

EMC

XtremIO Storage Array

Versions 4.0 and 4.0.1

User Guide

P/N 302-002-053

REV. 03

EMC²

Copyright © 2015 EMC Corporation. All rights reserved. Published in the USA.

Published August, 2015

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC², EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (<https://support.emc.com>).

CONTENTS

Preface

Part 1 Introduction

Chapter 1 System Description

System Overview.....	18
X-Brick	19
Scale-Out Architecture	20
5TB Starter Kit.....	21
System Features.....	21
Scalable Performance	21
Even Data Distribution.....	22
Inline Data Reduction.....	23
High Availability	25
Non-Disruptive Upgrade	26
Thin Provisioning	26
XtremIO Data Protection (XDP).....	27
Snapshots	28
VMware VAAI Integration	30
Data at Rest Encryption	31
XtremIO Management Server (XMS).....	31
System GUI	32
Command Line Interface.....	32
RESTful API	32
Ports and Protocols.....	33

Chapter 2 Using the Graphical User Interface (GUI)

GUI Window	36
Menu Bar Icons	37
Accessing the GUI	38
Installing a Local Java Bundle.....	43
Dashboard Workspace	45
Storage Pane.....	46
Performance Pane	47
Inventory Pane	48
Alerts Pane.....	49
Multiple Cluster Configuration.....	51
Multiple Cluster Configuration in GUI.....	51
Multiple Cluster Configuration in CLI	52
Configuration Workspace	53
Volumes View	54
Consistency Groups View	57
Snapshot Sets View	59
Initiator Groups View.....	61
Initiators View.....	63
Schedulers View	65

Inventory Workspace.....	67
Main Icons	68
Hardware Drop-Down Menu Options.....	69
Hardware Components' LEDs	70
Main Elements	72
Hardware Customize view	73
Inventory List View	74
Cluster Configuration	90
Alerts & Events Workspace.....	94
Alerts Tab.....	95
Events Tab	97
Reports Workspace	99
Administration Workspace	101
Security Tab	102
Notification Tab.....	105
XMS Tab.....	108
CLI Terminal Tab.....	110
Support Window	111
Chapter 3	Managing the Hardware
Managing Hardware Tags	116
Managing Tags, Using the GUI	116
Managing Tags, Using the CLI.....	120
Hardware Components' LEDs	121
Using the Identification LEDs.....	122
Chapter 4	Monitoring the Cluster
Monitoring the Storage	124
Monitoring the Efficiency.....	124
Monitoring the Volume Capacity.....	125
Monitoring the Physical Capacity.....	125
Monitoring the Performance	126
Monitoring the Performance, Using the GUI	126
Monitoring Performance, Using the CLI	127
Monitoring the Hardware Elements	127
Monitoring the Clusters	127
Monitoring the X-Bricks	129
Monitoring the Storage Controllers	130
Monitoring the SSDs	131
Monitoring the InfiniBand Switches.....	131
Monitoring the Data Protection Groups.....	132
Monitoring the Local Disks	134
Monitoring the Battery Backup Units	134
Monitoring the DAEs.....	135
Monitoring the Targets	136
Monitoring the Storage Elements	139
Monitoring the Volumes	139
Monitoring the Consistency Groups.....	142
Monitoring the Initiators.....	144
Monitoring the Initiator Groups	146
Monitoring the Snapshot Sets	148

Monitoring the Alerts	150
Monitoring Alerts, Using the GUI.....	150
Monitoring Alerts, Using the CLI	150
Managing the Reports	151
Predefined Reports.....	151
Viewing Reports	152
Managing Reports, Using the GUI	153
Managing Reports, Using the CLI.....	160
Chapter 5 Managing Volume Operations	
Overview.....	162
Managing Storage Elements Tags	163
Managing Tags, Using the GUI.....	164
Managing Tags, Using the CLI.....	167
Managing Volumes and Snapshots	168
Managing Volumes and Snapshots, Using the GUI	169
Managing Volumes and Snapshots, Using the CLI	203
Managing the Consistency Groups	204
Managing Consistency Groups, Using the GUI	204
Managing Consistency Groups, Using the CLI	225
Managing the Snapshot Sets	226
Managing Snapshot Sets, Using the GUI.....	226
Managing Snapshot Sets, Using the CLI	238
Managing the Initiator Groups.....	239
Managing Initiator Groups, Using the GUI.....	239
Managing Initiator Groups, Using the CLI.....	249
Managing Initiators	250
Managing Initiators, Using the GUI	250
Managing Initiators, Using the CLI	252
Managing Mapping	253
Basic Mapping Scenario.....	253
Using Tags for Mapping.....	256
Using the Mapping Wizard	258
Managing the Schedulers.....	261
Managing Schedulers, Using the GUI.....	261
Managing Schedulers, Using the CLI.....	263
Chapter 6 Managing Alerts and Events	
Managing the Alerts	266
Alerts Overview	266
Managing Alerts, Using the GUI	266
Managing Alerts, Using the CLI	270
Managing the Events.....	271
Managing Events, Using the GUI.....	271
Managing Events, Using the CLI.....	275

Chapter 7	Cluster Administration and Configuration	
	Configuring the iSCSI Portals and Routes.....	278
	Managing iSCSI Portals and Routes, Using the GUI	278
	Managing iSCSI Portals and Routes, Using the CLI	283
	Configuring the iSCSI Port Number	284
	Configuring the iSCSI Port via the GUI.....	284
	Setting the Maximum Transmission Unit for iSCSI.....	286
	Configuring Jumbo Frames via the GUI.....	287
	Configuring the Cluster Limits	288
	Configuring Cluster Limits via the GUI.....	288
	Configuring Cluster Limits via the CLI.....	289
	Configuring the Cluster ODX Mode.....	289
	Configuring the ODX Mode via the GUI.....	289
	Configuring the ODX Mode via the CLI	290
	Configuring the iSCSI Security Parameters (CHAP)	291
	Configuring CHAP via the GUI	292
	Configuring CHAP via the CLI	293
	Configuring the Cluster Encryption	293
	Configuring the User Accounts.....	294
	User Accounts Overview	294
	Managing User Accounts, Using the GUI.....	294
	Managing User Accounts, Using the CLI.....	297
	Configuring the LDAP Users Authentication	298
	Setting the XMS Server LDAP Configuration	299
	Configuring LDAP Settings via the GUI	300
	Configuring LDAP Settings via the CLI	307
	Configuring Email Settings	308
	Managing Email Settings, Using the GUI.....	308
	Managing Email Settings, Using the CLI.....	310
	Configuring the SNMP	311
	Configuring SNMP, Using the GUI	311
	Configuring SNMP, Using the CLI	313
	XtremIO MIB.....	313
	Configuring the Remote Syslog Notification	314
	Configuring Remote Syslog via the GUI	314
	Configuring Syslog Settings via the CLI	315
	Configuring the Default Inactivity timeout.....	316
	Configuring the Inactivity Timeout via the GUI.....	316
	Configuring Inactivity Timeout via the CLI	316
	Customizing the Login Screen Banner	317
	Customizing the Login Screen Banner via the GUI.....	317
	Customizing the Login Screen Banner via the CLI	317
Chapter 8	Cluster Operations	
	Powering Up the Cluster	320
	Powering Up the Cluster after an Emergency Shutdown	320
	Powering Up Procedure	320
	Locating the Cluster	321
	Powering Up the Battery Backup Units.....	322
	Powering Up the Storage Controllers	325
	Powering Up the XMS	326
	Starting the Cluster	327

Shutting Down the Cluster - Planned Shutdown.....	329
Planned Cluster Shutdown Overview	329
Pre-Shutdown Procedure.....	329
Shutting Down the Service	331
Shutting Down the Hardware.....	332
Shutting Down the Cluster - Emergency Shutdown.....	334
Changing the IP Configurations	336
Changing the IP Configuration in a Single Cluster Environment.....	336
Changing the IP Configuration in a Multiple Cluster Environment.....	339
Updating the XMS NTP Server Address	342
Setting the Cluster Time and Date	343
Managing the Virtual XMS	344
Deploying a Virtual XMS	344
Relocating a Virtual XMS	346
Restoring Access to the Virtual XMS	346

Chapter 9**CLI Guide**

Using the Command Line Interface (CLI)	350
Accessing the CLI via the GUI.....	350
Accessing the CLI via an SSH Client.....	351
Accessing the CLI via an SSH Key Authentication.....	351
Objects Naming Limitations	352
Completion Codes.....	353
CLI Commands Quick Finder.....	354
Basic CLI Commands.....	362
exit	362
help	362
quit.....	362
Cluster Related CLI Commands	363
set-context.....	363
show-sw-images	363
show-sw-image-details	363
assign-ssd	364
modify-target	364
modify-target-group	364
rename	365
show-bricks.....	366
show-bbus.....	367
show-storage-controllers.....	368
show-clusters.....	369
show-clusters-info.....	370
modify-clusters-parameters.....	371
show-clusters-savings.....	371
show-clusters-upgrade.....	372
show-clusters-upgrade-progress	373
show-cluster-expansion-progress.....	373
show-xms	374
show-xms-info	375
shutdown-xms	376
restart-xms.....	376
modify-xms-parameters	376
show-ip-addresses.....	377
modify-ip-addresses	378
modify-eth-port.....	378

create-ip-link.....	379
remove-ip-link.....	379
modify-ssh-firewall.....	379
test-ip-connectivity	380
show-storage-controllers-infiniband-ports.....	380
show-storage-controllers-infiniband-counters	381
show-infiniband-switches-ports	382
show-infiniband-switches	383
show-infiniband-switches-psus.....	384
show-daes-controllers.....	385
show-daes-psus.....	386
show-daes	387
add-ldap-config.....	388
modify-ldap-config	389
remove-ldap-config	389
show-ldap-configs.....	390
show-syslog-notifier.....	391
show-server-name.....	391
show-remote-servers-status	391
show-timezones.....	391
show-datetime.....	392
modify-datetime.....	392
show-dns-servers.....	392
modify-dns-servers	393
modify-server-name	393
modify-syslog-notifier	393
modify-login-banner.....	393
modify-webui	394
show-report	394
show-reports	395
show-reports-data.....	396
Basic Cluster Management CLI Commands	397
add-cluster.....	397
remove-cluster	397
start-cluster	397
stop-cluster.....	397
power-off	398
power-on.....	398
Volume Related CLI Commands	399
add-volume.....	399
remove-volume	399
modify-volume	400
clear-volume-reservation.....	400
show-volume	401
show-volumes.....	402
show-volume-snapshot-groups	403
create-snapshot	404
create-snapshot-and-reassign.....	404
create-scheduler	405
show-schedulers.....	406
modify-scheduler	407
remove-scheduler	407
resume-scheduler	407
suspend-scheduler	407
show-snapshots.....	408

show-snapshot-sets.....	409
show-snapshot-set	410
remove-snapshot-set	410
add-volume-to-consistency-group.....	411
remove-volume-from-consistency-group.....	411
create-consistency-group	411
show-consistency-group	412
show-consistency-groups.....	413
remove-consistency-group	413
modify-cluster-thresholds	414
show-clusters-thresholds	414
Initiator Group Related CLI Commands	415
add-initiator.....	415
add-initiator-group.....	416
modify-initiator	416
remove-initiator	417
remove-initiator-group	417
show-initiators	418
show-initiator-group.....	419
show-initiator-groups.....	420
show-targets	421
show-target-groups	422
show-discovered-initiators-connectivity	422
show-initiators-connectivity	423
show-chap	424
modify-chap.....	424
LUN Mapping Related CLI Commands	425
map-lun	425
show-lun-mappings	426
unmap-lun	426
Alert Related CLI Commands	427
acknowledge-alert.....	427
modify-alert-definition	427
show-alerts	428
show-alert-definitions	429
Event Related CLI Commands	430
show-events.....	430
show-event-details.....	431
show-event-handler-definitions.....	432
add-event-handler-definition	432
remove-event-handler-definition	432
modify-event-handler-definition	433
ISCSI Routing Related CLI Commands	434
add-iscsi-portal.....	434
add-iscsi-route	434
modify-iscsi-portal	434
remove-iscsi-portal	435
remove-iscsi-route	435
show-iscsi-portals	435
show-iscsi-routes	436
show-iscsi-counters	437
show-clusters-parameters	438
User Account Management Related CLI Commands	439
add-user-account.....	439
modify-user-account	439

modify-password	440
remove-user-account	440
show-user-accounts	440
Notification Related CLI Commands.....	441
show-email-notifier	441
modify-email-notifier.....	442
send-email-notification	442
show-snmp-notifier.....	443
modify-snmp-notifier.....	444
send-snmp-notification	444
show-syr-notifier	445
modify-syr-notifier.....	446
send-syr-notification	446
control-led	447
show-leds	447
Data Protection Related CLI Commands.....	448
remove-ssd	448
show-slots	448
show-ssds.....	449
show-ssd-sas-counters	450
add-ssd.....	451
show-data-protection-groups	452
show-clusters-data-protection-properties.....	453
Cluster Health Related CLI Commands.....	454
show-targets-fc-error-counters	454
show-target-groups-fc-error-counters	455
create-debug-info.....	455
show-debug-info	456
remove-debug-info.....	456
test-xms-storage-controller-connectivity.....	456
test-xms-tcp-connectivity	457
Storage Controllers Related CLI Commands	458
show-storage-controllers-info.....	458
show-storage-controllers-fw-versions	459
show-storage-controllers-psus	460
show-storage-controllers-sensors	461
show-local-disks	462
show-xenvs.....	463
activate-storage-controller	463
deactivate-storage-controller	463
Performance Related CLI Commands	464
show-initiator-groups-performance	464
show-initiator-groups-performance-small.....	465
show-initiator-groups-performance-unaligned.....	466
show-initiators-performance	467
show-initiators-performance-small.....	468
show-initiators-performance-unaligned.....	469
show-most-active.....	470
show-most-active-initiator-groups.....	471
show-most-active-volumes.....	472
show-volumes-performance	473
show-volumes-performance-small.....	474
show-volumes-performance-unaligned	475
show-data-protection-groups-performance	476
show-ssds-performance.....	476

show-clusters-performance	477
show-clusters-performance-small	478
show-clusters-performance-unaligned	479
show-clusters-performance-latency.....	479
show-target-groups-performance	480
show-target-groups-performance-small.....	481
show-target-groups-performance-unaligned.....	482
show-targets-performance	483
show-targets-performance-small.....	484
show-targets-performance-unaligned.....	485
export-performance-history	486
Tag Management CLI Commands	487
create-tag.....	487
tag-object	487
untag-object	487
modify-tag.....	487
remove-tag.....	488
show-tag	488
show-tags	488
Certificate Management CLI Commands	489
create-server-certificate-signing-request	489
modify-server-certificate.....	489
install-self-signed-server-certificate	490
show-server-certificate	490
show-server-certificate-signing-request.....	490

Appendix A**Alerts and Events Details**

General XMS Event Codes	492
Alerts Details	492
Events Details	513

Appendix B**Replacing the Default SSL Certificate**

Overview.....	536
Creating a CSR	536
Submitting the CSR	537
Converting the Certificate Format.....	537
Installing the Certificate	538
Installing a Third Party Certificate that was Created without CSR	539

Contents

PREFACE

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function properly or does not function as described in this document.

Note: This document was accurate at publication time. Go to EMC Online Support (<https://support.emc.com>) to ensure that you are using the latest version of this document.

Purpose

This document provides the required information for using the EMC XtremIO Storage Array.

Audience

This document is intended for the host storage administrator, system administrator, or operator who will be involved in managing the XtremIO Storage Array.

Related Documentation

The following EMC publications provide additional information:

- ◆ *XtremIO Storage Array Host Configuration Guide*
- ◆ *XtremIO Storage Array Site Preparations Guide*
- ◆ *XtremIO Storage Array Security Configuration Guide*
- ◆ *XtremIO Storage Array RESTful API Guide*
- ◆ *XtremIO Storage Array Release Notes*

Introduction

EMC XtremIO Storage Array User Guide is part of the XtremIO documentation set and is intended for use by system administrators responsible for performing day-to-day operations of an XtremIO cluster.

This document provides instructions for managing and monitoring the EMC XtremIO Storage Array.

Chapters in this document provide information on the following topics:

- ◆ [Chapter 1, “System Description”](#)
Provides a detailed overview of the system and its features.
- ◆ [Chapter 2, “Using the Graphical User Interface \(GUI\)”](#)
Provides a detailed description of the system’s GUI.
- ◆ [Chapter 3, “Managing the Hardware”](#)
Provides instructions for managing the cluster’s hardware components.
- ◆ [Chapter 4, “Monitoring the Cluster”](#)
Provides instructions for monitoring the cluster and its various elements and components, including advanced monitoring.
- ◆ [Chapter 5, “Managing Volume Operations”](#)
Provides instructions for managing Volumes, Initiator Groups and LUN mapping.
- ◆ [Chapter 6, “Managing Alerts and Events”](#)
Provides instructions for managing alerts and events.
- ◆ [Chapter 7, “Cluster Administration and Configuration”](#)
Provides instructions for configuring user accounts, email settings, SNMP, and notifications.
- ◆ [Chapter 8, “Cluster Operations”](#)
Provides instructions for operating the EMC XtremIO Storage Array.
- ◆ [Chapter 9, “CLI Guide”](#)
Provides a complete CLI guide, with all CLI commands grouped according to user activities.
- ◆ [Appendix A, “Alerts and Events Details”](#)
Provides detailed lists of all alerts and events.
- ◆ [Appendix B, “Replacing the Default SSL Certificate”](#)
Provides instructions for replacing the default SSL certificate for the XMS with a certificate issued by a trusted third party (Certificate Authority).

Note: For details on configuring hosts connected to the XtremIO storage, refer to the *XtremIO Host Configuration Guide*.

CHAPTER 1

System Description

This chapter includes the following topics:

◆ System Overview	18
◆ X-Brick	19
◆ Scale-Out Architecture	20
◆ System Features	21
◆ XtremIO Management Server (XMS)	31
◆ System GUI	32
◆ Command Line Interface	32
◆ RESTful API	32
◆ Ports and Protocols	33

System Overview

The XtremIO Storage Array is an all-flash system, based on a scale-out architecture. The system uses building blocks, called X-Bricks, which can be clustered together, as shown in [Figure 2](#).

The system operation is controlled via a stand-alone dedicated Linux-based server, called the XtremIO Management Server (XMS). Each XtremIO cluster requires its own XMS host, which can be either a physical or a virtual server. The array continues operating if it is disconnected from the XMS, but cannot be configured or monitored.

XtremIO's array architecture is specifically designed to deliver the full performance potential of flash, while linearly scaling all resources such as CPU, RAM, SSDs, and host ports in a balanced manner. This allows the array to achieve any desired performance level, while maintaining consistency of performance that is critical to predictable application behavior.

The XtremIO Storage Array provides a very high level of performance that is consistent over time, system conditions and access patterns. It is designed for high granularity true random I/O.

The cluster's performance level is not affected by its capacity utilization level, number of Volumes, or aging effects. Moreover, performance is not based on a "shared cache" architecture and therefore it is not affected by the dataset size or data access pattern.

Due to its content-aware storage architecture, XtremIO provides:

- ◆ Even distribution of data blocks, inherently leading to maximum performance and minimal flash wear
- ◆ Even distribution of metadata
- ◆ No data or metadata hotspots
- ◆ Easy setup and no tuning
- ◆ Advanced storage functionality, including Inline Data Deduplication and Compression, thin provisioning, advanced data protection (XDP), Snapshots, and more

X-Brick

[Figure 1](#) shows an X-Brick.

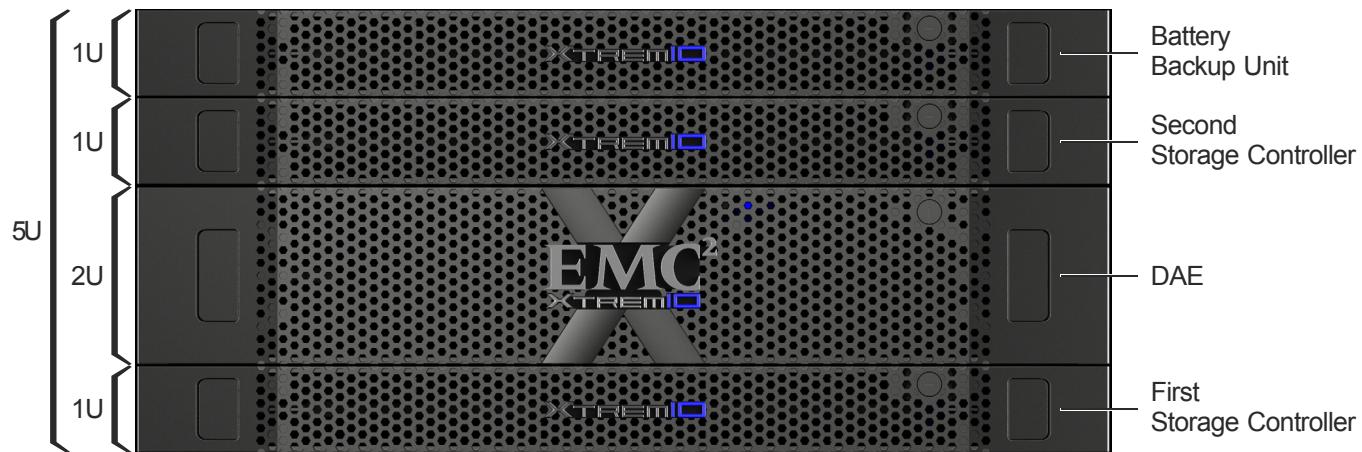


Figure 1 X-Brick

An X-Brick is the basic building block of an XtremIO array.

Each X-Brick is comprised of:

- ◆ One 2U Disk Array Enclosure (DAE), containing:
 - 25 eMLC SSDs (standard X-Brick) or 13-25 eMLC SSDs (5TB Starter Kit)
 - Two redundant power supply units (PSUs)
 - Two redundant SAS interconnect modules
- ◆ One Battery Backup Unit
- ◆ Two 1U Storage Controllers (redundant storage processors)

Each Storage Controller includes:

- Two redundant power supply units (PSUs)
- Two 8Gb/s Fibre Channel (FC) ports
- Two 10GbE iSCSI (SFP+) ports
- Two 40Gb/s InfiniBand ports
- One 1Gb/s management/IPMI port

Note: For details on X-Brick racking and cabinet requirements, refer to *EMC XtremIO Storage Array Site Preparation Guide*.

Note: For details on required rack spaces for all cluster configurations refer to *EMC XtremIO System Specification*
[\(http://www.emc.com/collateral/software/specification-sheet/h12451-XtremIO-ss.pdf\).](http://www.emc.com/collateral/software/specification-sheet/h12451-XtremIO-ss.pdf)

Scale-Out Architecture

An XtremIO Storage Array can include a single X-Brick or a cluster of multiple X-Bricks, as shown in [Figure 2](#) and [Table 1](#).

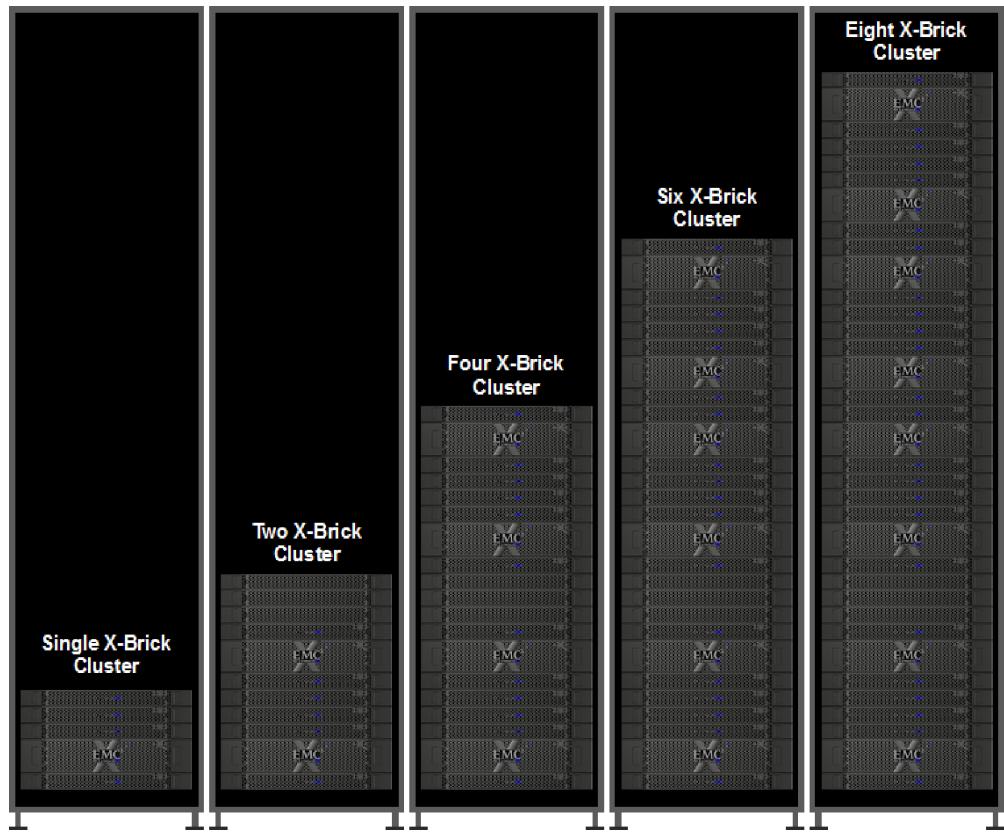


Figure 2 Cluster Configurations for Single, Two, Four, Six and Eight X-Brick clusters

Note: A 5TB Starter Kit is physically similar to a single X-Brick cluster, except for the number of SSDs in the DAE (13 SSDs in a 5TB Starter Kit instead of 25 SSDs in a standard single X-Brick).

With clusters of two or more X-Bricks, XtremIO array uses a redundant 40Gb/s QDR InfiniBand network for back-end connectivity between the Storage Controllers, ensuring a highly available, ultra-low latency network. The InfiniBand network is a fully managed component of the XtremIO array, and administrators of XtremIO arrays do not need to have specialized skills in InfiniBand technology.

A single X-Brick cluster consists of:

- ◆ One X-Brick
- ◆ One additional Battery Backup Unit

A cluster of multiple X-Bricks consists of:

- ◆ Two, four, six or eight X-Bricks
- ◆ Two InfiniBand Switches

Table 1 Cluster Configurations as Single and Multiple X-Brick clusters

	Single X-Brick cluster	Two X-Brick cluster	Four X-Brick cluster	Six X-Brick cluster	Eight X-Brick cluster
No. of X-Bricks	1	2	4	6	8
No. of InfiniBand Switches	0	2	2	2	2
No. of Additional Battery Backup Units	1	0	0	0	0

5TB Starter Kit

XtremIO's 5TB Starter Kit is identical to a standard X-Brick cluster, with the exception that it is equipped with only 13 SSDs instead of 25. The 5TB Starter Kit may be expanded to a regular X-Brick, using a Starter X-Brick (5TB) Expansion Kit which includes additional 12 SSD units.

System Features

Scalable Performance

XtremIO is designed so as to scale out in order to meet future performance and capacity needs, not only for new applications, but also for those already deployed. XtremIO's architecture allows performance and capacity to be increased by adding building blocks (X-Bricks), while maintaining a single point of management and balance of resources across the cluster.

Scale out is an intrinsic part of the XtremIO's architecture and can be performed without a forklift upgrade of the existing hardware or any need for prolonged data transfers.

When additional performance or capacity is required, the XtremIO Storage Array can be scaled-out by adding additional X-Bricks. Multiple X-Bricks are joined together over a redundant, high-availability, ultra-low latency InfiniBand network.

When the cluster expands, resources remain balanced, and data in the array is distributed across all X-Bricks to maintain consistent performance and equivalent flash wear levels.

Storage capacity and performance scale linearly, such that two X-Bricks supply twice the IOPS, four X-Bricks supply four times the IOPS, six X-Bricks supply six times the IOPS and eight X-Bricks supply eight times the IOPS of the single X-Brick configuration. However, the latency remains consistently low (less than 1ms) as the cluster scales out, as shown in [Figure 3](#).

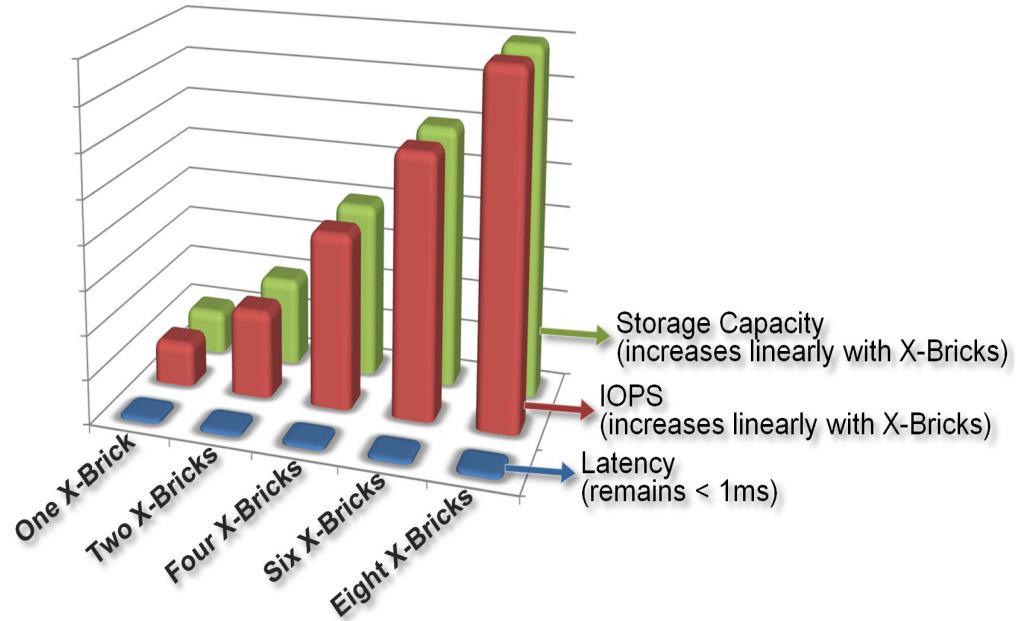


Figure 3 Linear Performance Scalability with Consistent Low Latency

Even Data Distribution

To external applications, XtremIO appears and behaves like a standard block storage array. However, due to its unique architecture, it takes a fundamentally different approach to internal data organization. Instead of using logical addresses, XtremIO uses the block content to decide where to place data blocks.

XtremIO uses data blocks internally. In a write operation, any data chunks that are larger than the native block size are broken down into standard blocks when they first enter the array. The system calculates a unique fingerprint for each of the incoming data blocks, using a special mathematical algorithm.

This unique fingerprint is used for two primary purposes:

- ◆ To determine where the data block is placed within the array
- ◆ Inline Data Reduction

Because of the way the fingerprinting algorithm works, the ID numbers appear completely random and are evenly distributed over the possible range of fingerprint values. This results in an even distribution of data blocks across the entire cluster and all SSDs within the array. In other words, with XtremIO it is neither necessary to check the space utilization levels on different SSDs, nor to actively manage equal data writes to every SSD. XtremIO inherently provides even distribution of data by placing the blocks based on their unique IDs.

Inline Data Reduction

XtremIO's unique Inline Data Reduction is achieved by utilizing the following techniques:

- ◆ Inline Data Deduplication
- ◆ Inline Data Compression

Inline Data Deduplication

Inline data deduplication is the removal of redundancies from data before it is written to the flash media.

XtremIO automatically and globally deduplicates data as it enters the system. Deduplication is performed in real-time and not as a post-processing operation. With XtremIO, there are no resource-consuming background processes and no additional reads/writes (which are associated with post-processing). Therefore, it does not negatively affect performance of the storage array, does not waste the available resources that are allocated for the host I/O, and does not consume flash wear cycles.

With XtremIO, data blocks are stored according to their content, and not according to their user level address within the Volumes. This ensures perfect load balancing across all devices in the system in terms of capacity and performance. Each time a data block is modified, it can be placed on any set of SSDs in the system, or not written at all if the block's content is already known to the system.

The system inherently spreads the data across the array, using all SSDs evenly and providing perfect wear leveling. Even if the same logical block address (LBA) is repeatedly written by a host computer, each write is directed to a different location within the XtremIO array. If the host writes the same data over and over again, it will be deduplicated, resulting in no additional writes to the flash.

XtremIO uses a content-aware, globally deduplicated cache for highly efficient data deduplication. The system's unique content-aware storage architecture enables achieving a substantially larger cache size with a small DRAM allocation. Therefore, XtremIO is the ideal solution for difficult data access patterns, such as the "boot storms" that are common in virtual desktop (VDI) environments.

The system also uses the content fingerprints, not only for Inline Data Deduplication, but also for uniform distribution of data blocks across the array. This provides inherent load balancing for performance and enhances flash wear level efficiency, since the data never needs to be rewritten or rebalanced.

Performing this process inline, and globally across the array, translates into fewer writes to the SSDs. This increases SSD endurance and eliminates performance degradation that is associated with post-processing deduplication.

XtremIO's Inline Data Deduplication and its intelligent data storage process ensure:

- ◆ Balanced usage of the system resources, maximizing the system performance
- ◆ Minimum amount of flash operations, maximizing the flash longevity
- ◆ Equal data distribution, resulting in evenly balanced flash wear across the system
- ◆ No system level garbage collection (as opposed to post-processing data reduction)
- ◆ Smart usage of SSD capacity, minimizing storage costs

Inline Data Compression

Inline Data Compression is the compression of the already deduplicated data **before** it is written to the flash media.

XtremIO automatically compresses data after all duplications have been removed. This ensures that the compression is performed only for unique data blocks. Data compression is performed in real-time and not as a post-processing operation.

The nature of the data set determines the overall compressibility rate. The compressed data block is then stored on the array.

Compression reduces the total amount of physical data that needs to be written on the SSD. This reduction minimizes the Write Amplification (WA) of the SSDs, thereby improving the endurance of the flash array.

XtremIO's Inline Data Compression provides the following benefits:

- ◆ Data compression is always inline and is never performed as a post-processing activity. Therefore, the data is always written only once.
- ◆ Compression is supported for a diverse variety of data sets (e.g. database data, VDI, VSI environments, etc.).
- ◆ Data compression complements data deduplication in many cases. For example, in a VDI environment deduplication dramatically reduces the required capacity for cloned desktops. Consequently, compression reduces the specific user data. As a result, an increased number of VDI desktops can be managed by a single X-Brick.
- ◆ Compression saves storage capacity by storing data blocks in the most efficient manner.
- ◆ When combined with XtremIO's powerful Snapshot capabilities, XtremIO can easily support petabytes of functional application data.

Total Data Reduction

XtremIO's data deduplication and data compression complement each other. Data deduplication reduces physical data, by eliminating redundant data blocks. Data compression further reduces the data footprint, by eliminating data redundancy within the binary level of each data block.

High Availability

Preventing data loss and maintaining service in case of multiple failures is one of the core features in the architecture of XtremIO's All Flash Storage Array.

From the hardware perspective, no component is a single point of failure. Each Storage Controller, DAE and InfiniBand Switch in the cluster is equipped with dual power supplies. The cluster also has dual Battery Backup Units and dual network and data ports (in each of the Storage Controllers). Two InfiniBand Switches are cross connected and create a dual data fabric. Both the power input and the different data paths are constantly monitored, and any failure triggers a recovery attempt or failover.

The software architecture is built in a similar way. Every piece of information that is not committed to the SSD is kept in multiple locations, called Journals. Each software module has its own Journal, which is not kept on the same Storage Controller, and can be used to restore data in case of unexpected failure. Journals are regarded as highly important and always kept on Storage Controllers with battery backed up power supplies. In case of a problem with the Battery Backup Unit, the Journal fails over to another Storage Controller, which is protected by another Battery Backup Unit. In case of global power failure, the Battery Backup Units ensure that all Journals are written to vault drives in the Storage Controllers and the cluster is turned off.

In addition, due to its scale-out design and the XDP data protection algorithm, each X-Brick is preconfigured as a single redundancy group. This eliminates the need to select, configure and tune redundancy groups.

XtremIO's Active-Active architecture is designed to ensure maximum performance and consistent latency. The cluster includes a self-healing mechanism that attempts to recover from any failure and resume full functionality. An attempt to restart a failed component is performed once before a failover action. Storage Controller failover is carried out as the last resort. Based on the nature of the failure, the cluster attempts to failover the relevant software component, while maintaining the operation of other components, thus minimizing the performance impact. The whole Storage Controller fails over only if recovery attempts are not successful or if the cluster must act in the best interest of protecting against data loss.

When a component that was temporarily unavailable recovers, a fallback is initiated. This process is carried out at the software component or Storage Controller level. An anti-bounce mechanism prevents the cluster from failing back to an unstable component or to a component that is under maintenance.

Non-Disruptive Upgrade

During Non-Disruptive Upgrades (NDU) of the XtremIO Operating System, the cluster performs the upgrade procedure on a live cluster, updates all Storage Controllers in the cluster, and restarts the cluster service. The NDU process takes less than 30 seconds. Since the underlying Linux Kernel is active throughout the upgrade process, the hosts do not detect any path disconnection during the application restart period.

In the rare case of a Linux kernel or firmware upgrade, it is possible to upgrade the XtremIO All Flash Array without any service interruption and without any risk of data loss. The NDU procedure is launched from the XtremIO Management Server and is able to upgrade the XtremIO software and the underlying operating system and firmware.

During Linux/firmware NDU, the cluster automatically fails over a component and upgrades its software. After completing the upgrade and verifying the component's health, the cluster fails back to it and the process repeats itself on other components. During the upgrade process the cluster is fully accessible, no data is lost, and the performance impact is kept to minimum.

Thin Provisioning

XtremIO storage is natively thin provisioned, using a small internal block size. This provides fine-grained resolution for the thin provisioned space.

All Volumes in the cluster are thin provisioned, meaning that the cluster consumes capacity only when it is actually needed. XtremIO determines where to place the unique data blocks physically inside the cluster after it calculates their fingerprint IDs. Therefore, it never pre-allocates or thick-provisions storage space before writing.

As a result of XtremIO's content-aware architecture, blocks can be stored at any location in the cluster (and only metadata is used to refer to their locations) and the data is written only when unique blocks are received.

Therefore, unlike thin provisioning with many disk-oriented architectures, with XtremIO there is no space creeping and no garbage collection. Furthermore, the issue of Volume fragmentation over time is not applicable to XtremIO (as the blocks are scattered all over the random-access array) and no defragmentation utilities are needed.

XtremIO's inherent thin provisioning also enables consistent performance and data management across the entire life cycle of the Volumes, regardless of the cluster capacity utilization or the write patterns to the cluster.

XtremIO Data Protection (XDP)

The XtremIO storage system provides "self-healing" double-parity data protection with a very high efficiency.

The system requires very little capacity overhead for data protection and metadata space. It does not require dedicated spare drives for rebuilds. Instead, it leverages the "hot space" concept, where any free space available in the array can be utilized for failed drive reconstructions. The system always reserves sufficient distributed capacity for performing a single rebuild.

In a rare case of double SSD failure, even with a full capacity of data, the array uses the free space to rebuild the data of one of the drives. It rebuilds the second drive once one of the failed drives is replaced. If there is enough free space to rebuild the data of both drives, it is performed simultaneously.

XtremIO maintains its performance, even at high capacity utilization, with minimal capacity overhead. The system does not require mirroring schemes (and their associated 100% capacity overhead).

XtremIO requires far less reserved capacity for data protection, metadata storage, Snapshots, spare drives and performance, leaving much more space for user data. This lowers the cost per usable GB.

The XtremIO storage system provides:

- ◆ N+2 data protection
- ◆ Incredibly low data protection capacity overhead of 8%
- ◆ Performance superior to any RAID algorithm (RAID 1, the RAID algorithm that is most efficient for writes, requires over 60% more writes than XtremIO Data Protection.)
- ◆ Flash endurance superior to any RAID algorithm, due to smaller amount of writes and even distribution of data
- ◆ Automatic rebuild in case of drive failure and faster rebuild times than traditional RAID algorithms
- ◆ Superior robustness with adaptive algorithms that fully protect incoming data, even when failed drives exist in the system
- ◆ Administrative ease through fail-in-place support

Snapshots

Snapshots are instantaneous copy images of Volume data with the state of the data captured exactly as it appeared at the specific point in time that the Snapshot was created, enabling users to save the Volume data state and then access the specific Volume data whenever needed, including after the source Volume has changed.

Creating Snapshots, which can be done at any time, does not affect system performance, and a Snapshot can be taken either directly from a source Volume or from other Snapshots within a source Volume's group (Volume Snapshot Group). XtremIO Snapshots are inherently writeable, but can be created as read-only to maintain immutability.

The original copy of the data remains available without interruption, while the Snapshot can be used to perform other functions on the data. Changes made to the Snapshot's source do not change or impact on the Snapshot data.

XtremIO's Snapshot technology is implemented by leveraging the content-aware capabilities of the system (Inline Data Reduction), optimized for SSD media, with a unique metadata tree structure that directs I/O to the right time stamp of the data. This allows efficient snapshotting that can sustain high performance, while maximizing the media endurance, both in terms of the ability to create multiple Snapshots and the amount of I/O that a Snapshot can support.

When creating a Snapshot, the system generates a pointer to the ancestor metadata (of the actual data in the system). Therefore, creating a Snapshot is a very quick operation that does not have any impact on the system and does not consume any capacity. Snapshot capacity consumption occurs only if a change requires writing a new unique block.

XtremIO Snapshots are space-efficient both in terms of additional metadata consumed and physical capacity. Snapshots are implemented, using redirect-on-write methodology, where new writes to the source Volume (or Snapshot) are redirected to new locations, and only metadata is updated to point to the new data location. This method guarantees no performance degradation while Snapshots are created.

Snapshots can be accessed like any other Volume in the cluster in read write access mode, and enable a wide range of uses, including:

- ◆ Logical corruption protection — Creating frequent Snapshots that are based on a defined recovery point objective (RPO) interval enables you to utilize Snapshots for recovery of logical data corruption. The Snapshots are saved in the system for as long as deemed necessary, and remain available for recovery use, should logical data corruption occur, thus enabling recovery of an earlier application state (prior to logical data corruption occurrence) to a known point in time prior to the corruption of the data.
- ◆ Backups — Presenting Snapshots to a backup server (or agent) enables offloading the backup process from the production server.
- ◆ Development and testing — Taking Snapshots of the production data enables the user to create multiple (space-efficient and high-performance) copies of the production system for the development and testing purposes.
- ◆ Clones — Using persistent writable Snapshots enables achieving clone-like capabilities. The Snapshots can act as clones of the production Volume to multiple servers. Clone performance is identical to that of the production Volume.

- ◆ Offline processing — Snapshots can be used as a means to offload data processing from the production server. For example, if you need to run a heavy process on data (which may be detrimental to the production server's performance), you can use Snapshots to create a recent copy of the production data and then mount it on a different server. The process can then be run (on the other server), without consuming the production server's resources.

XtremIO offers the following efficient tools for managing Snapshots and optimizing their usability:

- ◆ Consistency Groups — Consistency Groups (CG) are used to create a consistent image of a set of Volumes, usually used by a single application, such as database. With XtremIO CGs, you can create a Snapshot of all Volumes in a group, using a single command. This ensures that all Volumes are created at the same time. Many operations that are applied on a single Volume can also be applied on a CG.
- ◆ Snapshot Set — A Snapshot Set is a group of Snapshots that were taken, using a single command and represents a point in time of a group. A Snapshot Set can be the result of a Snapshot taken on a CG, on another Snapshot Set or on a set of Volumes that were selected manually. A Snapshot Set maintains a relationship with the ancestor from which it was created.
- ◆ Read-Only Snapshots — By design, XtremIO Snapshots are regular Volumes and are created as writable Snapshots. In order to satisfy the need for local backup and immutable copies, there is an option to create a read-only Snapshot. A read-only Snapshot can be mapped to an external host such as a backup application, but it is not possible to write to it.
- ◆ Scheduler — The Scheduler can be used for local protection use cases. It can be applied to a Volume, a CG or a Snapshot Set. Each Scheduler can be defined to run at an interval of seconds, minutes or hours. Alternatively, it can be set to run at a specific time of a day or a week. Each Scheduler has a retention policy, based on the number of copies the customer would like to hold or based on the age of the oldest Snapshot.
- ◆ Restore — Using a single command, it is possible to restore a production Volume or a CG from one of its descendant Snapshot Sets. The SCSI face of the production Volume will be moved to a Snapshot of the required Snapshot Set without the need for the host application to rescan and rediscover a new Volume.
- ◆ Refresh — The refresh command is a powerful tool for test and development environments and for the offline processing use case. With a single command, a Snapshot of the production Volume or CG is taken and the SCSI face of the Volume, which was mapped to the test and development application, is moved to it. This allows the test and development application to work on current data without the need to copy data or to rescan.

VMware VAAI Integration

XtremIO is fully VAAI compliant, allowing vSphere server to offload I/O intensive work to the XtremIO array and provide accelerated storage vMotion, VM provisioning, and thin provisioning functionality.

In addition, XtremIO's VAAI integration improves the X-copy efficiency even further, by making the whole operation metadata driven. With XtremIO, due to Inline Data Reduction and in-memory metadata, no actual data blocks are copied during the X-copy command. The cluster only creates new pointers to the existing data, and the entire process is carried out in the Storage Controllers' memory. Therefore, it does not consume the resources of the storage array and has no impact on the cluster performance.

For example, a VM image can be cloned extremely fast (even multiple times) with XtremIO.

The XtremIO features for VAAI support include:

- ◆ Zero Blocks/Write Same

Used for zeroing-out disk regions (VMware term: HardwareAcceleratedInit).

This feature provides accelerated Volume formatting.

- ◆ Clone Blocks/Full Copy/XCOPY

Used for copying or migrating data within the same physical array (VMware term: HardwareAcceleratedMove).

On XtremIO, this allows VM cloning to take place almost instantaneously, without affecting user I/O on active VMs.

- ◆ Record based locking/Atomic Test & Set (ATS)

Used during creation and locking of files on a VMFS Volume, for example, during powering-down/powering-up of VMs (VMware term: HardwareAcceleratedLocking).

This feature is designed to address access contention on ESX Volumes shared by multiple VMs.

- ◆ Block Delete/UNMAP/TRIM

Allows for unused space to be reclaimed, using the SCSI UNMAP feature (VMware term: BlockDelete; vSphere 5.x only). This can also be performed manually, in VMware version 5.1, using the vmkfstool command (for details, refer to VMware documentation).

Data at Rest Encryption

Data at Rest Encryption is designed to protect customer's data that is stored on non-volatile media, such as SSD, in case it is removed from the XtremIO cluster or from the customer premises.

The encryption is based on Self Encrypting Drives (SED). These drives have a special designed hardware component that performs the encryption without causing any performance degradation. The encryption key – Media Encryption Key (MEK) – is generated on board the drive and never leaves the drive. When encryption is enabled, the cluster generates an Authentication Key (AK) PIN that is used to lock and unlock the SSD encryption. The Authentication Key is kept securely in the cluster and is used to unlock the SSD during the system start. Removing an SSD from the cluster locks the SSD and renders the media on it unreadable.

If there is a suspicion that the PIN was compromised or when a periodical key rollover is required by regulations, a cluster re-encryption is performed to change the SSD authentication PIN.

XtremIO supports these encryption capabilities on supported hardware after software upgrade, even when the cluster is populated with data, without causing any data loss. The Authentication Key can also be changed instantly without losing data.

The XtremIO cluster encrypts the data that is stored on the DAE's SSD and on the internal Storage Controllers' SSD.

XtremIO Management Server (XMS)

The XMS enables you to control and manage the XtremIO cluster, including:

- ◆ Creating, formatting, and initializing new clusters
- ◆ Monitoring cluster health and events
- ◆ Monitoring cluster performance
- ◆ Collecting cluster performance statistics
- ◆ Providing GUI, CLI and RESTful API services to clients
- ◆ Implementing Volume management and Data Protection Groups operation logic
- ◆ Providing operational support functions such as stopping and starting the cluster or any of the Storage Controllers
- ◆ Collecting supporting materials (log bundle) on the cluster for support and offline troubleshooting purposes

The XMS is preinstalled with the CLI and GUI. It can be installed on a dedicated physical server, or as a VMware virtual host.

The XMS must have network access to management/IPMI addresses on all Storage Controllers in the XtremIO cluster, and must be accessible by any GUI/CLI client host machine. To ensure adequate communication between the XMS and the cluster, the XMS should be located in the same Local Area Network (LAN) as the cluster. This is especially true for a virtual XMS connected to the cluster.

Since the XMS is not in the data path, it can be disconnected from the XtremIO cluster without affecting the I/O. An XMS failure only affects monitoring and configuration activities, such as creating and deleting Volumes. However, when using a virtual XMS, it is possible to take advantage of VMware vSphere HA features to easily overcome such failures.

Even if the entire XMS server is lost or destroyed, a new XMS can still be recovered and rebuilt from the cluster. For more information, contact EMC Global Tech Support.

System GUI

The system GUI is implemented, using a Java client. The GUI client software communicates with the XMS, using standard TCP/IP protocols, and can be used in any location that allows the client to access the XMS.

The GUI provides easy-to-use tools for performing most of the cluster operations (certain management operations must be performed, using the CLI). Additionally, operations on multiple components, such as creating multiple Volumes, can only be performed using the GUI.

Command Line Interface

The system's Command Line Interface (CLI) allows administrators and other XtremIO cluster users to perform supported management operations. It is preinstalled on the XMS and can be accessed, using the standard SSH protocol or via CLI window in the GUI.

A CLI client package, which communicates with the XMS server via standard TCP/IP connections and can be installed on a Linux CentOS host with access to the XMS, is also available.

RESTful API

The XtremIO's RESTful API allows HTTP-based interface for automation, orchestration, query and provisioning of the system. With the RESTful API, third party applications can be used to control and fully administer the array. Therefore, it allows flexible management solutions to be developed for the XtremIO array.

For more information, refer to *XtremIO Storage Array RESTful API Guide*.

Ports and Protocols

Figure 4 describes the ports and protocols used by the XtremIO cluster.

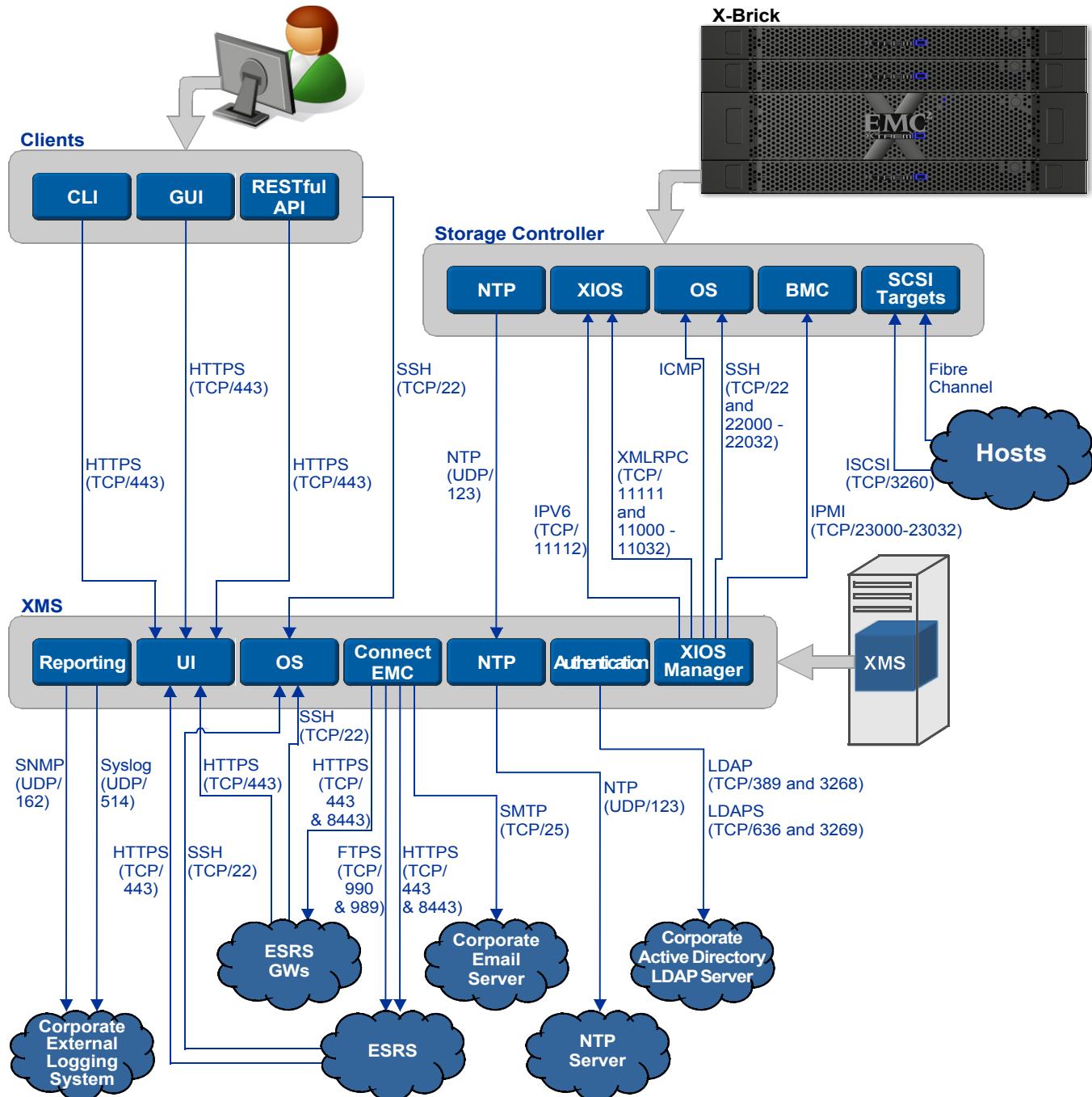


Figure 4 Ports and Protocols¹

1. ICMP between the XMS and the Storage Controller is used for diagnostic purposes only.

CHAPTER 2

Using the Graphical User Interface (GUI)

This chapter includes the following topics:

◆ GUI Window	36
◆ Menu Bar Icons	37
◆ Accessing the GUI	38
◆ Dashboard Workspace	45
◆ Multiple Cluster Configuration	51
◆ Configuration Workspace	53
◆ Inventory Workspace	67
◆ Alerts & Events Workspace	94
◆ Reports Workspace	99
◆ Administration Workspace	101
◆ Support Window	111

GUI Window

The XtremIO Storage Array provides a user-friendly GUI for managing and monitoring the cluster, without the need to be familiar with the CLI. In addition, the GUI presents a graphical representation of the cluster's state.

The interface is divided into the following sections, as shown in [Figure 5](#):

- ◆ Menu bar - contains icons for selecting the workspace you want to work in.
- ◆ Cluster information bar - shows the existing clusters in the system, the currently visible cluster and a cluster locator (in case of a multiple cluster configuration).
- ◆ Workspace - contains the window panes through which you can monitor and manage the cluster.
- ◆ Status bar - shows the clusters connection status, clusters and XMS date and time zone, current user name and logout button.

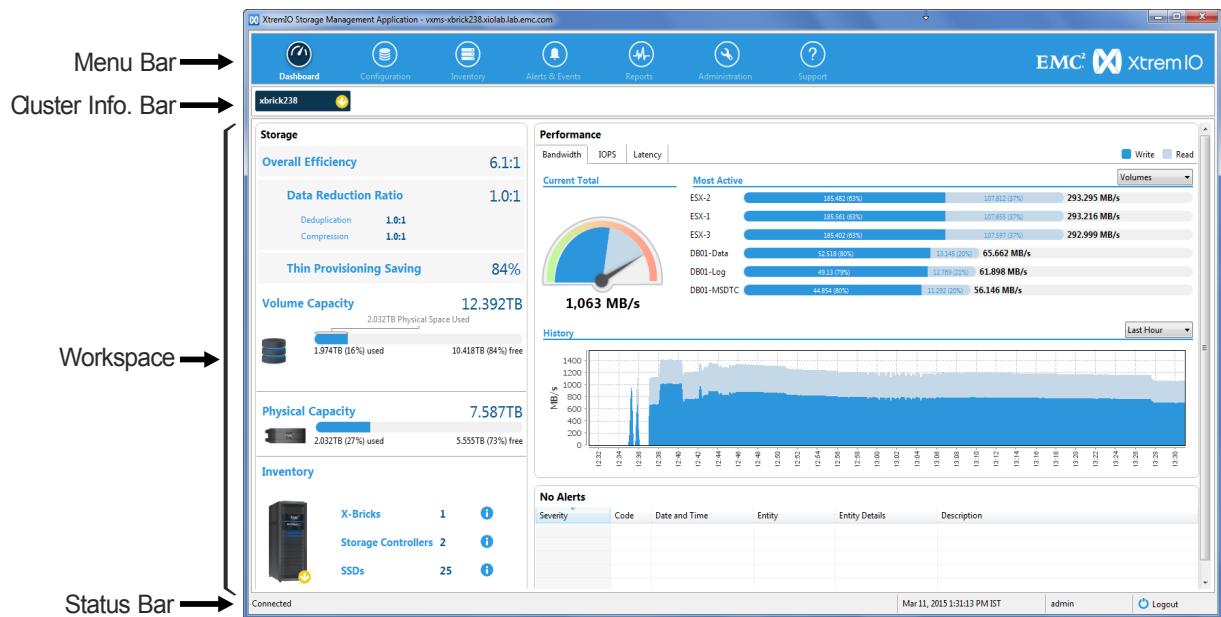


Figure 5 GUI Window Sections

Menu Bar Icons

[Table 2](#) explains the menu bar icons.

Table 2 Menu Bar Icons

Icon	Description
	Dashboard Displays the “ Dashboard Workspace ” (see page 45).
	Configuration Displays the “ Configuration Workspace ” (see page 53).
	Inventory Displays the “ Inventory Workspace ” (see page 67).
	Alerts & Events Displays the “ Alerts & Events Workspace ” (see page 94).
	Report Displays the “ Reports Workspace ” (see page 99).
	Administration Displays the “ Administration Workspace ” (see page 101).
	Support Displays the “ Support Window ” (see page 111).

Accessing the GUI

Note: For information on supported Java versions, refer to *XtremIO Storage Array Release Notes*.

To access the GUI:

1. In your browser, enter the IP address of the XMS, received from your system administrator to display the XtremIO Splash screen, as shown in [Figure 6](#).



Figure 6 XtremIO Splash Screen

2. If there are any Java interoperability issues, download the Java bundle (see “[Installing a Local Java Bundle](#)” on page 43).
3. Click the **root certificate** hyperlink to download the certificate.

4. When prompted, select **open** to open the certificate file.

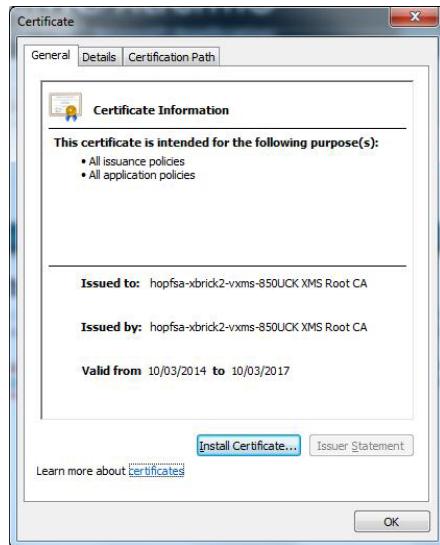


Figure 7 Certificate Dialog Box

5. In the Certificate dialog box, click **Install Certificate**.



Figure 8 Certificate Import Wizard - Welcome Screen

6. In the Certificate Import Wizard welcome screen, click **Next**.



Figure 9 Certificate Import Wizard - Certificate Store

7. In the Certificate Store screen, select the **Place all certificates in the following store** option, and click **Browse**.



Figure 10 Select Certificate Store - Trusted Root Certification Authorities

8. In the Select Certificate Store dialog box, select the **Trusted Root Certification Authorities** folder and click **OK**.

9. In the Certificate Import Wizard, click **Next**.

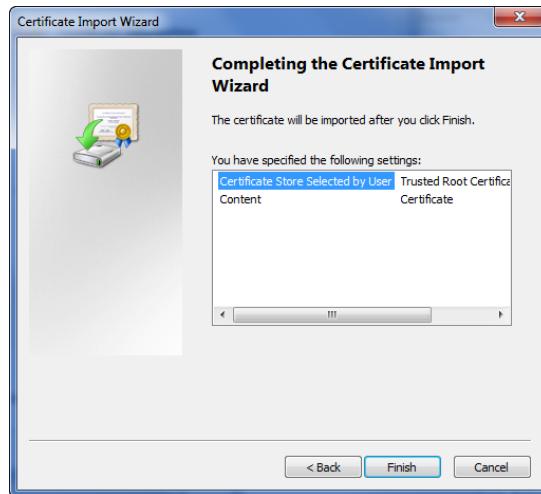


Figure 11 Certificate Import Wizard - Finish Screen

10. Click **Finish**.
11. Repeat steps 2-9 and select **Third-Party Root Certification Authorities** as the Certificate Store.

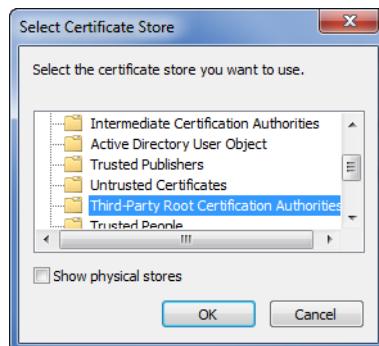


Figure 12 Select Certificate Store - Third-Party Root Certification Authorities

12. From the XtremIO splash screen, click **Launch**.
13. If you are asked to save the file webstart.jnlp, click **Save** and double-click the file to run it.

14. Wait for the application to load; the Login screen appears, as shown in [Figure 13](#).

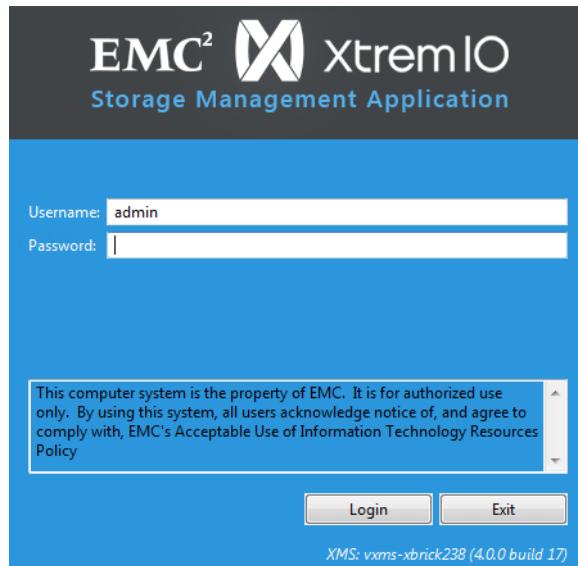


Figure 13 Login Screen

15. Enter your username and password as provided to you by your system/storage administrator.
16. Click **Login**; the system launches the XtremIO Storage Management Application and displays the Dashboard workspace, as shown in [Figure 17](#).

Note: For details on replacing the default SSL certificate for the XMS with a certificate issued by a trusted third party, refer to “Replacing the Default SSL Certificate” on [page 535](#).

Installing a Local Java Bundle

For any Java interoperability issues, XtremIO provides a pre-packaged GUI UI Java bundle to be downloaded, before logging in.

XtremIO offers Java bundles compatible with Windows and Macintosh Operating Systems. Upon launching the XtremIO GUI, the system detects the OS used by the clients and provides a link to a compatible Java bundle.

To install the local Java bundle:

1. In your browser, enter the IP address of the XMS, received from your system administrator to display the XtremIO Splash screen, as shown in [Figure 14](#).



Figure 14 XtremIO Splash Screen

2. Click the **Windows bundle** link at the bottom of the splash screen.

3. When prompted, select **open** to view the zip folder contents.

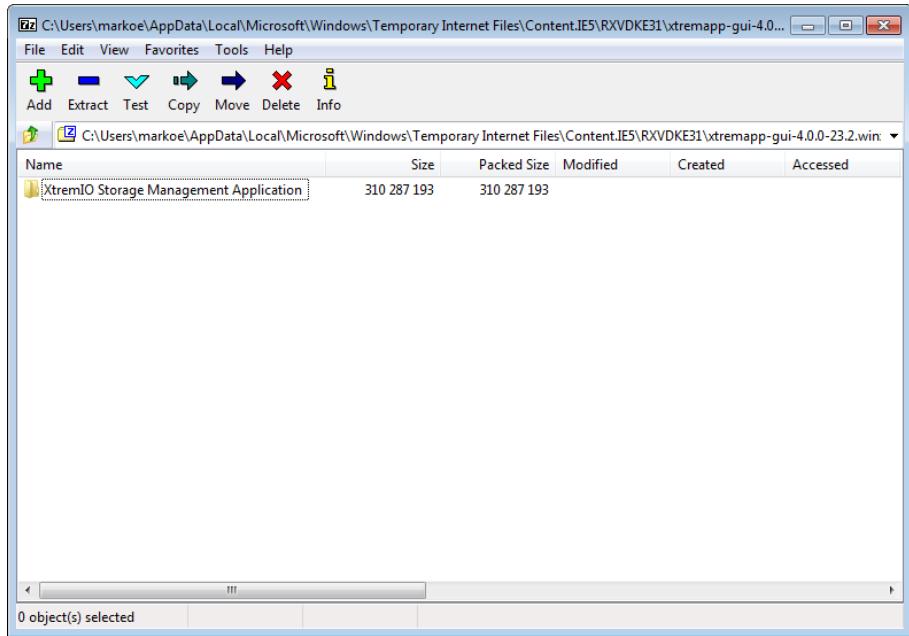


Figure 15 Zip Folder Contents

4. Extract the XtremIO Storage Management Application Folder by selecting the folder and clicking **Extract**. Use the browser to select a folder of your choice and click **OK**.
5. In your local folder, open the XtremIO Storage Management Application folder and double-click **XtremIO Launch.vbs**; the XtremIO Login Screen appears, as shown in Figure 16.

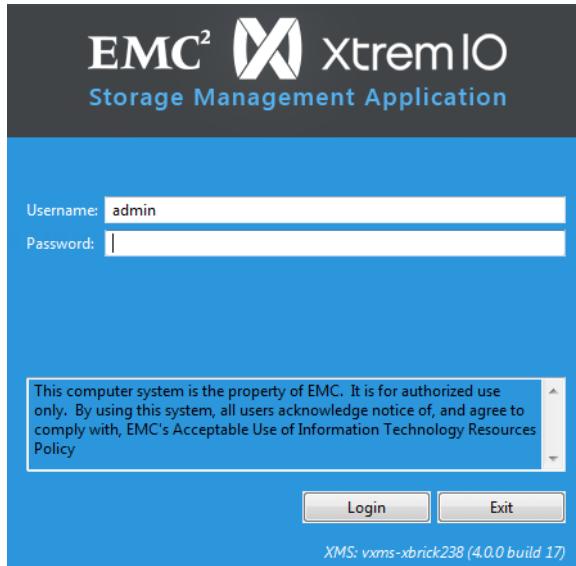


Figure 16 Login Screen

Note: It is recommended to create a shortcut to the **XtremIO Launch.vbs** file to make it accessible whenever a login is required.

Dashboard Workspace

The Dashboard workspace, as shown in [Figure 17](#), appears upon:

- ◆ Logging in to the XtremIO Storage Management Application
- ◆ Clicking the **Dashboard** icon from the Menu bar

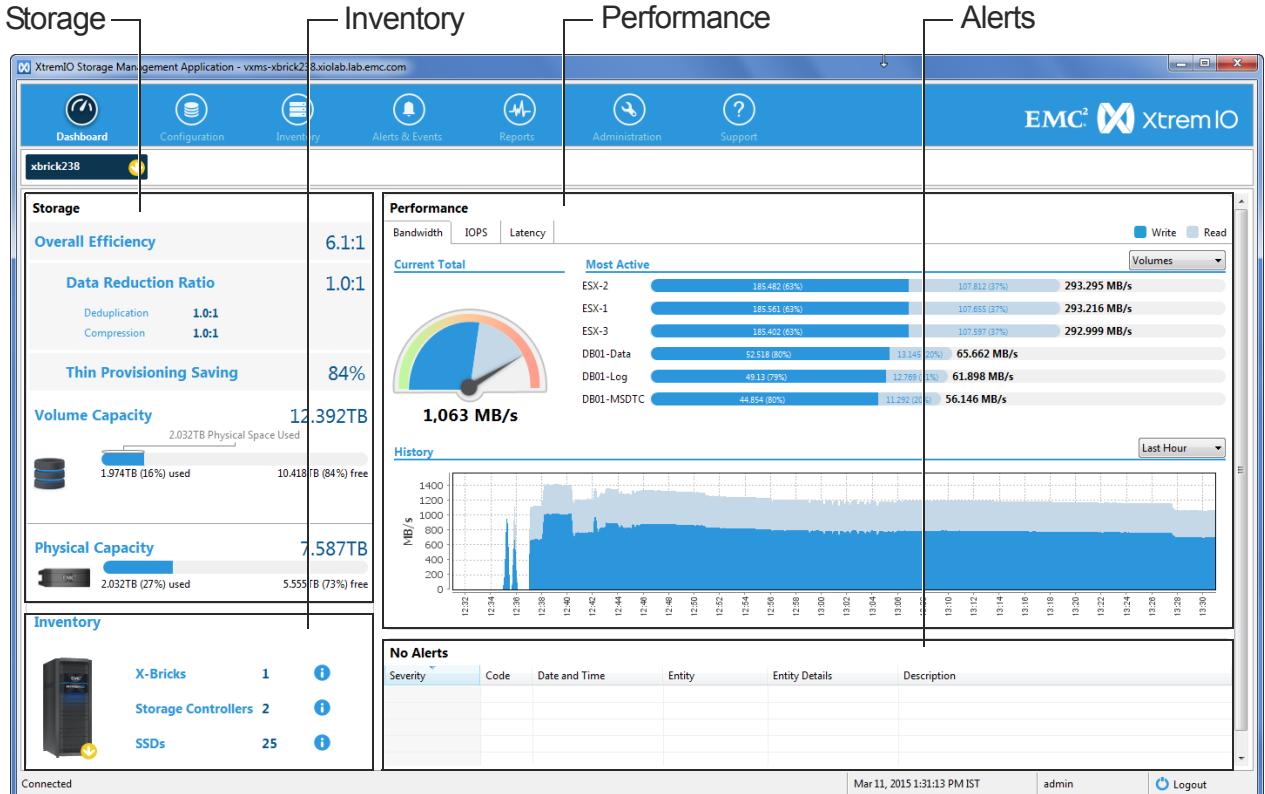


Figure 17 Dashboard Workspace

The Dashboard workspace is divided into the following panes:

- ◆ Storage (see [page 46](#))
- ◆ Inventory (see [page 48](#))
- ◆ Performance (see [page 47](#))
- ◆ Alerts (see [page 49](#))

Storage Pane

Figure 18 shows the Storage pane of the Dashboard workspace.

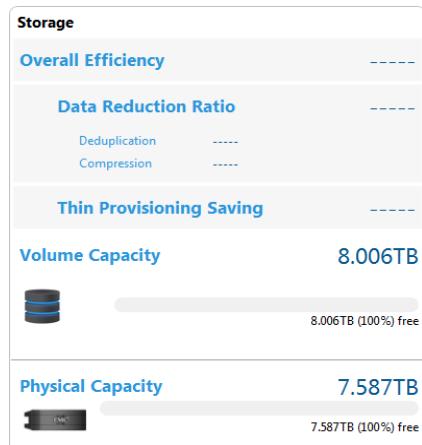


Figure 18 Storage Pane of the Dashboard Workspace

Via the Storage pane you can monitor the following parameters:

- ◆ Overall Efficiency
- ◆ Data Reduction Ratio
 - Data Deduplication
 - Data Compression
- ◆ Thin Provisioning Savings
- ◆ Volume Capacity (with a progress bar, showing used and free Volume capacity)
- ◆ Physical Capacity (with a progress bar, showing used and free physical capacity)

Performance Pane

Figure 19 shows the Performance pane of the Dashboard workspace and its main elements.

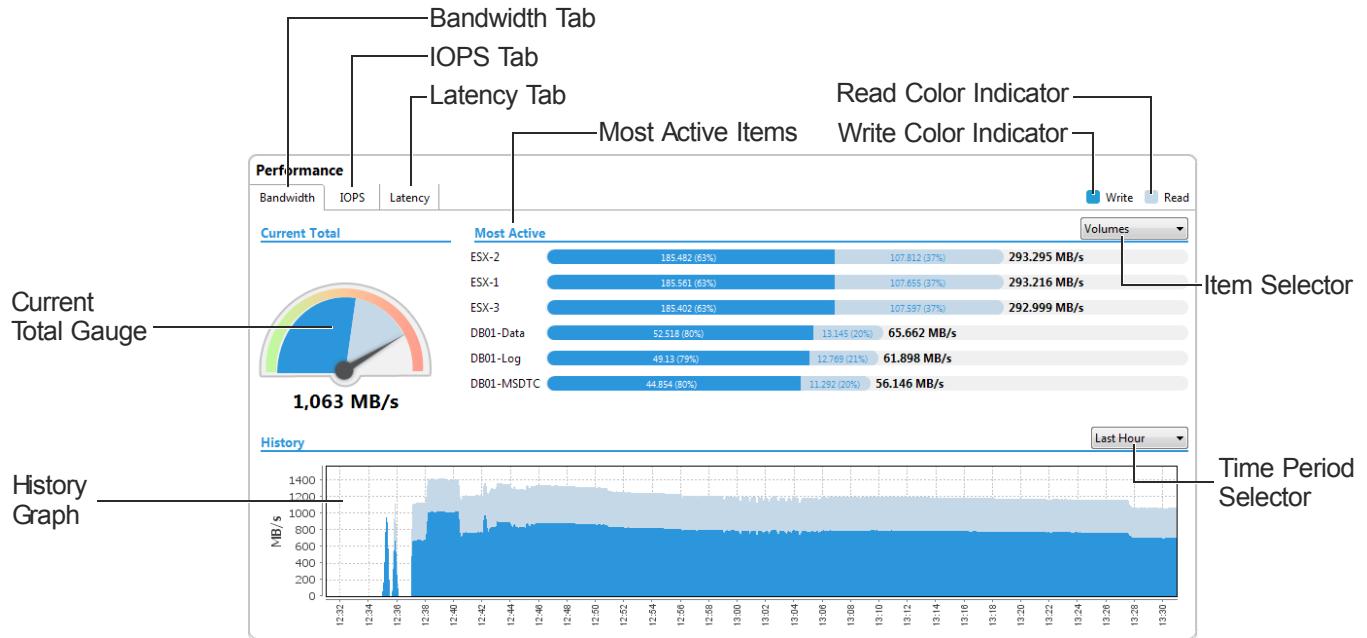


Figure 19 Performance Pane of the Dashboard Workspace

Table 3 describes the main elements of the Performance pane.

Table 3 Performance Pane Main Elements

Element	Description
Bandwidth Tab	Displays the cluster performance with Bandwidth as the unit of measure (MB/s).
IOPS Tab	Displays the cluster performance with IOPS as the unit of measure (IOPS rate).
Latency Tab	Displays the cluster performance with Latency as the unit of measure (μ s).
Most Active Items	Displays the 7 most active Block Sizes, Initiator Groups or Volumes (as selected in the Item Selector).
Read Color Indicator	Indicates the Read color (pale blue).
Write Color Indicator	Indicates the Write color (dark blue).
Current Total Gauge	Indicates the aggregated transfer rate for all Volumes by MB/s or IOPS.

Table 3 Performance Pane Main Elements

Element	Description
History Graph	Displays the performance history in terms of IOPS, Bandwidth or latency (according to the selected tab) over a selected period of time.
Item Selector	Enables you to select the desired item to monitor (Block Size, Initiator Group or Volume) from the drop-down list.
Time Period Selector	Enables you to select the desired time period from the drop-down list (Last Hour, Last 6 Hours, Last 24 Hours, Last 3 Days or Last Week) for the History Graph.

Inventory Pane

Figure 20 shows the Inventory pane of the Dashboard workspace, which displays a list of the cluster's hardware components and links to the components detailed data.



Figure 20 Inventory Pane of the Dashboard Workspace

- ◆ If a hardware component suffers from an alert, its color changes according to the alert's severity:
 - Yellow - minor alert
 - Orange - major alert
 - Red - critical alert
- ◆ Hovering the mouse pointer over the hardware component displays a tool-tip with information on the hardware status.
- ◆ Clicking a cluster component from the list opens the hardware workspace with the detailed data of the displayed component, as described in [page 67](#).

Alerts Pane

[Figure 21](#) shows the Alerts pane of the Dashboard workspace.

15 Alerts (11 major)					
Severity	Code	Date and Time	Entity	Entity Details	Description
Major	0400703	Feb 10, 2015 3:04:42 AM	Storage Controller	X1-SC1	The cluster has detected a potential risk for the journal health or persisten.
Major	0402503	Feb 10, 2015 3:04:41 AM	Storage Controller	X1-SC1	Storage Controller has stopped.
Major	0404702	Feb 10, 2015 3:04:41 AM	Storage Controller	X1-SC1	The cluster has detected a failure of the journal.
Minor	1600102	Feb 10, 2015 3:04:42 AM	DAE LCC	X1-DAE-LCC-A	DAE LCC SAS left port is down.
Minor	1600013	Feb 10, 2015 3:04:42 AM	DAE LCC	X1-DAE-LCC-B	DAE LCC health status is marginal.
Minor	1600013	Feb 10, 2015 3:04:42 AM	DAE LCC	X1-DAE-LCC-A	DAE LCC health status is marginal.

Figure 21 Alerts Pane of the Dashboard Workspace

The Alerts pane displays the current cluster alerts, which are color coded according to severity:

- ◆ Green - Cleared alert
- ◆ Blue - Information alert
- ◆ Yellow - Minor alert
- ◆ Orange - Major alert
- ◆ Red - Critical alert

For each alert the following details are listed:

- ◆ Severity
- ◆ Code
- ◆ Date and Time
- ◆ Entity
- ◆ Entity Details
- ◆ Description

You can sort the displayed alerts by each of these column headings.

To sort the alerts by a column heading, click the heading; The arrow, displayed above the selected heading indicates whether the sorting is in ascending or descending order.

Right-clicking the Alerts pane displays the Alerts drop-down menu, as shown in [Figure 22](#)

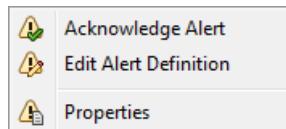


Figure 22 Alerts Pane Right-Click Drop-Down Menu

Table 4 describes the drop-down menu's active options.

Table 4 Alerts Pane Drop-Down Menu Options

Icon	Description
 Acknowledge Alert	Acknowledge Alert Acknowledges the selected alert and removes it from the Alerts list.
 Edit Alert Definition	Edit Alert Definition Enables you to change the selected alert's definition.
 Properties	Properties Displays the selected alert's properties.

Multiple Cluster Configuration

Multiple Cluster Configuration in GUI

When using a multiple cluster configuration, you can use the dashboard workspace to view each of the clusters data separately or a summary of all clusters.

Figure 23 displays the Dashboard workspace in a multiple cluster configuration.



Figure 23 Multiple Cluster View - Clusters Summary

Clicking **All Clusters** displays the aggregated data of all clusters managed by the XMS. The overall efficiency is displayed for all clusters and separately for each cluster.

When in an All Cluster view, the Configuration screen displays all of the clusters objects. However, to manipulate these objects (e.g. creating Volumes), you need to select a specific cluster.

The Inventory view displays a list of all clusters and their main properties.

Clicking a specific cluster displays the cluster data, as in a single cluster environment.

When working in a multiple cluster view, the following tabs display aggregated information for all clusters and each data item is associated to its cluster by the cluster name:

- ◆ Configuration
- ◆ Inventory
- ◆ Alerts and Events

The following tabs display the information in XMS level that is not associated with a specific cluster:

- ◆ Reports
- ◆ Administration

Multiple Cluster Configuration in CLI

When running cluster-related CLI commands in a multiple cluster configuration, it is required to specify the target cluster, using the `cluster-id` parameter.

If you wish to address a specific cluster during a CLI session, you can set the cluster context, using the `set-context` CLI command. After you set a context, it is not required to specify the cluster ID in cluster-related CLI commands. When the cluster context is set, you cannot manage other clusters via CLI, except for the specified cluster.

Note: When using the `cluster-id` parameter, it is recommended to specify the host name rather than the cluster ID, since the latter may change in case of cluster migration between XMSs (see below).

Note: Specifying the cluster ID in cluster-related commands is not required in single cluster configuration. However, it is recommended to specify the cluster ID to support a future change to a multiple cluster configuration.

Cluster migration from one XMS to another is performed, using the `add-cluster` and `remove-cluster` commands. When migrating a cluster, it is recommended to perform the following steps prior to removing the cluster from the XMS:

- ◆ Run the `show-reports-data` command, to export the cluster's performance data to a file.
- ◆ Run the `show-storage-controller` command and register one of the cluster's Storage Controllers IP addresses, to be used when the cluster is added to the XMS.

Configuration Workspace

To access the Configuration workspace, click the **Configuration** icon in the menu bar.

The Configuration workspace consists of an entity list pane and a main view pane. Clicking an entity from the list displays its detailed view in the main pane. Double-clicking an entity from the list opens the list of Tags that are defined for that entity.

The entity list consists of the following:

- ◆ Volumes
- ◆ Consistency Groups
- ◆ Snapshot Sets
- ◆ Initiator Groups
- ◆ Initiators
- ◆ Schedulers

Figure 24 shows the main panes in the Configuration Workspace.

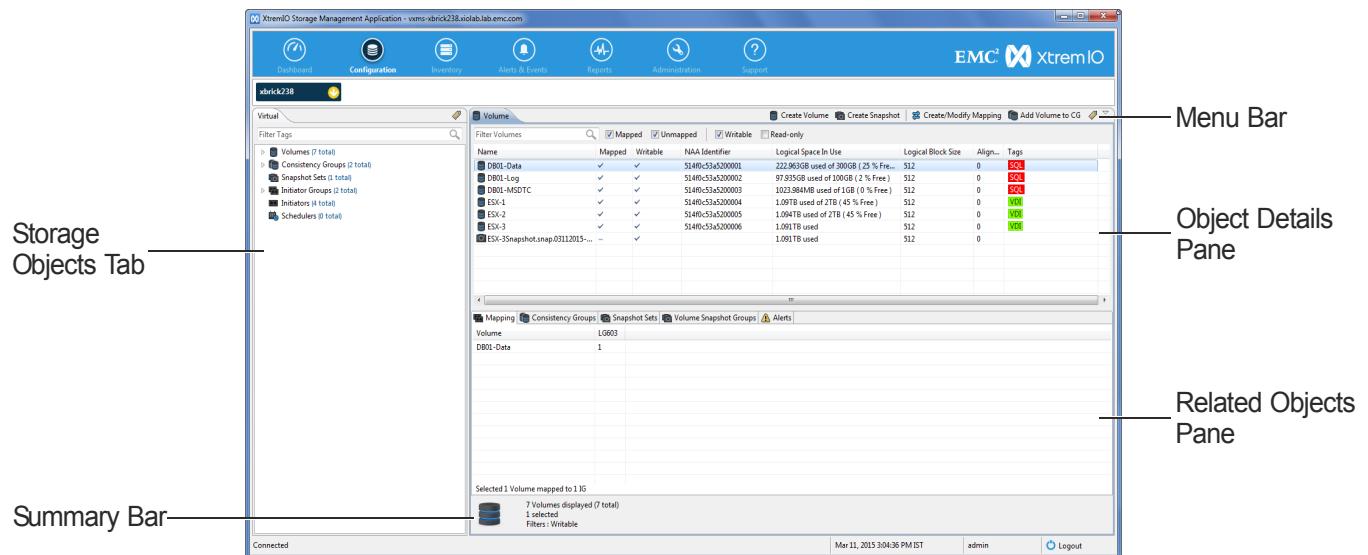


Figure 24 Configuration Workspace

Volumes View

To open the Volumes view, click **Volumes** in the entity list.

[Figure 25](#) shows the Volumes view.

Name	Mapped	Writable	NAA Identifier	Logical Space In Use	Logical Block Size	Align...	Tags
DB01-Data	✓	✓	5140c53a5200001	297.195GB used of 300GB (0 % Free)	S12	0	SQL
DB01-Log	✓	✓	5140c53a5200002	10.00GB used of 100GB (0 % Free)	S12	0	SQL
DB01-MSDTC	✓	✓	5140c53a5200003	1023.992MB used of 1GB (0 % Free)	S12	0	SQL
ESX-1	✓	✓	5140c53a5200004	2.361TB used	S12	0	VMware
ESX-1.snap.03112015-17:55:34	—	✓		2.361TB used	S12	0	VMware
ESX-1.snap.03112015-17:58:07	—	✓		2.361TB used	S12	0	VMware
ESX-1.snap.03112015-17:59:17	—	✓		2.361TB used	S12	0	VMware
ESX-2	✓	✓	5140c53a5200005	2.361TB used	S12	0	VMware
ESX-2.snap.03112015-17:55:34	—	✓		2.361TB used	S12	0	VMware
ESX-2.snap.03112015-17:58:07	—	✓		2.361TB used	S12	0	VMware
ESX-2.snap.03112015-17:59:17	—	✓		2.361TB used	S12	0	VMware

Figure 25 Volumes View

[Table 5](#) describes the main icons in the Volumes View.

Table 5 Volumes View Icons

Icon	Description
	Create Volume Enables you to add new Volumes.
	Create Snapshot Enables you to create Snapshots of defined Volumes (also available in the Volumes right-click menu).
	Create Mapping Maps the selected Volumes to the selected Initiator Groups (also available in the Volumes right-click menu).
	Add Volume to CG Adds the selected Volume to a Consistency Group (also available in the Volumes right-click menu).
	Manage Tags Enables you to manage the selected Volume's Tags (also available in the Volumes right-click menu).

The bottom pane provides separate tabs with details on the following Volume-related elements:

- ◆ Mapping
- ◆ Volume Snapshot Groups
- ◆ Consistency Groups
- ◆ Snapshot Sets
- ◆ Schedulers
- ◆ Alerts

Volumes Right-Click Menu

Figure 26 shows the drop-down menu, which appears upon right-clicking an item in the Volumes list.

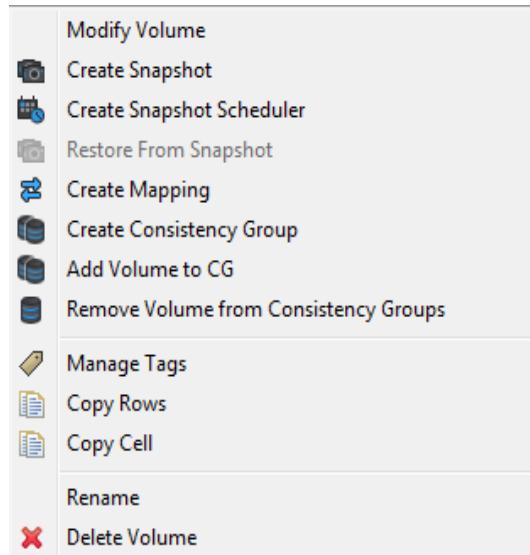


Figure 26 Volumes List Right-Click Drop-Down Menu

Table 6 describes the drop-down menu's active options.

Table 6 Volumes Pane Drop-Down Menu Active Options

Icon	Description
 Modify Volume	Modify Volume Enables you to resize a Volume and to modify the Volume alert settings.
 Create Snapshot	Create Snapshot Enables you to create a Snapshot of the selected Volume.
 Create Snapshot Scheduler	Create Snapshot Scheduler Enables you to create a Scheduler for generating Snapshots of a selected Volume.
 Restore From Snapshot	Restore From Snapshot Enables you to restore a selected Volume from a Snapshot.
 Create Mapping	Create Mapping Enables you to map the selected Volumes to the selected Initiator Groups.
 Create Consistency Group	Create Consistency Group Enables you to create a new Consistency Group.
 Add Volume to CG	Add Volume to CG Enables you to add a Volume to a Consistency Group.
 Remove Volume from Consistency Groups	Remove Volume from Consistency Group Enables you to remove a Volume from a Consistency Group.
 Manage Tags	Manage Tags Enables you to manage the selected Volume Tags.
 Copy Rows	Copy Rows Enables you to copy rows.
 Copy Cell	Copy Cell Enables you to copy a cell.
 Rename	Rename Enables you to change the name of the selected item.
 Delete Volume	Delete Volume Enables you to delete the selected Volume.

Consistency Groups View

To open the Consistency Groups view, click **Consistency Groups** in the entity list.

[Figure 27](#) shows the Consistency Groups view.

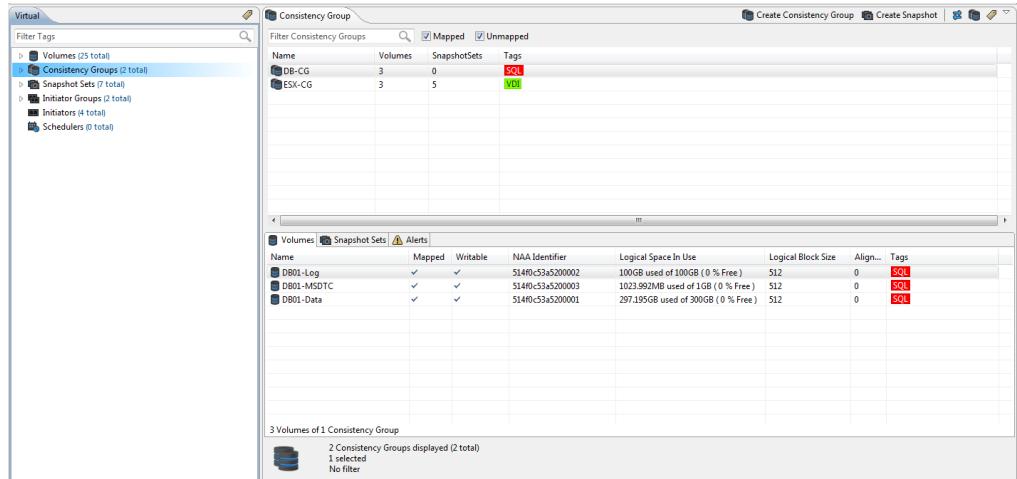


Figure 27 Consistency Groups View

[Table 7](#) describes the main icons in the Consistency Groups View.

Table 7 Consistency Groups View Icons

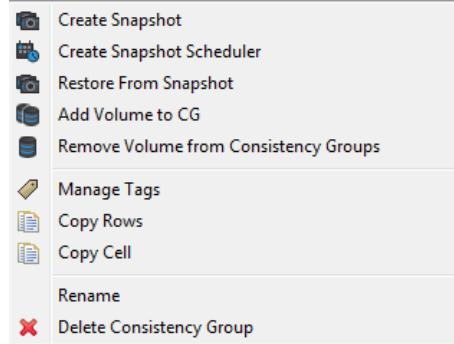
Icon	Description
	Create Consistency Group Enables you to add a new Consistency Group.
	Create Snapshot Enables you to create Snapshots of the defined Consistency Groups (also available in the Consistency Group right-click menu).
	Create Mapping Maps the selected Consistency Groups to the selected Initiator Groups (also available in the Consistency Group right-click menu).
	Add Volume to CG Enables you to add Volumes to the selected Consistency Group (also available in the Consistency Group right-click menu).
	Manage Tags Enables you to manage the selected Consistency Group's Tags (also available in the Consistency Group right-click menu).

The bottom pane provides separate tabs with details on the following Consistency-Group-related elements:

- ◆ Volumes
- ◆ Mapping of Member Volumes
- ◆ Snapshot Sets
- ◆ Schedulers
- ◆ Alerts

Consistency Group Right-Click Menu

[Figure 28](#) shows the drop-down menu, which appears upon right-clicking an item in the Consistency Groups pane.



[Figure 28](#) Consistency Groups Pane Right-Click Drop-Down Menu

[Table 8](#) describes the drop-down menu's options.

Table 8 Consistency Groups Pane Drop-Down Menu Options

Icon	Description
	Create Snapshot Enables you to create a Snapshot of the selected Consistency Group.
	Create Snapshot Scheduler Enables you to create a Scheduler for generating Snapshots of the selected Consistency Group.
	Restore From Snapshot Enables you to restore the selected Consistency Group from a Snapshot.
	Add Volume to CG Enables you to add a Volume to the selected Consistency Group.
	Remove Volume from Consistency Groups Enables you to remove a Volume from the selected Consistency Group.
	Manage Tags Enables you to manage the selected Consistency Group's Tags.
	Copy Rows Enables you to copy rows.
	Copy Cell Enables you to copy a cell.
	Rename Enables you to change the name of the selected item.
	Delete Volume Enables you to delete the selected Consistency Group.

Snapshot Sets View

To open the Snapshot Sets view, click **Snapshot Sets** in the entity list.

[Figure 29](#) shows the Snapshot Sets view.

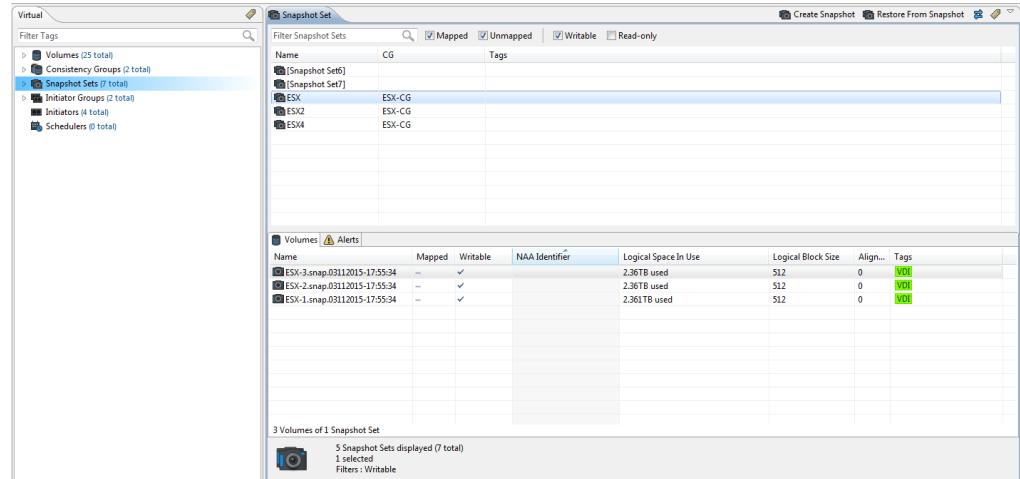


Figure 29 Snapshot Sets View

[Table 9](#) describes the main icons in the Snapshot Sets View.

Table 9 Snapshot Sets View Icons

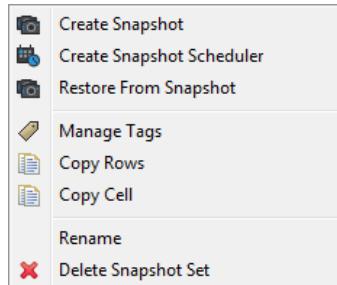
Icon	Description
	Create Snapshot Enables you to create Snapshots of the defined Consistency Groups (also available in the Snapshot Set right-click menu).
	Restore From Snapshot Enables you to restore the selected Snapshot Set from a Snapshot.
	Create Mapping Maps the selected Snapshot Set to the selected Initiator Groups (also available in the Snapshot Set right-click menu).
	Manage Tags Enables you to manage the selected Snapshot Set's Tags (also available in the Snapshot Set right-click menu).

The bottom pane provides separate tabs with details on the following Snapshot-Sets-related elements:

- ◆ Volumes
- ◆ Mapping of Member Volumes
- ◆ Consistency Groups
- ◆ Schedulers
- ◆ Alerts

Snapshot Sets Right-Click Menu

[Figure 30](#) shows the drop-down menu, which appears upon right-clicking an item in the Snapshot Sets pane.



[Figure 30](#) Snapshot Sets Pane Right-Click Drop-Down Menu

[Table 10](#) describes the drop-down menu's options.

[Table 10](#) Snapshot Sets View Icons

Icon	Description
Create Snapshot	Create Snapshot Enables you to create Snapshots of the defined Snapshot Sets.
Create Snapshot Scheduler	Create Snapshot Scheduler Enables you to create a Scheduler for generating Snapshots of the selected Snapshot Set.
Restore From Snapshot	Restore From Snapshot Enables you to restore the selected Snapshot Set from a Snapshot.
	Manage Tags Enables you to manage the selected Snapshot Set's Tags.
Copy Rows	Copy Rows Enables you to copy rows.
Copy Cell	Copy Cell Enables you to copy a cell.
Rename	Rename Enables you to change the name of the selected Snapshot Set.
Delete Volume	Delete Volume Enables you to delete the selected Snapshot Set.

Initiator Groups View

To open the Initiator Groups view, click **Initiator Groups** in the entity list.

[Figure 31](#) shows the Initiator Groups view.

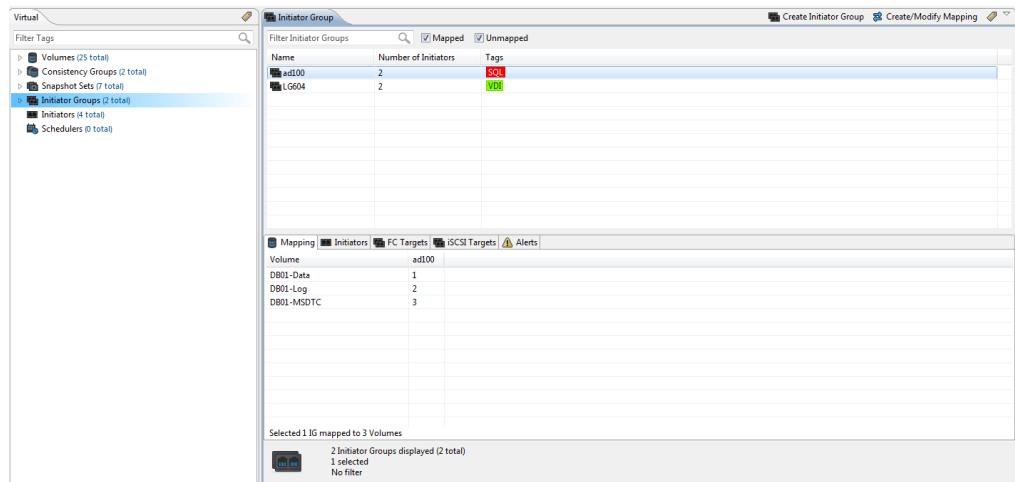


Figure 31 Initiator Groups View

[Table 11](#) describes the main icons in the Initiator Groups View.

Table 11 Initiator Groups View Icons

Icon	Description
	Create Initiator Group Enables you to create a new Initiator Group.
	Create Mapping Maps the selected Initiator Group to selected Volumes (also available in the Initiator Group right-click menu).
	Manage Tags Enables you to manage the selected Initiator Group's Tags (also available in the Initiator Group right-click menu).

The bottom pane provides separate tabs with details on the following Initiator-Groups-related elements:

- ◆ Mapping
- ◆ Initiators
- ◆ Targets
- ◆ Alerts

Initiator Groups Right-Click Menu

[Figure 32](#) shows the drop-down menu, which appears upon right-clicking an item in the Initiator Groups pane.

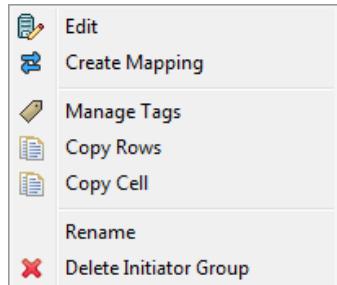


Figure 32 Initiator Group Pane Right-Click Drop-Down Menu

[Table 12](#) describes the drop-down menu icons.

Table 12 Initiator Groups View Icons

Icon	Description
	Edit Enables you to modify the properties of the selected Initiator Group.
	Create Mapping Maps the selected Initiator Group to selected Volumes.
	Manage Tags Enables you to manage the selected Initiator Group Tags.
	Copy Rows Enables you to copy rows.
	Copy Cell Enables you to copy a cell.
	Rename Enables you to change the name of the selected Initiator Group.
	Delete Initiator Group Enables you to delete the selected Initiator Group.

Initiators View

To open the Initiators view, click **Initiators** in the entity list.

[Figure 33](#) shows the Initiator Groups view.

