



SPECTRA LOGIC BLACKPEARL NAS

USER GUIDE

SpectraLogic.com

COPYRIGHT

Copyright © 2019-2026 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

ArcticBlue, BlackPearl, BlueScale, RioBroker, Spectra Cube, Spectra Logic, Spectra Vail, Spectra, SpectraGuard, StorCycle, TeraPack, TFinity, and TranScale are registered trademarks of Spectra Logic Corporation. All rights reserved worldwide. All other trademarks and registered trademarks are the property of their respective owners.

PART NUMBER

90990143 Revision J

REVISION HISTORY

Revision	Date	Description
G	February 2024	Updated for the BlackPearl Gen3 H series chassis and BlackPearl OS 5.7.3.
H	April 2025	Updated for the BlackPearl Gen 3 F Series chassis and BlackPearl OS 5.8.
I	September 2025	Updated for the BlackPearl OS 5.8.2 release and the Gen3 H 3310 chassis.
J	May 2026	Updated to BlackPearl Storage Manager and BlackPearl OS 5.9.2.

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

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:

- 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.
- 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");

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. 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.

SYSTEM BIOS

Resetting the system BIOS when not authorized by Spectra Logic Technical Support invalidates the system configuration. Spectra Logic reserves the right to charge for time and materials to reconfigure and recertify the system.

CONTACTING SPECTRA LOGIC

To Obtain General Information	
Spectra Logic Website: spectrallogic.com	
United States Headquarters	European Office
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	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.spectrallogic.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
Additional international numbers available at support.spectrallogic.com/home If you have a Spectra Logic Portal account, please log in for country-specific numbers at support.spectrallogic.com/support-contact-info	
Spectra Logic Sales	
Website: shop.spectrallogic.com	
United States and Canada Phone: 1.800.833.1132 or 1.303.449.6400 Fax: 1.303.939.8844 Email: sales@spectrallogic.com	Europe Phone: 44 (0) 870.112.2150 Fax: 44 (0) 870.112.2175 Email: eurosales@spectrallogic.com
To Obtain Documentation	
support.spectrallogic.com/documentations	

TABLE OF CONTENTS

Contacting Spectra Logic	7
Table of Contents	8
About This Guide	15
Intended Audience	15
Discontinued Components	15
BlackPearl User Interface Screens	15
Related Information	16
Related Publications	16
Spectra Logic Software User Guides	17
What's New	18
Chapter 1 - Product Overview	19
Overview	20
Features	20
Components	25
Front Bezel	25
Gen3 F Series	26
Gen3 H Series	30
Gen2 X Series	35
Gen2 S Series and Gen2 V Series	39
77-Bay and 107-Bay Expansion Nodes	46
Gen1 S Series, Gen1 P Series, and Gen1 V Series	48
44-Bay Expansion Node	54
96-Bay Expansion Node	57
Software	59
Operating System	59
Logical Volume Manager and File System	59
NFS and CIFS Servers	59
Command Line Interface	60
Chapter 2 - Configuring Initial Settings	61
Before You Begin	62
Install HBAs	62
Rackmount the Chassis	62

Install Drives	62
Connect Ethernet Cables	62
Power On the	63
Configure the BlackPearl Management Port	65
Log Into the BlackPearl User Interface	68
Configure the Data Connection	70
Configure an Aggregate Port Data Connection	70
Configure a Single Port Data Connection	72
Configure a Static Route	74
Create a User	76
Description of User Permissions	76
Create a User	77
Next Steps	79
Chapter 3 - Configuring Network Settings	80
Networking Best Practices	81
Configuration Method	81
Supported Network Connectivity	81
Required Open Firewall Ports	81
MTU Settings	82
Link Aggregation	82
Link Aggregation Port Utilization	83
Network Connectivity Tools	83
Troubleshooting	84
Configure Certificates	85
Configure Network Settings	87
Configure DNS Settings	87
Configure SMTP Settings	88
Configure Date and Time	89
Change the System Name	89
Configure Networking Services	91
Configure the Active Directory Service	91
Configure the SNMP Service	95
Configure Network Connections	97
Configure Ethernet Ports	97

Chapter 4 - Configuring Network Attached Storage	100
Create a NAS Storage Pool	101
Create a Volume	104
Create a NFS Share	108
Create a CIFS Share	110
Access Control for a CIFS Share	110
Create a CIFS Share	110
Set Permissions for a CIFS Share	113
Configure NFS and CIFS Services	115
Configure the NFS Service	115
Configure the CIFS Service	115
Configure NAS Replication	116
Add a NAS Target	117
Configure the Target System	118
Configure Volumes for NAS Replication	119
Chapter 5 - Configuring Security and Data Protection Features	122
Volume Snapshots	123
Create a Snapshot	123
Configure a Snapshot Schedule	125
Delete Snapshots	127
Delete a Snapshot Schedule	128
Restore to a Snapshot	129
Retrieve a Single File from a Snapshot	130
Multi-Factor Authentication	132
Enable Multi-Factor Authentication for a User	132
Log In to a System Configured to Use Multi-Factor Authentication	133
Update Multi-Factor Authentication for a User	134
Disable Multi-Factor Authentication for a User	135
Disable the Attack Hardened Service	136
Configure and Use Encryption	137
Configure the Encryption Service	137
Export Encryption Key to USB Drive	139
Change the Encryption Password	140
Unlock the Self-Encrypting Drives	141
PSID Erase an Encryption Drive	142

Chapter 6 - Additional Configuration Options	144
Configure Users	145
Description of User Types	145
Create a User	145
Edit a User	145
Delete a User	146
Chapter 7 - Managing Network Attached Storage	148
Manage NAS Replication	149
Manually Start NAS Replication	149
Restoring Files from a NAS Replication Target	149
Chapter 8 - Monitor the BlackPearl Solution	151
View System Messages	152
Types of Message Severity	152
View System Messages	153
View Performance Metrics	154
View Reports	156
Enable Remote Logging	157
Chapter 9 - BlackPearl NAS Hardware Operations	158
Monitor the Hardware	159
Front Bezel Visual Status Beacon	159
Configuring the Visual Status Beacon Color	161
Flash the Visual Status Beacon	162
System Status LEDs	163
View the Status of Hardware Components	167
Data Drive Status Definitions	168
View the Status of NAS Pools	169
View the Status of NAS Volumes	172
Reboot or Shut Down a BlackPearl NAS	174
Using the BlackPearl User Interface	174
Power-Cycle Reset	175
Replace a Failed Component	176
Identify the Failed Component	176
Activate Chassis Beacon	177
Replace the Failed Component	178
Installing Data Drives	179

Ensure ESD Protection	179
Install a Drive in a Gen3 H Series Chassis	180
Install a Drive in a Gen2 S Series Chassis	187
Install a Drive in a Gen2 V Series Chassis	188
Install a Drive in a Gen2 X Series Chassis	189
Install a Drive in a Gen1 Chassis	191
Chapter 10 - Maintaining the BlackPearl NAS Solution	194
Data Integrity Verification	195
Start Disk Media Data Integrity Verification	195
Cancel Disk Media Data Integrity Verification	196
Initiate RSC Backup	197
Manually Enter Activation Keys	198
Chapter 11 - Technical Support	199
About AutoSupport	200
Configure AutoSupport Mail Recipients	201
Create a New Mail Recipient	201
Edit a Mail Recipient	202
Send a Test Email	203
Delete a Mail Recipient	203
Log Sets	205
Configure a Log Set Schedule	206
Manually Generate Log Sets	207
Email a Log Set	208
Download a Log Set	209
Delete Log Sets	209
Access the Technical Support Portal	211
Create an Account	211
Log Into the Portal	212
Spectra Logic Technical Support	213
Before Contacting Support	213
Determine the Serial Number	213
Opening a Support Ticket	214
Search for Help Online	214
Submit an Incident Online	217
Submit an Incident by Phone	219

Remote Support	220
Enabling Remote Support	220
Disabling Remote Support	221
Chapter 12 - Frequently Asked Questions (FAQ)	222
Resolve a BlackPearl Management Port IP Address Conflict	223
Using the Console	223
Using a Separate Computer	223
Appendix A - IPMI Configuration	226
Appendix B - Specifications	230
Data Storage Specifications	231
System Specification	234
Size and Weight	238
Environmental Specifications	244
Temperature & Humidity	244
Heat Generation	249
Power Requirements	249
Input Power Requirements	249
Power Cord Specifications	252
Interface Specifications	255
System Interface Connectors	255
Expansion Node Interface Connectors	259
Network Interface Cables	259
Networking Naming Conventions	260
Universal Serial Bus (USB) Support	261
Appendix C - Regulatory & Safety Standards	262
EU Declaration of Conformity	263
Certifications	265
CE Marking	266
FCC Notice	266
Class A Emissions Warning	266
Laser Warning	267
Safety Standards and Compliance	268
Waste of Electronic and Electrical Equipment (WEEE) Directive	268

Restriction of Hazardous Substances in Electrical and Electronic Equipment (RoHS)	268
Conflict Minerals Policy	269
Recycling Your System	269
Appendix D - Open Source Code Acknowledgments & Package List	270
Apache	271
FreeBSD	272
Java	273
Samba	280
Nginx	281
Ruby	282
Ruby on Rails	283
ZFS	284
Included Packages	285
Index	309

ABOUT THIS GUIDE

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

This guide also describes the Spectra 44-bay expansion node, the 96-bay expansion node, the 77-bay expansion node, and the 107-bay 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 BlackPearl NAS master node and expansion nodes, *the system* is used to refer to both.

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 and with network connectivity protocols such as SAS and Ethernet. You also need to be familiar with installing, configuring, and using data file storage and data management software.

DISCONTINUED COMPONENTS

To view information about discontinued components of the BlackPearl NAS, log into the Support portal (see [Access the Technical Support Portal on page 211](#)), and navigate to **Documentation > Product Life Cycle Information**.

BLACKPEARL USER INTERFACE SCREENS

The BlackPearl user interface changes as new features are added or other modifications are made between software revisions. Therefore, the screens you see in the BlackPearl 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 BlackPearl NAS.

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 hardware 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

For additional information about the Spectra BlackPearl NAS, refer to the publications listed in this section.

Spectra BlackPearl NAS

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

- The *Spectra BlackPearl NAS Solution Gen1 Installation Guide* provides detailed instructions for installing a Gen1 BlackPearl NAS.
- The *BlackPearl NAS Quick Start Guide* provides instructions to rack mount and configure a Gen2 BlackPearl NAS solution.
- The *Spectra BlackPearl Network Setup Tips* document provides helpful instructions for troubleshooting common connectivity problems.

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

- The *Spectra BlackPearl Release Notes and Documentation Updates* provide the most up-to-date information about the BlackPearl NAS, including information about the latest software releases and documentation updates.
- The *Spectra 96-Bay Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive in the 96-bay expansion node.
- The *Spectra 96-Bay Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in the 96-bay expansion node.
- The *Spectra 96-Bay Chassis Power Supply Replacement Guide* provides instructions for replacing a failed power supply in the 96-bay expansion node.
- The *Spectra 96-Bay Chassis I/O Module Replacement Guide* provides instructions for replacing a failed I/O module in the 96-bay expansion node.
- The *Spectra 107-Bay Expansion Node FRU Guide* provides instructions for replacing fans, power supplies, drives, and SAS expanders in the 77-bay and 107-bay expansion node.
- The *Spectra BlackPearl H-Series Chassis Part Replacement Guide* provides instructions for replacing parts in the Spectra BlackPearl H-series chassis.

Spectra Logic Software User Guides

The guides for this section are for other Spectra Logic products that use the BlackPearl NAS as a core component.

- *Spectra Object Manager (formerly Vail) User Guide*
- *Spectra StorCycle User Guide*
- *Spectra Rio MediaEngine User Guide*

WHAT'S NEW

BlackPearl OS 5.9.2 brings with it the following changes and improvements:

User Interface Improvements

Multiple changes have been made to the BlackPearl user interface introduced in BlackPearl OS 5.9 to expand its feature set and improve user experience.

CHAPTER 1 - PRODUCT OVERVIEW

This chapter provides an overview of the Spectra Logic BlackPearl NAS features and components.

Overview	20
Features	20
Components	25
Front Bezel	25
Gen3 F Series	26
Gen3 H Series	30
Gen2 X Series	35
Gen2 S Series and Gen2 V Series	39
77-Bay and 107-Bay Expansion Nodes	46
Gen1 S Series, Gen1 P Series, and Gen1 V Series	48
44-Bay Expansion Node	54
96-Bay Expansion Node	57
Software	59
Operating System	59
Logical Volume Manager and File System	59
NFS and CIFS Servers	59
Command Line Interface	60

OVERVIEW

The BlackPearl NAS 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 BlackPearl NAS has 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 BlackPearl NAS includes the following features:

Attack Hardening

The BlackPearl NAS provides safeguards to protect against outside threats to your data. These features are critical to maintaining control of data in the case of ransomware attacks.

Immutable data snapshots, generated by trigger or on a configurable schedule, allow you to restore your data to a moment in time before the attack.

BlackPearl User Interface

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

Command Line Interface

The BlackPearl NAS can be configured, monitored, and maintained using a command line interface. The command line interface is documented in the [*Spectra BlackPearl NAS Solution Command Line Interface Guide*](#).

Easy Network-Based Administration

The BlackPearl NAS can be configured over an Ethernet network using a standard web browser.

Mirrored Boot Drives

The operating system is hosted on two mirrored drives.

Multi-Factor Authentication

The BlackPearl NAS offers multi-factor authentication, which enhances the security of your BlackPearl NAS by using an authenticator app to confirm the identity of any user trying to log in to the BlackPearl user interface. This prevents unauthorized access to the system even if the user credentials needed to access the system are compromised.

Rack-Mount Hardware

The BlackPearl chassis are 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. Rack-mounting hardware is included with each BlackPearl NAS.

Replicated Configuration

The BlackPearl NAS has mirrored system drives and replicates the data on the system drives to all data pools. If one or both boot drives fail, the recovers automatically when replacement boot drives are installed.

Redundant Hardware

The 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.

Network Attached Storage Features

Volume Snapshots

Volume Snapshots are images of a volume's configuration and data makeup as they were when the snapshot was generated. Snapshots are immutable and cannot be overwritten or altered. This protects against any data deletions, encryption, revision, alterations, or appendments. Restoring to triggered or time-based snapshots allow you to go "back in time" and restore the volume to the state it was in when the snapshot was created.

Snapshot Change Threshold

The BlackPearl NAS allows you to set a threshold for the amount of data in a snapshot that changes before a user is notified. Changes to the size of a snapshot may be caused by a ransomware attack

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®, macOS®, UNIX®, and Linux®. Solid state disk drives may be installed in your system to improve NFS performance.

Data Replication

You can select to replicate data from the NAS volumes on the BlackPearl NAS to one or more NAS replication targets.

Network File Interface

The Network File Interface (NFI) service allows you to automatically move data from your BlackPearl NAS to one or more BlackPearl NAS gateways, without the need to use a DS3 client. Data is transferred on a schedule and data copied from the BlackPearl NAS to the BlackPearl NAS can be configured to be kept on the BlackPearl NAS, or deleted. When a user needs access to data deleted from the BlackPearl NAS, the BlackPearl NAS copies it back to the BlackPearl NAS.

RAID-Protected Data Disks

Data drives in the BlackPearl NAS provide the's storage capacity. Disk drives are grouped into protected volumes with selectable parity options and automatic data integrity verification to protect against data corruption.

Metadata Performance Drives

Metadata Performance Drives increase performance when searching metadata, restoring small files, and in deduplication operations. These drives are dedicated to storing metadata information about all objects on the pool and are useful if you search many files before restoring them.

Write Performance Drives

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

Optional Hardware Features

HotPair

Two BlackPearl master nodes, a Gen2 X Series or Gen3 master node with two server modules 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.

Expansion Nodes

Expansion nodes can be connected to a master node to increase over capacity of the. For Gen1 master nodes, the 44-bay expansion node holds up to 44 disk drives with an active bezel and the 96-bay expansion node holds up to 96 disk drives. For Gen1 and Gen2 master nodes, the 77-bay and 107-bay expansion node holds up to 77 or 107 drives, respectively.

Networking Interfaces

Gen3 Chassis

The BlackPearl Gen3 chassis offer Ethernet HBA in 10/25 Gbps or 40/100 Gbps speeds for the data connection. The management interface uses a 1 Gbps Ethernet port.

Gen2 Chassis

1 Gigabit Ethernet

For the Gen2 X Series chassis includes an onboard 1 Gigabit Ethernet port to access the BlackPearl User Interface.

For the Gen2 V Series chassis, two onboard 1 Gigabit copper ports (10GBase-T) provide Ethernet connectivity for the with one dedicated port used to access the BlackPearl user interface.

10GBase-T Ethernet Connectivity

For the Gen2 S Series chassis, two onboard 10 Gigabit copper ports (10GBase-T) provide Ethernet connectivity for the with one dedicated port used to access the BlackPearl user interface.

Optionally, the Gen2 S and V series may include a two-port 10GBase-T network interface card to provide a data connections between hosts and the BlackPearl NAS.

25 Gigabit Ethernet

For Gen2 S and V Series chassis, an optional dual port, 25 Gigabit Ethernet (25 GigE) network interface card can be installed to provide high-speed data connections between hosts and the BlackPearl NAS.

100 Gigabit Ethernet

For Gen2 X Series chassis, a dual port, 100 Gigabit Ethernet (100 GigE) network interface card is installed to provide Ethernet connectivity for the.

1 Gigabit IPMI

For all Gen2 Chassis, a 1 Gigabit Ethernet port provides access to the system IPMI interface. On the Gen2 X series, the IPMI port is integrated with the BlackPearl management port.

Gen1 Chassis

10GBase-T Ethernet Connectivity

Two onboard 10 gigabit copper ports (10GBase-T) provide Ethernet connectivity for the with one dedicated port used to access the BlackPearl user interface.

10GBase-T Ethernet

An optional dual port, 10 gigabit copper (10GBase-T) network interface card can be installed to provide high-speed data connections between hosts and the BlackPearl NAS.

10 Gigabit Ethernet

A dual port, 10 Gigabit Ethernet (10 GigE) network interface card is installed to provide high-speed data connections between hosts and the BlackPearl NAS.

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 BlackPearl NAS.

COMPONENTS

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

Front Bezel

All BlackPearl chassis include a front bezel, which is attached with magnets.

Note: For the 77-bay, 96-bay and 107-bay expansion node, the bezel is permanently attached.



Figure 1 A 4U BlackPearl chassis with front bezel and visual status beacon.

In most cases, the front bezel includes a visual status beacon light bar which provides status information for the. See [Monitor the Hardware on page 159](#) for information about the status indicated by each visual status beacon color/pattern.

Gen3 F Series

Front View

Figure 2 shows the components on the front of the Gen3 F Series BlackPearl NAS with the front bezel removed.

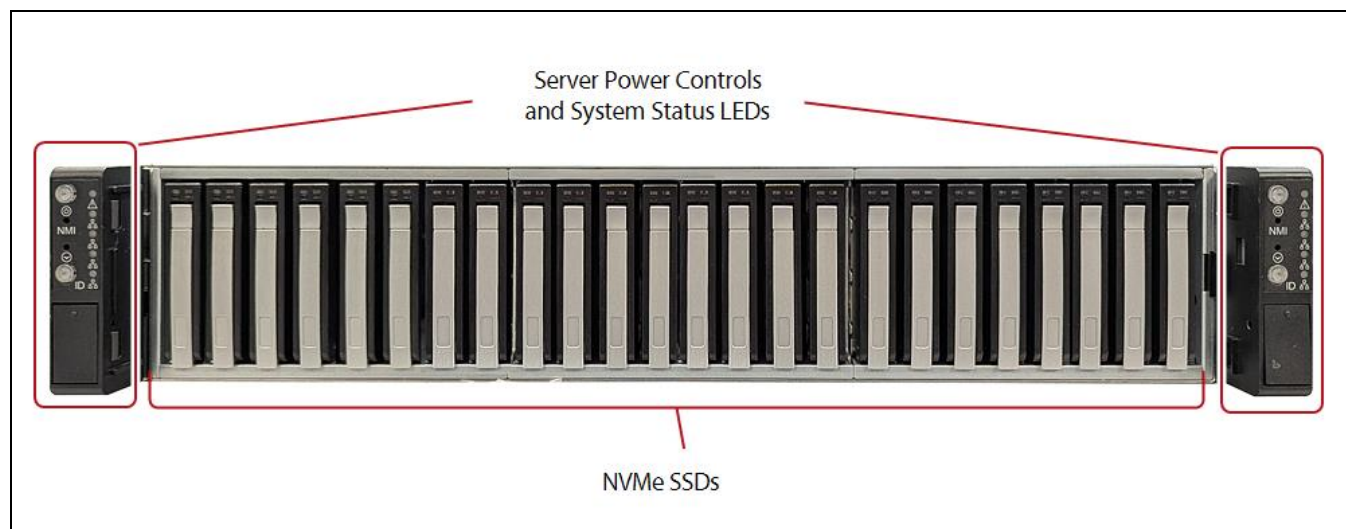


Figure 2 The front view of the Gen3 F Series BlackPearl NAS (front bezel removed).

Component	Description
Sever power controls	Power controls for each of the two installed server modules. The lower module uses the power controls on the left-hand side. The upper module (optional) uses the power controls on the right-hand side.
System status LEDs	The status LEDs indicate power status, server status, and the link status of motherboard Ethernet ports.
Data drives	The base Gen3 F Series BlackPearl NAS supports up to 24 high-performance NVMe drives mounted on individual drive sleds. The drive sleds slide into bays in the front of the chassis and lock in place. The front of each drive sled has a handle for removing the sled.
Data drive status LEDs	Two blue LEDs display drive status: • The left blue LED indicates drive activity. • The right red LED indicates a drive error.
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. Ensure each empty drive sled has a 'drive blank' installed in the sled for proper airflow and cooling.

Rear View

Figure 3 shows the major components on the rear of the Gen3 F series BlackPearl NAS.

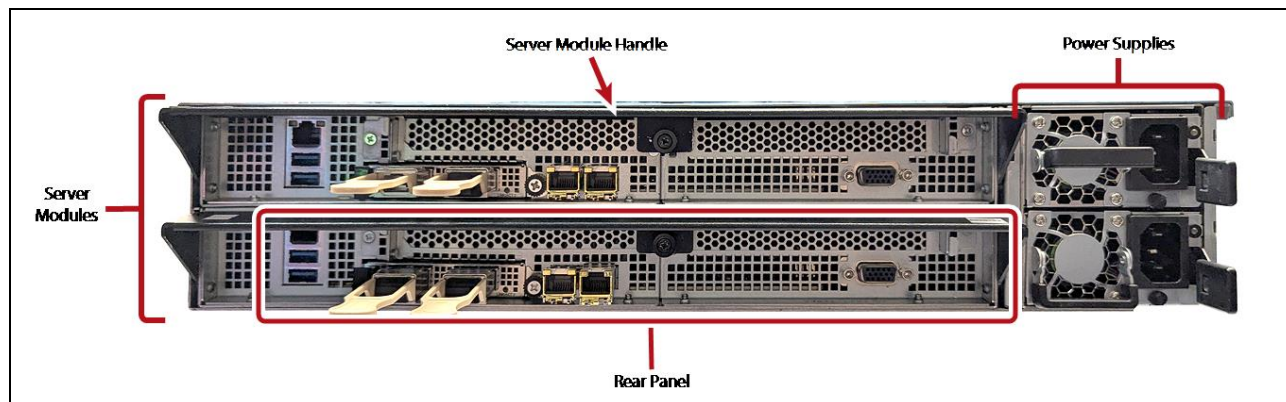


Figure 3 The rear view of the Gen3 F Series BlackPearl NAS.

Component	Description
Sever module	The BlackPearl Gen3 F series chassis supports up to two server modules. The bottom module is always installed. The top module is only installed in a HotPair configuration.
Rear panel	The rear panel of the Gen3 F Series BlackPearl server module allows for Ethernet, SAS, USB, IPMI, and other connections. See Rear Panel on the next page for a detailed description.
Power modules	The Gen3 F Series BlackPearl NAS includes two power modules. Each power module has active current sharing and supports N+1 redundancy. • Each power supply has its own AC power connector. • Each power supply has a bi-color LEDs to indicate power to the power module and status of the power module. • Not lit - Neither power module has AC power. • Amber solid - The power module experienced a critical event and shut down or the power cord is unplugged. • Green solid - The power module is on and OK.
Server module handle	The sever handle is used to install or uninstall the server module. When not in use, a thumbscrew locks the handle in place.

Rear Panel

Figure 4 shows the components on the rear panel of the Gen3 F Series BlackPearl master node.

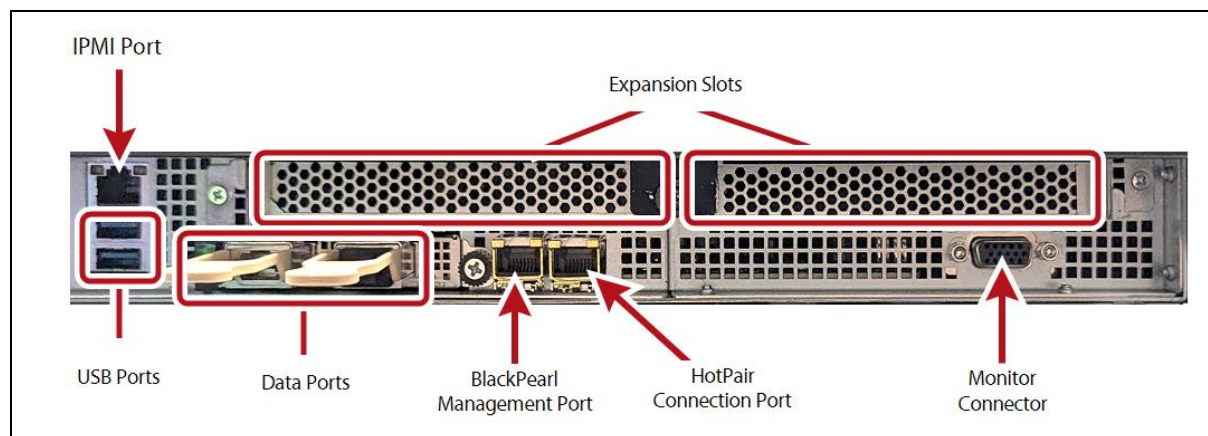


Figure 4 The Gen3 F Series BlackPearl rear panel components.

Component	Description
IPMI management port	See IPMI Configuration on page 226 for information on using IPMI management. The port has two status LEDs: • Activity / Link LED • Off - No Link • Blinking Amber - Data activity • On - Link • Speed LED • Off - Indicates 10 Mbps connection or no link • Amber - Indicates 100 Mbps connection • Green - Indicates 1 Gbps connection
USB ports	Four USB 3.1 Gen 1 Ports are available on the F Series BlackPearl chassis. If necessary, you can use these ports to connect a USB drive, or USB keyboard to the chassis for troubleshooting purposes as directed by Spectra Logic Technical Support.
Data Ports	Two 100 GigE ports provide the data connection to the BlackPearl NAS.
Expansion Slots	Two expansion slots provide support for either SAS or Fibre Channel connections.
BlackPearl management port	The BlackPearl management port is used to connect to a browser-based user interface to configure, manage, and monitor the BlackPearl NAS. The BlackPearl management port cannot be used for data transfer.

Component	Description
HotPair Connection port	The HotPair connection port is only used in a HotPair configuration.
Monitor connector	If necessary, you can connect a monitor to the VGA connector on the chassis for troubleshooting purposes. Only connect a monitor for initial configuration of the BlackPearl management port, or as directed by Spectra Logic Technical Support.

Internal Components

The following table describes the internal field replaceable components in the server module.

Internal Component	Description
Boot drives	Two NVMe M.2 boot drives provide high performance storage for the operating system and BlackPearl user interface. The NVMe M.2 boot drives are connected to the motherboard and are not hot-swappable.
Expansion slots and optional interface cards	The expansion slots accommodate optional interface cards to provide additional connectivity. • The Gen3 F series optionally includes: • Up to two optional four-port 12 GB SAS cards provide connectivity for up to eight 77-bay and 107-bay expansion nodes.

Gen3 H Series

Note: Except where noted, the information in this section applies to both the Gen 3 H 3310 and Gen 3 H 3300 series chassis.

Front View

Figure 5 shows the components on the front of the Gen3 H Series BlackPearl NAS with the front bezel removed.

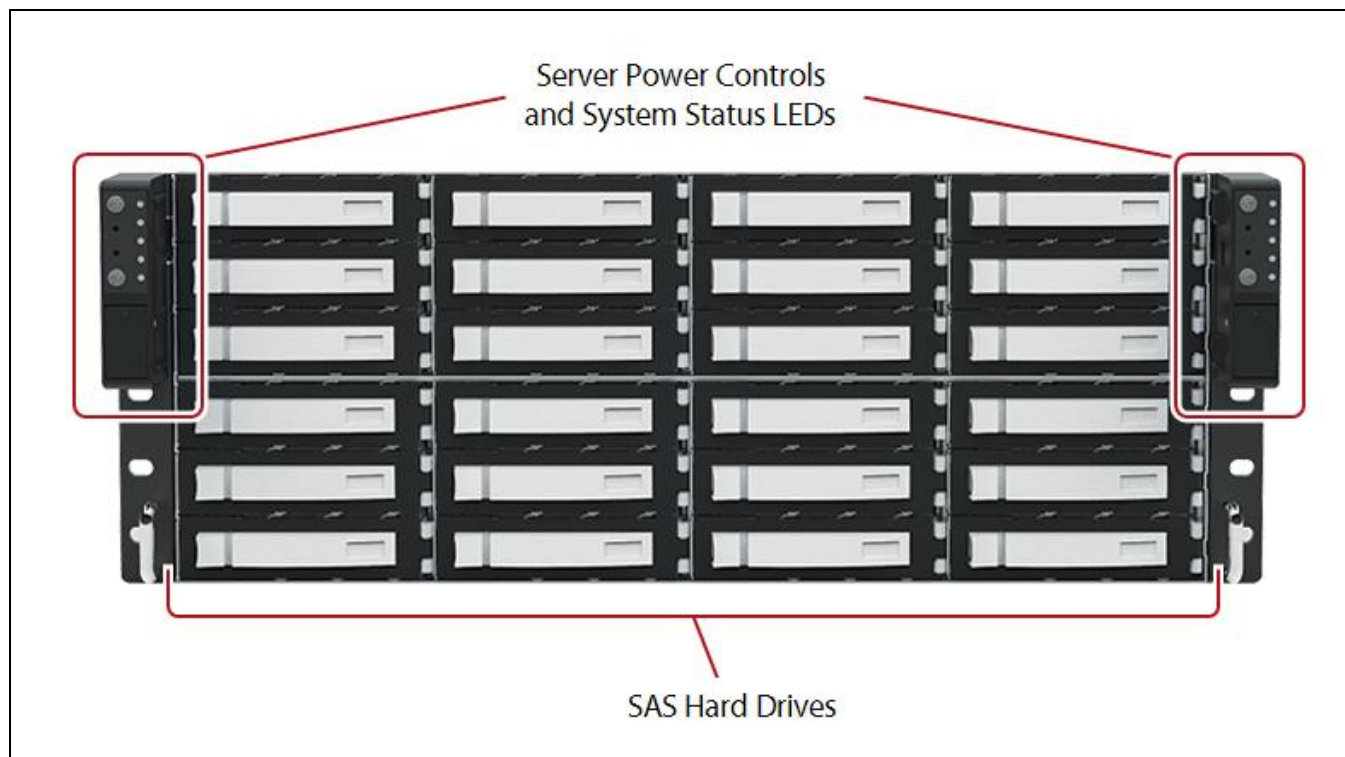


Figure 5 The front view of the Gen3 H Series BlackPearl NAS (front bezel removed).

Component	Description
Sever power controls	Power controls for each of the two installed server modules. The lower module uses the power controls on the left-hand side. The upper module (optional) uses the power controls on the right-hand side.
System status LEDs	The status LEDs indicate power status, server status, and the link status of motherboard Ethernet ports. Note: The LEDs are not visible with the bezel installed.
Data drives	The base Gen3 H Series BlackPearl NAS supports up to 24 high-performance SAS hard drives (HDDs) mounted on individual drive sleds.

Component	Description
	The drive sleds slide into bays in the front of the chassis and lock in place. The front of each drive sled has a handle for removing the sled.
Data drive status LEDs	Two blue LEDs display drive status: • The upper LED indicates drive activity. • The lower LED indicated a drive error. Note: The LEDs are not visible with the bezel installed.
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. Ensure each empty drive sled has a 'drive blank' installed in the sled for proper airflow and cooling.

Rear View

Figure 6 shows the major components on the rear of the Gen3 H BlackPearl NAS.

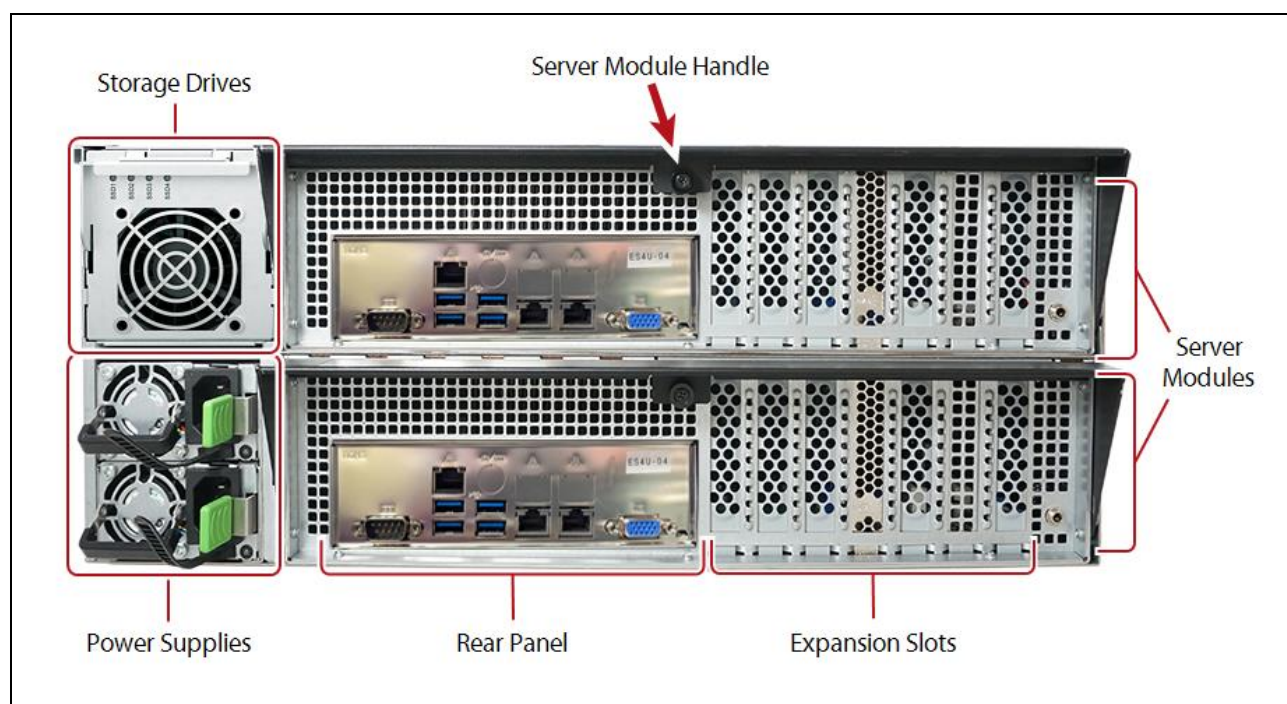


Figure 6 The rear view of the Gen3 H Series BlackPearl NAS.

Component	Description
Sever module	The BlackPearl Gen3 H chassis supports up to two server modules. The bottom module is always installed. The top module is only installed in a HotPair configuration.

Component	Description
Rear panel	The rear panel of the Gen3 H Series BlackPearl master node allows for Ethernet, SAS, USB, IPMI, and other connections. See Rear Panel on the next page for a detailed description.
Storage drives	The Gen 3 H Series supports up to four NVMe drives in the rear of the chassis for special allocation, metadata performance, and ZIL. Note: The Gen 3 H 3310 Series supports two additional NVMe drives mounted inside the chassis.
Expansion slots	The expansion slots in the Gen3 H series chassis allows for Ethernet, SAS, and Fibre Channel connections using optional HBA modules.
Power modules	The Gen3 H Series BlackPearl NAS includes two power modules. Each power module has active current sharing and supports N+1 redundancy. • Each power supply has its own AC power connector. • Each power supply has a bi-color LEDs to indicate power to the power module and status of the power module. • Not lit - Neither power module has AC power. • Amber solid - The power module experienced a critical event and shut down or the power cord is unplugged. • Green solid - The power module is on and OK.
Server module handle	The sever handle is used to install or uninstall the server module. When not in use, a thumbscrew locks the handle in place.

Internal Components

The following table describes the internal field replaceable components in the server module.

Internal Component	Description
Boot drives	Two NVMe M.2 boot drives provide high performance storage for the operating system and BlackPearl user interface. The NVMe M.2 boot drives are connected to the motherboard and are not hot-swappable.
Storage drives	The Gen 3 H 3310 Series supports two NVMe drives mounted inside the chassis for special allocation, metadata performance, and ZIL.
Midplane board	• The H 3300 Series chassis features a SAS 3 midplane board. • The H 3310 Series chassis features a SAS 4 midplane board.

Internal Component	Description
Expansion slots and optional interface cards	The expansion slots accommodate optional interface cards to provide additional connectivity. • The Gen3 H series includes a two port 1 GigE card to provide data connection between hosts and the BlackPearl NAS. • The Gen3 H series optionally includes: • One optional dual port 25 GigE HBAs using either 10 Gbps or 25 Gbps SFPs. Ports of the same type can be aggregated for better performance. • One optional dual port 100 GigE HBAs using either 40 Gbps or 100 Gbps SFPs. Ports of the same type can be aggregated for better performance. • Up to five optional four-port 12 GB SAS cards provide connectivity for up to eight 77-bay and 107-bay expansion nodes.

Rear Panel

Figure 7 shows the components on the rear panel of the Gen3 H Series BlackPearl master node.

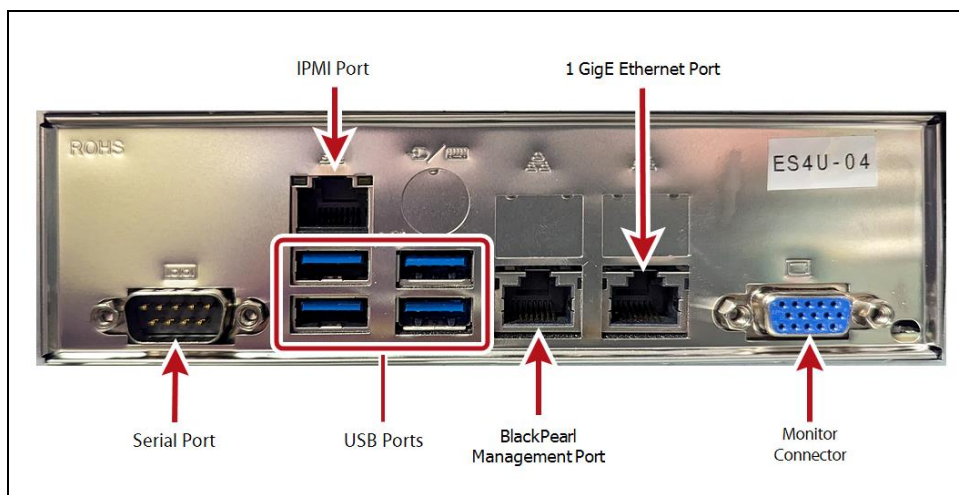


Figure 7 The Gen3 H Series BlackPearl rear panel components.

Component	Description
Monitor connector	If necessary, you can connect a monitor to the VGA connector on the chassis for troubleshooting purposes. Only connect a monitor for initial configuration of the BlackPearl management port, or as directed by Spectra Logic Technical Support.
Serial port	The serial port is only used in a HotPair configuration.

Component	Description
IPMI management port	See IPMI Configuration on page 226 for information on using IPMI management. The port has two status LEDs: • Activity / Link LED • Off - No Link • Blinking Amber - Data activity • On - Link • Speed LED • Off - Indicates 10 Mbps connection or no link • Amber - Indicates 100 Mbps connection • Green - Indicates 1 Gbps connection
USB ports	Four USB 3.1 Gen 1 Ports are available on the H Series BlackPearl chassis. If necessary, you can use these ports to connect a USB drive, or USB keyboard to the chassis for troubleshooting purposes as directed by Spectra Logic Technical Support.
1 Gigabit Ethernet ports	The Gen 3 H Series BlackPearl NASs include two 10GBase-T ports. The left 1 Gigabit port is dedicated as the BlackPearl management port and cannot be used for data transfer. The right 1 Gigabit port can be used for network connectivity tests on a 1 Gigabit network but is not sufficient for normal data storage operations. Each port has two status LEDs: • Activity / Link LED • Off - No Link • Blinking Yellow - Data activity • On - Link • Speed LED • Off - Indicates 10 Mbps connection or no link • Amber - Indicates 100 Mbps connection • Green - Indicates 1 Gbps connection
BlackPearl management port	The BlackPearl management port is used to connect to a browser-based user interface to configure, manage, and monitor the BlackPearl NAS. The BlackPearl management port cannot be used for data transfer.

Gen2 X Series

Front View

Figure 8 shows the components on the front of the Gen2 X Series BlackPearl NAS with the front bezel removed.

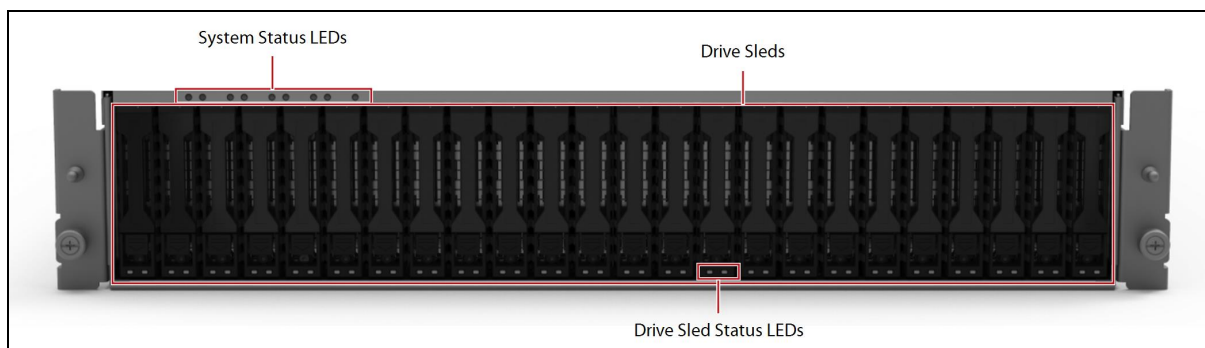


Figure 8 The front view of the Gen2 X Series BlackPearl NAS (front bezel removed).

Component	Description
System status LEDs	The status LEDs indicate power status, fan status, server status, and chassis status. See Monitor the Hardware on page 159 for more information. Note: The LEDs are not visible with the bezel installed.
Data drives	The base Gen2 X Series BlackPearl NAS supports up to 24 high-performance solid state drives (SSDs) mounted on individual drive sleds. The drive sleds slide into bays in the front of the chassis and lock in place. The front of each drive sled has a handle for removing the sled and a latch for locking the drive sled in place.
Data drive status LEDs	The blue LED indicates the location of the drive for servicing. The green / amber bi-color LED indicates the drive status. • Off - There is no SSD activity. • Green - SSD activity is detected. No faults are detected. • Solid Amber - The SSD experienced a fault and requires a service action. • Amber blinking at 1 Hz - The SSD is attempting to link. • Amber blinking at 2 Hz - The SSD failed to link. Note: The LEDs are not visible with the bezel installed.
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. Ensure each empty drive sled has a 'drive blank' installed in the sled for proper airflow and cooling.

Rear View

Figure 9 show the major components on the rear of the Gen2 X Series BlackPearl chassis.

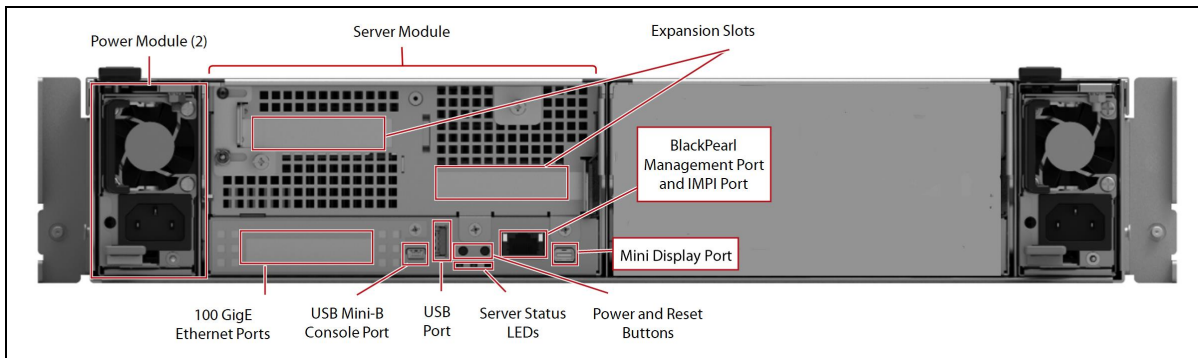


Figure 9 The rear view of the Gen2 X Series BlackPearl NAS.

Component	Description
Power modules	The Gen2 X Series BlackPearl NAS includes two power modules. Each power module has active current sharing and supports N+1 redundancy. • Each power supply has its own AC power connector. • Each power supply has a bi-color LEDs to indicate power to the power module and status of the power module. • Not lit - Neither power module has AC power. • Amber solid - The power module experienced a critical event and shut down or the power cord is unplugged. • Amber blinking - The power module detected hi-temp, hot spot temp, high current, or high-power warning, but continues to operate. • Green solid - The power module is on and OK.
Server status LEDs	The server module has three status LEDs below the server module power and reset buttons. A lit LED indicates the following: • Green - The server module has booted and is operating normally. A service action is not allowed. • Blue solid - The server module is being sent an identify command. • Blue blinking - A service action is allowed. • Amber - A server module fault has been detected.

Component	Description
Server Power and Reset buttons	The chassis powers on when power is connected or when the power button is pressed. Use the user interface, not the power button, to power down the chassis. To power on the chassis, insert a blunt pointed object (such as a paper clip) into the recessed opening to momentarily press the Power button. If directed by Spectra Logic Technical Support, use the server Power and Reset buttons to turn off power to the server module, or reset the server module CPU. Insert a blunt pointed object (such as a paper clip) into the recessed opening to press the Power or Reset button. • Press the Power button momentarily to initiate the normal shut-down sequence or to power on the server module. • Press and hold the Power button for 4 or more seconds to immediately power off the server module. • Press the Reset button momentarily to reset the power module.
BlackPearl management port and IPMI port	The BlackPearl management port is used to connect to a browser-based user interface to configure, manage, and monitor the Gen2 X Series BlackPearl NAS. The BlackPearl management port cannot be used for data transfer. The port has two status LEDs: • Green - Indicates port activity at 1000 Mb. • Amber - Indicates port activity at 100 Mb. This port is also used to access the system IPMI interface using a separate IP address than the BlackPearl management port.
USB ports	Use these ports to connect a USB drive to the chassis to load configuration keys, or to connect a USB drive, or USB keyboard to the chassis for troubleshooting purposes as directed by Spectra Logic Technical Support. The front bezel connects to the active server module's USB port while in production use.
USB Mini-B port	Provides a serial console connection to a USB serial port to access the BlackPearl management console.
Mini DisplayPort	Provides for a PCIe video connection to the BlackPearl management console.

Internal Components

The following table describes the internal field replaceable components.

Internal Component	Description
Server module	The server module in the Gen2 X Series BlackPearl NAS provides Ethernet, SAS, USB, and other connections. A second identically configured server module can be added for HotPair failover.
100 GigE Ethernet ports	The two 100 Gigabit Ethernet (100 GigE) ports are used for data transfer on an Ethernet network.
Expansion slots	The expansion slots accommodate optional interface cards to provide additional connectivity. • Up to two optional four-port SAS card provide connectivity for up to eight 77-bay and 107-bay expansion nodes.

Gen2 S Series and Gen2 V Series

Front View

Figure 10 shows the components on the front of the Gen2 S Series BlackPearl NAS with the front bezel removed. Figure 11 shows the components on the front of the Gen2 V Series BlackPearl NAS with the front bezel removed.

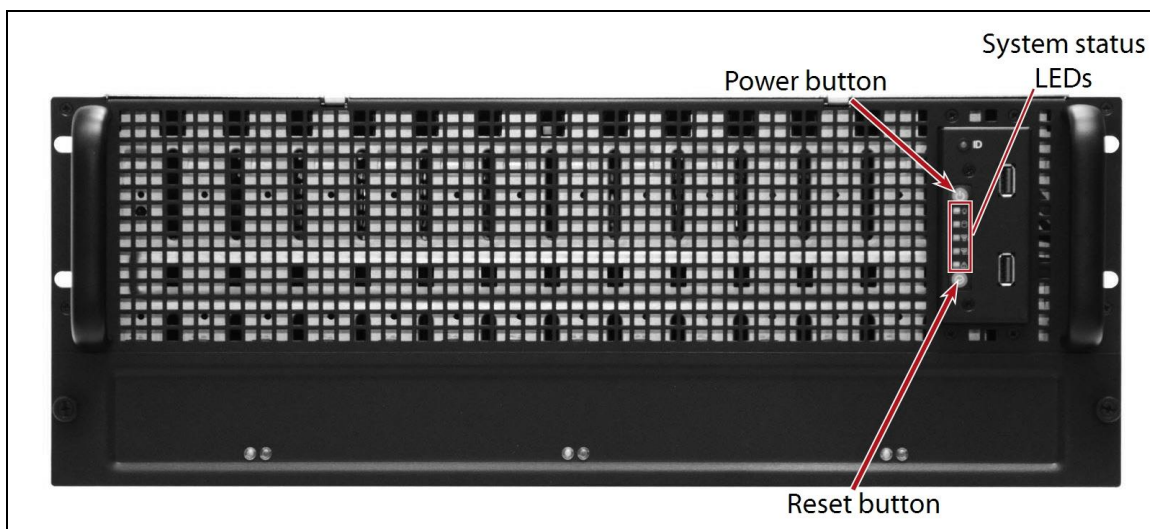


Figure 10 The front view of the Gen2 S Series BlackPearl 4U (front bezel removed).

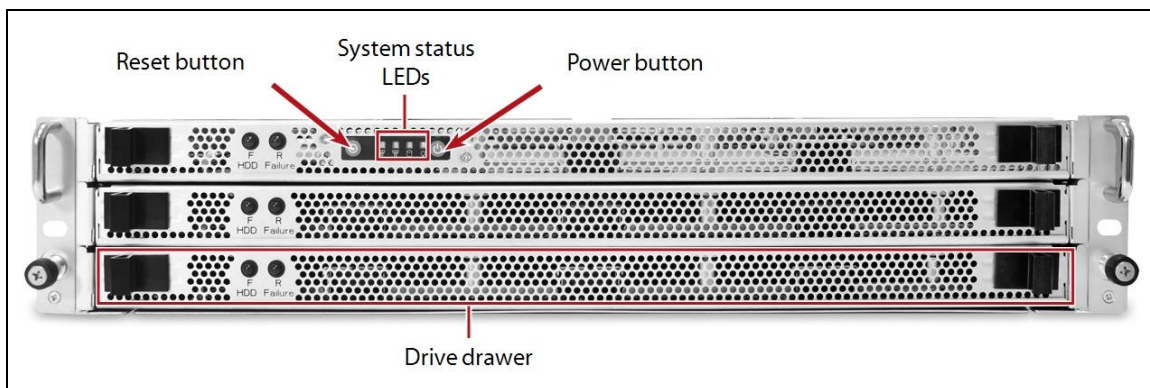


Figure 11 The front view of the Gen2 V Series BlackPearl 2U (front bezel removed).

Component	Description
Power button 	The chassis powers on when power is connected or when the power button is pressed. Use the user interface, not the power button, to power down the chassis.
Reset button	Only use the chassis reset button under direction of Spectra Logic Technical Support.

Component	Description
	
System status LEDs	The status LEDs indicate power status, disk and network activity, as well as hardware faults. See Monitor the Hardware on page 159 for more information. Note: The LEDs are not visible with the bezel installed.
Drive drawers (Gen2 V Series only)	Three drive drawers each contain eight drive bays for up to 24 high-performance disk drives. Depending on your order configuration, the BlackPearl NAS may optionally contain solid state drives to improve NAS write performance. See Features on page 20 for more information.

