Spectra Logic BlackPearl NAS Solution

User Guide

SpectraLogic.com

COPYRIGHT

Copyright © 2019-2025 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 H

REVISION HISTORY

Revision	Date	Description
E	April 2023	Updated for the BlackPearl OS 5.6 release.
F	October 2023	Updated for the BlackPearl OS 5.7 release.
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.

Notes:
- 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/*.

- To make sure you have the release notes for the most current version of the BlackPearl OS software, see the Spectra Logic Technical Support portal at *support.spectralogic.com/documentations/software-release-notes*.

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: *spectralogic.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.spectralogic.com*	
United States and Canada **Phone:** **Toll free US and Canada:** 1.800.227.4637 **International:** 1.303.449.0160	**Europe, Middle East, Africa** **Phone:** 44 (0) 870.112.2185 **Deutsch Sprechende Kunden** **Phone:** 49 (0) 6028.9796.507 **Email:** spectralogic@stortrec.de
Mexico, Central and South America, Asia, Australia, and New Zealand **Phone:** 1.303.449.0160	
Spectra Logic Sales	
Website: *shop.spectralogic.com*	
United States and Canada **Phone:** 1.800.833.1132 or 1.303.449.6400 **Fax:** 1.303.939.8844 **Email:** sales@spectralogic.com	**Europe** **Phone:** 44 (0) 870.112.2150 **Fax:** 44 (0) 870.112.2175 **Email:** eurosales@spectralogic.com
To Obtain Documentation	
Spectra Logic Website: *support.spectralogic.com/documentations*	

Table of Contents

ABOUT THIS GUIDE

This guide describes how to configure, monitor, and maintain the Spectra® BlackPearl® NAS (Network Attached Storage)solution 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 Solution 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 solution, log into the Support portal (see Access the Technical Support Portal on page 231), and navigate to **Documentation > Product Life Cycle Information**.

BLACKPEARLUSER 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 Solution.

Typographical Conventions

This document uses the following conventions to highlight important information:

⚠️	**WARNING**	Read text marked by the "Warning" icon for information you must know to avoid personal injury.
⚠️	**CAUTION**	Read text marked by the "Caution" icon for information you must know to avoid damaging the 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 solution, refer to the publications listed in this section.

Spectra BlackPearl NAS Solution

The following documents related to the Spectra BlackPearl NAS solution 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 Site Preparation Guide* provides important information that you should know before installing a BlackPearl NAS solution in your storage environment.

- The *Spectra BlackPearl NAS Solution Gen1 Installation Guide* provides detailed instructions for installing a Gen1 BlackPearl NAS solution.

- 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 solution, including information about the latest software releases and documentation updates.

- The *Spectra 12- & 36-Drive Chassis HBA Installation Guide* provides instructions for installing an HBA in a Gen1 master node.

- The *Spectra 12- & 36-Drive Chassis Boot Drive Replacement Guide* provides instructions for replacing a failed boot drive in a Gen1 master node.

- The *Spectra 12-, 36- & 45-Drive Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive in a Gen1 master node or 44-bay expansion node.

- The *Spectra 12-, 36- & 45-Drive Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in a Gen1 master node or 44-bay expansion node.

- The *Spectra 12-, 36- & 45-Drive Chassis Power Supply Replacement Guide* provides instructions for replacing a failed power supply in a Gen1 master node or 44-bay expansion node.

- The *Spectra 12-Drive Chassis HBA Replacement Guide* and *Spectra 36-Drive Chassis HBA Replacement Guide* provide instructions for replacing a failed HBA in a Gen1 master node.

- 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.

WHAT'S NEW

BlackPearl OS 5.8 brings with it the following changes and improvements:

Gen3 F-Series Chassis Support

The BlackPearl system offerings now include the new 2U F-Series chassis which features 24 drives mounted in the front of the chassis. The F-Series chassis also supports a HotPair configuration using two 1U servers in the 2U chassis.

OSW-2400 Switch Support

The BlackPearl system now supports the Spectra OSW-2400 SAS switch. The switch is a 1U form factor with 11 SAS ports.

Ultrium LTO-10 Support

The BlackPearl system now supports Ultrium LTO-10 tape drives in a Spectra tape library.

Configuration Enhancements for the Spectra Vail Application

The BlackPearl system database configuration is enhanced for better performance when used in conjunction with the Spectra Vail application.

Logset Push to AWS Bucket

The BlackPearl system now supports copying logsets to an external AWS bucket.

Logging Improvements

The BlackPearl system now gathers memory data and PGSQL history and includes them in the AutoSupport Log (ASL) files used by Spectra Logic Technical Support.

Gen2 Chassis NVMe Speed Improvements

Changes to the internal cabling of the Gen2 chassis provides improved speeds from NVMe drives.

CHAPTER 1 - PRODUCT OVERVIEW

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

OVERVIEW

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

Optimized for secondary storage, the highly versatile BlackPearl NAS solution 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 solution includes the following features:

Attack Hardening

The BlackPearl NAS solution 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 solution. It also lets you monitor the hardware and view system messages.

Command Line Interface

The BlackPearl NAS solution 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 solution 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 system now offers multi-factor authentication, which enhances the security of your BlackPearl system by using Google Authenticator 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 solution. Rack-mounting hardware is included with each BlackPearl NAS solution.

Replicated Configuration

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

Redundant Hardware

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

Network Attached Storage Features

Data Replication

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

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.

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.

Network File Interface

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

RAID-Protected Data Disks

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

Snapshot Change Threshold

The BlackPearl system now 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

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.

Write Performance Drives

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

Optional Hardware Features

HotPair

Two BlackPearl NAS master nodes or a Gen2 X Series 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 solution. 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

Gen1 Chassis

10GBase-T Ethernet Connectivity

Two onboard 10 gigabit copper ports (10GBase-T) provide Ethernet connectivity for the solution 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 solution.

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 solution.

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 solution.

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 solution 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 solution 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 solution.

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 solution.

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.

COMPONENTS

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

Front Bezel

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

Note: For the 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 solution. See Front Bezel Visual Status Beacon on page 201 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 solution with the front bezel removed.
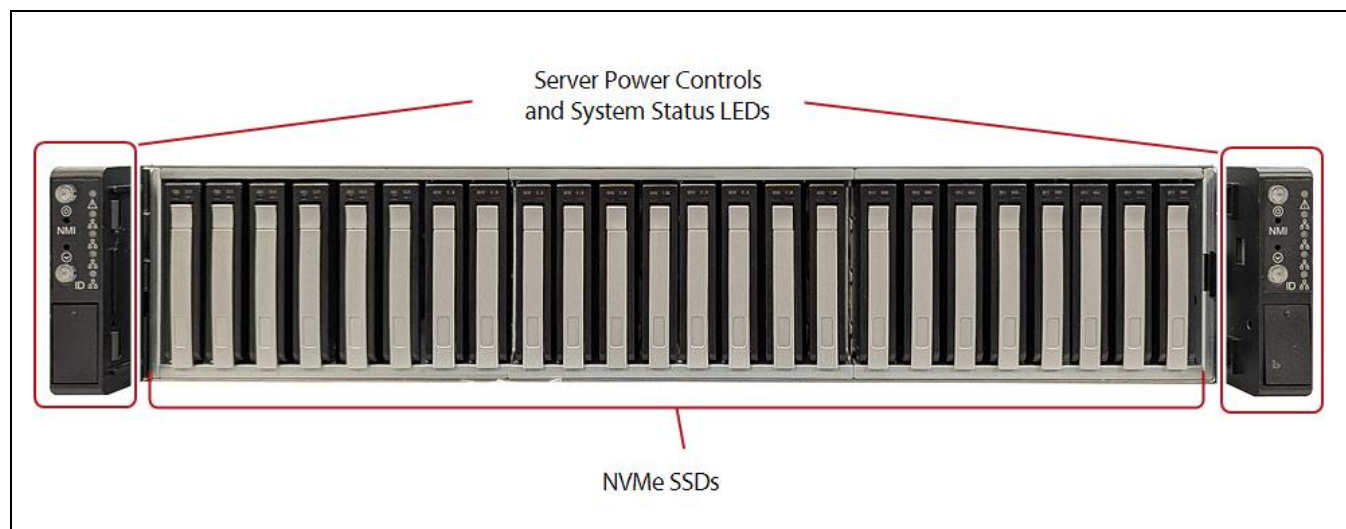
Figure 2 The front view of the Gen3 F Series BlackPearl NAS solution (front bezel removed).

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 solution 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 6 shows the major components on the rear of the Gen3 F series BlackPearl NAS solution.
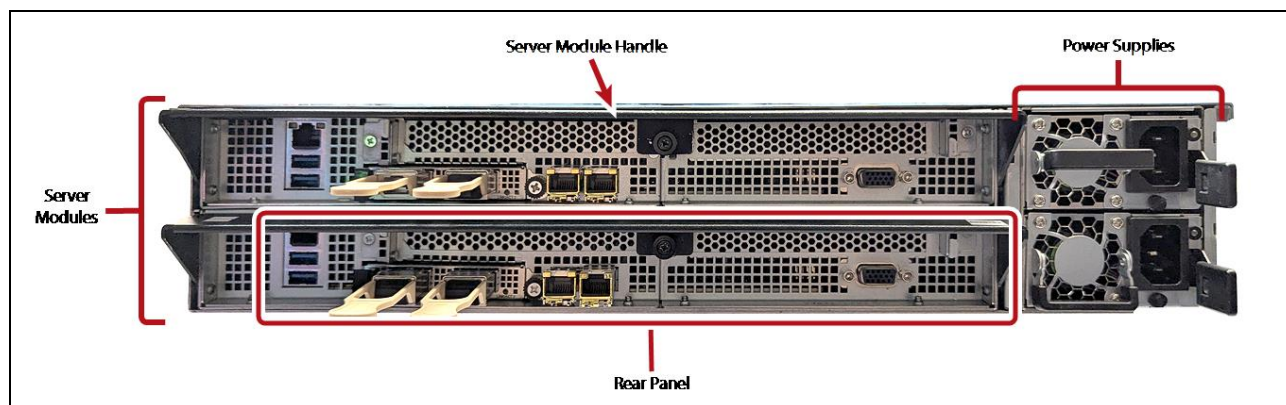
Figure 3 The rear view of the Gen3 F Series BlackPearl NAS solution.

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 NAS 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 solution 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 NAS master node.
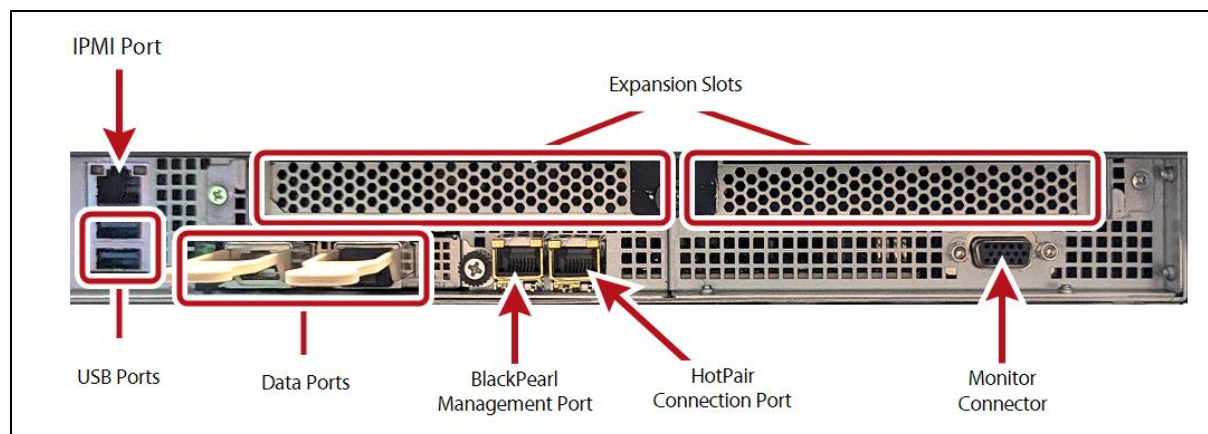
Figure 4 The Gen3 F Series BlackPearl NAS rear panel components.

Component	Description

IPMI management port	See IPMI Configuration on page 280 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 system.
Expansion Slots	Two expansion slots provide support for either SAS or Fibre Channel connections.

Component	Description
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 solution. The BlackPearl management port cannot be used for data transfer.
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

Front View

Figure 5 shows the components on the front of the Gen3 H Series BlackPearl NAS solution with the front bezel removed.
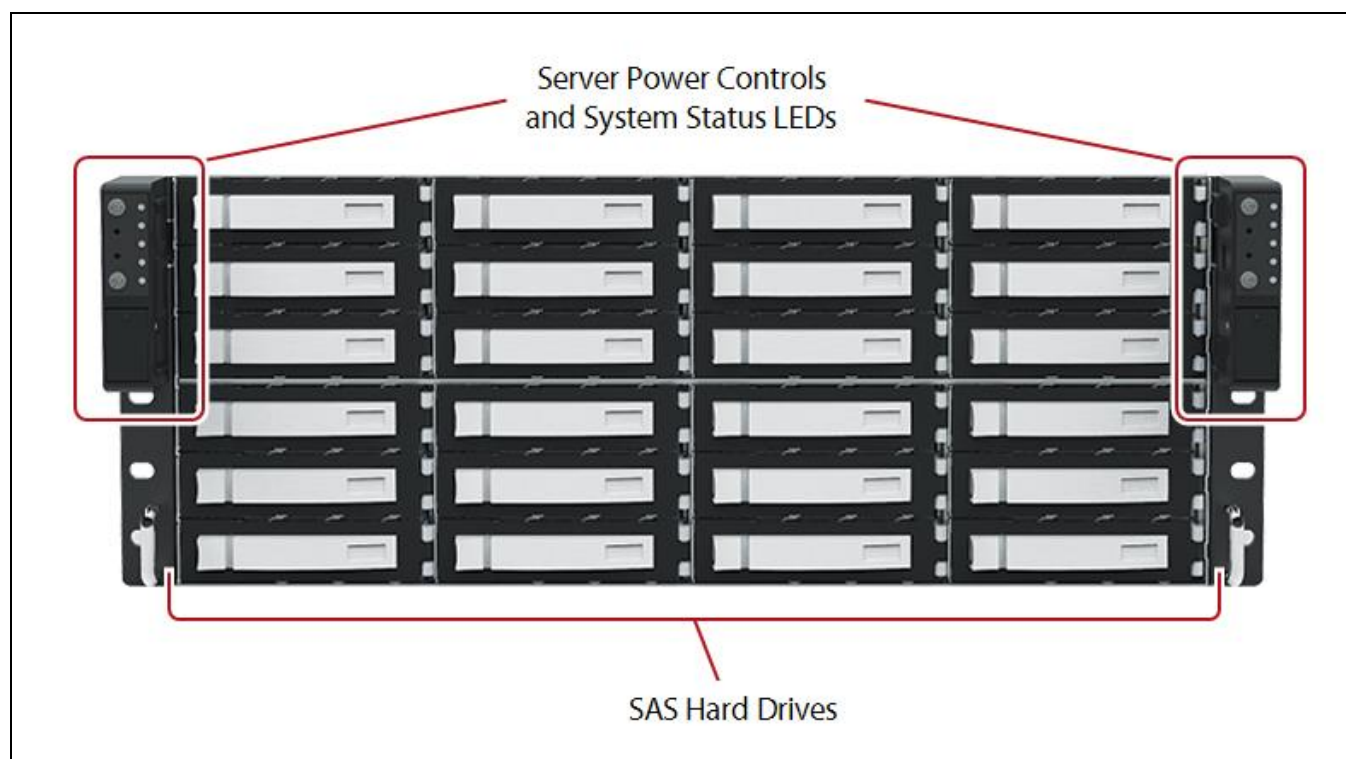
Figure 5 The front view of the Gen3 H Series BlackPearl NAS solution (front bezel removed).

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 solution supports up to 24 high-performance SAS hard drives (HDDs) 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.

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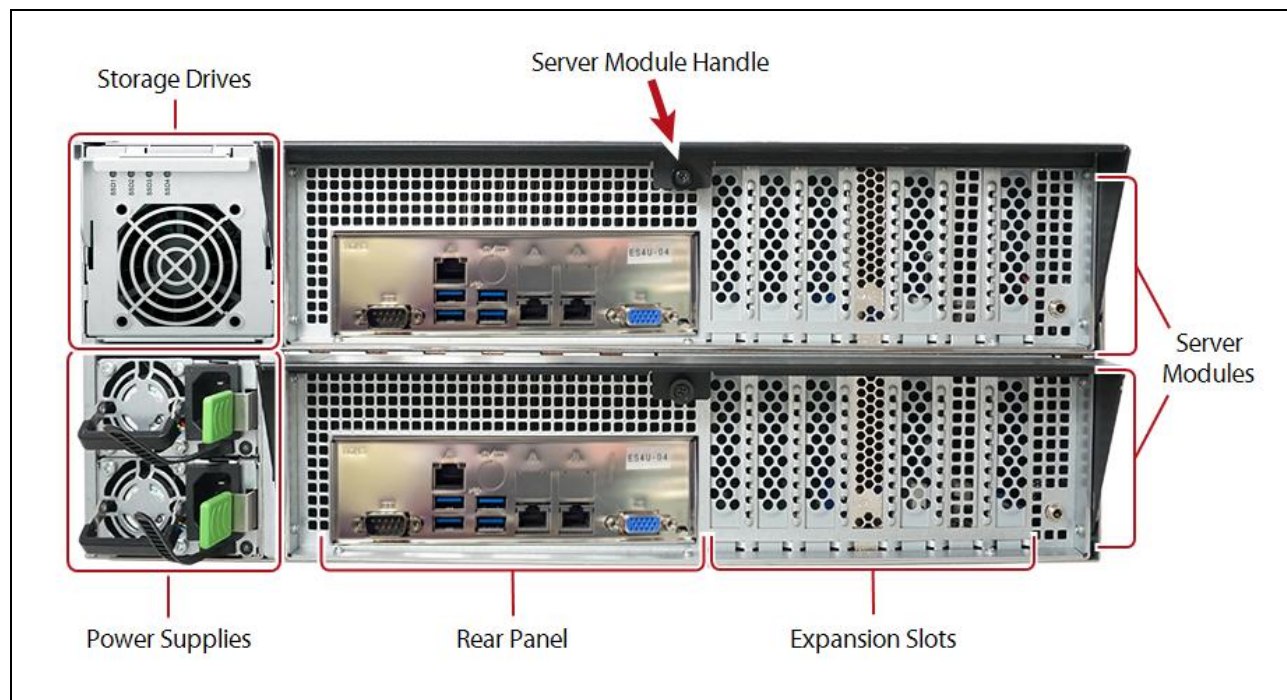
Figure 6 The rear view of the Gen3 H Series BlackPearl NAS solution.

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 NAS master node allows for Ethernet, SAS, USB, IPMI, and other connections. See Rear Panel on page 29 for a detailed description.
Storage drives	The Gen 3 H Series supports up to four NVMe drives for special allocation, metadata performance, and ZIL.
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 solution 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.

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 system.
	
	• 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 4 shows the components on the rear panel of the Gen3 H Series BlackPearl NAS master node.
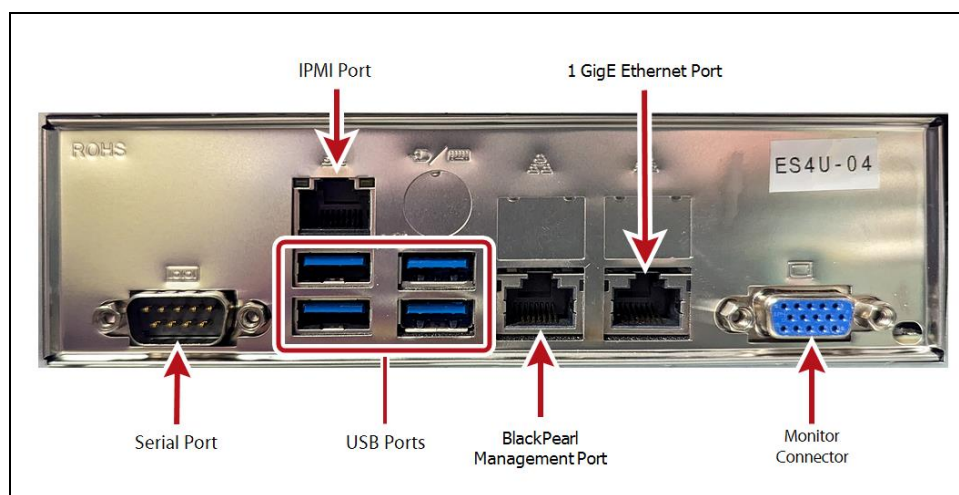
Figure 7 The Gen3 H Series BlackPearl NAS rear panel components.

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.

Component	Description
Serial port	The serial port is only used in a HotPair configuration.

IPMI management port	See IPMI Configuration on page 280 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 NAS solutions 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 solution. 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 solutions with the front bezel removed.
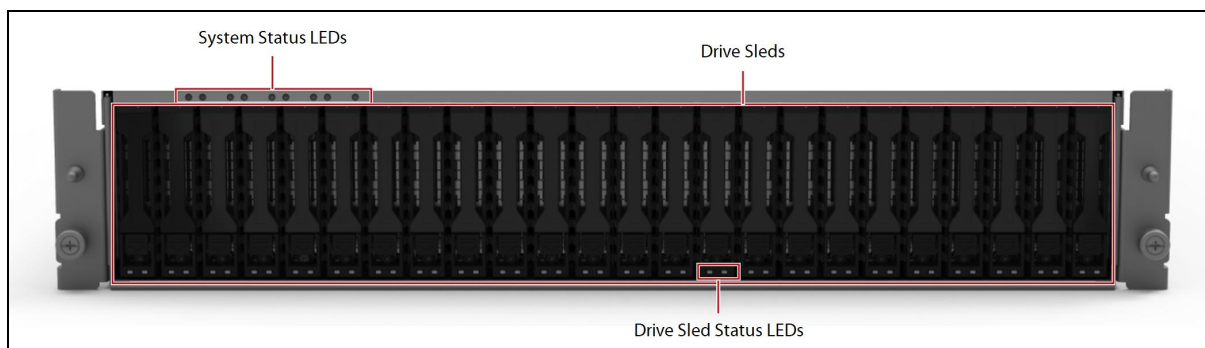
Figure 8 The front view of the Gen2 X Series BlackPearl NAS solution (front bezel removed).

Component	Description
System status LEDs	The status LEDs indicate power status, fan status, server status, and chassis status. See System Status LEDs on page 202 for more information. **Note:** The LEDs are not visible with the bezel installed.
Data drives	The base Gen2 X Series BlackPearl NAS solution 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 NAS chassis.
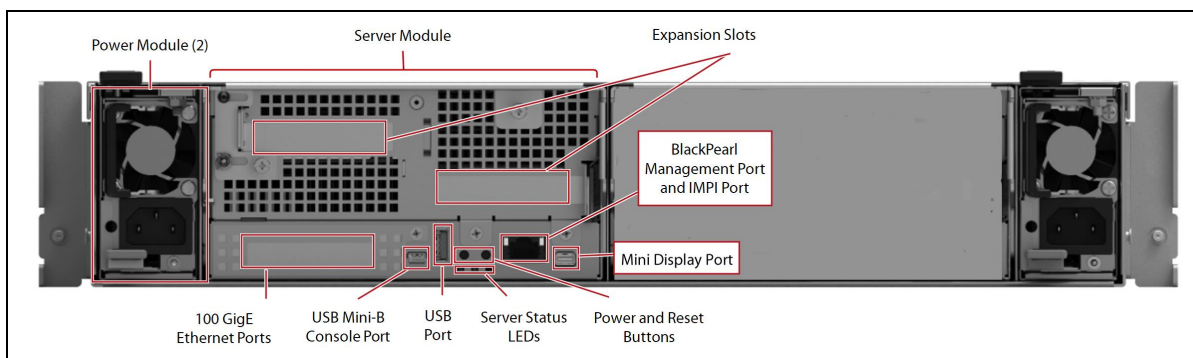
Figure 9 The rear view of the Gen2 X Series BlackPearl NAS solution.

Component	Description

Power modules	The Gen2 X Series BlackPearl NAS solution 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 monumentally 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 solution. 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 solution 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 solution with the front bezel removed. Figure 11 shows the components on the front of the Gen2 V Series BlackPearl NAS solution with the front bezel removed.

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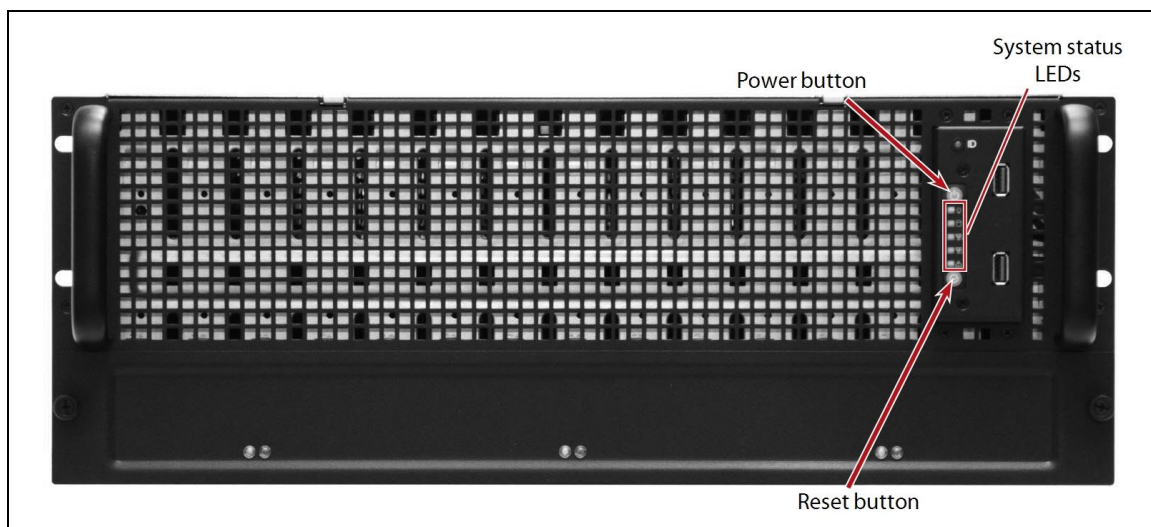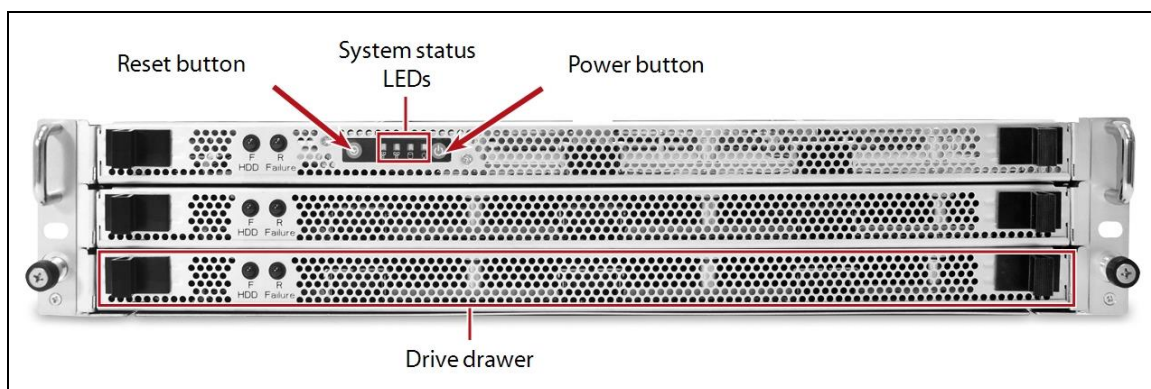

Figure 11 The front view of the Gen2 V Series BlackPearl NAS 2U solution (front bezel removed).

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.

Component	Description
Reset button	Only use the chassis reset button under direction of Spectra Logic Technical Support.
System status LEDs	The status LEDs indicate power status, disk and network activity, as well as hardware faults. See System Status LEDs on page 202 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 solution may optionally contain solid state drives to improve NAS write performance. See Write Performance Drives on page 23 for more information.

Rear View

Figure 12 shows the major components on the rear of the Gen2 S BlackPearl NAS solution. Figure 13 shows the major components on the rear of the Gen2 V Series BlackPearl NAS solution.
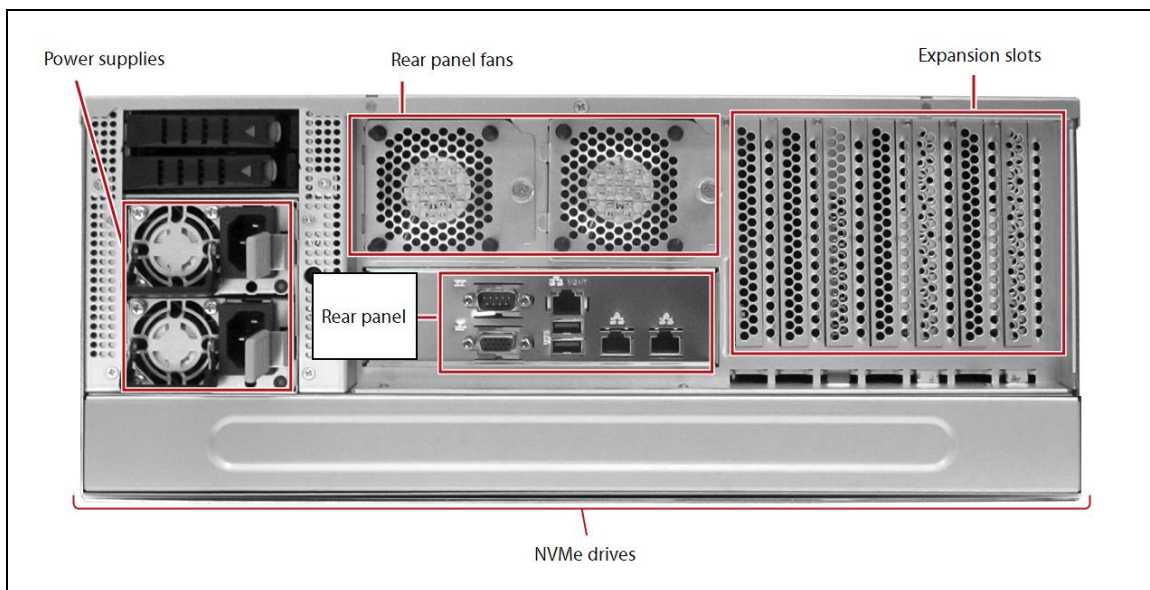
Figure 12 The rear view of the Gen2 S Series BlackPearl NAS 4U solution.
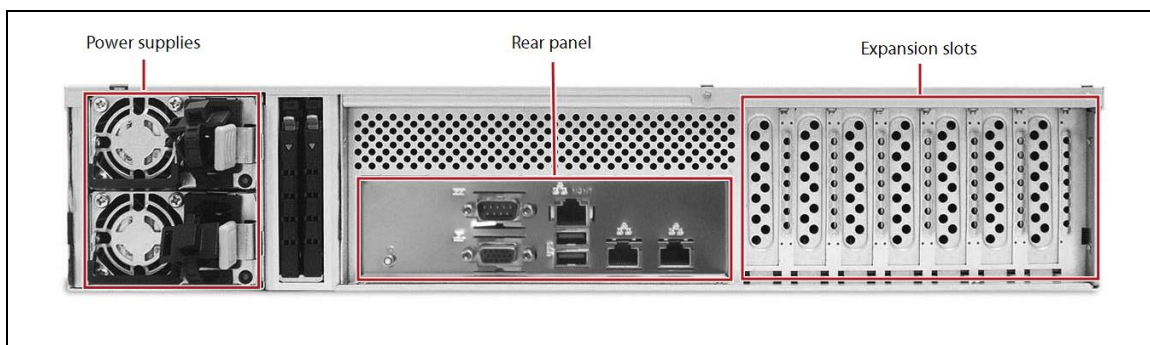
Figure 13 The rear view of the Gen2 V Series BlackPearl NAS 2U solution.

Component	Description
Power supplies	The standard BlackPearl NAS solution 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 NAS master node allows for Ethernet, SAS, USB, and other connections. See Rear Panel on page 44 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 solution. 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 NAS 4U and 2U master nodes.
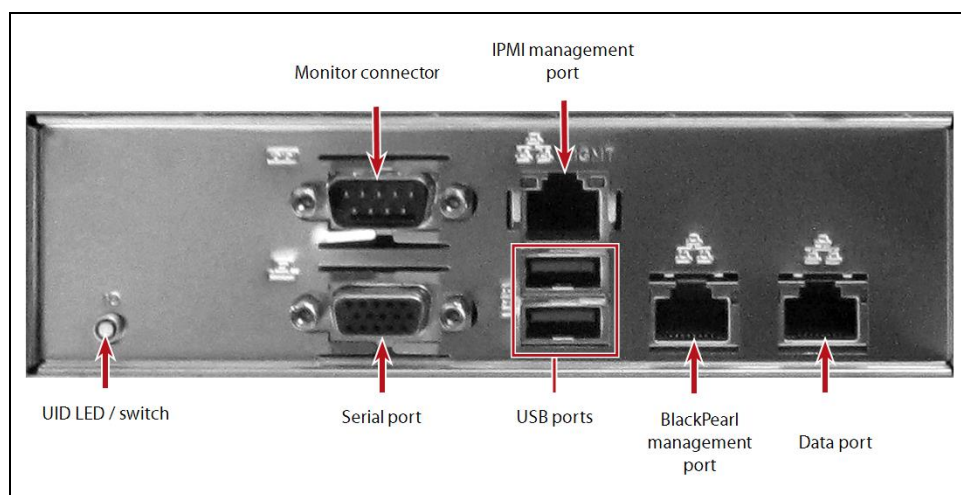
Figure 14 The Gen2 S Series and Gen 2 V Series BlackPearl NAS rear panel components.

Component	Description
UID LED / switch	Pressing the unit ID LED / switch displays a flashing blue pattern on the visual status beacon (see Front Bezel Visual Status Beacon on page 201) 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 280 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 NAS solutions 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 NAS solutions 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 solution. 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.
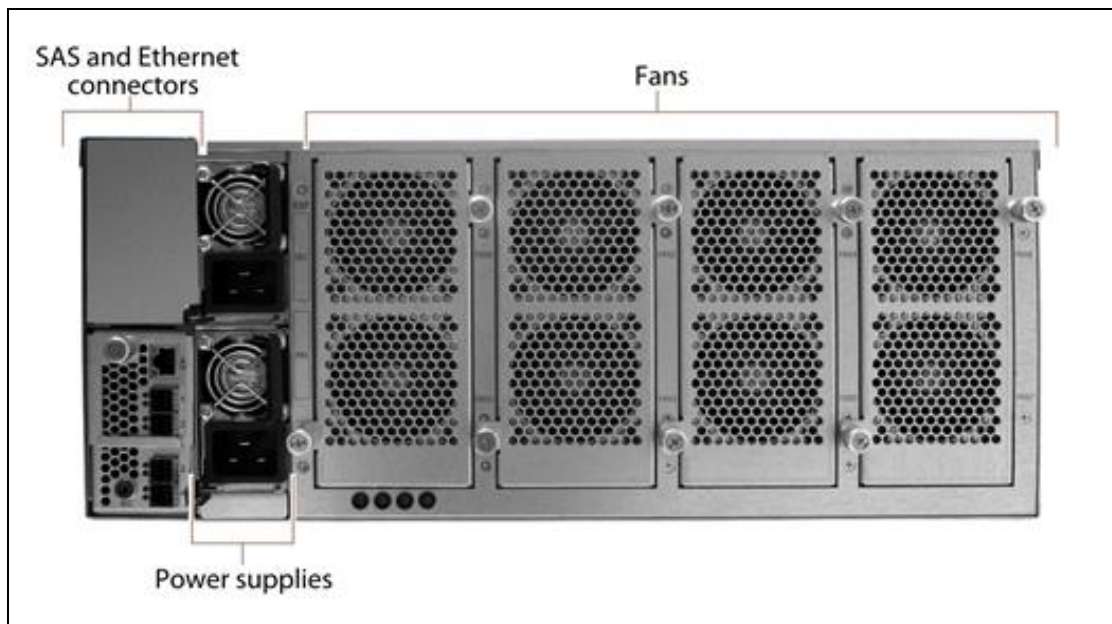
Figure 16 The rear view of the 77-bay and 107-bay expansion nodes.

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 NAS master node.
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 solution. 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 solution with the front bezels removed.
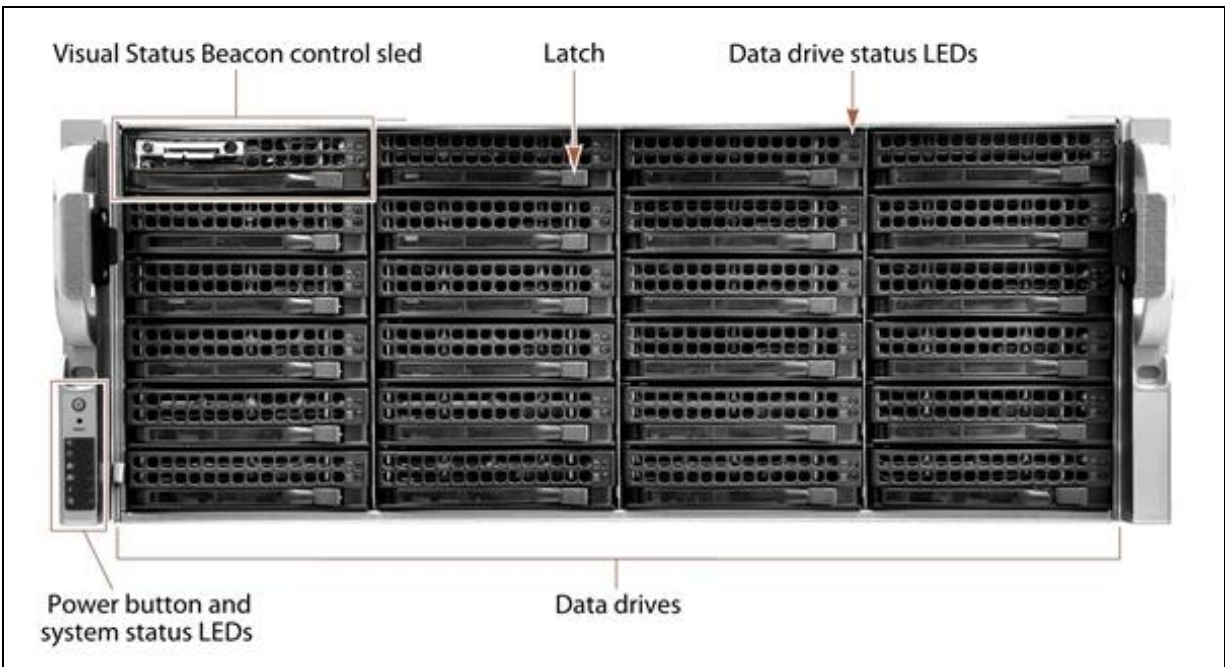

Figure 17 The front view of the Gen1 S and P Series BlackPearl NAS 4U master node (front bezel removed).
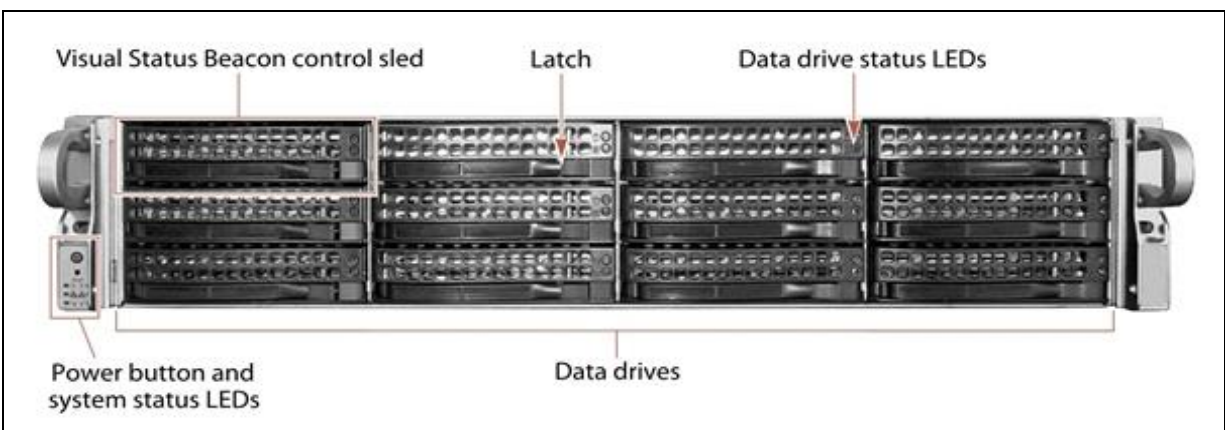

Figure 18 The front view of the Gen1 V Series BlackPearl NAS 2U master node (front bezel removed).

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 System Status LEDs on page 202 for more information. **Note:** The LEDs are not visible with the bezel installed.
Data drives	The BlackPearl NAS Gen1 S and P Series master nodes support up to 23 high-performance disk drives in the front of the chassis. The BlackPearl NAS 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 solution may optionally contain solid state drives to improve NAS write performance. See Write Performance Drives on page 23 for more information. **Note:** If the BlackPearl NAS 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 solution. The drive sleds slide into bays in the front of the BlackPearl NAS 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 NAS 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 NAS master node chassis.
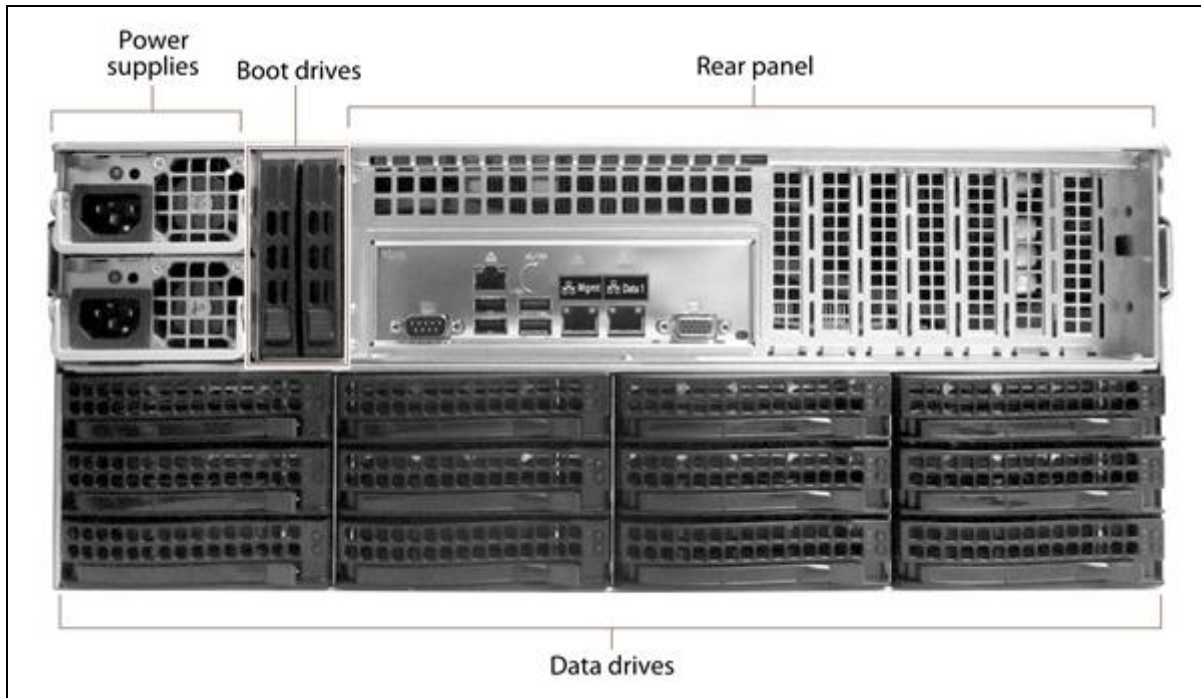

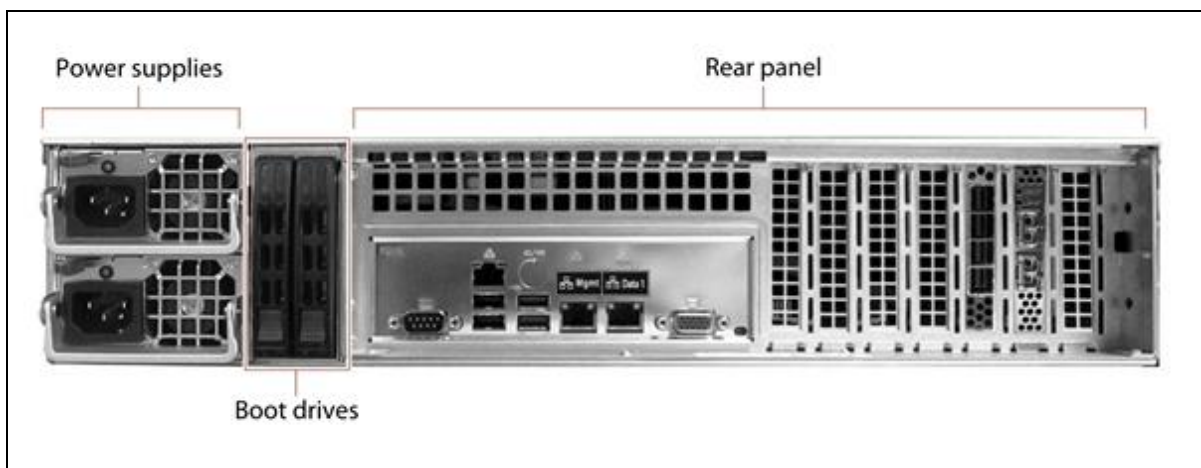**Figure 19** The rear view of the Gen1 S Series BlackPearl NAS 4U master node.

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

Component	Description
Power supplies	The standard BlackPearl NAS solution 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 solution allows for Ethernet, SAS, USB, and other connections. See Rear Panel on page 44 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 solution are hot swappable which allows for uninterrupted operation during replacement.
Data drives (BlackPearl NAS 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 Write Performance Drives on page 23 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 NAS 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 NAS 4U and 2U Gen1 S Series chassis.
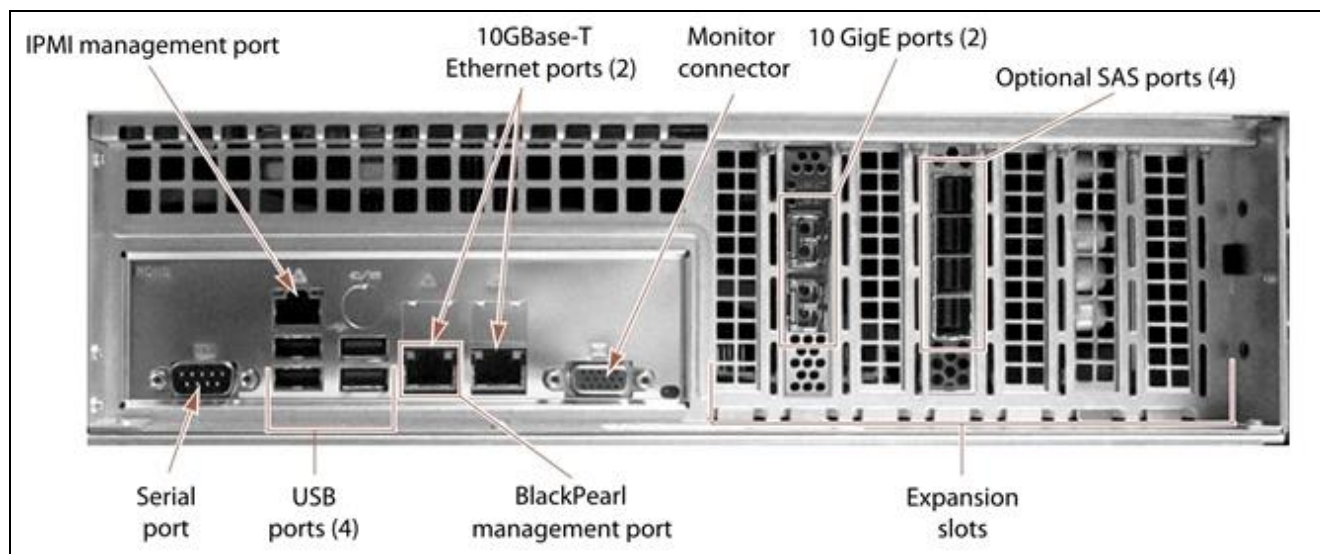

Figure 21 The Gen1 S Series BlackPearl NAS rear panel components.

Component	Description
IPMI management port	See IPMI Configuration on page 280 for information on using IPMI management.
10GBase-T Ethernet ports	The Gen1 S Series BlackPearl NAS 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 NAS 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 solution can contain different types of network interface cards, but can only use one card at a time. **Note:** Unless your BlackPearl NAS solution 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 solution. 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 solution. 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.
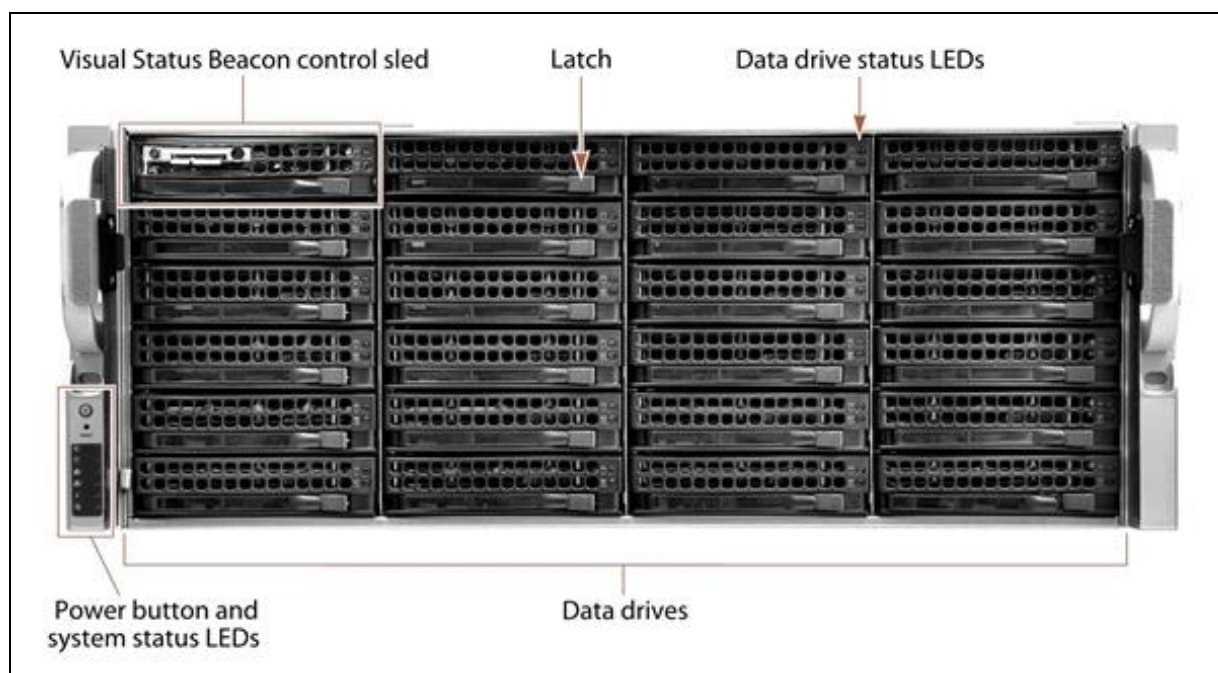

Figure 22 The front view of the 44-bay expansion node (front bezel removed).