The screenshot shows the 'Initiator' tab in the Initiators View. On the left, a sidebar lists 'Virtual' entities: Volumes (25 total), Consistency Groups (2 total), Snapshot Sets (7 total), Initiator Groups (2 total), Initiators (4 total), and Schedulers (0 total). The 'Initiators (4 total)' item is selected. The main pane displays a table of initiators:

Name	Initiator Group	Port Type	Port Address	Connection State	Number of Co...	CHAP Discovery Initiator User
LG603-1	ad100	FC	21:00:00:24:ff:4a:3e:2d	Connected	3	
LG603-2	ad100	FC	21:00:00:24:ff:4a:3e:2c	Connected	3	
LG604-1	LG604	FC	21:00:00:24:ff:4a:3cda	Connected	3	
LG604-2	LG604	FC	21:00:00:24:ff:4a:3cdb	Connected	3	

Below the table, there are tabs for FC Targets, iSCSI Targets, and Alerts. The FC Targets tab is selected, showing a list of initiator groups and their connections to storage ports (X1-SC1-fc1, X1-SC1-fc2, X1-SC2-fc1, X1-SC2-fc2). A specific connection for initiator group ad100 to port LG603-1 [21:00:00:24:ff:4a:3e:2d] is highlighted. At the bottom, a status bar indicates '4 Initiators displayed (4 total)', '1 selected', and 'No filter'.

Figure 33 Initiators View

[Table 13](#) describes the main icons in the Initiators View.

Table 13 Initiators View Icons

Icon	Description
	Manage Tags Enables you to manage the selected Initiator's Tags (also available via Initiators right-click menu).
	View Menu Enables you to select all items in the Initiators table.

The bottom pane provides separate tabs with details on the following Initiators-related elements:

- ◆ Targets
- ◆ Alerts

Initiators Right-Click Menu

[Figure 34](#) shows the drop-down menu, which appears upon right-clicking an item in the Initiators pane.

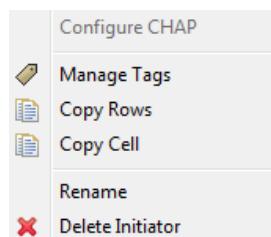


Figure 34 Initiators Right-Click Drop-Down Menu

Table 14 describes the drop-down menu icons.

Table 14 Initiator Groups Drop-Down Menu Icons

Icon	Description
 Configure CHAP	Configure CHAP Enables you to configure the Challenge-Handshake Authentication Protocol.
 Manage Tags	Manage Tags Enables you to manage the selected Initiator Tags.
 Copy Rows	Copy Rows Enables you to copy rows.
 Copy Cell	Copy Cell Enables you to copy a cell.
 Rename	Rename Enables you to change the name of the selected Initiator.
 Delete Initiator	Delete Initiator Enables you to delete the selected Initiator.

Schedulers View

To open the Schedulers view, click **Schedulers** in the entity list.

Figure [Figure 35](#) shows the Schedulers view.

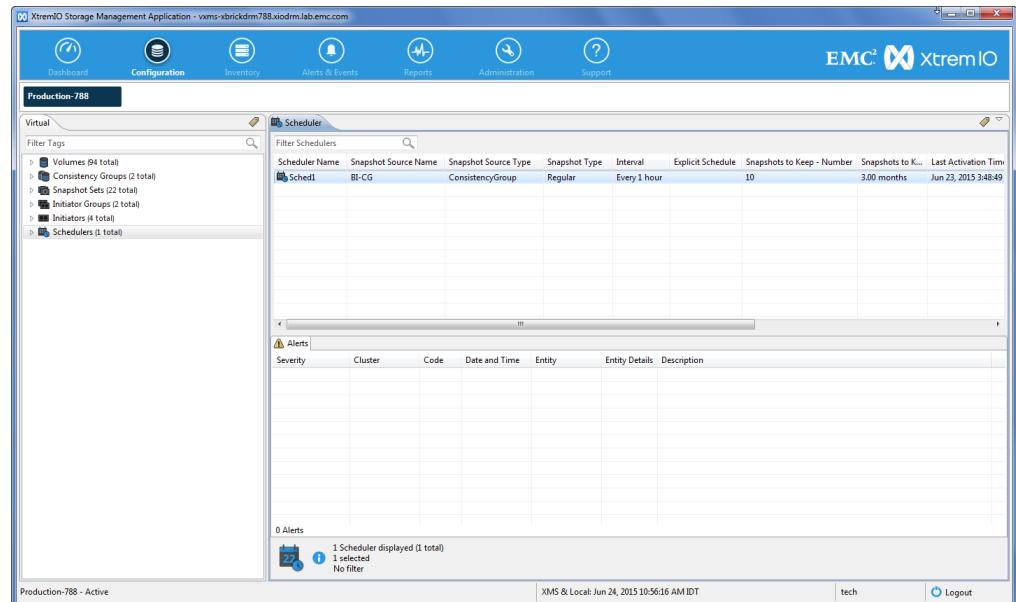


Figure 35 Schedulers View

[Table 15](#) describes the main icons in the Schedulers View.

Table 15 Schedulers View Icons

Icon	Description
	Manage Tags Enables you to manage the selected Schedulers Tags (also available via Schedulers right-click menu).
	View Menu Enables you to select all items in the Schedulers table.

The bottom pane provides details on Schedulers-related alerts.

Schedulers Right-Click Menu

[Figure 36](#) shows the drop-down menu, which appears upon right-clicking an item in the Schedulers pane.

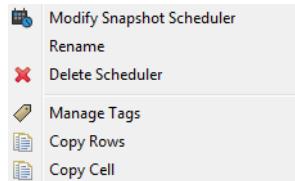


Figure 36 Schedulers Right-Click Drop-Down Menu

[Table 16](#) describes the drop-down menu icons.

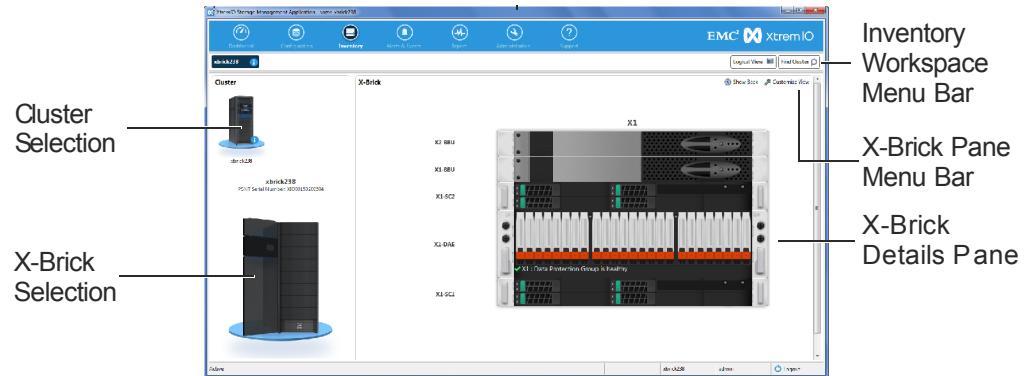
Table 16 Schedulers Right-Click Menu Icons

Icon	Description
Modify Snapshot Scheduler	Modify Snapshot Scheduler Enables you to modify the selected Scheduler parameters.
Rename	Rename Enables you to change the name of the selected Scheduler.
Delete Scheduler	Delete Scheduler Enables you to delete the selected Scheduler.
Resume Scheduler	Resume Scheduler Enables you to reactivate a suspended Scheduler.
Suspend Scheduler	Suspend Scheduler Enables you to suspend an active Scheduler.
Manage Tags	Manage Tags Enables you to manage the selected Scheduler Tags.
Copy Rows	Copy Rows Enables you to copy rows.
Copy Cell	Copy Cell Enables you to copy a cell.

Inventory Workspace

[Figure 37](#) shows the Inventory Workspace.

To access the Inventory workspace, click the **Inventory** icon in the menu bar.



[Figure 37](#) Inventory Workspace

- ◆ The Inventory workspace consists of the following sections:
 - Cluster Selection - displays the cluster or clusters in the system and the currently managed cluster.
 - X-Brick Selection - displays the X-Bricks of the managed cluster and allows the user to select an X-Brick to be presented in detail in the X-Brick Details pane.
 - X-Brick Details - displays the components of the X-Brick that is selected in the Cluster pane.
 - Inventory Workspace Menu Bar - provides options for manipulating the Inventory workspace display, as detailed in [Table 17](#).
 - X-Brick Pane Menu Bar - provides options for manipulating the X-Brick Details pane display, as detailed in [Table 18](#).
- ◆ If a hardware component has a pending alert, its color changes according to the alert's severity:
 - Yellow - minor alert
 - Orange - major alert
 - Red - critical alert
- ◆ In a multiple X-Brick cluster, selecting an X-Brick or an InfiniBand Switch in the Cluster pane (on the left) displays the details of the selected component in the X-Brick pane on the right.
- ◆ Hovering the mouse pointer over the a cluster, X-Brick or hardware component displays a tool-tip with information and status, as shown in [Figure 38](#).



Figure 38 Hovering the Mouse Cursor over the Hardware Component to View its Status

Main Icons

[Table 17](#) describes the main icons in the Inventory workspace Menu Bar.

Table 17 Inventory Workspace Menu Bar Icons

Icon	Description
	X-Brick Icon Displays the name of the currently managed X-Brick.
	Logical View Displays the logical view of the X-Brick and its components.
	Physical View Displays the physical image of the X-Brick and its components (default view).

[Table 18](#) describes the main icons in the X-Brick pane Menu Bar.

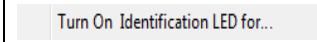
Table 18 X-Brick Pane Menu Bar Options

Icon	Description
	Show Front Displays the front side view of the hardware.
	Show Back Displays the back side view of the hardware.
	Customize View Enables you to show/conceal the status LEDs. When the Show Cable Connectivity option is selected, Customize View provides a rich dialog for selecting which cables to display and in what manner (for details, refer to “ Hardware Customize view ”).
	Show Cable Connectivity Displays the cable connectivity scheme on the back side of the hardware, as shown in Figure 43 .

Hardware Drop-Down Menu Options

[Table 19](#) describes the active options of drop-down menus, which appear upon right-clicking a hardware component.

Table 19 Hardware Drop-Down Menu Active Options

Icon	Description
 Turn On Identification LED for...	Turn On Identification LED for... Turns on the identification LED of the selected component.
 Change All Other ... Identification LEDs	Change All Other Identification LEDs Turns on/off the identification LEDs of all but the selected component.
 Add SSD	Add SSD Enables you to add an SSD to the cluster (appears when right-clicking an SSD).
 Remove SSD	Remove SSD Enables you to remove an SSD from the cluster (appears when right-clicking an SSD).
 Display Alerts	Display Alerts Displays alerts for the selected item.

Hardware Components' LEDs

Many of the XtremIO Storage Array hardware components are equipped with two LED types that enable you to monitor the components' health:

- ◆ Identification LED - Used to identify a component in the cluster.
- ◆ Status LED - Used to indicate the status of the component.

In addition to the actual LEDs on the physical hardware components, identical graphical representation of the LEDs appears in the GUI's hardware image.

The possible states of the LEDs are:

- ◆ Off
- ◆ On (beacon)

[Table 20](#) provides details of the hardware components' LEDs.

Table 20 Hardware Components' LEDs

Component	Identification LED	Identification LED Possible States	Status LED
Storage Controller	Yes	On, off	Yes
Storage Controller SSD	Yes	On, off	Yes
Storage Controller HDD	Yes	On, off	Yes
Storage Controller PSU & Fan	No	N/A	Yes
DAE	Yes	Blink, off	Yes
DAE SSD	Yes	Blink, off	Yes (called "Data LED")
DAE Controller	Yes	Blink, off	Yes
DAE PSU & Fan	No	N/A	Yes
Battery Backup Unit	No	N/A	Yes
InfiniBand Switch	No	N/A	Yes
InfiniBand Switch PSU	No	N/A	Yes
InfiniBand Switch Fan	No	N/A	Yes
Physical XMS	No	N/A	Yes
Physical XMS PSU & Fan	No	N/A	Yes

Using the GUI to Activate the Identification LEDs

You can identify a component in the cluster, using the following methods:

- ◆ Turning on the component's identification LED
- ◆ Turning on the LEDs of all other components (all but the selected component), if the component has failed and does not respond

To turn on a component's identification LED:

1. In the dashboard menu bar, click the **Inventory** icon.
2. Hover the mouse pointer over the relevant hardware component and right-click to open the drop-down menu.
3. Select **Turn On Identification LED for <component's name>**; a message appears, stating that the component's LED will be turned On/Off.



Figure 39 Turn On LED

4. Click **OK**.

Note: If the component's identification LED is already turned on, a check sign appears next to the **Turn On Identification LED** option and the message box that follows states that the LED will be turned **off**.

To turn all other identification LEDs on or off:

1. In the dashboard menu bar, click the **Hardware** icon.
2. Hover the mouse pointer over the relevant hardware component and right-click to open the drop-down menu.
3. Select **Change all other <component type> Identification LEDs**.



Figure 40 Change All Other LEDs

4. In the Change All Other Identification LEDs dialog box, select the desired state of the LEDs (On or Off) and click **OK**; the LEDs of all components, except for the LED of the component you want to identify, change their state.

Main Elements

[Figure 41](#), [Figure 42](#) and [Figure 43](#) show the possible displays of the Inventory workspace.



Figure 41 Hardware Front View

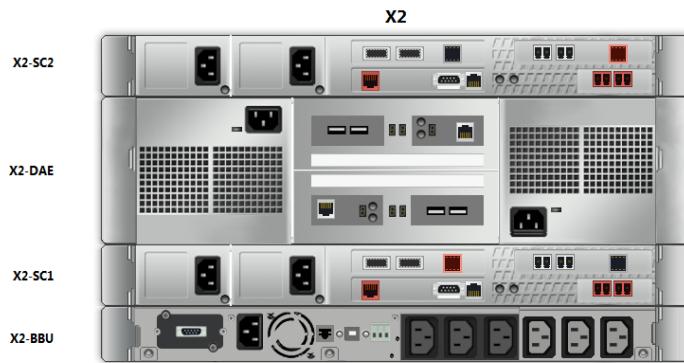


Figure 42 Hardware Back View

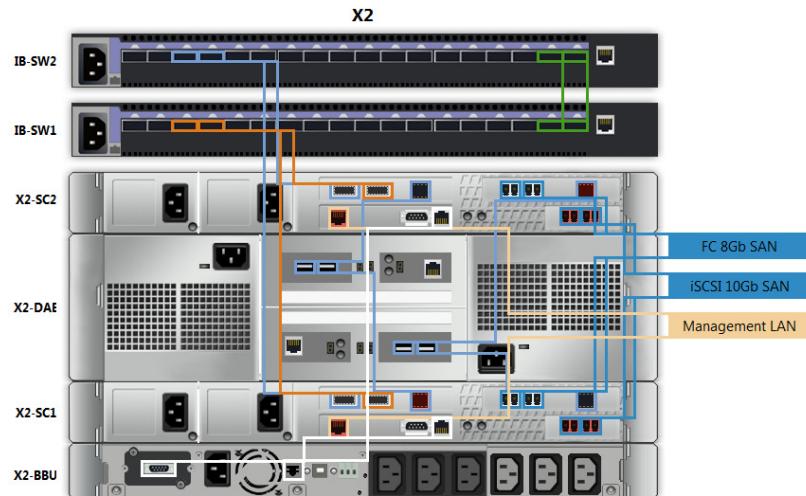


Figure 43 Hardware Back View with Cable Connectivity

Hardware Customize view

The Customize View option provides different results according to context:

- ◆ When the front or the back view are displayed, clicking **Customize View** enables you to show the displayed hardware components fault LEDs.

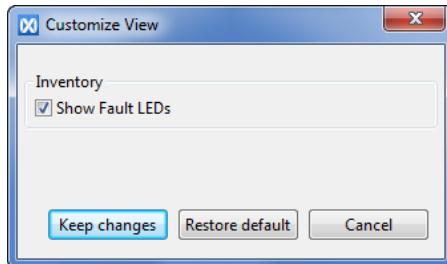


Figure 44 Customize View - Front or Back View

- ◆ When Cable Connectivity is displayed, clicking **Customize View** enables you to show the fault LEDs of the displayed components, and to set the following connectivity display parameters:
 - Displayed connectivity line type
 - Displayed connectivity type group
 - Displayed connectivity types
 - Connectivity display colors

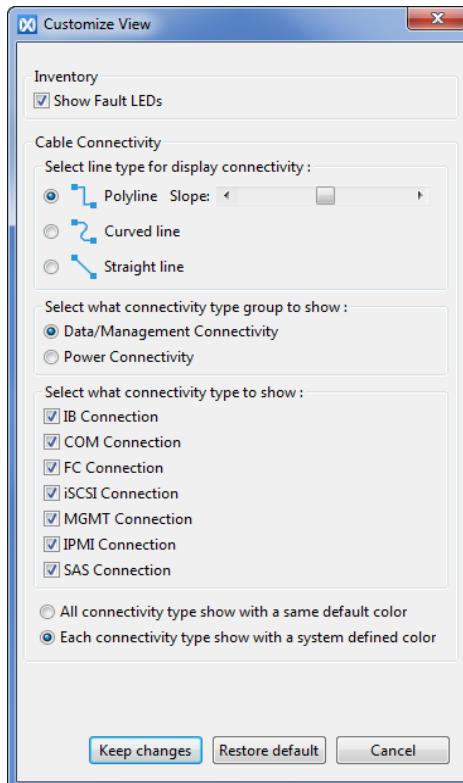


Figure 45 Customize View - Cable Connectivity

Inventory List View

To open the cluster's Inventory List view, click **Inventory List** in the Inventory workspace menu bar. You can also access the X-Brick's logical view by clicking one of the X-Brick's components in the Inventory pane of the Dashboard screen.

The Inventory List View provides details on the cluster's components. The following windows are displayed:

- ◆ Inventory List pane - displays a list of all cluster's components and their quantities.
- ◆ Component - displays a table of all instances of the selected component and provides detailed component data.
- ◆ Related entities - displays a table of entities that are relevant to the selected component and provides relevant data on each entity.
- ◆ Data summary - summarizes the number of displayed components and selected components.

Clusters View

To open the Clusters view, click **Clusters** in the Inventory List pane.

Figure 46 shows the Clusters view.

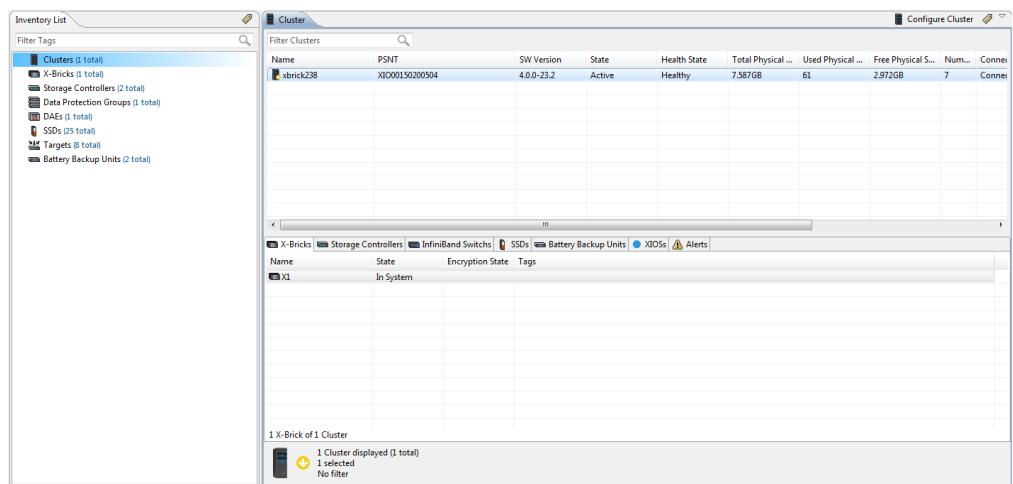
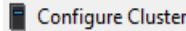


Figure 46 Inventory List - Clusters View

[Table 21](#) describes the main icons in the Clusters View.

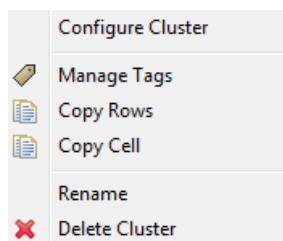
Table 21 Clusters View Icons

Icon	Description
 Configure Cluster	Configure Cluster Enables you to configure the selected cluster's properties (also available via Clusters right-click menu). See “ Cluster Configuration ” on page 90.
 Manage Tags	Manage Tags Enables you to manage the selected cluster's Tags (also available via Clusters right-click menu).
 View Menu	View Menu Enables you to select all items in the Clusters table.

The following data is provided for each cluster:

- ◆ Cluster name
- ◆ Cluster PSNT
- ◆ Cluster software version
- ◆ Cluster state
- ◆ Cluster health state
- ◆ Total physical capacity
- ◆ Used physical capacity (in percentage)
- ◆ Free physical capacity
- ◆ Number of Volumes
- ◆ Cluster connection state
- ◆ Cluster Tags

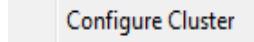
[Figure 47](#) shows the drop-down menu, which appears upon right-clicking an item in the Clusters table.



[Figure 47](#) Cluster Table Right-Click Menu

Table 22 describes the drop-down menu icons.

Table 22 Cluster View Right-Click Menu Icons

Icon	Description
 Configure Cluster	Configure Cluster Enables you to configure the selected cluster properties. See “Cluster Configuration” on page 90.
 Manage Tags	Manage Tags Enables you to assign a Tag to the selected cluster.
 Copy Rows	Copy Rows Enables you to copy rows.
 Copy Cell	Copy Cell Enables you to copy a cell.
 Rename	Rename Enables you to change the name of the selected cluster.
 Delete Cluster	Delete Cluster Enables you to delete the selected cluster.

The following related entities are displayed:

- ◆ X-Bricks
- ◆ Storage Controllers
- ◆ InfiniBand Switches
- ◆ SSDs
- ◆ Battery Backup Units
- ◆ Xenvs
- ◆ Alerts

X-Bricks View

To display the X-Bricks' window, click **X-Bricks** in the Inventory List pane.

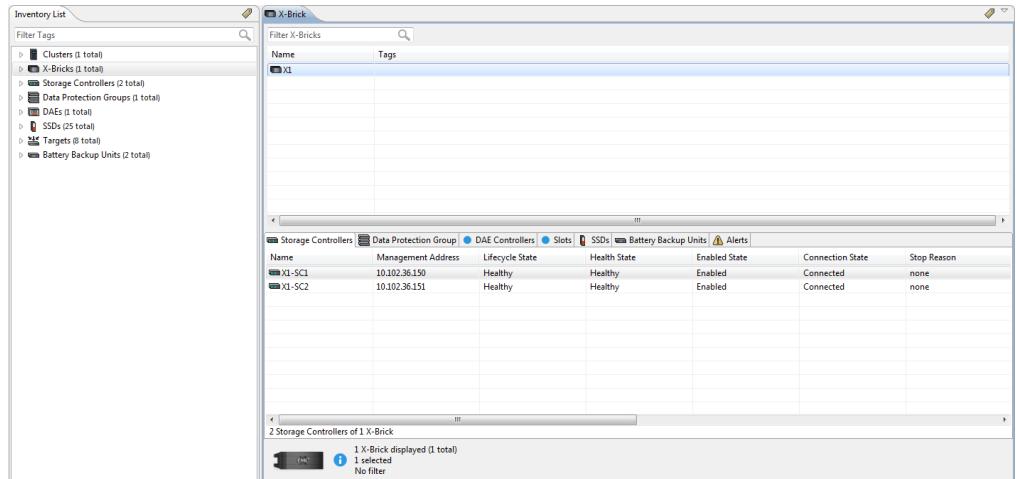


Figure 48 Inventory List - X-Bricks View

The following data is provided for each X-Brick:

- ◆ X-Brick name
- ◆ Cluster name
- ◆ X-Brick Tags

[Figure 49](#) shows the drop-down menu, which appears upon right-clicking an item in the X-Bricks table.

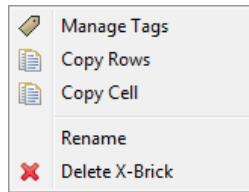


Figure 49 X-Brick Table Right-Click Menu

Table 23 describes the drop-down menu icons.

Table 23 X-Brick View Right-Click Menu Icons

Icon	Description
Manage Tags	Manage Tags Enables you to assign a Tag to the selected X-Brick.
Copy Rows	Copy Rows Enables you to copy rows.
Copy Cell	Copy Cell Enables you to copy a cell.
Rename	Rename Enables you to change the name of the selected X-Brick.
Delete X-Brick	Delete X-Brick Enables you to delete the selected X-Brick.

The following related entities are displayed:

- ◆ Storage Controllers
- ◆ Data Protection Groups
- ◆ DAE Controllers
- ◆ Slots
- ◆ SSDs
- ◆ Battery Backup Units
- ◆ Alerts

Storage Controllers View

To display the Storage Controllers' window, click **Storage Controllers** in the Inventory List pane.

Name	Management Address	Lifecycle State	Health State	Enabled State	Connection State	Stop Reason
XI-SC1	10.102.36.150	Healthy	Healthy	Enabled	Connected	none
XI-SC2	10.102.36.151	Healthy	Healthy	Enabled	Connected	none

Name	Lifecycle State	Slot Number	Type	Purpose	Encryption Status	Failure State	Product
XI-SC1-LocalDisk1	Healthy	0	SSD	Journal and Boot Disk	The SSD supports encry...	Ok	HITAC...
XI-SC1-LocalDisk2	Healthy	1	HDD	Trace Disk	Encryption is not suppo...	Ok	HITAC...
XI-SC1-LocalDisk3	Healthy	4	SSD	Journal Disk	Encryption is not suppo...	Ok	HITAC...
XI-SC1-LocalDisk4	Healthy	5	HDD	Trace Disk	Encryption is not suppo...	Ok	HITAC...

Figure 50 Inventory List - Storage Controllers View

The following data is provided for each Storage Controller:

- ◆ Storage Controller name
- ◆ Cluster name
- ◆ Management address
- ◆ Lifecycle state
- ◆ Health state
- ◆ Enabled state
- ◆ Connection state
- ◆ Stop reason
- ◆ SAS1 port state
- ◆ SAS1 port rate
- ◆ SAS2 port state
- ◆ SAS2 port rate
- ◆ Serial number
- ◆ Tags

[Figure 51](#) shows the drop-down menu, which appears upon right-clicking an item in the Storage Controllers table.



[Figure 51](#) Storage Controllers Table Right-Click Menu

Table 24 describes the drop-down menu icons.

Table 24 Storage Controllers View Right-Click Menu Icons

Icon	Description
Turn On Identification LED for Storage Controller ...	Turn On Identification LED for Storage Controller Turns on the identification LED of the selected Storage Controller.
Change All Other Storage Controllers Identification LEDs	Change All Other Storage Controllers Identification LEDs Turns on/off the identification LEDs of all but the selected Storage Controller.
Manage Tags	Manage Tags Enables you to assign a Tag to the selected Storage Controller.
Copy Rows	Copy Rows Enables you to copy rows.
Copy Cell	Copy Cell Enables you to copy a cell.
Rename	Rename Enables you to change the name of the selected Storage Controller.
Delete Storage Controller	Delete Storage Controller Enables you to delete the selected Storage Controller.

The following related entities are displayed:

- ◆ Local Disks
- ◆ Storage Controller Power Supply
- ◆ Targets
- ◆ Xenvs
- ◆ Alerts

Data Protection Groups View

To display the Data Protection Groups' window, click **Data Protection Groups** in the Inventory List pane.

Name	Protection State	Rebuild Progress	SSD Preparation	Proactive Metadata Loading	Total SSD Size	Useful SSD Space	UD SSD Space	In Use UD SSD Space	Free UD SSD Space
X1-DPG	Normal	Not In Progress	Not In Progress	Not In Progress	9.095TB	9.095TB	7.587TB	1.554TB	0

Index	Slot	X-Brick	WWN	Connection State	Size	Space In Use	DPG State	Lifecycle Status	Endurance Remaining (%)	Encryption Status
1	0	X1	wwn-0x0000cc04e04d...	Connected	372.529GB	66.11GB	In DPG	Healthy	100	The SSD is healthy
2	1	X1	wwn-0x0000cc04e04d2...	Connected	372.529GB	65.857GB	In DPG	Healthy	100	The SSD is healthy
3	2	X1	wwn-0x0000cc04e0098...	Connected	372.529GB	65.923GB	In DPG	Healthy	100	The SSD is healthy
4	3	X1	wwn-0x0000cc04e04c...	Connected	372.529GB	65.735GB	In DPG	Healthy	100	The SSD is healthy
5	4	X1	wwn-0x0000cc04e04d2...	Connected	372.529GB	65.585GB	In DPG	Healthy	100	The SSD is healthy
6	5	X1	wwn-0x0000cc04e060...	Connected	372.529GB	65.647GB	In DPG	Healthy	100	The SSD is healthy
7	6	X1	wwn-0x0000cc04e0098...	Connected	372.529GB	65.528GB	In DPG	Healthy	100	The SSD is healthy
8	7	X1	wwn-0x0000cc04e04c...	Connected	372.529GB	65.482GB	In DPG	Healthy	100	The SSD is healthy
9	8	X1	wwn-0x0000cc04e04c...	Connected	372.529GB	65.489GB	In DPG	Healthy	100	The SSD is healthy
10	9	X1	wwn-0x0000cc04e060fb...	Connected	372.529GB	65.336GB	In DPG	Healthy	100	The SSD is healthy
11	10	X1	wwn-0x0000cc04e04c...	Connected	372.529GB	65.303GB	In DPG	Healthy	100	The SSD is healthy

Figure 52 Inventory List - Data Protection Groups View

The following data is provided for each DPG:

- ◆ DPG name
- ◆ Cluster name
- ◆ DPG protection state
- ◆ Rebuild progress (percentage)
- ◆ SSD preparation progress (percentage)
- ◆ Proactive metadata loading
- ◆ Total SSD size
- ◆ Useful SSD space
- ◆ UD SSD space
- ◆ In use UD SSD space
- ◆ Free UD SSD space (percentage)
- ◆ Free UD SSD space level
- ◆ Tags

[Figure 53](#) shows the drop-down menu, which appears upon right-clicking an item in the Data Protection Group table.



Figure 53 Data Protection Group Table Right-Click Menu

Table 25 describes the drop-down menu icons.

Table 25 Data Protection Group View Right-Click Menu Icons

Icon	Description
Manage Tags	Manage Tags Enables you to assign a Tag to the selected Data Protection Group.
Copy Rows	Copy Rows Enables you to copy rows.
Copy Cell	Copy Cell Enables you to copy a cell.
Rename	Rename Enables you to change the name of the selected Data Protection Group.
Delete Data Protection Group	Delete Data Protection Group Enables you to delete the selected Data Protection Group.

The following related entities are displayed:

- ◆ SSDs
- ◆ Alerts

DAEs View

To display the DAEs' window, click **DAEs** in the Inventory List pane.

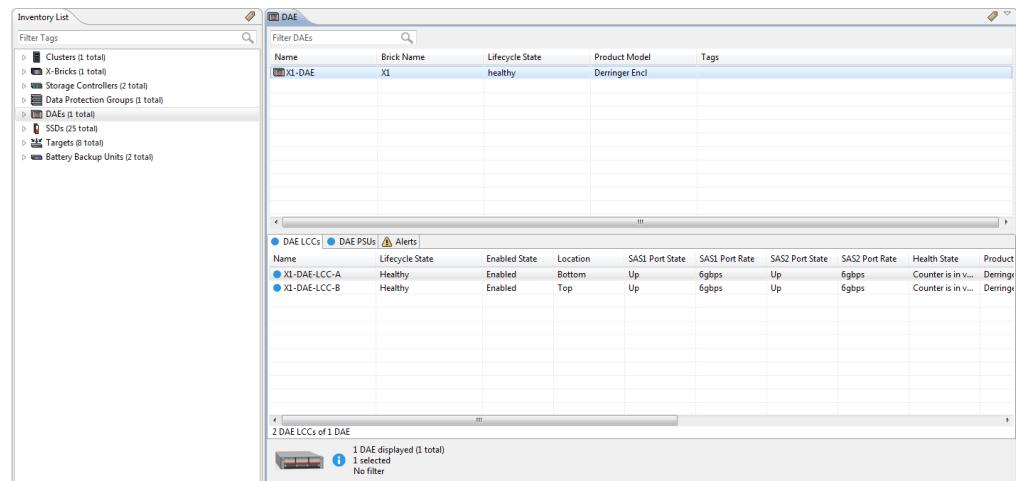


Figure 54 Inventory List - DAEs View

The following data is provided for each DAE:

- ◆ DAE name
- ◆ Cluster name
- ◆ X-Brick name
- ◆ Lifecycle state
- ◆ Product model
- ◆ Tags

Figure 55 shows the drop-down menu, which appears upon right-clicking an item in the DAEs table.

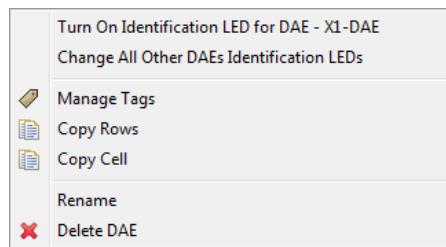


Figure 55 DAEs Table Right-Click Menu

Table 26 describes the drop-down menu icons.

Table 26 DAEs View Right-Click Menu Icons

Icon	Description
	Turn On Identification LED for DAE Turns on the identification LED of the selected DAE.
	Change All Other DAE Identification LEDs Turns on/off the identification LEDs of all but the selected DAE.
	Manage Tags Enables you to assign a Tag to the selected DAE.
	Copy Rows Enables you to copy rows.
	Copy Cell Enables you to copy a cell.
	Rename Enables you to change the name of the selected DAE.
	Delete DAE Enables you to delete the selected DAE.

The following related entities are displayed:

- ◆ DAE LCCs
- ◆ DAE PSUs
- ◆ Alerts

SSDs View

To display the SSDs' window, click **SSDs** in the Inventory List pane.

Index	Slot	X-Brick	WWN	Connection State	Size	Space In Use	DPG State	Lifecycle State	Endurance Remaining (%)	Encryption
1	0	X1	wwn-0x500cc0a04d047...	Connected	372.529GB	66.11GB	In DPG	Healthy	100	The SSD sup...
2	1	X1	wwn-0x500cc0a04d0608...	Connected	372.529GB	65.923GB	In DPG	Healthy	100	The SSD sup...
3	2	X1	wwn-0x500cc0a04d042...	Connected	372.529GB	65.857GB	In DPG	Healthy	100	The SSD sup...
4	3	X1	wwn-0x500cc0a04d041...	Connected	372.529GB	65.857GB	In DPG	Healthy	100	The SSD sup...
5	4	X1	wwn-0x500cc0a04d042...	Connected	372.529GB	65.857GB	In DPG	Healthy	100	The SSD sup...
6	5	X1	wwn-0x500cc0a04d0609...	Connected	372.529GB	65.847GB	In DPG	Healthy	100	The SSD sup...
7	6	X1	wwn-0x500cc0a04d0608...	Connected	372.529GB	65.828GB	In DPG	Healthy	100	The SSD sup...
8	7	X1	wwn-0x500cc0a04d042...	Connected	372.529GB	65.828GB	In DPG	Healthy	100	The SSD sup...
9	8	X1	wwn-0x500cc0a04d0608...	Connected	372.529GB	65.489GB	In DPG	Healthy	100	The SSD sup...
10	9	X1	wwn-0x500cc0a04d0609...	Connected	372.529GB	65.350GB	In DPG	Healthy	100	The SSD sup...
11	10	X1	wwn-0x500cc0a04d042...	Connected	372.529GB	65.303GB	In DPG	Healthy	100	The SSD sup...

0 Alerts

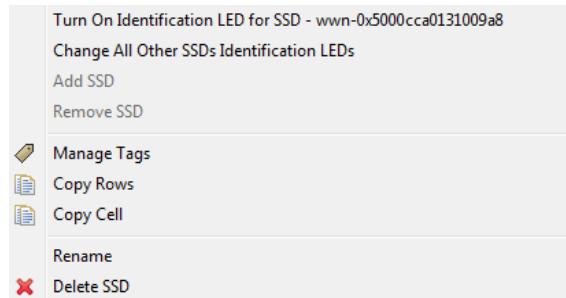
25 SSDs displayed (25 total)
1 selected
No Filter

Figure 56 Inventory List - SSDs View

The following data is provided for each SSD:

- ◆ SSD index
- ◆ Slot
- ◆ Cluster name
- ◆ X-Brick name
- ◆ WWN
- ◆ Connection state
- ◆ Size
- ◆ Space in use
- ◆ DPG state
- ◆ Lifecycle state
- ◆ Endurance remaining (percentage)
- ◆ Encryption state
- ◆ Enabled state
- ◆ Product model
- ◆ Serial number
- ◆ Tags

[Figure 57](#) shows the drop-down menu, which appears upon right-clicking an item in the SSDs table.



[Figure 57](#) SSDs Table Right-Click Menu

[Table 27](#) describes the drop-down menu icons.

Table 27 SSDs View Right-Click Menu Icons

Icon	Description
	Turn On Identification LED for SSD Turns on the identification LED of the selected SSD.
	Change All Other SSD Identification LEDs Turns on/off the identification LEDs of all but the selected SSD.
	Add SSD Enables you to add a new SSD to the list.
	Remove SSD Enables you to remove an SSD from the list.
	Manage Tags Enables you to assign a Tag to the selected SSD.
	Copy Rows Enables you to copy rows.
	Copy Cell Enables you to copy a cell.
	Rename Enables you to change the name of the selected SSD.
	Delete SSD Enables you to delete the selected SSD.

The bottom pane displays SSD-related alert information.

Target View

To display the Targets' window, click **Targets** in the Inventory List pane.

Name	Port Type	Port State	Port Speed	Port Address	Number of Portals	Tags
X1-SC1-fc1	FC	Up	8GFC	51:4f:0:c50:65:8f:4:c00	0	
X1-SC1-fc2	FC	Up	8GFC	51:4f:0:c50:65:8f:4:c01	0	
X1-SC1-iscsi1	iSCSI	Down	10Gb	iqn.2008-05.com.xtremio:xio0015...	0	
X1-SC1-iscsi2	iSCSI	Down	10Gb	iqn.2008-05.com.xtremio:xio0015...	0	
X1-SC2-fc1	FC	Up	8GFC	51:4f:0:c50:65:8f:4:c04	0	
X1-SC2-fc2	FC	Up	8GFC	51:4f:0:c50:65:8f:4:c05	0	
X1-SC2-iscsi1	iSCSI	Down	10Gb	iqn.2008-05.com.xtremio:xio0015...	0	
X1-SC2-iscsi2	iSCSI	Down	10Gb	iqn.2008-05.com.xtremio:xio0015...	0	

Portals | Alerts

Target Port Portal ID IP Address/Subnet VLAN

0 Portals of 1 Target

8 Targets displayed (8 total)
1 selected
No filter

Figure 58 Inventory List - Targets View

The following data is provided for each Target:

- ◆ Target name
- ◆ Cluster name
- ◆ Port type
- ◆ Port state
- ◆ Port speed
- ◆ Port address
- ◆ Number of portals
- ◆ Tags

Figure 59 shows the drop-down menu, which appears upon right-clicking an item in the Targets table.

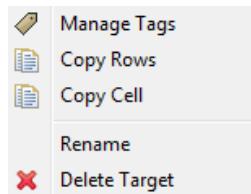


Figure 59 Targets Table Right-Click Menu

Table 28 describes the drop-down menu icons.

Table 28 Targets View Right-Click Menu Icons

Icon	Description
 Manage Tags	Manage Tags Enables you to assign a Tag to the selected Target.
 Copy Rows	Copy Rows Enables you to copy rows.
 Copy Cell	Copy Cell Enables you to copy a cell.
 Rename	Rename Enables you to change the name of the selected Target.
 Delete Target	Delete Target Enables you to delete the selected Target.

The following related entities are displayed:

- ◆ Portals
- ◆ Alerts

Battery Backup Units View

To display the Battery Backup Units' window, click **Battery Backup Units** in the Inventory List pane.

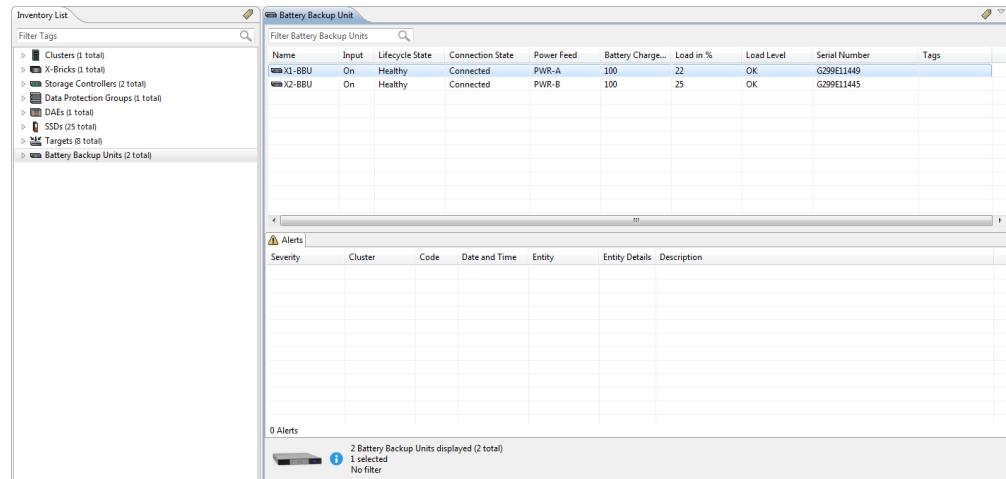


Figure 60 Inventory List - Battery Backup Units View

The following data is provided for each BBU:

- ◆ BBU name
- ◆ Cluster name
- ◆ Input
- ◆ Lifecycle state
- ◆ Connection state
- ◆ Power feed
- ◆ Battery charge percent level
- ◆ Load percent level
- ◆ Load level
- ◆ Serial number

Figure 61 shows the drop-down menu, which appears upon right-clicking an item in the BBUs table.



Figure 61 BBUs Table Right-Click Menu

Table 29 describes the drop-down menu icons.

Table 29 BBUs View Right-Click Menu Icons

Icon	Description
 Manage Tags	Manage Tags Enables you to assign a Tag to the selected BBU.
 Copy Rows	Copy Rows Enables you to copy rows.
 Copy Cell	Copy Cell Enables you to copy a cell.
 Rename	Rename Enables you to change the name of the selected BBU.
 Delete Battery Backup Unit	Delete BBU Enables you to delete the selected BBU.

The bottom pane displays Battery-Backup-Unit-related alert information.

Cluster Configuration

To access the Configure Cluster window:

1. Click the **Inventory** icon in the menu bar.
2. In the Inventory menu bar, click **Logical View**.
3. In the Inventory List tab, click **Clusters**.
4. Click a cluster to select it and click **Configure Cluster** in the menu bar (you can also right-click a cluster on the list and select **Configure Cluster** from the drop-down menu).

The Configure Cluster window includes the following tabs:

- ◆ Encryption
- ◆ VAAI TP Limit
- ◆ iSCSI Security Configuration
- ◆ iSCSI Network Configuration
- ◆ iSCSI Ports Configuration
- ◆ ODX Mode Configuration

Encryption Tab

Figure 62 shows the Encryption tab of the Configure Cluster window.

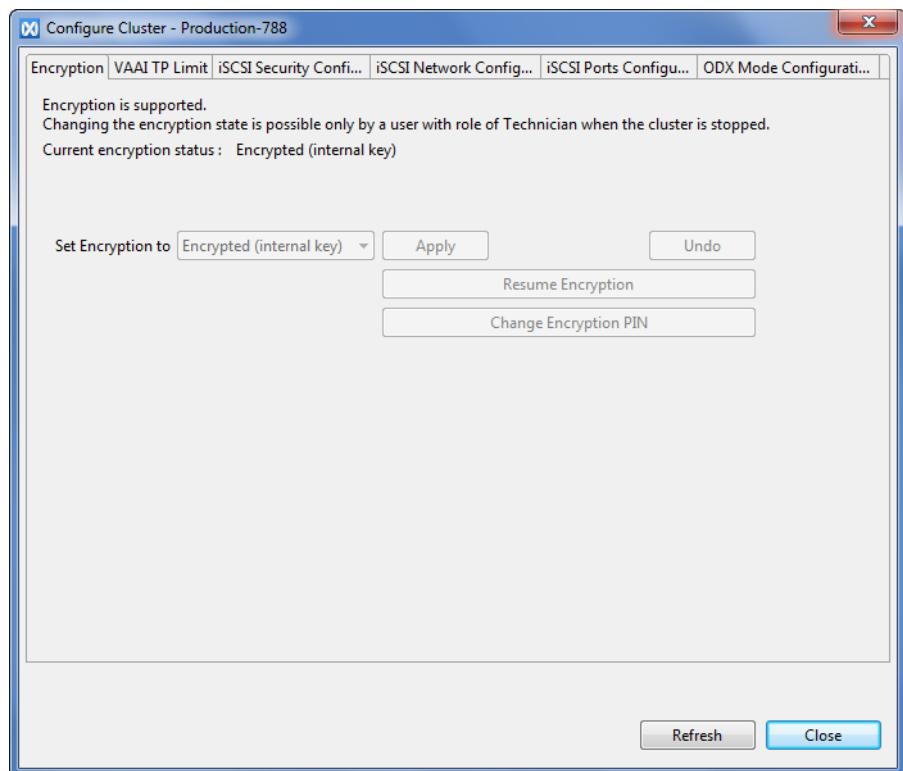


Figure 62 Configure Cluster - Encryption Tab

VAAI TP Limit Tab

[Figure 62](#) shows the VAAI TP Limit tab of the Configure Cluster window.

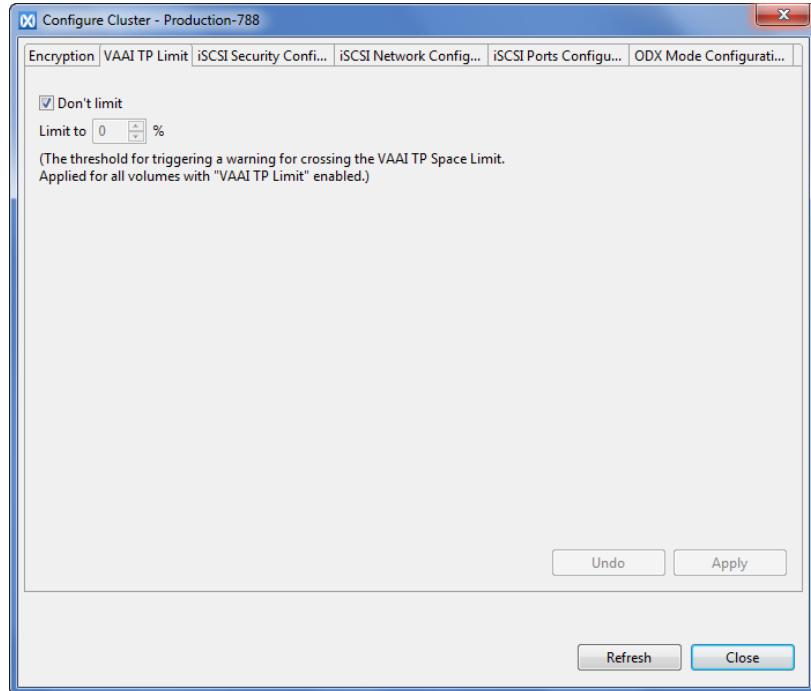


Figure 63 Configure Cluster - VAAI TP Limit Tab

iSCSI Security Configuration Tab

[Figure 62](#) shows the iSCSI Security Configuration tab of the Configure Cluster window.

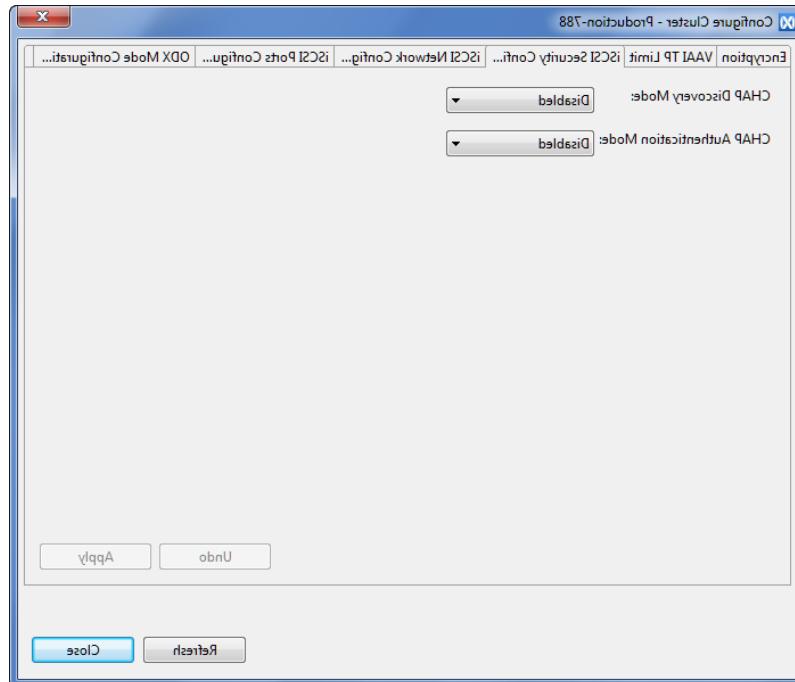


Figure 64 Configure Cluster - iSCSI Security Configuration Tab

iSCSI Network Configuration Tab

Figure 65 shows the iSCSI Network Configuration tab of the Configure Cluster window.

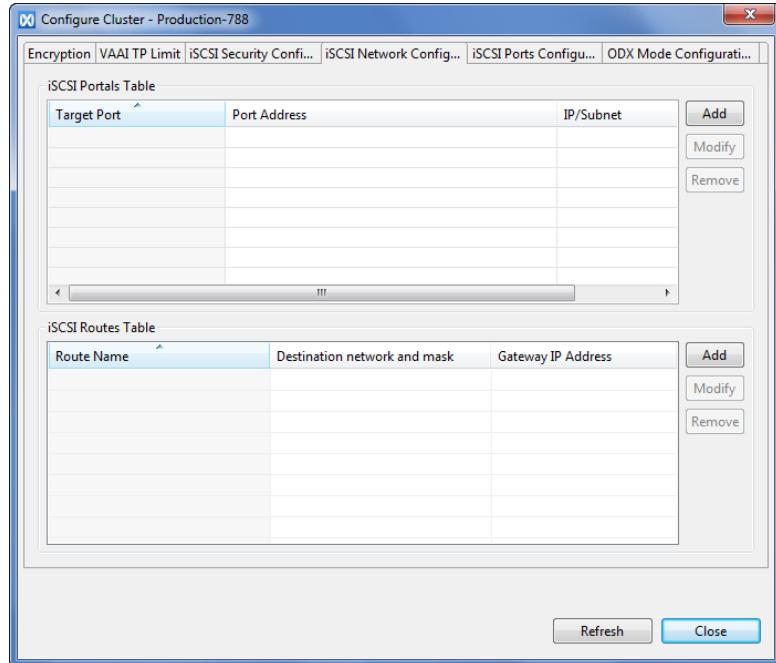


Figure 65 Configure Cluster - iSCSI Network Configuration Tab

iSCSI Ports Configuration Tab

Figure 66 shows the iSCSI Ports Configuration tab of the Configure Cluster window.

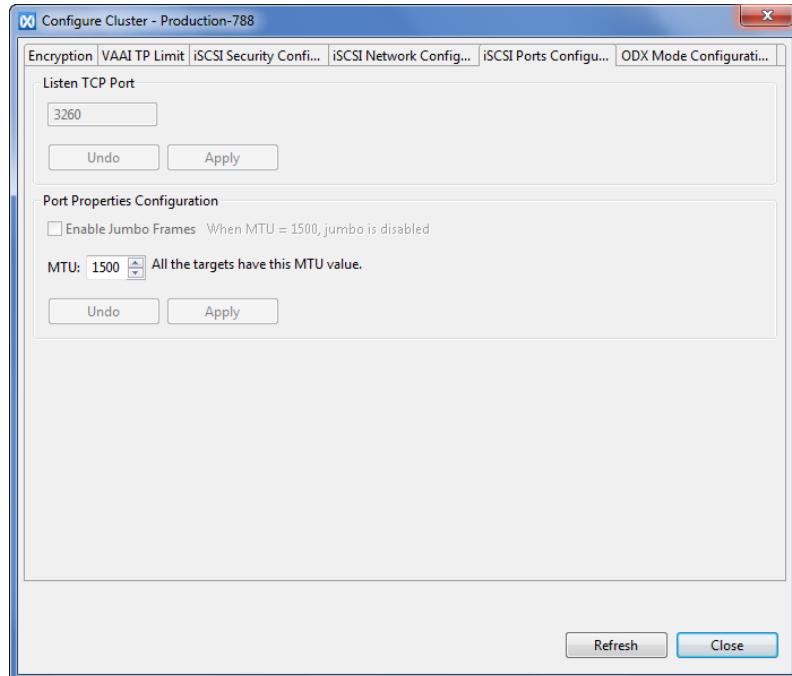


Figure 66 Configure Cluster - iSCSI Ports Configuration Tab

ODX Mode Configuration Tab

Figure 67 shows the ODX Mode Configuration tab of the Configure Cluster window.

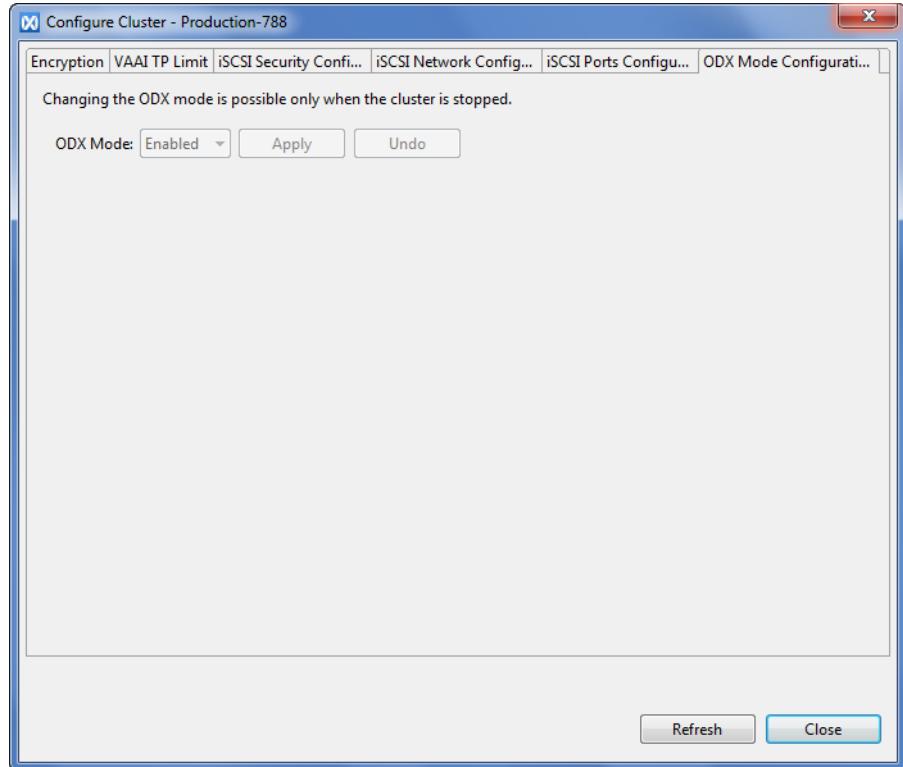


Figure 67 Configure Cluster - ODX Mode Configuration Tab

Alerts & Events Workspace

Figure 68 shows the Alerts & Events workspace (with the Alerts tab selected).

To access the Alerts & Events workspace, click the **Alerts & Events** icon in the menu bar.

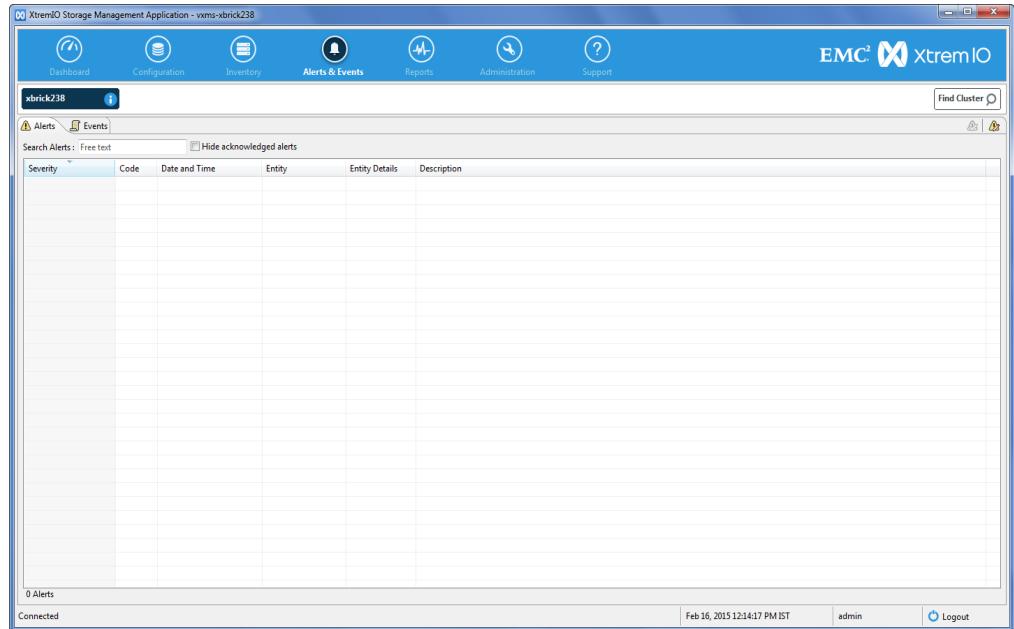


Figure 68 Alerts Tab in Alerts & Events Workspace

Alerts Tab

Figure 69 shows the main elements and icons of the Alerts tab in the Alerts & Events workspace.

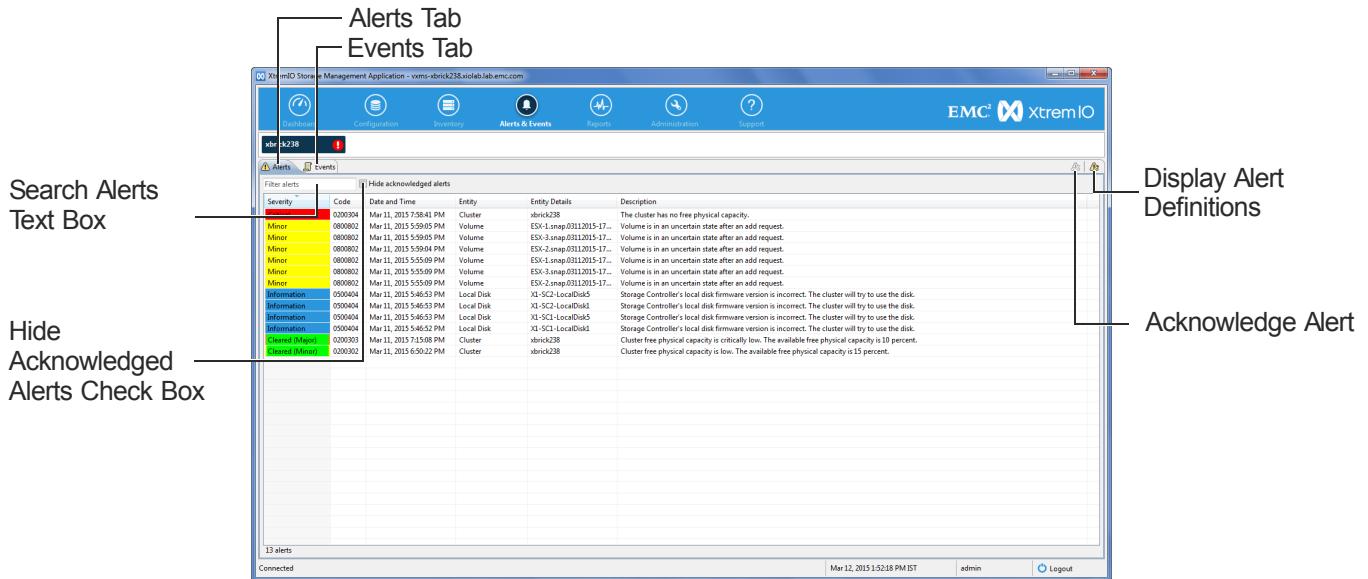


Figure 69 Main Elements and Icons of the Alerts Tab

Table 30 describes the Alerts tab elements and icons.

Table 30 Alerts Tab Elements and Icons

Icon	Description
	Search Alerts Text Box Enables you to narrow down the alerts display by typing a search string. The cluster displays only alerts that match the search string.
<input type="checkbox"/>	Hide Acknowledged Alerts Enables you to remove the acknowledged alerts from the display.
	Display Alert Definitions Displays Alert Definitions.
	Acknowledge Alert Acknowledges the selected alert.

The Alerts pane displays the managed cluster alerts, which are color coded according to severity:

- ◆ Green - Cleared alert
- ◆ Blue - Information alert
- ◆ Yellow - Minor alert
- ◆ Orange - Major alert
- ◆ Red - Critical alert

For each alert, the following details are listed:

- ◆ Severity
- ◆ Code
- ◆ Date and Time
- ◆ Entity
- ◆ Entity Details
- ◆ Description

You can sort the displayed alerts by each of these column headings.

To sort the alerts by a column heading, click the heading. The arrow, displayed above the selected heading, indicates whether the sorting is in ascending or descending order.

Right-clicking the Alerts pane displays the Alerts drop-down menu, as shown in [Figure 70](#)

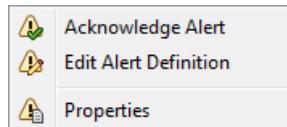


Figure 70 Alerts Pane Right-Click Drop-Down Menu

[Table 31](#) describes the drop-down menu's active options.

Table 31 Alerts Pane Drop-Down Menu Options

Icon	Description
Acknowledge Alert	Acknowledge Alert Acknowledges the selected alert.
Edit Alert Definition	Edit Alert Definition Enables you to change the selected alert's definition.
Properties	Properties Displays the selected alert's properties.

Events Tab

Figure 71 shows the Events tab in the Alerts & Events Workspace.

Figure 71 Events Tab

The Events tab consists of the following sections:

- ◆ Filters - Includes the filters you can use to determine which events are displayed.
- ◆ Events Display - Displays the constantly-updated events list.
- ◆ Display Info - Shows the currently-displayed page number. You can browse the events list by selecting a different page number or clicking **Next** and **Previous** to move forward and backward, respectively, through the list.

The Events Display pane shows the cluster's current events, which are color coded according to severity:

- ◆ Blue - Information event
- ◆ Yellow - Minor event
- ◆ Orange - Major event
- ◆ Red - Critical event

[Table 32](#) describes the parameters that are provided for each event.

Table 32 Event Parameters

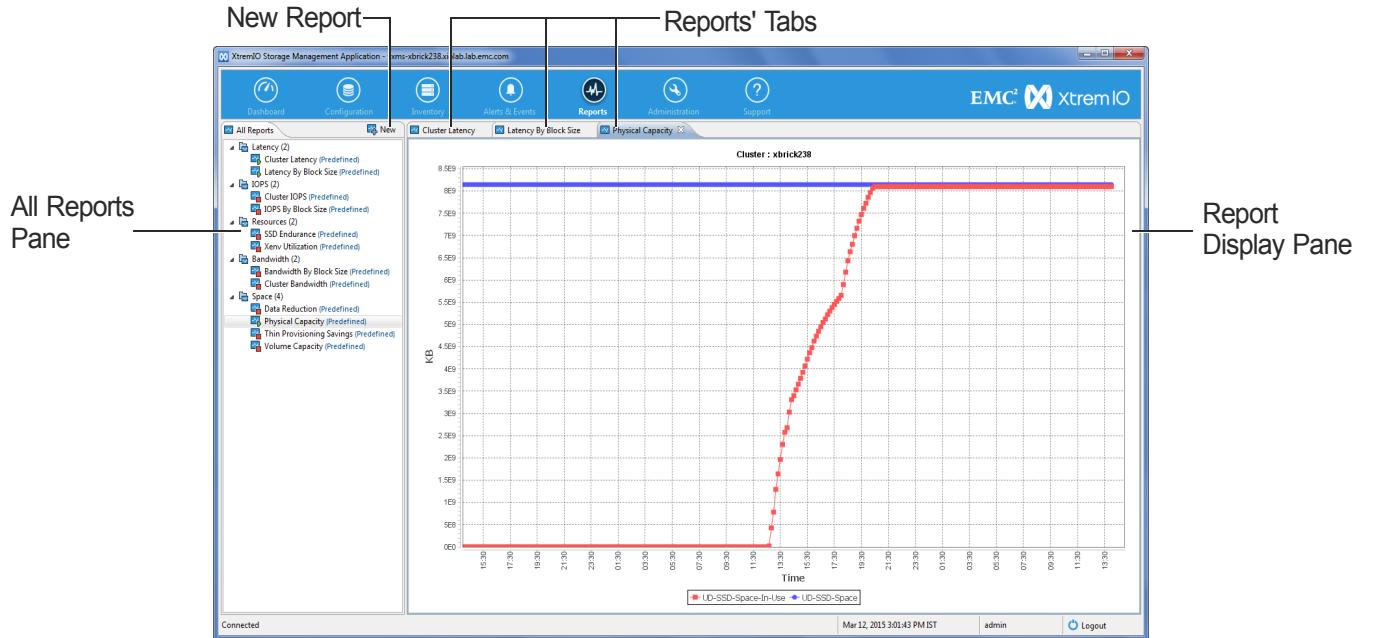
Event Parameter	Description
Severity	Displays the event's severity level both literally and by the assigned color.
Event Code	Specifies the event's unique code.
Date and Time	Indicates the date and time stamp of the event's occurrence.
Category	Specifies the event's category (Software, Audit Log, Security, Life Cycle, Hardware, Activity, State Change).
Entity	Specifies the entity to which the event refers.
Entity Details	Specifies the details of the event-related entity.
Description	Displays the event's detailed description.

You can sort the displayed events by each of these column headings. To sort the events by a column heading, click the heading. The arrow, displayed above each heading, indicates whether the sorting is in ascending or descending order.

Reports Workspace

[Figure 72](#) shows the Reports workspace and its main elements and icons.

To access the Reports workspace, click the **Reports** icon in the menu bar.



[Figure 72](#) Reports Workspace

[Table 33](#) describes the icons in the Reports workspace.

[Table 33](#) Reports Workspace Icons

Icon	Description
	New Report Enables you to add a new report.

Table 34 describes the active options of the drop-down menu, which appear upon right-clicking an item in the Reports workspace.

Table 34 Reports Workspace Drop-Down Menu Options

Icon	Description
Modify	Edit Report Enables you to modify the defined reports' properties.
Export Report Data	Export Report Data Enables you to export the selected report's data to a file.
Run	Open Report Opens the selected report and displays it in the main window (appears interchangeably with Close Report according to report's current state).
Stop And Close	Close Report Closes the selected report's display (appears interchangeably with Open Report according to the report's current state).
Delete	Delete Report Removes the defined report from the reports' list.
Copy	Copy Report Enables you to copy a report as a base for a new report.

Administration Workspace

Figure 73 shows the Administration workspace.

To access the Administration workspace, click the **Administration** icon in the menu bar.

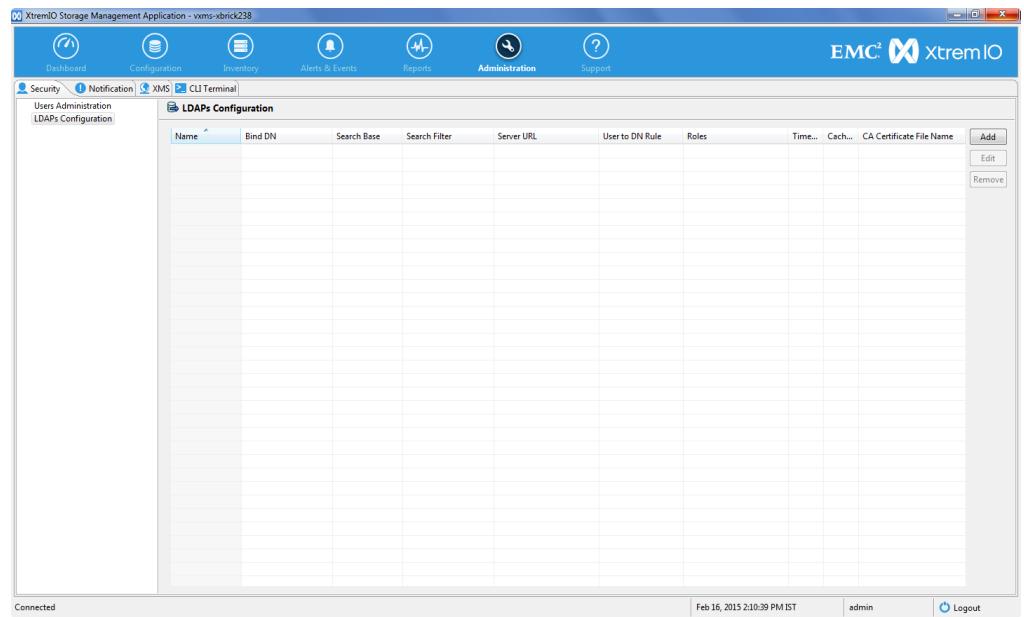


Figure 73 Administration Workspace (with Security Tab Selected)

When you select a tab in the Administration workspace, the available screens for that tab are displayed in the left pane. The Administration workspace consists of the following tabs:

- ◆ Security - The Security tab includes the following screens:
 - Users Administration
 - LDAP Configuration
- ◆ Notification - The Notification tab includes the following screens:
 - Email Configuration
 - SNMP Configuration
 - Syslog Configuration
- ◆ XMS - The XMS tab includes the following screens:
 - XMS Configuration
 - XMS Customization
- ◆ CLI Terminal

Upon selecting a tab, the tab's options are displayed in the left pane. When you select one of the options, the corresponding screen appears in the main pane of the Administration workspace.

Security Tab

Users Administration

Figure 74 shows the Users Administration screen.

To access the Users Administration screen, select the **Security** tab in the Administration workspace and then select the **Users Administration** option from the left pane of the Security tab.

User Name	Role	Is External	Timeout (min)	Public Key	
admin	Administrator	No	No timeout		Add
odx_user	Administrator	No	10		Edit
rp_user	Administrator	No	10		Remove

Log in as a different user...

Figure 74 Users Administration Screen

The Users Administration screen displays the defined users' list. For each user, the following details are listed:

- ◆ User Name
- ◆ Role
- ◆ Is External
- ◆ Timeout (in minutes)
- ◆ Public Key - for remote users

You can sort the displayed users by each of these column headings. To sort the users by a column heading, click the heading. The arrow, displayed above each heading, indicates whether the sorting is in ascending or descending order.

In the Users Administration screen you can:

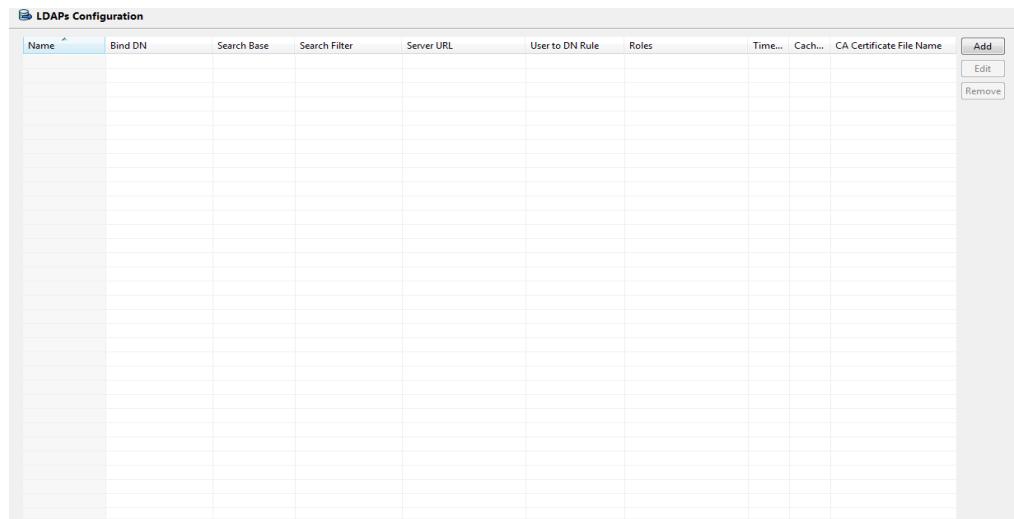
- ◆ With Admin role:
 - Add a user.
 - Edit user data.
 - Remove a user.
 - Log in as a different user.
- ◆ With Configuration or Read-Only roles:
 - Change your password.
 - Log in as a different user.

Note: A user with Configuration or Read-Only role cannot see other users in the cluster.

LDAP Configuration

[Figure 75](#) shows the LDAP Configuration screen.

To access the LDAP Configuration screen, select the **Security** tab in the Administration workspace and then select the **LDAP Configuration** option from the left pane of the Security tab.



[Figure 75](#) LDAP Configuration Screen

The LDAP Configuration screen displays the LDAP server configuration data, including the following details:

- ◆ LDAP profile Name
- ◆ Bind DN
- ◆ Search base
- ◆ Search filter
- ◆ Server URL
- ◆ User to DN rule
- ◆ Roles
- ◆ Timeout (in msec)
- ◆ Cache Expire (in hours)
- ◆ CA certificate file name

Using the LDAP Configuration screen, you can:

- ◆ Modify LDAP configuration profiles.
- ◆ Add and remove server URLs.
- ◆ Add, update and remove XMS role to Active Directory group mapping rules.

Notification Tab

Email Configuration

Figure 76 shows the Email Configuration screen.

To access the Email Configuration screen, select the **Email Configuration** option from the left pane of the Administration workspace.

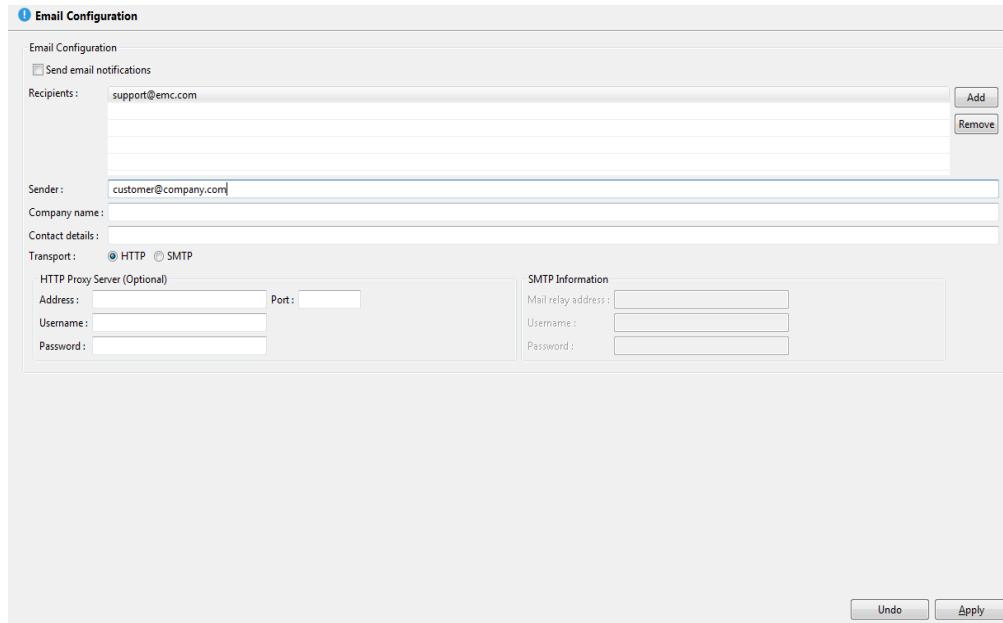


Figure 76 Email Configuration Screen

The Email Configuration screen displays email-related data. Sending email notifications allows the system administrators to remotely monitor the cluster.

The Email Configuration window enables you to:

- ◆ Select sending email notification and set the frequency.
- ◆ Add and remove mail recipients from the list.
- ◆ Configure email sender's properties.
- ◆ Determine the mail sending mechanism.

SNMP Configuration

Figure 77 shows the SNMP Configuration screen.

To access the SNMP Configuration screen, select the **SNMP Configuration** option from the left pane of the Administration workspace.

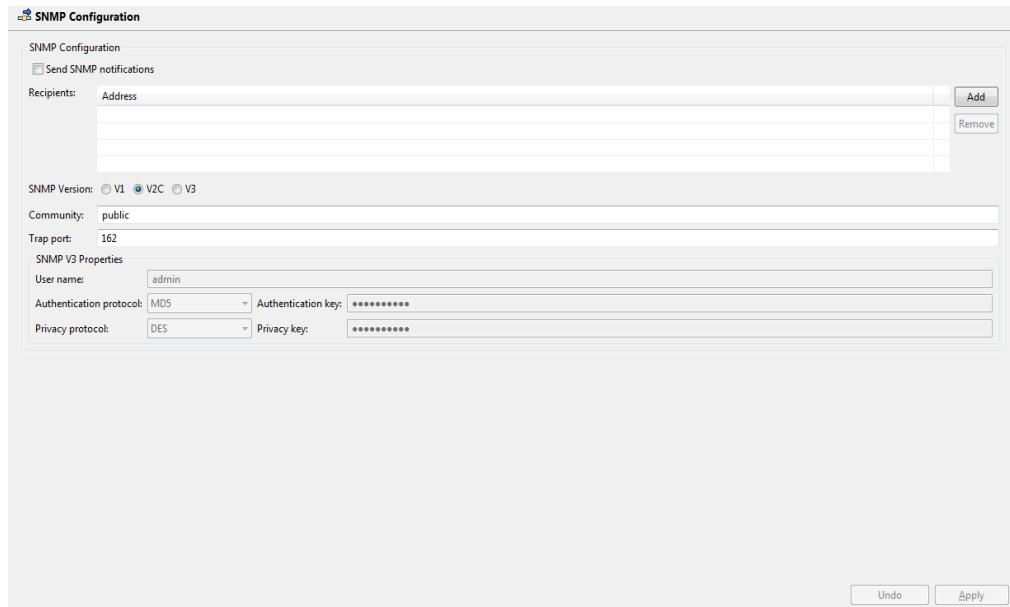


Figure 77 SNMP Configuration Screen

The SNMP Configuration screen enables you to send SNMP notification and configure the following SNMP notification configuration data:

- ◆ SNMP notification recipients list
- ◆ SNMP Version
- ◆ Community
- ◆ Trap Port
- ◆ SNMP V3 Properties

Syslog Configuration

Figure 78 shows the Syslog Configuration screen.

To access the Syslog Configuration screen, select the **Syslog Configuration** option from the left pane of the Administration workspace.

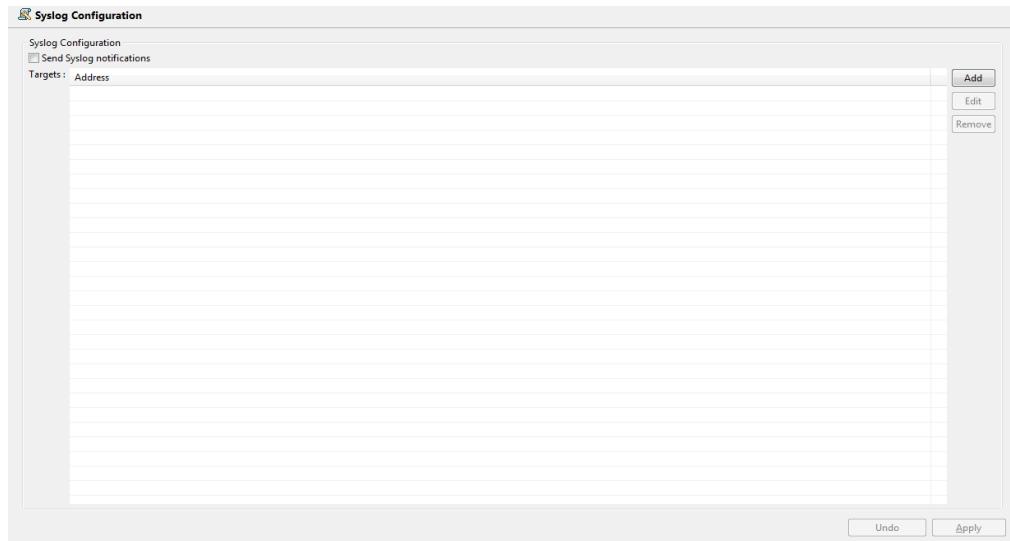


Figure 78 Syslog Configuration Screen

The Syslog Configuration screen lists the IP addresses or names of the Syslog servers, currently configured on the XMS, and enables you to send Syslog notifications.

Using the Syslog Configuration screen you can:

- ◆ Activate/Deactivate sending Syslog notifications.
- ◆ Update the Syslog servers list, by adding and removing servers.

XMS Tab

XMS Configuration

Figure 79 shows the XMS Configuration screen.

To access the XMS Configuration screen, select the **XMS** tab and then select the **XMS Configuration** option in the left pane of the XMS tab.

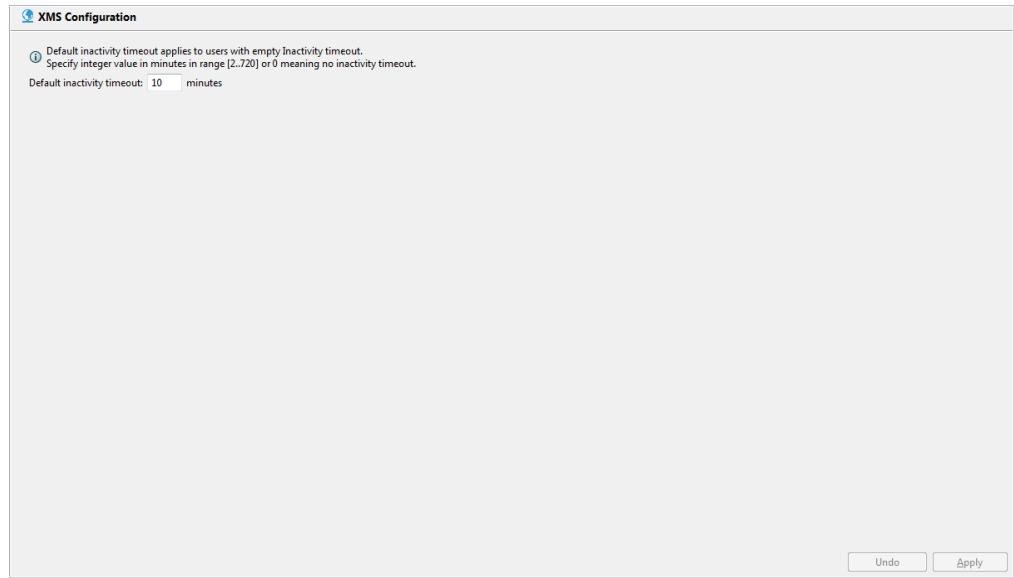


Figure 79 XMS Configuration Screen

The XMS Configuration screen enables you to set the XMS inactivity timeout.

XMS Customization

Figure 80 shows the XMS Customization screen.

To access the XMS Customization screen, select the **XMS** tab and then select the **XMS Customization** option in the left pane of the XMS tab.

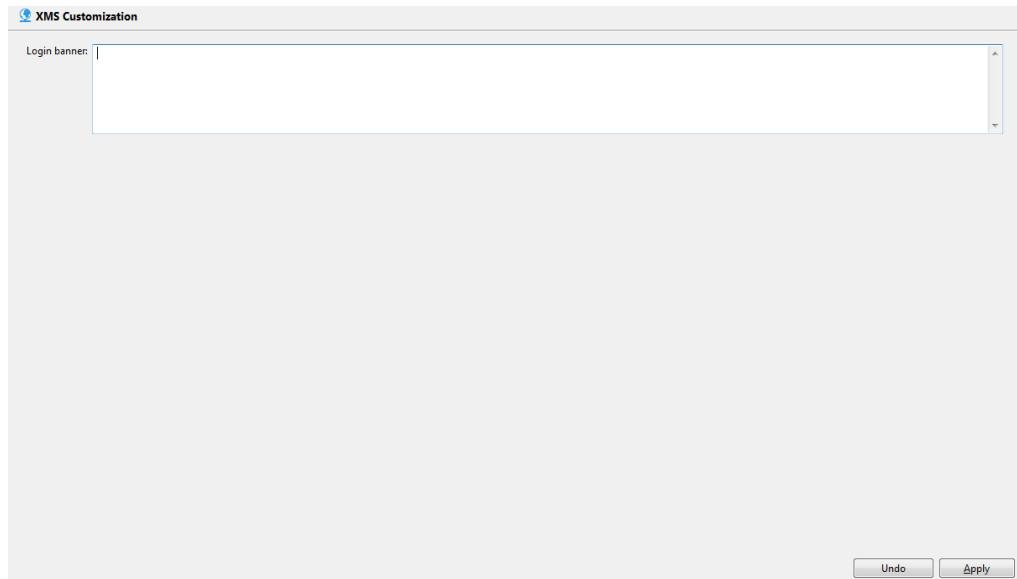


Figure 80 XMS Customization Screen

The XMS Customization screen enables you to set the login banner text.

CLI Terminal Tab

[Figure 81](#) shows the CLI Terminal screen.

To access the CLI Terminal screen, select the **CLI Terminal** tab in the Administration workspace.

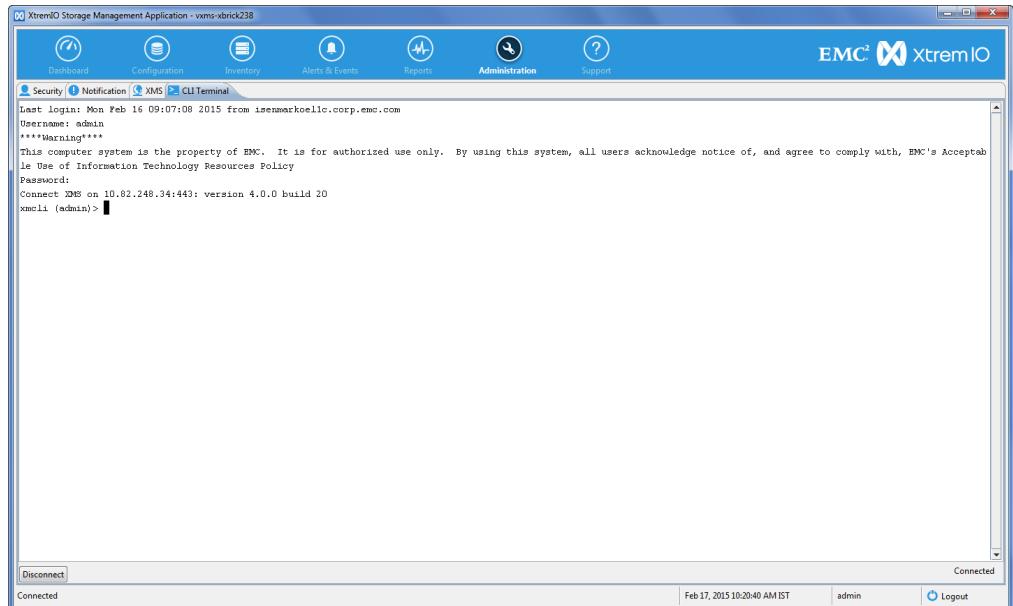


Figure 81 CLI Terminal Screen

The CLI Terminal screen enables you to use the command line interface and run CLI commands according to your user's role.

In the CLI Terminal, you can:

- ◆ Copy the displayed text by selecting the text.
- ◆ Paste the copied text into the command line by right-clicking the screen.
- ◆ Use the scroll bar to scroll the screen up/down.

Support Window

[Figure 82](#) shows the Support window.

To access the Support window, click the **Support** icon in the menu bar.

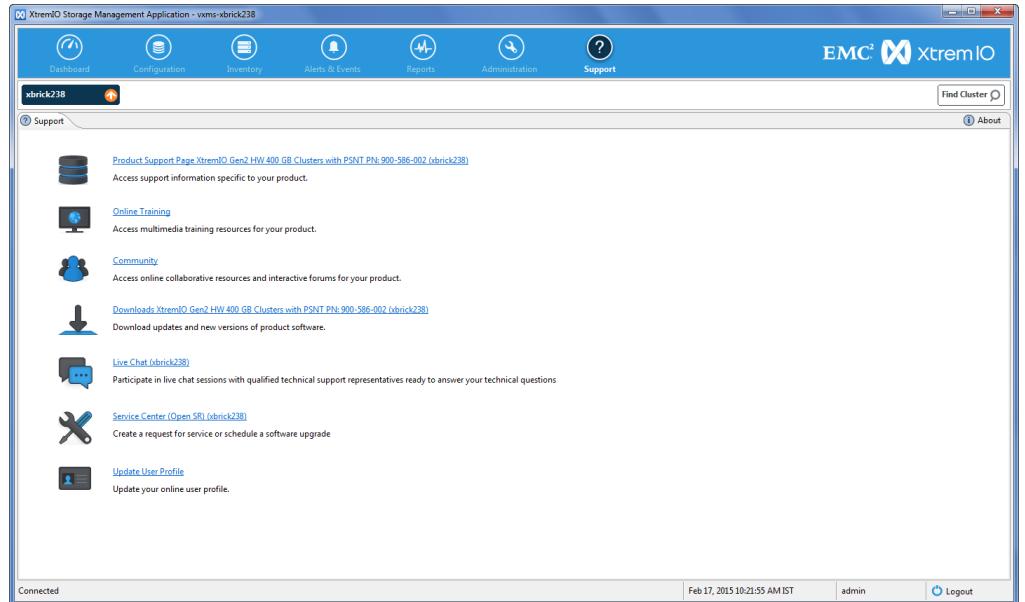


Figure 82 Support Window

The Support window provides the following options:

- ◆ Product Support page
- ◆ Online training
- ◆ Community
- ◆ Downloads
- ◆ Live chat
- ◆ Service center
- ◆ Update user profile

About Window

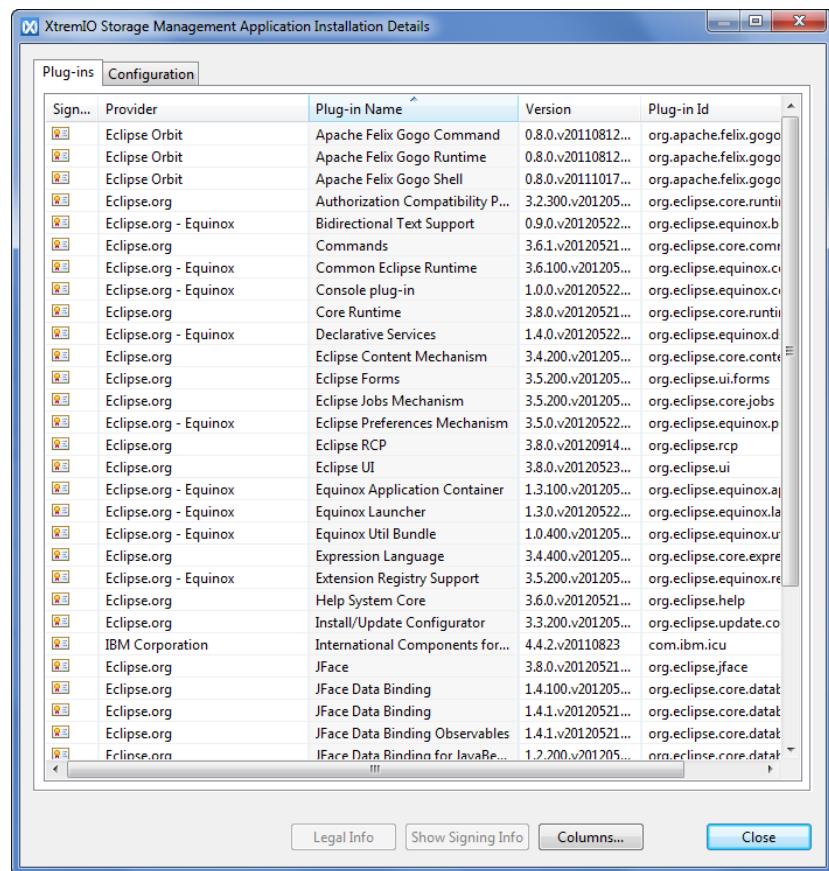
Figure [Figure 83](#) shows the About window.



Figure 83 About Window

The About window provides the following information:

- ◆ Product name
- ◆ Copyright statement
- ◆ System version and Build numbers
- ◆ Build ID
- ◆ Company's website URL
- ◆ Service request contact information
- ◆ Installation details (Clicking the **Installation Details** icon displays the Installation Details window, as shown in [Figure 84](#).)

**Figure 84** Installation Details Window

CHAPTER 3

Managing the Hardware

This chapter includes the following topics:

- ◆ [Managing Hardware Tags](#) 116
- ◆ [Hardware Components' LEDs](#) 121

Managing Hardware Tags

XtremIO Storage Array provides users with a tagging system for marking cluster hardware elements. Tagging elements enables users to logically group, locate and manage multiple entities and provides a clearer view of hardware elements affiliation.

Each object can have multiple Tags to reflect the object's function and position. Using Tag nesting, you can create a hierarchy that reflects the relationship between the cluster objects.

You can use tagging to aggregate objects, based on functional or business requirements.

Tags can be managed via the GUI and the CLI.

Managing Tags, Using the GUI

Creating Tags

You can create Tags for the following hardware elements:

- Clusters
- X-Bricks
- Data Protection Groups
- Storage Controllers
- DAEs
- SSDs
- Battery Backup Units
- Targets

To create Tags for cluster's hardware elements:

1. In the menu bar, click **Inventory**.
2. In the Inventory List (left pane), click the **Manage Tags** icon.

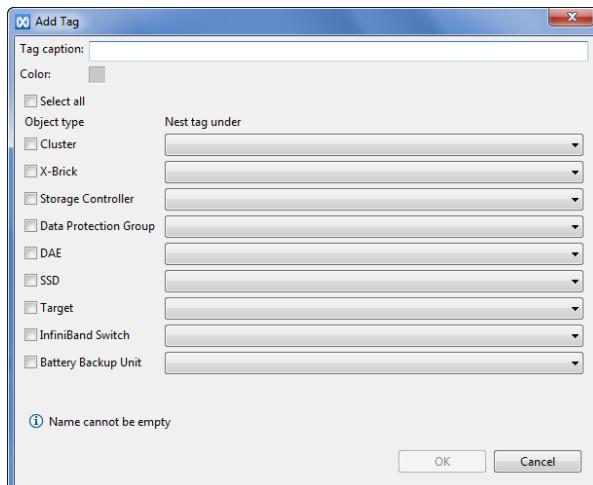


Figure 85 Add Tag - Inventory

3. Type a meaningful name in the Tag Caption field.

Note: A Tag name can have up to 64 characters. The following characters are allowed: alphanumeric symbols, space, ~ ! @ # \$ % ^ & * _ + { } | : < > ? / . -

4. Select a color for the Tag. You can select a different color for each object type by clicking the **Color** (gray square) to open the color palette, and clicking a color. If you want to select the same color to all object types, click **Set color to all**.
5. Select the object types you wish to assign the new Tag to. If you want to select all objects, click **Select All**.
6. Click **OK**; the new Tag is added to the selected object types.

Note: The created Tag is not assigned to specific objects. To assign the Tag to objects, see [“Assigning Tags to Hardware Elements” on page 118](#).

Assigning Tags to Hardware Elements

To assign a Tag to a hardware element:

1. In the menu bar, click **Inventory**.
2. In the Inventory List (left pane), click the object type you wish to Tag, to display the defined objects in the main window.
3. Right-click an object from the list in the main window and select **Manage Tags**. You can select multiple objects from the list, using the Ctrl and Shift keys.

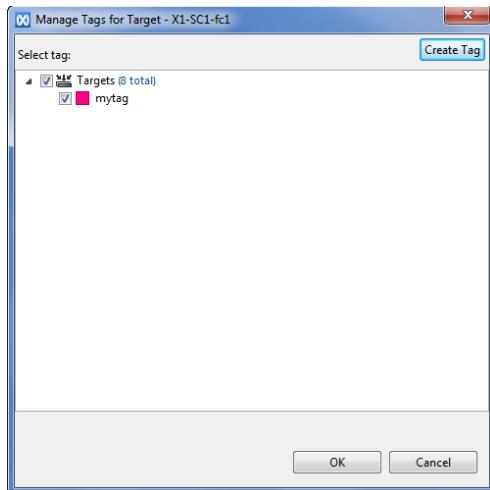


Figure 86 Assigning Tags to Physical Objects

The Manage Tags for <object type> window displays the object type and all the Tags that were defined for it.

Note: In case of multiple objects, the window is titled Manage Tags for <number of objects>.

4. Select the Tags you want to assign to the object and click **OK**.

Note: Another way to assign a Tag is to drag and drop the object you want to tag from the main window to the Tag that is located below the object type in the Inventory List tab.

Editing Tags

To edit Tags for hardware elements:

1. In the menu bar, click **Inventory**.
2. In the Inventory List (left pane), double-click the relevant object type to open the list of Tags defined for that object type.
3. Right-click the Tag you wish to modify and select **Modify Tag** from the drop-down list.

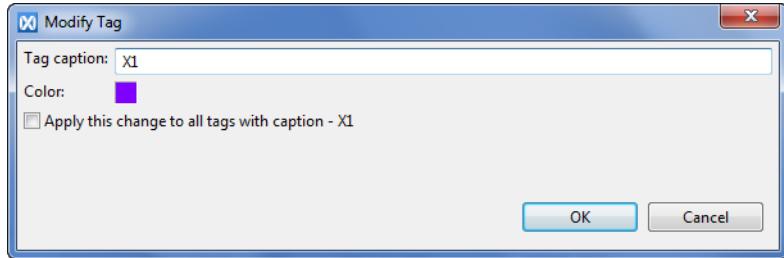


Figure 87 Modify Tag

In the Modify Tag dialog box you can edit the following parameters:

- Tag caption
- Tag color

If you wish to apply the changes to all Tags defined with the same caption, select that option.

4. Click **OK**.

Removing Tags

To remove a hardware element Tag:

1. In the menu bar, click **Inventory**.
2. In the Inventory List (left pane), double-click the relevant object type to open the list of Tags defined for that object type.
3. Right-click the Tag you wish to remove and select **Delete Tag** from the drop-down list.
4. Click **Yes** to confirm; the Tag is deleted from the object type Tag list.

Managing Tags, Using the CLI

Use the following CLI commands for managing Tags:

Command	Description
show-tags	Displays the details of all defined Tags.
show-tag	Displays the details of a specified Tag.
create-tag	Creates a Tag for an entity.
tag-object	Assigns a Tag to a specified object.
untag-object	Removes a Tag from a specified object.
modify-tag	Modifies a specified Tag caption.
remove-tag	Deletes a Tag from the Tags list.

Hardware Components' LEDs

The XtremIO Storage Array hardware components are equipped with two LED types that enable you to monitor the components' health:

- ◆ Identification LED - Used to identify a component in the cluster.
- ◆ Status LED - Used to indicate the status of the component.

In addition to the actual LEDs on the physical hardware components, identical graphical representation of all LEDs appear in the GUI's hardware image.

The possible states of the LEDs are:

- ◆ Off
- ◆ On (beacon)

[Table 35](#) provides details of the hardware components' LEDs.

Table 35 Hardware Components' LEDs

Component	Identification LED		Status LED	
	GUI	Physical	GUI	Physical
Storage Controller	Yes	Yes	Yes	Yes
Storage Controller SSD	Yes	Yes	Yes	Yes
Storage Controller HDD	Yes	Yes	Yes	Yes
Storage Controller PSU	No	No	Yes	Yes
DAE	Yes	Yes	Yes	Yes
DAE SSD	Yes	Yes	Yes	Yes
DAE Controller	Yes	Yes	Yes	Yes
InfiniBand Switch	No	No	No	Yes
InfiniBand Switch Power supply	No	No	No	Yes
InfiniBand Switch Fan	No	No	No	Yes
Battery Backup Unit	No	No	No	No
Physical XMS	N/A	Yes	N/A	No
Virtual XMS	N/A	No	N/A	No

Using the Identification LEDs

You can identify a component in the cluster, using the following methods:

- ◆ Turning on the component's identification LED
- ◆ Turning on the LEDs of all other components (all but the selected component), if the component has failed and does not respond

To turn on a component's identification LED:

1. In the dashboard menu bar, click the **Inventory** icon.
2. Hover the mouse pointer over the relevant hardware component and right-click to open the drop-down menu.
3. Select **Turn On Identification LED for <component's name>**; a message appears, stating that the component's LED will be turned On/Off.
4. Click **OK**.

Note: If the component's identification LED is already turned on, a check sign appears next to the **Turn On Identification LED** option and the message box that follows states that the LED will be turned **off**.