Rear View

Figure 12 shows the major components on the rear of the Gen2 S BlackPearl NAS. Figure 13 shows the major components on the rear of the Gen2 V Series BlackPearl NAS.

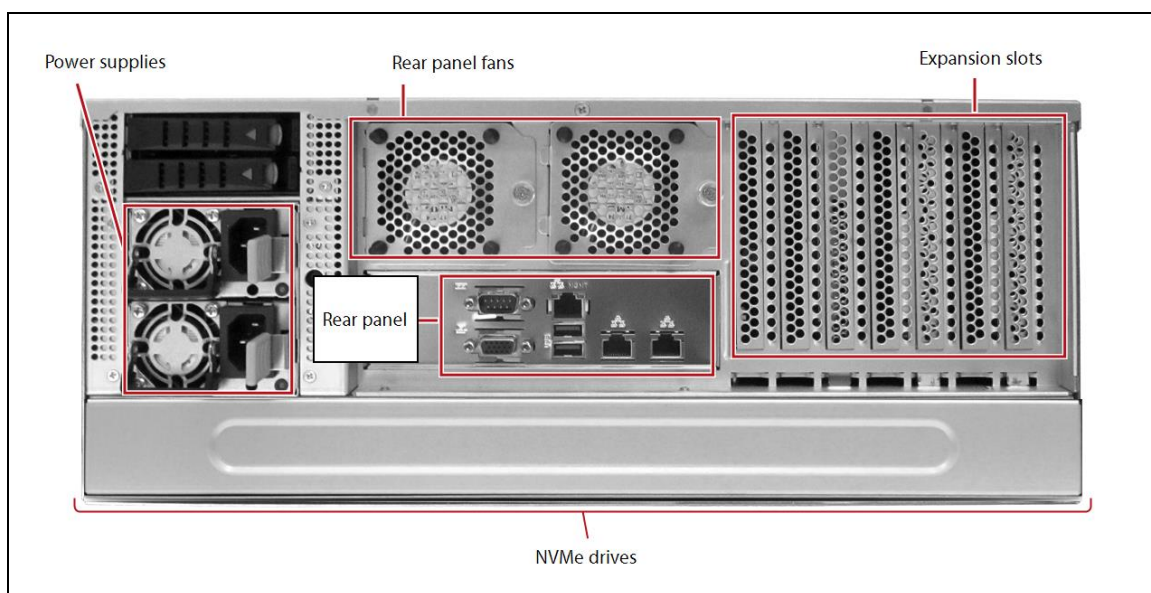


Figure 12 The rear view of the Gen2 S Series BlackPearl 4U.

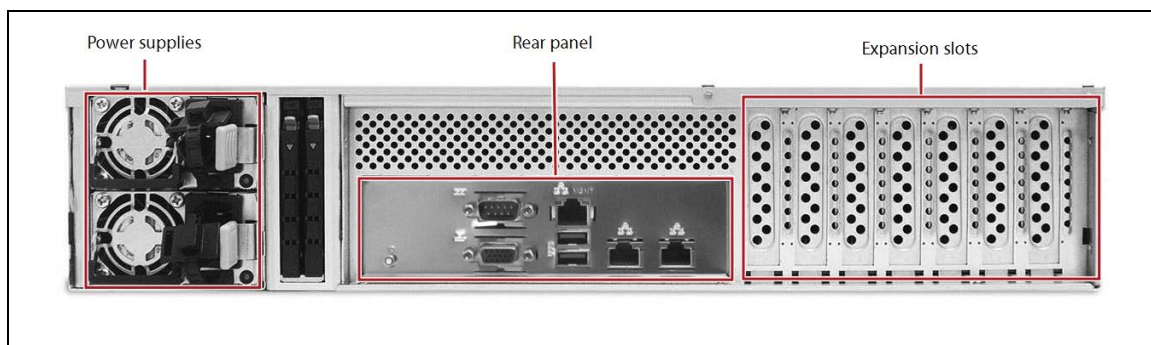


Figure 13 The rear view of the Gen2 V Series BlackPearl 2U.

Component	Description
Power supplies	The standard BlackPearl NAS configuration includes two power supplies to provide N+1 redundancy and fail-over protection. Each power supply has its own AC power connector.
Rear panel fans (Gen2 S Series only)	Two rear panel fans and four internal fans provide the cooling for the Gen2 S series chassis. The rear panel fans are hot-swappable. The Gen2 V series has three internal fans.
Rear panel	The rear panel of the Gen2 S Series and Gen2 V Series BlackPearl master node allows for Ethernet, SAS, USB, and other connections. See Rear Panel on page 43 for a detailed description.

Internal Components

The following table describes the internal field replaceable components.

Internal Component	Description
Boot drives	Two NVMe boot drives provide high performance storage for the operating system and BlackPearl user interface. The NVMe boot drives are connected to the motherboard and are not hot-swappable.
NVMe SSD drives	The Gen 2 S Series supports up to 10 NVMe drives for special allocation, metadata performance, and ZIL.
Expansion slots and optional interface cards	The expansion slots accommodate optional interface cards to provide additional connectivity. • The Gen2 V series includes a two port 10GBase-T card to provide data connection between hosts and the Gen2 V series. • The Gen2 S series optionally includes a two port 10GBase-T card to provide data connection between hosts and the Gen2 S series. • Up to two optional dual port 25 GigE cards provide a high-speed data connection between hosts and the Gen2 S Series and Gen2 V Series BlackPearl NAS. Ports of the same type can be aggregated for better performance. • Up to three optional four-port SAS cards provide connectivity for up to nine 77-bay and 107-bay expansion nodes.

Rear Panel

Figure 14 shows the components on the rear panel of the Gen2 S Series and Gen 2 V Series BlackPearl 4U and 2U master nodes.

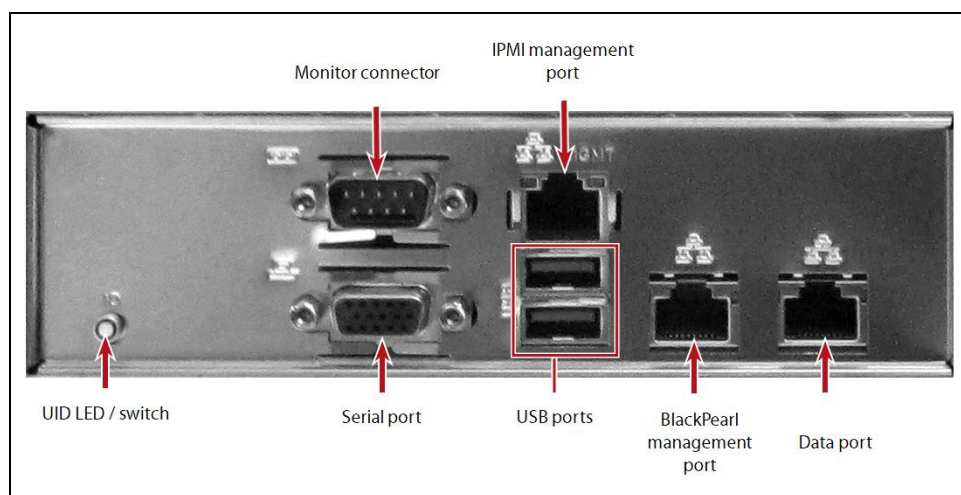


Figure 14 Gen2 S Series and Gen 2 V Series BlackPearl rear panel components.

Component	Description
UID LED / switch	Pressing the unit ID LED / switch displays a flashing blue pattern on the visual status beacon (see Monitor the Hardware on page 159) and the UID LED on the back of the chassis to make finding the chassis easier when moving between the front and rear of the rack.
Monitor connector	If necessary, you can connect a monitor to the VGA connector on the chassis for troubleshooting purposes. Only connect a monitor for initial configuration of the BlackPearl management port, or as directed by Spectra Logic Technical Support.
Serial port	The serial port is only used in a HotPair configuration.

Component	Description
IPMI management port	See IPMI Configuration on page 226 for information on using IPMI management. The port has two status LEDs: • Activity / Link LED • Off - No Link • Blinking Amber - Data activity • On - Link • Speed LED • Off - Indicates 10 Mbps connection or no link • Amber - Indicates 100 Mbps connection • Green - Indicates 1 Gbps connection
USB ports	Two USB 3.1 Gen 1 Ports are available on both the V Series and the S Series BlackPearl chassis. The S Series chassis also has one USB 3.1 Gen 2 Port (not shown). If necessary, you can use these ports to connect a USB drive, or USB keyboard to the chassis for troubleshooting purposes as directed by Spectra Logic Technical Support. The front bezel connects to one of the USB ports while in production use.
1 Gigabit Ethernet ports	The Gen 2 V Series BlackPearl NASs include two 10GBase-T ports. The left 1 Gigabit port is dedicated as the BlackPearl management port and cannot be used for data transfer. The right 1 Gigabit port can be used for network connectivity on a 1 Gigabit network. Each port has two status LEDs: • Activity / Link LED • Off - No Link • Blinking Yellow - Data activity • On - Link • Speed LED • Off - Indicates 10 Mbps connection or no link • Amber - Indicates 100 Mbps connection • Green - Indicates 1 Gbps connection Note: An optional 10GBase-T Ethernet card can be added for improved data transfer.

Component	Description
10GBase-T Ethernet ports	The Gen2 S Series BlackPearl NASs include two 10GBase-T ports. The left 10GBase-T port is dedicated as the BlackPearl management port and cannot be used for data transfer. The right 10GBase-T port can be used for network connectivity on a 10GBase-T network. Each port has two status LEDs: • Activity / Link LED • Off - No Link • Blinking Yellow - Data activity • On - Link • Speed LED • Off - Indicates 1 Gbps or 100 Mbps connection, or no link • On - Indicates 10 Gbps connection Notes: • The 10GBase-T ports auto-negotiate down to 1 Gbps or 100 Mbps. • Optional Ethernet cards can be added for data transfer.
BlackPearl management port	The BlackPearl management port is used to connect to a browser-based user interface to configure, manage, and monitor the BlackPearl NAS. The BlackPearl management port cannot be used for data transfer.

77-Bay and 107-Bay Expansion Nodes

Front View

Figure 15 shows the major components on the front of the 77-bay and 107-bay expansion nodes. There are no components or status indicators visible on the front of the 77-bay and 107-bay expansion nodes with the front bezel is attached.



Figure 15 The front view of the 77-bay and 107-bay expansion nodes.

Internal Components

The following table describes the internal field replaceable components.

Internal Component	Description
Data drives	The 77-bay and 107-bay expansion nodes supports up to 77 or 107 enterprise disk drives, respectively. Disk drives are mounted on individual drive sleds in the chassis. The drive sleds slide into bays in the top of the enclosure and lock in place.

Rear View

Figure 16 shows the major components on the rear of the 77-bay and 107-bay expansion nodes.

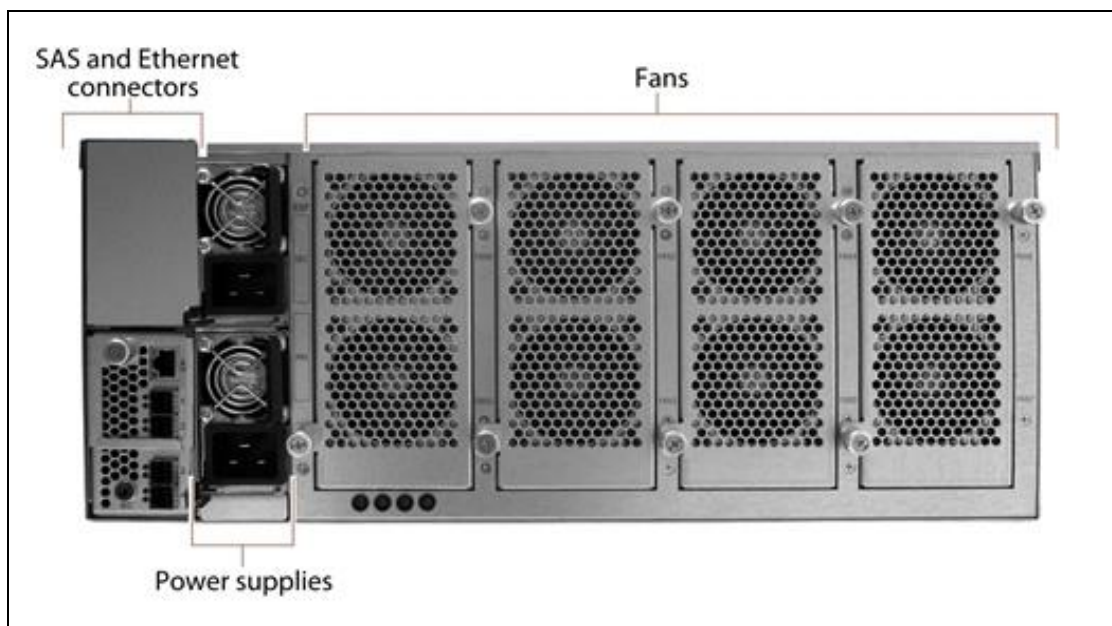


Figure 16 The rear view of the 77-bay and 107-bay expansion nodes.

Component	Description
SAS and Ethernet connectors	The rear panel of the 77-bay and 107-bay expansion nodes have one or two expander panels which include one Ethernet port and four SAS ports used to connect the 77-bay or 107-bay expansion node to a BlackPearl master node. When connecting the 77 bay expansion node to a BlackPearl Storage Manager chassis, connect one cable to each of the two controllers.
Fans	Eight hot-swappable fans, in banks of two, provide the cooling for the 77-bay and 107-bay expansion nodes.
Power supplies	The 77-bay and 107-bay expansion nodes 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.

Gen1 S Series, Gen1 P Series, and Gen1 V Series

Front View

Figure 17 shows the components on the front of the Gen1 S Series or Gen1 P Series BlackPearl NAS. All information is the same for the Gen1 S Series and Gen1 P Series unless specified.

Figure 18 shows the components on the front of the Gen1 V Series BlackPearl NAS with the front bezels removed.

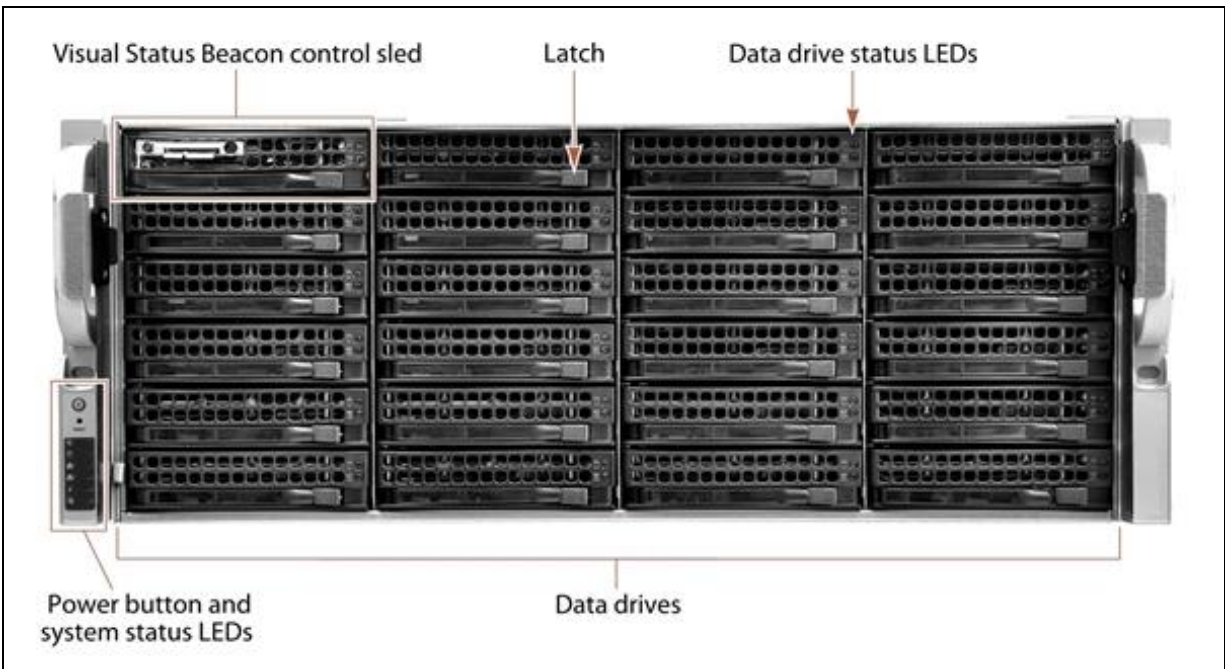


Figure 17 The front view of the Gen1 S and P Series BlackPearl 4U master node (front bezel removed).

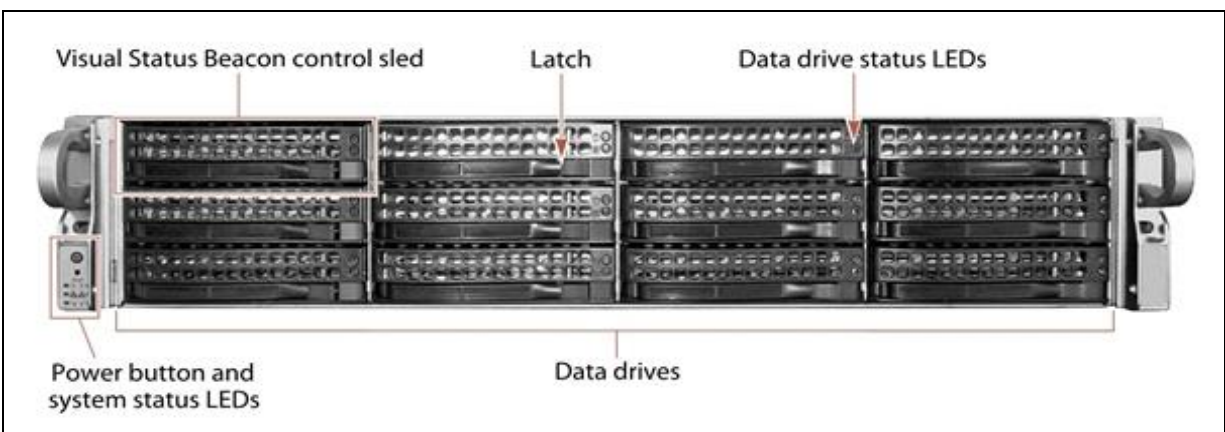


Figure 18 The front view of the Gen1 V Series BlackPearl 2U master node (front bezel removed).

Component	Description
Visual Status Beacon control sled	The drive sled in the upper left corner of the front of the chassis provides control for the Visual Status Beacon. A disk drive cannot be installed in this position.
Power button	The chassis powers on when power is connected or when the power button is pressed. Use the user interface, not the power button, to power down the chassis.
System status LEDs	The status LEDs indicate power status, disk and network activity, as well as hardware faults. See Monitor the Hardware on page 159 for more information. Note: The LEDs are not visible with the bezel installed.
Data drives	The BlackPearl Gen1 S and P Series master nodes support up to 23 high-performance disk drives in the front of the chassis. The BlackPearl Gen1 V Series master nodes support up to 12 data drives in the front of the chassis. Depending on your order configuration, the BlackPearl NAS may optionally contain solid state drives to improve NAS write performance. See Features on page 20 for more information. Note: If the BlackPearl Gen1 S and P Series master node uses a bezel without a Visual Status Beacon, 24 disk drives can be installed in the front of the. The drive sleds slide into bays in the front of the BlackPearl chassis and lock in place. The front of each drive sled has a handle for removing the sled from the chassis 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. Note: The LEDs are not visible with the bezel installed.
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

Figure 19 shows the major components on the rear of the Gen1 S or Gen1 P Series BlackPearl master node. All information is the same for the Gen1 S Series and Gen1 P Series unless specified. Figure 20 shows the major components of the Gen1 V Series BlackPearl master node chassis.

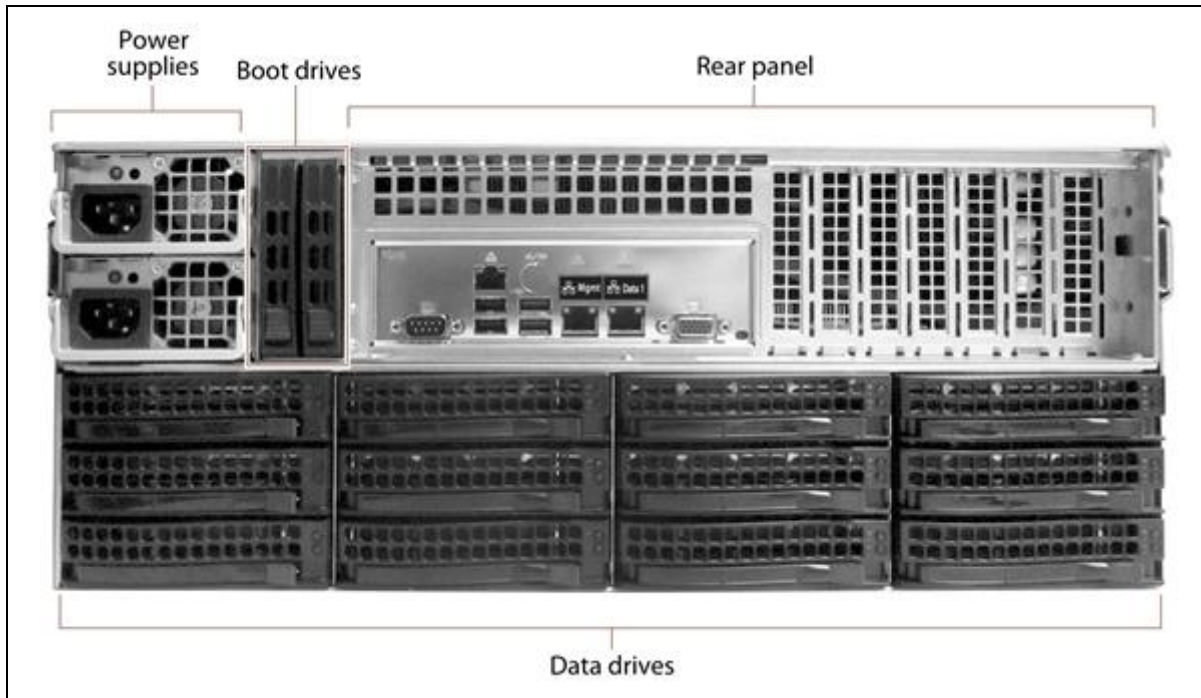


Figure 19 The rear view of the Gen1 S Series BlackPearl 4U master node.

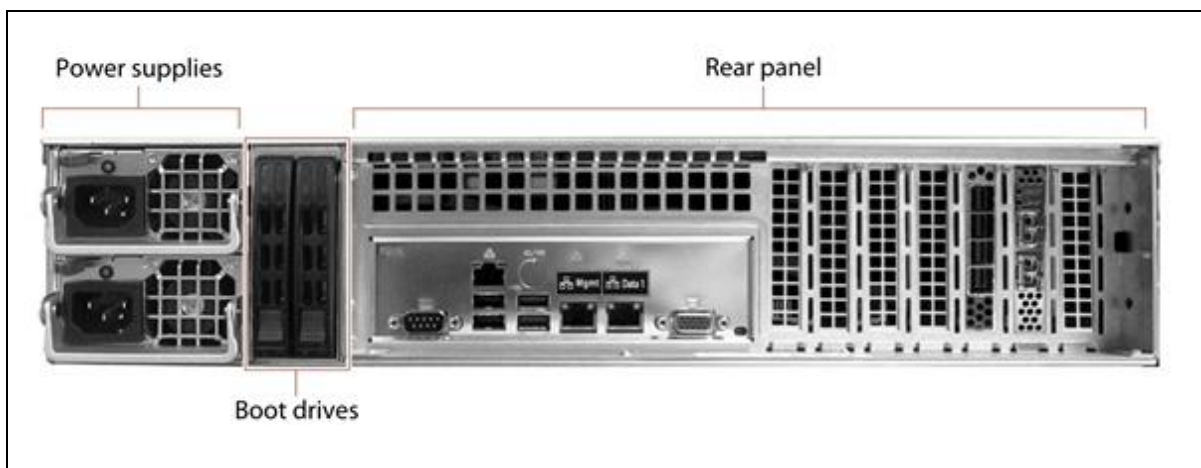


Figure 20 The rear view of the Gen1 V Series BlackPearl 2U master node.

Component	Description
Power supplies	The standard BlackPearl NAS configuration 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 Gen1 S Series BlackPearl NAS allows for Ethernet, SAS, USB, and other connections. See Rear Panel on the next page for a detailed description.
Boot drives	The boot drives provide storage for the operating system and BlackPearl user interface. The boot drives in the BlackPearl NAS are hot swappable which allows for uninterrupted operation during replacement.
Data drives (BlackPearl 4U master node only)	The BlackPearl NAS 4U master nodes support up to 12 data drives in the rear of the chassis. Depending on your order configuration, the BlackPearl NAS may optionally contain solid state drives to improve NAS write performance. See Features on page 20 for more information. Note: The BlackPearl NAS 2U master node does not have data drives in the rear of the chassis.
Empty drive sleds (BlackPearl 4U master node 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

Figure 21 shows the components on the rear panel of the BlackPearl 4U and 2U Gen1 S Series chassis.

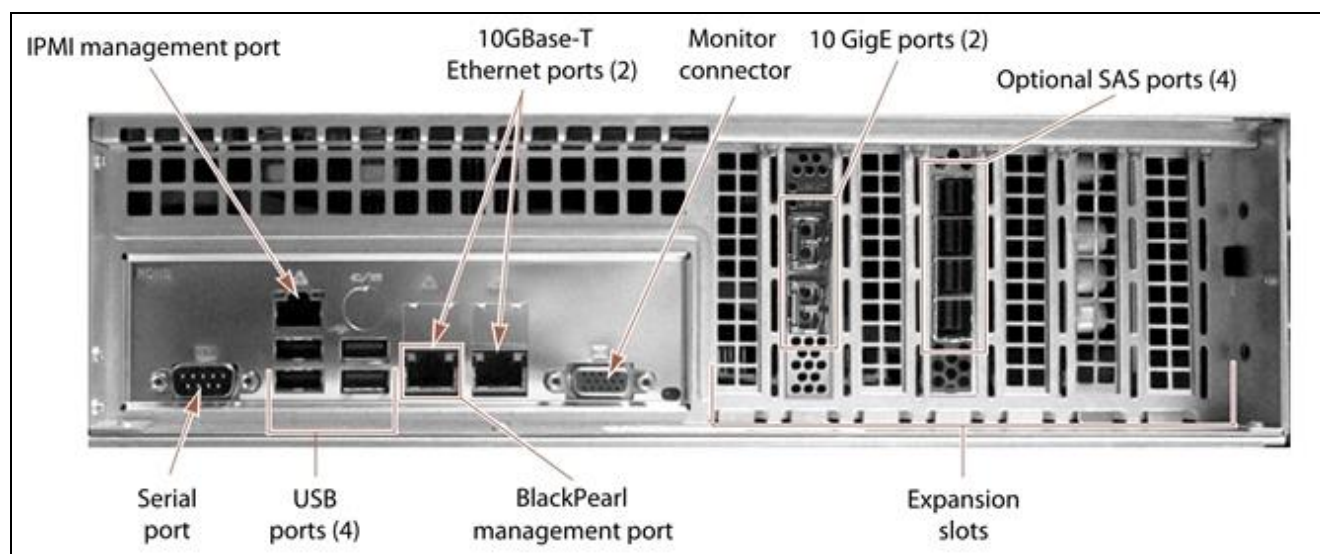


Figure 21 The Gen1 S Series BlackPearl rear panel components.

Component	Description
IPMI management port	See IPMI Configuration on page 226 for information on using IPMI management.
10GBase-T Ethernet ports	The Gen1 S Series BlackPearl master node 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 BlackPearl management port and cannot be used for data transfer. Notes: • The 10GBase-T ports auto-negotiate down to 1000Base-T. • Spectra Logic recommends using 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 BlackPearl 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.

Component	Description
10 GigE ports	The two 10 Gigabit Ethernet (10 GigE) ports can be used for network connectivity on a 10 GigE network. A can contain different types of network interface cards, but can only use one card at a time. Note: Unless your BlackPearl NAS includes a 40 GigE card or a 10GBase-T card, Spectra Logic recommends using the 10 GigE ports for data transfer to ensure maximum performance.
Expansion slots and optional interface cards	The expansion slots accommodate optional interface cards to provide additional connectivity. • An optional 40 GigE or 10GBase-T Ethernet network interface card can be used to provide a high-speed data connection between hosts and the Gen1 Series S BlackPearl NAS. Ports of the same type can be aggregated for better performance. • Optional two-port SAS cards each provide connectivity for up to one 44-bay expansion nodes, or up to two 77-bay, 96-bay, or 107-bay expansion nodes. • Optional four-port SAS cards each provide connectivity for up to two 44-bay expansion nodes, or up to four 77-bay, 96-bay, or 107-bay expansion nodes. • Optional two- or four-port Fibre Channel cards provide connectivity to Fibre Channel tape drives in a Spectra Logic or supported tape library. Each port connects to one drive.
BlackPearl management port	The BlackPearl management port is used to connect to a browser-based user interface to configure, manage, and monitor the Gen1 S Series BlackPearl NAS. The BlackPearl management port cannot be used for data transfer.
USB ports	If necessary, you can use these ports to connect a USB drive, or USB keyboard to the chassis for troubleshooting purposes. Only connect a USB drive or keyboard as directed by Spectra Logic Technical Support.
Serial port	The serial port is only used in a HotPair configuration.

44-Bay Expansion Node

Front View

Figure 22 shows the major components on the front of the 44-bay expansion node.

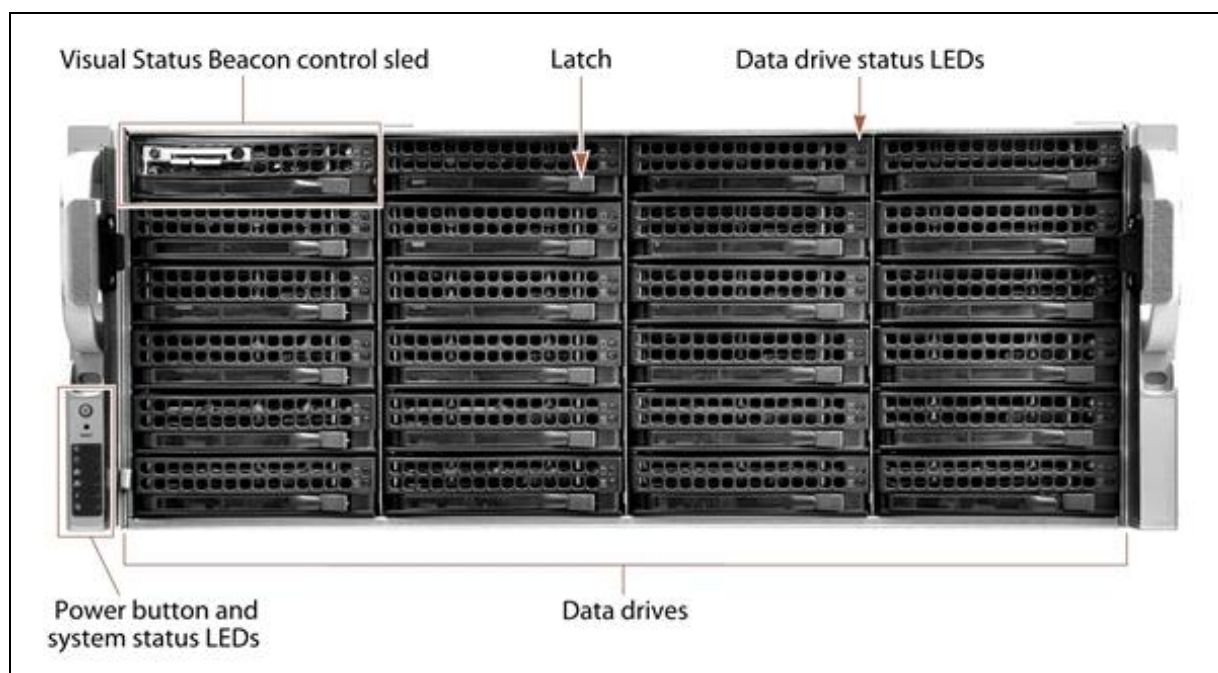


Figure 22 The front view of the 44-bay expansion node (front bezel removed).

Component	Description
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.
Power button	The power button powers on the AC power for the 44-bay expansion node. Use the user interface, not the power button, to power down the BlackPearl NAS, including the expansion node.
System status LEDs	The status LEDs indicate power status, disk and network activity, as well as hardware faults. See Monitor the Hardware on page 159 for more information.
Data drives	The front of the 44-bay expansion node supports up to 23 enterprise disk drives, 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 chassis and a latch for locking the drive sled in place.

Component	Description
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

Figure 23 shows the major components on the rear of the 44-bay expansion node.

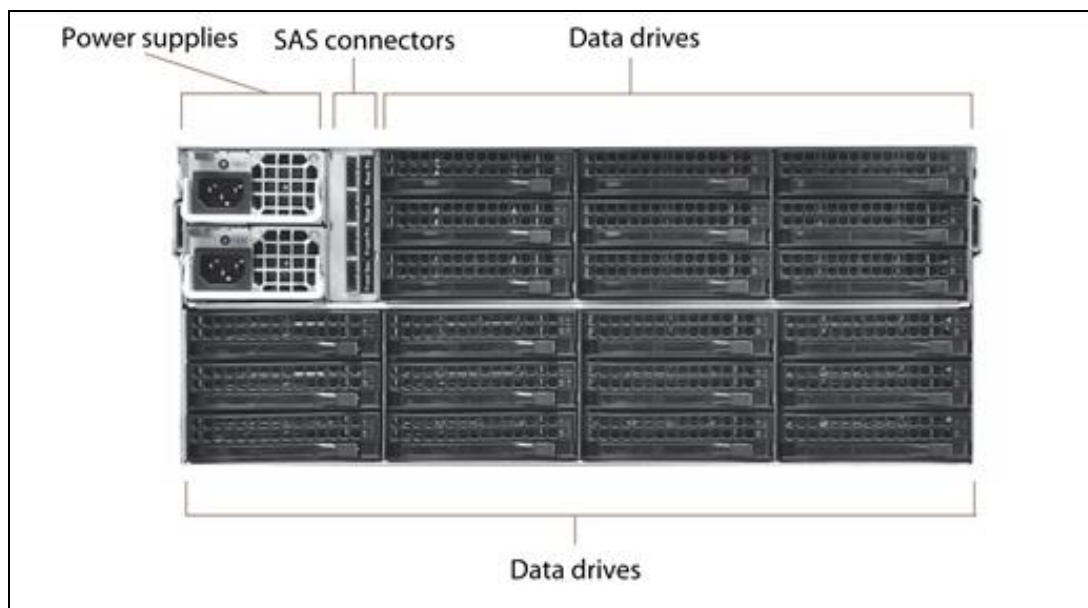


Figure 23 The rear view of the 44-bay expansion node.

Component	Description
Power supplies	The 44-bay 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 44-bay 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.

96-Bay Expansion Node

Front View

Figure 24 shows the major components on the front of the 96-bay expansion node. There are no components or status indicators on the front of the 96-bay expansion node.

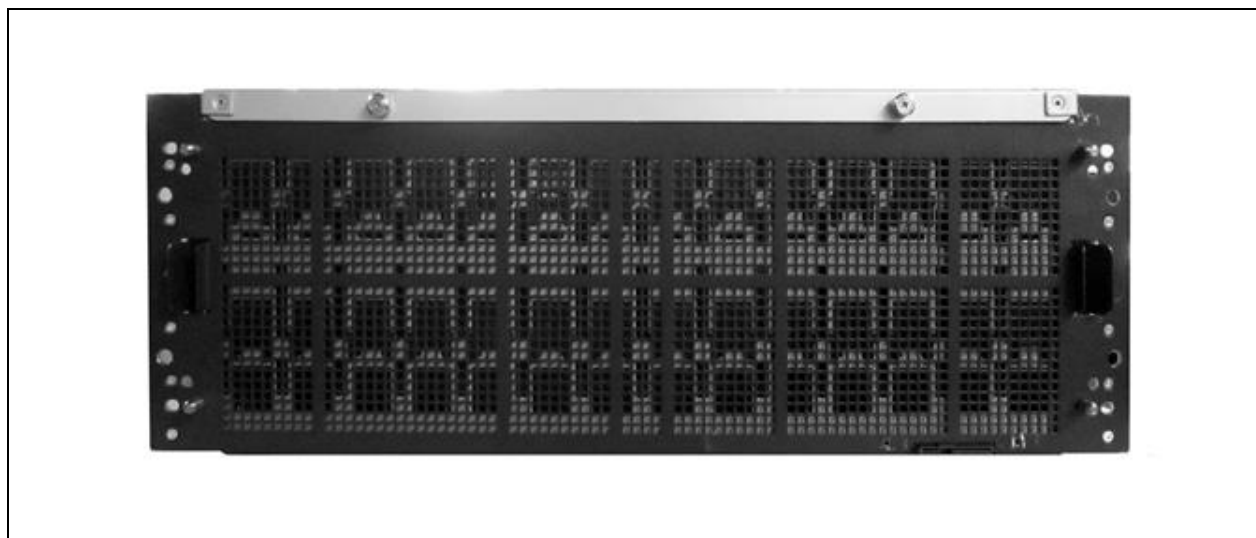


Figure 24 The front view of the 96-bay expansion node (front bezel removed).

Internal Components

The following table describes the internal field replaceable components.

Internal Component	Description
Data drives	The 96-bay expansion node supports up to 96 enterprise disk drives, mounted on individual drive sleds in the chassis. The drive sleds slide into bays in the top of the enclosure and lock in place.

Rear View

Figure 25 shows the major components on the rear of the 96-bay expansion node.

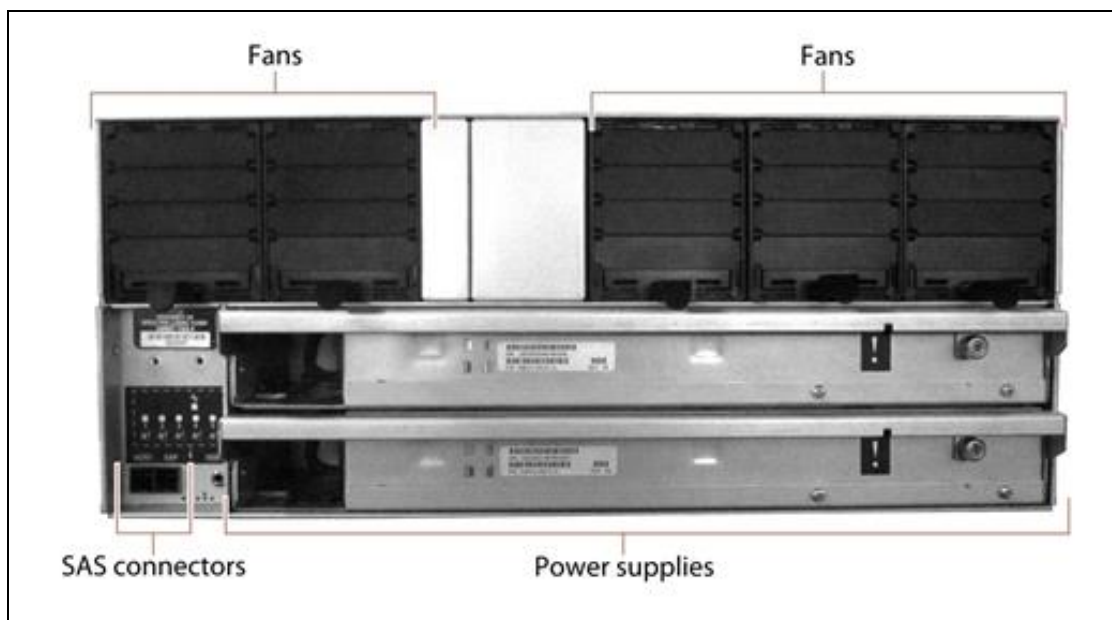


Figure 25 The rear view of the 96-bay expansion node.

Component	Description
Fans	Five hot-swappable fans provide the cooling for the 96-bay expansion node.
Power supplies	The 96-bay 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 96-bay expansion node has two SAS ports used to connect an expansion node to BlackPearl master node.

SOFTWARE

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

NFS and CIFS Servers

The NFS and CIFS servers running on the BlackPearl NAS 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, macOS operating system, UNIX, and Linux.

COMMAND LINE INTERFACE

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

CHAPTER 2 - CONFIGURING INITIAL SETTINGS

This chapter describes the initial setup of the Spectra BlackPearl NAS, necessary for operation in your environment.

Before You Begin	62
Install HBAs	62
Rackmount the Chassis	62
Install Drives	62
Connect Ethernet Cables	62
Power On the	63
Configure the BlackPearl Management Port	65
Log Into the BlackPearl User Interface	68
Configure the Data Connection	70
Configure an Aggregate Port Data Connection	70
Configure a Single Port Data Connection	72
Configure a Static Route	74
Create a User	76
Description of User Permissions	76
Create a User	77
Next Steps	79

BEFORE YOU BEGIN

If your BlackPearl NAS was installed by Spectra Logic Professional Services or in accordance with the *Spectra BlackPearl NAS Solution Site Preparation Guide* and the *Spectra BlackPearl NAS Quick Start Guide* (Gen2) or the *Spectra BlackPearl NAS Gen1 Installation Guide* (Gen1) the steps in this section are complete. They are provided here for reference. See [Next Steps](#) on page 79 to begin using your BlackPearl NAS.

INSTALL HBAs

Gen2 chassis ship with all HBAs installed.

For a Gen1 chassis, if necessary, use the instructions in the *Spectra 12- & 36-Drive Chassis HBA Installation Guide* to install optional HBAs.

RACKMOUNT THE CHASSIS

If desired, rackmount the chassis. Use the appropriate resource below:

- For a Gen3 H series or F Series, contact Spectra Logic Technical Support for instructions.
- For a Gen2 X, S, or V Series see the *BlackPearl Quick Start Guide*.
- For a Gen1 P, S, or V Series, see the *Spectra BlackPearl NAS Solution Gen1 Installation Guide*.

INSTALL DRIVES

After you rackmount the chassis, you may need to install the drives that shipped with your BlackPearl NAS. Use one of the sections below to install the drives.

- [Install a Drive in a Gen3 H Series Chassis on page 180](#)
- [Install a Drive in a Gen2 S Series Chassis on page 187.](#)
- [Install a Drive in a Gen2 V Series Chassis on page 188](#)
- [Install a Drive in a Gen2 X Series Chassis on page 189](#)

CONNECT ETHERNET CABLES

Before proceeding with the below sections, you must connect Ethernet cables to the management and data ports on the BlackPearl NAS rear panel. See one of the following for the location of the Ethernet ports on the rear of the master node:

- For a Gen3 F Series see [Rear Panel on page 28.](#)
- For a Gen3 H Series see [Rear Panel on page 33.](#)

- For a Gen2 X Series see [Rear View on page 36](#).
- For a Gen2 S or V Series see [Rear Panel on page 43](#).
- For a Gen1 P, S, or V Series, see [Rear Panel on page 52](#).

POWER ON THE

Use the instructions in this section to power on a BlackPearl NAS, and optionally, a 44-bay, 77-bay, 96-bay, or 107-bay expansion node. During the power-on sequence, the BlackPearl NAS initializes all of its installed components and starts the BlackPearl web server.

1. If your BlackPearl configuration includes one or more expansion nodes, power on the expansion nodes first. If you do not have any expansion nodes, skip to [Step 2 on page 64](#).
 - To power on a 77-bay, 96-bay, or 107-bay expansion node, connect power cables to the power supplies on the rear of the expansion node chassis (see [Figure 16 on page 47](#) and [Figure 25 on page 58](#)), then plug the power cables into power outlets near the chassis. The expansion node immediately powers on. Wait approximately four minutes while the expansion node initializes before powering on the BlackPearl master node.
 - To power on a 44-bay expansion node, remove the front bezel and then gently press the power button on the front panel. Wait approximately four minutes while the expansion node initializes before powering on the BlackPearl master node.

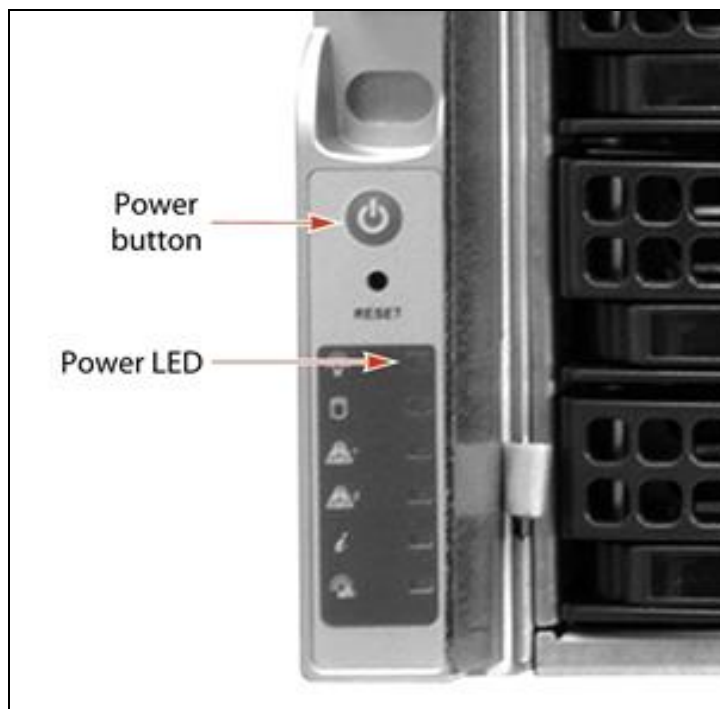


Figure 26 Press the power button (Gen 1 shown).

2. To power on a BlackPearl master node, connect power cables to the power supplies on the rear of the master node chassis. See one of the following for the location of the power supply connectors on the rear of the master node:
 - For a Gen3 F Series see [Rear Panel on page 28](#).
 - For a Gen3 H Series see [Rear Panel on page 33](#).
 - For a Gen2 X Series see [Rear View on page 36](#).
 - For a Gen2 S or V Series see [Rear Panel on page 43](#).
 - For a Gen1 P, S, or V Series, see [Rear Panel on page 52](#).
3. Plug the power cables into power outlets near the chassis. Wait while the BlackPearl NAS completes its power-on sequence, which takes approximately 5 to 10 minutes, depending on the configuration.

Note: Do not use the front panel power button to power down the. See [Reboot or Shut Down a BlackPearl NAS on page 174](#).

CONFIGURE THE BLACKPEARL MANAGEMENT PORT

**IMPORTANT**

You must connect Ethernet cables as described in [Connect Ethernet Cables on page 62](#) before either proceeding with the steps below.

The default IP address for the BlackPearl management port is set to **10.0.0.2**, with a netmask of **255.255.255.0**.

- If you do not want to change the default management port IP address, skip to [Log Into the BlackPearl User Interface on page 68](#).
- If your network is already using this IP address, or you want to configure a different IP address for the management port:
 - Use the BlackPearl console to configure the management port IP address. See the instructions below.
 - Use the 10.0.0.2 IP address to log into the BlackPearl user interface and then change the IP address. Skip to [Log Into the BlackPearl User Interface on page 68](#), then use the instructions in [Configure Network Connections on page 97](#)

Note: If you cannot use one of the methods above to change the Management port IP address, see [Resolve a BlackPearl Management Port IP Address Conflict on page 223](#) for an alternate method.

1. Connect a monitor and USB keyboard or KVM switch to the rear of the BlackPearl NAS.

Note: The Gen2 X Series chassis has a mini DisplayPort connection for the monitor. The other chassis have a VGA connection.

See one of the following for the location of the monitor and USB ports on the rear of the master node:

- For a Gen3 F Series see [Rear Panel on page 28](#).
- For a Gen3 H Series see [Rear Panel on page 33](#).
- For a Gen2 X Series see [Rear View on page 36](#).
- For a Gen2 S or V Series see [Rear Panel on page 43](#).
- For a Gen1 P, S, or V Series, see [Rear Panel on page 52](#).

The Console screen displays.

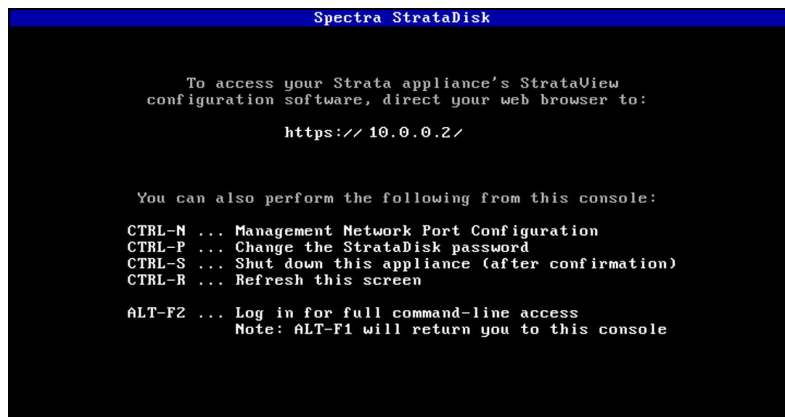


Figure 27 The Console screen.

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

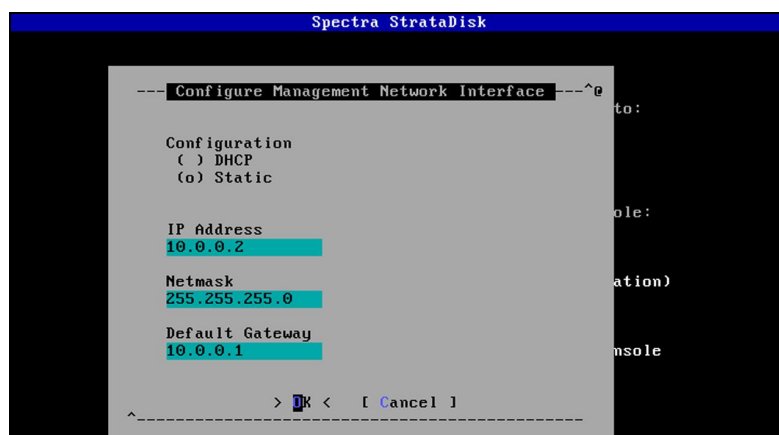


Figure 28 The Configure Management Network Interface screen.

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 network gateway.

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

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

5. You are now able to connect to the BlackPearl user interface with the IP address displayed in [Step 4](#).
6. Disconnect the monitor and USB keyboard from the BlackPearl NAS.

LOG INTO THE BLACKPEARL USER INTERFACE

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

- Notes:**
- 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.
 - To log into the BlackPearl user interface on a system that is configured to use Multi-Factor Authentication, see [Multi-Factor Authentication on page 132](#).
1. Using a standard web browser, enter the IP address for the BlackPearl management port configured in [Configure the BlackPearl Management Port on page 65](#).

Note: The BlackPearl user interface uses a secure connection.

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

The BlackPearl NAS ships with non-signed SSL certificates for both the data and management ports. When using the shipped certificates, you must pass a security check every time you attempt to access the management port to view the BlackPearl 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 85](#).
3. Enter the primary administrator username and password. The fields are case sensitive.
 - The default username is **Administrator**.
 - The default password is the serial number of the master node. Find the serial number on the sticker positioned on the top of the chassis, on the right-hand side, toward the front. The serial number is indicated by the letters "SN" on the sticker.

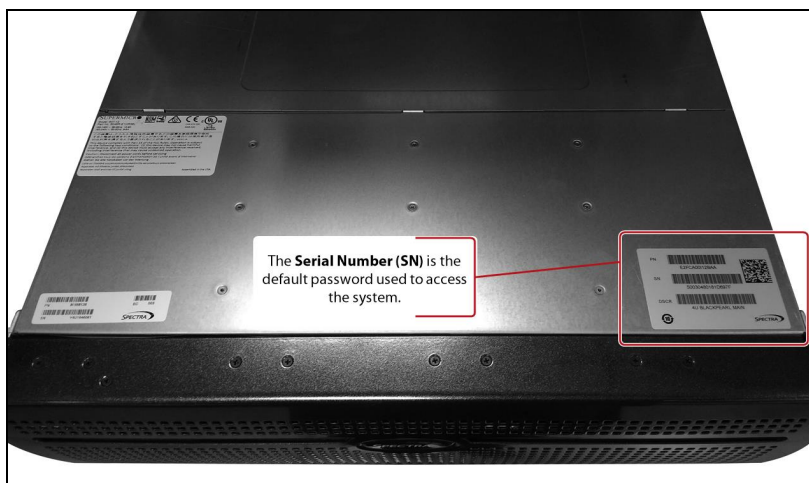


Figure 29 The BlackPearl serial number sticker.



Figure 30 The NAS Login screen.

4. Click **Login** to log in.

Note: Spectra Logic recommends that you change the default password for the primary administrator (see [Configure Users on page 145](#)).

