

Spectra Logic BlackPearl Converged Storage System

User Guide



SpectraLogic.com

Copyright

Copyright © 2014-2021 Spectra Logic Corporation. All rights reserved. This item and the information contained herein are the property of Spectra Logic Corporation.

Notices

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

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

Trademarks

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

Part Number

90990093 Revision V

Revision History

Revision	Date	Description
N	September 2017	Updated for the BlackPearl 4.0 release.
Q	January 2018	Updated for the BlackPearl 4.1.1 release. Revisions O & P were never released.
R	July 2018	Updated for the BlackPearl 5.0 release.
S	May 2019	Updated for the BlackPearl 5.1 release.
T	February 2020	Updated for the BlackPearl 5.1.4 release.
U	November 2020	Updated for the BlackPearl 5.2 release.
V	August 2021	Updated for the BlackPearl 5.3 release.

Note:

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

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

End User License Agreement

1. READ CAREFULLY

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

2. OWNERSHIP

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

3. GENERAL

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

4. SOFTWARE PRODUCT

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

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

5. GRANT OF LICENSE AND RESTRICTIONS

- A. Spectra grants you a non-exclusive, non-transferable End-User license right to install the Software Poduct 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.

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.co	om	
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, Aust Phone: 1.303.449.0160	ralia, and New Zealand	
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.co	om/documentation	

Table of Contents

Table of Contents	9
About This Guide	25
Intended Audience	25
BlackPearl User Interface Screens	25
Related Information	26
Related Publications	26
Tape Library User Guides	28
Online Forum	28
Chapter 1 - Product Overview	29
Overview	30
Features	30
Components	33
Gen2 X Series	33
Gen1 S Series, Gen1 P Series, and Gen1 V Series	37
96-Bay Expansion Node	43
107-Bay Expansion Node	45
BlackPearl User Interface	47
Menus	48
Status Icons	51
Supported Browsers	52
Chapter 2 - Initial Configuration	53
Before You Begin	54
Considerations for BlackPearl NAS Systems	54
Connect Ethernet Cables	54
Power On the System	55

	Configure the BlackPearl Management Port	56
	Automatically Import Activation Keys	57
	Log Into the BlackPearl User Interface	58
	Install NAS Drives	60
	Configure the Data Connection	61
	Configure an Aggregate Port Data Connection	61
	Configure a Single Port Data Connection	64
	Configure a Static Route	65
	Create a User	67
	Description of User Types	67
	Create a User	68
	View S3 Credentials	70
	Next Steps	71
Cł	napter 3 - Understanding Spectra Advanced Bucket Management Concepts	72
	Goals of Advanced Bucket Management	73
	Spectra S3 Overview	73
	Spectra S3 Clients	75
	BlackPearl Cache	75
	Storage Domains	75
	Data Policies	75
	Data Persistence Rules	76
	Data Replication Rules	77
	Tape Eject Strategy	77
	Tape and Disk Partitions	77
	Tape Partitions	78
	Tape Drive Reservation	78
	Tape Media Inspections	79

Disk Partitions	79
Special Considerations for Ejecting Tapes	80
Special Considerations for Reading Tapes in a Non-BlackPearl Environment	80
Example Configurations	81
Single Copy on Tape	82
Dual Copy on Tape	86
Single Copy on Nearline Disk	91
Single Copy on Nearline Disk and Tape	95
Single Copy on Nearline Disk and Dual Copy on Tape	100
Chapter 4 - Configuring Advanced Bucket Management	106
Create a Storage Pool	107
Create a Nearline Disk Pool	107
Create an Online Disk Pool	111
Create a Disk Partition	113
Create a Tape Partition	114
Create a Replication Target	115
Create a BlackPearl Target	115
Create an Amazon S3 Target	118
Create a Microsoft Azure Target	122
Create a Storage Domain	124
Create an Hourly Schedule	128
Create a Daily Schedule	129
Create a Weekly Schedule	129
Add a Storage Domain Member to a Storage Domain	129
Create a Data Policy	131
New Data Policy ACL for a Group	135
New Data Policy ACL for a User	136

Add Data Persistence Rules and Replication Rules to a Data Policy	136
Create a Bucket	142
Create a New Bucket ACL for a Group	144
Create a New Bucket ACL for a User	145
Transfer Data	146
Chapter 5 - Managing Advanced Bucket Management Settings	148
Manage a Storage Domain	149
Edit a Storage Domain Member	149
Exclude a Storage Domain Member	150
Cancel Storage Domain Member Exclusion	151
Delete a Storage Domain Member	151
Edit a Storage Domain	152
Delete a Storage Domain	153
Manage Data Replication Rules	154
Edit a BlackPearl Data Replication Rule	154
Edit an Amazon S3 Data Replication Rule	155
Edit a Microsoft Azure Data Replication Rule	156
Delete a Data Replication Rule	157
Manage a Data Policy	158
Edit a Data Policy	158
Delete a Data Policy	159
Delete a Data Policy ACL	160
Edit a Data Persistence Rule	160
Delete a Data Persistence Rule	162
Manage Replication Targets	163
Edit a BlackPearl Replication Target	163
Edit an Amazon Replication Target	164

Edit an Azure Replication Target	165
Verify a Replication Target	165
Put a Replication Target in Standby State	166
Activate a Replication Target	167
Delete a Replication Target	168
Manage a Disk Partition	168
Edit a Disk Partition	169
Delete a Disk Partition	169
Manage Online and Nearline Disk Pools	170
Import a Nearline or Online Disk Pool	170
Delete a Nearline or Online Disk Pool	172
Manage Buckets	172
Show Bucket Physical Placement	173
Edit a Bucket ACL	173
Delete a Bucket ACL	174
Edit a Bucket	174
Delete a Bucket	175
Chapter 6 - Additional Configuration Options	177
Configure Network Connections and Settings	178
Configure Ethernet Ports	179
Configure DNS Settings	185
Configure SMTP Settings	186
Configure Date and Time	187
Edit the System Name	188
Configure Networking Services	188
Configure the Spectra S3 Service	189
Configure the Active Directory Service	193

Configure the SNMP Service	197
Configure the Vail Service	199
Configure and Use Encryption	201
Configure the Encryption Service	201
Change the Encryption Password	202
Unlock the Self-Encrypting Drives	203
Create an Encryption Password USB Key	204
PSID Erase an Encryption Drive	205
Configure Users and S3 Groups	207
Description of User Types	207
Create a User	207
Edit a User	207
Change S3 Secret Key	210
Create an S3 Group	212
Remove an S3 Group Member	214
Edit an S3 Group	215
Delete a User or S3 Group	215
Configure Certificates	216
Manually Enter Activation Keys	217
Chapter 7 - Configuring Network Attached Storage	220
Overview of NAS Storage Pools, Volumes, and Shares	220
Storage Pools	221
Volumes and Shares	221
Naming Considerations	221
Create a NAS Storage Pool	221
Create a Volume	225
Create an Hourly Schedule	229

Create a Daily Schedule	230
Create a Weekly Schedule	231
Create a Share	232
Create a CIFS Share	232
Create an NFS Share	237
Configure NAS Services	238
Configure the CIFS Service	239
Configure the NFI Service	240
Configure the NFS Service	241
Configure the NAS Replication Service	242
Create an Hourly Schedule	246
Create a Daily Schedule	246
Create a Weekly Schedule	247
Chapter 8 - Managing Network Attached Storage	248
Managing Storage Pools	249
Edit a Storage Pool	249
Expand a Storage Pool	250
Delete a Storage Pool	251
Managing Volumes	252
Move a Volume	252
Cancel a Volume Move	252
Edit a Volume	253
Delete a Volume	255
Volume Snapshots	255
Create a Snapshot	256
Create a Snapshot Schedule	257
Delete a Snapshot Schedule	259

Delete Snapshots	260
Restore to a Snapshot	262
Retrieve a Single File from a Snapshot	263
Managing Shares	263
Edit a CIFS Share	264
Edit an NFS Share	264
Delete a Share	265
Managing NAS Replication	266
Manually Start NAS Replication	266
Cancel a NAS Replication In Progress	267
Restoring Files from a NAS Replication Target	268
Disable NAS Replication for a Volume	268
Edit the NAS Replication Service	269
Delete the NAS Replication Service Configuration	270
Managing NFI Replication	271
Edit the NFI Service	271
Delete the NFI Service Configuration	272
Manually Starting an NFI Replication	272
Reinitialize NFI Replication	272
Restoring Files From an NFI Target BlackPearl System	274
Chapter 9 - Working with Tape Libraries and Media	275
Tape Library Barcode Reporting	276
Format Tapes	276
Cancel Tape Format	278
Inspect Tapes	278
Eject Tapes	280
Edit Tape Eject Information	281

Eject a Single Tape	202
Cancel Tape Ejection	283
Eject Tapes from a T50e or T120 Library with Multiple Partitions	283
Import Tapes	284
Import Foreign Tapes	284
Imported Tape Object Name Restrictions for Amazon S3 Replication	on284
Import BlackPearl Foreign Tape(s)	285
Import LTFS Foreign Tape(s)	286
Compact a Tape Cartridge	288
Manage Tapes Not in Inventory	289
Mark Tape as Ejected	289
Delete Lost or Ejected Tape	29 0
Tape Library Options	290
Activate a Tape Library Partition	290
Put a Tape Library Partition into Standby	291
Delete a Tape Partition	292
Tape Drive Options	292
Tape Drive Reservation	293
Offline a Tape Drive	296
Online a Tape Drive	297
Remove a Tape Drive from a Tape Partition	299
Data Migration	300
Chapter 10 - Operating the BlackPearl System	301
S3 Operations	302
Download an Object	302
Cancel Spectra S3 Jobs	303
Edit an S3 Job	304

Clear All Canceled or Completed Jobs	305
Manually Starting the S3 Data Path Backend	306
Disallow New Jobs	306
Allow New Jobs	307
Monitor the BlackPearl System	308
Front Bezel Visual Status Beacon	309
Configuring the Visual Status Beacon Color	310
System Status LEDs	310
Check System Messages	313
View the Status of Hardware Components	314
View the Status of Services	316
View the Status of the System Pools	317
View Bucket Contents	319
View Spectra S3 Jobs Information	320
View Tape Media Information	322
View Performance Metrics	327
View Reports	329
Database Backup & Restore	330
Create a Database Backup Schedule	331
Manually Generate a Database Backup	335
Restore from a Database Backup	335
Delete Backup	337
Edit Backup Data Policy	338
Show Backup Physical Placement	338
Reboot or Shut Down a BlackPearl System	339
Using the BlackPearl User Interface	339

Power-Cycle Reset	341
Exit the BlackPearl User Interface	341
Chapter 11 - Using AutoSupport	342
About AutoSupport	343
Enter Contact Information	343
Configure Mail Recipients	344
Create a New Mail Recipient	344
Edit a Mail Recipient	345
Send a Test Email	346
Delete a Mail Recipient	347
Log Sets	348
Configure a Log Set Schedule	349
Manually Generate Log Sets	350
Email a Log Set	351
Download a Log Set	351
Delete Log Sets	352
Chapter 12 - Maintaining the BlackPearl System	353
Data Integrity Verification - Disk Media	353
Cancel Disk Media Verification	354
Data Integrity Verification - Tape Media	355
Cancel Tape Media Verification	356
Initiate RSC Backup	356
Accessing the Technical Support Portal	357
Create an Account	357
Log Into the Portal	359
Configuring Automated Software Upload	360
Updating Software	361

Check the Curre	ent Software Version	361
Check the Curre	ently Released Software Version	362
Download and S	Stage the Updated Software	363
Install the Upda	te	364
Replacing a Failed	l Component	365
Identify the Faile	ed Component	365
Chapter 13 - FAQ and	Troubleshooting	368
BlackPearl Cache		369
How is Cache U	sed and Allocated?	369
Why Does the B	lackPearl User Interface Display 80% Cache Usage?	370
Tape Partitions		370
	er Upgrade to Later Generations of Media in the Same Tape	370
What Happens V	When a Tape Partition is Placed in Standby/Quiesced?	371
What Happens V	When a Tape Partition is Re-Activated?	371
	ge the Tape Library Used by the BlackPearl System While Minact, Management Time, and System Downtime?	372
Tape Media		372
How Does a Use	er Know if Tape Media is Running Out of Space?	372
Can Data be Ove	erwritten on Existing Tapes?	372
Can WORM Me	dia be Used With the BlackPearl System?	373
Tape Media Ejection	on	373
	f a User Ejects a Tape From the Library Before Ejecting the Tap l User Interface?	
	er Configure Their T50e or T120 Library to Support Ejecting Taj Pearl System?	-
Tape Drive Cleani	ing	375
How Does a Use	er Know Their Cleaning Media is Expired?	375

How Does a User Use Cleaning Media in a T50e or T120 Library That Does Not Have a Cleaning Partition?	376
BlackPearl Database Backup	376
How Does a User Verify the Database Backup Schedule?	377
How Does a User Create a Bucket Isolated Data Policy for the Database Backup Tapes?	377
BlackPearl Component Hardware	. 378
How Does a User Know if a Component of the BlackPearl System Has an Error?	378
Intelligent Object Management (IOM)	378
Best Practices	. 379
Special Firewall Feature for Connecting to BlueScale	380
Introduction	380
Warning	380
Basic Steps	380
Capacity Mode versus Performance Mode	380
Chunks	380
Performance Mode	381
Capacity Mode	381
Tape Handling Refactor Starting with BlackPearl Software Version 5.3	381
General BlackPearl Notes	381
Tape Drive Failure Modes	. 382
Move Failures/Tape Stuck in Drive	382
Library, Drive, and Tape Failure Behavior in BlackPearl version 5.3	383
Enabling iSCSI For Use With the Spectra Swarm	385
Troubleshooting	388
Resolving a BlackPearl Management Port IP Address Conflict	397
Using the Console	397

Using a Separate Computer	397
Network Setup Tips	399
Configuration	400
Connectivity to the Network	400
Troubleshooting	403
Tools	403
Spectra Logic Technical Support	404
Before Contacting Support	404
Determine System Serial Number	405
Opening a Support Ticket	405
Remote Support	408
Enabling Remote Support	409
Disabling Remote Support	411
Appendix A - IPMI Configuration	413
Appendix B - Specifications	416
Data Storage Specifications	416
Drive Specifications	417
Capacity	418
System Specification	421
Size and Weight	422
Environmental Specifications	425
BlackPearl Gen2 X Series System	426
BlackPearl Gen1 S Series Systems, Gen1 V Series Systems, and 44-Bay	, 1
96-Bay Expansion Node	427
107-Bay Expansion Node	427
Heat Generation	428

Power Requirements	428
Input Power Requirements	428
Power Cord Specifications	430
Interface Specifications	432
System Interface Connectors	433
Expansion Node and Tape Drive Interface Connectors	434
Interface Cables	435
Universal Serial Bus (USB) Support	436
Appendix C - Installation Checklist	437
Appendix D - BlackPearl 1.0 Chassis Overview & Specifications	440
Components	440
Front View	440
Rear View	442
Rear Panel	443
Specifications	444
System Specification	445
Interface Specifications	445
Appendix E - Regulatory & Safety Standards	447
EU Declaration of Conformity	447
Certifications	451
CE Marking	451
FCC Notice	452
Class A Emissions Warning	452
Safety Standards and Compliance	452
Waste of Electronic and Electrical Equipment (WEEE) Directive	453
Restriction of Hazardous Substances in Electrical and Electronic Equipment (RoHS)	453

Recycling Your System	453
Conflict Minerals Policy	453
Appendix F - Open Source Code Acknowledgements & Package List	455
Apache	455
FreeBSD	455
Java	456
Samba	463
Nginx	464
Ruby	464
Ruby on Rails	466
ZFS	466
Included Packages	466
la day	407

About This Guide Intended Audience

About This Guide

This guide describes how to configure, monitor, and maintain the Spectra[®] BlackPearl Converged Storage System[®], sometimes referred to as the *system* in these instructions. It also provides product specifications.

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, Fibre Channel, and Ethernet. You also need to be familiar with installing, configuring, and using data file storage and archival software.

BLACKPEARL USER INTERFACE SCREENS

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

About This Guide Related Information

RELATED INFORMATION

This section contains information about this document and other documents related to the Spectra BlackPearl Converged Storage System.

Typographical Conventions

This document uses the following conventions to highlight important information:



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



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



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

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

Related Publications

For additional information about the Spectra BlackPearl Converged Storage System and the Spectra S3 interface, refer to the publications listed in this section.

Spectra BlackPearl Converged Storage System

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

- The Spectra BlackPearl Site Preparation Guideprovides important information that you should know before installing a BlackPearl system in your storage environment.
- The Spectra BlackPearl RackMount Installation Guideprovides detailed instructions for installing the BlackPearl system in a standard rack.

About This Guide Related Information

• The *Spectra BlackPearl Network Setup Tips* document provides helpful instructions for troubleshooting common connectivity problems.

- The Spectra BlackPearl Spectra S3 API Reference provides information on understanding and using the Spectra S3 API.
- The *BlackPearl Eon Browser User Guide* provides installation and usage information for the Spectra Eon browser.
- The Spectra BlackPearl & Verde HotPair Installation & Configuration Guide document provides detailed information on installing and using a the BlackPearl system in a HotPair configuration.

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 system, 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 the system.
- The *Spectra 12- & 36-Drive Chassis Boot Drive Replacement Guide* provides instructions for replacing a failed boot drive in the system.
- The *Spectra 12-, 36- & 45-Drive Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive after the system is installed.
- The *Spectra 12-, 36- & 45-Drive Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in the system.
- The Spectra 12-, 36- & 45-Drive Chassis Power Supply Replacement Guide provides instructions for replacing a failed power supply after the system is installed.
- The Spectra 12-Drive Chassis HBA Replacement Guide and Spectra 36-Drive Chassis HBA Replacement Guide provide instructions for replacing a failed HBA in the system.
- The *Spectra 96-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 107-bay expansion node.

About This Guide Online Forum

Tape Library User Guides

Spectra Logic Tape Libraries

User Guides for Spectra Logic tape libraries are posted on the Support Portal website at: support.spectralogic.com/documentation/user-guides.

IBM Tape Libraries

User Guides for compatible IBM® tape libraries are posted on the IBM Knowledge Center website at: ibm.com/support/knowledgecenter/products/.

ONLINE FORUM

Need help with Spectra Logic's S3 software development kits or the Spectra S3 API? Post your question at the Spectra Logic S3-SDK discussion forum located at: https://developer.spectralogic.com/forums

Chapter 1 - Product Overview

This chapter provides an overview of the Spectra Logic BlackPearl Converged Storage System features and components.

Topic	
Overview	page 30
Features	page 30
Components	page 33
Gen2 X Series	page 33
Gen1 S Series, Gen1 P Series, and Gen1 V Series	page 37
96-Bay Expansion Node	page 43
107-Bay Expansion Node	page 45
BlackPearl User Interface	page 47
Menus page 48	
Status Icons	page 51
Supported Browsers	page 52

OVERVIEW

The BlackPearl Converged Storage System allows data to move seamlessly into tape storage in a way not previously possible. It enables users to deploy a tier of deep storage that is cost effective, easy to manage, and scalable to exabytes of data.

FEATURES

The BlackPearl system includes the following features:

44-Bay Expansion Node

The BlackPearl 4U expansion node accommodates up to 44 disk drives with an active bezel, and 45 disk drives with a passive bezel. Up to eight 44-bay expansion nodes can be connected to a BlackPearl 4U system, which allows the system to use the 44-bay expansion nodes as storage domain targets. Up to two 44-bay expansion nodes can be connected to a BlackPearl 2U system.

96-Bay Expansion Node

The 96-bay expansion node accommodates up to 96 disk drives with an active or passive bezel. Up to nine 96-bay expansion nodes can be connected to a BlackPearl 4U system, which allows the system to use the 96-bay expansion nodes as storage domain targets. Up to two 96-bay expansion nodes can be connected to a BlackPearl 2U system.

107-Bay Expansion Node

The 107-bay expansion node acts as an expansion node for the BlackPearl converged storage system. The expansion node accommodates up to 107 disk drives with an active bezel.

BlackPearl User Interface

The BlackPearl user interface is used to perform configuration and management tasks on the BlackPearl system. It also lets you monitor the hardware and view system messages. The BlackPearl user interface also provides monitoring and control of some aspects of an attached Spectra Logic tape library.

Easy Network-Based Administration

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

HotPair

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

Integration with a Spectra Logic Tape Library

Fibre Channel and SAS HBAs can be installed to provide connectivity to a Spectra Logic tape library using LTO or TS11*xx* technology drives.

Integration with the IBM® TS4500 Tape Library

Fibre Channel HBAs can be installed to provide connectivity to the IBM TS4500 tape library using LTO or TS11*xx* technology drives.

Intelligent Object Management

With IOM, the BlackPearl system is capable of self-healing files present on the system, as well as automatically compacting data stored on tape, and provides an easy migration path from one type of storage to another. IOM also allows multiple object versioning and data prestaging from tape to disk, and improves tape library performance by reducing the number of cartridge mounts.

LTFS Format

The BlackPearl system with a supported tape library, writes data on tape in the open Linear Tape File System[®] (LTFS) format to ensure you are always able to access it.

Mirrored Boot Drives

The operating system is hosted on two mirrored drives.

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 system. Rack-mounting hardware is included with each BlackPearl system.

RAID-Protected Data Drives

The base BlackPearl system includes two solid-state drives which store the system database, and ten spinning disk drives which provide the system's caching capacity. The drives are grouped into volumes with double-parity protection and data integrity verification to protect against data corruption.

Redundant Hardware

The system features N+1 redundant power supplies and data drives that are hot-swappable for uninterrupted operation.

Spectra S3 Clients

Users can leverage a library of existing Spectra S3 clients available through the Spectra Logic Developer Program, or develop their own client. The user moves data through the client to the BlackPearl system and then the system handles all interaction with the tape library.

Spectra S3 Interface

The Spectra S3 interface is a data transport and communication interface that allows software clients to direct and manage "bulk" storage read or write operations of data objects. The first implementation supports bulk object storage operations with tape for accessibility to the lowest cost media option.

10GBase-T Ethernet Connectivity

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

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 system.

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 system.

100 Gigabit Ethernet

An optional dual port, 100 Gigabit Ethernet (100 GigE) network interface card can be installed to provide high-speed data connections between hosts and the BlackPearl system.

COMPONENTS

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

Gen2 X Series

Front View

Figure 1 show the components on the front of the Gen2 X Series BlackPearl systems with the front bezel removed.

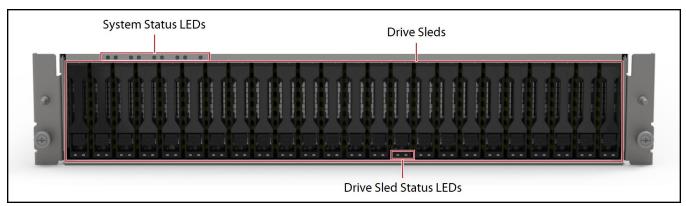


Figure 1 The front view of the Gen2 X BlackPearl system (front bezel removed).

Component	Description
Front bezel (not shown)	The front bezel mounts on the front of the chassis, and contains the Visual Status Beacon light bar which provides status information for the system. See Front Bezel Visual Status Beacon on page 309 for more information.
System status LEDs	The status LEDs indicate power status, fan status, server status, and chassis status. See System Status LEDs on page 310 for more information.
Data drives	The base Gen2 X Series BlackPearl Converged Storage system includes two 1.6 TB high-performance solid-state drives for database storage and four 6.4 TB high-performance solid-state drives for the object cache. The drive sleds slide into bays in BlackPearl 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	 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 has experienced a fault. A service action is required. Amber blinking at 1 Hz - The SSD is attempting to link. Amber blinking at 2 Hz - The SSD failed to link.
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 2 show the major components on the rear of the Gen2 X BlackPearl chassis.

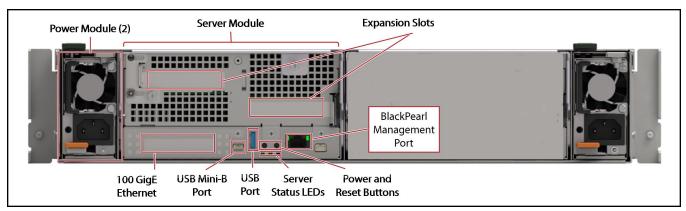


Figure 2 The rear view of the Gen2 X BlackPearl system.

Component	Description
Power modules	 The Gen2 X BlackPearl system 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 two LEDs to indicate power to the power module and status of the power module.
Server module	The server module in the Gen2 X Series BlackPearl system provides Ethernet, Fibre Channel, SAS, USB, and other connections.
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 Rest Buttons	The server Power and Reset buttons allow you to turn off or on 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	The BlackPearl management port is used to connect to a browser-based user interface to configure, manage, and monitor the Gen2 X Series BlackPearl system. 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.
100 GigE Ethernet ports	The two 100 Gigabit Ethernet (100 GigE) ports are used for data transfer on an Ethernet network.
USB and USB Mini-B 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. Only connect a USB drive or keyboard as directed by Spectra Logic Technical Support. The front bezel connects to the active server module's USB port while in production use.
Expansion slots	 The expansion slots accommodate optional interface cards to provide additional connectivity. An optional four-port SAS card provides connectivity to SAS drives in a Spectra Logic tape library, or provides connectivity for up to two 44-bay expansion nodes, and up to four 96-bay or 107-bay expansion nodes. A four-port 16 GB or 32 GB Fibre Channel card provides connectivity to four Fibre Channel tape drives in a Spectra Logic or supported tape library.

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

Front View

Figure 3 shows the components on the front of the Gen1 S Series or Gen1 P Series BlackPearl system. All information is the same for the Gen1 S Series and Gen1 P Series unless specified. Figure 4 shows the components on the front of the Gen1 V Series BlackPearl system with the front bezels removed.

For a description of the components on the BlackPearl 1.0 chassis, see "BlackPearl 1.0 Chassis Overview & Specifications" on page 440.

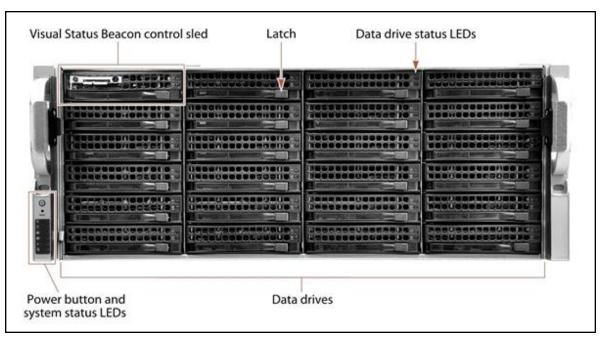


Figure 3 The front view of the Gen1 S Series BlackPearl 4U system (front bezel removed).

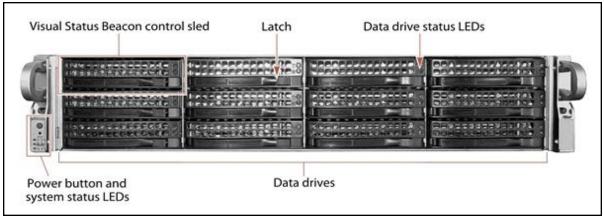


Figure 4 The front view of the Gen1 V Series BlackPearl 2U system (front bezel removed).

Component	Description
Front bezel (not shown)	The front bezel mounts on the front of the chassis, and contains the Visual Status Beacon light bar, if included, which provides status information for the system. See Front Bezel Visual Status Beacon on page 309 for more information.
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 power button controls the main AC power for the BlackPearl system.
System status LEDs	The status LEDs indicate power status, disk and network activity, as well as hardware faults. See System Status LEDs on page 310 for more information.
Data drives	The base BlackPearl 4U system includes one high-performance solid-state drive, and five spinning-disk drives mounted on individual drive sleds in the front of the chassis. Additional drives are installed in the rear of the chassis. The BlackPearl 2U system includes ten spinning-disk drives and two high-performance solid-state drives in the front of the chassis. The drive sleds slide into bays in BlackPearl 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.
Data drive status LEDs	Two LEDs on each drive sled indicate the status of the drive. One LED is for drive status while the other shows drive activity.
Empty drive sleds	Empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow.

Rear View

Figure 5 shows the major components on the rear of the Gen1 S or Gen1 P Series BlackPearl system. All information is the same for the Gen1 S Series and Gen1 P Series unless specified. Figure 6 shows the major components of the Gen1 V Series BlackPearl system chassis.

For a description of the components on the BlackPearl 1.0 chassis, see "BlackPearl 1.0 Chassis Overview & Specifications" on page 440.

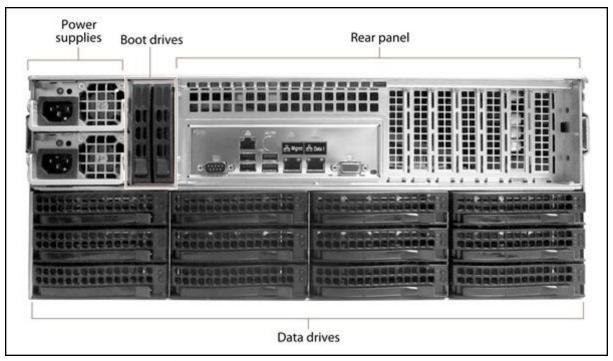


Figure 5 The rear view of the Gen1 S Series BlackPearl 4U system.

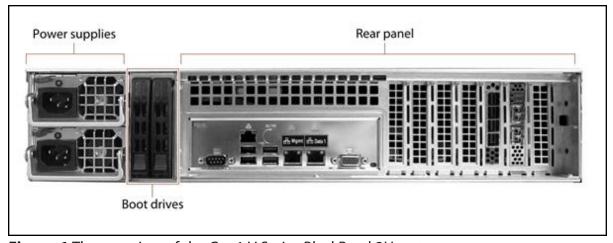


Figure 6 The rear view of the Gen1 V Series BlackPearl 2U system.

Component	Description
Power supplies	 The standard BlackPearl system 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 system allows for Ethernet, Fibre Channel, SAS, USB, and other connections. See Rear Panel on page 41 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 system are hot swappable which allows for uninterrupted operation during replacement.
Data drives (BlackPearl 4U system only)	The base Gen1 S Series BlackPearl 4U system includes one high-performance solid-state drive, and five spinning-disk drives mounted on individual drive sleds in the rear of the chassis. Additional drives are installed in the front of the chassis. The drive sleds slide into bays in the BlackPearl 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. Note: The Gen1 S Series BlackPearl 2U system does not have data drives in the rear of the chassis.
Empty drive sleds (BlackPearl 4U system 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 7 shows the components on the rear panel of the Gen1 S Series chassis for the BlackPearl 4U and 2U systems.

For a description of the components on the BlackPearl 1.0 chassis, see "BlackPearl 1.0 Chassis Overview & Specifications" on page 440.

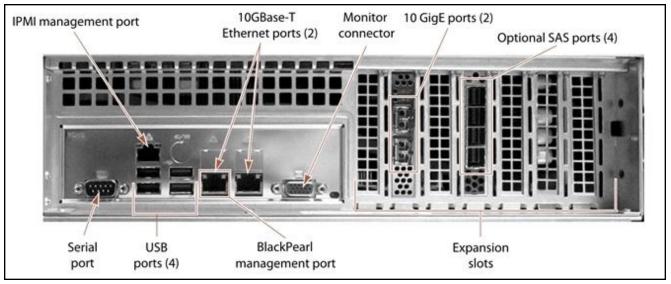


Figure 7 The Gen1 S Series BlackPearl rear panel components.

Component	Description
IPMI management port	See "IPMI Configuration" on page 413 for information on using IPMI management.
10GBase-T Ethernet ports	The Gen1 S Series BlackPearl system 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 100 GigE ports, 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 Gen1 S Series BlackPearl system 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 system can contain different types network interface cards, but can only use one card at a time. Note: Unless your system includes a 100 GigE network card, 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 100 GigE, 40 GigE, or 10GBase-T Ethernet network interface card can be used instead of the 10 GigE card to provide a high-speed data connection between hosts and the Gen1 Series S BlackPearl system. A system can contain different types of network interface cards, but can only use one type at a time. Ports of the same type can be aggregated for better performance. An optional two- or four-port SAS card provides connectivity to SAS drives in a Spectra Logic tape library, or provides connectivity for up to one or two 44-bay expansion nodes, and up to two or four 96-bay or 107-bay expansion nodes. A two- or four-port Fibre Channel card provides connectivity to two or four Fibre Channel tape drives in a Spectra Logic or supported tape library.
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 system. 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.

96-Bay Expansion Node

Front View

Figure 8 shows the major components on the front of the 96-bay expansion node.

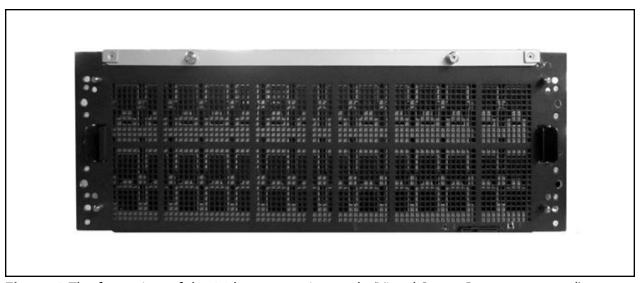


Figure 8 The front view of the 96-bay expansion node (Visual Status Beacon removed).

Component	Description
Front bezel (not shown)	The front bezel mounts on the front of the expansion node, and contains the Visual Status Beacon light bar, if included, which provides status information for the expansion node. See Front Bezel Visual Status Beacon on page 309 for more information.

Rear View

Figure 9 shows the major components on the rear of the 96-bay expansion node.

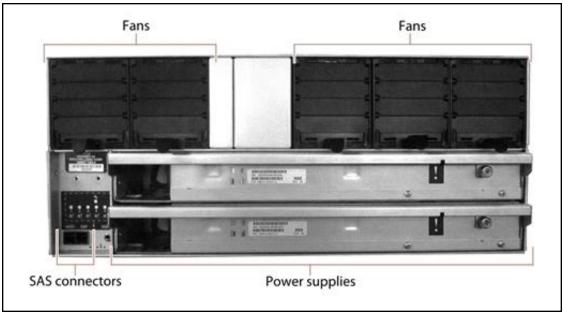


Figure 9 The rear view of the 96-bay expansion node.

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 a BlackPearl system.

107-Bay Expansion Node

Front View

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

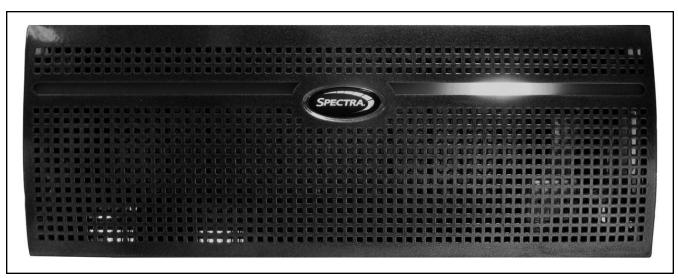


Figure 10 The front view of the 107-bay expansion node.

Component	Description
Front bezel	The front bezel mounts on the front of the expansion node, and contains the Visual Status Beacon light bar, if included, which provides status information for the expansion node. See Front Bezel Visual Status Beacon on page 309 for more information.
Data drive activity LEDs (not shown)	Numbered LEDs indicate drive activity for each drive in the expansion node.
Mute button (not shown)	The mute button silences the chassis alarm.
System status LEDs (not shown)	The status LEDs indicate power status, as well as hardware faults for fans, power supplies, and temperature.
Power button (not shown)	The power button controls the main AC power for the 107-bay expansion node.

Rear View

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

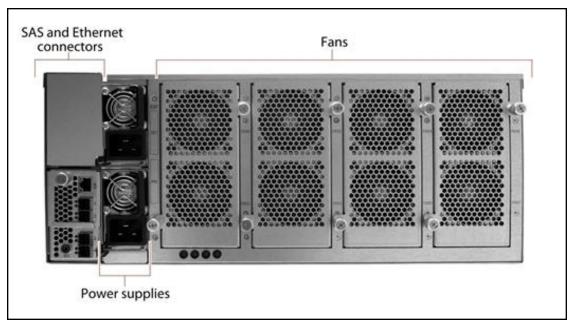


Figure 11 The rear view of the 107-bay expansion node.

Component	Description
SAS and Ethernet connectors	The rear panel of the 107-bay expansion node has one or two expander panels which include one Ethernet port and four SAS ports used to connect a 107-bay expansion node to a BlackPearl system.
Fans	Eight hot-swappable fans, in banks of two, provide the cooling for the 107-bay expansion node.
Power supplies	 The 107-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.

BLACKPEARL USER INTERFACE

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

Note: Prior to BlackPearl version 5.3, the data storage units displayed in the BlackPearl user interface used base 10 (MB, GB, TB). Starting with BlackPearl 5.3, the unit displayed are base 2 (MiB, GiB, TiB) to better reflect actual storage usage. Screen captures used in this guide may not match what is displayed in the BlackPearl user interface.

Menus

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

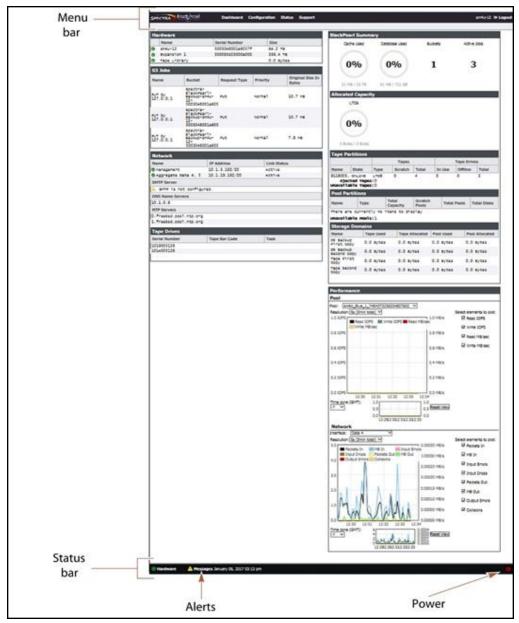


Figure 12 The Dashboard screen of the BlackPearl user interface.

The following table provides an overview of the screens available under each menu.

Menu	Available Options
Dashboard	The Dashboard navigation link returns you to the Dashboard screen from any other screen in the interface. The Dashboard screen displays the general status of the system, tape cache, 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 system.
Configuration	The Configuration menu provides access to controls for configuring all aspects of system operation. NAS Pools—Displays information about any currently configured storage 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. Buckets—Displays information about the currently configured buckets and lets you add, edit, or delete buckets. You can also view information about the objects contained in a bucket and the physical tape media associated with each bucket. Advanced Bucket Management Storage & Policy Management—Lets you configure partitions, and create new storage domains and data policies. Replication Targets—Lets you configure BlackPearl, Amazon® S3, and Microsoft® Azure® targets. Database Backup—Displays information about any currently generated backups on the system, as well as allows you to create new backups, either manually or on a schedule. 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 system, configure a static route, Domain Name Servers, date and time, as well as entering SMTP (Simple Mail Transport Protocol) information to allow the system to send emails. Certificates—Provides controls for installing signed, trusted SSL certificates for your data and management ports so that you do not need to resolve the security certificate warning when accessing these ports.

Menu	Available Options
Configuration (continued)	 Mail Recipients—Provides controls for configuring mail recipient accounts to receive emails when a message severity threshold is reached, or when AutoSupport Log sets (ASLs) are generated by the system. Users—Provides controls for creating new 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 system in your environment. Hardware—Displays information about the system, its components, tape libraries and associated tape drives, and disk expansion nodes and associated disk drives. Selecting the tabs on the Hardware screen displays detailed component status information. Tape Management—Provides controls for managing the tape media in the tape library connected to the BlackPearl system. S3 Jobs—Displays information about the status of all S3 jobs currently being processed by the system. Messages—Displays system messages for the system. Performance—Displays performance metrics for the tape cache, individual drives, network connections, and the CPUs in the integrated server. Reports—Provides controls for generating reports about the configuration and status of the system. Reports can be generated in XML or JSON (JavaScript Object Notation) formats.
Support	 The Support menu provides access for maintenance and troubleshooting options for the BlackPearl system. Software—Provides controls for updating the BlackPearl software. Activation Keys—Provides controls for entering activation keys. Logs—Displays any current ASL sets on the system and provides controls for generating a new log set. Documentation—Displays links to BlackPearl documentation. Contact Information—Displays contact information for Spectra Logic Technical Support, as well as the part and serial numbers for the system. 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 system. Clicking this link takes you to the Hardware screen.
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.
Power	Provides controls for rebooting and shutting down the system. Note: The connection to the user interface is lost after running the reboot command. Wait while the system reboots before attempting to reconnect to the user interface.

Status Icons

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

lcon	Meaning
	Component OK The component is functioning correctly.
1	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.
8	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® ChromeTM version 22 or later
- Mozilla® FireFox® version 27 or later
- Apple® Safari® version 7 or later
- Microsoft Internet Explorer® version 11 or later
- Opera Software Browser version 12 or later

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

Chapter 2 - Initial Configuration

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

Topic	
Before You Begin	page 54
Connect Ethernet Cables	page 54
Power On the System	page 55
Initial Configuration	page 53
Initial Configuration	page 53
Configure the BlackPearl Management Port	page 56
Automatically Import Activation Keys	page 57
Log Into the BlackPearl User Interface	page 58
Configure the Data Connection	page 61
Configure an Aggregate Port Data Connection	page 61
Configure a Single Port Data Connection	page 64
Configure a Static Route	page 65
Create a User	page 67
Description of User Types	page 67
Create a User	page 68
View S3 Credentials	page 70
Next Steps	page 71

BEFORE YOU BEGIN

Make sure the system is installed in accordance with the *Spectra BlackPearl Site Preparation Guide* and the *Spectra BlackPearl Rack-Mount Installation Guide*.

Additionally, make sure your Spectra Logic tape library is installed in accordance with it's *Site Preparation Guide*, available on the Support Portal website at support.spectralogic.com/documentation.

See "Installation Checklist" on page 437 on page page 437 for a checklist of installation steps.

Note: If your BlackPearl system was installed by Spectra Logic Professional Services, all the steps in this chapter were performed by the installer. Please see Next Steps on page 71 to begin using your BlackPearl system.

CONSIDERATIONS FOR BLACKPEARL NAS SYSTEMS

If you BlackPearl system includes NAS drives, it is important that the drives that are to be used for NAS are not installed in any chassis in the system when the system is powered on for the first time.

Drives used for the system database, system cache, and Nearline or Online storage pools must be installed before the system is powered on for the first time.

CONNECT ETHERNET CABLES

Before proceeding with the below sections, you must connect Ethernet cables to the management and data ports on the BlackPearl system rear panel. See Rear Panel on page 41 for the location of the Ethernet ports on the rear of the system.

POWER ON THE SYSTEM

Use the instructions in this section to power on a BlackPearl system, 44-bay, 96-bay, or 107-bay expansion node. During the power-on sequence, the BlackPearl system 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 55.
 - To power on a 96-bay or 107-bay expansion node, connect power cables to the power supplies on the rear of the expansion node chassis (see Figure 9 on page 44 and Figure 11 on page 46), 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.

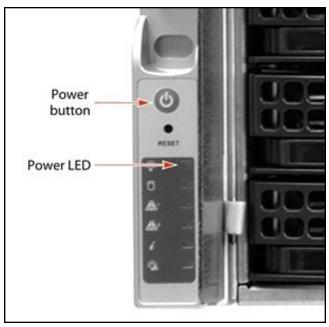


Figure 13 Press the power button.

2. To power on a BlackPearl Gen1 or Gen2 master node, connect power cables to the power supplies on the rear of the master node chassis (see Figure 5 on page 39 and Figure 6 on page 39), then plug the power cables into power outlets near the chassis. Wait while the BlackPearl system completes its power-on sequence, which takes approximately 5 to 10 minutes, depending on the configuration.

Note: Do not use the system's front panel power button to power down the system. See Reboot or Shut Down a BlackPearl System on page 339.

CONFIGURE THE BLACKPEARL MANAGEMENT PORT

The default IP address for the BlackPearl management port is set to 10.0.0.2, with a netmask of 255.255.25.0. If your network is already using this IP address, or you want to configure a different IP address for the management port, use the BlackPearl console to configure the management port IP address.

If you do not want to change the default management port IP address, skip to Log Into the BlackPearl User Interface on page 58.



You must connect Ethernet cables as described in Connect Ethernet Cables on **IMPORTANT** page 54 before either proceeding with the steps below or skipping this section and accepting the default IP address for the management port.

Note: Using the BlackPearl console is the recommended way to change the management port IP address. If you cannot use the console, see FAQ on page 1 for information on alternate methods.

1. Connect a monitor and USB keyboard to the rear of the BlackPearl system. See Rear Panel on page 41 to locate the monitor and USB connectors. The Console screen displays.

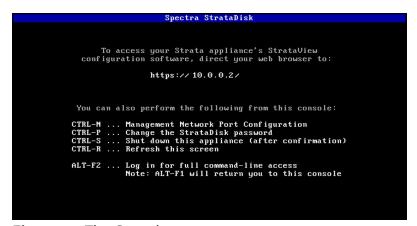


Figure 14 The Console screen.

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

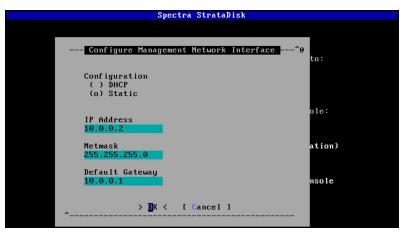


Figure 15 The Configure Management Network Interface screen.

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

- **5.** Connect a cable from your network to the BlackPearl management port on the BlackPearl system. 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 system.

AUTOMATICALLY IMPORT ACTIVATION KEYS

Activation keys enable features on the BlackPearl system. They are tied to the serial number of the system for which they are issued, and cannot be used on another system. Renewals of expired activation keys are obtained by contacting Spectra Logic Technical Support (see Contacting Spectra Logic on page 8).

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

Note: If your BlackPearl documentation kit does not contain a USB device, see Manually Enter Activation Keys on page 217 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 system. See Figure 7 on page 41. When the BlackPearl system detects the USB device it automatically imports the activation keys and power cycles the system.
- 2. Wait while the BlackPearl system performs its power-on sequence and then log into the BlackPearl user interface.



Do not remove the USB device until after the system power cycles and the **IMPORTANT** BlackPearl user interface displays a message that it is safe to remove the USB

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

- Remove the USB device.
- **ii.** On the menu bar, select **Status > Messages**. The messages screen displays.
- iii. Select the message about safely removing the USB device, and then select **Action** > **Mark as read**. The informational message closes.

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.

1. Using a standard web browser, enter the IP address for the BlackPearl management port configured in Configure the BlackPearl Management Port on page 56.

Note: The BlackPearl user interface uses a secure connection.

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

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

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 216.
- **3.** Enter the primary administrator username and password.

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

Notes:

- Spectra Logic recommends that you change the default password for the primary administrator (see Edit a User on page 207).
- If you are upgrading from a previous version of BlackPearl software, the existing administrator account "spectra" is retained and the "Administrator" account is automatically created without any permissions.
- If you are upgrading from a previous BlackPearl software version to software version 4.0 or later, the BlackPearl system retains any accounts created before the upgrade.

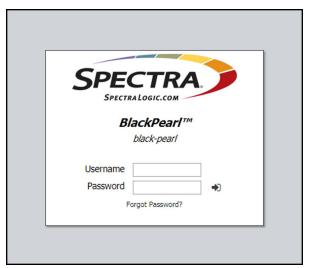


Figure 16 The BlackPearl Login screen.

4. Click > to log in.

Note: If this is an initial installation and activation keys have not been entered, the user interface displays the Verde logo and interface design. The interface changes to the BlackPearl interface and functionality after you enter all activation keys provided. See Automatically Import Activation Keys on page 57.



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

INSTALL NAS DRIVES

If your BlackPearl system includes NAS based storage, you must install the drives used for NAS storage before continuing. If your system does not include NAS storage, continue with Configure the Data Connection below.

Use the instructions below to install NAS drives into the BlackPearl system.

- **1.** Power the system down, including all expansion nodes, if present. See Reboot or Shut Down a BlackPearl System on page 339.
- **2.** Install the NAS drives into the master node and expansion nodes, if present. If multiple nodes are present, leave one hot spare drive per chassis out of the system until pool setup is complete. See the *Spectra BlackPearl Drive Installation Guide* for instructions.
- **3.** Power the system on, including all expansion nodes, if present. See Power On the System on page 55.
- 4. Continue with Configure the Data Connection below.

CONFIGURE THE DATA CONNECTION

This section describes using the BlackPearl user interface to configure one or more data connections for the BlackPearl system. The system includes two 10GBase-T ports, and two 10 GigE ports on the rear panel (see Figure 7 on page 41). Optionally, a 40 GigE card or 10GBase-T card can be installed in the system. The configuration steps are the same for all port types.

Notes:

- You can create one or more data connections to the system.
- You can configure link aggregation for better performance.
- While different types of Ethernet network interface cards can be installed in the same BlackPearl system, 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 & Verde HotPair *Installation & Configuration Guide* for information on configuring data connections.

Configure an Aggregate Port Data Connection

Link aggregation uses multiple Ethernet ports, configured with a single MAC address, to improve data transfer speeds. See Link Aggregation Notes on page 1 for more information.



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

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 system.

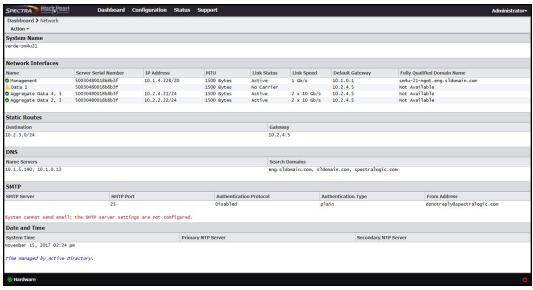


Figure 17 The Network screen.

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

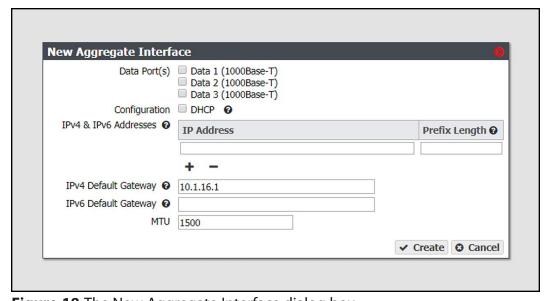


Figure 18 The New Aggregate Interface dialog box.

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

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

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

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

6. If applicable, enter the IPv4 Default Gateway.

Notes:

- If you selected DHCP in Step 4, this option is unavailable.
- The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl system.
- **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 system.
- The IPv6 Gateway does not need to be configured when the BlackPearl system 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 system.

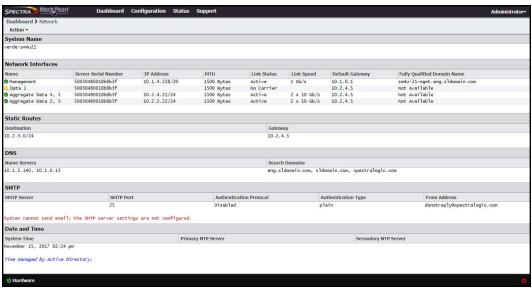


Figure 19 The Network screen.

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

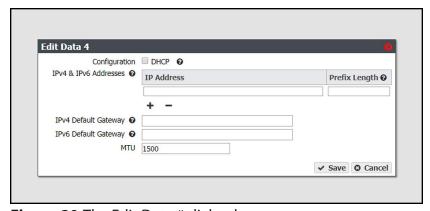


Figure 20 The Edit Data # dialog box.

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

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

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

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

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

5. If applicable, enter the IPv4 Default Gateway.

Notes:

- If you selected DHCP in Step 3, this option is unavailable.
- The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl system.
- 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 system.
- The IPv6 Gateway does not need to be configured when the BlackPearl system 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 system only supports communication with one default gateway. When configuring a BlackPearl system 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 system.

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

For example, if one data connection is on the 10.2.2.x network and another connection is on the 10.2.4.x network, when the 10.2.3.x network is connected externally to the 10.2.4.x network, a static route must be configured on the BlackPearl system 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 system 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.

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 19 on page 64).
- **2.** From the menu bar, select **Action > New Static Route**. The Static Route dialog box displays.



Figure 21 The Static Route dialog box.

- **3.** In the **Destination** field, enter either an IPv4 host address or network address that you want to access through the data connection.
- **4.** Enter the **Gateway** of the data connection used to communicate with the isolated network.
- 5. Click Create.
- **6.** Repeat Step 2 on page 66 through Step 5 for each host computer on the isolated network.

CREATE A USER

Use the instructions in this section to create users, which act as S3 users when interacting with the BlackPearl system through a Spectra S3 SDK (Software Development Kit) client, or Spectra S3 API. Each user has a unique S3 Access ID and Secret Key.

Description of User Types

There are three different types of users in the BlackPearl user interface. Administrator users, monitor users, and login users. Additionally, users can be combined with other users into S3 groups, in which all members of the group share the same permissions. 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. Starting with BlackPearl 4.0, the default username for the primary administrator is Administrator , with the password spectra . If you are upgrading from a previous version of BlackPearl software, the existing administrator account " spectra " is retained and the Administrator account is automatically created without any permissions. Note: Spectra Logic recommends changing the password for the primary administrator. See Edit a User on page 207.
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 ejecting tapes. This account is useful if you need to view the status of S3 jobs, or any other aspect of the user interface, or eject tapes, but do not have access to an administrator account. Note: 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. Note: For BlackPearl software versions older than BlackPearl 4.0, the monitor user account is created by default. If a system running BlackPearl 3.x or older is upgraded to BlackPearl 4.x or later, the existing monitor account is retained. The default username and password are both monitor using all lowercase letters. Note: Spectra Logic recommends that you change the default password for the monitor account. See Edit a User on page 207.
Login User	A user with Login permissions is able to log into the BlackPearl user interface. Note: Administrator and Monitor users must also have Login permission in order to log in to the BlackPearl user interface.

Create a User

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

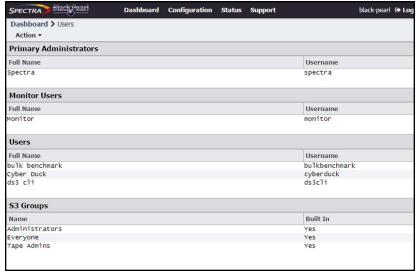


Figure 22 The Users screen.

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

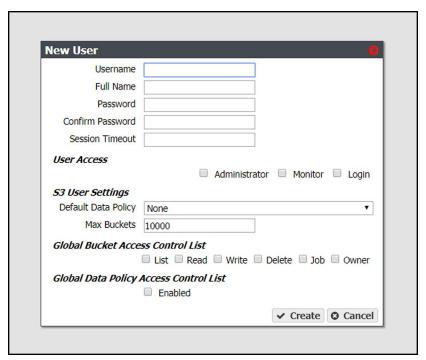


Figure 23 The New User dialog box.

3. Enter the desired **Username** for the user. The Username cannot contain capital letters or spaces and is limited to 16 characters. The Username is used to identify the user in the Spectra S3 environment.

- **4.** Enter the user's **Full Name**.
- **5.** Enter and confirm the desired **Password** for the user.
- **6.** If desired, enter the 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 67 for information on each level of user access permission.
 - **Note:** Administrator and Monitor users must also select **Login** in order to log in to the BlackPearl user interface.
- **8.** From the drop-down list, select a **Default Data Policy** for the user. If specified, the system uses the selected data policy for all buckets created by the user, unless a different policy is specified during bucket creation.
- **9.** Enter a value for the **Max Buckets** the user is allowed to create. The default value of 10000 is pre-entered.
- **10.** Select or clear options for the **Global Bucket Access Control List**. These options give or deny permission for the user being created to perform the action described in the table below, for all buckets present on the system, as well as any buckets created at a future date.

Name	Description
List	The user can see the bucket and can list the objects in a bucket.
Read	The user can get objects and create GET jobs.
Write	The user can put objects and create PUT jobs.
Delete	The user can delete objects, but cannot delete the bucket.
Job	The user can modify or cancel jobs created by other users. The user can also see the details of jobs created by other users. Note: All users can view all jobs, but by default, only the initiator of the job can see the full details of a job.
Owner	The user receives full access to all buckets, including all permissions listed above.

- **11.** If desired, under **Global Data Policy Access Control List**, select the check box to allow the user access to any data policy created on the system.
- **12.** Click **Create** to create the new user. The system generates a unique S3 Access ID and Secret Key for the user.
- 13. If desired, repeat Step 2 on page 68 through Step 12 to create additional users.

VIEW S3 CREDENTIALS

There are two methods you can use to view S3 credentials, through the User screen, or the User Profile screen.

Using the User Screen

- **1.** From the menu bar, select **Configuration > Users.** The Users screen displays (see Figure 22 on page 68).
- **2.** Select the user for which you want to view the S3 credentials from the User pane of the Users screen, and then select **Action > Show S3 Credentials**. The S3 Credentials dialog box displays.



Figure 24 The S3 Credentials dialog box.

3. Use the **S3 Access ID** and **S3 Secret Key** to access the BlackPearl system using a Spectra S3 client, Spectra S3 API, or Vail sphere.

Using the User Profile Screen

- **1.** From the right side of the menu bar, select *Current User* > **User Profile**. The User Profile screen displays.
- **2.** Select **Action > Show S3 Credentials**. The S3 Credentials dialog box displays.

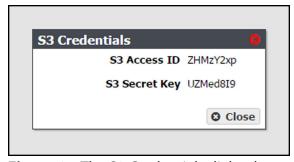


Figure 25 The S3 Credentials dialog box.

3. Use the **S3 Access ID** and **S3 Secret Key** to access the BlackPearl system using a Spectra S3 client, Spectra S3 API, or Vail sphere.

NEXT STEPS

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

- See Understanding Spectra Advanced Bucket Management Concepts on page 72 for information about Spectra S3 and Advanced Bucket Management concepts you need to understand before you begin designing the storage architecture of the BlackPearl system.
- If your system includes 96-bay expansion nodes, you can optionally change the configuration of nearline disk pools. See Manage Buckets on page 172.
- See Additional Configuration Options on page 177 for information about the additional options that can be configured on the BlackPearl system.
- See Operating the BlackPearl System on page 301 for information about day-to-day monitoring and operation of the system.
- See Using AutoSupport on page 342 to set up AutoSupport to collect and email log sets.
- See Maintaining the BlackPearl System on page 353 for maintenance options for the system.

Chapter 3 - Understanding Spectra Advanced Bucket Management Concepts

This chapter explains the concepts of the BlackPearl system advanced bucket management. It is important to understand the information in this chapter before you begin designing the storage architecture of the BlackPearl system.



It is difficult and time consuming to change a data policy once the system writes data to a bucket using the data policy. Make sure that you understand the concepts in this chapter and have thoughtfully planned your data policies before you start using the BlackPearl system to store data.

Topic	
Goals of Advanced Bucket Management	page 73
Spectra S3 Overview	page 73
Spectra S3 Clients	page 75
Storage Domains	page 75
Data Policies	page 75
Data Persistence Rules	page 76
Data Replication Rules	page 77
Tape Eject Strategy	page 77
Tape and Disk Partitions	page 77
Tape Partitions	page 78
Disk Partitions	page 79
Special Considerations for Ejecting Tapes	page 80
Special Considerations for Reading Tapes in a Non-BlackPearl Environment	page 80
Example Configurations	page 81
Single Copy on Tape	page 82
Dual Copy on Tape	page 86

Topic	
Single Copy on Nearline Disk	page 91
Single Copy on Nearline Disk and Tape	page 95
Single Copy on Nearline Disk and Dual Copy on Tape	page 100

GOALS OF ADVANCED BUCKET MANAGEMENT

The BlackPearl system provides a Spectra S3 front end interface to disk, tape and cloud storage. The BlackPearl Advanced Bucket Management (ABM) feature automates many aspects of deep storage including policy based multiple copies on diverse media types without the need for expensive middleware to operate the libraries and stream data to tape drives. The BlackPearl system delivers seamless data management enabling infinite retention, seamless growth, and unlimited retrieval of data for as low as pennies per Gigabyte.