To turn all other identification LEDs on or off:

1. In the dashboard menu bar, click the **Hardware** icon.
2. Hover the mouse pointer over the relevant hardware component and right-click to open the drop-down menu.
3. Select **Change all other <component type> Identification LEDs**.



4. In the Change All Other Identification LEDs dialog box, select the desired state of the LEDs (On or Off) and click **OK**; LEDs of all components, except for the LED of the component you want to identify, change their state.

CHAPTER 4

Monitoring the Cluster

This chapter includes the following topics:

◆ Monitoring the Storage	124
◆ Monitoring the Performance	126
◆ Monitoring the Hardware Elements	127
◆ Monitoring the Storage Elements	139
◆ Monitoring the Alerts	150
◆ Managing the Reports	151

Monitoring the Storage

To monitor the cluster storage status:

1. From the menu bar, click the **Dashboard** icon to display the Dashboard workspace, as shown in [Figure 17 on page 45](#).
2. Monitor the storage parameters in the Storage pane, as shown in [Figure 18 on page 46](#).

Monitoring the Efficiency

You can monitor the cluster efficiency status from the Efficiency section of the Storage pane in the Dashboard workspace.



Figure 88 Overall Efficiency Section

The Efficiency section displays the following data:

- ◆ Overall Efficiency - the disk space saved by the XtremIO Storage Array, calculated as:

$$\frac{\text{Volume capacity}}{\text{Physical space used}}$$

- ◆ Data Reduction Ratio - the inline data Deduplication and Compression ratio, calculated as:

$$\frac{\text{Logical space in use}}{\text{Physical space used}}$$

- ◆ Deduplication Ratio - the real-time Inline Data Deduplication ratio, calculated as:

$$\frac{\text{Logical space in use}}{\text{Unique data on SSD}}$$

- ◆ Compression Ratio - the real-time Inline Compression ratio, calculated as:

$$\frac{\text{Unique data on SSD}}{\text{Physical space used}}$$

- ◆ Thin Provisioning Savings - used disk space compared to allocated disk space

Monitoring the Volume Capacity

You can monitor the Volume capacity status in the Volume Capacity section of the Storage pane in the Dashboard workspace.

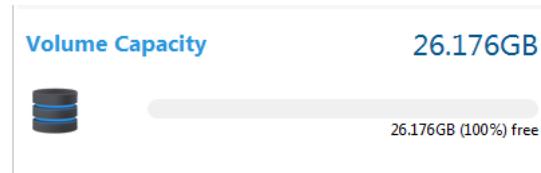


Figure 89 Volume Capacity Section

The Volume capacity section displays the following data:

- ◆ Total disk space defined by the Volumes
- ◆ Physical space used
- ◆ Logical space used

Hovering the mouse pointer over the Volume Capacity bar displays a tool-tip with detailed information.

Monitoring the Physical Capacity

You can monitor the physical capacity status from the Physical Capacity section of the Storage pane in the Dashboard workspace.



Figure 90 Physical Capacity Section

The Physical Capacity section displays the following data:

- ◆ Total physical capacity
- ◆ Used physical capacity

Hovering the mouse pointer over the Physical capacity bar displays a tool-tip with detailed information.

Monitoring the Performance

Monitoring the Performance, Using the GUI

To monitor the cluster performance, using the GUI:

1. From the menu bar, click the **Dashboard** icon to display the Dashboard workspace, as shown in [Figure 17 on page 45](#).
2. In the Performance pane (see [Figure 19 on page 47](#)), select the desired parameters:
 - Select the measurement unit of the display by clicking one of the following tabs:
 - Bandwidth - MB per second (MB/s)
 - IOPS - Input/Out operations per second
 - Latency - microseconds (μ s) - applies only to the activity history graph.
 - Select the desired item to be monitored from the Item Selector:
 - Block Size
 - Initiator Groups
 - Volumes
 - Set the Activity History time frame by selecting from one of the following periods from the Time Period Selector:
 - Last Hour
 - Last six Hours
 - Last 24 Hours
 - Last 3 Days
 - Last Week

The Activity History time frame starting point is the last time the XMS was started.

You can zoom in on the displayed history graph to view a more detailed display of a selected time period (i.e. more time points are displayed for the selected period).

To zoom in and out on the history graph:

1. Drag the mouse over the desired section in the history graph to select it.

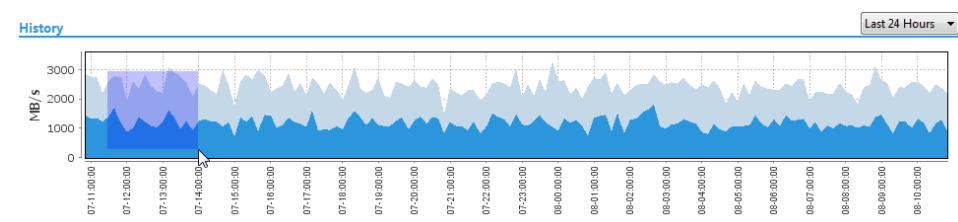


Figure 91 History Graph - Zoom-In

The highlighted section is displayed in a Zoomed view.

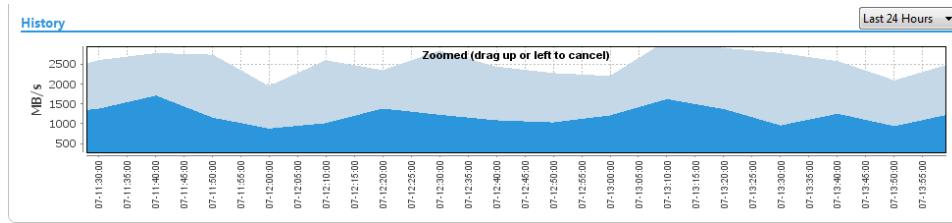


Figure 92 History Graph - Zoomed View

2. Repeat step 1 to zoom again on a selected section of the zoomed area.
3. Drag the mouse up or left to return to the regular graph view.

Note: Zooming in on the history graph displays the aggregated information in higher resolution. It does not increase the amount of aggregated information. To change the amount of aggregated data, select a different time frame from the drop-down menu.

For more information, see “[Performance Pane](#)” on page 47.

Monitoring Performance, Using the CLI

Use the following CLI commands for monitoring cluster’s performance:

Command	Description
show-most-active	Displays the most active Volumes and Initiator Groups.
show-most-active-initiator-groups	Displays performance data of the most active Initiator Groups.
show-most-active-volumes	Displays performance data of the most active Volumes.

Monitoring the Hardware Elements

Monitoring the Clusters

Monitoring Clusters, Using the GUI

You can quickly view the cluster’s general information by hovering the mouse pointer over the cluster in the Rack pane of the Inventory workspace.



Figure 93 Cluster Tool-Tip

The following information is displayed:

- ◆ Cluster name
- ◆ PSNT serial number
- ◆ Number of X-Bricks
- ◆ Overall cluster state
- ◆ Encryption status
- ◆ Severity

You can also monitor the cluster via the status bar of the GUI window.

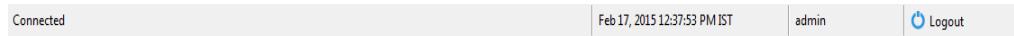


Figure 94 GUI Window - Status Bar

The status bar displays the following data:

- ◆ The cluster status
- ◆ XMS and clusters date and time zone
- ◆ Current logged-in user

Note: To view a summary of the existing clusters data, click **Logical View** in the Inventory workspace menu bar and then click **Clusters** in the Hardware tab. For details, see “[Clusters View](#)” on page 74

Monitoring Clusters, Using the CLI

Use the following CLI commands for monitoring clusters:

Command	Description
show-clusters	Displays the connected clusters' information.
show-clusters-info	Displays the connected clusters' information.
show-clusters-upgrade	Displays the clusters' upgrade status.
show-clusters-performance	Displays clusters' performance data.
show-clusters-performance-small	Displays clusters' performance data for small (under 4KB) blocks.
show-clusters-performance-unaligned	Displays clusters' performance data for unaligned blocks.
show-clusters-performance-latency	Displays clusters' performance latency data.
show-clusters-savings	Displays connected clusters iSCSI TCP port numbers.
show-clusters-savings	Displays savings parameters of the selected cluster.
show-clusters-thresholds	Displays thin provisioning soft limits for connected clusters.
show-clusters-data-protection-properties	Displays clusters' data protection properties.

Monitoring the X-Bricks

Monitoring the X-Bricks, Using the GUI

To view the X-Bricks information:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 37 on page 67](#).
2. Click **Graphical View** to display the graphical view of the cluster.
3. In the left pane, select the X-Brick whose Storage Controller you wish to monitor; the graphic view of the selected X-Brick is displayed in the main window.
4. The following actions enable you to view the displayed X-Brick's details in the main window:
 - Hovering the mouse pointer over different parts of the component to view the component's parameters and associated alerts
 - Clicking **Show Front** to view the X-Brick's front side
 - Clicking **Show Back** to view the X-Brick's back side
 - Clicking **Show Cable Connectivity** to view the X-Brick's cable connections
5. You can view the X-Brick's alerts by right-clicking the X-Brick and clicking **Display <X-Brick name> Alerts**

Note: To view a summary of X-Brick data, click **Logical View** in the Inventory workspace menu bar and then click **X-Bricks** in the Hardware tab. For more information, see [“X-Bricks View” on page 77](#).

Monitoring X-Bricks, Using the CLI

Use the following CLI command for monitoring X-Bricks:

Command	Description
show-bricks	Displays a list of X-Bricks and their associated cluster.
show-clusters	Displays connected clusters information.
show-storage-controllers	Displays the cluster's Storage Controllers information and status.
show-ssds	Displays a list of SSDs in the cluster and their properties.
show-bbus	Displays Battery Backup Units information.

Monitoring the Storage Controllers

Monitoring the Storage Controllers, Using the GUI

To view the Storage Controllers information:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 37 on page 67](#).
2. Click **Graphical View** to display the graphical view of the cluster.
3. In the left pane, select the X-Brick whose Storage Controller you wish to monitor.
4. Hover the mouse pointer over a Storage Controller graphic representation in the main window, to view the Storage Controller information.

You can view the Storage Controller's alerts by right-clicking the Storage Controller and clicking **Display <Storage Controller name> Alerts**.

Note: To view a summary of Storage Controller data, click **Logical View** in the Inventory workspace menu bar and then click **Storage Controllers** in the Hardware tab. For more information, see [“DAEs View” on page 82](#).

Monitoring the Storage Controllers, Using the CLI

Use the following CLI commands for monitoring storage controllers:

Command	Description
show-storage-controllers	Displays the cluster's Storage Controllers information and status.
show-storage-controllers-info	Displays the cluster's Storage Controllers information.
show-storage-controllers-fw-versions	Displays the Storage Controllers firmware version information.
show-storage-controllers-psus	Displays information on Storage Controllers power supply units.
show-storage-controllers-sensors	Displays a list of sensors and their related information.
test-xms-storage-controller-connectivity	Performs a connectivity check for a specified Storage Controller and its managing XMS.

Monitoring the SSDs

Monitoring the SSDs, Using the GUI

To view the SSDs information:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 37 on page 67](#).
2. Click **Graphical View** to display the graphical view of the cluster.
3. In the left pane, select the relevant X-Brick.
4. Hover the mouse pointer over an SSD graphic representation in the main window to view the SSD information.

You can view an SSD's alerts by right-clicking the SSD and clicking **Display <SSD name> Alerts**.

Note: To view a summary of SSDs data, click **Logical View** in the Inventory workspace menu bar and then click **SSDs** in the Hardware tab. For more information, see [“SSDs View” on page 84](#).

Monitoring the SSDs, Using the CLI

Use the following CLI commands for monitoring SSDs:

Command	Description
show-ssds	Displays a list of SSDs in the cluster and their properties.
show-ssds-performance	Displays the SSDs performance data.
show-slots	Displays a list of SSD slots and their properties.

Monitoring the InfiniBand Switches

Monitoring the InfiniBand Switches, Using the GUI

To view the InfiniBand Switches information:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 37 on page 67](#).
2. Click **Graphical View** to display the graphical view of the cluster.
3. In the left pane, select the relevant X-Brick.
4. Hover the mouse pointer over an InfiniBand Switch graphic representation in the main window to view the InfiniBand Switch information.

You can view an SSD's alerts by right-clicking the SSD and clicking **Display <SSD name> Alerts**.

Monitoring the InfiniBand Switches, Using the CLI

Use the following CLI commands for monitoring InfiniBand Switches:

Command	Description
show-infiniband-switches	displays InfiniBand Switches' information.
show-infiniband-switches-ports	Displays InfiniBand Switches' port information.
show-infiniband-switches-psus	Displays a InfiniBand Switches' PSU infomation.

Monitoring the Data Protection Groups

Data Protection Groups Overview

A Data Protection Group is a set of SSDs that form a redundancy group. Each Data Protection Group has a name, health state, and defined usable SSD space.

Each X-Brick contains one Data Protection Group, which is created during the initial configuration. The Data Protection Group cannot be removed.

A Data Protection Group's health is indicated by the following states:

- ◆ Protection state
- ◆ Process in progress

Data Protection Group State

The Data Protection Group state indicates the maximum number of disks that can fail before data loss. The possible state values are:

- ◆ Normal - The Data Protection Group is fully protected.
- ◆ Degraded - The Data Protection Group has encountered a single or dual SSD-failure with no data or service loss, but possible performance degradation. When there is sufficient free space, the Data Protection Group automatically initiates a rebuild. When capacity is insufficient or the cluster has reached its minimum number of SSDs, rebuild does not start until at least one failed SSD is replaced. When two SSDs fail, a critical alert is issued. The alert is cleared when the subsequent rebuild is complete.
- ◆ Error - The Data Protection Group has encountered more than two SSD failures. Multiple SSD failure is manageable, provided that the rebuild occurs before the next failure and there is sufficient space for an additional rebuild. If three SSDs fail simultaneously or are removed from an X-Brick, service is stopped and data loss occurs. In case of removed SSDs, if any of the SSDs is re-inserted, the cluster can be re-started and no data is lost.

Data Protection Process in Progress

The Data Protection Group process in progress state indicates that a process is being run. The process in progress is related to the current protection state.

The processes can be one of the following:

- ◆ Rebuild (including resync) - The Data Protection Group is performing a rebuild, following SSD failure. The rebuild process starts automatically without stopping the service.
- ◆ Integrate - A new SSD has been inserted and is being added to the Data Protection Group. The cluster identifies the new SSD and stops the rebuild process. This process results in increased space, allowing rebuilds to be completed successfully.
- ◆ Rebalance - The XtremIO Storage Array has added a new SSD to the Data Protection Group and is re-balancing the load.

When a Data Protection Group's state is unhealthy, the cluster issues the following alert: "Cluster is in a degraded mode, additional SSD failure will cause service and data loss". For more information, see "[Monitoring the Storage Elements](#)" on page 139.

Monitoring Data Protection Groups, Using the GUI

To view Data Protection Groups (DPGs) information:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 37 on page 67](#).
2. Click **Graphical View** to display the graphical view of the cluster.
3. In the left pane, select the relevant X-Brick.
4. Hover the mouse pointer over SSDs that are members of the DPG in the main window to view the Data Protection Group status.

You can view a DPG's alerts by right-clicking the DPG and clicking **Display <DPG name> Alerts**.

Note: To view a summary of DPGs data, click **Logical View** in the Inventory workspace menu bar and then click **Data Protection Groups** in the Hardware tab. For more information, see "[Data Protection Groups View](#)" on page 81.

Monitoring Data Protection Groups, Using the CLI

Use the following CLI commands for monitoring Data Protection Groups:

Command	Description
show-data-protection-groups	Displays XDP groups status and information.
show-clusters-data-protection-properties	Displays the clusters' data protection properties.
show-data-protection-groups-performance	Displays XDP groups performance information.

Monitoring the Local Disks

Monitoring the Local Disks, Using the GUI

To view Local Disks information:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 37 on page 67](#).
2. Click **Graphical View** to display the graphical view of the cluster.
3. In the left pane, select the relevant X-Brick.
4. Hover the mouse pointer over a Local Disk graphic representation in the main window to view the Local Disk information.

You can view a Local Disk's alerts by right-clicking the DPG and clicking **Display <Local Disk name> Alerts**.

Monitoring Local Disks, Using the CLI

Use the following CLI command for monitoring Local Disks:

Command	Description
show-local-disks	Displays the Storage Controller's local disks information.

Monitoring the Battery Backup Units

Monitoring the BBUs, Using the GUI

To view BBUs information:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 37 on page 67](#).
2. Click **Graphical View** to display the graphical view of the cluster.
3. In the left pane, select the relevant X-Brick.
4. Hover the mouse pointer over a BBU's graphic representation in the main window. Use both front and back views to view the BBU information.

You can view a BBU's alerts by right-clicking a BBU and clicking **Display <BBU name> Alerts**.

Note: To view a summary of existing BBUs data, click **Logical View** in the Inventory workspace menu bar and then click **Battery Backup Units** in the Hardware tab. For more information, see "[Battery Backup Units View](#)" on page 88.

Monitoring Battery Backup Units, Using the CLI

Use the following CLI command for monitoring BBUs:

Command	Description
show-bbus	Displays Battery Backup Units information.

Monitoring the DAEs

Monitoring the DAEs, Using the GUI

To view DAEs information:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 37 on page 67](#).
2. Click **Graphical View** to display the graphical view of the cluster.
3. In the left pane, select the relevant X-Brick.
4. Hover the mouse pointer over a DAE's graphic representation in the main window. Use both front and back views to view the DAE information.

You can view a DAE's alerts by right-clicking a DAE and clicking **Display <DAE name> Alerts**.

Note: To view a summary of DAEs data, click **Logical View** in the Inventory workspace menu bar and then click **DAEs** in the Hardware tab. For more information, see [“DAEs View” on page 82](#).

Monitoring DAEs, Using the CLI

Use the following CLI commands for monitoring DAEs:

Command	Description
show-daes	Displays the cluster's DAE information.
show-daes-psus	Displays a list of DAE power supply units (PSUs) and their properties.
show-daes-controllers	Displays a list of DAE LCCs (controllers) and their properties.

Monitoring the Targets

Targets Overview

A Target is a physical port, located on a Storage Controller.

The XtremIO Storage Array supports the following Target types:

- ◆ iSCSI - a 10GbE NIC port for connecting to iSCSI networks. There are two iSCSI Targets per Storage Controller.
- ◆ FC - an FC HBA port for connecting to fiber optic cable networks. There are two FC Targets per Storage Controller.

The cluster's Targets form the XtremIO Storage Array's front-end to which application servers connect for receiving storage services.

During the initial cluster configuration, the XtremIO Storage Array discovers each of the Storage Controller's Targets and adds them to a default Target Group.

Monitoring Targets, Using the GUI

To monitor the cluster's Targets, using the GUI:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 37 on page 67](#).
2. Click **Graphical View** to display the graphical view of the cluster.
3. In the left pane, select the relevant X-Brick.
4. Click **Show Back** to view the rear side of the X-Brick in the main window.
5. Hover the mouse pointer over the Storage Controllers to view the tool-tip information about the Target ports. The information includes port name, state, address, and existing alerts.

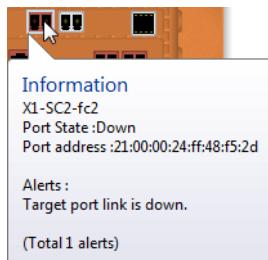


Figure 95 Tool-Tip Information

You can view a detailed view of a Target's alerts by right-clicking the Target and clicking **Display <Target name> Alerts**.

Note: To view a summary of Targets data, click **Logical View** in the Inventory workspace menu bar and then click **Targets** in the Hardware tab. For more information, see [“Cluster Configuration” on page 90](#).

For more information about Targets' connection, see [“Monitoring Initiators, Using the GUI” on page 144](#).

You can also monitor iSCSI portals and routes, using the iSCSI Network Configuration screen (see [“Notification Tab” on page 105](#)).

Monitoring Targets, Using the CLI

Use the following CLI commands for monitoring Targets:

Command	Description
show-targets	Displays the cluster Targets information.
show-target-groups	Displays a list of Target groups.
show-targets-fc-error-counters	Displays Fibre Channel error counter per Target.
show-target-groups-fc-error-counters	Displays Fibre Channel error counter per Target group.
show-targets-performance	Displays Targets' performance data.
show-targets-performance-small	Displays Targets' performance data for small (under 4KB) blocks.
show-targets-performance-unaligned	Displays Targets' performance data for unaligned blocks.
show-target-groups-performance	Displays Target groups' performance data.
show-target-groups-performance-small	Displays Target groups' performance data for small (under 4KB) blocks.
show-target-groups-performance-unaligned	Displays Target groups' performance data for unaligned blocks.

Monitoring the Storage Elements

Monitoring the Volumes

Volumes Overview

You can define various quantities of disk space as Volumes in an active cluster.

Volumes are defined by:

- ◆ Volume size - the quantity of disk space reserved for the Volume
- ◆ LB size - the logical block size in bytes
- ◆ Alignment-offset - a value for preventing unaligned access performance problems

Note: When using the GUI, selecting a predefined Volume type sets both the alignment-offset and LB size values. Using the CLI, you can define the alignment-offset and LB size values separately.

Monitoring Volumes, Using the GUI

To monitor the cluster's Volumes, using the GUI:

1. From the menu bar, click the **Configuration** icon to display the Configuration workspace, as shown in [Figure 24 on page 53](#).
2. In the Virtual tab (left pane) click **Volumes**. The main window displays the defined Volumes list.

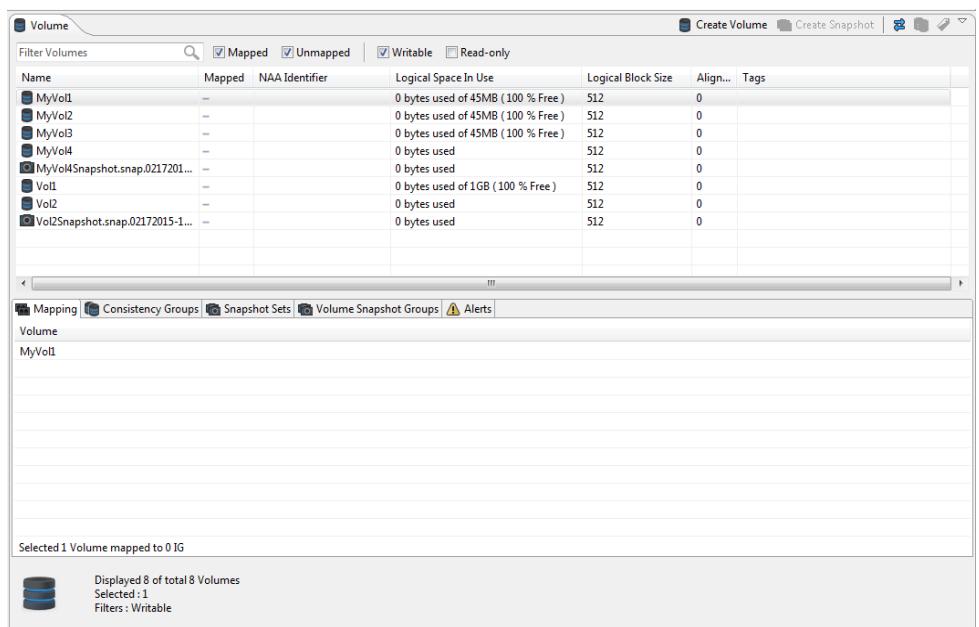


Figure 96 Configuration Workspace - Volumes Pane

For each Volume, the following properties are displayed:

- Volume Name
- Cluster Name
- Is Read Only
- Is Mapped
- NAA Identifier
- Space In Use (VSG)
- Volume Size
- Logical Block Size
- Alignment Offset
- Tags

You can filter the Volumes display by typing a search string in the filter window or by selecting one or more of the available filter options:

- Writable
- Read-Only
- Mapped
- Unmapped
- Volume
- Snapshot

3. Click a Volume in the top table and click a tab in the bottom table to view additional Volume-related data. Available data tabs include:

- Mapping
- Volume Snapshot Groups
- Consistency Groups
- Snapshot Sets
- Schedulers
- Alerts

Monitoring Volumes, Using the CLI

Use the following CLI commands for monitoring Volumes:

Command	Description
<code>show-volume</code>	Displays the specified Volume's information.
<code>show-volumes</code>	Displays a list of Volumes and their information.
<code>show-volume-snapshot-groups</code>	Displays the defined Snapshot groups and their parameters
<code>show-volumes-performance</code>	Displays Volumes' performance data.
<code>show-volumes-performance-small</code>	Displays Volumes' performance data for small (under 4KB) blocks.
<code>show-volumes-performance-unaligned</code>	Displays Volumes' performance data for unaligned blocks.

Monitoring the Consistency Groups

Consistency Groups Overview

Consistency Groups are a hierarchical layer above Volumes that enables grouping several Volumes together (e.g. Volumes that have a common database) and manipulating them so that data is cross-consistent for all members in the group.

Monitoring Consistency Groups, Using the GUI

To monitor the cluster's Consistency Groups, using the GUI:

1. From the menu bar, click the **Configuration** icon to display the Configuration workspace, as shown in [Figure 24 on page 53](#).
2. In the Virtual tab (left pane) click **Consistency Groups**. The main window displays the defined Consistency Groups list.

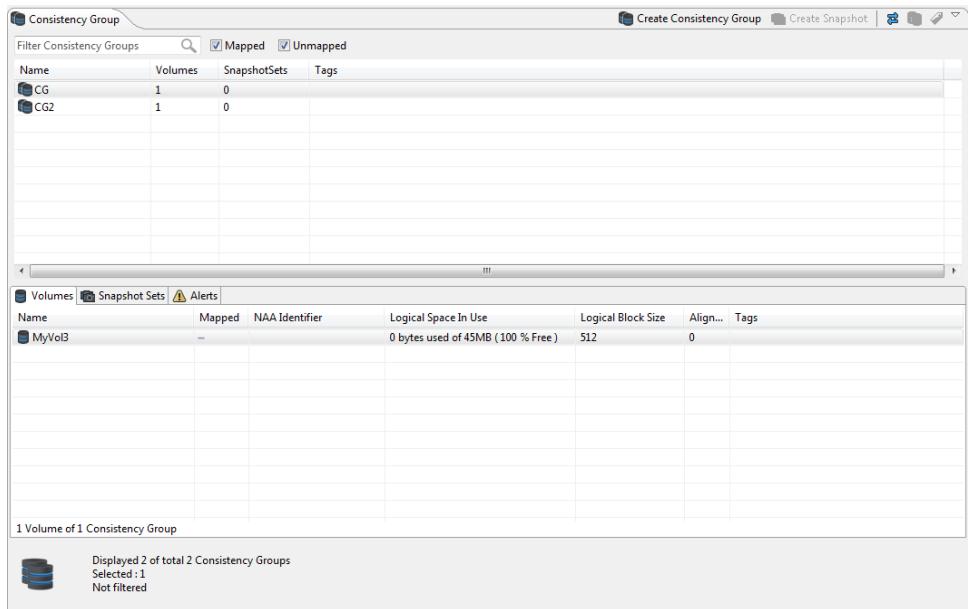


Figure 97 Configuration Workspace - Consistency Groups Pane

For each Consistency Group, the following properties are displayed:

- Consistency Group Name
- Cluster Name
- Is Read Only
- Is Mapped
- Number of Volumes
- Number of Snapshot Sets
- Tags

You can filter the Consistency Groups display by typing a search string in the filter window or by selecting one of the available filter options:

- Writable
- Read-Only
- Mapped
- Unmapped

3. Click a Consistency Group in the top table and click a tab in the bottom table to view additional Consistency-Group-related data. Available data tabs include:
 - Volumes
 - Mapping of Member Volumes
 - Snapshot Sets
 - Schedulers
 - Alerts

Monitoring Consistency Groups, Using the CLI

Use the following CLI commands for monitoring Consistency Groups:

Command	Description
show-volume	Displays the specified Volume's information.
show-volumes	Displays a list of Volumes and their information.
show-volume-snapshot-groups	Displays the defined Snapshot groups and their parameters.
show-volumes-performance	Displays Volumes' performance data.
show-volumes-performance-small	Displays Volumes' performance data for small (under 4KB) blocks.
show-volumes-performance-unaligned	Displays Volumes' performance data for unaligned blocks.

Monitoring the Initiators

Initiators Overview

The XtremIO Storage Array uses the term ‘Initiators’ to refer to ports which can access a Volume.

Monitoring Initiators, Using the GUI

To monitor the cluster’s Initiators, using the GUI:

1. From the menu bar, click the **Configuration** icon to display the Configuration workspace, as shown in [Figure 24 on page 53](#).
2. In the Virtual tab (left pane) click **Initiators**. The main window displays the defined Initiators list.

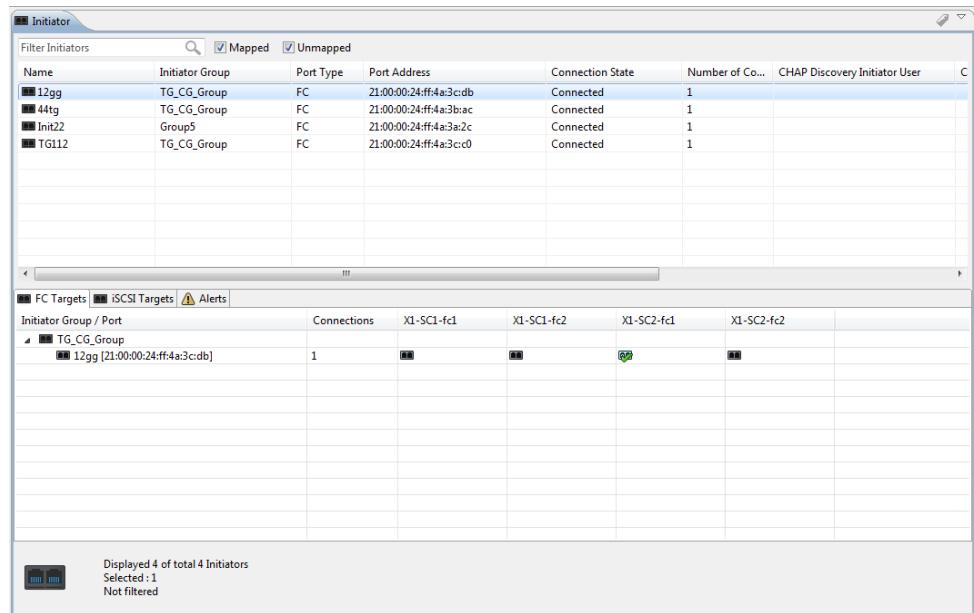


Figure 98 Configuration Workspace - Initiators Pane

For each Initiator, the following properties are displayed:

- Initiator Name
- Cluster Name
- Initiator Group
- Operating System
- Port Type
- Port Address
- Number of Connected Targets
- Tags

You can filter the Initiators display by typing a search string in the filter window or by selecting one of the available filter options:

- Mapped
 - Unmapped
3. Click an Initiator in the top table and click a tab in the bottom table to view additional Initiator-related data. Available data tabs include:
 - Targets
 - Alerts

Monitoring Initiators, Using the CLI

Use the following CLI commands for monitoring Initiators:

Command	Description
show-initiators	Displays Initiators' data.
show-initiators-performance	Displays Initiators' performance data.
show-initiators-performance-small	Displays Initiators' performance data for small (under 4KB) blocks.
show-initiators-performance-unaligned	Displays Initiators' performance data for unaligned blocks.
show-initiators-connectivity	Displays Initiators-Port connectivity and the number of connected Targets. Specifying the Target-details input parameter, provides the Initiators-Targets connectivity map.
show-discovered-initiators-connectivity	Displays the Initiators that are logged in to the cluster but not assigned to any Initiator Group.

Monitoring the Initiator Groups

Initiator Groups Overview

The XtremIO Storage Array uses the term ‘Initiators’ to refer to ports which can access a Volume. Initiators can be managed by assigning them to an Initiator Group. The Initiators within an Initiator Group share access to one or more of the cluster’s Volumes.

Monitoring Initiator Groups, Using the GUI

To monitor the cluster’s Initiator Groups, using the GUI:

1. From the menu bar, click the **Configuration** icon to display the Configuration workspace, as shown in [Figure 24 on page 53](#).
2. In the Virtual tab (left pane) click **Initiator Groups**. The main window displays the defined Initiator Groups list.

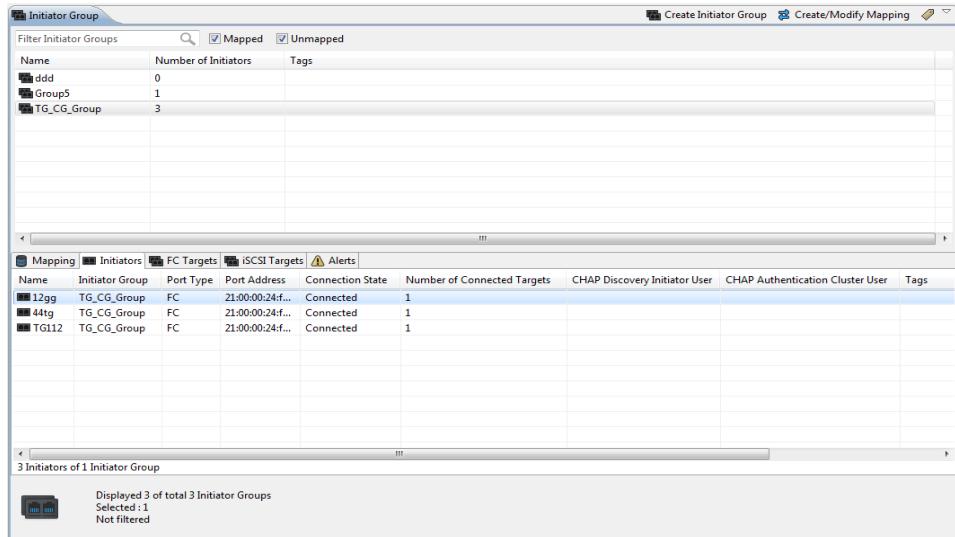


Figure 99 Configuration Workspace - Initiator Groups Pane

For each Initiator Group, the following properties are displayed:

- Initiator Group Name
- Cluster Name
- Number of Mapped Volumes
- Number of Connections
- Tags

You can filter the Initiator Groups display by selecting one or more of the available filter options:

- Mapped
- Unmapped

3. Click an Initiator Group in the top table and click a tab in the bottom table to view additional Initiator-Group-related data. Available data tabs include:
 - Mapping
 - Initiators
 - Targets
 - Alerts

Monitoring Initiator Groups, Using the CLI

Use the following CLI commands for monitoring initiator groups:

Command	Description
show-initiator-group	Displays information for a specific Initiator Group.
show-initiator-groups	Displays information for all Initiator Groups.
show-initiator-groups-performance	Displays Initiator Groups' performance data.
show-initiator-groups-performance-small	Displays Initiator Groups' performance data for small (under 4KB) blocks.
show-initiator-groups-performance-unaligned	Displays Initiator Groups' performance data for unaligned blocks.

Monitoring the Snapshot Sets

Snapshot Sets Overview

An XtremIO Storage Array Snapshot Set is an entity that groups a set of Snapshots generated at the same point in time. A Snapshot Set is created by performing a snapshot operation on a single Volume or multiple Volumes, a Snapshot Set or a Consistency Group.

Monitoring Snapshot Sets, Using the GUI

To monitor the cluster's Snapshot Sets, using the GUI:

1. From the menu bar, click the **Configuration** icon to display the Configuration workspace, as shown in [Figure 24 on page 53](#).
2. In the Virtual tab (left pane) click **Snapshot Sets**. The main window displays the defined Snapshot Sets list.

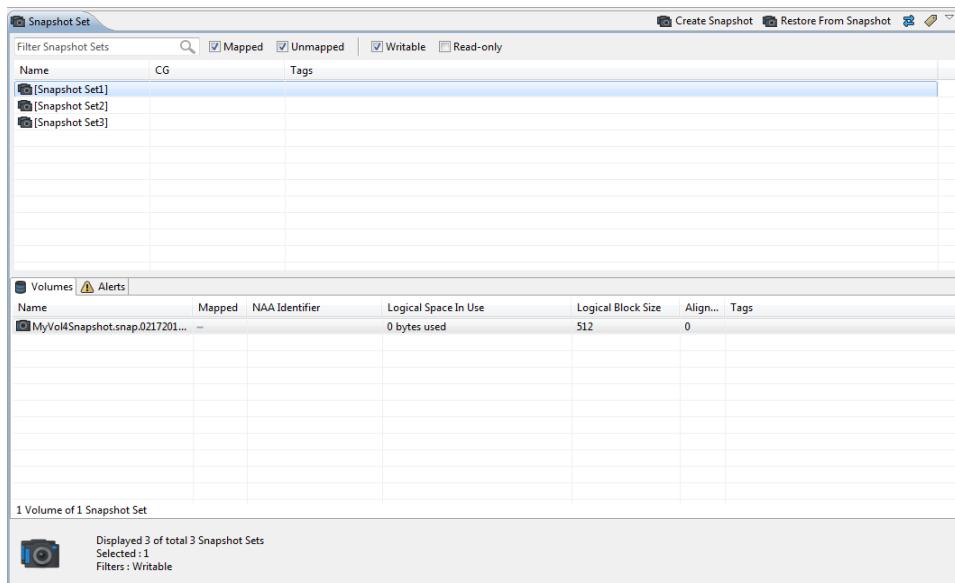


Figure 100 Configuration Workspace - Snapshot Sets Pane

For each Snapshot Set, the following properties are displayed:

- Snapshot Set Name
- Cluster Name
- Creation Time
- Is Read Only
- Is Mapped
- Originated From
- Number of Volumes
- Tags

You can filter the Snapshot Sets display by typing a search string in the filter window or by selecting one of the available filter options:

- Writable
 - Read-Only
 - Mapped
 - Unmapped
3. Click a Snapshot Set in the top table and select a tab in the bottom table to view additional Snapshot-Set-related data. Available data tabs include:
 - Volumes
 - Mapping of Member Volumes
 - Consistency Groups
 - Schedulers
 - Alerts

Monitoring Snapshot Sets, Using the CLI

Use the following CLI commands for monitoring Snapshot Sets:

Command	Description
show-snapshot-set	displays the parameters of a specified Snapshot Set.
show-snapshot-sets	Displays a list of Snapshot Sets and related information.
remove-snapshot-set	Removes a Snapshot Set.

Monitoring the Alerts

The XtremIO Storage Array provides a predefined list of alerts.

An alert indicates a condition that requires user attention and in some cases, user intervention.

To view the alerts list, refer to [“Alerts and Events Details” on page 491](#).

Monitoring Alerts, Using the GUI

The Alerts pane in the Dashboard workspace displays active alerts, as explained in [“Alerts Pane” on page 49](#).

You can right-click an alert to:

- ◆ Acknowledge the alert.
- ◆ Edit the alert’s definitions.
- ◆ View the alert’s properties.

When an alert is acknowledged or cleared, it is removed from the table.

- ◆ You can view the alerts of a specific hardware element by selecting the element from the list in the Inventory workspace and clicking the Alerts tab. See [“Monitoring the Hardware Elements” on page 127](#).
- ◆ You can view the alerts of a specific cluster element by selecting the element from the list in the Configuration workspace and clicking the Alerts tab. See [“Monitoring the Storage Elements” on page 139](#).
- ◆ You can view the full alerts list in the Alerts tab of the Alerts & Events workspace, as explained in [“Alerts & Events Workspace” on page 94](#).

Monitoring Alerts, Using the CLI

Use the following CLI commands for monitoring cluster’s alerts:

Command	Description
show-alerts	Displays a list of active alerts and their details.
show-alert-definitions	Displays a list of pre-defined alerts and their definitions.

Managing the Reports

XtremIO Storage Array enables you to collect historical data, perform analysis and run reports.

For a description of the Reports window, see [“Reports Workspace” on page 99](#).

Predefined Reports

XtremIO provides a set of predefined reports that cannot be edited or deleted. However, you can create a copy of a predefined report and modify it according to your needs to create a user-defined report. The predefined reports include:

- ◆ Latency
 - Latency by block size
 - System latency
- ◆ IOPS
 - IOPS by block size
 - System IOPS
- ◆ CPU
 - Xenv utilization
- ◆ Capacity
 - System capacity
 - System efficiency
- ◆ Bandwidth
 - Bandwidth by block size
 - System bandwidth
- ◆ Space
 - SSD endurance

The predefined reports are marked as "(Predefined)" after the report's title.

Viewing Reports

To view a report:

- ◆ Double-click the report name in the Reports list or right-click the report from the Reports list and select **Run** from the menu. The report data is displayed in the main window and the icon next to the report in the report list is changed to indicate that it is opened.

To view multiple reports:

- ◆ Double-click the reports you want to view and toggle between them by clicking the reports' tabs.

To view multiple reports in a split screen mode:

1. Double-click the reports you want to view.
2. Drag the tab of one of the opened reports to the bottom status bar; the screen is split and the dragged report can be viewed below the other opened reports.
3. You can repeat the drag-and-drop action to further split the screen. You can also drag a report into another report to create a separate tabbing of the two reports.

To zoom in and out on a report's view:

1. Right-click the report view and select **Zoom In** or **Zoom Out** from the drop-down list.
2. Select the relevant axes from the sub-list (both axis, domain axis or range axis); the report view is changed accordingly.

You can also drag the mouse to select a section of the report to zoom in on it.

Note: Zooming in on the report view displays the aggregated information in higher resolution. It does not increase the amount of aggregated information. To change the amount of aggregated data, select a different time frame when you define the report parameters.

To print the report view:

- ◆ Right-click the report view and select **Print** from the drop-down list.

To save the report view in png format:

1. Right-click the report view and select **Save as** from the drop-down list.
2. Select **PNG** from the sub-list.

Managing Reports, Using the GUI

Generating a Report

When you generate a new report, you need to address the following report parameters:

- ◆ Time frame - you can set the following time frames for the data collection:
 - Real-time monitor - generates a real-time monitor that polls data every five seconds. Data is displayed as a sliding window that is constantly updated. Closing and re-opening the monitor causes the previous data to be lost.
 - Last hour - provides data from the last 60 minutes in one minute polling granularity.
 - Last day - provides data from the last 24 hours in ten minutes polling granularity.
 - Last week - provides data from the last 7 days in one hour polling granularity.
 - Last year - provides data from the last 365 days in one day polling granularity.
 - Custom range - a user defined time frame. The user sets a start date and time (default setting - first day of available data) and an end date and time (default setting - current date and time).
- ◆ Access rights - specify the report's access rights, i.e. whether it is public or private (default - private). A private report is accessible to the report's creator. A public report can be viewed by all users, and can be edited and deleted by the report's creator. Reports that were generated as public by another user are marked as "public" and reports that were generated as public by you are marked "my public".

When a user account is deleted, private reports created by that user become inaccessible. Public reports can still be viewed by all users, but can be edited and deleted only by a Tech user.

- ◆ Category and entity type - specify the data you wish to collect, namely, a category and an entity type.

Possible Categories:

- Bandwidth - small and unaligned
- CPU
- Capacity
- Compression
- IOPS - small and unaligned
- Latency - small and unaligned
- Memory
- Performance
- Small
- Space
- Unaligned

Possible entity types:

- Cluster
 - Data Protection Group
 - Initiator
 - Initiator Group
 - Module
 - SSD
 - Target
 - Target Group
 - Volume
 - Volume Snapshot Group
 - XIOS
 - XMS
- ◆ Display type - select the display type of your report. Available display types:
- Table
 - Bar Chart
 - Pie Chart
 - Line Chart

Adding a Report

To add a report to the report list, you can generate a new report or edit a copy of a pre-defined report.

To generate a report:

1. In the menu bar, click the **Report** icon; the Report window appears.
2. In the All Reports pane, click **New**; the Add New Report wizard appears.

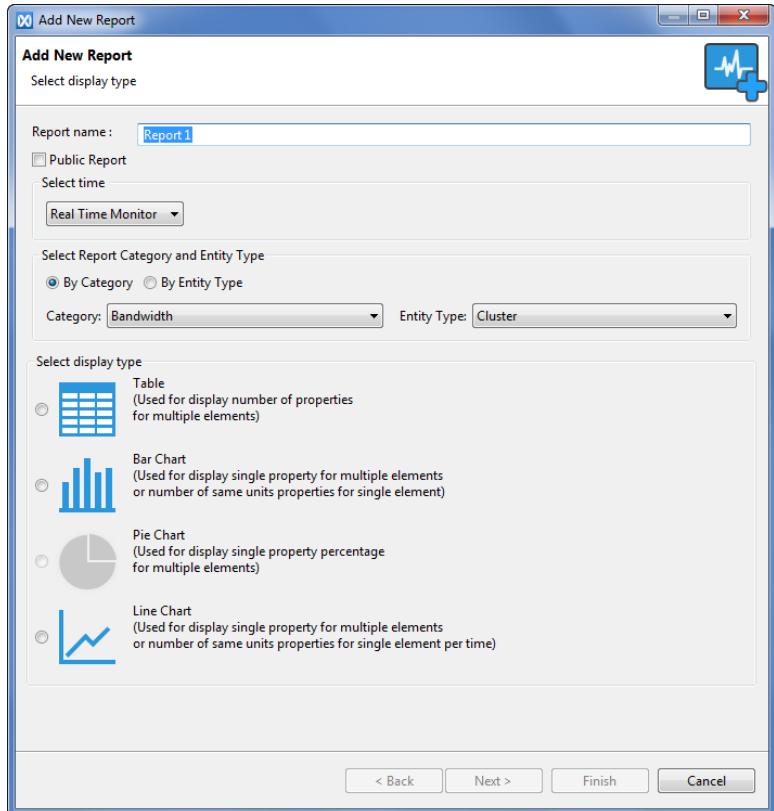
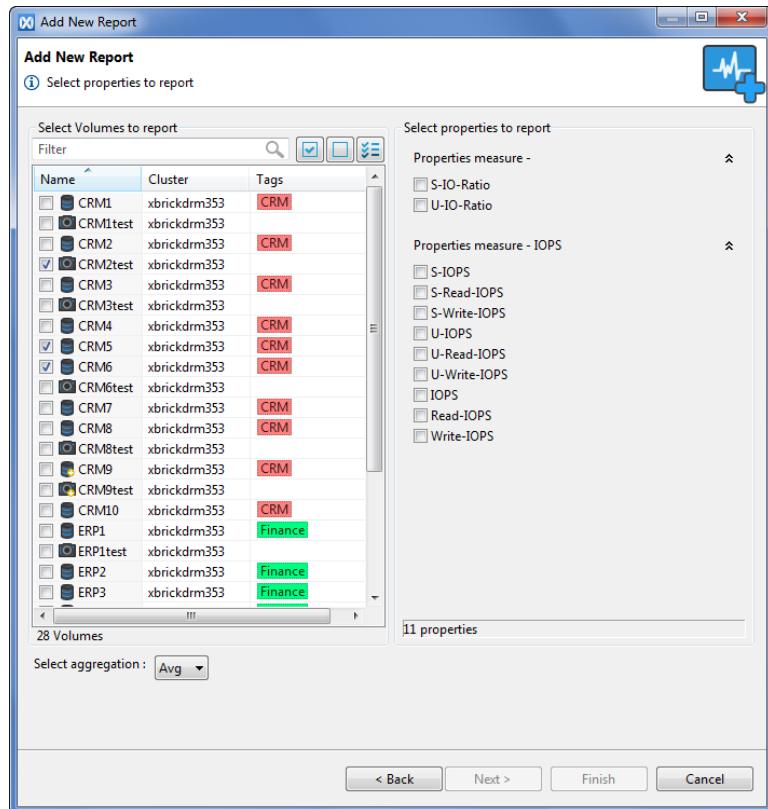


Figure 101 Add New Report - Display Type

3. Type a name for the report in the Report name field. The name does not have to be unique. The default assigned name is 'Report <index>' with an ascending serial number.
4. Set the report's access rights by selecting the Public Report checkbox, if you want the report to be viewed by other users (the report is private by default, i.e. the box is not selected).
5. Set the time frame for the report by selecting it from the drop-down list in the Select time section. If you select **Custom Time**, set the 'From' and 'To' date and time.
6. Select **Category** or **Entity Type** and select an item from the relevant drop-down list; the unselected drop-down list becomes active. Only the items that are relevant to your selection are displayed.
7. Select an item from the second list.

8. Select a display type by clicking one of the options. Only the relevant options are enabled.
9. Click **Next**.

**Figure 102** Add New Report - Properties

10. Select the relevant elements from the list. You can use the following:
 - Typing a string in the search window to filter the list.
 - Clicking the **Select All** icon to select all items on the list.
 - Clicking the **Deselect All** icon to unselect all items on the list.
 - Clicking the **Show All/Show Only Selected** icon to show all items or to show only the items you selected, respectively.

Note: Elements content and display differ according to the selected entity type.

11. Select the element's properties to appear in the report.

Note: Properties content and display differ according to the selected category and entity type.

12. Set the aggregation level (default is Average).

Note: Setting the aggregation level is not enabled for real-time reports.

13. Click **Next**.

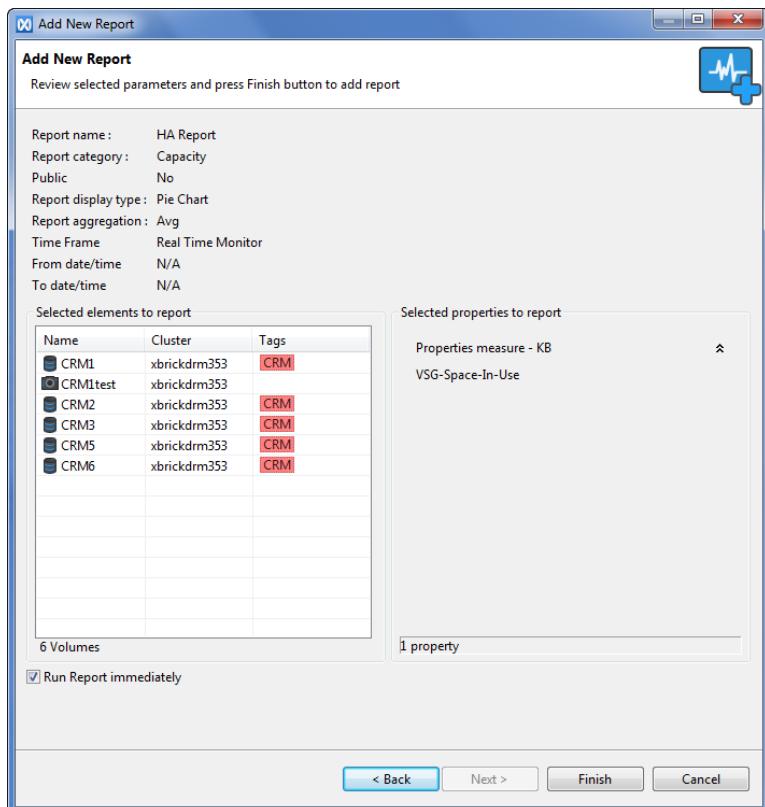


Figure 103 Add New Report - Review

14. If you want to run the report immediately after its creation, select **Run Report Immediately**.
15. Review the report's parameters and click **Finish**. The report is added to the report list and if you selected to run it upon creation, the report's data appears in the main window.

To edit a copy of a pre-defined report:

1. In the menu bar, click the **Report** icon; the Report window appears.
2. In the All Reports pane, right-click the report you want to modify and select **Copy** from the drop-down menu; the copy of the selected report appears below the source on the report list. The copy is titled <source report name>-copy (My Public).
3. Right-click the copy and select **Edit** from the drop-down list to modify the report's copy.

Note: When editing a copy of a report, you cannot change the category and entity type.

4. Edit the report's name in the Report name field. The report copy's default name is <source name>-copy. The name does not have to be unique.
5. Set the report's access rights. The report copy is public by default. To change it to private, clear the Public Report option.

6. Select a time frame from the drop-down list in the Select time section to edit the time frame for the report. If you select **Custom Time**, set the ‘From’ and ‘To’ date and time.
7. Click one of the display options to edit the display type. Only the relevant options are enabled.
8. Click **Next**.
9. Select the relevant elements from the list. You can use the following:
 - Filter the list by typing a string in the search window.
 - Select all items on the list by clicking the **Select All** icon
 - Unselect all items on the list by clicking the **Deselect All** icon
 - Show all available items by clicking the **Show All** icon 
 - Show only the items you selected by clicking the **Show Only Selected** icon 

Note: Elements content and display differ according to the selected entity type.

10. Select the element’s properties to appear in the report.

Note: Properties content and display differ according to the selected category and entity type.

11. Set the aggregation level (default is Average).

Note: Setting the aggregation level is not enabled for real-time reports.

12. Click **Next**.

13. If you want to run the report immediately after its creation, select **Run Report Immediately**.

14. Review the report’s parameters and click **Finish**; the edited report appears on the Reports list. If you selected to run it, the report’s data appears in the main window.

Editing a Report

To edit a report:

1. Right-click the report on the report list and select **Edit** from the drop-down list.

Note: When editing a copy of a report, you cannot change the category and entity type.

2. Edit the report’s name in the Report name field. The report copy’s default name is <source name>-copy. The name does not have to be unique.
3. Set the report’s access rights. The report copy is public by default. To change it to private, clear the Public Report option.
4. Select a time frame from the drop-down list in the Select Time section to edit the time frame for the report. If you select **Custom Time**, set the ‘From’ and ‘To’ date and time.

5. Click one of the display options to edit the display type. Only the relevant options are enabled.
6. Click **Next**.
7. Select the relevant elements from the list. You can use the following:
 - Filter the list by typing a string in the search window.
 - Click the **Select All** icon  to select all the items on the list.
 - Click the **Deselect All** icon  to unselect all the items on the list.
 - Click the **Show All/Show Only Selected** icon  to show all the items or to show only the items you selected, respectively.

Note: Elements content and display differ according to the selected entity type.

8. Select the element's properties to appear in the report.

Note: Properties content and display differ according to the selected category and entity type.

9. Set the aggregation level (default is Average).

Note: Setting the aggregation level is not enabled for real-time reports.

10. Click **Next**.

11. If you want to run the report immediately after its creation, select **Run Report Immediately**.

12. Review the report's parameters and click **Finish**; the edited report appears on the report list. If you selected to run it, the report's data appears in the main window.

Closing a Report

To close a report:

- ◆ In the Reports list, right-click the report and select **Stop and Close** from the drop-down menu or right-click the report tab and select **Close**; the report is closed and the icon next to the report in the report list is changed to indicate it is closed.

Deleting a Report

To delete a report:

- ◆ In the Reports list, right-click the report and select **Delete** from the drop-down menu; the report is deleted from the list.

Note: Predefined reports cannot be deleted.

Exporting a Report

To export a report:

1. Right-click the report from the Reports list and select **Export Report Data** from the menu.

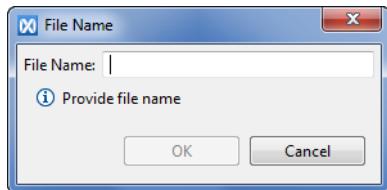


Figure 104 Export Report File Name

2. In the File Name dialog box, provide a name for the exported report file.
3. Click **OK**; the displayed success message specifies the exported report location.

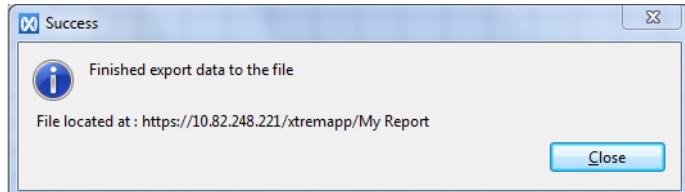


Figure 105 Export Report - Success Message

4. Click **Close**.

Note: The reports are exported in CSV format. The time stamp of the exported reports is in UTC time.

Managing Reports, Using the CLI

Use the following CLI commands for managing reports:

Command	Description
<code>show-report</code>	Displays the details of a specified report.
<code>show-reports</code>	Displays a list of defined reports.
<code>show-reports-data</code>	displays a report's data for a specified entity and category.

CHAPTER 5

Managing Volume Operations

This chapter includes the following topics:

◆ Overview	162
◆ Managing Storage Elements Tags	163
◆ Managing Volumes and Snapshots	168
◆ Managing the Consistency Groups	204
◆ Managing the Snapshot Sets	226
◆ Managing the Initiator Groups	239
◆ Managing Initiators	250
◆ Managing Mapping	253
◆ Managing the Schedulers	261

Overview

One of the primary capabilities of the XtremIO Storage Array is to provision Volumes (LUNs) to the connected servers.

A Volume is a defined quantity of disk space. Once you have created a Volume, you can provision it to your servers, enabling them to treat the Volume as a SCSI device.

Once Volumes are provisioned, it is possible to create Snapshots (instantaneous copy images) of Volume data.

XtremIO's Snapshot technology enables sustaining high performance, while maximizing the media endurance, both in terms of the ability to create multiple Snapshots and the amount of I/O that a Snapshot can support.

XtremIO uses the following storage objects for managing Snapshots and optimizing their usability:

- ◆ Volume Snapshot Groups - A Volume Snapshot Group (VSG) includes a Volume and all the Snapshots derived from it. The VSG is referred to in reports of used space, i.e. the space used by a Volume and all its derived snapshots is reported, rather than the space used by a single volume.
- ◆ Consistency Groups — Consistency Groups (CG) are used to create a consistent image of a set of Volumes. Using Consistency Groups, you can create Snapshots of all Volumes in a group, using a single command, thus ensuring that all Snapshots are created at the same point in time.
- ◆ Snapshot Set — A Snapshot Set is a group of Snapshots that were taken (of a Consistency Group or of multiple Volumes that are not members of a group), using a single command and represents a point in time of a group.
- ◆ Read-Only Snapshots — A read-only Snapshot cannot be changed by writing to it. Therefore, it provides an immutable copy of data and can be mapped to an external host, such as a backup application.
- ◆ Scheduler — The Scheduler defines a timetable for taking Snapshots of a Volume, a Consistency Group or a Snapshot Set.

To manage disk space, using Volumes:

1. Create a Volume and define its allocation of disk space (see “[Managing Volumes and Snapshots](#)” on page 168).
2. Create an Initiator Group and its related Initiators (ports) (see “[Managing the Initiator Groups](#)” on page 239).
3. Allow the Initiators to access the Volume's disk space by mapping the Initiator Group to a selected Volume (see “[Managing Mapping](#)” on page 253).

Managing Storage Elements Tags

XtremIO Storage Array provides users with a tagging system for marking the various storage elements. Tagging objects enables you to logically group, locate and manage multiple entities, and perform operations on multiple objects, using a single user command. You can use tagging to aggregate objects based on business requirements, and assign Tags according to related applications for ease-of-management.

Each object can have multiple Tags to reflect the object's function and position. Using Tag nesting, you can create a hierarchy that reflects the relationship between different cluster objects.

Tags can be used both via the GUI and the CLI.

Using Tags, you can perform the following:

- ◆ Filter Volumes for creating a Consistency Group.
- ◆ Filter objects for reports.
- ◆ Create aggregated Tag reports (using Volume Tags and IG Tags).
- ◆ Map all hosts of a cluster to a Volume (using IG Tags).

Managing Tags, Using the GUI

Creating Tags

You can create Tags for the following storage elements:

- ◆ Volumes
- ◆ Consistency Groups
- ◆ Snapshot Sets
- ◆ Initiator Groups
- ◆ Initiators
- ◆ Schedulers

To create Tags for cluster's storage elements:

1. In the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click the **Add Tag** icon.

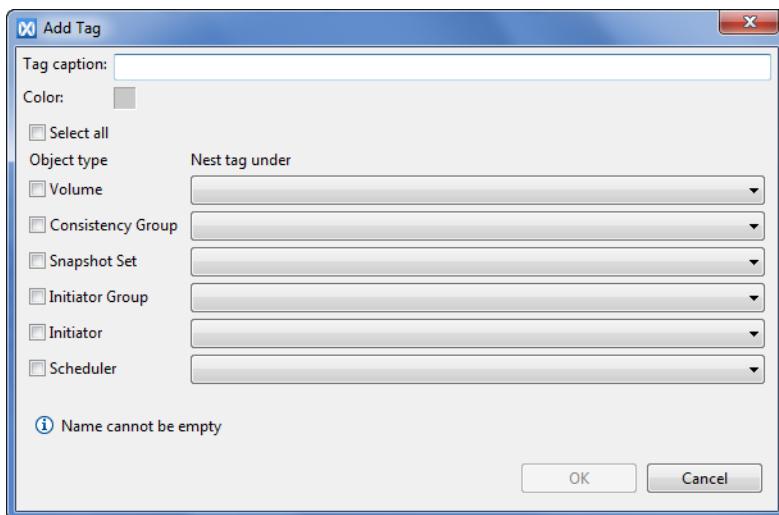


Figure 106 Add Tags - Configuration

3. Type a Tag name in the Tag caption field.

Note: A Tag name can have up to 64 characters. The following characters are allowed: alphanumeric symbols, space, ~ ! @ # \$ % ^ & * _ + { } | : < > ? / . -

4. Select the Tag color. You can select a different color for each object type by clicking the **Color** (gray) square to open the color palette and clicking a color.

5. Select the object types you wish to assign the new Tag to. If you want to select all objects, click **Select All**.
6. Click **OK**; the new Tag is added to the selected object types.

Note: The created Tag is not assigned to specific objects. To assign the Tag to objects, see “[Assigning Tags to Storage Elements](#)” on page 165.

Assigning Tags to Storage Elements

To assign a Tag to a storage element:

1. In the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click the object type you wish to tag to display the defined objects in the main window.
3. Right-click an object from the list in the main window and select **Manage Tags**. You can select multiple objects from the list, using the Ctrl and Shift keys.

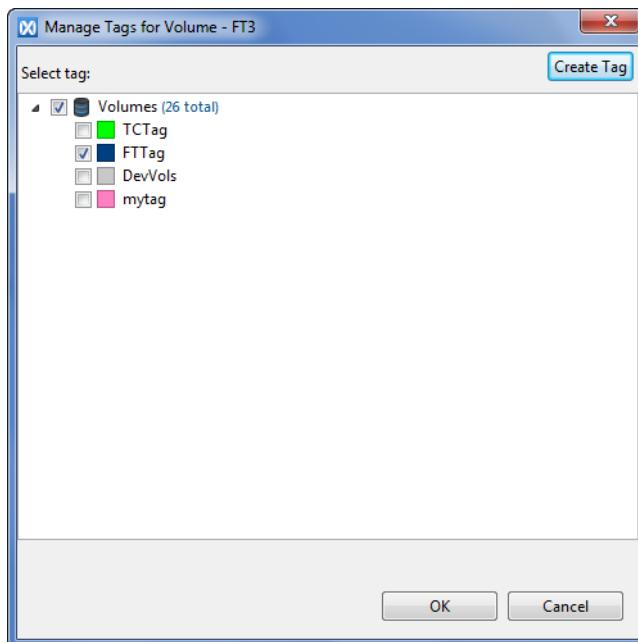


Figure 107 Assigning Tags to Logical Objects

The Manage Tags for <object> window displays the object type and all Tags that were defined for it. Tags that are already assigned to the object are checked.

Note: For multiple objects, the dialog box’s title is ‘Manage Tags for <number of objects>’.

4. Select the Tags you want to assign to the object and click **OK**.

Note: Another way to assign a Tag is to drag and drop the object you want to tag from the main window to the Tag that is located below the object type in the Virtual tab.

Editing Tags

To edit storage elements Tags:

1. In the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), double-click the relevant object type to open the list of Tags defined for that object type.
3. Right-click the Tag you wish to modify and select **Modify Tag** from the drop-down list.

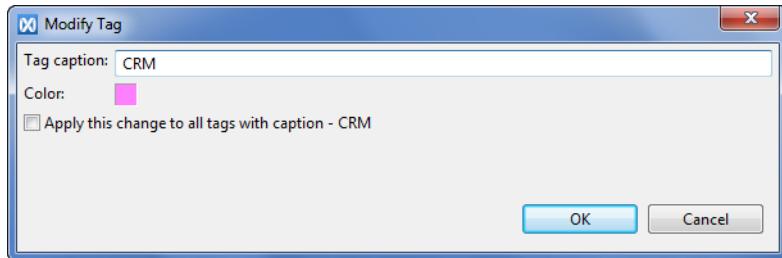


Figure 108 Modify Tag

4. In the Modify Tag dialog box you can edit the following parameters:
 - Tag caption
 - Tag color
5. If you wish to apply the changes to all Tags defined with the same caption, select that option.
6. Click **OK**.

Removing Tags

To remove storage elements Tags:

1. In the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), double-click the relevant object type to open the list of Tags defined for that object type.
3. Right-click the Tag you wish to remove and select **Delete Tag** from the drop-down list.
4. Click **Yes** to confirm; the Tag is deleted from the object type Tag list.

Managing Tags, Using the CLI

Use the following CLI commands for managing Tags:

Command	Description
show-tags	Displays the details of all defined Tags.
show-tag	Displays the details of a specified Tag.
create-tag	Creates a Tag for an entity.
tag-object	Assigns a Tag to a specified object.
untag-object	Removes a Tag from a specified object.
modify-tag	Modifies a specified Tag caption.
remove-tag	Deletes a Tag from the Tags list.

Managing Volumes and Snapshots

A Volume is a set of blocks, presented to the operating environment as a range of consecutive logical blocks with disk-like storage and I/O semantics. It is possible to define various quantities of disk space as Volumes in an active cluster.

Snapshots are instantaneous copy images of Volume data with the state of the data exactly as it appeared at the specific point in time the Snapshot was created. Snapshots enable you to save the Volume data state and then access the specific Volume data whenever needed, even after the source Volume has changed.

The Snapshot operation, which can be performed instantaneously and at any time, does not affect system performance, and a Snapshot can be taken either directly from a source Volume or from any of its Snapshots. Changes in the Volume data do not change the Snapshot.

Snapshots can be used to serve several purposes, such as a means of data protection and backup, data analysis and reporting.

Accessing Snapshots is performed the same way as accessing Volumes in the cluster in Read/Write access mode.

Snapshots can be saved in the system for as long as deemed necessary.

This section explains how to manage Volumes and Snapshots, using the XtremIO Storage Array GUI and CLI.

Managing Volumes and Snapshots, Using the GUI

Adding Volumes

Volumes have the following main characteristics:

- ◆ Volume size - the quantity of disk space reserved for the Volume
- ◆ LB size - the logical block size in bytes
- ◆ Alignment-offset - a value for preventing unaligned access performance problems

Note: In the GUI, selecting a predefined Volume type defines the alignment-offset and LB size values. In the CLI, you can define the alignment-offset and LB size values separately.

To add Volumes:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab, click **Volumes** to open the Volumes window.
3. In the Volume window menu bar, click **Create Volume**. You can also right-click Volumes in the Virtual tab and select **Create Volume**.

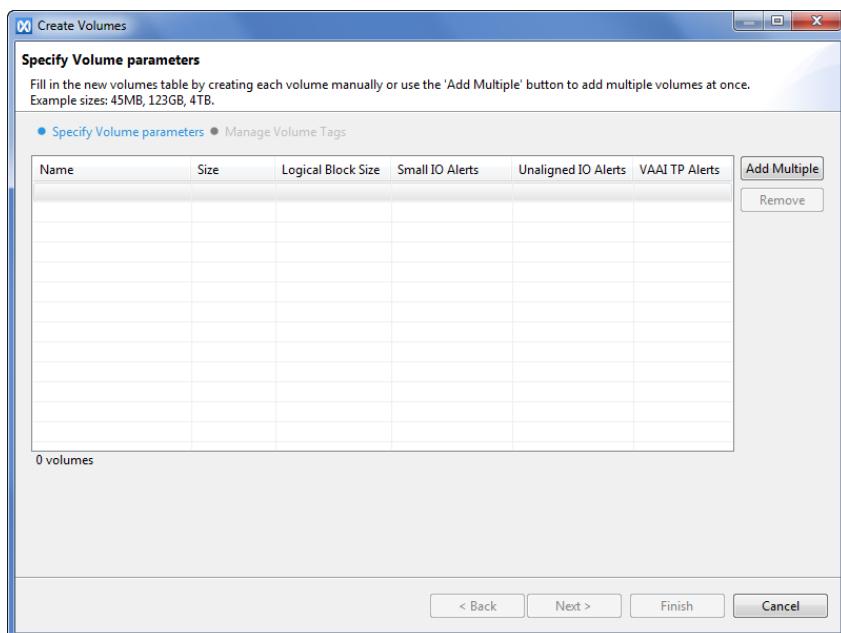


Figure 109 Create Volumes

4. In the Create Volumes screen, define the following:
 - Name - the name of the Volume (up to 128 characters)
 - Size - the amount of disk space allocated for this Volume:
 - Minimum Volume size is 1MB.
 - Size should be in multiples of 8KB.
 - Allowed units for allocation are KB, MB, GB, TB and PB.

- Logical Block Size - From the drop-down list, select one of the following types that define the LB size and alignment-offset:
 - Normal (512 LBs)
 - 4KB LBs
- Small IO Alerts - Set to **enabled** if you want an alert to be sent when small I/Os (<4KB) are detected.
- Unaligned IO Alerts - Set to **enabled** if you want an alert to be sent when unaligned I/Os are detected.
- VAAI TP Alerts - Set to **enabled** if you want an alert to be sent when the storage capacity reaches the set limit (refer to “[Configuring Cluster Limits via the GUI](#)” on page 288).

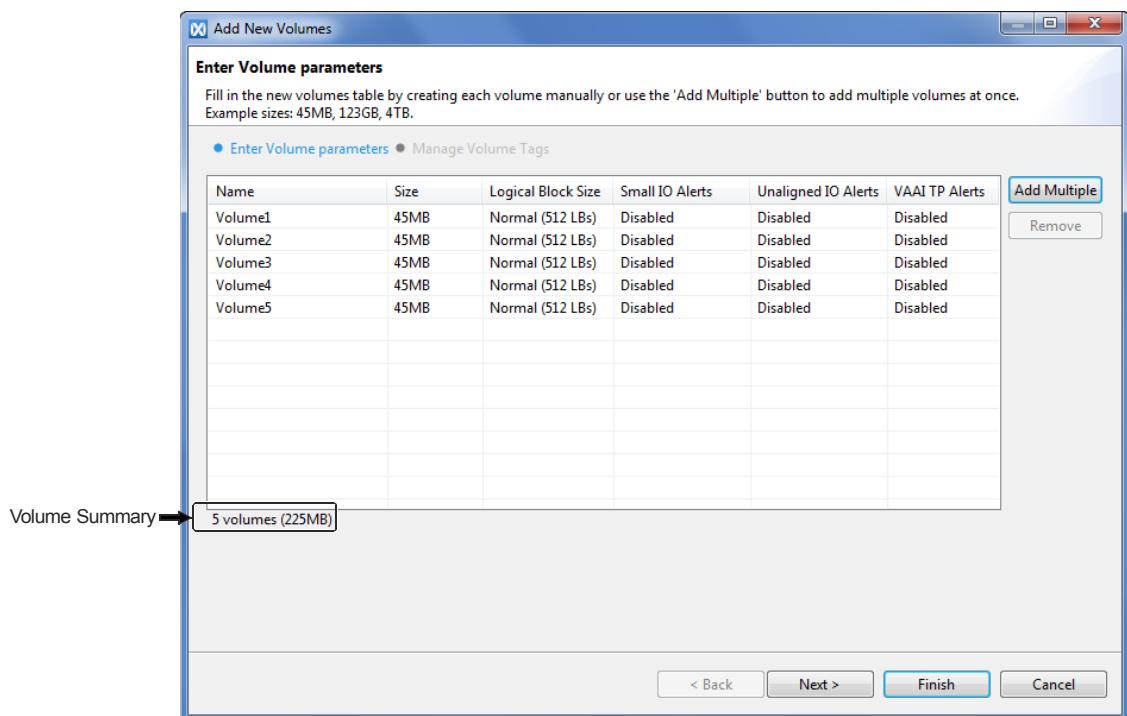


Figure 110 Add New Volumes - Summary Line

The summary line displays the number of Volumes defined in the list and their total disk space.

Note: Using this method, you can add multiple Volumes with varying definitions. If you want to add multiple Volumes with the same size and type, see “[Adding Multiple Volumes](#)”.

5. If you do not wish to assign Tags to the new Volumes, skip to [step 11](#).

Note: You can assign Tags to the new Volumes after Volume creation is completed. See “[Assigning Tags to Storage Elements](#)” on page 165.

- Click **Next** to assign Tags to the new Volumes.

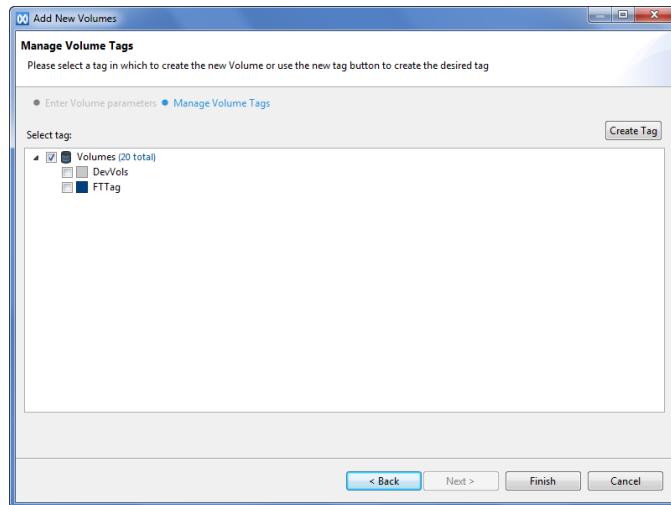


Figure 111 Add New Volumes - Manage Tags

The Manage Volume Tags window displays all the Tags that are currently defined for Volumes.

- Select the relevant Tag to assign it to the new Volumes. You can assign more than one Tag to a single Volume.
- If you wish to create a new Volume Tag, click **Create Tag**.

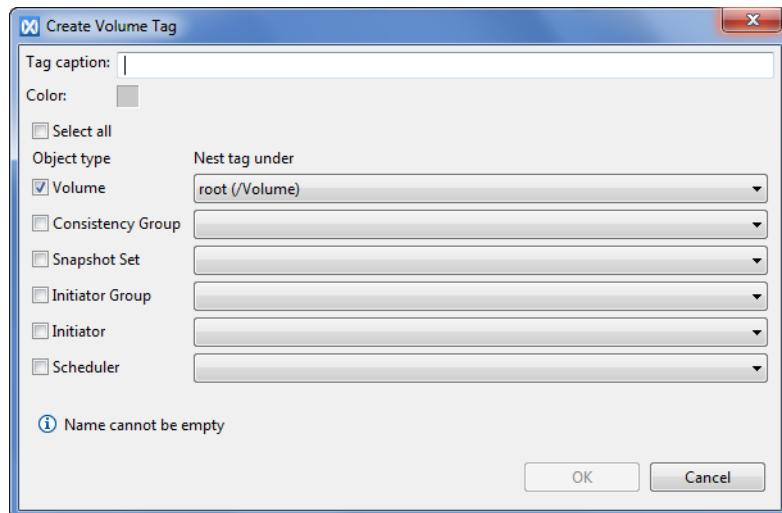


Figure 112 Create Volume Tag

- Set the Tag properties:
 - Tag name
 - Tag nesting path
 - Tag color

10. Click **OK**; the Tag is added to the Tag list in the Manage Volume Tags dialog box. Select the new Tag to assign it to the Volume.

Note: To create Tags not as part of the Volume creation procedure, see “[Managing Tags, Using the GUI](#)” on page 164.

11. Click **Finish**; the new Volumes are added in the Volumes table.

Adding Multiple Volumes

To add multiple Volumes with the same size and type:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab, click **Volumes** to open the Volumes window.
3. In the Volume window menu bar, click **Create Volume**. You can also right-click Volumes in the Virtual tab and select **Create Volume**.
4. In the Create Volumes window, click **Add Multiple**.

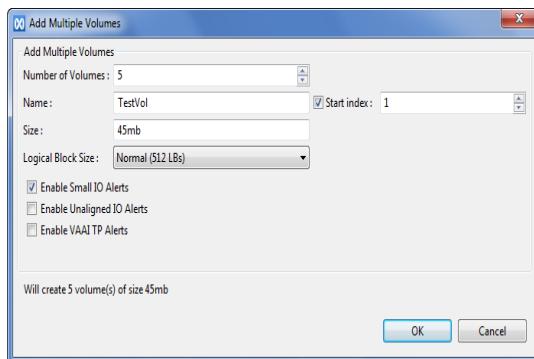


Figure 113 Add Multiple Volumes Dialog Box

5. Define the following:
 - Number of Volumes
 - Name - When you add multiple Volumes, all Volumes are assigned with a uniform prefix (set in the Name field) and a unique numeral suffix assigned automatically (e.g. vol1, vol2...).
 - Start Index - Each Volume must have a unique name. Each time you add multiple Volumes, the suffix automatically starts at 1. Therefore, adding multiple Volumes more than once while using the same prefix, results in repeating names.

To solve this, when you are adding Volumes with an existing prefix, select the **Start Index** option and set the start index to obtain unique names (e.g. if the existing Volumes are vol1, vol2 and vol3 and you want to create four more Volumes with the ‘vol’ prefix, set the Start Index at 4).

- Size - the amount of disk space allocated for this Volume:
 - Minimum Volume size is 1MB.
 - Size should be in multiples of 8KB.
 - Allowed units for allocation are KB, MB, GB, TB and PB.
 - Logical Block Size - From the drop-down list, select one of the following types that define the LB size and alignment-offset:
 - Normal (512 LBs)
 - 4KB LBs
 - Enable Small IO Alerts - Select this checkbox if you want an alert to be sent when small I/Os (<4KB) are detected.
 - Enable Unaligned IO Alerts - Select this checkbox if you want an alert to be sent when unaligned I/Os are detected.
 - Enable VAAI TP Alerts - Select this checkbox if you want an alert to be sent when the storage capacity reaches the set limit (refer to “[Configuring the Cluster Encryption](#)” on page 293).
6. Click **OK**; the new Volumes appear in the Volumes list of the Create Volume dialog box.
- Note:**
- You can use the following tools in the Add New Volumes window:
- ◆ Copy/Paste - Right-click a Volume and select Copy. Right-click in a row and select Paste.
 - ◆ Select multiple Volumes - Select a Volume, hold Shift and select additional Volumes.
 - ◆ Remove Volumes - Select a Volume and click Remove.
7. If you do not wish to assign Tags to the new Volumes, skip to [step 13](#).

Note: You can assign Tags to the new Volumes after Volume creation is completed. See “[Assigning Tags to Storage Elements](#)” on page 165.

8. Click **Next** to assign Tags to the new Volumes.

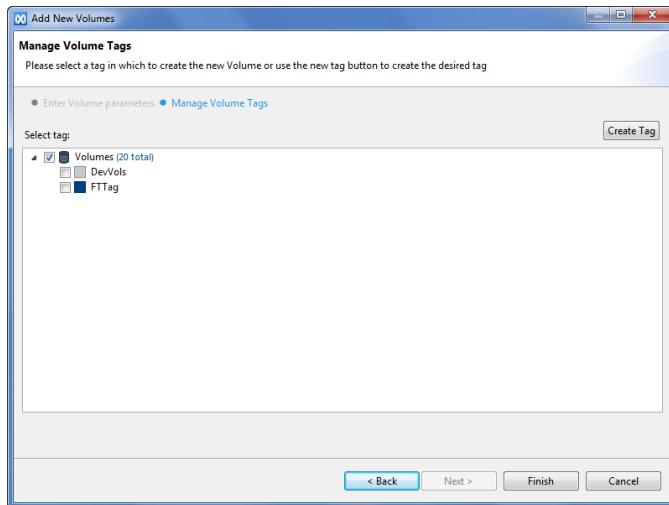


Figure 114 Add New Volumes - Manage Tags

The Manage Volume Tags window displays all the Tags that are currently defined for Volumes.

9. Select the desired Tag to assign it to the new Volumes. You can assign more than one Tag to a single Volume.
10. If you wish to create a new Volume Tag, click **Create Tag**.

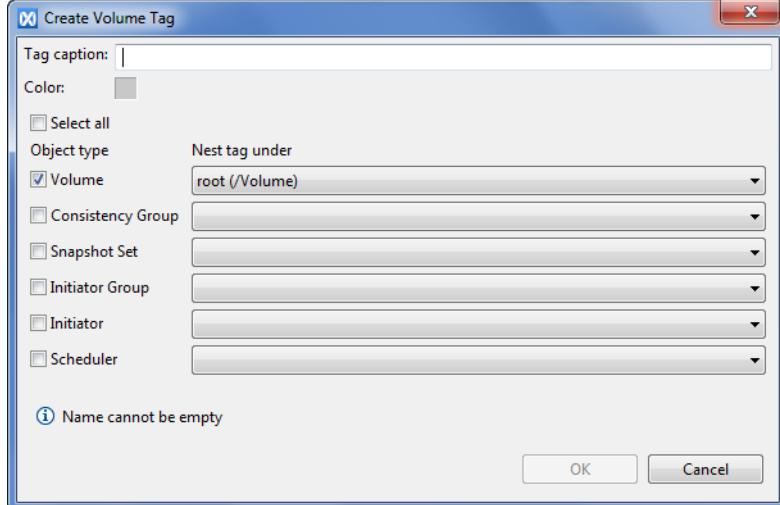


Figure 115 Create Volume Tag

11. Set the Tag properties:

- Tag name
- Tag nesting path
- Tag color

12. Click **OK**; the Tag is added to the Tag list in the Manage Volume Tags dialog box. Select the new Tag to assign it to the Volumes.

Note: To create Tags not as part of the Volume creation procedure, see “[Managing Tags, Using the GUI](#)” on page 164.

13. Click **Finish**; the new Volumes appear in the Volumes table in the Volumes window.

Creating Snapshots

The following Snapshot types are available:

- ◆ Snapshot of a Volume
- ◆ Snapshot of a Snapshot
- ◆ Snapshot Set - a Snapshot of a set of members (Volumes, Snapshots or a combination of both)

A Snapshot of a set of up to 256 members (maximum) can be created per operation, enabling the system to create a cross-consistent Snapshot containing the exact same-point-in-time image for all members. This can be carried out manually by selecting a set of Volumes for snapshotting, or by placing Volumes in a Consistency Group container and creating a Snapshot of the Consistency Group.

- ◆ Snapshot of tagged Volumes or Snapshots - the system creates a cross-consistent copy of all Volumes or Snapshots that are assigned a specific Tag.

To create a Snapshot, the following pre-conditions are required:

- ◆ Defined Volumes to be used as the source of the created Snapshot
- ◆ Defined Initiator Groups and Initiators (optional) - although not mandatory for defining Snapshots, Initiators enable mapping Volumes to host, allowing read and write operations to be performed.
- ◆ Mapping of Volumes to Initiators (optional) - to enable read and write operations.
- ◆ Tags (optional) - to simplify multiple Snapshot operations.

Regardless of the Snapshot’s source (single or multiple objects), the Snapshot operation results in a Snapshot Set.

To create a Snapshot:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab, click **Volumes** to open the Volumes window.
3. Select a Volume from the Volumes table.

Note: To select multiple members listed sequentially, select a member, hold Shift and select the additional members. To select multiple individual list members, select a member, hold Ctrl and select the additional list members.

4. In the Volumes table Menu Bar, click **Create Snapshot**. Another option is to right-click one of the selected objects and select **Create Snapshot** from the drop-down menu.

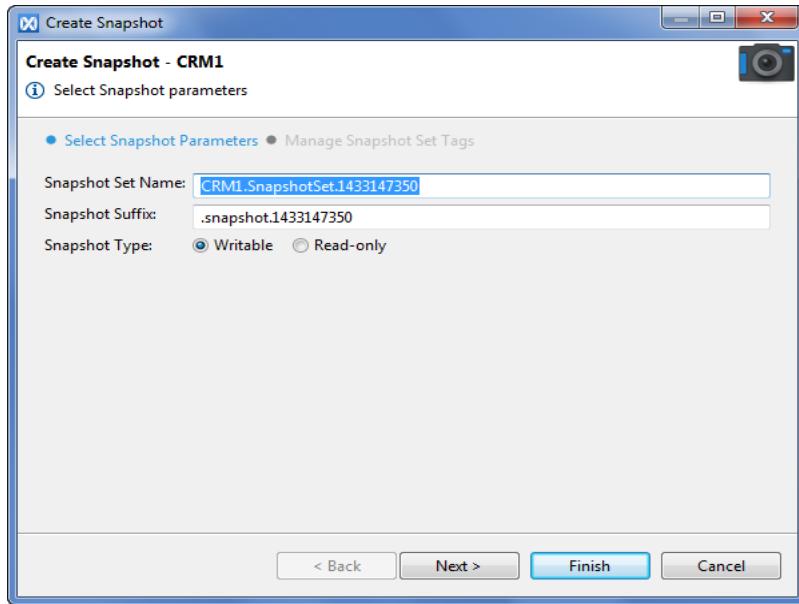


Figure 116 Create Snapshot Dialog Box

5. Set the new Snapshot Set name. The default name is <Volume-name>.SnapshotSet.<EPOCH>.
6. Set the Snapshot suffix that will be added to all the Snapshots in the Snapshot Set. The default suffix is .snapshot.<EPOCH>.
7. Set the Snapshot type by selecting Writable or Read-only (default value is Writable).
8. If you do not wish to assign Tags to the new Snapshot, skip to [step 14](#).

Note: You can assign Tags to the new Snapshot after its creation is completed. See [“Assigning Tags to Storage Elements” on page 165](#).

- Click **Next** to assign Tags to the new Snapshot Set.

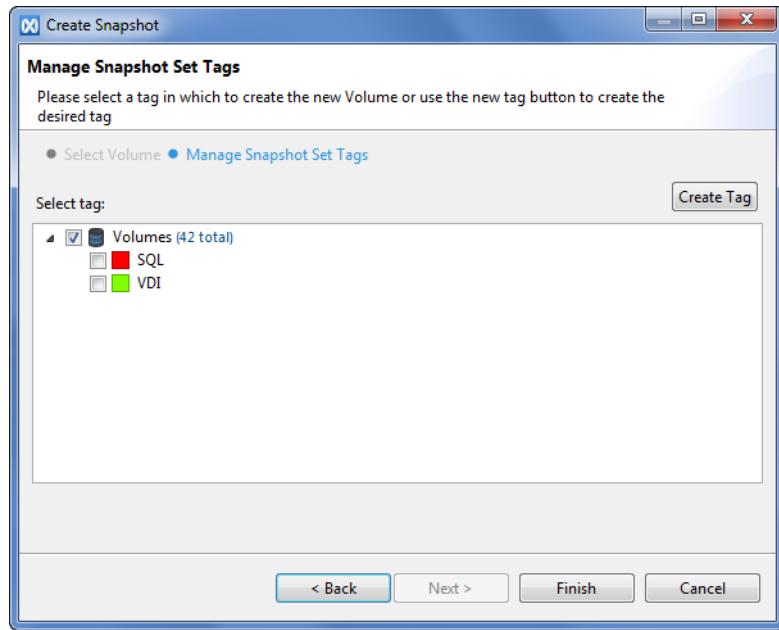


Figure 117 Create Snapshot - Manage Tags

The Manage Snapshot Set Tags window displays all Tags that are currently defined for storage objects.

- Select the relevant Tag to assign it to the new Snapshot. You can assign more than one Tag to a Snapshot Set.
- If you wish to create a new Tag, click **Create Tag**.

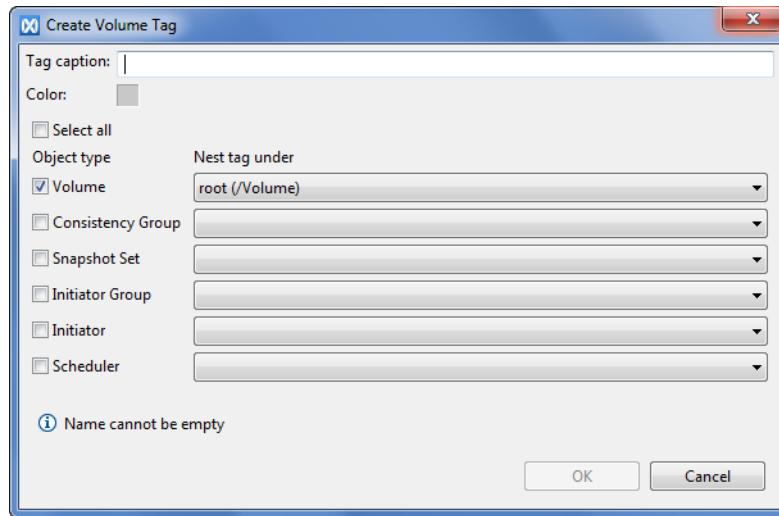


Figure 118 Create Volume Tag

12. Set the Tag properties:

- Tag caption
- Tag color
- Tag object type and nesting path

13. Click **OK**; the Tag is added to the Tag list in the Manage Snapshot Set Tags dialog box. Select the new Tag to assign it to the Snapshot Set.

Note: To create Tags not as part of the Snapshot Set creation procedure, see [“Managing Tags, Using the GUI” on page 164](#).

14. Click **Finish**; the new Snapshot Set appears in the Snapshot Set window, and the Snapshots included in the Snapshot Set appear in the Volumes window.

Note: It is recommended to view the created Snapshots in the Snapshot Set workspace. See [“Managing the Snapshot Sets” on page 226](#).

Snapshot Operations

The following operations are performed the same way for Snapshots and Volumes. Refer to the corresponding Volume procedures:

- ◆ Viewing Snapshots (refer to [“Viewing Volumes” on page 179](#))
- ◆ Viewing Snapshot properties (refer to [“Viewing Volume Properties” on page 180](#))
- ◆ Renaming Snapshots (refer to [“Renaming Volumes” on page 181](#))
- ◆ Deleting Snapshots (refer to [“Deleting Volumes” on page 183](#))
- ◆ Viewing Snapshot alerts (refer to [“Managing Volumes and Snapshots, Using the CLI” on page 203](#))
- ◆ Mapping Snapshots to Initiators (refer to [“Mapping Volumes to Initiator Groups” on page 190](#))
- ◆ Accessing Snapshots via Initiators (refer to [“Managing Initiator Groups, Using the CLI” on page 249](#))

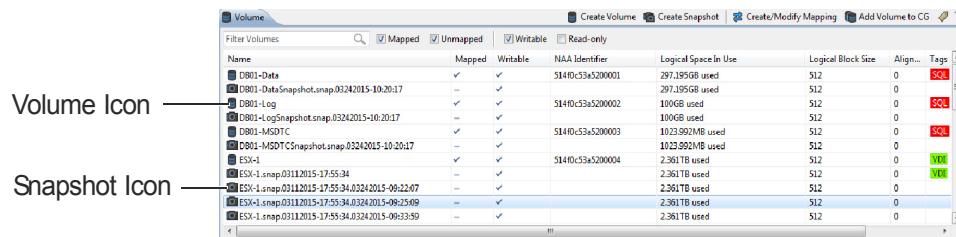
Viewing Volumes

Note: This procedure is used for Volumes and Snapshots.

To view Volumes and Snapshots:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab, double-click **Volumes** to open the Volume Tags list and display the Volume window.
3. If you wish to view only Volumes and Snapshots tagged by a specific Tag, click the Tag in the Volumes Tag list.

Note: The Volumes table includes both Volumes and Snapshots. Each object can be identified by its icon, as shown in [Figure 119](#).



Name	Mapped	Writable	NAA Identifier	Logical Space In Use	Logical Block Size	Align...	Tags
D801-Data	✓	✓	5140c3a5200001	297.195GB used	512	0	SQL
D801-DataSnapshot.snap.03242015-10-20:17	—	✓	5140c3a5200002	297.195GB used	512	0	SQL
D801-Log	✓	✓	5140c3a5200002	100GB used	512	0	SQL
D801-LogSnapshot.snap.03242015-10-20:17	—	✓	5140c3a5200003	100GB used	512	0	SQL
D801-MSDTC	✓	✓	5140c3a5200003	1023.992MB used	512	0	SQL
D801-MSDTCSSnapshot.snap.03242015-10-20:17	—	✓	5140c3a5200004	2.361TB used	512	0	NET
ESX-1	✓	✓	5140c3a5200004	2.361TB used	512	0	NET
ESX-1.snap.03112015-17-55-34	—	✓	5140c3a5200005	2.361TB used	512	0	NET
ESX-1.snap.03112015-17-55-34.03242015-09-22:07	—	✓	5140c3a5200006	2.361TB used	512	0	NET
ESX-1.snap.03112015-17-55-34.03242015-09-25:09	—	✓	5140c3a5200007	2.361TB used	512	0	NET
ESX-1.snap.03112015-17-55-34.03242015-09-33:59	—	✓	5140c3a5200008	2.361TB used	512	0	NET

Figure 119 Volumes and Snapshot Table

Viewing the Volume Performance

To view the Volume performance:

1. From the menu bar, click **Dashboard**.
2. Select the Bandwidth or IOPS tab to view performance according to those units.
3. In the **Most Active** section, make sure that **Volumes** is selected from the drop-down menu.

Note: You can view the top four most active Volumes in the Dashboard. To view the performance of all Volumes, use the [show-volumes](#) CLI command.

Viewing Volume Properties

Note: This procedure is used for Volumes and Snapshots.

To view Volume properties:

1. From the menu bar, click Configuration.
2. In the Virtual tab (left pane), click Volumes to display the Volumes window.

Name	Mapped	Writable	NAA Identifier	Logical Space In Use	Logical Block Size	Align...	Tags
DB01-Data	✓	✓	514f0c53a5200001	297.195GB used	512	0	SQL
DB01-DataSnapshot.snap.03242015-10:20:17	—	✓		297.195GB used	512	0	
DB01-Log	✓	✓	514f0c53a5200002	100GB used	512	0	SQL
DB01-LogSnapshot.snap.03242015-10:20:17	—	✓		100GB used	512	0	
DB01-MSDTC	✓	✓	514f0c53a5200003	1023.992MB used	512	0	SQL
DB01-MSDTCsnapshot.snap.03242015-10:20:17	—	✓		1023.992MB used	512	0	
ESX-1	✓	✓	514f0c53a5200004	2.361TB used	512	0	VDI
ESX-1.snap.03112015-17:55:34	—	✓		2.361TB used	512	0	VDI
ESX-1.snap.03112015-17:55:34.03242015-09:22:07	—	✓		2.361TB used	512	0	
ESX-1.snap.03112015-17:55:34.03242015-09:25:09	—	✓		2.361TB used	512	0	
ESX-1.snap.03112015-17:55:34.03242015-09:33:59	—	✓		2.361TB used	512	0	

Figure 120 Volumes Table

The Volumes table displays the following properties for each Volume:

- Volume name
- Cluster Name (in multiple clusters settings)
- Is Read Only
- Is mapped
- NAA identifier
- Space in Use (VSG)
- Volume Size
- Logical block size
- Alignment offset
- Tags

Renaming Volumes

Note: This procedure is used for Volumes and Snapshots.

To rename a Volume:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Volumes** to open the Volumes window.
3. Right-click the relevant Volume in the Volumes table and select **Rename** from the drop-down menu.

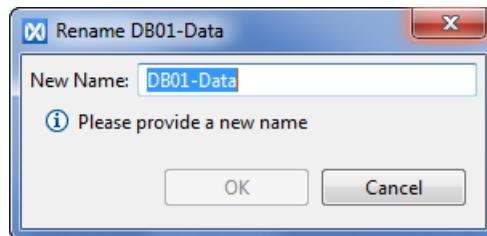


Figure 121 Rename Volume Dialog Box

4. In the Rename dialog box, enter the name for the Volume (up to 128 characters).
5. Click **OK**.

Modifying Volumes

Note: This procedure is used for Volumes and Snapshots.

The following Volume modifications can be made:

- ◆ Resize Volumes - Resizing a Volume (altering the amount of space allocated for the Volume) enables increasing¹ the size of mapped (exported) or unmapped volumes or Snapshots. Volumes do not have to be unmapped in order to be resized.
Resizing a volume with one or more Snapshots does not change the size of the existing Snapshots. Resizing a Snapshot does not change the size of its source entity.
- ◆ Enable or disable alerts:
 - Small I/O alerts
 - Unaligned I/O alerts
 - VAAI TP alerts

Note: Small I/O alerts, Unaligned alerts and VAAI TP alerts are described on [page 170](#).

1. The Resize feature in the current software version only enables increasing the Volume and Snapshot sizes.

To modify volume properties:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Volumes** to display the Volumes window.
3. Double-click the Volume you wish to modify; the **Modify Volume** dialog box is displayed (you can also right-click the Volume and select **Modify Volume** from the drop-down list).

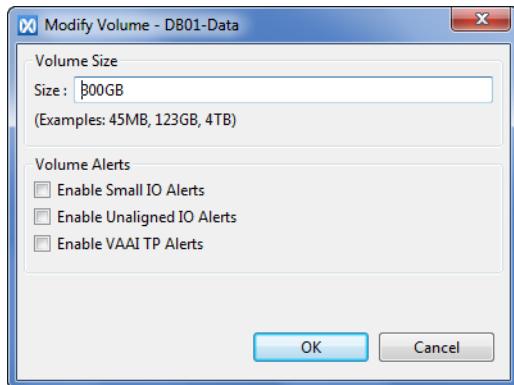


Figure 122 Modify Volume Dialog Box

4. Type the Volume size in the Size field:
 - Minimum Volume size is 1MB.
 - Size should be in multiples of 8KB.
 - Allowed units for allocation are KB, MB, GB, TB and PB.
5. Select or clear the Volume Alerts options to enable or disable the corresponding alerts.
6. Click **OK**.

Note: After resizing a Volume, the host must perform a full re-scan.

Deleting Volumes

Note: This procedure is used for Volumes and Snapshots.

Note: Mapped Volumes cannot be deleted. If you wish to delete mapped Volumes, unmap them prior to deletion.

To delete a Volume:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Volumes** to display the Volumes window.
3. Right-click the Volume you want to delete and select **Delete** from the drop-down menu. You can select multiple Volumes, using the Shift and Ctrl keys.

Note: To delete mapped Volumes, unmap the Volumes and then delete them.

Note: It is impossible to delete a Volume that is a member of a Consistency Group. All Volumes of the Consistency Group must be deleted.

4. Confirm the deletion by clicking **Yes**; the Volumes are deleted from the Volumes window.

Creating a Consistency Group

Consistency Groups (CG) are used to create a consistent image of a set of Volumes. Grouping multiple Volumes and Snapshots into a Consistency Group simplifies performing actions, such as creating Snapshots, and ensures that all Snapshots are created at the same point in time.

To create a Consistency Group:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Volumes** to display the Volumes window.
3. From the Volume list, select the Volumes/Snapshots you want to include in the Consistency Group. You can select multiple Volumes, using the Shift and Ctrl keys.
4. Right-click one of the selected Volumes and select **Create Consistency Group** from the drop-down menu.

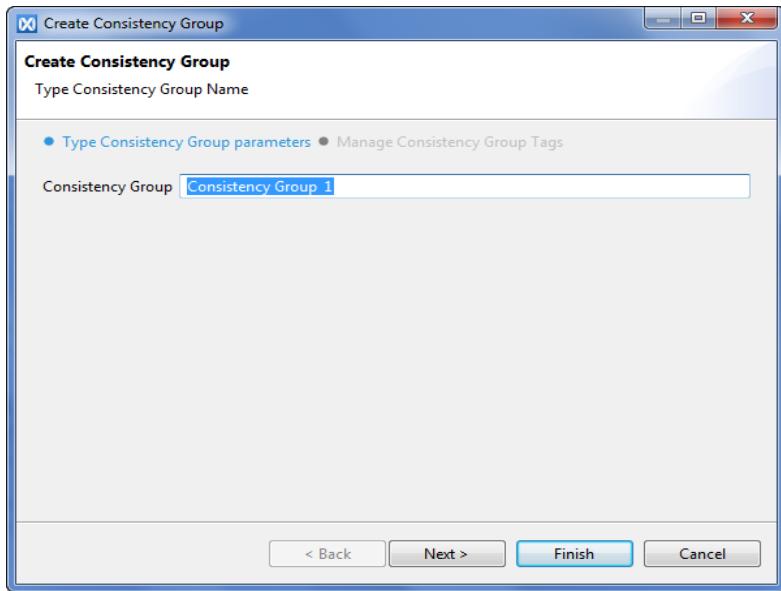


Figure 123 Create Consistency Group

5. In the Create Consistency Group dialog box, type a unique name for the Consistency Group.
6. If you do not wish to assign Tags to the new Consistency Group, skip to [step 12](#).

Note: You can assign Tags to the new Consistency Group after its creation is completed. See [“Assigning Tags to Storage Elements” on page 165](#).

- Click **Next** to assign Tags to the new Consistency Group.

