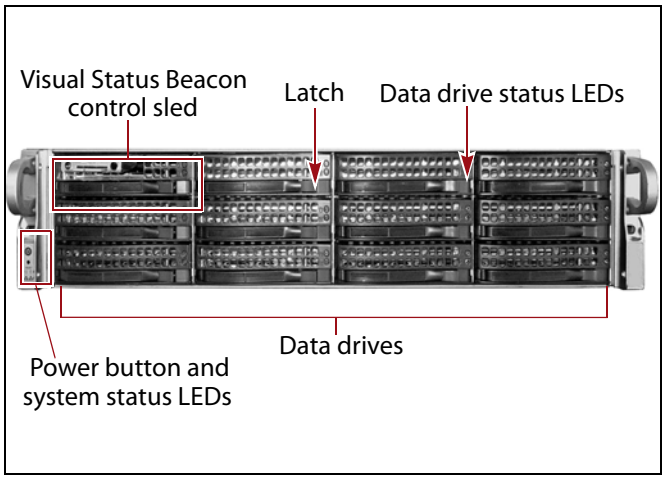


Figure 159 The front view of the Verde 2U master node (front bezel removed).

Component	Description
Front bezel (not shown)	The front bezel mounts on the front of the system, and contains the Visual Status Beacon light bar, which provides status information for the system. See Front Bezel Visual Status Beacon on page 131 for more information.
Visual Status Beacon control sled	The drive sled in the upper left corner of the front of the system provides control for the Visual Status Beacon. A disk drive cannot be installed in this position.
Power button	The power button controls the main AC power for the Verde NAS solution.
System status LEDs	The status LEDs indicate power status, disk and network activity, as well as hardware faults. See System Status LEDs on page 133 for more information.
Data drives	The Verde 4U master and expansion nodes supports up to twenty-three high-performance disk drives mounted on individual drive sleds in the front of the system. The Verde 2U master node supports up to eleven data drives. The drive sleds slide into bays in the front of the Verde enclosures and lock in place. The front of each drive sled has a handle for removing the sled from the system and a latch for locking the drive sled in place.
Data drive status LEDs	Two LEDs on each drive sled indicate the status of the drive. One LED is for drive status while the other shows drive activity.
Empty drive sleds	When fewer than the maximum number of drives are installed, empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow.

Rear View of Master Nodes

Figure 160 and Figure 161 show the major components on the rear of the Verde master nodes using the Verde 1.0 chassis.

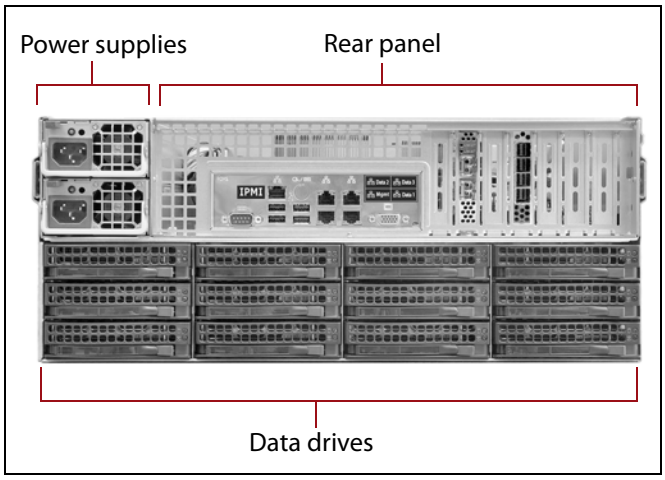


Figure 160 The rear view of the Verde 4U master node.

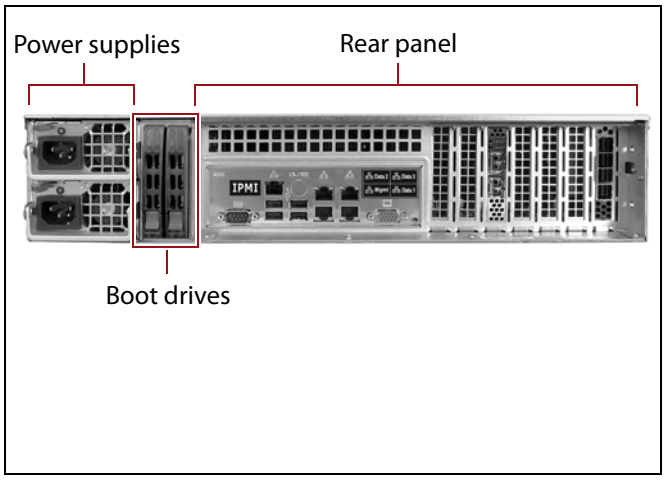


Figure 161 The rear view of the Verde 2U master node.

Component	Description
Power supplies	The Verde master node includes two power supplies to provide N+1 redundancy and fail-over protection. ▪ Each power supply has its own AC power connector. ▪ Each power supply has a single LED that lights to indicate when the power is on and functioning normally.
Rear panel	The rear panel of the Verde master node allows for Ethernet, SAS, USB, and other connections. See Rear Panel on page 223 for a detailed description.
Boot drives (Verde 2U master node only)	The boot drives provide storage for the operating system and Verde user interface. The boot drives are hot swappable which allows for uninterrupted operation during replacement. **Note:** The boot drives for the Verde 4U master node are located inside the chassis and are not accessible from the outside.
Data drives (Verde 4U master node only)	Up to twelve data drives can be installed in the rear of the system. **Note:** The Verde 2U master node does not have drives in the rear of the system.
Empty drive sleds (Verde 4U master node only)	When fewer than the maximum number of drives are installed, empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow.

Rear Panel

Figure 162 shows the components on the rear panel of the Verde 4U master node using the Verde 1.0 chassis. Components are in similar locations on the Verde 2U master node.