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 solution, including the expansion node.
System status LEDs	The status LEDs indicate power status, disk and network activity, as well as hardware faults. See System Status LEDs on page 202 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

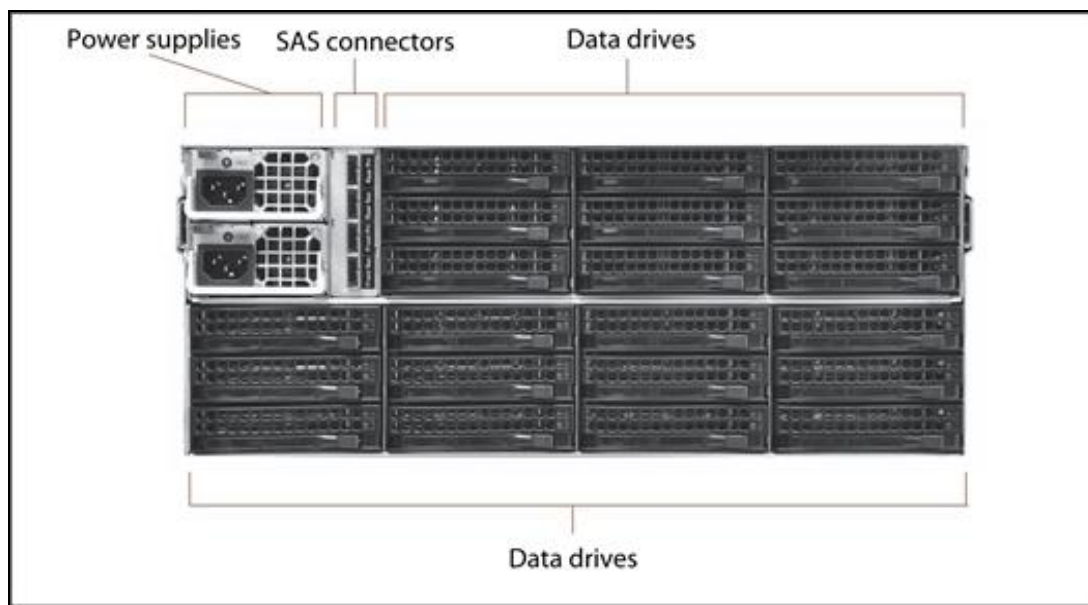Figure 23 shows the major components on the rear of the 44-bay expansion node.

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.
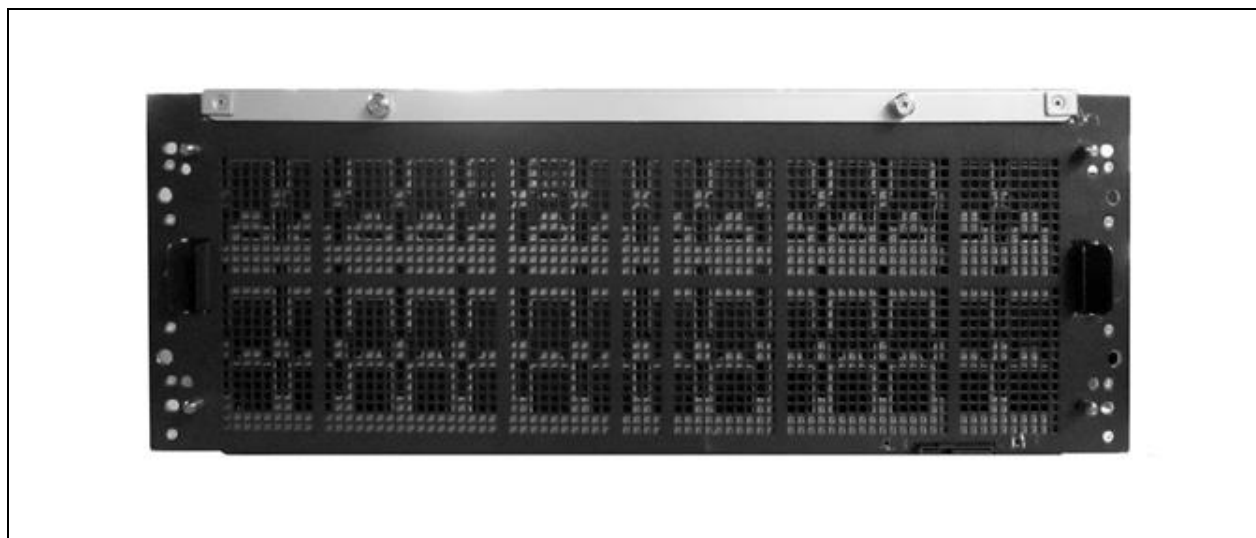

Figure 24 The front view of the 96-bay expansion node (front bezel removed).

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

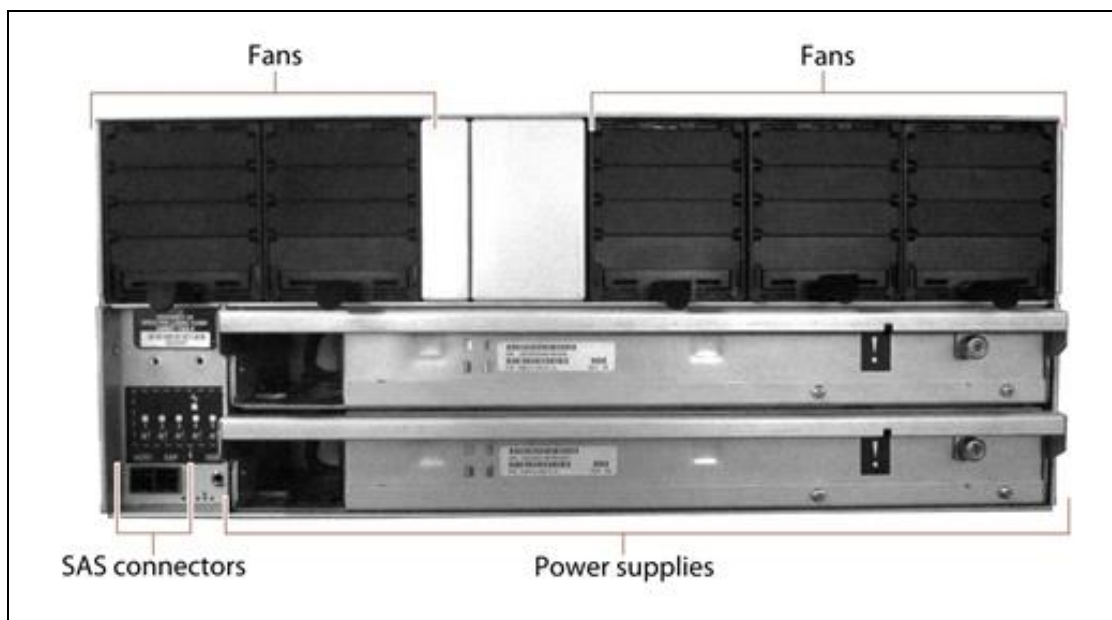Figure 25 shows the major components on the rear of the 96-bay expansion node.

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 NAS 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 solution 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 solution includes data verification to protect against corruption.

NFS and CIFS Servers

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

USER INTERFACE

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

Menus

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

Figure 26 The Dashboard screen of the BlackPearl NAS user interface.

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

> **Note:** Some options do not display in the system menu if the corresponding activation key is not installed.

Menu	Available Options
Dashboard	The **Dashboard** navigation link returns you to the Dashboard screen from any other screen. The Dashboard screen displays the general status of the solution, disk pools, volumes, and network connections. Clicking any of the panes on the Dashboard takes you to a details screen for that selection. The Dashboard screen also displays performance metrics for the solution.
Configuration	The **Configuration** menu provides access to controls for configuring all aspects of solution operation. • **NAS**

Menu	Available Options
	• **Pools**—Displays information about any currently configured NAS pools and lets you define new NAS pools, and edit or delete existing NAS pools.
	• **Volumes**—Displays information about any currently configured NAS volumes on an existing NAS pool and lets you define new NAS volumes, and edit or delete existing NAS volumes.
	• **Shares > CIFS**—Displays information about any currently configured CIFS shares and lets you define new shares, and edit or delete existing shares.
	• **Shares > NFS**—Displays information about any currently configured NFS shares and lets you define new shares, and edit or delete existing shares.
	• **Services**—Displays information about the currently configured services and lets you edit existing services.
	• **Network**—Provides controls for configuring the Ethernet ports on the BlackPearl NAS solution, configure a static route, Domain Name Servers, date and time, as well as entering SMTP (Simple Mail Transport Protocol) information to allow the solution to send emails.
	• **Certificates**—Provides controls for installing signed, trusted SSL certificates for your data and management ports so that you do not need to resolve the security certificate warning when accessing these ports.
	• **Mail Recipients**—Provides controls for configuring mail recipient accounts to receive emails when a message severity threshold is reached, or when AutoSupport Log sets (ASLs) are generated by the solution.
	• **Users**—Provides controls for creating new S3 user accounts that act as owners for buckets, editing the login password, and displaying the S3 credentials for each user
Status	The **Status** menu provides access to the tools for monitoring the BlackPearl NAS solution in your environment.
	• **Hardware**—Displays information about the solution, its components,and disk expansion nodes and associated disk drives. Selecting the tabs on the Hardware screen displays detailed component status information.
	• **NAS > Pools**—Displays information about any currently configured NAS pools.
	• **NAS > Volumes**—Displays information about any currently configured volumes on an existing NAS pool.
	• **Messages**—Displays system messages for the solution.
	• **Performance**—Displays performance metrics for individual drives, network connections, and the CPUs in the integrated server.
	• **Reports**—Provides controls for generating reports about the configuration and status of the solution. Reports can be generated in XML or JSON (JavaScript Object Notation) formats.

Menu	Available Options
Support	The **Support** menu provides access for maintenance and troubleshooting options for the BlackPearl NAS solution. • **Software**—Provides controls for updating the BlackPearl software. • **Activation Keys**—Provides controls for entering activation keys. • **Logs**—Displays any current ASL sets on the solution and provides controls for generating a new log set. • **Documentation**—Displays links to BlackPearl NAS documentation. • **Contact Information**—Displays contact information for Spectra Logic Technical Support, as well as the part and serial numbers for the solution. • **Tools > Data Integrity Verification**—Provides a tool for data integrity verification of storage pools.
Logout	Logs the current user out of the BlackPearl user interface and returns to the login screen.

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

Status Bar	Available Options
Hardware	Provides an at-a-glance status of the overall health of the BlackPearl NAS solution. Clicking this link takes you to the Hardware screen. For more information see View the Status of Hardware Components on page 208.
Messages	Displays the severity, date, and time of the highest severity unread message. Clicking this link takes you to the Messages screen. **Note:** This link does not display if there are no current system messages. For more information see Check System Messages on page 207.
Power	Provides controls for rebooting and shutting down the solution. For more information see Reboot or Shut Down a BlackPearl NAS Solution on page 218. **Note:** The connection to the user interface is lost after running the reboot command. Wait while the solution reboots before attempting to reconnect to the user interface.

Status Icons

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

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

Supported Browsers

The BlackPearl user interface supports the following standard web browsers:

- Google® Chrome™ version 22 or later

- Mozilla® FireFox® version 27 or later

- Apple® Safari® version 7 or later

- Microsoft Internet Explorer® version 11 or later

- Microsoft Edge® version 79.0.309 or later

- Opera Software Browser version 12 or later

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

COMMAND LINE INTERFACE

The command line interface provides text-based configuration, management, and monitoring of the Spectra BlackPearl NAS Solution. 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 solution. 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 - INITIAL CONFIGURATION

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

BEFORE YOU BEGIN

If your BlackPearl NAS solution 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 86 to begin using your BlackPearl NAS solution.

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, contact Spectra Logic Technical Support for instructions.
- For a Gen2 X, S, or V Series see the *BlackPearl NAS Solution 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 system. Use one of the sections below to install the drives.

- Install a Drive in a Gen3 H Series Chassis on page 240
- Install a Drive in a Gen2 S Series Chassis on page 247
- Install a Drive in a Gen2 V Series Chassis on page 248
- Install a Drive in a Gen2 X Series Chassis on page 249
- Install a Drive in a Gen1 Chassis on page 251

CONNECT ETHERNET CABLES

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

- For a Gen3 H Series see Rear Panel on page 29.

- For a Gen2 X Series see Rear View on page 37.

- For a Gen2 S or V Series see Rear Panel on page 44.

- For a Gen1 P, S, or V Series, see Rear Panel on page 53.

AUTOMATICALLY IMPORT ACTIVATION KEYS

Activation keys enable features on the BlackPearl NAS solution. They are tied to the serial number of the solution for which they are issued, and cannot be used on another solution. There are two types of activation keys; feature keys to enable features like NAS and the Vail application, and capacity keys that determine the amount of disk and tape storage available.

Renewals of expired activation keys are obtained by contacting Spectra Logic Technical Support (see Contacting Spectra Logic on page 7).

The USB device in the BlackPearl documentation kit contains the activation keys for the options that you purchased.

Note: If your BlackPearl NAS documentation kit does not contain a USB device, see Manually Enter Activation Keys on page 197 for instructions for manually entering the activation keys.

Follow these steps to import the keys.

1. Insert the USB device into a USB port on the back of the solution. See one of the following for the location of the Ethernet ports on the rear of the master node:

- For a Gen3 H Series see Rear Panel on page 29.
- For a Gen2 X Series see Rear View on page 37.
- For a Gen2 S or V Series see Rear Panel on page 44.
- For a Gen1 P, S, or V Series, see Rear Panel on page 53.

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

2. Power on the solution using the instructions in Power On the Solution on the next page.

3. Wait while the BlackPearl NAS solution performs its power-on sequence.

| ⚠️ | IMPORTANT | Do not remove the USB device until after the solution power cycles and the BlackPearl user interface displays a message that it is safe to remove the USB device. |

POWER ON THE SOLUTION

Use the instructions in this section to power on a BlackPearl NAS solution, and optionally, a 44-bay, 77-bay, 96-bay, or 107-bay expansion node. During the power-on sequence, the BlackPearl NAS solution 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 72.

   • 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 25 on page 59 and Figure 16 on page 48), 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.
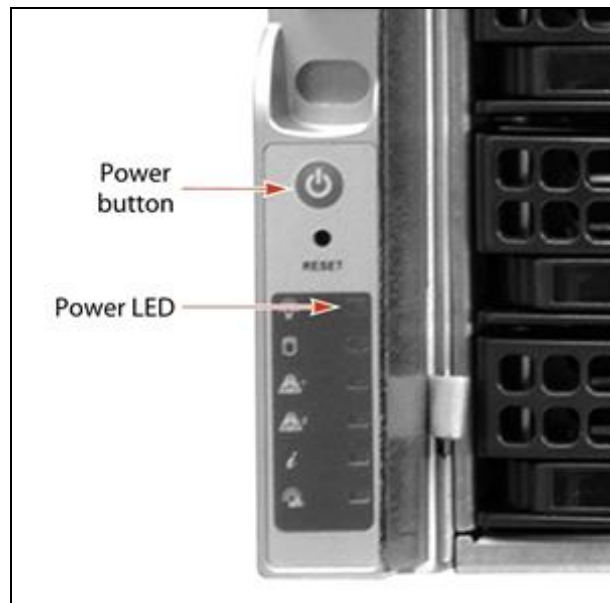

Figure 27 Press the power button.

2. To power on a BlackPearl Gen1, Gen2, or Gen3 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 H Series see Rear Panel on page 29.
- For a Gen2 X Series see Rear View on page 37.
- For a Gen2 S or V Series see Rear Panel on page 44.
- For a Gen1 P, S, or V Series, see Rear Panel on page 53.

Then plug the power cables into power outlets near the chassis. Wait while the BlackPearl NAS solution 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 solution. See Reboot or Shut Down a BlackPearl NAS Solution on page 218.

CONFIGURE THE BLACKPEARL MANAGEMENT PORT

	IMPORTANT	You must connect Ethernet cables as described in Connect Ethernet Cables on page 68 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 76.

* 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 76, then use the instructions in Configure the Management Port on page 116

    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 267 for an alternate method.

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

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:

The Console screen displays.

Figure 28 The Console screen.

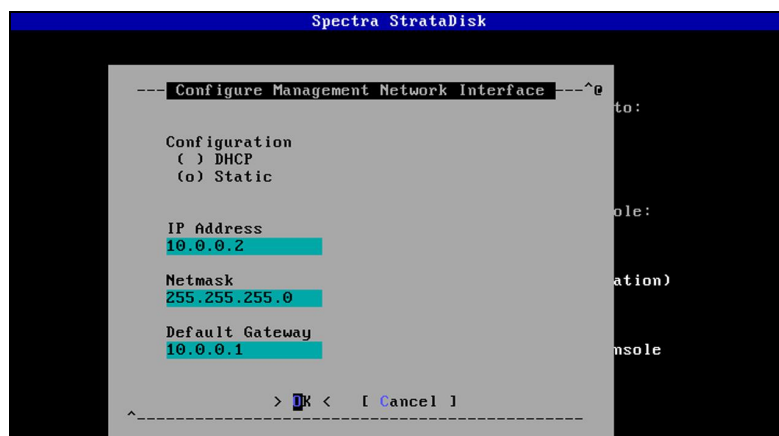2. Press **CTRL-N**. The Configure Management Network Interface screen displays.

Figure 29 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 solution.

LOG INTO THE BLACKPEARL USER INTERFACE

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

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

Note: To log into the BlackPearl user interface on a system that is configured to use Multi-Factor Authentication, see Log In to a System Configured to Use Multi-Factor Authentication on page 172.

1. Using a standard web browser, enter the IP address for the BlackPearl management port configured in Configure the BlackPearl Management Port on page 73.

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 solution 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 125.

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.
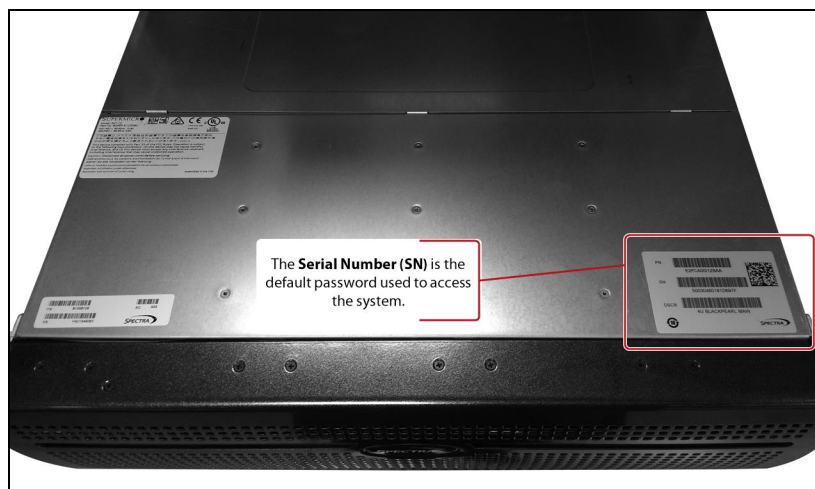

Figure 30 The BlackPearl serial number sticker.

Notes:
- Spectra Logic recommends that you change the default password for the primary administrator (see Edit a User on page 194).

- If you are running BlackPearl OS 4.0 through 5.3, the default username is **Administrator** and the default password is **spectra**.

- If this is the first time that you log in after importing activation keys, an informational message displays indicating that you can now safely remove the USB device. See Automatically Import Activation Keys on page 70 for instructions for closing the message.
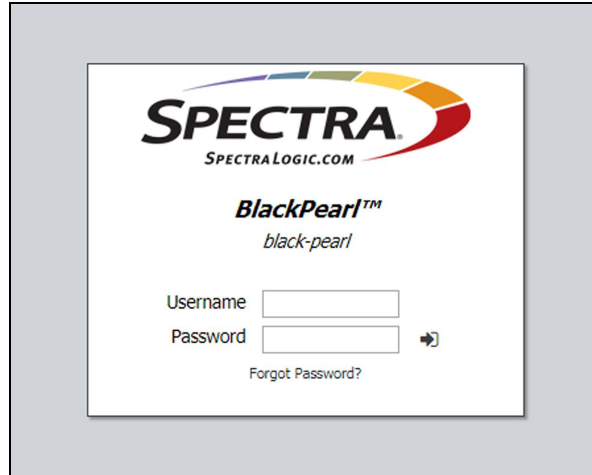
Figure 31 The BlackPearl Login screen.

4. Click ⏻ to log in.

⚠️ **IMPORTANT** The remainder of this guide assumes that you are logged in to the BlackPearl user interface.

CONFIGURE THE DATA CONNECTION

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

Notes:
- You can create one or more data connections to the solution.
- You can configure link aggregation for better performance.
- While different types of Ethernet network interface cards can be installed in the same BlackPearl NAS solution, 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.
- For a BlackPearl HotPair configuration, see the *Spectra BlackPearl HotPair Installation & Configuration Guide* for information on configuring data connections.

Configure an Aggregate Port Data Connection

Link aggregation uses multiple Ethernet ports, configured with a single MAC address, to improve data transfer speeds. See Link Aggregation on page 134 for more information.

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

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

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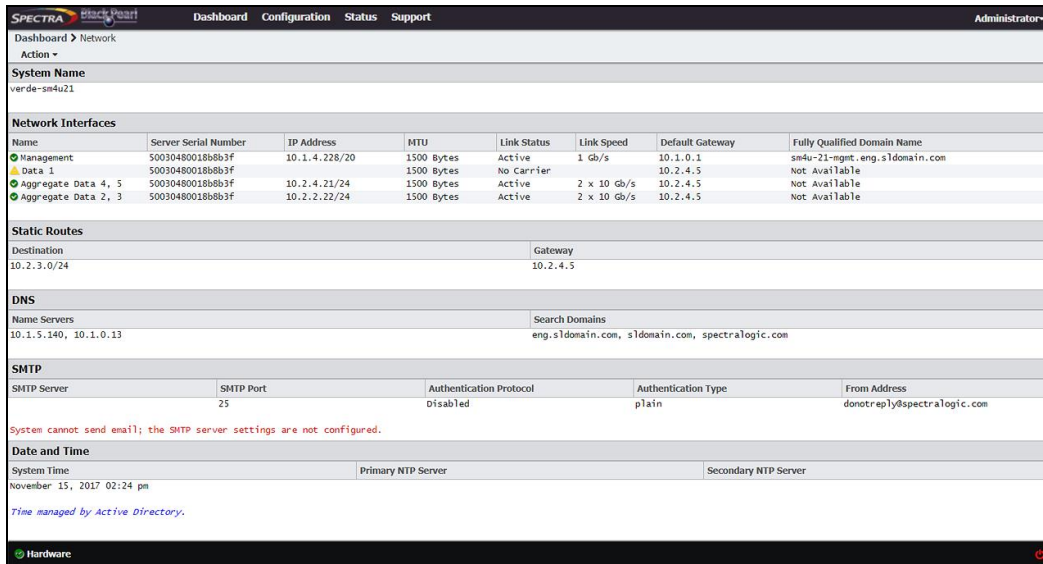

Figure 32 The Network screen.

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

Note: Depending on your hardware configuration, the New Aggregate Interface dialog box may look different than what is shown below.
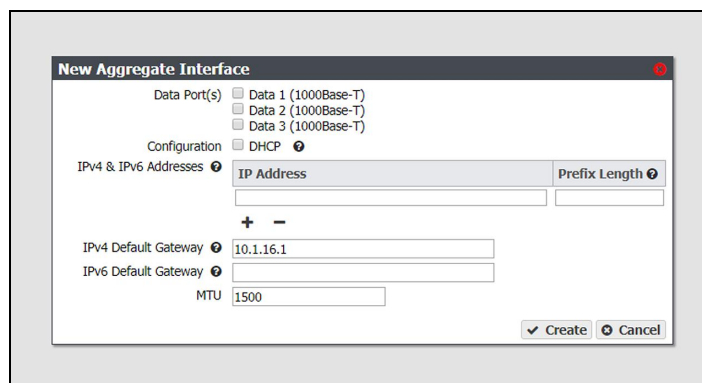
Figure 33 The New Aggregate Interface dialog box.

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

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

5. To configure a static IP address, click the **+** button and enter the following information:

- **IP Address**—Enter a valid IPv4 or IPv6 address.

Note: You cannot enter an IPv4 address if you selected DHCP in Step 4.

- **Prefix Length**—Enter the subnet mask.

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

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

Notes:
- If you selected DHCP in Step 4, this option is unavailable.
- The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl NAS solution.

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

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

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

9. Click **Create**.

Configure a Single Port Data Connection

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

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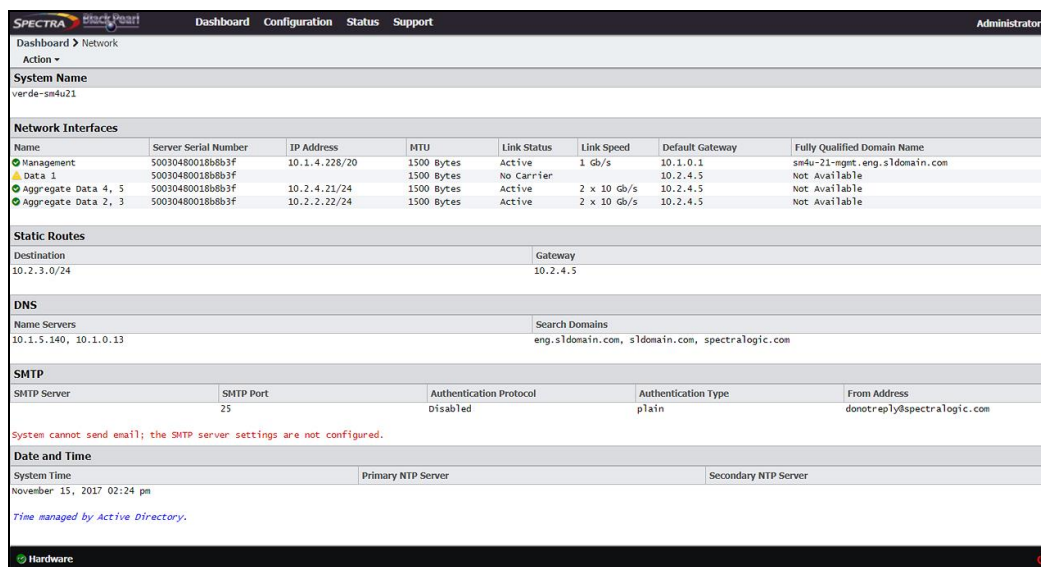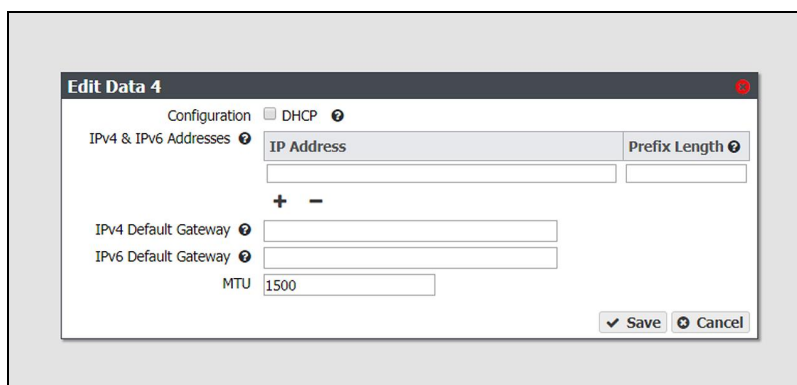

Figure 34 The Network screen.

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

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

Figure 35 The Edit Data # dialog box.

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

4. To configure a static IP address, click the **+** button and enter the following information:

  - **IP Address**—Enter a valid IPv4 or IPv6 address.

Note: You cannot enter an IPv4 address if you selected DHCP in Step 3.

  - **Prefix Length**—Enter the subnet mask.

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

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

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

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

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

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

8. Click **Save**.

Configure a Static Route

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

When configuring a solution 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 solution, a static route is required in order for the solution 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 solution to route communication with the 10.2.3.x network through the data connection on the 10.2.4.x network.

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

   Note: Static routes are only used with IPv4 addresses.

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

1. From the menu bar, select **Configuration > Network**, or select the Network pane from the Dashboard screen. The Network screen displays (see Figure 34 on page 81).

2. From the menu bar, select **Action > New Static Route**. The Static Route dialog box displays.
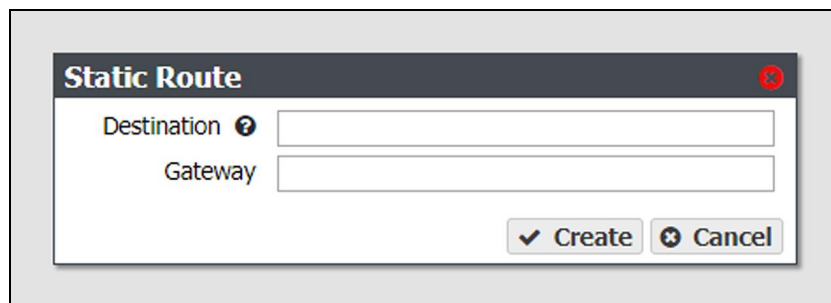
Figure 36 The Static Route dialog box.

3. In the **Destination** field, enter either an IPv4 host address or network address that you want to access through the data connection.

4. Enter the **Gateway** of the data connection used to communicate with the isolated network.

5. Click **Create**.

6. Repeat Step 2 through Step 5 for each host computer on the isolated network.

Additional Network Configuration

See Network Configuration on page 114 for instructions on configuring the management port, networking services, and adding SSL certificates.

CREATE A USER

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

Description of User Types

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

User	Description
Administrator	An administrator account is created by default. This account can access the BlackPearl user interface and has full control over all user interface functions. The default username for the primary administrator is **Administrator**, and 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. The administrator account is automatically created without any permissions. **Notes:** • Spectra Logic recommends changing the password for the primary administrator. See Edit a User on page 194. • If you are running BlackPearl OS 4.0 through 5.3, the default username is **Administrator** and the default password is **spectra**.
Monitor User	The monitor user account is created by default. This account 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 create a snapshot, but do not have access to an administrator account. The default username and password are both **monitor** using all lowercase letters. **Notes:** • Spectra Logic recommends that you change the initial password for the default monitor account. See Edit a User on page 194. • The monitor user can open any menu or function and attempt to edit settings, but these changes are ignored when the monitor user attempts to save the changes.
Login User	A user with Login permissions 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.

User	Description
CIFS User	A user with CIFS permission is able to access CIFS shares in a Windows workgroup environment.
SpectraApp	A user with SpectraApp permission is required to load the BlackPearl embedded dashboard in to the Spectra Vail, 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. From the menu bar, select **Configuration > Users.** The Users screen displays.

Figure 37 The Users screen.

2. Select **Action > New** from the menu bar. The New User dialog box displays.
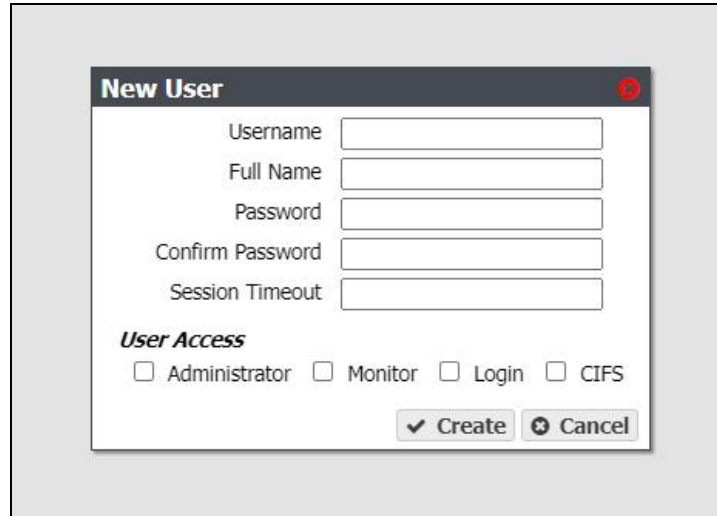
Figure 38 The New User dialog box.

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 Types on page 84
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 next steps depend on if you are configuring a BlackPearl NAS solution as a standalone
product, or if you plan to use your BlackPearl NAS solution in conjunction with a BlackPearl
nearline gateway.

- If you have a standalone BlackPearl NAS solution, continue to Configuring Network
  Attached Storage on page 87.

- If you plan to use your BlackPearl NAS solution with a BlackPearl nearline gateway,
  skip to Network File Interface on page 283.

CHAPTER 3 - 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 solution.

OVERVIEW OF NAS STORAGE POOLS, VOLUMES, AND SHARES

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

Storage Pools

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

Volumes and Shares

Volumes are located on each storage pool. Volumes can be configured with a minimum size and thin provisioned with a maximum size. When you create a volume, you can specify whether it uses compression, and whether the time stamp for files is updated when the file is read (access time). After the volume is created, it can be shared (made available for use by other computers on the network) via either the NFS service or the CIFS service.

Naming Considerations

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

Using BlackPearl NAS with the Spectra StorCycle Application

The StorCycle application can use symbolic links (symlinks). However, the BlackPearl NAS solution does not support symlinks. See the *StorCycle Application User Guide* for more information.

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 as described in Delete a Storage Pool on page 143. 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 solution 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. From the menu bar, select **Configuration > NAS > Pools**, or click the Pools pane on the Dashboard. The NAS Pools screen displays.

Figure 39 The NAS Pools screen.

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

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

Figure 40 The New Pool dialog box.

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

For this option....	Do the following...
Name	Enter a name for the pool. Pool names are limited to 48 characters. **Notes:** • The combined storage pool and volume name must be 78 characters or fewer. To avoid problems sharing volumes, Spectra Logic recommends a pool name of 32 characters or fewer. • Each pool name must be unique. This field is case sensitive. Only the following special characters are allowed: hyphen (-), underscore (_), colon (:), and period(.).
High Water Mark	Enter a percentage. When the used space on the pool reaches this percentage, an alert is generated. Enter 0 if you do not want to set an alert level.
Power Saving Mode	Using the drop-down menu, select the desired **Power Saving Mode**. Enabling the power saving mode sets the standby timer to 60 minutes for all drives in the pool, but only if all drives in the pool are capable of using a standby timer. When the disk pool is idle for 60 minutes, the drives spin-down to conserve power. **Notes:** • Spectra Logic recommends leaving power saving mode **disabled**. • To use this feature, all drives in the storage pool must be power-saving compatible.
Auto Trim (not pictured)	Select to enable Auto Trim on SSD and NVMe drives. Auto trim automatically clears unused data blocks from SSD or NVMe drives, which improves both performance and longevity. When enabled, files that are deleted are promptly marked for reuse, helping to maintain drive speed by reducing write amplification. This also prolongs drive lifespan by minimizing unnecessary write operations.
Select Drives To Use	Use the drop-down menu to select the number of drives to include in the pool. If your solution contains more than one type of disk drive, multiple drop-down menus are present, but only one type can be assigned to a pool. Any drive not in a storage pool acts as a global spare. A global spare drive is activated as soon as a drive configured in a storage pool fails.

For this option....	Do the following...
Select Protection Level	Use the radio buttons to select the protection level for the pool. Only one option can be selected. Use the Storage Pool Preview information to compare the fault tolerance and required overhead for each configuration.
	None—The pool is not configured to provide data protection. Any drive failure results in data loss.
	Mirror—Data is striped across two mirrors. Any detected data corruption is corrected using checksums. This type of RAID offers the best performance for small random reads and writes.
	Single parity—Data is striped across multiple single-parity arrays, which can tolerate one drive failure without data loss. This type of RAID has faster performance than double- and triple-parity based RAIDs.
	Double parity—Data is striped across multiple double-parity arrays, which can tolerate two drive failures without data loss. In most cases, double-parity provides the best balance between data protection, performance, and storage capacity.
	Triple parity—Data is striped across multiple triple-parity arrays, which can tolerate three drive failures without data loss. This type of RAID provides the most data protection.
Select Optimization Level	Use the slider to maximize either pool capacity or performance, or to mix the two options. Greater capacity means more storage space but slower performance. Higher performance means the pool is faster at reading or writing data with less overall capacity.
	Note: The Storage Pool Preview pane of the New Pool screen changes as you move the slider between Capacity and Performance to show the impact your changes have on the storage pool.
Select Write Performance	Use the drop-down menu to select the number of drives to use to increase write performance when the pool is shared using NFS. This feature is only intended for storage pools with NFS shares and typically has little impact on CIFS share performance.
Select Metadata Performance	Use the drop-down menu to select the number of drives to use to 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.
	Note: Metadata Performance drives can only be selected in multiples of three.
	Note: These drives are permanently part of the storage pool and cannot be removed.

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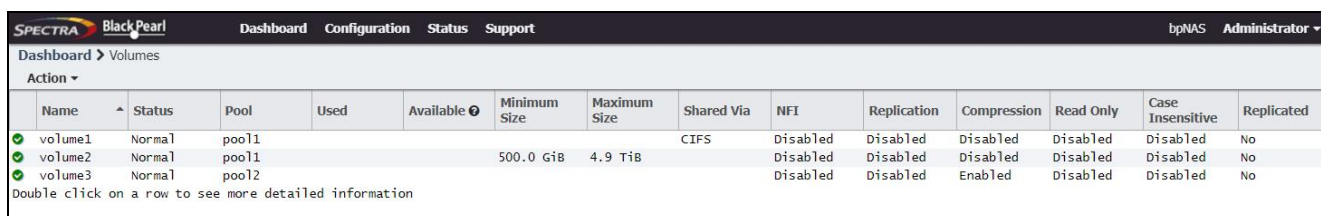
CREATE A VOLUME

Before you begin using a 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.

Note: If you want to configure the volume to use the NFI service (Network File Interface) to automatically transfer files from the NAS storage to a BlackPearl Nearline gateway, configure the NFI service before configuring the volume. See Network File Interface on page 283

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

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

Name	Status	Pool	Used	Available	Minimum Size	Maximum Size	Shared Via	NFI	Replication	Compression	Read Only	Case Insensitive	Replicated
volume1	Normal	pool1					CIFS	Disabled	Disabled	Disabled	Disabled	Disabled	No
volume2	Normal	pool1			500.0 GiB	4.9 TiB		Disabled	Disabled	Disabled	Disabled	Disabled	No
volume3	Normal	pool2						Disabled	Disabled	Enabled	Disabled	Disabled	No

Double click on a row to see more detailed information

Figure 41 The Volumes screen.

2. Select **Action > New**. The New Volume dialog box displays.

Figure 42 The New Volume dialog box.

3. Configure the volume as required for your environment.

For this option....	Do the following...
Name	Enter a name for the new volume. Volume names are limited to 62 characters or fewer. **Notes:** • The combined 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.
Pool	Select the disk pool on which to create the volume. If there are multiple disk pools configured on the solution, use the drop-down menu to select the **Pool** where you want to create the volume.

For this option....	Do the following...
Minimum Size	Select the desired unit size from the drop-down menu and enter a numerical value for the minimum size in the text box to the left of the unit size drop-down menu. This space is allocated immediately if there is sufficient space available on the 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.
Maximum Size	Select the desired unit size from the drop-down menu and enter a numerical value for the maximum size in the text box to the left of the unit size drop-down menu. **Notes:** • Volumes are thin provisioned, so it is possible for the combined allocated maximum storage of all volumes to exceed the physical space available. • Leave the **Minimum Size** and **Maximum Size** blank to create the volume with access to all available space on the disk pool.
Snapshot Change Threshold	Specify 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. • Allowed values are between 0 and 99. **Note:** Spectra Logic recommends configuring the Administrator user to receive emails when a warning event occurs. **Note:** The BlackPearl NAS solution 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.
Case Insensitive (CIFS)	If desired, select this option to configure the volume to treat all names as case insensitive, which can improve performance, especially in situations where directories contain a large number of files. **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.

For this option….	Do the following…
Compression	If desired, select the check box to enable data compression using ZFS LZ4 algorithm to allow the BlackPearl NAS solution 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 solution. This impact is less evident with Gen2 and Gen3 master nodes.
Access Time	If desired, select the check box to configure the solution to update the time stamp of a file when it is read from the volume. Selecting **Access Time** may slow performance.

Configure the 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 Nearline gateway. If desired, see Network File Interface on page 283 for instructions for configuring the NFI Volume Policy.

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

CREATE A SHARE

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

- Create a CIFS Share, below

- Create an NFS Share on page 101

Note: Shares are not available until network settings are configured. See Configure the Data Connection on page 78.

Create a CIFS Share

Spectra Logic recommends using Active Directory to control access to CIFS shares on the BlackPearl NAS solutions. To do this, continue with Join an Active Directory Domain, below.

However, if your Windows operating system environment does not use Active Directory, you can enable local administrator status on the solution to allow a specified user to access the CIFS shares in a Windows workgroup environment. The username and password configured on the BlackPearl NAS solution are used to access the CIFS shares when using a Windows workgroup environment. To do this, continue with Enable Local Administrator Status.

Join an Active Directory Domain

If your Windows environment uses Active Directory, you must join an Active Directory domain before creating a CIFS share. See Configure the Active Directory Service on page 127 for more information. After joining the Active Directory domain, continue with Create a CIFS Share on page 99.

Enable Local Administrator Status

If your Windows environment does not use Active Directory, you must edit a user to enable local administrator status.

> **Note:** Alternatively, you can create a new user with local administrator status. See Create a User on page 84.

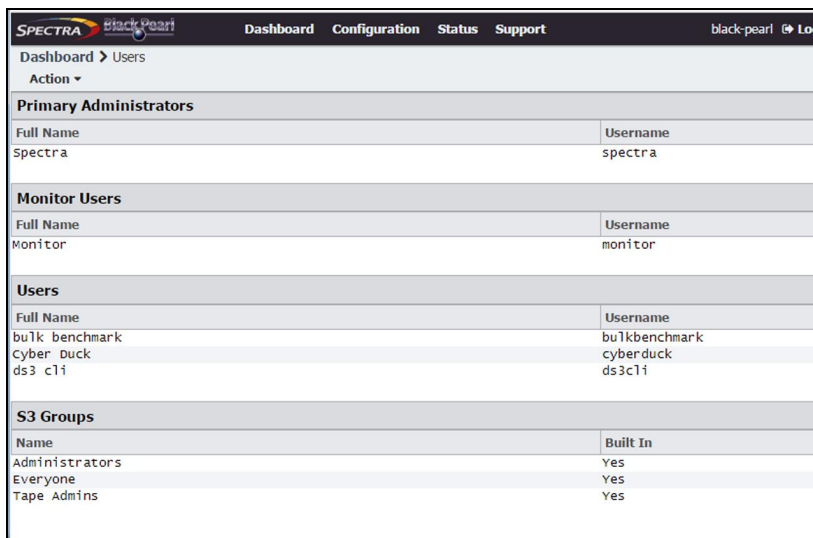1. From the menu bar, select **Configuration > Users**. The Users screen displays.

Figure 43 The Users screen.

2. Double-click the row for the user for which you want to enable local administrator status, or select the user, and then select **Action > Edit**. The Edit User dialog box displays.
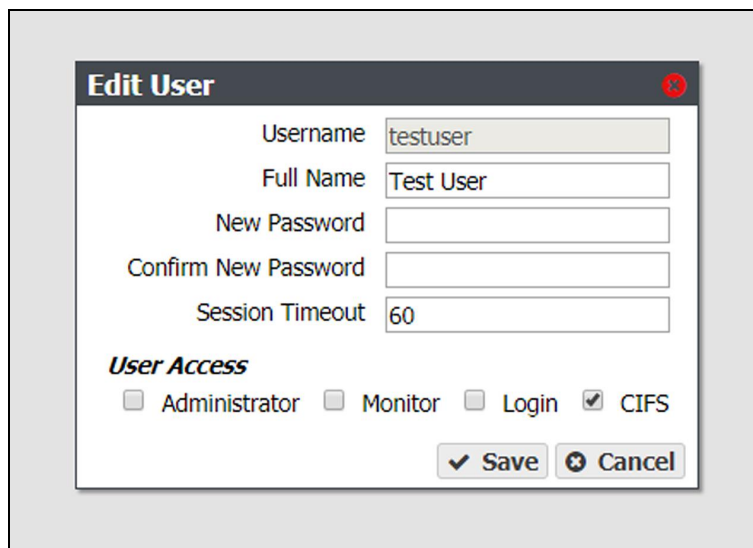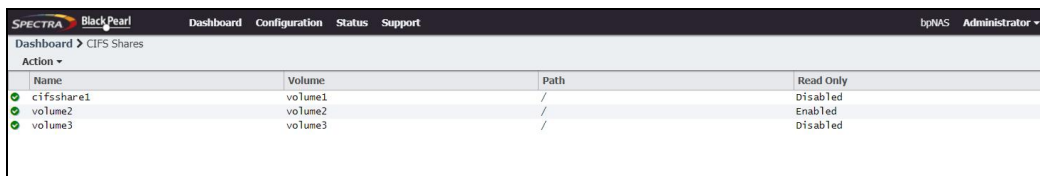
Figure 44 The Edit User dialog box.

3. Select the **CIFS** checkbox to enable the user to access CIFS shares in a Windows workgroup environment.

4. If desired, change other settings as described in Edit a User on page 194.

5. Click **Save**.

Create a CIFS Share

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

Figure 45 The CIFS Shares screen.

2. Select **Action > New**. The New CIFS Share dialog box displays to show the options for creating a new share.
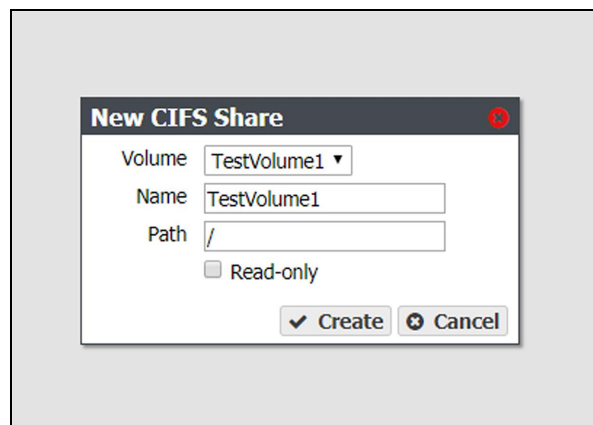
Figure 46 The New CIFS Share dialog box.

3. Use the drop-down menu to select the **Volume** you want to share.

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

4. Set the **Name** for the CIFS share. This is the name that is displayed in Active Directory configurations.

5. The network address displayed for **Path** is the address of the share you are currently configuring. The default path allows access to the root of the volume.

Notes:
- After creating the CIFS share, you can connect to it using your Windows-based host and create subdirectories in the share. You can then edit the share and use the **Path** field to allow access to specific directories by specifying the exact subdirectory (see Edit a CIFS Share on page 159).

  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.

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

6. If desired, select **Read-only** to configure the CIFS share as read only.

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

Set Permissions for 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.
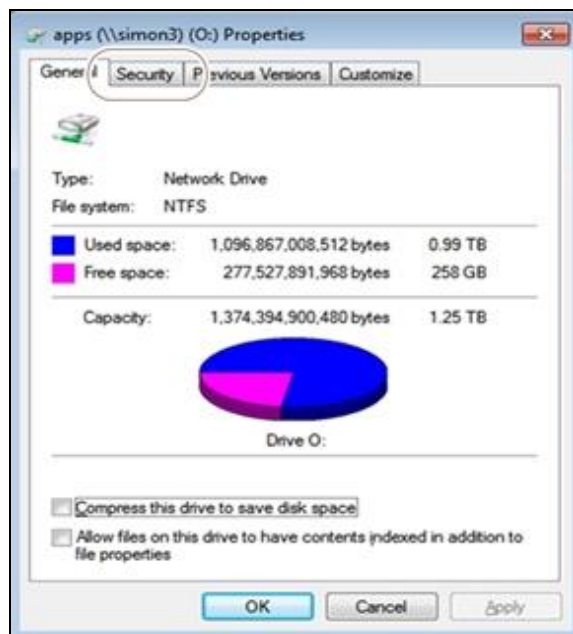

Figure 47 The Properties window.

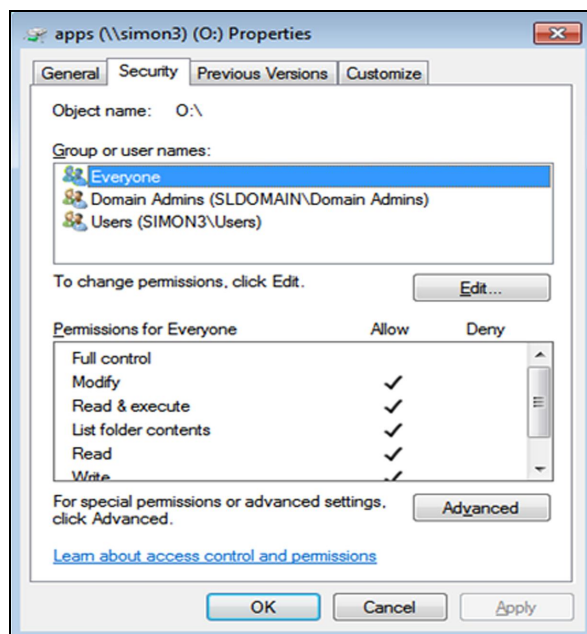**3.** Click **Security**. The Security tab displays.

Figure 48 The Security tab.

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

5. Click **OK**.

Note: Starting with BlackPearl OS 5.4, 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.

Create an NFS Share

Use the following steps to create an NFS share.

1. From the menu bar, select **Configuration > NAS > Shares > NFS**. The NFS Shares screen displays.
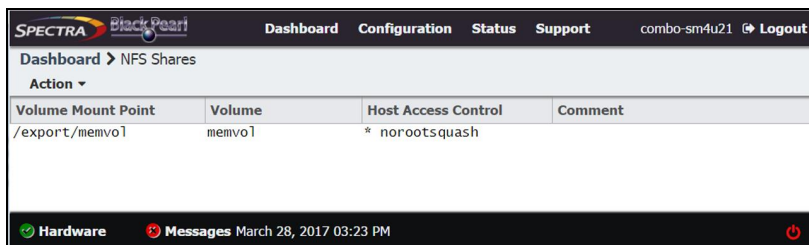
Figure 49 The NFS Shares screen.

2. Select **Action > New**. The New NFS Share dialog box displays.
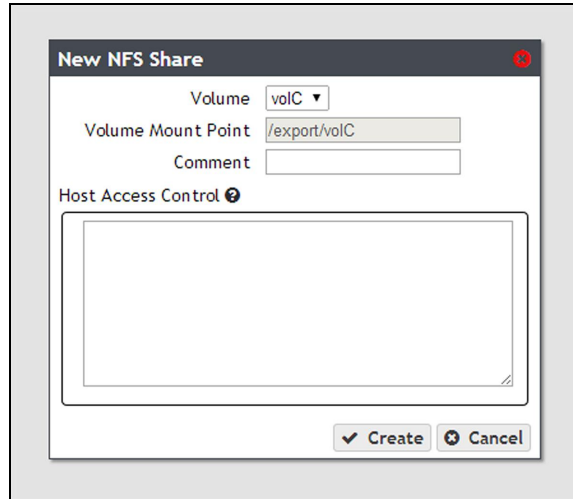
Figure 50 The New NFS Share dialog box.