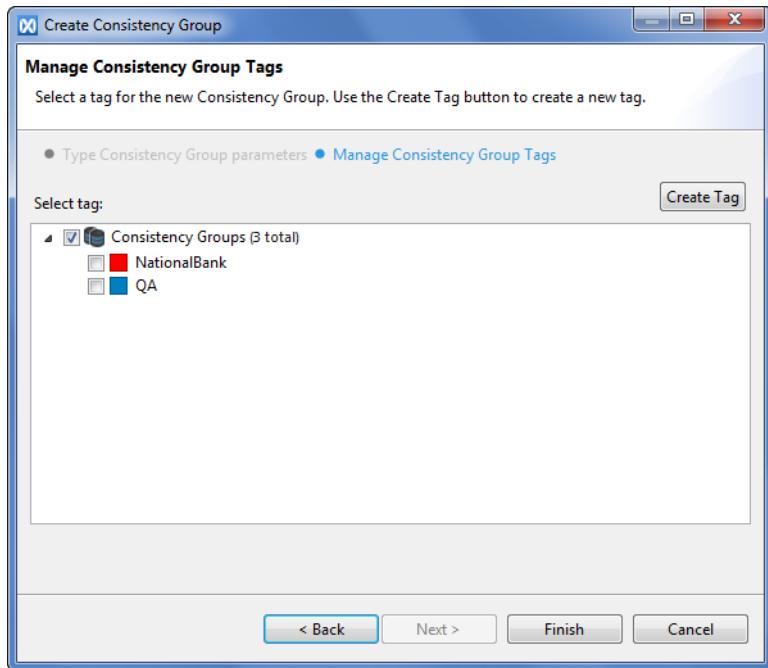


Figure 124 Create Consistency Group - Manage Tags

The Manage Consistency Group Tag window displays all Tags that are currently defined for Consistency Groups.

- Select the relevant Tag to assign it to the new Consistency Group. You can assign more than one Tag to a single Consistency Group.
- If you wish to create a new Consistency Group Tag click **Create Tag**.

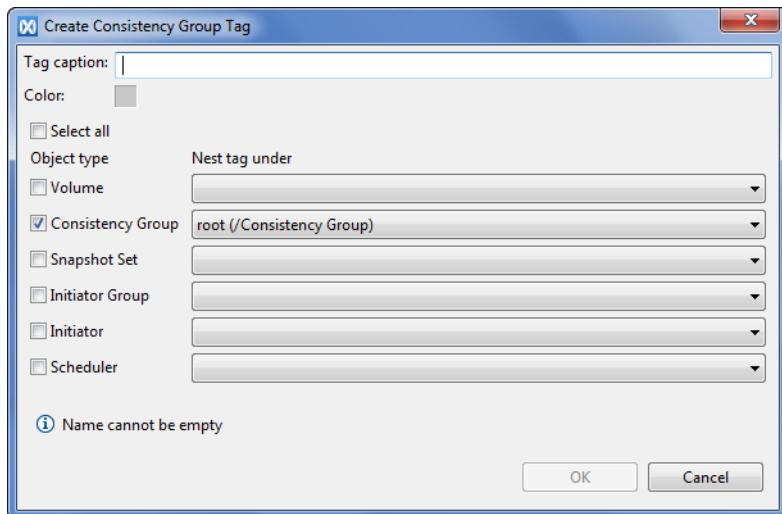


Figure 125 Create Consistency Group Tag

10. Set the Tag properties:

- Tag caption
- Tag color
- Tag nesting path
- Tag color

11. Click **OK**; the Tag is added to the Tag list in the Manage Consistency Group Tags dialog box. Select the new Tag to assign it to the Consistency Group.

Note: To create Tags not as part of the Consistency Group creation procedure, see [“Managing Tags, Using the GUI” on page 164](#).

12. Click **Finish**; the new Consistency Group is added to the Consistency Group table in the Consistency Group window.

Adding Volumes to a Consistency Group

To add Volumes to a Consistency Group:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Volumes** to display the Volumes window.
3. Select a Volume/Snapshot from the Volume list. You can select multiple Volumes, using the Shift and Ctrl keys.
4. In the Volume pane menu bar, click **Add Volume to Consistency Group**. You can also right-click the selected Volume and select **Add Volume to Consistency Group** from the drop-down menu.

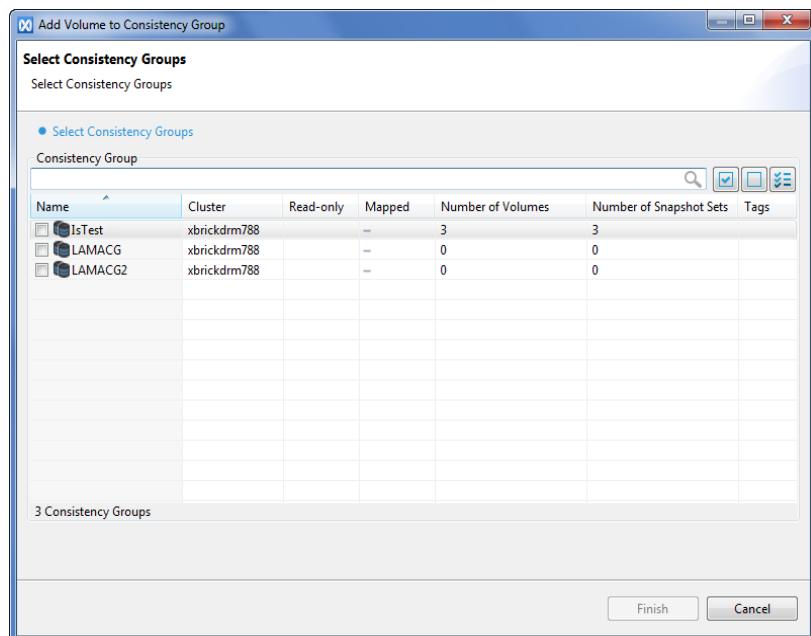


Figure 126 Add Volume to Consistency Group

5. Select the Consistency Groups to which you want to add the Volumes. You can select more than one Consistency Group, using the following options from the menu bar:
 - Type a text string to filter the displayed Consistency Group list.
 - Click the **Select All** icon to select all displayed Consistency Groups.
 - Click the **Deselect All** icon to revoke the Consistency Group selection.
 - Click the **Show All** icon  to display all defined Consistency Groups.
 - Click the **Show Only Selected** icon  to remove unselected Consistency Groups from the display.
6. Click **Finish**; the selected Volumes are added to the selected Consistency Groups.

Note: You can also add Volumes to a Consistency Group by first selecting a Consistency Group and then selecting Volumes to add to it. See “[Adding a Volume to a Consistency Group](#)” on page 218 for details.

Removing Volumes from a Consistency Group

Note: Removing a Volume from a Consistency Group prevents future Snapshots cross-consistency.

To remove Volumes from a Consistency Group:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Volumes** to open the Volumes window.
3. From the Volumes list, right-click a Volume/Snapshot from the Volume list that is a member of a Consistency Group and select **Remove Volume from Consistency Group** from the drop-down menu.

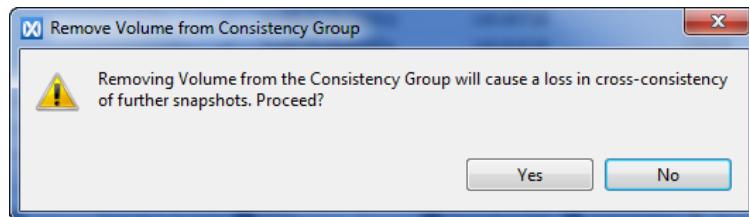


Figure 127 Remove Volume from Consistency Group - Warning

4. Click **Yes** to confirm; the Volume is removed from the Consistency Group.

Note: It is recommended to remove Volumes from a Consistency Group by first selecting a Consistency Group and then selecting Volumes to remove from it. See “[Removing a Volume from a Consistency Group](#)” on page 219 for details.

Creating a Snapshot Scheduler for Volumes or Snapshots

To create a Snapshot Scheduler:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Volumes** to display the Volumes window.
3. Select a Volume/Snapshot from the Volume list and click **Create Snapshot Scheduler** in the menu bar. You can also right-click the selected Volume and select **Create Snapshot Scheduler** from the drop-down list.

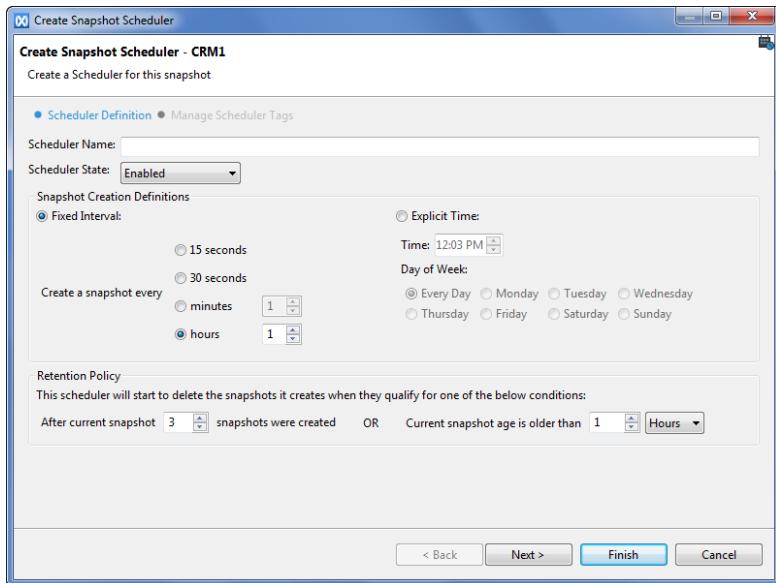


Figure 128 Create Snapshot Scheduler - Definition

4. In the Scheduler Definition dialog box, type in a unique name for the Scheduler.
5. The Scheduler is enabled by default. If you want to disable it, select **Disable** from the Scheduler State drop-down list.
6. In the Snapshot Creation Definitions, select whether you wish Snapshots to be created at a fixed interval or at a specified time.
7. If you selected the Fixed Interval option, set the time interval by selecting one of the following options:
 - 15 seconds
 - 30 seconds
 - Minutes (set the number)
 - Hours (set the number)
8. If you selected the Explicit Time option, set the time and select a day.
9. Set the Retention Policy:
 - Set the number of Snapshot that will be created before the current Snapshot is deleted.
 - Set the age limit in hours or days beyond which the current Snapshot is deleted.

10. If you do not wish to assign Tags to the new Scheduler, skip to [step 17](#).

Note: You can assign Tags to the Scheduler after the Scheduler creation is completed. See [“Assigning Tags to Storage Elements” on page 165](#).

11. Click **Next** to assign Tags to the new Scheduler.

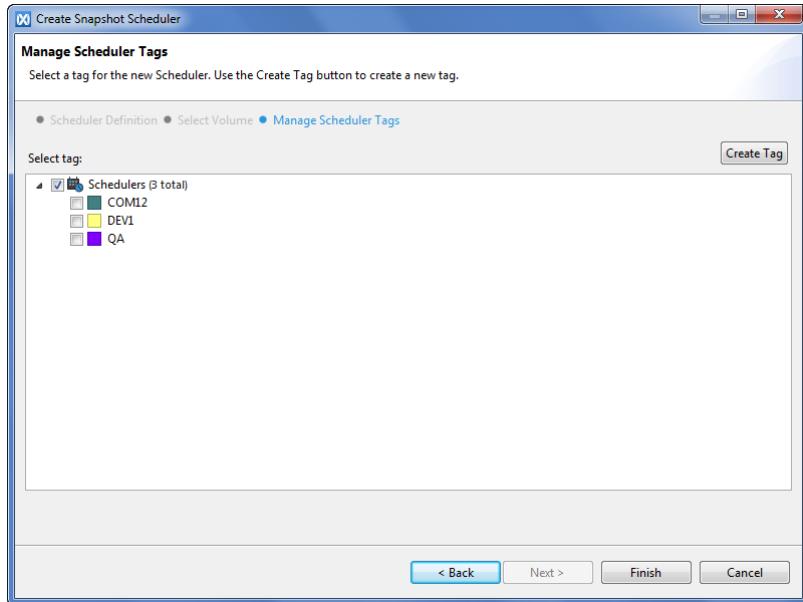


Figure 129 Create Snapshot Scheduler - Manage Tags

The Manage Scheduler Tags window displays all Tags that are currently defined for Schedulers.

12. Select the relevant Tag to assign it to the new Scheduler. You can assign more than one Tag to a single Scheduler.
13. If you wish to create a new Scheduler Tag, click **Create Tag**.

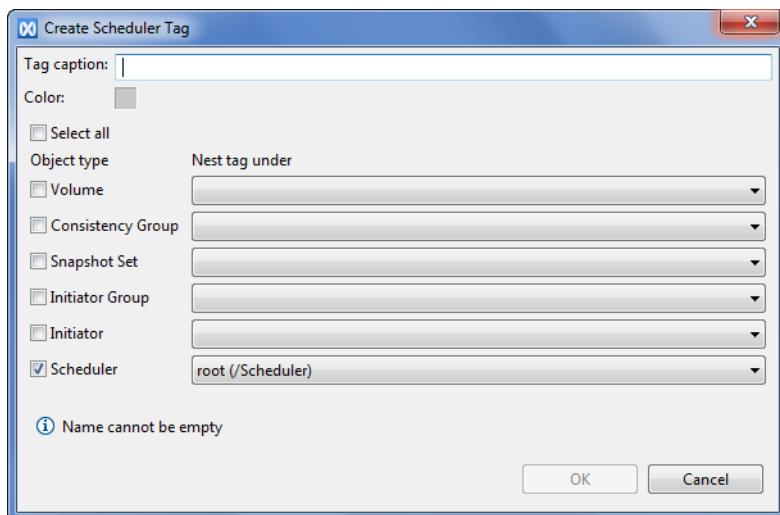


Figure 130 Create Scheduler Tag

14. Set the Tag properties:

- Tag caption
- Tag color
- Tag object type and nesting path

15. Click **OK**; the Tag is added to the Tag list in the Create Scheduler dialog box. Select the new Tag to assign it to the Scheduler.

Note: To create Tags not as part of the Volume creation procedure, see “[Managing Tags, Using the GUI](#)” on page 164.

16. Click **OK**.

17. Click **Finish**; the new Scheduler is added to the list in the Schedulers window and the new Snapshot Set that will contain all created snapshots is added to the Snapshot Set list in the Snapshot Sets window.

Mapping Volumes to Initiator Groups

Refer to “[Managing Mapping](#)” on page 253.

Restoring Data from a Snapshot

XtremIO enables your storage array to recover from data corruption by restoring the corrupted data from an undamaged backup copy (Snapshot), created at an earlier point in time. The restored Volume will contain the same data as the source backup.

To restore a production Volume, the Volume must have a read-only Snapshot, created at a point in time before the Volume's data was corrupted.

The restore operation uses the Snapshot to replace the corrupted production Volume without changing the SCSI face (NAA) of the restored entity. As a result, the corrupted Volume is restored without the need for remapping or rescanning on the host side.

Note: To enable restoring a Volume, unmount it before starting the restore procedure. After restoration is complete, re-mount the restored Volume.

Note: If the Volume you wish to restore is a member of a Consistency Group, it cannot be restored outside of the CG's context. Therefore, the entire Consistency Group must be restored.

Note: Data can be restored only from Read-Only source Volumes.

To restore a Volume's data from a Snapshot:

1. From the menu bar, click Configuration.
2. In the Virtual tab (left pane), click Volumes to display the Volumes window.
3. In the Volume list, right-click the Volume whose data you wish to restore, and click **Restore from Snapshot** from the drop-down list.

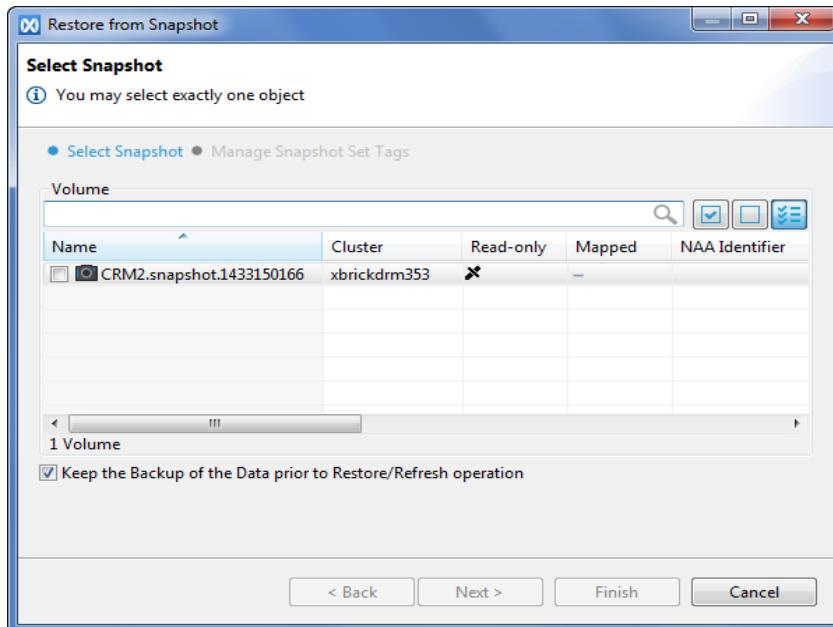


Figure 131 Restore from Snapshot - Select Snapshot

The Volume table displays the Snapshots taken for the specified Volume.

4. From the table, select a Snapshot you want to use as the source for restoring the Volume's data. Use the following options from the menu bar:
 - Type a text string to filter the displayed Snapshot list.
 - Click the **Select All** icon to select all displayed Snapshots.
 - Click the **Deselect All** icon to revoke the Snapshot selection.
 - Click the **Show All**  to display all defined Snapshots.
 - Click the **Show Only Selected** icon  to remove the unselected Snapshots from the display.

Note: You can select only one Snapshot from the list.

5. The Snapshot selected as the source for restoring data is kept by default. If you want to remove it, clear the **Keep the backup of the Data prior to Restore/Refresh operation** option.
6. If you do not wish to assign Tags to the created Snapshot, skip to [step 12](#).

Note: You can assign Tags to the Snapshot after the Snapshot creation is completed. See "[Assigning Tags to Storage Elements](#)" on page 165.

7. Click **Next** to assign Tags to the Snapshot Set.

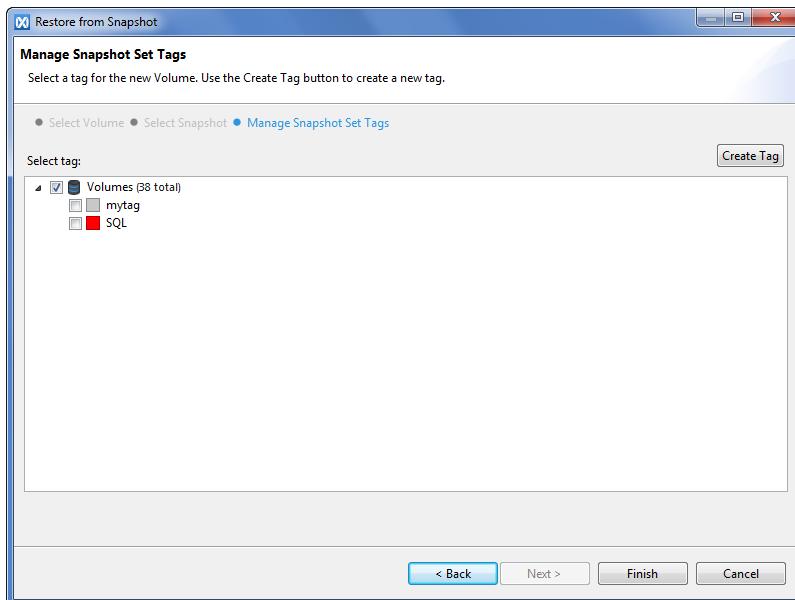


Figure 132 Restore from Snapshot - Manage Tags

The Manage Snapshot Sets Tags window displays all the Tags that are currently defined for Snapshot Sets.

8. Select the relevant Tag to assign it to the new Snapshot Set. You can assign more than one Tag to a single Snapshot Set.

9. If you wish to create a new Snapshot Set Tag click **Create Tag**.

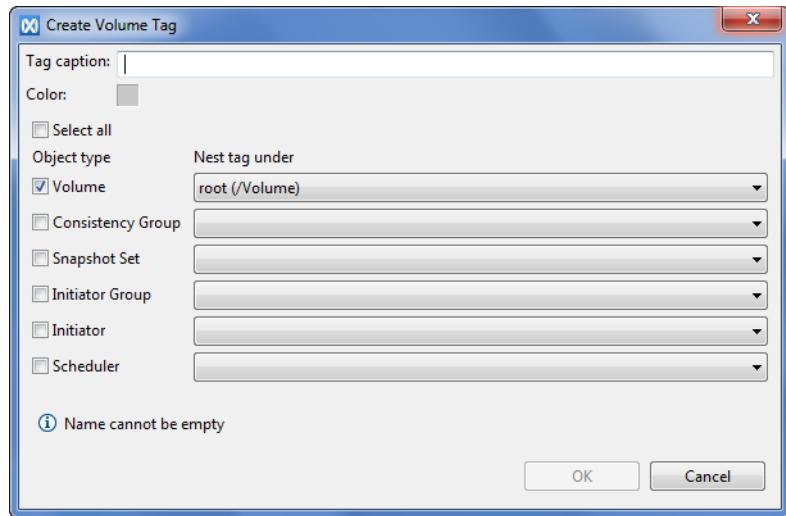


Figure 133 Create Volume Tag

10. Set the Tag properties:

- Tag caption
- Tag color
- Tag object type and nesting path

11. Click **OK**; the Tag is added to the Tag list in the Manage Snapshot Set Tags dialog box. Select the new Tag to assign it to the Snapshot Set.

Note: To create Tags not as a part of the restore from Snapshot procedure, see [“Managing Tags, Using the GUI” on page 164](#).

12. Click **Finish**; the new Snapshot Set is added to the Snapshot Set list and the new (restore) Snapshot is displayed in the Volumes table.

Refreshing a Volume

XtremIO enables you to take a Snapshot of an existing storage object, and later refresh the Snapshot data to match that of the source object's current state without the need to explicitly change the mapping and zoning of the host.

The refresh operation replaces an outdated storage object with an updated version without changing the SCSI face (NAA) of the refreshed object. As a result, the outdated object is refreshed without the need for remapping or rescanning on the host side.

The following examples are use cases that are supported by Refresh:

- ◆ Backup of production environment/Data Warehouse/Real-Time Analytics: A Snapshot Set taken of a Consistency Group with production Volumes, is mapped to a different host at a certain point in time, and then becomes periodically refreshed with data from the source Consistency Group with production Volumes.
- ◆ Refresh 'Development and Test' environments from a 'master copy' made from the production environment: The 'master copy' is a Snapshot Set taken at a certain point in time from the Consistency Group with production Volumes, and the Development and Test environment is a Snapshot Set that was initially taken from the production Consistency Group or the initial 'master copy', and is mapped to a different host. The Development and Test environment becomes refreshed periodically from a new master copy that was created from the production environment.

The refresh operation can be applied in the following cases:

- ◆ Refreshing a Snapshot with an updated source Volume
- ◆ Refreshing a source Volume with a Snapshot
- ◆ Refreshing a Snapshot with another Snapshot

Note: Before applying the refresh procedure, unmount the refreshed object. After refresh is complete, re-mount the refreshed object.

Note: If the Volume you wish to refresh is a member of a Consistency Group, it cannot be refreshed outside of the Consistency Group's context. Therefore, the entire Consistency Group must be refreshed.

To refresh a Snapshot:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Volumes** to display the Volumes window.
3. In the Volume list, right-click the Snapshot whose data you wish to refresh and click **Refresh** from the drop-down list.

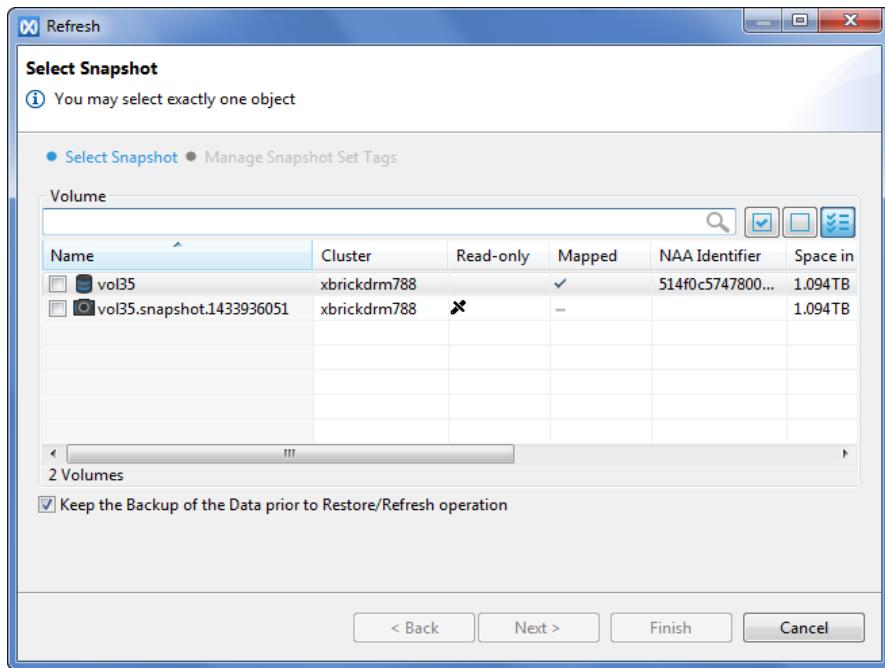


Figure 134 Refresh - Select Snapshot

The Select Snapshot window displays the selected Snapshot's source Volume and all Snapshots of the source Volume.

4. Select the Snapshot or Volume you want to use for refreshing the Snapshot, using the following options from the menu bar:
 - Type a text string to filter the displayed Snapshot list.
 - Click the **Select All** icon to select all displayed Snapshots.
 - Click the **Deselect All** icon to revoke the Snapshot selection.
 - Click the **Show All** icon to display all defined Snapshots.
 - Click the **Show Only Selected** icon to remove the unselected Snapshot from the display.

Note: You can select only one object from the list.

5. The Snapshot used as a source for refreshing the data is kept by default. If you want to remove it, clear the **Keep the backup of the Data prior to Restore/Refresh operation** option.

6. If you do not wish to assign Tags to the created Snapshot, skip to [step 12](#).

Note: You can assign Tags to the Snapshot after the Snapshot creation is completed. See [“Assigning Tags to Storage Elements” on page 165](#).

7. Click **Next** to assign Tags to the Snapshot.

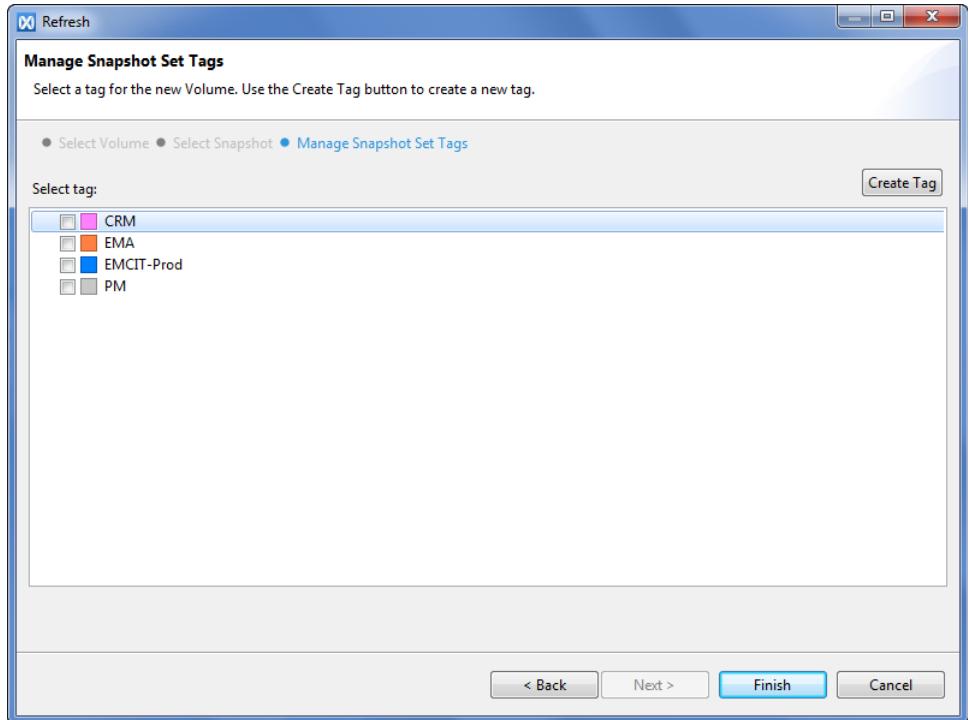
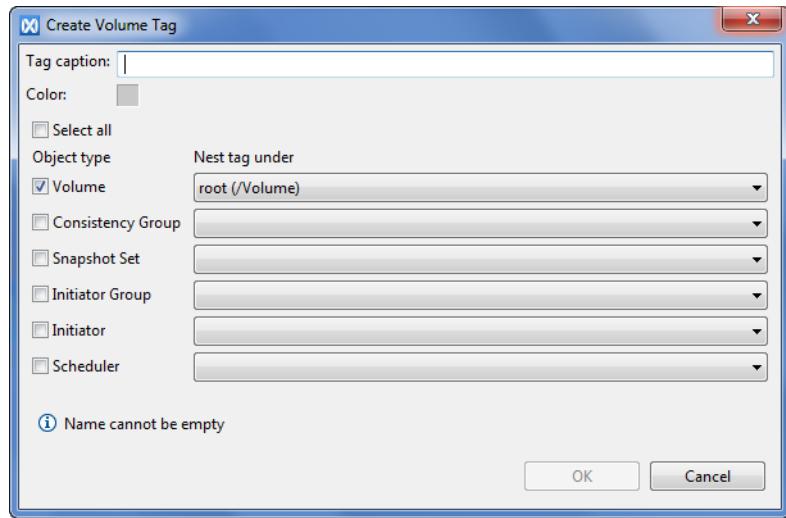


Figure 135 Refresh - Manage Tags

The Manage Snapshot Sets Tags window displays all Tags that are currently defined for Snapshot Sets.

8. Select the relevant Tag to assign it to the new Snapshot Set. You can assign more than one Tag to a single Snapshot Set.

9. If you wish to create a new Snapshot Set Tag, click **Create Tag**.



10. Set the Tag properties:

- Tag caption
- Tag identifying color
- Tag object type and nesting path

11. Click **OK**; the Tag is added to the Tag list in the Manage Snapshot Set Tags dialog box. Select the new Tag to assign it to the Snapshot Set.

Note: To create Tags not as part of the restore from Snapshot procedure, see [“Managing Tags, Using the GUI” on page 164](#).

12. Click **Finish**; the new (refresh) Snapshot is added to the Volumes table.

Viewing the Volumes-Related Information

The Volumes Window displays, in addition to the defined Volumes and Snapshots, additional related information. The following information is available in the pane below the Volumes table:

- ◆ Mapping
- ◆ Consistency Groups
- ◆ Snapshot Sets
- ◆ Volume Snapshot Groups
- ◆ Schedulers
- ◆ Alerts

To view the mapping information:

- ◆ Select a Volume and click the **Mapping** tab.

Volumes \ Initiator Groups	
CRM4Snap1	

Selected 1 Volume mapped to 0 IGs

Figure 136 Mapping Tab

The Mapping tab displays the following data:

- Volume
- Initiator Group

To view the Consistency Group information:

- ◆ Select a Volume and click the **Consistency Groups** tab.

Name	Cluster	Read-only	Mapped	Number of Volumes	Number of Snapshot Sets	Tags
0 Consistency Groups of 1 Volume						

101 Volumes displayed (101 in xbrickdrm788; 166 total)
1 selected
Filters : Cluster: xbrickdrm788

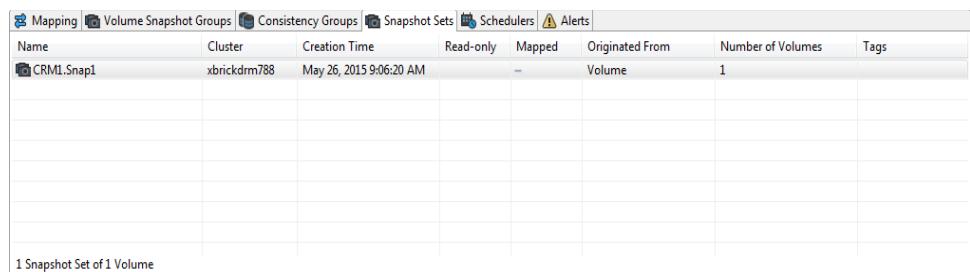
Figure 137 Consistency Groups Tab

The Consistency Groups tab displays the following data:

- Name
- Cluster
- Read-only
- Mapped
- Number of Volumes
- Number of Snapshot Sets
- Tags

To view the Snapshot Set information:

- ◆ Select a Volume and click the **Snapshot Sets** tab.



Name	Cluster	Creation Time	Read-only	Mapped	Originated From	Number of Volumes	Tags
CRM1.Snap1	xbrickdrm788	May 26, 2015 9:06:20 AM	—	Volume	1		

1 Snapshot Set of 1 Volume

Figure 138 Snapshot Sets Tab

The Snapshot Sets tab displays the following data:

- Name
- Cluster
- Creation Time
- Read-only
- Mapped
- Originated From
- Number of Volumes
- Tags

To view the Volume Snapshot Groups information:

- ◆ Select a Volume and click the **Volume Snapshot Groups** tab.

Name	Total Volumes	Include Hidden	Allocated Size	Space in Use (VSG)	Total Logical Vols	Thin Provisioning Ratio	Number of Internal Volumes
Volume Snapshot Group for volume: CRM2	5	No	5GB	0 bytes	0 bytes	0	0
CRM2	5	No	5GB	0 bytes	0 bytes	0	0

Figure 139 Volume Snapshot Groups Tab

The Volume Snapshot Groups tab displays the following data:

- VSG Name and Volume/Snapshot nesting
- Total Volumes
- Include hidden Volumes
- Allocated Size
- Space in Use (VSG)
- Total Logical Volumes Size
- Thin Provisioning Ratio
- Number of Internal Volumes
- Max Snapshot Reached
- Snapshot Removal in Progress

To view the Schedulers information:

- ◆ Select a Volume and click the **Schedulers** tab.

Scheduler Name	Cluster	Snapshot Sour...	Snapshot Type	Interval	Explicit Schedule	Snapshots to K...	Snapshots to T...	Last Activation Ti...
0 Schedulers of 1 Volume								

Figure 140 Schedulers Tab

The Schedulers tab displays the following data:

- Scheduler Name
- Cluster
- Snapshot Source Name
- Snapshot Source Type
- Snapshot Type
- Interval
- Explicit Schedule
- Snapshots to Keep - Number
- Snapshots to Keep - Time
- Last Activation Time
- Last Activation State
- Scheduler State
- Tags

To view the alerts information:

- ◆ Select a Volume and click the **Alerts** tab.

Severity	Cluster	Code	Date and Time	Entity	Entity Details	Description
0 Alerts						

Figure 141 Alerts Tab

The Alerts tab displays the following data:

- Severity
- Cluster
- Code
- Date and Time
- Entity
- Entity Details
- Description

Managing Volumes and Snapshots, Using the CLI

Use the following CLI commands for managing Volumes and Snapshots:

Command	Description
add-volume	Creates and adds a new Volume.
remove-volume	Removes a Volume.
modify-volume	Modifies a Volume's parameters.
show-volume	Displays the specified Volume's information.
show-volumes	Displays a list of Volumes/Snapshots (including properties of each), and the Volume Snapshot Group Index each Volume/Snapshot belongs to.
create-snapshot	Creates a Snapshot from a specified Volume.
create-snapshot-and-reassign	Creates a Snapshot from a specified Volume/Snapshot, Consistency Group, or Snapshot Sets and reassigns the Volume identity characteristic to the created Snapshot.
show-volume-snapshot-groups	Displays the Volume Snapshot Group and its members.
add-volume-to-consistency-group	Adds a Volume to a Consistency Group.
create-scheduler	Creates a new Snapshot Scheduler.
show-snapshots	Displays a list of Snapshots and related information.
map-lun	Maps a Volume to an Initiator Group and assigns a Logical Unit Number (LUN) to it.

Managing the Consistency Groups

A Consistency Group is a set of Volumes and Snapshots. Using Consistency Groups enables logically grouping together storage objects and simultaneously manipulating all members of the group (for example, creating cross-consistent Snapshots on several Volumes that serve a single database).

This section explains how to manage Consistency Groups.

Managing Consistency Groups, Using the GUI

Creating a Consistency Group

To create a Consistency Group:

1. From the menu bar, click Configuration.
2. In the Virtual tab, click **Consistency Groups** to open the Consistency Groups window.
3. From the Consistency Groups window menu bar, click **Create Consistency Group**. You can also right-click Consistency Groups in the Virtual tab and select **Create Consistency Group**.

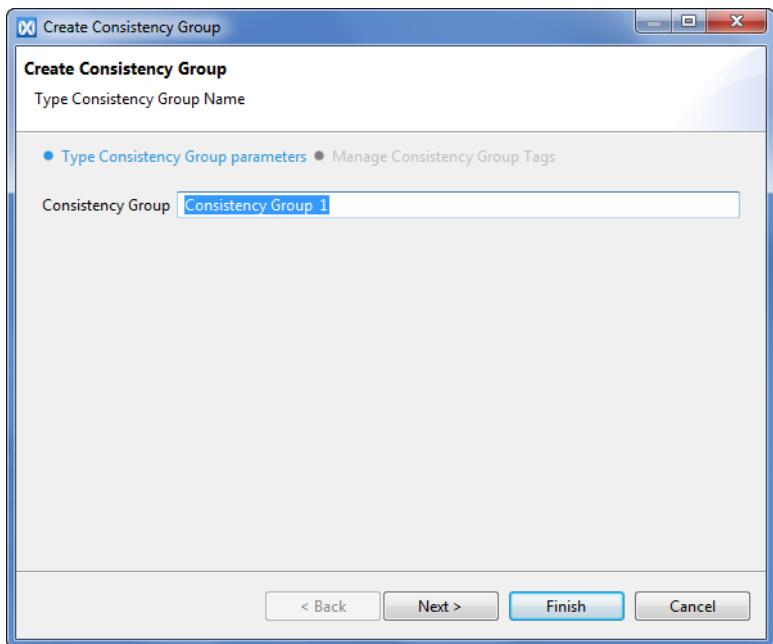


Figure 142 Create Consistency Group

4. Type a unique name for the Consistency Group.
5. If you do not wish to assign Tags to the new Consistency Group, skip to [step 11](#)

Note: You can assign Tags to the new Consistency Group after its creation is completed. See “[Assigning Tags to Storage Elements](#)” on page 165

- Click **Next** to assign Tags to the new Consistency Group.

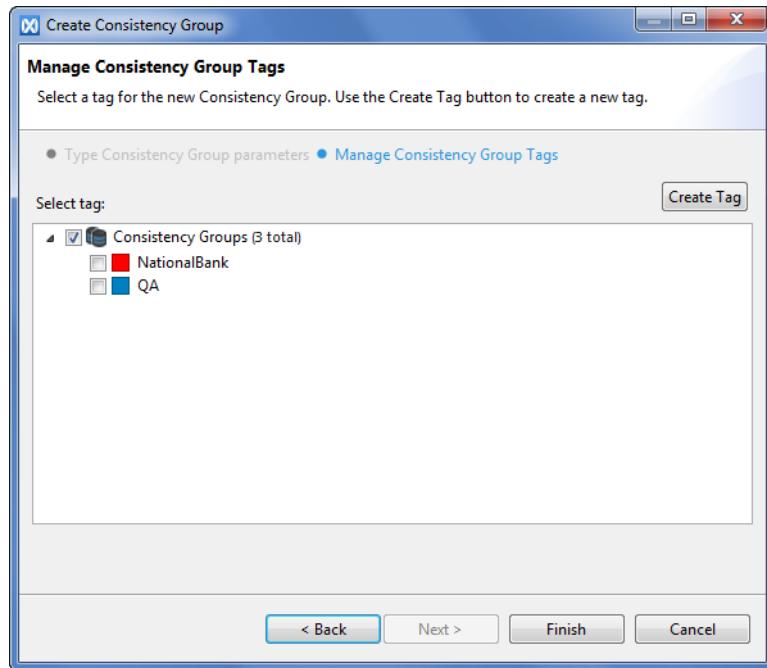


Figure 143 Create Consistency Group - Manage Tags

The Manage Consistency Group Tag window displays all the Tags that are currently defined for Consistency Groups.

- Select the relevant Tag to assign it to the new Consistency Group. You can assign more than one Tag to a single Consistency Group.
- If you wish to create a new Consistency Group Tag, click **Create Tag**.

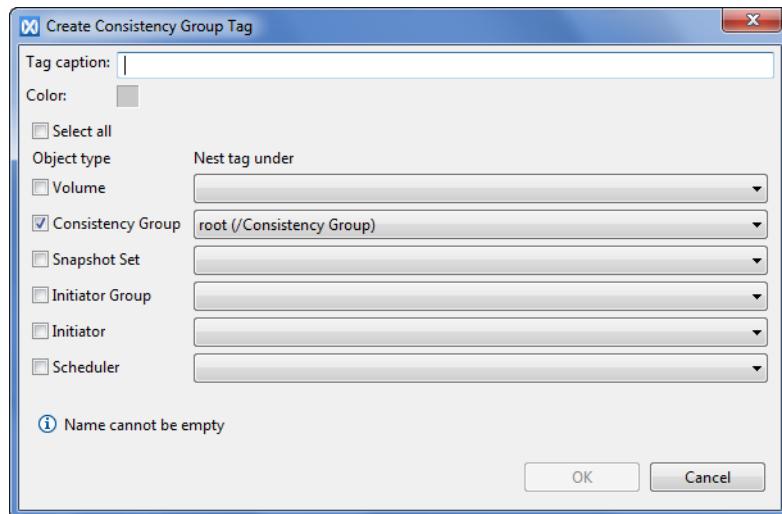


Figure 144 Create Consistency Group Tag

9. Set the Tag properties:

- Tag caption
- Tag color
- Tag object and nesting path

10. Click **OK**; the Tag is added to the Tag list in the Manage Consistency Group Tags dialog box. Select the new Tag to assign it to the Consistency Group.

Note: To create Tags not as part of the Consistency Group creation procedure, see [“Managing Tags, Using the GUI” on page 164](#).

11. Click **Finish**; the new Consistency Group appears in the Consistency Group table in the Consistency Group window.

Creating a Snapshot of a Consistency Group

A Snapshot of a Consistency Group is a Snapshot Set where all Snapshots are taken at the same point in time.

To create a Snapshot of a Consistency Group:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab, click **Consistency Groups** to open the Consistency Group view.
3. Right-click a Consistency Group and select **Create Snapshot** from the drop-down menu.

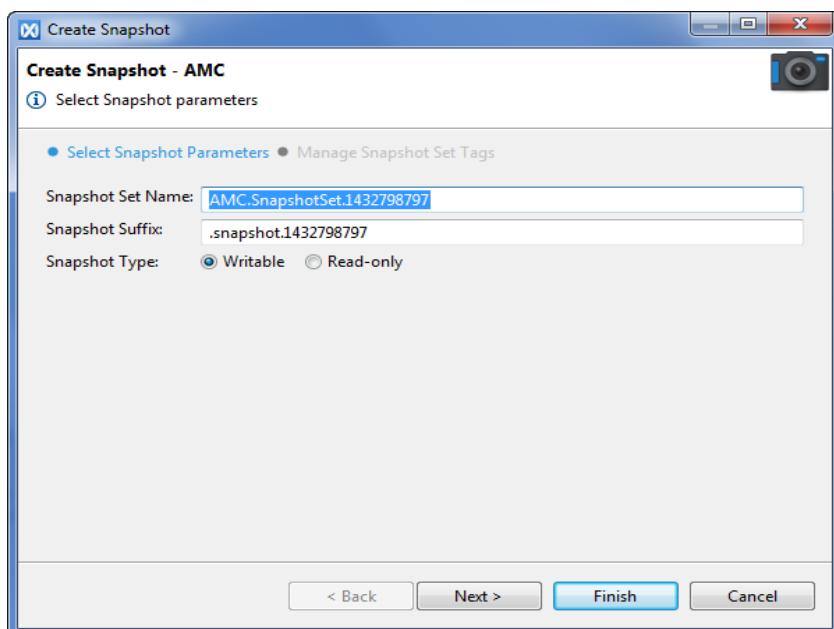


Figure 145 Create Consistency Group Snapshot - Snapshot Parameters

4. In the Select Snapshot Parameters window, configure the following:
 - Snapshot Set name (default name - <Consistency Group name>.SnapshotSet.<EPOCH>)
 - Snapshot suffix (default suffix - .snapshot.<EPOCH>)
 - Snapshot type (Writable or Read-only)
5. If you do not wish to assign Tags to the new Snapshot, skip to [step 11](#).

Note: You can assign Tags to the new Snapshot after its creation is completed. See [“Assigning Tags to Storage Elements” on page 165](#).

6. Click **Next** to assign Tags to the new Snapshot.

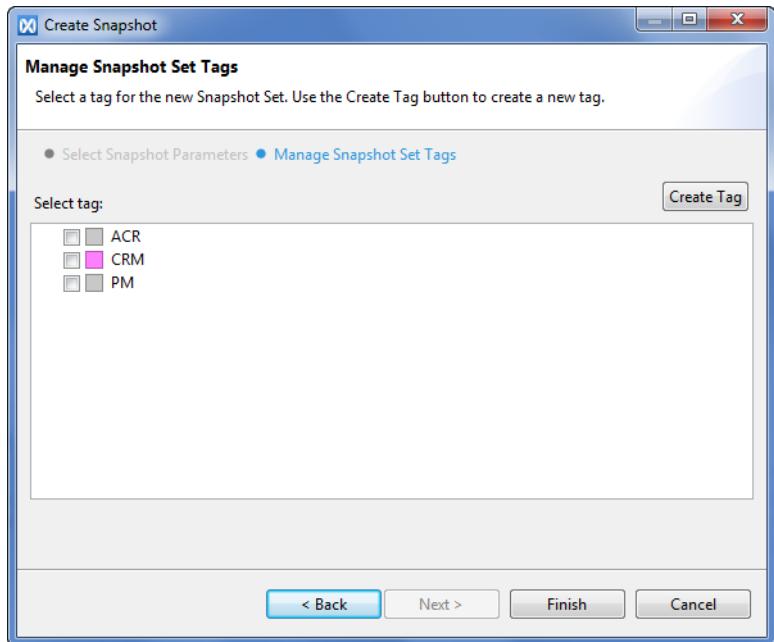


Figure 146 Create Consistency Group Snapshot - Manage Tags

The Manage Snapshot Set Tags window displays all the Tags that are currently defined for Snapshot Sets.

7. Select the desired Tag to assign it to the new Snapshot Set. You can assign more than one Tag to the Snapshot Set.

8. If you wish to create a new Snapshot Set Tag, click **Create Tag**.

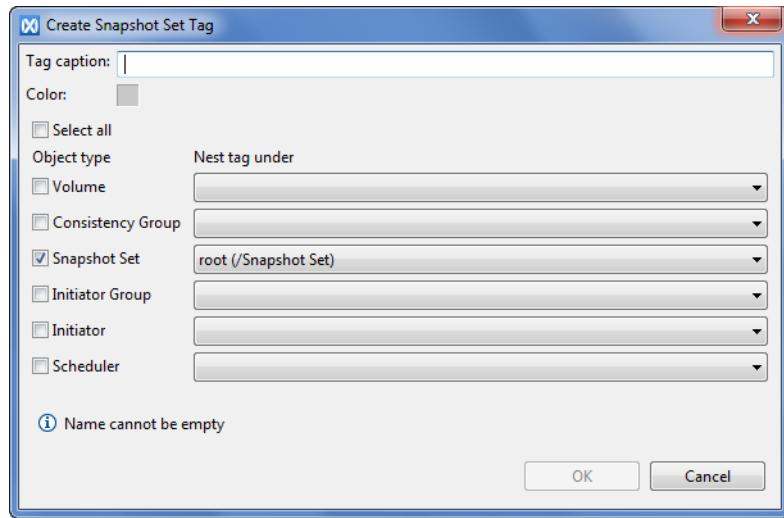


Figure 147 Create Snapshot Set Tag

9. Set the Tag properties:
 - Tag caption
 - Tag color
 - Tag object and nesting path
 10. Click **OK**; the Tag is added to the Tag list in the Manage Snapshot Set Tags dialog box. Select the new Tag to assign it to the Snapshot Set.
- Note:** To create Tags not as part of the Consistency Group Snapshot procedure, see "[Managing Tags, Using the GUI](#)" on page 164.
11. Click **Finish**; the new Snapshot Set appears in the Snapshot Set table in the Snapshot Set window.

Creating a Snapshot Scheduler for Consistency Groups

To create a Snapshot Scheduler for Consistency Group Snapshots:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Consistency Groups**.
3. Select a Consistency Group from the Volume list and click **Create Snapshot Scheduler** in the menu bar. You can also right-click the selected Consistency Group and select **Create Snapshot Scheduler** from the drop-down list.

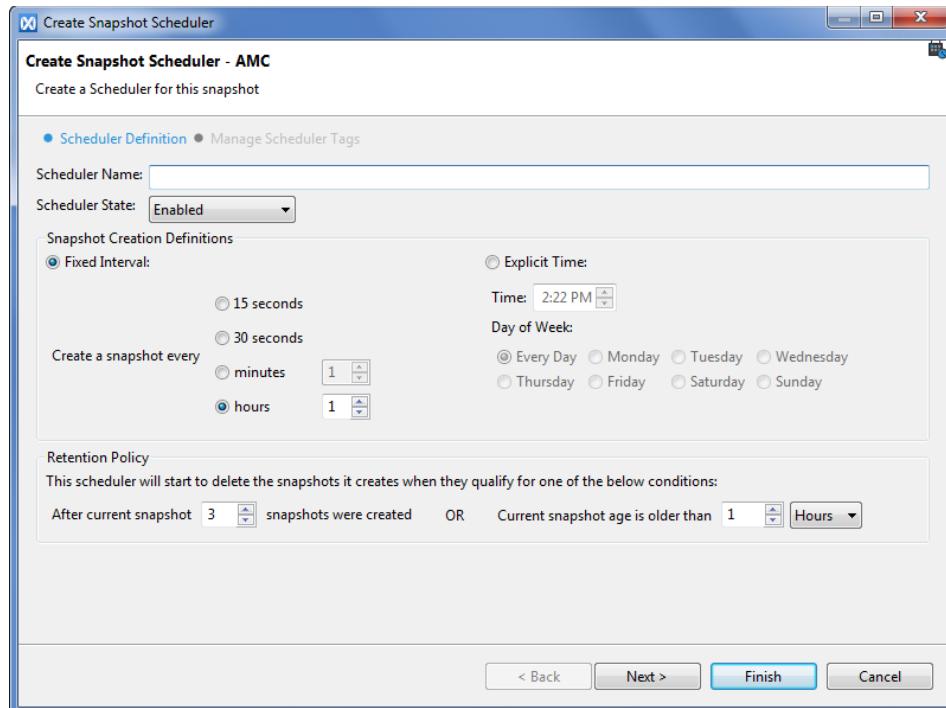


Figure 148 Create Snapshot Scheduler - Definition

4. In the Scheduler Definition dialog box, type a unique name for the Scheduler.
5. The Scheduler is enabled by default. If you want to disable it, select **Disable** from the Scheduler State drop-down list.
6. In the Snapshot Creation Definitions, select whether you wish Snapshots to be created at a fixed interval or at a specified time.
7. If you selected the Fixed Interval option, set the time interval by selecting one of the following options:
 - 15 seconds
 - 30 seconds
 - Minutes (set the number)
 - Hours (set the number)
8. If you selected the Explicit Time option, set the time and select a day.

9. Set the Retention Policy:

- Set the number of Snapshot that will be created before the current Snapshot is deleted.
- Set the age limit in hours or days beyond which the current Snapshot is deleted.

10. If you do not wish to assign Tags to the new Scheduler, skip to [step 17](#).

Note: You can assign Tags to the Scheduler after the Scheduler creation is completed. See [“Assigning Tags to Storage Elements” on page 165](#).

11. Click **Next** to assign Tags to the new Scheduler.

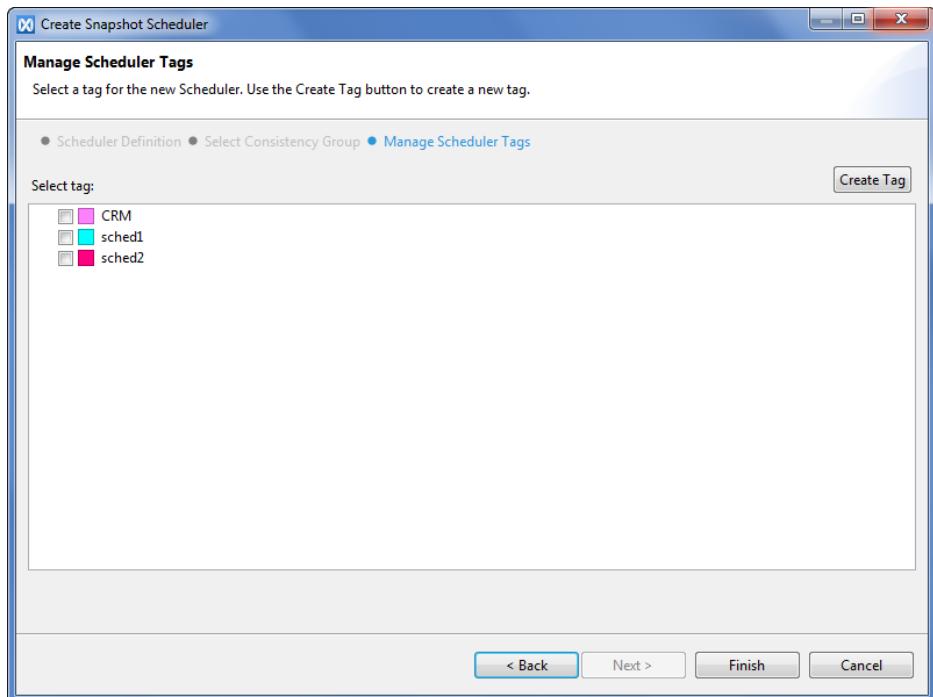


Figure 149 Create Snapshot Scheduler - Manage Tags

The Manage Scheduler Tags window displays all Tags that are currently defined for Schedulers.

12. Select the relevant Tag to assign it to the new Scheduler. You can assign more than one Tag to a single Scheduler.

13. If you wish to create a new Scheduler Tag click **Create Tag**.

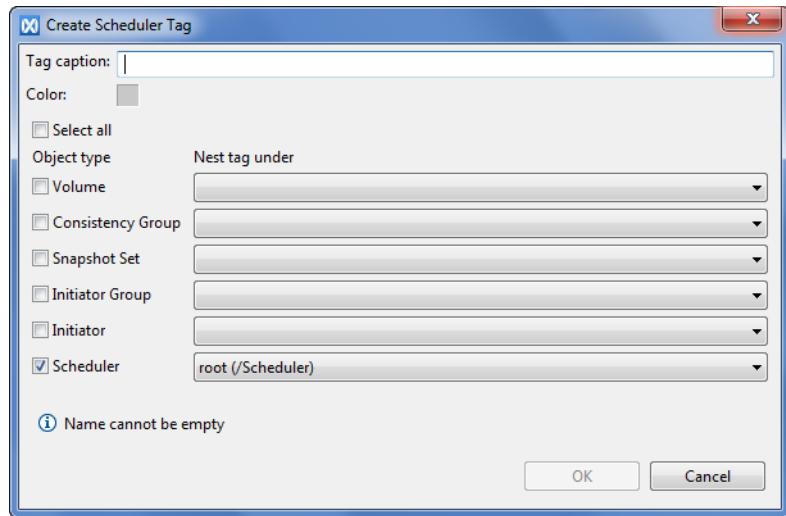


Figure 150 Create Scheduler Tag

14. Set the Tag properties:

- Tag caption
- Tag color
- Tag object and nesting path

15. Click **OK**; the Tag is added to the Tag list in the Create Scheduler dialog box. Select the new Tag to assign it to the Scheduler.

Note: To create Tags not as part of the Scheduler creation procedure, see “[Managing Tags, Using the GUI](#)” on page 164.

16. Click **OK**.

17. Click **Finish**; the new Scheduler is added to the list in the Schedulers window.

Restoring a Consistency Group from a Snapshot Set

XtremIO enables you to recover from data corruption of a Consistency Group by restoring the corrupted data from an undamaged backup copy (Snapshot Set) created in an earlier point in time. The restored Consistency Group will contain the same data as the Snapshot Set backup.

To restore a production Consistency Group, there must be a read-only Snapshot Set created at a point in time before the Consistency Group's data was corrupted.

The restore operation uses the Snapshot Set to replace the corrupted production Consistency Group without changing the SCSI face (NAA) of the restored entity. As a result, the corrupted Consistency Group is restored without the need for remapping or rescanning on the host side.

Note: To enable restoring a Consistency Group, unmount it before starting the restore procedure. After restoration is complete, re-mount the restored Volumes.

Note: Data can be restored only from Read-Only source Snapshot Sets.

To restore a Consistency Group from a Snapshot Set:

1. From the menu bar, click Configuration.
2. In the Virtual tab (left pane), click Consistency Groups.
3. In the Consistency Group list, right-click the Consistency Group whose data you wish to restore and click Restore from Snapshot from the drop-down list.

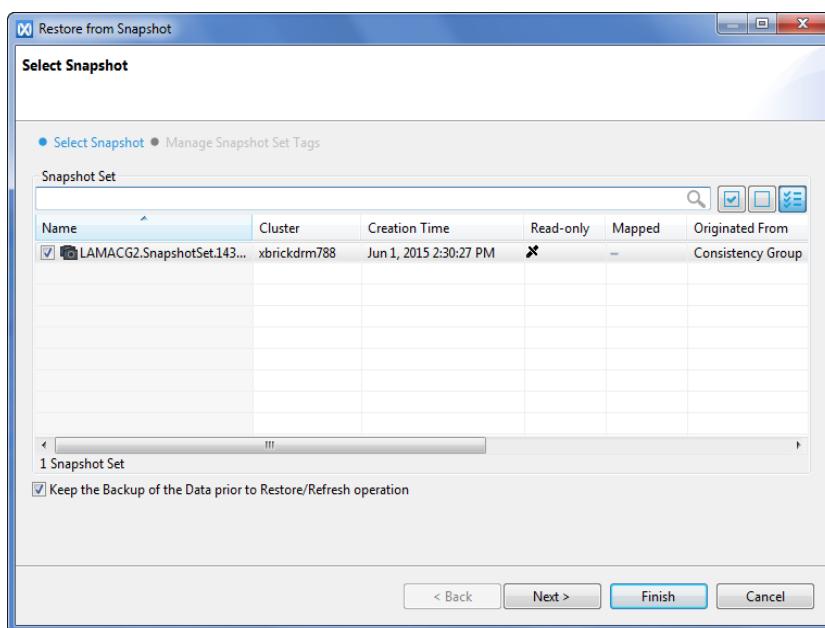


Figure 151 Restore from Snapshot - Select Snapshot

The Select Snapshot window displays all Snapshot Sets generated for the selected Consistency Group.

4. Select a Snapshot Set to be the source of the restore Snapshot, using the following options from the menu bar:
 - Type a text string to filter the displayed Snapshot list.
 - Click the **Select All** icon to select all displayed Snapshots.
 - Click the **Deselect All** icon to revoke the Snapshot selection.
 - Click the **Show All** icon  to display all defined Snapshots.
 - Click the **Show Only Selected** icon  to remove the unselected Snapshot from the display.

Note: You can only select one Snapshot Set from the list.

5. The source of the Snapshot is kept by default. If you want to remove it, clear the **Keep the backup of the Data prior to Restore/Refresh operation** option.
6. If you do not wish to assign Tags to the created Snapshot Set, skip to [step 12](#).

Note: You can assign Tags to the Snapshot Set after the Snapshot creation is completed. See “[Assigning Tags to Storage Elements](#)” on page 165.

7. Click **Next** to assign Tags to the Snapshot Set.

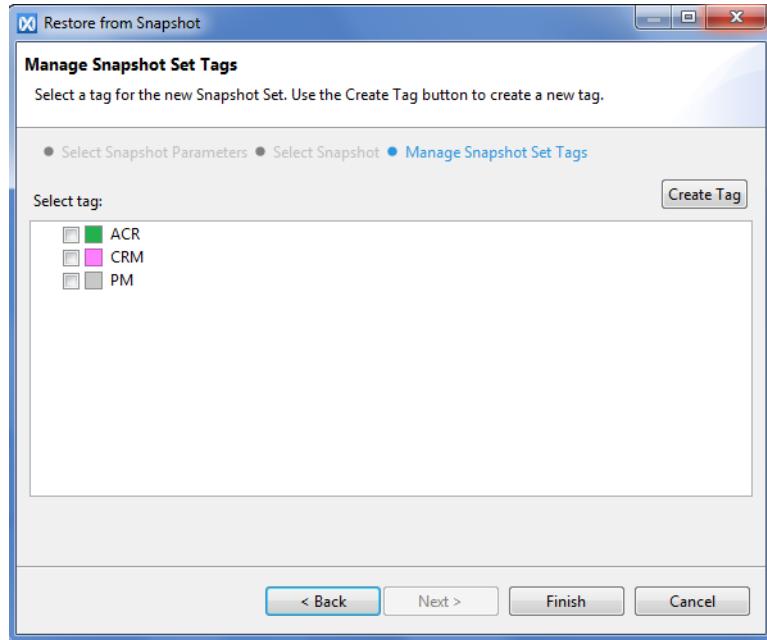


Figure 152 Restore from Snapshot - Manage Tags

The Manage Snapshot Sets Tags window displays all Tags that are currently defined for Snapshot Sets.

8. Select the relevant Tag to assign it to the new Snapshot Set. You can assign more than one Tag to a single Snapshot Set.

9. If you wish to create a new Snapshot Set Tag, click **Create Tag**.

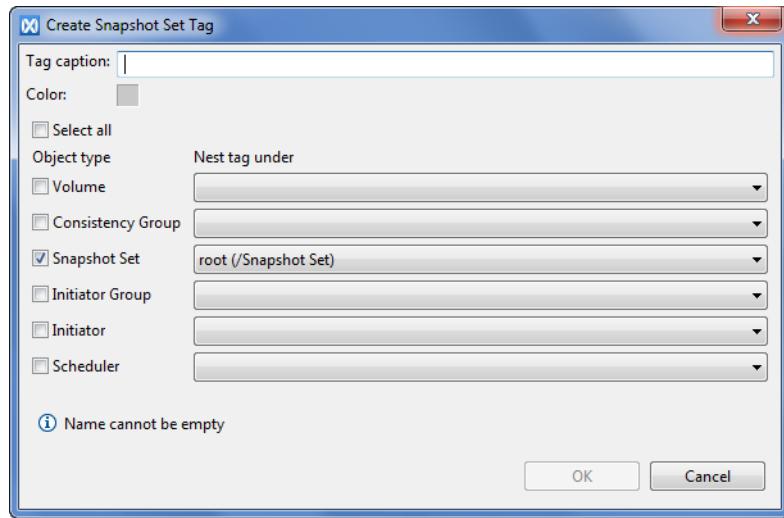


Figure 153 Create Snapshot Set Tag

10. Set the Tag properties:

- Tag name
- Tag nesting path
- Tag color

11. Click **OK**; the Tag is added to the Tag list in the Manage Snapshot Set Tags dialog box. Select the new Tag to assign it to the Snapshot Set.

Note: To create Tags not as part of the restore from Snapshot procedure, see [“Managing Tags, Using the GUI” on page 164](#).

12. Click **Finish**; The new (restore) Snapshot Set is added to the Snapshot Set table.

Refreshing a Consistency Group

XtremIO enables you to take a Snapshot of an existing storage object, and later refresh the Snapshot data to match that of the source object's current state without the need to explicitly change the mapping and zoning of the host.

The refresh operation replaces an outdated storage object with an updated version without changing the SCSI face (NAA) of the refreshed object. As a result, the outdated object is refreshed without the need for remapping or rescanning on the host side.

The following examples are use cases that are supported by Refresh:

- ◆ Backup of production environment/Data Warehouse/Real-Time Analytics: A Snapshot Set taken of a Consistency Group with production Volumes, is mapped to a different host at a certain point in time, and then becomes periodically refreshed with data from the source Consistency Group with production Volumes.
- ◆ Refresh ‘Development and Test’ environments from a ‘master copy’ made from the production environment: The ‘master copy’ is a Snapshot Set taken at a certain point in time from the Consistency Group with production Volumes, and the Development and Test environment is a Snapshot Set that was initially taken from the production Consistency Group or the initial ‘master copy’, and is mapped to a different host. The Development and Test environment becomes refreshed periodically from a new master copy that was created from the production environment.

The refresh operation can be applied in the following cases:

- ◆ Refreshing a Snapshot with an updated source Volume
- ◆ Refreshing a source Volume with a Snapshot
- ◆ Refreshing a Snapshot with another Snapshot

The prevalent use case is to refresh an outdated Snapshot or Snapshot Set with an updated source Volume or Consistency Group, respectively. However, you can use the Refresh procedure to refresh a Volume or Consistency Group with a Snapshot or Snapshot Set data, if necessary.

Note: Before applying the refresh procedure, unmount the refreshed object. After refresh is complete, re-mount the refreshed object.

To refresh a Consistency Group:

1. From the menu bar, click Configuration.
2. In the Virtual tab (left pane), click Consistency Groups.
3. In the Consistency Group list, right-click the Consistency Group whose data you wish to refresh and select Refresh from the drop-down list.

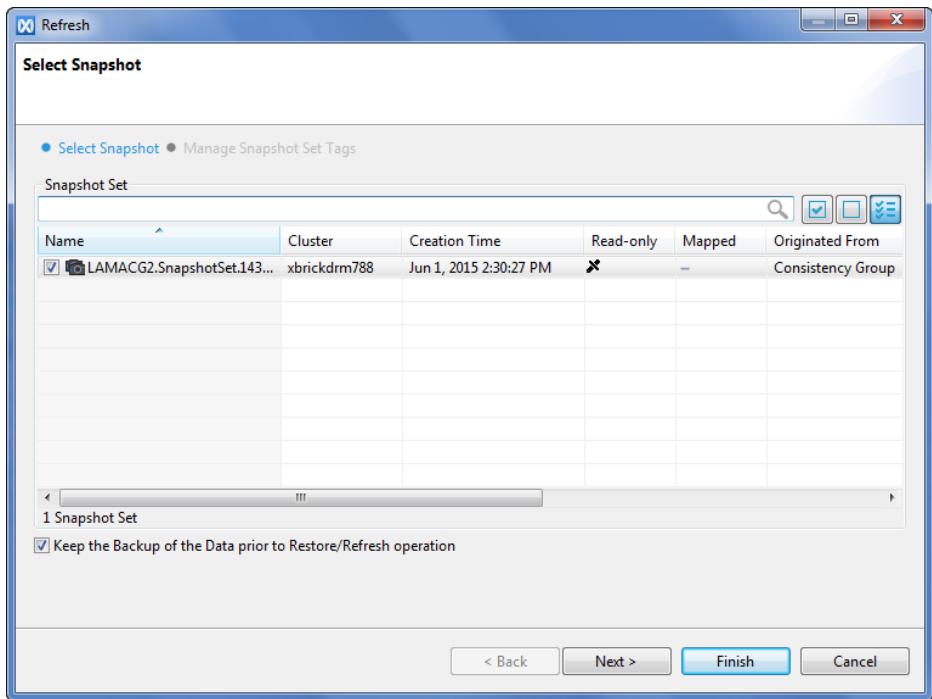


Figure 154 Refresh - Select Snapshot

The Select Snapshot window displays all Snapshot Sets of the selected Consistency Group.

4. Select the Snapshot Set you want to use for refreshing the Consistency Group, using the following options from the menu bar:
 - Type a text string to filter the displayed Snapshot list.
 - Click the **Select All** icon to select all displayed Snapshots.
 - Click the **Deselect All** icon to revoke the Snapshot selection.
 - Click the **Show All** icon  to display all defined Snapshots.
 - Click the **Show Only Selected** icon  to remove the unselected Snapshot from the display.

Note: You can only select one Snapshot Set from the list.

5. The source of the Snapshot is kept by default. If you want to remove it, clear the **Keep the backup of the Data prior to Restore/Refresh operation** option.

6. If you do not wish to assign Tags to the created Snapshot Set, skip to [step 12](#).

Note: You can assign Tags to the Snapshot after the Snapshot creation is completed. See [“Assigning Tags to Storage Elements” on page 165](#).

7. Click **Next** to assign Tags to the Snapshot Set.

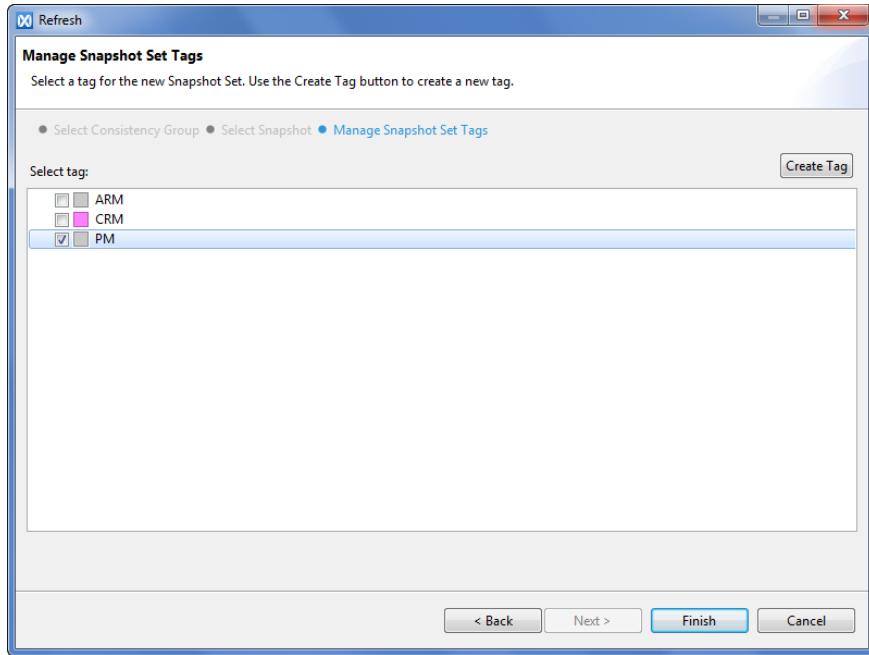


Figure 155 Refresh - Manage Tags

The Manage Snapshot Sets Tags window displays all the Tags that are currently defined for Snapshot Sets.

8. Select the relevant Tag to assign it to the new Snapshot Set. You can assign more than one Tag to a single Snapshot Set.
9. If you wish to create a new Snapshot Set Tag, click **Create Tag**.

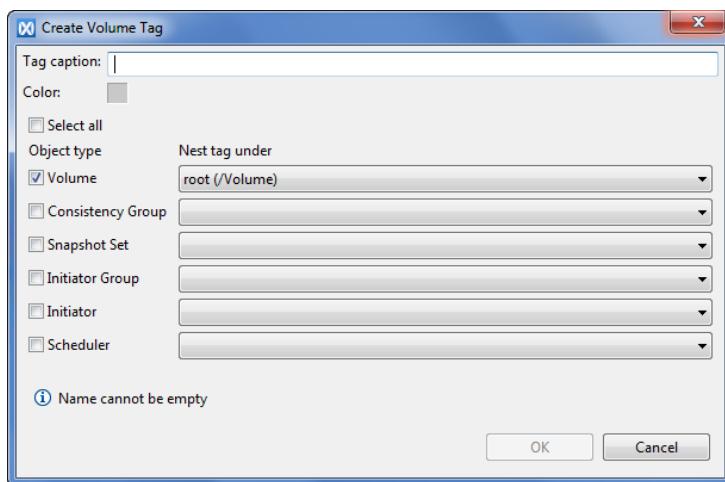


Figure 156 Create Snapshot Set Tag

10. Set the Tag properties:

- Tag caption
- Tag identifying color
- Tag object type and nesting path

11. Click **OK**; the Tag is added to the Tag list in the Manage Snapshot Set Tags dialog box. Select the new Tag to assign it to the Snapshot Set.

Note: To create Tags not as part of the restore from Snapshot procedure, see [“Managing Tags, Using the GUI” on page 164](#).

12. Click **Finish**; the new (refresh) Snapshot Set is added to the Snapshot Set table.

Adding a Volume to a Consistency Group

To add Volumes to a Consistency Group:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Consistency Groups**.
3. Select a Consistency Group and click **Add Volume to Consistency Group** in the menu bar, or right-click the Consistency Group and select **Add Volume to Consistency Group** from the drop-down menu.

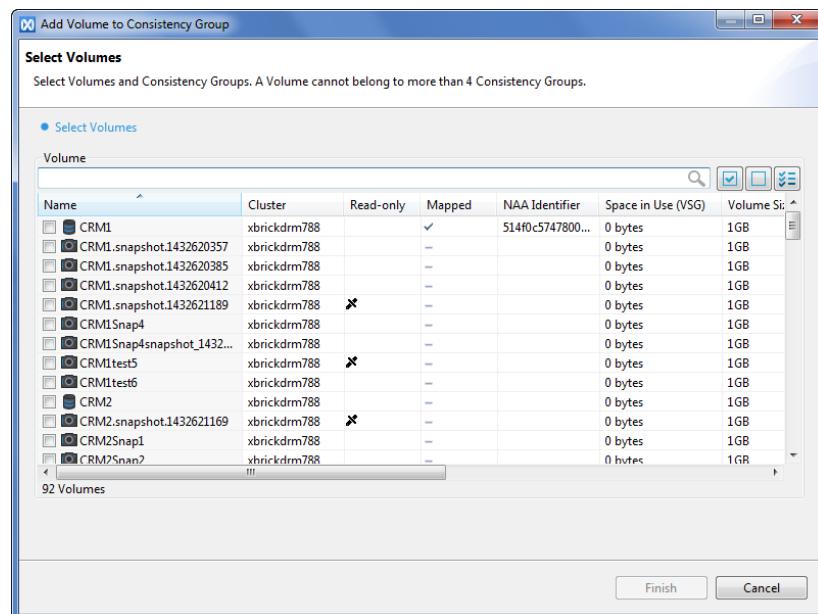


Figure 157 Add Volume to Consistency Group - Select Volumes

4. The defined Volumes appear in the Volume list. Select the Volume or Volumes you wish to add to the Consistency Group, using the following options from the menu bar:
 - Type a text string to filter the displayed Volume list.
 - Click the **Select All** icon to select all displayed Volumes.
 - Click the **Deselect All** icon to revoke the Volume selection.
 - Click the **Show All** icon  to display all defined Volumes.
 - Click the **Show Only Selected** icon  to remove the unselected Volumes from the display.
5. Click **Finish**; the selected Volumes are added to the Consistency Group.

Note: You can also add Volumes to a Consistency Group by selecting Volumes and then selecting the target Consistency Group. See “[Adding Volumes to a Consistency Group](#)” on [page 186](#) for details.

Removing a Volume from a Consistency Group

Note: Removing a Volume from a Consistency Group prevents cross-consistency of future Snapshots.

To remove Volumes from a Consistency Group:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Consistency Groups**.
3. From the Consistency Groups list, right-click a Consistency Group and select **Remove Volume from Consistency Group** from the drop-down menu.

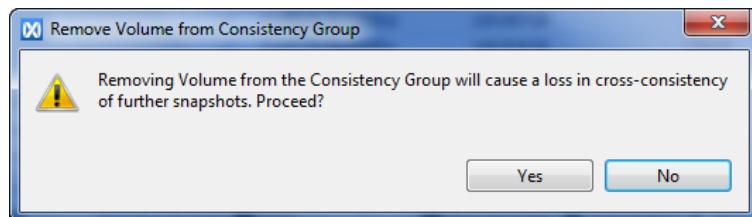


Figure 158 Remove Volume from Consistency Group - Warning

4. Click **Yes** to confirm.

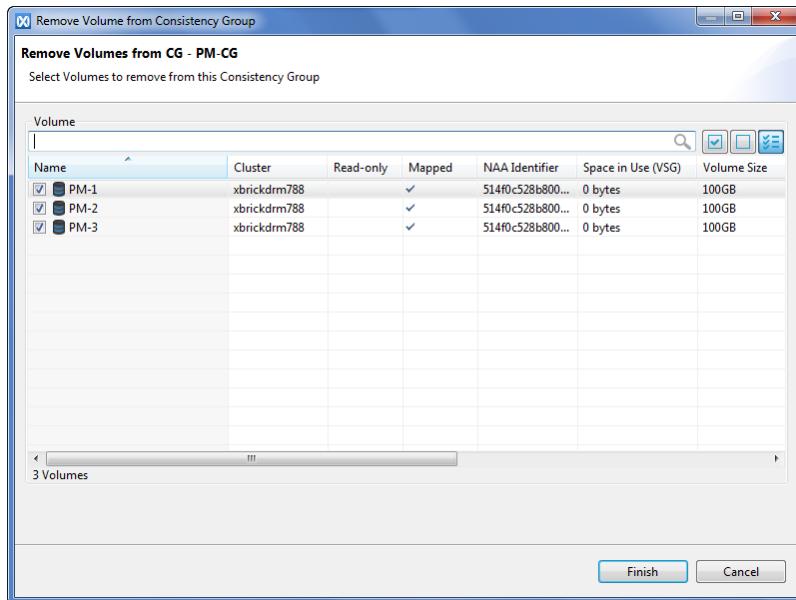


Figure 159 Remove Volume from Consistency Group

5. Select the Volume or Volumes that you wish to remove and click **Finish**; the Volume is removed from the Consistency Group.

Note: You can also remove Volumes from a Consistency Group by selecting Volumes and then selecting the target Consistency Group. See “[Removing Volumes from a Consistency Group](#)” on page 187 for details.

Deleting a Consistency Group

Note: Mapped Volumes cannot be deleted. If the Consistency Group includes mapped Volume, unmap them before deleting the group.

To delete a Consistency Group:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Consistency Groups**.
3. Right-click the Consistency Group you want to delete and select **Delete Consistency Group** from the drop-down menu. You can select multiple Consistency Groups, using the Shift and Ctrl keys.

Note: When you delete a Consistency Group, its Volumes are not deleted.

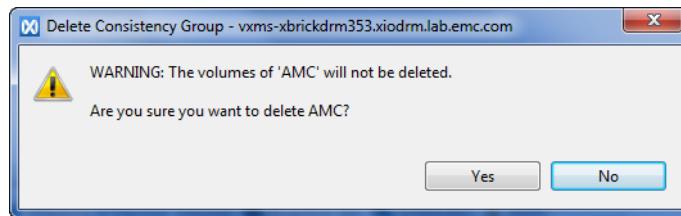


Figure 160 Delete Consistency Group Notification

4. Confirm the deletion by clicking **Yes**; the Consistency Group is deleted from the Consistency Group window.

Viewing the Consistency Groups Related Information

The Consistency Groups Window displays, in addition to the defined Consistency Groups, additional related information. The following information is available in the pane below the Consistency Group table:

- ◆ Volumes
- ◆ Mapping of Member Volumes
- ◆ Snapshot Sets
- ◆ Schedulers
- ◆ Alerts

To view the Volumes information:

- ◆ Select a Consistency Group and click the **Volumes** tab.

Name	Cluster	Read-only	Mapped	NAA Identifier	Space in Use (VSG)	Volume Size	Logical Block Size	Alignment Offset	T
vol1	xbrick3	✓	✓	5140c5151600...	4.913TB	2TB	512	0	
vol2	xbrick3	✓	✓	5140c5151600...	4.91TB	2TB	512	0	
vol3	xbrick3	✓	✓	5140c5151600...	6.391TB	2TB	512	0	
vol4	xbrick3	✓	✓	5140c5151600...	4.91TB	2TB	512	0	
vol5	xbrick3	✓	✓	5140c5151600...	6.392TB	2TB	512	0	
vol6	xbrick3	✓	✓	5140c5151600...	6.391TB	2TB	512	0	

6 Volumes of 1 Consistency Group

Figure 161 Volumes Tab

The Volumes tab displays the following data:

- Volume Name
- Cluster Name (in multiple cluster settings)
- Read-Only indication
- Mapped indication
- NAA Identifier
- Space in Use (VSG)
- Volume Size
- Logical Block Size
- Alignment Offset
- Tags

To view the Mapping of Member Volumes information:

- ◆ Select a Consistency Group and click the **Mapping of Member Volumes** tab.

The screenshot shows a table titled 'LUN Mapping IDs' with two columns: 'Volumes / Initiator Groups' and 'Igdrm1569' and 'Igdrm1570'. The data is as follows:

Volumes / Initiator Groups	Igdrm1569	Igdrm1570
vol1		4
vol2		6
vol3	5	
vol4		2
vol5	1	
vol6		3

Selected 1 Volume mapped to 2 IGS

Figure 162 Mapping of Member Volumes Tab

The Mapping of Member Volumes tab displays the following data:

- Volume Name
- Number of mappings created between the Volume and each Initiator Group

To view the Snapshot Sets information:

- ◆ Select a Consistency Group and click the **Snapshot Sets** tab.

The screenshot shows a table with the following columns: Name, Cluster, Creation Time, Read-only, Mapped, Originated From, Number of Volumes, and Tags. The data is as follows:

Name	Cluster	Creation Time	Read-only	Mapped	Originated From	Number of Volumes	Tags
[Snapshot Set60217]	xbrick3	Jun 14, 2015 9:32:26 PM	—	—	Consistency Group	6	
[Snapshot Set60218]	xbrick3	Jun 14, 2015 9:34:00 PM	—	—	Consistency Group	6	
[Snapshot Set60219]	xbrick3	Jun 14, 2015 9:36:00 PM	—	—	Consistency Group	5	
[Snapshot Set60220]	xbrick3	Jun 14, 2015 9:38:00 PM	—	—	Consistency Group	5	
[Snapshot Set60221]	xbrick3	Jun 14, 2015 9:40:00 PM	—	—	Consistency Group	6	
[Snapshot Set60222]	xbrick3	Jun 14, 2015 9:42:00 PM	—	—	Consistency Group	6	
[Snapshot Set60223]	xbrick3	Jun 14, 2015 9:44:00 PM	—	—	Consistency Group	6	
[Snapshot Set60224]	xbrick3	Jun 14, 2015 9:46:00 PM	—	—	Consistency Group	6	
[Snapshot Set60225]	xbrick3	Jun 14, 2015 9:48:00 PM	—	—	Consistency Group	6	
[Snapshot Set60226]	xbrick3	Jun 14, 2015 9:50:00 PM	—	—	Consistency Group	6	
[Snapshot Set60227]	xbrick3	Jun 14, 2015 9:52:00 PM	—	—	Consistency Group	5	

205 Snapshot Sets of 1 Consistency Group

Figure 163 Snapshot Sets Tab

The Snapshot Sets tab displays the following data:

- Snapshot Set Name
- Cluster Name (in multiple clusters settings)
- Creation Time
- Read-Only indication
- Mapped indication
- Originated From (entity name)
- Number of Volumes
- Tags

To view the Schedulers information:

- ◆ Select a Consistency Group and click the **Schedulers** tab.

Scheduler Name	Cluster	Snapshot Sour...	Snaph...	Snaph...	Interval	Explicit Schedule	Snapsh...	Snapsh...	Snapshots to K...	Last Activation Time
0 Schedulers of 1 Consistency Group										

Figure 164 Schedulers Tab

The Schedulers tab displays the following data:

- Scheduler Name
- Cluster Name (in multiple clusters settings)
- Snapshot Source Type
- Snapshot Type
- Interval
- Explicit Schedule
- Snapshots to Keep - Number
- Snapshots to Keep - Time
- Last Activation Time
- Last Activation State
- Scheduler State
- Tags

To view the Alerts information:

- ◆ Select a Consistency Group and click the **Alerts** tab.

Severity	Cluster	Code	Date and Time	Entity	Entity Details	Description
0 Alerts						

Figure 165 Alerts Tab

The Alerts tab displays the following data:

- Severity Level
- Cluster Name (in multiple clusters settings)
- Alert Code
- Date and Time
- Entity
- Entity Details
- Description

Managing Consistency Groups, Using the CLI

Use the following CLI commands for managing Consistency Groups:

Command	Description
add-volume-to-consistency-group	Adds a Volume to a Consistency Group.
create-consistency-group	Creates a new Consistency Group.
create-snapshot-and-reassign	Creates a Snapshot from a specified Volume/Snapshot, Consistency Group, or Snapshot sets and reassigns the Volume identity characteristic to the created Snapshot.
remove-consistency-group	Deletes a Consistency Group.
remove-volume-from-consistency-group	Removes a Volume from a Consistency Group.
show-consistency-group	Displays a specified Consistency Group's parameters.
show-consistency-groups	Displays all the defined Consistency Groups' parameters.
create-scheduler	Creates a new Snapshot scheduler.

Managing the Snapshot Sets

Managing Snapshot Sets, Using the GUI

Creating a Snapshot of a Snapshot Set

To create a Snapshot of a Snapshot Set:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab, click **Snapshot Sets** to display the Snapshot Sets window.
3. Select a Snapshot Set from the table and click **Create Snapshot** in the menu bar. You can also right-click the Snapshot Set and select **Create Snapshot** from the drop-down menu.

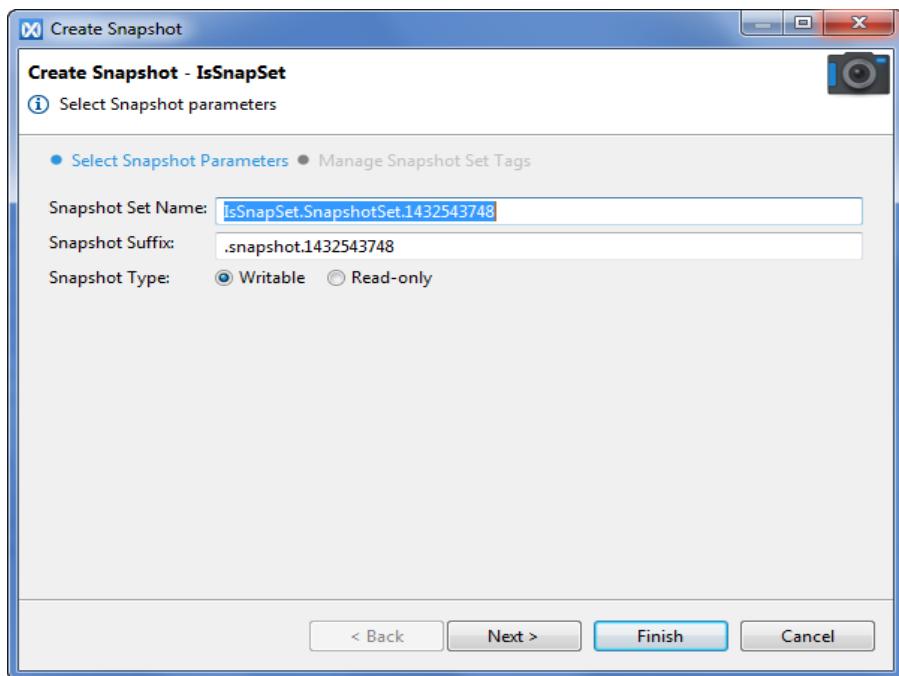


Figure 166 Create Snapshot - Select Snapshot Set

4. In the Create Snapshot dialog box, set the following parameters:
 - Snapshot Set name (default name - SnapshotSet.<epoch>)
 - Snapshot Suffix
 - Snapshot Type (Writable or Read-only)
5. If you do not wish to assign Tags to the new Snapshot, skip to [step 11](#) .

Note: You can assign Tags to the new Snapshot after its creation is completed. See [“Assigning Tags to Storage Elements” on page 165](#).

- Click **Next** to assign Tags to the new Snapshot.

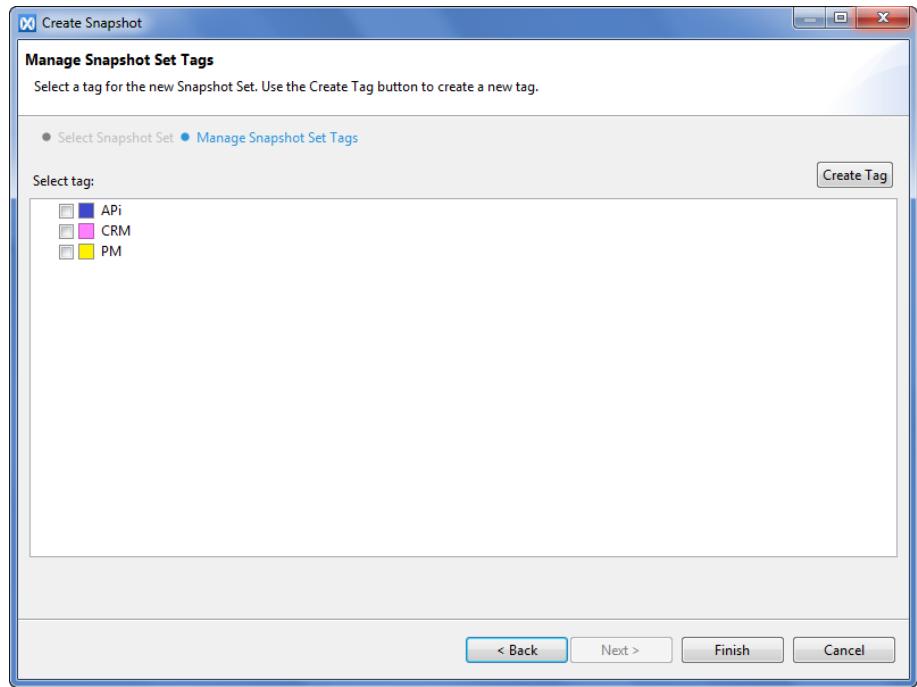


Figure 167 Create Snapshot - Manage Tags

The Manage Snapshot Set Tags window displays all the Tags that are currently defined for Snapshot Sets.

- Select the desired Tag to assign it to the new Snapshot. You can assign more than one Tag to a single Snapshot.
- If you wish to create a new Tag, click **Create Tag**.

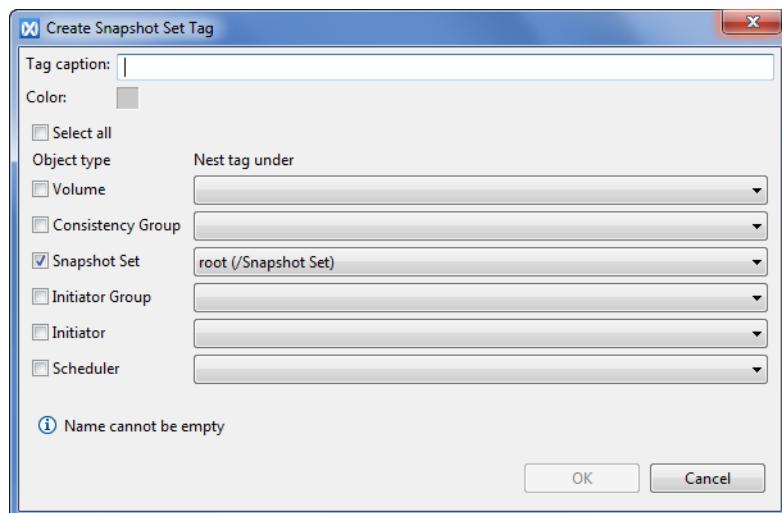


Figure 168 Create Volume Tag

9. Set the Tag properties:

- Tag name
- Tag color
- Tag object type nesting path

10. Click **OK**; the Tag is added to the Tag list in the Manage Snapshot Set Tags dialog box. Select the new Tag to assign it to the Snapshot.

Note: To create Tags not as part of the Snapshot creation procedure, see “[Managing Tags, Using the GUI](#)” on page 164.

11. Click **Finish**; the new Snapshot set is added to the Snapshot Set table in the Snapshot Set window.

Refreshing a Snapshot Set

To refresh a Snapshot Set:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Snapshot Sets** to display the Snapshot Set window.
3. In the Snapshot Set list, right-click the Snapshot Set whose data you wish to refresh and select **Refresh** from the drop-down list.

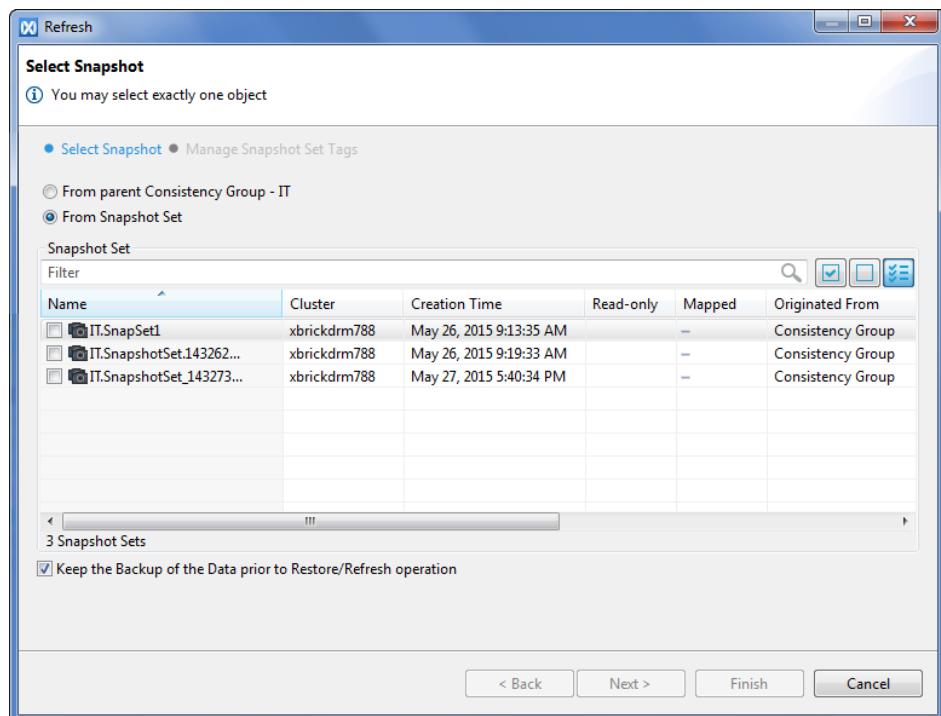


Figure 169 Refresh Snapshot Set

4. Select whether you wish to refresh from the parent Consistency Group to a child Snapshot Set or to refresh from another Snapshot Set.

5. If you selected to refresh from a Snapshot Set, select a Snapshot Set from the table, using the following options from the menu bar:

- Type a text string to filter the displayed Snapshot Set list.
- Click the **Select All** icon to select all displayed Snapshot Sets.
- Click the **Deselect All** icon to revoke the Snapshot Set selection.
- Click the **Show All** icon  to display all defined Snapshot Sets.
- Click the **Show Only Selected** icon  to remove the unselected Snapshot Sets from the display.

Note: You can select only one Snapshot Set from the list.

6. The source of the Snapshot before the refresh operation is kept by default. If you want to remove it, clear the **Keep the backup of the Data prior to Restore/Refresh operation** option.
7. If you do not wish to assign Tags to the created Snapshot, skip to [step 13](#).

Note: You can assign Tags to the Snapshot after the Snapshot creation is completed. See "[Assigning Tags to Storage Elements](#)" on page 165.

8. Click **Next** to assign Tags to the Snapshot.

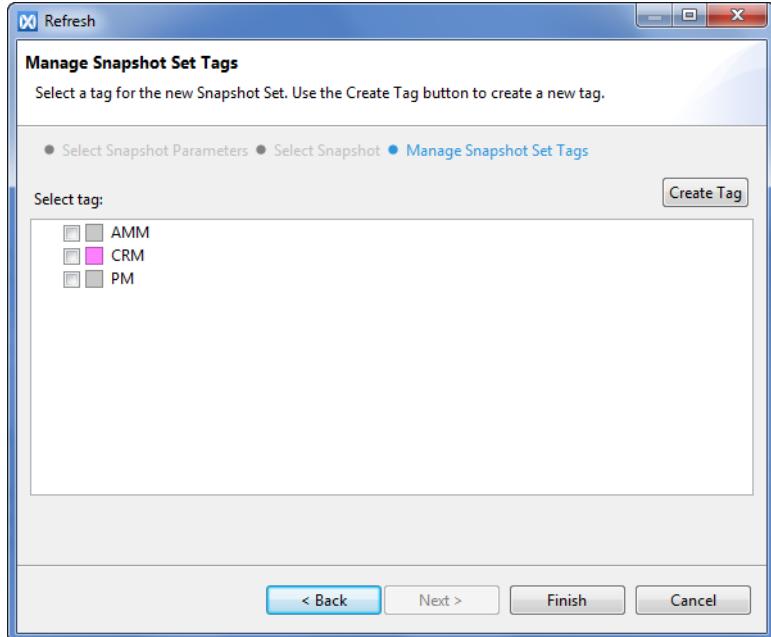


Figure 170 Refresh - Manage Tags

The Manage Snapshot Set Tags window displays all the Tags that are currently defined for Snapshot Sets.

9. Select the relevant Tag to assign it to the new Snapshot Set. You can assign more than one Tag for a single Snapshot Set.

10. If you wish to create a new Snapshot Set Tag, click **Create Tag**.

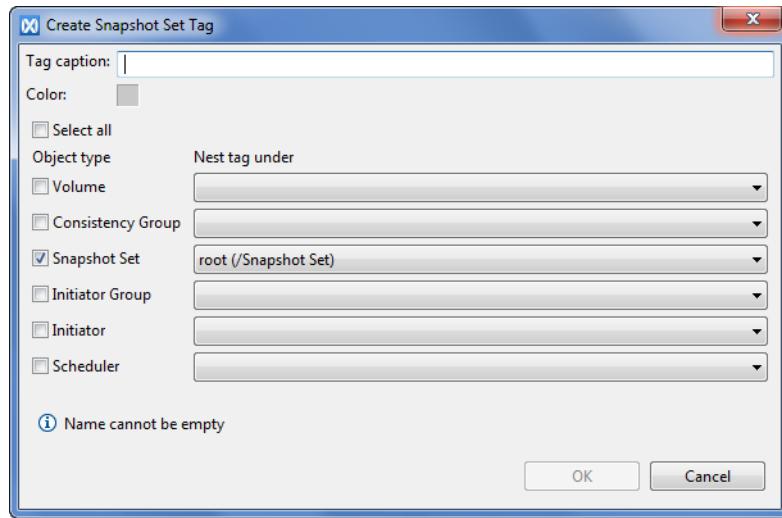


Figure 171 Create Snapshot Set Tag

11. Set the Tag properties:

- Tag caption
- Tag color
- Tag object type and nesting path

12. Click **OK**; the Tag is added to the Tag list in the Manage Snapshot Sets dialog box. Select the new Tag to assign it to the Snapshot Set.

Note: To create Tags not as part of the refresh procedure, see [“Managing Tags, Using the GUI” on page 164](#).

13. Click **Finish**; the new (refreshed) Snapshot Set is added to the Snapshot Set table.

Creating a Snapshot Scheduler for Snapshot Sets

To create a Snapshot Set Scheduler:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Snapshot Sets** to display the Snapshot Set window.
3. Right-click a Snapshot Set from the Snapshot Set list and select **Create Snapshot Scheduler** from the drop-down list.

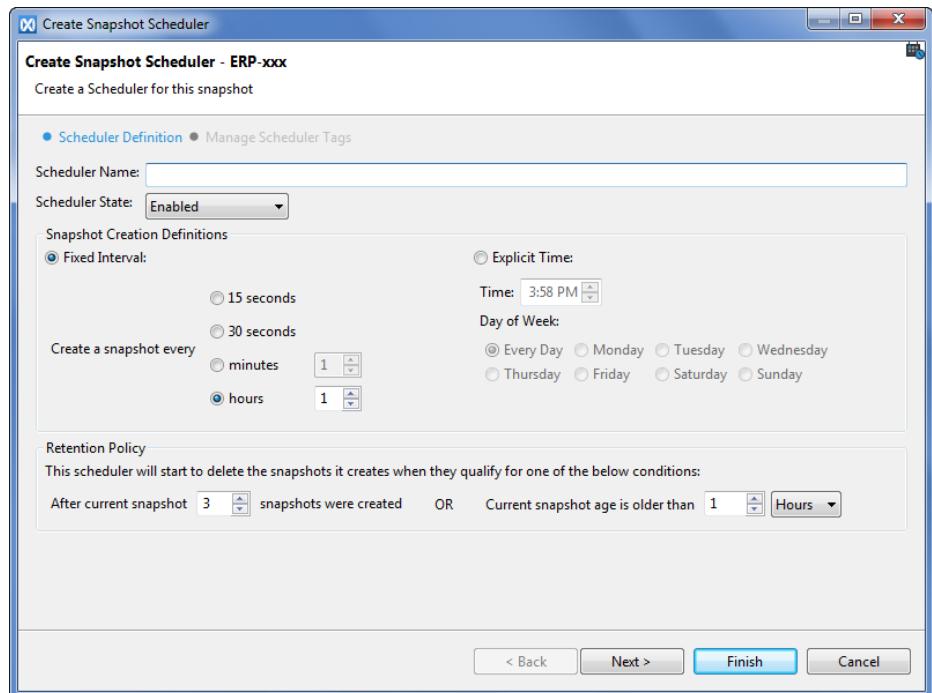


Figure 172 Create Snapshot Set Scheduler - Definition

4. In the Scheduler Definition dialog box, type a unique name for the Scheduler.
5. The Scheduler is enabled by default. If you want to disable it, select **Disable** from the Scheduler State drop-down list.
6. In the Snapshot Creation Definitions, select whether you wish Snapshots to be created at a fixed interval or at a specified time.
7. If you selected the Fixed Interval option, set the time interval by selecting one of the following options:
 - 15 seconds
 - 30 seconds
 - Minutes (set the number)
 - Hours (set the number)
8. If you selected the Explicit Time option, set the time and select a day.