SPECTRA S3 OVERVIEW

The BlackPearl Converged Storage System allows data to move seamlessly into deep storage in a way not previously possible. Spectra S3 is the first native REST-based interface to deep storage which enables easy archiving of large amounts of bulk data. It enables users to deploy tape, nearline disk, and online disk storage that is cost effective, easy to manage, and scalable to exabytes of data.

Spectra S3 utilizes the standard Amazon S3 operations plus additional operations specifically designed to optimize the transport of data objects to and from deep storage. The additional operations define the job so that the BlackPearl system interacts with the objects efficiently and define the data policy to customize where and for how long specific data is stored.

The first of these additional operations is called START BULK PUT. It is an HTTP PUT operation that provides the BlackPearl system with information about the objects that the client wants to send as a single job for storing on tape. The Create Bulk Put command is sent with a payload that is made up of a list of object names and corresponding object sizes. This information allows the BlackPearl system to plan the initial storage of the objects in its cache, and how it will store the data on tape. The response to the Create Bulk Put command is a specifically ordered list of how the BlackPearl system wants those files (objects) sent.

The second command is called Create Bulk Get. The Create Bulk Get command is actually an HTTP PUT command because it too contains a payload for the BlackPearl system. This payload is a list of objects that the client wants to get from the BlackPearl system. It is not necessary for the request payload to contain the size of the files because the BlackPearl system already knows the sizes of the objects (files). The response to the request is again an ordered list of the objects and information about the objects, including if they are already in the cache and ready to be retrieved from cache by a GET command.

Knowing the files that the client wants to retrieve, the BlackPearl system can make the best use of its resources in retrieving the objects. For example, if the list of objects spans across four different tapes and there are four tape drives available, those four tapes can all be loaded into drives and the objects can be read back in parallel, greatly improving the speed at which the client can get all of the objects. Without the Create Bulk Get request, the client would be asking the BlackPearl system for those objects in a less efficient manner.

Storing large amounts of bulk data on tape has historically presented challenges. Spectra S3 addresses these challenges:

- Tape drives are sequential block storage devices, with data laid out in a sequential
 manner along the full length of the tape. This makes it inefficient to retrieve data out of
 order. Spectra S3 plans and queues a large amount of data to be efficiently written to tape;
 it logically groups data on tape in a way that reflects how the client is likely to read it
 back.
- Because of the mechanical nature of the tape media and drives, tape drives demand a large amount of data to be available, via a fast connection. When data is not efficiently streamed for the tape drives to write (due to slow data buffering or a slow connection to the drive), the result is poor write performance. This poor performance is due to a phenomenon referred to as "shoe-shining". When a drive is sent a small amount of data, it writes the data and then is forced to stop. Because the tape cannot stop instantaneously, the drive overshoots a small amount and the tape is not in position for the next write operation. To compensate, the tape drive rewinds to get back to the correct position for the next write. If the next write also has a small amount of data, then the drive writes the next portion and again stops, overshoots, and rewinds, causing a back and forth "shoe-shining" like action. Spectra S3 caches data on the BlackPearl Converged Storage System before starting the transfer to tape, which prevents the shoe-shining behavior from occurring.
- Classically, different tape storage devices wrote data to tape in unique ways, locking you
 into a proprietary and single vendor solution to retrieve previously written data. Spectra
 S3 writes data to tape using the open source Linear Tape File System® (LTFS). With LTFS,
 data is always accessible with any LTFS enabled system.

For more information on the Spectra S3 interface, see the *Spectra BlackPearl Spectra S3 API Reference*.

Spectra S3 Clients

Users can leverage a library of existing Spectra S3 clients available through the Spectra Logic Developer Program, or develop their own client. The user moves data through the client to the BlackPearl system and then the system handles all interaction with the data storage hardware.

BLACKPEARL CACHE

The BlackPearl cache is allocated physical storage on either HDDs or SSDs installed in the system. The cache functions as a transient location for all data transferred to the BlackPearl system from a client, or transferred from tape storage to the BlackPearl system.

The capacity available for cache is managed by the BlackPearl data planner, where active jobs reserve various amounts of cache capacity known as 'chunks', and chunk size can vary.

When writing data to cache destined for tape storage, or restoring data from tape storage to the BlackPearl system, the chunk size is typically 2% of the capacity of a single tape cartridge. If the total job size is less than that amount, the chunk size reduces in size to match the job size.

STORAGE DOMAINS

A storage domain is a collection of data partitions and, when applicable, media type combinations. Storage domains define the possible places where data sent to the BlackPearl Converged Storage System can be stored. Data persistence rules and data policies further define where and for how long specific data is stored.

Entire data partition/media type combinations are members of storage domains. When additional capacity is required, a single storage pool or tape is allocated out of the member data partitions to fulfill the capacity requirement.

DATA POLICIES

A data policy defines data integrity policies (checksum type and end-to-end CRC requirements), default job priorities, and data persistence rules, which define where data should be written and for how long it should be kept. A data policy may be used by multiple buckets, but a bucket uses precisely one data policy.

A data policy consists of one or more permanent persistence rules, zero or more temporary persistence rules, and zero or more retired persistence rules. A persistence rule can be permanent, meaning that data is kept in the specified storage domain at all times, or temporary, meaning that data is kept in the specified storage domain under certain circumstances, and then it can be deleted from that storage domain. Existing permanent and temporary persistence rules may be retired so that the rule is not applied for any new incoming data, but continues to retain data previously written.

Data Persistence Rules

Each data policy must have one or more permanent persistence rules. Each persistence rule targets a specified storage domain. There are three types of persistence rules:

- Permanent A copy of the data is placed in the specified storage domain initially and maintained there permanently.
- **Temporary** A copy of the data is placed in the specified storage domain initially and maintained there at least until the specified retention period expires.
- **Retired** The rule is not applied for any new incoming data, but continues to retain data previously written.

Data is written to every storage domain for which there is a persistence rule with the type configured as permanent or temporary.

The same storage domain cannot be specified multiple times using different persistence rules in the same data policy. The same storage domain can be referred to across different data policies.

Data persistence rules must specify the level of physical isolation required for the data retention. There are two types of data retention:

- **Standard** Data is isolated according to the standard storage domain isolation requirements. When more storage is needed, a tape or pool is assigned to the storage domain. Any buckets using that storage domain can have data on the pool or tape, which can make it difficult to eject all of the tapes for a single bucket.
- Bucket Isolated Data from different buckets cannot be mixed on the same physical storage media.

Notes:

- The **Standard** isolation level provides the best capacity utilization and overall performance.
- Bucket Isolated allocates an entire tape or pool to a bucket when needed.
 Allocating an entire pool to a bucket may use up resources quickly and is not recommended.

Data Replication Rules

Data policies may also contain data replication rules. The BlackPearl system supports replicating data to the following targets:

- BlackPearl target A BlackPearl system remote to the local system that stores replicated data.
- Amazon S3 target An AWS S3 instance remote to the BlackPearl system that stores replicated data.
- Microsoft Azure target— A Microsoft Azure instance remote to the BlackPearl system that stores replicated data.

Tape Eject Strategy

A tape eject strategy must be considered as part of a data policy. Spectra recommends keeping at least one copy of all archived data in the library at all times. Libraries can be easily upgraded by purchasing more slot licenses, or, if the slots become completely full, upgrading the library itself to one with more slots using the exclusive Spectra TranScale technology.

A tape library user or administrator may decide to eject media cartridges from a tape library for any of the reasons described below:

- **Ejecting a copy for off-site disaster recovery:** The BlackPearl system allows a user to make multiple copies of data automatically. A typical use case is to create a "tape first copy" that is intended to be left in the library for easy retrieval as well as an "eject copy" intended to be removed from the library once full for archival at an alternate site for safety. See Configuring Advanced Bucket Management on page 106 for information on setting up multiple copies and ejecting a copy, and the *Tape Library User Guide* for details on the physical process of exporting and importing tapes into the library.
- Ejecting a copy of data for transfer to another location: In some work flows, a user ejects a tape to transfer the data to another facility. Individual tapes can be ejected manually using the BlackPearl user interface (see Eject Tapes on page 280).
- **Ejecting tapes to free up space in the library:** Some work flows and budgets require older or unused media to be ejected, making it not readily available to the BlackPearl system, in order to free up space in the tape library. After tapes are exported, new tapes are imported to provide the BlackPearl system with new media for storage operations.

TAPE AND DISK PARTITIONS

Tape and disk partitions are external data storage targets cabled to the BlackPearl system through SAS or Fibre Channel connections. Once created, partitions are assigned to storage domains.

Tape Partitions

Tape partitions refer to data partitions configured on Spectra Logic or other supported tape libraries. When you create a partition on a tape library attached to a BlackPearl system, the system automatically detects the tape library partition and adds it to the list of available partitions in the BlackPearl user interface. The system also automatically creates two commonly used storage domains: tape first copy, and tape second copy. For more information on storage domains, see Storage Domains on page 75.

Notes:

- Cleaning partitions are not added to the BlackPearl user interface.
- Tape drive cleaning is typically handled by the Spectra tape library. For more
 information on cleaning the library tape drives using the tape library, see your
 Tape Library User Guides.
- Tape drive cleaning is handled automatically by the IBM TS4500 tape library.
- Tape drive cleaning for Spectra Logic libraries can be initiated through the Spectra S3 API. See the *Spectra BlackPearl Spectra S3 API Reference* for more information.
- Tape drive cleaning cannot be initiated through the BlackPearl user interface.
- If the BlackPearl system is configured to transfer data to tape, make sure the
 partitions configured for use by the BlackPearl system do not contain WORM
 (Write Once-Read Many) media. The BlackPearl system is not compatible with
 WORM media.

Tape Drive Reservation

Tape drive reservation allows you to control how the tape drives are used to transfer data, by dedicating drives to accept only read commands or write commands, and to accept only jobs of a specified priority level or higher. With a large number of tape drives, using drive reservation can increase efficiency and reduce latency when either reading or writing data. Reserving tape drives for either reading or writing, or for a specified job priority level, is not required and is typically only used when read or write throughput and drive availability are important enough to dedicate tape drives to that function.

Note: Tape drive reservation is not recommended for BlackPearl systems connected to two or fewer tape drives.

Tape drive reservation is configured on both the drive, and library partition level.

- When reserving an individual tape drive, you can exclude the drive from performing reads, writes, or jobs lower than a specified level.
- You can also configure the library partition to reserve a specified number of drives for either reads or writes. This can prevent individual tape drive failures, or unavailable drives, from impacting the desired number of drives available for either read or write commands.

Note: Tape drives always allow inspection and verify tasks.

Tape Media Inspections

When new tape media is added to the BlackPearl system, the system inspects the tape cartridge as configured in the Spectra S3 service. However, all tapes that are new to the system require inspection before they are usable in a managed state. Additionally, under certain circumstances, the system may override the configured behavior for inspections on already managed tapes.

Inspection Behavior when the Tape Library is in Standby

With BlackPearl software version 5.2 or earlier, if there was an inventory change in the tape library while in standby, the BlackPearl system could react by re-inspecting all tapes in the library. Starting with BlackPearl version 5.3, the system no longer re-inspects tapes when there is an inventory change while the partition is in standby if the S3 service is set to "Never Inspect".

Inspection Behavior when the Tape Library is in Active Use

Prior to BlackPearl version 5.3, if a tape library associated with the BlackPearl system goes offline, or is otherwise made unavailable to the BlackPearl system, the tapes are marked as "Lost" by the BlackPearl system. When this occurs, the tape is considered to be a new tape, and is re-inspected when the tape library is made available. Starting with BlackPearl version 5.3, the BlackPearl system automatically quiesces the tape partition and prevents the tape cartridge being marked "Lost".

Disk Partitions

Disk partitions are comprised of storage pools on external SAS expansion nodes. There are two types of disk partitions. **Online** disk partitions are created on Spectra 44-bay expansion nodes, while **Nearline** disk partitions are created on Spectra 96-bay expansion nodes. 107-bay expansion nodes provide either **Online** or **Nearline** storage, depending on the type of drives installed.

 Online—Online storage using 44-bay expansion nodes is used as a temporary, highperformance storage target for highly transactional data. Nearline—Nearline storage using 96-bay expansion nodes is a cost effective storage target for deep storage. Nearline storage is not recommended for frequent reads or writes.

Nearline storage pools on the 96-bay expansion node are automatically created by the BlackPearl system when the system detects a sufficient number of disks for a new storage pool, and there is a capacity key installed on the system to license the additional storage space. Online storage pools are manually created using the BlackPearl user interface after you attach a 44-bay expansion node, or a 107-bay expansion node with SAS drives (see Create an Online Disk Pool on page 111).

Once storage pools are created, you must manually add them to disk partitions. For information on creating a disk partition, see Create a Disk Partition on page 113.

SPECIAL CONSIDERATIONS FOR EJECTING TAPES

If you plan to eject tapes, Spectra Logic recommends the following storage domain and data policy settings:

- Set the Write Optimization setting to **Capacity** when configuring a storage domain so that data is written to as few tapes as possible.
- Enable Bucket Isolation when configuring a data policy. This setting configures the bucket
 to have its own unique set of tapes. This ensures that tape media containing one bucket of
 information is not mixed with another bucket, making it easier to eject a bucket.

SPECIAL CONSIDERATIONS FOR READING TAPES IN A NON-BLACKPEARL ENVIRONMENT

The BlackPearl system stores data on LTO-5 or later generation Ultrium, or TS11xx technology tape media using the LTFS format. If you plan to eject tapes and read them in a non-BlackPearl system, you must follow the guidelines for Special Considerations for Ejecting Tapes on page 80 as well as the guidelines below when configuring your storage domains and data policies.

- The LTFS file name option should be set to **Object Name** when configuring a storage domain. This setting configures LTFS file names to use the format {bucket name}/{object name}, for example bucket1/video1.mov. If the tapes are ejected from the BlackPearl system and loaded into a non-BlackPearl system, the file names match the object names. If you do not configure this option, object names are assigned a UUID string, which is not human readable, but can be translated back to the actual file name using an external conversion tool.
- Object names must comply with LTFS file naming rules:

- The colon character (:) is not allowed in LTFS file names and therefore not allowed in BlackPearl object names. The slash character (/) is also technically not allowed in LTFS file names; however, the BlackPearl software can accommodate a slash in the object name and translates it as a directory in the LTFS file system (for example, directory1/directory2/video1.mov).
- Directory names have a limit of 255 characters.
- File names have a variable character limit. If you are using English ASCII characters, the limit is 1024 characters. If you are using a graphical language, such as Japanese, the limit is 512 characters.
- Spectra Logic does not recommend the following characters in LTFS file names or BlackPearl object names for reasons of cross-platform compatibility: control characters such as carriage return (CR) and line feed (LF), double quotation mark ("), asterisk (*), question mark (?), less than sign (<), greater than sign (>), backslash (\), forward slash (/) vertical line (|).
- **Blobbing Enabled** should be cleared when configuring a data policy. Blobbing allows an object larger than 1 TB to be broken into multiple blobs and then stored on multiple tapes. Tapes created with blobbing disabled are always readable by a non-BlackPearl system; tapes created with blobbing enabled may not be readable by a non-BlackPearl system when very large objects span across multiple tapes. With blobbing disabled, all files must have a size of 1 TB or less.
- The **Keep Latest** setting cannot be used for a data policy which uses a storage domain configured with the **LTFS File Name** option set to **Object Name**.

EXAMPLE CONFIGURATIONS

Below are explanations of the preconfigured data policies on the BlackPearl system, which include data persistence rules and storage domain targets.

Note: For information on additional data policy settings that are not available through the BlackPearl user interface, see the *Spectra BlackPearl Spectra S3 API Reference*.

Single Copy on Tape

This data policy is the most basic of the preconfigured data policies on the system. This policy creates a single copy of each object sent to the system on tape media. Once data is written on tape, it is removed from the BlackPearl cache if the system detects that more cache space is needed for incoming data.

Note: This data policy is automatically created when the system detects a tape partition.

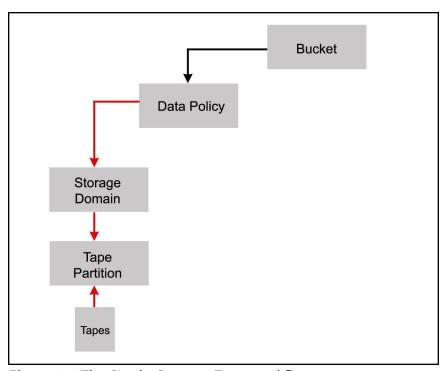


Figure 26 The Single Copy on Tape workflow.

The single copy on tape data policy is configured with the following attributes:

Parameter	Value	Description
Storage Domain - Tape First Copy - Data is written to the primary tape storage domain. This domain is created automatically when the system detects the first partition created on the tape library.		
Days to wait before verifying data	null	Data integrity verification is not performed automatically.
Secure Media Allocation	cleared	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.
Write Optimization	Capacity	Job chunks are written across as few pieces of media as possible. Fewer tape drives are used, so performance is lower.
LTFS File Naming	Object ID	File names use the format {bucket name}/{object id}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.
Media Ejection Allowed	cleared	Media ejection is not allowed.
Storage Domain and detected by t		Copy - The first tape partition created on the tape library
Таре Туре	varies	The tape type matching the latest generation of tape drive in the partition.
Write Preference	Normal	The system uses the partition after partitions with High write preference and before a partition with Low or Never Select write preference.
Auto Compaction Threshold	20	The percentage of a tape with deleted objects at which auto compaction is triggered. The default is 95. The minimum is 10.
Data Policy - Single Copy on Tape		
Blobbing Enabled	selected	Allows an object to be broken into multiple blobs.
Minimize Spanning	cleared	Jobs larger than 1 TB are allowed to span across multiple tapes or pools as needed to maximize capacity utilization and performance.

Parameter	Value	Description
Default GET Job Priority	High	When the storage domain receives a GET job, it is processed with high priority, which is before low and normal priority jobs. Jobs of different types are put in order based on priority. Note: When using a Spectra S3 client, this setting can be overridden when sending a GET job by specifying a different priority in the Get Job command. See the Spectra BlackPearl Spectra S3 API Reference for more information.
Default PUT Job Priority	Normal	When the storage domain receives a PUT job, it is processed with normal priority, which is after high priority jobs but before low and normal priority jobs. Jobs of different types are put in order based on priority. Note: When using a Spectra S3 client, this setting can be overridden when sending a PUT job by specifying a different priority in the Put Job command. See the Spectra BlackPearl Spectra S3 API Reference for more information.
Default VERIFY Job Priority	Low	When the storage domain receives a VERIFY job, it is processed with low priority, which is the lowest setting. Note: When using a Spectra S3 client, this setting can be overridden when sending a VERIFY job by specifying a different priority in the Create Verify Job command. See the <i>Spectra BlackPearl Spectra S3 API Reference</i> for more information.
Default Verify After Write	cleared	Data is not verified after a write.
Rebuild Priority	Low	If data is lost from tape media, the data is rebuilt using low priority, which is the lowest setting.
Checksum Type	MD5	Data using this storage domain is CRC checked using the MD5 checksum type. Data is CRC checked when it is written to cache with a PUT job, or read back from tape media with a GET job.
End-to-end CRC	No	This data policy does not use end-to-end CRC checking.
Versioning	None	In order to upload a new version of an object already PUT to the system, the first version must be deleted.

Parameter	Value	Description
Always Accept Replicated PUT Jobs	cleared	PUT jobs created for this data policy fail if one or more replication targets the system must PUT to are unavailable.
Data Persistence	Rule for Tape First Co	ру
Туре	Permanent	Data is moved to tape and maintained on tape media until data is deleted from a bucket. Note: When data is deleted from a bucket, it is removed from tape media, but individual tape media cartridges are not reclaimed for use until all data is deleted from a tape cartridge.
Bucket Isolation Level	Standard	Data from different buckets can be mixed on to the same piece of media.

Dual Copy on Tape

This data policy persists two copies of data for each PUT job the policy receives. Both copies of data are moved to tape media. This data policy provides enhanced data security in the case of disaster recovery, and is useful if you want to eject one copy of tape media for storage off site.

Note: This data policy is created automatically when the system detects the first and second tape partitions created on the tape library.

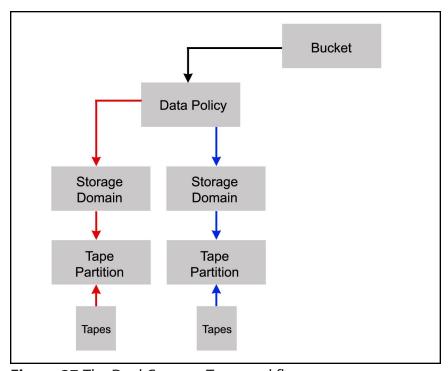


Figure 27 The Dual Copy on Tape workflow.

The dual copy on tape data policy is configured with the following attributes:

Parameter	Value	Description	
Storage Domain - Tape First Copy - Data is written to the primary tape storage domain. This domain is created automatically when the system detects the first tape partition created on the tape library.			
Days to wait before verifying data	null	Data integrity verification is not performed automatically.	
Secure Media Allocation	cleared	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.	
Write Optimization	Capacity	Job chunks are written across as few pieces of media as possible. Fewer tape drives are used, so performance is lower.	
LTFS File Naming	Object ID	File names use the format {bucket name}/{object id}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.	
Media Ejection Allowed	cleared	Media ejection is not allowed.	
Storage Domain Me	Storage Domain Member for Tape First Copy		
Таре Туре	varies	The tape type matching the latest generation of tape drive in the partition.	
Auto Compaction Threshold	20	The percentage of a tape with deleted objects at which auto compaction is triggered. The default is 95. The minimum is 10.	
Write Preference	Normal	The system uses the partition after partitions with High write preference and before a partition with Low or Never Select write preference.	
Storage Domain - Tape Second Copy - A second copy of the data is written to a tape storage domain optimized for tape ejection. This domain is created automatically when the system detects a tape partition created on the tape library.			
Days to wait before verifying data	null	Data integrity verification is not performed automatically.	

Parameter	Value	Description
Secure Media Allocation	cleared	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.
Write Optimization	Capacity	Job chunks are written across as few pieces of media as possible. Fewer tape drives are used, so performance is lower.
LTFS File Naming	Object ID	File names use the format {bucket name}/{object id}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.
Media Ejection Allowed	selected	Media ejection is allowed.
Auto Eject on Job Completion	cleared	Media is not auto ejected upon job completion.
Auto Eject on Job Cancel	cleared	Media is not auto ejected upon job cancellation.
Auto Eject on Media Full	cleared	Media is not auto ejected upon media full.
Scheduled Auto Eject	cleared	Media is not auto ejected on a schedule.
Таре Туре	varies	The tape type matching the latest generation of tape drive in the partition.
Write Preference	Normal	The system uses the partition after partitions with High write preference and before a partition with Low or Never Select write preference.
Data Policy - Dual Copy on Tape		
Blobbing Enabled	selected	Allows an object to be broken into multiple blobs.
Minimize Spanning	cleared	Jobs larger than 1 TB are allowed to span across multiple tapes or pools as needed to maximize capacity utilization and performance.

Parameter	Value	Description
Default GET Job Priority	High	When the storage domain receives a GET job, it is processed with high priority, which is before low and normal priority jobs. Jobs of different types are put in order based on priority. Note: When using a Spectra S3 client, this setting can be overridden when sending a GET job by specifying a different priority in the Get Job command. See the Spectra BlackPearl Spectra S3 API Reference for more information.
Default PUT Job Priority	Normal	When the storage domain receives a PUT job, it is processed with normal priority, which is after high priority jobs but before low and normal priority jobs. Jobs of different types are put in order based on priority. Note: When using a Spectra S3 client, this setting can be overridden when sending a PUT job by specifying a different priority in the Put Job command. See the Spectra BlackPearl Spectra S3 API Reference for more information.
Default VERIFY Job Priority	Low	When the storage domain receives a VERIFY job, it is processed with low priority, which is the lowest setting. Note: When using a Spectra S3 client, this setting can be overridden when sending a VERIFY job by specifying a different priority in the Create Verify Job command. See the Spectra BlackPearl Spectra S3 API Reference for more information.
Default Verify After Write	cleared	Data is not verified after a write.
Rebuild Priority	Low	If data is lost from tape media, the data is rebuilt using low priority, which is the lowest setting.
Checksum Type	MD5	Data using this storage domain is CRC checked using the MD5 checksum type. Data is CRC checked when it is written to cache with a PUT job, or read back from media with a GET job.
End-to-end CRC	No	This data policy does not use end-to-end CRC checking.

Parameter	Value	Description
Versioning	None	In order to upload a new version of an object already PUT to the system, the first version must be deleted.
Always Accept Replicated PUT Jobs	cleared	PUT jobs created for this data policy fail if one or more replication targets the system must PUT to are unavailable.
Data Persistence Ru	le for Tape First Copy	
Туре	Permanent	Data is moved to tape and maintained on tape media until data is deleted from a bucket. Note: When data is deleted from a bucket, it is removed from tape media, but individual tape media cartridges are not reclaimed for use until all data is deleted from a tape cartridge.
Bucket Isolation Level	Standard	Data from different buckets can be mixed on to the same piece of media.
Data Persistence Ru	le for Tape Second Co	ру
Туре	Permanent	Data is moved to tape and maintained on tape media until data is deleted from a bucket. Note: When data is deleted from a bucket, it is removed from tape media, but individual tape media cartridges are not reclaimed for use until all data is deleted from a tape cartridge.
Bucket Isolation Level	Standard	Data from different buckets can be mixed on to the same piece of media.

Single Copy on Nearline Disk

This data policy persists a single copy of each job sent to the system on to nearline disk, which is provided by 96-bay expansion nodes. Once data is written on nearline disk, it is removed from the BlackPearl cache if the system detects that more cache space is needed for incoming data.

Note: This data policy is automatically created when the system detects a nearline disk partition.

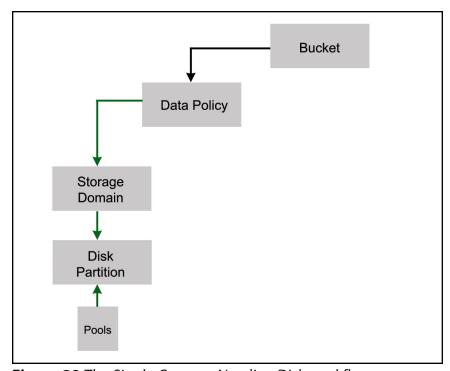


Figure 28 The Single Copy on Nearline Disk workflow.

The single copy on nearline disk data policy is configured with the following attributes:

Parameter	Value	Description
Storage Domain - Pool First Copy - Data is written to the primary nearline storage domain. This domain is created automatically after you create a nearline disk partition.		
Days to wait before verifying data	null	Data integrity verification is not performed automatically.
Secure Media Allocation	cleared	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.
Write Optimization	Capacity	Job chunks are written across as few pools as possible.
LTFS File Naming	Object ID	File names use the format {bucket name}/{object id}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.
Media Ejection Allowed	selected	Media ejection is allowed.
Auto Eject on Job Completion	cleared	Media is not auto ejected upon job completion.
Auto Eject on Job Cancel	cleared	Media is not auto ejected upon job cancellation.
Auto Eject on Media Full	cleared	Media is not auto ejected upon media full.
Scheduled Auto Eject	cleared	Media is not auto ejected on a schedule.
Storage Domain Me	mber for Pool First Co	py - The first nearline disk partition created.
Write Preference	Normal	The system uses the partition after partitions with High write preference and before a partition with Low or Never Select write preference.
Data Policy - Single Copy on Nearline Disk		
Blobbing Enabled	selected	Allows an object to be broken into multiple blobs.

Parameter	Value	Description
Minimize Spanning	cleared	Jobs larger than 1 TB are allowed to span across multiple tapes or pools as needed to maximize capacity utilization and performance.
Default GET Job Priority	High	When the storage domain receives a GET job, it is processed with high priority, which is before low and normal priority jobs. Jobs of different types are put in order based on priority. Note: When using a Spectra S3 client, this setting can be overridden when sending a GET job by specifying a different priority in the Get Job command. See the Spectra BlackPearl Spectra S3 API Reference for more information.
Default PUT Job Priority	Normal	When the storage domain receives a PUT job, it is processed with normal priority, which is after high priority jobs but before low and normal priority jobs. Jobs of different types are put in order based on priority. Note: When using a Spectra S3 client, this setting can be overridden when sending a PUT job by specifying a different priority in the Put Job command. See the Spectra BlackPearl Spectra S3 API Reference for more information.
Default VERIFY Job Priority	Low	When the storage domain receives a VERIFY job, it is processed with low priority, which is the lowest setting. Note: When using a Spectra S3 client, this setting can be overridden when sending a VERIFY job by specifying a different priority in the Create Verify Job command. See the Spectra BlackPearl Spectra S3 API Reference for more information.
Default Verify After Write	cleared	Data is not verified after a write.
Rebuild Priority	Low	If data is lost from disk, the data is rebuilt using low priority, which is the lowest setting.
Checksum Type	MD5	Data using this storage domain is CRC checked using the MD5 checksum type. Data is CRC checked when it is written to cache with a PUT job, or read back from media with a GET job.

Parameter	Value	Description	
End-to-end CRC	No	This data policy does not use end-to-end CRC checking.	
Versioning	None	In order to upload a new version of an object already PUT to the system, the first version must be deleted.	
Always Accept Replicated PUT Jobs	cleared	PUT jobs created for this data policy fail if one or more replication targets the system must PUT to are unavailable.	
Туре	Permanent	Data is moved to nearline disk and maintained on nearline disk until data is deleted from a bucket.	
Bucket Isolation Level	Standard	Data from different buckets can be mixed on to the same piece of media.	
Data Persistence Rul	Data Persistence Rule for Pool First Copy		
Туре	Permanent	Data is moved to disk and maintained on disk media until data is deleted from a bucket.	
Isolation Level	Standard	Data from different buckets can be mixed on to the same piece of media.	

Single Copy on Nearline Disk and Tape

This data policy persists a single copy of each job sent to the system on to both nearline disk and tape media. Once data is written on both disk and tape, it is removed from the BlackPearl cache if the system detects that more cache space is needed for incoming data.

Note: This data policy is automatically created when the system detects a disk partition and a tape partition.

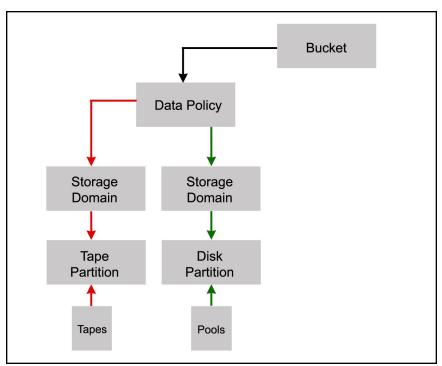


Figure 29 The Single Copy on Nearline Disk and Tape workflow.

The single copy on nearline disk and tape data policy is configured with the following attributes:

Parameter	Value	Description
Storage Domain - Tape First Copy - Data is written to the primary tape storage domain. This domain is created automatically when the system detects the first tape partition created on the tape library.		
Days to wait before verifying data	null	Data integrity verification is not performed automatically.
Secure Media Allocation	cleared	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.
Write Optimization	Capacity	Job chunks are written across as few pieces of media as possible. Fewer tape drives are used, so performance is lower.
LTFS File Naming	Object ID	File names use the format {bucket name}/{object id}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.
Media Ejection Allowed	cleared	Media ejection is not allowed.
Storage Domain Member for Tape First Copy		
Таре Туре	varies	The tape type matching the latest generation of tape drive in the partition.
Auto Compaction Threshold	20	The percentage of a tape with deleted objects at which auto compaction is triggered. The default is 95. The minimum is 10.
Write Preference	Normal	The system uses the partition after partitions with High write preference and before a partition with Low or Never Select write preference.
Storage Domain - Pool First Copy- Data is written to the primary nearline storage domain. This domain is created automatically after you create a nearline disk partition.		
Days to wait before verifying data	null	Data integrity verification is not performed automatically.

Parameter	Value	Description	
Secure Media Allocation	cleared	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.	
Write Optimization	Capacity	Job chunks are written across as few pools as possible.	
LTFS File Naming	Object ID	File names use the format {bucket name}/{object id}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.	
Media Ejection Allowed	selected	Media ejection is allowed.	
Auto Eject on Job Completion	cleared	Media is not auto ejected upon job completion.	
Auto Eject on Job Cancel	cleared	Media is not auto ejected upon job cancellation.	
Auto Eject on Media Full	cleared	Media is not auto ejected upon media full.	
Scheduled Auto Eject	cleared	Media is not auto ejected on a schedule.	
Storage Domain Member for Pool First Copy - The first nearline disk partition created.			
Write Preference	Normal	The system uses the partition after partitions with High write preference and before a partition with Low or Never Select write preference.	
Data Policy - Single Copy on Nearline Disk and Tape			
Blobbing Enabled	selected	Allows an object to be broken into multiple blobs.	
Minimize Spanning	cleared	Jobs larger than 1 TB are allowed to span across multiple tapes or pools as needed to maximize capacity utilization and performance.	

Parameter	Value	Description	
Default GET Job Priority	High	When the storage domain receives a GET job, it is processed with high priority, which is before low and normal priority jobs. Jobs of different types are put in order based on priority. Note: When using a Spectra S3 client, this setting can be overridden when sending a GET job by specifying a different priority in the Get Job command. See the Spectra BlackPearl Spectra S3 API Reference for more information.	
Default PUT Job Priority	Normal	When the storage domain receives a PUT job, it is processed with normal priority, which is after high priority jobs but before low and normal priority jobs. Jobs of different types are put in order based on priority. Note: When using a Spectra S3 client, this setting can be overridden when sending a PUT job by specifying a different priority in the Put Job command. See the Spectra BlackPearl Spectra S3 API Reference for more information.	
Default VERIFY Job Priority	Low	When the storage domain receives a VERIFY job, it is processed with low priority, which is the lowest setting. Note: When using a Spectra S3 client, this setting can be overridden when sending a VERIFY job by specifying a different priority in the Create Verify Job command. See the Spectra BlackPearl Spectra S3 API Reference for more information.	
Default Verify After Write	cleared	Data is not verified after a write.	
Rebuild Priority	Low	If data is lost from tape media, the data is rebuilt using low priority, which is the lowest setting.	
Checksum Type	MD5	Data using this storage domain is CRC checked using the MD5 checksum type. Data is CRC checked when it is written to cache with a PUT job, or read back from media with a GET job.	
End-to-end CRC	No	This data policy does not use end-to-end CRC checking.	

Parameter	Value	Description	
Versioning	None	In order to upload a new version of an object already PUT to the system, the first version must be deleted.	
Always Accept Replicated PUT Jobs	cleared	PUT jobs created for this data policy fail if one or more replication targets the system must PUT to are unavailable.	
Data Persistence Rule for Tape First Copy			
Туре	Permanent	Data is moved to tape and maintained on tape media until data is deleted from a bucket. Note: When data is deleted from a bucket, it is removed from tape media, but individual tape media cartridges are not reclaimed for use until all data is deleted from a tape cartridge.	
Bucket Isolation Level	Standard	Data from different buckets can be mixed on to the same piece of media.	
Data Persistence Rule for Pool First Copy			
Туре	Permanent	Data is moved to disk and maintained on disk media until data is deleted from a bucket.	
Isolation Level	Standard	Data from different buckets can be mixed on to the same media.	

Single Copy on Nearline Disk and Dual Copy on Tape

This data policy persists a single copy of each job sent to the system on to nearline disk and two copies of the job on to tape media. Once data is written on both disk and tape, it is removed from the BlackPearl cache if the system detects that more cache space is needed for incoming data.

Note: This data policy is automatically created when the system detects a disk partition and two tape partitions.

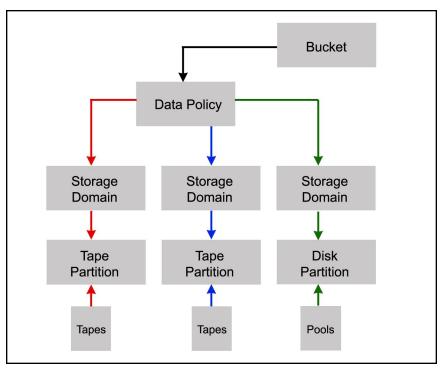


Figure 30 The Single Copy on Nearline Disk and Dual Copy on Tape workflow.

The single copy on nearline disk and dual copy on tape data policy is configured with the following attributes:

Parameter	Value	Description	
Storage Domain - Tape First Copy - Data is written to the primary tape storage domain. This domain is created automatically when the system detects the first tape partition created on the tape library.			
Days to wait before verifying data	null	Data integrity verification is not performed automatically.	
Secure Media Allocation	cleared	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.	
Write Optimization	Capacity	Job chunks are written across as few pieces of media as possible. Fewer tape drives are used, so performance is lower.	
LTFS File Naming	Object ID	File names use the format {bucket name}/{object id}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.	
Media Ejection Allowed	cleared	Media ejection is not allowed.	
Storage Domain Member for Tape First Copy			
Таре Туре	varies	The tape type matching the latest generation of tape drive in the partition.	
Write Preference	Normal	The system uses the partition after partitions with High write preference and before a partition with Low or Never Select write preference.	
Storage Domain - Tape Second Copy - A second copy of the data is written to a tape storage domain optimized for tape ejection. This domain is created automatically when the system detects a tape partition created on the tape library.			
Days to wait before verifying data	null	Data integrity verification is not performed automatically.	
Secure Media Allocation	cleared	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.	

Parameter	Value	Description	
Write Optimization	Capacity	Job chunks are written across as few pieces of media as possible. Fewer tape drives are used, so performance is lower.	
LTFS File Naming	Object ID	File names use the format {bucket name}/{object id}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.	
Media Ejection Allowed	selected	Media ejection is allowed.	
Auto Eject on Job Completion	cleared	Media is not auto ejected upon job completion.	
Auto Eject on Job Cancel	cleared	Media is not auto ejected upon job cancellation.	
Auto Eject on Media Full	cleared	Media is not auto ejected upon media full.	
Scheduled Auto Eject	cleared	Media is not auto ejected on a schedule.	
Storage Domain Member for Tape Second Copy			
Таре Туре	varies	The tape type matching the latest generation of tape drive in the partition.	
Auto Compaction Threshold	20	The percentage of a tape with deleted objects at which auto compaction is triggered. The default is 95. The minimum is 10.	
Write Preference	Normal	The system uses the partition after partitions with High write preference and before a partition with Low or Never Select write preference.	
Storage Domain - Pool First Copy- Data is written to the primary nearline storage domain. This domain is created automatically after you create a nearline disk partition.			
Days to wait before verifying data	null	Data integrity verification is not performed automatically.	
Secure Media Allocation	cleared	Media allocated to the storage domain may be reused by another storage domain if all data is deleted.	

Parameter	Value	Description		
Write Optimization	Capacity	Job chunks are written across as few pools as possible.		
LTFS File Naming	Object ID	File names use the format {bucket name}/{object id}, for example, bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82.		
Media Ejection Allowed	selected	Media ejection is allowed.		
Auto Eject on Job Completion	cleared	Media is not auto ejected upon job completion.		
Auto Eject on Job Cancel	cleared	Media is not auto ejected upon job cancellation.		
Auto Eject on Media Full	cleared	Media is not auto ejected upon media full.		
Scheduled Auto Eject	cleared	Media is not auto ejected on a schedule.		
Storage Domain Me	Storage Domain Member for Pool First Copy - The first nearline disk partition created.			
Write Preference	Normal	The system uses the partition after partitions with High write preference and before a partition with Low or Never Select write preference.		
Data Policy - Single	Copy on Nearline Disk	c and Dual Copy on Tape		
Blobbing Enabled	selected	Allows an object to be broken into multiple blobs.		
Minimize Spanning	cleared	Jobs larger than 1 TB are allowed to span across multiple tapes or pools as needed to maximize capacity utilization and performance.		
Default GET Job Priority	High	When the storage domain receives a GET job, it is processed with high priority, which is before low and normal priority jobs. Jobs of different types are put in order based on priority. Note: When using a Spectra S3 client, this setting can be overridden when sending a GET job by specifying a different priority in the Get Job command. See the Spectra BlackPearl Spectra S3 API Reference for more information.		

Parameter	Value	Description	
Default PUT Job Priority	Normal	When the storage domain receives a PUT job, it is processed with normal priority, which is after high priority jobs but before low and normal priority jobs. Jobs of different types are put in order based on priority. Note: When using a Spectra S3 client, this setting can be overridden when sending a PUT job by specifying a different priority in the Put Job command. See the Spectra BlackPearl Spectra S3 API Reference for more information.	
Default VERIFY Job Priority	Low	When the storage domain receives a VERIFY job, it is processed with low priority, which is the lowest setting. Note: When using a Spectra S3 client, this setting can be overridden when sending a VERIFY job by specifying a different priority in the Create Verify Job command. See the Spectra BlackPearl Spectra S3 API Reference for more information.	
Default Verify After Write	cleared	Data is not verified after a write.	
Rebuild Priority	Low	If data is lost from tape media, the data is rebuilt using low priority, which is the lowest setting.	
Checksum Type	MD5	Data using this storage domain is CRC checked using the MD5 checksum type. Data is CRC checked when it is written to cache with a PUT job, or read back from media with a GET job.	
End-to-end CRC	No	This data policy does not use end-to-end CRC checking.	
Versioning	None	In order to upload a new version of an object already PUT to the system, the first version must be deleted.	
Always Accept Replicated PUT Jobs	cleared	PUT jobs created for this data policy fail if one or more replication targets the system must PUT to are unavailable.	
Data Persistence Rule for Tape First Copy			

Parameter	Value	Description	
Туре	Permanent	Data is moved to tape and maintained on tape media until data is deleted from a bucket. Note: When data is deleted from a bucket, it is removed from tape media, but individual tape media cartridges are not reclaimed for use until all data is deleted from a tape cartridge.	
Bucket Isolation Level	Standard	Data from different buckets can be mixed on to the same piece of media.	
Data Persistence Rule for Tape Second Copy			
Туре	Permanent	Data is moved to tape and maintained on tape media until data is deleted from a bucket. Note: When data is deleted from a bucket, it is removed from tape media, but individual tape media cartridges are not reclaimed for use until all data is deleted from a tape cartridge.	
Bucket Isolation Level	Standard	Data from different buckets can be mixed on to the same piece of media.	
Data Persistence Rule for Pool First Copy			
Туре	Permanent	Data is moved to disk and maintained on disk media until data is deleted from a bucket.	
Isolation Level	Standard	Data from different buckets can be mixed on to the same media.	

Chapter 4 - Configuring Advanced Bucket Management

This chapter provides instructions on how to configure Advanced Bucket Management features.



It is difficult and time consuming to change a data policy once the system writes data to a bucket using the data policy. Make sure that you understand **IMPORTANT** the concepts in Understanding Spectra Advanced Bucket Management Concepts on page 72 and have thoughtfully planned your data policies before you start using the BlackPearl system to store data.

Topic	
Create a Storage Pool	page 107
Create a Nearline Disk Pool	page 107
Create an Online Disk Pool	page 111
Create a Disk Partition	page 113
Create a Tape Partition	page 114
Create a Replication Target	page 115
Create a BlackPearl Target	page 115
Create an Amazon S3 Target	page 118
Create a Microsoft Azure Target	page 122
Create a Storage Domain	page 124
Add a Storage Domain Member to a Storage Domain	page 129
Create a Data Policy	page 131
New Data Policy ACL for a Group	page 135
New Data Policy ACL for a User	page 136
Add Data Persistence Rules and Replication Rules to a Data Policy	page 136
Add a Data Persistence Rule to a Data Policy	page 136
Add a BlackPearl Data Replication Rule to a Data Policy	page 138

Topic	
Add an Amazon S3 Data Replication Rule to a Data Policy	page 140
Add a Microsoft Azure Data Replication Rule to a Data Policy	page 141
Create a Bucket	page 142
Create a New Bucket ACL for a Group	page 144
Create a New Bucket ACL for a User	page 145
Transfer Data	page 146

CREATE A STORAGE POOL

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. There are two types of storage pools; nearline storage, which is provided by a 96-bay expansion node, and online storage, which is provided by a 44-bay expansion node.

Note: Nearline pools created on a 96-bay expansion node have a hard coded capacity utilization limit percentage. On systems running BlackPearl 5.2 or later, this percentage is 95%. On systems running BlackPearl 5.1.x or older, the capacity limit percentage is 87%.

Depending on the drives installed, the 107-bay expansion node is used as either nearline or online storage.

Online and Nearline storage pools use compression. When viewing the details of an online or nearline pool, the user interface displays the physically used space on the pool, not the logically used space.

Once a storage pool is created, it can be added to a disk partition.

If your BlackPearl system does not include disk storage, continue with Create a Tape Partition on page 114.

Create a Nearline Disk Pool

Use the instructions in this section to create a nearline disk pool.

If your BlackPearl system does not include an 96-bay expansion node, or your 107-bay expansion node does not contain SATA drives, continue with Create an Online Disk Pool on page 111.

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

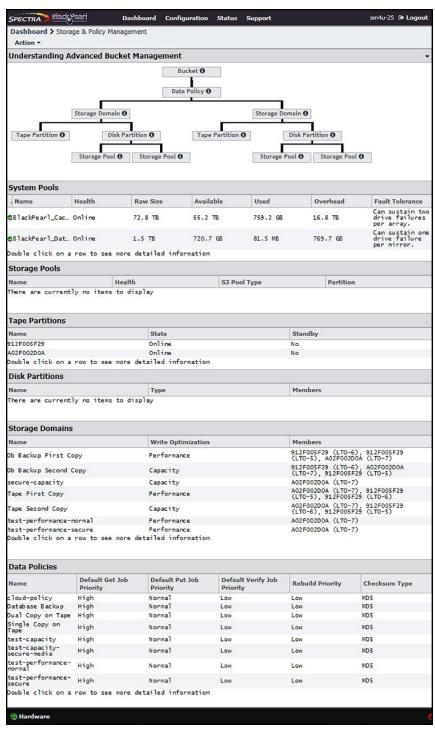


Figure 31 The Advanced Bucket Management screen.

2. Select Action > New Nearline Disk Pool. The New Nearline Disk pool dialog box displays.

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

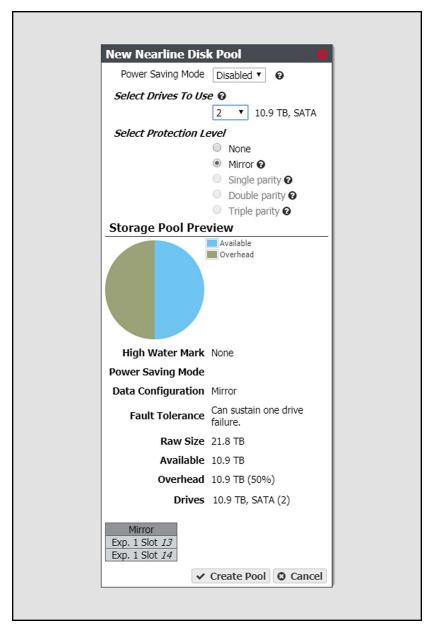


Figure 32 The New Nearline Disk Pool dialog box.

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
Power Saving Mode	Using the drop-down menu, select the desired Power Saving Mode . Enabling the power saving mode sets the standby timer to 60 minutes for all drives in the pool, but only if all drives in the pool are capable of using a standby timer. When the disk pool is idle for 60 minutes, the drives spin-down to conserve power.
Select Drives To Use	Use the drop-down menu to select the number of drives to include in the pool. If your system contains more than one type of disk drive, multiple drop-down menus are present, but only one type can be assigned to a pool. Any drive not in a storage pool acts as a global spare. A global spare drive is activated as soon as a drive configured in a storage pool fails.
Select Protection Level	Use the radio buttons to select the protection level for the pool. Only one option can be selected. Use the Storage Pool Preview information to compare the fault tolerance and required overhead for each configuration. None—The pool is not configured to provide data protection. Any drive failure results in data loss. Mirror—Data is striped across two mirrors. Any detected data corruption is corrected using checksums. This type of RAID offers the best performance for small random reads and writes. Single parity—Data is striped across multiple single-parity arrays, which can tolerate one drive failure without data loss. This type of RAID has faster performance than double- and triple-parity based RAIDs. Double parity—Data is striped across multiple double-parity arrays, which can tolerate two drive failures without data loss. In most cases, double-parity provides the best balance between data protection, performance, and storage capacity. Triple parity—Data is striped across multiple triple-parity arrays, which can tolerate three drive failures without data loss. This type of RAID provides the most data protection.

4. Click **Create Pool**. The new nearline disk pool is listed on the Advanced Bucket Management screen.

Create an Online Disk Pool

If you add a 44-bay or 107-bay expansion node with SAS drives to the BlackPearl system, or otherwise make online disks available for use, use the instructions in this section to create a new online disk pool.

If your BlackPearl system does not include a 44-bay expansion node, or a 107-bay expansion node with SAS drives, continue with Create a Disk Partition on page 113.

Use the instructions in this section to create an online disk pool.

1. From the menu bar, select Configuration > Advanced Bucket Management > Storage & Policy Management to display the Advanced Bucket Management screen (see Figure 31 on page 108).

2. Select Action > New Online Disk Pool. The New Online Disk pool dialog box displays.

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

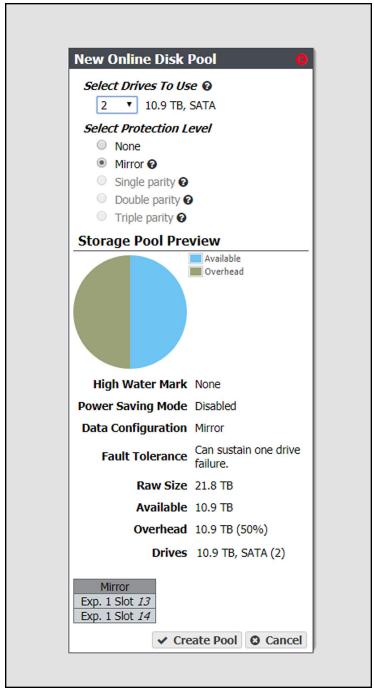


Figure 33 The New Online Disk Pool dialog box.

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
Select Drives To Use	Use the drop-down menu to select the number of drives to include in the pool. If your system contains more than one type of disk drive, multiple drop-down menus are present, but only one type can be assigned to a pool. Any drive not in a storage pool acts as a global spare. A global spare drive is activated as soon as a drive configured in a storage pool fails.
Select Protection Level	Use the radio buttons to select the protection level for the pool. Only one option can be selected. Use the Storage Pool Preview information to compare the fault tolerance and required overhead for each configuration. None—The pool is not configured to provide data protection. Any drive failure results in data loss. Mirror—Data is striped across two mirrors. Any detected data corruption is corrected using checksums. This type of RAID offers the best performance for small random reads and writes. Single parity—Data is striped across multiple single-parity arrays, which can tolerate one drive failure without data loss. This type of RAID has faster performance than double- and triple-parity based RAIDs. Double parity—Data is striped across multiple double-parity arrays, which can tolerate two drive failures without data loss. In most cases, double-parity provides the best balance between data protection, performance, and storage capacity. Triple parity—Data is striped across multiple triple-parity arrays, which can tolerate three drive failures without data loss. This type of RAID provides the most data protection.

4. Click **Create Pool**. The new online disk pool is listed on the Advanced Bucket Management screen.

CREATE A DISK PARTITION

Disk partitions are collections of one or more storage pools, which are configured on either 44-bay, 96-bay, or 107-bay expansion nodes, connected to the BlackPearl system. Disk partitions are specified in storage domains as storage targets.

Use the instructions in this section to create a new disk partition.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management**. The Advanced Bucket Management screen displays (see Figure 31 on page 108).

2. Select **Action > New Disk Partition**. The New Disk Partition dialog box displays.

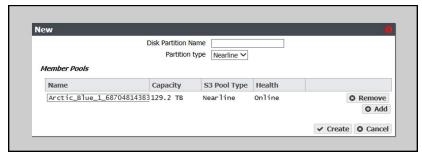


Figure 34 The New Disk Partition dialog box.

- 3. Enter a name for the disk partition in the **Disk Partition Name** field.
- **4.** Use the drop-down menu to select the **Partition type**. You cannot mix different types of storage pools in a disk partition.
 - Select Online to use a storage pool on a 44-bay expansion node, or a 107-bay expansion nodes with SAS drives.
 - Select Nearline to use a storage pool on an 96-bay expansion node, or a 107-bay expansion nodes with SATA drives.
- **5.** Add a storage pool to the disk partition.
 - **a.** In the Member Pools pane, click **Add**. A new row appears in the pane.
 - **b.** Use the **Name** drop down menu to select a storage pool from the list of previously configured storage pools. The Capacity, Type, and Health of the storage pool display.

Note: It may take up to 1 minute after creating an online or nearline storage pool before it displays in the Member Pools list.

- **c.** If desired, repeat Step a and Step b to add additional storage pools to the disk partition.
- **6.** Click **Create**. The new disk partition displays on the Advanced Bucket Management screen.

CREATE A TAPE PARTITION

Use the *Tape Library User Guides* for your Spectra Logic or other supported tape library to create a partition. Once the BlackPearl system detects a partition on a tape library connected to it, the tape partition is automatically listed on the Advanced Bucket Management screen.

If your BlackPearl system does not have a tape library, continue with Create a Replication Target below.

Note: If the BlackPearl system is configured to transfer data to tape, make sure the partitions configured for use by the BlackPearl system do not contain WORM (Write Once-Read Many) media. The BlackPearl system is not compatible with WORM media.

CREATE A REPLICATION TARGET

Replication targets allow you to configure the BlackPearl system to automatically replicate data to another BlackPearl system, or to the Azure or Amazon S3 clouds.

If your BlackPearl system does not include the feature to replicate data to cloud targets, continue with Create a Storage Domain on page 124.

Note: The instructions below describe configuring a target system that is later associated with a data policy. For instructions on creating NAS replication, see Configure the NAS Replication Service on page 242.

Create a BlackPearl Target

Configuring a BlackPearl target allows a data policy on one BlackPearl system to replicate data to a second system. If data is sent to a data policy that is not configured for replication, the data is not replicated to the target system.

With replication enabled, as soon as data is PUT to the cache of the source system it begins replicating to the target system. Storing multiple copies of the same data on different BlackPearl systems provides enhanced data security and disaster recovery if the source system fails. When you delete data from the source system, you can optionally specify to have the data deleted from the target system as well.

Note: If the source BlackPearl system uses object versioning but the target BlackPearl system does not, when an object is deleted on the source system, the delete is replicated to the target system. However, when IOM validates the data on the two systems, it detects that the object still exists on the source system, and self-heals the object on the target system again.



IMPORTANT Spectra Logic recommends using the same versioning settings on both the source and target BlackPearl systems.

Use the instructions in this section to configure a BlackPearl target.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen.

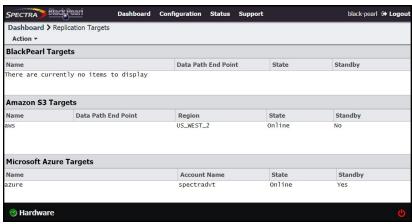


Figure 35 The Replication Targets screen

2. Select Action > New BlackPearl Target. The New BlackPearl Target dialog box displays.

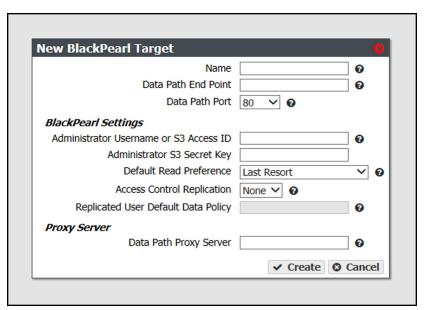


Figure 36 The New BlackPearl Target dialog box.

- **3.** Enter a name for the BlackPearl target in the **Name** field.
- **4.** Enter the system name of the target system, or the IP address of the target system's data port, as the **Data Path End Point**.

Note: Do not use the IP address of the target system's management port.

- **5.** Using the drop-down menu, select a value for the **Data Path Port**. Set this to the value of the port on which the target system's S3 server is running.
 - **Note:** Do not change this setting unless you configured the target system S3 server on a port other than the default.
- **6.** Enter the username or S3 Access ID of a user with administrator privileges on the target system in the **Administrator Username or S3 Access ID** field.
 - **Note:** Administrator credentials are used to configure and maintain the source/target relationship. They are not used for user driven replication operations.
- **7.** In the **Administrator S3 Secret Key** field, enter the S3 Secret Key of the user you entered in Step 6.
- **8.** Using the drop-down menu, select a value for the **Default Read Preference**. Data is normally read from the source system whenever possible. This setting determines from what location data is read back from the target system, if needed.

Name	Description
Last Resort	The source system only reads data from the target system if the source system cannot read from any of its own data partitions.
Minimum Latency	The source system reads the data from the data partition with the least latency no matter whether it is connected to the source system or the target system. For example, if the source system only has the data on tape and the target system has the data on pool, the data is read from the target pool. Note: Only use MINIMUM LATENCY when the network between the source and target is very inexpensive.
After Online Pool	The source system only reads data from the target system if the source system cannot read from an online pool.
After Nearline Pool	The source system only reads data from the target system if the source system cannot read from a nearline pool.
After Non-Ejectable Tape	The source system only reads data from the target system if the source system cannot read from a non-ejectable tape.
Never	Data is never read from the target system

9. Using the drop-down menu, select a value for **Access Control Replication**.

Name	Description
None	No access control information is replicated to the BlackPearl target. Note: The Administrator secret key on both the source and target BlackPearl systems must be identical when setting Access Control Replication to None.
Users	User creation, modification, and deletion is replicated to the BlackPearl target.

- **10.** If you selected Users in Step 9, you can optionally enter the name of a data policy previously configured on the target system to use as the **Replicated User Default Data Policy**. If configured, the system uses this target data policy as the default data policy for any users replicated to the target.
- **11.**Optionally, enter the IP address of the **Data Path Proxy Server**. If configured, the source system uses the specified proxy to connect to the target system.
- **12.** Click **Create**. The new BlackPearl target appears on the Advanced Bucket Management screen.

Create an Amazon S3 Target

Configuring an Amazon S3 target allows a data policy on the BlackPearl system to replicate data to the Amazon S3 cloud. With replication enabled, as soon as data is PUT to the cache of the source system it begins replication to the Amazon S3 cloud.

Note: Only Amazon Web Services (AWS) S3 is qualified as an Amazon S3 target. Other S3 services have not been tested.

Restrictions

The following restrictions apply to creating an Amazon S3 target:

- You cannot create two Amazon S3 targets using the same Data Path End Point and Access Key.
- You cannot create two Amazon S3 targets using the same Region and Access Key when the Data Path End Point has no value.
- You cannot link multiple Amazon S3 targets to the same Data Policy when both targets have no value for the Data Path End Point, and the prefix and suffix are the same for both targets.

Use the instructions in this section to configure an Amazon S3 target.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 35 on page 116).
- **2.** Select **Action > New Amazon S3 Target**. The New Amazon S3 Target dialog box displays.

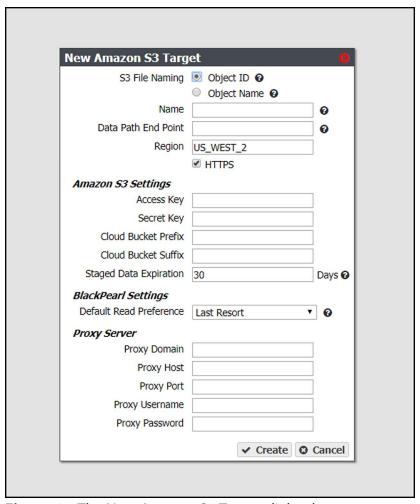


Figure 37 The New Amazon S3 Target dialog box.

- **3.** Select the type of **S3 File Naming** to use for the target.
 - Object ID objects display a UUID when viewed on the Amazon target.
 - Object Name objects display their name when viewed on the Amazon target.
- **4.** Enter a name for the Amazon S3 target in the **Name** field.