3. Use the drop-down menu to select the **Volume** you want to share.

4. The network address displayed for **Volume Mount Point** is the address of the share you are currently configuring.

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

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

6. 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 solution.

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

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

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

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

Create a Vail S3 Share

Use the following information to create a Vail S3 share.

Notes:
- You can only create a Vail S3 share after registering the BlackPearl NAS solution to a Vail sphere. See Configure a Vail Sphere on page 176 for more information.

- You cannot create a Vail S3 share on a volume configured to use NFI replication.

1. From the menu bar, select **Configuration > NAS > Shares > Vail S3**. The Vail S3 Shares screen displays.

2. Select **Action > New**. The New Vail S3 Share dialog box displays.
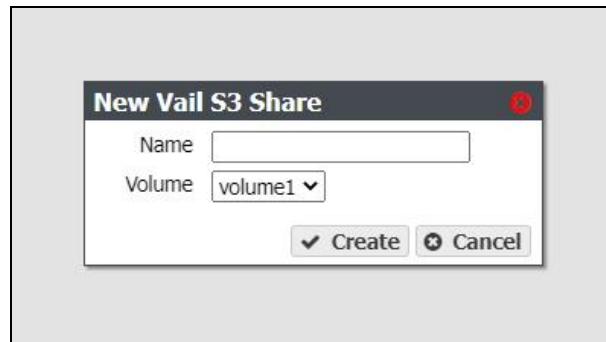
Figure 51 The New Vail S3 Share dialog box.

3. Enter the desired **Name** of the Vail S3 share.
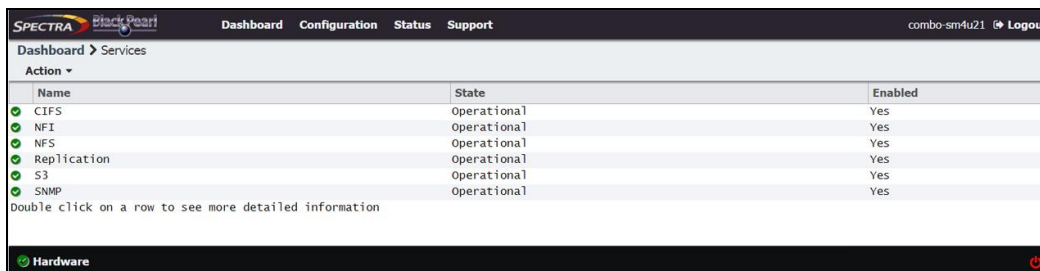
  Note: You cannot rename a Vail S3 share after it is created.

4. Click **Create**.

Configure NAS Services

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

Note: For information about networking services see Configure Network Connections and Settings on page 115.

Figure 52 The Services screen.

Configure the CIFS Service

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

Note: For information about using CIFS shares and joining an Active Directory domain, see Create a CIFS Share on page 97.

Add Advanced Parameter

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

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

---

1. From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 52 on page 104).

2. Double-click the **CIFS** row, or select the **CIFS** row and select **Action > Show Details**. The CIFS details screen displays.

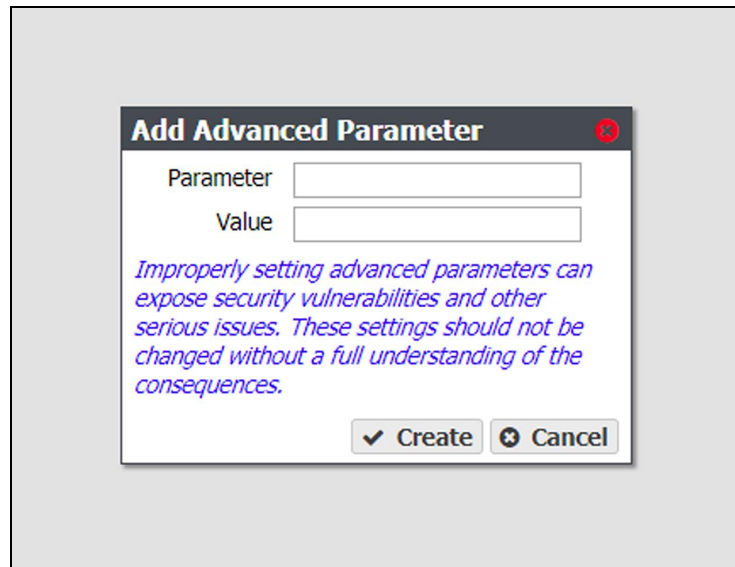3. Select **Action > Add Advanced Parameter**. The Add Advanced Parameter dialog box displays.

Figure 53 The Add Advanced Parameter dialog box.

4. Enter the desired **Parameter** and **Value**.

5. Click **Create**.

Configure the NFI Service

The NFI service (Network File Interface) automatically transfers files from the NAS volumes on the solution to BlackPearl managed object storage on a BlackPearl gateway.

> ⚠ **IMPORTANT**   See Network File Interface on page 283 for instructions for configuring NFI.

Note: This service is only for transferring files from NAS volumes on the solution to BlackPearl managed object storage on a BlackPearl Nearline gateway. To replicate NAS volumes to BlackPearl gateways with NAS enabled or to other BlackPearl NAS solutions use the NAS replication service (see Configure NAS Services on the previous page).

Configure the NFS Service

The BlackPearl user interface lets you configure the transmission protocols and number of threads used by the NFS service. Use the following steps to edit the NFS service.

1. Select **Configuration > Services** to display the Services screen (see Figure 52 on page 104).

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

3. On the NFS service details screen, select **Action > Edit**. The Edit NFS Service dialog box displays.
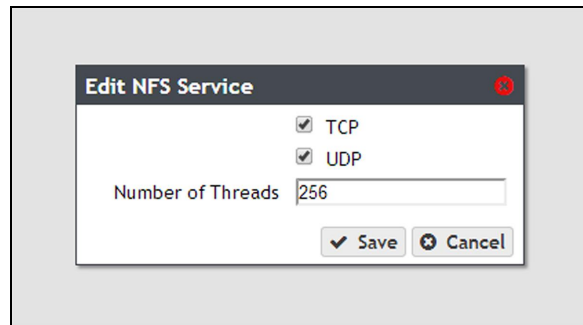

Figure 54 The Edit NFS Service dialog box.

4. Select or clear the **TCP** and **UDP** transmission protocols to enable or disable them, respectively.

5. Set the number of **Threads** for use by the service.

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

6. Click **Save**.

CONFIGURE NAS REPLICATION

If the BlackPearl NAS solution is on a network with Verde arrays, other BlackPearl NAS solutions, or BlackPearl gateways with NAS enabled, you can select to replicate data from the NAS volumes on the solution to one or multiple NAS replication targets. Replication uses the same data interface that the solution 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 gateway. These snapshots can be retained for archival purposes or restored on the target solution to replicate the data contained in the snapshot.

Once you configure the replication service, you need to configure each volume on the solution that you want to replicate. Use the instructions in this section to configure the replication service and to configure volumes for replication.

Notes:
- This replication service is only for replicating NAS volumes on the solution to BlackPearl gateways with NAS enabled or other BlackPearl NAS solutions. To replicate NAS volumes to BlackPearl managed object storage use NFI (see Configure NAS Replication above).

- 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 Ethernet Ports on page 115).

- Your firewall must allow the source solution 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.

Configure the NAS Replication Service

Note: For both the source solution and the targets, make sure you have completed the steps in Initial Configuration on page 67.

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

1. In the source solution's BlackPearl user interface, select **Configuration > Services** to display the Services screen (see).

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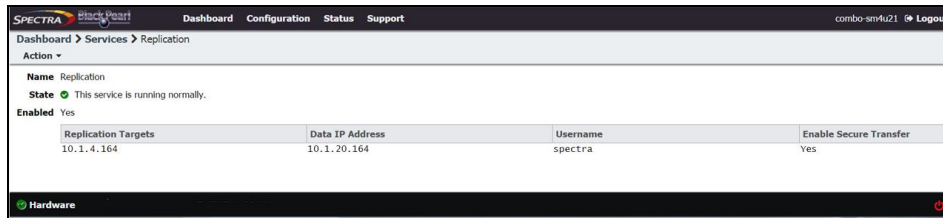

Figure 55 The Replication service details screen.
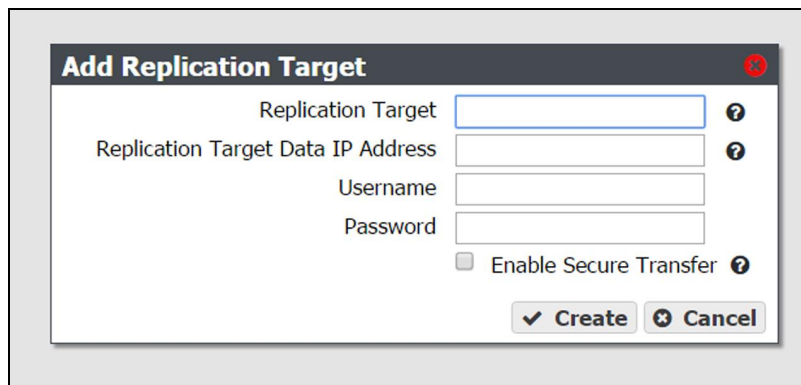
3. Select **Action > Create**. The Add Replication Target dialog box displays.

Figure 56 The Add Replication Target dialog box.

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

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

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

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

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

   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** check box to configure the solution to encrypt the replicated data before transferring it to the target. Data is encrypted using Secure Socket Layer (SSL).

9. Click **Save**.

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 76.

2. Create one or more storage pools as described in Create a NAS Storage Pool on page 89.

3. Create one or more volumes as described in Create a Volume on page 93. You must create one volume on the **target system** for each volume you want to replicate on the **source system**. Otherwise, you can create volumes when performing the steps in Configure Volumes for 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. In the source solution's BlackPearl user interface, select **Configuration > NAS > Volumes**. The Volumes screen displays.

2. Double-click the volume name you want to configure to replicate, or select the volume and select **Action > Show Details**. The details screen for the volume displays.

3. Select **Action > Configure Replication**. The Configure Replication dialog box displays.

Figure 57 The Configure Replication dialog box.

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

5. Select the **Replication Target** from the drop-down menu. The targets are listed by the IP address or hostname entered in Step 4 on page 108. If you only configured the solution to replicate to a single target, the target is preselected.

6. Enter the name of the storage pool on the target you want to use for replication in the **Destination Pool Name**. This field is case sensitive.

7. Enter the name of a volume that resides on the target storage pool you selected in Step 6 in the **Destination Volume Name** field, or enter the name for a new volume to be created on the specified storage pool. This field is not case sensitive.

⚠️ **CAUTION**   You cannot use this volume for normal data storage operations, it can only be used as a replication target. Any data in the specified target volume is deleted each time the solution 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.

8. Select the Hourly, Daily, or Weekly radial button for the **Replication Volume Policy Schedule**. The dialog box changes to show the configuration options for your selection. Use one of the sections below to complete the replication configuration for this volume.

   - Create an Hourly Schedule below— Replicate data every selected number of hours.
   - Create a Daily Schedule on the next page — Replicate data every selected number of days.
   - Create a Weekly Schedule on page 113 — Replicate data on certain days of the week.

Create an Hourly Schedule

Creating an hourly schedule for NAS replication is helpful in the case of a ransomware attack. With an hourly snapshot schedule, only data written in the last hour or less can be compromised by the ransomware attack. Data older than one hour can be restored from the most recent snapshot.

1. Select Hourly as the interval for the replication schedule (see Figure 57 on page 110).

2. Enter numbers for **Every _ hours on 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, the data is replicated every four hours at 15 minutes after the hour. The maximum setting for the **hours** field is 48, where the data replicates every two days. The maximum setting for the **minute** field is 59.

   Note: Spectra Logic recommends offsetting the minutes after the hour for starting replications so that there are not a large number of jobs starting at exactly the same time.

3. Click **Create**.

Create a Daily Schedule

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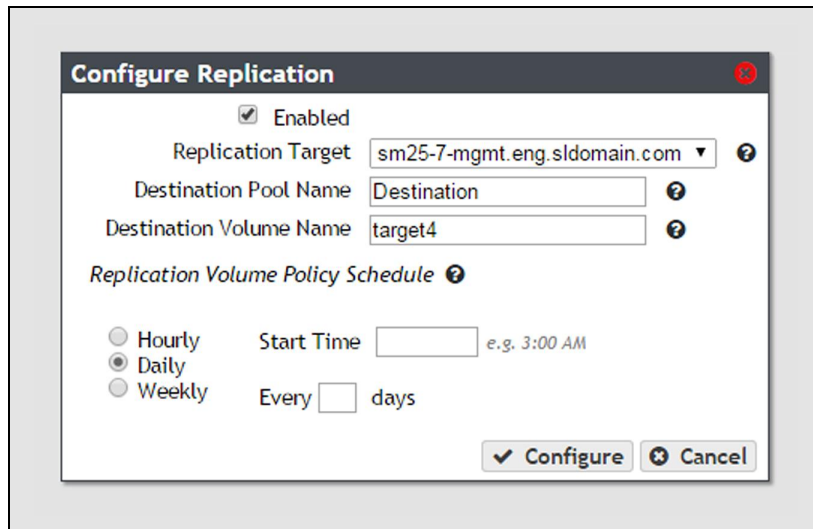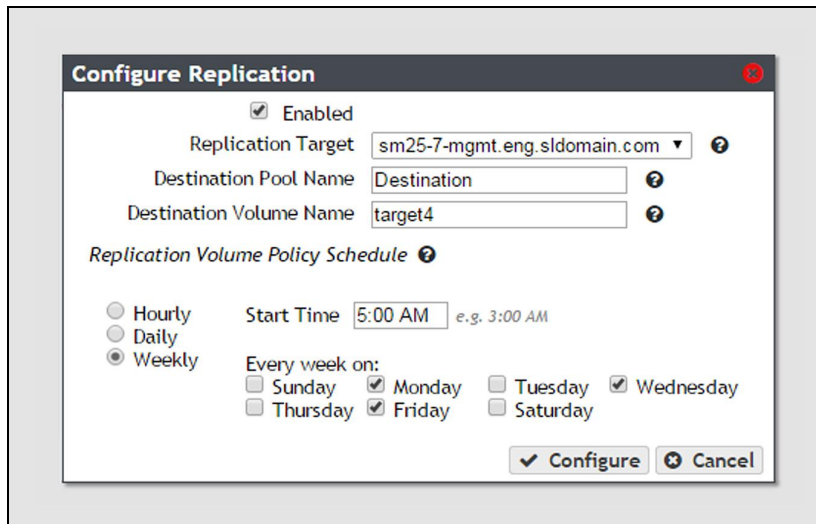

Figure 58 The Configure Replication dialog box showing the daily interval options.

2. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.

3. Enter a number for **Every _ days**. This value specifies the interval, in days, between data replications. The value entered is enumerated from the first day of the month. The schedule resets at the beginning of each month. For example, if this value is set to 2, the NAS volume replicates data every two days, starting with the 1st of the month, at the time specified in Step 2. A value of 30 runs on the 1st of the month, and then again on the 31st of the month (for months that have 31 days). To schedule data replication on the first of every month, set the interval to 31 days.

4. Click **Create**.

Create a Weekly Schedule

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

Figure 59 The Configure Replication dialog box showing the weekly interval options.

2. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.

3. Select one or more days for **Every week on:**. This determines the day(s) of each week the NAS volume replicates data. For example, based on the selections in Figure 59, the NAS volume replicates data every Monday, Wednesday, and Friday at 5:00 AM.

4. Click **Create**.

CHAPTER 3 - NETWORK CONFIGURATION

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

CONFIGURE NETWORK CONNECTIONS AND SETTINGS

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

Note: If configuring a HotPair system, see the *Spectra BlackPearl HotPair Installation & Configuration Guide* for instructions on configuring network connections.

Figure 60 The Network screen.

Configure Ethernet Ports

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

Notes:
- You can create one or more data connections to the solution.

- You can configure link aggregation for better performance.

- While different types of Ethernet network interface cards can be installed in the same BlackPearl NAS solution, 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 Initial Configuration on page 67. 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 Management Port

1. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays (see Figure 60 on page 115).

2. In the Network Interfaces pane, double-click the Management row, or select the Management row and then select **Action > Edit**. The Edit Management dialog box displays.
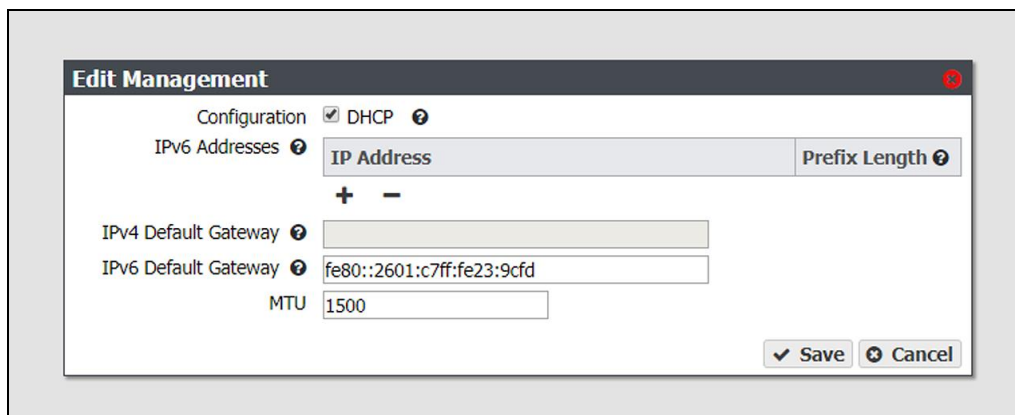
Figure 61 The Edit Management dialog box.

3. Select **DHCP** to configure the solution 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 in Step 3 on page 116.

- **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 **IPv4Default Gateway**.

   Notes:
   - If you selected DHCP in Step 3 on page 116, this option is unavailable.
   - The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl NAS solution.

6. If applicable, enter the **IPv6Default Gateway**.

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

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

8. Click **Save**.

   Note: When you change the IP address of the 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.

Edit an Aggregate Data Connection

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

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

1. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays (see Figure 60 on page 115).

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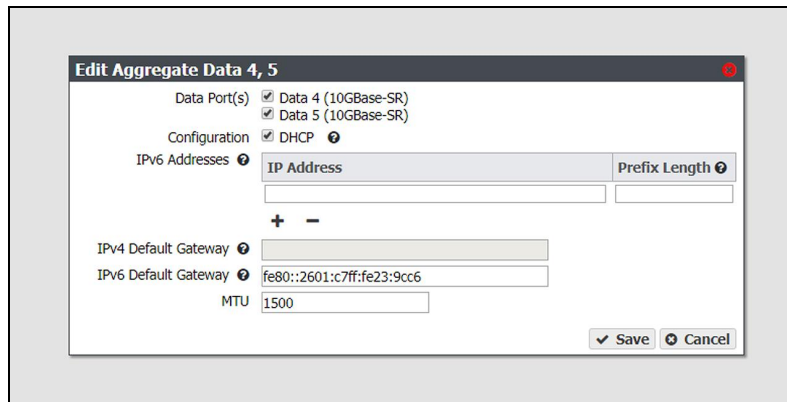

Figure 62 The Edit Aggregate *Data* dialog box.

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

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

5. To configure a static address, click the **+** button and enter the following information:

   • **IP Address**—Enter a valid IPv4 or IPv6 address.

   Note: You cannot enter an IPv4 address if you selected DHCP in Step 4.

   • **Prefix Length**—Enter the subnet mask.

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

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

6. If applicable, enter the **IPv4Default Gateway**.

   Notes: • If you selected DHCP in Step 4, this option is unavailable.

   • The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl NAS solution.

7. If applicable, enter the **IPv6Default Gateway**.

   Notes: • The gateway entered for the last configured IPv6 connection sets the default gateway for the BlackPearl NAS solution.

   • The IPv6 Gateway does not need to be configured when the BlackPearl NAS solution is connected to a SLACC network.

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

9. Click **Save**.

Edit a Data Connection

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

1. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays (see Figure 60 on page 115).

2. Select the row of the data connection you want to edit and select **Action > Edit**. The Edit *Data Connection* dialog box displays.
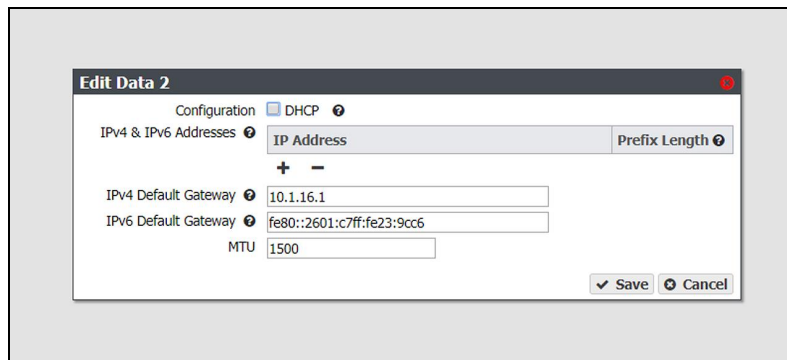
Figure 63 The Edit *Data* # dialog box.

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

4. To configure a static IP address, click the **+** button and enter the following information:

• **IP Address**—Enter a valid IPv4 or IPv6 address.

  Note: You cannot enter an IP address if you selected DHCP in Step 4.

• **Prefix Length**—Enter the subnet mask.

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

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

5. If applicable, enter the **IPv4Default Gateway**.

  Notes: • If you selected DHCP in Step 4, this option is unavailable.

    • The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl NAS solution.

6. If applicable, enter the **IPv6Default Gateway**.

Notes: • The gateway entered for the last configured IPv6 connection sets the default gateway for the BlackPearl NAS solution.

• The IPv6 Gateway does not need to be configured when the BlackPearl NAS solution is connected to a SLACC network.

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

8. Click **Save**.

Edit a Static Route

1. From the menu bar, select **Configuration > Network**, or select the Network pane from the Dashboard screen. The Network screen displays (see Figure 34 on page 81).

2. Double-click the static route you want to edit. The Static Route dialog box displays.
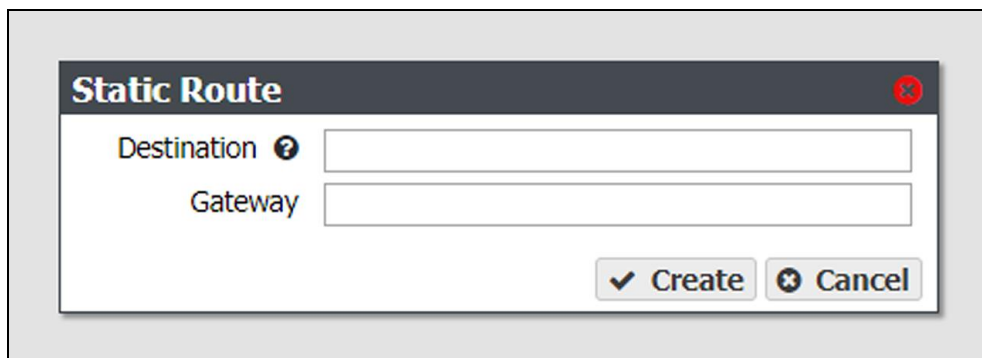
Figure 64 The Static Route dialog box.

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

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

5. Click **Create**.

Clear a Data Port Configuration

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

Note: The management port cannot be cleared. See Configure the Management Port on page 116 to change the management port settings.

1. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays (see Figure 60 on page 115).

2. Select the row of the configuration you want to clear and select **Action > Clear** from the menu bar. A confirmation window displays.

3. Click **Delete** to clear the Ethernet configuration.

Configure DNS Settings

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

1. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays (see).

2. In the DNS pane of the Network screen, double-click the single row, or select the row and then select **Action > Edit**. The Edit DNS screen displays.
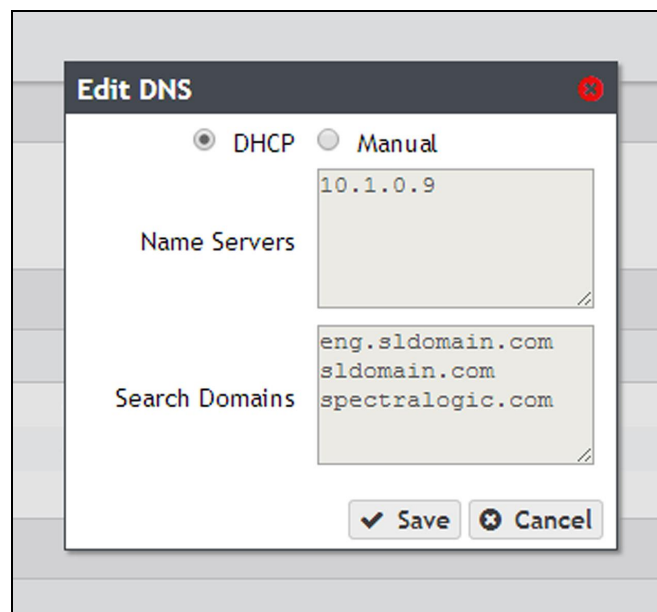
Figure 65 Edit DNS information.

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

—OR—

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

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

4. If the BlackPearl management port is configured with a static IP address, or if you selected **Manual**, enter the following information:

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

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

5. Click **Save**.

Configure SMTP Settings

Use the Email settings to associate the BlackPearl NAS solution with a mail server. The solution uses this SMTP server to send emails whenever ASLs or certain types of messages are generated.

1. From the menu bar, select **Configuration > Network**, or select the Network pane from the Dashboard screen. The Network screen displays.

Figure 66 The SMTP pane of the Network screen.

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

Figure 67 The Email dialog box.

3. Enter the **SMTP Server** and **SMTP Port** information.

4. Using the drop-down menu, select the **SMTP Authentication Type** required by your mail server.

5. If your SMTP server uses TLS (Transport Layer Security) authentication, select the **Enable TLS Authentication** check box and enter the required **Username** and **Password** information.

6. Enter an email address in the **From Address** field. This is the email address that displays as the sender whenever the solution generates an email. This email address should uniquely identify the BlackPearl NAS solution to assist in troubleshooting and be recognized by the SMTP server as a valid domain address.

7. Click **Save**.

Configure Date and Time

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

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

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

1. From the menu bar, select **Configuration > Network**, or select the Network pane from the Dashboard screen. The Network screen displays.

Date and Time		
System Time	Primary NTP Server	Secondary NTP Server
February 19, 2014 01:18 PM	0.freebsd.pool.ntp.org	1.freebsd.pool.ntp.org

Figure 68 The Date and Time pane of the Network screen.

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

Figure 69 The Time Settings dialog box.

3. Select **Manual** or **NTP**.

a. If you select **Manual**, enter the current time in the **Time** field. Enter either 12-hour time values and include AM or PM, or use 24-hour time values. Click the empty **Date** field. A calendar appears. Select the current date.

b. If you select **NTP**, enter the NTP server information for the **Primary NTP Server**. If desired, enter the NTP server information for the **Secondary NTP Server**.

4. Click **Save**.

Edit the System Name

1. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays.

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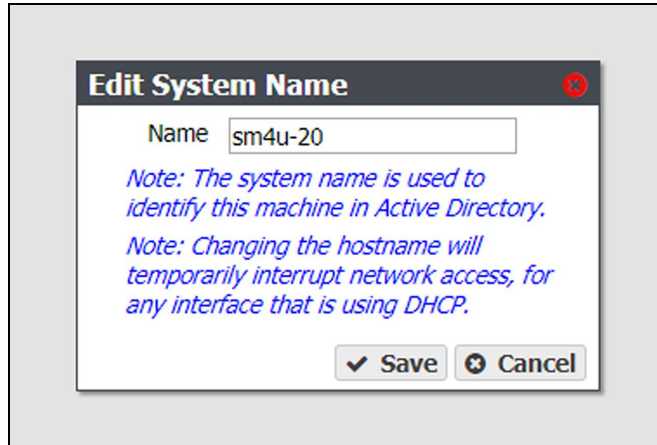

Figure 70 The Edit System Name dialog box.

3. Enter the desired **Name** for the solution. The solution 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 - BlackPearlSolution.domain.com

- If your solution is using BlackPearl OS 3.2.2, or earlier, there are no character restrictions on system names. However, Spectra Logic recommends limiting system names to letters, numbers, and hyphens to maintain compatibility with the RFC 1123 standard.

- The solution does not change previously configured system names using special characters when upgrading to BlackPearl OS 3.3, or later.

4. Click **Save**.

CONFIGURE CERTIFICATES

The BlackPearl NAS solution ships with non-signed SSL certificates for both the data and management ports on the solution. 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 solution accepts intermediate (chain) SSL certificates, and accepts RSA, DSA, and ECC certificates. The BlackPearl NAS solution accepts both encrypted and non-encrypted certificates.

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

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

Figure 71 The Certificates screen.

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

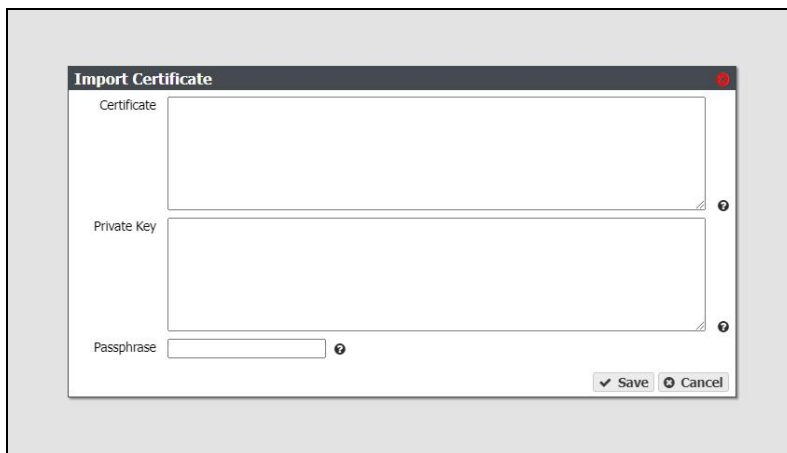3. Select **Action > Import Certificate**. The Import Certificate dialog box displays.

Figure 72 The Import Certificate dialog box.

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

   Note: The certificate must be in PEM format.

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

   Note: The private key must be in PEM format.

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

7. Click **Save**.

CONFIGURE NETWORKING SERVICES

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

For instructions on configuring NAS services, see Configure NAS Services on page 104.

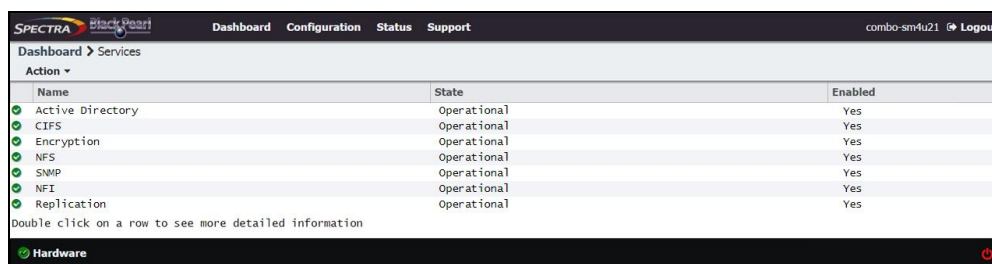To display the services screen, from the menu bar, select **Configuration > Services**.

Figure 73 The Services screen.

Configure the Active Directory Service

The Active Directory service in the BlackPearl user interface is used to connect the solution to a Windows Active Directory domain. Before you can join a domain, you must configure the BlackPearl NAS solution to use NTP. See Configure Date and Time on page 123.

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

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

Join Domain

1. From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 73 on page 126).

2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action > Show Details**. The Active Directory details screen displays.

3. On the Active Directory service details screen, select **Action > Join Domain**. The Join Domain dialog box displays.
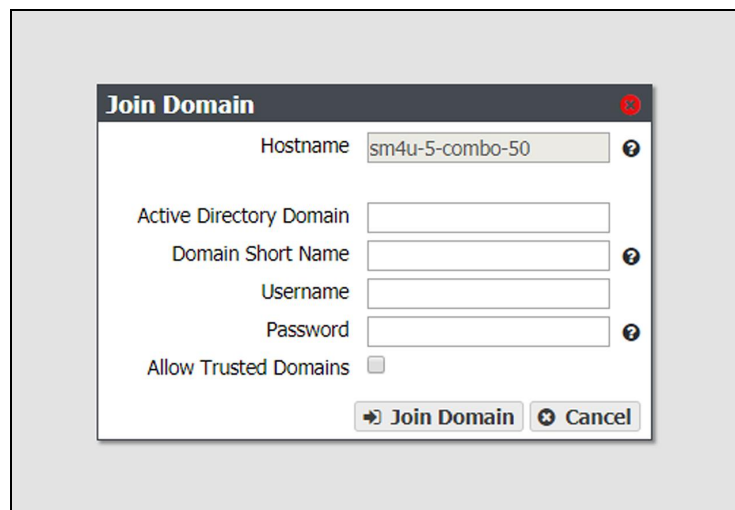

Figure 74 The Join Domain dialog box.

4. The **Hostname** identifies the BlackPearl NAS solution 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 Edit the System Name on page 124).

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

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

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

Notes: ● The BlackPearl NAS solution uses "Pre-Windows 2000" login names for Active Directory users. Login names greater than 20 characters in length, or containing special characters (for example '@') are not able to log into the BlackPearl user interface.

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

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

9. Click **Join Domain**.

Edit Domain

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

1. From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 73 on page 126).

2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action > Show Details**. The Active Directory details screen displays.

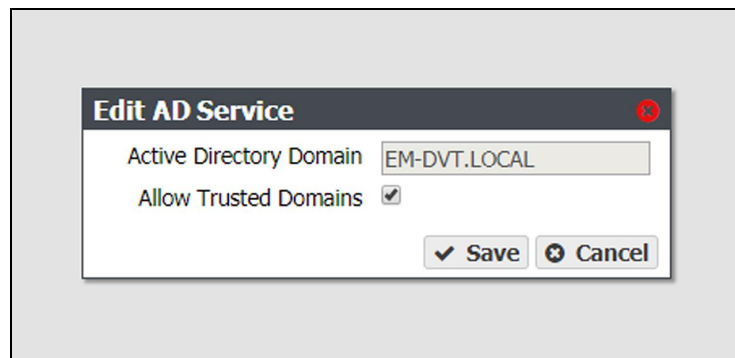3. Select **Action > Edit**. The Edit AD Service dialog box displays.

Figure 75 The Join Domain dialog box.

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

4. Select or clear **Allow Trusted Domains**.

5. Click **Save**.

Add Advanced Parameter

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

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

1. From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 73 on page 126).

2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action > Show Details**. The Active Directory details screen displays.

3. Select **Action > Add Advanced Parameter**. The Add Advanced Parameter dialog box displays.
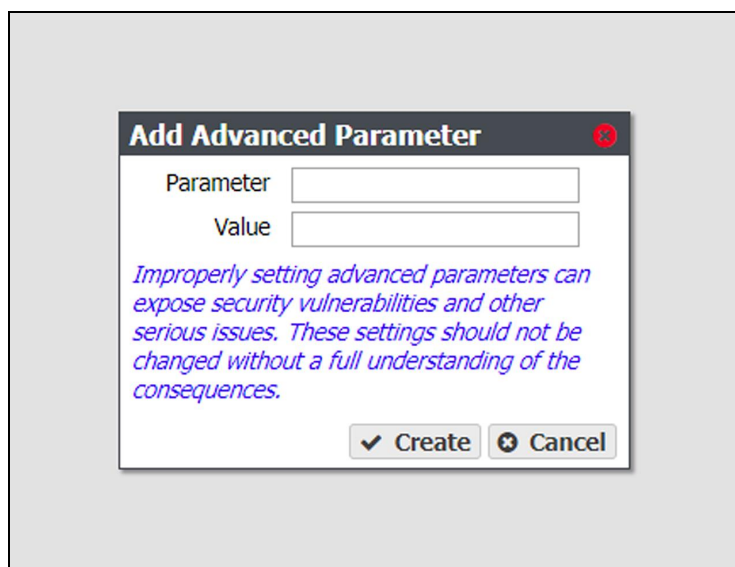
Figure 76 The Add Advanced Parameter dialog box.

4. Enter the desired **Parameter** and **Value**.

5. Click **Create**.

Edit Advanced Parameter

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

1. From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 73 on page 126).

2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action > Show Details**. The Active Directory details screen displays.

3. Select the advanced parameter which you want to edit, then select **Action > Edit Advanced Parameter**. The Edit Advanced Parameter dialog box displays.
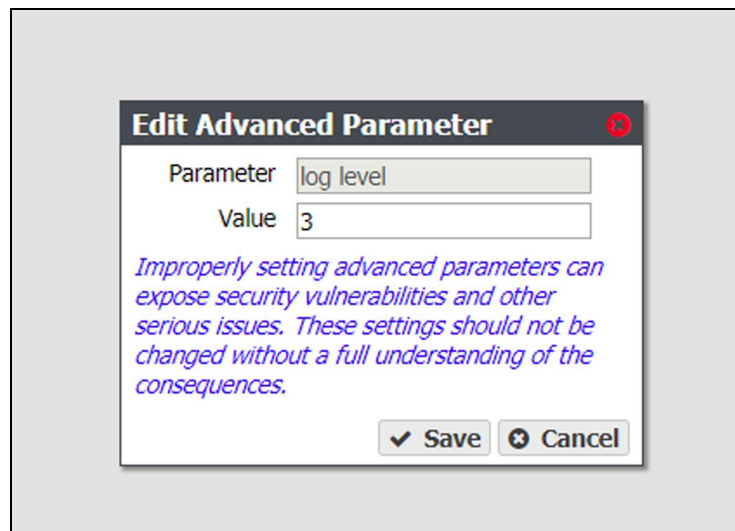
Figure 77 The Edit Advanced Parameter dialog box.

4. The **Parameter** field is greyed-out and cannot be changed.

5. Enter the desired **Value**.

6. Click **Save**.

Delete Advanced Parameter

1. From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 73 on page 126).

2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action > Show Details**. The Active Directory details screen displays.

3. Select the advanced parameter which you want to delete, then select **Action > Delete Advanced Parameter**. The Edit Advanced Parameter confirmation window displays.

4. Click **Delete**.

Leave Domain

1. From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 73 on page 126).

2. Double-click the **Active Directory** row, or select the **Active Directory** row and select **Action > Show Details**. The Active Directory details screen displays.

3. Select **Action > Leave Domain**. A confirmation window displays.

4. Click **Leave Domain**.

Configure the SNMP Service

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 73 on page 126).

2. Double-click the SNMP service, or select the SNMP service and select **Action > Show Details**. The SNMP details screen displays.

3. On the SNMP details screen, select **Action > Edit**. The Edit SNMP Service dialog box displays.
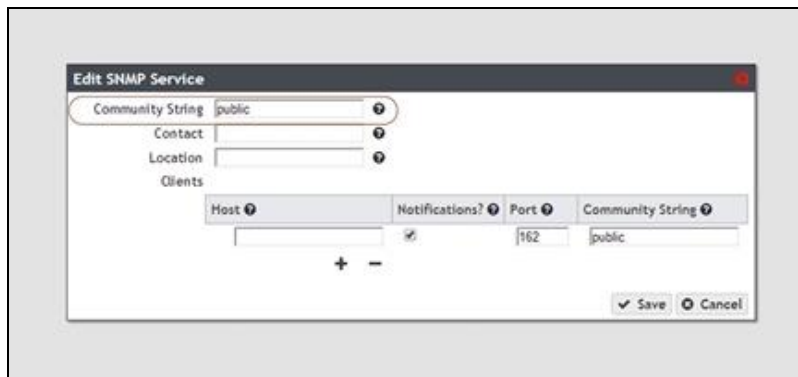
Figure 78 The Edit SNMP Service dialog box.

4. If desired, change the value of the **Community String**. Any incoming SNMP queries that use a different community string than the one set here fail. If no community string is specified, then the BlackPearl NAS solution responds to all SNMP queries.

5. Enter the primary contact for the BlackPearl NAS solution in the **Contact** field.

6. Enter the physical location of the solution in the **Location** field.

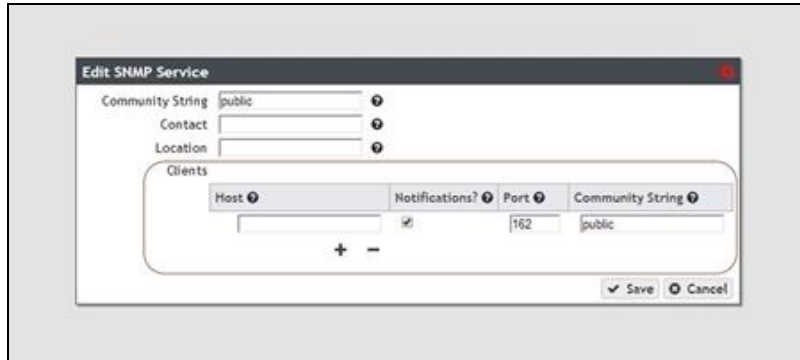**7.** If desired, add clients that are allowed to access the solution using SNMP.

Figure 79 The Edit SNMP Service dialog box.

    a. Click the **+** sign to add a client.

    b. Enter the host IP address in the **Host** field.

    c. If desired, select the **Notifications** check box to indicate that the SNMP client should receive outgoing notifications.

    d. Enter the port number to be used for SNMP communication in the **Port** field.

    e. Enter a community string value in the **Community String** field. This community string is set for each client. The clients monitor SNMP notifications for any that use the string specified here.

    f. Repeat Step a through Step e as needed to add additional clients.

8. Click **Save**.

Download the MIB File

If you want to communicate with the solution 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. Select **Configuration > Services** to display the Services screen (see Figure 73 on page 126).

2. Double-click the SNMP service row, or select the SNMP service row and select **Action > Show Details**. The SNMP details screen displays.

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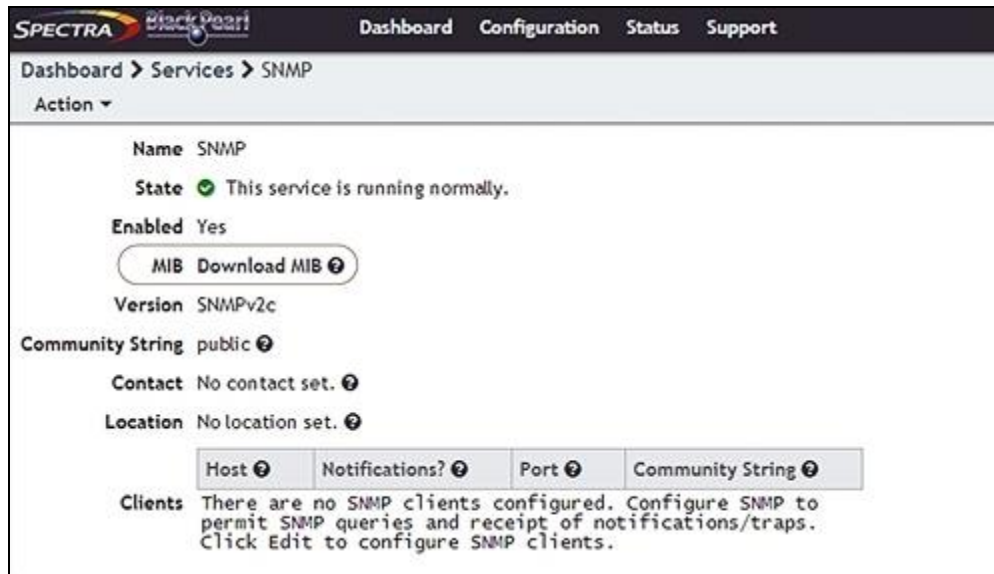

Figure 80 Download the MIB file.

4. Load the file into the network node manager program.

5. You can now use your network node manager program to communicate with the BlackPearl NAS solution, using the settings configured in Configure the SNMP Service on page 131.

NETWORK SETUP 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 solution 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 solution 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 .

Not Recommended:

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

MTU Settings

The BlackPearl solution 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 solution, then network switches must support link aggregation to aggregate or "trunk" the data ports together to provide higher bandwidth to the solution.

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 solution presents only one MAC address and one IP address.

- Using static link aggregation, the BlackPearl NAS solution 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 solution in order to achieve the highest throughput possible.

If only a single host is connected to the BlackPearl NAS solution 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 solution 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 solution 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 Solution 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 solution 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 solution. If the command fails to reach the BlackPearl NAS solution, see Cannot Ping the BlackPearl NAS Solution 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 solution 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 solution 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 Solution

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

- 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.

CHAPTER 4 - MANAGING NETWORK ATTACHED STORAGE

This chapter describes using the BlackPearl user interface to manage storage pools, volumes, and shares on the solution after configuring NAS. For initial NAS configuration steps, see Configuring Network Attached Storage on page 87.

MANAGE STORAGE POOLS

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

Edit a Storage Pool

You can edit an existing storage pool to enable encryption, enable auto-trim, select to use the pool as a shared resource pool (SRP) target, to change the value of the high water mark, and to select the number of write performance and metadata performance drives.

Use the following steps to edit a storage pool.

1. From the menu bar, select **Configuration > NAS > Pools**, or click the Pools pane on the Dashboard. The NAS Pools screen displays (see).

2. Select the pool you want to edit and select **Action > Edit**. The Edit *Pool Name* dialog box displays.

Figure 81 The Edit *Pool Name* dialog box.

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

3. If desired, enter a percentage for the **High Water Mark**. When the used space on the pool reaches this percentage, an alert is generated. Enter 0 if you do not want to set an alert level.

4. If desired, enable or disable **Power Saving Mode** for the storage pool. Enabling this feature configures the standby timer to 60 minutes. When there is no I/O to the storage pool for 60 minutes, the drives in the pool spin down and use minimal power.

Notes:
- Spectra Logic recommends leaving power saving mode **disabled**.
- To use this feature, all drives in the storage pool must be power-saving compatible.

5. If desired, select the **Encryption State**. To enable encryption, all drives in the storage pool must be self-encrypting drives (SEDs). If any non-SED drives are present in the pool, encryption is disabled even if you select to use encryption. When you configure the storage pool to use encryption, data written to the pool is encrypted at rest.

6. If desired, select the pool as a **Shared Resource Pool Backup Target**. The BlackPearl system uses a shared database that must be backed up to one or more NAS storage pools. When enabled, the BlackPearl system uses up to 2 TB of storage space for daily backups.

⚠️ **IMPORTANT**   Once enabled, an activation key is required to disable the Shared Resource Pool. Contact Spectra Logic Technical Support for assistance with this setting.

---

7. If desired, select to use **Auto Trim**. Auto trim automatically clears unused data blocks from SSD or NVMe drives, which improves both performance and longevity. When enabled, files that are deleted are promptly marked for reuse, helping to maintain drive speed by reducing write amplification. This also prolongs drive lifespan by minimizing unnecessary write operations.

8. If desired, use the **Write Performance Drives** drop-down menu to select the number of write performance drives to allocate to the storage pool.

9. If desired, use the **Metadata Performance Drives** drop-down menu to select the number of metatdata performance drives to allocate to the storage pool.

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

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

10. Click **Save**.

Expand a Storage Pool

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

Additionally, expanding a storage pool is used when you want to include different drive types than the type used when creating the pool.

   Notes: • Drive types must be the same block size.

   • The number of drives to be added to the storage pool must match the minimum number of drives for the existing stripe size.

   • Self-Encrypting Drives (SED) that are unused can be added to a non-encrypted partition.

⚠️ **IMPORTANT**   Contact your solutions architect before including multiple drive types in a storage pool.

Use the following steps to expand a storage pool.

1. From the menu bar, select **Configuration > NAS > Pools**, or click the Pools pane on the Dashboard. The NAS Pools screen displays (see Figure 39 on page 89).

2. From the list of existing storage pools, select the storage pool you want to expand, and then select **Action > Expand**. The Expand Pool screen displays options for adding additional drives to the storage pool.
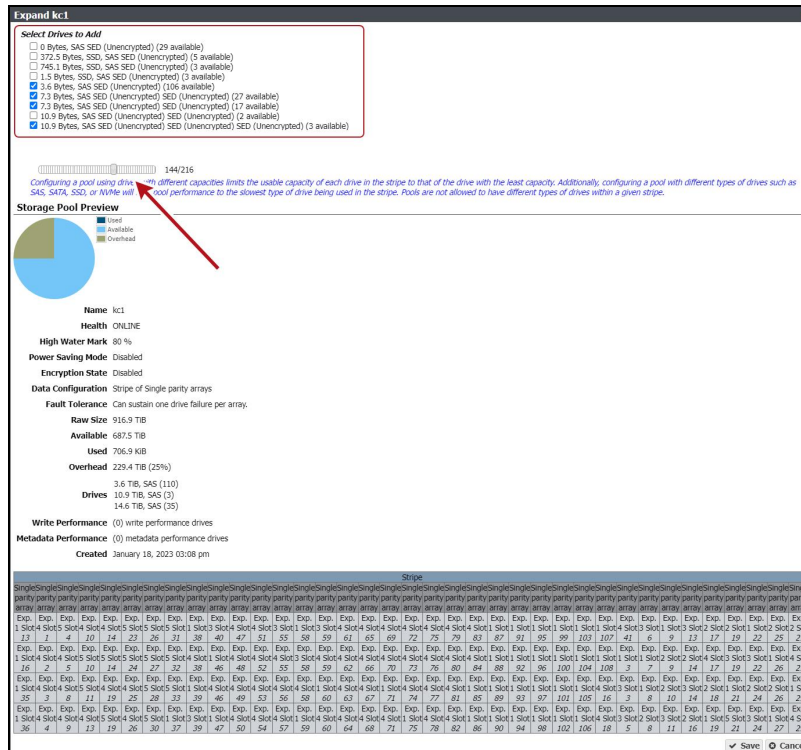

Figure 82 The Expand Pool screen.

3. Select the check box next to the type of drive(s) you want to add to the storage pool. By default, the check box for any drive type present in the solution is automatically selected.

4. Use the slider to increase the number of drives to use in the storage pool. As you make changes, the graphics beneath the slider update to show the impact your changes have on the storage pool.

Note: If you are mixing drive types, the number of drives to be added to the storage pool must match the minimum number of drives for the existing stripe size.

5. When you are satisfied with the new configuration, click **Save**. It may take up to three minutes for pool expansion to complete. Multiple expansions of the same storage pool may increase the time to complete.

Note: If you are adding self-encrypting drives to an encrypted storage pool, the drives are automatically encrypted and then added to the storage pool.

Delete a Storage Pool

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

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

Use the following steps to delete a storage pool.

1. From the menu bar, select **Configuration > NAS > Pools**, or click the Pools pane on the Dashboard. The NAS Pools screen displays (see Figure 39 on page 89).