CONFIGURE THE DATA CONNECTION

This section describes using the BlackPearl user interface to configure one or more data connections for the BlackPearl NAS. The configuration steps are the same for all standard and optional port types.

- Notes:**
- You can configure link aggregation for better performance.
 - While different types of Ethernet network interface cards can be installed in the same BlackPearl NAS, only one type port can be used in each link aggregation configuration.
 - You can only use the BlackPearl management port to access the BlackPearl user interface. You cannot use this port for data transfer.

Configure an Aggregate Port Data Connection

Link aggregation uses multiple Ethernet ports, configured with a single MAC address, to improve data transfer speeds. See [Networking Best Practices on page 81](#) for more information.



IMPORTANT

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

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

1. Use the toolbar in the upper-right to select **Configuration (wrench) > Network**.

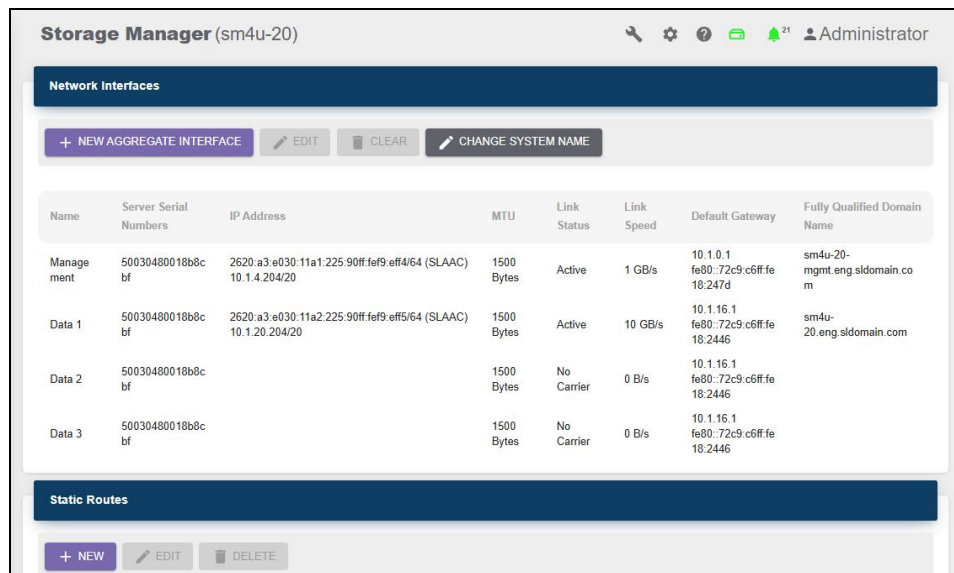


Figure 31 The Network screen.

2. Click **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 32 The Add Aggregate Interface dialog box.

3. Select the **Data Port(s)** you want to configure into an aggregate data interface.

Note: 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 the **DHCP** checkbox to configure the to automatically acquire an IPv4 address using DHCP. This setting does not apply to IPv6.

5. To configure a static IP address enter the following information:

- **IP Address**—Enter a valid IPv4 or IPv6 address.
- **Prefix Length**—Enter the subnet mask.

Notes: • You cannot enter an IPv4 address if you selected DHCP in [Step 4](#).

- If desired, you can enter 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 entered for the last configured IPv4 connection sets the default for the BlackPearl NAS.

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

- Notes:**
- The gateway entered for the last configured IPv6 connection sets the default gateway for the BlackPearl NAS.
 - The IPv6 Gateway does not need to be configured when the BlackPearl NAS 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 **Submit**.

Configure a Single Port Data Connection

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

To configure a single data port connection, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to configure a single port data connection will be added to a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

`https://ipaddress/legacy`

2. Use the toolbar in the upper-right to select **Configuration > Network**. The Network screen displays with information about the network connections of the.

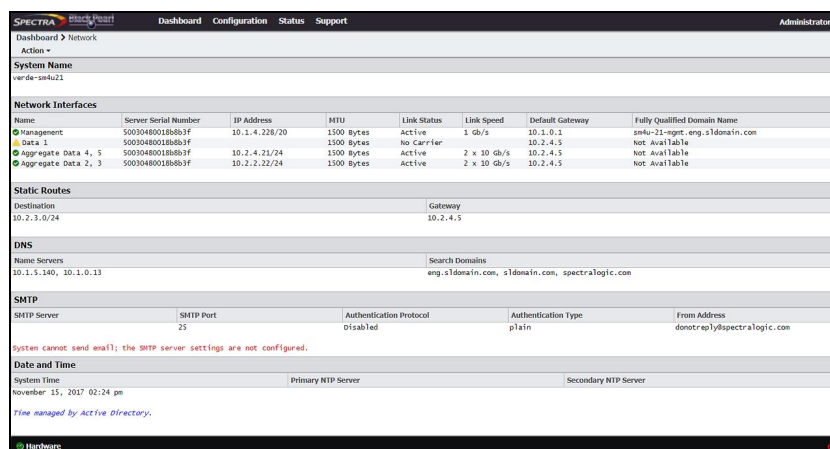


Figure 33 The Network screen.

3. 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 # dialog box may look different than what is shown below.

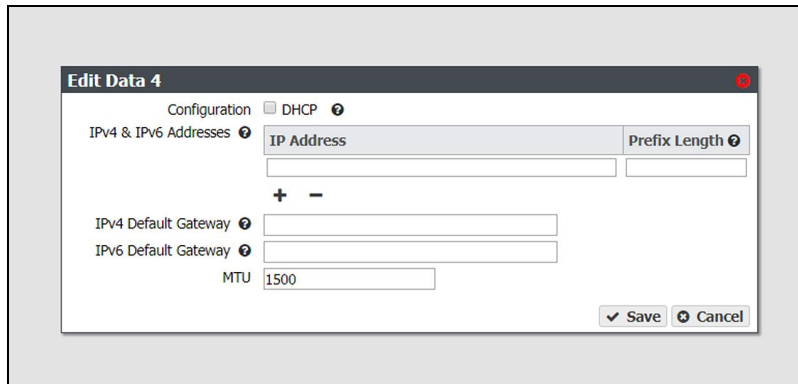


Figure 34 The Edit Data # dialog box.

4. Select the **DHCP** checkbox to configure the 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.

- **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, this option is unavailable.
- The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl NAS.

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

Notes:

- The gateway entered for the last configured IPv6 connection sets the default gateway for the BlackPearl NAS.
- The IPv6 Gateway does not need to be configured when the BlackPearl NAS 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 Static Route

The BlackPearl NAS only supports communication with one default gateway. When configuring a BlackPearl NAS 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 BlackPearl NAS.

When configuring a 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 BlackPearl NAS, a static route is required in order for the 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 BlackPearl NAS 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 BlackPearl NAS 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. Use the toolbar in the upper-right to select **Configuration (wrench) > Network**.

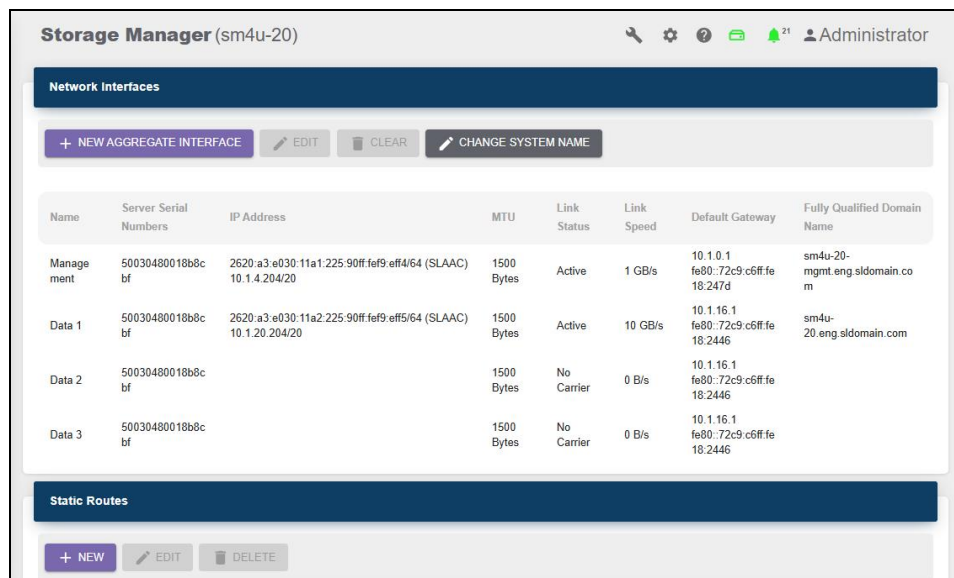


Figure 35 The Network screen.

2. In the Static Routes pane, click **New**. The Add Static Route dialog box displays.

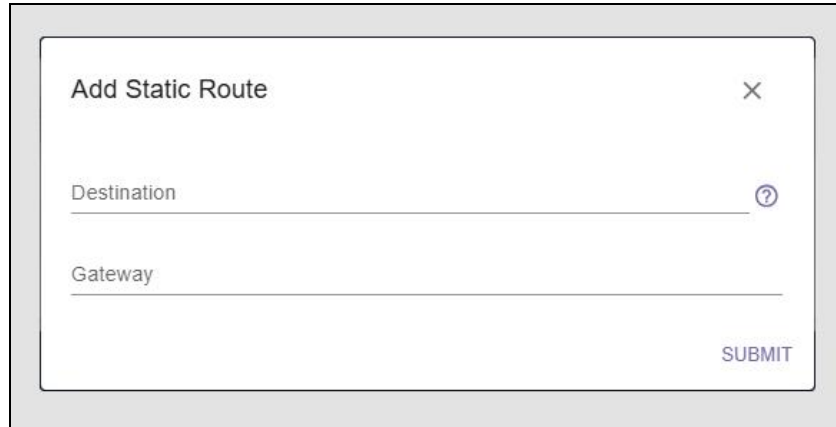
The image shows a dialog box titled "Add Static Route" with a close button (X) in the top right corner. Inside the dialog, there are two text input fields: "Destination" and "Gateway". The "Destination" field has a help icon (question mark in a circle) to its right. At the bottom right of the dialog is a "SUBMIT" button.

Figure 36 The Add 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 network **Gateway** of the data connection used to communicate with the isolated network.
5. Click **Create**.
6. Repeat for **each** host computer on the isolated network.

CREATE A USER

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

Note: The "Administrator" user is created automatically and assigned all permissions.

Description of User Permissions

There are five different types of users permissions in the BlackPearl user interface: Administrator, monitor, login, CIFS, and SpectraApp. Use the table below for a description of the user permission types.

Permission	Description
Administrator	A user with the Administrator permission has full control over all user interface functions. A primary Administrator account is created by default using the name "Administrator", and is automatically assigned all permissions. The default password is the serial number of the master node. Find the serial number on the sticker positioned on the top of the chassis, on the right-hand side, toward the front (see Figure 29 on page 68). Note: Spectra Logic recommends changing the password for the primary Administrator account. See Configure Users on page 145.
Monitor	A user with Monitor permission can access the BlackPearl user interface but cannot use any functions of the user interface other than creating a manual snapshot of a volume or marking a volume read only. This account is useful if you need to view the status jobs or any other aspect of the user interface, but do not have access to an account with administrator permission. Note: A user with the monitor permission can open any menu or function and attempt to edit settings, but these changes are ignored when the user attempts to save the changes.
Login	A user with Login permission is able to log into the BlackPearl user interface. Notes: • Administrator and Monitor users must also have Login permission in order to log in to the BlackPearl user interface. • The SpectraApp user requires Login permission in order to load the embedded dashboard into an external Spectra software application.
CIFS User	A user with CIFS permission is able to access CIFS shares in a Windows workgroup environment.

Permission	Description
SpectraApp	A user with SpectraApp permission is required to load the BlackPearl embedded dashboard in the StorCycle or RioBroker applications. See the documentation for your Spectra software application for instructions on loading the embedded dashboard. Notes: • A user with Administrator permission is required to create, edit, or delete a SpectraApp user. • The SpectraApp user requires Login permission in order to load the embedded dashboard into an external Spectra software application.

Create a User

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.

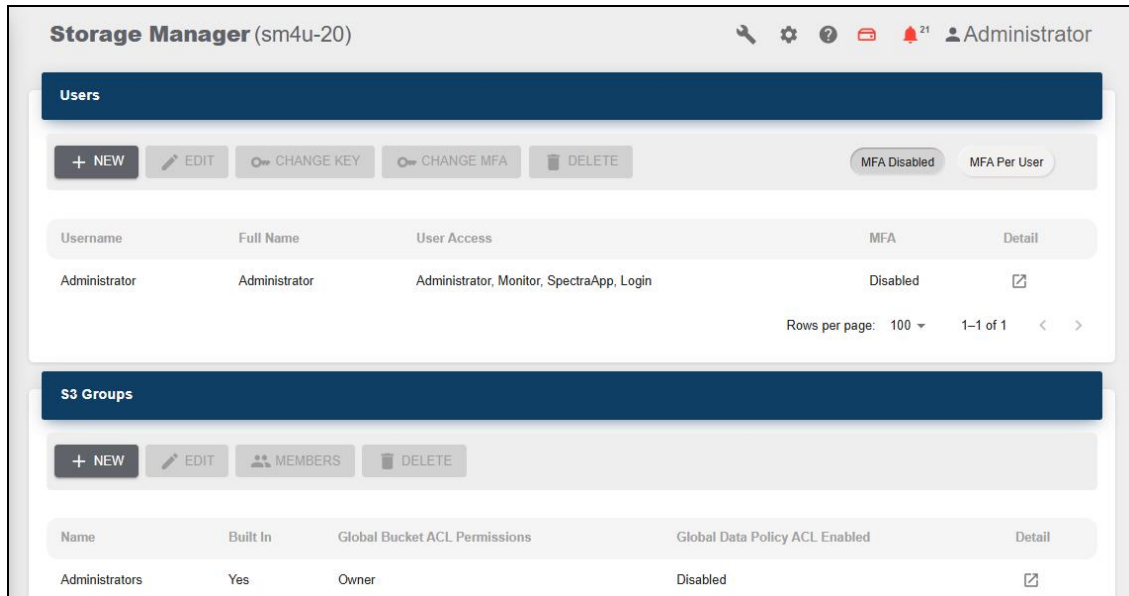


Figure 37 The Users screen.

2. In the Users pane, click **New**. The New User dialog box displays.

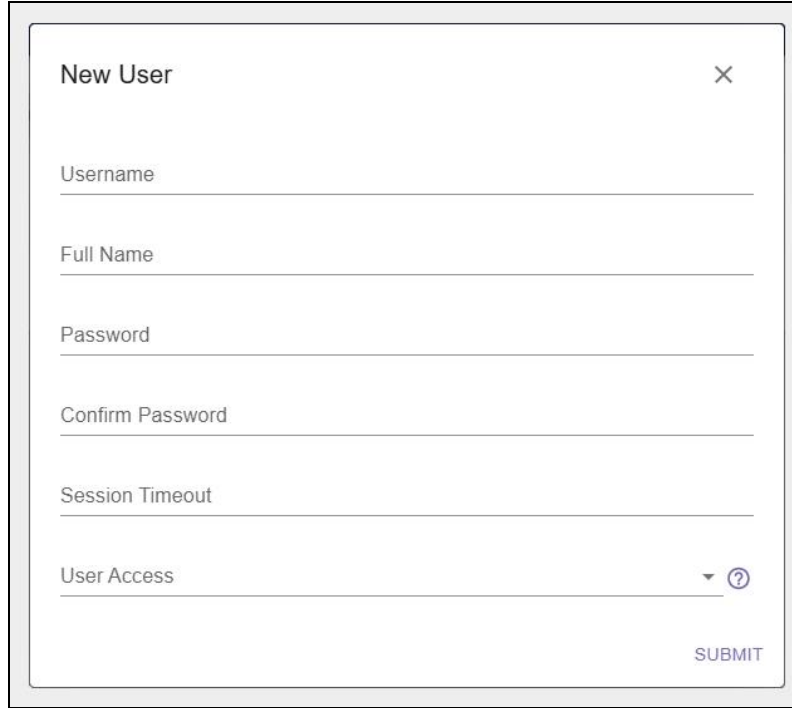
The image shows a 'New User' dialog box with a title bar containing the text 'New User' and a close button (X). The dialog box contains several input fields: 'Username', 'Full Name', 'Password', 'Confirm Password', 'Session Timeout', and 'User Access'. The 'User Access' field has a dropdown arrow and a help icon (question mark). A 'SUBMIT' button is located at the bottom right of the dialog box.

Figure 38 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.
7. Select one or more **User Access** permissions. See [Description of User Permissions on page 76](#) for information on each level of user access permission.

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

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

NEXT STEPS

The BlackPearl NAS now has the necessary components configured to begin designing your storage architecture. Continue with one of the following:

- To configure SSL certificates see [Configure Certificates on page 85](#).
- To configure DNS, SMTP, system time, and hostname, see [Configure Network Settings on page 87](#).

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

- If you have a standalone BlackPearl NAS, continue to [Configuring Network Attached Storage on page 100](#).
- If you plan to use your BlackPearl NAS with a BlackPearl Object, skip to Network File Interface on page 1.

CHAPTER 3 - CONFIGURING NETWORK SETTINGS

This chapter describes using the BlackPearl user interface to configure networking for the Spectra BlackPearl NAS.

Networking Best Practices	81
Configuration Method	81
Supported Network Connectivity	81
Required Open Firewall Ports	81
MTU Settings	82
Link Aggregation	82
Link Aggregation Port Utilization	83
Network Connectivity Tools	83
Troubleshooting	84
Configure Certificates	85
Configure Network Settings	87
Configure DNS Settings	87
Configure SMTP Settings	88
Configure Date and Time	89
Change the System Name	89
Configure Networking Services	91
Configure the Active Directory Service	91
Configure the SNMP Service	95
Configure Network Connections	97
Configure Ethernet Ports	97

NETWORKING BEST PRACTICES

The basic steps for configuring the management and data ports for access to your 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 BlackPearl NAS and utilize the Ethernet interfaces correctly.

Note: The BlackPearl management port is separate from the data ports. The management port and data ports have their own default routes.

Configuration Method

Use the BlackPearl management interface or the command line interface to configure the management and data ports. Do not attempt to access the directly and use the root console to modify interfaces. The management and command line interfaces are tightly integrated with the base operating system and configure additional features based on network changes.

Supported Network Connectivity

The following configurations are supported for the data path:

Recommended:

- A single logical connection using a network interface card. Use either one physical port, or two ports in link aggregation. For information on supported connection speeds, see [Specifications on page 230](#).

Not Recommended:

- Single gigabit logical connection utilizing one of the on-board motherboard ports and a Category 5e Ethernet cable.

Required Open Firewall Ports

Management Interface

Port	Description
TCP 22	SSH (Administrative access)
TCP 80/443	BlackPearl management interface
UDP 161	SNMP (Metrics & monitoring)

Data Interface

Port	Description
TCP 80/443	DS3 API (user configurable)
TCP 8080/8443	DS3 API (user configurable)
TCP 139/445	Samba/CIFS
UDP 137/138	Samba/CIFS
TCP 111 / 757 / 2049 / 4045 / 4046	NFS Storage Stack
UDP 111 / 757 / 2049 / 4045 / 4046	NFS Storage Stack
UDP 123	NTP
TCP 59373	BlackPearl NAS replication control link
TCP 59374 - 59400	BlackPearl NAS replication data transfer range

Firewall

Port	Description
UDP 161 (SNMP inbound)	This port must be open for your monitoring hosts to poll the BlackPearl system.
TCP 25, 465, or 587 (SMTP outbound)	If you configure email alerts in the BlackPearl user interface, the selected SMTP port must be open to allow the BlackPearl system to make outbound connections to your mail server.

MTU Settings

The BlackPearl NAS supports MTU values of 1500-9000. If you configure the MTU value to something other than the 1500 default value, make sure that your switch configuration and all the hosts on the network support the larger MTU settings, to avoid an impact on performance.

Link Aggregation

If link aggregation is configured for the BlackPearl NAS, then network switches must support link aggregation to aggregate or “trunk” the data ports together to provide higher bandwidth to the.

Network switches must support link aggregation using LACP (Link Aggregation Control Protocol), and hash the destination IP addresses. Typically you must manually configure LACP on the switch ports.

- If you **are** using link aggregation, the switch must be configured **to use** LACP on those ports.
- If you **are not** using link aggregation, the switch must be configured **to not use** LACP on those ports.

Network switches use different methods of routing traffic from hosts to NAS servers. For example, some switches route traffic based on both the MAC address and the IP address.

- Using DHCP link aggregation, the BlackPearl NAS presents only one MAC address and one IP address.
- Using static link aggregation, the BlackPearl NAS presents only one MAC address, but can have up to 16 IP addresses aliased to the MAC address.

Link Aggregation Port Utilization

The network switch rotates data transfers among the physical ports on the BlackPearl NAS in order to achieve the highest throughput possible.

If only a single host is connected to the BlackPearl NAS through a link aggregation connection, the measured performance is lower than the potential maximum transfer rate because only one physical port of the two port link aggregation is being utilized by the switch.

If a single share is configured with two different IP addresses, when two separate hosts begin data transfers, the resulting throughput is approximately twice that of a single host connection.

Note: You may need to configure more than two IP addresses on the BlackPearl NAS to force the switch hashing algorithm to utilize all physical ports to maximize performance.

Network Connectivity Tools

Ping

The ping command uses a request-response mechanism to verify connectivity to a remote network node. For example, to verify the connectivity from the switch to the BlackPearl NAS at 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. If the request times out, see [Cannot Ping the BlackPearl NAS on the next page](#).

Note: A response of 0 msec means that the time was less than 1 ms.

Traceroute

You can use the traceroute command to not only verify connectivity to a remote network node, but to track the responses from intermediate nodes as well.

For example, for a BlackPearl NAS at IP address 192.168.2.10, run the command shown below:

```
traceroute 192.168.2.10
```

The output of the command shows a numbered list indicating the number of hops encountered when tracing the packet from the switch to the BlackPearl NAS. If the command fails to reach the BlackPearl NAS, see [Cannot Ping the BlackPearl NAS](#) below.

Troubleshooting

No Port Link LED Light

When the management and data ports are configured correctly and attached to the network, the link lights on the network ports should be illuminated on both the BlackPearl NAS and the network switch. If the port lights are not illuminated:

- Make sure that cables are connected. Verify you are using the correct cable type and connectors. This is especially critical for connections utilizing SFPs.
- Check the port configuration on the network switch. The BlackPearl NAS only supports auto-negotiation. Make sure the switch is configured to match speeds on both ends of the connection.
- Verify that the switch ports are not administratively disabled. Consult the switch *User Guide* for information.

Cannot Ping the BlackPearl NAS

When the network ports are configured correctly, you should be able to ping the BlackPearl NAS from your network. If you cannot ping the BlackPearl NAS:

- Check the LACP settings on the switch.
 - If you **are** using link aggregation, the switch must be configured **to use** LACP on those ports.
 - If you **are not** using link aggregation, the switch must be configured **to not 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.

CONFIGURE CERTIFICATES

The BlackPearl NAS ships with non-signed SSL certificates for both the data and management ports on the. Because the certificates are not signed, you must pass a security check every time you attempt to access the management port to view the BlackPearl user interface, or when you attempt to transfer data using the data port.

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.



IMPORTANT

Starting with BlackPearl OS 5.6, the TLS version is updated to 1.3. Existing certificates using TLS 1.2 must be updated to use the new protocol version.

The BlackPearl NAS accepts intermediate (chain) SSL certificates, and accepts RSA, DSA, and ECC certificates. The BlackPearl NAS accepts both encrypted and non-encrypted certificates.

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

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Certificates**. The Certificates screen displays.

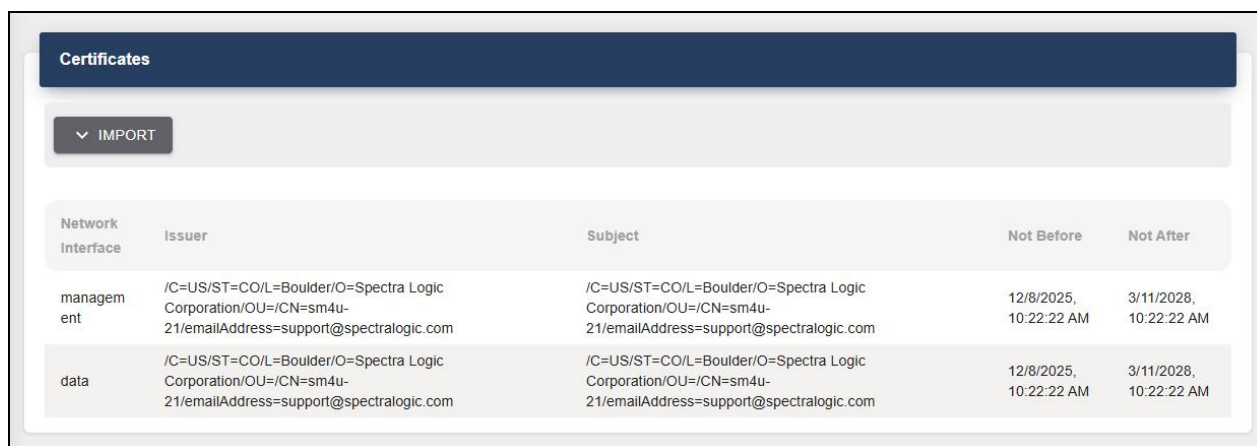


Figure 39 The Certificates screen.

2. Select either the **Management** or **Data** row, depending on for which port you want to import a new SSL certificate.

3. Click **Import**. The Import Certificate dialog box displays.

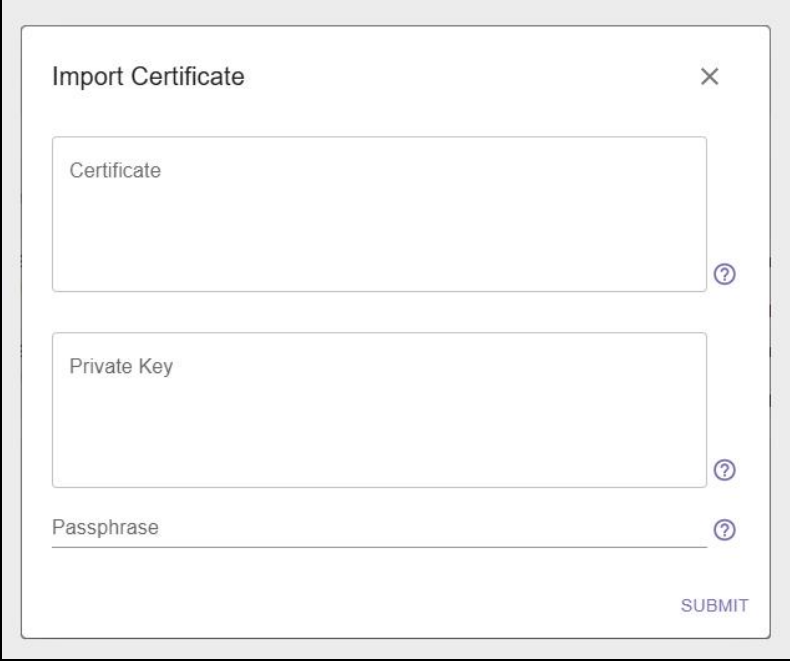
The image shows a dialog box titled "Import Certificate" with a close button (X) in the top right corner. Inside the dialog, there are three input fields: "Certificate", "Private Key", and "Passphrase". Each field has a question mark icon to its right. At the bottom right of the dialog is a "SUBMIT" button.

Figure 40 The Import Certificate dialog box.

4. From your source SSL certificate file, copy the Certificate portion of the file and paste the contents into the **Certificate** entry box.

Note: The certificate must be in PEM format.

5. From your source SSL certificate file, copy the Private Key portion of the file and paste the contents into the **Private Key** entry box.

Note: The private key must be in PEM format.

6. If necessary, enter the **Passphrase**. The Passphrase is used to encrypt the private key.
7. Click **Submit**.

CONFIGURE NETWORK SETTINGS

You can use the BlackPearl user interface to edit DNS and SNMP settings, set the system date and time, and set the system hostname.

Configure DNS Settings

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

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. In the DNS pane, click **Edit**. The Edit DNS dialog box displays.

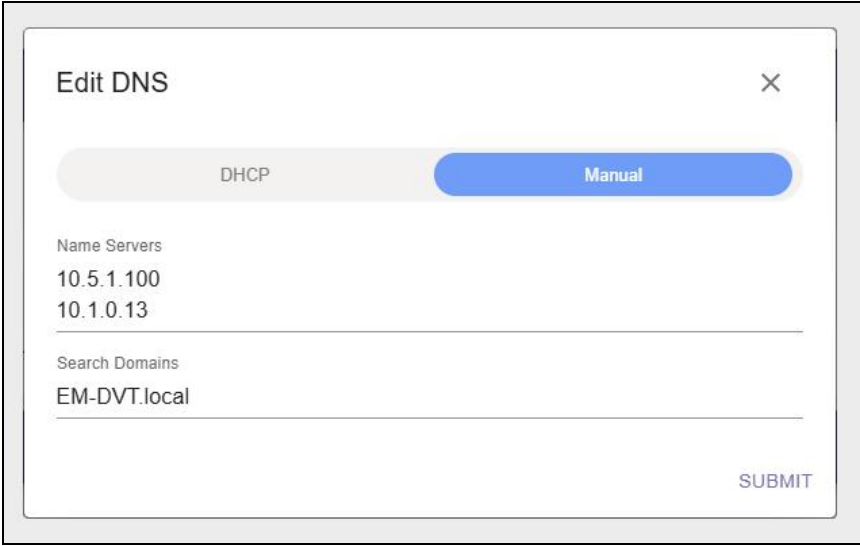


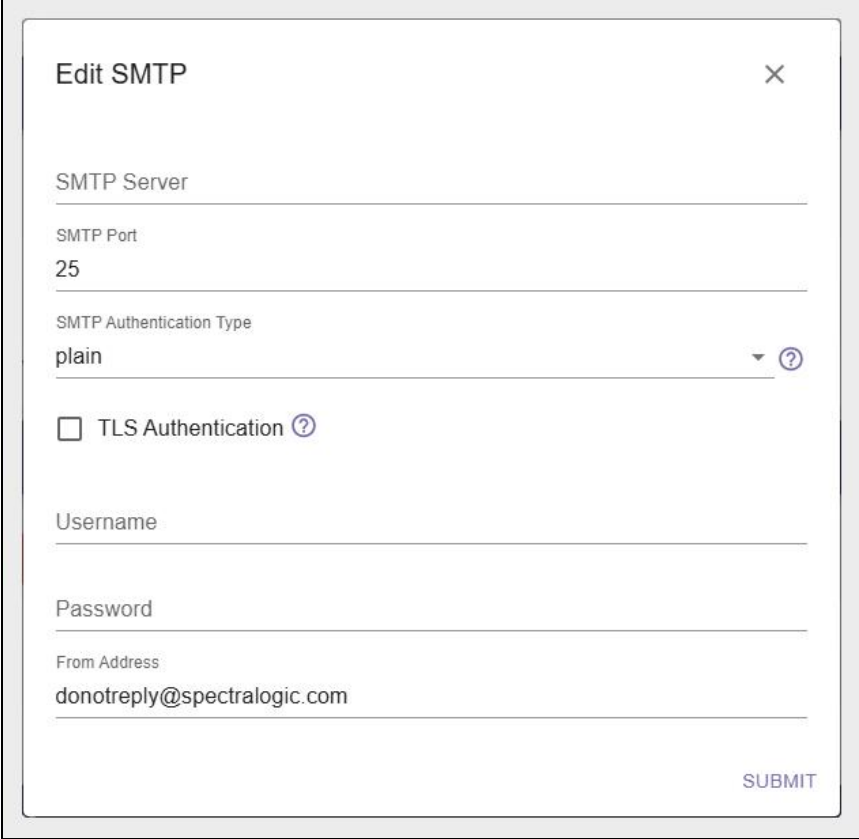
Figure 41 The Edit DNS dialog box.

3. Use the slider to select one of the following:
 - **DHCP** - The determines the address of name servers and search domains automatically.
 - **Manual** - Enter information for name servers and search domains 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 **Submit**.

Configure SMTP Settings

Use the SMTP settings to associate the BlackPearl NAS with a mail server. The uses this SMTP server to send emails whenever AutoSupport Logs (ASLs) or certain severites of messages are generated.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. In the SMTP pane, click **Edit**. The Edit SMTP dialog box displays.



The screenshot shows the 'Edit SMTP' dialog box. It has a title bar with 'Edit SMTP' and a close button (X). The form contains the following fields and controls:

- SMTP Server**: A text input field.
- SMTP Port**: A text input field containing the value '25'.
- SMTP Authentication Type**: A dropdown menu showing 'plain' with a question mark icon.
- TLS Authentication**: A checkbox that is currently unchecked, with a question mark icon.
- Username**: A text input field.
- Password**: A text input field.
- From Address**: A text input field containing the value 'donotreply@spectrallogic.com'.
- SUBMIT**: A button located at the bottom right of the dialog.

Figure 42 The Edit SMTP dialog box.

3. Enter the **SMTP Server** and **SMTP Port** information.
4. Use the **SMTP Authentication Type** drop-down menu to select the authentication required by your SMTP server.
5. If your SMTP server uses TLS (Transport Layer Security) authentication, select the **TLS Authentication** checkbox 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 generates an email. This email address should uniquely identify the BlackPearl NAS to assist in troubleshooting and be recognized by the SMTP server as a valid domain address.
7. Click **Submit**.

Configure Date and Time

The date and time can be set manually or using NTP (Network Time Protocol). The NTP settings are used to accurately control the current time on the BlackPearl NAS.

Note: If you plan to join an Active Directory domain, you must configure the BlackPearl NAS 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.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. In the Date and Time pane, click **Edit**. The Edit Date and Time dialog box displays.

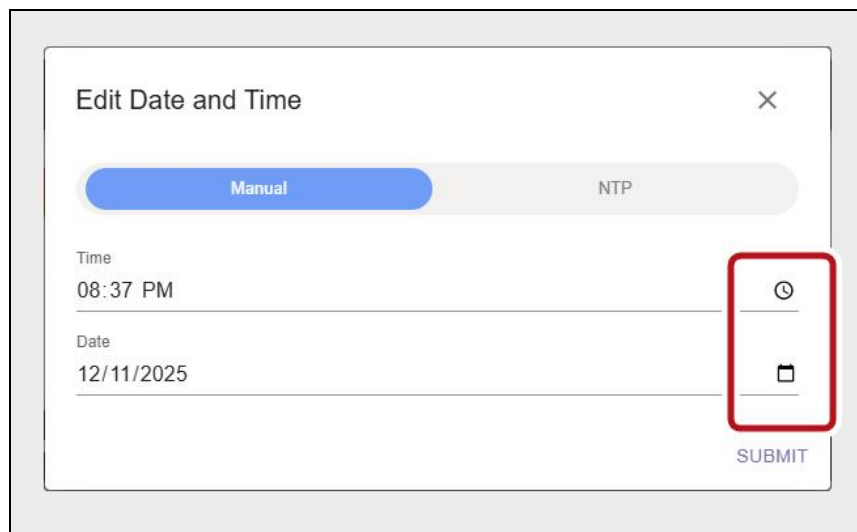


Figure 43 The Edit Date and Time dialog box.

3. Use the slider to select **Manual** or **NTP**.
 - If you select **Manual**:
 - a. Enter the current time in the **Time** field. Enter 12-hour time values and include AM or PM. Alternatively, click the clock icon and select the desired time.
 - b. Enter values in the **Date** field. Alternatively, click the calendar icon and select the desired date.
 - If you select **NTP** (not shown):
 - a. Enter the NTP server information for the **Primary NTP Server**.
 - b. If desired, enter the NTP server information for the **Secondary NTP Server**.
4. Click **Submit**.

Change the System Name

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.

2. In the Network Interfaces pane, click **Change System Name**. The Change System Name dialog box displays (not pictured).
3. Enter the desired **System Name** for the. The only allows letters, numbers, and the hyphen character (-) in the system name.

- Notes:**
- The system name cannot be only numbers.
 - The hyphen character is only allowed when the system name uses a delimiter.
 - The first section of the system name, up to a delimiter (for example, a period) cannot be longer than 15 characters:

Valid - BlackPearl.domain.com

Invalid - BlackPearlGateway.domain.com

4. Click **Submit**.

CONFIGURE NETWORKING SERVICES

Use the following instructions to configure Amazon compatible S3, Active Directory, and SNMP networking services on the BlackPearl NAS.

For instructions on configuring NAS services, see [Configure NFS and CIFS Services on page 115](#).

Configure the Active Directory Service

The Active Directory service in the BlackPearl user interface is used to connect the to a Windows Active Directory domain. Before you can join a domain, you must configure the BlackPearl NAS to use NTP. See [Configure Date and Time on page 89](#).

Note: If the BlackPearl NAS 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. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Active Directory pane, click **Join Domain**. The Join Domain dialog box displays.

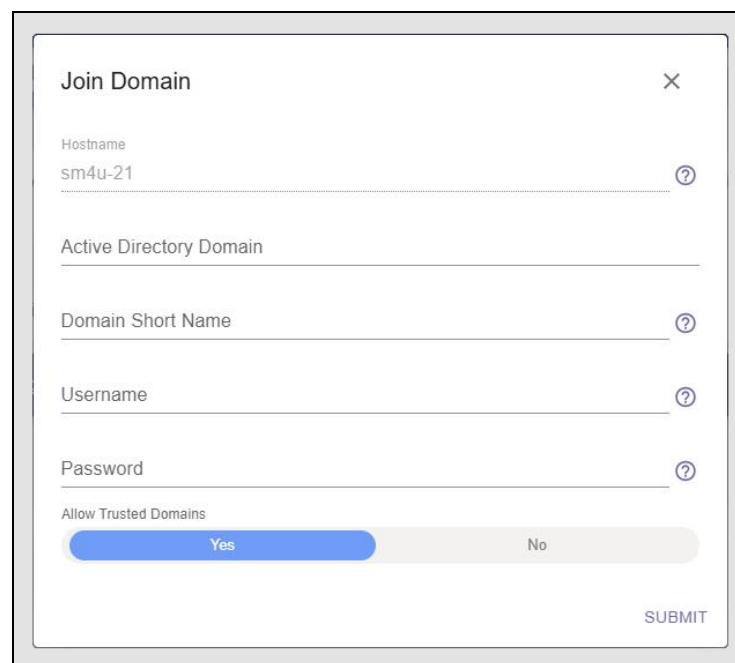
The image shows a 'Join Domain' dialog box with a title bar containing the text 'Join Domain' and a close button (X). The dialog contains several input fields: 'Hostname' with the value 'sm4u-21', 'Active Directory Domain', 'Domain Short Name', 'Username', and 'Password'. Each of these fields has a question mark icon to its right. Below these fields is a section labeled 'Allow Trusted Domains' with a toggle switch currently set to 'Yes'. At the bottom right of the dialog is a 'SUBMIT' button.

Figure 44 The Join Domain dialog box.

3. The **Hostname** identifies the BlackPearl NAS in the Active Directory domain.

Note: The hostname is unavailable and cannot be changed in the Join Domain dialog box. Use the Hardware screen to change the hostname if desired (see [Configure Network Connections on page 97](#)).

4. Enter the name of the **Active Directory Domain** you want to join.

5. Optionally, enter the **Domain Short Name** if your domain uses a non-standard workgroup name.

6. Enter the **Username** and **Password** for a user authorized to join the specified domain.

Notes:

- The BlackPearl NAS 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 BlackPearl user interface.
- You must enter the user name and password each time the BlackPearl NAS joins an Active Directory domain. The does not save this information.

7. Use the **Allow Trusted Domains** slider to select one of the following:

- **Yes** - Select this option if the Active Directory domain you want to join is a trusted domain.
- **No** - Select this option if the domain is not a trusted domain.

8. Click **Submit**.

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. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Active Directory pane, click **Add Parameter**.
3. Enter the desired **Parameter Name** and **Parameter Value**.
4. Click **Add**.

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. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Active Directory pane, click **Edit Parameter**.
3. Edit the **Parameter Name** and **Parameter Value** as desired.
4. Click **Submit**.

Edit Domain

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

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Active Directory pane, click **Edit Domain**. The Edit Domain confirmation screen displays (not shown).
3. Use the **Allow Trusted Domains** slider to select one of the following:
 - **Yes** - Select this option if the Active Directory domain you want to join is a trusted domain.
 - **No** - Select this option if the domain is not a trusted domain.
4. Click **Submit**.

Delete Advanced Parameter

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Active Directory pane, click **Delete Parameter**. The Delete Parameter confirmation screen displays (not shown).
3. Click **Delete**.

Leave Domain

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.

2. In the Active Directory pane, click **Leave Domain**. The Leave Domain confirmation screen displays (not shown).
3. Click **Leave Domain**.

Configure the SNMP Service

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the SNMP pane, click **Edit Settings**. The Edit SNMP Settings dialog box displays.

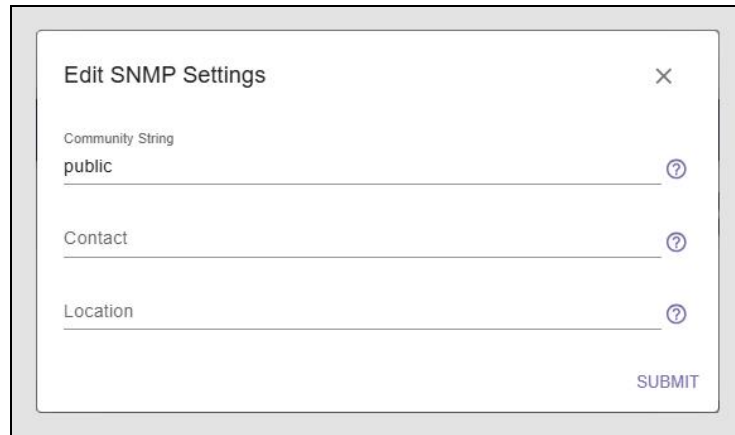


Figure 45 The Edit SNMP Settings dialog box.

3. 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 BlackPearl NAS responds to all SNMP queries.
4. Enter the primary contact for the BlackPearl NAS in the **Contact** field.
5. Enter the physical location of the in the **Location** field.
6. Click **Submit**.

Add SNMP Clients

After configuring the SNMP service, you must add clients to make SNMP queries to the BlackPearl NAS.

Here is how you add an SNMP client:

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.

2. In the SNMP pane, click **Add Client**. The Add SNMP Client dialog box displays.



Figure 46 The Add SNMP Client dialog box.

3. Enter the host IP address in the **Host** field.
4. Use the **Receive Notifications** slider to select one of the following:
 - **Yes** - The SNMP client receives outgoing notifications/traps.
 - **No** - The client does not receive outgoing notification/traps.
5. Enter the port number to be used for SNMP communication in the **Port** field
6. 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.
7. Click **Submit**.

Download the MIB File

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

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the SNMP pane, click **Download MIB**. Using your web browser, save the file to your local host.
3. Load the file into the network node manager program.
4. You can now use your network node manager program to communicate with the BlackPearl NAS, using the settings configured in [Configure Networking Services on page 91](#).

CONFIGURE NETWORK CONNECTIONS

You can use the BlackPearl user interface to configure the system Ethernet ports and configure static routes.

Note: If configuring a HotPair system, contact Spectra Logic Technical Support for instructions on configuring network connections.

Configure Ethernet Ports

This section describes using the BlackPearl user interface to configure the IP addressing for the Ethernet ports in the BlackPearl NAS. The may contain a variety of included and optional Ethernet network interface connections.

- Notes:**
- You can create one or more data connections to the.
 - You can configure link aggregation for better performance.
 - While different types of Ethernet network interface cards can be installed in the same BlackPearl NAS, only one type of port can be used in each link aggregation configuration.
 - You can only use the BlackPearl management port to access the BlackPearl user interface. You cannot use this port for data transfer.
 - The BlackPearl management port is used by external applications to trigger snapshots of NAS volumes.
 - The data connection(s) and BlackPearl management port are initially configured in [Configuring Initial Settings on page 61](#). 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 70](#)
- [Configure the Management Port below](#)
- [Add a Static Route on page 99](#)
- [Clear a Data Port Configuration on page 99](#)

Configure the Management Port

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. In the Network Interfaces pane, select the **Management** row and then click **Edit**. The Edit Data Interface dialog box displays.

Edit Data Interface [X]

Configuration ☐ DHCP ?

IPv4 & IPv6 Addresses ?

IP Address	Prefix Length	Actions
10.5.1.215	24	+ -
2620:a3:e030:1151:225:9	64	+ -

IPv4 Default Gateway
10.5.1.1 ?

IPv6 Default Gateway
fe80::72c9:c6ff:fe18:2476 ?

MTU
1500

SUBMIT

Figure 47 The Edit Management dialog box.

3. Select the **DHCP** checkbox to configure the 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 BlackPearl 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.

- **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**.

Note: The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl NAS.

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

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

7. Change the **MTU** value, if desired. If you set the MTU value to something other than 1500, make sure that your switch configuration supports larger MTU settings, as well as all the hosts on the network. Acceptable values are 576 to 65535.

Note: Most networking designs are configured to use a value of 1500 or 9000.

8. Click **Submit**.

Note: When you change the IP address of the BlackPearl 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.

Add a Static Route

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. In the Static Routes pane, click **New**. The Add Static Route dialog box displays (not shown).
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 network **Gateway** of the data connection used to communicate with the isolated network.
5. Click **Submit**.

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 97](#) to change the management port settings.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. Select the row of the configuration you want to clear and click **Clear**. A confirmation window displays (not shown).
3. Click **Delete** to clear the Ethernet configuration.

CHAPTER 4 - CONFIGURING NETWORK ATTACHED STORAGE

This chapter describes using the BlackPearl user interface to configure Network Attached Storage pools, volumes, and shares on a BlackPearl NAS.

Create a NAS Storage Pool	101
Create a Volume	104
Create a NFS Share	108
Create a CIFS Share	110
Access Control for a CIFS Share	110
Create a CIFS Share	110
Set Permissions for a CIFS Share	113
Configure NFS and CIFS Services	115
Configure the NFS Service	115
Configure the CIFS Service	115
Configure NAS Replication	116
Add a NAS Target	117
Configure the Target System	118
Configure Volumes for NAS Replication	119

CREATE A NAS STORAGE POOL

When creating a new NAS 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. You can then create a new storage pool using newly available drives.
- Any drives not configured in storage pools act as global spare drives. If a drive failure occurs, the immediately activates a global spare. When the failed drive is replaced it becomes a spare.
- Spectra Logic recommends leaving at least one drive for a global spare.

Use the following steps to create a new NAS storage pool.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Pools pane, click **New**. The Create Pool dialog box displays.

The screenshot shows the 'Create Pool' dialog box with the following configuration:

- Pool Name:** (empty field)
- High Water Mark:** 80%
- Power Saving Mode:** (disabled)
- Auto Trim:** (disabled)
- Drive Type:** 3.64 TiB, SAS
- Count:** 14
- Protection Level:** triple
- Optimization Level:** Capacity (selected), Performance
- Write Performance Drive Type:** No Drives Available
- Metadata Performance Drive Type:** No Drives Available
- Pool Preview:** A circular diagram showing a dark blue segment and a light blue segment.
- Raw Size:** 50.94 TiB
- Note:** If selected, data can be striped across multiple triple parity arrays, which can tolerate three drive failures without data loss.
- SUBMIT** button at the bottom right.

Figure 48 The Create 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.
4. Enter a **Pool Name**. The pool name is 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(.).

5. Enter a percentage for **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.
6. If desired, use the slider to enable **Power Saving Mode**. This option allows the disk drives in a disk pool to spin down after 60 minutes of inactivity.

Notes:

- This option is only available if all disk drives in the disk pool are capable of power saving mode.

- Spectra Logic recommends leaving Power Saving Mode **disabled**.

7. If desired, use the slider to enable **Auto Trim**. The option automatically removes unused data blocks from SSD and NVMe drives by marking deleted files as immediately ready for reuse, improving drive performance and longevity.
8. Use the **Drive Type** drop-down menu to select the disk drive type to use for the storage pool. Only one drive type can be used in a nearline pool.

Note: Any drive not in a disk pool acts as a global spare. A global spare drive is activated as soon as a drive configured in a disk pool fails.

9. Use the **Count** drop-down menu to select the number of drives of the previously selected type to use in the storage pool. If you plan to optimize the drive for capacity or performance, select an even number of drives.

10. Use the **Protection Level** drop-down menu to select the level of RAID protection to use on the storage pool:

- **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**—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**—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**—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.
- **None**—The pool is not configured to provide data protection. Any drive failure results in data loss.

Note: Spectra Logic does not recommend setting protection to None.

11. Use the **Optimization Level** slider to select one of the following:

- **Capacity** - The pool has more storage space, but slower performance.
- **Performance** - The pool is faster at reading and writing data with less overall capacity.

12. Use the **Write Performance Drive Type** drop-down menu to select the disk drive type to use for the write performance drives, which increase write performance when the pool is shared using NFS.

Note: This feature is only intended for storage pools with NFS shares and typically has little impact on CIFS share performance.

13. Use the **Count** drop-down menu to select the number of write performance drives to add to the storage pool.

14. Use the **Metadata Performance Drive Type** drop-down menu to select the disk drive type to use for metadata performance drives, which improve performance for restoring small files, deduplication operations, and when searching metadata.

Note: These drives are permanently part of the storage pool and cannot be removed.

15. Use the **Count** drop-down menu to select the number of metadata performance drives to add to the storage pool.

Note: Metadata Performance drives can only be selected in multiples of three.

16. Click **Submit**.

CREATE A VOLUME

Before you begin using a disk 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 you cannot share a volume using more than one method.

Volumes are thin provisioned, so it is possible for the combined allocated maximum storage of all volumes to exceed the physical space available.

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

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. Under Volumes pane, click **New**. The Create Volume dialog box displays.

The screenshot shows the 'Create Volume' dialog box with the following fields and options:

- Volume Name:** A text input field.
- Pool:** A dropdown menu currently showing 'p1'.
- Snapshot Change Threshold:** A text input field followed by a '%' symbol and a help icon.
- Min Size:** A text input field, a 'Unit' dropdown, and a help icon.
- Max Size:** A text input field, a 'Unit' dropdown, and a help icon.
- Record Size:** A dropdown menu currently showing '1 MiB' with a help icon.
- Case Insensitive (CIFS):** An unchecked checkbox with a help icon.
- Compression:** An unchecked checkbox with a help icon.
- Access Time:** An unchecked checkbox with a help icon.
- NFI Volume Policy:** A section header.
- NFI Enabled:** An unchecked checkbox with a help icon.
- SUBMIT:** A button at the bottom right.

Figure 49 The Create Volume dialog box.

3. Enter a **Volume Name**. Volume names are limited to 62 characters or fewer.

Notes:

- The combined disk 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 BlackPearl 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 BlackPearl user interface.

4. Use the **Pool** drop-down menu to select a previously configured disk pool on which you want to create a volume.

5. Enter a **Snapshot Change Threshold** percentage. This specifies the percentage of data change between consecutive snapshots that triggers a possible ransomware warning. If the percentage of data changes by more than the threshold, a message displays in the BlackPearl user interface, and an email is sent to the Administrator if the Administrator user is configured to receive warning emails.

Notes:

- Allowed values are between 0 and 99.
- Spectra Logic recommends configuring the Administrator user to receive emails when a warning event occurs.
- The BlackPearl NAS uses unique data to detect the specified percentage change when data is deleted. If you enable compression for this volume, when you change the data on the source, the percentage change on the source and the percentage change in the snapshot may not be the same. The BP uses the percentage change of the snapshot to determine when to trigger a warning.

6. Configure the **Minimum Size**:

Select the desired **Unit** size from the drop-down menu and enter a numerical value for the minimum size in the **Min Size** 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 disk 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 disk pool.

7. Configure the **Maximum Size**:

Select the desired **Unit** size from the drop-down menu and enter a numerical value for the maximum size in the **Max Size** 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 disk pool.

8. Use the **Record Size** drop-down menu to select a record size for the volume. This setting determines how data is divided and stored on disk. In general, larger values increase performance at the cost of increased storage space requirements.

**IMPORTANT**

The default value is 1 MiB. Only change this value at the direction of Spectra Logic.

9. If desired, select **Case Insensitive (CIFS)** 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.

- Notes:**
- This option should only be used for volumes shared using CIFS and **cannot** be changed after creating the volume.
 - Creating a CIFS share on a case-sensitive volume reduces performance.
 - Case-insensitive volumes are useful for Commvault® targets.

**CAUTION**

DO NOT enable this setting if you plan to share the volume using NFS.

10. If desired, select **Compression** to enable data compression using ZFS LZ4 algorithm to allow the BlackPearl to store more data. If the data being written is compressible there is typically an increase with store and restore operations, because less data is transferred to and from the disk drives. The size reduction of transferred files depends on how much the system can compress the data, and may fluctuate.