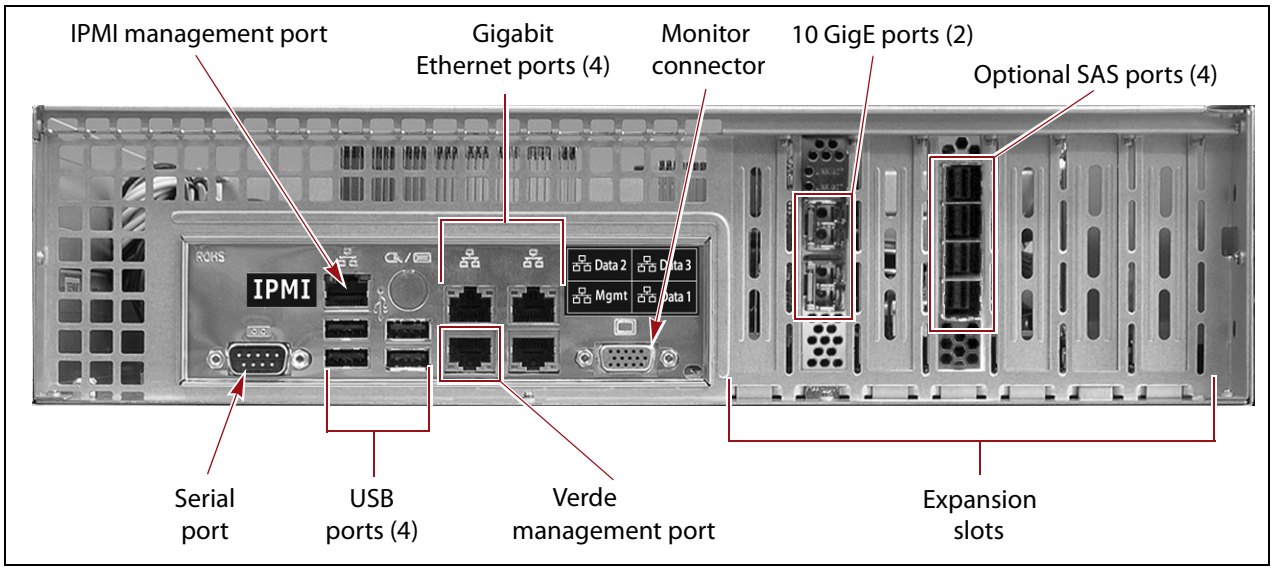


Figure 162 The rear panel components (Verde 4U master node pictured).

Component	Description
IPMI management port	Not currently supported.
Gigabit Ethernet ports (GigE)	The Verde master node includes four GigE ports. Three of the GigE ports can be used for network connections from hosts to the Verde NAS solution. The bottom left port of the four GigE ports is dedicated as the Verde management port and cannot be used for data transfer.
Monitor connector	If necessary, you can connect a monitor to the SVGA connector on the Verde master node for troubleshooting purposes. Only connect a monitor as directed by Spectra Logic Technical Support.
10 GigE ports	The two 10 Gigabit Ethernet (10 GigE) ports can be used for network connectivity on a 10 GigE network.
SAS ports (Optional)	Depending on your configuration, there may be SAS cards installed in available expansion slots. Each additional SAS card provides connectivity between the Verde master node and up to two Verde expansion nodes. Each card has four SAS ports. For information on how to connect cables between the master node and expansion node, see the *Spectra Verde NAS Solution Installation Guide.*
Expansion slots	The expansion slots accommodate optional interface cards to provide additional connectivity.
Verde management port	The Verde management port is used to connect to the browser-based user interface to configure, manage, and monitor the Verde NAS solution. The Verde management port cannot be used for data transfer.

Component	Description
USB ports	If necessary, you can use these ports to connect a USB drive, or USB mouse and USB keyboard to the system for troubleshooting purposes. Only connect a USB drive, keyboard, or mouse as directed by Spectra Logic Technical Support.
Serial port	The serial port is used to connect a primary master node to a secondary master node in a HotPair configuration. The two master nodes are connected using a null modem cable. For information on connecting cables for a HotPair configuration, see Appendix B HotPair Setup and Configuration starting on page 189.

SPECIFICATIONS

The following sections describe the specifications of the Verde 1.0 chassis, where they differ from the current chassis. See Appendix B Specifications on page 203 for specification information not listed here.

System Specification

The following tables provides an overview of the system devices installed in the Verde 4U, and Verde 2U master nodes.

Verde 2U Master Node

Parameter	Specifications
CPU	One multi-core processor
System disk drives	Two 250 GB SATA disk drives
Memory	32 GB (4 x 8 GB DIMMs)
Interface connections	▪ Four integrated Gigabit Ethernet ports ▪ One dual-port 10 Gigabit Ethernet NIC ▪ (Optional) four-port SAS card [a]

a. Each optional SAS card is used to connect the Verde master node to up to two Verde expansion nodes. If your installation does not include an expansion node, the card is not installed.

Verde 4U Master Node

Parameter	Specifications
CPU	Two multi-core processors
System disk drives	Two solid-state 64 GB DOMs
Memory	32 GB (4 x 8 GB DIMMs)
Interface connections	▪ Four integrated Gigabit Ethernet ports ▪ One dual-port 10 Gigabit Ethernet NIC ▪ (Optional) four-port SAS card [a]

a. Each optional SAS card is used to connect the Verde master node to up to two Verde expansion nodes. If your installation does not include an expansion node, the card is not installed.

Interface Specifications

This section provides information about the interfaces used to connect the Verde master nodes using the Verde 1.0 chassis to the host systems and to a Verde expansion node. It also provides information about the Ethernet interface used to access the Verde user interface.

Interface Connectors

This section provides information on the interface connectors in the Verde master nodes.

Verde Master Nodes

Interface Type	Number of Ports and Connector Type
Ethernet (GigE)	Four RJ-45 sockets
Ethernet (10 GigE)	Two SFP+ optical modules with a duplex LC connector
SAS	Four SFF-8644 sockets per optional SAS card [a]
Serial	One DB9 connector

a. Each SAS card is used to connect the Verde master node to up to two Verde expansion nodes. If your installation does not include an expansion node, the card is not installed.