9. Set the Retention Policy:

- Set the number of Snapshot Sets that will be created before the current Snapshot Set is deleted.
- Set the age limit in hours or days beyond which the current Snapshot Set is deleted.

10. If you do not wish to assign Tags to the new Scheduler, skip to [step 16](#).

Note: You can assign Tags to the Scheduler after the Scheduler creation is completed. See [“Assigning Tags to Storage Elements” on page 165](#).

11. Click **Next** to assign Tags to the new Scheduler.

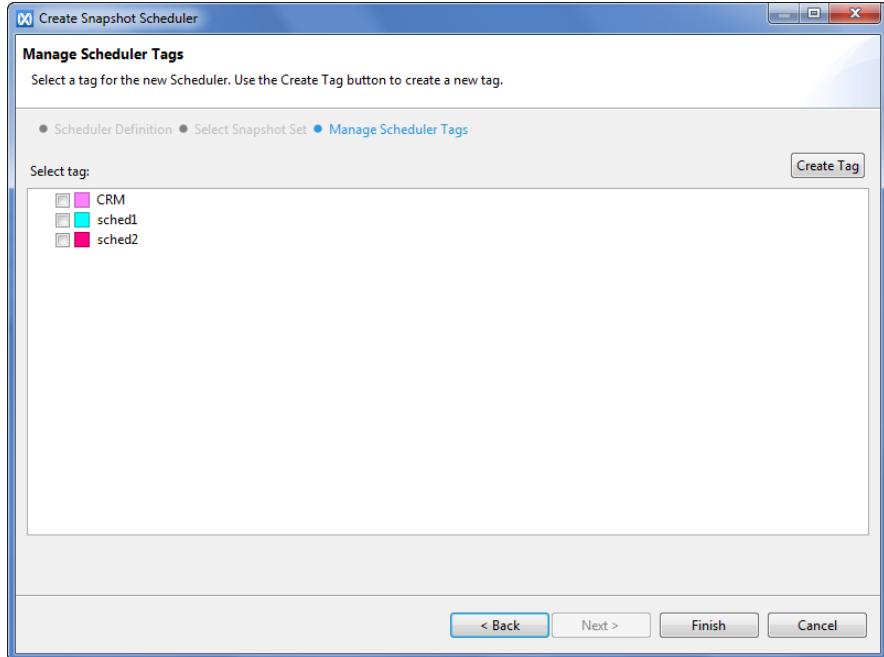


Figure 173 Create Snapshot Set Scheduler - Manage Tags

The Manage Scheduler Tags window displays all the Tags that are currently defined for Schedulers.

12. Select the relevant Tag to assign it to the new Scheduler. You can assign more than one Tag for a single Scheduler.

13. If you wish to create a new Scheduler Tag, click **Create Tag**.

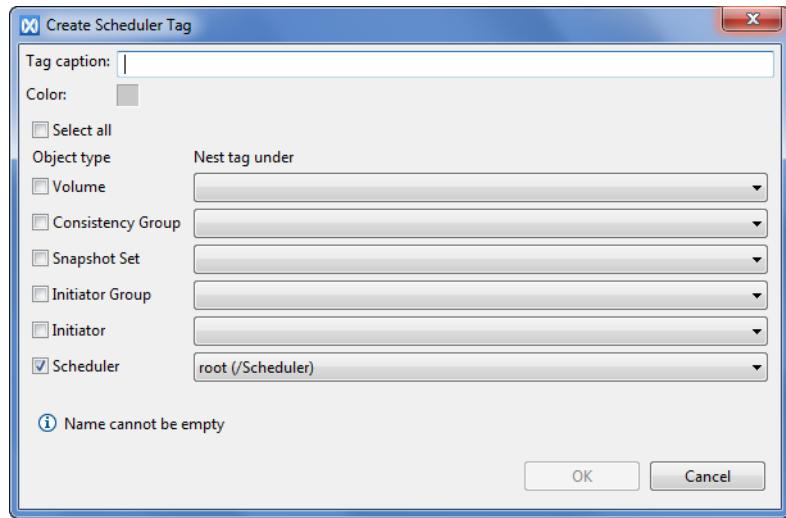


Figure 174 Create Scheduler Tag

14. Set the Tag properties:

- Tag caption
- Tag color
- Tag object type and nesting path

15. Click **OK**; the Tag is added to the Tag list in the Create Scheduler dialog box. Select the new Tag to assign it to the Scheduler.

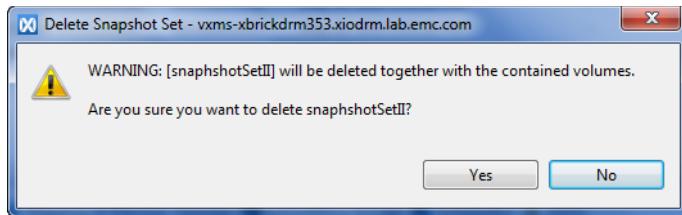
Note: To create Tags not as part of the Scheduler creation procedure, see “[Managing Tags, Using the GUI](#)” on page 164.

16. Click **Finish**; the new Scheduler is added to the list in the Schedulers window.

Deleting a Snapshot Set

To delete a Snapshot Set:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Snapshot Sets** to display the Snapshot Set window.
3. Right-click the Snapshot Set you want to delete and select **Delete Snapshot Set** from the drop-down menu. You can select multiple Snapshot Sets, using the Shift and Ctrl keys.



4. Confirm the deletion by clicking **Yes**; the Snapshot Set is deleted from the Snapshot Set list.

Viewing the Snapshot Sets Related Information

The Snapshot Sets Window displays, in addition to the defined Snapshot Sets, additional related information. The following information is available in the pane below the Snapshot Sets table:

- ◆ Volumes
- ◆ Mapping of Member Volumes
- ◆ Consistency Groups Sets
- ◆ Schedulers
- ◆ Alerts

To view the Volumes information:

- ◆ Select a Consistency Group and click the **Volumes** tab.

Name	Read-only	Mapped	NAA Identifier	Space in Use (VSG)	Volume Size	Logical Block Size	Alignment Offset	Tags
BI1.snapshot.1434608980	—			0 bytes	1TB	512	0	
BI2.snapshot.1434608980	—			0 bytes	1TB	512	0	
BI3.snapshot.1434608980	—			0 bytes	1TB	512	0	
BI4.snapshot.1434608980	—			0 bytes	1TB	512	0	

4 Volumes of 1 Snapshot Set

Figure 175 Volumes Tab

The Volumes tab displays the following data:

- Volume Name
- Cluster Name (in multiple cluster settings)
- Read-Only indication
- Mapped indication
- NAA Identifier
- Space in Use (VSG)
- Volume Size
- Logical Block Size
- Alignment Offset
- Tags

To view the Mapping of Member Volumes information:

- ◆ Select a Consistency Group and click the **Mapping of Member Volumes** tab.

Volumes / Initiator Groups
B1.snapshot.1434608980
B2.snapshot.1434608980
B3.snapshot.1434608980
B4.snapshot.1434608980

Selected 1 Volume mapped to 0 IGs

Figure 176 Mapping of Member Volumes Tab

The Mapping of Member Volumes tab displays the following data:

- Volume Name
- Number of mappings created between the Volume and each Initiator Group

To view the Consistency Groups Sets information:

- ◆ Select a Consistency Group and click the **Consistency Groups** tab.

Name	Read-only	Mapped	Number of Volumes	Number of Snapshot Sets	Tags
0 Consistency Groups of 1 Snapshot Set					

Figure 177 Consistency Groups Tab

The Consistency Groups tab displays the following data:

- Consistency Group Set Name
- Cluster Name (in multiple cluster settings)
- Read-Only indication
- Mapped indication
- Number of Volumes
- Number of Snapshot Sets
- Tags

To view the Schedulers information:

- ◆ Select a Consistency Group and click the **Schedulers** tab.

Scheduler Name	Snapshot Sour...	Snapsh...	Snap...	Interval	Explicit Schedule	Snapsh...	Snapshots to K...	Last Activation Time	Last Activati...
0 Schedulers of 1 Snapshot Set									

Figure 178 Schedulers Tab

The Schedulers tab displays the following data:

- Scheduler Name
- Cluster Name (in multiple cluster settings)
- Snapshot Source Type
- Snapshot Type
- Interval
- Explicit Schedule
- Snapshots to Keep - Number
- Snapshots to Keep - Time
- Last Activation Time
- Last Activation State
- Scheduler State
- Tags

To view the Alerts information:

- ◆ Select a Consistency Group and click the **Alerts** tab.

Volumes	Mapping of Member Volumes	Consistency Groups	Schedulers	Alerts		
Severity	Cluster	Code	Date and Time	Entity	Entity Details	Description
0 Alerts						

Figure 179 Alerts Tab

The Alerts tab displays the following data:

- Severity Level
- Cluster Name (in multiple cluster settings)
- Alert Code
- Date and Time
- Entity
- Entity Details
- Description

Managing Snapshot Sets, Using the CLI

Use the following CLI commands for managing Snapshot Sets:

Command	Description
create-snapshot	Creates a Snapshot from a specified Volume.
create-snapshot-and-reassign	Creates a Snapshot from a specified Volume/Snapshot, Consistency Group, or Snapshot Sets and reassigns the Volume identity characteristic to the created Snapshot.
show-snapshot-sets	Displays a list of Snapshot Sets and their data.
show-snapshot-set	displays the parameters of a specified Snapshot Set.
remove-snapshot-set	Removes a Snapshot Set
create-scheduler	Creates a new Snapshot scheduler.

Managing the Initiator Groups

The XtremIO Storage Array uses the term "Initiators" to refer to ports that can access a Volume.

Initiators can be managed by the XtremIO Storage Array by assigning them to an Initiator Group. To do this, edit an Initiator Group in the GUI and add the Initiator's properties, or run the relevant CLI command (refer to [“Managing Initiator Groups, Using the CLI” on page 249](#)).

The Initiators within an Initiator Group share access to one or more of the cluster's Volumes. You can define which Initiator Groups have access to which Volumes, using LUN mapping (refer to [“Managing Mapping” on page 253](#)).

This section explains how to manage Initiator Groups.

Managing Initiator Groups, Using the GUI

Viewing Initiator Groups

To view Initiator Groups:

1. From the menu bar, click **Configuration**.
2. If you wish to view all the defined Initiator Groups, click **Initiator Groups** to open the Initiator Groups window. To view only Initiator Groups tagged by a specific Tag, double-click **Initiator Groups** to open the Initiator Group Tags list and select a Tag from the list.

Name	Number of Initiators	Tags
ad100	2	SQL

Figure 180 Initiator Groups Table

Creating Initiator Groups

Note: Initiators are added to the cluster by defining them in an Initiator Group. You can define Initiators when adding a group or later by using the Edit Initiator Group option. To remove an Initiator, edit the group and delete the Initiator's properties.

To create an Initiator Group:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab, click **Initiator Groups** to display the Initiator Groups table.

3. In the Initiator Groups window menu bar, click **Create Initiator Group**. You can also right-click **Initiator Groups** in the Virtual tab and select **Create Initiator Group** from the drop-down menu.

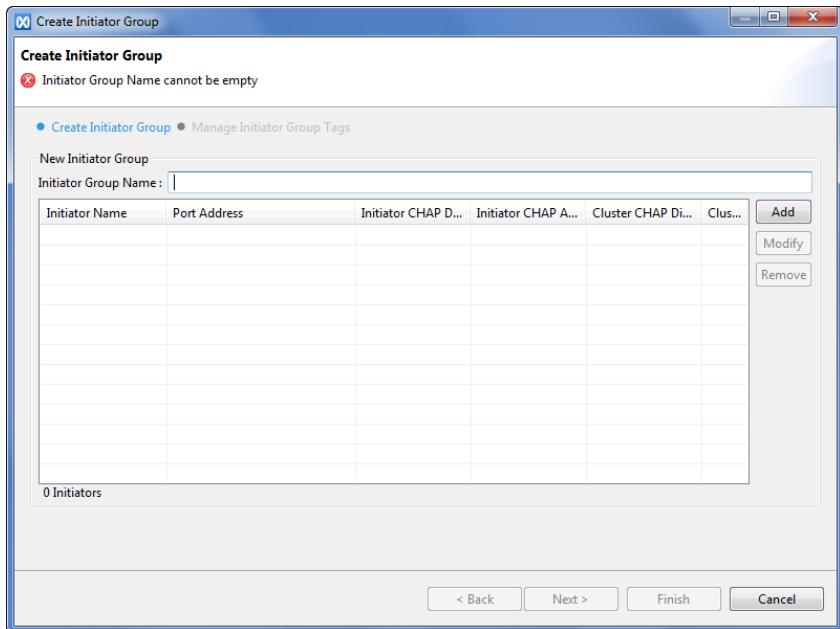


Figure 181 Create Initiator Group

4. In the Create Initiator Group dialog box, type a name for the group.
5. Click **Add** to add Initiators to the new Initiator Group; the Add Initiator Dialog box appears.

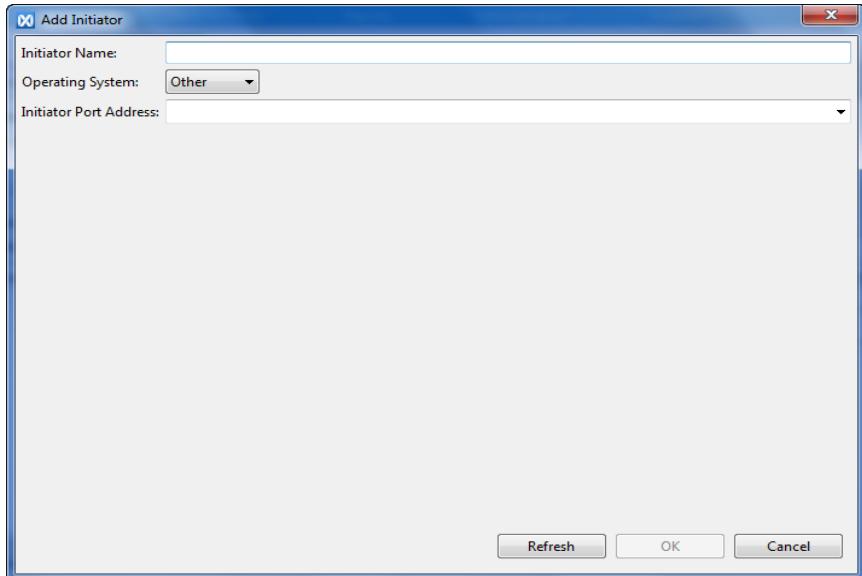


Figure 182 Add Initiator Dialog Box

6. In the Add Initiator dialog box, define the following:

- Initiator Name - enter a name for the Initiator. The name identifies the Initiator in the GUI or CLI lists.
- Operating System - Select from the drop-down list
- Initiator Port Address - add an Initiator's port address (i.e. the SCSI identification of the Initiator port). The port address depends on the port type, as follows:
 - iSCSI ports - addresses are in IQN or EUI format, e.g. eui.02004567A425678D, iqn.1991-05.com.microsoft:win-1htai3q0tmg
 - Fibre Channel ports - addresses using upper or lower case hexadecimal digit are valid, using the following formats:
 - * XX:XX:XX:XX:XX:XX
 - * XXXXXXXXXXXXXXXXXX
 - * 0XXXXXXXXXXXXXXX

Note: To see unused port addresses, click the **Initiator Port Address** drop-down arrow in the **Add Initiator** dialog box. If the Initiator was not previously discovered, the drop-down list is empty and you need to type the Initiator port address.

7. If you do not wish to assign Tags to the new Initiator Group, skip to [step 11](#).

Note: You can assign Tags to the new Initiator Group after the group creation is completed. See “[Assigning Tags to Storage Elements](#)” on page 165.

8. Click **Next** to assign Tags to the new Initiator Group.

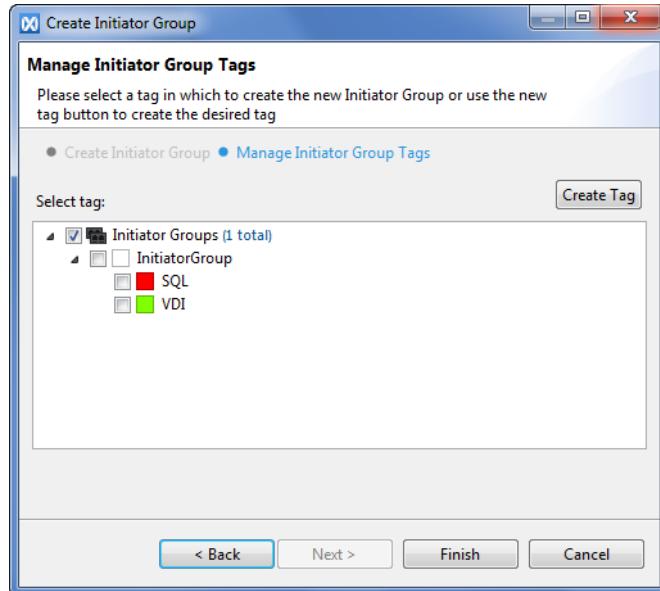


Figure 183 Create Initiator Group - Manage Tags

The Manage Initiator Group window displays all the Tags that are currently defined for Initiator Groups.

9. Select the relevant Tag to assign a Tag to the new Initiator Group. You can assign more than one Tag to a single group.
10. If you wish to create a new Initiator Group Tag, click **Create Tag**.

Note: To create Tags not as part of the Initiator Group creation procedure, see “[Managing Tags, Using the GUI](#)” on page 164.

11. Click **Finish**; the new Initiator Group is added to the Initiator Groups table.

Editing Initiator Groups

To edit an Initiator Group:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab, click **Initiator Groups** to display the Initiator Groups window.
3. Right-click the group you want to edit and select **Modify** from the drop-down menu.

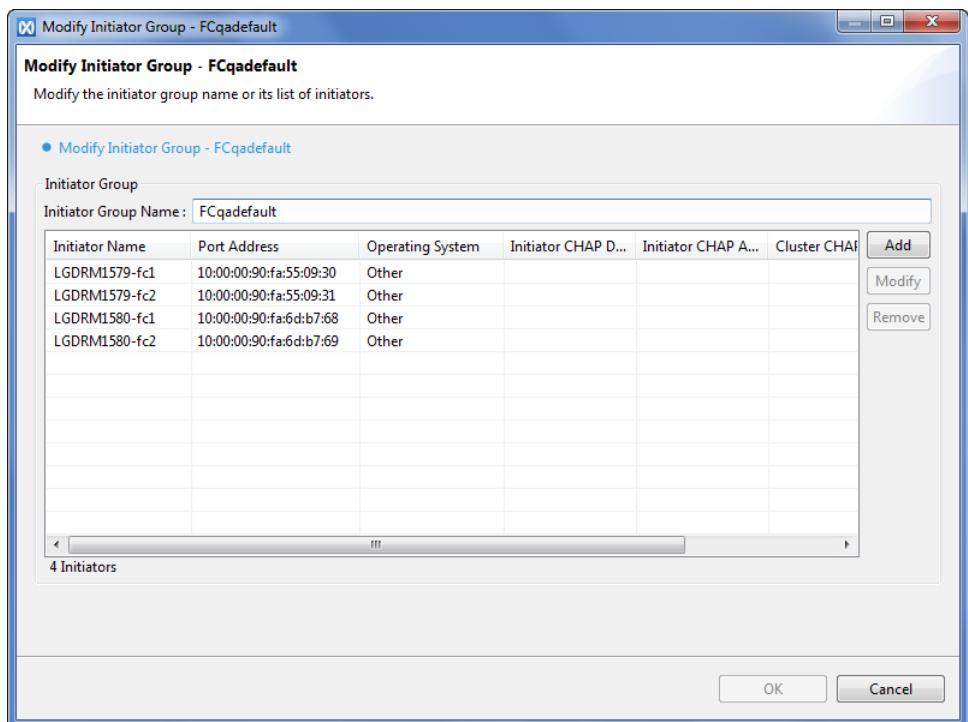


Figure 184 Modify Initiator Group

4. If you wish to modify the Initiator Group's name, type the new name in the Initiator Group Name field.
5. If you wish to delete an Initiator from the Initiator Group, select the Initiator and click **Remove**.
6. If you wish to modify the properties of an Initiator within the group, select the Initiator by clicking it and click **Modify**.

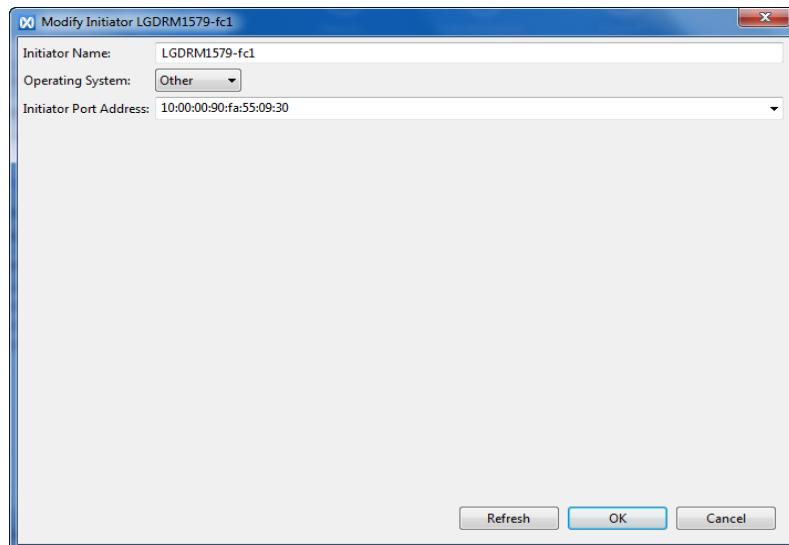


Figure 185 Modify Initiator - Fibre Channel

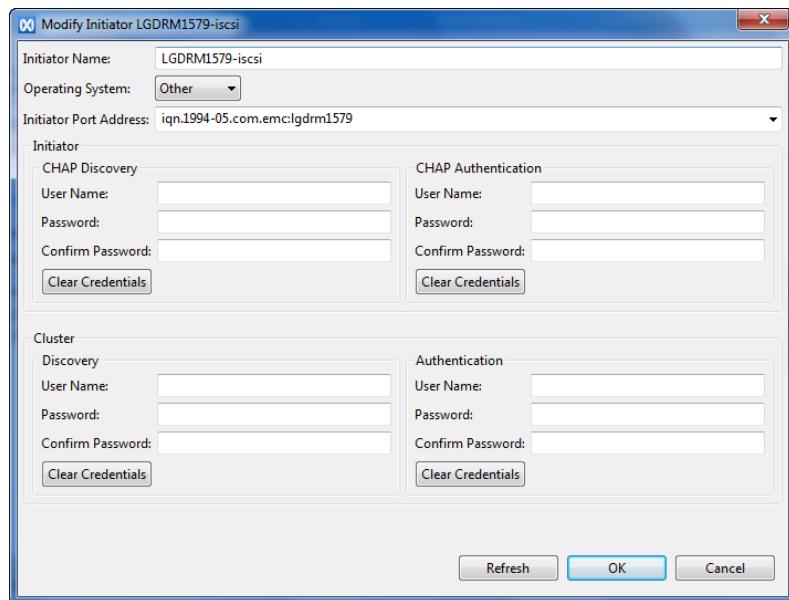


Figure 186 Modify Initiator - iSCSI

Note: The displayed dialog box is different for Fibre Channel and iSCSI Initiators.

7. In the Modify Initiator dialog box for Fibre Channel Initiators, modify the following as needed:

- Initiator Name
- Operating System - select one of the following options from the drop-down list:
Linux, Windows, ESX, Solaris, AIX, HP-UX, other
- Initiator Port Address (see “[To create an Initiator Group:](#)” on page 239)

Note: To use unused port addresses, click the drop-down arrow in the Initiator Port Address column.

In the Modify Initiator dialog box for iSCSI Initiators, modify the following as needed:

- Initiator Name
- Operating System - select one of the following options from the drop-down list:
Linux, Windows, ESX, Solaris, AIX, HP-UX, other
- Initiator Port Address - the SCSI identification of the Initiator port (see “[To create an Initiator Group:](#)” on page 239)

Note: To use unused port addresses, click the drop-down arrow in the Initiator Port Address column.

- CHAP Discovery (Initiator):
 - Name
 - Password
- CHAP Authentication (Initiator):
 - Name
 - Password
- CHAP Discovery (Cluster):
 - Name
 - Password
- CHAP Authentication (Cluster):
 - Name
 - Password

8. Click **OK**; the updated Initiator appears in the Initiator Group dialog box.
9. When you have completed modifying the Initiators, click **OK**; the updated Initiator Group appears in the Initiator Groups table.

Renaming Initiator Groups

To rename an Initiator Group:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Initiator Groups** to display the Initiator Group window.
3. Right-click the relevant Initiator Group in the Initiator Groups table and select **Rename** from the drop-down menu.



Figure 187 Rename Initiator Group Dialog Box

4. In the Rename dialog box, enter the name for the Initiator Group.
5. Click **OK**.

Deleting Initiator Groups

To delete an Initiator Group:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab, click **Initiator Groups** to display the Initiator Groups table.
3. Right-click the group you want to remove and select **Delete** from the drop-down menu.
4. Confirm the deletion by clicking **OK**.

Note: If you are deleting an Initiator Group that is mapped to Volumes, deleting the group disconnects it from the mapped Volumes.

5. In the dialog box, enter the folder name and click **OK**. The new folder appears in the Initiator Groups pane.

Creating and Modifying Mapping

Refer to “[Managing Mapping](#)” on page 253.

Viewing the Initiator Group Related Information

The Initiator Group Window displays, in addition to the defined Initiator Groups, additional related information. The following information is available in the pane below the Initiator Groups table:

- ◆ Mapping
- ◆ Initiators
- ◆ Targets
- ◆ Alerts

To view the mapping information:

- ◆ Select an Initiator Group and click the **Mapping** tab.

Volumes \ Initiator Groups	iSCSIqadefault
Clean1	41
Clean2	42
Clean3	43
Clean4	44
CRM1	40
vol2	2
vol4	4
vol5	5
vol7	7
vol13	13

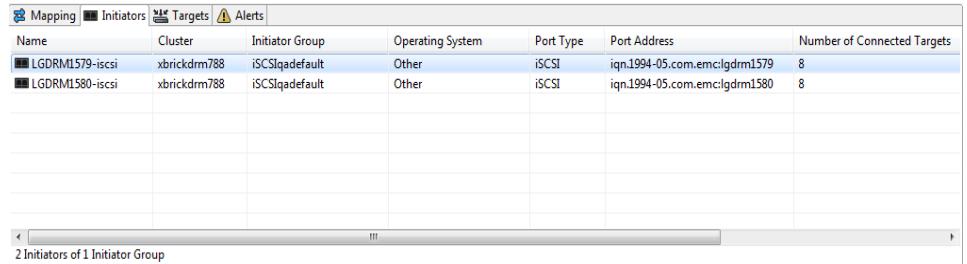
Figure 188 Mapping Tab

The Mapping tab displays the following data:

- Volume - the Volumes mapped to the selected Initiator Group
- LUN - the Logical Unit Number assigned for each connection

To view the Initiators information:

- ◆ Select an Initiator Group and click the **Initiators** tab.



The screenshot shows a table titled "Initiators" with the following data:

Name	Cluster	Initiator Group	Operating System	Port Type	Port Address	Number of Connected Targets
LGDRM1579-iscsi	xbrickdrm788	iSCSIqadefault	Other	iSCSI	iqn.1994-05.com.emc:lgdrm1579	8
LGDRM1580-iscsi	xbrickdrm788	iSCSIqadefault	Other	iSCSI	iqn.1994-05.com.emc:lgdrm1580	8

Below the table, a status bar indicates "2 Initiators of 1 Initiator Group".

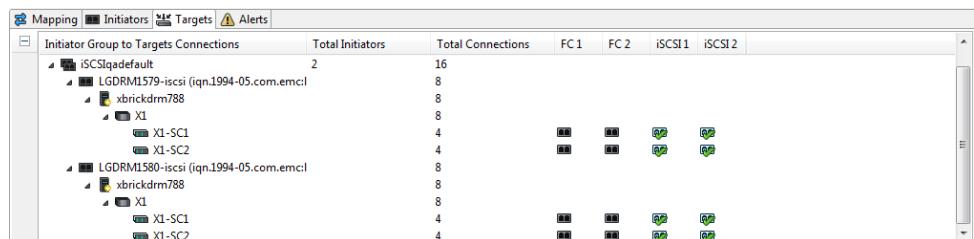
Figure 189 Initiators Tab

The Initiator tab displays the following data:

- Initiator Name
- Cluster (in a multiple cluster setting)
- Initiator Group
- Operating System
- Port Type
- Port Address
- Number of Connected Targets
- Tags

To view the Targets information:

- ◆ Select an Initiator Group and click the **Targets** tab.



The screenshot shows a table titled "Targets" with the following data:

Initiator Group to Targets Connections	Total Initiators	Total Connections	FC 1	FC 2	iSCSI 1	iSCSI 2
ISCSIqadefault	2	16				
LGDRM1579-iscsi (iqn.1994-05.com.emc:lgdrm1579)	8	8				
xbrickdrm788	8	8				
X1	8	8				
X1-X1-SC1	4	4				
X1-X1-SC2	4	4				
LGDRM1580-iscsi (iqn.1994-05.com.emc:lgdrm1580)	8	8				
xbrickdrm788	8	8				
X1	8	8				
X1-X1-SC1	4	4				
X1-X1-SC2	4	4				

Figure 190 iSCSI Targets Tab

The Targets tab displays the following data:

- Initiator Group to Target Connections
- Total Initiators
- Total Connections - the number of connected Targets
- A graphic portrayal of the Targets with indication for connection

To view the Alerts information:

- ◆ Select an Initiator group and click the **Alerts** tab.

Severity	Cluster	Code	Date and Time	Entity	Entity Details	Description
0 Alerts						

Figure 191 Alerts Tab

The Alerts tab displays the following data:

- Severity
- Cluster
- Code
- Date and Time
- Entity
- Entity Details
- Description

Managing Initiator Groups, Using the CLI

Use the following CLI commands for managing Initiator Groups:

Command	Description
add-initiator	Adds an Initiator and associates it with an existing Initiator Group.
add-initiator-group	Adds an Initiator Group and its associated Initiators to the XtreamIO cluster.
modify-initiator	Modifies the properties of an existing Initiator.
remove-initiator	Deletes an Initiator.
remove-initiator-group	Deletes an Initiator Group.
show-initiators	Displays Initiators' data.
show-initiator-group	Displays information for a specific Initiator Group.
show-initiator-groups	Displays information for all Initiator Groups.
show-targets	Displays the cluster Targets' interfaces (iSCSI or FC ports).
show-target-groups	Displays a list of Target Groups.
show-discovered-initiators-connectivity	Displays the Initiators-Targets connectivity map.
show-initiators-connectivity	Displays Initiators-Port connectivity and the number of connected Targets.
map-lun	Maps a Volume to an Initiator Group and assigns a Logical Unit Number (LUN) to it.

Managing Initiators

Managing Initiators, Using the GUI

Creating an Initiator

Refer to “[Creating Initiator Groups](#)” on page 239.

Editing an Initiator

Refer to “[Editing Initiator Groups](#)” on page 242.

Removing an Initiator

Refer to “[Editing Initiator Groups](#)” on page 242.

Renaming an Initiator

To rename an Initiator:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Initiators** to display the Initiators window.
3. Right-click the relevant Initiator in the Initiators table and select **Rename** from the drop-down menu.



Figure 192 Rename Initiator Dialog Box

4. In the Rename dialog box, edit the name for the Initiator.
5. Click **OK**.

Configuring CHAP

iSCSI Initiators and Targets prove their identity to each other, using the Challenge-Handshake Authentication Protocol (CHAP), which includes a mechanism to prevent clear text passwords from appearing on the wire.

You can configure CHAP for Initiator login and for the discovery phase. You can also configure Mutual CHAP for the Initiator to authenticate the XtremIO Targets.

Note: The following procedure refers only to iSCSI Initiators.

To configure an Initiator’s CHAP credentials:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab, click **Initiators** to display the Initiators window.

3. Right-click the Initiator you want to edit and select **Configure CHAP** from the drop-down menu.

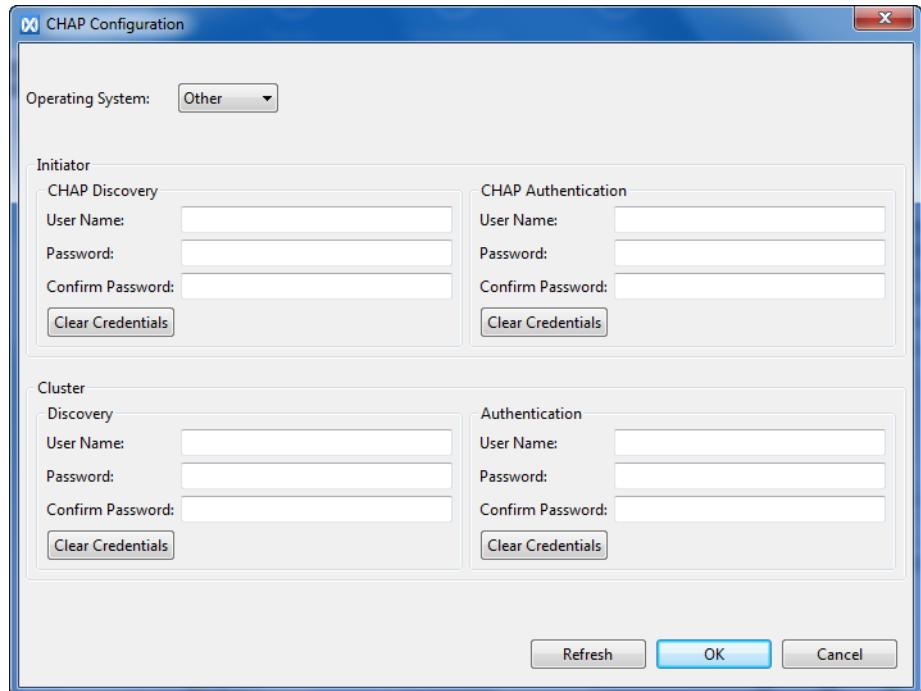


Figure 193 CHAP Configuration - iSCSI Initiators

4. In the CHAP Configuration dialog box, configure the following parameters:
 - Operating System - select one of the following options from the drop-down list: Linux, Windows, ESX, Solaris, AIX, HP-UX, other
 - CHAP Discovery (Initiator):
 - Name
 - Password
 - CHAP Authentication (Initiator):
 - Name
 - Password
 - CHAP Discovery (Cluster):
 - Name
 - Password
 - CHAP Authentication (Cluster):
 - Name
 - Password
5. Click OK.

Managing Initiators, Using the CLI

Use the following CLI commands for managing Initiators:

Command	Description
add-initiator	Adds an Initiator and associates it with an existing Initiator Group.
modify-initiator	Modifies the properties of an existing Initiator.
remove-initiator	Deletes an Initiator.
show-initiators	Displays Initiators' data.
rename	Renames a component of the XtremIO Storage Array.
show-chap	Displays the cluster's configured CHAP authentication and discovery modes.
modify-chap	Modifies Chap configuration parameters.

Managing Mapping

To allow Initiators within an Initiator Group to access a Volume's disk space, you can map the Volume to the Initiator Group.

When mapping a Volume to an Initiator Group, a Logical Unit Number (LUN) is automatically assigned.

You can map an Initiator Group to multiple Volumes. The Initiator Group's first mapping receives a LUN of 1. Additional mappings receive LUNs in sequential order. These numbers can be changed later to any desired LUN.

Basic Mapping Scenario

Mapping can be performed from either the Volumes or the Initiator Groups workspace.

To map Volumes to Initiator Groups:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Volumes** to display the Volumes window.
3. From the Volume list, click to select the Volume you wish to map. You can select multiple Volumes, using the Ctrl and Shift keys.
4. In the menu bar, click **Create/Update Mapping**. You can also right-click a selected Volume and select **Create/Update Mapping** from the drop-down menu.

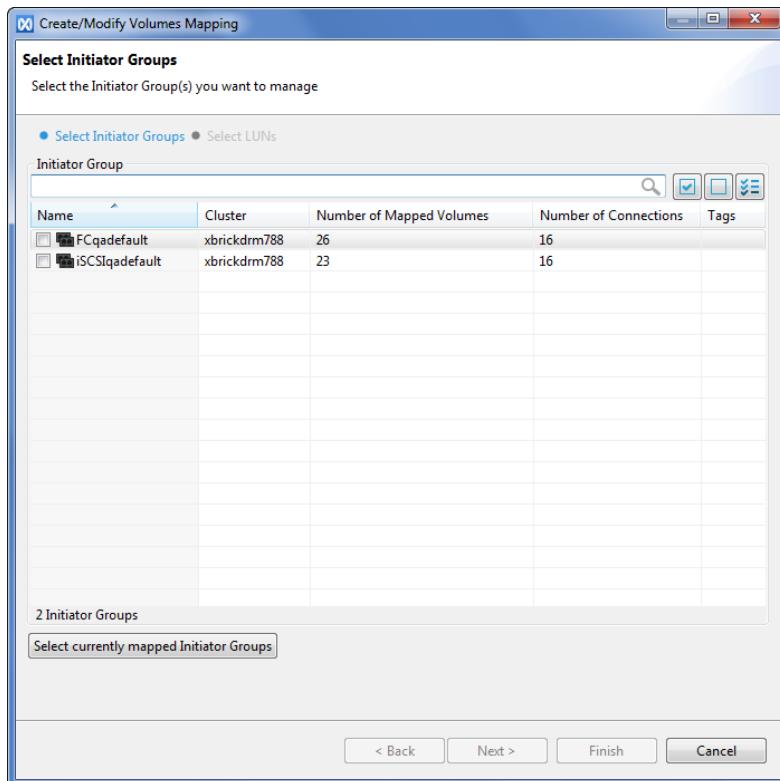


Figure 194 Create Mapping - Select Initiator Group

5. From the Initiator Groups pane in the Create Mapping dialog box, select the Initiator Groups you wish to map to the selected Volumes. Use the following options from the menu bar:

- Type a text string to filter the displayed Initiator Group list.
- Click the **Select All** icon to select all displayed Initiator Groups.
- Click the **Deselect All** icon to revoke the Initiator Group selection.
- Click the **Show All**  to display all defined Initiator Groups.
- Click the **Show Only Selected**  to remove the unselected Initiator Groups from the display.

Use the **Select Currently Mapped Initiator Groups** button to select the Initiator Groups that are already mapped to the Volumes you selected for mapping.

6. Click **Next**.

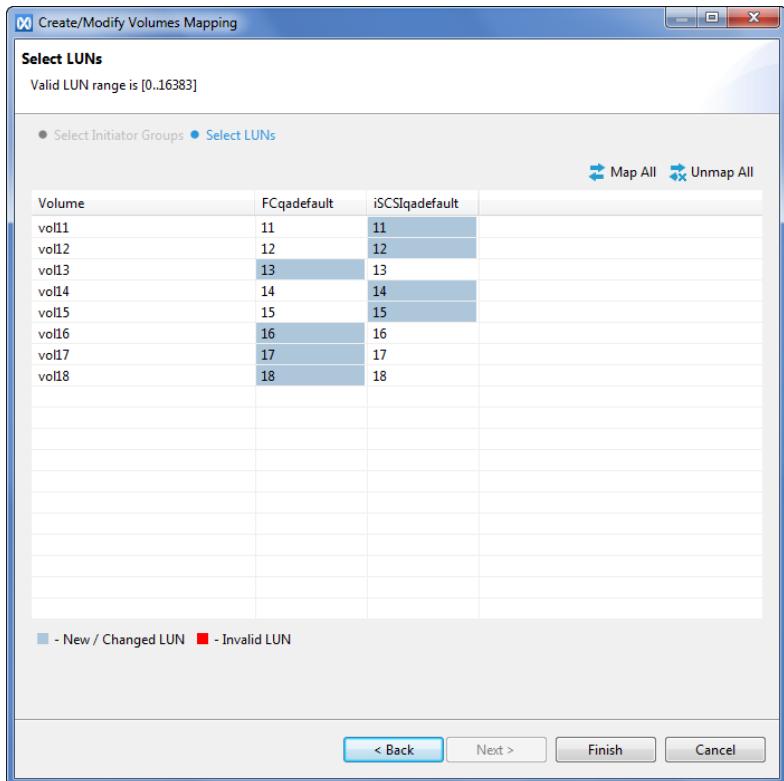


Figure 195 Create Mapping - Select LUNs

7. In the Select LUNs dialog box, you can change the LUN number assigned to the configured mapping. If you set an invalid LUN number, it appears in red.
8. Click **Finish**; the specified Volumes and Initiator Groups are mapped. A check sign is added for each of the mapped Volumes in the Mapped column of the Volumes window. For each Initiator Group, the number of mapped Volumes is indicated in the Initiator Groups table.

To map Initiator Groups to Volumes:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Initiator Groups** to display the Initiator Groups window.
3. From the Initiator Groups list, click to select the Initiator Group you wish to map. You can select multiple Initiator Groups, using the Ctrl and Shift keys.
4. In the menu bar, click **Create/Update Mapping**. You can also right-click a selected Initiator Group and select **Create/Update Mapping** from the drop-down menu.

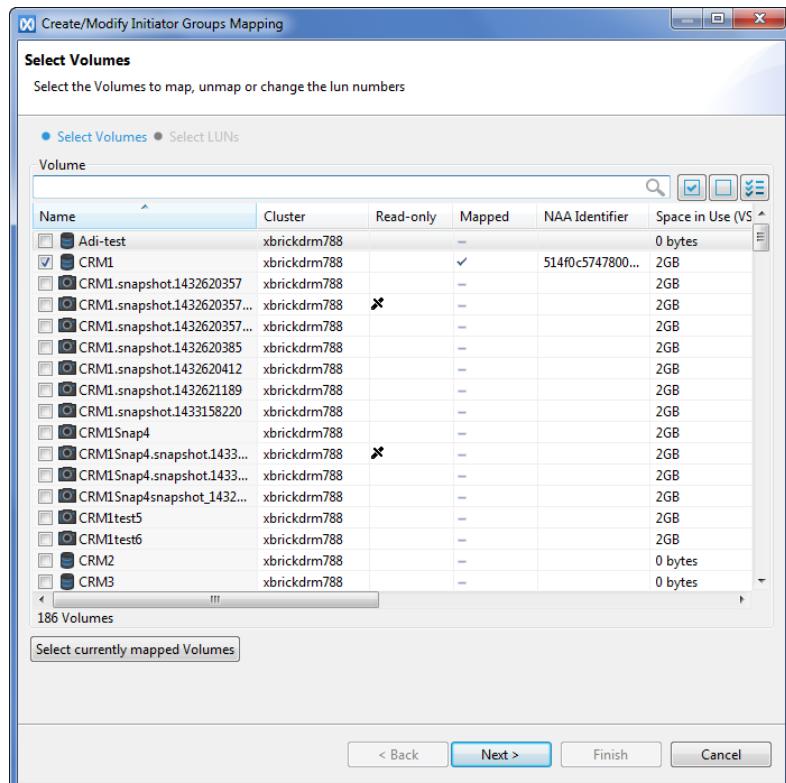


Figure 196 Create Mapping - Select Volumes

5. From the Volumes table in the Create Mapping dialog box, select the Volumes you wish to map to the selected Initiator Group. Use the following options from the menu bar:
 - Type a text string to filter the displayed Volumes list.
 - Click the **Select All** icon to select all displayed Volumes.
 - Click the **Deselect All** icon to revoke the Volumes selection.
 - Click the **Show All**  to display all defined Volumes.
 - Click the **Show Only Selected** icon  to remove the unselected Volumes from the display.
6. If you want to select Volumes that are already mapped to the Initiator Group you selected for mapping, click **Select Currently Mapped Volumes**.

7. Click **Next**.

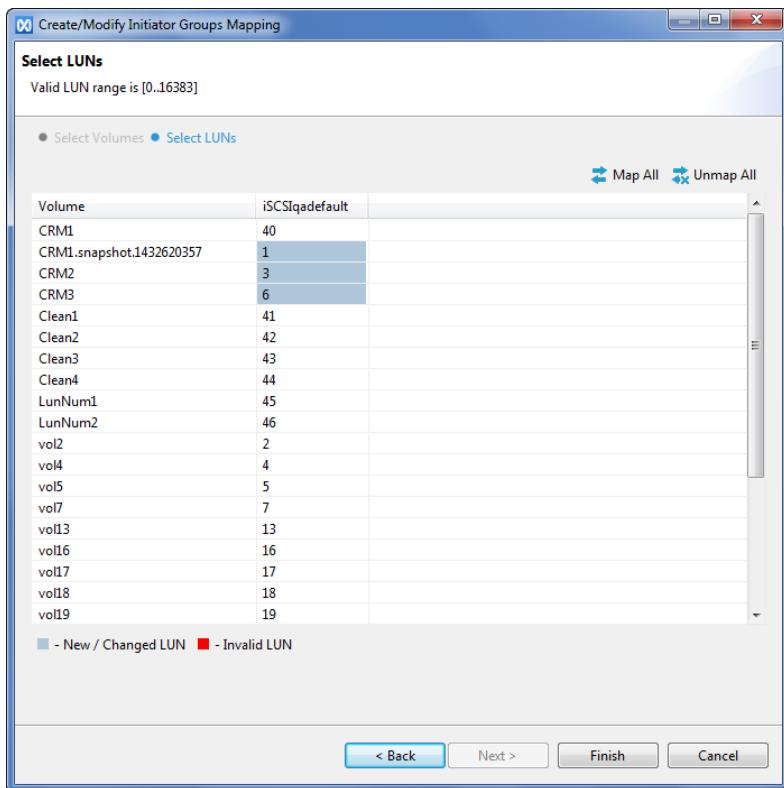


Figure 197 Create Mapping - Select LUNs

8. In the Select LUNs dialog box, you can change the LUN number assigned to the configured mapping. If you set an invalid LUN number, it appears in red.
9. Click **Finish**; the specified Initiator Groups and Volumes are mapped. A check sign is added for each of the mapped Volumes in the Mapped column of the Volumes window. For each Initiator Group, the number of mapped Volumes is indicated in the Initiator Groups table.

Using Tags for Mapping

Tags are not required to perform Volume mapping. However, using Tags can significantly simplify mapping of Volumes or Initiator Groups that represent a logical set.

Since Tags are used to represent logical grouping of objects based on a common characteristic or affiliation, it is possible to use Tags to simplify the object selection. Rather than selecting individual Volumes or Initiator Groups, you can simply select one or more Tags to perform mapping of the Volumes and Initiator Groups associated with these Tags.

To map Volumes to Initiator Groups, using Tags:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), double-click the object type you wish to use for mapping (e.g. Volumes, Consistency Groups, etc.); the Tag list for that object is displayed below the object's name.

3. In the Virtual tab, double-click **Initiator Groups**; the Tag list for Initiator Groups is displayed.
4. Select a Tag from each list (using the Ctrl key).
5. Right-click one of the Tags and select **Create/Modify Mapping**.

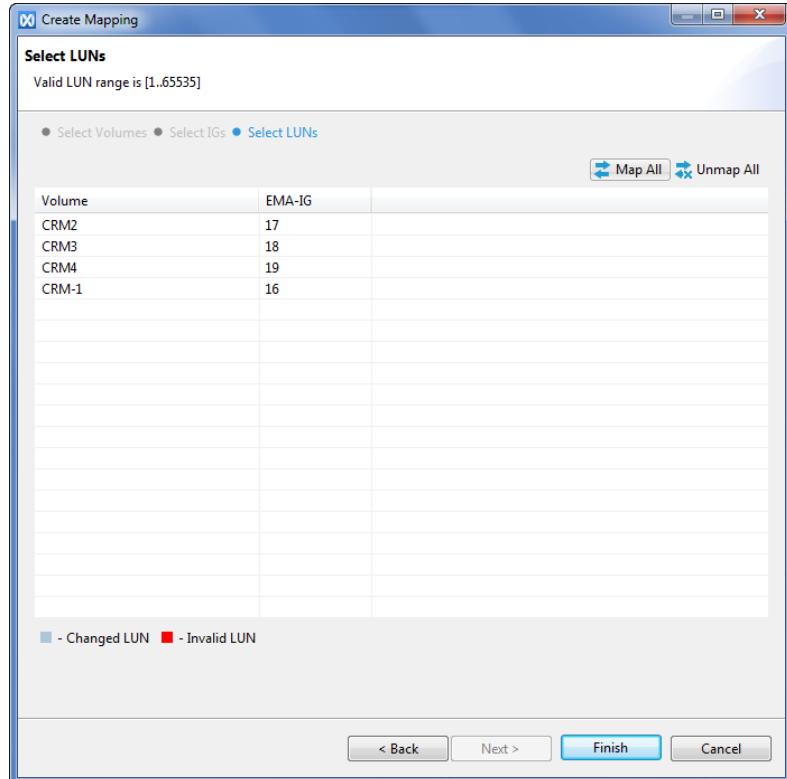


Figure 198 Mapping Wizard

The Mapping Wizard skips the Volume and Initiator Group selection steps (these steps are made redundant by using Tags) and displays the assigned LUNs.

6. Edit the assigned LUNs, if necessary.
7. Click **Finish** to apply the new mapping details.

Using the Mapping Wizard

The mapping wizard is a powerful tool that enables you to locate the relevant objects and perform mapping of multiple objects in a few simple steps.

- ◆ Wizard access - There are various ways to open the mapping wizard, according to the required mapping:
 - To map all Volumes associated with a Tag, right-click the Tag (nested under Volumes in the Virtual tab) and select **Create/Modify Mapping**.
 - To map all Initiator Groups associated with a Tag, right-click the Tag (nested under Initiator Groups in the Virtual tab) and select **Create/Modify Mapping**.
 - To map all Volumes in a Consistency Group, right-click the Consistency Group and select **Create/Modify Mapping**.
 - To map all Volumes in a Snapshot Set, right-click the Snapshot Set and select **Create/Modify Mapping**.

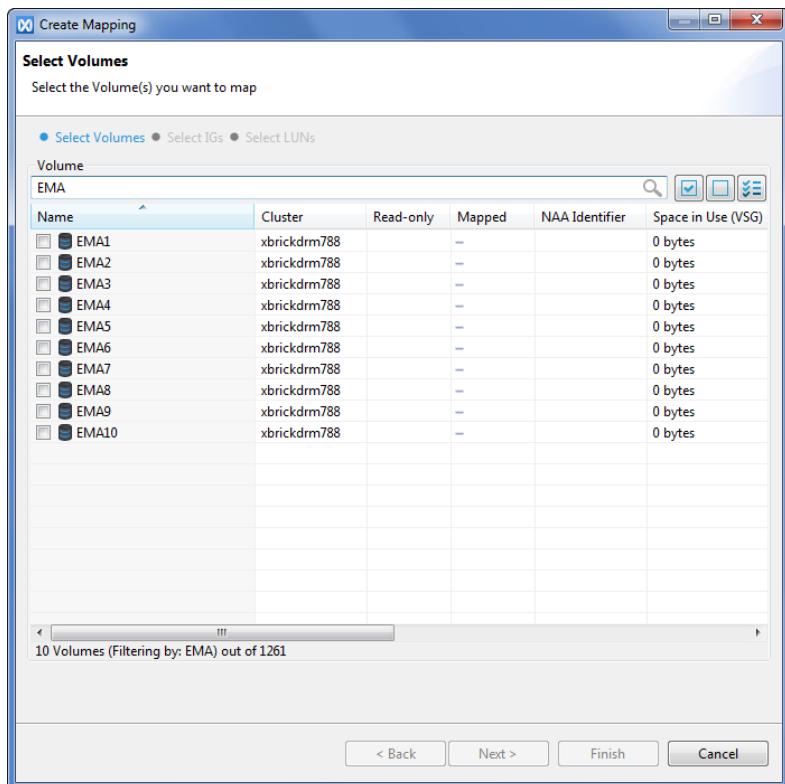


Figure 199 Mapping Wizard - Volumes

- ◆ Filtering - You can use the mapping wizard's filter to select the items you wish to map by typing a full or partial string in the filter field. You can filter the displayed items by any of the displayed fields, e.g. Tag name, NAA identifier, Volume name, size, etc.

The summary line below the table indicates the resulting number of items (out of the total available) and the filtering agent used.

- ◆ Selecting LUNs - In the Select LUNs window, you can edit the displayed LUN numbers. If a LUN number already exists in the cluster configuration, the number is displayed with white (regular) background. If a LUN number is different than the existing cluster configuration, it is displayed with a blue background. Invalid LUNs are displayed with a red background.

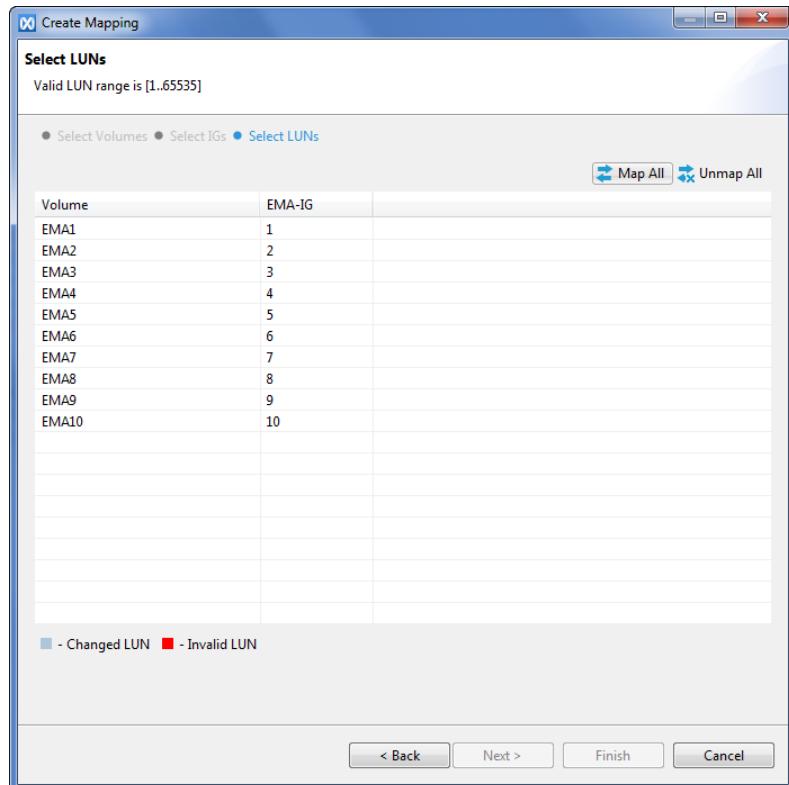


Figure 200 Mapping Wizard - LUNs

You can clear the LUN mapping table and refill it with existing LUN mappings, using the **Unmap All** and **Map All** buttons, respectively. The assigned LUN numbers are applied only when you click **Finish**.

The mapping table also displays mapping of a Volume across multiple Initiator Groups.

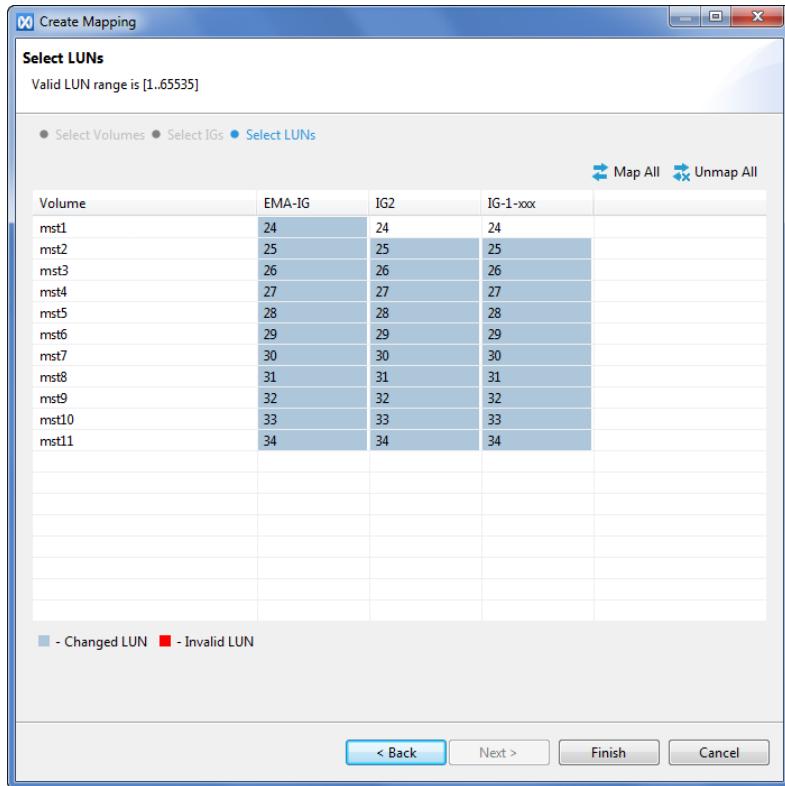


Figure 201 Mapping Wizard - Multiple LUNs

Managing the Schedulers

Managing Schedulers, Using the GUI

Creating a Scheduler

Refer to one of the following:

- ◆ “[Creating a Snapshot Scheduler for Volumes or Snapshots](#)” on page 188
- ◆ “[Creating a Snapshot Scheduler for Consistency Groups](#)” on page 209
- ◆ “[Creating a Snapshot Scheduler for Snapshot Sets](#)” on page 231

Modifying a Scheduler

To modify a Scheduler:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Schedulers** to display the Schedulers window.
3. Right-click the relevant Scheduler in the Schedulers table and select **Modify Snapshot Scheduler** from the drop-down menu.

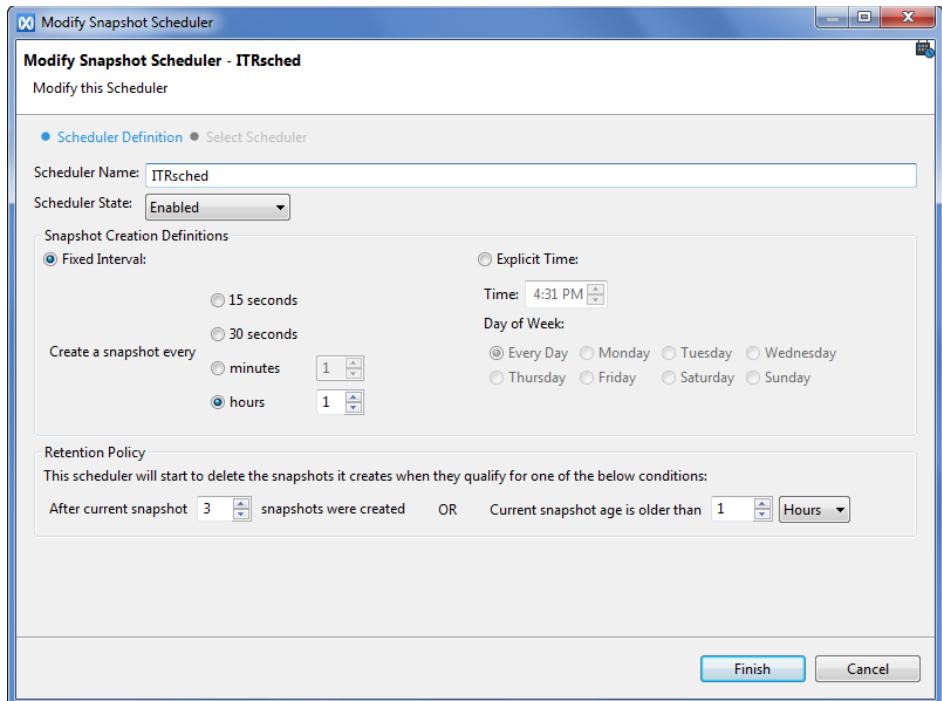


Figure 202 Modify Snapshot Scheduler

4. In the Modify Snapshot Scheduler dialog box, modify the necessary parameters out of the following:
 - Scheduler name
 - Scheduler state
 - Snapshot creation definition
 - Retention policy
5. Click **Finish**; the Scheduler's parameters are updated.

Renaming a Scheduler

To rename a Scheduler:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Schedulers** to display the Schedulers window.
3. Right-click the relevant Scheduler in the Schedulers table and select **Rename** from the drop-down menu.

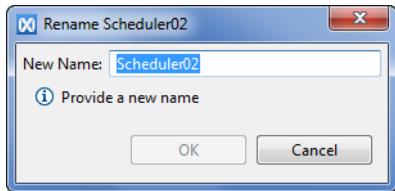


Figure 203 Rename Scheduler Dialog Box

4. In the Rename dialog box, edit the name for the Scheduler.
5. Click **OK**.

Deleting a Scheduler

To delete a Scheduler:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Schedulers** to display the Schedulers window.
3. Right-click the relevant Scheduler in the Schedulers table and select **Delete** from the drop-down menu.
4. Click **Yes** to confirm; the Scheduler is removed from the Schedulers list.

Suspending a Scheduler

To suspend a Scheduler:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Schedulers** to display the Schedulers window.
3. Right-click the relevant Scheduler in the Schedulers table and select **Suspend Scheduler** from the drop-down menu.
4. Click **Yes** to confirm; the Scheduler is suspended and the Scheduler State parameter in the Schedulers table is changed to **Disabled**.

Resuming a Suspended Scheduler

To resume a Suspended Scheduler:

1. From the menu bar, click **Configuration**.
2. In the Virtual tab (left pane), click **Schedulers**.
3. Right-click the relevant suspended Scheduler in the Schedulers table and select **Resume Scheduler** from the drop-down menu.
4. Click **Yes** to confirm; the Scheduler is reactivated and the Scheduler State parameter in the Schedulers table is changed to **Enabled**.

Managing Schedulers, Using the CLI

Scheduler Type and Time Parameters

When you define or modify a scheduler, it is required to specify (among other parameters) the `scheduler-type` parameter and the `time` parameter that derives from it.

Scheduler's type can be either `explicit` or `interval`.

- ◆ Interval scheduler - the time parameter specifies the time intervals at which snapshot are taken, and is specified in the format of `x:y:z` (hours : minutes : seconds).

The valid values for the time parameter are as follows:

- Hours: 0 - 72
- Minutes: 0 - 59
- Seconds: 0, 15, 30

At least one of the time parameter variants must have a value other than zero.

If Hours or Minutes values are other than zero, Seconds value must be zero (i.e. snapshots are created every x hours and y minutes).

If Seconds are specified (i.e. 15 or 30), Hours and Minutes' values must be zero (i.e. snapshots are created every 15 or 30 seconds).

Example of the time parameter usage for an interval scheduler:

```
create-scheduler scheduler-type=interval time=[1:30:0] ...
```

The scheduler created in the example creates a snapshot every hour and a half.

- ◆ Explicit scheduler - the time parameter specifies the specific day and time at which the snapshots are taken, and is specified in the format of x:y:z [day of the week : hour : minute].

The valid values for the time parameter are as follows:

- Day of the week: 0 stands for every day; 1- 7 stands for Sunday to Saturday, respectively
- Hour: 0 - 23
- Minute: 0 - 59

Example of the time parameter usage for an explicit scheduler:

```
create-scheduler scheduler-type=explicit time=[1:12:30] ...
```

The scheduler created in the example creates a snapshot every Sunday at 12:30.

Scheduler Related CLI Commands

Use the following CLI commands for managing Schedulers:

Command	Description
create-scheduler	Creates a new Snapshot Scheduler.
modify-scheduler	Modifies a Snapshot Scheduler's parameters.
remove-scheduler	Removes a Snapshot Scheduler.
resume-scheduler	Reactivates a suspended Snapshot Scheduler.
show-schedulers	Displays the defined Schedulers parameters
suspend-scheduler	Suspends an active Snapshot Scheduler.

CHAPTER 6

Managing Alerts and Events

This chapter includes the following topics:

- ◆ [Managing the Alerts](#) 266
- ◆ [Managing the Events.....](#) 271

Managing the Alerts

Alerts Overview

The XtremIO Storage Array's alert system has a pre-defined set of cluster-related alerts.

An alert indicates a condition that requires user attention and in some cases needs user intervention.

You can use the alert system to view active alerts, edit alerts properties, and display and acknowledge alerts.

Managing Alerts, Using the GUI

You can view the alerts in:

- ◆ The Alerts pane of the Dashboard workspace, as described in “[Alerts Pane](#)” on [page 49](#)
- ◆ The Alerts tab of the Alerts & Events workspace, as described in “[Alerts Tab](#)” on [page 95](#)

Displaying Alerts' Definitions

To display alert's definitions:

1. From the menu bar, click the **Alerts & Events** icon to display the Alerts & Events workspace, as shown in [Figure 68 on page 94](#).
2. From the Alerts tab, click the **Display Alert Definitions** icon (see [Figure 69 on page 95](#)); the Alert Definition dialog box appears.

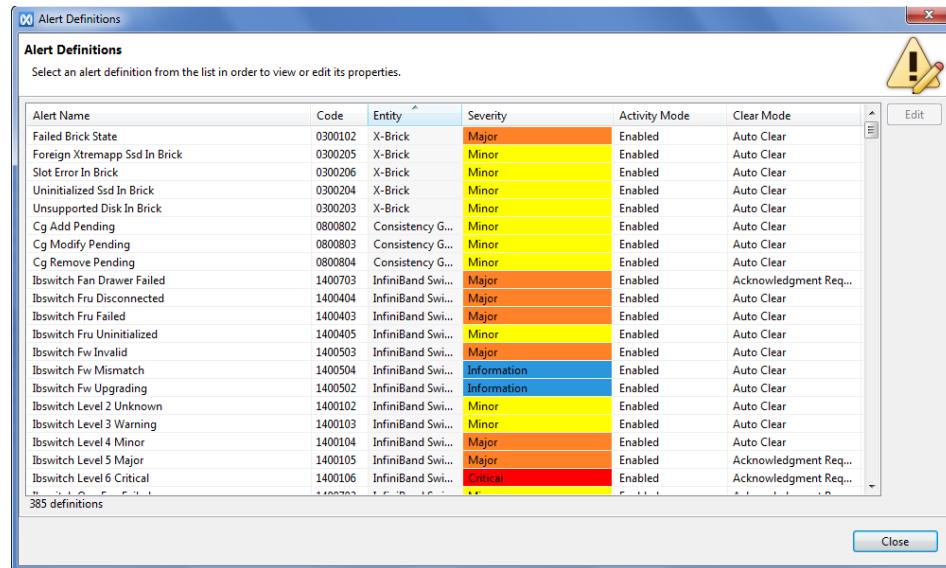


Figure 204 Alert Definition Dialog box

For each alert, the following information is displayed:

- Alert name
- Alert code
- Entity
- Severity level
- Activity mode
- Clear mode

You can edit an alert's definition by selecting it and clicking **Edit**, or by double-clicking the alert to open the Edit Alert Definition dialog box.

To close the Alert Definitions dialog box, click **Close**.

Editing Alert Definition

To edit an alert's Definition:

1. From the Alerts tab, click the **Display Alert Definitions** icon (see [Figure 69 on page 95](#)); the Alert Definition dialog box appears.
2. Double-click an alert or click an alert to select it and click **Edit**; the Edit Alert Definition dialog box appears.

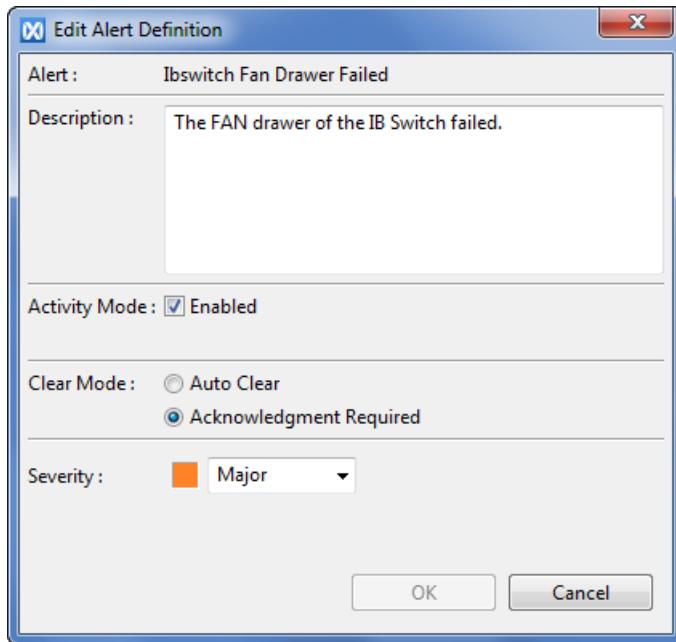


Figure 205 Edit Alert Definition Dialog Box

Note: You can also open the Edit Alert Definition dialog box by right-clicking an alert in the Alerts tab and selecting **Edit Alert Definition** from the drop-down menu.

3. Modify the following characteristics:
 - Activity Mode - Determines whether the alert is enabled or disabled.
 - Clear Mode - Determines whether the alert is cleared automatically when the condition it refers to is resolved, or requires acknowledgment.
 - Severity - Determines the severity level of the alert (displayed both textually and by color).
4. Click **OK**.

Viewing the Alert Properties

To view an alert's properties:

1. Double-click an alert in the Alerts tab or right-click an alert to select it and select **Properties** from the drop-down menu; the Alert Properties dialog box appears.

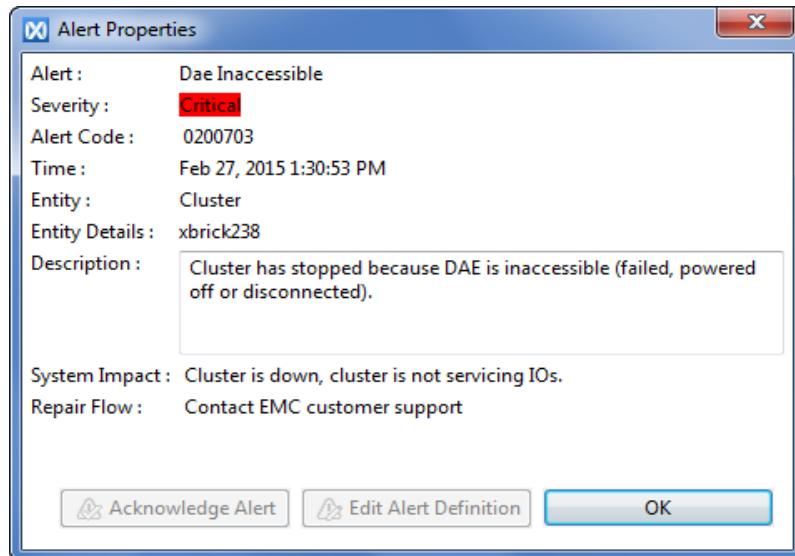


Figure 206 Alert Properties Dialog Box

The Alert Properties dialog box displays the following:

- Alert's name
- Alert's severity level
- Alert's code
- Alert's time stamp, indicating when it was first recognized by the XMS
- Name of the entity to which the alert refers
- The entity's details
- Alert's description
- System Impact - the possible impact of the active alert on the cluster
- Repair Flow - the required repair action to be performed on the cluster

You can acknowledge the alert or edit its definition in the Alert Properties dialog box.

2. Click **OK** to close the dialog box.

Acknowledging an Alert

When you acknowledge an alert, it is removed from the Alert panel of the dashboard. However, acknowledged alerts remain on the Alert List and the word "Acknowledged" is added in parentheses to the Severity column.

Alerts that have the Clear Mode field set as "Acknowledge Required", remain on the Alert list even after the alert issue is resolved, and can be removed from the Alert list only after they are acknowledged (the alert may be acknowledged before the issue is resolved).

To acknowledge an alert:

- ◆ Right-click the alert and select **acknowledge alert**.

Note: You can remove the acknowledged alerts from the displayed alerts' list by clicking the **Hide Acknowledged Alerts** check box in the Alerts tab of the Alerts & Events workspace.

Managing Alerts, Using the CLI

Setting Thresholds

Using the CLI it is possible to set thresholds for user capacity and receive alerts when the set threshold is exceeded. You can set the threshold for the following alerts:

- ◆ `user_physical_capacity_high`
- ◆ `user_physical_capacity_very_high`

The alerts' default parameters are:

- ◆ State - disabled
- ◆ Severity - minor
- ◆ Threshold -
 - `user_physical_capacity_high` - 70%
 - `user_physical_capacity_very_high` - 80%

To view the alerts' settings, run the `show-alert-definitions` CLI command.

To modify the alerts' settings run the `modify-alert-definitions` CLI command.

Managing Alerts

Use the following CLI commands for managing alerts:

Command	Description
acknowledge-alert	Acknowledges an alert and removes it from the dashboard Active Alerts list. The alert remains in the Alert List window. Alerts with Clear Mode set to Acknowledge Required, remain on the Alert List until they are acknowledged.
modify-alert-definition	Modifies the alert definition properties for a specified alert type.
show-alert-definitions	Displays a list of pre-defined alerts and their definitions.

Managing the Events

Managing Events, Using the GUI

Viewing Events' Properties

To view events' properties:

1. From the menu bar, click the **Alerts & Events** icon to display the Alerts & Events workspace, as shown in [Figure 68 on page 94](#).
2. Select the Events tab, as shown in [Figure 71 on page 97](#).
3. Double-click an event to open the Event Properties dialog box.

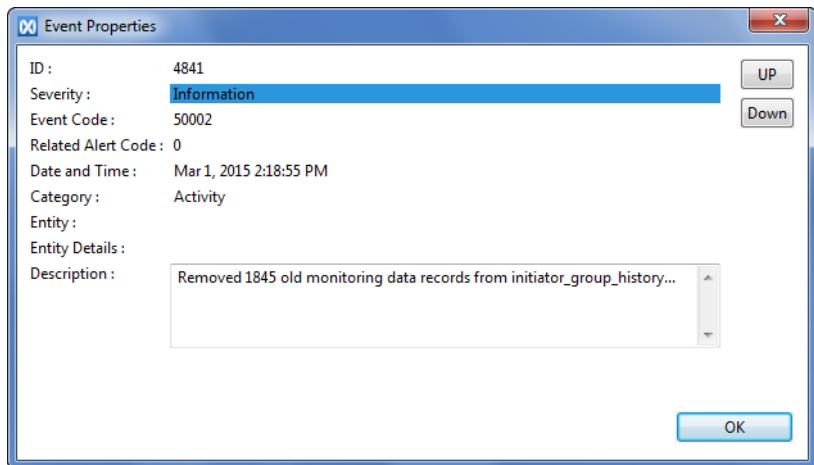


Figure 207 Event Properties Dialog Box

The Event Properties dialog box displays the following:

- Event's ID
 - Event's severity level
 - Event's code
 - Related alert code
 - Event's time stamp indicating when it was first recognized by the XMS
 - Event's category
 - Name of the entity to which the event refers
 - Entity's details
 - Event's description
4. Browse through the events list, using the **Up** and **Down** buttons.
 5. Click **OK** to close the dialog box.

Filtering Events

You can filter events, using the filters in the Events tab of the Alerts & Events workspace.

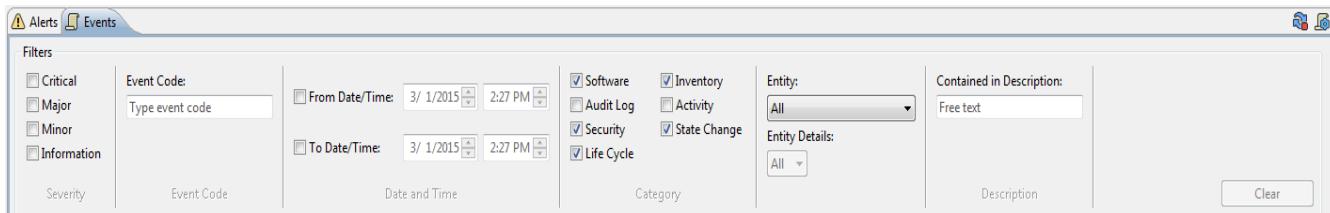


Figure 208 Event Filters

The filters include:

- ◆ Severity level - Select one or more of the following levels:
 - Critical
 - Major
 - Minor
 - Information
- ◆ Event Code - Type an event code or a part of an event code to view only the matching events.
- ◆ Date and Time - Set a date and time frame by selecting From Date/Time, To Date/Time, or both, and setting the date and time data.
- ◆ Category - Select one or more of the following categories:
 - Software
 - Audit Log
 - Security
 - Life Cycle
 - Inventory
 - Activity
 - State Change
- ◆ Entity - Select the entity and entity details from the respective drop-down lists.
- ◆ Search - Type a search string to search for matching events.

To clear event filters settings, click **Clear**.

Managing Event Handlers

Event handlers allow you to perform various actions for events with different properties.

You can add, edit and remove event handlers according to your needs.

To display the Event Handlers dialog box:

1. From the menu bar, click the **Alerts & Events** icon to display the Alerts & Events workspace, as shown in [Figure 68 on page 94](#).
2. From the Events tab, click the **Display Event Handlers** icon (located in the top-right corner of the window); the Event Handlers dialog box appears.

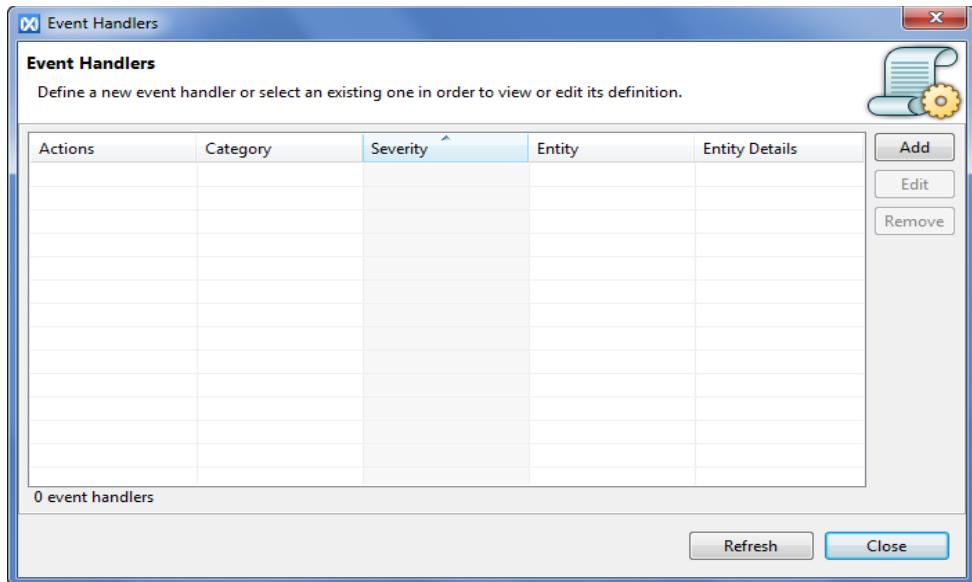


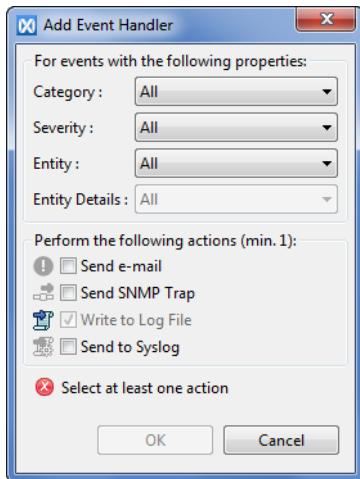
Figure 209 Event Handlers Dialog Box

For each event handler, the following information is displayed:

- Actions - the actions that are performed following the event
- Category - the event's category
- Severity - the event's severity level
- Entity - the entity type to which the event refers
- Entity Details - the specific entity to which the event refers

To add an event handler:

1. In the Event Handlers dialog box, click **Add**; the Add Event Handler dialog box appears.

**Figure 210** Add Event Handler Dialog Box

2. Set the event properties for which to perform the action (for detailed categories values, refer to [Filtering Events](#)):
 - a. Click the Category drop-down list to expand it and select an event category (default is All).
 - b. Click the Severity drop-down list to expand it and select a severity level (default is All).
 - c. Click the Entity drop-down list to expand it and select an entity type (default is All).
 - d. If you selected an entity (other than All), click the Entity Details drop-down list to select the entity details.
3. Select the actions to be performed following the events you defined. You need to select at least one of the following actions:
 - Send e-mail
 - Send SNMP Trap
 - Write to Log File - this option is automatically performed and therefore grayed out.
 - Send to Syslog
4. Click **OK**; the new event handler is added to the Event Handler table.

Note: When setting a severity level, only events with the selected severity level are addressed. This does not affect events with other (higher or lower) severity levels.

To edit an event handler properties:

1. In the Event Handlers dialog box, select an event handler by clicking its entry in the table.
2. Click **Edit**; the Edit Event Handler dialog box appears.

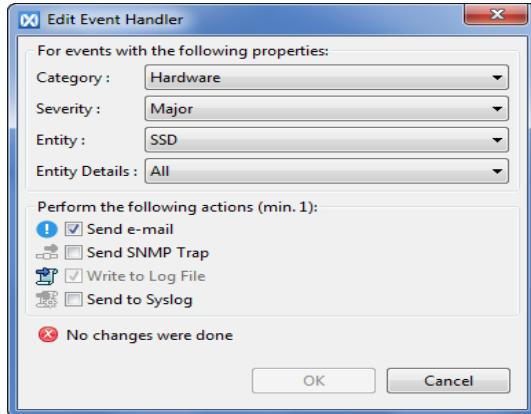


Figure 211 Edit Event Handler Dialog Box

3. Edit the event handler properties and click **OK**; the updated event handler appears in the Event Handlers table.

To remove an event handler:

1. In the Event Handler dialog box, select an event handler by clicking its entry in the table.
2. Click **Remove**.
3. Confirm removal by clicking **Yes** in the Remove Event Handler dialog box; the event handler is removed from the Event Handlers table.

Managing Events, Using the CLI

Use the following CLI commands for managing events:

Command	Description
add-event-handler-definition	Adds a definition to an event handling rule.
remove-event-handler-definition	Deletes the event handling rule definitions.
modify-event-handler-definition	Modifies the definition of event handling rules.
show-event-handler-definitions	Displays the event handling rule definitions.

CHAPTER 7

Cluster Administration and Configuration

This chapter includes the following topics:

◆ Configuring the iSCSI Portals and Routes.....	278
◆ Configuring the iSCSI Port Number	284
◆ Setting the Maximum Transmission Unit for iSCSI.....	286
◆ Configuring the Cluster Limits.....	288
◆ Configuring the Cluster ODX Mode.....	289
◆ Configuring the iSCSI Security Parameters (CHAP)	291
◆ Configuring the Cluster Encryption	293
◆ Configuring the User Accounts.....	294
◆ Configuring the LDAP Users Authentication	298
◆ Configuring Email Settings	308
◆ Configuring the SNMP	311
◆ Configuring the Remote Syslog Notification.....	314
◆ Configuring the Default Inactivity timeout.....	316
◆ Customizing the Login Screen Banner	317

Configuring the iSCSI Portals and Routes

To establish an iSCSI connection for transferring data, you should first define an iSCSI portal. An iSCSI portal is an IPv4 address and port associated with a Target port.

Each iSCSI Target can be associated with multiple portals.

If an IP connection requires routing to remote networks, you can define routing rules that apply to the iSCSI Target ports only.

Managing iSCSI Portals and Routes, Using the GUI

Configuring the iSCSI Portals

To configure an iSCSI portal:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 73 on page 101](#).
2. Click **Inventory List** to view the list of hardware elements.
3. In the Hardware tab (left pane), click **Clusters** to view the defined clusters in the main window.
4. Select the relevant cluster and click **Configure Cluster** from the menu bar.
5. In the Configure Cluster Dialog box, click the **iSCSI Network Configuration** tab; the iSCSI Network Configuration screen appears, as shown in [Figure 212](#).

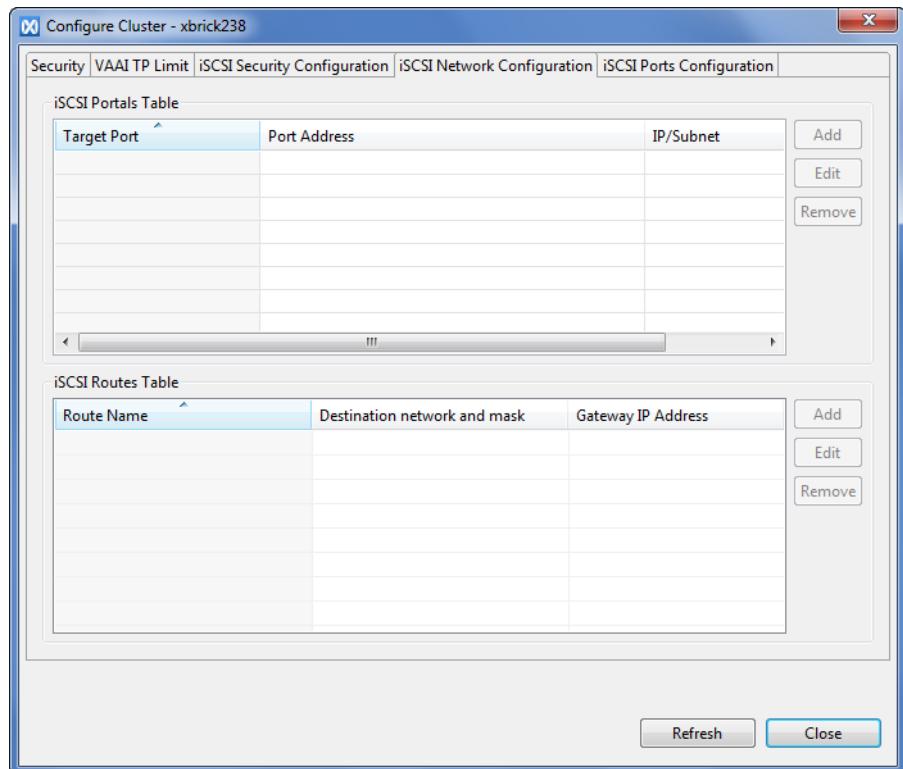


Figure 212 Configure Cluster - iSCSI Network Configuration Tab

6. In the iSCSI Portal Table, click **Add**; the Add iSCSI Portal dialog box appears.

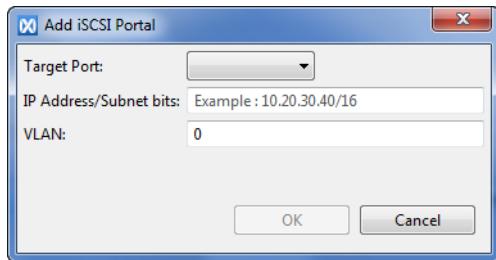


Figure 213 Add iSCSI Portal Dialog Box

7. Select a Target port from the Target Port drop-down list.
8. Type the portal's IP address and subnet bits.

Note: iSCSI Targets cannot have the same subnet as the management network.

9. Click **OK** to confirm and close the dialog box; the defined portal is added to the iSCSI portals table.

Click the arrow next to the Target port name, to view all the defined portals associated with a Target port.

Note: Only active/relevant options are described in Add iSCSI Portal dialog box.

Modifying the iSCSI Portal Data

To modify the iSCSI portal data:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 73 on page 101](#).
2. Click **Inventory List** to view the list of hardware elements.
3. In the Hardware tab (left pane), click **Clusters** to view a list of the defined clusters in the main window.
4. Select the relevant cluster and click **Configure Cluster** from the menu bar.
5. In the Configure Cluster dialog box, click the **iSCSI Network Configuration** tab; the iSCSI Network Configuration screen appears, as shown in [Figure 212](#).
6. In the iSCSI Portal table, click the portal you wish to modify and click **Modify**.

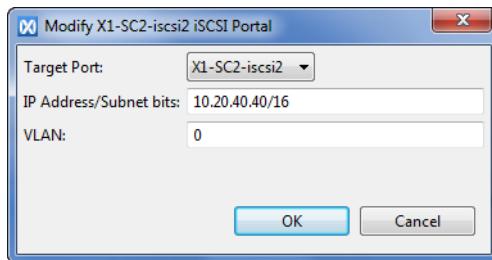


Figure 214 Modify iSCSI Portal Dialog Box

7. Modify the portal's parameters (Target Port, IP Address/Subnet bits).
8. Click **OK** to confirm the changes and close the dialog box.

Removing an iSCSI Portal

To remove an iSCSI portal:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 73 on page 101](#).
2. Click **Inventory List** to view the list of hardware elements.
3. In the Hardware tab (left pane), click **Clusters** to view a list of the defined clusters in the main window.
4. Right-click the relevant cluster and select **Configure Cluster** from the drop-down menu.
5. In the Configure Cluster dialog box, click the **iSCSI Network Configuration** tab.
6. In the iSCSI Portal table, click the portal you wish to remove and click **Remove**.
7. Click **Yes** to confirm the removal; the portal is deleted from the table.

Configuring the iSCSI Routes

In rare cases, iSCSI Initiators are connected to different network subnets and require a router to connect to the iSCSI portals.

To configure an iSCSI route:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 73 on page 101](#).
2. Click **Inventory List** to view the list of hardware elements.
3. In the Hardware tab (left pane), click **Clusters** to view a list of the defined clusters in the main window
4. Select the relevant cluster and click **Configure Cluster** in the menu bar.
5. In the Configure Cluster dialog box, click the **iSCSI Network Configuration** tab.
6. In the iSCSI Routes Table, click **Add**; the Add iSCSI Route dialog box appears.

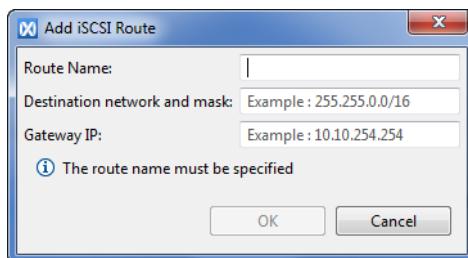


Figure 215 Add iSCSI Route Dialog Box

7. Type the route name.
8. Type the destination subnet/subnet bits according to the displayed example.
9. Type the gateway IP according to the displayed example.
10. Click **OK** to confirm and close the dialog box; the defined route is added to the iSCSI Routes table.

Modifying an iSCSI Route

To modify a defined iSCSI route:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 73 on page 101](#).
2. Click **Inventory List** to view the list of hardware elements.
3. In the Hardware tab (left pane), click **Clusters** to view a list of the defined clusters in the main window.
4. Select the relevant cluster and click **Configure Cluster** in the menu bar.
5. In the Configure Cluster dialog box, click the **iSCSI Network Configuration** tab.
6. In the iSCSI Routes table, click the route entry you want to modify and click **Modify**; the Modify iSCSI Route dialog box appears.

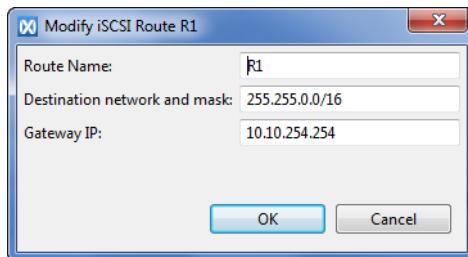


Figure 216 Modify iSCSI Route Dialog Box

7. Modify the iSCSI route parameters.
8. Click **OK** to confirm the changes and close the dialog box.

Removing an iSCSI Route

To remove an iSCSI route:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 73 on page 101](#).
2. Click **Inventory List** to view the list of hardware elements.
3. In the Hardware tab (left pane), click **Clusters** to view a list of the defined clusters in the main window.
4. Select the relevant cluster and click **Configure Cluster** in the menu bar.
5. In the Configure Cluster dialog box, click the **iSCSI Network Configuration** tab.
6. In the iSCSI Route table, click to select the route entry you wish to remove.
7. Click **Remove**.
8. Click **Yes** to confirm route's removal; the route is deleted from the table.

Managing iSCSI Portals and Routes, Using the CLI

Use the following CLI commands for managing iSCSI portals and routes:

Command	Description
add-iscsi-portal	Maps a portal to a Target.
add-iscsi-route	Adds and configures iSCSI route parameters.
remove-iscsi-portal	Deletes a portal mapping from a Target.
remove-iscsi-route	Deletes an iSCSI routing configuration.
show-iscsi-portals	Displays a list of iSCSI portals and their properties.
show-iscsi-routes	Displays a list of iSCSI routes and their properties.

Configuring the iSCSI Port Number

Using the iSCSI Ports Configuration screen you can:

- ◆ Change iSCSI TCP port -
The XtremIO cluster uses the iSCSI default port (3260). You can change the default port.
- ◆ Enable or disable jumbo frames -
When jumbo frames are enabled, you can set the Ethernet adapter MTU to any value between 1500 bytes and 9216 bytes.

Configuring the iSCSI Port via the GUI

The Listen TCP Port field displays port 3260 by default.

Note: Configuring the iSCSI port number can be done only when the cluster is inactive.

Note: The default TCP Port value is grayed out. To enable the field and change the port number, the cluster needs to be stopped.

To change the TCP Port number:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **CLI Terminal** tab to open the CLI terminal.
3. Stop the cluster, using the `stop-cluster` CLI command (for details, refer to [“stop-cluster” on page 397](#)). Wait for a confirmation that the cluster has stopped.
1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 73 on page 101](#).
2. Click **Inventory List** to view the list of hardware elements.
3. In the Hardware tab (left pane), click **Clusters** to view a list of the defined clusters in the main window
4. Select the relevant cluster and click **Configure Cluster** in the menu bar.

5. In the Configure Cluster dialog box, click the **iSCSI Ports Configuration** tab.

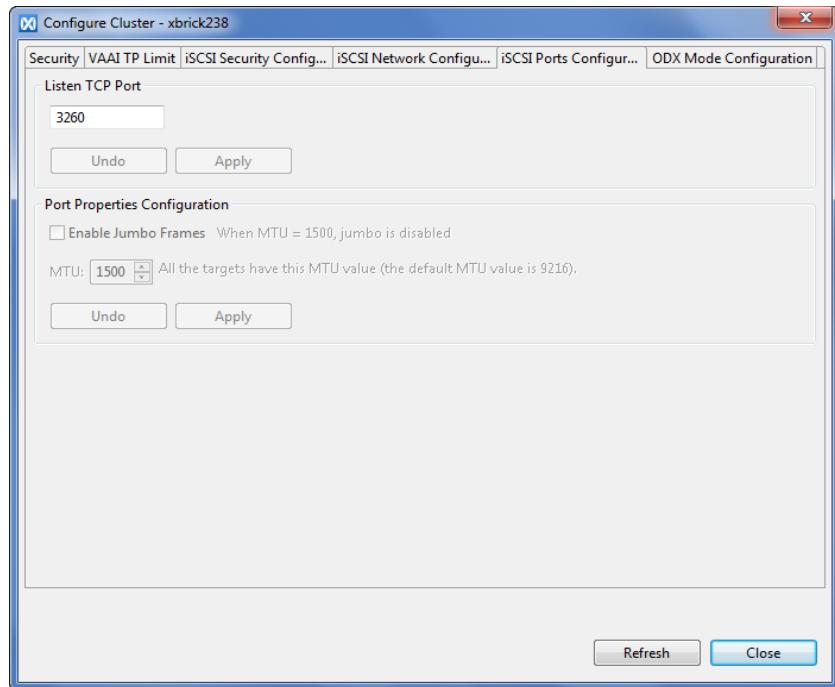


Figure 217 Configure Cluster - iSCSI Ports Configuration Tab

6. In the **Listen TCP Port** field, enter the new port number.
7. Click **Apply** and **Close**.
8. Click **Administration** and then click the **CLI Terminal** tab to return to the CLI terminal.
9. Restart the cluster, using the `start-cluster` CLI command (for details, refer to “[start-cluster](#)” on page 397). Wait for a confirmation that the cluster has started.

Setting the Maximum Transmission Unit for iSCSI

iSCSI networks enable traffic of SCSI commands over TCP/IP data packets. Setting the Maximum Transmission Unit (MTU) may influence the bandwidth, latency and reliability of the network.

With the XtremIO Storage Array, the maximum transmission unit can be set to a value ranging from 1,500 bytes (default) up to 9,216 bytes. The top value is referred to as jumbo frames.

The following are the main pros and cons of increasing the default MTU size:

Pros:

- ◆ Each packet carries more user data, while protocol overheads, such as headers or underlying per-packet delays, remain fixed.
- ◆ Fewer packets are processed for the same amount of data.

Cons:

- ◆ Large packets occupy a slow link for more time than smaller packets, causing greater delays to subsequent packets.
- ◆ Larger packets are more likely to be corrupt. Corruption of a single bit in a packet requires that the entire packet be retransmitted.

To transfer a packet successfully from one NIC to another, the entire LAN path must be configured to support the specific packet's size. Otherwise, the packet may be either fragmented to a supported size, or in other cases, discarded (if the TCP header "**Don't Fragment**" flag is set). When increasing the MTU, it is necessary to verify that every NIC on the path (between the host and the XtremIO Storage Controller) supports the requested MTU.

Configuring Jumbo Frames via the GUI

When enabled, Jumbo Frames Maximum Transmission Unit (MTU) is set by default to 9216. Re-enabling the Jumbo Frames option after disabling it, displays the last MTU value set before it was disabled.

Note: Enabling and disabling the Jumbo Frame option is carried out per cluster and requires restarting the iSCSI service which will cause existing connections to drop.

Note: When configuring jumbo frames:

- ◆ The set MTU should match the maximal MTU supported in your networking infrastructure.
- ◆ All networking devices, including switches and hosts, should support the new MTU.

Disregarding this or setting a wrong MTU can result in packet fragmentation or discarded packets.

To enable the Jumbo Frames option:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 73 on page 101](#).
2. Click **Logical View** to view the list of hardware elements.
3. In the Hardware tab (left pane), click **Clusters** to view a list of the defined clusters in the main window
4. Right-click the relevant cluster and select **Configure Cluster** from the drop-down menu.
5. In the Configure Cluster dialog box, click the **iSCSI Ports Configuration** tab.
6. In the Port Properties Configuration section, select the **Enable Jumbo Frames** option.
7. Set the MTU value, using the up and down arrows.
8. Click **Apply**.

Configuring the Cluster Limits

The Cluster Limits section in the Cluster Configuration screen enables you to set a thin provisioning soft limit (TPST). The limit is set as a percentage of the storage capacity and can be up to 100%. The set limit is used as the threshold that triggers sending a warning on the SCSI interface for Volumes with set VAAI limits.

Configuring Cluster Limits via the GUI

To set the cluster VAAI TP limit:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 73 on page 101](#).
2. Click **Inventory List** to view the list of hardware elements.
3. In the Hardware tab (left pane), click **Clusters** to view a list of the defined clusters in the main window.
4. Select the relevant cluster and click **Configure Cluster** in the menu bar.
5. In the Configure Cluster dialog box, click the **VAAI TP Limit** tab.