2. From the list of existing storage pools, select the storage pool you want to delete, and then select **Action > Delete**. A dialog box displays asking you to confirm the deletion.
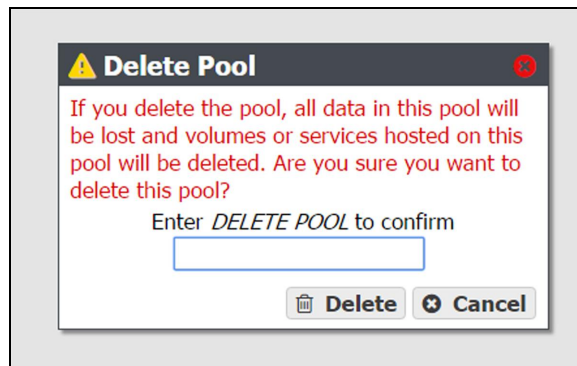
Figure 83 Confirm the storage pool deletion.

3. Type `DELETE` in the entry field and click **Delete** to delete the storage pool. Expanded pools may take up three minutes to delete.

   Note: If you deleted an encrypted pool, the drives in the pool are automatically erased and reset.

4. If desired, create a new storage pool that includes the disks no longer in use, as described in Create a NAS Storage Pool on page 89.

MANAGE VOLUMES

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

Move a Volume

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

> ⚠️ **IMPORTANT** Access to CIFS shares is lost when moving the share while simultaneously transferring data to or from the share.

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

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

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 41 on page 93).

2. Select the volume you want to move to a different storage pool, and then select **Action > Move**. The Move Volume dialog box displays.

3. Use the drop-down menu to select the destination pool for the volume.
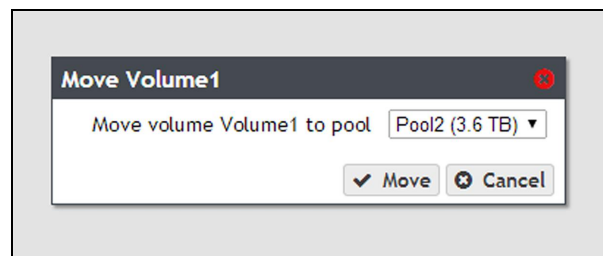
Figure 84 Select the destination pool for the volume.

4. Click **Move**. The volume is moved to the selected pool.

Cancel a Volume Move

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

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 41 on page 93).

2. Select the volume you want to cancel moving to a different storage pool, and then select **Action > Cancel Move**. The Cancel Move Volume dialog box displays.

3. Click **Cancel Move** to cancel the in-progress volume move.

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

Edit a Volume

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

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 41 on page 93).

2. Double-click the volume you want to edit, or select the volume and then select **Action > Edit**. The Edit *Volume name* screen displays.

Figure 85 The Edit Volume screen.

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

For this option....	Do the following...

Name	Enter a new name for the volume. Volume names are limited to 62 characters or fewer.
	
	 ⚠️ **IMPORTANT** — **DO NOT** rename a volume that is used by the Spectra Vail application.
	
	Notes:
	
	  • The combined storage pool and volume name must be 78 characters or fewer.
	  • NFS does not allow spaces in share names. As a result, any spaces in the volume name are replaced by underscores in the corresponding NFS share name. The 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.
	  • If you change the name of a volume that is being shared, the share point is maintained after the volume name change.

Minimum Size	Select the desired unit size from the drop-down menu and enter a numerical value for the minimum size in the text box to the left of the unit size drop-down menu. This space is allocated immediately if there is sufficient space available on the storage pool. If there is insufficient space available, saving the modified volume fails.

Maximum Size	• Select the desired unit size from the drop-down menu and enter a numerical value for the maximum size in the text box to the left of the unit size drop-down menu.
	Notes:
	  • The maximum size must be greater than the current amount of used space on the volume.
	  • Volumes are thin provisioned, so it is possible for the combined allocated maximum storage of all volumes to exceed the physical space available.

Snapshot Change Threshold	Specify 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. • Allowed values are between 0 and 99. **Note:** Spectra Logic recommends configuring the Administrator user to receive emails when a warning event occurs.

For this option....	Do the following...
	Note: The BlackPearl NAS solution uses unique data to detect the specified percentage change when data is deleted. If you enable compression for this volume, it is possible that the volume may contain compressed data that is not unique. When data is deleted it may not reach the specified threshold, which does not trigger a warning when the deletion occurs.
Compression	If desired, select the check box to enable the solution to compress data stored in NAS.
	If desired, select the check box to enable data compression using ZFS to allow the BlackPearl NAS solution 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 solution. This impact is less evident with Gen2 and Gen3 master nodes.
	Note: Changing the compression setting only affects data written to the volume after the compression setting is changed. It does not affect data already on the volume.
Access Time	If desired, select the check box to configure the solution to update the time stamp of a file when it is read from the volume. Selecting **Access Time** may slow performance.
Read Only	If desired, select the check box to configure the volume so that data can be read, but not written to the volume.
NFI Volume Policy	If desired, edit the NFI Volume policy configurations. See Configure Network File Interface on page 289.

4. Click **Save**.

Delete a Volume

Use the following steps to delete a volume.

1. From the <u>menu</u> bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The **Volumes screen** displays (see Figure 41 on page 93).

2. Select the volume you want to delete and then select **Action > Delete**. A dialog box displays asking you to confirm the deletion.

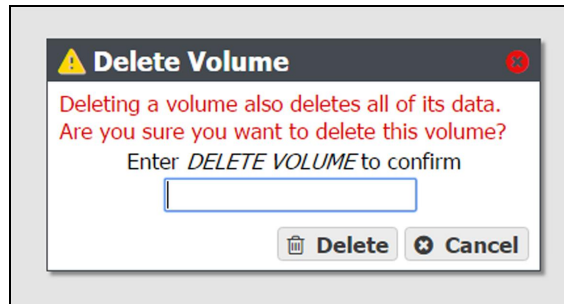⚠ **CAUTION**   Deleting a volume deletes all data in the volume. This action cannot be undone.

Figure 86 Confirm the volume deletion.

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

VOLUME SNAPSHOTS

Volume Snapshots are images of a volume's configuration and data makeup as they were when the snapshot was generated. Restoring to a previously created snapshot allows you to go "back in time" and restore the volume to the state it was in when the snapshot was created.

Notable features of volume snapshots are:

- Snapshots are immutable to the outside word. 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 solution until they are manually deleted, or the set Maximum Number of Snapshots limit is reached. When the limit is reached, the oldest snapshot is deleted freeing up capacity held by that snapshot.

Snapshots are created instantly without any impact to system performance. Snapshots initially occupy very little space on the storage pool, but grow as data is 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

Use the following steps to create a snapshot.

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see).

2. Double-click the volume you want to use to create a snapshot, or select the volume, and then select **Action > Show Details**. The details screen for that volume displays.
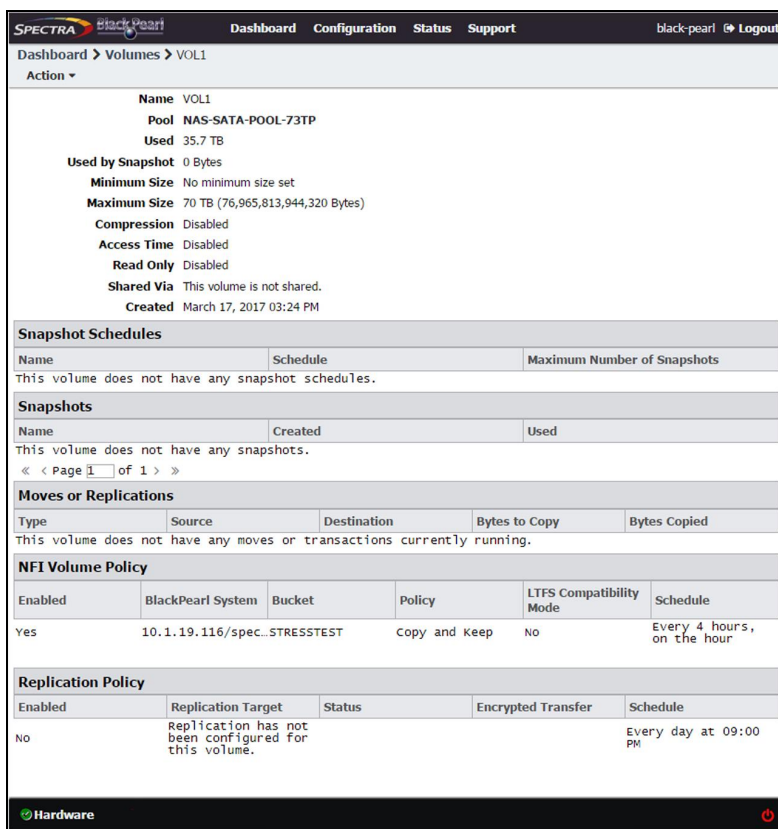
Figure 87 The Volume details screen.

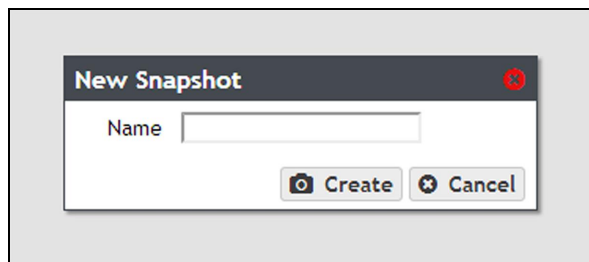**3.** On the Volume details screen, select **Action > New Snapshot**. The New Snapshot dialog box displays.

Figure 88 The New Snapshot dialog box.

4. Enter a name for the snapshot in the **Name** field.

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

Create a Snapshot Schedule

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

- Create an Hourly Schedule below — Create snapshots every selected number of hours.
- Create a Daily Schedule on the next page — Create snapshots every selected number of days.
- Create a Weekly Schedule on page 153 — Create snapshots on certain days of the week.

Create an Hourly Schedule

1. On the Volume details screen (see Figure 87 on page 150), select **Action > New Snapshot Schedule**. The New Snapshot Schedule dialog box displays.

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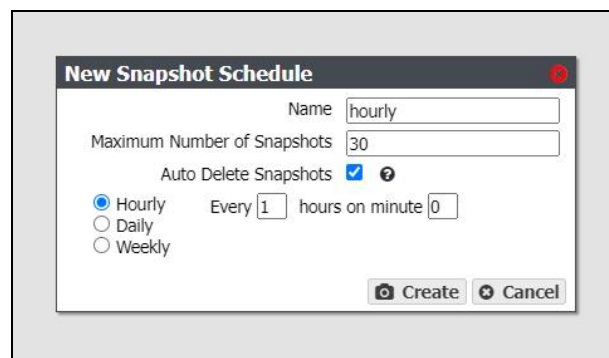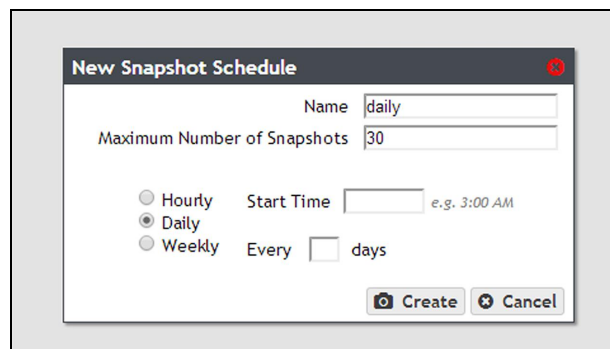

Figure 89 The New Snapshot Schedule dialog box showing the hourly interval options.

3. Change the default name of the snapshot schedule, if desired.

   Note: Snapshot schedule names must be unique.

4. Enter a number for the **Maximum Number of Snapshots**. When the maximum number is reached, the solution deletes the oldest snapshot.

5. If desired, select **Auto Delete Snapshots** to allow the BlackPearl NAS solution to automatically delete the oldest snapshot when the solution reaches the specified **Maximum Number of Snapshots**. If you do not enable this feature, when the system reaches the specified **Maximum Number of Snapshots**, the solution stops creating snapshots until snapshots are manually deleted.

   Note: Spectra Logic recommends enabling this feature.

6. Enter numbers for **Every _ hours on minute** _. These values specify the interval in hours between generating 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, the NAS volume creates a snapshot every four hours at 15 minutes after the hour. The maximum setting for the **hours** field is 48, where the NAS volume creates a snapshot every two days. The maximum setting for the **minute** field is 59.

Note: Spectra Logic recommends offsetting the minutes after the hour for starting snapshots so that there are not a large number of jobs starting at exactly the same time.

7. Click **Create**.

Create a Daily Schedule

1. On the Volume details screen (see), select **Action > New Snapshot Schedule**. The New Snapshot Schedule dialog box displays.

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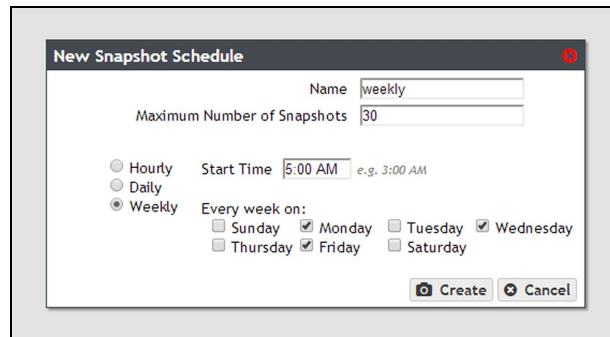

Figure 90 The New Snapshot Schedule dialog box showing the daily interval options.

3. Change the default name of the snapshot schedule, if desired.

Note: Snapshot schedule names must be unique.

4. Enter a number for the **Maximum Number of Snapshots**. When the maximum number is reached, the solution deletes the oldest snapshot.

5. If desired, select **Auto Delete Snapshots** to allow the BlackPearl NAS solution to automatically delete the oldest snapshot when the solution reaches the specified **Maximum Number of Snapshots**. If you do not enable this feature, when the system reaches the specified **Maximum Number of Snapshots**, the solution stops creating snapshots until snapshots are manually deleted.

Note: Spectra Logic recommends enabling this feature.

6. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.

7. Enter a number for **Every _ days**. This value specifies the interval, in days, between generating snapshots. The value entered is enumerated from the first day of the month. The schedule resets at the beginning of each month. For example, if this value is set to 2, the NAS volume creates a snapshot every two days, starting with the 1st of the month, at the time specified in Step 6. A value of 30 runs on the 1st of the month, and then again on the 31st of the month (for months that have 31 days). To schedule generating snapshots on the first of every month, set the interval to 31 days.

8. Click **Create**.

Create a Weekly Schedule

1. On the Volume details screen (see Figure 87 on page 150), select **Action > New Snapshot Schedule**. The New Snapshot Schedule dialog box displays.

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

Figure 91 The New Snapshot Schedule dialog box showing the weekly interval options.

3. Change the default name of the snapshot schedule, if desired.

   Note: Snapshot schedule names must be unique.

4. Enter a number for the **Maximum Number of Snapshots**. When the maximum number is reached, the solution deletes the oldest snapshot.

5. If desired, select **Auto Delete Snapshots** to allow the BlackPearl NAS solution to automatically delete the oldest snapshot when the solution reaches the specified **Maximum Number of Snapshots**. If you do not enable this feature, when the system reaches the specified **Maximum Number of Snapshots**, the solution stops creating snapshots until snapshots are manually deleted.

   Note: Spectra Logic recommends enabling this feature.

6. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.

7. Select one or more days for **Every week on:**. This determines the day(s) of each week the NAS volume generates snapshots. For example, based on the selections in Figure 91, the NAS volume creates a snapshot every Monday, Wednesday, and Friday at 5:00 AM.

8. Click **Create**.

Delete a Snapshot Schedule

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

> **Note:** Deleting a snapshot schedule does not delete the snapshots previously created by the snapshot schedule. To delete snapshots, see Delete Snapshots below.

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

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 41 on page 93).

2. Double-click the volume for which you want to delete the snapshot schedule, or select the volume, and then select **Action > Show Details**. The details screen for that volume displays.

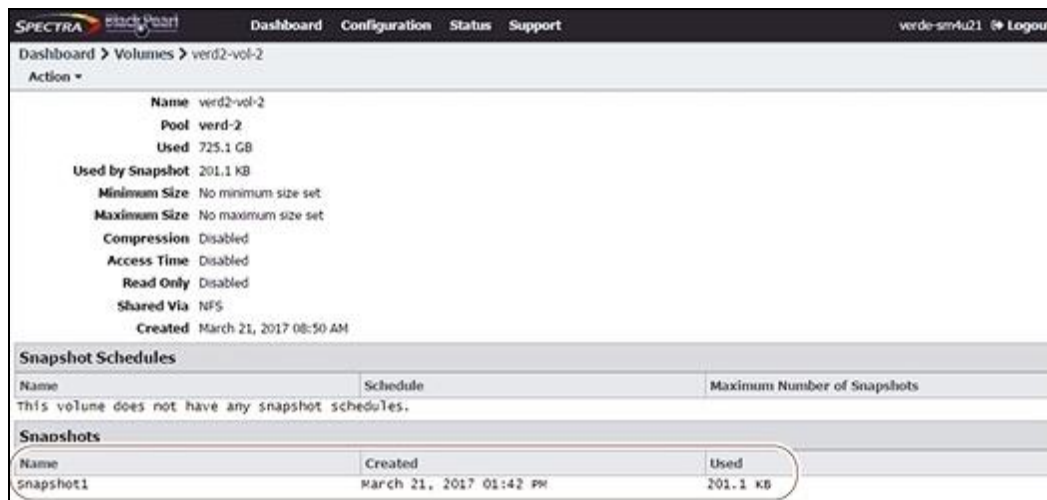3. Select the snapshot schedule you want to delete and select **Action > Delete Snapshot Schedule**. A confirmation window displays.
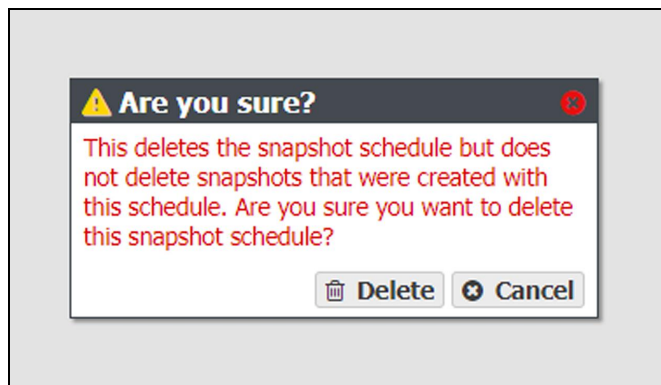
Figure 92 Confirm the snapshot schedule deletion.

4. Click **Delete**.

Delete Snapshots

Use the following steps to delete a one or more snapshots.

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 41 on page 93).

2. Double-click the volume you for which you want to delete snapshot, or select the volume, and then select **Action > Show Details**. The details screen for that volume displays.
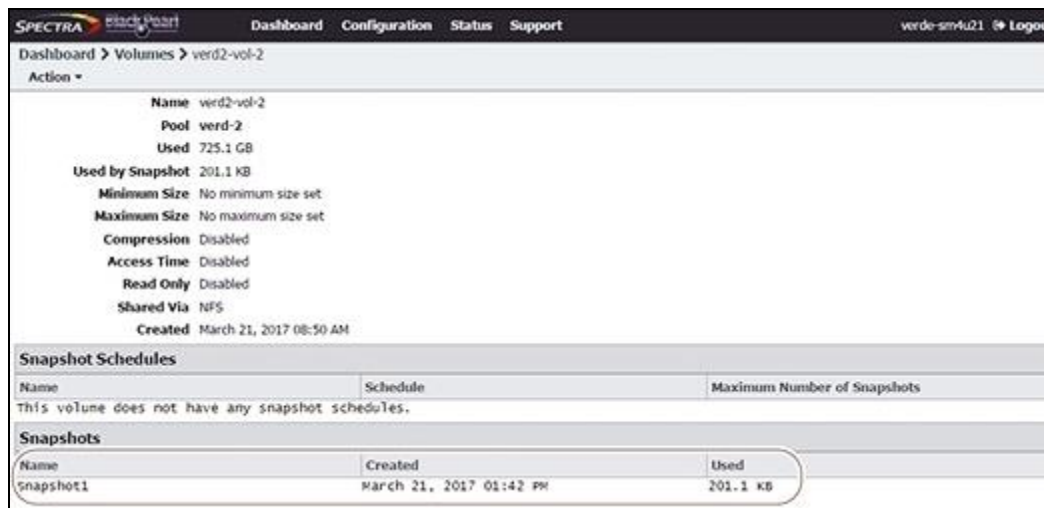
Figure 93 The Volume details screen showing a snapshot.

3. Delete the snapshot(s):

- To delete a single snapshot, select the snapshot you want to delete, and then select **Action > Delete Snapshot**.

- To delete all snapshots select **Action > Delete All Snapshots.**

A confirmation window displays.
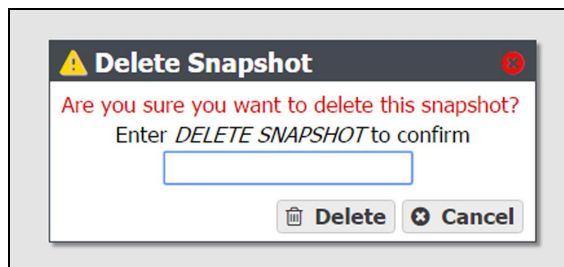
Figure 94 Confirm the snapshot deletion
(Delete Snapshot window shown).

4. Type the indicated text in the entry field and click **Delete** to delete the selected snapshot, or all snapshots.

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 Retrieve a Single File from a Snapshot on the next page.

- You cannot restore to a snapshot if the volume contains a Vail share using the BlackPearl user interface. Use API or CLI commands to restore a snapshot when the volume contains a Vail share.

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 41 on page 93).

2. Double-click the volume you want to restore using a previously generated snapshot, or select the volume, and then select **Action > Show Details**. The details screen for that volume displays.
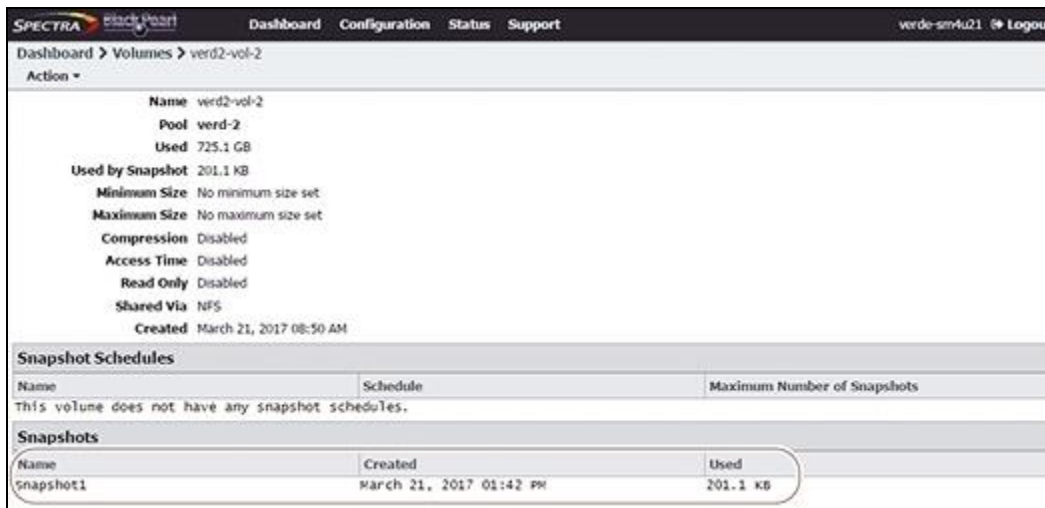

Figure 95 The Volume details screen.

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

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

4. A dialog box displays, asking you to confirm the rollback. Select **Rollback** to restore the volume to its state when the snapshot was created.
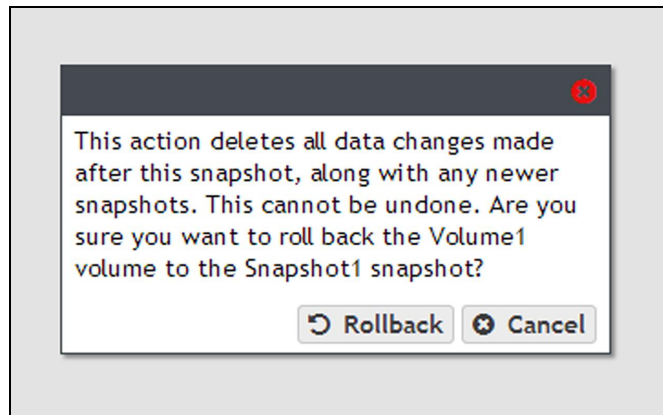
Figure 96 Confirm the volume snapshot rollback.

Retrieve a Single File from a Snapshot

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

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

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

1. If necessary, locate the snapshot from which you want to restore a file.

   a. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 41 on page 93).

   b. Double-click the volume you for which you want to delete snapshot, or select the volume, and then select **Action > Show Details**. The details screen for that volume displays.

Figure 97 The Volume details screen showing a snapshot.

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

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.

MANAGE SHARES

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

> **Note:** You cannot edit a Vail S3 share.

Edit a CIFS Share

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

1. From the menu bar, select **Configuration > Shares > CIFS**. The CIFS Shares screen displays.

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

Figure 98 The Edit NFS Share dialog box.

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

4. Click **Save**.

Edit an NFS Share

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

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

2. Select the share you want to edit, and then select **Action > Edit**. The NFS Share Edit screen displays.
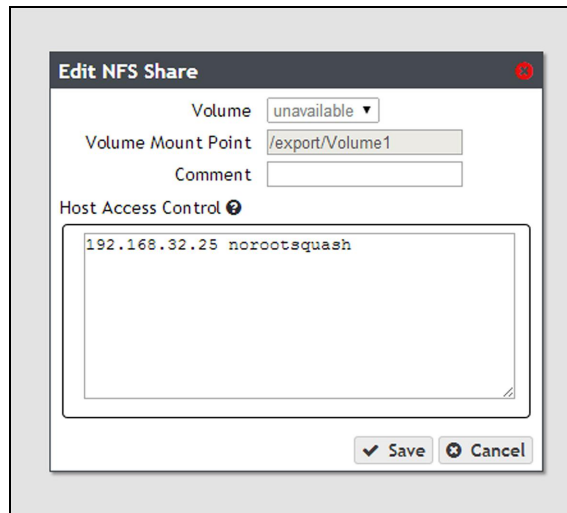
Figure 99 The Edit NFS Share dialog box.

3. Make the desired changes (see Create a Share on page 97 for more information), and click **Save**.

Delete a Share

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

Use the following steps to delete the share.

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

—OR—

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

—OR—

If you need to delete a Vail share, from the menu bar, select **Configuration > Shares > Vail S3**. The Vail S3 Shares screen displays.

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

Note: You cannot delete a Vail S3 share with data persisted to the volume. You must first delete the share as Storage in the Vail management console, then delete the share in the BlackPearl user interface.

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

Note: Clicking **Delete** does not delete the volume. It only removes the volume from the list of shares and makes it inaccessible to remote hosts. The volume is still listed present on the solution and listed on the Volumes screen.
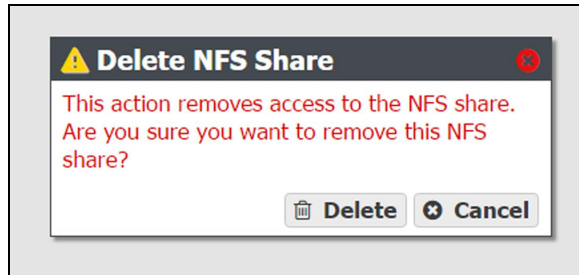
Figure 100 Confirm removing the share.

MANAGE NAS REPLICATION

After configuring replication (see Configure NAS Services on page 104), 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.

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

1. On the source system's BlackPearl user interface, select **Configuration > NAS > Volumes**. The Volumes screen displays.

2. Double-click the volume name you want to replicate, or select the volume and select **Action > Show Details**. The details screen for the volume displays.

3. Select **Action > Replicate Now**. A confirmation window displays.
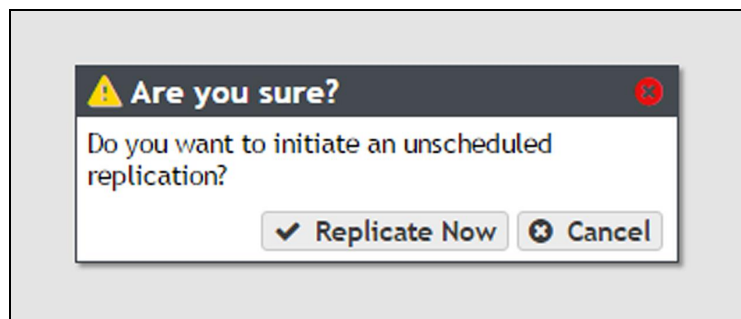
Figure 101 The Replicate Now confirmation window.

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

Cancel a NAS Replication In Progress

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

Note: Starting with BlackPearl OS 5.4, you can no longer cancel an in-progress NAS replication. After starting a NAS replication, you must wait for it to complete.

1. On the source system's BlackPearl user interface, select **Configuration > NAS > Volumes**. The Volumes screen displays.

2. Double-click the volume name for which you want to cancel replication, or select the volume and select **Action > Show Details**. The details screen for the volume displays.

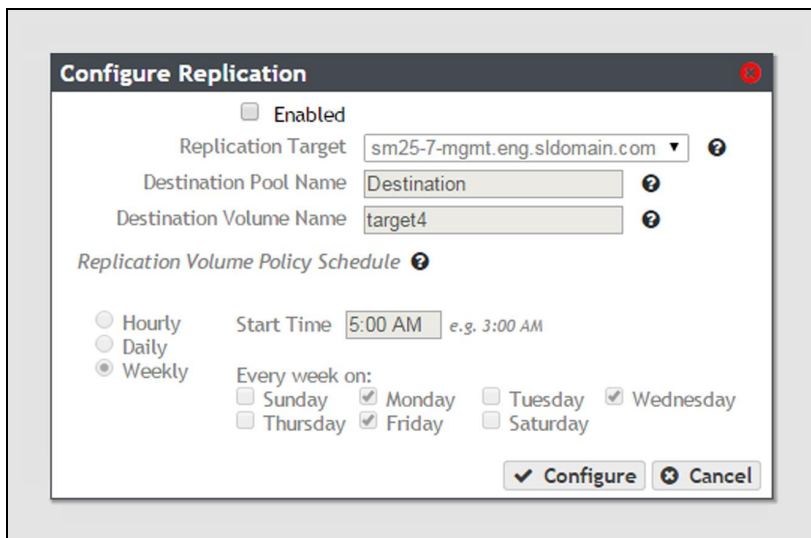3. Select **Action > Cancel Replication**. A confirmation window displays.
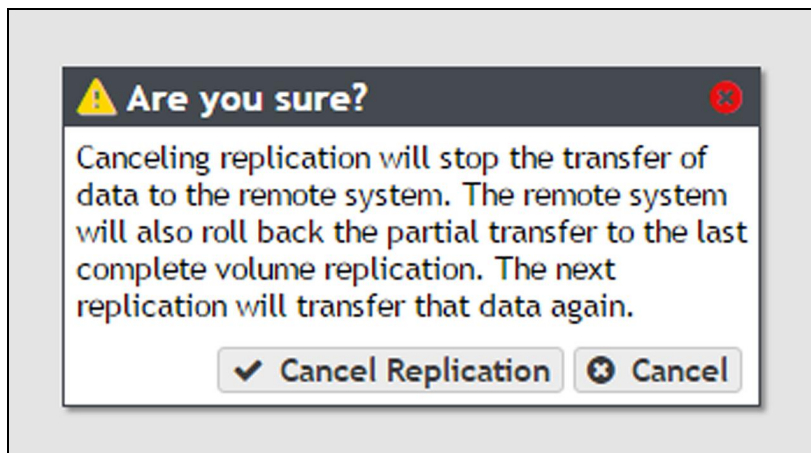
Figure 102 The Cancel Replication confirmation window.

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

Restoring Files from a NAS Replication Target

If the source solution 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. From the menu bar, select **Configuration > NAS > Volumes**. The Volumes screen displays.

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

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

    d. Click **Save**.

2. Depending on your operating system environment, create either a CIFS or NFS share, selecting the replicated volume during the creation process. See Create a Share on page 97 for instructions.

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

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

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

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

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

    d. Click **Save**.

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

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

6. If desired, stop sharing the NAS replication target volume. See Delete a Share on page 160.

Disable NAS Replication for a Volume

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

1. On the source system's BlackPearl user interface, select **Configuration > NAS > Volumes**. The Volumes screen displays.

2. Double-click the volume name you want to stop replicating, or select the volume and select **Action > Show Details**. The details screen for the volume displays.

3. Select **Action > Configure Replication**. The Configure Replication dialog box displays.

Figure 103 The Configure Replication dialog box.

4. Clear the **Enabled** check box. The other options on the dialog box grey out and become un-editable.

5. Click **Configure**. The volume no longer replicates to the target.

Edit the NAS Replication Service

1. On the source solution's BlackPearl user interface, select **Configuration > Services** to display the Services screen (see Figure 73 on page 126).

2. Double-click the Replication service, or select the service, and then select **Action > Show Details**. The Replication service details screen displays.
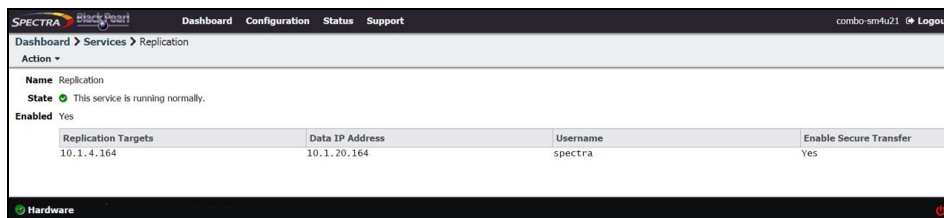
Figure 104 The Replication service details screen.

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

Figure 105 The Modify Replication Service dialog box.

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

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

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

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

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

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

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

9. Click **Save**.

Delete the NAS Replication Service Configuration

1. On the source solution's BlackPearl user interface, select **Configuration > Services** to display the Services screen (see Figure 73 on page 126).

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

Figure 106 The Replication service details screen.

3. Select the replication target in the Replication service details screen, and select **Action > Delete**. The Delete Replication Target dialog box displays.

4. Click **Delete** to remove the NAS replication target. The solution no longer replicates data to the target.

5. Repeat Step 3 and Step 4 to delete additional NAS replication targets, if desired.

CHAPTER 5 - ADDITIONAL CONFIGURATION OPTIONS

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

MULTI-FACTOR AUTHENTICATION

The Spectra BlackPearl NAS solution offers multi-factor authentication as part of Attack Hardened storage, which enhances the security of your solution by using Google Authenticator to confirm the identity of any user trying to log in to the BlackPearl solution. This prevents unauthorized access to the solution 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 Google Authenticator to complete the account creation. After the QR code is scanned, Google Authenticator generates a six-digit number every 30 seconds, and does not require cell or internet access to generate these codes.
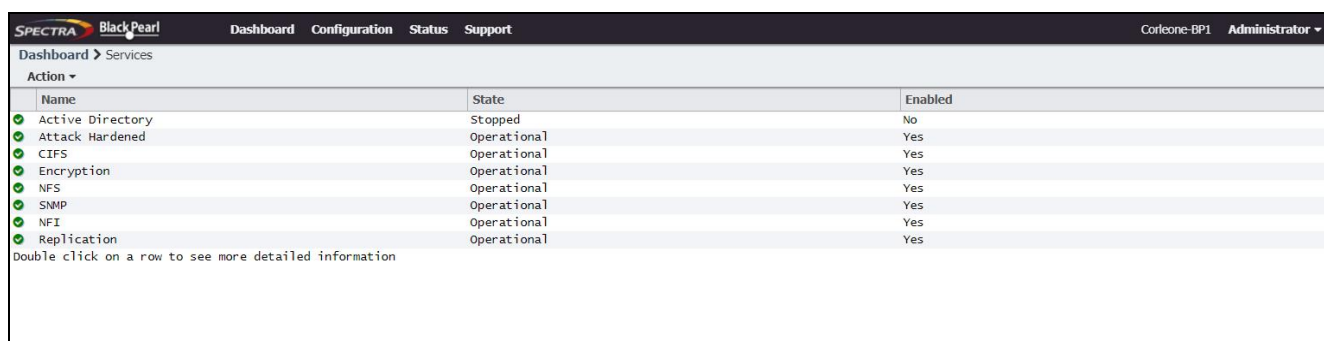
After multi-factor authentication is enabled, when the user attempts to log in to the BlackPearl user interface, after entering their username and password, they must enter the six-digit number generated by Google Authenticator within 30 seconds to complete the log in.

> **Note:** Only Administrator users can configure the Attack Hardened Service and enable Multi-Factor authentication for a user.

Enable the Attack Hardened Service

Before you can enable multi-factor authentication for users, you must enable the Attack Hardened service.

1. Select **Configuration > Services**. The Services screen displays.

Figure 107 The Services screen.

2. Select the Attack Hardened service row, then select **Action > Edit**. The Edit Attack Hardened Service dialog box displays.

   Note: You can also **double-click** the service row to edit the service.

Figure 108 The Edit Attack Hardened Service dialog box.

3. Using the **MFA Mode** drop-down menu, select **Per User**.

4. In the dialog box, enter `CHANGE MFA`, then click **Save**.

	CAUTION	After enabling the service, you must configure each user to use Multi-Factor Authentication before MFA is required for the user to log in to the BlackPearl user interface.

Enable Multi-Factor Authentication for a User

Note: The user account on the target system configured for NAS replication cannot use multi-factor authentication.

1. If necessary, download and install Google Authenticator on your mobile phone.

2. In the BlackPearl user interface, select **Configuration > Users**. The Users screen displays.

3. If necessary, create a new user (see Create a User on page 84), then continue with Step 4.

4. Select the user and then select **Action > Enable MFA**. The Generate MFA Code dialog box displays.

Figure 109 The Generate MFA Code dialog box.

5. Click **Generate MFA Code**. The Confirm MFA Code dialog box displays.

Figure 110 The Confirm MFA Code dialog box displaying a users QR code.

6. Use Google Authenticator on your phone to **scan** the QR code displayed in the BlackPearl user interface. The username and BlackPearl system name display in Google Authenticator, and the authenticator begins generating codes for the user.

Note: If you cannot scan the QR code, enter the **Setup Key** into Google Authenticator.

7. In the BlackPearl user interface, in the Confirm MFA Code dialog box, enter `CHANGE MFA FOR` *user's full name*, and click **Confirm MFA**.

The next time the user logs into the BlackPearl user interface, they must use the code generated by Google Authenticator 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 73.

 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 solution 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 125.

3. Enter the **Username** and **Password**.
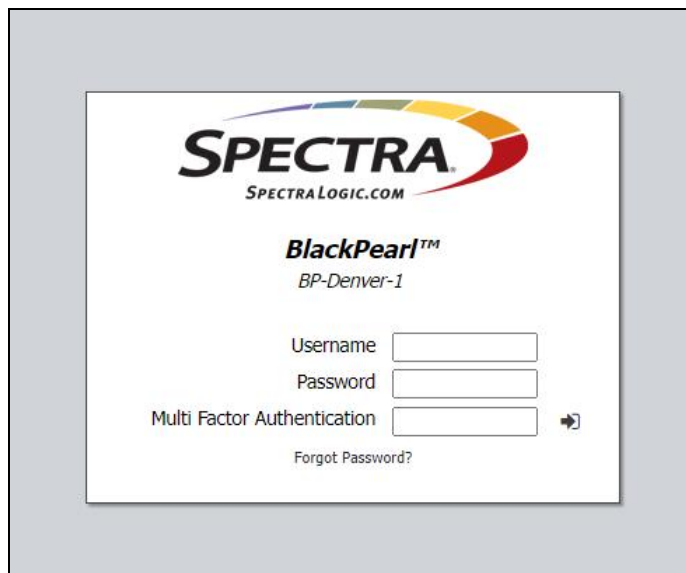
Figure 111 The Login screen with Multi-Factor Authentication enabled on the system.

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

Note: The code refreshes every 30 sections. If the code refreshes before you complete the login, you must clear the field and enter the new code.

Note: If you have more than one user or BlackPearl system 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 ➡️ to log in.

Update Multi-Factor Authentication for a User

If desired, you can update the token that Google Authenticator 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. In the BlackPearl user interface, select **Configuration > Users**. The Users screen displays.

2. Select the user and then select **Action > Update MFA**. The Generate MFA Code dialog box displays.

Figure 112 The Generate MFA Code dialog box.

3. Click **Generate MFA Code**. The Confirm MFA Code dialog box displays.

Figure 113 The Confirm MFA Code dialog box displaying a users QR code.

4. Use Google Authenticator on your phone to **scan** the QR code displayed in the BlackPearl user interface. The username and BlackPearl system name display in Google Authenticator, and the authenticator begins generating codes for the user.

Note: If you cannot scan the QR code, enter the **Setup Key** into Google Authenticator.

5. In the BlackPearl user interface, in the Confirm MFA Code dialog box, enter `CHANGE MFA FOR user's full name`, and click **Confirm MFA**.

   The next time the user logs into the BlackPearl user interface, they must use the code generated by Google Authenticator to complete the login.

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. In the BlackPearl user interface, select **Configuration > Users**. The Users screen displays.

2. Select the user and then select **Action > Disable MFA**. The Disable MFA dialog box displays.

Figure 114 The Disable MFA dialog box.

3. In the dialog box, enter `DISABLE MFA FOR user's full name`, and click **Disable MFA**.

   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 solution.

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 Update Multi-Factor Authentication for a User on page 173)

1. Select **Configuration > Services**. The Services screen displays (see Figure 107 on page 169).

2. Select the Attack Hardened service row, then select **Action > Edit**. The Edit Attack Hardened Service dialog box displays (see Figure 108 on page 170).

    Note: You can also **double-click** the service row to edit the service.

3. Using the **MFA Mode** drop-down menu, select **Off**.

4. In the dialog box, enter CHANGE MFA, and then click **Save**.

CONFIGURE A VAIL SPHERE

Use the instructions in this section to configure the BlackPearl NAS solution to communicate with a Vail sphere. After registering with a Vail sphere, you can create NAS-based Vail S3 shares on the BlackPearl NAS solution.

Notes:
- You can only register or edit a Vail sphere after entering a Vail activation key. See Manually Enter Activation Keys on page 197.

- All other aspects of the Vail application are controlled in the Vail management console. See the *Vail User Guide* for information on configuring and using the Vail application.

Register with a Vail Sphere

The Vail service configures a BlackPearl NAS solution for use with a Spectra Vail sphere. The Vail service only displays in the Services menu after an activation key is entered. Use the instructions in this section to register a Vail sphere with a BlackPearl NAS solution.

Here is how to register a BlackPearl S3 solution with a Vail sphere:

1. If desired, change the system name of the BlackPearl S3 solution:

    a. Select **Status > Hardware**.
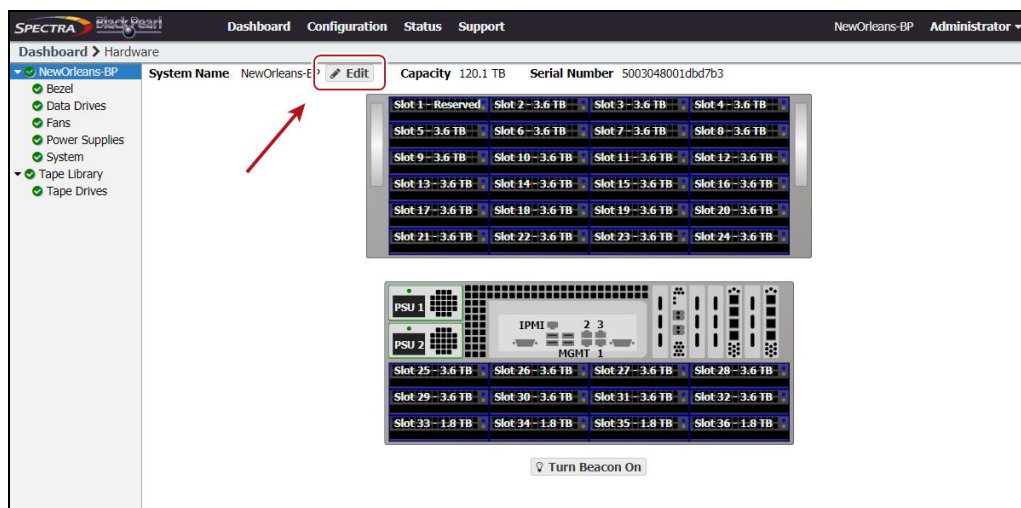
Figure 115 The BlackPearl user interface Hardware screen.

    b. Click **Edit**, enter the desired **Name**, and click **Save**.

Note: Spectra Logic recommends using the physical location of the BlackPearl system as the system name, for example Dallas.BlackPearl1-Object-Standard. The BlackPearl system name is limited to 15 characters before the first delimiter.

2. If necessary, add the Vail activation key provided by Spectra Logic:

   a. In the BlackPearl user interface, select **Support > Activation Keys**.

   b. Select **Action > New**.

   c. Enter the **Activation Key** and click **Save**.

3. In the BlackPearl user interface, select **Configuration > Services**.

4. Select the Vail service, then select **Action > Show Details**.
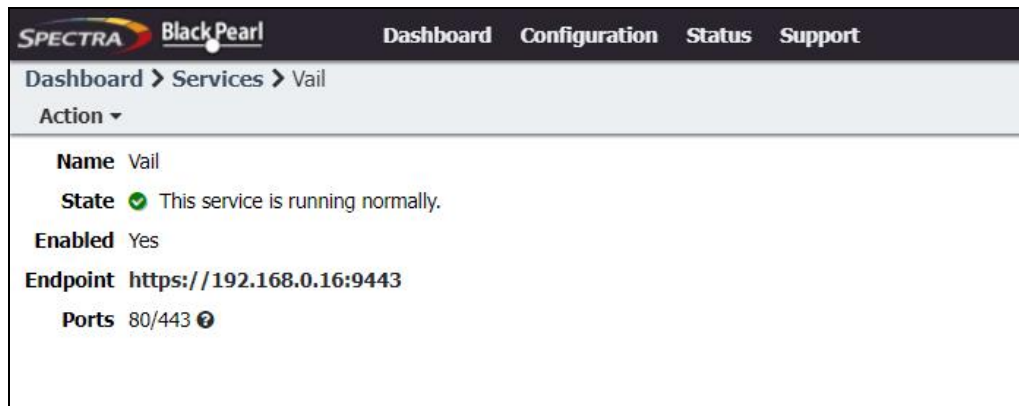
Figure 116 The Vail service details screen.

5. If desired, select **Action > Edit** to change the pair of ports used by the Vail application for HTTP and HTTPS connections. The ports automatically selected depend on if you have buckets created on your BlackPearl system.

   • If buckets are configured on your BlackPearl system, the pair of ports selected is 80/443.

   • If no buckets are configured, the pair of ports selected is 8080/8443.

Note: Whichever pair of ports is used by the Vail application, the other pair is used by the BlackPearl DS3 service. If you change the pair of ports for the Vail application, the DS3 service ports change to use the opposite pair of ports.

6. Click the **Endpoint** link in the Vail service details screen. A new web browser launches. The default web certificate is invalid, use your browser to bypass the certificate screen.
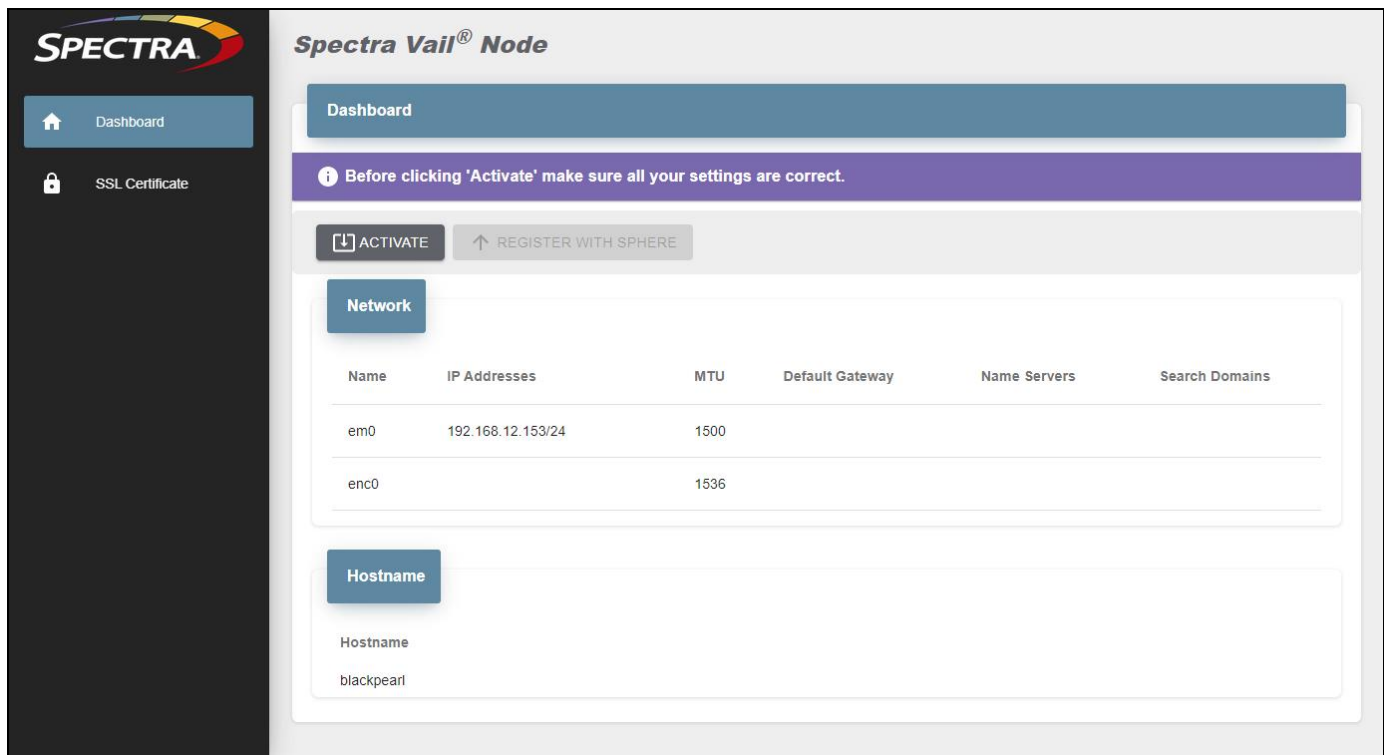
Figure 117 The Vail Node Dashboard - Activate and Register view.