5. Enter a **Data Path End Point** (system name or IP address) or a **Region** to identify the remote Amazon S3 target.

Acceptable regions are: Note: Dashes (-) in the standard AWS S3 region code must be replaced by underscores (_) in the text entered in the Region field.		
 us_east_1 us_east_2 us_west_1 us_west_2 eu_west_1 eu_west_2 eu_central_1 	 ap_south_1 ap_southeast_1 ap_southeast_2 ap_northeast_1 ap_northeast_2 	sa_east_1cn_north_1ca_central_1gov_cloud

Notes:

- If you enter both a Data Path End Point and a Region, the system uses the Data Path End Point and ignores the Region.
- You cannot use the same Data Path End Point or Region for multiple Amazon S3 targets.
- **6.** By default, **HTTPS** is selected so that the replication uses a secure connection. If desired, clear **HTTPS** to use HTTP.
- **7.** Enter the S3 Access Key of a user with administrator privileges for the Amazon S3 account in the **Access Key** field.

Note: Administrator credentials are used to configure and maintain the source/target relationship. They are not used for user driven replication operations.

- **8.** In the **Secret Key** field, enter the S3 Secret Key of the user you entered in Step 7.
- 9. Optionally, enter a Cloud Bucket Prefix and/or Cloud Bucket Suffix. Bucket names on the BlackPearl system must be unique within the system, but bucket names in AWS S3 must be unique across the world. To permit friendlier, shorter local bucket names on the BlackPearl system while avoiding naming conflicts with AWS S3, the system adds the defined Cloud Bucket Prefix and Cloud Bucket Suffix to the BlackPearl bucket name when it replicates the bucket. For example, if Cloud Bucket Prefix=prefix, Cloud Bucket Suffix=suffix, and the bucket name=name, the resulting name of the bucket on the Amazon S3 target is prefix-name-suffix.

Note: The prefix and/or suffix must adhere to the replication target naming requirements.

10. Enter a **Staged Data Expiration** time in days using any value between 1 and 365. The default is 30. When data is pre-staged by the S3 service so that the BlackPearl system can retrieve the data in an S3-standard manner, you must specify an expiration period in days. This is the minimum number of days before the pre-staged copy expires. If the system does not retrieve all of the data before the copy expires, it has to pre-stage the data again, incurring additional delays and costs.

Note: Spectra Logic strongly discourages configuring a **Staged Data Expiration** of less than 7 days as any potential cost savings are offset by the possibility of multiple stagings.

11. Using the drop-down menu, select a value for the **Default Read Preference**. Data is normally read from the source system whenever possible. This setting determines when data is read back from the Amazon S3 target, if needed.

Note: Spectra Logic recommends that **Default Read Preference** be kept at the default of **Last Resort**.

Name	Description
Last Resort	The source system only reads data from the target if the source system cannot read from any of its own data partitions.
Minimum Latency	The source system reads the data from the data partition with the least latency no matter whether it is connected to the source system or the target.
After Online Pool	The source system only reads data from the target if the source system cannot read from an online pool.
After Nearline Pool	The source system only reads data from the target if the source system cannot read from a nearline pool.
After Non- Ejectable Tape	The source system only reads data from the target if the source system cannot read from a non-ejectable tape.
Never	Data is never read from the target.

12. Optionally, enter the information for a proxy server:

Field	Description
Proxy Domain	Domain name for the proxy server.
Proxy Host	The host name or IP address for the proxy server through which the system connects.
Proxy Port	The proxy server port through which the system connects.
Proxy Username	The username used when connecting through the proxy server.
Proxy Password	The password used when connecting through the proxy server.

Field	Description
Proxy Domain	Domain name for the proxy server.
Proxy Host	The host name or IP address for the proxy server through which the system connects.
Proxy Port	The proxy server port through which the system connects.
Proxy Username	The username used when connecting through the proxy server.
Proxy Password	The password used when connecting through the proxy server.

13. Click **Create**. The new Amazon S3 target appears on the Replication Targets screen.

Create a Microsoft Azure Target

Configuring a Microsoft Azure target allows a data policy on the BlackPearl system to replicate data to the Microsoft Azure cloud. With replication enabled, as soon as data is PUT to the cache of the source system it begins replication to the Microsoft Azure cloud.

Use the instructions in this section to configure a Microsoft Azure target.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 35 on page 116).

2. Select **Action > New Microsoft Azure Target**. The New Microsoft Azure Target dialog box displays.

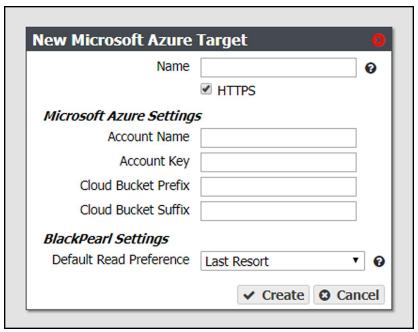


Figure 38 The New Microsoft Azure Target dialog box.

3. Enter a name for the Microsoft Azure target in the **Name** field.

Note: Each Azure target name must be unique. You cannot create two Azure targets with the same name.

- **4.** By default, **HTTPS** is selected so that the replication uses a secure connection. If desired, clear the **HTTPS** check box to use HTTP.
- **5.** Enter the account name for the Microsoft Azure account in the in the **Account Name** field. **Note:** You can not use the same **Account Name** for multiple Microsoft Azure targets.
- **6.** In the **Account Key** field, enter the account key associated with the account entered in Step 5.
- 7. Optionally, enter a Cloud Bucket Prefix and/or Cloud Bucket Suffix. Bucket names on the BlackPearl system must be unique within the system, but bucket names in Microsoft Azure must be unique across the world. To permit friendlier, shorter local bucket names on the BlackPearl system while avoiding naming conflicts with Microsoft Azure, the system adds the defined Cloud Bucket Prefix and Cloud Bucket Suffix to the BlackPearl bucket name when it replicates the bucket. For example, if Cloud Bucket Prefix=prefix, Cloud Bucket Suffix=suffix, and the bucket name=name, the resulting name of the bucket on the Azure target is prefix-name-suffix.

Note: The prefix and/or suffix must adhere to the replication target naming requirements.

8. Using the drop-down menu, select a value for the **Default Read Preference**. Data is normally read from the source system whenever possible. This setting determines when data is read back from the Microsoft Azure target, if needed.

Note: Spectra Logic recommends that **Default Read Preference** be kept at the default of **Last Resort**.

Name	Description
Last Resort	The source system only reads data from the target if the source system cannot read from any of its own data partitions.
Minimum Latency	The source system reads the data from the data partition with the least latency no matter whether it is connected to the source system or the target.
After Online Pool	The source system only reads data from the target if the source system cannot read from an online pool.
After Nearline Pool	The source system only reads data from the target if the source system cannot read from a nearline pool.
After Non- Ejectable Tape	The source system only reads data from the target if the source system cannot read from a non-ejectable tape.
Never	Data is never read from the target.

9. Click **Create**. The new Microsoft Azure target appears on the Replication Targets screen.

CREATE A STORAGE DOMAIN

A storage domain is a named collection of member data partitions and, when applicable, media type combinations. Storage domains define the possible places where the BlackPearl Converged Storage System stores data that is sent to it. Data persistence rules and data policies further define where and for how long to store specific data.

Entire data partition/media type combinations are members of storage domains. When a bucket requires additional capacity, a single disk partition or tape is allocated out of the members to fulfill the capacity requirement.

Use the instructions in this section to create a new storage domain.

From the menu bar, select Configuration > Advanced Bucket Management > Storage & Data Policy Management to display the Advanced Bucket Management screen (see Figure 31 on page 108).

New Storage Domain Name Days to wait before verifying data a ☐ Secure Media Allocation ② Write Optimization Capacity @ O Performance @ LTFS File Naming Object ID @ Object Name @ Media Ejection Allowed Auto Eject on Job Completion Auto Eject on Job Cancel Auto Eject on Media Full Auto Eject Media Full Threshold GB 🗸 Auto Eject Verify Task Priority None Scheduled Auto Eject Hourly Start Time 12:00 AM e.g. 3:00 AM Daily Weekly Every 1 days ✓ Create ② Cancel

2. Select **Action > New Storage Domain**. The New Storage Domain dialog box displays.

Figure 39 The New Storage Domain dialog box.

- 3. Enter a name for the storage domain in the Storage Domain Name field.
- **4.** Enter a value for **Days to wait before verifying data**. The system automatically performs a data integrity verification for all tape media in the storage domain that are unchanged after the specified number of days pass, to ensure the data written to the tape cartridge is still viable. If null, data integrity verification is not performed automatically.

Notes:

- By default, all data on the tape is verified. You can customize the amount of data to be verified in Configure the Spectra S3 Service on page 189.
- When this verification completes, the Last Verified field on the tape details screen is updated.
- While the verification is in progress, client access has priority over the data integrity verification.
- You can also initiate data integrity verification for tape media manually. See
 Data Integrity Verification Tape Media on page 355 for more information.
- Disk pools are not subject to automatic data integrity verification. However, you can initiate data integrity verification for disk pools manually. See Data Integrity Verification Disk Media on page 353 for more information.

5. Select or clear **Secure Media Allocation**. If enabled, Secure Media Allocation ensures that media allocated to the storage domain always remains in the storage domain. Even if all data on the media is deleted, the media will not be reallocated to another storage domain.

Note: Secure Media Allocation should only be enabled when, for compliance purposes, the user must be certain which media ever contained any data for the storage domain (usually, to physically destroy the media once the data is no longer needed), or to force rotating through media when new backups are created and old backups are deleted.

6. Select the **Write Optimization** for the storage domain. This setting specifies whether job chunks are written as quickly as possible or across as few pieces of media as possible.

The BlackPearl system writes to tape drives based on chunks, with default chunk size of approximately 128 GB, or 2% of the tape media capacity. When there is a queue of jobs, the BlackPearl system aggregates smaller jobs or smaller chunks into a size of approximately 128 GB for each tape drive read or write task.

When running in **Capacity** mode, the BlackPearl system uses as few tape cartridges or disk pools as possible. The system only allocates a new tape cartridge or disk pool when capacity is needed.

When running in **Performance** mode, the BlackPearl system spreads the chunks or aggregations across all available tape drives, or disk pools. The number of tape drives used can be limited by using tape drive reservations.

The consequence of using performance mode with tape media is that during a restore
or GET job, more tape drives and tapes cartridges are required to restore a data set
that was initially spread across many tapes. This can drastically reduce overall
performance during restores, as the system takes longer to get access to the full data
set.

Note: Only use performance mode at the direction of Spectra Logic.

For more information on capacity and performance modes, see Capacity Mode versus Performance Mode on page 380.

Note: If the storage domain is assigned to a data policy and "Minimize Spanning" is enabled for the data policy, it overrides the capacity mode and performance mode logic for a given job, up to 1 TB in size. Minimize spanning increases the chunk size to 1 TB, and always keeps one chunk on a single tape regardless of write mode. If the job is larger than 1 TB, then multiple chunks are used and the system uses the logic for capacity mode vs performance mode, where different chunks may transfer to different tapes.

7. Select the LTFS File Name option for the storage domain.

Note: This setting only applies to tape media. If the storage domain includes tape partition(s), you must specify the LTFS File Name option for the storage domain. This option specifies how the system names the file when it writes them to tape.

There are two options for the **LTFS File Name**:

Object Name — LTFS file names use the format {bucket name}/{object name}, for example bucket1/video1.mov. Object names must comply with LTFS file naming rules. If the tapes are ejected from the BlackPearl system and loaded into a non-BlackPearl tape partition, the file names match the object names.

Notes:

- The colon character (:) is not allowed in LTFS file names and therefore not allowed in BlackPearl object names. The slash character (/) is also technically not allowed in LTFS file names; however, the BlackPearl software can accommodate a slash in the object name and translates it as a directory in the LTFS file system (e.g. directory1/directory2/video1.mov).
- Spectra Logic does not recommend the following characters in LTFS file names or BlackPearl object names for reasons of cross-platform compatibility: control characters such as carriage return (CR) and line feed (LF), double quotation mark ("), asterisk (*), question mark (?), less than sign (<), greater than sign (>), backslash (\), forward slash (/) vertical line (|).
- **Object ID** LTFS file names use the format {bucket name}/{object id}, for example bucket1/1fc6f09c-dd72-41ea-8043-0491ab8a6d82. Object names do not need to comply with LTFS file naming rules. The system saves object names as LTFS extended attributes allowing any third party application to reconstruct all the data including the object names.



If this storage domain is assigned to a data policy that uses versioning, after **IMPORTANT** data is persisted, you cannot change this setting from Object ID to Object Name.

8. Optionally, select the **Media Ejection Allowed** check box to enable media ejection options for the storage domain. Clear the check box to disallow media ejection for the storage domain.

Note: This setting only applies to tape media.

If you select to allow media ejection, configure the following options:

- **a.** Select or clear options for auto media ejection.
 - **Auto Eject on Job Completion** select this option to have the system automatically eject tape(s) when a job completes.
 - **Auto Eject on Job Cancel** select this option to have the system automatically eject tape(s) when a user cancels a job.
 - **Auto Eject on Media Full** select this option to have the system automatically eject tape(s) when a tape is full.

Note: If you select for media to automatically eject when the media is full, you can optionally configure the **Auto Eject Media Full Threshold**, which determines when the system marks a piece of media as full, and queues the piece of media for ejection. Select the desired unit size from the drop-down menu and enter a numerical value for the media full threshold in the text box to the left of the unit size drop-down menu.

- **b.** Using the **Auto Eject Verify Task Priority** drop-down menu, select a task priority for tapes to be verified when they are automatically ejected. Selecting **None** means that the system does not verify tapes before ejecting them.
- **c.** Select or clear the **Scheduled Auto Eject** check box. If enabled, this option automatically ejects all tape media on a set schedule. Use the instructions below to configure either hourly, weekly, or daily automatic tape ejection.

Note: Scheduled Auto Eject operates independently from the condition-based auto eject options discussed in Step a on page 128. For example, if you select to have tape media auto eject when full, the system ejects a tape cartridge when it meets the media full threshold. Additionally, when the scheduled auto eject is met, the system ejects <u>all</u> tape cartridges, regardless of whether they have reached the media full threshold.

Create an Hourly Schedule

- **i.** Select **Hourly** as the interval for the tape ejection schedule (see Figure 39 on page 125).
- **ii.** Enter a number for **Every** _ **hours on the hour**. This value specifies the interval, in hours, between ejecting tapes. For example, if this value is set to 4, the system ejects tapes every four hours.

Create a Daily Schedule

- **i.** Select **Daily** as the interval for the tape ejection schedule (see Figure 39 on page 125).
- **ii.** Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
- **iii.** Enter a number for **Every** _ **days**. This value specifies the interval, in days, between ejecting tapes.

Create a Weekly Schedule

- **i.** Select **Weekly** as the interval for the tape ejection schedule (see Figure 39 on page 125).
- **ii.** Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
- **iii.** Select one or more days for **Every week on:**. This determines the day(s) of each week the system ejects tapes.
- **9.** Click **Create**. The new storage domain displays on the Advanced Bucket Management screen.

Add a Storage Domain Member to a Storage Domain

Once a storage domain is created, you must add storage domain members. Entire data partition/media type combinations are members of storage domains. When a bucket requires additional capacity, a single disk partition or tape cartridge is allocated out of the members to fulfill the capacity requirement.

Use the instructions in this section to add a storage domain member to a storage domain.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).

2. Double-click the storage domain for which you want to add a new storage domain member in the Storage Domains pane, or select the storage domain and select Action > Show Details from the menu bar. The Storage Domain details screen displays.

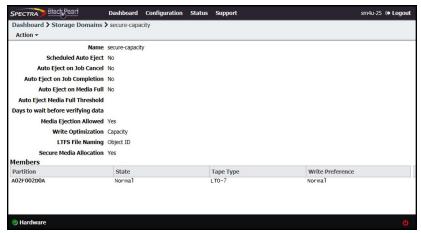


Figure 40 The Storage Domain details screen.

3. Select **Action > New Storage Domain Member**. The New Storage Domain Member dialog box displays.

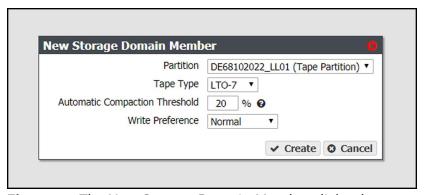


Figure 41 The New Storage Domain Member dialog box.

4. Use the **Partition Name** drop-down menu to select a tape or disk partition from the list of previously created partitions.

Note: You cannot add a disk partition to a storage domain that already uses a tape partition, and you cannot add a tape partition to a storage domain that already uses a disk partition.

5. Use the **Tape Type** drop-down menu to select the media type for a tape partition.

Notes:

- You must select the media type that matches the media present in the tape library partition. If the partition contains multiple generations of media, select the highest version.
- This option does not display if you selected a disk partition in Step 4 on page 130.
- **6.** Enter a percentage for the **Automatic Compaction Threshold**. Automatic compaction occurs when the percentage of deleted objects on a tape cartridge exceeds this value. The default percentage is 95.

Note: If you selected a disk partition in Step 4 on page 130, this setting is unavailable.

- **7.** Use the **Write Preference** drop-down menu to select the write preference for this member of the storage domain. This setting determines the preferred usage of the partition when additional capacity is needed. The system uses a partition with **High** write preference before a partition with **Normal** write preference, and so on. Use **Never Select** to indicate that a partition is read-only.
- **8.** Click **Create**. The new storage domain member displays on the Storage Domain details screen.

CREATE A DATA POLICY

A data policy defines data integrity policies, default job attributes, and persistence and replication rules, which define where data is written and for how long it is kept. A data policy may be used by multiple buckets, but a bucket uses precisely one data policy.

Use the instructions in this section to create a new data policy.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).

2. Select **Action > New Data Policy**. The New Data Policy dialog box displays.

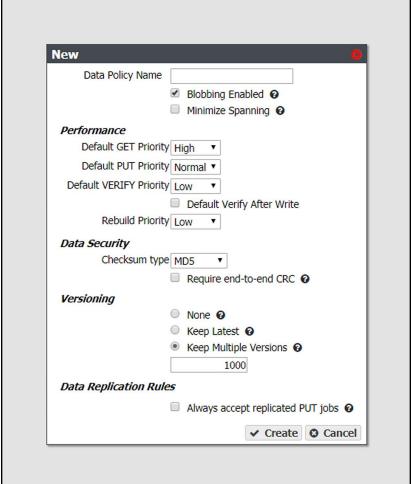


Figure 42 The New Data Policy dialog box.

- 3. Enter a name for the data policy in the **Data Policy Name** field.
- **4.** Select or clear the **Blobbing Enabled** check box. When enabled this setting allows an object to be broken into multiple blobs. If disabled, an object must be exactly one blob. Blobbing must be enabled to handle objects larger than 1 TB, to use multi-part upload, or to break up an object into multiple blobs.

Note: Disabling blobbing guarantees that an object will never span multiple tapes or storage pools, since a blob cannot span multiple media.

5. Select or clear the **Minimize Spanning** check box. When enabled, this setting minimizes the spanning of data across multiple tapes or pools. Jobs less than 1 TB never span media.

Notes:

- When "Minimize Spanning" is enabled, it overrides a storage domain's capacity mode and performance mode logic for a given job, up to 1 TB in size. Minimize spanning increases the chunk size to 1 TB, and always keeps one chunk on a single tape regardless of write mode. If the job is larger than 1 TB, then multiple chunks are used and the system uses the logic for capacity mode vs performance mode, where different chunks may transfer to different tapes.
- Enabling this option can adversely affect capacity utilization and performance.
- **6.** Select the **Performance** characteristics for the data policy. Each priority determines the resources assigned and the processing order. Jobs with priority **Urgent** can use up all of the resources and prevent other jobs from making progress. Use this priority sparingly.
 - **a.** Use the drop-down menu to select the **Default GET Priority**.
 - **b.** Use the drop-down menu to select the **Default PUT Priority**.
 - **c.** Use the drop-down menu to select the **Default VERIFY Priority**.
 - **d.** Select or clear **Default Verify After Write**. Clients may specify whether or not to verify data immediately after writes when creating a PUT job. If the client does not specify a policy for verification of data after writes, this selection determines whether a verify is done. If done, the verification uses the checksum type specified in Step 7 below.

Notes:

- After the PUT job completes, the tape remains in the drive during data verification.
- Only the data just written by the PUT job is verified.
- This verification does not update the **Last Verified** field on the tape details screen.
- Selecting **Default Verify After Write** reduces system write throughput by up to 50%.
- This setting does not apply to replication targets.
- e. Use the drop-down menu to select the Rebuild Priority.

- **7.** Select the **Data Security** options for the data policy.
 - **a.** Use the drop-down menu to select the **Checksum type**. This setting specifies the type of checksum used to verify data integrity for data in any bucket using this data policy, and the type of checksum required for end-to-end CRC, if specified.

Notes:

- CRC, MD5, and SHA-512 perform the best for their corresponding cryptographic strengths on the BlackPearl system.
- Using SHA-256 and SHA-512 reduces single stream performance and may reduce throughput capabilities of the system.
- **b.** If you want to enable end-to-end security for each GET or PUT job, select the **Require** end-to-end CRC check box.
- **8.** Select the type of **Versioning** you want to use for the data policy. You must select either None, Keep Latest, or Keep Multiple Versions.



IMPORTANT If you select **Keep Multiple Versions**, you are not able to change this setting after the data policy is created.

- **None**—Only one version of an object may exist at any time and the version number of the object is always 1.
- **Keep Latest**—Only one version of the data is available at a time. When a new version of an object is written, the old version is retained until the new version is fully written in compliance with the data policy, and then the old version is deleted.
- **Keep Multiple Versions** (*default*)—When a new version of an object is written, it is added as the latest version of the object. Any previous versions of the object, up to the value specified, are retained and accessible. The default value of 1000 is pre-entered.

Notes:

- The **Keep Latest** setting cannot be used for a data policy which uses a storage domain configured with the **LTFS File Name** option set to **Object Name**. See Create a Storage Domain on page 124 for more information.
- The **Keep Latest** setting requires that the PUT job for the earlier version of the object complete before the PUT of the latest version of the object with the same name in order for the PUT job to succeed.



If you select **Keep Multiple Versions**, if the PUT of the earlier version is not complete before the PUT of the latest version, the BlackPearl system believes the latest version to be the same object as the earlier version and rejects it, and only the earlier version is retained.

9. If you plan to configure a data replication target, select or clear the **Always accept replicated PUT jobs** check box. This option controls whether all PUT jobs for this data policy are created even if one or more replication targets the system must PUT to are unavailable, or if there are global issues that would likely prevent the completion of the job.

Note: Using this parameter is discouraged, and using it for jobs on both the source and target systems at the same time is extremely discouraged. Running jobs on both systems when they are not able to communicate with each other can create replication conflicts that must be manually resolved.

10. Click **Create**. The new data policy displays on the Advanced Bucket Management screen.

New Data Policy ACL for a Group

Use the instruction in this section to create a new data policy ACL for a group.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Select the row for the data policy for which you want to create a new ACL for a group, then select **Action > Show Details**. The Data Policy details screen displays.
- **3.** From the menu bar, select **Action > New Data Policy ACL For Group**. The New Data Policy ACL For Group dialog box displays.



Figure 43 The New Data Policy ACL For Group dialog box.

- 4. Using the Name drop-down menu, select the group to be assigned to the data policy ACL.
- 5. Click Create.

New Data Policy ACL for a User

Use the instruction in this section to create a new data policy ACL for an individual user.

- 1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Select the row for the data policy for which you want to create a new ACL for a user, then select **Action > Show Details**. The Data Policy details screen displays.
- **3.** From the menu bar, select **Action > New Data Policy ACL For User**. The New Data Policy ACL For User dialog box displays.



Figure 44 The New Data Policy ACL For User dialog box.

- **4.** Using the **Name** drop-down menu, select the user to be assigned to the data policy ACL.
- 5. Click Create.

Add Data Persistence Rules and Replication Rules to a Data Policy

Once a data policy is created, you must add persistence rules. A persistence rule is either permanent, meaning that data is kept in the specified storage domain at all times, or temporary, meaning that data is kept in the specified storage domain under certain circumstances, and then it can be deleted from that storage domain. Existing permanent and temporary persistence rules, and replication rules, may be retired so that the rule is not applied for any new incoming data, but will continue to retain data previously written. A data policy must include at least one permanent persistence rule.

Add a Data Persistence Rule to a Data Policy

1. If necessary, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).

2. Double-click the data policy in the Data Policies pane, or select the data policy and select **Action > Show Details** from the menu bar. The Data Policy details screen displays.

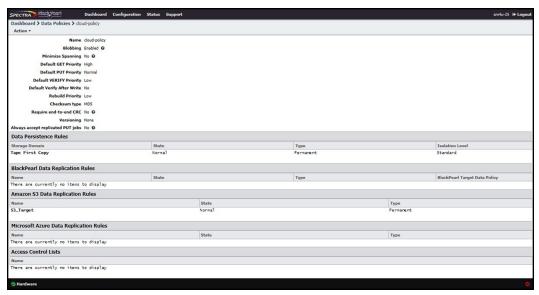


Figure 45 The Data Policy details screen.

3. Select **Action > New Data Persistence Rule**. The New Data Persistence Rule dialog box displays.

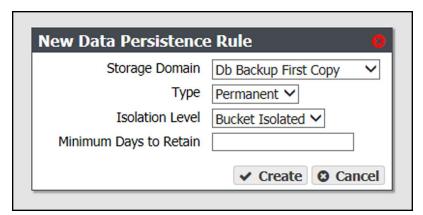


Figure 46 The New Data Persistence Rule dialog box.

4. Use the **Storage Domain** drop-down menu to select a storage domain from the list of previously created storage domains.

5. Use the **Type** drop-down menu to select whether the data persistence rule to use for the for the storage domain is **Temporary**, **Permanent** or **Retired**.

Notes:

- The **Temporary** setting cannot be used for a storage domain that targets a tape library.
- When importing data, a **Temporary** persistence rule does not trigger copying data to a disk pool unless the data is staged with IOM (Intelligent Object Management) active and running. See Intelligent Object Management (IOM) on page 378 for information on IOM.
- **6.** Use the **Isolation Level** drop-down menu to select the level of physical isolation required for the storage domain.
 - Standard This allows data from different buckets to reside on the same physical media, and may provide increased performance. This setting is recommended data policies configured to use disk storage.
 - Bucket Isolated Data from different buckets cannot be mixed on the same physical storage media. This setting is recommended data policies configured to use tape storage.

Notes:

- The **Standard** isolation level provides the best capacity utilization and overall performance.
- Bucket Isolated allocates an entire tape or pool to a bucket when needed.
 Allocating an entire pool to a bucket may use up resources quickly and is not recommended.
- **7.** Enter the **Minimum Days to Retain** in the entry field to specify the minimum number of days the system should retain data written using a temporary persistence rule.
 - **Note:** The **Minimum Days to Retain** for a persistence rule targeting a storage domain using a nearline pool (an 96-bay or 107-bay expansion node) must be 90 days or greater.
- **8.** Click **Create**. The new data persistence rule displays on the Data Policy details screen.

Add a BlackPearl Data Replication Rule to a Data Policy

- 1. If necessary, select Configuration > Advanced Bucket Management > Storage & Data Policy Management to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Double-click the data policy in the Data Policies pane, or select the data policy and select **Action > Show Details** from the menu bar. The Data Policy details screen displays (see Figure 45 on page 137).

3. Select **Action > New BlackPearl Data Replication Rule**. The New BlackPearl Data Replication Rule dialog box displays.

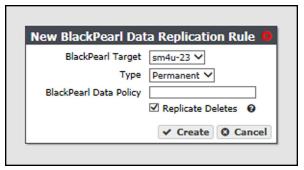


Figure 47 The New BlackPearl Data Replication Rule dialog box.

- **4.** Use the **BlackPearl Target** drop-down menu to select a replication target from the list of previously created replication targets.
- **5.** Use the **Type** drop-down menu to select whether the data persistence rule to use for the for the storage domain is **Permanent** or **Retired**.

Note: You cannot create a replication rule as **Retired**. You can only modify a rule from permanent to retired after the data policy is created.

6. In the **BlackPearl Data Policy** entry field, enter the name of the data policy on the target BlackPearl system to use when creating the bucket for replicated data. Alternatively, you can leave the field blank.

Notes:

- The data policy name is case sensitive.
- If the field is left blank and the BlackPearl target was configured with the setting "Replicated User Default Data Policy" enabled, and Access Control Replication was set to "Users", the default data policy on the target system is used. If no default is set on the target system and the target system is configured with more than one data policy, the replication fails.
- **7.** Select or clear the **Replicate Deletes** check box. When selected, any time a replicated file is deleted from the source system, it is also deleted from the target system.

Note: Replicated objects do not immediately delete. Objects are only deleted after running a verify operation on the bucket.

8. Click **Create**. The new BlackPearl data replication rule displays on the Data Policy details screen.

Add an Amazon S3 Data Replication Rule to a Data Policy

- **1.** If necessary, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Double-click the data policy in the Data Policies pane, or select the data policy and select **Action > Show Details** from the menu bar. The Data Policy details screen displays (see Figure 45 on page 137).
- **3.** Select **Action > New Amazon S3 Data Replication Rule**. The New Amazon S3 Data Persistence Rule dialog box displays.



Figure 48 The New Amazon S3 Data Replication Rule dialog box.

- **4.** Use the **Amazon S3 Target**drop-down menu to select an Amazon S3 replication target from the list of previously created replication targets.
- **5.** Use the **Type** drop-down menu to select whether the data persistence rule to use for the for the replication target is **Permanent** or **Retired**.
 - **Note:** You cannot create a replication rule as **Retired**. You can only modify a rule from permanent to retired after creating the replication rule.
- **6.** Use the **Initial Data Placement** drop-down menu to select the storage class for any objects transferred to the AWS S3 instance. See Storage Classes for detailed descriptions of the storage classes provided by AWS.
 - **Note:** The BlackPearl system uses "standard" restore for objects archived to Glacier and Glacier Deep Archive storage classes. Restore times are approximately 3-5 hours for Glacier, and 12 hours for Glacier Deep Archive, plus object download time.
 - Standard Provides high availability and performance for frequently accessed data.
 - Reduced Redundancy Provides storage of objects on multiple devices across
 multiple facilities, but does not replicate objects as many times as Amazon S3 standard
 storage. The lower level of redundancy results in less durability and availability, but
 also lower storage costs.
 - Standard IA (default) Provides fast access to less frequently accessed data.
 - Glacier Provides secure, long-term archive for rarely accessed data.

- **Glacier Deep Archive** Provides a low-cost, secure long-term archive for data that does not require quick retrieval.
- **7.** Select or clear the **Replicate Deletes** check box. When selected, any time a replicated file is deleted from the source system, it is also deleted from the target.
- **8.** If desired, modify the **Max Blob Part Size**. This parameter defines the maximum object part size used when sending data to an Amazon S3 target. Larger blob sizes make public cloud workflows simpler, but may make it more difficult or impossible to reliably transmit blobs. Less reliable network connections to the public cloud require smaller blob sizes. The maximum blob size is 1 TB. The default maximum blob size is 1 GB.

Note: To prevent data transfer failures, it is important that this value not exceed the maximum blob size that the target is able to accept.

9. Click **Create**. The new Amazon S3 replication rule displays on the Data Policy details screen.

Add a Microsoft Azure Data Replication Rule to a Data Policy

- **1.** If necessary, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Double-click the data policy in the Data Policies pane, or select the data policy and select **Action > Show Details** from the menu bar. The Data Policy details screen displays (see Figure 45 on page 137).
- **3.** Select **Action > New Microsoft Azure Data Replication Rule**. The New Microsoft Azure Data Replication Rule dialog box displays.

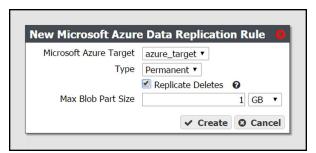


Figure 49 The New Microsoft Azure Data Replication Rule dialog box.

- **4.** Use the **Microsoft Azure Target** drop-down menu to select a Microsoft Azure replication target from the list of previously created replication targets.
- **5.** Use the **Type** drop-down menu to select whether the data persistence rule to use for the for the replication target is **Permanent** , or **Retired**.

Note: You cannot create a replication rule as **Retired**. You can only modify a rule from permanent to retired after creating the replication rule.

6. Select or clear the **Replicate Deletes** check box. When selected, any time a replicated file is deleted from the source system, it is also deleted from the target.

Note: Replicated objects do not immediately delete. Objects are only deleted after running a verify operation on the bucket.

7. If desired, modify the **Max Blob Part Size**. This parameter defines the maximum object part size used when sending data to a Microsoft Azure target. Larger blob sizes make public cloud workflows simpler, but may make it more difficult or impossible to reliably transmit blobs. Less reliable network connections to the public cloud require smaller blob sizes. The maximum blob size is 1 TB. The default maximum blob size is 1 GB.

Note: To prevent data transfer failures, it is important that this value not exceed the maximum blob size that the target is able to accept.

8. Click **Create**. The new Microsoft Azure replication rule displays on the Data Policy details screen.

CREATE A BUCKET

Buckets are data transfer targets for read and write operations. The system stages data written to it on the cache and optimizes how it writes buckets to storage domains for best performance.

Clients write data to the system using a "bulk PUT" command, and read from the system with a "bulk GET" command. For more information on using these commands see the *Spectra BlackPearl Spectra S3 API Reference*.

Note: Buckets can also be created using a Spectra S3 client, or Spectra S3 API.



If you are creating a bucket that is used in a BlackPearl replication

IMPORTANT configuration, you must create the bucket on the source system, and let it replicate to the target system.

Use the instructions in this section to configure a bucket.

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

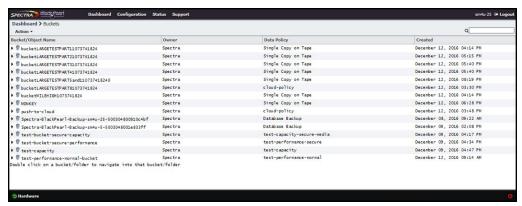


Figure 50 The Buckets screen.

2. Select **Action > New** from the menu bar. The New Bucket dialog box displays.

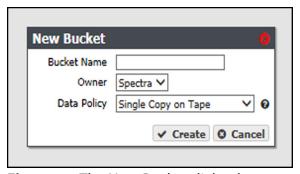


Figure 51 The New Bucket dialog box.

3. Enter a name for the bucket in the **Bucket Name** field.

When creating a bucket for use with an Amazon S3 or Microsoft Azure replication target, the bucket name must adhere to the cloud target naming requirements. The BlackPearl system attempts to create the bucket on the replication target using the name entered in Step 3 with the appended Cloud Bucket Prefix and Suffix, if applicable.



- For **BlackPearl software version 3.5.2 or earlier**, the BlackPearl system 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 causing possible data collision and bucket ownership/permission problems.
- For BlackPearl software version 4.0 or later, if the bucket name is incompatible with the naming requirements of the cloud target provider, bucket creation fails and an error message displays.

Notes:

- The bucket name cannot contain a colon (:), forward slash (/), or space.
- The bucket name cannot exceed 255 characters.
- **4.** Using the drop-down menu, select an **Owner** for the bucket from the list of users already created on the system.
- **5.** Using the drop-down menu, select a **Data Policy** for the bucket from the list of previously created data policies on the system. The bucket uses this data policy when transferring data.
- **6.** Click **Create**. The Buckets screen displays with the newly created bucket listed.

Create a New Bucket ACL for a Group

Use the instructions in this section to create a new Access Control List (ACL) using the specified group for a bucket.

1. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 50 on page 143).

2. Select the bucket for which you want to create an ACL and select **Action > Show Details**. The bucket details screen displays.

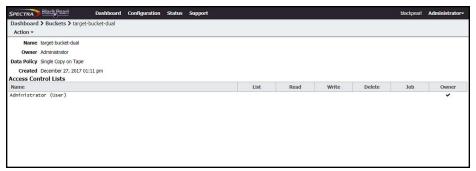


Figure 52 The bucket details screen.

3. Select **Action > New Bucket ACL For Group**. The New Bucket ACL For Group dialog box displays.

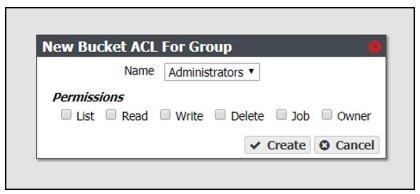


Figure 53 The New Bucket ACL For Group dialog box.

- **4.** Using the **Name** drop-down list, select a group from the list of exiting S3 groups on the BlackPearl system.
- **5.** Select the desired **Permissions** for the group ACL.
- 6. Click Create.

Create a New Bucket ACL for a User

Use the instructions in this section to create a new Access Control List (ACL) using the specified user for a bucket.

1. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 50 on page 143).

2. Select the bucket for which you want to create an ACL and select **Action > Show Details**. The bucket details screen displays.

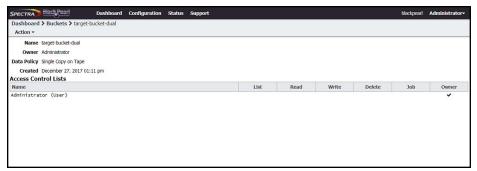


Figure 54 The bucket details screen.

3. Select **Action > New Bucket ACL For User**. The New Bucket ACL For User dialog box displays.



Figure 55 The New Bucket ACL For Group dialog box.

- **4.** Using the **Name** drop-down list, select a user from the list of exiting users on the BlackPearl system.
- **5.** Select the desired **Permissions** for the user ACL.
- 6. Click Create.

TRANSFER DATA

After completing the above sections of this chapter, you are ready to begin transferring data to, and from, the BlackPearl system.

- To transfer data using the EON Browser, consult the EON Browser User Guide.
- To transfer data using the Spectra RioBroker® application, consult the *Spectra RioBroker User Guide*.

- To transfer data using the Spectra StorCycle® application, consult the *Spectra StorCycle User Guide*.
- To transfer data using a Spectra S3 client, consult the *Spectra BlackPearl Spectra S3 API Reference*, and documentation specific to each Spectra S3 client.



The Spectra BlackPearl system limits the number of simultaneous active jobs. The number of simultaneous jobs differs depending on the software installed on the BlackPearl system.

- BlackPearl 3.x is limited to 1,000 simultaneous active jobs.
- BlackPearl 4.x is limited to 1,000 simultaneous active jobs.
- BlackPearl 5.x is limited to 10,000 simultaneous active jobs.

Chapter 5 - Managing Advanced Bucket Management Settings

This chapter describes using the BlackPearl user interface to manage storage domains, data policies, disk partitions, and buckets on the system after configuring Advanced Bucket Management. For initial Advanced Bucket Management configuration steps, see "Configuring Advanced Bucket Management" on page 106 on page 220.

Торіс	
Manage a Storage Domain	page 149
Edit a Storage Domain Member	page 149
Exclude a Storage Domain Member	page 150
Cancel Storage Domain Member Exclusion	page 151
Delete a Storage Domain Member	page 151
Edit a Storage Domain	page 152
Delete a Storage Domain	page 153
Manage Data Replication Rules	page 154
Edit a BlackPearl Data Replication Rule	page 154
Edit an Amazon S3 Data Replication Rule	page 155
Edit a Microsoft Azure Data Replication Rule	page 156
Delete a Data Replication Rule	page 157
Manage a Data Policy	page 158
Edit a Data Policy	page 158
Delete a Data Policy	page 159
Delete a Data Policy ACL	page 160
Edit a Data Persistence Rule	page 160
Delete a Data Persistence Rule	page 162
Manage Replication Targets	page 163
Edit a BlackPearl Replication Target	page 163
Edit an Amazon Replication Target	page 164
Edit an Azure Replication Target	page 165
Verify a Replication Target	page 165

Topic	
Put a Replication Target in Standby State	page 166
Activate a Replication Target	page 167
Delete a Replication Target	page 168
Manage a Disk Partition	page 168
Edit a Disk Partition	page 169
Delete a Disk Partition	page 169
Manage Online and Nearline Disk Pools	page 170
Import a Nearline or Online Disk Pool	page 170
Delete a Nearline or Online Disk Pool	page 172
Manage Buckets	page 172
Manage Buckets	page 172
Show Bucket Physical Placement	page 173
Edit a Bucket ACL	page 173
Delete a Bucket ACL	page 174
Edit a Bucket	page 174
Delete a Bucket	page 175

MANAGE A STORAGE DOMAIN

Use the instructions in this section to edit or delete a storage domain member or a storage domain.

Edit a Storage Domain Member

Use the instructions in this section to change the write preference for a storage domain member.

Note: For every storage domain, at least one storage domain member must have a write preference other than **Never_Select**.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).

- **2.** Double-click the row for the storage domain with the storage domain member that you want to edit, or select the storage domain row and then select **Action > Show Details**. The Storage Domain details screen displays (see Figure 40 on page 130).
- **3.** Select the storage domain member row and then select **Action > Edit Storage Domain Member**.

Note: Do not click the partition name when selecting the data persistence rule row or the Partition details screen will open.

The Edit Storage Domain Member dialog box displays.

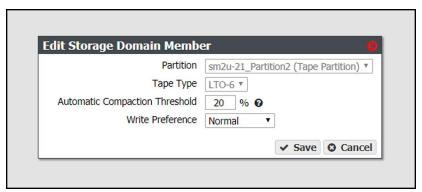


Figure 56 The Edit Storage Domain Member dialog box.

- **4.** If desired, edit the percentage for the **Automatic Compaction Threshold**. Automatic compaction occurs when the percentage of deleted objects on a tape cartridge exceeds this value.
- **5.** If desired, using the drop down menu, edit the **Write Preference** field as necessary. See Add a Storage Domain Member to a Storage Domain on page 129 for a description of each field.

Note: When editing a storage domain member, the **Partition** and **Tape Type** settings are unavailable.

6. Click **Save**. The edited storage domain member displays on the Storage Domain details screen.

Exclude a Storage Domain Member

Use the instructions in this section to exclude a storage domain member. This command migrates data off of the selected storage domain member before deleting the storage domain member.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).

- **2.** Double-click the row for the storage domain with the storage domain member that you want to exclude, or select the storage domain row and then select **Action > Show Details**. The Storage Domain details screen displays (see Figure 40 on page 130).
- **3.** Select the desired storage domain member row and then select **Action > Exclude Storage Domain Member**.

Note: Do not click the partition name when selecting the data persistence rule row or the Partition details screen will open.

The Exclude Storage Domain Member dialog box displays.

4. Type EXCLUDE in the entry field and then click **Exclude**.

Cancel Storage Domain Member Exclusion

Use the instructions in this section to cancel a storage domain member exclusion in process.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Double-click the row for the storage domain with the storage domain member that is currently being excluded, or select the storage domain row and then select **Action > Show Details**. The Storage Domain details screen displays (see Figure 40 on page 130).
- **3.** Select the desired storage domain member row and then select **Action > Cancel Storage Domain Member Exclusion**.

Note: Do not click the partition name when selecting the data persistence rule row or the Partition details screen will open.

The Cancel Storage Domain Member Exclusion dialog box displays.

4. Type CANCEL in the entry field and then click **Cancel**.

Delete a Storage Domain Member

Use the instructions in this section to delete a storage domain.

Notes:

- You cannot delete a storage domain member that has a tape or pool assigned to the storage domain.
- You cannot delete the last storage domain member of a storage domain assigned to a data policy.
- 1. From the menu bar, select Configuration > Advanced Bucket Management > Storage & Data Policy Management to display the Advanced Bucket Management screen (see Figure 31 on page 108).

- 2. Double-click the row for the storage domain with the storage domain member that you want to edit, or select the storage domain row and then select **Action > Show Details**. The Storage Domain details screen displays (see Figure 40 on page 130).
- 3. Select the storage domain member row and then select **Action > Delete Storage Domain** Member.

Note: Do not click the partition name when selecting the data persistence rule row or the Partition details screen will open.

A confirmation dialog box displays.



Figure 57 The delete storage domain member confirmation dialog box.

4. Type DELETE into the entry field, and then click **Delete**.

Edit a Storage Domain

Use the instructions in this section to change the parameters for a storage domain.



If this storage domain is assigned to a data policy that uses versioning, after **MPORTANT** data is persisted, you cannot change this setting from Object ID to Object

Note: If an edit you select is not allowed, the system generates an error message when you click **Save**, explaining why the edit is not allowed.

 From the menu bar, select Configuration > Advanced Bucket Management > Storage & **Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).

2. Select the row for the storage domain that you want to edit and then select **Action > Edit**. The Edit storage domain screen displays

Note: Alternatively, select **Action > Edit Storage Domain** from the storage domain details screen.

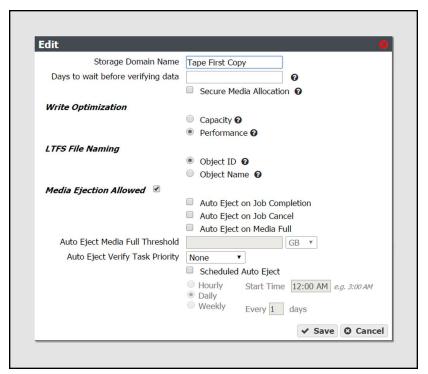


Figure 58 The Edit Storage Domain dialog box.

- **3.** Edit the fields as necessary. See Create a Storage Domain on page 124 for a description of each field.
- **4.** Click **Save**. The edited storage domain displays on the Advanced Bucket Management screen.

Delete a Storage Domain

Use the instructions in this section to delete a storage domain.

Note: You cannot delete a storage domain if it is used by a data policy. See Delete a Data Replication Rule on page 157 for instructions on removing the storage domain from a data policy.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).

2. Select the row for the storage domain that you want to delete and then select **Action > Delete**. A confirmation dialog box displays.



Figure 59 The delete storage domain confirmation dialog box.

3. Type DELETE into the entry field, and then click **Delete**.

MANAGE DATA REPLICATION RULES

Edit a BlackPearl Data Replication Rule

Use the instructions in this section to change the type, data policy, or whether to replicate deletes, for a BlackPearl data replication rule.

Note: Some edits are restricted based on whether a bucket is currently using the data policy. If an edit is not allowed, an error message displays when you click **Save**.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Double-click the data policy with the BlackPearl data replication rule that you want to edit, or select the data policy and then select **Action > Show Details**. The Data Policy details screen displays (see Figure 45 on page 137).

3. Double-click the row of the BlackPearl data replication rule that you want to edit, or select the row for the replication rule and then select **Action > Edit Rule**.

Note: Do not click the target name when selecting the data persistence rule row or the Replication Targets screen will open.

The Edit BlackPearl Data Replication Rule dialog box displays.

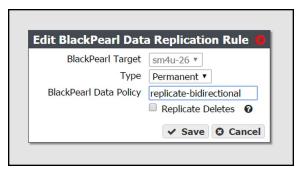


Figure 60 The Edit BlackPearl Data Replication Rule dialog box.

- **4.** The BlackPearl target name is unavailable and cannot be changed.
- **5.** Edit the fields as necessary. See Add a BlackPearl Data Replication Rule to a Data Policy on page 138 for a description of each field.
- **6.** Click **Save**. The edited BlackPearl data replication rule displays on the Data Policy details screen.

Edit an Amazon S3 Data Replication Rule

Use the instructions in this section to change the type, Initial Data Placement, whether to Replicate Deletes, or the Max Blob Size for an Amazon S3 data replication rule.

Note: Some edits are restricted based on whether a bucket is currently using the data policy. If an edit is not allowed, an error message displays when you click **Save**.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Double-click the data policy with the Amazon S3 replication rule that you want to edit, or select the data policy and then select **Action > Show Details**. The Data Policy details screen displays (see Figure 45 on page 137).

3. Double-click the row of the Amazon S3 data replication rule that you want to edit, or select the row for the replication rule and then select **Action > Edit Rule**.

Note: Do not click the target name when selecting the data persistence rule row or the Replication Targets screen will open.

The Edit Amazon S3 Data Replication Rule dialog box displays.



Figure 61 The Edit Amazon S3 Data Replication Rule dialog box.

- **4.** The Amazon S3 target name is unavailable and cannot be changed.
- **5.** Edit the fields as necessary. See Add an Amazon S3 Data Replication Rule to a Data Policy on page 140 for a description of each field.
- **6.** Click **Save**. The edited Amazon S3 data replication rule displays on the Data Policy details screen.

Edit a Microsoft Azure Data Replication Rule

Use the instructions in this section to change the type, whether to Replicate Deletes, or the Max Blob Size for a Microsoft Azure data replication rule.

Note: Some edits are restricted based on whether a bucket is currently using the data policy. If an edit is not allowed, an error message displays when you click **Save**.

- From the menu bar, select Configuration > Advanced Bucket Management > Storage & Data Policy Management to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Double-click the data policy with the Microsoft Azure replication rule that you want to edit, or select the data policy and then select **Action > Show Details**. The Data Policy details screen displays (see Figure 45 on page 137).
- **3.** Double-click the row of the Microsoft Azure data replication rule that you want to edit, or select the row for the replication rule and then select **Action > Edit Rule**.

Note: Do not click the target name when selecting the data persistence rule row or the Replication Targets screen will open.

The Edit Microsoft Azure Data Replication Rule dialog box displays.

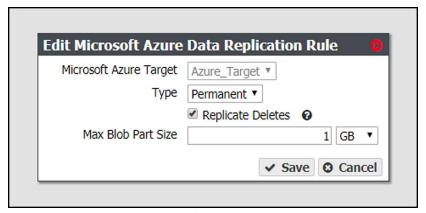


Figure 62 The Edit Microsoft Azure Data Replication Rule dialog box.

- **4.** The Microsoft Azure target name is unavailable and cannot be changed.
- **5.** Edit the fields as necessary. See Add a Microsoft Azure Data Replication Rule to a Data Policy on page 141 for a description of each field.
- **6.** Click **Save**. The edited Microsoft Azure data replication rule displays on the Data Policy details screen.

Delete a Data Replication Rule

Use the instructions in this section to delete a data replication rule for any type of target from a data policy.

Note: You cannot delete a data replication rule if the data policy is used by a bucket. See Delete a Bucket on page 175 for instructions for deleting buckets using a data policy.

- 1. From the menu bar, select Configuration > Advanced Bucket Management > Storage & Data Policy Management to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Double-click the data policy with the replication rule that you want to delete, or select the data policy and then select **Action > Show Details**. The Data Policy details screen displays (see Figure 45 on page 137).
- **3.** Select the row for the replication rule and then select **Action > Delete Rule**.

Note: Do not click the target name when selecting the data persistence rule row or the Replication Targets screen will open.

A confirmation dialog box displays.



Figure 63 The delete data replication rule confirmation dialog box.

4. Type DELETE into the entry field, and then click **Delete**.

MANAGE A DATA POLICY

Use the instructions in this section to manage access control lists (ACLs), and to edit or delete persistence rules, replication rules, and data policies.

Edit a Data Policy

Use the instructions in this section to edit a data policy.



If you previoulsy configured the data policy Versioning setting to **Keep IMPORTANT Multiple Versions**, you are not able to change this setting after the data policy was created.

Note: If an edit you selected is not allowed, the system generates an error message, when you click **Save**, explaining why the edit is not allowed. For example, you cannot change the **Checksum type** if the data policy is used by a bucket.

1. From the menu bar, select Configuration > Advanced Bucket Management > Storage & **Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).

2. Select the row for the data policy that you want to edit and then select **Action > Edit**. The Edit Data Policy screen displays.

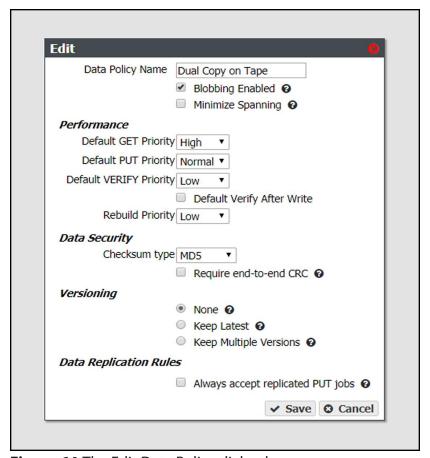


Figure 64 The Edit Data Policy dialog box.

- **3.** Edit the fields as necessary. See Create a Data Policy on page 131 for a description of each field.
- **4.** Click **Save**. The edited data policy displays on the Advanced Bucket Management screen.

Delete a Data Policy

Use the instructions in this section to delete a data policy.

Note: You cannot delete a data policy if any buckets exist that use the specified data policy. See Delete a Bucket on page 175 for instructions for deleting buckets using a data policy.

From the menu bar, select Configuration > Advanced Bucket Management > Storage & Data Policy Management to display the Advanced Bucket Management screen (see Figure 31 on page 108).

2. Select the row for the data policy that you want to delete and then select **Action > Delete**. A confirmation dialog box displays.



Figure 65 The delete data policy confirmation dialog box.

3. Type DELETE into the entry field, and then click **Delete**.

Delete a Data Policy ACL

Use the instruction in this section to delete a data policy ACL.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Select the row for the data policy for which you want to delete an ACL, then select **Action** > **Show Details**. The Data Policy details screen displays.
- **3.** Select the row for the data policy ACL which you want to delete.
- **4.** From the menu bar, select **Action > Delete Data Policy ACL**. A confirmation window displays.
- 5. Click Delete.

Edit a Data Persistence Rule

Use the instructions in this section to change the type, Isolation Level, or Minimum Days to Retain for a data persistence rule.

Note: Some edits are restricted based on whether a bucket is currently using the data policy. If an edit is not allowed, an error message displays when you click **Save**.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).

- **2.** Double-click the data policy with the persistence rule that you want to edit, or select the data policy and then select **Action > Show Details**. The Data Policy details screen displays (see Figure 45 on page 137).
- **3.** Double-click the row of the persistence rule that you want to edit, or select the row for the persistence rule and then select **Action > Edit Rule**.

Note: Do not click the storage domain name when selecting the data persistence rule row or the Storage Domain details screen will open.

The Edit Data Persistence Rule dialog box displays.

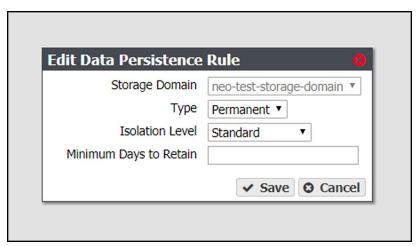


Figure 66 The Edit Data Persistence Rule dialog box.

- **4.** The **Storage Domain** setting is unavailable and cannot be changed.
- **5.** Edit the fields as necessary. See Add Data Persistence Rules and Replication Rules to a Data Policy on page 136 for a description of each field.
- **6.** Click **Save**. The edited data persistence rule displays on the Data Policy details screen.

Delete a Data Persistence Rule

Use the instructions in this section to delete a data persistence rule from a data policy.



CAUTION Deleting a persistence rule deletes all data associated with the rule.

Notes:

- You cannot delete a data persistence rule if the data policy is used by a bucket. See Delete a Bucket on page 175 for instructions for deleting buckets using a data policy.
- You cannot delete a persistence rule if it is the last permanent persistence rule for a data policy.
- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Double-click the data policy with the persistence rule that you want to delete, or select the data policy and then select **Action > Show Details**. The Data Policy details screen displays (see Figure 45 on page 137).
- **3.** Select the row for the persistence rule and then select **Action > Delete Rule**.

Note: Do not click the storage domain name when selecting the data persistence rule row or the Storage Domain details screen will open.

A confirmation dialog box displays.



Figure 67 The delete data persistence rule confirmation dialog box.

4. Type DELETE into the entry field, and then click **Delete**.

Manage Replication Targets

Use the instruction in this section to manage existing replication targets.

Edit a BlackPearl Replication Target

Use the instructions in this section to modify the configuration of an existing BlackPearl replication target.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 35 on page 116).
- **2.** Double-click the BlackPearl replication target that you want to edit, or select the replication target and then select **Action > Edit**. The Edit BlackPearl Target dialog box displays.

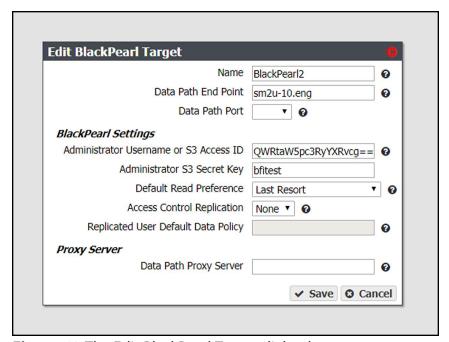


Figure 68 The Edit BlackPearl Target dialog box.

- **3.** Edit the fields as necessary. See Create a BlackPearl Target on page 115 for a description of each field.
- **4.** Click **Save**. The edited BlackPearl replication target displays on the Replication Targets screen.

Edit an Amazon Replication Target

Use the instructions in this section to modify the configuration of an existing Amazon replication target.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 35 on page 116).
- **2.** Double-click the Amazon replication target that you want to edit, or select the replication target and then select **Action > Edit**. The Edit Amazon S3 Target dialog box displays.

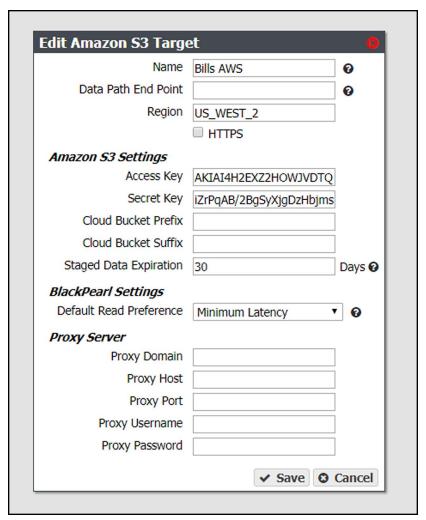


Figure 69 The Edit Amazon S3 Target dialog box.

- **3.** Edit the fields as necessary. See Create an Amazon S3 Target on page 118 for a description of each field.
- **4.** Click **Save**. The edited Amazon replication target displays on the Replication Targets screen.

Edit an Azure Replication Target

Use the instructions in this section to modify the configuration of an existing Azure replication target.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 35 on page 116).
- **2.** Double-click the Azure replication target that you want to edit, or select the replication target and then select **Action > Edit**. The Edit Microsoft Azure Target dialog box displays.

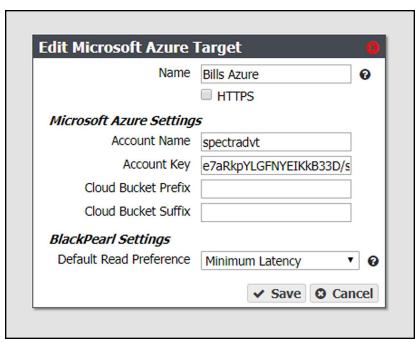


Figure 70 The Edit Microsoft Azure Target dialog box.

- **3.** Edit the fields as necessary. See Create a Microsoft Azure Target on page 122 for a description of each field.
- 4. Click Save. The edited Azure replication target displays on the Replication Targets screen.

Verify a Replication Target

Use the instructions in this section to verify connectivity to the target and optionally verify replicated data on the replication target.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 35 on page 116).

2. Double-click the replication target for which you want to verify connectivity, or select the replication target and then select **Action > Verify Data**. The Verify *target type* Target dialog box displays.

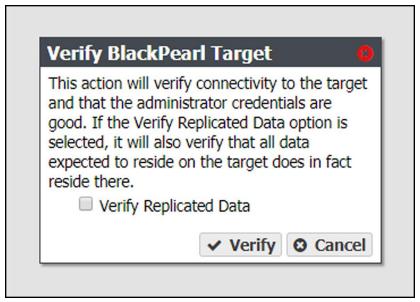


Figure 71 The Verify *target type* Target dialog box.

3. If desired, select **Verify Replicated Data** to confirm that the expected data resides on the replication target.

Note: Depending on the amount of data on the replication target, this process may take a long time to complete.

4. Click **Verify**. The system confirms connectivity to the target and optionally verifies the replicated data.

Put a Replication Target in Standby State

If you need to perform service on a replication target, it is recommended that you first put the replication target into a standby state. Otherwise, the BlackPearl system may attempt to use the target while it is in service.

Use the instructions in this section to place a replication target into a standby state. No data is transferred to the replication target while in standby.

1. From the menu bar, select Configuration > Advanced Bucket Management > Replication Targets to display the Replication Targets screen (see Figure 35 on page 116).

2. Select the replication target that you want to put into standby and then select **Action > Put Target in Standby**. The Put Target in Standby dialog box displays.