The data compression process uses CPU cycles to perform the compression. If compression is enabled for non-compressible data, for example JPEG images or movie files that use the H. 264 codec, the compression process may use an excessive number of CPU cycles, slowing the overall performance of the. This impact is less evident with Gen2 and Gen3 master nodes.

11. If desired, select **Access Time** to configure the to update the time stamp of a file when it is read from the volume.

Note: Enabling this option may slow performance.

12. Do one of the following:

- If you are configuring this volume to use NFI replication, continue to [Configure NFI Volume Policy on the next page](#).
- If you are not configuring NFI, click **Submit**.

Configure NFI Volume Policy



IMPORTANT

The options for the NFI Volume Policy are only used to transfer files from the NAS volume to object storage on a BlackPearl NAS.

The screenshot shows a 'Create Volume' dialog box with a close button (X) in the top right corner. The 'NFI Volume Policy' section is active, showing a checked 'NFI Enabled' checkbox with a help icon. Below this, the 'Copying Rule' is set to 'Copy and Keep' (highlighted in blue) with 'Copy and Delete' as an alternative. The 'BlackPearl System' and 'Bucket' fields are empty, each with a help icon. The 'NFI Schedule' section shows 'Repeat' set to 'Hourly' and 'Every' set to '1' hour(s) at Minute '00'. A 'SUBMIT' button is located at the bottom right of the dialog.

Figure 50 The Create Volume dialog box - NFI Options.

CREATE A NFS SHARE

After you create one or more volumes, you can share a volume using the NFS service.

Note: Shares are not available until network settings are configured. See [Configure the Data Connection on page 70](#).

Use the following steps to create an NFS share.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Shares pane, use the slider on the right side to select **NFS**.

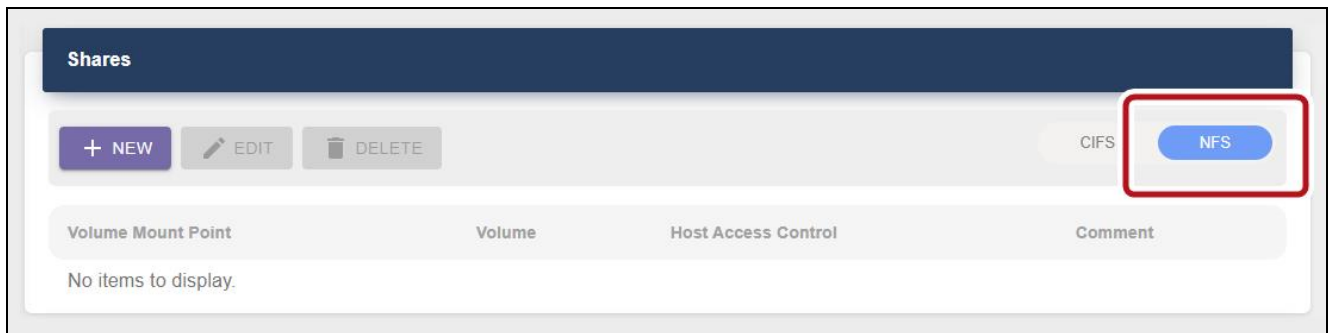


Figure 51 The NAS screen - Shares pane - NFS.

3. In the Shares pane, click **New**. The Create Share dialog box displays.

Figure 52 The New NFS Share dialog box.

4. Use the **Volume** drop-down menu to select the previously configured volume you want to share using NFS.

5. 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.

6. If desired, enter a comment in the **Comment** field. This comment only displays on the BlackPearl user interface.
7. In the **Host Access Control** pane, 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 BlackPearl NAS.

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.

8. Click **Submit**.

CREATE A CIFS SHARE

After you create one or more volumes, you can share a volume the CIFS service for use in a Windows environment. Creating a CIFS share consists of 3 major steps:

1. Joining an Active Directory or enabling CIFS access control - this step is usually only required the first time you create a CIFS share. See [Access Control for a CIFS Share below](#).
2. Creating the CIFS share. [Create a CIFS Share below](#)
3. Setting Permissions for CIFS Share - This step is required for each CIFS share you create. See [Set Permissions for a CIFS Share on page 113](#)

Note: Shares are not available until network settings are configured. See [Configure the Data Connection on page 70](#).

Access Control for a CIFS Share

Spectra Logic recommends using Active Directory to control access to CIFS shares on the BlackPearl NASs.

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

- [Configure the Active Directory Service on page 91](#)

-OR-

- [Enable CIFS User Access on page 146](#)

Once you have completed one of the above, continue to [Create a CIFS Share below](#).

Create a CIFS Share

1. If necessary, join an Active Directory domain or configure a user for CIFS user access as described in [Access Control for a CIFS Share above](#). You do not need to do both. This step is usually only required when you create the first CIFS share.
2. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.

3. In the Shares pane, use the slider on the right side to select **CIFS**.



Figure 53 The NAS screen - Shares pane - CIFS.

4. In the Shares pane, click **New**. The Create CIFS Share dialog box displays.

The screenshot shows a 'Create CIFS Share' dialog box. It has a title bar with a close button (X). The form contains the following fields: 'Share Name' with the value 'kctest', 'Volume' with a dropdown menu showing 'kctest', and 'Path' with the value '/'. Below these fields is a 'Read Only' section with two buttons: 'Enabled' (gray) and 'Disabled' (blue). The 'Disabled' button is selected. At the bottom right of the dialog is a 'SUBMIT' button.

Figure 54 The Create CIFS Share dialog box.

5. Enter a **Share Name** for the CIFS share. This is the name that is displayed in Active Directory configurations.
6. Use the **Volume** drop-down menu to select the previously configured volume you want to share using CIFS.

Note: Creating a CIFS share on a case-sensitive volume reduces performance.

7. Enter the desired network access for the **Path** to the share. The default path allows access to the root of the volume.

After creating the CIFS share, you can connect to it using your Windows-based host and create subdirectories in the share. You can use the **Path** field to allow access to specific directories by specifying the exact subdirectory.

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.

Note: If you use a path that starts with two slashes (for example `\\path`) you are unable to edit permissions after the share is created.

8. Use the **Read Only** slider to select one of the following:
 - **Enabled** - The system prevents any data from being written to the share.
 - **Disabled** - Both read and write operations are available.
9. Click **Submit**.

Set Permissions for a CIFS Share

When a CIFS share is created, the default permission is “Everyone”. This allows the 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.

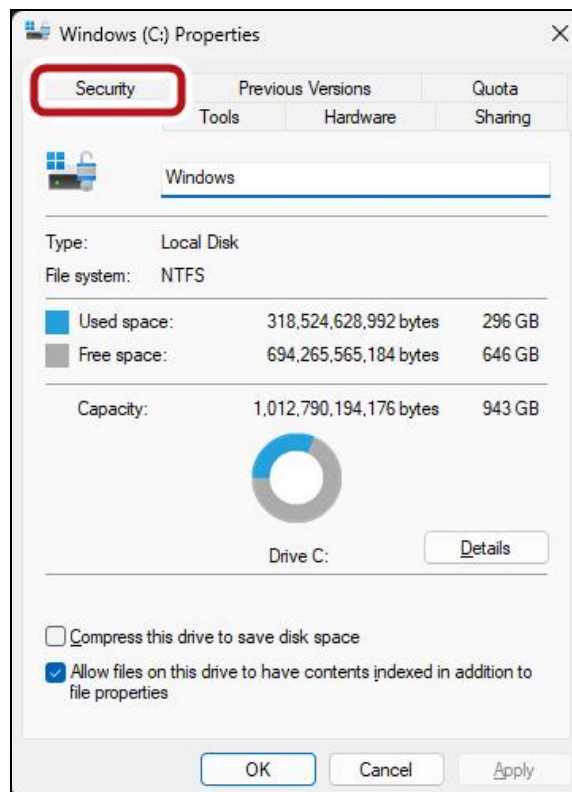


Figure 55 The Properties window.

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

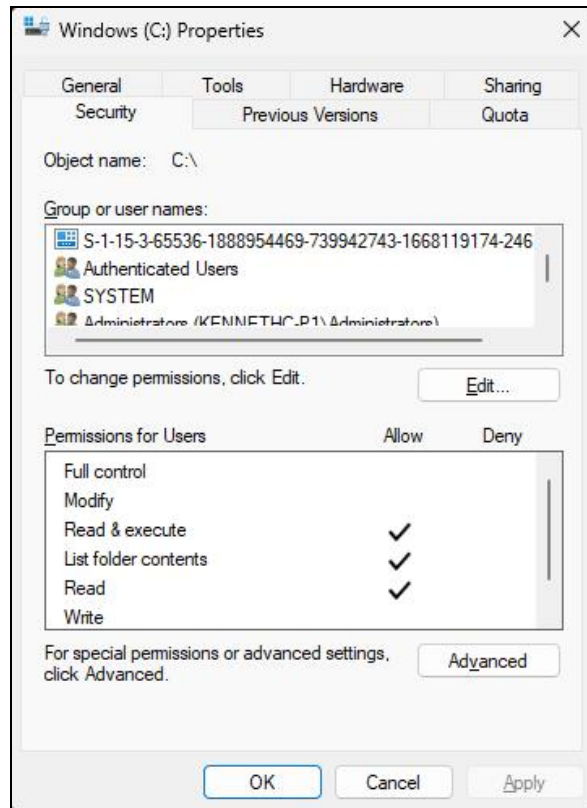


Figure 56 The Security tab.

4. Add, or remove users, or modify permissions for users as needed for your storage environment.

5. Click **OK**.

Note: If you remove the "Everyone" group permission in Windows, you must log out of Windows, and then log in again for the change to take effect.

CONFIGURE NFS AND CIFS SERVICES

The NFS and CIFS services are methods of sharing NAS volumes for use by other computers on the network.

Configure the NFS Service

If desired you can configure the transmission protocols and number of threads used by the NFS service. Use the following steps to edit the NFS service.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the NFS pane, click **Edit**. The Edit NFS Settings dialog box displays (not shown).
3. Use the sliders to enable or disable the **TCP** and **UDP** transmission protocols.
4. Enter the number of **Threads** for use by the service.

Note: The default setting is sufficient for most network configurations.

5. Click **Save**.

Configure the CIFS Service

If desired, you can add an advanced parameter for the CIFS service. Advanced parameters are used to adjust/set global or share specific Samba parameters.

Additionally, parameters can be edited and deleted after they are created.



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. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the CIFS pane, click **Add Parameter**. The Add Advanced Parameter dialog box displays (not shown).
3. Enter the desired **Parameter Name** and **Parameter Value**.
4. Click **Create**.

CONFIGURE NAS REPLICATION

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

This feature also allows you to easily transfer snapshot data stored on NAS volumes to a remote BlackPearl NAS. These snapshots can be retained for archival purposes or restored on the target to replicate the data contained in the snapshot.

Once you configure the replication service, you need to configure each volume on the that you want to replicate.

Note: This replication service is only for replicating NAS volumes on the to BlackPearls with NAS enabled or other BlackPearl NAS solutions. To replicate NAS volumes to BlackPearl managed object storage, use NFI replication (see [Create a Volume on page 104](#)).

Use the instructions in this section to configure the NAS replication service and to configure volumes for replication.

- Notes:**
- There must be enough space on the target to hold the replicated data, or the replication fails.
 - Multiple volumes on the source device cannot replicate to a single volume on the target. Each volume on the source device must replicate to a different volume on the target.
 - If multiple devices replicate to the same target, the target must use a different volume for each replication source.
 - You must configure the data ports on the source and the target systems before you can configure replication (see [Configure Network Connections on page 97](#)).
 - Your firewall must allow the source and all targets configured for replication to access **port 59373** for configuring replication, and **ports 59374-59400** for replication data transfers.
 - The user account on the target system used for configuring NAS replication cannot be configured to use multi-factor authentication.
 - For both the source and the targets, make sure you have completed the steps in [Configuring Initial Settings on page 61](#).

Add a NAS Target

Use the instruction in this section to add a NAS target.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Replication Targets pane, use the **Replication Type** drop-down menu to select NAS.

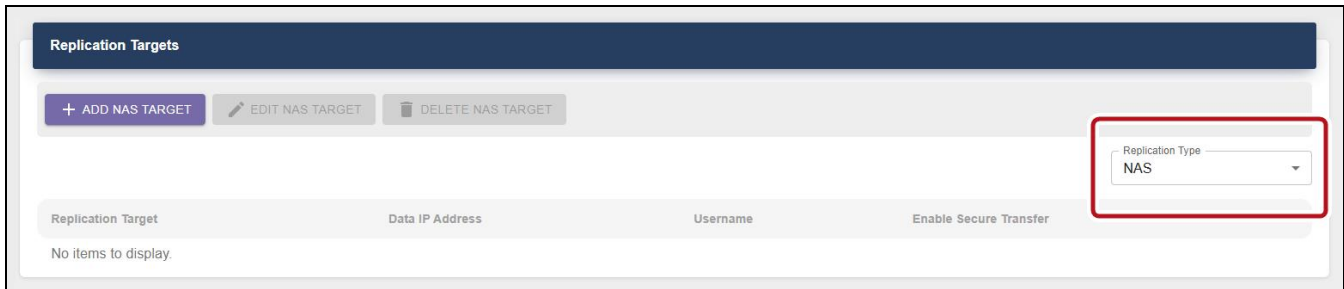


Figure 57 The NAS screen - Replication Targets pane.

3. In the Replication Targets pane, click **Add NAS Target**. The Add Target dialog box displays.

Figure 58 The Add 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.
Note: Replications fail if the user account on the target system is configured to use multi-factor authentication.
7. Enter the user password in the **Password** field, if one is set. Otherwise, leave the field blank.
8. Select the **Enable Secure Transfer** checkbox to configure the to encrypt the replicated data before transferring it to the target. Data is encrypted using Secure Socket Layer (SSL).
9. Click **Submit**.

Configure the Target System

If you have not already done so, use the instructions below to create a disk pool and volume to be the target for the replication.

1. Log into the BlackPearl on the **target system** as described in [Log Into the BlackPearl User Interface on page 68](#).
2. Create one or more storage pools as described in [Create a NAS Storage Pool on page 101](#).
3. Create one or more volumes as described in [Create a Volume on page 104](#). You must create one volume on the **target system** for each volume you want to replicate on the **source system**. Additionally, you can create volumes when performing the steps in [Configure NAS 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 NAS Replication

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.

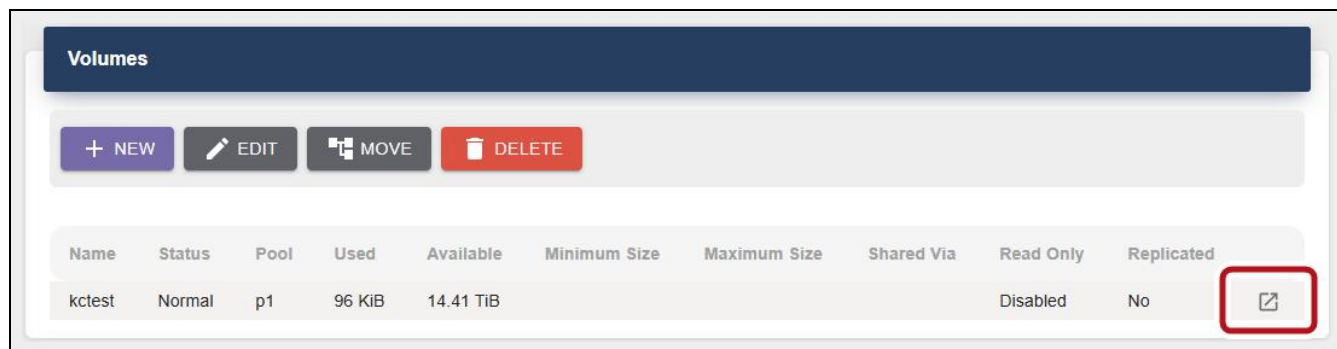


Figure 59 The NAS screen - Volumes pane - Details button.

2. In the Volumes pane, on the right side, click the **Details** button for the Volume you want to enable NAS replication. The details screen for the volume displays.

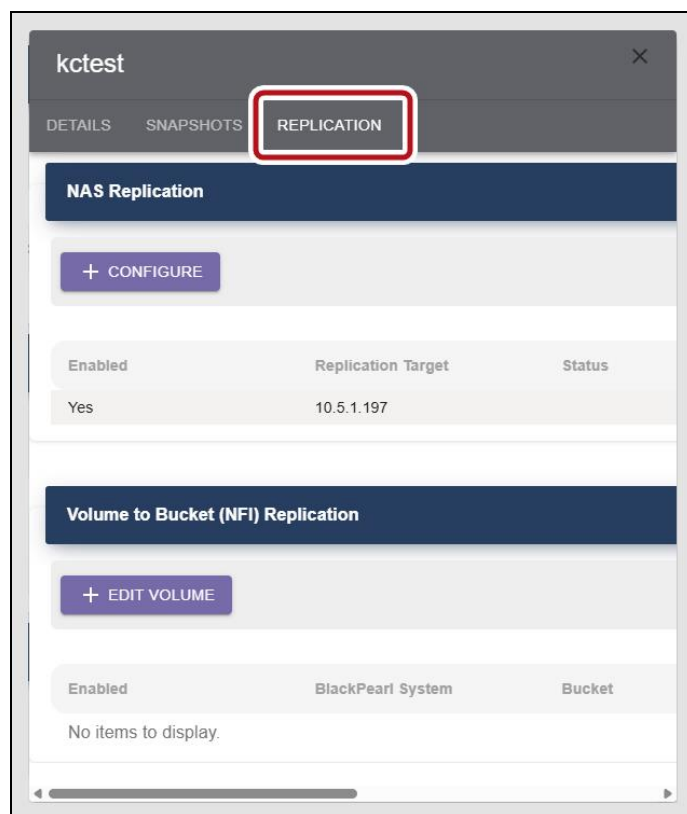


Figure 60 The Volume details screen - Replication.

3. Select the **Replication** tab at the top of the screen.

4. In the NAS Replication pane, click **Configure**. The Configure NAS Replication dialog box displays.

Figure 61 The Configure NAS Replication dialog box.

5. Use the **Enabled** slider to select **Yes** to enable NAS replication for the volume.
6. Use the **Replication Target** drop-down menu to select a previously configured NAS replication target. The targets are listed by the IP address or hostname entered when you configured the target.
7. Enter the **Destination Pool Name** of the storage pool on the target you want to use for replication. This field is case sensitive.
8. Enter the **Destination Volume Name** of a volume that resides on the target storage pool you selected in [Step 7](#), or enter a 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 replicates data to the target.

- 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 volume is erased each time data is replicated. Confirm the warning message to continue.

9. Use the **Repeat** drop-down menu to select one of the following:

- Select **Hourly** and use the **Hours** and **Minute** drop-down menus to select values for **Every _ Hours at Minute _**. These values specify the interval in hours between replicating data, and the number of minutes after the top of the hour when the job starts. For example, if the values are set to 4 and 15, a data is replicated every four hours, at 15 minutes after the hour.
- Select **Daily** and enter a value for **Every** to specify the interval, in days, between replicating data. Then use the **Hour** and **Minute** drop-down menus to specify the time of day to start the replication.
- Select **Weekly** and use the **Every** drop-down menu to select one or more day(s) of the week on which to replicate data. Then use the **Hour** and **Minute** drop-down menus to specify the time of day to start the job.

10. Click **Submit**.

CHAPTER 5 - CONFIGURING SECURITY AND DATA PROTECTION FEATURES

This chapter describes using the BlackPearl user interface to configure security options for the, such as Multi-Factor Authentication, volume snapshots, encryption, and database backups, all which help you maintain the security of your system and data.

Volume Snapshots	123
Create a Snapshot	123
Configure a Snapshot Schedule	125
Delete Snapshots	127
Delete a Snapshot Schedule	128
Restore to a Snapshot	129
Retrieve a Single File from a Snapshot	130
Multi-Factor Authentication	132
Enable Multi-Factor Authentication for a User	132
Log In to a System Configured to Use Multi-Factor Authentication	133
Update Multi-Factor Authentication for a User	134
Disable Multi-Factor Authentication for a User	135
Disable the Attack Hardened Service	136
Configure and Use Encryption	137
Configure the Encryption Service	137
Export Encryption Key to USB Drive	139
Change the Encryption Password	140
Unlock the Self-Encrypting Drives	141
PSID Erase an Encryption Drive	142

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.

Notable features of volume snapshots are:

- Snapshots are immutable to the outside world. Snapshots cannot be overwritten or altered, and can only be deleted by a BlackPearl administrator.
- Snapshots can be used to restore access to data in the case of a ransomware attack, and can be useful in restoring a file that was accidentally deleted.
- Snapshots are created manually, on a schedule, or triggered by external applications such as the Spectra StorCycle application.

Volume snapshots are retained on the 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 the 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 modified or 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 0 bytes 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

Here is how you create a snapshot:

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Volumes pane, select the row of the volume for which you want to generate a snapshot, then click the **Details** button on the right-hand side of the row.

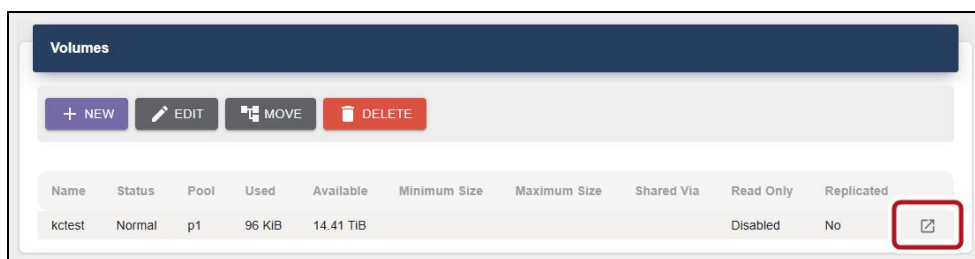


Figure 62 The NAS screen - Volumes pane - Details button.

3. On the Volume Details window, click **Snapshots**.
4. In the Snapshots pane, click **New**.

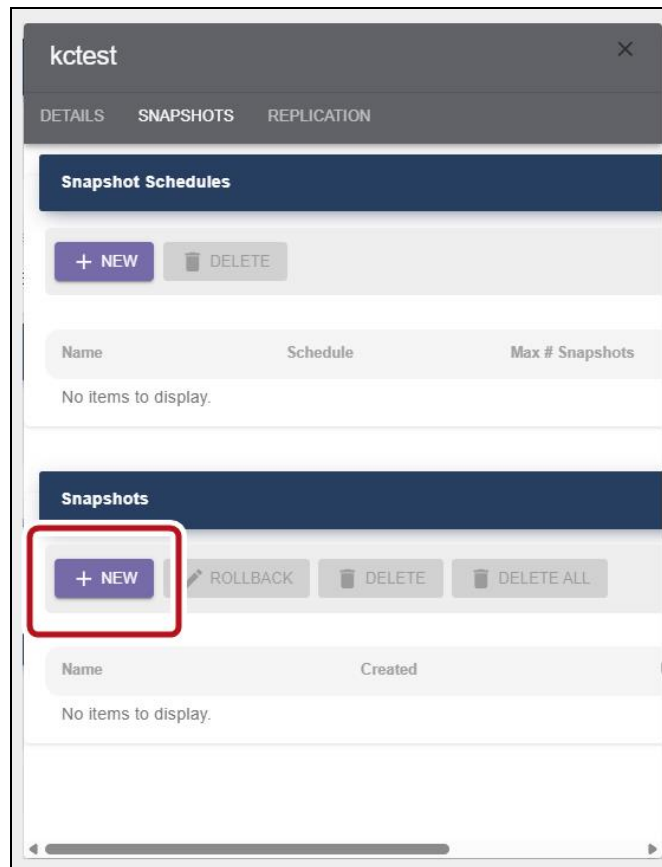


Figure 63 The Volume Details window - Snapshots pane - New Snapshot button.

5. Enter a **Name** for the Snapshot.



Figure 64 The New Snapshot dialog box.

6. Click **Submit**.

Configure a Snapshot Schedule

Snapshot schedules can be configured at intervals based on hours, number of days, or days of the week.

Here is how you configure a snapshot schedule:

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Volumes pane, select the row of the volume for which you want to configure a snapshot schedule, then click the **Details** button on the right-hand side of the row.

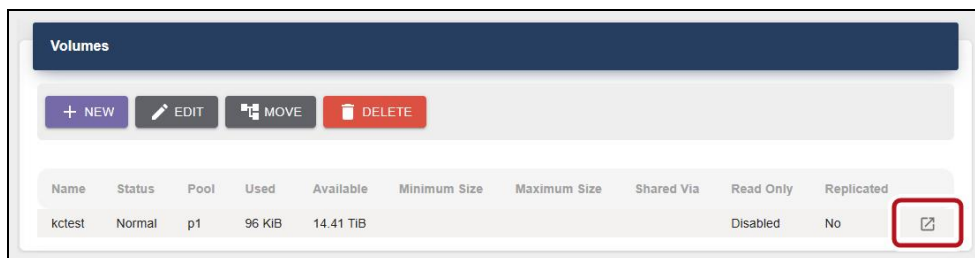


Figure 65 The NAS screen - Volumes pane - Details button.

3. On the Volume Details window, click **Snapshots**.
4. In the Snapshot Schedules pane, click **New**.

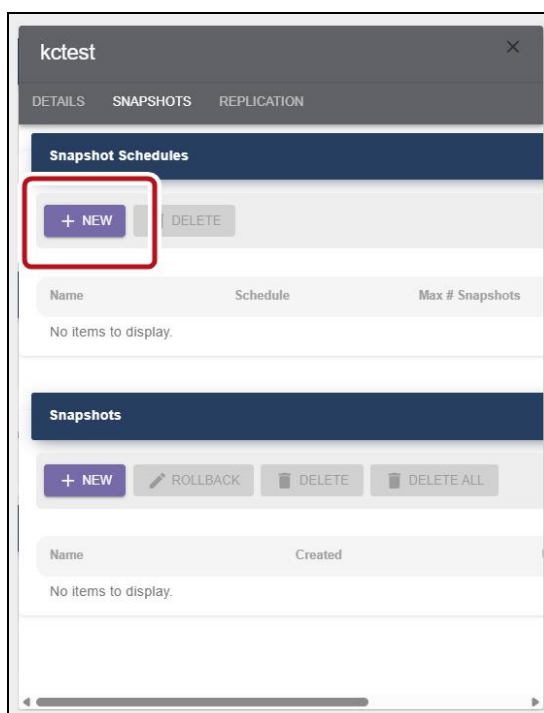


Figure 66 The Volume Details window - Snapshots pane - New Snapshot Schedule button.

5. On the New Snapshot Schedule dialog box, enter a **Name** for the schedule.

Note: Snapshot schedule names must be unique.

Figure 67 The New Snapshot Schedule dialog box

6. Enter a value for the **Maximum Number of Snapshots** for the volume. When this limit is reached, one of the behaviors described [Step 7](#) occurs.

7. Use the **Auto Delete Snapshots** slider to select one of the following:

- **Enabled** - When the maximum number of snapshots is reached, the oldest snapshot is deleted to free space for the next snapshot.
- **Disabled** - When the maximum number of snapshots is reached, the BlackPearl NAS stops creating new snapshots for the volume.

8. Use the **Repeat** drop-down menu to select one of the following:

- Select **Hourly** and use the **Hours** and **Minute** drop-down menus to select values for **Every _ Hours at Minute _**. These values specify the interval in hours between generating volume snapshots, and the number of minutes after the top of the hour when the job starts. For example, if the values are set to 4 and 15, a snapshot is created every four hours, at 15 minutes after the hour.
- Select **Daily** and enter a value for **Every** to specify the interval, in days, between generating volume snapshots. Then use the **Hour** and **Minute** drop-down menus to specify the time of day to create the snapshot.
- Select **Weekly** and use the **Every** drop-down menu to select one or more day(s) of the week on which to generate volume snapshots. Then use the **Hour** and **Minute** drop-down menus to specify the time of day to create the snapshot.

9. Click **Submit**.

Delete Snapshots

Here is how you delete one or more snapshots:

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Volumes pane, select the row of the volume for which you want to delete a snapshot, then click the **Details** button on the right-hand side of the row.

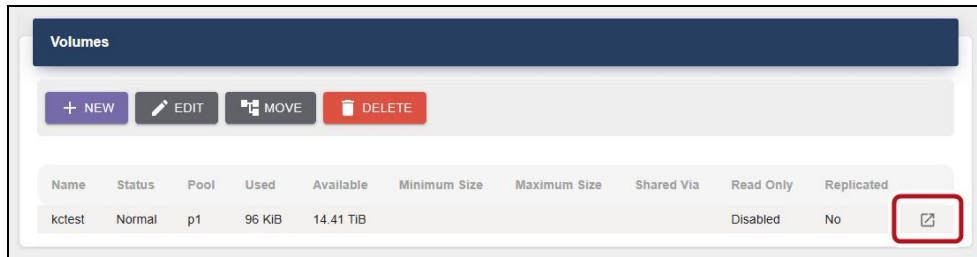


Figure 68 The NAS screen - Volumes pane - Details button.

3. On the Volume Details window, click **Snapshots**.
4. In the Snapshot pane, do one of the following:
 - To delete a single snapshot - select the snapshot and click **Delete**.
 - To delete all snapshots - click **Delete All**.

A confirmation screen displays (not shown).

5. Enter the required information in the entry field to confirm the deletion, then click **Submit**.

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 Snapshots on the previous page](#).

Here is how you delete a snapshot schedule:

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
2. In the Volumes pane, select the row of the volume for which you want to delete a snapshot schedule, then click the **Details** button on the right-hand side of the row.

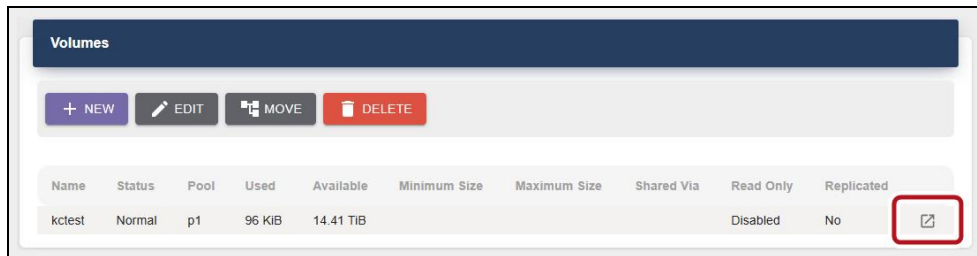


Figure 69 The NAS screen - Volumes pane - Details button.

3. On the Volume Details window, click **Snapshots**.
4. In the Snapshot Schedules pane, select the schedule you want to delete, then click **Delete**. A confirmation screen displays (not show).
5. Click **Submit**.

Restore to a Snapshot

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

- Notes:**
- If you only want to restore a single file in the snapshot, see [Volume Snapshots on page 123](#).
 - You cannot restore to a snapshot if the volume contains a BlackPearl Object Manager (Vail) share using the BlackPearl user interface. Use API or CLI commands to restore a snapshot when the volume contains an Object Manager share.
1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
 2. In the Volumes pane, select the row of the volume for which you want to restore a snapshot, then click the **Details** button on the right-hand side of the row.

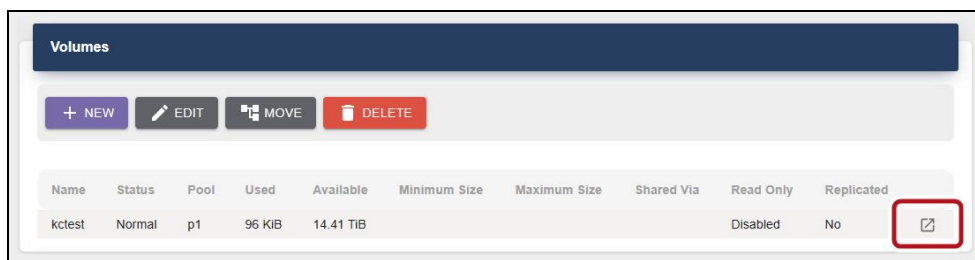


Figure 70 The NAS screen - Volumes pane - Details button.

3. On the Volume Details window, click **Snapshots**.

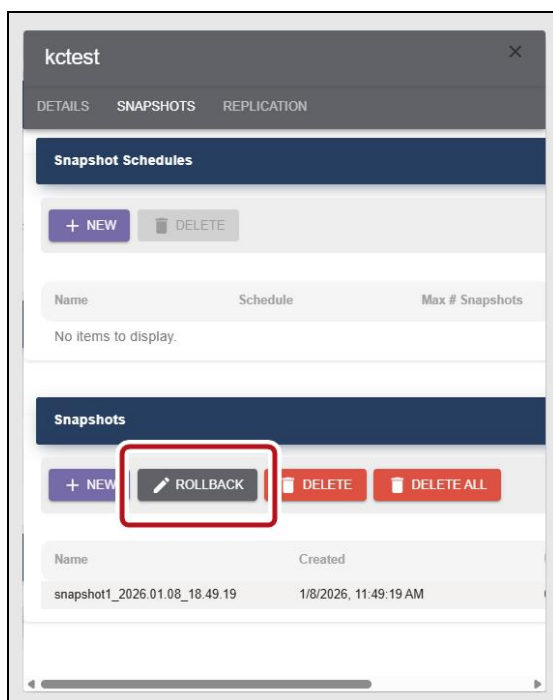


Figure 71 The Volume Details window - Snapshots pane - Rollback button.

4. In the snapshots list, select the snapshot you want to use to restore the volume and click **Rollback**. A confirmation screen displays.

**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.

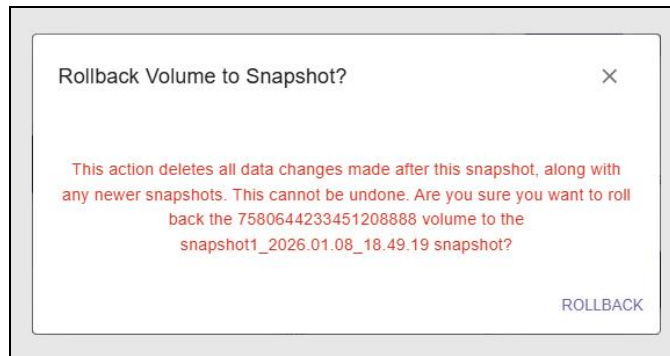


Figure 72 Confirm the volume snapshot rollback.

5. Click **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. If necessary, locate the snapshot from which you want to restore a file.
 - a. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.
 - b. In the Volumes pane, select the row of the volume for which you want to restore a snapshot, then click the **Details** button on the right-hand side of the row.

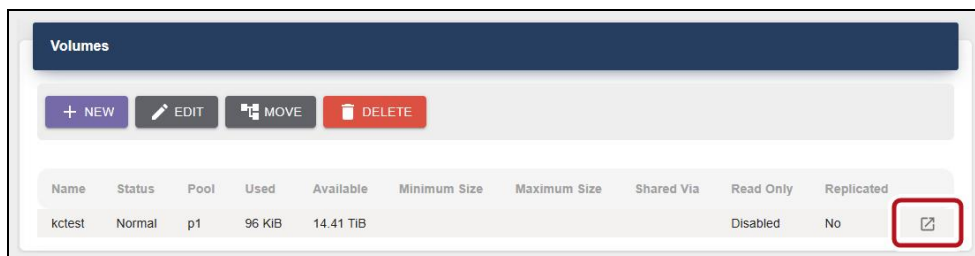


Figure 73 The NAS screen - Volumes pane - Details button.

- c. Locate the snapshot from which you want to restore a file and record the name, if desired.

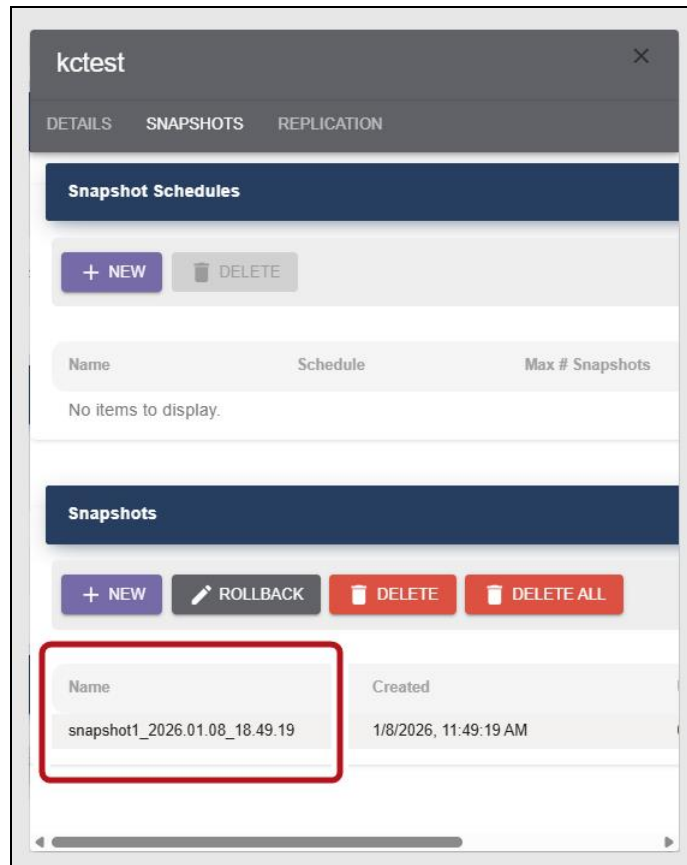


Figure 74 The NAS screen - Volumes pane - Snapshot name.

2. 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:\")
3. 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

4. The specified directory displays. All files contained in the snapshot display.
5. Locate the file you want to restore and copy it to the appropriate location.

MULTI-FACTOR AUTHENTICATION

The Spectra BlackPearl NAS offers multi-factor authentication as part of Attack Hardened storage, which enhances the security of your by using Google Authenticator or Microsoft Authenticator to confirm the identity of any user trying to log in to the BlackPearl NAS. This prevents unauthorized access to the even if the user credentials needed to access the system are compromised.

Multi-factor authentication works on a per-user basis by generating a token in the form of a QR code for a selected system user. The user scans the QR code using the Authenticator app to complete the account creation. After the QR code is scanned, the Authenticator app generates a six-digit number every 30 seconds, and does not require cell or internet access to generate these codes.

After multi-factor authentication is enabled, when the user attempts to log in to the BlackPearl user interface, after entering their username and password, they must enter the six-digit number generated by the Authenticator app within 30 seconds to complete the log in.

Enable Multi-Factor Authentication for a User

- Notes:**
- Only Administrator users can configure the Attack Hardened Service and enable Multi-Factor authentication for a user.
 - The user account on the target system configured for NAS replication cannot use multi-factor authentication.
1. If necessary, download and install Google Authenticator or Microsoft Authenticator on your mobile phone.
 2. In the BlackPearl user interface, use the toolbar in the upper-right to select **Settings (gear icon) > Users**.

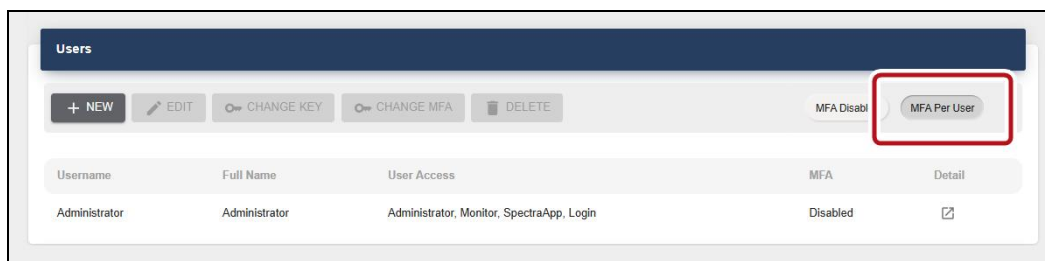


Figure 75 The Users screen - MFA Per User button.

3. If necessary, enable the MFA feature:
 - a. Click **MFA Per User**. A confirmation screen displays (not pictured).
 - b. Enter `CHANGE MFA` in the entry field, then click **Submit**.

4. Select the user and then click **Change MFA**. The Change MFA dialog box displays.



Figure 76 The Change MFA dialog box.

5. Use the Authenticator app on your phone to **scan** the QR code displayed in the BlackPearl user interface. The username and BlackPearl NAS name display in the Authenticator app, and the authenticator begins generating codes for the user.
6. In the BlackPearl user interface, in the Confirm MFA Code dialog box, enter **CHANGE MFA**, and click **Submit**.

The next time the user logs into the BlackPearl user interface, they must use the code generated by the Authenticator app to complete the log in process.

Log In to a System Configured to Use Multi-Factor Authentication

1. Using a standard web browser, enter the IP address for the BlackPearl management port configured in [Configure the BlackPearl Management Port on page 65](#).

Note: The BlackPearl user interface uses a secure connection.

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

The BlackPearl NAS ships with non-signed SSL certificates for both the data and management ports. When using the shipped certificates, you must pass a security check every time you attempt to access the management port to view the BlackPearl 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 85](#).

3. Enter the **Username** and **Password**.

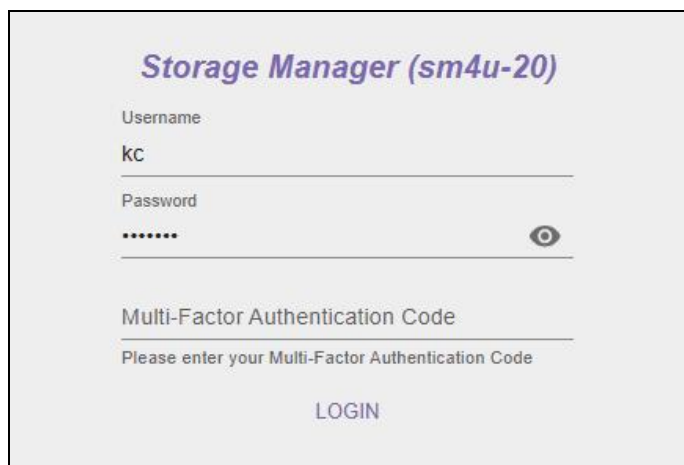
The image shows a login screen for 'Storage Manager (sm4u-20)'. It has a light gray background. At the top, the title 'Storage Manager (sm4u-20)' is in a purple font. Below it, there are three input fields: 'Username' with the text 'kc', 'Password' with masked characters '*****' and an eye icon to its right, and 'Multi-Factor Authentication Code'. Below the MFA field is a hint: 'Please enter your Multi-Factor Authentication Code'. At the bottom center is a purple 'LOGIN' button.

Figure 77 The Login screen with Multi-Factor Authentication enabled on the system.

4. Using Google Authenticator on your phone, enter the six-digit **Multi-Factor Authentication Code** for the user.

- Notes:**
- The code refreshes every 30 seconds. If the code refreshes before you complete the login, you must clear the field and enter the new code.
 - If you have more than one user or BlackPearl NAS configured in Google Authenticator, use the *username@systemname* to locate the correct code. The system name is displayed under the product name on the login screen.

5. Click **Login**.

Update Multi-Factor Authentication for a User

If desired, you can update the token that the Authenticator app uses to generate the MFA code. This is necessary if you disabled the Attack Hardened service, and then later re-enabled the service. This can also be used to provide enhanced security as required by your security environment by updating authentication credentials while still maintaining access for the user.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.

2. Select the user and then click **Change MFA**. The Change MFA dialog box displays.
3. Use the slider to select **Update MFA**.



Figure 78 The Change MFA dialog box.

4. Use the Authenticator app on your phone to **scan** the QR code displayed in the BlackPearl user interface. The username and BlackPearl NAS name display in the Authenticator app, and the authenticator begins generating codes for the user.
5. In the BlackPearl user interface, in the Confirm MFA Code dialog box, enter CHANGE MFA, and click **Submit**.

The next time the user logs into the BlackPearl user interface, they must use the code generated by the Authenticator app to complete the log in process.

Disable Multi-Factor Authentication for a User

Use this option to no longer require a user to enter an MFA code when logging in to the BlackPearl user interface.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. Select the user and then click **Change MFA**. The Change MFA dialog box displays (not shown).
3. Use the slider to select **Disable MFA**.
4. In the dialog box, enter CHANGE MFA, and click **Submit**.

The user is no longer required to enter a six-digit authentication code when logging in to the BlackPearl user interface.

Disable the Attack Hardened Service

Disabling the Attack Hardened service disables multi-factor authentication for the BlackPearl NAS.

Note: Disabling the Attack Hardened service deletes the tokens for all users configured to use multi-factor authentication. If you re-enable the Attack Hardened service, each user will need to update their multi-factor authentication token. See [Multi-Factor Authentication on page 132](#).

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. In the upper-right corner of the Users pane, click **MFA Disabled**. A confirmation screen displays (not pictured).
3. Enter `CHANGE MFA` in the entry field, then click **Submit**.

CONFIGURE AND USE ENCRYPTION

If your BlackPearl NAS includes disk or solid state 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.

- Notes:**
- An activation key is required to enable this feature.
 - The encryption provided by SEDs is 'encryption at rest'. If a drive is stolen the data on it is unreadable.

Configure the Encryption Service

Use the encryption service to set the level of encryption and create a password to unlock the drives following a power cycle. You can select to store the password on the, 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.



CAUTION

Spectra Logic recommends creating and storing multiple copies of the password used to encrypt data to avoid losing access to encrypted data.

1. If necessary, enter the activation key to enable the encryption service as described in [Manually Enter Activation Keys on page 198](#).
2. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.

3. In the Encryption pane of the Users screen, click **Edit Service**. The Edit Encryption Service dialog box displays.

Figure 79 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. Drives must be set to unencrypted for each storage pool. See Configure and Use Encryption on the previous page for instructions.
Encrypt and Store Password	The self-encrypting drives encrypt data transferred to them, and the password to unlock the drives is stored on the BlackPearl NAS. The drives are automatically unlocked when the BlackPearl NAS initializes.  CAUTION Even though the password is stored on the system, it is important to record the password and store it in a secure location to avoid losing access to the encrypted data. The password may also be required in the cases of chassis replacement, or the addition of more BlackPearl NASs to the storage architecture that may access the encrypted drives. Spectra Logic recommends storing multiple copies of the password.

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 BlackPearl user interface.
7. If necessary, enter the **Multi Factor Authentication** code for the user (not shown). See [Multi-Factor Authentication on page 132](#) for information on obtaining the multi-factor authentication code.

Note: This field only displays if multi-factor authentication is enabled for the currently logged in user.

8. Enter `ENCRYPT` into the confirmation dialog box.
9. Click **Submit**.

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

Export Encryption Key to USB Drive

Use the instructions in this section to export the encryption key to a USB drive for storage in case of disaster recovery. This key can be used to re-import the encryption key if necessary.



CAUTION

Spectra Logic recommends creating and storing multiple copies of the password used to encrypt data to avoid losing access to encrypted data. Additionally, Spectra Logic recommends exporting the encryption key to multiple types of storage media.

1. Connect a USB key in to a USB port on the rear of the BlackPearl chassis.
2. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
3. In the Encryption pane on the Users screen, click **USB Key**. The Export Key to USB dialog box displays (not shown).
4. Enter the **User Password** of the user currently logged into the BlackPearl user interface.
5. Click **Submit**.

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

Change the Encryption Password

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

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Encryption pane on the Users screen, click **Change Password**. The Change Encryption Password dialog box displays.

Note: If multi-factor authentication is enabled for the user currently logged in to the BlackPearl user interface, an additional entry field displays in the Change Encryption Password dialog box. (Additional entry field not shown).

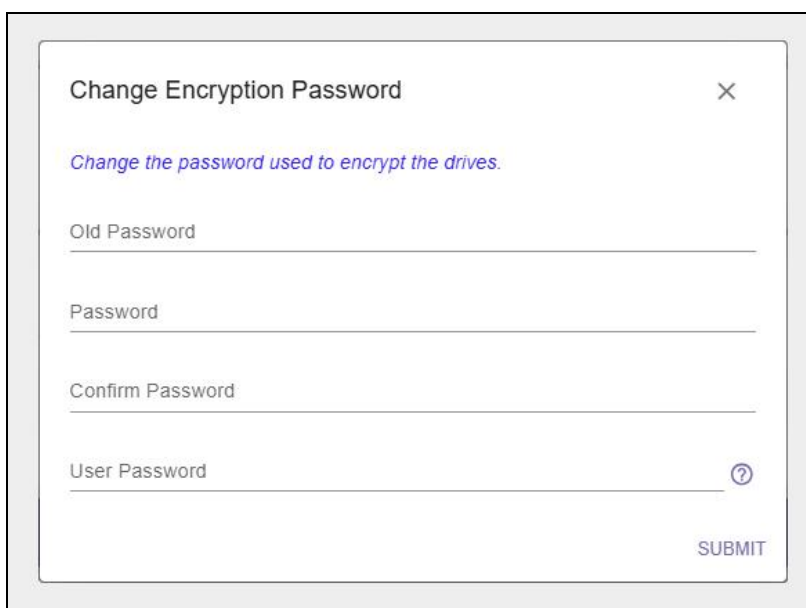


Figure 80 The Change Encryption Password dialog box.

3. Enter the current password in the **Old Password** entry field.
4. Enter the desired new **Password**, and then **Confirm Password**.
5. Enter the **User Password** of the user currently logged in to the BlackPearl user interface.
6. If necessary, enter the **Multi Factor Authentication** code for the user. See [Multi-Factor Authentication on page 132](#) for information on obtaining the multi-factor authentication code.

Note: This field only displays if multi-factor authentication is enabled for the currently logged in user.

7. Click **Submit**.



IMPORTANT

After changing the password, update the USB keys and/or manual records stored in secure locations.

Unlock the Self-Encrypting Drives

If necessary, use the instructions below to manually unlock the self-encrypting drives after the initializes.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
2. In the Encryption pane on the Users screen, click **Unlock All Disks**. The Unlock All Disks dialog box displays.

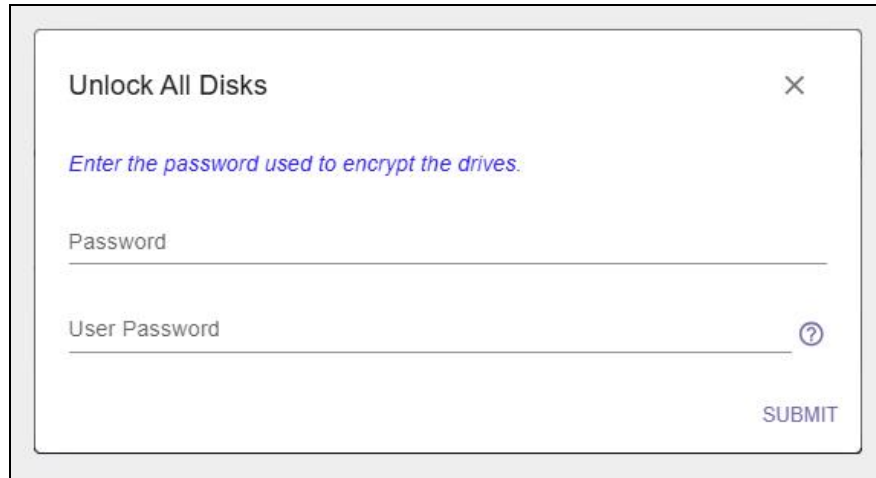


Figure 81 The Unlock All Disks dialog box.

3. Enter the encryption **Password**.
4. Enter the **User Password** of the user currently logged in to the BlackPearl user interface.
5. Click **Submit**.

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 BlackPearl 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.

Note: PSID erasure of a drive is useful if you need to return a failed drive to Spectra Logic. When a drive is PSID erased, Spectra Logic cannot access data on the drive.



CAUTION

Performing a PSID Erase on a drive makes all data on the drive permanently inaccessible.

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

To PSID erase a drive, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to PSID erase a drive will be added to the new user interface in a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with `/legacy`. For example:

`https://ipaddress/legacy`

2. Use the toolbar in the upper-right to select **Status > Hardware** or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays.
3. Click **Data Drives**. The hardware screen refreshes and displays all disk drives present in the.
4. Record the slot number and serial number for each drive you want to PSID erase.
5. Power down the as described in [Reboot or Shut Down a BlackPearl NAS on page 174](#).
6. Locate the drive(s) in the chassis using the slot number and verify the serial number(s) you recorded in [Step 4](#).
7. Locate the PSID value on the drive label and record the value.
8. Repeat for any additional drives you want to erase.
9. Power on the as described in [Power On the on page 63](#).
10. Log into the BlackPearl legacy user interface as described in [Step 1 on page 142](#).

11. Use the toolbar in the upper-right to select **Status > Hardware** or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays.
12. Click **Data Drives**. The hardware screen refreshes and displays all disk drives present in the.
13. On the row of the drive you want to erase, click **PSID Erase**. The PSID Erase dialog box displays.