7. If desired, update the SSL certificate before registering with the sphere:

    a. In the taskbar of the Vail VM node management console, click **SSL Certificate**.

    b. Under the **SSL Certificate** banner, click **Edit**.
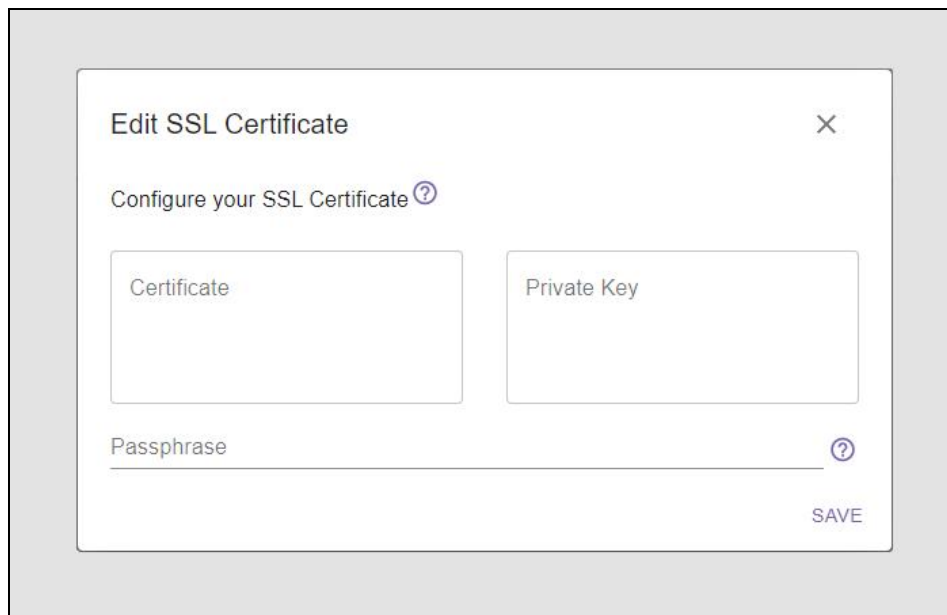
Figure 118 The Edit SSL Certificate screen.

    c. Enter the desired **Certificate** and **Private Key** in PEM format.

    d. If necessary, enter the **Passphrase** used to encrypt the private key.

    e. Click **Save**.

8. On the Vail dashboard screen, click **Activate**.
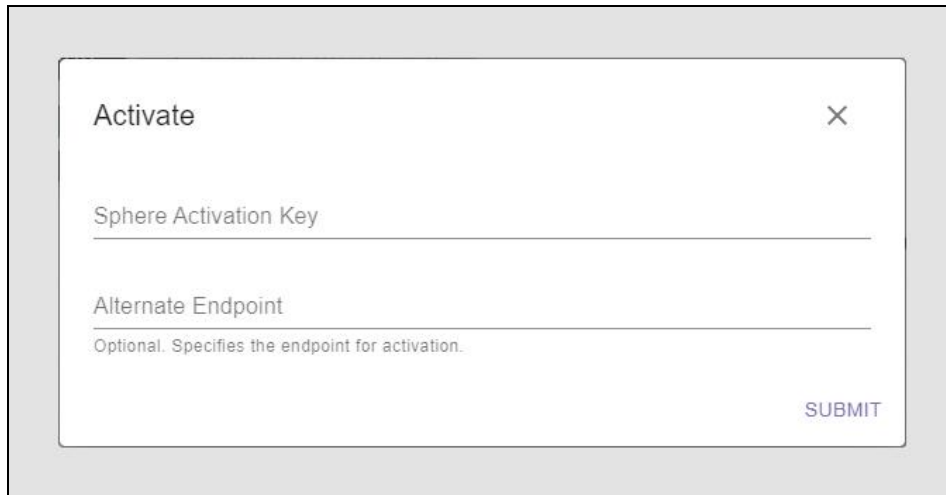
Figure 119 The Activate screen.

9. Enter the **Sphere Activation Key** and **Alternate Endpoint** provided by Spectra Logic.

Note: This key is known as the "Vail activation key" in the BlackPearl user interface, and the "Sphere activation key" in the Vail application interface. The key is the same value in both cases. This is the same key entered in

10. Click **Submit**. Wait approximately 15 seconds while the Vail management console refreshes.

11. On the Vail dashboard screen, click **Register With Sphere**.
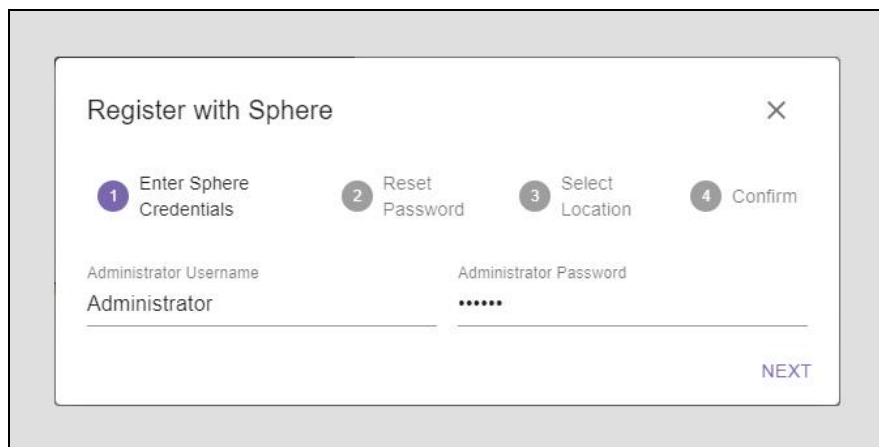
Figure 120 The Register with Sphere - Credentials screen.

12. Enter the **Administrator Username** and **Administrator Password**.

- If this is the first BlackPearl system to register with a sphere, enter the credentials sent to the email address you provided to Spectra Logic when the sphere was created in AWS.

Note: You may need to set an email/MX rule to allow emails from AWS to the address entered when the sphere was created.

- Otherwise enter the credentials provided by your system administrator.
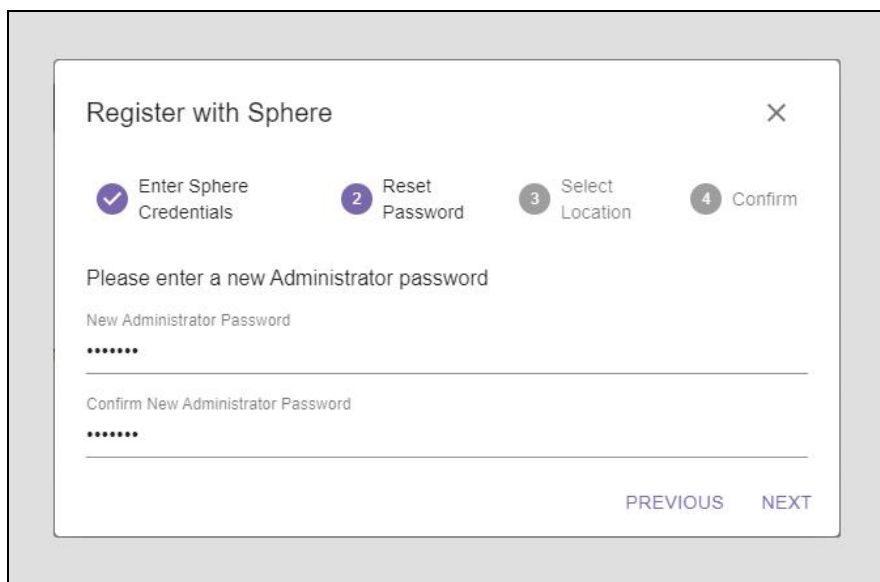
13. Click **Next**. If this is the first BlackPearl system to register with a sphere, you are prompted to set a new password. Otherwise, continue with Step 15.

Figure 121 The Register with Sphere - Reset Password screen.
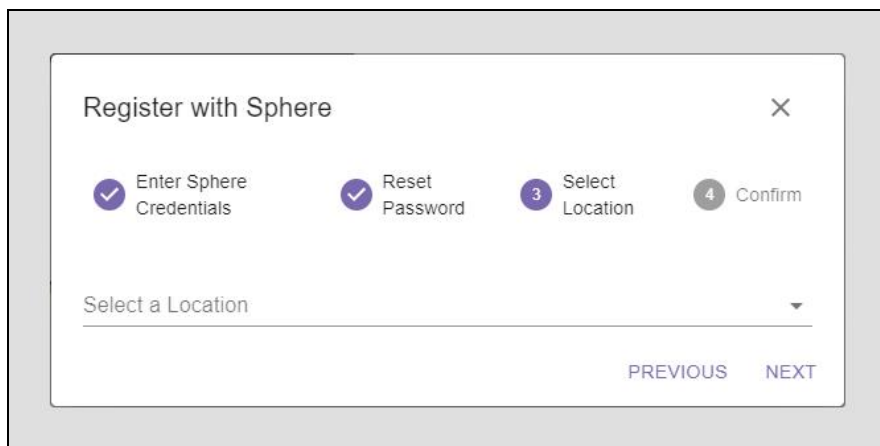
14. Enter a **New Administrator Password**, confirm the password, and click **Next**.

Figure 122 The Register with Sphere - Select Location screen.
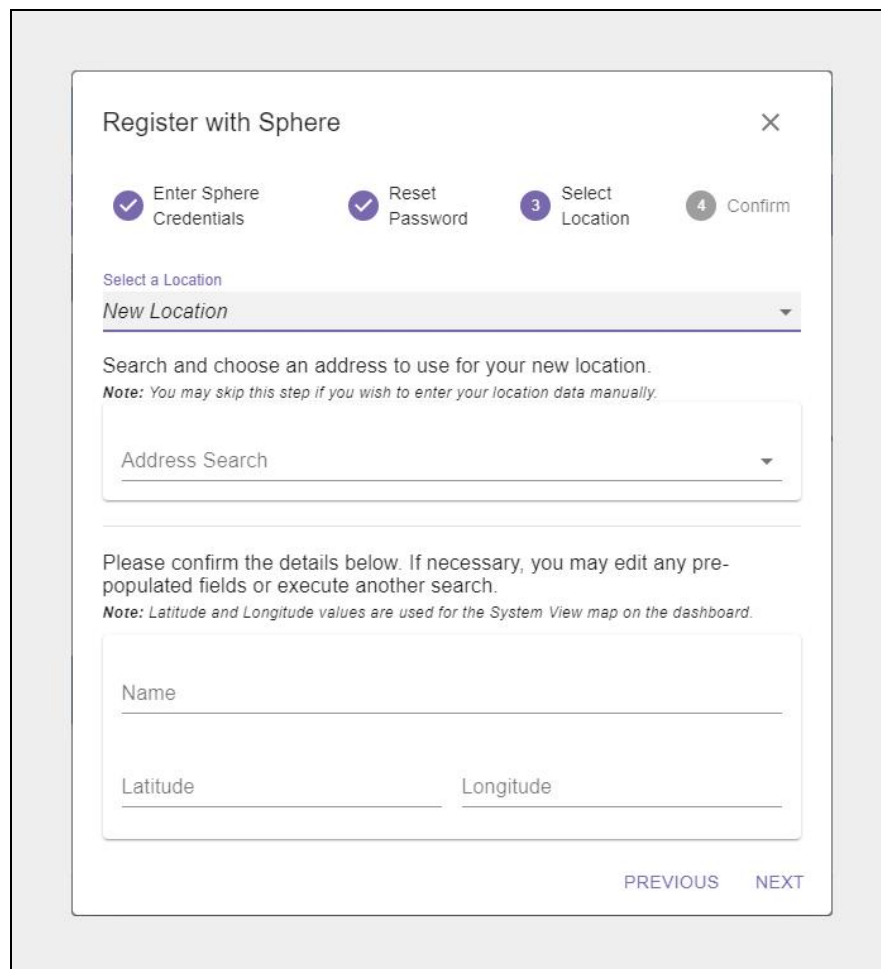
15. On the Select Location screen, chose to create a new location, or to use an existing location:

- **Create a New Location below**
- **Select an Existing Location on page 183**

Create a New Location

Here is how to create a new location:

1. To create a new location, use the drop-down to select **New Location**.

2. To map a location, you can search for the location, manually enter the latitude and longitude, or create a location with no corresponding geographic location.

Figure 123 The Register with Sphere - New Location screen.

- To search for a location...

    a. In the **Address Search** field, enter a geographic location. You can enter a full or partial postal address, city, county, province, or country.

    b. Select the correct match from the list.

    Note: If no match is located, try changing the format of the address you entered. For example, use 9th Street in place of Ninth St.

    c. If desired, manually edit the **Name**.

    Spectra Logic recommends naming each location after its physical location in the world.

    For example, if Vail resources are located in Dallas, use that as the location name if there is only one Vail resource in that city. If there are multiple Vail resources consolidated in the same city, use suffixes to identify each group such as Dallas-HQ, Dallas-Research, or Dallas-Production.

    d. Confirm the information is correct and click **Next**.

- To manually enter a location...

    a. Enter the desired **Name**.

    Spectra Logic recommends naming each location after its physical location in the world.

    For example, if Vail resources are located in Dallas, use that as the location name if there is only one Vail resource in that city. If there are multiple Vail resources consolidated in the same city, use suffixes to identify each group such as Dallas-HQ, Dallas-Research, or Dallas-Production.

    b. Enter the **Latitude** and **Longitude** of the location.

    Notes:
    - When entering a value for **Latitude**, use positive values for locations north of the equator, and negative values for locations south of the equator.

    - When entering a value for **Longitude**, use positive values for locations east of the prime meridian, and negative values for locations west of the prime meridian.

    c. Click **Next**.

- To skip entering a location...

  a. Enter the desired **Name**.

    Spectra Logic recommends naming each location after its physical location in the world.

    For example, if Vail resources are located in Dallas, use that as the location name if there is only one Vail resource in that city. If there are multiple Vail resources consolidated in the same city, use suffixes to identify each group such as Dallas-HQ, Dallas-Research, or Dallas-Production.

  b. Click **Next**.

  Note: If you do not enter an address or latitude and longitude, the location displays on the right-hand pane of the Vail dashboard, but does not display on the world map.

3. Confirm the information is correct, and click **Register**.

  Wait while the BlackPearl system registers with the Vail sphere. This may take several minutes, during which time the Vail management console may display communication errors.

Select an Existing Location

Here is how to select an existing location:

1. Using the drop-down menu, **Select a Location** where you want to associate the BlackPearl Vail node and click **Next**.
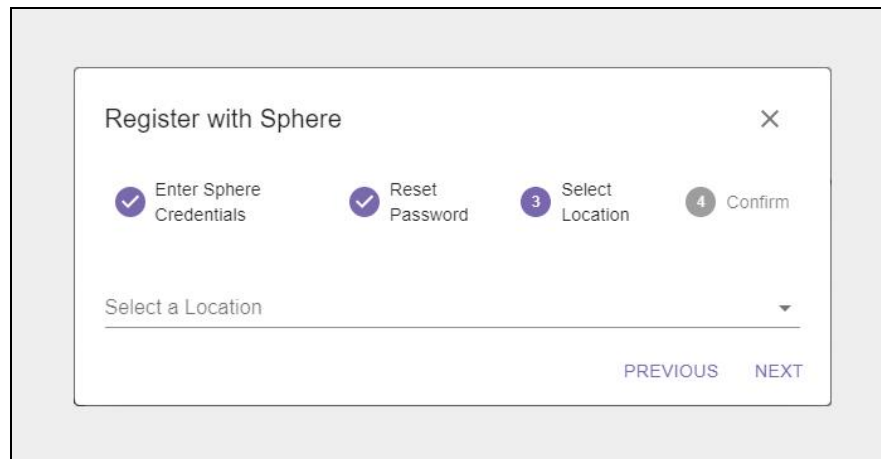
Figure 124 The Register with Sphere - Select Location screen.

2. Confirm the information is correct, and click **Register**.

  Wait while the BlackPearl system registers with the Vail sphere. This may take several minutes, during which time the Vail management console may display communication errors.

Edit the Vail Service

If desired, you can change the ports that the BlackPearl NAS solution uses to communicate with a Vail sphere.

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 73 on page 126).

2. Double-click the Sphere service, or select the service, and then select **Action > Show Details**. The details screen for the Sphere service displays.
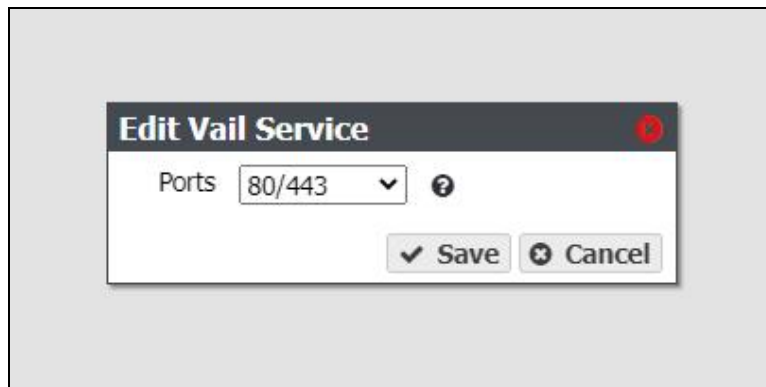
3. Select **Action > Edit**. The Edit Vail Service dialog box displays.

Figure 125 The Edit Vail Service dialog box.

4. Use the **Ports** drop-down menu to select the desired ports.

5. Click **Save**.

CONFIGURE AND USE ENCRYPTION

If your BlackPearl NAS solution includes disk or flash 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 solution power cycle. You can select to store the password on the solution, 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 197.

2. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 73 on page 126).

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

Figure 126 The Encryption service details screen.

4. Select **Action > Edit Service**.The Edit Encryption Service dialog box displays.

Note: If multi-factor authorization is enabled for the user currently logged in to the BlackPearl user interface, an additional entry field displays in the Edit Encryption Service dialog box.

Figure 127 The Edit Encryption Service dialog box.

5. 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 Encrypt or Decrypt a NAS Storage Pool on page 191 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 solution. The drives are automatically unlocked when the BlackPearl NAS solution 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 systems to the storage architecture that may access the encrypted drives. Spectra Logic recommends storing multiple copies of the password.
Encrypt and Don't Store Password	The self-encrypting drives encrypt data transferred to them, but the BlackPearl NAS solution does not store the password to unlock the drives. You must manually enter the password each time the BlackPearl NAS solution initializes. **Note:** This option is no longer available starting with BlackPearl OS 5.6. This setting is also allows you to create a USB device with the encryption password. You can use the USB device when the solution initializes to unlock the drives. Store the USB device in a safe location, not attached to the BlackPearl NAS solution, at all other times. ⚠️ **CAUTION** — Since the password is not stored on the system, you must record and store multiple copies of the password using either USB drives and/or manual records to avoid losing access to the encrypted data.

6. Enter a **Password** to unlock the self-encrypting drives, and then **Confirm** the password.

7. Enter the **User Password** of the user currently logged in to the BlackPearl user interface.

8. If necessary, enter the **Multi Factor Authentication** code for the user. See Multi-Factor Authentication on page 169 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.

9. Enter `ENCRYPT` into the confirmation dialog box.

10. Click **Save**.

   Note: You may need to navigate away from the encryption details screen and then back for the solution 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. See Email the Encryption Key on the next page

If your BlackPearl system is running BlackPearl OS 5.5 or earlier, and if the encryption service is configured to not store the password on the BlackPearl NAS solution, the USB key can be used to unlock the encrypted drives when the BlackPearl system initializes. Insert the USB key when the solution initializes to unlock the drives. Remove it from the solution USB port and store it in a safe location at all other times.

   Note: This feature is no longer available starting with BlackPearl OS 5.6.

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 73 on page 126).

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

3. Select **Action > Export Key to USB**. The Export key to USB confirmation window displays.

Figure 128 The Export key to USB confirmation window.

4. Enter the **User Password** of the user currently logged into the BlackPearl user interface.

5. Click **Create**.

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

Email the Encryption Key

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. See Export Encryption Key to USB Drive on the previous page

You must configure an email recipient and an SMTP server before you can email the encryption key. If necessary, use the instructions in the sections below.

- **Configure Mail Recipients on page 258**
- **Configure SMTP Settings on page 122**

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 73 on page 126).

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

3. Select **Action > Email key**. The Email key confirmation window displays.
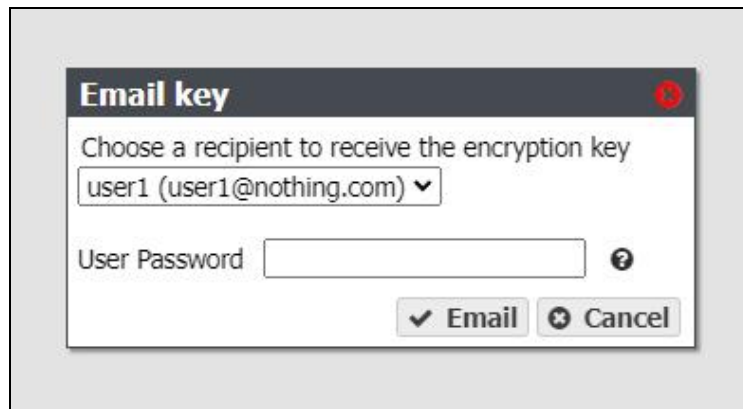
Figure 129 The Email key confirmation window.

4. Use the drop-down menu to select an **email recipient** to receive the encryption key.

5. Enter the **User Password** for the currently logged into the BlackPearl user interface.

6. Click **Email**.

Change the Encryption Password

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

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 73 on page 126).

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

3. Select **Action > Change Password**. The Change Password dialog box displays.

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 Password dialog box.
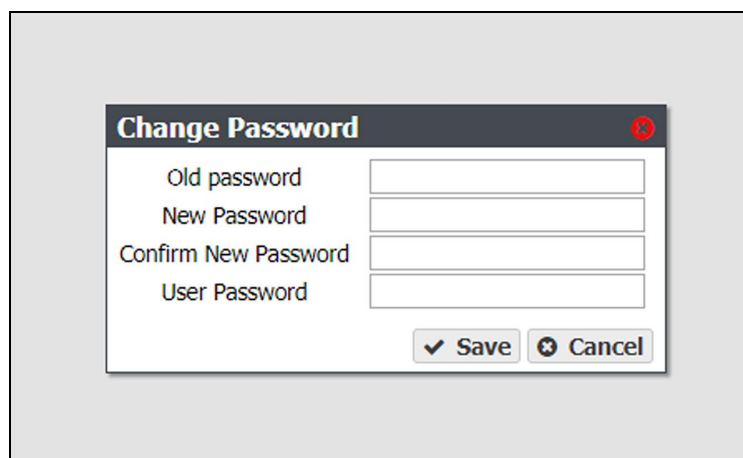
Figure 130 The Change Password dialog box.

4. Enter the (current) **Old Password**.

5. Enter the desired **New Password**, and then **Confirm** the new password.

6. Enter the **User Password** of the user currently logged in to the BlackPearl user interface.

7. If necessary, enter the **Multi Factor Authentication** code for the user. See Multi-Factor Authentication on page 169 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. Click **Save**.

⚠️ **IMPORTANT** After changing the password, update the USB keys and/or manual records stored in secure locations. See Export Encryption Key to USB Drive on page 187.

Unlock the Self-Encrypting Drives

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

1. From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 73 on page 126).

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

3. Select **Action > Unlock Drives**. The Enter Password dialog box displays.
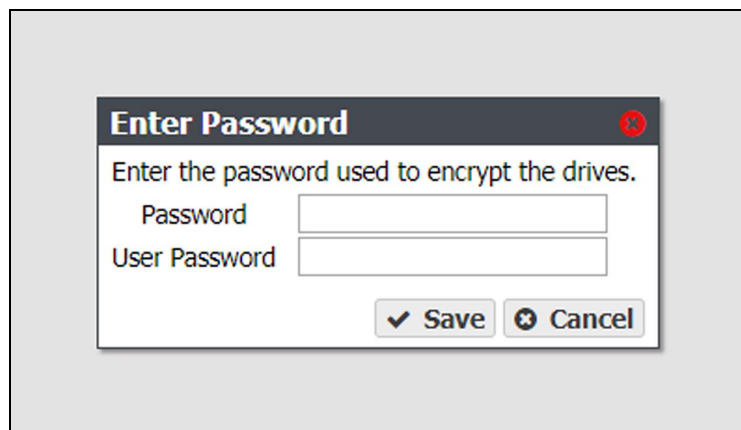
Figure 131 The Enter Password dialog box.

4. Enter the encryption **Password**.

5. Enter the **User Password** of the user currently logged in to the BlackPearl user interface.

6. Click **Save**.

Encrypt or Decrypt a NAS Storage Pool

Use the steps in this section to encrypt or decrypt the drives in a NAS storage pool after creating the pool.

1. From the menu bar, select **Configuration > NAS > Pools**.

2. Select the disk pool for which you want to enable encryption, then select **Action > Edit**.
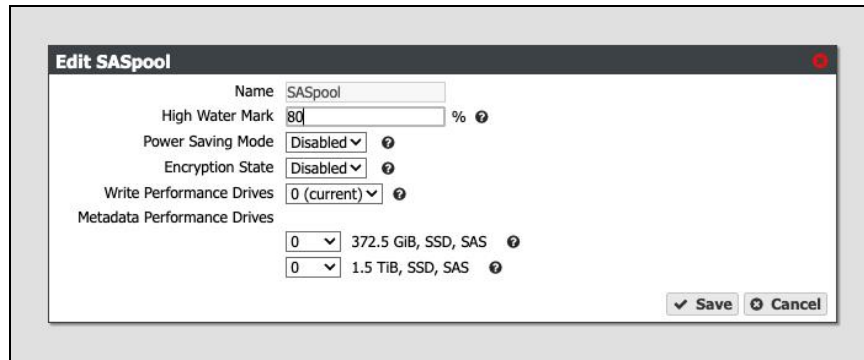
Figure 132 The Edit *storage pool* dialog box.

3. Using the **Encryption State** drop-down menu, select **Enabled** to encrypt the drives in the pool or **Disabled** to decrypt the drives.

4. If desired, make any other changes as described in Edit a Storage Pool on page 140.

5. Click **Save**.

Encrypt or Decrypt a Nearline or Online Disk Pool

Use the steps in this section to encrypt or decrypt the drives in a Nearline or Online disk pool after creating the pool.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management**.

2. Select the disk pool for which you want to enable encryption, then select **Action > Edit**.
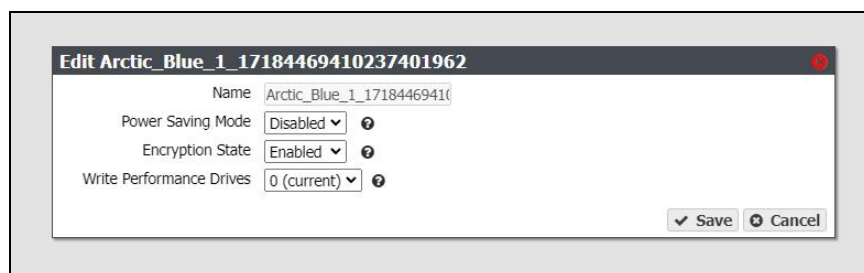
Figure 133 The Edit *disk pool* dialog box.

3. Using the **Encryption State** drop-down menu, select **Enabled** to encrypt the drives in the pool or **Disabled** to decrypt the drives.

4. If desired, make any other changes as described in Edit a Nearline or Online Disk Pool on page 1.

5. Click **Save**.

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.

1. From the menu bar, select **Status > Hardware** or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays (see Figure 148 on page 209).

2. Click **Data Drives**. The hardware screen refreshes and displays all disk drives present in the solution.

3. Record the slot number and serial number for each drive you want to PSID erase.

4. Power down the solution as described in Reboot or Shut Down a BlackPearl NAS Solution on page 218.

5. Locate the drive(s) in the chassis using the slot number and verify the serial number(s) you recorded in Step 3.

6. Locate the PSID value on the drive label and record the value.

7. Repeat Step 5 and Step 6 for any additional drives you want to erase.

8. Power on the solution as described in Power On the Solution on page 71.

9. Log into the solution as described in Log Into the BlackPearl User Interface on page 76.

10. From the menu bar, select **Status > Hardware** or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays (see Figure 148 on page 209).

11. Click **Data Drives**. The hardware screen refreshes and displays all disk drives present in the solution.

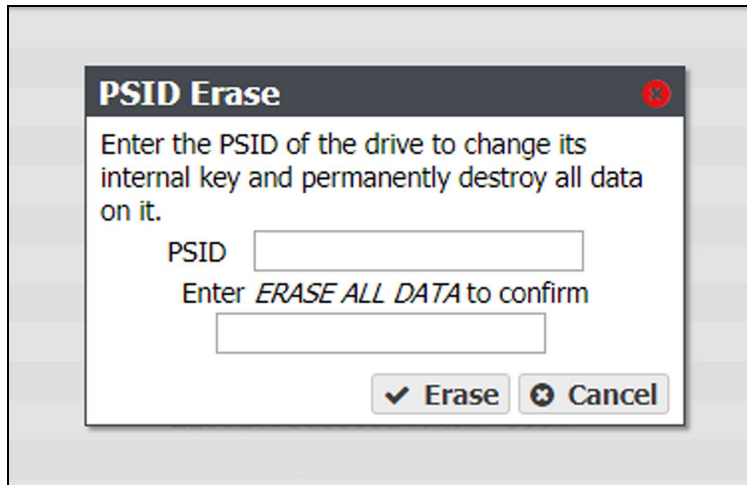**12.** On the row of the drive you want to erase, click PSID Erase. The PSID Erase dialog box displays.

Figure 134 The PSID Erase dialog box.

13. Enter the PSID value you recorded in in the **PSID** entry field.

14. Type `ERASE ALL DATA` in the confirmation entry field.

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

---

15. Click **Erase**.

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

CONFIGURE USERS

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

Description of User Types

See Description of User Types on page 84 for information about each user type.

Create a User

To create a user, see Create a User on page 84.

Edit a User

1. From the menu bar, select **Configuration > Users**. The Users screen displays a list of all configured users (see on page 84).

2. Double-click the name of the user you want to edit, or select the user and then select **Action > Edit**. The Edit Users dialog box displays.

Figure 135 The Edit User dialog box.

3. The **Username** is unavailable and cannot be changed.

4. If desired, edit the user's **Full Name**.

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

   Note: The new password does not take effect until after you log out of the BlackPearl (see Exit the BlackPearl User Interface on page 217).

6. If desired, enter a value for the **Session Timeout** in minutes. This value cannot exceed 999 minutes.

7. Select one or more **User Access** permissions. See Description of User Types on page 84 for information on each level of user access permission.

8. Click **Save**.

Delete a User

1. From the menu bar, select **Configuration > Users**. The Users screen displays a list of all configured users (see on page 84).

2. Select the user you want to delete, and then select **Action > Delete**. A confirmation window displays.

3. Click **Delete** to delete the user.

ENABLE REMOTE LOGGING

Remote Logging is a feature that allows the BlackPearl system 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 the next page.

2. From the menu bar, select **Configuration > Services**. The Services screen displays.

3. Double-click the **Remote Logging** service, or select the service and then select **Action > Show Details**. The details screen for the remote logging service displays.
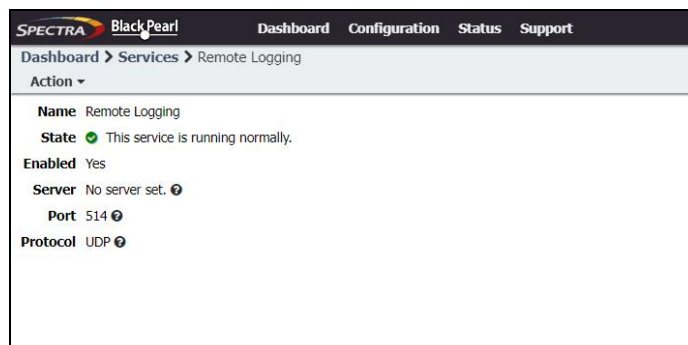
Figure 136 The Remote Logging Service details screen.

4. Select **Action > Edit**. The Edit Remote Logging Service dialog box displays.
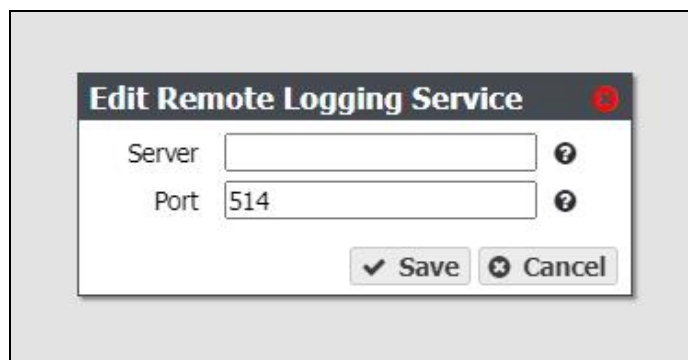
Figure 137 The Edit Remote Logging Service dialog box.

5. Enter a hostname or IP address for the remote logging **Server**.

6. Enter the **Port** used to communicate with the remote logging server.

   Note: The default port is 514.

7. Click **Save**.

MANUALLY ENTER ACTIVATION KEYS

If this is an initial installation and your BlackPearl documentation kit included a USB device, see Automatically Import Activation Keys on page 70 for instructions for importing activation keys.

Note: After entering certain Product keys, the system automatically reboots. Starting with BlackPearl OS 5.4.2, after the system initializes, you are automatically logged into the BlackPearl management interface and do not need to enter login information.

Use the following instructions to manually enter activation keys.

1. Determine the order for installing the activation keys.

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

- If you want to manually enter the activation keys for an initial installation, they must be entered in the following order
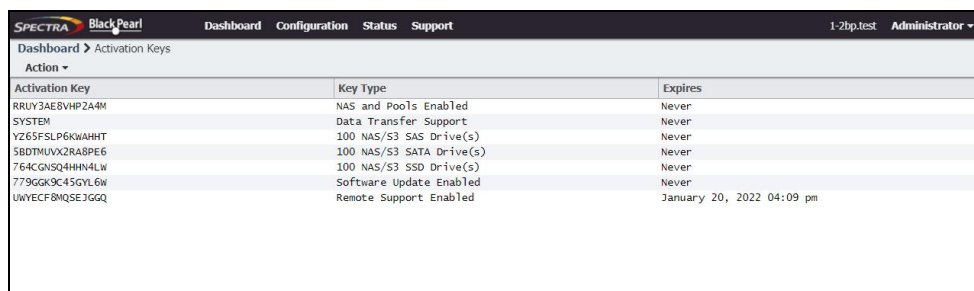
⚠	**IMPORTANT**	For an initial installation, the activation keys must be entered in the order described in these instructions. Failure to enter the keys in the proper order causes an error.

    a. Capacity keys

Key Type	Description
NAS/S3 SAS Count	Enables the specified number of SAS drives present in the system for NAS storage.
NAS/S3 SATA Count	Enables the specified number of SATA drives present in the system for NAS storage.
NAS/S3 SSD Count	Enables the specified number of SSDs present in the system for NAS storage.

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

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

Figure 138 The Activation Keys screen.

3. Select **Action > New**. The Enter Activation Key dialog box displays.
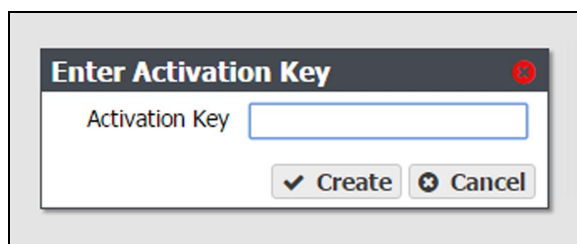
Figure 139 The Enter Activation Key dialog box.

4. Enter the key, exactly as provided, in the Activation Key field and click **Create** to save the key on the solution. The Activation Keys screen displays with the newly entered key listed.

5. If necessary, repeat Step 3 through Step 4 to add additional keys.

CHAPTER 6 - OPERATING THE BLACKPEARL NAS SOLUTION

This chapter describes procedures for day-to-day monitoring and operation of the Spectra BlackPearl NAS Solution.

MONITOR THE BLACKPEARL NAS SOLUTION

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

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

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

- System messages provide important information about the BlackPearl NAS solution and its operation (see Check System Messages on page 207 for more information).

- Icons on the Hardware screen provide overall status of the hardware components in each group (see View the Status of Hardware Components on page 208 for more information). Clicking the text next to each icon displays detailed status information for the components in the group.

- You can also use the BlackPearl user interface to do the following:

    - View the status of services (see View the Status of Services on page 210).

    - View the status of NAS pools, volumes, and shares (see View the Status of NAS Pools on page 211, View the Status of NAS Volumes on page 213, and "View the Status of NAS Shares" on page 214).

    - View performance metrics for the drives, CPUs, and network (see View Performance Metrics on page 214).

    - View the current network configuration settings (see Configure Network Connections and Settings on page 115).

    - Reboot or shutdown the solution (see Reboot or Shut Down a BlackPearl NAS Solution on page 218).

Front Bezel Visual Status Beacon

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

Color Display	Condition
Purple Scroll	The solution is operating normally. **Note:** The color displayed when the solution is operating normally can be changed on the Hardware screen. See Configuring the Visual Status Beacon Color on the next page for more information.
Yellow Scroll	The solution is experiencing a Warning condition. Log in to the BlackPearl user interface to determine the cause of the warning.
Red Scroll	The solution is experiencing an Error condition. Log in to the BlackPearl user interface to determine the cause of the error.
Rainbow	The solution is currently powering on and performing self-tests.
Flashing Blue	The beacon feature was activated for this solution. This can help you identify a specific solution when you have more than one solution in your environment. See View the Status of Hardware Components on page 208 for instructions on activating the beacon.
Pulsing Red	The Visual Status Beacon lost communication with the solution. This can occur if the solution experiences a software hang.
No Light	The BlackPearl NAS solution 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 solution is configured to display a purple scrolling light on the Visual Status Beacon when the solution is operating normally. If desired, you can change the color displayed for normal operation.

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

2. Click **Bezel**. The Bezel pane of the Hardware screen displays.

3. Click the colored box next to **Select Bezel Color**. The color picker window displays.
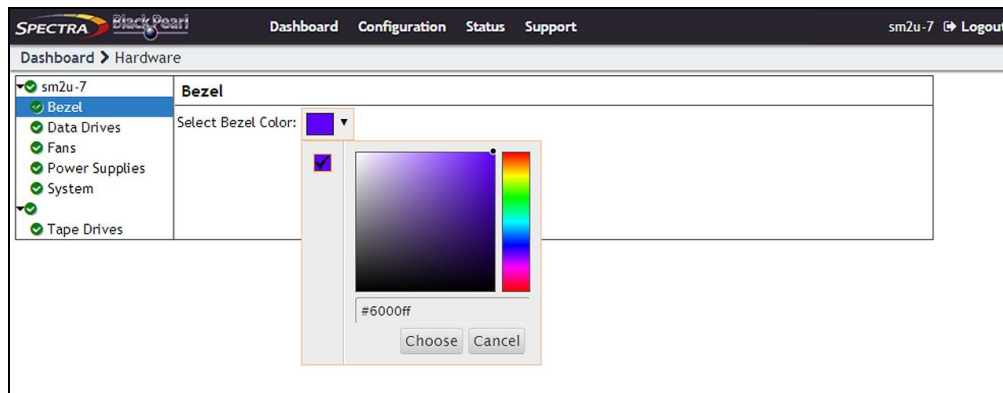
Figure 140 Use the color picker to set the color of the Visual Status Beacon when the solution is operating normally.

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

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

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

System Status LEDs

The system status LEDs provide information about the status of the solution, 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 141 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 Identify the Failed Component on page 254 for instructions.

Gen2 X Series Chassis

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

Figure 142 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 Identify the Failed Component on page 254 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 143 The top right section of the front of the Gen2 S Series chassis, with the front bezel removed, showing system status LEDs.

Figure 144 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.
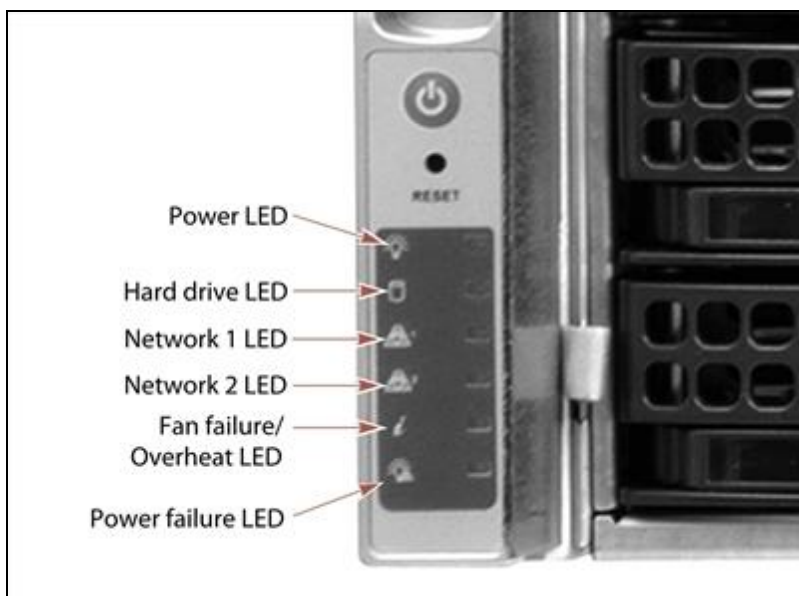
Figure 145 The left side of the front of the Gen1 S Series chassis showing system status LEDs.

LED	Function
Power	Indicates if the unit is powered on or off.
Hard Drive	Indicates boot drive activity. To see the activity of a data drive, see Data drive status LEDs on page 36.
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 solution. 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.

Check System Messages

Check the system messages regularly. These messages provide important information about the BlackPearl NAS solution 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 solution may occur.
Warning	Notifies the user of a failure that may adversely impact the BlackPearl NAS solution.
Critical	Notifies the user of a failure that caused significant adverse impact to the BlackPearl NAS solution.

If any system messages are generated by the solution, the status bar displayed at the bottom of all BlackPearl screens shows the severity, date, and time of the highest severity unread message. If there are no system messages, this text does not display.
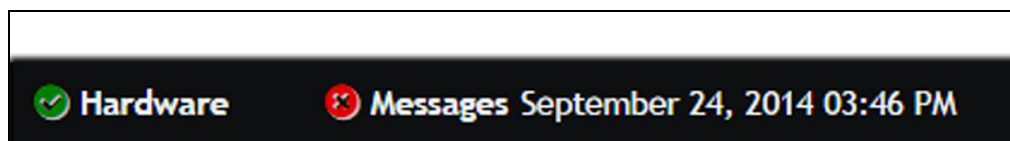
Figure 146 A system message displayed on the BlackPearl user interface status bar.

Use the instructions in this section to check system messages.

1. From the menu bar, select **Status > Messages**, or click the Messages link on the status bar, to display the Messages screen.
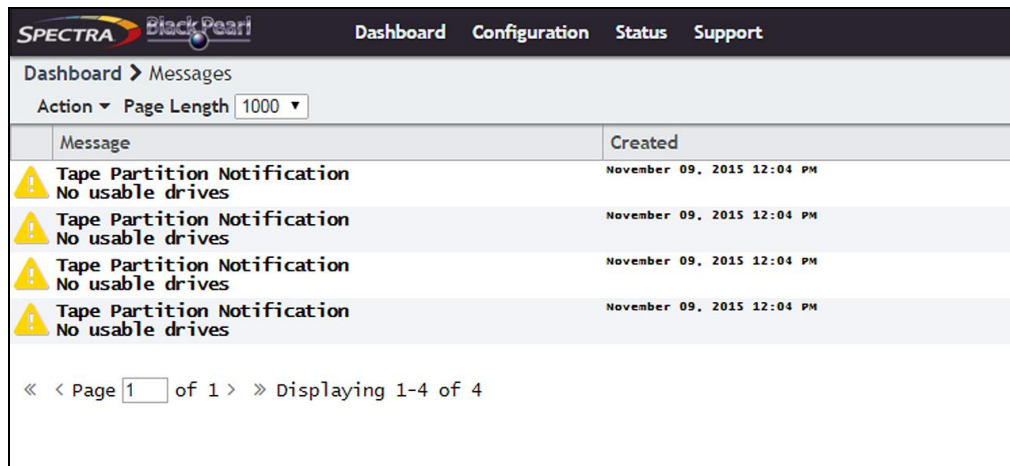
Figure 147 The Messages screen.

Pay extra attention to any messages flagged with the Warning or Error icon (see Status Icons on page 64), and follow any recommended steps. Contact Spectra Logic Technical Support if you need assistance (see Contacting Spectra Logic on page 7).

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

2. If desired, use the **Page Length** drop-down menu to limit the Messages screen to the specified number of messages.

3. To mark a single message as read, select the message and then select **Action > Mark as read**. To mark all messages as read, select **Action >Mark all as read**.

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

View the Status of Hardware Components

The BlackPearl user interface lets you monitor the status of hardware components in the solution without having direct physical access. This is especially useful when your BlackPearl NAS solution 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. From the menu bar, select **Status > Hardware** or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays.
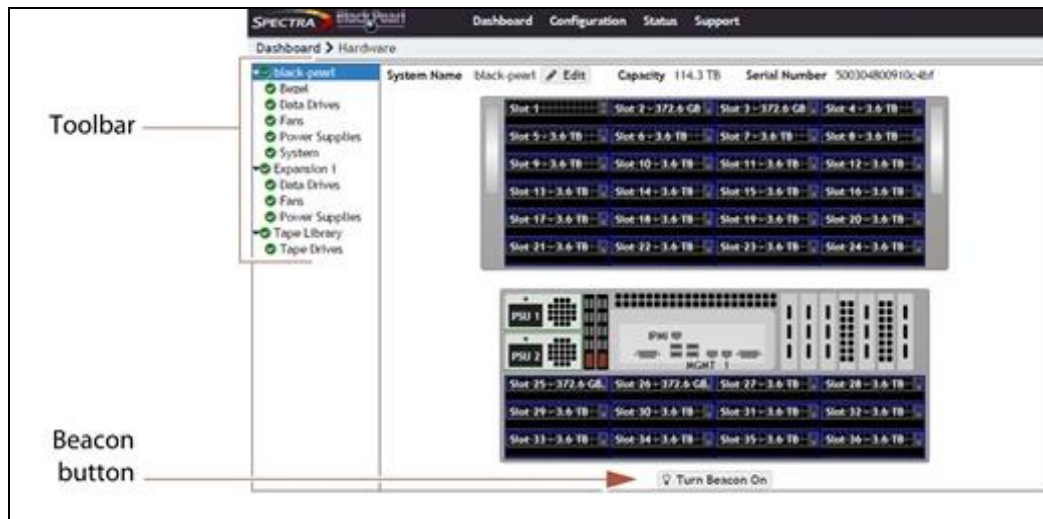
Figure 148 The Hardware screen. Gen1 S Series 4U chassis shown.

2. Use the toolbar menu on the left-hand side of the screen to view detailed information about component groups. The following table describes the types of information on each details screen. An icon next to each component indicates the status (see Status Icons on page 64 for a description of the icons).

Clicking...	Shows the...
Bezel	Color of the Visual Status Beacon that is displayed during normal operation. See Front Bezel Visual Status Beacon on page 201 for more information about the colors displayed by the Visual Status Beacon.
Data Drives	• Slot number of each drive • Status of each drive (see Data Drive Status on the next page) • Drive size, 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)
Fans	• Status of midplane fans
Power Supplies	• Power supply status and wattage **Note:** Power supply information is not available for the 77-bay or 107-bay expansion node.
System	• CPU status and temperature

Clicking...	Shows the...
	• System memory status and size • Status, manufacturer, model, size, and serial number for each boot drive
Turn Beacon On (*Below chassis graphic*)	Click **Turn Beacon On** to cause the Visual Status Beacon light on a BlackPearl NAS solution to flash blue. This is useful when you have multiple solutions and need to locate a specific one, for example to replace a component. Click the button a second time to stop the light from flashing.

Data Drive Status

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 system and must be imported.
Rebuilding	The drive is rebuilding. This typically occurs when a spare drive is promoted in the storage pool to Normal.
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 Services

The Services screen provides status information about services that are currently installed on the BlackPearl NAS solution.

From the menu bar, select **Configuration > Services** to display the Services screen.
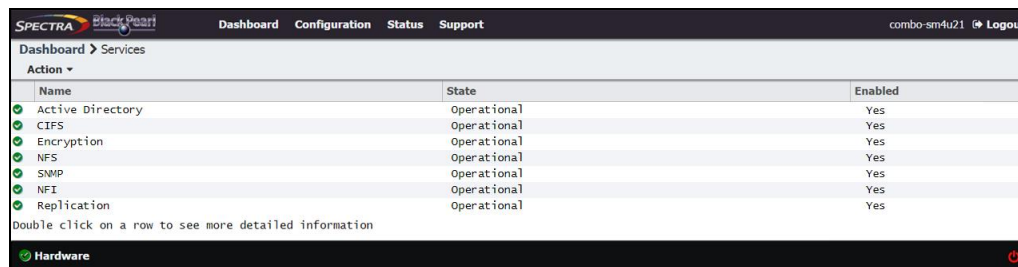
Figure 149 The Services screen.

The Services screen displays the following information:

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

View the Status of NAS Pools

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

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

2. The status of each storage pool is indicated by the status icons on the left side of the screen.
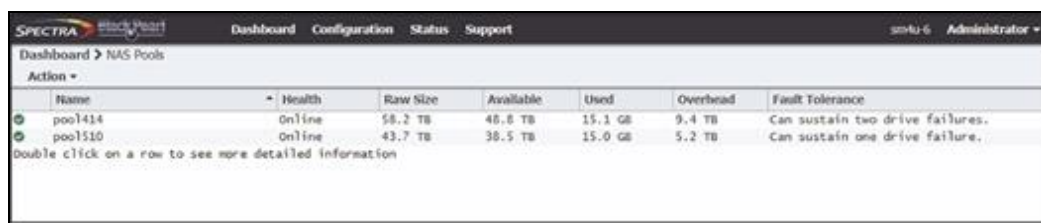
Figure 150 The Pools screen.

The Pools screen displays the following information.

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

3. To view additional information about a NAS pool, select the pool and then select **Action > Show Details**. The *pool name* details screen displays.
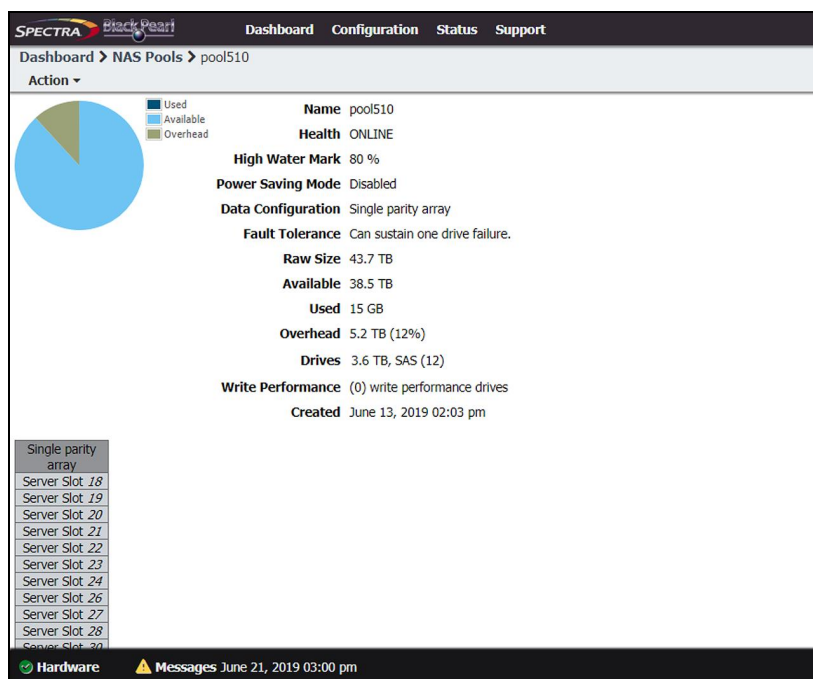
Figure 151 A NAS Pool details screen.