Figure 72 The Put Target in Standby dialog box.

3. Click **Deactivate**. The target is now in standby.

Activate a Replication Target

Use the instructions in this section to activate a replication target currently in standby. Once activated, data transfers are allowed to the replication target.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 35 on page 116).
- **2.** Select the replication target that you want to activate and then select **Action > Activate Target**. The Activate Target dialog box displays.



Figure 73 The Activate Target dialog box.

3. Click **Activate**. The target is now in an active state.

Delete a Replication Target

Use the instructions to delete an existing replication target.



CAUTION If you delete a replication target, all data on the target is deleted.

Note: You cannot delete a replication target if it is used by a data policy. See Delete a Data Replication Rule on page 157 for instructions on removing a replication target from a data policy.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Replication Targets** to display the Replication Targets screen (see Figure 35 on page 116).
- **2.** Select the replication target that you want to delete and then select **Action > Delete**. The Delete *target type* Target dialog box displays.

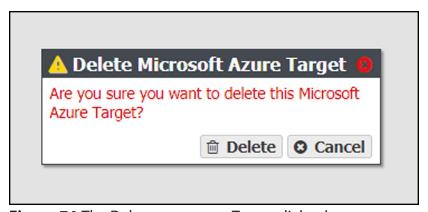


Figure 74 The Delete target type Target dialog box.

3. Click **Delete** to delete the selected replication target.

MANAGE A DISK PARTITION

Use the instructions in this section to edit or delete a disk partition.

Edit a Disk Partition

Use the instructions in this section to change the parameters for a disk partition.

Notes:

- You cannot remove a member pool that contains data.
- You cannot remove the last member pool of a disk partition assigned to a storage domain.
- 1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Data Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Select the disk partition row and then select **Action > Edit**. The Edit Disk Partition dialog box displays.

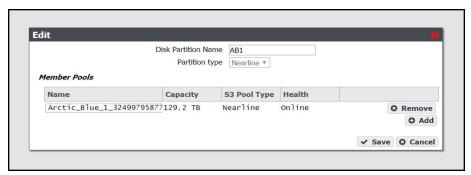


Figure 75 The Edit Disk Partition dialog box.

- **3.** Edit the fields as necessary. See Create a Storage Pool on page 107 for a description of each field.
- **4.** Click **Save**. The edited disk partition displays on the Advanced Bucket Management screen.

Delete a Disk Partition

Use the instructions in this section to delete a disk partition.

Note: You cannot delete a disk partition that is a member of any storage domain. See Delete a Storage Domain Member on page 151 for information on deleting the disk partition from a storage domain.

1. From the menu bar, select Configuration > Advanced Bucket Management > Storage & Data Policy Management to display the Advanced Bucket Management screen (see Figure 31 on page 108).

2. Select the row of the disk partition you want to delete and then select **Action > Delete**. A confirmation dialog box displays.



Figure 76 The Delete Disk Partition confirmation dialog box.

3. Type DELETE into the entry field, and then click **Delete**.

Manage Online and Nearline Disk Pools

Use the instructions in this section to manage nearline and online disk pools. For information on managing network attached storage (NAS) disk pools, see Managing Storage Pools on page 249.

Import a Nearline or Online Disk Pool

Data present on storage pools on expansion nodes can be moved from one BlackPearl system to another, either to increase name space redundancy, or as part of disaster prevention. Use the instructions in this section to import a pool.

- **1.** Ensure the expansion node containing the pool you want to import is cabled to the BlackPearl system master node.
- **2.** Ensure the settings for the Spectra S3 service **Default Conflict Resolution Mode** are set to your preference. See Configure the Spectra S3 Service on page 189 for more information.
- **3.** From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).

4. Disk pools eligible for import display with a health of **Foreign**. Select the nearline pool you want to import in the Storage Pools pane, and select **Action > Import Pool**. The Import dialog box displays.

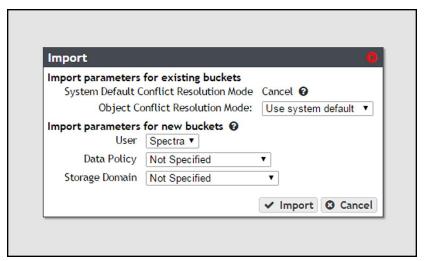


Figure 77 The Import dialog box.

- **5.** Configure the import parameters for existing buckets present on the storage pool.
 - **a.** The **System Default Conflict Resolution Mode** is configured when editing the Spectra S3 service and is not editable in this dialog box. See Configure the Spectra S3 Service on page 189 for more information.
 - **b.** Using the drop-down menu, select a behavior for **Object Conflict Resolution Mode**. This setting configures how the system handles a file name conflict when importing foreign objects on the storage pool to an existing bucket.

Value	Description
Use system default	The system uses the behavior displayed in the System Default Conflict Resolution Mode row of the Import dialog box.
Cancel	Abort the import process if a file name conflict is discovered.
Accept Most Recent	Keep the file with the most recent creation date.
Accept Existing	Keep the file currently in the BlackPearl database.

- **6.** Configure the import parameters for new buckets present on the storage pool.
 - **a.** Using the drop-down menu, select the **User** to be the owner of the imported bucket(s).
 - **b.** Using the drop-down menu, select the **Data Policy** to use for the imported bucket(s).

- **c.** Using the drop-down menu, select the **Storage Domain** to use for the imported bucket (s).
- 7. Click Import.

Delete a Nearline or Online Disk Pool

If you want to delete an online or nearline disk pool (for example, to create a larger pool after adding additional disks to the system) use the instructions in this section to delete a disk pool.

Note: You must delete all objects contained in the disk pool before you can delete the pool.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Select the pool you want to delete in the Storage Pools pane, and select **Action > Delete**. A confirmation dialog box displays.



Figure 78 The Delete Nearline Disk Pool confirmation dialog box.



Figure 79 The Delete Online Disk Pool confirmation dialog box.

3. Enter DELETE POOL into the entry field and click **Delete**. The disk pool is deleted.

MANAGE BUCKETS

Use the instructions in this section to configure ACLs for a bucket, edit, or delete a bucket. For instructions on creating a new bucket, see Create a Bucket on page 142.

Show Bucket Physical Placement

Once data is transferred to the BlackPearl system, you can view the physical placement of the data. The BlackPearl user interface displays data placement on disk pools, tapes, and replication targets. Use the instructions in this section to view physical placement of a specified bucket.

- **1.** From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 50 on page 143).
- **2.** Select the bucket for which you want to view physical placement and select **Action > Show Physical Placement**. The *Bucket* Physical Placement screen displays.

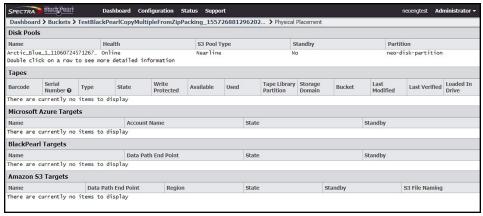


Figure 80 The Bucket Physical Placement screen.

Edit a Bucket ACL

Use the instructions in this section to edit an Access Control List (ACL) for a bucket.

- **1.** From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 50 on page 143).
- **2.** Select the bucket for which you want to edit an ACL and select **Action > Show Details**. The bucket details screen displays (see Figure 52 on page 145).

3. Select the Access Control List you want to edit and select **Action > Edit Bucket ACL**. The Edit Bucket ACL dialog box displays.

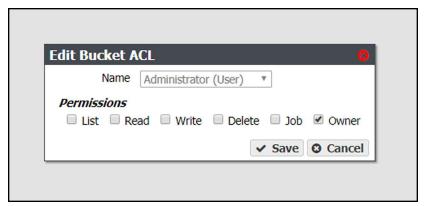


Figure 81 The Edit Bucket ACL dialog box.

Note: You cannot change the user of an existing bucket ACL list. The **Name** drop-down list is unavailable.

- **4.** Select or clear the desired **Permissions** for the bucket ACL.
- 5. Click Save.

Delete a Bucket ACL

Use the instructions in this section to delete an Access Control List (ACL) for a bucket.

- **1.** From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 50 on page 143).
- **2.** Select the bucket for which you want to delete an ACL and select **Action > Show Details**. The bucket details screen displays (see Figure 52 on page 145).
- **3.** Select the Access Control List you want to delete and select **Action > Delete Bucket ACL**. The Delete Bucket ACL confirmation dialog box displays.
- 4. Click Delete.

Edit a Bucket

Use the instructions in this section to change the owner of a bucket or to change the data policy used by the bucket.

1. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 50 on page 143).

2. Select the bucket you want to edit and select **Action > Edit**. The Edit Bucket dialog box displays.

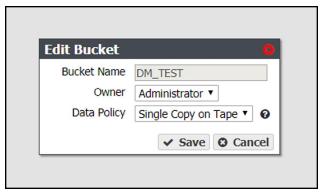


Figure 82 The Edit Bucket dialog box.

- **3.** The **Bucket Name** is unavailable and cannot be changed.
- **4.** From the drop-down list, change the **Owner** assigned to the bucket.



After changing bucket owners, you may need to reconfigure your client application to access the bucket.

- **5.** Use the **Data Policy** drop down menu to change the data policy assigned to the bucket. For more information on data policies, see Data Policies on page 75.
- **6.** Click **Save**.

Delete a Bucket

Use the instructions in this section to delete a bucket.



When you delete a bucket, all data contained in the bucket is lost. Any tapes associated with the bucket are marked as Free, and are available to the system AUTION for other storage operations immediately. Any bucket data that was written to tape media is retained until the tape is loaded into a drive and new data is written.

1. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 50 on page 143).

2. Select the bucket you want to delete and select **Action > Delete**. A confirmation dialog box displays.

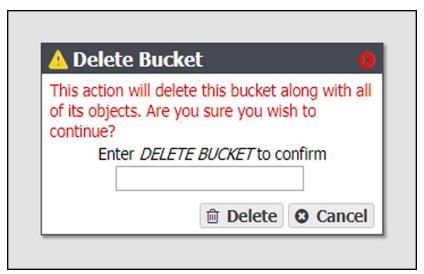


Figure 83 The bucket delete confirmation dialog box.

3. Type DELETE BUCKET into the entry field, and then click **Delete**.

Chapter 6 - Additional Configuration Options

This chapter describes using the BlackPearl user interface to configure additional options for the Spectra BlackPearl Converged Storage System.

Topic	
Configure Network Connections and Settings	page 178
Configure Ethernet Ports	page 179
Configure DNS Settings	page 185
Configure SMTP Settings	page 186
Configure Date and Time	page 187
Edit the System Name	page 188
Configure Networking Services	page 188
Configure the Spectra S3 Service	page 189
Configure the Active Directory Service	page 193
Configure the SNMP Service	page 197
Configure the Vail Service	page 199
Configure and Use Encryption	page 201
Configure the Encryption Service	page 201
Change the Encryption Password	page 202
Unlock the Self-Encrypting Drives	page 203
Create an Encryption Password USB Key	page 204
PSID Erase an Encryption Drive	page 205
Configure Users and S3 Groups	page 207
Description of User Types	page 207
Create a User	page 207
Edit a User	page 207
Change S3 Secret Key	page 210
Create an S3 Group	page 212
Remove an S3 Group Member	page 214
Edit an S3 Group	page 215

Topic	
Delete a User or S3 Group	page 215
Configure Certificates	page 216
Manually Enter Activation Keys	page 217

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.

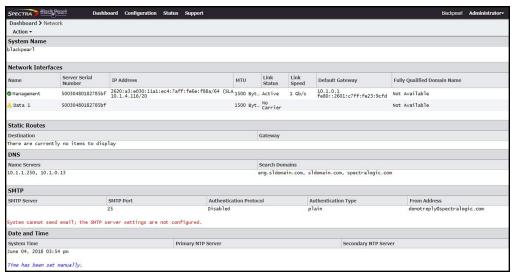


Figure 84 The Network screen.

Configure Ethernet Ports

This section describes using the BlackPearl user interface to configure the IP addressing for the Ethernet ports in the BlackPearl system. The system includes two 10 GigE ports on the rear panel (see Figure 7 on page 41). Optionally, a two-port 40 GigE card can be installed.

Notes:

- You can create one or more data connections to the system.
- You can configure link aggregation for better performance.
- While different types of Ethernet network interface cards can be installed in the same BlackPearl system, 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.
- The data connection(s) and BlackPearl management port are initially configured in Initial Configuration on page 53. Use the instructions in this section to configure network settings after initial setup is complete.

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

- Configure the Data Connection on page 61
- Configure the Management Port below
- Edit an Aggregate Data Connection on page 181
- Edit a Static Route on page 184
- Clear a Data Port Configuration on page 184

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.

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.

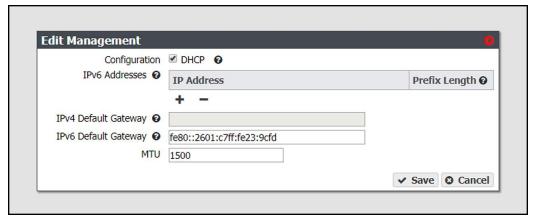


Figure 85 The Edit Management dialog box.

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



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 180.

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

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

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

Notes:

- If you selected DHCP in Step 3 on page 180, this option is unavailable.
- The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl system.

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 system.
- The IPv6 Gateway does not need to be configured when the BlackPearl system 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.



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

- 1. From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays (see Figure 84 on page 178).
- 2. Select the row of the data connection you want to edit and select **Action > Edit**. A the Edit Aggregate *Data Connection* dialog box displays.

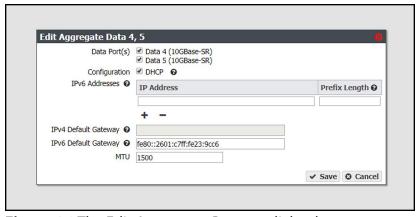


Figure 86 The Edit Aggregate *Data* #,# dialog box.

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

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

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

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

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

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

Notes:

- If you selected DHCP in Step 4, this option is unavailable.
- The gateway entered for the last configured IPv4 connection sets the default gateway for the BlackPearl system.
- 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 system.
- The IPv6 Gateway does not need to be configured when the BlackPearl system 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 84 on page 178).

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

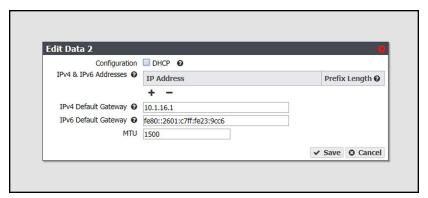


Figure 87 The Edit *Data* # dialog box.

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

Note: You cannot enter an 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 **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 system.
- **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 system.
- The IPv6 Gateway does not need to be configured when the BlackPearl system 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 19 on page 64).
- **2.** Double-click the static route you want to edit. The Static Route dialog box displays.



Figure 88 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 179 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 84 on page 178).
- **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 system are used to allow domain name lookup on the system. Use the following instructions to enter DNS information on the system.

- **1.** From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays (see Figure 84 on page 178).
- **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.

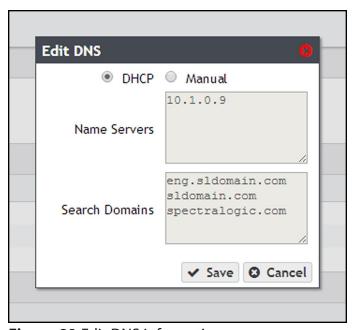


Figure 89 Edit DNS information.

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

-OR-

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

Note: The buttons for **DHCP** and **Manual** are only usable when the 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 system with a mail server. The system 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.

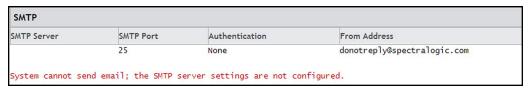


Figure 90 The SMTP pane of the Network screen.

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 91 The Email dialog box.

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

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

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

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



Figure 92 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.

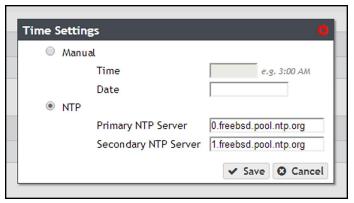


Figure 93 The Time Settings dialog box.

- 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.

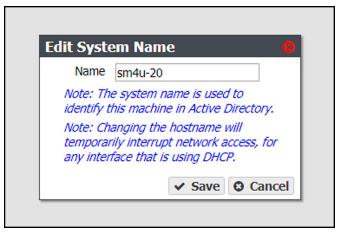


Figure 94 The Edit System Name dialog box.

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

Notes:

- 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 BlackPearlSystem.domain.com
- If your system is using firmware BlackPearl 3.2.2, or earlier, there are no character restrictions on system names. However, Spectra Logic recommends limiting system names to letters, numbers, and hyphens to maintain compatibility with the RFC 1123 standard.
- The system does not change previously configured system names using special characters when upgrading to BlackPearl 3.3, or later.
- 4. Click Save.

CONFIGURE NETWORKING SERVICES

Use the following instructions to configure networking services on the BlackPearl system. For instructions on configuring NAS services, see Configure NAS Services on page 238.

Configure the Spectra S3 Service

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

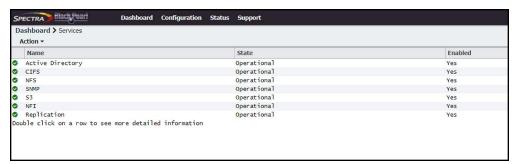


Figure 95 The Services screen.

- **2.** Double-click the S3 service, or select the S3 service and select **Action > Show Details**. The S3 details screen displays.
- **3.** On the S3 service details screen, select **Action > Edit**. The Edit S3 Service dialog box displays.

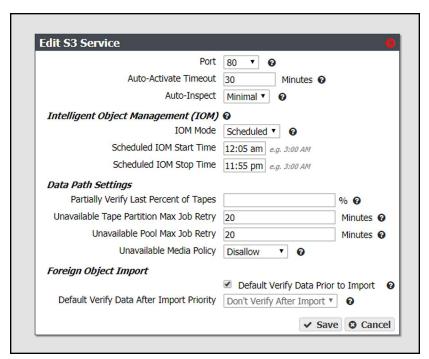


Figure 96 The Edit S3 Service dialog box.

4. Using the drop-down list, select the **Port** used for the HTTP connection to the S3 service. **Note:** The HTTPS connection is always available on port 443.

5. Enter a value in minutes in the **Auto-Activate Timeout** entry field. This value specifies the amount of time that must pass between the S3 data path backend shutdown and the restart before it will not be auto-activated. For example, if the system is powered off for longer than the specified timeout value, you must manually restart the S3 data path backend after powering on the system.

Notes:

- To manually start the data path backend, see Reboot or Shut Down a BlackPearl System on page 339.
- If the **Auto-Activate Timeout** is set to 0, the data path backend will never auto-activate.
- **6.** Using the drop-down menu, select a behavior for **Auto-Inspect**. This setting configures whether tape inspections are performed by the system based on a tape's last known state, or each time the BlackPearl is initialized.

Value	Description
Full	Tapes are scheduled for inspection if an inspection is necessary given the tape's current state, as well as every time the BlackPearl system is initialized.
Minimal	Tapes are scheduled for inspection if an inspection is necessary given the tape's current state.
Never	Tapes are not automatically scheduled for inspection.

Notes:

- All tapes new to the BlackPearl system are inspected regardless of the autoinspect setting.
- With BlackPearl software version 5.2 or earlier, if there was an inventory change in the tape library while in standby, the BlackPearl system could react by reinspecting all tapes in the library. Starting with BlackPearl version 5.3, the system no longer re-inspects tapes when there is an inventory change while the partition is in standby if the S3 service is set to "Never Inspect".

7. Use the **IOM Mode** drop-down menu to select the behavior for Intelligent Object Management. Enabling this option allows for automatic object recovery, automatic tape compaction, and data migration at a system-wide level. See Intelligent Object Management (IOM) on page 378 for information on IOM.

Value	Description
Enabled	The BlackPearl system processes IOM operations as needed. If you select this option, the IOM Start Time and IOM Stop Time fields are unavailable.
Scheduled	IOM processes only run during the period between the IOM Start Time and IOM Stop Time. Note: If you set the start and stop time to the same value, IOM operations do not run.
Disabled	The BlackPearl system does not perform any IOM operations.

Notes:

- IOM is enabled by default. Spectra Logic recommends leaving the feature enabled.
- Automatic tape compaction is configured on a per tape partition basis (see Tape Partition Drive Reservation on page 294 for more information).
- Data migration is initiated manually. See Data Migration on page 300 for more information.
- If this option is currently enabled, when the setting is disabled, any in-progress IOM operations are suspended.
- **8.** Enter a percentage value for **Partially Verify Last Percentage of Tapes**. This setting specifies the percentage of the total reported capacity of the tape cartridge scanned by an automatic or on demand data integrity verification. The system starts the scan at the specified percentage of the tape capacity before the EOD (End of Data) marker and ends the scan at the EOD marker. For example, if you specify ten percent, the verification process scans the last 250 GB of a 2.5 TB LTO-6 tape cartridge, or the last 600 GB of a 6 TB LTO-7 tape cartridge.
 - Leave the field blank to configure data integrity verification to scan all data present on the tape cartridge.
 - Percentage values of zero and 100 are not supported.
 - See Data Integrity Verification Tape Media on page 355 for information about on demand tape media data integrity verification.

- **9.** Enter a value, in minutes, for **Unavailable Tape Partition Max Job Retry**. This setting specifies the maximum number of minutes that can elapse between the first failed attempt to GET or VERIFY job data (due to a tape partition being offline, in an error state, or deactivated), before a subsequent failure will trigger a retry to process the job data. This only applies to GET or VERIFY jobs.
- **10.** Enter a value, in minutes, for **Unavailable Pool Max Job Retry**. This setting specifies the maximum number of minutes that can elapse between the first failed attempt to GET or VERIFY job data (due to a pool partition being offline, in an error state, or deactivated), before a subsequent failure will trigger a retry to process the job data. This only applies to GET or VERIFY jobs.
- **11.** Using the drop-down menu, select a behavior for **Unavailable Media Policy**. This setting configures how the system behaves where there is unavailable tape or disk partitions when creating new jobs or retrying to process job data.

Value	Description
Allow	New job requests for unavailable media are allowed and will retry for the duration of the Unavailable Tape Partition Max Job Retry or Unavailable Pool Max Job Retry setting.
Discouraged	Unavailable partitions can be used, but only if no other media is available.
Disallow	New job requests for unavailable media fail.

- **12.** Select or clear **Default Verify Data Prior to Import**. Selecting this option verifies data on imported tape media before it makes the data available to the system.
- **13.** Using the drop-down menu, select a priority for **Default Verify Data After Import Priority**. This option makes imported foreign options available, and schedules a verify job with the selected priority at a later time.

Note: This option is unavailable if you selected **Default Verify Data Prior to Import** in Step 12 on page 192.

14. Click Save.

Configure the Active Directory Service

The Active Directory service in the BlackPearl user interface is used to connect the system to a Windows Active Directory domain. Before you can join a domain, you must configure the BlackPearl system to use NTP. See Configure Date and Time on page 187.

Note: If the BlackPearl system 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 95 on page 189).
- 2. Double-click the Active Directory row, or select the Active Directory row and select ActionShow 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.

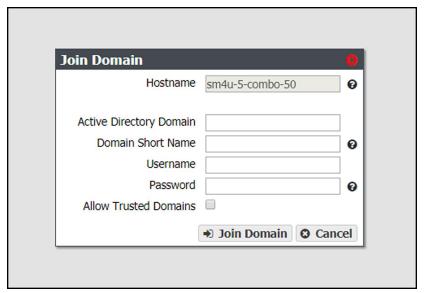


Figure 97 The Join Domain dialog box.

4. The **Hostname** identifies the BlackPearl system 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 188).

- **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 system 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 system joins an Active Directory domain. The system does not save this information.
- **8.** If desired, select **Allow Trusted Domains** if the Active Directory domain you want to join is a trusted domain.
- 9. Click Join Domain.

Edit Domain

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

- **1.** From the menu bar, select **Configuration > Services**. The Services screen displays (see Figure 95 on page 189).
- 2. Double-click the Active Directory row, or select the Active Directory row and select ActionShow Details. The Active Directory details screen displays.
- **3.** Select **Action > Edit**. The Edit AD Service dialog box displays.

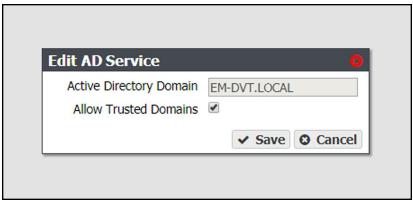


Figure 98 The Join Domain dialog box.

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.



Improperly configuring advanced parameters can expose security vulnerabilities **CAUTION** 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 95 on page 189).
- **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.

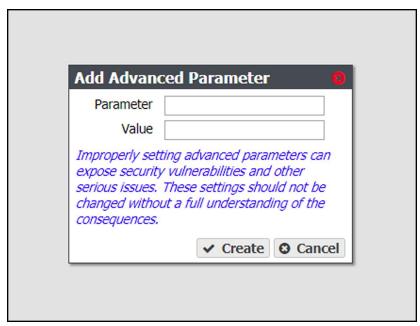


Figure 99 The Add Advanced Parameter dialog box.

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

Edit Advanced Parameter



Improperly configuring advanced parameters can expose security vulnerabilities **CAUTION** 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 95 on page 189).
- 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.

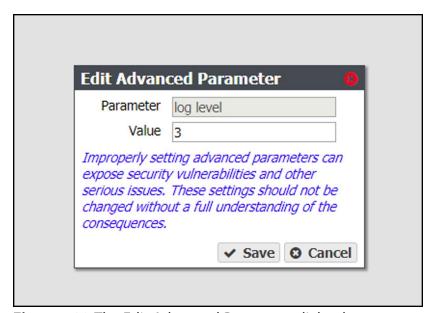


Figure 100 The Edit Advanced Parameter dialog box.

- **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 95 on page 189).
- 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 95 on page 189).
- **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 95 on page 189).
- **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.

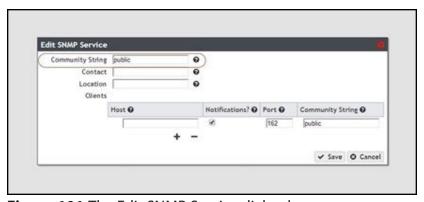


Figure 101 The Edit SNMP Service dialog box.

- **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 system responds to all SNMP queries.
- **5.** Enter the primary contact for the BlackPearl system in the **Contact** field.
- **6.** Enter the physical location of the system in the **Location** field.

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

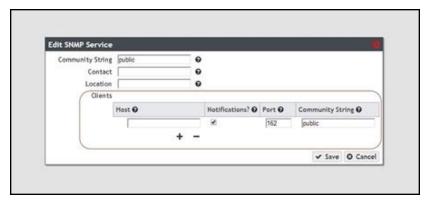


Figure 102 The Edit SNMP Service dialog box.

- 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 system using SNMP, you must first download the BlackPearl Converged Storage System 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 95 on page 189).
- **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 103 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 system, using the settings configured in Configure the SNMP Service on page 197.

Configure the Vail Service

The Vail service configures a BlackPearl system 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 configure the Vail service.

- **1.** From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 95 on page 189).
- **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 Sphere dialog box displays.

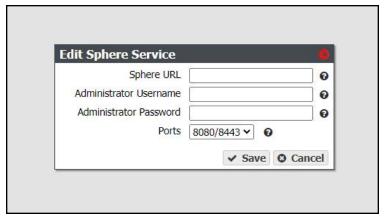


Figure 104 The Edit Sphere service dialog box.

- **4.** Enter the **Sphere URL**, and the **Administrator Username** and **Password** of the Vail application administrator account.
- **5.** Using the **Ports** drop-down menu, select the pair of ports to use to communicate with the Vail application.

Note: For existing BlackPearl systems, Spectra Logic recommends setting this value to the pair of ports your S3 service is not currently using. If necessary, see the S3 service details screen to determine the ports currently in use by the S3 service.

Note: For new BlackPearl systems, Spectra Logic recommends using the **80/443** pair of ports.

6. Click **Save**. The Edit Sphere dialog box refreshes to display the Location drop-down menu.



Figure 105 The Edit Sphere service dialog box with Location drop-down menu.

7. Using the **Location** drop-down menu, select the desired location previously configured in the Vail application, and click **Save**.

CONFIGURE AND USE ENCRYPTION

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

Note: This feature only applies to disk-based storage. Tape storage encryption is configured on the tape library. See your *Tape Library User Guides for information about tape encryption*.

Configure the Encryption Service

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

- **1.** From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 95 on page 189).
- **2.** Double-click the Encryption service, or select the service, and then select **Action > Show Details**. The details screen for the Encryption service displays.



Figure 106 The Encryption service details screen.

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



Figure 107 The Edit Encryption Service dialog box.

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

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

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

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

Change the Encryption Password

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

- **1.** From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 95 on page 189).
- **2.** Double-click the Encryption service, or select the service, and then select **Action > Show Details**. The details screen for the Encryption service displays.

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

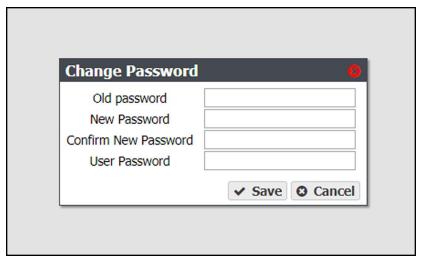


Figure 108 The Change Password dialog box.

- **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.

Unlock the Self-Encrypting Drives

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

- **1.** From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 95 on page 189).
- **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 109 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.

Create an Encryption Password USB Key

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

- **1.** From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 95 on page 189).
- **2.** Double-click the Encryption service, or select the service, and then select **Action > Show Details**. The details screen for the Encryption service displays.

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



Figure 110 The Create USB Key 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 system and store it in a safe location until it is needed.

PSID Erase an Encryption Drive

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



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

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

- **1.** From the menu bar, select **Status > Hardware** or click the Hardware pane on the Dashboard, or click the Hardware link on the status bar. The Hardware screen displays (see Figure 212 on page 315).
- **2.** Click **Data Drives**. The hardware screen refreshes and displays all disk drives present in the system.
- 3. Record the slot number and serial number for each drive you want to PSID erase.

- **4.** Power down the system as described in Reboot or Shut Down a BlackPearl System on page 339.
- **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 system as described in Power On the System on page 55.
- **9.** Log into the system as described in Log Into the BlackPearl User Interface on page 58.
- **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 212 on page 315).
- **11.**Click **Data Drives**. The hardware screen refreshes and displays all disk drives present in the system.
- **12.**On the row of the drive you want to erase, click PSID Erase. The PSID Erase dialog box displays.

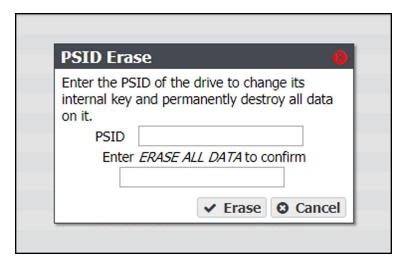


Figure 111 The PSID Erase dialog box.

- 13. Enter the PSID value you recorded in Step 6 on page 206 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 AND S3 GROUPS

Use the instructions in this section to create a new S3 user group, edit existing users, change passwords, and configure the session timeout setting.

Description of User Types

See Description of User Types on page 67 for information about each user type.

Create a User

To create a user, see Create a User on page 67.

Edit a User

There are two methods you can use to edit a user, through the User screen, or the User Profile screen.

Note: If you use the User Profile screen to edit a user, you are only able to change the password, session timeout, and full name of the user.

Using the Users Screen

1. From the menu bar, select **Configuration > Users**. The Users screen displays a list of all configured users (see Figure 22 on page 68).

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.

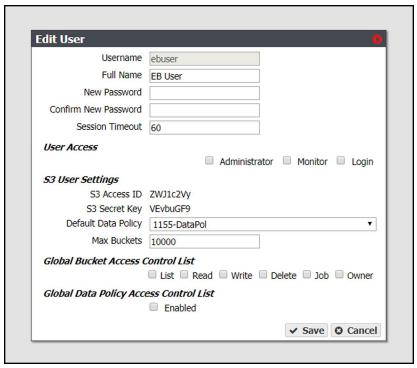


Figure 112 The Edit User dialog box.

- **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 desired **New Password**, then **Confirm New Password**.

Note: The new password does not take effect until after you log out of the BlackPearl user interface (see Exit the BlackPearl User Interface on page 341).

- **6.** If desired, edit the value for the **Session Timeout** in minutes. This value cannot exceed 999 minutes.
- **7.** Select or clear one or more **User Access** permissions. See Description of User Types on page 67 for information on each level of user access permission.
- **8.** The **S3 Access ID** and **S3 Secret Key** fields are unavailable cannot be changed when editing a user. To change the S3 secret key, see Change S3 Secret Key on page 210.
- **9.** If desired, using the drop-down menu, select a different **Default Data Policy** for the user. The system uses the selected data policy for all buckets created by the user, unless a different policy is specified during bucket creation.
- **10.** If desired, edit the value for the **Max Buckets** the user is allowed to create.

11. Select or clear options for the **Global Bucket Access Control List**. These options give or deny permission for the user being created to perform the action described in the table below, for all buckets present on the system, as well as any buckets created at a future date.

Name	Description
List	The user can see the bucket and can list the objects in a bucket.
Read	The user can get objects and create GET jobs.
Write	The user can put objects and create PUT jobs.
Delete	The user can delete objects, but cannot delete the bucket.
Job	The user can modify or cancel jobs created by other users. The user can also see the details of jobs created by other users. Note: All users can view all jobs, but by default, only the initiator of the job can see the full details of a job.
Owner	The user receives full access to all buckets, including all permissions listed above.

- **12.** Under **Global Data Policy Access Control List**, select the **Enabled** to allow the user access to any data policy created on the system.
- 13. Click Save.

Using the User Profile Screen

1. From the right side of the menu bar, select *Current User* > **User Profile**. The User Profile screen displays.

2. Select **Action >Edit**. The Edit User Screen displays.



Figure 113 The Edit User dialog box.

- 3. If desired, edit the user's Full Name.
- **4.** If you are changing the password, enter the desired **New Password**, then **Confirm New Password**.

Note: The new password does not take effect until after you log out of the BlackPearl user interface (see Exit the BlackPearl User Interface on page 341).

- **5.** If desired, edit the value for the **Session Timeout** in minutes. This value cannot exceed 999 minutes.
- 6. Click Save.

Change S3 Secret Key

If an S3 secret key is compromised, or you otherwise want to change it, use the instructions in this section to change an S3 secret key for a user. There are two methods you can use to change S3 credentials, through the User screen, or the User Profile screen.

Using the Users Screen

1. From the menu bar, select **Configuration > Users**. The Users screen displays a list of all configured users (see Figure 22 on page 68).

2. Select the user for which you want to change the S3 secret key, and then select **Action > Change S3 Secret Key**. The Change S3 Secret Key window displays.

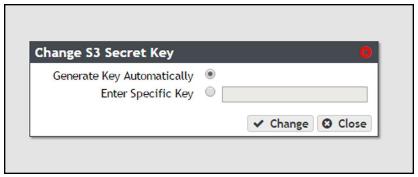


Figure 114 The Change S3 Secret Key dialog box.

- 3. Select either Generate Key Automatically or Enter Specific Key.
- **4.** Optionally, if you selected **Enter Specific Key**, enter the desired key in the entry box.
- **5.** Click **Change** to change the S3 secret key for the user.

Using the User Profile Screen

- **1.** From the right side of the menu bar, select *Current User* > **User Profile**. The User Profile screen displays.
- **2.** Select **Action > Change S3 Secret Key**. The Change S3 Secret Key window displays.



Figure 115 The Change S3 Secret Key dialog box.

- **3.** Select either **Generate Key Automatically** or **Enter Specific Key**.
- **4.** Optionally, if you selected **Enter Specific Key**, enter the desired key in the entry box.
- **5.** Click **Change** to change the S3 secret key for the user.

Create an S3 Group

An S3 group on the BlackPearl system is a group of previously created S3 users. Members of an S3 group can be individual users, or groups of users. When creating an S3 group, you specify the global bucket and data policy access control lists.

Use the instructions in this section to create a new S3 group.

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



Figure 116 The Users screen.

2. Select Action > New S3 Group from the menu bar. The New S3 Group dialog box displays.

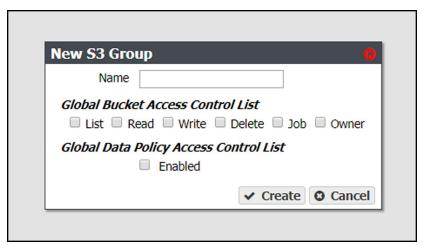


Figure 117 The New S3 Group dialog box.

- **3.** Enter the desired **Name** for the group.
- **4.** Select or clear options for the **Global Bucket Access Control List**. These options give or deny permission for the group being created to perform the action described in the table below, for all buckets present on the system, as well as any buckets created at a future date.

Note: The access control list options selected for an S3 group complement the options previously selected for each member of the group. For example, if a user has Read permission and is added to an S3 group that has Write permission, the user now has both Read and Write permissions.

Name	Description
List	The S3 group can see the bucket and can list the objects in a bucket.
Read	The S3 group can get objects and create GET jobs.
Write	The S3 group can put objects and create PUT jobs.
Delete	The S3 group can delete objects, but cannot delete the bucket.
Job	The S3 group can modify or cancel jobs created by other users. The S3 group can also see the details of jobs created by other users. Note: All users can view all jobs, but by default, only the initiator of the job can see the full details of a job.
Owner	The S3 group receives full access to all buckets, including all permissions listed above.

- **5.** Under **Global Data Policy Access Control List**, select **Enabled** to allow the user access to any data policy created on the system.
- **6.** Click **Create** to create the new S3 group.

 Use the instructions below to add groups or individual users to the S3 group.

Add a Group Member to an S3 Group

- **1.** From the menu bar, select **Configuration > Users**. The Users screen displays (see Figure 116 on page 212).
- **2.** Double-click the S3 group to which you want to add a different S3 group as a member, or select the group and from the menu bar select **Action > Show Details**.
- **3.** From the menu bar, select **Action > Add Group Member**. The Add Group Member dialog box displays.

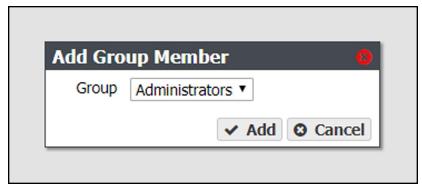


Figure 118 The Add Group Member dialog box.

- **4.** Using the **Group** drop-down menu, select the S3 group to add as a member.
- 5. Click Add.

Add a User Member to an S3 Group

- **1.** From the menu bar, select **Configuration > Users**. The Users screen displays (see Figure 116 on page 212).
- **2.** Double-click the S3 group to which you want to add an individual user as a member, or select the group and from the menu bar select **Action > Show Details.**
- **3.** From the menu bar, select **Action > Add User Member**. The Add Group Member dialog box displays.

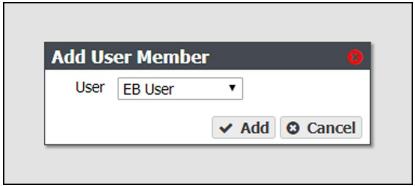


Figure 119 The Add User Member dialog box.

- **4.** Using the **User** drop-down menu, select the user to add as a member.
- 5. Click Add.

Remove an S3 Group Member

Use the following instructions to remove a group or user from an S3 group.

- **1.** From the menu bar, select **Configuration > Users**. The Users screen displays (see Figure 116 on page 212).
- **2.** Double-click the S3 group from which you want to remove an individual user or group as a member, or select the group and from the menu bar select **Action > Show Details**.
- **3.** From the menu bar, select **Action > Remove Member**. The Remove Member confirmation screen displays.
- 4. Click Delete.

Edit an S3 Group

Use the following instructions to edit an S3 group.

- **1.** From the menu bar, select **Configuration > Users**. The Users screen displays (see Figure 116 on page 212).
- **2.** Select the S3 group which you want to edit and from the menu bar select **Action > Edit**. The Edit S3 Group dialog box displays.

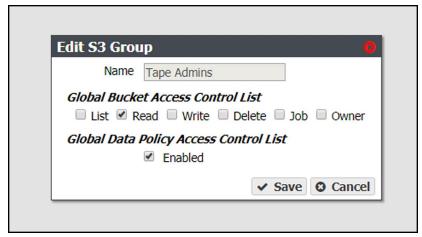


Figure 120 The Edit S3 Group dialog box.

- **3.** If desired, select or clear options for the **Global Bucket Access Control List**. These options give or deny permission for the group being created to perform the action described in the table below, for all buckets present on the system, as well as any buckets created at a future date. See Create an S3 Group on page 212 for a description of each user type.
- **4.** Under **Global Data Policy Access Control List**, select **Enabled** to allow the user access to any data policy created on the system.
- 5. Click Save.

Delete a User or S3 Group

- **1.** From the menu bar, select **Configuration > Users**. The Users screen displays a list of all configured users and S3 groups (see Figure 22 on page 68).
- **2.** Select the user or S3 group you want to delete, and then select **Action > Delete**. A confirmation window displays.
- **3.** Click **Delete** to delete the user or S3 group.

CONFIGURE CERTIFICATES

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

The BlackPearl system accepts intermediate (chain) SSL certificates, and accepts RSA, DSA, and ECC certificates. The BlackPearl system 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 121 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.

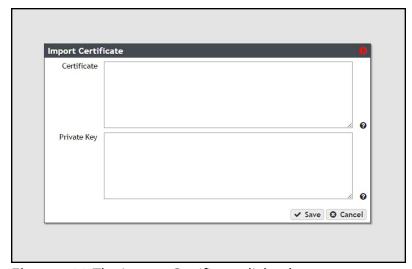


Figure 122 The Import Certificate dialog box.

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. 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 57 for instructions for importing activation keys.

Use the following instructions to manually enter activation keys.

- **1.** Determine the order for installing the activation keys.
- If this is not an initial installation, you can enter activation keys in any order. Proceed with Step 2 on page 218.
- If you want to manually enter the activation keys for an initial installation, they must be entered in the following order



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

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

Кеу Туре	Description	
EM_S3_SAS_COUNT	Enables the specified number of SAS drives present in the BlackPearl system, 44-bay, or 107-bay expansion node, if the 107-bay expansion node contains SAS drives	
EM_S3_SATA_COUNT	Enables the specified number of SATA drives present in a 96-bay or 107-bay expansion node, if the 107-bay expansion node contains SATA drives.	

Кеу Туре	Description	
EM_S3_SSD_COUNT	Enables the specified number of SSD drives present in the BlackPearl 4U system.	
EM_S3_TAPE_COUNT	Enables the specified number of tape slots present in the attached Spectra Logic or supported tape library.	

b. Product key - There is only one product key for the BlackPearl system.

Кеу Туре	Description	
EM_S3	Enables the system to use the BlackPearl interface and functionality.	

- **c.** All other keys Any additional keys included on the Software Activation Key Certificate, such as the Software Update key or the EM_NAS product key, can be entered in any order.
- **2.** Select **Support > Activation Keys** to display the Activation Keys screen. Any previously entered keys are listed.

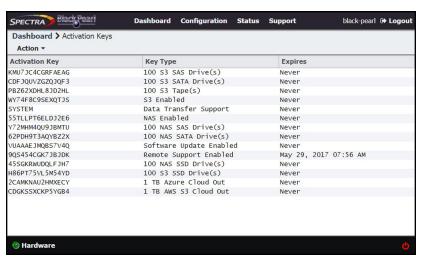


Figure 123 The Activation Keys screen.

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



Figure 124 The Enter Activation Key dialog box.

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

Chapter 7 - Configuring Network Attached Storage

This chapter describes using the optional Network Attached Storage (NAS) features. If you have not purchased a NAS activation key, these features do not display in the BlackPearl user interface.

Topic	
Overview of NAS Storage Pools, Volumes, and Shares	page 220
Storage Pools	page 221
Volumes and Shares	page 221
Naming Considerations	page 221
Create a NAS Storage Pool	page 221
Create a Volume	page 225
Create a Share	page 232
Create a CIFS Share	page 232
Create an NFS Share	page 237
Configure NAS Services	page 238
Configure the CIFS Service	page 239
Configure the NFI Service	page 240
Configure the NFS Service	page 241
Configure the NAS Replication Service	page 242

OVERVIEW OF NAS STORAGE POOLS, VOLUMES, AND SHARES

Storage pools, volumes, and shares are the logical components used to interact with the 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.

CREATE A NAS STORAGE POOL

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

- Each storage pool requires a minimum of one drive. Spectra Logic recommends using eight drives or more in a storage pool to reduce the impact of the overhead. Overhead is the space on the storage pool used to store parity data, and not used for data storage.
- Drives can only be associated with one storage pool. To create a new storage pool using drives that are already configured in an existing storage pool, you must first delete the existing storage pool as described in Delete a Storage Pool on page 251. 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 system 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 storage pool.

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

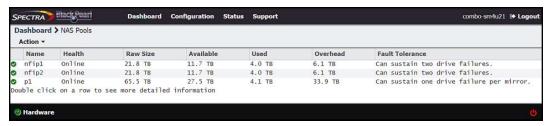


Figure 125 The NAS Pools screen.

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

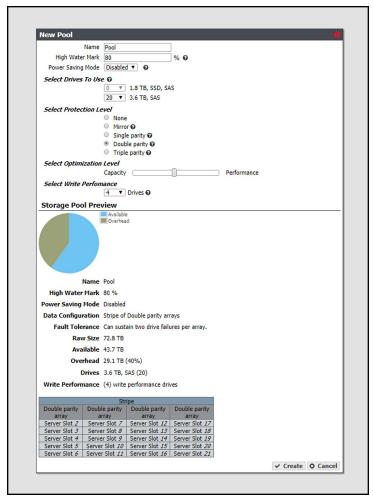


Figure 126 The New Pool dialog box.

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	
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. Note: SpectraLogic recommends leaving power saving mode disabled .
Select Drives To Use	Use the drop-down menu to select the number of drives to include in the pool. If your system contains more than one type of disk drive, multiple drop-down menus are present, but only one type can be assigned to a pool. Any drive not in a storage pool acts as a global spare. A global spare drive is activated as soon as a drive configured in a storage pool fails.

For this option	
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.

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

CREATE A VOLUME

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

Note: If you want to configure the volume to use the NFI service (Network File Interface) to automatically transfer files from the NAS storage to the local system's storage domains or to a remote BlackPearl system, configure the NFI service before configuring the volume. See Configure the NFI Service on page 240.

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

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

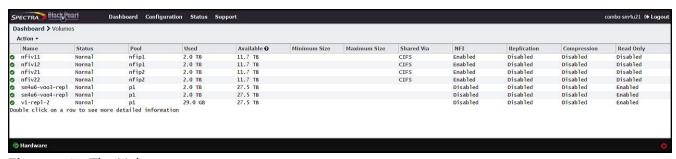


Figure 127 The Volumes screen.

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

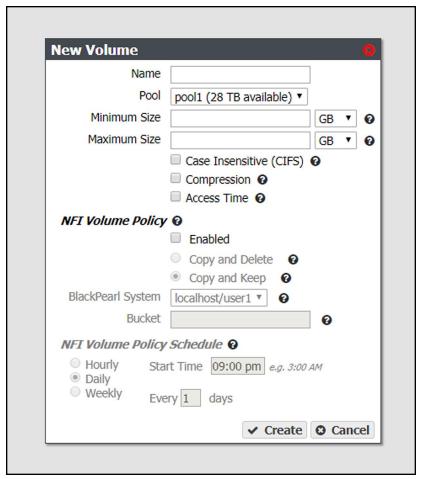


Figure 128 The New Volume dialog box.

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.

For this option	Do the following
Pool	Select the storage pool on which to create the volume. If there are multiple storage pools configured on the system, 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. Note: This option should only be used for volumes shared using CIFS and cannot be changed after creating the volume. DO NOT enable this setting if you plan to share the volume using NFS.
Compression	If desired, select the check box to enable the BlackPearl system to compress stored data. If the data being written is compressible there is an increase in write performance to the volume, which is dependent on how much compression occurs on the data being written. The data compression process uses CPU cycles to perform the compression. If compression is enabled and non-compressible data is written to the volume, the compression process may use an excessive number of CPU cycles, slowing the overall performance of the system.
Access Time	If desired, select the check box to configure the system to update the time stamp of a file when it is read from the volume. Selecting Access Time may slow performance.

Configure the NFI Volume Policy

The NFI service is used to automatically transfer files from the NAS volume to the local system's storage domains or to a remote BlackPearl system. If you do not want to configure NFI for this volume, continue with Step 4 on page 231.

- **a.** Select the **Enabled** check box to enable the **NFI Volume Policy**.
- **b.** 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.

- c. Using the drop-down menu, select a **BlackPearl System** configured in Configure the NFI Service on page 240.
- **d.** Enter the name of the **Bucket** to use to store the data on the BlackPearl system. If the bucket does not exist, it is automatically created.

Notes:

- The bucket name cannot contain a colon (:), forward slash (/), or space.
- The bucket name cannot exceed 255 characters.
- If you plan to modify files in the NAS volume you must enter the name of the bucket with a data policy that uses versioning. See Step 8 on page 134.
- 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.



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 IMPORTANT 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.

e. Configure the NFI Volume Policy Schedule:

The NFI Volume Policy Schedule transfers data from the NAS volume to a BlackPearl system at intervals based on number of hours, days, or days of the week. Decide which interval to use for the schedule and follow the appropriate instructions.

- Create an Hourly Schedule below—Transfer data every selected number of hours.
- Create a Daily Schedule on page 246—Transfer data every selected number of days.
- Create a Weekly Schedule on page 247—Transfer data on certain days of the week.

Create an Hourly Schedule

a. 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.

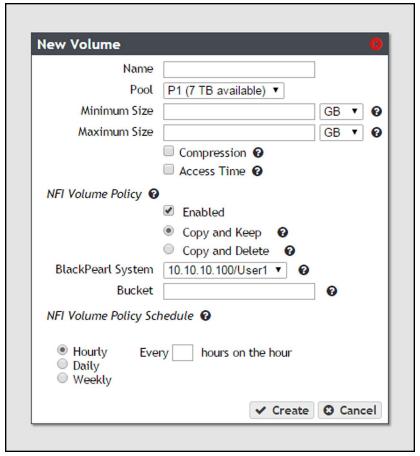


Figure 129 The New Volume dialog box showing the hourly interval options.

- **b.** Enter a number for **Every** _ **hours on the hour**. This value specifies the interval, in hours, between transferring data to the BlackPearl system. For example, if this value is set to 4, the system copies data every four hours. The maximum setting for this field is 48, where the system copies data every two days.
- **c.** Continue to Step 4 on page 231.

Create a Daily Schedule

a. 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.

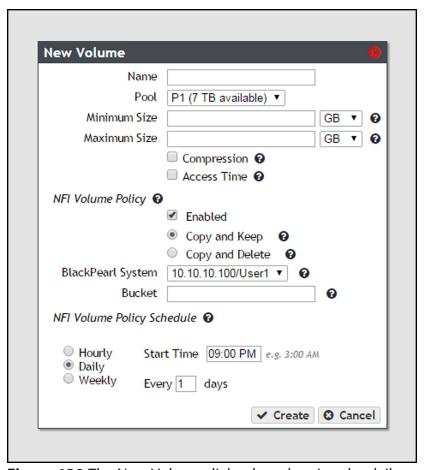


Figure 130 The New Volume dialog box showing the daily interval options.

- **b.** Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
- **c.** Enter a number for **Every** _ **days**. This value specifies the interval, in days, between transferring data to the BlackPearl system. For example, if this value is set to 2, the system copies data every two days at the time specified in Step b.
- **d.** Continue to Step 4 on page 231.

Create a Weekly Schedule

a. 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.

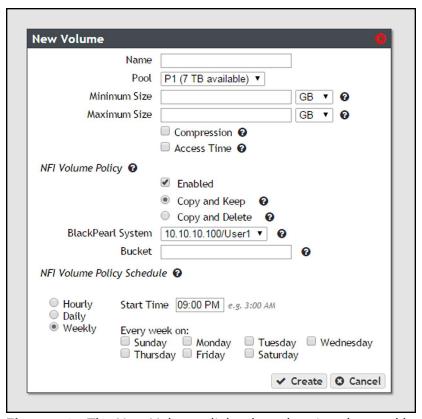


Figure 131 The New Volume dialog box showing the weekly interval options.

- **b.** Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
- **c.** Select one or more days for **Every week on:**. This determines the day(s) of each week the system copies data to the BlackPearl system.
- **4.** Click **Create**. 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 237

Note: Shares are not available until network settings are configured. See Configure the Data Connection on page 61.

Create a CIFS Share

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

Join an Active Directory Domain

If your Windows environment uses Active Directory, you must join an Active Directory domain before creating a CIFS share. See Configure the Active Directory Service on page 193 for more information.

Continue with Enable Local Administrator Status below.

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 67.

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

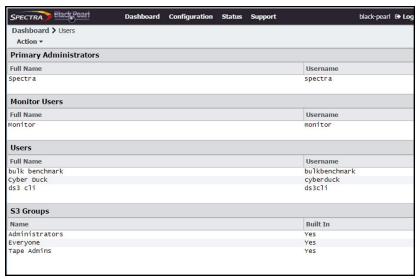


Figure 132 The Users screen.

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.

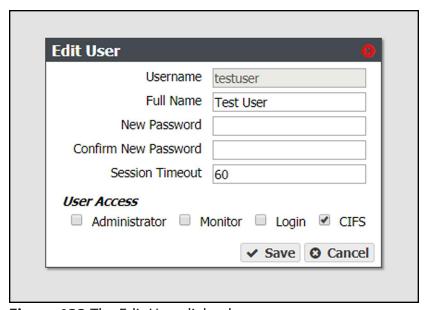


Figure 133 The Edit User dialog box.

- **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 207.
- 5. Click Save.
- **6.** Continue with Create a CIFS Share on page 234.

Create a CIFS Share

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



Figure 134 The CIFS Shares screen.

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

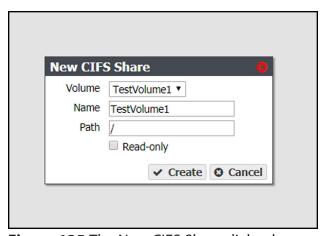


Figure 135 The New CIFS Share dialog box.

- **3.** Use the drop-down menu to select the **Volume** you want to share.
- **4.** Set the **Name** for the CIFS share. This is the name that is displayed in Active Directory configurations.

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

Note: After creating the CIFS share, you can connect to it using your Windows-based host and create subdirectories in the share. You can then edit the share and use the **Path** field to allow access to specific directories by specifying the exact subdirectory (see Edit an NFS Share on page 264).

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

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

- **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 a user creating the initial shares to easily set the proper permissions for additional users without requiring the Active Directory Domain administrator password.

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

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

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

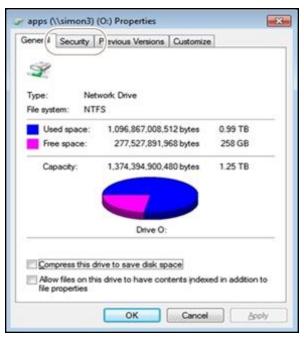


Figure 136 The Properties window.

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

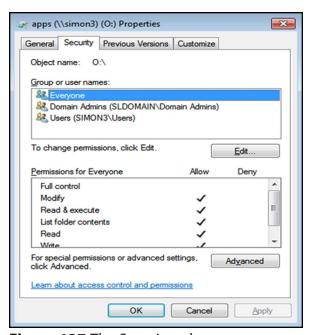


Figure 137 The Security tab.

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

Create an NFS Share

Use the following steps to create an NFS share.

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

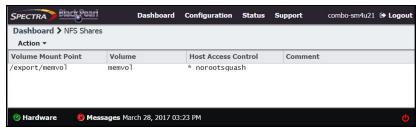


Figure 138 The NFS Shares screen.

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

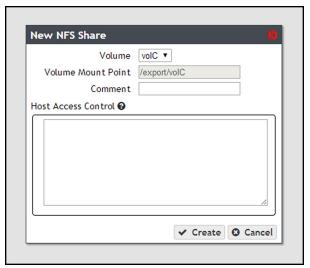


Figure 139 The New NFS Share dialog box.

- **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 Converged Storage System 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 system.

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

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

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

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

CONFIGURE NAS SERVICES

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

Note: For information about networking services see Configure Network Connections and Settings on page 178.

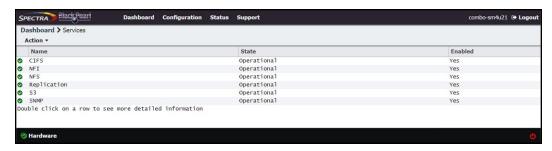


Figure 140 The Services screen.

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 232.

Add Advanced Parameter

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



Improperly configuring advanced parameters can expose security vulnerabilities **AUTION** 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 140 on page 238).
- **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.

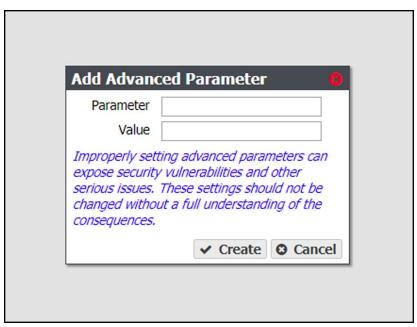


Figure 141 The Add Advanced Parameter dialog box.

- **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 system to BlackPearl managed object storage on the same system or on a remote BlackPearl system.

- **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.

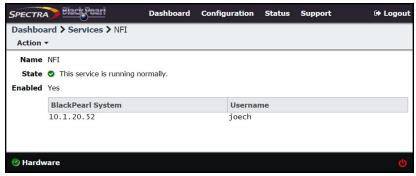


Figure 142 The NFI service details screen.

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

Configure the NFI Service to Use the local BlackPearl

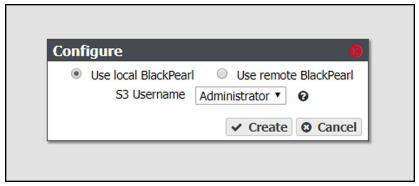


Figure 143 The Configure dialog box for a local BlackPearl.

- a. Select Use local BlackPearl.
- **b.** Using the drop-down menu, select the **S3 Username** to use for the NFI service.
- c. Click Create.

Configure the NFI Service to Use the Remote BlackPearl

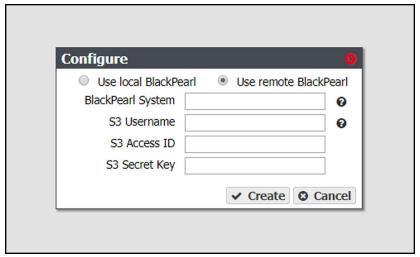


Figure 144 The Configure dialog box for a local BlackPearl.

- a. Select Use remote BlackPearl
- b. Enter the IP address or the DNS name of the data port of the BlackPearl system to which you want to connect in the BlackPearl System entry field. If you do not know the IP address or DNS name of the data port on the BlackPearl system, select Configuration > Network to view the Network screen.

Note: If your system is running BlackPearl software version 3.5.3, or later, all BlackPearl NFI targets must use BlackPearl 3.3.0, or later.

- **c.** Enter a value for the **S3 Username**. The S3 Username helps you identify the user credentials provided for the BlackPearl system.
- **d.** Enter the S3 security credentials of a user previously created on the BlackPearl system in the **S3 Access ID** and **S3 Secret Key** fields. See View S3 Credentials on page 70.
- e. Click Create.

If desired, repeat the appropriate section to configure additional BlackPearl systems or additional S3 security credentials.

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 140 on page 238).
- **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.

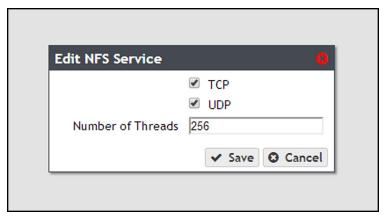


Figure 145 The Edit NFS Service dialog box.