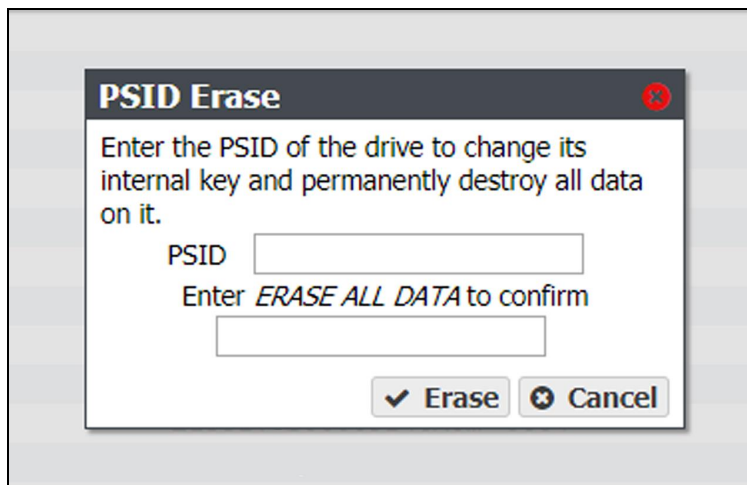


Figure 82 The PSID Erase dialog box.

14. Enter the PSID value you recorded in [Step 4 on page 142](#) in the **PSID** entry field.
15. Type `ERASE ALL DATA` in the confirmation entry field.



CAUTION

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

16. Click **Erase**.
17. Repeat for any additional drives you want to erase.

CHAPTER 6 - ADDITIONAL CONFIGURATION OPTIONS

This chapter describes using the BlackPearl user interface to configure additional options for the Spectra BlackPearl NAS.

Configure Users	145
Description of User Types	145
Create a User	145
Edit a User	145
Delete a User	146

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 [Create a User on page 76](#) for information about each user type.

Create a User

To create a user, see [Create a User on page 76](#).

Edit a User

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. In the User pane, select the user you want to edit and then click **Edit**. The Edit User screen displays.

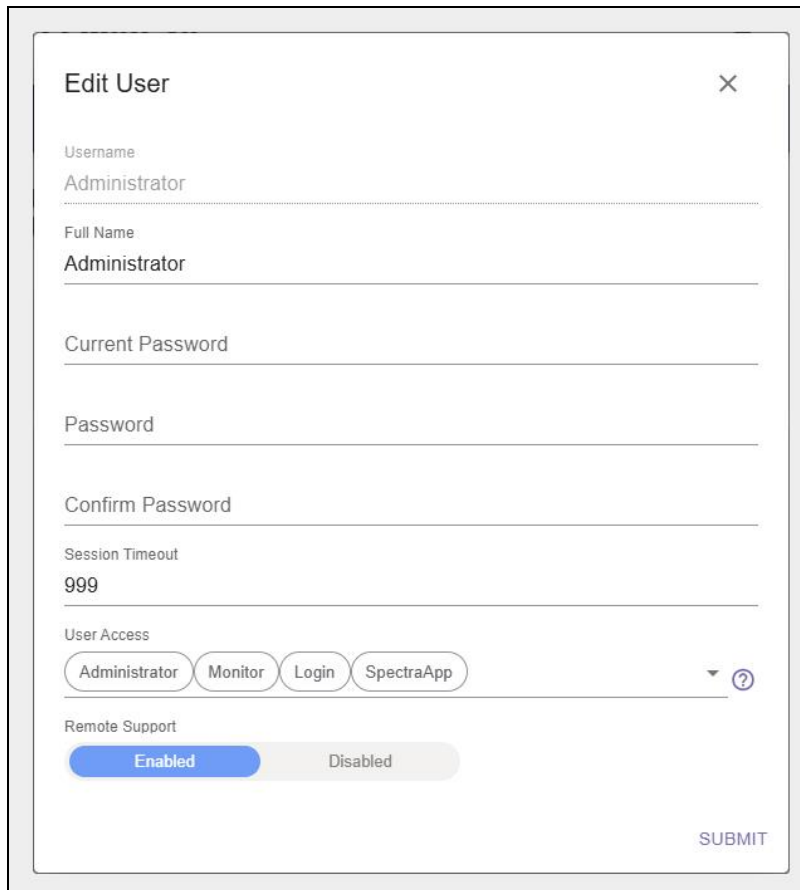


Figure 83 The New User dialog box.

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 BlackPearl (see).
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 [Create a User on page 76](#) for information on each level of user access permission.
8. If directed by Spectra Logic Technical Support, use the **Remote Support** slider to **Enable** or **Disable** remote support as directed.
9. Click **Save**.

Delete a User

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. In the User pane, select the user you want to edit and then click **Edit**. The Edit User screen displays (not shown).
3. Select the user you want to delete, and then click **Delete**. A confirmation window displays.
4. Click **Delete** to delete the user.

Enable CIFS User Access

If you are creating CIFS shares and if your Windows environment does not use Active Directory, you must edit a user to enable CIFS user access, also known as local administrator status.

Note: Alternatively, you can create a new user with CIFS user access. See [Create a User on page 76](#).

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. Select the user and click **Edit**. The Edit User dialog box displays.

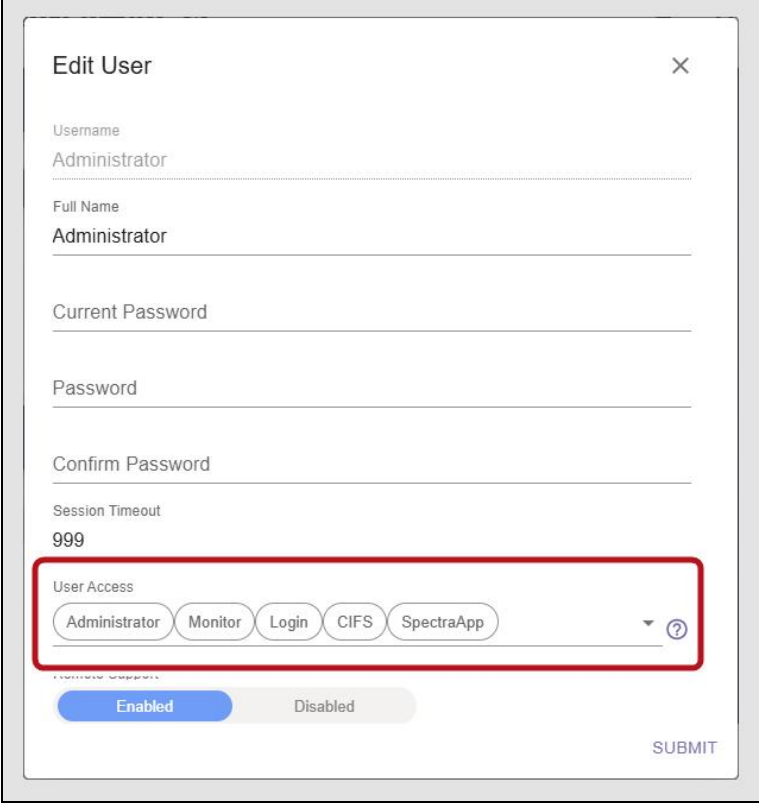
The image shows a dialog box titled "Edit User" with a close button (X) in the top right corner. The dialog contains several input fields: "Username" with the value "Administrator", "Full Name" with the value "Administrator", "Current Password", "Password", and "Confirm Password". Below these is a "Session Timeout" field with the value "999". A "User Access" section is highlighted with a red rectangle; it features a dropdown menu with the current selection "Administrator" and a list of other options: "Monitor", "Login", "CIFS", and "SpectraApp". Below the dropdown are two buttons: "Enabled" (highlighted in blue) and "Disabled". A "SUBMIT" button is located in the bottom right corner of the dialog.

Figure 84 The Edit User dialog box.

3. Use the **User Access** drop-down menu to select **CIFS**.
4. If desired, change other settings as described in [Configure Users on page 145](#).
5. Click **Submit**.
6. Continue to [Configure Users on page 145](#).

CHAPTER 7 - MANAGING NETWORK ATTACHED STORAGE

This chapter describes using the BlackPearl user interface to manage the creation and use of volume snapshots, and managing NAS replication.

For initial NAS configuration steps, see [Configuring Network Attached Storage on page 100](#).

Manage NAS Replication	149
Manually Start NAS Replication	149
Restoring Files from a NAS Replication Target	149

MANAGE NAS REPLICATION

After configuring replication (see [Configure NAS Replication on page 116](#)), 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 volume 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 volume continues on its previously defined schedule.

1. On the source system's BlackPearl user interface, use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**.

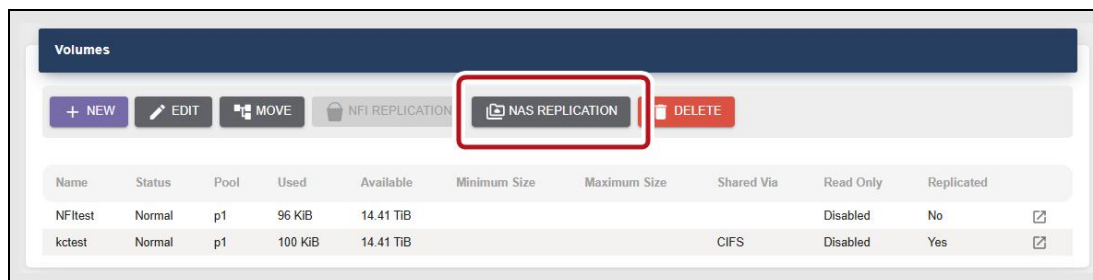


Figure 85 The NAS screen - Volumes pane - NAS Replication button.

2. Select the volume name you want to replicate and click **NAS Replication**. A confirmation window displays (not shown).
3. Click **Submit** to begin a manual NAS replication.

Restoring Files from a NAS Replication Target

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

1. On the source system's BlackPearl user interface, clear the write-protected status of the replicated volume.

Note: You cannot add a share while the volume has write-protection enabled.

- a. Use the toolbar in the upper-right to 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** checkbox.
 - 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 CIFS Share on page 110](#) or [Create a NFS Share on page 108](#) 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. Use the toolbar in the upper-right to 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** checkbox.
 - 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.
- 6. If desired, stop sharing the NAS replication target volume.

CHAPTER 8 - MONITOR THE BLACKPEARL SOLUTION

This chapter describes using the BlackPearl user interface to monitor the system messages, performance, and reports.

View System Messages	152
Types of Message Severity	152
View System Messages	153
View Performance Metrics	154
View Reports	156
Enable Remote Logging	157

VIEW SYSTEM MESSAGES

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

Types of Message Severity

Messages displayed in the BlackPearl 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 as part of normal operation occurred which requires some sort of user interaction, and until this occurs, adverse impact to the BlackPearl NAS may occur.
Warning	Notifies the user of a failure that may adversely impact the BlackPearl NAS.
Critical	Notifies the user of a failure that caused significant adverse impact to the BlackPearl NAS.

View System Messages

Use the instructions in this section to check system messages.

1. Click **Messages (bell icon)**.

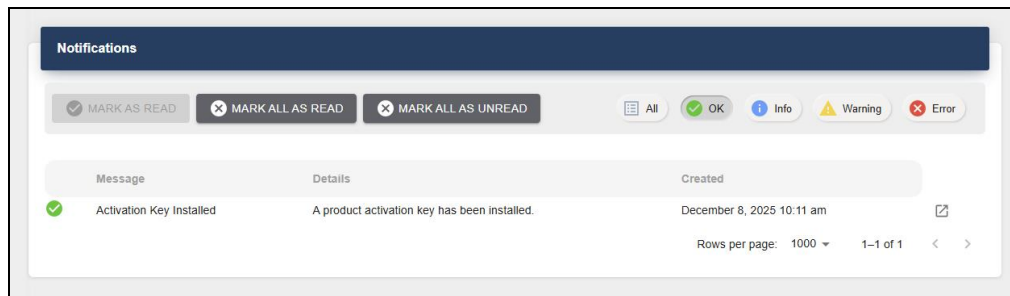


Figure 86 The Messages screen.

Pay extra attention to any messages flagged with the Warning or Critical icon and follow any recommended steps. Contact Spectra Logic Technical Support if you need assistance (see [Contacting Spectra Logic on page 7](#)).

2. If desired, use the **Rows Per Page** 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 click **Mark As Read**. To mark all messages as read, click **Mark All As Read**.

- Notes:**
- You cannot delete messages. The automatically deletes the oldest messages on a first-in, first-out basis as space is required, retaining the most recent messages. The holds 10,000 messages.
 - Messages can also be marked as **Unread**.

VIEW PERFORMANCE METRICS

The Performance screen displays performance metrics for the BlackPearl storage pools, CPUs, network traffic, and individual disk drives. Performance graphs can be configured to display either the last 5 minutes of activity, or the last 24 hours.

Here is how you view performance metrics:

1. From the left-hand menu, click **Performance**.

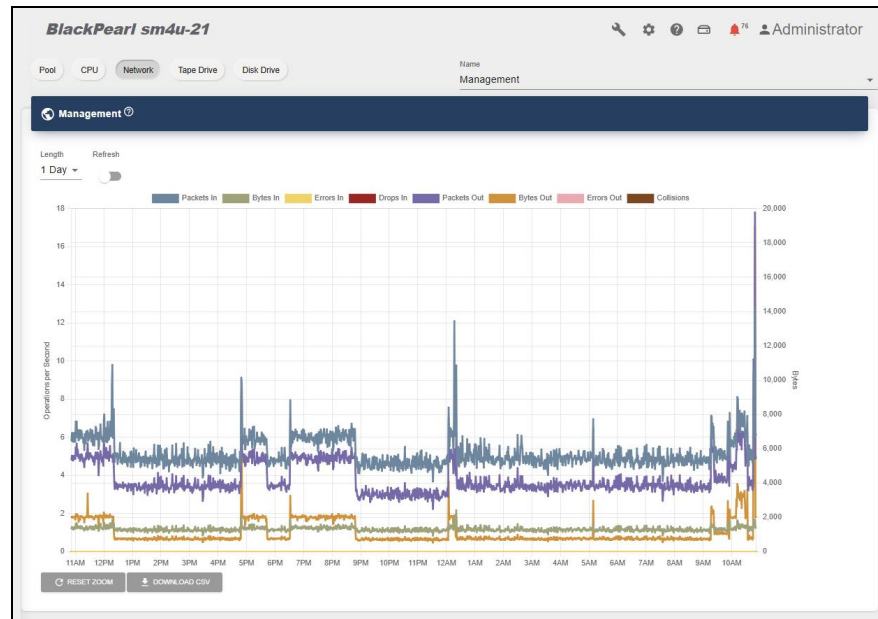


Figure 87 The Performance screen.

2. Select **Pools, CPU, Network, or Disk Drive** to display performance information about the selected component.
3. Use the **Name** drop-down menu in the upper-right corner to select an individual component of the selected category.
4. Use the **Length** drop-down menu to select the time interval to display. The data can be displayed in 6 second increments (5 minutes total) or 1 hour increments (1 day total).
5. Use the **Element buttons** at the top of the graph to select to display or hide graph elements.

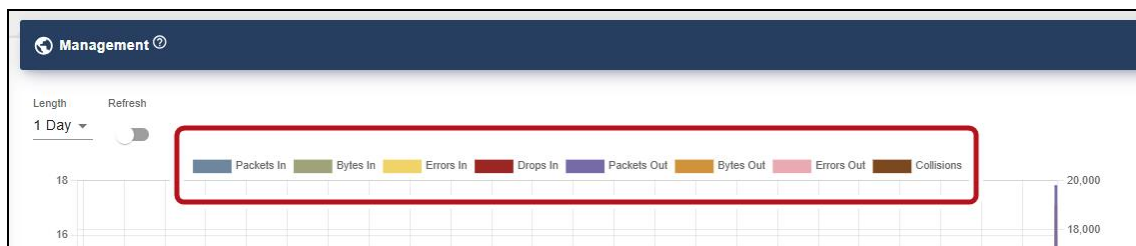


Figure 88 The Performance screen - Element buttons.

6. To see the performance data in greater detail, use the mouse to **click and drag** the cursor horizontally over the section of the detail graph that you want to magnify. The highlighted section of data is shown on the graph.
7. Click **Reset Zoom** to reset the graph to the default view.
8. If desired, click **Download CSV** 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.

VIEW REPORTS

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

1. From the left-hand menu, click **Reports**.

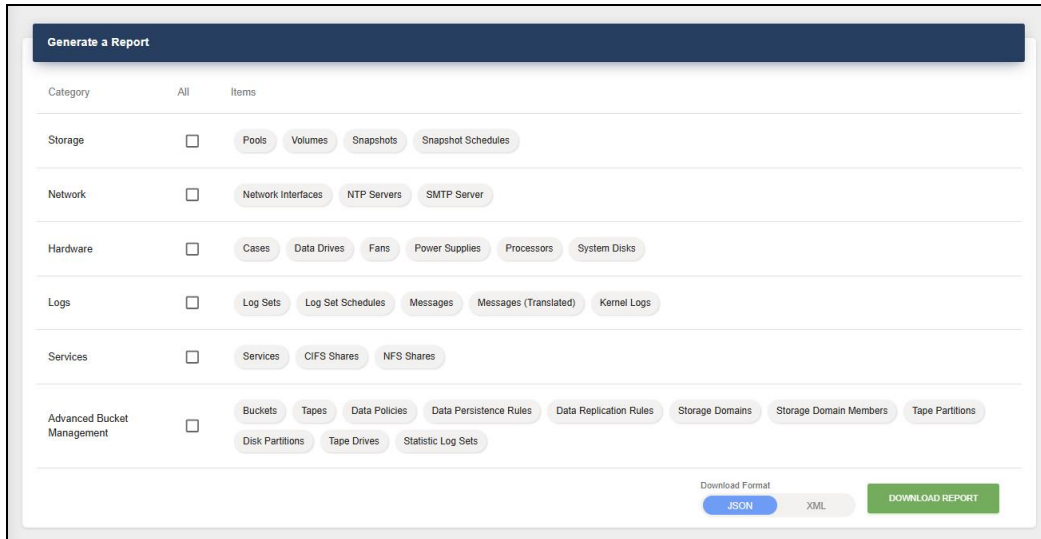


Figure 89 The Reports screen.

Note: Depending on the configuration of your BlackPearl NAS, the information displayed may look different than the image above.

2. Select the **All** checkbox next to the report(s) you want to generate, or **select individual components**.
3. Use the **Download Format** slider to select either JSON or XML formatting for the downloaded report(s).
4. Click **Download Report**. The selected reports are saved to your local host.

ENABLE REMOTE LOGGING

Remote Logging is a feature that allows the BlackPearl NAS to send any messages generated by the system to a syslog server.

Use the instructions in this section to enable remote logging.

1. Enter the Remote Logging activation key as described in [Manually Enter Activation Keys on page 198](#).
2. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Services and Protocols**.
3. In the Remote Logging pane, click **Edit**. The Edit Remote Logging Service dialog box displays.

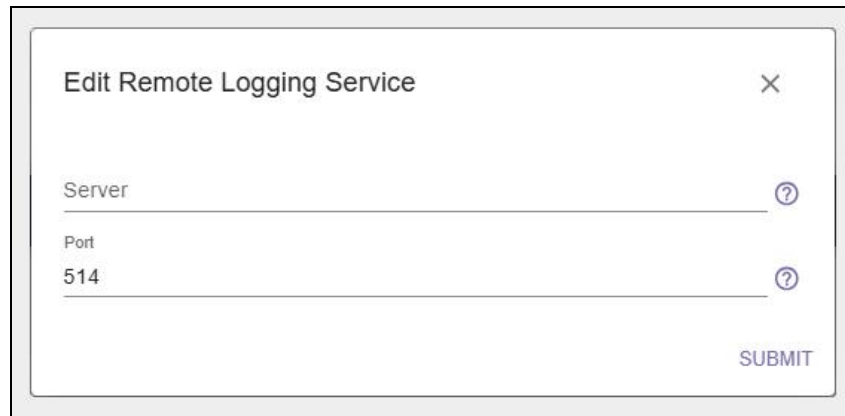


Figure 90 The Edit Remote Logging Service dialog box.

4. Enter a hostname or IP address for the remote logging **Server**.
5. Enter the **Port** used to communicate with the remote logging server.
Note: The default port is 514.
6. Click **Submit**.

CHAPTER 9 - BLACKPEARL NAS HARDWARE OPERATIONS

This chapter describes hardware operations for the Spectra BlackPearl NAS, including hardware monitoring, activating the chassis beacon, installing drives, and diagnosing failed components.

Monitor the Hardware	159
Front Bezel Visual Status Beacon	159
Configuring the Visual Status Beacon Color	161
Flash the Visual Status Beacon	162
System Status LEDs	163
View the Status of Hardware Components	167
Data Drive Status Definitions	168
View the Status of NAS Pools	169
View the Status of NAS Volumes	172
Reboot or Shut Down a BlackPearl NAS	174
Using the BlackPearl User Interface	174
Power-Cycle Reset	175
Replace a Failed Component	176
Identify the Failed Component	176
Activate Chassis Beacon	177
Replace the Failed Component	178
Installing Data Drives	179
Ensure ESD Protection	179
Install a Drive in a Gen3 H Series Chassis	180
Install a Drive in a Gen2 S Series Chassis	187
Install a Drive in a Gen2 V Series Chassis	188
Install a Drive in a Gen2 X Series Chassis	189
Install a Drive in a Gen1 Chassis	191

MONITOR THE HARDWARE

The BlackPearl NAS features multiple tools to help you monitor the health and performance system hardware components including:

- The Visual Status Beacon light bar in the front bezel changes color to indicate the current status of the (see [Front Bezel Visual Status Beacon below](#)).

Note: The front bezels in BlackPearl Gen1 2U master nodes, and some Gen1 4U chassis, do not include a Visual Status Beacon light bar.

- LEDs on the front of the BlackPearl chassis indicate system status and error conditions (see [System Status LEDs on page 163](#)
- Icons on the Hardware screen provide overall status of the hardware components in each group (see [View the Status of Hardware Components on page 167](#)).
- You can also use the BlackPearl user interface to do the following:
 - View the status of NAS pools and volumes (see [View the Status of NAS Pools on page 169](#) and [View the Status of NAS Volumes on page 172](#)).

Front Bezel Visual Status Beacon

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

Color Display	Condition
Purple Scroll	The is operating normally. Note: The color displayed when the is operating normally can be changed on the Hardware screen. See Configuring the Visual Status Beacon Color on page 161 for more information.
Yellow Scroll	The is experiencing a Warning condition. Log in to the BlackPearl user interface to determine the cause of the warning.
Red Scroll	The is experiencing an Error condition. Log in to the BlackPearl user interface to determine the cause of the error.
Rainbow	The is currently powering on and performing self-tests.
Flashing Blue	The beacon feature was activated for this . This can help you identify a specific when you have more than one in your environment. See Flash the Visual Status Beacon on page 162 for instructions on activating the beacon.

Color Display	Condition
Pulsing Red	The Visual Status Beacon lost communication with the . This can occur if the experiences a software hang.
No Light	The BlackPearl NAS is powered off.

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

Configuring the Visual Status Beacon Color

The BlackPearl NAS is configured to display a purple scrolling light on the Visual Status Beacon when the is operating normally. If desired, you can change the color displayed for normal operation.

To configure the bezel color, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to configure the bezel color will be added to the new user interface in a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

`https://ipaddress/legacy`

2. Use the toolbar in the upper-right to select **Status > Hardware**, or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays.
3. Click **Bezel**. The Bezel pane of the Hardware screen displays.
4. Click the colored box next to **Select Bezel Color**. The color picker window displays.

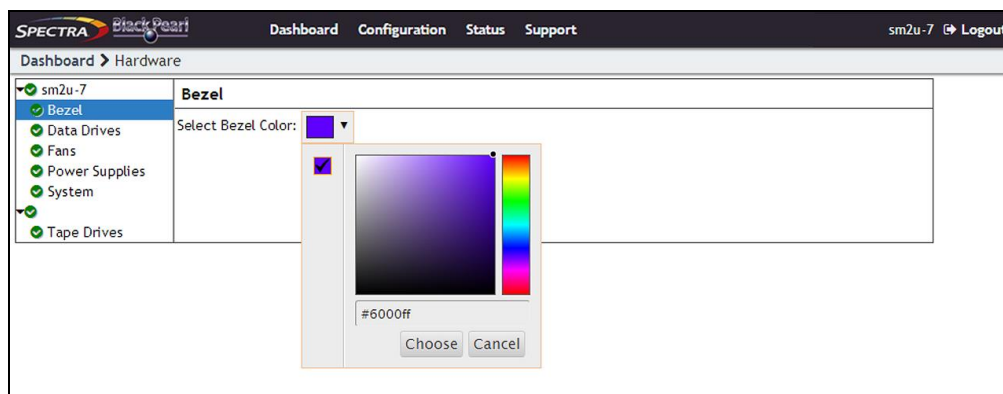


Figure 91 Use the color picker to set the color of the Visual Status Beacon when the is operating normally.

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

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

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

Flash the Visual Status Beacon

To activate the visual status beacon to flash blue, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to enable this feature will be added to a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with `"/legacy"`. For example:

`https://ipaddress/legacy`

2. Use the toolbar in the upper-right to select **Status > Hardware**, or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays.

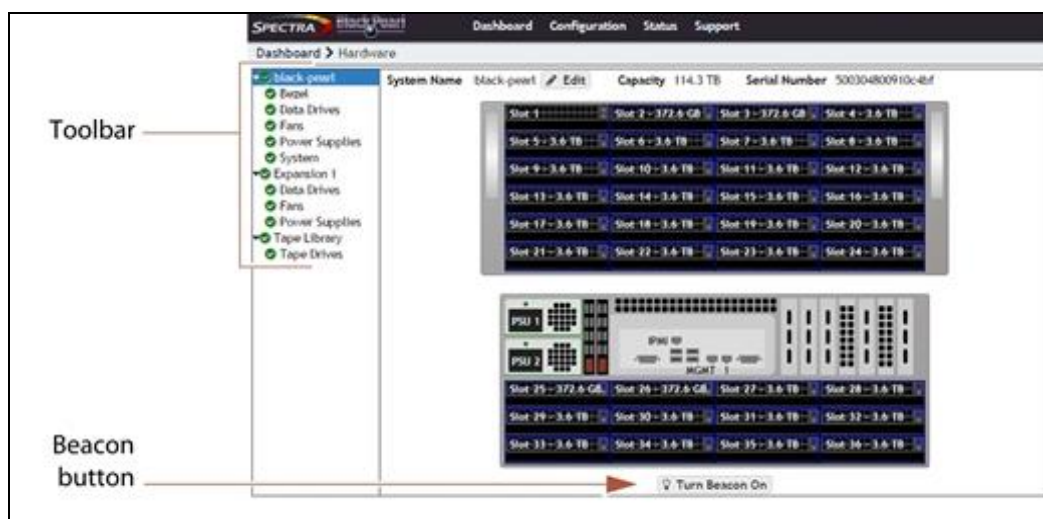


Figure 92 The Turn Beacon On button.

3. In the chassis graphic, click **Turn Beacon On**. Click the button again to stop the beacon from flashing.

System Status LEDs

The system status LEDs provide information about the status of the, its fans, network connections, and power supplies.

Gen3 H Series Chassis

The table below lists each system status LED, from top to bottom, and its function.



Figure 93 The Gen3 H Series chassis system status LEDs.

Location	LED	Color	Meaning When Lit
Upper-left	Chassis Power	Blue	The enclosure is powered on and operating correctly. OFF: The enclosure is not powered on.
Upper-right	Chassis Fault	Amber	One or more components within the enclosure have experienced a fault requiring a service action.
Middle-right	Network Activity	Green	The system is sending/receiving network traffic on an Ethernet port on the motherboard.
Lower-left	Chassis Identify	Blue	The enclosure is receiving an identify command. The chassis can also be located using the Visual Status Beacon. See Flash the Visual Status Beacon on the previous page for instructions.

Gen2 X Series Chassis

The table below lists each system status LED, in order from left to right, and its function.



Figure 94 The top left section of the front of the Gen2 X chassis (front bezel removed) showing system status LEDs.

Location	LED	Color	Meaning When Lit
1	Chassis Identify	Blue	The enclosure is receiving an identify command. The chassis can also be located using the Visual Status Beacon. See Flash the Visual Status Beacon on page 162 for instructions.
2	Chassis Fault	Amber	One or more components within the enclosure have experienced a fault requiring a service action.
3	Chassis Power	Green	The enclosure is powered on and operating correctly. OFF: The enclosure is not powered on.
4	Server Fault	Amber	One or more server modules have experienced a fault requiring a service action.
5	Server OK	Green	Both server modules are powered on and operating correctly.
6	Fan Fault	Amber	One or more fan modules have experienced a fault requiring a service action.
7	Fans OK	Green	All fan modules are powered on and operating correctly.
8	PM Fault	Amber	One or more power modules have experienced a fault requiring a service action.
9	PMs OK	Green	Both power modules are powered on and operating correctly.
10	Not in use	N/A	N/A

Gen2 S Series and Gen2 V Series Chassis

The table below lists each system status LED, in order from left to right, and its function.



Figure 95 The top right section of the front of the Gen2 S Series chassis, with the front bezel removed, showing system status LEDs.



Figure 96 The top left section of the front of the Gen2 V Series chassis, with the front bezel removed, showing system status LEDs.

Icon	LED	Meaning When Lit
	Chassis Power	The enclosure is powered on and operating correctly. OFF: The enclosure is not powered on.
	System HDD Activity	Indicates activity on the system disks.
	LAN Activity	The upper or left most LED indicates LAN activity on the BlackPearl management port. The lower or right most LED indicates LAN activity on the data port.
	Service ID	This LED is only present on the Gen2 S Series chassis.
HDD Tray LEDs - V Series only		
F	HDD Failure	One or more drives in the front row of the drive tray have failed.
R	HDD Failure	One or more drives in the rear row of the drive tray have failed.

Gen1 S Series and Gen1 V Series Chassis

The table below lists each system status LED and its function.

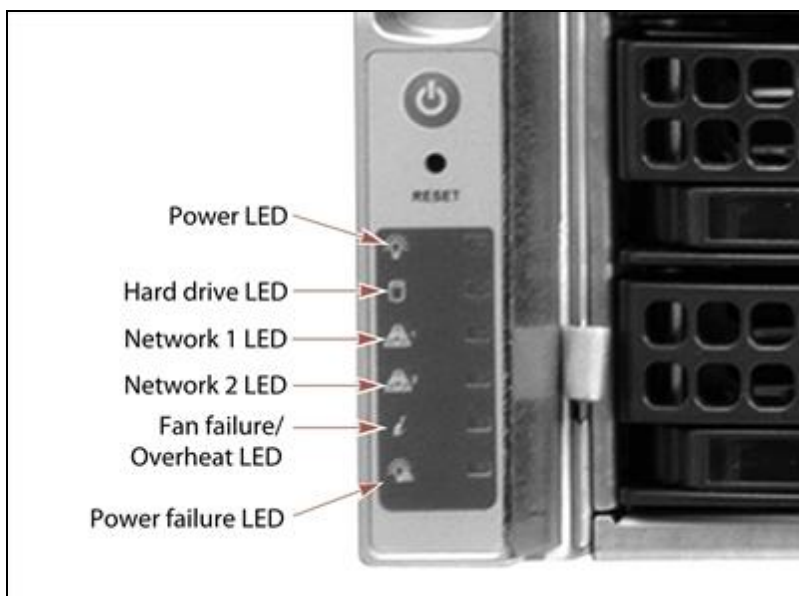


Figure 97 The left side of the front of the Gen1 S Series chassis showing system status LEDs.

LED	Function
Power	Indicates if the unit is powered on or off.
Hard Drive	Indicates boot drive activity.
Network 1	Indicates network activity on the BlackPearl 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. Check the BlackPearl user interface to determine which fan failed. • If the LED is solid red, it indicates an overheat condition. Check the BlackPearl user interface to view the status of the. If the problem persists, contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 7.
Power Failure	Indicates a power supply failure. Check the BlackPearl user interface to determine which power supply failed.

View the Status of Hardware Components

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

Use the following instructions to check the status of hardware components.

1. Click **Hardware (hard drive icon)**. The Hardware screen displays.

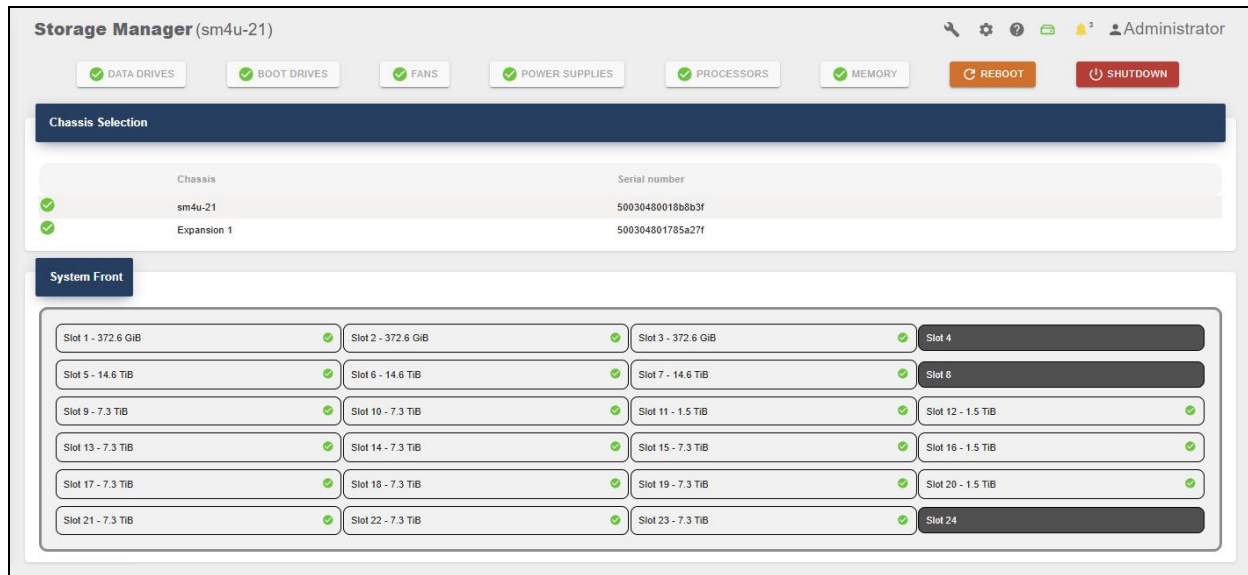


Figure 98 The Hardware screen.

2. If your system contains multiple chassis, under the Chassis Selection pane, select the row of the chassis for which you want to view information.
3. Use the buttons on the top of the Hardware screen to jump to that category to view detailed information about the selected component groups.

Clicking...	Shows the...
Data Drives	• Status of each drive (see Data Drive Status Definitions on the next page) • The status of the pool to which the drive is assigned. • Slot number of each drive • Drive size, type, serial number, and firmware level • The name of the pool to which the drive is assigned • If the drive is a SED (Self-Encrypting Drive) • If the drive is currently encrypted • The wear level of the drive (SSD and NVMe drives only)
Boot Drives	• The status of each drive

Clicking...	Shows the...
	The serial number, manufacturer, model, size, and firmware of the drive
Fans	Status and speed of fans
Power Supplies	Power supply status and wattage Note: Power supply information is not available for the 77-bay or 107-bay expansion node.
Processors	- CPU status and temperature - Hyperthreading status - CPU Fan status
Memory	System memory size

**IMPORTANT**

To view the status of the SAS ports on a 78-drive expansion node, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to configure a single port data connection will be added to a later version of the BlackPearl OS.

Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

`https://ipaddress/legacy`

Data Drive Status Definitions

The table below describes each status for a data drive when viewed on the Hardware screen of the BlackPearl user interface.

Status	Description
Normal	The drive is in use in a storage pool and is functioning normally.
Spare	The drive not currently in use in the assigned storage pool.
Spare-Available	Unused drive.
Critical	The drive is in a critical state. Contact Spectra Logic Technical Support.
Exported	The drive belongs to a storage pool that was previously exported.
Foreign	The drive is from a different BlackPearl NAS and must be imported.
Rebuilding	The drive is rebuilding. This typically occurs when a spare drive is promoted in the storage pool to Normal.

Status	Description
Unbranded	A drive not sold by Spectra Logic. This drive cannot be used by the system.
Empty	No drive is present in the slot.
SED Initialization Failed	The drive failed to initialize encryption.
SED Unlock Failed	The drive failed to unlock encryption.

View the Status of NAS Pools

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

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**. The NAS screen displays.

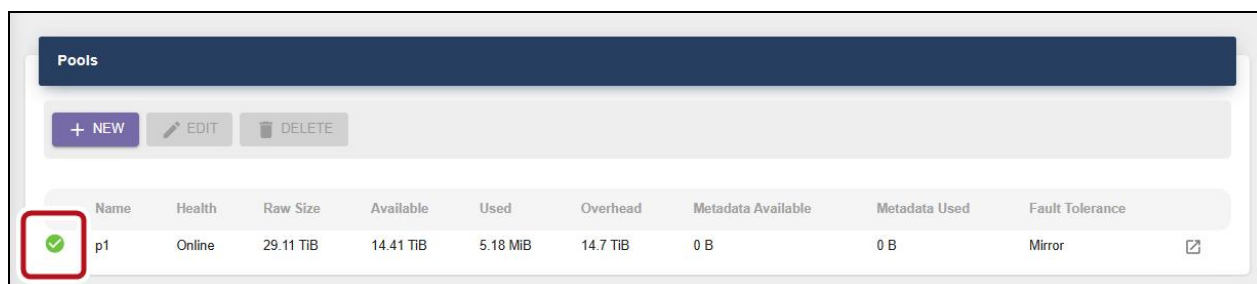


Figure 99 The NAS screen - Pools pane - Status icon.

- The status of each pool is indicated by the status icons on the left side of the screen.
- The Pools pane 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.

This column...	Shows...
Overhead	The amount of disk space used for overhead, such as parity data.
Metadta Available	The amount of disk space available for metadata information.
Metadata Used	The amount of disk space used by metadata information.
Fault Tolerance	The fault tolerance setting for each pool.

2. To view additional information about a NAS pool, click the **Details** button on the right side of the screen. The *pool name* details screen displays.

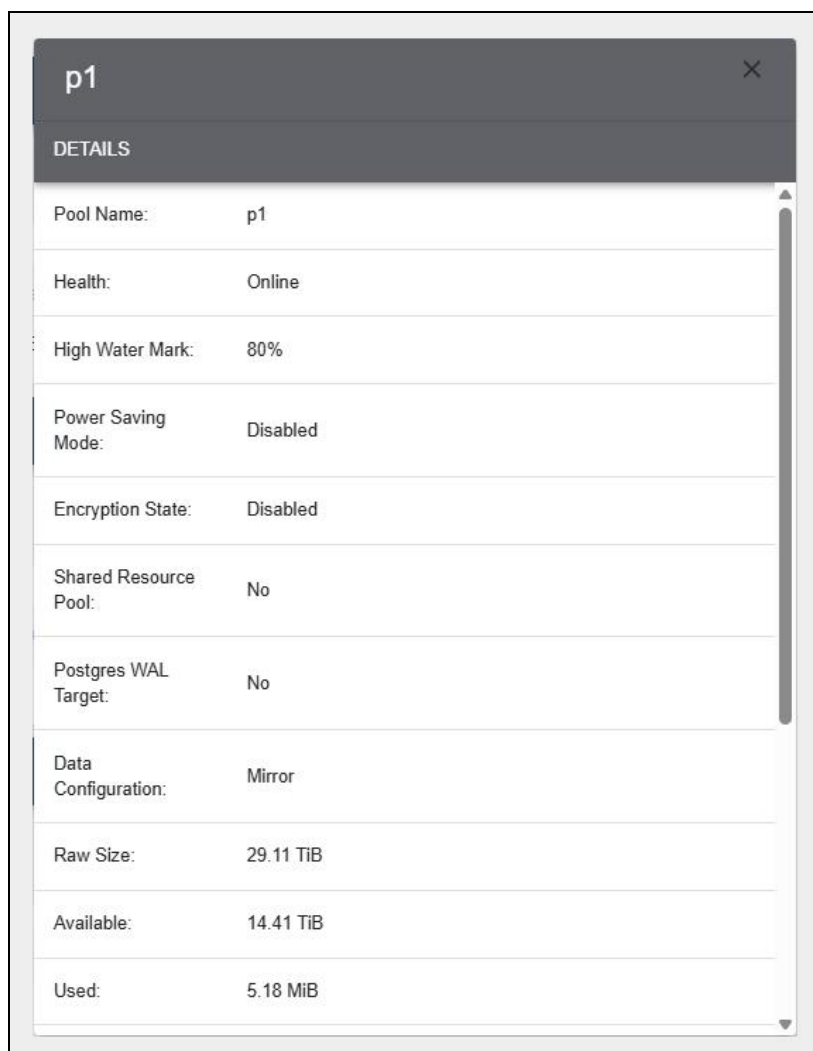


Figure 100 A NAS Pool details screen (partial shown).

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.
Encryption State	Indicates if the pool is encrypted.
Shared Resource Pool	
Postgres WAL Target	
Data Configuration	The protection level for the pool.
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.
Created	The timestamp of when the pool was created.

View the Status of NAS Volumes

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

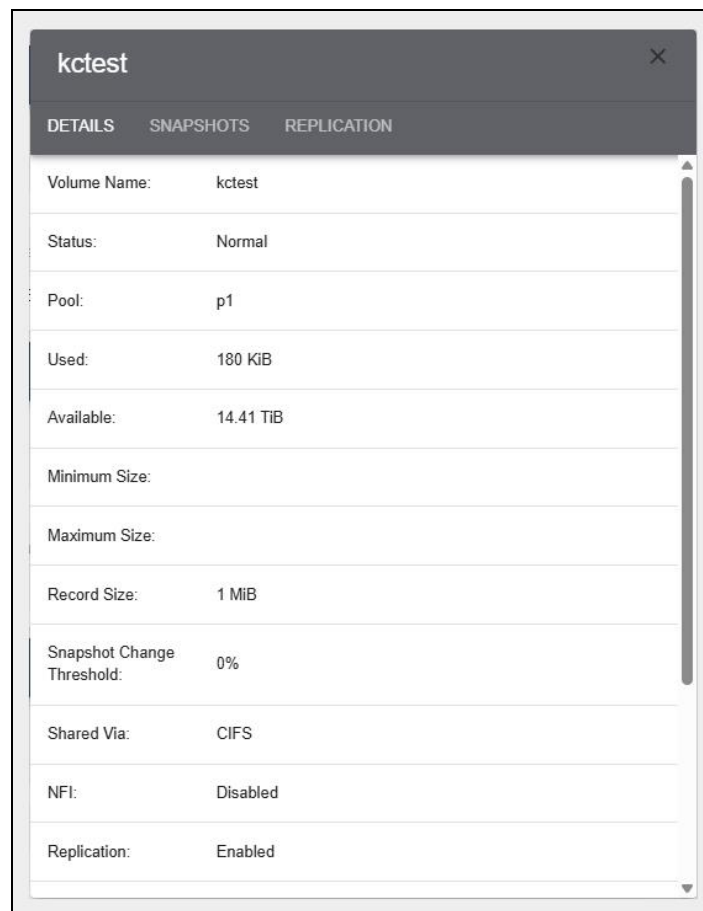
1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > NAS**. The NAS screen displays.
2. The status of each volume is indicated by the status column on the left side of the screen.



Name	Status	Pool	Used	Available	Minimum Size	Maximum Size	Shared Via	Read Only	Replicated
kctest	Normal	p1	180 KiB	14.41 TiB			CIFS	Disabled	Yes

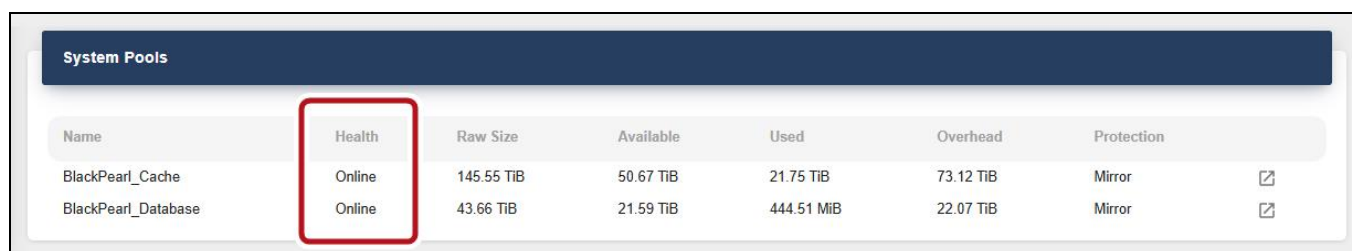
Figure 101 The NAS screen - Volumes pane - Status column.

3. To view additional information about a volume, click the **Details** button on the right side of the screen. The *volume name* details screen displays.



kctest	
DETAILS	SNAPSHOTS
Volume Name:	kctest
Status:	Normal
Pool:	p1
Used:	180 KiB
Available:	14.41 TiB
Minimum Size:	
Maximum Size:	
Record Size:	1 MiB
Snapshot Change Threshold:	0%
Shared Via:	CIFS
NFS:	Disabled
Replication:	Enabled

Figure 102 A NAS Volume details screen (partial).



System Pools							
Name	Health	Raw Size	Available	Used	Overhead	Protection	
BlackPearl_Cache	Online	145.55 TiB	50.67 TiB	21.75 TiB	73.12 TiB	Mirror	↗
BlackPearl_Database	Online	43.66 TiB	21.59 TiB	444.51 MiB	22.07 TiB	Mirror	↗

Figure 103 The Buckets screen - System Pools pane - Health column.

REBOOT OR SHUT DOWN A BLACKPEARL NAS

This section discusses rebooting or shutting down a.

Using the BlackPearl User Interface

Use the following instructions to reboot or shutdown a system using the BlackPearl user interface.

1. Click **Hardware (hard drive icon)** in the upper-right corner of the user interface.

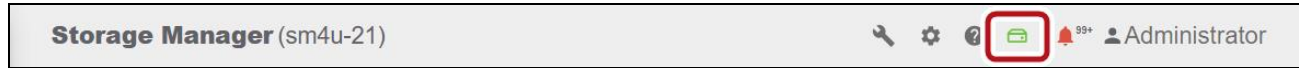


Figure 104 The Hardware button in the upper-right corner of the user interface.

2. Click either **Reboot** or **Shutdown**. A confirmation screen displays (not shown).

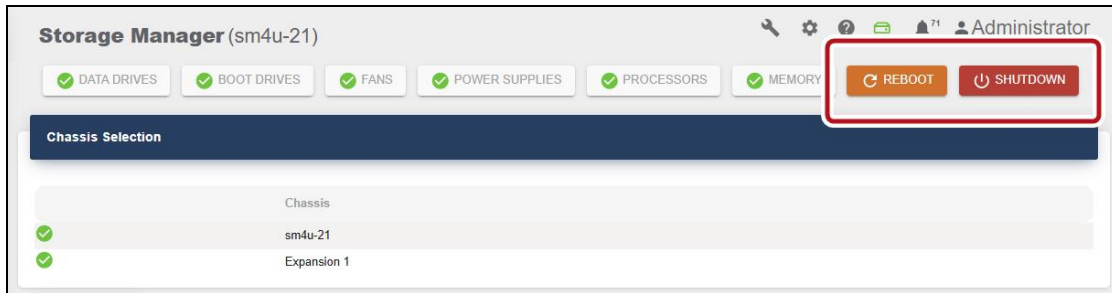


Figure 105 The Hardware screen - Reboot and Shutdown buttons.

3. Click **Submit**.

Power-Cycle Reset

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



CAUTION

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

REPLACE A FAILED COMPONENT

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

Identify the Failed Component

1. Click **Hardware (hard drive icon)** in the upper-right corner of the user interface.



Figure 106 The Hardware button in the upper-right corner of the user interface.

2. Locate the failed component. An **X** in a red circle indicates a failure (icon not shown below).

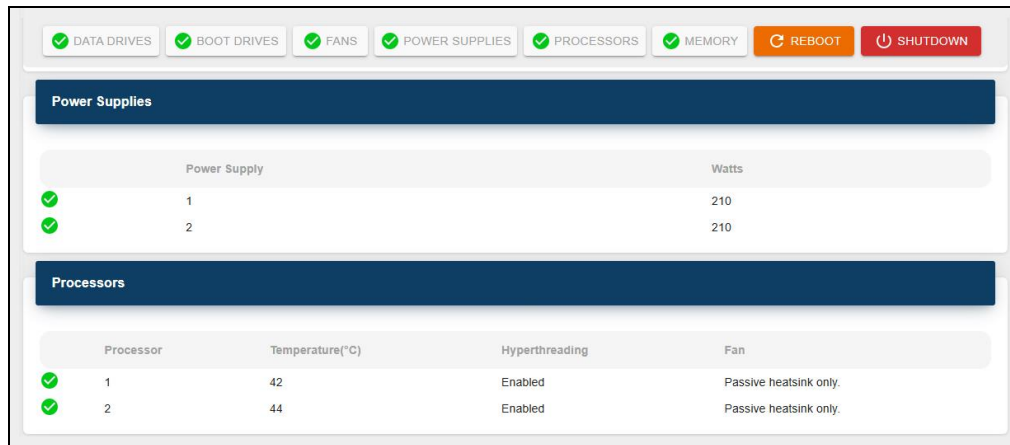


Figure 107 The top section of the Hardware screen.

Activate Chassis Beacon

If you have multiple BlackPearl NASs, you can use the beacon feature to help locate the with the failed component.

To activate the chassis beacon, you must access the legacy user interface used in BlackPearl OS 5.8.x and earlier. Functionality to activate the chassis beacon will be added to the new user interface in a later version of the BlackPearl OS.

1. Using a standard web browser, enter the IP address for the BlackPearl management port and append the address with "/legacy". For example:

`https://ipaddress/legacy`

2. On the Hardware screen, click the server name. The screen refreshes to show the main Hardware screen.

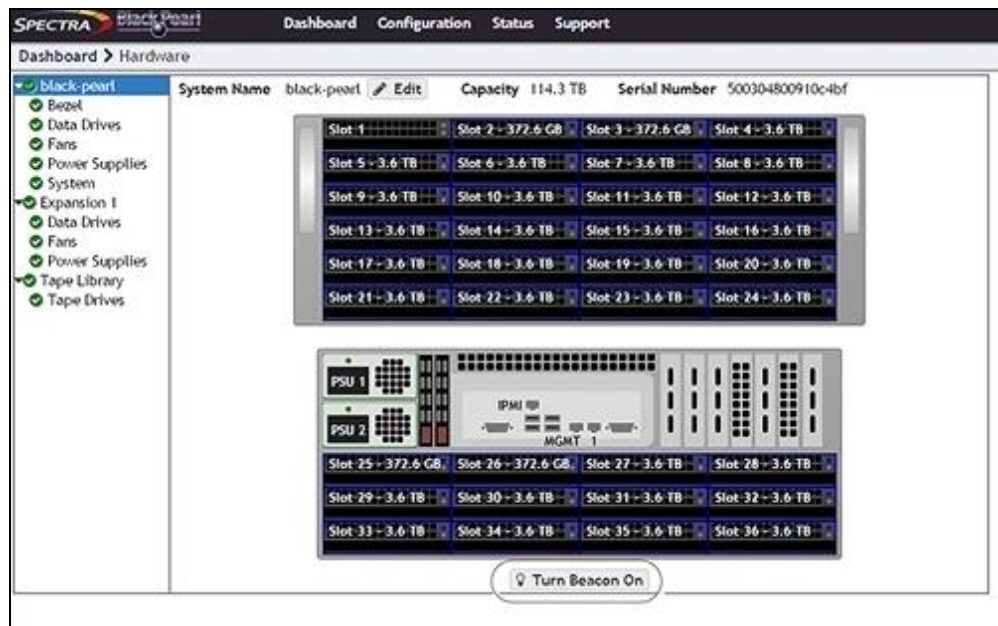


Figure 108 The Hardware screen. Gen1 S Series 4U chassis shown.

3. Click **Turn Beacon On**. The BlackPearl NAS Visual Status Beacon light bar flashes blue, making it easy to find.
4. After you locate the unit in your data center, click **Turn Beacon Off** to stop the lights from flashing.

Replace the Failed Component

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 96-Bay Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive in the 96-bay expansion node.
- The *Spectra 96-Bay Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in the 96-bay expansion node.
- The *Spectra 96-Bay Chassis Power Supply Replacement Guide* provides instructions for replacing a failed power supply in the 96-bay expansion node.
- The *Spectra 96-Bay Chassis I/O Module Replacement Guide* provides instructions for replacing a failed I/O module in the 96-bay expansion node.
- The *Spectra 107-Bay Expansion Node FRU Guide* provides instructions for replacing fans, power supplies, drives, and SAS expanders in the 77-bay and 107-bay expansion node.
- The *Spectra BlackPearl H-Series Chassis Part Replacement Guide* provides instructions for replacing parts in the Spectra BlackPearl H-series chassis.