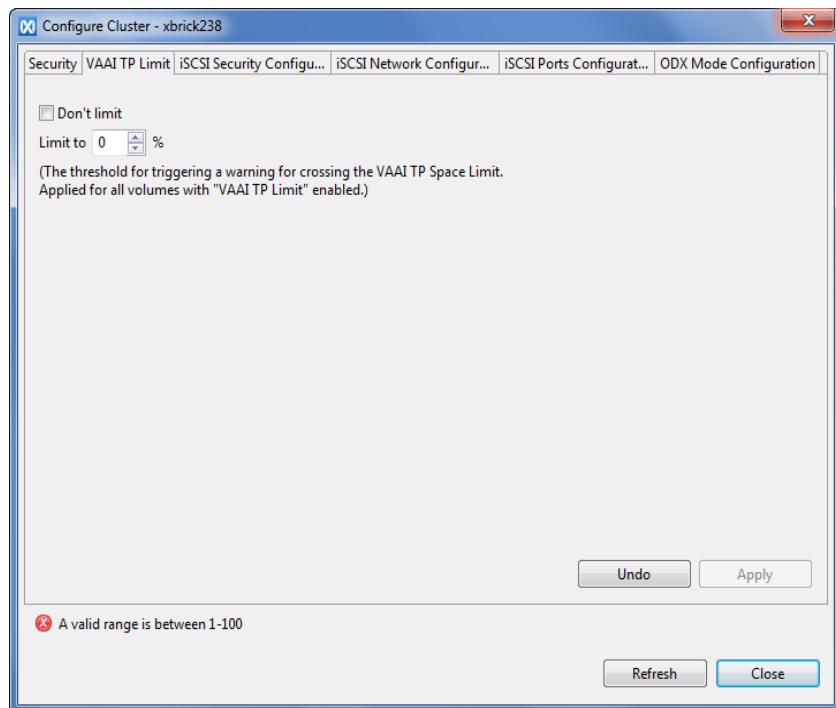


Figure 218 Configure Cluster - VAAI TP Limit Tab

6. In the VAAI TP Limit section, leave the **don't limit** option unselected, to set a thin provisioning soft limit.
7. Set the limit, using the up and down arrows. The limit can be set between 1% and 100%.
8. Click **Apply** and **Close**.

Configuring Cluster Limits via the CLI

Using the CLI, it is possible to set thresholds for user capacity and receive alerts when the threshold is exceeded. Refer to “[Setting Thresholds](#)” on page 270 for details.

Use the following CLI command for setting the cluster limits:

Command	Description
modify-cluster-thresholds	Modifies the properties for thin provisioning soft limits for connected clusters.
modify-alert-definition	Modifies the alert definition properties for a specified alert type.

Configuring the Cluster ODX Mode

XtremIO is an ODX-capable storage array, supporting offloaded read and write operations for Windows environments. ODX is supported within the domain of an XtremIO array (i.e. source and destination LUNs must reside on the same array).

XtremIO provides the Initiator with its preferred optimal transfer size (0 - 256MB). However, Initiators are not obligated to use the optimal size.

ODX support is provided on all FE interfaces (FC or iSCSI) and is supported for both Volumes and Snapshots.

Configuring the ODX Mode via the GUI

Note: The ODX Mode field is grayed out. To enable the field and configure the ODX mode, the cluster needs to be stopped.

To configure the ODX mode:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **CLI Terminal** tab to open the CLI terminal.
3. Stop the cluster, using the `stop-cluster` CLI command (for details, refer to “[stop-cluster](#)” on page 397). Wait for a confirmation that the cluster has stopped.
1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 73 on page 101](#).
2. Click **Inventory List** to view the list of hardware elements.
3. In the Hardware tab (left pane), click **Clusters** to view a list of the defined clusters in the main window
4. Select the relevant cluster and click **Configure Cluster** in the menu bar.

5. In the Configure Cluster dialog box, click the **ODX Mode Configuration** tab.

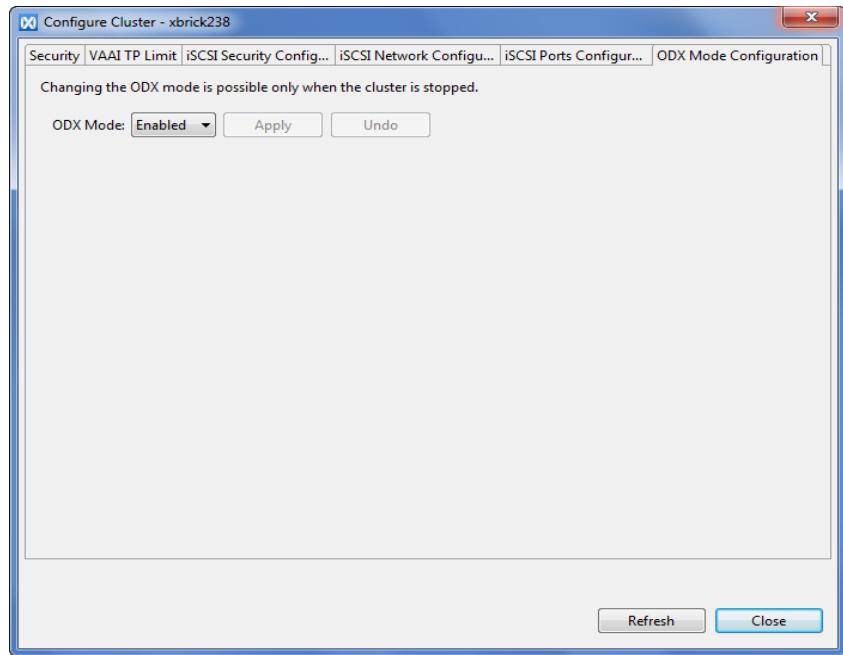


Figure 219 Configure Cluster - ODX Mode Configuration Tab

6. In the **ODX Mode** field, select Enabled or Disabled from the drop-down list..
7. Click **Apply** and **Close**.
8. Click **Administration** and then click the **CLI Terminal** tab to return to the CLI terminal.
9. Restart the cluster, using the `start-cluster` CLI command (for details, refer to [“start-cluster” on page 397](#)). Wait for a confirmation that the cluster has started.

Configuring the ODX Mode via the CLI

Use the following CLI command for setting the cluster’s ODX mode:

Command	Description
<code>modify-clusters-parameters</code>	Modifies various cluster parameters.
<code>show-clusters-parameters</code>	Displays various cluster parameters.

Configuring the iSCSI Security Parameters (CHAP)

iSCSI Initiators and Targets prove their identity to each other, using the Challenge-Handshake Authentication Protocol (CHAP), which includes a mechanism to prevent clear text passwords from appearing on the wire.

It is possible to configure CHAP for Initiator login and for the discovery phase. It is also possible to configure Mutual CHAP for the Initiator to authenticate the XtremIO Targets.

When using CHAP, each Initiator that is added to an Initiator Group is assigned with a username and password (sometimes called CHAP secret). The same username and password must be configured on the host's side and be used for the first login. Initiators that do not provide the correct username and password are rejected and will not be able to read and write data.

It is possible to configure CHAP username and password for the discovery phase. When configured, hosts must provide the correct username and password to be able to discover the available Targets on the XtremIO cluster.

Note: Login username and password cannot be the same as the discovery username and password.

When Mutual CHAP is configured, the hosts authenticate the cluster, using a pre-configured username and password. When Mutual CHAP is enabled, a unique set of username and password is configured for each Initiator for login and discovery. The system administrator must configure the username and password on the host side to enable it to authenticate the XtremIO Targets.

Note: When working in Mutual CHAP mode (Initiator and Target), the cluster's username and password should be different from any of the Initiators' usernames and passwords.

Configuring CHAP via the GUI

To configure the Initiators discovery CHAP:

1. From the menu bar, click the **Inventory** icon to display the Inventory workspace, as shown in [Figure 73 on page 101](#).
2. Click **Inventory List** to view the list of hardware elements.
3. In the Hardware tab (left pane), click **Clusters** to view a list of the defined clusters in the main window.
4. Select the relevant cluster and click **Configure Cluster** in the menu bar.
5. In the Configure Cluster dialog box, click the **iSCSI Security Configuration** tab.

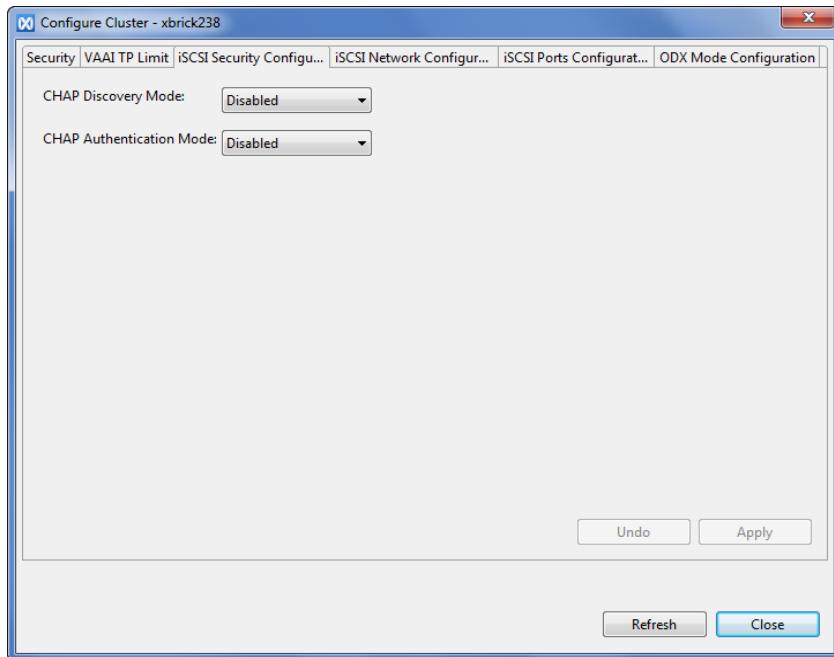


Figure 220 Configure Cluster - iSCSI Security Configuration Tab

6. If you want to configure CHAP for discovery, select the value for **CHAP Discovery Mode** from the drop-down list as follows:
 - Disabled - default mode, CHAP Discovery is not active.
 - Initiator - the Target allows discovery only for Initiators with pre-configured name and password.
 - Initiator and Target - Initiator and Target perform authentication before discovery.
7. If you want to configure CHAP for authentication, repeat [step 6](#) in the **CHAP Authentication Mode** area.

Note: when enabling CHAP (either "Initiator" or "Initiator and Target" mode), it is required to configure the iSCSI Initiators with Username and Password.

Configuring CHAP via the CLI

Use the following CLI command for setting the cluster's ODX mode:

Command	Description
modify-chap	Modifies CHAP configuration parameters.
show-chap	Displays the cluster's configured CHAP authentication and discovery modes.

Configuring the Cluster Encryption

To configure the cluster encryption, contact EMC Global Tech Support.

Configuring the User Accounts

User Accounts Overview

You can create user accounts and define their authorization roles as required. Each user account has its own User ID (i.e. the user account name), password, and the user's authorized capabilities and roles.

You can create user accounts for remote CLI users. These users can access the cluster only via the CLI. When creating a user account for a remote user, a public key is defined instead of a password.

The following user accounts are built into the cluster with predefined authorization roles and cannot be removed, renamed or modified:

- ◆ Admin - This role can perform all user commands and manage all user accounts, except for the Tech user account.
- ◆ Tech - This role can perform all commands and manage all user accounts. This account is for use only by XtremIO Storage Array trained support personnel.

Managing User Accounts, Using the GUI

Adding a User

To add a new user:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Security** tab and select **Users Administration** from the left pane; the Users Administration screen appears, as shown in [Figure 74 on page 102](#).
3. Click **Add** to open the Add New User dialog box (you can also right-click an existing user and select **Add**).

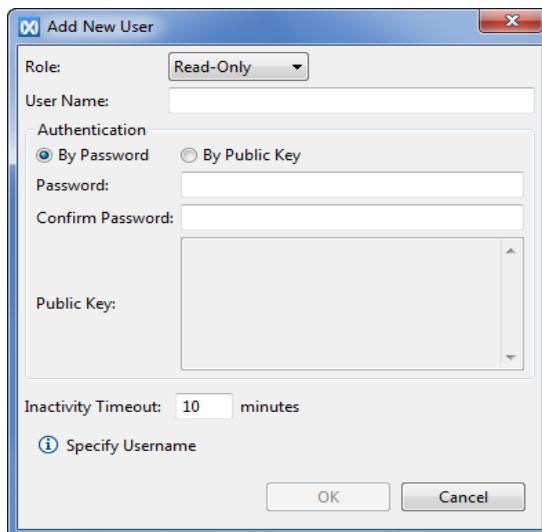


Figure 221 Add New User Dialog Box

4. Select the new user's role from the drop-down list (Administrator, Configuration, or Read-Only).
5. Type a unique user name.
6. Select the authentication method, according to the user type (By Password or By Public Key).
7. If you selected the Password option, type a password and confirm it.
If you selected the Public Key option, enter the public key.

Note: Public key users are limited to CLI access and are used to run scripts from external hosts without requiring a password. Creating the user on the external hosts and generating an SSH public key pair is out of the scope of this document and should be carried out according to the external hosts' OS procedures.

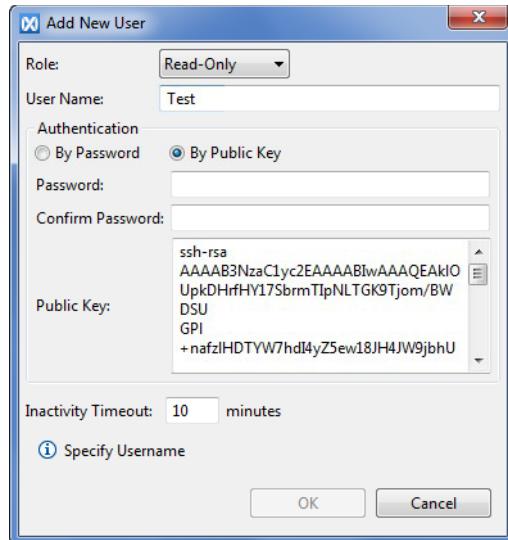


Figure 222 Add New User Dialog Box - Public Key

8. Set the Inactivity Timeout for the user. The displayed default value is set in the XMS Configuration screen (see “Configuring the Default Inactivity timeout” on page 316).
9. Click **OK** to confirm and close the dialog box; the new user is added to the user's list.

Note: If the added user was authenticated by an external server (i.e. Active Directory) and is not locally defined, the Is External field is set to Yes.

Modifying the User Role, Name and Password

To modify a user's data:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Security** tab and select **Users Administration** from the left pane; the Users Administration screen appears, as shown in [Figure 74 on page 102](#).
3. In the users table, click the relevant user to select it and then click **Modify** to open the Modify User dialog box (you can also right-click the user's entry and select **Modify**). The parameters in the dialog box match the edited user type (i.e. password or public key).

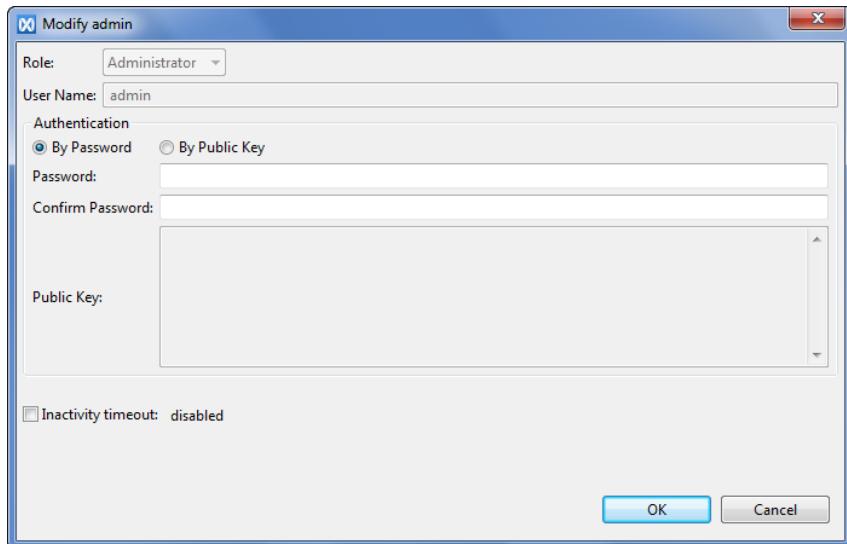


Figure 223 Modify User Data Dialog Box

4. Modify the user's characteristics. You can change the user's role, name, password or public key and inactivity timeout.
5. Click **OK** to confirm the changes and close the dialog box.

Removing a User

To remove a user:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Security** tab and select **Users Administration** from the left pane; the Users Administration screen appears, as shown in [Figure 74 on page 102](#).
3. In the users table, select the user's entry and click **Remove** (you can also right-click the user's entry and select **Remove**).
4. Click **OK** to confirm the deletion and close the dialog box.

Logging In as a Different User

To log in as a different user:

1. From the Dashboard, click the **Logout** button (see “[GUI Window](#)” on page 36); the Log in dialog box appears.
2. Type the other user’s name and password and click **Login**.

Managing User Accounts, Using the CLI

Use the following CLI commands for managing user accounts:

Command	Description
add-user-account	Adds a new user account.
remove-user-account	Removes a user account.
remove-user-account	Modifies the user account parameters.
modify-password	Used to modify one’s own password, or for entitled users (Configuration and Admin) to modify others’ passwords.
show-user-accounts	Displays the user accounts information.

Configuring the LDAP Users Authentication

The Lightweight Directory Access Protocol (LDAP) is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

XtremIO Storage Array supports LDAP users' authentication. Once configured for LDAP authentication, the XMS redirects users' authentication to the configured LDAP or Active Directory (AD) servers and allows access to authenticated users only. Users' XMS permissions are defined, based on a mapping between the users' LDAP/AD groups and XMS roles.

The XMS server LDAP Configuration feature allows using single or multiple servers for the external users' authentication for their login to the XMS server.

The LDAP operation is performed once when logging with external user credentials to an XMS server. The XMS server operates as an LDAP client and connects to an LDAP service running on an external server. The LDAP Search is performed, using the pre-configured LDAP Configuration profile and the external user login credentials.

LDAP profiles are used when authentication is performed against several Directory Services in one Active Directory Forest. Each profile is checked in order and once a positive answer is received the user is authenticated. If no positive answer is received, the user is denied access. It is recommended to define two servers URLs per profile for high-availability of the service. The two servers used should be of the same Directory Service and should act as backup for one another. The XMS connects to the first server URL on the list and only if there is no response (time-out), it connects to the second server URL.

If the authentication is successful, the external user logs in to the XMS server and accesses the full or limited XMS server functionality (according to the XMS Role that was assigned to the AD user's Group). The external user's credentials are saved in the XMS server cache and a new user profile is created in the XMS User Administration configuration. From that point, the external user authentication is performed internally by the XMS server without connecting to an external server. The XMS server will re-perform the LDAP Search only after the LDAP Configuration Cache time expires or at the next successful external user login if the external user credentials were removed from the XMS server User Administration manually.

XtremIO LDAP integration supports the following LDAP options:

- ◆ LDAP – clear text LDAP communication between XMS and LDAP server. LDAP uses the default port 389 or port 3268 for global catalog.
- ◆ LDAPS – secure LDAP communication, using Transport Layer Security (TLS) between the XMS and the LDAP server. LDAPS can be used either with a root certificate to validate the server authenticity or without it. LDAPS uses the default port 636 or 3269 for global catalog.
- ◆ Start TLS – secure LDAP communication that starts at a non-secure port and enhances the security mid-session. Start TLS uses port 389 or port 3268 for global catalog.

LDAP user authentication can be configured and managed via either GUI or CLI.

Setting the XMS Server LDAP Configuration

Before setting the XMS server LDAP configuration, note the following:

- ◆ An administrative access to the DS server is required to define or modify the required information on the DS server. As an option, the DS Groups distinguishedName, DS Users userPrincipalName and other required information can be obtained remotely, using a third party LDAP browsing software with the DS administrative (Bind DN) user access.
- ◆ LDAP configuration parameters and values should be set in accordance with the DS server (for example Microsoft Active Directory) users and groups configuration.

Configuring LDAP Settings via the GUI

Adding the LDAP Configurations

To add an LDAP configuration:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Security** tab and select **LDAP Configuration** from the left tab; the LDAP Configuration screen appears, as shown in [“LDAP Configuration Screen” on page 103](#).
3. Click **Add**; the Add New LDAP Configuration dialog box appears.

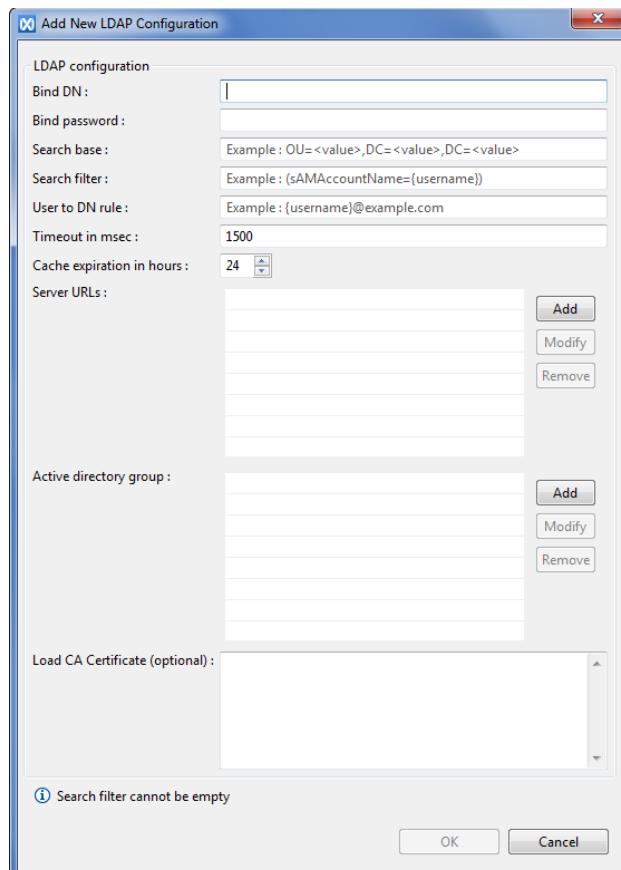


Figure 224 Add New LDAP Configuration Dialog Box

4. Set the following parameters to configure the LDAP authentication:

Parameter	Description	Mandatory
Bind DN	A full Distinguished Name of a user that has permissions for querying groups and perform searches on behalf of other users	Yes
Bind Password	A password for the Bind DN	Yes
Search Base	<p>Defines the starting point of the search in the DS directory tree. A search base is built from multiple objects, separated by commas, including:</p> <ul style="list-style-type: none"> • cn: common name • ou: organizational unit • o: organization • c: country • dc: domain 	No
Search Filter	<p>An LDAP expression that defines which user object attribute is checked against which part of the user input</p> <p>For example:</p> <ul style="list-style-type: none"> • <code>sAMAccountName={sam}</code> - looks for a user attribute called <code>sAMAccountName</code>, that matches the "user" name to the right of a backslash or to the left of an at ('@') sign of the user input during log in. • <code>sAMAccountName={username}</code> - looks for a user attribute called <code>sAMAccountName</code>, that matches the user name as entered by the user. • <code>UserPrincipalName={username}</code> - looks for a user attribute called <code>UserPrincipalName</code>, in the format of <code>user@domain</code>, that matches the user name as entered by the user. <p>The user's input is parsed according to the following fields:</p> <ul style="list-style-type: none"> • <code>{username}</code> - user name as entered by the user • <code>{user}</code> - user name after translation by "username_to_dn" pattern • <code>{domain}</code> - the field to the left of the backslash after "username_to_dn" translation • <code>{sam}</code> - "user" name to the right of a backslash or to the left of an at ('@') sign after "user_to_dn" translation • <code>{domain_dn}</code> - contents of the "domain" field, reconstructed into Distinguished Name syntax. 	Yes
User to DN Rule	<p>A rule that modifies the user's input before the search criteria for simplified use. The rule can append a prefix or a suffix to the user's input to save typing.</p> <p>Examples:</p> <ul style="list-style-type: none"> • <code>Ds1/{username}</code> - adds the <code>Ds1/</code> prefix to the user's input • <code>{username}@domain.com</code> - adds the <code>@domain.com</code> postfix to the user input 	No

Parameter	Description	Mandatory
Timeout	The time in seconds before switching to the secondary server or failing the request following the server's failure to reply	No
Cache Expire	The time in hours (1 to 24) before the cached user authentication expires and re-authentication is required	Yes
Server URLs	LDAP server addresses. Format can be either <code>ldap://<IP></code> or <code>ldap://<hostname></code> (except when using certificates, see note below). See “ Configuring the Server URLs ” on page 304.	Yes
Active Directory Groups	XMS roles assignment to DS groups (represented by their DN). See “ Configuring the Active Directory Rules ” on page 305.	Yes
CA Certificate	Used for server root certificate validation (for LDAPS). The certificate should be in PEM format.	No

Note: When using a certificate, the XMS validates the certificate correctness, including the server name. In this case, make sure that the server URLs are defined in name format and are matching the names in the certificate.

- Click **OK**; the new LDAP configuration profile is added to the configuration table.

Note: You can configure up to ten LDAP profiles.

Note: For an LDAP configuration profile example, see “[Configuring LDAP Settings via the CLI](#)” on page 307.

Editing the LDAP Configurations

To edit an LDAP configuration:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Security** tab and select **LDAP Configuration** from the left tab; the LDAP Configuration screen appears, as shown in [“LDAP Configuration Screen” on page 103](#).
3. Double-click the entry you want to edit or select the entry and click **Edit**; the Edit LDAP Configuration dialog box appears.

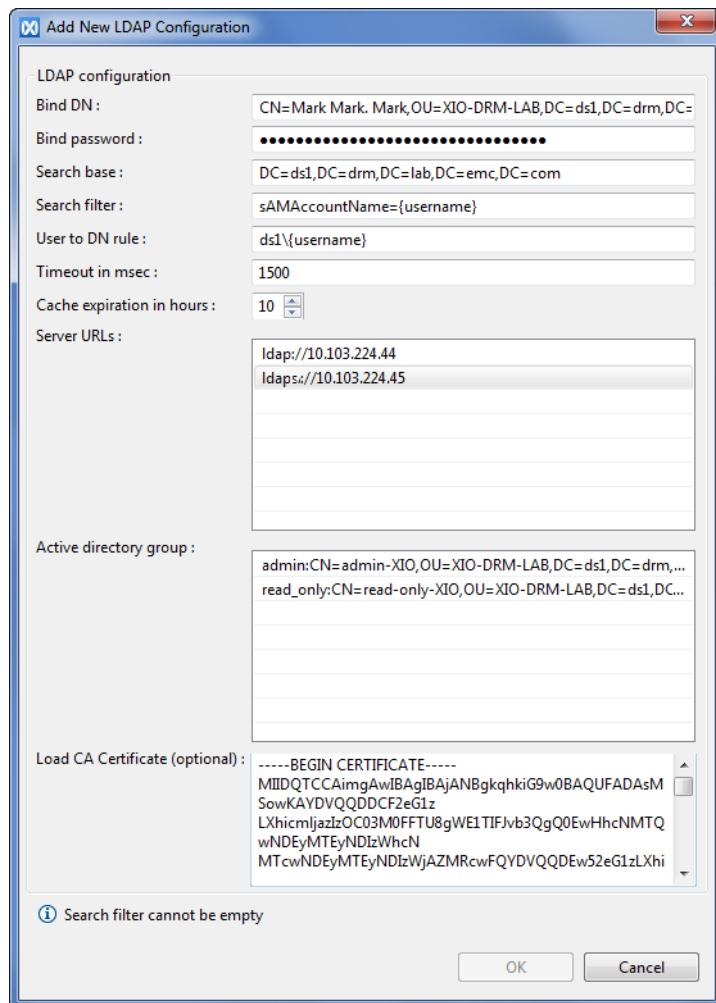


Figure 225 Edit LDAP Configuration Dialog Box

4. Edit the relevant configuration parameters (to edit Active Directory Groups, refer to [“Configuring the Active Directory Rules” on page 305](#)).
5. Click **OK** to save the changes.

Removing the LDAP Configurations

To remove an LDAP configuration:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Security** tab and select **LDAP Configuration** from the left tab; the LDAP Configuration screen appears, as shown in [“LDAP Configuration Screen” on page 103](#).
3. Double-click the entry you want to remove and click **Remove**.
4. Click **Yes** to confirm; the entry is removed from the LDAP configuration table.

Configuring the Server URLs

To add a server URL:

1. In the Add New LDAP Configuration dialog box, click the **Add** button to the right of the Server URLs section; the Add Server URL dialog box appears.

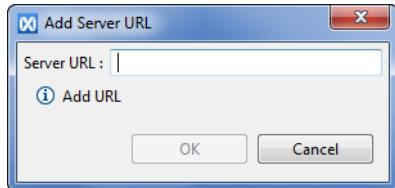


Figure 226 Add Server URL Dialog Box

2. Type the URL (IP address or full name), including the protocol LDAP, LDAPS or LDAPTLS and the optional port (e.g. LDAP://10.2.2.3). Use the following formats according to the desired protocol:

Protocol	Format
LDAP	ldap://10.2.2.3
LDAPS	ldaps://10.2.2.3
Start TLS	ldaptls://10.2.2.3

Note: If no port is specified, the default ports 389 and 636 are used for LDAP and LDAPS, respectively. For global catalog, include the GC port (usually port 3268 for LDAP and 3269 LDAPS).

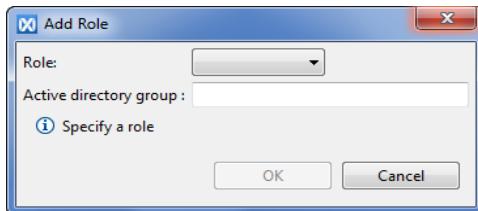
3. Click **OK**; the new URL is added to the Server URLs list.

To remove a server URL:

1. In the LDAP Configuration screen, double-click the relevant entry or select it and click **Edit** to open the Edit LDAP Configuration dialog box.
2. In the Server URLs list, select the URL you want to remove and click the **Remove** button to the right of the Server URLs section; the selected URL is removed from the Server URLs list.
3. Click **OK** to save the changes.

Configuring the Active Directory Rules**To add an Active Directory mapping rule:**

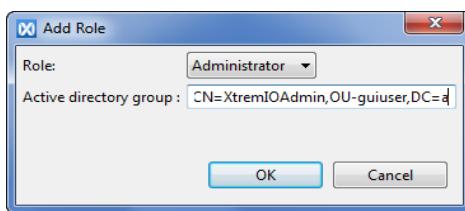
1. In the Add New LDAP Configuration dialog box, click the **Add** button to the right of the Active Directory Group section; the Add Role dialog box appears.

**Figure 227** Add Role Dialog Box

2. From the **Role** drop-down menu, select the XMS role (Administrator, Configuration, or read-only).
3. In the **Active directory group** field, type the Distinguished Name (DN) of the AD group you want to map to the selected role.
4. Click **OK**; the new mapping rule is added to the Active Directory Group list.

To edit an Active Directory mapping rule:

1. In the LDAP Configuration screen, double-click the entry you want to edit or select it and click **Edit** to open the Edit LDAP Configuration dialog box.
2. In the Active Directory Group pane, select the rule you want to edit and click **Edit**; the Add Role dialog box appears.

**Figure 228** Add Role Dialog Box - Edit

3. In the Add Role dialog box, edit the mapping rule properties and click **OK**.
4. In the Edit LDAP Configuration dialog box, click **OK** to save the changes.

To remove an Active Directory mapping rule:

1. In the LDAP Configuration screen, double-click the entry you want to edit or select the entry and click **Edit** to open the Edit LDAP Configuration dialog box.
2. In the Active Directory Group pane, select the rule you want to remove and click **Remove**.
3. Click **OK**; the selected rule is removed from the mapping rules list.
4. In the Edit LDAP Configuration dialog box, click **OK** to save the changes.

Using the LDAP Authentication**To use LDAP Authentication:**

1. Define an LDAP server and system parameters (LDAP protocol and a port if it is different than the default).
2. Define a user with a search permission on the defined LDAP server. Enter the user name and password in the Bind DN and Bind Password fields, respectively.

Note: The XMS uses the defined user (Bind DN) when searching for authenticated users.

3. Define the search starting point (Search Base) to make the search more efficient. Searching sub-trees is supported.
4. Define the search filter, i.e. which user AD attribute to search for and what part of the user's input to use.

For example:

for using the full user input and searching for UserPrincipalName, define the following search filter: `(UserPrincipalName={username})`

5. Identify the AD groups associated with XMS user roles.
6. Define a mapping between the AD groups and XMS user roles.

You can simplify the login process for user by automatically adding a prefix or suffix to the user entry and using the User to DN rule, thus omitting the need to enter the full domain name. For example, adding `@example.com` to the username, renders entering `username@example.com` unnecessary.

To use the global catalog:

1. Add the default catalog port to the server URL (e.g. `LDAP://1.1.1.1:3268`).
2. Enter the Bind DN and Bind Password.
3. Define the search filter. It is recommended to use a UserPrincipalName that is unique in the catalog.
4. Map the AD groups to the XMS roles.

Note: For using global catalog, do not enter a Search Base and do not use a "User to DN" rule.

Configuring LDAP Settings via the CLI

Use the following CLI commands for managing the LDAP server configuration:

Command	Description
add-ldap-config	Adds a new LDAP configuration profile to the LDAP configuration table.
modify-ldap-config	Modifies an LDAP configuration profile.
remove-ldap-config	Removes an LDAP configuration profile from the LDAP configuration table.
show-ldap-configs	Displays the LDAP users' authentication configuration data.

The following examples display the output of the `show-ldap-configs` command for different environments:

- ◆ Output for Linux environment:

```
xmcli (admin)> show-ldap-configs
Index: 1
Bind DN: CN=Manager,DC=fbu,DC=umsg,DC=lab,DC=emc,DC=com
Search Base: OU=Users,DC=fbu,DC=umsg,DC=lab,DC=emc,DC=com
Search Filter: CN={username}
LDAP Servers: ['ldap://10.245.XX.XX']
User to DN Rule:
CN={username},OU=Users,DC=fbu,DC=umsg,DC=lab,DC=emc,DC=com
Role Mapping:
['admin:CN=XIOGUIadmins,OU=Users,DC=fbu,DC=umsg,DC=lab,DC=emc,DC=com']
Timeout: 1500
Credentials-Expiration (hours): 24
```

- ◆ Output for Windows environment:

```
xmcli (admin)> show-ldap-configs
Index: 1
Bind DN:
CN=Administrator,CN=Users,DC=fbu,DC=umsg,DC=lab,DC=emc,DC=com
Search Base: ou=XIO,dc=fbu,dc=umsg,dc=lab,dc=emc,dc=com
Search Filter: sAMAccountname={username}
LDAP Servers: ['ldap://10.245.XX.XX']
User to DN Rule:
Role Mapping:
['admin:CN=XIOadmins,OU=XIO,DC=fbu,DC=umsg,DC=lab,DC=emc,DC=com']
Timeout: 1500
Credentials-Expiration (hours): 24
```

The following example displays the usage of the add_ldap_config command:

```
xmcli (admin)> add-ldap-config binddn="CN=Mark Mark.
Mark, OU=XIO-DRM-LAB, DC=ds1, DC=drm, DC=lab, DC=emc, DC=com"
bindpw="welcome1" search-base="DC=ds1, DC=drm, DC=lab, DC=emc, DC=com"
search-filter="sAMAccountName={sam}"
server-urls=["ldap://10.103.224.44",
"ldap://10.103.224.45"]
roles=[ "admin:CN=admin-XIO,OU=XIO-DRM-LAB,DC=ds1,DC=drm,DC=lab,DC=emc
,DC=com"]
xmcli (admin)>
```

Configuring Email Settings

Managing Email Settings, Using the GUI

Enabling Email Notifications

To enable email notifications:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Notification** tab, and select **Email Configuration** from the left pane; the Email Configuration screen appears, as shown in [Figure 76 on page 105](#).
3. Select the **Send email notifications** option.
4. Set the frequency of sending email notifications (in hours), using the up and down arrows.
5. Click **Apply** to save the changes.

Adding Email Recipients

To add a new email recipient:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Notification** tab, and select **Email Configuration** from the left pane; the Email Configuration screen appears, as shown in [Figure 76 on page 105](#).
3. Click **Add**; the Add Recipient dialog box appears.

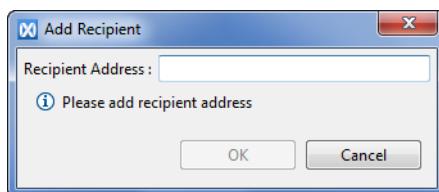


Figure 229 Add Email Recipient Dialog Box

4. Type the recipient's email address.

5. Click **OK** to confirm and close the dialog box; the new recipient is added to the recipients list.

Note: Click **Undo** to revoke the changes you made.

6. Click **Apply** to save the changes.

Removing Email Recipients

To remove an email recipient:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Notification** tab, and select **Email Configuration** from the left pane; the Email Configuration screen appears, as shown in [Figure 76 on page 105](#).
3. Select the recipient you want to remove.
4. Click **Remove**; the recipient is deleted from the recipients list.

Note: Click **Undo** to revoke the recipient's removal.

5. Click **Apply** to save the changes.

Configuring the Email Sender Properties

To configure the email sender properties:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Notification** tab, and select **Email Configuration** from the left pane; the Email Configuration screen appears, as shown in [Figure 76 on page 105](#).
3. Type the sender email address in the Sender text box.
4. Type the company's name in the Company Name text box.
5. Type the required contact information in the Contact Details text box.

Note: Click **Undo** to revoke configuration.

6. Click **Apply** to save the changes.

Configuring the Email Sending Mechanism

To configure the email sending mechanism:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Notification** tab, and select **Email Configuration** from the left pane; the Email Configuration screen appears, as shown in [Figure 76 on page 105](#).
3. Click one of the Transport options (HTTP or SMTP) to select the mail sending topology:
 - If you select HTTP, fill in the HTTP Proxy Server fields (Address, Port, Username, and Password).
 - If you select SMTP, fill in the SMTP Information fields (Mail Relay Address, Username, and Password).

Note: Click **Undo** to revoke configuration.

4. Click **Apply** to save the changes.

Managing Email Settings, Using the CLI

Use the following CLI commands for managing Email settings:

Command	Description
modify-email-notifier	Modifies the email notification settings.
show-email-notifier	Displays the Email notification settings.

Configuring the SNMP

Note: To make sure the correct host information is sent via the SNMP traps, it is required to use a valid DNS configuration or use the CLI command “[modify-server-name](#)” on [page 393](#).

Configuring SNMP, Using the GUI

Enabling the SNMP Notifications

To enable SNMP notifications:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Notification** tab, and select **SNMP Configuration** from the left pane; the SNMP Configuration screen appears, as shown in [Figure 77 on page 106](#).
3. Select the **Send SNMP notifications** option.
4. Click **Apply** to save the changes.

Adding an SNMP Notification Recipient

To add an SNMP notification recipient:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Notification** tab and select **SNMP Configuration** from the left pane; the SNMP Configuration screen appears, as shown in [Figure 77 on page 106](#).
3. Click **Add**; the Add Recipient dialog box appears.

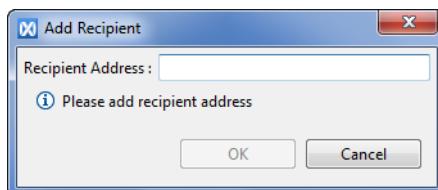


Figure 230 Add SNMP Notification Recipient Dialog Box

4. Type the recipient’s address.
5. Click **OK** to confirm and close the dialog box; the new recipient is added to the table.

Note: Click **Undo** to revoke the changes.

6. Click **Apply** to save the changes.

Removing an SNMP Notification Recipient

To remove an SNMP notification recipient:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Notification** tab and select **SNMP Configuration** from the left pane; the SNMP Configuration screen appears, as shown in [Figure 77 on page 106](#).
3. In the SNMP Recipients table, click to select a recipient entry.
4. Click **Remove**.
5. Click **Yes** to confirm; the recipient is removed from the table.
6. Click **Undo** to revoke changes.
7. Click **Apply** to save the changes.

Configuring the SNMP Properties

To configure the SNMP properties:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Notification** tab and select **SNMP Configuration** from the left pane; the SNMP Configuration screen appears, as shown in [Figure 77 on page 106](#).
3. Select the SNMP Version (V1, V2C or V3).
4. If you selected V3 as the SNMP version, configure the following properties:
 - User name
 - Authentication protocol (No Authentication, MD5, SHA1 or Unexpected Value)
 - Authentication key
 - Privacy protocol (No Privacy, DES, AES128 or Unexpected Value)
 - Privacy key
5. Set the Community field (the default entry is public [read-only]).
6. Set the Trap Port field (the default entry is 162).

Note: Click **Undo** to revoke changes.

7. Click **Apply** to save the changes.

Configuring SNMP, Using the CLI

Use the following CLI commands for managing SNMP configuration:

Command	Description
modify-snmp-notifier	Modifies the SNMP notification settings.
show-snmp-notifier	Shows the SNMP notification settings.

XtremIO MIB

XtremIO MIB is a trap definition file that can be installed in an external trap receiver/SNMP trap and be used to parse XtremIO SNMP traps.

To use the XtremIO MIB:

1. Download the XtremIO MIB file from the EMC Support page for XtremIO.
2. Import the XtremIO MIB to your SNMP server, according to the server procedures (outside the scope of this guide).
3. Configure SNMP traps in XMS (refer to “[Configuring the SNMP](#)” on page 311).
4. Start using the MIB.

Note: The Object IDs that are sent in the trap text are internal to XtremIO and are not mapped by this MIB.

Configuring the Remote Syslog Notification

The XtremIO Storage Array enables you to send events to a remote syslog server. You can configure up to 6 syslog servers and use the event handlers' configuration to select the events that will be sent via the syslog interface.

Remote syslog can be configured via the GUI or CLI.

Configuring Remote Syslog via the GUI

Enabling Syslog Notification

To enable Syslog notification:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Notification** tab and select **Syslog Configuration** from the left pane; the Syslog Configuration screen appears, as shown in [“CLI Terminal Tab” on page 110](#).
3. Select the **Send Syslog Notification** option.
4. Click **Apply** to save the changes.

Adding a Syslog Server

To add a Syslog server:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Notification** tab and select **Syslog Configuration** from the left pane; the Syslog Configuration screen appears, as shown in [“CLI Terminal Tab” on page 110](#).
3. Click **Add**; the **Add Syslog Target** dialog box appears.

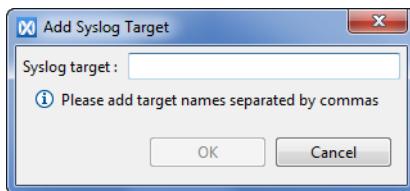


Figure 231 Add Syslog Target Dialog Box

4. Type the server IP address or name. You can include the optional port (e.g. 10.1.1.1:1022).
5. Click **OK**; the server is added to the Target list.
6. Click **Apply** to save the changes.

Removing a Syslog Server

To remove a Syslog server:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **Notification** tab and select **Syslog Configuration** from the left pane; the Syslog Configuration screen appears, as shown in [“CLI Terminal Tab” on page 110](#).
3. Select the server you want to remove by clicking it.
4. Click **Remove**; the server is removed from the Target list.
5. Click **Apply** to save the changes.

Selecting Events for Syslog Server

To select the event that will be sent to the Syslog server, refer to [“Managing Event Handlers” on page 273](#).

Configuring Syslog Settings via the CLI

Use the following CLI commands for managing Syslog notification configuration:

Command	Description
show-syslog-notifier	Displays the Syslog server notification status and data.
modify-syslog-notifier	Enables Syslog configuration.

Configuring the Default Inactivity timeout

The XtremIO Storage array enables you to set the inactivity timeout duration, after which users are requested to log in to the cluster again.

The default inactivity timeout is ten minutes and it can be changes in full minute granularity. The possible inactivity timeout range is 0 (no timeout) to 12 hours.

User accounts that are created after the inactivity timeout configuration will have the new default value.

The user is notified 60 seconds before the timeout expiration. When the timeout expires, the user is prompted for the username and password. After logging in, the screen that appeared before timeout expiration re-appears.

All logins and re-logins actions are logged in the audit log.

The XtremIO Storage Array also enables you to set an inactivity timeout per user to allow monitoring clients to be connected with no interruptions. For details, see “[Configuring the User Accounts](#)” on page 294.

Configuring the Inactivity Timeout via the GUI

To configure the inactivity timeout via the GUI:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **XMS** tab and select **XMS Configuration** from the left pane; the XMS Configuration screen appears, as shown in [Figure 80 on page 109](#).
3. Type in the new default inactivity timeout value and click **Apply**.

Configuring Inactivity Timeout via the CLI

Use the following CLI commands for configuring the inactivity timeout:

Command	Description
show-xms	Displays the XtremIO management System information
modify-xms-parameters	Modifies the XMS's user inactivity timeout.

Customizing the Login Screen Banner

You can customize the login screen banner by adding text. XtremIO supports customizing the login banner in SSH, HTML and JAVA:

- ◆ SSH - The customized text is displayed when an SSH session is opened.
- ◆ HTML - The customized text is displayed in the HTML landing page, below the download button.
- ◆ Java - The customized text is displayed in the Java Login spalsh screen.

Note: The added banner text can be up to 4KB in size.

The login screen banner customization can be done via both GUI and CLI.

Customizing the Login Screen Banner via the GUI

To customize the login banner via the GUI:

1. From the menu bar, click the **Administration** icon to display the Administration workspace, as shown in [Figure 73 on page 101](#).
2. Click the **XMS** tab and select **XMS Customization** from the left pane; the XMS Customization screen appears, as shown in [Figure 80 on page 109](#).
3. Type in the customized text and click **Apply**.

Customizing the Login Screen Banner via the CLI

Use the following CLI command for customizing the XMS banner:

Command	Description
modify-login-banner	Enables you to customize the XMS banner text.

CHAPTER 8

Cluster Operations

This chapter includes the following topics:

◆ Powering Up the Cluster	320
◆ Shutting Down the Cluster - Planned Shutdown	329
◆ Shutting Down the Cluster - Emergency Shutdown	334
◆ Changing the IP Configurations	336
◆ Setting the Cluster Time and Date	343
◆ Managing the Virtual XMS	344

Powering Up the Cluster

Powering Up the Cluster after an Emergency Shutdown

Note: This procedure should be carried out before powering up the cluster only if the performed emergency shutdown involved disconnecting the DAE power cables of X-Brick No. 1, as described in “[Shutting Down the Cluster - Emergency Shutdown](#)” on page 334.

Before powering up the cluster:

1. Check if the two DAE power cables of X-Brick No. 1 (usually the lowest X-Brick in the rack) are connected to their ports, as shown in [Figure 232](#).



Figure 232 Power Connection Ports (Shown with Arrows) on the Rear Side of DAE

- If the DAE power cables are connected to their ports, skip to [step 2](#).
 - If the DAE power cables are disconnected from their ports, proceed as follows:
 - a. Make sure that the cluster’s power is turned off, by verifying that the rack’s PDU (to which the cluster is connected) is turned off.
Note: Make sure that no other equipment is connected to the PDU.
 - b. Connect the two DAE power cables of X-Brick No. 1 (usually the lowest X-Brick in the rack) to their ports, as shown in [Figure 232](#).
 - c. Turn on the rack’s PDU (to which the cluster is connected).
2. Proceed to [Powering Up Procedure](#).

Powering Up Procedure

Note: This procedure requires running XMCLI commands with Administrator privileges.

- ◆ If the cluster has been shut down due to a power loss, it automatically restarts when the power is restored.
- ◆ To start the cluster for the first time, carry out the complete powering up procedure, as described below.
- ◆ To start the cluster following an emergency shut down, carry out the complete powering up procedure, as described below. Before powering up the Battery Backup Units, power up the PDU that was powered off during the emergency shut down.
- ◆ To restart the cluster following a logical shutdown (such as a `stop-cluster` command), you can perform only the procedure for “[Starting the Cluster](#)” on [page 327](#).

Note: If the cluster was shut down, using an emergency shutdown procedure, turn on the rack's PDU (to which the cluster is connected).

To power up the cluster, carry out the following procedures:

1. See the Note above.
2. “[Powering Up the Battery Backup Units](#)” on page 322
3. “[Powering Up the Storage Controllers](#)” on page 325
4. “[Powering Up the XMS](#)” on page 326
5. “[Starting the Cluster](#)” on page 327

Locating the Cluster

Before starting or stopping the cluster, it is important to verify that you are performing the procedure on the correct cluster.

To locate the correct cluster:

1. Physically locate the appropriate cluster and its components.
2. Run the following XMCLI command to obtain the name and index of the appropriate cluster:

```
show-clusters
```

```
xmcli (admin)> show-clusters
Cluster-Name      Index   State     Conn-State    ...
Xbrick1           1        active    connected    ...
Xbrick2           2        active    connected    ...
```

Note: When executing a procedure for starting or stopping the cluster, specify the cluster name or index whenever it is required to run a cluster-related command.

Note: It is recommended to use the cluster name (and not the cluster ID) as the cluster identifier in cluster-related XMCLI commands.

Powering Up the Battery Backup Units

Note: If the cluster was shut down in an emergency procedure, power up the PDU that was powered off during the emergency shut down before powering up the Battery Backup Units.

Note: if the Battery Backup Units were shut down due to a power outage, they power up automatically when they are charged to 70% of their full capacity.

Battery Backup Units of an XtremIO cluster can be of one of the following types:

- ◆ If the front panel of the Battery Backup Unit is as shown in [Figure 233](#), the Battery Backup Unit is **5P 1550i R**.

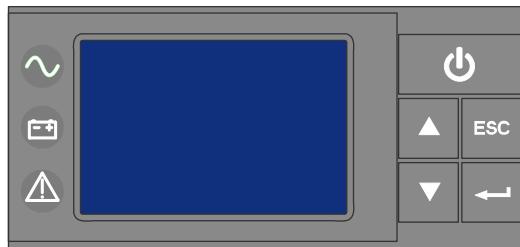


Figure 233 Front Panel of the 5P 1550i Battery Backup Unit

- ◆ If the front panel of the Battery Backup Unit is as shown in [Figure 234](#), the Battery Backup Unit is **1550 Evolution**.

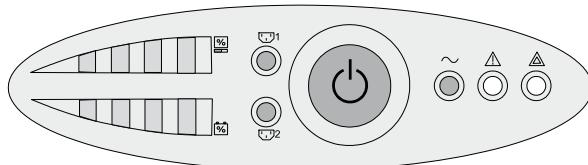


Figure 234 Front Panel of the 1550 Evolution Battery Backup Unit

Powering Up the 5P 1550i Battery Backup Units

To power up the 5P 1550i R Battery Backup Units:

1. Verify that the graphical LCD display of the Battery Backup Unit is lit (indicating that the Battery Backup Unit is receiving mains power).
2. Verify that the Power On indicator (on the front panel of the Battery Backup Unit, as shown in [Figure 235](#)) is not lit.

Note: If the Power On indicator is lit, the Battery Backup Unit is already powered up.



Figure 235 Power Button and Power On Indicator on the Front Panel of the 5P 1550i Battery Backup Unit

3. Press and hold the Power button to turn on the Battery Backup Unit, as shown in [Figure 235](#).
4. Wait for the Battery Backup Unit to complete its startup self test.
5. Verify that:
 - The Power On indicator is lit, as shown in [Figure 236](#).
 - The graphical LCD display shows the Normal mode screen, as shown in [Figure 236](#).



Figure 236 5P 1550i Battery Backup Unit Powered On

6. Repeat the above steps to power up all Battery Backup Units in the cluster.

Note: In order to start the cluster, at least one of the Battery Backup Units (in a single X-Brick cluster), or one Battery Backup Unit per X-Brick pair (in a multiple X-Brick cluster) must be charged to not less than 70% of its full capacity (as indicated on the graphical LCD display).

Powering Up the 1550 Evolution Battery Backup Units

To power up the 1550 Evolution Battery Backup Units:

1. Verify that the Charge indicator LEDs (on the front panel of the Battery Backup Unit, as shown in [Figure 237](#)) are lit (indicating that the Battery Backup Unit is receiving mains power).

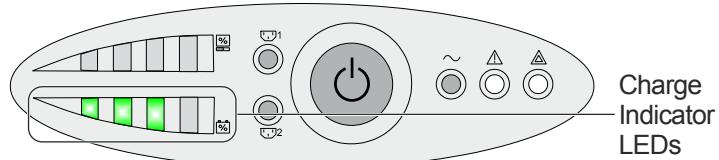


Figure 237 Charge Indicator LEDs on the Front Panel of the 1550 Evolution Battery Backup Unit

2. Verify that the Power button (on the front panel of the Battery Backup Unit, as shown in [Figure 238](#)) is not lit.

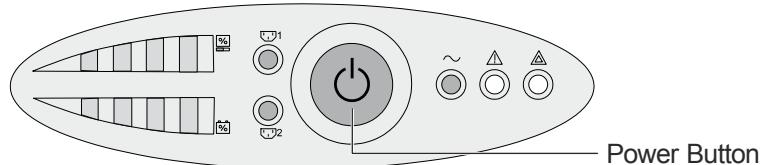


Figure 238 Power Button on the Front Panel of the 1550 Evolution Battery Backup Unit

3. Press and hold the Power button to turn on the Battery Backup Unit.
4. Wait for the Battery Backup Unit to complete its startup self test, until its LED indicators become steady.
5. Verify that the Load Protected indicator of the Battery Backup Unit is lit, as shown in [Figure 239](#).

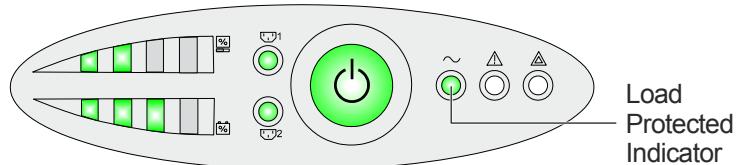


Figure 239 Load Protected Indicator on the Front Panel pf the 1550 Evolution Battery Backup Unit

6. Repeat the above steps to power up all Battery Backup Units in the cluster.

Note: To start the cluster, at least one of the Battery Backup Units (in a single X-Brick cluster), or one Battery Backup Unit per X-Brick pair (in a multiple X-Brick cluster) must be charged to not less than 70% of its full capacity (i.e. three lit charge indicator LEDs, as shown in [Figure 237](#)).

Powering Up the Storage Controllers

Note: if the Storage Controllers were shut down due to a power outage, they power up automatically when the Battery Backup Units are powered up.

To power up the Storage Controllers:

1. Locate the relevant cluster and obtain its name and index. Refer to “[Locating the Cluster](#)” on page 321 for details.
2. Run the following XMCLI command to view all of the Storage Controllers in the cluster.

```
show-storage-controllers cluster-id=<cluster-name>
```

```
xmcli (admin)> show-storage-controllers cluster-id="Xbrick1"
Storage-Controller-Name Index Mgr-Addr IB-Addr-1 IB-Addr-2 IPMI-Addr Brick-Name Index Cluster-Name Index State Enabled-State Unorderly-Stop-Reason Conn-State IPMI-State
X1-SC1 1 10.76.218.197 169.254.0.1 169.254.0.2 10.76.214.197 X1 1 Xbrick1 1 healthy enabled none connected connected
X1-SC2 2 10.76.218.198 169.254.0.17 169.254.0.18 10.76.214.198 X1 1 Xbrick1 1 healthy enabled none connected connected
```

Note: You can run the XMCLI command only if the cluster has already been initialized.

3. For each Storage Controller whose Conn-State is not shown as connected, power on the Storage Controllers manually, by pressing the Power button on the top-right side of the front panel, as shown in [Figure 240](#).



Figure 240 Power Button on the Front Panel of the Storage Controller

4. Run the `show-storage-controllers` XMCLI command again to confirm that all the Storage Controllers are connected.

Note: Verify that you specify the correct cluster name.

Powering Up the XMS

To power up the XMS, proceed as follows:

- ◆ If the cluster uses a virtual XMS machine, follow the instructions for “[Powering Up the Virtual XMS](#)” on page 326.
- ◆ If the cluster uses a physical XMS machine, follow the instructions for “[Powering Up the Physical XMS](#)” on page 326.

Powering Up the Virtual XMS

To power up the virtual XMS machine:

1. In the vSphere client application, select the **Hosts & Clusters** view.
2. From the **Inventory** pane, locate the virtual XMS.
3. Right-click the XMS and, from the drop-down menu, select **Power > Power On**.
4. Verify that the XMS has started.

Powering Up the Physical XMS

To power up the physical XMS machine:

1. Verify that the Power button (on the top-right side of the physical XMS, as shown in [Figure 241](#)) is not lit.

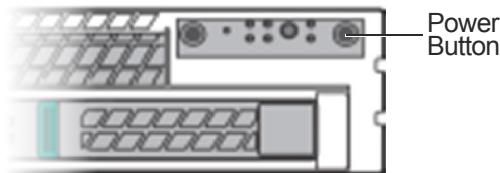


Figure 241 Power Button on the Front Panel of the Physical XMS

Note: If the Power button is lit, the XMS is already powered up.

2. Press the Power button to turn on the XMS and wait for it to power up; the button's green light illuminates.
3. Verify that the XMS has completed powering up by issuing a PING command to the XMS's defined IP Address and receiving a successful reply.

Starting the Cluster

To start the cluster:

1. Locate the relevant cluster and obtain its name and index. Refer to “[Locating the Cluster](#)” on page 321 for details.
2. Verify that all of the following components in the rack are powered up:
 - Physical XMS (optional unit)
 - PDU
 - Battery Backup Units (powered up and charged)
 - Storage Controllers
 - DAEs
 - InfiniBand Switches (only in multiple X-Brick clusters)

Note: If the last service stop has been due to an unexpected event, such as a power disruption, the service automatically restarts.

3. Run the following XMCLI command and wait for its successful completion.

```
start-cluster cluster-id=<cluster name>
```

NOTICE

Verify that you specify the correct cluster name.

```
xmcli (admin)> start-cluster cluster-id="Xbrick1"
The process may take a few minutes. Please do not interrupt.
Started Cluster
xmcli (admin)>
```

Note: This process may take several minutes.

4. Run the `show-clusters` XMCLI command and view the results to verify that:

- State is active.
- Conn-State is connected.

```
xmcli (admin)> show-clusters
Cluster-Name      Index     State      Conn-State    ...
Xbrick1           1          active     connected    ...
Xbrick2           2          active     connected    ...
```

Note: If the cluster is not active and connected, contact EMC Global Tech Support.

5. Run the following XMCLI command to check whether SYR notifications are configured on the cluster:

```
show-syr-notifier
```

6. If SYR notifications are disabled, run the following XMCLI command to enable them:

```
modify-syr-notifier enable
```

7. Run the following XMCLI command to check whether Email Notifications are configured on the cluster:

```
show-email-notifier
```

8. If Email notifications are disabled, run the following XMCLI command to enable them:

```
modify-email-notifier enable
```

Note: You can also enable other notifiers (e.g. SNMP, SYSLOG, etc.).

Shutting Down the Cluster - Planned Shutdown

Planned Cluster Shutdown Overview

To Shut down the cluster, carry out the following procedures:

1. [“Pre-Shutdown Procedure” on page 329](#)
2. [“Shutting Down the Service” on page 331](#)
3. [“Shutting Down the Hardware” on page 332](#)

Pre-Shutdown Procedure

Before starting the shutdown procedure, it is important to verify that you are shutting down the correct cluster. It is also important to verify that no I/O operations are in progress.

To perform the pre-shutdown procedure:

1. Locate the relevant cluster and obtain its name and index. Refer to [“Locating the Cluster” on page 321](#) for details.
2. Run the `show-clusters` XMCLI command. Review the output to verify the following:
 - The `State` parameter is active.
 - The `Conn-State` parameter is connected.

```
xmcli (admin)> show-clusters
Cluster-Name      Index   State     Conn-State    ...
Xbrick167          1       active    connected    ...
Xbrick185          2       active    connected    ...
```

Note: If the cluster is not active and connected, contact EMC Global Tech Support.

3. Verify that no I/O requests are sent from the host, as follows:

- Verify that user applications are stopped and that any mount points are dismounted.
- Run the following XMCLI command:

```
show-clusters-performance
```

```
xmcli (admin)> show-clusters-performance
Cluster-Name Index Write-BW(MB/s) Write-IOPS Read-BW(MB/s) Read-IOPS BW(MB/s) IOPS ...
Xbrick1 1 0.000 0 0.000 0 0.000 0 ...
```

Verify that all output counters for the relevant cluster display zero, indicating no I/O requests from the host.

- Run the following XMCLI command:

```
show-targets-performance cluster-id=<cluster name>
```

```
xmcli (admin)> show-targets-performance cluster-id="Xbrick1"
Name Index Write-BW(MB/s) Write-IOPS Read-BW(MB/s) Read-IOPS BW(MB/s) IOPS Total-Write-IOS Total-Read-IOS
X1-SC1-fc1 1 0.000 0 0.000 0 0.000 0 0 0
X1-SC1-fc2 2 0.000 0 0.000 0 0.000 0 0 0
X1-SC1-iscsi1 5 0.000 0 0.000 0 0.000 0 0 0
X1-SC1-iscsi2 6 0.000 0 0.000 0 0.000 0 0 0
X1-SC2-fc1 11 0.000 0 0.000 0 0.000 0 0 0
X1-SC2-fc2 12 0.000 0 0.000 0 0.000 0 0 0
X1-SC2-iscsi1 15 0.000 0 0.000 0 0.000 0 0 0
X1-SC2-iscsi2 16 0.000 0 0.000 0 0.000 0 0 0
```

Verify that all output counters display zero, indicating no I/O requests from the host.

4. Disable Email notifications to prevent shutdown-induced notifications from being sent to the Email:

- Run the following XMCLI command to check whether Email Notifications are enabled on the cluster:

```
show-email-notifier
```

- If Email notifications are enabled, run the following XMCLI command to disable them:

```
modify-email-notifier disable
```

5. Disable SYR notification to prevent shutdown-induced notifications from being sent to SYR:

- Run the following XMCLI command to check whether SYR notifications are configured on the cluster:

```
show-syr-notifier
```

- If SYR notifications are enabled, run the following XMCLI command to disable them:

```
modify-syr-notifier disable
```

Note: You can also disable other notifiers (e.g. SNMP, SYSLOG, etc.).

Shutting Down the Service

This procedure should be carried out to shut down the service in regular circumstances.

Note: If you need to perform an emergency shutdown, refer to “[Shutting Down the Cluster - Emergency Shutdown](#)” on page 334.

Note: If the XMS is not accessible, shutting down the service as described in the following procedure is not possible. An emergency shutdown procedure should be performed instead. Refer to “[Shutting Down the Cluster - Emergency Shutdown](#)” on page 334.

To shut down the service:

1. Perform the “[Pre-Shutdown Procedure](#)” on page 329.
 - If the cluster state is `stopped`, the service is already down and no further action is required.
 - If the state is `active`, proceed to the next step.
 - If the state is other than `stopped` or `active`, contact EMC Global Tech Support, due to a risk of data loss.
2. Run the following XMCLI command to initiate the service shutdown.

```
stop-cluster cluster-id=<cluster name>
```

NOTICE

Verify that you specify the correct cluster name.

The following message appears:

```
xmcli (admin)>stop cluster cluster-id="Xbrick1"
Warning: You are about to stop the cluster service. All
connected initiators will be denied access to cluster data.
Are you sure you want to stop <cluster name>? (Yes/No) :
```

3. Enter `Yes` and wait until the cluster completes carrying out the command and displays the following message.

```
Stopped Cluster Xbrick1. Cluster state: stopped
```

Note: This process may take several minutes.

- Run the `show-clusters` XMCLI command and verify that the State of the relevant cluster is stopped.

```
xmcli (admin)> show-clusters
Cluster-Name Index State Conn-State ... Total-Writes Total-Reads Stop-Reason
xbrick1 1 stopped connected ... 11.472T 17.209T user_deactivated
```

Note: If performing the above steps does not stop the cluster (if the State is not stopped), contact EMC Global Tech Support.

Shutting Down the Hardware

To shut down the hardware:

- Verify that the service is shut down properly, as per the instructions in “[Shutting Down the Service](#)” on page 331.

NOTICE

If the service is not shut down properly, data loss may occur upon shutting down the hardware.

- Run the following XMCLI command to shut down the cluster’s Storage Controllers. Wait for the command to complete successfully.

```
power-off cluster-id=<cluster name>
```

NOTICE

Verify that you are specifying the correct cluster name.

```
xmcli (admin)> power-off cluster-id="Xbrick1"
```

- Turn off the cluster power supply by turning off the rack’s PDU (to which the cluster is connected).

Note: Make sure that no other equipment is connected to the PDU.

4. Power off the Battery Backup Unit by pressing its power button.

5. Power off the XMS by running the following XMCLI command:

```
shutdown-xms shutdown-type=machine
```

If the cluster uses a physical XMS, instead of using the above XMCLI command, you can turn it off by pressing the Power button (on the top-right side of the physical XMS), as shown in [Figure 242](#).

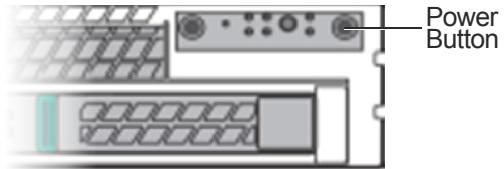


Figure 242 Power Button on the Front Panel of the Physical XMS

Note: If you wish to start the cluster, refer to [“Starting the Cluster” on page 327](#) for details.

Shutting Down the Cluster - Emergency Shutdown

This procedure should only be carried out to power off the cluster in an emergency situation, where it is not possible to power off the cluster via the XMS.

Note: If possible, it is recommended to power off the cluster via the XMS, as described in “[Shutting Down the Cluster - Planned Shutdown](#)” on page 329.

To physically power off the cluster in case of an emergency:

1. Press the power button of at least two Storage Controllers simultaneously for five seconds, to stop the cluster service and power off the Storage Controllers.

Note: If the cluster is connected to ESRS, a dial-home is sent to EMC, indicating that the cluster has performed an emergency shutdown. A member of the EMC Global Tech Support will contact you for follow-up.

2. Check the status of the orange LED indicators of all DAEs and SSDs.
 - If the orange LED indicators of all DAEs and SSDs start to blink, perform the following steps:
 - a. Wait for the orange LED indicators of all DAEs and SSDs to stop blinking (approximately five minutes). This time period allows the cluster to harden the volatile data on disks.
 - b. Wait for the blue LED indicators of the Storage Controllers (ID LEDs) to blink.
 - c. Wait for the Storage Controllers green LED indicators (Power LEDs) to turn off.
Note: At this point, the Storage Controllers’ blue ID LEDs are still blinking.
 - d. When the Storage Controllers’ Power LEDs are turned off, disconnect the power from the system by powering down the rack’s PDUs.
Note: Make sure that no other equipment is connected to the PDUs.
 - e. Skip to [step 3](#), to power off the Battery Backup Unit and complete the shutdown procedure.

NOTICE

Do not disconnect the power at this stage. If the cluster is not given the required time to secure the volatile data on the disks, data loss may occur upon shutting down the hardware.

- If the orange LED indicators of all DAEs and SSDs do not start blinking within a ten seconds time frame, perform the following steps:
 - a. Pull out the two DAE power cables of X-Brick 1 (usually the lowest X-Brick in the rack) from their ports, as shown in [Figure 243](#).



Figure 243 Power Connection Ports on the Rear Side of the DAE

- b. Wait for five minutes to allow the cluster to harden the volatile data on disks.

NOTICE

If the cluster is not given the required time to secure the volatile data on the disks, data loss may occur upon shutting down the hardware.

- c. Disconnect the power from the cluster by powering down the rack's PDUs.

Note: Make sure that no other equipment is connected to the PDUs.

3. Power off the Battery Backup Units in the XtremIO cluster by pressing the power button on each BBU.

Note: If you wish to power up the cluster, refer to “[Powering Up the Cluster after an Emergency Shutdown](#)” on page 320 for details.

Changing the IP Configurations

Changing the IP Configuration in a Single Cluster Environment

This section describes how to change the cluster and XMS IP addresses in the following scenarios:

- ◆ Equipment and cables are not moved.
- ◆ Cables are moved.
- ◆ Equipment is moved.

Changing the IP Configurations without Equipment and Cable Relocation

To change the IP configurations of the cluster and XMS, without relocating equipment and cables:

1. Log in to the XMCLI as admin.
2. Run the following XMCLI command to modify the Management IPs of the XMS and Storage Controllers:

```
modify-ip-addresses
```

Usage: modify_ip_addresses property=value list			
PROPERTY	MANDATORY	DESCRIPTION	VALUE
cluster-id	No	Cluster ID	id:name or index
rollback	No	Rollback changes in case of failure	N/A
sc-gw-addr	One from Group 1	Storage Controller Gateway Address	IP Address
sc-ip-list	One from Group 1	Storage Controller List	[sc-id=value sc-ip-sn="value" ...]
xms-gw-addr	One from Group 1	XMS Gateway Address	IP Address
xms-ip-sn	One from Group 1	XMS IP/Subnet	IP Address/Subnet

For example:

```
xmcli (admin)> modify-ip-addresses sc-ip-list=[sc-id=1
sc-ip-sn="10.76.219.133/20",sc-id=2 sc-ip-sn="10.76.219.134/20"]
xms-ip-sn="10.76.208.77/20" rollback
```

ATTENTION: Only a subset of the cluster's IP addresses are being modified
Are you sure you want to partially modify IP settings? (Yes/No): yes

ATTENTION: XMS can lose connection to nodes.

Are you sure you want to modify IP settings? (Yes/No): yes

...

Storage-Controller-Name	Index	IP-Subnet	...
X1-SC1	1	10.76.219.133/20	
X1-SC2	2	10.76.219.134/20	

Note: If the XMS and SYM addresses are wrong, the cluster rolls back to the old configuration.

Note: If the IP address for one of the Storage Controllers is wrong, run the `change-ip-addresses` command again with the correct address.

Changing the IP Configurations with Cable Relocation

To change the IP configurations of the cluster and XMS, with relocating cables:

1. Log in to the XMCLI as admin.
2. Run the `modify-ip-addresses` CLI command to modify the Management IPs of the XMS and Storage Controllers. Do not enable rollback.

Usage: <code>modify_ip_addresses property=value list</code>			
PROPERTY	MANDATORY	DESCRIPTION	VALUE
cluster-id	No	Cluster ID	id:name or index
rollback	No	Rollback changes in case of failure	N/A
sc-gw-addr	One from Group 1	Storage Controller Gateway Address	IP Address
sc-ip-list	One from Group 1	Storage Controller List	[sc-id=value sc-ip-sn="value" ...]
xms-gw-addr	One from Group 1	XMS Gateway Address	IP Address
xms-ip-sn	One from Group 1	XMS IP/Subnet	IP Address/Subnet

For example:

```
xmcli (admin)> modify-ip-addresses sc-ip-list=[sc-id=1
sc-ip-sn="10.76.219.133/20",sc-id=2 sc-ip-sn="10.76.219.134/20"]
xms-ip-sn="10.76.208.77/20"

ATTENTION: Only a subset of the cluster's IP addresses are being modified
Are you sure you want to partially modify IP settings? (Yes/No): yes
ATTENTION: XMS can lose connection to nodes.
Are you sure you want to modify IP settings? (Yes/No): yes
...
Storage-Controller-Name    Index    IP-Subnet      ...
X1-SC1                    1        10.76.219.133/20
X1-SC2                    2        10.76.219.134/20
```

3. Move the cables to the new network.

Note: If the XMS and SYM addresses are wrong, change them, using xinstall.

Note: If the IP address for one of the Storage Controllers is wrong, run the `change-ip-addresses` command again with the correct address.

Changing the IP Configurations with Equipment and Cable Relocation

To change the IP configurations of the cluster and XMS, with relocating equipment and cables:

1. Log in to the XMCLI as admin.
2. Run the `modify-ip-addresses` XMCLI command to modify the Management IPs of the XMS and Storage Controllers. Do not enable rollback.

Usage: <code>modify_ip_addresses property=value list</code>			
PROPERTY	MANDATORY	DESCRIPTION	VALUE
cluster-id	No	Cluster ID	id:name or index
rollback	No	Rollback changes in case of failure	N/A
sc-gw-addr	One from Group 1	Storage Controller Gateway Address	IP Address
sc-ip-list	One from Group 1	Storage Controller List	[sc-id=value sc-ip-sn="value" ...]
xms-gw-addr	One from Group 1	XMS Gateway Address	IP Address
xms-ip-sn	One from Group 1	XMS IP/Subnet	IP Address/Subnet

For example:

```
xmcli (admin)> modify-ip-addresses sc-ip-list=[sc-id=1
sc-ip-sn="10.76.219.133/20",sc-id=2 sc-ip-sn="10.76.219.134/20"]
xms-ip-sn="10.76.208.77/20"
```

ATTENTION: Only a subset of the cluster's IP addresses are being modified
Are you sure you want to partially modify IP settings? (Yes/No): yes

ATTENTION: XMS can lose connection to nodes.

Are you sure you want to modify IP settings? (Yes/No): yes

```
...
Storage-Controller-Name    Index    IP-Subnet      ...
X1-SC1                   1        10.76.219.133/20
X1-SC2                   2        10.76.219.134/20
```

3. Shut down the XMS, using the emergency shutdown procedure. Refer to [“Shutting Down the Cluster - Emergency Shutdown” on page 334](#) for details.
4. When all Storage Controllers are shut down, move the equipment and cables to the new network.

Note: If the XMS and SYM addresses are wrong, change them, using xinstall.

Note: If the address for one of the Storage Controllers is wrong, run the `change-ip-addresses` command again with the correct address.

Changing the IP Configuration in a Multiple Cluster Environment

This section describes how to change the cluster and XMS IP addresses in a multiple cluster environment. The following scenarios are described:

- ◆ Equipment and cables are not moved.
- ◆ Cables are moved.
- ◆ Equipment is moved.

Changing the IP Configurations without Equipment and Cable Relocation

To change the IP configurations of the cluster and XMS, without relocating equipment and cables:

1. Log in to the XMCLI as admin.
2. For each cluster, run the `modify-ip-addresses` XMCLI command to modify the Storage Controllers' IP addresses. Do not enable rollback.

Usage: <code>modify_ip_addresses property=value list</code>			
PROPERTY	MANDATORY	DESCRIPTION	VALUE
cluster-id	No	Cluster ID	id:name or index
rollback	No	Rollback changes in case of failure	N/A
sc-gw-addr	One from Group 1	Storage Controller Gateway Address	IP Address
sc-ip-list	One from Group 1	Storage Controller List	[sc-id=value sc-ip-sn="value" ...]
xms-gw-addr	One from Group 1	XMS Gateway Address	IP Address
xms-ip-sn	One from Group 1	XMS IP/Subnet	IP Address/Subnet

For example:

```
xmcli (admin)> modify-ip-addresses sc-ip-list=[sc-id=1
sc-ip-sn="10.76.219.133/20",sc-id=2 sc-ip-sn="10.76.219.134/20"]
xms-ip-sn="10.76.208.77/20" rollback
```

ATTENTION: Only a subset of the cluster's IP addresses are being modified
Are you sure you want to partially modify IP settings? (Yes/No): yes

ATTENTION: XMS can lose connection to nodes.

Are you sure you want to modify IP settings? (Yes/No): yes

...

Storage-Controller-Name	Index	IP-Subnet	...
X1-SC1	1	10.76.219.133/20	
X1-SC2	2	10.76.219.134/20	

3. When the IP addresses of all Storage Controllers are modified, run the `modify-ip-addresses` XMCLI command to modify the XMS IP address.
4. For each cluster, verify that the cluster is available on the new network.

Note: If the XMS and SYM addresses are wrong, the cluster rolls back to the old configuration.

Note: If the IP address for one of the Storage Controllers is wrong, run the `change-ip-addresses` command again with the correct address.

Changing the IP Configurations with Cable Relocation

To change the IP configurations of the cluster and XMS, with relocating cables:

1. Log in to the XMCLI as admin.
2. For each cluster, run the `modify-ip-addresses` XMCLI command to modify the Storage Controllers' IP addresses. Do not enable rollback.

Usage: <code>modify_ip_addresses property=value list</code>			
PROPERTY	MANDATORY	DESCRIPTION	VALUE
cluster-id	No	Cluster ID	id:name or index
rollback	No	Rollback changes in case of failure	N/A
sc-gw-addr	One from Group 1	Storage Controller Gateway Address	IP Address
sc-ip-list	One from Group 1	Storage Controller List	[sc-id=value sc-ip-sn="value" ...]
xms-gw-addr	One from Group 1	XMS Gateway Address	IP Address
xms-ip-sn	One from Group 1	XMS IP/Subnet	IP Address/Subnet

For example:

```
xmcli (admin)> modify-ip-addresses sc-ip-list=[sc-id=1
sc-ip-sn="10.76.219.133/20",sc-id=2 sc-ip-sn="10.76.219.134/20"]
xms-ip-sn="10.76.208.77/20" rollback
```

ATTENTION: Only a subset of the cluster's IP addresses are being modified
Are you sure you want to partially modify IP settings? (Yes/No): yes

ATTENTION: XMS can lose connection to nodes.

Are you sure you want to modify IP settings? (Yes/No): yes

```
...
Storage-Controller-Name    Index    IP-Subnet      ...
X1-SC1                    1        10.76.219.133/20
X1-SC2                    2        10.76.219.134/20
```

3. When the IP addresses of all Storage Controllers are modified, run the `modify-ip-addresses` XMCLI command to modify the XMS IP address.
4. Move the cables to the new network.
5. For each Cluster, verify that the cluster is available on the new network.

Note: If the XMS and SYM addresses are wrong, the cluster rolls back to the old configuration.

Note: If the IP address for one of the Storage Controllers is wrong, run the `change-ip-addresses` command again with the correct address.

Changing the IP Configurations with Equipment and Cable Relocation

To change the IP configurations of the cluster and XMS, with relocating equipment and cables:

1. Log in to the XMCLI as admin.
2. For each cluster, run the `modify-ip-addresses` XMCLI command to modify the Storage Controllers' IP addresses. Do not enable rollback.

Usage: <code>modify_ip_addresses property=value list</code>			
PROPERTY	MANDATORY	DESCRIPTION	VALUE
cluster-id	No	Cluster ID	id:name or index
rollback	No	Rollback changes in case of failure	N/A
sc-gw-addr	One from Group 1	Storage Controller Gateway Address	IP Address
sc-ip-list	One from Group 1	Storage Controller List	[sc-id=value sc-ip-sn="value" ...]
xms-gw-addr	One from Group 1	XMS Gateway Address	IP Address
xms-ip-sn	One from Group 1	XMS IP/Subnet	IP Address/Subnet

For example:

```
xmcli (admin)> modify-ip-addresses sc-ip-list=[sc-id=1
sc-ip-sn="10.76.219.133/20",sc-id=2 sc-ip-sn="10.76.219.134/20"]
xms-ip-sn="10.76.208.77/20" rollback
```

ATTENTION: Only a subset of the cluster's IP addresses are being modified
Are you sure you want to partially modify IP settings? (Yes/No): yes

ATTENTION: XMS can lose connection to nodes.

Are you sure you want to modify IP settings? (Yes/No): yes

```
...
Storage-Controller-Name    Index    IP-Subnet      ...
X1-SC1                   1        10.76.219.133/20
X1-SC2                   2        10.76.219.134/20
```

3. When the IP addresses of all Storage Controllers are modified, run the `modify-ip-addresses` XMCLI command to modify the XMS IP address.
4. Shut down the XMS, using the emergency shutdown procedure. Refer to “[Shutting Down the Cluster - Emergency Shutdown](#)” on page 334 for details.
5. When all Storage Controllers are shut down, move the equipment and cables to the new network.
6. For each cluster, verify that the cluster is available on the new network.

Note: If the XMS and SYM addresses are wrong, the cluster rolls back to the old configuration.

Note: If the IP address for one of the Storage Controllers is wrong, run the `change-ip-addresses` command again with the correct address.

Updating the ESRS Configurations

If ESRS is used, the ESRS configurations should be updated by EMC Global Tech Support personnel after changing the XMS IP addresses.

To update the ESRS configurations, contact the EMC Global Tech Support.

Updating the XMS NTP Server Address

This procedure configures the time zone and updates the XMS NTP time sync service with the new NTP server(s).

To update the XMS NTP Server Address:

1. Log in to the XMCLI as admin.
2. Use the `modify-datetime` XMCLI command to set the time zone.

```
xmcli (admin)> modify-datetime timezone=US/Eastern  
Cluster time is now: 2013-10-24 16:30:12 EDT
```

3. Use the `modify-datetime` XMCLI command to set the new NTP server address(es) on the XMS.

```
xmcli (admin)> modify-datetime  
ntp-servers=["10.10.10.20","10.10.10.30"]  
Replace the current ntp-server list:[‘10.10.10.20’,‘10.10.10.30’]?  
Yes/No: Yes  
Syncing to time servers: [‘10.10.10.20’,‘10.10.10.30’]
```

Note: It may take up to one hour for clocks to sync.

4. Run the `show-datetime` XMCLI command to verify that the clocks are synchronized:

```
xmcli (admin)> show-datetime  
Mode          NTP-Servers   Cluster-Time           Cluster-Time-Zone  
Automatic    10.10.10.20  2014-10-23 16:30:12 EST  US/Eastern  
                         10.10.10.30
```

Setting the Cluster Time and Date

It is recommended to use an NTP server to synchronize date and time across the cluster. However, you can disable the NTP server synchronization by setting the cluster's date and time manually.

To set the cluster's date and time manually:

1. Log in to the XMCLI as admin.
2. Use the `modify-datetime` XMCLI command to set the time zone (if needed).

```
xmcli (admin)> modify-datetime timezone=US/Eastern
Cluster time is now: 2014-12-11 16:30:12 EST
```

3. Use the `modify-datetime` XMCLI command to manually set the date and time.

```
xmcli (admin)> modify-datetime datetime="2014-12-10 17:32:41"
Cluster time is now: 2014-12-10 17:32:41 EST
```

4. Run the `show-datetime` XMCLI command and verify that the mode is set to Manual, indicating that the NTP server synchronization is disabled:

```
xmcli (admin)> show-datetime
Mode      NTP-Servers   Cluster-Time           Cluster-Time-Zone
Manual          2014-12-10 17:32:48 EST US/Eastern
```

Managing the Virtual XMS

Deploying a Virtual XMS

Note: For Virtual XMS requirements, refer to the *XtremIO Storage Array Site Preparation Guide*.

An OVA image (VMware template machine file type), which includes all required packages for installing the XMS, is provided.

To install a virtual XMS in preparation for the XtremIO cluster installation, opt to deploy the OVA template.

Note: If you choose not to deploy the OVA template, the deployment will be performed as part of the cluster installation procedure.

To deploy an OVA image:

1. Access the EMC Support page for XtremIO.
2. Download the OVA Template. For details on which OVA Template to download from the Support page, refer to the *XtremIO Storage Array Release Notes* of the version you are installing.

Note: Before proceeding, access the EMC Support page and verify that the MD5 checksum of the package you downloaded matches the MD5 checksum that appears in the support page for that package.

3. Log in to the vCenter Server, using the vSphere Web Client.
4. Select an inventory object that is a valid parent object of the virtual XMS machine (e.g. datacenter, folder, cluster, resource pool or host).

5. Select **Actions > All vCenter Actions > Deploy OVF Template.**

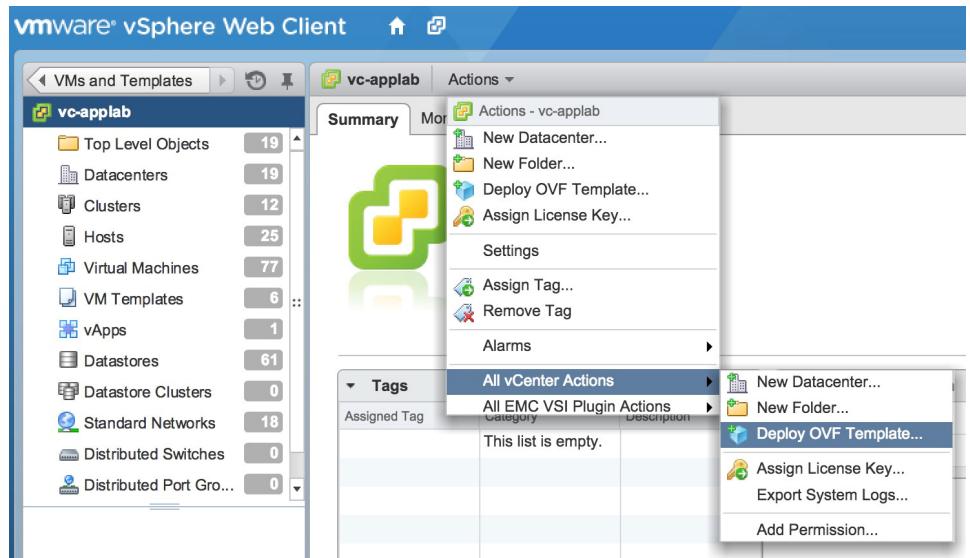


Figure 244 Deploy OVA Image

6. In the 1a Select Source pane, click **Local file** and then click **Browse**.
7. Select the XMS OVA template and click **Next**.

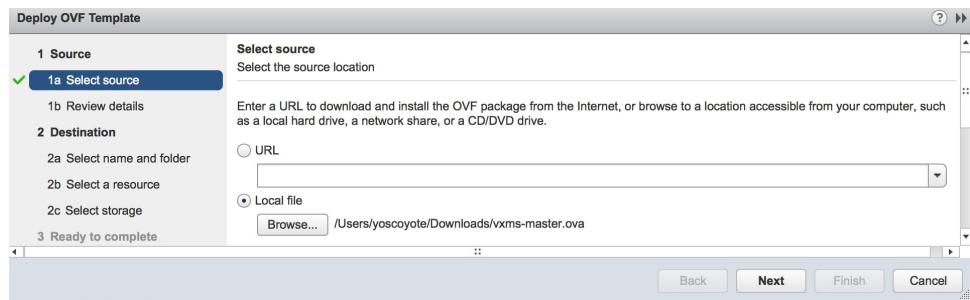


Figure 245 Display OVA Template

8. In the 1b Review Details pane, review the details of the OVA Template and click **Next**.
9. In the 2a Select Name and Folder pane, type a name for the virtual XMS and select a destination folder and click **Next**.
10. In the 2b Select a Resource pane, select a server/cluster to run the virtual XMS and click **Next**.
11. In the 2c Select Storage pane, select a datastore to provision the virtual XMS.
12. In the Select virtual disk format drop-down list, select **Thin Provision** disk format for the XMS's virtual disk and click **Next**.

Note: It is recommended to deploy a virtual machine with 'Thin Provision' settings to ensure that the XMS does not consume more space than it actually requires. With XtremIO version 4.0, 200GB of disk capacity are pre-allocated for the virtual XMS, following cluster initialization.

13. In the 2d Select networks pane, configure the network used for the virtual XMS and click **Next**.
14. In the 3 Ready to complete pane, verify that the virtual XMS VM that is about to be created meets (or exceeds) the following requirements:

Parameter	Value
RAM	8GB capacity
CPU	2 X vCPU
NIC	1 X vNIC
Virtual HD	Single HD with 900GB capacity (recommended (thin-provisioned)

15. Click **Finish** to deploy the template.
16. Connect to the virtual XMS via a physical console, using a pre-defined IP address or a vSphere Web Client console.

Relocating a Virtual XMS

Once a virtual XMS has been deployed, it can be relocated to another ESX server and/or virtual storage location. Relocation of the virtual XMS can be achieved seamlessly without disrupting the cluster or virtual XMS, by leveraging VMware vSphere to perform either a vMotion or Storage vMotion function.

All virtual XMS requirements must be met in full for the ESX server and virtual storages' new destination, including protected shared storage (for details, see the *XtremIO Storage Array Site Preparation Guide*).

Note: It is very important to ensure that the new destination location of the virtual storage for the virtual XMS does not originate from an XtremIO cluster.

Restoring Access to the Virtual XMS

The Virtual XMS should be deployed on a thin provisioning virtual disk. Storage capacity for the virtual XMS is allocated on demand rather than all in advance. Refer to the *XtremIO Storage Array Site Preparations Guide* for details on the required storage resources for the Virtual XMS.

As a result, the Virtual XMS may encounter a scenario in which the datastore it is deployed on is full because it was fully consumed by other virtual machines deployed on the same datastore as the Virtual XMS.

When the ESX host detects such a state, it suspends the Virtual XMS and displays a warning indicating that no more disk space is available for the Virtual XMS. The warning is displayed on the vCenter Server webUI.

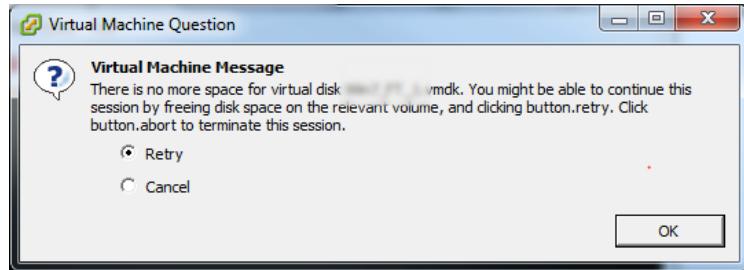


Figure 246 Virtual Disk Full Warning

At this point the Virtual XMS is suspended and there is no access to any XtremIO management interface that is executed from the XMS (e.g. CLI, GUI, RESTful API and SSH). However, there is no impact on cluster service on any of the clusters that are connected to the affected Virtual XMS.

The following procedure is used to restore access to the Virtual XMS.

To restore access to the virtual XMS:

1. Take steps to free disk space on the affected datastore (e.g. by removing other virtual machines that are no longer needed from the datastore). Alternatively, you can extend the datastore by allocating additional storage resources to it.
2. If additional time is required, select the **Cancel** option on the displayed warning and click **OK**; the virtual XMS is powered off due to the lack of free disk space on the affected datastore.

Note: Trying to power up a Virtual XMS when the datastore it is deployed on is full, will fail with an error.

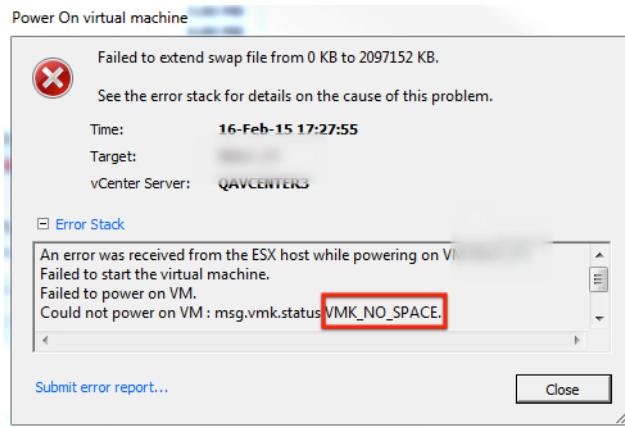


Figure 247 Power Virtual Machine Failure Message

3. When there is sufficient free disk space and the XMS is suspended, select the **Retry** option on the displayed warning and click **OK** to resume the Virtual XMS operation. If the Virtual XMS is powered off, power it up, using vSphere webUI. At this point access to all XMS interfaces is resumed.

CHAPTER 9

CLI Guide

This chapter includes the following topics:

◆ Using the Command Line Interface (CLI)	350
◆ Objects Naming Limitations	352
◆ Completion Codes.....	353
◆ CLI Commands Quick Finder.....	354
◆ Basic CLI Commands.....	362
◆ Cluster Related CLI Commands	363
◆ Basic Cluster Management CLI Commands	397
◆ Volume Related CLI Commands	399
◆ Initiator Group Related CLI Commands	415
◆ LUN Mapping Related CLI Commands	425
◆ Alert Related CLI Commands	427
◆ Event Related CLI Commands	430
◆ ISCSI Routing Related CLI Commands	434
◆ User Account Management Related CLI Commands	439
◆ Notification Related CLI Commands.....	441
◆ Data Protection Related CLI Commands	448
◆ Cluster Health Related CLI Commands	454
◆ Storage Controllers Related CLI Commands	458
◆ Performance Related CLI Commands	464
◆ Tag Management CLI Commands.....	487
◆ Certificate Management CLI Commands	489

Using the Command Line Interface (CLI)

You can manage and monitor the XtremIO Storage Array, using the CLI.

You can access the CLI via:

- ◆ The GUI (see “[Accessing the CLI via the GUI](#)” on page 350)
- ◆ An SSH client (see “[Accessing the CLI via an SSH Client](#)” on page 351)
- ◆ An SSH key authentication (see “[Accessing the CLI via an SSH Key Authentication](#)” on page 351)

Accessing the CLI via the GUI

To access the CLI through the GUI:

1. From the main menu, select Administration.
2. From the left pane, select CLI Terminal; the CLI Terminal screen appears, as shown in [Figure 248](#), allowing you to run CLI commands according to your user’s role.

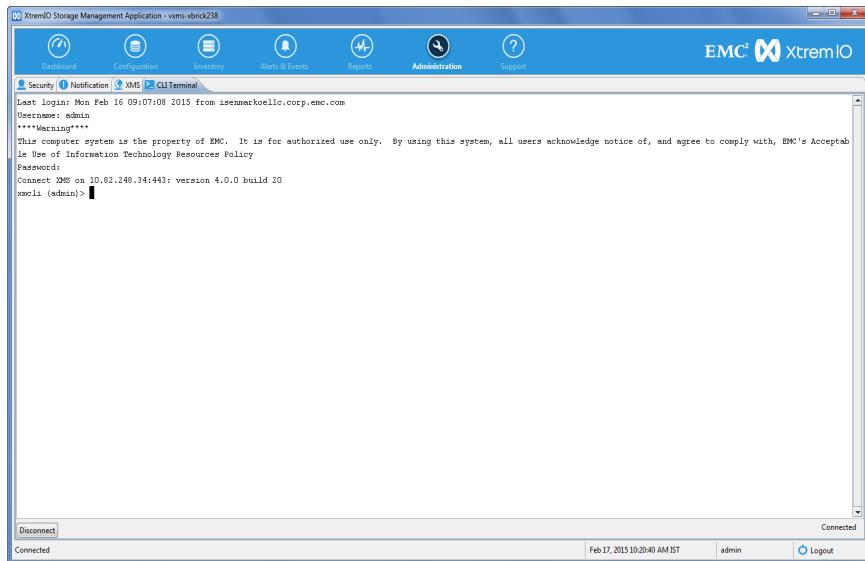


Figure 248 CLI Terminal Pane

Accessing the CLI via an SSH Client

Note: The CLI access via SSH requires two sets of credentials. The first set is generic to any user. The second set is user-specific according to the user assigned to you by the System or Storage Administrator.

To access the CLI via an SSH client:

1. SSH to the XMS server with the following credentials:
 - User - xmsadmin
 - Password - the password assigned by your system administrator
2. Log in to XtremIO, using the username and password assigned by your system administrator (refer to “[Managing User Accounts, Using the GUI](#)” on page 294); the XMCLI session prompt appears, allowing you to run only XMCLI commands according to your user’s role.

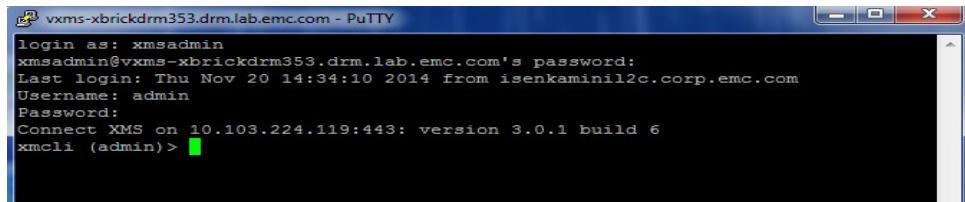


Figure 249 CLI Terminal - Session Prompt

Accessing the CLI via an SSH Key Authentication

An administrator may register a user account via an SSH Key Authentication which does not require credentials to log in.

To access the CLI via an SSH key authentication:

1. Create a user on a remote server and generate an SSH public key pair.
2. Copy the user’s public key content to your clipboard.
3. Log in to the XMCLI with an administrative account.
4. Run the `add-user-account` XMCLI command with the "public-key" parameter.
5. From the remote server, log in to the XMS, using `ssh user@xms`; the user logs into the XMCLI directly.

Objects Naming Limitations

Volume and folder names used as parameters in the CLI commands must comply with the following limitations:

- ◆ Allowed length: up to 64 characters
- ◆ Valid characters:
 - Alphanumeric characters
 - Space character
 - The following characters: ~ ! @ # \$ % ^ * _ + { } | : ? . -
- ◆ Invalid characters: & / <> ()

Completion Codes

The following table contains a list of general completion codes that can be issued by any command.

Output Parameter	Description
unauthorized_command	The user account which issued this command does not have the required authorization level.
user_not_found	The specified user account does not exist.
ok	The command completed successfully.
invalid_command	The issued command is invalid.
invalid_input	Invalid values were entered with the command. For example, a string was entered for a property that requires an IP address.
system_communication_error	The management server cannot communicate with the cluster, possibly due to a network error.
system_general_error	An error has occurred in the cluster.
system_is_busy	The command cannot be completed because the cluster is busy.
system_timeout	the command timed out before it was completed.
no_sys_response_retrying	The management server lost communication with the cluster after a command was issued and it is not known if the command completed successfully. This error should clear once communication with the cluster has been restored.
uncertain_object_error	The current state of the component for which this command was issued is not known. An uncertainty_error completion code has already been issued for this component. If this completion code appears, some XMCLI commands display "pending" under the certainty-state field. If this persists, contact XtremIO.
invalid_in_cur_sys_state	The command is invalid because of the current Cluster State . For example, a stop-cluster command was issued and the cluster is already stopped.