Verde Expansion Node

Interface Type	Number of Ports and Connector Type
SAS	Four SFF-8088 sockets

Network Interface Cables

The type of cables required to connect the Verde master node to the network depend on the type of interface being used.

Interface Type	Cable Requirements
Ethernet (GigE)	Shielded Category 5 (10/100BaseT connection) data-grade cable with a RJ-45 connector
Ethernet (10 GigE)	Multimode optical cable with a duplex LC connector
SAS	6 Gbps 4-lane cable with SFF-8644 and SFF-8088 connectors
Serial	Female to female null modem cable with DB9 connectors

APPENDIX C

Regulatory & Safety Standards

When installed in accordance with this guide the Spectra Verde master nodes and the Verde expansion nodes comply with the safety and regulatory agency standards listed in this appendix.

EU DECLARATION OF CONFORMITY

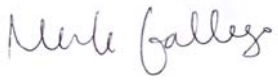
We:

Spectra Logic Corporation
6101 Lookout Road
Boulder, CO 80301 USA

declare under sole responsibility that the

Spectra Verde master nodes and the Verde expansion nodes

to which this declaration relates, meets the essential health and safety requirements and is in conformity with the EU Directives listed below using the relevant section of the EU standards and other normative documents listed in the following table.



Nicole Gallego

Senior Director of Manufacturing and Quality Operations

Directive	Compliance
EU EMC Directive 89/336/EEC	Essential health and safety requirements relating to electromagnetic compatibility.
EN 55022 (CISPER 22) Class A	Limits and methods of measurements of radio interference characteristics of information technology equipment.
EN 55024	1998, Information Technology Equipment - Immunity Characteristics Limits and Methods of Measurement.
EN 61000-4-2	1995 + A1:1998+A2: 2001, Electrostatic Discharge
EN 61000-4-3	1995 + A1:1998 + A2:2001, ENV 50204: 1995, Radiated RF Immunity
EN 61000-4-4	1995 + A1:2001, Electrical Fast Transient/Burst

Directive	Compliance
EN 61000-4-5	1995 + A1:2001 + A2:2001, Surge Immunity
EN 61000-4-6	1996 + A1:2001 + A2:2001, Conducted RF Immunity
EN 61000-4-8	1994 + A1:2001, Power Frequency H-field Immunity
EN 61000-4-11	1994 + A1:2001, Voltage Dips and Interrupts
EN 61000-3-2	2000, Power Line Harmonics
EN 61000-3-3	1995, Power Line Flicker
EC Low Voltage Directive 72/336/EEC	Essential health and safety requirements relating to electrical equipment designed for use with certain violate limits.
EN 60950-1 (EN 60950-1)	Safety requirements of information technology equipment including electrical machines.

Certifications

Country	Certification	Covers
Canada	UL	System
China	CCC	Power supply only
EU	CE	System
Mexico	NOM	Supermicro 2U and 4U chassis, Sanmina chassis
Taiwan	BSMI	Power supply only
USA	UL, FCC	System
Japan	VCCI	System

The Verde NAS solution complies with all safety-relevant provisions referring to:

- Protection against electrical hazards
- Protection against hazards such as:
  - Mechanical hazards
  - Fire hazards
  - Noise
  - Vibration

The safety issues of this information technology equipment type have been evaluated by a government-accredited European third-party organization, such as Nemko.

CE MARKING

The CE marking is affixed on this device according to Article 10 of the EU Directive 90/336/EEC.

Note: To meet CE certification requirements, you must be running the Verde NAS solutions on uninterruptable power supplies.

FCC NOTICE

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to CFR 47 Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user is required to correct the interference at the user's own expense.

SAFETY STANDARDS AND COMPLIANCE

The Spectra Verde master nodes and the Verde expansion nodes comply with the following domestic and international product safety standards.

- EN 60950-1 Second Edition
- UL 60950-1 Second Edition
- CSA-C22.2 No. 60950-1-03
- Low Voltage Directive (EU: CE Mark)

Waste of Electronic and Electrical Equipment (WEEE) Directive

The following symbol on the back of this product indicates that this product meets the European Directive 2000/96/EC on Waste Electrical and Electronic Equipment known as the WEEE directive. This directive, only applicable in European Union countries, indicates that this product should not be disposed of with normal unsorted municipal waste.

Within participating European Union countries, special collection, recycling, and disposal arrangement have been established for this product. At the end of life, the product user should dispose of this product using special WEEE collection systems. These special systems mitigate the potential affects on the environment and human health that can result from hazardous substances that may be contained in this product.

European Union users should contact their local waste administration for WEEE collection instructions for this product.

Restriction of Hazardous Substances in Electrical and Electronic Equipment (RoHS)

The RoHS marking indicates that this product is in compliance with European Council Directive 2011/65/2008, on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Recycling Your Verde NAS Solution

For information on recycling your Spectra product, check the Spectra Logic website at: http://www.spectralogic.com/environment.

Conflict Minerals Policy

Spectra Logic is committed to complying with the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas, as well as the applicable requirements of Section 1502 of the Dodd-Frank Act, which aims to prevent the use of minerals that directly or indirectly finance or benefit armed groups in the Democratic Republic of the Congo (DRC) or in adjoining countries ("conflict minerals").

Affected suppliers to Spectra Logic will be required to commit to being or becoming "conflict-free" (which means that such supplier does not source conflict minerals) and sourcing, where possible, only from conflict-free smelters. Each affected supplier to Spectra Logic will be required to provide completed EICC-GeSI declarations evidencing such supplier's commitment to becoming conflict-free and documenting countries of origin for the tin, tantalum, tungsten, and gold that it purchases.

For more information on Spectra Logic's conflict minerals program contact *conflictminerals@spectralogic.com*.

APPENDIX D

Open Source Code Acknowledgements & Package List

Copyright © 2010 - 2020 Spectra Logic Corporation. All rights reserved.