INSTALLING DATA DRIVES

Use the following instructions to add new drives to a BlackPearl chassis.

Ensure ESD Protection

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

- 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 BlackPearl chassis caused by failure to protect it from electrostatic discharge (ESD) voids the BlackPearl chassis' 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.
-
-

Select the instructions for your chassis:

- Install a Drive in a Gen3 H Series Chassis
- Install a Drive in a Gen2 S Series Chassis
- Install a Drive in a Gen2 V Series Chassis on page 188
- Install a Drive in a Gen2 X Series Chassis on page 189
- Install a Drive in a Gen1 Chassis on page 191

Install a Drive in a Gen3 H Series Chassis

Install Data Drives

Use the instructions in this section to replace a SAS drive in the BlackPearl H Series chassis.

1. Remove the front bezel.
 - a. Using one hand, press and hold the tab on the left-hand side of the chassis.

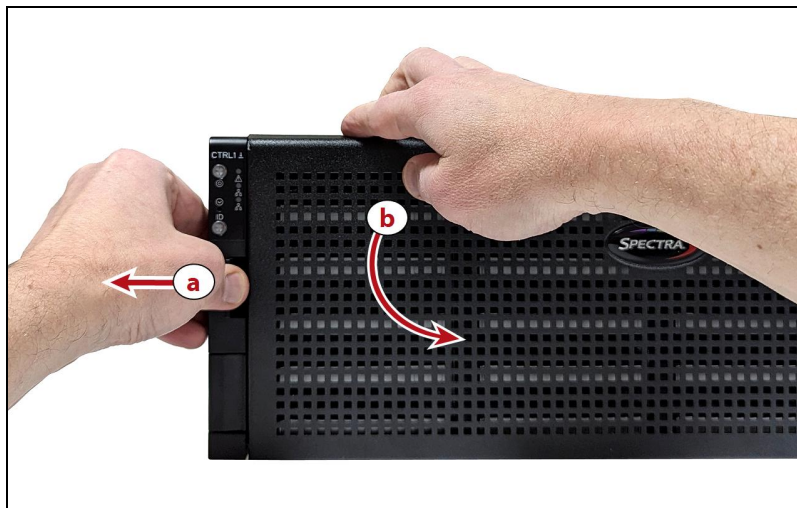


Figure 109 Remove the front bezel.

- b. Use your other hand to pull the faceplate away from the chassis.
2. Press the locking tab on the left side of the sled you want to remove to extend the handle.

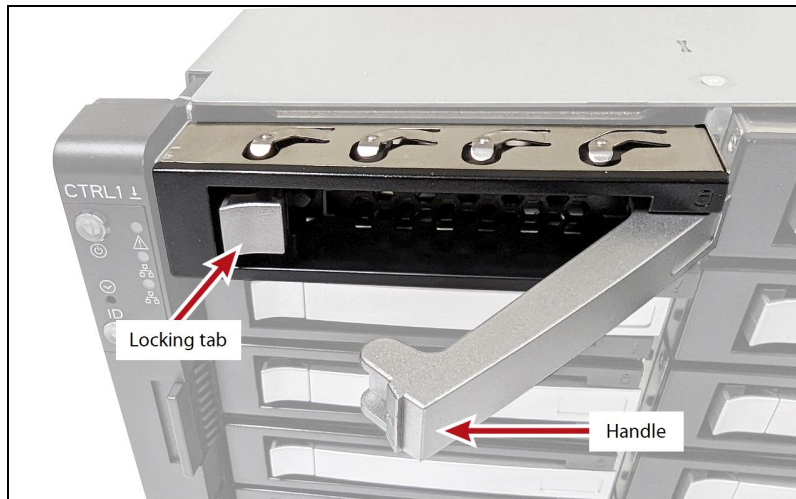


Figure 110 Unlock the drive sled.

3. Pull the handle to remove the drive sled from the chassis.
4. Remove the drive from the anti-static bag.
5. With the front of the drive sled facing you, insert the right side of the drive into the sled. PEMs on the right side of the sled insert into the screw holes in the side of the drive.



Figure 111 Screw holes in drive.

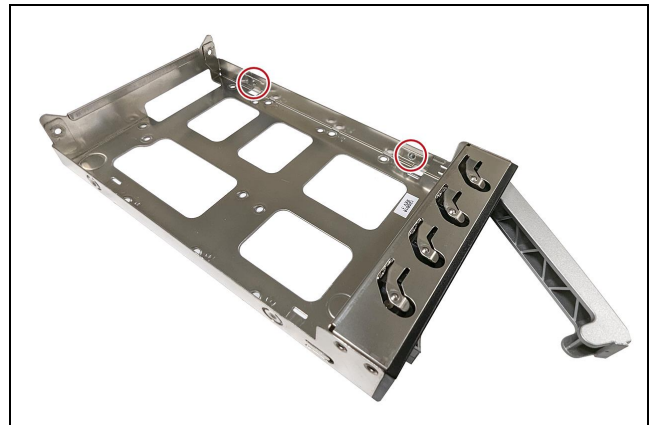


Figure 112 PEMs on right side of sled.

6. Rotate the left side of the drive down into the sled until it snaps into place.



Figure 113 Unlock the drive sled.

7. Slide the drive sled all the way into the chassis, then rotate the sled handle towards the chassis until it locks into place.



Figure 114 Insert drive into chassis.

8. Attach the front bezel.
 - a. Orient the front bezel with the Spectra logo upright and facing you.
 - b. Insert the tabs on the right side of the chassis power control faceplate into the slots on the right side of the front bezel.

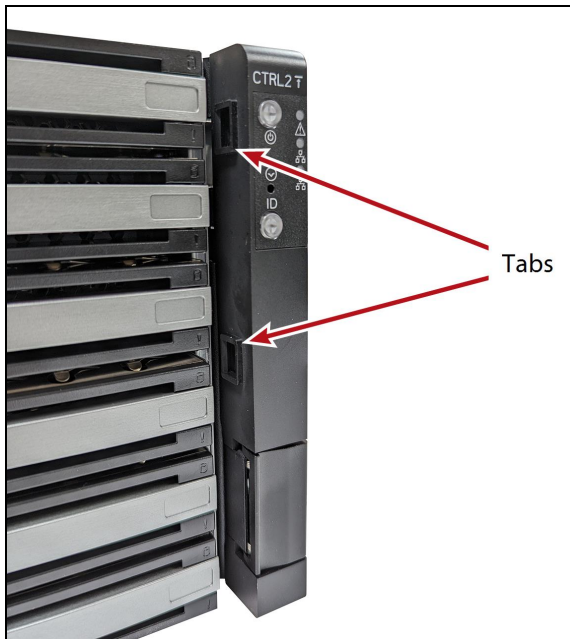


Figure 115 Tabs on the side of power control.

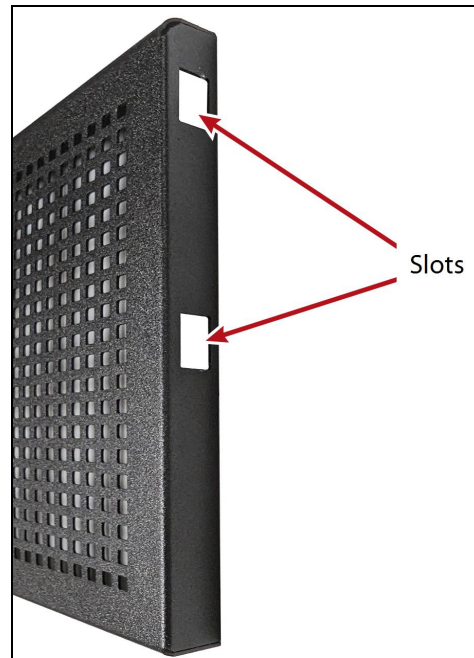


Figure 116 Slots in side of front bezel.

- c. Rotate the left side of the front bezel towards the chassis until the tab on the left side of the chassis snaps into place.

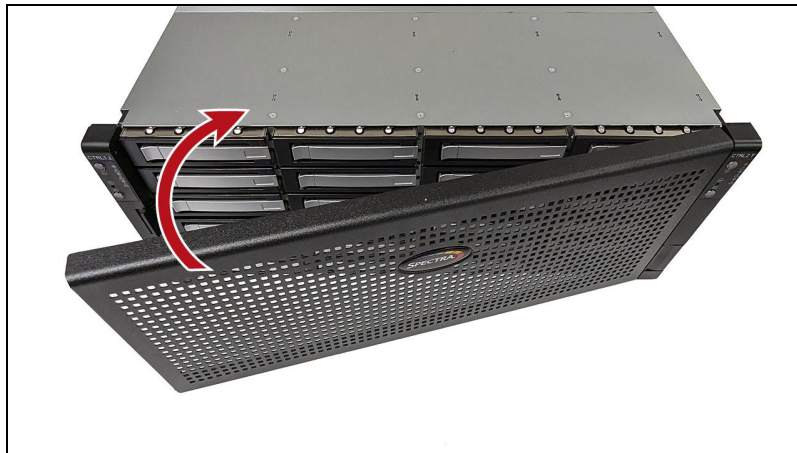


Figure 117 Insert drive into chassis.

Install NVMe Drives

Use the instructions in this section to replace an NVMe drive in the BlackPearl H Series chassis.

Note: If you install a NVMe drive into a powered-on H Series chassis, the system does not recognize the drive until you reboot the system. If you install an NVMe drive into a powered-on HotPair solution, you need to reboot both nodes of the solution.

1. Rotate the handle of the NVMe drive fan module down.

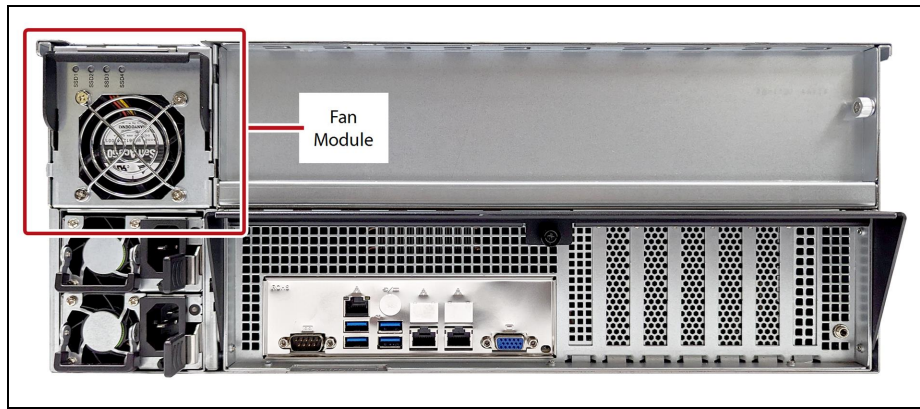


Figure 118 The NVMe drive fan module.

2. While holding the handle of the fan module, use your thumb to press and hold down the locking latch at the top of the fan module, then pull the module away from the chassis.

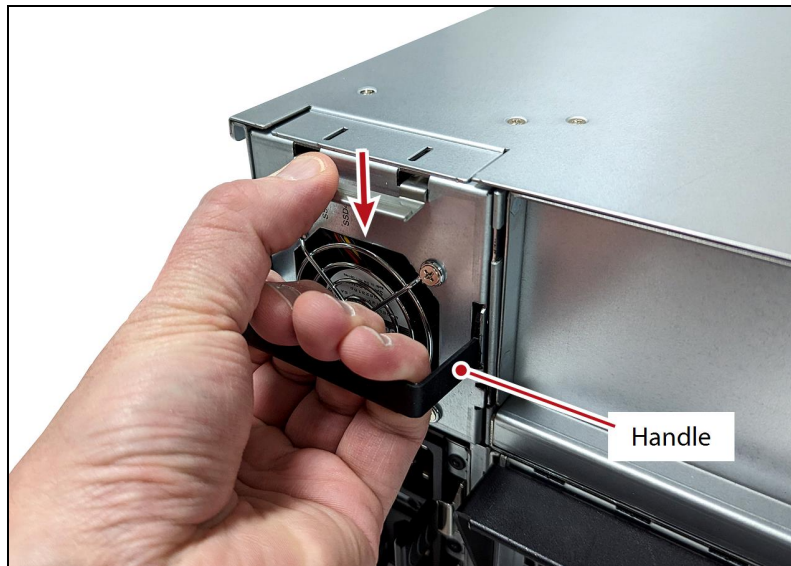


Figure 119 Remove the NVMe drive fan module.

3. Press the tab on the right side of the sled you want to remove to extend the handle.

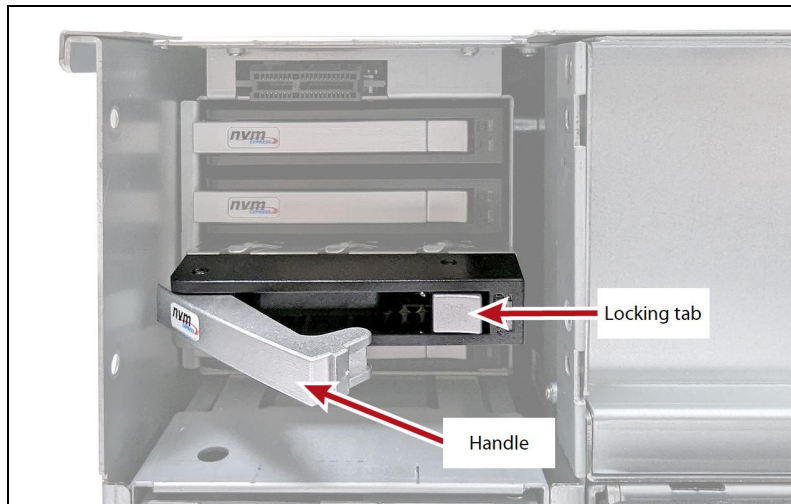


Figure 120 Unlock the drive sled.

4. Pull the handle to remove the drive sled from the chassis.
5. Remove the drive from the anti-static bag.
6. With the front of the drive sled facing you, insert the right side of the NVMe drive into the sled. PEMs on the right side of the sled insert into the screw holes on the side of the drive.



Figure 121 Screw holes in drive.

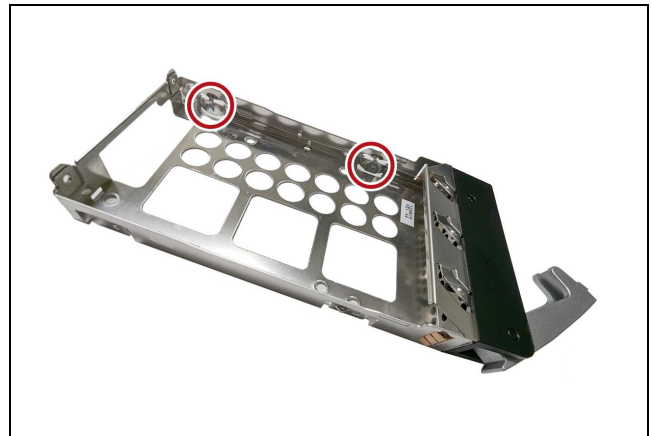


Figure 122 PEMs on right side of sled.

7. Rotate the left side of the drive down into the sled until it snaps into place.

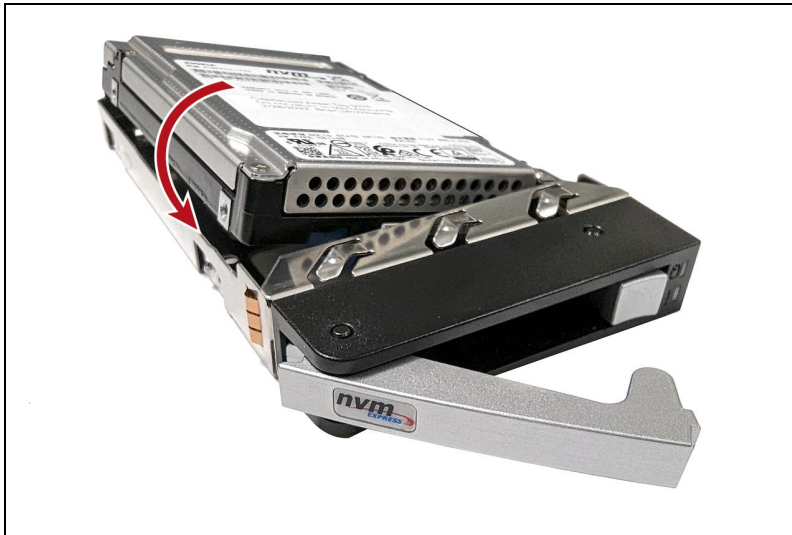


Figure 123 Install the drive into the sled.

8. Slide the drive sled all the way into the chassis, then rotate the sled handle towards the chassis until it locks into place.

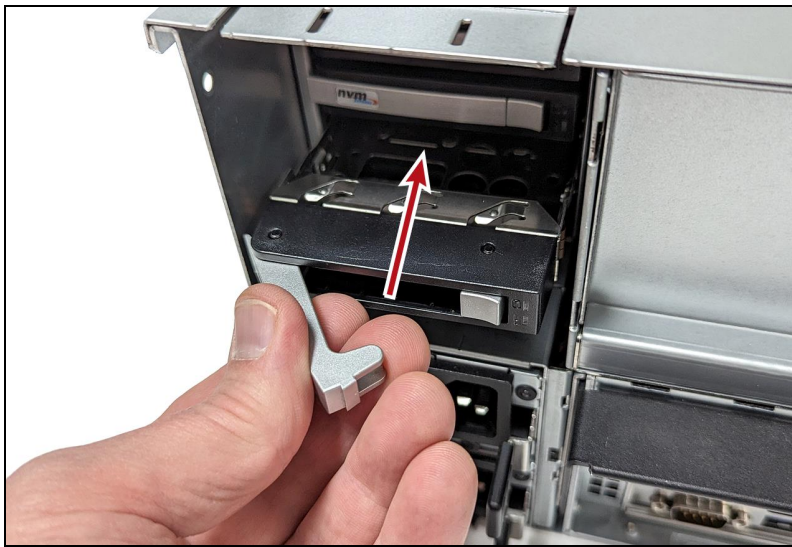


Figure 124 Insert drive into chassis.

9. Repeat [Step 3](#) through [Step 8](#) as need until all drives are installed.
10. Orient the fan module with the drive status lights at the top of the module.
11. Push the module into the chassis until it locks into place.

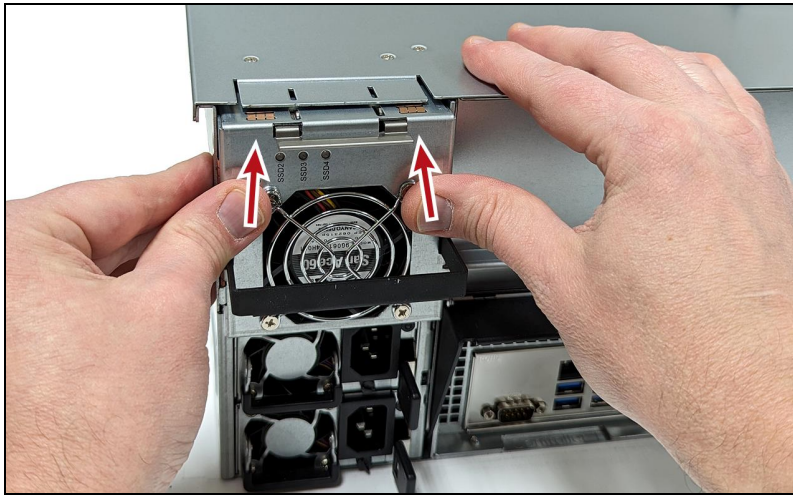


Figure 125 Insert drive into chassis.

12. Rotate the fan module handle upwards until it locks in place.

Install a Drive in a Gen2 S Series Chassis

1. Disconnect the bezel USB connection and remove the bezel from the chassis. The bezel is held on with magnets.
2. Extend the chassis from the rack far enough to remove the front top cover.
3. Simultaneously press the top cover release buttons (1) on both sides of the chassis.

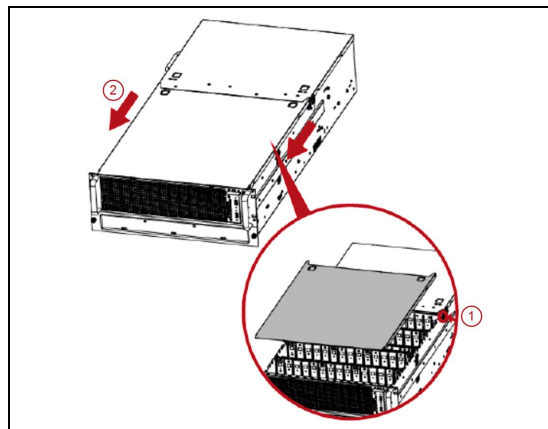


Figure 126 Remove the front top cover.

4. Slide the front top cover toward the front of the chassis (2) and lift the cover upward to remove it.

5. Rotate the drive sled locking tab upward (3).

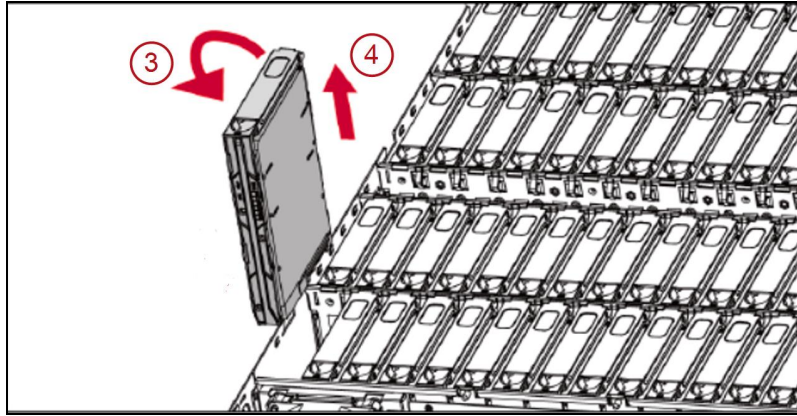


Figure 127 Remove the drive from the BlackPearl chassis.

6. Lift the drive sled out of the chassis (4).
7. Match the dimples on the drive sled with the dimples on the drive and insert the drive into the drive sled.

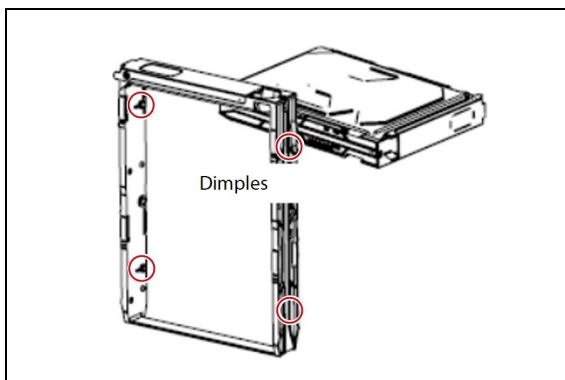


Figure 128 Match the dimples on the drive sled to the dimples on the drive.

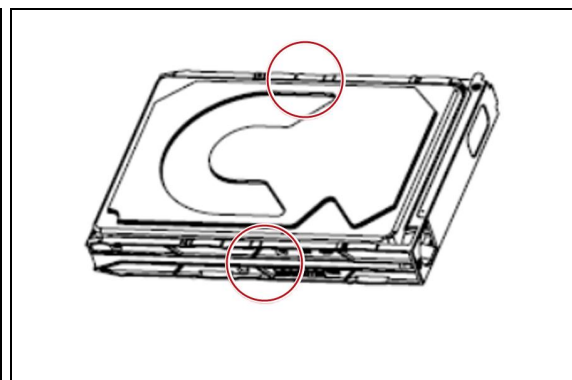


Figure 129 The drive installed in the drive sled.

8. With the locking tab in the open position, slide the drive sled back into the chassis and move the locking tab to the locked position. The drive sled slides in easily; do not force it.
9. Repeat these instructions, starting with [Step 5 on page 188](#) for each additional drive.
10. After installing all of the new drives, slide the cover back on the chassis.
11. Reattach the front bezel and the bezel USB connection.

Install a Drive in a Gen2 V Series Chassis

1. Disconnect the bezel USB connection and remove the front bezel from the chassis. The front bezel is held on by magnets.
2. Press the release buttons (1) on the ends of a tray inward to unlock it.

3. Pull the tray out of the chassis(2).

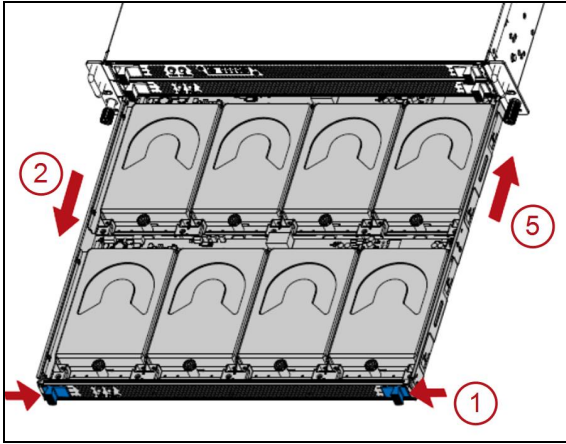


Figure 130 Remove the drive tray.

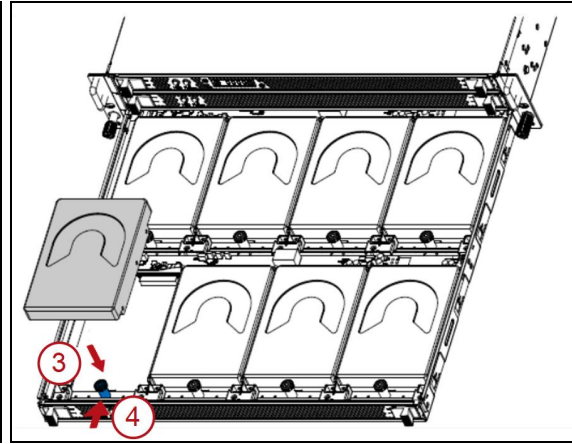


Figure 131 Install the drive.

4. Insert a drive into the chassis (3). If necessary, push the plunger (4) inward to seat the drive. Make sure that the drive is aligned and locked into the tray.
5. Repeat [Step](#) until all drives are installed or the tray is full.
6. Push the tray into the chassis (5).
7. If necessary, repeat these instructions starting with [Step 2 on page 188](#) for additional drive trays.
8. Reattach the front bezel and the bezel USB connection.

Install a Drive in a Gen2 X Series Chassis

The drives used in the Gen2 X Series chassis are mounted on drive sleds that ensure proper data and electrical connection with the backplane inside the chassis.

1. Disconnect the bezel USB connection and remove the front bezel from the chassis. The front bezel is held on by magnets.
2. Identify the location where you want to install the drive.

3. Press the release catch (1) on the drive carrier in the direction of the arrow to open the handle (2). Rotate the drive sled handle upward (3) and extend the drive sled slightly out of the chassis by pulling the middle of the handle.

**CAUTION**

Use care to avoid damaging the release latch and drive sled handle.



Figure 132 Drive sled parts.



Figure 133 Remove the drive sled with drive blank and insert the drive sled with drive.

4. Grab the carrier frame below the release handle and pull the drive sled completely out of the drive bay.

**CAUTION**

When hot-swapping a drive or drive sled, the replacement must be completed within five (5) minutes to maintain proper system airflow and cooling. If a replacement will take longer than five minutes, install a drive carrier containing a drive blank to prevent thermal damage to the system.

5. Dispose of the empty sled in accordance with your company's guidelines.
6. New drives are shipped installed in a drive sled. Press the release catch (1 in [Figure 132 on page 190](#)) on the drive sled in the direction of the arrow to release the handle.
7. With the drive handle (2) in the open position, grab the drive sled just below the handle and gently push the drive sled into the drive bay until the handle engages. The drive sled slides in easily; do not force it.
8. Press the drive handle (2) downward until the release latch connects with the release catch (1) and the drive locks in place.
9. Repeat these instructions, starting with [Step 2 on page 189](#) for each additional drive.
10. Reattach the front bezel and the bezel USB connection.

Install a Drive in a Gen1 Chassis

The drives used in the Gen1 BlackPearl NAS are mounted on drive sleds that ensure proper data and electrical connection with the backplane inside the BlackPearl NAS.

Remove the Front Bezel

If you are installing a new drive in the front of the, 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.

Remove the Empty Drive Sled

Use the following steps to remove an empty drive sled.

1. Locate the empty drive bays where you want to install a new drive.

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

2. Slide the drive sled locking tab to the right to release the drive sled handle.

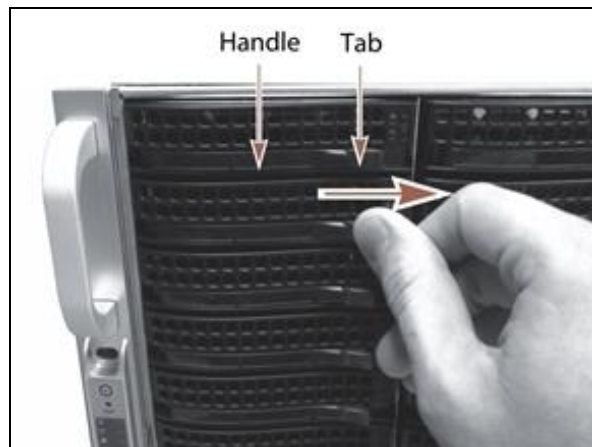


Figure 134 Slide the tab to the right to release the drive sled handle.

3. 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.

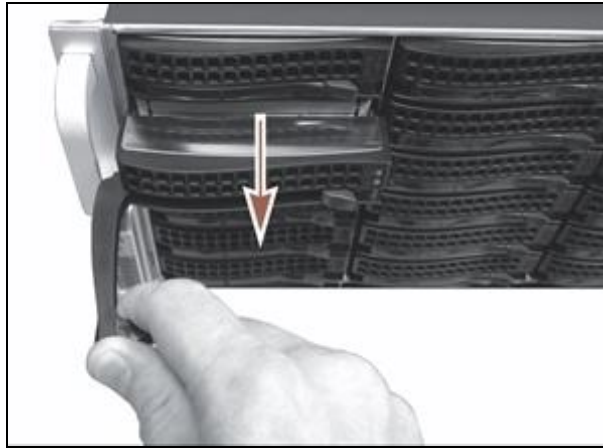


Figure 135 Pull the sled out of the.

4. 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 136 Install the drive into the BlackPearl NAS.

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.

CHAPTER 10 - MAINTAINING THE BLACKPEARL NAS SOLUTION

This chapter describes software maintenance procedures for the Spectra BlackPearl NAS solution.

Data Integrity Verification	195
Start Disk Media Data Integrity Verification	195
Cancel Disk Media Data Integrity Verification	196
Initiate RSC Backup	197
Manually Enter Activation Keys	198

DATA INTEGRITY VERIFICATION

The BlackPearl NAS allows you to perform on-demand data integrity verifications on any disk pools connected to the. 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.

Start Disk Media Data Integrity Verification

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

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Data Integrity Verification**.

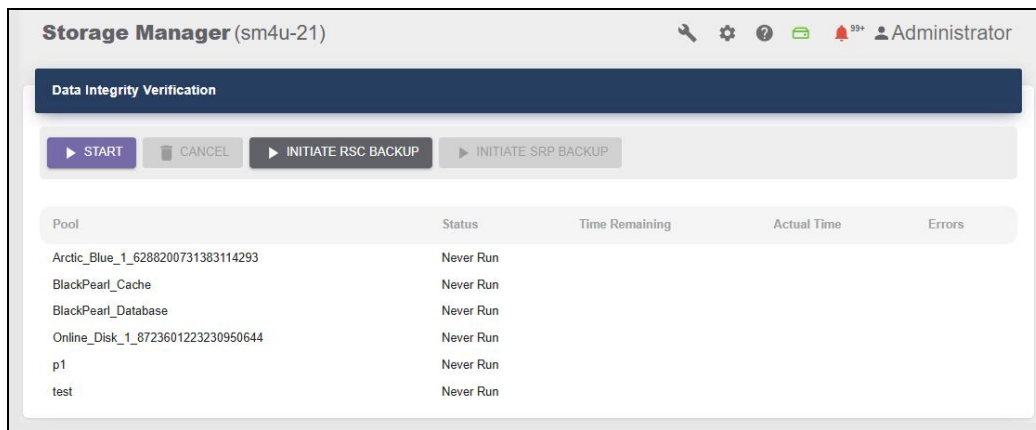


Figure 137 The Data Integrity Verification screen.

2. Select the disk pool for which you want to start the data integrity verification and click **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**.



CAUTION

In the event that the data integrity verification detects suspect objects, they are listed in the Suspect Objects pane. If possible, retrieve the object from another storage domain, delete the object from the and then PUT the object again.

The affected files cannot be retrieved from the storage pool, and may need to be transferred to the BlackPearl NAS again, if the data policy did not specify multiple copies of the data. If you do not have copies of the affected files on your host or another location, they are lost.

Cancel Disk Media Data Integrity Verification

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

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Data Integrity Verification**.
2. Select the pool for which you want to stop verification and click **Cancel**. A confirmation screen displays.
3. Click **Submit** to stop the verification.

INITIATE RSC BACKUP

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

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Data Integrity Verification**.

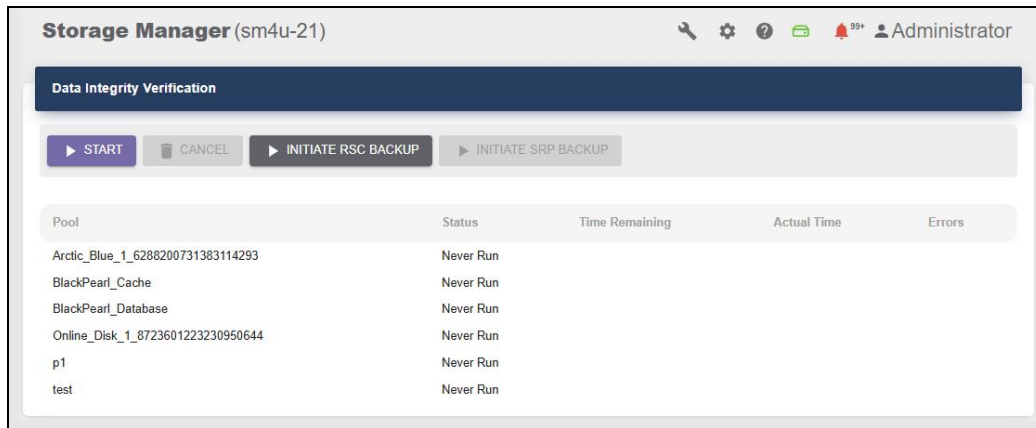


Figure 138 The Data Integrity Verification screen.

2. Click **Initiate RSC Backup**. A confirmation screen displays (not shown).
3. Click **Submit** to manually backup the current configuration.

MANUALLY ENTER ACTIVATION KEYS

Use the following instructions to manually enter activation keys.



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.

1. When manually entering the activation keys for an initial installation, they **must** be entered in the following order:

- Capacity keys
- Product keys
- All other keys

If this is not an initial installation, you can enter activation keys in any order. Proceed with [Step 2 on page 198](#).

Capacity keys:

Key Type	Description
<product type> SAS Count	Enables the specified number of SAS drives present in the system for NAS storage.
<product type> SATA Count	Enables the specified number of SATA drives present in the system for NAS storage.
<product type> SSD Count	Enables the specified number of SSDs present in the system for NAS storage.

All Other Keys:

Any additional keys included on the Software Activation Key Certificate, for example the Software Update key, can be entered in any order, as long as they are entered after the product keys.

2. Use the toolbar in the upper-right to select **Settings (gear icon)> Activation Keys**.
3. In the Activation Keys pane, click **Add**. The Add Activation Key dialog box displays (not shown).
4. Enter the **Activation Key**.
5. Click **Submit**.
6. If necessary, repeat [Step 3](#) through [Step 5](#) to add additional keys.

CHAPTER 11 - TECHNICAL SUPPORT

This chapter describes using the BlackPearl user interface to configure the support features of the Spectra BlackPearl NAS, and how to submit a support ticket to Spectra Logic.

About AutoSupport	200
Configure AutoSupport Mail Recipients	201
Create a New Mail Recipient	201
Edit a Mail Recipient	202
Send a Test Email	203
Delete a Mail Recipient	203
Log Sets	205
Configure a Log Set Schedule	206
Manually Generate Log Sets	207
Email a Log Set	208
Download a Log Set	209
Delete Log Sets	209
Access the Technical Support Portal	211
Create an Account	211
Log Into the Portal	212
Spectra Logic Technical Support	213
Before Contacting Support	213
Determine the Serial Number	213
Opening a Support Ticket	214
Search for Help Online	214
Submit an Incident Online	217
Submit an Incident by Phone	219
Remote Support	220
Enabling Remote Support	220
Disabling Remote Support	221

ABOUT AUTOSUPPORT

AutoSupport lets the BlackPearl NAS automatically contact mail recipients when certain kinds of messages are generated. It is also used to generate AutoSupport Log (ASL) sets for use by Spectra Logic Technical Support. You can configure the to email ASL sets when critical events occur, or on a monthly basis. You can also choose to have mail recipients receive ASL sets.

CONFIGURE AUTOSUPPORT 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 Recipient screen to add, edit, or delete mail recipient accounts.

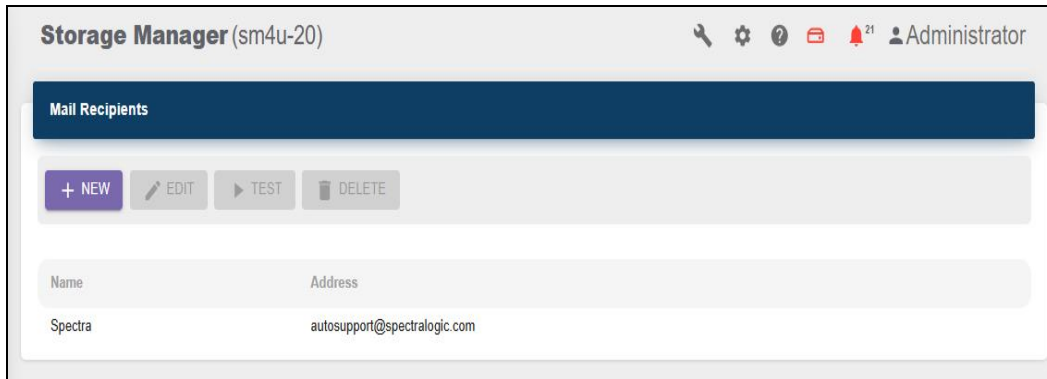


Figure 139 The Mail Recipients screen.

Create a New Mail Recipient

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Mail Recipients**. The Mail Recipients screen displays.
2. Click **New**. The New Mail Recipient dialog box displays.

Figure 140 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. Note: 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 BlackPearl NAS on the first of each month. Error log sets are sent anytime an error occurs that causes the to generate a log set.
Choose the message severities you want to receive	Select from the listed message types which severities of message this mail recipient should receive. The BlackPearl NAS automatically sends email messages of the selected severity to the recipient when they are generated. Note: For the mail recipient to receive all messages generated by the, select all boxes.

4. Click **Submit** to save the information. The Mail Recipients screen re-displays with the new mail recipient added to the list of mail recipients.

Edit a Mail Recipient

Use the following steps to edit a mail recipient account.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Mail Recipients**. The Mail Recipients screen displays.

2. From the list of mail recipients, select the name and then click **Edit**. The Edit Mail Recipient dialog box displays.

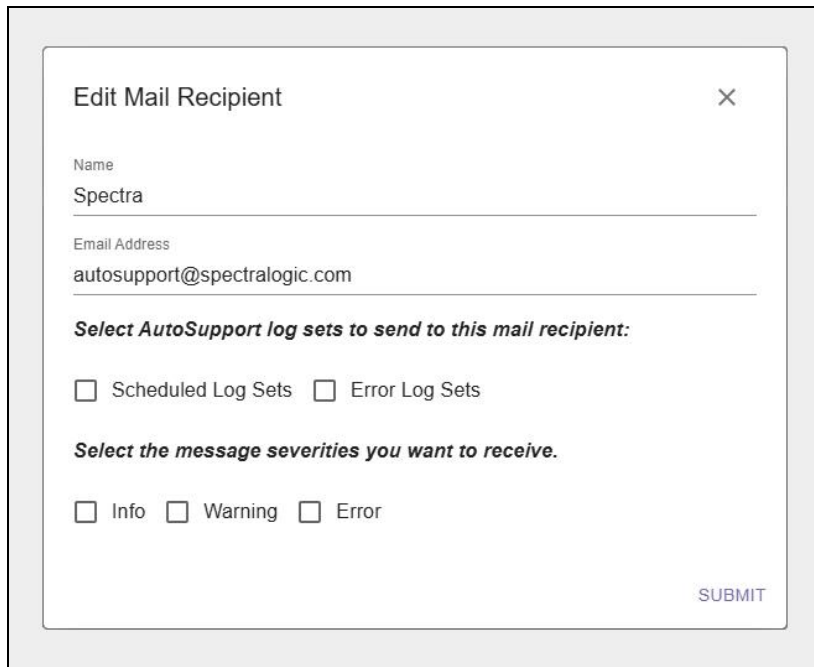


Figure 141 The Edit Mail Recipient dialog box.

3. Change the information for the recipient as required and then click **Submit**.

Send a Test Email

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

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Mail Recipients**. The Mail Recipients screen displays.
2. From the list of mail recipients, select the name of the recipient you want to receive a test email, and then click **Test**. The Send Test Email dialog box displays.
3. Click **Send**. The BlackPearl NAS immediately sends a test email to the selected account.
4. Verify the user received the email from the BlackPearl NAS. If the email is not received, verify that you entered the SMTP server settings correctly (see [Configure the SNMP Service on page 95](#)).

Delete a Mail Recipient

Use the following steps to delete a mail recipient account.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Mail Recipients**. The Mail Recipients screen displays.
2. From the list of mail recipients, select the name of the recipient you want to delete, and then click **Delete**. The Delete Mail Recipient dialog box displays (not shown).

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

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

LOG SETS

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

- **Log Sets** contain information about the configuration and status of the BlackPearl NAS 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 and are used by Spectra Logic Technical Support for in-depth troubleshooting. Statistic log sets are too large to be mailed directly from the and must be downloaded.
- **Kernel Log Sets** are generated whenever a process on the fails. This report cannot be generated manually.

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

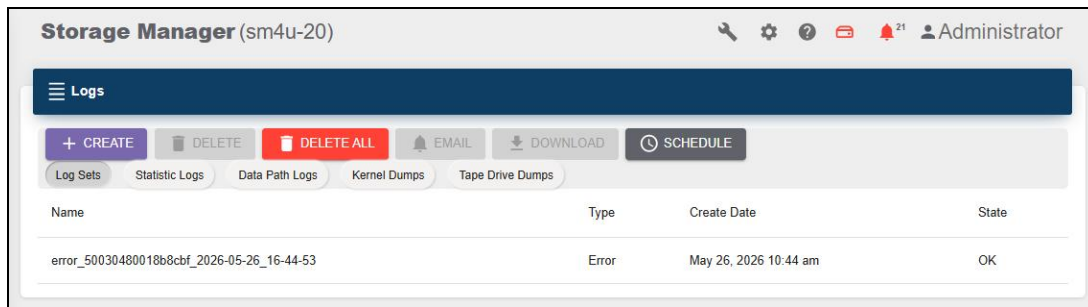
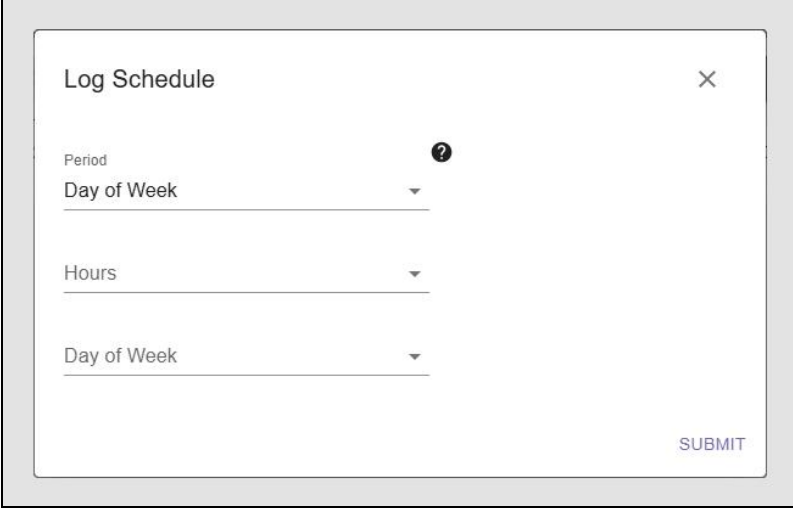


Figure 142 The Logs screen.

Configure a Log Set Schedule

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

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Logs**. The Logs screen displays.
2. Click **Schedule**. The Log Schedule dialog box displays.



The screenshot shows a 'Log Schedule' dialog box. It has a title bar with the text 'Log Schedule' and a close button 'X'. The main area contains three sections: 'Period' with a 'Day of Week' dropdown menu and a help icon '?'; 'Hours' with a dropdown menu; and another 'Day of Week' dropdown menu. A 'SUBMIT' button is located at the bottom right of the dialog.

Figure 143 The Log Schedule dialog box.

3. Use the **Period** drop-down menu to select the frequency of the log schedule.
4. Use the **Hours** drop-down menu to select the hour when you want the system to generate the log set.
5. If you selected **Day of Week** or **Day of Month**, use the corresponding drop-down menu to select the day(s) on which to run the schedule.
6. Click **Submit**.

Manually Generate Log Sets

Although the BlackPearl NAS auto 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. Use the toolbar in the upper-right to select **Settings (gear icon) > Logs**. The Logs screen displays.
2. Click **Create**. The Create Manual Logset dialog box displays.

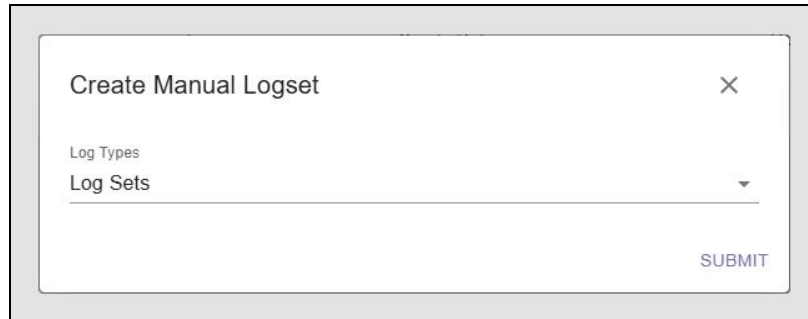


Figure 144 The Create Manual Logset dialog box.

3. Use the **Log Types** drop-down menu to select the type of log to generate:
 - **Log Set** - generates a log set for use in general troubleshooting.
 - **Statistic Logs** - generates a log set used for in-depth troubleshooting. This log is not human readable.
4. Click **Submit**.

Email a Log Set

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

- Notes:**
- You must configure the SMTP settings on the before you can send emails. See [Configure the SNMP Service on page 95](#) to configure the SMTP settings.
 - Statistic Log Sets are too large to be emailed from the, and must be downloaded. See [Download a Log Set on the next page](#).

- Use the toolbar in the upper-right to select **Settings (gear icon) > Logs**. The Logs screen displays.
- Use the **logset type** buttons in the upper-right to select the type of logs to display.

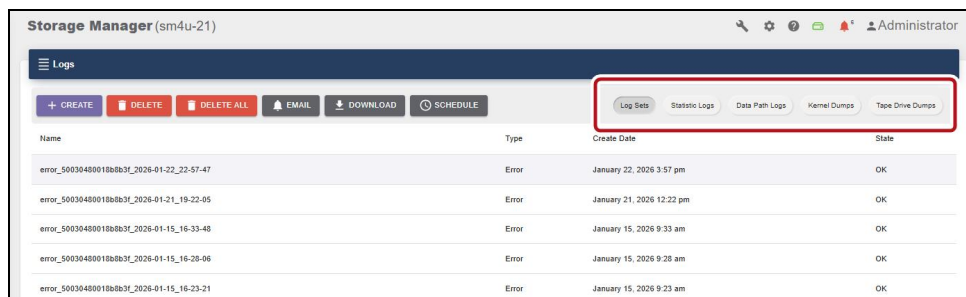


Figure 145 The Logs screen - Logset Type buttons

- Select the logset you want to email and click **Email**. The Email Logset dialog box displays.



Figure 146 The Email Logset dialog box.

- Use the **Mail Recipients** drop-down menu to select one or more configured mail recipients.
- Click **Submit**.

Download a Log Set

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

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Logs**. The Logs screen displays.
2. Use the **logset type** buttons in the upper-right to select the type of logs to display.

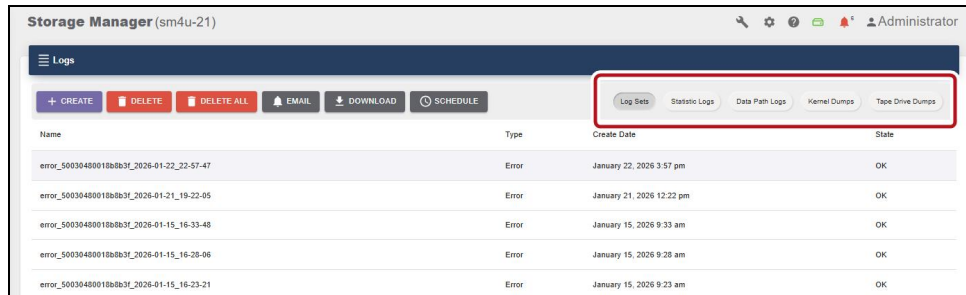


Figure 147 The Logs screen - Logset Type buttons

3. Select the logset you want to download and click **Download**. The Download Logset screen displays (not shown).
4. On the Download Logset screen, click **Submit**.

Delete Log Sets

Delete a Single Log Set

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

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Logs**. The Logs screen displays.
2. Use the **logset type** buttons in the upper-right to select the type of logs to display.

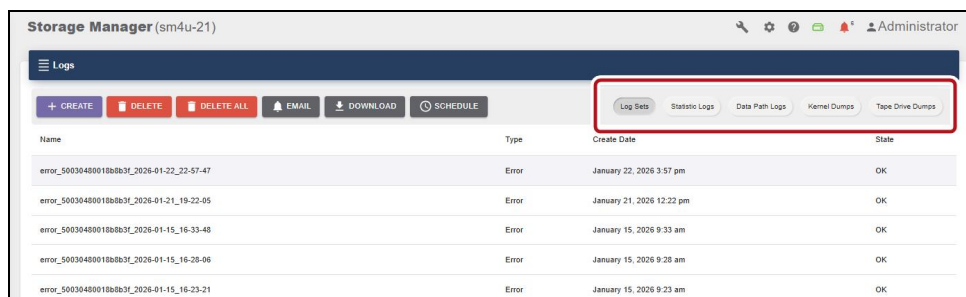


Figure 148 The Logs screen - Logset Type buttons

3. Select the logset you want to delete and click **Delete**. The Delete Log screen displays (not shown)
4. On the Delete Log screen, click **Submit**.

Delete All Log Set of a Specified Type

Use the instructions in this section to delete all log sets of a specified type of log.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Logs**. The Logs screen displays.
2. Click **Delete All**. The Delete All dialog box displays.



Figure 149 The Delete All dialog box.

3. Use the **Log Types** drop-down menu to select which type of logs to delete.
4. Click **Submit**.

ACCESS THE TECHNICAL SUPPORT PORTAL

The Spectra Logic Technical Support portal provides access to the Knowledge Base, the current version of BlackPearl software for the, 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 BlackPearl software, or to open a support ticket.

Note: If you own 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**.