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

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

6. Click Save.

Configure the NAS Replication Service

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

Once you configure the replication service, you need to configure each volume on the system 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 system to other systems with NAS enabled. To replicate NAS volumes to BlackPearl managed object storage use NFI (see Configure the NFI Service on page 240).
- 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 system with the volumes to replicate and the targets before you can configure replication (see Configure Ethernet Ports on page 179).
- Your firewall must allow the source system and all targets configured for replication to access port 59373 for configuring replication, and ports 59374-59400 for replication data transfers.

Configure NAS Replication

Note: For both the source system and the targets, make sure you have completed the steps in "Initial Configuration" on page 53 starting on page page 53.

- **1.** In the source system's BlackPearl user interface, select **Configuration > Services** to display the Services screen (see Figure 140 on page 238).
- **2.** Double-click the Replication service, or select the service, and then select **Action > Show Details**. The Replication service details screen displays.



Figure 146 The Replication service details screen.

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

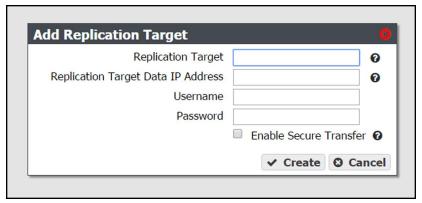


Figure 147 The Add Replication Target dialog box.

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

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

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

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

- **6.** Enter the username of a user with administrator privileges configured on the target in the **Username** field.
- **7.** Enter the user password in the **Password** field, if one is set. Otherwise, leave the field blank.
- **8.** Select the **Enable Secure Transfer** check box to configure the system to encrypt the replicated data before transferring it to the target. Data is encrypted using Secure Socket Layer (SSL).
- 9. Click Save.

Configure Volumes for NAS Replication

- **1.** In the source system'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.

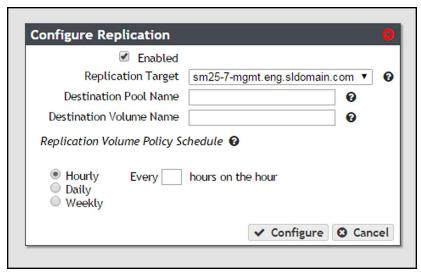


Figure 148 The Configure Replication dialog box.

- **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 244. If you only configured the system to replicate to a single target, the target is preselected.
- **6.** Enter the name of the storage pool on the target 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.



You cannot use this volume for normal data storage operations, it can only be **AUTION** used as a replication target. Any data in the specified target volume is deleted each time the system 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 below Replicate data every selected number of days.
 - Create a Weekly Schedule on page 247 Replicate data on certain days of the week.

Create an Hourly Schedule

- 1. Select Hourly as the interval for the replication schedule (see Figure 148 on page 245).
- **2.** Enter a number for **Every** _ **hours on the hour**. This value specifies the interval, in hours, between replicating data. For example, if this value is set to 4, the system replicates data every four hours.
- 3. Click Create.

Create a Daily Schedule

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

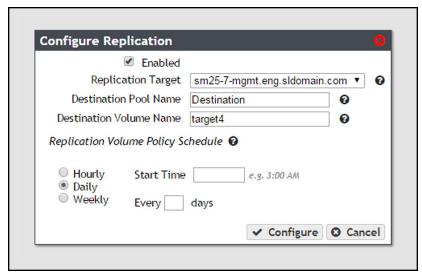


Figure 149 The Configure Replication dialog box showing the daily interval options.

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

Create a Weekly Schedule

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

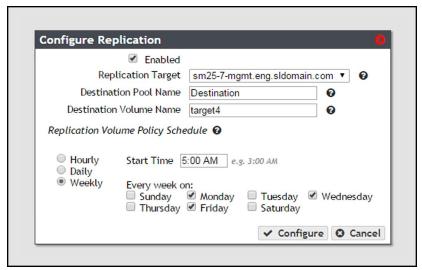


Figure 150 The Configure Replication dialog box showing the weekly interval options.

- **2.** Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
- **3.** Select one or more days for **Every week on:** This determines the day(s) of each week the system replicates data. For example, based on the selections in Figure 150, the system replicates data every Monday, Wednesday, and Friday at 5:00 AM.
- 4. Click Create.

Chapter 8 - Managing Network Attached Storage

This chapter describes using the BlackPearl user interface to manage storage pools, volumes, and shares on the system after configuring NAS. For initial NAS configuration steps, see "Configuring Network Attached Storage" on page 220 on page 220.

Topic	
Managing Storage Pools	page 249
Edit a Storage Pool	page 249
Expand a Storage Pool	page 250
Delete a Storage Pool	page 251
Managing Volumes	page 252
Move a Volume	page 252
Cancel a Volume Move	page 252
Edit a Volume	page 253
Delete a Volume	page 255
Volume Snapshots	page 255
Create a Snapshot	page 256
Create a Snapshot Schedule	page 257
Delete a Snapshot Schedule	page 259
Delete Snapshots	page 260
Restore to a Snapshot	page 262
Retrieve a Single File from a Snapshot	page 263
Managing Shares	page 263
Edit a CIFS Share	page 264
Edit an NFS Share	page 264
Delete a Share	page 265
Managing NAS Replication	page 266
Manually Start NAS Replication	page 266
Cancel a NAS Replication In Progress	page 267
Restoring Files from a NAS Replication Target	page 268

Торіс	
Disable NAS Replication for a Volume	page 268
Edit the NAS Replication Service	page 269
Delete the NAS Replication Service Configuration	page 270
Managing NFI Replication	page 271
Edit the NFI Service	page 271
Delete the NFI Service Configuration	page 272
Manually Starting an NFI Replication	page 272
Restoring Files From an NFI Target BlackPearl System	page 274

MANAGING STORAGE POOLS

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

Edit a Storage Pool

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

- **1.** From the menu bar, select **Configuration > NAS > Pools**, or click the Pools pane on the Dashboard. The NAS Pools screen displays (see Figure 125 on page 222).
- **2.** Select the pool you want to edit and select **Action > Edit**. The Edit *Pool Name* dialog box displays.

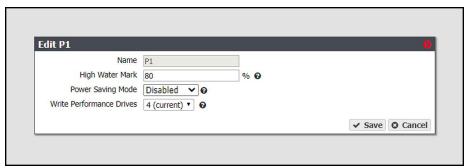


Figure 151 The Edit Pool Name dialog box.

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.

Note: SpectraLogic reccomends leaving power saving mode **disabled**.

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

Expand a Storage Pool

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

- **1.** From the menu bar, select **Configuration > NAS > Pools**, or click the Pools pane on the Dashboard. The NAS Pools screen displays (see Figure 125 on page 222).
- **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.

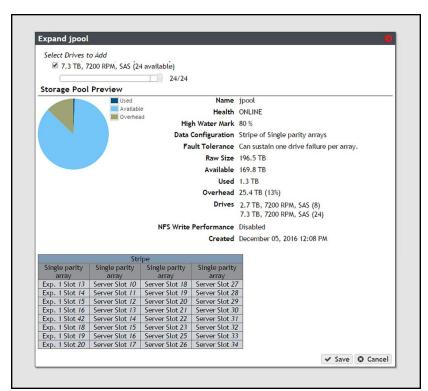


Figure 152 The Expand Pool screen.

- **3.** Select the check box next to the type of drive you want to add to the storage pool. By default, the check box for any drive type present in the system is automatically selected. Spectra Logic recommends that you avoid mixing drive types in a pool.
- **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.
- **5.** When you are satisfied with the new configuration, click **Save**.

Delete a Storage Pool

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



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 125 on page 222).
- **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 153 Confirm the storage pool deletion.

- **3.** Type DELETEin the entry field and click **Delete** to delete the storage pool.
- **4.** If desired, create a new storage pool that includes the disks no longer in use, as described in Create a NAS Storage Pool on page 221.

MANAGING VOLUMES

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

Move a Volume

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

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



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

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

- **1.** From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 127 on page 225).
- **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 154 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 127 on page 225).

- **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.

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 127 on page 225).
- **2.** Double-click the volume you want to edit, or select the volume and then select **Action > Edit**. The Edit *Volume name* screen displays.

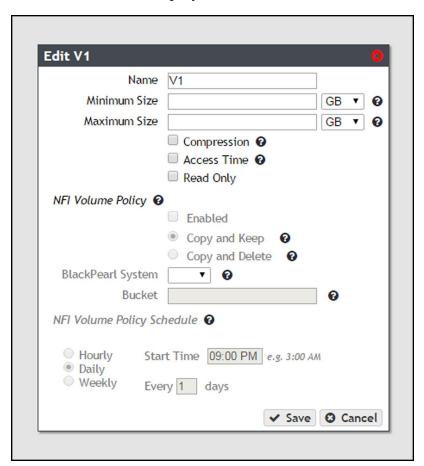


Figure 155 The Edit Volume screen.

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. 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.		
Compression	If desired, select the check box to enable the system to compress data stored in NAS. Note: Changing the compression setting only affects data written to the volume after the compression setting is changed. It does not affect data already on the volume.		
Access Time	If desired, select the check box to configure the system to update the time stamp of a file when it is read from the volume. Selecting Access Time may slow performance.		
Read Only	If desired, select the check box to configure the volume so that data can be read, but not written to the volume.		
NFI Volume Policy	If desired, edit the NFI Volume policy configurations. See Configure the NFI Volume Policy on page 228.		

Delete a Volume

Use the following steps to delete a volume.

- **1.** From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 127 on page 225).
- **2.** Select the volume you want to delete and then select **Action > Delete**. A dialog box displays asking you to confirm the deletion.



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



Figure 156 Confirm the volume deletion.

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

VOLUME SNAPSHOTS

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

Snapshots are created instantly without any impact to system performance. Snapshots initially occupy very little space on the storage pool, but grow as data is 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 Figure 127 on page 225).
- **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.

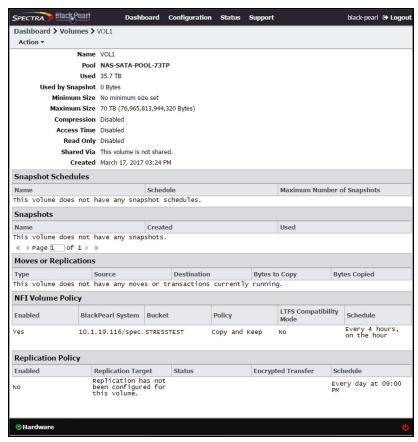


Figure 157 The Volume details screen.

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

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



Figure 158 The New Snapshot dialog box.

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

Create a Snapshot Schedule

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

- Create an Hourly Schedule below Create snapshots every selected number of hours.
- Create a Daily Schedule on page 258 Create snapshots every selected number of days.
- Create a Weekly Schedule on page 259 Create snapshots on certain days of the week.

Create an Hourly Schedule

- **1.** On the Volume details screen (see Figure 157 on page 256), 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.

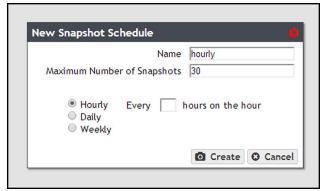


Figure 159 The New Snapshot Schedule dialog box showing the hourly interval options.

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

Create a Daily Schedule

- **1.** On the Volume details screen (see Figure 157 on page 256), 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.

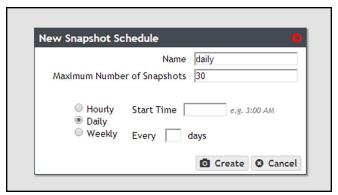


Figure 160 The New Snapshot Schedule dialog box showing the daily interval options.

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

Create a Weekly Schedule

- **1.** On the Volume details screen (see Figure 157 on page 256), 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.

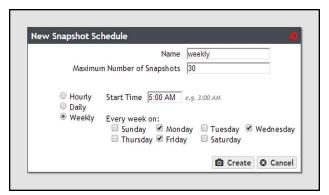


Figure 161 The New Snapshot Schedule dialog box showing the weekly interval options.

- **3.** Change the default name of the snapshot schedule, if desired.
- **4.** Enter a number for the **Maximum Number of Snapshots**. When the maximum number is reached, the system deletes the oldest snapshot.
- **5.** Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
- **6.** Select one or more days for **Every week on:** This determines the day(s) of each week the system generates snapshots. For example, based on the selections in Figure 161, the system creates a snapshot every Monday, Wednesday, and Friday at 5:00 AM.
- 7. Click Create.

Delete a Snapshot Schedule

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

Note: Deleting a snapshot schedule does not delete the snapshots previously created by the snapshot schedule.

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 127 on page 225).

- 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.

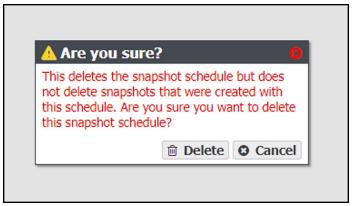


Figure 162 Confirm the snapshot schedule deletion.

4. Click Delete.

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

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 127 on page 225).

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.

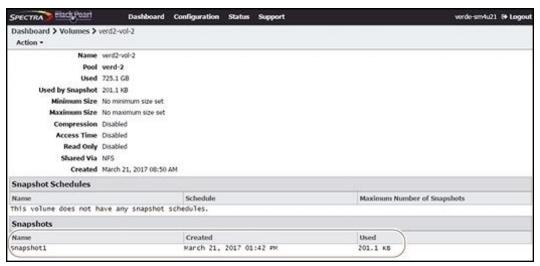


Figure 163 The Volume details screen showing a snapshot.

- **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 164 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.

- **1.** From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 127 on page 225).
- **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.

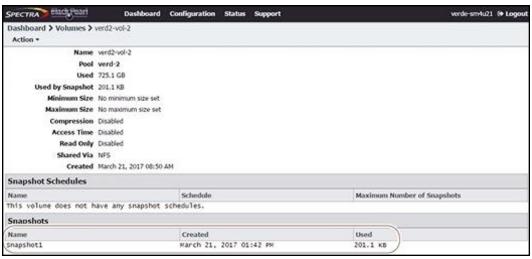


Figure 165 The Volume details screen.

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



Rollback deletes all data changes made after the snapshot was created, and AUTION 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.

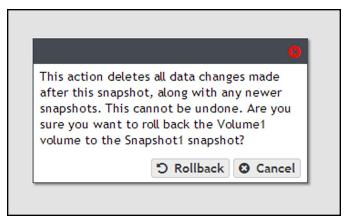


Figure 166 Confirm the volume snapshot rollback.

Retrieve a Single File from a Snapshot

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

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

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

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

Z:\zfs\snapshot\snapshot name

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

MANAGING SHARES

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

Edit a CIFS Share

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

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

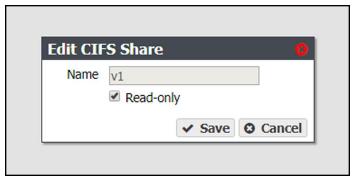


Figure 167 The Edit NFS Share dialog box.

- **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.

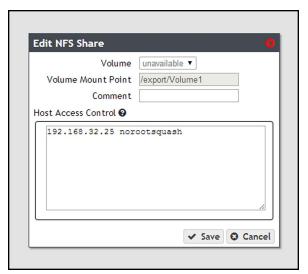


Figure 168 The Edit NFS Share dialog box.

3. Make the desired changes (see Create a Share on page 232 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.

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

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

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



Figure 169 Confirm removing the share.

MANAGING NAS REPLICATION

After configuring replication (see Managing NAS Replication on page 266), 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 system 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.** In the 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 170 The Replicate Now confirmation window.

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

- **1.** In the 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.

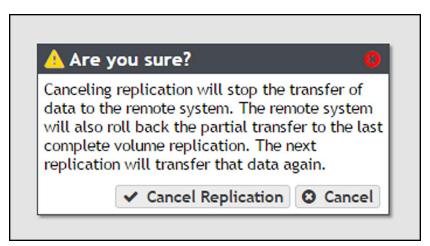


Figure 171 The Cancel Replication confirmation window.

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 system 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. 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 232 for instructions.
- **3.** If desired, write protect the replicated volume before you copy files from the volume.

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

- a. From the menu bar, select Configuration > NAS > Volumes. The Volumes screen displays.
- **b.** Select the replicated volume and select **Action > Edit**. The Edit *volume name* dialog box displays.
- **c.** Select the **Read Only** check box.
- d. Click Save.
- **4.** Using your host machine, connect to the new share on the replication target.
- **5.** Copy the needed files from the replication target share to the source system.
- **6.** If desired, stop sharing the NAS replication target volume. See Delete a Share on page 265.

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. In the 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.

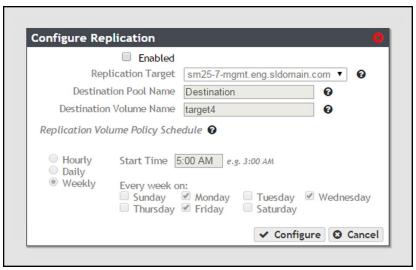


Figure 172 The Configure Replication dialog box.

- **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 system's BlackPearl user interface, select **Configuration > Services** to display the Services screen (see Figure 95 on page 189).
- **2.** Double-click the Replication service, or select the service, and then select **Action > Show Details**. The Replication service details screen displays.



Figure 173 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 174 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 system 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 system's BlackPearl user interface, select **Configuration > Services** to display the Services screen (see Figure 95 on page 189).

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



Figure 175 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 system no longer replicates data to the target.
- **5.** Repeat Step 3 and Step 4 to delete additional NAS replication targets, if desired.

MANAGING 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.

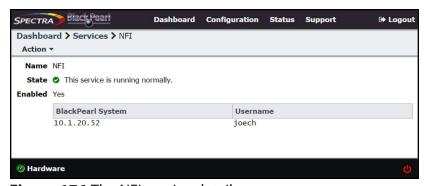


Figure 176 The NFI service details screen.

- **3.** Select **Action > Edit**. The Edit NFI dialog box displays.
- 4. Edit the settings as described in Configure the NFI Service on page 240.
- 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.

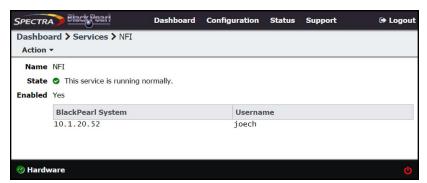


Figure 177 The NFI service details screen.

- **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 system.

- **1.** From the menu bar, select **Configuration > NAS > Volumes**, or click the Volumes pane on the Dashboard. The Volumes screen displays (see Figure 127 on page 225).
- 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 127 on page 225).

- 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.

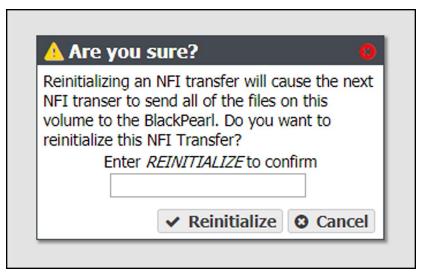


Figure 178 The Reinitialize NFI Transfer confirmation window.

4. Type REINITIALIZE in the entry field and click **Reinitialize** to reinitialize the NFI transfer.

Restoring Files From an NFI Target BlackPearl System

If files copied to the BlackPearl system using the NFI service are deleted from the NAS, you can retrieve the files from the BlackPearl storage domains using the Spectra EON Browser, Spectra Deep Storage Browser, or a Spectra S3 client. If you only need to retrieve a small number of files, Spectra Logic recommends using the EON Browser.

- For instructions for installing, configuring, and using the EON Browser, see the BlackPearl Eon Browser User Guide.
- For instructions for installing, configuring, and using the Deep Storage Browser, use the documentation provided to you when you installed the program.

Note: To retrieve a file you must use the S3 credentials for the user configured in the NFI service when starting a session in the EON Browser or Deep Storage Browser.

- If you do not know which user is configured in the NFI service, see Configure the NFI Service on page 240.
- If you do not know the S3 credentials of the user, see View S3 Credentials on page 70. It is helpful to leave the S3 Credentials dialog box open in the BlackPearl user interface, so that you can easily copy and paste the credential values when configuring the EON Browser or Deep Storage Browser.

Chapter 9 - Working with Tape Libraries and Media

This chapter describes using the BlackPearl user interface to perform tasks relating to tape libraries and tape media.

Topic	
Tape Library Barcode Reporting	page 276
Format Tapes	page 276
Cancel Tape Format	page 278
Inspect Tapes	page 278
Eject Tapes	page 280
Edit Tape Eject Information	page 281
Eject a Single Tape	page 282
Cancel Tape Ejection	page 283
Eject Tapes from a T50e or T120 Library with Multiple Partitions	page 283
Import Tapes	page 284
Import Foreign Tapes	page 284
Imported Tape Object Name Restrictions for Amazon S3 Replication	page 284
Import BlackPearl Foreign Tape(s)	page 285
Import LTFS Foreign Tape(s)	page 286
Compact a Tape Cartridge	page 288
Manage Tapes Not in Inventory	page 289
Mark Tape as Ejected	page 289
Delete Lost or Ejected Tape	page 290
Tape Library Options	page 290
Activate a Tape Library Partition	page 290
Put a Tape Library Partition into Standby	page 291
Delete a Tape Partition	page 292
Tape Drive Options	page 292

Topic	
Tape Drive Reservation	page 292
Offline a Tape Drive	page 296
Online a Tape Drive	page 297
Remove a Tape Drive from a Tape Partition	page 299
Data Migration	page 300

TAPE LIBRARY BARCODE REPORTING

Once a tape library and associated tape media are under the control of the BlackPearl system, it is important that you do not change the barcode reporting option on the Spectra Logic tape library.



IMPORTANT If you must change the barcode reporting on the tape library for any reason, contact Spectra Logic Technical Support before proceeding.

FORMAT TAPES

If you import new tapes into the library, they must be formatted before they can be used by the system. Use the instructions in this section to format tapes.

Note: If the BlackPearl system is configured to transfer data to tape, make sure the partitions configured for use by the BlackPearl system do not contain WORM (Write Once-Read Many) media. The BlackPearl system is not compatible with WORM media.

For information on increasing library capacity, and importing or exporting tape media, see your library *Tape Library User Guides*.



CAUTION Any data currently on the tape media is lost during the format operation.

Tapes are not eligible for formatting if they have a state of EJECTED, LOST, EJECT_PENDING, or OFFLINE. In addition, the **Force** parameter must be used to format a tape that contains data written by a BlackPearl system, to format a tape before it is inspected, to format a tape that has already been formatted by a BlackPearl system, or to format a tape that currently has reads or writes scheduled. If a tape contains data written by the current BlackPearl system, you must delete the objects and buckets before formatting the tape even if the force parameter is selected.

1. From the menu bar, select **Status > Tape Management**. The Tape Management screen displays. Any unformatted tapes display a state of Unknown on the Tape Management screen.

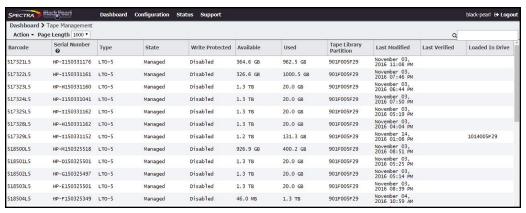


Figure 179 The Tape Management screen.

2. Select the tape cartridge you want to format and select **Action > Format Tape**, or to format all tapes with a state of Unknown, select **Action > Format All Unmanaged Tapes**. A confirmation dialog box displays.



Figure 180 The Format Tape confirmation dialog box.



Figure 181 The Format All Unmanaged Tapes confirmation dialog box.

3. If desired, select the **Force** option.

Note: If the selected tape contains data from the BlackPearl system, you cannot format the tape unless you select the **Force** option.



IMPORTANT

Do not use the **Force** option to force a format on a cleaning tape. If you do so the cleaning tape is set to "expired" and no longer usable for cleaning drives.

4. Enter FORMAT in the entry field and click **Format Tape**, or **Format All Unmanaged Tapes**. The system instructs the library to load the selected tapes into tape drives configured in the library, to format the tape(s) for LTFS. This is the format used by the BlackPearl system. This process can take up to 5 minutes per tape.

Cancel Tape Format

If desired, you can cancel a queued tape format, or cancel all queued tape formats. Use the instructions in this section to cancel one or more tape formats.

- **1.** From the menu bar, select **Status > Tape Management**. The Tape Management screen displays (see Figure 179 on page 277).
- **2.** Cancel tape format(s):
- To cancel a single tape format:
 - **a.** Select the tape row, then select **Action > Cancel Tape Format**. A confirmation window displays.
 - **b.** Click Cancel Tape Format.
- To cancel all queued tape formats:
 - **a.** select **Action > Cancel All Tape Formats**. A confirmation window displays.
 - **b.** Click Cancel All Tape Formats.

INSPECT TAPES

Tapes are normally inspected automatically by the system. If you use the tape library's user interface to move a tape cartridge in a partition associated with a BlackPearl system, the tape may transition to the Pending Inspection state (see State on page 316) and become unusable by the system. To return the cartridge to a usable state, manually request an inspection of the cartridge.

Use the instructions in this section to inspect a tape.

1. From the menu bar, select **Status > Tape Management**. The Tape Management screen displays. Any tapes requiring inspection display a state of Pending Inspection on the Tape Management screen.

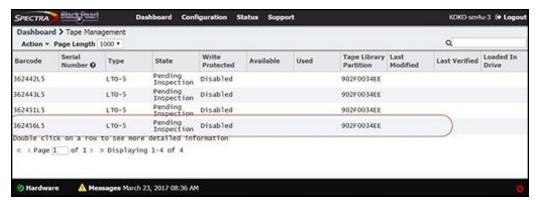


Figure 182 The Tape Management screen.

- **2.** Select the tape you want to inspect, and then select **Action > Inspect**. The Inspect Tape dialog box displays.
- **3.** Click **Inspect** to begin inspecting the tape.

EJECT TAPES

Tape media and the data they contain can be removed from the BlackPearl system by ejecting them. Once tapes are ejected from the system, they can be imported into another BlackPearl system, or stored off site.



Do not use the Spectra Logic or supported tape library front panel or RLC **IMPORTANT** connection to move tape cartridges while the tape library is under the control of the BlackPearl system.

Notes:

- Always store tapes ejected from the Spectra tape library in TeraPack® magazines. When tapes are outside the library, Spectra Logic recommends storing them in magazines with dust covers. See "Storing Cartridges" in your Spectra Logic Tape Library User Guides for more information.
- For instructions on storing tape media ejected from an IBM TS4500 tape library, see the TS4500 User Guide.
- Spectra T50e and T120 libraries must be configured in Standard eject mode in order for the BlackPearl system to automatically eject tapes. If your library has only one partition, it is already in Standard eject mode. If there is more than one partition, including a cleaning partition, in order for the BlackPearl system to automatically eject tapes you must delete partitions until only one remains, and then edit the remaining partition to use Standard mode. See your Spectra Logic Tape Library User Guides for more information on partition management. To manually eject tapes from a T50e or T120 library with multiple partitions, see Eject Tapes from a T50e or T120 Library with Multiple Partitions on page 283.
- If you plan to eject tapes to be used in a non-BlackPearl environment, see Special Considerations for Ejecting Tapes on page 80 for important information on how to configure your BlackPearl system so that tapes written by the system are readable in a non-BlackPearl environment.

Tapes are ejected one at a time. Use the following instructions to eject one or more tapes from the BlackPearl system.

Edit Tape Eject Information

If desired, you can enter information about the eject location of a tape cartridge and assign it a label before you eject the tape from the system. You are also asked to enter this information when you eject a tape.

- **1.** Select **Status > Tape Management** to display the Tape Management screen (see Figure 179 on page 277).
- **2.** Select the tape you want to eject, and then select **Action > Edit**. The Edit Tape dialog box displays.

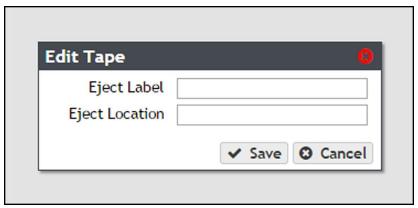


Figure 183 The Edit Tape dialog box.

- **3.** Enter information in the **Eject Label** and **Eject Location** fields. This information is stored on the BlackPearl database and is visible when re-importing the tape into a BlackPearl system.
- 4. Click Save.

Eject a Single Tape

Ejecting a tape moves that tape to the Entry/Exit pool of a Spectra Logic tape library, or the I/O slots of an IBM tape library. Any objects on the exported tape are inaccessible until the tape is re-imported into a storage pool.

- **1.** Select **Status > Tape Management** to display the Tape Management screen (see Figure 179 on page 277).
- **2.** Select the tape you want to eject, and then select **Action > Eject Tape**. The Eject Tape dialog box displays.



Figure 184 The Eject Tape dialog box.

- **3.** If desired, enter information in the **Eject Label** and **Eject Location** fields. This information is stored on the BlackPearl database and is visible when re-importing the tape into a BlackPearl system. You are not required to enter this information.
 - **Note:** If you previously entered information for this tape cartridge, prior to ejecting it, as described in Edit Tape Eject Information on page 281, that information is displayed in the entry fields automatically.
- **4.** Click **Eject**. The tape is marked as ejected in the BlackPearl system database, and moved the Entry/Exit pool of a Spectra Logic tape library, or the I/O slots of an IBM tape library. Consult your *Tape Library User Guides* for instructions on exporting tape media from the library.

Cancel Tape Ejection

If you requested a tape eject but it has not yet started, you can cancel the ejects in progress. Any tapes not already moved to the Entry/Exit pool of a Spectra Logic tape library, or the I/O slots of an IBM tape library are left in the storage partition and are usable by the BlackPearl system. Any tapes that were moved to the Entry/Exit pool or I/O slots must be exported from the library and re-imported as described in Import Tapes on page 284.

- **1.** Select **Status > Tape Management** to display the Tape Management screen (see Figure 179 on page 277).
- **2.** Cancel the ejection:
 - To cancel all tape ejections, select Action > Cancel All Ejects.
 - To cancel a single tape ejection, select the tape for which you want to cancel the ejection, and then select **Action > Cancel Tape Eject**.

Eject Tapes from a T50e or T120 Library with Multiple Partitions

If a T50e or T120 library with multiple partitions is associated with a BlackPearl system, you cannot use the BlackPearl system to eject the tapes because of the library's shared eject port. In this situation, use the following steps to eject tapes.

- **1.** Use the library's front panel to eject the tapes. See "Export Specific Cartridges from the Library" in the *Spectra T120 User Guide* or "Create a Move Queue" in the *Spectra T50e User Guide* for instructions.
- **2.** Mark the tapes as ejected in the BlackPearl user interface. See Mark Tape as Ejected on page 289.

IMPORT TAPES

Use the instructions in this section to import tape media into the BlackPearl system database.

- **1.** Import the tape media into the Entry/Exit pool of a Spectra Logic tape library, or the I/O slots of an IBM tape library associated with the BlackPearl system as described in your *Tape Library User Guides*.
- **2.** Select **Status > Tape Management** from the menu bar. The Tape Management screen displays (see Figure 179 on page 277).
- **3.** Select **Action > Online All Tapes**. A confirmation window displays.
- **4.** Click **Online All Tapes**. The tapes present in the Entry/Exit pool of a Spectra Logic tape library, or the I/O slots of an IBM tape library are physically moved into the library storage pool and display on the Tape Management screen.
 - If you imported new media, the tape cartridges need to be formatted as described in Format Tapes on page 276.
 - If you imported media previously exported from the BlackPearl system, it is automatically assigned to the bucket to which it was previously associated. The objects stored on the tape media are immediately available for retrieval.



If the bucket associated with the imported tape media no longer exists, the tape cartridges are marked for formatting and reclaimed by the system.

IMPORT FOREIGN TAPES

When inspecting tapes in the tape library, if the BlackPearl system determines that one or more tape cartridges have been previously used in a different BlackPearl system or a different LTFS system, the system marks those tapes as BlackPearl foreign or LTFS foreign. Importing foreign tapes imports the selected tape cartridges into the BlackPearl database.

Imported Tape Object Name Restrictions for Amazon S3 Replication

If you plan migrate data from foreign tapes to an Amazon S3 target, the object names on foreign tape media must conform to the naming convention restrictions of an Amazon S3 target.

The following characters are not compatible with Amazon S3 targets. Any object using one of these characters prevents the object from migrating to the Amazon S3 target.

- Backslash (\)
- Left curly bracket ({)
- Right curly bracket (})
- Caret (^)
- Percent character (%)
- Grave accent / back tick (`)
- Right square bracket (])
- Left square bracket ([)
- Quotation marks ("")
- Greater Than symbol (>)
- Less Than symbol (<)
- Tilde (~)
- Pound / hash tag character (#)
- Vertical bar / pipe (|)
- Non-printable ASCII characters (128–255 decimal characters)

Import BlackPearl Foreign Tape(s)

Use the instructions in this section to import BlackPearl foreign tapes.

Note: If one or more buckets being imported does not already exist, the data policy, storage domain, and user to use for any new buckets must be specified.

1. Select **Status > Tape Management** from the menu bar. The Tape Management screen displays.

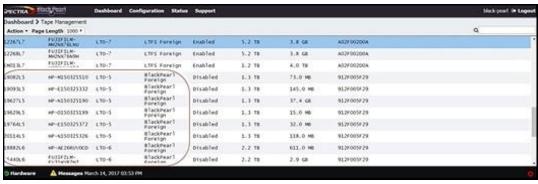


Figure 185 The Tape Management screen with BlackPearl foreign tapes listed.

2. Select Action > Import All Foreign BlackPearl Tapes or select the individual BlackPearl foreign tape that you want to import, and select Action > Import Foreign Tape. The Import Foreign BlackPearl Tape or Import All Foreign BlackPearl Tapes dialog box displays. The import settings are the same for importing a single tape or all BlackPearl foreign tapes.

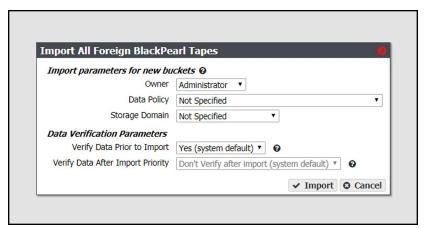


Figure 186 The Import Foreign BlackPearl Tape dialog box.

- **3.** Using the **Owner** drop-down list, select a user from the list of previously created users to be the owner of all buckets on the foreign tape.
- **4.** Using the **Data Policy** drop-down list, select a data policy from the list of previously created data policies for all buckets on the foreign tape.
- **5.** Using the **Storage Domain** drop-down list, select a storage domain from the list of previously created storage domains for all buckets on the foreign tape.
- **6.** Using the **Verify Data Prior to Import** drop-down list, select whether or not to verify the data on the media before importing.
- **7.** Using the **Verify Data After Import Priority** drop-down list, select whether or not to verify the data on the media after importing. This setting makes imported foreign options available, and schedules a verify job with the selected priority at a later time.

Note: This option is unavailable if you selected **Verify Data Prior to Import** in Step 6.

- 8. Click Import. The foreign tape is imported into the BlackPearl system.
- 9. Repeat Step 2 through Step 8 to import additional BlackPearl foreign tapes.

Import LTFS Foreign Tape(s)

Importing LTFS tape media must be done while the Intelligent Object Management (IOM) service is disabled. See Configure the Spectra S3 Service on page 189 for instructions on disabling the IOM service.

After you finish importing foreign LTFS tape media, you can re-enable IOM, which may trigger the creation of missing copies of files as required by the associated data policy. After the LTFS import completes, you can manually start an IOM migration.

Note: The BlackPearl system and Spectra Logic make a best effort to import foreign LTFS tapes. The BlackPearl support contract does not guarantee import of, nor cover any issues while importing foreign LTFS tapes. For the subset of LTFS tapes that cannot be imported, the Spectra Logic Professional Services team can help with the migration process.

Use the instructions in this section to import LTFS foreign tapes.



LTFS foreign tapes must have the physical write-protect tab set in the "write-IMPORTANT" protected" position before you import them into the BlackPearl system. Tapes not set to write protected are not imported.

- 1. **Disable** the IOM service as described in Configure the Spectra S3 Service on page 189.
- **2.** Select **Status > Tape Management** from the menu bar. The Tape Management screen displays.

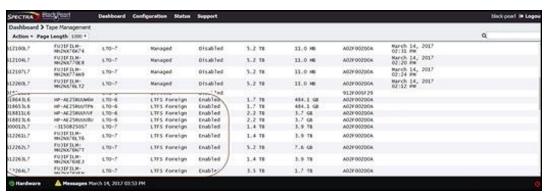


Figure 187 The Tape Management screen with LTFS foreign tapes listed.

3. Select **Action > Import All Foreign LTFS Tapes** or select the individual foreign tape that you want to import, and select **Action > Import Foreign Tape**. The Import Foreign LTFS Tape or Import All Foreign LTFS Tapes dialog box displays. The import settings are the same for importing a single tape or all LTFS foreign tapes.

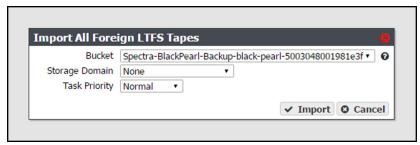


Figure 188 The Import All Foreign LTFS Tapes dialog box.

4. Using the **Bucket** drop-down list, select the bucket into which to import the LTFS foreign tape(s).

Note: The bucket must have a data policy including a persistence rule for a tape storage domain, or the import fails.

- **5.** If the bucket's data policy includes dual copy on tape, use the **Storage Domain** dropdown list to specify into which storage domain to import the tape.
- **6.** Using the **Task Priority** drop-down list, select the priority for the import process. The priority determines the job order and resources.
- **7.** Click **Import**. The foreign LTFS tapes are imported into the BlackPearl system.
- **8.** After the import completes, enable the IOM service as described in Configure the Spectra S3 Service on page 189.



If you import additional LTFS foreign tapes at a later date, you must disable **IMPORTANT** IOM again before the import operation, and enable it after the import is complete.

COMPACT A TAPE CARTRIDGE

If a tape partition is configured to automatically compact tapes, but you want a specified tape cartridge to be compacted before it is normally selected for tape compaction, you can force the BlackPearl system to compact a tape cartridge into the next tape compaction cycle.

Use the instructions in this section to add a tape cartridge to the next auto compaction cycle.

1. Select **Status > Tape Management** from the menu bar. The Tape Management screen displays (see Figure 179 on page 277).

2. Select the tape cartridge you want to add to the compaction cycle, and select **Action > Compact Tape**. The Compact Tape dialog box displays.



3. In the entry field, enter COMPACT TAPE, and click **Compact**. The tape cartridge is added to the next auto compaction cycle.

MANAGE TAPES NOT IN INVENTORY

Additional functions of the Tape Management screen allow you to mark a tape missing from the tape library inventory as ejected, and to delete lost or ejected tapes.

Mark Tape as Ejected

If you export a tape cartridge from the tape library inventory before ejecting the tape from the BlackPearl system, the tape displays as "Not in Inventory" on the Tape Management screen. If you cannot, or do not want to re-import the tape into the tape library, use the instructions in this section to mark the tape as "Ejected".

- **1.** Select **Status > Tape Management** from the menu bar. The Tape Management screen displays (see Figure 179 on page 277).
- **2.** If desired, edit the tape eject information as described in Edit Tape Eject Information on page 281.
- Select the tape with a status of "Not in Inventory" and selectAction > Mark Tape Not In Inventory As Ejected. A confirmation window displays.
- **4.** In the confirmation window, click **Confirm**. The Tape Management screen updates the tape status to "Ejected".

Delete Lost or Ejected Tape

If desired, you can delete tape cartridges that are lost or were ejected from the library so that they no longer display on the Tape Management screen. This is useful if you ejected tapes and do not plan to ever use them again with the BlackPearl system.

Note: If you re-import a tape that you previously marked as deleted, the tape has a status of "Foreign". See Import Foreign Tapes on page 284 for more information.

Use the instruction in this section to delete a lost or ejected tape from the BlackPearl database.

- **1.** Select **Status > Tape Management** from the menu bar. The Tape Management screen displays (see Figure 179 on page 277).
- **2.** Select the tape with a status of "Not in Inventory" and select **Action > Delete Lost or Ejected Tape**. A confirmation window displays.
- **3.** In the confirmation window, click **Delete**. The system deletes the tape from the database and it no longer displays on the Tape Management screen.

TAPE LIBRARY OPTIONS

The following sections describe putting a tape library or tape drive into standby, and deleting an existing tape partition.

Activate a Tape Library Partition

If you add a new tape library to your BlackPearl system, or your existing tape library has completed service, you must activate the tape partition in the BlackPearl user interface before the system is able to transfer data to the tape library.

Note: With BlackPearl software version 5.2 or earlier, if there was an inventory change in the tape library while in standby, the BlackPearl system may react by re-inspecting all tapes in the library. Starting with BlackPearl version 5.3, the system no longer re-inspects tapes when there is an inventory change while the partition is in standby if the S3 service is set to "Never Inspect".

Use the instructions in this section to activate a tape library.

Note: If you are activating a new tape library, you must create a partition on the library so that the BlackPearl system can automatically detect the new tape library.

1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).

2. Select the tape partition in the Tape Partitions pane, and select **Action > Activate Tape Partition**. The Activate Tape Partition confirmation window displays.



Figure 189 The Activate Tape Partition confirmation window.

3. Click **Activate**. The tape partition is activated and is usable by the BlackPearl system.

Put a Tape Library Partition into Standby

If you need to perform service on the tape library associated with your BlackPearl system, you must first put the tape library into a standby state. Otherwise, the BlackPearl system may attempt to use the tape library while it is in service. Putting the tape library into standby allows you to service the tape library without disconnecting the interface cables between the tape library and the BlackPearl system.

Note: After the tape partition is placed in standby, any currently running tape operations continue until they are complete, which may take 30 mintues or longer.

Use the instructions in this section to put a tape library partition into standby.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Select the tape partition in the Tape Partitions pane, and select **Action > Put Tape Partition in Standby**. The Put Tape Partition in Standby confirmation window displays.



Figure 190 The Put Tape Partition in Standby confirmation window.

3. Click **Deactivate**. The tape partition enters the standby state.

Note: If you have multiple partitions in the same tape library configured for use by the BlackPearl system, you must repeat steps Step 2 on page 291 and Step 3 for each partition in the tape library that requires service.

Note: After the tape partition is placed in standby, any currently running tape operations continue until they are complete, which may take 30 minutes or longer.

Once you complete service on the tape library, return the tape library to service using the steps in Activate a Tape Library Partition on page 290.

Delete a Tape Partition

If desired, you can delete a specified existing tape partition from the BlackPearl system. Any tapes in the partition that contain data are disassociated from the partition. Any tapes without data on them and all tape drives associated with the partition are deleted from the BlackPearl system configuration. This request is useful if the partition should never have been associated with the BlackPearl system or if the partition was deleted from the library.

Note: You must put the tape partition into standby before you can delete the tape partition. See Put a Tape Library Partition into Standby on page 291 for more information.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Select the tape partition that you want to delete and select **Action > Delete**. A confirmation window displays.
- **3.** Enter DELETE in the entry box.
- 4. Click Delete.

TAPE DRIVE OPTIONS

The following sections describe reserving tape drives, setting a drive to an online or offline state, and removing a tape drive from a partition.

Tape Drive Reservation

Tape drive reservation allows you to control how the tape drives are used to transfer data, by dedicating drives to accept only read commands or write commands, and to accept only jobs of a specified priority level or higher. With a large number of tape drives, using drive reservation can increase efficiency and reduce latency when either reading or writing data. Reserving tape drives for either reading or writing, or for a specified job priority level, is not required and is typically only used when read or write throughput and drive availability are important enough to dedicate tape drives to that function.

Note: Tape drive reservation is not recommended for BlackPearl systems connected to two or fewer tape drives.

Tape drive reservation is configured on both the drive, and library partition level.

- When reserving an individual tape drive, you can exclude the drive from performing reads, writes, or jobs lower than a specified level.
- You can also configure the library partition to reserve a specified number of drives for either reads or writes. This can prevent individual tape drive failures, or unavailable drives, from impacting the desired number of drives available for either read or write commands.

Note: Tape drives always allow inspection and verify tasks.

Drive Reservation Best Practices

If a BlackPearl system tape partition only has a small number of tape drives, reservations may not improve the overall performance, but may cause greatly reduced performance if a tape drive fails or goes offline. On a larger tape system, using drive reservation can increase efficiency and reduce latency when either reading or writing data.

It is a best practice to always have two tape drives available for writes to allow the system additional tape failure handling retry logic.

When reserving an individual tape drive, setting the Minimum Task Priority to normal excludes low priority jobs, such as default IOM jobs, from using that tape drive. It also excludes all low priority jobs which may include write or read jobs, which may not be desired if IOM management is the primary use case.

Some BlackPearl workflows and use cases place more importance on ensuring data is written into tape storage as quickly as possible in a very predictable manner. In these use cases, reserving a majority of the tape drives for writes ensures those tape drives are not interrupted or used by reads from a GET job. For example, if there are seven tape drives in a BlackPearl system with a 20 (or more) disk drive cache pool, reserving four of the tape drives for writes provides maximum throughput for writes. Those four tape drives cannot be used for GET or restore jobs that need to read data from tape.

For use cases where restoring data is more critical, using tape partition drive reservation is best. For example, if there are seven tape drives in a BlackPearl system with a 20 (or more) disk drive cache pool, the tape partition can reserve a minimum number of drives for read operations to five. Setting the policy to capacity mode, and enabling minimize spanning will also help increase overall read performance. These settings will generally restrict the write throughput on BlackPearl system to a single tape drive (or two drives for dual copy), making the effective sustained write performance on the BlackPearl system approximately 300 MBps. This leaves approximately 500 MBps worth of available throughput in the cache to be used for reads across the five reserved tape drives. This available bandwidth is spread across the five tape drives, which the BlackPearl system can utilize to restore subsets of data spread across a large number of tapes.

Tape Partition Drive Reservation

If desired, you can reserve a specified number of tape drives for read or write operations by editing the library partition.

By setting drive reservation on the tape partition instead of individual drives, it can prevent individual tape drive failures, or unavailable drives, from impacting the desired number of drives reserved for either read or write commands.

Note: Reserving drives in a tape partition does not allow you to specify which specific drive(s) are reserved for read or write operations. To reserve a specific drive in the library, see Individual Tape Drive Reservation on page 295.

Use the instructions in this section to reserve drives in a partition.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- 2. Select the tape partition that contains the drive(s) you want to reserve or make available in the Tape Partitions pane, and select Action > Show Details. The Tape Partition details screen displays.
- **3.** Select **Action > Edit**. The Edit dialog box displays.



Figure 191 The Edit dialog box.

- **4.** If desired, edit the number of drives you want to reserve for read operations in the Minimum Read Reserved Drives. Alternatively, click the up and down arrows in the entry field (not shown).
 - **Note:** Drives reserved for a read operations are occasionally used for background operations or tape inspection, but are never used for write operations.
- **5.** If desired, edit the number of drives you want to reserve for write operations in the **Minimum Write Reserved Drives**. Alternatively, click the up and down arrows in the entry field.
 - **Note:** Drives reserved for a write operations are occasionally used for background operations or tape inspection, but are never used for read operations.
- **6.** Select or clear **Automatic Tape Compaction**. When selected, the system automatically reclaims unused tape space caused by deleted objects that still reside on a tape.
 - **Note:** In addition to selecting Automatic Tape Compaction, IOM must be enabled for the automatic tape compaction process to run. See Configure the Spectra S3 Service on page 189 for information on configuring IOM.
- **7.** Click **Save**.

Individual Tape Drive Reservation

If desired, you can reserve a specified tape drive in an existing library partition to dedicate the drive to either read or write operations, or to make the drive available for both types of operations. You can also choose to reserve a drive for operations at or above a configured priority.



Do not change the Minimum Task Priority when there are active jobs in IMPORTANT progress. If you set the priority higher than the priority of active jobs to tape, those jobs do not complete.

- From the menu bar, select Configuration > Advanced Bucket Management > Storage & **Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Select the tape partition that contains the drive(s) you want to reserve in the Tape Partitions pane, and select **Action > Show Details**. The Tape Partition details screen displays.

3. Select the tape drive you want to reserve in the Tape Drives pane, and select **Action > Reserve Tape Drive**. The Reserve Tape Drive dialog box displays.

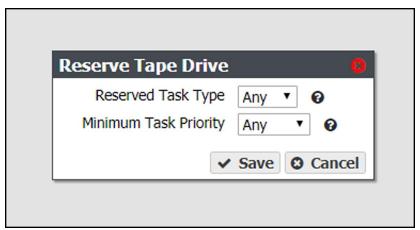


Figure 192 The Reserve Tape Drive dialog box.

- **4.** Using the **Reserve Task Type** drop-down menu, select the type of operation for which you want to reserve the tape drive:
 - Select **Read** to reserve the drive for read operations and exclude allowing PUT job write tasks from using that drive.
 - Select **Write** to reserve the drive for write operations and exclude allowing GET job read tasks from using that drive.
 - Select Any to make the drive available for both read and write operations.

Note: Tape drives always allow inspection and verify tasks.

5. Using the **Minimum Task Priority** drop-down menu, select the Minimum Task Priority; the drive is reserved for tasks at or above the selected priority.

Note: When reserving an individual tape drive, setting the Minimum Task Priority to normal excludes low priority jobs such as default IOM jobs from using that tape drive, which may not be desired if IOM management is the primary use case. It also excludes all low priority jobs which may include write or read jobs.

6. Click Save.

Offline a Tape Drive

If you need to perform service on a tape drive in the tape library associated with your BlackPearl system, you must first offline the tape drive. Otherwise, the BlackPearl system may attempt to use the tape drive while it is in service.

Use the instructions in this section to offline a tape drive.

- 1. From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Select the tape partition that contains the drive you want to offline in the Tape Partitions pane, and select **Action > Show Details**. The Tape Partition details screen displays.

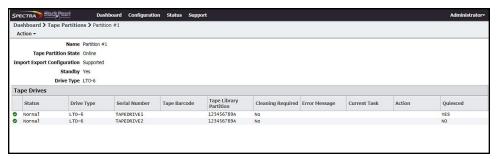


Figure 193 The Tape Partition details screen.

3. Select the tape drive you want to offline in the Tape Drives pane and select **Action > Offline Tape Drive**. The Offline Tape Drive confirmation window displays.



Figure 194 The Offline Tape Drive confirmation window.

4. Click **Deactivate**. The tape drive is now offline.

Once you complete service on the tape drive, make the tape drive available to the BlackPearl system using the steps in Online a Tape Drive on page 297.

Online a Tape Drive

If you add a new tape drive to a partition in your tape library, or finish service on an existing tape drive, you must online the tape drive in the BlackPearl user interface before the system is able to transfer data to the tape drive.

Tape drives appear offline for two different reasons. Either a user set a drive to be offline in the BlackPearl user interface, or the BlackPearl system is unable to communicate with the drive in the tape library.

- Drives that are offline with a Quiesced value of "Yes" were either manually set to offline by a user, or the BlackPearl system detected an error condition that was caused by a drive failure, and marked the drive as offline and quiesced it to prevent further use by the BlackPearl system.
- Offline drives with a Quiesced value of "No" indicate that the BlackPearl system cannot communicate with the drive. Examine your tape library to determine the cause of the problem, or contact Spectra Logic Technical Support (see "Contacting Spectra Logic" on page 8).

Use the instructions in this section to online a tape drive.

Note: If you are activating a new tape drive, you must configure the drive in a partition on the library so that the BlackPearl system can automatically detect the new tape drive.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Select the tape partition that contains the drive you want to online in the Tape Partitions pane, and select **Action > Show Details**. The Tape Partition details screen displays.



Figure 195 The Tape Partition details screen.

3. Select the tape drive you want to online in the Tape Drives pane, and select **Action > Online Tape Drive**. The Online Tape Drive confirmation window displays.



Figure 196 The Online Tape Drive confirmation window.

4. Click **Activate**. The tape partition is now online and is usable by the BlackPearl system.

Remove a Tape Drive from a Tape Partition

If desired, you can delete a specified tape drive in a tape library partition.

Note: Removing a drive makes the drive inaccessible to the BlackPearl system. It has no effect on the tape library configuration.

- **1.** From the menu bar, select **Configuration > Advanced Bucket Management > Storage & Policy Management** to display the Advanced Bucket Management screen (see Figure 31 on page 108).
- **2.** Select the tape partition that contains the drive you want to remove in the Tape Partitions pane, and select **Action > Show Details**. The Tape Partition details screen displays.

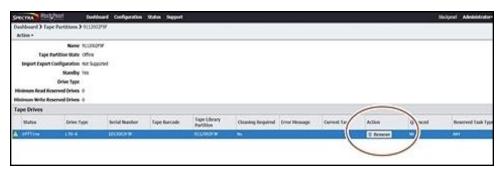


Figure 197 The Tape Partition details screen.

- **3.** Click **Remove** on the row of the tape drive you want to remove from the tape partition. A confirmation window displays.
- 4. Click Delete.

DATA MIGRATION

If desired, you can migrate data from one technology to another within a storage domain. This migration method is only available for permanent copies of data. The BlackPearl system supports the following data migration:

- Tape to tape
- · Disk to disk
- Disk to tape
- Tape to tape

The instructions below describe migrating data from a storage domain member using one tape technology to a storage domain member using a different tape technology. However, the process is similar for any of the above listed migration types.

Use the instructions in this section to migrate data.



This process assumes that all required data policies, data persistence rules, storage domains, and storage partitions are already configured on the BlackPearl system. If you need to create any of the above, use the instructions in "Configuring Advanced Bucket Management" on page 106.

- **1.** If necessary, create a tape partition that contains the new media technology (see Create a Tape Partition on page 114). This is the **target tape** partition.
- 2. If ejecting the older generation of tapes is desired, in the BlackPearl user interface, select **Status > Tape Management** to navigate to the tape management screen and make a note of all tape barcodes associated with the storage domain.
- **3.** Add the **target tape** partition to the storage domain as a storage domain member (see Add a Storage Domain Member to a Storage Domain on page 129).
- **4.** In the same storage domain, select the **source tape** storage domain member from which you want to migrate data and select **Action > Exclude**. The **source tape** storage domain member now displays "exclusion in progress".
- **5.** Select **Status > S3 Jobs** to examine the S3 Jobs screen and verify the IOM read and write operations are initiated. Wait until all operations complete.
- **6.** Manually create a database backup (see Manually Generate a Database Backup on page 335). The data migration is now complete.
- **7.** If desired, using the list of tapes you recorded in Step 2, eject tapes from the **source tape** partition (see Eject Tapes on page 280).

Chapter 10 - Operating the BlackPearl System

This chapter describes procedures for day-to-day monitoring and operation of the Spectra BlackPearl Converged Storage System.

Topic	
S3 Operations	page 302
Download an Object	page 302
Cancel Spectra S3 Jobs	page 303
Edit an S3 Job	page 304
Clear All Canceled or Completed Jobs	page 305
Manually Starting the S3 Data Path Backend	page 306
Disallow New Jobs	page 306
Allow New Jobs	page 307
Monitor the BlackPearl System	page 308
Front Bezel Visual Status Beacon	page 309
Configuring the Visual Status Beacon Color	page 310
System Status LEDs	page 310
Check System Messages	page 313
View the Status of Hardware Components	page 314
View the Status of Services	page 316
View the Status of the System Pools	page 317
View Bucket Contents	page 319
View Spectra S3 Jobs Information	page 320
View Tape Media Information	page 322
View Performance Metrics	page 327
View Reports	page 329
Database Backup & Restore	page 330
Create a Database Backup Schedule	page 331
Manually Generate a Database Backup	page 335

Topic	
Restore from a Database Backup	page 335
Delete Backup	page 337
Edit Backup Data Policy	page 338
Show Backup Physical Placement	page 338
Reboot or Shut Down a BlackPearl System	page 339
Using the BlackPearl User Interface	page 339
Power-Cycle Reset	page 341
Exit the BlackPearl User Interface	page 341

S3 OPERATIONS

Use the instructions in this section to manually download an object, cancel an S3 job, or to manually start the datapath backend.

Download an Object

Objects present on the BlackPearl system can be downloaded using the BlackPearl user interface, a Spectra S3 client, or the Spectra Eon Browser. For information on using the Spectra Eon Browser, see the BlackPearl Eon Browser User Guide.

Use the instructions in this section to download an object through the BlackPearl user interface.



The object must be a single blob. If blobbing is enabled for the data policy **IMPORTANT** and the object is greater than the maximum blob size, the object must be downloaded through a Spectra S3 client or the Spectra Eon Browser.

Note: Only one object can be selected for download at a time.

1. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 31 on page 108).

2. Double-click the bucket that contains the object you want to download. The Bucket Details screen displays a list of all objects in the bucket.

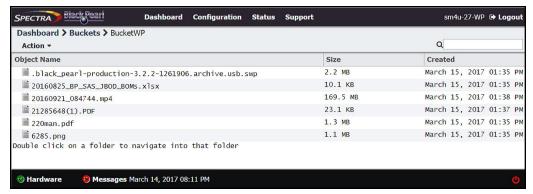


Figure 198 The Bucket details screen.

3. Select the object you want to download, and select **Action > Download**. The object begins downloading through your web server.

Cancel Spectra S3 Jobs

You can use the BlackPearl user interface to cancel an in-progress Spectra S3 job, or to cancel all S3 jobs, instead of using your Spectra S3 client.

Use the instructions in this section to cancel a Spectra S3 job(s).

1. From the menu bar, select **Status > S3 Jobs** to display the S3 Jobs screen.



Figure 199 The S3 Jobs screen.

- **2.** Cancel one or more in-progress jobs.
 - **a.** Select the job to cancel and then select **Action > Cancel** or select **Action > Cancel All Jobs**. The Cancel Job or Cancel All Jobs screen displays.



Figure 200 The Cancel Job screen.

- **b.** Optionally, select **Delete Uploaded Objects** to delete any objects associated with a current in-progress PUT job that are already uploaded to the system.
- c. Click Yes to cancel all S3 jobs, or the individual selected S3 job.

Edit an S3 Job

If desired, you can edit the name and priority level of an active S3 job. Use the instructions in this section to edit the name or priority of a Spectra S3 job(s).

Note: You cannot edit completed jobs.

1. From the menu bar, select **Status > S3 Jobs** to display the S3 Jobs screen.

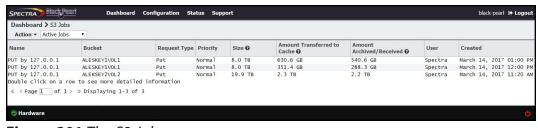


Figure 201 The S3 Jobs screen.

2. Select the row of the S3 job for which you want to change the name, and select **Action > Edit Job**. The Edit Job dialog box displays.

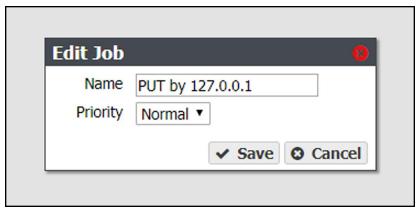


Figure 202 The Edit Job dialog box.

- **3.** Enter the desired Name.
- **4.** Using the drop-down menu, select the job **Priority**.
- 5. Click Save.

Clear All Canceled or Completed Jobs

If desired, you can clear completed or canceled jobs from the BlackPearl user interface.

1. From the menu bar, select **Status > S3 Jobs** to display the S3 Jobs screen.

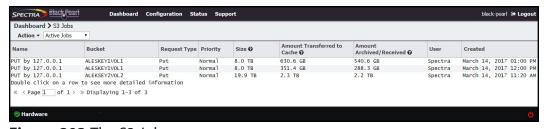


Figure 203 The S3 Jobs screen.

- **2.** Clear canceled or completed jobs:
 - To clear all canceled jobs, select **Action > Clear All Canceled Jobs.**
 - To clear all completed jobs, select **Action > Clear All Completed Jobs.**
- 3. A confirmation window displays. Click Clear to confirm clearing the jobs.

Manually Starting the S3 Data Path Backend

If the BlackPearl system is powered off for longer than the timeout value specified in the S3 service options, the data path backend must be manually started. Use the instructions in this section to manually start the data path backend.

- **1.** From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 95 on page 189).
- **2.** Double-click the S3 service, or select the S3 service and select **Action > Show Details**. The S3 details screen displays.
- **3.** On the S3 service details screen, select **Action > Activate Data Path Backend**. The Activate Data Path Backend confirmation window displays.



Figure 204 The Activate Data Path Backend screen.

4. Click Activate.

Disallow New Jobs

If desired, you can stop the BlackPearl system from accepting new S3 jobs.