This appendix contains the licenses and notices for open source software used in the Verde product. If you have any questions or want to receive a copy of the free/open source software to which you are entitled under the applicable free/open source license(s) (such as the Common Development and Distribution License (CCDL)), contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

APACHE

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at:

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

FREEBSD

Copyright © 1992-2020 The FreeBSD Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE FREEBSD PROJECT ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FREEBSD PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the FreeBSD Project.

JAVA

ORACLE AMERICA, INC. ("ORACLE"), FOR AND ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES UNDER COMMON CONTROL, IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY SELECTING THE "ACCEPT LICENSE AGREEMENT" (OR THE EQUIVALENT) BUTTON AND/OR BY USING THE SOFTWARE YOU ACKNOWLEDGE THAT YOU HAVE READ THE TERMS AND AGREE TO THEM. IF YOU ARE AGREEING TO THESE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE LEGAL AUTHORITY TO BIND THE LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO BE BOUND BY THE TERMS, THEN SELECT THE "DECLINE LICENSE AGREEMENT" (OR THE EQUIVALENT) BUTTON AND YOU MUST NOT USE THE SOFTWARE ON THIS SITE OR ANY OTHER MEDIA ON WHICH THE SOFTWARE IS CONTAINED.

1. DEFINITIONS. "Software" means the software identified above in binary form that you selected for download, install or use (in the version You selected for download, install or use) from Oracle or its authorized licensees, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Oracle, and any user manuals, programming guides and other documentation provided to you by Oracle under this Agreement. "General Purpose Desktop Computers and Servers" means computers, including desktop and laptop computers, or servers, used for general computing functions under end user control (such as but not specifically limited to email, general purpose Internet browsing, and office suite productivity tools). The use of Software in systems and solutions that provide dedicated functionality (other than as mentioned above) or designed for use in embedded or function-specific software applications, for example but not limited to: Software embedded in or bundled with industrial control systems, wireless mobile telephones, wireless handheld devices, kiosks, TV/STB, Blu-ray Disc devices, telematics and network control switching equipment, printers and storage management systems, and other related systems are excluded from this definition and not licensed under this Agreement. "Programs" means (a) Java technology applets and applications intended to run on the Java Platform, Standard Edition platform on Java-enabled General Purpose Desktop Computers and Servers; and (b) JavaFX technology applications intended to run on the JavaFX Runtime on JavaFX-enabled General Purpose Desktop Computers and Servers. “Commercial Features” means those features identified in Table 1-1 (Commercial Features In Java SE Product Editions) of the Java SE documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html. “README File” means the README file for the Software accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

2. LICENSE TO USE. Subject to the terms and conditions of this Agreement including, but not limited to, the Java Technology Restrictions of the Supplemental License Terms, Oracle grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally the Software complete and unmodified for the sole purpose of running Programs. THE LICENSE SET FORTH IN THIS SECTION 2 DOES NOT EXTEND TO THE COMMERCIAL FEATURES. YOUR RIGHTS AND OBLIGATIONS RELATED TO THE COMMERCIAL FEATURES ARE AS SET FORTH IN THE SUPPLEMENTAL TERMS ALONG WITH ADDITIONAL LICENSES FOR DEVELOPERS AND PUBLISHERS.

3. RESTRICTIONS. Software is copyrighted. Title to Software and all associated intellectual property rights is retained by Oracle and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that the Software is developed for general use in a variety of information management applications; it is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use the Software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Oracle or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4. DISCLAIMER OF WARRANTY. THE SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ORACLE FURTHER DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

5. LIMITATION OF LIABILITY. IN NO EVENT SHALL ORACLE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF ORACLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ORACLE'S ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

6. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Oracle if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon termination, you must destroy all copies of Software.

7. EXPORT REGULATIONS. You agree that U.S. export control laws and other applicable export and import laws govern your use of the Software, including technical data; additional information can be found on Oracle's Global Trade Compliance web site (http://www.oracle.com/products/export). You agree that neither the Software nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

8. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Oracle that Oracle owns the ORACLE and JAVA trademarks and all ORACLE- and JAVA-related trademarks, service marks, logos and other brand designations ("Oracle Marks"), and you agree to comply with the Third Party Usage Guidelines for Oracle Trademarks currently located at

http://www.oracle.com/us/legal/third-party-trademarks/index.html . Any use you make of the Oracle Marks inures to Oracle's benefit.

9. U.S. GOVERNMENT LICENSE RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation shall be only those set forth in this Agreement.

10. GOVERNING LAW. This agreement is governed by the substantive and procedural laws of California. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, or Santa Clara counties in California in any dispute arising out of or relating to this agreement.

11. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

12. INTEGRATION. This Agreement is the entire agreement between you and Oracle relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

A. COMMERCIAL FEATURES. You may not use the Commercial Features for running Programs, Java applets or applications in your internal business operations or for any commercial or production purpose, or for any purpose other than as set forth in Sections B, C, D and E of these Supplemental Terms. If You want to use the Commercial Features for any purpose other than as permitted in this Agreement, You must obtain a separate license from Oracle.

B. SOFTWARE INTERNAL USE FOR DEVELOPMENT LICENSE GRANT. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File incorporated herein by reference, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

C. LICENSE TO DISTRIBUTE SOFTWARE. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File, including, but not limited to the Java Technology Restrictions and Limitations on Redistribution of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that: (a) is a complete, unmodified reproduction of this Agreement; or (b) protects Oracle's interests consistent with the terms contained in this Agreement and that includes the notice set forth in Section H, and (vi) you agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software. The license set forth in this Section C does not extend to the Software identified in Section G.

D. LICENSE TO DISTRIBUTE REDISTRIBUTABLES. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File, including but not limited to the Java Technology Restrictions and Limitations on Redistribution of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the README File ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified, and only bundled as part of Programs, (ii) the Programs add significant and primary functionality to the Redistributables, (iii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README File), (iv) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (v) you only distribute the Redistributables pursuant to a license agreement that: (a) is a complete, unmodified reproduction of this Agreement; or (b) protects Oracle's interests consistent with the terms contained in the Agreement and includes the notice set forth in Section H, (vi) you agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software. The license set forth in this Section D does not extend to the Software identified in Section G.