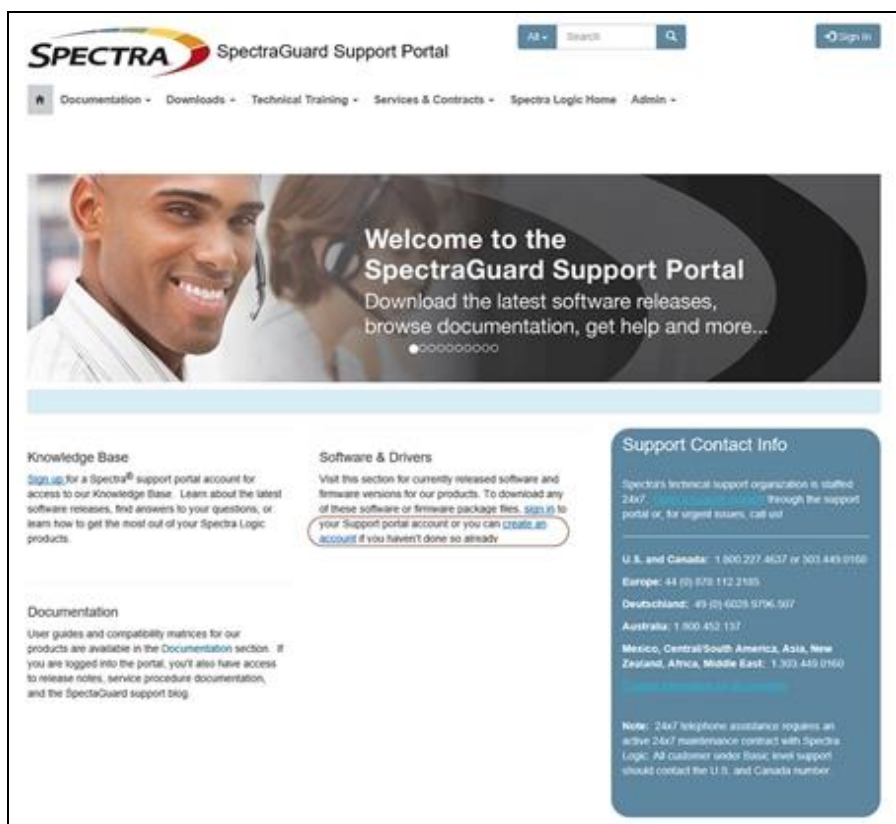


Figure 150 The Spectra Logic Technical Support portal home page.

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

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 BlackPearl NAS, 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 [Monitor the Hardware on page 159](#)) 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 BlackPearl 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 [Spectra Logic Technical Support above](#)).

Determine the Serial Number

If you have more than one BlackPearl NAS, it is necessary to determine the serial number of the before contacting Spectra Logic Technical Support. Use the following steps to determine the serial number.

1. Use the toolbar in the upper-right to select **Help & Support (question mark icon) > About**.
2. The serial number is listed in the Product Information pane.

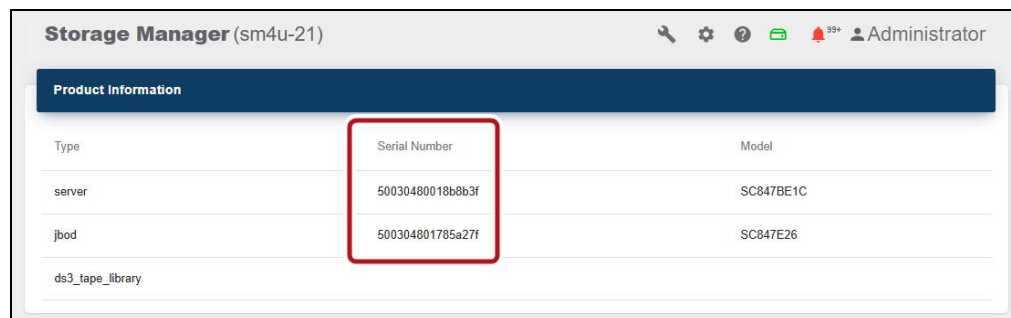


Figure 152 The Product Information screen - Serial Number column.

OPENING A SUPPORT TICKET

You can open a support incident using the Spectra Logic Technical Support portal or telephone.

Search for Help Online

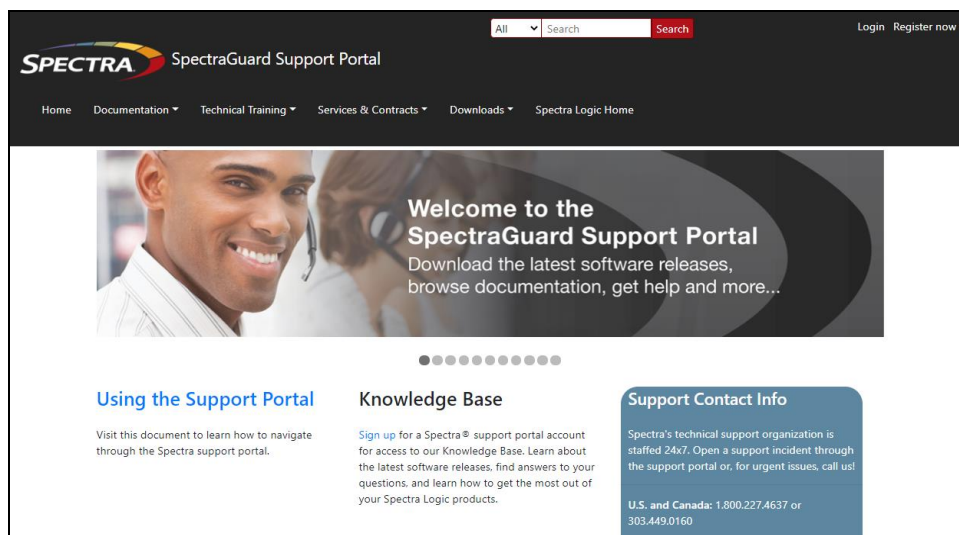


Figure 153 The Spectra Logic Technical Support portal home page.

1. Make notes about the problem, including what happened just before the problem occurred.
2. Gather the following information:
 - Your Spectra Logic customer number
 - Company name, contact name, phone number, and email address
 - The library serial number (see [Determine the Serial Number on the previous page](#))
 - Type of host system being used
 - Type and version of host operating system being used
 - Type and version of host storage management software being used
3. If necessary, log in to the Support Portal by clicking **Login**, enter your **email address** and **password**, and click **Log in**.

Note: See [Access the Technical Support Portal on page 211](#) if you have not previously created an account on the Technical Support portal.

4. From any page, select **Incident>Incidents & Inventory**.

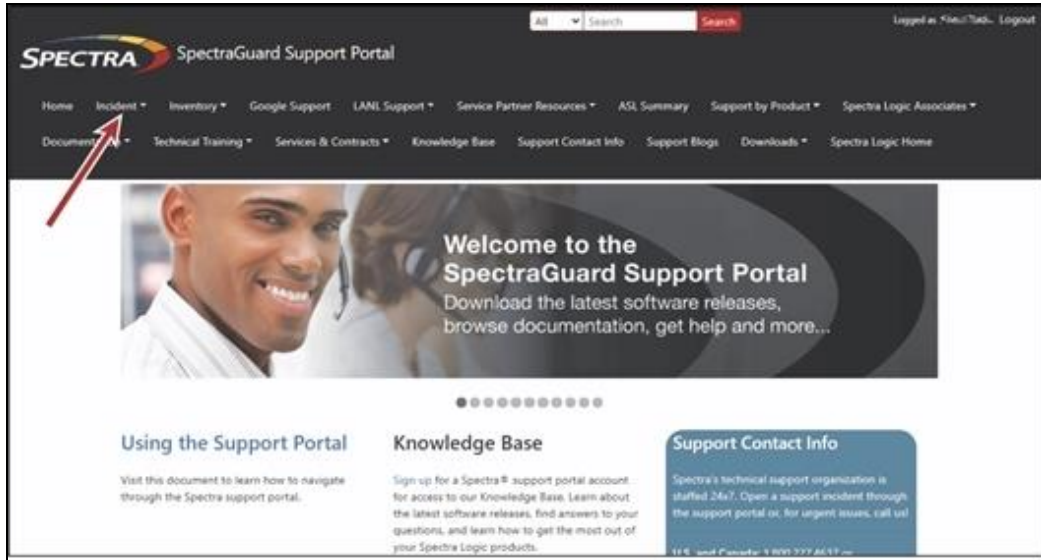


Figure 154 Select **Incidents > Incidents & Inventory**.

5. Select **Open or View Incidents**.

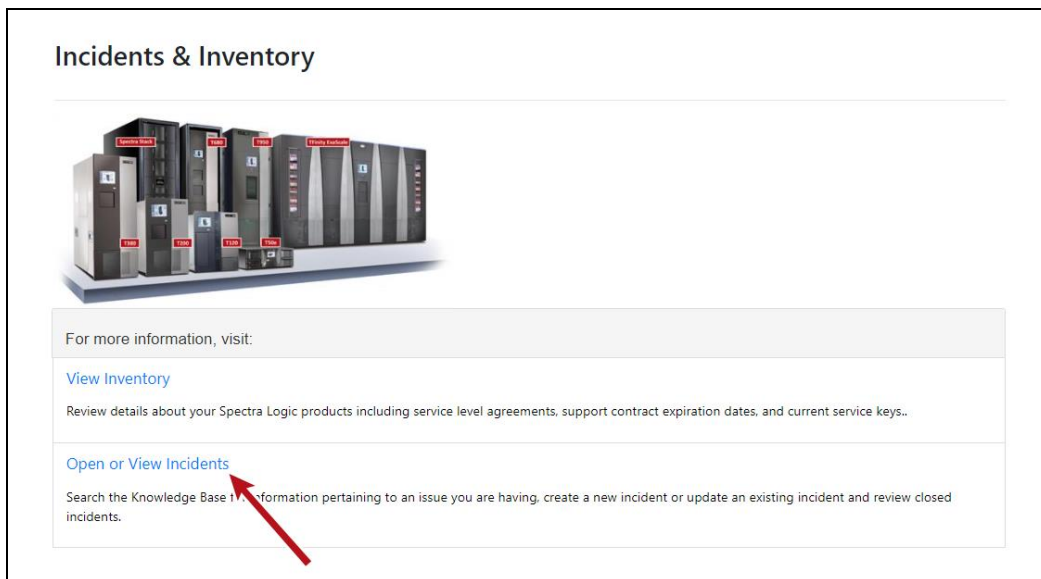


Figure 155 Select **Open or View Incidents**.

6. In the Search dialog box, enter a term or phrase about your problem (1) and click **Search** (2).

Open or View Incidents

What can we help you with?

Search Search

Serial Number: Product Status: Active Created Date: mm/dd/yyyy

[Export to Excel](#)

Incident N...	Product	Account	Date Open...	Subject	Description	Modified On	Problem R...
294900	TLB0421021 - Spectra T120 Library	Spectra Logic Corporation - Boulder	03-05-2021	Open by ASL parser	This is a test - please disregard. Subject = Manual T120 AutoSupport Log Set for Library TLB0421021 on 03-05-2021 11:58:34	4/20/2021 5:05 PM	

Figure 156 Enter a search phrase and click **Search**.

7. If the search does not provide an answer, click **Open a New Incident**.

Open or View Incidents

What can we help you with?

export Search

search results for *export* Sort by Relevance

[T120 Import/Export Modes 20200709194431340](#)

T120 Import/Export Modes, by the operator's selection. **Exporting** tapes When a tape is selected by the host software to be **exported**. Moves" button. **Exporting** tapes Like the Shared mode, all **exports** initiated by the host software, 's process for importing and **exporting** tapes, to and from the library. The different modes also, available for single partition libraries. The 8 EE slots in the EE port are available for import and **export**, port, are physical moves. As a result, the number of tapes to be imported or **exported** in a single

[Operators cannot import or export media 20201130201216990](#)

User with operator privileges cannot import or export tapes to a partition's storage slots.

[Spectra TFinity Library User Guide 20200827222441320](#)

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. . In particular, but without limitation, the Software Product may not be **exported** or re-**exported**. Modules (LCM and RCM) 50 **Exporting** Controllers. 230 IMPORT AND **EXPORT**

[Next](#) [Open a New Incident](#)

Figure 157 Click **Open a New Incident**.

8. On the Create Incident page, enter the requested information providing as much detail as possible. When you are finished, click **Submit**.

Create Incident

Severity *

Problem Description *

Email addresses to include in correspondence

Customer *

Product *

Select files...

DELIVERY Address For Shipping Parts

6101 Lookout Rd, Boulder, CO 80301-3580 UNITED STATES

☐ Confirm The Ship To Address

Submit

Figure 158 Enter information about your incident and click **Submit**.

Submit an Incident Online

1. Make notes about the problem, including what happened just before the problem occurred.
2. Gather the following information:
 - Your Spectra Logic customer number
 - Company name, contact name, phone number, and email address
 - The library serial number (see [Determine the Serial Number on page 213](#))
 - Type of host system being used
 - Type and version of host operating system being used
 - Type and version of host storage management software being used
3. If necessary, log in to the Support Portal by clicking **Login**, enter your **email address** and **password**, and click **Log in**.

Note: See [Access the Technical Support Portal on page 211](#) if you have not previously created an account on the Technical Support portal.

4. From any page, select **Inventory>My Inventory**.

5. Locate the row of the product for which you want to submit an incident and click **Create Incident**.

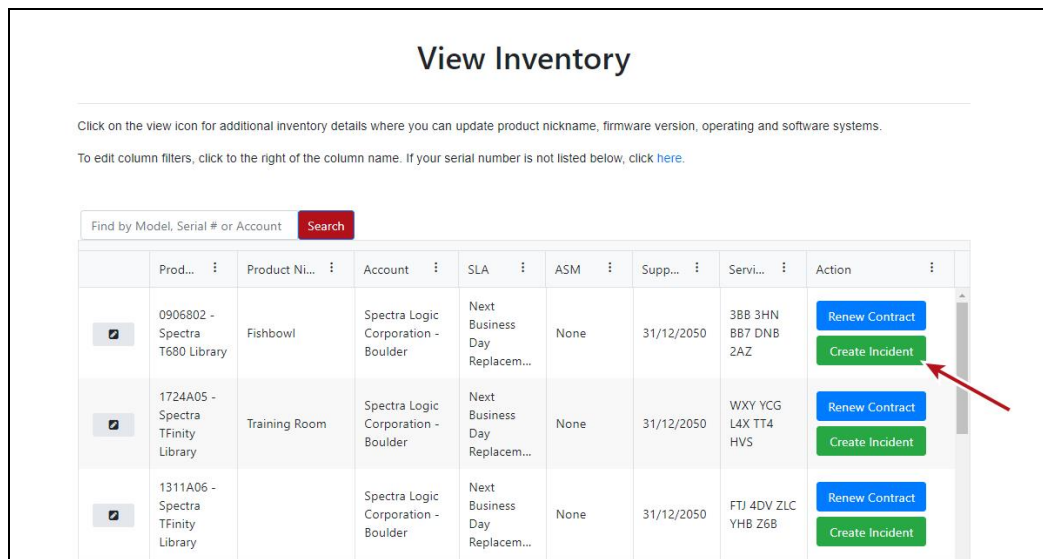


Figure 159 Click **Create Incident**.

6. On the Create Incident page, enter the requested information providing as much detail as possible. When you are finished, click **Submit**.

The screenshot shows the 'Create Incident' form. It has the following fields and elements:

- Severity ***: A dropdown menu.
- Problem Description ***: A large text area.
- Email addresses to include in correspondence**: A text input field.
- Customer ***: A dropdown menu with 'Spectra Logic Corporation - Boulder' selected.
- Product ***: A dropdown menu with '0906802 - Spectra T680 Library' selected.
- Select files...**: A button to upload files.
- DELIVERY Address For Shipping Parts**: A text input field with the address '6101 Lookout Rd, Boulder, CO 80301-3580 UNITED STATES'.
- ☐ Confirm The Ship To Address
- Submit**: A red button.

Figure 160 Enter information about your incident and click **Submit**.

Submit an Incident by Phone

Contact Spectra Logic Technical Support by phone using the information below.

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
Additional international numbers available at support.spectralogic.com/home If you have a Spectra Logic Portal account, please log in for country-specific numbers at support.spectralogic.com/support-contact-info	

REMOTE SUPPORT

Remote Support is an option that allows Spectra Logic Technical Support personnel to access the root console of the. This option is for troubleshooting purposes only.

Enabling Remote Support

1. Enter the Remote Support activation key as described in [Manually Enter Activation Keys](#) on page 198.

Note: The Remote Support activation key is only valid for 24 hours. When the key expires, remote access is automatically disabled.

2. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
3. Select the **Administrator** account and then click **Edit**. The Edit User dialog box displays.

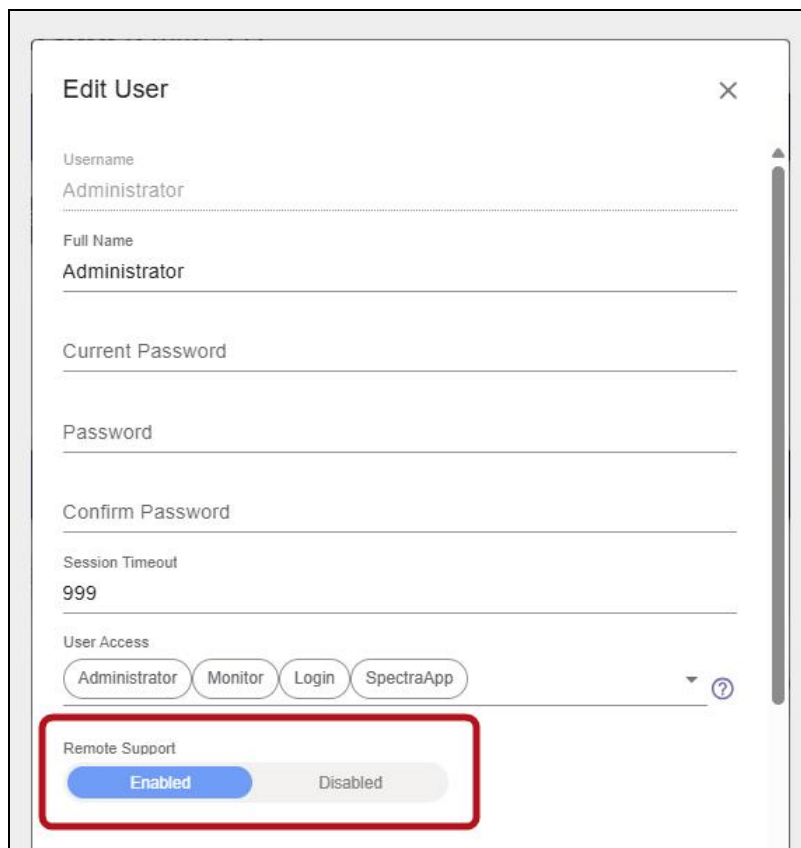
The image shows a screenshot of the 'Edit User' dialog box. The dialog has a title bar with 'Edit User' and a close button. Inside, there are several input fields: 'Username' with 'Administrator', 'Full Name' with 'Administrator', 'Current Password', 'Password', and 'Confirm Password'. Below these is a 'Session Timeout' field with '999'. Then there is a 'User Access' section with four buttons: 'Administrator', 'Monitor', 'Login', and 'SpectraApp'. At the bottom, there is a 'Remote Support' section with a slider. The slider is currently set to 'Enabled' (blue) and 'Disabled' (grey). A red rectangle highlights the 'Remote Support' section.

Figure 161 The Edit User dialog box - Remote Support slider.

4. Use the **Remote Support** slider to select **Enabled**.

Note: The Enable Remote Support checkbox does not display until you enter a Remote Support activation key.

5. Click **Submit** (not pictured).



IMPORTANT

After Spectra Logic Technical Support informs you that they no longer require root access to the, you should disable Remote Support to prevent any potential unauthorized access.

The Remote Support activation key is only valid for 24 hours. When the key expires, remote access is automatically disabled.

Disabling Remote Support

Use the instruction in this section to disable Remote Support.

Note: The Remote Support activation key is only valid for 24 hours. When the key expires, remote access is automatically disabled.

1. Use the toolbar in the upper-right to select **Settings (gear icon) > Users**.
2. Select the **Administrator** account and then click **Edit**. The Edit User dialog box displays.

Figure 162 The Edit User dialog box - Remote Support slider.

3. Use the **Remote Support** slider to select **Disabled**.
4. Click **Submit** (not pictured).

CHAPTER 12 - FREQUENTLY ASKED QUESTIONS (FAQ)

Resolve a BlackPearl Management Port IP Address Conflict	223
Using the Console	223
Using a Separate Computer	223

RESOLVE A BLACKPEARL MANAGEMENT PORT IP ADDRESS CONFLICT

The default address of the BlackPearl 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 BlackPearl 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 BlackPearl NAS as described in [Log Into the BlackPearl User Interface on page 68](#). 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 BlackPearl NAS to your network.

Using the Console

Using the BlackPearl NAS console is the recommended way to change the BlackPearl management port IP address. For instructions on using the console to configure the management port IP address, see [Configure the BlackPearl Management Port on page 65](#).

Using a Separate Computer

If you cannot use the console, use a computer or laptop disconnected from any existing network to change the BlackPearl 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 BlackPearl management port on the BlackPearl NAS. See [Components on page 25](#) to locate the management port.
3. Open a web browser on the computer. For a list of compatible browsers, see [Supported Browsers](#).
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 BlackPearl user interface uses a secure connection.

5. Resolve the security certificate warning for the BlackPearl user interface. The warning displays because the 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 primary administrator username and password. The fields are case sensitive.
 - The default username is **Administrator**.
 - The default password is the serial number of the master node. Find the serial number on the sticker positioned on the top of the chassis, on the right-hand side, toward the front. The serial number is indicated by the letters "SN" on the sticker.

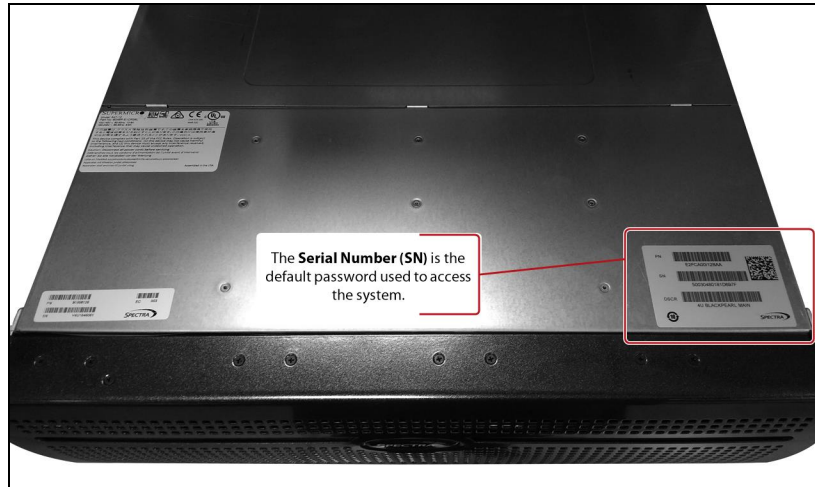


Figure 163 The BlackPearl serial number sticker.

1. Use the toolbar in the upper-right to select **Configuration (wrench icon) > Network**.
2. In the Network Interfaces pane, select the **Management** row and then click **Edit**. The Edit Data Interface dialog box displays.

IP Address	Prefix Length	Actions
10.5.1.215	24	+ -
2620:a3:e030:1151:225:9	64	+ -

Figure 164 The Edit Management dialog box.

3. Select the **DHCP** checkbox to configure the 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 BlackPearl 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.

- **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. Enter the **IPv4 Default Gateway**.

Note: If you selected DHCP in [Step on page 223](#), this option is unavailable.

6. Enter the **IPv6 Default Gateway**.

7. Change the **MTU** value, if desired. If you set the MTU value to something other than 1500, make sure that your switch configuration supports larger MTU settings, as well as all the hosts on the network. Acceptable values are 576 to 65535.

Note: Most networking designs are configured to use a value of 1500 or 9000.

8. Click **Submit**.

Note: When you change the IP address of the BlackPearl 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.

9. Disconnect the Ethernet cable from the BlackPearl management port.

10. Connect a cable from your network to the management port on the BlackPearl NAS. You are now able to connect to the with the IP address configured.

APPENDIX A - IPMI CONFIGURATION

This appendix provides instructions for configuring IPMI for the BlackPearl NAS using the 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 performance.

1. If the BlackPearl NAS is currently powered on, shut down the as described in [Reboot or Shut Down a BlackPearl NAS on page 174](#).
2. Connect a monitor and USB keyboard to the rear of the BlackPearl NAS. See [Components on page 25](#) to locate the monitor and USB connectors.
3. Power on the monitor.
4. Power on the as described in [Power On the on page 63](#).
5. When prompted by the, press **DEL** to enter the BIOS.

Note: The only displays this prompt for a few seconds. If you do not press **DEL** in time to enter the BIOS, let the complete it's boot process, then reboot the and repeat [Step 4](#).

6. If necessary, log into the IPMI interface.

- The username is **admin**.
- The default password depends on when the product was sold by Spectra Logic.
 - For BlackPearl NASs sold **after** February 2024, the password is the serial number of the master node with the characters '@a' appended to the end of the serial number. For example:
`productserialnumber@a`
 - For BlackPearl NASs sold **before** February 2024, the password is the serial number of the master node.

Find the serial number on the sticker positioned on the top of the chassis, on the right-hand side, toward the front.

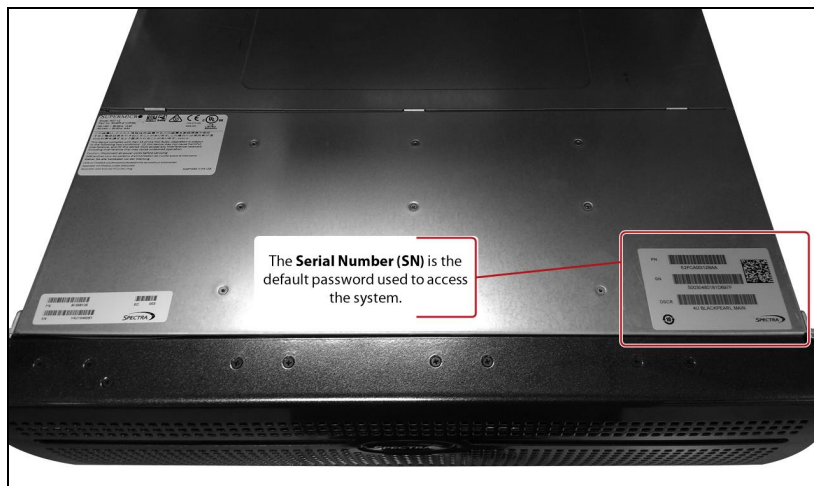


Figure 165 The BlackPearl serial number sticker.

7. Use the keyboard to navigate to the **IPMI** tab and then select **BMC Network Configuration**. The current settings of the BMC configuration display.

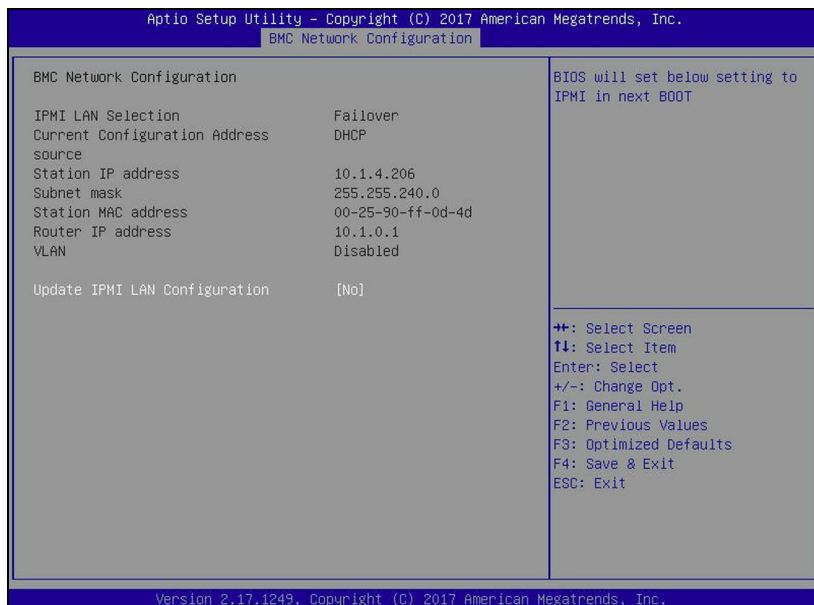


Figure 166 The BMC Configuration screen.

8. Use the keyboard to select **Update IPMI LAN Configuration**. A confirmation window displays. Select **YES** to continue. The current IPMI settings display.

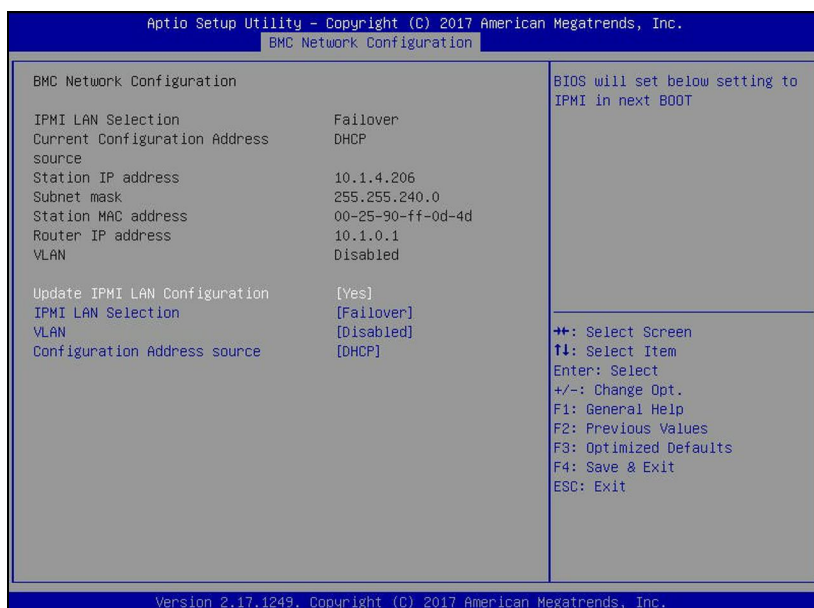


Figure 167 Current IPMI settings.

9. 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 startup, detect if the dedicated IPMI port is connected. If not, the uses the LAN1 port for IPMI traffic.

10.If desired, select **VLAN** to enable or disable VLAN as needed.

11.To change the IPMI address settings, select **Configuration Address source**. The current address source information displays.

12.Select **Static** or **DHCP** addressing.

- If you select **DHCP**, skip to [Step 14](#).
- If you select **Static**, IP addressing fields display.

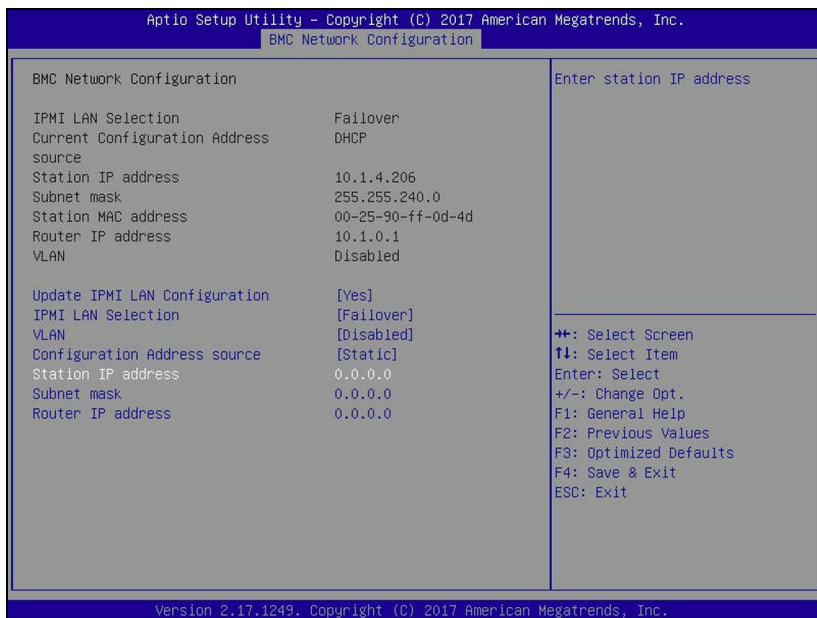


Figure 168 Enter Static IP information.

13.Configure the **Station IP address**, **Subnet mask**, and **Router IP address** with the desired address values.

Note: Only IPv4 addresses are valid.

14.Press **F4** to exit the BIOS and save the entered settings. The BlackPearl NAS reboots.

APPENDIX B - SPECIFICATIONS

This appendix provides detailed specifications for the BlackPearl NAS master nodes, the 44-bay expansion node, 77-bay expansion node, 96-bay expansion node, and 107-bay expansion node. The specifications listed here pertain to the currently shipping BlackPearl chassis.

Data Storage Specifications	231
System Specification	234
Size and Weight	238
Environmental Specifications	244
Temperature & Humidity	244
Heat Generation	249
Power Requirements	249
Input Power Requirements	249
Power Cord Specifications	252
Interface Specifications	255
System Interface Connectors	255
Expansion Node Interface Connectors	259
Network Interface Cables	259
Networking Naming Conventions	260
Universal Serial Bus (USB) Support	261

DATA STORAGE SPECIFICATIONS

The following tables show the data storage specifications for the BlackPearl NASs.

- Notes:**
- 1 TB is defined as 1,000,000,000,000 bytes.
 - 1 GB is defined as 1,000,000,000 bytes.

BlackPearl Gen3 F Series

Drive Purpose	Drive Type
NAS	24 NVMe SSD Gen5 Drive storage capacities: 1.6 TB, 6.4 TB, 12.8 TB, or 25.6 TB.

BlackPearl Gen3 H Series

Drive Purpose	Drive Type
Write Performance, Metadata Performance, or NAS	4, 8, 16, 20, or 22 TB Spinning-Disk SAS

BlackPearl Gen2 X Series

Drive Purpose	Drive Type
Write Performance, Metadata Performance, or NAS	• 1.6 TB SSD Gen4 • 6.4 TB SSD Gen4

BlackPearl Gen2 S Series and Gen2 V Series

Drive Purpose	Drive Type
Write Performance, Metadata Performance	• 1.6 TB SSD Gen4 • 6.4 TB SSD Gen4 (S Series only)
NAS	• 4 TB SAS HDD • 8, 12, and 20 TB SAS Self-Encrypting Drive

BlackPearl Gen1 S Series 4U

Drive Purpose	Drive Type
NAS	• 4, 8, or 12 TB Spinning-Disk SAS • 12 or 16 TB Spinning-Disk SATA • 8, 12, and 20 TB SAS Self-Encrypting Drive

BlackPearl Gen1 P Series 4U

Drive Purpose	Drive Type
NAS	960, 1600, or 1920 GB Solid-State SAS

BlackPearl Gen1 V Series 2U

Drive Purpose	Drive Type
NAS	• 4, 8, 12, or 16 TB Spinning-Disk SAS • 12 or 16 TB Spinning-Disk SATA • 8, 12, and 20 TB SAS Self-Encrypting Drive

44-Bay Expansion Node

Drive Purpose	Specification
NAS	• 4, 8, 12, or 16 TB Spinning-Disk SAS • 12 or 16 TB Spinning-Disk SATA • 8, 12, and 20 TB SAS Self-Encrypting Drive

77-Bay Expansion Node

Drive Purpose	Specification
NAS	• 800 GB Solid-State SAS • 4, 8, 12, or 16 TB Spinning-Disk SAS ¹ • 12 or 16 TB Spinning-Disk SATA • 8, 12, and 20 TB SAS Self-Encrypting Drive

96-Bay Expansion Node

Drive Purpose	Specification
NAS	8, 12, or 16 TB Spinning-Disk SATA

107-Bay Expansion Node

Drive Purpose	Specification
NAS	• 800 GB Solid-State SAS • 4, 8, 12, or 16 TB Spinning-Disk SAS • 12 or 16 TB Spinning-Disk SATA • 8, 12, and 20 TB SAS Self-Encrypting Drive

¹) 16 TB SAS drives only supported in a HotPair configuration.

SYSTEM SPECIFICATION

The following tables provide an overview of the devices in the BlackPearl NASs.

Gen3 F Series BlackPearl NAS

Parameter	Specifications
CPU	One 64-bit 24 core CPU
System disk drives	Two 512 GB M.2 NVMe
Memory	512 GB (8 x 64 GB DIMMs)
Interface connections	• One integrated 10 GigE Ethernet port ^a • One integrated 1 GigE IPMI port • One standard dual-port 100 GigE Ethernet card • (Optional) Four-port SAS card ^b

Gen3 H Series 3300 & 3310 BlackPearl NAS

Parameter	Specifications
CPU	One 64-bit 8 core CPU (base) One 64-bit 24 core CPU (upgrade)
System disk drives	Two 512 GB M.2 NVMe
Memory	256 GB (4 x 64 GB DIMMs) 512 GB (8 x 64 GB DIMMs)
Interface connections	• One integrated 1 GigE Ethernet port ^c • One integrated 1 GigE IPMI port • One standard dual-port 25 GigE or 100 GigE Ethernet card • (Optional) Four-port SAS card ^d

^a) Dedicated to the BlackPearl user interface for management.

^b) Each SAS card is used to connect the BlackPearl master node to disk expansion nodes.

^c) Dedicated to the BlackPearl user interface for management.

^d) Each SAS card is used to connect the BlackPearl master node to disk expansion nodes.

Gen2 X Series BlackPearl NAS

Parameter	Specifications
CPU	One 64-core CPU
System disk drives	Two 480 GB NVMe
Memory	512 GB (8 x 64 GB DIMMs)
Interface connections	• One integrated 1 GigE Ethernet ports ^a • One standard two-port 100 GigE Ethernet card • (Optional) Four-port SAS card ^b

Gen2 V Series BlackPearl NAS

Parameter	Specifications
CPU	One 16-core CPU
System disk drives	Two 480 GB M.2 SSD
Memory	256 GB (4 x 64 GB DIMMs)
Interface connections	• Two integrated 10GBase-T Ethernet ports ^c • (Optional) Dual-port 100 Gigabit Ethernet NIC • (Optional) Four-port SAS card ^b

a) Dedicated to the BlackPearl user interface for management.

b) Each SAS card is used to connect the BlackPearl master node to disk expansion nodes.

c) One port is available for data transfers, one port is dedicated to the BlackPearl user interface for management.

Gen2 S Series BlackPearl NAS

Parameter	Specifications
CPU	One 32-core CPU
System disk drives	Two 480 GB M.2 SSD
Memory	128 GB (8 x 16 GB DIMMs)
Interface connections	• Two integrated 10GBase-T Ethernet ports ^a • (Optional) Dual-port 100 Gigabit Ethernet NIC • (Optional) four-port SAS card ^b

Gen1 V Series BlackPearl 2U

Parameter	Specifications
CPU	One multi-core processor
System disk drives	Two 500 GB SATA disk drives
Memory	32 GB (4 x 8 GB DIMMs) 64 GB (8 x 8 GB DIMMs or 4 x 16 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 • (Optional) two-port SAS card ^b

^a) One port is available for data transfers, one port is dedicated to the BlackPearl user interface for management.

^b) Each SAS card is used to connect the BlackPearl master node to disk expansion nodes.

Gen1 S Series BlackPearl 4U

Parameter	Specifications
CPU	Two multi-core processors
System disk drives	Two 500 GB SATA disk drives
Memory	64 GB (8 x 8 GB DIMMs) 128 GB (16 x 8 GB DIMMs or 8 x 16 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 ^b

^a) One port is available for data transfers, one port is dedicated to the BlackPearl user interface for management.

^b) Each SAS card is used to connect the BlackPearl master node to disk expansion nodes.

SIZE AND WEIGHT

The following tables provide the size and weight of each chassis. Specifications are provided for each unit in both an operational environment, and in the shipping container.

Gen3 F Series BlackPearl NAS

Parameter	Gen3 F Series BlackPearl NAS	Shipping Container ^a
Dimensions - Height (4U) - Width - Depth	3.5 in. (8.9 cm) 19 in. (48.3 cm) 30 in. (76.2 cm)	12 in. (30.5 cm) 25 in. (73.6 cm) 37 in. (94 cm)
Weight - Chassis without drives - Each NVMe drive	55 lb (25 kg) 0.5 lb (0.23 kg)	77 lb (35 kg)

Gen3 H 3310 Series BlackPearl

Parameter	Gen3 H 3310 Series BlackPearl	Shipping Container ^b
Dimensions - Height (4U) - Width - Depth	7 in. (17.8 cm) 19 in. (48.3 cm) 29 in. (73.7 cm) ^c	18 in. (45.7 cm) 25 in. (73.6 cm) 39 in. (99 cm)
Weight - Chassis without drives - Each NVMe drive	72 lb (33 kg) - single node 89 lb (40 kg) - dual node 0.5 lb (0.23 kg)	

^a) Includes chassis, drives, box, and packaging.

^b) Includes chassis, drives, box, and packaging.

^c) Includes the front bezel.

Gen3 H 3300 Series BlackPearl NAS

Parameter	Gen3 H 3300 Series BlackPearl NAS	Shipping Container ^a
Dimensions • Height (4U) • Width • Depth	7 in. (17.8 cm) 19 in. (48.3 cm) 29 in. (73.7 cm) ^b	18 in. (45.7 cm) 25 in. (73.6 cm) 39 in. (99 cm)
Weight • Chassis without drives • Each SAS drive	75 lb (34 kg) 1.5 lb (0.67 kg)	114 lb (51.8 kg)

Gen2 X Series BlackPearl NAS

Parameter	Gen2 X Series BlackPearl NAS	Shipping Container ^c
Dimensions • Height (2U) • Width • Depth	3.5 in. (8.9 cm) 19 in. (48.3 cm) 29 in. (73.7 cm) ^d	
Maximum Weight Including rail kit ^e	60 lb (27.2 kg)	

Gen2 V Series BlackPearl NAS

Parameter	Gen2 V Series BlackPearl NAS	Shipping Container ^a
Dimensions • Height (2U)	3.5 in. (8.9 cm)	11.5 in. (29.2 cm)

a) Includes chassis, drives, box, and packaging.

b) Includes the front bezel.

c) Includes chassis, drives, box, and packaging.

d) Includes the front bezel.

e) Weights are approximate.

Parameter	Gen2 V Series BlackPearl NAS	Shipping Container ^a
• Width • Depth	19 in. (48.3 cm) 33 in. (83.8 cm) ^b	23.7 in. (60.2 cm) 45 in. (114.3 cm)
Weight ^c • Empty chassis • Additional for each HDD • Additional for each SSD	72 lb (32.7 kg) 1.8 lb (0.8 kg) 0.8 lb (0.4 kg)	

Gen2 S Series BlackPearl NAS

Parameter	Gen2 S Series BlackPearl NAS	Shipping Container ^a
Dimensions • Height (2U) • Width • Depth	7 in. (17.8 cm) 19 in. (48.3 cm) 37.5 in. (95.3 cm) ^b	15.9 in. (40.4 cm) 23.7 in. (60.2 cm) 46.9 in. (119.1 cm)
Weight ^c • Empty chassis • Additional for each HDD • Additional for each SSD	99 lb (44.9 kg) 1.8 lb (0.8 kg) 0.8 lb (0.4 kg)	

Gen1 V Series 2U BlackPearl NAS

Parameter	Gen1 V Series 2U BlackPearl NAS	Shipping Container ^a
Dimensions • Height (2U) • Width	3.5 in. (8.9 cm) 19 in. (48.3 cm)	13.25 in. (33.7 cm) 26 in. (66.0 cm)

a) Includes chassis, drives, box, and packaging.

b) Includes the front bezel.

c) Weights are approximate.

Parameter	Gen1 V Series 2U BlackPearl NAS	Shipping Container ^a
• Depth	27.5 in. (69.9 cm) ^b	34.25 in. (87.0 cm)
Weight ^c		
• Empty chassis	37.2 lb (16.9 kg)	N/A
• Empty chassis with:		
• 4 HDDs & 2 SSDs	46.7 lb (21.2 kg)	67.7 lb (30.7 kg)
• 9 HDDs & 2 SSDs	55.7 lb (25.3 kg)	76.7 lb (34.8 kg)

Gen1 S Series 4U BlackPearl NAS and 44-Bay Expansion Node

Parameter	Gen1 S Series 4U BlackPearl NAS and 44-Bay Expansion Node	Shipping Container ^a
Dimensions		
• Height (4U)	7 in. (17.8 cm)	17.5 in. (44.5 cm)
• Width	19 in. (48.3 cm)	27 in. (68.6 cm)
• Depth	29.5 in. (74.9 cm) ^b	39 in. (99.0 cm)
Weight ^c		
• Empty chassis	57 lb (25.8 kg)	91.3 lb (41.4 kg)
• Additional for each HDD	1.8 lb (0.8 kg)	1.8 lb (0.8 kg)
• Additional for each SSD	0.8 lb (0.4 kg)	0.8 lb (0.4 kg)

77-Bay Expansion Node

Parameter	77-bay Expansion Node	Shipping Container
Dimensions		
• Height (4U)	7 in. (17.8 cm)	21.1 in. (53.6 cm)
• Width	19 in. (48.3 cm)	26.6 in. (67.6 cm)
• Depth	32 in. (81 cm) ^b	44.1 in. (112 cm)

a) Includes chassis, drives, box, and packaging.

b) Includes the front bezel.

c) Weights are approximate.

Parameter	77-bay Expansion Node	Shipping Container
	38.5 in. (97.8 cm) ^a	
Weight ^b • Empty chassis • Additional for each HDD • Additional for each SSD • Additional for rack mounting kit • Fully loaded chassis with rack mounting kit	1.5 lb (0.67 kg) 0.8 lb (0.36 kg) 21 lb (9.5 kg)	127 lb (57.8 kg) 242 lb (110 kg) ^c

96-Bay Expansion Node

Parameter	96-bay Expansion Node	Shipping Container
Dimensions • Height (4U) • Width • Depth	7 in. (17.8 cm) 19 in. (48.3 cm) 40 in. (101.6 cm) ^b	14 in. (35.6 cm) 24.5 in. (62.2 cm) 43.5 in. (110.5 cm)
Weight ^c • Empty chassis • Additional for each HDD • Additional for rack mounting kit • Fully loaded chassis	76 lb (34.5 kg) 1.8 lb (0.8 kg) 21 lb (9.5 kg) 270 lb (122.5 kg)	108 lb (49 kg) ^d 1.8 lb (0.8 kg) 21 lb (9.5 kg) 302 lb (137 kg)

^a) Includes optional cable management arm.

^b) Weights are approximate.

^c) Includes chassis and packaging.

^d) Includes chassis and packaging.

107-Bay Expansion Node

Parameter	107-bay Expansion Node	Shipping Container
Dimensions • Height (4U) • Width • Depth	7 in. (17.8 cm) 19 in. (48.3 cm) 41 in. (104.1 cm) ^a 47.5 in. (120.6 cm) ^b	18.4 in. (46.7 cm) 24.3 in. (61.7 cm) 52.3 in. (132.8 cm)
Weight ^c • Empty chassis • Additional for each disk drive • Additional for rack mounting kit • Fully loaded chassis with rack mounting kit	88.5 lb (40.1 kg) 1.5 lb (0.67 kg) 21 lb (9.5 kg) 270 lb (122.5 kg)	180 lb (81.6 kg) 336 lb (152.4 kg) ^d

^a) Includes the front bezel.

^b) Includes optional cable management arm.

^c) Weights are approximate.

^d) Includes chassis and packaging.

ENVIRONMENTAL SPECIFICATIONS

Temperature & Humidity

The tables below show the temperature, humidity, and altitude requirements for each chassis.

Gen3 F Series BlackPearl NAS

Parameter	Operating Environment ^a	Storing and Shipping (Non-Operating) Environment ^b	Transit Conditions Storage Environment
Humidity		5% to 95% (non-condensing)	10% to 90% (non-condensing)
Temperature	32° F to 86° F ^c (0° C to 30° C)	–4° F to 158° F (–20° C to 70° C)	–40° F to 140° F (–40° C to 60° C)
Altitude	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 40,000 ft (-61 m to 12,192 m)
Maximum wet bulb temperature			

a) When moving the BlackPearl NAS or 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 BlackPearl NAS or expansion node in its original packaging. The packaging protects the BlackPearl NAS from condensation caused by extreme temperature variations (27° F per hour or 15° C per hour, or more).

c) Maximum operating temperature is specified at sea level and is 2 percent lower per 1,000 ft (305 m) of increased altitude.

Gen3 H Series 3300 & 3310 BlackPearl NAS

Parameter	Operating Environment ^a	Storing and Shipping (Non-Operating) Environment ^b	Transit Conditions Storage Environment
Humidity		5% to 95% (non-condensing)	10% to 90% (non-condensing)
Temperature	32° F to 95° F ^c (0° C to 35° C)	−4° F to 158° F (−20° C to 70° C)	−40° F to 140° F (−40° C to 60° C)
Altitude	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 40,000 ft (-61 m to 12,192 m)
Maximum wet bulb temperature			

Gen2 X Series BlackPearl NAS

Parameter	Operating Environment ^a	Storing and Shipping (Non-Operating) Environment ^b	Transit Conditions Storage Environment
Humidity	20% to 80% (non-condensing)	10% to 90% (non-condensing)	10% to 90% (non-condensing)
Temperature	41° F to 95° F ^c (5° C to 35° C)	−40° F to 113° F (−40° C to 45° C)	−40° F to 140° F (−40° C to 60° C)
Altitude	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 40,000 ft (-61 m to 12,192 m)
Maximum wet bulb temperature	84° F (29° C)	95° F (35° C)	

a) When moving the BlackPearl NAS or 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 BlackPearl NAS or expansion node in its original packaging. The packaging protects the BlackPearl NAS from condensation caused by extreme temperature variations (27° F per hour or 15° C per hour, or more).

c) Maximum operating temperature is specified at sea level and is 2 percent lower per 1,000 ft (305 m) of increased altitude.

Gen2 S Series and Gen2 V Series BlackPearl NAS

Parameter	Operating Environment ^a	Storing and Shipping (Non-Operating) Environment ^b
Humidity	5% to 95% (non-condensing)	5% to 95% (non-condensing)
Temperature	50° F to 95° F (10° C to 35° C)	32° F to 122° F (0° C to 50° C)
Altitude	-200 ft to 10,000 ft (-61 m to 3,048 m)	-200 ft to 10,000 ft (-61 m to 3,048 m)
Maximum wet bulb temperature	84° F (29° C)	95° F (35° C)

Gen1 S Series and Gen1 V Series BlackPearl NAS

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 ft (3,048 m)	Sea level to 39,370 ft (12,000 m)
Maximum wet bulb temperature	84° F (29° C)	95° F (35° C)

a) When moving the BlackPearl NAS or 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 BlackPearl NAS or expansion node in its original packaging. The packaging protects the BlackPearl NAS from condensation caused by extreme temperature variations (27° F per hour or 15° C per hour, or more).

44-Bay 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 ft (3,048 m)	Sea level to 39,370 ft (12,000 m)
Maximum wet bulb temperature	84° F (29° C)	95° F (35° C)

77-Bay 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 ft to 10,000 ft (–61 m to 3,048 m)	–200 ft to 40,000 ft (–61 m to 12,192 m)

a) When moving the BlackPearl NAS or 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 BlackPearl NAS or expansion node in its original packaging. The packaging protects the BlackPearl NAS from condensation caused by extreme temperature variations (27° F per hour or 15° C per hour, or more).

96-Bay 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 ft to 10,000 ft (–61 m to 3,048 m)	–200 ft to 40,000 ft (–61 m to 12,192 m)

107-Bay 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 ft to 10,000 ft (–61 m to 3,048 m)	–200 ft to 40,000 ft (–61 m to 12,192 m)

a) When moving the 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 expansion node is in its original packaging. The packaging is designed to protect the 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 approximate heat generation of each BlackPearl chassis.

Chassis	Heat Generation at Maximum Wattage
Gen3 F Series 2U master node	3412-5459 BTUs/hour
Gen3 H Series 4U master node	2729 - 4092 BTUs/hour
Gen2 X Series 2U master node	5460 BTUs/hour
Gen2 V Series 2U master node	2729 BTUs/hour
Gen2 S Series 4U master node	5460 BTUs/hour
Gen1 V Series 2U master node	3138 BTUs/hour
Gen1 S or P Series 4U master node	3410 - 4365 BTUs/hour
44-bay expansion node	3751 - 4775 BTUs/hour
77-bay expansion node	3950 BTUs/hour
96-bay expansion node	3751 BTUs/hour
107-bay expansion node	6820 BTUs/hour

POWER REQUIREMENTS

The BlackPearl NASs, 44-bay, 77-bay, 96-bay, and 107-bay expansion nodes, have the following power requirements.



CAUTION

Failure to meet the cabling and power specifications could damage your BlackPearl NAS, result in data loss, or both.

Input Power Requirements

The following tables provide the input power requirements for each or expansion node.