CLI Commands Quick Finder

Command	Description	Page
acknowledge-alert	Acknowledges an alert and removes it from the active alerts list.	427
activate-storage-controller	Activates a replaced or non-active Storage Controller.	463
add-cluster	Adds a cluster to the existing cluster configuration.	397
add-event-handler-definition	Adds a definition to an event handling rule.	432
add-initiator	Adds an Initiator and associates it with an existing Initiator Group.	415
add-initiator-group	Adds an Initiator Group and its associated Initiators to the XtremIO cluster.	416
add-iscsi-portal	Maps a portal to a Target.	434
add-iscsi-route	Adds and configures iSCSI route parameters.	434
add-ldap-config	Adds a new LDAP configuration profile to the LDAP configuration table.	388
add(ssd)	Adds an SSD to the X-Brick and initializes it.	451
add-user-account	Adds a new user account.	439
add-volume	Configures and adds a new Volume.	399
add-volume-to-consistency-group	Adds a Volume to a Consistency Group.	411
assign(ssd)	Assigns an existing SSD to a Data Protection Group.	364
clear-volume-reservation	Removes LUN reservations to release them for access.	400
control-led	Turns an indicator LED on or off.	447
create-consistency-group	Creates a new Consistency Group.	411
create-debug-info	Creates a debug archive log collection.	455
create-ip-link	Establishes an IP link to a remote cluster.	379
create-scheduler	Creates a new Snapshot Scheduler.	405
create-server-certificate-signing-request	Instructs the server to generate a public-private key pair and a certificate signing request.	489
create-snapshot	Creates a Snapshot from a specified Volume.	404
create-snapshot-and-reassignment	Creates a Snapshot from a specified Volume/Snapshot, Consistency Group, or Snapshot Sets and reassigns the Volume identity characteristic to the created Snapshot.	404
create-tag	Adds a Volume or Initiator Group folder.	487
deactivate-storage-controller	Deactivates an active Storage Controller.	463
exit	Closes the CLI terminal.	362

Command	Description	Page
export-performance-history	Exports the cluster's performance history to CSV file.	486
help	Displays available CLI commands.	362
install-self-signed-server-certificate	Installs the new self signed certificate.	490
map-lun	Maps a Volume to an Initiator Group and assigns a Logical Unit Number (LUN) to it.	425
modify-alert-definition	Modifies alert definition properties for a specified alert type.	427
modify-chap	Modifies CHAP configuration parameters.	424
modify-clusters-parameters	Modifies the iSCSI TCP port number.	371
modify-cluster-thresholds	Modifies the properties for thin provisioning soft limits for connected clusters.	414
modify-datetime	Sets or modifies the cluster's date and time, timezone, or NTP server parameters.	392
modify-dns-servers	Sets or modifies the IP address of the primary and secondary DNS servers.	393
modify-email-notifier	Modifies the email notification settings.	442
modify-eth-port	Modifies the Ethernet port of the cluster.	378
modify-event-handler-definition	Modifies the definition of event handling rules.	433
modify-initiator	Modifies the properties of an existing Initiator.	416
modify-ip-addresses	Modifies the XMS networking configuration.	378
modify-iscsi-portal	Modifies an iSCSI portal parameters.	434
modify-ldap-config	Modifies an LDAP configuration profile.	389
modify-login-banner	Enables customization of the login banner text.	393
modify-password	Modifies the user's password.	440
modify-scheduler	Modifies a Snapshot Scheduler's parameters.	407
modify-server-certificate	Initiates loading of a signed certificate and a key.	489
modify-server-name	Defines or modifies the XMS's URL.	393
modify-snmp-notifier	Modifies the SNMP notification settings.	444
modify-ssh-firewall	Modifies the lock mode of the SSH firewall.	379
modify-syrs-notifier	Modifies the ESRS (EMC Secure Remote Support) notification parameters.	446
modify-syslog-notifier	Sets or modifies the Syslog notifier list.	393
modify-tag	Modifies a specified Tag's caption.	487
modify-target	Modifies a Target's parameters.	364
modify-target-group	Modifies a Target group's parameters.	364

Command	Description	Page
modify-user-account	Modifies the user-account parameters.	439
modify-volume	Modifies a Volume's parameters.	400
modify-webui	Enables or disables XtremIO WebUI technology preview mode.	394
modify-xms-parameters	Modifies the XMS's user inactivity timeout.	376
power-off	Powers off a Storage Controller or an entire cluster.	398
power-on	Powers up a Storage Controller.	398
quit	Closes the CLI terminal.	362
remove-cluster	Removes a cluster from the existing cluster configuration.	397
remove-consistency-group	Deletes a Consistency Group.	413
remove-debug-info	Deletes the debug info file.	456
remove-event-handler-definition	Deletes event handling rule definitions.	432
remove-initiator	Deletes an Initiator.	417
remove-initiator-group	Deletes an Initiator Group.	417
remove-ip-link	Removes an IP link to a remote cluster.	379
remove-iscsi-portal	Deletes a portal mapping from a Target.	435
remove-iscsi-route	Deletes an iSCSI routing configuration.	435
remove-ldap-config	Removes an LDAP configuration profile from the LDAP configuration table.	389
remove-scheduler	Removes a Snapshot Scheduler.	407
remove-snapshot-set	Removes a Snapshot Set	410
remove(ssd)	Removes an SSD from a Data Protection Group.	448
remove-tag	Deletes a Volume or Initiator Group's folder.	488
remove-user-account	Removes a user account.	440
remove-volume	Removes a Volume.	399
remove-volume-from-consistency-group	Removes a Volume from a Consistency Group.	411
rename	Renames a component of the XtremIO Storage Array.	365
restart-xms	Restarts XtremIO management system.	376
resume-scheduler	Reactivates a suspended Snapshot Scheduler.	407
send-email-notification	Sends an Email notification.	442
send-snmp-notification	Sends an SNMP notification.	444
send-sys-notification	Sends a predefined ESRS (EMC Secure Remote Support) information notification.	446

Command	Description	Page
set-context	Sets a cluster context in a multiple cluster environment and renders the need to specify the cluster ID unnecessary.	363
show-alert-definitions	Displays a list of pre-defined alerts and their definitions.	429
show-alerts	Displays a list of active alerts and their details.	428
show-bbus	Displays Battery Backup Units information.	367
show-bricks	Displays a list of X-Bricks and their associated cluster.	366
show-chap	Displays the cluster's configured CHAP authentication and discovery modes.	424
show-cluster-expansion-progress	Displays indicators of the cluster expansion process progress.	373
show-clusters	Displays the connected clusters information.	369
show-clusters-data-protectio-n-properties	Displays the clusters' data protection properties.	453
show-clusters-info	Displays the connected clusters information.	370
show-clusters-parameters	Displays the parameters of the selected cluster.	438
show-clusters-performance	Displays the clusters' performance data.	477
show-clusters-performance-latency	Displays the clusters' performance latency data.	479
show-clusters-performance-small	Displays the clusters' performance data for small (under 4KB) blocks.	478
show-clusters-performance-unaligned	Displays the clusters' performance data for unaligned blocks.	479
show-clusters-savings	Displays savings parameters of the selected cluster.	371
show-clusters-thresholds	Displays thin provisioning soft limits for the connected clusters.	414
show-clusters-upgrade	Displays the clusters' software upgrade status.	372
show-clusters-upgrade-progr	Displays indicators of the clusters' software upgrade progress.	373
show-consistency-group	Displays a specified Consistency Group's parameters.	412
show-consistency-groups	Displays all the defined Consistency Groups' parameters.	413
show-daes	Displays the cluster's DAE information.	387
show-daes-controllers	Displays a list of DAE controllers and their properties.	385
show-daes-psus	Displays a list of DAE power suppliers and their properties.	386
show-data-protection-groups	Displays XDP groups status and information.	452
show-data-protection-groups-perf	Displays Data Protection Groups performance information.	476

Command	Description	Page
show-datetime	Displays the cluster's time-related information.	392
show-debug-info	Displays debug information created using 'create-debug-info' command.	456
show-discovered-initiators-connectivity	Displays the Initiators-Targets connectivity map.	422
show-dns-servers	Displays the IP addresses of the primary and secondary DNS servers (if configured).	392
show-email-notifier	Displays Email notification settings.	441
show-event-details	Displays the details of the specified event.	431
show-event-handler-definitions	Displays event handling rule definitions.	432
show-events	Displays the cluster's events.	430
show-infiniband-switches	Displays InfiniBand Switches' information.	383
show-infiniband-switches-ports	Displays InfiniBand Switches' port information.	382
show-infiniband-switches-psus	Displays InfiniBand Switches' PSUs information	384
show-initiator-group	Displays information for a specific Initiator Group.	419
show-initiator-groups	Displays information for all Initiator Groups.	420
show-initiator-groups-performance	Displays Initiator Groups' performance data.	464
show-initiator-groups-performance-small	Displays Initiator Groups' performance data for small (under 4KB) blocks.	465
show-initiator-groups-performance-unaligned	Displays Initiator Groups' performance data for unaligned blocks.	466
show-initiators	Displays Initiators' data.	418
show-initiators-connectivity	Displays Initiators-port connectivity and the number of connected Targets.	423
show-initiators-performance	Displays Initiators' performance data.	467
show-initiators-performance-small	Displays Initiators' performance data for small (under 4KB) block sizes.	468
show-initiators-performance-unaligned	Displays Initiators' performance data for unaligned data block.	469
show-ip-addresses	Displays the XMS networking configuration, including IP addresses, network mask and default GW.	377
show-iscsi-counters	Displays iSCSI-related counters.	437
show-iscsi-portals	Displays a list of iSCSI portals and their properties.	435
show-iscsi-routes	Displays a list of iSCSI routes and their properties.	436
show-ldap-configs	Displays the LDAP server configuration parameters.	390

Command	Description	Page
show-leds	Displays the values for the identification and status LEDs.	447
show-local-disks	Displays the Storage Controller's local disks information.	462
show-lun-mappings	Displays the Storage Controller's local disks information.	426
show-most-active	Displays the most active Volumes and Initiator Groups.	470
show-most-active-initiator-groups	Displays performance data of the most active Initiator Groups.	471
show-most-active-volumes	Displays performance data of the most active Volumes.	472
show-remote-servers-status	Displays NTP, DNS, gateway servers information.	391
show-report	Displays the details of a specified report.	394
show-reports	Displays a list of defined reports.	395
show-reports-data	Displays data for a specified entity and category.	396
show-schedulers	Displays the defined schedulers parameters.	406
show-server-certificate	Displays the currently loaded certificate.	490
show-server-certificate-signing-request	Displays the certificate signing request.	490
show-server-name	Displays the server name, according to the name configuration mode.	391
show-slots	Displays a list of SSD slots and their properties.	448
show-snapshot-set	displays the parameters of a specified snapshot set.	410
show-snapshot-sets	Displays a list of snapshot sets and their data.	409
show-snapshots	Displays a list of snapshots and related information.	408
show-snmp-notifier	Displays SNMP notification configuration.	443
show-ssd-sas-counters	Displays a specified SSD's SAS counters information.	450
show-ssds	Displays a list of SSDs in the cluster and their properties.	449
show-ssds-performance	Displays SSDs' performance data.	476
show-storage-controllers	Displays the cluster's Storage Controllers information and status.	368
show-storage-controllers-fw-versions	Displays the Storage Controllers' firmware version information.	459
show-storage-controllers-infiniband-counters	Displays Storage Controllers' InfiniBand different counters.	381
show-storage-controllers-infiniband-ports	Displays Storage Controllers' InfiniBand port information.	380

Command	Description	Page
show-storage-controllers-info	Displays the Storage Controllers' information.	458
show-storage-controllers-psus	Displays the Storage Controller's power supply units information.	460
show-storage-controllers-sensors	Displays a list of sensors and their related information.	461
show-sw-image-details	Displays software updates and versions that are included in the package. Content may vary between different versions.	363
show-sw-images	Displays the names and version numbers of the available software images.	363
show-syr-notifier	Displays ESRS (EMC Secure Remote Support) information notification configuration.	445
show-syslog-notifier	Displays the Syslog server notification status.	391
show-tag	Displays the details of a specified Tag.	488
show-tags	Displays a list of all defined Tags.	488
show-target-groups	Displays a list of Target Groups.	422
show-target-groups-fc-error-counters	Displays Fibre Channel error counter per Target Group.	455
show-target-groups-performance	Displays Target Groups' performance data.	480
show-target-groups-performance-small	Displays Target Groups' performance data for small (under 4KB) blocks.	481
show-target-groups-performance-unaligned	Displays Target Groups' performance data for unaligned blocks.	482
show-targets	Displays the cluster Targets' information.	421
show-targets-fc-error-counters	Displays Fibre Channel error counter per Target.	454
show-targets-performance	Displays Targets' performance data.	483
show-targets-performance-small	Displays Targets' performance data for small (under 4KB) blocks.	484
show-targets-performance-unaligned	Displays Targets' performance data for unaligned blocks.	485
show-timezones	Displays the timezones list.	391
show-user-accounts	Displays user accounts information.	440
show-volume	Displays the specified Volume's information.	401
show-volume-snapshot-groups	Displays a list of Volumes with their associated snapshots and their parameters.	403
show-volumes	Displays a list of Volumes and their information.	402
show-volumes-performance	Displays Volumes' performance data.	473
show-volumes-performance-small	Displays Volumes' performance data for small (under 4KB) blocks.	474

Command	Description	Page
show-volumes-performance-unaligned	Displays Volumes' performance data for unaligned blocks.	475
show-xenvs	Displays a list of Storage Controller x-envs and their properties.	463
show-xms	Displays XtremIO management system information.	374
show-xms-info	Displays information on server statistics, disk usage and Ethernet interfaces.	375
shutdown-xms	Stops the XMS service or shuts down the XtremIO Management System.	376
start-cluster	Starts a stopped cluster and enables it to respond to host IOs and process data.	397
stop-cluster	Stops an active cluster and disables data processing in an orderly manner.	397
suspend-scheduler	Suspends an active snapshot scheduler.	407
tag-object	Moves a Volume or an Initiator Group to a folder.	487
test-ip-connectivity	Performs a connectivity test to a specified IP address.	380
test-xms-storage-controller-connectivity	Performs a connectivity test to a specified Storage Controller and its managing XMS.	456
test-xms-tcp-connectivity	Performs a connectivity check for a specified TCP port and the XMS.	457
unmap-lun	Removes a Volume's LUN mappings.	426
untag-object	Removes a Tag from a specified object.	487

Basic CLI Commands

exit

The `exit` command closes the CLI terminal and returns to the administration screen.

Displayed data is removed upon exiting the CLI terminal and does not appear when the terminal is reopened.

help

The `help` command displays a list of all available CLI commands, or provides full usage information of a specified command.

quit

The `quit` command closes the CLI terminal and returns to the administration screen.

Displayed data is removed upon exiting the CLI terminal and does not appear when the terminal is reopened.

Cluster Related CLI Commands

set-context

The `set-context` command sets a cluster context in a multiple cluster environment and renders the need to specify the cluster ID unnecessary.

Input Parameter	Description	Value	Mandatory
all	All clusters	N/A	One from Group 1
cluster-id	Cluster ID	Name or Index	One from Group 2

Mandatory groups:

Group1:[‘all’, ‘cluster-id’]

Exclusive groups:

Group1:[‘all’]

Group2:[‘cluster-id’]

show-sw-images

The `show-sw-images` command displays the names and version numbers of the available software images.

Output Parameter	Description
Package-Name	The name of the software package
Package-is-Valid	Indicates if the software package is valid.
Version	Version number of the software package
MD5-Signature	The image’s MD5 signature

show-sw-image-details

The `show-sw-image-details` command displays software updates and versions that are included in the package. The content may vary between different versions.

Input Parameter	Description	Value	Mandatory
package	Software package file name	File name	Yes

assign-ssd

The `assign-ssd` command assigns an existing SSD to a Data Protection Group.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
dpg-id	XDP group ID	Name or index	Yes
ssd-id	SSD ID	Name or index	Yes

modify-target

The `modify-target` command modifies a Target parameters.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
mtu	Maximum transmission unit size	Integer	Yes
tar-id	The Target's name or index number	Name or index	Yes

modify-target-group

The `modify-target` command modifies a Target Group's parameters.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
mtu	Maximum transmission unit size	Integer	Yes
tg-id	Target Group ID	Name or index	Yes

rename

The `rename` command renames a component of the XtremIO Storage Array.

Input Parameter	Description	Value	Mandatory
new-caption	New caption	String	One from Group 1*
new-name	New name	String	One from Group 1*
sc-id	Storage Controller ID	Name or index	One from Group 2**
cluster-id	Cluster ID	Name or index	One from Group 2**
xms-id	XMS ID	Name or index	One from Group 2**
vol-id	Volume ID	Name or Index	One from Group 2**
dpg-id	Data Protection Groups ID	Name or index	One from Group 2**
tar-id	Target ID	Name or index	One from Group 2**
tag-id	Tag ID	Name or Index	One from Group 2**
storage-controller-psu-id	Storage Controller PSU ID	Name or Index	One from Group 2**
snapshot-set-id	Snapshot Set ID	Name or Index	One from Group 2**
dae-lcc-id	DAE LCC ID	Name or Index	One from Group 2**
tg-id	Target Group ID	Name or Index	One from Group 2**
dae-id	DAE ID	Name or Index	One from Group 2**
mdl-id	Module ID	Name or index	One from Group 2**
ib-switch-id	InfiniBand Switch ID	Name or Index	One from Group 2**
ssd-id	SSD ID	Name or index	One from Group 2**
xenv-id	XENV ID	Name or index	One from Group 2**
ig-id	Initiator Group ID	Name or index	One from Group 2**
brick-id	Brick ID	Name or index	One from Group 2**
usr-id	User ID	Name or index	One from Group 2**
initiator-id	Initiator ID	Name or index	One from Group 2**
dae-psu-id	DAE PSU ID	Name or Index	One from Group 2**
snapgrp-id	SG ID	Name or Index	One from Group 2**
local-disk-id	LocalDisk ID	Name or Index	One from Group 2**
ib-switch-psu-id	InfiniBand Switch PSU ID	Name or Index	One from Group 2**
cg-id	Consistency Group ID	Name or Index	One from Group 2**

*)Group1:[‘new-caption’, ‘new-name’]

**)Group2:[‘tag-id’, ‘dae-lcc-id’, ‘ib-switch-id’, ‘brick-id’, ‘cluster-id’, ‘dpg-id’, ‘ig-id’, ‘ib-switch-psu-id’, ‘dae-psu-id’, ‘snapgrp-id’, ‘initiator-id’, ‘mdl-id’, ‘sc-id’, ‘ssd-id’, ‘tar-id’, ‘storage-controller-psu-id’, ‘cg-id’, ‘tg-id’, ‘local-disk-id’, ‘dae-id’, ‘usr-id’, ‘vol-id’, ‘xenv-id’, ‘xms-id’, ‘snapshot-set-id’]

show-bricks

The `show-bricks` command displays a list of X-Bricks and their associated cluster.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Brick-Name	The X-Brick's name
Index	The X-Brick's index number
Cluster-Name	The cluster's name
Index	The cluster's index number
State	The X-Brick's current state: <ul style="list-style-type: none">• Not_in-sys - the X-Brick is not an active part of the cluster.• In_sys - the X-Brick is part of the cluster.

show-bbus

The `show-bbus` command displays Battery Backup Units information.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The BBU's name
Index	The BBU's index number
Model	The BBU's model
Serial-Number	The BBU's serial number
Power-Feed	The BBU's power feed (A or B)
State	Indicates if the BBU is healthy, disconnected, failed, or, initializing.
Connectivity-State	The BBU's connectivity state to the Storage Controller
Enabled-State	Indicates whether the BBU is enabled
Input	Indicates if there is external power feed to the BBU (on or off).
Battery-Charge	Percentage of BBU battery charge. If the BBU is unreachable or disabled, this parameter is NULL.
BBU-Load	Percentage of the current BBU load
Voltage	The input voltage of the BBU. If the BBU is unreachable or disabled, this parameter is NULL.
FW-Version	The BBU's Firmware version
Part-Number	A string identifier of the part (assigned by EMC)
Brick-Name	The X-Brick's name
Index	The X-Brick's index number
Cluster-Name	The cluster's name
Index	The cluster's index number

show-storage-controllers

The `show-storage-controllers` command displays the cluster's Storage Controllers information and status.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Storage-controller-Name	The Storage Controller's name
Index	The Storage Controller's index number
Mgr-Addr	The management IP of the Storage Controller
IB-Addr-1	The Storage Controller's internal back-end IP address for port 1, used for communication to the InfiniBand Switch
IB-Addr-2	The Storage Controller's internal back-end IP address for port 2, used for communication to the InfiniBand Switch
Brick-Name	The ID of the X-Brick to which the Storage Controller belongs
Index	The X-Brick's index number
Cluster-Name	The name of the cluster to which the Storage Controller belongs
Index	The cluster's index number
State	The Storage Controller's state
Health-State	A summary state that describes the Storage Controller's overall state, including hardware and software components of Xtremapp (currently to be ignored).
Enabled-State	The Storage Controller's enabled state
Stop-Reason	The reason for the Storage Controller's stop (if any)
Conn-State	The Storage Controller's connectivity state to the XMS

show-clusters

The `show-clusters` command displays connected clusters information.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Cluster-Name	The cluster's name
Index	The cluster's index number
State	The cluster's current state
Conn-State	Connection status: <ul style="list-style-type: none">• Disconnected - XMS currently is disconnected from the cluster.• Connected - XMS is currently connected to the cluster.
Num-of-Vols	The total number of defined Volumes in the cluster
Num-of-Internal-Volumes	Number of internal Volumes
Vol-Size	The total amount of disk space defined for all Volumes in the cluster
UD-SSD-Space	The total physical space (i.e. SSD) available to the XtremIO Storage Array
Logical-Space-In-Use	The total logical address space written to the cluster before deduplication
UD-SSD-Space-in-Use	The physical (i.e. SSD) space currently in use after deduplication. This value may be lower than the Address-Space property if the deduplication ratio is greater than 1.
Total-Writes	The total bytes written to the cluster since installation
Total-Reads	The total bytes read by the cluster since installation
Stop-Reason	The reason for cluster halt (if any)
Size-and-Capacity	The cluster's capacity

show-clusters-info

The `show-clusters-info` command displays connected clusters information.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No
vertical	Vertical layout	N/A	No

Output Parameter	Description
Cluster-Name	The cluster's name
Index	The cluster's index number
State	The cluster's current state
Conn-State	Connection status: <ul style="list-style-type: none"> Disconnected - XMS currently is disconnected from the cluster. Connected - XMS is currently connected to the cluster.
Activation-Time	Time stamp of cluster activation in DATE & TIME format, e.g. Tue Oct 8 11:12:42 2013
Start-Time	Time stamp of cluster start in DATE & TIME format, e.g. Tue Oct 8 11:12:42 2013
SW-Version	The software version of the cluster
PSNT	The cluster's Product Serial Number Tag (assigned by EMC)
Encryption-Mode	The cluster's encryption mode
Encryption-Supported	Indicates if the cluster is encryption supported.
Encryption-Mode-State	The cluster's encryption mode's state
Compression-Mode	The cluster's compression mode
SSH-Firewall-Mode	The cluster's SSH firewall mode
OS-Upgrade-Ongoing	Indicates if an OS upgrade process is ongoing.
Cluster-Expansion-In-Progress	Indicates if cluster expansion is in progress.
Upgrade-State	The cluster's upgrade status

modify-clusters-parameters

The `modify-clusters-parameters` command modifies various cluster parameters.

Input Parameter	Description	Value	Mandatory*
cluster-id	The cluster's ID	Name or Index	No
debug-create-timeout	Debug info creation timeout	'high', 'none', 'normal'	One from Group 1
iscsi-tcp-port	iSCSI TCP Port	Integer	One from Group 1
obfuscate-debug	Obfuscate debug info	'enabled', 'disabled'	One from Group 1
odx-mode	ODX mode	'enabled', 'disabled'	One from Group 1

*)Group1:[‘debug-create-timeout’, ‘iscsi-tcp-port’, ‘obfuscate-debug’, ‘odx-mode’]

show-clusters-savings

The `show-clusters-savings` command displays savings parameters of the selected cluster.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Cluster-Name	The cluster's name
Index	The cluster's index number
Data-Reduction-Ratio	The cluster's data reduction ratio (calculated using the data deduplication and data compression)
Thin-Provisioning-Ratio	The cluster's thin provisioning ratio (used disk space compared to allocated disk space)
Dedup-Ratio	The cluster's deduplication ratio (calculated data written to the array compared to unique data on SSD)
Compression-Factor	The cluster's compression factor (calculated using the unique data on the SSD compared to the physical capacity used)

show-clusters-upgrade

The `show-clusters-upgrade` command displays clusters' software upgrade status.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Cluster-Name	The cluster's name
Index	The cluster's index number
State	The cluster's state
Upgrade-State	The cluster's upgrade state
Start-Time	A time stamp indicating the cluster's upgrade starting point
Activation-Time	A time stamp indicating when the current software was activated
Storage-Controller-Name	The Storage Controller's name
Index	The Storage Controller's index number
Mgr-Addr	The management IP address of the Storage Controller
SW-Version	The Storage Controller's software version
SW-Build	The software build number
OS-Version	The OS version
FW-State	The firmware's state
Upgrade-Failures	Indicates if upgrade failed.

show-clusters-upgrade-progress

The `show-clusters-upgrade-progress` command displays indicators of the clusters' software upgrade progress.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Storage-Controller-Name	The Storage Controller's name
Index	The Storage Controller's index number
Cluster-Name	The cluster's name
Index	The cluster's index number
Step-Number	The current upgrade step number
Step-Information	Current upgrade step information

show-cluster-expansion-progress

The `show-cluster-expansion-progress` command displays indicators of the cluster expansion process progress.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
data-migration	Show data migration information	N/A	No
duration	Monitor duration	seconds	No
frequency	Monitor intervals	seconds	No

show-xms

The `show-xms` command displays the XtremIO management System information.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The Management cluster's name
Index	The Management cluster's index number
Xms-IP-Addr	The IP address of the XMS
Xms-Mgmt-Ifc	The interface name for the XMS IP management
REST-API-Protocol-Version	Version number of the REST API protocol
IP-Version	IP version (IPV4, IPV6)
Default-User-Inactivity-Timeout	Default user inactivity timeout

show-xms-info

The `show-xms-info` command displays information on server statistics, disk usage and Ethernet interfaces.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Server Statistics

Output Parameter	Description
Name	The Management server's name
Index	The Management server's index number
Avg-CPU	Average CPU usage
Total-RAM	Total RAM capacity
Used-RAM	Used RAM capacity
Curr-Logs-Size	Current size of logs
Uptime	Time measured since XMS was down

Disk Usage

Output Parameter	Description
Name	Disk name
Index	Disk index number
1k-Blocks	Number of 1k blocks on disk
Available	The available space on the disk
Used	The used space on the disk

Ethernet Interfaces

Output Parameter	Description
Name	Interface name
Index	Interface index number
IP	Interface IP address
MAC-Address	Interface MAC address
State	Interface state (up, down)
Received-Bytes	Number of received bytes
Received-Packets	Number of received packets
Sent-Bytes	Number of sent bytes
Sent-Packets	Number of sent packets
Dropped-Packets	Number of dropped packets

shutdown-xms

The `shutdown-xms` command stops the XMS service or shuts down the XtremIO Management System.

Input Parameter	Description	Value	Mandatory
shutdown-type	Shutdown type	service (default), machine	No

restart-xms

The `restart-xms` command restarts the XtremIO Management System.

Input Parameter	Description	Value	Mandatory
restart-type	Restart type	service (default), machine	No

modify-xms-parameters

The `show-xms-parameters` command modifies the XMS's user inactivity timeout.

Input Parameter	Description	Value	Mandatory
default-user-inactivity-timeout	User Inactivity Timeout in minutes	Integer	Yes

show-ip-addresses

The `show-ip-addresses` command displays the XMS networking configuration, including IP addresses, network mask and default GW.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Input Parameter	Description
Name	XMS name
Index	XMS index
Xms-IP-Addr	XMS IP address
Xms-GW-Addr	XMS Gateway address
Storage-Controller-Name	Storage Controller name
Index	Storage Controller index
Cluster-Name	Cluster Name
Index	Cluster index
Mgr-Addr-Subnet	Management Storage Controller address subnet mask
MGMT-GW-IP	Management Storage Controller Gateway IP address

modify-ip-addresses

The `modify-ip-addresses` command modifies the XMS networking configuration, including IP addresses, network mask and default GW.

Input Parameter	Description	Value	Mandatory*
cluster-id	Cluster ID	Name or Index	No
rollback	Rollback changes in case of failure	N/A	No
sc-gw-addr	Storage Controller's management network gateway address	IP address	One from Group 1
sc-ip-list	Storage Controllers' IP list	[sc-id=value sc-ip-sn=value ipmi-ip-sn=value,...]	One from Group 1
xms-gw-addr	XMS gateway address	IP address	One from Group 1
xms-ip-sn	XMS IP/Subnet	IP address/Subnet	One from Group 1

*)Group1:[‘sc-gw-addr’, ‘sc-ip-list’, ‘xms-gw-addr’, ‘xms-ip-sn’]

modify-eth-port

The `modify-eth-port` command modifies the Ethernet port of the cluster.

Input Parameter	Description	Value	Mandatory*
cluster-id	Cluster ID	Name or Index	No
mgmt-port-autoneg-mode	Ethernet port Auto-negotiation mode	enabled, disabled	One from Group 1
mgmt-port-duplex	Ethernet port duplex	full, half	One from Group 1
mgmt-port-speed	Ethernet port speed	100MB, 1GB	One from Group 1

*)Group1:[‘mgmt-port-autoneg-mode’, ‘mgmt-port-duplex’, ‘mgmt-port-speed’]

create-ip-link

The `create-ip-link` command establishes an IP link to a remote cluster.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
ip-link-name	IP Link name	String	Yes
ip-link-pairing-label	IP Link pairing label	String	Yes
protocol	Protocol	Protocol	Yes
remote-cluster-id	Remote cluster ID	Name or Index	Yes
remote-domain	Remote domain	IP or DNS address remote domain	Yes
remote-ip-addr	Remote IP address	IP address/subnet bits	Yes
sc-id	Storage Controller ID	Name or Index	
target-id	Target ID	Name or Index	Yes

remove-ip-link

The `remove-ip-link` command removes an IP link to a remote cluster.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
ip-link-id	IP Link ID	Name or Index	Yes

modify-ssh-firewall

The `modify-ssh-firewall` command modifies the lock mode of the SSH firewall.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
ssh-firewall-mode	SSH firewall mode	locked, unlocked	Yes

test-ip-connectivity

The `test-ip-connectivity` command performs a connectivity test to a specified IP address.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
interface	Interface	ISCSI1, ISCSI2, sc_management	Yes
ip-addr	IP address to test connectivity to	IP address	Yes
sc-id	Storage Controllers' ID source	Name or index	Yes

show-storage-controllers-infiniband-ports

The `show-storage-controllers-infiniband-ports` command displays Storage Controllers' InfiniBand port information.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	Port's name
Index	Index number in the cluster
Port-Index	Port's index number
Peer-Type	Connected device type
Port-In-Peer-Index	Index of port in connected device
Link-Rate-In-Gbps	Link rate in Giga bit per second
Port-State	The port's state: up or down
Storage-Controller-Name	Storage Controller's name
Index	Storage Controller's index number
Brick-Name	X-Brick's name
Index	X-Brick's index number
Cluster-Name	Cluster's name
Index	Cluster's index number
Health-Level	Port's health level

show-storage-controllers-infiniband-counters

The `show-storage-controllers-infiniband-counters` command displays Storage Controllers' InfiniBand different counters.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Storage-Controller-Name	The Storage Controller's name
Index	The Storage Controller's index
Port-Index	The port's index number
Symb-Errs	These properties indicate standard diagnostic counters for InfiniBand ports.
Symb-Errs-pm	
Symb-Errs-pl	
Recovers	
Recovers-pm	
Recovers-pl	
Lnk-Downed	
Lnk-Downed-pm	
Lnk-Downed-pl	
Rcv-Errs	
Rcv-Errs-pm	
Rcv-Errs-pl	
Rmt-Phys-Errs	
Rmt-Phys-Errs-pm	
Rmt-Phys-Errs-pl	
Integ-Errs	
Integ-Errs-pm	
Integ-Errs-pl	
Link-Rate-In-Gbps	The link rate in Gbps

show-infiniband-switches-ports

The `show-infiniband-switches-ports` command displays InfiniBand Switches' port information.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Port-Index	The port number on the switch
Peer-Type	Connected device type (Storage Controller or InfiniBand Switch)
Port-In-Peer-Index	Index of port in connected device
Link-Rate-In Gbps	Link rate in Giga bit per second (usually 40Gbps)
Port-State	The port's state: up or down
IBSwitch-Name	The InfiniBand Switch's name
IBSwitch-Index	The InfiniBand Switch's index number
Cluster-Name	The cluster's name
Index	The cluster's index number

show-infiniband-switches

The `show-infiniband-switches` command displays InfiniBand Switches' information.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The InfiniBand Switch's name
Index	The InfiniBand Switch's index number
Index-in-Cluster	The port number in the InfiniBand Switch
Serial-Number	The InfiniBand Switch's serial number
Part-Number	A string identifier of the part (assigned by EMC)
State	The InfiniBand Switch's current functional status
FW-Version	Firmware version
FW-Version-Error	Indicates if there is an error in the InfiniBand Switch's FW version.
FAN-Drawer-State	The status of the FAN drawer

show-infiniband-switches-psus

The `show-infiniband-switches-psus` command displays InfiniBand Switches' PSUs information.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The PSU's name
Index	The PSU's index number
Cluster-Name	The cluster's name
Index	The cluster's serial number
Index-In-Cluster	The PSU number in the InfiniBand Switch
Location	The PSU's physical location (right or left)
Input-Power	Indicates whether input power is on or off
State	PSU's health state

show-daes-controllers

The `show-daes-controllers` command displays a list of DAE controllers (LCCs) and their properties.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The DAE Controller's name
Index	The DAE Controller's index number
Model	The DAE Controller's model
Serial-Number	The DAE Controller's serial number
State	The field replaceable unit state (healthy, disconnected, failed, or initializing)
Enabled-State	Indicates if DAE Controller is enabled.
HW-Revision	The DAE Controller's hardware revision number
index-in-DAE	The controller's index in relation to the DAE
Location	The DAE Controller's physical location (bottom or up)
FW-Version	The DAE Controller's firmware version
Part-Number	A string identifier of the part (assigned by EMC)
DAE-Name	The DAE's name
DAE-Index	The DAE's index number
Brick-Name	The X-Brick's name
Index	The X-Brick's index number
Cluster-Name	The cluster's name
Index	The cluster's index number

show-daes-psus

The `show-daes-psus` command displays a list of DAE power supply units (PSUs) and their properties.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The PSU's name
Index	The PSU's index number
Serial-Number	The PSU's serial number
Location-Index	The PSU's index in relation to the Storage Controller
Power-Feed	The PSU's power feed (A or B)
State	The field replaceable unit state (healthy, disconnected, failed, or initializing)
Input	Indicates if there is input power to the supply (on or off).
Location	The PSU's physical location in the DAE
HW-Revision	The PSU's hardware revision
Part-Number	A string identifier of the part (assigned by EMC)
DAE-Name	The DAE's name
DAE-Index	The DAE's Index number
Brick-Name	The X-Brick's name
Index	The X-Brick's index number
Cluster-Name	The cluster's name
Index	The cluster's index number

show-daes

The `show-daes` command displays the cluster's DAE information.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The DAE's name
Index	The DAE's index number
Model	The DAE's model
Serial-Number	The DAE's serial number
State	The field replaceable unit state (healthy, disconnected, failed, or initializing)
FW-Version	The DAE's firmware version
Part-Number	A string identifier of the part (assigned by EMC)
Brick-Name	The X-Brick's name
Index	The X-Brick's index number
Cluster-Name	The cluster's name
Index	The cluster's index number
HW-Revision	The DAE's hardware revision number

add-ldap-config

The `add-ldap-config` command adds a new LDAP configuration profile to the LDAP configuration table.

Input Parameter	Description	Value	Mandatory
binddn	Bind DN	CN=<value>,OU=<value>,DC=<value>,DC=<value>	Yes
bindpw	Bind Password	Password	Yes
ca-cert-data	X509 server certificate	String	No
cache-expire	Credential Expiration	Credentials cache expiration (default: 24 hours)	No
roles	Role to DN Mapping List	["admin:CN=SuperUsers,DC=example,DC=com", "read_only:CN=Users,DC=example,DC=com"]	Yes
search-base	Search Base	OU=<value>,DC=<value>,DC=<value>	No
search-filter	Search Filter	sAMAccountName={username}	No
server-urls	Server URLs	["ldap://ad.example.com"]	Yes
timeout	Connection Timeout	Integer (default: 1500 seconds)	No
user-to-dn-rule	User to DN substitution	{username}@example.com	No

modify-ldap-config

The `modify-ldap-config` command modifies an LDAP configuration profile.

Input Parameter	Description	Value	Mandatory
binddn	Bind DN	CN=<value>,OU=<value>,DC=<value>,DC=<value>	No
bindpw	Bind Password	Password	No
ca-cert-data	X509 server certificate	String	No
cache-expire	Credential Expiration	Credentials cache expiration (default: 24 hours)	No
ldap-config-id	LDAP configuration ID	Index	Yes
roles	Role to DN Mapping List	["admin:CN=SuperUsers,DC=example,DC=com","read_only:CN=Users,DC=exmaple,DC=com"]	No
search-base	Search Base	OU=<value>,DC=<value>,DC=<value>	No
search-filter	Search Filter	sAMAccountName={username}	No
server-urls	Server URLs	["ldap://ad.exmaple.com"]	No
timeout	Connection Timeout	Integer (default: 1500 seconds)	No
user-to-dn-rule	User to DN substitution	{username}@example.com	No

remove-ldap-config

The `remove-ldap-config` command removes an LDAP configuration profile from the LDAP configuration table.

Input Parameter	Description	Value	Mandatory
ldap-config-id	LDAP configuration profile ID	index	Yes

show-ldap-configs

The `show-ldap-configs` command displays the LDAP server configuration parameters.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Index	The number of entry in the LDAP configuration table
Bind-DN	A distinguished name for querying groups and performing searches on behalf of other users
Search-Base	The starting point for the search in the directory tree. Comprises of multiple objects separated by commas, including: <ul style="list-style-type: none"> • cn: common name • ou: organizational unit • o: organization • c: country
Search-Filter	Determines what entries are returned, following a search. For example: <ul style="list-style-type: none"> • sAMAccountName={sam} • sAMAccountName={username}
LDAP-Servers	The field replaceable unit state (healthy, disconnected, failed, or initializing)
User-to-DN-Rule	A mapping of the user input to the search criteria
Role-Mapping	A list of XMS roles - Active Directory group mapping roles
Timeout	The time in seconds before switching to the secondary server or failing the request, in case no answer is received from the server
Credentials-Expiration	The time in hours (1 to 24) before the cached user authentication expires and re-authentication is required
CA-Cert-File	Certificate file for server validation (when LDAPS protocol is used)

show-syslog-notifier

The `show-syslog-notifier` command displays the Syslog server notification status.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Enabled	Indicates if the Syslog server notification option is enabled or disabled.
Targets	Displays the list of Syslog Targets with optional port.

show-server-name

The `show-server-name` command displays the server name, according to the name configuration mode, as follows:

- ◆ Fixed mode - the server name is manually set by the user (using [modify-server-name](#)).
- ◆ DNS mode - the server name is drawn from reverse DNS lookup (enabled, using [modify-server-name](#)).
- ◆ Dynamic mode - the server name is set according to the user's URL request.

show-remote-servers-status

The `show-remote-servers-status` command displays NTP, DNS, gateway servers information.

Output Parameter	Description
Server-Type	The server's type (DNS, Gateway)
Server-IP	The server's IP address
Server-Status	The server's status (reachable/unreachable)

show-timezones

The `show-timezones` command displays the timezones list.

show-datetime

The `show-datetime` command displays time-related information.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Mode	Either manual (when no NTP servers are defined) or automatic (when one or more NTP servers are defined)
NTP-Servers	Displays the list of defined NTP Servers.
Cluster-Time	The cluster's set date and time
Cluster-Time-Zone	Time zone in which the cluster is located
UTC-Offset	The offset from Greenwich time (in Hours)
DST	Indicates if Daylight Saving Time is applied.

modify-datetime

The `modify-datetime` command sets or modifies the cluster's date and time, timezone, or NTP server parameters. The command's input parameters must include at least one of these parameters.

Input Parameter	Description	Value	Mandatory*
datetime	Datetime	Datetime string, e.g. 2013-12-20 17:46:24	One from Group 1
ntp-servers	NTP server list	List of NTP servers	One from Group 1
timezone	Time zone	Time zone, e.g. US/Pacific	One from Group 1

*) Group 1:[‘datetime’, ‘ntp-server’, ‘timezone’]

show-dns-servers

The `show-dns-servers` command displays the IP addresses of the primary and secondary DNS servers (if configured).

Output Parameter	Description
Primary	Primary DNS server IP Address
Secondary	Secondary DNS server IP Address

modify-dns-servers

The `modify-dns-servers` command sets or modifies the IP address of the primary DNS server (mandatory input) and/or the secondary DNS server (optional input).

Input Parameter	Description	Value	Mandatory*
primary	Primary IP Address	IP Address	One from Group 1
secondary	Secondary IP Address	IP Address	One from Group 1

*Group1) ['primary', 'secondary']

modify-server-name

The `modify-server-name` command defines or modifies the XMS's URL. The user can also enable/disable reverse DNS lookup to retrieve the URL, based on the XMS's IP address.

Input Parameter	Description	Value	Mandatory*
enable-reverse-dns	Indicates if to enable reverse DNS lookup.	N/A	One from Group 1
enable-user-url	Server redirects based on user URL	N/A	
server-name	Server name	E.g. xms.example.com	One from Group 1

*Group1) ['enable-reverse-dns', 'server-name']

modify-syslog-notifier

The `modify-syslog-notifier` command sets or modifies the Syslog notifier list. There can be up to 6 Syslog notifiers.

Input Parameter	Description	Value	Mandatory*
disable	Disable	N/A	One from Group 1
enable	Enable	N/A	One from Group 1
targets	Target list	List of Syslog Targets with optional port (required when enabling)	No

*Group1) ['disable', 'enable']

modify-login-banner

The `modify-login-banner` command enables to customize the login banner text.

Input Parameter	Description	Value	Mandatory
banner	CLI/GUI banner	ascii string	Yes

modify-webui

The `modify-webui` command enables or disables XtremIO WebUI technology preview mode.

Input Parameter	Description	Value	Mandatory*
disable	Disable	N/A	One from Group 1
enable	Enable	N/A	One from Group 1

show-report

The `show-report` command displays the details of a specified report.

Input Parameter	Description	Value	Mandatory
report-id	Report ID	Name or Index	Yes

Output Parameter	Description
Name	Report's name
Index	Reports Index number
Title	Report's title
Entity	Report's entity subject
Category	Report's category
Object-List	Object list referred to in the report
Property-List	Properties displayed in the report
Source-Definition	The report's source
View-Type	The report's view type
Public	Indicates if report is public.

show-reports

The `show-reports` command displays a list of defined reports.

Input Parameter	Description	Value	Mandatory
report-id	Report ID	Name or Index	Yes

Output Parameter	Description
Name	Report's name
Index	Reports Index number
Title	Report's title
Entity	Report's entity subject
Category	Report's category
Granularity	Reporting granularity
From-Time	Time of report start
To-Time	Time of report end
Time-Frame	Report's time frame
Source-Definition	Report's source
Public	Indicates if report is public

show-reports-data

The `show-reports-data` command displays a report's data for a specified entity and category.

Input Parameter	Description	Value	Mandatory
category	Report category	String	Yes
cluster-id	Cluster ID	Name or Index	No
entity	Class	String	Yes
export-to-file	File name	String	No
from-time	From Date/Time	date/time format (e.g. "2015-05-2310:14:15")	No
granularity	Data granularity	text string.auto for best match	No
obj-list	Object ID list	List of ids: Name or Index	No
time-frame	Time frame for monitoring	Text string to use without from/to	No
to-time	To Date/Time	date/time format ((e.g. "2015-05-2310:14:15"))	No
vertical	Vertical layout	N/A	No

Basic Cluster Management CLI Commands

add-cluster

The `add-cluster` command adds a cluster to the existing cluster configuration.

Input Parameter	Description	Value	Mandatory
force	Force add	N/A	No
sc-mgr-host	Storage Controller IP address or host name	Host Name	Yes

remove-cluster

The `remove-cluster` command removes a cluster from the existing cluster configuration.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	Yes

start-cluster

The `start-cluster` command starts a stopped cluster and enables it to respond to host I/Os and process data.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster's ID	Name or index	No
force	Force stop	N/A	No

stop-cluster

The `stop-cluster` command stops an active cluster (active x-envs only) and disables data processing in an orderly manner.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster's ID	Name or index	No

Note: Do not use this command unless specifically instructed to do so by EMC Global Tech Support.

power-off

The `power-off` command powers off a Storage Controller or an entire cluster.

Powering off a Storage Controller disconnects all connected hosts from the paths to this controller. However, power-cycling entire cluster causes the entire cluster not to respond to host I/O requests. The Storage Controller must be deactivated before this command can run.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
sc-id	Storage Controller's ID	Name or index	No

▲CAUTION

Unless otherwise requested by EMC Global Tech Support, this command should not be used to shut down the Cluster. For instructions on shutting down the cluster, refer to [“Shutting Down the Cluster - Planned Shutdown” on page 329](#).

power-on

The `power-on` command powers up a Storage Controller.

Powering on a Storage Controller connects all hosts to this controller. Powering on the entire cluster causes the entire cluster to respond to host I/O requests.

Input Parameter	Description	Value	Mandatory
sc-id	Storage Controller's ID	Name or index	Yes
cluster-id	Cluster's ID	Name or index	No

Volume Related CLI Commands

add-volume

The `add-volume` command creates and adds a new Volume.

Input Parameter	Description	Value	Mandatory
alignment-offset	Alignment offset according to block size	<ul style="list-style-type: none"> For 512 block size, offset range is 0-7. for 4096 block size, there is no offset. If omitted, offset is 0. 	No
cluster-id	Cluster ID	Name or index. Can be omitted if only one cluster is defined.	No
lb-size	Block size	512 (default) or 4096	No
small-io-alerts	Small I/O alerts	Enabled or Disabled	No
unaligned-io-alerts	Unaligned I/O alerts	Enabled or Disabled	No
vaaI-tp-alerts	VAAI TP Alerts	Enabled or Disabled	No
vol-name	Volume name	String (up to 128 characters)	Yes
vol-size	Volume size	Integer suffixed by [mgtpk]. e.g. vol-size="10t", creates a Volume of 10TB. Volume size must be in multiples of 8K.	Yes
tag-list	Tag ID list	List of IDs: Name or Index	No

remove-volume

The `remove-volume` command removes a Volume.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
vol-id	Volume ID	Name or index	Yes

modify-volume

The `modify-volume` command modifies a Volume's parameters.

Input Parameter	Description	Value	Mandatory*
cluster-id	Cluster ID	Name or Index	No
small-io-alerts	Small I/O alerts	Enabled or Disabled	One from Group1
unaligned-io-alerts	Unaligned I/O alerts	Enabled or Disabled	One from Group1
vaai-tp-alerts	VAAI TP alerts	Enabled or Disabled	One from Group1
vol-id	Volume ID	Name or index	Yes
vol-name	Volume name	String (up to 128 characters)	One from Group1
vol-size	Volume size	Integer suffixed by [mgtpk]. Volume size must be in multiples of 8K.	One from Group1

*)Group1: ['small-io-alerts', 'unaligned-io-alerts', 'vaai-tp-alerts', 'vol-name', 'vol-size']

clear-volume-reservation

The `clear-volume-reservation` command removes LUN reservations to release them for access.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
vol-id	Volume ID	Name or index	Yes

show-volume

The `show-volume` command displays the specified Volume's information.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No
vol-id	Volume's id	Name or index	Yes

Output Parameter	Description
Volume-Name	The Volume's name
Index	The Volume's index number
Vol-Size	The Volume's block size
LB-Size	The Volume's type
VSG-Space-In-Use	The total user data space written to the Volume Snapshot Group before deduplication and compression
Offset	The Volume's defined alignment offset
Ancestor-Name	The Volume that was the Snapshot source for this volume
Index	The ancestor's index number
VSG-Index	The Volume Snapshot Group's index
Cluster-Name	The name of the cluster to which the Volume belongs
Index	The cluster's index number
Small-IO-Alerts	Indicates whether small I/O alerts are enabled.
Unaligned-IO-Alerts	Indicates whether unaligned I/O alerts are enabled.
VAAI-TP-Alerts	Indicates whether VAAI TP alerts are enabled.
Total-Writes	The total number of write operations written to a Volume. A logical space before deduplication.
Total-Reads	The total number of reads on a Volume. A logical space before deduplication.
Created-By	The creator of the Volume (XMS, Scheduler)
Volume-Type	The Volume type (regular, read-only)
NAA-Identifier	The SCSI Network Address Authority (NAA) identifier for the Volume, as exposed to the Initiators
Certainty-State	Indicates if there is a pending command associated with the Volume.
Tags	The list of Tags assigned to the Volume

show-volumes

The `show-volumes` command displays a list of Volumes and related information.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No
sg-id	Snapshot Group ID	Name or Index	No
tag-list	Tag ID list	List of IDs: Name or Index	No

Output Parameter	Description
Volume-Name	The Volume's name
Index	The Volume's index number
Vol-Size	The Volume's provisioned disk space
LB-Size	The Volume's type
VSG-Space-In-Use	The total user data space written to the Volume Snapshot Group before deduplication and compression
Offset	The Volume's defined alignment offset
Ancestor-Name	The Volume that was the Snapshot source for this Volume
Index	The ancestor's index number
VSG-Index	The Volume Snapshot Group index number
Cluster-Name	The name of the cluster to which the Volume belongs
Index	The cluster's index number
Small-IO-Alerts	Indicates whether small I/O alerts are enabled.
Unaligned-IO-Alerts	Indicates whether unaligned I/O alerts are enabled.
VAAI-TP-Alerts	Indicates whether VAAI TP alerts are enabled.
Total-Writes	The total number of write operations written to a Volume. A logical space before deduplication.
Total-Reads	The total number of reads on a Volume. A logical space before deduplication.
NAA-Identifier	The SCSI Network Address Authority (NAA) identifier for the Volume
Certainty-State	Indicates if there is a pending command associated with the Volume.

Output Parameter	Description
Created-By	The creator of the Volume (XMS, Scheduler)
Volume-Type	The Volume type (regular, read-only)
Created	The date and time of the snapshot creation

show-volume-snapshot-groups

The `show-volume-snapshot-groups` command displays a list of Volumes with their associated Snapshots and their parameters.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Index	The VSG index number
Num-of-Vols	The number of Volumes in the VSG
Num-of-Internal-Volumes	The number of Volumes created by external application for internal usage.
Vol-Size	The amount of disk space allocated for the Volume
Thin-Provisioning-Ratio	The ratio of thin provisioning in the Snapshot group
Logical-Space-In-Use	The amount of logical disk space in the Volume
Reached-Max-Snapshots	Indicates if the maximum number of Snapshots allowed for the Snapshot group has been reached (including the deleted Snapshots that still consume resources).
Removing-Snapshots-In-Progress	Indicates if Snapshots are currently being deleted or merged (i.e. more Snapshots can be created soon).

create-snapshot

The `create-snapshot` command creates a Snapshot from a specified Volume.

Input Parameter	Description	Value	Mandatory*
cluster-id	Cluster ID	Name or Index	No
consistency-group-id	Consistency Group ID	Name or Index	One from Group 1
snap-suffix	Snapshot name suffix	String	No
snapshot-set-id	Snapshot Set ID	Name or Index	One from Group 1
snapshot-set-name	Snapshot Set name	String	No
snapshot-type	Snapshot type	'regular' or 'readonly'	No
tag-list	Tag ID list	List of IDs: Name or Index	One from Group 1
volume-list	Volume list	List of IDs: Name or Index	One from Group 1

*)Group 1: ['consistency-group-id', 'snapshot-set-id', 'tag-list', 'volume-list']

create-snapshot-and-reassign

The `create-snapshot-and-reassign` command creates a Snapshot from a specified Volume/Snapshot, Consistency Group, or Snapshot sets and reassigns the Volume identity characteristic to the created Snapshot.

Input Parameter	Description	Value	Mandatory*
backup-snap-suffix	Snapshot name suffix	String	No
backup-snapshot-type	Snapshot type	'readonly', 'regular'	No
cluster-id	Cluster ID	Name or Index	No
from-consistency-group-id	ID of the Consistency Group being snapped	Name or Index	One from Group1
from-snapshot-set-id	ID of the Snapshot Set being snapped	Name or Index	One from Group1
from-volume-id	ID of the Volume being snapped	Name or Index	One from Group1
no-backup	Remove source object	N/A	No
snapshot-set-name	Created Snapshot Set name	String	No
to-consistency-group-id	ID of the target Consistency Group	Name or Index	One from Group2
to-snapshot-set-id	ID of the target Snapshot Set	Name or Index	One from Group2
to-volume-id	ID of the target Volume	Name or Index	One from Group2

*)Group1: ['from-consistency-group-id', 'from-snapshot-set-id', 'from-volume-id']

*)Group2: ['to-consistency-group-id', 'to-snapshot-set-id', 'to-volume-id']

create-scheduler

The `create-scheduler` command creates a new Snapshot scheduler. Refer to [“Scheduler Type and Time Parameters” on page 263](#) for details on the `scheduler-type` and `time` parameters.

Input Parameter	Description	Value	Mandatory*
<code>cluster-id</code>	Cluster ID	Name or Index	No
<code>scheduler-type</code>	Scheduler type	Interval or Explicit	Yes
<code>snapshot-object-id</code>	Snapped object ID	Name or Index	Yes
<code>snapshot-object-type</code>	Class	String	Yes
<code>snapshot-type</code>	Snapshot type	String	No
<code>snapshots-to-keep-number</code>	Number of Snapshots to keep	Integer	One from Group 1
<code>snapshots-to-keep-time</code>	Timeframe for keeping Snapshots	Integer with [dmy] suffix	One from Group 1
<code>suffix</code>	Snapshot name suffix	String	No
<code>time</code>	Time	String in x:y:z format	Yes

*)Group1: ['snapshots-to-keep-number', 'snapshots-to-keep-time']

show-schedulers

The `show-schedulers` command displays the defined schedulers parameters.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameters	Description
Name	The scheduler's name
Index	The scheduler's index number
Snapped-Object-Id	The ID of the snapped object
Snapped-Object-Type	The type of the snapped object
Suffix	The created Snapshots assigned suffix
Cluster-Time-Zone	The cluster time zone
Snapshot-History-to-Keep-by-Time	The time frame in which to keep Snapshots
Number-Of-Snapshots-To-Keep	The maximum number of Snapshots to keep
Scheduler-Type	The scheduler type (Interval or Explicit)
Schedule	The set schedule
Enabled-State	The scheduler's state
Last-Activation-Time	The scheduler's last activation time
Last-Activation-State	The scheduler's last activation state

modify-scheduler

The `modify-scheduler` command modifies a Snapshot scheduler's parameters. Refer to “[Scheduler Type and Time Parameters](#)” on page 263 for details on the `scheduler-type` and `time` parameters.

Input Parameter	Description	Value	Mandatory
<code>cluster-id</code>	Cluster ID	Name or Index	No
<code>scheduler-id</code>	Scheduler ID	Name or index	Yes
<code>scheduler-type</code>	Scheduler type	Interval or Explicit	No
<code>snapshot-object-id</code>	Snapped object ID	Name or Index	No
<code>snapshot-object-type</code>	Class	String	No
<code>snapshot-type</code>	Snapshot type	String	No
<code>snapshots-to-keep-number</code>	Number of Snapshots to keep	Integer	No
<code>snapshots-to-keep-time</code>	Time frame for keeping Snapshots	Integer with [hdy] suffix	No
<code>suffix</code>	Snapshot name suffix	String	No
<code>time</code>	Time	String in x:y:z format	No

remove-scheduler

The `remove-scheduler` command deletes a Snapshot scheduler.

Input Parameter	Description	Value	Mandatory
<code>cluster-id</code>	Cluster ID	Name or Index	No
<code>scheduler-id</code>	Scheduler ID	Name or index	Yes

resume-scheduler

The `resume-scheduler` reactivates a suspended Snapshot scheduler.

Input Parameter	Description	Value	Mandatory
<code>cluster-id</code>	Cluster ID	Name or Index	No
<code>scheduler-id</code>	Scheduler ID	Name or index	Yes

suspend-scheduler

The `suspend-scheduler` suspends an active Snapshot scheduler.

Input Parameter	Description	Value	Mandatory
<code>cluster-id</code>	Cluster ID	Name or Index	No
<code>scheduler-id</code>	Scheduler ID	Name or index	Yes

show-snapshots

The `show-snapshots` command displays a list of Snapshots and related information.

Input Parameter	Description	Value	Mandatory
ancestor-vol-id	Ancestor Volume ID	Name or Index	Yes
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No
sg-id	Snapshot Group ID	Name or Index	
tag-list	Tag ID list	List of IDs: Name or Index	No

Output Parameters	Description
Volume-Name	The Volume's name
Index	The Volume's index number
Vol-Size	The Volume's provisioned disk space
LB-Size	The Volume's type
VSG-Space-In-Use	The total user data space written to the Volume Snapshot Group before deduplication and compression
Offset	The Volume's defined alignment offset
Ancestor-Name	The Volume that was the Snapshot source for this Volume
Index	The ancestor's index number
VSG-Index	The Volume Snapshot Group index number
Cluster-Name	The name of the cluster to which the Volume belongs
Index	The cluster's index number
Parent-Folder-Name	The full path name of the folder containing this Volume
Index	The index of the volume folder containing this Volume
Small-IO-Alerts	'disabled', 'enabled'
Unaligned-IO-Alerts	'disabled', 'enabled'
VAAI-TP-Alerts	'disabled', 'enabled'
Total-Writes	The total amount of write actions
Total-Reads	The total amount of read actions
NAA-Identifier	The SCSI Network Address Authority (NAA) identifier for the Snapshot
Certainty-State	Indicates if there is a pending command associated with the Initiator.

Output Parameters	Description
Created-By	The creator of the Snapshot (XMS, Scheduler)
Snapshot-Type	The Snapshot type (regular, read-only)
Created	The date and time on which the Snapshot was created

show-snapshot-sets

The `show-snapshot-sets` command displays a list of Snapshot sets and related information.

Input Parameter	Description	Value	Mandatory
cg-id	Consistency Group ID	Name or Index	No
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No
tag-list	Tag ID list	List of IDs: Name or Index	No

Output Parameters	Description
Name	The Snapshot Set's name
Index	The Snapshot Set's index number
Cluster-Name	The cluster's name
Index	The cluster's index number
Consistency-Group-Name	The Consistency Group's name
CG-ID	The Consistency Group's index number
Num-of-Vols	The number of snapped Volumes in the Snapshot Set
Creation-Time	The Snapshot Set's date and time of creation
Volume-List	The list of snapped Volumes in the Snapshot Set
Created-By	The owner entity of the Snapshot Set

show-snapshot-set

The `show-snapshot-set` command displays the parameters of a specified Snapshot Set.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No
ss-id	Snapshot Set ID	Name or Index	Yes

Output Parameters	Description
Name	The Snapshot Set's name
Index	The Snapshot Set's index number
Cluster-Name	The cluster's name
Index	The cluster's index number
Consistency-Group-Name	The Consistency Group's name
CG-ID	The Consistency Group's index number
Num-of-Vols	The number of snapped Volumes in the Snapshot Set
Creation-Time	The Snapshot Set's date and time of creation
Volume-List	The list of snapped Volumes in the Snapshot Set
Tags	The list of Tags assigned to the Snapshot Set

remove-snapshot-set

The `remove-snapshot-set` command deletes a Snapshot set.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
ss-id	Snapshot Set Index number	Name or Index	Yes

add-volume-to-consistency-group

The `remove-volume-from-consistency-group` command adds a Volume to a Consistency Group.

Input Parameter	Description	Value	Mandatory
cg-id	Consistency Group ID	Name or Index	Yes
cluster-id	Cluster ID	Name or Index	No
vol-id	Volume ID	Name or Index	Yes

remove-volume-from-consistency-group

The `remove-volume-from-consistency-group` command removes a Volume from a Consistency Group.

Input Parameter	Description	Value	Mandatory
cg-id	Consistency Group ID	Name or Index	Yes
cluster-id	Cluster ID	Name or Index	No
vol-id	Volume ID	Name or Index	Yes

create-consistency-group

The `create-consistency-group` command creates a new Consistency Group.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
consistency-group-name	Consistency Group name	String	No
tag-list	Tag ID list	List of ids: Name or Index	No
vol-list	Object ID list	List of ids: Name or Index	No

show-consistency-group

The `show-consistency-group` command displays the parameters of a specified Consistency Group.

Input Parameter	Description	Value	Mandatory
cg-id	Consistency Group ID	Name or Index	Yes
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameters	Description
Name	The Consistency Group's name
Index	The Consistency Group's index number
Cluster-Name	The cluster's name
Index	The cluster's index number
Volume-List	The Consistency Group's members list
Tags	The Consistency Group's associated Tags
Created-By	The consistency group creator
Certainty-State	Indicates if there is a pending command associated with the Consistency Group.

show-consistency-groups

The `show-consistency-groups` command displays the parameters of all defined Consistency Groups.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No
tag-list	Tag ID list	List of ids: Name or Index	No

Output Parameters	Description
Name	The Consistency Group's name
Index	The Consistency Group's index number
Cluster-Name	The cluster's name
Index	The cluster's index number
Num-of-Vols	The number of Volumes in the Consistency Group
Created-By	The Consistency Group creator
Certainty-State	Indicates if there is a pending command associated with the Consistency Group.

remove-consistency-group

The `remove-consistency-group` command deletes a Consistency Group.

Input Parameter	Description	Value	Mandatory
cg-id	Consistency Group ID	Name or Index	Yes
cluster-id	Cluster ID	Name or Index	No

modify-cluster-thresholds

The `modify-cluster-thresholds` modifies the properties for thin provisioning soft limits for connected clusters.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or index	No
vaaI-tp-limit	VAAI TP Limit	Range 0 - 100	Yes

show-clusters-thresholds

The `show-clusters-thresholds` command displays thin provisioning soft limits for connected clusters.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Cluster-Name	The cluster's name
Index	The cluster's index number
Thin-Provisioning-Soft-Limit	Percentage value of limit placed on storage space

Initiator Group Related CLI Commands

An Initiator Group (IG) is a set of Initiators that would probably translate to a host with multiple HBAs or a cluster of hosts.

Using Initiator groups makes it easier to group the operation of LUN masking on this entity.

add-initiator

The `add-initiator` command adds an Initiator and associates it with an existing Initiator Group.

Input Parameter	Description	Value	Mandatory
cluster-authentication-password	CHAP authentication cluster password	String	No
cluster-authentication-user-name	CHAP authentication cluster user name	String	No
cluster-discovery-password	CHAP discovery cluster password	String	No
cluster-discovery-user-name	CHAP discovery cluster user name	String	No
cluster-id	Cluster ID	Name or Index	No
ig-id	Initiator Group ID	name or index	Yes
initiator-authentication-password	CHAP authentication password	String	No
initiator-authentication-user-name	CHAP authentication user name	String	No
initiator-discovery-password	CHAP discovery password	String	No
initiator-discovery-user-name	CHAP discovery user name	String	No
initiator-name	Initiator name	String	No
operating-system	Operating system	linux, windows, esx, solaris, aix, hpx, other	No
port-address	Port address (iQNs or WWNs)	String	Yes

add-initiator-group

The `add-initiator-group` command adds an Initiator Group and its associated Initiators to the XtreamIO cluster.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
ig-name	Initiator Group name	String	No
initiator-list	List of associated Initiators (name and port number)	[initiator-name=value port-address=value,...] (port-address is the Initiator iQN or WWN)	No
tag-list	Tag ID list	List of IDs: Name or Index	No

modify-initiator

The `modify-initiator` command modifies the properties of an existing Initiator.

Input Parameter	Description	Value	Mandatory*
cluster-authentication-password	CHAP authentication cluster password	String	One from Group 1
cluster-authentication-user-name	CHAP authentication user name	String	One from Group 1
cluster-discovery-password	CHAP discovery password	String	One from Group 1
cluster-discovery-user-name	CHAP discovery user name	String	One from Group 1
cluster-id	Cluster ID	Name or Index	No
initiator-authentication-password	CHAP authentication password	String	One from Group 1
initiator-authentication-user-name	CHAP authentication user name	String	One from Group 1
initiator-discovery-password	CHAP discovery password	String	One from Group 1
initiator-discovery-user-name	CHAP discovery user name	String	One from Group 1
initiator-id	Initiator ID	Name or index	Yes
initiator-name	Initiator name	String	One from Group 1
port-address	Port address	String	One from Group 1
remove-cluster-authentication-credentials	Remove CHAP cluster authentication credentials.	N/A	One from Group 1

Input Parameter	Description	Value	Mandatory*
remove-cluster-discovery-credentials	Remove CHAP cluster discovery credentials.	N/A	One from Group 1
remove-initiator-authentication-credentials	Remove CHAP Initiator authentication credentials.	N/A	One from Group 1
remove-initiator-discovery-credentials	Remove CHAP Initiator discovery credentials.	N/A	One from Group 1

*)Group 1:

['cluster-authentication-password','cluster-authentication-user-name','cluster-discovery-password','cluster-discovery-user-name','initiator-authentication-password','initiator-authentication-user-name','initiator-discovery-password','initiator-discovery-user-name','initiator-name','port-address','remove-cluster-authentication-credentials','remove-cluster-discovery-credentials','remove-initiator-authentication-credentials','remove-initiator-discovery-credentials']

remove-initiator

The `remove-initiator` command deletes an Initiator.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
initiator-id	Initiator ID	Name or index	Yes

remove-initiator-group

The `remove-initiator-group` command deletes an Initiator Group.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or INdex	No
ig-id	Initiator Group ID	Name or index	Yes

show-initiators

The `show-initiators` command displays Initiators' data.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Initiator-Name	The Initiator's name
Index	The Initiator's index number
Port-Type	The Initiator's port type (iSCSI or FC)
Port-Address	The Initiator's port address (WWN or iQN)
IG-Name	The associated Initiator Group's name
Index	The associated Initiator Group's index number
Certainty-State	Indicates if there is a pending command associated with the Initiator.
Chap-Authentication-Initiator-User-name	CHAP authentication Initiator user name
Chap-Discovery-Initiator-User-Name	CHAP discovery Initiator user name
Chap-Authentication-Cluster-User-Name	CHAP authentication cluster user name
Chap-Discovery-Cluster-User-Name	CHAP discovery cluster user name

show-initiator-group

The `show-initiator-group` command displays information for a specific Initiator Group.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	id: Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No
ig-id	Initiator Group ID	Name or index	Yes

Output Parameter	Description
IG-Name	The Initiator Group's name
Index	The Initiator Group's index number
Num-of-Initiators	The number of Initiators in the Initiator Group
Num-of-Vols	The number of Volumes mapped to the Initiator Group
Certainty-State	Indicates if there is a pending command associated with the Initiator Group.
Tags	The Tags assigned to the Initiator Group (full path name and index)

show-initiator-groups

The `show-initiator-groups` command displays information for all Initiator Groups.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	id: Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No
tag-list	Tag ID list	List of ids: Name or Index	No

Output Parameter	Description
IG-Name	The Initiator Group's name
Index	The Initiator Group's index number
Num-of-Initiators	Number of Initiators in the group
Num-of-Vols	Number of Volumes mapped to the Initiator Group
Certainty-State	Indicates if there is a pending command associated with the Initiator Group.

show-targets

The `show-targets` command displays the cluster Targets' interfaces (iSCSI or FC ports).

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	id: Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The Target's name
Index	The Target's index number
Cluster Name	The relevant cluster's name
Index	The relevant cluster's index
Port-Type	The Target's port type (FC or iSCSI)
Port-Address	The Target's port address
Mac-Addr	The MAC (Ethernet) address of the iSCSI Target port
Port-Speed	The actual port's speed
Port-State	The port's state: up or down
Health-Level	Indicates result of port diagnostics performed on Target port.
Storage-Controller-Name	The name of the Storage Controller the Target is associated to
Index	The Storage Controller's index number
TG-Name	The name of the Target Group to which the Target belongs
Index	The Target Group's index number
MTU	Maximum transmission unit size
Jumbo-Frames	Indicates whether jumbo frames are enabled.
Certainty-State	Indicates if there is a pending command associated with the Target.

show-target-groups

The `show-target-groups` command displays a list of Target Groups.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	id: Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
TG-Name	The Target Group's name
Index	The Target Group's index number
Cluster-Name	The name of the cluster to which the Target Group is related
Index	The cluster's index number

show-discovered-initiators-connectivity

The `show-discovered-initiators-connectivity` command displays the Initiators-Targets connectivity map.

Input Parameter	Description	Value
target-details	Target details info	N/A

Output Parameter	Description
Port-type	Initiator's port type (iSCSI or FC)
Port-address	Initiator's port address
Num-of-conn-targets	Number of Targets the Initiator is connected to

show-initiators-connectivity

The `show-initiators-connectivity` command displays Initiators-port connectivity and the number of connected Targets.

Input Parameter	Description	Value	Mandatory
target-details	Target details info	N/A	No

Output Parameter	Description
Name	The Target's name
Index	The Target's index number
Port-Type	The Initiator's port type (iSCSI or FC)
Port-Address	The Initiator's port address
Num-Of-Conn-Targets	The number of Targets the Initiator is connected to

show-chap

The `show-chap` command displays the cluster's configured CHAP authentication and discovery modes.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Cluster-Name	The cluster's name
Index	The cluster's index
Chap-Discovery-Mode	The CHAP discovery mode (Disabled, Initiator, Initiator and Target)
Chap-Authentication-Mode	The CHAP authentication mode (Disabled, Initiator, Initiator and Target)

modify-chap

The `modify-chap` command modifies CHAP configuration parameters.

Input Parameter	Description	Value	Mandatory*
chap-authentication-mode	CHAP Authentication Mode	'Disabled', 'Initiator', 'Initiator and Target'	One from Group 1
chap-discovery-mode	CHAP Discovery Mode	'Disabled', 'Initiator', 'Initiator and Target'	One from Group 1
cluster-ID	Cluster Identification	Name or Index	No

*) Group 1: ['chap-authentication-mode', 'chap-discovery-mode']

LUN Mapping Related CLI Commands

map-lun

The `map-lun` command maps a Volume to an Initiator Group and assigns a Logical Unit Number (LUN) to it.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	id: Name or Index	No
ig-id	Initiator Group ID	Name or Index. If omitted, means "undefined initiators".	Yes
lun	The number of the logical unit as exposed to the host Initiator. Host/OS may place limits on the allowed maximum value.	Integer	No
tg-id	Target group ID	Name or ID	No
vol-id	Volume ID	Name or ID	Yes

show-lun-mappings

The `show-lun-mappings` command displays the LUN mapping information between Volumes and Initiators.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No
ig-id	Initiator Group ID	Name or Index	
vol-id	Volume ID	Name or Index	

Output Parameter	Description
Volume-Name	The mapped Volume's name
Index	The mapped Volume's index number
IG-Name	The mapped Initiator Group's name
Index	The mapped Initiator Group's index number
TG-Name	The mapped Target Group's name
Index	The mapped Target Group's index number
LUN	The LUN value
Mapping-Index	The mapping index number
Certainty-State	Indicates if there is a pending command associated with the object.

unmap-lun

The `unmap-lun` command removes a Volume's LUN mappings.

Input Parameter	Description	Value	Mandatory*
all	All mappings	N/A	One from Group 1
cluster-id	Cluster ID	id: Name or Index	No
ig-id	Initiator Group ID	Name or index. If omitted, it means 'undefined initiators'.	One from Group 1
tg-id	Target Group ID	Name or index	No
vol-id	Volume ID	Name or index	Yes

*) Group 1: ['all', 'ig-id']

Alert Related CLI Commands

acknowledge-alert

The `acknowledge-alert` command acknowledges an alert and removes it from the dashboard Active Alerts list. The alert remains in the Alert List window. Alerts with Clear Mode set to Acknowledge Required, remain in the Alert List until they are acknowledged.

Input Parameter	Description	Value	Mandatory
alert-id	Index number of the alert to acknowledge.	Name or index	Yes

modify-alert-definition

The `modify-alert-definition` command modifies alert definition properties for a specified alert type.

Input Parameter	Description	Value	Mandatory*
activity-mode	Monitor duration	'disabled', 'enabled'	One from Group 1
alert-type	Alert type	All defined alerts	Yes
clearance-mode	Clearance mode	'auto-clear', 'ack-required'	One from Group1
send-to-call-home	Send to Call-Home	Send SYR notification upon raise	One from Group1
severity	Severity level	'information', 'minor', 'major', 'critical'	One from Group1
threshold	Threshold value	Range 0 - 100	One from Group1

*)Group 1: ['activity-mode', 'clearance-mode', 'send-to-call-home', 'severity', 'threshold']

show-alerts

The `show-alerts` command displays a list of active alerts and their details.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Index	The alert's ID
Description	The alert's description
Severity	The alert's severity level (Information, Major, Critical, or Minor)
Raise-Time	The date and time on which the alert was raised
Entity	The cluster component to which the alert refers
Name	The component's name
Index	The component's index number
Alert-Type	The alert's type
State	The alert's status
Alert-Code	The alerts code number

show-alert-definitions

The `show-alert-definitions` command displays a list of pre-defined alerts and their definitions.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Alert-Type	The alert's type
Short-Description	The alert's description
Activity-Mode	Indicates if to issue an alert upon state change.
Clearance-Mode	The alert's clearance mode: <ul style="list-style-type: none">• Acknowledgment required• Auto clear
Severity	If no threshold is defined, it indicates the alert severity level.
Alert-Code	The alert's unique code
Send-To-Call-Home	Sends SYR notification when the alert is raised.
Use-Modified	Indicates that the alert definition was modified by the user.

Event Related CLI Commands

show-events

The `show-events` command displays cluster and XMS events. The input parameters are filters that limit the displayed output.

Input Parameter	Description	Value	Is Mandatory
category	Event category	'audit', 'state_change', 'hardware', 'activity', 'security', 'lifecycle', 'software'	No
cluster-id	Cluster ID	Name or Index	No
entity	Event's associated entity	String	No
entity-details	Entity ID	Name or index	No
free-text	Free text search	String	No
from-date-time	Date and time start point	date/time format: "2013-11-23", "2013-11-23 10:14:15", "2013-11-23 10:14:15.123"	No
from-event-id	Show events following this event id	Positive integer	No
limit	Maximum number of records to display that adhere to all the filter criteria	Integer	No
prop-list	Allows to show more or less properties than the default output parameters.	List of strings	No
severity	Severity level	Information, Major, Critical, Minor	No
to-date-time	Date and time end time	date/time format: "2013-11-23", "2013-11-23 10:14:15", "2013-11-23 10:14:15.123"	No
vertical	Displays the command output in a non-tabular format (vertical lines).	vertical (e.g. <code>show-events vertical</code>)	No

Output Parameter	Description
Event ID	Event Index number
Date/Time	Date and time of the event
Event Code	Event code

Output Parameter	Description
Related Alert Code	Related alert code
Category	Event category
Severity	Event severity level
Cluster ID	Cluster Index Number
Entity	The entity to which the event refers
Entity Details	Entity details
Description	Event description

show-event-details

The `show-event-details` command displays the details of the specified event.

Input Parameter	Description	Value	Mandatory
event-id	Event ID	Positive Integer	Yes
full-object	Full Object	N/A	No

Output Parameter	Description
Event-ID	Event ID as specified in the input
Date/Time	Date and time of the event
Event-Code	Event code
Category	Event category
Severity	Event severity level
Entity	The entity to which the event refers
Entity-Details	Entity details
Description	Event description
Related-Events	Events related to the detailed event
User	The name of the user that invoked the operation
User-Location	The location (IP address) of the user that invoked the operation
User-Type	The type of access the user used

show-event-handler-definitions

The `show-event-handler-definitions` command displays event handling rule definitions.

Output Parameter	Description
ID	Event's ID
Actions	Event's action (email, SNMP, log)
category	Event's category
Severity	Event's severity level (Information, Major, Critical, Minor)
Entity	Event's associated entity
Entity-Details	Entity's details
Related-Alert-Code	The related alert code

add-event-handler-definition

The `add-event-handler-definition` command adds a definition to an event handling rule.

Input Parameter	Description	Value	Mandatory
actions	Action list	List of actions: email, snmp.	Yes
category	Event category	'audit', 'state_change', 'hardware', 'activity', 'security', 'lifecycle', 'software'	Yes
entity	Entity	String	No
entity-details	Entity Id	Name or index	No
related-alert-code	Related alert code	Alert code number	No
severity	Severity level	'information', 'major', 'critical', 'minor'	No

remove-event-handler-definition

The `remove-event-handler-definition` command deletes event handling rule definitions.

Input Parameter	Description	Value	Mandatory
event-handler-id	Event handler definition ID	ID	Yes

modify-event-handler-definition

The `modify-event-handler-definition` command modifies the definition of event handling rules.

Input Parameter	Description	Value	Mandatory
actions	Action list	List of actions to perform: email, SNMP	Yes
category	Event category	'audit', 'state_change', 'hardware', 'activity', 'security', 'lifecycle', 'software'	No
entity	Entity	String	No
entity-details	Entity ID	Name or index	No
event-handler-id	Event handler definition ID	ID	Yes
related-alert-code	Related Alert Code	Alert code number	No
severity	Severity level	'information', 'major', 'critical', 'minor'	No

iSCSI Routing Related CLI Commands

add-iscsi-portal

The `add-iscsi-portal` maps a portal (a combination of an IP address, IP port, and optionally a VLAN) to a Target. This mapping enables the Target port to accept iSCSI traffic via the portal.

Note: iSCSI Targets cannot have the same subnet as the management network.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	id: Name or Index	No
ip-addr	Portal IP Address	IP Address/Subnet Bits	Yes
tar-id	Target ID	Name or index	Yes
vlan	VLAN ID	0 (no VLAN tag) to 4094	No

add-iscsi-route

The `add-iscsi-route` command adds and configures iSCSI route parameters.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster Index number	Name or Index	No
destination-network-and-mask	Destination network and mask	Destination network/mask	Yes
gateway	Gateway IP Address	IP Address	Yes
iscsi-route-name	iSCSI Route name	String	No

modify-iscsi-portal

The `modify-iscsi-portal` command modifies an iSCSI portal parameters.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster Index number	Name or Index	No
ip-addr	Portal IP address	IP address/subnet bits	One from Group 1
portal-id	Portal ID	Index	Yes
vlan	VLAN ID	Integer	One from Group 1

remove-iscsi-portal

The `remove-iscsi-portal` command deletes a portal mapping from a Target. The Target will no longer receive iSCSI traffic via the portal.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	id: Name or Index	No
ip-addr	Portal's IP Address	IP Address/Subnet Bits	Yes

remove-iscsi-route

The `remove-iscsi-route` command deletes an iSCSI routing configuration.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	id: Name or Index	No
iscsi-route-id	iSCSI route id	Name or index	Yes

show-iscsi-portals

The `show-iscsi-portals` command displays a list of iSCSI portals and their properties.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	id: Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Portal-Index	The Target portal index
Target-Name	The Target port name
Index	The port's index number
IP-Address	The portal's IP address
Port-Address	The port's address
VLAN	The port's virtual LAN
Certainty-State	Indicates if there is a pending command associated with the iSCSI portal.

show-iscsi-routes

The `show-iscsi-routes` command displays a list of iSCSI routes and their properties.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	id: Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The route's name
Index	The route's index number
Destination-Network-and-Mask	The route's destination subnet
Gateway	The route's gateway
Certainty-State	Indicates if there is a pending command associated with the iSCSI route.

show-iscsi-counters

The `show-iscsi-counters` command displays iSCSI counters information.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The iSCSI counter name
Index	The iSCSI counter index number
Cluster-Name	The cluster's name
Index	The cluster's index number
Port-Address	Port address
Num-PKTS-Rx	Number of packets received
Total-KB-Rx	Total packets received
Num-PKTS-Tx	Number of packets transmitted
Total-KB-Tx	Total packets transmitted
Num-Crc-Err	Number of detected CRC errors
Num-NO-Buff-Err	Number of detected No Buffer errors
Num-Tx-Err	Number of detected transmission errors

show-clusters-parameters

The `show-clusters-parameters` command displays connected clusters iSCSI TCP port numbers.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Cluster-Name	The cluster's name
Index	The cluster's index number
ODX-Mode	Indicates whether ODX (Microsoft's Offloaded Data Transfer) is enabled.
iSCSI-TCP--Port	The cluster's iSCSI listen TCP port number (default 3260)
Obfuscate-Debug-Info	Indicates whether log bundle obfuscates client sensitive information.
Debug-Info-Creation-Timeout	The timeout used for log bundle creation

User Account Management Related CLI Commands

add-user-account

The `add-user-account` command adds a new user account to XMS.

Input Parameter	Description	Value	Mandatory*
inactivity-timeout	Inactivity timeout in minutes	Integer	No
password	User Password	String	One from Group1
public-key	User public key	public key	One from Group1
role	User Role	admin/configuration/read-only	Yes
usr-name	User Name	String	Yes

*)Group 1: ['password', 'public-key']

modify-user-account

The `modify-user-account` command modifies the user-account parameters.

Input Parameter	Description	Value	Mandatory*
inactivity-timeout	Inactivity timeout in minutes	Integer	One from Group1
password	User password	String	One from Group1
public-key	User public key	String	One from Group1
role	User role	'read_only', 'admin', 'configuration', 'technician'	One from Group1
usr-id	User ID	Name or index	Yes
usr-name	User name	String	One from Group 1

*)Group 1: ['inactivity-timeout', 'password', 'public-key', 'role', 'usr-name']

modify-password

The `modify-password` command modifies the user's password. If the `usr-id` parameter is not provided, then the current user's password is modified.

Input Parameter	Description	Value	Mandatory
password	User password	String	No
usr-id	User ID	Name or index	No

remove-user-account

The `remove-user-account` command removes a user account.

If the account is currently active (i.e. a command is in progress), account removal may fail.

Only users with administrative roles can remove other user accounts. Users cannot remove their own accounts.

Input Parameter	Description	Value	Mandatory
usr-id	User ID	Name or index	Yes

show-user-accounts

The `show-user-accounts` command displays user accounts information.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The user's name
Index	The user's index number
Role	The user's permission level
External-Account	Indicates if the user was authenticated by an external server and is not defined locally.
Inactivity-Timeout	The number of minutes with no activity after which the user needs to re-login

Notification Related CLI Commands

show-email-notifier

The `show-email-notifier` command displays Email notification settings.

Output Parameter	Description
Enabled	The active status of the email notifier
Transport	Mail transport to user: <ul style="list-style-type: none"> • HTML • SMTP
Sender	Sender's email address
Recipients	List of email recipients
Proxy-Address	The proxy server's address for HTML mail
Proxy-Port	The proxy server's port for HTML mail
Proxy-User	The proxy server's user for HTML mail
Mail-Relay-Address	The mail relay server for SMTP mail
Mail-User	The user for SMTP mail delivery
Company-Name	The sender's company name
Contact-Details	The sender's contact details

modify-email-notifier

The `modify-email-notifier` command modifies the email notification settings.

Input Parameter	Description	Value	Mandatory
company-name	The company's name	Company name	No
contact-details	The contact details	Contact details	No
disable	Disables the mail notifier.	N/A	No
enable	Enables the mail notifier.	N/A	No
mail-password	A password for SMTP mail relay	Password for SMTP mail relay	No
mail-relay-address	IP or DNS for SMTP mail relay	IP or DNS for SMTP mail relay	No
mail-user	A user for SMTP mail relay	User for SMTP mail relay	No
proxy-address	IP or DNS address for HTTP proxy	IP or DNS for HTTP proxy	No
proxy-password	A password for HTTP proxy	Password for HTTP proxy	No
proxy-port	A port for HTTP proxy	Port for HTTP proxy	No
proxy-user	A user name for HTTP proxy	user name for HTTP proxy	No
recipient-list	A list of email recipients	List of recipients	No
sender	The sender's email address	Sender	No
transport	The mail transport mechanism to be used	SMTP or HTTP	No

send-email-notification

The `send-email-notification` command sends an email notification.

Input Parameter	Description	Value	Mandatory
text	Description text	N/A	Yes

show-snmp-notifier

The `show-snmp-notifier` command displays SNMP notification configuration.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Enabled	Indicates if SNMP notification is enabled or disabled.
Recipients	Notifications' recipients
SNMP-Version	SNMP version
Trap-Port	TCP port for SNMP traps (default port 162)
Community	Used for SNMP authentication
User-Name	SNMP v3 username
Auth-Key	SNMP v3 authentication key
Priv-Key	SNMP v3 privilege key
Auth-Protocol	SNMP v3 authentication protocol
Priv-Protocol	SNMP v3 privilege protocol

modify-snmp-notifier

The `modify-snmp-notifier` command modifies the SNMP notification settings.

Input Parameter	Description	Value	Mandatory
auth-key	SNMP v3 authentication key	String	No
auth-protocol	SNMP v3 authentication protocol	md5, sha, no_auth	No
community	SNMP community string	String	No
disable	Indicates if the notification is disabled.	N/A	One from Group1*
enable	Indicates if the notification is enabled.	N/A	One from Group1*
port	UDP port (default 162)	Port number	No
priv-key	SNMP v3 privilege key	String	No
priv-protocol	SNMP v3 privilege protocol	des, aes128, no_priv	No
recipient-list	Recipient server list	List: IP or server name	No
username	SNMP v3 username	String	No
version	SNMP version	v1, v2c or V3	No

*)Group 1: ['disable', 'enable']

send-snmp-notification

The `send-snmp-notification` command sends an SNMP notification.

Input Parameter	Description	Value	Mandatory
text	Description text	N/A	Yes

show-syr-notifier

The `show-syr-notifier` command displays ESRS (EMC Secure Remote Support) information notification configuration.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Enabled	Indicates if support information notification is enabled or disabled.
Frequency	Notification frequency (hours)
ConnectEMC-Config	A divider between the SYR notifier configuration information (Enabled, Frequency), and the various settings related to the xms configuration of ConnectEMC and ESRS
Site Name	Indicates the customer's site where the cluster is installed.
PSNT	The cluster's Product Serial Number Tag (assigned by EMC)

modify-syr-notifier

The `modify-syr-notifier` command modifies the ESRS (EMC Secure Remote Support) notification parameters.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	name or index	No
connection-type	Connection type	SYR Notifier connection type (possible values: "esrgw", "ipclient", "email", "ftps")	No
disable	Disable	N/A	No
email-password	Mail password	Mail server password	No
email-sender	Mail sender	Sender name	No
email-server	Mail server	Hostname or IP for mail server	No
email-user	Mail username	Mail server username	No
enable	Enable	N/A	No
esrs-gw-host	Gateway host	IP for ESRS Gateway	No
esrs-gw-host-secondary	Secondary Gateway host	IP for ESRS Gateway	No
frequency	frequency	Hours (positive number)	No
site-name	Site name	Name (can contain spaces)	No

send-syr-notification

The `send-syr-notification` command sends a predefined ESRS (EMC Secure Remote Support) information notification.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	name or index	No
test-event	Send a test event.	N/A	No

control-led

The `control-led` command beacons the identification LED.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	id: name or index	No
entity	FRU	'SSD', 'DAECLCC', 'LocalDisk', 'StorageController', 'DAE'	Yes
inverse-mode	Apply on all except for the specified one.	N/A	No
led-mode	The desired LED mode	'On', 'Off', 'blinking'	Yes
object-id-list	Object ID list	List of IDs: name or index if class=node, format is ["X1-N1", X1-N2"]	Yes

show-leds

The `show-leds` command displays the values for the identification and status LEDs.

Output Parameter	Description
Entity	The type of the entity represented by the LED
Name	The name of the entity represented by the LED
Index	The index of the entity represented by the LED
Identify-Beacon	The identification LED status (off/blinking)
Status-Beacon	The status LED status (off/blinking)

Data Protection Related CLI Commands

remove-ssd

The `remove-ssd` command removes an SSD from a Data Protection Group. An SSD that belongs to a Data Protection Group cannot be removed.

If the SSD has already been physically removed from its slot in the X-Brick, the SSD is immediately eliminated from cluster records. If it is still inserted, its status is defined as Eject Pending. After it is removed, the cluster automatically removes the SSD.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	id: name or index	No
ssd-id	SSD ID	Name or index	Yes

show-slots

The `show-slots` command displays a list of SSD slots within the DAE, and their properties.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	id: Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Cluster-Name	The cluster's name
Index	The cluster's index number
Brick-Name	The name of the X-Brick to which the slot belongs
Index	The X-Brick's index number within the DAE
Slot #	The DAE slot number
State	The slot's current status in relation to an SSD
Error	Indicates an error related to the slot.
UID	The unique identifier (WWN) of the disk inserted in the slot
Product-Model	The model of the SSD inserted in the slot
SSD-Size	The size of the SSD inserted in the slot

show-ssds

The `show-ssds` command displays a list of SSDs in the cluster and their properties.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
SSD-Name	The SSD's name
Index	The SSD's index number
Brick-Name	The name of the X-Brick in which the SSD is inserted
Index	The X-Brick's index number
Slot #	The X-Brick's DAE slot number in which the SSD is inserted
Product-Model	The SSD's model
FW-Version	The SSD's firmware version
FW-State	The SSD's firmware state
Part-Number	A string identifier of the part (assigned by EMC)
SSD-Size	The SSD's disk space size
DPG-Name	The name of the XDP group to which the SSD is associated
Index	The Data Protection Group's index number
State	The SSD's current status
Position-State	The SSD's current position status
Endurance-Remaining-%	Percentage of the SSD's remaining endurance
Certainty-State	Indicates if there is a pending command associated with the SSD.
SSD-Encryption-Status	Indicates if encryption is enabled.

show-ssd-sas-counters

The `show-ssd-sas-counters` command displays a list of diagnostic counters that can indicate problems in the SAS link between the DAE controller and a specified SSD.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No
ssd-id	SSD ID	Name or Index	Yes

Output Parameter	Description
Name	The SSD's name
Index	The SSD's index number
Cluster-Name	The cluster's name
Index	The cluster's index number
Port-Index	The port index number
Invalid-Dwords	The number of invalid Dwords over the link
Disparity-Errors	The number of Dwords with a running disparity errors
Loss-Dword-Sync	The number of times the link lost Dword synchronization
Phy-Resets	The number of times the SAS phy undergone reset

add-ssd

The `add-ssd` command adds an SSD to the X-Brick and initializes it.

Input Parameter	Description	Value	Mandatory
brick-id	X-Brick ID	Name or index	Yes
cluster-id	Cluster ID	id: name or index	No
is-encrypted-unreadable-ssd		N/A	No
is-foreign-xtremapp-ssd	Allows to override the foreign SSD state and add a foreign SSD to the X-Brick.	N/A	No
ssd-name	SSD's Name	String	No
ssd-uid	SSD's UID	String	Yes

show-data-protection-groups

The `show-data-protection-groups` command displays XDP groups status and information.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The Data Protection Group's name
Index	The Data Protection Group's index number
State	The Data Protection Group's state
Useful-SSD-Space	The available physical capacity in the Data Protection Group
UD-SSD-Space	The total SSD space available to the XtremIO Storage Array for user data
UD-SSD-Space-In-Use	The SSD space currently in use
Rebuild-Progress	The progress of a rebuild action for the Data Protection Group following SSD failure
Preparation-Progress	The Data Protection Group is being added to the cluster and is in preparation.
Proactive-Metadata-Loading	Indicates whether there is lazy load in progress.
Rebuild-Prevention	Indicates if a rebuild was prevented due to insufficient user data space.
Brick-Name	The X-Brick's name
Index	The X-Brick's index number
Cluster-Name	The cluster's name
Index	The cluster's index number

show-clusters-data-protection-properties

The `show-clusters-data-protection-properties` command displays clusters' data protection properties.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Cluster-Name	The cluster's name
Index	The cluster's index number
Min-SSDs-Per-Healty-DPG	The minimum number of active SSDs for a healthy state Data Protection Group
Max-SSDs-Per-DPG	The maximum number of SSDs allowed per Data Protection Group

Cluster Health Related CLI Commands

show-targets-fc-error-counters

The `show-targets-fc-error-counters` command displays Fibre Channel error counter per Target.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The Target's name
Index	The Target's index number
Dumped-Frames	The total number of dumped frames
Sync-Loss	The total number of synchronization losses
Signal-Loss	The number of times an invalid CRC error has occurred
Invalid-Crc	The total number of invalid CRC frames
Link-Failure	The total number of link failures
Prim-Seq-Err	The number of prime sequential protocol errors

show-target-groups-fc-error-counters

The `show-target-groups-fc-error-counters` command displays Fibre Channel error counter per Target Group.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
TG-Name	The Target Group's name
Index	The Target Group's index number
Dumped-Frames	The total number of dumped frames
Sync-Loss	The total number of synchronization losses
Signal-Loss	The number of times an invalid CRC error has occurred
Invalid-Crc	The total number of invalid CRC frames
Link-Failure	The total number of link failures
Prim-Seq-Err	The number of prime sequential protocol errors

create-debug-info

The `create-debug-info` command creates a debug archive log collection.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	id: Name or Index	No
datetime	e.g. 2012-05-15 11:58:48	date-time string	No
debug-info-name	Debug info name	String (without spaces or special characters)	No
debug-level	Debug level of the log collection. When omitted, default is Medium	tiny, small, medium (default) large, huge	No
sc-mgr-host	Storage Controller IP Address or Hostname	Host name	No

show-debug-info

The `show-debug-info` command displays all the debug information available in XMS.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The debug information's name
Index	The debug information's index number
Cluster-Name	The name of the cluster to which the Storage Controller belongs
Index	The cluster's index
Debug-Level	The debug level of the log collection: tiny, small, medium, large, huge
Creation-Start-Time	Time stamp of log creation starting point
Create-Time	Time stamp of debug collection completion
Output-Url	Copy this URL to access/DL the debug file.

remove-debug-info

The `remove-debug-info` command deletes the debug info file.

Input Parameter	Description	Value	Mandatory
debug-info-id	Name or index of the archive.	Name or index	Yes

test-xms-storage-controller-connectivity

The `test-xms-storage-controller-connectivity` command performs a connectivity check for a specified Storage Controller and its managing XMS.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or index	No
packet-size	Packet size	Positive Integer	No
sc-id	Storage Controller ID	Name or Index	Yes

test-xms-tcp-connectivity

The `test-xms-tcp-connectivity` command performs a connectivity check for a specified TCP port and the XMS.

Input Parameter	Description	Value	Mandatory
port	Server TCP Port	Port number	Yes
server	Server IP Address	IP address	Yes

Storage Controllers Related CLI Commands

show-storage-controllers-info

The `show-storage-controllers-info` command displays the Storage Controllers' information.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Storage-Controller-Name	The Storage Controller's name
Index	The Storage Controller's index number
Mgr-Addr	The IP address used to access the Storage Controller's manager
Brick-Name	The Storage Controller management interface
Index	The X-Brick's index number
Cluster-Name	The name of the cluster to which the Storage Controller belongs
Index	The cluster's index number
State	The Storage Controller's activity state
Conn-State	The Storage Controller's connectivity status
SW-Version	The Storage Controller's software version
SW-Build	The software build number
HW-Model	The Storage Controller's hardware model
OS-Version	The OS version number
Serial-Number	The Storage Controller's serial number
Part-Number	A string identifier of the part (assigned by EMC)
Sym-Storage-Controller	Indicates if SYM runs on the Storage Controller.
SC-Start-Timestamp	Date and time of the last start-up (after reboot)

show-storage-controllers-fw-versions

The `show-storage-controllers-fw-versions` command displays the Storage Controllers' firmware version information.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Storage-Controller-Name	The Storage Controller's name
Index	The Storage Controller's index number
Local-Disk-Controller	Local Disk controller ID
PCI-Disk-Controller	PCI Disk controller firmware
IPMI-BMC	IPMI firmware
FC-HBA	FC Targets firmware
PCI-10GE-HBA	iSCSI Targets firmware
PCI-IB-HBA	InfiniBand Targets firmware
BIOS	Storage Controller BIOS firmware
SDR	Sensor Device Record (a FW related to the Storage Controller IPMI sensors)
ME	Sub-component of the BMC

show-storage-controllers-psus

The `show-storage-controllers-psus` command displays the Storage Controller's power supply units (PSUs) information.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	PSU's name
Index	PSU's index number
Serial-Number	PSU's serial number
Location-Index	The PSU's index in relation to the Storage Controller
Power-Feed	The PSU's power feed
State	The field replaceable unit state (healthy, disconnected, failed or in transient state)
Enabled-State	Indicates if PSU is enabled.
Input	Indicates if there is input power to the supply (on or off).
Location	The PSU's physical location (right or left)
HW-Revision	PSU's hardware revision
Part-Number	A string identifier of the part (assigned by EMC)
Storage-Controller-Name	Storage Controller's name
Index	Storage Controller's index number
Brick-Name	X-Brick's name
Index	X-Brick's index number
Cluster-Name	Cluster's name
Index	Cluster's index number

show-storage-controllers-sensors

The `show-storage-controllers-sensors` command displays a list of sensors and their related information.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	Name or Index	No
duration	Monitor duration	Seconds	No
fault-only	Show only faulty sensors	N/A	No
frequency	Monitor intervals	Seconds	No
sc-id	Storage Controller ID	Name or Index	No
sensor-type	Filter by sensor type	'temperature', 'power_unit', 'current', 'fan', 'voltage', 'processor', 'power_supply'	No

Output Parameter	Description
Storage-Controller-Name	The Storage Controller's name
Index	The Storage Controller's Index Number
Sensor-Type	The sensor's type
Sensor-Name	The sensor's name
Health-State	The sensor's health state
Value	The sensor's current value
Upper-Threshold	The sensor's upper threshold
Lower-Threshold	The sensor's lower threshold
Units	The sensor's measurement units

show-local-disks

The `show-local-disks` command displays the Storage Controller's local disks information.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The disk's name
Index	The disk's index number
Serial-Number	The disk's serial number
Location-Index	The disk's location in the server
State	State of the disk: healthy or fault
Enabled-State	Enabled or disabled
FW-Version	Firmware version
Part-Number	A string identifier of the part (assigned by EMC)
UID	Unique ID
Disk-Type	Disk type (SSD or HDD)
Disk-Expected-Type	The disk type the cluster expects to have for the drive (SSD or HDD)
Disk-Purpose	The disk's purpose (journal_and_boot_disk, trace_disk)
Storage-Controller-Name	Storage Controller's name
Index	Storage Controller's index number
Brick-Name	X-Brick's name
Index	X-Brick's index number
Cluster-Name	Cluster's name
Index	Cluster's index number
Encryption-Status	Indicates if encryption is enabled.

show-xenvs

The `show-xenvs` command displays a list of Storage Controller x-envs and their properties.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
XEnv-Name	The x-env's name
Index	The x-env's index number
CPU (%)	The current percentage of CPU usage
CSID	The unique clustering ID used for internal messaging
State	The x-env's current state: active or inactive
Storage-Controller-Name	The Storage Controller's name
Index	The Storage Controller's index number
Brick-Name	The X-Brick's name
Index	The X-Brick's index number

activate-storage-controller

The `activate-storage-controller` command activates a replaced or non-active Storage Controller.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	ID: Name or Index	No
sc-id	Storage Controller object ID	Name or index	Yes

deactivate-storage-controller

The `deactivate-storage-controller` command deactivates an active Storage Controller (e.g. for replacing purposes).

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	ID: Name or Index	No
sc-id	Storage Controller object ID	Name or index	Yes

Performance Related CLI Commands

show-initiator-groups-performance

The `show-initiator-groups-performance` command displays Initiator groups' performance data.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
IG-Name	Initiator Group name
Index	Initiator Group index
Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS.
Write-IOPS	
Read-BW (MB/s)	
Read-IOPS	
BW (MB/s)	
IOPS	
Total-Write-IOs	
Total-Read-IOs	

show-initiator-groups-performance-small

The `show-initiator-groups-performance-small` command displays Initiator Groups' performance data for small (under 4KB) blocks.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
IG-Name	The Initiator Group's name
Index	The Initiator Group's index
S-Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS of I/Os which are smaller than 4KB.
S-Write-IOPS	
S-Read-BW (MB/s)	
S-Read-IOPS	
S-BW (MB/s)	
S-IOPS	
Total-S-Write-IOs	
Total-S-Read-IOs	

show-initiator-groups-performance-unaligned

The `show-initiator-groups-performance-unaligned` command displays Initiator Groups' performance data for unaligned blocks (I/O blocks whose size is not a multiplication of 4KB or which have an offset).

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
IG-Name	The Initiator Group's name
Index	The Initiator Group's index
U-Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS of unaligned I/Os which are greater than 4KB I/Os.
U-Write-IOPS	
U-Read-BW (MB/s)	
U-Read-IOPS	
U-BW (MB/s)	
U-IOPS	
Total-U-Write-IOS	
Total-U-Read-IOS	

show-initiators-performance

The `show-initiators-performance` command displays Initiators' performance data.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Initiator-Name	The Initiator's name
Index	The Initiator's index number
Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS.
Write-IOPS	
Read-BW (MB/s)	
Read-IOPS	
BW (MB/s)	
IOPS	
Total-Write-IOs	
Total-Read-IOs	

show-initiators-performance-small

The `show-initiators-performance-small` command displays Initiators' performance data for small (under 4KB) block sizes.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Initiator-Name	The Initiator's name
Index	The Initiator's index number
S-Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS of I/Os which are smaller than 4KB.
S-Write-IOPS	
S-Read-BW (MB/s)	
S-Read-IOPS	
S-BW (MB/s)	
S-IOPS	
Total-S-Write-IOs	
Total-S-Read-IOs	

show-initiators-performance-unaligned

The `show-initiators-performance-unaligned` command displays Initiators' performance data for unaligned data block (I/O blocks whose size is not a multiplication of 4KB or which have an offset).

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Initiator-Name	The Initiator's name
Index	The Initiator's index number
u-Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS of unaligned I/Os which are greater than 4KB I/Os
u-Write-IOPS	
u-Read-BW (MB/s)	
u-Read-IOPS	
u-BW (MB/s)	
u-IOPS	
Total-U-Write-IOs	
Total-U-Read-IOs	

show-most-active

The `show-most-active` command displays the most active Volumes and Initiator Groups.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No
Measurement Type	Filtering criteria	bw or iops	No

Output Parameter	Description
Volume-Name	The component's name
Index	The component's index
Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS.
Read-BW (MB/s)	
Write-IOPS	
Read-IOPS	
BW (MB/s)	
IOPS	

show-most-active-initiator-groups

The `show-most-active-initiator-groups` command displays performance data of the most active Initiator Groups.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No
Measurement Type	Filtering criteria	bw or iops	No

Output Parameter	Description
IG-Name	Initiator Group's name
Index	Initiator Group's index number
Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS.
Read-BW (MB/s)	
Write-IOPS	
Read-IOPS	
BW (MB/s)	
IOPS	

show-most-active-volumes

The `show-most-active-volumes` command displays performance data of the most active Volumes.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No
Measurement Type	Filtering criteria	bw or iops	No

Output Parameter	Description
Volume-Name	The Volume's name
Index	The Volume's index number
Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS.
Read-BW (MB/s)	
Write-IOPS	
Read-IOPS	
BW (MB/s)	
IOPS	

show-volumes-performance

The `show-volumes-performance` command displays Volumes' performance data.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Volume-Name	The Volume's name
Index	The Volume's index number
Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS.
Read-BW (MB/s)	
Write-IOPS	
Read-IOPS	
BW (MB/s)	
IOPS	
Total-Write-IOs	
Total-Read-IOs	

show-volumes-performance-small

The `show-volumes-performance-small` command displays Volumes' performance data for small (under 4KB) blocks.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Volume-Name	The Volume's name
Index	The Volume's index number
S-Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS of I/Os which are smaller than 4KB.
S-Read-BW (MB/s)	
S-Write-IOPS	
S-Read-IOPS	
S-BW (MB/s)	
S-IOPS	
Total-S-Write-IOs	
Total-S-Read-IOs	

show-volumes-performance-unaligned

The `show-volumes-performance-unaligned` command displays Volumes' performance data for unaligned blocks (I/O blocks whose size is not a multiplication of 4KB or which have an offset).