- **1.** From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 95 on page 189).
- **2.** Double-click the S3 service, or select the S3 service and select **Action > Show Details**. The S3 details screen displays.

3. On the S3 service details screen, select **Action > Disallow New Jobs**. The Disallow New Jobs confirmation window displays.



Figure 205 The Disallow New Jobs confirmation window.

4. Click Submit.

Allow New Jobs

If you have configured the BlackPearl system to no longer accept new S3 jobs, use the instructions in this section to configure the system to allow new jobs.

- **1.** From the menu bar, select **Configuration > Services** to display the Services screen (see Figure 95 on page 189).
- **2.** Double-click the S3 service, or select the S3 service and select **Action > Show Details**. The S3 details screen displays.
- **3.** On the S3 service details screen, select **Action > Allow New Jobs**. The Allow New Jobs confirmation window displays.



Figure 206 The Allow New Jobs confirmation window.

4. Click Submit.

MONITOR THE BLACKPEARL SYSTEM

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 system and its components.

- The Visual Status Beacon light bar in the front bezel changes color to indicate the current status of the system (see Front Bezel Visual Status Beacon on page 309).
- System messages provide important information about the BlackPearl system and its operation (see Check System Messages on page 313 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 314 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 316).
 - View the status of the database and cache (see View the Status of the System Pools on page 317).
 - View performance metrics for the drives, CPUs, cache, and network (see View Performance Metrics on page 327).
 - View the current network configuration settings (see Configure Network Connections and Settings on page 178).
 - View the status of any Spectra S3 jobs running on the system (see View Spectra S3 Jobs Information on page 320).
 - View the status of media in the associated tape library (see View Tape Media Information on page 322).
 - Reboot or shutdown the system (see Reboot or Shut Down a BlackPearl System on page 339).

Front Bezel Visual Status Beacon

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

Color Display	Condition
Purple Scroll	The system is operating normally. Note: The color displayed when the system is operating normally can be changed on the Hardware screen. See Configuring the Visual Status Beacon Color on page 310 for more information.
Yellow Scroll	The system is experiencing a Warning condition. Log in to the BlackPearl user interface to determine the cause of the warning.
Red Scroll	The system is experiencing an Error condition. Log in to the BlackPearl user interface to determine the cause of the error.
Orange Scroll	The system is experiencing a move failure in the attached tape library. Log in to the BlackPearl user interface to determine the cause of the error.
Rainbow	The system is currently powering on and performing self-tests.
Flashing Blue	The beacon feature was activated for this system. This can help you identify a specific system when you have more than one system in your environment.
Pulsing Red	The Visual Status Beacon lost communication with the system. This can occur if the system experiences a software hang.
No Light	The BlackPearl system 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 system is configured to display a purple scrolling light on the Visual Status Beacon when the system 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.

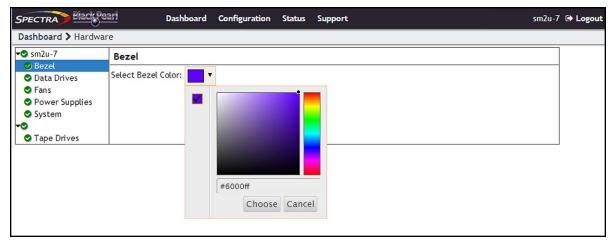


Figure 207 Use the color picker to set the color of the Visual Status Beacon when the system is operating normally.

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

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

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

System Status LEDs

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

Gen2 X Series Chassis

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



Figure 208 The top left section of the front of the Gen2 X chassis 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 365 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

Gen1 S Series and V Series Chassis

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

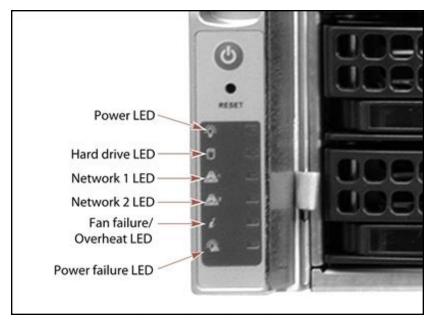


Figure 209 The left side of the front of the Gen1 S Series chassis showing system status LEDs.

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 34.
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 system. If the problem persists, contact Spectra Logic Technical Support. See Contacting Spectra Logic on page 8.
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 system 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:

Туре	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 system may occur.
Warning	Notifies the user of a failure that may adversely impact the BlackPearl system.
Critical	Notifies the user of a failure that caused significant adverse impact to the BlackPearl system.

If any system messages are generated by the system, 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.

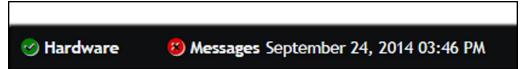


Figure 210 A system message displayed on the BlackPearl user interface status bar.

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.

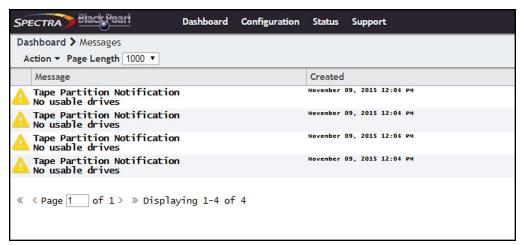


Figure 211 The Messages screen.

Pay extra attention to any messages flagged with the Warning or Error icon (see Status Icons on page 51), and follow any recommended steps. Contact Spectra Logic Technical Support if you need assistance (see Contacting Spectra Logic on page 8).

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

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

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

View the Status of Hardware Components

The BlackPearl user interface lets you monitor the status of hardware components in the system, and the connected library tape drives, without having direct physical access. This is especially useful when your BlackPearl system 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.

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.

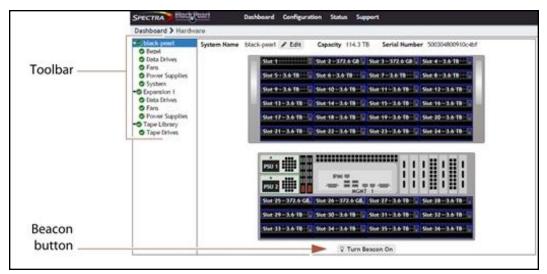


Figure 212 The Hardware screen. Gen1 S Series 4U chassis shown.

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 51 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 309 for more information about the colors displayed by the Visual Status Beacon.
Data Drives	 Slot number of each drive Status of each drive Drive size, serial number, and firmware level The name of the cache to which the drive is assigned
Fans	Status of midplane fans
Power Supplies	• Power supply status and wattage Note: Power supply information is not available for the 107-bay expansion node.
System	 CPU status and temperature System memory status and size Status, manufacturer, model, size, and serial number for each boot drive
Tape Drives	Status of tape drives in the tape library connected to the system

Clicking	Shows the
Turn Beacon On	Click Turn Beacon On to cause the Visual Status Beacon light on a BlackPearl system to flash blue. This is useful when you have multiple systems and need to locate a specific one, for example to replace a component. Click the button a second time to stop the light from flashing.

View the Status of Services

The Services screen provides status information about services that are currently installed on the BlackPearl system.

From the menu bar, select **Configuration > Services** to display the Services screen.



Figure 213 The Services screen.

The Services screen displays the following information:

This column	Shows
Name	The name of the service running on the system.
State	The status of the service on the BlackPearl Converged Storage System system. • Starting—The service is starting up. • Operational—The service is running. • Stopped—The service is not running.
Enabled	 Whether or not the service is enabled at system startup. Yes—Service automatically starts when the system is powered on. No—Service does not start when the system is powered on.

View the Status of the System Pools

The System Pools pane of the Advanced Bucket Management screen provides status information about the database and cache pools configured on the BlackPearl system, as well as status information for each system pool.

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

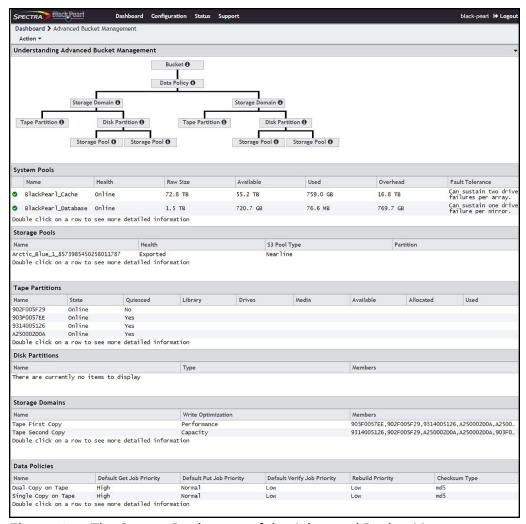


Figure 214 The System Pools pane of the Advanced Bucket Management screen.

The System Pools pane displays the following information.

This column	Shows
Name	The name of each system pool. This name cannot be edited.
Health	The current health of each system 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 system pool.
Available	The amount of unused storage space in each system pool.
Used	The amount of used storage space in each system pool.
Overhead	The amount of disk space used for overhead, such as parity data.
Fault Tolerance	The fault tolerance setting for each system pool.

2. To view additional information about a system pool, select the system pool and then select **Action > Show Details**. The *system pool name* details screen displays.

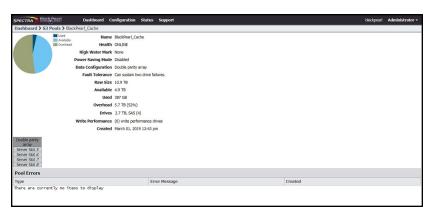


Figure 215 The BlackPearl_Cache details screen.

The system pool name details screen displays the following information:

This row	Shows
Name	The name of the pool. This name cannot be edited.
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.

This row	Shows
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.
Pool Errors	Gives details of pool errors if any.

View Bucket Contents

Use the instructions in this section to view the contents of a bucket configured on the BlackPearl system.

1. From the menu bar, select **Configuration > Buckets**. The Buckets screen displays (see Figure 50 on page 143).

2. Double-click the name of the bucket for which you want to view the contents. The details screen for the bucket displays.

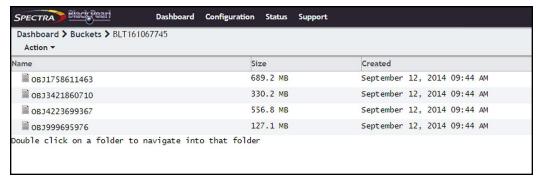


Figure 216 The details screen for a selected bucket.

The bucket details screen displays the following information for each object contained in the bucket:

This row	Shows
Object Name	The name of an object in the specified bucket.
Size	The size of the object.
Created	The timestamp of when the object was written to the bucket.

View Spectra S3 Jobs Information

The S3 Jobs screen displays the status of all Spectra S3 jobs the system is currently processing, all canceled jobs, and all completed jobs.

From the menu bar, select **Status > S3 Jobs** to display the S3 Jobs screen.

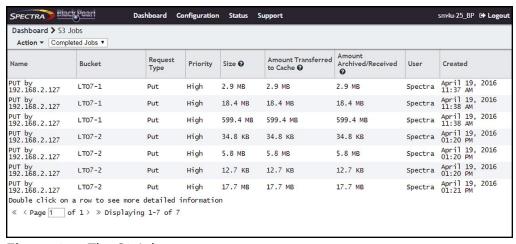


Figure 217 The S3 Jobs screen.

Use the job status drop-down menu to select **Active Jobs**, **Canceled Jobs**, or **Completed Jobs** as desired.

The S3 Jobs screen displays the following information:

This column	Shows
Name	The name of the job request, which is generated automatically using the job request type and IP address of the source or destination host. Note: Multiple jobs of the same request type from the same host IP address all have the same name.
Bucket	The name of the bucket that is acted on by the job request. Note: Jobs created from standard S3 PUT and GET requests do not display a bucket name in the S3 Jobs screen.
Request Type	If the job is a "PUT" (write), "GET" (read), or "VERIFY (verify) operation.
Priority	The priority for processing the job. The job priority determines the resources assigned and the processing order. Values: Critical, Urgent, High, Normal, Low, Background .
Size	The amount of data to be transferred by the job.
Amount Transferred to Cache	The amount of data that was transferred to the cache for this job. For PUTs, this is the amount of data successfully transferred to the system from the client. For GETs, this is the amount of data either in cache originally, or loaded into cache from tape. For VERIFY jobs, this is the amount of data loaded into cache from the permanent data store.
Amount Archived/Received	The amount of data that is completely processed for this job. For PUTs, this indicates the amount of data written to tape media. For GETs, this indicates the amount of data that was read successfully by the client. For VERIFY jobs, this is the amount of data loaded into cache from the permanent data store.
User	The S3 user that initiated the job.
Created	The timestamp of when the job was created.
Date Canceled (Canceled jobs only)	The timestamp of when the job was canceled.
Date Completed (Completed jobs only)	The timestamp of when the job completed.

View Tape Media Information

The Tape Management screen allows you to view the status of all tapes in the associated Spectra Logic or supported tape library, or in a specified bucket.

- 1. Display the Tape Management Screen:
- To view the status of all tapes in the associated tape library, from the menu bar, select **Status > Tape Management.** The Tape Management screen displays.

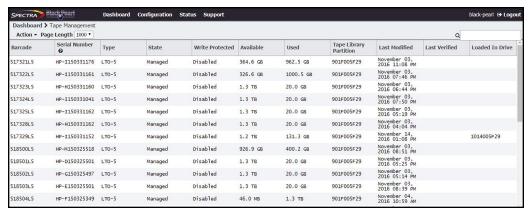


Figure 218 The Tape Management screen.

- To view the status of the tapes associated with a bucket:
 - **a.** From the menu bar, select **Configuration > Buckets**. The Buckets screen displays.
 - **b.** Select the bucket for which you want to view the tape media information, and select **Action > Show Physical Placement**. The Physical Placement screen displays.

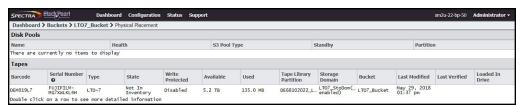


Figure 219 The Physical Placement screen showing the storage pools and tapes for a specified bucket.

The Tape Management and Physical Placement screens display the following information:

This column	Shows
Barcode	The barcode label on the tape cartridge.
Serial Number	The tape manufacturer serial number for the tape cartridge.

This column	Shows
Туре	The media type. Values: LTO-5, LTO-6, LTO-7, LTO-7 Type M, LTO-8, TS1140, TS1150, TS1155, TS1160
State	The status of the tape: During normal operation, the tape state is MANAGED. Other possible states are: • NORMAL— The tape is ready for use. • AUTO COMPACTION IN PROGRESS — The tape is in the process of having unused tape space, due to deleted objects that still reside on a tape, reclaimed. • BAD — The tape has been identified as bad due to I/O errors or too many write cycles. • BAR CODE MISSING — The barcode for the tape is unknown or missing. • CANNOT FORMAT DUE TO WRITE PROTECTION — The tape is write-protected and cannot be formatted. • DATA CHECKPOINT FAILURE — The tape should have data on it that is recognizable to the BlackPearl system, but the system could not verify that the data on the tape is at the correct checkpoint or there was an error rolling back to a checkpoint. • DATA CHECKPOINT FAILURE DUE TO READ ONLY — The tape should have data on it that is recognizable to the BlackPearl system, but the system could not verify that the data on the tape is at the correct checkpoint or there was an error rolling back to a checkpoint because the tape is read only. • DATA CHECKPOINT MISSING — The tape should have data on it that is recognizable to the BlackPearl system, but the checkpoint containing the data could not be found on the tape. • EJECT FROM EE PENDING — The tape is in the Entry/Exit (E/E) pool waiting to be physically ejected. • EJECT TO EE IN PROGRESS — The tape is currently being moved to the E/E pool. • EJECT TO EE IN PROGRESS — The tape is currently being formatted. • FORBIGN — A tape from another BlackPearl system. This data must be copied into a bucket on this system before it is accessible. • FORMAT IN PROGRESS — The tape is currently being formatted. • FORMAT IN PROGRESS — The tape is currently being inported into a bucket on this system before it is accessible. • FORMAT IN PROGRESS — The tape is currently being formatted. • IMPORT PENDING — A FOREIGN tape is in the process of being imported into a bucket. • IMPORT PENDING — A FOREIGN tape is not supported by the BlackPearl

This column	Shows
State	 LTFS WITH FOREIGN DATA — An LTFS formatted tape not associated with a BlackPearl system. This data must be copied into a bucket on this system using a raw import before it is accessible. OFFLINE — The tape is in the E/E pool and requires user confirmation to move it to the storage pool and make it online. ONLINE IN PROGRESS — The tape is in the process of being moved from the E/E pool to the storage pool. When complete, its state will change to PENDING INSPECTION. ONLINE PENDING — The tape was OFFLINE and received user confirmation to bring it online, but this action has not yet begun. PENDING INSPECTION — The tape has not yet been inspected. RAW IMPORT IN PROGRESS — The data on an LTFS formatted tape not associated with a BlackPearl system is being imported into the BlackPearl system. RAW IMPORT PENDING — An LTFS formatted tape not associated with a BlackPearl system is queued to have the data it contains imported into the BlackPearl system. SERIAL NUMBER MISMATCH — The tape serial number does not match the one stored in the BlackPearl system. UNKNOWN — The tape contains unknown data or is otherwise unavailable to the BlackPearl system.
Write Protected	The status of the write-protect switch on the cartridge.
Available	The amount of unused space that is available for data on the tape cartridge.
Used	The amount of space on the tape cartridge containing data.
Tape Library Partition	The serial number of the partition on the Spectra Logic or supported tape library containing the tape cartridge.
Storage Domain	The storage domain to which the tape is assigned.
Bucket	The bucket to which the tape is assigned.
Last Modified	The timestamp of the last time data was written to the tape cartridge.
Last Verified	The timestamp of the last time data was verified on the tape cartridge, by either a manual verification, or when the number of days specified in the storage domain that owns the tape passed.

This column	Shows
Loaded In Drive	The BlueScale serial number of the tape drive in which the tape cartridge is loaded.

2. To display detailed information about a tape cartridge, double click the tape cartridge row. A details screen for the selected tape displays.

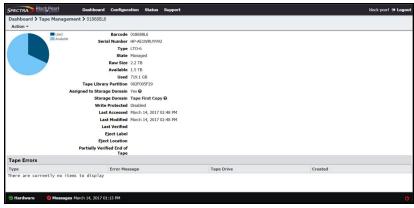


Figure 220 The details screen for a selected tape.

The details screen for a selected tape cartridge displays the following:

This row	Shows	
Barcode	The barcode label on the tape cartridge.	
Serial Number	The manufacturer assigned serial number for the tape cartridge.	
Туре	The media type. Values: LTO-5, LTO-6, LTO-7, LTO-7 Type M, LTO-8, TS1140, TS1150, TS1155, TS1160	
State	The status of the tape. See State on page 323 for a list of tape cartridge states.	
Raw Size	The raw size of the tape.	
Available	The amount of unused space that is available on the tape cartridge.	
Used	The amount of space on the tape containing data.	

This row	Shows
Tape Library Partition	The serial number of the partition on the Spectra Logic or other supported tape library containing the tape cartridge.
Assigned to Storage Domain	Whether the tape is allocated to a storage domain. Values: Yes , No
Storage Domain	The storage domain to which the tape is assigned.
Bucket	The bucket to which the tape is assigned.
Write Protected	The status of the write-protect switch on the cartridge.
Last Accessed	The timestamp of the last time the tape was loaded into a tape drive.
Last Modified	The timestamp of the last time data was written to, or read from, the tape cartridge.
Last Verified	The timestamp of the last time data was verified on the tape cartridge, by either a manual verification, or when the number of days specified in the storage domain that owns the tape passed.
Eject Label	A user-defined label entered when the tape is ejected.
Eject Location	A user-defined label entered when the tape is ejected.
Partially Verified End of Tape	The timestamp of the last time the system verified the data on the specified percentage of the tape before the end of data.

If there are any tape errors associated with the specified cartridge, they display in the **Tape Errors** pane of the details screen.

The following commands are available from the **Action** menu on the tape cartridge details screen. Use the links below for more detailed information about each command.

- **Edit** See Edit Tape Eject Information on page 281.
- **Eject Tape** See Eject Tapes on page 280.
- Cancel Tape Eject See Cancel Tape Ejection on page 283.
- **Format Tape** See Format Tapes on page 276.

View Performance Metrics

The Performance screen displays performance metrics for the BlackPearl cache, 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**. The Performance screen displays.

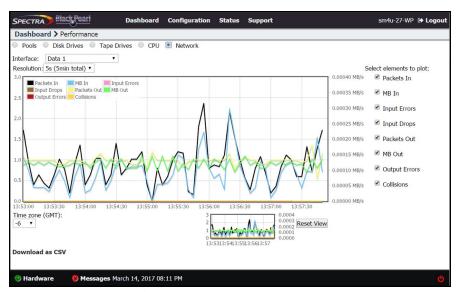


Figure 221 The Performance screen.

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

Note: If you select **Pools**, **Disk Drives**, **Tape Drives**, or **Network**, use the **Pool**, **Disk Drive**, **Tape Drive**, or **Interface** drop-down menu to select a specific pool, disk drive, tape 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.

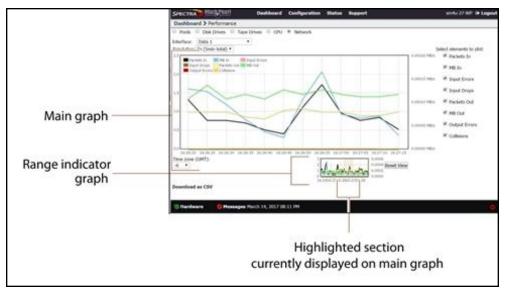


Figure 222 Highlight a section of data to show in greater detail.

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 system, 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.

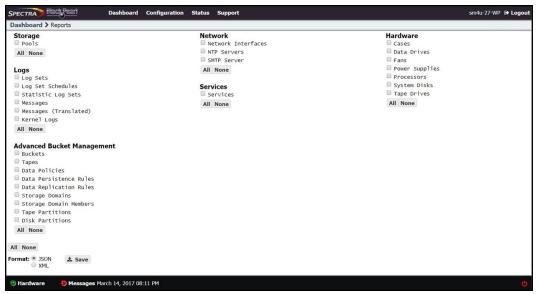


Figure 223 The Reports screen.

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.

DATABASE BACKUP & RESTORE

The BlackPearl system database contains a list of all objects stored on the system cache, tape, and disk media. Backing up the database allows you to restore the database in the event of hardware failure. The database backup does not function as a true backup in that it does not backup or restore objects referenced in the database, only the database itself.

When restoring a database, the system is not aware of any changes to data after creating the database backup.

- Files that exist in the database, but were deleted after the creation of the database backup are not restored.
- New files added or modified after the creation of the database backup are still persisted on a storage medium.

Verify disk pools and tape media so that the database synchronizes with the actual data present on the system.

Database backups are stored on a bucket on the BlackPearl system, and kept based on the settings of a preconfigured data policy named "Database Backup".

Note: If your BlackPearl system does not contain a tape library, the database backup policy must be manually created.

If desired, you can modify the settings of the preconfigured data policy, or create a new data policy for database backups (see Create a Data Policy on page 131). If you create a new data policy, you will need to edit the database backup configuration to use the new policy (see Edit Backup Data Policy on page 338).

Note: Spectra Logic recommends using the default data policy.

The bucket used for database backups is automatically created when the first backup is generated, either manually, or on a schedule. The database backup bucket is listed on the Buckets screen of the BlackPearl user interface with the name "Spectra-BlackPearl-Backup-system name-product serial number". This bucket cannot be used for data storage.

Note: If you change the system name after the database backup bucket is created, the bucket name does not change.

Backups can be generated manually, or by schedule. When creating a database backup schedule, you specify how many copies of the database to keep at one time. When the system generates a backup that exceeds the value configured, the oldest database backup is automatically deleted.

Note: The default schedule on the BlackPearl system generates a backup once per day, and retains a maximum of two backups.



Creating a backup of the database is a process intensive procedure. Spectra Logic recommends configuring a backup schedule to run during periods of low system activity. Additionally, creating only one backup a day is recommended.

Note: If your BlackPearl system does not contain any permanent local storage, the database backup file must be downloaded manually to your host computer.

Create a Database Backup Schedule

Database backup 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 backups every selected number of hours.
- Create a Daily Schedule on page 332—Create backups every selected number of days.
- Create a Weekly Schedule on page 333—Create backups on certain days of the week.

Create an Hourly Schedule

- **1.** From the menu bar, select **Configuration > Database Backup.** The Database Backup screen displays (see Figure 227 on page 335).
- 2. Select Action > Change Schedule. The Modify Database Backup Schedule screen displays.

3. Select **Hourly**. The Modify Database Backup Schedule screen changes to display the options for an hourly backup schedule.

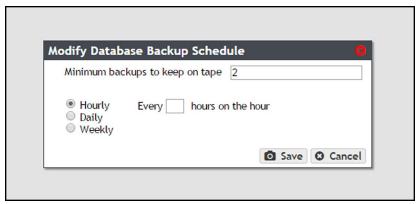


Figure 224 The Modify Database Backup Schedule screen.

4. Enter a number for the **Minimum backups to keep on tape**. When the system generates a backup, it determines the number of fully persisted backups and automatically deletes the oldest backups exceeding this number.

Note: Although the minimum number of backups is always respected, at some times there may be more than the minimum present on the system.

- **5.** Enter a number for **Every** _ **hours on the hour**. This value specifies the interval, in hours, between generating backups. For example, if this value is set to 4, the system creates a backup every four hours.
- 6. Click Save.

Create a Daily Schedule

- **1.** From the menu bar, select **Configuration > Database Backup**. The Database Backup screen displays (see Figure 227 on page 335).
- **2.** Select **Action > Change Schedule**. The Modify Database Backup Schedule screen displays.

3. Select **Daily**. The Modify Database Backup Schedule screen changes to display the options for a daily backup schedule.

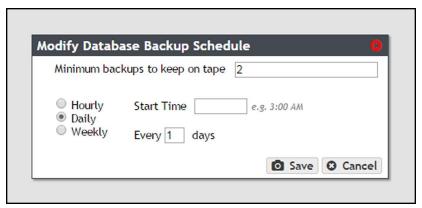


Figure 225 The Modify Database Backup Schedule screen.

4. Enter a number for the **Minimum backups to keep on tape**. When the system generates a backup, it determines the number of fully persisted backups and automatically deletes the oldest backups exceeding this number.

Note: Although the minimum number of backups is always respected, at some times there may be more than the minimum present on the system.

- **5.** Enter a time value for **Start Time**, and include AM or PM after the value. this field is not case sensitive.
- **6.** Enter a number for **Every_days**. This value specifies the interval, in days, between generating database backups. For example, if this value is set to 2, the system generates a backup every two days at the time specified in Step 5.
- 7. Click Save.

Create a Weekly Schedule

- **1.** From the menu bar, select **Configuration > Database Backup.** The Database Backup screen displays (see Figure 227 on page 335).
- 2. Select Action > Change Schedule. The Modify Database Backup Schedule screen displays.

3. Select **Weekly**. The Modify Database Backup Schedule screen changes to display the options for a daily backup schedule.

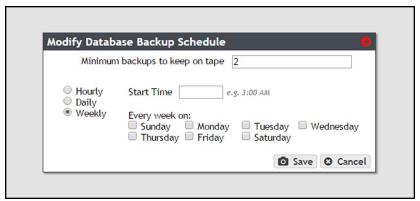


Figure 226 The Modify Database Backup Schedule screen.

4. Enter a number for the **Minimum backups to keep on tape**. When the system generates a backup, it determines the number of fully persisted backups and automatically deletes the oldest backups exceeding this number.

Note: Although the minimum number of backups is always respected, at some times there may be more than the minimum present on the system.

- **5.** Enter a time value for **Start Time**, and include AM or PM after the value. This field is not case sensitive.
- **6.** Select one or more days for **Every week on:**. This determines the day(s) of each week the system generates database backups.
- 7. Click Save.

Manually Generate a Database Backup

Use the instructions in this section to create a database backup manually.

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



Figure 227 The Database Backup screen.

2. Select **Action > Start Immediate Backup**. A confirmation window displays.

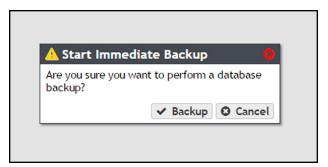


Figure 228 The Start Immediate Backup confirmation window.

3. Click Backup.

Restore from a Database Backup

Restoring a database backup returns the system to the state it was in when the backup was created. All objects written to the system after the backup was created are inaccessible.



Restoring a database backup deletes all data changes made after the backup AUTION was created, and deletes any backups that were saved after the one you are using for the restore process. This action cannot be undone.

There are two ways to restore from a database backup; restoring from a manual or automatic database backup, or restoring from an arbitrary file. Restoring from an arbitrary file is useful if you have copied your database backup files to another bucket.

Note: If you are restoring using a database backup that resides on an 96-bay expansion node, after restoring the backup, when the system completes initialization, you must re-import the pool on the 96-bay expansion node containing the backup file used to restore the database.

Restore Using a Database Backup

Use the following instructions to restore a database backup.

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

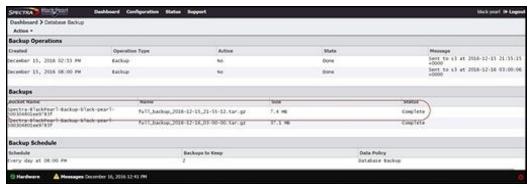


Figure 229 The Database Backup screen.

2. Select the backup you want to restore in the Backups pane, and then select **Action > Restore from Backup**. A confirmation dialog box displays.

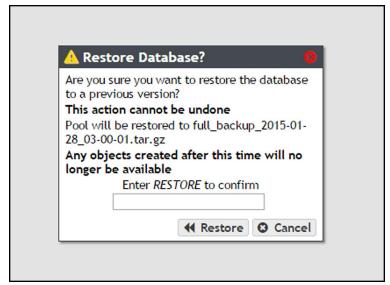


Figure 230 The Restore Database? confirmation dialog box.

3. Enter RESTORE in the entry field, and then click **Restore**. The database is restored to the state it was in when the backup was generated.

Restore Using an Arbitrary File

Use the instructions in this section to restore a database backup using an arbitrary file, such as a database backup that was copied to a different bucket than the one normally used for database backups.

- **1.** From the menu bar, select **Configuration > Database Backup**. The Database Backup screen displays (see Figure 229 on page 336).
- **2.** Select **Action > Restore from Arbitrary File**. A confirmation window displays.

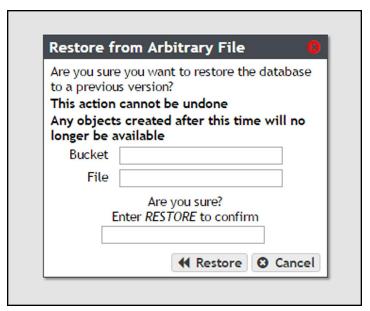


Figure 231 The Restore from Arbitrary File confirmation dialog box.

- **3.** Enter the name of the bucket containing the file in the **Bucket** field.
- **4.** Enter the filename of the file in the **File** field.
- **5.** Enter RESTORE in the entry field, and then click **Restore**. The database is restored to the state it was in when the backup was generated.

Delete Backup

Use the following instructions to delete a database backup.

1. From the menu bar, select **Configuration > Database Backup.** The Database Backup screen displays (see Figure 229 on page 336).

- **2.** Select the backup you want to delete in the Backups pane, and then select **Action > Delete**. A confirmation dialog box displays.
- **3.** Enter DELETE BACKUP in the entry field and click **Delete**. The backup is deleted.

Edit Backup Data Policy

Use the following instructions to edit the data policy used for the database backup bucket.

- **1.** From the menu bar, select **Configuration > Database Backup**. The Database Backup screen displays.
- **2.** From the menu bar select **Action > Edit Data Policy**. The Edit Data Policy screen displays.



Figure 232 The Edit Data Policy screen.

3. Use the **Data Policy to Use** drop-down menu to select a new data policy for the database backup bucket.

Show Backup Physical Placement

Use the following instructions to display what piece(s) of tape media or what storage pool is used by a database backup.

1. From the menu bar, select **Configuration > Database Backup**. The Database Backup screen displays (see Figure 227 on page 335).

2. From the list of existing backups, select the backup for which you want to view physical placement and select **Action > Show Backup Physical Placement**. The screen refreshes to show you the storage pool or tape media the backup currently occupies.



Figure 233 The Database Backup Physical Placement screen.

REBOOT OR SHUT DOWN A BLACKPEARL SYSTEM

This section discusses rebooting or shutting down a system.

Using the BlackPearl User Interface

Use the following instructions to reboot or shutdown a system 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.

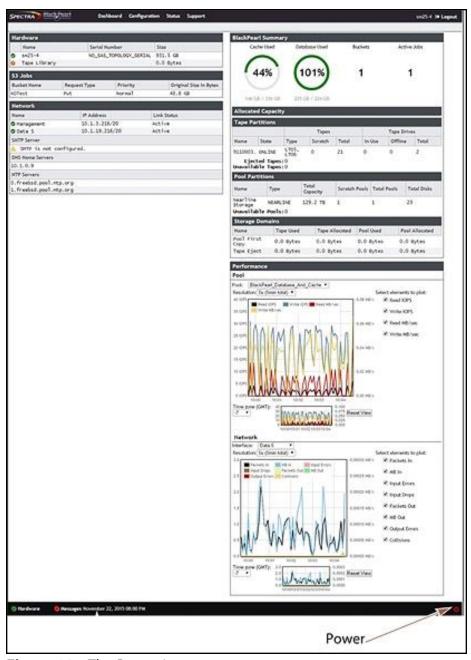


Figure 234 The Power icon.

- 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 system to recover from an error. To power-cycle reset a BlackPearl system, remove the front bezel, and then press and hold the front panel power button (Figure 13 on page 55) until the button's LED turns off. After a few moments, press the button again to turn the system back on.



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

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 and S3 Groups on page 207.

Chapter 11 - Using AutoSupport

This chapter describes using the BlackPearl user interface to configure the support features of the Spectra BlackPearl Converged Storage System.

Topic	
About AutoSupport	page 343
Enter Contact Information	page 343
Configure Mail Recipients	page 344
Create a New Mail Recipient	page 344
Edit a Mail Recipient	page 345
Send a Test Email	page 346
Delete a Mail Recipient	page 347
Log Sets	page 348
Configure a Log Set Schedule	page 349
Manually Generate Log Sets	page 350
Email a Log Set	page 351
Download a Log Set	page 351
Delete Log Sets	page 352

ABOUT AUTOSUPPORT

AutoSupport lets the BlackPearl system 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 system 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 system 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 235 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.

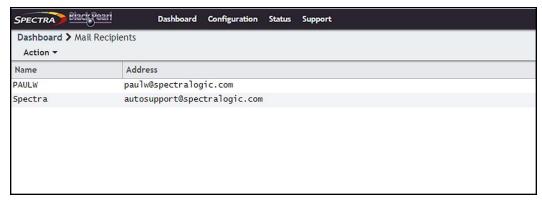


Figure 236 The Mail Recipients screen.

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.

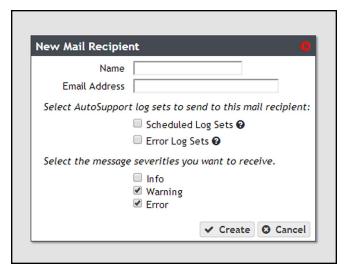


Figure 237 The New Mail Recipient dialog box.

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.
The address cannot contain spaces or other non-alphan characters (for example, an ampersand, &).	
Select Scheduled Log Sets, Error Log Sets, both options, or neither the mail recipient. Scheduled log sets are sent from the BlackPear Converged Storage System system on the first of each month. Error Log Sets, both options, or neither the mail recipient sets to send to this mail recipient are sent anytime an error occurs that causes the system to generate	
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 Converged Storage System system 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 system, select all boxes.

- **4.** Click **Create** to save the information. The Mail Recipients screen re-displays with the new mail recipient added to the list of mail recipients.
- **5.** Repeat Step 1 on page 344 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 Figure 236 on page 344).

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.

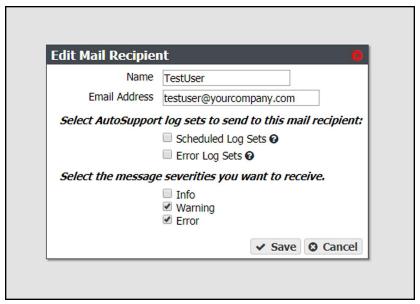


Figure 238 Edit the information for the selected mail recipient.

3. Change the information for the recipient as required and then click **Save**. See Step 3 on page 345 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 236 on page 344).
- **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**.

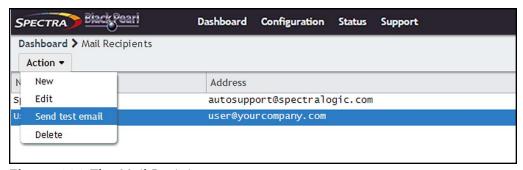


Figure 239 The Mail Recipients screen.

The BlackPearl system immediately sends a test email to the selected account.

3. Verify the user received the email from the BlackPearl system. If the email is not received, verify that you entered the SMTP server settings correctly (see Configure SMTP Settings on page 186).

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 236 on page 344).
- **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.

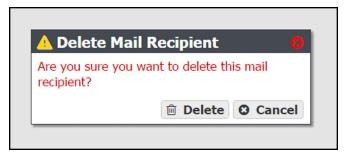


Figure 240 Delete the selected mail recipient.

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

LOG SETS

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

- Log Sets contain information about the configuration and status of the BlackPearl system and are used for general troubleshooting. Log sets can be mailed to configured mail recipients or to Spectra Logic Technical Support.
- Statistic Log Sets contain performance data about the system and are used by Spectra Logic Technical Support for in-depth troubleshooting. Statistic log sets are too large to be mailed directly from the system and must be downloaded.
- **Kernel Log Sets** are generated whenever a process on the system fails. This report cannot be generated manually.
- Data Path Log Sets are used to determine if there is a problem in the data planner code. This logset contains no customer data and is used by Spectra Logic Technical Support.

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



Figure 241 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 Figure 241).
- **2.** Select **Action > New Log Set Schedule**. The New Log Set Schedule dialog box displays.

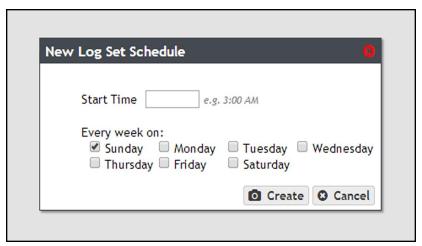


Figure 242 The New Log Set Schedule dialog box.

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

Manually Generate Log Sets

Although the BlackPearl system 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. Continue with Email a Log Set on page 351 or Download a Log Set on page 351.

-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 327. Continue with Download a Log Set on page 351.

-OR-

Select Action > New Data Path Log to generate a log set used for troubleshooting the
data communication path to the system and its associated tape library. The New Data
Path Log dialog box displays.

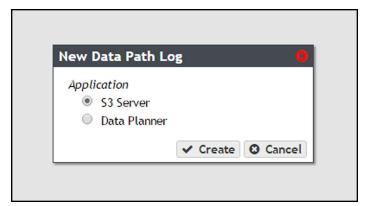


Figure 243 The New Data Path Log dialog box.

i. Select the **Application** for which you want to generate a log set.

Application	Description
S3 Server	The S3 Server log shows all Spectra S3 API commands sent to the system.
Data Planner	The Data Planner log shows how data sent to the system is organized and stored to tape.

- ii. Click Create.
- iii. Continue with Email a Log Set below or Download a Log Set on page 351.

Email a Log Set

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

Note: You must configure the SMTP settings on the system before you can send emails. See Configure SMTP Settings on page 186 to configure the SMTP settings.

- **1.** From the menu bar, select **Support > Logs**. The Logs screen displays (see Figure 241 on page 348).
- **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 system, and must be downloaded. See Download a Log Set, below.

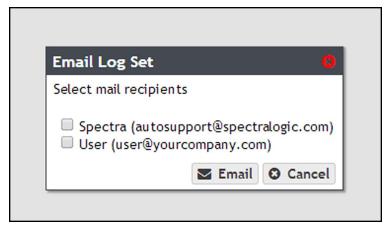


Figure 244 The Email Log Set dialog box.

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

Download a Log Set

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

- **1.** From the menu bar, select **Support > Logs**. The Logs screen displays (see Figure 241 on page 348).
- **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 Figure 241 on page 348).
- **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 system.	
Action > Delete All Statistic Log Sets	Deletes all statistic log sets on the system.	
Action > Delete All Kernel Logs	Deletes all kernel log sets on the system.	
Action > Delete All Data Path Logs	Deletes all data path log sets on the system.	

Chapter 12 - Maintaining the BlackPearl System

This chapter describes the maintenance procedures for the Spectra BlackPearl Converged Storage System.

Topic	
Data Integrity Verification - Disk Media	page 353
Cancel Disk Media Verification	page 354
Data Integrity Verification - Tape Media	page 355
Cancel Tape Media Verification	page 356
Initiate RSC Backup	page 356
Accessing the Technical Support Portal	page 357
Create an Account	page 357
Log Into the Portal	page 359
Configuring Automated Software Upload	page 360
Updating Software	page 361
Check the Current Software Version	page 361
Check the Currently Released Software Version	page 362
Download and Stage the Updated Software	page 363
Install the Update	page 364
Replacing a Failed Component	page 365
Identify the Failed Component	page 365

DATA INTEGRITY VERIFICATION - DISK MEDIA

The BlackPearl system allows you to perform on-demand data integrity verifications on any disk pools connected to the system, including the internal disk pools containing the BlackPearl cache and database. 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.

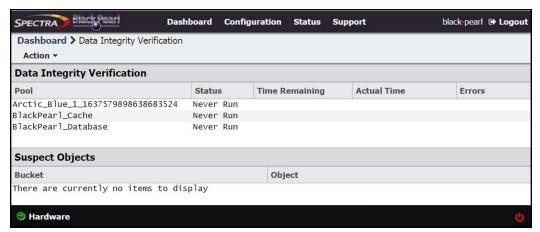


Figure 245 The Data Integrity Verification screen.

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.



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 system 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 system again, if the data policy did not specify multiple copies of the data. If you do not have copies of the affected files on your host or another location, they are lost.

Cancel Disk Media 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.

DATA INTEGRITY VERIFICATION - TAPE MEDIA

The BlackPearl system automatically performs data integrity verification for any tape cartridge that is unchanged for the number of days specified in a given storage domain. See Create a Storage Domain on page 124 for more information.

The BlackPearl user interface also allows you to perform an on-demand data integrity verification on any data tape cartridge present in the tape library connected to the system. Performing a data integrity verification on a tape cartridge is useful when you want to ensure the data on the tape is stored correctly. Spectra Logic recommends verifying any tape you plan to export from your BlackPearl system and store off-site.

You can configure the system to verify the entire tape, or a specified percentage of the total reported capacity of the tape cartridge. If you specify a percentage, the system starts the scan the specified percentage of the tape capacity before the EOD (End of Data) marker and ends the scan at the EOD marker. This is useful when you only want to validate the most recent data written to the tape. See Configure the Spectra S3 Service on page 189 for more information.

You can select to verify a single specified tape cartridge, or to verify all tape cartridges using a single operation.

Notes:

- If there are cleaning tapes present in a data partition, they display on the Tape Management screen. However, it is not possible to individually verify a cleaning tape, and cleaning tapes do not undergo data integrity verification if you opt to verify all tapes in a single operation.
- Cleaning tapes in cleaning partitions are not processed by data integrity verification.

Use the instruction in this section to verify data on tape media.

1. From the menu bar, select **Status > Tape Management.** The Tape Management screen displays.

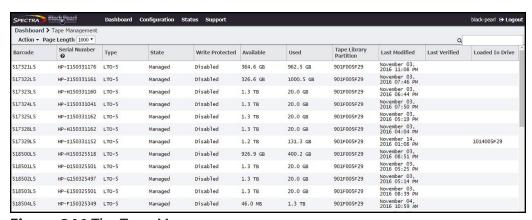


Figure 246 The Tape Management screen.

2. To verify data on an individual tape, select the tape in the Tape Management screen, and then select Action > Verify Tape. To verify data on all tapes in the tape library, select Action > Verify All Tapes.

Note: The time required to **Verify All Tapes** varies based on the number of tapes in the library. Large libraries can take a very long time to complete the verification.

A confirmation window displays. Click **Verify** to begin the data integrity verification.



In the event that the data integrity verification fails, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 8) for assistance in determining the affected files on the tape cartridge. The affected files cannot be retrieved from the tape cartridge, and may need to be transferred to the BlackPearl system 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 Tape Media Verification

If desired, you can cancel queued data integrity verification. Only tapes currently queued for data integrity verification are canceled. Any tapes undergoing verification when the cancel command is issued will complete the verification process.

- **1.** From the menu bar, select **Support > Tools > Data Integrity Verification.** The Data Integrity Verification screen displays.
- **2.** Select the tape for which you want to cancel verification in the Tape Management screen, and then select **Action > Cancel Tape Verification**.

Note: To stop verification on all tapes in the tape library, select **Action > Cancel All Tapes Verifications.**

3. A confirmation screen displays. Click **OK** to stop the tape verification(s).

INITIATE RSC BACKUP

The replicated system configuration backup stores the current configuration of all settings for the BlackPearl system on a storage pool present in the system. This backup occurs automatically each time you create a storage pool, or once every seven days. If you make major changes to your BlackPearl system, 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 Figure 245 on page 354).
- **2.** Select **Action > Initiate RSC Backup.** A confirmation screen displays.
- 3. Click **Initiate RSC Backup** to manually backup the current system configuration.

Accessing the Technical Support Portal

The Spectra Logic Technical Support portal provides access to the Knowledge Base, the current version of BlackPearl software for the system, 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.

If you do not yet have a portal account, access the Technical Support portal login page at support.spectralogic.com. On the home page, click **create an account.** Enter the requested information to create your account and click **Sign Up**. When the account is approved, you will receive an email with a temporary password. Use your email address and the password provided in the email to log in to your account.

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 8).

1. Access the Technical Support portal login page at support.spectralogic.com.

2. On the home page, click **create an account**.



Figure 247 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.

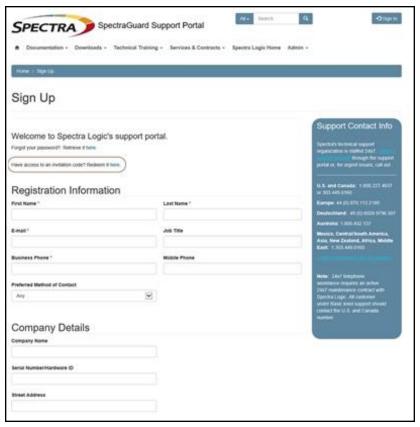


Figure 248 Follow the link to enter your invitation code or enter your registration information.

• 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.

CONFIGURING AUTOMATED SOFTWARE UPLOAD

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

Note: You must have a current software update key entered in the system you want to configure to use Automated Software Upload. See Database Backup & Restore on page 330 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.

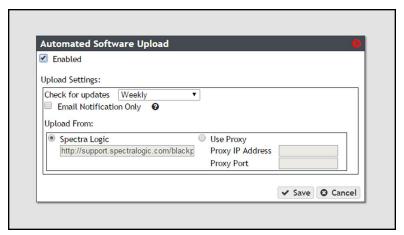


Figure 249 The Automated Software Upload dialog box.

- **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 download the file.
- 6. Select either Spectra Logic or Use Proxy as the Upload From location.



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

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

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

UPDATING SOFTWARE

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

Note: You must have a current software update key entered in the system you want to update. See Database Backup & Restore on page 330 for more information.

If Automated Software Upload is enabled, the system sends an email to all users configured to receive Warning or Informational emails (see Configure Mail Recipients on page 344) and posts a system message to the Messages screen. If configured to do so, the system also downloads the updated software.

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

- If the update package downloaded automatically, skip to Install the Update on page 364.
- 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 363.
- If you do not know if the system needs an update installed, continue with Check the Current Software Version below.

Check the Current Software Version

Use the following steps to determine the current software version running on your BlackPearl system.

- **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.

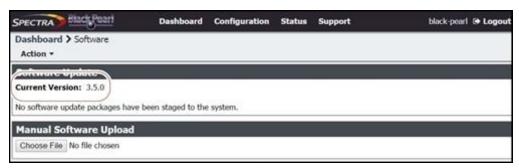


Figure 250 The current BlackPearl software version.

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 357 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 system in the **Spectra Product** column. The currently released BlackPearl software version is listed in the **Current Version** column.

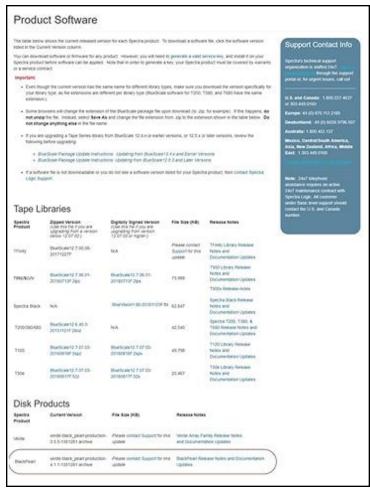


Figure 251 The Product Software screen.

4. Compare the Current Version available for the BlackPearl system to the version installed on the system.

Download and Stage the Updated Software

Use the instructions in this section to download and stage the updated software for the BlackPearl system.

- **1.** Log into your account on the Technical Support portal at support.spectralogic.com.
- **2.** Select **Downloads > Product Software**. The Product Software Screen displays.

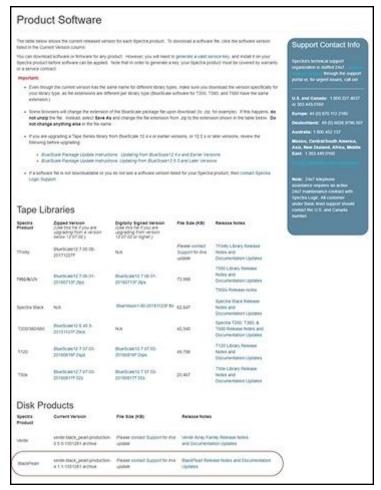


Figure 252 The Product Software screen.

- **3.** Locate the BlackPearl system in the **Spectra Product** 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 system.

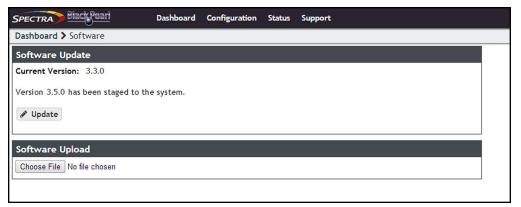


Figure 253 The Software Update screen with an available software package listed.

Install the Update

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

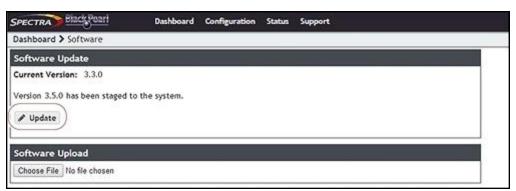


Figure 254 The Software Update screen with a software package staged to the system.

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



Figure 255 The Software Update screen showing the progress of an update.

- **4.** When the update is complete, the BlackPearl system automatically reboots to begin using the latest software.
- **5.** Restart file storage operations.

REPLACING A FAILED COMPONENT

If a component in a BlackPearl system is not functioning properly, the system 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 51).

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.

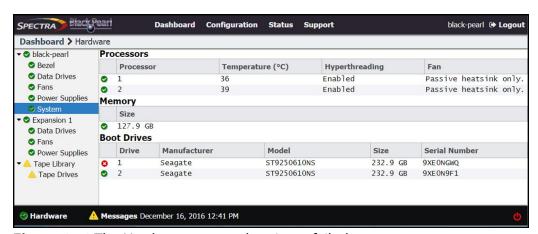


Figure 256 The Hardware screen showing a failed component.

2. If you have multiple BlackPearl systems, you can use the beacon feature to help locate the system with the failed component. On the Hardware screen, click the server name. The screen refreshes to show the main Hardware screen.

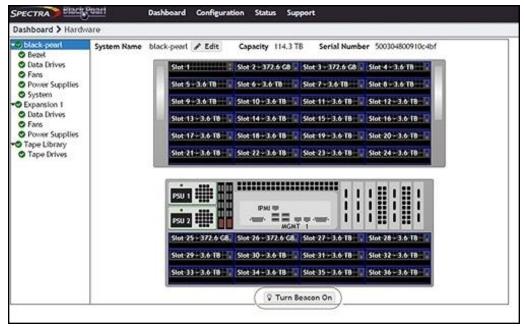


Figure 257 The Hardware screen. Gen1 S Series 4U chassis shown.

- **3.** Click **Turn Beacon On**. The BlackPearl system 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 Boot Drive Replacement Guide* provides instructions for replacing a failed boot drive in the system.
 - The *Spectra 12-, 36- & 45-Drive Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive after the system is installed.
 - The *Spectra 12-, 36- & 45-Drive Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in the system.
 - The Spectra 12-, 36- & 45-Drive Chassis Power Supply Replacement Guide provides instructions for replacing a failed power supply after the system is installed.
 - The Spectra 12-Drive Chassis HBA Replacement Guide and Spectra 36-Drive Chassis HBA Replacement Guide provide instructions for replacing a failed HBA in the system.
 - The *Spectra 96-Drive Chassis Drive Replacement Guide* provides instructions for replacing a failed data drive in the 96-bay expansion node.

- The *Spectra 96-Drive Chassis Fan Replacement Guide* provides instructions for replacing a failed fan in the 96-bay expansion node.
- The *Spectra 96-Drive Chassis Power Supply Replacement Guide* provides instructions for replacing a failed power supply in the 96-bay expansion node.
- The *Spectra 96-Drive 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 107-bay expansion node.

Chapter 13 - FAQ and Troubleshooting

Use the information in this appendix to troubleshoot problems on the Spectra BlackPearl Converged Storage System as they arise, before contacting Spectra Logic Technical Support.

Topic	
BlackPearl Cache	page 369
Tape Partitions	page 370
Tape Media	page 372
Tape Media Ejection	page 373
Tape Drive Cleaning	page 375
BlackPearl Database Backup	page 376
BlackPearl Component Hardware	page 378
Intelligent Object Management (IOM)	page 378
Special Firewall Feature for Connecting to BlueScale	page 380
Capacity Mode versus Performance Mode	page 380
Tape Handling Refactor Starting with BlackPearl Software Version 5.3	page 381
Enabling iSCSI For Use With the Spectra Swarm	page 385
Troubleshooting	page 388
Resolving a BlackPearl Management Port IP Address Conflict	page 397
Using the Console	page 397
Using a Separate Computer	page 397
Network Setup Tips	page 399
Configuration	page 400
Connectivity to the Network	page 400
Troubleshooting	page 403
Tools	page 403
Spectra Logic Technical Support	page 404

Topic	
Before Contacting Support	page 404
Determine System Serial Number	page 405
Opening a Support Ticket	page 405
Remote Support	page 408
Enabling Remote Support	page 409
Disabling Remote Support	page 411

BLACKPEARL CACHE

How is Cache Used and Allocated?

The BlackPearl cache is allocated physical storage on either HDDs or SSDs installed in the system. The cache functions as a transient location for all data transferred to the BlackPearl system from a client, or transferred from tape storage to the BlackPearl system.

The capacity available for cache is managed by the BlackPearl data planner, where active jobs reserve various amounts of cache capacity known as 'chunks'. Up to 85% of the cache can be reserved for jobs with a job priority level of 'high', or less. The remaining 15% of cache capacity is only available for jobs with a priority level of 'urgent'.

The cache is managed by chunk allocations. The chunk size can vary. When writing data to cache destined for tape storage, or restoring data from tape storage to the BlackPearl system, the chunk size is typically 2% of the capacity of a single tape cartridge. If the total job size is less than that amount, the chunk size reduces in size to match the job size. An internal job, such as IOM migration, can also reserve cache capacity. If needed, internal jobs can reserve all of the available cache capacity based on job priority, which may impact other jobs, occasionally preventing or delaying them from accessing cache chunks. If IOM is impacting normal production use, the Schedule IOM feature in the S3 service allows you to set a schedule to minimize downtime.

Why Does the BlackPearl User Interface Display 80% Cache Usage?

BlackPearl Software Version 5.2 or Earlier

After the system is in use, the Cache Used circle graph on the user interface dashboard hovers around 80% used capacity. When a task for a chunk, or the full job, completes, the data planner does not immediately delete those objects, but leaves them in the cache, available for reclaiming. Data from completed tasks remains in cache until more capacity is needed, or the used capacity exceeds 80%. When this threshold is reached, the BlackPearl system proactively deletes some of the data from completed tasks. The user interface dashboard only displays the actual data bytes in cache. Iit does not reflect cache capacity used by active jobs. To see how much cache capacity is currently used by active jobs, on the Jobs page of the user interface, select **Active Jobs**, and calculate the difference between "Amount Transferred to Cache" and "Amount Received/Archived".

BlackPearl Software Version 5.3 or Later

The Cache Used capacity graph on the user interface dashboard now displays only the actual capacity used by active jobs. It no longer displays the capacity of objects that are available in cache for a GET job. This information is available by examining the used capacity cache pool details screen, which is accessed from either the Advanced Bucket Management screen, or the Hardware page by double-clicking the pool labeled "BlackPearl_Cache".

TAPE PARTITIONS

How Does a User Upgrade to Later Generations of Media in the Same Tape Library?

The method used to add a newer generation of tape media depends on if the new and existing media are compatible, and if the existing tape drives are to be used for migration. If a media migration is required, keeping the older tape drives may increase performance during the migration.

A newer generation of media and drives can be added to an existing tape partition, if it is a one generation advancement. For example, adding LTO-7 media and drives into a library originally purchased with LTO-6 drives and media.

If the existing media is compatible with the new drives, the tape partition is upgraded to the new drive generation, and the old drives are removed.

However, if the old media **cannot** be used (either read from or written to) with the newer drives (for example, LTO-6 media cannot be read by LTO-8 tape drives) then a second tape partition is required to support the new tape drives and media. The new tape partition can be in the same tape library, or a separate tape library.

After completing changes to the tape library, add the new tape media into existing storage domain(s), and ensure the newer media generation has a higher write preference than the older generation. For example, set the write preference on LTO-7 media to "normal", then set LTO-6 media to a lower setting such as "never". If a data migration to the newer higher-density media is desired, then exclude the older storage domain member media, which then forces IOM migration for all data within that individual storage domain. See Migration for more details.

What Happens When a Tape Partition is Placed in Standby/Quiesced?

After an administrator issues a tape partition quiesce command, the BlackPearl system stops any new tape drive tasks for that partition. Any existing tasks are allowed to complete, which may take 30 minutes or more. After the tape task is complete for a tape drive, the drive is automatically unloaded and the tape is returned to its previous slot. While the tape partition is in standby, the BlackPearl system does not issue any internal tape task commands. The BlackPearl S3 service stays enabled and active while the tape partition is in standby, which allows any Spectra S3 applications, such as the Eon Browser or Spectra StorCycle application, to write data into, or to request data from the BlackPearl system. The write jobs go into the BlackPearl cache and wait until the tape partition is ready. For a restore or GET job, if the requested data is only available on tape, the job request returns a status that the tape partition is offline, and includes the tape barcodes required for the job.

What Happens When a Tape Partition is Re-Activated?

While the partition is in standby, the BlackPearl system monitors the tape partition robotic exporter for any updates or changes, such as a change in the library inventory. When the tape partition comes out of standby and is activated, the BlackPearl system automatically begins to use the partition as normal. With BlackPearl software version 5.2 or earlier, if there was an inventory change in the tape library while in standby, the BlackPearl system could react by re-inspecting all tapes in the library. Starting with BlackPearl version 5.3, the system no longer re-inspects tapes when there is an inventory change while the partition is in standby if the S3 service is set to "Never Inspect".

How do I Change the Tape Library Used by the BlackPearl System While Minimizing the Impact, Management Time, and System Downtime?

If you plan to upgrade the library used by the BlackPearl system, for example change from a Spectra T120 to a Spectra Stack, it is advised to work with Spectra Logic Technical Support before changing the tape partition used by the BlackPearl system, and before moving any tapes to the new tape library or partition.



IMPORTANT Create a manual database backup before changing to a new tape library or partition.