The *pool name* details screen displays the following information:
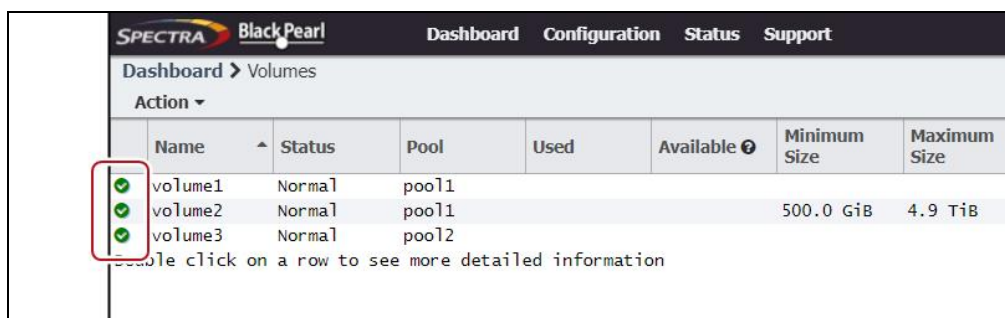
This row...	Shows...
Name	The name of the pool.

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

View the Status of NAS Volumes

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

1. From the menu bar, select **Status > NAS > Volumes** to display the Volumes screen.

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

Figure 152 The Volumes screen.

View the Status of NAS Shares

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

1. From the menu bar, select **Configuration > NAS > Shares > CIFS** to display the CIFS Shares screen, select **Configuration > NAS > Shares > NFS** to display the NFS Shares screen, or select **Configuration > NAS > Shares > Vail S3** to display Vail Shares.

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

Figure 153 The CIFS Shares screen.

View Performance Metrics

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

Use the instructions in this section to view performance metrics.

1. From the menu bar, select **Status > Performance** or click the Performance pane on the Dashboard. The Performance screen displays. The Performance screen displays.
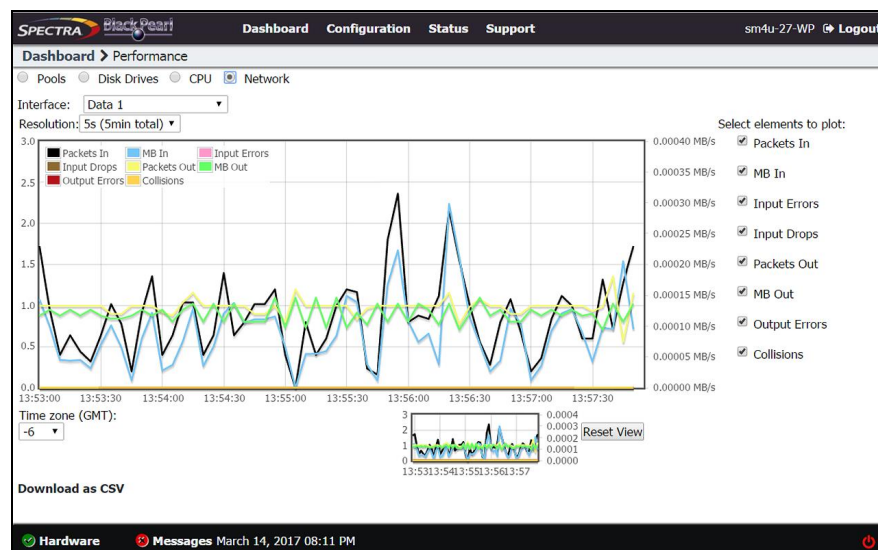
Figure 154 The Performance screen.

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

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

3. Select the time interval using the **Resolution** drop-down menu. The data can be displayed in 1 second increments (5 minutes total) or 1 hour increments (25 hours total).

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

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

6. If desired, click **Download as CSV** on the lower, left side of the panel, to download a comma separated value file containing the data for the graph you are currently viewing. The file can then be imported into Microsoft Excel® or other software applications that support this file type.

7. To see the performance data in greater detail, select the desired section you want to magnify in either the main or range indicator graph. Using the mouse, click and drag the cursor horizontally over the section of the detail graph that you want to magnify. The highlighted section of data is shown on the main graph.

The range indicator graph continues to display the original range of data, with the section that is currently being shown on the main graph highlighted.
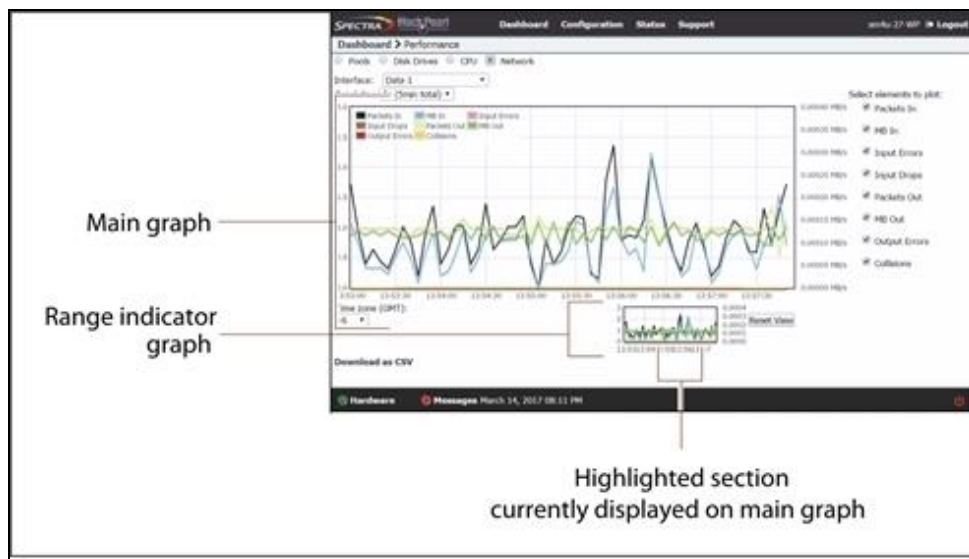
Figure 155 Highlight a section of data to show in greater detail.

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

View Reports

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

1. From the menu bar, select **Status > Reports** to display the Reports screen.
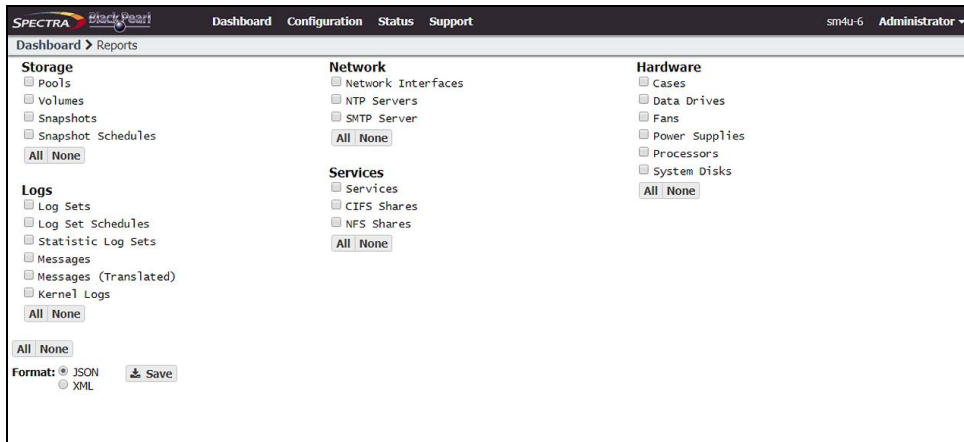
Figure 156 The Reports screen.

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

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

3. Select the **Format** for the report(s). Only one format can be selected.

4. Click **Save**. The selected reports are saved to your local host.

5. Open the report using a compatible program.

EXIT THE BLACKPEARL USER INTERFACE

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

If the active session is idle for more than the set session timeout, the current user is automatically logged out. This setting can be configured on the Accounts screen. The default is 60 minutes. See Configure Users on page 194.

REBOOT OR SHUT DOWN A BLACKPEARL NAS SOLUTION

This section discusses rebooting or shutting down a solution.

Using the BlackPearl User Interface

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

1. Click the power icon in the lower right-hand corner of any screen in the BlackPearl user interface. The Power screen displays.
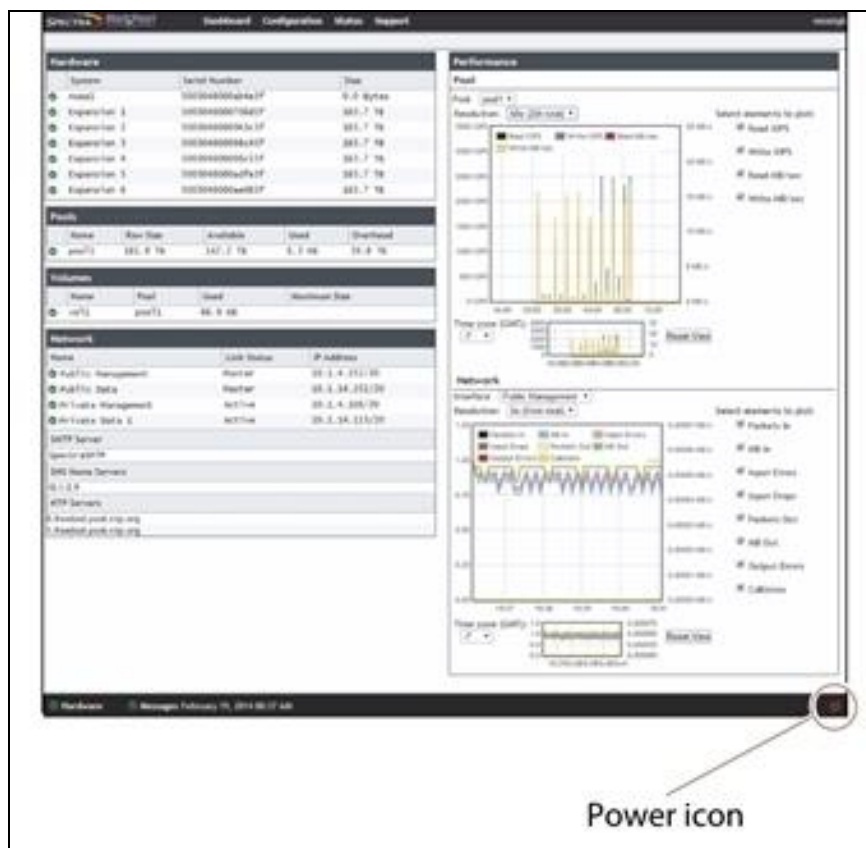
Figure 157 The Power icon.

2. Click either **Reboot** or **Shutdown**.

3. A confirmation screen appears. Confirm the selection to perform the reboot or shutdown.

Power-Cycle Reset

Under some circumstances, Spectra Logic Technical Support may direct you to perform a power-cycle reset of a BlackPearl NAS solution to recover from an error. To power-cycle reset a BlackPearl NAS solution, remove the front bezel, and then press and hold the front panel power button (Figure 27 on page 71) until the button's LED turns off. After a few moments, press the button again to turn the solution back on.

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

CHAPTER 7 - EMBEDDED DASHBOARD

This chapter describes the embedded dashboard of the BlackPearl management interface. The embedded dashboard is used by other Spectra Logic applications to display an overview of the system, display jobs, tape management, and other common functions within the Spectra application. However, the embedded dashboard may be used separately for certain tasks in place of the BlackPearl management console.

USING THE EMBEDDED DASHBOARD

The embedded dashboard allows you to quickly view the status of critical aspects of the BlackPearl NAS NAS solution and easily perform commonly used functions of the system.
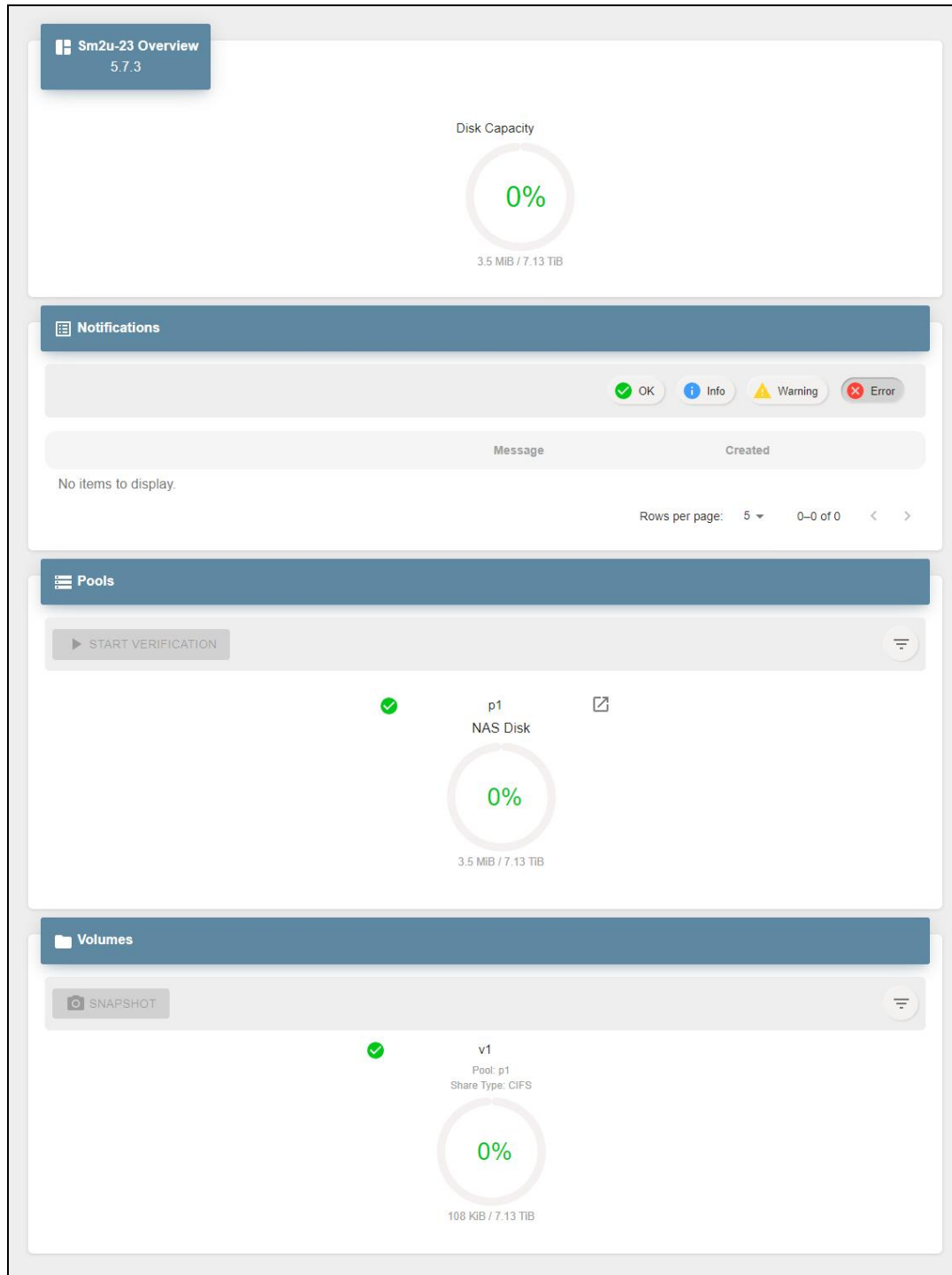
Figure 158 The Embedded Dashboard.

VIEW THE STATUS OF THE BLACKPEARL SYSTEM

Use the sections below to view the status of multiple aspects of the BlackPearl NAS solution.

View System Overview

The Overview pane provides a quick look at the most critical aspects of the BlackPearl NAS solution.
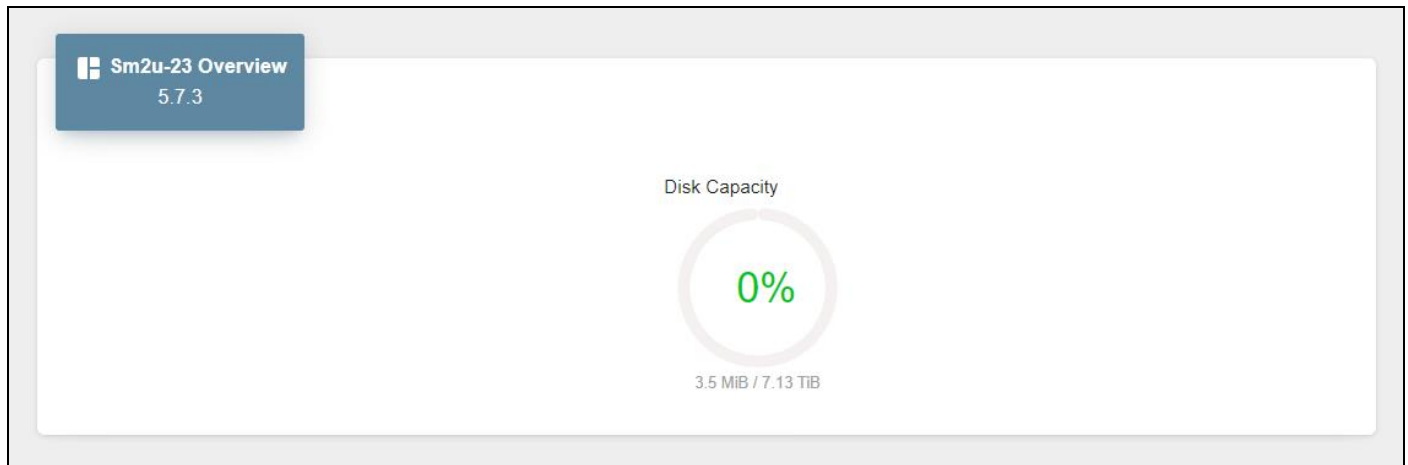
Figure 159 The Overview pane.

1. The capacity of all disk-based storage connected to the BlackPearl NASsolution and percentage of used space.

Mouse-over the green section of any percentage graph to display the amount of used space, and over the gray section to display the amount of remaining space.
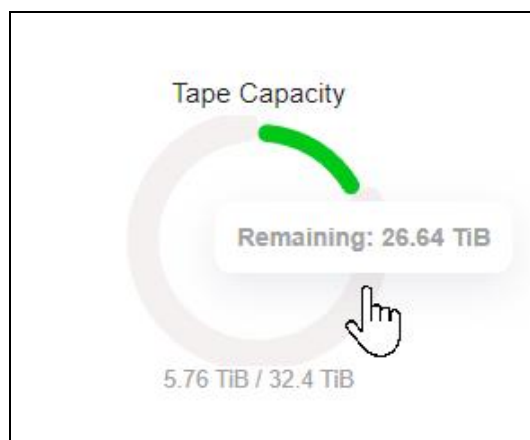
Figure 160 Mouse-over a graph to view specific details.

View Notifications

Notifications provide information about errors that occur on the system, caution messages that alert you to issues that may impact your workflow, and informational messages. Additionally, notifications may provide troubleshooting advice to help you resolve issues that may occur.
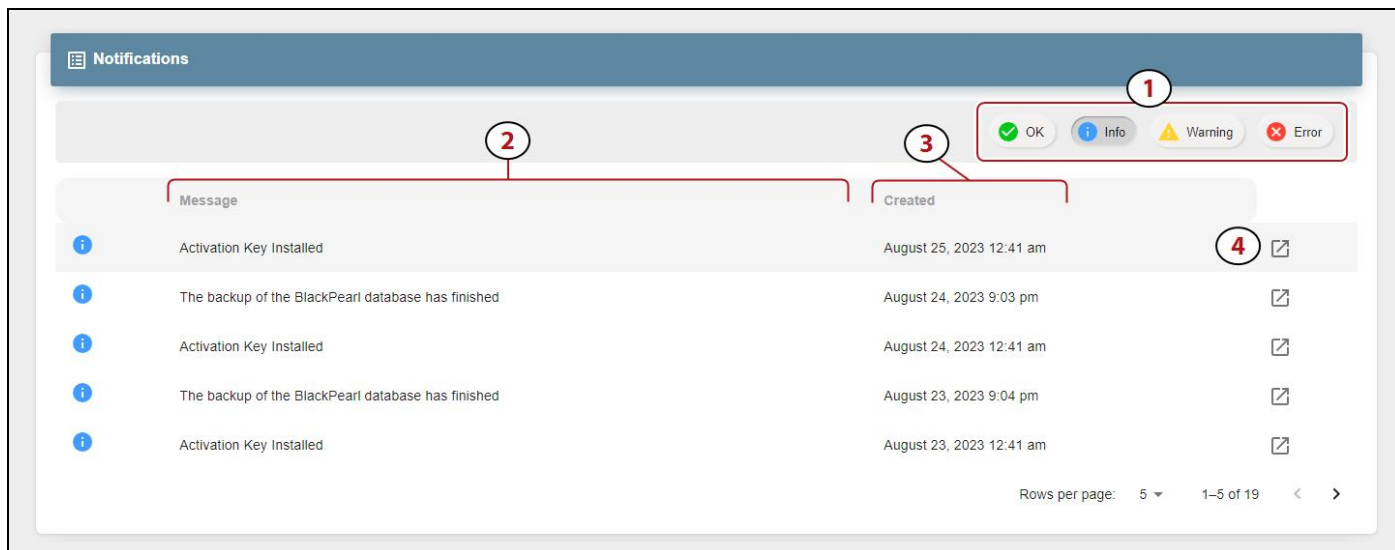
Figure 161 The Notifications pane.

1. Use the **Notification Type** buttons to switch between OK, Info, Warning, and Error messages.

2. Contains a brief description of the notification.

3. Displays the timestamp the notification was generated.

4. Click the **Details Button** to view additional message **Details** and **Troubleshooting Advice**.
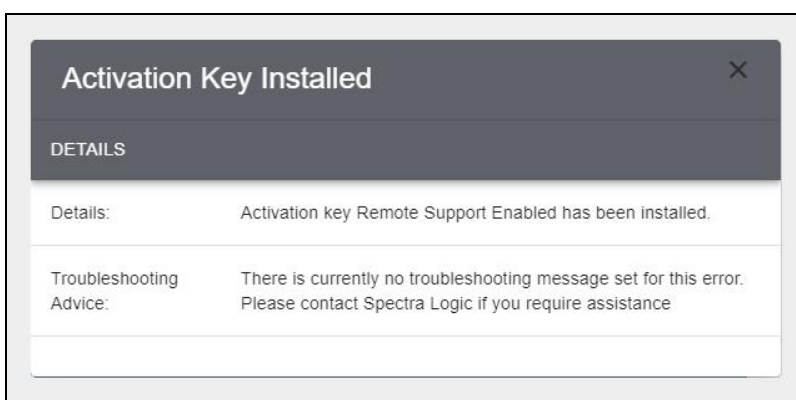
Figure 162 The Notification details dialog box.

View Pools

The Pools pane displays information about all disk storage pools configured on the BlackPearl NAS solution.
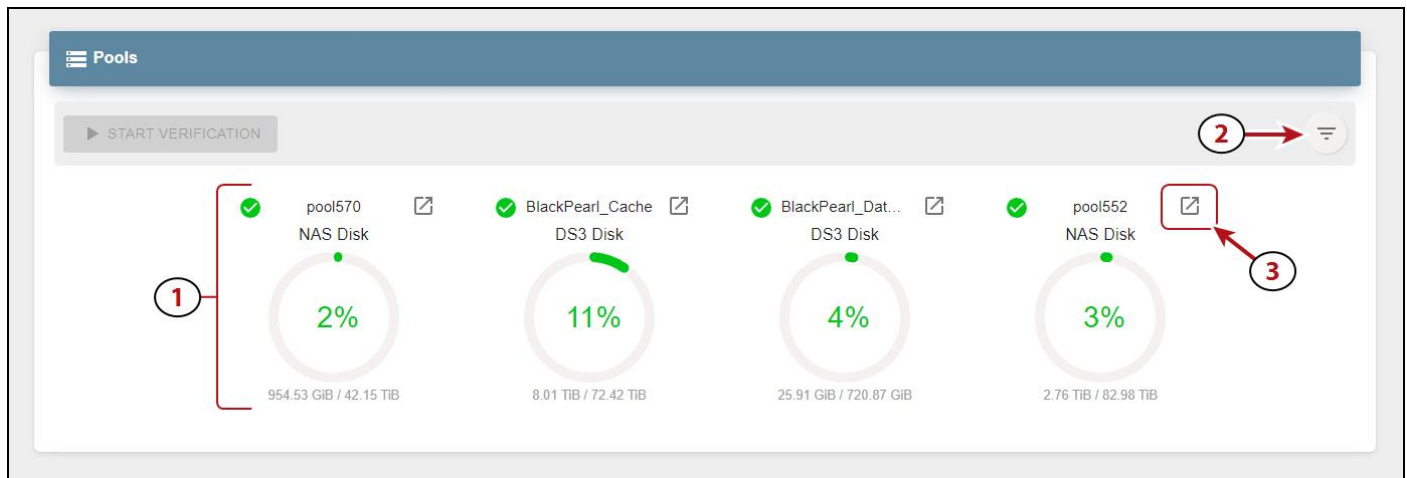
Figure 163 The Pools pane.

1. Each percentage graph displays both the used and remaining space for the associated pool.

2. Use the **Filter** button to select which pools to display on the Pools pane.

3. Click the **Details** button to view additional information about a specified pool.
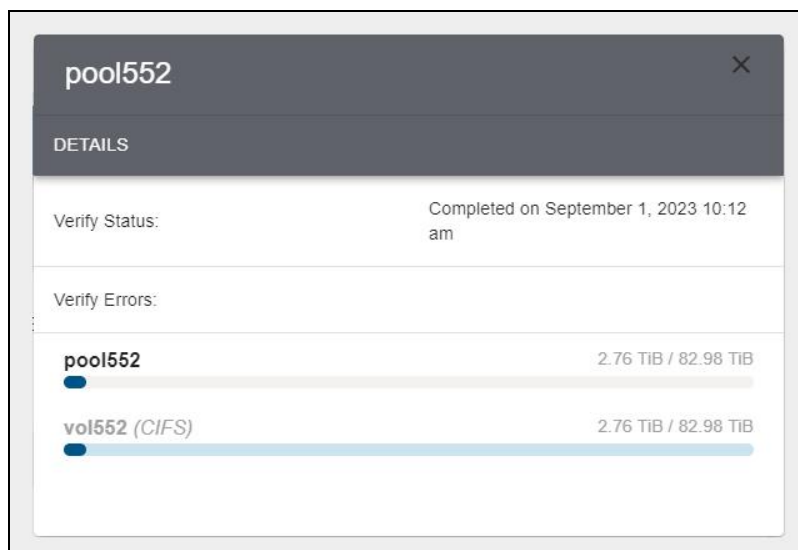
Figure 164 The pool details dialog box.

Use the **Start Verification** button to verify the data contained on the pool. See for more information.

View Volumes

The Volumes pane displays information about all volumes configured on the BlackPearl NAS solution.
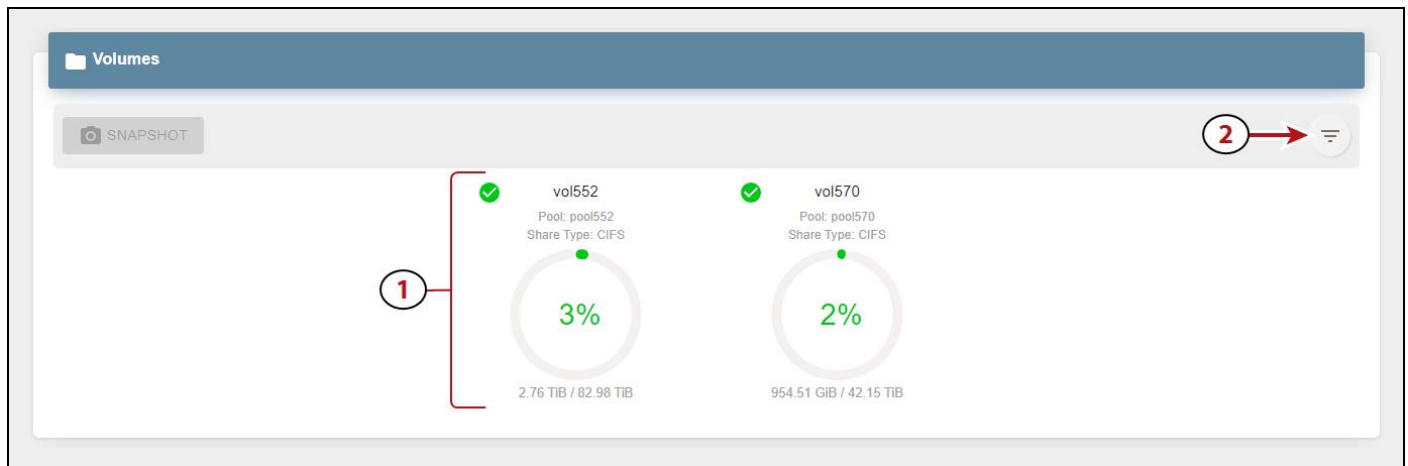
Figure 165 The Volumes pane.

1. Each percentage graph displays both the used and remaining space for the associated pool.

2. Use the **filter button** to select which pools to display on the Pools pane.

Use the **Snapshot** button to create a snapshot. For more information see Create a Volume Snapshot on the next page.

Dashboard Actions

In addition to displaying information about the BlackPearl NAS system, the embedded dashboard allows you to perform the most frequently-used actions as described in the sections below.

Create a Volume Snapshot

A volume snapshot is an image 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.

See Volume Snapshots on page 149 for more information.

Here is how to create a volume snapshot:

1. In the BlackPearl dashboard, navigate to the **Volumes** pane.

2. **Select** the volume for which you want to create a snapshot.

3. Click **Snapshot**.

4. If desired, edit the pre-generated **Snapshot** name.
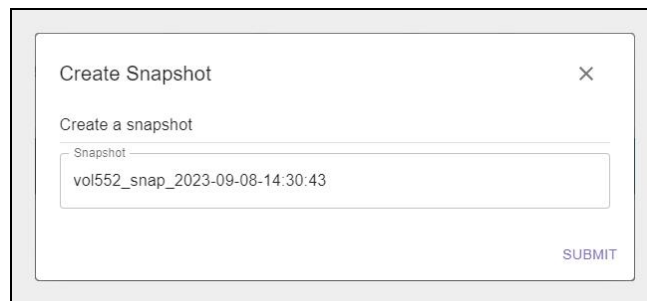
Figure 166 The Export Tape dialog box.

5. Click **Submit**.

Start a Storage Pool Verification

The BlackPearl system can perform a data integrity verification of all data on a selected storage pool to confirm it is still viable.

Here is how to start data verification on a storage pool:

1. In the BlackPearl dashboard, navigate to the **Pools** pane.

2. **Select** the pool that you want to verify.

3. Click **Start Verification**.

4. Click **Submit**.

CHAPTER 8 - MAINTAINING THE BLACKPEARL NAS SOLUTION

This chapter describes the maintenance procedures for the Spectra BlackPearl NAS Solution.

DATA INTEGRITY VERIFICATION

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

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

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

1. From the menu bar, select **Support > Tools > Data Integrity Verification.** The Data Integrity Verification screen displays.
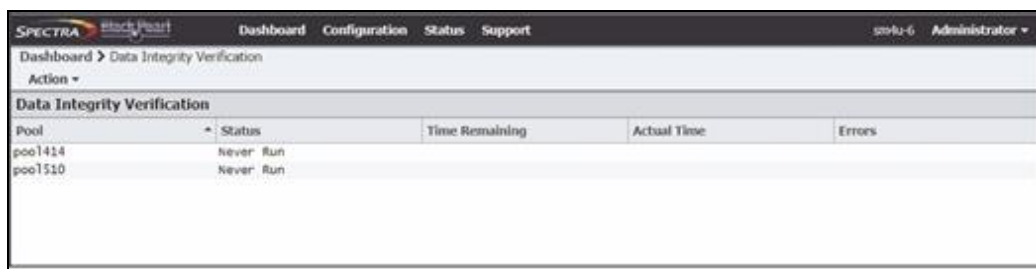
Figure 167 The Data Integrity Verification screen.

2. Select the disk pool for which you want to start the data integrity verification, and select **Action > Start.** A confirmation screen displays.

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

3. Click **Start Data Verification**.

⚠️ 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 solution and then PUT the object again. delete and then reimport the object, The affected files cannot be retrieved from the storage pool, and may need to be transferred to the BlackPearl NAS solution 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 Data Integrity Verification

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

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

2. Select the pool for which you want to stop verification in the Data Integrity Verification screen, and then select **Action > Cancel**.

3. A confirmation screen displays. Click **OK** to stop the verification.

INITIATE RSC BACKUP

The replicated system configuration backup stores the current configuration of all settings for the BlackPearl NAS solution on a storage pool present in the solution. 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 solution, Spectra Logic recommends that you backup the configuration manually.

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

1. From the menu bar, select **Support > Tools > Data Integrity Verification.** The Data Integrity Verification screen displays (see).

2. Select **Action > Initiate RSC Backup.** A confirmation screen displays.

3. Click **Initiate RSC Backup** to manually backup the current solution configuration.

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 solution, and additional service and support tools. You can also open or update a support incident and upload log files.

Create an Account

Access to User Guides and compatibility matrices does not require you to create an account. You must create a user account and log in to access Release Notes or repair documents, to download the latest version of 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**.
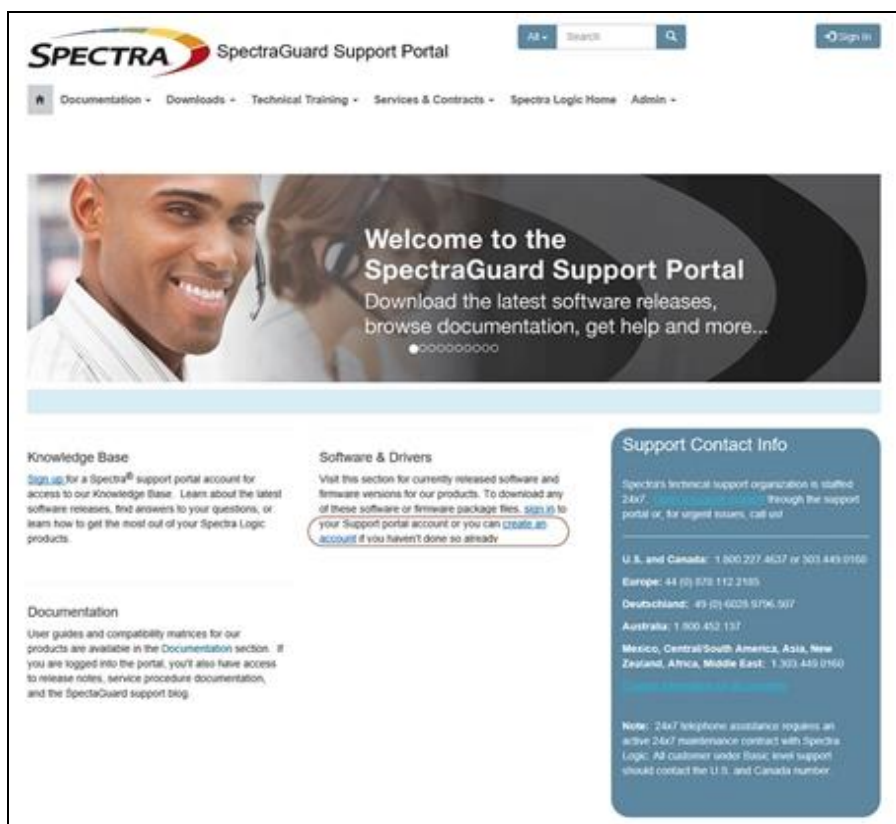
Figure 168 The Spectra Logic Technical Support portal home page.

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 169 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.

CONFIGURE AUTOMATED SOFTWARE UPLOAD

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

Note: You must have a current software update key entered in the solution you want to configure to use Automated Software Upload. See Manually Enter Activation Keys on page 197 for more information.

Use the instructions in this section to configure Automated Software Upload.

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

2. Select **Action > Edit Automated Software Upload**. The Automated Software Upload dialog box displays.
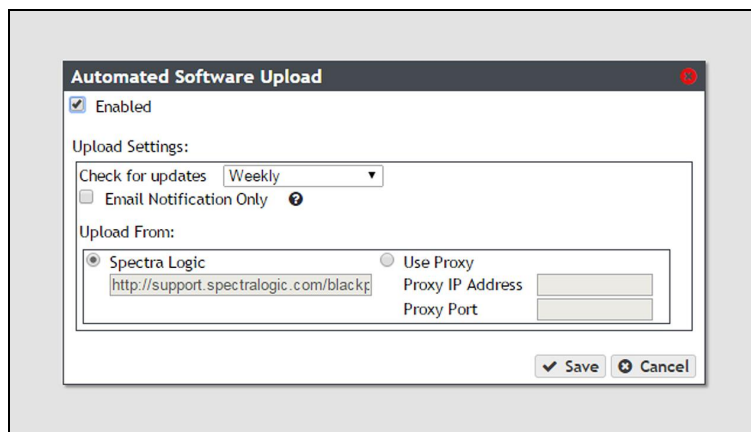
Figure 170 The Automated Software Upload dialog box.

3. Select the **Enabled** check box to enable the feature.

4. Use the drop-down menu to select the **Check for updates** frequency.

5. Optionally, select the **Email Notifications Only** check box to only receive an email when an updated software package is available instead of automatically downloading the file.

6. Select either **Spectra Logic** or **Use Proxy** as the **Upload From** location.

⚠ **IMPORTANT**   Spectra Logic recommends using the **Spectra Logic** package server.

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

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

7. Click **Save**.

UPDATE THE SOFTWARE

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

> **Note:** You must have a current software update key entered in the solution you want to update. See Manually Enter Activation Keys on page 197 for more information.

If Automated Software Upload is enabled, the solution sends an email to all users configured to receive Warning or Informational emails (see Configure Mail Recipients on page 258) and posts a system message to the Messages screen. If configured to do so, the solution also downloads the updated software.

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

- If the update package downloaded automatically, skip to Install the Update on page 238.

- If you were notified that an update is required, but the update did not download automatically, skip to Download and Stage the Updated Software on page 237.

- If you do not know if the solution needs an update installed, continue with Check the Current Software Version below.

⚠ **IMPORTANT**	When upgrading to OS 5.4.x or later, if you connect to a tape library through a fabric switch which has zoning configured to use WWPNs, make sure to update the switch zoning configuration to include the updated HBA WWPNs. This zoning configuration update must be done prior to upgrading the BlackPearl system to avoid a forced full tape inspection of all tape media.

Check the Current Software Version

Use the following steps to determine the current software version running on your BlackPearl NAS solution.

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

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

Figure 171 The current BlackPearl software version.

Check the Currently Released Software Version

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

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

   Note: See Create an Account on page 231 for information about creating an account and accessing the Technical Support portal.

2. Select **Downloads > Product Software**.

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

Figure 172 The Product Software screen.

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

Download and Stage the Updated Software

Use the instructions in this section to download and stage the updated software for the BlackPearl NAS solution.

1. Log into your account on the Technical Support portal at *support.spectralogic.com*.

2. Select **Downloads > Product Software**. The Product Software Screen displays.

Figure 173 The Product Software screen.

3. Locate the BlackPearl NAS solution in the **SpectraProduct** column. The currently released BlackPearl software version is listed in the **Current Version** column.

4. Click the name of the BlackPearl package. The package begins downloading through your web browser. Do not unzip the downloaded file.

5. From the BlackPearl menu bar, select **Support > Software** to display the Software screen. Click **Choose File.** Using your web browser, browse to the location of the update file and select the file to upload. The file is staged to the solution.
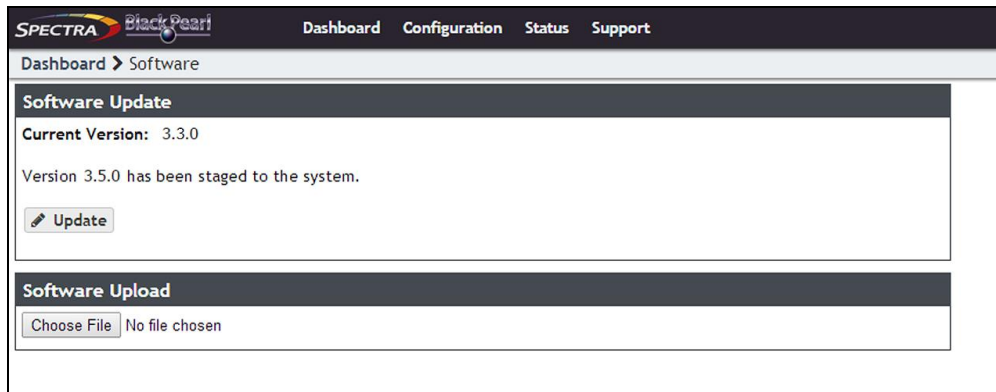
Figure 174 The Software Update screen with an available software package listed.

Install the Update

1. Discontinue all file storage operations on the BlackPearl NAS solution. The solution automatically reboots as part of the update process.

2. From the menu bar, select **Support > Software** to display the Software screen. The Software screen displays with the software upload file staged to the solution.
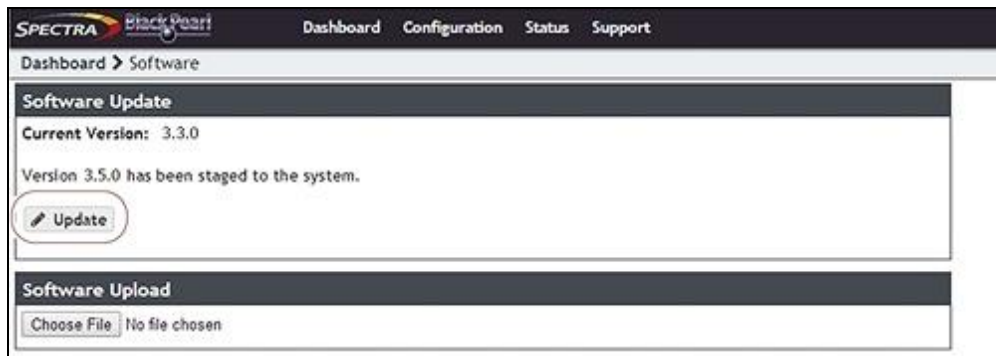
Figure 175 The Software Update screen with a software package staged to the solution.

3. Click **Update**. A progress bar shows the progress of the update.
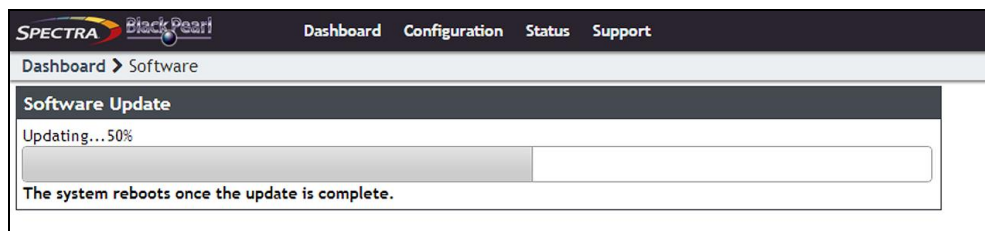
Figure 176 The Software Update screen showing the progress of an update.

4. When the update is complete, the BlackPearl NAS solution automatically reboots to begin using the latest software.

5. Restart file storage operations.

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 248
- Install a Drive in a Gen2 X Series Chassis on page 249
- Install a Drive in a Gen1 Chassis on page 251

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.
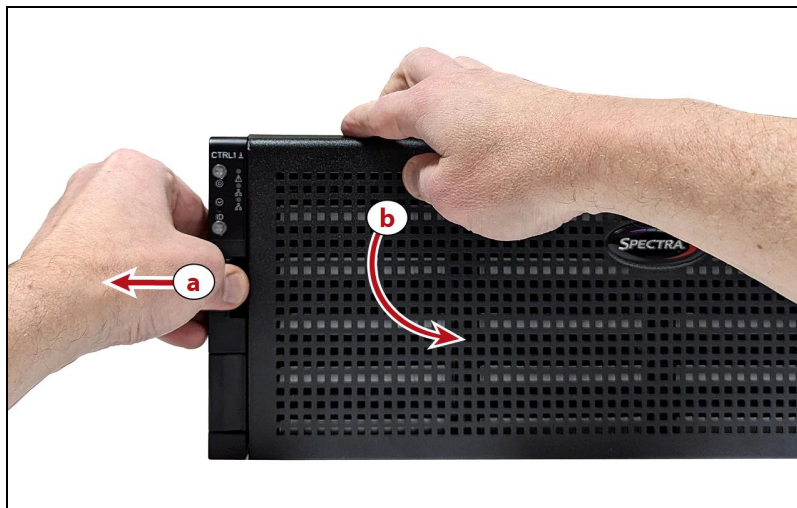
Figure 177 Remove the front bezel.

   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.
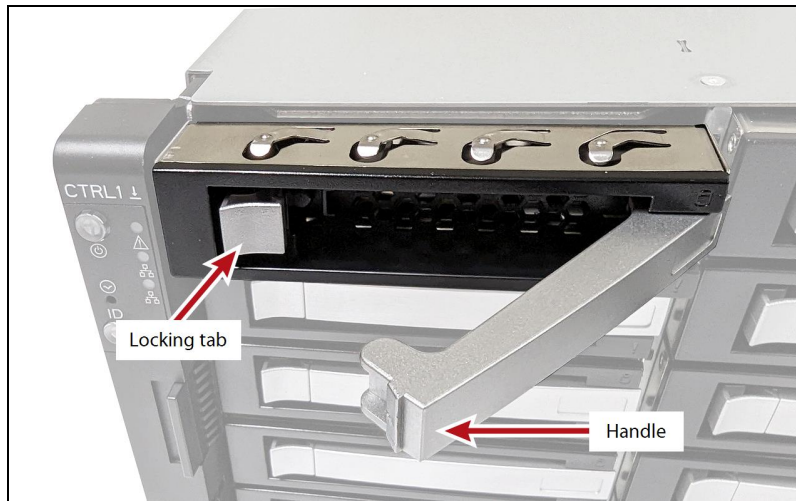
Figure 178 Unlock the drive sled.

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 179 Screw holes in drive.   **Figure 180** PEMs on right side of sled.
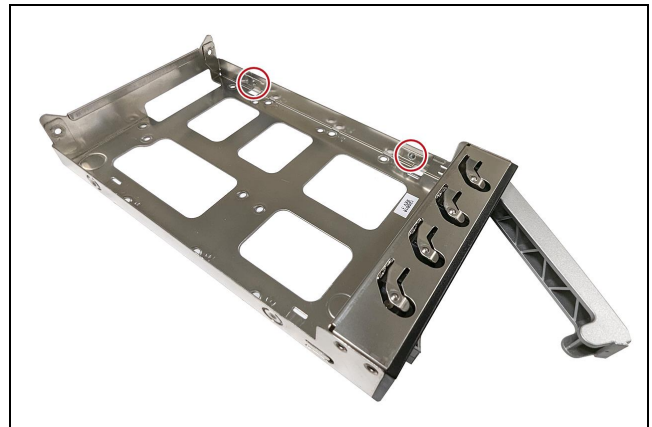
6. Rotate the left side of the drive down into the sled until it snaps into place.

Figure 181 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 182 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.
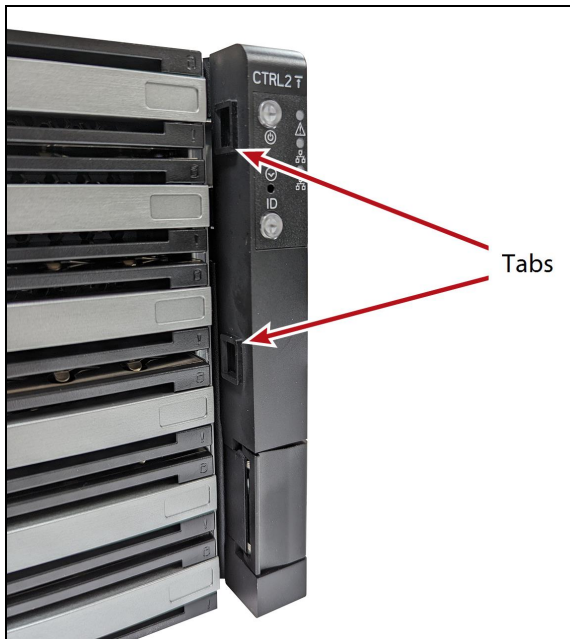
Figure 183 Tabs on the side of power control.
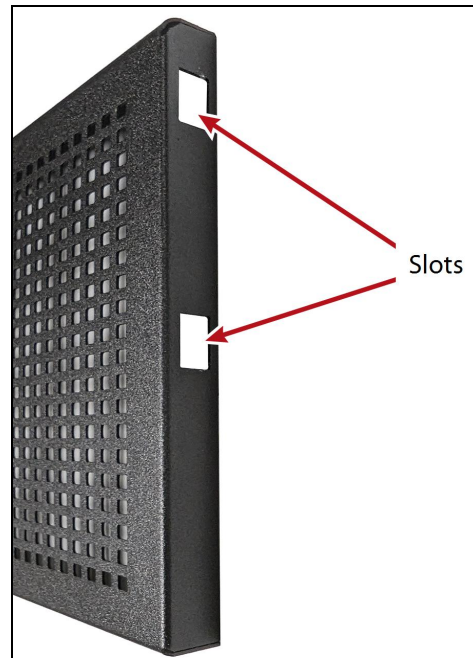
Figure 184 Slots in side of front bezel.

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 185 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.
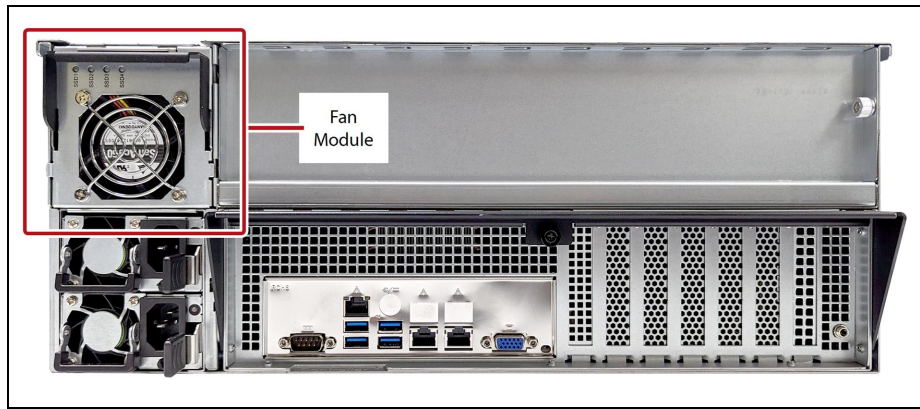
Figure 186 The NVMe drive fan module.

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.
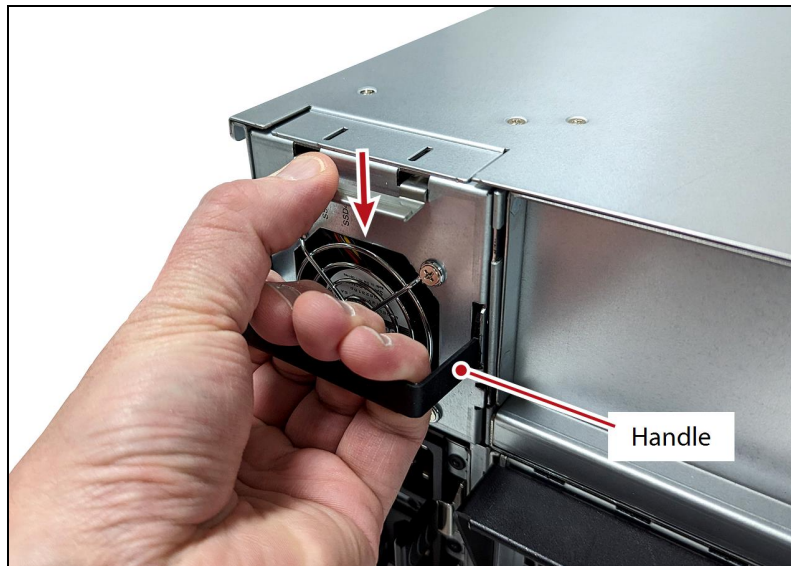
Figure 187 Remove the NVMe drive fan module.