E. DISTRIBUTION BY PUBLISHERS. This section pertains to your distribution of the JavaTM SE Development Kit Software (“JDK”) with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, Oracle hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the JDK on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the JDK on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the JDK from the applicable Oracle web site; (iii) You must refer to the JDK as JavaTM SE Development Kit; (iv) The JDK must be reproduced in its entirety and without any modification whatsoever (including with respect to all proprietary notices) and distributed with your Publication subject to a license agreement that is a complete, unmodified reproduction of this Agreement; (v) The Media label shall include the following information: “Copyright [YEAR], Oracle America, Inc. All rights reserved. Use is subject to license terms. ORACLE and JAVA trademarks and all ORACLE- and JAVA-related trademarks, service marks, logos and other brand designations are trademarks or registered trademarks of Oracle in the U.S. and other countries.” [YEAR] is the year of Oracle's release of the Software; the year information can typically be found in the Software’s “About” box or screen. This information must be placed on the Media label in such a manner as to only apply to the JDK; (vi) You must clearly identify the JDK as Oracle's product on the Media holder or Media label, and you may not state or imply that Oracle is responsible for any third-party software contained on the Media; (vii) You may not include any third party software on the Media which is intended to be a replacement or substitute for the JDK; (viii) You agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of the JDK and/or the Publication; ; and (ix) You shall provide Oracle with a written notice for each Publication; such notice shall include the following information: (1) title of Publication, (2) author(s), (3) date of Publication, and (4) ISBN or ISSN numbers. Such notice shall be sent to Oracle America, Inc., 500 Oracle Parkway, Redwood Shores, California 94065 U.S.A , Attention: General Counsel.

F. JAVA TECHNOLOGY RESTRICTIONS. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun", “oracle” or similar convention as specified by Oracle in any naming convention designation.

G. LIMITATIONS ON REDISTRIBUTION. You may not redistribute or otherwise transfer patches, bug fixes or updates made available by Oracle through Oracle Premier Support, including those made available under Oracle's Java SE Support program.

H. COMMERCIAL FEATURES NOTICE. For purpose of complying with Supplemental Term Section C.(v)(b) and D.(v)(b), your license agreement shall include the following notice, where the notice is displayed in a manner that anyone using the Software will see the notice:

Use of the Commercial Features for any commercial or production purpose requires a separate license from Oracle. “Commercial Features” means those features identified Table 1-1 (Commercial Features In Java SE Product Editions) of the Java SE documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html

I. SOURCE CODE. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

J. THIRD PARTY CODE. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME file accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME file, the disclaimer of warranty and limitation of liability provisions in paragraphs 4 and 5 of the Binary Code License Agreement shall apply to all Software in this distribution.

K. TERMINATION FOR INFRINGEMENT. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right.

L. INSTALLATION AND AUTO-UPDATE. The Software's installation and auto-update processes transmit a limited amount of data to Oracle (or its service provider) about those specific processes to help Oracle understand and optimize them. Oracle does not associate the data with personally identifiable information. You can find more information about the data Oracle collects as a result of your Software download at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

SAMBA

Samba is provided under the terms of the GNU General Public License (GPL version 3)

For more details and for the full text for each of these licenses, read the LICENSES and COPYING files included with the source packaging of this software.

On Debian GNU/Linux systems, the complete text of the GNU General Public License can be found in `/usr/share/common-licenses/GPL'.

NGINX

Copyright (C) 2002-2020 Igor Sysoev

Copyright (C) 2011-2020 Nginx, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RUBY

Ruby is copyrighted free software by Yukihiro Matsumoto <matz@netlab.jp>.

You can redistribute it and/or modify it under either the terms of the 2-clause BSDL (see the file BSDL), or the conditions below:

1. You may make and give away verbatim copies of the source form of the software without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.
2. You may modify your copy of the software in any way, provided that you do at least ONE of the following:
   a. place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or by allowing the author to include your modifications in the software.
   b. use the modified software only within your corporation or organization.
   c. give non-standard binaries non-standard names, with instructions on where to get the original software distribution.
   d. make other distribution arrangements with the author.

3. You may distribute the software in object code or binary form, provided that you do at least ONE of the following:
   a. distribute the binaries and library files of the software, together with instructions (in the manual page or equivalent) on where to get the original distribution.
   b. accompany the distribution with the machine-readable source of the software.
   c. give non-standard binaries non-standard names, with instructions on where to get the original software distribution.
   d. make other distribution arrangements with the author.
4. You may modify and include the part of the software into any other software (possibly commercial). But some files in the distribution are not written by the author, so that they are not under these terms.

   For the list of those files and their copying conditions, see the file LEGAL.
5. The scripts and library files supplied as input to or produced as output from the software do not automatically fall under the copyright of the software, but belong to whomever generated them, and may be sold commercially, and may be aggregated with this software.
6. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