With BlackPearl software version 5.1 or earlier, moving tapes to a new partition may require a BlackPearl foreign import, which must be done for each storage domain. You will need to eject the tapes in batches, by storage domain, from the old partition, and import them into the new partition using a foreign import into storage domains associated with each exported batch. If necessary, repeat the process for additional storage domains.

If any tapes that have been ejected from the BlackPearl system are not stored on-site, those tapes must be rotated back on-site and imported through the new partition, or Spectra Logic Technical Support must manually update the database to re-associate those external tapes with the new partition.

TAPE MEDIA

How Does a User Know if Tape Media is Running Out of Space?

The available tape media capacity should be monitored per the daily operation and maintenance procedures by using the BlackPearl dashboard to ensure that adequate media is available for BlackPearl system to use for planned archive jobs, or to maintain a minimum available capacity per company policy.

Can Data be Overwritten on Existing Tapes?

With a full administrator login and multiple confirmation screens, any tape can be manually reformatted and put back into the blank media pool for use by the BlackPearl system. For example, older tapes with expired data.

Users with adequate permissions for a bucket could also use the BlackPearl user interface, a BlackPearl client, or an S3 browser tool like the Spectra Eon Browser to delete objects from a bucket. When all objects on a tape have been deleted, the tape is automatically reformatted and put back into the blank media pool.



Deleting objects or buckets is a manual process and extreme caution should be exercised to ensure that only data that is no longer needed is deleted.

Can WORM Media be Used With the BlackPearl System?

The BlackPearl system is not compatible with WORM (Write Once-Read Many) media. If the BlackPearl system is configured to transfer data to tape, make sure the partitions configured for use by the BlackPearl system do not contain WORM media.

TAPE MEDIA EJECTION

A tape eject strategy must be considered as part of a data policy. For information about the default data policies and options available to customize data policies, see Understanding Spectra Advanced Bucket Management Concepts on page 72. For additional information about ejecting and importing tapes, see Eject Tapes on page 280 and Import Tapes on page 284.

Spectra recommends keeping at least one copy of all archived data in the library at all times. Spectra Logic tape libraries can be easily upgraded by purchasing more slot licenses, or, if the slots become completely full, upgrading the library itself to one with more slots using the exclusive Spectra TranScale technology.

A tape library user or administrator may decide to eject media cartridges from a tape library for any of the reasons described below:

- **Ejecting a copy for off-site disaster recovery:** The BlackPearl system allows a user to make multiple copies of data automatically. A typical use case is to create a "tape first copy" that is intended to be left in the library for easy retrieval as well as an "eject copy" intended to be removed from the library once full for archival at an alternate site for safety. See see Understanding Spectra Advanced Bucket Management Concepts on page 72 for information on setting up multiple copies and ejecting a copy, and the *Tape Library User Guide* for details on the physical process of exporting and importing tapes into the library.
- **Ejecting a copy of data for transfer to another location:** In some work flows, a user ejects a tape or an entire bucket to transfer the data to another facility. Individual tapes or entire buckets can be ejected manually using the BlackPearl user interface (see Eject Tapes on page 280).

• Ejecting tapes to free up space in the library: Some work flows and budgets, require older or unused media to be ejected, making it not readily available. Individual tapes or entire buckets can be ejected manually using the BlackPearl user interface (see Eject Tapes on page 280).

"Eject" has multiple definitions within the system:

• From the BlackPearl system's perspective, eject means that a tape has been marked as ejected in the BlackPearl database and an instruction has been given to the tape library to move the tape for ejection from the library.

Note: You cannot eject a tape that is currently in use.

 From a tape library perspective, eject indicates the physical process of exporting tapes from the library.

Note: For instructions on exporting a tape from an IBM TS4500 tape library, see the see the *TS4500 User Guide*.

What Happens if a User Ejects a Tape From the Library Before Ejecting the Tape in the BlackPearl User Interface?

Tape media should not be exported from the tape library without first ejecting the tapes in the BlackPearl user interface.

If you suspect that a tape was exported from the library without being ejected from the BlackPearl system, in the BlackPearl user interface, select **Status > Tape Management**. The Tape Management screen displays. Re-import the tape with the status "Managed Not In Inventory".

See the *Tape Library User Guide* for instructions for importing the tape into a Spectra Logic tape library. For instructions on importing a tape into an IBM TS4500 tape library, see the see the *TS4500 User Guide*.

Once the tape is re-imported into the tape library, use the BlackPearl user interface to Online the tape as described in Import Tapes on page 284. Once the tape has a status of Online, the system inspects the tape and uses it as needed.

If a tape is exported from the tape library and is queued for a job, the client displays an error. If the client error message does not display the barcode of the tape, in the BlackPearl user interface, select **Status > Messages**, or click the **Messages** link on the status bar, to display the Messages screen. Inspect the messages to determine the barcode of the missing tape. See the *Tape Library User Guide* for instructions for importing the tape into a Spectra Logic tape library. For instructions on importing a tape into an IBM TS4500 tape library, see the see the *TS4500 User Guide*. Once the tape is re-imported, the system inspects the tape and uses it as needed.

How Does a User Configure Their T50e or T120 Library to Support Ejecting Tapes From the BlackPearl System?

The BlackPearl eject function allows you to eject tapes from the BlackPearl user interface, which are then moved to the Entry/Exit port on the tape library.

In order to use the BlackPearl eject function on a T50e or T120 library, you must configure a single partition and select **Standard** as the partition's Entry/Exit Port Mode. If you configure the partition to use either the Shared or Queued Eject mode, or you configure more than one partition on your library, ejects from the BlackPearl system fail.

See "Configuring and Managing Partitions" in the *T50e Library User Guide*, or "Partition Management" in the *T120 Library User Guide* for instructions on configuring a partition to use the Standard mode for the Entry/Exit port.

Note: The Spectra Stack, T200, T380, T680, T950 and TFinity libraries do not have limitations on the partition count or Entry/Exit mode for BlackPearl tape ejection.

TAPE DRIVE CLEANING

How Does a User Know Their Cleaning Media is Expired?

Cleaning media expires after a specified number of uses to ensure that drives are thoroughly cleaned. The BlackPearl system does not track cleaning media health. Only the tape library tracks cleaning media health. When a piece of cleaning media expires, a message is posted to the System Messages screen in the tape library's BlueScale interface.

Expired cleaning media is automatically ejected from an IBM TS4500 tape library.

If your cleaning media are LTO or TS11xx tapes with MLM enabled, you can proactively monitor the status of cleaning media through the tape library's BlueScale interface.

Notes:

- If your cleaning tapes are not MLM-enabled, you cannot use MLM to
 proactively monitor cleaning media. You must use the messages posted to the
 System Messages screen to determine when a piece of cleaning media expires.
- If there are no cleaning tapes with cleans remaining, see your *Tape Library User Guides for instructions on exchanging expired cleaning media*.

Use the instructions in this section to determine if your cleaning media is expired or about to expire.

Spectra Logic T120 and larger libraries

- **1.** Log in to the BlueScale interface as described in your *Tape Library User Guide*.
- **2.** Select **General > Media Lifecycle Management**. The MLM Report screen displays.

- **3.** Select the partition from the **Partition** drop-down list and **Cleans Remaining** from the **Report** drop-down list.
- **4.** Click **Go**. The screen re-displays to show the number of cleans remaining for all cleaning cartridges present in the partition. Confirm at least one tape still has cleans remaining.

Spectra Logic T50e library

- **1.** Log in to the BlueScale interface as described in the Spectra T50e Library User Guide.
- **2.** Click **MENU**, then select **General > MLM**. The MLM Reports screen displays.
- **3.** Select **Total Library** from the **Partition** drop-down list and **Cleans Remaining** from the **Report** drop-down list.
- **4.** Click **Go**. The MLM Reports screen refreshes to display the Cleanings Remaining report with a list of the barcode labels for all cleaning tapes in the selected location and the number of cleanings remaining for each tape.

How Does a User Use Cleaning Media in a T50e or T120 Library That Does Not Have a Cleaning Partition?

In order to use the BlackPearl eject function on a T50e or T120 library, the library can only have a single data partition. In order for drives to be automatically cleaned, you must store cleaning media in the single data partition on your T50e or T120 library.

When the BlackPearl system detects cleaning media in the data partition, the system automatically cleans drives when cleaning is requested by a tape drive.

BLACKPEARL DATABASE BACKUP

The BlackPearl database is contained on a set of flash (SSD) drives within BlackPearl system. Information on every object stored by the system is saved, including object name, policy, physical location (including which tape or disk location), and other information critical for search and retrieval of objects. While all of this information could be retrieved by allowing the system to physically load and read every tape, this is a time consuming process and some bucket location information may be lost. If the database is lost, no data is lost, but retrieval becomes difficult.

Therefore, scheduling regular backups of the database is a best practice to ensure long term reliable operation. The BlackPearl user interface allows the administrator to set up regular and automatic database backups to both tape and disk, and also allows creation of an off site eject copy. The default database backup schedule generates a backup once per day, and retains a maximum of two backups.

How Does a User Verify the Database Backup Schedule?

From the BlackPearl menu bar, select **Configuration > Database Backup**. The Database Backup screen displays. In the Backup Schedule pane, view the current schedule. In the Backups pane, view the date code in the name of the complete backups available to verify the most recent backups.



Figure 258 The Database Backup screen.

Note: See Database Backup & Restore on page 330 for more information.

How Does a User Create a Bucket Isolated Data Policy for the Database Backup Tapes?

Creating a bucket isolated data policy for your database backup tapes ensures that only the database backup bucket is present on a tape cartridge. This makes off-site archival of your database backup tapes easier. Use the instruction in this section to create a data policy with bucket isolation.

- **1.** Follow the instructions in Create a Storage Domain on page 124 to create a new storage domain for the database backups.
- **2.** Follow the instructions in Create a Data Policy on page 131 to create a new data policy for the database backups. It is helpful to use a name similar to "DataBaseBackup". Make sure you select **Bucket Isolation** when assigning the storage domain created in Step 1 to the data policy.
- **3.** Select **Configuration > Database Backup**. The Database Backup screen displays.
- **4.** Select **Action > Edit Data Policy**. The Modify Data Policy window displays.
- **5.** Using the **Data Policy to Use** drop-down menu, select the data policy you created in Step 2.

BLACKPEARL COMPONENT HARDWARE

How Does a User Know if a Component of the BlackPearl System Has an Error?

During installation of the BlackPearl system, users are configured to receive emails if the BlackPearl system or the tape library issues a warning or error message. See "Configure Mail Users" in your *Tape Library User Guide* and Configure Mail Recipients on page 344 to verify or set up email recipients.

Use the information in the message emails, and the Messages screen in the BlackPearl user interface, and the Spectra Logic tape library's BlueScale user interface, along with the Troubleshooting section page 388 to correct any issues.

Note: For instructions on messaging and error reporting on an IBM TS4500 tape library, see the *TS4500 User Guide*.

INTELLIGENT OBJECT MANAGEMENT (IOM)

With IOM, the BlackPearl system is capable of self-healing files present on the system, as well as automatically compacting data stored on tape, and providing an easy migration path from one type of storage to another. IOM also allows multiple object versioning and data prestaging from tape to disk, and improves tape library performance by reducing the number of cartridge mounts.

Intelligent Object Management (IOM) has several key roles, including:

- Self-healing to rebuild a missing copy of data. Self-healing includes rebuilding a new storage domain member after it is added as an additional copy of data on the data policy.
- Migrating a copy of data to new or different media within a given storage domain by excluding the other storage domain member.
- Tape compaction, which moves all valid data off of a tape to other tapes in that storage domain, which allows the compacted tape to be reused or decommissioned.

IOM works by creating both a PUT job and GET job for the data it needs to move. IOM may create additional jobs depending on workload. When running an IOM migration, the system creates a pair of jobs for each storage domain, and additional job(s) for any tape cartridge(s) that are ejected from the tape library.

Best Practices

Spectra Logic recommends running IOM on a subset of data when possible.

- Migration Example If there are five storage domains where each domain is isolated from the other storage domains, use IOM to migrate one storage domain at a time. Within that storage domain, add a new storage domain member, and exclude the other member to start the IOM migration. See Add a Storage Domain Member to a Storage Domain on page 129 and Exclude a Storage Domain Member on page 150 for instructions.
- **Self-healing Example** Start with a data policy that only has a single, smaller capacity bucket. This data policy is duplicated with the same configuration settings. It is then possible change the bucket(s) to use the new data policy. Then modify the new data policy to add an additional storage domain, which triggers the IOM self-healing job to rebuild the missing copy of data. See Create a Data Policy on page 131 and Edit a Data Policy on page 158.

Considerations for IOM Resource Impact

The BlackPearl system can be configured to limit or prevent the impact of IOM operations on the normal production workload. The main considerations are the cache pool size and throughput, and the number of tape drives available for IOM. The BlackPearl tape drive task priority can be set to limit which, and how many, tape drives are available for IOM operations. This also limits the impact on cache bandwidth.

If throughput and bandwidth need to be prioritized for the normal production workflow, or if there is not enough throughput available, then a hardware configuration change may be necessary to meet the project goals. Throughput can be increased by adding additional disk drives to the cache pool, while adding additional tape drives increases the systems available bandwidth. If further improvements are necessary, the chassis can be upgraded to new hardware.

Note: Contact the Spectra Logic Professional Services team for help sizing and managing both migration and self-healing IOM projects, as well as assistance with hardware upgrades to improve the throughput bandwidth of your system.

SPECIAL FIREWALL FEATURE FOR CONNECTING TO BLUESCALE

Introduction

The BlackPearl system can act as a gateway for a Spectra Logic tape library network management interface. This feature enables a private network behind the BlackPearl system, where Proxy/NAT information is entered into the BlackPearl system to allow a connection to either a BlueScale library or BlueVision library with the BlackPearl system.

Warning

- This will greatly reduce performance of the overall system.
- Only use at the direction of Spectra Logic Technical Support.
- Consult your Professional Services team for proper configurations when a tape library management gateway is required.

Basic Steps

- **1.** Obtain the key from Technical Support.
- 2. Enter the "EM BlueScale" key in the BlackPearl user interface.
- **3.** Connect the tape library management port directly to the RJ45 data port on the BlackPearl chassis.
- **4.** Enter tape library Proxy/NAT information for the tape library in the BlackPearl user interface.
- **5.** Verify the connection for the tape library remote management interface using a client browser.

CAPACITY MODE VERSUS PERFORMANCE MODE

Chunks

The BlackPearl system writes to tape drives based on chunks, with default chunk size of approximately 128 GB, or 2% of the tape media capacity. When there is a queue of jobs, the BlackPearl system aggregates smaller jobs or smaller chunks into a size of approximately 128 GB for each tape drive read or write task.

Performance Mode

When running in performance mode, the BlackPearl system spreads the chunks or aggregations across all available tape drives, or disk pools. The number of tape drives used can be limited by using tape drive reservations. It is recommended to use performance mode only at the direction of Spectra Logic. There may be other methods to increase performance while using capacity mode based on workloads and use cases.

The consequence of using performance mode with tape media is that during a restore or GET job, more tape drives and tapes cartridges are required to restore a data set that was initially spread across many tapes. This can drastically reduce overall performance during restores, as the system takes longer to get access to the full data set.

Capacity Mode

When running in capacity mode, the BlackPearl system uses as few tape cartridges or disk pools as possible. The system only allocates a new tape cartridge or disk pool when capacity is needed.

This means that for smaller jobs, the BlackPearl system only writes to one tape drive regardless of how fast the cache is. However, the system monitors the total job queue capacity, and if there is more data in the queue than there is capacity on the tape(s) available, it will allocate an additional tape and start writing data to the newly allocated tape in parallel.

Note: When the data policy setting "Minimize Spanning" is enabled, it overrides the capacity mode and performance mode logic for a given job, up to 1 TB in size. Minimize spanning increases the chunk size to 1 TB, and always keeps one chunk on a single tape regardless of write mode. If the job is larger than 1 TB, then multiple chunks are used and the system uses the logic for capacity mode vs performance mode, where different chunks may transfer to different tapes.

TAPE HANDLING REFACTOR STARTING WITH BLACKPEARL SOFTWARE VERSION 5.3

Use the information in this section to understand the changes to tape handling in BlackPearl software version 5.3.

General BlackPearl Notes

• Tape drives can be taken offline and new drives brought online without restarting the BlackPearl system.

- For clearing a 'stuck' tape drive reservation, the sa(4) driver reserves a drive on open and releases it on close using SCSI-2 reservations that are not persistent. A power cycle or drive reset clears the reservation. The reason for the reservation is to ensure no other initiator attempts to use the tape drive while the BlackPearl system is using it.
- Most drive sense is handled by the sa(4) driver and LTFS. The tape drivers used by the BlackPearl system almost exclusively interacts with a tape drive via libltfs. The LTFS library handles all sense codes itself or through its tape device drivers, and returns a generic error when a failure of the LTFS library management occurs.
- The BlackPearl system does not issue reset tape drive commands.

Tape Drive Failure Modes

The BlackPearl system does not react to many sense codes from tape drives, as the BlackPearl management code only receives them from the tape library management subsystem when the BlackPearl system attempts to read tape MAM attributes, such as determining the density of a piece of tape media or issuing a Test Unit Ready (TUR).

Most of the hard failures the BlackPearl system encounter include:

- Read and write errors.
- Command timeout issues due to the drive firmware being stuck on a process.
- A tape cartridge physically stuck in a tape drive.
- Tape drive seek errors.

When the BlackPearl system experiences any of these issues inside a libltfs call, a generic sense code is returned to the system management code.

Move Failures/Tape Stuck in Drive

Information about move failures comes from the changer device, and not a tape drive. The BlackPearl system detects these events through the tape library management subsystem. Currently, the BlackPearl system responds to sense codes from the media changer device as recommended in the Spectra TSeries Developer Guide. When a move failure occurs, the BlackPearl system is limited to just retrying the move.

Note: Spectra Logic is currently investigating other tape and media changer errors to add new functionality for restoring drive operation based on sense codes received from the tape library.

• **Encryption failure** – The 5.3.0 data planner now handles this failure. This is not handled by BlackPearl software 5.2 or earlier, and the BlackPearl system instead tries all tapes in the library.

- **Hardware failure** The 5.3.0 data planner now handles this failure. This is not handled by BlackPearl software 5.2 or earlier, and the BlackPearl system continues to retry using the drive or tape.
- **Read failure** The 5.3.0 data planner handles this failure using new tape handler logic. BlackPearl software versions prior to version 5.3 have error handling to move a tape to at least two tape drives before marking the tape as bad. Starting with BlackPearl version 5.3, the system retries the read using up to three tape drives.
- **Write failure** The 5.3.0 data planner handles this failure using new tape handler logic. BlackPearl software versions prior to version 5.3 have error handling to move a tape to at least two tape drives before marking the tape as bad. Starting with BlackPearl version 5.3, the system retries the write using up to three tape drives.
- MAM failure This error is handled by driver retry logic.
- **LTFS failure** This is a failure other than Encryption, Hardware, or read/write failures. This failure is not handled in software version 5.3 and the BlackPearl system will try all tapes in the library.
- Replace tape drive This operation does not require a BlackPearl reboot. (See point 1 below in Library, Drive, and Tape Failure Behavior in BlackPearl version 5.3 on page 383).
- Add a new tape drive This operation does not require a BlackPearl reboot. (See point 1 below in Library, Drive, and Tape Failure Behavior in BlackPearl version 5.3 on page 383).

Library, Drive, and Tape Failure Behavior in BlackPearl version 5.3

Use the information in this section to understand the behavior of the BlackPearl system when encountering failures in tape library operation.

- 1. Lower level kernel and tape backend behavior:
 - **a.** The tape backend communicates with the media changer via SCSI pass-through. Generally, any retries are handled in the tape library management subsystem and not the kernel. If the kernel handles the retries, the BlackPearl system receives Unit Attention conditionals from the library that tell the BlackPearl system that the inventory has changed.
 - **b.** The tape library management subsystem communicates with a tape drive via SCSI pass-through, tape driver IOCTLs, and LTFS. Depending on which of the approximately 50 tape drive calls LTFS is issuing, LTFS communicates with the tape drive via read/write communications to the tape driver, tape driver IOCTLs, or via SCSI pass-through. LTFS specifies whether or not it retries SCSI pass-through commands. For read/write, the sa(4) driver does not retry.

- 2. For move failures of any kind, the tape library management subsystem tries the move command again through the pass device (with no CAM retries) up to five times. The driver does no error handling for the BlackPearl system. For each attempt that fails, the BlackPearl system examines the sense code and tries to take remedial action on it. If the sense code does not indicate a terminal failure, the BlackPearl system tries again, otherwise the system returns a failure. If the system exhausts all retries and is attempting a drive-to-drive move, the source drive is put into an error state. Otherwise the CCBFailure error is returned.
- **3.** Tape error handling (the "3-strikes to quiesce" rule)
 - **a.** Three consecutive failures on a tape drive on the same operation should not occur, because the BlackPearl system stops retrying the operation on the drive and currently loaded tape after two failures before trying with a different drive or a different tape.
 - **b.** The BlackPearl system will quiesce a drive if it has outstanding (not cleared) failures for three tapes regardless of how many failures per tape there are, of what tasks originated the failures, and of what type of failures they are. Failure type does matter when clearing failures. The BlackPearl system ages failures out of memory after 24 hours, no longer counting against the drive for this quiesce rule. However, the failures are retained in the database.
 - **c.** Here's an example scenario for events on a single tape drive:
 - **i.** Tape A fails twice with two write failures. That is considered one strike and not two, because the failures occurred on only one tape.
 - **ii.** Tape B fails with an import failure, which is considered the second strike on the tape drive.
 - **iii.** Tape C successfully writes some data, clearing all write failures for the drive. This reduces the number of strikes counted against the drive back to one strike.
 - **iv.** Tape B fails with a write failure. The drive is still considered to have just one strike because there was already a failure with tape B.
 - **v.** Tape C fails with a write failure, which is considered a second strike on the tape drive.
 - **vi.** Tape D is successfully inspected by the tape drive. No changes to the strike count occur, because the BlackPearl system does not have any inspect failures to clear.
 - vii. Tape D fails with a write failure. Since all of these events occurred in a span of 24 hours, none of the errors has aged out, and this failure is considered a third strike on the drive (using strikes from failures with tapes B, C, D), and the BlackPearl system quiesces the tape drive.
 - **d.** The default number of strikes (three) can be changed by Spectra Logic Technical Support. If set to zero, the BlackPearl system will not automatically quiesce the tape drive.

- **4.** An LTFS Encryption error, or 500 Hardware error from tape drive causes the BlackPearl system to quiesce the tape drive.
- **5.** Manual quiescing of individual tape drive is still permitted.
- **6.** If the BlackPearl "Auto-Inspect" data path is set to "Never Inspect", quiescing a tape partition causes the BlackPearl system to stop monitoring or reconciling a tape library change (tape inspections are not eliminated). Instead, the BlackPearl system no longer "loses" the tapes, because the system is not monitoring the tape library, and therefore the system does not have reason to inspect the same tapes after the tape partition is brought online. If the BlackPearl "Auto-Inspect" data path is set to "Full", then the system inspects the tapes when the partition is brought online. If the tape library inventory changes, new tapes require inspection regardless of setting.
- **7.** If a tape library disappears unexpectedly (for example a RIM or robot connection is accidentally disconnected), the BlackPearl system automatically quiesces the tape partition, and does not mark the tapes as lost. Then item 6 applies, and tapes are not inspected if the data path is set to "Never Inspect".

The auto-quiesce feature is set to "ON" by default for BlackPearl software version 5.3.0. The system follows normal quiesce behavior, and waits for chunks writing/reading from tapes to finish before taking tape drives offline.

If the auto-quiesce feature is set to "OFF", the tape cartridges are marked as "lost".

ENABLING ISCSI FOR USE WITH THE SPECTRA SWARM

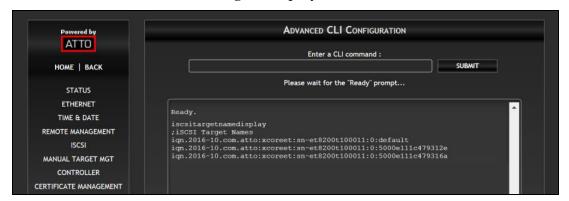
The BlackPearl system can communicate with the Spectra Swarm using the iSCSI protocol. This allows the BlackPearl to use SAS tape drives connected to the Spectra Swarm bridge.

The instructions below assume an understanding of creating and editing files in the FreeBSD environment. You must also have the BlackPearl system and Spectra Swarm installed and configured.

This procedure is to be used only at the direction of Spectra Logic Technical Support (see Contacting Spectra Logic on page 8).

- **1.** Log in to the Spectra Swarm user interface. See the *Spectra Swarm Install and Configuration Guide* for instructions.
- 2. Determine the target partition iSCSI name.
 - a. In the left-hand pane, click Advanced. The Advanced screen displays.

b. In the Enter a CLI Commmand dialog box, enter iscsitargetnamedisplay and click **Submit**. The list of iSCSI targets displays.



The name of each target is based on the WWN of each partition connected to the Spectra Swarm bridge. See *Spectra Swarm Install and Configuration Guide* the if you need to determine which WWN is associated with each partition.

Note: The default target is a collection of all iSCSI targets attached to the bridge, and is not reccomended for use with the BlackPearl system.



IMPORTANT

Using the default target may cause drive reservation errors with other applicances connected to the Spectra Swarm.

- 3. Determine the Spectra Swarm bridge data port IP address.
 - **a.** In the left-hand pane of the Swarm user interface, click **Ethernet**. The Ethernet Port Configuration screen displays.



b. Select the desired data port to display the IP Address for the port.

- **4.** Access the BlackPearl system FreeBSD command line interface.
- **5.** Create the file /etc/iscsi.conf .
- **6.** Once created, enter the following in the **iscsi.conf** file for each partition you want the BlackPearl system to access.

```
tlx <where x is the number of the partition>
{
    TargetAddress = <Spectra Swarm Data Port IP>
    TargetName = <iSCSI Target Name>
}
```

For example:

```
t10
{
<192.168.1.10>
<iqn.2016-10.com.atto:xcoreet:sn-
et8200t100011:0:5000e111c479312e>
}
```

7. Save the /etc/iscsi.conf file.

8. Open the /etc/rc.conf file and add the following startup flags.

9. Enable the iSCSI modules by adding the following line under the "builtin services" section of the **/etc/rc.conf** file.

```
iscsid enable="YES"
```

- **10.** Save the /etc/rc.conf file.
- **11.** The BlackPearl system must be restarted for this change to take effect. During system initialization, the BlackPearl system automatically connects to all iSCSI targets defined in the /etc/iscsi.conf file.

If the tape partition does not display in the BlackPearl user interface, contact Spectra Logic Technical Support for assistance (see Contacting Spectra Logic on page 8).

TROUBLESHOOTING

This section helps you troubleshoot problems with the Spectra BlackPearl system and the attached Spectra tape library.

Note: Troubleshooting steps below that describe actions that involve a tape library apply only to Spectra Logic tape libraries.

If your problem is not addressed by any of the below entries, contact Spectra Logic Technical Support for assistance (see Contacting Spectra Logic on page 8).

Issue	Resolution
An email is sent from the tape library indicating that drives need cleaning	If the BlackPearl system is connected to a Spectra T200 , T380 , T680 , T950 , or TFinity library , the library should be configured with a cleaning partition, which automatically cleans drives when cleaning is requested by the drive. If the BlackPearl system is connected to a Spectra T50e or T120 library , there can only be one partition on the library if you want to use the BlackPearl systems' eject function. If there is cleaning media in the data partition, the BlackPearl system automatically initiates cleaning tape drives using this media.
	• If your cleaning tapes are LTO or TS11xx technology and MLM-enabled, you can use the MLM feature to monitor the status of cleaning media. Check that valid cleaning media is present in the cleaning partition as described below.
	1. Log in to the BlueScale interface as described in your <i>Tape Library User Guide</i> .
	2. T50e - Select MENU > General > Media Lifecycle Management. All other libraries - Select General > Media Lifecycle Management. The MLM Report screen displays.
	3. Using the Partition drop-down menu, select Total Library.
	4. Using the Report drop-down menu, select Cleans Remaining.
	5. Click Go . The screen re-displays to show the number of cleans remaining for all cleaning cartridges present in the library. Confirm at least one tape still has cleans remaining.
	• If your cleaning tapes are not MLM-enabled, you cannot use MLM to monitor cleaning media. You must use the messages posted to the tape library's System Messages screen to determine when a piece of cleaning media expires.
	If there are no cleaning tapes with cleans remaining, use the <i>Tape Library User Guide</i> appropriate for your library type for instructions on exchanging expired cleaning media.
	If you continue to receive emails that drives are not being cleaned, contact Spectra Logic Technical Support for assistance (see Contacting Spectra Logic on page 8).

Issue	Resolution
An email is sent from the tape library regarding a problem with a tape drive	 Check the tape library's BlueScale interface to ensure that the tape drives are functioning normally. 1. Log in to the BlueScale interface as described in your <i>Tape Library User Guide</i>. 2. Review any System Messages that were posted by the library and take any action described in the message(s). If the system messages do not provide enough information to resolve the issue, look for additional information on the DLM (Drive Lifecycle Management) Details screen. 1. From the menu bar, select Configuration > DLM. The DLM screen displays. 2. Examine the status of each tape drive. If a drive shows any status besides a good status (green check mark in a circle), click Details for that drive, and take any action described in the details screen. 3. Once the tape drives are returned to good status, retry the job. Note: If you cannot return your tape drives to good status, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 8).
An email is sent from the tape library that a tape drive cannot eject a tape cartridge	Contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 8).
An email is sent from the tape library that indicates a robotics failure in the library	Gather an ASL as described in the "Configuring and Using AutoSupport" chapter in your <i>Tape Library User Guide</i> , and contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 8).

Issue	Resolution
An email is sent from the tape library indicating	If the BlackPearl system detects a media error with a tape cartridge, the system attempts to roll-back to a previously saved, known good checkpoint. Use the instructions in this section to resolve a media error.
a tape cartridge experienced a	1. Make note of the tape barcode that experienced the media error, and what drive it was in when the error occurred.
read or write error	2. Log in to the tape library as described in your <i>Tape Library User Guide</i>.3. Use the instructions in "Cleaning a Drive" in your <i>Tape Library User Guide</i>to clean the affected drive twice.
	4. See "Use DLM to Test an LTO Drive" in your <i>Tape Library User Guide</i> to test the drive. If the drive test fails, contact Spectra Logic Technical Support for assistance (see Contacting Spectra Logic on page 8).
	5. In the BlackPearl user interface, select Status > Tape Management . The Tape Management screen displays.
	6. Select the tape that experienced the error, and then select Action > Eject Tape . The Eject Tape dialog box displays.
	7. If desired, enter information in the Eject Label and Eject Location fields. This information is stored on the BlackPearl database and is visible when reimporting the tape into a BlackPearl system.
	8. Click Eject . The tape is marked as ejected in the BlackPearl system database, and moved to the Entry/Exit pool in the attached tape library.
	9. Export the cartridge from the tape library as described in your <i>Tape Library User Guide</i> .
	10 Inspect the cartridge for damage. If the tape does not show any signs of damage, re-import the cartridge into the tape library. If the cartridge is damaged, discard the cartridge.
	If you continue to experience media errors, contact Spectra Logic Technical Support for assistance (see Contacting Spectra Logic on page 8).
The BlackPearl system reports tapes as "Write Protected" on the Tape Management	If the tape has write protection set intentionally to protect valuable data from being overwritten, then select another tape. If the tape no longer needs to remain write protected, use your <i>Tape Library User Guide</i> to export the tape and disable write protection. Then re-import the tape cartridge into the tape library.
screen	Note: If the tape is still reported as Write Protected, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 8).

Issue	Resolution
A system message on the BlackPearl system reports "No tapes available" for a storage domain	When the BlackPearl system runs out of usable tape media, it posts a message that indicates there are "No tapes available." Import additional cartridges into the tape library as described in your <i>Tape Library User Guide</i> . Note: If your tape library is at full capacity, you may need to exchange full tapes for new ones, or increase the capacity license on your library. If exchanging tapes, you must eject the tapes from the BlackPearl system before exporting the tapes from the tape library. See Eject Tapes on page 280.
The BlackPearl system displays an error message when attempting to eject a tape	In order to use the BlackPearl eject function on a T50e or T120 library, you must configure a single partition and select Standard as the partition's Entry/Exit Port Mode. If you configure the partition to use either the Shared or Queued Eject mode, or you configure more than one partition on your library, ejects from the BlackPearl system fail. See "Configuring and Managing Partitions" in the <i>T50e Library User Guide</i> , or "Partition Management" in the <i>T120 Library User Guide</i> for instructions on configuring a partition to use the Standard mode for the Entry/Exit port.
An email is sent from the BlackPearl system indicating that the tape backend is deactivated	 This issue can occur if the attached tape library either reboots or powers down. If the tape library reboots, wait while the library completes initialization. The BlackPearl system automatically establishes communication with the tape library once it completes its initialization. If the tape library powers down, power on the library by pressing the power button on the front panel (see your <i>Tape Library User Guide</i> for more information). Then wait while the library completes initialization. The BlackPearl system automatically establishes communication with the tape library once it completes it's initialization. You may need to activate the data path backend on the BlackPearl system. In the BlackPearl user interface, select Configuration > Services. The Services screen displays. Select the S3 Service and select Action > Show Details. The S3 Service details screen displays. On the S3 Service detail screen, make sure the Data Path Backend Activated is set to Yes. If not, select Action > Activate Data Path Backend. If you continue to experience problems with the tape library, gather an AutoSupport log as described in your <i>Tape Library User Guide</i>, and contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 8).

Issue	Resolution
An email is sent from the BlackPearl system indicating that a tape it needs to complete a GET operation is not present in the tape library	The tape may have been exported from the tape library either on purpose or by mistake. Locate and re-import the tape into the tape library as described in your <i>Tape Library User Guide</i> . Once the tape is re-imported into the tape library, use the BlackPearl user interface to Online the tape as described in Import Tapes on page 284. Once the tape has a status of Online, the system inspects the tape and uses it as needed.
An email is sent from the BlackPearl system indicating a hardware failure	Over time, replaceable components in the BlackPearl system may wear down and fail. Use the instructions in this section to determine the failed component. 1. In the BlackPearl user interface, select Status > Hardware. The Hardware screen displays. 2. Examine the Hardware screen for any failed components, which are designated by a red X in a circle. 3. Contact Spectra Logic Technical Support to request a part replacement (see Contacting Spectra Logic on page 8). Spectra Logic provides you with the replacement part. The documentation for all replacement parts can be found on the Spectra Logic support portal, at support.spectralogic.com, after you log in to the portal. The list of customer replaceable parts is as follows. Any other part failures are resolved by on-site Spectra representatives. • Data Drives • Boot Drives • Fans • Power Supplies • HBAs • Tape Drives (installed in the tape library)

Issue	Resolution
An email is sent from the BlackPearl system indicating that the cache is full	 The BlackPearl cache can become full for several reasons: For PUT jobs, one or more data repositories (tape library, disk partition) is offline, or does not have sufficient space to write all the data currently in the cache. Data will sit in the cache until the problem is corrected. Check to make sure the data path backend is activated. 1. In the BlackPearl user interface, select Configuration > Services. The Services screen displays. 2. Select the S3 service, and select Action > Show Details. 3. On the service detail screen, ensure the status of Data Path Backend Activated is Yes. If the data path is not enabled, select Action > Activate Data Path Backend. Check to make sure that no tape libraries are in standby state. 1. From the menu bar, select Configuration > Advanced Bucket Management > Storage & Policy Management. The Advanced Bucket Management screen displays. 2. Under Tape Partitions, make sure all tape partitions listed show a State of Online and a Standby status of No. If any tape partitions are in standby state, select the tape partition, and then select Action > Activate Tape Partition. Check for system messages that indicate the partition is out of space. See A system message on the BlackPearl system reports "No tapes available" for a storage domain on page 392. For GET jobs, data retrieved into the cache will remain in the cache until the client either gets the data or the job is canceled. Either use your client to complete the GET job, or cancel the job as described below. 1. In the BlackPearl user interface, select Status > S3 Jobs. The S3 Jobs screen displays. 2. Select the job you want to cancel and select Action > Cancel Job.
An email is sent from the BlackPearl system indicating that the database is full	If the database reaches full capacity, the BlackPearl system is no longer usable. Additional drives must be installed to accommodate the database size. Contact Spectra Logic Technical Support for assistance (see Contacting Spectra Logic on page 8).

Issue	Resolution
A system message on the BlackPearl system indicates that the database is not being backed up	 The BlackPearl system reports a failure to backup the database in the system messages. Check the system messages to determine the cause. 1. In the BlackPearl user interface, select Status > Messages. The Messages screen displays. 2. Examine the list of messages for additional information about the failure. If the database backup schedule is not configured, the BlackPearl system displays the following message once per day: "The database is not being backed up. Select a data policy from the Database backup screen to enable backups". See Database Backup & Restore on page 330 for more information.
The BlackPearl system does not display tapes with duplicate barcodes on the Tape Management screen	Although a Spectra tape library allows duplicate barcodes within the same partition, the BlackPearl system does not allow duplicate barcodes. Any tapes with duplicate barcodes are not displayed on the Tape Management screen and are not used by the system. 1. Use your <i>Tape Library User Guide</i> to eject tapes with duplicate barcodes. 2. Apply new, non-duplicate barcodes to the tapes and re-import them into the tape library. 3. The BlackPearl system automatically inspects and uses the tapes as needed.
The BlackPearl Tape Management screen shows media in the attached tape library as "Inspect Failed"	 The BlackPearl system uses tapes formatted with LTFS to store data. Only LTO-5 and higher Ultrium or TS 11xx technology tape media supports LTFS. If your tape library contains LTO-4 or older media, or you import LTO-4 or older media into a partition being utilized by a BlackPearl system, the unsupported pieces of media display a Type of "Inspect Failed" on the Tape Management screen. Use the following steps to export LTO-4 and older media from your tape library. 1. In the BlackPearl user interface, select Status > Tape Management. The Tape Management screen displays. 2. Examine the Tape Management screen for any tapes that display a Type of "Inspect Failed". Make note of all barcodes of "Inspect Failed" tapes. 3. Select the affected tape, and then select Action > Eject Tape. The Eject Tape dialog box displays. 4. If desired, enter information in the Eject Label and Eject Location fields. This information is stored on the BlackPearl database and is visible when reimporting the tape into a BlackPearl system. 5. Click Eject. The tape is marked as ejected in the BlackPearl system database, and moved to the Entry/Exit pool in the attached tape library. 6. Export the media from the tape library as described in your <i>Tape Library User Guide</i>.

Issue	Resolution
The BlackPearl system displays a system message that a "Job did not complete in a 24 hour period"	If the BlackPearl system experiences a network error when transferring data, the data transfer fails. Network errors occur due to a variety of circumstances. Use the information in this section to help you troubleshoot a network error. Network errors may occur if the client is saturating the network with information. Consider reducing the number of threads the client uses to transfer data. For example, a 1 GB connection should be set to a maximum of 3 threads. Network errors may also occur due to problems with cabling, network switch issues, or SAN issues. See the Network Setup Tips on page 399 for troubleshooting information. If you cannot resolve the network issue, use the steps below to collect logs and open a ticket with Spectra Logic Technical Support. 1. In the client software, collect a set of logs, if available. 2. Download the Archive Provider logs on to your local host computer. 3. In the BlackPearl user interface, select Support > Logs. The Logs screen displays. 4. Select Action > New Log Set to generate a log set for use in general troubleshooting. 5. Select the log set you just generated, and then select Action > Download. The log set begins downloading to your host computer. 6. Submit a support incident using the Spectra Logic Technical Support portal as described in Opening a Support Ticket on page 405.
The BlackPearl user interface does not appear to update correctly	The BlackPearl system may have rebooted. If the system reboots, all inprogress jobs are resumed or restarted, but the BlackPearl user interface is not being updated. Log out and then log back in to re-establish a connection with the system.

RESOLVING 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 system as described in Log Into the BlackPearl User Interface on page 58. 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 system to your network.

Using the Console

Using the BlackPearl Converged Storage System 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 56.

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 system. See Rear Panel on page 41 to locate the management port.
- **3.** Open a web browser on the computer. For a list of compatible browsers, see Supported Browsers on page 52.
- **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 system does not have a security certificate.

Notes:

- Consult your browser documentation for instructions on how to resolve the security certificate warning.
- The absence of the certificate does not affect functionality.
- **6.** Enter the login username and password.
 - The default username is **Administrator** and password is **spectra**.
- **7.** From the menu bar, select **Configuration > Network**, or click the Network pane from the Dashboard screen. The Network screen displays.
- **8.** In the Network Interfaces pane, double-click the Management row, or select the Management row and then select **Action > Edit**. The Edit Management dialog box displays.

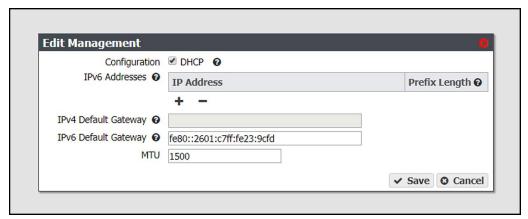


Figure 259 The Edit Management dialog box.

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



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 398, 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 system. You are now able to connect to the system with the IP address configured.

NETWORK SETUP TIPS

The BlackPearl management port is separated from the data ports. The management port and data ports have their own default routes. This does not prevent a user from having the management and data ports utilizing the same network, if desired.

The basic steps for configuring the management and data ports for access to the network are simple and straight-forward. However, each network environment is unique and may require some additional troubleshooting in order to properly connect to the BlackPearl system and utilize the 10GBase-T, 10 GigE, or 40 GigE interfaces correctly.

Configuration

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

Connectivity to the Network

The following configurations are supported for the data path:

Recommended:

- For the 10 GigE optical card:
 - Single 10 GigE logical connection using one of the 10 GigE physical ports
 - -OR-
 - Single 20 GigE logical connection using two 10 GigE physical ports (link aggregation)
- For the 40 GigE optical card:
 - Single 40 GigE logical connection using one of the 40 GigE physical ports
 - -OR-
 - Single 80 GigE logical connection using two 40 GigE physical ports (link aggregation)
- For the 10GBase-T card:
 - Single 20 gigabit logical connection using two 10GBase-T physical ports (link aggregation)
 - -OR-
 - Single 30 gigabit logical connection using three 10GBase-T physical ports (the two ports on the card and the one spare onboard port) (link aggregation)

Not Recommended:

- Single gigabit logical connection utilizing one of the 10GBase-T physical ports and a Category 5e Ethernet cable
 - -OR-
- Single 10 gigabit logical connection utilizing one of the 10GBase-T physical ports and a Category 6 Ethernet cable

Assign the appropriate IP address to the management and data ports either statically or using DHCP. If you are setting the MTU to something other than 1500, ensure that your switch configuration, as well as all the hosts on the network, support larger MTU settings. The BlackPearl system can support jumbo frames (MTU=9000), but all switches and hosts on the network must be configured to support jumbo frames if this is selected, or performance might be degraded.

Link Aggregation Notes

Switches use different methods of routing traffic from hosts to NAS servers. There are also many different network configurations to move data from hosts to NAS servers. For example, some Cisco switches route traffic based on the MAC address and the IP address. The BlackPearl system presents only one MAC address and one IP address when the data ports are aggregated via DHCP; if static link aggregation is chosen, the BlackPearl system presents only one MAC address, but can have up to 16 IP addresses aliased to the MAC address. It is up to the switch to rotate data transfers among the physical ports on the BlackPearl system in order to achieve the highest throughput possible.

Additionally, if link aggregation is configured for the BlackPearl system, then switches must also be able to support link aggregation to aggregate or "trunk" the data ports together to provide higher bandwidth into the system. Switches must support link aggregation using LACP (Link Aggregation Control Protocol), and the switches must hash the destination IP addresses. Manually configure LACP on the switch ports. LACP does not get enabled automatically.

For example, if only a single host is connected to the BlackPearl system through a link aggregated 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 mounted two times using different IP addresses and transfers are started to that share from two separate hosts, the resulting throughput would be approximately twice that of a single host connection. You may need to configure more than two IP addresses on the BlackPearl system to force the switch hashing algorithm to utilize all physical ports to maximize performance.

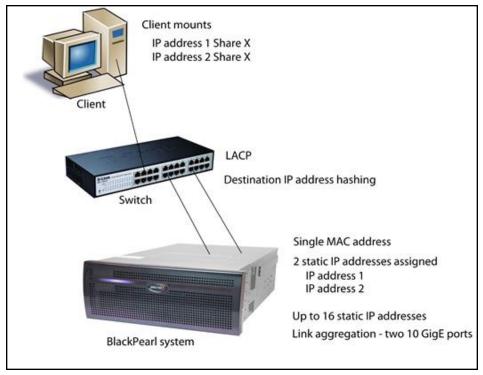


Figure 260 Connection example utilizing two IP addresses assigned to a single share.

Once configured correctly and attached to the network, the status in the user interface indicates the speed of the connection and whether the port is active. The link lights on the network ports should be on and active at both the BlackPearl system and the network switch.

From your network, use the "ping" command (see Ping on page 403) to test the assigned IP address for the BlackPearl management port or data port. If this is not successful, use the following troubleshooting tips to ascertain if the problem is a network setup issue.

Troubleshooting

Port Link LED Does Not Light

- Check the port configuration on the network switch. The BlackPearl system only supports
 auto-negotiation. Make sure the switch is configured to match speeds on both ends of the
 connection.
- Check the cables that connect the port to the other device. Make sure that they are connected. Verify that you are using the correct cable type and connectors. This is especially critical for 10 GigE and 40 GigE connections utilizing SFPs.
- Verify that the switch ports are not administratively disabled. Consult the switch *User Guide* for more information.

Port Link LED is Lit, But I Cannot Ping the BlackPearl system

- Check the LACP settings on the switch. If you are using link aggregation on the BlackPearl system, the switch MUST be configured to use LACP on those ports. If you are not using link aggregation, the switch must be configured NOT to use LACP on those ports.
- Check the VLAN (Virtual Local Area Network) settings on the switch. Ensure that the ports are assigned to the correct VLAN.

Tools

Ping

The ping command is a simple tool, based on a request-response mechanism, to verify connectivity to a remote network node. The ping command is based on ICMP (Internet Control Message Protocol). The request is an ICMP Echo request packet and the reply is an ICMP Echo Reply. Like a regular IP packet, an ICMP packet is forwarded based on the intermediate routers' routing table, until it reaches the destination. After it reaches the destination, the ICMP Echo Reply packet is generated and returned to the originating node.

For example, to verify the connectivity from the switch to the IP address 192.168.2.10, run the command shown below from the switch command line or client:

All ICMP Echo requests should receive replies including information about the round trip time it took to receive the response. A response of 0 msec means that the time was less than 1 ms. If the request times out, then check the settings on the switch to which the BlackPearl system is connected.

Traceroute

You can use the traceroute command, if it is available, or something similar, to not only verify connectivity to a remote network node, but to track the responses from intermediate nodes as well. The traceroute command sends a UDP packet to a port that is likely to not be used on a remote node with a TTL of 1. After the packet reaches the intermediate router, the TTL is decremented, and the ICMP time-exceeded message is sent back to the originating node, which increments the TTL to 2, and the process repeats. After the UDP packet reaches a destination host, an ICMP port-unreachable message is sent back to the sender. This action provides the sender with information about all intermediate routers on the way to the destination.

For example, for a BlackPearl system at IP address 192.168.2.10, the output of the command shown below,

```
traceroute 192.168.2.10
```

shows a numbered list indicating the number of hops encountered when tracing the packet from the switch to the BlackPearl system.

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 system, 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 313) 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 Opening a Support Ticket below).

Determine System Serial Number

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

- **1.** From the menu bar, select **Support > Contact Information**. The Contact Information screen displays.
- **2.** The system serial number is listed in the Product Information pane.



Figure 261 The system serial number.

Opening a Support Ticket

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

- **1.** Make notes about the problem, including what happened just before the problem occurred.
- **2.** Gather the following information:
 - Company name, contact name, phone number, and email address
 - Type of host system being used
 - Type and version of host operating system being used
 - Type and version of host file storage software being used
- **3.** Submit a support incident.
 - To use the Spectra Logic Technical Support portal:
 - **i.** Log into your account on the Technical Support portal at support.spectralogic.com.

Note: See Create an Account on page 357 if you did not previously create an account on the Technical Support portal.

ii. Select Incidents & Inventory > Open or View Incidents, or on the Home page, click Open a Support Incident.



Figure 262 Select **Incidents & Inventory > Open or View Incidents** to open a support incident.

iii. On the Open or View Incidents page, you are given an opportunity to search for existing support content that may help you solve your problem immediately. If the search does not provide an answer, click **Open a New Incident**.

Note: You must perform a search before you are able to open a new support incident.

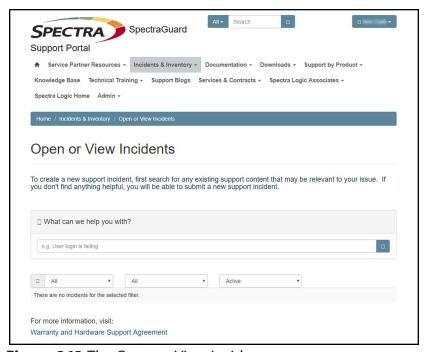


Figure 263 The Open or View Incidents page.

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

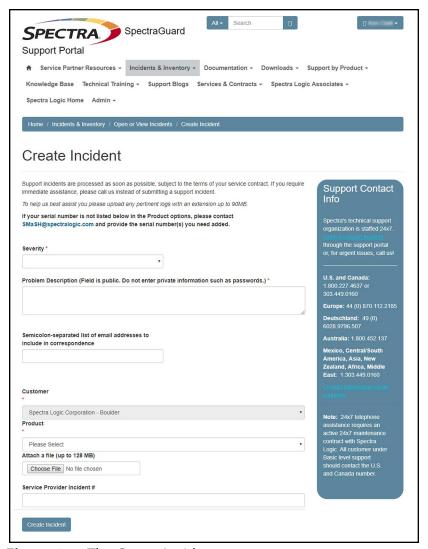


Figure 264 The Create Incident page.

• If it is within the hours of coverage provided by your support contract, contact Spectra Logic Technical Support by telephone. See Contacting Spectra Logic on page 8.

REMOTE SUPPORT

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

Enabling Remote Support

- **1.** Enter the Remote Support activation key as described in Configure Network Connections and Settings on page 178.
- **2.** From the menu bar, select **Configuration > Users**. The Users screen displays a list of all configured users.
- **3.** Edit the primary administrator account to enable remote support.

Notes:

- If you are running BlackPearl 3.x or earlier, the primary administrator account is named "Spectra".
- If you are running BlackPearl 4.x or later, the primary administrator account is named "Administrator".
- If you have upgraded from BlackPearl 3.x to BlackPearl 4.0 or later, the settings and permissions of the primary administrator account are migrated from the "Spectra" user, to the "Administrator" user. The "Spectra" user is maintained on the BlackPearl system after the upgrade, but is no longer the primary administrator.

- For systems running BlackPearl 3.x or earlier, double-click the Spectra account in the Primary Administrators pane, or select the Spectra account, and then select Action > Edit. The Edit User dialog box appears.
- For systems running BlackPearl 4.x or later, double-click the Administrator account in the Primary Administrators pane, or select the Administrator account, and then select Action > Edit. The Edit User dialog box appears.



Figure 265 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 178 for more information.

5. Click Save.



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

Disabling Remote Support

Use the instruction in this section to disable Remote Support.

- **1.** From the menu bar, select **Configuration > Users**. The Users screen displays a list of all users configured on the system.
- **2.** Edit the primary administrator account to disable remote support.

Notes:

- If you are running BlackPearl 3.x or earlier, the primary administrator account is named "Spectra".
- If you are running BlackPearl 4.x or later, the primary administrator account is named "Administrator".
- If you have upgraded from BlackPearl 3.x to BlackPearl 4.0 or later, the settings and permissions of the primary administrator account are migrated from the "Spectra" user, to the "Administrator" user. The "Spectra" user is maintained on the BlackPearl system after the upgrade, but is no longer the primary administrator.

- For systems running BlackPearl 3.x or earlier, double-click the Spectra account in the Primary Administrators pane, or select the Spectra account, and then select Action > Edit. The Edit User dialog box appears.
- For systems running BlackPearl 4.x or later, double-click the Administrator account in the Primary Administrators pane, or select the Administrator account, and then select Action
 Edit. The Edit User dialog box appears.



Figure 266 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 system using the system BIOS.



DO NOT make any changes in the BIOS other than changing the IPMI settings **CAUTION** as described below. Changing any other setting is not supported by Spectra Logic and may cause adverse system performance.

- 1. If the BlackPearl system is currently powered on, shut down the system as described in Reboot or Shut Down a BlackPearl System on page 339.
- 2. Connect a monitor and USB keyboard to the rear of the BlackPearl system. See Rear Panel on page 41 to locate the monitor and USB connectors.
- **3.** Power on the system as described in Power On the System on page 55.
- **4.** When prompted by the system, press **DEL** to enter the system BIOS.
 - **Note:** The system only displays this prompt for a few seconds. If you do not press **DEL** in time to enter the BIOS, let the system complete it's boot process, then reboot the system and repeat Step 4.
- **5.** Using the keyboard, navigate to the **IPMI** tab and then select **BMC Network Configuration**. The current settings of the BMC configuration display.



Figure 267 The BMC Configuration screen.

6. Using the keyboard, select **Update IPMI LAN Configuration**. A confirmation window displays. Select **YES** to continue. The current IPMI settings display.



Figure 268 Current IPMI settings.

- **7.** If desired, select **IPMI LAN Selection**. Change the configured setting as needed.
 - **Dedicated** Always uses the dedicated IPMI port for IPMI traffic.
 - Shared Always uses the LAN1 port for IPMI traffic.
 - **Failover** On system startup, detect if the dedicated IPMI port is connected. If not, the system uses the LAN1 port for IPMI traffic.
- **8.** If desired, select **VLAN** to enable or disable VLAN as needed.
- **9.** To change the IPMI address settings, select **Configuration Address source**. The current address source information displays.

- 10. Select Static or DHCP addressing.
 - If you select **DHCP**, skip to Step 12.
 - If you select **Static**, IP addressing fields display.



Figure 269 Enter Static IP information.

11.Configure the **Station IP address**, **Subnet mask**, and **Router IP address** with the desired address values.

Note: Only IPv4 addresses are valid.

12. Press **F4** to exit the BIOS and save the entered settings. The BlackPearl system reboots.

Appendix B - Specifications

This appendix provides detailed specifications for the BlackPearl systems, the 44-bay expansion node, 96-bay expansion node, and the 107-bay expansion node. The specifications listed here pertain to the currently shipping BlackPearl chassis.

Note: For specifications that differ for the BlackPearl 1.0 chassis, see "BlackPearl 1.0 Chassis Overview & Specifications" on page 440 on page page 440.

Specification	
Data Storage Specifications	page 416
Drive Specifications	page 417
Capacity	page 418
System Specification	page 421
Size and Weight	page 422
Environmental Specifications	page 425
Power Requirements	page 428
Input Power Requirements	page 428
Power Cord Specifications	page 430
Interface Specifications	page 432
System Interface Connectors	page 433
Interface Cables	page 435
Universal Serial Bus (USB) Support	page 436

Note: All specifications in this chapter are subject to change without notice.

DATA STORAGE SPECIFICATIONS

The following tables show the data storage specifications for the BlackPearl systems.

Notes:

- 1 TB is defined as 1,000,000,000,000 bytes.
- 1 GB is defined as 1,000,000,000 bytes.

Drive Specifications

BlackPearl Gen2 X Series

Drive Purpose	Drive Type
Database Storage	1.6 TB NVMe SSD Gen4
Object Cache	6.4 TB NVMe SSD Gen4

BlackPearl Gen1 S Series 4U System

Drive Purpose	Drive Type
Database Storage	400 or 800 GB Solid-State SAS
Object Cache	 4, 8, 12, or 16 TB Spinning-Disk SAS 12 TB Spinning-Disk Self-Encrypting Drives

BlackPearl Gen1 P Series 4U System

Drive Purpose	Drive Type
Database Storage	400 or 800 GB Solid-State SAS
Object Cache	• 960, 1600, or 1920 GB Solid-State SAS

BlackPearl Gen1 V Series 2U System

Drive Purpose	Drive Type
Database Storage	400 or 800 GB Solid-State SAS
Object Cache	 4, 8, 12, or 16 TB Spinning-Disk SAS 12 TB Spinning-Disk Self-Encrypting Drives

44-Bay Expansion Node

Drive Purpose	Specification
Storage Pools or NAS	 4, 8, 12, or 16 TB Spinning-Disk SAS 12 or 16 TB Spinning-Disk SATA 12 TB Spinning-Disk Self-Encrypting Drives

96-Bay Expansion Node

Drive Purpose	Specification
Storage Pools or NAS	8, 12, or 16 TB Spinning-Disk SATA

107-Bay Expansion Node

Drive Purpose	Specification
Storage Pools or NAS	 800 GB Solid-State SAS 4, 8, 12, or 16 TB Spinning-Disk SAS ^a 12 or 16 TB Spinning-Disk SATA 12 TB Spinning-Disk Self-Encrypting Drives

Capacity

Parameter	Specification
Gen2 X Series BlackPearl System	4 - 6.4 TB drives - 25.6 TB 12 - 6.4 TB drives - 76.8 TB 20 - 6.4 TB drives - 128 TB

a) 16 TB SAS drives only supported in a HotPair configuration.

Parameter	Specification
Gen1 S Series BlackPearl 4U System object cache capacity	10 - 4 TB drives - 40 TB 10 - 8 TB drives - 80 TB 10 - 12 TB drives - 120 TB 10 - 16 TB drives - 160 TB 20 - 4 TB drives - 80 TB 20 - 8 TB drives - 160 TB 20 - 12 TB drives - 240 TB 20 - 16 TB drives - 320 TB
Gen1 P Series BlackPearl 4U System object cache capacity	10 - 960 GB drives - 9.6 TB 10 - 1600 GB drives - 16 TB 10 - 1920 GB drives - 19.2 TB 20 - 960 GB drives - 19.2 TB 20 - 1600 GB drives - 32 TB 20 - 1920 GB drives - 38.4 TB
Gen1 V Series BlackPearl 2U System object cache capacity	4 - 4 TB drives - 16 TB 4 - 8 TB drives - 32 TB 4 - 12 TB drives - 48 TB 4 - 16 TB drives - 64 TB 9 - 4 TB drives - 36 TB 9 - 8 TB drives - 72 TB 9 - 12 TB drives - 108 TB 9 - 16 TB drives - 144 TB
44-bay expansion node	Active Bezel Maximum ^a 44 - 8 TB drives - 352 TB 44 - 12 TB drives - 528 TB 44 - 16 TB drives - 704 TB Passive Bezel Maximum ^b 45 - 8 TB drives - 360 TB 45 - 12 TB drives - 540 TB 45 - 16 TB drives - 720 TB

a) A 44-bay expansion node with an active bezel requires a Visual Status Beacon control sled installed in one drive storage slot.

b) A 44-bay expansion node with a passive bezel does not require a Visual Status Beacon control sled and can hold one additional data storage drive.

Parameter	Specification
96-bay expansion node	25 - 8 TB drives - 200 TB 25 - 12 TB drives - 300 TB 25 - 16 TB drives - 400 TB 50 - 8 TB drives - 400 TB 50 - 12 TB drives - 600 TB 50 - 16 TB drives - 800 TB 75 - 8 TB drives - 600 TB 75 - 12 TB drives - 600 TB 75 - 12 TB drives - 900 TB 75 - 16 TB drives - 1200 TB 96 - 8 TB drives - 768 TB 81 - 12 TB drives - 972 TB a 77 - 16 TB drives - 1232 TB b
107-bay expansion node	107 - 4 TB drives - 428 TB 107 - 8 TB drives - 856 TB 107 - 12 TB drives - 1284 TB 107 - 16 TB drives - 1712 TB

a) Limited to 81 drives based on available power supply wattage.