3. Press the tab on the right side of the sled you want to remove to extend the handle.
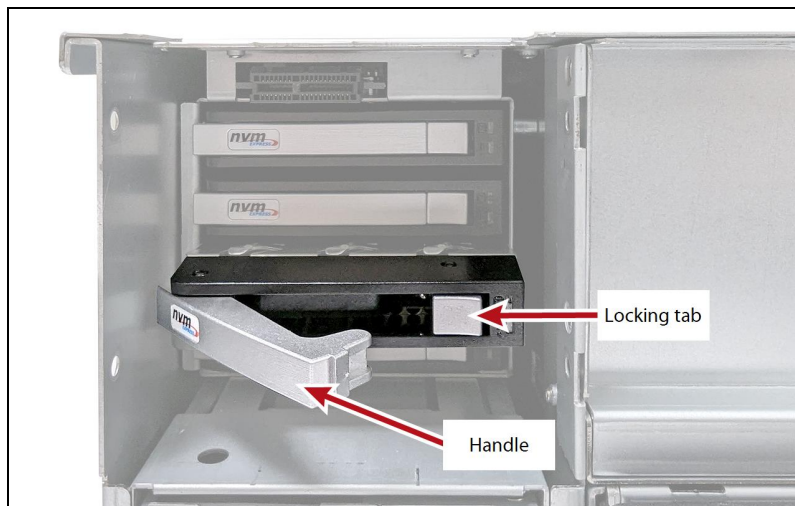
Figure 188 Unlock the drive sled.

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 189 Screw holes in drive.

Figure 190 PEMs on right side of sled.

7. Rotate the left side of the drive down into the sled until it snaps into place.
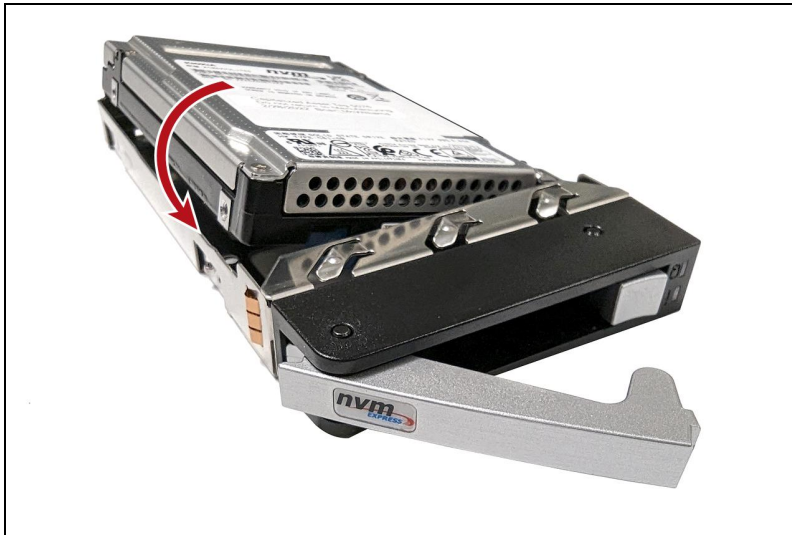
Figure 191 Install the drive into the sled.

8. Slide the drive sled all the way into the chassis, then rotate the sled handle towards the chassis until it locks into place.
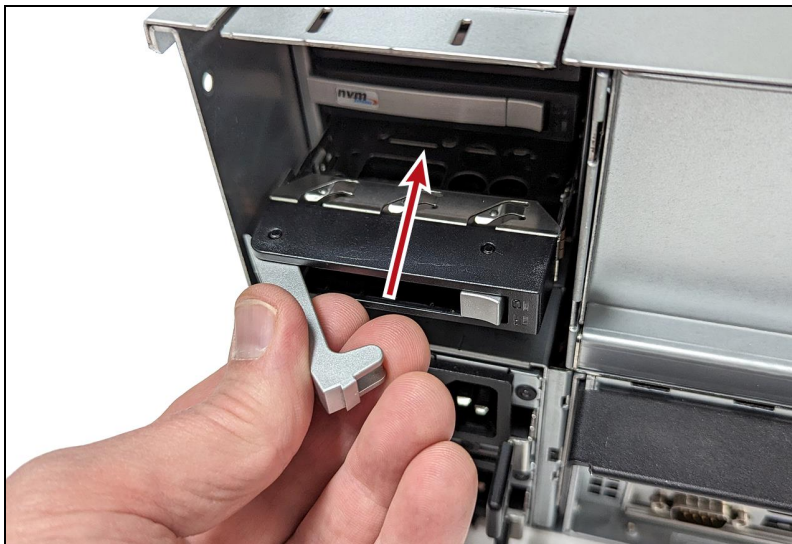
Figure 192 Insert drive into chassis.

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.
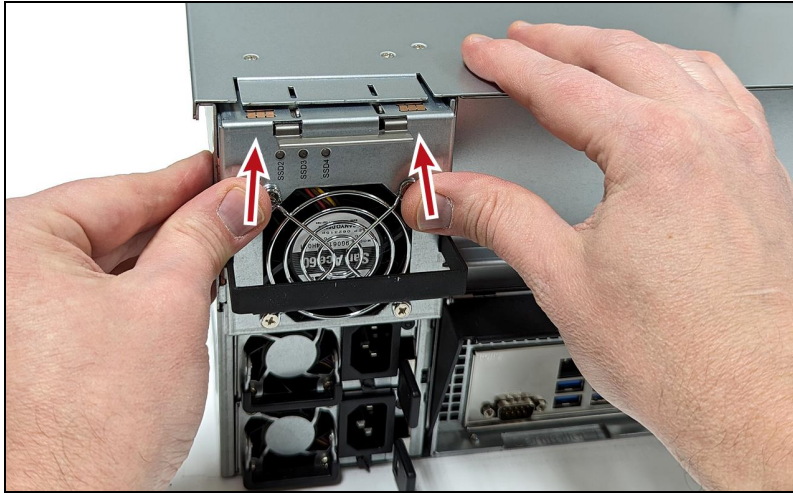
Figure 193 Insert drive into chassis.

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.
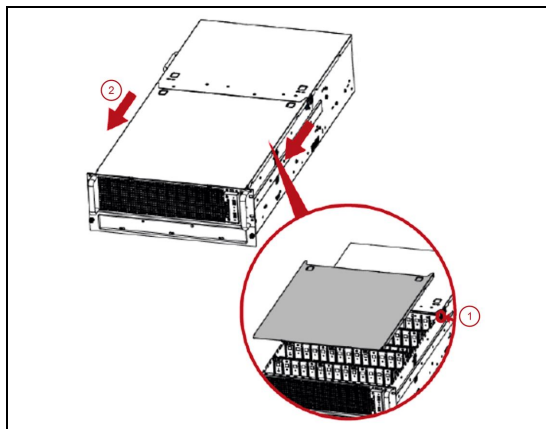
Figure 194 Remove the front top cover.

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**).
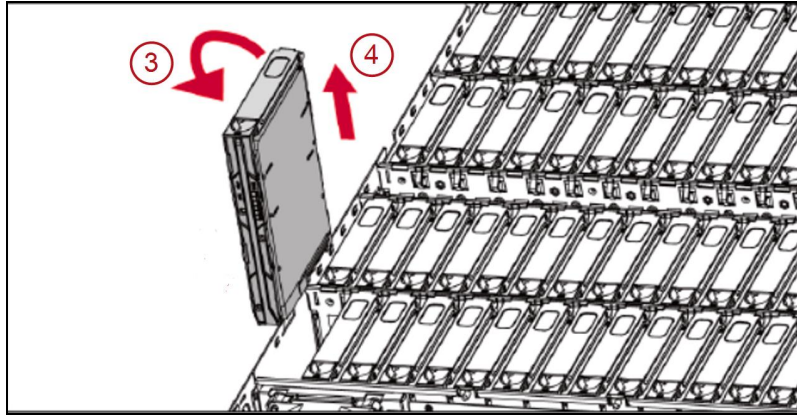
Figure 195 Remove the drive from the BlackPearl chassis.

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.
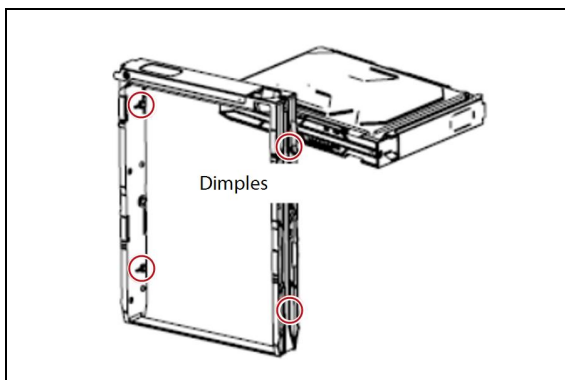
Figure 196 Match the dimples on the drive sled to the dimples on the drive.
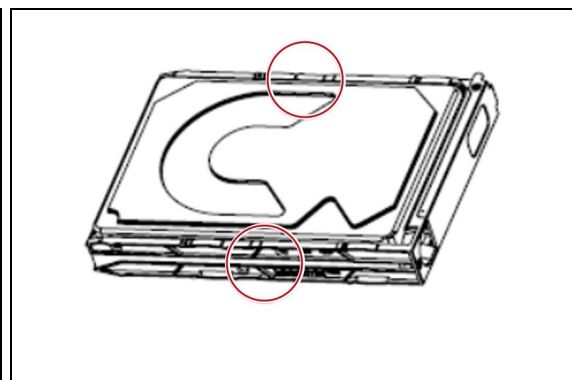
Figure 197 The drive installed in the drive sled.

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 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**).
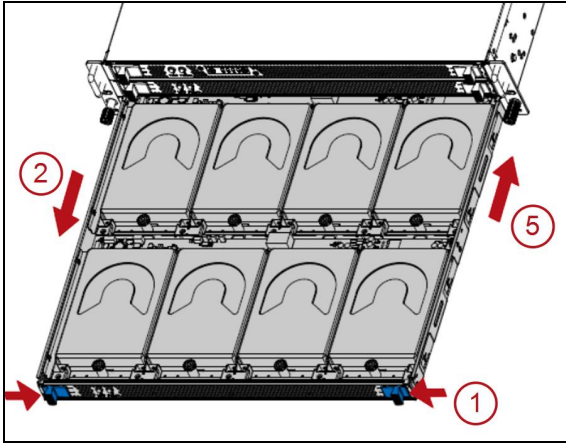
Figure 198 Remove the drive tray.
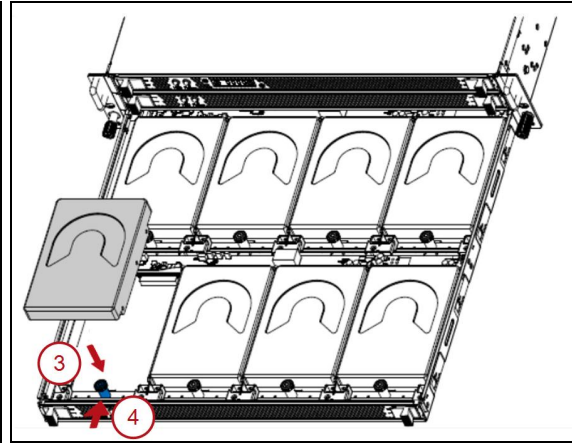
Figure 199 Install the drive.

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 4 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 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 200 Drive sled parts.
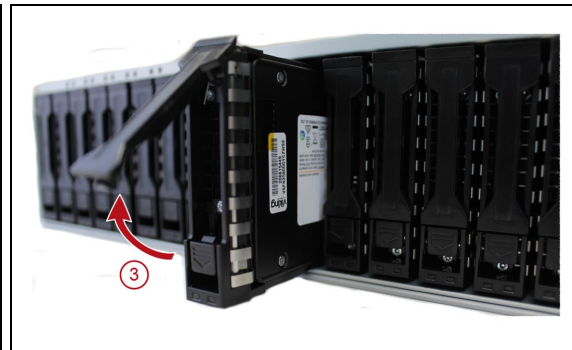
Figure 201 Remove the drive sled with drive blank and insert the drive sled with drive.

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 200 on page 250) 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 249 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 solution are mounted on drive sleds that ensure proper data and electrical connection with the backplane inside the BlackPearl NAS solution.

Remove the Front Bezel

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

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 solution includes an active bezel, do not install a drive in slot 1, which is the top left drive in the front of the solution. 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.
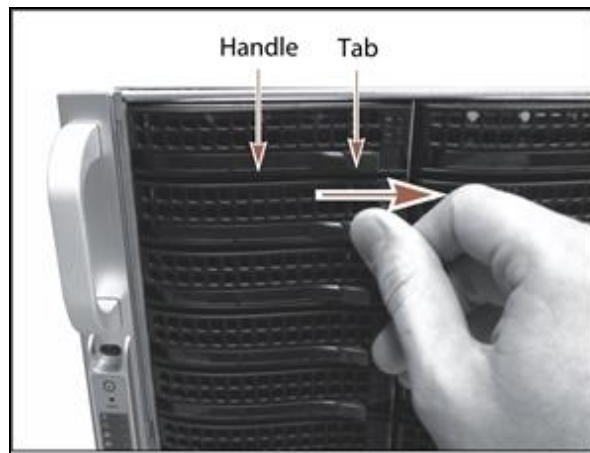
Figure 202 Slide the tab to the right to release the drive sled handle.

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.
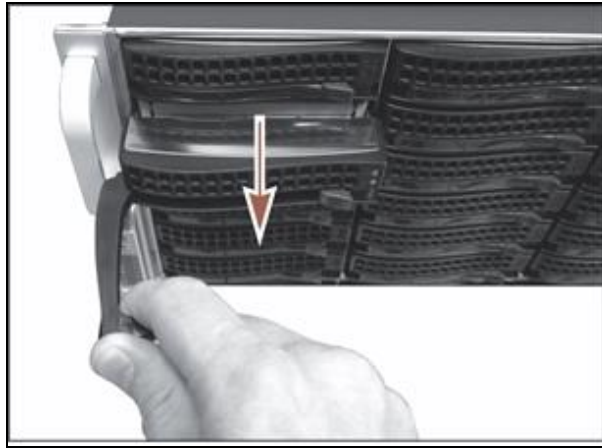
Figure 203 Pull the sled out of the solution.

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 204 Install the drive into the BlackPearl NAS solution.

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.

REPLACE A FAILED COMPONENT

If a component in a BlackPearl NAS solution is not functioning properly, the solution generates a message and the hardware icon on the status bar of the BlackPearl user interface changes to an error icon (see Status Icons on page 64).

Identify the Failed Component

1. From the menu bar, select **Status > Hardware**. The Hardware screen displays. The malfunctioning component is indicated by an error icon.
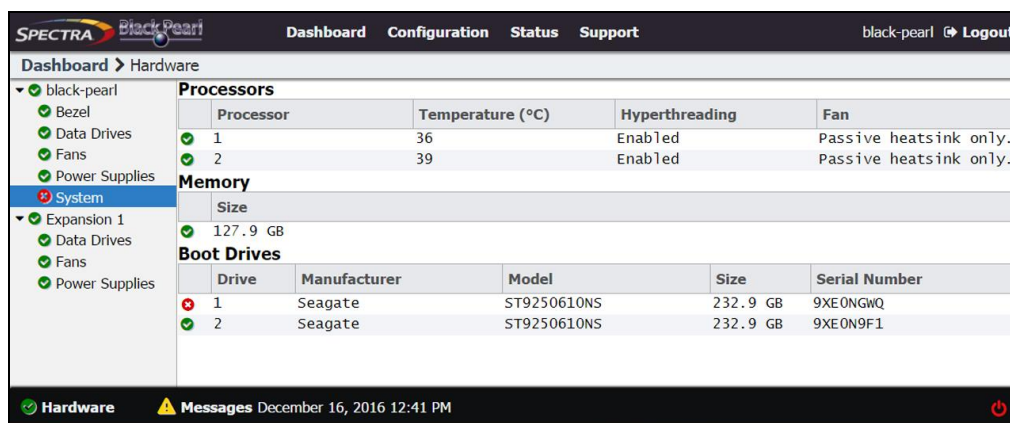
Figure 205 The Hardware screen showing a failed component.

2. If you have multiple BlackPearl NAS solutions, you can use the beacon feature to help locate the solution with the failed component. On the Hardware screen, click the server name. The screen refreshes to show the main Hardware screen.
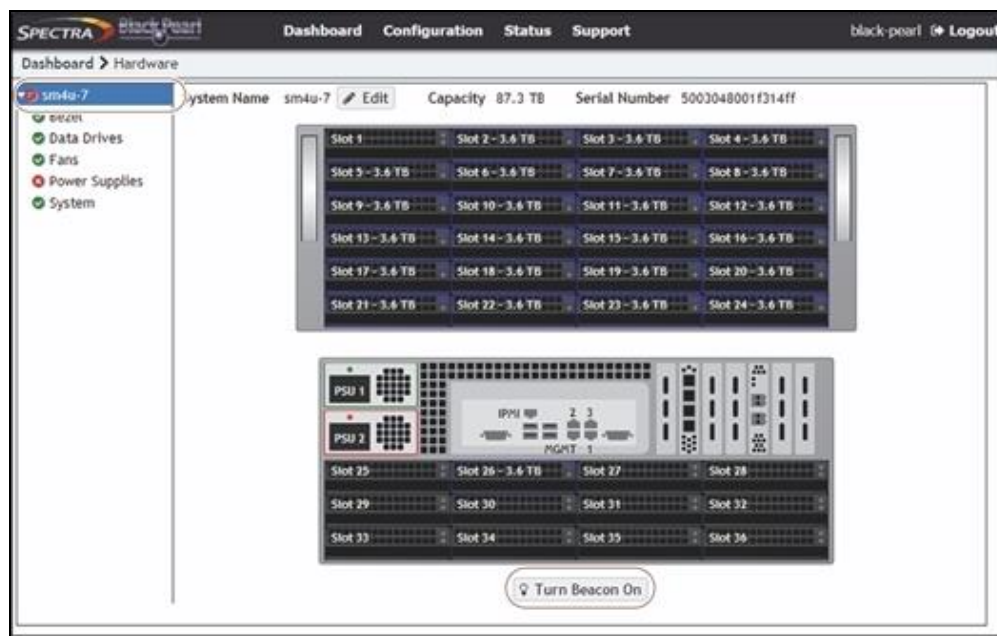
Figure 206 The Hardware screen.

3. Click **Turn Beacon On**. The BlackPearl NAS solution 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.

5. For specific part replacement procedures, refer to one of the following guides, which can be found after logging into the Spectra Logic support portal at *support.spectralogic.com*.

- The *Spectra 12- & 36-Drive Chassis HBA Installation Guide* provides instructions for installing an HBA in a Gen1 master node.

- The *Spectra 12- & 36-Drive Chassis Boot Drive Replacement Guide* provides instructions for replacing a failed boot drive in a Gen1 master node.

- The *Spectra 12-, 36- & 45-Drive Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive in a Gen1 master node or 44-bay expansion node.

- The *Spectra 12-, 36- & 45-Drive Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in a Gen1 master node or 44-bay expansion node.

- The *Spectra 12-, 36- & 45-Drive Chassis Power Supply Replacement Guide* provides instructions for replacing a failed power supply in a Gen1 master node or 44-bay expansion node.

- The *Spectra 12-Drive Chassis HBA Replacement Guide* and *Spectra 36-Drive Chassis HBA Replacement Guide* provide instructions for replacing a failed HBA in a Gen1 master node.

- 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.

CHAPTER 9 - USING AUTOSUPPORT

This chapter describes using the BlackPearl user interface to configure the support features of the Spectra BlackPearl NAS Solution.

ABOUT AUTOSUPPORT

AutoSupport lets the BlackPearl NAS solution 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 solution to email ASL sets when critical events occur, or on a monthly basis. You can also choose to have mail recipients receive ASL sets.

ENTER CONTACT INFORMATION

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

1. From the menu bar, select **Support > Contact Information** to display the Contact Information screen.

2. Click **New** in the Customer Contact Information pane. The New Contact Information dialog box displays.
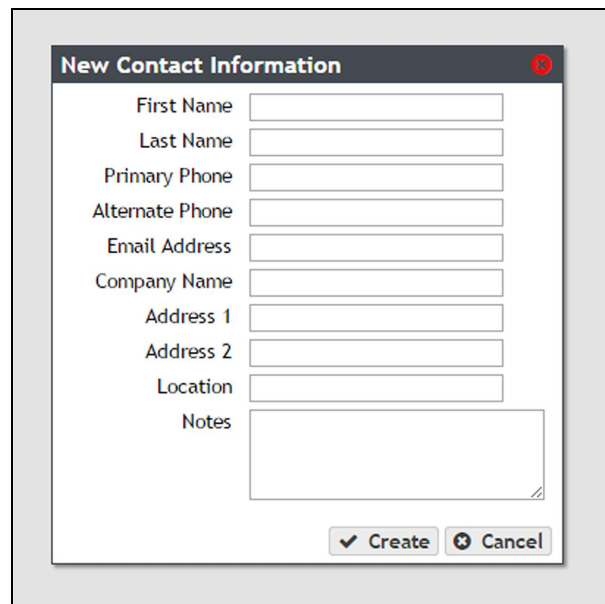
Figure 207 The New Contact Information dialog box.

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

CONFIGURE MAIL RECIPIENTS

You can configure AutoSupport to email system messages and log sets, as they are generated, to selected recipients. All log sets and messages are sent to a previously configured mail recipient. You cannot send log sets or messages directly to an email address. Use the Mail Recipient screen to add, edit, or delete mail recipient accounts.
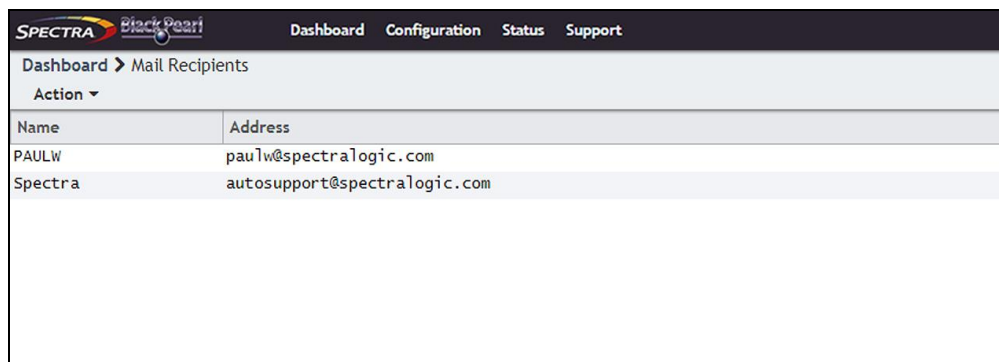
Figure 208   The Mail Recipients screen.

Create a New Mail Recipient

1. From the menu bar, select **Configuration > Mail Recipients**. The Mail Recipients screen displays.

2. Select **Action > New**. The New Mail Recipient dialog box displays.
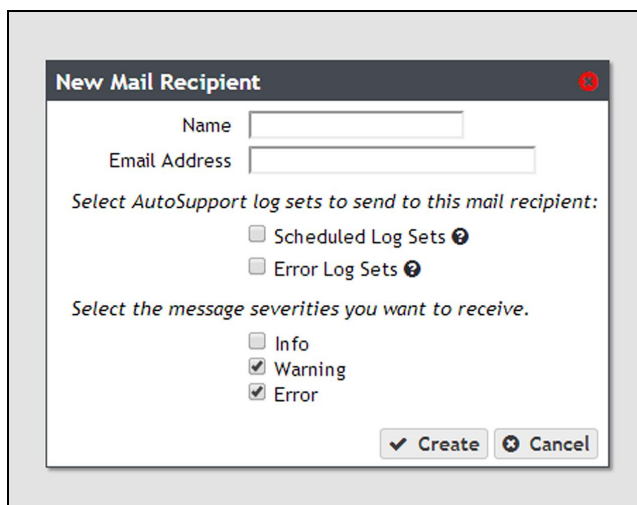
Figure 209   The New Mail Recipient dialog box.

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 solution on the first of each month. Error log sets are sent anytime an error occurs that causes the solution 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 solution 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 solution, select all boxes.
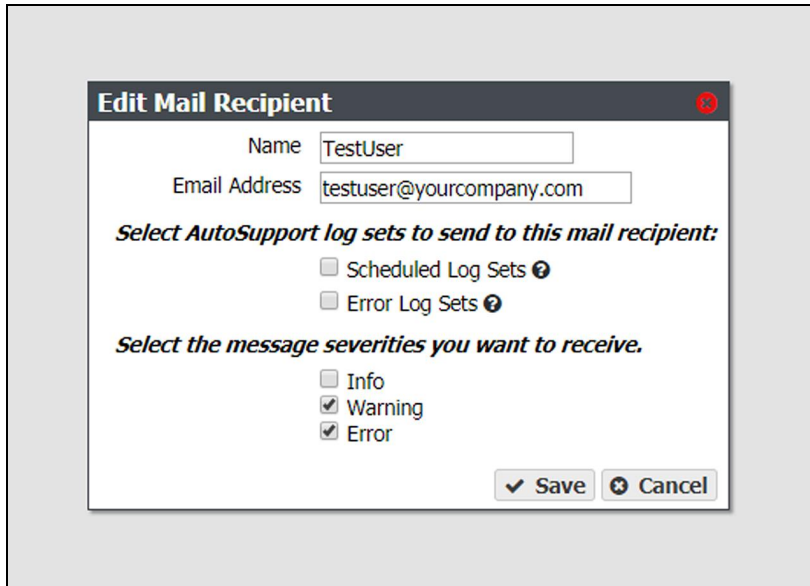
4. Click **Create** to save the information. The Mail Recipients screen re-displays with the new mail recipient added to the list of mail recipients.

5. Repeat through Step 4 to configure additional mail recipients.

Edit a Mail Recipient

Use the following steps to edit a mail recipient account.

1. From the menu bar, select **Configuration > Mail Recipients**. The Mail Recipients screen displays with any already configured mail recipients listed (see).

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

Figure 210 Edit the information for the selected mail recipient.

3. Change the information for the recipient as required and then click **Save**. See Step 3 on page 259 for a description of each setting.

Send a Test Email

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

1. From the menu bar, select **Configuration > Mail Recipients**. The Mail Recipients screen displays with any already configured mail recipients listed (see Figure 208 on page 258).

2. From the list of mail recipients, select the name of the recipient you want to receive a test email, and then select **Action > Send test email**.
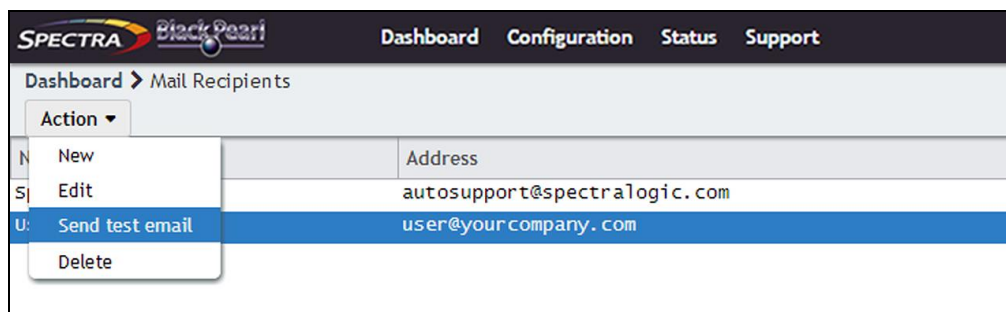
Figure 211 The Mail Recipients screen.

The BlackPearl NAS solution immediately sends a test email to the selected account.

3. Verify the user received the email from the BlackPearl NAS solution. If the email is not received, verify that you entered the SMTP server settings correctly (see Configure SMTP Settings on page 122).

Delete a Mail Recipient

Use the following steps to delete a mail recipient account.

1. From the menu bar, select **Configuration > Mail Recipients** to display the Mail Recipients screen with any already configured mail recipients listed (see Figure 208 on page 258).

2. From the list of mail recipients, select the name of the recipient whose account you want to delete and then select **Action > Delete**. A dialog box displays asking you to confirm the deletion of the mail recipient.

   Note: The default **Spectra** mail recipient cannot be deleted.
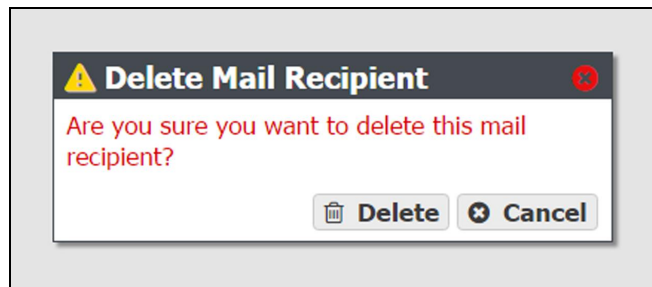
Figure 212 Delete the selected mail recipient.
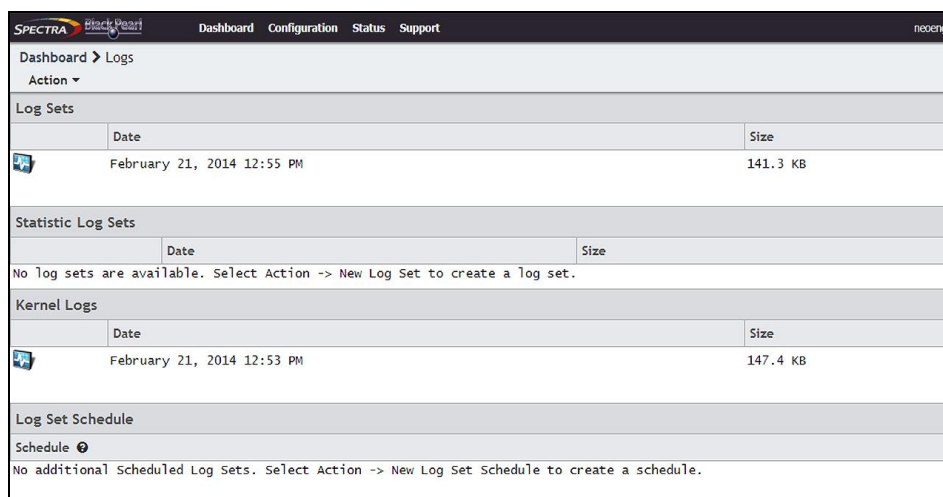
3. Click **Delete** to confirm the deletion.

LOG SETS

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

- **Log Sets** contain information about the configuration and status of the BlackPearl NAS solution and are used for general troubleshooting. Log sets can be mailed to configured mail recipients or to Spectra Logic Technical Support.

- **Statistic Log Sets** contain performance data about the solution and are used by Spectra Logic Technical Support for in-depth troubleshooting. Statistic log sets are too large to be mailed directly from the solution and must be downloaded.

- **Kernel Log Sets** are generated whenever a process on the solution 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 213 The Logs screen.

Configure a Log Set Schedule

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

1. From the menu bar, select **Support > Logs.** The Logs screen displays (see).

2. Select **Action > New Log Set Schedule**. The New Log Set Schedule dialog box displays.
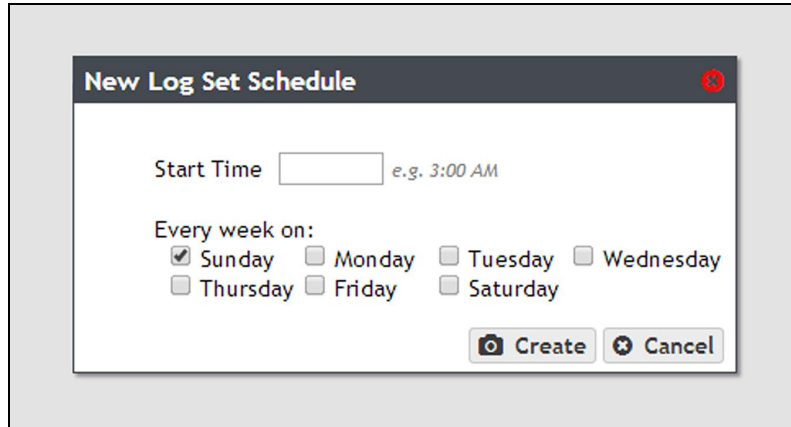
Figure 214 The New Log Set Schedule dialog box.

3. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.

4. Select one or more days for **Every week on:**. This determines the day(s) of the week the solution generates log sets.

5. Click **Create**. The Logs screen displays showing the newly created Log Set Schedule.

Manually Generate Log Sets

Although the BlackPearl NAS solution 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. From the menu bar, select **Support > Logs**. The Logs screen displays.

2. Create the desired log set:

- Select **Action > New Log Set** to generate a log set for use in general troubleshooting.

  —OR—

- Select **Action > New Statistic Log Set** to generate a log set used for in-depth troubleshooting. This log is not human readable. To see performance statistics in a human readable form, see View Performance Metrics on page 214.

Email a Log Set

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

Note: You must configure the SMTP settings on the solution before you can send emails. See Configure SMTP Settings on page 122 to configure the SMTP settings.

1. From the menu bar, select **Support > Logs.** The Logs screen displays (see on page 262).

2. Select the log set you want to email, and then select **Action > Email**. The Email Log Set dialog box displays.

Note: Statistic Log Sets are too large to be emailed from the solution, and must be downloaded. See Download a Log Set, below.
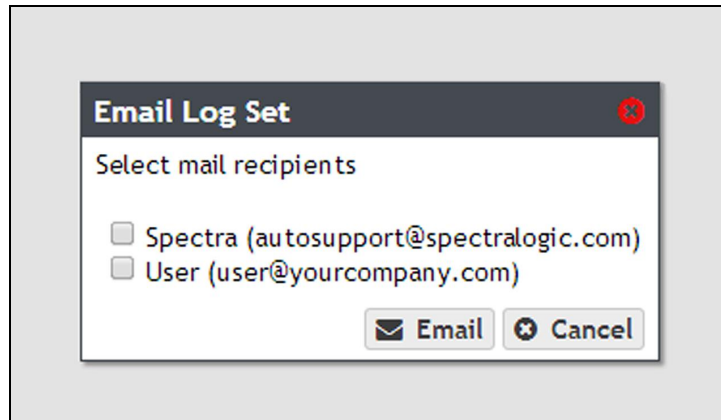
Figure 215 The Email Log Set dialog box.

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

Download a Log Set

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

1. From the menu bar, select **Support > Logs.** The Logs screen displays (see on page 262).

2. Select the log set you want to download, and then select **Action > Download**. The log set begins downloading to your host computer.

Delete Log Sets

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

1. From the menu bar, select **Support > Logs**. The Logs screen displays (see on page 262).

2. Select the log set you want to delete, and then select **Action > Delete**. A confirmation window displays asking you to confirm the action.

3. Click **Delete** to remove the log set.

4. Optionally, use one of the following to delete multiple log sets:

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

CHAPTER 10 - TROUBLESHOOTING AND SUPPORT

Use the information in this appendix to troubleshoot problems on the Spectra BlackPearl NAS Solution as they arise, before contacting Spectra Logic Technical Support.

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 solution as described in Log Into the BlackPearl User Interface on page 76. 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 solution 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 73.

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 solution. See Rear Panel on page 44 to locate the management port.

3. Open a web browser on the computer. For a list of compatible browsers, see Supported Browsers on page 65.

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 solution does not have a security certificate.

   Notes: • Consult your browser documentation for instructions on how to resolve the security certificate warning.

   • The absence of the certificate does not affect functionality.

6. Enter the login username and password.

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

Note: If you are running BlackPearl OS 4.0 through 5.3, the default username is **Administrator** and the default password is **spectra**. Starting with BlackPearl OS 5.4, the default password is the Serial Number (SN) printed on the front-right corner on the top of the chassis.

7. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays.

8. In the Network Interfaces pane, double-click the Management row, or select the Management row and then select **Action > Edit**. The Edit Management dialog box displays.
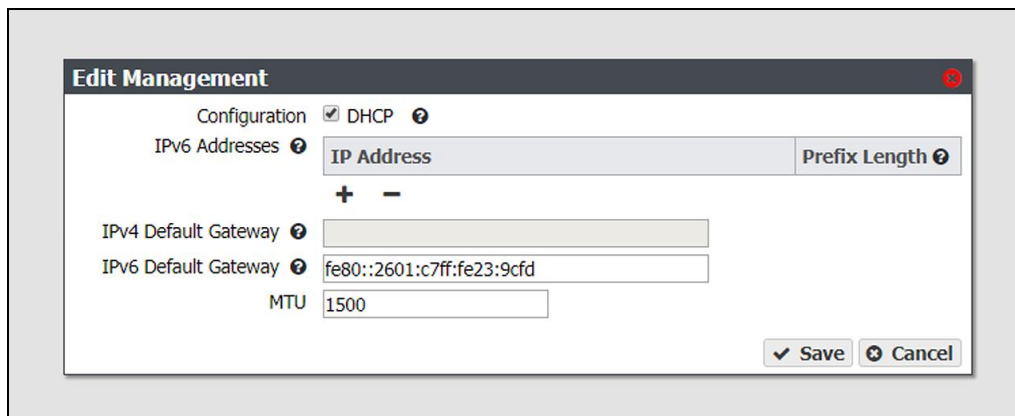
Figure 216 The Edit Management dialog box.

9. Select **DHCP** to configure the solution 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.

10. To configure a static IP address, click the **+** button and enter the following information:

- **IP Address**—Enter a valid IPv4 or IPv6 address.

Note: You cannot enter an IPv4 address if you selected DHCP in Step 9.

- **Prefix Length**—Enter the subnet mask.

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

11. Enter the **IPv4 Default Gateway**.

Note: If you selected DHCP in Step 9 on page 268, this option is unavailable.

12. Enter the **IPv6 Default Gateway**.

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

14. Click **Save**.

Note: When you change the IP address of the 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.

15. Disconnect the Ethernet cable from the BlackPearl management port.

16. Connect a cable from your network to the management port on the BlackPearl NAS solution. You are now able to connect to the solution with the IP address configured.

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 solution, use the information in this section to attempt to resolve the problem.

System Messages

If you are encountering problems, review any System Messages that were posted (see Check System Messages on page 207) 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 Solution Serial Number

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

1. From the menu bar, select **Support > Contact Information**. The Contact Information screen displays.

2. The solution serial number is listed in the Product Information pane.
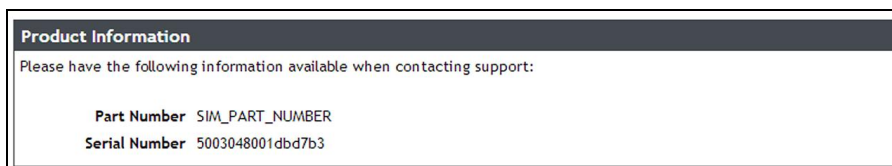
Figure 217 The solution serial number.

OPENING A SUPPORT TICKET

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

Search for Help Online
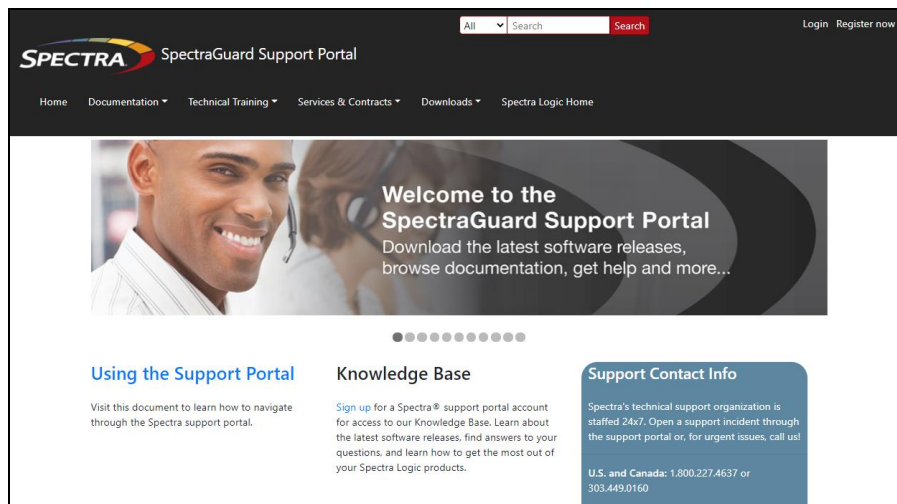
Figure 218 The Spectra Logic Technical Support portal home page.

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 Library Serial Number)

    • 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 Spectra Logic Technical Support on the previous page if you have not previously created an account on the Technical Support portal.

4. From any page, select **Incident>Incidents & Inventory**.
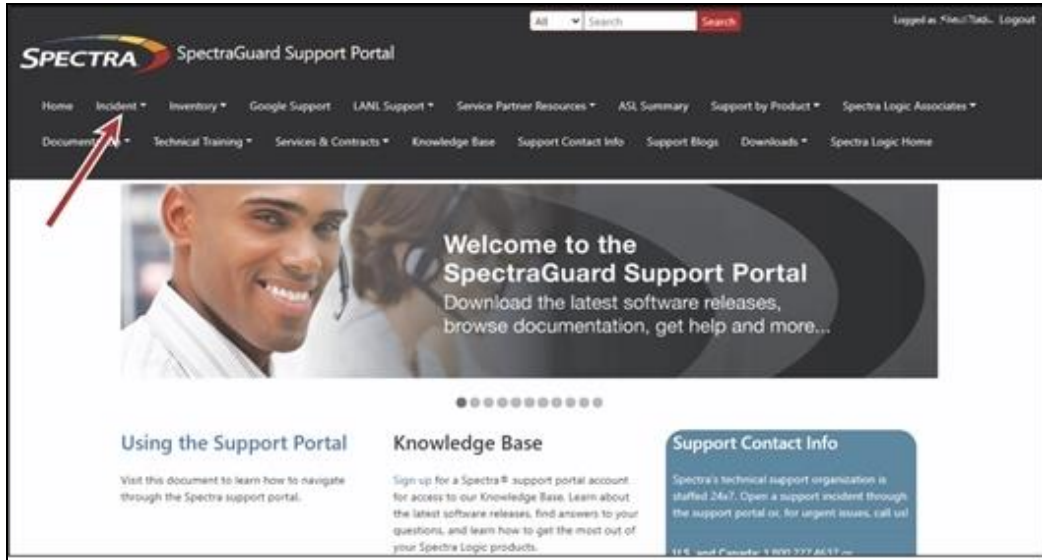
Figure 219 Select **Incidents>Incidents & Inventory**.

5. Select **Open or View Incidents**.
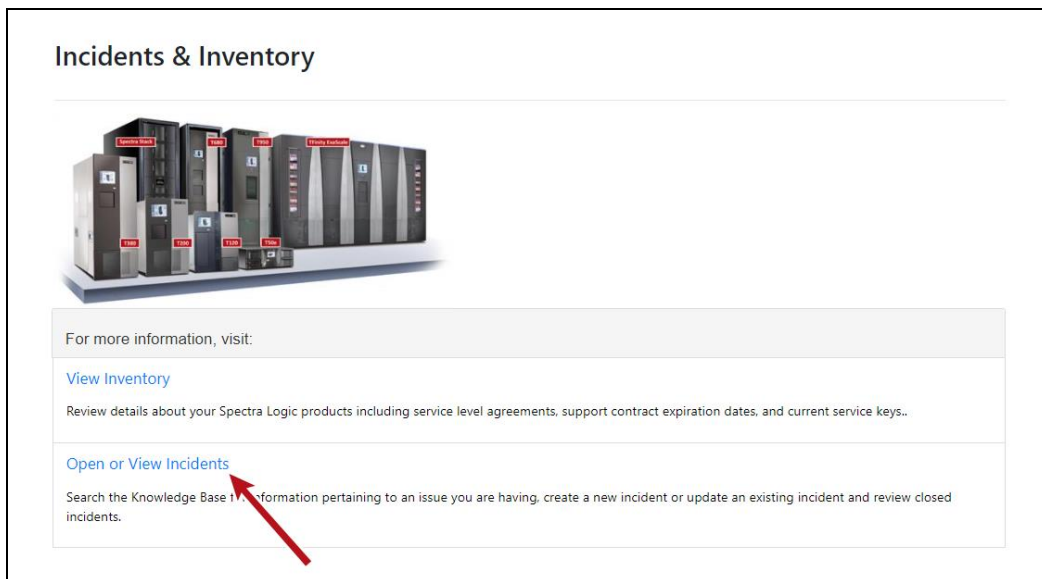
Figure 220 Select **Open or View Incidents**.

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

Figure 221 Enter a search phrase and click **Search**.

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

Figure 222 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**.

Figure 223 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 Library Serial Number)

- 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 Spectra Logic Technical Support on page 270 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**.
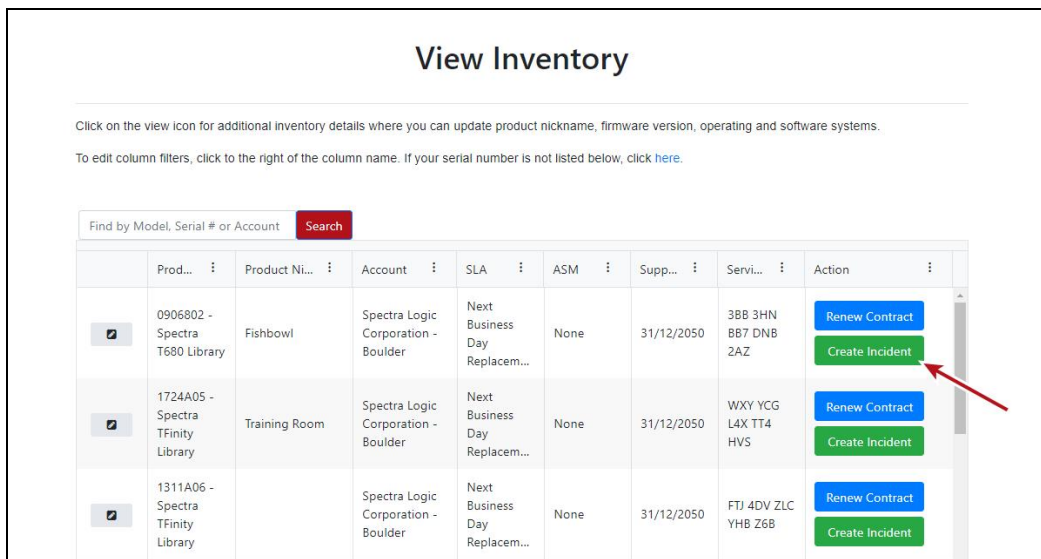
Figure 224 Click **Create Incident**.

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

Figure 225 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 **Email:** spectralogic@stortrec.de
Mexico, Central and South America, Asia, Australia, and New Zealand **Phone:** 1.303.449.0160	

REMOTE SUPPORT

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

Enabling Remote Support

1. Enter the Remote Support activation key as described in Configure Network Connections and Settings on page 115.

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

2. From the menu bar, select **Configuration > Users**. The Users screen displays a list of all configured users.

3. Double-click the **Administrator** account, or select the **Administrator** account, and then select **Action > Edit**. The Edit User dialog box displays.

Figure 226 The Edit User dialog box.

4. Select the **Enable Remote Support** check box.

Note: The Enable Remote Support check box does not display until you enter a Remote Support activation key. See Configure Network Connections and Settings on page 115 for more information.

5. Click **Save**.

⚠️ IMPORTANT   After Spectra Logic Technical Support informs you that they no longer require root access to the solution, you should disable Remote Support to prevent any potential unauthorized access. See Disabling Remote Support for more information.

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. From the menu bar, select **Configuration > Users**. The Users screen displays a list of all users configured on the solution.

2. Double-click the **Administrator** account, or select the **Administrator** account, and then select **Action > Edit**. The Edit User dialog box displays.

Figure 227 The Edit User dialog box.

3. Clear the **Enable Remote Support** check box.

4. Click **Save**.

Appendix A - IPMI Configuration

This appendix provides instructions for configuring IPMI for the BlackPearl NAS solution using the solution 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 solution performance.

1. If the BlackPearl NAS solution is currently powered on, shut down the solution as described in Reboot or Shut Down a BlackPearl NAS Solution on page 218.

2. Connect a monitor and USB keyboard to the rear of the BlackPearl NAS solution. See Rear Panel on page 44 to locate the monitor and USB connectors.

3. Power on the solution as described in Power On the Solution on page 71.

4. When prompted by the solution, press **DEL** to enter the solution BIOS.

   Note: The solution only displays this prompt for a few seconds. If you do not press **DEL** in time to enter the BIOS, let the solution complete it's boot process, then reboot the solution and repeat Step 4.

5. If necessary, log into the IPMI interface. The username is **admin**. 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. The fields are case sensitive.
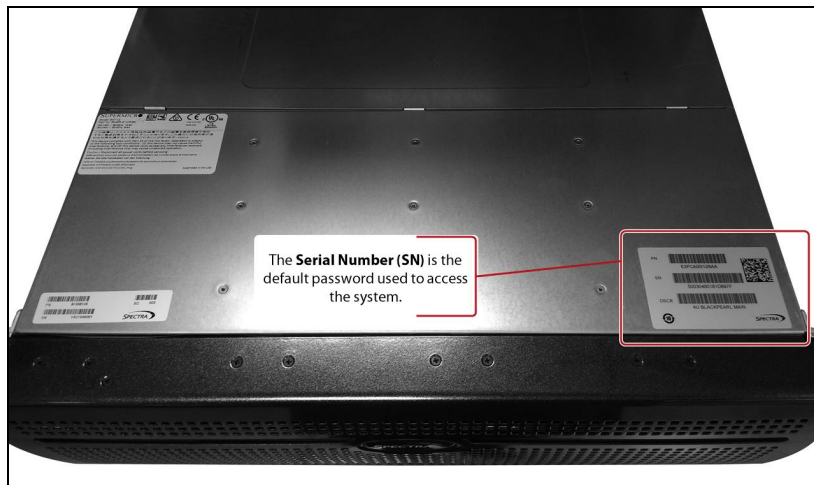
Figure 228 The BlackPearl serial number sticker.