RUBY ON RAILS

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

ZFS

COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 1.0

INCLUDED PACKAGES

alsa-lib-1.1.2

apr-1.6.2.1.6.0

atf-0.21

avahi-app-0.7_2

bash-4.4.12_2

black_pearl-2.3_1

bluestorm_backend-2.0.1699941_7

bluestorm_frontend-2.1.1719512

bluestorm_gui-2.0.1717812_2

bluestorm_mgmt-2.0.1716751

bluestorm_tests-2.0.1657344_1

bluestorm_workers-2.0.1719648_6

boost-libs-1.64.0

c-ares-1.12.0_1

ca_root_nss-3.31

cdbcmd-0.0.1666162,1

cmocka-1.1.1_1

compat10x-amd64-10.3.1003000.20170608

cscope-15.8b

ctags-5.8

curl-7.61.1

cyrus-sasl-2.1.26_12

dbus-1.10.16_1

dbus-glib-0.108

dejavu-2.37

dmidecode-3.1_1

ds3-3.2.0.1701306

e2fsprogs-libuuid-1.43.4

expat-2.2.1
fieldmod-1.0.0.1366684
fio-2.21
fontconfig-2.12.1,1
freetype2-2.8
fsx-1.0.1657335_1
fusefs-libs-2.9.5
gamin-0.1.10_9
gdb-7.12.1_2
gdbm-1.13_1
gettext-runtime-0.19.8.1_1
glib-2.50.2_3,1
gmp-6.1.2
gnome_subr-1.0
gnupg-2.1.21_2
gnutls-3.6.6_1
go-1.10.1,1
gobject-introspection-1.50.0,1
icu-58.2_2,1
indexinfo-0.2.6
iozone-3.457
iperf-2.0.9
iperf3-3.2
ipmitool-1.8.18_1
jakarta-commons-daemon-1.0.15
jansson-2.12
java-zoneinfo-2017.b
javavmwrapper-2.5_2
ksh93-20120801_2
kyua-0.13_4,3
libarchive-3.3.3,1
libassuan-2.4.3
libdaemon-0.14_1
libedit-3.1.20170329_2,1

libevent-2.1.8
libffi-3.2.1
libfontenc-1.1.3_1
libgcrypt-1.8.3
libgpg-error-1.27
libiconv-1.14_10
libinotify-20180201_1
libksba-1.3.5
liblz4-1.7.5,1
libnghttp2-1.33.0
libsmi-0.4.8_1
libsunacl-1.0.1
libtasn1-4.12
libunistring-0.9.7
libunwind-20170113_1
libuv-1.18.0
libxml2-2.9.7
libxslt-1.1.29_1
libyaml-0.1.6_2
lnav-0.8.2_1
logrotate-3.9.2
lua52-5.2.4
lutok-0.4_6
lzo2-2.10_1
mbuffer-2016.06.13
mhash-0.9.9.9_4
mkfontdir-1.0.7
mkfontscale-1.1.2
monit-5.23.0_4
mtx-1.3.12_1
ncurses-6.0_3
net-snmp-5.7.3_17
netperf-2.7.0
nettle-3.4.1_1

nginx-1.12.2,2
node8-8.11.4_1
npth-1.5
openjdk8-8.131.11
openldap-sasl-client-2.4.45
p4-2016.1.1492381
pcre-8.40_1
pdksh-5.2.14p2_6
perl5-5.24.4
pgbadger-9.1
pinentry-1.0.0_2
pinentry-tty-1.0.0
pkg-1.10.1
popt-1.16_2
postgresql96-client-9.6.10
postgresql96-contrib-9.6.10
postgresql96-server-9.6.10
py27-dnspython-1.15.0
py27-iso8601-0.1.11
py27-setuptools-36.0.1
python2-2_3
python27-2.7.15
readline-7.0.3
redis-3.2.9
rrdtool-1.6.0_2
ruby-2.4.5,1
ruby24-gems-2.6.14
rubygem-actioncable5-5.1.2
rubygem-actionmailer5-5.1.2
rubygem-actionpack5-5.1.2
rubygem-actionview5-5.1.2
rubygem-activejob5-5.1.2
rubygem-activemodel-serializers-xml-1.0.1
rubygem-activemodel5-5.1.2

rubygem-activerecord-import-0.19.0_1
rubygem-activerecord5-5.1.2
rubygem-activeresource5-5.0.0
rubygem-activesupport4-4.2.9
rubygem-activesupport5-5.1.2
rubygem-addressable-2.5.1
rubygem-arel-8.0.0,1
rubygem-aws-sdk-2.10.9
rubygem-aws-sdk-core-2.10.9
rubygem-aws-sdk-resources-2.10.9
rubygem-aws-sigv4-1.0.0
rubygem-azure-0.7.9
rubygem-azure-core-0.1.8
rubygem-backports-3.8.0
rubygem-bindex-0.5.0
rubygem-bluestorm_cli-3.0.0.1709633
rubygem-builder-3.2.3
rubygem-bundler-1.15.1
rubygem-byebug-9.0.6
rubygem-capybara-2.14.4
rubygem-childprocess-0.7.1
rubygem-coffee-rails-rails5-4.2.2
rubygem-coffee-script-2.4.1
rubygem-coffee-script-source-1.12.2
rubygem-colorize-0.8.1
rubygem-concurrent-ruby-1.0.5
rubygem-cookiejar-0.3.3
rubygem-crass-1.0.2
rubygem-cucumber-2.4.0_2
rubygem-cucumber-core-2.0.0_2
rubygem-cucumber-wire-0.0.1
rubygem-daemons-1.2.4
rubygem-devdctl-0.1.0.1652489
rubygem-devstat_stat-0.0.1.1280468

rubygem-diff-lcs-1.3
rubygem-digest-crc-0.4.1
rubygem-docile-1.1.5
rubygem-ds3-0.0.1.1358398
rubygem-ds3apitest-0.1.0.1366684_6
rubygem-ejs-1.1.1
rubygem-em-http-request-1.1.5
rubygem-em-socksify-0.3.1
rubygem-erubi-1.6.1
rubygem-eventmachine-1.2.3
rubygem-execjs-2.7.0
rubygem-faraday-0.13.0
rubygem-faraday_middleware-0.12.2
rubygem-faye-1.2.4
rubygem-faye-websocket-0.10.7
rubygem-ffi-1.9.18
rubygem-ffi-locale-1.0.1_2
rubygem-ffi-ncurses-0.4.0_3
rubygem-fio_rb-1.1.0.1141562
rubygem-freebsd_cam-1.0.6.1687748
rubygem-freebsd_mps-1.1.1.1325934
rubygem-freebsd_ses-1.3.2.1325934
rubygem-gherkin-4.1.3
rubygem-globalid-rails5-0.4.0
rubygem-http_parser.rb-0.6.0
rubygem-i18n-0.8.6,2
rubygem-i18n-js-3.0.0
rubygem-inifile-3.0.0
rubygem-ipaddress-0.8.3_4
rubygem-jasmine-2.6.0
rubygem-jasmine-core-2.6.4
rubygem-jbuilder-rails5-2.7.0
rubygem-jmespath-1.3.1
rubygem-jquery-rails-rails5-4.3.1