 $[\]ensuremath{\text{b}}\xspace$ Limited to 77 drives based on available power supply wattage.

SYSTEM SPECIFICATION

The following tables provide an overview of the system devices in the BlackPearl systems.

Gen2 X Series BlackPearl System

Parameter	Specifications
CPU	One 64-core CPU
System disk drives	Two 480G NVMe
Memory	256 GB (8 x 32 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 Optional four-port Fibre Channel cards ^c

Gen1 V Series BlackPearl 2U System

Parameter	Specifications
CPU	One multi-core processors
System disk drives	Two 500 GB SATA disk drives
Memory	32 GB (4 x 8 GB DIMM) 64 GB (8 x 8 GB DIMMS or 4 x 16 GB DIMMs)
Interface connections	 Two integrated 10GBase-T Ethernet ports ^d (Optional) One dual-port 10 Gigabit Ethernet NIC (Optional) four-port SAS card ^b (Optional) two-port SAS card ^b (Optional) two-port Fibre Channel card ^c

a) Dedicated to the BlackPearl user interface for system management.

b) Each SAS card is used to connect the BlackPearl master node to disk expansion nodes or SAS tape drives.

c) Each Fibre Channel card is used to connect the BlackPearl master node to Fibre Channel tape drives

d) One port is available for data transfers, one port is dedicated to the BlackPearl user interface for system management.

GEN1 S Series BlackPearl 4U System

Parameter	Specifications
CPU	Two multi-core processors
System disk drives	Two 500 GB SATA disk drives
Memory	64 GB (8 x 8 GB DIMM) 128 GB (16 x 8 GB DIMM or 8 x 16 GB DIMM)
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 (Optional) two-port Fibre Channel card ^c

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.

a) One port is available for data transfers, one port is dedicated to the BlackPearl user interface for system management.

b) Each SAS card is used to connect the BlackPearl master node to disk expansion nodes or SAS tape drives.

c) Each Fibre Channel card is used to connect the BlackPearl master node to Fibre Channel tape drives

Gen2 X Series BlackPearl System

Parameter	Gen2 X Series BlackPearl System	Shipping Container ^a
Dimensions • Height (2U) • Width • Depth	3.5 in. (8.7 cm) 19 in. (48.3 cm) 29 in. (73.7 cm) ^b	TBD
Maximum Weight Including rail kit ^c	61.2 lb (27.8 kg)	TBD

Gen1 V Series BlackPearl 2U System

Parameter	Gen1 V Series BlackPearl 2U System	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 (17.2 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 BlackPearl 4U System and 44-Bay Expansion Node

Parameter	Gen1 S Series BlackPearl 4U System 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 disk drive Additional for each Solid-State drive 	57 lb (25.8 kg) 1.8 lb (0.8 kg) 0.8 lb (0.4 kg)	91.3 lb (41.4 kg) 1.8 lb (0.8 kg) 0.8 lb (0.4 kg)

96-Bay Expansion Node

Parameter	96-bay Expansion Node	Shipping Container
Dimensions • Height (4U) • Width • Depth	6.9 in. (17.5 cm) 19 in. (48.3 cm) 40 in. (101.6 cm) ^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 disk drive Additional for rack mounting kit 	76 lb (34.5 kg) 1.8 lb (0.8 kg) 21 lb (9.5 kg)	108 lb (48.9 kg) ^d 1.8 lb (0.8 kg) 21 lb (9.5 kg)

a) Includes chassis, drives, box, and packaging.

b) Includes the front bezel.

c) Weights are approximate.

d) Includes chassis and packaging.

107-Bay Expansion Node

Parameter	107-bay Expansion Node	Shipping Container
Dimensions • Height (4U)	7 in. (17.8 cm)	18.4 in. (46.7 cm)
Width Depth	17 in. (43.2 cm) 41 in. (104.1 cm) ^a	24.3 in. (61.7 cm) 52.3 in. (132.8 cm)
Weight ^b		
Empty chassis	84.4 lb (38.3 kg)	180 lb (81.6 kg)
 Additional for each disk drive 	1.5 lb (0.67 kg)	
Additional for rack mounting kit	21 lb (9.5 kg)	
Fully loaded chassis	265 lb (120.2 kg)	336 lb (152.4 kg) ^c

ENVIRONMENTAL SPECIFICATIONS

The tables below show the temperature, humidity, and altitude requirements for the Gen2 X Series BlackPearl systems, Gen1 S Series BlackPearl systems, Gen1 V Series BlackPearl, 96-bay, and 107-bay expansion nodes.

a) Includes the front bezel.

b) Weights are approximate.

c) Includes chassis and packaging.

BlackPearl Gen2 X Series System

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 ^c	41° F to 95° F (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)	

BlackPearl Gen1 S Series Systems, Gen1 V Series Systems, and 44-Bay Expansion Nodes

Parameter	Operating Environment ^a	Storing and Shipping (Non-Operating) Environment ^b
Humidity	8% to 90% (non-condensing)	5% to 95% (non-condensing)
Temperature	50° F to 95° F (10° C to 35° C)	-40° F to 158° F (-40° C to 70° C)
Altitude	Sea level to 10,000 feet (3,048 meters)	Sea level to 39,370 feet (12,000 meters)
Maximum wet bulb temperature	84° F (29° C)	95° F (35° C)

a) When moving the BlackPearl system 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 system or expansion node in its original packaging. The packaging protects the BlackPearl system 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.

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 feet to 10,000 feet (-61 meters to 3,048 meters)	-200 feet to 40,000 feet (-61 meters to 12,192 meters)

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 feet to 10,000 feet (-61 meters to 3,048 meters)	-200 feet to 40,000 feet (-61 meters to 12,192 meters)

a) When moving the 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 heat generation of each BlackPearl chassis.

Chassis	Heat Generation at Maximum Wattage
Gen2 X Series	5460 BTUs/hour
Gen1 V Series BlackPearl 2U master node	3138 BTUs/hour
Gen1 S Series BlackPearl 4U master node	3410 - 4365 BTUs/hour
44-bay expansion node	3751 - 4775 BTUs/hour
96-bay expansion node	3751 BTUs/hour
107-bay expansion node	6820 BTUs/hour

POWER REQUIREMENTS

The BlackPearl systems, 44-bay, 96-bay, and 107-bay expansion nodes, have the following power requirements.



Failure to meet the cabling and power specifications could damage your system, result in data loss, or both.

Input Power Requirements

The following tables provide the input power requirements for each system or expansion node.

Gen2 X Series BlackPearl System

Parameter	Requirements
Input Voltage	200–240 VAC, 40 A peak, 1600 watts maximum
Input Frequency	50–60 Hz

Gen1 V Series BlackPearl 2U System

Parameter	Requirements
Input Voltage	100–240 VAC, 11–4.5 A, 920 watts maximum
Input Frequency	50–60 Hz

Gen1 S Series BlackPearl 4U System

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

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 systems are part of the unit and are not intended for use with any other equipment.



IMPORTANT Confirm the PDU used with the BlackPearl system 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.



Using extension cords in conjunction with the cords provided with an 96-bay expansion node or 107-bay expansion node, may cause serious damage.

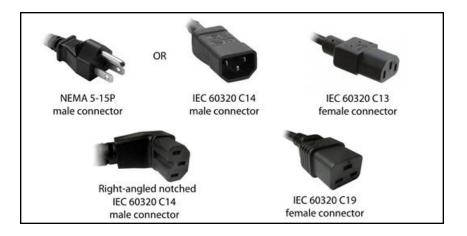
RNING WARNUNG Die Verwendung von Verlängerungskabeln in Verbindung mit den Kabeln, die mit einem 96-Schacht-Erweiterungsknoten oder 107-Schacht-Erweiterungsknoten geliefert werden, kann schwere Schäden verursachen.

Note: 96-bay expansion nodes ship with cables for use with the chassis. These power cables have a down-angled C15 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	 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	 Gen2 X Series BlackPearl Master Node: Male: Connector must be of the proper type, rating, and safety approval. Female: IEC 60320 C13 Gen1 S Series and Gen1 V Series BlackPearl Master Node: Male: Connector must be of the proper type, rating, and safety approval. Female: IEC 60320 C13 44-Bay Expansion Node: Male: Connector must be of the proper type, rating, and safety approval. Female: IEC 60320 C13 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	Gen2 X Series BlackPearl Master Node: • Male: Connector must be of the proper type, rating, and safety approval. • Female: IEC 60320 C13 Gen1 S Series and Gen1 V Series BlackPearl Master Node: • Male: Connector must be of the proper type, rating, and safety approval. • Female: IEC 60320 C13 44-Bay Expansion Node: • Male: Connector must be of the proper type, rating, and safety approval. • Female: IEC 60320 C13 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 system to expansion nodes, tape drives, and host systems.

Note: For "Interface Specifications" for the BlackPearl 1.0 chassis, see "BlackPearl 1.0 Chassis Overview & Specifications" on page 440 on page page 440.

System Interface Connectors

Gen2 X Series

Interface Type	Number of Ports and Connector Type
Ethernet • 1 Gig E • 100 GigE	One RJ-45 socket Two QSFP28 sockets.
SAS (12 Gbps) (Optional)	 Four SFF-8644 sockets per 12 Gbps SAS card provide connections to two or four 96-bay expansion nodes, or two or four 107-bay disk expansion nodes, using one port per expansion node. Four SFF-8644 sockets per 12 Gbps SAS card provide connection to sixteen SAS tape drives, using one port for four tape drives.
Fibre Channel (16 Gb or 32 Gb) (Optional)	Four SFP+ optical modules with LC connectors per Fibre Channel card provide connections to four Fibre Channel tape drives in the tape library, using one port for each tape drive.

Gen1 S Series and Gen1 V Series

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)	 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. Four SFF-8644 sockets per optional 6 Gbps SAS card provide connections to 16 SAS tape drives, using one port for four tape drives.

Interface Type	Number of Ports and Connector Type
SAS (12 Gbps)	 Two or four SFF-8644 sockets per optional 12 Gbps SAS card provide connections to two or four 96-bay expansion nodes, or two or four 107-bay disk expansion nodes, using one port per expansion node. Two or four SFF-8644 sockets per optional 12 Gbps SAS card provide connection to eight or sixteen SAS tape drives, using one port for four tape drives.
Fibre Channel (8 Gb)	Two or four SFP+ optical modules with LC connectors per optional 8 Gb Fibre Channel card provide connections to two Fibre Channel tape drives in the tape library, using one port for each tape drive.

Expansion Node and Tape Drive 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 system.
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 system.
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.
SAS Tape Drive	 T50e library: Two SFF-8088 ports per tape drive. Only a single port is required to connect the tape drive to a BlackPearl system. Either port can be used for the connection. All other libraries: One SFF-8088 port per tape drive. The single port is required to connect the tape drive to a BlackPearl system.
Fibre Channel Tape Drive	 T50e and T120 libraries: One multimode optical LC port per tape drive. The single port is required to connect the tape drive to a BlackPearl system All other libraries: Two multimode optical LC ports per tape drive. Only a single port is required to connect the tape drive to a BlackPearl system. Either port can be used for the connection.

Interface Cables

The type of cables required to connect the BlackPearl system to an Ethernet network, a 44-bay, 96-bay, or 107-bay expansion node, a SAS tape drive, or a Fibre Channel tape drive 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 may be provided by the customer.
Ethernet (10 GigE)	SFP+ transceiver multimode optical cable with duplex LC connectors. Note: Cables may 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 may be provided by the customer.
Ethernet (100 GigE)	100 GbE QSFP28 cable. Note: Cables may 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. 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. SAS tape drive: 6 Gbps 4 lane fan-out cable with SFF-8644 and four SFF-8088 connectors. One SAS cable is required for every four SAS tape drives. Note: Cables may be provided by the customer.

Interface Type	Cable Requirements
Fibre Channel	50 micron—400-M5-SN-I classification optical cable with LC connectors. One fiber cable is required for each Fibre Channel tape drive. Note: Cables may be provided by the customer.

Universal Serial Bus (USB) Support

Spectra Logic supports using the USB ports on the system for the following:

- USB mass storage devices (for example, flash drives)
- Keyboards & pointer devices (for example, a computer mouse)
- CD or DVD drives with USB interface

Appendix C - Installation Checklist

This chapter provides a checklist for installing a BlackPearl system. If your BlackPearl system was installed by Spectra Logic Professional Services, all of the applicable steps in this checklist were performed by the installer.

Create a Sup	Create a Support Portal Account Date Completed		
	Create an Account on page 357		
Install and Co	onfigure the Spectra Tape Library - See your Tape Library User Gu	ides	
	Install the library in a rack (Spectra Stack, T120, and T50e only)		
	Remove the shipping lock or shipping screw (Spectra Stack, T120, and T50e only)		
	Install the tape drives (Spectra Stack, T120, and T50e only)		
	Connect the cables		
	Install the option activation keys and update the BlueScale software (Spectra Stack, T120, and T50e only)		
	Log in to the BlueScale user interface		
	Configure network settings		
	Update the BlueScale software (T200, T380, T680, T950, and TFinity libraries only)		
	Configure date and time		
	Create additional users		
	Configure SMTP and mail users		
	Create a partition		
	Backup the library configuration.		
	Import data and cleaning tape cartridges/magazines		
Continue to the next page.			

Install and Co	Install and Configure the Spectra BlackPearl system Date Completed		
	Install HBAs in the system. See <i>The Spectra 12-Drive Chassis & 36-Drive Chassis HBA Installation</i> guide.		
	Rack mount the system and 44-bay expansion nodes. See the <i>BlackPearl Rack Mounting Guide</i> for instructions.		
	WARNING: 96-bay and 107-bay expansion nodes are always installed by Spectra Logic Professional Services.		
	Install drives. See the BlackPearl Drive Installation Guide.		
	Connect Ethernet Cables on page 54.		
	Power On the System on page 55.		
	Configure the BlackPearl Management Port on page 56.		
	Automatically Import Activation Keys on page 57.		
	Log Into the BlackPearl User Interface on page 58.		
	Configure the Data Connection on page 61.		
	Configure SMTP Settings on page 186.		
	Manually Starting the S3 Data Path Backend on page 306.		
	Configure NAS Services on page 238.		
	Create a Storage Pool on page 107.		
	Create a Disk Partition on page 113.		
	Select a data policy. See Understanding Spectra Advanced Bucket Management Concepts on page 72.		
	Set the default data policy for the administrator. See Edit a User on page 207.		
	Create a User on page 67.		
	View S3 Credentials on page 70.		
	Configure Mail Recipients on page 344.		
Continue to the next page.			

Install and Configure the Spectra BlackPearl system		Date Completed
	Check if tapes are ready for use. See View Tape Media Information on page 322. Tapes should have a status of Managed, Managed Format in Progress, Managed Format Pending, or Pending Inspection.	
	Manually Generate a Database Backup on page 335.	

Appendix D - BlackPearl 1.0 Chassis Overview & Specifications

This chapter provides an overview and specifications for the Spectra Logic BlackPearl Converged Storage System 1.0 chassis.

Topic	
Components	page 440
Front View	page 440
Rear View	page 442
Rear Panel	page 443
Specifications	page 444
System Specification	page 445
Interface Specifications	page 445

COMPONENTS

The following sections show the locations of and briefly describe the BlackPearl 1.0 chassis major front and rear panel components.

Front View

Figure 270 and Figure 271 show the components on the front of the BlackPearl systems with the front bezel removed.

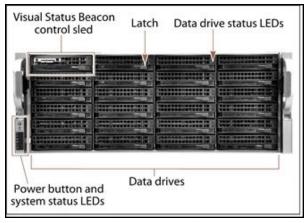


Figure 270 The front view of the BlackPearl Converged Storage System 4U system.

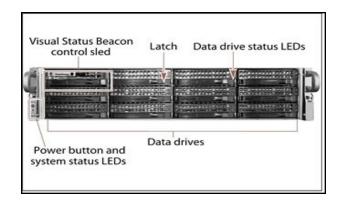


Figure 271 The front view of the BlackPearl Converged Storage System 2U system.

Component	Description
Front bezel (not shown)	The front bezel mounts on the front of the chassis, and contains the Visual Status Beacon light bar, which provides status information for the system. See Front Bezel Visual Status Beacon on page 309 for more information.
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 power button controls the main AC power for the BlackPearl system.
System status LEDs	The status LEDs indicate power status, disk and network activity, as well as hardware faults. See System Status LEDs on page 310 for more information.
Data drives	The base BlackPearl Converged Storage System 4U system includes one high-performance solid-state drive, and five spinning-disk drives mounted on individual drive sleds in the front of the chassis. Additional drives are installed in the rear of the chassis. The BlackPearl 2U system includes ten spinning-disk drives in the front of the chassis. The drive sleds slide into bays in BlackPearl 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.
Data drive status LEDs	Two LEDs on each drive sled indicate the status of the drive. One LED is for drive status while the other shows drive activity.
Empty drive sleds	Empty drive sleds are installed in the unused drive bays to prevent contaminants from entering the enclosure and to maintain proper air flow.

Rear View

Figure 272 and Figure 273 show the major components on the rear of the BlackPearl system.

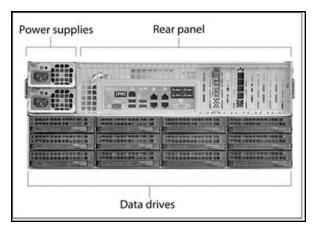


Figure 272 The rear view of the BlackPearl Converged Storage System 4U system.

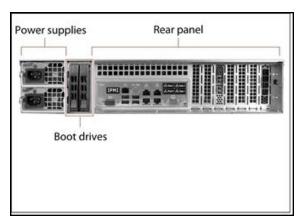


Figure 273 The rear view of the BlackPearl Converged Storage System 2U system.

Component	Description
Power supplies	 The standard BlackPearl system 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 BlackPearl system allows for Ethernet, Fibre Channel, SAS, USB, and other connections. See Rear Panel on page 443 for a detailed description.
Boot drives	The boot drives provide storage for the operating system and BlackPearl user interface. The boot drives for the BlackPearl 2U system are hot swappable which allows for uninterrupted operation during replacement. Note: The boot drives for the BlackPearl 4U system are located inside the chassis and are not accessible from the outside.
Data drives (BlackPearl 4U system only)	The base BlackPearl Converged Storage System 4U system includes one high-performance solid-state drive, and five spinning-disk drives mounted on individual drive sleds in the rear of the chassis. Additional drives are installed in the front of the chassis. The drive sleds slide into bays in the BlackPearl 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. Note: The BlackPearl 2U system does not have data drives in the rear of the chassis.

Component	Description	
Empty drive sleds (BlackPearl 4U system 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 274 shows the components on the rear panel of the BlackPearl Converged Storage System 4U and 2U systems.

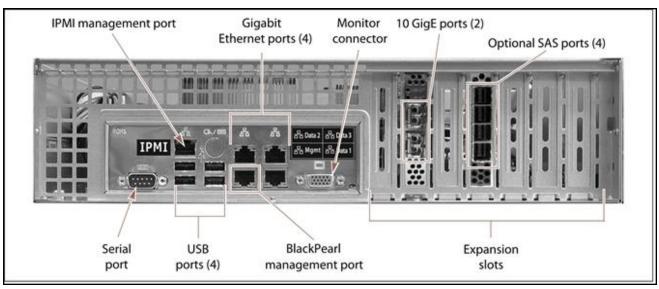


Figure 274 The BlackPearl rear panel components.

Component	Description	
IPMI management port	Not currently supported.	
Gigabit Ethernet ports (GigE)	The BlackPearl system includes four GigE ports. Three of the GigE ports can be used for network connectivity on a GigE network. The bottom left port of the four GigE ports is dedicated as the BlackPearl management port and cannot be used for data transfer. Note: Spectra Logic recommends using the 10 GigE ports for data transfer to ensure maximum performance.	

Component	Description	
Monitor connector	If necessary, you can connect a monitor to the SVGA connector on the BlackPearl system for troubleshooting purposes. Only connect a monitor for initial configuration of the BlackPearl management port, or as directed by Spectra Logic Technical Support.	
10 GigE ports	The two 10 Gigabit Ethernet (10 GigE) ports can be used for network connectivity on a 10 GigE network. Note: Spectra Logic recommends using the 10 GigE ports for data transfer to ensure maximum performance.	
SAS ports (optional)	Depending on your configuration, there may be a SAS card installed in an vailable expansion slot. The SAS card provides connectivity to SAS drives in Spectra Logic tape library.	
Fibre Channel ports (optional, not shown)	Depending on your configuration, there may be a Fibre Channel card installed in an available expansion slot. The Fibre Channel card provides connectivity to Fibre Channel drives in a Spectra Logic tape library.	
Expansion slots	The expansion slots accommodate optional interface cards to provide additional connectivity. An installed 10 Gigabit Ethernet network interface card provides high-speed data connection between hosts and the BlackPearl system. An optional SAS or Fibre Channel card provides connectivity between the BlackPearl system and tape drives in a Spectra Logic tape library.	
BlackPearl management port	The BlackPearl management port is used to connect to a browser-based user interface to configure, manage, and monitor the BlackPearl system. 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	Not currently used.	

SPECIFICATIONS

The following sections describe the specifications of the BlackPearl 1.0 chassis, where they differ from the current chassis. See "Specifications" on page 416 on page 416 for specification information not listed here.

System Specification

The following table provides an overview of the system devices installed in the BlackPearl systems.

BlackPearl 2U System

Parameter	Specifications
CPU	One multi-core processors
System disk drives	Two 250 GB SATA disk drives
Memory	64 GB (4 x 16 GB DIMMs)
Interface connections	 Four integrated Gigabit Ethernet ports One dual-port 10 Gigabit Ethernet NIC (Optional) four-port SAS card (Optional) two-port Fibre Channel card

BlackPearl 4U System

Parameter	Specifications
CPU	Two multi-core processors
System disk drives	Two 250 GB SATA disk drives
Memory	128 GB (8 x 16 GB DIMMs)
Interface connections	 Four integrated Gigabit Ethernet ports One dual-port 10 Gigabit Ethernet NIC (Optional) four-port SAS card (Optional) two-port Fibre Channel card

Interface Specifications

This section provides information about the interfaces used to connect a BlackPearl system with a BlackPearl 1.0 chassis, to the host systems.

Interface Connectors

Interface Type	Number of Ports and Connector Type	
Ethernet (GigE)	Four RJ-45 sockets	
Ethernet (10 GigE)	Two SFP+ optical modules with a duplex LC connector	
SAS	Four SFF-8644 sockets per optional SAS card	
Fibre Channel Two SFP+ optical modules with LC connectors per optional Fibre Channel card		

Network Interface Cables

The type of cables required to connect the BlackPearl system to the network depend on the type of interface being used.

Interface Type	Cable Requirements	
Ethernet (GigE)	Shielded Category 5 (10/100BaseT connection) data-grade cable with an RJ-45 connector	
Ethernet (10 GigE)	Multimode optical cable with duplex LC connectors	
SAS	6 Gbps 4-lane cable with SFF-8644 and SFF-8088 connectors	
Fibre Channel	50 micron – 400-M5-SN-I classification	

Appendix E - Regulatory & Safety Standards

The Spectra BlackPearl Converged Storage System 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

We:

Spectra Logic Corporation 6101 Lookout Road Boulder, CO 80301 USA

declare under sole responsibility that the

Spectra BlackPearl Converged Storage System

to which this declaration relates, meets the essential health and safety requirements and is in conformity with the EU Directives listed below using the relevant section of the EU standards and other normative documents listed in the following table.

Mule Galles

Nicole Gallego

Senior Director of Manufacturing and Quality Operations

Directive	Compliance	
EU EMC Directive 89/336/EEC	Essential health and safety requirements relating to electromagnetic compatibility.	
EN 55022 (CISPER 22) Class A	Limits and methods of measurements of radio interference characteristics of information technology equipment.	
EN 55024	1998, Information Technology Equipment - Immunity Characteristics Limits and Methods of Measurement.	
EN 61000-4-2	1995 + A1:1998+A2: 2001, Electrostatic Discharge	

Directive	Compliance	
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.	



Document # 99100002 V1.2

DECLARATION OF CONFORMITY

According to ISO/IEC 17050-1:2004

 ϵ

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: JBOD 108

Model Number: 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 Electromagnetic Compatibility

Directive: 2014/35/EU

EN 60950-1:2006 +A11:2009 +A1:2010

+A12:2011 +A2:2013

IEC 62368-1 second edition

EN 62479:2010

Directive 2014/30/EU EN55032: 2012, Class A

EN55024: 2010

EN 61000 3-2:2014

EN 61000 3-3:2013

6285 Lookout Road Boulder, CO 80301-3580 303-449-6400 800-833-1132 Fax: 303-939-8844

SPECTRA LOGIC.COM

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

May 27, 2020

Nicole Gallego

Vice President of Operations

Merle Calles

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	СЕ	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 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.

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 Converged Storage System system on uninterruptable power supplies.

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"

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 목적으로합니다.
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.

SAFETY STANDARDS AND COMPLIANCE

The Spectra BlackPearl Converged Storage System system 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.



RECYCLING YOUR SYSTEM

For information on recycling your Spectra appliance, check the Spectra Logic website at: spectralogic.com/environment.

CONFLICT MINERALS POLICY

Spectra Logic is committed to complying with the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas, as well as the applicable requirements of Section 1502 of the Dodd-Frank Act, which aims to prevent the use of minerals that directly or indirectly finance or benefit armed groups in the Democratic Republic of the Congo (DRC) or in adjoining countries ("conflict minerals").

Affected suppliers to Spectra Logic will be required to commit to being or becoming "conflict-free" (which means that such supplier does not source conflict minerals) and sourcing, where possible, only from conflict-free smelters. Each affected supplier to Spectra Logic will be required to provide completed EICC-GeSI declarations evidencing such supplier's commitment to becoming conflict-free and documenting countries of origin for the tin, tantalum, tungsten, and gold that it purchases.

For more information on Spectra Logic's conflict minerals program contact *conflictminerals@spectralogic.com*.

Appendix F - Open Source Code Acknowledgements & Package List

Copyright © 2010 - 2021 Spectra Logic Corporation. All rights reserved.

This appendix contains the licenses and notices for open source software used in the BlackPearl Converged Storage System product. If you have any questions or want to receive a copy of the free/open source software to which you are entitled under the applicable free/open source license(s) (such as the Common Development and Distribution License (CCDL)), contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 8).

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 © 1992-2021 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) 2002-2021 Igor Sysoev Copyright (C) 2011-2021 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

```
alsa-lib-1.1.2_2
```

apache-commons-daemon-1.2.3

apr-1.7.0.1.6.1_1

atf-0.21

avahi-app-0.8

bash-5.1.4_1

black_pearl-2.3_2

bluestorm_backend-2.0.2266326_7

bluestorm_frontend-2.1.2275716

bluestorm_gui-2.0.2275716_3

bluestorm_mgmt-2.0.2275716

bluestorm_tests-2.0.1658291_1

bluestorm_workers-2.0.2267322_6

boost-libs-1.72.0_3

brotli-1.0.9,1

c-ares-1.17.1

ca_root_nss-3.62

cdbcmd-0.0.1774343,1

compat10x-amd64-10.4.1004000.20181014

compat11x-amd64-11.2.1102000.20181014

cscope-15.9

ctags-5.8

curl-7.75.0

cyrus-sasl-2.1.27_1

dbus-1.12.20_3

dbus-glib-0.110

dejavu-2.37_1

dfu-util-0.10

dmidecode-3.3

ds3-3.2.0.1701306

e2fsprogs-libuuid-1.46.2

expat-2.2.10

fieldmod-2.0.0.2265460

fio-3.26

fontconfig-2.13.93,1

freetype2-2.10.4

fsx-1.0.2275716_1

fusefs-libs-2.9.9_2

gamin-0.1.10_10

gdb-10.1_1

gdbm-1.19

gettext-runtime-0.21

glib-2.66.7_1,1

gmp-6.2.1

gnome_subr-1.0

gnupg-2.2.27

gnutls-3.6.15

icu-68.2,1

indexinfo-0.3.1

iozone-3.491

iperf-2.1.0.r2

iperf3-3.9

ipmitool-1.8.18_3

jansson-2.13.1

java-zoneinfo-2021.a

javavmwrapper-2.7.7

ksh93-93.u_1,2

kyua-0.13_5,3

libarchive-3.5.1,1

libassuan-2.5.4

libdaemon-0.14_1

libedit-3.1.20191231,1

libevent-2.1.12

libffi-3.3_1

libfontenc-1.1.4

libgcrypt-1.9.2_1

libgpg-error-1.41

libiconv-1.16

libinotify-20180201_2

libksba-1.5.0

liblz4-1.9.3,1

libnghttp2-1.43.0

libsmi-0.4.8_1

libsunacl-1.0.1

libtasn1-4.16.0_1

libunistring-0.9.10_1

libunwind-20201110

libuv-1.41.0

libxml2-2.9.10_3

libxslt-1.1.34_1

libyaml-0.2.5

lnav-0.9.0

logrotate-3.13.0_1

lua52-5.2.4

lutok-0.4_7

mbuffer-20200929

mhash-0.9.9.9_5

mkfontscale-1.2.1

monit-5.27.2

mpfr-4.1.0

mtx-1.3.12_1

ncurses-6.2.20210313

net-snmp-5.9_3,1

netperf-2.7.1.p20170921_1

nettle-3.6

nginx-1.18.0_47,2

node14-14.16.0

npth-1.6

openjdk8-8.282.08.1

openIdap-sasl-client-2.4.57

p4-2016.1.1492381_3

pcre-8.44

pdksh-5.2.14p2_6

perl5-5.32.1_1

pgbadger-11.5

pinentry-1.1.1

pinentry-curses-1.1.1

pkg-1.16.3

png-1.6.37_1

popt-1.18_1

postgresql96-client-9.6.21

postgresql96-contrib-9.6.21

postgresql96-server-9.6.21

python37-3.7.10

readline-8.1.0

redis-6.0.12

rrdtool-1.7.2_4

ruby-2.6.6_2,1

ruby26-gems-3.0.8

rubygem-actioncable5-5.1.7

rubygem-actionmailer5-5.1.7

rubygem-actionpack5-5.1.7

rubygem-actionview5-5.1.7

rubygem-activejob5-5.1.7

rubygem-activemodel-serializers-xml-1.0.2

rubygem-activemodel4-4.2.11.3

rubygem-activemodel5-5.1.7

rubygem-activerecord-import-1.0.8

rubygem-activerecord4-4.2.11.3

rubygem-activerecord5-5.1.7

rubygem-activeresource-5.1.1

rubygem-activesupport4-4.2.11.3

rubygem-activesupport5-5.1.7_1

rubygem-addressable-2.7.0

rubygem-arel6-6.0.4

rubygem-arel8-8.0.0,1

rubygem-aws-eventstream-1.1.0

rubygem-aws-partitions-1.429.0

rubygem-aws-sdk-3.0.1

rubygem-aws-sdk-accessanalyzer-1.16.0

rubygem-aws-sdk-acm-1.39.0

rubygem-aws-sdk-acmpca-1.33.0

rubygem-aws-sdk-alexaforbusiness-1.44.0

rubygem-aws-sdk-amplify-1.28.0

rubygem-aws-sdk-amplifybackend-1.2.0

rubygem-aws-sdk-apigateway-1.59.0

rubygem-aws-sdk-apigatewaymanagementapi-1.20.0

rubygem-aws-sdk-apigatewayv2-1.31.0

rubygem-aws-sdk-appconfig-1.13.0

rubygem-aws-sdk-appflow-1.7.0

rubygem-aws-sdk-appintegrationsservice-1.1.0

rubygem-aws-sdk-applicationautoscaling-1.50.0

rubygem-aws-sdk-applicationdiscoveryservice-1.34.0

rubygem-aws-sdk-applicationinsights-1.17.0

rubygem-aws-sdk-appmesh-1.34.0

rubygem-aws-sdk-appregistry-1.4.0

rubygem-aws-sdk-appstream-1.50.0

rubygem-aws-sdk-appsync-1.39.0

rubygem-aws-sdk-athena-1.35.0

rubygem-aws-sdk-auditmanager-1.3.0

rubygem-aws-sdk-augmentedairuntime-1.11.0

rubygem-aws-sdk-autoscaling-1.55.0

rubygem-aws-sdk-autoscalingplans-1.30.0

rubygem-aws-sdk-backup-1.27.0

rubygem-aws-sdk-batch-1.44.0

rubygem-aws-sdk-braket-1.6.0

rubygem-aws-sdk-budgets-1.37.0

rubygem-aws-sdk-chime-1.41.0

rubygem-aws-sdk-cloud9-1.30.0

rubygem-aws-sdk-clouddirectory-1.30.0

rubygem-aws-sdk-cloudformation-1.48.0

rubygem-aws-sdk-cloudfront-1.48.0

rubygem-aws-sdk-cloudhsm-1.28.0

rubygem-aws-sdk-cloudhsmv2-1.32.0

rubygem-aws-sdk-cloudsearch-1.28.0

rubygem-aws-sdk-cloudsearchdomain-1.23.0

rubygem-aws-sdk-cloudtrail-1.33.0

rubygem-aws-sdk-cloudwatch-1.49.0

rubygem-aws-sdk-cloudwatchevents-1.41.0

rubygem-aws-sdk-cloudwatchlogs-1.39.0

rubygem-aws-sdk-codeartifact-1.7.0

rubygem-aws-sdk-codebuild-1.69.0

rubygem-aws-sdk-codecommit-1.41.0

rubygem-aws-sdk-codedeploy-1.38.0

rubygem-aws-sdk-codeguruprofiler-1.13.0

rubygem-aws-sdk-codegurureviewer-1.15.0

rubygem-aws-sdk-codepipeline-1.41.0

rubygem-aws-sdk-codestar-1.28.0

rubygem-aws-sdk-codestarconnections-1.13.0

rubygem-aws-sdk-codestarnotifications-1.9.0

rubygem-aws-sdk-cognitoidentity-1.30.0

rubygem-aws-sdk-cognitoidentityprovider-1.49.0

rubygem-aws-sdk-cognitosync-1.25.0

rubygem-aws-sdk-comprehend-1.43.0

rubygem-aws-sdk-comprehendmedical-1.24.0

rubygem-aws-sdk-computeoptimizer-1.14.0

rubygem-aws-sdk-configservice-1.58.0

rubygem-aws-sdk-connect-1.41.0

rubygem-aws-sdk-connectcontactlens-1.1.0

rubygem-aws-sdk-connectparticipant-1.10.0

rubygem-aws-sdk-core-3.112.0

rubygem-aws-sdk-costandusagereportservice-1.29.0

rubygem-aws-sdk-costexplorer-1.58.0

rubygem-aws-sdk-customerprofiles-1.3.0

rubygem-aws-sdk-databasemigrationservice-1.51.0

rubygem-aws-sdk-dataexchange-1.12.0

rubygem-aws-sdk-datapipeline-1.25.0

rubygem-aws-sdk-datasync-1.29.0

rubygem-aws-sdk-dax-1.28.0

rubygem-aws-sdk-detective-1.14.0

rubygem-aws-sdk-devicefarm-1.40.0

rubygem-aws-sdk-devopsguru-1.4.0

rubygem-aws-sdk-directconnect-1.38.0

rubygem-aws-sdk-directoryservice-1.38.0

rubygem-aws-sdk-dlm-1.39.0

rubygem-aws-sdk-docdb-1.28.0

rubygem-aws-sdk-dynamodb-1.59.0

rubygem-aws-sdk-dynamodbstreams-1.28.0

rubygem-aws-sdk-ebs-1.12.0

rubygem-aws-sdk-ec2-1.225.0

rubygem-aws-sdk-ec2instanceconnect-1.12.0

rubygem-aws-sdk-ecr-1.41.0

rubygem-aws-sdk-ecrpublic-1.2.0

rubygem-aws-sdk-ecs-1.74.0

rubygem-aws-sdk-efs-1.37.0

rubygem-aws-sdk-eks-1.49.0

rubygem-aws-sdk-elasticache-1.53.0

rubygem-aws-sdk-elasticbeanstalk-1.41.0

rubygem-aws-sdk-elasticinference-1.11.0

rubygem-aws-sdk-elasticloadbalancing-1.30.0

rubygem-aws-sdk-elasticloadbalancingv2-1.60.0

rubygem-aws-sdk-elasticsearchservice-1.49.0

rubygem-aws-sdk-elastictranscoder-1.28.0

rubygem-aws-sdk-emr-1.42.0

rubygem-aws-sdk-emrcontainers-1.2.0

rubygem-aws-sdk-eventbridge-1.19.0

rubygem-aws-sdk-firehose-1.36.0

rubygem-aws-sdk-fms-1.34.0

rubygem-aws-sdk-forecastqueryservice-1.11.0

rubygem-aws-sdk-forecastservice-1.15.0

rubygem-aws-sdk-frauddetector-1.16.0

rubygem-aws-sdk-fsx-1.34.0

rubygem-aws-sdk-gamelift-1.41.0

rubygem-aws-sdk-glacier-1.36.0

rubygem-aws-sdk-globalaccelerator-1.29.0

rubygem-aws-sdk-glue-1.84.0

rubygem-aws-sdk-gluedatabrew-1.5.0

rubygem-aws-sdk-greengrass-1.38.0

rubygem-aws-sdk-greengrassv2-1.2.0

rubygem-aws-sdk-groundstation-1.16.0

rubygem-aws-sdk-guardduty-1.44.0

rubygem-aws-sdk-health-1.33.0

rubygem-aws-sdk-healthlake-1.2.0

rubygem-aws-sdk-honeycode-1.5.0

rubygem-aws-sdk-iam-1.48.0

rubygem-aws-sdk-identitystore-1.4.0

rubygem-aws-sdk-imagebuilder-1.19.0

rubygem-aws-sdk-importexport-1.25.0

rubygem-aws-sdk-inspector-1.33.0

rubygem-aws-sdk-iot-1.66.0

rubygem-aws-sdk-iot1clickdevicesservice-1.27.0

rubygem-aws-sdk-iot1clickprojects-1.27.0

rubygem-aws-sdk-iotanalytics-1.37.0

rubygem-aws-sdk-iotdataplane-1.27.0

rubygem-aws-sdk-iotdeviceadvisor-1.1.0

rubygem-aws-sdk-iotevents-1.22.0

rubygem-aws-sdk-ioteventsdata-1.14.0

rubygem-aws-sdk-iotfleethub-1.1.0

rubygem-aws-sdk-iotjobsdataplane-1.26.0

rubygem-aws-sdk-iotsecuretunneling-1.10.0

rubygem-aws-sdk-iotsitewise-1.19.0

rubygem-aws-sdk-iotthingsgraph-1.13.0

rubygem-aws-sdk-iotwireless-1.2.0

rubygem-aws-sdk-ivs-1.7.0

rubygem-aws-sdk-kafka-1.34.0

rubygem-aws-sdk-kendra-1.21.0

rubygem-aws-sdk-kinesis-1.31.0

rubygem-aws-sdk-kinesisanalytics-1.30.0

rubygem-aws-sdk-kinesisanalyticsv2-1.25.0

rubygem-aws-sdk-kinesisvideo-1.31.0

rubygem-aws-sdk-kinesisvideoarchivedmedia-1.31.0

rubygem-aws-sdk-kinesisvideomedia-1.27.0

rubygem-aws-sdk-kinesisvideosignalingchannels-1.9.0

rubygem-aws-sdk-kms-1.42.0

rubygem-aws-sdk-lakeformation-1.12.0

rubygem-aws-sdk-lambda-1.59.0

rubygem-aws-sdk-lambdapreview-1.25.0

rubygem-aws-sdk-lex-1.34.0

rubygem-aws-sdk-lexmodelbuildingservice-1.43.0

rubygem-aws-sdk-lexmodelsv2-1.1.0

rubygem-aws-sdk-lexruntimev2-1.1.0

rubygem-aws-sdk-licensemanager-1.24.0

rubygem-aws-sdk-lightsail-1.45.0

rubygem-aws-sdk-locationservice-1.1.0

rubygem-aws-sdk-lookoutforvision-1.2.0

rubygem-aws-sdk-machinelearning-1.26.0

rubygem-aws-sdk-macie-1.27.0

rubygem-aws-sdk-macie2-1.23.0

rubygem-aws-sdk-managedblockchain-1.20.0 Official

rubygem-aws-sdk-marketplacecatalog-1.10.0 Official

rubygem-aws-sdk-marketplacecommerceanalytics-1.31.0

rubygem-aws-sdk-marketplaceentitlementservice-1.25.0

rubygem-aws-sdk-marketplacemetering-1.33.0

rubygem-aws-sdk-mediaconnect-1.29.0

rubygem-aws-sdk-mediaconvert-1.63.0

rubygem-aws-sdk-medialive-1.64.0

rubygem-aws-sdk-mediapackage-1.37.0

rubygem-aws-sdk-mediapackagevod-1.21.0

rubygem-aws-sdk-mediastore-1.31.0

rubygem-aws-sdk-mediastoredata-1.28.0

rubygem-aws-sdk-mediatailor-1.35.0

rubygem-aws-sdk-migrationhub-1.30.0

rubygem-aws-sdk-migrationhubconfig-1.10.0

rubygem-aws-sdk-mobile-1.25.0

rubygem-aws-sdk-mq-1.35.0

rubygem-aws-sdk-mturk-1.28.0

rubygem-aws-sdk-mwaa-1.1.0

rubygem-aws-sdk-neptune-1.33.0

rubygem-aws-sdk-networkfirewall-1.1.0

rubygem-aws-sdk-networkmanager-1.10.0

rubygem-aws-sdk-opsworks-1.31.0

rubygem-aws-sdk-opsworkscm-1.41.0

rubygem-aws-sdk-organizations-1.57.0

rubygem-aws-sdk-outposts-1.14.0

rubygem-aws-sdk-personalize-1.21.0

rubygem-aws-sdk-personalizeevents-1.16.0

rubygem-aws-sdk-personalizeruntime-1.21.0

rubygem-aws-sdk-pi-1.26.0

rubygem-aws-sdk-pinpoint-1.51.0

rubygem-aws-sdk-pinpointemail-1.25.0

rubygem-aws-sdk-pinpointsmsvoice-1.22.0

rubygem-aws-sdk-polly-1.39.0

rubygem-aws-sdk-pricing-1.25.0

rubygem-aws-sdk-prometheusservice-1.2.0

rubygem-aws-sdk-qldb-1.12.0

rubygem-aws-sdk-qldbsession-1.12.0

rubygem-aws-sdk-quicksight-1.43.0

rubygem-aws-sdk-ram-1.23.0

rubygem-aws-sdk-rds-1.115.0

rubygem-aws-sdk-rdsdataservice-1.24.0

rubygem-aws-sdk-redshift-1.54.0

rubygem-aws-sdk-redshiftdataapiservice-1.5.0

rubygem-aws-sdk-rekognition-1.48.0

rubygem-aws-sdk-resourcegroups-1.34.0

rubygem-aws-sdk-resourcegroupstaggingapi-1.36.0

rubygem-aws-sdk-resources-3.94.0

rubygem-aws-sdk-robomaker-1.33.0

rubygem-aws-sdk-route53-1.46.0

rubygem-aws-sdk-route53domains-1.29.0

rubygem-aws-sdk-route53resolver-1.23.0

rubygem-aws-sdk-s3-1.89.0

rubygem-aws-sdk-s3control-1.28.0

rubygem-aws-sdk-s3outposts-1.1.0

rubygem-aws-sdk-sagemaker-1.79.0

rubygem-aws-sdk-sagemakeredgemanager-1.1.0

rubygem-aws-sdk-sagemakerfeaturestoreruntime-1.1.0

rubygem-aws-sdk-sagemakerruntime-1.30.0

rubygem-aws-sdk-savingsplans-1.13.0

rubygem-aws-sdk-schemas-1.11.0

rubygem-aws-sdk-secretsmanager-1.44.0

rubygem-aws-sdk-securityhub-1.40.0

rubygem-aws-sdk-serverlessapplicationrepository-1.33.0

rubygem-aws-sdk-servicecatalog-1.58.0

rubygem-aws-sdk-servicediscovery-1.32.0

rubygem-aws-sdk-servicequotas-1.13.0

rubygem-aws-sdk-ses-1.37.0

rubygem-aws-sdk-sesv2-1.16.0

rubygem-aws-sdk-shield-1.34.0

rubygem-aws-sdk-signer-1.28.0

rubygem-aws-sdk-simpledb-1.25.0

rubygem-aws-sdk-sms-1.28.0

rubygem-aws-sdk-snowball-1.36.0

rubygem-aws-sdk-sns-1.38.0

rubygem-aws-sdk-sqs-1.36.0

rubygem-aws-sdk-ssm-1.104.0

rubygem-aws-sdk-ssoadmin-1.6.0

rubygem-aws-sdk-ssooidc-1.9.0

rubygem-aws-sdk-states-1.38.0

rubygem-aws-sdk-storagegateway-1.53.0

rubygem-aws-sdk-support-1.29.0

rubygem-aws-sdk-swf-1.26.0

rubygem-aws-sdk-synthetics-1.11.0

rubygem-aws-sdk-textract-1.23.0

rubygem-aws-sdk-timestreamquery-1.3.0

rubygem-aws-sdk-timestreamwrite-1.3.0

rubygem-aws-sdk-transcribeservice-1.51.0

rubygem-aws-sdk-transcribestreamingservice-1.26.0

rubygem-aws-sdk-transfer-1.31.0

rubygem-aws-sdk-translate-1.30.0

rubygem-aws-sdk-waf-1.37.0

rubygem-aws-sdk-wafregional-1.38.0

rubygem-aws-sdk-wafv2-1.16.0

rubygem-aws-sdk-wellarchitected-1.2.0

rubygem-aws-sdk-workdocs-1.29.0

rubygem-aws-sdk-worklink-1.22.0

rubygem-aws-sdk-workmail-1.35.0

rubygem-aws-sdk-workmailmessageflow-1.11.0

rubygem-aws-sdk-workspaces-1.50.0

rubygem-aws-sdk-xray-1.36.0

rubygem-aws-sigv2-1.0.1

rubygem-aws-sigv4-1.2.2

rubygem-bindata-2.4.8

rubygem-bindex-0.8.1

rubygem-bluestorm_cli-3.0.0.2267048

rubygem-builder-3.2.4

rubygem-bundler-2.2.11,1

rubygem-byebug-11.1.3

rubygem-capybara-3.35.3

rubygem-childprocess3-3.0.0

rubygem-coffee-rails-rails5-4.2.2

rubygem-coffee-script-2.4.1

rubygem-coffee-script-source-1.12.2

rubygem-colorize-0.8.1

rubygem-concurrent-ruby-1.1.8

rubygem-cookiejar-0.3.3

rubygem-crass-1.0.4

rubygem-cucumber-5.3.0_1

rubygem-cucumber-core-8.0.1_2

rubygem-cucumber-create-meta2-2.0.4

rubygem-cucumber-cucumber-expressions10-10.3.0

rubygem-cucumber-gherkin15-15.0.2_1

rubygem-cucumber-html-formatter9-9.0.0

rubygem-cucumber-messages13-13.2.1

rubygem-cucumber-tag-expressions-2.0.4

rubygem-cucumber-wire-4.0.1_2

rubygem-daemons-1.3.1

rubygem-devdctl-0.1.0.2275716

rubygem-devstat_stat-0.0.1.1280468

rubygem-diff-lcs-1.4.4

rubygem-digest-crc-0.4.1

rubygem-docile-1.3.5

rubygem-ds3-0.0.1.1358398

rubygem-ds3apitest-0.1.0.1673930_6

rubygem-ejs-1.1.1

rubygem-em-http-request-1.1.5

rubygem-em-socksify-0.3.2

rubygem-erubi-1.10.0

rubygem-etc-1.2.0

rubygem-eventmachine-1.2.7

rubygem-execjs-2.7.0

rubygem-faraday-1.3.0

rubygem-faraday-net_http-1.0.1

rubygem-faraday_middleware-1.0.0

rubygem-faye-1.2.4

rubygem-faye-websocket-0.10.7

rubygem-ffi-1.14.2

rubygem-ffi-locale-1.0.1_2

rubygem-ffi-ncurses-0.4.0_3

rubygem-fio_rb-1.1.0.1686791

rubygem-freebsd_cam-1.0.7.1953869

rubygem-freebsd_mps-1.1.1.1325934

rubygem-freebsd_ses-1.3.2.1325934

rubygem-globalid-rails5-0.4.2

rubygem-http_parser.rb-0.6.0

rubygem-i18n-1.8.9,2

rubygem-i18n-js-3.0.11

rubygem-inifile-3.0.0

rubygem-io-console-0.5.9

rubygem-ipaddress-0.8.3_4

rubygem-irb-1.3.4

rubygem-jbuilder-rails5-2.11.2

rubygem-jmespath-1.4.0

rubygem-jquery-rails-rails5-4.4.0

rubygem-json-2.3.1

rubygem-json_pure-2.3.1

rubygem-key_verify-1.0.1.1750298

rubygem-libifconfig-0.1.0.2275716_1

rubygem-libxml-ruby-3.1.0

rubygem-live_record-0.2.1.1686790

rubygem-liveresource-2.1.2.1638704

rubygem-loofah-2.9.0

rubygem-lsiexp-1.2.4.1780170

rubygem-mail-2.7.1,2

rubygem-method_source-1.0.0

rubygem-middleware-0.1.0

rubygem-mini_mime-1.0.2

rubygem-minitest-5.14.1

rubygem-mocha-1.11.2

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-1.2.1

rubygem-net-ssh-6.0.2,2

rubygem-nio4r-2.5.5

rubygem-nokogiri-1.11.1

rubygem-open4-1.3.4

rubygem-os-1.1.1

rubygem-pam-1.5.2.2267479

rubygem-passenger-nginx-6.0.7_1

rubygem-pg-1.2.3

rubygem-pkg-config-1.4.5

rubygem-pmbus-1.1.2.1718448

rubygem-power_assert-1.2.0

rubygem-pqueue-2.1.0

rubygem-pretty-xml-0.2.2

rubygem-protobuf-cucumber-3.10.8

rubygem-public_suffix-4.0.6_6

rubygem-puma-5.1.1

rubygem-racc-1.5.2

rubygem-rack-2.2.3,3

rubygem-rack-test-1.1.0

rubygem-rack16-1.6.13

rubygem-rails-dom-testing-rails5-2.0.3_1

rubygem-rails-html-sanitizer-1.3.0

rubygem-rails5-5.1.7_2

rubygem-railties5-5.1.7

rubygem-rake-13.0.3

rubygem-rb-fsevent-0.10.3

rubygem-rb-inotify-0.10.1

rubygem-rb-kqueue-0.2.5_1

rubygem-rbcurse-1.5.3

rubygem-rbcurse-core-0.0.14_1

rubygem-rbcurse-extras-0.0.0

rubygem-rdoc-6.3.0

rubygem-redis-4.2.5

rubygem-redis-actionpack-rails5-5.2.0

rubygem-redis-activesupport-rails5-5.2.0

rubygem-redis-rack-2.1.3

rubygem-redis-rails-rails5-5.0.2

rubygem-redis-store-1.9.0

rubygem-regexp_parser-1.8.2

rubygem-reline-0.2.4

rubygem-rice-2.2.0

rubygem-rrd-ffi-0.2.14_3

rubygem-rspec-expectations-3.10.1

rubygem-rspec-support-3.10.2

rubygem-ruby-termios-1.0.2

rubygem-ruby2_keywords-0.0.4

rubygem-rubyzip-2.3.0

rubygem-sass-3.7.4

rubygem-sass-listen-4.0.0

rubygem-sass-rails-rails5-6.0.0

rubygem-sassc-2.4.0

rubygem-sassc-rails-rails5-2.1.2_1

rubygem-selenium-webdriver-3.142.7_1

rubygem-serialport-1.3.1_2

rubygem-simplecov-0.19.0

rubygem-simplecov-html-0.12.2

rubygem-smart_data-0.0.2.1686790

rubygem-snmp-1.2.0

rubygem-spectra_acl-1.2.1.1978621_1

rubygem-spectra_cli-1.0.2.1933739

rubygem-spectra_platform-1.3.1.2422786

rubygem-spectra_support-5.0.0.2275716

rubygem-spectra_view-2.3.0.2422680_9

rubygem-spectra_workers-5.0.0.2275716

rubygem-spring-2.1.1

rubygem-sprockets-rails-rails5-3.2.2

rubygem-sprockets3-3.7.2

rubygem-sqlite3-1.4.2

rubygem-staf4ruby-0.1.3.1325934,1

rubygem-sys-uname-1.2.2

rubygem-tape_backend-0.1.1676819

rubygem-test-unit-3.3.6

rubygem-thin-1.7.2

rubygem-thor-1.1.0

rubygem-thread_safe-0.3.6

rubygem-tilt-2.0.9

rubygem-turbolinks-5.2.1

rubygem-turbolinks-source-5.2.0

rubygem-tzinfo1-1.2.9

rubygem-uglifier-4.1.20

rubygem-uuidtools-2.1.5

rubygem-web-console3-rails5-3.7.0

rubygem-websocket-driver-0.7.3

rubygem-websocket-extensions-0.1.5

rubygem-xpath-3.2.0

rubygem-yard-0.9.26

rubygem-zfs-0.0.12.2275716

samba413-4.13.7_1

sedutil-1.12.2267418

sg3_utils-1.45

smartmontools-7.2_1

smp_utils-0.98_1

source-highlight-3.1.9_1

spectra_ltfs-2.4.2.1.2275716_1

sqlite3-3.34.1,1

staf-3.4.26_1

stress-1.0.4_1

stress-ng-0.12.05

t5seeprom-0.0.1135916_1

talloc-2.3.1

tdb-1.4.3,1

tevent-0.10.2_1

tidy-html5-5.7.28

tmux-3.1c

tomcat-native-1.2.24_1

tomcat85-8.5.64

verde_hotpair-2.1.2275716

vim-8.2.2569

zip-3.0_1

zsh-5.8

Index

Α Activation keys entering manually 217 importing automatically 57 Active Directory, join 232 Amazon S3 data replication rule about 140 add to data policy 140 delete 157 edit 155 Amazon S3 target about 118 create 118 Apache, open source acknowledgement 455 autosupport about 343 configure mail recipient 344 enter contact information 343 В BlackPearl components 33, 41, 440, 444 features 30 monitoring 308 overview 30 power 55 serial number 405 size and weight 422 specifications 421, 445 updating 361 BlackPearl data replication rule about 138 add to data policy 138

delete 157 edit 154

BlackPearl software
current available version 362
BlackPearl target
about 115
create 115
BlackPearl user interface
about 47
current version 361
exit 341
log in 58
menus 48
overview 47
status icons 51
supported browsers 49, 52
bucket
about 142
configure 172
create 142
delete 175
edit 174
C
CE Marking 451
certificates
configure 216
CIFS
configure service 239
create new share 232
edit share 264
remove sharing 265
set permissions 235
cleaning cartridges, using with MLM
Cleans Remaining report 376
Cleans Remaining, MLM report 376
component OK icon 51
components
front view 37, 440
rear panel 41, 443
configuring
bucket 172

certificates 216	disk partition
CIFS service 239	about 107, 113
DNS 185	create 107, 113
email 186	delete 169
Ethernet ports 179	edit 169
mail recipients 344	DNS, configure 185
NAS replication 243	documentation
NAS storage pools 221	typographical conventions 26
NAS volumes 225	
network connections 178	E
NFI 240	.,
NFI volume policy 228	email
NFS service 241	configuring 186
NTP 187	send test 346
S3 service 189	Spectra Logic offices 8
services 188, 238	error condition icon 51
shares 232	Ethernet ports, configure 179
SMTP 186	EU Declaration of Conformity 447
snapshots 255	_
user 207	F
Conflict Mineral Policy 453	fax numbers, Spectra Logic 8
contact information, enter 343	FCC Notice 452
contacting Spectra Logic 8	Free BSD
contacting, Technical Support 404	open source acknowledgement 455
corporate headquarters, Spectra Logic 8	front view 37, 440
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1	
D	н
data integrity verification	hardware
disk pools 353	monitor status 314
tape media 355	
data persistence rule	'
about 136	icons
add to data policy 136	component OK 51
delete 162	error condition 51
edit 160	information 51
data policy	unknown state 51
about 131	warning 51
create 131	information icon 51
delete 159	
edit 158	

]
J	restore files from a replication
Java	target 268
open source acknowledgement 456	NAS storage pools
opensource action meagement 100	about 221
L	create new 221
	delete 251
license agreement, software 4	expand 250
	options 110, 113, 223
М	protection levels 110, 113, 224
mail recipients	requirements 221
add 344	NAS volumes
configure 344	about 221
mailing address, Spectra Logic 8	configure 225
maintenance, replace component 365	create new CIFS share 232
management port, use 179	create new NFS share 237
MIB file, download 198	create snapshot 256
Microsoft Azure data replication rule	delete 255
about 141	delete snapshot 260
add to data policy 141	edit 253
delete 157	edit share 264
edit 156	move 252
Microsoft Azure target	options 226, 228
about 122	remove sharing 265
create 122	replication 242
MLM reports	restore file from snapshot 263
Cleans Remaining 376	restore snapshot 262
Crown remaining or c	scheduled snapshots 257
N	snapshot restore 262
	snapshots 255
NAS replication	nearline disk pool
cancel replication in progress 267	import 170
configure 243	network
configure schedule 246	cables 435, 446
configure volumes 244	configure 178
delete 270	configure DNS 185
disable 268	NFI
edit configuration 269	configure 228, 240
manual 266	edit service 240, 271
NAS volumes 242	restore files 274

NFS	R
configure service 241	rear panel 41, 443
create new share 237	rear view 39, 442
edit share 264	recycling 453
remove sharing 265	regulatory
Nginx, open source	CE Marking 451
acknowledgement 464	Conflict Mineral Policy 453
NTP	EU Declaration of Conformity 447
configuring 187	FCC Notice 452
	RoHS 453
0	Safety Standards and Compliance 452
online disk pool	WEEE Directive 453
create 111	replication, see NAS replication 269
delete 172	reports, MLM
import 170	Cleans Remaining 376
open source acknowledgement	RoHS 453
Apache 455	Ruby on rails, open source acknow-
Free BSD 455	ledgement 466
Java 456	Ruby, open source acknowledgement 464
Nginx 464	
Ruby 464	S
Ruby on rails 466	S3 group
ZFS 466	create 212
P	S3 service
	configure 189
performance metrics 327	Safety Standards and Compliance 452
phone numbers, Spectra Logic offices 8	sales, contacting 8
pools, see NAS storage pools, nearline	serial number
disk pools, or online disk pools 221	where to find 405
portal	services
accessing for technical support 357,	CIFS 239
359	configuring 188, 238
See also technical support 408	NAS replication 242
power	NFI 240
power off 339	NFS 241
power on 55	status 316
reboot 339	shares
requirements 428	about 221

	I
configure 232	create 124
create new CIFS 232	delete 153
create new NFS 237	edit 152
delete 265	storage domain member
edit 264	about 129
manage 263	adding 129
SMTP	delete 151
configure 186	edit 149-151
snapshots	storage pools, see NAS storage pools,
about 255	nearline disk pools, or online disk
configure 255	pools, 221
create new 256	support
daily, create 246, 258	contacting 404
delete 260	opening ticket 405
hourly, create 246, 257	support portal
restore 262	accessing 357
retrieve single file 263	support ticket
scheduled, about 257	sending 405
weekly, create 247, 259	system messages 313
SNMP service	system name
configure 193, 197	edit 188
software	
license agreement 4	т
software version	
check current available version 362	tape partition
specifications	about 114
data storage 416	create 114
environmental 425	technical support
power 428	accessing the Technical Support
power cords 430	portal 357, 359
size and weight 422	contacting 8
system 421, 445	See also portal[technical support
Spectra Logic	zzz] 408
contacting 8	222] 100
Spectra S3	typographical conventions 26
clients 75	
online forum 28	U
status lights 310	unknown state icon 51
storage domain	updates
about 124	download 363
	download 500

```
USB, support 436
user
  configure 207
  delete 210
  edit 207
  types 207
V
Visual Status Beacon, lights 309
volumes, see NAS volumes 221
W
warning icon 51
website
  Spectra Logic 8
WEEE Directive 453
WORM tape media, not supported 78,
     115, 276
```

Z

ZFS, open source acknowledgement 466