Gen3 F Series BlackPearl NAS

Parameter	Requirements
Input Voltage	100-120 VAC, 13 A, 1000 watts maximum 200-240 VAC, 10 A, 1600 watts maximum

Parameter	Requirements
Input Frequency	50–60 Hz

Gen3 H Series 3300 and 3310 BlackPearl NAS

Parameter	Requirements
Input Voltage	100-127 VAC, 10 A, 800 watts maximum 200–240 VAC, 8 A, 1200 watts maximum
Input Frequency	50–60 Hz

Gen2 X Series BlackPearl NAS

Parameter	Requirements
Input Voltage	200–240 VAC, 7 A, 1600 watts maximum
Input Frequency	50–60 Hz

Gen2 V Series BlackPearl NAS

Parameter	Requirements
Input Voltage	100-240 VAC, 8-4 A, 800 watts maximum
Input Frequency	50–60 Hz

Gen2 S Series BlackPearl NAS

Parameter	Requirements
Input Voltage	200–240 VAC, 10 A, 1600 watts maximum
Input Frequency	50–60 Hz

Gen1 V Series 2U BlackPearl NAS

Parameter	Requirements
Input Voltage	100–240 VAC, 11–4.5 A, 920 watts maximum
Input Frequency	50–60 Hz

Gen1 S Series 4U BlackPearl NAS

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

44-Bay 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

77-Bay Expansion Node

Parameter	Requirements
Input Voltage	200–240 VAC, 12 A, 1600 watts maximum
Input Frequency	50–60 Hz

96-Bay Expansion Node

Parameter	Requirements
Input Voltage	90–264 VAC, 1100 watts maximum
Input Frequency	47–63 Hz

107-Bay Expansion Node

Parameter	Requirements
Input Voltage	200–240 VAC, 15 A, 2000 watts maximum
Input Frequency	50–60 Hz

Power Cord Specifications

The power cords included with the BlackPearl NASs are part of the unit and are not intended for use with any other equipment.

**IMPORTANT**

Confirm the PDU used with the BlackPearl NAS 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.

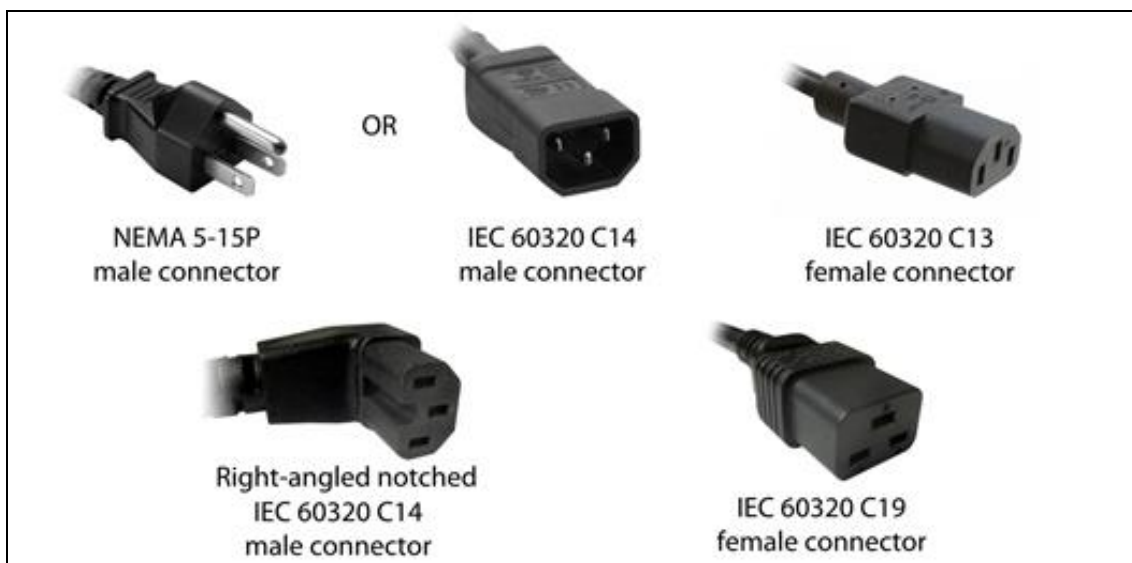
Power cords must comply with local electrical codes.

**WARNING**

Using extension cords in conjunction with the cords provided with a 77-bay expansion node, a 96-bay expansion node, or 107-bay expansion node, may cause serious damage.

WARNUNG Die Verwendung von Verlängerungskabeln in Verbindung mit den Kabeln, die mit einem 77-Schacht-Erweiterungsknoten, 96-Schacht-Erweiterungsknoten, oder 107-Schacht-Erweiterungsknoten geliefert werden, kann schwere Schäden verursachen.

Note: 96-bay expansion nodes ship with cables for use with the chassis. These power cables have a right-angled notched C14 connector, which is required for the 96-bay expansion node. Only use the cords provided by Spectra Logic with the 96-bay expansion node.



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	Gen1 S, P and V Series, Gen2 X and V Series, Gen 3 H Series, and 44-Bay Expansion Node: • 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	Gen1 S, P, and V Series, Gen2 X, S, and V Series, Gen 3 H Series, Gen 3 F Series, and 44-Bay Expansion Node: • Male: NEMA 5-15P or IEC-60320 C14 • Female: IEC 60320 C13 77-Bay Chassis Expansion Node: • Male: Connector must be of the proper type, rating, and safety approval. • Female: IEC 60320 C19 96-Bay Expansion Node: • Male: Connector must be of the proper type, rating, and safety approval. • Female: Right-angled notched IEC 60320 C14 107-Bay 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	Gen1 S, P, and V Series, Gen2 X, S, and V Series, Gen 3 H Series, Gen 3 F Series, and 44-Bay Expansion Node: • Male: Connector must be of the proper type, rating, and safety approval. • Female: IEC 60320 C13 77-Bay Chassis Expansion Node: • Male: Connector must be of the proper type, rating, and safety approval. • Female: IEC 60320 C19 96-Bay Expansion Node: • Male: Connector must be of the proper type, rating, and safety approval. • Female: Right-angled notched IEC 60320 C14 107-Bay Chassis Expansion Node: • Male: Connector must be of the proper type, rating, and safety approval. • Female: IEC 60320 C19

Power Connection Best Practice

For greater power redundancy, connect each of the two power cords to separate circuits.

INTERFACE SPECIFICATIONS

This section provides information about the interfaces used to connect a BlackPearl NAS to expansion nodes and host systems.

System Interface Connectors

Gen3 F Series BlackPearl NAS

Interface Type	Number of Ports and Connector Type
Ethernet • 25 and 100 GigE	Two QSFP28 sockets.
IPMI Management Port	One RJ-45 socket.
SAS (12 Gbps) (Optional)	Four SFF-8644 sockets per 12 Gbps SAS card provide connections to four 77-bay, 96-bay, or 107-bay disk expansion nodes, using one port per expansion node.

Gen3 H Series 3300 & 3310 BlackPearl NAS

Interface Type	Number of Ports and Connector Type
Ethernet • 1 GigE • 25 and 100 GigE	Two RJ-45 sockets. Two QSFP28 sockets.
IPMI Management Port	One RJ-45 socket.
SAS (12 Gbps) (Optional)	Four SFF-8644 sockets per 12 Gbps SAS card provide connections to four 77-bay, 96-bay, or 107-bay disk expansion nodes, using one port per expansion node.

Gen2 X Series BlackPearl NAS

Interface Type	Number of Ports and Connector Type
Ethernet • 1 Gig E • 100 GigE	One RJ-45 socket Two QSFP28 sockets.
SAS (12 Gbps) (Optional)	Four SFF-8644 sockets per 12 Gbps SAS card provide connections to four 77-bay, 96-bay, or 107-bay disk expansion nodes, using one port per expansion node.

Gen2 S Series and V Series BlackPearl NAS

Interface Type	Number of Ports and Connector Type
Ethernet 1 Gigabit (Gen2 V series only)	Two RJ-45 sockets.
Ethernet 10GBase-T (Gen2 S series only)	Two RJ-45 sockets.
IPMI Management Port	One RJ-45 socket.
Ethernet 10GBase-T (Optional)	Two RJ-45 sockets.
Ethernet (100 GigE) (Optional)	Two SFP28 optical modules with a duplex LC connector per optional 100 GigE NIC.
SAS (12 Gbps) (Optional)	Four SFF-8644 sockets per 12 Gbps SAS card provide connections to four 77-bay, 96-bay, or 107-bay disk expansion nodes, using one port per expansion node.

Gen1 S Series and Gen1 V Series BlackPearl NAS

Interface Type	Number of Ports and Connector Type
Ethernet (1000BaseT, 10GBase-T)	Two RJ-45 sockets.
IPMI Management Port	One RJ-45 socket
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) (Optional)	Four SFF-8644 sockets per optional 6 Gbps SAS card provide connections to two 44-bay expansion nodes, using two ports for each expansion node.
SAS (12 Gbps) (Optional)	Two or four SFF-8644 sockets per optional 12 Gbps SAS card provide connections to two or four 77-bay, 96-bay, or 107-bay disk expansion nodes, using one port per expansion node.

Expansion Node Interface Connectors

Interface Type	Number of Ports and Connector Type
44-Bay Expansion Node	Two SFF-8088 ports per 44-bay expansion node. Both ports are required to connect the expansion node to a BlackPearl NAS.
77-Bay Expansion Node	- Four SFF-8644 ports per expander in the 77-bay expansion node. Maximum of two expanders. - One 1 GigE Ethernet port per expander in the 77-bay expansion node. Maximum of two expanders.
96-Bay Expansion Node	Two SFF-8644 ports per 96-bay expansion node. Only a single port is required to connect the expansion node to a BlackPearl NAS.
107-Bay Expansion Node	- Four SFF-8644 ports per expander in the 107-bay expansion node. Maximum of two expanders. - One 1 GigE Ethernet port per expander in the 107-bay expansion node. Maximum of two expanders.

Network Interface Cables

The type of cables required to connect the BlackPearl NAS to an Ethernet network, a 44-bay, 77-bay, 96-bay, or 107-bay 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 an RJ-45 connector. 10/100/1000Base-T - Shielded Category 5 data-grade cable with an RJ-45 connector. Note: Cables to be provided by the customer.
Ethernet (10 GigE)	SFP+ transceiver multimode optical cable with duplex LC connectors. Note: Cables to be provided by the customer.
Ethernet (25 GigE)	SFP28 transceiver multimode optical cable with duplex LC connectors. Note: Cables to be provided by the customer.
Ethernet (40 GigE)	QSFP+ transceiver MPT optical cables with duplex LC connectors, or copper cables with QSFP+ connector. Note: Cables to be provided by the customer.
Ethernet (100 GigE)	100 GbE QSFP28 cable. Note: Cables to be provided by the customer.
SAS	44-bay expansion node: 6 Gbps 4 lane cable with SFF-8644 and SFF-8088 connectors. Two SAS cables are required for each 44-bay expansion node. Note: Two SAS cables are included with each 44-bay expansion node. 77-bay expansion node: 12 Gbps cable with SFF-8644 connectors. One SAS cable is required for each 77-bay expansion node. 96-bay expansion node: 12 Gbps cable with SFF-8644 connectors. One SAS cable is required for each 96-bay expansion node. 107-bay expansion node: 12 Gbps cable with SFF-8644 connectors. One SAS cable is required for each 107-bay expansion node. Note: One SAS cable is included with each 96-bay expansion node or 107-bay expansion node.

Networking Naming Conventions

SFP naming (LC fiber)

- 1G is SFP
- 10G is SFP+
- 25G is SFP28

QSFP naming (MPO/MTP fiber)

- 40G is QSFP+ (4 lanes)
- 50G is QSFP28 (2 lanes)
- 100G is QSFP28 (4 lanes)

Universal Serial Bus (USB) Support

Spectra Logic supports using the USB ports on the 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

APPENDIX C - REGULATORY & SAFETY STANDARDS

The Spectra BlackPearl NAS complies with the safety and regulatory agency standards listed below when installed by a Spectra Logic certified engineer or third-party provider.

EU DECLARATION OF CONFORMITY



SPECTRA

Document # 9910000x V1.0

DECLARATION OF CONFORMITY

According to ISO/IEC 17050-1:2004



Manufacturer's Name: Spectra Logic Corporation

Manufacturer's Address: 6101 Lookout Road, Boulder CO,80301

Declares under sole responsibility that the product as delivered

Product Name: Black Pearl Converge

Model Number: BP-4U AIC, BP-2U AIC, JBOD 78, JBOD 108

Product options: This declaration covers all options of the above product(s)

Complies with the essentials of the following European Directives, and carries the CE marking accordingly:

Safety

Directive: 2014/35/EU

IEC 62368-1:2014 (First Edition)

IEC 62368-1:2017 (Second edition)

EN 60950-1:2006 +A11:2009 +A1:2010 +A12:2011 +A2:2013

EN 62479:2010

Electromagnetic Compatibility

Directive 2014/30/EU

EN55032: 2012, Class A

EN55032: 2015+A11:2020

EN 61000 3-2:2014

EN 61000 3-3:2013

Restriction of the use of certain hazardous substances

IEC 63000 / EN 50581-2012

EN 62321

(EC)1907/2006 REACH

2011/65/EU RoHS

2012/19/EU WEEE



Mike Beaty
Sr. Director Operations
September 26, 2023

6101 Lookout Road
Boulder, CO 80301

www.SpectraLogic.com
+1 303-449-6400 Worldwide
+1 800-833-1132 US/Canada

Directive	Compliance
EU EMC Directive 89/336/EEC	Essential health and safety requirements relating to electromagnetic compatibility.
EN 55022 (CISPR 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
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 voltage limits.
EN 60950-1 (EN 60950-1)	Safety requirements of information technology equipment including electrical machines.

Certifications

Country	Certification	Covers ^a
Australia	RCM	826-9, 847-12, 847JBOD-14, SP-5, JBOD 108
Canada	UL	826-9, 847-12, 847JBOD-14, SP-5, JBOD 108
EU	CE	826-9, 847-12, 847JBOD-14, SP-5, JBOD 108
Mexico	NOM	826-9, 847-12, 847JBOD-14, SP-5, JBOD 108
USA	UL, FCC	826-9, 847-12, 847JBOD-14, SP-5, JBOD 108
Japan	VCCI	826-9, 847-12, 847JBOD-14, SP-5, JBOD 108

The BlackPearl NAS 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.

a) The BlackPearl 4U System is regulatory model number "826-9", The BlackPearl 2U System is regulatory model number "847-12". The 44-Bay Expansion Node is regulatory model number "847JBOD-14", The 96-Bay Expansion Node is regulatory model number "BSP-5". The 107-Bay Expansion Node is regulatory model number "JBOD 108"

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 BlackPearl NAS on uninterpretable 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.

CLASS A EMISSIONS WARNING

Type of Equipment	User's Guide
A급 기기 (업무용 방송통신기자재)	이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.
Class A Equipment (Industrial Broadcasting & Communication Equipment)	This equipment is Industrial (Class A) electromagnetic wave suitability equipment and seller or user should take notice of it, and this equipment is to be used in the places except for home.

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

LASER WARNING

Optical Transceivers

A Class 1 laser assembly, in the optical transceiver, is mounted on each Fibre Channel or Ethernet electronics card. This laser assembly is registered with the DHHS and is in compliance with IEC825. These products contain components that comply with performance standards that are set by the U.S. Food and Drug administration. This means that these products belong to a class of laser products that do not emit hazardous laser radiation. This classification was accomplished by providing the necessary protective housings and scanning safeguards to ensure that laser radiation is inaccessible during operation or is within Class 1 limits. External safety agencies have reviewed these products and have obtained approvals to the latest standards as they apply to this product type.

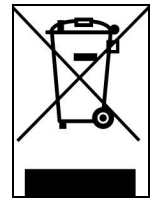
SAFETY STANDARDS AND COMPLIANCE

The Spectra BlackPearl NAS complies 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.



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 Spectra Logic for more information.

RECYCLING YOUR SYSTEM

For information on recycling your Spectra, check the Spectra Logic website at: spectralogic.com/environment.

APPENDIX D - OPEN SOURCE CODE ACKNOWLEDGMENTS & PACKAGE LIST

Copyright © 2010 - 2026 Spectra Logic Corporation. All rights reserved.

This appendix contains the licenses and notices for open source software used in the BlackPearl NAS. 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 © 1992-2026 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 Java™ 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 Java™ 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) 2002-2026 Igor Sysoev

Copyright (C) 2011-2026 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 BSD (see the file BSD), 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.
 - a. give non-standard binaries non-standard names, with instructions on where to get the original software distribution.
 - b. 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 2.1

INCLUDED PACKAGES

Judy-1.0.5_3
alsa-lib-1.2.2_1
apache-commons-daemon-1.2.4
apr-1.7.0.1.6.1_2
atf-0.21
avahi-app-0.8
awscli-1.20.61
bash-5.1.16
black_pearl-3.0_4
bluestorm_backend-2.0.3206514_7
bluestorm_frontend-2.1.3207762
bluestorm_gui-2.0.3207767_6
bluestorm_mgmt-2.0.3207724
bluestorm_tests-2.0.2886232_1
bluestorm_workers-2.0.3199353_7
boost-libs-1.72.0_7
brotli-1.0.9,1
c-ares-1.18.1
ca_root_nss-3.77
cdbcmd-0.0.3150262,1
compat10x-amd64-10.4.1004000.20181014
compat11x-amd64-11.2.1102000.20181014
ctags-5.8
curl-8.1.2
cyrus-sasl-2.1.28
dbus-1.12.20_5
dbus-glib-0.112
dejavu-2.37_1
dfu-util-0.11_1

dmidecode-3.3
ds3-3.2.0.1701306
e2fsprogs-libuuid-1.46.5
encodings-1.0.5,1
expat-2.5.0
expect-5.45.4_3,1
fieldmod-2.0.0.2867631
fio-3.30
font-bh-ttf-1.0.3_4
font-misc-ethiopic-1.0.4
font-misc-meltho-1.0.3_4
fontconfig-2.13.94_2,1
freetype2-2.12.0
fsx-1.0.2959490_1
fusefs-libs-2.9.9_2
gamin-0.1.10_10
gdb-11.2
gdbm-1.23
gettext-runtime-0.21
giflib-5.2.1
glib-2.70.4_5,2
gmp-6.2.1
gnome_subr-1.0
gnupg-2.3.3_3
gnutls-3.7.9
goserver-0.0.1.3208413_4
graphite2-1.3.14
harfbuzz-4.2.0
icu-71.1,1
indexinfo-0.3.1
intel-ipsec-mb-1.1

iozone-3.491
iperf-2.1.7
iperf3-3.11
ipmitool-1.8.18_3
jansson-2.14
javavmwrapper-2.7.9
jbigkit-2.1_1
jpeg-turbo-2.1.3
jq-1.6
ksh93-93.u_1,2
kyua-0.13_6,3
lcms2-2.12
libICE-1.0.10,1
libSM-1.2.3,1
libX11-1.8.6,1
libXau-1.0.9
libXdmcp-1.1.3
libXext-1.3.4,1
libXfixes-6.0.0
libXi-1.8,1
libXrandr-1.5.2
libXrender-0.9.10_2
libXt-1.2.1,1
libXtst-1.2.3_2
libarchive-3.6.0,1
libassuan-2.5.5
libcyaml-1.3.1
libdaemon-0.14_1
libedit-3.1.20210910,1
libevent-2.1.12
libffi-3.4.2

libfontenc-1.1.4
libgcrypt-1.9.4
libgpg-error-1.45
libiconv-1.16
libidn2-2.3.2
libinotify-20211018
libksba-1.6.0
liblz4-1.9.3,1
libnghttp2-1.46.0
libpsl-0.21.1_4
libpthread-stubs-0.4
libqrencode-4.1.1
libsmi-0.4.8_1
libssh2-1.10.0,3
libsunacl-1.0.1
libtasn1-4.18.0
libunistring-1.0
libunwind-20211201
libuv-1.42.0
libxcb-1.14_1
libxml2-2.9.13_2
libxslt-1.1.35_3
libyaml-0.2.5
llvm14-14.0.1
lnav-0.10.1
logrotate-3.13.0_1
lua52-5.2.4
lua53-5.3.6
lutok-0.4_7
mbuffer-20211018
mhash-0.9.9.9_5

mkfontscale-1.2.1
monit-5.32.0
mpdecimal-2.5.1
mpfr-4.1.0_1
mtx-1.3.12_1
ncurses-6.3
net-snmp-5.9_3,1
netperf-2.7.1.p20170921_1
nettle-3.7.3
nginx-1.24.0_10,3
node16-16.20.1
npth-1.6
oniguruma-6.9.7.1
openjdk17-17.0.2+8.1
openldap24-client-2.4.59_4
p4-2016.1.1492381_3
pam_google_authenticator-1.09,1
pcre-8.45_1
pcre2-10.39_1
pdksh-5.2.14p2_6
perl5-5.32.1_1
pg_cron-1.6.4
pgbadger-11.8
pinentry-1.2.0
pinentry-curses-1.2.0
pkg-1.17.5_1
png-1.6.37_1
popt-1.18_1
postgresql14-client-14.8
postgresql14-contrib-14.8
postgresql14-server-14.8_1

py38-boost-libs-1.72.0_1
py38-boto3-1.18.61
py38-botocore-1.21.61
py38-certifi-2021.10.8
py38-cffi-1.15.0
py38-charset-normalizer-2.0.12
py38-colorama-0.4.4
py38-cryptography-3.3.2
py38-dateutil-2.8.2
py38-docutils-0.17.1,1
py38-idna-3.3
py38-jmespath-0.10.0
py38-openssl-20.0.1,1
py38-passlib-1.7.4
py38-pyasn1-0.4.8
py38-pycparser-2.21
py38-pysocks-1.7.1
py38-requests-2.27.1
py38-rsa-4.8
py38-s3transfer-0.5.0
py38-setuptools-57.0.0
py38-six-1.16.0
py38-urllib3-1.26.9,1
py38-yaml-5.4.1
python-3.8_3,2
python3-3_3
python38-3.8.17
readline-8.1.2
redis-7.0.12
rrdtool-1.7.2_6
ruby-3.0.5,1

ruby30-gems-3.3.11
rubygem-actioncable61-6.1.6
rubygem-actionmailbox61-6.1.6
rubygem-actionmailer61-6.1.6
rubygem-actionpack61-6.1.6
rubygem-actiontext61-6.1.6
rubygem-actionview61-6.1.6
rubygem-activejob61-6.1.6
rubygem-activemodel-serializers-xml-1.0.2_2
rubygem-activemodel61-6.1.6
rubygem-activerecord-import-1.4.0_2
rubygem-activerecord61-6.1.6
rubygem-activeresource-6.0.0_1
rubygem-activestorage61-6.1.6
rubygem-activesupport61-6.1.6
rubygem-addressable-2.8.0
rubygem-aws-eventstream-1.2.0
rubygem-aws-partitions-1.577.0
rubygem-aws-sdk-3.1.0
rubygem-aws-sdk-accessanalyzer-1.29.0
rubygem-aws-sdk-account-1.6.0
rubygem-aws-sdk-acm-1.51.0
rubygem-aws-sdk-acmpca-1.48.0
rubygem-aws-sdk-alexaforbusiness-1.56.0
rubygem-aws-sdk-amplify-1.40.0
rubygem-aws-sdk-amplifybackend-1.17.0
rubygem-aws-sdk-amplifyuibuilder-1.5.0
rubygem-aws-sdk-apigateway-1.76.0
rubygem-aws-sdk-apigatewaymanagementapi-1.30.0
rubygem-aws-sdk-apigatewayv2-1.42.0
rubygem-aws-sdk-appconfig-1.25.0

rubygem-aws-sdk-appconfigdata-1.5.0
rubygem-aws-sdk-appflow-1.26.0
rubygem-aws-sdk-appintegrationsservice-1.13.0
rubygem-aws-sdk-applicationautoscaling-1.62.0
rubygem-aws-sdk-applicationcostprofiler-1.9.0
rubygem-aws-sdk-applicationdiscoveryservice-1.44.0
rubygem-aws-sdk-applicationinsights-1.30.0
rubygem-aws-sdk-appmesh-1.45.0
rubygem-aws-sdk-appregistry-1.15.0
rubygem-aws-sdk-apprunner-1.13.0
rubygem-aws-sdk-appstream-1.65.0
rubygem-aws-sdk-appsync-1.52.0
rubygem-aws-sdk-athena-1.53.0
rubygem-aws-sdk-auditmanager-1.23.0
rubygem-aws-sdk-augmentedairuntime-1.22.0
rubygem-aws-sdk-autoscaling-1.78.0
rubygem-aws-sdk-autoscalingplans-1.40.0
rubygem-aws-sdk-backup-1.43.0
rubygem-aws-sdk-backupgateway-1.3.0
rubygem-aws-sdk-batch-1.61.0
rubygem-aws-sdk-billingconductor-1.0.0
rubygem-aws-sdk-braket-1.18.0
rubygem-aws-sdk-budgets-1.49.0
rubygem-aws-sdk-chime-1.67.0
rubygem-aws-sdk-chimesdkidentity-1.9.0
rubygem-aws-sdk-chimesdkmeetings-1.9.0
rubygem-aws-sdk-chimesdkmessaging-1.10.0
rubygem-aws-sdk-cloud9-1.45.0
rubygem-aws-sdk-cloudcontrolapi-1.7.0
rubygem-aws-sdk-clouddirectory-1.41.0
rubygem-aws-sdk-cloudformation-1.68.0

rubygem-aws-sdk-cloudfront-1.63.0
rubygem-aws-sdk-cloudhsm-1.39.0
rubygem-aws-sdk-cloudhsmv2-1.42.0
rubygem-aws-sdk-cloudsearch-1.40.0
rubygem-aws-sdk-cloudsearchdomain-1.33.0
rubygem-aws-sdk-cloudtrail-1.48.0
rubygem-aws-sdk-cloudwatch-1.64.0
rubygem-aws-sdk-cloudwatchevents-1.57.0
rubygem-aws-sdk-cloudwatchevidently-1.5.0
rubygem-aws-sdk-cloudwatchlogs-1.52.0
rubygem-aws-sdk-cloudwatchrum-1.4.0
rubygem-aws-sdk-codeartifact-1.19.0
rubygem-aws-sdk-codebuild-1.88.0
rubygem-aws-sdk-codecommit-1.51.0
rubygem-aws-sdk-codedeploy-1.49.0
rubygem-aws-sdk-codeguruprofiler-1.24.0
rubygem-aws-sdk-codegurureviewer-1.30.0
rubygem-aws-sdk-codepipeline-1.53.0
rubygem-aws-sdk-codestar-1.38.0
rubygem-aws-sdk-codestarconnections-1.24.0
rubygem-aws-sdk-codestarnotifications-1.19.0
rubygem-aws-sdk-cognitoidentity-1.40.0
rubygem-aws-sdk-cognitoidentityprovider-1.65.0
rubygem-aws-sdk-cognitosync-1.36.0
rubygem-aws-sdk-comprehend-1.60.0
rubygem-aws-sdk-comprehendmedical-1.36.0
rubygem-aws-sdk-computeoptimizer-1.32.0
rubygem-aws-sdk-configservice-1.77.0
rubygem-aws-sdk-connect-1.68.0
rubygem-aws-sdk-connectcontactlens-1.11.0
rubygem-aws-sdk-connectparticipant-1.22.0

rubygem-aws-sdk-connectwisdomservice-1.6.0
rubygem-aws-sdk-core-3.130.1
rubygem-aws-sdk-costandusagereportservice-1.40.0
rubygem-aws-sdk-costexplorer-1.76.0
rubygem-aws-sdk-customerprofiles-1.20.0
rubygem-aws-sdk-databasemigrationservice-1.67.0
rubygem-aws-sdk-dataexchange-1.26.0
rubygem-aws-sdk-datapipeline-1.36.0
rubygem-aws-sdk-datasync-1.45.0
rubygem-aws-sdk-dax-1.39.0
rubygem-aws-sdk-detective-1.28.0
rubygem-aws-sdk-devicefarm-1.51.0
rubygem-aws-sdk-devopsguru-1.23.0
rubygem-aws-sdk-directconnect-1.54.0
rubygem-aws-sdk-directoryservice-1.49.0
rubygem-aws-sdk-dlm-1.50.0
rubygem-aws-sdk-docdb-1.42.0
rubygem-aws-sdk-drs-1.4.0
rubygem-aws-sdk-dynamodb-1.74.0
rubygem-aws-sdk-dynamodbstreams-1.38.0
rubygem-aws-sdk-ebs-1.26.0
rubygem-aws-sdk-ec2-1.307.0
rubygem-aws-sdk-ec2instanceconnect-1.24.0
rubygem-aws-sdk-ecr-1.56.0
rubygem-aws-sdk-ecrpublic-1.12.0
rubygem-aws-sdk-ecs-1.99.0
rubygem-aws-sdk-efs-1.54.0
rubygem-aws-sdk-eks-1.74.0
rubygem-aws-sdk-elasticache-1.76.0
rubygem-aws-sdk-elasticbeanstalk-1.51.0
rubygem-aws-sdk-elasticinference-1.21.0

rubygem-aws-sdk-elasticloadbalancing-1.40.0
rubygem-aws-sdk-elasticloadbalancingv2-1.77.0
rubygem-aws-sdk-elasticsearchservice-1.65.0
rubygem-aws-sdk-elastictranscoder-1.38.0
rubygem-aws-sdk-emr-1.59.0
rubygem-aws-sdk-emrcontainers-1.14.0
rubygem-aws-sdk-eventbridge-1.38.0
rubygem-aws-sdk-finspace-1.11.0
rubygem-aws-sdk-finspace-1.14.0
rubygem-aws-sdk-firehose-1.48.0
rubygem-aws-sdk-fis-1.13.0
rubygem-aws-sdk-fms-1.49.0
rubygem-aws-sdk-forecastqueryservice-1.21.0
rubygem-aws-sdk-forecastservice-1.33.0
rubygem-aws-sdk-frauddetector-1.32.0
rubygem-aws-sdk-fsx-1.55.0
rubygem-aws-sdk-gamelift-1.56.0
rubygem-aws-sdk-gamesparks-1.0.0
rubygem-aws-sdk-glacier-1.46.0
rubygem-aws-sdk-globalaccelerator-1.39.0
rubygem-aws-sdk-glue-1.109.0
rubygem-aws-sdk-gluedatabrew-1.22.0
rubygem-aws-sdk-greengrass-1.49.0
rubygem-aws-sdk-greengrassv2-1.17.0
rubygem-aws-sdk-groundstation-1.27.0
rubygem-aws-sdk-guardduty-1.56.0
rubygem-aws-sdk-health-1.47.0
rubygem-aws-sdk-healthlake-1.13.0
rubygem-aws-sdk-honeycode-1.17.0
rubygem-aws-sdk-iam-1.68.0
rubygem-aws-sdk-identitystore-1.15.0

rubygem-aws-sdk-imagebuilder-1.40.0
rubygem-aws-sdk-importexport-1.35.0
rubygem-aws-sdk-inspector-1.43.0
rubygem-aws-sdk-inspector2-1.4.0
rubygem-aws-sdk-iot-1.88.0
rubygem-aws-sdk-iot1clickdevicesservice-1.37.0
rubygem-aws-sdk-iot1clickprojects-1.37.0
rubygem-aws-sdk-iotanalytics-1.49.0
rubygem-aws-sdk-iotdataplane-1.39.0
rubygem-aws-sdk-iotdeviceadvisor-1.14.0
rubygem-aws-sdk-iotevents-1.33.0
rubygem-aws-sdk-ioteventsdata-1.26.0
rubygem-aws-sdk-iotfleethub-1.11.0
rubygem-aws-sdk-iotjobsdataplane-1.36.0
rubygem-aws-sdk-iotsecuretunneling-1.20.0
rubygem-aws-sdk-iotsitewise-1.40.0
rubygem-aws-sdk-iotthingsgraph-1.23.0
rubygem-aws-sdk-iottwinmaker-1.4.0
rubygem-aws-sdk-iotwireless-1.22.0
rubygem-aws-sdk-ivs-1.20.0
rubygem-aws-sdk-kafka-1.49.0
rubygem-aws-sdk-kafkaconnect-1.7.0
rubygem-aws-sdk-kendra-1.48.0
rubygem-aws-sdk-keyspaces-1.2.0
rubygem-aws-sdk-kinesis-1.41.0
rubygem-aws-sdk-kinesisanalytics-1.40.0
rubygem-aws-sdk-kinesisanalyticsv2-1.40.0
rubygem-aws-sdk-kinesisvideo-1.41.0
rubygem-aws-sdk-kinesisvideoarchivedmedia-1.43.0
rubygem-aws-sdk-kinesisvideomedia-1.37.0
rubygem-aws-sdk-kinesisvideosignalingchannels-1.19.0

rubygem-aws-sdk-kms-1.55.0
rubygem-aws-sdk-lakeformation-1.26.0
rubygem-aws-sdk-lambda-1.83.0
rubygem-aws-sdk-lambdapreview-1.35.0
rubygem-aws-sdk-lex-1.45.0
rubygem-aws-sdk-lexmodelbuildingservice-1.57.0
rubygem-aws-sdk-lexmodelsv2-1.23.0
rubygem-aws-sdk-lexruntimev2-1.15.0
rubygem-aws-sdk-licensemanager-1.40.0
rubygem-aws-sdk-lightsail-1.64.0
rubygem-aws-sdk-locationsservice-1.21.0
rubygem-aws-sdk-lookoutequipment-1.10.0
rubygem-aws-sdk-lookoutforvision-1.14.0
rubygem-aws-sdk-lookoutmetrics-1.15.0
rubygem-aws-sdk-machinelearning-1.37.0
rubygem-aws-sdk-macie-1.38.0
rubygem-aws-sdk-macie2-1.44.0
rubygem-aws-sdk-managedblockchain-1.32.0
rubygem-aws-sdk-managedgrafana-1.7.0
rubygem-aws-sdk-marketplacecatalog-1.21.0
rubygem-aws-sdk-marketplacecommerceanalytics-1.41.0
rubygem-aws-sdk-marketplaceentitlementsservice-1.35.0
rubygem-aws-sdk-marketplacemetering-1.41.0
rubygem-aws-sdk-mediaconnect-1.44.0
rubygem-aws-sdk-mediaconvert-1.88.0
rubygem-aws-sdk-medialive-1.86.0
rubygem-aws-sdk-mediapackage-1.52.0
rubygem-aws-sdk-mediapackagevod-1.36.0
rubygem-aws-sdk-mediastore-1.41.0
rubygem-aws-sdk-mediastoredata-1.38.0
rubygem-aws-sdk-mediatailor-1.54.0

rubygem-aws-sdk-memorydb-1.8.0
rubygem-aws-sdk-mgn-1.12.0
rubygem-aws-sdk-migrationhub-1.40.0
rubygem-aws-sdk-migrationhubconfig-1.20.0
rubygem-aws-sdk-migrationhubrefactorspaces-1.5.0
rubygem-aws-sdk-migrationhubstrategyrecommendations-1.4.0
rubygem-aws-sdk-mobile-1.35.0
rubygem-aws-sdk-mq-1.46.0
rubygem-aws-sdk-mturk-1.40.0
rubygem-aws-sdk-mwaa-1.15.0
rubygem-aws-sdk-neptune-1.45.0
rubygem-aws-sdk-networkfirewall-1.15.0
rubygem-aws-sdk-networkmanager-1.22.0
rubygem-aws-sdk-nimblestudio-1.13.0
rubygem-aws-sdk-opensearchservice-1.10.0
rubygem-aws-sdk-opsworks-1.41.0
rubygem-aws-sdk-opsworkscm-1.52.0
rubygem-aws-sdk-organizations-1.69.0
rubygem-aws-sdk-outposts-1.30.0
rubygem-aws-sdk-panorama-1.7.0
rubygem-aws-sdk-personalize-1.40.0
rubygem-aws-sdk-personalizeevents-1.27.0
rubygem-aws-sdk-personalizeruntime-1.32.0
rubygem-aws-sdk-pi-1.39.0
rubygem-aws-sdk-pinpoint-1.67.0
rubygem-aws-sdk-pinpointemail-1.35.0
rubygem-aws-sdk-pinpointsmsvoice-1.32.0
rubygem-aws-sdk-pinpointsmsvoicev2-1.0.0
rubygem-aws-sdk-polly-1.54.0
rubygem-aws-sdk-pricing-1.37.0
rubygem-aws-sdk-prometheusservice-1.14.0

rubygem-aws-sdk-proton-1.15.0
rubygem-aws-sdk-qlldb-1.25.0
rubygem-aws-sdk-qlddbsession-1.22.0
rubygem-aws-sdk-quicksight-1.64.0
rubygem-aws-sdk-ram-1.39.0
rubygem-aws-sdk-rds-1.143.0
rubygem-aws-sdk-rdsdataservice-1.34.0
rubygem-aws-sdk-recyclebin-1.2.0
rubygem-aws-sdk-redshift-1.80.0
rubygem-aws-sdk-redshiftdataapiservice-1.19.0
rubygem-aws-sdk-rekognition-1.66.0
rubygem-aws-sdk-resiliencehub-1.4.0
rubygem-aws-sdk-resourcegroups-1.45.0
rubygem-aws-sdk-resourcegroupstaggingapi-1.47.0
rubygem-aws-sdk-resources-3.128.0
rubygem-aws-sdk-robomaker-1.47.0
rubygem-aws-sdk-route53-1.62.0
rubygem-aws-sdk-route53domains-1.40.0
rubygem-aws-sdk-route53recoverycluster-1.11.0
rubygem-aws-sdk-route53recoverycontrolconfig-1.10.0
rubygem-aws-sdk-route53recoveryreadiness-1.10.0
rubygem-aws-sdk-route53resolver-1.37.0
rubygem-aws-sdk-s3-1.113.0
rubygem-aws-sdk-s3control-1.50.0
rubygem-aws-sdk-s3outposts-1.13.0
rubygem-aws-sdk-sagemaker-1.121.0
rubygem-aws-sdk-sagemakerredgemanager-1.11.0
rubygem-aws-sdk-sagemakerfeaturestoreruntime-1.12.0
rubygem-aws-sdk-sagemakerruntime-1.42.0
rubygem-aws-sdk-savingsplans-1.26.0
rubygem-aws-sdk-schemas-1.23.0

rubygem-aws-sdk-secretsmanager-1.59.0
rubygem-aws-sdk-securityhub-1.63.0
rubygem-aws-sdk-serverlessapplicationrepository-1.43.0
rubygem-aws-sdk-servicecatalog-1.70.0
rubygem-aws-sdk-servicediscovery-1.46.0
rubygem-aws-sdk-servicequotas-1.23.0
rubygem-aws-sdk-ses-1.47.0
rubygem-aws-sdk-sesv2-1.27.0
rubygem-aws-sdk-shield-1.48.0
rubygem-aws-sdk-signer-1.38.0
rubygem-aws-sdk-simpliedb-1.35.0
rubygem-aws-sdk-sms-1.40.0
rubygem-aws-sdk-snowball-1.49.0
rubygem-aws-sdk-snowdevicemanagement-1.7.0
rubygem-aws-sdk-sns-1.53.0
rubygem-aws-sdk-sqs-1.51.0
rubygem-aws-sdk-ssm-1.134.0
rubygem-aws-sdk-ssmcontacts-1.13.0
rubygem-aws-sdk-ssmincidents-1.13.0
rubygem-aws-sdk-ssoadmin-1.16.0
rubygem-aws-sdk-ssooidc-1.19.0
rubygem-aws-sdk-states-1.48.0
rubygem-aws-sdk-storagegateway-1.67.0
rubygem-aws-sdk-support-1.41.0
rubygem-aws-sdk-swf-1.36.0
rubygem-aws-sdk-synthetics-1.26.0
rubygem-aws-sdk-textract-1.37.0
rubygem-aws-sdk-timestreamquery-1.16.0
rubygem-aws-sdk-timestreamwrite-1.14.0
rubygem-aws-sdk-transcribeservice-1.74.0
rubygem-aws-sdk-transcribestreamingservice-1.42.0

rubygem-aws-sdk-transfer-1.52.0
rubygem-aws-sdk-translate-1.44.0
rubygem-aws-sdk-voiceid-1.6.0
rubygem-aws-sdk-waf-1.47.0
rubygem-aws-sdk-wafregional-1.48.0
rubygem-aws-sdk-wafv2-1.38.0
rubygem-aws-sdk-wellarchitected-1.15.0
rubygem-aws-sdk-workdocs-1.39.0
rubygem-aws-sdk-worklink-1.32.0
rubygem-aws-sdk-workmail-1.49.0
rubygem-aws-sdk-workmailmessageflow-1.21.0
rubygem-aws-sdk-workspaces-1.67.0
rubygem-aws-sdk-workspacesweb-1.3.0
rubygem-aws-sdk-xray-1.47.0
rubygem-aws-sigv2-1.1.0
rubygem-aws-sigv4-1.4.0
rubygem-bindata-2.4.10
rubygem-bindex-0.8.1
rubygem-bluestorm_cli-3.0.0.3155059
rubygem-bootsnap-1.11.1
rubygem-builder-3.2.4
rubygem-bundler-2.3.11,1
rubygem-byebug-11.1.3
rubygem-capybara-3.36.0
rubygem-childprocess-4.1.0
rubygem-colorize-0.8.1
rubygem-concurrent-ruby-1.1.10
rubygem-cookiejar-0.3.3
rubygem-crack-0.4.5
rubygem-crass-1.0.6
rubygem-cucumber-7.1.0_3

rubygem-cucumber-core-10.1.1_1
rubygem-cucumber-create-meta-6.0.4_1
rubygem-cucumber-cucumber-expressions14-14.0.0
rubygem-cucumber-gherkin22-22.0.0
rubygem-cucumber-html-formatter17-17.0.0_1
rubygem-cucumber-messages17-17.1.1
rubygem-cucumber-tag-expressions-4.1.0
rubygem-cucumber-wire-6.2.1_1
rubygem-daemons-1.4.1
rubygem-dalli-3.2.1
rubygem-devdctl-0.1.0.3141754
rubygem-devstat_stat-0.0.1.3141769
rubygem-diff-lcs-1.5.0
rubygem-digest-crc-0.6.4
rubygem-docile-1.4.0
rubygem-ds3-0.0.1.1358398
rubygem-ds3apitest-0.1.0.1759726_8
rubygem-e2mmap-0.1.0
rubygem-ejs-1.1.1
rubygem-em-http-request-1.1.7
rubygem-em-socksify-0.3.2
rubygem-erubi-1.10.0
rubygem-etc-1.3.0
rubygem-eventmachine-1.2.7
rubygem-execjs-2.8.1_2
rubygem-faraday-1.9.3
rubygem-faraday-em_http-1.0.0
rubygem-faraday-em_synchrony-1.0.0
rubygem-faraday-excon-1.1.0
rubygem-faraday-httpclient-1.0.1
rubygem-faraday-multipart-1.0.3

rubygem-faraday-net_http-1.0.1
rubygem-faraday-net_http_persistent-1.2.0
rubygem-faraday-patron-1.0.0
rubygem-faraday-rack-1.0.0
rubygem-faraday-retry-1.0.3
rubygem-faraday_middleware-1.2.0
rubygem-faye-1.4.0
rubygem-faye-websocket-0.11.1
rubygem-ffi-1.15.5
rubygem-ffi-locale-1.0.1_2
rubygem-ffi-ncurses-0.4.0_3
rubygem-fio_rb-1.1.0.2908800
rubygem-freebsd_cam-1.0.7.3188006
rubygem-freebsd_mps-1.1.1.3141765
rubygem-freebsd_ses-1.3.2.3183772
rubygem-globalid-rails61-1.0.0
rubygem-hashdiff-1.0.1
rubygem-http_parser.rb-0.8.0
rubygem-i18n-1.10.0,2
rubygem-i18n-js-3.0.11
rubygem-inifile-3.0.0
rubygem-io-console-0.5.11
rubygem-ipaddress-0.8.3
rubygem-irb-1.4.1
rubygem-jbuilder-rails61-2.11.5
rubygem-jmespath-1.6.1
rubygem-jquery-rails-rails61-4.4.0
rubygem-json-2.5.1
rubygem-json_pure-2.6.1
rubygem-jwt-2.3.0
rubygem-key_verify-1.0.1.3141771

rubygem-libifconfig-0.1.0.2959489_1
rubygem-libxml-ruby-3.2.2_1
rubygem-live_record-0.2.1.3141773
rubygem-liveresource-2.1.2.3180522
rubygem-loofah-2.16.0
rubygem-lsiexp-1.2.4.3175307
rubygem-mail-2.7.1_2,2
rubygem-marcel-1.0.2
rubygem-matrix-0.4.2
rubygem-method_source-1.0.0
rubygem-mime-types-3.4.1
rubygem-mime-types-data-3.2022.0105
rubygem-mini_mime-1.1.2
rubygem-minitest-5.15.0
rubygem-mocha-1.13.0
rubygem-msgpack-1.5.1
rubygem-multi_json-1.15.0
rubygem-multi_test-0.1.2_1
rubygem-multipart-post-2.1.1
rubygem-net-ping-2.0.8
rubygem-net-scp-3.0.0
rubygem-net-ssh-6.1.0,2
rubygem-nio4r-2.5.8
rubygem-nokogiri-1.13.4
rubygem-open4-1.3.4
rubygem-os-1.1.4
rubygem-pam-1.5.2.3141780
rubygem-passenger-nginx-6.0.12_2
rubygem-pg-1.3.5
rubygem-pkg-config-1.4.7
rubygem-pmbus-1.1.2.3141787

rubygem-power_assert-2.0.1
rubygem-pqueue-2.1.0
rubygem-pretty-xml-0.2.2
rubygem-psych-4.0.3
rubygem-public_suffix-4.0.7
rubygem-puma-5.6.4
rubygem-racc-1.6.0
rubygem-rack-2.2.6.2,3
rubygem-rack-proxy-0.7.2
rubygem-rack-test-1.1.0_2
rubygem-rails-dom-testing-rails61-2.0.3
rubygem-rails-html-sanitizer-1.4.2
rubygem-rails61-6.1.6
rubygem-railties61-6.1.6
rubygem-rake-13.0.6
rubygem-rb-kqueue-0.2.8
rubygem-rbcurse-1.5.3
rubygem-rbcurse-core-0.0.14_2
rubygem-rbcurse-extras-0.0.0
rubygem-rdoc-6.4.0
rubygem-redis-4.6.0
rubygem-regexp_parser-2.1.1
rubygem-reline-0.3.1
rubygem-rexml-3.2.5
rubygem-rice-2.2.0
rubygem-rrd-ffi-0.2.14_4
rubygem-rspec-expectations-3.11.0
rubygem-rspec-support-3.11.0
rubygem-ruby-termios-1.1.0
rubygem-ruby2_keywords-0.0.5
rubygem-rubyzip-2.3.2

rubygem-sass-rails-rails61-6.0.0
rubygem-sassc-rails-rails61-2.1.2
rubygem-sassc22-2.2.1
rubygem-selenium-webdriver-4.1.0
rubygem-semantic_range-3.0.0
rubygem-serialport-1.3.2
rubygem-simplecov-0.21.2
rubygem-simplecov-html-0.12.3
rubygem-simplecov_json_formatter-0.1.4
rubygem-smart_data-0.0.2.3141789
rubygem-snmp-1.2.0
rubygem-spectra_acl-1.2.1.2959489_2
rubygem-spectra_cli-1.0.2.3197626
rubygem-spectra_platform-1.3.1.3187661
rubygem-spectra_support-5.0.0.3150998
rubygem-spectra_view-2.3.0.3207748_10
rubygem-spectra_workers-5.0.0.3207786
rubygem-spring-4.0.0
rubygem-sprockets-rails-rails61-3.4.2
rubygem-sprockets3-3.7.2_2
rubygem-sqlite3-1.4.2
rubygem-staf4ruby-0.1.3.3141819,1
rubygem-stringio-3.0.1
rubygem-sys-uname-1.2.2
rubygem-tape_backend-0.1.3163739
rubygem-test-unit-3.5.3
rubygem-thin-1.8.1_2
rubygem-thor-1.2.1
rubygem-thwait-0.2.0
rubygem-tilt-2.0.10
rubygem-turbolinks-5.2.1

rubygem-turbolinks-source-5.2.0
rubygem-tzinfo-2.0.4
rubygem-uglifyer-4.2.0
rubygem-uuidtools-2.2.0
rubygem-web-console-rails61-4.2.0
rubygem-webdrivers-5.0.0
rubygem-webmock-3.14.0
rubygem-webpacker-rails61-5.4.3_2
rubygem-webrick-1.7.0
rubygem-websocket-driver-0.7.5
rubygem-websocket-extensions-0.1.5
rubygem-xpath-3.2.0
rubygem-yard-0.9.27
rubygem-zeitwerk-2.5.4
rubygem-zfs-0.0.12.3154388
samba413-4.13.17_5
sedutil-1.12.3198939
sg3_utils-1.45
smartmontools-7.3
smp_utils-0.99
source-highlight-3.1.9_1
spectra_ltfs-2.5.0.0.3136603
sqlite3-3.38.5,1
staf-3.4.26_1
stress-1.0.4_1
stress-ng-0.13.12
t5seeprom-0.0.1366684_1
talloc-2.3.1
tcgstorageapi-1.0_2
tcl86-8.6.12
tdb-1.4.3,1

tevent-0.10.2_1
tidy-html5-5.8.0_2
tiff-4.3.0
tmux-3.2a
tomcat-native-1.2.35
tomcat85-8.5.91
vail-3.1.0_4
verde_hotpair-3.0.3206585
vim-8.2.4669
xorg-fonts-truetype-7.7_1
xorgproto-2021.5
yarn-1.22.18
zfs-stats-1.3.1
zip-3.0_1
zsh-5.8.1
zstd-1.5.2

INDEX

A

Activation keys

entering manually 198

Apache, open source acknowledgement 271

autosupport

about 200

configure mail recipient 201

B

bezel, removing 191

BlackPearl

components 25, 29, 33, 43, 52

features 20

monitoring 159

overview 20

power 63

serial number 213

size and weight 238

specifications 234

BlackPearl NAS

software 59

BlackPearl user interface

log in 68

C

CE Marking 266

certificates

configure 85

CIFS

about 59

configure service 115

set permissions 113

command line interface 60

components

front view 39, 48

rear panel 43, 52

configuring

certificates 85

CIFS service 115

DNS 87

email 88

Ethernet ports 97

mail recipients 201

NAS replication 117

NAS storage pools 101

NAS volumes 104

network connections 87, 97

NFI volume policy 107

NFS service 115

NTP 89

services 91, 115-116

shares 108, 110

SMTP 88

snapshots 123

user 145

Conflict Mineral Policy 269

contacting Spectra Logic 7

contacting, Technical Support 213

corporate headquarters, Spectra Logic 7

D

data drive

- install new 192

- remove 191

data integrity verification

- disk pools 195

DNS, configure 87**documentation**

- typographical conventions 16

drive, install new 179

E

email

- configuring 88

- send test 203

- Spectra Logic offices 7

Ethernet ports, configure 97**EU Declaration of Conformity 263**

F

fax numbers, Spectra Logic 7**FCC Notice 266****Free BSD**

- about 59

- open source acknowledgement 272

front view 39, 48

H

hardware

- monitor status 167

J

Java

- open source acknowledgement 273

L

LEDs

- data drives 55

license agreement, software 3**logical volume manager and file system,
about 59**

M

mail recipients

- add 201

- configure 201

mailing address, Spectra Logic 7**maintenance, replace component 176****management port, use 97****MIB file, download 96**

N

NAS replication

- configure 117
- configure volumes 119
- manual 149
- restore files from a replication target 149

NAS storage pools

- create new 101
- requirements 101

NAS volumes

- configure 104
- create snapshot 123
- delete snapshot 127
- restore file from snapshot 130
- restore snapshot 129
- scheduled snapshots 125
- snapshot restore 129
- snapshots 123

network

- cables 259
- configure 87, 97
- configure DNS 87

NFI

- configure 107

NFS

- about 59
- configure service 115

Nginx, open source acknowledgement 281

NTP

- configuring 89

O

open source acknowledgement

- Apache 271
- Free BSD 272
- Java 273
- Nginx 281
- Ruby 282
- Ruby on rails 283
- ZFS 284

P

performance metrics 154

phone numbers, Spectra Logic offices 7

portal

- accessing for technical support 211-212

power

- power off 174
- power on 63
- reboot 174
- requirements 249

R

rear panel 43, 52

rear view 41, 50, 56

recycling 269

regulatory

- CE Marking 266
- Conflict Mineral Policy 269

EU Declaration of Conformity 263
FCC Notice 266
RoHS 268
Safety Standards and Compliance 268
WEEE Directive 268

replication

configure target system 118

RoHS 268

Ruby on rails, open source
acknowledgement 283

Ruby, open source acknowledgement 282

S

Safety Standards and Compliance 268

sales, contacting 7

serial number

where to find 213

services

CIFS 115
configuring 91, 115-116
NFS 115

shares

configure 108, 110

SMTP

configure 88

snapshots

about 123
configure 123
create new 123
delete 127
restore 129

retrieve single file 130
scheduled, about 125

SNMP service

configure 91, 95

software

license agreement 3

specifications

data storage 231
environmental 244
power 249
power cords 252
size and weight 238
system 234

Spectra Logic

contacting 7

status lights 163

support

contacting 213

support portal

accessing 211

support ticket

opening 214

system messages 152

system name

edit 89

T

technical support

accessing the Technical Support portal 211-212
contacting 7

typographical conventions 16

U

USB, support 261

user

configure 145

edit 145

types 145

V

Visual Status Beacon, lights 159

W

website

Spectra Logic 7

WEEE Directive 268

Z

ZFS, open source acknowledgement 284