rubygem-json-2.1.0
rubygem-json_pure-2.1.0
rubygem-key_verify-1.0.1.1660612
rubygem-libifconfig-0.1.0.1366684_1
rubygem-libxml-ruby-3.0.0
rubygem-live_record-0.2.1.1638336
rubygem-liveresource-2.1.2.1638704
rubygem-loofah-2.2.3
rubygem-lsiexp-1.2.4.1669735
rubygem-mail-2.6.6,2
rubygem-metaclass-0.0.4
rubygem-method_source-0.8.2
rubygem-mime-types-3.1
rubygem-mime-types-data-3.2016.0521
rubygem-minitest-5.10.2
rubygem-mocha-1.2.1
rubygem-multi_json-1.12.1
rubygem-multi_test-0.1.2_1
rubygem-multipart-post-2.0.0
rubygem-net-ping-1.7.8
rubygem-net-scp-1.2.1
rubygem-net-ssh-4.1.0,2
rubygem-nio4r-2.1.0
rubygem-nokogiri-1.8.0_1
rubygem-open4-1.3.4
rubygem-os-1.0.0
rubygem-pam-1.5.2.1082167
rubygem-passenger-5.1.11
rubygem-pg-0.21.0
rubygem-phantomjs-2.1.1.0
rubygem-pkg-config-1.2.3
rubygem-pmbus-1.1.2.1718448
rubygem-power_assert-1.0.2
rubygem-pqueue-2.1.0

rubygem-pretty-xml-0.2.2
rubygem-public_suffix-2.0.5_7
rubygem-puma-3.9.1
rubygem-rack-2.0.5,3
rubygem-rack-test-0.6.3_1
rubygem-rack16-1.6.8
rubygem-rails-deprecated_sanitizer-rails5-1.0.3
rubygem-rails-dom-testing-rails5-2.0.3
rubygem-rails-html-sanitizer-1.0.4
rubygem-rails5-5.1.2
rubygem-railties5-5.1.2
rubygem-rake-12.0.0_1
rubygem-rb-kqueue-0.2.5
rubygem-rbcurse-1.5.3
rubygem-rbcurse-core-0.0.14_1
rubygem-rbcurse-extras-0.0.0
rubygem-rdoc-4.3.0_1
rubygem-redis-3.3.3
rubygem-redis-actionpack-rails5-5.0.1_1
rubygem-redis-activesupport-rails5-5.0.3
rubygem-redis-rack-2.0.2
rubygem-redis-rails-rails5-5.0.2
rubygem-redis-store-1.3.0
rubygem-rice-2.1.1
rubygem-rrd-ffi-0.2.14_3
rubygem-rspec-expectations-3.6.0
rubygem-rspec-support-3.6.0
rubygem-ruby-termios-1.0.2
rubygem-rubyzip-1.2.1
rubygem-sass-3.4.25
rubygem-sass-rails-rails5-5.0.6
rubygem-selenium-webdriver-3.4.3
rubygem-simplecov-0.14.1
rubygem-simplecov-html-0.10.1

rubygem-smart_data-0.0.2.1359693
rubygem-snmp-1.1.1
rubygem-spectra_acl-1.2.1.1657344_1
rubygem-spectra_cli-1.0.2.1709633
rubygem-spectra_platform-1.3.1.1686790
rubygem-spectra_support-5.0.0.1644282
rubygem-spectra_view-2.3.0.1719690_7
rubygem-spectra_workers-5.0.0.1718457
rubygem-spring-rails5-2.0.2
rubygem-sprockets-rails-rails5-3.2.0
rubygem-sprockets3-3.7.1_1
rubygem-sqlite3-1.3.13
rubygem-staf4ruby-0.1.3.1325934,1
rubygem-systemu-2.6.4
rubygem-tape_backend-0.1.1671618
rubygem-test-unit-3.2.5
rubygem-thin-1.7.2
rubygem-thor-0.19.4
rubygem-thread_safe-0.3.6
rubygem-tilt-2.0.7
rubygem-turbolinks-rails5-5.0.1
rubygem-turbolinks-source-5.0.3
rubygem-tzinfo-1.2.3
rubygem-uglifier-3.2.0
rubygem-uuidtools-2.1.5
rubygem-web-console-3.5.1
rubygem-websocket-driver-0.6.5_1
rubygem-websocket-extensions-0.1.2
rubygem-xpath-2.1.0
rubygem-yard-0.9.9
rubygem-zfs-0.0.12.1642179
samba48-4.8.11_2
sedutil-1.0.1643852
sg3_utils-1.42

smartmontools-7.0

smp_utils-0.98_1

spectra_ltfs-2.4.1.0.1698234_2

sqlite3-3.22.0_1

staf-3.4.23_3

t5seeprom-0.0.1366684_1

talloc-2.1.14

tdb-1.3.16,1

tevent-0.9.37

tidy-html5-5.4.0_2

tmux-2.5

tomcat-native-1.2.12

tomcat85-8.5.16_1

verde_hotpair-2.1.1679414

vim-8.0.0702

xproto-7.0.31

zip-3.0_1

zsh-5.3.1_1

INDEX

A

Activation keys
  importing automatically 43
activation keys, enter 127
Active Directory, join 63
agency declarations
  CE marking 229
  certifications 228
  conflict mineral policy 230
  EU declaration of conformity 227
  FCC 229
  RoHS 230
  safety standards and compliance 229
  WEEE 229
Apache, open source acknowledgement 231
automated software upload
  configuring 160
AutoSupport
  about 147
  configure log set schedule 152
  configure mail recipient 148
  delete log set 154
  download log set 154
  email log set 153
  enter contact information 147
  generate log set 153
  log set 151