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Volume-Name	The Volume's name
Index	The Volume's index number
U-Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS of unaligned I/Os which are greater than 4KB.
U-Read-BW (MB/s)	
U-Write-IOPS	
U-Read-IOPS	
U-BW (MB/s)	
U-IOPS	
Total-U-Write-IOs	
Total-U-Read-IOs	

show-data-protection-groups-performance

The `show-data-protection-groups-performance` command displays XDP groups performance information.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The Data Protection Group's name
Index	The Data Protection Group's index number
Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS.
Read-BW (MB/s)	
Write-IOPS	
Read-IOPS	
BW (MB/s)	
IOPS	

show-ssds-performance

The `show-ssds-performance` command displays SSDs' performance data.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The SSD's name
Index	The SSD's index number
Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS.
Read-BW (MB/s)	
Write-IOPS	
Read-IOPS	
BW (MB/s)	
IOPS	

show-clusters-performance

The `show-clusters-performance` command displays clusters' performance data.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Cluster-Name	The cluster's name
Index	The cluster's index number
Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS.
Read-BW (MB/s)	
Write-IOPS	
Read-IOPS	
BW (MB/s)	
IOPS	
Total-Write-IOs	
Total-Read-IOs	

show-clusters-performance-small

The `show-clusters-performance-small` command displays clusters' performance data for small (under 4KB) blocks.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Cluster-Name	The cluster's name
Index	The cluster's index number
S-Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS of I/Os which are smaller than 4KB.
S-Read-BW (MB/s)	
S-Write-IOPS	
S-Read-IOPS	
S-BW (MB/s)	
S-IOPS	
Total-S-Write-IOs	
Total-S-Read-IOs	

show-clusters-performance-unaligned

The `show-clusters-performance-unaligned` command displays clusters' performance data for unaligned blocks (I/O blocks whose size is not a multiplication of 4KB or which have an offset).

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Cluster-Name	The cluster's name
Index	The cluster's index number
U-Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS of unaligned I/Os which are greater than 4KB.
U-Read-BW (MB/s)	
U-Write-IOPS	
U-Read-IOPS	
U-BW (MB/s)	
U-IOPS	
Total-U-Write-IOs	
Total-U-Read-IOs	

show-clusters-performance-latency

The `show-clusters-performance-latency` command displays clusters' performance latency data.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Cluster-Name	The cluster's name
Index	The cluster's index number
Write-Latency	The latency for write operations (in μ sec)
Read-Latency	The latency for read operations (in μ sec)
Avg-Latency	The average latency (in μ sec)

show-target-groups-performance

The `show-target-groups-performance` command displays Target Groups' performance data.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
TG-Name	The Target Group's name
Index	The Target Group's index number
Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS.
Read-BW (MB/s)	
Write-IOPS	
Read-IOPS	
BW (MB/s)	
IOPS	
Total-Write-IOs	
Total-Read-IOs	

show-target-groups-performance-small

The `show-target-groups-performance-small` command displays Target Groups' performance data for small (under 4KB) blocks.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
TG-Name	The Target Group's name
Index	The Target Group's index number
S-Write-BW (MB/s)	
S-Read-BW (MB/s)	
S-Write-IOPS	
S-Read-IOPS	
S-BW (MB/s)	
S-IOPS	
Total-S-Write-IOs	
Total-S-Read-IOs	

These properties indicate the current Bandwidth/IOPS of I/Os which are smaller than 4KB.

show-target-groups-performance-unaligned

The `show-target-groups-performance-unaligned` command displays Target Groups' performance data for unaligned blocks (I/O blocks whose size is not a multiplication of 4KB or which have an offset).

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
TG-Name	The Target Group's name
Index	The Target Group's index number
U-Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS of unaligned I/Os which are greater than 4KB.
U-Read-BW (MB/s)	
U-Write-IOPS	
U-Read-IOPS	
U-BW (MB/s)	
U-IOPS	
Total-U-Write-IOS	
Total-U-Read-IOS	

show-targets-performance

The `show-targets-performance` command displays Targets' performance data.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The Target's name
Index	The Target's index number
Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS.
Read-BW (MB/s)	
Write-IOPS	
Read-IOPS	
BW (MB/s)	
IOPS	
Total-Write-IOs	
Total-Read-IOs	

show-targets-performance-small

The `show-targets-performance-small` command displays Targets' performance data for small (under 4KB) blocks.

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The Target's name
Index	The Target's index number
S-Write-BW (MB/s)	
S-Read-BW (MB/s)	
S-Write-IOPS	
S-Read-IOPS	
S-BW (MB/s)	
S-IOPS	
Total-S-Write-IOs	
Total-S-Read-IOs	

These properties indicate the current Bandwidth/IOPS of I/Os which are smaller than 4KB.

show-targets-performance-unaligned

The `show-targets-performance-unaligned` command displays Targets' performance data for unaligned blocks (I/O blocks whose size is not a multiplication of 4KB or which have an offset).

Input Parameter	Description	Value	Mandatory
duration	Monitor duration	Seconds	No
frequency	Monitor intervals	Seconds	No

Output Parameter	Description
Name	The Target's name
Index	The Target's index number
U-Write-BW (MB/s)	These properties indicate the current Bandwidth/IOPS of unaligned I/Os which are greater than 4KB.
U-Read-BW (MB/s)	
U-Write-IOPS	
U-Read-IOPS	
U-BW (MB/s)	
U-IOPS	
Total-U-Write-IOS	
Total-U-Read-IOS	

export-performance-history

The `export-performance-history` command exports the cluster's performance history to CSV file. The exported data can be up to seven days back. Records interval is five seconds.

Input Parameter	Description	Value	Mandatory
filename	Name of the export file	String	No

The exported data consists of the following fields:

Field	Description
Date-Time	Date and time of the system reading. Readings are collected in 5 seconds granularity.
Write-BW (KB)	The total Write Bandwidth (in KB) over the sampling period
Read-BW (KB)	The total Read Bandwidth (in KB) over the sampling period
Write-IOPs	The Write IOPS over the sampling period
Read-IOPs	The Read IOPS over the sampling period
Write-Latency (usec)	The average write latency over the sampling period
Read-Latency (usec)	The average read latency over the sampling period
Avg-Latency (usec)	The average latency, which is a weighted average between read latency and write latency, over the sampling period

Tag Management CLI Commands

create-tag

The `create-tag` command creates a Tag for an entity.

Input Parameter	Description	Value	Mandatory
entity	Entity	String	Yes
tag-name	Tag name	full path Tag name	Yes

tag-object

The `tag-object` command assigns a Tag to a specified object.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	ID:Name or index	No
entity	Entity	String	Yes
entity-details	Entity ID	Name or index	Yes
tag-id	Tag ID	Name or index	Yes

untag-object

The `untag-object` command removes a Tag from a specified object.

Input Parameter	Description	Value	Mandatory
cluster-id	Cluster ID	ID:Name or index	No
entity	Entity	String	Yes
entity-details	Entity ID	Name or index	Yes
tag-id	Tag ID	Name or index	Yes

modify-tag

The `modify-tag` command modifies a specified Tag caption.

Input Parameter	Description	Value	Mandatory
caption	New Tag caption	String	Yes
tag-id	Tag ID	Name or Index	Yes
xms-id	XMS ID	Name or Index	No

remove-tag

The `remove-tag` command deletes a Tag from the tags list.

Input Parameter	Description	Value	Mandatory
tag-id	Tag ID	Name or index	Yes

show-tag

The `show-tag` command displays the details of a specified Tag.

Input Parameter	Description	Value	Mandatory
tag-id	Tag ID	Name or index	Yes

Output Parameter	Description
Name	The Tag's full path name
Index	The Tag's index number
Entity	The entity type
Number-of-Items	The number of entities assigned with the Tag
Creation-Time	The date and time of the Tag's creation
Object-List	List of all objects assigned with the specified Tag (name and index)

show-tags

The `show-tags` command displays the details of all defined Tags.

Output Parameter	Description
Name	The Tag's full path name
Index	The Tag's index number
Entity	The entity type
Number-of-Items	The number of entities assigned with the Tag
Creation-Time	The date and time of the Tag's creation

Certificate Management CLI Commands

create-server-certificate-signing-request

The `create-server-certificate-signing-request` command instructs the server to generate a public-private key pair and a certificate signing request (CSR) that can be sent to a third party certification authority (CA) for signing.

Input Parameter	Description	Value	Mandatory
cert-common-name	Fully qualified domain name	Domain name, e.g. xms.example.com	No
cert-country	Certificate country name	Two letter ISO_3166-1 country code, e.g. US	No
cert-email	Email address	Email address	No
cert-ip	IP address	Ip address	No
cert-locality	Locality	String	No
cert-org-name	Organization name	String	No
cert-org-unit-name	Organizational unit name	String	No
cert-state	State or province	String	No
server-key-size	Server key size	Integer between 2048 and 4096	No
server-key-string	Server private key	String	No

modify-server-certificate

The `modify-server-certificate` command initiates loading of a signed certificate and a key. It is possible to load a signed certificate, matching the current CSR or a signed certificate paired with a private key.

Input Parameter	Description	Value	Mandatory
chain-certificate-string	Chain of X509 Certificates	String	No
server-certificate-string	X509 Server Certificate	String	Yes
server-key-string	X509 private key	String	No

install-self-signed-server-certificate

The `install-self-signed-server-certificate` command installs the new self signed certificate.

Input Parameter	Description	Value	Mandatory
<code>cert-common-name</code>	Fully qualified domain name	domain name, e.g. <code>xms.example.com</code>	No
<code>cert-ip</code>	IP Address	IP Address	No
<code>server-certificate-signing-request-string</code>	Certificate Signing Request	String	No
<code>server-key-string</code>	RSA private key, if the CSR was not created by XMS	String	No

show-server-certificate

The `show-server-certificate` command displays the currently loaded certificate.

show-server-certificate-signing-request

The `show-server-certificate-signing-request` command displays the certificate signing request.

APPENDIX A

Alerts and Events Details

This section provides details on the available alerts and events in the XtremIO system.

This section includes the following topics:

- ◆ [General XMS Event Codes](#) 492
- ◆ [Alerts Details](#) 492
- ◆ [Events Details](#) 513

General XMS Event Codes

The following are general XMS event codes:

- ◆ 5000100 - all audit events
- ◆ 5000200 - all events that are triggered by user action
- ◆ 5000000 - all other XMS events

Alerts Details

Alert Name	Alert Code	Description	Field	Severity
sys_ud_ssd_space_limited	0200302	Cluster's free physical capacity is low. Threshold: more than 85 percent is used.		Minor
sys_ud_ssd_space_very_limited	0200303	Cluster's free physical capacity is critically low. Threshold: more than 90 percent is used.		Major
sys_ud_ssd_space_no_free	0200304	The cluster has no free physical capacity.		critical
sys_stopping	0200505	Cluster service is stopping: Stop reason is <field1>.	Field1:stopped_reason	Critical
sys_stopped	0200506	Cluster service has stopped:<field1>-<field2>.	Field1:sys_stop_type Field2:stopped_reason	Critical
sys_starting	0200507	Cluster is in the process of starting.		Minor
def_sys_in_failed_state	0200508	Cluster initialization has failed.		Critical
sys_state_unknown	0200509	Cluster state cannot be determined. XMS is unable to obtain the cluster state.		Major
sys_state_down	0200511	Cluster state is down.		Critical
sys_stop_failed	0200512	Cluster service has failed to stop.		Critical
sys_failed_stop	0200604	Cluster stop failure		major
sys_unorderly_stopping	0200606	Cluster service stop, with fast journal flushing, is in progress.		Major
sys_orderly_stopping	0200607	Cluster stop, with full journal flushing, is in progress.		major
system_upgrade_bring_up	0200806	Cluster is starting with the new upgraded version.		Minor
system_upgrade_waiting_for_version	0200807	Upgrade process is waiting for the new version to be activated.		minor

Alert Name	Alert Code	Description	Field	Severity
system_upgrade_preparing	0200808	Upgrade process is preparing the cluster for upgrade.		minor
system_upgrade_failed	0200809	Upgrade process has failed with reason <field1>.	Field1: upgrade_failure_reason	major
system_rollback_ongoing	0200811	Upgrade process has failed. Rollback is in progress.		major
disconnected_from_sys_mgr	0200901	Cluster manager is running, but it is disconnected from XMS due to <field1>.	Field1: sys_mgr_conn_error_reason	minor
sys_sharedmemory_limited	0201002	Shared memory consumption is high. <field1> percent is used. Threshold: more than 90 percent is used	Field1: shared_memory_in_use_ratio	minor
sys_sharedmemory_very_limited	0201003	Shared memory consumption has reached critically low level. <field1> percent is used. Threshold: more than 95 percent is used	Field1: shared_memory_in_use_ratio	major
sys_sharedmemory_no_free	0201004	Shared memory pool has been depleted. <field1> percent is used	Field1: shared_memory_in_use_ratio	critical
data_consistency_error	0201102	Data consistency error was encountered.		critical
sys_sharedmem_inefficiency_medium	0202002	System shared memory pools are not optimally balanced.		major
sys_sharedmem_inefficiency_high	0202003	System shared memory pools are imbalanced.		critical
vaai_tp_limit_threshold_exceeded	0202102	Cluster's VAAI thin provisioning soft limit of <field1> percent has been exceeded. The threshold is <field1> percent.	Field1: vaai_tp_limit	minor
sys_expansion_progress_yes	0202202	Cluster expansion is in progress.		minor
sys_encrypt_started	0202302	Data at Rest Encryption has started.		information
sys_encrypt_switch_incomplete	0202303	Data at Rest Encryption is incomplete.		major
sys_chap_init_missing_cluster_credentials	0202401	CHAP is enabled. Add cluster authentication credentials to initiators. Otherwise, a failure will occur when an initiator is disconnected and then re-connected.		minor

Alert Name	Alert Code	Description	Field	Severity
sys_chap_init_missing_credentials	0202502	CHAP is enabled. Add authentication credentials to initiators. Otherwise, a failure will occur when an initiator is disconnected and then re-connected.		minor
sys_hw_pkg_inconsistent	0203101	Not all Storage Controllers have the same hardware package.		major
failed_brick_state	0300102	XMS has detected an X-Brick that is not configured to be part of a cluster.		major
unsupported_disk_in_brick	0300203	Unsupported disk type or model was detected in slot <field1>.	Field1: ssd_slot_array[].slot_num	minor
uninitialized_ssd_in_brick	0300204	Uninitialized disk was detected in slot <field1>.	Field1: ssd_slot_array[].slot_num	minor
foreign_xtremapp_ssd_in_brick	0300205	Foreign SSD from a different X-brick or cluster was detected in slot <field1>. id=<field2>.	Field1: ssd_slot_array[].slot_num Field2: ssd_slot_array[].slot_uid	minor
slot_error_in_brick	0300206	The state of slot <field1> cannot be determined due to an error: <field2>	Field1: ssd_slot_array[].slot_num Field2: ssd_slot_array[].slot_error_reason	major
sas1_port_down	0400202	Storage Controller SAS port 1 is down.		major
sas2_port_down	0400302	Storage Controller SAS port 2 is down.		major
node_sas1_3gbps_rate	0400403	SAS port is running at partial rate of 3GBPS.		minor
disconnected_from_node_mgr	0400503	Storage Controller is disconnected from the XMS.		major
notifier_disabled	0406202	Event notifiers were disabled.		information
journal_fault	0400703	Journaling on this Storage Controller has been disabled.		major
journal_dumping	0400704	Journal information is in the process of destaging from the Storage Controller memory to persistent media (SSDs).		major
backend_storage_controller_error	0400802	Storage Controller's SAS controller state is undetermined.		major
node_ram_too_low	0400902	Insufficient RAM: actual is <field1> but expected is <field2>.	Field1: ram Field2: expected_ram	major

Alert Name	Alert Code	Description	Field	Severity
node_temp_level_2_unknown	0401102	Storage Controller temperature IPMI information is unavailable.		minor
node_temp_level_3_warning	0401103	IPMI reported abnormal temperature.		minor
node_temp_level_4_minor	0401104	IPMI reported abnormal temperature.		minor
node_temp_level_5_major	0401105	IPMI reported abnormal temperature.		major
node_temp_level_6_critical	0401106	IPMI reported abnormal temperature.		major
node_fan_level_2_unknown	0401202	Storage Controller fan IPMI information is unavailable.		minor
node_fan_level_3_warning	0401203	IPMI reported abnormal fan sensor indications.		minor
node_fan_level_4_minor	0401204	IPMI reported abnormal fan sensor indications.		minor
node_fan_level_5_major	0401205	IPMI reported abnormal fan sensor indications.		major
node_fan_level_6_critical	0401206	IPMI reported abnormal fan sensor indications.		major
node_volt_level_2_unknown	0401302	Storage Controller voltage IPMI information is unavailable.		minor
node_volt_level_3_warning	0401303	IPMI reported abnormal voltage levels.		minor
node_volt_level_4_minor	0401304	IPMI reported abnormal voltage levels.		minor
node_volt_level_5_major	0401305	IPMI reported abnormal voltage levels.		major
node_volt_level_6_critical	0401306	IPMI reported abnormal voltage levels.		major
node_curt_level_2_unknown	0401402	Storage Controller current IPMI information is unavailable.		minor
node_curt_level_3_warning	0401403	IPMI reported abnormal current levels.		minor
node_curt_level_4_minor	0401404	IPMI reported abnormal current levels.		minor
node_curt_level_5_major	0401405	IPMI reported abnormal current levels.		major
node_curt_level_6_critical	0401406	IPMI reported abnormal current levels.		major
eth_port_down	0401602	Storage Controller management port is down.		major

Alert Name	Alert Code	Description	Field	Severity
eth_port_unknown	0401603	Storage Controller management port state cannot be determined.		major
node_ib1_level_2_unknown	0401702	InfiniBand port 1: link status cannot be determined.		minor
node_ib1_level_3_warning	0401703	InfiniBand port 1: link status is not healthy. The port state is <field1>.	Field1: ib1_port_state	minor
node_ib1_level_4_minor	0401704	InfiniBand port 1: link status is not healthy. The port state is <field1>.	Field1: ib1_port_state	minor
node_ib1_level_5_major	0401705	InfiniBand port 1: link status is not healthy. The port state is <field1>.	Field1: ib1_port_state	major
node_ib1_level_6_critical	0401706	InfiniBand port 1: link status is not healthy. The port state is <field1>.	Field1: ib1_port_state	major
node_wrong_ib1_port_connection	0401802	Storage Controller's InfiniBand port 1 is connected to the wrong port on the InfiniBand Switch.		major
node_wrong_ib1_switch_connected	0401803	Storage Controller's InfiniBand port 1 is connected to the wrong InfiniBand Switch.		major
node_ib1_port_down	0401902	Storage Controller InfiniBand port 1 is down.		major
node_ib1_port_unknown	0401903	Storage Controller InfiniBand port 1 port state cannot be determined.		major
node_ib2_level_2_unknown	0402102	InfiniBand port 2: link status cannot be determined.		minor
node_ib2_level_3_warning	0402103	InfiniBand port 2: link status is not healthy. The port state is <field1>.	Field1: ib2_port_state	minor
node_ib2_level_4_minor	0402104	InfiniBand port 2: link status is not healthy. The port state is <field1>.	Field1: ib2_port_state	minor
node_ib2_level_5_major	0402105	InfiniBand port 2: link status is not healthy. The port state is <field1>.	Field: ib2_port_state	major
node_ib2_level_6_critical	0402106	InfiniBand port 2: link status is not healthy. The port state is <field1>.	Field ib2_port_state	major
node_wrong_ib2_port_connection	0402202	Storage Controller's InfiniBand port 2 is connected to the wrong port on the InfiniBand Switch.		major

Alert Name	Alert Code	Description	Field	Severity
node_wrong_ib2_switch_connected	0402203	Storage Controller's InfiniBand port 2 is connected to the wrong InfiniBand Switch.		major
node_ib2_port_down	0402302	Storage Controller InfiniBand port 2 is down.		major
node_ib2_port_unknown	0402303	Storage Controller InfiniBand port 2 is unknown.		major
upgrade_failed	0402403	Storage Controller upgrade has failed: <field1>. Current version is <field2>.	Field1: upgrade_failure_reason Field2: sw_version	major
node_upgrade_in_progress	0402404	Storage Controller upgrade is in progress.		minor
node_orderly_stop	0402502	Storage Controller has stopped gracefully.		major
node_unorderly_stop	0402503	Storage Controller has stopped.		major
node_failed_stop	0402504	Storage Controller stop process has failed. Cluster is in unrecoverable state and data integrity is suspected.		major
node_orderly_stopping	0402505	Storage Controller is in the process of graceful stop.		major
node_unorderly_stopping	0402506	Storage Controller is in the process of immediate stop.		major
node_user_disabled	0402602	Storage Controller was deactivated (disabled) by user request.		major
node_system_disabled	0402603	Storage Controller has been deactivated by the cluster.		major
node_fru_failed	0402703	Storage Controller is faulty.		major
node_fru_disconnected	0402704	Storage Controller has been removed (physically or logically).		major
node_fru_uninitialized	0402705	Storage Controller is not initialized.		minor
node_fru_prepare_failed	0402706	Storage Controller prepare has failed		minor
node_fw_upgrading	0402802	Storage Controller's software or firmware is being upgraded.		information
node_fw_invalid	0402803	Storage Controller's software or firmware version is incompatible <field1>. Storage Controller cannot be used.	Field1: fw_failure_detail	major

Alert Name	Alert Code	Description	Field	Severity
node_fw_mismatch	0402804	Unexpected Storage Controller's software or firmware version has been detected: <field1>.	Field1: fw_failure_detail	minor
node_free_ram_low	0402902	The Storage Controller's memory utilization is high.		major
node_file_descriptors_high	0402912	Excessive number of open file descriptors		major
mgmt_port_half_duplex	0403102	Storage Controller management port is set to half duplex.		major
node_dimm_level_2_unknown	0403302	Storage Controller DIMM memory card information is unavailable.		minor
node_dimm_level_3_warning	0403303	Memory card (DIMM) health fault		minor
node_dimm_level_4_minor	0403304	Memory card (DIMM) health fault		minor
node_dimm_level_5_major	0403305	Memory card (DIMM) health fault		major
node_dimm_level_6_critical	0403306	Memory card (DIMM) health fault		major
inconsistent_fc_tar_speed	0403402	Cluster's FC Target ports are running at different speeds.		minor
inconsistent_scsi_tar_speed	0403502	iSCSI Target ports do not have the same speed.		minor
node_sas2_3gbps_rate	0403603	SAS port is running at the partial rate of 3GBPS		minor
remote_journal_failed	0403702	The cluster has detected a potential risk for the remote journal (mirrored) health or persistency. Journaling at the remote Storage Controller was disabled by the cluster to keep data consistency and persistency.		minor
remote_journal_dumping	0403703	The remote journal information is in the process of destaging from the Storage Controller memory to persistent media (SSDs).		major
node_eth_10m_rate	0403801	ETH management port is at sub-optimal rate of 10M.		major
node_eth_100m_rate	0403802	ETH management port is at sub-optimal rate of 100M.		minor
node_ethport_level_2_unknown	0403902	Management link health status cannot be determined.		minor

Alert Name	Alert Code	Description	Field	Severity
node_ethport_level_3_warning	0403903	Management link health status is marginal.		minor
node_ethport_level_4_minor	0403904	Management link health is limited.		minor
node_ethport_level_5_major	0403905	Management link health is problematic. Attention is required.		major
node_ethport_level_6_critical	0403906	Management link health is faulty. Immediate attention is required.		major
node_sas1_conn_wrong_lcc	0404002	Storage Controller SAS port 1 is connected to the wrong DAE Controller.		major
node_sas1_conn_wrong_lcc_port	0404003	Storage Controller SAS port 1 is connected to the wrong port of the DAE Controller.		major
node_sas1_conn_unknown_dae	0404004	Storage Controller SAS port 1 is not connected to the DAE of this Storage Controller's X-Brick.		major
node_sas1_level_2_unknown	0404102	SAS port 1 link health status cannot be determined.		minor
node_sas1_level_3_warning	0404103	SAS port 1 link is sub-optimal.		minor
node_sas1_level_4_minor	0404104	SAS port 1 link is sub-optimal.		minor
node_sas1_level_5_major	0404105	SAS Port 1 link is faulty.		major
node_sas1_level_6_critical	0404106	SAS Port 1 link is faulty.		major
node_sas2_level_2_unknown	0404202	SAS port 2 link health status cannot be determined.		minor
node_sas2_level_3_warning	0404203	SAS port 2 link is sub-optimal.		minor
node_sas2_level_4_minor	0404204	SAS port 2 link is sub-optimal.		minor
node_sas2_level_5_major	0404205	SAS Port 2 link is faulty.		major
node_sas2_level_6_critical	0404206	SAS Port 2 link is faulty.		major
node_fp_temperature_warning	0404502	Storage Controller temperature is high as reported by front panel sensor.		major
node_fp_temperature_high	0404503	Storage Controller temperature is critically high as reported by front panel sensor.		critical
node_ipmiport_invalid_wiring	0404602	Dedicated IPMI link internal cable is connected incorrectly.		major
journal_failover	0404702	The cluster has detected a journal fault in this Storage Controller.		major

Alerts and Events Details

Alert Name	Alert Code	Description	Field	Severity
journal_failback	0404703	The cluster has detected a journal failover in this Storage Controller.		major
journal_failed	0404704	The cluster has detected a journal fallback in this Storage Controller.		minor
ded_ipmi_port_down	0404902	Storage Controller dedicated IPMI port connected to the peer Storage Controller is down.		major
node_discover_dae_true	0405002	Cluster has discovered new DAE hardware.		minor
node_discover_daepsu_true	0405102	Cluster has found new DAE PSU. Replace procedure is required.		minor
node_discover_ibsw_true	0405202	Cluster has found new InfiniBand Switch. Replace procedure is required.		minor
node_discover_localdisk_true	0405302	Cluster has found new Local Disk. Replace procedure is required.		minor
node_discover_localdisk_true	0405402	Cluster has found new Storage Controller PSU. Replace procedure is required.		minor
node_sas2_conn_wrong_lcc	0405502	Storage Controller SAS port 2 is connected to the wrong DAE Controller.		major
node_sas2_conn_wrong_lcc_port	0405503	Storage Controller SAS port 2 is connected to the wrong port of the DAE Controller.		major
node_sas2_conn_unknown_dae	0405504	Storage Controller SAS port 2 is not connected to the DAE of this Storage Controller's X-Brick.		major
node_discover_dae_ctrl_true	0405602	Cluster has found new DAE Controller. Replace procedure is required.		minor
node_discover_bbu_true	0405702	Cluster has found new BBU. Replace procedure is required.		minor
node_disk_limited_space	0406102	Disk space level is low. <field1> Kbytes is available.	Field1:free_disk_space	minor
node_disk_no_free_space	0406103	Not enough disk space. Only <field1> Kbytes is available.	Field1:free_disk_space	major
node_tech_tunnel_opened	0407002	Technician tunnel to XMS is open. Please close it when maintenance is done.		major

Alert Name	Alert Code	Description	Field	Severity
disk_empty	0500102	Storage Controller local disk in slot <field1> of type <field2> used as <field3> is empty.	Field1: slot_num Field2: local_disk_type Field3: local_disk_purpose	major
disk_unanticipated_disk	0500103	Storage Controller local disk slot <field1> is expected to be empty, but contains a disk.	Field1:slot_num	major
disk_unsupported_disk	0500104	Storage Controller local disk in slot <field1> is an unsupported disk model or type.	Field1:slot_num	major
disk_uninitialized	0500106	Storage Controller local disk in slot <field1> is uninitialized.	Field1:slot_num	major
localdisk_user_disabled	0500202	Storage Controller local disk was deactivated (disabled) by user request.		major
localdisk_system_disabled	0500203	Cluster has disabled the Storage Controller local disk.		major
localdisk_fru_failed	0500303	Storage Controller's local disk has failed.		major
localdisk_fru_disconnected	0500304	Storage Controller's local disk is disconnected.		major
localdisk_fru_uninitialized	0500305	Storage Controller's local disk is not initialized.		minor
localdisk_fru_prepare_failed	0500306	Storage Controller's local disk prepare failed.		minor
localdisk_fw_upgrading	0500402	Firmware is being upgraded.		information
localdisk_fw_invalid	0500403	Storage Controller's local disk firmware version is incompatible.		major
localdisk_fw_mismatch	0500404	Storage Controller's local disk firmware version is incorrect.		minor
nodepsu_user_disabled	0600201	Storage Controller PSU was manually disabled by user request.		major
nodepsu_system_disabled	0600203	Cluster has disabled the Storage Controller PSU.		major
nodepsu_fru_failed	0600303	Storage Controller's PSU has failed.		major
nodepsu_fru_disconnected	0600304	Storage Controller's PSU is disconnected from the cluster.		major
nodepsu_fru_uninitialized	0600305	Storage Controller's PSU is not initialized.		minor
nodepsu_fru_prepare_failed	0600306	Storage Controller's PSU prepare has failed.		minor
nodepsu_fw_upgrading	0600402	Firmware is in the process of being upgraded.		information

Alert Name	Alert Code	Description	Field	Severity
nodepsu_fw_mismatch	0600404	Storage Controller's PSU firmware version is incorrect. The cluster will try to use the PSU.		minor
nodepsu_no_input	0600701	Storage Controller's PSU has no input.		major
rg_degraded	0800102	An SSD has failed and the DPG resiliency is degraded.		major
rg_dual_failure	0800103	DPG has a dual SSD failure and is in degraded protection mode.		critical
rg_error	0800104	DPG group has too many simultaneous SSD failures.		critical
rg_double_degrade	0800106	DPG has two simultaneous SSD failures and is in degraded protection mode.		critical
rebuild_0_to_20_done	0800211	DPG rebuild has started.		information
rebuild_20_to_40_done	0800221	DPG rebuild is in progress. More than <field1> percent of the rebuild has completed.	Field1:rebuild_progress	information
rebuild_40_to_60_done	0800231	DPG rebuild is in progress. More than <field1> percent of the rebuild has completed.	Field1:rebuild_progress	information
rebuild_60_to_80_done	0800241	DPG rebuild is in progress. More than <field1> percent of the rebuild has completed.	Field1:rebuild_progress	information
rebuild_99_done	0800251	DPG rebuild is in progress. More than <field1> percent of the rebuild has been completed.	Field1:rebuild_progress	information
prepare_0_to_20_done	0800321	DPG SSD preparation is in progress. <field1> percent of the process has been completed.	Field1:ssd_preparation_progress	information
20_to_40_done	0800331	DPG SSD preparation is in progress. <field1> percent of the process has been completed.	Field1:ssd_preparation_progress	information
prepare_40_to_60_done	0800341	DPG SSD preparation is in progress. <field1> percent of the process has been completed.	Field1:ssd_preparation_progress	information
prepare_60_to_80_done	0800351	DPG SSD preparation is in progress. <field1> percent of the process has been completed.	Field1:ssd_preparation_progress	information

Alert Name	Alert Code	Description	Field	Severity
prepare_99_done	0800361	DPG SSD preparation is in progress. <field1> percent of the process has been completed.	Field1: ssd_preparation_progress	information
rg_no_available_rebuilds	0800402	DPG cannot sustain any more SSD failures.		major
rg_low_on_available_rebuilds	0800403	DPG can sustain only one additional SSD failure.		minor
small_io_ratio_low	0800602	Volume small block I/O ratio has reached <field1> percent.	Field1: small_io_ratio	minor
small_io_ratio_medium	0800603	Volume small block I/O ratio has reached <field1> percent.	Field1: small_io_ratio	minor
small_io_ratio_high	0800604	Volume small block I/O ratio has reached <field1> percent.	Field1: small_io_ratio	major
unalign_io_ratio_low	0800702	Volume unaligned block I/O ratio has reached <field1> percent.	Field1: unaligned_io_ratio	minor
unalign_io_ratio_medium	0800703	Volume unaligned block I/O ratio has reached <field1> percent.	Field1: unaligned_io_ratio	minor
unalign_io_ratio_high	0800704	Volume unaligned block I/O ratio has reached <field1> percent.	Field1: unaligned_io_ratio	major
vol_add_pending	0800802	Volume is in an ambiguous state after an add request.		minor
volume_modify_pending	0800803	Volume is in an ambiguous state after a modification request.		minor
volume_remove_pending	0800804	Volume is in an ambiguous state after a remove request.		minor
rebalance_0_to_20_done	0800902	DPG balance is in progress. <field1> percent of the process has been completed.	Field1: rebuild_progress	information
rebalance_20_to_40_done	0800903	DPG balance is in progress. <field1> percent of the process has been completed.	Field1: rebuild_progress	information
rebalance_40_to_60_done	0800904	DPG balance is in progress. <field1> percent of the process has been completed.	Field1: rebuild_progress	information
rebalance_60_to_80_done	0800905	DPG balance is in progress. <field1> percent of the process has been completed.	Field1: rebalance_progress	information
rebalance_99_done	0800906	DPG balance is in progress. <field1> percent of the process has been completed.	Field1: rebalance_progress	information
ssd_not_in_rg	0900102	SSD is not configured in any DPG.		information

Alert Name	Alert Code	Description	Field	Severity
ssd_failed_in_rg	0900103	SSD has failed.		major
ssd_eject_pending	0900105	SSD is waiting to be ejected from its SSD slot.		minor
ssd_diag_level_2_unknown	0900202	State of the SSD cannot be determined. The SSD state is unknown.		minor
ssd_diag_level_4_minor	0900204	Diagnostics detected a problem in the SSD.		minor
ssd_diag_level_5_major	0900205	Diagnostics detected a major problem in the SSD.		major
ssd_diag_level_6_critical	0900206	Diagnostics detected a critical problem in the SSD.		major
ssd_link1_level_2_unknown	0900302	Link 1 state of the SSD cannot be determined. The SSD state is unknown.		minor
ssd_link1_level_3_warning	0900303	Cluster diagnostics detected a minor problem in link 1 of the SSD.		minor
ssd_link1_level_4_minor	0900304	Cluster diagnostics detected a problem in link 1 of the SSD.		minor
ssd_link1_level_5_major	0900305	Cluster diagnostics detected a major problem in link 1 of the SSD.		major
ssd_link1_level_6_critical	0900306	Cluster diagnostics detected a critical problem in link 1 of the SSD.		major
ssd_link2_level_2_unknown	0900402	Link 2 state of the SSD cannot be determined. The SSD state is unknown.		minor
ssd_link2_level_3_warning	0900403	Cluster diagnostics detected a minor problem in link 2 of the SSD.		minor
ssd_link2_level_4_minor	0900404	Cluster diagnostics detected a problem in link 2 of the SSD.		minor
ssd_link2_level_5_major	0900405	Cluster diagnostics detected a major problem in link 2 of the SSD.		major
ssd_link2_level_6_critical	0900406	Cluster diagnostics detected a critical problem in link 2 of the SSD.		major
ssd_user_disabled	0900602	SSD was manually disabled by user request.		major
ssd_system_disabled	0900603	The cluster has disabled the SSD. It will no longer be in service.		major
ssd_fru_failed	0900703	SSD has failed.		major

Alert Name	Alert Code	Description	Field	Severity
ssd_fru_disconnected	0900704	SSD is disconnected.		major
ssd_fru_uninitialized	0900705	SSD is not initialized.		minor
ssd_fru_prepare_failed	0900706	SSD is not initialized.		minor
ssd_fw_upgrading	0900802	Firmware is in process of being upgraded.		information
ssd_fw_invalid	0900803	Firmware version of the SSD is incompatible.		major
ssd_fw_mismatch	0900804	Firmware version of the SSD is incorrect.		minor
ssd_add_pending	0901102	SSD add request has not completed successfully.		minor
ssd_modify_pending	0901103	SSD modify request has not completed successfully.		minor
ssd_remove_pending	0901104	SSD remove request has not completed successfully.		minor
ssd_limited_endurance	0901202	Wear level (endurance) of the SSD is low. The remaining wear level for this SSD is <field1> percent.	Field1:percent_endurance_r remaining	minor
ssd_very_limited_endurance	0901203	Wear level (endurance) of the SSD is very low and has reached a critical level. The remaining wear level for this SSD is <field1> percent.	Field1:percent_endurance_r remaining	major
ssd_none_remaining_endurance	0901204	SSD endurance level is exhausted and completely worn out. The remaining wear level for this SSD is <field1> percent.	Field1:percent_endurance_r remaining	critical
tar_not_found	1100202	Target port is not found or missing.		major
tar_fc_counter	1100203	Target port has FC counter error.		minor
target_level_2_unknown	1100402	Target port state cannot be determined. The Target port state is unknown.		minor
target_level_3_warning	1100403	Target port diagnostics detected a minor problem.		minor
target_level_4_minor	1100404	Target port diagnostics detected a problem.		minor
target_level_5_major	1100405	Target port diagnostics detected a major problem.		major
target_level_6_critical	1100406	Target port diagnostics detected a critical problem.		major

Alert Name	Alert Code	Description	Field	Severity
target_add_pending	1100502	Target is in an ambiguous state after an add request.		minor
target_modify_pending	1100503	Target is in an ambiguous state after a modification request.		minor
target_remove_pending	1100504	Target is in an ambiguous state after a remove request.		minor
xenv_failover	1200107	Internal sub-process (xenv) state is performing failover.		major
xenv_failback	1200108	Internal sub-process (xenv) state is performing failback as part of process recovery.		information
module_failover	1300106	Internal sub-process (module) state is performing fail-over.		major
module_failback	1300107	Internal sub-process (module) state is performing fail-back as part of process recovery.		information
ibswitch_level_2_unknown	1400102	InfiniBand Switch link state for port <field1> cannot be determined. The link state is unknown.	Field1:port_index	minor
ibswitch_level_3_warning	1400103	InfiniBand Switch link state for port <field1> has a minor problem.	Field1:port_index	minor
ibswitch_level_4_minor	1400104	InfiniBand Switch link state for port <field1> has a problem.	Field1:port_index	major
ibswitch_level_5_major	1400105	InfiniBand Switch link state for port <field1> has a major problem.	Field1:port_index	major
ibswitch_level_6_critical	1400106	InfiniBand Switch link state for port <field1> has a critical problem.	Field1:port_index	major
ibswitch_user_disabled	1400302	The InfiniBand Switch was manually disabled by user request.		major
ibswitch_system_disabled	1400303	The cluster has disabled the InfiniBand Switch.		major
ibswitch_fru_failed	1400403	InfiniBand Switch has failed.		major
ibswitch_fru_disconnected	1400404	InfiniBand Switch is disconnected.		major
ibswitch_fru_uninitialized	1400405	InfiniBand Switch is not initialized.		minor
ibswitch_fru_prepare_failed	1400406	InfiniBand Switch prepare has failed.		minor
ibswitch_fw_upgrading	1400502	Firmware is in the process of being upgraded.		information

Alert Name	Alert Code	Description	Field	Severity
ibswitch_fw_invalid	1400503	InfiniBand Switch firmware version is incompatible.		major
ibswitch_fw_mismatch	1400504	InfiniBand Switch firmware version is incorrect.		minor
ibswitch_unknown_model	1400505	The InfiniBand Switch model is not supported in this cluster's software version.		major
ibswitch_wrong_connection	1400602	Incorrect connection between Storage Controller(s) and InfiniBand Switch was detected.		major
ibswitch_s2s_ib1_port_down	1400801	InfiniBand Switch to InfiniBand Switch port 17 is down.		minor
ibswitch_s2s_ib2_port_down	1400901	InfiniBand Switch to InfiniBand Switch port 18 is down.		minor
no_ups_load	1500102	No power (load) is being consumed from the BBU.		major
low_threshold_ups_load	1500103	Power being consumed from the BBU is excessive. The current power consumption (load) is <field1> percent of the BBU's full load capability.	Field1:ups_load_in_percent	minor
med_threshold_ups_load	1500104	Power being consumed from the BBU is excessive. The current power consumption (load) is <field1> percent of the BBU's full load capability.	Field1:ups_load_in_percent	major
high_threshold_ups_load	1500105	BBU is overloaded. The current power consumption (load) is <field1> percent of the BBU's full load capability.	Field1:ups_load_in_percent	major
ups_node_1_disconnected	1500203	Serial communication to the BBU is disconnected from Storage Controller 1, but is connected from Storage Controller 2.		major
ups_node_2_disconnected	1500204	Serial communication to the BBU is disconnected from Storage Controller 2, but is connected from Storage Controller 1.		major
ups_no_external_power	1500402	There is no external power feed from grid <field1> to the BBU. BBU may be powered off or running on battery.	Field1:power_feed	major
ups_low_bat_failure_true	1500502	BBU charge level is low: <field1> percent. Power input to the BBU is present, but the battery is insufficiently charged.	Field1:ups_battery_charge_in_percent	major

Alert Name	Alert Code	Description	Field	Severity
ups_low_bat_no_input	1500602	BBU charge level is low: <field1> percent. Power input to the BBU is not present.	Field1:ups_battery_charge_in_percent	major
ups_low_bat_run_failure_true	1500702	Battery Backup Unit has low runtime. Current battery runtime value is: <field1> seconds.	Field1:battery_runtime	major
ups_overld_failure_true	1500802	BBU is overloaded. The current power consumption (load) is <field1> percent of the BBU's full load capability.	Field1:ups_load_in_percent	major
ups_bypass_active_failure_true	1501102	Battery Backup Unit bypass mode is activated (there is no protection against power dips or outages).		major
ups_need_bat_replce_failure_true	1501302	The cluster has detected that the Battery Backup Unit should be replaced.		major
ups_user_disabled	1501401	The Battery Backup Unit has been manually disabled by user request.		major
ups_system_disabled	1501403	Cluster has disabled the Backup Battery Unit.		major
ups_fru_failed	1501503	BBU has failed. Failure reason: <field1>	Field1:ups_alarm	major
ups_fru_disconnected	1501504	BBU is disconnected from the cluster.		major
ups_fru_uninitialized	1501505	BBU is not initialized.		minor
ups_fru_prepare_failed	1501506	BBU is not initialized		minor
ups_fw_upgrading	1501602	Firmware is in the process of being upgraded.		information
ups_fw_invalid	1501603	BBU firmware version is incompatible.		major
ups_fw_mismatch	1501604	BBU firmware version is incorrect. The cluster will try to use the BBU.		minor
sas_sas1_port_down	1600202	DAE Controller SAS Port 1 is down.		major
sas_connectivity_down	1600302	DAE Controller SAS connection is down.		critical
sas_connectivity_degraded	1600303	DAE Controller SAS connectivity is sub-optimal.		minor
jbodcontroller_user_disabled	1600402	The DAE Controller was manually disabled by user request.		major

Alert Name	Alert Code	Description	Field	Severity
jbodcontroller_system_disabled	1600403	The cluster has disabled the DAE LCC. It will no longer be in service.		major
jbodcontroller_fru_failed	1600503	The <field1> DAE Controller has failed.	Field1:location	major
jbodcontroller_fru_disconnected	1600504	The <field1> DAE Controller is disconnected.	Field1:location	major
jbodcontroller_fru_uninitialized	1600505	The <field1> DAE Controller is not initialized.	Field1:location	minor
jbodcontroller_fru_prepare_failed	1600506	The <field1> DAE Controller is not initialized.	Field1:location	minor
jbodcontroller_fw_upgrading	1600602	Firmware is in the process of being upgraded.		information
jbodcontroller_fw_invalid	1600603	Firmware version of the <field1> Controller is incorrect. The cluster will try to use the DAE Controller.	Field1:location	major
jbodcontroller_fw_mismatch	1600604	Firmware version of the DAE's <field1> DAE Controller is incorrect. The cluster will try to use the DAE Controller.	Field1:location	minor
node_lcc_level_2_unknown	1600912	DAE Controller health information is unavailable. The cluster is unable to read the information.		minor
node_lcc_level_3_warning	1600913	DAE Controller health status is marginal.		minor
node_lcc_level_4_minor	1600914	DAE Controller health status is limited.		minor
node_lcc_level_5_major	1600915	DAE Controller health status is problematic. Attention is required.		major
node_LCC_level_6_critical	1600916	DAE Controller health status is faulty. Immediate attention is required.		major
lcc_sas2_port_down	1601102	DAE Controller SAS Port 2 is down.		minor
jbodpsu_user_disabled	1700202	The DAE PSU was manually disabled by user request.		major
jbodpsu_system_disabled	1700203	The cluster has disabled the DAE PSU. It will no longer be in service.		major
jbodpsu_fru_failed	1700303	The <field1> DAE PSU has failed.	Field1:location	major
jbodpsu_fru_disconnected	1700304	The <field1> DAE PSU is disconnected.	Field1:location	major

Alert Name	Alert Code	Description	Field	Severity
jbodpsu_fru_uninitialized	1700305	The <field1> DAE PSU is not initialized.	Field1:location	minor
jbodpsu_fru_prepare_failed	1700306	The <field1> DAE PSU prepare failed.	Field1:location	minor
jbodpsu_fw_upgrading	1700402	Firmware is in the process of being upgraded.		information
jbodpsu_fw_invalid	1700403	Firmware version of the <field1> DAE PSU is incompatible. The PSU cannot be used.	Field1:location	major
jbodpsu_fw_mismatch	1700404	Firmware version of the <field1> DAE PSU is incorrect. The cluster will try to use the PSU.		minor
dae_psu_ac_lost	1700702	No AC feed to DAE PSU was detected.		major
dae_psu_ac_out_of_range	1700703	DAE PSU AC is out of range.		major
dae_psu_ac_failed	1700704	DAE PSU AC failure was detected.		major
ibswitchpsu_user_disabled	1700802	The InfiniBand Switch PSU was manually disabled by user request.		major
ibswitchpsu_system_disabled	1700803	The cluster has disabled the InfiniBand Switch PSU. It will no longer be in service.		major
ibswitchpsu_fru_failed	1700903	The <field1> InfiniBand Switch PSU has failed.	Field1:location	major
ibswitchpsu_fru_disconnected	1700904	The <field1> InfiniBand Switch PSU is disconnected.	Field1:location	major
ibswitchpsu_fru_uninitialized	1700905	The <field1> InfiniBand Switch PSU is not initialized.	Field1:location	minor
ibswitchpsu_fru_prepare_failed	1700906	The <field1> InfiniBand Switch PSU prepare has failed.	Field1:location	minor
ibswitchpsu_no_external_power	1701502	Power input to the InfiniBand Switch PSU has failed.		major
jbod_fru_failed	1800303	DAE has failed.		major
jbod_fru_disconnected	1800304	DAE is disconnected from the cluster.		major
jbod_fru_uninitialized	1800305	DAE is not initialized.		minor
jbod_fru_prepare_failed	1800306	DAE is not initialized.		minor
jbod_fru_prepare_failed	1800306	DAE is not initialized.		minor
snapshotgroup_add_pending	1900102	Volume Snapshot Group is in an ambiguous state after an add request.		minor

Alert Name	Alert Code	Description	Field	Severity
snapshotgroup_modify_pending	1900103	Volume Snapshot Group is in an ambiguous state after a modification request.		minor
snapshotgroup_remove_pending	1900104	Volume Snapshot Group is in an ambiguous state after a remove request.		minor
discovery_chap_initiators_missing_credentials_true	1901102	CHAP is enabled. Add discovery credentials to initiators. Otherwise, a failure will occur when an initiator is disconnected and then re-connected.		major
xms_disk_low_free_space	2000002	Disk free space level is low. <field1> Kbytes are available.	Field1:free_space	major
xms_disk_no_free_space	2000003	Insufficient disk space: <field1> Kbytes are available.	Field1:free_space	critical
xms_disk_very_low_free_space	2000004	Disk space level is critically low. <field1> Kbytes are available.	Field1:free_space	major
xms_memory_low	2000012	XMS memory level is low. <field1> Kbytes are available.	Field1:free_memory	major
xms_memory_full	2000013	XMS has insufficient free memory: only <field1> Kbytes are available.	Field1:free_memeory	critical
xms_wrong_cn_true	2000102	XMS certificate contains wrong Common Name.		major
xms_disk_second_low_free_space	2000202	Disk space level of second partition is low. <field1> Kbytes are available.	Field1:free_disk_space_secondary	major
xms_disk_second_very_low_free_space	2000203	Disk space level of second partition is critically low. <field1> Kbytes are available.	Field1:free_disk_space_secondary	major
xms_disk_second_no_free_space	2000204	Not enough disk space for second partition. XMS will block most operations. only <field1> Kbytes are available.	Field1:free_disk_space_secondary	critical
ig_add_pending	2300102	The Initiator Group add request has not completed successfully.		minor
ig_modify_pending	2300103	The Initiator Group modification request has not completed successfully.		minor
ig_remove_pending	2300104	The Initiator Group remove request has not completed successfully.		minor
initiator_add_pending	2400102	The initiator is in an ambiguous state after an add request.		minor

Alerts and Events Details

Alert Name	Alert Code	Description	Field	Severity
initiator_modify_pending	2400103	The initiator is in an ambiguous state after a modification request.		minor
initiator_remove_pending	2400104	The initiator is in an ambiguous state after a removal request.		minor
scheduler_last_activation_failed	2500203	Last activation of scheduler has failed. Scheduler snapshot creation and deletion has been suspended.		major
scheduler_last_activation_obj_not_found	2500204	Last activation of scheduler has failed. Invalid source object of the scheduler.		major
scheduler_last_activation_vsg_max_reached	2500205	The number of volumes in a Volume Snapshot Group has reached the limit.		major
scheduler_last_activation_cluster_volumes_max_reached	2500206	The number of volumes in the cluster has reached the limit.		major

Events Details

Event Name	Event Code	Description	Field	Field Value	Event Category
SYSTEM_EXPANSION_IN_PROGRESS	02022	Cluster expansion in progress changed from <field1> to <field2>.	Field 1: old_value Field 2: cluster_expansion_i_n_progress	<ul style="list-style-type: none"> • no • yes 	State_Change
SYSTEM_SHAREDMEMORY_IN_USE_RATIO_LEVEL	02010	Shared memory space utilization is <field1> percent of the total shared memory pool. The shared memory utilization state is <field2>.	Field1: shared_memory_in_use_ratio	Integer: 0 - 100	Software
			Field2: shared_memory_in_use_ratio_level	<ul style="list-style-type: none"> • healthy • limited_free_space • very_limited_space • no_free_space 	Software
NODE_ETH_LINK_LEVEL	04039	ETH management link state was changed from <field1> to <field2>.	Field1:old_value Field2:eth_link_healh_level	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warining • level_4_minor • level_5_major • level_6_critical 	Software
NODE_SAS2_PORT_RATE	04036	SAS port 2 rate changed from <field1> to <field2>.	Field1:old_value Field2:sas2_port_rate	<ul style="list-style-type: none"> • 12gbps • 6gbps • 3gbps • down • unknown 	Hardware
NODE_INTERNAL_SENSOR_HEALTH	04015	Storage Controller internal processors health state was changed from <field1> to <field2>.	Field1:old_value Field2:internal_sensor_health_state	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Hardware
LOCAL_DISK_ENABLED_STATE	05002	The enabled state for the local disk was changed from <field1> to <field2>.	Field1:old_value Field2:enabled_state	<ul style="list-style-type: none"> • enabled • user_disabled • system_disabled 	State_Change
NODE_PSU_FRU_STATE	06003	Life cycle state of the Storage Controller PSU in <field1> was changed from <field2> to <field3>.	Field1:location	<ul style="list-style-type: none"> • left • right 	State_Change
			Field2:old_value Field3:fru_lifecycle_state	<ul style="list-style-type: none"> • healthy • initializing • failed • disconnected • uninitialized • prepare_failed 	

Event Name	Event Code	Description	Field	Field Value	Event Category
SSD_LINK1_HEALTH	09003	Link 1 state for SSD was changed from <field1> to <field2>.	Field1:old_value Field2:ssd_link1_health_state	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Software
SSD_FRU_FW_VERSION_STATE	09008	Firmware version of the SSD is <field1>. Current firmware version is <field2>.	Field1:fw_version_error	<ul style="list-style-type: none"> • no_error • upgrading • invalid_fw_version • mismatch_fw_version 	Software
			Field2:fw_version	Assigned fw version number	
IB_SWITCH_IB_PORT_PEER_GUID	14012	InfiniBand Switch port peer guide for port <field1> was changed.	Field1:port_index	<ul style="list-style-type: none"> • same • changed 	State_Change
JBOD_CONTROLLER_SAS_CONNECTIVITY_STATE	16003	DAE Controller SAS connectivity state was changed from <field1> to <field2>.	Field1:old_value Field2:sas_connectivity_state	<ul style="list-style-type: none"> • connected • disconnected • degraded 	State_Change
SYSTEM_HEALTH_STATE	02013	Cluster state was changed from <field1> to <field2>.	Field1:old_value Field2:sys_health_state	<ul style="list-style-type: none"> • healthy • partial_fault • degraded • failed 	State_Change
SYSTEM_UD_SSD_SPACE_LEVEL	02003	Free physical capacity is low. The cluster has only <field1> percent free storage capacity.	Field1:free_ud_ssd_space_in_percent	<ul style="list-style-type: none"> • healthy • limited_free_space • very_limited_free_space • no_free_space 	Software
SYSTEM_STATE	02005	Cluster state was changed from <field1> to <field2>.	Field1:old_value Field2:sys_state	<ul style="list-style-type: none"> • start • configured • initializing • active • stopping • stopped • starting • failed • unknown • down • stop_failed 	State_Change
SYSTEM_SYS_STOP_TYPE	02006	Cluster stop mode was changed from <field1> to <field2> state.	Field1:old_value Field2:sys_stop_type	<ul style="list-style-type: none"> • none • dae_stopped • stopped • failed_stop • unknown • stopping • dae_stopping 	Software

Event Name	Event Code	Description	Field	Field Value	Event Category
SYSTEM_SYS_STOPPED_REASON	02007	Cluster has stopped with the reason of <field1>.	Field1:stopped_reason	<ul style="list-style-type: none"> • none • multiple_disk_failure • dae_inaccessible • user_deactivated • multiple_ups_failures • double_node_in_brick_failure • restart_failure • sw_failure • hw_failure • ha_failure • ups_protect_limited • disk_mount_failure • power_off_button_pressed 	Software
SYSTEM_UPGRADE_STATE	02008	Cluster upgrade process has changed its state from <field1> to <field2>. <field3>	Field1:old_value	<ul style="list-style-type: none"> • no_upgrade_done • testing_validity • stopping_service • new_version_detected • upgrade_succeeded • bringing_up_new_version • waiting_for_new_version • preparing_system • upgrade_failed • rollback_in_progress 	State_Change
			Field2:upgrade_state	<ul style="list-style-type: none"> • String 	
SYSTEM_MANAGER_CONNECTION_STATUS	02009	The XMS connection to the Cluster Manager has changed to <field1>. Error reason is <field2>.	Field 1: sys_mgr_conn_status	<ul style="list-style-type: none"> • disconnected • connected • unknown 	State_Change
			Field 2: sys_mgr_conn_error_reason	<ul style="list-style-type: none"> • no_route_to_host • connection_reset_by_peer • connection_refused 	
SYSTEM_FC_PORT_SPEED	04034	FC port speed for targets changed from <field1> to <field2>.	Field1:old_value	<ul style="list-style-type: none"> • not_in_use • inconsistent • 1gfc • 8gfc • 10gfc • 16gfc 	State_Change
SYSTEM_SCSI_PORT_SPEED	04035	iSCSI port speed for targets changed from <field1> to <field2>.	Field1:old_value	<ul style="list-style-type: none"> • not_in_use • inconsistent • 10mb • 100mb • 1gb • 10gb • 40gb 	State_Change

Event Name	Event Code	Description	Field	Field Value	Event Category
SYSTEM_CONSISTENCY_STATE	02011	Cluster consistency state was changed from <field1> to <field2>.	Field1:old_value Field2:consistency_state	<ul style="list-style-type: none"> • healthy • error 	Software
SYSTEM_TP_LIMIT_CROSSING	02021	The cluster VAAI thin provisioning soft limit state is <field1>. The threshold is <field2> percent.	Field1:vaai_tp_limit_crossing	<ul style="list-style-type: none"> • healthy • threshold_exceeded 	Hardware
			Field2:vaai_tp_limit	Integer: 0 - 100	
BRICK_STATE	03001	X-Brick state was changed from <field1> to <field2>.	Field1:old_value Field2:brick_state	<ul style="list-style-type: none"> • in_sys • not_in_sys 	Software
BRICK_SLOT_STATE	03002	X-Brick DAE Slot <field1> state was changed from <field2> to <field3>.	Field1:ssd_slot_array[].slot_num	Integer: 1 - 25	Software
			Field2:old_value Field3:ssd_slot_array[].slot_state	<ul style="list-style-type: none"> • empty • resident_ssd • unsupported_disk • uninitialized_ssd • foreign_xtremapp_ssd • error 	
NODE_ETH_PORT_RATE	04038	ETH management port rate changed from <field1> to <field2>	Field1:old_value Field2:sas1_port_rate	<ul style="list-style-type: none"> • 10mb • 100mb • 1gb • 10gb • 40gb 	Hardware
NODE_HEALTH_STATE	04048	Storage Controller's state was changed from <field1> to <field2>.	Field1:old_value Field2:node_health_state	<ul style="list-style-type: none"> • healthy • partial_fault • degraded • failed 	State_Change
NODE_STATE	04001	The Storage Controller state was changed from <field1> to <field2>.	Field1:old_value Field2:node_state	<ul style="list-style-type: none"> • active • not_in_sys • prepared_decoupled • stopping • stopped • starting • failed 	State_Change
SAS_HBA_DOWN	04002	State of the Storage Controller SAS port 1 (connected to DAE) was changed from <field1> to <field2>.	Field1:old_value Field2:sas1_port_state	<ul style="list-style-type: none"> • up • down • unknown • system_disabled 	State_Change
SAS_HBA_DOWN2	04003	State of the storage Controller SAS HBA 2 (connected to DAE) was changed from <field1> to <field2>.	Field1:old_value Field2:sas2_port_state	<ul style="list-style-type: none"> • up • down • unknown • system_disabled 	Hardware

Event Name	Event Code	Description	Field	Field Value	Event Category
NODE_SAS1_PORT_RATE	04004	SAS port 1 rate changed from <field1> to <field2>.	Field1:old_value Field2:sas1_port_rate	<ul style="list-style-type: none"> • 12gbps • 6gbps • 3gbps • down • unknown 	Hardware
NODE_MGR_CONN_STATE	04005	XMS connection to the Storage Controller was changed to <field1>.	Field1:node_mgr_conn_state	<ul style="list-style-type: none"> • connected • controlled_disconnect • disconnected • unknown 	State_Change
NODE_JOURNAL_HEALTH_STATE	04007	Storage Controller journal state was changed from <field1> to <field2>.	Field1:old_value Field2:node_journaling_health_state	<ul style="list-style-type: none"> • healthy • ready • fault • dumping 	Software
NODE_LOW_RAM_LEVEL	04009	Storage Controller's available RAM is insufficient. The required RAM level is <field1>. The current RAM level is <field2>.	Field1:expected_ram	Integer (MB)	Hardware
			Field2:ram	Integer (MB)	
NODE_TEMPERATURE_HEALTH	04011	Storage Controller IPMI temperature health state changed from <field1> to <field2>.	Field1:old_value Field2:temperature_health_state	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Hardware
NODE_FAN_HEALTH	04012	Storage Controller fan health state was changed from <field1> to <field2>.	Field1:old_value Field2:fan_health_state	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Hardware
NODE_VOLTAGE_HEALTH	04013	Storage Controller IPMI voltage health state was changed from <field1> to <field2>.	Field1:old_value Field2:voltage_health_state	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Hardware
NODE_CURRENT_HEALTH	04014	Storage Controller IPMI current health state was changed from <field1> to <field2>.	Field1:old_value Field2:current_health_state	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Hardware

Event Name	Event Code	Description	Field	Field Value	Event Category
DIMM_HEALTH	04033	Storage Controller memory card (DIMM) health state has changed from <field1> to <field2>.	Field1:old_value Field2:dimm_health_state	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Hardware
NODE_ETH_PORT_STATE	04016	Storage Controller management port state was changed from <field1> to <field2>.	Field1:old_value Field2:eth_port_state	<ul style="list-style-type: none"> • up • down • unknown 	State_Change
NODE_IB1_LINK_LEVEL	04017	Storage Controller link 1 InfiniBand network state was changed from <field1> to <field2>.	Field1:old_value Field2:ib1_link_health_level	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	State_Change
NODE_IB1_PORT_MISCONNECTION	04018	Storage Controller InfiniBand port 1 connection state was changed from <field1> to <field2>.	Field1:old_value Field2:ib1_port_misconnection	<ul style="list-style-type: none"> • healthy • wrong_port • wrong_switch 	Software
NODE_IB1_PORT_STATE	04019	Storage Controller InfiniBand port 1 state was changed from <field1> to <field2>.	Field1:old_value Field2:ib1_port_state	<ul style="list-style-type: none"> • up • down • unknown 	State_Change
NODE_IB2_LINK_LEVEL	04021	Storage Controller link 2 InfiniBand network state was changed from <field1> to <field2>.	Field1:old_value Field2:ib2_link_health_level	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Software
NODE_IB2_PORT_MISCONNECTION	04022	Storage Controller InfiniBand port 2 connection state was changed from <field1> to <field2>.	Field1:old_value Field2:ib2_port_misconnection	<ul style="list-style-type: none"> • healthy • wrong_port • wrong_switch 	Software
NODE_IB2_PORT_STATE	04023	Storage Controller InfiniBand port 2 state was changed from <field1> to <field2>.	Field1:old_value Field2:ib2_port_state	<ul style="list-style-type: none"> • up • down • unknown 	State_Change
NODE_SAS1_HBA_LINK_LEVEL	04041	Storage Controller SAS port 1 state was changed from <field1> to <field2>.	Field1:old_value Field2:sas1_hba_port_health_level	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Hardware

Event Name	Event Code	Description	Field	Field Value	Event Category
NODE_SAS2_HBA_LINK_LEVEL	04042	Storage Controller SAS port 2 state was changed from <field1> to <field2>.	Field1:old_value Field2:sas2_hba_port_health_level	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Hardware
NODE_UPGRADE_STATE	04024	Storage Controller upgrade state was changed from <field1> to <field2>. <field3>.	Field1:old_value Field2:upgrade_state	<ul style="list-style-type: none"> • no_upgrade_done • upgrade_succeeded • upgrade_in_progress • upgrade_failed 	State_Change
			Field3:upgrade_failure_reason	<ul style="list-style-type: none"> • String 	
NODE_STOP_TYPE	04025	Storage Controller stop type was changed from <field1> to <field2>; <field3>	Field1:old_value Field2:node_stop_type	<ul style="list-style-type: none"> • none • dae_stopped • stopped • failed_stop • dae_stopping • stopping • replaced 	Software
			Field3:node_stop_reason	<ul style="list-style-type: none"> • lost_connectivity_with_node • initiated_locally_by_node • critical_process_died • xms_initiated_emergency_shutdown • pm_initiated_emergency_shutdown • user_deactivated • orderly_shutdown_fail • xms_initiated_orderly_shutdown • fw_upgrade • node_initiated_emergency_shutdown • lost_connectivity_with_ib_switch • lost_connectivity_with_other_node • node_backend_storage_controller_state 	
NODE_ENABLED_STATE	04026	The enabled state for the Storage Controller has changed from <field1> to <field2>.	Field1:old_value Field2:enabled_state	<ul style="list-style-type: none"> • enabled • user_disabled • system_disabled 	State_Change

Event Name	Event Code	Description	Field	Field Value	Event Category
NODE_FRU_STATE	04027	Storage Controller life cycle state was changed from <field1> to <field2>.	Field1:old_value Field2:fru_lifecycle_state	<ul style="list-style-type: none"> • healthy • initializing • failed • disconnected • uninitialized • prepare_failed 	State_Change
NODE_FRU_FW_VERSION_STATE	04028	Storage Controller software or firmware version is <field1>.	Field1:fw_version_error	<ul style="list-style-type: none"> • no_error • upgrading • invalid_fw_version • mismatch_fw_version 	Software
LOCAL_DISK_DISK_FAILURE	05001	Storage Controller local disk in slot <field1> was changed from <field2> to <field3>.	Field1:slot_num	Integer: 1 - 8	Hardware
			Field2:old_value Field3:disk_failure	<ul style="list-style-type: none"> • ok • empty • unanticipated_disk • unsupported_disk • error • uninitialized 	
LOCAL_DISK_FRU_STATE	05003	Life cycle state of the Storage Controller local disk has changed from <field1> to <field2>.	Field1:old_value Field2:fru_lifecycle_state	<ul style="list-style-type: none"> • healthy • initializing • failed • disconnected • uninitialized • prepare_failed 	State_Change
LOCAL_DISK_FRU_FW_VERSION_STATUS	05004	Firmware version of the Storage Controller local disk is <field1>. Current firmware version is <field2>.	Field1:fw_version_error	<ul style="list-style-type: none"> • no_error • upgrading • invalid_fw_version • mismatch_fw_version 	Software
			Field2:fw_version	<ul style="list-style-type: none"> • Assigned fw version number 	
NODE_PSU_POWER_FAILURE	06001	Storage Controller PSU in <field1> has <field2>.	Field1:location	<ul style="list-style-type: none"> • left • right 	Hardware
			Field2:power_failure	<ul style="list-style-type: none"> • clear • unknown • warning • minor • major • critical 	
NODE_PSU_ENABLED_STATE	06002	The enabled state of the Storage Controller PSU has changed from <field1> to <field2>.	Field1:old_value Field2:enabled_state	<ul style="list-style-type: none"> • enabled • user_disabled • system_disabled 	State_Change

Event Name	Event Code	Description	Field	Field Value	Event Category
NODE_PSU_FRU_FW_VERSION_STATE	06004	Storage Controller PSU firmware version is <field1>. Current firmware version is <field2>.	Field1:fw_version_error	<ul style="list-style-type: none"> • no_error • upgrading • invalid_fw_version • mismatch_fw_version 	Software
			Field2:fw_version	Assigned fw version number	
NODE_PSU_INPUT	06007	Input State of the Storage Controller PSU in <field1> was changed to <field2>.	Field1:location	<ul style="list-style-type: none"> • left • right 	Software
			Field2:input	<ul style="list-style-type: none"> • uninitialized • off • on 	
RG_PROTECTION_STATE	08001	DPG group protection state was changed from <field1> to <field2>.	Field1:old_value Field2:protection_state	<ul style="list-style-type: none"> • normal • degraded • dual_failure • error • initializing • double_degraded 	Software
RG_REBUILD_IN_PROGRESS	08002	DPG rebuild is in progress. At least <field1> percent completed. User data space in use=<field2>	Field1:rebuild_progress	Integer: 0 - 100	Software
			Field2:ud_ssd_space_in_use	<ul style="list-style-type: none"> • done • 0_to_20_percent_done • 20_to_40_percent_done • 40_to_60_percent_done • 60_to_80_percent_done • 99_percent_done 	
RG_SSD_PREPARATION_IN_PROGRESS	08003	DPG group is preparing the SSD to be introduced into the DPG. <field1> percent of the process has been completed.	Field1:ssd_preparation_progress	<ul style="list-style-type: none"> • done • 0_to_20_percent_done • 20_to_40_percent_done • 40_to_60_percent_done • 60_to_80_percent_done • 99_percent_done 	Software
RG_REBALANCE_IN_PROGRESS	08009	DPG group rebalance is in progress. <field1> percent of the process has been completed.	Field1:rebalance_progress	<ul style="list-style-type: none"> • done • zero_to_20_percent_done • 20_to_40_percent_done • 40_to_60_percent_done • 60_to_80_percent_done • 99_percent_done 	Software

Event Name	Event Code	Description	Field	Field Value	Event Category
RG_AVAILABE_REBUILDS	08004	DPG number of available rebuilds was changed from <field1> to <field2>.	Field1:old_value Field2:available_rebuilds	<ul style="list-style-type: none"> • 0 • 1 • 2 • 3 • 4 • 5 	Software
RG_UD SSD_SPACE_LEVEL	08005	DPG group has low free capacity. The available free capacity is <field1> percent.	Field1:rg_ud_ssd_percent_free_space	Integer: 0 - 100	Software
VOLUME_SMALL_IO_RATIO	08006	The volume small block I/O ratio changed from <field1> to <field2>. The ratio is <field3> percent.	Field1:old_value Field2:small_io_ratio_level	<ul style="list-style-type: none"> • ok • low • medium • high 	Software
			Field3:small_io_ratio	Integer: 0 - 100	
VOLUME_UNALIGNED_IO_RATIO	08007	The unaligned block I/O ratio changed from <field1> to <field2>. The ratio is <field3> percent.	Field1:old_value Field2:unaligned_io_ratio_level	<ul style="list-style-type: none"> • ok • low • medium • high 	Software
			Field3:unaligned_io_ratio	Integer: 0 - 100	
SSD_RG_STATE	09001	SSD state was changed from <field1> to <field2>.	Field1:old_value Field2:ssd_state	<ul style="list-style-type: none"> • in_rg • not_in_rg • failed_in_rg • eject_pending • assigning_to_rg 	Software
SSD_ENDURANCE_REMAINING	09012	SSD wear level (Endurance) for SSD was changed to <field1>.	Field1:percent_endurance_remaining_level	Integer: 0 - 100	Hardware
SSD_DIAGNOSTIC_HEALTH	09002	SSD diagnostic state was changed from <field1> to <field2>.	Field1:old_value Field2:diagnostic_health_state	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Hardware
SSD_LINK2_HEALTH	09004	Link 2 state for SSD was changed from <field1> to <field2>.	Field1:old_value Field2:ssd_link2_health_state	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Software

Event Name	Event Code	Description	Field	Field Value	Event Category
SSD_ENABLED_STATE	09006	The enabled state for the SSD has changed from <field1> to <field2>.	Field1:old_value Field2:enabled_state	<ul style="list-style-type: none"> • enabled • user_disabled • system_disabled 	State_Change
SSD_FRU_STATE	09007	SSD lifecycle state was changed from <field1> to <field2>.	Field1:old_value Field2:fru.lifecycle_state	<ul style="list-style-type: none"> • healthy • initializing • failed • disconnected • uninitialized • prepare_failed • trigger_update 	State_Change
TARGET_TAR_ERROR_REASON	11002	Target port error <field1> was detected.	Field1:error_reason	<ul style="list-style-type: none"> • none • not_found • fc_counters 	Software
TARGET_PORT_STATE	11003	Target port state was changed from <field1> to <field2>.	Field1:old_value Field2:port_state	<ul style="list-style-type: none"> • up • down • unknown 	State_Change
TARGET_TAR_HEALTH_STATE	11004	Target health state was changed from <field1> to <field2>.	Field1:old_value Field2:port_state	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Software
XENV_STATE	12001	Xenv state was changed from <field1> to <field2>.	Field1:old_value Field2:xenv_state	<ul style="list-style-type: none"> • inactive • boot • init • active • failed • invalid • failover • fallback 	State_Change
MODULE_STATE	13001	Internal sub-process (module) state was changed from <field1> to <field2>.	Field1:old_value Field2:mdl_state	<ul style="list-style-type: none"> • active • xenv_boot • init • inactive • failed • failover • fallback 	State_Change
IB_SWITCH_LINK_HEALTH_LEVEL	14001	InfiniBand Switch link state for port <field1> was changed from <field2> to <field3>.	Field1:port_index	Integer: 0 - 17	Software
			Field2:old_value Field3:ports[].ib_link_health_level	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	

Event Name	Event Code	Description	Field	Field Value	Event Category
IB_SWITCH_S2S_1_PORT_STATE	14008	InfiniBand Switch port state for InfiniBand Switch-to-InfiniBand Switch port 17 has changed from <field1> to <field2>.	Field1:old_value Field2:inter_switch_ib1_port_state	<ul style="list-style-type: none"> • down • active • reconnecting • unknown 	State_Change
IB_SWITCH_S2S_2_PORT_STATE	14009	InfiniBand Switch port state for InfiniBand Switch-to-InfiniBand Switch port 18 has changed from <field1> to <field2>.	Field1:old_value Field2:inter_switch_ib2_port_state	<ul style="list-style-type: none"> • down • active • reconnecting • unknown 	State_Change
IB_SWITCH_IB_PORT_STATE	14002	InfiniBand Switch port state for port <field1> was changed from <field2> to <field3>.	Field1:port_index	Integer: 0 - 17	State_Change
			Field2:old_value Field3:ports[].port_state	<ul style="list-style-type: none"> • down • up • unknown 	
IB_SWITCH_ENABLED_STATE	14003	InfiniBand Switch state was changed from <field1> to <field2>.	Field1:old_value Field2:enabled_state	<ul style="list-style-type: none"> • enabled • user_disabled • system_disabled 	State_Change
IB_SWITCH_FRU_STATE	14004	InfiniBand Switch lifecycle state was changed from <field1> to <field2>.	Field1:old_value Field2:fru_lifecycle_state	<ul style="list-style-type: none"> • healthy • initializing • failed • disconnected • uninitialized • prepare_failed 	State_Change
IB_SWITCH_FRU_FW_VERSION_STATE	14005	InfiniBand Switch firmware version is <field1>. Current firmware version is <field2>.	Field1:fw_version_error	<ul style="list-style-type: none"> • no_error • upgrading • invalid_fw_version • mismatch_fw_version 	Software
			Field2:fw_version	Assigned fw version number	
UPS_LOAD_PERCENT	15001	BBU load state was changed from <field1> to <field2>.	Field1:old_value Field2:ups_load_percent_level	<ul style="list-style-type: none"> • ok • no_load • no_threshold_crossed • med_threshold_crossed • high_threshold_crossed 	Hardware
UPS_CONN_STATE	15002	BBU connection state was changed from <field1> to <field2>.	Field1:old_value Field2:ups_conn_state	<ul style="list-style-type: none"> • connected • disconnected • sc_1_disconnected • sc_2_disconnected • n_r 	State_Change
UPS_INPUT	15004	BBU external power feed state has changed from <field1> to <field2>.	Field1:old_value Field2:ups_input	<ul style="list-style-type: none"> • on • off 	Software

Event Name	Event Code	Description	Field	Field Value	Event Category
UPS_LOW_BATTERY_HAS_INPUT	15005	State of the Backup Battery Unit (with power input feed) Low Battery Level was changed from <field1> to <field2>. Current battery charge level is <field3>.	Field1:old_value Field2:is_low_battery_has_input	<ul style="list-style-type: none"> • false • true • invalid_state 	Software
			Field3:is_low_battery_has_input	<ul style="list-style-type: none"> • Integer 	
UPS_LOW_BATTERY_NO_INPUT	15006	State of the Battery Backup Unit (without power input feed) Low Battery Level was changed from <field1> to <field2>.	Field1:old_value Field2:is_low_battery_no_input	<ul style="list-style-type: none"> • false • true • invalid_state 	Software
UPS_LOW_BATTERY_RUNTIME	15007	Battery Backup Unit low runtime state has changed from <field1> to <field2>. Current battery runtime value is: <field3> seconds.	Field1:old_value Field2:is_low_battery_runtime	<ul style="list-style-type: none"> • false • true • invalid_state 	Software
			Field3:battery_runtime	<ul style="list-style-type: none"> • Integer 	
UPS_OVERLOAD	15008	State of the Battery Backup Unit input overload has changed from <field1> to <field2>. Current BBU load is: <field3>	Field1:old_value Field2:is_low_battery_runtime	<ul style="list-style-type: none"> • false • true • invalid_state 	Software
			Field3:ups_load_in_percent	<ul style="list-style-type: none"> • Integer 	
UPS_BYPASS_ACTIVE	15011	State of the Battery Backup Unit bypass mode was changed from <field1> to <field2>.	Field1:old_value Field2:is_bypass_active	<ul style="list-style-type: none"> • false • true • invalid_state 	Software
UPS_NEEDS_BATTERY_REPLACEMENT	15013	Battery Backup Unit replacement requirement state has changed from <field1> to <field2>.	Field1:old_value Field2:ups_need_battery_replacement	<ul style="list-style-type: none"> • false • true • invalid_state 	Hardware
UPS_ENABLED_STATE	15014	The enabled state for the Battery Backup Unit has changed from <field1> to <field2>.	Field1:old_value Field2:enabled_state	<ul style="list-style-type: none"> • user_disabled • enabled • system_disabled 	State_Change
UPS_FRU_STATE	15015	Life cycle state of the BBU was changed from <field1> to <field2>.	Field1:old_value Field2:fru_lifecycle_state	<ul style="list-style-type: none"> • healthy • initializing • failed • disconnected • uninitialized • prepared_failed 	State_Change

Event Name	Event Code	Description	Field	Field Value	Event Category
UPS_FRU_FW_VERSION_STATE	15016	Firmware version of the BBU is <field1>. Current firmware version is <field2>.	Field1:fw_version_error	<ul style="list-style-type: none"> • no_error • upgrading • invalid_fw_version • mismatch_fw_version 	Software
			Field2:fw_version	Assigned fw version number	
JBOD_CONTROLLER_SAS1_PORT_STATE	16002	DAE Controller SAS Port 1 port state has changed from <field1>to <field2>.	Field1:old_value Field2:sas1_port_state	<ul style="list-style-type: none"> • up • down • unknown 	State_Change
JBOD_CONTROLLER_SAS2_PORT_STATE	16011	DAE Controller SAS Port 2 port state has changed from <field1>to <field2>.	Field1:old_value Field2:sas2_port_state	<ul style="list-style-type: none"> • up • down • unknown 	State_Change
JBOD_CONTROLLER_ENABLED_STATE	16004	State of the <field1> DAE Controller was changed from <field2> to <field3>.	Field1:location	<ul style="list-style-type: none"> • left • right • uninitialized (if the system cannot determine the DAE Controller port) 	State_Change
			Field2:old_value Field3:enabled_state	<ul style="list-style-type: none"> • enabled • user_disabled • system_disabled 	
JBOD_CONTROLLER_FRU_STATE	16005	Life cycle state of the <field1> DAE Controller was changed from <field2> to <field3>.	Field1:location	<ul style="list-style-type: none"> • left • right • uninitialized (if the system cannot determine the DAE Controller port) 	State_Change
			Field2:old_value Field3:fru_lifecycle_state	<ul style="list-style-type: none"> • healthy • initializing • failed • disconnected • uninitialized • prepare_failed 	
JBOD_CONTROLLER_FRU_FW_VERSION_STATE JBOD_CONTROLLER_HEALTH_LEVEL	16006	Firmware version of the <field1> DAE Controller is <field2>. Current firmware version is <field3>.	Field1:location	<ul style="list-style-type: none"> • left • right • uninitialized (if the system cannot determine the DAE Controller port) 	Software
			Field2:fw_version_error	<ul style="list-style-type: none"> • no_error • upgrading • invalid_fw_version • mismatch_fw_version 	
			Field3:fw_version	<ul style="list-style-type: none"> • Assigned fw version number 	

Event Name	Event Code	Description	Field	Field Value	Event Category
JBOD_CONTROLLER_HEALTH_LEVEL	16009	DAE Controller health state was changed from <field1> to <field2>.	Field1:old_value Field2:lcc_health_level	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Hardware
JBOD_PSU_INPUT	17001	Input state of the DAE PSU in <field1> was changed to <field2>.	Field1:location	<ul style="list-style-type: none"> • top • bottom • left • right 	Hardware
			Field2:input	<ul style="list-style-type: none"> • off • on 	
JBOD_PSU_POWER_FAILURE	17007	The <field1> DAE PSU has <field2>.	Field1:location	<ul style="list-style-type: none"> • top • bottom • left • right 	Hardware
			Field2:power_failure	<ul style="list-style-type: none"> • no_error • ac_lost • ac_out_of_range • failure_detected 	
JBOD_PSU_ENABLED_STATE	17002	State of the <location> DAE PSU was changed from <field1> to <field2>.	Field1:location	<ul style="list-style-type: none"> • top • bottom • left • right 	State_Change
			Field2:old_value Field3:enabled_state	<ul style="list-style-type: none"> • enabled • user_disabled • system_disabled 	
JBOD_PSU_FRU_STATE	17003	Life cycle state of the <field1> DAE PSU was changed from <field2> to <field3>.	Field1:location	<ul style="list-style-type: none"> • top • bottom • left • right 	State_Change
			Field2:old_value Field3:fru_lifecycle_state	<ul style="list-style-type: none"> • healthy • initializing • failed • disconnected • uninitialized • prepare_failed 	
IB_SWITCH_INPUT	17015	InfiniBand Switch PSU input state was changed from <field1> to <field2>.	Field1:old_value Field2:input	<ul style="list-style-type: none"> • on • off 	Software
IB_SWITCH_PSU_ENABLED_STATE	17008	InfiniBand Switch PSU state was changed from <field1> to <field2>.	Field1:old_value Field2:enabled_state	<ul style="list-style-type: none"> • enabled • user_disabled • system_disabled 	State_Change

Event Name	Event Code	Description	Field	Field Value	Event Category
IB_SWITCH_PSU_FRU_STATE	17009	Lifecycle state of the <field 1> InfiniBand Switch PSU has changed from <field 2> to <field 3>.	Field 1:location Field 2:old_value Field 3: fru_lifecycle_state	<ul style="list-style-type: none"> • left • right <ul style="list-style-type: none"> • healthy • initializing • failed • disconnected • uninitialized • prepared_failed 	State_Change
JBOD_PSU_FRU_FW_VERSION_STATE	17004	Firmware version of the <field 1> DAE PSU is <field 2>. Current firmware version is <field 3>.	Field 1: location Field 2: fw_version_error Field 3: fw_version	<ul style="list-style-type: none"> • left • right <ul style="list-style-type: none"> • no_error • upgrading • invalid_fw_version • mismatch_fw_version <ul style="list-style-type: none"> • Assigned fw version number 	Software
JBOD_FRU_STATE	18003	DAE life cycle state was changed from <field1> to <field2>.	Field1:old_value Field2:fru_lifecycle_state	<ul style="list-style-type: none"> • healthy • initializing • failed • disconnected • uninitialized • prepared_failed 	State_Change
SYSTEM_SYS_SC_PWR_BUTTONS	02026	Power button pressed state changed from <field1> to <field2>.	Field 1: old_value Field 2: sc_power_buttons	<ul style="list-style-type: none"> • not_pressed • shutdown_request • shutdown_not_available 	State_Change
SYS_SSD_HI_UTILIZATION_THLD_CROSSING	02037	Threshold crossing of SSD high utilization threshold: Value changed to <field1>. There are <field2> KB remaining.	Field 1: ssd_high_utilization_thld_crossing Field 2: free_ud_ssd_space	<ul style="list-style-type: none"> • healthy • exceeded 	user_threshold
SYS_SSD_VERY_HI_UTILIZATION_THLD_CROSSING	02038	Threshold crossing of SSD very high utilization: Value changed to <field1>. There are <field2> KB remaining.	Field 1: ssd_very_high_utilization_thld_crossing Field 2: ud_free_ssd_space_in_kb)	<ul style="list-style-type: none"> • healthy • exceeded 	
SYSTEM_ENCRYPT_SWITCH	02023	Cluster state was changed from <field1> to <field2>.	Field 1: old_value Field 2: sys_health_state	<ul style="list-style-type: none"> • none • during_switch • switch_incomplete • switch_failed 	State_Change
CONSISTENCY_GROUP_CERTAINTY	08008	Consistency Group's state was changed from <field1> to <field2>.	Field 1: old_value Field 2: certainty_state	<ul style="list-style-type: none"> • ok • add_pending • modify_pending • remove_pending 	Software

Event Name	Event Code	Description	Field	Field Value	Event Category
DIMM_HEALTH	04033	Storage Controller memory card (DIMM) health state was changed from <field1> to <field2>.	Field 1: old_value Field 2: dimm_health_state	<ul style="list-style-type: none"> • level_1_clear • level_2_unknown • level_3_warning • level_4_minor • level_5_major • level_6_critical 	Hardware
DPG_PROACTIVE_METADATA_LOADING	08010	State of the DPG proactive metadata loading in progress changed from <field1> to <field2>.	Field 1: old_value Field 2: proactive_metadata_loading	<ul style="list-style-type: none"> • false • initial_state • final_state 	Software
IB_SWITCH_WRONG_SC_CONNECTION	14005	Incorrect connection between Storage Controller(s) and InfiniBand Switch found: <field1>.	Field 1: wrong_sc_connection_detected)	<ul style="list-style-type: none"> • none • yes 	Hardware
IG_CERTAINTY_STATE	23001	IG's state was changed from <field1> to <field2>.	Field 1: old_value Field 2: certainty_state	<ul style="list-style-type: none"> • ok • add_pending • modify_pending • remove_pending 	Software
INITIATOR_CERTAINTY_STATE	24001	Initiator's state was changed from <field1> to <field2>.	Field 1: old_value Field 2: certainty_state	<ul style="list-style-type: none"> • ok • add_pending • modify_pending • remove_pending 	Software
INITIATOR_CHAP_AUTHENTICATION	02025	State of the Authentication CHAP, some initiators missing credentials state was changed from <field1> to <field2>.	Field 1: old_value Field 2: authentication_chap_initiators_missing_credentials	<ul style="list-style-type: none"> • false • true 	State_Change
INITIATOR_CHAP_CLUSTER_AUTHENTICATION	02024	State of the discovery CHAP some initiators missing cluster credentials was changed from <field1> to <field2>.	Field 1: old_value Field 2: authentication_chap_initiators_missing_cluster_credentials	<ul style="list-style-type: none"> • false • true 	State_Change
INITIATOR_CHAP_DISCOVERY	19011	State of the discovery CHAP some initiators missing credentials was changed from <field1> to <field2>.	Field 1: old_value Field 2: discovery_chap_initiators_missing_credentials	<ul style="list-style-type: none"> • false • true 	Software
MODE_ISCSI_DAEMON_STATE	06008	Storage Controller iSCSI daemon state changed from <field1> to <field2>.	Field 1: old_value Field 2: iscsi_daemon_state	<ul style="list-style-type: none"> • healthy • failed 	Software
NODEDED_IPMI_LINK_STATE	04046	Dedicated ETH management for IPMI link state was changed from <field1> to <field2>.	Field 1: old_value Field 2: dedicated_ipmi_link_conn_state	<ul style="list-style-type: none"> • ok • invalid_wiring • disconnected 	Software

Event Name	Event Code	Description	Field	Field Value	Event Category
NODEDED_IPMI_PORT_STATE	04049	Storage Controller dedicated IPMI management port state was changed from <field1> to <field2>.	Field 1: old_value Field 2: dedicated_ipmi_port_state	<ul style="list-style-type: none"> • up • down • unknown 	State_Change
NODE_DISCOVERY_BBU	04057	Cluster has found new BBU. Replace procedure is required.	Field 1: ups_discovery_needed	<ul style="list-style-type: none"> • false • true 	Hardware
NODE_DISCOVERY_DAE	04050	Cluster has discovered new DAE hardware. Replace procedure is required.	Field 1: jbod_dn	<ul style="list-style-type: none"> • false • true 	Hardware
NODE_DISCOVERY_DAE_CTRL	04056	Cluster has found new DAE Controller. Replace procedure is required.	Field 1: jbod_lcc_discovery_needed	<ul style="list-style-type: none"> • false • true 	Hardware
NODE_DISCOVERY_DAE_PSU	04051	Cluster has found new DAE PSU. Replace procedure is required	Field 1: jbod_psu_dn	<ul style="list-style-type: none"> • false • true 	Hardware
NODE_DISCOVERY_IBSW	04052	Cluster has found new InB Switch. Replace procedure is required.	Field 1: ib_switches_dn	<ul style="list-style-type: none"> • false • true 	Hardware
NODE_DISCOVERY_LOCALDISK	04053	Cluster has found Local Disk. Replace procedure is required.	Field 1: local_disk_dn	<ul style="list-style-type: none"> • false • true 	Hardware
NODE_DISCOVERY_SCPSU	04054	Cluster has found Storage Controller PSU. Replace procedure is required.	Field 1: node_psu_dn	<ul style="list-style-type: none"> • false • true 	Hardware
NODE_DISK_SPACE_UTILIZATION_LEVEL	04061	Storage Controller Disk space is <field 1> Kbytes. The disk space utilization state is <field 2>.	Field 1: free_disk_space Field 2: disk_space_utilization_level	<ul style="list-style-type: none"> • Integer • healthy • limited_free_space • no_free_space 	Software
NODE_FP_TEMPERATURE_STATE	04045	Storage Controller front panel temperature sensor was changed from <field1> to <field2>.	Field 1: old_value Field 2: node_fp_temperature_state	<ul style="list-style-type: none"> • normal • warning • high • invalid 	Hardware
NODE_HIGH_FILE_DESCRIPTORS	04029	Storage Controller has high number of file descriptors.	Field 1: node_high_file_descriptors	<ul style="list-style-type: none"> • ok • high_file_descriptors 	Software

Event Name	Event Code	Description	Field	Field Value	Event Category
NODE_JOURNAL_STATE	04047	Storage Controller journal state was changed from <field1> to <field2>.	Field 1: old_value Field 2: journal_state	<ul style="list-style-type: none"> • healthy • failed • failover • fallback 	Software
NODE_MGM_PORT_DUPLEX_LEVEL		Storage Controller management port duplex setting was changed to <field 1>.	Field 1: mgmt_port_duplex	<ul style="list-style-type: none"> • full • half 	Hardware
NODE_PWR_BUTTONS	04059	Power button pressed state changed from <field1> to <field2>.	Field 1: old_value Field 2: sc_power_buttons	<ul style="list-style-type: none"> • not_pressed • short_press_2_sc • short_press_1_sc • long_press_1_sc 	State_Change
NODE_SAS1_MISCONFIG	04041	Storage Controller SAS port 1 (connected to DAE) connectivity issue was <field1> and is now <field2>.	Field 1: old_value Field 2: sas1_port_misconfiguration	<ul style="list-style-type: none"> • none • wrong_lcc • wrong_lcc_port • unknown_dae 	Hardware
NODE_SAS2_MISCONFIG	04055	Storage Controller SAS port 2 (connected to DAE) connectivity issue was <field1> and is now <field2>.	Field 1: old_value Field 2: sas2_port_misconfiguration	<ul style="list-style-type: none"> • none • wrong_lcc • wrong_lcc_port • unknown_dae 	Hardware
NODE_TECH_TUNNEL	04070	State of Technician Tunnel to XMS was changed from <field1> to <field2>.	Field 1: old_value Field 2: tunnel_state	<ul style="list-style-type: none"> • closed • opened 	Software
SCHEDULER_LAST_ACTIVATION_STATUS	25002	Last activation state of scheduler was changed from <field1> to <field2>.	Field 1: old_value Field 2: last_activation_status	<ul style="list-style-type: none"> • successful • never_run • failed • snapped_object_not_found • max_volumes_in_vsg_reached • max_volumes_in_cluster_reached 	State_Change
SCHEDULER_STATE	25001	Scheduler state was changed from <field1> to <field2>.	Field 1: old_value Field 2: scheduler_state	<ul style="list-style-type: none"> • enabled • user_disabled • 	State_Change
SNAPSHOT_GROUP_CERTAINTY_STATUS	19001	Volume Snapshot Group's state was changed from <field1> to <field2>.	Field 1: old_value Field 2: certainty_state	<ul style="list-style-type: none"> • ok • add_pending • modify_pending • remove_pending 	Software
SSD_CERTAINTY_STATE	09011	SSD state was changed from <field1> to <field2>.	Field 1: old_value Field 2: certainty_state	<ul style="list-style-type: none"> • ok • add_pending • modify_pending • remove_pending 	Software

Event Name	Event Code	Description	Field	Field Value	Event Category
SYS_SSD_HI_UTILIZATION_THLD_CROSSING	02037	Threshold crossing of SSD high utilization threshold: Value changed to <field 1>. There are <field 2>KB remaining.	Field 1: ssd_high_utilization_thld_crossing	• Integer	user_threshold
			Field 2: ud_free_ssd_space_in_kb	• healthy • exceeded	
SYS_SSD_VERY_HI_UTILIZATION_THRESHOLD_CROSSING	02037	Threshold crossing of SSD very high utilization threshold: Value changed to <field 1>. There are <field 2>KB remaining.	Field 1: ssd_very_high_utilization_thld_crossing	• Integer	user_threshold
			Field 2: ud_free_ssd_space_in_kb	• healthy • exceeded	
SYSTEM_ENCRYPT_SWITCH	02023	Data at Rest Encryption mode is being changed from <field1> to <field2>.	Field 1: old_value Field 2: mode_switch_status	• none • during_switch • switch_incomplete • switch_failed	State_Change
SYSTEM_HW_PKG_CONSISTENCY	02031	State of hardware package ids was changed from <field1> to <field2>.	Field 1: old_value Field 2: hardware_package_consistency	• inconsistent • consistent	State_Change
SYSTEM_NOTIFIER	04062	Event notifiers changed from <field1> to <field2>.	Field 1: old_value Field 2: under_maintenance	• false • true	State_Change
SYSTEM_OS_UPGRADE	04058	Storage Controller's OS upgrade is in progress.	Field 1: os_upgrade_in_progress	• false • true	State_Change
SYSTEM_SHAREDMEMORY_EFFICIENCY_LEVEL	02020	Shared memory efficiency level changed from <field1> to <field2>.	Field 1: old_value Field 2: shared_memory_efficiency_level	• healthy • medium_inefficiency • high_inefficiency	State_Change
SYSTEM_UD_SSD_SPACE_LEVEL	02003	Free physical capacity is low. The cluster has only <field 1> percent free storage capacity.	Field 1: free_ud_ssd_space_level	• Integer	Software
TARGET_CERTAINTY_STATE	11005	Target's state was changed from <field1> to <field2>.	Field 1: old_value Field 2: certainty_state	• ok • add_pending • modify_pending • remove_pending	Software
VOLUME_CERTAINTY_STATE	08008	Volume's state was changed from <field1> to <field2>.	Field 1: old_value Field 2: certainty_state	• ok • add_pending • modify_pending • remove_pending	Software

Event Name	Event Code	Description	Field	Field Value	Event Category
XMS_DISK_SPACE_SECONDARY_UTILIZATION_LEVEL	20002	XMS Disk space for partition /var/common is <field 1> Kbytes. The disk space utilization state is <field 2>.	Field 1: free_disk_space_secondary	• Integer	Software
			Field 2: disk_space_secondary_utilization_level	• healthy • limited_free_space • very_limited_free_space • no_free_space	
XMS_DISK_SPACE_UTILIZATION_LEVEL	20000	XMS Disk space is <field 1> Kbytes. The disk space utilization state is <field 2>.	Field 1: free_space)	• Integer	Software
			Field 2: disk_space_utilization_level	• healthy • limited_free_space • very_limited_free_space • no_free_space	
XMS_MEMORY_UTILIZATION_LEVEL	20000	XMS memory is <field 1> Kbytes. The memory utilization state is <field 2>.	Field 1: free_memory	• Integer	Software
			Field 2: memory_utilization_level	• healthy • limited_free_memory • no_free_memory	
XMS_WRONG_CN	20001	XMS certificate contains wrong Common Name (CN).	Field 1: wrong_cn_in_csr	• false • true	Software

APPENDIX B

Replacing the Default SSL Certificate

This section provides instructions for replacing the default SSL certificate for the XMS with a certificate issued by a trusted third party (Certificate Authority).

This section includes the following topics:

◆ Overview	536
◆ Creating a CSR	536
◆ Submitting the CSR	537
◆ Converting the Certificate Format	537
◆ Installing the Certificate	538
◆ Installing a Third Party Certificate that was Created without CSR	539

Overview

It is recommended to generate a Certificate Signing Request (CSR) on the XMS and have it signed by a trusted issuer/Certificate Authority to produce a valid certificate.

To replace the default SSL certificate, perform the following procedures:

1. [“Creating a CSR”](#)
2. [“Submitting the CSR”](#) (to sign the certificate request)
3. [“Converting the Certificate Format”](#) (to convert the PEM format to a single-line according to the machine type - Linux or Windows)
4. [“Installing the Certificate”](#)

Creating a CSR

To create a CSR:

1. Log in to the CLI as `admin`.
2. Run the following command to create a CSR. Provide your cluster's hostname as the Common Name:

```
create-server-certificate-signing-request
cert-common-name="cluster-hostname"
```

3. Provide additional optional information for the certificate:

Input Parameter	Description	Value	Mandatory
<code>cert-common-name</code>	Fully qualified domain name	Domain name, e.g. <code>xms.example.com</code>	No
<code>cert-country</code>	Certificate country name	Two letter ISO_3166-1 country code, e.g. US	No
<code>cert-mail</code>	Email address	Email address	No
<code>cert-locality</code>	Locality	String	No
<code>cert-org-name</code>	Organization name	String	No
<code>cert-org-unit-name</code>	Organizational unit name	String	No
<code>cert-state</code>	State or province	String	No
<code>server-key-size</code>	Server key size	Integer between 2048 and 4096	No
<code>server-key-string</code>	Server private key	String	No

Submitting the CSR

To submit the certificate request:

1. Copy the output beginning: -----BEGIN CERTIFICATE REQUEST----- and ending: -----END CERTIFICATE REQUEST----- to a text file and submit it to your Certificate Authority for signing.
2. Verify that the signed certificate is in one of the following formats:
 - Open SSL PEM
 - Base-64 encoded X.509

Note: The resulting signed certificate (usually with a .crt or .cer extension) should start with:-----BEGIN CERTIFICATE-----

Converting the Certificate Format

Note: In the following procedures, if the issuer uses an intermediate/chain certificate, repeat procedures 1-3 for the intermediate/chain certificate as well.

To convert the certificate format on a Linux machine:

1. Log in to your Linux/Unix host or a Windows host with Perl installed.
2. Copy the PEM encoded certificate to a temporary file and save it.
3. If the certificate file was created on a Windows machine, run the dos2unix <certificate name> command.
4. Run the following command:

```
perl -pe 's/\n\\n/g' cert.text >cert_modified.txt
```
5. Copy the file content from your host (if it is Linux/Unix).
6. Verify that:
 - Word wrapping is turned off (to enable a one line output). If there are lines ending with \n, delete them.
 - The line begins with five hyphens.

To convert the certificate format on a Linux machine:

1. Open the certificate file in Notepad++ (or a similar tool).
2. Run a replace command (Ctrl+H) to replace \r\n with \\n. Verify that the extended search mode is selected.

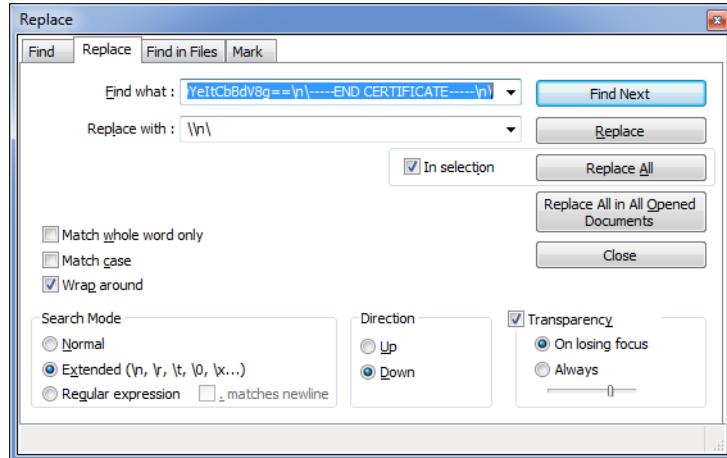


Figure 250 Replace Dialog Box

Installing the Certificate

Run the following command to install the certificate:

```
modify-server-certificate  
server-certificate-string="string>" chain-certificate-string="root certificate>"
```

Note: The `chain-certificate-string` argument **must** be included. If no intermediate certificate is required, leave it as an empty string.

Note: The IP address of the XMS (which should be static) can be added to the Subject Alternative Name field in the certificate itself, in addition to the DNS Name. In this case, the browsers will not display warnings when the XMS is accessed by IP instead of the hostname.

Installing a Third Party Certificate that was Created without CSR

It is possible to create a certificate at the Certificate Authority (CA) without issuing a CSR from the XMS. In this case, the private key does not exist in the XMS and has to be imported as well.

To install a third party certificate without CSR:

Note: Steps 1 to 3 are out of scope of this guide and depend on the CA in use.

1. Generate the certificate at the CA, using the XMS's full DNS name. You can add the XMS IP address to the Subject Alternative Name field in the certificate itself, in addition to the DNS Name.
2. Specify that the Private Key is not password protected.
3. Export the Certificate and Private Key:
 - Open SSL PEM
 - Base-64 encoded X.509

Note: The resulting signed certificate (usually with a `.crt` or `.cer` extension) should start with:-----BEGIN CERTIFICATE-----

4. Convert the certificate and private key. See "[Converting the Certificate Format](#)" on [page 537](#).
5. Run the following command to install the certificate:

```
modify-server-certificate  
server-certificate-string="<one-line modified certificate  
string>" chain-certificate-string="<optional intermediate  
root certificate>" server-key-string="< one-line modified  
key string>"
```