6. Using the keyboard, navigate to the **IPMI** tab and then select **BMC Network Configuration**. The current settings of the BMC configuration display.
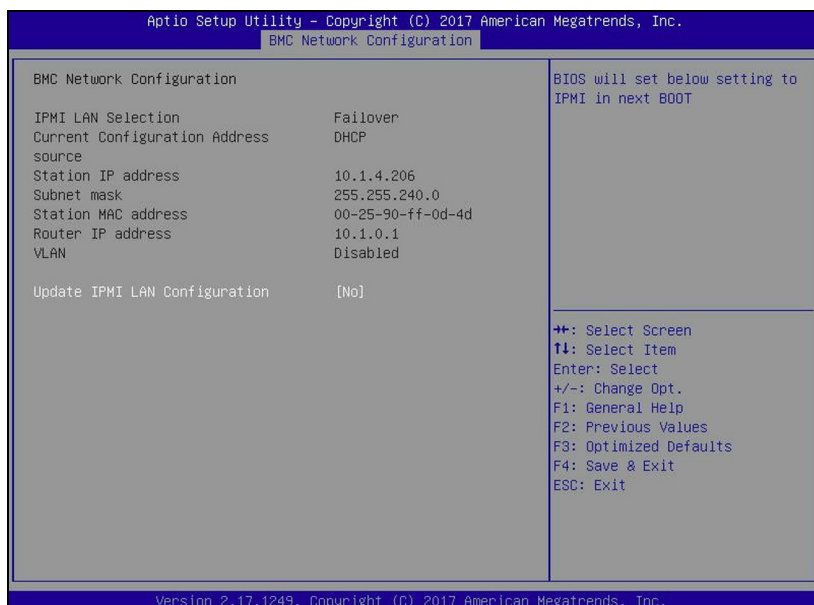
Figure 229 The BMC Configuration screen.

7. Using the keyboard, select **Update IPMI LAN Configuration**. A confirmation window displays. Select **YES** to continue. The current IPMI settings display.
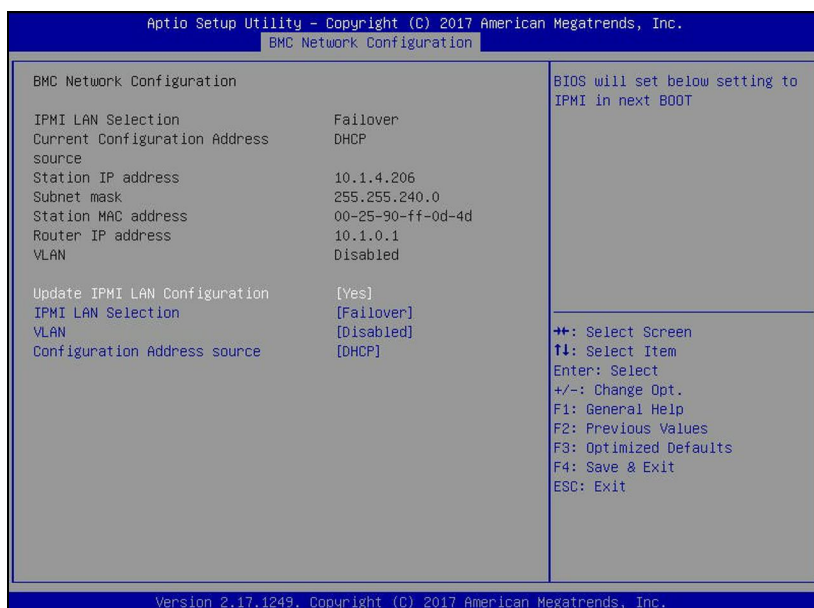
Figure 230 Current IPMI settings.

8. 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 solution startup, detect if the dedicated IPMI port is connected. If not, the solution uses the LAN1 port for IPMI traffic.

9. If desired, select **VLAN** to enable or disable VLAN as needed.

10. To change the IPMI address settings, select **Configuration Address source**. The current address source information displays.

11. Select **Static** or **DHCP** addressing.

- If you select **DHCP**, skip to .

- If you select **Static**, IP addressing fields display.
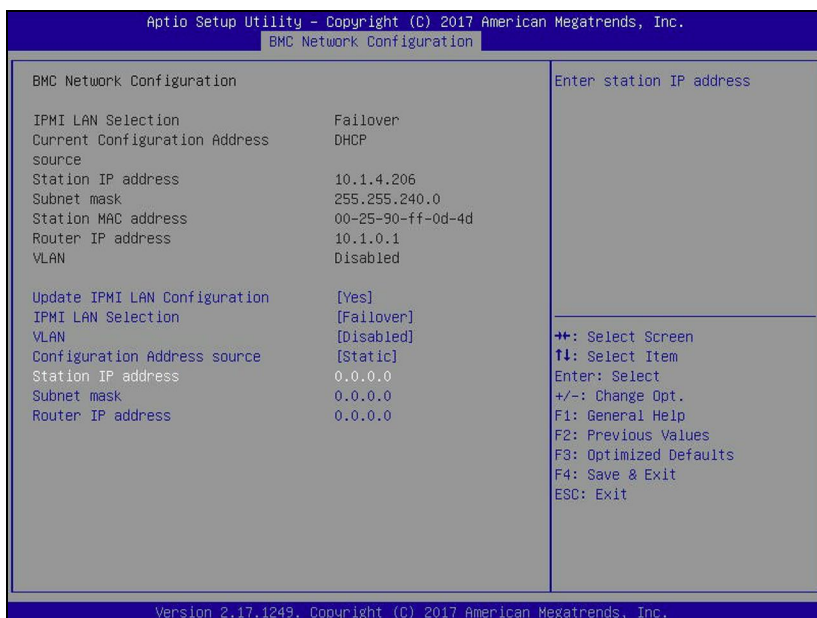
Figure 231 Enter Static IP information.

12. Configure the **Station IP address**, **Subnet mask**, and **Router IP address** with the desired address values.

   Note: Only IPv4 addresses are valid.

13. Press **F4** to exit the BIOS and save the entered settings. The BlackPearl NAS solution reboots.

APPENDIX B - NETWORK FILE INTERFACE

283

OVERVIEW

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

When a user needs access to data deleted from the BlackPearl NAS solution, they can use the Spectra Eon Browser or an API client to retrieve the files from the BlackPearl gateway.

REQUIREMENTS

The Network File Interface service has the following requirements:

- Files being stored as objects to a BlackPearl Nearline gateway must follow the Amazon S3 naming restrictions. See *http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html* for more information.

- If the target BlackPearl gateway is running software version 3.0 or later, then the gateway has Advanced Bucket Management (ABM) capabilities. When using an ABM-enabled system with NFI, you must first configure buckets on the BlackPearl gateway, and configure data policies for the user using NFI to transfer data to the gateway. See the *Spectra BlackPearl Nearline Gateway User Guide* for instructions on creating buckets and configuring data policies.

- If you plan to modify files on the BlackPearl NAS share configured for NFI replication, you must configure the target BlackPearl gateway as described in Configure a BlackPearl Gateway for Versioning on the next page.

- If the target BlackPearl gateway is configured to transfer data to tape, make sure the tape library does not contain WORM (Write Once-Read Many) media. The BlackPearl gateway is not compatible with WORM media.

CONFIGURE A BLACKPEARL GATEWAY FOR VERSIONING

If you plan to modify files on the BlackPearl NAS share that is configured for NFI replication, you must configure the target BlackPearl gateway with a storage domain and data policy that allow versioning as described in this section. If you do not plan to modify files on the BlackPearl NAS share, skip to Configure Network File Interface on page 289.

Once you create the required storage domain and data policy, you can then either:

- Create a bucket using the required data policy and specify that bucket when configuring the NFI service.

- Create a user and specify the required data policy as the default data policy. Then when the NFI service creates a bucket specifying that user as the owner, the bucket is created using the required data policy.

Use the instructions below to create a storage domain and data policy that allow versioning.

1. If you have not done so already, follow the instructions in the "Initial Configuration" chapter of the *Spectra BlackPearl Nearline Gateway User Guide*.

   Note: You may find it helpful to read the information in the "Understanding Spectra Advanced Bucket Management Concepts" chapter of the *Spectra BlackPearl Nearline Gateway User Guide*.

2. Log into the BlackPearl user interface as described in the *Spectra BlackPearl Nearline Gateway User Guide*.

3. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management**. The Advanced Bucket Management screen displays.

4. If necessary, configure disk and tape partitions on the system as described in the *Spectra BlackPearl Nearline Gateway User Guide*.

5. Select **Action > New Storage Domain**. The New Storage Domain dialog box displays.

   a. Configure the storage domain as desired. See the *Spectra BlackPearl Nearline Gateway User Guide* for instructions.

   b. For the **LTFS File Naming** option, you must select **Object ID**.

   c. After you finish configuring the storage domain, click **Create**.

6. Select **Action > New Data Policy**. The New Data Policy dialog box displays.

   a. Configure the data policy as desired. See the *Spectra BlackPearl Nearline Gateway User Guide* for instructions.

   b. For the **Versioning** option, you must select **Keep Latest**.

   c. After you finish configuring the data policy, click **Create**.

7. Add a data persistence rule.

a. Double-click the data policy in the Data Policies pane, or select the data policy and select **Action > Show Details** from the menu bar.

b. Select **Action > New Data Persistence Rule**. The New Data Persistence Rule dialog box displays.

c. Use the **Storage Domain** drop-down menu to select the storage domain you created in Step 5, above.

d. Configure the data persistence rule as desired. See the *Spectra BlackPearl Nearline Gateway User Guide* for instructions.

e. Click **Create**. The new data persistence rule displays on the Data Policy details screen.

8. Once you create the data policy, you must either create bucket(s) using that data policy, or create a new user with the data policy you created selected as the default for that user. Choose the corresponding instructions below:

- Create a Bucket Using the Required Data Policy below

  -OR-

- Create a User Using the Required Data Policy on the next page

Create a Bucket Using the Required Data Policy

Use the instructions in this section to create bucket(s) on the BlackPearl gateway that allow versioning.

1. In the BlackPearl user interface, select **Configuration > Buckets**. The Buckets screen displays.

2. From the menu bar, select **Action > New Bucket**. The New Bucket dialog box displays.

    a. Configure the bucket as desired. See the *Spectra BlackPearl Nearline Gateway User Guide* for instructions.

    b. Using the **Data Policy** drop down menu, select the data policy you created in Step 6 on page 286.

3. Click **Create**. The bucket is now listed on the Buckets screen.

Notes:
- You must enter the name of the bucket you just created when configuring a volume to use NFI replication.

- You need to create a bucket for each volume you plan to configure for NFI replication.

4. Continue to Configure Network File Interface below.

Create a User Using the Required Data Policy

Use the instructions in this section to create a user on the BlackPearl gateway with a default data policy that allows versioning.

1. In the BlackPearl user interface, select **Configuration > Users**. The Users screen displays.

2. From the menu bar, select **Action > New**. The New User dialog box displays.

    a. Configure the user as desired. See the *Spectra BlackPearl Nearline Gateway User Guide* for instructions.

    b. Using the **Default Data Policy** drop down menu, select the data policy you created in Step 6 on page 286.

3. Click **Create**. The new user displays on the Users Screen.

   Note: You must enter the name and S3 credentials for this user when configuring the NFI service so that buckets created for this user use the specified default data policy.

4. Continue to Configure Network File Interface below.

CONFIGURE NETWORK FILE INTERFACE

After configuring the BlackPearl gateway for versioning as described in Configure a BlackPearl Gateway for Versioning on page 286, use the instructions in the following sections to configure the BlackPearl NAS solution to use the Network File Interface service.

Configure the NFI Service

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

2. Double-click the NFI service, or select the service, and then select **Action > Show Details**. The details screen for the NFI service displays.
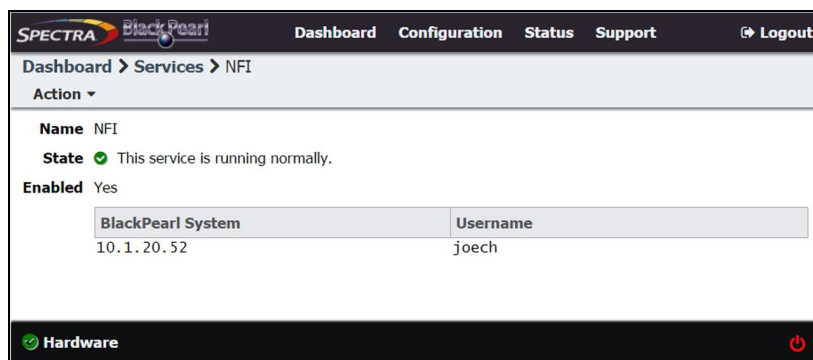
Figure 232 The NFI service details screen.

3. Select **Action > Configure**. The Configure dialog box displays.
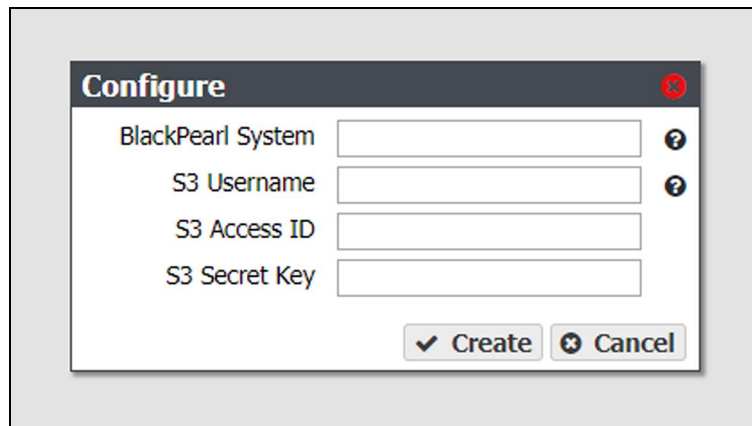
Figure 233 The Configure dialog box.

4. Enter the IP address or the DNS name of the data port of the target BlackPearl gateway to which you want to connect in the **BlackPearl System** entry field. If you do not know the IP address or DNS name of the BlackPearl gateway, consult the *Spectra BlackPearl Nearline Gateway User Guide* for instructions.

Note: If your BlackPearl NAS solution is running BlackPearl OS version 3.5.3, or later, all BlackPearl NFI targets must use BlackPearl OS 3.3.0, or later.

5. Enter a value for the **S3 Username**. The S3 Username helps you identify the user credentials provided for the BlackPearl gateway.

6. Enter the S3 security credentials of a user previously created on the BlackPearl gateway in the **S3 Access ID** and **S3 Secret Key** fields. If you have not created a user in the BlackPearl user interface, or do not know the security credentials for that user, consult the *Spectra BlackPearl Nearline Gateway User Guide* for instructions.

Notes:
- If you plan to modify files on the BlackPearl NAS shares and you created a data policy and assigned it to a user as described in Configure a BlackPearl Gateway for Versioning on page 286, you must enter the username and S3 credentials for that user so that buckets created by the NFI service use the correct data policy.

- If you plan to modify files on the BlackPearl NAS shares and you previously created buckets with the data policy created in Configure a BlackPearl Gateway for Versioning on page 286, you can choose any S3 user to enter here.

- If you do not plan to modify files on the BlackPearl NAS shares, you can choose any S3 user with access to the buckets to enter here.

7. Click **Create**.

8. If desired, repeat Step 3 on page 289 through Step 7 to configure additional target BlackPearl gateways or additional S3 security credentials.

Configure a Volume with NFI

Once the NFI service is configured to communicate with your target BlackPearl gateway, configure a volume to copy data to the BlackPearl gateway.

Note: Before you can create a volume, you must first create a storage pool. See Create a NAS Storage Pool on page 89, if necessary.

IMPORTANT — The combined length of the names of both the storage pool and volume used for NFI cannot exceed 52 bytes, or the NFI job fails. Most English characters are 1 byte.

---

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

Name	Status	Pool	Used	Available	Minimum Size	Maximum Size	Shared Via	NFI	Replication	Compression	Read Only	Case Insensitive	Replicated
volume1	Normal	pool1					CIFS	Disabled	Disabled	Disabled	Disabled	Disabled	No
volume2	Normal	pool1			500.0 GiB	4.9 TiB		Disabled	Disabled	Disabled	Disabled	Disabled	No
volume3	Normal	pool2						Disabled	Disabled	Enabled	Disabled	Disabled	No

Double click on a row to see more detailed information

Figure 234 The Volumes screen.

2. Double-click the volume you want to edit, or select the volume and then select **Action >
   Edit**. The Edit *volume name* dialog box displays

   —OR—

   Select **Action > New**. The New Volume dialog box displays.

Figure 235 The New Volume dialog box.

3. Configure the volume as required for your environment.

For this option....	Do the following...
Name	Enter a name for the new volume. Volume names are limited to 62 characters or fewer. **Notes:** • The combined storage pool and volume name must be 78 characters or fewer. • NFS does not allow spaces in share names. As a result, any spaces in the volume name are replaced by underscores in the corresponding NFS share name. The 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.
Pool	Select the storage pool on which to create the volume. If there are multiple storage pools configured on the solution, use the drop-down menu to select the **Pool** where you want to create the volume.
Minimum Size	Select the desired unit size from the drop-down menu and enter a numerical value for the minimum size in the text box to the left of the unit size drop-down menu. This space is allocated immediately if there is sufficient space available on the storage pool. If there is insufficient space available, volume creation fails. **Note:** Leave the **Minimum Size** and **Maximum Size** blank to create the volume with access to all available space on the storage pool.
Maximum Size	Select the desired unit size from the drop-down menu and enter a numerical value for the maximum size in the text box to the left of the unit size drop-down menu. **Notes:** • Volumes are thin provisioned, so it is possible for the combined allocated maximum storage of all volumes to exceed the physical space available. • Leave the **Minimum Size** and **Maximum Size** blank to create the volume with access to all available space on the storage pool.
Case Insensitive (CIFS)	If desired, select this option to configure the volume to treat all names as case insensitive, which can improve performance, especially in situations where directories contain a large number of files. **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.

For this option....	Do the following...
	⚠️ **CAUTION** **DO NOT** enable this setting if you plan to share the volume using NFS.
Compressi on	If desired, select the check box to enable the BlackPearl NAS solution to compress stored data. If the data being written is compressible there is an increase in write performance to the volume, which is dependent on how much compression occurs on the data being written. The data compression process uses CPU cycles to perform the compression. If compression is enabled and non-compressible data is written to the volume, the compression process may use an excessive number of CPU cycles, slowing the overall performance of the solution.
Access Time	If desired, select the check box to configure the solution to update the time stamp of a file when it is read from the volume. Selecting **Access Time** may slow performance.

4. Select the **Enabled** check box to enable the **NFI Volume Policy**.

5. Select either **Copy and Keep**, or **Copy and Delete**.

This option....	Does the following...
Copy and Keep	New or changed data in the volume is copied to the BlackPearl managed object storage and retained in the NAS volume.
Copy and Delete	Data in the volume is copied to the BlackPearl managed object storage and then deleted from the NAS volume.

6. Using the drop-down menu, select a **BlackPearl System** configured in .

7. Enter the name of the **Bucket** to use to store the data on the BlackPearl gateway. If the bucket does not exist, it is automatically created.

Notes:
- The bucket name cannot contain a colon (:), forward slash (/), or space.

- The bucket name cannot exceed 255 characters.

- If you plan to modify files in the NAS volume, the target BlackPearl gateway must use credentials for a user with a default data policy that uses versioning, or you must enter the name of the bucket with a data policy that uses versioning. See Configure a BlackPearl Gateway for Versioning on page 286.

- If the bucket data policy includes a replication rule for an Amazon S3 or Microsoft Azure target, the bucket name must also conform to the naming conventions of that cloud provider.

⚠	**IMPORTANT**	BlackPearl bucket names are case sensitive, but for some cloud targets, bucket names must be all lower case. The BlackPearl software changes bucket names with upper case letters to all lower case letters when needed. If you are using bucket names that only differ by case, the buckets are combined on the cloud target. For example, the BlackPearl buckets 'Index' and 'index' both map to the cloud bucket 'index', causing possible data collision and bucket ownership/permission problems.

8. Configure the **NFI Volume Policy Schedule**:

The NFI Volume Policy Schedule transfers data from the BlackPearl NAS solution to a BlackPearl gateway at intervals based on number of hours, days, or days of the week. Decide which interval to use for the schedule and follow the appropriate instructions.

- Create an Hourly Schedule on the next page —Transfer data every selected number of hours.
- Create a Daily Schedule on page 296—Transfer data every selected number of days.
- Create a Weekly Schedule on page 297—Transfer data on certain days of the week.

Create an Hourly Schedule

1. In the New Volume dialog box, select **Hourly** as the interval for the policy schedule. The dialog box changes to display options for the hourly interval setting

Figure 236 The New Volume dialog box showing the hourly interval options.

2. Enter numbers for **Every _ hours on minute** _. These values specify the interval in hours between data transfers 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, the NAS volume transfers data to the target BlackPearl gateway every four hours at 15 minutes after the hour. The maximum setting for the **hours** field is 48, where the NAS volume transfers data every two days. The maximum setting for the **minute** field is 59.

Note: Spectra Logic recommends offsetting the minutes after the hour for starting NFI transfers so that there are not a large number of jobs starting at exactly the same time.

3. Click **Create**.

4. Continue to .

Create a Daily Schedule

1. In the New Volume dialog box, select **Daily** as the interval for the policy schedule. The dialog box changes to display options for the daily interval setting.

Figure 237 The New Volume dialog box showing the daily interval options.

2. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.

3. Enter a number for **Every _ days**This value specifies the interval, in days, between data transfers to the BlackPearl gateway. The value entered is enumerated from the first day of the month. The schedule resets at the beginning of each month. For example, if this value is set to 2, the NAS volume transfers data every two days, starting with the 1st of the month, at the time specified in Step 2. A value of 30 runs on the 1st of the month, and then again on the 31st of the month (for months that have 31 days). To schedule data transfers on the first of every month, set the interval to 31 days.

4. Click **Create**.

5. Continue to Create a Share on the next page.

Create a Weekly Schedule

1. In the New Volume dialog box, select **Weekly** as the interval for the policy schedule. The dialog box changes to display options for the weekly interval setting.

Figure 238 The New Volume dialog box showing the weekly interval options.

2. Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.

3. Select one or more days for **Every week on:**. This determines the day(s) of each week the NAS volume copies data to the BlackPearl gateway.

4. Click **Create**.

5. Continue to Create a Share.

Create a Share

After creating a volume and configuring the NFI Volume Policy Schedule, you must create a share for the volume. See Create a Share on page 97. Once you create a share for the volume, you can begin file storage operations.

MANAGE NFI REPLICATION

Edit the NFI Service

If desired, you can change the configuration of the previously configured NFI service.

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

2. Double-click the NFI service, or select the service, and then select
Action > Show Details. The details screen for the NFI service displays.
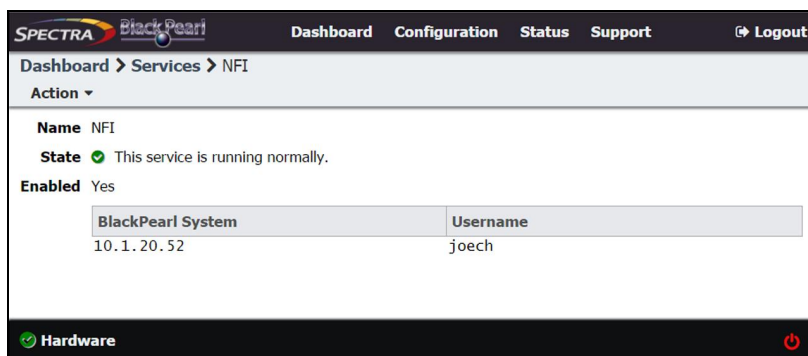
Figure 239 The NFI service details screen.

3. Select **Action > Edit**. The Edit NFI dialog box displays.

4. Edit the settings as described in Configure the NFI Service on page 289.

5. Click **Save**.

Delete the NFI Service Configuration

If desired, you can delete (clear) the NFI service configuration.

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

2. Double-click the NFI service, or select the service, and then select
Action > Show Details. The details screen for the NFI service displays.
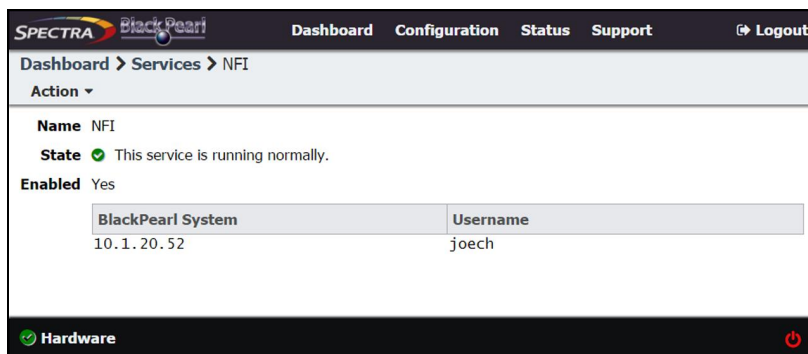
Figure 240 The NFI service details screen.

3. Select **Action > Delete**. A confirmation window displays.

4. Confirm the deletion of the NFI service configuration.

Manually Starting an NFI Replication

If desired, you can manually initiate an NFI replication to the target gateway.

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 41 on page 93).

2. Double-click the volume for which you want to manually start an NFI replication, or select the volume, and then select **Action > Show Details**. The details screen for that volume displays.

3. Select **Action > Initiate NFI Transfer**.

4. Click **Initiate NFI Transfer** to begin the replication.

Reinitialize NFI Replication

If desired, you can elect to reinitialize an NFI replication, which transfers all the files in the volume to the BlackPearl target during the next NFI replication.

1. From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 41 on page 93).

2. Double-click the volume for which you want to manually start an NFI replication, or select the volume, and then select **Action > Show Details**. The details screen for that volume displays.

3. Select **Action > Reinitialize NFI Transfer**. A confirmation window displays.
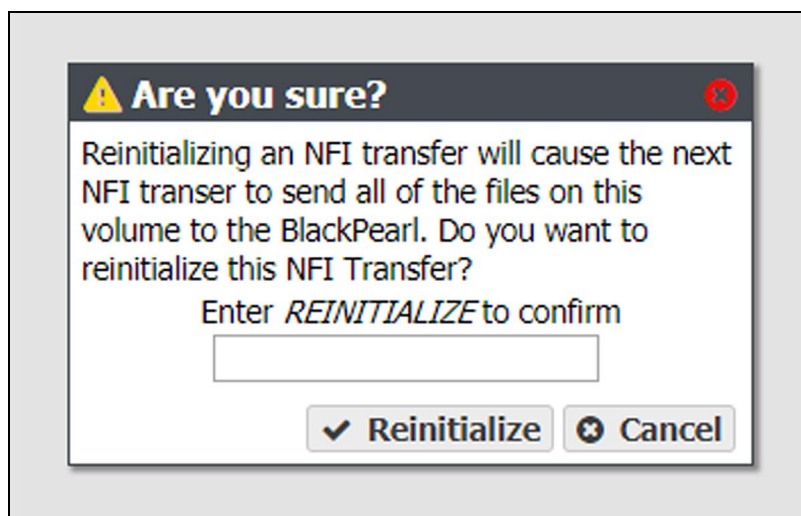
Figure 241 The Reinitialize NFI Transfer confirmation window.

4. Type `REINITIALIZE` in the entry field and click **Reinitialize** to reinitialize the NFI transfer.

Edit the NFI Volume Policy

Use the instructions in to change how data is copied from the NAS volume to a BlackPearl gateway.

RESTORING FILES FROM AN NFI TARGET BLACKPEARL GATEWAY

If files copied to the BlackPearl gateway using the NFI service are deleted from the BlackPearl NAS solution, or the BlackPearl NAS solution fails, you can retrieve files from the BlackPearl gateway using the Spectra Eon Browser, Spectra Deep Storage Browser, or a DS3 client. If you only need to retrieve a small number of files, Spectra Logic recommends using the Eon Browser.

Restore Files Using the Eon Browser

For instructions for installing, configuring, and using the Eon Browser, see the *BlackPearl Eon Browser User Guide*.

Restore Files Using a DS3 Client

Consult the documentation for your DS3 client to restore files from an NFI target BlackPearl gateway.

APPENDIX C - SPECIFICATIONS

This appendix provides detailed specifications for the BlackPearl NAS solution 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

The following tables show the data storage specifications for the BlackPearl NAS solutions.

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 Solution

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 Solution

Drive Purpose	Drive Type
NAS	960, 1600, or 1920 GB Solid-State SAS

BlackPearl Gen1 V Series 2U Solution

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 NAS solutions.

Gen3 F Series BlackPearl Solution

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 BlackPearl Solution

Parameter	Specifications
CPU	One 64-bit 8 core CPU
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 solution 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 solution management.

[d] Each SAS card is used to connect the BlackPearl master node to disk expansion nodes.

Gen2 X Series BlackPearl Solution

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 Solution

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 solution 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 solution management.

Gen2 S Series BlackPearl Solution

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 Solution

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 solution management.

b) Each SAS card is used to connect the BlackPearl master node to disk expansion nodes.

Gen1 S Series BlackPearl 4U Solution

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 solution 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 Solution

Parameter	Gen3 F Series BlackPearl NAS Solution	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 Series BlackPearl NAS Solution

Parameter	Gen3 H Series BlackPearl NAS Solution	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 SAS drive	75 lb (34 kg) 1.5 lb (0.67 kg)	114 lb (51.8 kg)

[a] Includes chassis, drives, box, and packaging.

[b] Includes chassis, drives, box, and packaging.

[c] Includes the front bezel.

Gen2 X Series BlackPearl NAS Solution

Parameter	Gen2 X Series BlackPearl NAS Solution	Shipping Container [a]
Dimensions • Height (2U) • Width • Depth	3.5 in. (8.9 cm) 19 in. (48.3 cm) 29 in. (73.7 cm) [b]	
Maximum Weight Including rail kit [c]	60 lb (27.2 kg)	

Gen2 V Series BlackPearl NAS Solution

Parameter	Gen2 V Series BlackPearl NAS Solution	Shipping Container [a]
Dimensions • Height (2U) • Width • Depth	3.5 in. (8.9 cm) 19 in. (48.3 cm) 33 in. (83.8 cm) [b]	11.5 in. (29.2 cm) 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)	

[a] Includes chassis, drives, box, and packaging.

[b] Includes the front bezel.

[c] Weights are approximate.

Gen2 S Series BlackPearl NAS Solution

Parameter	Gen2 S Series BlackPearl NAS Solution	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 Solution

Parameter	Gen1 V Series 2U BlackPearl NAS Solution	Shipping Container [a]
Dimensions • Height (2U) • Width • Depth	3.5 in. (8.9 cm) 19 in. (48.3 cm) 27.5 in. (69.9 cm) [b]	13.25 in. (33.7 cm) 26 in. (66.0 cm) 34.25 in. (87.0 cm)

Weight [c]
• Empty chassis
• Empty chassis with:
  • 4 HDDs & 2 SSDs
  • 9 HDDs & 2 SSDs
	37.2 lb (16.9 kg)
	
	46.7 lb (21.2 kg)
	55.7 lb (25.3 kg)
		N/A
		
		67.7 lb (30.7 kg)
		76.7 lb (34.8 kg)

---

[a] Includes chassis, drives, box, and packaging.

[b] Includes the front bezel.

[c] Weights are approximate.

Gen1 S Series 4U BlackPearl NAS Solution and 44-Bay Expansion Node

Parameter	Gen1 S Series 4U BlackPearl NAS Solution and 44-Bay Expansion Node	Shipping Container [a]
Dimensions • Height (4U) • Width • Depth	7 in. (17.8 cm) 19 in. (48.3 cm) 29.5 in. (74.9 cm) [b]	17.5 in. (44.5 cm) 27 in. (68.6 cm) 39 in. (99.0 cm)
Weight [c] • Empty chassis • Additional for each HDD • Additional for each SSD	57 lb (25.8 kg) 1.8 lb (0.8 kg) 0.8 lb (0.4 kg)	91.3 lb (41.4 kg) 1.8 lb (0.8 kg) 0.8 lb (0.4 kg)

77-Bay Expansion Node

Parameter	77-bay Expansion Node	Shipping Container
Dimensions • Height (4U) • Width • Depth	7 in. (17.8 cm) 19 in. (48.3 cm) 32 in. (81 cm) [b] 38.5 in. (97.8 cm) [d]	21.1 in. (53.6 cm) 26.6 in. (67.6 cm) 44.1 in. (112 cm)
Weight [e] • Empty chassis • Additional for each HDD • Additional for each SSD • Additional for 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)

[a] Includes chassis, drives, box, and packaging.

[b] Includes the front bezel.

[c] Weights are approximate.

[d] Includes optional cable management arm.

[e] Weights are approximate.

Parameter	77-bay Expansion Node	Shipping Container
• Fully loaded chassis with rack mounting kit		242 lb (110 kg) [a]

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) [b] 1.8 lb (0.8 kg) 21 lb (9.5 kg) 302 lb (137 kg)

a) Includes chassis and packaging.

b) 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 Solution

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 solution 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 solution or expansion node in its original packaging. The packaging protects the BlackPearl NAS solution 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 BlackPearl NAS Solution

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 Solution

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 solution 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 theBlackPearl NAS solution or expansion node in its original packaging. The packaging protects the BlackPearl NAS solution 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 Solution

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 Solution

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 solution 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 solution or expansion node in its original packaging. The packaging protects the BlackPearl NAS solution 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 solution 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 solution or expansion node in its original packaging. The packaging protects the BlackPearl NAS solution 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	
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 NAS solutions, 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 solution, result in data loss, or both.

Input Power Requirements

The following tables provide the input power requirements for each solution or expansion node.

Gen3 F Series BlackPearl NAS Solution

Parameter	Requirements
Input Voltage	100-120 VAC, 13 A,

Parameter	Requirements
	200–240 VAC, 10 A,
Input Frequency	50–60 Hz

Gen3 H Series BlackPearl NAS Solution

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 Solution

Parameter	Requirements
Input Voltage	200–240 VAC, 7 A, 1600 watts maximum
Input Frequency	50–60 Hz

Gen2 V Series BlackPearl NAS Solution

Parameter	Requirements
Input Voltage	100-240 VAC, 8-4 A, 800 watts maximum
Input Frequency	50–60 Hz

Gen2 S Series BlackPearl NAS Solution

Parameter	Requirements
Input Voltage	200–240 VAC, 10 A, 1600 watts maximum
Input Frequency	50–60 Hz

Gen1 V Series 2U BlackPearl NAS Solution

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 Solution

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 NAS solutions are part of the unit and are not intended for use with any other equipment.

| ⚠ | IMPORTANT | Confirm the PDU used with the BlackPearl NAS solution has enough amperage for the power supply in each chassis included in your installation. |

Cables provided by Spectra Logic are between 6 ft (1.8m) to 6.5 ft (2m) in length. If you need to use a longer cord, make sure it conforms to the specifications listed below.

Power cords must comply with local electrical codes.

| ⚠ | 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.
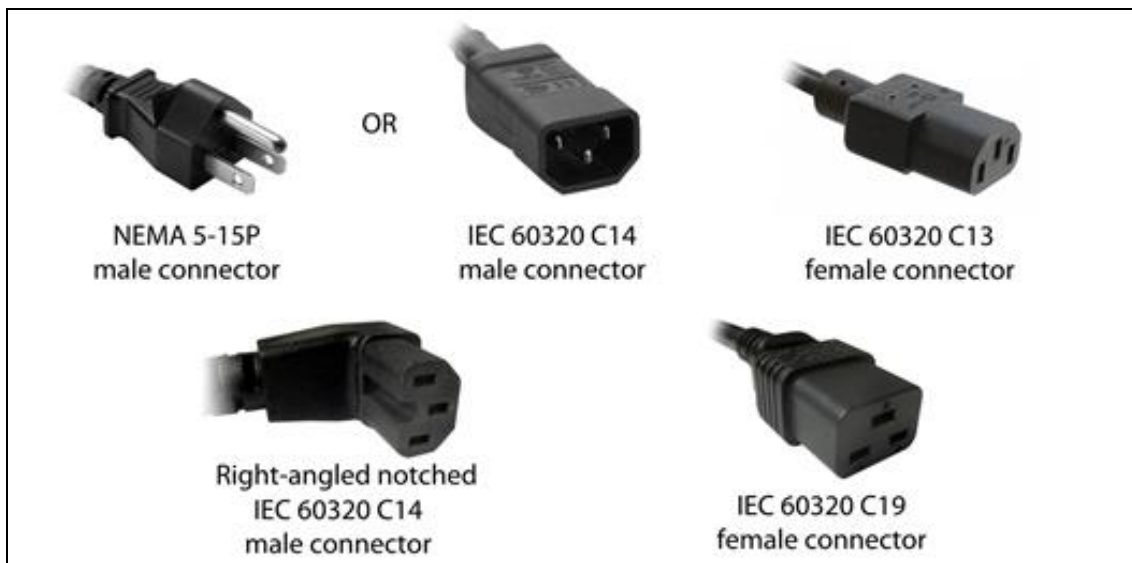
North American 120 Volt-AC Power Cord

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

INTERFACE SPECIFICATIONS

This section provides information about the interfaces used to connect a BlackPearl NAS solution to expansion nodes and host systems.

System Interface Connectors

Gen3 F Series BlackPearl NAS Solution

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 BlackPearl NAS Solution

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 Solution

Interface Type	Number of Ports and Connector Type
Ethernet	

Interface Type	Number of Ports and Connector Type
• 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 Solution

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 Solution

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 solution.
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 solution.
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 solution 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 solution 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 D - REGULATORY & SAFETY STANDARDS

The Spectra BlackPearl NAS Solution 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

CE

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

Mike Beaty
Sr. Director Operations
September 26, 2023

6101 Lookout Road   www.SpectraLogic.com
Boulder, CO 80301   +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 (CISPER 22) Class A	Limits and methods of measurements of radio interference characteristics of information technology equipment.
EN 55024	1998, Information Technology Equipment - Immunity Characteristics Limits and Methods of Measurement.
EN 61000-4-2	1995 + A1:1998+A2: 2001, Electrostatic Discharge
EN 61000-4-3	1995 + A1:1998 + A2:2001, ENV 50204: 1995, Radiated RF Immunity
EN 61000-4-4	1995 + A1:2001, Electrical Fast Transient/Burst
EN 61000-4-5	1995 + A1:2001 + A2:2001, Surge Immunity
EN 61000-4-6	1996 + A1:2001 + A2:2001, Conducted RF Immunity
EN 61000-4-8	1994 + A1:2001, Power Frequency H-field Immunity
EN 61000-4-11	1994 + A1:2001, Voltage Dips and Interrupts
EN 61000-3-2	2000, Power Line Harmonics
EN 61000-3-3	1995, Power Line Flicker
EC Low Voltage Directive 72/336/EEC	Essential health and safety requirements relating to electrical equipment designed for use with certain violate limits.
EN 60950-1 (EN 60950-1)	Safety requirements of information technology equipment including electrical machines.

Certifications

Country	Certification	Covers [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 system 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 solution 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.

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 solution 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.
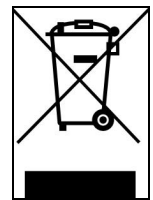
Within participating European Union countries, special collection, recycling, and disposal arrangement have been established for this product. At the end of life, the product user should dispose of this product using special WEEE collection systems. These special systems mitigate the potential affects 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 solution, check the Spectra Logic website at: *spectralogic.com/environment*.

APPENDIX E - OPEN SOURCE CODE ACKNOWLEDGMENTS & PACKAGE LIST

This appendix contains the licenses and notices for open source software used in the BlackPearl NAS solution. 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 © 1992-2024 The FreeBSD Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE FREEBSD PROJECT ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FREEBSD PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the FreeBSD Project.

JAVA

ORACLE AMERICA, INC. ("ORACLE"), FOR AND ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES UNDER COMMON CONTROL, IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY SELECTING THE "ACCEPT LICENSE AGREEMENT" (OR THE EQUIVALENT) BUTTON AND/OR BY USING THE SOFTWARE YOU ACKNOWLEDGE THAT YOU HAVE READ THE TERMS AND AGREE TO THEM. IF YOU ARE AGREEING TO THESE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE LEGAL AUTHORITY TO BIND THE LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO BE BOUND BY THE TERMS, THEN SELECT THE "DECLINE LICENSE AGREEMENT" (OR THE EQUIVALENT) BUTTON AND YOU MUST NOT USE THE SOFTWARE ON THIS SITE OR ANY OTHER MEDIA ON WHICH THE SOFTWARE IS CONTAINED.

1. DEFINITIONS. "Software" means the software identified above in binary form that you selected for download, install or use (in the version You selected for download, install or use) from Oracle or its authorized licensees, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Oracle, and any user manuals, programming guides and other documentation provided to you by Oracle under this Agreement. "General Purpose Desktop Computers and Servers" means computers, including desktop and laptop computers, or servers, used for general computing functions under end user control (such as but not specifically limited to email, general purpose Internet browsing, and office suite productivity tools). The use of Software in systems and solutions that provide dedicated functionality (other than as mentioned above) or designed for use in embedded or function-specific software applications, for example but not limited to: Software embedded in or bundled with industrial control systems, wireless mobile telephones, wireless handheld devices, kiosks, TV/STB, Blu-ray Disc devices, telematics and network control switching equipment, printers and storage management systems, and other related systems are excluded from this definition and not licensed under this Agreement. "Programs" means (a) Java technology applets and applications intended to run on the Java Platform, Standard Edition platform on Java-enabled General Purpose Desktop Computers and Servers; and (b) JavaFX technology applications intended to run on the JavaFX Runtime on JavaFX-enabled General Purpose Desktop Computers and Servers. "Commercial Features" means those features identified in Table 1-1 (Commercial Features In Java SE Product Editions) of the Java SE documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html. "README File" means the README file for the Software accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

2. LICENSE TO USE. Subject to the terms and conditions of this Agreement including, but not limited to, the Java Technology Restrictions of the Supplemental License Terms, Oracle grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally the Software complete and unmodified for the sole purpose of running Programs. THE LICENSE SET FORTH IN THIS SECTION 2 DOES NOT EXTEND TO THE COMMERCIAL FEATURES. YOUR RIGHTS AND OBLIGATIONS RELATED TO THE COMMERCIAL FEATURES ARE AS SET FORTH IN THE SUPPLEMENTAL TERMS ALONG WITH ADDITIONAL LICENSES FOR DEVELOPERS AND PUBLISHERS.

3. RESTRICTIONS. Software is copyrighted. Title to Software and all associated intellectual property rights is retained by Oracle and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that the Software is developed for general use in a variety of information management applications; it is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use the Software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Oracle or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4. DISCLAIMER OF WARRANTY. THE SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ORACLE FURTHER DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

5. LIMITATION OF LIABILITY. IN NO EVENT SHALL ORACLE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF ORACLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ORACLE'S ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

6. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Oracle if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon termination, you must destroy all copies of Software.

7. EXPORT REGULATIONS. You agree that U.S. export control laws and other applicable export and import laws govern your use of the Software, including technical data; additional information can be found on Oracle's Global Trade Compliance web site (http://www.oracle.com/products/export). You agree that neither the Software nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

8. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Oracle that Oracle owns the ORACLE and JAVA trademarks and all ORACLE- and JAVA-related trademarks, service marks, logos and other brand designations ("Oracle Marks"), and you agree to comply with the Third Party Usage Guidelines for Oracle Trademarks currently located at

http://www.oracle.com/us/legal/third-party-trademarks/index.html. Any use you make of the Oracle Marks inures to Oracle's benefit.

9. U.S. GOVERNMENT LICENSE RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation shall be only those set forth in this Agreement.

10. GOVERNING LAW. This agreement is governed by the substantive and procedural laws of California. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, or Santa Clara counties in California in any dispute arising out of or relating to this agreement.

11. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

12. INTEGRATION. This Agreement is the entire agreement between you and Oracle relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

A. COMMERCIAL FEATURES. You may not use the Commercial Features for running Programs, Java applets or applications in your internal business operations or for any commercial or production purpose, or for any purpose other than as set forth in Sections B, C, D and E of these Supplemental Terms. If You want to use the Commercial Features for any purpose other than as permitted in this Agreement, You must obtain a separate license from Oracle.

B. SOFTWARE INTERNAL USE FOR DEVELOPMENT LICENSE GRANT. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File incorporated herein by reference, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

C. LICENSE TO DISTRIBUTE SOFTWARE. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File, including, but not limited to the Java Technology Restrictions and Limitations on Redistribution of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that: (a) is a complete, unmodified reproduction of this Agreement; or (b) protects Oracle's interests consistent with the terms contained in this Agreement and that includes the notice set forth in Section H, and (vi) you agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software. The license set forth in this Section C does not extend to the Software identified in Section G.

D. LICENSE TO DISTRIBUTE REDISTRIBUTABLES. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File, including but not limited to the Java Technology Restrictions and Limitations on Redistribution of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the README File ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified, and only bundled as part of Programs, (ii) the Programs add significant and primary functionality to the Redistributables, (iii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README File), (iv) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (v) you only distribute the Redistributables pursuant to a license agreement that: (a) is a complete, unmodified reproduction of this Agreement; or (b) protects Oracle's interests consistent with the terms contained in the Agreement and includes the notice set forth in Section H, (vi) you agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software. The license set forth in this Section D does not extend to the Software identified in Section G.

E. DISTRIBUTION BY PUBLISHERS. This section pertains to your distribution of the JavaTM SE Development Kit Software ("JDK") with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, Oracle hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the JDK on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the JDK on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the JDK from the applicable Oracle web site; (iii) You must refer to the JDK as JavaTM SE Development Kit; (iv) The JDK must be reproduced in its entirety and without any modification whatsoever (including with respect to all proprietary notices) and distributed with your Publication subject to a license agreement that is a complete, unmodified reproduction of this Agreement; (v) The Media label shall include the following information: "Copyright [YEAR], Oracle America, Inc. All rights reserved. Use is subject to license terms. ORACLE and JAVA trademarks and all ORACLE- and JAVA-related trademarks, service marks, logos and other brand designations are trademarks or registered trademarks of Oracle in the U.S. and other countries." [YEAR] is the year of Oracle's release of the Software; the year information can typically be found in the Software's "About" box or screen. This information must be placed on the Media label in such a manner as to only apply to the JDK; (vi) You must clearly identify the JDK as Oracle's product on the Media holder or Media label, and you may not state or imply that Oracle is responsible for any third-party software contained on the Media; (vii) You may not include any third party software on the Media which is intended to be a replacement or substitute for the JDK; (viii) You agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of the JDK and/or the Publication; ; and (ix) You shall provide Oracle with a written notice for each Publication; such notice shall include the following information: (1) title of Publication, (2) author(s), (3) date of Publication, and (4) ISBN or ISSN numbers. Such notice shall be sent to Oracle America, Inc., 500 Oracle Parkway, Redwood Shores, California 94065 U.S.A, Attention: General Counsel.

F. JAVA TECHNOLOGY RESTRICTIONS. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun", "oracle" or similar convention as specified by Oracle in any naming convention designation.

G. LIMITATIONS ON REDISTRIBUTION. You may not redistribute or otherwise transfer patches, bug fixes or updates made available by Oracle through Oracle Premier Support, including those made available under Oracle's Java SE Support program.

H. COMMERCIAL FEATURES NOTICE. For purpose of complying with Supplemental Term Section C.(v)(b) and D.(v)(b), your license agreement shall include the following notice, where the notice is displayed in a manner that anyone using the Software will see the notice:

Use of the Commercial Features for any commercial or production purpose requires a separate license from Oracle. "Commercial Features" means those features identified Table 1-1 (Commercial Features In Java SE Product Editions) of the Java SE documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html

I. SOURCE CODE. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

J. THIRD PARTY CODE. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME file accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME file, the disclaimer of warranty and limitation of liability provisions in paragraphs 4 and 5 of the Binary Code License Agreement shall apply to all Software in this distribution.

K. TERMINATION FOR INFRINGEMENT. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right.

L. INSTALLATION AND AUTO-UPDATE. The Software's installation and auto-update processes transmit a limited amount of data to Oracle (or its service provider) about those specific processes to help Oracle understand and optimize them. Oracle does not associate the data with personally identifiable information. You can find more information about the data Oracle collects as a result of your Software download at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

SAMBA

Samba is provided under the terms of the GNU General Public License (GPL version 3)

For more details and for the full text for each of these licenses, read the LICENSES and COPYING files included with the source packaging of this software.

On Debian GNU/Linux systems, the complete text of the GNU General Public License can be found in `/usr/share/common-licenses/GPL'.

NGINX

Copyright (C) 2002-2024 Igor Sysoev

Copyright (C) 2011-2024 Nginx, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RUBY

Ruby is copyrighted free software by Yukihiro Matsumoto <matz@netlab.jp>.

You can redistribute it and/or modify it under either the terms of the 2-clause BSDL (see the file BSDL), or the conditions below:

1. You may make and give away verbatim copies of the source form of the software without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may modify your copy of the software in any way, provided that you do at least ONE of the following:

   a. place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or by allowing the author to include your modifications in the software.

   b. use the modified software only within your corporation or organization.

   c. give non-standard binaries non-standard names, with instructions on where to get the original software distribution.

   d. make other distribution arrangements with the author.

3. You may distribute the software in object code or binary form, provided that you do at least ONE of the following:

   a. distribute the binaries and library files of the software, together with instructions (in the manual page or equivalent) on where to get the original distribution.

   b. accompany the distribution with the machine-readable source of the software.

   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

bash-5.1.16

black_pearl-3.0_4

bluestorm_backend-2.0.3020678_7

bluestorm_frontend-2.1.3022552

bluestorm_gui-2.0.3030423_6

bluestorm_mgmt-2.0.3030423

bluestorm_tests-2.0.2886232_1

bluestorm_workers-2.0.3039984_6

boost-libs-1.72.0_7

brotli-1.0.9,1

c-ares-1.18.1

ca_root_nss-3.77

cdbcmd-0.0.1774343,1

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

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-0.0.1.3020678

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

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

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

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

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-finspacedata-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-locationservice-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-marketplaceentitlementservice-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-qldb-1.25.0

rubygem-aws-sdk-qldbsession-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-sagemakeredgemanager-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-simpledb-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-3.0.0.2959489

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-0.1.0.2933665

rubygem-devstat_stat-0.0.1.3018334

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-1.0.7.3018334

rubygem-freebsd_mps-1.1.1.3018334

rubygem-freebsd_ses-1.3.2.3018334

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-1.0.1.2979196

rubygem-libifconfig-0.1.0.2959489_1

rubygem-libxml-ruby-3.2.2_1

rubygem-live_record-0.2.1.1686790

rubygem-liveresource-2.1.2.2910675

rubygem-loofah-2.16.0

rubygem-lsiexp-1.2.4.3033324

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-1.5.2.3014781

rubygem-passenger-nginx-6.0.12_2

rubygem-pg-1.3.5

rubygem-pkg-config-1.4.7

rubygem-pmbus-1.1.2.1718448

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-0.0.2.2714935

rubygem-snmp-1.2.0

rubygem-spectra_acl-1.2.1.2959489_2

rubygem-spectra_cli-1.0.2.3020677

rubygem-spectra_platform-1.3.1.3026227

rubygem-spectra_support-5.0.0.2983962

rubygem-spectra_view-2.3.0.3042319_10

rubygem-spectra_workers-5.0.0.3033306

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-0.1.3.3018334,1

rubygem-stringio-3.0.1

rubygem-sys-uname-1.2.2

rubygem-tape_backend-0.1.2882562

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-uglifier-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-0.0.12.3011237

samba413-4.13.17_5

sedutil-1.12.2996028

sg3_utils-1.45

smartmontools-7.3

smp_utils-0.99

source-highlight-3.1.9_1

spectra_ltfs-2.5.0.0.3020678

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

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-3.0.0_2

verde_hotpair-3.0.3041571

vim-8.2.4669

xorg-fonts-truetype-7.7_1

xorgproto-2021.5

yarn-1.22.18

zip-3.0_1

zsh-5.8.1

zstd-1.5.2

INDEX

A

B

C

O

P

R

S