B

bezel, removing 167
browsers, supported 37

C

CE marking 229
certificates
  configure 126
certifications 228
CIFS
  about 33
  create new share 63
  edit share 92
  remove sharing 93
  set permissions 65
CIFS service
  configuring 69
command line interface 37
component OK icon 37
components
  front view 21, 221
  rear panel 25, 223
configuring
  automated software upload 160
  certificates 126
  CIFS service 69
  date and time 109
  DNS 107
  email 108
  Ethernet ports 101
  mail recipients 148
  network connections 101
  NFI service 69
  NFS service 70
  NTP 109
  services 68
  shares 63
  SMTP 108
  snapshots 84
  SNMP 117
  storage pools 57
  system name 110
  user 125
  Visual Status Beacon 132
  volumes 60
conflict mineral policy 230
contact information, enter 147
contacting
  Technical Support 179
contacting Spectra Logic 7
corporate headquarters, Spectra Logic 7

D

dashboard 34
data drive
  install new 168
  remove 167
data integrity verification 156
data ports, configure 46
Deep Storage Browser
  configuring 200
  installing 199
  retrieving a file 202
DNS, configure 107
documentation
  typographical conventions 16
drive, install new 166

E

email
  configuring 108
  send test 150
  Spectra Logic offices 7
error condition icon 37
Ethernet ports, configure 101
EU declaration of conformity 227

F

fax numbers, Spectra Logic 7
FCC notice 229
Free BSD
  about 33
  open source acknowledgement 231
front view 21, 221

H

hardware
monitor status 135

I

icons
component OK 37
error condition 37
information 37
unknown state 37
warning 37
information icon 37

J

Java
open source acknowledgement 232

L

LEDs
data drives 22, 27, 221
system status 133
license agreement, software 3
log on 44
log sets 151
configure a schedule 152
delete 154
delete a schedule 154
download 154
emailing 153
generate 153
types 151
logical volume manager and file system, about 33

M

mail recipients
add 148
configure 148
delete 151
edit 149
mailing address, Spectra Logic 7
maintenance, replace component 169
management port
configure 102
conflicting address 173
MIB, download 118

N

NAS volumes
edit share 92
network
cables 214, 226
configure 101
configure DNS 107
NFI
configure 191
configure schedule 195
configure versioning 188
configure volume 192
overview 186
requirements 186
restore files 197
NFI service
configuring 69
edit 191
NFS
about 33
create new share 67
edit share 92
remove sharing 93
NFS service
configuring 70
Nginx, open source acknowledgement 240
NTP
configuring 109

O

open source acknowledgement
Apache 231
Free BSD 231
included packages 243
Java 232
Nginx 240
Ruby 241
Ruby on rails 242
ZFS 243

P

performance metrics 141
phone numbers, Spectra Logic offices 7
ping, tool 178
pools, see storage pools 56
portal
creating an account 157
log in 159
power
power off 144
power on 39
reboot 144
requirements 209

R

rear panel 25, 223
rear view 23, 28, 222
reboot 144
remote support 183
disabling 185
enabling 184
replication
cancel replication in progress 95
configure 71
configure folders 73
configure replication service 70
configure schedule 74
configure target system 73
delete 98

replication (*continued*)
disable 96
edit configuration 97
manual 94
restore files from a replication target 96
reports 143
RoHS 230
Ruby on rails, open source acknowledgement 242
Ruby, open source acknowledgement 241

S

safety standard and compliance 229
sales, contacting 7
serial number 180
services
CIFS 69
configuring 68
NFI 69
NFS 70
SNMP 117
status 140
shares
about 56
configuring 63
create new CIFS 63
create new NFS 67
delete 93
edit 92
manage 92
view status 139
shutdown 144
SMTP
configuring 108
snapshots
about 84
configuring 84
create new 85
daily, create 75, 87
delete 89
hourly, create 74, 86
restore 90
retrieve single file 91
scheduled, about 86
weekly, create 76, 87
SNMP
configuring 117
SNMP service
configure 112
software
automated software upload 160
license agreement 3
updating 161
software version
check current available version 162
check current installed version 161
specifications
capacity 205
data storage 204
environmental 215
interface 213, 225
network cables 214, 226
power 209
power cords 211
size and weight 207
system 206, 224
Spectra Logic
contacting 7
manuals, obtaining 16
status icons 37
storage pools
about 56
create new 57
delete 80
expand 79, 79
options 59
protection levels 59
requirements 57
view status 136
support
contacting 179
opening ticket 180
support portal
accessing 157
support ticket
sending 181
system messages 134
system name
configuring 110
system status LEDs 133

T

technical support
contacting 7
creating a portal account 157
log in 159
tools 178
ping 178
traceroute 179
traceroute, tool 179
troubleshooting
contacting support 179
management port IP conflict 173
network setup 175
typographical conventions 16

U

unknown state icon 37
updating
software 161
USB, support 214
user
configure 125
edit 125, 125
types 125

V

Verde
components 21 to 26, 221 to 223
features 19
monitoring 130
overview 19
size and weight 207
software 33
specifications 206, 224
Verde software
current available version 162
current installed version 161
download new version 163
updating 161

Verde web interface
about 33
dashboard 34
log in 44
log out 145
menus 34
status icons 37
supported browsers 37
Visual Status Beacon
configuring 132
lights 131
volumes
about 56
configure 60
create new CIFS share 63
create new NFS share 67
create snapshot 85
delete 84
delete snapshot 89
edit 82
move 81
options 61, 193, 194
remove sharing 93
restore file from snapshot 91
restore snapshot 90
scheduled snapshots 86
snapshot restore 90
snapshots 84
view status 139

W

warning icon 37
website
obtaining Spectra Logic manuals 16
Spectra Logic 7
WEEE 229

Z

ZFS, open source acknowledgement 243